



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

Počítačové sítě

Jiří Jelínek

Úvod

Záměrem předkládaného textu je poskytnout zájemcům základní materiál pro studium kurzu Počítačové sítě.

Tento kurz vás seznámí se principy, na kterých jsou založeny současné informační a komunikační technologie. Získáte představu, co se odehrává v počítačové síti, při dnes běžných úkonech, jako je přenos souboru, načtení webové stránky. Získáte přehled o zkratkách používaných v souvislosti s počítačovými sítěmi. Získáte celkový náhled na problematiku počítačových sítí, jak se vyvíjely od historie až po současnost.

Tento text je koncipován jako seznámení s jednotlivými oblastmi, neklade si za cíl vytvořit odborníka na projektování a správu počítačových sítí. Po prostudování předkládaného textu budete mít základní znalosti a dovednosti potřebné k vybudování vlastního kurzu informatiky nebo programování, kam problematika počítačových sítí patří.

Obsah

| | | |
|----------|--|------------------------|
| 1 | Vznik počítačových sítí | celkem 4 strany |
| 1.1 | Motivace ke vzniku počítačových sítí | 1/4 |
| 1.2 | Využití počítačových sítí | 2/4 |
| 1.3 | Úrovně integrace počítačů | 3/4 |
| 2 | Architektura počítačových sítí | celkem 13 stran |
| 2 | Architektura počítačových sítí | 1/13 |
| 2.1 | Vrstvy jako základ architektury | 1/13 |
| 2.2 | Princip vrstevového síťového modelu | 2/13 |
| 2.3 | Pojmy související s členěním do vrstev | 2/13 |
| 2.4 | Spojované a nespojované služby | 3/13 |
| 2.5 | Referenční model Open System Interconnection | 5/13 |
| 2.6 | Vrstvy referenčního modelu ISO/OSI | 6/13 |
| 2.7 | Historie referenčního modelu ISO/OSI | 8/13 |
| 2.8 | Vrstvy OSI RM a architektura internetu | 9/13 |
| 2.8.1 | Existující nižší vrstvy | 11/13 |
| 2.8.2 | Vrstva přizpůsobení se médiu | 11/13 |
| 2.8.3 | Síťová vrstva | 11/13 |
| 2.8.4 | Transportní vrstva | 12/13 |
| 2.8.5 | Aplikační vrstva | 12/13 |

3 Topologie a druhy počítačových sítí celkem 15 stran

| | |
|---|-------|
| 3 Topologie a druhy počítačových sítí | 1/15 |
| 3.1 Technické prostředky pro počítačové sítě | 1/15 |
| 3.1.1 Připojené počítače a servery | 1/15 |
| 3.1.2 Spoje (kabely, linky, kanály) | 2/15 |
| 3.1.3 Aktivní prvky (přepojovací prvky) | 2/15 |
| 3.1.4 Pojmy rámec a paket | 3/15 |
| 3.2 Druhy sítí podle jejich rozlehlosti | 3/15 |
| 3.2.1 LAN (Local Area Network) | 3/15 |
| 3.2.2 WAN (Wide area Network) | 4/15 |
| 3.2.3 Rozdíly mezi LAN a WAN | 4/15 |
| 3.2.4 WLAN (Wireless Local Area Network) | 5/15 |
| 3.2.5 VLAN (Virtual Local Area Network) | 6/15 |
| 3.2.6 MAN (Metropolitan Area Network) | 6/15 |
| 3.2.7 PAN (Personal Area Network) | 7/15 |
| 3.3 Topologie počítačových sítí | 7/15 |
| 3.3.1 Hvězdicová topologie | 7/15 |
| 3.3.2 Sběrnicová topologie | 8/15 |
| 3.3.3 Kruhová topologie | 10/15 |
| 3.3.4 Stromová topologie | 12/15 |
| 3.3.5 Topologie obecného grafu | 13/15 |
| 3.3.6 Samostatný počítač (virtuální síť) | 14/15 |
| 3.3.7 Satelitní síť | 14/15 |
| 3.3.8 Bezdrátová síť založená na blízké infrastruktuře | 14/15 |

4 Fyzická vrstva počítačových sítí celkem 20 stran

| | |
|--|-------|
| 4 Fyzická vrstva počítačových sítí | 1/20 |
| 4.1 Kroucená dvojlinka | 1/20 |
| 4.1.1 Historie a fyzika přenosu signálu | 1/20 |
| 4.1.2 Kroucená dvojlinka v počítačových sítích | 3/20 |
| 4.2 Strukturovaná kabeláž | 5/20 |
| 4.2.1 Požadavky na strukturovanou kabeláž | 6/20 |
| 4.2.2 Topologie strukturované kabeláže | 7/20 |
| 4.3 Koaxiální kabel | 9/20 |
| 4.3.1 Vlastnosti koaxiálního kabelu | 9/20 |
| 4.3.2 Konektory pro koaxiální kabel | 11/20 |
| 4.4 Optický kabel | 12/20 |
| 4.4.1 Vlastnosti optického vlákna | 14/20 |
| 4.4.2 Vícevidové vlákno | 14/20 |
| 4.4.3 Jednovidové vlákno | 15/20 |
| 4.4.4 Využití optického vlákna, konektory | 16/20 |
| 4.4.5 Vlnový multiplex (WDM) | 16/20 |
| 4.5 Srovnání optického kabelu, koaxiálu, dvojlinky | 18/20 |

5 Ethernet**celkem 26 stran**

| | | |
|-------|---|-------|
| 5.1 | Vznik Ethernetu | 1/26 |
| 5.2 | Topologie Ethernetu..... | 3/26 |
| 5.2.1 | Sběrníková topologie | 3/26 |
| 5.2.2 | Strukturovaná kabeláž..... | 6/26 |
| 5.2.3 | Sběrníková topologie | 7/26 |
| 5.2.4 | Hvězdicová a stromová topologie..... | 9/26 |
| 5.2.5 | Strukturovaná kabeláž..... | 10/26 |
| 5.2.6 | Topologie obecný graf..... | 10/26 |
| 5.3 | Přístup k médiu | 11/26 |
| 5.3.1 | Přístupová metoda CSMA/CD..... | 11/26 |
| 5.3.2 | Přístup k mediu v dnešním Ethernetu..... | 12/26 |
| 5.3.3 | Formát rámce | 12/26 |
| 5.3.4 | Adresy | 13/26 |
| 5.3.5 | Kolizní okénko..... | 14/26 |
| 5.3.6 | Důsledky CSMA/CD | 15/26 |
| 5.4 | Hub versus switch, routery..... | 16/26 |
| 5.4.1 | Hub (rozbočovač)..... | 16/26 |
| 5.4.2 | Switch (přepínač) | 17/26 |
| 5.4.3 | Bridge (most, media konvertor)..... | 18/26 |
| 5.4.4 | Router (směrovač)..... | 19/26 |
| 5.4.5 | Gateway (brána)..... | 21/26 |
| 5.5 | Přepínaný Ethernet, rychlý Ethernet | 22/26 |
| 5.5.1 | Přístup k mediu v dnešním Ethernetu | 22/26 |
| 5.5.2 | Plně duplexní provoz (full duplex) | 24/26 |
| 5.5.3 | Fast Ethernet | 24/26 |
| 5.5.4 | Gigabitový Ethernet..... | 25/26 |
| 5.5.5 | Desetigigabitový Ethernet..... | 26/26 |

6 Internet celkem 23 stran

| | | |
|--------|---|-------|
| 6.1 | Vznik internetu | 1/23 |
| 6.2 | Historie internetu | 2/23 |
| 6.3 | Standartizace internetu | 4/23 |
| 6.3.1 | Typický navrhovatel RFC - IETF | 4/23 |
| 6.3.2 | Vydané RFC mají přidělen stav | 4/23 |
| 6.3.3 | RFC a standardizační autority (ISO, ANSI) | 5/23 |
| 6.4 | Internet protokol | 6/23 |
| 6.4.1 | RFC 791 a RFC 2460 | 6/23 |
| 6.4.2 | IP adresy | 7/23 |
| 6.4.3 | Přidělování od centrální autority k zákazníkovi | 7/23 |
| 6.4.4 | Prefix | 8/23 |
| 6.4.5 | Podsítě | 8/23 |
| 6.4.6 | Beztrždní adresování a směrování | 9/23 |
| 6.4.7 | Neveřejné adresy | 10/23 |
| 6.4.8 | Překladač neveřejných adres | 10/23 |
| 6.4.9 | IP datagram | 11/23 |
| 6.4.10 | Fragmentace | 12/23 |
| 6.5 | Protokoly pro práci s fyzickou vrstvou | 12/23 |
| 6.5.1 | Address Resolution Protocol (ARP) | 13/23 |
| 6.5.2 | Reverse Address Resolution Protocol (RARP) | 14/23 |
| 6.5.3 | Internet Control Message Protocol (ICMP) | 14/23 |
| 6.5.4 | Internet Group Management Protocol (IGMP) | 15/23 |
| 6.6 | UDP komunikace, User Datagram Protocol | 15/23 |

| | |
|---|-------|
| 6.7 TCP komunikace, Transmission Control Protocol | 17/23 |
| 6.7.1 Zajištění spolehlivosti | 18/23 |
| 6.7.2 Časování potvrzení | 18/23 |
| 6.7.3 Nastavení časovače | 18/23 |
| 6.7.4 Okénko (Sliding window) | 19/23 |
| 6.7.5 TCP datagram, segment, TCP hlavička | 19/23 |
| 6.7.6 Navázání spojení | 20/23 |
| 6.7.7 Ukončení spojení | 21/23 |
| 6.8 Aplikační protokoly | 22/23 |

Literatura**celkem 1 strana**



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

1 Vznik počítačových sítí

1.1 Motivace ke vzniku počítačových sítí

Za prvotní cíl bývá uváděna komunikace mezi lidmi, počátky sahají podobně jako u většiny odvětví do vojenského a akademického, vědeckého prostředí.

Ve čtyřicátých - padesátých letech minulého století se postupně formuje myšlenka rozhraní pro programování počítačů. Původní uspořádání počítač (programovatelnou paměť řízený procesor) s děrnými štítky coby vstup i výstup výpočetní úlohy spěje k současnému modelu, kdy používáme monitor, klávesnici k interaktivní práci, výstupem může být například tiskárna. Myš byla vynalezena Douglasem Engelbartem ve Stanfordském výzkumném institutu až v roce 1963, až cca za 5 let byla samotným vynálezcem představena veřejnosti a až za další dva roky Douglas Engelbart si ji nechal patentovat (1970).

Ve snaze postavit stroj na zpracování informací v objemu umožňující například numerický výpočet, třídění dat nebo vyhledání, postavili vědci velké stroje, velkou spotřebou energie s vysokými pořizovacími i provozními náklady.

Takovéto samostatné stroje měly jen omezené využití. Východiskem bylo vytvořit více terminálů tj. "monitorů s klávesnicemi". Přenos informací mezi terminálem a hlavním strojem byl postupně zobecňován až do modelu, kdy terminál obsahuje jednoduchý počítač zpracovávající informace z klávesnice a generující signál pro monitor.

Informace mezi terminálem a hlavním strojem se přenášely přes komunikační linku (port) obecnějším a obecnějším způsobem (například i přes telefonní síť).

Z této doby pochází i spojení uživatelský účet, protože za možnost pracovat se superpočítačem, zadat mu výpočet se platilo. Počítače byly brzy vybaveny víceuživatelským prostředím a k informacím v nich uložených mohlo přistupovat více lidí a navzájem spolu komunikovat.

Uspořádání superpočítač a terminály ještě nebylo počítačovou sítí, ale už tehdy bylo používáno ke komunikaci mezi lidmi (elektronická pošta s možností zanechat kromě dopisu adresátovi soubor například s výsledkem z pracování).

O počítačové síti můžeme mluvit až v případě propojování tehdejších superstrojů. Propojení čtyřech počítačů bylo realizováno v roce 1969. Cílem bylo odzkoušet navrženou více vrstvou architekturu a techniku datových rámců (balíčků, paketů). Takto realizovaná síť dostala název ARPANET, zkušenosti vyústili až v návrh postupu, na který staví dnešní internet.

1.2 Využití počítačových sítí

1.2.1 Využití velkých počítačů

Původní motivace pro vznik počítačové sítě, do dnes platné (zadávání výpočetních úloh velkým počítačům), z dnešního pohledu se jedná jen o aplikaci současných sítí.

1.2.2 Komunikace

Komunikace mezi uživateli. Dominantní využití současné globální počítačové sítě, dále komunikace mezi programy, distribuované aplikace.

1.2.3 Sdílení prostředků

Sdílení dat, společný diskový prostor. V osmdesátých a devadesátých letech byla rozšířená představa o bezdiskových stanicích, jednoduchých bezdiskových moderních terminálech zpřístupňující data na počítačové síti.

Dostupnost paměťových médií tuto vizi odsunula na neurčito, v současné však narůstá množství dat, které jsou uloženy mimo počítač se kterým v danou dobu pracujeme (mapy, jízdní řády, sociální sítě, google doc atp).

Sdílení technických prostředků, drahé periferie, tiskárny, velké kapacity. Nadčasové (platí dříve i dnes).

1.2.4 Vyšší spolehlivost

Zálohování, záměrná redundance realizovaná přes počítačovou síť.

1.2.5 Úspora nákladů

Rychlá počítačová síť umožňuje efektivně sdílet prostředky, více snadno dostupných počítačů je rychlejší a levnější než jeden super stroj.

Dnes už superstroje jako samostatné výkonné počítače v postatě nestavíme. Vznikají spíše gridy a klastry. Výjimkou je platforma mainframe.

1.3 Úrovně integrace počítačů

1.3.1 Superpočítač

Superpočítač umožňuje komunikaci uživatelů (termiály mohou být geograficky vzdálené). Programy komunikují přímo, například přes funkce operačního systému.

V případě superpočítače se nejedná nutně o počítačovou síť (počítač je jen jeden, terminály mohou být připojeny pomocí portů zcela bez počítačové sítě, jak ji známe dnes).

Od roku 2000 nastává renesance platformy Mainframe (vše na velkém superpočítači), samozřejmě zde je již využívána počítačová síť.

1.3.2 Samostatné počítače

Samostatné počítače jsou používány ojediněle, například naprogramovaný řídicí počítač (obecně spíše jednoduché počítače).

1.3.3 Počítačová síť

Skupina autonomních, navzájem propojených (komunikujících) počítačů. Rozšířené, dnes je však časté, že počítače s výpočetním výkonem vyšším než superpočítače před několika lety se stávají pouhými terminály, např. přes webové rozhraní.

1.3.4 Distribuovaný systém

Skupina počítačů, která se chová jako kompaktní celek (uživatel běžně neví, na kterém stroji byla jeho úloha zpracována).

Používá se pojem klastr, pokud distribuovaný systém realizován na běžných PC s různým výkonem, různou dostupností, různou architekturou, různým operačním systémem a nevyžaduje, aby byly stroje neustále dostupné a spuštěné používá se termín grid.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

2 Architektura počítačových sítí

2.1 Vrstvy jako základ architektury

Vývoj standardizace síťové komunikace začínal v 70. letech, kdy vznikaly první významnější rozlehlé sítě, budované podle vlastních koncepcí předních výrobců počítačů. Brzy vznikla potřeba jednotného standardu, kterým by bylo možno propojit počítačové systémy různých typů a koncepcí, pocházející od různých výrobců.

Zatím co počítače se mohou dynamicky vyvíjet a relativně často, může ve vývoji docházet ke zvratům, některé postupy mohou být zcela přepracovány, nebo zrušeny (například zavedený strop operační paměti v MSDOS a jeho následné zrušení) a nahrazeny zcela odlišnými, oboru počítačových sítí toto možné není.

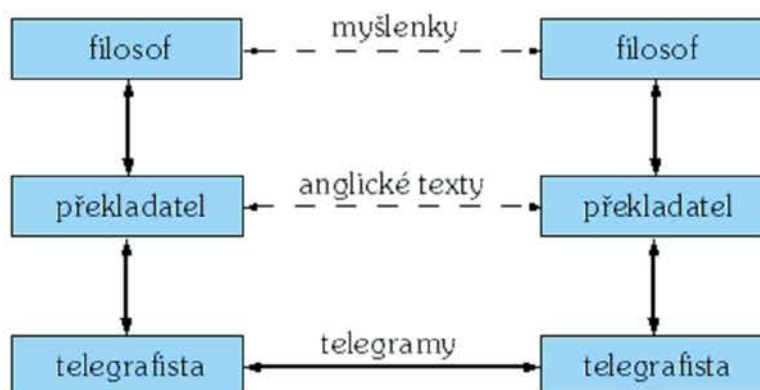
Dříve i dnes se pomocí počítačových sítí propojovaly počítače zcela odlišnými procesory, operačními systémy a především koncepcemi vyvíjeny odlišnými společnostmi. Pokud v oboru počítačových sítí nějaký postup zavedeme je jasné, že bude používán dlouhou dobu, protože už nebude záležitostí jednoho výrobce, ale bude spojovat starší současné i budoucí technologie.

Příkladem může být například analogový telefon, který přes překotný vývoj elektroniky, úplné změny telefonních ústředen nedoznal zásadních změn, byl změněn způsob vytáčení, u lepších přístrojů přibyla identifikace volajícího. Napěťové úrovně signálů, použita kroucená dvojlinka, napájecí napětí zůstalo v podstatě beze změn.

V případě počítačových sítí bychom mohli říci, že síťová a transportní vrstva se v podstatě 30 let neměnila a nyní se blíží doba, kdy ke změnám dojde. Naopak fyzická vrstva a spojová vrstva se v určitých mezích několikrát zásadním způsobem modifikovala.

2.2 Princip vrstevného síťového modelu

Komunikace probíhá domluveným protokolem na úrovni dané vrstvy. Na vývoj dané vrstvy se může soustředit samostatný tým inženýrů, a může ji vymezeným způsobem měnit. Například na našem obrázku může být modifikována (modernizována) funkce telegrafisty, lze například vyměnit překladatele. Celá architektura si po těchto změnách zachovala svou strukturu.



Obrázek 2.1 – Komunikace ve třívrstevném uspořádání

2.3 Pojmy související s členěním do vrstev

2.3.1 Protokol

Protokolem se domlouvají dva počítače na téže vrstvě (hlavičky, dotazy, odpovědi, atp.). Zprávy jsou předávány podřízené vrstvě. Protokol je nezávislý na implementaci, umožňuje vzájemnou spolupráci (Interoperabilitu).

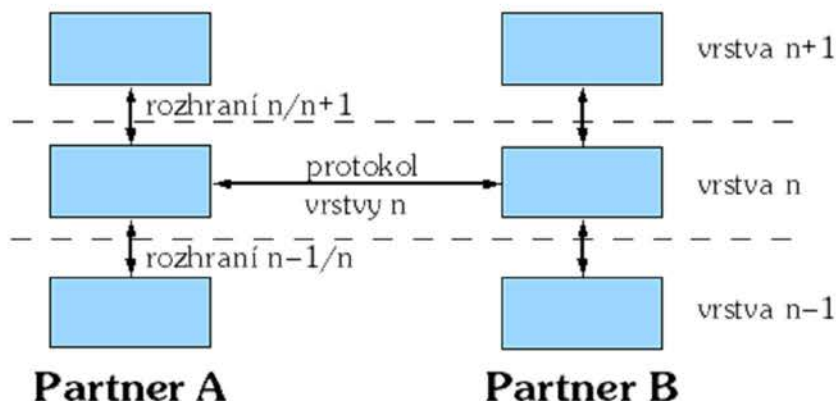
2.3.2 Rozhraní

Rozhraní je definice služeb nabízených nadřízené vrstvě. Implementaci určuje zdejší protokol, nadřízená vrstva o ní nic neví. Rozhraní závisí na implementaci (např. OS).

2.3.3 Hlavičky

Každý dotaz předaný nižší vrstvě je považován za data která jsou opatřena hlavičkou, dochází tedy přidávání a odebírání hlaviček.

Typickým příkladem z praxe může být zapouzdření IP rámce do paketu Ethernetu (komunikace a rozhraní transportní vrstvy směrem níže).



Obrázek 2.2 – Rozhraní a protokol ve vrstvách počítačové sítě

2.4 Spojované a nespojované služby

2.4.1 Spojované služby

Spojovaná služba (Connection-oriented Service) pracuje na obdobném principu, jako telefonní systém. Chcete-li s někým hovořit po telefonu, musíte nejprve vytočit jeho číslo, a on musí na vaše volání odpovědět zvednutím telefonu. Tím mezi vámi vzniká spojení, prostřednictvím kterého spolu komunikujete, a které na konci hovoru zaniká (položením sluchátka).

Analogicky je tomu i v případě dvou entit na stejných úrovních, které spolu chtějí komunikovat - nejprve musí být mezi nimi navázáno spojení. Jakmile je toto spojení navázáno, chová se v jistém smyslu jako roura - vysílající do ní na jedné straně vkládá to, co si přeje odeslat, a příjemce si to na druhé straně ve stejném pořadí odebírá.

Spojované služby

- Naváže spojení a jím pak protékají data (právě jako telefon).
- Dodržuje pořadí rámců.
- Menší nároky (na aplikační vrstvu).

2.4.2 Nespojované služby

Nespojovanou službu (Connectionless Service) lze naopak přirovnat k běžné listovní poště. Ta nepočítá se zřízením spojení mezi odesilatelem a příjemcem, ale místo toho považuje jednotlivé části přenášených dat (zprávy) za samostatné celky, opatřené adresou svého konečného příjemce, a doručuje je nezávisle na ostatních zprávách. Jednotlivé zprávy tedy mohou být v principu přenášeny různými cestami, takže se může i stát, že při příjmu nebude zachováno jejich správné pořadí - což se u spojované služby stát nemůže.

Nespojované služby

- Každý paket přepravován samostatně (jako samostatné dopisy).
- Pružnější a robustnější, reaguje na změny v síti.
- Univerzálnější a lépe odpovídá charakteru sítí.

2.4.3 Teorie a praxe

V lokálních sítích mají přenosy obvykle nespojovaný (connectionless) charakter. Původní verze referenčního modelu ISO/OSI (viz. dále) však počítala pouze se spojovanými (connection-oriented) službami a protokoly, a zavedení nespojovaných protokolů bylo provedeno až dodatečně.

2.4.4 Spolehlivost nabízené služby

Spolehlivá služba (Reliable Service) je taková, která nikdy neztrácí žádná data.

Obvykle je tato služba realizována prostřednictvím vhodného mechanismu potvrzování (kdy příjemce potvrzuje úspěšné přijetí resp. znovu žádá o vyslání dat, které byly přijaty chybně). S tím je ovšem spojena určitá režie, která nemusí být vždy žádoucí - představme si např. přenos digitalizovaného zvuku.

Zde je jistě výhodnější raději občas přijmout chybná data (tj. poněkud zkreslený zvuk), než připustit výpadky, způsobované potvrzováním resp. opakovaným přenosem chybně přijatých dat.

Proto mají své opodstatnění i nespolehlivé služby (Unreliable Services), což je ovšem poněkud zavádějící označení - je vhodné chápat je spíše jako služby, které mají vysokou míru spolehlivosti, neposkytují však stoprocentní záruku úspěšnosti přenosu.

2.5 Referenční model Open System Interconnection

Model ISO/OSI je referenční komunikační model označený zkratkou slovního spojení "International Standards Organization / Open System Interconnection" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů).

