

Marijo Nižetić, Marija Vrdoljak

LOKALNE I PRISTUPNE MREŽE

Skripta

**SVEUČILIŠNI STUDIJSKI CENTAR
ZA STRUČNE STUDIJE**
STUDIJI ELEKTRONIKE I ELEKTROENERGETIKE

Split, 2010.

Predgovor

Ova skripta nastala je temeljem višegodišnjeg prikupljanja materijala i predavanja kolegija *Lokalne i pristupne mreže* kojeg je pri Sveučilišnome studijskom centru za stručne studije splitskoga sveučilišta održavala dr. sc. Marija Vrdoljak red. prof.. S predavačkih folija prof. Vrdoljak, materijale je u elektronički oblik pretvorio Marijo Nižetić dipl. inž. el., sadašnji predavač kolegija, uz dodatne preinake i intervencije. Cilj ovoga postupka jest zajedničko, udruženo ostvarenje udžbenika za studente navedenoga kolegija.

Za sada, ovo je sirov, neformatiziran materijal kojeg čeka ozbiljan uređivački zahvat. Uz to, materijal se stalno nadopunjuje najnovijim opisima svjetskih dostignuća u predmetnoj problematici s naglaskom na praktičnu iskoristivost novootkrivenih spoznaja. Tehnološki prevladane opisane cjeline neće se izbaciti iz ove skripte nego će se samo prebaciti u poglavlje povijesnoga pregleda (is)korištenih tehnologija.

Posebno naglašavam velik trud koji je prof. Vrdoljak uložila u prikupljanje i slaganje predmetne materije s ciljem brzoga prenošenja najnovijih spoznaja, dostignuća i primjene tehnoloških rješenja sa svjetske i nacionalne razine na razinu proučavanja i praktične poduke studenata našega sveučilišta.

Trajan zadatak je i dalje nastaviti proširivati skriptu po ovakvim principima, ažurno prateći tehnološke promjene, idući ukorak s njima, a sve u cilju kvalitetnoga osiguranja cjeloživotnog učenja i studenata i profesora.

U Splitu: prosinac 2009. godine

Marijo Nižetić

Dodatna literatura:

1. Alen Bažant et. al. *Osnovne arhitekture mreža*, Element - Zagreb, 2003.
2. Annabel Z. Dodd, [*The Essential Guide to Telecommunications*](#), The Third Edition, Copyright © 2001, Pearson Education, Inc, publishing as PRENTICE HALL., INC, ISBN 0130649074
3. Regis J. (Bud) Bates, Donald W. Gregory, [*Voice and Data Communication Handbook*](#), Library of Congress Cataloging-in-Publication Data, McGraw-Hill series on computer communications, 1997, ISBN 0-07-006396-6

SADRŽAJ

1.	LOKALNE MREŽE	1
1.1.	Pristupni mehanizam "Token-Bus"	1
1.2.	Pristupni mehanizam "Token Ring"	1
1.3.	Pristupni mehanizam CSMA/CD.....	2
2.	SUSTAV KLASSE ETHERNET	2
2.1.	Kontroler.....	3
2.1.1.	Primopredajnik	3
2.2.	Primjer primjene lokalne mreže klase Ethernet	3
3.	THE TWIN TOWERS OF KUALA LUMPUR CITY CENTER.....	4
4.	ETHERNET MREŽA - TOPOLOGIJE I PROTOKOLI.....	5
4.1.	Topologije Ethernet mrežaa formati okvira.....	5
5.	ODNOS SLOJEVA ETHERNET PROTOKOLA I OSI MODELA.....	7
5.1.	Identifikacija NIC kartica sustava Ethernet	7
6.	ETHERNET TEHNOLOGIJE	7
7.	PODJELA DSL TEHNOLOGIJA	8
7.1.	Simetrične DSL tehnologije	9
7.2.	Asimetrične DSL tehnologije	10
7.2.1.	Diskretna višetonska modulacija (DMT)	11
7.3.	ADSL Sustavi	12
7.3.1.	Referentni model ADSL sustava	13
7.3.2.	Usluge koje podržava ADSL tehnologija.....	15
7.3.3.	Povezivanje ADSL sustava s informacijskim mrežama.....	16
7.4.	Telefonski razdjelnik.....	18
7.5.	Pristupni multipleksor DSLAM.....	18
7.6.	ADSL modemi	19
7.7.	Protokolarni složaj u ADSL vezi.....	20
8.	USLUGE KOJE PODRŽAVA ADSL SUSTAV	21
8.1.	Usluge poslovnih korisnika	21
8.2.	Usluge kućnih korisnika.....	21
8.2.1.	Pristup Internetu	21
8.2.2.	Video na zahtjev (VoD).....	21
8.3.	1000 Mb/s Ethernet (Gigabitni Ethernet)	23
8.4.	Vrste 1000 Mb/s Ethernet sustava	23
9.	GRADSKA MREŽA ETHERNET (E-MAN)	24
9.1.	Tehnologije gradske mreže (MAN).....	24
9.2.	Značajke i strukture E-MAN mreže	24
10.	ČVOR GRADSKO MREŽE (MAN)	25
10.1.	Nove MAN aplikacije	26
11.	NADOGRADNJA ETHERNET MREŽA	26
11.1.	Uspostava brzih mreža.....	26
11.2.	Nadogradnja Brzog Etherneta ili FDDI mreže radne grupe	27
12.	MOGUĆNOST NADOGRADNJE ETHERNET MREŽA	27
13.	POREDBA PRIVATNIH I VIRTUALNIH PRIVATNIH MREŽA.....	28
13.1.	Privatne mreže.....	28
13.2.	Virtualne privatne mreže.....	29
13.2.1.	Prednosti uporabe virtualne privatne mreže (VPN).....	29
13.3.	Prednosti virtualnih privatnih mreža u poredbi s privatnim mrežama.....	31
13.4.	Vrste virtualnih privatnih mreža	32
14.	VPN TEHNOLOGIJE	34
14.1.	Funkcije ostvarivanja sigurnosti prijenosa podataka	34
14.2.	Ostvarivanje virtualne privatne mreže putem Interneta	39
14.3.	Protokoli razvijeni za VPN	40
14.3.1.	Protokol tuneliranja od točke do točke (PPTP)	40
14.3.2.	Protokol za prosljeđivanje na drugom sloju (L2F)	41
14.3.3.	Protokol tuneliranja na drugom sloju (L2TP)	41
14.3.4.	IP sigurnosni protokol (IPSec).....	42
15.	KOMPONENTE VIRTUALNE PRIVATNE MREŽE.....	43

16.	VPN USLUGA U NAŠOJ ZEMLJI I U SVIJETU	44
16.1.	VPN usluga T-Com: virtualna privatna birana mreža (VPDN)	44
16.2.	VPN usluge u svijetu	46
16.2.1.	Sigurnosni Internet protokol (IPSec)	47
17.	WLAN MREŽA STANDARDA 802.11 b	48
17.1.	Fizički sloj	49
17.2.	Sloj podatkovne veze	50
17.3.	Pridruživanje pristupnim točkama	52
17.4.	Načini rada bežične LAN mreže	53
17.5.	Modulacija	55
17.6.	Oblik okvira	55
17.7.	Konfiguracije bežične LAN mreže	56
17.7.1.	Konfiguracija jedne ćelije	56
17.7.2.	Konfiguracija preklapajućih ćelija	57
17.7.3.	Višećelijska konfiguracija	57
17.7.4.	Višekoračna konfiguracija	58
17.8.	Karakteristike bežične LAN mreže	59
17.8.1.	Domet i pokrivanje	59
17.8.2.	Propusnost	59
17.8.3.	Cjelovitost i pouzdanost	59
17.8.4.	Kompatibilnost s postojećim mrežama	59
17.8.5.	Sposobnost zajedničkog rada bežičnih uređaja	59
17.8.6.	Dozvola za rad	60
17.8.7.	Jednostavnost instalacije	60
17.8.8.	Troškovi instaliranja i održavanja	60
17.8.9.	Sigurnost	60
18.	SPECTRUM 24 WLAN MREŽA	60
18.1.	Pristupna točka (AP)	61
18.2.	Mrežne topologije Spectrum 24 WLAN mreže	61
18.3.	Ćelijsko pokrivanje	64
18.4.	Smjernice za instaliranje WLAN mreže	64
18.5.	Odabir mjesta pristupne točke	64
18.6.	Antene pristupne točke	65
18.7.	Višestruki prijenos	65
18.8.	Konstruktivski materijali zgrade	65
18.9.	Veličina ćelije bežične LAN mreže	66
19.	PROBLEMATIKA PROJEKTIRANJA VELIKE LOKALNE BEŽIČNE MREŽE	66
19.1.	Bežične lokalne mreže	66
19.2.	Projektiranje velike bežične mreže	67
19.3.	Pristup projektiranju bežične mreže	68
19.4.	Postupak izvedbe bežične mreže	68
19.5.	Određivanje početnih lokacija pristupnih točaka	69
19.6.	Postavljanje pristupnih točaka	69
19.7.	Postupak odabira AP lokacija	70
19.8.	Pridruživanje frekvencija pristupnim točkama	73
19.9.	Programski alat za izradu nacrtu	73
20.	LOKALNE MREŽE I UMREŽAVANJE: OSNOVNI POJMOVI	74
20.1.	Uvod	74
21.	LOKALNE I METROPOLITANSKE MREŽE	75
21.1.	Vrste lokalnih mreža	75
21.2.	Osnovno o performansama lokalnih mreža	79
21.3.	LAN protokoli	81
22.	BRZE LOKALNE I METROPOLITANSKE MREŽE	83
22.1.	Pregled važnih arhitektura	83
22.2.	FDDI	83
22.3.	DQDB IEEE 802.6 (dvostruka sabirnica, distribuirani redovi čekanja, kompatibilnost s ATM)	85
22.4.	Ograničenja kod današnjih lokalnih i Metropolitanskih mreža	87
23.	POVEZIVANJE LOKALNIH MREŽA	88
23.1.	Osnovni elementi potrebni za umrežavanje lokalnih mreža	88
23.2.	Uporaba mostova kod povezivanja lokalnih mreža	90
23.3.	Upotreba usmjeritelja	91
24.	PRISTUPNE MREŽE	92
24.1.	Širokopojasni pristup	93

24.2.	Digitalne pretplatničke linije.....	94
24.2.1.	Arhitektura DSL sustava.....	94
24.2.2.	ADSL2.....	95
24.2.3.	ADSL2plus.....	96
24.2.4.	VDSL.....	97
24.2.5.	VDSL2.....	98
24.2.6.	Usporedba DSL tehnologija.....	98
24.3.	Primjena Etherneta u širokopojasnom pristupu.....	99
24.4.	Tehnologije širokopojasnog pristupa.....	101
24.5.	Tehnologije bežičnog optičkog pristupa.....	104
24.6.	Širokopojasni pristup koaksijalnim kabelima.....	104
24.7.	Satelitski širokopojasni pristup.....	105
24.8.	Širokopojasni pristup vodovima elektroenergetske mreže.....	106
24.9.	Širokopojasni fiksni bežični pristup.....	107
24.9.1.	WiMAX.....	108
24.9.2.	Ostale bežične pristupne tehnologije.....	110
24.10.	Stanje širokopojasnog pristupa Internetu u zemljama EU-a.....	111
24.11.	Usluge s dodanom vrijednošću i IPTV.....	114

1. LOKALNE MREŽE

Lokalna mreža, LAN (*Local Area Network*) je komunikacijska mreža koja omogućava međusobno povezivanje terminala, osobnih računala, periferne opreme, telefona, senzora, video-predajnika i prijemnika, faksimila i slične opreme na malom prostoru (unutar jedne ili više zgrada).

Zahtjevi koji se postavljaju na lokalne mreže su:

- relativno visoka brzina prijenosa podataka,
- mogućnost priključenja nekoliko stotina računala na zajednički komunikacijski kanal,
- mogućnost osiguravanja najjednostavnijih mehanizama koji imaju zahtijevanu funkcionalnost i performanse,
- dobre osobine u pogledu učestalosti pogrešaka u prijenosu podataka i dobru pouzdanost,
- kompatibilnost, odnosno mogućnost povezivanja uređaja različitih proizvođača u mrežu,
- efikasno korištenje komunikacijske mreže,
- stabilnost pod velikim opterećenjem,
- lako realiziranje pristupa svim korisnicima, sustava,
- lako instaliranje malih sustava i mogućnost njihova proširenja,
- lako ostvarivanje rekonfiguracije mreže i lako održavanje,
- niska cijena.

Tri glavne tehnološke osobine lokalnih mreža su:

- topologija mreže,
- prijenosni medij,
- tehnika kontrole pristupa mediju.

Osnovne topologije lokalnih mreža jesu:

- zvijezda,
- prsten,
- sabirnica i
- stablo.

Prijenosni medij može biti: upleteni dvožični kabel, koaksijalni kabel i optičko vlakno.

Izbor prijenosnog medija ovisi o:

- udaljenosti između stanica (maksimalno 2 km)
- potrebnoj brzini prijenosa (standardno u području reda veličine Mb/s do reda veličine Gb/s)

Kao tehnike kontrole pristupa prijenosnom mediju u mrežama LAN najčešće se koriste tri standardizirana rješenja: "*Token-Bus*", "*Token Ring*" i CSMA/CD.

1.1. Pristupni mehanizam "*Token-Bus*"

- stanice formiraju logički prsten (tako da nakon zadnje stanice na sabirnici slijedi prva) i fizički su spojeni na sabirnicu;
- logički redosljed stanica neovisan je o fizičkom rasporedu;
- svaka stanica poznaje prethodnu i sljedeću stanicu u nizu;
- pristup mediju definiran je pomoću upravljačkog okvira, tzv. *token*;
- za vrijeme posjedovanja okvira, stanica može sama odašiljati pakete podataka;
- stanici prestaje pravo na pristup u sljedećim uvjetima:
 - stanica je bez pripremljenih paketa namijenjenih odašiljanju,
 - stanica je odaslala sve pripremljene pakete,
 - isteklo je maksimalno vrijeme.

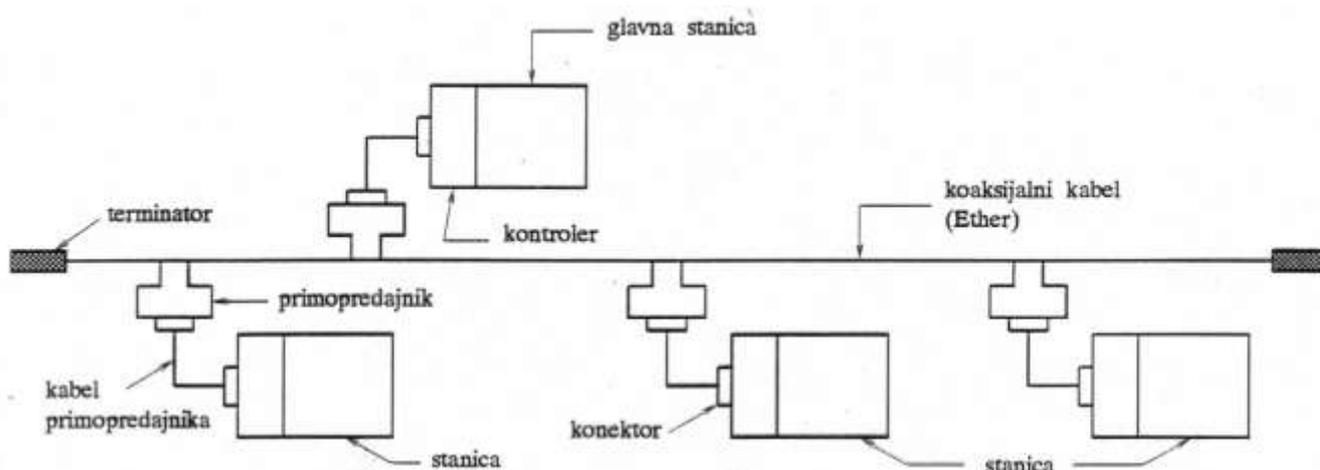
1.2. Pristupni mehanizam "*Token Ring*"

- blok posebno odabranih bitova (*token*) putuje prstenom;
- stanica koja želi odašiljati, čeka na *token*;
- kada *token* naiđe, stanica ga prihvaća uz promjenu jednog bita u njemu, čime on postaje početni dio okvira koji stanica dalje popunjava podacima;
- nakon ove transformacije *token* više ne postoji u prstenu;
- ostale stanice nemaju pristup dok se ne ispune oba sljedeća uvjeta:
 - stanica je završila s prijenosom svog okvira,
 - početni dio odašlanog okvira, nakon obilaska prstenom, ponovno je došao do polazne stanice.

1.3. Pristupni mehanizam CSMA/CD

- metoda višestrukog pristupa otkrivanjem nosioca s detekcijom sudara, CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*);
- pristup u mehanizmu CSMA/CD je slučajan;
- stanica koja želi komunikaciju "osluškuje" stanje medija i ponaša se po sljedećim pravilima:
 - ako je medij slobodan, odašilje,
 - ako je medij zauzet, osluškuje dok se medij ne oslobodi,
 - ako pri odašiljanju dođe do "sudara", čeka slučajno odabrano vrijeme i ponovno odašilje.

2. SUSTAV KLASKE ETHERNET



Slika 1. Tipična Ethernet implementacija

Osnovni elementi ove lokalne mreže su:

- zajednički prijenosni medij, tj. koaksijalni kabel maksimalne dužine 500 m bez repetitora, odnosno Ethernet koaksijalni kabel dužine 2500 m s repetitorima;
- stanice, kontroleri kabela primopredajnika i primopredajnici.

2.1 Stanica

- osnovni uređaj komunikacijskog sustava koji se može adresirati;
- nije priključena izravno na prijenosni sustav već pristup ostvaruje preko kontrolera i sučelja između kontrolera i prijenosnog sustava;
- u povezivanju stanica u mrežu terminala uvijek je jedna određena stanica centralna (primarna), dok su ostale periferne (sekundarne);
- centralna stanica (računalo ili koncentrator) upravlja komunikacijom u svim fazama u smjeru prema perifernim stanicama;

2.1. Kontroler

Kontroler je sučelje za računalo; a obavlja funkcije za pristup zajedničkom komunikacijskom kanalu:

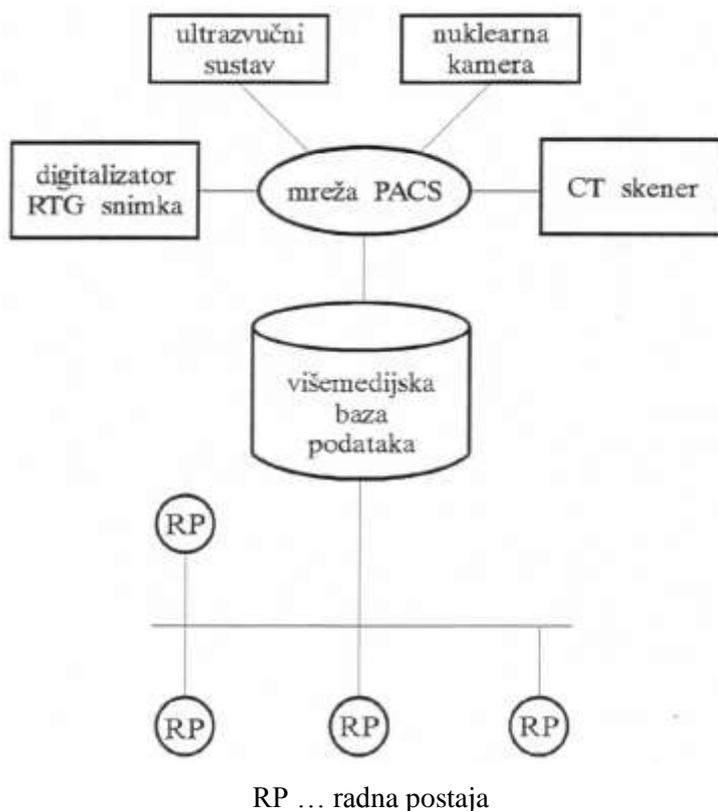
- konverziju signala,
- kodiranje i dekodiranje,
- serijsko-paralelnu konverziju,
- prepoznavanje adrese,
- otkrivanje pogrešaka,
- privremeno pohranjivanje poruka,
- CSMA/CD upravljanje kanalom,
- formiranje transmisijskih paketa.

2.1.1. Primopredajnik

Primopredajnik je jednostavan sklop koji povezuje kontroler sa zajedničkim komunikacijskim kanalom nazvanim Ether i obavlja sljedeće funkcije:

- prenosi podatke od kontrolera u zajednički komunikacijski kanal,
- prenosi podatke iz zajedničkog kanala u kontroler,
- otkriva prisutnost signala u zajedničkom kanalu kojega odašilje neko drugo računalo,
- otkriva sudar koji nastupa kada dva ili više računala istovremeno zaposjedaju zajednički kanal,
- napaja prijenosni sustav.

2.2. Primjer primjene lokalne mreže klase Ethernet



Slika 2. Bolnički komunikacijski sustav

Bolnica je tipična sredina u kojoj se može primijeniti lokalna mreža za prijenos slike, govora i podataka. Jedan takav bolnički komunikacijski sustav prikazan je na slici 2.

Unutar bolnice danas se koristi mreža za prijenos i pohranu slika, PACS (*Picture Archiving and Communication System*), koja se temelji na tehnologijama lokalnih mreža, a predstavlja prvu fazu u razvoju širokopojasne medicinske komunikacijske mreže.

U području medicinskih komunikacija, radi se na razvoju raznih standarda koji definiraju prijenos medicinskih slika između uređaja za akviziciju slike te uređaja za reprodukciju i pohranjivanje. Proučavaju se različite konfiguracije sustava za prijenos RTG slika preko konvencionalnih lokalnih mreža korištenjem CSMA/CD metode pristupa prijenosnom mediju.

Prostorna i kontrastna rezolucija dva su važna parametra koja karakteriziraju jednu sliku. Prostorna rezolucija odgovara produktu broja horizontalnih i vertikalnih piksela¹. Kontrastna rezolucija predstavlja broj sivih nijansi ili broj boja kojima se mogu prikazati pojedini pikseli: Broj mogućih boja ili nijansi kreće se u opsegu od 256 za 8 bita/pikselu do 16.777.216 za 24 bita/pikselu. Budući da su slike koje se prenose ovom lokalnom mrežom visoke rezolucije, jedan je od glavnih problema pronalaženje slike u memoriji i njeno reproduciranje na monitoru radne postaje s minimalnim kašnjenjem.

U centralnu memoriju sustava pohranjuju se dvije verzije RTG slika, i to slike od 1024×1024 piksela za normalu reprodukciju i slike od 2048×2048 piksela, za reprodukciju uvećanja pojedinog dijela slike (obje imaju istu kontrastnu rezoluciju). Kada se izda zahtjev za reprodukciju slike tada se slika od 1024×1024 piksela poziva iz memorije i trenutno prikazuje na monitoru radne postaje. U slučaju zahtjeva za uvećavanjem pojedinog dijela slike, prenosi se ekvivalentni podatak verzije 2048×2048 piksela iste slike od centralne memorije do radne postaje.

Očito je da komunikacija slikama zahtijeva prijenos velike količine podataka. Ova se količina ne smije smanjivati korištenjem kompresije, jer ona dovodi do smanjivanja kvalitete slike, a to može rezultirati pogrešnom dijagnozom.

Smanjivanje potrebne pojasne širine prijenosnog medija postiže se tehnikom "predusmjeravanja». Ona podrazumijeva pohranu slika u lokalne memorije radnih postaja, čime se rasterećuje prijenosni medij.

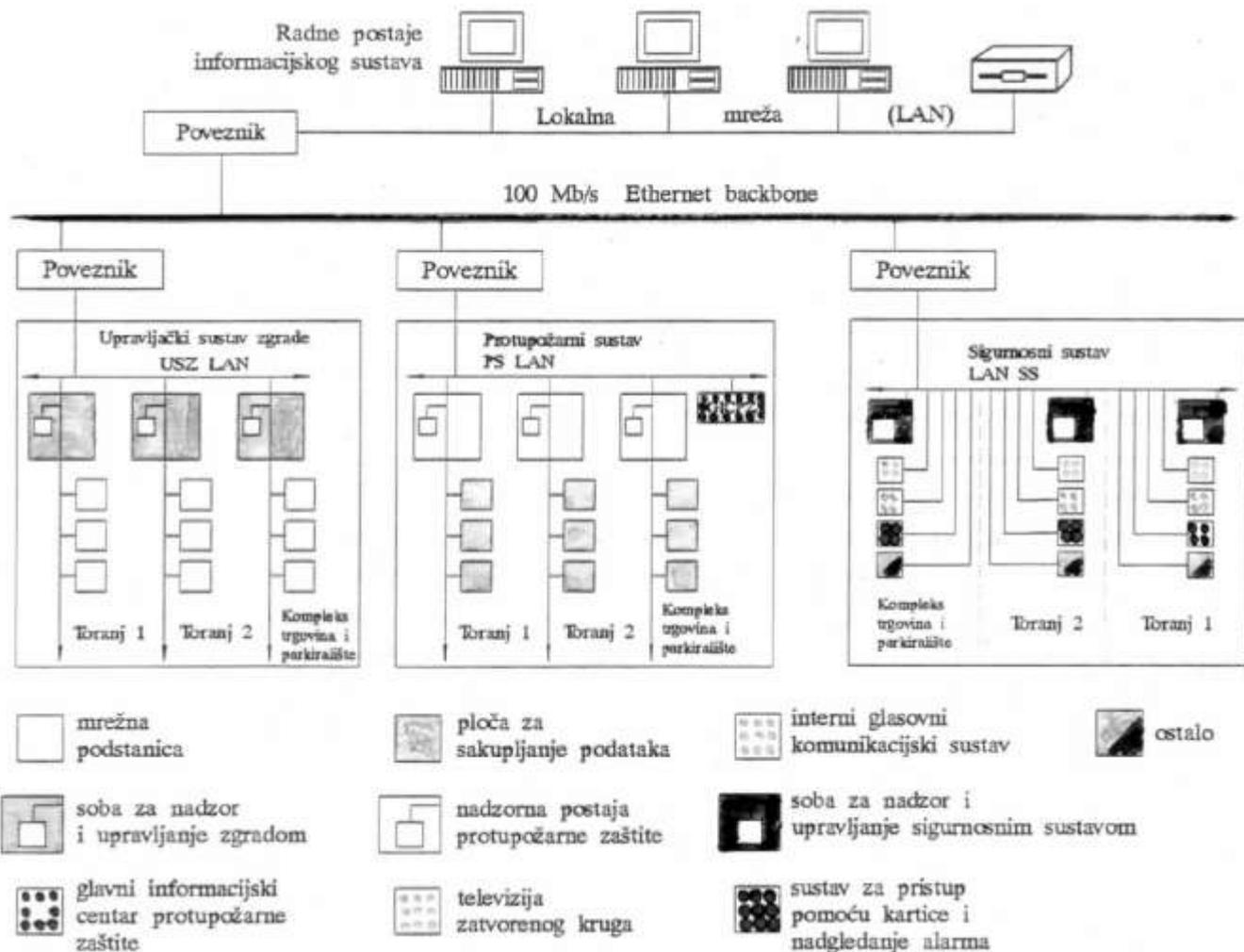
Da bi se RTG snimak mogao pohraniti u višemedijsku bazu podataka potrebno ga je digitalizirati. Uređaji koji vrše digitalizaciju RTG snimaka, tj. mirne slike, koriste tehniku faksimila. Faksimil podrazumijeva prijenos mirnih slika, teksta, crteža i natpisa reprodukcijom crno-bijele boje i tonova sive boje. Crno-bijela slika može se predstaviti kao skup diskretnih elementarnih površina, pri čemu svaka od njih ima jednu nijansu u spektru. Nijanse se kreću od bijele preko sive do crne.

Dokument, tj. mirna slika, skenira se svjetlosnim snopom koji je fokusiran sustavom leća. U zavisnosti od toga je li analizirani element površine slike svjetliji ili tamniji, dobiva se veći ili manji intenzitet reflektirane svjetlosti. Nakon toga se reflektirana svjetlost sustavom leća usmjerava na svjetlosno-električni pretvarač, foto sklop. Posredstvom foto sklopa dobiva se električni signal koji je vjerna slika skenirane linije te on predstavlja modulirajući signal. Ovo je osnovni princip rada faksimila.

3. THE TWIN TOWERS OF KUALA LUMPUR CITY CENTER

- poslovna zgrada malezijske naftne kompanije *Petronas*,
- jedna od najviših zgrada na svijetu (450 m, 88 katova)
- "Inteligentna zgrada" - zgrada opremljena komunikacijskim sustavom i ostalim automatski upravljanim sustavima koji s minimalnom potrošnjom energije pružaju maksimalnu udobnost i sigurnost.
- Komunikacijski sustav mora omogućavati: usluge konvencionalne telefonije, komunikaciju podacima, video-konferenciranje, elektroničku poštu i drugo.

¹ Piksela je najmanji element na koji se može razlučiti sliku. Kod sivih slika to je sjajnost jedne točke, a kod slika u boji to je sjajnost triju primarnih boja koje zajedno daju boju te točke.



Komunikacijski sustav obuhvaća tri posebne lokalne mreže:

- LAN za nadzor i upravljanje sigurnosnim sustavom
- LAN za nadzor i upravljanje sustavom protupožarne zaštite
- LAN za upravljanje zgradom (rasvjeta, dizala, klima-uređaji)

Ove tri mreže međusobno povezuje četvrta - sveobuhvatna lokalna mreža informacijskog sustava zgrade (100 Mb/s *Ethernet backbone*).

4. ETHERNET MREŽA - TOPOLOGIJE I PROTOKOLI

Za rad Ethernet sustava definirane su tri prijenosne brzine:

- 10 Mb/s - 10 Base-T Ethernet
- 100 Mb/s - brzi Ethernet
- 1000 Mb/s - Gigabitni Ethernet

Ethernet sustav temelji se na CSMA/CD protokolu.

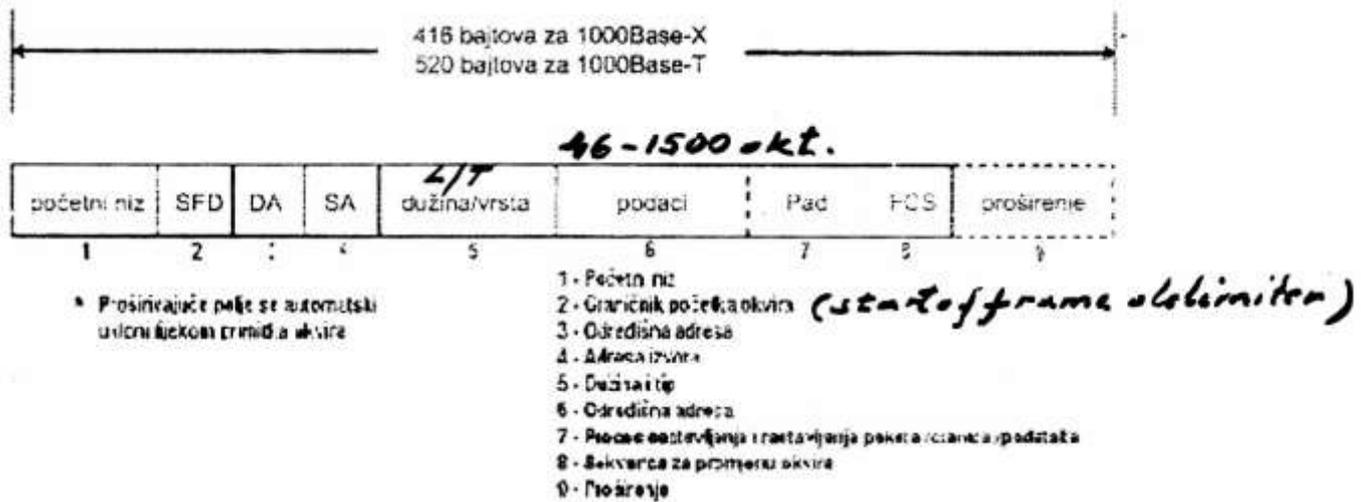
Osnovne značajke protokola CSMA/CD:

- jednostavna i jeftina implementacija.
- velika topološka fleksibilnost,
- uspješno povezivanje i rad standardom usklađenih proizvoda bez obzira na proizvođača.

4.1. Topologije Ethernet mrežaa formati okvira

- sabirnica

- zvijezda s prospojnikom kao centralnom mrežnom jedinicom
- prsten.



Slika 1. MAC okvir s proširivajućim poljem za gigabitni prijenos

MAC okvir sadrži:

- sedam polja i
- proširivajuće nepodatkovno polje koje se dodaje okvirima kraćim od 46 okteta minimalne dužine pri gigabitnom prijenosu da bi ga ostale stanice mogle primijeniti.

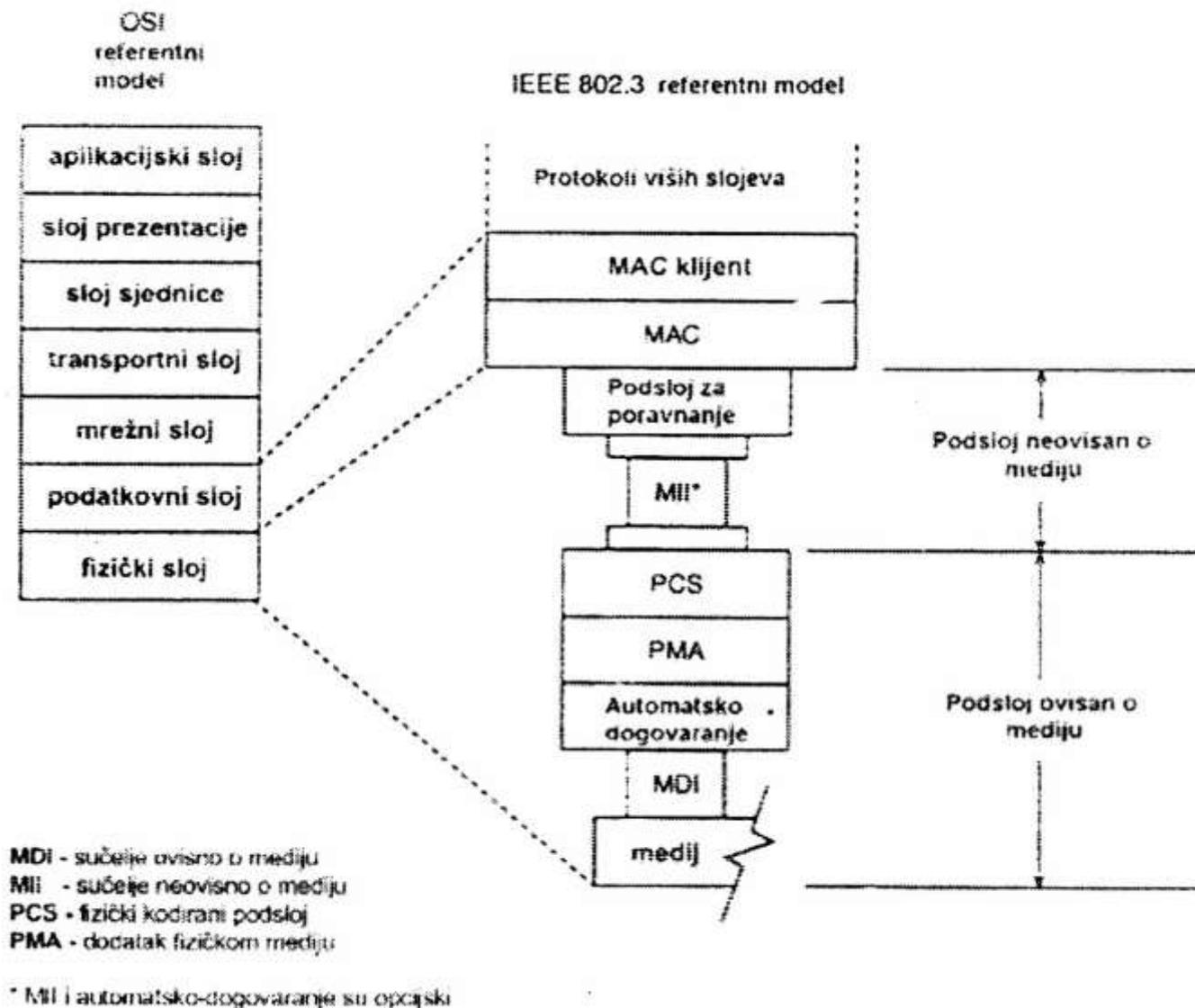
Parametar	10 Mb/s	100 Mb/s	1000 Mb/s
Minimalna veličina Minimalna okvira	74 bajta	74 bajta	520 bajtova
Maksimalni promjer sudara (DTE to DTE)	100 m UTP	100 m UTP; 412 m optičkog vlakna	100 m UTP; 316 m optičkog vlakna
Maksimalni promjer domena sudara s repetitorima	2500 m	205 m Smanjenje promjera zbog uočljivosti sudara	200 m Proširenje s nepodatkovnim poljem ako bi se zadržalo maksimalan promjer
Maksimalni broj repetitora u mrežnoj stazi	5	2 smanjenje	1

Tablica 1. Ograničenja za poludupleksni rad

Načini prijenosa:

- poludupleksni, .obosmjerni neistodobni prijenos,
- potpuno dupleksni, (funkcionalno jednostavniji, jer ne uključuje natjecanje za prijenosni medij, CSMA/CD) – dvosmjerni istodobni.

5. ODNOS SLOJEVA ETHERNET PROTOKOLA I OSI MODELA



Slika 2. Odnos slojeva Ethernet protokola i OSI modela

- Fizički sloj IEEE 802.3 odgovara OSI fizičkom sloju

Sloj podatkovnog linka IEEE 802.3 dijeli se na:

- podsljov nadzora pristupa mediju, MAC (*Media Access Control*)
- MAC - klijent podsljov:
 - podsljov nadzora logičkog linka, LLC (*Logical Link Control*)
 - prenosni entitet (*Bridge Entity*).

5.1. Identifikacija NIC kartica sustava Ethernet

Trodijelni naziv proizvoda temeljen na atributima fizičkog sloja:

- 10Base-T = 10 Mb/s, osnovni frekvencijski pojas, prijenos preko dvije UTP parice,
- 100Base-T4 = 100 Mb/s, osnovni frekvencijski pojas, prijenos preko četiri UTP parice.

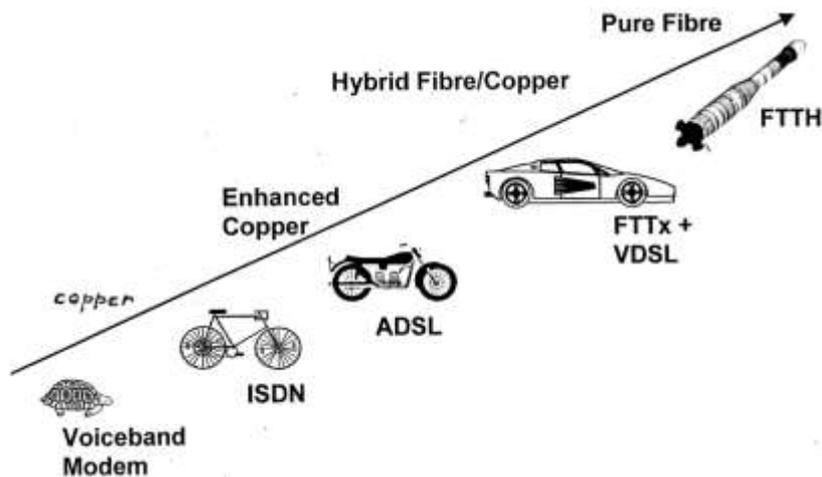
6. ETHERNET TEHNOLOGIJE

Tablica 2. Usporedba osnovnih značajki fizičkog sloja različitih Ethernet sustava

Ethernet verzija	Količina podataka	Kôd	Kabliranje	Potpuno dupleksni rad
10Base-T	10 MBd	Manchester	dvije parice UTP kabela kategorije 3 ili boljeg	podržava
100Base-X	125 MBd	4B/5B	dvije parice UTP kabela kategorije 5 ili Tip 1 STP ili boljeg	Podržava 1995
100Base-T4	33 MBd	8B/6T	četiri parice UTP kabela kategorije 5 ili boljeg (2)	Ne podržava 1995
100Base-T2	25 MBd	PAM 5x5	dvije parice UTP kabela kategorije 5 ili boljeg	Podržava - poluduplex 1997

Postoje tri standarda fizičkog sloja za 100 Mb/s Ethernet:

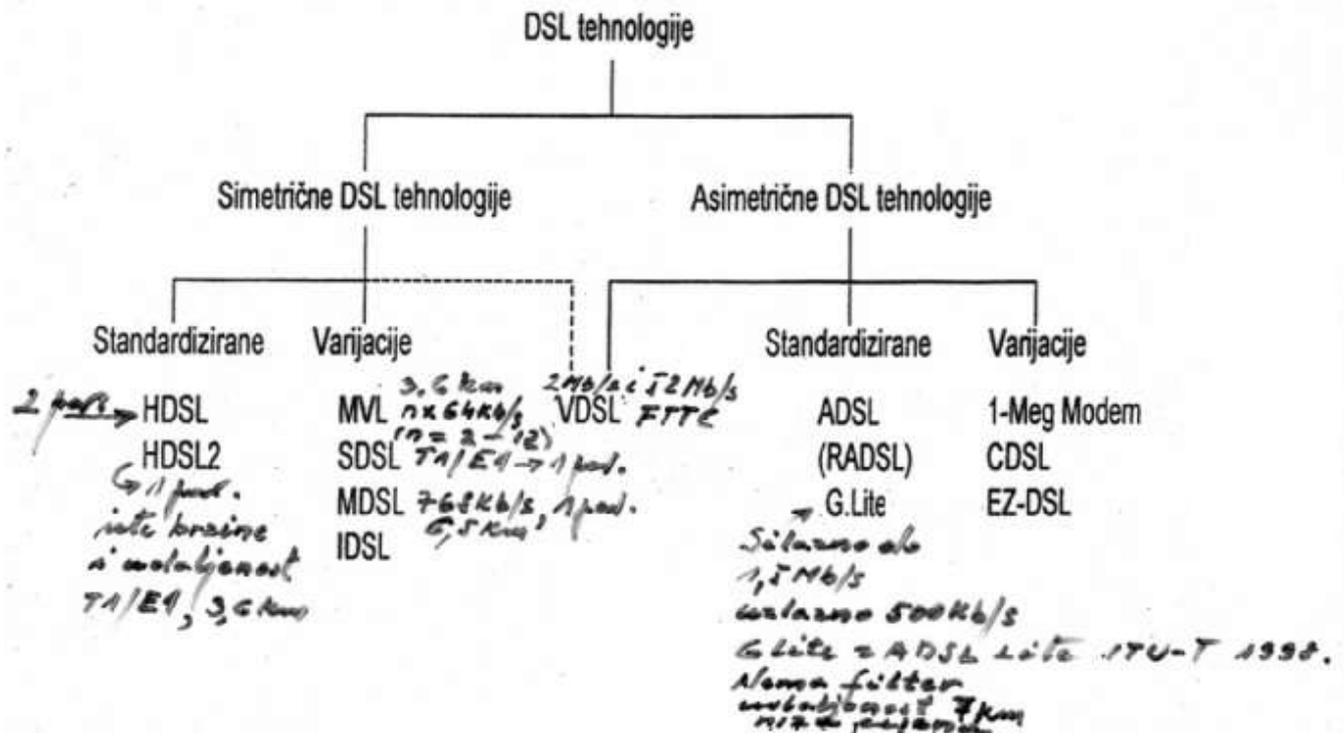
- 100Base-X
- 100Base-T4
- 100Base-T2



Slika x.y Razvitak pristupnih mreža

7. PODJELA DSL TEHNOLOGIJA

XDSL je zajednički akronim za grupu prijenosnih tehnologija koje povećavaju efikasnost uporabe postojećih bakrenih parica u pretplatničkoj petlji i omogućuju uvođenje širokopoljnih usluga prema krajnjim korisnicima. Do danas je razvijeno ili se još razvija desetak xDSL prijenosnih tehnologija.



Slika 2.1 Podjela DSL tehnologija

Ove se tehnologije - ovisno o vrijednostima brzina prijenosa informacija od krajnjeg korisnika, odnosno prema krajnjem korisniku – mogu podijeliti u dvije glavne skupine:

- skupinu simetričnih DSL tehnologija koje omogućuju istu brzinu prijenosa podataka u oba smjera i,
- skupinu asimetričnih tehnologija kod kojih brzina prijenosa podataka ovisi o smjeru prijenosa.

7.1. Simetrične DSL tehnologije

Digitalna pretplatnička linija velike podatkovne brzine (HDSL) je najčešće upotrebljavana prijenosna tehnologija simetrične DSL skupine koja omogućuje brzine prijenosa T1 (1,5 Mb/s), odnosno E1 (2 Mb/s) po cijeni koje su niže od cijena za klasične iznajmljene T1 ili E1 linije. Za razliku od ostalih xDSL tehnologija HDSL upotrebljava dvije bakrene parice i ne prenosi POTS signal. Napredak na području digitalne obrade signala (ponišćavanje jeka i primjena modulacijskih postupaka omogućuje značajno smanjivanje pojasne širine T1, odnosno E1 HDSL linija u odnosu na klasične T1, odnosno E1 iznajmljene linije). Zavisno o duljini bakrene parice T1-HDSL zahtijeva pojasnu širinu u opsegu od 80-240 KHz, dok je za klasičnu iznajmljenu T1 liniju potrebna pojasna širina od 1,5 MHz. Maksimalna duljina bakrenih parica na kojoj HDSL tehnologija može funkcionirati je 3,66 km pri čemu se upotrebljava 2B1Q linijsko kodiranje. HDSL «dubler» može povećati ovu duljinu na 7,32 km, pri čemu otpor petlje mora biti manji od 900 Ω, a ukupno prigušenje manje od -35 dB. Očekuje se da će HDSL2 za razliku od HDSL tehnologije zahtijevati samo jednu bakrenu paricu za prijenos podataka istom brzinom na istu udaljenost.

Osim standardiziranih simetričnih DSL tehnologija prijenosa, HDSL skupina uključuje i druge varijacije ove skupine.

Višestruka virtualna linija, MVL (*Multiple Virtual Line*) je komercijalno rješenje tvrtke *Paradyne* koje omogućuje brzine prijenosa od 128 kb/s do 768 kb/s, pri čemu brzine prijenosa mogu biti $N \times 64$ kb/s ($N = 2 \dots 12$). Za razliku od HDSL, odnosno HDSL2 prijenosne tehnologije MVL imaju mogućnost prijenosa POTS signala bez uporabe razdjelnika koji odvaja analogni govorni pojas od prijenosa podataka.

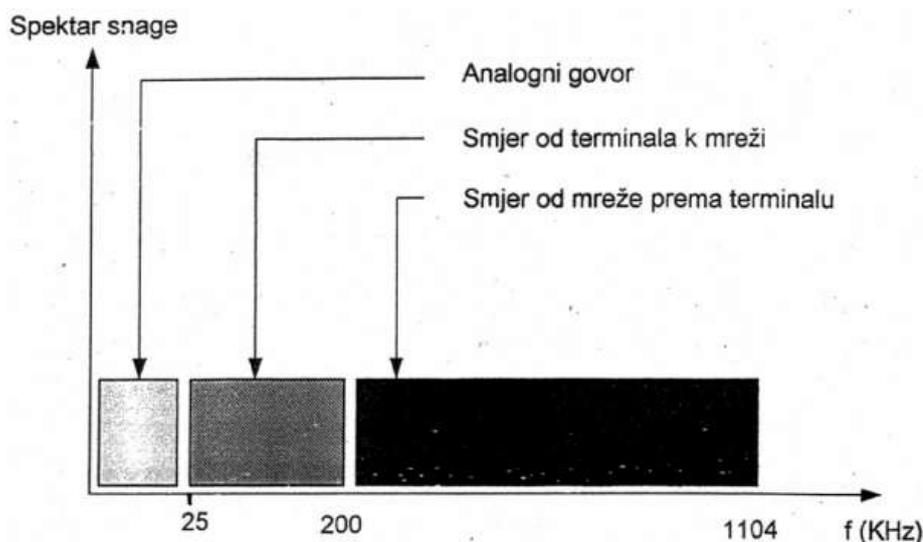
Digitalna pretplatnička linija s jednom bakrenom paricom, SDSL (*Single Line DSL*) omogućuje prijenos podataka brzinama koje mogu biti 768 kb/s ili T1/E1 pri čemu se upotrebljava samo jedna parica. Otpor bakrene parice mora biti manji od 900 Ω , a ukupno gušenje SDSL linije mora biti manje od -35 dB.

Digitalna pretplatnička linija smanjene brzine prijenosa, MDSL (*Moderate Bit Rate DSL*) omogućuje brzinu prijenosa podataka od 768 kb/s preko jedne bakrene parice na udaljenost od 6,41 km. ISDN digitalna pretplatnička linija (IDSL) se može priključiti na ISDN komutaciju. SDSL, MDSL i IDSL ne podržavaju analogne telefonske linije u pristupnoj mreži.

7.2. Asimetrične DSL tehnologije

ADSL tehnologija ima najveći domet od svih xDSL tehnologija. ADSL tehnologija je nastavak razvitka HDSL tehnologije. Za razliku od HDSL-a, primjenom ADSL tehnologije ostvaruje se nesimetrični promet koji je veći od mreže prema terminalu nego od terminala prema mreži. Asimetrični prijenos s većim kapacitetom u dolaznom smjeru prilagođen je novim uslugama (pretraživanje po Internetu, video na zahtjev, kupovanje na daljinu i drugo), pri čijim ostvarivanjima korisnik pristupa poslužitelju preko javne mreže. Korisnik šalje kratke upite poslužitelju; Zavisno od upita poslužitelj odgovara dužim porukama u obliku datoteka podataka, digitalnih zvukova, digitalnih slika ili video snimaka.

ADSL je učinkoviti način prijenosa za ostvarivanje ponude multimedijских usluga krajnjem korisniku preko postojeće lokalne petlje. Slika 2.2 prikazuje kako se pojasna širina lokalne petlje upotrebljava u ADSL sustavu.



Slika 2.2. ADSL frekvencijski spektar

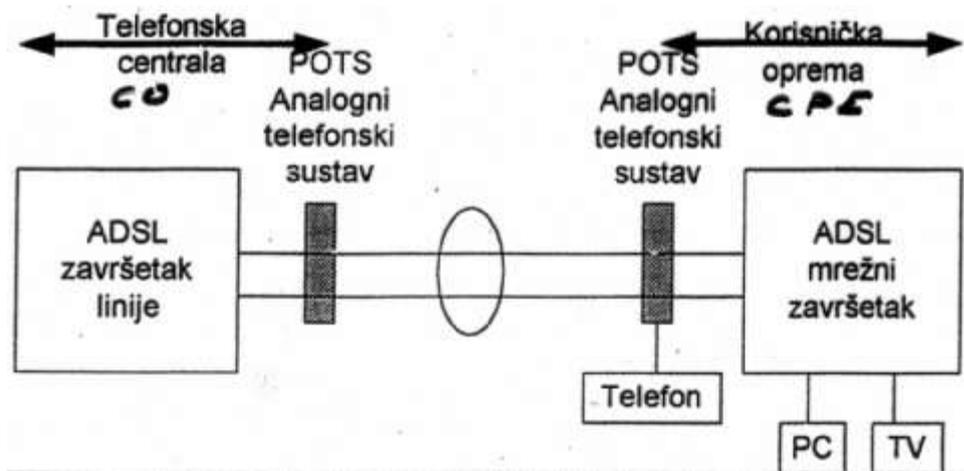
Međutim, preslušavanje je jedan od najznačajnijih ograničavajućih čimbenika za digitalni prijenos u lokalnoj petlji: Pri primjeni ADSL tehnike preslušavanje na daljem kraju, FEXT (*Far End Cross-Talk*) je dominantno preslušavanje. Preslušavanje na bližem kraju, NEXT (*Near End Cross-Talk*) se izbjegava odvajanjem smjera prijenosa od terminala prema mreži od smjera mreža - terminal u frekvencijskoj domeni.

Donji i gornji dio pojasne širine upotrebljava se za uzlazni odnosno silazni smjer prijenosa (slika 2.2). Frekvencijsko područje od 0 do 4 KHz upotrebljava, POTS (*Plain Old Telephone System*) analogni telefonski sustav.

Drugim riječima frekvencijsko područje između 25 i 200 KHz upotrebljava se za prijenos zahtjeva od korisnika do poslužitelja U ovom frekvencijskom području mogu se ostvariti brzine do 640 kb/s.

Dio spektra od 200 KHz do 1104 KHz služi za prijenos zahtjevnijih usluga od poslužitelja do korisnika.

Tehnike kompresije primjenom standarda MPEG 2 za video i audio kompresiju u današnje vrijeme ograničava brzinu video signala na 2 – 4 Mb/s. Stoga se dva MPEG-2 komprimirana signala mogu prenijeti do korisnika uporabom ADSL pristupne linije. Slika 2.3. prikazuje ADSL pristupnu liniju.



Slika 2.3. ADSL pristupna linija

Iz slike 2.3. vidi se, da se jedna upletena parica upotrebljava između telefonske centrale, CO (*Central Office*) i korisničke opreme, CPE (*Customer premises Equipment*). ADSL modemi postavljaju se na oba kraja linije.

U ADSL sustavu primjenjuju se dvije vrste modulacije:

- amplitudna modulacija bez nosioca (potisnuti nositelj)/fazna modulacija, CAP (*Carrier-less Amplitude Modulation/Phase Modulation*), i
- diskretna višetonjska modulacija, DMT (*Discrete Multi-tone Modulation*).

7.2.1. Diskretna višetonjska modulacija (DMT)

Standardom diskretne višetonjske modulacije frekvencijski pojas lokalne petlje analognog sustava od 1,1 MHz (počevši od 0 Hz) dijeli se na 256 podnosioca (*sub-carriers*) koji se često nazivaju podkanali. Svaki podkanal ima pojasnu širinu od 4,3125 KHz, što ukupno iznosi 1,104 MHz. Neki podkanali imaju specijalne namjene, a neki se uopće ne upotrebljavaju. Primjerice, kanal 64 na 276 kHz je rezerviran za prijenos pilotskih signala.

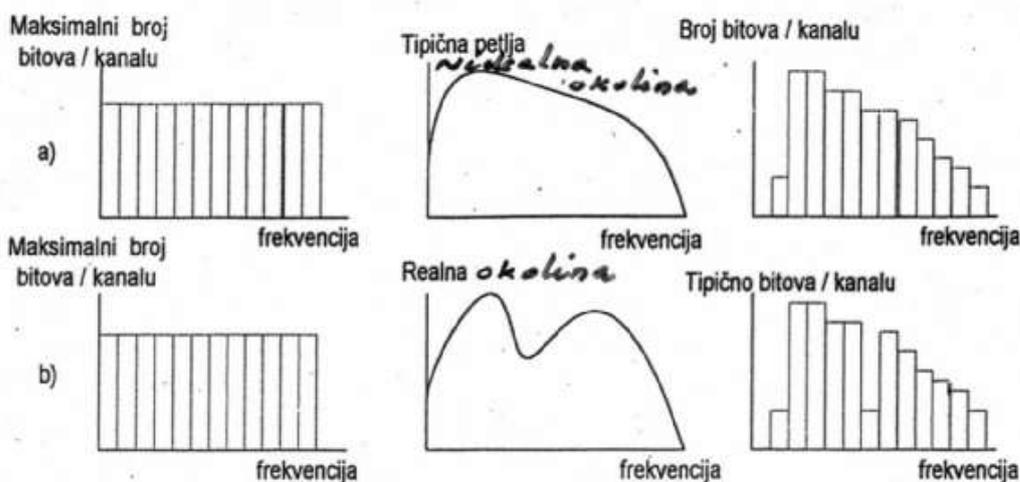
U većini DMT sustava upotrebljava se samo 250 ili 249 podkanala za prijenos informacija. Niži podkanali, 1 do 6, u većini slučajeva rezervirani su za prijenos 4 KHz analognog govornog signala. Kako $6 \times 4,3125 \text{ KHz}$ iznosi 25,876 KHz, to znači da se 25 KHz uzima kao najniža frekvencija u ADSL uslugama. Pri tome postoji zaštitni pojas između analognih govornih kanala i kanala za prijenos DMT signala. Napomenimo i to, da su gubici snage signala na frekvencijama 250-tog i viših kanala tako visoki, da ih je teško upotrijebiti za prijenos informacija u dugoj pretplatničkoj petlji.

Postoje 32 uzlazna (*upstream*) i 250 silaznih (*downstream*) kanala, što znači da je prijenos u sustavima asimetričan. Uzlazni kanali obično počinju s kanalom broj 7. Kao što je rečeno pojasna širina svakog podkanala iznosi 4,3125 KHz i samo onda kada se primjenjuje poništavanje jeke postoji 250 silaznih podkanala. Kada se primjenjuje samo FDM za nadzor jeke tada tipično postoje 32 uzlazna podkanala i 218 ili manje silaznih podkanala, jer u ovom slučaju nema prekrivanja podkanala.

Kao što je već rečeno uzlazni kanali zauzimaju niži dio spektra iz dva razloga. Prigušenje signala u ovom dijelu spektra je manje i pretplatnički predajnik je napajan nižom snagom od predajnika lokalne centrale. Drugi je razlog što u lokalnoj centrali postoji veći šum i mogućnost preslušavanja, pa je razumno upotrijebiti niži dio frekvencijskog područja za prijenos uzlaznih signala. Kada je ADSL sustav, koji primjenjuje DMT modulacijsku tehniku, aktivan, krajnji uređaji ispituju prigušenje u svakom podkanalu; a također i šum.

Kao što je spomenuto svi se podkanali ne upotrebljavaju za prijenos informacija. Neki su rezervirani za upravljanje mrežom i za mjerenje performanse. Primjerice, u silaznom smjeru upotrebljava se samo 249 od 256 podkanala za prijenos informacija. U svakom od podkanala primjenjuju se vlastite tehnike kodiranja temeljene na QAM modulaciji. Stvarna prednost DMT tehnike je što primjenom praćenja performanse (koja se temelji na toj tehnici) ima za posljedicu više bita o kanalu u nekim podkanalima, a ukupna je propusnost sustava jednaka sumi svih bitova u aktivnim podkanalima. Treba naglasiti da se u ADSL sustavima u kojima se primjenjuje DMT, stalno prati performansa, odnosno pogreške.

Brzina pojedinog i grupe podkanala može varirati, pri čemu DMT osigurava granularnost od 32 kb/s. Drugim riječima, DMT uređaj može djelovati na 768 kb/s tj. na brzini nižoj za 32 kb/s, što ovisi o uvjetima radne okoline. Međutim, CAP uređaj omogućuje granularnost od 340 kb/s (768 kb/s ili 428 kb/s), dok čista QAM osigurava granularnost tako finu kao što je 1 b/s. Napomenimo i to; da neki proizvođači oglašavaju da njihovi ADSL uređaji temeljeni na CAP mogu također osiguravati granularnost od 32 kb/s: Stručnjaci smatraju da je finija granulacija prednost koja može utjecati na prihvaćanje i uporabu sustava od strane korisnika.



Slika 2.4. Djelovanje diskretne višetonske tehnologije u pretplatničkoj petlji sustava ADSL

Iz slike 2.4a vidi se odraz stanja u ADSL sustavu, koji djeluje u skoro idealnoj sredini, a duljina bakrene parice iznosi 5.48 km. Jedino prigušenje u sustavu je uzrokovano propagiranjem signala (slika 2.4.a) koje ovisi o duljini parice i frekvenciji signala. Slika 2.4.b prikazuje djelovanje sustava, tj. tipičnu petlju u realnoj okolini. Razmotrimo najprije sliku 2.4.a. Dijagram na lijevoj strani prikazuje maksimalan broj bita u sekundi po kanalu koji bi uređaj trebao odašiljati i primiti. Međutim, iz dijagrama u sredini vidi se stanje u tipičnoj petlji. Dijagram prikazuje vrijednost prigušenja koje se mijenja ovisno o frekvenciji. Na višim frekvencijama je efekt udaljenosti dominantan. Na nižim frekvencijama dominantni su utjecaji impulsnog šuma i preslušavanja. Iz ovog dijagrama vidi se također da u srednjem dijelu frekvencijskog područja (25 KHz do 1,1 MHz) pojačanje signala lagano pada povećanjem frekvencije.

Važno je naglasiti da DMT uređaj može mjeriti pojačanje u svakom podkanalu i podešavati stvaran broj bita u sekundi po kanalu u skladu sa stvarnim profilom linijskog pojačanja, što je vidljivo iz gornjeg desnog prikaza (slika 2.4.a). Dijagram u sredini slike 2.4.b prikazuje realni profil pojačanja petlje, a desni dijagram na ovoj slici pokazuje svojstvenu adaptivnost u svakom pojedinom kanalu DMT uređaja u skladu s profilom stvarnog linijskog pojačanja. Stoga je razumljivo da se DMT-ADSL sustav naziva ADSL s adaptivnom brzinom, RADSL (*Rate Adaptive ADSL*). Drugim riječima, DMT adaptira brzinu bitova svakoga kanala u skladu s omjerom S/N u danom spektralnom području.

7.3. ADSL Sustavi

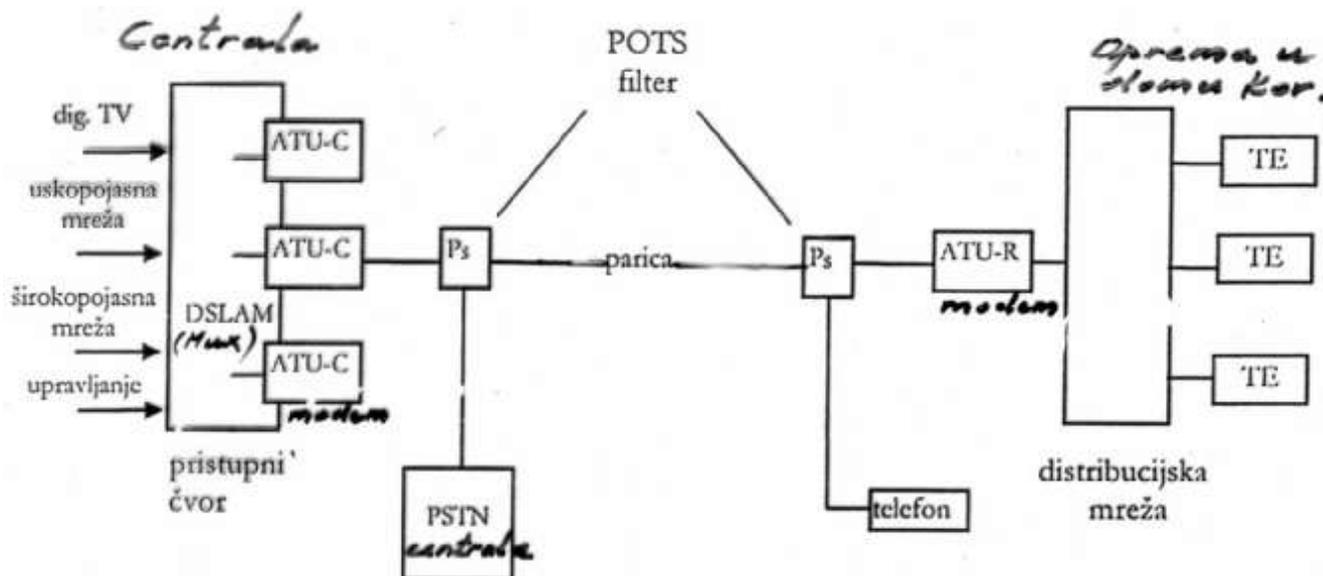
ADSL (*Asymmetric Digital Subscriber Line*), asimetrična digitalna pretplatnička linija) jedna je od tehnologija koje se upotrebljavaju u pristupnim mrežama širokopojasnih sustava koristeći telefonske bakrene parice za prijenos podataka brzinama do 8 Mbit/s u dolaznom smjeru i do 1 Mbit/s u

odlaznom smjeru u odnosu na krajnjeg korisnika (asinkroni prijenos). ADSL sustavi upotrebljavaju frekvencijski opseg do 1.1 MHz za razliku od klasične telefonije koja koristi frekvencije do samo 4 kHz. Namjena ovih sustava je da maksimalno iskoriste postojeće bakrene kapacitete u pristupnim mrežama dok se ne završi njihova zamjena optičkim kabelima, čime se operatorima omogućuje ostvarivanje značajnih prihoda uz relativno manja ulaganja.

