RM OSI

Každé komunikačné zariadenie má svoje fyzické rozhranie (konektor, káble, obvody generujúce napäťové úrovne, modulárory, obvody na synchronizáciu, logické obvody na kódovanie a ošetrenie chybovosti, časť v ktorej je implementovaná logika pre nadviazanie a zrušenie spojenia časť na rozsekanie veľkých súborov na časti schopné prejsť s danou sieťou a tak ďalej....)

Aby bol vo veciach poriadok a aby bolo možné jednotlivé časti a funkcie komunikačných zariadení dobre opísať a porovnať so zariadeniami iných výrobcov, je vhodné mať určitý štandardný systém, na ktorý sa dá odvolať. Z komerčných dôvodov nebolo prípustné, aby sa takýmto štandardom stal napríklad komunikačný model používaný fy. IBM príp. inej firmy. Preto Medzinárodná štandardizačná organizácia **ISO** vytvorila model, označovaný ako **RM OSI** (**R**eference **M**odel – **O**pen **S**ystem **I**nterconnection. Za základ zvolila **vrstvový** model skladajúci sa zo 7-ich vrstiev. Pomocou modelu RM OSI možno opísať akýkoľvek komunikačný systém a jeho funkcie. Špecifikáciu RM OSI možno nájsť medzi ISO normami pod označením ISO/IEC 7498-1: 1994.

Princíp **vrstvového modelu** a fungovanie jednotlivých vrstiev možno ukázať na nasledovnom príklade, kedy sa Africký biológ snaží komunikovať so svojím kolegom, Indickým biológom.

Africký biológ	biologické pojmy	Indický biológ
Tlmočník: africký jazyk - angličtina	angličtina	Tlmočník: indický jazyk - angličtina
Telefón	zvukový signál	Telefón

Obaja biológovia chápu biologické pojmy, ale komunikujú vďaka tlmočníkom, ktorí síce nerozumejú biológii ale dorozumejú sa spoločným jazykom - angličtinou. Aj táto komunikácia však prebieha vďaka nižšej vrstve – telefónu, ktorý nevie nič o angličtine, ale je schopný preniesť zvukové signály.
Pre susedné vrstvy platí, že spodnejšia vrstva poskytuje **komunikačnú službu** vrstve nad sebou. V našom prípade tlmočník poskytuje služby biológovi, teda nadradenej vrstve.
Pre partnerské vrstvy (na tej istej úrovni) dvoch komunikujúcich systémov platí, že komunikujú pomocou **komunikačného protokolu,** t.j. pomocou dohodnutých formátov dát a dohodnutých pravidiel na ich výmenu. Napríklad tlmočníci medzi sebou komunikujú anglickým jazykom. Protokol znamená, že používajú určité dohodnuté slová a pravidlá (na začiatku sa predstavia, v prípade, že jeden z nich zle rozumel, vyžiada si zopakovanie danej vety, prípadne vyhláskovanie a podobne)

Využijúc odbornú terminológiu, môžeme uvedené pojmy zadefinovať nasledovne:

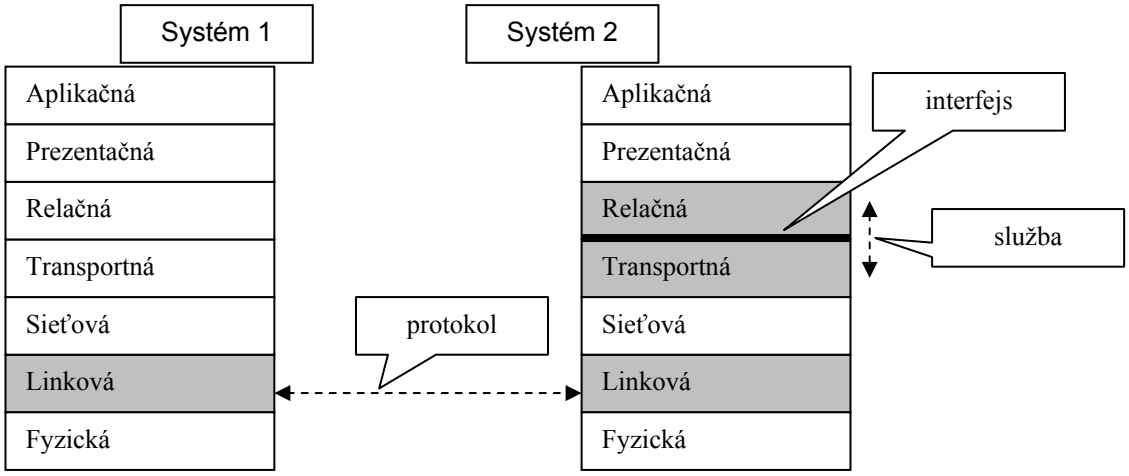
Komunikačná služba je súbor primitív (operácií), ktoré daná vrstva poskytuje vrstve nad ňou. Vzťahuje sa na interfejs (rozhranie) medzi dvomi vrstvami. Kvôli predstave možno využívanie služby prirovnať k volaniu funkcie v programovacom jazyku, pričom sa dáta predávajú ako argumenty volanej funkcie (pozri obrázok neskôr).

Pre užívateľa sú potom služby definované prostredníctvom servisných primitív, čo sú správy vymieňané medzi vrtvami. Hovoríme o 4 druhoch primitív:
- request
- indication
- response
- confirm

Samotné zabezpečenie služby, je už záležitosťou protokou, ktorý zostáva pre používateľa skrytý.

Komunikačný protokol (peer protokol) je súbor pravidiel a formátov rámcov, paketov resp. správ, ktoré sú vymieňané medzi peer-entity na úrovni rovnakej vrstvy.

RM OSI model definuje nasledovných 7 vrstiev:



Layer 1 - Fyzická vrstva (Physical)
- zaoberá sa problematikou komunikačného kanála, definuje **fyzické prenosové médium** (typy káblov, prenosové frekvencie), **modulačné techniky**, tvary signálov (napäťové úrovne), druhy **konektorov**, prenosovú rýchlosť, **kódovanie** a podobne. Pre vyššiu (Linkovú) vrstvu poskytuje službu – umožňuje prenos postupnosti bitov cez daný komunikačný kanál. Príkladom je V.24, V35, X.21.

Layer 2 – Linková vrstva (Data-link)
- využíva služby Fyzickej vrstvy (prenos bitov) ⇒ linková vrstva sa o prenos bitov nestará
- zabezpečuje spojenie medzi zdrojom a prijímačom (prijímačmi) – priame spojenie linkou
- zostavuje dáta z vyššej vrstvy do rámcov (**framing**), zabezpečuje ich bezchybný prenos (**error-control**), riadi tok dát (**flow control**). Pri LAN sieťach sa v rámci tejto vrstvy rieši aj zdieľanie prístupu viacerých zdrojov (vysielačov) na spoločné médium (**medium-access control**)
- skoro všetky štandardy Linkovej vrstvy sú založené na HDLC (LAPB pri X.25 a LLC pri 802.x LAN)

Layer 3 – Sieťová vrstva (Network)
- definuje funkcie, ktoré zabezpečujú komunikáciu zariadení aj vtedy, keď nemajú priame spojenie
- umožňuje zapájať do sietí rôzne druhy zariadení a ich vzájomnú komunikáciu
- zavádza hlavne **adresovanie**, **routing** a prípadne aj riadenie chybovosti
- Príklad – X.25 (NP), IP

Layer 4 – Transportná vrstva (Transport)
- využíva služby sieťovej vrstvy, ktorá umožňuje prenos dát zo zdroja do ľubovoľného príjímača v sieti na základe globálnych (sieťových) adries
- vytvára prístupové miesta pre komunikáciu vyšších vrstiev, často aplikácií
- pre vyššiu vrstvu vytvára víziu priameho prepojenia medzi dvomi koncovými zariadeniami v sieti
- stará sa o error-control a flow-control (obdobne ako linková vrstva)
- Príklad - TCP

Layer 5 – Relačná vrstva (Session)
- stará sa o riadenie dialógu medzi koncovými systémami

Layer 6 – Prezentačná vrstva (Presentation)
- umožňuje definovať rôzne druhy kódovania dát a následne robiť medzi nimi konverziu (napríklad konverzia medzi kódmi ASCII a EBCDIC)

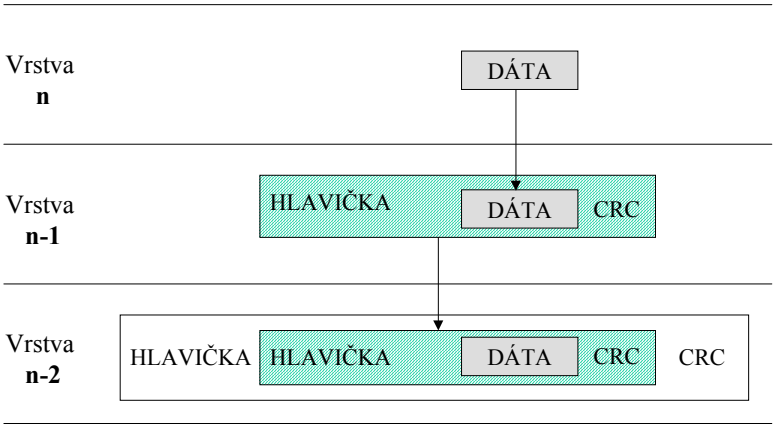
Layer 7 – Aplikačná vrstva (Application)
- táto vrstva predstavuje komunikujúcu aplikáciu. Aplikácia „rozumie“ významu prenášaných dát, vie, či sa jedná o mail, sťahovanie súborov a pod.
- napr. FTP, HTTP

Je potrebné podotknúť, že 7 vrstiev bolo vybraných viac z politicko-komerčných dôvodov, ako z dôvodov pragmatických. Faktom je, že vhodnejší by bol model 5 vrstvový, pretože vrstvy 5 a 6 spravidla nemajú čo robiť, a Aplikačná vrstva (7) je aplikovaná priamo nad Transportnej vrstve (4). To je aj prípad protokolov rodiny TCP/IP. Navyše, funkcií pripadajúcich na linkovú vrstvu je relatívne veľa – hlavne pri sieťach LAN.

Protocol suite (protocol family) – sústava protokolov, na jednej vrstve ich môže byť definovaných aj viacero.
Protocol stack – sústava protokolov, na každej vrstve je však definovaný iba 1 konkrétny

Enkapsulácia

Spodná vrstva poskytuje služby vrstve nadradenej cez dohodnutý interfejs, cez tzv. prístupový bod danej služby. Dáta od hornej vrstvy umiestni spodná vrstva do vlastných rámcov, ktoré okrem samotných prenášaných dát obsahujú ďalšie pomocné informácie – napríklad adresu, CRC, číslo rámca a pod. Takémuto zabaleniu dát hovoríme **enkapsulácia** – obaľovanie. Nasledovný obrázok znázorňuje postupné obaľovanie dát smerom od vrchu nadol. Každá vrstva si pritom obalí dodané dáta (alebo celý rámec, ktorý považuje tiež iba za dáta vyššej vrstvy) a vytvorí vlastný rámec.



Sieťové architektúry

Sieťová architektúra označuje architektúru, aká je použitá pri danom type siete. Architektúra neznamená konkrétnu sieť, podobne ako v stavebníctve architektúra označuje štýl a spôsob akým sú konkrétne budovy, v našom prípade siete, vybudované.
Rôzne typy sieťových architektúr možno rozdeliť do týchto charakteristických skupín:

LAN local area network
- ide o prepojenie distribuovaných skupín DTE (spravidla počítačov, serverov, periférnych zariadení...) umiestnených v jednej budove, príp. komplexe budov. Všeobecne ide o akékoľvek komunikujúce zariadenia – špeciálne technológie, snímače, ústredne, vysielače – čokoľvek
- z hľadiska zaradenia do RM OSI modelu špecifikujú Fyzickú a Linkovú vrstvu (dve spodné vrstvy)
- najrozšírenejšie sú štandardy IEEE rady 802.x, ktoré sú spravidla vytvárané podľa de-facto štandardov (napr. Ethernet, Token Ring...). IEEE štandardy sú preberané ako ISO štandardy, označované sú ISO 8802.3
- prenosové rýchlosti spravidla 10, 100, 1000 Mbps

WAN – wide area network
- používajú prostriedky na diaľkový prenos údajov (telekomunikačné linky)
- prepájajú body na veľké vzdialenosti, ale spravidla pomalými linkami (v porovnaní s LANmi)
- príkladom sú siete X.25, Frame Relay
- prenosové rýchlosti – často menej ako jednotky Mbps (často 64kbps, 2Mbps...)

MAN – metropolitan area network
- niečo medzi LAN a WAN
- spravidla ako chrbticová sieť mesta, resp. podniku s viacerými budovami v meste
- prenosové rýchlosti – rádovo 100Mbps
- príkladom sú siete FDDI, DQDB

Všeobecne však možno povedať, že toto delenie je dané historickým vývojom a nové technológie tieto rozdiely postupne stierajú. Napr. vytvorením optického backbone na báze Gigabitového Ethernetu po území celého Slovenska vzniká sieť, ktorá má parametre siete LAN (rýchlosť, oneskorenie...) a je rozsiahla ako WAN.

Prenosové médiá

Prenosové média sú jedným z najdôležitejších komponentov siete. Dátové prenosy prebiehajú najmä po **metalických médiách**, v súčasnosti už ale dominantné postavenie preberajú **optické prenosové médiá**, tzv. optické vlákna, optické káble. Okrem toho (od čias pána Marconniho), je využívaný aj **bezdrôtový (wireless) prenos** pomocou rádiových vĺn. Vtedy je prenosovým médiom okolitý priestor (prenos vzduchom, éterom).

