

MULTIPLEKSERJI Multiplekserji imajo nalogo povečati izkoristek skupnega prenosnega medija s tehniko delitve fizičnega kanala na več logičnih in neodvisnih kanalov. Predpogoj pa je, da medij omogoča večjo prenosno širino, kot jo povprečno potrebujejo vse delovne postaje skupaj. Fizični kanal tukaj ne pomeni fizičnega kabla, saj se tehnika multipleksiranja uporablja tudi na brezžičnih tehnikah. Obstaja več različnih vrst multipleksov, mi pa si bomo ogledali predvsem :

- časovni multipleks.
- frekvenčni multipleks.
- statistični multipleks.

Frekvenčni multipleks (FDM ali Frequency Division Multipleks) Frekvenčno multipleksiranje je metoda, kjer celotno frekvenčno širino fizičnega kanala razdelimo na večje število pod. kanalov z nižjimi nosilnimi frekvencami in si s tem ustvarimo večje število med seboj neodvisnih prenosnih medijev. Ta tip multipleksa je primeren za širokopasovne prenosne medije, kot je koaksialni kabel, optični kabel ter nekateri tipi brezžičnih prenosov. Ker temelji na delitvi frekvenčne širine je očitno, da je ta metoda primerna za analogne potrebe. Če se uporabljamo za digitalne signale, je treba digitalne signale najprej spremeniti s pomočjo konverterjev. Ta tip multipleksa ustvari na izhodnem prenosnem mediju paralelne in istočasne komunikacijske signale. Ti kanali so neodvisni, zato niso potrebni dodatni kontrolni mehanizmi za ugotavljanje dogajanja na ostalih kanalih preden delovnim postajam dovolijo oddajo sporočil. **Casovni multipleks (TDM all Time Division Multipleks)** Časovno multipleksiranje je metoda, ki vsaki delovni postaji, ki je na TDM priključena, dodeli časovni period, znotraj katerega lahko določena delovna postaja oddaja svoja sporočila (seveda so sporočila lahko pripravljena preden dobi postaja ta čas s strani multiplekserja na razpolago). To pomeni, da za razliko od FDM-a, kjer vsaki delovni postaji dodelimo en mali del celotne frekvenčne širine prenosnega medija za stalno, tukaj določeni delovni postaji na razpolago celotno širino prenosnega medija, vendar le za kratek čas in v določenih časovnih presledkih.

Ta metoda je primerna za prenosne medije z majhno širino prenosnega pasu, oziroma z majhno hitrostjo prenosa podatkov, kot sta telefonska ali podatkovna parica, vendar le v povezavi s počasnimi aplikacijami, terminali ter podobno. Vsota vhodnih hitrosti v multiplekser je lahko največ tako velika, kot je izhodna hitrost. Ker TDM tehnika v bistvu vsaki postaji na mreži omogoča in dodeli nek kratek časovni period, v katerem ima delovna postaja popolno kontrolo nad medijem, se tukaj pojavi problem dolžine, pakiranja in krmiljenja podatkovnih paketov. Zaradi tega se tu velikokrat sreujemo z bit mux-i, ki vsaki delovni postaji dodelijo trajanje enega bita, bajt (byt) mux-i, ki postajam omogočajo posiljanje sporočil dolgih en bajt. paketni mux-i pa omogočajo posiljanje daljših sporočil, vendar vsako ovijejo v poseben okvir, kjer se nahajajo vsi potrebni kontrolni znaki za pravično zaporednost paketov. Prednost TDM-a pred ostalimi je tudi v tem, da lahko prenesa tako analogne kakor digitalne signale. Znotraj iste mreže se lahko nahajata oba tipa multiplekserjev skupaj z nekaterimi

podvariantami. Lahko jih vezemo v kaskade. Število vhodnih kanalov pa mora brti enako številu izhodnih kanalov, ne glede na to, za kakšen tip mux-a gre.

1.3.3 Statistični multipleks

Vsi terminali ali računalniki v mreži se ne uporabljajo enako pogosto. Nekateri pogosto, drugi občasno, tretji so časovno nepredvidljivi itd. TDM in FDM vzpostavljata fiksne prenosne kanale, neodvisno od tega ali so le-ti aktivni (oddajajo sporočila) ali ne. Ta problem pa rešuje statistični multiplekser.

Statistični mux deluje na principu dinamične dodelitve prenosnih kanalov tistim uporabnikom, ki jih potrebujejo. To dodeljevanje se lahko upravlja ročno preko podatkov o obremenitvah ali avtomatično s pomočjo vgrajenih algoritmov za ugotavljanje aktivnosti. Učinkovitost te tehnike je veliko višja kakor pa statičnih muxov. Ta mux dodeljuje vire (čas ali prenosno širino) proporcionalno aktivnosti delovne postaje. Pojavi se težava nadzora nad delovanjem.

Ker nikoli ni znano, koliko kanalskih kapacitet bo neka delovna postaja potrebovala, je potrebno uporabiti velike memorije, pri velikih obremenitvah vzpostaviti in upravljati čakalne vrste ter podobno, kar ima vpliv na visoke cene tovrstnih multiplekserjev.

3 OSNOVNI GRADNIKI LOKALNIH MREŽ

3.1 PRENOSNI MEDIJ

Prenosni medij je edini in osnovni del, brez katerega ne more obstajati nobena mreža. Osnovna funkcija prenosnega medija je fizični prenos signalov med komunicirajočimi delovnimi postajami ter s tem

povezava vseh enot v zazdeljeno celoto.

Pravilen izbor prenosnega medija, ključno vpliva na celotno delovanje lokalne mreže!

Glede ozicjenja bi LAN-e lahko razdvojili v dve skupini.

- V prvi je značilno, da znotraj iste mreže lahko uporabimo različne prenosne medije, all pa za drugafine postavitve iste lokalne mreže uporabimo različne prenosne medije.

- V drugi skupini so LAN-i, ki uporabljajo samo en tip prenosnega medija.

Ko izberemo odgovarjajoči LAN, nas proizvajalec s priporočili opozori, katere prenosne medije je za to mrežo možno uporabiti. V teh priporočilih je zajeto:

- maksimalne razdalje posameznega kosa kabla, slabljenja na kablu, kar nam služi za izračune v času projektiranja lokalne računalniške mreže.

- velikokrat so, posebno pri močnejših lokalnih računalniških mrežah, za le-te razviti prav posebni prenosni kabli, jih ne rezemo in ne lotamo, temveč jih že pripravljene za vključitev dobimo od proizvajalca, tako da notranjosti teh kablov ne vidimo.

Glavni tipi prenosnih medijev so:

- koaksialni kabel,
- parica (telefonska in podatkovna),
- optični kabel.
- brezicni prenosniki.

3.1.1 Koaksialni kabel

Koaksialni kabel je izredno popularen prenosni medij lokalnih računalniških mrež. Dosti se je uporabljal pri hitrih baseband mrežah in praktično se vedno pri Broadband mrežah. Danes ga v glavnem z nadomeščamo z UTP in optičnimi kabli.

Opis kabla:

Sestavljen je iz osnovnega bakrenega ali aluminijastega vodnika, ki gre skozi izolacijski material, katerega naloga je izolacija pred nasprotnim polom (kovinski pleteni plasc) in določanje impedancne upornosti (50 Ω, 75 Ω, itd.)

Kovinski, običajno pleteni plasc, zagotavlja razen nasprotne polarizacije izredno močno zaščito pred zunanjimi električnimi, radiofrekvenčnimi in radiacijskimi vplivi. Zunanji zaščitni izolacijski material, prevlečen preko vseh teh sestavin pa ščiti koaksialen kabel pred vplivi okolja.

Za razliko od ostalih prenosnih medijev je koaksialni kabel največkrat izpeljan z enim samim centralnim vodnikom ali drugače povedano, zelo malo se v lokalnih računalniških mrežah pojavljajo kabli, znotraj katerih bi bilo več koaksialcev. Zato pa zaradi izjemne prenosne širine tega kabla lahko uporabimo tehniko multipleksiranja, s pomočjo katere lahko vzpostavimo veliko število logičnih kanalov.

Poznamo dva tipa 50-kih koaksialnih kablov:

- debeli koaksialni kabel (Thick).
- tanki koaksialni kabel (Thin).

3.1.1.1 Debeli koaksialni kabel

Je cca 13 mm debel koaksialni kabel rumene barve.

- brez ojačevalca lahko prenaša signal do razdalje 500 m.
- na tanki koaksialni kabel se priklaplja preko posebnih priključkov imenovanih "vampir", ki so namešteni na oddajniku,
- povezava od oddajnika do mrežne kartice je izvedena preko oddajnega kabla na AUI konektor (DB 15 konektor).

Ostali koaksialni kabel

3.1.1.2 Tanki koaksialni kabel

i

Je cca 7mm debel gibljivi koaksialni kabel običajno rjave barve.

- brez ojačevalca lahko prenaša signal do razdalje 185 m,
- za baseband mreže običajno uporabljamo tanki koaksialni kabel tipa RG 58 z impedanco 50 Ω.

Poznamo več vrst tankih koaksialnih kablov glede na izvedbo :

- RG-58 A/U finozični tokovodnik
- RG-58 /U ploiini tokovodnik
- RG-58 C/U vojaška izvedba RG-58 A/U
- RG-59 broadband kabel
- RG-6 uporabljen za broadband mreže z višjimi frekvencami
- RG 62 kabel za Arcnet mreže

Point vodnik (RG-58/U)

Finof^ant vodnik

(RG-58 MJ)

Slika 3- 4: Vrste tankih koaksialnih kablov

Prednosti koaksialnega kabia:

- velika Sirina prenosnega pasu (bandwith), ki sega preko 400 Mhz.
- visoka hitrost prenosa podatkov (10-50 Mbps).
- neobfiutljivost na električne in radijske motnje.