Prošlo je gotovo desetljeće otkako je izvorni prijedlog ADSL-a stigao pred telekomunikacijska standardizacijska tijela. Zamisao ADSL-a je za to vrijeme mijenjana i usklađivana sa zahtjevima tržišta. Razvijeno je više generacija opreme i provedena su brojna probna ispitivanja kako bi se dokazala opravdanost uvođenja ADSL sustava.

7.3.1. Referentni model ADSL sustava

Referentni model ADSL sustava prema preporuci ADSL Forum [29], prikazan je na slici 1.3.



Slika 1.3. Referentni model ADSL sustava

Osnovni dijelovi ADSL sustava su:

- ATU-C: ADSL Transmission Unit - Central Office, modem na strani mreže. Može biti ugrađen u pristupni čvor.
- ATU-R: ADSL Transmission Unit - Remote, modem na strani korisnika.

Pristupni čvor: Točka koncentracije za širokopojasne i uskopojasne podatke. Može biti smješten u objektu pristupne centrale ili u udaljenom objektu.

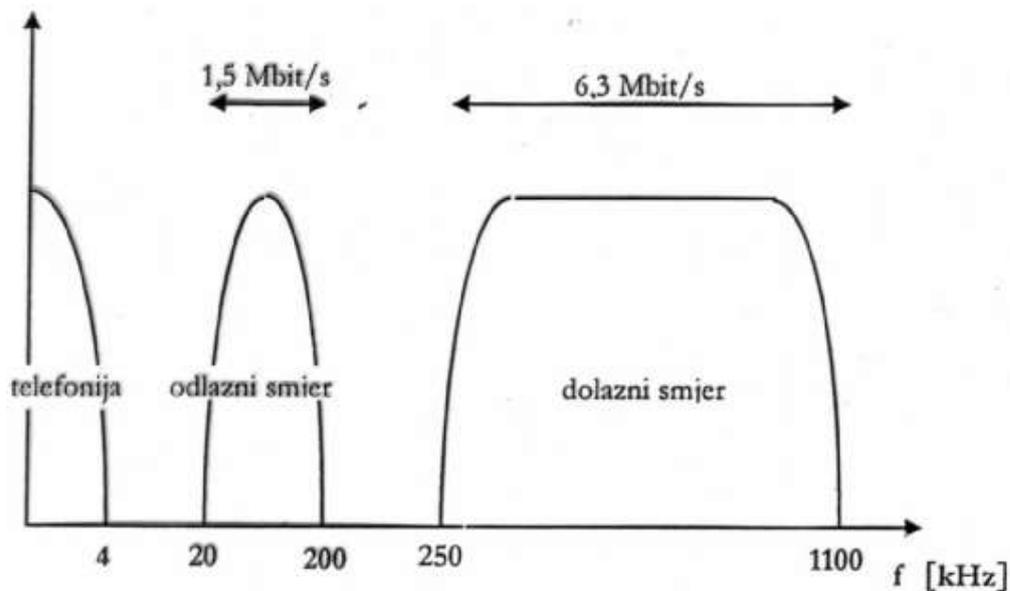
Parica: Bakrena telefonska linija. Može biti različite duljine, promjera, starosti i prijenosnih svojstava.

Distribucijska mreža: Sustav za povezivanje ATU-R modema na prilagodne uređaje (npr. Set-top box, PC sučelje, LAN usmjerivač). Može biti point-to-point ili point-to-multi point strukture, pasivna ili aktivna mreža. Multipoint struktura može biti sabirnička ili zvjezdasta.

Filtar: Filtri odvajaju signale visoke frekvencije (ADSL) od signala niske frekvencije (POTS) na mrežnoj i korisničkoj strani. Filtar može biti zaseban ili ugrađen u ATU modem. Proizvođači mogu isporučivati ADSL sustave sa ili bez POTS filtra.

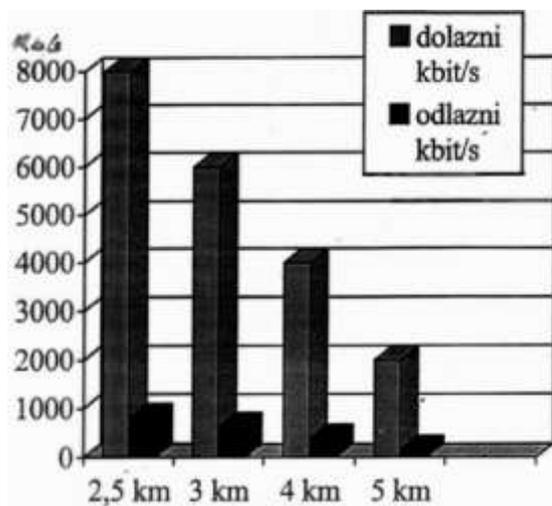
DSLAM: (Digital Subscriber Line Access Multiplexer) je pristupni multiplekser za DSL linije.

Na slici 1.4, prikazana je raspodjela frekvencijskoga spektra u ADSL modemu.

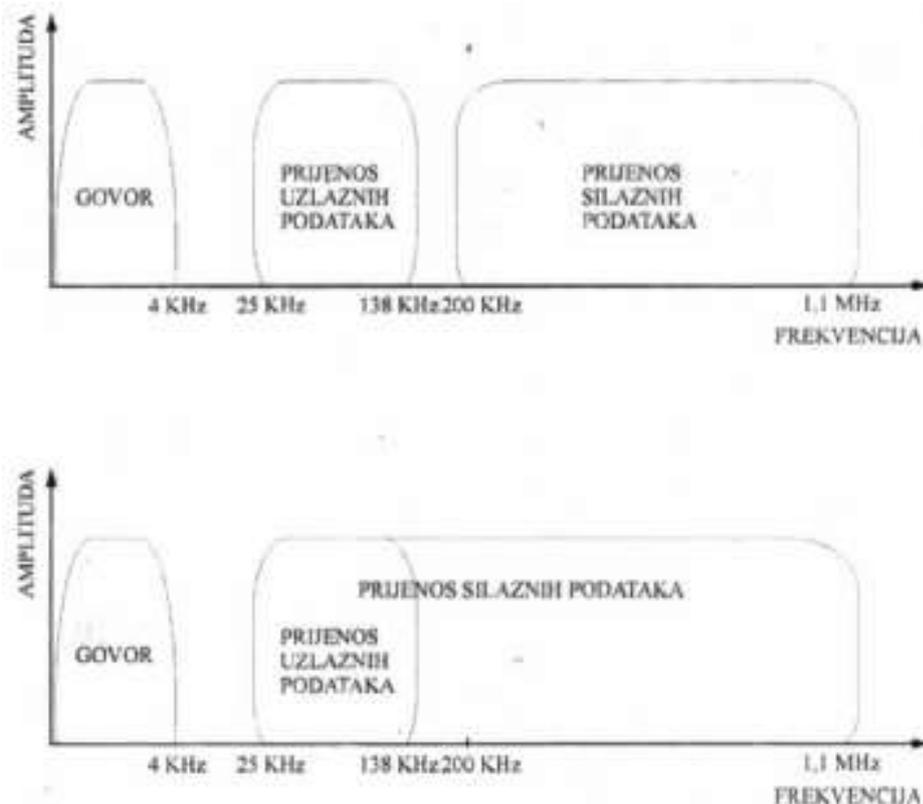


Slika 1.4. Raspodjela frekvencijskog spektra u ADSL modemu

Slika 1.5 prikazuje brzine prijena uporabom ADSL tehnologije na bakrenoj parici promjera 0,4 mm u ovisnosti o duljini parice.



Slika 1.5. Odnos brzine prijena i duljine parice uporabom ADSL sustava



Slika 24. Frekvencijska područja prijenosa

- a) pri uporabi FDM multipleksiranja
- b) pri uporabi poništivača jeke

Prema ANSI standardu u ADSL sustavu mora se upotrijebiti DMT modul, tj. FDM multipleksiranje s ortogonalnim podnosiocima (OFDM).

7.3.2. Usluge koje podržava ADSL tehnologija

Usluge koje podržava ADSL tehnologija mogu se svrstati u dvije osnovne skupine: poslovne usluge i korisničke usluge.

a) Poslovne usluge

Povezivanje i pristup LAN-ovima

Povezivanje udaljenog korisnika na LAN ili povezivanje dvaju ili više međusobno udaljenih LAN-ova može se ostvariti preko ADSL linije. Ova usluga je danas najbrže izvediva za HT, jer zahtjeva najmanje zahvata na postojećoj infrastrukturi. ADSL može zamijeniti uslugu današnjih iznajmljenih vodova tzv. velikim korisnicima.

b) Korisničke usluge

Pristup Internetu

Brzina prijenosa preko ADSL linije omogućuje primjenu raznih multimedijских aplikacija ponuđenih preko WWW-a. Uporaba ove tehnologije premješta prometno usko grlo s korisničke strane na stranu pružatelja Internet usluga koji bi trebao višestruko povećati izlaznu brzinu i propusnost mreže (rješenje je ATM prethodno, danas Ethernet MAN).

Internet promet se može prenositi bilo spajanjem ADSL linije na mrežu Internet poslužitelja i usmjerivača, bilo spajanjem ADSL linije na ATM mrežu koja prenosi Internet promet. Drugi način je brži i bolji, ali je za njegovu realizaciju potreban prijenos TCP-IP prometa preko ATM mreže.

Distribucija TV programa

Istovremeno se prenosi samo jedan kodirani TV kanal (MPEG2 format). U Hrvatskoj se ova usluga ponekad zove i usluga kabelske televizije KTV).

Video na zahtjev, VoD (Video on Demand)

Video sadržaj se prenosi u digitalnom formatu uporabom MPEG2 kodiranja na strani video poslužitelja. MPEG dekodirer smješten je u računalu ili *set top box* (prilagodnom uređaju za televizor) pretvara kod u video signal studijske kvalitete. Zajedno s «vijestima na zahtjev» i sličnim teleuslugama čini sustav tzv. interaktivne televizije (iTV).

Teleusluge

Razne distributivne i interaktivne usluge su moguće:

- kupovina iz kuće,
- interaktivno oglašavanje,
- telemedicina,
- interaktivne igre,
- učenje na daljinu,
- interaktivni priručnici,
- rad kod kuće,
- telekonferencija itd.

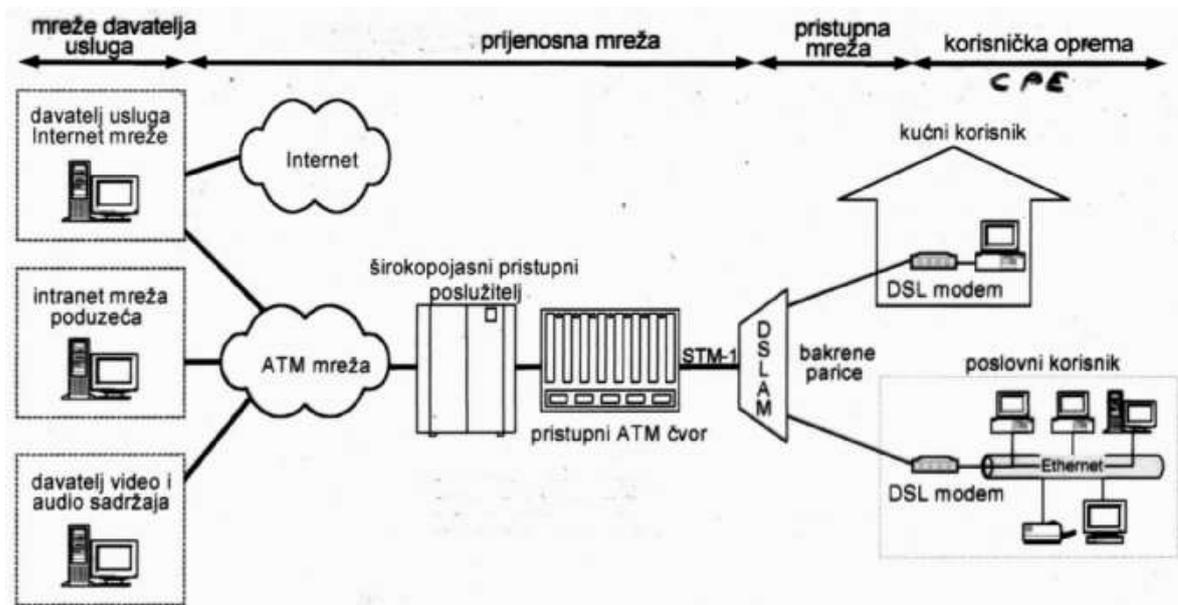
U novije vrijeme pretraživanje digitalnih video knjižnica postaje jedna od najznačajnijih teleusluga. Pristup takvim naprednim sadržajnim uslugama zahtjeva napredak u komunikacijskim tehnologijama "posljednje milje".

ADSL Lite

ADSL Lite je naziv za ADSL, sustav bez filtra za odvajanje uskopojasnog telefonskog prometa (POTS). Pojavljuje se još i naziv CDSL (*Consumer DSL*) i drugi. ADSL Lite standard je utvrdio ITU-T u listopadu 1998. godine kao G.Lite specifikaciju (službeno ITU-T preporuka G.992.2). Ovi sustavi su izgrađeni prvenstveno za uslugu brzog pristupa Internetu, odnosno kao zamjena za postojeće spore modeme koji rade u govornom frekvencijskom području. Najveća razlika između ADSL-a i ADSL Lite-a osim filtra je smanjena brzina rada. ADSL Lite omogućuje brzinu prema korisniku do 1,5 Mbit/s za razliku od 8 Mbit/s kod običnog ADSL-a. Duljina parice za ADSL Lite može biti i do 7 km. Glavne prednosti ove tehnologije su vrlo jednostavna instalacija (bez dodatnog ožičenja za POTS) i niža cijena.

7.3.3. Povezivanje ADSL sustava s informacijskim mrežama

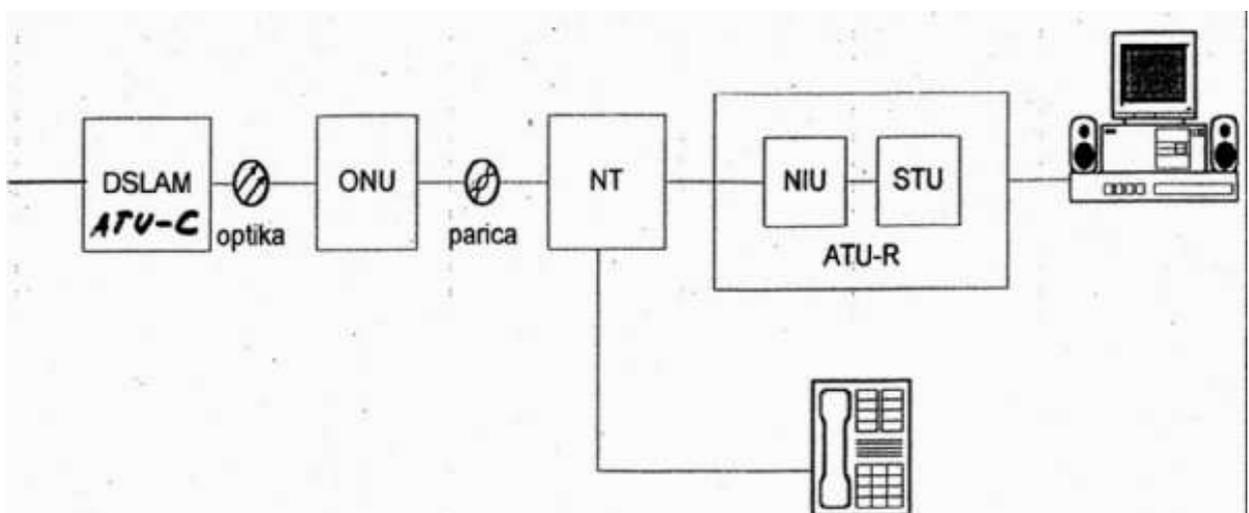
ADSL pristupni sustavi su načelno neovisni o vrsti prometa koji se njima prenosi do korisnika. O potrebama korisnik i mreže ovisi da li će se ADSL sustav povezati s ATM prijenosnom mrežom ili *Ethernet/FastEthernet* lokalnom mrežom odnosno da li će prenositi ATM stanice ili IP pakete.



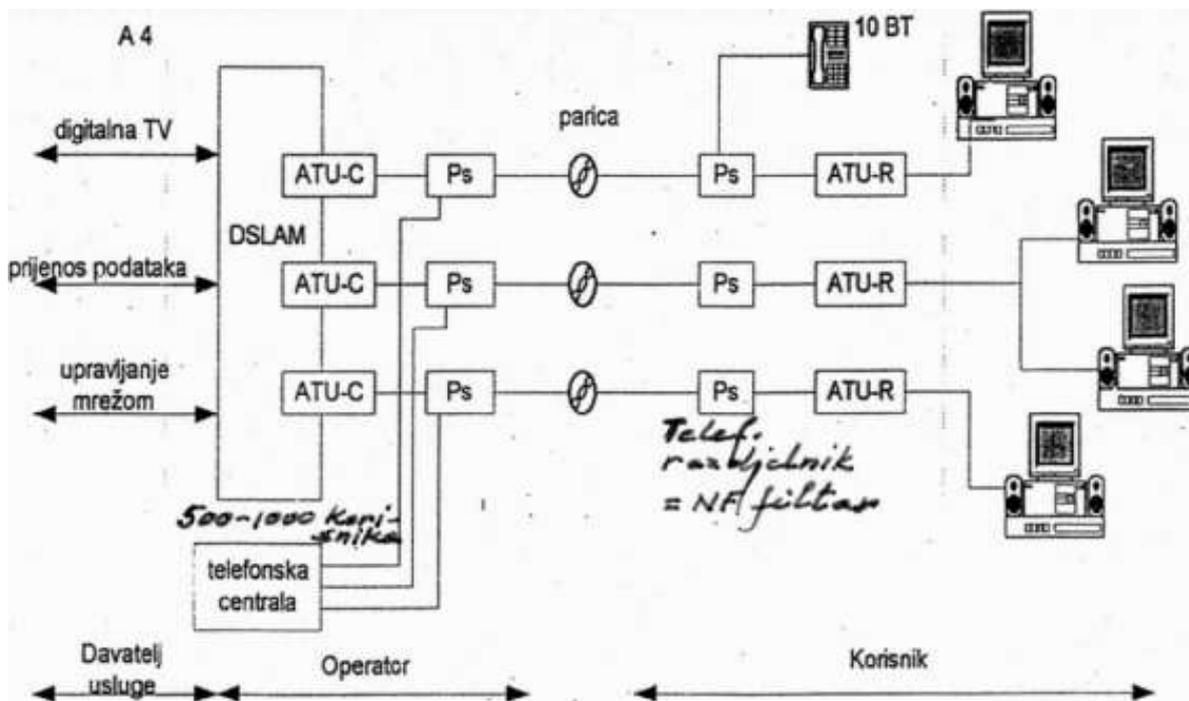
Slika x.y Arhitektura širokopojasne pristupne mreže temeljene na DSL tehnologiji

Širokopojasna integrirana mreža uključuje:

- opremu na strani korisnika,
- pristupnu mrežu,
- prijenosnu mrežu i davatelja usluga.
- DSL modemi imaju Ethernet sučelje prema korisničkom računalu, odnosno LAN mreži.
- Prijenos podataka od DSL modema do mreže davatelja usluga odvija se preko ATM mreže (sada preko Ethernet).
- Stoga je potrebno omogućiti uzajamno djelovanje LAN i ATM mreže što je moguće uporabom:
 - L2TP protokola
 - PPP opunomoćenika (PPP proxy).



Slika 3.1. ADSL referentni model



Slika 3.2. ADSL arhitektura od centrale do korisnika

Iz slike 3.2. se vidi da se informacije pohranjene u poslužiteljima (*servers*) u mrežama davatelja usluga putem prijenosne mreže i sučelja A4 dovode do pristupnog multipleksora digitalne pretplatničke linije, DSLAM. Pristupni multipleksor DSLAM, sadrži nekoliko ADSL transmisijskih jedinica ATU-C (*ADSL Transmisijski jedinica ...*). Ove jedinice služe za komunikaciju s udaljenim ADSL transmisijskim jedinicama ATU-R (*ADSL Transmisijski jedinica - Remote*) koje se nalaze na strani korisnika. ATU-C i ATU-R u principu se mogu smatrati modemima, samo što se jedan modem (ATU-R) nalazi na strani korisnika, a drugi ATU-C u zgradi centrale (slika 3.2.).

Jedinica ATU-R na korisničkoj strani je priključena na medij sa zajedničkim širokopojasnim pristupom. To je neophodno kako bi korisnik mogao na jedan zakupljeni mrežni priključak priključiti nekoliko računala i TV-a s prilagodnim sklopom. Komunikacija između jedinica ATU-R i korisničkih uređaja obavlja se najčešće preko Ethernet (ili ATM mreže u prošlosti).

7.4. Telefonski razdjelnik

Iz slike 3.2. se vidi da je osim uređaja DSLAM, ATU-C i ATU-R prisutan i razdjelnik kao element arhitekture. Na slici 3.2 označen je s Ps. Ovaj sklop istodobno omogućuje odvijanje telefonske usluge i širokopojasnih usluga. U najjednostavnijem obliku to je nisko-propusni filter koji odvaja analogni telefonski signal od signala viših frekvencija koji se obrađuje u ADSL modemima. Ovo je najpovoljnija izvedba razdjelnika, jer su pasivne komponente znatno pouzdanije od aktivnih (ne zahtijevaju napajanje).

Telefonska usluga je izuzetno pouzdana i korisnici to zahtijevaju. Smanjena pouzdanost telefonske usluge pri uvođenju širokopojasnog pristupa uzrokovala bi nezadovoljstvo korisnika. Osim toga i pored mogućnosti uporabe videokonferencije kao sredstva komuniciranja, i mala nedostupnost klasične govorne usluge za korisnika nije prihvatljiva.

7.5. Pristupni multipleksor DSLAM

Osnovne funkcije DSLAM multipleksora:

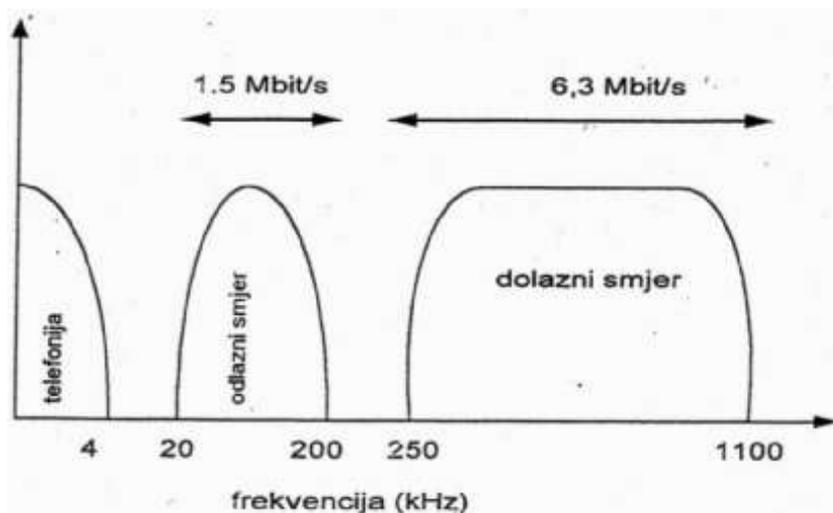
- postavljanje ATU-C sučelja,
- multipleksiranje prometa s ATU-C sučelja na jedan link prema prijenosnoj mreži,
- demultipleksiranje dolaznog prometa iz prosljeđivanje na odgovarajući ATU-C,
- pregovaranje o brzini na ADSL liniji,

- upravljanje mrežom i ATU-R sklopovima,

Današnji ADSL uređaji su predviđeni za posluživanje 500 do 1000 pretplatnika. DSLAM za ovako velik broj pretplatnika se instalira u prostoriji centrale. Ako je broj pretplatnika manji, DSLAM multipleksor se može, približiti korisniku, pri čemu se ostvaruje povećavanje brzine prijenosa.

7.6. ADSL modemi

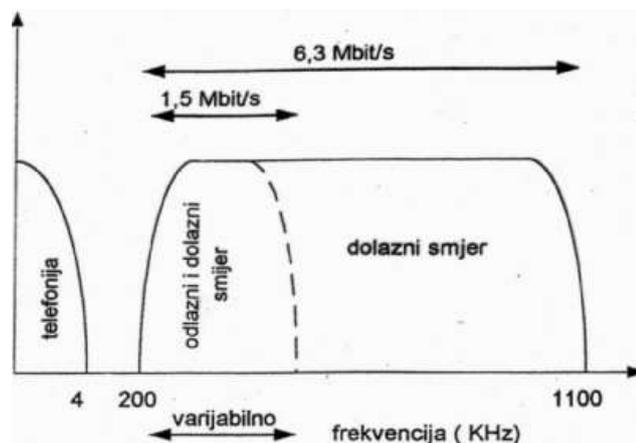
Najvažnija uloga ADSL modema (ATU-C i ATU-R) je pridjeljivanje frekvencija, ostvarivanje frekvencijskog multipleksa, poništavanje jekke i postavljanje odgovarajuće brzine. Slike 3.3. i 3.4. prikazuju raspodjele frekvencijskog spektra u ADSL modemu uz poništavanje jekke. U oba prikaza frekvencije ispod 4 KHz su namijenjene za potrebe telefonije.



Slika 3.3. Raspodjela spektra u ADSL modemu ostvarena uporabom frekvencijskog multipleksa

Frekvencijski multipleksni signali zaposjedaju odvojene frekvencijske pojaseve za odlazni i dolazni smjer. Nedostatak je ovog pristupa što se zaposjeda, značajan dio ukupnog frekvencijskog spektara. Pri primjeni metode s poništavanjem jekke, dolazi do preklapanja frekvencijskih područja za odlazni i dolazni smjer. Tehnika poništavanja jekke upotrebljavala se je i u ranijim izvedbama modema u govornom području, primjerice u modemima V.32 i V.34. Ako postoji nekoliko odjeka na liniji (zbog neprilagodbe) problem se komplicira, a ovo uređaj znatno poskupljuje. Namještanje brzine je proces u kojem se ADSL modemi dogovaraju o brzini kojom će izmjenjivati podatke. Proces je sličan onome u analognim modemima, a služi kako bi se na najbolji način iskoristila linija unatoč njezinim nedostacima.

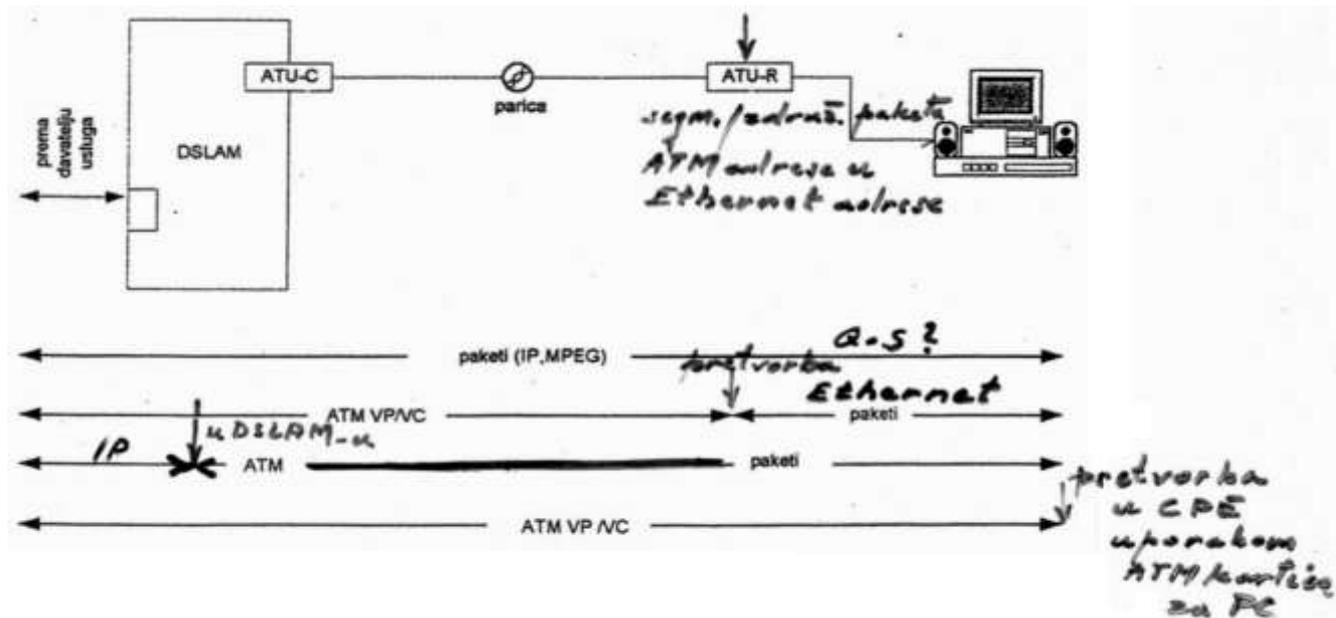
Kako se smetnje na liniji mogu javiti naknadno ili se stanje na liniji može popraviti tijekom sesije, namještanje brzine se mora provoditi periodički za vrijeme trajanja veze.



Slika 3.4. Raspodjela spektra u ADSL modemu - poništavanje jekke

7.7. Protokolarni složaj u ADSL vezi

Predloženo je nekoliko protokolnih složaja za ADSL pristup. ADSL Forum i ATM Forum razvili su zasebna rješenja. Na slici 3.5, prikazana su moguća protokolna rješenja u ADSL sustavu.



Slika 3.5. Moguća protokolarna rješenja u ADSL sustavu

A. Postupci pretvorbe u ATU-R:

1. Operacije segmentiranja i združivanja u korisničkoj opremi
2. Preslikavanje ATM adrese u Ethernet adresu u ATU-R (u DSLAM)

B. Postupci pretvorbe u DSLAM-u:

1. Segmentiranje i združivanje paketa odjednom za sve korisnike

C. Postupci pretvorbe u korisničkoj opremi, primjerice uporabom ATM mrežnih kartica u PC-u.

Prva opcija je upotreba paketa za prijenos informacija na relaciji od davatelja usluga do korisnika. Paketi su, ovisno o vrsti usluge, IP ili paketi MPEG transportnog toka. Veliki je nedostatak ovog pristupa što se ne može jamčiti kakvoća usluge. Stoga se preporučuje uporaba ATM tehnologije do određene udaljenosti, primjerice do distribucijske mreže ili korisnika. Za sada je vrlo vjerojatno da će se u prijenosnoj mreži koristiti ATM tehnologija.

Mnogi telekomunikacijski operatori, uključujući i HT, ubrzano su radili na izgradnji javne ATM mreže: Korisnička mreža će se i dalje pretežno temeljiti na Ethernet tehnologiji, zbog niže cijene u usporedbi s ATM tehnologijom.

Na mjestu sučeljavanja Ethernet i ATM mreže potrebno je obaviti:

- operaciju segmentiranja i združivanja paketa duljine 1,5 kByte (Ethernet) u pakete duljine 48 Bajta (ATM). Ova operacija ima za posljedicu veliko kašnjenje signala na putu prema korisniku, jer prikupljanje ATM ćelija za formiranje Ethernet paketa dugo traje,
- preslikavanje ATM adresa u Ethernet adrese.

Pretvorba se može obaviti i u ATU-R sklopu. U ovom slučaju, problem jamstva kakvoće usluge je riješen svugdje osim u korisničkoj mreži, a to i nije dužnost operatora.

Treća opcija bilo bi obavljanje pretvorbe u DSLAM uređaju. U ovom se slučaju operacije segmentacije i združivanja provode istodobno za sve korisnike u pristupnoj mreži, a to bitno pojeftinjuje opremu. Najveći problem kod ovog pristupa je preslikavanje adresa. Kao jedna od mogućnosti je upotreba PPP protokola (*Point-to-Point Protokol*) s kraja na kraj (od davatelja usluge do korisnika).

Četvrta opcija uključuje obavljanje pretvorbe u korisničkoj opremi. Ovo rješenje bitno povećava cijenu opreme i jako ovisi o Microsoft-ovoj tržišnoj strategiji. Microsoft u novim operacijama podržava ATM kartice. Ovo predstavlja prekretnicu u prodaji ATM mrežnih kartica za osobna računala, a povećanje prodaje kartica vodi njihovu pojeftinjenju.

8. USLUGE KOJE PODRŽAVA ADSL SUSTAV

Usluge koje podržava ADSL sustav mogu se svrstati u dvije osnovne skupine: usluge poslovnih i usluge kućnih korisnika.

8.1. Usluge poslovnih korisnika

Usluge zanimljive za poslovne korisnike koje podržava ADSL sustav su pristup Internetu širokopojasnim brzinama, povezivanje udaljenih poslovnih mreža, video-telefonija, videokonferencija i faksimil u boji. Povezivanje udaljenog korisnika na poslovnu mrežu ili povezivanje dvaju ili više međusobno udaljenih poslovnih LAN-ova može se ostvariti preko ADSL linije. Ovu uslugu danas može HT najbrže implementirati uz najmanje zahvate na postojećoj infrastrukturi. ADSL može zamijeniti uslugu današnjih iznajmljenih vodova tzv. velikim korisnicima.

8.2. Usluge kućnih korisnika

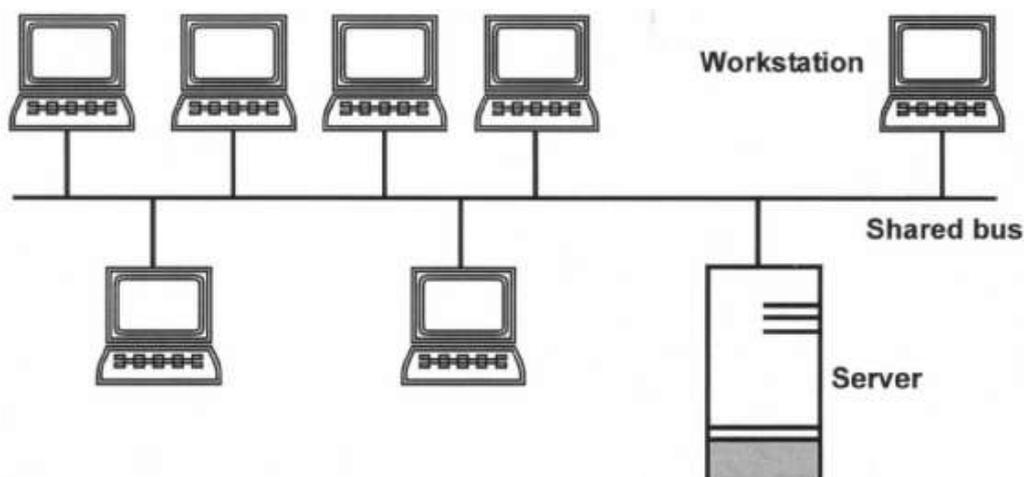
Najzanimljivije usluge za kućne korisnike koje podržava ADSL sustav su pristup Internetu širokopojasnim brzinama, video na zahtjev, distribucija TV programa, mrežne igre, rad kod kuće, tele-trgovina i video-nadzor.

8.2.1. Pristup Internetu

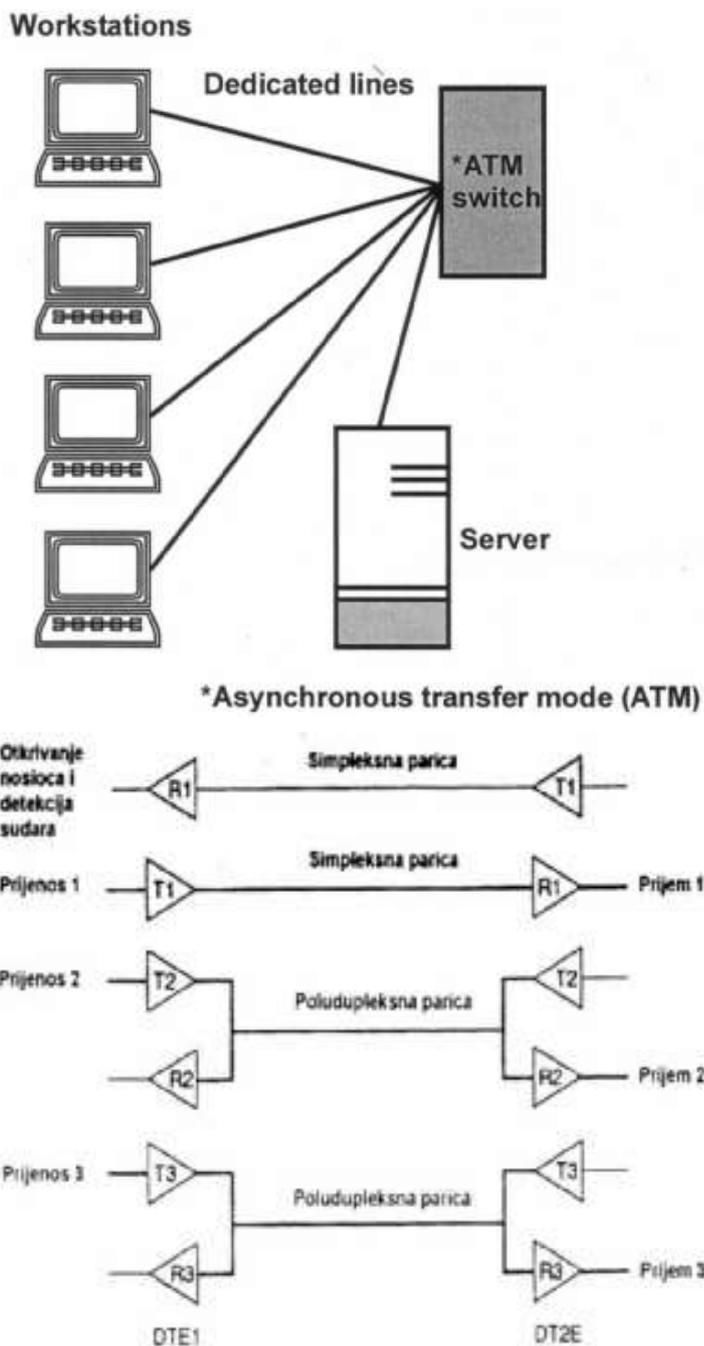
Brzina prijenosa preko ADSL linije omogućuje primjenu raznih multimedijских aplikacija ponuđenih preko WWW-a. Uporaba ove tehnologije premješta prometno usko grlo s korisničke strane na stranu pružatelja Internet usluga koji bi trebao višestruko povećati izlaznu brzinu i propusnost mreže (rješenje je ATM). Internet promet se može prenositi spajanjem ADSL linije na mrežu Internet poslužitelja i usmjerivača ili spajanjem ADSL linije na ATM mrežu koja prenosi Internet promet. Drugi način je brži i bolji, ali je za njegovu realizaciju potrebno ostvariti prijenos TCP/IP prometa preko ATM mreže.

8.2.2. Video na zahtjev (VoD)

Sustav video na zahtjev može omogućiti različite razine interakcije između poslužitelja i klijenta (NVoD, VoD) kao i oblike pristupa u stvarnom i nestvarnom vremenu. Osnovni elementi VoD sustava su: video poslužitelj, video upravitelj, video klijent i prijenosni medij. Sažeti video sadržaj se prenosi od video poslužitelja do korisnika u digitalnom formatu - uporabom MPEG2



[2] Ethernet i druge lokalne mreže (LAN) prisiljavaju korisnike koristiti isti komunikacijski medij što dovodi do kašnjenja [gore]. ATM LAN [dolje] daje kontrolu središnjem ATM čvoru koji svakom korisniku pridjeljuje punu pojasnu širinu mreže toliko dugo koliko mu je ona potrebna. Takvo pridjeljivanje ne zahtjeva da svi korisnici komuniciraju na istoj brzini bitova ili preko istoga fizičkog medija.



Prijenosne staze za DTE i prikazane zadebljano

Slika 2.3. Uporaba 100Base-T4 žičanih parica pri prijenosu okvira

100Base-T4 koristi 8B/6T shemu kodiranja u kojoj se svaki bajt podataka preslikava u uzorak od šest ternarnih (tri razine: +1, 0, -1) simbola poznat kao 6T kodna grupa. Iz slike 2-3. vidi se da se tri žičane parice rabe za prijenos okvira, dok se jedna upotrebljava za otkrivanje nosioca i detekciju sudara.

100Base-T2 specifikacija razvijena je kao bolja alternativa za nadgradnju mreža s instaliranim kablom kategorije 3, nego što je to omogućavala specifikacija 100Base-T4.

Definirana su dva važna nova cilja:

- omogućavanje komunikacije preko dvije parice kategorije 3 ili boljeg kabela,
- podržavanje i poludupleksnog i dupleksnog rada.

100Base-T2 koristi drukčiji postupak prijenosa signala od bilo koje prethodne Ethernet implementacije s upletenim paricama. Umjesto da se koriste dva simpleksna linka da bi se formirao jedan dupleksni link, uporabom 100Base-T2 dvojne dupleksne (*dual-duplex*) transmisijske metode istodobno se šalju kodirani signali u oba smjera po bakrenim paricama.

8.3. 1000 Mb/s Ethernet (Gigabitni Ethernet)

Brzo prihvaćanje 100 Mb/s Ethernet, zbog niske cijene i kompatibilnosti s postojećim lokalnim mrežama klase Ethernet, pridonijelo je popularnosti Ethernet tehnologije. S 1000 Mb/s Ethernetom, koji je standardiziran 1998. godine, Ethernet tehnologija je postala mrežnim rješenjem ovoga stoljeća. Gigabitni Ethernet, poput drugih standarda koji se temelje na OSI modelu, implementira funkcionalnosti definirane standardom fizičkoga sloja, odnosno mehaničke, električke i proceduralne značajke te uspostavljanje, održavanje i raskidanje veze između mrežnih uređaja. Za komuniciranje putem Gigabitnog Ethernet standard IEEE 802.3 definira nekoliko standarda fizičkoga sloja (PHY). Dva PHY standarda osiguravaju prijenos preko svjetlovodnog prijenosnog medija (slika 2-4.) [2]:

1000Base-SX (*Short Wavelength Fiber*) uporabom višemodnog svjetlovoda kratke valne duljine (850 nm), primjerice, u temeljnoj mreži zgrade na udaljenosti 300-550 m i većoj,

1000Base-LX (*Long Wavelength Fiber*) uporabom jednomodnog svjetlovoda dugačke valne duljine (1300 nm), primjerice, u temeljnoj mreži kampa, na udaljenostima 3 i više kilometara.

8.4. Vrste 1000 Mb/s Ethernet sustava

1000Base-SX (<i>Short Wavelength Fiber</i>)	}	Norme za prijenos poruke svjetlovodu
1000Base-LX (<i>Long Wavelength Fiber</i>)		
1000Base-CX (<i>Short Run Copper</i>)	}	Preko 2 STP, kabliranje unutar soba
1000Base-T		Preko 4 UTP kategorije 5 (kabliranje po kutovima)

Tablica 3. Podržavanje konfiguracija linkova 100Base X

Konfiguracija linka	1000Base-CX	1000Base-SX 850nm valna dužina	1000Base-LX 1300nm val: dužina
150 S2 STP bakar	podržava	ne podržava	ne podržava
125/62,5 μm višemodni svjetlovod	ne podržava	podržava	podržava
125/50 μm višemodni svjetlovod	ne podržava	podržava	podržava
125/10 μm jednomodni svjetlovod	ne podržava	podržava	podržava
dozvoljeni konektori	IEC stil 1 ili optički kanal stil 2	SFF MT-RJ ili dupleksni SC	SFF MT-RJ ili dupleksni SC

Tablica 4. Poredba značajki 10 Mb/s Ethernet, 100 Mb/s Ethernet i 1000 Mb/s Ethernet

značajke mreža	Ethernet 10 Base-T	Brzi Ethernet 100 Base-T	Gigabitni Ethernet
Brzina: podataka	10 Mb/s	100 Mb/s	1 Gb/s
UTP kategorije 5	100 (min.) m	100 m	100 m
STP/koaksijalni kabel	500 m	100 m	25 m +

Višemodni svjetlovod	2 km	412 m * 2 km**	550 m +
Jednomodni svjetlovod	25 km	20 km	5 km

* ... IEEE spec. poludupleksni prijenos

** ... IEEE spec. potpuno dupleksni prijenos

9. GRADSKA MREŽA ETHERNET (E-MAN)

Tijekom proteklih 25 godina Ethernet tehnologija dominira kao standard za lokalne mreže (LAN) širom svijeta.

Pri uvođenju Ethernet tehnologije u gradsku mrežu (E-MAN) treba postići istu jednostavnost upotrebe i nisku cijenu kao u lokalnim mrežama.

9.1. Tehnologije gradske mreže (MAN)

Gradske mreže (MAN) temelje se na različitim tehnologijama.

U upotrebi su najprisutnije:

- SONET,
- SDH

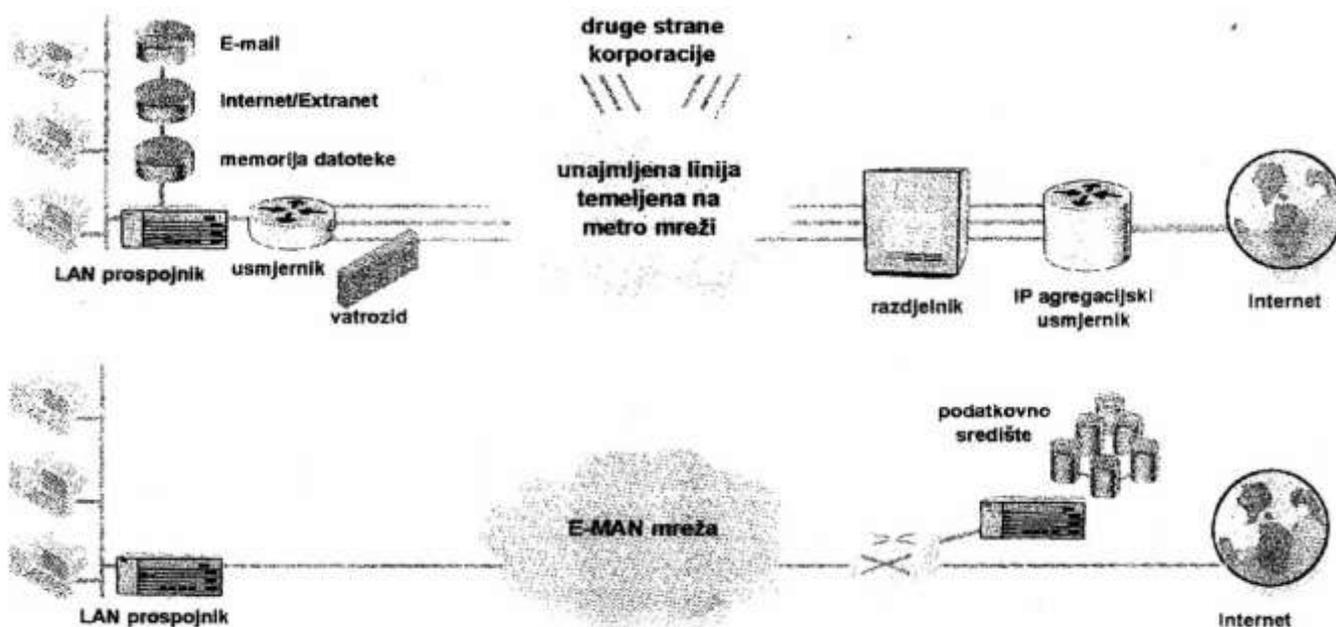
SONET/SDH tehnologije također se mogu koristiti za prijenos Ethernet prometa *od točke do točke*.

Izgradnja mreže temeljene na Ethernet tehnologiji je jeftinija nego SONET/SDH mreže.

SONET/SDH mreže koriste se za prijenos tradicionalnog prometa, dok se nova E-MAN prekrivajuća mreža može iskoristiti za prijenos povećanog podatkovnog prometa koji se uglavnom temelji na IP protokolu. Cilj je osigurati korisnicima Ethernet mreža kakvoću prijenosa kao u javnoj telefonskoj mreži uz nižu cijenu.

E-MAN ... atraktivna kao komplementarna mreža SONET/SDH mrežama

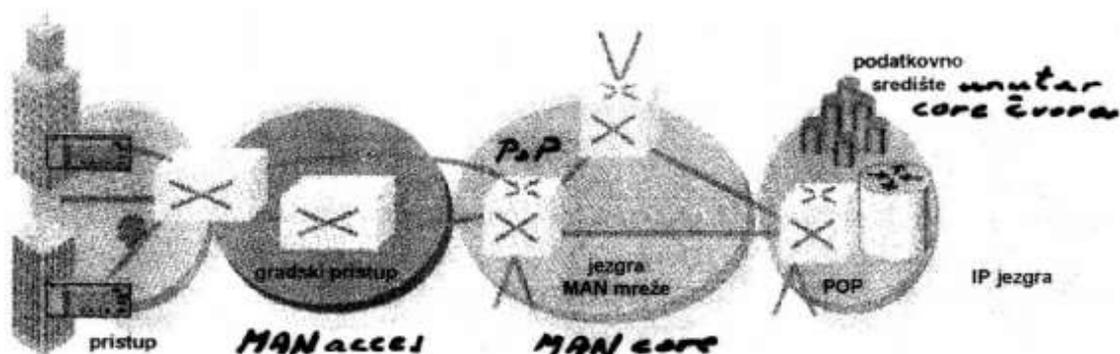
9.2. Značajke i strukture E-MAN mreže



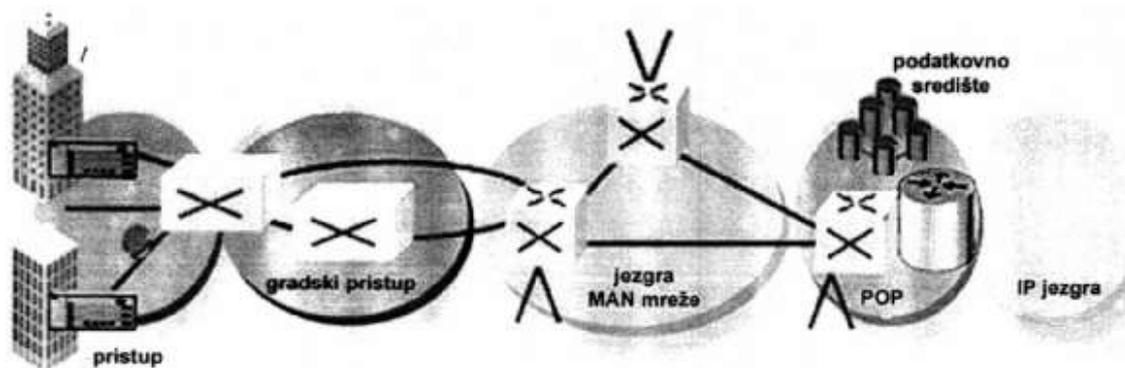
Slika 3-2. Ethernet gradska mreža kao pružatelj usluga

Struktura tipične E-MAN mreže je prikazana na slici 3-3. Iz ove slike vidi se da *metro* pristupni dio (*Metro Access Part*) združuje promet iz različitih zgrada unutar jednog gradskog područja. E-MAN

mreža obično ima topologiju svjetlovodnih prstena gdje svaki *metro* pristupni prsten sadrži između 5 i 10 čvorova. Ti prsteni prenose promet od korisnika do sučelja (POP točaka) koja su međusobno povezana jezgrenom gradskom mrežom (*Metro Core*). Jezgrena gradska mreža uobičajeno pokriva nekoliko gradova ili veliko industrijsko područje.



Slika 3-3. Struktura Ethernet-gradske mreže



Slika 4. Struktura Ethernet-gradske mreže

E-MAN mrežu čine:

- prstenasta svjetlovodna gradska pristupna mreža,
- jezgra MAN mreže.

Prednost uporabe svjetlovodnih prstena:

- osiguravanje otpornosti na presijecanje kabela i na kvarove u čvorovima,
- mogućnost obnavljanja prometa unutar 50 ms nakon prekida,
- zaštitni prsteni dokazana tehnologija za osiguravanje zaštite prometa unutar SONET/SDH mreža.

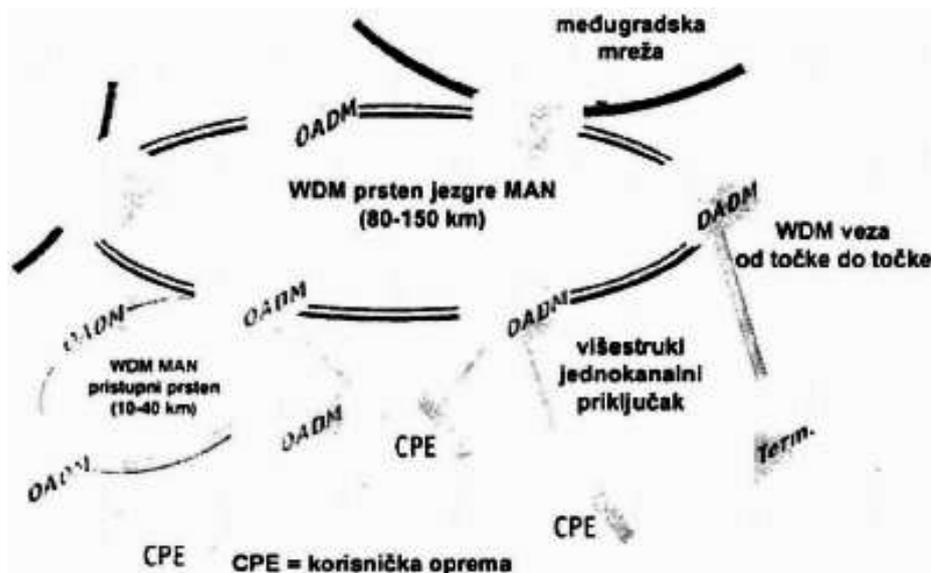
Razlika između zaštitnih SONET/SDH i E-MAN prstena:

- u SONET/SDH prstenima zaštita korisničkog sadržaja je organizirana na razini kontejnera (u korisničkom opterećenju STM okvira - prospajanje kanala),
- u E-MAN mreži promet je paketni (ne postoje kanali između čvorova), pa se uvodi nova zaštitna tehnologija - otporni paketni prsteni s prospajanjem paketa, RPR (*Resilience Packet Ring*),
- RPR zaštita osigurava zaštitu samo onim razredima usluga koji to zahtijevaju, dok SONET/SDH zaštitni prsteni osiguravaju zaštitu za sav promet.

10. ČVOR GRADSKJE MREŽE (MAN)

Tijekom zadnjih godina operatori su većinu svojih ulaganja usredotočili na temeljne (*backbone*) mreže u skladu s njihovim prioritetom da udovolje rastućim zahtjevima za pojasnom širinom koji se javljaju kao posljedica Internet revolucije. Nakon ulaganja u povećanje pojasne širine temeljne mreže za mrežne operatore je došao trenutak da unovče svoja ulaganja i prošire ponudu usluga što će donijeti dobitak. Stoga se središte zanimanja i nadmetanje u današnjoj telekomunikacijskoj industriji

pomaknulo prema gradskoj mreži. MAN (*Metropolitan Area Network*), jer se ona smatra rješenjem za zadržavanje pretplatnika i pružanje usluga s dodatnom vrijednošću (*Added-value Services*).



Slika 4.1. Pristupna mreža i jezgra MAN mreže

Nedavno istraživanje tržišta pokazalo je da prekapacitiranost (*over-capacity*) u javnim mrežama širom svijeta puno brže smanjuje cijenu međugradskih veza nego smanjivanje troškova izgradnje tih mreža. Za razliku od temeljne mreže, gdje konvergencija Internet protokola višeprotokolnog komutiranja temeljem oznaka IP/MPLS otvara mogućnost postizanja veće učinkovitosti, gradsku mrežu obilježava uporaba mnoštva aplikacija i protokola koji se trebaju transparentno prenijeti do središnjih ureda operatora u svrhu isporuke usluga. Najtipičnija poslovna nedoumica glede MAN mreža odnosi se na donošenje odluke o ostvarivanju transparentnosti usluga ili veće učinkovitosti mreže. To će biti glavni čimbenik koji će odrediti strategiju bilo kojeg operatora i bilo kojeg prodavatelja opreme namijenjene za gradsku mrežu. Pristupna i jezgrena MAN mreža prikazane su na slici 4.1.

10.1. Nove MAN aplikacije

Potrebe za većom pojasnom širinom u gradskoj mreži generiraju poslovni i rezidencijski korisnici. Stoga je razumljivo da je širokopojasni pristup zajednički nazivnik za različite pristupne tehnologije koje se temelje na uporabi bakrenih parica (digitalna pretplatnička linija, xDSL), koaksijalnog kabela CMTS (*Cable Modem Termination System*) i svjetlovoda (svjetlovodno vlakno do ..., FTTx), pa do fiksnog bežičnog (lokalni distribucijski sustav, LMDS) i mobilnog pristupa (opće paketne radijske usluge/svjetski sustavi pokretnih telekomunikacija, GPRS/UMTS). Unatoč ogromnim razlikama koje postoje između navedenih tehnologija, sve ove tehnologije obilježava povećavanje brzine prijenosa podataka do krajnjeg korisnika za jedan red veličine u usporedbi s tradicionalnim uskopojasnim rješenjima. Stoga one otvaraju vrata mnoštvu novih usluga.

11. NADogradnja Ethernet mreža

Početne aplikacije Gigabitnog Etherneta ostvarene su u kampovima i zgradama gdje su se zahtijevale veće pojasne širine između usmjernika, prospojnika, hubova, repetitora i servera. Primjeri gigabitnih veza uključuju: veze prospojnik-usmjernik, prospojnik-prospojnik, prospojnik-server i repetitor-prospojnik.

11.1. Uspostava brzih mreža

Združivanje linkova (*link aggregation*) je jedna od novijih opcija sposobnosti MAC podsloja koja omogućuje da se nekoliko fizičkih linkova združi u jedan logički kanal veće brzine.

Združivanje linkova treba promatrati kao opciju mrežne konfiguracije koja se primarno koristi za međuveze koje zahtijevaju veće brzine prijenosa podataka nego što im mogu omogućiti pojedinačni linkovi, kao što je slučaj pri povezivanju prospojnik-prospojnik i prospojnik-poslužitelj datoteke.

Združivanje linkova može biti iskorišteno u Ethernet mreži bilo koje prijenosne brzine.

Može se ostvariti samo:

- na paralelnim točka-točka linkovima
- na linkovima koji podržavaju potpuno dupleksni rad iste brzine.

Postojeći linkovi kategorije 5 podržavaju sve trenutne Ethernet prijenosne brzine od 10 Mb/s do 1000 Mb/s. Treba ispitati njihovu sposobnost za podržavanje gigabitne brzine.

Višemodni svjetlovod ne može se koristiti za sve instalacije temeljne mreže. Jednomodni svjetlovod može podržati sve dužine do 10.000 metara pri 1000 Mb/s u temeljnoj mreži, te podržava uporabu pri 10 Gb/s u budućim temeljnim mrežama.

11.2. Nadogradnja Brzog Etherneta ili FDDI² mreže radne grupe

Između svih tehnologija lokalnih mreža velike brzine Brzi Ethernet ili 100 Base-T ima vodeću ulogu. Potrebe za mrežama još većih prijenosnih brzina na razinama temeljne mreže, servera, MAN i WAN mreža su očigledne.

100 Base-T je idealna tehnologija koja omogućuje ekonomičnu nadogradnju do Gigabitnog Etherneta.

U svim scenarijima nadogradnje Brzog Etherneta do Gigabitnog Etherneta ostaju nepromijenjeni:

- mrežni operacijski sustav (NOS),
- aplikacije,
- NIC pogonitelji (*drivers*),
- postojeće bakrene parice,
- višemodni svjetlovodi,
- investicije u aplikacije mrežnog upravljanja,
- alati.

Standard 10 Gigabitnog Etherneta podržava:

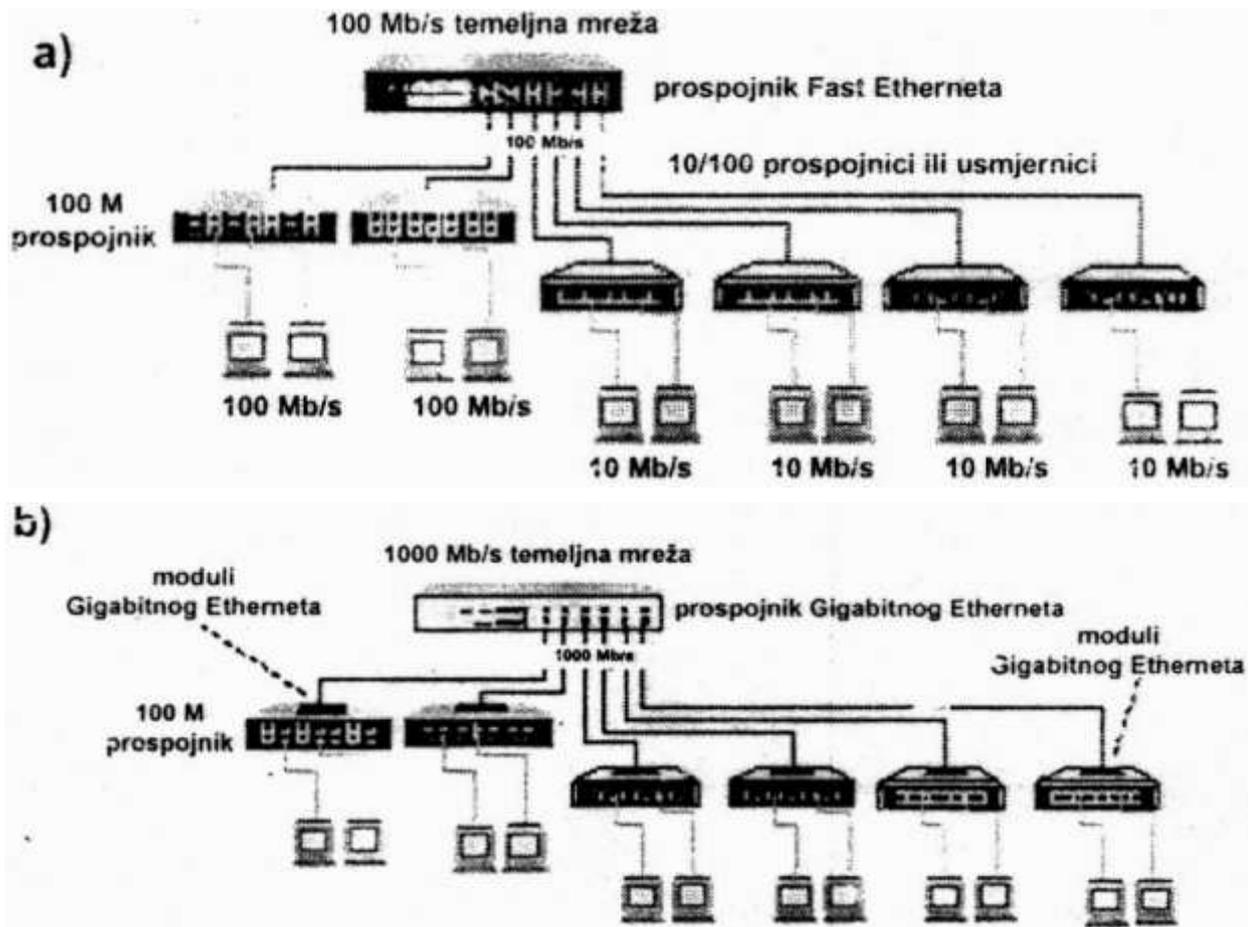
- jednomodne svjetlovođe na udaljenostima preko 40 km,
- izgradnju linkova veoma velike brzine po niskoj cijeni,
- povezivanje zemljopisno udaljenih lokalnih mreža preko postojećih SONET/SDH/TDM mreža.