Metalické médiá

Najjednoduchším prenosovým médiom je **dvojžilová linka**, ktorá sa skladá z dvoch navzájom odizolovaných vodivých žíl. Hlavne z telefónie sú známe šnúry typu SYKFY, ktoré obsahujú spravidla 2 medené žily obalené mäkkým dielektrikom. Okrem toho sú používané rôzne druhy dvoj, štor a viac **vodičových šnúr, káblov** a káblikov. Tieto prenosové médiá sú vhodné iba na prenos pri relatívne nízkych prenosových rýchlostiach, sú náchylné na šum, rušenie, presluchy a podobne.

Ďalším prenosovým médiom je tzv. **krútená dvojlinka** (Twisted Pair - **TP**). V základnom prevedení sa používa netienená TP (unshielded twisted pair- **UTP**). Väčšiu odolnosť voči rušeniu má tienená krútená dvojlinka (Shielded Twisted pair)- **STP**, ktorá je však drahšia. V súčasnosti sa v našich podmienkach najviac používa tzv. **FTP** – Fóliovaná TP, ktorá je tienená, možno ju spoľahlivo použiť v sieťach s prenosovou rýchlosťou 100Mbps, resp. 1Gbps. FTP je v podstate podmožinou STP, na tienenie však používa iba fóliu (nie metalické opletenie) a hlavne je impedančne rovnocenná s UTP kabelážou. UTP je tiež použiteľné na vyššie rýchlosti (100Mbps), ale kvôli vyžarovaniu pri vysokých frekvenciách (rádovo 100MHz) je potrebné uloženie do tienených žľabov. Toto sa bohužiaľ často nedodržuje a potom dochádza k vzájomnému, ťažko predvídateľnému rušeniu (dôsledok nedodržiavania elektromagnetickej kompatibility EMC).

Hlavne v LAN sieťach je historicky veľmi rozšírené použitie tzv. **koaxiálneho kábla** (koaxial cable), ktorý je tvorený vnútorným vodičom, okolo ktorého je nanesená vrstva dielektrika. Na tejto vrstve je vodivé opletenie, ktoré je pokryté ďalšou izolačnou vrstvou - vonkajším plášťom. Hlavný efekt vodivého opletenia je v odtienení vnútorného vodiča od vplyvu vonkajších rušení. Hlavnými parametrami sú útlm a impedancia. V lokálnych sieťach Ethernet sa používa v dvoch základných prevedeniach:

- tzv. hrubý Ethernet (Thick Ethernet), alebo tiež žltý kábel Yelow Cable vzhľadom na svoju charakteristickú farbu. Priemer kábla je 10 mm má štvornásobné opletenie a impedanciu 50 ohm. Jeden segment tohto kábla môže mať dĺžku až 500 metrov. Nevýhoda je vysoká cena a malá ohybnosť.
- vo väčšine prípadov sa používa tenký Ethernet (Thin Ethernet), ktorý má rovnakú impedanciu, ale polovičný priemer. Pretože má vyšší útlm a menšiu odolnosť voči rušeniu používa sa v segmentoch do dĺžky max. 185 metrov. Výhoda je nižšia cena a väčšia ohybnosť. Prenosová rýchlosť u oboch typov je 10 Mbps.

Optické prenosové médiá

Pre rýchlejšie prenosové rýchlosti sa s výhodou využíva ako prenosové médium svetlovod, obyčajne vo forme **optického vlákna**. Pre prenos signálov pomocou svetla je potrebný celý optický prenosový systém, zložený zo zdroja, prenosového média a prijímača. Zdrojom svetla môže byť luminiscenčná dióda LED (Light Emitting Diode), alebo drahšia laserová dióda, ktoré emitujú svetelné impulzy na základe privádzaného prúdu. Detektorom na prijímacej strane je fotodióda, ktorá prenáša dopadajúce svetlo na elektrické signály.

Úlohou prenosového média je dopraviť svetelný lúč od zdroja k detektoru s minimálnymi stratami. K tomuto účelu sa používa tenké optické vlákno (optical fiber), tvorené jadrom (core) a plášťom (cladding). Jadro má najčastejšie priemer jednotiek až desiatok mikrometrov a je vyrobené zo skla, alebo z plastu. Pri vedení v optickom vlákne sa využívajú výhody vedenia svetla a využíva sa systém úplných odrazov od povrchu vlákna. Pri priemere vlákna 50, resp. 62,5 μm je vlákno schopné viesť rôzne vlny svetelných lúčov tzv. vidy. Vtedy hovoríme o mnohovidovom vlákne (**multimode fiber**). Vyššie prenosové rýchlosti, rádovo až Gbps je možné dosiahnuť na jednovidovom vlákne (monomode, **singlemode fiber**). Ide o veľmi tenké vlákna, s priemerom jadra 9 μm, ktoré sú tak tenké, že sa „do nich vojde iba jeden svetelný lúč“. Ich obrovskou výhodou je nízky útlm a nízke skreslenie vysielaných signálov. Preto je možné pomocou singlemódových vlákien prenášať dáta vyššími rýchlosťami a na väčšie vzdialenosti. Samozrejme, nič nie je zadarmo. Singlemódové vlákna sú drahšie ako multimódové. Navyše aj celé systémy pracujúce so singlemódovými vláknami používajú drahšie zariadenia – na vysielacej strane spravidla laserové diódy, nie iba LED diódy ako multimódové.

Jedno vlákno sa používa na jednosmerný prenos, preto na spojenie dvoch zariadení sa používajú 2 vlákna (1 pár). Optické vlákna sa spájajú do optického kábla, ktorého obal ich chráni pred mechanickým poškodením, ale aj účinkom vody, ktorá má negatívny vplyv na prenosové vlastnosti. Okrem veľkej prenosovej rýchlosti je výhodou optických vlákien ich odolnosť voči elektromagnetickému a elektrostatickému rušeniu, ako aj ochrana pred odpočúvaním.

Voľný priestor ako médium - bezdrôtový prenos

Pre bezdrôdový prenos, teda prenos okolitým voľným priestorom sa využívajú rôzne frekvenčné pásma a v závislosti od požadovaných výsledných vlastností prenosového dátového kanála aj rôzne modulačné techniky. Pre zaujímavosť možno spomenúť aspoň nasledovné:

Mikrovlnné spoje – spravidla používané na spojenie bod-bod. Takýto spoj vyžaduje, aby sa bola medzi komunikujúcimi zariadeniami priama viditeľnosť.
Bezdrôtové WLAN siete – sú spôsoby na prepojenie (spravidla) počítačov medzi sebou a vytváranie LAN sietí, pričom sa komunikuje bezdrôtovo. Podrobnejšie informácie sú uvedené v samostatnej časti.
VSAT technológie – (very small apperture terminal) sú satelitné systémy, ktoré na Zemi používajú vysielacie/prijímacie stanice vybavené malou satelitnou anténou (spravidla parabolická offsetová anténa priemeru cca 1,4m) a medzi sebou komunikujú cez satelit – spravidla geostacionárny. Zariadenie, ktoré na satelite prijíma a následne vysiela signály (pre-vysiela) medzi pozemskými stanicami sa nazýva transponder. Pre svoj prenos využívajú v súčasnosti pásmo **C** , **Ku** a do budúcnosti **Ka**.

L (1-2GHz)
S (2-3 GHz)
C (4-6 GHz)
X (7-8 GHz)
Ku (11-18 GHz)
Ka (20-30 GHz)

Prístupové metódy na zdieľanie spoločného média

Pokiaľ má k jednému prenosovému médiu prístup viacero staníc súčasne (viaceré môžu vysielať naraz) môže dochádzať ku kolíziám pri prenose. Typickým príkladom je bezdrôtový prenos a použitie tzv. vysielačiek. Vtedy môžu naraz pristupovať viacerí užívatelia ako vysielacie stanice (zdroje) a viacerí ako prijímacie stanice. Je vhodné **zaviesť do samotného využívania spoločného média určitý poriadok**, aby sa všetci nesnažili vysielať naraz a navzájom sa nerušili. Možností je niekoľko, spravidla však možno hovoriť o metódach, kedy je vopred presne daný spôsob ako možno dané médium využívať (vtedy ide o tzv. **deterministický** prístup) a metódy, kedy sa pristupuje na médium náhodne (tzv. **stochastické**). Podrobnejšie k jednotlivým metódam nasledovnom.

deterministické zdieľanie média

Ide o metódy, kedy je spôsob prístupu na použitie média pre prenos dát presne určený. Je daný vopred známou dohodou.

TDMA - časový multiplex (time division multiple access)
všetci zdieľajú jedno prenosové médium
každý môže toto médium využívať iba počas jemu vyhradenému časovému úseku, tzv. **slotu**
(samozrejme, všetci musia byť synchronizovaní a slušní, t.j. vysielať iba počas svojho intervalu)

FDMA - frekvenčný multiplex (frequency division multiple access)
každý má pridelené svoje frekvenčné pásmo
pridelené pásma sú volené tak, aby si navzájom neprekážali

WDMA - vlnový multiplex (wavelength division multiple access)
používa sa pri optických prenosových systémoch
pre jednotlivé stanice sú pridelené vlnové dĺžky
v podstate sa jedná o frekvenčný multiplex (pridelenie vlnovej dĺžky znamená pridelenie frekvencie)

CDMA - kódový multiplex (code division multiple access)
je veľmi „prešpekulovaná“ metóda
založená na pôvodne vojenskej metóde vysielania s rozprestretým (spread) spektrom
v princípe existujú dva spôsoby realizácie a to buď DSSS alebo FHSS

nedeterministické (stochastické) zdieľanie média

Pri týchto metódach nie je prístup na médium riadený, t.j. nie je vopred daný. Na médium pristupujú stanice vtedy, keď práve potrebujú. Samozrejme, môže dochádzať ku kolíziám a preto je potrebné aplikovať opatrenia, ako kolíziám predchádzať a keď už nastanú, ako sa s nimi vysporiadať. Pretože pri týchto metódach je prístup na médium náhodný a nie je možné určiť a zaručiť čas, dokedy daná zdrojová stanica doručí dáta cieľovej stanici, nazývame tieto metódy **stochastické**. Najznámejšio stochastickou metódou na zdieľanie spoločného média je metóda CSMA/CD, ktorá je použitá pri sieťach typu Ethernet.

prístupová metóda CSMA/CD

CS – carrier sense
– všetky stanice počúvajú nosnú a zisťujú, či je médium obsadené alebo prázdne
MA – multiple access
- viaceré stanice pristupujú na jedno spoločné médium a spoločne ho zdieľajú

- v danom okamihu môže používať médium iba jeden
CD – collision detection
- stanice detekujú vzniknuté kolízie a následne sa podľa toho správajú

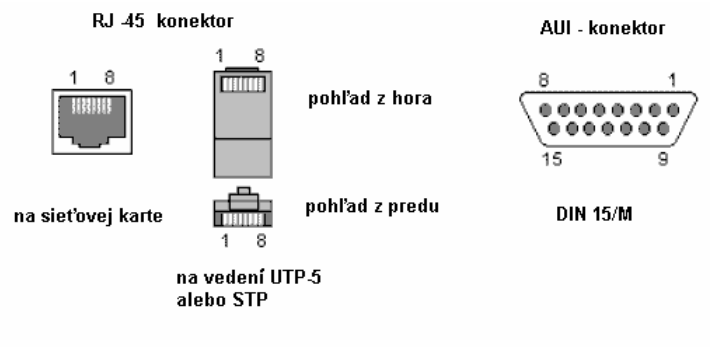
Princíp CSMA/CD je možné vysvetliť na nasledujúcom príklade:
Na jednej chodbe je niekoľko kancelárií a ľudia medzi sebou komunikujú tak, že si kričia cez chodbu (**Multiple Access**). Predpokladajme, že keby kričali viacerí naraz, tak sa to pomieša a nikto nebude nič rozumieť. Naraz teda môže do chodby kričať iba jeden. Metóda CSMA/CD to zabezpečuje nasledovne:
- Keď chcem kolegovi niečo zakričať, tak najprv počúvam (**Carrier Sense**), či je ticho na chodbe. Ak už niekto kričí, tak čakám kým prestane (raz musí prestať, pretože každý môže kričať iba maximálny dohodnutý čas). Keď je ticho, tak začnem kričať ja.
- Samozrejme, pokiaľ na takéto ticho čakal aj niekto iný, tak zrejme začne kričať naraz so mnou. Na chodbe potom počuť pomiešané hovory a keď si to uvedomíme (**Colission Detection**), tak obaja stíchneme (samozrejme, predtým ešte zanadávame, aby o tom vedela celá chodba – „keď už kolízia, tak poriadna“).
- Po takejto kolízii sa obaja odmlčíme na náhodne stanovenú dobu (obaja si hodíme kockou, a toľko sekúnd každý z nás počká). Po tejto odmlke začnem kričať (ak už medzitým nezačal kolega). Takto sa s určitou pravdepodobnosťou vyhneme kolízii, ibaže by obidvom padlo rovnaké číslo a znovu by sme sa začali prekrikovať – vtedy postup opakujeme.

Presne takýto princíp je implementovaný aj v sieťach typu Ethernet a má nasledovné vlastnosti:
- každý počuje všetko a je len na ňom, čo s prijatými dátami urobí
- čím viac nás na chodbe je, tým je viac kolízií a celkovo sa menej prenesie
- pri tejto metóde nie sú priority, t.j. ani urgetné správy nemožno zakričať prioritnejšie
- nie je možné dopredu vypočítať a ani zaručiť, do akého času sa budem môcť preniesť správu (kričať), preto túto metódu nazývame stochastickou – náhodnou

Existujú aj ďalšie modifikácie CSMA metódy, napr. CSMA/CA (**C**ollision **A**voidance – predchádzanie kolíziám). Takáto metóda je použitá pri bezdrôtových WLAN sieťach.