• «*

*

Pomanjkljivosti koaksialnega kabia:

- veliko dražji od parice,
- relativno zahtevna postavitcv,
- kratka dolzina nepretrganega kabelskega segmenta/""

3.1.2 Parica

Parica je v osnovi dvojna izolirana prepletena žica, ki je nastala za potrebe telefonskih komunikacij. Je eden najstarejših prenosnih medijev za posiljanje sporočil. Najbolj je razširjen tudi v lokalnih računalskih mrežah. resda predvsem pri preprostejših in cenejših LAN-ih, katerih je največ. Geprav ga v zadnjem času vedno uspešneje zamenjuje njegov naslednik, podatkovna parica. LAN tehnologija, ki pretežno in še naprej intenzivno uporablja ta prenosni medij, je PBX.

Slika 3- 5: Telefonska parica

Prednosti telefonske parice:

- nizka cena,
- ze obstoječa kablaza.
- preprosta namestitcv.

Pomanjkljivosti telefonske parice:

- občutljivost na motnje.
- nizka hitrost prenosa podatkov.

Pomanjkljivosti telefonske parice, ki izvirajo iz govorne orientiranosti tega medija, so deino odpravljene s podatkovno, ki je zelo podobna. Ie da je ovita z dodatnim kovinskim plascem. Kovinski plasc prepreeuje tako električne kot radiofrekvenčne motnje iz okolja, kot oddajanje lastnih signalov v okolje. S tern smo sicer deino izgubili obe prednosti klasične telefonske parice, pridobili pa smo za nekaj visjo ceno na vseh ostalih parametrih. zaradi cesar se ta tip prenosnega medija veliko uporablja.

UTP

Oktop

Slika 3- 6: Oklopljena in neoklopljena sukana parica

3.1.2.1 Kategorije kablov UTP:

1. kategorija : Standardni telefonski DTP kabli, ki uporabljajo za prenos glasu ne pa podatkov.
2. kategorija : Kabli za prenos podatkov do 4Mb/s. Vsebuje 4 prepletene parice.
3. kategorija : Kabli za prenos podatkov do 10Mb/s. Vsebuje 4 prepletene parice s tremi prepleti na cevelj.
4. kategorija : Kabli za prenos podatkov do 16Mb/s. Vsebuje 4 prepletene parice. Vsebuje 4 prepletene parice s tremi prepleti na cevelj.
5. kategorija : Kabli za prenos podatkov do 100Mb/s. Vsebuje 4 prepletene parice bakrene žice s tremi

prepleti na cevelj. " ^, — ——— - ••^

3.1.2.2 Impedance UTP kablov so:

- IQ.QP,.
- ' • 1200.'
- 150Q.

3.1.2.3 Oznacevanje UTP kablov:

- UTP - neoklopljen prepleten par
- STP - oklopljen prepleten par
- FTP - prepleten par odporen na motnje
- F-STP - vsak par oklopljen s folijo, folija tudi okoli bakrenega opjeta
- EMC - elektromagnetna zascita

Slika 3-7; Vtičnica in vtikac RJ45 za UTP kable

3.1.3 Opticni kabel

Optični kabel uporablja za prenos informacij svetlobo.

3.1.3.1 Svetloba:

Svetloba je elektromagnetno valovanje v mikrometerskem (μm) valovnem področju. Vidni del svetlobnega spektra obsega aktivno valovno področje v razmerju valovnih dolžin 1:2 med vijolično ($\lambda = 0,38 \mu\text{m}$) in rdečo ($\lambda = 0,76 \mu\text{m}$) svetlobo. Pripadajoče frekvenčno področje obsega pas med 400 THz in 800 THz. V svetlobni spekter stojimo poleg vidne še nevidno infrardečo ($\lambda > 0,76 \mu\text{m}$) in ultravijolično ($\lambda < 0,38 \mu\text{m}$) svetlobo. Infrardeči spekter se razteza vse do milimetrskih ali submilimetrskih valov radijskega spektra. ultravijolični spekter pa vse do zarkov X.

Danes se optične komunikacije izvajajo v infrardečem področju. Delijo se na tri področja: $\lambda > 1,5 \mu\text{m}$ (spektralna okna), ki so se uveljavila iz praktičnih razlogov ter zaradi nekaterih optimalnih lastnosti kremenovega stekla. Uveljavili so se pasovi:

- 850 nm (prvo spektralno okno), se je uveljavilo v zgodnjem razvoju optičnih komunikacij zaradi obstoječe tehnologije izdelave polprevodniških GaAs laserjev za to valovno dolžino.
- 1300 nm (drugo spektralno okno), se je uveljavilo zaradi ničelne snovne disperzije vlakna,
- 1550 nm (tretje spektralno okno), se je uveljavilo zaradi najmanjšega slabljenja optičnega vlakna na tem področju.

Optični kabel je zaradi svojih lastnosti izredno atraktiven medij v najhitrejših lokalnih mrežah in backbone mrežah. Primeren je predvsem za point-to-point zveze. Sestavljen je iz posebnega vlakna, izdelanega iz posebne plastike ali večnega stekla, mehanicno trdnost in odpornost na erozivno delovanje od zunaj mu zagotavlja eden ali več slojev izolacije.

Kabli z optičnimi vlakni so najprimemnejši medij za povečanje prenosnih hitrosti v lokalnih omrežjih in omrežjih na širšem območju. Pred bakrenimi kabli imajo vrsto prednosti:

- so popolnoma neprevodni,
- neobčutljivi so na elektromagnetne motnje in udar strele,
- ne poznajo presluha.
- njihovo slabljenje ni odvisno od hitrosti prenosa,
- so lahki in omogočajo večjo gostoto vgradnje,
- se odlikujejo po visoki pasovni širini.
- omogočajo popolno varnost podatkov.

3.1.3.2 Vrste optičnih vlaken

- optična vlakna uporabljamo kot dielektrične valovode.
- optična vlakna za komuniciranje so izdelana iz zelo čistega kremenovega stekla in njihov zunanji premer je standardiziran na $125 \mu\text{m}$,
- zaščitena so vsaj s primarno zaščito premera 250 μm in običajno se s sekundarno zaščito različnih premerov,
- za zaščito steklenih optičnih vlaken se uporabljajo umetne plastične mase. Optično vlakno je sestavljeno iz dveh različnih stekel:
- Centralno področje imenujemo jedro, zunanje področje obloga.

- Celotna struktura pa je še vedno steklo, ki pa ima različne lomne količnike.
- Lomni količnik jedra je večji od lomnega količnika obloge.

V osnovi poznamo dva različna tipa vlaken:

- enorodovno in
- mnogorodovno vlakno.
- Enorodovno • Mnogorodovno

- enorodovno vlakno ima jedro premer samo 9 μm in dovoljuje širjenje samo enega rodu svetlobnega valovanja. Standardno enorodovno vlakno je dimenzionirano za prenos pri 1,30 μm .
- Premaknjeno vlakno pa je dimenzionirano za prenos pri 1,55 μm . To omogoča aplikacije od lokalnih pristopnih omrežij (analognih in digitalnih) do dolgih visokokapacitetnih zvez,
- mnogorodovno vlakno ima premer jedra 50 μm ali 62,5 μm . Dovoljuje širjenje nekaj sto rodovom svetlobnega valovanja. Večja velikost jedra omogoča lažje spajanje vlaken in usmerjanje svetlobe iz izvorov (LED, VCSEL, laser,...). Mnogorodovna vlakna se uporabljajo v lokalnih omrežjih in računalniških omrežjih.

Tako enorodovno kot tudi mnogorodovno vlakno ima zunanjo oblogo, ki jo imenujemo primarna zascita. Le-ta služi za izboljšanje mehanskih lastnosti vlakna.

3.1.3.3 Izgube v optičnih vlaknih:

V optičnem vlaknu se pojavlja slabljenje zaradi:

- Rayleighovo sipanje, ki razprši svetlobo, ki potem izhaja iz vlakna,
- absorpcija, ki svetlobo pretvarja v toploto.
- absorpcija zaradi Hidroksidnih (OH) ionov, ki so prisotni v steklu. Prisotni so le določeni ioni, ki imajo izrazite absorpcijske vrhove. Najbolj značilen vrh je pri 1400 nm, ki locuje drugo in tretje spektralno okno.

4 POVEZOVALNIKI

4.1 Ponavljalnik (repeater) in Koncentrator (hub)

Naloga ponavljalnika je, da signal, ki ga sprejme na enem vmesniku, ojači in obnovi ter preusmeri na preostale vmesnike. Pri tem pride do majhnih zakasnitev, zato je število ponavljalnikov v omrežju omejeno.

Oslabljen signal Repeater

Pri načrtovanju omrežja moramo strogo upoštevati pravilo o maksimalnem številu ponavljalnikov, saj v nasprotnem primeru lahko pride do motenj v delovanju omrežja. Ponavljalnike uporabimo v primerih:

- ko se pojavijo potrebe po povečanju:
 - o števila delovnih postaj, o fizične razsežnosti omrežja,
- ko želimo povezovati omrežja iz različnih prenosnih medijev.

Glede na različne prenosne medije je namreč omejeno maksimalno število postaj, ki jih lahko povežemo med seboj in dolžina prenosnega medija, ki te postaje povezuje. Ponavljalniki se med seboj ločijo:

..... :-,.....