Tehnologija koja će Gigabitni Ethernet podići na razinu 10 Gb/s Etherneta već postoji. Uporaba te tehnologije proširit će se na MAN i WAN mreže uz očuvanje ranijih ulaganja ponuđača usluga u postojeću infrastrukturu Ethernet mreže.

12. MOGUĆNOST NADOGRAĐNJE ETHERNET MREŽA

U svim verzijama nadgradnje 100 Mb/s Etherneta do Gigabitnog Etherneta maksimalno se iskorištava postojeća mrežna infrastruktura.

² *Fiber Distributed Data Interface*



Slika 11. Nadgradnja temeljne mreže komutiranog brzog Etherneta

Nadgradnja uključuje zamjenu 100 Mb/s prospojnika sa 1000 Mb/s prospojsnikom.

13. POREDBA PRIVATNIH I VIRTUALNIH PRIVATNIH MREŽA

13.1. Privatne mreže

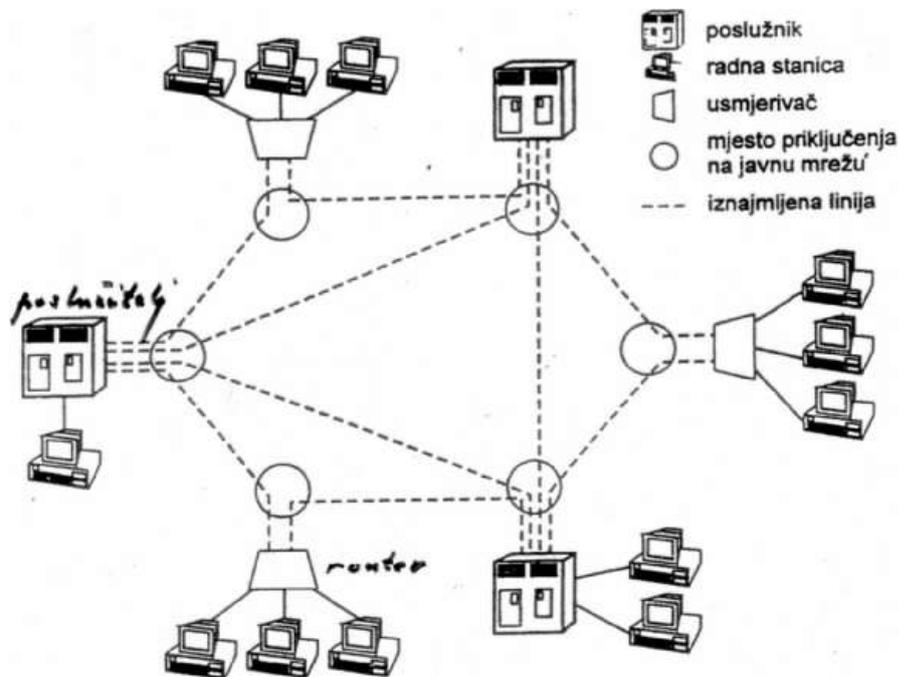
Privatne mreže velikih poslovnih korisnika u prošlom desetljeću ostvarivane su uporabom zakupljenih linija. Izgradnjom privatne mreže poslovni korisnik se orijentira na uporabu vlastite instalirane opreme, što ima prednosti i nedostatke.

Prednosti uporabe privatnih mreža:

- fleksibilnost i potpuno neovisno upravljanje mrežom,
- jeftinija mrežna tehnologija,
- visoki stupanj sigurnosti podataka.

Nedostaci uporabe privatnih mreža:

- potreban je velik početni kapital za izgradnju, održavanje i upravljanje vlastitom mrežom, obuku osoblja i osiguravanje čitave mrežne infrastrukture,
- odvajanje značajnih finansijskih sredstava za razvoj mreže u budućnosti,
- linije među centralama potrebno je projektirati za vršnu brzinu prometa, što ima za posljedicu veliku zalihost linija i velik dodijeljen kapacitet vezi,
- potrebna je oprema za obavljanje funkcija prospajanja i usmjeravanja.



Slika 1.1. Primjer privatne mreže s unajmljenim linijama

Slika 1.1. prikazuje privatnu mrežu sa zakupljenim linijama. Poslužnici su povezani na udaljene skupine multipleksiranih radnih stanica, dok je svaki poslužnik, kao i udaljena radna stanica povezan s dva zasebna računala, kako bi se osigurala raspoloživost sustava. Poslužnik obavlja i funkcije usmjerivača i prenosnika.

Odlučujući čimbenici pri donošenju odluka o gradnji vlastite privatne mreže, za mnoge poslovne korisnike su fleksibilnost i sigurnost od neovlaštenoga pristupa podacima. Međutim, zbog povećanih troškova održavanja i upravljanja mrežom, sve više poslovnih korisnika prelazi na jeftiniju varijantu umrežavanja svojih lokalnih mreža preko javne telekomunikacijske mreže. Drugim riječima, u sadašnje vrijeme sve više poslovnih korisnika odlučuje se za realizaciju virtualne privatne mreže.

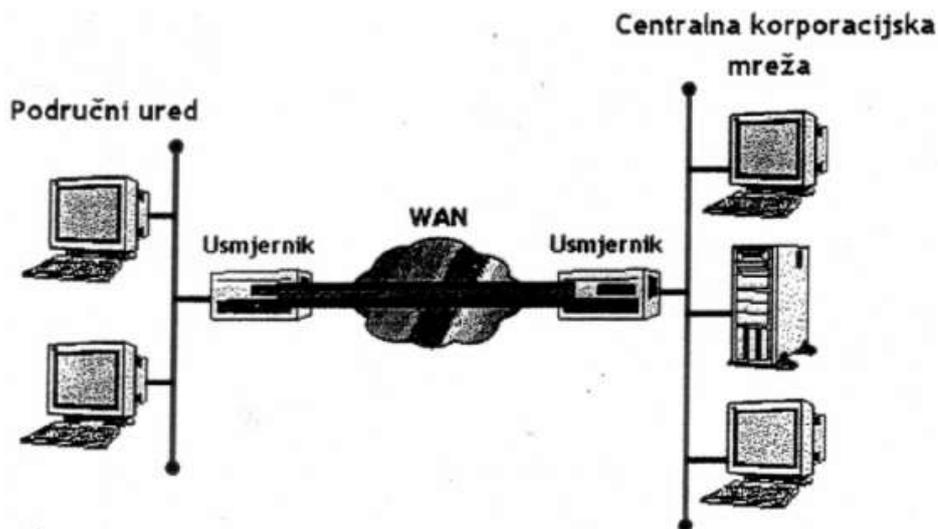
13.2. Virtualne privatne mreže

Za razliku od privatnih mreža, virtualna privatna mreža je privatna računalna mreža ostvarena uporabom infrastrukture javne telekomunikacijske mreže (primjerice, Interneta). Privatnost se ostvaruje tuneliranjem i sigurnosnim postupcima. Pristup korisnika u virtualnoj privatnoj mreži ostvaruje se uporabom zajedničkih pristupnih linija do mrežnih prospojnika koji na zahtjev korisnika osiguravaju određeni kapacitet virtualnog kanala za komunikaciju između računala i radnih stanica.

13.2.1. Prednosti uporabe virtualne privatne mreže (VPN)

Dok VPN mreža nudi izravno smanjivanje troškova za razliku od primjerice uporabe unajmljenih linija, ona također osigurava i druge prednosti uključujući manje troškove koji su rezultat smanjivanja potrebe za opremom i obučavanjem osoblja, te povećane fleksibilnosti i skalabilnosti glede broja istodobnih tunela koje VPN poveznik (*gateway*) može podržati.

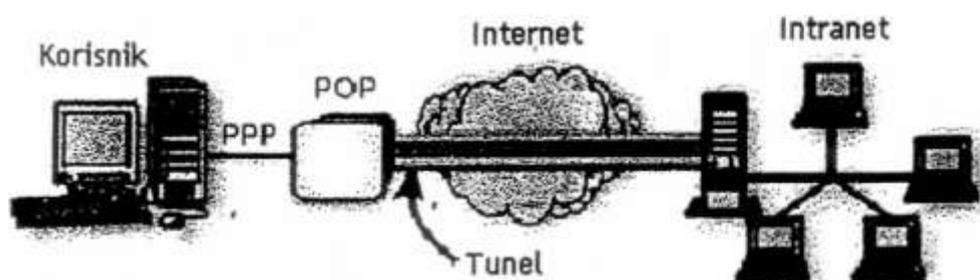
Virtualne mreže ostvarene preko Interneta mogu riješiti mnoge probleme poslovnih korisnika. VPN omogućuju mrežnim upraviteljima ekonomično povezivanje udaljenih razgranatih ureda i projektnih timova u centralnu korporacijsku mrežu i osiguravaju daljinski pristup zaposlenicima, što smanjuje zahtjeve za opremom i podrškom (slika 1.2.).



Slika 1.2. VPN povezivanje razgranatih ureda u privatni intranet

VPN mreža koristeći otvorenu, distribucijsku infrastrukturu Interneta, prenosi podatke između korporacijskih lokalnih mreža, ne oviseći o namjenskim unajmljenim linijama ili o ³ (*frame relay*) permanentnim virtualnim krugovima. Kompanije koje koriste VPN preko Interneta, uspostavljaju vezu preko lokalnih spojnih točaka POP njihovog davaoca Internet usluga (ISP), koji osigurava prijenos podataka do odredišta putem Interneta. Međutim, Internet je javna mreža koja ne jamči kakvoću ni sigurnost prijenosa podataka, pa VPN podržava mjere za zaštitu podataka od prisluškivanja i neovlaštenoga pristupa.

VPN nisu ograničene samo na korporacijske mreže i povezivanje razgranatih geografski udaljenih ureda, nego omogućuju i sigurnu povezivost mobilnih radnika. Ovi radnici se mogu povezati na VPN mrežu njihove kompanije uspostavljajući vezu preko lokalnih spojnih točaka, POP (*Point of Presence*) njihovog lokalnog davatelja Internet usluge, smanjujući tako troškove komuniciranja, instalacija i održavanja velikih modemskih sustava korporacijskih mreža (slika 1.3.).



POP ... mjesto pristupa u javnu mrežu (*Point of Presence*)

Slika 1.3. VPN povezivanje udaljenog korisnika na privatni intranet

Glavne prednosti VPN mreža su:

- smanjivanje troškova komuniciranja prenošenjem podataka putem Interneta, zbog čega nije potrebno plaćati međuzupanijske impulse (troškovi međuzupanijskih impulsa smanjeni su korištenjem VPN, jer se komunikacijska linija uspostavlja pozivanjem telefonskog broja unutar županijske mrežne skupine),
- smanjivanje troškova ostvarivanja mreže uporabom resursa javne telekomunikacijske mreže, te smanjivanjem broja pristupnih linija do središnjeg tvrtkinog računalnog sustava (najveći broj kompanija plaća mjesečne iznose za dvije vrste komunikacijskih linija:
 - brze linkove za pristup Internetu i *frame relay*,
 - ISDN PRA ili E1 linije za prijenos podataka.

VPN omogućuje da se podaci prenose putem postojećih brzih linkova za pristup Internetu, čime se smanjuje potreba za dodatnim komunikacijskim kapacitetima),

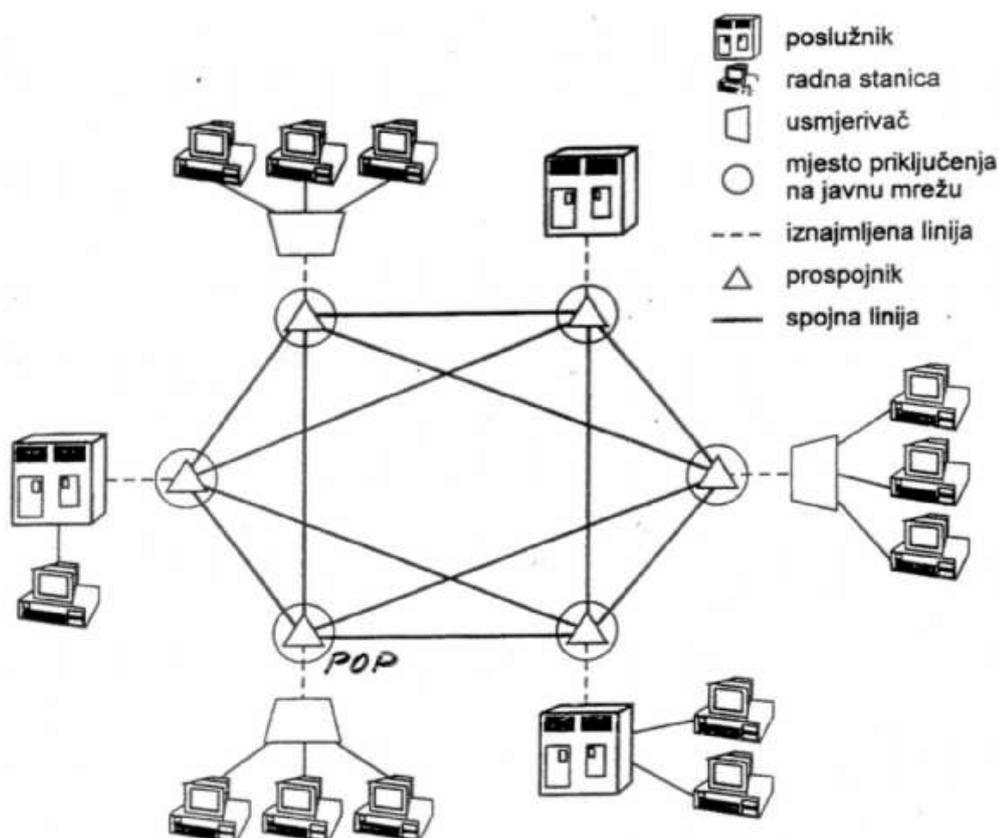
³ Navesti hrvatski naziv

- smanjivanje troškova održavanja i upravljanja komunikacijskom opremom (kompanija prepušta davaocu Internet usluga održavanje i upravljanje komunikacijskom opremom, što znači da je kompaniji omogućen pristup privatnoj računalnoj mreži putem pristupnih točaka (POP) njezinog davaoca Internet usluga).

13.3. Prednosti virtualnih privatnih mreža u poredbi s privatnim mrežama

Prednosti virtualnih privatnih mreža u poredbi s privatnim mrežama su višestruke:

- vlasnik virtualne mreže ne treba ulagati financijska sredstva u prijenosne komutacijske sustave, a jedini je trošak nabavka krajnje opreme (terminala),
- smanjuju se troškovi pristupa u mrežu,
- tekući troškovi su proporcionalni uporabi mrežnih resursa, a ne odnose se na zahtijevanu vršnu brzinu kao kod privatnih mreža,
- VPN mreža osigurava visoki stupanj raspoloživosti i pouzdanosti, pokrivenost širokog područja, a također i zaštitu od neovlaštenog pristupa podacima (visoki stupanj raspoloživosti osigurava moderna mrežna arhitektura projektirana za budući razvoj, dok zaštitu od neovlaštenog pristupa podacima osiguravaju dodatne usluge kao što su zatvorene skupine korisnika, identifikacija korisnika mreže i razmjena adresa između pozvanog i pozivajućeg korisnika),
- VPN mreža kao dio nacionalne mreže omogućuje povezivanje s međunarodnom mrežom, a pristup je osiguran iz analogne (POTS) telefonske mreže ili digitalne mreže integriranih usluga ISDN.
- obučeno i kvalificirano osoblje javne telekomunikacijske mreže stalno je dostupno za konzultiranje i rješavanje eventualnih nastalih problema,
- funkcionalnost i spektar usluga stalno se povećavaju s nadgradnjama sklopovske i programske podrške,
- osiguravanje širokog spektra usluga korisnicima kao što su: elektronička pošta, sustav razmjene poruka (MHS - *Message Handling System*) baziran na X.400, videotex usluga i drugo.



Slika 1.4. Primjer virtualne privatne mreže

Slika 1.4. prikazuje grupu poslužnika, usmjernika, udaljenih skupina radnih stanica i točaka pristupa u javnu mrežu kao dio virtualne privatne mreže. U toj mreži prospojnici obavljaju prospajanje i usmjeravanje paketa oslobađajući usmjernike i poslužnike od tih funkcija. Prospojnici su međusobno povezani vezama visokih brzina prijenosa koje su zajedničke za veći broj korisnika kojima osiguravaju velik broj usluga dinamičkim dodjeljivanjem zajedničkih resursa. Svakom korisniku potrebna je samo jedna pristupna linija, što umanjuje troškove povezivanja u odnosu na troškove povezivanja u privatnoj mreži.

Virtualna privatna mreža omogućuje tvrtkama da kroz privatnu računalnu mrežu povežu zemljopisno udaljene urede i radnike uporabom Interneta kao infrastrukture za povezivanje. U tom smislu VPN služi kao vrlo prihvatljiv nadomjestak za stalne veze i telefonske (modemske) veze.

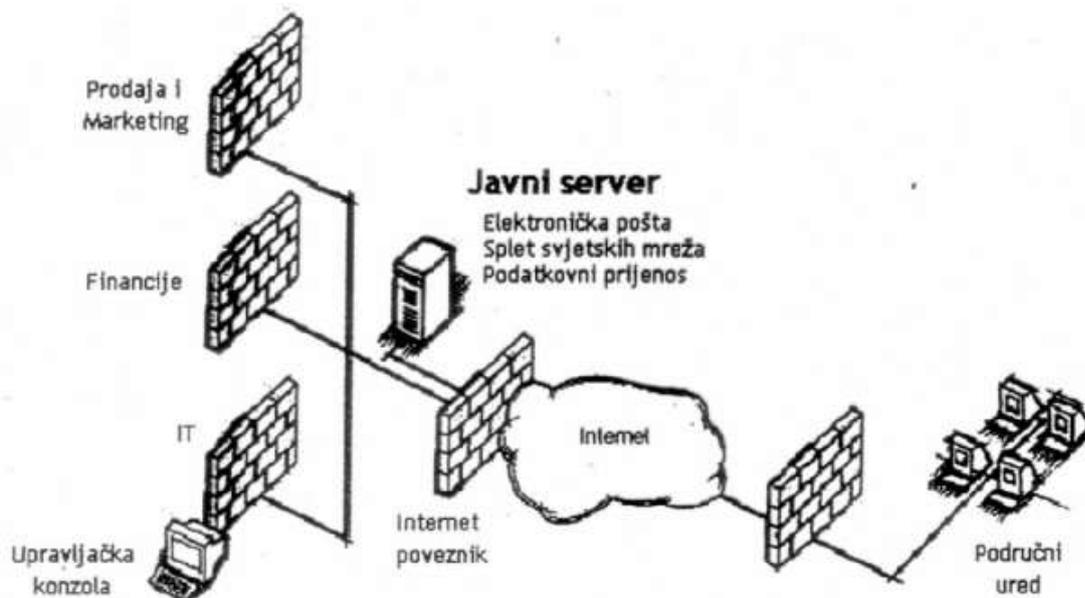
VPN je fleksibilan način komuniciranja koji povećava djelotvornost mreže, te korisniku štedi vrijeme i novac.

13.4. Vrste virtualnih privatnih mreža

Postoje različite vrste virtualnih privatnih mreža, a uz svaku je vezan specifičan skup tehnoloških zahtjeva. Obzirom na vrstu, VPN mreže mogu se svrstati u tri kategorije:

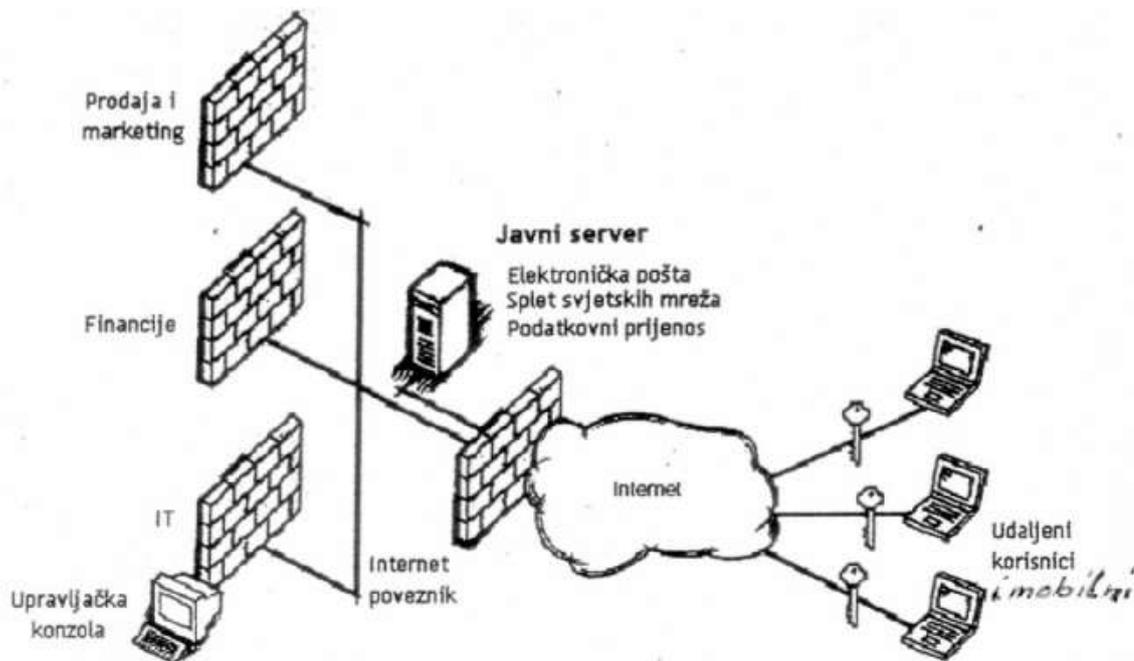
- Intranet VPN mreže,
- VPN mreže s udaljenim pristupom i
- ekstranet VPN mreže.

Intranet VPN mreže između korporacijskih odjela i područnih ureda. Intranet VPN mreže omogućuju sigurno komuniciranje između odjela kompanije i njezinih područnih ureda (slika 1.5.). Primarni tehnološki zahtjevi koji se postavljaju na takvu mrežu su: snažno šifriranje podataka kako bi se zaštitile osjetljive informacije, pouzdanost kako bi se osigurala pravodobna mogućnost ostvarivanja kritičnih aplikacija, skalabilnost upravljanja da bi se ono moglo prilagoditi brzom povećavanju broja novih korisnika, ureda i aplikacija.



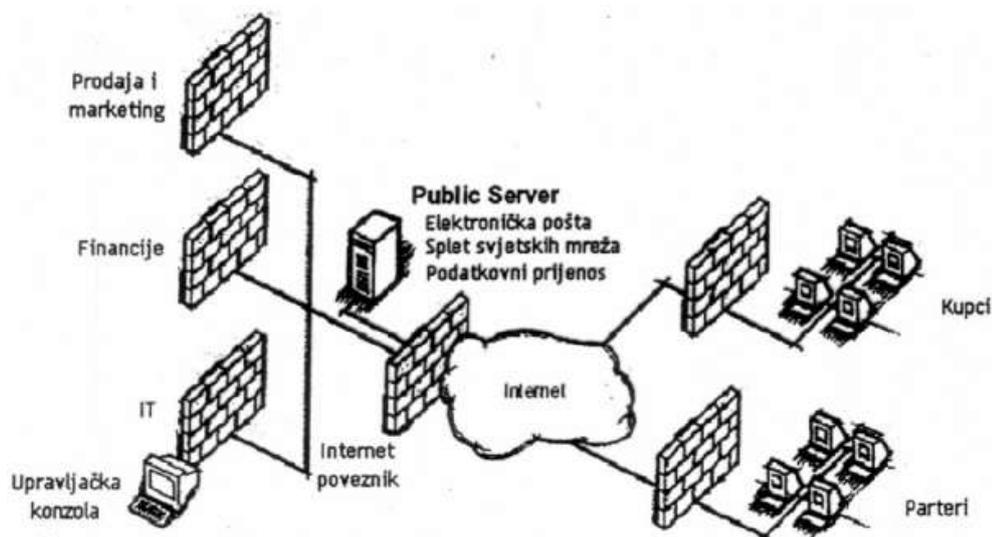
Slika 1.5. Intranet virtualna privatna mreža

VPN s udaljenim pristupom je mreža koja omogućuje komunikaciju između korporacijske mreže i udaljenih ili mobilnih djelatnika (slika 1.6.). Primarni tehnološki zahtjevi koji se postavljaju na takvu mrežu su provjera vjerodostojnosti radi ovjere identiteta udaljenih i mobilnih korisnika, centralizirano upravljanje i visoki stupanj skalabilnosti glede omogućavanja pristupa velikom broju korisnika VPN mreži.



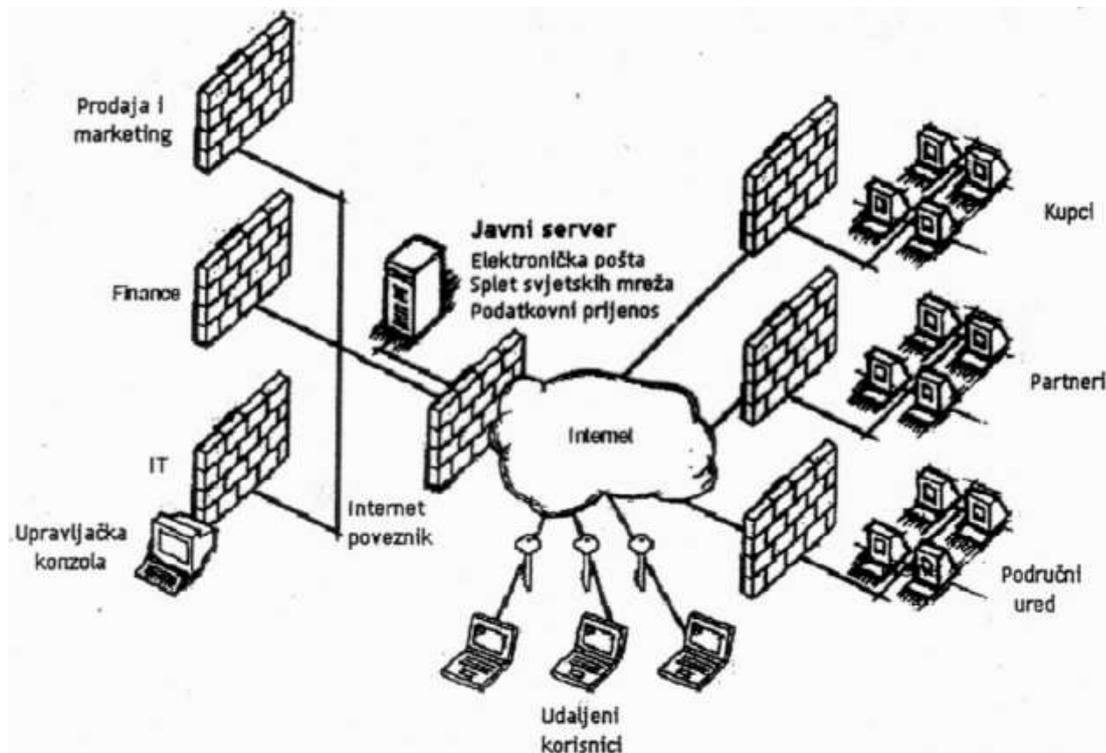
Slika 1.6. Virtualna privatna mreža s udaljenim pristupom

Ekstranet VPN mreža omogućuje komunikaciju između korporacije i njezinih strateških partnera, korisnika ili dobavljača (slika 1.7.). Takva mreža zahtijeva otvoreno rješenje koje se temelji na standardima da bi se osigurala interoperabilnost s različitim rješenjima koja mogu implementirati strateški partneri. Prihvaćeni standard za VPN mreže temeljene na Internetu je standard sigurnosnog protokola Interneta IPsec (*Internet Protocol Security*). Jednako je važan i nadzor prometa da bi se eliminirala prometna zagušenja u pristupnim točkama mreže i mogla jamčiti brza isporuka i odziv kritičnih podataka.



Slika 1.7. Ekstranet virtualna privatna mreža

Rješenje virtualne privatne mreže mora podržavati sve tri gore navedene aplikacije (intranet virtualna privatna mreža, virtualna privatna mreža s udaljenim pristupom, ekstranet virtualna privatna mreža) da bi se udaljenim i mobilnim djelatnicima, područnim uredima širom svijeta, te strateškim partnerima omogućio pristup mrežnim resursima. Međutim, ako korporacija planira implementirati samo jednu od tri vrste VPN u danom trenutku, tada mora to odabrano rješenje osiguravati dodavanje jedne ili obje preostale vrste VPN mreže (slika 1.8.).



Slika 1.8. Implementacija sve tri vrste VPN mreža

14. VPN TEHNOLOGIJE

Dva primarna čimbenika o kojima treba voditi računa pri ostvarivanju VPN mreže preko Interneta su sigurnost i radni učinak. Međutim, protokol nadzora prijenosa / međumrežni protokol TCP/IP i Internet nisu projektirani tako da bi osiguravali ta dva čimbenika, jer veliki broj korisnika i vrsta aplikacija ne zahtijevaju jake sigurnosne mjere niti zajamčene performanse. Kako VPN mreža, temeljena na Internetu, treba poslužiti kao pouzdana zamjena za unajmljene linije ili druge WAN veze, tehnologije koje jamče sigurnost i mrežne performanse moraju se dodati Internetu.

Standardi za sigurnosne mrežne protokole na IP mrežama su razvijeni, pa se IP mreže mogu koristiti pri kreiranju VPN mreža. Rad na osiguravanju zajamčenih performansi je veoma intenzivan, ali rezultati toga rada za sada nisu primijenjeni u IP mreži u širokim razmjerima.

TCP (*Transmission Control Protocol*) osigurava pouzdan transport s kraja na kraj, pomoću mehanizma potvrde i retransmisije uz očuvani redosljed niza okteta.

Najvažniji Internetski protokoli koji djeluju na transportnome sloju su TCP i UDP.

14.1. Funkcije ostvarivanja sigurnosti prijenosa podataka

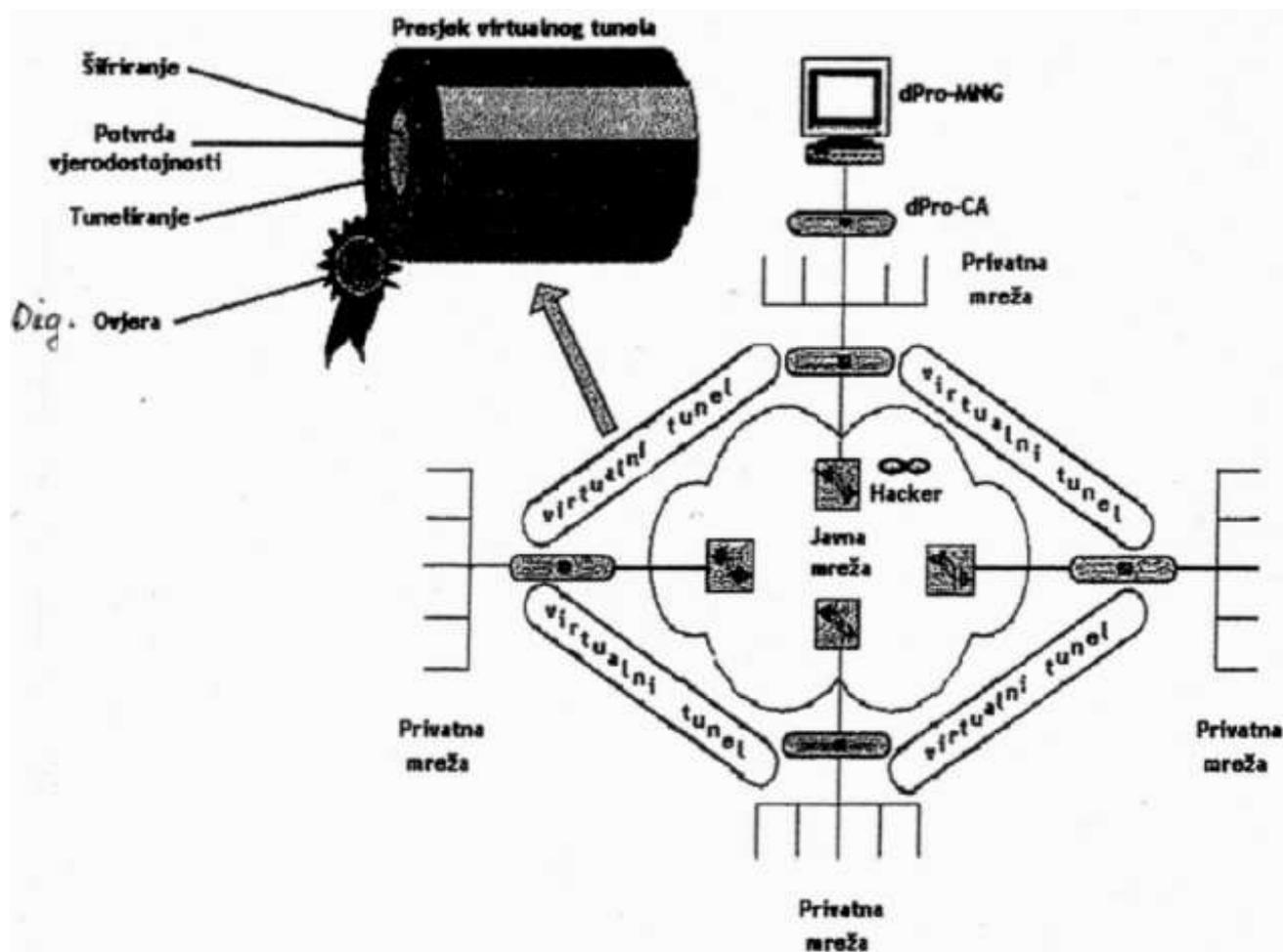
VPN mreže trebaju omogućiti četiri kritične funkcije koje će jamčiti sigurnost podataka, a to su:

- provjera vjerodostojnosti - utvrđivanje da li podaci potječu iz izvora za koji se to tvrdi,
- nadzor pristupa - sprječavanje upada u mrežu neovlaštenim korisnicima,
- ostvarivanje povjerljivosti - sprječavanje čitanja ili kopiranja podataka dok prolaze kroz mrežu Internet,
- ostvarivanje integriteta podataka - osiguravanje pouzdanog protoka podataka kroz Internet.

IP sam za sebe nije dovoljan za dostavu datagrama od izvora do odredišta, kada se izvor i odredište nalaze različitim mrežama. U tom slučaju potrebna je podrška protokola mrežnog sloja, protokola usmjeravanja i protokola nadzora.

Funkcije IP: adresiranje, specifikacija vrste usluge, fragmentacija poruke i ponovno sastavljanje, te specifikacija potrebnih mogućnosti. IP ne vodi računa da li je datagram stigao na odredište i to u ispravnome redoslijedu.

Slika 2.1. prikazuje mrežu koja sadrži četiri privatne mreže uzajamno povezane preko javne telekomunikacijske mreže. Privatne mreže se nalaze između sigurnosnih VPN uređaja i povezane su na javnu mrežu preko usmjerivača. Podaci se prenose kroz javnu mrežu po dodijeljenoj sigurnoj stazi. tzv. virtualnom tunelu.



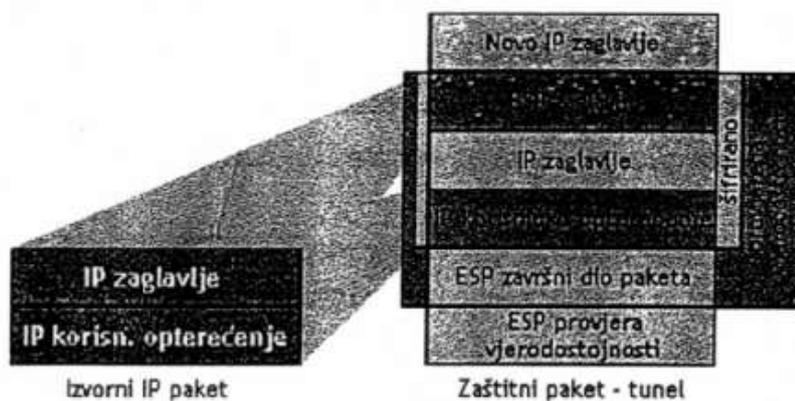
Slika 2.1. Sigurnosni algoritmi VPN mreža

Za provjeru vjerodostojnosti na razini korisnika u VPN mreži i nadzor pristupa mrežnim resursima upotrebljavaju se lozinke, protokoli, usluga za provjeru vjerodostojnosti na daljinu, primjerice usluga RADIUS (*Remote Authentication Dial-In User Service*), digitalna ovjera (*digital certification*) i karakteristični pristupni znakovi temeljeni na sklopovlju. Privatnost informacija koje se prenose kroz VPN je zaštićena šifriranjem podataka.

U prošlosti su se ostvarivale privatne mreže unajmljivanjem žičanih linija po kojima bi se odvijao promet jednog korporacijskog korisnika. Kako bi se ta koncepcija proširila i na Internet, gdje se promet mnogih korisnika odvija preko iste veze, predloženi su brojni protokoli za ostvarivanje tunela. Tuneliranje je način ostvarivanja veze između točaka ulaza i izlaza u složenoj mreži. Softver na strani klijenata inicira tunel, a ekvivalentni softver na centralnoj strani ga završava.

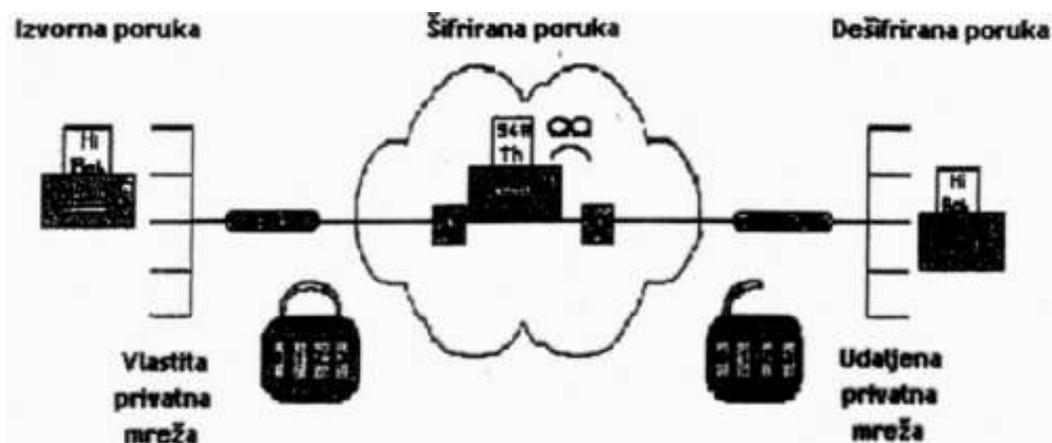
Pri tome se upotrebljavaju slijedeći protokoli:

- protokol kojim predajnik ovija (*encapsulate*) podatke (*payload*) i zaglavlje svog paketa u veći IP paket,
- *host* protokol kojim se dodaje novo IP zaglavlje za ostvarivanje usmjeravanja paketa kroz mrežu,
- protokol koji se upotrebljava za prijenos paketa kroz mrežu (slika 2.2.).



Slika 2.2. IPSec zaštita podataka

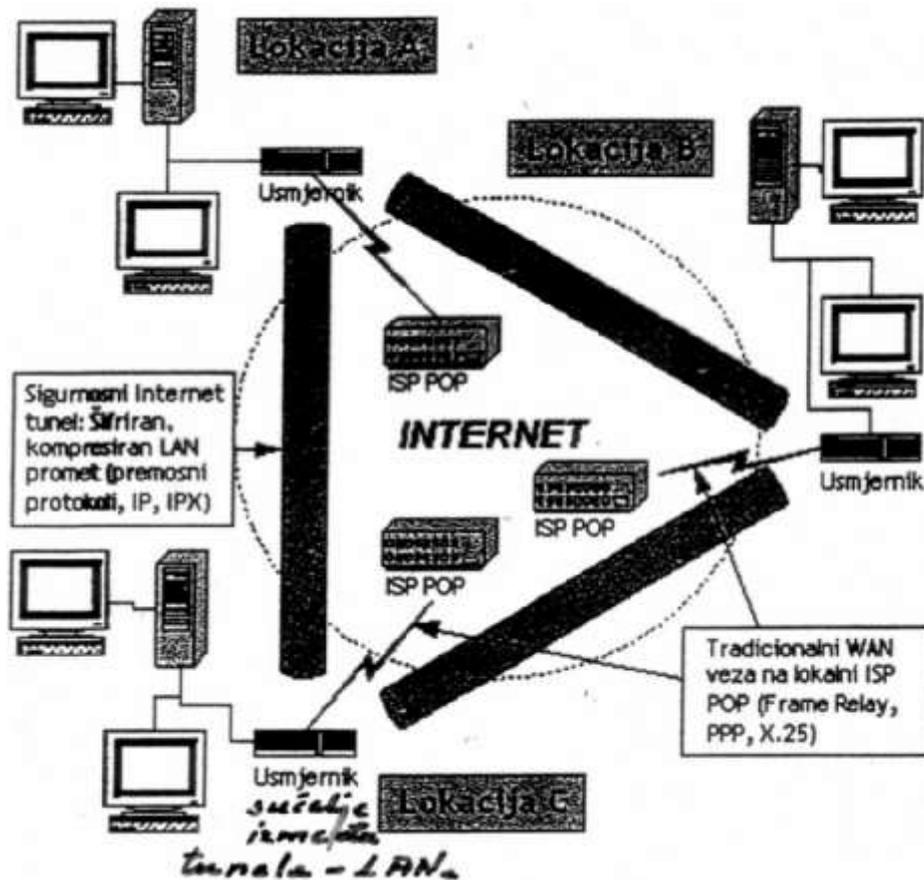
Ovijeni paketi mogu se zaštititi od neovlaštenih korisnika uporabom tehnika šifriranja, što prikazuje slika 2.3.



Slika 2.3. Zaštita poruka uporabom šifriranja

Tuneli mogu sadržavati dvije vrste krajnjih točaka: računalo ili LAN sa sigurnosnim poveznikom koji može biti usmjerivač ili vatrozid. Međutim, ipak se samo dvije kombinacije ovih krajnjih točaka uzimaju u obzir pri projektiranju VPN mreže.

U primjeru LAN-LAN tuneliranja, koji je prikazan na slici 2.4., sigurnosni poveznik u svakoj krajnjoj točki služi kao sučelje između tunela i privatne lokalne mreže. U takvim slučajevima korisnici lokalnih mreža mogu transparentno koristiti tunel za međusobnu komunikaciju.



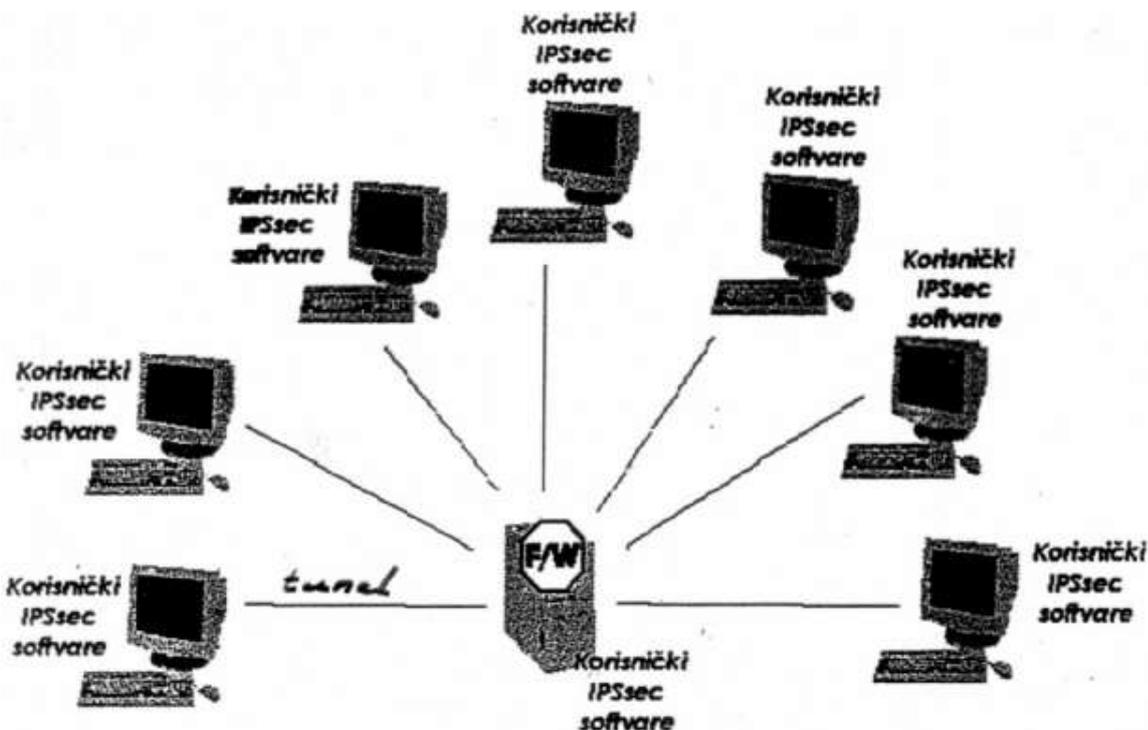
Slika 2.4. LAN-LAN tuneliranje

Drugi primjer tuneliranja prikazan je na slici 2.5. Klijent-LAN tunel je vrsta tunela namijenjena mobilnim korisnicima koji se žele priključiti na korporacijsku lokalnu mrežu. Klijent, tj. mobilni korisnik koji želi uspostaviti vezu s korporacijskom mrežom radi razmjene podataka, pokreće stvaranje tunela uporabom posebnog programa (*Client Program*) na svom računaru za komuniciranje s poveznikom, zaštićujući određenu LAN mrežu.

Program klijenta je program koji omogućuje računalu da djeluje kao klijent.

Zadaci tog programa su:

- osigurava korisničko sučelje za slanje zahtjeva poslužitelju,
- formatira zahtjev da ga poslužitelj razumije,
- formatira odgovor poslužitelja da ga korisnik razumije.



Slika 2.5. Klijent - LAN tuneliranje

Riječ "virtualno" u VPN podrazumijeva da je mreža logički formirana, neovisno o fizičkoj strukturi podslojne mreže, u ovom slučaju, Interneta. VPN mreža, za razliku od unajmljenih linija koje su se upotrebljavale u tradicionalnim korporacijskim mrežama, ne podržava stalne veze između krajnjih točaka korporacijske mreže. Veza između dva centra ostvaruje se samo onda kada je potrebna. Kada više nije potrebna, veza se isključuje stavljajući pojasnu širinu i druge mrežne resurse na raspolaganje ostalim mrežnim korisnicima. Veze koje rabi VPN mreža nemaju iste fizičke karakteristike kao veze koje se rabe u lokalnoj mreži.

Aplikacijski promet tipično se dijeli u četiri grupe, iako su ga neke kompanije uspjele podijeliti u 12 grupa. Različiti korisnici ili grupe korisnika zahtijevaju različite razine zaštite i sigurnosti prometa. Postoje četiri razine zaštite i sigurnosti prometa:

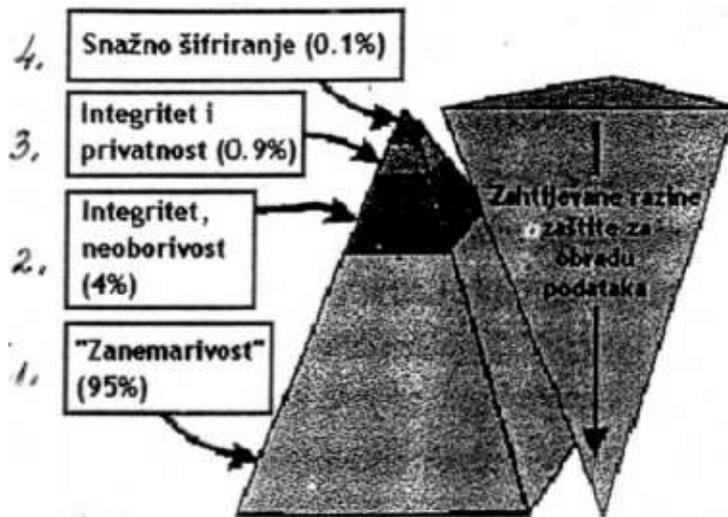
RAZINA 1: zanemarivost zaštite (*don't care*). Podaci koji ne zahtijevaju primjene posebnih postupaka zaštite, odnosno kod kojih se zaštita zanemaruje, pripadaju prvoj razini zaštite prometa. Provjera vjerodostojnosti korisnika i šifriranje podataka ne primjenjuju se. Procjenjuje se da približno 95% podataka spada u ovu skupinu (slika 2.6).

RAZINA 2: integritet podataka, neoborivost (*integrity, non-refutability*). Podaci s drugom razinom zaštite nisu osjetljivi, ali moraju biti zaštićeni tijekom prijenosa. Zahtijeva se provjera vjerodostojnosti, ali ne i šifriranje podataka.

RAZINA 3: integritet podataka i privatnost (*data integrity and privacy*). Ovi podaci zahtijevaju osiguravanje privatnosti u stanovitoj mjeri. Stoga se primjenjuje provjera vjerodostojnosti i slabo šifriranje podataka.

RAZINA 4: snažno šifriranje (*strong encryption*). Ovi podaci zahtijevaju osiguravanje maksimalne privatnosti, pa se koristi snažno šifriranje podataka i provjera vjerodostojnosti na razini korisnika.

Slika 2.6. prikazuje tipičnu podjelu prometa prema razini zaštite i sigurnosti.



Slika 2.6. Vrste prometa i razine zaštite

14.2. Ostvarivanje virtualne privatne mreže putem Interneta

Telekomunikacije s neprestano novim i sve sofisticiranijim komunikacijskim mogućnostima umnogome su pridonijele širenju poslovanja s područja jednog grada i države na područja više država pa i kontinenta. Razvoj Interneta utjecao je na bolju komunikacijsku povezanost u smislu prijenosa podataka i dostupnosti informacija.

Mogućnost razmjene informacija, suradnja s poslovnim partnerima, davaocima usluga i s klijentima osnove su današnjeg poslovanja. Međutim, povećanjem opsega poslovanja i broja zaposlenika i klijenata, održavanje kakvoće komunikacije postaje sve veći izazov. Tako se paralelno širenjem Interneta počela rađati ideja o ostvarivanju "vlastite" poslovne mreže uporabom infrastrukture Interneta. Pitanje sigurnosti prijenosa podataka počelo se rješavati primjenom vlastitih rješenja proizvođača opreme i operativnih sustava. Tako se na tržištu pojavio Microsoft-ov PPTP i Cisco-ov L2F standard za tuneliranje podataka.

Stanice koje su članice istoga VLAN-a mogu međusobno komunicirati preko LAN komutatora drugog sloja. Stanice koje su članice različitih VLAN-ova, mogu međusobno komunicirati samo posredstvom usmjernika. Informacije se prenose u okvirima MAC formata.

Mogućnost prijenosa podataka po dodijeljenim sigurnim stazama, tzv. tunelima dovela je do ideje kreiranja VPN mreže uporabom javne mrežne infrastrukture Interneta. Nastavilo se raditi na standardizaciji, nastao je novi L2TP protokol i sve više se počinju razvijati tehnike šifriranja podataka kako bi se što bolje zaštitili podaci na, svima dostupnom, Internetu. VPN usluga je široko prihvaćena u SAD i to ne samo zbog široke rasprostranjenosti Interneta nego i zbog znatno niže cijene VPN usluga u odnosu na klasične usluge prijenosa podataka.

Osnovan je i Konzorcij virtualne privatne mreže, VPNC (*Virtual Private Network Consortium*), zbog velikog broja pružatelja VPN usluge. VPNC okuplja proizvođače opreme i programske podrške za VPN.

Glavni ciljevi VPNC su:

- promoviranje proizvoda svojih članica javnosti i potencijalnim kupcima,
- osiguravanje međusobnog rada između proizvoda različitih proizvođača opreme,
- davanje objašnjenja javnosti i potencijalnim kupcima u vezi VPN tehnologije i standarda,
- pružanje podrške i reklamiranje ispitivanja interoperabilnosti,
- podrška Forumu svjetskih proizvođača VPN opreme.

Cilj organizacije nije kreiranje novih standarda, nego podrška standardima radne skupine IETF na kojima se temelji proizvodnja opreme, rad i održavanje opreme VPN mreže.

IETF (*Internet Engineering Task Force*) je inženjerska radna skupina Interneta, odnosno radno tijelo za razvoj Interneta.

upravljačko polje	odredišna MAC adresa	izvorišna MAC adresa	LLC PDU LLC PCI + LLC SDU	polje za zaštitu okvira od pogrešaka
-------------------	----------------------	----------------------	------------------------------	--------------------------------------

Slika x.y: Generička struktura MAC PDU (MAC okvira)

Kreiranje MAC protokola podataka jedinice (PDU):

Na sloju iznad LLC kreiraju se paketi (npr. IP),

Paketi na podsloju LLC postaju servisne podatkovne jedinice (LLC SDU) na temelju protokolne upravljačke informacije – PCI. To znači da je LLC PDU = LLC PCI + LLC SDU (korisnička informacija).

Prijenos podataka preko Interneta ili drugih javnih mreža putem VPN tunela temelji se na uporabi različitih tehnika tuneliranja, odnosno protokola drugog sloja kao što su PPTP, L2F, L2TP. Ovjera vjerodostojnosti pošiljaoca podataka i njihovo šifriranje, odnosno zaštita IP komunikacije u tunelu ostvaruje se uporabom IPSec protokola.

14.3. Protokoli razvijeni za VPN

Predložena su četiri različita protokola za kreiranje VPN mreža preko Interneta:

- protokol tuneliranja od točke do točke PPTP (*Point-to-point Tunneling Protocol*),
- protokol za prosljeđivanje na drugom sloju L2F (*Layer 2 Forwarding Protocol*),
- protokol tuneliranja na drugom sloju L2TP (*Layer 2 Tunneling Protocol*) i
- sigurnosni protokol IPSec.

Jedan od razloga postojanja nekoliko protokola je što neke kompanije rabe VPN kao zamjenu za servere s udaljenim pristupom dopuštajući mobilnim korisnicima i razgranatim uredima pristup u zaštićenu korporacijsku mrežu putem lokalnog davaoca Internet usluga, ISP (*Internet Service Provider*). Drugima VPN služi za prijenos prometa u sigurnim tunelima preko Interneta između zaštićenih lokalnih mreža.

Protokoli koji su razvijani za VPN odražavaju mogućnosti uporabe za različite namjene. Tako su PPTP, L2F i L2TP protokoli uglavnom namijenjeni za uporabu u biranim (dial-up) VPN mrežama, dok je IPSec protokol u prvom redu namijenjen za LAN-LAN tuneliranje.

Koji će se protokol izabrati, ovisi o tome kako se planira rabiti VPN mreža. Nekad su ograničenja glede uporabe protokola vezana za korištenu opremu, jer se uvijek ne može imati nadzor nad opremom. Primjerice, pri ostvarivanju VPN mreže za povezivanje s poslovnim partnerom nismo u poziciji diktirati koju će opremu on upotrijebiti na svojim lokacijama.

14.3.1. Protokol tuneliranja od točke do točke (PPTP)

Jedan od prvih protokola koji je razvijen za VPN je protokol tuneliranja od točke do točke, PPTP - protokol. Taj je protokol bio u širokoj upotrebi za birane VPN mreže, otkad je Microsoft ponudio PPTP klijenta u uslužnom paketu za Windows 95. Microsoftovo uključivanje PPTP klijenta u Windows 98 praktično osigurava njegovu kontinuiranu uporabu slijedećih nekoliko godina, premda nije vjerojatno da će PPTP postati uobičajen standard propisan od nekog tijela za normizaciju [primjerice, inženjerske radne skupine Interneta, IETF (*Internet Engineering Task Force*)].

Protokol koji se najviše upotrebljava za daljinski pristup Internetu je protokol za komunikaciju od točke do točke, PPP. Protokol PPTP je izgrađen na funkcionalnosti PPP protokola kako bi se omogućio daljinski pristup koji se može ostvariti tunelom kroz Internet do odredišta. PPTP ovija PPP pakete rabeći modificiranu verziju protokola GRE (*Generic Routing Encapsulation*) koji pruža PPTP protokolu fleksibilnost podržavanja protokola različitih od IP, kao što su IPX (*Internet Packet Exchange*) i NetBEUI (*Network Basic Input/Output System Extended User Interface*).

Osim relativno jednostavne klijent podrške za PPTP protokol, jedna od glavnih prednosti protokola PPTP je što je dizajniran za uporabu na drugom sloju modela otvorenih komunikacija (OSI), za razliku od IPSec protokola, koji je dizajniran za rad na trećem sloju. Podržavanjem podatkovne komunikacije na drugom sloju, PPTP može koristiti razne protokole preko svojih tunela. Međutim, postoje i neka ograničenja protokola PPTP. Taj protokol ne omogućuje snažno šifriranje za zaštitu podataka i ne podržava nijednu metodu temeljenu na znaku (*Token-based Methods*), tj. na karakterističnoj kombinaciji bitova za provjeru vjerodostojnosti pošiljatelja podataka.

Značajke PPTP protokola:

- dizajniran za tuneliranje prometa od korisnika do komunikacijske mreže; radi na drugom sloju OSI modela,
- može podržavati različite protokole (IPX NetBEUI), a ne samo IP,
- rabi protokol od točke do točke (PPP) za provjeru vjerodostojnosti udaljenog korisnika,
- ne omogućuje snažno šifriranje i ne podržava metodu temeljenu na *tokenu* za provjeru vjerodostojnosti pošiljatelja podataka.

14.3.2. Protokol za prosljeđivanje na drugom sloju (L2F)

Protokol za prosljeđivanje (podataka) na drugom sloju (L2F) također se pojavljuje u ranom razdoblju razvitka VPN mreže. L2F protokol dizajniran je za tuneliranje prometa od korisnika do njegove korporacijske mreže kao i PPTP protokol. Jedna od glavnih razlika između PPTP i L2F protokola je što L2F tuneliranje nije ovisno o Internet protokolu (IP) i može se izravno rabiti s različitim tehnologijama prijenosa informacija kao što je prosljeđivanje okvira (*frame relay*) ili asinkroni način prijenosa (ATM).

Poput PPTP protokola, L2F protokol rabi PPP protokol za utvrđivanje vjerodostojnosti udaljenog biranog korisnika. L2F se razlikuje od PPTP protokola, jer dopušta podršku većem broju veza kroz tunel. Uspoređujući PPTP dizajn, L2F rabi PPP protokol za utvrđivanje vjerodostojnosti biranog (*dial-up*) korisnika.

Osnovna razlika L2F i PPTP protokola:

- L2F tuneliranje može se ostvariti uporabom različitih prijenosnih tehnologija (ATM, *frame relay*, nije ovisno o Internetu).

14.3.3. Protokol tuneliranja na drugom sloju (L2TP)

L2TP je protokol druge razine, zbog čega nudi korisnicima istu fleksibilnost kao PPTP protokol za rukovanje protokolima različitim od Internet protokola (IP), kao što su IPX i NetBEUI. L2TP protokol je dizajnirala radna skupina IETF kao nasljednika PPTP i L2F protokola. L2TP je dizajniran da otkloni nedostatke ranije razvijenih protokola i postane standard koji će odobriti radna skupina IETF.

L2TP upotrebljava PPP protokol kako bi omogućio birani (*dial-up*) pristup koji se može ostvariti tuneliranjem kroz Internet do odredišta. Ipak, L2TP definira svoj vlastiti protokol za tuneliranje temeljen na L2F protokolu. Namjena L2TP protokola je definirana za različite tehnologije prijenosa, uključujući X.25, prosljeđivanje okvira i ATM.

Značajke L2TP:

- otklanja nedostatke ranije razvijenih protokola (PPTP, L2F),
- podržava različite prijenosne tehnologije (ATM, X25, *frame relay*),
- rabi sigurnosni protokol IPSec i prošireni PPP za provjeru vjerodostojnosti.

L2TP rabi metode šifriranja IPSec protokola i uključuje mehanizme za provjeru vjerodostojnosti unutar PPP protokola, jer rabi PPP protokol za birane (*dial-up*) linkove. L2TP, slično kao i PPTP protokol, podržava uporabu PPP-ovog proširenog protokola za provjeru vjerodostojnosti, koji služi za druge sustave provjere vjerodostojnosti u sustavu kao što je RADIUS.

PPTP, L2F i L2TP protokoli ne podržavaju šifriranje niti postupke za upravljanje ključevima potrebnim za šifriranje. Sadašnji nacrt standarda L2TP protokola preporuča da se IPSec rabi za šifriranje i upravljanje ključem u IP okružju. Budući nacrt PPTP standarda možda će to isto donijeti.

14.3.4. IP sigurnosni protokol (IPSec)

Najnoviji, ali možda najvažniji protokol je IPSec, koji je razvijen kao rezultat nastojanja da se zaštite paketi IP protokola slijedeće generacije, tj. paketi šeste verzije Internet protokola IPv6 (*Version 6 of Internet Protocol*). Protokol IPSec također se može rabiti i sa sadašnjom četvrtom verzijom protokola IP (IPv4).