Jedná se o doporučený model definovaný organizací ISO v roce 1983, který rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev. Zmíněné vrstvy jsou též známe pod označením Sada vrstev protokolu.

Úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě a nezatěžovat vyšší vrstvu detaily o tom jak je služba ve skutečnosti realizována. Než se data přesunou z jedné vrstvy do druhé, rozdělí se do paketů.

V každé vrstvě se pak k paketu přidávají další doplňkové informace (formátování, adresa), které jsou nezbytné pro úspěšný přenos po síti.

Tabulka 2.1 – Referenčního modelu ISO/OSI

| | Datové jednotky | Vrstva | Funkce |
|--------------|-----------------|----------------|---|
| Host layers | Data | 7. Aplikační | Síťové procesy a aplikace |
| | | 6. Prezentační | Šifrování a reprezentace dat |
| | | 5. Relační | Interhost komunikace |
| | Segment | 4. Transportní | End-to-end spojení a spolehlivost (TCP) |
| Media layers | Paket/datagram | 3. Síťová | Směrování a logické adresování (IP) |
| | Frame | 2. spojová | Fyzické adresování (MAC & LLC) |
| | bit | 1. Fyzická | Media, signál, binární transmise |

2.6 Vrstvy referenčního modelu ISO/OSI

2.6.1 Fyzická vrstva (physical layer)

Definuje prostředky pro komunikaci s přenosovým médiem a s technickými prostředky rozhraní. Dále definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení. Je hardwarová.

2.6.2 Linková vrstva (data link layer)

Zajišťuje integritu toku dat z jednoho uzlu sítě na druhý. V rámci této činnosti je prováděna synchronizace bloků dat a řízení jejich toku. Je hardwarová.

2.6.3 Síťová vrstva (network layer)

Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos informací do požadovaného cílového uzlu. V lokální síti vůbec nemusí být pokud se nepoužívá směrování. Je hardwarová ale když směrování řeší PC s dvěma síťovými kartami je softwarová.

2.6.4 Transportní vrstva (transport layer)

Definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu (provádí některé chybové kontroly). Řeší například rozdělení souboru na pakety a potvrzování. Je softwarová.

2.6.5 Relační vrstva (session layer)

Koordinuje komunikace a udržuje relaci tak dlouho, dokud je potřebná. Dále zajišťuje zabezpečovací, přihlašovací a správní funkce. Je softwarová.

2.6.6 Prezentační vrstva (presentation layer)

Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Je softwarová.

2.6.7 Aplikační vrstva (application layer)

Je to v modelu vrstva nejvyšší. Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků. Je softwarová.

2.7 Historie referenčního modelu ISO/OSI

První počítačové sítě v dnešním slova smyslu - pro rutinní provozování na komerčním principu, a nikoli pro experimentální účely - se začínají budovat někdy v polovině 70. let, kdy se také na trhu objevují první produkty určené pro tyto sítě. Problém byl ale v tom, že příslušné produkty byly ryze proprietární (tj. specifické pro konkrétního výrobce) a neumožňovaly vzájemnou interoperabilitu.

Jednalo se o řešení, uvedená na trh velkými firmami (tehdy hlavně IBM a DEC) a koncipovaná podle partikulárních zájmů, představ i tradic příslušných firem (například firma IBM koncipovala svou síťovou architekturu SNA spíše jako způsob budování rozsáhlých terminálových sítí ke svým střediskovým počítačům). To, co velmi brzy začalo chybět, byla taková síťová architektura, která by byla dostatečně otevřená, tedy nezávislá na konkrétním výrobcu, široce dostupná ve svých specifikacích, umožňující požadovanou kompatibilitu a vzájemnou interoperabilitu řešení od různých výrobců a otevírající prostor konkurenci (a naopak nevytvářející závislost zákazníka na jediném "dvorním" dodavateli).

Úkolu vypracovat takovouto nezávislou architekturu se nakonec dobrovolně ujala mezinárodní standardizační organizace ISO (International Standards Organization, správně: International Organization for Standardization), sdružující národní standardizační organizace většiny vyspělých zemí světa. Zpočátku byl její záměr takový, že vypracuje jednotný standard pro fungování otevřených systémů - tedy vlastně pro fungování všech počítačů jako takových, aniž by se nutně muselo jednat o uzly zapojené do nějaké sítě. Mělo se to jmenovat "Open Systems Architecture" (doslova: architektura otevřených systémů), ale samozřejmě se brzy ukázalo, že něco takového je nad tehdejší možnosti (a určitě i dnešní, nehledě již na účelnost). Proto lidé z organizace ISO poněkud slevili, zejména v tom ohledu, že se nebudou zabývat fungováním počítačů jako takových, ale pouze tím, co se týká jejich vzájemné komunikace.

Z honosného projektu "Open Systems Architecture" se tak stalo realističtější "Open Systems Interconnection Architecture" (doslova: architektura vzájemného propojování sítí).

Nakonec však bylo nutné něco slevit i z této omezené představy, důvodem totiž byl zejména styl práce lidí z organizace ISO, kteří nepovažovali za možné přejímat jinde vyvinutá a jinde standardizovaná řešení, ale připouštěli pouze to, co sami schválí a vydají jako vlastní standard (takže vlastně nedůvěřovali v kompetentnost kohokoli jiného). Díky tomu, i díky dalším faktorům, se postup prací natolik zpomalil, že se záhy ukázalo jako nezbytné opět něco slevit: nevydávat vše jako skutečnou síťovou architekturu, tedy včetně všech protokolů, ale pouze jako určitý prázdný rámec - jako představu o tom, kolik má být hierarchických vrstev a co mají dělat, ale bez konkrétních protokolů, které by do těchto vrstev "zapadaly" (s tím, že tyto protokoly budou dopracovávány postupně podle toho, jak budou pokračovat práce na jejich vývoji).

Konkrétním výsledkem pak musela být i další změna názvu. Z přechodného "Open Systems Interconnection Architecture" se posléze stal "Reference Model for Open Systems Interconnection" (doslova "referenční model pro propojování otevřených systémů").

Přitom slovní spojení "referenční model" je zde použito právě pro zdůraznění toho, že jde o obecnou koncepci, vzor, rámec resp. model (a nikoli o konkrétní a striktně definovaný předpis), který bude teprve postupem času naplňován konkrétními návody (protokoly) podle toho, jak tyto budou dostupné.

2.8 Vrstvy OSI RM a architektura internetu

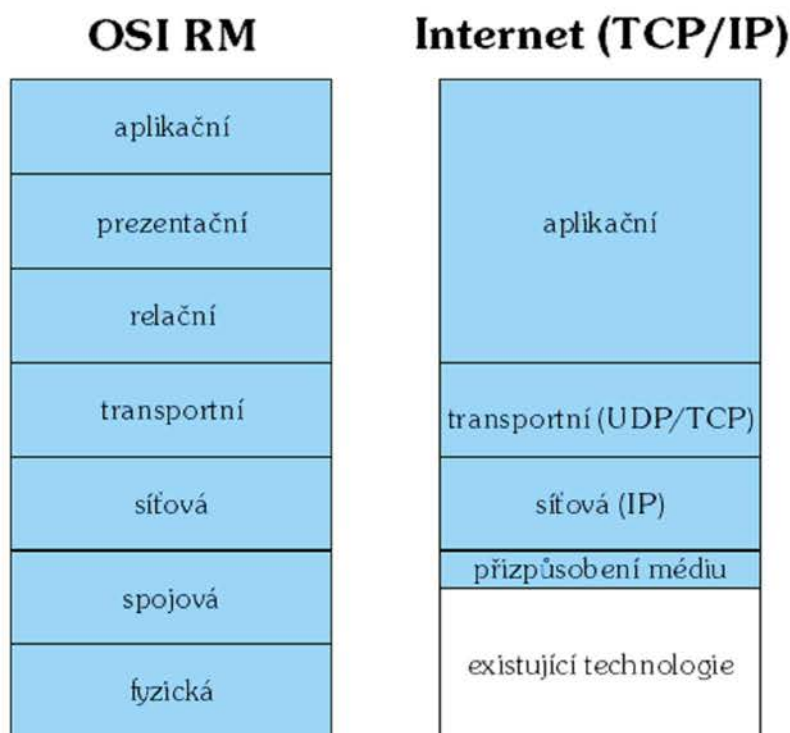
Uspořádání internetu tak jak jej známe (IPv4, viz. samostatná kapitola Internet) se datuje k roku 1974 až 1979, se standardizací v lednu 1980.

Doporučení OSI je užito jen z části, však velmi vhodným způsobem (IP byl navrhován dříve než OSI RM). Nižší vrstvy nejsou standardizovány,

od začátku se předpokládá vazba na existující technologie, kterým je ponechán volný prostor pro dynamický vývoj. Podobně je to nestandardizováním prezentační a aplikační vrstvy (relační vrstva se přidružuje k transportní a aplikační).

Při tvorbě modelu TCP/IP bylo základním požadavkem to, aby prostřednictvím protokolů TCP/IP bylo možné vzájemně propojit i takové sítě, které mohly být vybudovány i na dosti odlišných principech a přenosových technologiích (tedy například sítě Ethernet, Token Ring, později FDDI, ATM, sítě s dvoubodovými spoji atd.).

Už od počátku se tedy nejednalo komplexní síťovou technologii, ale o most mezi existujícími technologiemi, právě proto internet, jak jej známe v konkurenčním prostředí ostatních návrhů uspěl.



Obrázek 2.3 – OSI RM a architektura internetu

2.8.1 Existující nižší vrstvy (existující technologie)

Hlavní myšlenka: nemá smysl vynalézat kolo. Vývojáři internetového protokolu vůbec nižší vrstvy nestandardizovali a tento přístup významně přispěl ke skutečnosti, že již v roce 1983, kdy bylo pomocí IP propojeno cca 1000 počítačů, vzniká pojem internet.

Začíná být zřejmé, že vyšší vrstvy budou nadčasové a nižší (fyzické, spojové vrstvy) se budou moci vyvíjet a budou proměnné v čase (stejně jako hardware a operační systémy počítačů).

2.8.2 Vrstva přizpůsobení se médiu

Někdy zvaná též „Vrstva síťového rozhraní“. Vrstva vždy řeší pouze problematiku, jak přenášet IP po dané technologii nižší vrstvy.

Úkolem je zakrýt případná specifika konkrétních síťových technologií a vytvořit nad nimi jednotné prostředí nabízející jednotné služby, jednotný způsob adresování apod.

Na rozdíl od vyšších vrstev není naplněna v rámci TCP/IP žádnými protokoly, naopak se snaží přizpůsobit existujícím řešením (např. Ethernet).

Pro novou technologii stačí definovat, jak po ní přepravovat IP a lze novou technologii hned používat, pro vyšší vrstvy pak není podstatné zda fyzickou vrstvou je například Ethernet nebo datové rámce musely překonat například trasu přes ADSL, WiFi atp.

2.8.3 Síťová vrstva

Podobně jako v ISO/OSI modelu zajišťuje směrování, zajišťuje však nespojovaný přenos pomocí jednoduché datagramové služby, nezabývá se spolehlivostí přenosu. Měla by se soustředit především na co možná nejrychlejší přenos dat.

Na této vrstvě pracuje Internet Protocol (IP). Ten je nespojovaný a bez záruk, tzn. že se sice snaží o bezchybný přenos, ale když se mu to nepodaří a někde se něco ztratí či poškodí, nepovažuje za svou povinnost postarat se o nápravu (a místo toho očekává, že o případnou nápravu se postarají vyšší vrstvy).

Jeho nespojovaný charakter je dán tím, že při přenosu dat nepočítá s přímým navázáním spojení mezi odesílatelem a příjemcem, a místo toho posílá všechna data „do neznáma“.

Vrstva jako Internet Protokol drží pohromadě celý internet a zajišťuje schopnost různých systémů vzájemně spolupracovat, poskytovat si služby, dosáhnout vzájemné součinnosti (tzv. Interoperabilita).

2.8.4 Transportní vrstva

Zajišťuje komunikaci mezi koncovými účastníky tj. přes rozhraní operačního systému přímo aplikační programy.

Podle jejich požadavků a nároků může vrstva regulovat tok dat oběma směry. Na této vrstvě pracují dva protokoly - TCP a UDP.

Protokol TCP (Transmission Control Protocol) poskytuje spojované a spolehlivé služby a tím mění charakter služeb síťové vrstvy.

protokol UDP (User Datagram Protocol) poskytuje nespojované služby bez záruk (zachovává charakter služeb síťové vrstvy).

2.8.5 Aplikační vrstva

Architektura internetu je ve srovnání s referenčním modelem ISO/OSI velmi strohá. Jedná se o protokoly konkrétních aplikací.

Autoři TCP/IP dospěli k závěru, že požadavky na podpůrné služby (například služby zajišťující konverze přenášených dat, korektní průběh relací apod.) budou méně časté, a že naopak budou časté aplikace, které tyto služby využívat nebudou.

Relační a prezentační vrstva implementována není (zmíněné podpůrné funkce musí zvládnout přímo aplikace). Podobně jako v případě nejnižších vrstev se jednalo o prozíravé rozhodnutí pro návrhu TCP/IP.

Původními službami aplikační vrstvy jsou elektronická pošta (SMTP, POP, IMAP), přenos souborů (FTP) a vzdálené přihlašování (TELNET), dodatečně vzniká DNS a DHCP, až z velkým časovým odstupem vznikají další (WWW až za deset let!, v roce 1991).

Aplikace mohou realizovat uspořádání dvoubodové komunikace nebo i složitější peer-to-peer (komunikace rovný s rovným, myšleno mezi více počítači nebo aplikacemi) a Klient-server (server nebo více severu řídí ostatní klienty sítě).

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

3 Topologie a druhy počítačových sítí

3.1 Technické prostředky pro počítačové sítě

3.1.1 Připojené počítače a servery

Do této skupiny počítejme i periferie, datová úložiště, měřicí přístroje, zabezpečovací zařízení VoIP telefony vybavené síťovým adaptérem (též zván síťová karta nebo NIC - Network Interface Controller).



Obrázek 3.1 – Hardware typicky tvořící počítačovou síť

3.1.2 Spoje (kabely, linky, kanály)

Tuto skupinu tvoří metalické vodiče (kroucená dvojlinka, koaxiální kabel), optické kabely, rádiové bezdrátové spoje, bezdrátové optické spoje (většinou laserové, infračervené). Této oblasti se budeme věnovat v samostatné kapitole - Fyzická vrstva počítačových sítí.

3.1.3 Aktivní prvky (přepojovací prvky)

Rozbočovač (hub, koncentrátor) - pouze zesiluje signál a umožní vytvořit například realizovat sběrnici (sběrníkovou topologii) přesto, že spoje jsou dvoubodové a fyzicky zapojené do hvězdy. Ze všech aktivních prvků má téměř nulové zpoždění. Spojuje několik segmentů sítě do jednoho, provoz v jedné části sítě se přenesení i do ostatních částí a narozdíl od přepínače tedy zaměstnává celou síť. Do této skupiny patří i síťový most (bridge) - spojuje dva fyzicky oddělené segmenty sítě, může měnit rozhraní (mediakonvertor), například Ethernet - WiFi, Ethernet - DSL. Rozbočovač nebo-li hub je běžně používán v průmyslovém ethernetu.

Přepínač (switch) - spojuje alespoň dvě zařízení v rámci jednoho segmentu sítě nebo v rámci více segmentů, odděluje síťový provoz, adresným způsobem doručuje rámce, čímž narozdíl od rozbočovače nezatěžuje ostatní části sítě. Oproti rozbočovači znemožňuje snadný monitoring sítě (přepínače vyšší třídy umožňují monitoring a diagnostiku pomocí speciálního portu).

Směrovač (též zván router) - přesměrovává komunikaci do jiného segmentu sítě stejného typu, například může přenášet data mezi dvěma fyzicky samostatnými ethernetovými sítěmi přes TCP/IP úroveň komunikace (v obou sítích vystupuje jako počítač - v každé s jinou IP adresou a jinou adresou fyzické vrstvy). Může snadno realizovat bezpečnostní zábranu (firewall).

Opakovač (též zváný repeater) - opravuje a zesiluje poškozený signál správně načasovaný ho vysílá dál.

Modem (modulátor a demodulátor), transceiver (vysílač a přijímač) je technicky složitější verze mediakonvertoru, rozbočovače, typicky pro překonání obtížnější trasy (telefonní linka), dlouhý dvoubodový spoj.

3.1.4 Pojmy rámec a paket

Rámec je blok dat s hlavičkou na úrovni linkové vrstvy, skládá se ze záhlaví, zápatí a samotných přenášených dat. Záhlaví obsahuje MAC adresu odesílatele i příjemce dat.

Paket je blok dat s hlavičkou na úrovni síťové, případně vyšší vrstvy. Součástí paketu jsou síťové adresy (typicky IP adresy) obou koncových účastníků a informace potřebné pro potvrzování a případně i řízení toku.

3.2 Druhy sítí podle jejich rozlehlosti

3.2.1 LAN (Local Area Network)

Lokální počítačová síť se vyznačuje tím, že počítače jsou propojeny na menším geografickém území (tedy v rámci firmy, budovy, místnosti, atp.).

V rámci LAN se nejvíce používá přepínaný ethernet (kroucená dvojlinka, optické vlákno) doplněný WiFi (IEEE802.11).

- Již od svého vzniku vysoké rychlosti (10Mb/s až 10Gb/s).
- Primárně určená pro sdílení prostředků.
- Nízká chybovost.

3.2.2 WAN (Wide area Network)

Komunikační síť, která pokrývá rozsáhlé území, jako je spojení zemí, kontinentu.

Internet jen nejrozsáhlejší a nejznámější veřejná WAN. Fyzickou vrstvou je pronajatá kabeláž (optické vlákno, mikrovlnné spoje, satelity), nejvíce je dnes používána technologie Frame relay.

- Velké rozpětí rychlostí (64kb/s až 10Gb/s).
- Chybovost je závislá na technologii.

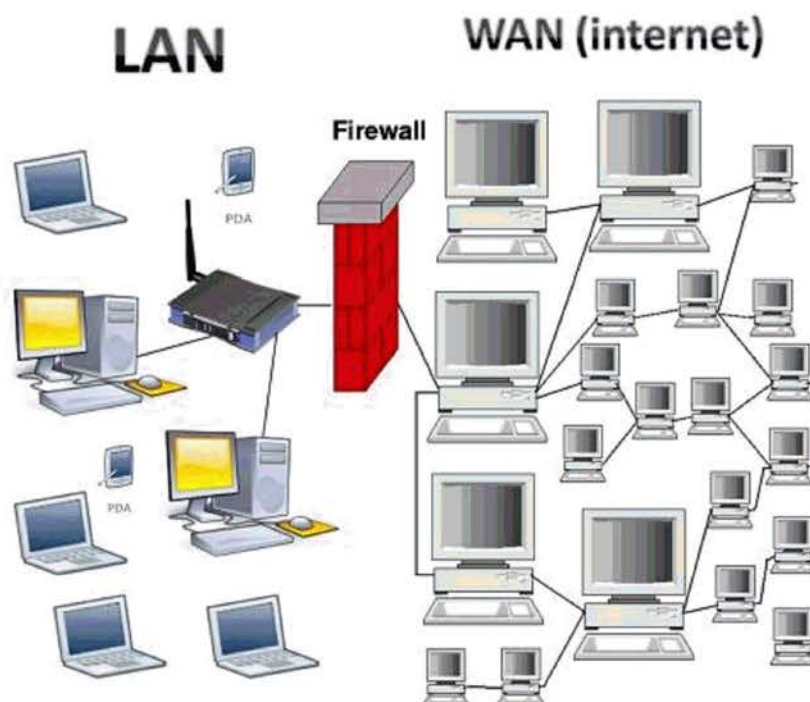
3.2.3 Rozdíly mezi LAN a WAN

V různých literárních pramenech bývají srovnávané sítě LAN a WAN, ohledně rychlosti, rozlehlosti, spolehlivosti atp. Nalézt lze různé další zkratky - PAN, MAN atp. (viz. další text).

Přínos a význam takového členění sítí je sporný (nelze například již tvrdit, že lokální sítě jsou rychlejší, když rychlosti páteřních spojů jsou pravidla ještě vyšší).

Označení LAN a WAN je dnes často užíváno u routerů integrujících bezpečnostní ochranu (firewall) lokální sítě (viz. obrázek 3.2).

Obecně můžeme říci, že jednotlivé LAN sítě se propojují přes WAN síť, aby byla zajištěna komunikace na velké vzdálenosti se servery umístěnými právě ve WAN (internet).



Obrázek 3.2 – Typické uspořádání LAN připojené k internetu

3.2.4 WLAN (Wireless Local Area Network)

Bezdrátová lokální síť je obdobou běžné LAN, ale jednotlivé prvky nejsou fyzicky propojeny drátem (kroucená dvojlinka, optické vlákno), ale jsou propojeny bezdrátově.

Nevýhodou je například to, že se špatně omezuje šíření signálu, a případný útočník nemusí získat přímo fyzický přístup k zásuvce (nebo například do budovy škol firmy), jako v případě drátových sítí.

Většina víceúčelových zařízení (např. router/firewal - Ethernet, Wi-Fi, ADSL, 3G) touto zkratkou označuje právě konfiguraci bezdrátové části sítě. Je možné například nastavit jinou úroveň zabezpečení pro bezdrátovou část sítě.

3.2.5 VLAN (Virtual Local Area Network)

Nejen v prostředí školy může být zajímavé provozovat například dvě do určité míry samostatné sítě LAN (na kroucené dvojlince) a celý systém doplnit například Wi-Fi. Toto uspořádání umožní nastavit odlišná bezpečnostní pravidla (učebny x kanceláře).

Klasický ethernet by vyžadoval dvojí kabeláž mezi budovami a omezenou flexibilitu v konfiguraci. Vyspělejší síťové prvky umožňující na jedné infrastruktuře realizovat více (virtuálních) lokálních sítí, pouhou (vzdálenou konfigurací lze daný počítač přepojit do jiné lokální sítě - jiné adresy a jiné možnosti).

Každý ethernetový rámec je doplněn informací, ke které lokální síť přísluší, a v koncovém síťovém prvku je tato informace zbaven a poslán příslušné síťové kartě počítače. Virtuální LAN je obdobou klasické lokální sítě s tím, že LAN závisí na fyzickém uspořádání a propojení, kdežto VLAN vzniká logicky uvnitř fyzické LAN.

3.2.6 MAN (Metropolitan Area Network)

Sít, která spojuje jednotlivé LAN, ale nepřekračuje hranice města či metropolitní oblasti. Často používá bezdrátové spojení nebo optická vlákna.

MAN může být vlastněna jednou organizací, ale většinou se jedná o propojení několika nezávislých objektu. Můžeme mít například několik poboček firmy v jednom městě. Dříve se využívalo technologií jako ATM a FDDI, ale dnes dominuje opět ethernet (označovaný jako metro-ethernet).

Nasadit lze například techniku VLAN a vytvářet na společné infrastruktuře lokální sítě jednotlivých celků města (dopravní podnik, magistrát, městská policie).