- po številu segmentov, ki jih povezujejo.
- po tipu konektorjev (ki so vezani na prenosni medij)

Najbolj tipičen ponavljalnik je bil z dvema priključki. Z razvojem novih standardov in s tem prenosnih medijev, se je pojavila potreba po povezovanju omrežij, ki uporabljajo različne prenosne medije (tanki in debeli koaksialni vodnik, parica, optika).

Danes je najbolj pogosto uporabljen ponavljalnik prav gotovo 10BaseT koncentrator (hub), ki je v bistvu ponavljalnik z več vmesniki. Navadno imajo koncentratorji 8, 12, 16 ali 24 vmesnikov.

Slika 4-1: Koncentrator

4.2 Klasično Ethernet omrežje s koncentratorjem:

Delovne postaje, ki so povezane med seboj s prenosnim medijem in na tej povezavi ne vsebujejo nobene naprave za medomrežno povezovanje, tvorijo svoj segment omrežja.

Slika 4-2: Segment omrežja

6e postaje locuje koncentrator. pravimo, da so postaje na istem logicnem segmentu, saj potujejo vsi

paketi podatkov do vseh naprav.

Ponavljalniki so vedno manj uporabljajo zaradi številnih pomanjkljivosti:

- stevilo ponavljalnikov v omrežju je omejeno in zato niso primerni za gradnjo večjih omrežij,
- ne moremo povečati prepustnosti omrežja,
- ne moremo ločevati prometa med posameznimi segmenti oziroma razdeliti omrežja na podomrežja,
- fizična razsežnost omrežja je odvisna od topologije in uporabljene tehnologije, omejena na nekaj 100 m do nekaj kilometrov.

>

Ker ponavljalnik ne preverja vsebine paketa, ampak signal le ojači in obnovi, ga prištevamo med naprave, ki delujejo na 1. (fizičnem) nivoju referencnega modela ISO/OSI. Ponavljalniki ne prevajajo ali filtrirajo.

Ponavljalnik ne omogoča komunikacije med dvema različnima komunikacijskima protokoloma, kot sta na primer 802.3 LAN (Ethernet) in 802.5 LAN (Token ring).

5 NAPRAVE ZA MEDMREZNO POVEZOVANJE

So naprave, ki povezujejo lokalna omrežja oziroma posamezne segmente lokalnih omrežij med seboj. Najbolj pogosto uporabljene naprave so:

- premoscevalnik (bridge)
- usmerjevalnik (router),
- preklopno stikalo (switch)
- protokolni konverter (gateway)

5.1 Premoscevalnik - most (bridge)

Premoscevalnik (bridge) je novejšega izvora kot ponavljalnik. Je zahtevnejša naprava, saj podatke (pakete) ne le ojači in pošlje na ustrezen vmesnik, temveč jih najprej shrani v medpomnilnik. Podatke (pakete) v medpomnilniku preveri in v primeru, da premoscevalnik ne ugotovi napake, paket pošlje naprej na ustrezen vmesnik (enega ali več) premoscevalnika, glede na ciljni naslov. Ker se paket najprej shrani, in ker je potreben določen čas, da premoscevalnik ugotovi, na kateri vmesnik poslati paket, so premoscevalniki počasnejši od ponavljalnikov. Najbolj sta se uveljavili dve vrsti premoscevalnikov:

- transparentni premoscevalniki (transparent bridges),

sami določajo pot po kateri bo potoval paket. Taksno ime imajo zato, ker so končnim postajam 'nevidni' oziroma transparentni. Transparentni premoscevalniki uporabljajo STA (*Spanning Tree Algorithm*) algoritem za iskanje optimalnih poti pri prenosu paketov. Sporocila, ki si jih med seboj posiljajo premoscevalniki, se imenujejo BPDU (*Bridge Protocol Data Units*). Priključimo jih med enake lokalne računalniške mreže, ne da bi pri tem spreminjali obstoječe stanje. STA algoritem se uporablja za povezovanje omrežij Ethernet.

- Premoscevalniki SRB (Source Routing Bridges)

^

^^

pa delujejo nekoliko drugače. Ze iz imena je razvidno, da mora končna postaja, ki želi poslati paket, sama ugotoviti optimalno pot. Informacijo o optimalni poti mora vključiti v poslani paket. Naloga premoscevalnikov je, da na podlagi informacije, ki je vsebovana v paketu samem, paket 'dostavijo' na segment na katerem se nahaja naslovljena končna postaja. SRB algoritem se uporablja za povezovanje omrežij Token Ring.

- Slika 5-1: Premoscevalnik (bridge)

Ker so transparentni premoscevalniki mnogo počasnejši od premoscevalnikov SRB, si osnovno delovanje premoscevalnikov ponazorimo na primeru delovanja transparentnih premoscevalnikov.

Premoscevalnik sprejme vse pakete iz vseh segmentov na katerih se nahaja s svojimi vmesniki. Premoscevalnik ima za vsak svoj vmesnik vpisane MAC naslove postaj, ki se nahajajo na istem segmentu kot pripadajoči vmesnik. Premoscevalnik pregleda vsak paket in se odloča po naslednjih kriterijih:

- Če razpozna, da je ponorni naslov vpisan v tabeli za vmesnik, ki je sprejel ta paket, pomeni, da se naslovljena postaja nahaja na istem segmentu in paket zavrže,
- če se ponorni naslov ne ujema z ponornimi naslovi v tabeli vmesnika, ki je paket sprejel, pogleda v tabelo ostalih vmesnikov in:

o pošlje paket na tisti vmesnik, v katerega tabeli se naslov nahaja,

o poslje paket na vse vmesnike. ce se ponorni naslov ne nahaja v nobeni izmed tabel vmesnikov Naslov MAC (Media Access Control) je enoumno določen naslov računalnika, definiran na nivoju strojne opreme. V omrežjih Ethernet je to njegov naslov v krajevni mreži. Ko je računalnik povezan na internet, se naslovu MAC priredi naslov IP. Naslovi MAC so 48 bitni, v sestnajstiskem številskem sistemu pa so predstavljeni z 12 mestnim številom.

P.[^]Jp.y[^]J[^]pr.[^]pp.p.[^]pY.[^]JpJ.K?..¹

Med postopkom inicializacije pregleduje premoševalnik vse MAC naslove paketov. Vsak novi izvorni naslov shrani v interno tabelo, razdeljeno na posamezne segmente. Če je povezanih zelo veliko število delovnih postaj, postanejo tabele obsežne in delovanje premoševalnika se upočasni.

Paketi potujejo med premoševalniki po različnih poteh. Da ne bi prislo do kroženja paketa zaradi vzporednih poti se uporablja STA (*Spanning Tree Algoritem*) algoritem, ki ima nalogo da:

- ustvari topologijo brez zank (med dvema točkama je možna le ena pot, ostale povezave niso aktivne)
- v primeru izpada aktivne povezave aktivira neaktivno povzavo tako, da je možna povezava med poljubnima premoševalnikoma, vendar samo po eni poti.

Katere postaje bodo aktivne in katere neaktivne, izračuna STA algoritem na podlagi uteži, ki jih določi administrator omrežja. Tjih izbere tako, da so aktivne tiste povezave, ki jih zeji. Informacijo o stanju povezav in izmenjavo tabel med premoševalniki zagotavljajo sporočila BPDU, ki se periodično izmenjujejo med premoševalniki.

Ker premoševalniki operirajo z MAC naslovi, ki so definirani na 2. (logični) plasti referenčnega modela OSI, pravimo, da so premoševalniki naprave, ki delujejo na 2. plasti modela OSI.

Premoševalnik ima naslednje lastnosti:

- število premoševalnikov v omrežju ni omejeno,
- fizična razsežnost omrežja, ki ga povezujejo premoševalniki je takorekci neomejena,
- s premoševalniki lahko deino povečamo prepustnost omrežja,
- omogočajo povezavo različnih LAN omrežij med seboj: Ethernet, Token Ring, FDDI....
- Med seboj jih ločimo po:

o številu segmentov, ki jih povezujejo,

o LAN tehnologijah, ki jih podpirajo: Ethernet, Token Ring, FDDI....

o algoritmih za določanje poti po kateri bo potoval paket.

Poznamo:

- lokalne premoševalnike (angleško *local bridge*), ki med seboj povezujejo segmente lokalnega omrežja in
- oddaljene (angleško *remote bridge*), ki med seboj povezujejo oddaljena lokalna omrežja.

Telefonska linija

Premoševalniki so počasne naprave, zato jih v lokalnih omrežjih izpodrivajo preklopna stikala, v prostranih omrežjih (povezovanje oddaljenih lokalnih omrežij) pa usmerjevalniki.

5.2 Usmerjevalnik (router)

Usmerjevalnik je naprava, ki v kompleksnem omrežju poišče najboljšo pot za posiljanje podatkov. Usmerjevalnik izbere najboljšo pot glede na podatke, ceno in veljavne poti. Tudi usmerjevalniki podobno kot premoševalniki filtrirajo pakete in jih prepuščajo le v segmente, v katere so namenjeni. S tem zmanjšujejo promet v omrežju. Za razliko od premoševalnikov pa usmerjajo pakete na podlagi IP naslovov.

Delujejo lahko tudi kot požarni zid (firewall).

Požarni zid je pregrada, ki preprečuje nezazelenim paketom vstopati ali izstopati v/iž določenih delov mreže. Zato je tipična uporaba usmerjevalnika na mestu, kjer se krajevna mreža priključuje na internet. Z vpisom v sezname dostopa določimo, kateri zunanji in notranji računalniki so dostopni in kateri protokoli so dovoljeni. Npr. dostop iz zunanjih omrežij do notranjega spletnega streznika je omogočen, prepovedan pa je dostop do drugih streznikov. Za to povezavo je potreben protokol IP.