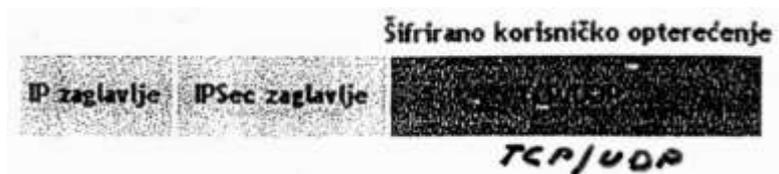
Poboljšanje protokola IPv6 u odnosu na sadašnji IPv4 protokol ogleda se u:

- povećanju IP adrese od 32 na 128 bitova, što je nužno obzirom na budući rast Interneta,
- poboljšanju usmjeravanja paketa,
- podržavanju kakvoće usluge (QoS).

IPSec protokol dopušta predajniku provjeru vjerodostojnosti ili šifriranje svakog IP paketa ili istodobnu primjenu oba postupka.

IPSec omogućuje:

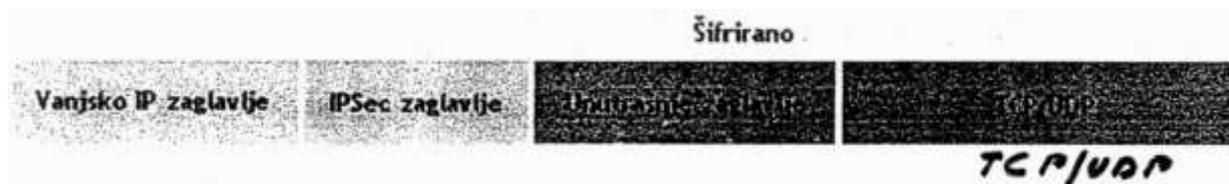
- predajniku provjeru vjerodostojnosti i/ili šifriranje svakog IP paketa verzije IPv4 i IPv6,,
- dva moda uporabe:
 - transportni mod (provjera vjerodostojnosti i šifriranje samo korisničkog opterećenja) i
 - tunelski mod (provjera vjerodostojnosti i šifriranje čitavog IP paketa – bolji za zaštitu IP paketa na Internetu.



Slika 2.7. Uporaba IPSec protokola u transportnom modu

Postoje dva različita moda uporabe IPSec protokola: transportni i tunelski mod. U transportnom modu obavlja se provjera vjerodostojnosti ili šifriranje samo transportnog slojnog segmenta IP paketa, zbog čega je pogodniji za uporabu u lokalnim mrežama (slika 2.7.).

U tunelskom modu obavlja se provjera vjerodostojnosti ili šifriranje čitavog IP paketa zbog čega je pogodniji za uporabu u Internet mreži (slika 2.8.).



Slika 2.8. Uporaba IPSec paketa u tunelskom modu

Transportni mod IPSec protokola može se pokazati korisnim u mnogim situacijama, dok tunel mod IPSec protokola omogućuje bolju zaštitu od napada i praćenje prometa (*Traffic Monitoring*) na Internetu.

IPSec protokol se uzima kao najbolje rješenje glede sigurnosti u IP okružju, jer osigurava povjerljivost, integritet podataka, provjeru valjanosti i upravljanje ključem.

IPSec protokol je dizajniran samo za baratanje IP paketima, dok su protokoli PPTP i L2TP pogodniji za uporabu u višeprotokolnom ne-IP okruženju.

Za tvrtke koje zahtijevaju fleksibilnu globalnu mrežu, siguran prijenos podataka podržavanje udaljenih korisnika i extraneta, IPSec je najprikladnije rješenje.

UDP (*User Datagram Protocol*) omogućava nespojnu nepouzdanu uslugu transporta UDP paketa povrh IP-a. UDP paketi nisu numerirani (ne može se utvrditi redoslijed paketa na prijemnoj strani), ne provjerava se da li je prilikom transporta došlo do pogreške ili nije. O pouzdanosti se brine sama aplikacija. Na UDP-u se temelji npr. aplikacija transfera datoteka, TFTP (*Trivial File Transfer Protocol*)

15. KOMPONENTE VIRTUALNE PRIVATNE MREŽE

Virtualna privatna mreža koja se temelji na uporabi Interneta ima četiri glavne komponente: Internet, sigurnosne poveznike, sigurnosne nadzorne servere i mehanizme za po vjerodostojnosti.

Internet omogućuje temeljnu podlogu za VPN mreže. Sigurnosni poveznici se nalaze između javne i privatne mreže sprečavajući neovlaštene upade u privatnu mrežu. Oni također omogućuju tuneliranje i šifriranje privatnih podataka prije prijensa u javnu mrežu. Sigurnosni poveznici za VPN mreže uglavnom se uklapaju u jednu od slijedećih kategorija: usmjernici, vatrozidovi, integrirani VPN *hardware* i VPN *software*.

Usmjernici moraju ispitati i obraditi svaki paket koji napušta lokalnu mrežu, što znači da oni trebaju obaviti šifriranje paketa. Isporučitelji VPN usluga usmjernika obično nude dva tipa proizvoda: dodatni softver ili sklopovsku pločicu sa zaštitnim koprocesorskim uređajem. Ovaj drugi proizvod uporabljiv je za situacije kada je potrebna veća propusnost. Kompanije koje već rabe usmjernike određenih proizvođača mogu smanjiti troškove nadgradnje VPN mreže ugradnjom podrške za šifriranje.

Mnogi proizvođači vatrozidova u svoje proizvode ugrađuju mogućnost tuneliranja. Vatrozidovi, poput usmjernika moraju procesirati sav IP promet preko filtara definiranih za vatrozid. Zbog svih funkcija obrade koje trebaju izvršiti, vatrozidovi nisu pogodni za tuneliranje u velikim mrežama s velikim volumenom prometa. Kombiniranje tuneliranja i šifriranja s vatrozidom vjerojatno je najbolje rješenje za male mreže s malim volumenom prometa, iako oni poput usmjernika mogu biti mjesto kvara u VPN mreži.

Četiri glavne komponente VPN:

- Internet – temeljna podloga VPN,
- sigurnosni poveznici (usmjernici, vatrozidovi, integriran VPN sklop i VPN program) – sprječava neovlaštene upade u VPN,
- sigurnosni nadzorni server – za prepoznavanje ovjerenog prometa temeljem pristupnih nadzornih lista ili drugih informacija vezanih za korisnika,
- potvrde vjerodostojnosti za provjeru ključeva za šifriranje podijeljenih među centrima i za provjeru korisnika uporabom digitalne potvrde.

Izgradnja VPN uporabom vatrozidova je rješenje koje je izvedivo za neke mreže. VPM mreže koje se temelje na vatrozidu su dobar izbor za relativno male mreže koje prenose male količine podataka (reda 1-2 Mb/s po WAN linku) i ne zahtijevaju često rekonfiguraciju.

Jedno od mogućih VPN rješenja uključuje uporabu specijalnog hardvera koji je dizajniran za tuneliranje, šifriranje i provjeru vjerodostojnosti korisnika. Ovi uređaji uglavnom rade kao mostovi za šifriranje koji su obično smješteni između mrežnih usmjerivača i WAN linkova. Većina ovih hardverskih tunela je dizajnirana za LAN-LAN konfiguracije, dok neki proizvodi podržavaju klijent-LAN tuneliranje.

VPN softver služi za kreiranje i upravljanje tunelima između dva sigurnosna poveznika ili udaljenog korisnika i sigurnosnog poveznika. Softverski VPN sustavi nude optimalnu potrošnju za relativno male sustave koji ne obrađuju veliki promet. Ta rješenja se mogu primijeniti na postojećim serverima i

dijeliti resurse s njima, a mogu poslužiti i za upoznavanje problematike VPN mreža. Mnogi od ovih softverskih VPN sustava su prilagođeni za klijent-LAN veze.

Pored sigurnosnog poveznika važna komponenta VPN mreže je sigurnosni nadzorni server. Taj server sadrži pristupne nadzorne liste i ostale informacije vezane za korisnika, koje sigurnosni poveznik rabi za prepoznavanje ovjerenog prometa. Primjerice, u nekim sustavima pristup se može nadzirati uporabom RADIUS servera.

Potvrde vjerodostojnosti su potrebne za provjeru ključeva podijeljenih među centrima, a mogu poslužiti i za provjeru pojedinaca uporabom digitalnih potvrda. Kompanije imaju mogućnost ugradnje posebnog korporacijskog servera za održavanje vlastite baze podataka digitalnih potvrda za korisnike. Kada korporacijska VPN mreža preraste u extranet, potrebna je i uporaba potvrde vjerodostojnosti za provjeru korisnika od strane poslovnog partnera.



Slika x.y: Model Internetske usluge klijent-poslužitelj

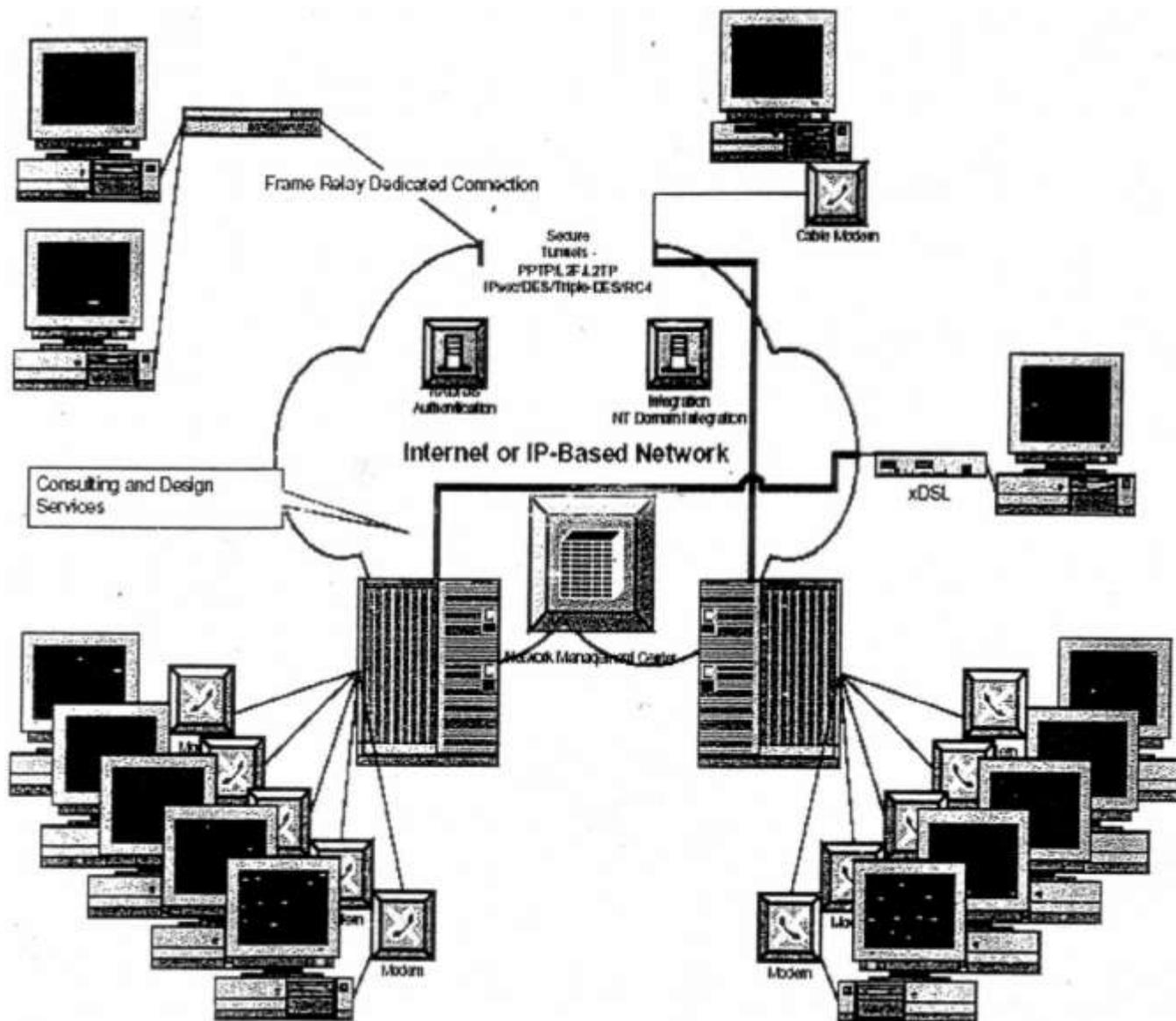
Program klijenta je *software* koji omogućuje računalu da djeluje kao klijent. Zadaci programa su: pruža korisniku sučelje za slanje zahtjeva poslužitelju, formira zahtjev da ga server razumije, formatira odgovor servera da ga korisnik razumije.

16. VPN USLUGA U NAŠOJ ZEMLJI I U SVIJETU

Vrlo je teško kreirati uslugu u domeni VPN koja bi odgovarala svim profilima korisnika i zadovoljila sve njihove potrebe, odnosno jednostavne do složenijih komunikacijskih i sigurnosnih zahtjeva. Stoga T-Com, prateći svjetske trendove i nastojeći dati pravi odgovor na komunikacijske zahtjeve svojih korisnika, osim postojeće usluge virtualne privatne birane mreže, VPDN *basic*, uvodi i dodatne usluge s većim mogućnostima.

16.1. VPN usluga T-Com: virtualna privatna birana mreža (VPDN)

VPN usluga T-Com-a temelji se na zakupu fiksnog pristupa Internetu i uspostavljanju "odvojenih veza" putem Interneta. Pri tome se upotrebljava tehnika L2TP tuneliranja i IPSec protokol za zaštitu podataka koji se prenose. Ukoliko se korisnik na svoju lokalnu mrežu spaja s udaljene lokacije putem birane (dial-up) veze, govorimo o biranoj (dial-up) VPN ili VPDN mreži (slika 4.1.).



Slika 4.1. Virtualna privatna birana mreža (VPDN)

Značajke VPN usluge T-Com-a:

- fiksni pristup Internetu i uspostava sigurnosnih staza (tunela) uporabom L2TP,
- zaštita podataka uporabom IPSec,
- komuniciranje putem birane (dial-up) veze (riječ je o VPDN mreži),
- omogućuje povezivanje do 100 udaljenih lokacija,
- korisnik VPDN rabi modemske ulaze,
- korisnik se povezuje s centralnom lokacijom VPDN koristeći modemske ulaze, podizanje tunela L2TP preko ISDN ili POTS mreže.

Usluga *Basic* VPDN, koju je T-Com predstavio na sajmu Info 2001, namijenjena je korisnicima koji imaju potrebu za povremenim povezivanjem do 100 udaljenih lokacija. Korisnik VPDN usluge rabi T-Com modemske ulaze, te se putem ISDN ili POTS uz podizanje L2TP tunela, spaja na centralnu lokaciju korporacijske mreže priključene stalnom vezom na T-Com. Usluga uključuje tuneliranje podataka do centralne lokacije korporacije, pa korisnik nema izlaz na Internet nego je razmjena podataka moguća samo unutar kreirane VPN mreže.

Izlaz korisnika VPDN usluge na Internet može se ostvariti putem centralne lokacije korisnika. Usluga spajanja centralne lokacije određuje se prema cjeniku VPN usluge, tj. prema cjeniku PRO, PRO-DUAL ili PRO-TREND usluge, ako korisnik želi izlaz na Internet. Spajanje VPDN korisnika uključuje registraciju korisničkih računa za zatraženi broj klijenata. Svakom korisničkom računu se dodjeljuje korisničko ime i lozinka za pristup usluzi.

Kako sve više kompanija shvaća prednosti implementacije VPN usluga za povezivanje svojih lokacija, putem stalnih ili biranih (dial-up) veza, Sektor podatkovnih mreža i negovornih usluga, u suradnji sa Sektorom pripreme plasmana i nadzora nad uslugama, razvio je uslugu koja zadovoljava potrebe korisnika. T-Com posjeduje vrhunsku infrastrukturu i uz pomoć njihovih stručnjaka, korisnici mogu izgraditi robusnu, privatnu i skalabilnu VPN mrežu.

16.2. VPN usluge u svijetu

Svjetska iskustva govore o razlikama u ponudi VPN mreža kod pojedinih ponuđača glede vrste pristupa (analogni, ISDN, ADSL ili pristup stalnom vezom), upotrijebljenih protokola, načina potvrde vjerodostojnosti te dodatnih mogućnosti. Neke od poznatih svjetskih kompanija koje nude usluge u vezi s VPN mrežama su: *Global Crossing*, *WorldCom*, *Ardent Communication*, *AT&T* i *Genuity*.

Kompanija *Global Crossing* je uvela VPN usluge temeljene na Internetu u listopadu 2001. godine. *Global Crossing* je osnovan 1997. godine, a trenutačno posjeduje veliku mrežu koja povezuje više od 200 svjetskih gradova s ukupno 100 000 milja optike.

Prisutni su u Sjevernoj i Južnoj Americi, Europi i Aziji.

Njihova ponuda sastoji se od triju različitih usluga: *SmartRoute IP VPN Service*, *ExpressRoute IP VPN Service* i *Premises-Based IP VPN Service*.

SmartRoute IP VPN Service je usluga koja omogućuje korisnicima odrediti prioritet prometa birajući između triju različitih razina prioriteta. Usluga rabi IPsec protokol, a ponuda uključuje brzine od 2 do 34 Mb/s.

ExpressRoute IP VPN Service - ova usluga rabi MPLS protokol (*Multi-Protocol Label Switching*). Usluga je namijenjena velikim kompanijama ili davateljima usluga koji imaju potrebe za velikim kapacitetima - do 155Mb/s ili gigabitni Ethernet. Usluga se naplaćuje prema uporabi.

Premises-Based IP VPN Service - usluga je namijenjena kompanijama koje imaju potrebu za manjim kapacitetima. Pristupnu opremu, uključujući i usmjernike, kupuje korisnik, ali je konfigurira *Global Crossing*.

U lipnju 2001. godine i *WorldCom* kompanija je najavila svoju IP VPN uslugu. Kao i mnoge druge kompanije i *WorldCom* vidi budućnost u ponudi ove usluge. Njihova usluga rabi IPsec protokol, omogućuje povezivanje više stotina lokacija, a upravljanje je jednostavno. Podržava pristup zakupljenim vezama ili putem komutirane telefonske mreže.

Ardent Communication kompanija osnovana je 1993. godine, pruža usluge pristupa Internetu u SAD. Svoju IP VPN uslugu uvela je u listopadu 2001. godine. Usluga rabi MPLS protokol i jamči kakvoću usluge.

AT&T kompanija također omogućuje korisniku da odabere protokol koji želi koristiti: *Point-to-point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP) ili IPsec. Korisnik također može odabrati 56-bitnu ili 128-bitnu shemu šifriranja, a i načine provjere vjerodostojnosti. Korisnik može odabrati i vrstu opreme na svojoj strani - *Nortel* ili opremu temeljenu na *Linuxu*.

Kompanija *Genuity* također nudi pristup putem zakupljenog voda i dial-up veze, podržava digitalnu potvrdu. To je jedna je od rijetkih kompanija koja nudi sporazum na razini usluge, SLA (*Service-Level Agreement*), kojim se definira maksimalan broj izgubljenih paketa. Korisnici dobivaju kredit u koliko je broj izgubljenih paketa veći od 1 %.

Ovo su samo neke od kompanija koje nude VPN usluge. Svakim danom sve više kompanija nudi VPN usluge temeljene na Internetu. Ponude variraju, ali svim ponudama zajedničko je isticanje jednostavnosti VPN usluge, ekonomičnosti, te mogućnosti da vlasnik prepusti svoju mrežu drugome, kako bi brinuo o njoj.

Treba naglasiti da se najvažniji sigurnosni zahtjev odnosi na korisnički promet preko jezgrene mreže davatelja usluga. Kako jezgrenu mrežu može sačinjavati nekoliko mreža različitih davatelja usluga, to

je jedan od uzroka da VPN nije potpuno sigurna mreža. Čak i onda kada je davatelj usluga vlasnik čitave mreže, korisnik se može zaštititi od neovlaštenih pristupa mreži.

16.2.1. Sigurnosni Internet protokol (IPSec)

Protokol koji nastoji ostvariti sigurni prijenos podataka preko mreže mora pružati tri osnovne sigurnosne usluge:

- ovjeru vjerodostojnosti (*authentication*) - ovjeru vjerodostojnosti korisnika i izvora paketa (provjeru da li paketi potječu iz izvora za koji se to tvrdi),
- provjeru integriteta (*integrity check*) - provjeru da li je sadržaj paketa mijenjan tijekom prijenosa (namjerno ili zbog slučajnih pogrešaka),
- ostvarivanje povjerljivosti (*confidentiality*) - zaštitu jasnog teksta poruke uobičajeno sa šifriranjem i sigurnom distribucijom ključeva za šifriranje.

Međutim, IP mreža poput Interneta teško ostvaruje gore navedeno. Različite vrste sigurnosnih protokola definirane su za različite aplikacije u Internetu (primjerice, *secure socket layer* za web promet, *secure shell* za prijave udaljenih korisnika, *pretty good privacy* za elektroničku poštu). Njihov je zajednički nedostatak što su aplikacijski specifični pa se prilikom gradnje aplikacije mora graditi i novi sigurnosni mehanizam.

IPSec pruža navedene sigurnosne usluge potrebne za sigurno komuniciranje i za razliku od drugih sigurnosnih protokola osigurava:

- transparentnost za sve aplikacije (IPSec se implementira na mrežnom sloju),
- bolju zaštitu protiv sigurnosnih napada (otporan na napade: uskraćivanje usluge, čovjek u sredini, na rječnik),
- neovisnost o mrežnoj topologiji (može se upotrijebiti s bilo kojom mrežnom topologijom),
- mogućnost za uzajamno djelovanje različitih implementacija različitih proizvođača, (IPSec je prihvaćen kao norma).

IPSec je zapravo skup protokola koji nudi usluge na IP sloju, omogućujući sustavu da odabere zahtijevane sigurnosne protokole, odredi algoritam/algoritme za sigurnosne usluge i obavi sigurnu izmjenu ključeva radi ostvarivanja zahtijevanih usluga. IPSec može se upotrijebiti za zaštitu jedne ili više staza između para glavnih računala (*hostova*) između para sigurnosnih poveznika (*Security gateways*) ili između sigurnosnih poveznika i glavnog računala. Termin *sigurnosni poveznik* odnosi se na usmjernik ili vatrozid u kojem su implementirani IPSec protokoli.

Sigurnosne usluge se implementiraju uporabom sigurnosnih protokola i asocijacija koje je definirala IPSec radna skupina IETF tijela za razvoj Interneta.

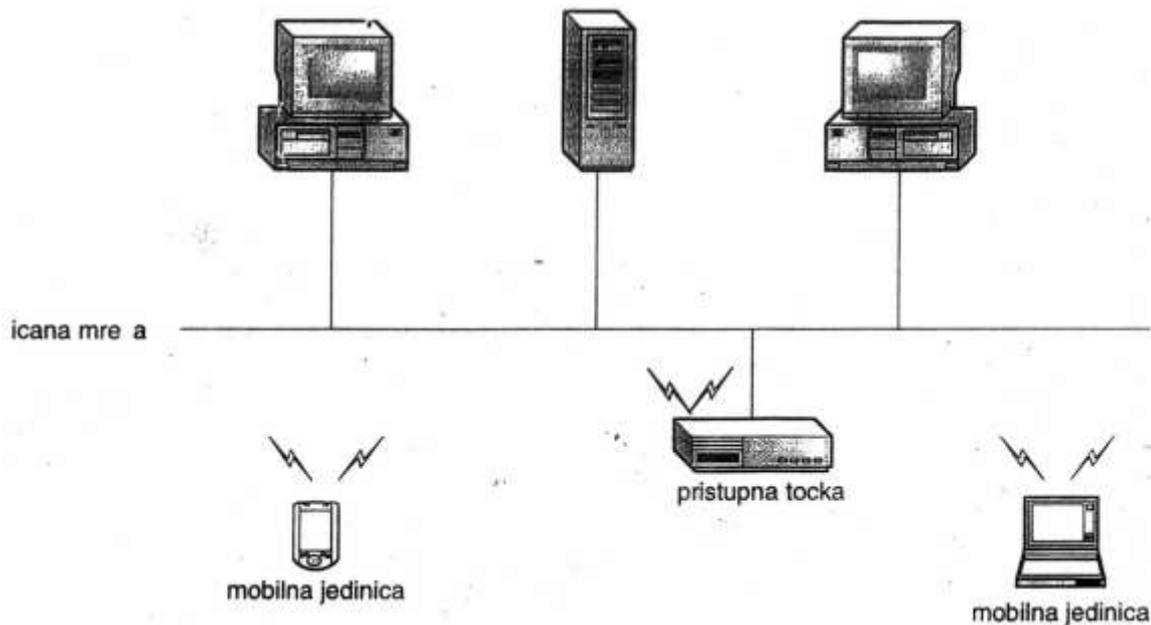
To su niže navedeni protokoli:

- Zaglavlje ovjere vjerodostojnosti, AH (*authentication header*) - protokol koji omogućuje ovjeru vjerodostojnosti izvora podataka, integritet podataka te zaštitu od ponovljenog napada.
- Protokol sigurnosnog enkapsuliranja korisničkog opterećenja, ESP (*Encapsulating Security Payload Protocol*) koji pruža ovjeru vjerodostojnosti izvora podataka, osigurava povjerljivost podataka putem šifriranja, integritet podataka i opcijski zaštitu protiv ponovljenog napada.
- Protokol izmjene ključeva Interneta, IKE, (*Internet Key Exchange Protocol*) temelji se na protokolu ISAKMP. To je protokol dogovaranja sigurnosnih usluga između dva IPSec entiteta. Dogovaranje obuhvaća: metode ovjere vjerodostojnosti, metode šifriranja, uporabu ključeva, vrijeme uporabe ključeva prije njihove promjene.

Sigurnosna asocijacija Interneta i protokol upravljanja ključevima, ISAKMP (*Internet Security Association and Key Management Protocol*) - je metoda za automatsko definiranje sigurnosnih asocijacija (skup sigurnosnih informacija koji se odnosi na veze dane mreže ili skup veza) i baratanje ključevima za šifriranje.

17. WLAN MREŽA STANDARDA 802.11 b

Bežične lokalne mreže odašilju i primaju podatke slobodnim prostorom, osiguravaju pokretljivost korisnika, mogućnost povezivanja i pristup postojećim mrežnim resursima, primjerice Internetu i različitim *on-line* uslugama s različitih lokacija (slika 1.).



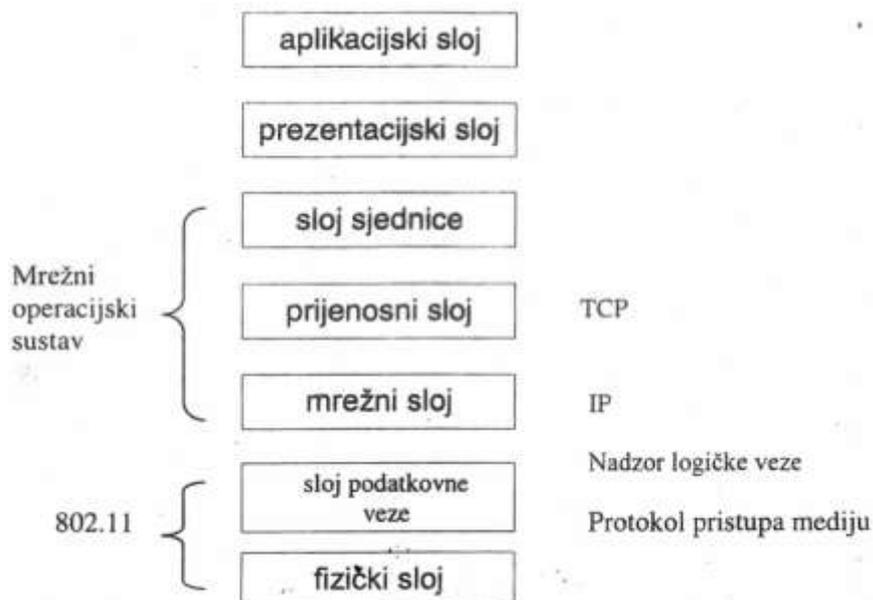
Slika 1. Bežična LAN mreža

Široko prihvaćanje WLAN (*Wireless Local Area Network*) tehnologije ovisi o standardizaciji koja treba osigurati kompatibilnost i pouzdanost WLAN opreme različitih proizvođača. Standard za bežični LAN 802.11 odobrio je Institut inženjera elektrotehnike i elektronike, IEEE (*Institute of Electrical and Electronics Engineers*), 1997. godine. WLAN mreža koja se temelji na ovom standardu omogućuje brzine prijenosa od 1 Mb/s do 2 Mb/s.

Standard 802.11b, prihvaćen je 1999. godine, a osnovno mu je obilježje kompatibilnost s osnovnim standardom te povećavanje brzine prijenosa podataka do 11 Mb/s. WLAN mreža temeljena na ovom standardu može ostvariti performanse i propusnost usporedivu sa žičanim Ethernetom.

Standard 802.11 definira specifikacije pristupa prijenosnom mediju, MAC (*Media Access Control*) i fizičke razine, PHY (*Physical Layer*), tj. prva dva sloja ISO modela lokalne mreže (slika 2.).

Bilo koja aplikacija LAN, mrežni operacijski sustav ili protokol mogu lako ostvariti međudjelovanje s WLAN 802.11 standardom.



Slika 2. Standard 802.11 i ISO model

Osnovna arhitektura, svojstva i usluge mreže temeljene na 802.11b standardu su definirane prvobitnim standardom 802.11. Specifikacija 802.11b utječe samo na fizički sloj, dodajući veće brzine prijenosa i veću robusnu povezanost.

17.1. Fizički sloj

LAN mreža može se izgraditi uporabom sljedećih tehnologija:

- infracrvene,
- mikrovalne,
- i radio-frekvencijske tehnologije.

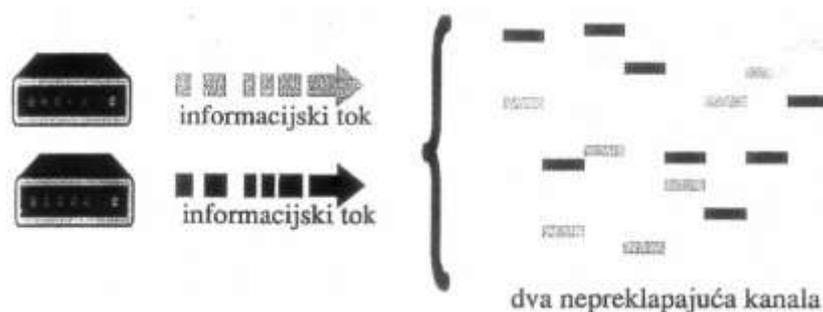
Radio-frekvencijska tehnologija s raspršenim spektrom upotrebljava se najčešće, jer omogućuje veću pouzdanost i propusnost, malu gustoću snage i redundanciju. Stoga su ovakve mreže otporne na šum i interferenciju.

Postoje dvije vrste tehnologija s raspršenim spektrom:

tehnologija raspršenog spektra s poskakivanjem frekvencije, FHSS (*Frequency Hopping Spread Spectrum Technology*),

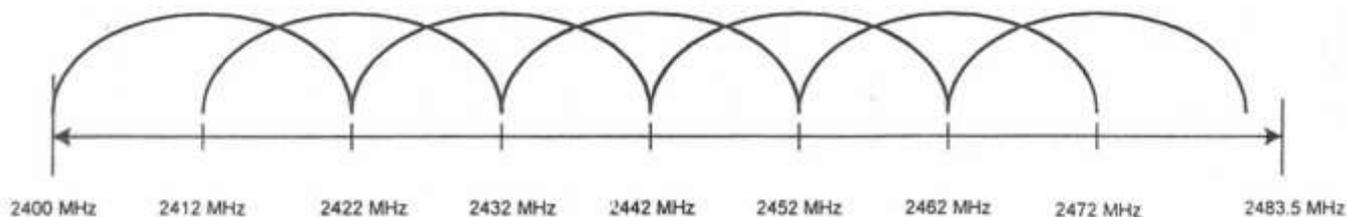
tehnologija raspršenog spektra s izravnim nizom, DSSS (*Direct Sequence Spread Spectrum Technology*).

Frekvencijski pojas (2.4 GHz) u FHSS sustavima dijeli se u mnogo malih podkanala (primjerice 75 podkanala širine 1 MHz). Predajnik odašilje kratke nizove podataka na određenoj frekvenciji određeno vrijeme i potom se prebacuje na drugu frekvenciju (slika 3.).



Slika 3. FHSS prijenos

Predajnik i prijemnik trebaju biti sinkronizirani prema sekvenci poskakivanja⁴ kako bi podržali logički kanal, jer u suprotnom dolazi do gubitka podataka. Sustav koji se temelji na tehnologiji poskakivanja frekvencije otporan je na interferenciju, jer se frekvencija stalno mijenja. Ako se pojavi interferencija na jednoj frekvenciji podaci se ponovno odašilju na drugoj frekvenciji. Kontinuirano mijenjanje frekvencije čini FHSS sustav manje podložnim presretanju i preslušavanju prijenosa od neovlaštenih stanica. Tim se postiže visoki stupanj sigurnosti prijenosa. FHSS tehnologija ima i relativno jednostavan radio-dizajn, ali prijenos brzinama ne prelazi 2 Mb/s. To ograničenje postavilo je Savezno povjerenstvo za komunikacije, FCC (*Federal Communications Commission USA*), propisima koji ograničavaju širinu podkanala na 1 MHz. Ovim se propisima zahtijeva uporaba FHSS sustava preko čitavog 2.4 GHz pojasa, što znači da moraju često poskakivati, a to dovodi do visokog preteka preskakanja.



Slika 4. Preklapajući kanali standarda 802.11b u Europi

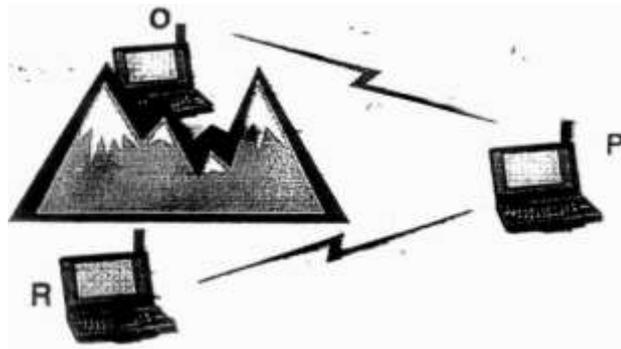
Međutim, DSSS sustavi dijele 2.4 GHz pojas na četrnaest 22 MHz kanala. Susjedni kanali se djelomično preklapaju, a od toga su tri kanala nepreklapajuća (slika 4.). Podaci se šalju 22 MHz kanalom bez skakutanja po drugim kanalima, a pri modulaciji signala se upotrebljava generirani slučajni niz. Bitovi podataka se preslikavaju u kodirane uzorke koji se dekodiraju na prijemnoj strani. Ako je jedan ili više bitova u uzorku oštećeno tijekom prijenosa, ugrađene statističke tehnike mogu obnoviti podatke, stoga nema potrebe za ponovnim prijenosom. DSSS sustavi postižu brzine i do 11 Mb/s, otporniji su na prekide i smetnje (zbog sposobnosti raspršenja signala na šire frekvencijsko područje) u odnosu na FHSS sustave, pa imaju nešto veći domet. Sve tehnologije 802.11 su izvedene tako da su interoperabilne sa žičanim Ethernet LAN mrežama i drugim uređajima iste vrste. Standard 802.11b WLAN koristi samo DSSS tehnologiju, jer FHSS sustavi ne mogu podržati zahtijevane brzine prijenosa.

Pri primjeni DSS tehnike, raspršenje spektra podatkovnog toka ostvaruje se zamjenom jedinica (1) u izvornom podatkovnom toku sa specifičnim slijedom podbitova tzv. čipova (*chips*), a nule (0) se zamjenjuju inverzijom navedenih podbitova. Što je signal raspršeniji manja je vjerojatnost frekvencijske interferencije.

17.2. Sloj podatkovne veze

Sloj podatkovne veze sadrži dva podsloja: protokol pristupa mediju, MAC (*Media Access Control*) i nadzor logičke veze, LLC (*Logical Link Control*). U tradicijskim LAN mrežama primjenjuje se uglavnom metoda višestrukog pristupa otkrivanjem nosioca i otkrivanjem sudara CSMA/CD kao protokol pristupa mediju.

⁴ Engleski naziv i definicija???

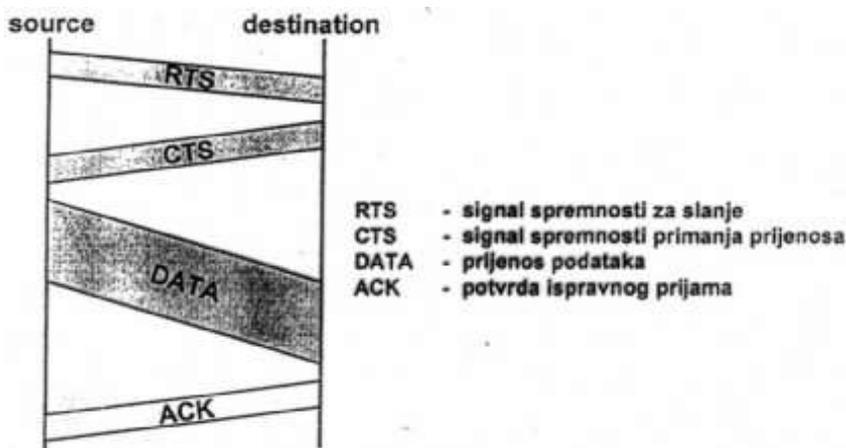


Slika 5. Problem skrivene stanice

Pri korištenju ovog pristupa stanica osluškuje ima li prometa na mreži prije nego li će početi odašiljanje. Ako netko već odašilje, stanica će pričekati i pokušati ponovno. Ako dvije stanice istodobno odašilju doći će do sudara paketa, odnosno gubitka informacije. Kada se otkrije sudar obje stanice prekidaju odašiljanje. Potom ponovno pokušavaju poslati dotične pakete.

Metoda pristupa mediju CSMA/CD dobro funkcionira kod žičanih LAN mreža. Međutim od WLAN mreža se pojavljuje problem skrivene stanice (slika 5.). Primjerice, ako stanica R nije u mogućnosti «čuti» stanicu O, a stanica O već odašilje, stanica R će početi istodobno odašiljati i dolazi do sudara. Ovaj se problem rješava uporabom protokola višestrukog pristupa otkrivanjem nosioca i izbjegavanjem sudara, CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*).

Primjenom ovog protokola stanica osluškuje medij kako bi detektirala eventualni prijenos podataka. Ako prijenos postoji, ne pokušava slati podatke. U protivnome, ona ne započinje odmah s odašiljanjem paketa, već prvo šalje signal spremnosti za slanje, RTS (*Ready to Send*). Ovaj signal sadrži adresu primatelja podataka i predviđeno trajanje prijensa. Na taj se način ostale stanice obavještavaju koliko trebaju čekati prije nego li i same otpočnu odašiljanje. Stanica koja je označena kao primatelj u RTS signalu, po primitku ovoga signala šalje obavijest o spremnosti primanja podataka, CTS (*Clear to Send*). Nakon toga započinje prijenos podataka (DATA), a primitak svakog paketa mora se potvrditi (ACK), što je vidljivo iz slike 6.



Slika 6. Metoda četverostrukog usklađivanja

ACK mehanizam veoma uspješno rješava interferenciju i slične radio probleme. Paket podataka u WLAN, mreži koja se temelji na standardu 802.11 ima veće zaglavlje u odnosu na zaglavlje paketa u mreži Ethernet pa mreža temeljena na standardu 802.11 ima sporije performanse nego ekvivalentna mreža Ethernet.

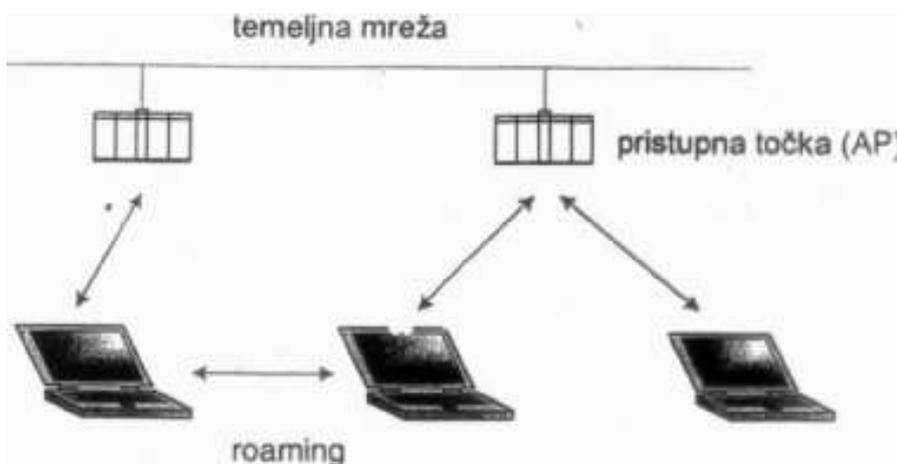
MAC sloj protokola 802.11 osigurava dva svojstva: CRC ispitni zbroj (*Cyclic Redundancy Check*) i fragmentaciju paketa. Svaki paket ima proračunati i odijeljeni CRC ispitni zbroj koji osigurava neometan prijenos podataka. Fragmentacijom paketa veći paketi razbijaju se na manje jedinice, što je korisno pri zagušenju prometa ili kada dođe do interferencije, jer manji paketi imaju veće izgleda da će neometano stići na odredište. U mnogim slučajevima ova tehnika smanjuje potrebu za

retransmisijom i poboljšava performansu bežične mreže. MAC sloj je odgovoran za ponovno sastavljanje primljenih fragmenata, automatski dovršavajući transparentni proces prema protokolima viših razina.

17.3. Pridruživanje pristupnim točkama

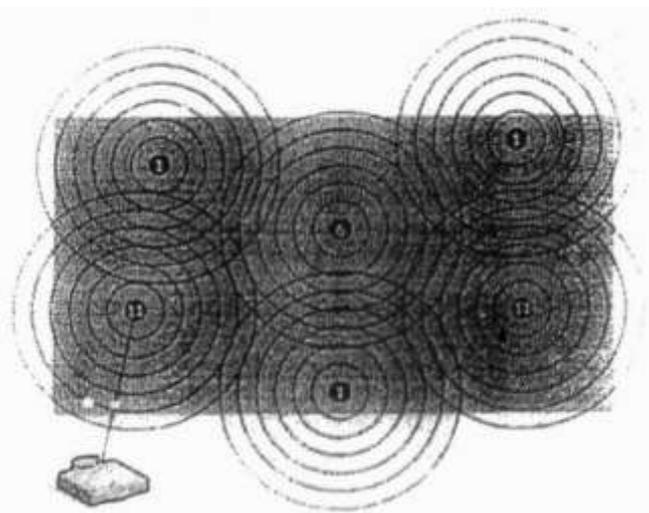
Povezivanje korisnika s pristupnom točkom definira MAC sloj protokola 802.11. Kada paket temeljen na protokolu 802.11 dođe na granicu jedne ili više pristupnih točaka, s obzirom na snagu signala i učestalost pogreške paketa, korisnik odabire pristupnu točku. Ukoliko je prihvaćen od pristupne točke, korisnik se prilagođava radio kanalu na kojem je pristupna točka.

U određenim vremenskim intervalima (periodično) korisnik pregledava sve 802.11 kanale procjenjujući da li druge pristupne točke imaju bolje performanse. Ako ustanovi da je to tako, pridružuje se novoj pristupnoj točki, prebacujući se na radio kanal na kojem je nova pristupna točka (slika 7.).



Slika 7. AP roaming

Do pridruživanja novoj pristupnoj točki obično dolazi, jer se bežična stanica fizički udaljava od izvorne točke. Informacijski signal slabi zbog tog udaljavanja, promjena radio karakteristika u zgradi ili zbog velikog prometa mreže na izvornoj točki pristupa. Posljednji slučaj je poznat kao balansiranje korisničkim opterećenjem, pri čemu se efikasnije raspodjeljuje promet WLAN mreže preko dostupne bežične infrastrukture. Postupak dinamičnog pridruživanja pristupnim točkama omogućuje mrežnim menadžerima izgradnju WLAN mreža s veoma širokom pokrivenošću stvarajući niz preklapajućih 802.11b ćelija.



Slika 8. Neograničen roaming

Da bi bili uspješni, IT (*Information Technology*) menadžeri će zasigurno ponovo upotrijebiti kanal, vodeći brigu da postave svaku pristupnu točku tako, da se 802.11 DSSS kanal ne preklapa s korištenim

kanalom susjedne pristupne točke (slika 8). Od četrnaest djelomično preklapajućih kanala, specificiranih 802.11 DSSS tehnikom, samo su tri kanala koja se ne preklapaju i upravo oni su najbolji za višecelijsko preklapanje.

Međutim, ako su dvije pristupne točke u nizu (na granici) jedna za drugom i ako su postavljene na istom ili djelomično preklapajućim kanalima, mogu prouzročiti međusobnu interferenciju. To dovodi do smanjivanja dostupnosti pojase širine na mjestu preklapanja.

17.4. Načini rada bežične LAL mreže

Standardom 802.11 definirana su dva načina djelovanja WLAN mreže:

- infrastrukturni način,
- *ad hoc* način.

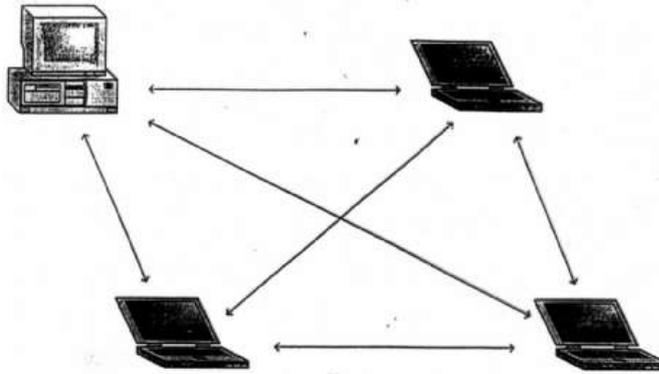
Pri primjeni infrastrukturnog načina rada točku bežična mreža sadrži barem jednu pristupnu točku povezanu s infrastrukturom žičane mreže i niz bežičnih krajnjih stanica (slika 9.). Ova konfiguracija naziva se osnovna uslužna skupina, BSS (*Basic Service Set*). BSS skupina je osnovni standardni građevni element WLA 802.11 mreža. Dvije ili više BSS skupine čine podmrežu, a to je proširena uslužna skupina, ESS (*Extended Service Set*). Kako većina korporacijskih WLAN mreža zahtijeva pristup žičanoj LAN mreži za usluge pristupa Internetu, pa se za prijenos datoteka i drugo koristi infrastrukturni način.



Slika 9. Infrastrukturni način

Kod *ad hoc* načina rada bežične stanice, koje čine neovisne BSS skupine, komuniciraju izravno jedna s drugom bez uporabe pristupne točke ili veze s žičanom mrežom (slika 10). Stanice pri tom uzajamno komuniciraju prema modelu rada ravnopravnih stanica (*peer-to-peer*). Kako ne postoji bazna jedinica, nitko ne daje dozvolu odašiljanja povezanim stanicama. Stoga je ovaj način veoma jednostavan za postavljanje, ali je ograničen glede fizičkih udaljenosti i mogućnosti.

Uzajamno povezane BSS skupine čine infrastrukturu, koja se po standardu 802.11 sastoji od nekoliko elemenata. Dvije ili više BSS skupina povezuju se distribucijskim sustavom, DS (*Distributed System*), čime se povećava opseg funkcije distribucijskog sustava realiziran uporabom pristupnih točaka, AP (*Access Point*). Pristupna točka omogućuje povezivanje BSS skupina, odnosno segmentiranje mreže radi povećanja brzine rada i dometa.



Slika 10. Ad hoc mreža ili IBSS

Definirane usluge koje DS sustav treba podržavati su: usluge stanica, SS (*Station Services*) i usluge distribucijskog sustava, DSS (*Distribution System Services*).

Usluga stanica podrazumijeva provjeru vjerodostojnosti (autentifikacija), deautentifikaciju, privatnost i dostavu MSDU (*MAC Service Data Unit*) okvira. Kod bežičnih sustava pristup prijenosnom mediju nije ograničen fizički kao kod kablinskih sustava. Stoga se za pristup mreži treba izvršiti provjera prava pristupa mrežne stanice, čime stanica potvrđuje svoj identitet i pravo pristupa uslugama. Ovo se naziva provjera vjerodostojnosti i obavlja se između stanica unutar IBSS ili stanice i pristupne točke unutar BSS sustava.

Postoje dva osnovna načina provjere vjerodostojnosti unutar arhitekture standarda 802.11 b:

- otvorena provjera vjerodostojnosti, OSA (*Open System Authentication*), kod koje svaka stanica koja to zatraži dobiva pravo pristupa mreži,
- provjera vjerodostojnosti zajedničkim ključem, SKA (*Shared Key Authentication*), gdje korisnici trebaju posjedovati zajednički ključ koji je ranije dostavljen svim povjerljivim stanicama (instalacijom s diskete).

Deautentifikacija se pokreće kada neka od stanica želi prekinuti vezu s pristupnom točkom, a privatnost je usluga korištenja algoritama šifriranja (WEP) radi sprječavanja prisluškivanja prijenosa od strane neovlaštenih stanica. Dostava MSDU okvira osigurava prijenos podataka provjere vjerodostojnosti i šifriranja između različitih MAC pristupnih točaka.

Skupina IBSS (*Independent Basic Service Set*) je neovisna osnovna uslužna. Za prijenos podataka izvan IBSS skupine, jedna stanica u IBSS mora djelovati kao poveznik (*gateway*) ili usmjernik (*router*), pri čemu rabi programsko rješenje.

Distribucijski sustav ostvaruje pet usluga: povezivanje, raskidanje, ponovno povezivanje, distribuciju i integraciju BSS skupina. Usluge povezivanja, raskidanja i ponovnog povezivanja osiguravaju mobilnost bežičnih stanica (kretanje između BSS segmenata unutar istog ESS segmenata i kretanja između različitih ESS segmenata). Stanica definira svoju pripadnost nekom BSS segmentu povezivanjem s nekom pristupnom točkom. Ovaj način povezivanja je dinamički ukoliko su stanice u pokretu.

Kako stanica može biti priključena istodobno samo na jednu pristupnu točku (tako DS uvijek zna gdje se stanica nalazi), potrebno je dinamički povezivati i raskidati veze s pristupnim točkama. Ovo skakanje veze s jedne na drugu pristupnu točku omogućuje korisniku nesmetano ostvarivanje prijenosa podataka dok je u pokretu, a naziva se *roaming*. Roaming se podržava samo unutar istog ESS segmenta. Ukoliko prijedemo u drugi SS segment veza biva ponovno uspostavljena, ali se započeti prijenos ne nastavlja transparentno, nego ga treba ponovno uspostaviti. Usluge distribucije i integracije omogućuju prijenos korisničkih podataka do odredišta, u koliko je odredište povezano na drugu pristupnu točku, odnosno BSS segment.

17.5. Modulacija

Standard 802.11 DSSS specificira 11-bitovna Barkerova sekvenca za kodiranje podataka poslanih slobodnim prostorom. Niz od 11 chip-ova predstavlja jedan podatkovni bit (1 ili 0) koji se pretvara u oblik zvan simbol, a može se slati zrakom.

Tablica 1. Specifikacija brzine prijenosa podataka

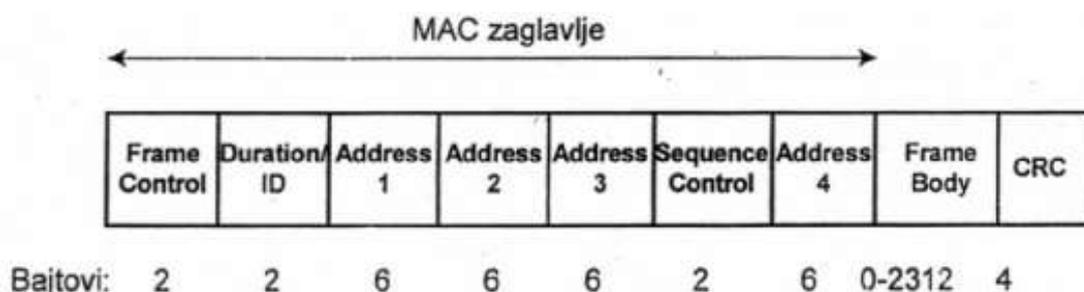
brzina prijenosa podataka	duljina koda	modulacija	brzina simbola	bit (simbol)
1 Mb/s	11 (Barkerova sekvenca)	BPSK	1 MS/s	1
2 Mb/s	11 (Barkerova sekvenca)	QPSK	1 MS/s	2
5,5 Mb/s	8 (CCK)	QPSK	1,375 MS/s	4
11 Mb/s	8 (CCK)	QPSK	1,375 MS/s	8

Simboli prenošeni brzinom od 1 Mb/s koriste digitalnu modulaciju s binarnim faznim pomakom, BPSK (*Binary Phase Shift Keying*). Pri prijenosu brzinom od 2 Mb/s bolje je upotrebljavati četverofaznu digitalnu modulaciju, QPSK (*Quadrature Phase Shift Keying*), pri čemu se povećavanjem djelotvornosti uporabe pojasne širine udvostručuje brzina prijenosa podataka.

Kod 802.11b standarda, zbog povećavanja brzine prijenosa, upotrebljavaju se napredne tehnike kodiranja. 802.11b specificira uporabu CCK (*Complementary Code Keying*) modulacije, koja sadrži niz od 64 8-bitovnih kodnih riječi (radije nego dvije 11-bitovne Barkerove sekvence). Kao niz, ove kodne riječi imaju jedinstveno matematičko svojstvo koje omogućuje primatelju da ih ispravno razdvoji jednu od druge, čak i u prisutnosti znatnog šuma i višestazne interferencije (npr. interferencije uzrokovane primanjem višestruke radio refleksije unutar zgrade). Za brzine prijenosa od 5.5 Mb/s koristi se CCK za kodiranje 4 bita po nosiocu, dok se kod 11 Mb/s brzina kodira 8 bitova po nosiocu. U oba slučaja koristi se QPSK modulacija i signal od 1.357 MS/s (tablica 1.).

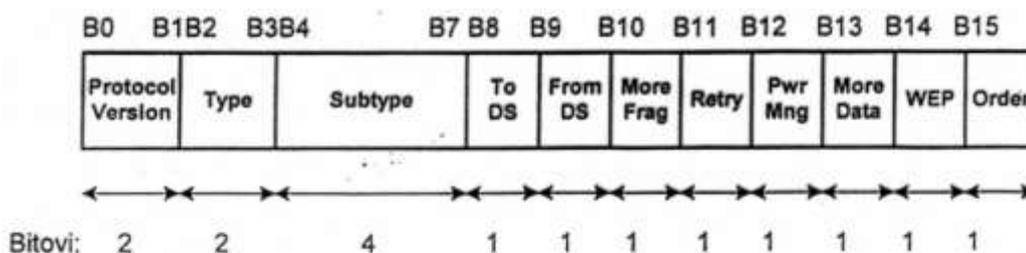
17.6. Oblik okvira

Standard 802.11 specificira i strukturu okvira prijenosa bežičnim LAN sustavima. Svaki okvir se sastoji od MAC zaglavlja, tijela okvira i provjere ispravnosti okvira, FCS (*Frame Check Sequence*). Osnovni okvir je prikazan na slici 11 (duljina polja je dana u bajtovima).



Slika 11: Oblik MAC osnovnog okvira

MAC zaglavlje sadrži 30 bajtova, a sastoji se od sedam polja: kontrole okvira, trajanja i identifikacije, prve adrese, druge adrese, treće adrese, kontrole sekvence i četvrte adrese.



Slika 12. Polje kontrole okvira

Polje kontrole okvira (*Frame Control Field*) je dužine 2 bajta, a sastoji se od 11 potpolja kao što je prikazano na slici 12 (duljine polja u bitovima):

- polje „Protocol Version“ je dužine 2 bita i sadrži verziju 802.11 standarda. Inicijalna vrijednost će biti 0, nakon što 802.11 bude konačno dovršen, dok su sve ostale vrijednosti rezervirane.
- polja „Type“ i „SubType“ su dužine 2 i 4 bita. Prva dva polja, odnosno potpolja definiraju funkcije dotičnog okvira. Svako od preostalih 8 polja ima dužinu 1 bit.
- „To DS“ polje označava ulazi li okvir u DS sustav (tada je 1).
- „From DS“ polje označava napušta li okvir DS sustav (tada je opet 1).
- „More Frag“ polje je 1 kada je ovaj okvir dio većeg okvira.
- „Retry“ polje označava je li okvir ponovio poslani prijašnji okvir.
- „Power Management“ polje označava je li je stanica pošiljatelj u štednom modu (*Power Saving Mode*).
- „More dana“ polje označava kako postoji još MSDU okvira, okvir koji prenosi informacije o MAC usluzi mreže za dotičnu stanicu u međuspremniku.
- U „WEP“ polju postavljen je bit "1", ako je tijelo okvira šifrirano WEP algoritmom.
- U „Order polju“ postavljen je bit "1", ako okviri u prijenosu moraju obvezno biti primljeni u pravom redoslijedu.

Polje trajanja i identifikacije („Duration/ID“) je dužine 2 bajta, a sadrži podatke o vremenu trajanja svakog polja i identifikaciju stanice pošiljatelja kontrolnih okvira. Adresna polja identificiraju BSS sustave, odnosno adresu primatelja, pošiljatelja te adrese prijammnika odnosno predajnika. Svako adresno polje je dužine 6 bajtova. što je standardno za MAC adrese.

Polje kontrole sekvence je dužine 2 bajta i podijeljeno je u dva potpolja, broj fragmenata i broj sekvence. Broj fragmenata je dužine 4 bita i označava na koliko je fragmenata MSDU okvir razbijen, dok je broj sekvence dužine 12 bitova i označava broj sekvence MSDU paketa. Tijelo okvira je dužine od 0 do 2312 bajtova i sadrži samo podatke koji se prenose, dok je polje provjere ispravnosti okvira (FCS) dužine 32 bitova i sadrži cikličku provjeru pogrešaka, CRC (*Cyclic Redundancy Check*).

17.7. Konfiguracije bežične LAN mreže

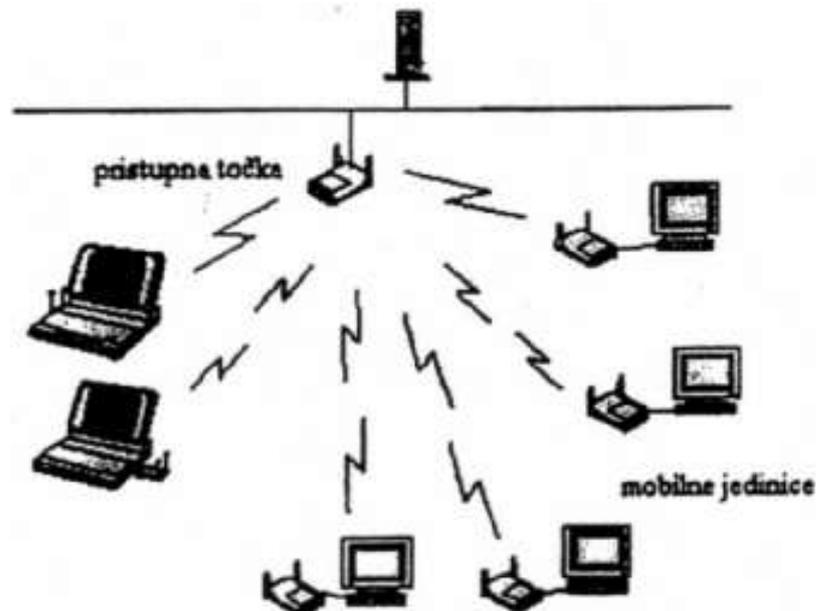
Postoje četiri konfiguracije bežične LAN mreže:

- konfiguracija jedne ćelije – WLAN mreža sastoji se od pristupne točke i bežičnih radnih stanica koje su s njom povezane,
- konfiguracija preklapajućih ćelija - WLAN mreža sastoji se od dvije ili više susjednih pristup točaka čija se područja pokrivanja pomalo preklapaju,
- viševićijska konfiguracija - WLAN mreža sastoji se od nekoliko pristupnih točaka instaliranih na istoj lokaciji što povećava pristupnost,
- višekoračna konfiguracija (*multi-hop*) - WLAN mreža sadrži AP-WB (*bridge*) parove koji proširuju područje pokrivenosti mreže.

Bežična LAN mreža uglavnom sadrži nekoliko tih konfiguracija na različitim mjestima unutar sustava. Konfiguracija jedne ćelije je najjednostavnija i služi kao osnova za druge konfiguracije.

17.7.1. Konfiguracija jedne ćelije

Konfiguracija jedne ćelije najjednostavnija je konfiguracija WLAN mreže. Ona sadrži pristupnu točku i s njom povezane bežične radne stanice.

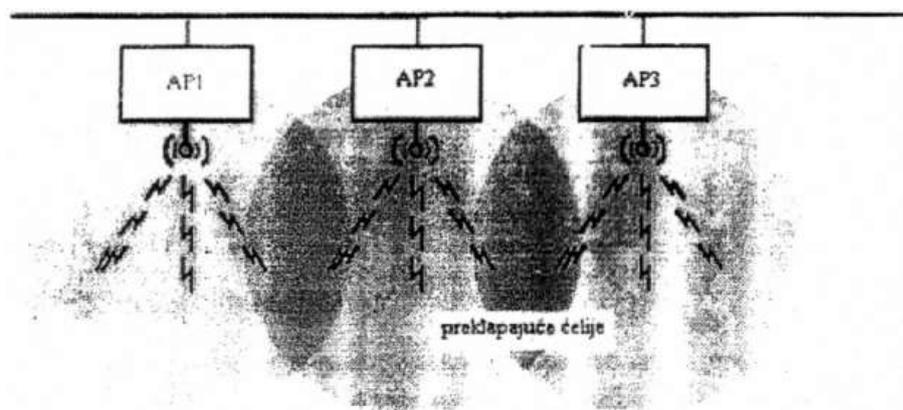


Slika 13. Konfiguracija jedne ćelije

Ova konfiguracija se koristi za male demonstracije gdje se samo želi pokazati da se različiti uređaji mogu povezati u mrežu bez kablova i u uređima gdje se nalazi samo nekoliko (približno 10) korisnika na malom prostoru (slika 13).

17.7.2. Konfiguracija preklapajućih ćelija

Ako su dvije susjedne pristupne točke smještene blizu jedna drugoj, dio područja pokrivenosti jedne pristupne točke preklapa se s područjem pokrivenosti druge pristupne točke (slika 14.).