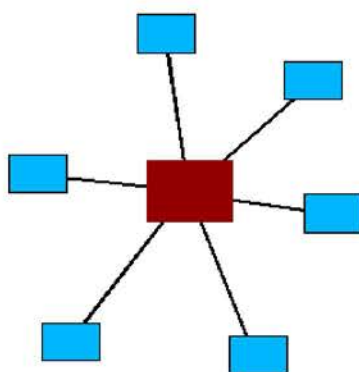
3.2.7 PAN (Personal Area Network)

Osobní síť, je to velice malá počítačová síť používaná pro propojení jeho osobních elektronických zařízení typu mobilní telefon, PDA, notebook atd., rozlehlost je ze sítě nejmenší (10metrů), příkladem je Bluetooth v kanceláři, v automobilu nebo síť například měřicích systémů (Bluetooth 100metrů).

3.3 Topologie počítačových sítí

3.3.1 Hvězdicová topologie

- Jedná se o nejpoužívanější způsob propojování počítačů do počítačové sítě. Počítače jsou propojeny pomocí kabelových segmentů (UTP, STP) k centrálnímu prvku - přepínači.
- Mezi každými dvěma stanicemi existuje vždy jen jedna cesta. Toto zapojení pochází z počátků používání výpočetní techniky, kdy byly počítače připojeny k centrálnímu počítači (mainframe).
- Přechodně byla vytlačována v lokálních sítích (1980-1994) sběrníkovým uspořádáním - ethernet na koaxiálním kabelu.
- V současnosti tato topologie dominuje v LAN díky Ethernetu na kroucené dvojlince.



Obrázek 3.3 – Grafické znázornění hvězdicové topologie

Výhody

- Pokud selže jeden počítač nebo kabel nebude fungovat spojení pouze pro jednu stanici a ostatní stanice mohou vysílat i přijímat nadále.
- Umožňuje paralelní provoz - vyšší výkonnost v porovnání se sběrníkovou topologií při stejné nominální přenosové rychlosti. To souvisí s tím, že na jednom kabelu je připojen pouze jeden počítač a tudíž jednak nedochází ke kolizím mezi pakety a také může současně přenášet data více počítačů.
- Umožňuje oddělený provoz - centrální prvek může vnést zabezpečení
- Snadno se nastavuje a rozšiřuje
- Závady se dají snadno nalézt

Nevýhody

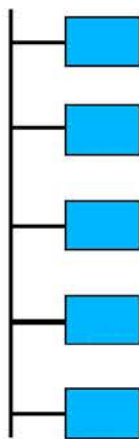
- vyžadováno velké množství kabelů - ke každému počítači jeden.
- Potřeba extra hardware v porovnání se sběrníkovou topologií (ten však může být laciný).
- V případě selhání centrálního síťového prvku přestane fungovat celá síť. Proto je dobré chránit ho před výpadkem el. proudu záložním zdrojem energie (UPS).

3.3.2 Sběrníková topologie

Spojení zprostředkovává jediné přenosové médium (sběrnice), ke kterému jsou připojeny všechny uzly sítě (koncové počítače). Fyzicky se může jednat o koaxiální kabel nebo pozemní rádiový bezdrátový spoj.

Sběrnice je jednoduché zapojení, má nízké pořizovací náklady, avšak také své nevýhody. Problém nastává, jakmile chtějí dva klienti na síti vysílat ve stejný okamžik - vzniká kolize.

zhledem k tomu, že se tato situace děje poměrně často, musí mít systémy, které používají ke vzájemné komunikaci sběrnicovou topologii implementované schéma pro vyvarování se takových kolizí. V počítačových sítích se používá tzv. systém náhodného přístupu (CSMA), který se kolizím snaží předcházet a v případě že nastanou - řeší je.



Obrázek 3.4 – Grafické znázornění sběrnicové topologie

Výhody

- Snadná realizace a snadné rozšíření již stávající sítě.
- Nevyžaduje tolik kabeláže jako např. hvězdicová topologie.
- Vhodná pro malé nebo dočasné sítě, které nevyžadují velké rychlosti přenosu.

Nevýhody

- Nesnadné odstraňování závad.
- Omezená délka kabelu a také počtu stanic.
- Pokud nastane nějaký problém s kabelem, celá síť přestane fungovat.
- Výkon celé sítě rapidně klesá při větších počtech stanic nebo při velkém provozu.

3.3.3 Kruhová topologie

Při zapojení počítačů v kruhu stačí triviální protokoly k řízení sítě - jednoduché následnictví.

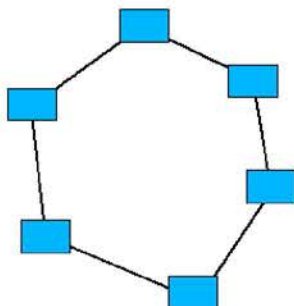
Obvyklým způsobem řešení komunikace je implementace tokenu (oprávnění promluvit), který si stanice v kruhu postupně předávají a který jeho držitel umožňuje vysílat, přičemž ostatní stanice pouze naslouchají.

Zpráva tak prochází přes všechny mezilehlé počítače v kruhu, přičemž její zpoždění na každém uzlu je jen jeden bit (tj. v zápětí po načtení příchozího signálu je signál vyslán dále).

Přerušením kruhu dojde k narušení komunikace, proto některé technologie pracují se záložním kruhem (například FDDI).

Realizaci nelze na první pohled odlišit od hvězdy, protože zpravidla bývá používán centrální prvek, koncentrátor, který kruh realizuje pomocí dvoubodových spojů na kroucené dvojlince.

Kruhová topologie je tedy logickým uspořádáním fyzicky je uspořádání hvězdicové.



Obrázek 3.5 – Grafické znázornění sběrníkové topologie

Výhody

- Přenos dat je relativně jednoduchý, protože pakety se posílají jedním směrem.
- Přidání dalšího uzlu má jen malý dopad na šířku pásma.
- Nevznikají kolize.
- Minimální zpoždění (v bitech podle počtu uzlů).
- Průchodnost sítě je z výše uvedených důvodů ze všech ostatních topologií nejvyšší při zátěži.
- Snadná možnost implementace záruk na množství přenesených dat za jednotku času.
- Možství kabelů může být menší, než u hvězdicové topologie.

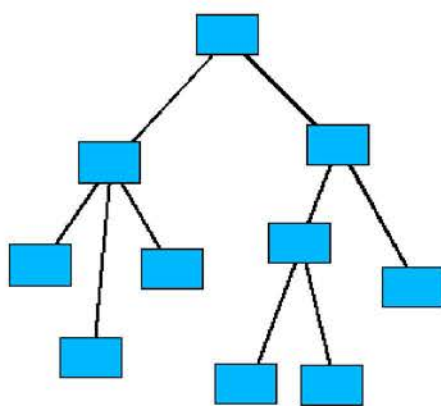
Nevýhody

- Data musí projít přes všechny členy kruhu, což zvyšuje riziko poruchy.
- Přerušením kruhu vzniká problém.
- Při přidání nového uzlu je nutné dočasně kruh přerušit (u Token ringu jen na zanedbatelný okamžik).
- Vstup a výstup (zapnutí a vypnutí) stanice je logicky a implementačně komplikovaná operace.

3.3.4 Stromová topologie

Vychází z hvězdicové topologie spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd.

Takovéto propojení se používá především v rozsáhlých počítačových sítích ve velkých firmách. Jednotlivé hvězdice často představují jednotlivá oddělení firmy, patra budovy nebo celé budovy. Tyto hvězdice jsou pak též spojeny hvězdicovitým způsobem.



Obrázek 3.6 – Grafické znázornění stromové topologie

Výhody

- Pokud selže jeden aktivní síťový prvek, ostatní části sítě mohou dále pokračovat.
- Snižuje se potřebné množství kabelů.
- Zvýšení bezpečnosti - zvyšuje se obtížnost odposlouchávání síťové komunikace.
- Lze oddělovat provoz, vytvářet virtuální lokální sítě vhodnou konfigurací aktivních prvků.

Nevýhody

- Reálný výkon závisí na uspořádání
- Existují zranitelná místa, při jejichž výpadku je celá síť ochromena

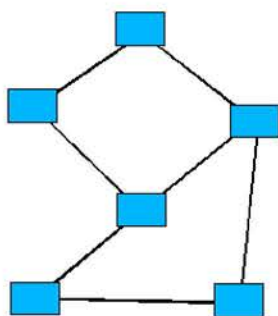
3.3.5 Topologie obecného grafu

Někdy nazývaná smyčková, pletivová, Mesh topologie.

Obsahuje redundantní spoje (WAN sítě, internet, ...).

Každé zařízení je propojené s každým (full mesh), běžná je alternativa, kdy se některé spoje vynechají (částečný mesh).

Směrování v ČR.



Obrázek 3.7 – Grafické znázornění topologie obecného grafu

Výhody

- Velká spolehlivost. Když některý spoj vypadne data si k cíli najdou jinou cestu.

Nevýhody

- Větší počet aktivních prvků.
- Velké nároky na aktivní prvky (musí hledat optimální nastavení pro směrování).

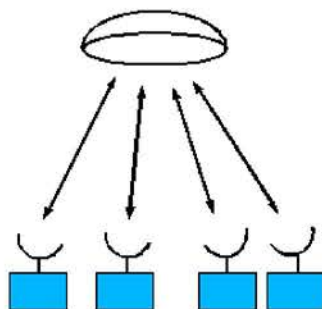
3.3.6 Samostatný počítač (virtuální síť)

Není zřejmé, která z výše uvedených topologií situaci lépe vystihuje, pokud se jedná víceprocesorový počítač s kvalitním OS, pak aplikační vrstva dosahuje full mesh.

3.3.7 Satelitní síť

Uspořádání je shodné s hvězdou, účastníci se „neslyší“ přímo. Nepotřebuje kabely ani jinou infrastrukturu ve své blízkosti.

Velké zpoždění ($>0,5\text{sec}$) neumožňuje interaktivní práci, běžné používané protokoly typické pro jiné sítě mohou selhávat.



Obrázek 3.8 – Grafické znázornění topologie satelitní sítě

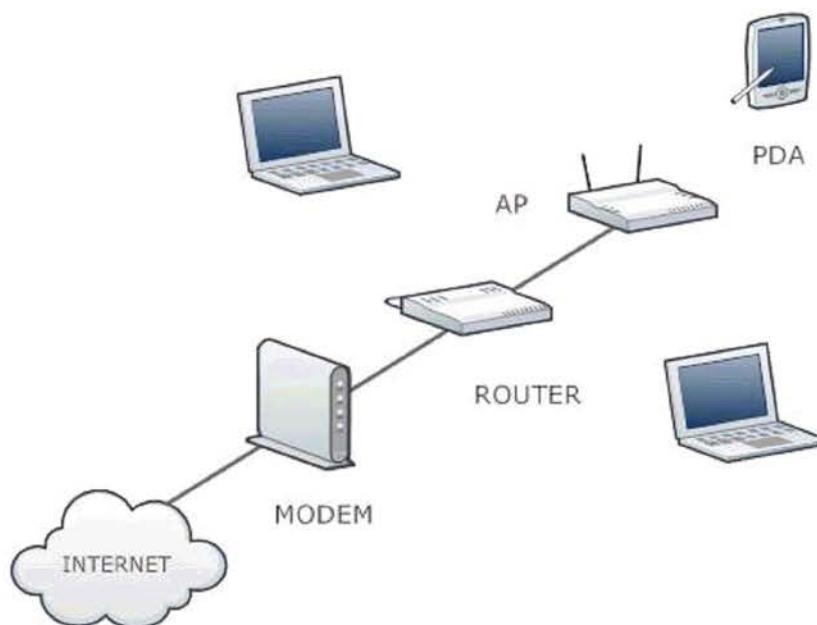
3.3.8 Bezdrátová síť založená na blízké infrastruktuře

Umožňuje mobilitu poblíž přístupového bodu, nevyžaduje zcela volný výhled (například na oblohu ve srovnání se satelitním uspořádáním).

Vyšší energetické nároky. Nižší šířka pásma ve srovnání metalickým vodičem nebo optikou.

Nedostatek frekvencí a povolení vysílat výkonem umožňujícím pokrýt významnější prostor. V režimu bez centrálního prvku je blízko ke sběrníkové topologii (zařízení si konkurují).

V režimu s centrálním prvkem připomíná spíše kruh a hvězdu, centrální prvek uděluje oprávnění, v jednodušší variantě jednotlivá zařízení mohou komunikovat pouze přes centrální prvek.



Obrázek 3.9 – Grafické znázornění topologie sítě založené na blízké infrastruktuře



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

4 Fyzická vrstva počítačových sítí

4.1 Kroucená dvojlinka

4.1.1 Historie a fyzika přenosu signálu

Dvojlinka obecně byla historicky první použité medium na přenos signálu. První technické zkušenosti pocházejí z telekomunikací. Již při přenosu hlasu, kdy bylo počítáno s frekvencemi max. 3 až 4 KHz se projevila fyzikální podstata elektrického proudu, elektromagnetického pole, elektromagnetického záření.

Na dlouhých telefonních spojích došlo k takzvaným přeslechům. Historicky každý pár přenášel jeden telefonní hovor a přeslech byl efekt, že v pozadí telefonního hovoru byly slyšet další telefonní hovory jako důsledek vyzařování a zpětného příjmu elektromagnetické vlny.

Tento efekt lze odstranit samostatným v kroucením každého páru. Kroucení párů v kabelu není náhodné, musí být propracované tak, aby docházelo co možná nejmenšímu útlumu signálu.

Každý signál musí mít svůj pár vodičů a proud přenášející signál musí být symetrický (součet proudů v obou vodičích daného páru musí být nulový).

Kabely jsou vyráběny v různých kvalitách, například telefonní kabel vyžaduje mnohem nižší kvalitu kroucení jednotlivých párů.

Pokud je jedná o koncovou spojku, tedy jeden pár, není kroucení ani nutné, minimalizace vyzařování a rušení je dosaženo pouze tím, že vodiče jsou po celou trasu v těsné blízkosti. U kabelu určeného například pro Gbit/s přenos jsou požadavky naopak extrémní.

V průmyslových aplikacích, kdy se na kabel (tj. na celé páry vodičů) mohou naindukovat velké proudy, které mohou vyřazovat s činnosti vstupní obvody síťového rozhraní je nutné všechny páry chránit společným stíněním (STP). Ve speciálních aplikacích dokonce je nutné stínit každý pár samostatně.

Má-li kroucená dvojlinka (Twisted Pair) přenášet vysokofrekvenční signál musí být správně impedančně přizpůsobena. Nejlepších výsledků lze dosáhnout, když se bude jednat o dvoubodový spoj (sběrnici lze použít při nižších požadavcích na šířku pásma - například v komunikačních sběrnících RS485, nebo telefonní linka - dva, tři, telefony na jedné lince).



Obrázek 4.1 – Kroucená dvojlinka - Hardware

4.1.2 Kroucená dvojlinka v počítačových sítích

Poprvé použita v sítích IBM (Token Ring), použity konektory, RJ11, RJ45. Nestíněná je označována Unshielded Twisted Pair, UTP. Stíněná je označována Shielded Twisted Pair, STP. Typicky dvoubodový spoj – topologie hvězdy, stromy, kruhy.

Velmi populární a dnes již klasické a standardní médium, spoje lze zhotovit snadno pomocí dostupných kleští, zaručenou mechanickou odolnost má strojně zhotovený spoj.

Spoj zakončený konektorem RJ45 musí být zapojený tak, aby byla zajištěna zpětná kompatibilita zásuvky při použití konektoru RJ11 například pro telefonní linku.

Spoj určený pro propojení dvou síťových rozhraní "stejného typu", tj. dva počítače nebo dva síťové prvky je zapojen tak, že se páry RX a TX kříží. Síťové prvky zpravidla použití kříženého kabelu obvykle nevyžadují (přepojují vstupy výstupy automaticky), v případě dvou počítačů nebo dalších speciálních aplikací (síťové mosty) se může křížený kabel hodit.

Kvalitu vyjadřuje kategorie spoje.

Kategorie 1

- Tento typ rozvodů není určen k datovým přenosům, lze jej použít např. k telefonním rozvodům.
- Přenosové rychlosti do 1 Mbit/s, vhodné např. pro analogové telefonní rozvody, ISDN a podobně.

Kategorie 2

- Určen pro přenos dat, s maximální šířkou pásma 1,5 MHz.
- Používá se pro digitální přenos zvuku a především pro rozvody IBM Token Ring.
- Přenosové rychlosti kolem 4 Mbit/s.

Kategorie 3

- Rozvody určené pro rozvody dat a hlasu s šířkou pásma 16 MHz a přenosovou rychlostí do 10 Mbit/s.
- Využívá se u datových přenosů označovaných jako 10Base-T Ethernet.

Kategorie 4

- Určen pro přenos dat v síti Token ring, s šířkou pásma 20 MHz a přenosovou rychlostí do 16 Mbit/s.

Kategorie 5

- Pracuje v šířce pásma do 100 MHz.
- Rozvody pro počítačové sítě s přenosovou rychlostí 100 Mbit/s, resp. 1 Gbit/s v případě využití všech 8 vláken.
- Využíván u 100 Mbit/s TPDDI a 155 Mbit/s ATM. V současné době je nahrazen standardem kategorie 5e.

Kategorie 5e

- Pracuje rovněž v šířce pásma do 100 MHz, avšak vyžaduje nové způsoby měření parametrů a v některých parametrech je přísnější.
- Cílem je provozovat 1 Gbit/s. Využíván u 100 Mbit/s TPDDI, 155 Mbit/s ATM a GigabitEthernet.

Kategorie 6

- Pracuje s šířkou pásma 250 MHz. Využívá se pro ultrarychlé páteční aplikace v oblasti lokálních sítí.
- V současné době nejpopulárnější kabeláž pro nově budované rozvody. Aplikace například při přenosu obrazu na velkoplošné obrazovky.

Kategorie 6a

- Pracuje s šířkou pásma 500 MHz. Používá se pro zvláště rychlé páteřní aplikace v oblasti lokálních sítí.
- Využívá se i pro 10GBASE-T Ethernet (10 Gbit/s).

Kategorie 7

- Pracuje v šířce pásma do 600 - 700 MHz.
- V současné době se provádí první pokusy s tímto standardem.
- Kabel je plně stíněný - každý pár je stíněn zvlášť Al fólií a kabel sám má ještě celkový štít.
- Plně stíněná konstrukce má ale za následek větší váhu, větší vnější průměr a menší ohebnost kabelu než UTP nebo STP.
- Používá se pro přenosy plné šířky videa, teleradiologii.
- Pro vysoké náklady (kabel i komponenty) zatím nerošířen.

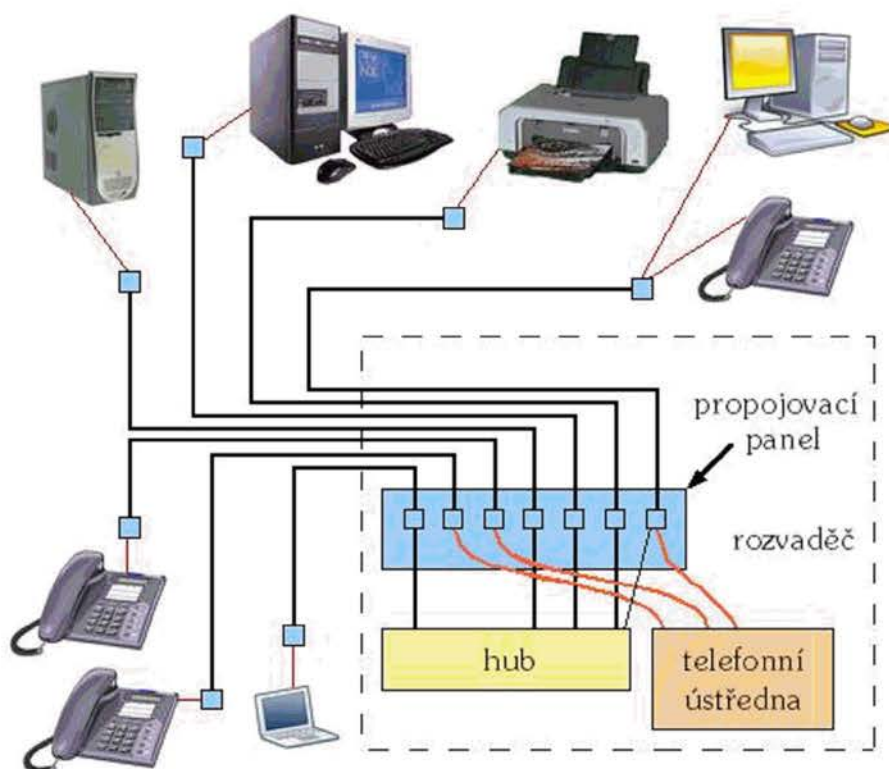
4.2 Strukturovaná kabeláž

Postupným budováním stále rozsáhlejších a modernějších sítí se vyvinula ucelená a dobře propracovaná představa o tom, jak by se rozvody počítačových sítí měly budovat.

Dnes se prakticky všechny nové síťové rozvody budují podle zásad tzv. „strukturované kabeláže“.

Strukturovaná kabeláž současného typu je založena právně na kroucené dvojlince (určitou přechodnou dobu existovaly i instalace založené na koaxiálním kabelu).

Kabeláž ode všech zásuvek je svedena do jednoho centra, zásuvka se tak může „stěhovat s uživatelem“.



Obrázek 4.2 – Typické využití strukturované kabeláže

4.2.1 Požadavky na strukturovanou kabeláž

Vlastní kabelové rozvody jsou vedené tak, aby nepřekážely. Životnost kabelových rozvodů je obecně mnohem delší než životnost zařízení, která je budou využívat. Provedení kabeláže je velmi drahé (dnes dokonce dražší, než cena hardwaru, který se k těmto rozvodům připojuje).

Síťové rozvody jsou zcela záměrně předimenzovány, zároveň je snaha zavádět síťové rozvody i do takových místností či částí budovy, kde dnes ještě není žádné připojení požadováno.

Kvalitní rozvody tak, aby se minimalizovalo nebezpečí poruch a závad, čehož se dosahuje používáním kvalitních kabelů, konektorů, zástrček a dalších instalačních prvků, i vhodnými instalačními postupy (například vedením kabelů lištami apod.).

Univerzálnost strukturované kabeláže - bude možné rozvody využít pro více různých účelů (například telefonní rozvody, rozvody pro zabezpečovací zařízení apod.). Používané materiály již jsou natolik spolehlivé a trvanlivé a metodika budování strukturované kabeláže je dnes již tak dobře propracovaná, že firmy jsou ochotny poskytovat velmi dlouhé záruky - dnes standardně 15 let.

4.2.2 Topologie strukturované kabeláže

Pro správné pochopení podstaty strukturované kabeláže je dobré si uvědomit, že jde jen o ryze pasivní rozvody. Součástí strukturované kabeláže nejsou ani koncové uzly (uživatelské pracovní stanice), ani nejrůznější servery či aktivní síťové prvky.

Celková topologie systémů strukturované kabeláže je inspirována filosofií Ethernetu na kroucené dvojlince, ale na druhé straně je natolik univerzální, že může být použita i pro jiné sítě a jejich kombinace.

Topologie strukturované kabeláže je v zásadě stromovitá (v základní variantě hvězdovitá, viz. obrázek).

Důležitým konstrukčním prvkem strukturované kabeláže je rozvodná skříň, do níž se musí vejít všechny spojovací prvky (propojovací kabel, rozbočovače, ústředna atd.).

V nejnižších „patrech“ jsou použity rozvody na bázi kroucené dvojlinky, omezené svým dosahem na 100 metrů. Tyto rozvody „sbírají“ koncové přípojky ve svém dosahu, a „slučují“ je do větších celků (v případě klasického Ethernetu běžným switechem).

