

FDDI je mehanizem token passing mg multipaketnega tipa z zahtevano prenosno hitrostjo 100 Mbps, kar je tudi s standardom (ANSI **X3T9.5**) predvidena hitrost delovanja teh lokalnih računalniških mrež. Multipaketni token passing mehanizem uporablja žeton, s katerim njegov lastnik dobi pravico za oddajo podatkov, oziroma dobi na razpolago prenosni medij. Takoj za oddajo podatkovnega paketa pa mu doda še žeton. Na ta način žeton «poriva» pakete po mreži. Ob vsakem izpadu mreže ali na samem začetku delovanja je, potrebno najprej vzpostaviti žeton. Tudi ta mehanizem uporablja natečaj za začetno pridobitev žetona, vendar bistveno drugačen od tistega pri token ring ali token bus pristopu. Ko žetona zaradi kakršnegakoli razloga ni več na mreži, začnejo vse postaje oddajati sporočilo želim žeton, v čigar okvirju vsaka delovna postaja vpiše najkrajši čas, ki ga potrebuje v primeru sinhronnega delovanja. **Čas za sinhrono delovanje je tisti čas, v katerem mora delovna postaja dobiti prenosni medij na razpolago.** Ta čas pa ni nič drugega kot čas, v katerem mora žeton obkrožiti mrežo, da bo postaja lahko sinhrono delovala. Zato tudi ime za ta čas, obhodni ali TRT (Token Rotation Time) čas. Vsaka delovna postaja, ki je oddala svoj TRT v času inicializacije mreže, primerja le-tega z vsakim TRT-jem, ki je vpisan v krožečih, želim žeton" okvirjih. Če je dobljeni čas nižji od Časa v njenem ali predhodno dobljenem okvirju, si le-tega vpiše v svoj kontrolni register. Po tem, ko ti okvirji obkrožijo celoten obroč, imajo na ta način vse delovne postaje vnesen enak TRT, ki se imenuje operativni Čas. Postaja, ki je ta čas generirala, pa je zmagovalec tega natečaja. TRT v delujoči mreži ni vedno enak, saj ga spreminja vsaka postaja, ki se v komunikacijski proces vključi in se spreminja z vsakim obhodom. Če neka delovna postaja v delujoči mreži dobi žeton na razpolago prej kot znaša inicializacijski operativni čas Topr, lahko oddaja kakršnakoli sporočila, do izteka tega časa. Če pa dobi žeton po preteku operativnega časa, lahko mreži posreduje le-ta slednja visokoprioritetna sporočila imenovana tudi „sinhroni paketi“, ki ji omogočajo vzdrževanje aplikacij v realnem času. Na ta način se vzdržuje komunikacijska časovnost vseh aplikacij v tovrstnem LAN-u znotraj potrebnih meja. Vidimo, da vsaka delovna postaja mora meriti čas, potreben za obhod žetona. To pomeni, da mora po vsaki oddaji žetona postaviti svoj žetonski časomerilec na začetek. Velja, da je vse v redu, če se operativni čas ne podvoji. Če čas, potreben za obhod žetona» doseže ali preseže $2Topr$, se to smatra kot napaka v mreži in se sproži že opisani postopek za njeno ponovno vzpostavitev. Ta pristopni mehanizem se imenuje časovno-žetonska (Timed Token) pristopna metoda. Dolgost TRT-ja pa nam tudi pove, kolikšna je prepustnost FDDI LAN-a. Če je TRT večji od operativnega časa, je očitna velika obremenjenost mreže in s tem nizka prepustnost. TRT nižji od operativnega pa kaže na njeno neobremenjenost. Še ena majhna funkcionalna razlika je med multiple token passing in FDDI mehanizmom. Pri FDDI mehanizmu delovna postaja žeton dejansko iz mreže pobere. Pri token passing-u pa delovna postaja, ko dobi žeton, v bistvu samo spremeni en njegov bit (npr. žeton ima obliko 11111110, prvi bit sprevrže na 0 in dobi vrednost 01111110), ter na ta način tvori v okvirju polje začetek paketa ali BOM (Beginning Of Message), ki ga kar, produži naprej na mrežo, za njim pa mu dodaja ostale podatke. To lahko počne, ker ji elektronika v mrežni vmesni kartici in princip delovanja omogočata tako hitrost oddajanja podatkov, kot je prenosna hitrost medija. Pri FDDI pa šele sedaj, ko je žeton vzela iz mreže delovna postaja pripravi podatke, (prej jih tudi ne more, saj šele ko dobi žeton, ve, kolikšen je TRT) ter koliko in kakšne podatke lahko posreduje) odda podatke na mrežo ter jim pripne popolnoma nanovo narejeni žeton. Prenosni medij, je tovrstnih lokalnih računalniških mrežah podvojen, Prenosni medij, ki se tukaj uporablja, je izključno optični kabel (standard predpisuje tri premere optičnih vlaken). Vsak segment takega kabla zahteva (segment je tukaj neprekinjen del optičnega kabla), tako na začetku kot na koncu, relativno zahtevne vmesnike, ki pretvarjaJo električne impulze v svetlobne in obratno. Ravno tako morajo ti vmesniki omogočiti nadaljevanje svetlobe v naslednji kabelski segment, če je vozlišče neaktivno. Ti vmesniki so vedno aktivni, ne glede na to, ali je delovna postaja v mrežo vključena ali ne. FDDI standard omogoča priključitev 1000 vozlišč zato strah pred izpadom te mreže očitno, saj ena sama napaka pri enem vmesniku ali prekinitve enega kabelskega segmenta lahko podre celotno mrežo. To pa so razlogi, zakaj FDDI standard opredeljuje dvojno kablajo. Redundančna kablaja ni nič nenavadnega tudi pri ostalih topologijah in pristopnih mehanizmi, vendar jo edino pri tem LAN-u opredeljuje standard. Z dvojno kablajo je vsekakor dosežena najvišja zanesljivost delovanja, vendar je potrebna dodatna aparatura oprema vozlišč. V primeru prekinitve kabla delovne postaje najprej znotraj časa $2*TRT$ ne dobijo na razpolago žetona. Ker še ne vedo, za kakšno napako gre, najprej poskušajo, vzpostaviti žeton, kar jim ne uspe. Po tem spoznanju se začne poseben postopek za vzpostavitev obroča (ring recovery), na naslednji način. Delovne postaje začnejo oddajati „svarilni“ paket, ki opozarja na resno napako mreže. Vsaka delovna postaja, ki ta paket dobi, ga odda naprej naslednji zapovrstni postaji v mreži. Če delovna postaja ugotovi, da njen paket ni uspel doseči naslednje postaje v zaporedju, predvideva, da je na tem segmentu prišlo do prekinitve. Tako lokalizira napako. Delovna postaja nato promet preusmeri preko sekundarnega (notranjega) obroča, kar je spet naloga teh vmesnikov. Tako je ponovno vzpostavljena komunikacija na obroču, dokler se fizična napaka obroča ne odstrani. Vendar standard ne predvideva ring-recovery za vse tipe postaj, kar pomeni, da obstajajo določene prekinitve, lahko izključijo delovno postajo, To velja za tiste delovne postaje, skozi katere gre samo en, primarni ali zunanji obroč. Če v našem primeru pride do prekinitve optičnega kabla na segmentu med žičnim vozliščem in postajo C ali D, ti dve postaji nista več na mreži. Take cenejše delovne postaje so znane kot Class B postaje, tiste, skozi katere gresta pa oba obroča in katere zaradi tega potrebujejo kompleksnejšo aparaturo opremo, pa kot Class A sestavne enote. FDDI standard je na fizičnem nivoju specifičen optične in mehanske karakteristike steklenih vlaken, energijske nivoje, kodno/dekodirne postopke za prenos digitalnih signalov na optični kabel ki so različni od ostalih itd. Maksimalna dolžina kablov je lahko 200km in nanjo je lahko priključenih največ 1000 delovnih postaj. Če imamo sekundarni obroč kot zaščito pred izpadom potem je število priključenih postaj omejeno na 500 in maksimalna dolžina kablov je lahko 100km. Ponavljalniki pa morajo biti vmes priključeni na vsaka 2km.