-
-

5.2.1 Prednosti usmerjevalnikov pred premoševalniki so predvsem naslednje:

- omogočajo delitev omrežij na podomrežja na podlagi omrežnih naslovov, ki jih lahko uredimo na logičen, hierarhičen in človeku razumljiv način.
- sporočila razpršenega oddajanja (*broadcast*) so omejena na podomrežja. Predstavljajmo si npr.

omrežje Internet zgrajeno iz premoscevalnikov. Vsako taksno sporočilo bi doseglo prav vse postaje v Internetu. Količina tega prometa bi prav gotovo nekajkrat presešla 'kristni' promet v Internetu,

- usmerjevalniki imajo vgrajene funkcije za filtriranje prometa. S tem lahko določimo promet med podomrežji (preprečimo, da se promet med podomrežjama T93.27.5.1% za storitev www' fri' prepove za storitev ftp). Filtre uporabljamo za povečanje varnosti omrežij.

- omogočajo prenos paketov po vzporednih poteh, s čimer povečamo prepustnost omrežja,

- premoscevalniki so neprimerni za povezavo oddaljenih lokalnih omrežij, kjer se uporablja klicni način vzpostavitve zveze med oddaljenima lokacijama (analogni klic. ISDN), ker je nemogoče definirati pravila za selekcijo paketov. Npr. kateri paketi so tisti, ki naj sprožijo postopek vzpostavitve zveze (sprožiti jo morajo paketi, ki so namenjeni oddaljenemu lokalnemu omrežju) in kdaj se naj zveza prekine (ko ni več paketov namenjenih oddaljenemu lokalnemu omrežju).

Glavna naloga usmerjevalnikov je usmerjanje protokolov (IP, IPX, DecNet, AppleTalk, OSI, XNS). Ker pa vseh protokolov ni mogoče usmerjati (LAT, LLC, MOP, NetBeui, NetBios), morajo usmerjevalniki omogočati tudi prenosanje protokolov. Tako usmerjevalniki danes združujejo funkcijo usmerjanja in funkcijo prenosanja.

Protokolov, ki ne vsebujejo informacije omrežnega sloja, to so LAT, LLC, MOP, NetBeui, NetBios, ni mogoče usmerjati. Zaradi tega se brez uporabe teh protokolov izrazito zmanjšuje. »

Usmerjevalniki operirajo z mreznimi naslovi, ki so definirani na 3. plasti referenčnega modela OSI. In zato pravimo, da je usmerjevalnik naprava, ki deluje na 3. (mrežni) plasti modela.

Usmerjevalniki se uporabljajo tako v lokalnih omrežjih (LAN), kot v prostranih omrežjih (WAN).

y

Usmerjevalniki komunicirajo z drugimi usmerjevalniki in ne z oddaljenimi računalniki.

Za izgradnjo usmerjevalne tabele uporabljajo posebne algoritme. Ti so:

- OSPF (open shortest path first).
- RIP (routing information protocol),
- NLSP (NetWare link services protocol).

V lokalnih omrežjih so jih začela izpodrivati preklopna stikala, ki delujejo na enak način kot premoscevalniki. Lahko pa imajo vgrajeno tudi funkcijo usmerjanja.

Vzroki:

- usmerjevalniki so bili prvotno namenjeni predvsem povezovanju prostranih omrežij. V prostanih omrežjih pa je prepustnost (število paketov v sekundi) bistveno manjša kot znotraj lokalnega omrežja,
- usmerjevalniki navadno podpirajo veliko število protokolov in funkcij, ki jih v lokalnih omrežjih navadno ne potrebujemo in so zaradi tega izredno dragi (cena na posamezen priključek LAN usmerjevalnika).
- klasični usmerjevalniki ne omogočajo tvorbe navideznih omrežij. Če želimo prestaviti uporabnika z enega segmenta na drugega, moramo spremeniti nastavitve delovne postaje, kar pri navideznih usmerjevalnikih ni potrebno.

«

5.2.2 Navidezni usmerjevalnik (virtual ruter)

je ponavadi vgrajen v obliki modula v centralno preklopno stikalo. Navidezni usmerjevalnik ima namesto fizičnih vmesnikov navidezne vmesnike. Če bi v omrežju z navadnim usmerjevalnikom želeli enega od uporabnikov preseliti na drugo fizično lokacijo, bi to za seboj potegnilo tudi vključitev na drug segment omrežja in spremembo nastavitvev za to delovno postajo. Če bi imeli nastavljene kakšne filtre na usmerjevalniku, pa še spremembo nastavitvev usmerjevalnika. Ker navidezni usmerjevalnik uporablja navidezne vmesnike in ne fizične vmesnike, ni potrebno pri selitvi uporabnikov prekonfigurirati niti delovnih postaj, niti navideznega usmerjevalnika. Uporabniki se lahko nahajajo kjerkoli v krajevni mreži. Delovne skupine določimo programsko.

Usmerjevalniki se med seboj razlikujejo predvsem po tem:

- katere LAN tehnologije podpirajo: Ethernet, Fast Ethernet, Token Ring, FDDI, ATM,...
- katere WAN tehnologije podpirajo: ISDN, Frame Relay, X.25, ATM,...
- katere protokole usmerjajo: IP, IPX, DecNet (faza 4, faza 5), AppleTalk.
- katere protokole uporabljajo za izmenjavo informacije med usmerjevalniki (RIP v1, RIP v2, IGRP, OSPF, EGP, BGP, ES-IS, IS-IS, ...).
- katere vnaprej pripravljene filtre imajo za posamezne protokole.

- kolikсна je prepustnost, kar pomeni Stevilo paketov, ki jih lahko usmerijo v sekundi.

V zadnjem 6asu je dobil usmerjevalnik nekatere dodatne funkcije:

- prenos govora preko protokola IP (VoIP)
- prenos govora preko omrežja Frame Relay (VoFR) Sifriranje (*enkripcija*) podatkov.

To pomeni, da imajo usmerjevalniki programsko opremo in vmesnike, ki omogočajo priklop telefonov in telefonskih central. Imajo pa tudi programsko all celo posebno

strojno opremo za enkripcijo podatkov, s cimer zagotovimo varnost podatkov na prenosni poti. 5.2.3 Algoritmi za usmerjanje morajo zadostiti naslednjim kriterijem:

- Izbira optimalne poti: na podlagi parametrov, ki jih doloci upravljalec omrežja, morajo usmerjevalniki v omrežju dolociti optimaino pot, po kateri bo posamezen paket potoval. To je vsekakor najbolj zahtevna in pomembna naloga.
- Enostavnost: algoritem za izmenjavo informacij med usmerjevalniki naj bo najbolj enostaven (da ne obremenjuje procesne mod usmerjevalnikov) in naj povzroča kar najmanj prometa (ki predstavlja nekoristen promet na prenosni poti med usmerjevalniki).
- Robustnost: algoritmi morajo delovati zanesljivo v vseh pogojih, v katerih se lahko znajde omrežje.
- Hitra konvergenca algoritma za usmerjanje: pri dolocanju optimalne poti sodeljujejo vsi usmerjevalniki. Ko pride v omrežju do izpada katere od komponent omrežja, (modemska zveza, vmesnik na usmerjevalniku, usmerjevalnik,...). morajo vsi usmerjevalniki dobiti informadjo o tern dogodku in na novo izracunati optimaino pot. V primeru, da je algoritem konvergira prepocasi, lahko pride do krozenja paketov.
- Fleksibilnost: algoritem se mora hitro in na ustrezen nacin prilagoditi spremembam v omrežju. Te spremembe so lahko npr.: sprememba prepustnosti in zakasnitve na doloceni povezavi.

5-2.3.1 Usmerjevalniki za iskanje optimalne poti uporabljajo razlicne vrste algoritmov za usmerjanje:

- staticni in dinamicni algoritmi (statifini in dinamifini usmerjevalniki):

• Staticni algoritmi so neprilagodljivi, saj se spremenijo le s posegom upravljaica -> .. omrežja in se uporabljajo v enostavnejših omrežjih, ki se le malo spreminjajo. Pri staticnih usmerjevalnikih moramo rocno nastaviti usmerjevalne tabele, o dinamicni algoritmi se sami prilagajajo razmeram v omrežju. Dinamicni usmerjevalniki avtomaticno ugotovijo poti in sami sestavijo tabelo. Tf so bolj - razviti, saj uporabijo podatke drugih usmerjevalnikov. Pri vsakem podatku se odlocijo kako poslati podatek po omrežju.

t centralizirani in distribuirani algoritmi:

o centralizirani algoritmi: izbira optimalne poti se raCuna v centraini napravi, ki periodicno zbira informacije od vseh usmerjevalnikov, izracuna optimalne poti in jim poslje tabelo optimalnih poti. Prednost je v tern, da se usmerjevalnikom ni potrebno ukvarjati z računanjem optimalne poti, poleg tega pa je zagotovljeno, da obstaja le en izračun optimalne poti. Slabosti pa so, da je celotno omrežje odvisno od izpada ene naprave, da mora biti prepustnost omrežja do te naprave velika in da usmerjevalniki, ki so v drevesni topologiji blizje, prej dobijo novo informacijo o optimaini poteh kot usmerjevalniki, ki so daleč. To lahko v posameznih primerih povzroci krozenje paketov.