Z rozvodných míst nejnižší úrovně pak vedou další spoje směrem „nahoru“ (tzv. uplinky, typicky z optických vláken) do propojovacích míst vyšších úrovní - zde může být i několik „pater“, a v každém z nich se mohou jednotlivé celky nižších úrovní slučovat či navzájem propojovat - ať již prostřednictvím mostů, směrovačů, tzv. switchů apod.

Vše je přitom záměrně univerzální, tak aby jednotlivá propojovací místa (realizovaná typizovanými rozvodnými skříněmi) bylo možné osadit podle konkrétních potřeb různými aktivními prvky, a vytvořit tak téměř libovolnou logickou (a do určité míry i fyzickou) topologii počítačové sítě.



Obrázek 4.3 – Příklad kabeláže v rozvodné skříní

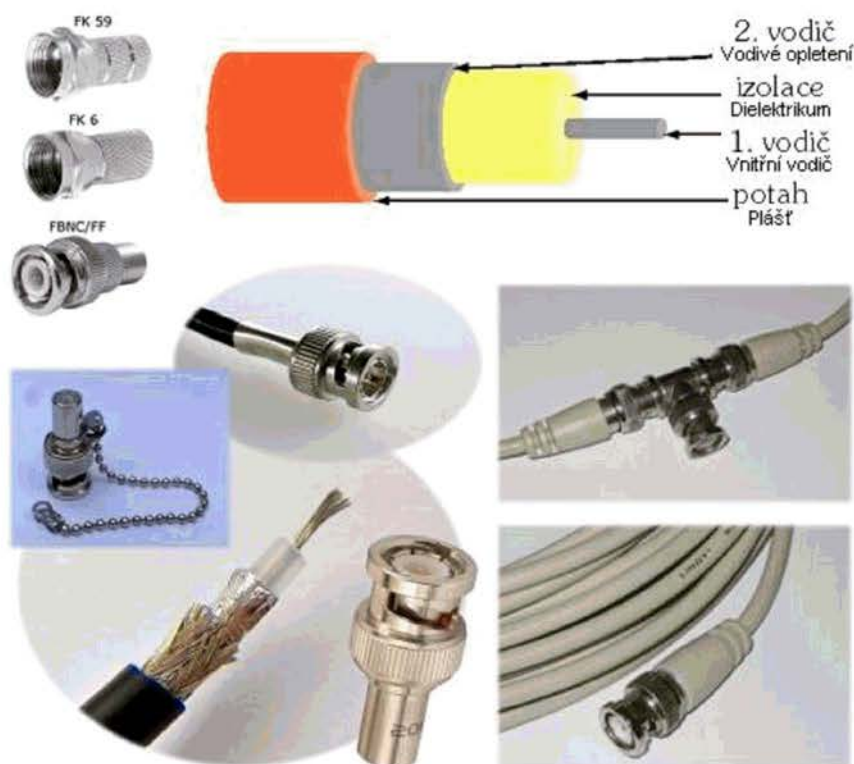
4.3 Koaxiální kabel

4.3.1 Vlastnosti koaxiálního kabelu

Koaxiální kabel je asymetrický elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým nebo trubkovým vodičem vnitřním.

Vnější vodič nazýváme často stíněním a vnitřní vodič jádrem. Vnější a vnitřní vodič jsou odděleny nevodivou vrstvou (dielektrikum).

Nejčastější funkcí koaxiálního kabelu je přenos elektromagnetického vlnění o vysokém kmitočtu (řádově do 50 GHz), u vysokých frekvencí signálu se jedná se o jakýsi vlnovod.



Obrázek 4.4 – Koaxiální kabel a použité konektory

Koaxiální kabel je nejstarším typem používaným v počítačových sítích. Měl velký vliv na rozvoj počítačových sítí (LAN). Motivem jeho použití nebyla pouze ona obrovská šířka pásma, ale především eliminace vícenásobného příjmu signálu a minimální rušení a šum.

Až po vývoji nových integrovaných obvodů, metod jak modulovat/demodulovat signál, vyrovnat se s vícenásobným příjmem a šumem mohla být používána levnější kroucená dvojlinka (i ta nelepší kategorie 7 umožňuje přenášet signály jen málo převyšující 600MHz, a ta se již začíná podobat koaxiálu - stínění, dielektrikum).

Nezastupitelný je dále v anténních systémech a je dále používán v počítačových sítích operátorů kabelové televize (kombinované systémy digitální televize, internet 100MB a výše, telefon).

V souvislosti s technologií Ethernet bývá v různých pramenech uváděno, že jeho přenosová rychlost je pouze 10MB/s a na kroucené dvojlince je dosahováno 100x vyšších rychlostí, to je však pouze specifikum Ethernetu nikoliv vlastnost tohoto média!

Základním rozdílem při použití koaxiálního kabelu, kroucené dvojlinky nebo optického vlákna je to, že na koaxiálním kabelu je možné dělat odbočky, a je tudíž možné jej využít pro tzv. vícebodové spoje (vzájemně propojující více koncových uzlů pomocí T-konektorů).

Naproti tomu na kroucené dvojlince ani na optickém vlákne není možné dělat odbočky, a tato přenosová média jsou tudíž použitelná jen pro dvoubodové spoje (a potřebné „rozbočení“ se musí zajistit elektronickou cestou, ve vhodných rozbočovačích - hubech).

Potíž však byla v tom, že při poruše jednoho z počítačů navzájem propojených koaxiálním kabelem přišli o možnost komunikace zároveň všichni, kteří byli připojeni k porouchanému segmentu sítě.

Přesná lokalizace závady pak bývala velice náročná. S kroucenou dvojlinkou je tomu poněkud jinak. Když zde dojde k nějaké závadě, možnost komunikace ztrácí zpravidla jen jeden určitý koncový uzel, ale ostatní mohou pracovat dále.

Použití koaxiálního kabelu pro dvoubodový spoj a přenos digitálního signálu je dnes luxusem, a záležitostí speciálních aplikací, dále je si nutné uvědomit, že musí být použity koaxiály dva (RX, TX), původní Ethernet byl pouze poloduplexní.

4.3.2 Konektory pro koaxiální kabel

Konektor BNC (British Naval Connector)

- Připájený/nalisovaný na konec kabelu.
- Používán zpravidla v měřicí technice (v minulosti též v ethernetu a proto je známý).
- Určen pro časté připojování a odpojování.
- T-konektor BNC, I-konektor BNC, umožňují spoje a větvení.
- Terminátor - obyčejný odpor 50Ω absorbuje energii VF signálu.

FK konektor

- Používán pro trvalejší instalace.
- Je jednodušší a přitom vhodný pro nejvyšší frekvence signálu.
- Dnes velmi rozšířen v satelitní a televizní technice.

Další vysokofrekvenční konektory

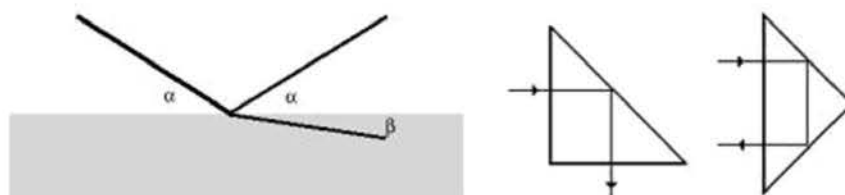
- Velké verze ve výkonové vysílací technice.
- Miniaturní pro GSM, Wi-Fi aplikace.

4.4 Optický kabel

Je tvořen jedním nebo více optickými vlákny, která jsou spolu s vhodnou vystýlkou uložena ve vnějším obalu. Jádru má průměr řádově několik jednotek až desítek mikrometrů a je obvykle vyrobeno z různého druhu skla.

Tento typ kabelu je založen na odlišném principu než předchozí. Data nejsou přenášena elektricky v kovových vodičích pohybem elektronového obalu atomů, ale fotony, světelnými impulsy v průsvitných vláknech.

Při vedení světelného signálu se využívá jevu zvaného úplný odraz, ke kterému dochází na rozhraní jádra a pláště při vhodné volbě materiálu jádra a pláště.



Obrázek 4.5 – Dopad, lom a odraz světla

Na obrázku je znázorněn princip dopadu lomu a odrazu světla. Optická hustota vlákna musí být ve srovnání s pláštěm světlovodu významně vyšší, aby k lomu β znázorněnému na obrázku vůbec nedošlo.

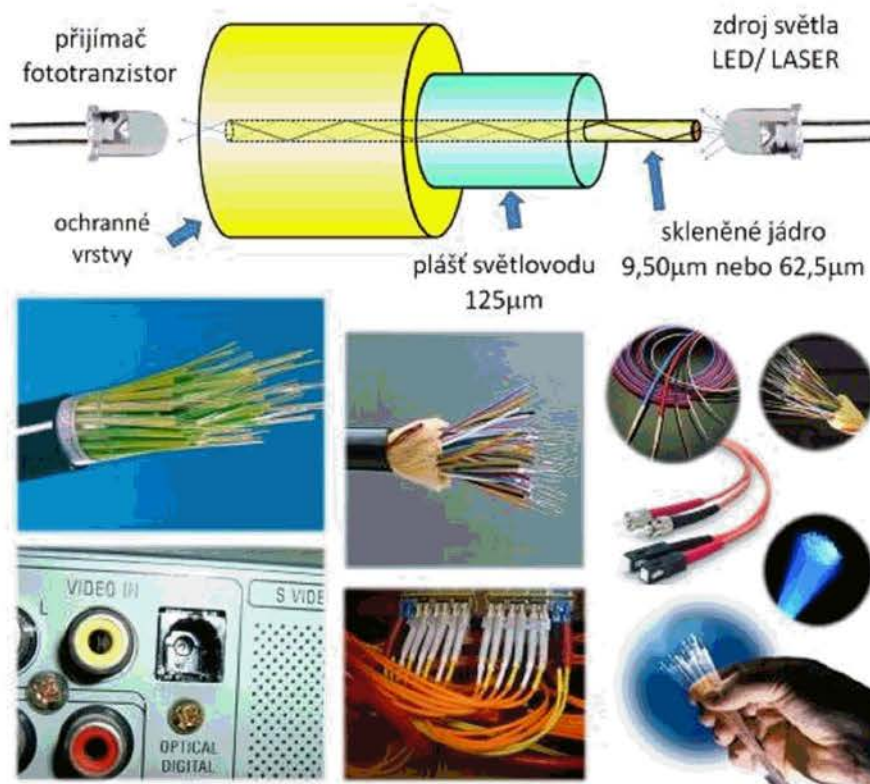
Fotony zůstávají tak „uvězněny“ ve vláknech a šíří se bez významných ztrát na druhý konec kabelu (podobný efekt můžeme pozorovat pouhým okem, například pod vodou se nám hladina od určitého kritického uhlu jeví jako zrcadlo).

Optické kabely umožňují přenos signálu na velké vzdálenosti (až 10 km při využití jednovlákenných optických vláken, viz dále) bez použití aktivních prvků.

Výhodou optických kabelů je naprostá odolnost vůči elektromagnetickému rušení (fotony jsou elektricky neutrální částice na rozdíl od elektronů), velmi nízké ztráty a vysoká přenosová rychlost.

Před přenosem je třeba zajistit převod elektrického signálu na optický, což zajišťují LED diody nebo laserové diody, které generují světelné impulsy podle přiváděného proudu (tzv. generátor).

Na druhé straně vedení je třeba optický signál přenést zpět na elektrický, což zajišťují fotodiody, fototranzistory (tzv. detektor).



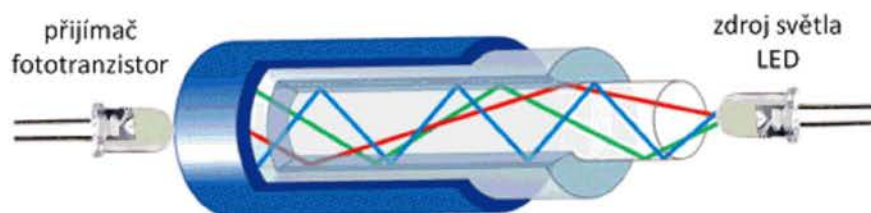
Obrázek 4.6 – Aplikace optického vlákna

4.4.1 Vlastnosti optického vlákna

- Uváděn bývá zpravidla rozměr jádra a jeho obalu.
- obrovská šířka pásma (terabity)
- nerušitelné, neruší (nevyzařuje, neindukuje el. mag. vlnění)
- standardní pro venkovní spoje
- nelze odposlouchávat („napíchnout“)
- dvoubodový spoj, odbočka nebyla uspokojivě vyřešena
- poměrně drahé, ale dostupné již na běžné aplikace
- méně pružné

4.4.2 Vícevidové vlákno

- Anglicky multimode (MM) - při průchodu vláknem je světelná energie rozdělena na více paprsků (tzv. vidů), na konec kabelu dojdou jednotlivé vidy s časovým odstupem, což vede ke zkreslení signálu.
- Různoběžné paprsky urazí různé vzdálenosti - viz. obrázek, kde jsou paprsky, které urazí odlišnou vzdálenost, znázorněny různou barvou.
- Odezva na sestupnou hranu je dohasínání na straně přijímače.
- Světelným zdrojem je svítivá polovodičová dioda (LED).
- Dosah stovky metrů až 2 kilometry.
- Tyto kabely jsou levnější, ovšem mají horší optické vlastnosti.
- Jejich jádro má průměr 50, 62,5 nebo 100 mikrometrů (obal 125 mikrometrů).



Obrázek 4.7 – Šíření světla ve vícevidovém vlákně

4.4.3 Jednovidové vlákno

- Anglicky singlemode (SM) - kabelem prochází jeden paprsek (bez odlišných lomů a drah).
- Jednovidová optická vlákna mají jádro o velmi malém průměru (typicky 9 mikrometrů).
- Světelným zdrojem je Laser.
- Tyto kabely mají lepší optické vlastnosti, vyšší přenosovou kapacitu, přenášejí na větší vzdálenost (dnes v řádu desítek kilometrů až stovek kilometrů), ale jsou dražší.



Obrázek 4.8 – Konektory optických spojů

4.4.4 Využití optického vlákna, konektory

Optické kabely se dají použít ve všech topologiích, nejčastěji v páteřním vedení.

Používají se dva typy zakončení optického kabelu - kulatý konektor ST a hranatý konektor SC (vzhled viz. předchozí obrázek 4.8).

Na konci každého kabelu je nutný převodník (transceiver) pro převod elektrických impulsů na světelné paprsky a naopak.

Dalším prvkem je konvertor, který dovoluje napojit optický kabel na kroucenou dvojlinku.

Zakončení optického kabelu vyžaduje speciální a drahé pomůcky. Zakončení je prováděno firmou jako služba (nelze řešit své pomocí).

Přenosová rychlost optických kabelů se pohybuje od stovek megabitů až k mnoha gigabitům za sekundu, přičemž další zvyšování dosažitelných přenosových rychlostí díky technologickému pokroku lze očekávat. Na druhé straně realizace optické sítě je finančně nákladná i technicky náročná.

4.4.5 Vlnový multiplex (WDM)

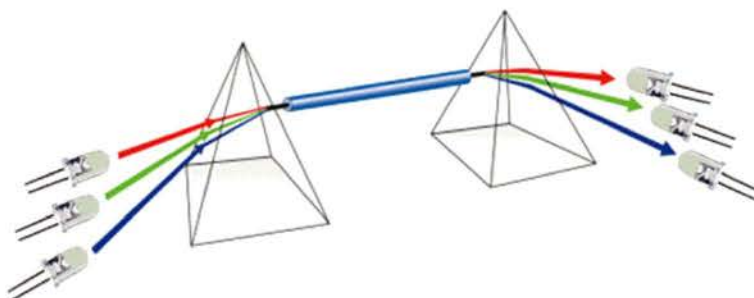
Vlnový multiplex je technologie, kterou se při přenosu multiplexuje více optických signálů v jednom optickém vlákne s použitím rozdílných vlnových délek (barev) LED nebo laserů.

Princip je znázorněn na následujícím obrázku 4.9. Je tak umožněno rozšířit kapacitu média nebo provést obousměrnou komunikaci na jednom optickém vlákne.

Pojem vlnový multiplex se nejčastěji používá při přenosu informace optickým způsobem (signál bývá popsán svojí vlnovou délkou). Zatímco frekvenční multiplex se typicky používá při rádiovém přenosu informace (charakteristickým znakem signálu bývá jeho frekvence).

Stejně jako se při frekvenčním multiplexu pro různé signály používají různé frekvence, tak pro komunikaci po optickém vlákně je použit WDM za použití nosných různých vlnových délek.

Ostatně vlnová délka je nepřímo úměrná frekvenci daného vlnění, navíc optický i rádiový signál jsou pouze dvě možné formy elektromagnetického vlnění.



Obrázek 4.9 – Princip vlnového multiplexu (WDM)

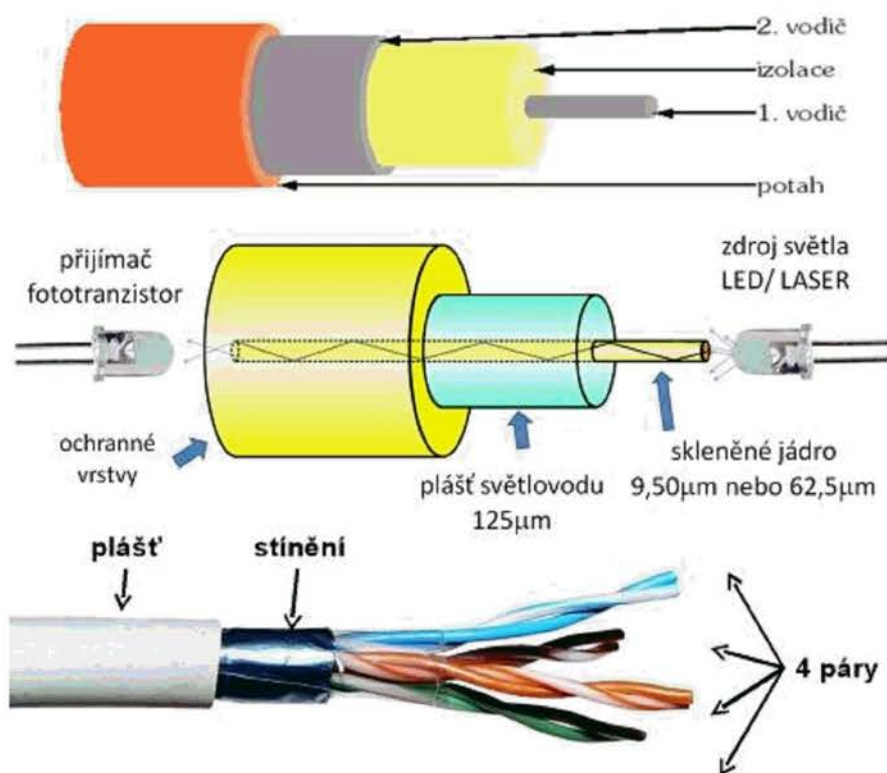
Koncept byl poprvé publikován v roce 1970 a v roce 1978 byl WDM realizován v laboratořích. První WDM umělo kombinovat dva signály. Moderní systémy umožňují až 160 signálů a umožňují rozšířit 10 Gbit/s optický systém na teoretickou kapacitu 1.6 Tbit/s přes jeden optický pár.

WDM je populární v telekomunikačních společnostech, protože jim umožňuje rozšiřovat kapacitu sítě bez nutnosti pokládání dalších optických vláken. Při použití WDM a optických zesilovačů, můžou umístit více generací technologie v jejich optické infrastruktuře, bez nutnosti renovace pátevní sítě. Kapacita může být navyšována jednoduchým rozšířením multiplexu na každém konci.

Nejčastěji se používají opticko-elektricko-optické převodníky na samém okraji transportní sítě, čímž je zachována interoperabilita s existujícími zařízení s optickými rozhraními. Většina WDM systému pracuje na jednovidových optických vláknech, které mají průměr jádra 9 μm , ale i na vícevidových optických vláknech je WDM možné.

4.5 Srovnání optického kabelu, koaxiálu, kroucené dvojlinky

Optický kabel se principiálně podobá koaxiálu. Rozdíl je především v materiálech a rozměrech. Koaxiál můžeme dále jako elektrický vodič srovnávat s dvoulinkou.



Obrázek 4.10 – Srovnání optického kabelu, koaxiálu, kroucené dvojlinky

Koaxiál

- V případě koaxiálu je elektromagnetické vlnění (rozměr vlny cca 1 metr) vytvořené elektrickým proudem na povrchu středního vodiče.
- Podle konstrukce (rozměrů a materiálů) vykazuje koaxiál útlum signálu, který roste s frekvencí. Je li vše správně nastaveno, tzv. vlnová impedance přizpůsobená impedanci zdroje i přijímače signálu (obvykle 50Ω nebo 75Ω) je přenos signálu je principiálně možný na relativně velké vzdálenosti (stovky metrů až jednotky km - kabelová televize).

Optické vlákno

- V případě optického vlákna jsou elektromagnetické vlny (fotony) přivedené do prostoru bez metalického vodiče ze zdroje jako je LED nebo Laser (elektromagnetické vlny mají rozměr cca 0,0005mm).
- Narušení podmínek úplného odrazu světla vede ke ztrátě signálu. Dosud nebylo u optického vlákna vyřešeno snadné větvení. Další rozdíl mezi koaxiálem a optickým kabelem je tedy, že optický kabel je striktně dvoubodový spoj.
- Na rozdíl od koaxiálu nabízí optické vlákno útlum nezávislý na frekvenci elektromagnetického vlnění, tj. od blízkého infračerveného až po viditelné spektrum.
- Šířka pásma (maximální frekvence namodulovaného signálu) však klesá s délkou kabelu (viz. předchozí problematika jednovidového a vícevidového vlákna).
- Optické vlákno může tedy nabídnout terabitové rychlosti přenosu nebo může být jen o málo lepší než nejkvalitnější (a velmi drahý) koaxiál.

Kroucená dvojlinka

- U dvojlinky je základem přenosu signálu elektrický proud. Energie se u vysokofrekvenčního signálu transformuje na elektromagnetické vlnění a zpět na elektrický proud (v obou vodičích daného páru teče stejný proud jen opačného směru).
- Protože každý pár vodičů vytváří ještě magnetické pole v rytmu daného signálu je zapotřebí dvojlinku kroutit (v případě kabelu každý pár z jiným počtem překroucení na jednotku délky).
- Útlum signálu strmě roste s délkou, hrozí vícenásobný příjem signálu (například telefonní linka a DSL modem), útlum strmě roste s frekvencí střídavého elektrického proudu.

- Různé aplikace, různé délky a různé rychlosti přenosu pomocí Kroucené dvojlinky:
 - SATA - 1 m.
 - USB - 5 metrů.
 - různé porty - 10 metrů.
 - ethernet - 100 metrů.
 - DSL - 2 km.
- Medium má tedy nejvyšší požadavky na modulaci a demodulaci signálu, používány jsou metody podobné jako u bezdrátového přenosu, velký rozvoj → investice do modulátoru a demodulátoru se vyplatí, protože kroucená dvojlinka je nejlevnější a nejflexibilnější (konektory, manipulace s kabelem atp.) a částečně vytlačuje koaxiál z dalších oborů (televizní technika).



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

5 Ethernet

5.1 Vznik Ethernetu

Síť principiálně podobnou dnešnímu Ethernetu poprvé sestavil a testoval Robert Melancton Metcalfe ve firmě XEROX v roce 1970.