LDDI pristopna metoda jemlje svojo zasnovo iz CSMA/CP mehanizma, ki je pravzaprav edina CSMA pristopna metoda z determiniranim delovanjem. To pa pomeni, da LDDI mehanizem garantira maksimalen čakalni čas za dostop na prenosni medij. V tem primeru ni trkov ali kolizij na mreži, vendar ni niti žetona oziroma njegovega okvirja. To, da LDDI mehanizem ne uporablja trkov, pomeni da nima niti kompleksnih protokolov za upravljanje z njimi, kar potencialno tej mreži omogoča veliko hitrejšo delovanje. Žetonskega okvirja ta pristopna metoda ne pozna, uvaja pa zato enega drugega, ki igra ključno vlogo pri tem mehanizmu in sicer RT (Resynchronization Time) okvir. LDDI pristopna metoda bazira na končnem minljivem času, znotraj katerega je medij po predhodnem prenosu podatkov prazen. Vsaka postaja na mreži ima svoj poseben čas, potreben da zazna ali je postaja neposredno pred njo že zasedla prenosni medij. Ta čas ali slot je

vzpostavljen na ta način, da delovna postaja lahko zazna, ali je drugi uporabnik neposredno pred njo že začel s podatkovno transmisijo. Če je, delovna postaja odstopi, če pa predhodna delovna postaja znotraj tega časa ni zasedla medija predpostavlja, da ji je medij na razpolago in začne z oddajanjem. Ta čas imenovan AAO (Arbitrated Access Opportunity) je čas, potreben da signal prepotuje 06 ene do druge delovne postaje, ki pripadeta zaporedna AAO časa. Za to, da bodo vse delovne postaje vedele kdaj in kje na mreži postopek začne pa skrbi RT okvir. Vedno znova je poslan potem, ko so vse delovne postaje pri enem obhodu izvedle svojo oddajo podatkov. RT je poslan na mrežo, ko je delovna postaja z najdaljšim AAO časom zaključila z oddajanjem podatkov. Pojava RT okvirja pri delovni postaji, pa pomeni, da le ta resetira svoj čas na začetek. Na ta način se vzpostavlja sinhronizacija v LAN-u. RT okvir pošilja postaja z najnižjim AAO časom, saj se vsak oddajni cikel začne pri njej. Če nima namena ničesar poslati, odda RT okvir naslednji delovni postaji (delovni postaji z prvim višjim AAO-jem), drugače pa pošlje normalen informacijski okvir. Poseben WF (Waiting Flag) mehanizem. skrbi, da bi imele vse delovne postaje omejen čas oziroma zamik za dostop na prenosni medij. Iz tega sledi, da s pomočjo njega ugotavljamo tudi napake na mreži. Če je namreč neka delovna postaja v okvari. se lahko zgodi da ko pride na vrsto zaradi pokvarjenega ali ,neskončnega AAO časa zaduši mrežo. Ravno WF to onemogoči in tudi lokalizira delovno postajo ki to počne. Zanimiva je tudi rešitev pri tej pristopni metodi, po kateri lahko sprejemnik informacije takoj odda odgovor. To je rešeno s pomočjo tako imenovanega PAO (Priority Access Opportunity) časa. Delovna postaja, ki na koncu svojega informacijskega okvirja doda PAO polje (maksimalno 64 bita dolgo) omogoča sprejemni postaji, da takoj po sprejemu podatkov pošlje visoko prioritetni odovor. Vendar samo enkrat, pomeni, da se dve delovni postaji ne moreta kar naprej pogovarjati. Pri LDDI ni pomembna vsebina okvirja, pač pa prisotnost signala na prenosnem mediju. Razporeditev delovnih postaj nima vpliva na dogajanje. če so namreč delovne postaje med seboj konstantno oddaljene, so tudi AAO časi enolični (urejeni po naraščajočem ali padajočem vrstnem redu) in brez rezerv. kar pomeni dejansko izredno hitrost delovanja tega pristopne metode. Če pa so delovne postaje naključno razmetane, je potrebno uvajati določene sigurnostne časovne zamike, kar se manifestira v upočasnjevanju metode.