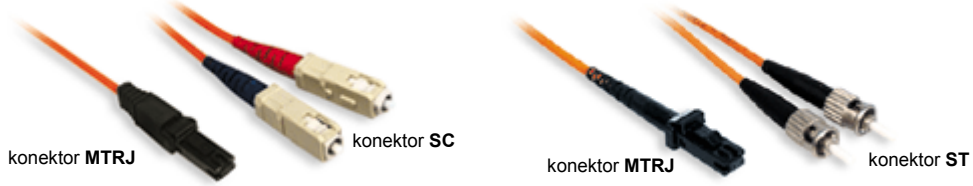
Konektory

Pre metalické vedenia prepájajúce modem s verejnou telekomunikačnou sieťou sa používajú konektory typu RJ-11. Na prepojenie počítačov pomocou káblov UTP a STP sa používajú konektory typu RJ-45 s tienením a bez tienenia. Pre koaxiálne vedenia a ich prepojenie sa používajú konektory označované ako BNC pričom tu existujú dva základne typy a to pre impedanciu 50 a 75Ω. Ďalším, dnes už zriedka používaným konektorom je konektor označovaný ako AUI. Tento konektor bol používaný pri starších typoch sieťových kariet a zariadení na prepojenie sa používal konektor DIN 15/M.

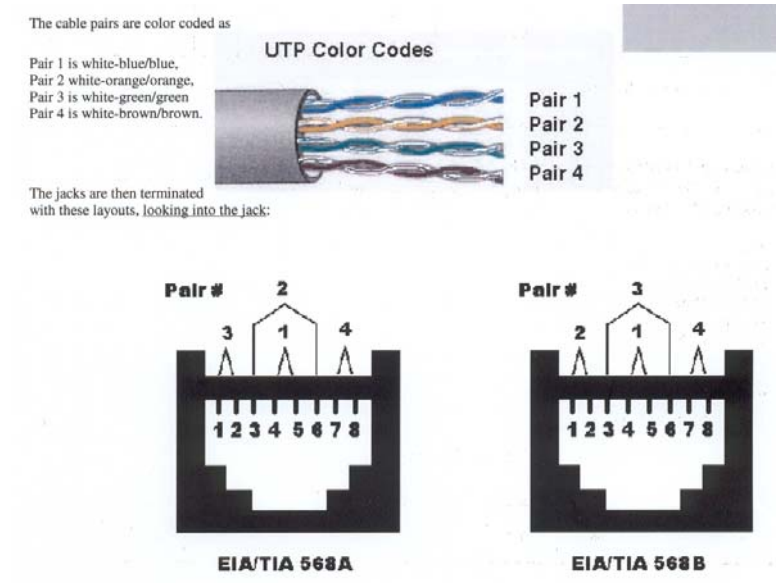


Obrázok: Konekory RJ-45 a AUI používané v LAN sieťach

Pre optické vedenia sa používajú špeciálne konektory. Obvykle sa používajú na prepojenie serverov alebo špeciálnych sieťových zariadení, napr. HUB-ov, SWITCH-ov a pod.



Obrázok: Optické konektory MTRJ-SC a MTRJ-ST



Obrázok: Krútená dvojlinka (UTP) a jej zapojenia na konektory RJ-45

Typy pre výrobu prepojovacích káblov:
Priamy (straight) kábel: 568A ←→ 568A, resp. 568B ←→ 568B (z funkčného hľadiska ekvivalent)
Krížený (cross) kábel: 568A ←→ 568B
Pri nedodržaní zapojenia krútených párov (napr. dve stočené žily musia končiť na pinoch 4,5) sú degradované frekvenčné prenosové vlastnosti kábla. Následkom sú napr. stavy, že 10Mbps funguje, 100Mbps sa už "nechytí".

LAN siete

Sieť typu LAN (Local Area Network) je prepojenie distribuovaných skupín DTE (spravidla počítačov, serverov, periférnych zariadení...) umiestnených v jednej budove, príp. komplexe budov. Všeobecne ide o akékoľvek komunikujúce zariadenia – špeciálne technológie, snímače, ústredne, vysielače atď. Vzhľadom na menšie vzdialenosti bolo možné vyvinúť technológie, ktoré poskytujú vyššie prenosové kapacity ako na sieťach WAN. Z hľadiska zaradenia do RM OSI modelu špecifikujú Fyzickú a Linkovú vrstvu, pričom Linková vrstva je kvôli komplexnosti rozdelená na podvrstvy MAC a LLC.

Fyzická vrstva definuje spôsob vysielania a prijímania bitov, generovanie a odstraňovanie preambuly kvôli synchronizácii , kódovanie/dekódovanie signálov. Ďalej definuje samotné prenosové médium, typy konektorov atď.

Linková vrstva je pri LANoch pomerne komplexná a preto je rozdelená na dve podvrstvy – LLC a MAC. Dôvodom je, že tradičné linkové protokoly (HDLC) nepoznajú riadenie prístupu pre viaceré zdroje a na viaceré ciele a navyše postačuje jedna špecifikácia protokolu LLC, ktorý môže byť použitý v spojení s viacerými MAC podvrstvami.

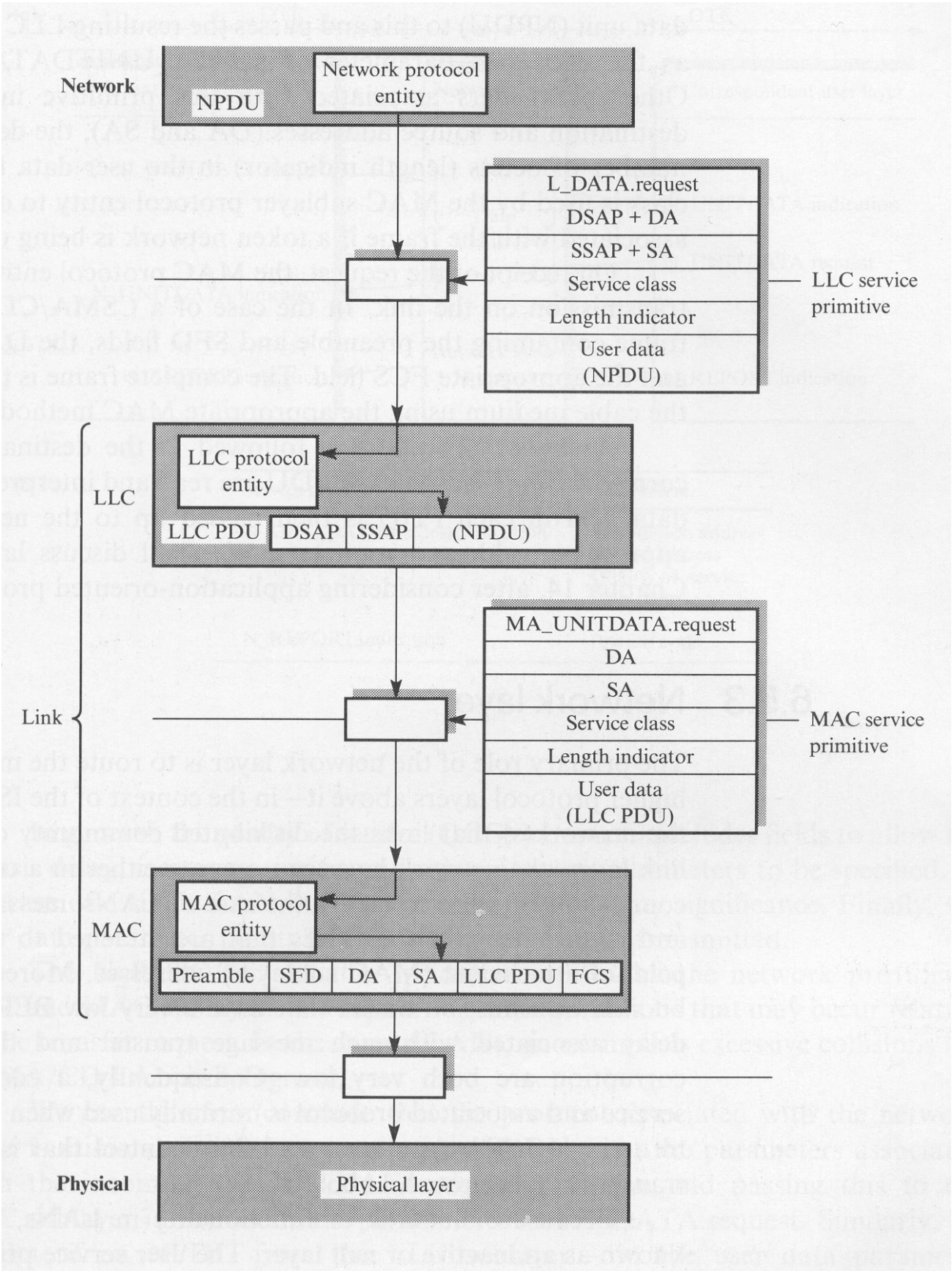
MAC podvrstva (Medium Access Control) zabezpečuje formátovanie dát do rámcov (**frejming**) a spätne získanie dát z prijatých rámcov vrátane detekcie chýb (CRC validation). Ďalej zabezpečuje vyhodnotenie adries a **riadi prístup na** spoločné prenosové **médium** pomocou prístupovejmetódy (CSMA/CD, Token ring, token bus, wireless CSMA/CA).
Bez ohľadu na samotnú prístupovú metódu (CSMA/CD, Token ring, token bus, wireless) je definovaný štandardný súbor primitív pre LLC podvrstvu, aby táto mohla prenášať LLC PDU protiľahlej vrstve.
MAC sublayer service primitívy sú:

MA_UNITDATA.request, MA_UNITDATA.indication, MA_UNITDATA.confirm,

a tieto sú vymieňané medzi priľahlými podvrstvami – LLC a MAC. Každá service primitíva má priradené parametre, ako napr. destination address, service data unit (v tomto prípade je to LLC PDU), požadovaná class of service (priorita - pri token ringu a token buse).

LLC podvrstva (Logical Link Control) špecifikuje linkový protokol odvodený od HDLC. Zabezpečuje error control, flow control, link management. Prostredníctvom prístupových bodov SAP poskytuje pre vyššie vrstvy tri druhy služieb – spojovo orientovanú, bez spojovej orientácie s potvrdzovaním, bez spojovej orientácie bez potvrdzovania. V praxi sa využíva služba **bez spojovej orientácie bez potvrdzovania.** Táto služba má iba dve servisné primitívy L_DATA.request a L_DATA.indication ktoré sú posielané v UI rámcoch (Unnumbered Information).

Nasledovný obrázok znázorňuje interakcie medzi jednotlivými vrstvami. Prehľadne zobrazuje význam interfejs, entita, PDU a SDU na jednotlivých podvrtvách.



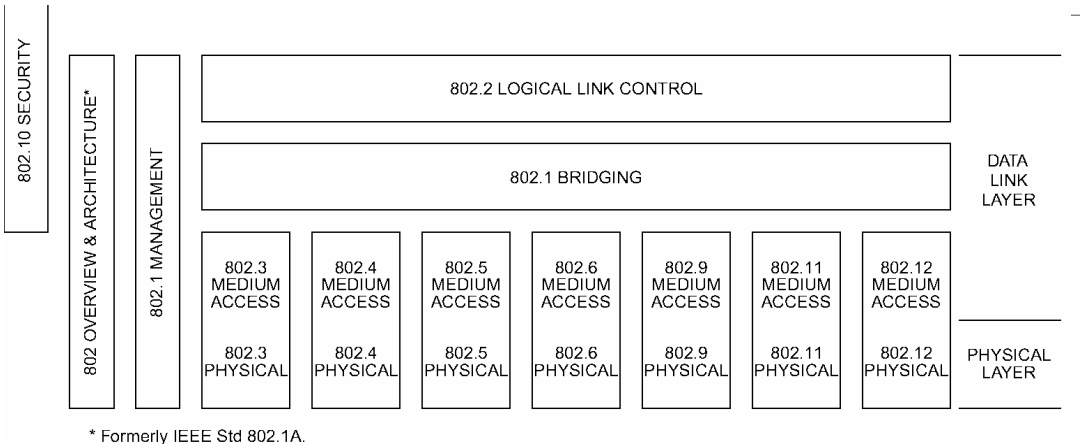
Najrozšírenejšie štandardy špecifikujúce siete LAN sú štandardy IEEE rady 802.xy, ktoré sú spravidla vytvárané na základe de-facto štandardov (napr. Ethernet-u, Token Ring-u...). Štandardy IEEE 802.x sú preberané aj ako ISO štandardy, označované sú ISO 8802.x.

Príklad:
Štandard IEEE 802.3 špecifikuje siete typu CSMA/CD a bol vytvorený na základe existujúceho štandardu siete Ethernet.

Jednotlivé vrstvy, ktoré špecifikujú siete LAN možno zobraziť nasledovne:

<table>
<tr><td colspan="2">Vyššie vrstvy</td><td>Príklady štandardov IEEE 802.x</td></tr>
<tr><td rowspan="2">Linková vrstva</td><td>LLC podvrstva</td><td>802.2 LLC</td></tr>
<tr><td>MAC podvrstva</td><td>802.3 MAC</td></tr>
<tr><td colspan="2">Fyzická vrstva</td><td>802.3 PHY</td></tr>
</table>

Štandardy 802.x možno zapadajú do RM OSI modelu nasledovne:



O čom hovoria jednotlivé štandardy:
802.1 Higher Layer Interface
802.2 LLC
802.3 CSMA/CD (Ethernet)
802.4 Token Bus
802.5 Token Ring
802.6 MAN –DQDB
....
802.11 Wireless LAN
802.12 100 (Base) VG-AnyLAN

Druhy LAN-ov
LAN siete môžu byť organizované do rôznych **topológií**, najčastejšie je to **zbernica, hviezda, kruh, príp. strom**. Je potrebné poznamenať, že topológie môžu byť logické a fyzické. Napríklad sieť typu Ethernet má logickú štruktúru zbernice, keď sa však použijú zariadenia HUB tak fyzická topológia je v tvare hviezdy.

Podľa toho, aké **prenosové médium** využívajú poznáme LAN siete s pevným prenosovým médiom (**wired**), ktoré využívajú koaxiálny kábel, krútenú dvojlinku prípadne optické vlákna a LAN siete, ktoré využívajú šírenie voľným priestorom – bezdrôtové (**wireless**) siete.