- algoritmi, ki dopuscajo eno ali ve6 poti:

o nekateri algoritmi dopusčajo ve6 vzporednih poti po katerih potujejo paketi med dvema koncna tockama. Ti algoritmi so bolj zahtevni. Njihova prednost je v tern, da zagotavljajo boijso prepustnost omrežja in redundanco.

- enonivojski in hierarhicni algoritmi:

o pri enonivojskih algoritmih vsi usmerjevalniki izmenjujejo informacijo med seboj, o pri hierarhicnih algoritmih poteka izmenjava informacijetako, da imajo nekatere naprave prednost pred ostalimi.

- kdo izbere celotno prenosno pot:

o v doloteni starejsih sistemih je bila izbira prenosne poti prepuscena postaji, ki je ?elela poslati sporoCilo, medtem ko se danes skoraj izklju6no uporablja na6in, pri katerem je izbira poti prepuš6ena usmerjevalnikom.

- izmenjava usmerjevalnih tabel:

o usmerjevalnik poslje vsem ostalim usmerjevalnikom v omre^ju le tisti del tabele za usmerjanje (link state algoritmi), ki se nanaSa le na stanje lastnih povezav. Prednost je v tern, da teije pride do zank. Slabost pa je, da se poSilja velika koli6ina informadje, so bolj kompleksni za izracunavanje (potrebna vefija procesna moC in veC spomina) in so tako drাজji s stalis6a implementacije. Primeri usmerjevalnih

protokolov, ki uporabljajo ta algoritem:

OSPF, IS - IS, DecNet faza V.

o usmerjevalnik poslje celotno tabelo za usmerjanje le sosednjim usmerjevalnikom (distance vector algoritmi). Primeri usmerjevalnih protokolov, ki uporabljajo ta algoritem: RIP, IGRP, DecNet faza IV, RTMP.

5.2.3.2 Kriteriji na podlagi katerih naj algoritmi racunajo optimaino pot:

- Zanesljivost vsake omrezne povezave: dolocene povezave veckrat izpadejo kot druge. Za ocenitev zanesljivosti se lahko uporabijo tudi drugi kriteriji. Kriterije navadno vnese upravljalec omrezja.

..... .. „;:..

- Zakasnitev je eden od najbolj pogosto uporabljanih kriterijev in je odvisna od prepustnosti povezav, zasedenosti omrezja, nastavitve usmerjevalnikov (npr. prioriteta za doloCen tip prometa) in fizicne razdalje.

- Prepustnost: vefija prepustnost ni zadostno zagotovilo, da bo ta pot optimalna. saj je

- - potrebno upoštevat se zasedenost povezav. - ;:•.-. . ,. .- . ^-.,

- ' Obremenjenost usmerjevalnika: uporabimo lahko kriterije kot so npr. razpolozljiva in/ali najveqa zmogljivost CPU, stevilo paketov na sekundo in podobno

- MTU: upoštevat je potrebno najveqijo velikost paketov (*Maximum Transfer Unit*), ki bodo potovali Cez posamezne omrezne povezave. Omejitev Etherneta 1.5 kB, FDDI-ja 4 kB, medtem ko je pri Token Ringu prakticno neomejena.

- Stro^ek posamezne povezave: kot primer naj navedemo, da se bo podjetje, ki zeii poslovati z nizkimi stroški, raje odlocilo za uporabo ene od privatnih povezav, ceprav ima mo^nost uporabe javnih povezav z manj^o zakasnitvijo.

Primer

Imamo majhno TCP/IP mrezo, ki se sestoji iz INTRANET segmenta in treh izhodov -vozlis6. IP-mreza Stevilka tega segmenta je 200.1.2. UporabniSke steviike - host numbers za uporabnike A, B in C so 1,2 in 3. To so naslovi razreda - C in nam tako dovoljujejo, da imamo 254 vozli^6 - kon6nih naprav, terminalov na tem segmentu mre^e. Vsak od teh vozlov ima svoj pripadajo6i intranet naslov, ki so ponavadi 6-bitov dolgi. Ponavadi so zapisani v heksadecimaini obliki, loteno s pomiSljaji. (02-FE-87-4A-8C-19 primer)

200.1.2.1 200.1.2.2 200.1.2.3

NETWORK 200.1.2

Slika 5-3: Intranet mreza

A zeii poslati paket podatkov k C in pozna njegov (P-naslov. Da bi pdslal paket po intranetu, mora A vedeti tudi C-jev intranet naslov. ARP (The Address Resolution Protocol) se uporablja za dinamicno odkrivanje teh naslovov. ARP vsebuje interno tabelo IP-naslovov in njim pripadajoce intranet naslove. Ko A poskusa poslati IP - paket k C-ju, takrat ARP pogleda v svoje tabelo za C-jev I P-naslov in tako odkrije vhod. ARP bo potem poslje poseben zahtevni paket po mrezi, katerega prejme vsako kon6no vozlisce. Ce ima neko konCno vozlisfie pripadajoOi I P-naslov , ki je v na^em primeru C, bo le to vrnilo v svojem odgovornem paketu svoj intranet naslov nazaj k A. Takoj ko A prejme ta paket z C - ju pripadajocim intranet naslovom, le ta obnovi svoje tabele z naslovi. S C-jevim intranet naslovom pa lahko IP - pakete posilja k njemu direktno.

Recimo, da imamo dve loceni intranet mrezi, ki ju med sabo veze C, ki ima viogo ruterja-usmerjevalnika.

00-01-02-03-04-05

00-11-22-33-44-55

€&-S5^4-3^teM-ff^?^•^BWdW NaffiKR DDEEAADD "•'1U-5A-4D-6C*-C3-QX - — -

? Slika 5-4:Mre2i z usmerjevalnikom

f

Ker sta to dva razlicna intranet segmenta, ima vsaka od mre2 svojo C-razredno mrežno Stevilko. To je

potrebno, ker mora usmerjevalnik vedeti katero mrežo mora uporabiti, da bo dosegel posamezno napravo. Če želi poslati A paket E-ju, mora najprej paket poslati k C-ju, ki potem paket usmeri k E. To je doseženo tako, da A uporabi C-jev intranet naslov in E-jev IP-naslov. Ti intranet naslovi se vzdržujejo s pomočjo ARP-ja. Če bi bil E-ju doložen enak internet naslov tako kot A-ju, potem bi A poskušal doseči E na tak način kot je prej poskušal doseči C - s pošiljanjem ARP zahtevka po mreži in upanju na pozitiven odgovor. Ker sta oba na različnih fizičnih zikah, ta ne bo nikoli videl ARP-jeve zahteve. taka dostava paketa ni možna.

5.2.3.3 Direktno usmerjanje

je prikazano v prvem primeru, ko A skuša komunicirati s C-jem. Prav tako tudi v zadnjem primeru, ko je A komunicira z B. V primeru, ko paketa podatkov ni potrebno dodatno usmerjati. Iz tega sledi, da ko imata pošiljatelj in naslovnik enako mrežno Stevilko se uporablja direktno usmerjanje (direct routing).

5.2.3.4 Indirektno usmerjanje

se uporablja, ko mrežni Stevilki pošiljatelja in naslovnika nista enaki. To je primer, ko mora biti paket usmerjan preko vozlišča, ki ve, kako doseči naslovnika - preko usmerjevalnika.

Ko je A poskušal poslati paket E-ju, mora imeti neko informacijo, ki mu pove preko koga mora poslati paket, da bo dosegel E. To posebno vozlišče se imenuje "gateway" usmerjevalnik med dvema mrežama. **UNJ.X-pYa,metoda.zai.dodajanjeptjza.A:**

Route add [destinationIp] [gateway] [metric] - metric pomeni koliko krogov do naslovnika. V našem primeru bi se zapis glasil:

```
Route add 200.1.2.1 200.1.2.3.1
```

Ta zapis pove A-ju, da uporabi C kot izhodna vrata - gateway. Podobno je tudi v primeru ko E želi doseči A;

```
route add 200.1.2.1 200.1.3.10.1
```

Ta zapis bo uporabljen, da pove E-ju, da naj uporabi C kot izhodna vrata, da bi dosegel A.

Zato je potrebno, da ima C dva ip-naslova po eden za vsako posamezno mrežo. Na ta način A preko C-jevega ip-naslova . ve da je na svoji lastni mreži, podobno je tudi za E. Tako bo C-jev usmerjevalni modul, preko mrežne številke vedel, katero naj uporabi, da bo paket prispel na cilj.

V večini primerov sploh ne bi bilo potrebno ročno dodajanje te usmerjevalne poti. Normalno bi zadostovalo, da postavimo C kot izhodna vrata za vsa vozlišča, izhode na obeh mrežah. To pomeni, da bi v primeru, ko pošiljatelj in prejemnik ne bi bila na direktni povezavi, le ti paketi bili poslani k C-ju glavnemu usmerjevalcu za obe mreži.

* *

5.2.4 Statično usmerjanje in dinamično usmerjanje

5.2.4.1 Statično usmerjanje

se izvaja na podlagi že vnaprej postavljenih tabel, ki ostanejo nespremenjene.

dokler jih ročno ne spremenimo. To je najosnovnejša oblika usmerjanja in ponavadi zahteva, da imajo vse naprave statično definirane naslove in da ostanejo vse naprave na svojih mrežah - jih ne selimo, prestavljamo.

Dmgače mora uporabnik, ročno spreminjati usmerjevalne tabele, da bi sledil spremembam v topologiji mreže in njenimi naslovi. Ponavadi obstaja vsaj en statistični vnos za mrežo in se normalno kreira kar sam, ko postavljamo mrežo.