Slika 14. Konfiguracija preklapajućih ćelija

Ovo preklapanje prostora ima dva važna svojstva:

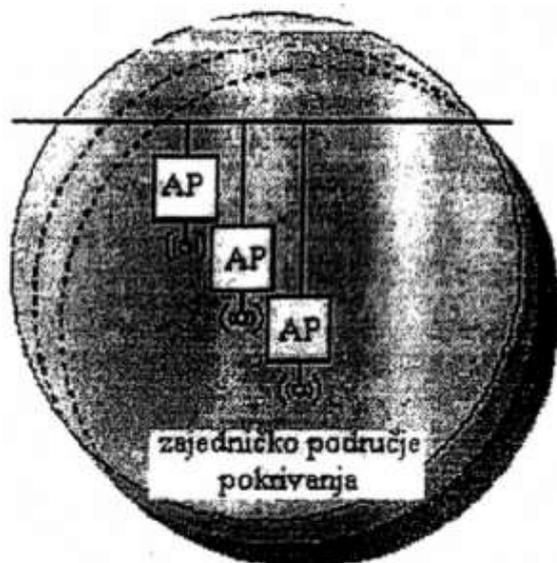
- svaka radna stanica smještena na preklapajućem prostoru može se povezati i komunicirati s prvom ili s drugom pristupnom točkom,
- svaka radna stanica može se bešavno pomicati kroz djelomično preklapajući pokriveni prostor bez gubitka veze s mrežom. Ovo svojstvo naziva se bešavni roaming.

Konfiguracija preklapajućih ćelija koristi se za pokrivanje kata ili cijele zgrade gdje se korisnici žele kretati sa svojim mobilnim jedinicama bez gubitka veze s mrežom.

17.7.3. Višećelijska konfiguracija

U prostorima koji su prenatrpani korisnicima i gdje se obavlja veliki promet koristi se višećelijska konfiguracija (slika 15.). Kod ove konfiguracije nekoliko pristupnih točaka se instalira na istoj

lokaciji. Svaka pristupna točka ima isto područje pokrivanja, a svaka radna stanica u preklapajućem prostoru može se povezati i komunicirati s bilo kojom pristupnom točkom koja pokriva to područje.

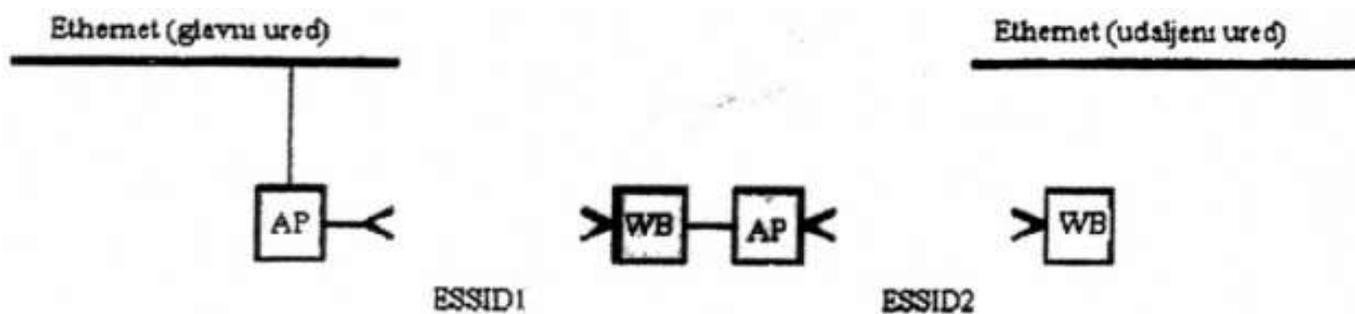


Slika 15. Višećelijska konfiguracija

Ova se konfiguracija primjerice može koristiti u konferencijskim sobama, gdje je više korisnika koji se žele istovremeno povezati na mrežu, pa se zahtijeva veća propusnost.

17.7.4. Višekoračna konfiguracija

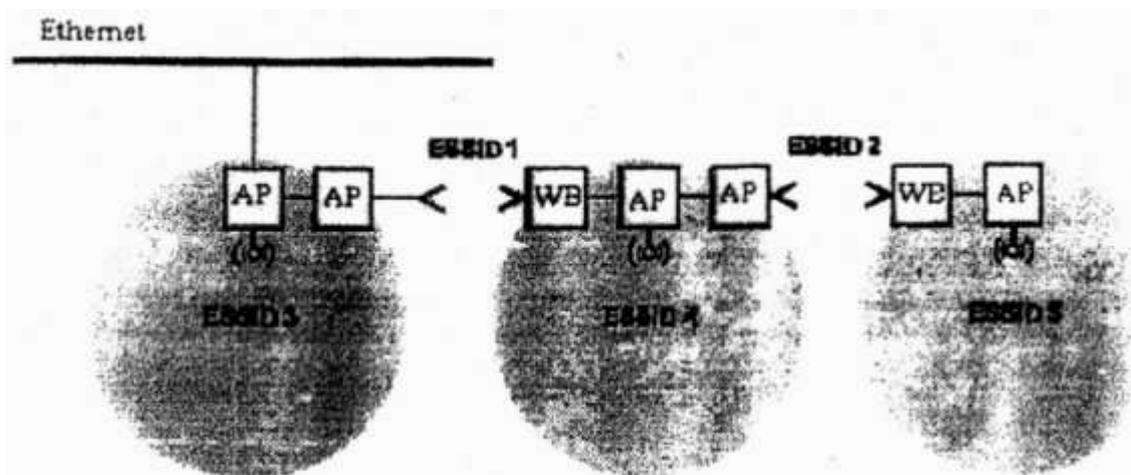
Kada treba povezati dva područja koja nisu na liniji vidljivosti, koristi se AP-WB (*bridge*) par koji se postavi na lokaciju s koje se mogu vidjeti izvorne lokacije (slika 16.).



Slika 16. Višekoračna konfiguracija

Tada ova treća lokacija služi kao prosljeđivačka točka.

Na prostoru gdje žičana LAN mreža nije dostupna, može se dodati još jedna pristupna točka AP-WB releju koja distribuira promet bežične temeljne mreže. Na ovaj način može se proširiti granica sustava (Slika 17.),



Slika 17. Proširena višekoračna konfiguracija

Ova konfiguracija se koristi kada se žele povezati različite zgrade na istu mrežu.

17.8. Karakteristike bežične LAN mreže

17.8.1. Domet i pokrivanje

Udaljenost na kojoj se može ostvariti komunikacija uporabom radio frekvencijskih (RF) i infracrvenih (IR) valova je funkcija izvedbe samih uređaja što uključuje predajnu snagu i izvedbu prijarnika. Međudjelovanje je s objektima zatvorenog prostora kao što su zidovi, metal pa čak i ljudi utječu na prostiranje energije, a time i domet i pokrivanje pojedinog sustava. Čvrsti objekti blokiraju infracrvene signale, što nameće dodatna ograničenja. Većina bežičnih LAN mreža koristi RF tehnologiju, jer radio valovi prolaze kroz unutrašnje zidove i prepreke. Domet varira od 100 do 1000 m, a pokrivanje se može ostvariti roamingom.

17.8.2. Propusnost

Čimbenici koji utječu na propusnost sustava su: broj korisnika, domet i višestazno prostiranje signala, topologija i tehnologija izvedbe, te i uska grla pri prelasku na žičanu LAN mrežu. Bežična LAN mreža osigurava propusnost dostatnu za većinu uredskih aplikacija, što uključuje elektroničku poštu, pristup perifernoj opremi, Internetu, višekorisničkim bazama podataka i aplikacijama.

17.8.3. Cjelovitost i pouzdanost

Bežična tehnologija je opravdala svoje postojanje kroz više od 50 godina i u komercijalne i u vojne svrhe. Robusna izvedba dokazanih bežičnih LAN tehnologija i ograničena udaljenost na kojoj putuje signal osiguravaju pouzdanu vezu i cjelovitost podataka.

17.8.4. Kompatibilnost s postojećim mrežama

Većina bežičnih LAN mreža omogućuje povezivanje sa žičanim mrežama tipa *Ethernet* ili *Token Ring*. Mrežni operacijski sustav podržava čvorove WLAN mreža preko upravljačkog programa (*driver*), dakle kao i svaki drugi LAN čvor.

17.8.5. Sposobnost zajedničkog rada bežičnih uređaja

Korisnici trebaju biti svjesni činjenice da bežični LAN sustavi različitih proizvođača ne moraju biti sposobni za zajednički rad, jer sustavi različitih tehnologija prijenosa i različitog frekvencijsko~područja ne mogu zajednički djelovati. Sustavi se mogu temeljiti na istoj tehnologiji i čak djelovati u

istom frekvencijskom pojasu, ali ne mogu ostvariti zajednički rad, ako postoje razlike u izvedbi opreme.

17.8.6. Dozvola za rad

Bežične LAN mreže su projektirane i izvedene tako da ne zahtijevaju posebnu dozvolu za rad, jer koriste frekvencije iz industrijsko-znanstveno-medicinskog pojasa, ISM (*Industrial-Scientific-Medical Band*) tj. od 902 - 928 MHz, 2.4 - 2.483 GHz, 5,15 - 5.35 GHz i 5.725 - 5.875 GHz. Sustavi koji koriste uskopojasni radio prijenos moraju zatražiti posebnu dozvolu za uporabu radio frekvencije.

17.8.7. Jednostavnost instalacije

Instaliranje bežične LAN mreže može biti brzo i jednostavno, jer eliminira potrebu za provlačenje kabela kroz stropove i zidove, a prenosivost sustava omogućuje prekonfiguraciju i ispitivanje mreže prije instaliranja na pravoj lokaciji.

17.8.8. Troškovi instaliranja i održavanja

Implementiranje WLAN mreža uključuje troškove infrastrukture bežičnih pristupnih točaka, (AP) i WLAN adaptera za mobilne korisnike. Troškovi infrastrukture ovise o broju pristupnih točaka, zahtijevanom području pokrivanja kao i o broju i vrsti korisnika. ali se ipak može reći da su manji od troškova kabliranja i održavanja tradicionalnih žičanih LAN mreža.

17.8.9. Sigurnost

Bežična tehnologija ima svoje korijene u vojnim primjenama, pa je sigurnost prometa u takvoj mreži jedan od kriterija koji se mora zadovoljiti. To se postiže složenim tehnologijama prijenosa, zaštitnim kodiranjem, algoritmima i drugo.

18. SPECTRUM 24 WLAN MREŽA

Spectrum 24 je ćelijska mreža s raspršenim spektrom koja djeluje u frekvencijskom području između 2.4 i 2.5 GHz. Ova tehnologija omogućuje izgradnju mreže velikog kapaciteta uporabom višestrukih pristupnih točaka. *Spectrum 24* WLAN mreža sastoji se od hardverskih i softverskih komponenata koje se bežično integriraju sa žičanim okruženjem. *Spectrum 24* uključuje pristupne točke, softver, LAN adapter i menadžment alate. PCMCIA kartica se instalira u terminale, *laptop* računala i druge uređaje za brzu, jednostavnu i bežičnu vezu sa *Spectrum 24* WLAN mrežom.

Spectrum 24 2 Mb/s sustave nudi kompanija *Symbol*. Oni podržavaju prijenos podataka i govora preko IP aplikacija i *Spectrum 24 High Rate*, tj. 11 Mb/s sustave za održavanje aplikacija koje sadržavaju velike datoteke kao što su multimedijske prezentacije i prijenosi baza podataka. .

Osnovna obilježja *Spectrum 24* proizvoda su:

- mosna arhitektura (omogućuje komunikaciju između žičanih i radio dijelova mreže).
- dizajn temeljen na IEEE 802.11 i 802.11b standardu,
- bežični roaming za mobilne korisnike,
- promjenjiva brzina prijenosa podataka (omogućuje 1 Mb/s, 2 Mb/s i 11 Mb/s) uređajima komunikaciju u istom mrežnom okruženju.
- automatsko prepoznavanje *Spectrum 24* Mb/s (FH) i 11 Mb/s (DS) radio kartica,
- 10 Base-T Ethernet s RJ45 mrežnim sučeljem.

Spectrum 24 uređaji koriste elektromagnetske valove za bežični prijenos električnih signala. Korisnici komuniciraju s mrežom uspostavljajući radio vezu između terminala i pristupnih točaka. Za prijenos digitalnih podataka od jednog uređaja do drugog koristi se frekvencijska modulacija, FM (*Frequency Modulation*), pri čemu se podatkovni signal utiskuje u prijenosni signal. Modulirani signal se

propagira kroz slobodan prostor putem elektromagnetskih valova. Prijemna antena ih prima, a prijamni uređaj demodulira te se na njegovu izlazu dobiva prvobitni (originalni) podatkovni signal.

Spectrum 24 uređaji upotrebljavaju jedinstveni hardverski kodirani pristup mediju (MAC) ili IEEE adrese. MAC adrese određuju uređaje koji šalju i primaju podatke. MAC adresa je 48-bitni broj napisan kao šest heksadekadskih bitova odvojenih dvotočkama.

18.1. Pristupna točka (AP)

Povezanost između žičane LAN mreže i radiom opremljenih mobilnih jedinica (*Symbol Spectrum 24* terminali, PC kartice, PCI adapteri, skeneri) ostvaruje se s pristupnim točkama. Pristupna točka nadzire Ethernet promet i prosljeđuje odgovarajuću Ethernet poruku mobilnoj jedinici preko Spectrum 24 mreže. Također nadgledava radio promet mobilne jedinice i prosljeđuje njezine pakete do Ethernet mreže.

Pristupna točka sadrži i podržava:

- dijagnostičku opremu za otkrivanje pogrešaka,
- bežično MAC sučelje,
- 10 Base-T Ethernet pristupno sučelje,
- višestruki prijenos ugrađenih antena,
- 127 mobilnih jedinica, MU (*Mobile Unit*),
- jednostavan mrežni upravljački protokol, SNMP (*Simple Network Management Protocol*),
- mobilni IP protokol,
- šifriranje podataka,
- protokol za dinamičko konfiguriranje računala, HCP (*Dynamic Host Configuration Protocol*),
- hipertekstualni prijenosni protokol, HTTP (*Hyper Text Transport Protocol*),
- obnavljač funkcija.

Mobilna jedinica komunicira putem pristupne točke ravnopravno s drugim mrežnim uređajima. Pristupna točka prima podatke od svog žičanog sučelja i prosljeđuje ih prikladnom sučelju. AP je povezana sa žičanom mrežom i s izvorom napajanja. Pričvršćuje se na zidove ili strop ovisno o zahtjevima i mjestu instaliranja. AP zahtijeva jednu antenu za odašiljanje i primanje. Međutim, sustav dvostruke antene omogućuje AP točki odabiranje boljeg radio signala.

18.2. Mrežne topologije Spectrum 24 WLAN mreže

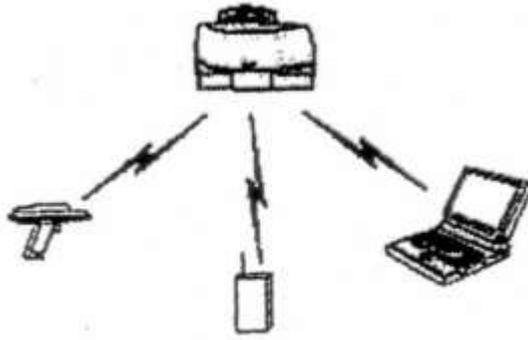
U bežičnim mrežama Spectrum 24 mogu se ostvariti različite topologije mreže.

To ovisi o slijedećim čimbenicima:

- funkciji AP u mreži,
- brzini prijenosa podataka,
- bežičnom AP (WLAP) sučelju,

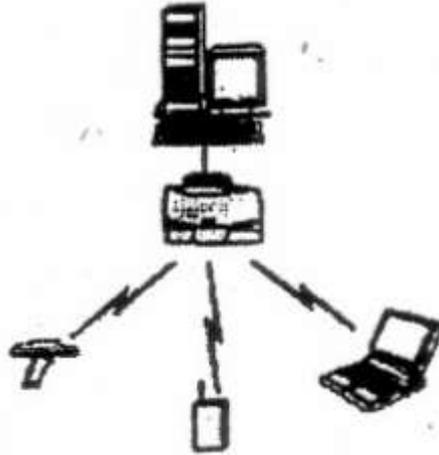
Moguće su sljedeće topologije WLAN mreže:

- jednoćelijska bežična mreža s ravnopravnim mobilnim jedinicama, koja sadrži jednu AP unutar žičane mreže (slika 18),



Slika 18. Jednoćelijska bežična mreža s ravnopravnim mobilnim jedinicama

- jednoćelijska mreža s jednom AP koja može povezivati Ethernet i radio mrežu (slika 19).



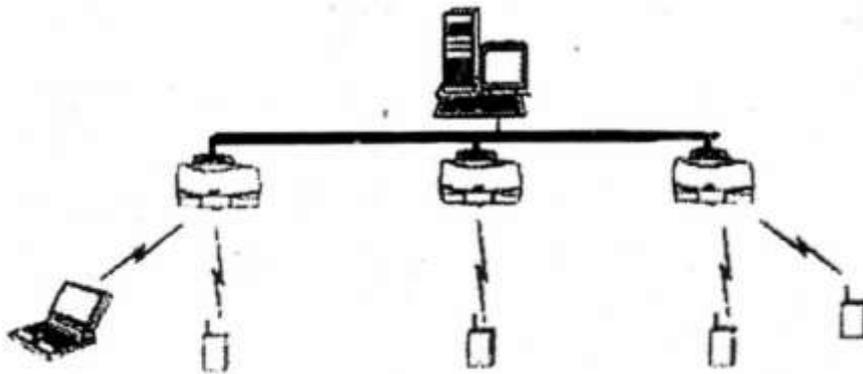
Slika 19. Jednoćelijska bežična mreža

- višćelijska mreža s više AP koje mogu koegzistirati kao odvojene, individualne mreže na istom mjestu bez interferencije upotrebljavajući različite identifikatore proširene uslužne skupine, ESS_ID (slika 20),



Slika 20. Višćelijska mreža s različitim identifikatorom ESS_ID

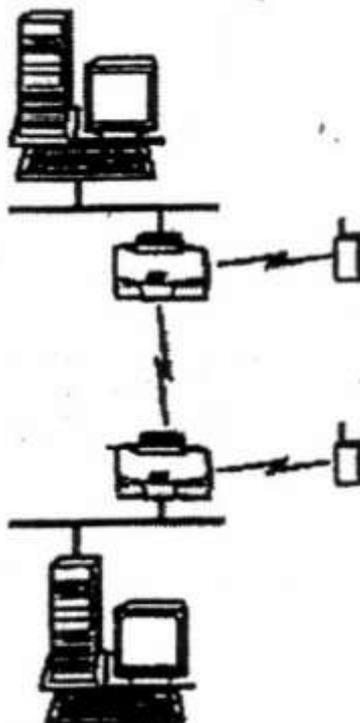
- višćelijska mreža s više međusobno povezanih AP koje osiguravaju bolju pokrivenost mrežom i bolje performanse kada se koriste isti ESS_ID (slika 21),



Slika 21. Višćelijska mreža s istim identifikatorom ESS_ID

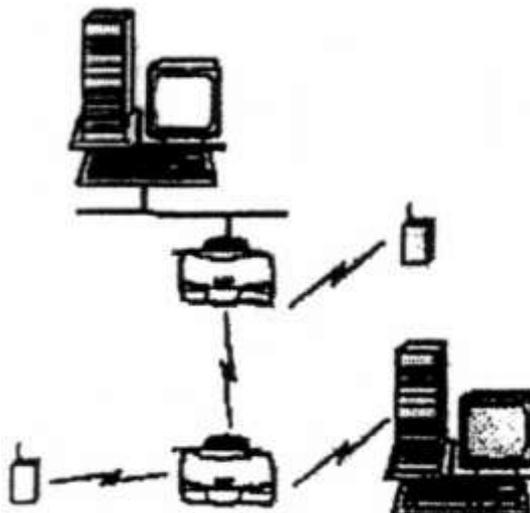
U bežičnom AP sučelju bežična AP-AP veza služi:

- kao most za povezivanje dviju Ethernet mreža (slika 22);



Slika 22. Povezivanje dviju Ethernet mreža s AP-AP vezom

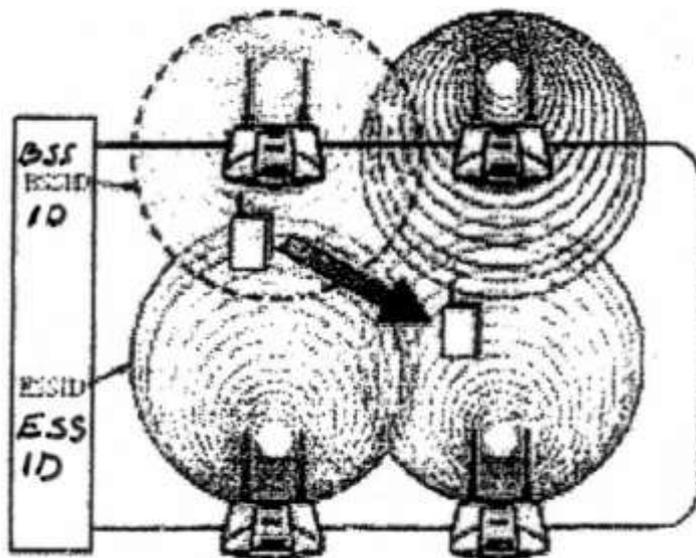
- kao repetitor za proširenje pokrivenosti prostora bez dodatnih kabela (slika 23),



18.3. Čelijsko pokrivanje

Pristupna točka AP s mobilnim jedinicama MU čini tzv. uslužnu skupinu (BSS) ili ćeliju. Ukoliko se mobilna jedinica nalazi na području određene ćelije ona se pridružuje i komunicira s pristupnom točkom te ćelije. Svaka ćelija ima identifikator osnovne uslužne skupine, BSS_ID (*Basic Service Set Identifier*). U 802.11 standardu AP MAC adresa predstavlja BSS_ID. Dodavanjem pristupnih točaka LAN mreži uspostavlja se više ćelija u okuženju i dobiva se RF mreža uporabom istog identifikatora proširene uslužne skupine, ESS_ID (*Extended Service Set Identifier*).

Pristupne točke s istim identifikatorom ESS_ID određuju područje pokrivanja. Mobilna jedinica traži pristupne točke s odgovarajućim identifikatorom ESS_ID, te se sinkronizira s postupnom točkom zbog uspostave komunikacije. To omogućuje mobilnoj jedinici kretanje unutar područja pokrivenosti.



Slika 24. Identifikatori BSS_ID i ESS_ID

Kako se mobilna jedinica kreće od ćelije do ćelije, prekapča se s jedne na drugu pristupnu točku. Do prekapčanja dolazi nakon što mobilna jedinica analizira kakvoću prijema na dotičnoj lokaciji. Na osnovi najveće snage signala i najniže distribucije opterećenja određuje se neka druga pristupna točka s kojom će mobilna jedinica komunicirati. Ukoliko mobilna jedinica ne nađe pristupnu točku s prihvatljivom snagom signala, tada traži bilo koju pristupnu točku.

18.4. Smjernice za instaliranje WLAN mreže

Prilikom izgradnje bežične mreže treba voditi računa o:

- odabiru mjesta pristupnih točaka,
- višestrukome prijenosu,
- konstrukcijskim materijalima zgrade,
- veličini ćelije.

18.5. Odabir mjesta pristupne točke

WLAN produkti su robusni, bez kvarova (*Trouble-Free Units*), napravljeni da efikasno rade pod različitim uvjetima. Slijedeće smjernice osiguravaju optimalnu pokrivenost i rad bežične LAN mreže.

Metalni objekti

Mjesto pristupne točke mora biti očišćeno od metalnih objekata i udaljeno od pokretnih objekata kao što su metalni ventilator ili vrata.

Mikrovalna peć

Za ostvarivanje najbolje performanse mreže mjesto pristupne točke ne smije biti kraj izvora zračenja koji emitira na 2.4 GHz frekvencijama kao što je mikrovalna peć.

Izvori grijanja

Pristupna točka treba biti smještena dalje od izvora grijanja kao što su radijatori i klima uređaji. Prilikom odabira lokacije pristupne točke treba voditi računa o visini pristupne točke, prikladnosti lokacije i željenom području pokrivanja.

Visina

Pristupna točka trebala bi biti najmanje 1.5 metar od poda, podalje od visokog uredskog namještaja unutar područja pokrivanja. Pristupna točka može se postaviti na visoku policu, ili se može zakačiti na strop ili zid.

Lokacija

Pristupnu točku treba instalirati na sredini prostora željenog područja pokrivanja. Dobre lokacije su:

- u središtu velike prostorije,
- u središtu hodnika,
- na sjecištu dvaju hodnika.

Većina zgrada ima metalnu konstrukciju ili metalne komponente, pa se preporuča instalacija pristupnih točaka na stropovima hodnika, jer se radio valovi proizvoda temeljenih na WLAN 802.11 standardu reflektiraju duž metalnih dijelova i prolaze u urede kroz vrata i staklene dijelove.

18.6. Antene pristupne točke

Postoje ograničenja glede mjesta instalacije WLAN mreže, što je izravno povezano s pokrivenošću područja signalom. Polumjer pokrivenosti AP s neusmjerenim (*omni-directional*) antenama iznosi oko 300 metara na otvorenom prostoru. U uredima ima mnogo prepreka koje smanjuju radijus pokrivenosti na 50 -70 metara (ovisno o građevnom materijalu i uredskom namještaju). Neusmjerena antena odašilje i prima radio valove u svim smjerovima. Pokrivenost prostora je kružna s antenom u sredini.

Usmjerene antene odašilju i primaju radio valove u smjeru antene. Snaga iza i sa strana antene je smanjena. Pokrivenost prostora je ovalna s antenama na oba kraja. Ove antene se koriste na mjestima gdje se zahtijeva osiguranje veće udaljenosti preko relativno uskog prostora.

18.7. Višestruki prijenos

Jedna antena za osiguravanje dobre performanse dovoljna je kod aplikacija gdje se ne očekuje *višestazna propagacija*. Međutim, u slučajevima kada se očekuje *višestazna propagacija* preporuča se upotreba dviju antena. Primarna antena koristi se i za odašiljanje i za prijem, a sekundarna samo za prijem radio signala. Vodeća ideja višestrukog prijema je minimizirati interferenciju ili iščezavanje signala uporabom prijamnog signala što veće snage.

18.8. Konstrukcijski materijali zgrade

Konstrukcijski materijali zidova, pregrada, stropova, podova i namještaj u uredima utječu na ćelijsku pokrivenost prostora (tablica 2).

Tablica 2. Moguće zapreke signala, njihove dimenzije i gubici koje prouzrokuju.

Zapreka	Dodatni gubici	Efektivna širina	Aproksimativna širina
otvoren prostor	0 dB	100 %	300 m
prozor bez metalne boje	3 dB	70 %	215 m
prozor s metalnom bojom	5 - 8 dB	50 %	150 m
lagani zid (suhozid)	5 - 8 dB	50 %	150 m

srednji zid (drvo)	10 dB	30 %	100 m
teški zid (kruta jezgra 6)	15 – 20 dB	15 %	50 m
vrlo teški zid (kruta jezgra 12)	20 – 25 dB	10 %	30 m
pod/strop (kruta jezgra)	15 – 20 dB	15 %	50 m
pod/strop (vrlo kruta jezgra)	20 – 25 dB	10 %	30 m

Ovi materijali mogu uzrokovati gubitak radio signala zbog njihove unutarnje strukture:

- radio signal ne može proći kroz metalne objekte, već se reflektira od njih,
- kroz drvo, staklo i plastiku prolazi dio signala, a jedan dio se reflektira,
- voda i objekti s velikom vlažnošću apsorbiraju veliki dio radio signala.

18.9. Veličina ćelije bežične LAN mreže

Maksimalna udaljenost između pristupne točke i staničnog adaptera određuje veličinu ćelije. Udaljenost varira ovisno o konstrukciji zgrade i prirodi okruženja. Postoji nekoliko tipičnih kategorija unutrašnjeg prostora: otvoreni, poluotvoreni i zatvoreni prostor.

Otvoreni unutrašnji prostor

Otvoreni unutrašnji prostor je otvoreni uredski prostor bez pregrada i zapreka između pristupne točke i radne stanice. Predložena maksimalna udaljenost između AP i radne stanice je 200 metara.

Poluotvoreni unutrašnji prostor

Poluotvoreni unutrašnji prostor je otvoreni prostor djelomično podijeljen na individualna radna mjesta, primjerice u tvornicama, skladištima, robnim kućama. Predložena maksimalna udaljenost između AP i radne stanice je 100 metara.

Zatvoreni unutrašnji prostor

Zatvoreni unutrašnji prostor podrazumijeva katove podijeljene na pojedine urede odijeljene zidovima od betona i željeza, primjerice u bolnicama, tvrtkama, školama, veleučilištima, fakultetima, privatnim kućama. Predložena maksimalna udaljenost između AP i radne stanice je 50 metara.

19. PROBLEMATIKA PROJEKTIRANJA VELIKE LOKALNE BEŽIČNE MREŽE

Bežičnu lokalnu mrežu treba tako projektirati da cijelo ciljno područje bude pokriveno radijskim signalom odnosno da ne postoje rupe u pokrivenosti signala te da njezin kapacitet bude odgovarajući za očekivano prometno opterećenje. Ovim se uvjetima može udovoljiti upotrebom odgovarajuće kombinacije lokacija pristupnih točaka, pridružene frekvencije te određivanja praga prijemnika.

19.1. Bežične lokalne mreže

Namjena je bežičnih lokalnih mreža da omoguće bežično komuniciranje u svako doba i na svakom mjestu. Tijekom 1990-ih godina, razvojem opreme koja je tada bila raspoloživa u PCMCIA obliku, bežične lokalne mreže omogućuje mobilnost korisnika koja je jednaka kroz zgradu ili kroz kompleks zemljišta i zgrada.

One djeluju u industrijskim, znanstvenim i medicinskim (ISM) pojasevima na 915 MHz, 2.4 GHz te 5 GHz. Originalni WLAN standard IEEE 802.11 (s brzinama do 2 Mb/s) omogućuje uporabu tehnologije raspršenog spektra s poskakivanjem frekvencije ili s izravnim nizovima u 2.4 GHz pojasu. Također omogućuje rad na infracrvenim frekvencijama. WLAN standardi IEEE 802.11b omogućavaju rad s brzinama do 11 Mb/s u 2.4 GHz pojasu, a koristi izmijenjenu verziju IEEE 802.11 tehnologije raspršenog spektra s izravnim nizovima. Suvremeni IEEE 802.11 standard s visokim brzinama prijenosa koristi ortogonalni sustav višestrukog prijenosa s frekvencijskom raspodjelom (OFDM) da bi omogućio rad u 5 GHz pojasu na brzinama do 54 Mb/s.

IEEE 802.11b oprema već je raspoloživa na tržištu, dok je IEEE 802.11a oprema dostupna od 2002 godine.

WLAN mreža obuhvaća mrežne adaptere (NA) i mrežne pristupne točke (AP). Mrežni adapter dostupan je kao PC kartica koja se instalira u pokretno računalo, a omogućuje mu pristup AP točki.

Mrežni adapter obuhvaća predajnik, prijammnik, antenu i hardver koji osiguravaju podatkovno sučelje pokretnom računalu.

AP je podatkovni most/bazna radio postaja koja je montirana na fiksnoj poziciji i povezana s žičanom LAN mrežom. AP, koja obuhvaća predajnik, prijammnik, antenu i most, omogućuje pokretnim računalima opremljenim NA opremom komuniciranje s žičanom lokalnom mrežom. Most koji je dio AP točke usmjerava pakete od ili prema žičanoj mreži. Svaka AP ima radijski opseg od približno 20 do više od 300 m, ovisno o danom proizvodu, antenama i okolišu u kojemu djeluje. Pristupne točke prema tome, mogu se povezati s IEEE 802.3 (Ethernet) žičanim lokalnim mrežama.

Većina žičanih lokalnih mreža omogućuje roaming tj. uporabu mobilnih postaja izvan područja na kojemu je korisnik prijavljen. Da bi prekapčanje mobilne postaje s jedne osnovne postaje na drugu bilo uspješno, potrebno je ažurirati tabele u mostovima (koje sadrži svaka pristupna točka) pri kretanju. mobitela iz jednog područja u drugo. U bežičnim lokalnim mrežama izravna se komunikacija ravnopravnih mobitela može osigurati na jedan od dva načina. U nekim bežičnim lokalnim mrežama mobitel može komunicirati izravno s drugim mobitelom. U drugim mrežama, dva mobitela mogu komunicirati samo ako se njihovi odaslati podaci prenose kroz posrednu pristupnu točku (AP), čak jako iako su mobiteli u dosegu.

Uporabom tehnologije raspršenog spektra s izravnim slijedom (DSSS) u IEEE 802.11 i 802.11b mrežama raspršuje se signal preko široko frekvencijsko pojasa što omogućava otpornost odaslatih signala na različite smetnje i neželjene utjecaje višestazne propagacije signala. IEEE 802.11b WLAN mreža radi pri brzini prijenosa od 11 Mb/s, a zauzima širinu frekvencijskog pojasa od približno 26 MHz Precizna dodjela spektra za 2.4 GHz ISM se razlikuje za jednu zemlju od druge. U Sjevernoj Americi taj pojas iznosi od 2.400 do 2.4835 GHz.

IEEE 802.11 i 802.11b mreže upotrebljavaju višestruki pristup detekcijom nosioca (CSMA) uz shemu pristupa mediju s izbjegavanjem sudara (CA) koja je slična CSMA/CD shemi upotrijebljenoj u IEEE 802.3 (*Ethernet*) lokalnim mrežama. Tehnika otkrivanja sudara (CD) upotrijebljena u žičanoj lokalnoj mreži ne može se primijeniti u bežičnoj mreži, jer je jakost signala koji se odašilje u vlastitoj anteni puno veća od jakosti signala koji se prima od bilo kojeg drugog odašiljača. Stoga, CSMA/CA shema dodaje brojna svojstva osnovnoj CSMA shemi kako bi se smanjio broj sudara koji se mogu dogoditi, ako se upotrijebi samo CSMA shema bez mogućnosti otkrivanja sudara.

19.2. Projektiranje velike bežične mreže

Izazovi u izgradnji velike bežične mreže su značajni. Oni uključuju projektiranje mreže koja će pokrivati cijeli kompleks zgrada i zemljišta te osigurati odgovarajući kapacitet mreže koji će podržavati prometno opterećenje koje nastaje pri komunikaciji na tom kompleksu. WLAN projekt sadrži dvije komponente: odabir AP lokacija i dodjeljivanje radio frekvencija AP točkama.

Pri izgradnji bežične lokalne mreže s višestrukim pristupnim točkama (AP), mora se voditi računa o osiguranju odgovarajuće radio pokrivenosti pažljivim lociranjem AP točaka. Iskustvo pokazuje da se lociranje tih točaka mora temeljiti na mjerenjima, a ne samo na proračunima. Ova mjerenja obuhvaćaju opsežna ispitivanja i pažljiva razmatranja problema propagacije radio valova kada je uslužno područje veliko, kao primjerice studentski kamp.

Raspored i konstrukcija zgrada određuju područje pokrivenosti svake pristupne točke. Tipično odašiljanje seže do 300 m u otvorenom okolišu, ali kroz zidove i druge prepreke u uredima taj se doseg smanjuje do 20-60 m. Drvo, žbuka i staklo nisu ozbiljna prepreka radio prijenosu bežične

lokalne mreže, ali opeka i betonski zidovi mogu biti značajna prepreka. Najveća prepreka radio prijenosu u uredskom okruženju je metal, kao onaj u stolovima, kabinetima i dizalima.

Radna svojstva mreže su također problem. AP i pokretna računala unutar svog područja pokrivenosti rade slično kao računala na segmentu Ethernet, odnosno postoji samo određena širina raspoloživog frekvencijskog pojasa, a mora se dijeliti za AP i za pokretna računala. IEEE 802.11b protokol s uporabom CSMA/CA sheme osigurava mehanizam koji omogućuje svim jedinicama da dijele iste resurse pojasne širine.

19.3. Pristup projektiranju bežične mreže

Pri odabiru AP lokacija mora se spriječiti pojava rupa u pokrivenosti, tj. pojava područja u kojima usluga bežične mreže nije omogućena korisnicima. S druge strane, pristupne točke treba postaviti što dalje jednu od druge kako bi se smanjila cijena opreme i instalacije. Osim toga, preklapanje pokrivenosti dviju pristupnih točaka koje rade na istom radio kanalu uzrokuje smanjivanje radnih svojstava. Ovo je razlog zašto ne bismo smjeli u bežičnu lokalnu mrežu postaviti više AP točaka nego je to potrebno. Smanjivanjem preklapanja između područja pokrivenosti AP točaka, smanjuje se i istokanalno preklapanje.

Svaki projekt zgrade mora se temeljiti na pažljivim mjerenjima jačine signala. To je izazovno, jer je zgrada trodimenzionalan prostor, a AP smještena na jednom katu zgrade osigurava pokrivenost signalom i na susjednim katovima iste zgrade, a možda i u drugim zgradama. Nakon što su definirane lokacije AP točaka i izmjerena njihova područja pokrivenosti dodjeljujemo im radio kanale. Jedanaest radio kanala su dostupni u 2,400 - 2,4835 GHz pojasu koji se upotrebljava u Sjevernoj Americi. Stoga pristupne točke mogu djelovati na tri zasebna nesmetana kanala. Upotreba višestrukih kanala može također pomoći u smanjivanju istokanalnog preklapanja, čime se smanjuje mogućnost utjecaja na radio svojstva. Nakon toga dodjeljuje se jedan od 3 kanala svakoj pristupnoj točki AP uz uvjet minimalnog istokanalnog preklapanja. Pridruživanje ovih frekvencija ostvaruje se različitim postupcima koji osiguravaju optimalnu ili približno-optimalnu dodjelu tih radio kanala.

Pri projektiranju također se mora razmotriti usluga za područja s velikom i malom gustoćom korisnika. Ako je mnogo korisnika koncentrirano na malom području (području s velikom gustoćom), bit će potrebno koristiti specijalne tehnike pri izradi projekta za takva područja. Međutim, za očekivati je da će većina područja biti s malom gustoćom. Ipak će postojati neka područja, primjerice razredne učionice, predavaonice na fakultetima, koja će imati veliku gustoću korisnika.

U slučaju područja s velikom gustoćom korisnika, koriste se dvije tehnike i to: povećavanje praga prijelnika i uporaba višestrukih radio kanala. Upotreba višestrukih radio kanala omogućuje upotrebu višestrukih AP točaka kako bi se osigurala pokrivenost u istom fizičkom prostoru. Primjerice, mogu se upotrijebiti tri AP točke koja rade na tri različita kanala kako bi se pokrila velika predavaonica s velikom koncentracijom korisnika.

19.4. Postupak izvedbe bežične mreže

Kako je propagacija radio valova unutar jedne zgrade često nepravilna i rijetko potpuno predvidljiva projektiranje mreže za unutrašnjost zgrade uključuje 5 koraka:

- početni odabir AP lokacija,
- ispitivanje i ponovnu izradbu projekta mreže, što znači prilagodbu lokacija pristupnih točaka temeljenu na mjerenjima jakosti signala.
- izradbu mape pokrivenosti područja signalom,
- dodjelu frekvencija pristupnim točkama,
- službeno ispitivanje, odnosno pregledavanje AP lokacija i završna mjerenja jakosti signala na odabranim frekvencijama.

U sljedećem odjeljku opisat ćemo tehniku kojom se realizira prvi korak projekta, tj. početni odabir lokacija pristupnih točaka (AP). Prvi projekt je pokusni i treba se izmijeniti u drugom koraku.

Nakon početnog odabira lokacija AP točaka, one se privremeno instaliraju na odabranim lokacijama. Područja pokrivenosti tih AP točaka i preklapanja između njihovih područja također se moraju izmjeriti. Obično se pronađu rupe u pokrivenosti i/ili preklapanja. Na osnovi rezultata mjerenja AP lokacije se prilagođavaju, a ako je potrebno rade se ponovna mjerenja, pa pretrage i tako dalje sve dok se ne definiše prihvatljivi projekt mreže.

Nakon što se odaberu konačne AP lokacije izrađuje se mapa pokrivenosti. Ona se može napraviti automatskim projektiranjem pomoću računala (Auto-CAD dizajn) ili primjenom drugih računalnih tehnika. Zatim se dodjeljuju frekvencije pristupnim točkama na način da se što više smanjuju istokanalna preklapanja. Slijede cjelokupno pregledavanje i završna mjerenja za cijelu zgradu, a rezultati ovih mjerenja se unose u dokumente.

19.5. Određivanje početnih lokacija pristupnih točaka

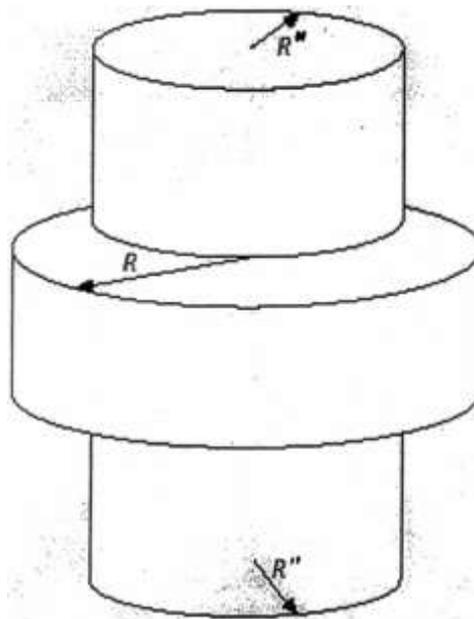
Opisat ćemo postupak početnog odabira AP lokacija u području niske gustoće korisnika. Pri odabiru lokacija za pristupne točke treba voditi računa da ne postoje rupe u pokrivenosti signalom, te da se što više smanje preklapanja između i kroz AP. Ako se upotrijebi previše pristupnih točaka, cijena opreme i instalacije će biti viša no što je potrebno, a radna svojstva mreže mogu se pogoršati. Količina preklapanja pokrivenosti u istokanalnom području određuje se pomoću lokacije AP i dodjele frekvencije AP točki. Definiše se područje pokrivenosti signalom da bi smo odredili prijemnu snagu signala. Odabiranje razine praga signala omogućuje odgovarajući omjer signala i šuma (s/n).

Ako se primjerice, pri izradi nacрта za IEEE 802.11b WLAN izmjeri razina buke u određenom ambijentu od 95 dBm, a 10 dB S/N je potreban da bi se osigurala najbolja izvedba, možemo dopustiti dodatnih 5 dB tako, da razina buke bude viša od 95 dBm.

U ovom bi se slučaju mogao odabrati prag od 80 dBm. Kada postoje područja visoke gustoće korisnika, predlaže se napraviti prvo razdiobu AP točaka za takva područja, a zatim da područja s niskom gustoćom popune praznine između područja s visokom gustoćom korisnika.

19.6. Postavljanje pristupnih točaka

U ovom će se odjeljku dati objašnjenje idealizirane pokrivenosti pristupnih točaka. Ovaj se opis daje samo zbog uvida u moguće rasporede pristupnih točaka koji se mogu primijeniti u različitim zgradama.



Slika 26. Koaksijalni cilindri pokrivenosti signalom pristupne točke

Uzmimo da volumen pokrivenosti signalom pristupne točke ima oblik triju koaksijalnih cilindara, što je prikazano na slici 26. Središnji cilindar predstavlja pokrivenost na katu na kojem je locirana pristupna točka i ima radijus R .

Pristupna točka (AP) smještena je na osi tog cilindra. Gornji i donji cilindri predstavljaju pokrivenost na katovima iznad i ispod onoga na kojem je locirana AP točka i ima radijus R'' koji je manji od R . Visina svakog od tri cilindra je visina kata u zgradi. Ova se tri cilindra mogu smatrati jednim objektom koji se pokreće kako se kreće lokacija pristupne točke. Problem postavljanja pristupnih točaka unutar zgrade može se shvatiti kao problem postavljanja tih geometrijskih oblika unutar zgrade na način da se popune svi prostori, tj. pokrije područje signalom sa što manjim preklapanjem. Volumen i područja pokrivenosti nisu savršeni cilindri pa se određuje prosječan radijus područja pokrivenosti unutar zgrade i njega uzimamo kao radijus idealiziranog cilindričnog volumena pokrivenosti. To se može postići na način da se definira prihvatljiv prag jačine signala, primjerice 80 dBm, te da se odredi prosječna udaljenost od pristupne točke na kojoj jačina signala pada ispod tog praga.

19.7. Postupak odabira AP lokacija

Početan odabir AP lokacija počinje s nizom mjerenja jačine signala unutar zgrade. Ova se mjerenja trebaju obaviti na cijelom području zgrade, pri čemu treba obratiti pozornost na konstrukciju zgrade tako, odnosno uočiti značajke cijelog dijela zgrade.

Ta mjerenja imaju dva cilja: da se podijeli zgrada na dijelove koji su relativno više ili manje izolirani te jedan od drugoga s gledišta širenja signala te da se odredi prosječan radijus pokrivenosti područja jedne pristupne točke. Mjerenja jačine signala također se koriste kako bi se odredio radijus pokrivenosti signalom R na katu gdje je smještena AP točka kao i onaj na susjednom katu R'' od te iste pristupne točke.

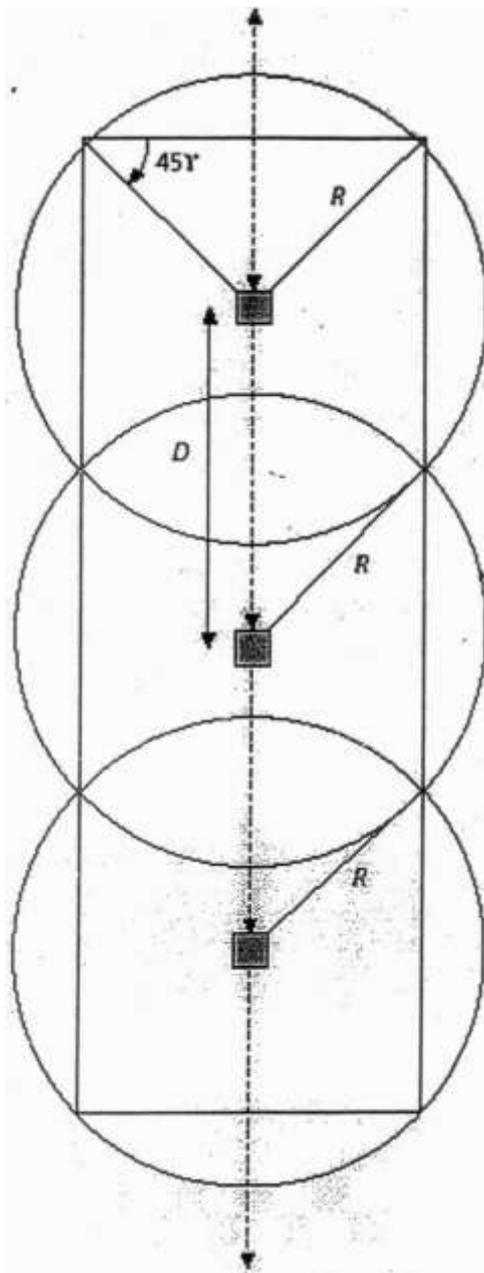
Pristupne točke se mogu smjestiti unutar zgrade u nizu koji je linearan ili kvadratnog oblika. Primjer linearnog niza prikazan je na slici 27, a primjer kvadratnog rasporeda pristupnih točaka na slici 28. Svaka od njih pokazuje kako se pristupne točke mogu smjestiti u zgradi sa samo jednim katom.

Potrebno je samo locirati AP na način koji će smanjiti što je više moguće preklapanja među područjima pokrivenosti AP. Linearan niz se upotrebljava kada je zgrada duža nego šira u odnosu na radijus R , a kvadratni kada je širina zgrade velika naspram R .

S druge strane, u zgradi koja ima više od jednog kata mora se razmotriti pokrivenost signalom i na susjednom katu od jedne pristupne točke, AP. Obično se postupa na slijedeći način: krećemo se po dužini (ili širini) zgrade, pri tome postavljamo pristupne točke prvo na jednom, a zatim na susjednom katu. U tom slučaju pokrivenost susjednog kata mora biti usklađena s pokrivenošću pristupne točke s tog kata. Opisat ćemo četiri primjera izrade projekta bežične mreže za unutrašnjost neke zgrade.

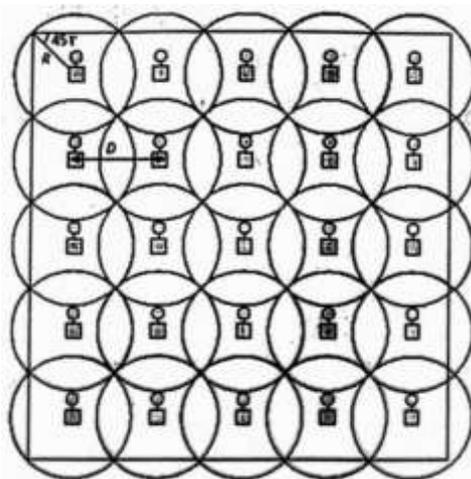
Primjeri se razlikuju po tome radi li se o jednokatnoj ili višekatomjarnoj zaradi, te prema usporedbi širine zgrade i radijusa R i R'' . U svakom se primjeru predloži odgovarajući pristup za postavljanje AP točke, te se ilustrira sa slikama. Pune crte pokazuju pokrivenost na jednom katu, a iscrtane linije pokazuju pokrivenost na susjednim katovima.

Prvi primjer: Linearni niz postavljanja AP točaka u jednokatnoj zgradi je prikazan na slici 27. Jednokatna zgrada (ili ona koja zahtijeva bežičnu pokrivenost signalom na samo jednom katu) čija širina (najmanja vanjska dimenzija) nije velika u odnosu na R . D predstavlja udaljenost između susjednih pristupnih točaka.



Slika 27. Linearni niz postavljanja AP točaka u jednokatnoj zgradi

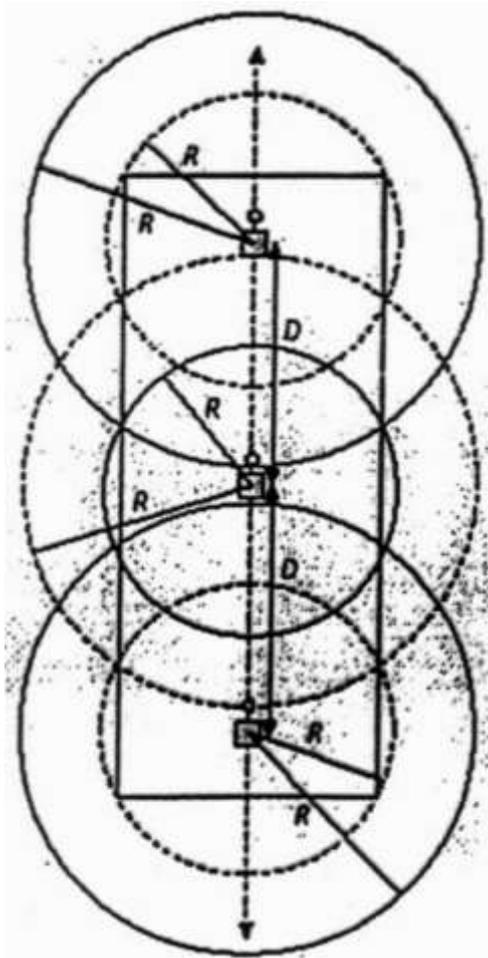
Drugi primjer: Kvadratni niz postavljanja AP točaka u jednokatnoj zgradi je prikazan na slici 28:



Slika 28. Kvadratni niz postavljanja AP točaka u jednokatnoj zgradi

Jednokratna zgrada (ili ona koja zahtijeva bežičnu pokrivenost na samo jednom katu) čija je širina (najmanja vanjska dimenzija) velika u odnosu na R . D označava udaljenost između susjednih pristupnih točaka.

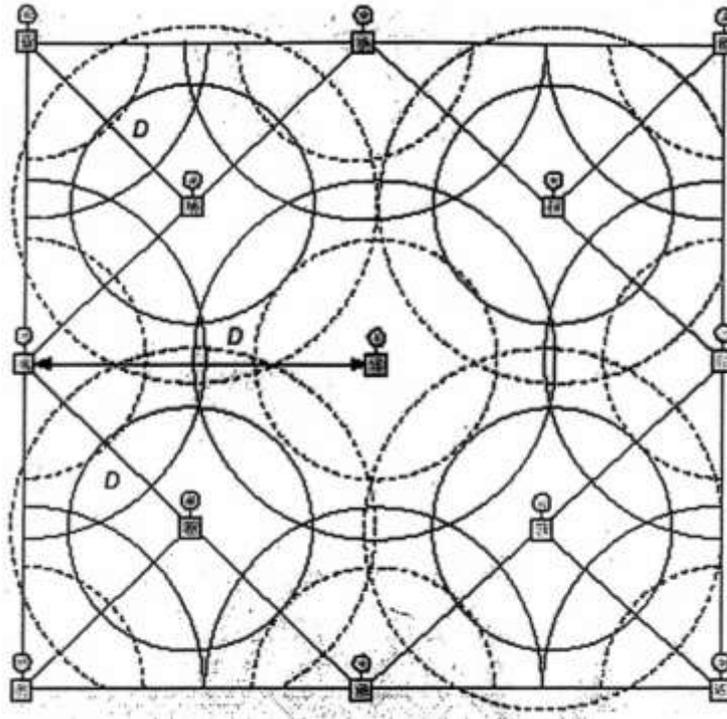
Treći primjer: Linearni niz postavljanja AP točaka u višekatnoj zgradi prikazan je na slici 29.



Slika 29. Linearni niz postavljanja AP točaka u višekatnoj zgradi

Prikazana je višekatna zgrada čija širina (najmanja vanjska dimenzija) nije velika u odnosu na R i R'' . D'' označava udaljenost između susjednih pristupnih točaka na različitim katovima.

Četvrti primjer: Kvadratni niz postavljanja AP točaka u višekatnoj zgradi je prikazan na slici 30.



Slika 30. Kvadratni niz postavljanja AP točaka u višekatnoj zgradi

Višekatna zgrada ima širinu (najmanja vanjska dimenzija) veliku u odnosu na R i R' : D označava udaljenost između susjednih pristupnih točaka na istom katu, a D'' na različitim katovima.

19.8. Pridruživanje frekvencija pristupnim točkama

Nakon što se završilo postavljanje pristupnih točaka i napravila mapa koja prikazuje pokrivenost područja signalom, slijedi pridruživanje frekvencija pristupnim točkama. U USA i Kanadi koriste se 3 kanala (kanali 1, 6 i 11) koji se ne preklapaju. Jedna od tih frekvencija može se pridružiti svakoj od pristupnih točaka na način da se minimizira istokanalno preklapanje. Dodjela frekvencija je u biti problem bojanja izrađene mape s 3 boje.

Kada je poznato područje pokrivenosti signalom, mogu se upotrijebiti različiti algoritmi za dodjelu frekvencija pristupnim točkama. Ako se koristi računalo, onda je najrazumnije provjeriti istokanalno preklapanje signala za sve moguće dodjele frekvencija. To oduzima dosta vremena, pa je poželjno koristiti računalo. Postoje algoritmi koji zahtijevaju manje utrošenog vremena, a mogu dati skoro optimalne rezultate.

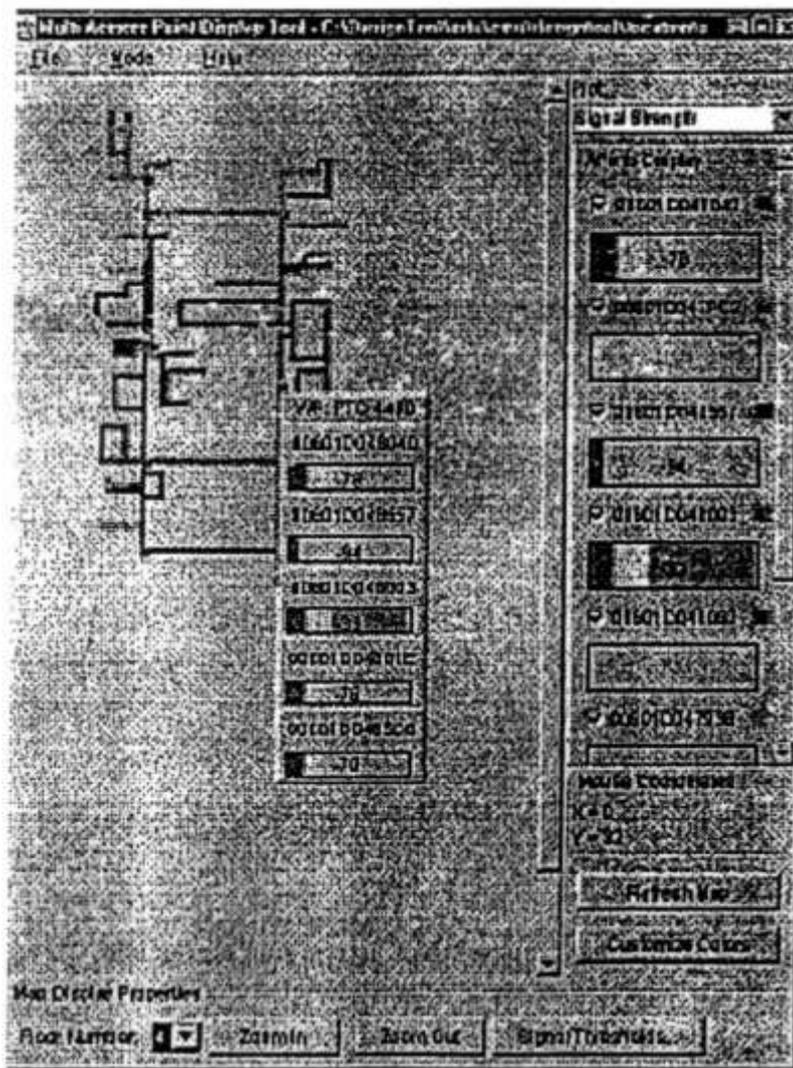
Međutim, pogodno je koristiti izrađenu mapu pokrivenosti zgrade signalom koja predočava preklapanja, pa se mogu pridruživati frekvencije tako da istokanalne pristupne točke imaju samo mala preklapanja.

Preporučuje se prvo dodijeliti frekvencije u područjima visoke koncentracije korisnika, a zatim u područjima manje koncentracije korisnika. Ako se primjerice, koriste tri pristupne točke da bi se pokrilo područje velike koncentracije korisnika, onda se tim pristupnim točkama dodjeljuju tri različita kanala.

Pristupne točke koje pokrivaju područja s velikom koncentracijom korisnika obično će imati mala preklapanja s pristupnim točkama koje pokrivaju područja s malom koncentracijom korisnika.

19.9. Programski alat za izradu nacрта

Da bi se olakšala izradba projekta, razvijen je programski alat koji pomaže pri lociranju pristupnih točaka, te pri dodjeli frekvencija. Program omogućuje da se odrede područja koja su pokrivena signalom, jednostavno obilaženjem, tj. hodaženjem oko ciljnog područja.



Slika 31. Prikaz programskog alata

Program generira mape pokrivenosti signalom svih pristupnih točaka Također izvršava optimalne dodjele frekvencija za određeno područje pokrivenosti te omogućuje korisniku virtualno premještanje pristupnih točaka i predviđanje područja pokrivenosti na toj novoj lokaciji Taj alat je od velike pomoći pri projektiranju bežične lokalne mreže. Tipičan prikaz na zaslonu uređaja koji pokazuje područja pokrivenosti nekoliko pristupnih točaka na jednom katu zgrade je dan na slici 31.

20. LOKALNE MREŽE I UMREŽAVANJE: OSNOVNI POJMOVI

20.1. Uvod

U tekstu su sažeto prikazani osnovni pojmovi klasičnih korporacijskih mreža: LAN, MAN, PBX, sustavi za povezivanje (most, usmjeritelj itd.) kao i neki uobičajeni primjeri njihovog umrežavanja. Također su navedeni važniji zahtjevi za integraciju raznih vrsta (multimedijskih) usluga, jer je to bitno obilježje korporacijskih mreža.

Značaj korporacijskih mreža u izuzetnom je porastu u posljednje vrijeme, a to je rezultat sve veće potreba za komunikacijom geografski raspršenih poslovnih sredina.

21. LOKALNE I METROPOLITANSKE MREŽE

U ovom poglavlju dajemo pregled najvažnijih LAN i MAN mreža. Pri tome je najveća pažnja posvećena tzv. konvencionalnim mrežama koje su standardizirane u okviru IEEE 802, odnosno ISO 8802, skupine standarda (slika 1).

Navedimo samo važnije IEEE odbore:

- 802.1: *High Level Interface (HLI)*
- 802.2: *Logical Link Control (LLC)*
- 802.3: *CSMA/CD Networks*
- 802.4: *Token Bus Networks*
- 802.5: *Token Ring Networks*
- 802.6 *Metropolitan Area Networks (MAN)*
- 802.7: *Broadband Technical Advisory Group (BBTAG)*
- 802.8: *Fiber Optic Technical Advisory Group (FOTAG)*
- 802.9: *Integrated Services LAN (ISLAN) Interface*
- 802.10: *Standard for Interoperable LAN Security (SILS)*
- 802.11: *Wireless LAN (WLAN)*,
- 802.12: *Demand Priority Access Method (DPAM)* – komercijalni naziv: 100VG AnyLan
- 802.14: *Cable-TV Based Broadband Communication Network*

21.1. Vrste lokalnih mreža

Lokalne mreže mogu se podijeliti obzirom na:

- vrstu prijenosa,
- topologiju, tj. konfiguraciju čvorova i grana,
- pristupni protokol,
- zajednički prijenosni medij i
- brzinu prijenosa po zajedničkom mediju.

Lokalna mreža (LAN) je komunikacijska mreža koja međusobno povezuje različite krajnje uređaje (PCI, *laptop*, radne stanice) na ograničenom prostoru (unutar jedne ili više susjednih zgrada) i omogućuje razmjenu informacija između tih uređaja velikim prijenosnim brzinama. (od 1 MB/s do ~GB/s). LAN je obično u vlasništvu jedne organizacije. Broj povezanih krajnjih uređaja u LAN je ograničen do par stotina krajnjih uređaja. Prvi LAN-ovi imali su 1990. zajednički prijenosni medij, a od sredine 90-tih uvode se LAN komutatori.

LLC	IEEE 802.2			Podslaj LLC implementiran softverski i jednak za sve LAN-ove	
MAC	IEEE 802.3 SCMA	IEEE 802.4 Token Bus	IEEE 802.5 Token Ring	FDDI	II. sloj (2 podsloja) specifičan MAC za svaku LAN
PHY	Sabirnica		Prsten		I. sloj

Slika 1. IEEE 802 skupina LAN/MAN standarda

Vrsta prijenosa

Osnovna gruba podjela lokalnih mreža proizlazi iz frekvencijskog pojasa unutar kojeg se obavlja prijenos signala Tako se temeljni frekvencijski pojas (*base-band*) definira kao onaj pojas kojim se obavlja prijenos izvorno bez uporabe modulacije. Digitalni signali se ubacuju na medij uporabom bilo *Manchester* ili diferencijalnog *Manchester* koda, a cijeli se frekvencijski spektar prijenosnog medija koristi za prijenos signala. Prijenos je dvosmjern, a obično se kao medij koristi kabel (50 Ω) ili danas oklopljena upredena parica i optički kabel. Neoklopljena upredena parica (UTP) susreće se u tri kategorije (standard EIA-568-A) za koje su definirane prijenosne karakteristike za brzine do 16 MHz (kategorija 3), do 20 MHz (kategorija 4) i do 100 MHz. (kategorija 5) Kategorije 3 i 5 su najčešće korištene: kategorija 3 (obična telefonska parica je instalirana u većini zgrada, dok se nove

(pre)instalacije uglavnom rade s kategorijom 5. Oklopljena upredena parica (STP) ima bolja svojstva na nižim brzinama (zaštićena je od vanjskih elektromagnetskih utjecaja), skuplja je i neprikladna za instaliranje Standard EIA-568 definira STP 150 Ω i UTP 100 Ω za kabel, konektore itd. Prijenos u transponiranom frekvencijskom pojasu, tj. širokopojasni (*Broadband*) sustav, u području lokalnih mreža smatra se onaj koji zahtijeva širinu kanala veću od 4 kHz. Obavlja se analogni prijenos informacija uporabom modema, a moguće je koristiti više kanala (uporabom FDM) za podatke, govor, sliku itd. Obično se koristi CATV koaksijalni kabel (75 Ω).