V LAN sieťach je medzi jednotlivými stanicami zdieľané jedno prenosové médium pomocou prístupovej metódy (MAC). Podľa toho, akú **prístupovú metódu** využívajú na prístup na spoločné prenosové médium môžeme hovoriť o LAN sieťach typu **CSMA_CD** (predstaviteľom je Ethernet, resp. 802.3), typu **Control Token** (Token Ring, Token Bus) a iných typov (DQDB, FDDI, VG-AnyLAN).

LAN siete typu Ethernet

Najrožšírenejším a najpoužívanejším typom LAN siete sú siete založené na technológii Ethernet. Ethernet je relatívne stará technológia, prežila vďaka flexibilite, jednoduchosti a spätnej kompatibilite. Existuje viacero druhov sietí založených na tejto technológii. Možno definovať 3 kategórie sietí typu Ethernet, hlavne podľa prenosových rýchlostí:

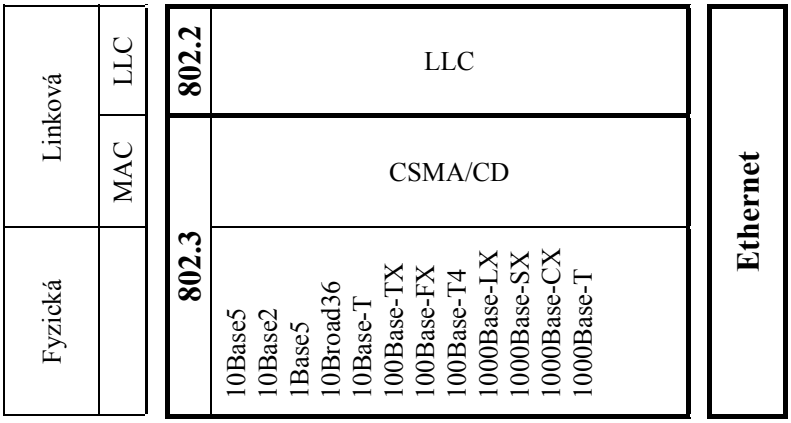
špecifikácie **Ethernet a IEEE802.3** – 10Mbps na koaxiálnom kábli
špecifikáciu **Fast Ethernet** – 100Mbps na Twisted-pair
špecifikáciu **Gigabit Ethernet** – 1000Mbps

História

Základ tvorí baseband LAN špecifikácia od firmy Xerox zo 70-tych rokoch. Táto bola postavená na koaxiálnom kábli, rýchlosti 10Mbps, používajúc prístupovú metódu CSMA/CD. Pomenovanie Ethernet sa v súčasnoti používa pre všetky CSMA/CD siete, v roku 1980 bola na jeho základe vytvorená špecifikácia IEEE 802.3. Následne bola v rámci spoločného vývoja firiem DEC, Intel a Xerox vytvorená špecifikácia Ethernet version 2, ktorá je kompatibilná s IEEE 802.3.

Zaradenie do RM OSI

Hlavný rozdiel v špecifikáciách Ethernet a 802.3 je v tom, že 802.3 špecifikuje iba MAC podčasť Linkovej vrstvy, pričom Ethernet špecifikácia definuje celú Linkovú vrstvu. Na druhej strane, Ethernet špecifikuje iba jedno prenosové médium, pričom IEEE 802.3 ich definuje niekoľko (rôzne druhy koaxiálnych káblov, krútených dvojliniek a optických vlákien).



Základné vlastnosti

LAN siete typu Ethernet sú broadcast-based siete, t.j. každý rámec je vyslaný všetkým staniciam a tak všetky stanice vidia všetky rámce v sieti. Takže každá stanica musí rozhodnúť, či jej daný rámec patrí, alebo nie. (V tzv. promiscuidnom móde prijíma stanica všetky rámce). CSMA/CD siete sú určené hlavne pre aplikácie, pri ktorých komunikačné médium musí vedieť prenášať sporadickú, príležitostne obrovskú trafiku pri veľkých rýchlostiach. Nezaručuje však napr. doručiteľnosť správy (**QoS –** Quality of Service) do určitého času. Neexistujú priority, prístup je stochastický, pri preťažení siete ide priepustnosť prudko dole a žiadne stanice (bez rozdielu) nemôžu komunikovať.

Ako prístupovú metódu využíva CSMA/CD (vysvetlené v predošlej časti). Tu len dodávame nasledovnú aplikáciu vysvetlenia na technické podmienky (nie chodba a kancelárie):

- stanica počúva, keď je ticho, tak začne vysielať svoj rámec
- zároveň aj počúva, či niekto iný svojím vysielaním neporušil/neruší jej vlastné vysielanie
- to môže nastať vtedy, keď stanice začnú vysielať naraz, resp. vysielanie jednej ešte nedorazilo k ďalšej vysielania-chtivej stanici, ktorá teda predpokladá, že médium je voľné (z toho vyplýva dôležitý vzťah medzi **minimálnou dĺžkou rámca** a **maximálnou dĺžkou segmentu** spoločného média – kábla)
- pri takejto kolízii obe stanice teda zastavia vysielanie, dokonca ešte vyšlú signál, ktorým to "pokazia úplne", nastavia si back-off timer na náhodne vygenerovanú hodnotu a po takomto čase znovu skúsia vysielať.
- štatisticky sú vygenerované backoff-timre tak rozdielne, že nedôjde ku kolízii už raz kolidovaných staníc
- pri tejto metóde nie sú priority – je to stochastický prístup zdielania média
- medzi jednotlivými rámcami musí byť Inter Frame Gap – časová medzera pre ostatných (aby sa dostali aj iní k slovu, t.j. princíp slušnosti – vždy, keď som využil spoločné medium na moju komunikáciu – obmedzenú

veľkosťou rámca, tak na chvíľočku stíchnem, a nechám možnosť pre ostatných, aby začali vysielať – ak chcú)

Poznámka:
Toto je historický fakt – platí pri Ethernete, resp. základnom 802.3. Pri switchoch už nie, ale treba poznať princíp, lebo napr. pri „ARP poisoningu" a zaplavení ARP tabuľky switcha falošnými údajmi je možné z neho spraviť HUB – a potom hovoríme o Ethernete. Okrem toho je faktom, že táto technológia je rozšírená aj v takých oblastiach, ako sú výrobné prevádzky, riadiace systémy a pod. Je to vďaka "hrubej sile", teda predimenzovaniu kapacít, ktoré Ethernet technológia ponúka (prenosové rýchlosti 10Mbps, 100Mbps a už aj 1Gbps sú dnes úplne bežne používané).

Formát rámcov
Na linkovej vrstve hovoríme o rámcoch (frejmoch), napr. HDLC rámec. Medzi formátom rámca podľa špecifikácie Ethernet a IEEE 802.3 je malý rozdiel:

Ethernet

7	1	6	6	2	46-1500	4
Preamble	SOF	Destination address	Source address	type	data	FCS

IEEE 802.3

7	1	6	6	2	46-1500	4
Preamble	SOF	Destination address	Source address	Length	802.2 header and data	FCS

- *preamble* – striedajúce sa 0 a 1-ky (zapískanie na médium)
- *SOF (Start of Frame)* – oznámenie, že pískanie končí a začína rámec – dvomi jednotkami na konci SOF
- *DA a SA (Destination, Source Address)* – tzv. **MAC adresy** dĺžky 6B (48bitov)– prvé 3 Byte označujú výrobcu, ďalšie 3 konkrétnu kartu. SA je vždy unicast, DA môže byť unicast, multicat alebo broadcast
- *Type* – (iba pri Ethernete) – definuje protokol vyššej vrstvy (napr. IP)
- *Length* (iba 802.3) – počet Byte-ov v nasledujúcom poli (v poli pred FCS)
- *Data* – údaje z vyššej vrsty, Ethernet neumožňuje padding, t.j. musí ich byť aspoň 46, pri 802.3 je možné aj menej vďaka padding Bytes (minimálna dĺžka celého rámca je 64B, aby mohla fungovať detekcia kolízie CSMA/CD aj na maximálnej dĺžke kábla)
- *FCS* – obsahuje CRC hodnotu kvôli kontrolu neporušenosti rámca. Je to "best effort" služba, t.j. pri zistení, že rámec je porušený ho už druhá vrstva zahodí, a nepošle vyššie.

Oba druhy rámcov sa súčasne môžu a v praxi aj často používajú na jednej sieti.

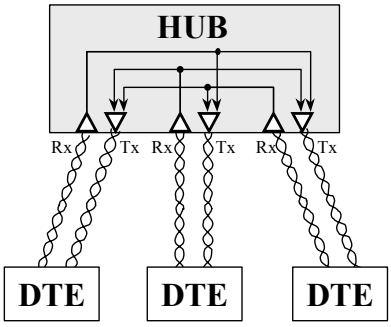
Porovnanie fyzických charakteristík Ethernet a 802.3 špecifikácií

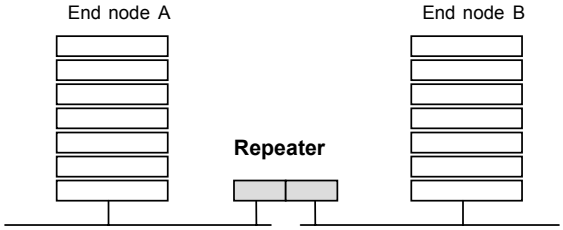
Characteristic	Ethernet Value	IEEE 802.3 Values 10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Data rate (Mbps)	10	10	10	10	10	100
Signaling method	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Maximum segment length (m)	500	500	185	100	2,000	100
Media	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Unshielded twisted-pair cable
Topology	Bus	Bus	Bus	Star	Point-to-point	Bus

Na Ethernet špecifikáciu sa najviac podobá 802.3 10Base5 (t.j. 50 Ohm, hrubý koax)

V súčasnosti sa najviac ako médium pre Ethernet LANy používa krútená dvojlinka, spravidla inštalovaná v budovách vo forme štruktúrovanej kabeláže (pôvodný koaxiálny kábel už nájdeme málokde, princíp však zostáva zachovaný). Spoločne so zariadením nazývaným HUB je priamou náhradou koaxiálneho kábla (logicky to je stále to isté čo koaxiál). Zariadenie HUB iba elektronicky opakuje všetky prišlé signály na ostatné porty – stanice samotné vykonávajú CSMA/CD tak isto, ako pri koaxiálnom kábli. HUB je koncentrátor, do ktorého sa pripájajú koncové stanice a HUB medzi nimi umožňuje komunikáciu. Je možné zapojiť aj viacero zariadení HUB za sebou, resp. do stromovej štruktúry a tak zvýšiť počet zariadení pripojených do siete. Treba si však uvedomiť, že HUB je náhrada koaxiálu a že všetky pripojené stanice zdieľajú 1 prenosové médium a pomocou CSMA/CD metódy sa oň "bijú". Čím je staníc viac, tým je reálna prenosová kapacita pripadajúca na jednu stanicu nižšia a priepustnosť siete prudko klesá.
HUB je zariadenie pracujúce na prvej (fyzickej) vrstve RM OSI modelu, nepozná teda formát rámcov a pracuje iba na úrovni prenosu bitov, resp. prenášaných signálov. Funkčne ho možno prirovnať k opakovaču.

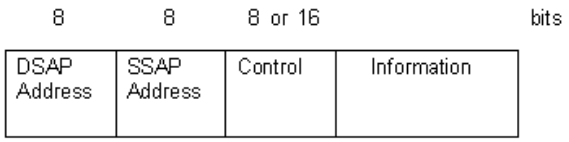
Funkcia zariadenia HUB – náhrada za pôvodný koaxiálny kábel





LLC

Some discussion is warranted on the LLC field. The 802.2 committee developed the **Logical Link Control (LLC)** to operate with 802.3 Ethernet as seen in the above diagram. LLC is based on the HDLC format and more detail can be found by following the link. Whereas Ethernet II (2.0) combines the MAC and the Data link layers restricting itself to connectionless service in the process, IEEE 802.3 separates out the MAC and Data Link layers. 802.2 (LLC) is also required by Token Ring and FDDI but cannot be used with the Novell 'Raw' format. There are three types of LLC, Type 1 which is connectionless, Type 2 which is connection-oriented and Type 3 for Acknowledged Connections.



The **Service Access Point (SAP)** is used to distinguish between different data exchanges on the same end station and basically replaces the Type field for the older Ethernet II frame. The **Source Service Access Point (SSAP)** indicates the service from which the LLC data unit is sent, and the **Destination Service Access Point (DSAP)** indicates the service to which the LLC data unit is being sent. As examples, NetBIOS uses the SAP address of **F0** whilst TCP uses the SAP address of **06**. The Control Field identifies the type of LLC, of which there are three:

- **Type 1** - uses **Unsequenced Information (UI)** (Indicated by a Control Field value of **03**) frames to set up unacknowledged connectionless sessions.
- **Type 2** - uses **Information (I)** frames and maintains the sequence numbers during an acknowledged connection-oriented transmission.
- **Type 3** - uses **Acknowledged Connection (AC)** frames in an acknowledged connectionless service.

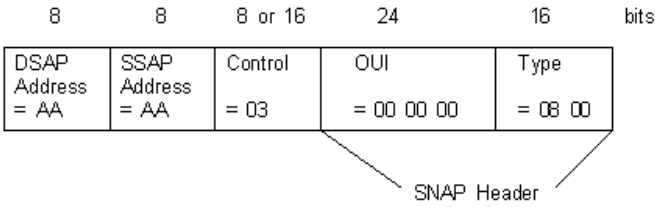
3.2 I/G and U/L within the MAC address

With an Ethernet MAC address, the first octet uses the lowest significant bit as the I/G bit (Individual/Group address) only and does not have such a thing as the U/L bit (Universally/Locally administered). The U/L bit is used in Token Ring A destination Ethernet MAC address starting with the octet '05' is a group or multicast address since the first bit (LSB) to be transmitted is on the right hand side of the octet and is a binary '1'. Conversely, '04' as the first octet indicates that the destination address is an individual address. Of course, in Ethernet, all source address will have a binary '0' since they are always individual.