5.2.4.2 Dinamično usmerjanje

uporablja posebne informacijske protokole, da avtomatično obnavljajo usmerjevalne tabele s potmi, znane kot peer routers.

5.3 Preklopna stikala (switch)

• \ /
*

Preklopna stikala so naprave, ki delujejo na 2. povezovalni plasti referenčnega modela OSI in so namenjena predvsem povečanju prepustnosti znotraj lokalnega omrežja. Zamenjujejo ponavljalnike, premoščevalnike in usmerjevalnike. Od ponavljalnikov jih loči način delovanja, ki je v osnovi enak kot pri premoščevalniku. Od

SERŠ Maribor 2003/04 Kopiranje prepovedano 61

premoščevalnikov in usmerjevalnikov pa jih ločijo bistveno boljše karakteristike in nižja cena na posamezen priključek. Razlog je v tem, da so preklopna stikala naprave namenjene točno določeni funkciji. V ta namen so uporabljena izredno hitra vezja, poleg tega pa v preklopnih stikalih ni vgrajenih cel kup funkcij, ki so lastne usmerjevalnikom. Tako dobimo cenejše in hitrejša naprave, ki podpirajo veliko število funkcij, pomembnih za delovanje lokalnega omrežja.

Poglejmo si princip delovanja preklopnih stikal tako, da primerjamo delovanje omrežja Ethernet s preklopnimi stikali in klasično omrežje Ethernet s koncentradorjem. Pri klasičnem Ethernet omrežju si vse postaje, vključno s strežniki, znotraj enega segmenta delijo prepustnost 10 Mbit/s. To pomeni, da je prepustnost, ki pripada posamezni delovni postaji, bistveno nižja kot 10 Mbit/s.

iz mehanizma delovanja Ethernet sledi, da lahko v vsakem trenutku oddaja vsaka postaja svoj gre za t.i. deljeni medij. Dodatna slabost je tudi v tem, da vse postaje na segmentu 'vidijo' vse poslane pakete. To pomeni, da lahko s pomočjo analizatorjev prometa (ki so npr. že sestavni deli Windows NT strežnikov, mnoge druge programe pa lahko dobimo na Internetu) pregledujemo promet. Tako lahko pregledujemo vsebino, ki se prenaša po omrežju, včasih pa lahko pridemo celo do gesel, če niso šifrirana. Vidimo torej, da imamo pri klasičnem Ethernetu dve poglavni težavi: problem prepustnosti in problem varnosti.

5.3.1 Omrežje Ethernet s preklopnim stikalom

Osnova vsakega preklopnega stikala je hitro vodilo (*High Speed Backplane*), preko katerega poteka komunikacija med posameznimi vmesniki preklopnega stikala. Na vmesnike so priključeni bodisi segmenti lokalnega omrežja, bodisi končne delovne postaje in strežniki. Hitro vodilo, katerega prepustnost je navadno podana v Gbit/s omogoča, da je v vsakem trenutku možnih več simultanih povezav skozi preklopno stikalo. Na ta način dobimo večjo prepustnost celotnega omrežja. Pot paketa skozi stikalo poteka od vmesnika, ki ga je sprejel, preko hitrega vodila do vmesnika, kjer se nahaja naslovljena postaja. Na ostale vmesnike paket ne potuje. Na ta način je zagotovljena tudi varnost. Algoritem delovanja stikala je podoben algoritmu premoščevalnikov in temelji na MAC naslovih. V glavnem vsa omrežja, ki jih gradimo danes, uporabljajo segmentacijo do delovnega mesta. S tem zagotovimo polno prepustnost in varnost do posamezne delovne postaje in strežnikov v omrežju.

Povečanje prepustnosti različnih vrst preklopnih stikal dosežemo z uporabo hitrih tehnologij kot so npr. Fast Ethernet, Gigabit Ethernet in ATM.

5.3.2 Vrste preklopnih stikal:

Preklopna stikala se med seboj ločijo predvsem po:

- podprtih tehnologijah - centralna stikala navadno podpirajo veliko število tehnologij (Token Ring, FDDI, ATM in podobno). Nadstropna stikala pa navadno podpirajo le eno tehnologijo: npr. Ethernet ali Fast Ethernet na strani uporabnikov in imajo navadno 1 ali 2 vmesnika za priključitev v hitro hrbtenico omrežja.
- modularnosti - (število razširitev mest),
- skladnosti • (število stikal, ki lahko gredo v sklad in hitrost povezave znotraj sklada),
- prepustnosti stikala - (v milijonih paketov v sekundi).
- prepustnosti hitrega vodila - (v Gigabit-ih v sekundi).
- podpori usmerjanju različnih protokolov - navadno IP in IPX (preklapljanje na 3. plasti modela OSI).
- možnosti implementacije navideznih omrežij - oziroma VLAN (Virtual LAN),
- delovanju pri preobremenitvi - na posameznih vmesnikih oziroma na hitrem vodilu.
- po zakasnitvah, ki nastanejo, ko paketi potujejo skozi preklopno stikalo.

Zakasnitve so odvisne od dolžine paketov. • po možnosti določanja prioritete prometa, „

• po možnosti filtriranja paketov,
• po možnosti nadzora in upravljanja,
• po številu postaj, ki jih lahko priključimo na posamezen vmesnik,
• po redundantnih povezavah, ki jih nastavimo s pomočjo programske opreme, ^ po možnosti multipleksiranja hrbtemčnih; povezav (2 družima npr. 4. Fast Ethernet hrbtenične povezave v načinu 'Full Duplex' in na ta način dobimo prepustnost 800 Mbit/s) » po mehanizmu premoščanja: ..

o uporabljajo enak algoritem, kot premoščevalniki. kjer se paket v celoti shrani v medpomnilniku. Preveri se na katerem vmesniku je vpisan ponorni naslov in ga pošlje na odgovarjajoči vmesnik. Za vse skupaj skrbi centralna procesna enota. ki je ena sama. algoritem pa se izvaja v programski opremi stikala.

o uporablja algoritem 'Cut through': paket se ne shrani. ampak se prebere le do pomega naslova in takoj pošlje na odgovarjajoči vmesnik. Algoritem je izredno hiter, slabost pa je v tem, da se pošiljajo tudi ti. slabi paketi. saj ne preverja ali je paket brez napak,

o uporablja distribuirano preklapljanje: vsak vmesnik oziroma manjše skupine vmesnikov imajo dodeljen poseben del strojne opreme, ki je namenjen pošiljanju paketov na hitro vodilo. Poleg večje hitrosti delovanja je prednost v boljši odpornosti na izpad. saj v primem okvare izpadejo le določeni vmesniki. V primeru premoščanja pa pride do izpada celotnega stikala, v kolikor odpove centralna logika.

5.3.3 Arhitektura preklopnega stikala

S pomočjo preklopnih stikal in uvedbo navideznih omrežij lahko lokalno računalniško omrežje prilagodimo organizacijski strukturi. To pomeni, da lahko tvorimo logične skupine uporabnikov ne glede na fizično lokacijo le-teh. Največkrat tvorimo zaprte skupine uporabnikov, katerim dovolimo povezljivost do naprav skupnega pomena.

Na ta način pridobimo:

- povečanje varnosti - ne dopustimo, da bi lahko uporabniki poljubno komunicirali med seboj, ampak je možna komunikacija le znotraj skupine in z napravami skupnega pomena (usmerjevalnik v Internetomrežje, strežniki, tiskalniki,...)
- razpršeno oddajanje - se ne širi po celotnem omrežju, ampak je omejeno na posamezna navidezna omrežja
- mobilnost uporabnikov - navidezna omrežja največkrat uporabljamo skupaj z navideznim usmerjevalnikom (Virtual Router).

5.4 Protokolni konverter (gateway)

Protokolni konverter je naprava za medomrežno povezovanje, ki povezuje omrežja, katera delujejo na podlagi popolnoma različnih protokolnih skladov. Protokolni sklad tvorijo protokoli, ki se nahajajo znotraj plasti določenega referenčnega modela. Protokolni konverter deluje tako, da razpakira in usmerja podatke iz enega v drugo okolje. Tako lahko tisto okolje ki je podatke dobilo dela normalno z njimi. saj protokolni konverter razpakira podatke tako da zadovoljujejo potrebam dljnega sistema. Lahko tudi spremenijo format sporočila, tako da bo format nato enak kot ga ima protokolni konverter in bo aplikcijski program znal delati z podatki, ki jih je dobil. Na primer, protokolni konverter za elektronsko pošto, kot na primer X.400, sprejme podatke v enem formatu, jih prevede in te podatke nato pošlje naprej v formatu, ki ga uporablja sprejemnik. > Protokolni konverter povezuje dve omrežji ki ne uporabljata:

- dveh enakih komunikacijskih protokolov,
- podatkovnih struktur,

- jezikov.
- arhitektur.

Ker so v tem primeru lahko različni protokoli prav na vseh plasteh. pravimo. da deluje protokolni konverter na vseh plasteh vključno z aplikacijsko plastjo. Naloga protokolnega konverterja je, da različnim računalniškim sistemom. ki med seboj niso neposredno združljivi, dajejo občutek, kot da komunicirajo z enakim sistemom na drugi strani. Najbolj pogosto uporabljeni protokolni konverterji se uporabljajo v okoljih SNA, za protokolno konverzijo med protokoli LAT in IP ter med IP in IPX.

5.4.1 Delovanje protokolnega konverterja

Protokolni konverterji se uporabljajo za posebne naloge. kar pomeni, da so namenjeni za poseben tip prenosa. So pogosto namenjeni temu kot jih imenujemo (Windows NT Server to SNA gateway).