Síť přenášela data rychlostí 3Mbit/s a byla nazývána „experimentálním ethernetem“.

První standard vznikl v roce 1976, jeho označení je IEEE 802.3. V roce 1980 vzniklo konsorcium tří firem (Digital, Intel, Xerox), které stanovilo první parametry nejstaršího Ethernet systému s přenosovou rychlostí 10Mbit/s, vznikl tak klasický Ethernet, tak jak ho pod tímto názvem známe dnes (někdy také označovaný jako DIX).

V roce 1985 byl Ethernet standardizován postupně nejprve na půdě IEEE pod standardem IEEE 802.3 a později na půdě ISO pod standardy 8803.2 (Ethernet II, DIX).

Všechna zařízení vyráběna po roce 1985 vyhovují oběma těmto standardům. DIX Ethernet a IEEE 802.3 standard jsou funkčně kompatibilní, je zde rozdíl ve významu jednoho pole v rámci (viz. kapitola Přístup k mediu).

Ethernet od svého počátku byl založen na přístupové metodě CSMA/CD. Tento způsob (ne)řízení přenosu jej odlišoval od ostatních technologií, které v obecné konkurenci prorazil.

Základním pojmem u této metody „řízení přenosu“ je kolize - situace, kdy v jednom okamžiku vysílají dvě nebo více stanic. Ethernet kolizi připouští a řeší opakováním pokusů o přenos podobně, jako někdy postupují lidé - diskutující kolektiv.



Obrázek 5.1 – Vznik ethernetu, hardware kdysi a dnes

Ethernet byl od začátku vyvíjen pro kancelářské aplikace a je tak používán do dnes. Jeho masivní rozšíření a zlevnění kabeláže i síťových prvků jej prosadilo v technických i v průmyslových aplikacích.

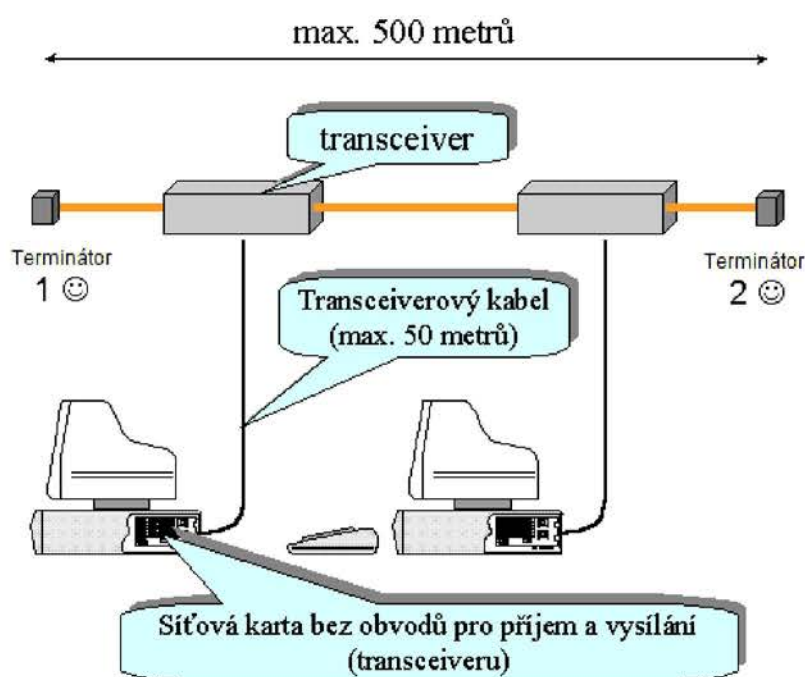
V kancelářské verzi i v průmyslových aplikacích je dnes původní algoritmus CSMA/CD potlačován a nahrazován, pokaždé však odlišným způsobem (viz. kapitola Hub versus switch).

5.2 Topologie Ethernetu

5.2.1 Sběrníková topologie založená na koaxiálu

Topologie Ethernetu byla vždy striktně sběrníková. Původní elektrická realizace byla založena na tzv. tlustém koaxiálu, který mohl být bez jakéhokoliv aktivního prvku dlouhý 500 metrů. Koaxiál tvořil onen prostor (ether) pro šíření signálů bez odrazů a vícenásobného příjmu. Síťové prvky naslouchaly elektricky vysokým vnitřním odporem (a vysílaly do zátěže 50 ohm).

Energie signálu se mařila tzv. terminátorech (VF rezistor 50 ohm). Posilováním signálu bylo možné zvyšovat vzdálenost (délku páteře sítě) až na 2 km. Tato vzdálenost již dále zvyšovat nešla (problém kolizního okénka viz. článek Přístup k mediu). Přenosová rychlost byla na osmdesátá léta poměrně vysoká (10Mb/sec).

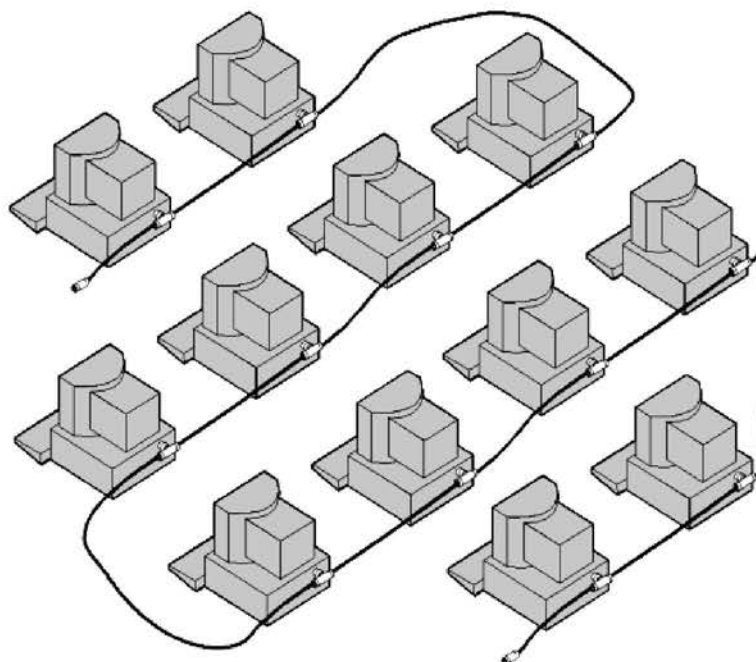


Obrázek 5.2 – Původní ethernet založený a tlustém koaxiálu

Tlustý koaxiál byl nepřerušovaný kabel (obvykle žluté barvy), na který se připojoval speciálními „upířími“ kleštěmi transceiver (střední vodič nebyl porušen, stínění minimálně).

Výhodou topologie byla možnost připojit počítač až 50 m od páteře. Páteř obvykle se „proplazila“ celou budovou. Fyzické uspořádání lze vidět na předchozím obrázku 5.2.

Tlustý koaxiál vyžadoval speciální vybavení (velmi speciální kleště) a dovednost (porušení kabelu bylo fatální).



Obrázek 5.3 – Ethernet založený a tenkém koaxiálu – učebna

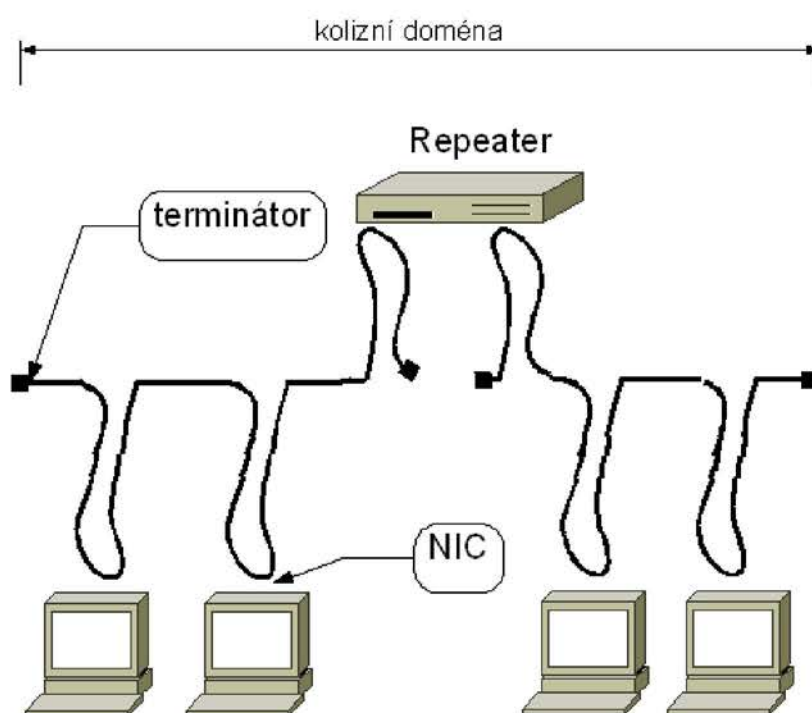
Tenký koaxiál je prostá náhrada tlustého kabelu běžným koaxiálem s BNC konektory (používáno tehdy i dnes v měřicí technice, ve vysílací technice).

Podle způsobu provedení byla vzdálenost výrazně kratší (50m-200m podle kvality realizace).

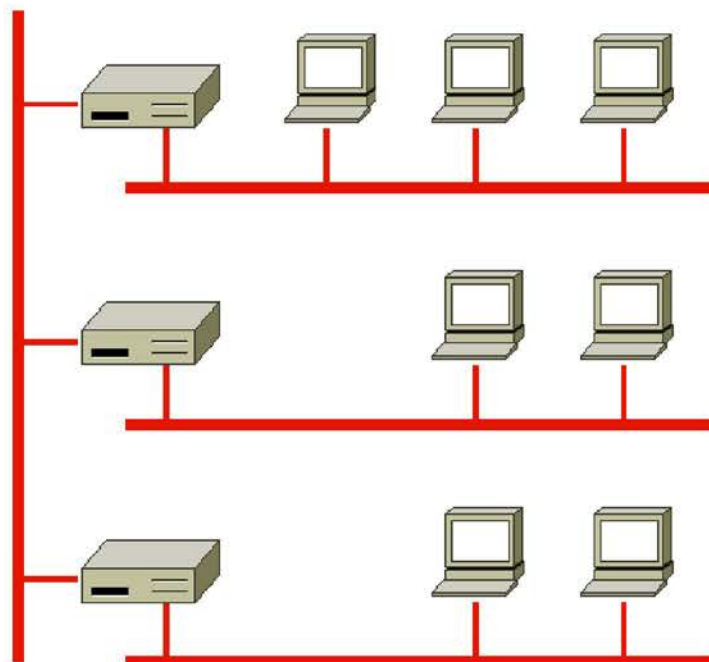
Tento způsob byl později normalizován (10Base2) s tím, že transceiver byl integrován přímo do rozhraní počítače (zkrácení rozměru sítě o transceiverové kabely).

Zapojování takovýchto lokálních sítí bylo velmi populární například v učebnách - viz. předchozí obrázek 5.3. V administrativních budovách byl malý rozměr sítě kompenzován opakovači viz. obrázek 5.4. a 5.5.

Fyzická realizace připouštěla i větvení, ale stále se jednalo o jeden prostor, o tzv. jednu kolizní doménu jako hraniční rozměr byl uváděna vzdálenost 910 m na místo teoretických 2 km.



Obrázek 5.4 – Ethernet založený a tenkém koaxiálu – kancelářské prostředí



Obrázek 5.5 – Ethernet založený a tenkém koaxiálu – kancelářské prostředí s větvením

5.2.2 Strukturovaná kabeláž založená na koaxiálu

Upouštění od tlustého kabelu mělo za následek obtížnou realizaci sítě (odbočky od páteře již nebyly možné). Aby bylo možné se alespoň trochu vrátit k původním možnostem, tj. najít náhradu za transceiverové odbočky byly vyvinuty zásuvky EAD.

Zásuvky EAD umožňovaly připojit fyzicky zdánlivě hvězdicovitě počítače do jedné infrastruktury. Signál musel projít všemi zásuvkami. Každá zásuvka představovala narušení páteře a její prodloužení od metry a metry koaxiálního vedení k počítači a zpět k zásuvce.

Nevýhodou byla nižší spolehlivost, strukturovaná kabeláž sloužila jen pro počítačovou síť (např. telefon potřeboval svou vlastní infrastrukturu).

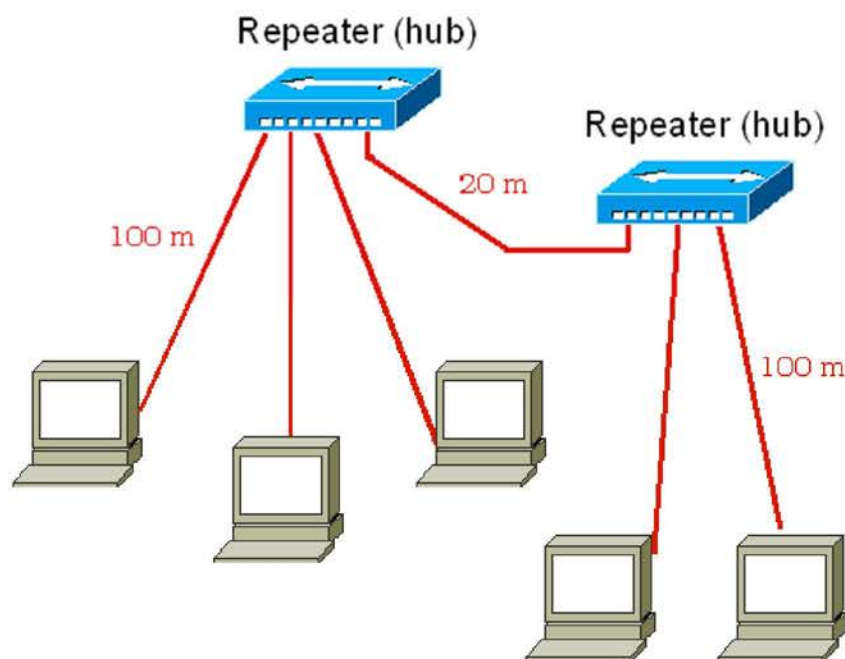


Obrázek 5.6 – Strukturovaná kabeláž založená na tenkém koaxiálu

5.2.3 Sběrníková topologie založená na kroucené dvojlince

Sběrníková topologie založená na kroucené dvojlince je znázorněná na obrázku. Ano čtete správně, topologie je logicky skutečně sběrníková.

Sběrnice je fyzicky zdánlivě zapojená do hvězdy nebo stromu, to je pravda, signál z každého rozhraní je však šířen v celé síti, ke všem účastníkům, jako by byli na připojení na jenom starém dobrém tlustém koaxiálu ☺.



Obrázek 5.7 – Zapojení sítě ethernet pomocí rozbočovačů a kroucené dvojlinky

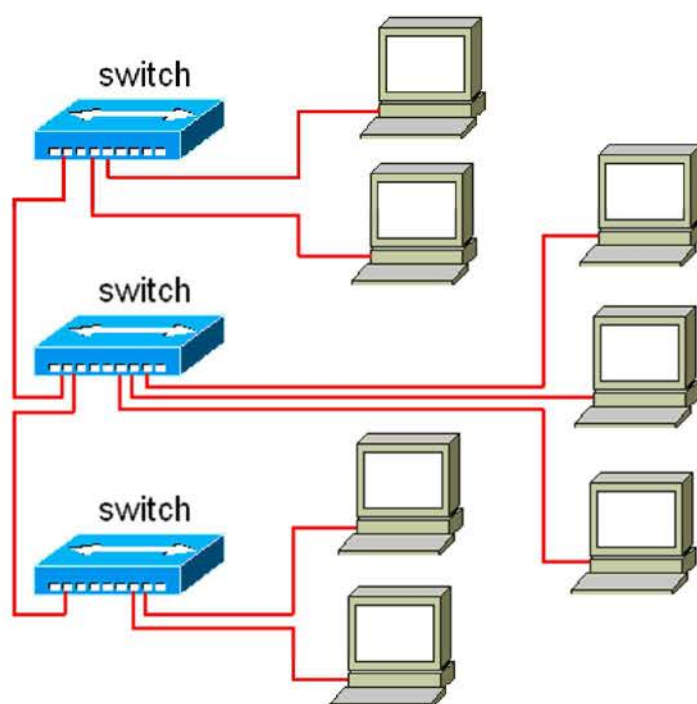
Spoje jsou dvoubodové jen proto, že je použita kroucená dvojlinka a každé síťové rozhraní má integrovaný terminátor a je tak podobně jako u koaxiálu bráněno odrazům a vícenásobnému příjmu. Na obrázku jsou patrné též délky. Jeden spoj může být maximálně 100metrů dlouhý. Celá síť nesmí přesáhnout rozměr 220 m. Toto zkrácení délek vychází z deseti-násobení přenosové rychlosti (zrychlení z 10Mbit/sec na 100 Mbit/sec vedlo ke zkrácení kolizní domény z přibližně 2 km na 220 metrů).

Přechod z koaxiálu byl v minulosti pozvolný, protože onen nárůst vodičů uživatele odrazoval, výrazné zlevnění vodičů UTP i rozbočovačů postupně uživatele k přechodu na kroucenou dvojlinku přimělo.

Algoritmus CSMA/CD je v tomto případě limitující, jedině jeho vyřazením lze dále zvyšovat vzdálenosti (viz. kapitola Hub versus switch).

5.2.4 Hvězdicová a stromová topologie založená na kroucené dvojlince

Přechod kancelářského ethernetu na hvězdicovou technologii je realizován výměnou centrálních rozbočovačů za přepínače (SWITCHe). Algoritmus CSMA/CD je síťovým adaptérem deaktivován a komunikace se stane plně duplexní (adaptér může 100Mbit/sec přijímat a současně vysílat - nehlídají ze žádné kolize, směrování na fyzické vrstvě zajišťuje právě SWITCH).



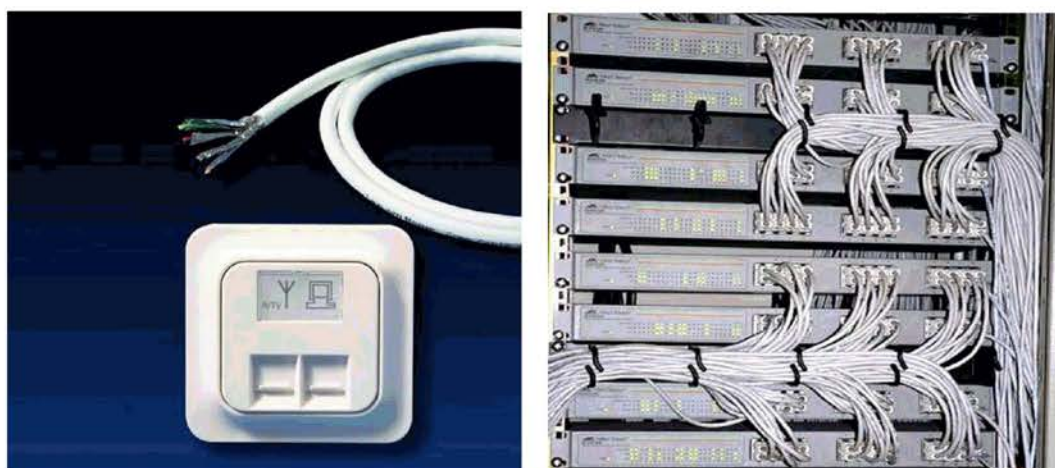
Obrázek 5.8 – Zapojení sítě ethernet pomocí přepínačů a kroucené dvojlinky

Kvalita sítě je do značné míry dána síťovými prvky, výpadek centrálního prvku je fatální. Při použití kvalitnějšího spoje lze zvyšovat vzdálenosti (koaxiální linka, vícevidové vlákno nebo dokonce jednovidové vlákno).

5.2.5 Strukturovaná kabeláž založená na kroucené dvojlince

Při stavbě nových budov se vyplatí investovat do infrastruktury aniž by bylo v době investice bezprostředně zapotřebí. Princip spočívá v položení kilometrů vodičů již při stavbě. Dominuje především hvězdicovitá struktura - viz. obrázky 5.9 níže.

V datovém centru jsou obvykle umístěny jak přepínače sítě ethernet, tak telefonní ústředna, dále například zabezpečení budovy (více v předešlém článku Strukturovaná kabeláž v kapitole Fyzická vrstva počítačových sítí).

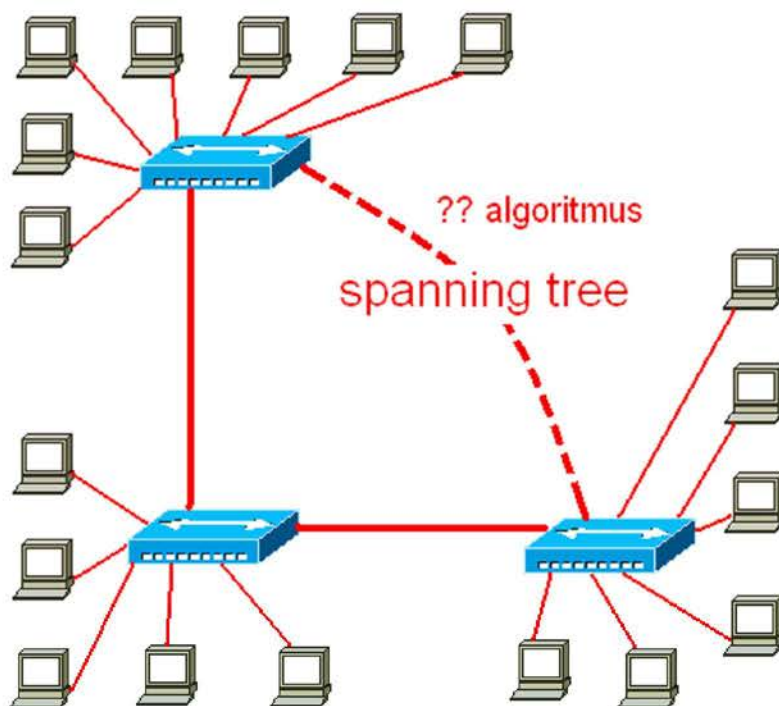


Obrázek 5.9 – Zapojení sítě ethernet přes zásuvky RJ45, tvorba strukturované kabeláže

5.2.6 Topologie obecný graf založená na kroucené dvojlince

Běžné přepínače (rozbočovače už vůbec ne) nepřipouštějí duplicitní propojení jinak běžně používané v celosvětové síti internet.

Na obrázku 5.10 je znázorněna situace, kdy by bylo příhodné realizovat duplicitní linku. Profesionální přepínače umožňují duplicitní linku obsluhovat, funkce je většinou známá pod označením „spanning tree“.



Obrázek 5.10 – Zapojení sítě ethernet pomocí přepínačů a kroucené dvojlinky s duplicitním spojem

Nejedná se o topologii obecného grafu v pravém slova smyslu, rozbočovače striktně realizují hvězdu, přidané linky „spanning tree“ zpravují jako záložní a při výpadku příslušného portu je pokouší aktivovat.

5.3 Přístup k médiu

5.3.1 Přístupová metoda CSMA/CD

Stanice, která chce vysílat data, naslouchá, zda síť již není využívána jinou stanicí (část CSMA, kde CS - Carrier Sense - znamená možnost „příposlechu“ přenosu, MA - Multiple Access - vyjadřuje celkový charakter přenosového média, které je sdílené a přístup k němu mají všechny uzly současně a je tedy možné i současné vysílání více uzlů).