Multiple Token Passing Žeton na svoji poti pobira in prenese vsa sporočila, ki jih ima kaka postaja na mreži pripravljena, namesto samo enega. Žeton pripotuje k prvi postaji. Ta ga zazna ter začasno shrani. Podatkovni nivo sedaj posreduje celotno sporočilo fizičnemu nivoju, ki shranjeni žeton doda na konec sporočila ter tako oblikovan okvir posreduje prenosnemu mediju. Celoten okvir pripotuje k drugi postaji, ki ima ravno tako pripravljeno sporočilo. Fizični nivo druge postaje že po ustaljenem načinu kopira okvir v svoj vhodni vmesni pomnilnik ter pri tem pregleduje še naslov ter išče žeton. Ko žeton zazna, prenese pripravljeno sporočilo na njegovo mesto ter ga na koncu svojega okvirja doda celotnemu sporočilu ter to vse skupaj posreduje naprej po mreži. Celoten proces se v vsaki postaji ponovi. Na ta način nastane na mreži veriga okvirjev, katere žeton poriva naprej. Zaradi takega delovanja je očitno. da **se** mora vsak okvir, ki ga kaka delovna postaja posreduje prenosnemu mediju, končati s poljem. ki označuje konec pripadajočega okvirja, ter začeti s poljem. ki označuje njegov začetek. Osnovni koncept token passinga je precej izboljššan. Mehanizem. potreben za takšno delovanje, je bolj zapleten. Očiten je problem dolžine celotnega sporočila. V teoretičnem primeru je dolžina vsote vseh sporočil **enaka celotni dolžini** mreže (takoj za žetonom se nahaja prvo sporočilo). Zaradi količine procesiranja, ki je proporcionalna dolžini celotne informacije na mreži, pri tem mehanizmu pride do občutnega upadanja hitrosti mreže pri velikih komunikacijskih obremenitvah. Očitna težava pri tem mehanizmu so velikosti vmesnih pomnilnikov, kar se rešuje na različne načine. Ravno zaradi reševanja "dolžinskega" problema je veliko variacij na multiple-token-passing-ring mehanizem, zato se pojavlja tudi veliko različnih imen tovrstne pristopne metode. Vsa ostala problematika tega pristopa je podobna osnovnemu token passing mehanizmu.

PriorityToken Passing Ta pristopni mehanizem loči uporabnike po prioriteti. Žetonu je dodana še ena funkcija. To je funkcija prioritete. Žeton namreč ni več stalno iste oblike, temveč vsebuje znotraj sebe polje, ki definira trenutno prioriteto. Žeton najprej po že znanem načinu obkroži obroč z najvišjo prioriteto, kar pomeni, da lahko v tem krogu komunicirajo samo tisti uporabniki, ki takšno prioriteto imajo. V naslednjem obhodu žeton zniža prioritetni nivo ter tako omogoča prenašanje sporočil uporabnikov z nižjo prioriteto. Ko na ta način preide preko vseh prioriternih nivojev (mimogrede, teh nivojev je zelo malo. tipično 3 do 4, največji pa 8) zopet preide na najvišjega. Drugi pristop tega principa pa uporablja žeton, ki spremeni prioritetni nivo šele tedaj. Ko so zaključene vse komunikacije na trenutnem prioriternem nivoju, kar pomeni, da lahko žeton z isto prioriteto obkroži obroč tudi večkrat. Token passing s prioriteto predvideva in specificira tudi IEEE standard.