Na primer: Gateway vzame podatke in izvirnega okolja odvzame stari sklad protokolov prepakira podatke in doda nov sklad protokolov iz ciljnega okolja.

Da se dovoli prenos, mora protokolni konverter:

- dekapsulirati (dekodirati) sprejete podatke z omrežnim protokolnim skladom.
- enkapsulirati (kodirati) podatke, ki jih pošlje naprej s kompletnim protokolnim skladom ciljnega okolja.

5.4.2 Mainframe protokolni konverter:

Protokolne konverterje lahko tudi uporabljamo za komuniciranje med osebnimi računalniki in miniračunalnikom oziroma mainframe okoljem. To lahko storimo tako, da priključimo nek protokolni konverter kot gosta na to okolje in ta nato komunicira z računalniki. ki ne zaznajo inteligentnih računalnikov povezanih v LAN. V LAN okolju se splošno en računalnik kot protokolni konverter. S posebnimi aplikacijskimi programi v namizju računalnika lahko dostopamo in komuniciramo z mainframe računalnikom. Uporabniki lahko dostopajo do podatkov na mainframe računalniku, kot da bi le ti bili na njihovih računalnikih.

Primer pretvarjanja protokolov na različnih nivojih OSI sistema:

6 ZASNOVALAN-a

f

Upravljanje in kontrola nad mrežo ter nudenje uslug sta izvedena na dva načina:

- vse funkcije ali usluge so zbrane na enem mestu v mreži (centralizirana kontrola).
- funkcije ali so razmetane med delovne postaje na njej (distibuirana kontrola).

6.1 LAN-i so lahko zasnovani:

- s centraliziranim ali
- distribuiranim nudenjem uslug,
- so zaprti vase in namenjeni posebnim obdelavam ali
- so odprti in povezljivi z okolico.

Tisto, kar narekuje zasnovano lokalne računalniške mreže, je predvsem cilj, ki ga le-ta ima ter stanje tehnološkega razvoja.

Izbor tako ali drugače zasnovanega LAN-a pogojuje delovno okolje, v katerem bo izbrana mreža delovala. če je namen LAN-a povezava PC-jev, mi pa potrebujemo mrežo za povezavo neinteligentnih terminalov, prav gotovo ni smotno uporabljati LAN z distribuiranim nadzorom delovanja. saj neinteligentni terminali preprosto nimajo možnosti zahtevnega procesiranja programske opreme. ki pri distribuiranem pristopu mora biti v njih locirana.

Če imamo specifično delovno okolje, znotraj katerega se izvaja le prenos posameznih podatkov ali datotek ali potrebujemo kako manjšo uslugo s strani mreže, bomo izbrali mrežo

z distribuiranim nudenjem uslug. V teh primerih se usluge nahajajo kar v posameznih delovnih postajah, kar je veliko smotnejše kot pa uporabiti drage in močne centralizirane namenske posredovalnike in podobno.

6.1.1 Centralizirano in distribuirano vodenje in nadzor

•

Upravljanje in kontrola nad mrežo in njenim delovanjem je lahko locirana na enem mestu ali pa je dodeljena vsaki delovni postaji. Nadzor nad mrežo in njenim delovanjem ni vedno v funkcionalni navezi z njenim tipom, topologijo ali čim podobnim, je pa notranja izvedba teh mehanizmov s tem močno povezana. Notranja izvedba centralizirane kontrole na topologiji vodila (kar se le redko uporablja) je močno drugačna od izvedbe na topologiji obroča (mimogrede, LAN, ki uporablja topologijo obroča in centralizirano kontrolo, se imenuje zanka).

Dva elementa igrata ključno vlogo. To sta pristopna metoda in alokacija.

- Pristopna metoda določa, KDO in KDAJ bo dobil prenosni medij na razpolago.
- Alokacija pa skrbi za to, KOLIKO kanalskih kapacitet in časa bo prenosni medij vozlišču oziroma delovni postaji dodeljen.

6.1.1.1 Centraliziran nadzor in vodenje

potemtakem pomeni, da je ves komunikacijski sistem, potreben za dostop na mrežo ter alokacijo kanala, vsebovan v enem temu namenjenem (dedicated) vozlišču. To določa, katero vozlišče lahko pošilja sporočila, kdaj mu je to dovoljeno, na kakšen način, kontrolira potek zveze in podobno.

To vozlišče, imenujemo centralno ali glavno (master) vozlišče. ostala pa pomožna (tributaries) vozlišča.

Pomembno se je zavedati, da je velikost in zmožnost tako zasnovane mreže v direktni funkciji z močjo centralnega računalnika pri mrežah s centraliziranim upravljanjem in kontrolo, dodajanje novega uporabnika (terminala, računalnika itd.) pomeni upadanje performans celotne mreže in ta upad čutijo vsi uporabniki take mreže.

6.1.1.2 Distribuiran nadzor in vodenje

načelno velja, da dodajanje novih uporabnikov, katerih pogoj je zmožnost lastnega procesiranja, povzročajo združevanje posameznih procesnih moči v mogočen procesni potencial, kar se manifestira v povečanju celotnih performans LAN-a, za vse uporabnike.

Tehniki, ki omogoča komunikacijo med postajami, po vnaprej določenem, takim ali drugačnem redu iz enega mesta, pravimo polling. Polling je v bistvu determinirano pozivanje postaj na pošiljanje sporočil in se za centralizirano kontrolo velikokrat imenuje centraliziran polling, da bi ga lahko ločili od njemu nasprotnega distribuiranega pollinga. Izveden je lahko fiksno, kar pomeni, da zaporedoma kliče vse postaje, in tista, ki kako sporočilo ima, ga mreži tudi posreduje. Lahko pa je izveden na podlagi prioritete, intenzivnosti dela posameznih postaj ali podobno in ni zapovrsten, je pa določljiv in spremenljiv. V grobem, ko govorimo o pollingu, imamo pred očmi predvsem master-slave, oziroma request-response korelacijo med centralnim računalnikom, zadnjeje^T^za^vodenje in nadzor nad zvezacnuna o njega priključenimi delovnimi postajami.

Ker pri centralizirani kontroli običajno potekajo vsi komunikacijski procesi skozi centralno vozlišče, je ta način vodenja in kontrole lokalne računalniške mreže primeren, če je komunikacija predvsem usmerjena iz strani zunanjih vozlišč k notranjemu ali obratno (intenzivna uporaba skupnih baz podatkov, aplikacij in podobno). če pa prevladuje potreba po direktnih komunikacijah med zunanjimi vozlišči, je ta pristop vprašljiv in običajno neprimeren (distribuirane in fizično ločene ter vsebinsko različne obdelave).

Če centralno komunikacijsko vozlišče odpove, se poruši celotna mreža. Vendarje veliko

okolij, kjer je taka mreža optimalna. pa tudi računalniki so pri svojem delovanju zanesljivi, tako da je takih porušitev zelo malo.

Pri distribuiranem nadzoru nad delovanjem LAN-a delovne postaje dostopajo na mrežo, se povezujejo z drugim vozliščem, izmenjujejo podatke, zasedajo kapacitete medija itd., neodvisno ena od druge, pač glede na pravila, po katerih je kontrola izpeljana, in ki se nahajajo pri distribuiranem pristopu na vsaki delovni postaji mreže.

6.1.2 Centralizacija in distribucija mrežnih uslug

Nadzor nad delovanjem lokalne računalniške mreže je centraliziran ali distribuiran, mreža lahko zasnovana tako, da so centralizirane ali distribuirane tudi usluge, ki jih mreža nudi končnemu uporabniku. Za razliko od prej pa tukaj ni tako natančne meje med centraliziranim in distribuiranim pristopom.

- če so vse usluge zbrane na posredovalnikih, namenjenih izključno posredovanju uslug, je to centraliziran pristop. čeprav je teh posredovalnih računalnikov lahko več,
- če pa je vsako vozlišče uporabljivo tako kot povprečna delavna postaja, kot posredovalnik, ki lahko svoje usluge nudi ostalim uporabnikom na mreži. pravimo temu distribuiran način mrežnih uslug.

Pri kompleksnih LAN-ih je opazna tendenca v smeri distribuirane kontrole in centraliziranih mrežnih uslug.

6.1.2.1 Centralizacija mrežnih uslug ima dva ključna razloga: . .

- Stalna raspoložljivost mreže pomeni, da so nam vse usluge mreže kadarkoli in kjerkoli na razpolago. ne glede na stanje uporabnikov na njej (pri distribuiranih uslugah je nemalokdaj pomembno celo zaporedje vključevanja delovnih postaj v mrežo).
- Centralizacija mrežnih uslug pa istočasno močno olajša in poenostavi razvoj in - delovanje tako sistemske kot aplikativne programske opreme, lažja sta vzdrževanje in nadzor tako nad podatki kakor nad celotno mrežo, omogočena sta večja zaščita in varnost podatkov, lažje je vključevanje oziroma dodajanje novih uslug in podobno. -

6.1.2.2 Distribucija mrežnih uslug:

Pri manj zahtevnih LAN okoljih pa je smotna distribucija mrežnih uslug. Ta rešitev ima prednosti pri ceni, prilagodljivosti (prerazporejanje uslug tam, kjer je to potrebno) in podobno.