Je-li síť již využívána, čeká stanice po náhodně zvolený interval. Zjistí-li stanice, že je na síti klid, začne vysílat - současně se snaží zjistit, jestli nedošlo ke kolizi (část CD - Collision Detection - detekce kolize).

Kolize znamená, že začala současně vysílat jiná stanice - při kolizi dochází ke střetu signálů a jejich zkreslení. Dojde-li ke kolizi, pak pracovní stanice, která toto zjistí, přestane vysílat a vyšle na síť krátký kolizní signál (jam). Vyslání jam signálu znamená, že i ostatní stanice přestanou vysílat a zopakují pokus o vysílání opět po náhodně zvoleném časovém intervalu.

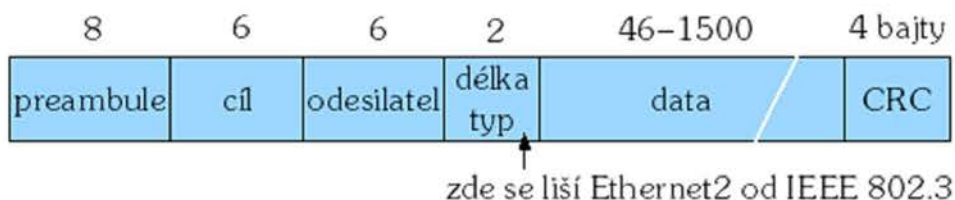
Je-li vysílání přerušeno kolizí 16x za sebou, je pokus o vysílání zprávy ukončen (přerušen) definitivně a vyšší vrstva obdrží chybové hlášení. Přitom při každém následujícím přerušení vysílání kolizí se náhodná prodleva volí z dvojnásobně delšího intervalu.

5.3.2 Přístup k mediu v dnešním přepínaném Ethernetu

Stanice vysílá a přijímá rámce podle požadavků vyšších vrstev. Přepínač co by protějšek každému síťovému adapteru zajišťuje směrování podle adres fyzické vrstvy - MAC (viz. článek Přepínaný Ethernet, rychlý Ethernet).

5.3.3 Formát rámce

Rámec obsahuje nejprve určitou vysílací předebru tzv. preamble: 10101010...10101010...10101011 (umožňuje adaptéru synchronizovat příjem, poslední jednička startuje další přenos). Dále adresy cíl, odesílatel: vždy 48-bitová adresa MAC. (viz. odstavec Adresy).



Obrázek 5.11 – Formát rámce v síti ethernet

Dále délka, typ: délka přenesených dat (IEEE 802.3), druh přepravovaných dat (Ethernet 2). Dále data: Nesená informace (datový balíček vyšší vrstvy, typicky IP) doplněná "vatou" na minimální délku 46 bajtů.

Nakonec CRC, kontrolní součet, číslo vypočtené na straně odesílatele i příjemce, následně porovnáno - při neshodě jako by rámec nebyl - vyšší vrstva musí výpadek ošetřit opakováním.

5.3.4 Adresy

K tomu, aby bylo možné uzel v síti jednoznačně identifikovat, je potřeba přidělit mu určité označení. Takovéto označení, tzv. MAC adresa, musí být především jednoznačná v rámci sítě, která umožňuje přímou komunikaci počítačů. V rámci sítí po celém světě, které mohou být navzájem propojeny, by neměla nastat situace, kdy se vyskytnou dva či větší počet počítačů se shodnými adresami.

Pokud by se vyskytly počítače se stejnými MAC adresami v různých, navzájem oddělených sítích, problém by nevznikl. Komplikace by nastaly při duplicitě MAC adres v rámci jedné sítě, ovšem vzhledem k tomu, že uživatelé mohou svůj počítač přenést a připojit do jiné sítě, je lepší jednoznačnost adres dodržet v rámci celého světa. Nejjednodušší z hlediska používání a zpracování je použití čísla ve dvojkové soustavě uložené v paměti přímo na desce síťové karty.

Adresa převzatá z MAC rámce může být velmi jednoduše porovnána s adresou uloženou v paměti adaptéru, a může tak být rozhodnuto, zda přijatý rámec je určen danému uzlu či nikoli.

Jednoznačnosti pak je dosaženo tím, že MAC adresa je uložena již při výrobě pevně do paměti síťového adaptéru, přičemž každému adaptéru je přidělena adresa odlišná od adres všech ostatních vyrobených adaptérů.

MAC adresa začíná částí přidělenou výrobcí (může se jednat například o první tři bajty) s dále doplněným pořadovými číslicemi při výrobě. O přidělování kódů výrobcům se jménem ISO stará organizace IEEE.

Rozdělení MAC adresy na dvě části zajišťuje jednoznačnost MAC adresy každého adaptéru, délka adresy 48 b pak zaručuje, že adresový prostor je obrovský, neboť počet přidělitelných adres dosahuje zhruba téměř tří trilionů (přibližně jedna adresa na dva čtverečné kilometry zemského povrchu). Díky způsobu přidělování adres však nejde o nevyčerpatelný zdroj, již nyní existují odhady, kdy dojde k jejich vyčerpání.

Jednotlivé 8 bitové části MAC adresy jsou obvykle uváděny jako dvojice hexadecimálních číslic. Zápis 48 bitové adresy v binárním formátu (pomocí nul a jedniček) je zbytečně dlouhý, a proto se MAC adresy vyjadřují pomocí hexadecimálních číslic. Vždy jedna 4 bitová část je převedena na hexadecimální číslo.

Příklad zápisu: 09-A1-28-A0-D8-F3.

5.3.5 Kolizní okénko

Je limitujícím faktorem nepřepínaného Ethernetu. Informace se po mediu (kovový elektrický vodič, optické vlákno) šíří konečnou rychlostí ($0,5c$ až $0,9c$, c =maximální rychlost 299 792 458 metr/sec).

Může tedy nastat situace, že počítač 1 (na obrázku) začne vysílat na společné volné medium informaci pro počítač 2. Za velmi krátkou dobu nebo dokonce ve stejný okamžik začne vysílat též počítač 3, který úspěšně detekoval volné medium (signál z počítače 1 ještě k němu nedoletěl).

Pokud síť splňuje maximální rozměry počítač 1 i počítač 3 detekují během svého vysílání kolizi. Vyčkají náhodně dlouho dobu a celý proces opakují (až se „zadaří“).

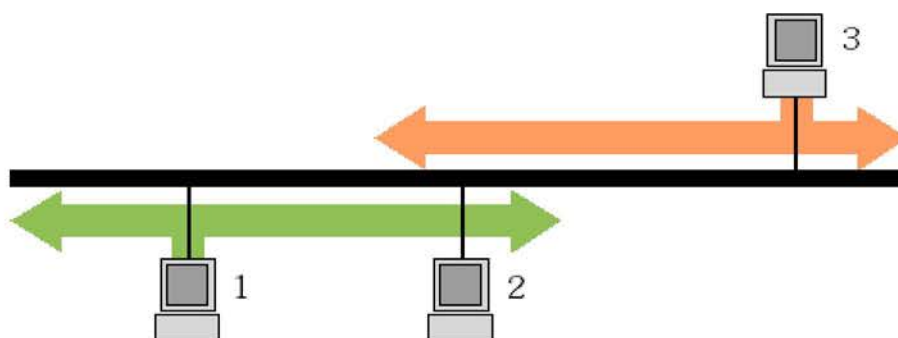
Pokud síť ovšem přesahuje maximální normou definované rozměry v jedné kolizní doméně hrozí, že počítač 1 i počítač 3 ukončí vysílání bez detekce kolize.

Signál bude kolidovat v místě počítače 2, který rámec zahodí, protože nebude souhlasit CRC. Síť tak bude vykazovat velmi časté ztráty datových rámců.

Podmínka kolizního okénka: **čas obsazení média < čas vysílání nejkratšího rámce**, jinak hrozí neobjevené kolize.

Nepřekonatelnost kolizního okénka - problém se zrychlováním sítí.

Nutnost jiného řízení provozu tj. přepínání v kancelářském Ethernetu nebo komunikace master-slave v průmyslovém Ethernetu.



Obrázek 5.12 – Kolizní okénko v síti ethernet s CSMA/CD

5.3.6 Důsledky CSMA/CD

Každá kolize znamená určitý promarněný čas (data jsou poškozena, přenos se musí opakovat).

V době největšího zájmu přibývá kolizí a efektivita využití media klesá.

5.4 Hub versus switch, routery

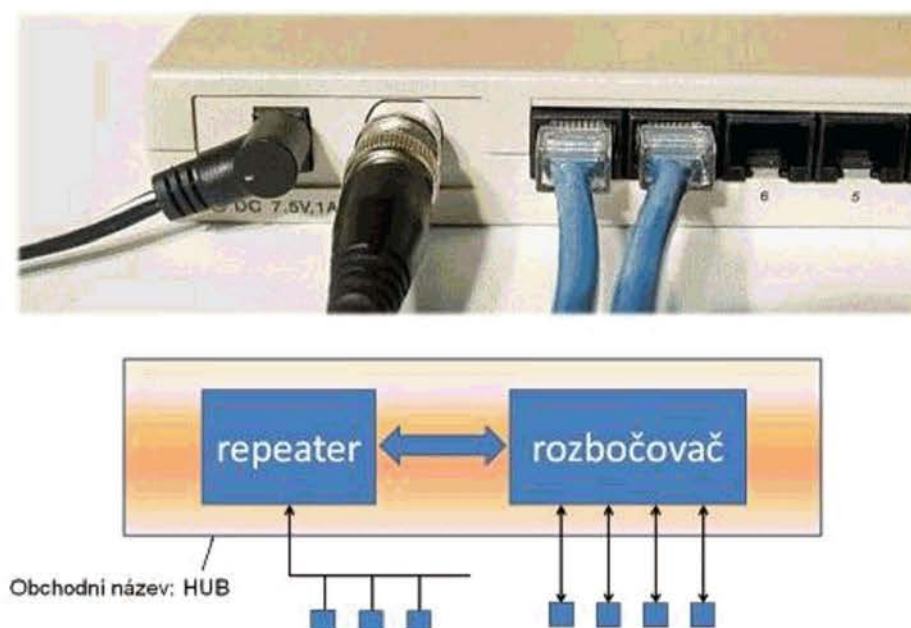
5.4.1 Hub (rozbočovač)

Vzešel z původního repeateru (opakovače) při přechodu Ethernetu z koaxiálního kabelu na kroucenou dvojlinku. Na obrázku je zobrazeno klasické kombinované provedení.

Skutečný Hub je pouhý zesilovač signálu, regeneruje signál zpět na čitelnou „0“ a „1“, jak mile rozliší 0 a 1 posílá dál na všechny porty (není schopen propojovat prvky z odlišnou přenosovou rychlostí).

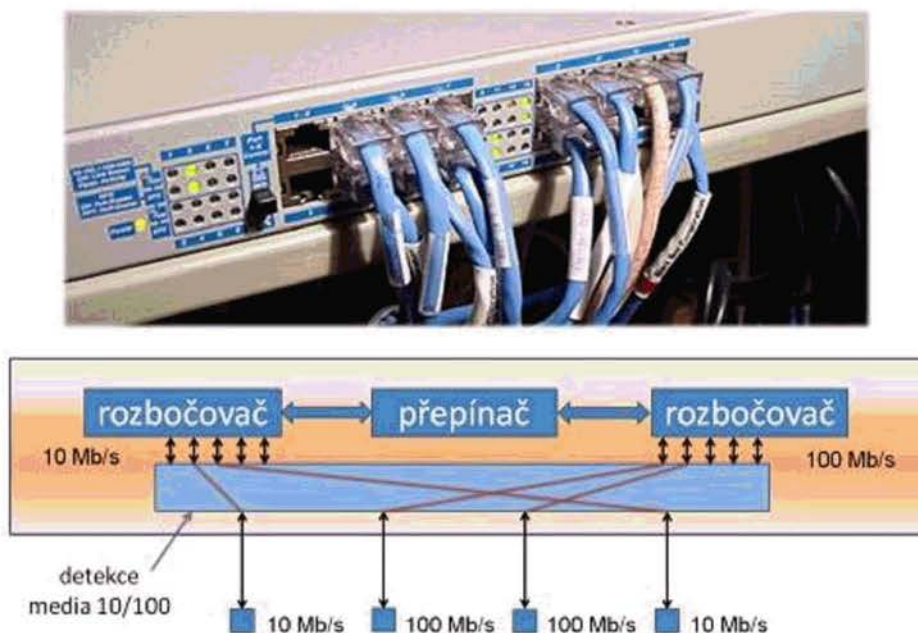
Je základní komponentou v současném průmyslovém Ethernetu, z kanceláří byl postupně vytlačen přepínači (Switch).

Pod názvem Hub (nebo i Switch) bývají často prodávána kombinovaná zařízení. Princip jednoho kombinovaného zařízení (vytvářející jednu jedinou kolizní doménu) je patrný na obrázku 5.13.



Obrázek 5.13 – Ethernet Hub s opakovačem

Další takové zařízení je na obrázku 5.14, vytváří dvě kolizní domény oddělené přepínačem.



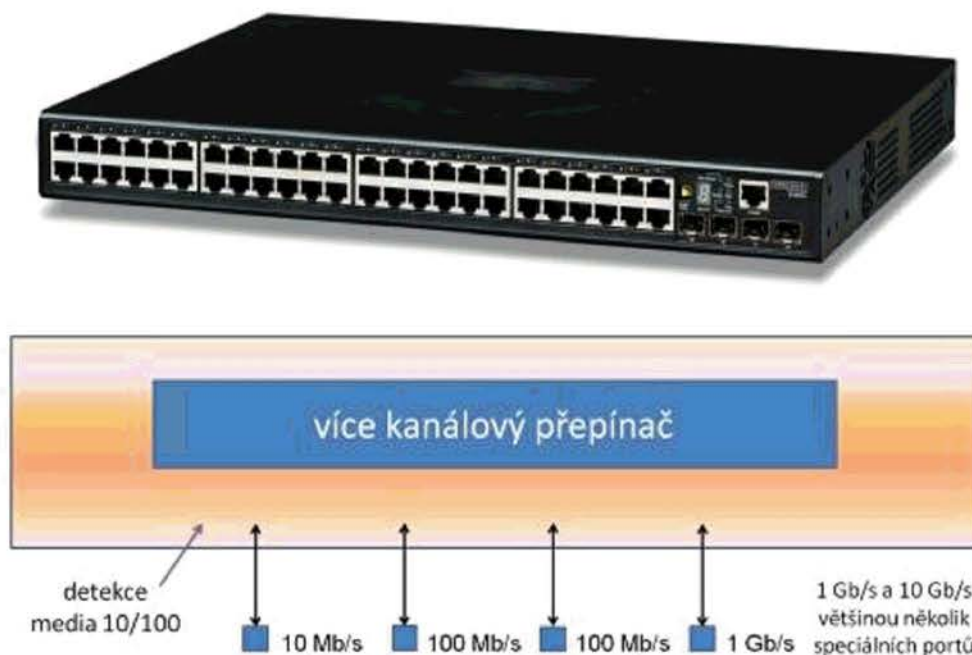
Obrázek 5.14 – Ethernet Hub s přepínačem

5.4.2 Switch (přepínač)

Podstatně složitější zařízení z automatickou konfigurací umožňující spojovat zařízení z různou přenosovou rychlostí (viz. obrázek obrázek 5.15). Z adres odesílatele se postupně dozví „kde kdo sedí“.

Rámce určené pro zatím neznámého adresáta pošle všem (pravděpodobně se v zápětí z odpovědi dozví, kde je).

Problém s cykly a redundancí v síti, běžné Switche nepřipouští redundanci, topologie musí být hvězdou nebo stromem, obecný graf je nepřipustný.



Obrázek 5.15 – Ethernet Switch

Složitější přístroje pro rozsáhlé LAN umožňují redundanci přeci jen obsluhovat technikou „spanning tree“. Redundantní spoje deaktivuje a v obecném grafu si vyznačí strom, při výpadcích obnovuje deaktivované linky. Praxe ukazuje problémy a nekompatibility mezi různými výrobci. Více též v odstavci Přepínaný Ethernet, rychlý Ethernet.

5.4.3 Bridge (most, media konvertor)

Jedná se o předchůdce Switche, má dva nebo jen několik málo portů. V podstatě plní dvě funkce - filtruje rámce a propojuje dvě různé sítě - segmenty sítě (dříve kolizní domény).

Většinou se jedná o sítě se stejnou strukturou paketů v linkové vrstvě, tedy buď Ethernet nebo Token Ring, nebo dnes bezdrátové sítě WiFi. Takovéto mosty se nazývají homogenní.

Je to aktivní prvek, který dokáže rozlišit, zda data zůstanou v segmentu, ze kterého byla vyslána, nebo zda se mají převést do dalšího segmentu sítě. Mosty používáme v případě, že chceme spojit dvě, anebo více sítí LAN, prodloužit délku segmentu (příp. zvýšit počet připojených stanic) nebo chceme snížit zatížení sítě.

Most musí znát své nejbližší okolí, a proto si udržuje tabulku adres připojených stanic. Dnes se pro vytváření a aktualizaci tabulky adres používá téměř výhradně tzv. „samoučení“ - switch (most) vytváří si tabulku postupně sám na základě realizovaných propojení. Jde o nejčastější případ.

Most je schopen fungovat i tehdy, když tyto informace nebude mít k dispozici. Pak bude fungovat podobně jako opakovač, a rozešle každý přijatý rámec na všechny strany - tím přenos nebude efektivní, ale na krátkou dobu to lze připustit. Toho se využívá během procesu učení.

Mosty v původním pojetí jsou dnes vytlačeny přepínači. Pod pojmem most spíše dnes rozumíme konverzi mezi technologiemi (například Ethernet a Wi-Fi nebo Ethernet a DSL).

5.4.4 Router (směrovač)

Podobně jako Bridge spojuje Router dvě nebo několik málo sítí. Přenos informací mezi sítěmi je však realizován na vyšší vrstvě (typicky na IP).

Směrovač vystupuje v obou sítích jako počítač s odlišnou IP adresou i MAC adresou.

Směrovač musí znát skutečnou topologii celé sítě (resp. všech propojených sítí). Objem potřebných informací je výrazně větší než u linkové vrstvy.

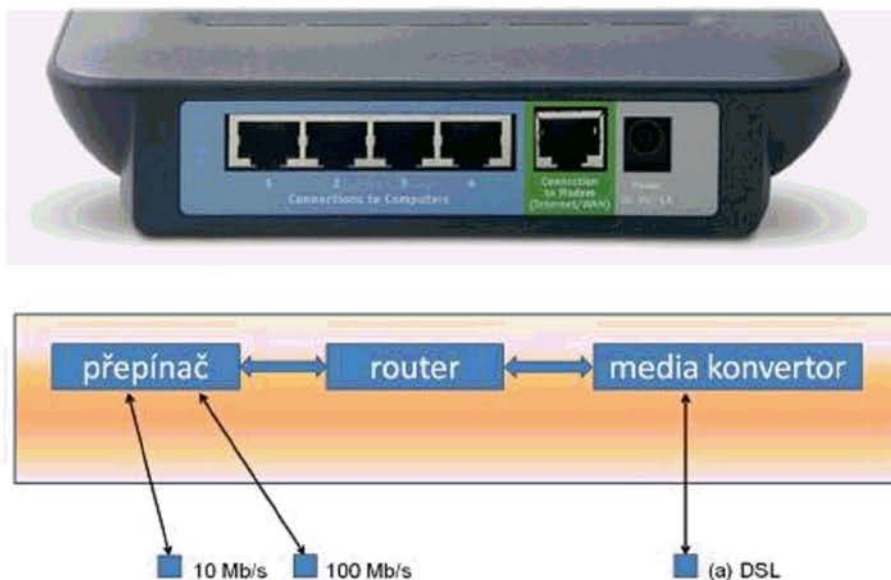
Úkolem směrovače je vybrat vhodnou cestu pro posílaný rámec ze síťového uzlu na uzel jiné sítě, při čemž obě sítě mohou být odděleny několika jinými sítěmi, příp. velkou vzdáleností.

Má v sobě zabudovanou filtraci paketů rozšířenou o inteligentní směrování s využitím IP adres.

Směrovač je závislý na použitém protokolu síťové vrstvy. Směrovač může propojovat sítě různých architektur (Ethernet, Wi-Fi FDDI, Token Ring,...).

Směrovače jsou typickým prvkem rozsáhlých sítí WAN, ale používají se i v sítích LAN, kde se používají např. pro připojení lokální sítě k Internetu.

Router je záležitostí profesionálních aplikací, ale pod názvem Router jsou dnes běžně dostupné právě kombinované přístroje pro malé firmy a domácnosti (obrázek 5.16).



Obrázek 5.16 – Router s integrovaným přepínačem a mostem

Takový Router zpravidla realizuje nejen směrování, ale přiděluje neveřejné IP adresy ve vnitřní lokální síti, lepší kousky umožňují filtrování a zabezpečení. Výhodou je především integrovaný media konvertor na DSL nebo GSM a 3G modem.

Jedná se většinou o přístroje s relativně malým výkonem, který sotva dostačuje na zpracování přenosu rámců na dnes nabízené připojení v řádech desítek Mbitů. Některé uživatelky ocení například vzhled přístroje, tak aby ladil například s notebookem – viz. obrázek ☺.



Obrázek 5.17 – Malý GSM router na cesty

5.4.5 Gateway (brána)

Mosty, switche a směrovače se nezajímají o datový obsah rámců resp. paketů. Jejich zájem o data zpravidla končí u adres. Mohou propojovat jen takové systémy, které do rámců/paketů „balí“ stejná data tj. stejné systémy, eventuálně systémy lišící se v přenosových technologiích nižších vrstev.

Pro spolupráci odlišných systémů je nutné rozumět přenášeným datům a provádět jejich konverzi. To je úkolem bran (gateways), brány jsou vždy aplikačně orientované, rozumí jen datům od určité aplikace, pracují tedy na aplikační vrstvě. Slouží k připojení počítačové sítě k jiné síti, k nějakému cizímu prostředí. Brány jsou realizovány softwarově a jsou vždy aplikačně orientované, např. brána pro přenos elektronické pošty, pro tisk atd. Brány jsou nutné pro spolupráci odlišných systémů.

5.5 Přepínaný Ethernet, rychlý Ethernet

5.5.1 Přístup k mediu v dnešním přepínaném Ethernetu

Ethernet má za sebou významný mezník ve svém vývoji, od kolizních domén s algoritmem CSMA/CD dospěl k přepínané síti vyžadující centrální prvky.

Stanice vysílá a přijímá rámce podle požadavků vyšších vrstev. Přepínač co by protějšek každému síťovému adapteru zajišťuje směrování podle adres fyzické vrstvy - MAC. Nemá-li informaci, na kterém portu se nachází cílový počítač s konkrétní adresou, pošle rámec všem, při první odpovědi se "poučí", tj. doplní svou směrovací tabulku.