PRISTOPNE METODE Delovanje LAN-a se veže predvsem na način dostopa oziroma zasedbe prenosnega medija, zaradi česar te mehanizme imenujemo pristopne metode. Delimo jih na:• deterministične - kjer lahko napovemo čas, ko neka postaja v omrežju dobi pravico do oddajanja:o TDMA,o pozivanje,o podajanje žetona,• nedeterministične - dostop do medija je naključen. ni posebnega postopka, ki bi razdeljeval prenosno zmogljivost:o postopki brez poslušanja,o postopke s poslušanjem pred oddajanjem,o postopke s poslušanjem pred in med oddajanjem. **CSMA** je metoda, največkrat uporabljena pri topologiji vodila. Pri tem pristopu dobi dostop na mrežo tista postaja. ki prva reagira, ko je mreža prazna (ni prometa na kablju). To pomeni, da pri tem mehanizmu ne obstaja nobena prioriteta ali vnaprej določena zapovrstnost dostopa na prenosni medij. CSMA je najbolj značilen predstavnik več točkovne komunikacije. **Token passing ring** je zelo uspešna metoda pri visokih obremenitvah mreže in ima take svobode dostopa do medija kakor CSMA. Tukaj mora delovna postaja dobiti dovoljenje, da lahko svoja sporočila odda mreži. Mehanizem je značilen za obročaste topologije. **Token passing bus** je mehanizem, ki poskuša združiti prednosti CSMA topologije in token passing pristopne metode. Ta mehanizem uporablja fizično topologijo vodila, da bi na njej simuliral logično topologijo obroča. **Sloted rings** ali empty slots pa uporablja namesto enega paketa, ki kroži v mreži in je neprimerno „krajši“ od dolžine prenosnega medija, več podobnih paketov. Problem je, da pri večji količini paketov v mreži postajajo funkcije za upravljanje delovanja izredno kompleksne in s tem močno oslabijo konceptualne prednosti tega protokola. Mehanizem je osredotočen na komunikacijo točka-točka, tako kot vsi token passing mehanizmi. **FDDI** je namenjen optičnim kablom in izjemno visokimi hitrostmi prenosa reda 100 Mbps in več. Protokol je dokaj specializiran in ga ni možno prenesti na baseband mreže z drugimi tipi prenosnih medijev. Uporablja se največ za hrbtenične mreže. **LDDI** je poskus izveleč iz

koaksialnega kabla toliko, kolikor dejansko nudi Vodilo za ta protokol je pristopni mehanizem CSMA/CP. po katerega vzoru je tudi realiziran. Uporaben je v broadband mrežah ter kot hitra baseband hrbtenična mreža.

TOKEN RING (IEEE 802.5) Podjetje IBM, kjer so prvotno različico obroča z žetonom tudi razvili m predlagali standard. je kot osnovno tehnologijo za svoja lokalna omrežja izbralo prav obroč z žetonom. V okviru organizacije IEEE je bil leta 1985 sprejet standard z oznako 802.5, ki natančno opredeljuje obroč z žetonom kot lokalno računalniško omrežje. Pristop postaj do prenosnega sredstva je omogočen z uporabo posebnega okvira (frame) - Žetona, ki kroži med postajami v omrežju. Prav kroženje žetona po omrežju zagotavlja postajam enakopravnost, saj je vsaka na vrsti takrat, ko pride Žeton mimo nje - za razliko od omrežja ethernet, pri katerem postaje tekmujejo za pravico oddajanja. To je tudi razlog, da obroč z žetonom deluje dobro tudi pri visoki obremenjenosti, medtem ko pri omrežju ethernet v takem primeru pride do velikih težav zaradi množice trkov.

CSMA/CE Pri tem mehanizmu so trki odpravljeni. kar pomeni, da kolizija ni več sestavni del tega mehanizma. Vsaka postaja dobi svoj čas, v katerem lahko oddaja svoja sporočila. Ta čas je za vsako postajo v mreži različen. Pred oddajo sporočil na mrežo postaje, vsaka zase, neodvisno ena od druge, izračunajo neko časovno vrednost. Fizični nivoji preverijo, če je prenosni medij že zaseden. Če ni. postaje vseeno ne pričnejo takoj oddajati sporočil. temveč počakajo. da se izračunani čas izteče. Ta Čas imenujemo DST (Deference Slot Time) in je določen z algoritmom, ki se neodvisno izvede v vsaki postaji za vsak prenos in ji da enolično Časovno vrednost. Najmanjša razlika med dvema izračunanima vrednostma mora biti večja od časa, potrebnega, da se signal prenese po mreži. Vidimo, da se ponovni proces prenosa sproži takoj po ugotovitvi, da mreža ni prazna. Sedaj je razumljivo, zakaj mora biti DST za trenutek večji od časa. potrebnega za prenos signala z enega na drugi skrajni konec. Očitno je, da ni potrebno čakati, da bi vse postaje razpoznale trk, tako kot pri CSMA/CD mehanizmu, temveč je dovolj zaznati, da je nekdo s sporočanjem že začel.