LLC protokol omogućuje protokolima višeg sloja (u OSI referentnom modelu lokalne mreže to su protokoli mrežnog sloja) da zajednički dijele (*share*) – upotrebljavaju fizički link u LAN-u.

Topologije lokalnih mreža

Na području lokalnih mreža prisutne su sve moguće topologije. Međutim, samo neke su često korištene. Odmah treba istaknuti razliku između logičke topologije (arhitekture) i fizičke topologije.

Logička topologija lokalne mreže pokazuje logiku povezanosti između krajnjih stanica. Najčešće korištene takve topologije kod LAN-ova su sabirnica i prsten u mnogobrojnim varijantama: jednostruke, dvostruke, jednosmjerne, dvosmjerne, itd. Tipični primjeri mreža su *Ethernet* i DQDB (*Distributed Queue Dual Bus*) prstenasti *Token Ring* i FDDI (*Fiber Distributed Data Interface*). Općenito, kad govorimo o topologiji neke lokalne mreže, tada mislimo na njenu logičku konfiguraciju.

Fizička topologija pokazuje kako je fizički izvedena (instalirana) pojedina lokalna mreža. U tom slučaju obično govorimo o kabliranju ili ožičenju lokalne mreže. Fizički se lokalna mreža može izgraditi gotovo na sve moguće načine, primjerice kao zvijezda, stablo ili mreža većeg stupnja povezanosti (*mesh*), kada između čvorova postoji veći broj putova. Na primjer, logički prsten se može izgraditi kao fizička zvijezda. Izbor fizičke topologije ovisi o mogućnostima kabliranja npr. potrebnim građevinskim zahvatima u zgradi), zahtjevima za pouzdanost (npr. obzirom na namjerne i nenamjerne kvarove), troškovima itd.

Pristupni protokoli

Metoda pristupa većeg broja korisnika zajedničkom mediju je najšire korištena razlika pojedinih lokalnih mreža. Pristupni protokol MAM (*Multi Access Method*), je skupina pravila koja određuje redoslijed kojim stanice mogu pristupiti korištenju zajedničkog medija (komunikacijskih kanala). Pristupni protokol zahtjevi trebaju zadovoljiti neke uvjete od kojih su najvažniji sljedeći: jednostavnost, racionalnost (sam protokol mora trošiti male komunikacijske i procesorske resurse medija i stanica), robusnost i ravnopravnost.

U slučaju grešaka kod prijenosa i pristupa mediju protokol se mora sam moći "izvući" iz takvih situacija (robusnost). U idealnom slučaju mehanizam oporavka trebao bi biti uključen samo u onim stanicama koje komuniciraju u trenutku kad dolazi do grešaka.

Ravnopravnost ili poštenje (*fairness*) u pristupu zajedničkom mediju omogućuje svim stanicama ravnopravno korištenje mrežnih kapaciteta. To znači da niti jedna od stanica ne može zauzeti sav prijenosni kapacitet i time monopolizirati mrežne resurse. Dakako, neke mreže koriste prioritetni pristup mediju. Ovdje su stanice podijeljene u prioritetne razrede tako da one stanice iz višeg prioritetnog razreda mogu pristupiti većem mrežnom kapacitetu nego stanice s nižim prioritetom. Naravno, to baš i nije pošteno, a implicira da nekim stanicama treba blokirati pristup mediju u trenucima velikog prometnog opterećenja (tzv. tranzijentno blokiranje).

Pristup mediju u LAN mrežama upravljan u MAC (*Medium Access Control*) podsloju. Kao i kod svakog upravljanja (kontrole) ovdje i ovdje postoji centralizirana i decentralizirana kontrola pristupa mediju. Kod centraliziranog pristupa, stanica može pristupiti mediju tek nakon što primi odobrenje iz centra, a kod decentraliziranog pristupa sve stanice kolektivno obavljaju kontrolne funkcije pristupa mediju te dinamički određuju redoslijed pojedinačnog pristupa. I jedan i drugi pristup imaju dobre i loše strane, ali je decentralizirani dominantan kod lokalnih mreža. Druga gruba podjela kontrole pristupa ovisi da li je pristup sinkron ili asinkron.

Kod sinkronog pristupa određeni kapacitet dodjeljuje se pojedinoj vezi. Takva deterministička metoda nije optimalna za LAN/MAN mreže, gdje potrebni komunikacijski kapaciteti pojedine stanice općenito nisu predvidivi. Asinkroni (dinamički) postupak ima očite prednosti i možemo ga podijeliti u tri skupine: ciklički, slučajan i rezervacijski pristup mediju. Prva dva pristupa su dominantna u LAN mrežama.

Budući da su ovdje posebno važna svojstva prometa koji generiraju stanice, podsjetimo se na dvije osnovne vrste prometa prisutnih kod mreža: približno kontinuirani promet - struja bitova (*stream traffic*) - takva je obično govorna veza ili prijenos velike datoteke i usnopljen ili praskav promet (*burst traffic*) - kakav je najčešće običan interaktivni promet terminal-računalo). Kod uobičajenih LAN mreža prometa posebno je izrazit usnopljen promet.

Ciklički ili kružni pristup (*Round Robin*) za veliki broj stanica,

Polling – centraliziranim upravljačkim pristupom; token bus i Token Ring - decentraliziranim upravljačkim pristupom.⁵

Kod ovog jednostavnog pristupnog protokola svaka stanica u sekvencijalnom logičkom redosljedju dobiva odobrenje za predaju okvira mediju.. Naravno, kad stanica dobije odobrenjem ona može odustati od predaje okvira (npr. nema ništa za slanje), ali nakon isteka odobrenog vremena ona pravo odašiljanja prosljeđuje idućoj stanici u logičkoj (sekvenci). Upravljanje može biti centralizirano i decentralizirano. "Polling" kod terminalskih mreža je primjer centraliziranog upravljanja. *Token Bus* i *Token Ring* su primjeri decentraliziranog upravljanja (kontrole) pristupa zajedničkom mediju. Kad je aktivan velik broj stanica, ova je metoda vrlo učinkovita. Kod aktivnosti malog broja stanica, tj. kod malog prometa, obično su druge pristupne metode znatno učinkovitije.

Slučajan pristup (Ethernet)

Kod ove pristupne metode sve stanice mogu slučajno pristupiti mediju, bez centralne kontrole redosljeda pristupa (po prirodi stvari to je decentralizirana metoda). U biti, stanice zauzimaju medij u međusobnom natjecanju pa se metoda i natjecateljska (*contention*). Jednostavnost, visoka učinkovitost kod malog i srednjeg prometa, te prikladnost za posluživanje usnopljenog prometa su glavne prednosti ove pristupne metode. Kod veliko prometa (aktivnosti velikog broja stanica) može doći do prometnog kolapsa (*deadlock*), tj. do degradacije performansi (veliko kašnjenje, mala ili gotovo nikakva propusnost). Tipičan protokol te vrste kod LAN mreža je IEEE 802.3 CSMA/CD, Ethernet.

Rezervacijski pristup

Rezervacijski pristup mediju, centralizirani ili decentralizirani, je prikladan za kontinuirani promet. Obično je vrijeme na mediju odijeljeno u odsječke slično kao kod sinkronog vremenskog multipleksa (TDM), a stanica koja želi pristup rezervira budući vremenski odsječak, praktički na neograničeno vrijeme. Rezervacija može biti centralizirana ili decentralizirana. Ova se metoda zove TDMA (*Time Division Multiple Access*) i često se koristi kod paketnih radio i satelitskih komunikacija. Postoji i stariji FDMA (*Frequency Division Multiple Access*) i u novije vrijeme CDMA (*Code Division Multiple Access*) i WDMA (*Wavelength Division Multiple Access*).

Zajednički prijenosni medij

Obzirom na prijenosni medij (fizički sloj OSI modela koji još određuje i druge fizičke elemente prijenosa, npr. konektore, linijski kod itd.) lokalne mreže dijelimo na žične i bežične.

Žični mediji

Glavni predstavnici su bakreni i optički (jednomodni i višemodni) prijenosni mediji. Ovdje dajemo samo neke osnovne karakteristike bakrenih medija. Za detalje (npr. UTP 5, strukturalno kabliranje, *hubbing*⁶ itd. vidjeti navedenu literaturu).

⁵ Pravilno smjestiti u kontekst!!!!!!!!!!!!!!

⁶ Da li je možda hubbing??????

U uobičajenim (sporim) lokalnim mrežama gotovo isključivo se koriste bakreni mediji. Za svaku vrstu mreže postoje standardi koji detaljno definiraju električka svojstva medija (npr. karakterističnu impedanciju, maksimalnu udaljenost između stanica itd.): Navodimo neke uobičajene karakteristike iz IEEE 802.3 standarda koji vrijedi za Ethernet mrežu.

Fizičke karakteristike Ethernet IEEE 802.3

(Upredena (neoklopljena) parica kategorije 3 (10Base-T): jeftino rješenje za najveće udaljenosti od 250 m kod brzine 10 Mbit/s i najveće udaljenosti 100 m kod brzine od 10 Mbit/s; osjetljivost na smetnje je značajna. Postoje 5, 5c, 6 UTP.

Tanki Ethernet (10Base2): tanki koaksijalni kabel koji omogućuje jednostavno uredsko kabliranje i jeftino priključenje stanica (BNC-T konektor), najveća duljina segmenta je 185 m, najmanja udaljenost između stanica 0,5 m, a najveći dozvoljeni broj stanica na jednom segmentu je 30.

Debeli Ethernet (10Base5): najbolje i najskuplje rješenje koje omogućuje priključivanje (pomoću MAU jedinca) najviše 100 stanica do udaljenosti od 500 m uz najmanji razmak između stanica 2,5 m. Medij – globalni koaksijalni kabel.

Brzi Ethernet (100Base-T): zvjezdasta topologija koja se može realizirati na više načina uz različite troškove i ograničenja: npr. 100Base-TX (2 UTP 5 ili dva STP), 100Base-T4 (4 UTP 3 ili UTP 5), 100Base-FX (2 optičke niti).

Navedimo samo da se na fizičkome sloju LAN može proširiti (tzv. prošireni LAN) s najviše pet segmenata u jednu stablasto oblikovanu mrežu najvećeg raspona do 2500 m, odnosno do 925 m (10Base2). Spajanje segmenata obavlja se pomoću prijenosnika (*repeater*) koji može imati jedan ili više priključaka (*portova*) - slika 2.

UTP ... *Un-shielded Twisted Pair*, neoklopljena upletena parica,

STP ... *Shielded Twisted Pair*, oklopljena upletena parica,

10Base2 – oznaka inačice standarda IEEE 802.3:

10 ... prijenosna brzina 10 Mb/s,

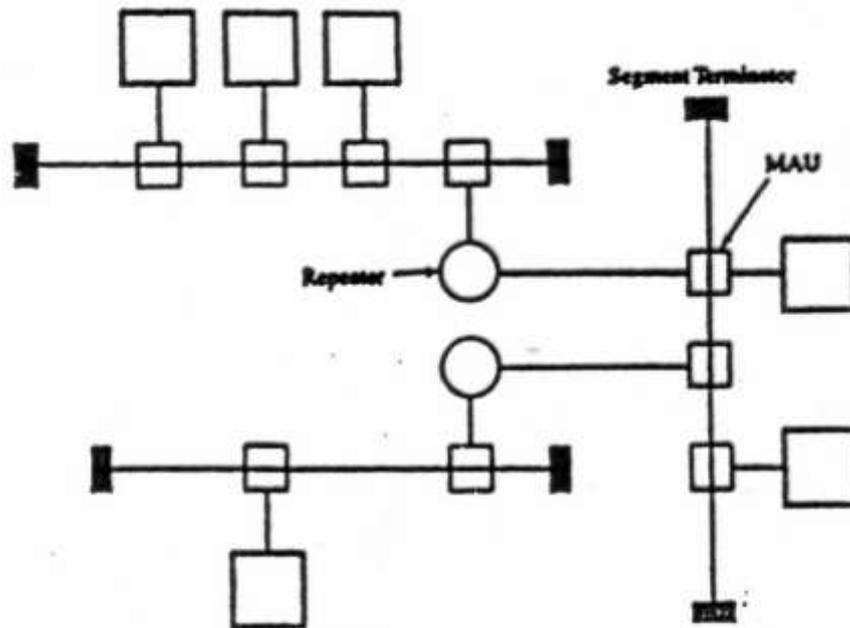
Base ... *base-band* – označava rad u osnovnom pojasu,

2 ... maksimalna dozvoljena duljina segmenta izražena u stotinama metara.

Bežični mediji

Vrlo je intenzivan razvoj bežičnih lokalnih mreža koje se odlikuju sljedećim prednostima:

- ne treba kablirati kod preoblikovanja mreže;
- velika pokretnost radnih stanica (neke mogu biti uvijek pokretne);
- lako uključivanje na brzu osnovnu mrežu (npr. na MAN);
- potiče razvoj tzv. personalnih komunikacija.



Slika 2 - Primjer za prošireni LAN

Obzirom na korišteni frekvencijski spektar, bežični LAN-ovi se dijele u dvije glavne skupine:

Radio LAN: moguće je postići veće brzine ali uz veće troškove, osjetljivost na interferencije je znatna, frekvencije uglavnom moraju biti odobrene (licencirane). važnije podvrste obzirom na frekvencijsko područje, odnosno korištenu modulaciju: mikrovalno (GHz) i "raspršeni spektar" (*spread spectrum*, MHz).

Infracrveni LAN ograničen je na manje brzine (velika disperzija signala), geografska pokrivenost je mala (optička vidljivost), mali troškovi, ne treba odobrenje frekvencija.

Brzina prijenosa po zajedničkom mediju

Obzirom na brzinu LAN-ovi se mogu podijeliti na sljedeće glavne skupine:

Spori. Brzina je obično 10 Mbit/s - 20 Mbit/s, a tipični predstavnici te skupine su uobičajeni LAN-ovi: Ethernet i IEEE 802.3 CSMA/CD brzine do 10 Mbit/s, IEEE 802.4 *Token Bus* i IEEE 802.5 *Token Ring* brzine 4 i 16 Mbit/s. Postoje žični (bakreni) i bežični LAN-ovi tih brzina.

Brzi: Brzina se obično kreće između 50 Mbit/s i 100 Mbit . Prijenosni medij je optičko vlakno (jednomodno ili višemodno), a tipični su predstavnici *Fast Ethernet* 100Base-T(100 Mbit/s), 100GV *AnyLan* (Mbit/s), FDDI - ANSI standard i DQDB - IEEE 802.6 MAN standard.

Superbrzi: Brzina je reda Gbit/s. Neki primjeri su UltraNet i CP (*Crossbar Processor*). Ograničeno geografsko područje (za sada LAN i MAN mreže), a uobičajaje te bakreni medij. ANSI je razvio standard (odbor ANSI X3T9.3) za HiPPI (*High Performance Parallel Interface*) za povezivanje brzih (super)računala na temelju bakrenog prijenosnog medija.

Ultrabrzi; Brzine ulaze u područje Tbit/s. Razvijeno je više eksperimentalnih mreža (npr. *Multi-hop network*, AT&T), prijenosni medij je jednomodno vlakno, a pristupni medij je valni multipleks (WDMA).

21.2. Osnovno o performansama lokalnih mreža

Između brojnih mjera performansi LAN i MAN mreža najčešće su korištene sljedeće:

- Kašnjenje D: vrijeme od očetka odašiljanja paketa (okvira), do njegove uspješne isporuke odredištu.
- Propusnost mreže S: ukupna brzina prijenosa podataka između čvorova (obavljeni promet).
- Iskoristivost medija I: dio ukupnoga korištenog kapaciteta.

Parametar S je često normaliziran obzirom na kapacitet pa ga se može interpretirati i kao iskoristivost medija l . Na primjer, ako se u trajanju od 1 s Ethernet mrežom prenosi 1 Mbit tada je $S = 0,1$. Dakako, ova se propusnost odnosi na ukupnu količinu prenesenih bita, tj. i informacijskih i svih dodatnih bita (zaglavljiva okvira, zaštitni biti itd.). Postoje brojne analize performansi LAN i MAN mreža i mi ih ovdje ne iznosimo zbog ograničenosti prostora. Navedimo samo da su najčešće S i D prikazani u ovisnosti od ponuđenoga prometa koji je ovdje ukupan broj paketa svih vrsta ponuđenih mreži; taj je promet također često izražen kao dio kapaciteta mreže.

Najvažniji čimbenici koji utječu na performanse LAN i MAN mreža su sljedeći:

- Kapacitet,
- Propagacijsko kašnjenje,
- Duljina okvira,
- Mrežni protokol,
- Ponuđeno prometno opterećenje,
- Broj stanica priključenih na mrežu.

Ovdje ćemo raspraviti samo prva tri čimbenika. Navedimo da kod LAN protokola najveći utjecaj ima MAC protokol, dok se LLC obično uzima u obzir kod analize performansi s kraja na kraj (npr. kod umrežavanja). Ponuđeni promet i broj stanica se najčešće smatraju neovisnim varijablama, tako da se analize svode na ovisnost performansi od tih dviju varijabli. Kod umrežavanja LAN mreža uporabom WAN mreže (npr. X.25, satelitska veza) važna je i učestalost grešaka koja uvjetuje ponovno odašiljanje okvira što smanjuje propusnost mreže. Naravno, kod analize performansi same LAN mreže to nije bitno, jer je učestalost grešaka u lokalnoj mreži vrlo mala.

Bitna razlika između lokalnih i međumjesnih mreža je u brzini prijenosa C i duljini komunikacijskog puta d . Umnožak Cd je važno obilježje neke mreže, koje neposredno određuje njene performanse. Ako je brzina propagacije signala kroz mrežu v , približno $2/3$ brzine svjetlosti (tj. $v = 200\,000$ km/s, odnosno $5\ \mu\text{s}/\text{km}$), tada Cd/v odgovara duljini komunikacijskog puta izražena u bitima. Na primjer, ako je duljina Ethernet kabela 1 km tada je njegova "duljina" u bitima $10\ \text{Mbit/s} \times 5\ \mu\text{s} = 50$ bit. Drugim riječima, 50 bita „juri“ između para stanica na krajevima kabela. Zamislimo da naša mreža ima 100 puta veću duljinu. Tada bi duljina veze bila 5000 bita, pa bi mrežom "letjelo" barem 10 000 bita prije nego bi predajnik primio potvrdu o ispravnom ili neispravnom prijemu odaslanih paketa. Slično bi bilo i s povećanjem brzine prijenosa.

Uzmimo sada da je duljina paketa (okvira) L bita, tj. da vrijeme potrebno predajniku da ubaci okvir na medij iznosi L/C . Tada je Cd/vL omjer duljine puta u bitima i duljine okvira, ili omjer propagacijskoga kašnjenja d/v i trajanja predaje okvira L/C . Omjer Cd/vL je kod LAN mreža obično između 0,01 i 0,1, a za brze mreže može biti veći od 1. Na primjer, uzmimo da dvije lokalne Ethernet mreže međusobno komuniciraju preko geostacionarne satelitske veze brzine 1 Mbit/s za koju je propagacijsko kašnjenje u jednom smjeru oko 250 ms. Ako pretpostavimo da se obavlja prijenos neke datoteke s Ethernet okvirima maksimalne duljine $L = 1500$ byte; tada će "zrakom letjeti" u jednom smjeru oko $250\ \text{ms} \times 1\ \text{Mbit/s} = 250\,000$ bita, odnosno oko 21 Ethernet okvira. Drugim riječima, oko 42 okvira u svakom trenutku nije pod kontrolom predajnika. Ako bi povećali brzinu prijenosa na 10 Mbit/s tada bi imali oko 420 nekontroliranih okvira što je izvor nestabilnosti i niza drugih vrlo teških problema posebno kod kanala s izraženim smetnjama kakav je slučaj kod satelitskih veza. Slični se problemi javljaju i kod MAN mreža i općenito kod brzih mreža. Ne ulazeći u daljnje rasprave niza prisutnih poteškoća navedimo da se često koristi umnožak $C \times \text{RTD}$ (*Round Trip Delay*) umjesto CD), kao mjera performansi neke mreže; RTD je ukupno kašnjenje (suma kašnjenja zbog propagacije; predaje, prijema, obrade itd.) potrebno da predajnik dobije potvrdu ispravnog prijema odaslanog okvira (paketa). Na temelju tih parametara mogu se odrediti propusnost i iskoristivost LAN mreža što ovdje ne izlažemo.

21.3. LAN protokoli

U nastavku dajemo revijalni pregled najvažnijih MAC protokola korištenih kod uobičajenih LAN mreža.

IEEE 802.3 CSMA/CD, Ethernet

Preteča ovoga protokola bio je ALOHA protokol razvijen za paketne radio mreže. Kod tog protokola (tzv. čista ALOHA), neka stanica kad ima okvir za slanje, ona ga i pošalje. Zatim ona sluša maksimalno RTD vrijeme koje je jednako dvostrukom najvećem vremenu kašnjenja okvira između dviju najudaljenijih stanica. Ako ne čuje potvrdu ispravnoga prijama okvira unutar tog vremena, ona ponovo odašilje isti okvir. Naravno, okvir može biti neispravan zbog šuma u kanalu ili zbog interferencije s drugim okvirom koji je poslala neka druga stanica (tzv. sudar ili kolizija okvira). Prijemna stanica jednostavno ignorira pogrešan okvir, a za ispravni šalje potvrdu pozitivnog prijama. Ova jednostavnost protokola plaćena je njegovom neučinkovitošću; porastom prometa (tj. aktivnošću velikoga broja stanica) najveća iskoristivost medija (kanala) je svega oko 18 %. Kod poboljšanog PLOHA protokola, tzv. S-PLOHA (*Slotted ALOHA*), vrijeme na kanalu je podijeljeno na jednake odsječke čije je trajanje jednako trajanju odašiljanja okvira. Sve stanice su sinkronizirane s nekim centralnim taktom, a odašiljanje je dozvoljeno samo na početku pojedinog odsječka. Time su sudari paketa mogući samo na početku vremenskog odsječka čime je učinkovitost udvostručena tj. iznosi najviše 37 %.

Oba PLOHA protokola, osim slabe učinkovitosti, ne koriste osnovnu prednost lokalnih mreža: propagacijsko kašnjenje između stanica je vrlo malo u usporedbi s trajanjem odašiljanja okvira. Primjerice, ako je vrijeme propagacije između dviju stanica veliko u usporedbi s vremenom odašiljanja okvira tada će proći znatno vrijeme prije nego okvir dođe do određene stanice, a u tom intervalu mogu druge stanice slati svoje okvire pa je vjerojatnost sudara velika (manja propusnost). Ako je pak, propagacijsko kašnjenje malo u usporedbi s trajanjem odašiljanja okvira tada nakon početka odašiljanja okvira sve ostale stanice to mogu "čuti" i odustati od slanja svojih okvira sve dok kanal ne postane "gluh". Sudari su rijetki i događaju se uglavnom kad dvije stanice gotovo istovremeno žele odaslati svoje okvire. Dakle, sudari se događaju uglavnom unutar jednog TD. To je bio i glavni razlog za razvoj CSMA (*Carrier Sense Multiple Access*) protokola. On u biti radi po pravilu „slušaj pa onda govori“, tj. ako je medij zauzet, stanica odlaže svoje odašiljanje paketa za neki vremenski odsječak. Ako tada dođe do sudara okvira, jer su barem dvije stanice istovremeno pristupile mediju, svaka će stanica čekati određeno vrijeme potvrde prijema (ovisno od TD i vremena potrebnog određenoj stanici da pristupi mediju). Ako stanica ne primi potvrdu, ona ponovo pokušava odaslati okvir, jer pretpostavlja da je došlo do sudara.

Maksimalna iskoristivost CSMA ovisi od duljine okvira i vremena propagacije: dulji okviri i manje propagacijsko kašnjenje daju veću iskoristivost. Postoje brojni algoritmi za odlaganje pristupa mediju na određeno vrijeme. Primjerice, kod tzv. "CSMA" protokola, stanica čeka slučajan vremenski interval i onda ponovo proba pristupiti mediju. Kod "1-persistent CSMA" ona sluša medij sve dok on ne postane „gluh“ pa onda ponovo proba odaslati okvir.

Ako se dogodi sudar, onda čeka slučajno vrijeme i ponovo pokuša odaslati paket "p-persistent CSMA" protokol je u biti kombinacija gornja dva protokola.

Iako je CSMA protokol učinkovitiji od oba PLOHA protokola, to je još uvijek nedovoljno. Kad dođe do sudara dva okvira, medij se ne koristi tijekom njihovoga odašiljanja čime smanjuje propusnost. To se može poboljšati upotrebom pravila „slušaj dok govoriš“: kad stanica otkrije sudar (CD, *Collision Detection*), ona prekine odašiljanje okvira i obavještava (pomoću tzv. "jamming" signala) ostale stanice o postojanju sudara. Nakon toga čeka slučajan vremenski odsječak (obično je to cjelobrojni višekratnik od TD) i opet proba poslati okvir uporabom CSMA protokola. Postoje brojni algoritmi za izbor „slučajnog“ vremenskog odsječka prije novog slanja okvira. Ethernet i IEEE 802.3 koriste "Binary Exponential Back-off" metodu: nakon prvog sudara stanica odabire 0 ili 1 RTD odsječak prije

nego proba opet odaslati okvir; nakon drugog sudara izabire se slučajan broj iz skupa 0, 1, 2, 3, nakon ponovnog sudara taj se odsječak udvostručuje itd.

Sažeto se može reći da je CSMA/CD protokol jednostavan, pruža stanicama ravnopravan pristup mediju i ima dobre performanse za mali i srednji promet. Najkritičnija je detekcija sudara, dijagnostika grešaka te loše performanse za velika prometna opterećenja.

IEEE 802.4 Token Bus

Opis ovog protokola dajemo sasvim ukratko, jako je on osnova za neke druge protokole. Svaka stanica na sabirnici zna koja je stanici ispred, a koja je iza nje tj. one su povezane u logički prsten. Naravno, fizički one mogu biti spojene na sabirnicu bilo gdje. Svaka stanica dobiva pravo pristupa mediju pomoću kontrolnog okvira (*token*) koji sadrži adresu odredišne stanice. Stanici je pristup mediju dozvoljen za određeno fiksno trajanje kako ne bi došlo do monopoliziranja mreže. Minimalna duljina tog vremena odgovara vremenu transmisije kontrolnog okvira do sljedeće stanice u logičkoj sekvenciji (kad nema ništa za slanje).

Istaknimo samo da su najveće prednosti ovog protokola u odličnim performansama (visokoj propusnosti) koje se ne degradiraju povećanjem duljine medija, kontroliranom pristupu mediju i unaprijed poznatom najvećem vremenu čekanja. Glavni su nedostaci složenost protokola i dodatna kontrolna (redundantna) informacija koja se ubacuje u mrežu (izražena je kod malog prometnog opterećenja).

IEEE 802.5 Token Ring

Ovaj važan protokol ćemo ovdje također kratko opisati. Jednoj njegovoj modifikaciji (FDDI) kasnije će biti posvećena veća pažnja.

Protokol koristi kratki kontrolni okvir (*token*) koji kruži duž prstena kad su stanice nezauzete. On odobrava (kontrolira) pristup mediju: stanica koja želi slati okvire mora čekati (tj. ona kopira svaki okvir, bit po bit, koji prolazi pokraj nje) sve dok ne detektira prolaz kontrolnog okvira. Kad ga "uhvati" ona ga pretvara (zauzima), promjenom jednog bita u novi kontrolni okvir (*connector*) koji je, početak njenog okvira. Dakle, stanica priljepi na takav zauzet kontrolni okvir svoje podatke. Sada nema slobodnog kontrolnog okvira na prstenu pa ostale stanice moraju čekati, a ubačeni okvir kruži duž prstena sve do izvorišne stanice koja ga uklanja iz prstena. Naravno, odredišna stanica, samo kopira njoj adresirani okvir ali ga ne uklanja iz prstena. Predajna stanica ubacuje novi kontrolni znak (tj. slobodni) kad su ispunjeni sljedeći uvjeti. (a) stanica je završila slanje svog okvira i, (b) početak njenog odaslanog okvira se vratio u izvorišnu stanicu. Ako je duljina prstena (izražena u bitovima) manja od duljine okvira, uvjet (a) povlači uvjet (b), tj. stanica promijeni bit zauzeća u pridošlom kontrolnom okviru i time ga pretvori u novi (slobodni) kontrolni okvir. Ako to nije slučaj, stanica ubacuje nov kontrolni okvir odmah nakon završetka slanja svojeg okvira ali još uvijek prije početka prijema vlastitog odaslanog okvira. Sada može nekoliko okvira kružiti prstenom što može zamrsiti otklanjanje mogućih grešaka.

Ovaj je protokol vrlo učinkovit kod velikih prometnih opterećenja i pruža pošten pristup mediju.

Navedimo još da postoje i drugi protokoli za pristup prstenu, a najpoznatiji je prsten čije je vrijeme TD podijeljeno na odsječke fiksne duljine koji kontinuirano kruže duž prstena (slično TDM). Takav je prsten poznat pod imenom *Pierceov prsten* ili *Cambridge prsten* (ISO 8802-7).

22. BRZE LOKALNE I METROPOLITANSKE MREŽE

22.1. Pregled važnih arhitektura

Dajemo kraći pregled topologija za HSLAN⁷ i MAN mreža koje su bilo komercijalno raspoložive ili su neposredno pred komercijalizacijom a nisu utemeljene na ATM tehnologiji.

Prstenasti MAN

Prva generacija MAN arhitektura razvila se iz postojećih LAN standarda zamjenom bakrenog optičkim medijem. Tako se primjerice, FDDI razvio na temelju IEEE 802.5 Token Ring standarda. Sastoji se od dvostrukog optičkog prstena (primarnog i sekundarnog) i višeznakovnog (*multi-token*) protokola, a radi na brzini od 100 Mbit/s uz najveću udaljenost do 200 km. Varijanta FDDI nazvana FDDI-II, podržava isokroni promet. Podsjetimo se da je isokroni prijenos postupak slanja i sinkronih i asinkronih informacija na sinkroni način tj. sinkroni i asinkroni promet se multipleksira u sinkrone okvire. U obje vrste mreža, okvir se uklanja iz izvorišne stanice nakon pune rotacije oko prstena. Propusnost se može prosječno učeterostručiti ako odredište uklanja okvir. Mreža Meta Ring upravo koristi takav postupak (*buffer-insertion ring*) čime je brzina FDDI povećana na 800 Mbit/s.

Sabirničke arhitekture (jednostruke i dvostruke)

Uobičajene sabirničke protokole (Ethernet, Token Bus) nije bilo moguće ubrzati pa je razvijen novi pristupni protokol, tzv. "*implicit token*" jednostrukoj linearnoj sabirnici. To je bio uređen, a ne potpuno slučajan pristup mediju. Grubo govoreći krajnja stanica nakon kontrolnoga okvira (*token*) šalje svoje okvire u skupini (povorci), a nakon jednog potpunog ciklusa ona počinje odašiljati novi ciklus takve povorke okvira. Na svakom sučelju treba obaviti regeneraciju signala, sam kontrolni okvir (*token*) ne treba obrađivati. Brojne su mreže razvijene na toj osnovi; npr. *FastNet*, *ExpressNet*, *U-Net Magnet* itd. Jedno često spominjano poboljšanje koristi se u mreži *Buzznet*. Ona koristi hibridni protokol: CSMA/CD protokol kod malog prometnog opterećenja, a znakovni protokol kod velikog prometnog opterećenja.

Postoje brojne realizacije dvostruke sabirničke arhitekture. DQDB je najpoznatiji rezervacijski protokol za takvu strukturu. Ovdje svaka s stanica ima lokalni red čekanja pomoću kojeg se obavlja rezervacija "kanala". Ovakav mehanizam distribuirane rezervacije vrlo je jednostavan i učinkovit. Rezervacija se obavlja unutar okvira (tj. neke njegove lokacije služe za rezervaciju, tzv. *piggybacked*) čime se izbjegava kašnjenje nastalo zbog "praznog ciklusa" kontrolnog okvira, a iskoristivost kanala je gotovo potpuna kad sustav radi s jednom predajnom stanicom. Ova je strategija široko prihvaćena kao MAN standard (IEEE 802.6) i zbog visokog stupnja kompatibilnosti s ATM (npr. fiksna i jednako dugačka ćelija kod oba standarda itd.). DQDB → kompatibilan s ATM,

22.2. FDDI

Prva verzija FDDI razvijena je samo za podatkovne aplikacije, a nova verzija FDDI-II integrira podatkovne i izokrone usluge. FDDI se temelji na topologiji dvostrukog prstena.

Osnovne prednosti su:

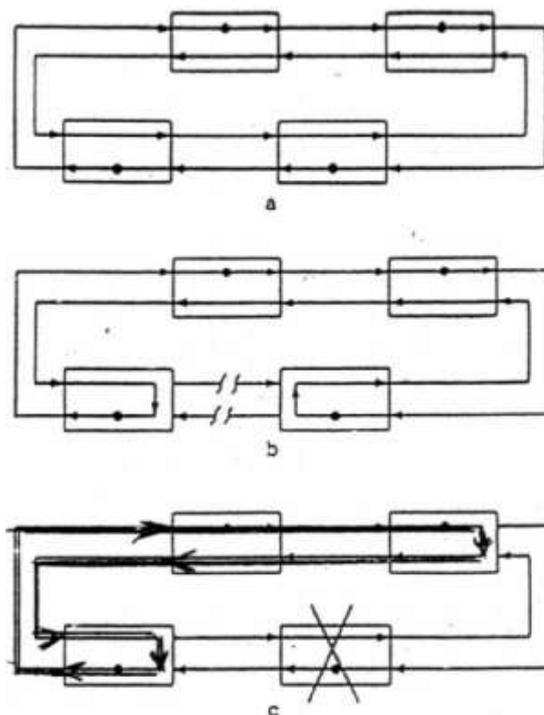
- Prsten ne pretpostavlja ograničenja na duljinu linkova, broj stanica i ukupni raspon MAN-a.;
- Mogu se postići visoke performanse uz visoku neosjetljivost na prometna preopterećenja i ravnopravnu dodjelu mrežnih resursa.;
- Dvostruki prsten je otporan na kvarove (slika 3).;
- Linkove između stanica je moguće pojedinačno optimizirati (linkovi su od točke do točke).

FDDI je proizašao iz IEEE 802.5 Token Ring standarda i definiran je u ANSI odboru X3T9.5, a prihvaćen je i od ISO udruge. Obzirom na sličnost s vrlo učinkovitim (kod velikog prometnog

⁷ Značenje akronima ?????????????

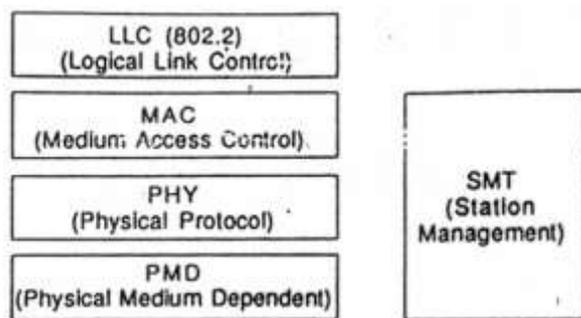
opterećenja) znakovnim (*token*) protokolom ovdje navodimo samo važnije specifičnosti FDDI standarda.

Unutar donja dva sloja OSI modela IEEE 802 skupina standarda definira podslojeve koji se koriste za LAL i MAN primjene (slika 4.), Definirane su dvije alternativne varijante za PMD (*Physical Medium Dependent*) kod FDDI: osnovni PMD koristi višemodno vlakno na prozoru od 1325 nm i SMF-PMD jednomodno vlakno). Prva alternativa je jeftinija (koristi se jeftiniji LED predajnik), a kabel ima dva vlakna (po jedno za svaki smjer u normalnom načinu rada). Druga varijanta je skuplja: koristi predajnik s laserskom diodom, a udaljenosti između stanica mogu biti do 100 km. Na jednom prstenu mogu se koristiti obje te varijante: npr. na kraćim udaljenostima koristi se višemodno, a na duljim jednomodno vlakno.



Slika 3 Rekonfiguracija dvostrukog FDDI prstena: (a) normalni način rada, (b) kvar na linku i (c) kvar u čvoru

Na fizikalnom podsloju (PHY na slici 4) brzina prijenosa je 1 Mbit/s ali zbog uporabe koda 4B/5B preko PMD se postiže brzina prijenosa od 125 Mbaud/s. Najveća duljina okvira je 4500 okteta (ograničeno zbog moguće akumulacije kolebanja – *jitter*). Mreža se sama može rekonfigurirati u slučaju grešaka, a vrijeme obnavljanja konfiguracije na fizikalnom sloju je izračunato za najviše 500 stanica i optičko vlakno duljine 100 km (*duplex*).



Slika 4 - Arhitektura FDDI protokola

U prstenu svaka stanica prosljeđuje primljeni okvir susjednoj stanici. Ako je odredišna adresa okvira jednaka njenoj vlastitoj adresi, ona okvir kopira u svoj spremnik. Okvir nastavlja kruženje duž prstena sve dok ne stigne o izvorišne stanice koja ga uklanja iz prstena na temelju usporedbe svoje adrese i izvorišne adrese u okviru. Tijekom uklanjanja okvira, izvorišna stanica šalje simbol IDLE na prsten:

Kontrolni okvir se također šalje. Ako stanica želi odaslati okvir, ona to može samo kad je "ulovila" kontrolni okvir. Kad je završila s odašiljanjem jednog ili više okvira, kontrolni okvir se opet ubacuje omogućavajući time idućoj stanici koja čeka na odašiljanje okvira, da ga "uhvati". U trenutku kad stanica koja je "uhvatila" kontrolni okvir želi odaslati okvir, kroz dugačak i aktivan prsten već kruže brojni ranije ubačeni okviri. Oni će dakako biti uklonjeni iz prstena u stanicama koje su ih odaslale, prije nego dođu u prijemnik stanice koja trenutno odašilje okvir. Ulaz u prijemnik te stanice se sastoji od IDLE znaka i «ostatka» uklonjenih okvira, tj. nekorisni okviri dolaze u stanicu koja posjeduje kontrolni okvir. U svakom slučaju, stanica koja predaje okvire uklanja iz prstena sve što dođe u njen prijemnik. "Ostaci" okvira postoje zato, jer stanica uklanja okvir na temelju usporedbe svoje adrese s izvorišnom adresom u okviru, a to se provodi nakon što je već dobar dio okvira prosljeđen susjednoj stanici - SA (*Source Address*) polje je dosta daleko od početka okvira.

Nakon završetka odašiljanja predajna stanica šalje novi kontrolni okvir koji će susjedna stanica «uhvatiti» ukoliko čeka na odašiljanje svojih okvira. Osim toga, ona nastavlja slanje IDLE znaka sve dok ne primi SD novog okvira. Tada MAC mehanizam ponovo inicira ispitivanje svih pridošlih okvira, uklanjanje onih kojima je ta stanica izvorište i prosljeđivanje (bit po bit) svih ostalih okvira.

Vidimo veliku sličnost ovo protokola s IEEE 802.5.

Dvije bitne razlike su vezane uz

- a) ubacivanje kontrolnog okvira u prsten (FDDI ubacuje novi kontrolni okvir neposredno iza informacijskih okvira, dok 802.5 novi kontrolni okvir ubacuje tek kad se početak odaslanog informacijskog okvira vratio u stanicu.) i
- b) rezervaciju kapaciteta.

Da bi se osigurali od vječnog zauzimanje kontrolnog okvira, koristi se TTR (*Time Token Rotation*) protokol koji stvarno-vremenskim ("*stream*") uslugama (govor, video) daje veći prioritet nego podatkovnim (osigurava se njihova vremenska transparentnost); a preostali kapacitet se koristi za čisto paketne aplikacije koje vremenski nisu zahtjevne. TTR protokol se temelji na mjerenju vremena boravka kontrolnog okvira na prstenu. TTRT (*Target Token Rotation Time*) je definirana granična vrijednost jednaka za sve stanice na prstenu, a svaka stanica još ima dva vremenska brojila: TRT (*Token Rotation Time*) koji bilježi vrijeme zadnje primljenog kontrolnog okvira i THT (*Token Hold Time*) koji sadrži vrijeme dozvoljenog boravka kontrolnog okvira u toj stanici.

Stvarno-vremenski promet može se uvijek slati, unutar dodijeljenog kapaciteta nakon što je zauzet kontrolni okvir. Paketske usluge mogu zauzeti kontrolni ($TRT < TTRT$) okvir samo kad je vrijeme od zadnjeg prijema manje od TTRT. To osigurava da se slobodno vrijeme popunjava s prometom nalik paketskom tijekom njegovog prijenosa THT se umanjuje. Iskoristivost prstena je uvijek bolja od (TTRT-RL)/TTRT, gdje je RL (*Ring Latency*) uglavnom ovisan od propagacijskog kašnjenja prstena bez prometnog opterećenja. Garantira se da će vrijeme odziva prstena biti manje od dvostruke vrijednosti TTRT.

Moguće je odrediti različite performanse za FDDI ovisno od prometa (tj. različitih veličina paketa) i konfiguracije mreže (broja stanica, udaljenost i sl.). Postoje brojne, studije i znanstveni izvještaji o performansama FDDI a ovdje dajemo samo osnovne zaključke. Za kratke pakete najveće prometno opterećenje je blizu 60 %, a za vrlo duge pakete može se doseći vrlo veliko prometno opterećenje posebno kod kratkih prstena. Pritom je dakako, kašnjenje za duge pakete znatno veće nego za kratke. Također se pokazuje da duljina prstena ima bitno veći utjecaj na performanse od broja stanica na prstenu. Tako su kraći prsteni znatno učinkovitiji od dugačkih, jer je potrebno vrijeme kruženja kontrolnog okvira između susjednih stanica znatno duže kod duljih prstena.

22.3. DQDB IEEE 802.6 (dvostruka sabirnica, distribuirani redovi čekanja, kompatibilnost s ATM)

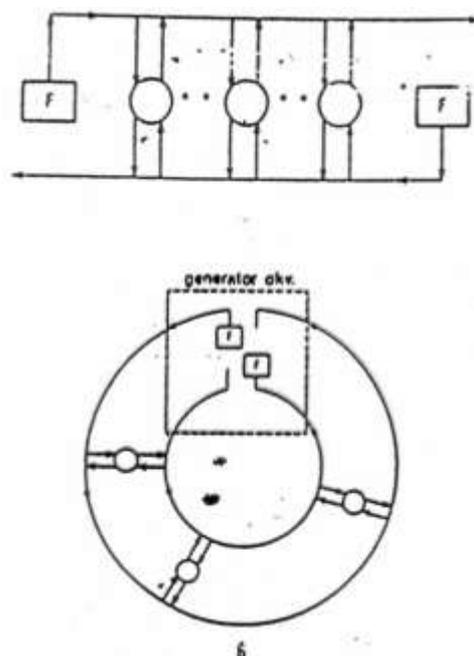
DQDB je standard za MAN, definiran u pododboru IEEE 802.6, a temelji se na topologiji dvostruke sabirnice i pristupnog mehanizma distribuiranih redova čekanja. Početno se taj distribuirani pristupni mehanizam (1988. godine) javio u Australiji pod imenom QPSX (*Queued Packet and Synchronous*

Switch). Razvoj se unutar IEEE 802 odvijao paralelno sa standardizacijom ATM unutar ITU pa je postignuta vrlo velika kompatibilnost između dva standarda.

Uz dvije jednosmjerne suprotno usmjerene sabirnice potrebna je tzv. «*head end*» stanica koja generira DQDB okvire (segmente u DQDB terminologiji) - slika 5(a).

Pristupne jedinice (čvorovi) su povezani na obje sabirnice uporabom odgovarajućih ulazno/izlaznih jedinica. Ulazne jedinice su spojene na sabirnicu za učitavanje pridošlih podataka (oni prolaze transparentno kroz čvorove), a izlazne su spojene na ispisnu sabirnicu. Ispisivanje podataka na svakoj sabirnici obavlja se pomoću logičke ILI funkcije između podataka koji su već na sabirnici i podataka iz čvora (ukoliko su raspoloživi).

DQDB standard namijenjen za aplikacije visoke performanse i brzina (34, 45, 140 ili 155 Mbit/s), paketnu i kanalnu komutaciju u MAN mrežama koje su konceptualno ekvivalentne LAN mrežama, ali pokrivaju veća područja (čitave gradove). DQDB definira poput ATM-a, ćeliju sa zaglavljem od 5 okteta (malo se razlikuje od ATM-a) i korisničko opterećenja (*payload*) od 48 okteta. DQDB, za razliku od FDDI, nije specificiran za prijenos samo po svjetlovodnom vlaknu nego i za radio relejne i satelitske linkove.



Slika 5 DQDB arhitektura (a) dvostruke sabirnice i (b) dvostruke sabirnice spojene kao otvoren prsten.

Time se postiže visoki stupanj pouzdanosti, jer podaci ne prolaze kroz čvor, a kvar ili uklanjanje čvora iz sabirnice ne remeti ispravan rad mreže. Ako pak dođe do kvara na sabirnici tada se mora aktivirati procedura za njenu rekonfiguraciju. To je jedino moguće ako je sabirnica instalirana kao dvostruki otvoreni prsten (slika 5b). U tom se slučaju sabirnice zatvaraju na svojim krajevima (uklanjajući tako funkcije generatora okvira), a mjesta prekida ili kvara sabirnice se sada smatraju “prirodnim krajnjim točkama sabirnice, S druge strane, čvorovi u kvaru postaju generatori okvira, a krajevi sabirnice se moraju zatvoriti u prsten (zato moraju i biti na istoj lokaciji, tj. mora se instalirati prstenasta konfiguracija sabirnice).

Ne ulazeći u daljnje obrazlaganje rada DQDB navedimo da su performanse takve mreže ovisne od pozicije stanice na sabirnici tj. prisutni su problemi ravnopravnog pristupa korisnika DQDB mreži koji se rješavaju primjenom metoda rezervacije. Stanica mreže koristi sljedeći vremenski odsječak, ako je na brojaču vremenskih odsječaka (koje zahtijevaju druge stanice) vrijednost jednaka nuli u trenutku kad stanica želi poslati poruku. Vrijednost na brojaču se povećava za svaki odsječak, što po zahtjevu (druga stanica), a koji dolazi iz smjera odredišta. Ova se vrijednost smanjuje za svaki prazan odsječak prema odredištu. To znači da svaka stanica podržava brojanje vremenskih odsječaka za svaki smjer

prijenosa, Paketi varijabilne dužine prispjeli iz lokalnih mreža u DQDB mrežu cijepaju se 53 oktetna segmenta za prijenos u vremenskim odsječcima po odabranoj sabirnici.

22.4. Ograničenja kod današnjih lokalnih i Metropolitanskih mreža

Kao i kod WAN mreža (vidi poglavlje: *Arhitekture mreža*) glavna ograničenja proizlaze iz dostignutog stupnja tehnološkog razvoja i komercijalizacije tog razvoja. Ta tehnološka ograničenja utječu na brzinu, arhitekturu i mogućnosti postojećih i budućih mreža.

Treba odmah reći da su aktualne (bakrene) ne-komutirane vrste LAN-ova topološki jednostavne (od točke do točke) i nefleksibilne. Problematično je, ako ne i nemoguće, ostvariti "više-kanalske" veze, tj. istovremeno obavljanje više komunikacija kroz zajednički medij.

S optičkim prijenosnim medijem moguće je realizirati složene arhitekture LAN/MAN mreža, poput zvjezdastih i stablastih konfiguracija. Tako je, primjerice, u stablastu konfiguraciju moguće distribuirati nekoliko tisuća stanica na velikom području uporabom pasivnih optičkih elemenata i optičkoga pojačala smještenoga u korijen stabla. Komercijalizacija takvog rješenja se, dakako, tek očekuje.

Današnji brzi LAN-ovi poput FDDI i DQDB, temelje se na (više-modnom) optičkom vlaknu, direktnoj detekciji optičkog signala, jeftinim (LED) predajnicima, Na jedno-modnom vlaknu te mreže mogu dostići brzine od 1 Gbit/s, a buduće mreže bi uporabom valnog multipleksa, trebale dostići područje brzina Tbit/s.

Najnovija istraživanja usmjerena su na kombinaciju WDM i potpunog optičkog prijenosa, gdje se optički signal komutira na čisto fotoničkoj osnovi. Time se uklanjaju nepoželjne i dugotrajne elektro-optičke pretvorbe unutar mreže. To će imati za posljedicu mogućnost izgradnje složenijih mrežnih struktura.

Danas najpoznatija složenija konfiguracija (tj. ona većeg stupnja povezanosti - "mash» arhitektura) je MSN (*Manhattan Street Network*) koja je organizirana kao kvadratična rešetkasta mreža. Da bi se izbjegli efekti postupka "spremi i proslijedi» (tj. potreba za spremnicima i svim problemima koji iz toga proizlaze), koristi se relativno jednostavno usmjeravanje (*deflection routing*). Ono se obavlja u svakom čvoru takve rešetke. Svaki čvor ima točno dva ulaza i izlaza. Ako su oba ulaza zainteresirana za isti izlaz, samo jedan paket se šalje na taj izlaz, a drugi se šalje na «pogrešan izlaz». Sada se taj «pogrešno» usmjereni paket forsirano usmjerava oko pripadnog «oka» rešetkaste mreže. Time se izbjegava potreba za spremanjem paketa u čvorovima rešetke (niža cijena čvora), premda se ponešto smanjuje propusnost mreže. Sve u svemu, dobre strane MSN mreže su dobra pokrivenost gradskog područja, jednostavnost protokola i čvorova i moguća «neograničena» propusnost, jer mreža raspolaže brojnim paralelnim (točnije konkurentnim) stazama usmjeravanja. Glavni je nedostatak MSN mreže neučinkovito podržavanje isokronog i difuznog (*broadcast, multicast*) prometa. Optičke mreže koje se temelje na WDM pristupu trebaju pomiriti dobre i loše strane MSN arhitekture, dakako uz pretpostavke daljeg tehnološkog napretka. Istaknimo da višeslojna mrežna arhitektura s osnovnim prstenom na vrhu hijerarhije i nekoliko nižih slojeva distribuiranih prstena (vidi Tema 3) treba biti osnova budućih ultrabrzih mreža. Pristupna mreža bi se temeljila na WDM pristupu u zajedničkom mediju. Sada se mogu uočiti i neke slabosti takve arhitekture. Prvo, niti FDDI niti DQDB (*Distribute Queue Dual Bus*) - dvostruka sabirnica s distribuiranim redovima čekanja (za rezervaciju «kanala») nisu prikladne arhitekture za upotrebu WDM zbog visokih troškova adaptacije. Naime, WDM omogućuje ostvarenje brojnih istovremenih veza (kanala) na jednom vlaknu (terabitske brzine) ali svaka stanica mora imati sučelje s filtrom spliterom i pojačalom što su veliki zahtjevi. Drugi nedostatak je vezan uz zahtjeve na most (bridge) koji treba povezivati susjedne slojeve u takvoj arhitekturi. Njegova praktična propusnost bi uz takve brzine trebala biti barem 100 kilopaketa/s. Pri tome se javljaju još i problemi vremenske transparentnosti kod govorne i video usluge nakon prolaska preko nekoliko mostova.

Sažeto, jedino sagledivo rješenje za ultrabrze mreže je potpuno optička mreža; pasivni optički elementi, WDM, optičko komutiranje, upravljanje kojim se, upravljajući dodjelom valnih duljina,

dinamički rekonfigurira topologija mreže ovisno od prometne situacije u mreži i zahtjeva korisnika. Neposredniji zadatak povezivanja LAN/MAN/WAN mreža još je uvijek otvoreno područje, a tipičan aktualan istraživački izazov može se sročiti sljedećim pitanjem:

“Kako ostvariti sučelje CL (*connectionless*) okoline koja je tipična za LAN mreže, sa CO (*connection*) orijentiranom ATM okolinom, koja je standardizirani transportni protokol za B-ISDN.

23. POVEZIVANJE LOKALNIH MREŽA

Tehnička ograničenja na fizičko proširenje, broj stanica, performanse i operacijska ograničenja na sigurnost i održavanje, zahtijevaju povezivanje više lokalnih mreža u jedinstvenu mrežu.

23.1. Osnovni elementi potrebni za umrežavanje lokalnih mreža

Most (*Bridge*)

Djelovanje mosta je ilustrirano na sl. 6(b). Most radi na slojevima 1 i 2 OSI modela, povezujući LAN-ove iste vrste. Dakle, most osigurava povezivanje preko LLC i MAC podsloja (DLL sloj OSI modela). Budući da radi ispod mrežnog sloja, most je neovisan od korištenog protokola (OSI slojevi 3-7 moraju biti jednaki u krajnjim stanicama) pa se često zove i transparentni most ili MAC most (radi na tom podsloju). On "čita" sve prolazeće pakete, ali interpretira samo izvorišne i odredišne adrese (i eventualno još neke kontrolne informacije) pojedinog paketa.

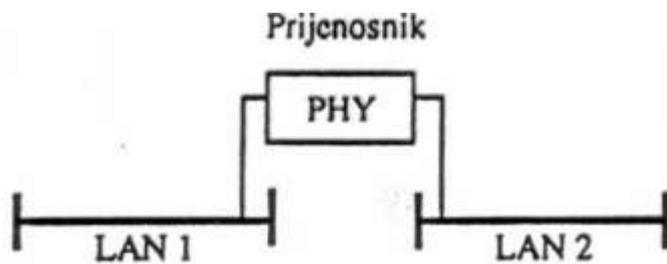
Okvir se prvo prime i sprema, a zatim proslijede drugom LAN-u ovisno od odluke o isporuci okvira. Zapravo se okviri "filtriraju" kroz most: svrha je tog filtriranja da se onemogući isporuka okvira za koje znano da im je odredište u izvornome LAN-u. Tako se lokalni pomet zadržava u LAN-u iz kojeg je potekao, a samo ne-lokalni promet se prosljeđuje. Iako su dva LAN-a povezana na razini okvira, oni ne dijele međusobno lokalne promete već samo među-promet.

Most obavlja 3 osnovne funkcije:

- filtriranje (*filtering*) okvira na osnovi odredišne adrese upisane u okviru,
- prosljeđivanje (*forwarding*) okvira iz jednoga u drugi LAN brzinom koja je jednaka brzini u drugome LAN-u,
- učenje (*learning*) topologije LAN-a na temelju izvorišnih adresa upisanih u primljene okvire.

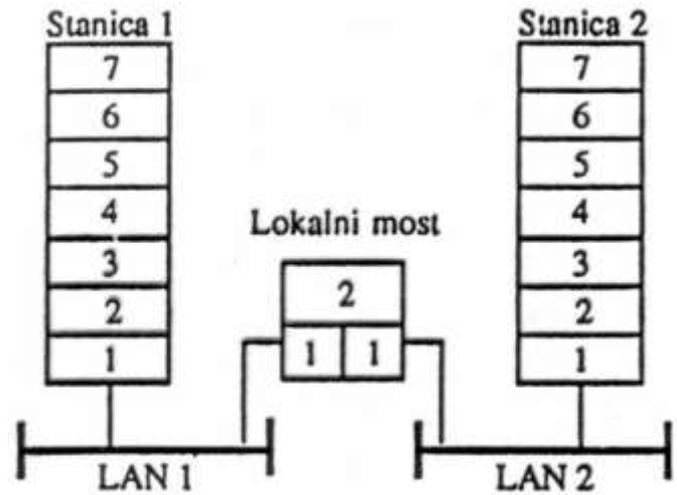
Prijenosnik (*repeater*)

Suprotno se postiže prijenosnikom, gdje su dva LAN-a također povezana na razini okvira (fizikalni sloj), ali svakim LAN-om prolazi i promet drugoga tako da učinkovitost svakog LAN-a može biti smanjena (slika 6.a). To ima za posljedicu i smanjenje sigurnosti. Treba također istaknuti da most djeluje na principu „spremi i proslijedi“ (dakle, nema komutacije paketa, ali nema konverzije protokola niti modificiranja formata ili sadržaja okvira pa se zato može koristiti za proširenje LAN-a na udaljenosti koje su veće od granica koje se mogu dostići uporabom prijenosnika.



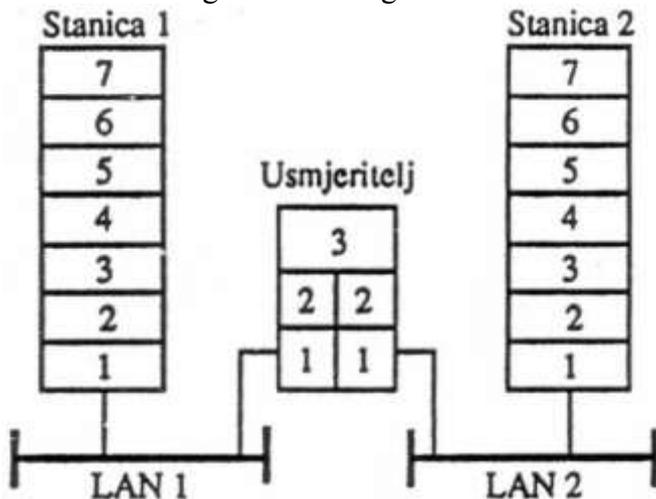
(a) prijenosnik (*repeater*)

Prosljeđuje se međusobno sav promet što smanjuje učinkovitost i sigurnost svakog LAN-a.



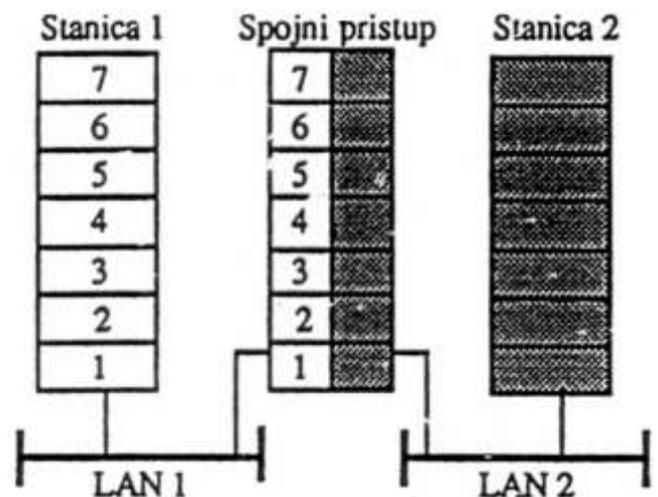
(b) Lokalni most (*bridge*)

Nema obrade protokola. Vrlo brzo prosljeđuje. Za LAN-ove iste vrste čita sve, interpretira samo adrese. Prosljeđuje se samo ne-lokalni promet principom „spremi i prosljedi“ (bez konverzije protokola - OSI slojevi moraju jednaki od 3. do 7. sloja na krajnjim stanicama.



(c) Usmjeritelj (*router*)

Sporiji od mosta, jer obrađuje drugi i treći sloj protokola. Omogućuje konverziju LAN i WAN protokola.



(d) Spojni pristup (*gateway*)

Povezuje mrežu potpuno neovisnim protokolnim složajima, kontrola prometa i umjeravanje.

Slika 6. Osnovni elementi za umrežavanje lokalnih mreža

Most djeluje velikom brzinom, jer nije potrebna obrada protokola (samo treba obaviti jednostavne odluke o usmjeravanju i prosljeđivanju okvira što se može obaviti vrlo brzo); npr. tipična brzina je 25000 paketa/s. Uobičajeni mostovi imaju dva priključka (porta), ali postoje i oni s više priključaka.

Sumarno, vidi se da je most vrlo brz u djelovanju, transparentan je s višim slojevima, za izolira lokalni promet i može se koristiti za proširenje veličine LAN-a. Lokalizacija prometa osigurava viši stupanj sigurnosti.

Usmjeritelj (*router*)

Na slici 6(c) je prikazan usmjeritelj koji prima okvire od jednoga LAN-a procesira ih sve do trećeg sloja, a zatim ih prosljeđuje funkcijama trećeg (mrežnog) sloja drugog LAN-a. Oni zatim odlaze prema nižim slojevima sve do konačnog odašiljanja. To traje znatno vrijeme pa zato usmjeritelj radi mnogo sporije od mosta.

Usmjeritelj obrađuje i drugi i treći sloj protokola i često je jedino moguće rješenje za umrežavanje lokalnih mreža. Na primjer, ako dva povezana LAN-a imaju različite formate okvira most nije u stanju riješiti tu nekompatibilnost. Ako takva dva LAN-a imaju zajednički sloj mrežnog protokola, tada se usmjerenjem može obaviti njihovo povezivanje.

Ukratko, usmjeritelji su sporiji od mostova, ovisе od mrežnog protokola (*internet Protocol IP*); najpoznatiji IP je DoD-IP koji je dio TCP/IP standarda, a i ISO definira OSI-IP protokol –ISO 8473 standard) i omogućuju konverziju LAN i WAN protokola. Usmjeritelji se danas u LAN-ovima sve češće zamjenjuju LAN komutatorima trećeg sloja koji se ne temelji na softverskoj nego na hardverskoj implementaciji prosljeđivanja paketa zbog čega je brzina rada tih komutatora znatno veća od brzine rada usmjeritelja.

Spojni put (*gateway*)

U slučaju dvije mreže djeluju s potpuno neovisnim protokolnim složajima (npr. ISO i SNA) ni most ni usmjeritelj se ne mogu upotrijebiti. Kako je prikazano na slici 6(d) spojni pristup implementira cijeli protokolni složaj za svaku mrežu te omogućuje željeno povezivanje na ekvivalentnom sedmom ISO sloju.

Očito je da su performanse spojnog pristupa lošije u usporedbi s mostom i usmjeriteljem.