The first 3 octets of the MAC address form the Organisational Unique Identifier (OUI) assigned to organisations that requires their own group of MAC addresses. A list of OUIs can be found at OUI Index.

3.3 Subnetwork Access Protocol (SNAP)

The SNAP protocol was introduced to allow an easy transition to the new LLC frame format for vendors. SNAP allows older frames and protocols to be encapsulated in a Type 1 LLC header so making any protocol 'pseudo-IEEE compliant'. SNAP is described in RFC 1042. The following diagram shows how it looks:

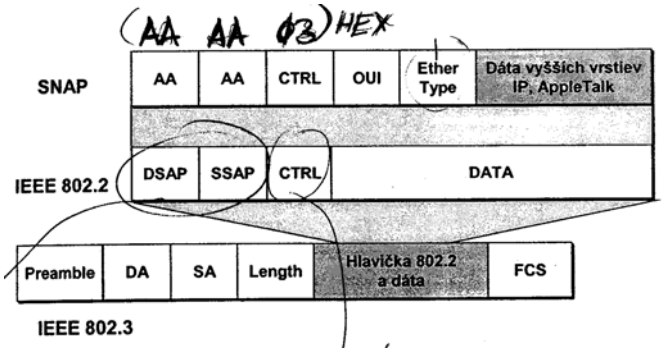


As you can see, it is an LLC data unit (sometimes called a **Logical Protocol Data Unit (LPDU)**) of Type 1 (indicated by 03). The DSAP and SSAP are set to **AA** to indicate that this is a SNAP header coming up. The SNAP header then indicates the vender via the **Organisational Unique Identifier (OUI)** and the protocol type via the Ethertype field. In the example above we have the OUI as 00-00-00 which means that there is an Ethernet frame, and the Ethertype of 08-00 which indicates IP as the protocol. The official list of types can be found at Ethertypes. More and more vendors are moving to LLC1 on the LAN but SNAP still remains and crops up time and time again.

Have a look at the document IPX for further discussion of 802.3 and 802.5 headers (SNAP etc.) in an IPX environment.

Subnetwork Access Protocol – SNAP

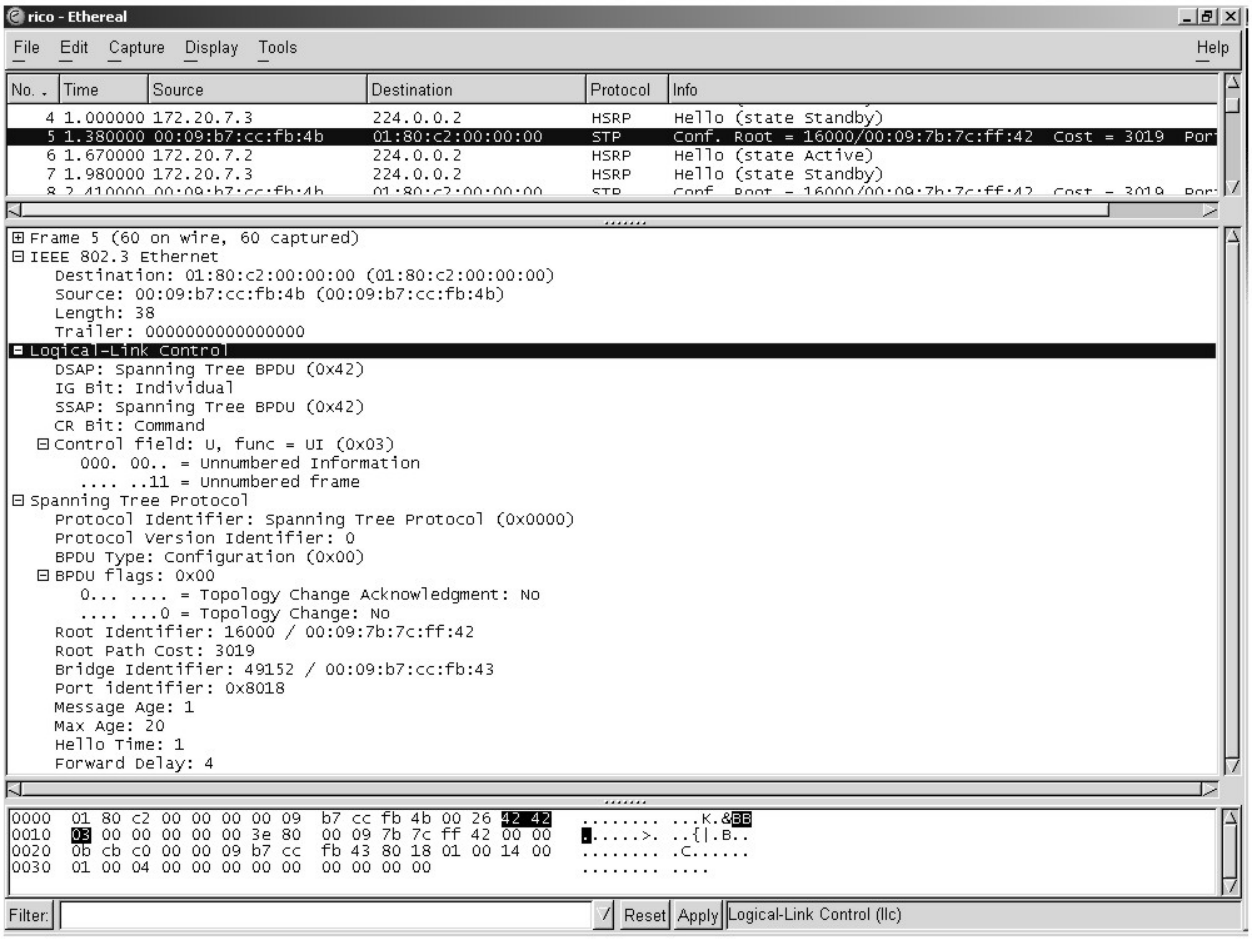
- enkapsulácia protokolov tretej vrstvy, ktoré nie sú úplne OSI kompatibilné, napr. aj IP do 802.2 je možné pomocou SNAP
- funguje to tak, že ako DSAP a SSAP sa natvrdo napíše hodnota AA, a je jasné, že sa encapsuluje

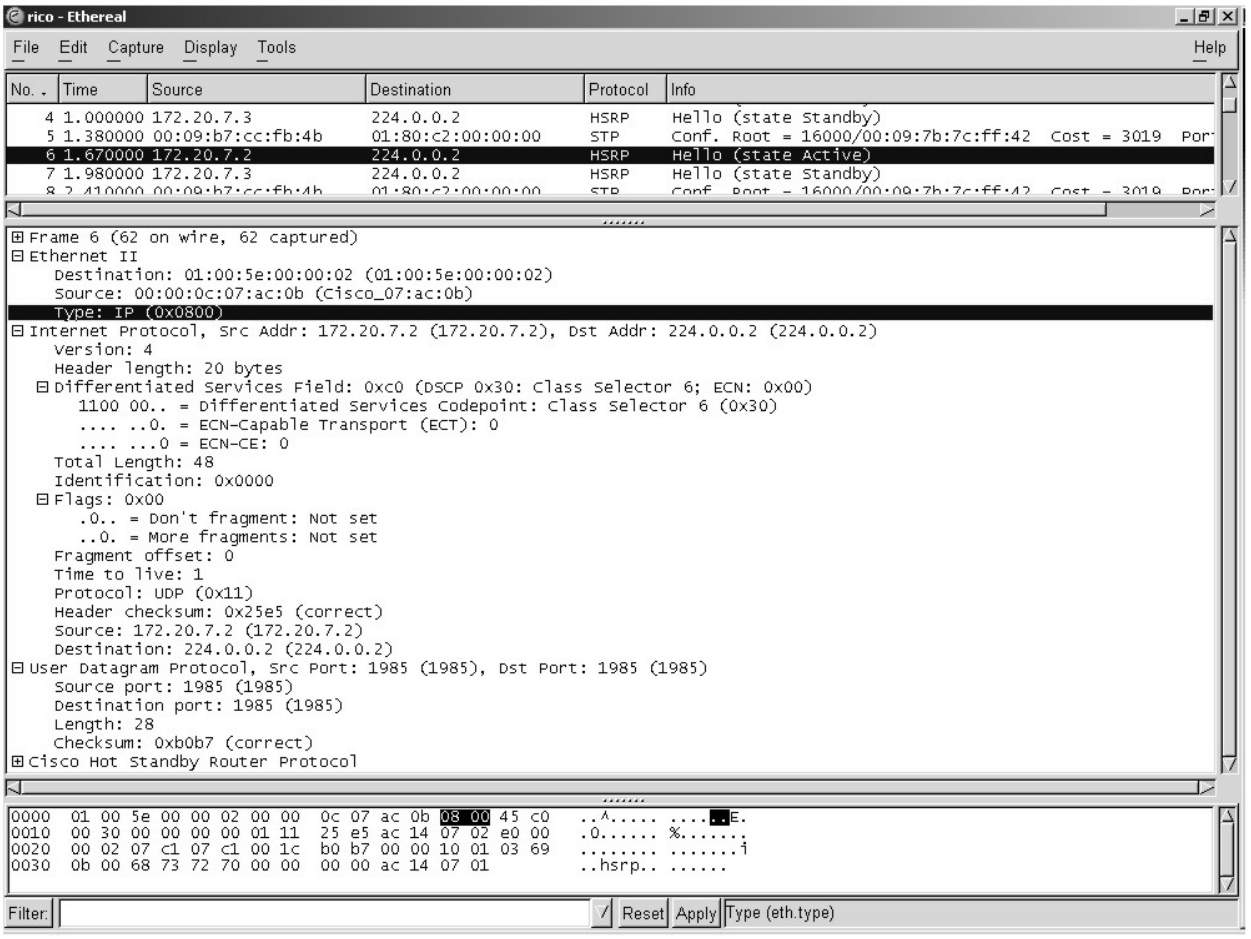


pôvodný protokol akoby do Ethernet II rámca (v hlavičke SNAP-u je Ethertype pole)

The LLC defines service access for protocols that conform to the Open System Interconnection (OSI) model for network protocols. Unfortunately, many protocols do not obey the rules for those layers. Therefore, additional information must be added to the LLC in order to provide information regarding those protocols. Protocols that fall into this category include IP and IPX. The method used to provide this additional protocol information is called a Subnetwork Access Protocol, or SNAP frame. A SNAP encapsulation is indicated by the SSAP and DSAP addresses being set to "0 x AA". When that address is seen, we know that a SNAP header follows. The SNAP header is 5 bytes long: the first 3 bytes consist of the organization code, which is assigned by the IEEE; the second 2 bytes use the type value set from the original Ethernet specifications.

Porovnanie a koexistencia rámcov 802.3 a Ethernet v.II





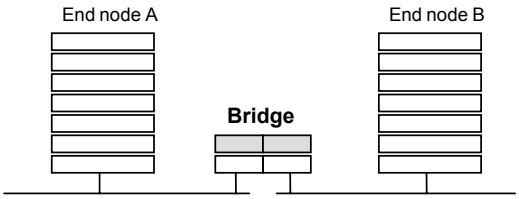
LAN Bridging

Ďalším spôsobom ako prepájať časti siete siete, resp. celé siete je prepájanie pomocou tzv. mostov (bridgov). Bridge je zariadenie pracujúce na druhej, linkovej úrovni. Spočiatku (od 80. rokov) bridge prepájali rámce medzi homogénnymi sieťami, v súčasnosti sú dostupné aj bridge medzi rôznymi sieťami.

O **transparentom bridgingu** hovoríme hlavne v Ethernet sieťach, kedy prepájajú segmenty Ethernet sietí na základe cieľovej adresy a lokálnej tabuľky. Pri iných typoch sieťach, napr. pri Token ringoch hovoríme o tzv. **source-route bridgingu**, kedy bridge prepájajú prepája na základe cesty, ktorá je celá obsiahnutá v samotnom rámci. Pokiaľ je potrebné prepojiť rôzne druhy LAN sietí, spravidla Ethernet a Token ring musí dôjsť k preklad formátov rámcov a princípov jednotlivých sietí. Vtedy hovoríme o tzv. **translation bridgingu**, prípadne **source route translation bridgingu**, ktorý je kombináciou algoritmov transparentného a source-route bridgingu.

Bridge môžu byť lokálne, alebo vzdialené (remote). Lokálne prepájajú segmenty v tej istej oblasti, vzdialené spájajú viaceré segmenty LAN v rôznych oblastiach obyčajne cez telekomunikačné linky. Preto musia prispôsobovať rýchlosti medzi LAN a WAN, obyčajne silným bufferingom.

Vzhľadom na štandardy 802.x a ich spoločnú LLC vrstvu, sú bridge pracujúce na MAC podvrstve, vtedy spájajú rovnaké siete, a sú aj bridge pracujúce na LLC podvrstve, spájajúce aj nehomogénne siete – napr. 802.3 a 802.5. Samozrejme bridgovanie rozdielnych sietí nie je dokonalé, napr. Ethernet nemá priority.



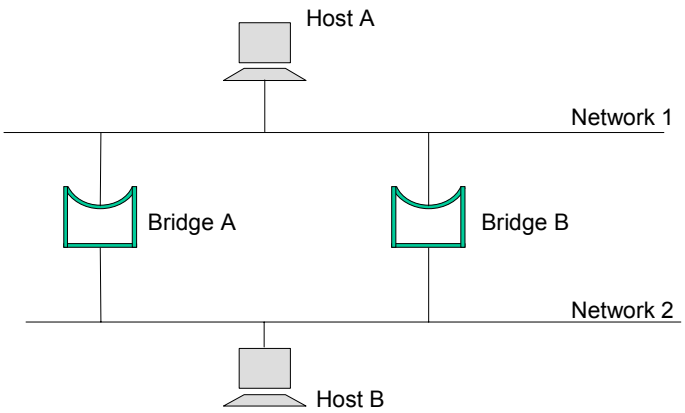
V súčasnosti už obyčajne **funkciu bridgov**, ktoré prepájajú rôzne druhy sietí, ale aj vzdialené segmenty jedného typu siete **vykonávajú** zariadenia pracujúce na tretej vrstve, teda **routre**.