CSMA/CD (...,with Collision Detection) CS - Carrier sense (občutljivost na signal), vse postaje zaznavajo ali je prenosni medij že v uporabi ali ne. To zaznavajo zato, ker vedo kolikšen je najvišji možni energetski nivo na prenosnem mediju, ko je le-ta prazen. **MA-Multipte access** (večkratni dostop),ko je prenosni medij prost sme z vzpostavljanjem zveze pričeti katerakoli postaja **CD** - Collision Detection zmožnost oddajne postaje, da ugotovi nastanek trka. Postaja. ki želi poslati sporočilo, pošlje po mreži opozorilno polje ali preambulo, s katero opozori vse postaje na mreži, da bo pričela oddajati. Po preteku preambule postaja odda sporočilo na mrežo. Čas, ki Je potreben zato, da sporočilo doseže skrajni konec mreže in se vrne nazaj imenujemo **propagacijski zamik**. Postaja, ki je oddala sporočilo ves Čas prenosa opazuje dogajanje na mreži, saj lahko samo ona ugotovi all je prišlo do trka podatkov na mreži. Če je prišlo do trka podatkov. morata obe postaji, ki sta podatke oddajali. le te oddajati Se toliko časa, da obe zaznata, da je prišlo do kolizije. **Zaradi tega je najkrajša možna dolžina okvirja pri tej pristopni metodi natančno** določena. Procedura za obdelavo trkov v odvisnosti od algoritma počaka neki naključen čas in nato ponovno prične z oddajanjem. Vse ostale postaje na mreži, ki so v tem Času sprejele to nedokončano sporočilo, ga sprejmejo kot veljavno. Podatkovni nivo vsebuje namreč znotraj sebe mehanizem, ki taka manjkajoča ali popačena sporočila prepozna in jih zavrže. **Pri visokih obremenitvah se karakteristike takšne mreže močno poslabšajo.** Dobre strani te pristopne metode bi bile: takojšen dostop na mrežo,• manjše kot je število postaj na mreži, ki želijo medsebojno komunicirati, večja je hitrost dostopa na mrežo oziroma prenosni medij, » zaradi možnosti ugotavljanja stanja na kablu pred oddajanjem podatkov, je v splošnem število trkov dokaj nizko in mreža je izredno hitra, » daljša kot so sporočila, manjše je število trkov glede na celoten čas zasedenosti mreže, zato lahko z nastavitvijo dolžine okvirja optimiziramo delovanje le-te, napake na mreži je možno, vendar težko odkrivati in odpravljati, metoda ni primerna za okolja, kjer se zahteva natančna zapovrstnost dogajanja kot so npr. mreže s procesnimi napravami, roboti, sinhronimi terminali, real-time aplikacijami itd. **Ta način ugotavljanja trkov na mreži je zaradi ojačanja na fizičnih prenosnih medijih, omejen na cca 2500m.**

CSMA/CA Glavna značilnost tega mehanizma je, da nima funkcij za obdelavo trkov. S tem odpade tudi potreba po spremljanju dogajanja na prenosnem mediju v času prenašanja sporočil. Oddajna postaja, ki oddaja sporočilo na mrežo nima nobenega vpogleda v to, ali je sporočilo uspešno pripotovalo na cilj ali ne. Če so podatki zaradi kolizije izgubljeni, se aktivira ERT (Error Recovery Task) funkcija za odpravo napak, ki se nahaja na višjih nivojih. saj pri tem pristopu šele ti ugotovijo, da je s sporočilom nekaj narobe. Zaradi take poenostavitve je ta mehanizem izredno učinkovit in kratek. Ugotavljanje in postopki za odpravljanje napak na tako visokih nivojih so zelo časovno potratni, zato ta mehanizem ni uporaben za velike obremenitve mrež je pa zanimiv in zelo uporaben za L-AN-e, ki delujejo v preprostejših in komunikacijsko nezahtevnih okoljih.

TOKEN BUS (IEEE 802.4) Ta mehanizem je tudi distribuiranega tipa in je s funkcionalnega stališča zelo podoben predhodno opisani token passing ring pristopni metodi. Za fizično povezavo med delovnimi postajami uporablja topologijo vodila. za delovanje pa vzpostavi logično topologijo obroča. To lahko naredi, ker pri fizični topologiji vodila vsaka postaja na LAN-u sliši, kaj in kdaj se na mreži nekaj dogaja. Token bus mehanizem deluje s pomočjo žetona, ki **ne** potuje **po fizičnem** zaporedju delovnih postaj, pač pa potuje po dinamičnem adresnem zaporedju. s Čimer tvori že omenjeni logični obroč (standard predvideva padajoče adresno zaporedje), Tukaj dinamično adresno zaporedje pomeni. da je naslednje sprejemno vozlišče tisto. čigar naslov se v krožečem žetonu nahaja in se z dodajanjem ali odvzemanjem delovnih postaj iz lokalne računalniške mreže fleksibilno prilagaja stanju. Če je vse v redu, deluje **ta** mehanizem zelo preprosto. Postaja, ki ima žeton in zaključi prenos podatkov, izvede še postopek. potreben za vzdrževanje logičnega obroča . Po zaključku teh procesov v polje naslova vpiše addresso naslednje postaje v mreži ter takšen žeton pošlje na vodilo. Ker vse postaje na vodilu ..slišijo" žeton. alokacija namembne postaje ne predstavlja nobenih težav. Le-ta žeton sprejme, opravi prenos podatkov, če Jih ima, izvede vzdrževalno funkcijo, v polje naslovov vpiše naslov svoje in naslednje postaje, ter tako oblikovan žeton, kakor njegov predhodnik, posreduje ostalim postajam na mreži. Ta proces se stalno ponavlja. Vzpostavitev logičnega obroča se izvede na začetku in po vsakem izpadu mreže. Po vzpostavitvi mreže pa je logični obroč potrebno stalno vzdrževati. Vzdrževanje logičnega obroča pomeni, da mora mreža nemoteno omogočati

vkjučevanje in izključevanje delovnih postaj. ne da bi pri tem bita kakorkoli ogrožena, Tega problema pri prejšnjih mehanizmih ni bilo, saj so se delovne postaje vključevale in izključevale iz mreže s fizično preklopitvijo ali prijavo in niso motile delovnih navad. Tukaj pa za to mora skrbeti sam mehanizem, saj samo pripojitev ali prijava postaje nič ne pomeni, dokler ni delovna postaja sestavni del obroča. Žeton ni več sestavljen samo iz posebne bitne razporeditve, pač pa ima že sam žeton nujno potrebni dve polji, naslov oddajne postaje in naslov naslednje sprejemne postaje v logičnem obroču. Naslov naslednje sprejemne (logično zaporedne) postaje na obroču žetonu posreduje njegov trenutni lastnik. Vidimo, da žeton ni več stalno enak in pasiven, pač pa se spreminja vrednost njegovih polj v vsaki delovni postaji na taki mreži. Ker je fizična topologija topologija vodila, potrebujemo tudi dolgo uvodno polje za sinhronizacijo, ter kontrolna polja za predvideno in planirano kroženje žetona (celoten okvir žetona je prikazan v poglavju o okvirjih). Tako se pri tej mreži srečamo z dvema obsežnima okvirjema, stalno prisotnima m potrebnima za delovanje tega mehanizma; prvi je okvir Žetona, drugi pa sam informacijski okvir.