23.2. Uporaba mostova kod povezivanja lokalnih mreža

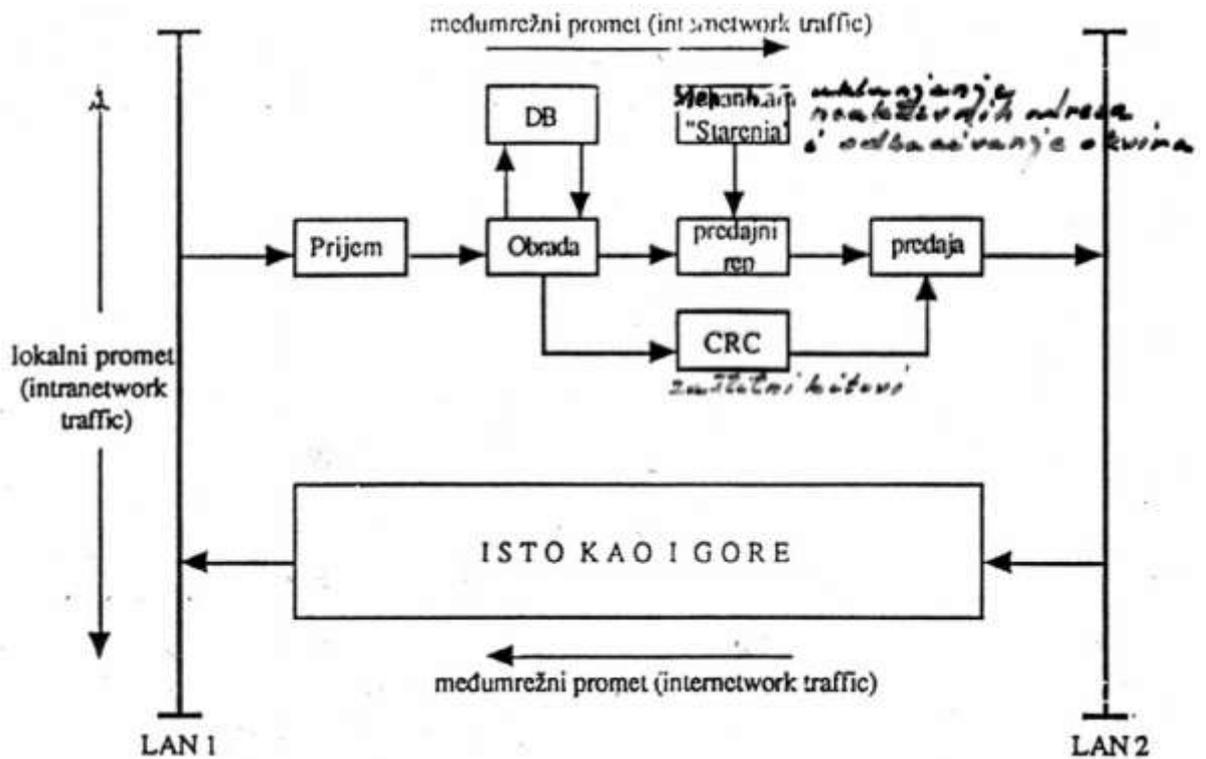
Vrste mostova su: lokalni i udaljeni.

Lokalni most

Na slici 7. prikazane su glavne funkcije mosta. On djeluje jednako s obzirom na oba LAN-a (simetrično). Okviri se primaju i prosljeđuju ovisno od rezultata usporedbe odredišne adrese u svakom okviru sa sadržajem filtarskog spremnika podataka. Most održava tu "bazu podataka" (DB) samoučenjem prisutnih adresa stanica u svakom LAN-u preko nadzora izvorišnog adresnog polja unutar okvira. Da bi se savladala mogućnost da se stanica pomiče između LAN-ova (tj. možemo ju isključiti ili preseliti na drugo mjesto u mreži), mehanizam starenja (*timer*) je potreban za uklanjanje adresa koje nisu aktivne unutar nekog vremena.

Uvijek je moguće do dođe do pogreške u okviru dok se on nalazi unutar mosta. Zato je važno da se zaštitni bitovi (CRC) u okviru ponovno ne izračunavaju u mostu, već se oni (CRC) izvlače iz pridošloga okvira te se ponovno koriste kad se okvir odašilje na izlazni LAN. Time se osigurava integritet podataka s kraja na kraj. Kada se donese odluka o daljnjem prosljeđivanju okvira, oni se prenose u transmisijski red čekanja, iz kojeg će se uzimati kad god je to moguće, te odašiljati prema izlaznom LAN-u. Okviri koji u mostu borave duže od dozvoljenog maksimuma, odbacuju se pomoću mehanizma starenja.

Sporiji mostovi mogu koristiti programsko pretraživanje i održavanje DB do se kod bržih mostova to obavlja sklopovski.



Slika 7. Glavne funkcije mosta

Udaljeni most

Lokalni most povezuje LAN-ove koji su na istoj fizičkoj lokaciji tj. most je „kutija“ s priključkom za svaki LAN. Udaljeni most omogućuje povezivanje LAN-ova na različitim lokacijama. Ovdje postoji efektivno pola mosta na svakoj lokaciji, a obje polovice su povezane nekim mehanizmom prijenosa podataka (npr. optičko vlakno, satelit itd.). Konceptualno takav most može biti izrađen „prijelomom“ lokalnog mosta i uporabom podatkovne veze, po mogućnosti s protokolom na razini veze (DLL), između tih polovica. Zato govorimo o polu-mostu ili udaljenom mostu na svakoj lokaciji. Uporabom brzog prijenosa podataka na vezi između udaljenih mostova omogućuje se i velika brzina između LAN-ova pa ta vrsta most ima veliki značaj (LAN-WAN-LAN) Vremenska kašnjenja prisutna kod rada udaljenog mosta kompliciraju mehanizme starenja i stavljanja okvira u transmisijski red čekanja

23.3. Upotreba usmjeritelja

Usmjeritelj (*router*) djeluje na trećem (mrežnom ili IP sloju) OSI modela. Veća inteligencija prisutna u usmjeritelju omogućuje mu kontrolu prometa i usmjeravanja. Uz vrlo profinjene tehnike pretraživanja tablica usmjeravanja, usmjeritelj određuje optimalne staze (rute) kroz mrežu. Time se može ravnomjerno prometno opteretiti višestruke staze između izvorišnih i odredišnih LAN-ova, tj. bitno se mogu umanjiti moguća zagušenja u mreži. Tijekom eventualnih zagušenja, za razliku od mosta, usmjeritelj može i obnoviti okvire tako da ne dođe do njihovog prekomjernog gubljenja.

Usmjeritelj paralelno obavlja dvije osnovne funkcije:

- Prosljeđivanje paketa iz jedne u drugu mrežu na osnovi odredišne adrese (npr. IP adrese) u zaglavlju paketa i tablice rutera.;
- Proračunavanje rute transfera paketa pomoću algoritma usmjeravanja, koristeći protokole: „Routing Information Protocol“ i „Open Shortest Path First“ i adrese.

Obzirom na načine usmjeravanja prometa usmjeritelji se dijele na statičke i dinamičke. Statički koriste staze (rute) koje su unaprijed određene (tzv. fiksne staze) od npr. voditelja (menagera) mreže, dok dinamički određuju staze usmjeravanja na temelju „povijesti“ mrežnog prometa i ponašanja mreže odnosno usmjeravanja. U slučaju znatno zahtjevnijih ili ekstenzivnijih aktivnosti u WAN mreži

preporuča se potreba usmjeritelja s dinamičkim usmjeravanjem. Kod jednostavnijih umrežavanja, poput zvjezdolikih, svaki usmjeritelj održava svoju statičku tablicu usmjeravanja.

Najjednostavniji usmjeritelji podržavaju samo jedan protokol. Oni s većim brojem protokola većim brojem priključaka (portova), dakako, češće se koriste. Uz RISC procesore postižu se brzine na unutarnjoj sabirnici od 800 Mbit/s, što omogućuje povezivanje na višim stupnjevima vremenskog multipleksa (npr. iznajmljenim kanalom) kao i s MAN mrežom (npr. FDDI).

Pogledajmo sada još malo rad algoritma dinamičkoga usmjeravanja. Usmjeritelji moraju međusobno izmjenjivati informacije potrebne za ažuriranje tablica usmjeravanja, tj. oni moraju moći razdvojiti pakete s takvim informacijama. Većina usmjeritelja koristi RIP (*Routing Information Protocol*) algoritam koji izračunava distancu između mjeritelja i odredišta izraženu najmanjim brojem grana („hop“-ova). Pri tome RIP ignorira ostale attribute staze usmjeravanja poput kapaciteta svake grane (bit/s) i stvarne duljine pojedine grane (km). Posljedica je da stvarno odabrana staza nije i najbolja. Osim toga, uporabom RIP protokola unosi se u mrežu određena redundancija. Na primjer, svaki usmjeritelj mora slati kopiju svoje tablice do svakog susjednog usmjeritelja približno svakih 30 s. U velikim mrežama, primjerice, sastavljenim od grana kapaciteta do 64 kbit/s to dodatno prometno opterećenje može znatno smanjiti propusnost i druge performanse mreže.

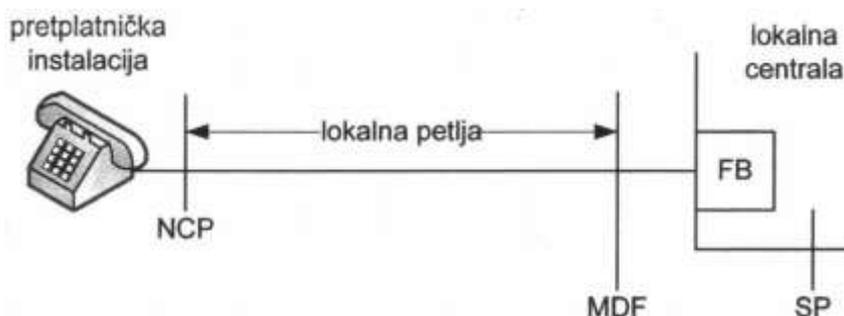
Da bi izbjegli dodano opterećenje mreže takvim "jalovim" prometom možemo se poslužiti jednom od sljedećih metoda. Prva je da se rjeđe ažuriraju tablice usmjeravanja. To, međutim, povećava vrijeme odziva (reakcije) usmjeritelja u slučaju kvarova ili pojave zagušenja: Druga se metoda svodi na slanje kopija tablica usmjeravanja samo kad dođe do promjene stanja grane. Novi standard nazvan OSPF (*Open Shortest Path First*) obuhvaća drugu metodu. Uz dodatnu logiku, u slučaju kvara ili zagušenja, usmjeritelj može bilo odbaciti pakete ili još bolje, informirati izvorište da uspori slanje paketa (treći i četvrti slojevi OSI modela su zadušeni za kontrolu toka i kontrolu zagušenja najčešće uporabom klizećih prozora, kontrolom brzine generiranja bitova ili kombinacijom ovih postupaka).

Navedimo samo da paketi u pojedinim pod-mrežama mogu imati različite veličine (npr. najveće duljine paketa u Ethernet i X.25 WAN mreži su različite).

Danas su mostovi zamijenjeni LAN komutatorima drugog sloja (*Layer 2 Switch*) u kojem su za razliku od mosta, funkcije mosta implementirane hardverski. LAN komutator obavlja istu funkciju kao i most s većim brojem priključaka (*multiport bridge*). Danas sve vrste lokalnih mreža rabe komutiranu mrežnu arhitekturu. Osnova komutiranja → tablica komutiranja (MAC adresa i broj izlaznog priključka).

24. PRISTUPNE MREŽE

Pojednostavljeno rečeno, pristupna mreža se sastoji od lokalnih petlji, za koje se ponekad rabi i naziv pretplatničke linije (*subscriber lines*), te od pridružene im mrežne opreme. Pristupna mreža krajnjim korisnicima omogućava povezivanje s jezgrenom mrežom preko koje pristupaju raznim uslugama. Lokalne petlje povezuju lokacije krajnjih korisnika usluge s lokalnim centralama (Slika 5-1).



Legenda:

Točka priključenja na mrežu, NCP (*Network Connection Point*)

Glavni razdjelnik, MDF (*Main Distribution Frame*)

Komutacijska točka, SP (*Switching Point*)
Sklop za napajanje linije, FB (*Feeder Bridge*)

Slika 5-1: Lokalna petlja kao linija za pristup PSTN-u

U svijetu je instalirano više od milijarde fiksnih pristupnih linija. Osim putem fiksnih linija, danas se jezgrenoj mreži sve češće pristupa i kroz pokretne mreže. Tradicionalna pristupna mreža sastoji se, uglavnom, od kabela s neoklopljenim upredenim paricama, UTP (*Unshielded Twisted Pair*). Proračun iz 2000. godine, koji je izradila tvrtka *Paradyne*, pokazuje da diljem svijeta približno 700 milijuna paričnih pretplatničkih linija povezuje rezidencijalne i poslovne korisnike s javnom komutiranom telefonskom mrežom, PSTN (*Public Switched Telephone Network*). Više od 95% takvih lokalnih petlji sastoji se od jedne upredene parice koja podržava tradicionalnu fiksnu analognu govornu telefonsku uslugu, POTS (*Plain Old Telephone Service*).

24.1. Širokopoljasni pristup

Razvojem Interneta i protokola TCP/IP pojavila se i rastuća potreba za korištenjem drugih usluga u pristupnom dijelu mreže osim tradicionalnog POTS-a. Paralelno s razvojem Interneta tijekom devedesetih godina prošlog stoljeća razvijen je i koncept širokopoljasne digitalne mreže integriranih usluga, B-ISDN (*Broadband Integrated Services Digital Network*). Granica između uskopojasne (*narrowband*) i širokopoljasne komunikacije postavljena je na 2 Mbit/s (u SAD-u na 1,5 Mbit/s), tj. na brzinu veću od brzine primarnog pristupa ISDN-u (PRA). Međutim, naknadno je ta granica pomaknuta prema nižim brzinama, tj. na 144 kbit/s koliko iznosi podatkovna brzina osnovnog pristupa ISDN-u (BRA).

Na samom početku 21. stoljeća širokopoljasni pristup Internetu (*Broadband Internet Access*) postao je jedna od ključnih smjernica suvremenih telekomunikacija. Širokopoljasni pristup Internetu nije više isključivo mjera tehnološke razvijenosti nekog društva, već govori i o njegovom razvoju u cjelini. Zemlje članice Ujedinjenih naroda (UN) donijele su na skupovima "*World Summit on the Information Society*" (WSIS), održanima u prosincu 2003. godine u Ženevi i u studenome 2005. godine u Tunisu, zaključke koji predstavljaju ključnu podlogu za dokumente o razvoju informatičkog društva. Održavanje skupova WSIS (www.wsis.org) podržala je Generalna skupština UN-a rezolucijom u prosincu 2001. godine, a prvome skupu su nazočili predstavnici 175 zemalja članica LTN-a, među kojima i predstavnici Republike Hrvatske. Na tom su skupu sudionici zajednički donijeli dva važna dokumenta: deklaraciju nazvanu "*Declaration of Principles*" i akcijski plan "*Plan of Action*". Drugi skup WSIS, na kojem su nazočili predstavnici 174 zemlje članice UN-a (uključujući i predstavnike Republike Hrvatske), održan je kako bi se pokrenuo plan djelovanja donesen u Ženevi, a na njemu su kreirana dva važna dokumenta: "*Tunis Commitment*" i "*Tunis Agenda for the Information Society*". U tim je dokumentima, između ostalog, prikazana i vizija izgradnje informacijskog društva koje će biti usmjereno na čovjeka, inkluzivno i razvojno orijentirano, te će svakome omogućiti kreiranje, pristup, korištenje i dijeljenje informacija i znanja. Upravo riječ pristup u navedenoj viziji opravdava sve napore koji se poduzimaju u području širokopoljasnog pristupa Internetu.

U novije se vrijeme sve češće rabi i termin indeks digitalnog pristupa, DAI (*Digital Access Index*) koji odražava mogućnosti pojedinaca u određenim državama da pristupaju informacijskim i komunikacijskim tehnologijama (ICT). Tu je mjeru definirao ITU, a obuhvaća 178 zemalja. DAI se kreće u granicama između 0 i 1. Prema podacima za 2002. godinu, najveći DAI imala je Švedska (0,85), dok je DAI Hrvatske iznosio 0,59, čime je svrstana u zemlje s višom razinom pristupa ICT u. Nemogućnost pristupa ICT u stvara tzv. digitalni jaz (*digital divide*) između država, kao i između pojedinih regija unutar država. Stoga je prigodom realizacije širokopoljasnog pristupa Internetu posebno važno obratiti pozornost na ruralna područja u kojima je, diljem svijeta, razvijenost telekomunikacija na osjetno nižoj razini negoli u gradskim i prigradskim područjima. Za razvoj ruralnih telekomunikacija veliku odgovornost snosi upravo država koja, poreznom politikom i zakonskom regulativom, treba telekomunikacijskim operatorima stimulirati investiranje u ruralne mreže, kao sektor s tradicionalno dugotrajnim povratom uloženog kapitala (*Return on Investment*,

ROI). Slijedi sažet prikaz tehnologija koje se danas najčešće rabe za realizaciju širokopojasnog pristupa [14].

24.2. Digitalne pretplatničke linije

U vrijeme kad su se na tržištu pojavile tehnologije digitalne pretplatničke linije, DSL (*Digital Subscriber Line*) [13] alternativni oblici pristupa jezgrenoj mreži bili su sljedeći:

- pristup POTS kanalima s pomoću modema (*voice-band* modem, dial-up modem)
 - prijenosne brzine 33.600 bit/s ili najviše 56 kbit/s u smjeru prema korisniku;
- pristup uskopojasnim ISDN-om (N-ISDN)
 - osnovni pristup (BRA) - prijenosna brzina 160 kbit/s, podatkovna brzina (na raspolaganju korisniku) 144 kbit/s
 - primarni pristup (PRA) - prijenosna brzina 2,048 Mbit/s, podatkovna brzina 1,984 Mbit/s;
- pristup mrežom kableske televizije s pomoću kabelskih modema i
- pristup prijenosnim E1-sustavima - prijenosna brzina 2,048 Mbit/s.

Pristup POTS kanalima, BRA-om i kabelskim modemima uglavnom je bio namijenjen kućnim korisnicima, a PRA i E1 sustavi poslovnim korisnicima. U devedesetim godinama prošlog stoljeća započeo je ubrzani masovni razvoj i primjena xDSL-a diljem svijeta (generički naziv xDSL često se rabi kako bi se njime označile sve DSL tehnologije). Standardizacijom xDSL-a na svjetskoj razini bavi se organizacija ITU-T, a osim nje standarde donose i ETSI te ANSI. Za promociju tehnologije brine se organizacija DSL Forum.

Osnovna podjela DSL tehnologija je na asimetrične i simetrične (Tablica 5-1), pri čemu se simetričnost odnosi na prijenosne brzine u dolaznom i odlaznom smjeru prijenosa signala. Dolazni smjer (*downstream* ili *downlink*) je smjer od lokalne centrale prema korisničkom području, dok se suprotan smjer prijenosa naziva odlazni smjer (*upstream* ili *uplink*). Ako su brzine u oba smjera međusobno jednake, riječ je o simetričnoj DSL tehnologiji. U suprotnome se radi o asimetričnoj DSL tehnologiji.

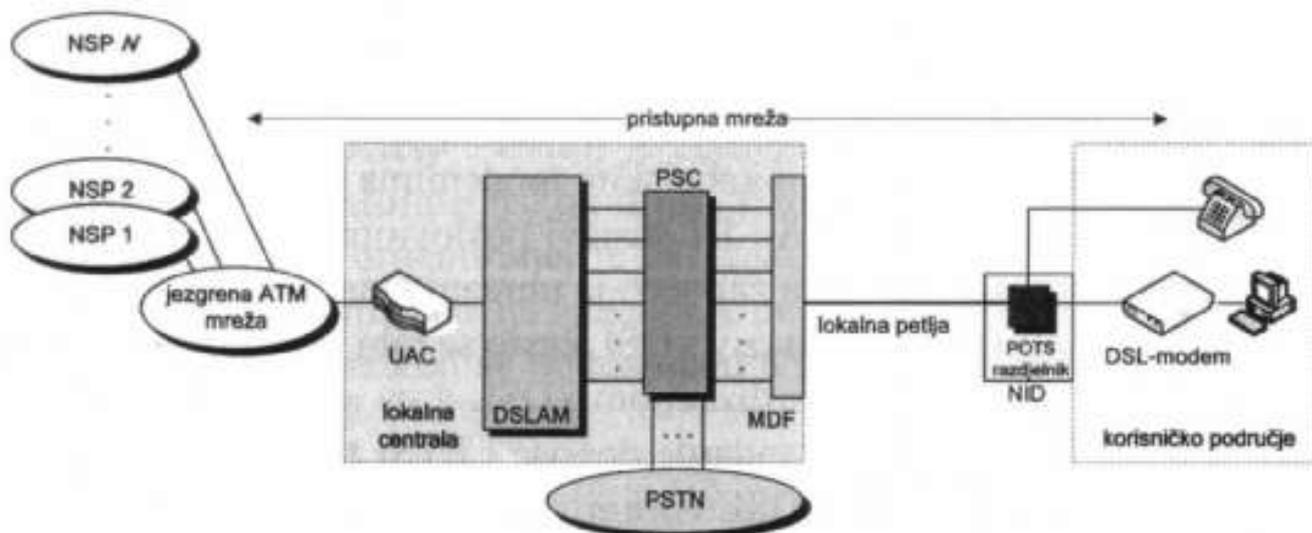
Tablica 5-1: Simetrične i asimetrične DSL-tehnologije

Asimetrične DSL tehnologije	Simetrične DSL tehnologije
ADSL (G.dmt), ADSL over ISDN, G.lite, RADSL	IDSL - ISDN over DSL
ADSL2 (G.dmt.bis), half-rate ADSL2 (G.lite.bis), ADSL2plus, RE-ADSL2	HDSL, HDSL2
VDSL, VDSL2	SDSL (npr. M/SDSL), SHDSL, ESHDSL

Asimetrične su tehnologije bolje standardizirane preporukama ITU-T a, dok je od simetričnih tehnologija ITU-T standardizirao HDSL i SHDSL. Upravo pod generičkim nazivom SDSL (*Symmetric DSL*) kriju se brojne proizvođačke inačice xDSL-a.

24.2.1. Arhitektura DSL sustava

Slika 5-1 prikazuje osnovnu konfiguraciju DSL-a [8]. POTS razdjelnik (POTS *splitter*) u dolaznom smjeru odvaja POTS promet od DSL prometa i integriran je u mrežno sučelje, NID (*Network Interface Device*). Ponekad se na korisničkom području umjesto razdjelnika rabe mikro-filtri (*micro filters*) ili mikro-razdjelnici (*micro splitters*). Prednost obaju navedenih uređaja je u tome što ih krajnji korisnik može samostalno instalirati.



Slika 5-1: Osnovna konfiguracija DSL-a s podrškom za POTS

Na drugom kraju DSL poveznice (link), tj. u lokalnoj centrali, lokalna je petlja ožičena na glavni razdjelnik (MDF) koji povezuje krajnje DSL korisnike izravno s pristupnim DSL multipleksorom, DSLAM (*Digital Subscriber Line Access Multiplexer*), odnosno s modemskim DSL karticama ugrađenima u DSLAM. Najnovija generacija DSLAM-ova ima ugrađenu funkcionalnost mrežnog sloja utemeljenu na protokolu IP. Zbog toga se takvi DSLAM-ovi nazivaju i IP/DSL komutatori (*IP/DSL Switches*). Kad se POTS prometni tokovi prenose zajedno s podatkovnim prometnim tokovima istim lokalnim petljama (takav se koncept pristupa naziva i *DSL over POTS*), POTS promet i podatkovni promet se u lokalnoj centrali frekvencijski razdvajaju s pomoću višestrukog POTS razdjelnika, PSC (*POTS splitter Chassis*).

DSLAM multipleksira DSL promet koji potječe od mnogobrojnih krajnjih DSL korisnika na brzu jezgrena ATM mrežu (ATM je skraćenica od engleskog pojma *Asynchronous Transfer Mode*, što u prijevodu znači asinkroni način prijenosa) putem tzv. univerzalnog pristupnog koncentratora, UAC (*Universal Access Concentrator*) smještenog u lokalnoj centrali. Osim DSL prometa, UAC može, također, koncentrirati i ostale vrste prometa. UAC odabire davatelja mrežne usluge, NSP (*Network Service Provider*), kojemu je potrebno proslijediti podatke krajnjih korisnika, te zatim usmjerava ili komutira podatke prema brzom spojnomo vodu (*trunk*) - prema odabranom NSP-u.

Trenutačno su za rezidencijalne i manje poslovne korisnike najatraktivnije sljedeće DSL tehnologije: ADSL2, ADSL2+, VDSL i VDSL2. Slijedi njihov detaljniji opis.

24.2.2. ADSL2

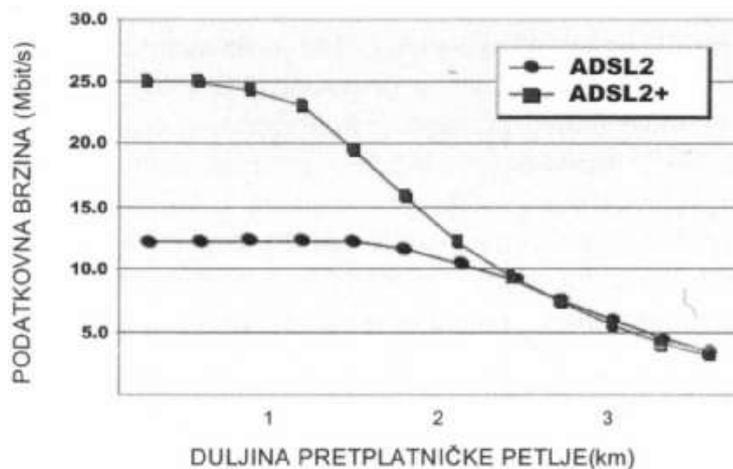
ADSL2 je posebno dizajniran radi poboljšanja brzine i dometa prijenosa u odnosu na izvornu inačicu ADSL-a, a ima i bolje performanse na dugačkim linijama u prisutnosti uskopojasnih smetnji. ADSL2 omogućava postizanje dolaznih brzina do otprilike 12 Mbit/s i odlaznih brzina do 1 Mbit/s (Slika 5-2), ovisno o duljini lokalne petlje i drugim relevantnim čimbenicima. Takvo znatno povećanje prijenosne brzine u dolaznom smjeru posljedica je toga što ADSL2 postiže bolju učinkovitost korištenog modulacijskog postupka.

Glavne prednosti ADSL2 pred izvornom inačicom ADSL-a sadržane su u sljedećem:

Dijagnostika - u odnosu na izvornu inačicu ADSL-a, ADSL2 primopredajnici su poboljšani dodavanjem opsežnih dijagnostičkih mogućnosti. Spomenute mogućnosti temelje se na softverskim alatima za rješavanje problema tijekom i nakon završetka instalacije, za nadziranje performansi sustava tijekom rada te za utvrđivanje potrebe za nadogradnjom sustava.

Poboljšanja glede potrošnje električne energije - prva generacija ADSL primopredajnika je danonočno rabila određenu fiksnu snagu napajanja električnom energijom, čak i kad nisu aktivno prenosili korisničke podatke. Imajući u vidu milijune instaliranih ADSL modema diljem svijeta, moguće je

uštedjeti znatnu količinu električne energije ako bi ti modemi za vrijeme neaktivnih perioda mogli prijeći u tzv. pričuveno (*stand-by*) stanje poput, npr., osobnih računala. Kako bi odgovorio na taj problem, standard tehnologije ADSL2 definira dva načina upravljanja potrošnjom električne energije koji omogućavaju smanjenje potrošnje uz istodobno očuvanje funkcionalnosti stalne prosjojenosti krajnjih korisnika ADSL-a.



Slika 5-1: Prijenosne brzine ostvarene s pomoću ADSL2+ (izvor: DSL Forum, 2003.) ; kružići na grafu odnose se na ADSL2, a kvadratići na ADSL2+

Prilagodba prijenosne brzine - nepovoljne promjene razina preslušavanja u kabelskoj grupi mogu dovesti do ispada nekog ADSL sustava iz rada. Preslušavanja (štetni prijenos energije s jedne parice na drugu) su samo jedan od razloga zbog kojeg neki ADSL sustav može prekinuti komunikacijske veze koje su njime ostvarene. Drugi razlozi uključuju izvore radijskog ometanja u AM-području frekvencija (*Amplitude Modulation*, AM - amplitudna modulacija), temperaturne promjene i prodor vlage u kabelsku grupu. ADSL2 odgovara na te probleme kontinuiranom prilagodbom prijenosne brzine u stvarnom vremenu, SRA (*Seamless Real-time Data Rate Adaptation*). SRA omogućava ADSL2 sustavima da mijenjaju prijenosnu brzinu i za vrijeme rada, i to bez prekidanja prijenosa.

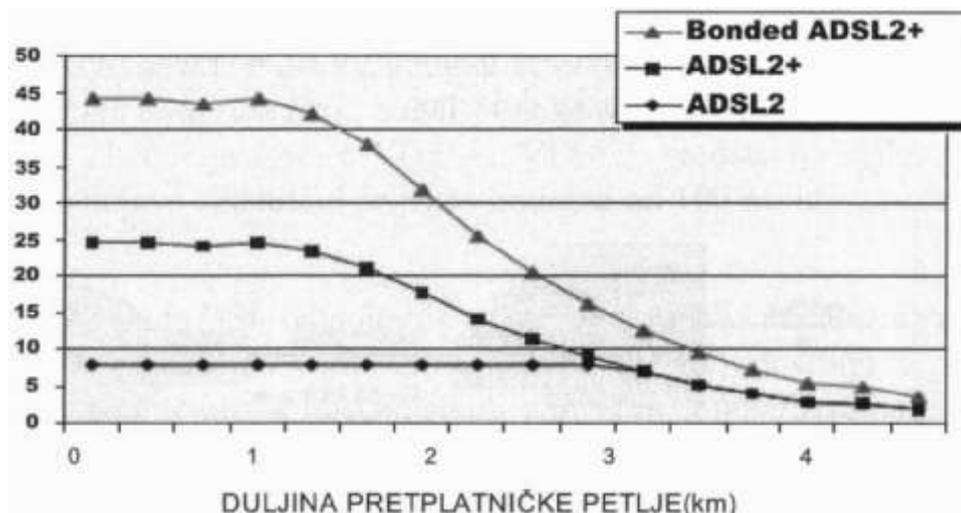
Usnopljavanje linija (*line bonding*) - zahtjev koji je zajednički svim operatorima je mogućnost da raznim krajnjim korisnicima mogu pružati različite razine usluge. Prijenosne brzine prema kućnim i poslovnim korisnicima moguće je znatno povećati tzv. usnopljavanjem linija. Kako bi podržao usnopljavanje linija, ADSL2 standard definira uporabu inverznog ATM multipleksiranja, IMA (*Inverse Multiplexing for ATM*) koji je standardizirao ATM Forum. Pomoću koncepta IMA, ADSL2 podržava usnopljavanje do najviše 32 upredene parice u jednu ADSL2 poveznicu. Rezultat usnopljavanja linija su veće prijenosne brzine, što dovodi i do povećanja broja krajnjih korisnika kojima je moguće ponuditi takvu uslugu (povećava se pokrivenost uslugom).

ADSL2 pruža dodatna poboljšanja u odnosu na izvornu inačicu ADSL-a:

- poboljšana međusobna operabilnost između primopredajnika različitih proizvođača;
- brza uspostava poveznice - skraćeno trajanje inicijalizacije poveznice s 10 sekundi na manje od tri sekunde;
- podrška paketskim uslugama - u ADSL2 je ugrađen i sloj skraćeno nazvan PMT TC (*Packet Mode Transmission Trans-Convergence*) koji podržava usluge poput, npr. prijenosa Ethernet okvira.

24.2.3. ADSL2plus

Za razliku od prvih dvaju članova skupine ADSL standarda, koji specificiraju korištenje dolaznog kanala do gornje granične frekvencije od 1,1 MHz, gornja granična frekvencija dolaznog kanala u ADSL2plus postavljena je na 2,2 MHz. Rezultat toga je znatno povećanje dolaznih prijenosnih brzina na lokalnim petljama kraćima od otprilike 1500 m (Slika 5-3). Odlazna prijenosna brzina seže do 1 Mbit/s. Naravno, obje brzine ovise o uvjetima u lokalnoj petlji. ADSL2plus je moguće iskoristiti i u svrhu smanjenja preslušavanja.



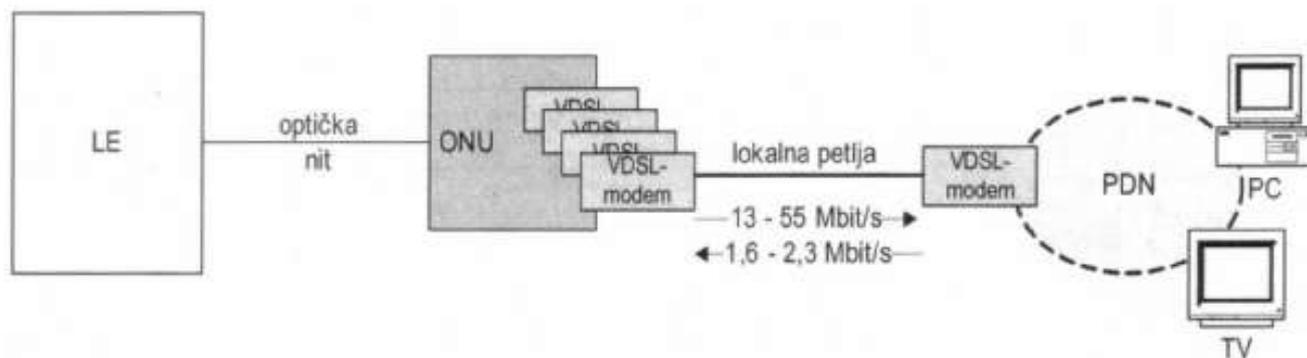
Slika 5-3: Prijenosne brzine i dometi prijena koje podržava ADSL2 (izvor: DSL Forum, 2003.); rombovi se odnosi na ADSL, kvadratići na ADSL2 realiziran jednom upredenom paricom, a trokutići na usnopljanje linija

24.2.4. VDSL

Već je neko vrijeme sasvim jasno da telekomunikacijski operatori diljem svijeta donose odluke (ili će ih donijeti uskoro) o uključivanju postojećih paričnih lokalnih petlji u svoje širokopojasne pristupne mreže sljedeće generacije. Obzirom da krajnji korisnici postaju sve zahtjevniji glede prijenosnih brzina, ADSL bi mogao, unatoč novijim inačicama ADSL2 i ADSL2+, iskazati slabe performanse u složenoj okolini u kojoj je potreban istodoban prijenos govorne telefonije, interaktivnog videa i brzih podatkovnih usluga na veće udaljenosti između krajnjih korisnika i lokalne centrale. U takvim mrežnim scenarijima, gdje operatori radije odabiru kao rješenje kombinaciju optičkih niti i upredenih parica, VDSL postaje dobar izbor.

VDSL je jedna od tehnologija koje omogućavaju ostvarenje koncepta FTTN (*Fiber to the Neighborhood*). Arhitekturu FTTN-a čini kombinacija optičkih niti, koje povezuju lokalnu centralu, LE (*Local Exchange*) s optičkim mrežnim jedinicama (*Optical Network Unit - ONU*), i upredenih parica koje povezuju krajnje korisnike s ONU-ima. VDSL-modemi su instalirani na oba kraja svake lokalne VDSL-petlje, realizirane jednom upredenom paricom. Slika 5-4 prikazuje arhitekturu FTTN-a, odnosno VDSL-a.

VDSL podržava simetričan i asimetričan prijenos. Koristi se frekvencijskim područjem do 12 MHz. Cijena koju VDSL plaća zbog povećanja brzine u odnosu na ADSL je smanjeni domet prijena (Tablica 5-2). Dolazne brzine podržane VDSL-om višekratnici su brzine od 155,52 Mbit/s, korištene u SDH-sustavima, odnosno SONET sustavima: 51,84 Mbit/s, 25,92 Mbit/s i 12,96 Mbit/s. Odlazne brzine podržane VDSL-om moguće je podijeliti u tri skupine: 1,6 - 2,3 Mbit/s, 19,2 Mbit/s i brzine koje su jednake dolaznoj.



Slika 5-4: Arhitektura FTTN-sustava i VDSL-a kao njegovog sastavnog dijela; PDN (*Premises Distribution Network*) - mreža korisničkog područja

Tablica 5-2: Prijenosne brzine podržane VDSL-om

Inačica VDSL-a	Domet (m)	Dolazna brzina (Mbit/s)	Odlazna brzina Mbit/s
asimetrična	900	26	3
asimetrična	300	52	6
simetrična	900	13	13
simetrična	300	26	26

24.2.5. VDSL2

Dana 27. svibnja 2005. godine objavljena je nova preporuka ITU-T a kojom je definirana druga inačica tehnologije VDSL, nazvana skraćeno VDSL2. VDSL2 je simetrična prijenosna usluga koja podržava prijenosnu brzinu od 100 Mbit/s u oba smjera. Proširenjem frekvencijskog pojasa VDSL2 sve do 30 MHz novi primopredajnici podržavaju simetrične brzine od 100 Mbit/s jednom upređenom paricom do udaljenosti veće od 350 metara. VDSL2 je, prije svega, specificiran kako bi podržao prijenos višekanalnog HDTV-a (*High Definition Television*), videa na zahtjev i videokonferencija te prijenos govora protokolom IP (VoIP). Dakle, VDSL2 predstavlja dobro rješenje za *triple play* usluge (integrirani prijenos podataka, govora i videa istom pretplatničkom petljom).

24.2.6. Usporedba DSL tehnologija

Digitalna pretplatnička linija velike prijenosne brzine, HDSL (*High Bit-rate DSL*) je bila prva DSL tehnologija koja je doživjela uspjeh na tržištu, asimetrična digitalna pretplatnička linija, ADSL (*ASymmetric DSL*) je doživjela najveći rast na tržištu, dok digitalna pretplatnička linija vrlo velike prijenosne brzine, VDSL (*Very High data rate DSL*) i dalje nudi najveće prijenosne brzine od svih DSL-a. Najnovija inačica VDSL-a, VDSL2, predstavlja najbržu DSL-tehnologiju i podržava simetrični prijenos brzinom od 100 Mbit/s uz domet od 300 metara.

Najbolji izbor glede DSL-tehnologija za glavninu malih i rezidencijalnih poslovnih korisnika, SOHO (*Small Office/Home Office*), posebno u gradovima i prigradskim područjima s postavljenom paričnom infrastrukturom, predstavlja ADSL: potpuno je standardiziran (što je iznimno važno operatorima, ali i korisnicima), njegova prijenosna brzina u oba smjera je zadovoljavajuća za pristup Internetu, podržava korištenje regeneratora (regeneratori omogućavaju produljenje dometa prijenosa), njegov maksimalan domet čini ga atraktivnim čak i u malim gradovima i selima gdje je postavljena odgovarajuća kabelska infrastruktura, te podržava istodoban prijenos POTS-a i ADSL podataka zajedničkom upređenom paricom. Tablica 5-3 donosi sažetu usporedbu DSL-tehnologija.

Tablica 5-3: Usporedba DSL tehnologija (izvor: Cisco)

xDSL	Standard?	Maksimalna dolazna brzina	Maksimalna odlazna brzina	Maksimalan domet	Regeneracij a signala?	Podrška POTS-u?
ISDN	Da	128 kbit/s	128 kbit/s	5486 m	Ne	Da
IDSL	Da	144 kbit/s	144 kbit/s	5486 m	Ne	Ne
HDSL	Ne	2,320 Mbit/s	2,320 Mbit/s	3658 m	Da	Ne
HDSL2	Da	1,544 Mbit/s	1,544 Mbit/s	3658 m	Da	Ne
SDSL	Ne	2,320 Mbit/s	2,320 Mbit/s	5486 m	Ne	Ne
SHDSL	Da	2,320 Mbit/s	2,320 Mbit/s	5486 m	Da	Ne
ADSL	Da	8 Mbit/s	640 kbit/s	5486 m	Da	Da
G.lite	Da	1,5 Mbit/s	512 kbit/s	5486 m	Da	Da
VDSL	Ne	56 Mbit/s	13 Mbit/s	1372 m	Planirano	Trenutačno ne

Posebno je važno istaknuti da su prijenosna brzina, ostvariva nekom DSL tehnologijom, i domet te tehnologije obrnuto proporcionalni: što je prijenosna brzina veća to je i domet ostvariv uz tu brzinu manji. Drugim riječima, nemoguće je nekom DSL tehnologijom istodobno ostvariti i maksimalnu

brzinu i maksimalan domet. Za implementaciju bilo koje inačice ADSL-a, a posebno ADSL2 i ADSL2+, važna je prosječna duljina pretplatničke petlje na nekom području. Što je ona manja, to je ostvariva brzina ADSL-om veća. U velikim gradovima u Hrvatskoj ta je duljina manja od 1 km, što omogućava implementaciju ADSL2 i ADSL2+ bez većih poteškoća i u kontekstu zahtjevnih usluga, poput *triple play* usluge (integrirani prijenos podataka, govora i videa istom pretplatničkom petljom).

Naravno, uvijek je potrebno voditi i računa da prigodom implementacije DSL tehnologija nad postojećom kabelskom infrastrukturom postoji problem dodjele DSL-a pojedinim paricama u zajedničkom kabelu koji povezuje centralu i krajnje korisnike. Nemoguće je svim paricama u nekom kabelu pridijeliti neku DSL tehnologiju jer bi u takvom scenariju međusobni štetni utjecaji (tzv. preslušavanja) između parica u kabelu bili preveliki i dodatno bi ograničili domet i kvalitetu prijenosa. Primjena statičkog ili dinamičkog upravljanja spektrom, tj. dodjelom prijenosnih sustava pojedinim paricama u zajedničkom kabelu, postala je nužnost, posebno u uvjetima izdvajanja lokalnih petlji, LLU (*Local Loop Unbundling*). U Republici Hrvatskoj LLU je propisan "Pravilnikom o pristupu izdvojenoj petlji", a sam proces izdvajanja petlji regulira Hrvatska agencija za telekomunikacije. Proglašeni operator (u Republici Hrvatskoj HT - Hrvatske telekomunikacije d.d.) je po Zakonu o telekomunikacijama obvezan pružati uslugu pristupa izdvojenoj petlji.

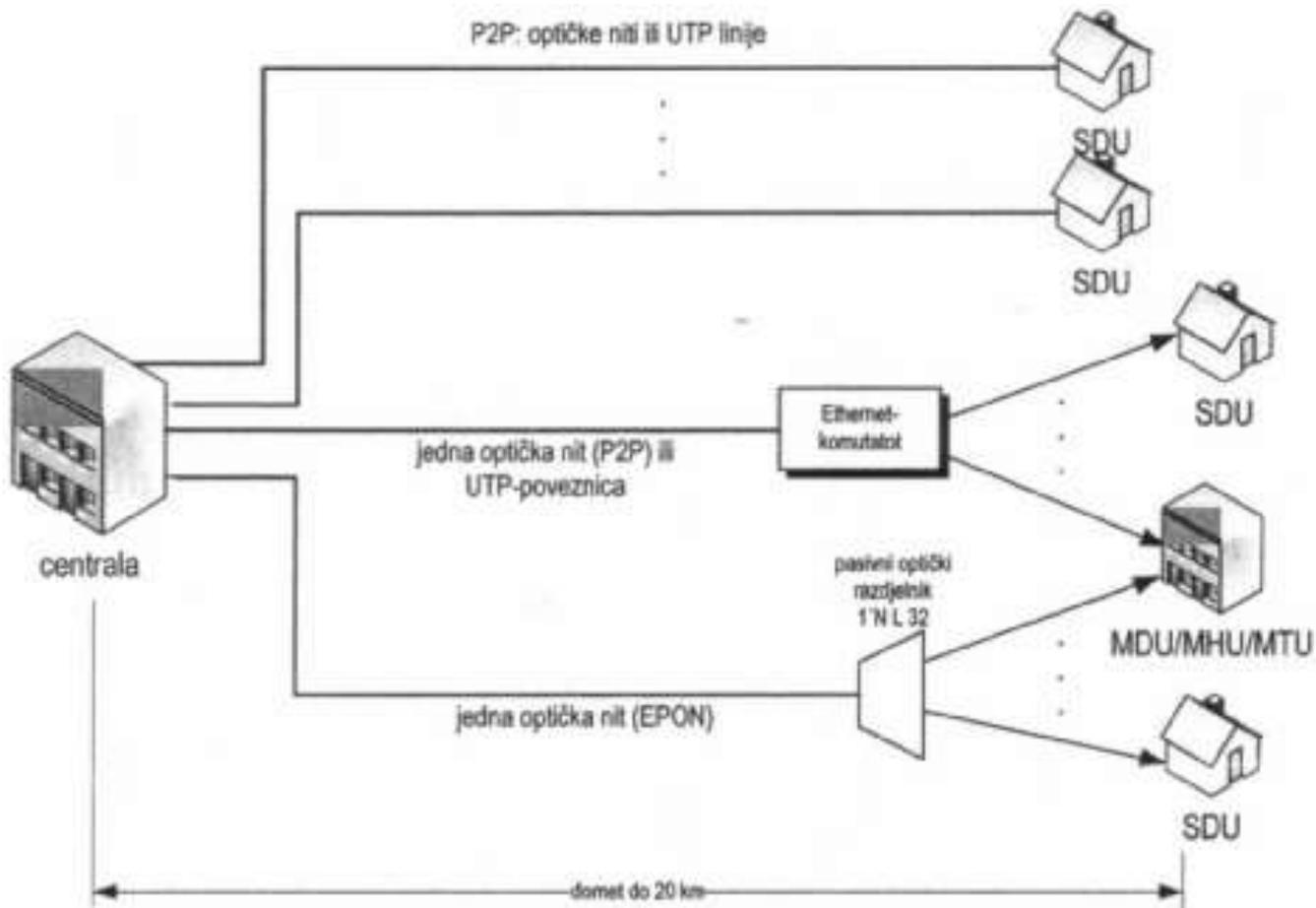
24.3. Primjena Etherneta u širokopojasnom pristupu

Pored stalnih promjena pristupnih mreža na fizičkom sloju, zbivaju se permanentne promjene i na višim slojevima, a posebno na drugom, tzv. sloju podatkovne poveznice. Većina pristupnih mreža bila je orijentirana na korištenje tehnologije ATM koja pokazuje iznimno dobra svojstva glede kvalitete usluge što je pruža višim protokolarnim slojevima. Međutim, nedovoljna učinkovitost ATM-a u situacijama kada se na mrežnom sloju rabi protokol IP, kao i složeni mehanizmi razošiljanja i slanja ćelija na veći broj krajnjih odredišta, doveli su do orijentacije dizajnera pristupnih mreža na protokol Ethernet koji se jednostavno integrira s IP-em. Stoga je razvijena cijela skupina pristupnih rješenja nazvana *Ethernet in the First (Last) Mile*, skraćeno nazvana EFM. Pored navedenog, korištenje Etherneta u pristupnoj mreži smanjuje broj potrebnih protokolnih konverzija s kraja na kraj mreže, što pridonosi smanjenju kašnjenja koje te konverzije uzrokuju te smanjenju troškova izgradnje mreže.

EFM pruža jedinstven pristup prijenosu Ethernet prometa trima različitim topologijama, pri čemu je svaka od njih pokrivena odgovarajućom inačicom EFM-a:

- mreže od točke do točke upredenim paricama - EFMC (*EFM Copper*)
 - prijenos Ethernet okvira upredenim paricama;
- optičke mreže od točke do točke - EFMF (*EFM Fiber*)
 - prijenos Ethernet okvira optičkim nitima od točke do točke i
- optičke mreže od točke prema većem broju točaka - EFMP (*EFMPON, EPON*)
 - prijenos Ethernet okvira pasivnom optičkom mrežom, PON (*Passive Optical Network*).

Definirana je i četvrta inačica, nazvana hibridni EFM, EFMH (*EFM Hybrid*). Operatori mogu kreirati EFMH topologije miješanjem EFMC-a, EFMF-a i EFMP-a. Slika 5-5 prikazuje različite topologije pristupne mreže koja kao pristupnu tehnologiju rabi EFM.



Legenda:

SDU (*Single Dwelling Unit*) - manji stambeni objekt

MDU (*Multiple Dwelling Unit*) - apartmani, domovi

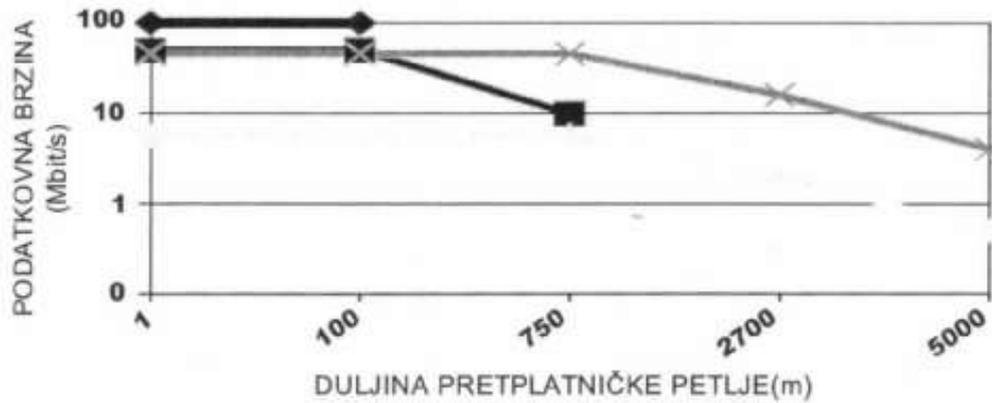
MTU (*Multiple Tenant Unit*) - uredske zgrade, poslovni kampusi

MHU (*Multiple Hospitality Unit*) - hoteli, bolnice, aerodromi i sl.

Slika 5-5: Arhitektura pristupne mreže utemeljene na EFM-u

EFMC je jednostavno i jeftino rješenje za pružanje brzog pristupa i usluga krajnjim korisnicima, a naročito je atraktivan rezidencijalnim i poslovnim korisnicima. Može koegzistirati s POTS-om, N-ISDN-om, ADSL-om i VDSL-om u zajedničkim paričnim kabelima, jer je spektralno usklađen s tim uslugama.

Odbor IEEE-a zadužen za EFM postavio je sljedeći cilj glede EFMC-a: ostvariti prijenosne brzine od barem 10 Mbit/s uz domet prijenosa od najmanje 750 metara, ili barem 2 Mbit/s uz domet prijenosa od najmanje 2.700 metara, oboje po postojećim neoklopljenim upredenim paricama. Odbor za standardizaciju EFM, a postavio je te ciljeve kao minimalne brzine, ali standard ne ograničava sustave na striktno korištenje tih brzina. Većina danas dostupnih EFMC sustava podržava osjetno veće brzine uz navedene domete. Odnos između prijenosnih brzina i dometa prikazuje Slika 5-6.



Slika 5-6: Odnos između prijenosnih brzina EFMC-a i dometa prijenosa (izvor: EFMA, 2004.); rombovi - standard 100BASE-TX, kvadratići - EFMC SR, trokutići - EFMC LR i križići - usnopljena EFMC-poveznica od 8 parica

Fizički sloj EFMC-a rabi u podlozi modulacijske tehnike xDSL-a (npr. VDSL ili SHDSL). ITU-T i ANSI su standardizirali proširenu inačicu nazvanu G.SHDSL.bis (ili *Extended SHDSL*, ESHDSL), a prihvatio ju je i IEEE-ov odbor za standardizaciju EFM-a. G.SHDSL.bis omogućava simetričan prijenos brzinom 5,7 Mbit/s.

Definirane su dvije vrste fizičkog sloja EFMC-a

- EFMC kratkog dometa (EFMC SR), skraćeno nazvan IOPASS-TS i
- EFMC dugog dometa (EFMC LR), skraćeno nazvan 2BASE-TL.

Pored navedenoga, EFMC podržava i usnopljanje linija (na sličan način kao i ADSL2, ali bez korištenja ATM-a). Ethernet, kao pristupna tehnologija, nudi znatne prednosti pred tradicionalnim (*legacy*) tehnologijama korištenima u prvoj miliji:

- jednostavan je, međunarodno prihvaćen standard koji će omogućiti međusobnu operabilnost sustava;
- pruža učinkovitu osnovu za prijenos *triple play* usluga;
- EFM-infrastruktura je skalabilna;
- EFM pruža jedinstveni protokol drugog sloja s kraja na kraj mreže i
- mrežni operatori mogu iskoristiti jedinstven pristup kreiranju različitih mrežnih arhitektura na svim razinama mreže: pristupnoj, gradskoj i temeljnoj.

Tradicionalna rješenja pristupa mreži, npr. xDSL i kabelski modemi, odgovarajuća su za tržišta s niskom razinom penetracije, i to u područjima gdje su korisnici raštrkani na većoj površini. Nasuprot tome, EFM je pristupno rješenje koje je prilagođeno zgradama s većim brojem poslovnih ili stambenih jedinica s velikim brojem i gustoćom krajnjih korisnika. I dok je većina drugih pristupnih rješenja usmjerena na pokrivanje uslugom, EFM je fokusiran na penetraciju.

24.4. Tehnologije širokopolasnog pristupa

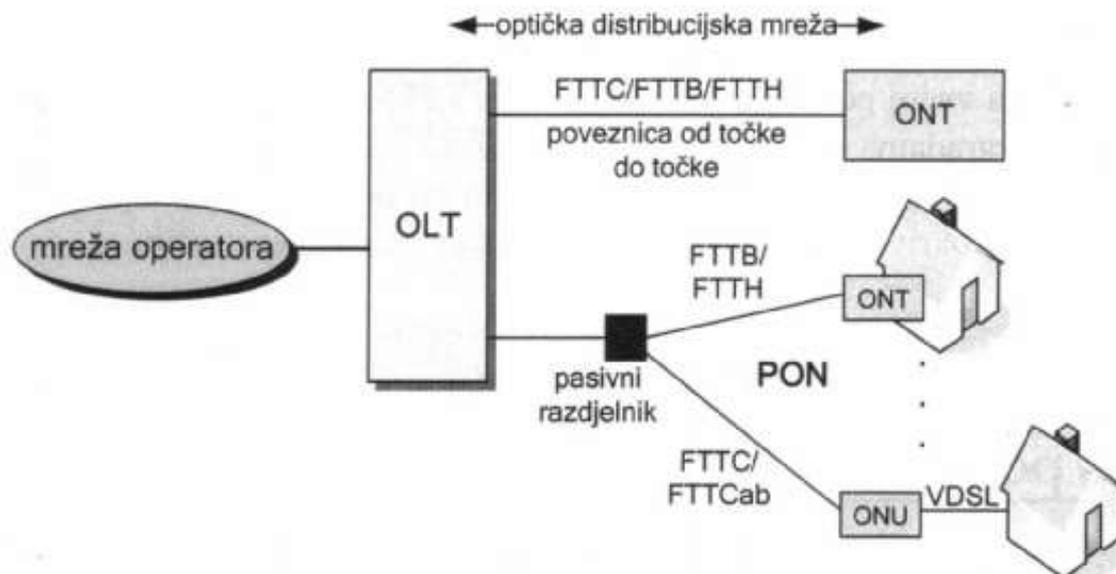
Optički pristup moguće je realizirati optičkim nitima i bežično. Ako se radi o pristupu pomoću optičkih niti, tada govorimo o konceptima, FTTx (*Fiber to the x*):

- optičke niti do stana, FTTH (*Fiber to the Home*),
- optičke niti do zgrade, FTTB (*Fiber to the Building*),
- optičke niti do pločnika, FTTC (*Fiber to the Curb*) ili, FTTK (*Fiber to the Kerb*⁸),
- optičke niti do kabineta, FTTCab (*Fiber to the Cabinet*).

Pristup optičkim nitima (FTTx tehnologije) je oduvijek predstavljao najkvalitetniju varijantu širokopolasnog pristupa jer omogućava postizanje velikih prijenosnih brzina i dometa prijenosa. Jedina prepreka masovnijem uvođenju FTTx tehnologija su njihova cijena i regulatorni uvjeti u većini zemalja koji zahtijevaju opsežne i skupe zahvate u kabelskoj infrastrukturi i samim time dodatno

⁸ Provjeriti ovu riječ (engleski)????????????

pridonose povećanju troškova realizacije pristupne mreže, što se, pak, dugoročno odražava i na cijenu usluga. Slika 5-7 prikazuje arhitekturu FTTx sustava.



Slika 5-7: Arhitektura FTTx-sustava

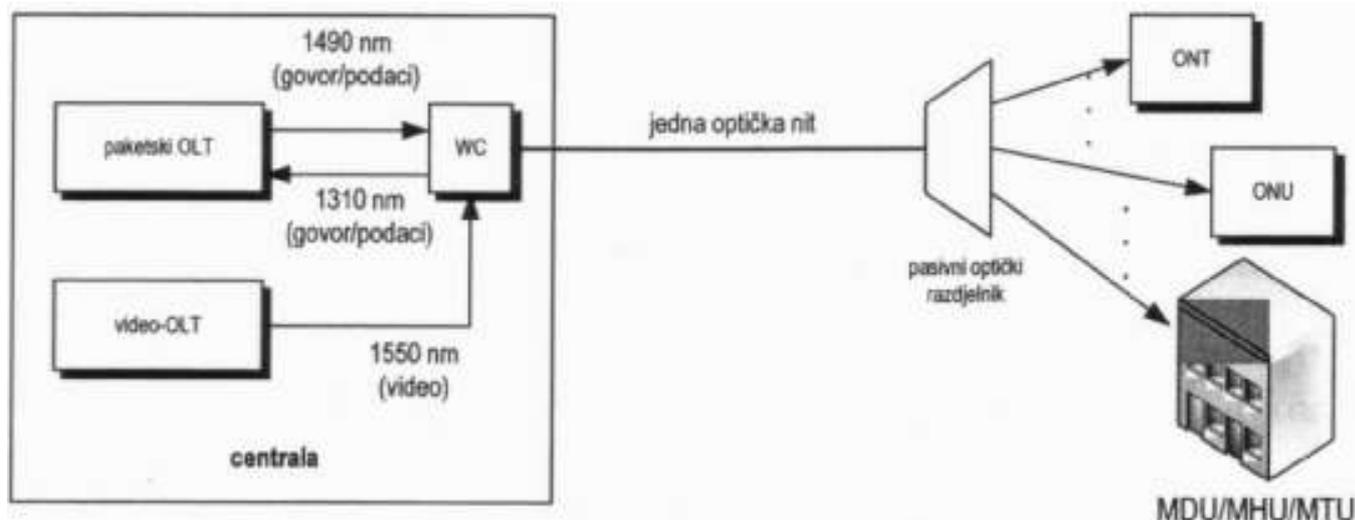
U sustavima FTTH i FTTB optički linijski terminal, OLT (*Optical Line Terminal*) povezan je pomoću optičkih niti s optičkim mrežnim završecima, ONT (*Optical Network Termination*) instaliranim u kućama ili zgradama. U FTTC i FTTCab OLT je s pomoću optičkih niti povezan s optičkim mrežnim jedinicama, ONU (*Optical Network Unit*) smještenima u blizini skupine kuća ili zgrada koje su, pak, nekom od DSL tehnologija (ADSL ili VDSL) povezane s mrežnim završecima, NT (*Network Termination*) unutar samih kuća ili zgrada.

Pristupnu mrežu utemeljenu na FTTx tehnologijama fizički je moguće realizirati pomoću:

- poveznica od točke do točke, od kojih svaka izravno povezuje centralu i krajnjeg korisnika ili
- optičke mreže.

Osnovna prednost korištenja pasivnih optičkih mreža, pred optičkim poveznicama od točke do točke, jest u uštedama u izgradnji kableske infrastrukture, jer uporaba PON-a smanjuje potrebnu količinu optičkih niti. Snaga signala koji se šalju prema krajnjim korisnicima dijeli se u omjeru $1 : N$, pri čemu je N broj krajnjih korisnika vezanih na pasivni optički razdjelnik (*Passive Optical Splitter*).

Kod pasivnih optičkih mreža utemeljenih na vremenskom multipleksiranju (TDM-PON) podaci se u smjeru prema krajnjem korisniku prenose načelom razasijavanja (*broadcast*), dok se u smjeru od korisnika prema mreži podaci prenose višestrukim pristupom mediju (*multiple medium access*), tj. ukupan raspoloživi pojas poveznice koja povezuje OLT s ONU-om dijeli se između krajnjih korisnika. O broju krajnjih korisnika ovisi kolika će im prijenosna brzina biti na raspolaganju (nije definirana gornja granica na krajnji broj korisnika). Međutim, praktično ograničenje na krajnji broj korisnika predstavlja maksimalno pristupno kašnjenje (*access delay*). Sukladno tome, broj krajnjih korisnika po jednom razdjelniku obično ne prelazi 64. Slika 5-8 prikazuje generičku arhitekturu PON-a.



Slika 5-8: Arhitektura PON-a

Ovisno o mehanizmu korištenom za prijenos podataka optičkim nitima, definirano je nekoliko vrsta TDM-PON-ova:

- APON (*ATM over PON*)
- EPON (*Ethernet over PON*)
- BPON (*Broadband PON*) i
- GPON (*Gigabit PON*),

APON se koristi ATM-om kao protokolom nad fizičkim slojem. Prijenosne brzine koje podržava APON kreću se do 622,080 Mbit/s u dolaznom smjeru i do 155,520 Mbit/s u odlaznom smjeru. Domet prijenosa iznosi do 20 km, a optička poveznica koja povezuje OLT i ONU može posluživati najviše 32 krajnja korisnika.

BPON definira PON-ove koji omogućavaju pristup dolaznom brzinom do 1.244,16 Mbit/s i odlaznom brzinom do 622,080 Mbit/s. APON je jedna od inačica BPON-a, koja se koristi ATM-om.

GPON se koristi brzinama prijenosa (simetričnima ili asimetričnima) od 155,520 Mbit/s, 622,080 Mbit/s, 1.244,16 Mbit/s i 2,488.32 Mbit/s. Domet prijenosa iznosi do 20 km (uz uporabu regeneratora i do 60 km).

EPON (sinonim za EPON je EFMP) podržava prijenosne brzine definirane Ethernet standardima: 10 Mbit/s, 100 Mbit/s, 1 Gbit/s ili 10 Gbit/s.

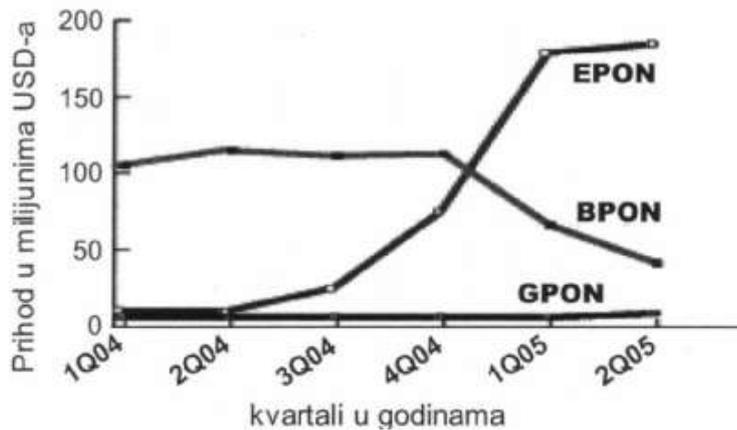
Definirana su dva EFMP standarda fizičkog sloja:

- 1000BASE-PX10, domet prijenosa 10 km i
- 1000BASE-PX20, domet prijenosa 20 km.