6.1.3 Zaprti in odprti LAN

Med proizvajalci LAN-ov lahko opazimo tri pristope:

- prvi podpirajo povezljivost med določenimi tipi delovnih postaj (multitasking-multiuser postaje, terminalne CAD/CAM postaje, merilne delovne postaje itd.), ki niso nujno od istega proizvajalca.
- v drugi skupini so tisti, katerih LAN-i so pisani na kožo opremi posameznega velikega proizvajalca računalniške opreme, in teh je vedno manj,
- v tretjo skupino spadajo tisti, ki podpirajo povezovanje raznorodne opreme, od različnih proizvajalcev in z različnimi protokoli in standardi. Značilno za prvo in delno drugo skupino je, da je komunikacijska programska oprema zelo specializirana, lastniška in težko prenosljiva iz ene na drugo lokalno računalniško mrežo. Ker je ta LAN odvisen od aparature opreme oziroma od proizvajalca le-te, jim velikokrat rečemo tudi aparaturno ali proizvodno odvisne mreže. Ker so namenjene predvsem komunikaciji med direktno medsebojno povezano opremo, so zaradi protokolov, ki optimizirajo takšno povezljivost in so običajno lastniške, zelo težko ali celo nepovezljive z okolico. Takim mrežam pravimo zaprte lokalne mreže. Nasprotno pa se tretji tip proizvajalcev, katerih namen je omogočiti komunikacijo med vsemi mogočimi opremami (vendor independent), intenzivno naslanja na komunikacijske standarde. Zaradi standardov omogočajo povezljivost LAN-a tako navznoter

kakor navzven. Ker je povezava LAN-a navzven eden ključnih sestavnih delov tega koncepta, so take mreže znane kot odprte (open system) mreže.

Standard ISO - OSI je sestavljen iz dveh delov. Prvi del predstavlja referenčni model OSI, katerega cilj je predpisati okvir za razvoj standardov. Drugi del tvorijo konkretni protokoli, ki se uporabljajo na posameznih plasteh referenčnega modela. Ti protokoli so standardizirani in omogočajo komunikacijo računalniške opreme najrazličnejših proizvajalcev.

Razdelimo jih lahko v štiri večje skupine:

- LAN protokoli so definirani na prvi in drugi plasti OSI modela in določajo komunikacijo po različnih medijih lokalnega omrežja.
- WAN protokoli so definirani na prvih treh plasteh OSI modela in določajo komunikacijo preko prostranega omrežja WAN (*Wide Area Network*),
- usmerjevalni protokoli so protokoli, ki omogočajo izbiro optimalne poti med usmerjevalniki,
- usmerjeni protokoli so tisti protokoli, ki jih usmerjevalniki lahko usmerjajo in so definirani na 4. do 7. plasti OSI modela.

7.5.8 LAN standardi

- LAN standardi so standardi, skupek pravil ali protokolov, ki omogočajo, da lahko računalniška oprema na lokalni računalniški mreži medsebojno izmenjuje informacije na vsem v mreži enoten, razumljiv in kar se da kvaliteten način.
- LAN standardi pokrivajo oziroma standardizirajo samo področje prenosa podatkov med delovnimi postajami na isti mreži.
- standard lokalnih računalniških mrež naj bi poenotil mehanizme, ki ključno vplivajo na področje uporabe lokalnih računalniških mrež.
- LAN standardi se nanašajo samo na tisti del komunikacij, ki omogoča zanesljiv in hiter prenos podatkov med medsebojno povezanimi delovnimi postajami,
- obstaja več mehanizmov, ki omogočajo tovrstno medsebojno komunikacijo in seveda tudi več pripadajočih standardov.

Nekaj problemov, ki jih morajo rešiti vsi standardi, ne glede na specifičnosti in lastnosti mehanizmov, katerim pripadajo, so:

- kako sprejeti in pravilno interpretirati sporočila iz višjih komunikacijskih nivojev,
- kako in kdaj omogočiti zainteresirani delovni postaji dostop in zasedbo prenosnega medija,
- kako zainteresiranemu uporabniku preprečiti dostop na mrežo, ko je le-ta že v uporabi,
- kako medsebojno povezati uporabnike,
- koliko kapacitet prenosnega medija dodeliti vsakemu vozlišču na LAN-u.
- kako ugotavljati točnost prenosa podatkov in ukrepati v primeru nepravilnosti.
- kako vzpostaviti začetno stanje v mreži.

Večji del teh mehanizmov sta standardizirali mednarodni organizaciji IEEE in ANSI. Standardi lokalnih računalniških mrež pokrivajo samo področje prenosa podatkov na isti mreži, zajemajo samo najnižja dva nivoja komunikacijskega procesa. Omenjena nivoja sta nivo zveze ali povezave (data link level) in fizični nivo. Njuno vlogo smo spoznali v prejšnjem poglavju.

Slika 7.7 nam prikazuje večino trenutno veljavnih in sprejetih standardov na nivoju lokalnih računalniških mrež.

7.5.9 Sestava komunikacijskega nivoja

V grobem lahko rečemo, da so nivoji sestavljeni iz treh funkcionalnih komponent. To so:

- zgornji in spodnji mednivojski vmesniki, ki omogočajo prenos podatkov med dotikajočimi se nivoji. ter pri katerih so točke sprejema in oddaje podatkov in kontrolnih znakov natančno določene (SAP Service Access Point).
- upravljalni vmesnik, ki omogoča zunanje vodenje, nadzorovanje in spreminjanje komunikacijskih uslug dotičnega nivoja (ni prisoten pri vseh nivojih).
- procesni del, ki izvaja vnaprej določena opravila iz njegove pristojnosti oziroma kateri konkretno realizira funkcije dotičnega nivoja.

Mednivojska komunikacija poteka s pomočjo PDU (Protocol Data Unit) okvirjev, ki so rezultat obdelav procesnega dela nivoja. Slika 7.9 nam prikazuje nivoje pri baseband lokalnih računalniških mrežah, oziroma tiste nivoje, ki so pri teh mrežah standardizirani.

- Fizični nivo ima v glavnem enak namen in funkcije kakor pri opisanem OSI/ISO,
- Nivo zveze pa se v LAN-ih deli na dva podnivoja:

o Zgornji podnivo je LLC (Logical Link Control). o spodnji pa MAC (Media Access Control).

Podana standardizacija se nanaša predvsem na baseband lokalne računalniške mreže. Nekatero baseband pristopno metodo na broadband lokalnih računalniških mrežah, ki jih IEEE tudi specificira, pa se razlikujejo od tistih na baseband LAN-ih (delitev na prikazane nivoje je ista). Ravno tako je opisana standardizacija za delovanje baseband LAN-ov potrebna in zadostna. Dočim pri broadband lokalnih računalniških mrežah pokriva samo en del delovanja teh mrež. V splošnem lahko rečemo, da broadband LAN-i za svoje celotno delovanje uporabljajo "mešanico" formalnih in neformalnih standardov. PBX tehnologija pa uporablja za svoje delo predvsem standarde, ki so v domeni standardov za telefonsko komunikacijo.

7.5.9.1 Fizični nivo

ima v glavnem enak namen in funkcije kakor pri opisanem OSI/ISO. Standardizirane so vse električne in mehanske lastnosti za vsak tip MAC. Objekt, ki fizično komunikacijo v LAN omogoča, se imenuje okvir in ga za vsako pristopno metodo posebej določa standard.

Okvir

• Okvir je ključni objekt, ki omogoča komunikacijo. Vanj so naložena pravila in napotki, ki ukazujejo na podatke. Vse to prevaža naokrog po mreži. Vsak LAN komunikacijski protokol oziroma pristopni mehanizem in njemu prirejen standard imata svojo obliko okvirja. LAN standardi definirajo okvirje na spodnjih dveh nivojih (okvirji, so takšni, kot se prenosnemu mediju posredujejo). Okvirji vseh ostalih višjih nivojev so vsebovani v podatkovnem ali informacijskem polju. Iz tega sledi, da protokoli oziroma okvirji lokalnih računalniških mrež, namenjeni zanesljivemu prenosu informacij, nimajo vsebinsko nič skupnega z višje ležečimi okvirji, ki so seveda končni produkt teh višjih nivojev. Za LAN komunikacijske protokole je popolnoma vseeno, ali deluje v DNA, XNS, TCP/IP itd. okolju ali ne. Njegova naloga je, da tisto kar dobi, kvalitetno prenese naslovniku.

Okvirji so sestavljeni iz polj ali zastavic (flags), kjer ima vsako polje natančno določen pomen

in mesto. saj mu jih opredeljuje standard. Ta polja ali zastavice se postavljajo tako pred informacijami, ki jih mora okvir prenesti, pri DLL nivoju pa tudi za njimi, izključno zaradi nadzora pravilnosti prenosa podatkov. Mreža za svoje delovanje uporablja veliko različnih okvirjev:

] • Za kontrolirano vzdrževanje mreže, inidativ^nijn nkrppanjfi v primem napak, "dogovarjanje" med delovnimi postajami itd Tpm nkvirjem pravimo kontrolni

.okvirjiL

\ • dmgi tip okvirjev je povezan s token passing pristopnimi metodami in jih^ Jmenujemo žetonski okvirji.

) • tre^i okvir. ki prfinaša po mreži podatke se imenuje informacijski okvir.

•

Sami standardi pa imenujejo. oziroma uporabljajo, enolična imena za vsak okvir posebj, ne pa samo za skupine. Določeni okvirji pri potovanju po mreži ne menjajo vsebine svojih polj (npr. žetonski okvir nekaterih token passing ring mehanizmov). nasprotno pa drugi spreminjajo to vsebino občasno ali pa ob vsakem ^dotiku" z delovno postajo. Na sliki 7.9 so prikazani informacijski okvirji, in to za vse pristopne metode, ki jih bomo v nadaljevanju spoznavali.