Transparentné bridge

Prvé boli vyvinuté vo firme DEC (Digital Equipment Corporation) začiatkom 80-tych rokov. Neskôr boli zahrnuté do štandardu 802.1. V Ethernet/802.3 sieťach sú veľmi rozšírené. Pomenovanie "transparentné" majú preto, lebo samotná operácia bridgovania častí siete je pre koncové stanice transparentná. Transparentné bridge sa po zapnutí naučia topológiu na základe analýzy zdrojových adries prichádzajúcich rámcov. Po príchode rámca bridge zistí, či pozná cieľovú adresu (pozrie sa do svojej tabuľky). Ak pozná, pošle rámec na príslušný interface, ak nie pošle na všetky (flooding). V každom prípade si však do tabuľky vloží zdrojovú adresu a zviaže ju s interfejsom, z ktorého rámec prišiel. Transparentné bridge účinne izolujú trafiku vrámci jednotlivých segmentov, čo môže vylepšiť ich priepustnosť.

Bridging loops

Bez dobrého bridge-to-bridge protokolu, transparent bridge algoritmus zlyhá pri viacnásobných cestách, resp. slučkách. Nasledovný obrázok opisuje prípad vzniku nekorektného správania sa (učenia a následného forwardingu) transparentných bridgov zapojených do slučky.



Čo sa vlastne stane:
- Host A pošle frame na Host B
- Oba bridge dostanú tento rámec, zapíšu si, že Host A je na sieti 1 a (oba!!) pošlú rámec na sieť 2 (hostu B)
- Sieť 2 je zdielané médium, takže to pošlú postupne, povedzme, že Bridge A pošle rámec pre Host B skôr
- vtedy tento rámec dostane aj Bridge B, a zo zdrojovej adresy sa naučí, že Host A je na sieti 2 (lebo odtiaľ prišiel rámec, nevie, že prišiel z bridgu), cieľová adresa – teda host B je na sieti 2, tak rámec neforwardne – nechá ho tak
- na Bridge B pritom ešte čaká na forwardnutie na sieť 2 pôvodný rámec z Hosta A na Host B, tak ho teda pošle na sieť 2
- Teraz sa zase Bridge A chybne naučí, že Host A je na sieti 2
- Keď host B chce poslať odpoveď na Host A, bridge rámce nepošlú na sieť 1, lebo si myslia, že Host A je na sieti 2

V prípade, že by sa jednalo o broadcast rámec, tak by bridge donekonečna preposielali jeho kópie a naplno by zaťažili sieť – nastal by tak kolaps siete. Bridge sa takýmto spôsobom vedia "oklamať" a obyčajne dôjde k úpnej záplave siete, v menej horšom prípade k mylným informáciám v tabuľkách bridgov a teda "odstrihnutím" niektrorých hostov. Riešením je Spanning Tree Algoritmus.

STA – spanning tree algoritmus

Tento algoritmus bol vyvinutý firmou DEC a následne prijatý ako štandard **IEEE 802.1d** (nie však úplne totožné, ani nie kompatibilné). Princíp spočíva vo vytvorená takej štruktúry siete, ktorá neobsahuje slučky – ako vetviaci sa strom (vychádza sa z teórie grafov, podľa ktorej pre každú štruktúru prepojenia nodov existuje stromové zapojenie bez slučiek). Nadbytočné (redundantné) vetvy nie sú fyzicky odstránené, ale sú uvedené napr. do stavu *blocking*. Následne takéto porty môžu byť aktivované, v prípade zlyhania/výpadku hlavnej linky.

Ako je vlastne STA implementovaný?
- zvolí sa route, potom najlepšie cesty k nemu, tie sa aktivujú a ostatné sú uvedené do stavu blocking
- je na to samostatný protokol, v hello-time intervale behajú neustále hello pakety, aby sa sieť vedela zrekonfigurovať, konfiguračné správy sa volajú BPDU (bridge protocol data unit)
- všetky rozhodnutia o topológii pri transparentnej topológii sa robia lokálne – každý si rozhoduje sám (neexistuje centrálna autorita) na základe výmeny správ so susedmi.

8.3 Spanning Tree Initialisation

On initial setup, all participating bridges declare themselves to be the root, they then exchange Hello (or Configuration) **Bridge Protocol Data Units (BPDU)** containing specific bridge information. The BPDUs are sent to the well-known multicast address **0x0180c2000000**. There are two types of BPDUs, **Configuration BPDUs** used for bridge and port elections, and there are **Topology Change Notification (TCN) BPDUs** which are sent back up towards the root when there is a topology change. BPDUs are sent to a well-known multicast address.

8.4 Bridge Protocol Data Unit (BPDU)

These BPDUs are in the following format:

2	1	1	1	8	4	8	2	2	2	2	2 Octets
Protocol ID	Version	Message Type	Flags	Root ID	Root Cost	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

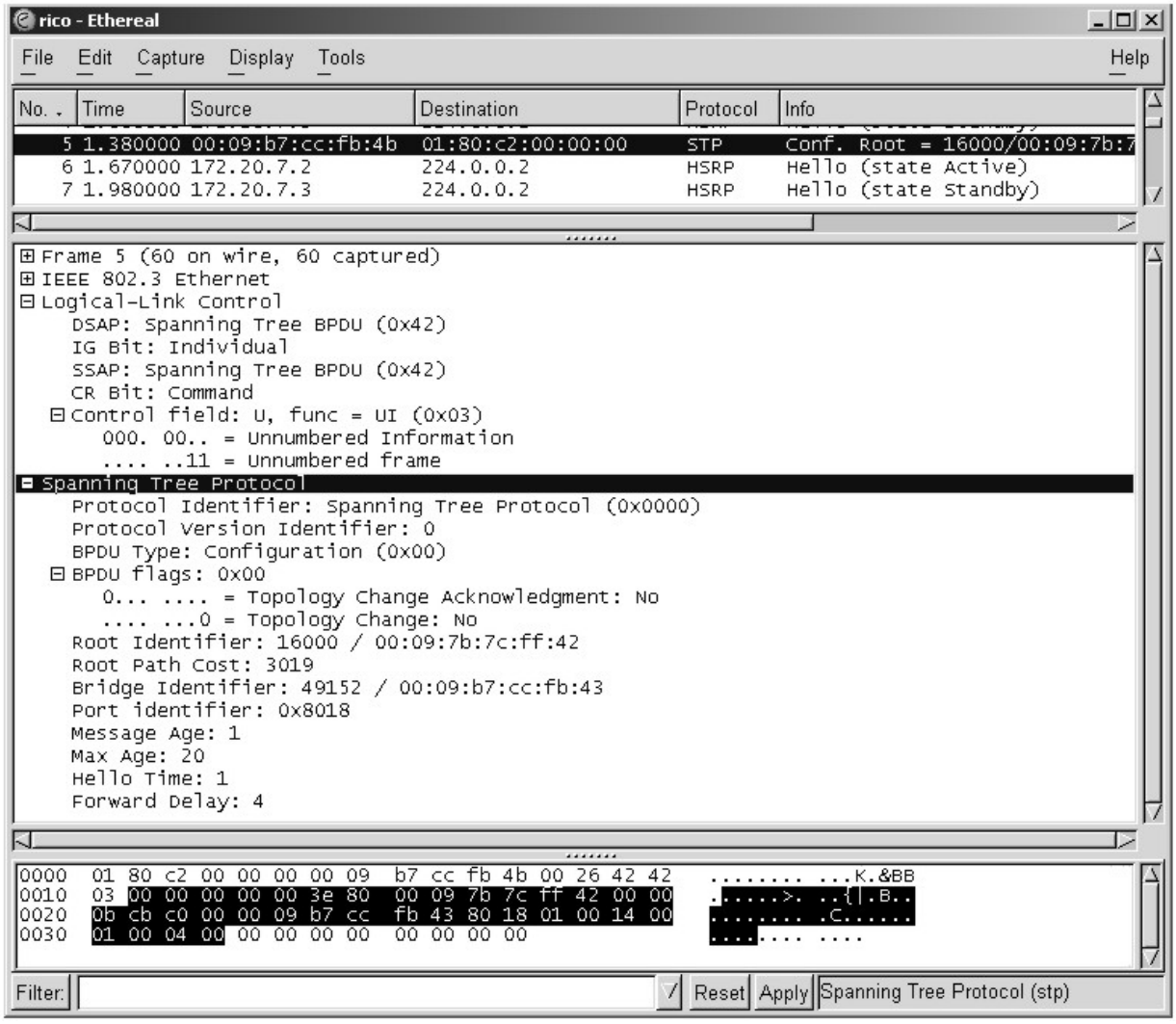
- **Protocol ID** - indicates that the packet is a BPDU.
- **Version** - the version of the BPDU being used.
- **Message Type** - the stage of the negotiation.
- **Flags** - two bits are used to indicate a change in topology and to indicate acknowledgement of the TCN BPDU.
- **Root ID** - the root bridge priority (2 bytes) followed by the MAC address (6 bytes).
- **Root Path Cost** - the total cost to from this particular bridge to the designated root bridge.
- **Bridge ID** - the bridge priority (2 bytes) followed by the MAC address (6 bytes), lowest value wins! The default bridge priority is 0x8000 (32768_{10}).
- **Port ID** - the ID of the port from which are transmitted the BPDUs, a root port, this is made up of the configured port priority and the bridge MAC address.
- **Message Age** - timers for aging messages (only has effect on the network if the root bridge is configured with this parameter).
- **Maximum Age** - the maximum message age before information from a BPDU is dropped because it is too old and no more BPDUs have been received. (only has effect on the network if the root bridge is configured with this parameter). The default value for this is 20 seconds.

- **Hello Time** - the time between BPDU configuration messages sent by the root bridge (only has effect on the network if the *root* bridge is configured with this parameter). The default value for this is 2 seconds.
- **Forward Delay** - this temporarily stops a bridge from forwarding data to give a chance for information of a topology change to filter through to all parts of the network. This means that ports that need to be turned off in the new topology have a chance to be switched off before the new ports are turned on (only has effect on the network if the root bridge is configured with this parameter). The default value for this is 15 seconds.

The timers are based on the assumption that the diameter of the network is no more than 7 bridges/switches away from the root (including the root bridge).

The following port costs are the current IEEE defaults:

- 10Gbps : 1
- 1Gbps : 4
- 622Mbps : 6
- 155Mbps : 14
- 100Mbps : 19
- 45Mbps : 39
- 16Mbps : 62
- 10Mbps : 100
- 4Mbps : 250



Root ID – 2B priority + MAC adresa roota
Bridge ID – identifikuje odosieľateľa
Root path cost – cena cesty, ktorú má odosielajúci bridge k root bridgu
Port ID- ID portu, z ktorého bola správa odoslaná – využíva sa na odstránenie slučiek
Správa o zmene topológie obsahuje iba prvé 4B (protocol ID, protocol version a message type = 128).

Once the the root bridge has been determined this interface becomes the **Root Port**. Then the other bridges designated to be part of the tree, determine whether any ports are not root ports. These non-designated ports are then placed into the following conditions in order:

- **Blocking Mode** - where no frames are forwarded and just Hello BPDUs are listened to, this lasts for 20 seconds, which is the **Maximum Age Time**.
- Then ports change from Blocking Mode to **Listening Mode** where they remain for 15 seconds (this is called the **Forward Delay Time**), where no data frames are forwarded, they are just listened to, BPDUs however, are both received AND sent.
- Then the ports change to **Learning Mode** for another 15 seconds (again using the Forward Delay time), where still no data frames are forwarded, and addresses are being learned as the bridge/switch builds the forwarding tables.
- Finally, the designated ports move to **Forwarding Mode**, where data frames are forwarded now as well as addresses still being learned.

After this process, if a port fails, then it is placed into a **Disabled State**.

From this sequence, it can be seen that the worst case scenario is if a link is up but it fails to see any more BPDUs, there will be a 20 second wait before the information from the last BPDU ages out. At this point, the port goes into listening mode for 15 seconds and then learning mode for 15 seconds before it starts forwarding data frames again. This adds up to 50 seconds with the default timers.

LAN switche

V súčasnosti sú spravidla v Ethernet sieťach používané tzv. **switche**, ktoré možno považovať za zariadenia vyvinuté z bridgov. Z funkčného hľadiska ich možno opísať ako mnohoportové bridge. Vzájomné porovnanie ich vlastností uvádza nasledovná tabuľka:

switch	bridge
veľa funkcionality realizovaného na HW	implementované SW
aj cez 500 portov	max. 16 portov
vysoká agregovaná bandwidth	
nízka latencia	

Spôsoby prepínania rámcov vo switchoch
Základné metódy sú Store and Forward a Cut-through. V súčasnosti už existuje aj niekoľko hybridov.

- store and forward celý rámec sa načíta, skontroluje a potom prepošle
- cut-through odošle rámec okamžite po zistení cieľovej adresy (bez kontroly)
- fragment free (na cisco), modifikované cut-through, odošle po kontrole prvých 64B
- treshold detection (adaptive switching) – prepínanie medzi jednotlivými módmi podľa výskytu chýb

Spôsob prechodu medzi jednotlivými módmi:

Switching mód:	Defects:	Then, adaptive mode changes the switching mode to:
Cut-through	High numbers of CRC errors	Store-and-forward
	High numbers of runts	Fragment-free
Fragment-free	High numbers of CRC errors	Store-and-forward
	Low numbers of runts	Cut-through
Store-and-forward	Low numbers of CRC errors	Fragment-free
	Low numbers of CRC errors and runts	Cut-through

Switche majú spravidla implementovaný aj transparentný bridging, obyčajne formou **Spanning tree protokolu** (STP). Napr. Cisco má na svojich zariadenia implementovaný Spanning Tree Protocol, ktorý je ešte vylepšený o Port fast, Uplink fast a Backbone fast. Normálne trvá cca 30 sekúnd, kým sa všetky bridge zrekonfigurujú a aktivujú nový port.