Inicializacija Začetna vzpostavitev ali inicializacija je v bistvu poseben primer dodajanja novih postaj. Ta proces se sproži ob začetnem pogonu mreže ter po popolnih izpadih. Bistvo tega procesa je v pridobitev žetona. V stanju pred vzpostavitvijo je mreža seveda popolnoma prazna. Vsaka postaja, ki želi pošiljati sporočila, opazi to stanje, in vsaka od njih lahko sproži postopek vzpostavitve. Vzemimo, da med ostalimi postaja C, ki ima potrebo po komuniciranju, tudi hoče vzpostaviti mrežo. V ta namen pošlje na mrežo poseben "kandidiram za žeton" okvir z neko vnaprej določeno dolžino. Takoj po izteku časa, potrebnega, da se okvir te dolžine razleze po mreži, prisluhne, kakšne so posledice. Če na mreži zazna neko "ne-prazno" stanje, ve, da je neka druga delovna postaja poslala na mrežo daljši okvir in se izloči iz nadaljnjega tekmovanja. Pri "kandidiram za žeton" okvirju je namreč pomemben čas trajanja okvirja, ne pa njegova vsebina, zato je popolnoma vseeno, ali je bit okvir po-staje C cel čas v koliziji z nekim drugim okvirjem. Če pa zazna po izteku predvidenega časa prazno mrežo, skrajša dolžino okvirja in proces ponovi. Ta proces se ponavlja, dokler postaja ne porabi vseh predvidenih in vnaprej določenih dolžin "kandidiram za žeton" okvirja. Če po zadnjem poskusu tudi ne zazna prisotnosti daljšega okvirja, ve, da je zmagala na tem natečaju, in da ima žeton (oziroma, da ga lahko prva generira). Po tej zmagi je ta postaja poklicana, da sedaj vzpostavi logični obroč.

Vzpostavitev logičnega obroča Ko postaja poseduje žeton, sproži postopek za prijavo ostalih delovnih postaj, ki se želijo vključiti v komunikacijski proces. V ta namen pošlje na mrežo "prijavni" okvir, v katerem specificira naslovno področje. Če tega področja ne bi bilo, bi prijavni okvir veljal za vse postaje in bi v primeru, da se želi v obroč vključiti več postaj istočasno, prišlo do konfliktov (fizična topologija je topologija vodila in vse postaje sledijo dogajanju), ki se manifestirajo v trkih z nam že znanimi lastnostmi in posledicami. Po oddaji tega okvirja počaka na odgovor. Postaja, ki se namerava vključiti v logični obroč in katere naslov se nahaja v podanem področju, to z "potrditvenim" okvirjem, v katerem se njen naslov nahaja, sporoči. Dobljeni naslov pa postaja, ki žeton ima, vpiše v naslovno polje "naslednja postaja" v žetonih. Tako oblikovan žeton posreduje naprej tej postaji, ki proces ponovi. Ko se žeton vrne k izvorni postaji, je logični obroč vzpostavljen.

Vzdrževanje logičnega obroča Vzdrževanje logičnega obroča pomeni dodajanje in odzemanje delovnih postaj brez porušitve mreže. Ta faza pa ni nič drugega, kot pošiljanje "prijavnega" okvirja. Postaja, ki se želi vključiti v mrežo, zazna prisotnost tega okvirja ter vrne "želim vstopiti" okvir, v katerem je naveden njen naslov. Delovna postaja, ki je prijavni okvir poslala, ta naslov vnese v polje "naslednja postaja", ter ji žeton tudi odda. Od sedaj naprej je nova postaja sestavni del obroča. Postaja, ki namerava obroč zapustiti, preprosto po tem, ko je žeton sprejela, ne reagira. Na ta način sproži fault recovery mehanizem (mehanizem za odpravo napak), ki je zelo podoben postopku za vzpostavitev obroča, vendar se izvede samo na predelu manjkajoče postaje. Ker pa je ta pristop časovno potraten, je v uporabi način, po katerem postaja, ki namerava zapustiti obroč, po tem, ko je dobila žeton, vpiše v polje svojega naslova naslov naslednje postaje (samo ona namreč ve, komu poslati žeton) ter ga vrne predhodni postaji s pripombo "vzpostavi novo pot". Le-ta to tudi naredi in žeton, ki ima vpisan novi naslov naslednje postaje, posreduje naprej, seveda si ta novi naslov tudi prepíše v svoj register. Tako postaja, ki je to želela, ni več v igri. Ta mehanizem vsebuje tudi uslugo, ki delovni postaji, ki vsebuje žeton in še ni kompletirala svojega sporočila, omogoča, da žeton začasno preda naslednji postaji. z obvezo, da ji ga po končanem podatkovnem prenosu vrne. Zaradi te in podobnih lastnosti se ta pristopni mehanizem optimalno prilagodi okolju, v katerem deluje.