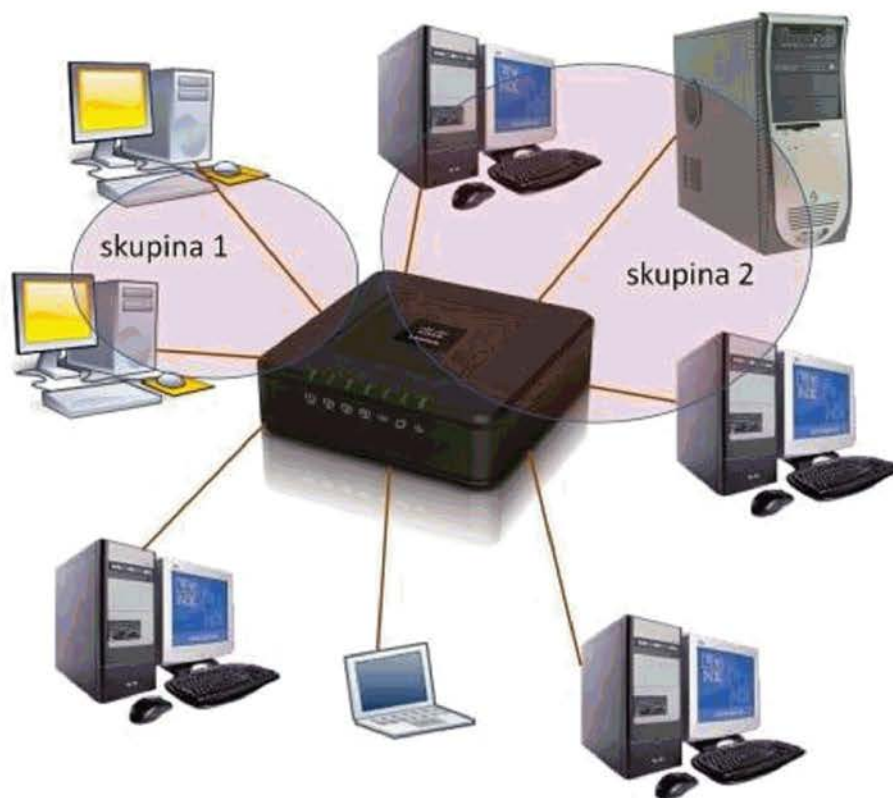
Přepínače se liší svými algoritmy pro směrování. Nejjednodušší verze přepínače „store and forward“ každý rámec uloží, poté najde cíl a potom jej pošle rámec na daný port, případně v kombinované síti jej prosadí pomocí algoritmu CSMA/CD do příslušné kolizní domény. Každý přepínač může tedy stále fungovat jako vícekanálový most mezi kolizními doménami (použijeme-li kombinaci přepínačů a rozbočovačů).

Přepínače pro velké sítě pracují efektivněji a datový rámec začnou preposílat hned jak obdrží preambuli a hlavičku s MAC adresáta. Další funkce přepínačů se orientují na zabezpečení (zámky portů pro konkrétní MAC, filtrování rámců podle obsahu datového balíčku vyšší vrstvy - typicky IP, VLAN funkce atp).

Obecně může platit, že síť založená na přepínaném Ethernetu vykazuje vyšší propustnost. Na obrázku 5.18 je naznačena situace, kdy dvě skupiny počítačů komunikují intenzivně především mezi sebou.

Přepínač tak obslouží tyto skupiny tak, že součet Mb/s může významně přesáhnout jmenovitou rychlost (například 100Mb/s).

V případě, kdy by byl použit rozbočovač by naopak vlivem kolizí došlo k přenosu s efektivní rychlostí nižší než jmenovitá rychlost.



Obrázek 5.18 – Router s integrovaným přepínačem a mostem

Současně platí, že pokud budou všechny počítače komunikovat výhradně s jedním strojem (například se směrovačem zprostředkujícím přístup do celosvětové sítě, což je obvyklá situace) nasazení přepínače nic zásadního nepřinese, v případě, že přepínač bude jednoduchého typu „store and forward“ lze čekat i horší výsledek!

5.5.2 Plně duplexní provoz (full duplex)

Sestavíme-li síť pouze s přepínačů, mizí sdílení media, každý účastník může ihned vysílat a nemusí během vysílání současně naslouchat za účelem detekování kolize, resp. na kroucené dvojlince, kde je připojen k přepínači ani nemůže, protože přepínač posílá data jen příjemci, tedy ani zpět odesílateli jako rozbočovač. Přijímač odesílajícího účastníka tedy volný a může fungovat zcela nezávisle a přijímat jiná data v jeden okamžik (CSMA/CD je zcela vyřazen).

V současnosti všechny Ethernet rozhraní režim full duplex podporují a režim je zpravidla rozhraním detekován automaticky.

5.5.3 Fast Ethernet

Tento standard je označován 100BaseX a platí pro něj stejná pravidla jako v původním Ethernetu 10BaseT.

Přístup ke společnému mediu (pokud je společné a nepřepínané) je řízen metodou přenosu dat CSMA/CD.

Stejný formát rámce a adres MAC, shodná logika - software vyšších vrstev beze změn.

Definován IEEE 8023u (1995).

Stejné medium - kroucená dvojlinka nebo optika. Mizí pouze možnost používat koaxiál.

Odlišnosti od původního Ethernetu:

- 10x rychlejší přenos dat (100Mb/s) a jako důsledek 10x menší rozměr kolizní domény.
- Maximální rozměr sítě na kroucené dvojlince je 220 metrů (100m+10m+10m+100m), počítáno je tedy se dvěma rozbočovači (norma připouští i tři, při snížení dosahu).
- Optický segment nesmí být delší než 412 metrů.

Media pro Fast Ethernet:

- 100BASE-TX - 2 pary UTP kategorie 5.
- 100BASE-T4 - 4 pary UTP kategorie 3, 4, 5, 5e, 6.
- 100BASE-FX - optické vlákno.

5.5.4 Gigabitový Ethernet

Definován IEEE 802.3z (optika), IEEE 802.3ab (UTP) - 1998.

Rychlost 1 Gb/s, stejný formát rámců i CSMA/CD (spíše symbolicky, používá se full duplex).

Gigabitový Ethernet lze chápat jako reakci na neustále rostoucí nároky soudobých aplikací, které mají čím dál tím větší požadavky na přenos dat.

Gigabitový Ethernet není jen desetinásobným „nafouknutím“ něčeho již existujícího - je řešením, které si vytváří dostatek výkonu k tomu, aby mohlo následně vyjít vstříc i specifickým potřebách v oblasti garance kvality služeb. Na druhé straně je gigabitový Ethernet řešením, které opět důsledně staví na kompatibilitě se stávajícími verzemi Ethernetu.

Media pro Gigabitový Ethernet:

- 1000BASE-TX - pro kroucenou dvojlinku kategorie 5 (UTP i STP), s použitím čtyř párů, délka 25m, délka 100m.
- 1000BASE-SX - pro vícevidové optické kabely 50 mikrometru, délka 200m.
- 1000BASE-SX - pro vícevidové optické kabely 62,5 mikrometru, délka 500m.
- 1000BASE-LX - pro vícevidové optické kabely 1300 nm - 500m.

- 1000BASE-LX - pro jednovidové optické kabely 1300 nm - 2 km (až 5 km).
- 1000BASE-CX - koaxiální kabel STP (twinax) - délka 25 m.

5.5.5 Desetigigabitový Ethernet

Opět zachovává formát rámce, mizí CSMA/CD - komunikace vždy plně duplexní.

Definován IEEE 802.3ae (2002).

Především optická vlána a laser (i pro vícevidová), pokud UTP, tak kategorie 7.

Media pro Desetidigabitový Ethernet:

- 10GBASE - vícevidové vlákno 62,5 micrometru - 30 m (speciální provedení až 300 m).
- 10GBASE - jednovidové 10 km (40 km).

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

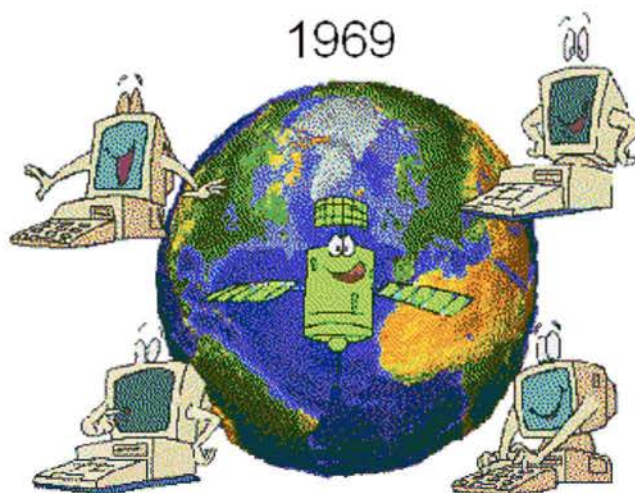
Registrační číslo: CZ.1.07/2.2.00/28.0118

6 Internet

6.1 Vznik internetu

V roce 1958 byla založena grantová agentura (Defense) Advanced Research Projects Agency - (D)ARPA s cílem podpořit malé týmy vědců v rámci obnovení vedoucího technologického postavení USA, které nebylo v té době částečně ve stínu úspěchů v SSSR (vypuštění Sputniku).

V rámci podpořeného projektu ARPANET byla dne 29.10.1969 spuštěna první počítačová síť, která propojila čtyři velké počítače univerzit v různých státech USA a to decentralizovaným způsobem, kde jsou jednotlivé uzly rovny a nevniká snadno zničitelné centrum.



6.1 – Vznik internetu

6.2 Historie internetu

- **1962** - podpořen projekt ARPANET grantovou agenturou ARPA - realizace decentralizované sítě.
- **1969** - ARPANET uvedena do provozu (čtyři uzly)
- viz. obrázek 6.1 ☺
- **1972** - ARPANET rozšířena na cca 20 směrovačů a 50 počítačů, použit Network Control Program (NCP).
- **1972** - Ray Tomlinson vyvíjí první e-mailový program (snaha od začátku využít síť pro komunikaci mezi lidmi).
- **1973** - začátek přípravy nového protokolu TCP/IP jako náhrady za stávající protokol NCP.
- **1979** - experimentální provoz IPv4 tak, jak je používán ještě dnes (1980 vydáno RFC 791).
- **1983** - Unix verze 4.2 podporuje již jen TCP/IP v4, z ARPANETu oddělena síť MILNET (Military Network), vznik Domain Name System (DNS), první komerční aplikace od SUN, internet má již téměř 1000 uzlů.
- **1984** - překročeno 1000 uzlů, zavedeno DNS (vyvinut program BIND pro DNS).
- **1987** - překročeno 10 000 uzlů, vzniká pojem „Internet“.
- **1989** - překročeno 100 000 uzlů, vědec ze švýcarského CERN Tim Berners-Lee publikuje návrh vývoje WWW (Information Management: A Proposal).
- **1990** - končí ARPANET, Tim Berners-Lee a Robert Cailliau publikují koncept hypertextu.
- **1991** - nasazení WWW v evropské laboratoři CERN (nástěnka vědců).

- **1992** - překročen 1 milion uzlů, připojen Bílý dům (vstup vládních institucí na Internet), oficiálně připojena Česká republika (13. února připojeno ČVUT v Pražských Dejvicích).
- **1993** - vznik akademické sítě CESNET, Marc Andreessen vyvíjí nekomerčně první WWW prohlížeč Mosaic.
- **1994** - internet se celkově komercializuje, vyvinut prohlížeč Netscape Navigator.
- **1996** - 10 mil. uzlů, 500 tis. www serverů, Ivo Lukačovič zakládá internetový portál Seznam.cz.
- **1997** - české projekty TEN-34 a TEN-34CZ (34Mb/s).
- **1998** - projekt TEN-155.
- **1999** - rozšiřuje se Napster.
- **2000** - 100 mil. uzlů, 250 milionů uživatelů, první 2,5Gb/s v ČR.
- **2001** - GEANT (10 Gb/s) a CESNET2 (2,5 Gb/s).
- **2005** - 900 milionů uživatelů, slovo internet se v čechách začíná psát malým písmenem.
- **2010** - přes 2 miliardy uživatelů, ve Finsku jako první zemi na světě mají lidé podle zákona nárok na internet.
- **2007** - ustavena pracovní skupina pracovní verze HTML5
- **2011** - došlo k vyčerpání adres IPv4 na globální úrovni - IANA (Internet Assigned Numbers Authority) přidělila poslední dvě volné IP/8 (predikce vyčerpání počítala až s únorem 2012), zvolen mezinárodní den IPv6 - 8. června.
- **2012** - HTML5 specifikace ve fázi „Candidate Recommendation“
- **2013** - nedostatek adres IPv4 na straně RIR (Regional Internet Registry), jednotlivé RIR pracují s posledními přidělenými IP/8. Skutečný nedostatek adres odhadován na rok 2020.

6.3 Standartizace internetu

Založena na dokumentech RFC - Request For Comments (žádost o komentáře). Přestože se nejedná o klasické normy, popisují internetové protokoly a řídí se podle nich drtivá většina internetu.

Jednotlivé RFC dokumenty vydává editor RFC podle příkazů Internet Architecture Board. Každé RFC má při zveřejnění přiděleno číslo. Vydané RFC se nikdy neruší, pouze se v budoucnu může upravit vydáním novějšího RFC. Celkem je dokumentů již přes 4000.

Podávat návrh RFC mohou vybrané organizace, ale je možné i nezávislé podání. Samotný proces schvalování dokumentů před publikací je poměrně komplikovaný a liší se jednak dle zdroje dokumentu a jednak dle jejich kategorie.

6.3.1 Typický navrhovatel RFC - Internet Engineering Task Force (IETF)

- Velká komunita návrhářů, provozovatelů, výzkumníků.
- Účast dobrovolná, organizována do tématických pracovních skupin.
- Vyvíjí nové protokoly, služby atp.
- Pracovní dokument (draft) má platnost ½ roku.

6.3.2 Vydané RFC mají přidělen stav

- **Proposed standard:** návrh (ustálené, bez implementace).
- **Draft standard:** alespoň 2 nezávislé implementace, dostatek zkušeností s provozem.
- **Internet standard:** zralé, stabilní.
- **Experimental:** zkoumá se.
- **Informational:** čistě pro informaci uživatelů.
- **Historic:** nahrazeno novějším dokumentem.

6.3.3 RFC a klasické standardizační autority (ISO, ANSI)

- Na rozdíl od klasických norem a standardů vydávaných klasickými normotvornými institucemi (jako např. ISO, ANSI apod.) vznikají RFC poněkud jiným způsobem.
- Původními autory jednotlivých RFC jsou obvykle konkrétní experti, kteří se snaží řešit konkrétní problém, jehož řešení nabídnou ve formě návrhu RFC internetové veřejnosti (jako tzv. Internet Draft).
- Pokud je dané řešení (často již dobře fungující v rámci nějakého pilotního provozu) uznáno za přínosné, dokument se vydá jako RFC.
- Toto pragmatické řešení standardů sestavovaných jednotlivci či malými skupinami na základě praktických zkušeností má mnohé výhody oproti formálnějším procesům standardizačních komisí u úřadů typu ISO.
- Standardy vytvořené pomocí RFC jsou (vzhledem k neexistenci jakékoli skutečné moci na jejich vynucování) až na výjimky dodržovány, přičemž pomohly rozšíření internetu do dnešních celosvětových rozměrů.
- Ve srovnání s klasickými standardizačními autoritami je proces s RFC méně formální, je například radiční vydávat na apríla žertovný očíslovaný dokument. Samotný proces tvorby je zdokumentován v RFC 2026.

6.4 Internet protokol

Internet Protokol je základní protokol síťové vrstvy a celého internetu. Provádí vysílání datagramů kde směr je řízen IP adresami obsaženými v jejich záhlaví.

Poskytuje vyšším vrstvám síťovou službu bez vyhrazeného spojení. Každý datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesilateli a pořadovém čísle datagramu ve zprávě.

Datagramy putují sítí nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě, síť s topologií „obecný graf“ nezaručuje, že jednotlivé datagramy budou putovat stejnou cestou.

Doručení datagramu není zaručeno, spolehlivost musí zajistit vyšší vrstvy (TCP spojení nebo samotná aplikace).

Tento protokol se dále stará o segmentaci a znovusestavení datagramů do a z rámců podle protokolu nižší vrstvy (např. Ethernet).

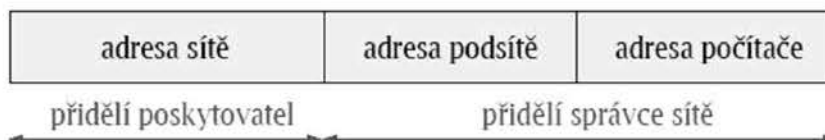
V současné době používán protokol IP verze 6 a IP verze 4.

6.4.1 RFC 791 a RFC 2460

- Drží internet pohromadě - podpora jednotného IP, hlava rodiny TCP/IP (IPv4, dnes IPv6).
- Umožňuje kterémukoli zařízení komunikovat s ostatními.
- Bez spojení (samostatné datagramy).
- Bez záruk (best effort).

6.4.2 IP adresy

- Každé rozhraní má svou adresu.
- Při použití IPv4 32bitové číslo ($2^{32} = 4\,294\,967\,296$), cca 4 miliardy různých IP adres (v osmdesátých letech minulého století při vzniku internetu velká rezerva, současné době nedostatečný počet).
- Při použití IPv6 128 bitové číslo ($2^{128} \approx 3,4 \times 10^{38}$), cca $6,7 \times 10^{23}$ IP adres na 1 m² zemského povrchu.
- Hexadecimální zápis
2001:0587:2d03:0115:0391:00ff:5ce8:0a15 (IPv6), dříve tečkovaný desítkový zápis např. 195.211.105.5 (IPv4).
- Celosvětově jednoznačné, distribuované přidělování.
- Zhledem k tomu, že první 64bitová i druhá 64 bitová část jsou samy o sobě jednoznačné (viz. odstavec Podsítě, tabulka) je vlastně adres 2⁶⁴, tj. $1,8 \times 10^{19}$ a **na jeden 1m² zemského povrchu připadá „pouze“ 36 165 adres ☺**.
- Internet není síť počítačů s IP adresami, ale síť sítí (adresy mají hierarchickou strukturu).



6.2 – obecná hierarchická struktura IP adres

6.4.3 Přidělování adres od centrální autority až směrem k zákazníkovi

- Centrální autorita - IANA (Internet Assigned Numbers Authority).
- Regionální autorita - RIR (Regional Internet Registry) - RIPE NCC (Evropa a blízký východ), ARIN (Severní Amerika), LACNIC (Latinská Amerika), APNIC (Asie a Pacifik), AFRINIC (Afrika).
- Lokální poskytovatel internetu - LIR (Local Internet Registry)

- Zákazník, spravuje adresu podsítě a připojuje zařízení s adresou rozhraní (výsledná adresa je 128 bitů dle obrázku 6.3)

| 16 bitů | 16 bitů | 16 bitů | 16 bitů | 64 bitů |
|----------------|---------------|---------------|----------------|-----------------|
| přiděluje IANA | přiděluje RIR | přiděluje LIR | adresa podsítě | adresa rozhraní |

6.3 – Přidělování adres od centrální autority - struktura IPv6 adresy

6.4.4 Prefix

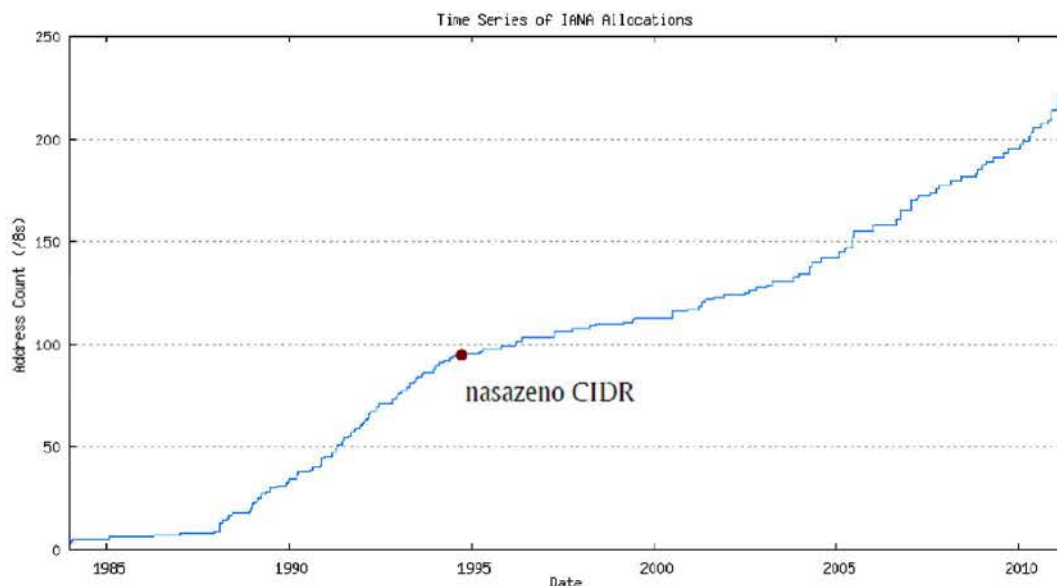
- Prefix je začátek IP adresy.
- Délka může být různá, zápis s lomítkem - odděluje hodnotu adresy od specifikace významných bitů.
- Zápis s rozměrem prefixu: 160.218.0.0/16 - kolik bitů od začátku adresy platí
- Zápis s maskou: 160.218.0.0/255.255.0.0 - maska, 11...1 na místě významných bitů, 00...0 na místě nevýznamných bitů.
- Část adresy, jež není součástí prefixu, bývá vynulována
- Prefix používá se při přidělování adres, směrování, ...

6.4.5 Podsítě

- Počítače přímo spojené ve 2. vrstvě (Ethernetem), počítače ve stejné podsíti spolu komunikují přímo.
- Masku podsítě určuje hranici mezi adresou podsítě a počítače. Obsahuje 1 v bitech adresy sítě a podsítě, 0 jinde.
- 160.218.14.153 s maskou podsítě 255.255.255.0. Síť 160.218, podsítě 14, počítač 153, hranici stanoví správce sítě. V IPv6 je adresa počítače sestavena z MAC, podsítě je zpravidla 16-ti bitové číslo.

6.4.6 Beztržní adresování a směrování

- Classless Internet Domain Routing (CIDR) definován RFC 1517, RFC 1518, RFC 1519 a RFC 1520.
- V roce 1995 zaveden s cílem šetřit adresy IPv4, sítě dostaly jen tolik prostoru, kolik opravdu potřebovaly. V IPv6 nepotřebné (zatím ☺).
- Původně byly 3 délky adresy sítě - třídy A/8, B/16, C/24 neosvědčilo se - málo adres třídy B, velké směrovací tabulky, plýtvání adresami, proto vzniklo CIDR.
- Založeno na sdílení prefixů, ISP dostane prefix, např. 160.218.0.0/16, jeho části (např. 160.218.1.0/24) přiděluje zákazníkům, mimo síť ISP lze celý jeho prostor shrnout pod jediný prefix 160.218.1/16.
- Podsítě není nutno nastavovat „po bajtech“ masku lze volit libovolně (např. maska 255.255.248.0 umožní podsít pro 2048 tis. počítačů a není nutno volit mezi 256 a 65536).
- Efekt CIDR byl významný, společně s NAT odložil okamžik vyčerpání adres IPv4 o deset let.



6.4 – Alokace adres IPv4

6.4.7 Neveřejné adresy

- RFC 1918 definovalo adresy pro soukromé sítě (10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16), další způsob jak šetřit adresy v IPv4.
- Nejsou směrovány v internetu, nesmí překročit lokální síť.
- Dnes využívány pro rozšíření adresního prostoru v kombinaci s NAT.