Poznámka:
Switche nemožno poprepájať medzi sebou tak, aby vznikli slučky, pretože by došlo ku kolapsu siete. Riešením je implementácia Spannig tree algoritmu, ktorá však so sebou prináša processing a predĺženie "mŕtvych" časov po pripojení nových zariadení, čo nie je vždy z prevádzkového hľadiska prípustné.

Kritériá a obmedzenia pri dizajnovaní sietí typu Ethernet

The Ethernet standard assumes it will take roughly 50 microseconds for a signal to reach its destination (51,4μs)

10Mbps Ethernet is subject to the "5-4-3" rule of repeater placement: the network can only have five segments connected; it can only use four repeaters; and of the five segments, only three can have users attached to them; the other two must be inter-repeater links.

Network Type	Max Nodes Per Segment	Max Distance Per Segment
10BASE-T	2	100m
10BASE2	30	185m
10BASE5	100	500m
10BASE-FL	2	2000m

Fast Ethernet has modified repeater rules, since the minimum packet size takes less time to transmit than regular Ethernet. The length of the network links allows for a fewer number of repeaters. In Fast Ethernet networks, there are two classes of repeaters. Class I repeaters have a latency of 0.7 microseconds or less and are limited to one repeater per network. Class II repeaters have a latency of 0.46 microseconds or less and are limited to two repeaters per network. The following are the distance (diameter) characteristics for these types of Fast Ethernet repeater combinations:

Fast Ethernet	Copper	Fiber
No Repeaters	100m	412m*
One Class I Repeater	200m	272m
One Class II Repeater	200m	272m
Two Class II Repeaters	205m	228m

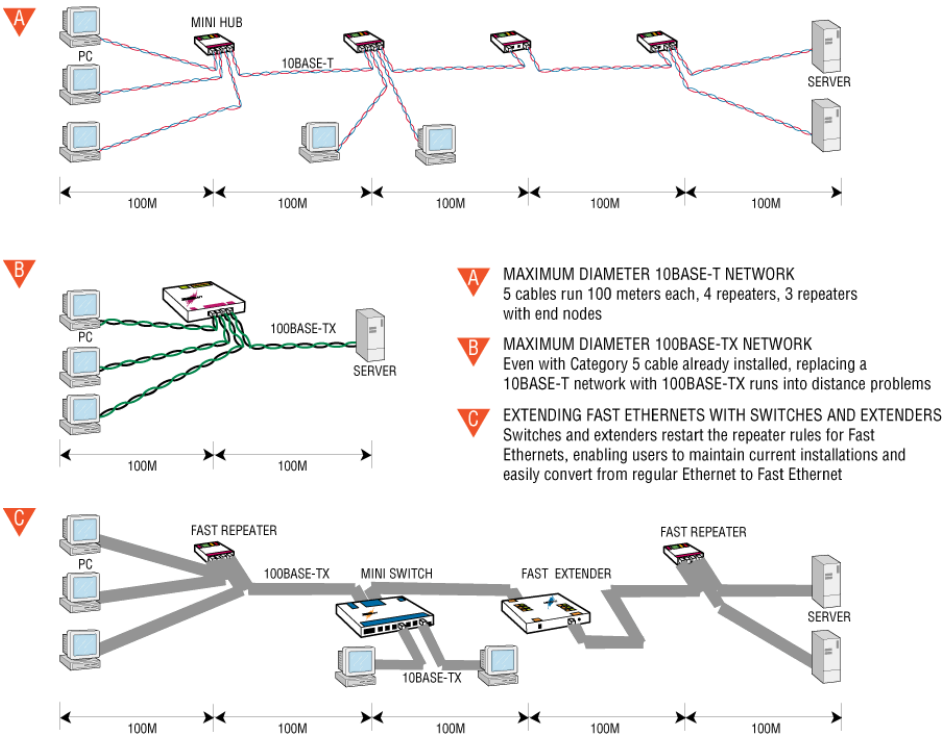
** Full Duplex Mode 2 km*

When conditions require greater distances or an increase in the number of nodes/repeaters, then a bridge, router or switch can be used to connect multiple networks together. These devices join two or more separate networks, allowing network design criteria to be restored.

There is no such thing as the 5-4-3 rule in Fast Ethernet. All 10Base-T repeaters are considered to be functionally identical. Fast Ethernet repeaters are divided into two classes of repeater, Class I and Class II. A Class I repeater has a repeater propagation delay value of 140 bit times, whilst a Class II repeater is 92 bit times. The Class I repeater (or Translational Repeater) can support different signalling types such as 100BaseTx and 100BaseT4. A Class I repeater transmits or repeats the incoming line signals on one port to the other ports by first translating them to digital signals and then retranslating them to line signals. The translations are necessary when connecting different physical media (media conforming to more than one physical layer specification) to the same collision domain. Any repeater with an MII port would be a Class I device. Only one Class I repeater can exist within a single collision domain, so this type of repeater cannot be cascaded. There is only allowed one Class I repeater hop in any one segment.

A Class II repeater immediately transmits or repeats the incoming line signals on one port to the other ports: it does not perform any translations. This repeater type connects identical media to the same collision domain (for example, TX to TX). At most, two Class II repeaters can exist within a single collision domain. The cable used to cascade the two devices is called and unpopulated segment or IRL (Inter-Repeater Link). The Class II repeater (or Transparent Repeater) can only support one type of physical signalling, however you can have two Class II repeater hops in any one segment (Collision Domain).

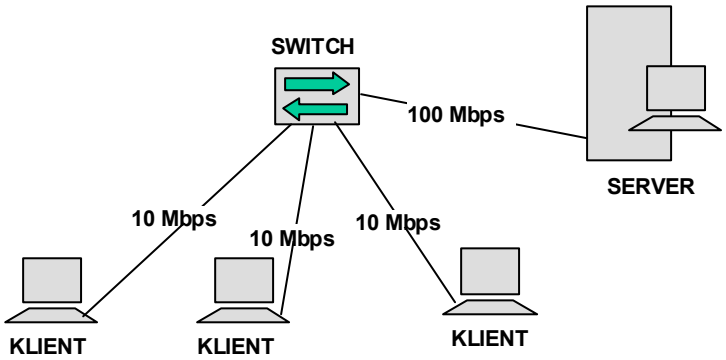
Each network connected via one of these devices is referred to as a separate collision domain in the overall network.



Each port on the hub sends a 'Link Beat Signal' which checks the integrity of the cable and devices attached, a flickering LED on the front of the port of the hub tells you that the link is running fine. The maximum number of hubs (or, more strictly speaking, repeater counts) that you can have in one segment is 4 and the maximum number of stations on one broadcast domain is 1024.

The 4 repeater limit manifests itself in 10/100BaseT environments where the active hub/switch port is in fact a repeater, hence the name multi-port repeater. Generally, the hub would only have one station per port but you can cascade hubs from one another up to the 4 repeater limit. The danger here of course, is that you will have all the traffic from a particular hub being fed into one port so care would need to be taken on noting the applications being used by the stations involved, and the likely bandwidth that the applications will use.

Pri použití zariadení switch v Ethernet sieťach hovoríme o tzv. **Ethernet switching**-u. Je to veľmi efektívny spôsob zvýšenia priepustnosti siete, pretože eliminuje tzv. kolízne domény, t.j. oddelí od seba skupiny zariadení zdieľajúce to isté médium. Celková priepustnosť siete tak niekoľkonásobne vzrastie. Takýmto spôsobom umožňuje viacero komunikácií naraz (samozrejme nie na jeden port). Pri portoch s rôznou rýchlosťou umožňuje napr. viacerým 10Mbps staniciam komunikovať naraz so serverom, ktorý má pripojenie 100 Mbps.

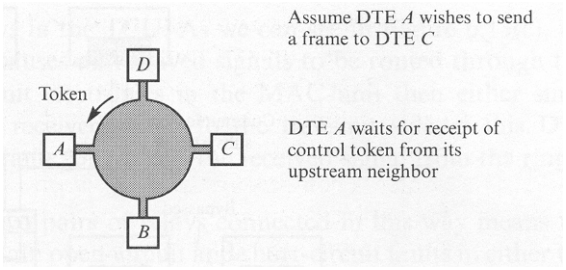


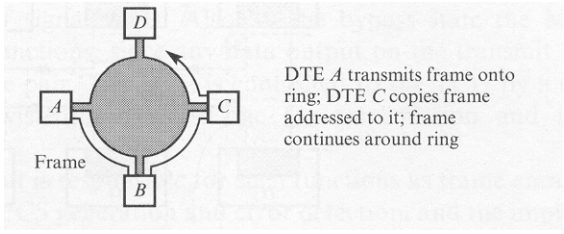
Token Ring

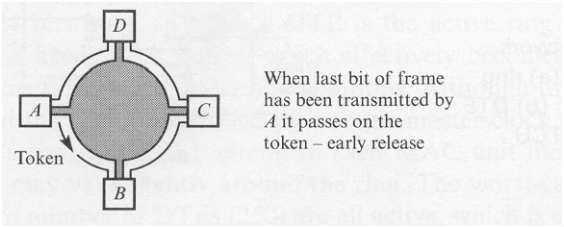
Pôvodne vyvinutý v IBM v 70-tych rokoch. 802.5 je (skoro identická) úplne kompatibilná s IBM Token Ring-om, ktorý v podstate kopíruje.
Jediný rozdiel je v samotnej špecifikácii, kde napr. topológia u IBM Token ringu je *star* a 802.5 ju nešpecifikuje, ale aj tak všetky implementácie majú star topológiu. Podobne je to s médiom, ked IBM Token ring špecifikuje twisted-pair.
Obe siete sú predstaviteľom sietí s MAC metódou **token passing**.
Existujú priority pre jednotlivé rámce, kolízie nemôžu nastať – je to deterministická sieť, dá sa vypočítať, do akého času bude schopná stanica vysielať – a teda aj doručiť správu. Okrem toho má zabudovaných niekoľko fault-management mechanizmov. Preto sú tieto siete oveľa vhodnejšie na kritické aplikácie.

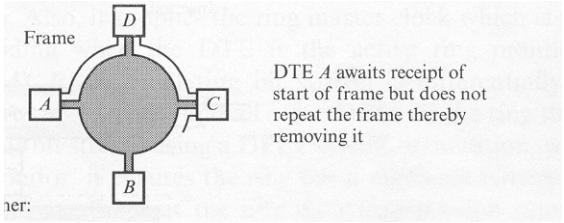
	IBM Token Ring	802.5
Data rates	4 or 16 Mbps	4 or 16 Mbps
Station segment	280 STP, 72 UTP	250
Topology	**Star**	**Not specified**
Media	**Twisted pair**	**Not specified**
Signaling	Baseband	Baseband
Access method	Token passing	Token passing
Encoding	Differential manchester	Differential manchester

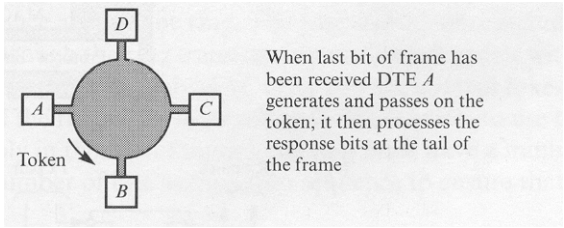
vysielanie rámca v Token ringu











Princíp:

- stanice sú zapojené v logickom kruhu, fyzicky sú zapojené do hviezdy.
- stanice si do kruhu posielajú malý, 3B rámec – token
- stanica A chce vysielať, musí si počkať na token, a pokiaľ je jej priorita väčšia alebo rovná priorite nastavenej v tokene, tak môže vyslať rámec
- tento rámec je opakovaný (t.j. každý bit je prijatý a hneď aj preposlaný) postupne všetkými stanicami v kruhu, až kým nedokrúži späť do zdrojovej stanice, ktorá ho zruší ("zhltne")
- okrem prevyslania si destination zariadenie ešte samozrejme rámec skopíruje doseba, a nastaví A (address-recognized) a C (copy) bit. Tak zdroj vie, že cieľové zariadenie je aktívne a že si rámec skopírovalo
- zdrojové zariadenie uvoľní token (môže ho držať len určitý maximálny čas), a to buď až po zhltnutí obehnutého rámca (pri 4Mbps), alebo token pošle hneď na konci vysielaného rámca (tzv. Early token release – pri 16Mbps)
- pokiaľ by takéto zariadenie medzitým vypadlo, hrozilo by nekonečné krúženie rámca v ringu, a teda aj jeho obsadenie. Tomu predchádza Aktívny monitor (vždy len jedna stanica v sieti), ktorý si každý okoloidúci rámec označí (M bit =1) a keď ide okolo druhýkrát, tak ho zruší a vygeneruje nový token.