Kontrola pretoka Poleg ponovnega oddajanja nepravilno sprejetih ali izgubljenih PPE mora biti omogočena tudi kontrola pretoka podatkov med procesi. Kontrola pretoka je potrebna iz različnih razlogov: • potreba po sinhronizaciji med sprejemnikom in oddajnikom, ker sprejemnik ne more porabiti podatkov tako hitro, kot mu jih pošilja oddajnik, • omejene pomnilniške kapacitete sprejemnika, ki mora prekiniti sprejem, da ne pride do izgube podatkov, • aplikacijske in uporabniške omejitve. Kontrola pretoka se lahko izvaja na dva načina: prvi je zasnovan na neposrednem opazovanju pomnilnika, drugi pa upošteva povprečno obremenjenost pomnilnika in hitrost prenosa uravnava glede na število trenutno nepotrjenih protokolarnih podatkovnih enot PPE.

Mehanizmi potrjevanja zagotavljajo avtomatsko odpravljanje napak, ki se lahko zgodijo pri prenosu protokolarnih sporočil ali pa njihova vsebina sprejemniku semantično ne ustreza. Izvedba takih mehanizmov je seveda možna le pri povezanih storitvah. V primeru, da so sprejeti podatki kakorkoli oporečni, je potrebno zagotoviti avtomatsko ponovitev pošiljanja. Mehanizem potrjevanja je opredeljen s sistemom pošiljanja PPE ter sporočil ACK in NACK, Postopke odpravljanja napak v angleščini označujemo z Error Control. **PDU**-Protocol Data Unit - protokolarna podatkovna enota ali PPE. **Secondary**-sprejemnik. **SDU**-Service data unit-storitvena podatkovna enota ali **ACK**-Acknowledge-pozitivna potrditev. **NACK**-Not Acknowledge-negativna potrditev, **ARQ**-Automatic Repeat Request-zahteva za avtomatsko ponovitev. Glede na pravilo, po katerem deluje oddajnik, ločimo dva osnovna načina potrjevanja: **Sprotno potrjevanje**: Pošiljatelj odda PPE šele takrat, ko sprejme potrditev predhodne PPE, zato ta način potrjevanja imenujemo tudi pošlji in čakaj. Dobra lastnost potrjevanja je, da pri takem načinu pošiljanja ne more priti do **poplavljanja** sprejemnika