Broj krajnjih korisnika u EPON-u ograničen je na 16 ili 32.

Pored navedenih inačica PON-ova koji se koriste TDM-om u odlaznom smjeru komunikacije, PON-ove je moguće iskoristiti zajedno s WDM-om. Tada je svakom korisniku dodijeljena zasebna valna duljina pa je problem višestrukog pristupa zajedničkom mediju jednostavniji, a postizive prijenosne brzine po svakom korisniku puno veće. Jedina negativna strana WDM-PON-ova je u njihovoj visokoj cijeni u odnosu na tradicionalne PON-ove.

Slika 5-9 prikazuje trenutačno stanje glede prihoda od PON tehnologija u svijetu. Evidentno je naglašeno povećanje implementacije i prihoda EPON-a, dok se BPON očito rabi sve manje. Prihod od GPON-a bilježi vrlo blagi porast što ukazuje na to da se rabi puno manje od EPON-a. Razlog tome je sve veća prihvaćenost protokola Ethernet kao standarda u pristupnim mrežama.



Slika 5-9: Prihod (izražen u USD) od raznih vrsta PON-ova u razdoblju od prvog kvartala 2004. do drugog kvartala 2005. godine (Izvor: Dell'Oro Group)

U FTTx sustavima, koji rabe poveznice od točke do točke, danas se najčešće u uporabi koncept, EFMF (*Ethernet in the First Mile Fiber*). Tablica 5-4 prikazuje inačice EFMF-a.

Tablica 5-4: Opcije fizičkog sloja EFMF-a; SMF (*Single Mode Fiber*) - jednomodna optička nit

	100 Mbit/s, SMF	1 Gbit/s, SMF
dvije niti	100BASE-LX10, 10 km	1000BASE-LX, 5 km 1000BASE-LX10, 10 km
jedna nit	100BASE-BX10-D, 10 km 100BASE-BX10-U, 10 km	1000BASE-BX10-D, 10 km 1000BASE-BX10-U, 10 km

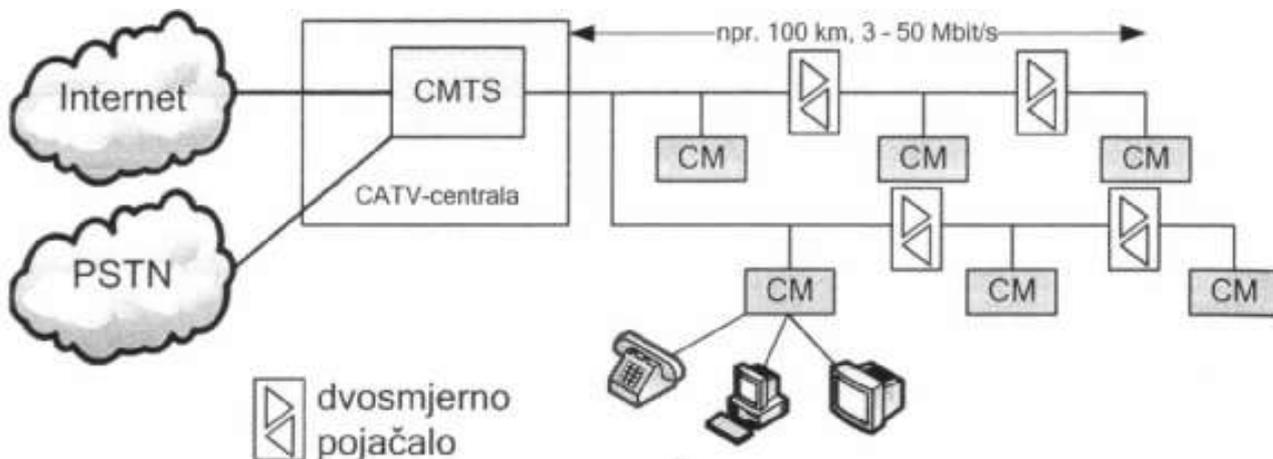
24.5. Tehnologije bežičnog optičkog pristupa

Bežični optički pristup naziva se izvorno, FSO (*Free Space Optics*). FSO podržava veze od točke do točke, s prijenosnim brzinama do 1,25 Gbit/s. Uskoro se očekuje i oprema koja će podržavati brzine do 10 Gbit/s. Pri prijenosnoj brzini od 155 Mbit/s domet prijenosa iznosi 2000 metara. Međutim, raspoloživost FSO poveznice ovisna je o njezinoj duljini i prijenosnoj brzini. Do 150 metara poveznica je raspoloživa sve vrijeme i po svim vremenskim uvjetima. Međutim, ako promatramo poveznicu duljine 800 m, njezina raspoloživost pri brzini od 155 Mbit/s pada na 99,5%, dok pri duljini od 1500 metara iznosi 99%. Naravno, ako je korisniku nužna stopostotna pouzdanost veze ostvarene tehnologijom FSO, tada je nužno korištenje redundantne poveznice. U području FSO-a nedostaju dovršeni standardi na svjetskoj razini. Uglavnom su standardizirane samo pojedine komponente sustava, ali ne i sustav u cjelini.

24.6. Širokopolasni pristup koaksijalnim kabelima

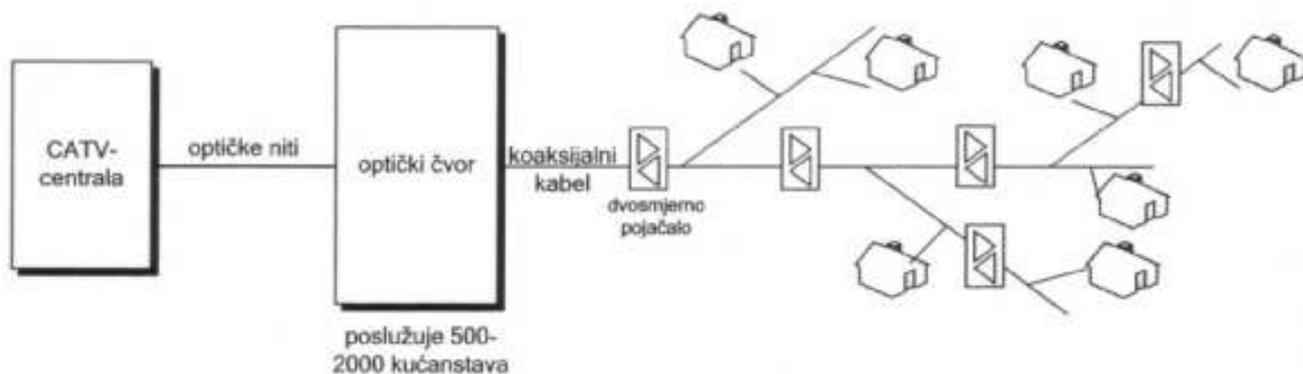
Širokopolasni pristup Internetu koaksijalnim kabelima realizira se s pomoću kablinskih modema, CM (*Cable Modem*). Kablinski modemi su koaksijalnim kabelima povezani sa završnim sustavom, CMTS (*Cable Modem Termination System*) koji predstavlja sastavni dio CATV centrale (*head-end*) operatora kablinske mreže (Slika 5-10).

Domet sustava može biti vrlo velik zahvaljujući uporabi pojačala. Iako je na taj način moguće razašiljati signal kablinske televizije (CATV) velikoj skupini krajnjih korisnika uz relativno mali broj kabela (jedan CMTS može posluživati i do 2000 korisnika po jednom TV kanalu), prigodnom korištenja kablinskih modema za pristup Internetu svi korisnici, koji su povezani sa CMTS-om s pomoću zajedničkog koaksijalnog kabela, dijele ukupnu prijenosnu brzinu. Osim toga, u kablinskoj mreži s dijeljenim pristupom intenziviran je problem sigurnosti, odnosno privatnosti komunikacije.



Slika 5-10: Osnovna arhitektura pristupa Internetu kabelskim modemima

Mreža koja povezuje operatorov koncentrador s kabelskim modemima može biti izvedena na dva načina: isključivo pomoću koaksijalnih kabela ili kao hibridna optičko-koaksijalna mreža, HFC (*Hybrid Fiber/Coax*), što je danas najčešći slučaj u svijetu (Slika 5-11). U HFC mreži signali se iz centrale optičkim nitima prenose do optičkih čvorova od kojih se dalje koaksijalnim kablom distribuiraju krajnjim korisnicima.



Slika 5-11: Topologija HFC mreže

Tipične ukupne prijenosne brzine koje je moguće postići kabelskim modemima su: 55,2 Mbit/s u dolaznom smjeru i 3 Mbit/s u odlaznom smjeru (najnoviji standardi omogućavaju i do 30 Mbit/s u odlaznom smjeru). Prijenosne brzine po jednom korisniku iznose tipično: od 500 do 1000 kbit/s u dolaznom smjeru i od 256 do 500 kbit/s u odlaznom smjeru. Glavni standard u području kabelskih modema poznat je pod nazivom DOCSIS.

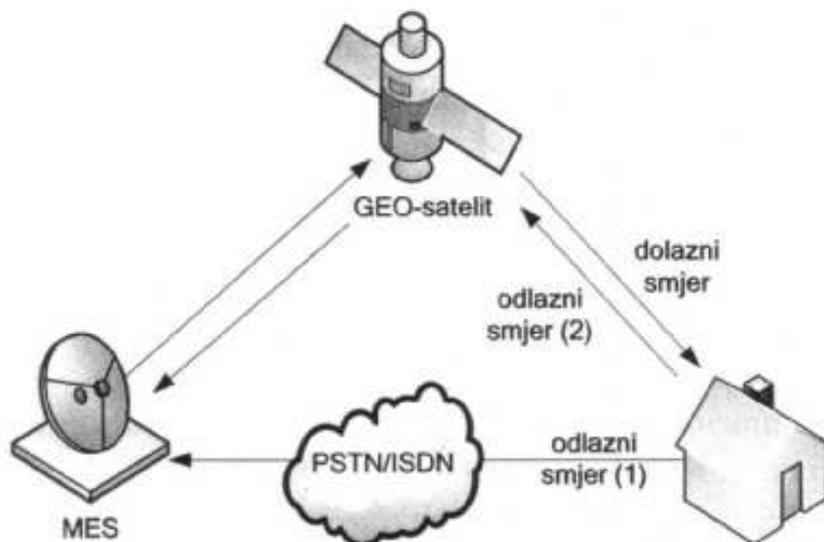
24.7. Satelitski širokopojasni pristup

Postoje razna rješenja za realizaciju širokopojasnog pristupa Internetu uporabom satelitskog prijenosa. Velik dio utemeljen je na tehnologijama poput: DVB-RCS (*Digital Video Broadcast with Return Channel via Satellite*) i DVB-RCT (*Digital Video Broadcast with Return Channel Terrestrial*). Kao što im i naziv govori, DVB sustavi su primarno namijenjeni razširivanju videa, ali se satelitski kanali mogu iskoristiti i za povezivanje s Internetom.

U vrijeme dok su se satelitske komunikacije rabile isključivo za slanje TV signala prema korisnicima, "povratni" put nije niti bio aktualan. Međutim, uvođenjem pristupa Internetu javlja se problem realizacije prijenosa signala u smjeru od krajnjih korisnika prema mreži. U konceptu DVB-RCS povratni je put realiziran također satelitski. Za takav se sustav često govori da rabi dvosmjernu satelitsku vezu (*two-way satellite*). Nasuprot tome, u konceptu DVB-RCT povratni je put realiziran zemaljskom vezom, tj. preko biranih linija, N-ISDN-om ili nekom drugom opcijom (Slika 5-12).

Pored DVB-a, za realizaciju širokopojasnog pristupa Internetu rabe se i VSAT sustavi (*Very Small Aperture Terminal*). VSAT sustavi se sastoje od tri komponente: VSAT stanice krajnjeg korisnika

(VSAT *Remote Earth Station*), glavne zemaljske VSAT stanice, MES (*Master Earth Station*) i geostacionarnog (GEO) satelita. Većina satelitskih sustava krajnjim korisnicima nudi brzine u rasponu od 64 kbit/s do 2 Mbit/s. Satelitski se prijenos smatra najkvalitetnijim rješenjem za udaljene korisničke lokacije (ruralna područja), iako je cijena satelitskih veza visoka i stoga ovaj način prijenosa nije konkurentan drugim pristupnim tehnologijama.



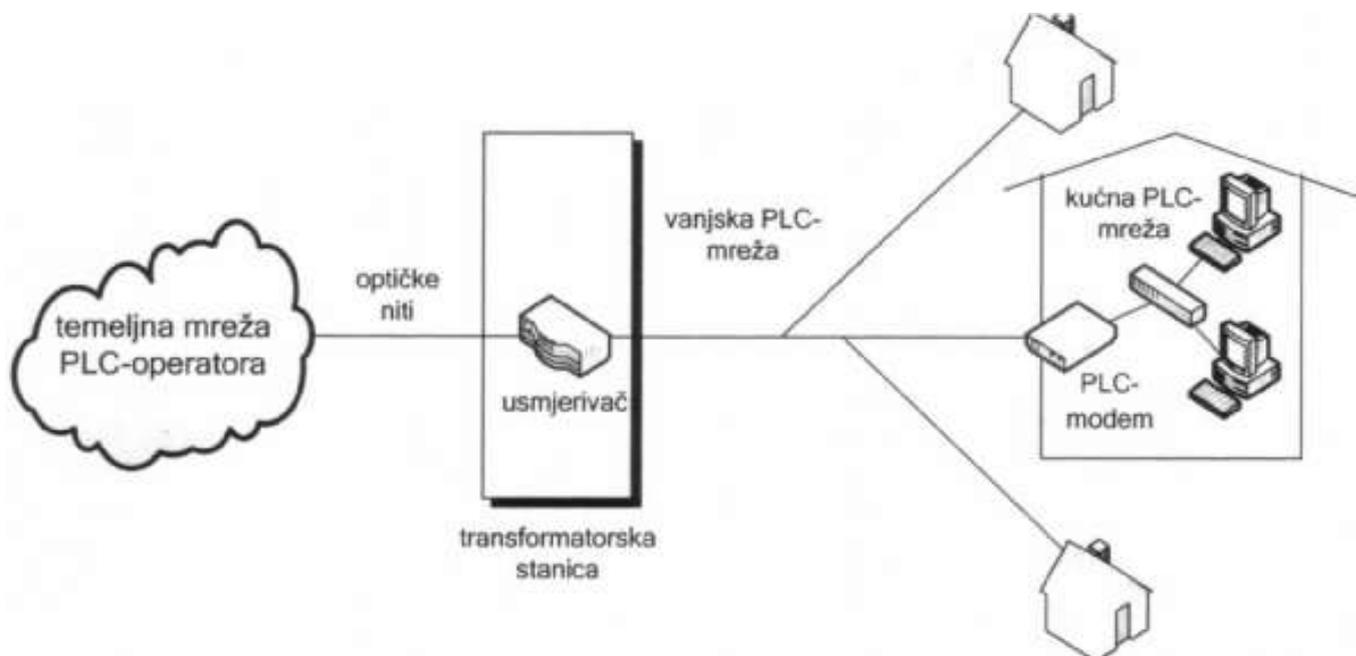
Slika 5-12: Satelitski pristup s povratnim kanalom: (1) kroz PSTN/N-ISDN ili (2) realiziranim satelitskom poveznicom

24.8. Širokopolasni pristup vodovima elektroenergetske mreže

Komunikacije vodovima elektroenergetske mreže su posebno interesantne operatorima distribucijske elektroenergetske mreže poput, npr., Hrvatske elektroprivrede (HEP). Osnovna ideja PLC-a je da se širokopolasni podaci optičkim nitima prenose iz jezgrene mreže do transformatorskih stanica, od kojih se razvode vodovima elektroenergetske mreže do krajnjih korisnika (Slika 5-13). PLC mreža između transformatorske stanice i PLC modema na korisničkom području naziva se vanjska (*outdoor*) PLC mreža, a ona u kući unutarnja (*indoor*).

Već dulje vrijeme postoje standardi za uskopojasni prijenos podataka PLC-om. Prijenosni PLC sustavi, kreirani sukladno tim standardima, uglavnom služe za upravljanje elektroenergetskim postrojenjima na daljinu i rade u niskom području frekvencija (spektar signala seže do 500 kHz). Prijenosne brzine u tim sustavima kreću se do nekoliko desetaka kbit/s.

Nazivom *Broadband Power-line* (BPL) označene su one PLC mreže koje prenose podatke širokopolasnim brzinama. Postoje dvije skupine BPL tehnologija: pristupni BPL (*Access BPL*), koji se implementira nad vanjskom PLC mrežom, i BPL unutar zgrade (*In-building BPL*) implementiran nad kućnom PLC mrežom.



Slika 5-13: Topologija pristupne mreže realizirane PLC-om

Danas pristupni BPL podržava prijenos podataka brzinama do 45 Mbit/s, i to u oba smjera, dolaznom i odlaznom. Pristupni BPL, slično kao i mreža kablanske televizije, predstavlja dijeljeni medij. Stoga je potrebno ograničiti broj korisnika pristupnog BPL-a po svakoj transformatorskoj stanici kako bi se ta agregatna brzina dijelila s manjim brojem. Osnovna mana pristupnog BPL-a je nedostatak standarda prihvaćenih na svjetskoj razini. U kućnim PLC mrežama uglavnom se rabi standard *HomePlug*. Brzine prijenosa koje podržava taj standard kreću se u rasponu do 14 Mbit/s.

Najveći problem koji i dalje predstavlja glavnu kočnicu za širu primjenu PLC-a je problem elektromagnetske kompatibilnosti PLC sustava.

24.9. Širokopolasni fiksni bežični pristup

Iako DSL tehnologije dominiraju na tržištu, telekom operatori se sve više orijentiraju na bežične tehnologije. Bežične širokopolasne tehnologije predstavljaju atraktivno rješenje za brzi pristup Internetu i podatkovnim, govornim i video uslugama. Podjednako je primjenjiv kod rezidencijalnih i poslovnih korisnika, a trenutačno je standardima predviđeno korištenje područja frekvencija od 2 GHz do 66 GHz. Velika je prednost bežičnih tehnologija pred žičnim i optičkim tehnologijama u relativno niskoj cijeni implementacije. Međutim, bežične pristupne mreže još uvijek ne mogu, po svojim prijenosnim performansama, parirati žičnim i optičkim mrežama.

Najznačajnije tehnologije širokopolasnog fiksnog bežičnog pristupa, kao ciljne skupine tehnologija koje mogu ponuditi kvalitetan širokopolasni pristup Internetu, su: LMDS (*Local Multipoint Distribution Service*), MMDS (*Multi-channel Multipoint Distribution Service*), IEEE 802.16 (komercijalno nazvan WiMAX), HIPERACCESS i HIPERMAN.

MMDS je licencirana usluga dometa 5 km, što znači da jedan antenski sustav može, uz dovoljnu snagu zračenja, pokriti područje cijelog grada. Naravno, treba voditi računa o tome da krajnji korisnici zajednički dijele raspoložive kanale i da s porastom njihova broja pada propusnost (*throughput*) veza. Ostvarive prijenosne brzine kreću se u rasponu od 500 do 1000 kbit/s, iako neki tvrde da je moguće postići i 10 Mbit/s.

LMDS je moguće implementirati kao tehnologiju od točke do točke ili od točke prema većem broju točaka. Maksimalne ostvarive prijenosne brzine LMDS PTP kreću se između 155 i 622 Mbit/s, uz domet od 2 km. Realno postizive prijenosne brzine sežu do 45 Mbit/s, odnosno do 311 Mbit/s pri

prijenosu snopova⁹ (*bursts*) podataka. Za razliku od MMDS-a, koji je prikladniji za rezidencijalne i SOHO korisnike, ciljana skupina korisnika LMDS-a su srednje i velike tvrtke.

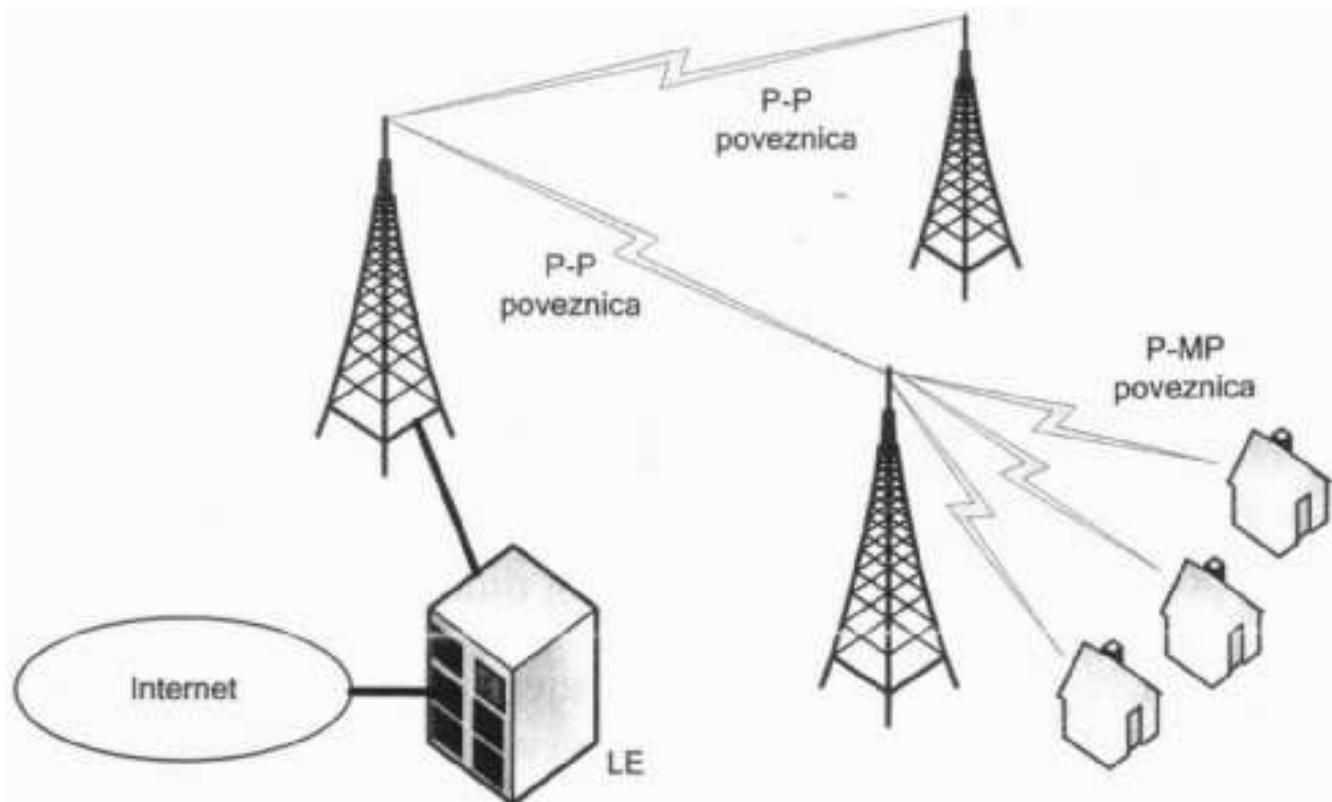
24.9.1. WiMAX

WiMAX je popularni naziv standarda za realizaciju gradskih bežičnih mreža (*Wireless Metropolitan Area Networks*). Svjetska standardizacijska organizacija IEEE odredila je 1998. godine radnu skupinu nazvanu 802.16 *Working Group* koja je zadužena za razvoj bežičnog standarda za gradske mreže. Prva inačica standarda nazvana je IEEE 802.16, a njezin komercijalni naziv je WiMAX što je skraćenica od *Worldwide Interoperability for Microwave Access*. WiMAX, prije svega, treba promatrati kao tehnologiju za realizaciju fiksnog bežičnog pristupa, FWA (*Fixed Wireless Access*). Prva inačica definirala je sustav koji rabi područje frekvencija od 10 GHz do 66 GHz. S obzirom da takav sustav zahtijeva optičku vidljivost između predajnika i prijarnika, radna je skupina nastavila razvijati i drugu inačicu, nazvanu IEEE 802.16a, koja rabi frekvencijsko područje od 2 GHz do 11 GHz i ne zahtijeva spomenutu optičku vidljivost. Kao takva, puno je bolje prilagođena radu u gusto naseljenim područjima. Nakon što je 2001. godine objavljen standard IEEE 802.16a, 2004. godine je ta inačica doradena i nazvana IEEE 802.16d (ili IEEE 802.16-2004). Tom su nadopunom standarda poboljšane performanse WiMAX poveznice u odlaznom smjeru komunikacije. Konačno, inačica standarda nazvana IEEE 802.16e trebala bi riješiti i problem mobilnosti krajnjeg korisnika, i to sve do brzina kretanja od 110 do 130 km/h, kao i asimetrično sučelje za prijenosna računala i komunikatore, koje će im omogućiti izravnu povezanost, pomoću ugrađene mrežne kartice, s WiMAX mrežom (a ne putem bežičnog LAN-a kao što je dotad bilo planirano). Kako bi se stvorili bolji uvjeti za prihvaćanje ove tehnologije, 2001. godine osnovan je WiMAX Forum, kao neprofitna organizacija koja promovira WiMAX. HIPERACCESS i HIPERMAN su standardi organizacije ETSI kompatibilni sa standardom IEEE 802.16.

WiMAX je naročito interesantan za primjenu u ruralnim područjima koja tradicionalno nemaju razvijenu telekomunikacijsku infrastrukturu. Izgradnja WiMAX mreže u takvim područjima daleko je isplativija za operatore od, npr., izgradnje parične infrastrukture za xDSL tehnologije ili optičke infrastrukture za FTTx arhitekture. Primjena WiMAX-a u ruralnim područjima krajnjim će korisnicima omogućiti širokopojasni pristup telekomunikacijskoj mreži i uslugama i ublažiti tzv. digitalnu podjelu. Nasuprot tome, u gradskim područjima proboj WiMAX-a će biti teži zbog već postojeće parične ili optičke infrastrukture pa u tom segmentu treba očekivati jaku konkurenciju između žično-optičkih i bežičnih mreža. Općenito gledano, kompetitivnost WiMAX-a ovisi o prijenosnim brzinama i dometima koje je moguće postići tom tehnologijom, kao i o kvaliteti prijenosne usluge koju ta bežična arhitektura pruža krajnjim korisnicima. Upravo se na tom planu ostvaruju permanentna poboljšanja čime WiMAX postaje sve veći konkurent xDSL-u i FTTx-u.

U samom početku WiMAX je bio dominantno predviđen za bežični prijenos govora i podataka, i rezidencijalnih i poslovnih korisnika. Stalna poboljšanja prijenosne usluge približila su WiMAX skupu onih tehnologija koje omogućavaju kvalitetan prijenos *triple play* usluga. U odnosu na postojeće mobilne mreže, WiMAX pruža znatno širi prijenosni pojas frekvencija, a samim time i veće ostvarive prijenosne brzine. Osim toga, podizanje dometa na čak 20 km omogućava jako dobru pokrivenost terena s relativno malim brojem baznih stanica.

⁹ praskova ???????



Slika 5-14: Širokopolasni bežični pristup tehnologijom WiMAX

Arhitektura WiMAX mreže podjednako podržava poveznice od točke do točke (P-P) i od točke prema većem broju točaka (P-MP) - Slika 5-14. U P-P topologiji mreža se sastoji od jedne ili više P-P poveznica koje se koriste jako usmjerenim antenama. U P-MP topologiji mreža se sastoji od baznih stanica, od kojih je svaka s pomoću P-MP poveznica povezana s krajnjim korisničkim uređajima. U mješovitoj mrežnoj topologiji krajnji korisnički uređaji mogu ne samo primati signal od baznih stanica, već i usmjeravati promet prema drugim korisnicima. Na taj je način moguće povećati pokrivenost terena jer svaka nova korisnička stanica može, ujedno, djelovati i kao nova bazna stanica. Stvarne WiMAX mreže uglavnom rabe kombinaciju P-P i P-MP topologija. Obično se P-P poveznice rabe za povezivanje baznih stanica s temeljnom mrežom, dok se stanice prema krajnjim korisnicima služe P-MP poveznicama. Bazine stanice mogu se s temeljnom mrežom povezivati i s pomoću P-P poveznica izvedenih optičkim nitima ili zakupljenim kanalima (najčešće žično). Trenutačno na tržištu nema velikog broja mješovitih FWA sustava, već su, uglavnom, prisutni sustavi koji se koriste P-MP topologijom.

Posebno je važno istaknuti da je područje pokrivanja svake bazne stanice podijeljeno u sektore (za svaki se sektor rabi posebna usmjerena antena) čime se po svakom sektoru postiže veća snaga signala te sukladno tome, i veća prijenosna brzina i domet prijenosa negoli u slučaju kad antena bazne stanice zrači signal u svim smjerovima.

Frekvencijska područja od posebnog interesa za primjenu WiMAX-a su pojasevi oko 2,5, 3,5 i 5,8 GHz. U Hrvatskoj je, planom dodjele frekvencijskog spektra za širokopolasne nepokretne bežične sustave, predviđeno područje od 3,4 do 3,6 GHz (za korištenje ovog područja potrebna je dozvola nadležnog tijela; u Republici Hrvatskoj to je Hrvatska agencija za telekomunikacije), kao i područje od 24,5 do 26,5 GHz (također je potrebna dozvola). Oba su područja namijenjena isključivo za civilnu uporabu. Za potrebe FWA moguće je iskoristiti i tzv. ISM pojaseve frekvencija za čije korištenje nije potrebna dozvola. U Republici Hrvatskoj to su područja od 2,4 GHz do 2,5 GHz (za civilnu uporabu) te pojasevi od 5,725 do 5,83 GHz (za civilnu i vojnu uporabu) i od 5,85 GHz do 5,925 GHz (samo za civilnu uporabu). Međutim, korištenje tih pojaseva je svjestan rizik jer u tom području već rade mnogi bežični mikrovalni sustavi, a posebno bežični LAN-ovi pa je i mogućnost interferencije s tim sustavima veća negoli u strogo namjenskim pojasevima.

Sukladno standardu IEEE 802.16, dolazni smjer komunikacije riješen je vremenskim multipleksiranjem (TDM), pri čemu je svakom krajnjem korisniku pridijeljen jedan ili više vremenskih odsječaka. U odlaznom smjeru višestruki je pristup riješen tehnikom TDMA. Širina kanala u Europi iznosi 28 MHz. Dvosmjernost komunikacije rješava se frekvencijski, FDD (*Frequency Division Duplex*) ili vremenski (*Time Division Duplex*, TDD). Za razliku od toga, standard IEEE 802.16a predviđa uporabu modulacijskog postupka, OFDM (*Orthogonal Frequency Division Multiplexing*) i adekvatnu tehniku višestrukog pristupa OFDMA. Protokol kojim se WiMAX koristi na podsloju upravljanja pristupom mediju, MAC (*Medium Access Control*) spojno je orijentiran pa se i nespojne usluge preslikavaju u veze.

Posebna je pozornost, u dizajnu podsloja i protokola MAC, posvećena kvaliteti usluge kojom su predviđene tri vrste veza:

- osnovna veza korištena za prijenos kratkih i vremenski kritičnih poruka,
- veze za prijenos standardnih protokola poput: DHCP, TFTP, SNMP i dr.,
- ostale vrste veza, npr. veze rezervirane za razaslanje signala.

Kako bi QoS mehanizam dobro funkcionirao, krajnji korisnici pristupaju mreži temeljem dozvola koje im izdaje bazna stanica. Prijenosne brzine podržane standardom IEEE 802.16 mogu biti i veće od 70 Mbit/s, dok standard IEEE 802.16a podržava prijenosne brzine do 25 Mbit/s. Širine kanala variraju od 1,5 do 20 MHz. Domet prijenosa ostvariv WiMAX-om seže i do 50 km, uz tipičan promjer ćelije od 13 do 20 km.

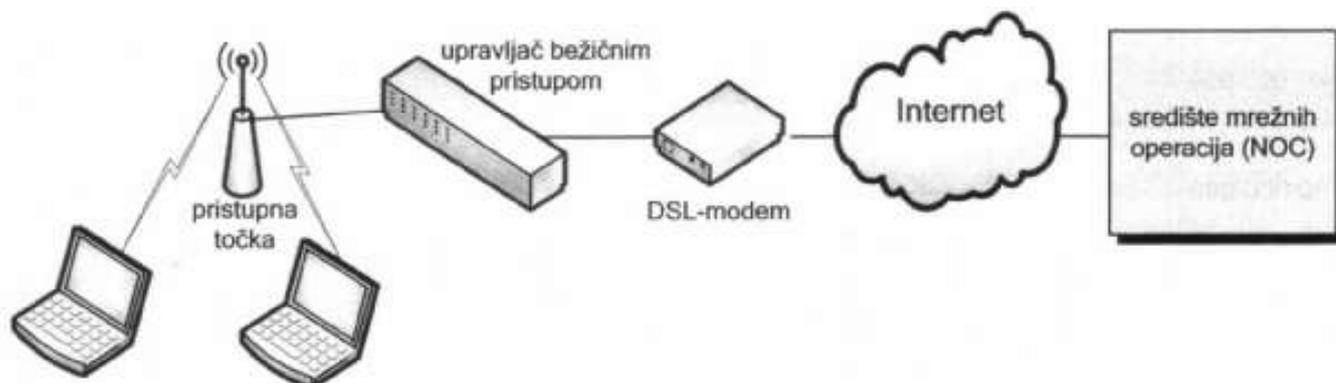
24.9.2. Ostale bežične pristupne tehnologije

Od ostalih bežičnih pristupnih tehnologija često se spominje i Wi-Fi (komercijalni naziv za tehnologije definirane skupinom standarda IEEE 802.11). U području širokopojasnog pristupa Internetu posebno su zanimljive pristupne lokacije s velikom gustoćom korisnika (*hotspots*) koje korisnicima omogućavaju pristup Internetu preko bežičnog LAN-a, WLAN (*Wireless LAN*). Najčešća im je primjena u hotelima i ugostiteljskim objektima. Korisnicima se nudi mogućnost korištenja usluge uz plaćanje *pre-paid* karticom te mogućnost plaćanja kreditnim karticama.

Podaci koji mogu dodatno ukazati na važnost pristupnih lokacija su sljedeći:

- 30 milijuna korisnika pristupnih lokacija u 2004. (prema tvrtki *Gartner*),
- očekivani broj korisnika u 2007. - 70 milijuna,
- 43.850 lokacija u 2003. i oko 50.000 u 2004. godini (prema In-Stat/ MDR).
- očekivani broj pristupnih lokacija u 2008. u svijetu: 200.000.

Tehnologije IEEE 802.11 koriste se, uglavnom, nelicenciranim dijelom frekvencijskog spektra, tzv. ISM pojasom (*Industrial, Scientific, Medical*), što znači da za njihovo korištenje nisu potrebne posebne dozvole nadležnih državnih tijela. Koristeći se nekom od tih tehnologija moguće je postići prijenosne brzine do 54 Mbit/s (efektivno do 25 Mbit/s), a najnoviji standardi omogućavaju čak 100 Mbit/s efektivno.



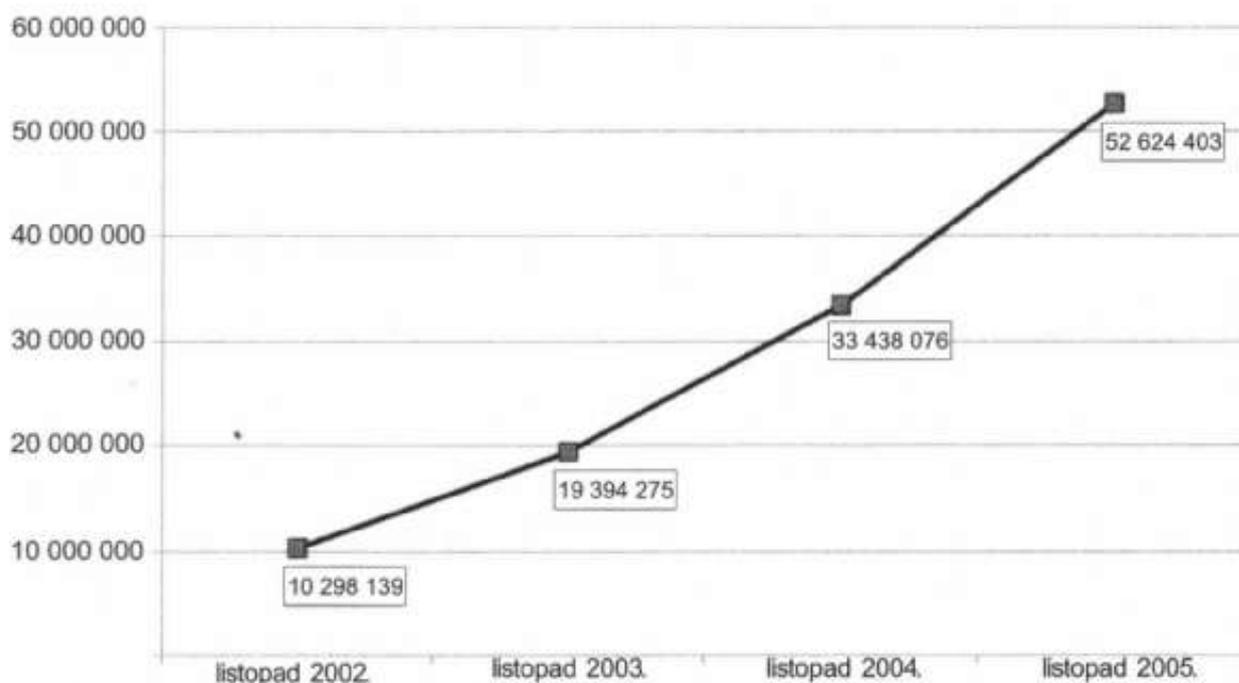
Slika S-1 S: Jedan od načina realizacije pristupne lokacije; u NOC-u se provodi autentifikacija, autorizacija i praćenje korisničkih računa (*accounting*)

24.10. Stanje širokopojasnog pristupa Internetu u zemljama EU-a

U ovom odjeljku dan je pregled stanja u području širokopojasnog pristupa u zemljama Europske unije (EU), s povremenim osvrtom na prvih 15 zemalja članica (EU15) ili na 25 članica (EU25), koliko ih je EU brojio do posljednjeg proširenja. Oznaka EU10 odnosi se na 10 zemalja čijim je učlanjenjem EU15 proširen na EU25. Cilj pregleda je ukazati na dinamiku zbivanja u jednom od najpropulzivnijih sektora telekomunikacija - području širokopojasnih pristupnih mreža.

Prema podacima za listopad 2005. godine, zemlje EU-a posjeduju 52,6 milijuna fiksnih širokopojasnih linija (Slika 5-16), što daje prosječnu penetraciju (broj linija na 100 stanovnika) od 11,5% (za usporedbu, u listopadu 2004. ta je penetracija iznosila 7,3%).

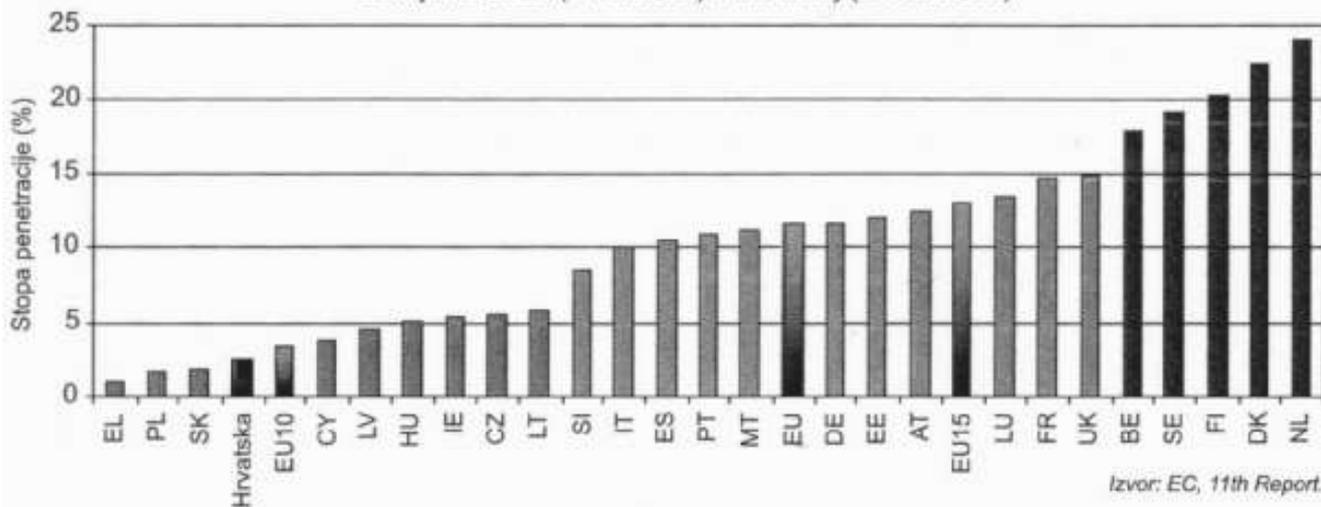
Sukladno tome, dnevni porast broja fiksnih širokopojasnih linija u zemljama EU-a u 2005. iznosi 52.000, u usporedbi s 38.000 novih linija u 2004. Slika 5-17 prikazuje stupanj razvijenosti širokopojasnog pristupa Internetu u pojedinim zemljama EU-a i u Hrvatskoj.



Slika 5-16: Porast broja fiksnih širokopojasnih pristupnih linija u EU-u

Stopa penetracije širokopojasnih priključaka u zemljama EU-a (1.10.2005.) i Hrvatskoj (31.12.2005.)

Stopa penetracije širokopojasnih priključaka u zemljama EU-a (1.10.2005.) i Hrvatskoj (31.12.2005.)



Slika 5-17: Broj širokopojasnih linija na 100 stanovnika (stopa penetracije, izražena u postocima) u pojedinim zemljama Europske unije i Hrvatskoj (stanje na dan 31. prosinca 1006.) te prosječna vrijednost za EU10 i EU15 (stanje na dan 1. listopada 2005.)

Penetracija fiksnog širokopojasnog pristupa u zemljama EU-a visoka je promatramo li je i na svjetskoj razini. Prema podacima za razdoblje lipanj - srpanj 2005. samo Južna Koreja ima veću penetraciju od najbolje pozicionirane članice EU-a, Nizozemske (Tablica 5-5).

Tablica 5-5: Penetracija širokopojasnog pristupa fiksnim linijama u svijetu (lipanj - srpanj 2005.)

Zemlja	J: Koreja	Nizozemska	Danska	Island	Švicarska	Kanada
Penetracija (%)	25,5%	22,4%	22,0%	21,7%	20,3%	19,2%
Zemlja	Finska	Norveška	Belgija	Švedska	Japan	SAD
Penetracija (%)	18,7%	18,2%	17,4%	17,1%	16,4%	14,5%

Za usporedbu sa zemljama EU15 i EU10, Hrvatska je krajem 2005. godine imala oko 100.000 širokopojasnih linija (od toga najviše ADSL-a) što na približno 4,5 milijuna stanovnika predstavlja penetraciju širokopojasnog pristupa od približno 2,5%.

Porast broja širokopojasnih implementacija uzrokovan je, prije svega, sve izraženijom konkurencijom između operatora te njihovom željom da povećaju sve slabiji prihod od fiksne analogne telefonije (POTS). Prihod od fiksnih podatkovnih usluga raste stopom od 11,5% godišnje. Stanje razvijenosti širokopojasnog pristupa Internetu svakako oslikava i usporedba broja širokopojasnih linija na 100 stanovnika.

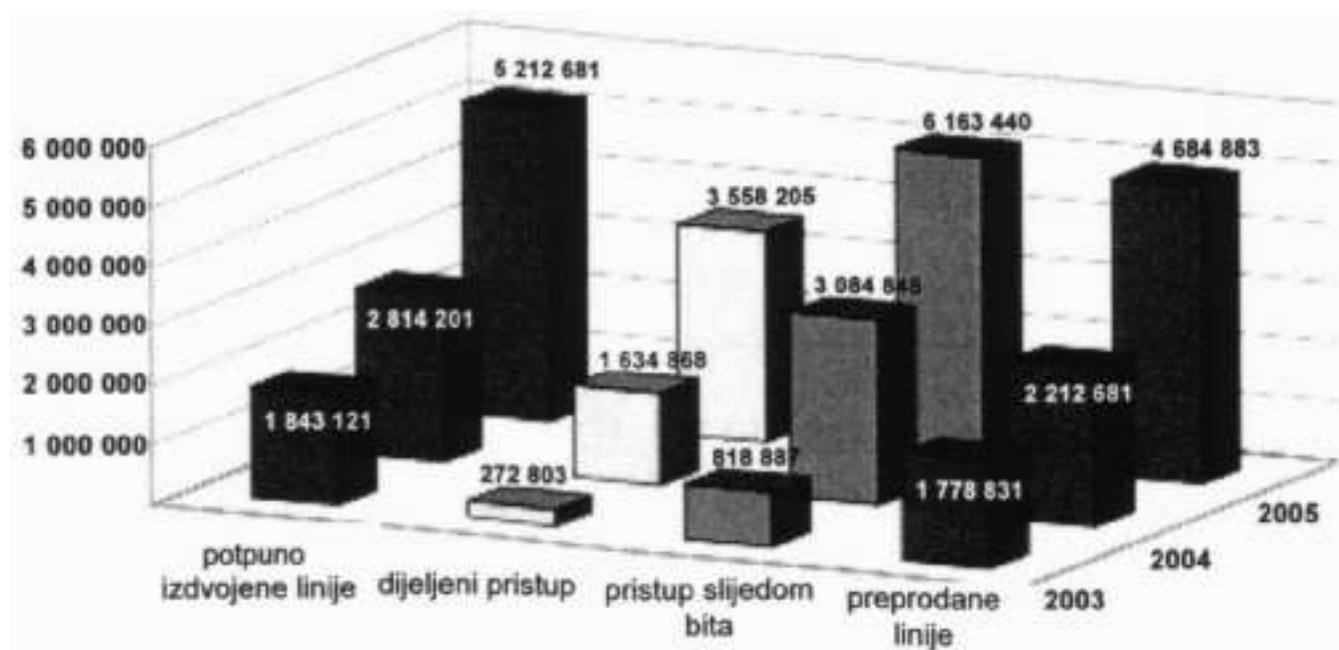
Dinamika u području širokopojasnog pristupa ne očituje se samo u porastu broja linija, već i u povećanju broja ponuđenih usluga. Na primjer, pružatelji DSL usluga sve češće nude svojim korisnicima VoIP, ne bi li ih tako stimulirali na povećano korištenje mreže. Za spomenutu dinamiku najzaslužniji su poboljšani omjer cijena i performansi, porast korištenja Interneta u općem smislu, povećana dostupnost Interneta i stalno rastuća svijest korisnika o Internetu kao izvoru poslovnih informacija, zabavnih i ostalih sadržaja. Širokopojasne linije se sve više rabe za pristup poslovnim aplikacijama, a ne samo za brzi pristup Internetu. Sve veći broj operatora nudi svojim korisnicima kombinaciju videa, govornih i podatkovnih usluga (tzv. *triple play*).

Porast broja širokopojasnih implementacija uzrokovan je, prije svega, sve izraženijom konkurencijom između operatora s dobrom zakonskom regulativom povoljnom za operatore i korisnike. Udio novih operatora na tržištu širokopojasnog pristupa iznosi 49,8% u zemljama EU-a. Pritom u Ujedinjenom Kraljevstvu operator proizašao iz razdoblja monopola (*incumbent*) zauzima 25% tržišta, a na Cipru čak 100%.

Penetracija širokopojasnog pristupa najveća je u onim zemljama članicama EU-a gdje postoji konkurencija između operatora glede komunikacijske infrastrukture (kabelske ili druge) i glede LLU-a.

Za porast penetracije najzaslužnija su dva čimbenika:

- odlučna akcija regulatornih tijela, posebno u obliku određivanja cijena,
- u nekim zemljama novi operatori počinju povećavati vlastita ulaganja u infrastrukturu.



Slika 5-18: Broj DSL-a novih operatora i razne vrste pristupa; podaci su dani za 1. listopada 1003.,1004. i 1005. godine

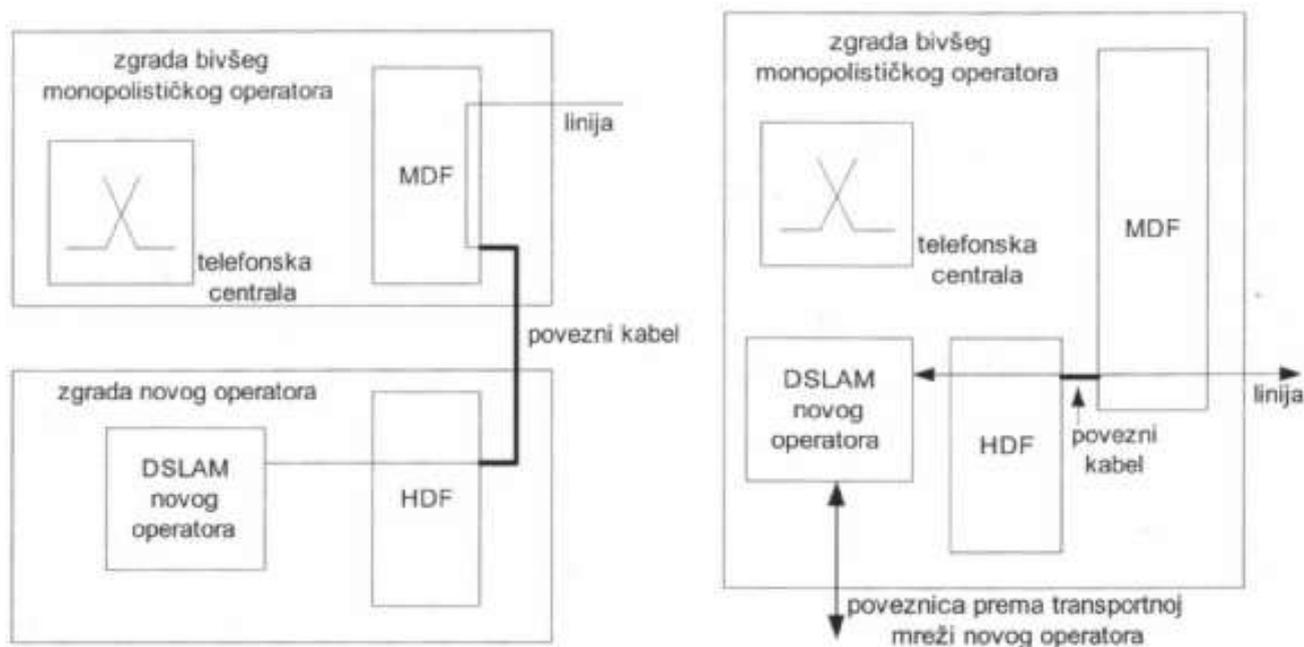
Slika 5-18 prikazuje razdiobu pretplatničkih linija koje su operatori proizašli iz razdoblja monopola, sukladno sklopljenim ugovorima, predali novim operatorima na korištenje. Ukupan broj takvih linija iznosio je 1. listopada 2005. godine 18.919.229.

Glede korištenja kabelske infrastrukture operatora proizašlog iz razdoblja monopola od strane novih operatora postoje četiri vrste pristupa:

- pristup strujom bita
 - definicija struje bita (*bitstream*) je sljedeća: brzi pristup struji bita odnosi se na one scenarije pristupa u kojima operator iz razdoblja monopola instalira brzu pristupnu poveznicu prema korisničkom području (*customer premises*) i nakon toga omogućava trećoj strani (novom operatoru) da raspolaže tom poveznicom, a novi operator, pak, strujom bita može pružati brze usluge krajnjim korisnicima. Uslugu struje bita moguće je definirati kao pružanje prijenosnog kapaciteta između krajnjeg korisnika spojenog na telefonsku liniju i točke interkonekcije raspoložive novom operatoru. Struja bita je veleprodajni proizvod;
 - za razliku od ostalih veleprodajnih proizvoda u području brzog pristupa, struja bita dopušta novim operatorima da svojim krajnjim korisnicima pružaju i vlastite usluge s dodanom vrijednošću (*Value-Added Services, VAS*);
 - DSLAM održava operator iz razdoblja monopola;
- pristup preprodanim linijama (*resale lines*)
 - za razliku od struje bita, pri jednostavnoj preprodaji linija (*simple resale*) novi operator ne može ponuditi diferencirani proizvod (tj. proizvod s drukčijim tehničkim obilježjima) u odnosu na osnovnu DSL uslugu koju mu prodaje operator proizašao iz razdoblja monopola. Novi operator može isključivo reklamirati, distribuirati i naplaćivati proizvod. U osnovi, novi operator pri jednostavnoj preprodaji linija pruža krajnjim korisnicima portal;

- dijeljeni pristup (*shared access*)
 - dijeljeni pristup je veleprodajni proizvod. U slučaju dijeljenog pristupa, pozicionirani operator nastavlja krajnjim korisnicima Pružati uslugu POTS, dok novi operatori tim istim lokalnim petljama pružaju korisnicima brze podatkovne usluge (npr. osnovnu DSL uslugu i preko nje širokopojasni pristup Internetu). Pritom je važno naglasiti da novi operator održava svoj DSLAM;
- pristup izdvojenim linijama
 - pristup izdvojenim linijama je veleprodajni proizvod. U slučaju potpunog izdvajanja lokalne petlje, operator proizašao iz razdoblja monopola daje novom operatoru “cijelu“ upređenu paricu (tj. cijeli prijenosni pojas) u najam. Uz LLU se veže i pojam kolokacije (*co-location*), tj. načina fizičkog povezivanja novog operatora na paricu. Ako se radi o potpunoj fizičkoj kolokaciji (*full co-location*), tada je oprema operatora-korisnika smještena u zgradi operatora proizašlog iz razdoblja monopola (razdjelnik i DSLAM), dok u slučaju udaljenije kolokacije (*distant location*) novi operator smješta svoju opremu u posebnu zgradu. U oba je slučaja vlasnik poveznog kabela (*tie-cable*) operator proizašao iz razdoblja monopola. U slučaju virtualne kolokacije, opremu koju rabi operator-korisnik postavlja, održava i njome upravlja isključivo operator proizašao iz razdoblja monopola.

Osim potpunog izdvajanja lokalne petlje (*full unbundling*), postoji i tzv. izdvajanje podpetlje (*sub-loop unbundling*). Tipičan primjer primjene ovakvog pristupa je VDSL. U tom se mrežnom scenariju izdvaja lokalna petlja u zadnjih 500 metara do korisnika, točnije od optičke mrežne jedinice (ONU) do korisničkog VDSL modema, dok optičku poveznicu do ONU-a održava pružatelj usluge. U Europskoj uniji je izdvajanje podpetlje obvezatno, u skladu sa specifikacijom tijela EU-a zaduženih za regulativu u telekomunikacijama.



Slika 5-19: Kolokacija - na slici lijevo prikazana je udaljena kolokacija, a na slici desno fizička kolokacija; HDF (*Handover Distribution Frame*) - razdjelnik novog operatora

24.11. Usluge s dodanom vrijednošću i IPTV

Najvažniji čimbenik koji utječe na prihvaćanje tehnologija širokopojasnog pristupa od strane krajnjih korisnika su usluge s dodanom vrijednošću. xDSL, FTTx ili WiMAX ne mogu sami po sebi, unatoč sve boljim performansama, probuditi interes krajnjih korisnika za prijelaz s postojećeg modemskog ili ISDN pristupa na širokopojasni pristup. Stoga je uvođenje usluga poput videa na zahtjev (*Video on Demand, VoD*) i drugih širokopojasnih usluga, koje je nemoguće realizirati tehnologijama uskopojasnog pristupa, nužno kako bi se povećala penetracija širokopojasnog pristupa. Usluge s

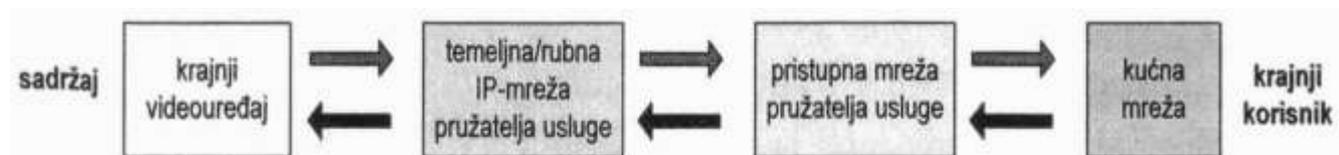
dodanom vrijednošću su definirane kao poboljšanja osnovne pristupne usluge ostvarene DSL-om. Primjeri VAS-a su sljedeći: VoD, VoDSL (*Voice over DSL*), glazba kodirana MPEG-om (*Moving Pictures Expert Group Music*), umreženo igranje između većeg broja igrača (*Multi-Player Gaming*), videokonferencije, razošiljanje TV signala (*broadcast TV*) i virtualne privatne mreže (VPN). *Pioneer Consulting* je proračunao da usluge s dodanom vrijednošću predstavljaju dobru priliku za zaradu na tržištu, koja varira od 15,8 do 26,6 milijarda USD-a godišnje, ovisno o načinima naplate troškova korištenja usluga koje operatori odaberu.

IPTV je skup usluga s dodanom vrijednošću, a naziv je skraćenica od *Internet Protocol Television*. U osnovi, radi se o konceptu transfera TV sadržaja IP paketima, za razliku od tradicionalnog prijenosa TV signala razošiljanjem kroz bežični medij. IPTV usluge se prenose privatnom mrežom operatora, a ne Internetom ili drugim javnim mrežama. Takva je privatna mreža posebno dimenzionirana za transfer IPTV a, kako bi krajnjim korisnicima bila pružena usluga visoke kvalitete. Obzirom da se mrežom za transfer IPTV a ujedno prenose i drugi prometni tokovi, poput podatkovnih i govornih (VoIP), video se dodjeljuje najviši prioritet u mreži. Usluga IPTV može biti linearna ili na zahtjev. U oba slučaja usluga je trenutačna (slično kao kod razošiljanja putem TV odašiljača ili u kabelskoj mreži) - IPTV ne predviđa skidanje video-datoteka (*downloading*) s namjenskih poslužitelja. Osim pružanja usluge transfera programa koji idu uživo, IPTV može ponuditi i uslugu video na zahtjev te neke druge usluge koje svaki operator može zasebno razviti. Osnovna prednost IPTV a pred tradicionalnim razošiljanjem TV signala je u interaktivnosti usluge, drugim riječima, krajnji korisnik može prema mreži slati zahtjeve sa sadržajima.

Za nagli porast interesa za IPTV em zaslužni su sljedeći čimbenici:

- sve veća raširenost Gigabit Ethernet (protokol prijenosne brzine 1 Gbit/s) i nove pristupne tehnologije utemeljene na protokolu Ethernet (EFM);
- sposobnost IP mreža u pružanju više razine kvalitete usluge;
- razvoj IP usmjerivača i Ethernet komutatora visokih performansi, posebno prilagođenih IPTV u;
- napredne softverske aplikacije koje upravljaju isporukom videa krajnjim korisnicima.

Slika 5-20 prikazuje osnovne elemente od kojih se sastoji IPTV mreža.



Slika 5-20 Elementi IPTV mreže

Arhitektura IPTV mreže preuzeta je od općenitog modela nazvanog komutirani digitalni video SDV (*Switched Digital Video*). U takvoj se mrežnoj arhitekturi prema pojedinačnim korisnicima šalje samo odabrani kanal (ili kanali, ako korisnik zahtijeva više njih). Slanje videa korisnicima realizirano je slanjem IP paketa na veći broj odredišta (*IP multicasting*), uglavnom pomoću protokola IGMP (*IP Group Membership Protocol*). U krajnjem video-uređaju (*video head-end*) sadržaj, bilo linearni bilo na zahtjev, pretvara se u format pogodan za distribuciju IPTV mrežom. Pritom se najčešće rabi neka od inačica standarda MPEG, MPEG-2 ili MPEG-4. Nakon kodiranja svaki se kanal pakira u IP pakete i šalje kao slijed prema većem broju odredišta (*multicast stream*) ili kao slijed prema jednom odredištu (*unicast stream*). Pristupna mreža za potrebe IPTV-a mora biti izgrađena nekom od naprednih širokopojsnih pristupnih tehnologija, a predviđene su, uglavnom, one ranije opisane u ovom dokumentu. Kućna mreža može biti realizirana kao lokalna Ethernet mreža, pomoću standarda *HomePlug* (PLC-mreža) ili bežično (npr. pomoću standarda IEEE 802.11). Krajnji se korisnik povezuje IPTV uslugom pomoću krajnjeg korisničkog uređaja STB (*Set-top box*). Sam softver koji omogućuje korištenje IPTV usluge podržava arhitekturu klijent/poslužitelj, pri čemu je klijent za korisnika instaliran u STB-u.

Skup usluga IPTV podržava: slanje TV programa, video na zahtjev, plaćanje po odgledanom sadržaju, PPV (*Pay Per View*), transfer televizijske usluge visoke razlučivosti slike (HDTV) i uslugu osobnog videorekordera, PVR (*Personal Video Recorder*). Isporuka takvih usluga krajnjem korisniku zahtijeva da cijela mreža, i temeljna i pristupna, ima na raspolaganju dovoljne prijenosne kapacitete, da transfer IP paketa ima visoku kvalitetu te da je u mrežu ugrađena zadovoljavajuća razina sigurnosti, i na razini transfera i na razini sadržaja. Prigodom korištenja *triple play* usluga, krajnjem je korisniku u dolaznom smjeru potrebna podatkovna brzina između 24 i 30 Mbit/s.

Sljedeća predviđanja pokazuju da je IPTV usluga koja će operatorima donijeti znatan porast prihoda:

- Tvrtka *Informa* predviđa da će do 2010. oko 25,9 milijuna korisnika diljem svijeta koristiti IPTV i generirati prihod veći od 10 milijarda USD;
- Tvrtka *Multimedia Research* predviđa da će broj korisnika IPTV-a porasti s 1,9 milijuna u 2004. na 25,3 milijuna u 2008, godini te da će prihodi porasti sa 635 milijuna na 7,2 milijarda USD;
- Istraživanja tvrtke *Pak Associates* pokazuju da u Španjolskoj gotovo 80% stanovništva pokazuje interes za korištenje naprednih TV usluga, dok u Ujedinjenom Kraljevstvu i Japanu oko 75% ljudi pokazuje sklonost prema prelasku na takve usluge.

Naravno, razvoj IPTV-a i popratnih tehnologija nije ni približno završen. Nužno je potrebno doraditi sve segmente mreže kako bi usluga i njezino korištenje bili što sličniji tradicionalnoj TV usluzi na kakvu su krajnji korisnici naviknuli.

Sljedeći problemi još uvijek nisu u potpunosti riješeni:

- pri prebacivanju s jednog na drugi kanal tijekom gledanja TV programa može nastupiti relativno veliko kašnjenje ako slanje na veći broj odredišta u mreži nije dovoljno dobro riješeno;
- kolebanje kašnjenja paketa u mreži (*delay jitter*) može dovesti do treperenja slike na ekranu TV uređaja;
- prijenos videa oslanja se na transportni protokol UDP koji nema ugrađene mehanizme za siguran transfer paketa.
- Stoga je za pružanje usluge IPTV nužno permanentno praćenje rada mreže i usluge.