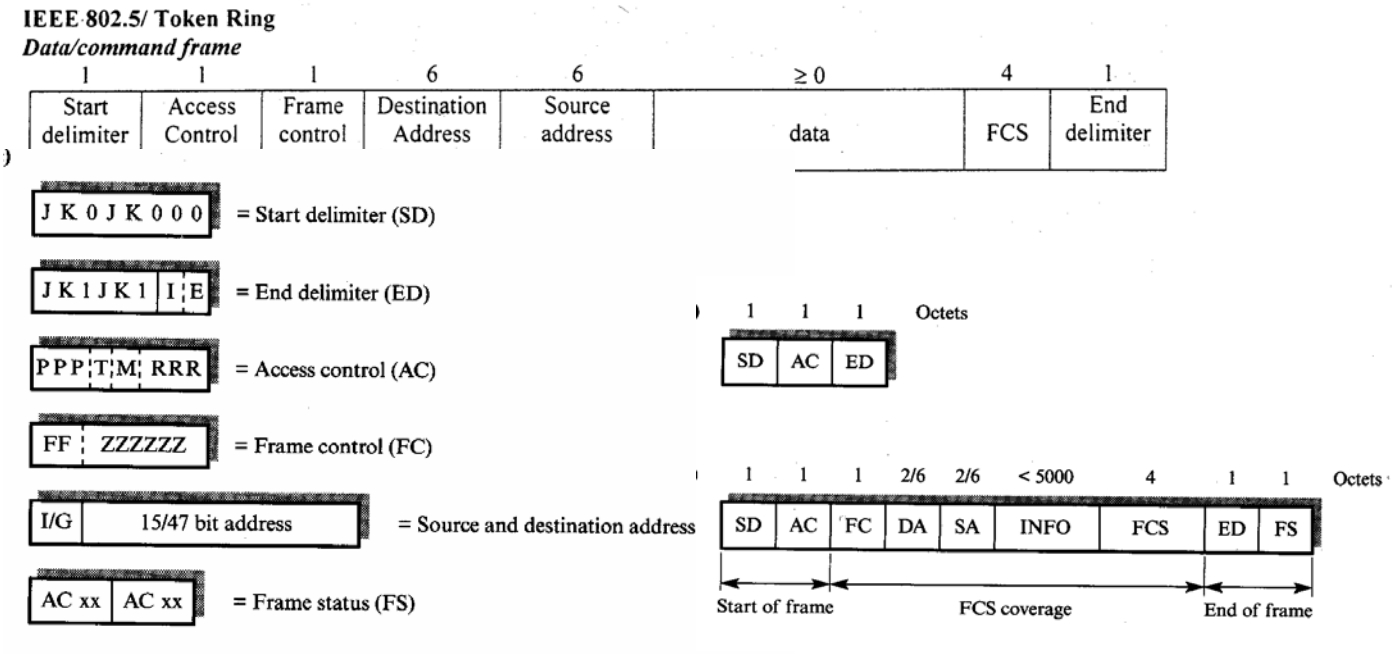
zapojenie do ringu

- kruh je vytvorený tzv. trunk káblom (twisted pair), ktorý spája tzv. trunk coupling unit (TCU). Toto sú elektronické zariadenia s dvomi relé, ktoré vedia robiť napr. bypass, resp. inserted mode (odbočovače typu T).
- zariadenie, resp. jeho MAC časť (MAC unit) sa pripája pomocou Medium Interface kábla (STP – 2 páry) do TCU. Keď je pripojené zariadenie neaktívne, TCU je v bypass móde.
- takýchto TCU môže byť viacero v jednom zariadení, tzv. koncentrátore (niečo ako HUB) a potom sa už zariadenie pripájajú štruktúrovanou kabelážou priamo do koncentrátora
- IBM používa iba takého koncentrátory, nazýva ich multistation access unit (MSAU), stanica sa do nich pripája lobe káblom, samotné MSAU sa prepájajú patch káblami.

MAC unit
vykonáva

- frame encapsulation and de-encapsulation
- FCS generation and error detection
- implementation of MAC algorithm
- keď je v stave active monitor – master clock
  - každý rámec je aktívnym monitorom enkódovaný do Differential Manchester, všetky ostatné stanice majú fázový záves odvodený z tohto toku
  - aktívny monitor navyše zabezpečuje minimum latency time, čo je čas meraný v bitoch potrebný na obehnutie celého ringu (fyzické šírenie + zdržanie na jednotlivých staniciach pri retransmisiách) keď žiadna zo staníc nič nevysiela. Preto má u seba tzv. elastický buffer nastavený na 27 bitov, ktorým vyrovnáva rozdiely o +/-3 bity. Takto môže token obiehať vždy rovnako rýchlo.

formát rámcov



polia SD a ED jednoznačne určujú začiatok a koniec rámca. Normálne bity sú kódované diferenciálnym manchestrom, t.j. prechod je vždy v strede periódy, v týchto poliach majú úrovne celé trvanie.
J – symbol rovnakej polarity ako predošlý, K – otáča polaritu.
bity I a E

- pri tokene vždy rovné nule
- bit I - pri normálnom rámci = 0 znamená, že ide o posledný rámec v postupnosti, ak je rovný 1 tak sa jedná o prvý rámec (resp. niektorý v strede sekvencie)
- bit E – indikuje error – ak hociktorá stanice detekuje chybu (napr. kontrolou CRC), nastaví tento bit na 1 – oznamuje vysielacej stanici, že bola detekovaná chyba

pole AC

- PPP - 3 priority bity
- T – token bit (T=0 token, T=1 frame)
- M – monitor bit
- RRR – 3 reservation bity

pole FC – frame control
definuje typ rámca, ak FF bity indikujú MAC frame, tak daný rámec prijmú všetky DTE a ak je potrebné reagujú podľa ZZZZZZ bitov. Ak FF indikuje I frame (informačný), tak daný rámec prijme len stanica podľa DA

polia SA, DA
16 alebo 48 bitov dlhá adresa, v rámci jedného ringu však iba jeden druh (dlhá alebo krátka)

manchester – 0 = 01 1 = 10
dif. manchester - prechod v strede periódy vždy
0 = zmena polarity oproti predošlému (01 ak bolo 01), 10 ak bolo 10
1 = polarita oproti predošlému zostáva (10 ak bolo 01) 01 ak bolo 10
inak povedané, používa sa priradenie 01 resp. 10, diferenciálny znamená, že 1 sa zakóduje ako zmena, teda opačná dvojica ako predošlá, 0 sa zakóduje rovnakou dvojicou.

pole INFO
prenáša data, resp. doplnkové info, pokiaľ ide o MAC rámce
dĺžka je obmedzená len max. dobou, počas ktorej môže DTE vysielať, v praxi sa však spravidla používa nastavenie na 5 000 B

pole FCS – 32 bitové CRC

pole FS – frame status
A – address-recognized bit
C – copy bit
vysielacia stanica ich nastaví na 0, cieľová stanica nastaví A = 1 ak sa spoznala ako cieľová, a ak daný rámec skopírovala nastaví aj C=1. Z toho potom môže zdrojová stanica usúdiť, či je cieľ živý a ak je, či aj správu prijal.
bity sú 2x kvôli bezpečnosti

bližší popis fungovania

frame tranmission

- prijatie service request na vyslanie data message z vyššej vrstvy (LLC)
- encapsulácia dát v MAC unite do príslušného formátu
- MAC unit čaká na token s prioritou nižšou, resp. rovnou priorite pripraveného rámca
- zakaždým, keď ide token okolo, kontrolujú sa aj rezervačné bity, pokiaľ nie je zarezervovaná vyššia priorita, tak si ju MAC unit rezervuje, inak ich musí nechať tak
- teraz treba počkať, kým konečne príde token s príslušnou prioritou
- môže začať vysielanie
- akonáhle začalo vysielanie, MAC unit prestane opakovať vstup (už iba všetko hltá), až kým sa neobjaví vlastný rámec po obehnutí celého ringu, ten prečíta, zistí A a C bity a následne vyšle token

- stanica môže vyslať aj viacej rámcov naraz, pokiaľ samozrejme ďalšie čakajúce vyhovujú priorite a stanica neprekročila maximum token holding time, spravidla nastavený na 10ms

frame reception
- MAC unit opakuje rámce (repeating) – t.j. na jednom páre prijíma, a na druhý to isté vysiela
- okrem toho detekuje začiatok a koniec rámcov (pomocou SD, ED sekvencií) a rozhodujú, či má byť rámec skopírovaný, alebo len repeated
- ak FF bity indikujú, že ide o MAC frame, tak je rámec skopírovaný a ak treba, MAC unit reaguje na ZZZZZZ bity. Ak ide o Informačný rámec a súhlasí cieľová DA adresa, tak je rámec skopírovaný nabafrovaný na ďalšie spracovanie. V každom prípade sú A a C bity príslušne nastavené pred preposlaním rámca.

priority operation
- rámce s vyššou prioritou sú vždy prenášané na ringu ako prvé
- rámce s rovnakou prioritou majú rovnaké prístupové práva

- stanica, ktorá zobrala token s nižšou prioritou ho po použití vráti na pôvodnú prioritnú úroveň
- samozrejme, pokiaľ má ďalšie čakajúce rámce, ale už jej vypršal čas, môže hneď rezervovať najvyššiu prioritu svojich čakajúcich rámcov. Stále si však musí pamätať pôvodnú, nízku prioritu.

- celé je to dosť zložité, každá stanica si udržuje niekoľko registrov s hodnotami priorít

Ring management

Doteraz boli popísané štandarné postupy, keď je už všetko rozbehnuté, a bezchybovo to funguje. Táto časť rieši práve hraničné situácie – ako naštartovať, ako sa vysporiadať s výpadkami, poruchami a pod.

Initialization

- zariadenie sa chce pripojiť do ringu
- ide do inicializačného módu
- zistí, či jeho zdrojovú adresu niekto nepoužíva
- informuje jeho downstrem suseda, že ide do ringu
- pošle duplicate address test MAC frame, ktorý má DA jeho adresu
- pokiaľ ju niekto príjme a nastaví A bit =1, tak už jeho adresu niekto používa, oznámi to sieťovej management podvrstne a ide do bypass stavu
- ak sa vráti s A=0, tak pošle ďalší MAC frame – standby monitor present SMP MAC frame
- na základe tohto rámca si jeho najbližší downstreem sused zapíše jeho adresu ako UNA (upstream neighbor's address), nastaví A a C bity na 1 aby to už nerobili ďalší a pošle dorotovať rámec. UNA adresa je dôležitá pre fault detection a monitoring funkcie
- tým je inicializačná fáza skončená

standby monitor
- po inicializácii môže už stanica normálne prijímať a vysielať rámce
- ide však ešte do stanby monitor stavu – neustále sleduje správnu funčnosť ringu
- sleduje všetky tokeny a špeciálne active monitor present AMP MAC rámce, ktoré vysiela active monitor
- ak tokeny a AMP MAC rámce nechodia pravidelne, ide do claim token stavu, kde neustále vysiela claim token CT MAC rámce. ak sa príjme takýto CT MAC rámec so svojou SA, tak to išlo od neho, obehlo ring a nikto iný sa nepokúšal stať sa aktívnym monitorom, ide do stavu active monitor. Inak zostáva v stave standby monitor (ak prišiel CT MAC s inou SA, tak ho niekto predbehol – nech:)

active monitor
- akonáhle sa DTE stane active monitor, insertne jeho lattency buffer (nastavený na 27 bitov) do ringu a povolí jeho vlastné hodiny.
- potom pošle purge PRG MAC frame – vyčistí ring
- potom pošle active monitor present AMP MAC frame, a hneď za ním aj token

- prvý downstream sused si zapíše UNA, prepošle rámec s nastavenými A=1, C=1. Následne inicializuje neighbour notification poslaním SMP rámca ďalšiemu, ten ďalšiemu...
- toto spoznávanie je pravidelne inicializované aktívnym monitorom (zasa pošle AMP MAC frame)

Active and Standby Monitors
Every station in a token ring network is either an active monitor (AM) or standby monitor (SM) station. However, there can be only one active monitor on a ring at a time. The active monitor is chosen through an election or monitor contention process.

The monitor contention process is initiated when

i) a loss of signal on the ring is detected,
ii) an active monitor station is not detected by other stations on the ring or
iii) when a particular timer on an end station expires such as the case when a station hasn't seen a token frame in the past 7 seconds.
The station with the highest MAC address will win the election process. Every other station becomes a standby monitor. All stations must be capable of becoming an active monitor station if necessary.

The active monitor performs a number of ring administration functions. The first function is to operate as the master clock for the ring in order to provide synchronization of the signal for stations on the wire. Another function of the AM is to insert a 24-bit delay into all frame transmissions. A third function for the AM is to ensure that a frames on the ring is present or to detect a broken ring. Lastly, the AM is responsible for removing circulating frames from the ring.

Token Ring Insertion Process
Token ring stations must go through a 5-phase ring insertion process before being allowed to participate in the ring network. If any of these phases fail, the token ring station will not insert into the ring and the token ring driver may report an error.

Phase 0 (Lobe Check) - A station first performs a lobe media check. A station is wrapped at the MSAU and is able to send 2000 test frames down its transmit pair which will loop back to its receive pair. The station checks to ensure it can receive these frames without error.

Phase 1 (Physical Insertion) - A station then sends a 5 volt signal to the MSAU to open the relay.
Phase 2 (Address Verification) - A station then transmits MAC frames with its own MAC address in the destination address field of a token ring frame.
When the frame returns and if the address copied and frame recognized bits are set, the station knows there is another station using its MAC address on the ring and will then de-insert.

Phase 3 (Participation in Ring Poll) - Before transmitting any data, the station must participate in the periodic (every 7 seconds) ring poll process. This is where stations identify themselves on the network as part of the MAC management functions.
Phase 4 (Request Initialization) - Finally a station sends out a special request to a parameter server to obtain configuration information. This frame is sent to a special functional address, typically a token ring bridge, which may hold timer and ring number information with which to tell the new station about.

Beaconing

- určené na riešenie vážnych porúch, ako napr. prerušenie kábla
- ak stanica už dlho nedostala AMP MAC frame (vypršal timeout)
- stanica začne vysielať beacon BCN MAC frame až kým ich znova nepríjme, resp. nevyprší timeout
- ak vyprší timeout, notifikuje network management sublayer
- ak je prijatý BCN, a SA je zhodná so stanicou, považuje sa stav za opravený a nastupuje do claim token stavu, ak bola SA iná, ide iba do stanby monitor stavu (zas niekto predbehol)
- ak má sieť iba jeden ring, tak pri poruche sa musí čakať na odstránenie, ak má ešte jeden stanby ring, najlepšie v opačnom smere. V takom prípade TCU – trunk coupling unit (relé) môže vyhodiť vadnú časť ringu do bypass stavu (resp. to inteligentne urobí MSAU – prekonfiguruje sieť)