s podatki, saj sprejemnik lahko podatek zavrne ali prekliče. **Slabost** sprotnega potrjevanja pa je počasnost **protokola** in nizka izkoriščenost prenosnega kanala. **Tekoče pošiljanje:** Pošiljatelj oddaja PPE, ne da bi čakal na potrditev predhodno oddanih PPE. Dobra **lastnost** protokola s tekočim pošiljanjem je boljše izkoriščanje prenosnega kanala, saj smo v primeru sprotnega potrjevanja videli, da oddajnik velik del časa miruje - ne oddaja, ker čaka na sprejem potrditve. Pravilo protokola s tekočim pošiljanjem je preprosto: pošiljaj, kolikor hočeš in kakor hitro hočeš. To pomeni, da oddajnik pošilja PPE, ne da bi čakal na sprejem njihovih potrditev (ACK ali NACK). Zato ima lahko v določenem trenutku oddajnik nepotrjenih več oddanih PPE, ki jih mora shraniti tudi v čakalno vrsto nepotrjenih PPE za morebitno ponovno pošiljanje. Potrditve morajo vsebovati zaporedno številko paketa, na katerega se nanašajo. Slika 7.12 prikazuje prenos zaporedja šestih PPE. Oglejmo način polnjenja in praznjenja čakalne vrste nepotrjenih sporočil. Prenosi na sliki potekajo brez napak. • Idle RQ - tekoče potrjevanje. • Send and wait - pošlji in čakaj. Ne glede na tip potrjevanja razlikujemo dve inačici glede na to ali sprejemnik pošilja le pozitivne ali tudi negativne potrditve: • o posrednem potrjevanju govorimo, če sprejemnik potrjuje zgolj pravilno sprejete PPE (na napake sklepamo, če ne dobimo potrditve sprejema), • o neposrednem potrjevanju pa govorimo, kadar sprejemnik negativno potrdi nepravilno sprejeto PPE, pozitivno pa pravilno sprejeto, **Sprotno posredno potrjevanje** Pri sprotne posrednem potrjevanju protokol potrjuje samo pravilno sprejete protokolarne podatkovne enote PPE. Če v določenem času za poslano PPE oddajnik ne sprejme potrditve, to vzame, kot da je prišlo do napake pri prenosu. Možni sta dve situaciji. v katerih oddajnik ne dobi potrditve ACK: • PPE ni pravilno sprejeta ali se med prenosom izgubi, sploh ne pride do sprejemnika, • potrditveno sporočilo ACK se med prenosom izgubi ali pride do oddajnika v neprepoznavni obliki. Oddajnik po določenem času ugotovi, da sprejem določene PPE ni bil uspešen. Parameter časovne kontrole določa, kako dolg je ta čas. Časovna kontrola je interni mehanizem, ki zagotavlja, da komunicirajoči procesi v primeru napak ne čakajo neskončno dolgo na odziv, ki se ne bo zgodil (na primer na sprejem izgubljenega potrditvenega sporočila ACK). Časovna kontrola se sproži ob vsaki oddaji PPE; ob izteku (točka K) pa oddajnik ustrezno ukrepa. Poleg mehanizma časovne kontrole oddajnik potrebuje tudi Število ponovitev določene operacije, kar omeji dovoljeno število neuspehov istega tipa. To je potrebno iz enakih razlogov kot časovna kontrola, saj bi sicer na primer ob "pretrgani žici" oddajnik ponavljat oddajo istega PPE do onemoglosti. **Protokol s posrednim sprotnim potrjevanjem za svoje delovanje potrebuje naslednje parametre:** • časovno kontrolo oddajnika, • časovno kontrolo sprejemnika, • število ponovnih oddaj podatkovnih paketov in potrditev, • časovno kontrolo sprejemnika za primer izpada oddajnika. Zaporedna številka podatkovnega paketa je potrebna zato, da lahko protokol zazna večkrat sprejete pakete. Tudi kontrolna sporočila bi lahko vsebovala zaporedno številko paketa, na katerega se nanašajo, vendar pa to nima posebnega smisla, saj je v vsakem primeru jasno, da se nanašajo na zadnji oddani paket. **Sprotno neposredno potrjevanje** Protokol s sprotnim neposrednim potrjevanjem se od pravkar opisanega razlikuje po tem, da v primeru napake sprejemnik odda neposredno obvestilo - negativno potrditveno sporočilo NACK. Tako oddajniku ni treba čakati do izteka časovne kontrole. • Dokler ni napak, se protokol obnaša popolnoma enako kot protokol s posrednim sprotnim potrjevanjem. Enako se obnaša tudi, če se izgubi PPE ali ACK. • posredna inačica ne razlikuje med primeroma, ko se PPE izgubi in ko se med prenosom popači. V neposredni inačici pa nastopi razlika v primeru popačenja PPE(N+f). Sprejemnik ne molči, temveč takoj pošlje oddajniku negativno potrditveno sporočilo NACK, s čimer pospeši dogajanje. Oddajniku ni treba čakati na iztek časovne kontrole, temveč nemudoma ponovno pošlje PPE(N+1). • če se ACK ali NACK izgubita med prenosom, oddajnik po izteku časovne kontrole ponovno pošlje PPE. V primeru izgubljene potrditve ACK pride kasneje do večkratnih sprejemov istega sporočila. Določeni morajo biti isti parametri oddajnika in sprejemnika. **Tekoče pošiljanje - posredno potrjevanje** Tudi ta mehanizem posrednega potrjevanja s tekočim pošiljanjem ne razlikuje med izgubo in nepravilnim sprejemom PPE ali ACK. Kaj se zgodi, če sprejemnik sprejme popačeno PPE(N+1) ali pa se ta med prenosom izgubi: • Oddajnik posredno iz sekvence potrditvenih sporočil ugotovi, da je prišlo do napake pri paketu PPE(N+f). V našem primeru potrditvenemu paketu ACK(N) namreč ne sledi paket ACK(N+1), temveč kar ACK(N+2) in ACK(N+3), • ko oddajnik namesto pričakovanega ACK(N+1) sprejme potrditev ACK(N+2), mu je jasno, da PPE(N+1) ni bil sprejet. Zato ponovno pošlje PPE(N+1) - v primeru na sliki namesto PPE(N+5), • sprejemnik ves čas shranjuje pravilno sprejete pakete. Nepravilen vrstni red sprejetih paketov PPE, nastane zaradi napačnega sprejema PPE(N+1). Vrstni red PPE v vmesnem pomnilniku je: N, N+2, N+3, N+4, N+1, N+5. • sprejemnik mora sporočila obdržati v začasni čakalni vrsti vsaj do trenutka. Ko pravilno sprejme manjkajočo PPE(N+1), šele potem jih lahko v pravilnem vrstnem redu uvrsti v svoj delovni pomnilnik. Oddajnik spozna, da paket PPE(N) ni potrjen, ko sprejme namesto ACK(N) ACK(N+1)* Zato ponovno odda PPE(N). Za sprejemnik je dogajanje brez posebnosti, dokler ponovno ne sprejme PPE(N): ko zazna podvojen paket, mora odvečne kopije zavreči. **Tekoče pošiljanje - neposredno potrjevanje** Sprejemnik potrjuje pravilno sprejete pakete z ACK(N), nepravilno sprejete pa z NACK(N). Izgubljenih ne potrjuje, ker ne ve zanje. Oddajnik ugotovi izgubo paketa, ko manjka njegova potrditev - ob sprejemu potrditve naslednjega paketa iz zaporedja. Izgubljene in negativno potrjene pakete ponovno odpošilja. Če se izgubi ACK(N) ali NACK(N), se paket ponovno odpošlje po sprejemu potrditve naslednjega paketa iz zaporedja. Osnovno inačico neposrednega potrjevanja izboljšamo in tako zmanjšamo število prenesenih potrditvenih paketov. Uvedemo potrjevanje zaporedja; z oddajo pozitivne potrditve paketa N potrdimo pravilen sprejem vseh paketov iz zaporedja do vključno N-tega. • izgubi se paket PPE(N+1). Sprejemnik to ugotovi, ko za paketom PPE(N) sprejme paket PPE(N+2). • ker gre za neposredno potrjevanje, sprejemnik odda negativno potrditev NACK(N+1), s čimer zahteva ponovno pošiljanje manjkajočega paketa. • medtem oddajnik že odda PPE(N+3). Ko sprejme NACK(N+1), ponovno odda PPE(N+1), nakar nadaljuje s PPE(N+4), • sprejemnik potrdi sprejem paketa PPE(N+4) z ACK(N+4). S tem potrdi celotno zaporedje PPE(N+2), PPE(N+3), PPE(N+1), PPE(N+4). Nazadnje potrdi še PPE(N+5). Slaba stran tega načina je, da dovoljuje napačen vrstni red sprejemanja podatkovnih paketov. Po oddaji NACK sprejemnik ne odda pozitivne potrditve, dokler pravilno ne sprejme ponovljene ustrezne PPE.