6.4.8 Překladač neveřejných adres

- Network Address Translation (NAT), RFC 3022.
- Překládá adresy mezi dvěma částmi sítě, mění IP adresy a porty v procházejících IP datagramech.
- Typicky: lokální síť s neveřejnými adresami připojená NATem do internetu - celá síť je adresována jedinou veřejnou IP adresou.
- Běžně implementováno např. v ADSL modemech.
- Záznam v konverzní tabulce se vytváří, když počítač „zevnitř“ odesílá paket „ven“.
- Komunikaci nutno navazovat zevnitř - dokud není záznam v tabulce, jsou vnitřní počítače nedosažitelné (nemají veřejné adresy).
- Narušuje přímou komunikaci (videokonference, iptelefonie) - nutno přes prostředníka s veřejnou adresou.
- Omezení dostupnosti vnitřní sítě má pozitivní dopady na bezpečnost, dokonce IPv6, kde NAT není zapotřebí, musel nabídnout bezpečnostní náhradu (RFC 4864 - Local Network Protection for IPv6). Lze též použít stavový firewall, který ve výchozím nastavení vpustí dovnitř jen datagramy z adres, na něž nedávno odešel datagram z koncové sítě. Uživatelům v IPv6 se může po dřívější anonymitě za NAT v IPv4 "stýskat".

6.4.9 IP datagram

- Verze 4, 6.
- Délka hlavičky: ve 32bitových slovech (max. 60 B).
- TOS: Type of Service, požadavky na přepravu.
- Celková délka: max. 65 535 B.
- TTL: Time to Live, každý směrovač zmenší alespoň 1, při vynulování zahodí - ochrana proti zacyklení.
- Protokol: kterému protokolu 4. vrstvy patří data (TCP, UDP).
- CRC: nezahrnuje data (tuto pojistku plní nižší vrstvy).
- Zobrazeno na obrázku.

| | | | | |
|---------------------------------------|-------------------|----------|-------------------|-----------------|
| verze | délka hlavičky | TOS | celková délka [B] | |
| identifikátor | | | přízn. | posun fragmentu |
| TTL | | protokol | CRC hlavičky | |
| odesílatel (IP adresa) | | | | |
| adresát (IP adresa) | | | | |
| volby (nepovinné, proměnlivé složení) | | | | |
| data | | | | |

6.5 – Datagram TCP (paket)

6.4.10 Fragmentace

- IP protokol se fragmentací přizpůsobuje existující technologii nižší vrstvy.
- IP datagram může být významně větší než rámec (MTU, Maximum Transmission Unit) přenášený nižší vrstvou (typicky Ethernetem).
- Je-li datagram > MTU, bude rozdělen na fragmenty.
- Fragmentované datagramy mají všechny stejný identifikátor, posun fragmentu udává, na které pozici původního datagramu začínají data tohoto fragmentu.
- V příznacích mají všechny fragmenty kromě posledního nastaven „More Fragments“, je aktualizována celková délka.
- Fragmenty jsou samostatnými datagramy, přepravovány nezávisle, mohou být dále fragmentovány, skládá až příjemce datagramu.
- Mezi příznaky je i „Don't fragment“, který zakazuje datagram fragmentovat.
- MTU cesty - odesílatel se snaží najít co největší velikost, která nezpůsobí fragmentaci, která je sama osobně neefektivní (dnes reálně do rámce Ethernetu umístit jeden celý IP datagram).

6.5 Protokoly pro práci s fyzickou vrstvou

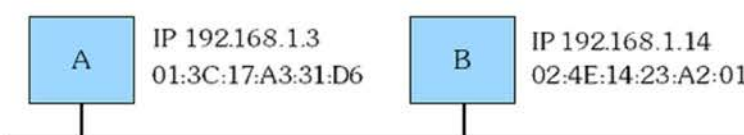
Síťová vrstva implementuje pomocné protokoly umožňující identifikaci chyb a vzájemné přiřazování IP adres fyzickým adresám.

V IPv6 dominuje objevování sousedů (Neighbor Discovery) pomocí sekvence několika ICMPv6 zpráv.

V IPv4 souvislost mezi fyzickou adresou MAC a IP adresou nebyla (IPadresa neobsahovala MAC), řešeno vysíláním všem (veřejný rámec, broadcast) s dotazem na přiřazení IP a MAC - ARP, viz. dále.

6.5.1 Address Resolution Protocol (ARP)

- Protokol zabezpečuje přiřazení IP adres fyzickým adresám linkové vrstvy. Vlastní komunikace v síti se uskutečňuje pomocí fyzických adres.
- Protokol má dvě základní funkce:
 - získání MAC adres odpovídajících cílovým IP adresám.
 - udržování tabulek přiřazení IP a MAC adres na každém z uzlů sítě.



A→všem: Kdo má IP 192.168.1.14? Já jsem IP 192.168.1.3, Eth 01:3C:17:A3:31:D6

všichni: zapíší do ARP cache údaje o A

B→A: Já jsem IP 192.168.1.14,
Eth 02:4E:14:23:A2:01

6.6 – Address Resolution Protocol (ARP)

- Postup:
 - Když IP protokol obdrží žádost o vyslání datagramu, získá z vyšší vrstvy IP adresu cílového uzlu, prohledá existující ARP tabulku.
 - Když cílová IP adresa v ní není uvedena, vyšle ARP Request, tj. veřejný rámec (broadcast) s žádostí o MAC adresu, která patří příslušné IP adrese.
 - Na tuto žádost odpoví ARP protokol uzlu s příslušnou logickou IP adresou, a to rámcem odpovědi (ARP Reply), která nese žádanou MAC adresu.
 - ARP protokol si pak aktualizuje ARP tabulku, současně tak učiní všichni nejbližší sousedé - typicky počítače v lokální síti (Ethernet). Mechanismus je zřejmý z obrázku 6.6.

6.5.2 Reverse Address Resolution Protocol (RARP)

- Protokol byl používán při znalosti fyzické adresy pro získání vlastní IP adresy. Nejčastěji pro zjištění vlastní IP adresy při startu systému (v případě bezdiskových stanic, které potřebují zjistit svoji IP adresu od serveru v síti).
- Stanice vygeneruje žádost RARP na všeobecnou adresu se svou fyzickou adresou a očekává odpověď s informací o přidělené IP adrese. RARP server obsahuje databázi hardwarových adres (MAC) s přiřazenými IP adresami. RARP žádost obsahuje vlastní hardwarovou adresu a RARP server vrací odpověď s vyplněnou korespondující IP adresou žadatele. Formát RARP zpráv je shodný s ARP.
- Vlastní IP adresa je nedostatečná informace pro plnou komunikaci stanice (chybí maska, brána, DNS, ...), proto je RARP dnes již nahrazen komplexnějšími protokoly z aplikační vrstvy (BootP nebo DHCP).

6.5.3 Internet Control Message Protocol (ICMP)

- Slouží na přenos chybových a řídicích zpráv mezi uzly a směrovači. Zprávy protokolu jsou přenášeny v přesně definované formě v datové části IP paketů.
- K funkcím protokolu ICMP patří:
 - Testování dostupnosti a stavu cílového uzlu sítě IP (Echo Request/Reply).
 - Řízení zahlcení sítě a toku paketů (Source quench).
 - Aktualizace směrovacích tabulek uzlů z IP směrovačů (Redirect).
 - Odeslání masky podsítě (Address mask request/Reply).

6.5.4 Internet Group Management Protocol (IGMP)

- Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti.
- Řeší i situaci, kdy jsou v síti připojeny dva a více multicastových routerů, protože pak by mohlo dojít v síti k šíření nadbytečných informací. Routery pracují ve dvou stavech. „dotazovač“, který zasílá dotazy na členství a „posluchač“, který pouze naslouchá a je neaktivní.
- Postup:
 - Stanice se pomocí zpráv „Membership report“ a „Leave group“ přihlašuje nebo odhlašuje do multicastové skupiny.
 - Zároveň však router zasílá periodický dotaz „General query“ ke stanicím v lokální síti, jestli je v ní alespoň jedna stanice, která chce ze skupiny informace odebírat.
 - Pokud mu žádná do 10 sekund neodpoví, vymaže z tabulky záznam o skupině. Tento dotaz řeší problém kdy se nějaká stanice, např. před vypnutím, nestihne z odběru skupiny odhlásit.

6.6 UDP komunikace, User Datagram Protocol

Definován RFC 768:

- Cílem je pouze adresovat aplikace, které si tak nezávisle mohou zasílat datagramy nezávisle jedna na druhé, je potom nepodstatné zda komunikující aplikace běží na jednom stroji nebo jsou to dva nejvzdálenější stroje na zemi.
- Datagramová služba bez záruk vyhovující řadě aplikací (DHCP, DNS, interaktivní - IP telefonie, ...). Každá aplikace každé na světě může poslat datagram (kromě NAT v IPv4 ..). Přesto UDP rotokolem je na síti přenášeno jen řádově 2 procenta dat.

- Adrese přidán port, tím je zjevněna adresace na úroveň aplikace (každá aplikace sleduje jen "svůj" port).

| | |
|------------------|------------------|
| port odesílatele | port příjemce |
| délka | kontrolní součet |

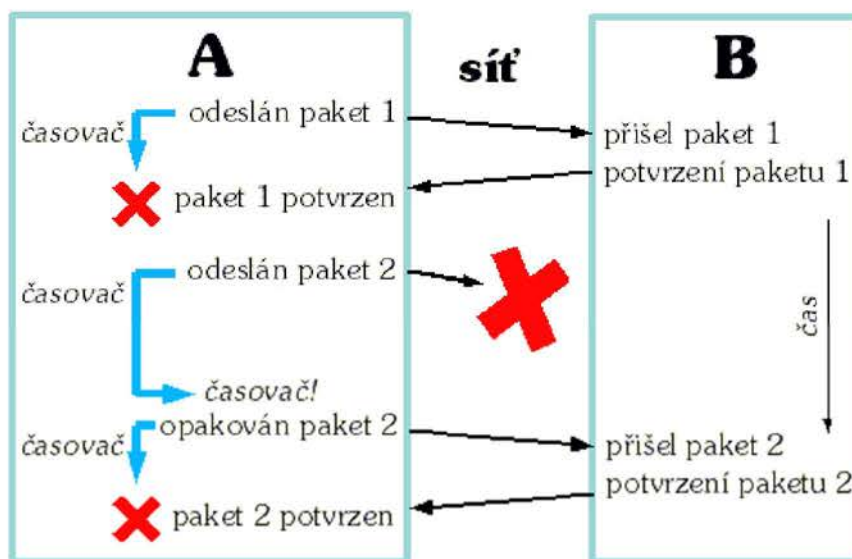
6.7 – Rozšíření datagramu (paketu) pro UDP

- 65 536 portů (na rozdíl od IP adres V4 bylo a je 16-ti bitové číslo nadčasové velké a není nutné jej měnit).
- Komunikující aplikace se připojí k portu (služba OS), kde naslouchají, přijímají a odesílají data. Při odesílání je nutné znát číslo portu dané aplikace, čísla portů obvyklých služeb jsou standardizovány (nezadá-li uživatel doplněn je standardní pro daného protokolu), klienti používají náhodná vyšší čísla portu. Porty 1-1023 jsou tzv. dobře známé, obvyklé (anglicky well known ports) a na Unixech a odvozených operačních systémech jsou potřeba práva uživatele root, aby je bylo možné použít. Porty 1024-49151 jsou registrované porty. Porty 49152-65535 jsou používány pro komunikaci klienta se serverem.
- Kvůli chybějícím zárukám se UDP aplikace musí smířit s nějakými ztrátami, chybami nebo duplikacemi. Některé aplikace (jako třeba TFTP) mohou podle potřeby přidávat jednoduchý mechanismus spolehlivosti do aplikační vrstvy. Aplikace používající UDP nejčastěji opravný mechanismus nepotřebují, a dokonce jím mohou být zdržovány (IP telefonie). Pokud aplikace vyžaduje vysoký stupeň spolehlivosti, může se místo něj použít TCP.
- Protože UDP postrádá mechanismus předcházení a regulace zahlcení sítě, je nutné nadbytečné UDP datagramy na routerech zahazovat. Jako částečné řešení tohoto problému je navrhován protokol DCCP (Datagram Congestion Control Protocol).

6.7 TCP komunikace, Transmission Control Protocol

Definován RFC 793:

- Spolehlivá přeprava, vyžaduje většina aplikací přenášející souvislá data (soubory).
- Protokol obsluhuje proud bitů bez struktury (bitová roura).
- Spojovaná služba, virtuální okruhy, spojení udržováno na koncích, pod ním nespojované IP (datagramy putující sítě nezávisle podobně jako UDP).
- Pomocí vyrovnávací paměti odesílatel a příjemce rozděluje/seskupuje data pro maximální efektivitu
- Přenos (bitová roura) plně duplexní spojení bez ohledu na fyzickou vrstvu (pokud fyzická vrstva pracuje v poloduplexním režimu (nepřepínaný Ethernet, Wi-Fi), jsou parametry přenosu mírně horší, ale aplikační vrstva pracuje shodným způsobem (pouze zadává data do bitové roury a čte příchozí data).



6.8 – Zajištění spolehlivosti při TCP komunikaci

6.7.1 Zajištění spolehlivosti

- Potvrzování řeší ztráty paketů, viz obrázek 6.8.
- TCP se vypořádá s přehozením paketů a duplikací na straně příjemce - pořadová čísla, TCP čísluje bajty (oktety).
- Protokol potvrzuje nejdelší souvislý prefix od začátku vysílání (posílá číslo bajtu, který očekává).
- Jednoduché, jednoznačné a optimalizované, ztráta potvrzení nemusí způsobit opakování.
- Nelze oznámit mezeru.
- Potvrzování není tak jednoduché jako na obrázku, nepotvrzuje se každý datagram a nepotvrzuje se hned, viz. dále.

6.7.2 Časování potvrzení

- Piggybacking - potvrzení se snaží přibalit k datům v protisměru.
- Čeká 200 ms, jestli se nevyskytne vhodný paket.
- Problém: jak nastavit časovač pro opakování.
- Příliš malý - bude se zbytečně opakovat.
- Příliš velký - výpadek bude objeven pozdě.
- Neexistuje univerzální hodnota, musí se přizpůsobovat chování sítě.

6.7.3 Nastavení časovače

- Vychází z průměrné doby odezvy (RTT) a průměrné odchylky (MD).
- Dorazí potvrzení se zpožděním M:
 - $\text{odchylka} = M - \text{RTT}$
 - $\text{RTT} = \text{RTT} + 0,125 \cdot \text{odchylka}$
 - $\text{MD} = \text{MD} + 0,25 \cdot (|\text{odchylka}| - \text{MD})$
 - $\text{časovač} = \text{RTT} + 4 \cdot \text{MD}$
- Opakovaným paketům časovač zdvojnásobí.
- Pro opakované nepočítá.

6.7.4 Okénko (Sliding window)

- Zvyšuje efektivitu - nemusí se čekat na potvrzení.
- Brání zahlcení pomalého příjemce.
- Smí vysílat jen po horní hranici okénka, pak čeká, viz. princip na obrázku 6.9.
- Velikost okénka určuje příjemce, nesmí však „couvnout“.
- Prázdné okénko - musí čekat, až je příjemce otevře.



6.9 – Posuvné okénko (Sliding window) při TCP komunikaci

6.7.5 TCP datagram, segment, TCP hlavička

- Délka hlavičky v IPv4 ve 32b slovech, obecně viz. obrázek 6.10.
- Příznaky:
 - URG - segment obsahuje urgentní data
 - ACK - obsahuje platné potvrzení
 - PSH - předat cílové aplikaci co nejrychleji (push)
 - RST - náhlé ukončení spojení (reset)
 - SYN - zahájení spojení (synchronizace pořadových čísel)
 - FIN - končím odesílání dat, polouzavření
- Kontrolní součet je počítán z pseudohlavičky + hlavičky + data.

| | | | |
|--|--|----------------------|-----------------|
| port odesílatele | | port příjemce | |
| pořadové číslo číslo 1. bajtu | | | |
| potvrzení (pořadové číslo číslo očekávaného bajtu) | | | |
| délka hlav. | | příznaky | velikost okénka |
| kontrolní součet | | konec urgentních dat | |
| volby (jsou-li) | | | |
| data (jsou-li) | | | |

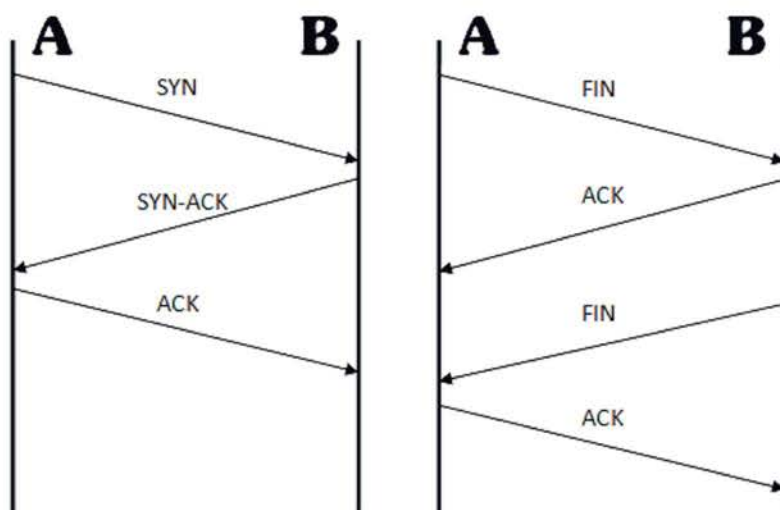
6.10 – Rozšíření datagramu (paketu) pro TCP segment

6.7.6 Navázání spojení

- Aby se mohla vysílat data pomocí TCP protokolu, je nejprve třeba vytvořit spojení. Pro navázání spojení se používá třicestný handshake (potřesení ruky), obrázek 6.11 vlevo.
- V průběhu navazování spojení se obě strany dohodnou na čísla sekvence (sequence number). Číslo sekvence a odpovědi (sequence, acknowledgement number) jsou 32bitové hodnoty uváděné v TCP hlavičce.
- Pro navázání spojení se posílá TCP segment, který má nastaveny příznaky (flags) v TCP hlavičce. Jedná se o 8 bitových hodnot **CWR** (Congestion Window Reduced), **ECE** (ECN-Echo), **URG** (Urgent), **ACK** (Acknowledgement), **PSH** (Push), **RST** (Reset), **SYN** (Synchronize), **FIN**.

- **Navázání spojení probíhá ve třech krocích:**

- Klient pošle **SYN** packet s uvedeným číslem sekvence (x), číslo odpovědi 0.
- Druhá strana si uloží číslo sekvence (x) a odpoví **SYN-ACK**, jako číslo sekvence nastaví svoje číslo (y) a do čísla odpovědi vloží (x+1) - další očekávanou hodnotu.
- Klient odpoví **ACK**, číslo sekvence (x+1), číslo odpovědi (y+1).



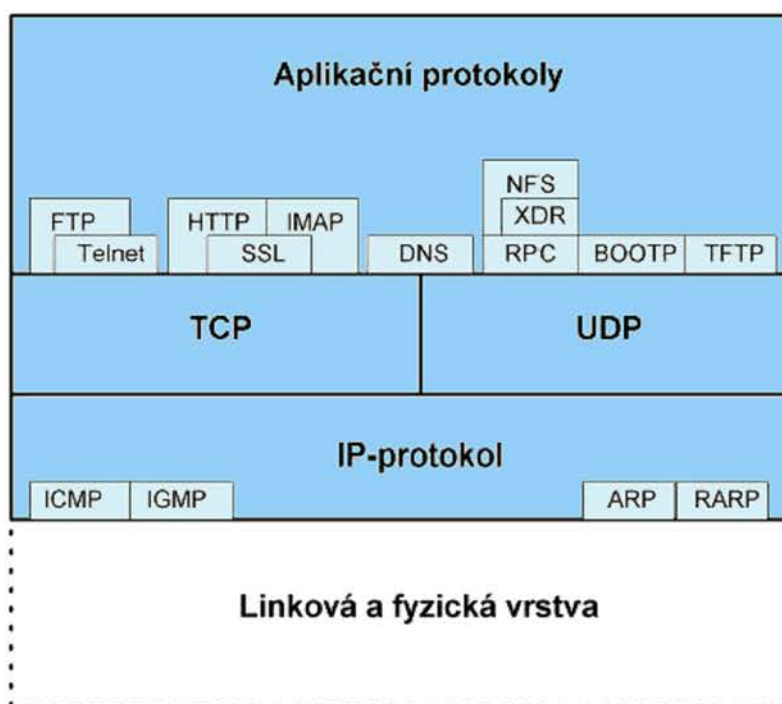
6.11 – Navázání a ukončení spojení při TCP komunikaci

6.7.7 Ukončení spojení

- Založeno na polouzavření (half-close).
- Jedna strana ohlašuje, že ukončila vysílání, dále ale přijímá a potvrzuje data - protějšek může dokončit.
- Principy při ukončení spojení jsou podobné jako při jeho navazování, též na obrázku 6.11 vpravo.
- Nejčastěji se používá čtyřcestný handshake, kdy každá strana samostatně uzavře spojení. Zde se používá sekvence **FIN** s odpovědí **ACK**.

6.8 Aplikační protokoly

- Tvoří aplikační vrstvu síťové architektury TCP/IP.
- Některé protokoly jsou závislé na službě TCP transportní vrstvy (FTP, Telnet, HTTP, ...).
- Některé protokoly využívají (vyžadují) pouze službu UDP transportní vrstvy (DHCP, BOOTP, TFTP, ...).
- Méně často protokoly využívají UDP i TCP službu transportní vrstvy „současně“ (DNS používá pro dotazy při překladech UDP, při přenosu konfigurace doplňkově TCP).
- Aplikační vrstvu tvoří i uživatelské programy používající vlastní protokol (pro aktualizace na nové verze, přenos dat, obrazu, zvuku, chat).



6.12 – Protokoly a vrstvy dle architektury internetu

Často používané aplikační protokoly (některé též podepřené RFC dokumenty):

- Bootstrap Protocol (BOOTP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Telecommunication Network (Telnet)
- Secure Shell (SSH)
- Remote Desktop Protocol (RDP)
- Lightweight Directory Access Protocol (LDAP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Trivial Transfer Protocol (TFTP)
- Network File System (NFS)
- Server Message Block (SMB)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Post Office Protocol (POP, POP3)



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PŘF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

Literatura

- [1] Tanenbaum A.S. *Computer Networks*. Prentice Hall 2002.
 - [2] T. J. Velte, A.T. Velte. *Síťové technologie Cisco*. Brno: Computer Press, 2003. 743 s. ISBN 80-7226-857-0.
 - [3] I. Rukovanský, O. Kratochvíl. *Bezdrátové počítačové sítě*. Kunovice : Evropský polytechnický institut, 2007. 82 s. ISBN 978-80-7314-112-7.
 - [4] Peterka J. Archív článků [online]. Dostupné z: <<http://www.earchiv.cz>>.
 - [5] Stevens W. R. *TCP/IP Illustrated volume 1*, Addison-Wesley 1994.
 - [6] R. Pužmanová. *Moderní komunikační sítě od A do Z*. 2. aktualizované vydání. Brno: Computer Press, 2006. 432 s. ISBN 80-251-1278-0.
 - [7] Standardy RFC, IEEE, ISO, OSI [online]. Dostupné z [www: <http://standards.ieee.org/>](http://standards.ieee.org).
 - [8] L. Dostálek, A. Kabelová. *Velký průvodce protokoly TCP/IP a systémem DNS*. Praha: Computer Press, 2002, ISBN 80-7226-675-6
-