Univerzita Palackého Olomouc

Katedra technické a informační výchovy

Soubor přednášek do předmětu:

Technologie počítačových sítí

prof. PhDr. MILAN KLEMENT, Ph.D.

OLOMOUC 2023

prof. PhDr. Milan Klement, Ph.D.

1. Úvod do počítačových sítí

Cíle počítačové sítě:

- dovoluje sdílený přístup k výpočetním zdrojům,
- dovoluje sdílený přístup k programům a datovým souborům,
- medium pomocí kterého mohou geograficky rozptýlení uživatelé komunikovat (e-mail, teleconferencing apod.),
- elektronická obec – skupina uživatelů,
- informační dálnice, národní informační struktura,
- cyberprostor.

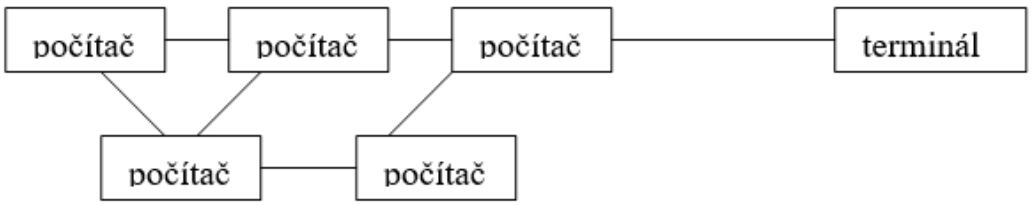
Historický vývoj:

1. **Systémy vzdáleného přístupu**

- veškeré výpočty jsou uskutečňovány na vzdáleném počítači

2. **Počítačové sítě**

- počítačová síť umožňuje realizovat výpočet kdekoliv, nejen na jednom konkrétním počítači
- úloha jako celek běží většinou na jednom počítači ⇒ nutnost programového vybavení i dat nutných k řešení úlohy na tomto počítači



3. **Distribuované systémy**

- množina počítačů a terminálů
- výpočet neprobíhá pouze na jednom počítači, ale na několika najednou
- nutnost rozdělení úloh v síti

Rozsah počítačových sítí

- v dnešní době počítačové sítě překonávají velké vzdálenosti a rozprostírají se na velké ploše naší planety

WAN – Wide Area Networks

- národní, nadnárodní a světové počítačové sítě ⇒ tisíce a stovky kilometrů

- využití současných infrastruktur ⇒ přenos dat a telefonních hovorů po jedné síti
- původní rychlost 100 kb/s dnes až 100 Mb/s

MAN – Metropolitan Area Networks

- sítě v městských oblastech a regionech ⇒ několik desítek kilometrů,
- propojení pomocí optických spojů a radiových směrových spojů
- rychlost přenosu až 100 Mb/s

LAN – Local Area Networks

- počítačové sítě uvnitř budov a areálů ⇒ několik metrů až několik kilometrů
- většinou v majetku instituce, která je vytvořila
- využití speciálních spojení (kroucená dvoulinka, koaxiální kabel, optické vlákno) např. ETHERNET – 10 Mb/s, 100 Mb/s, 1 Gb/s

1.1 Základní pojmy

- **LAN (Local area network)** je skupina počítačů a ostatních zařízení jako jsou například tiskárny, plottery, scannery a modemy propojená navzájem ***kabeláží***. V každém počítači je nainstalována ***síťová karta.*** Síťové karty (počítače) jsou obvykle propojeny přes ***HUB*** nebo přes ***SWITCH***. Zřídka se propojují jeden s druhým. Provoz celé počítačové sítě pak zajišťuje ***síťový operační systém***.
- **Kabeláž** fyzicky spojuje jednotlivé účastníky sítě. Může být koaxiální, twisted pair -"kroucená dvoulinka" nebo optická.
- **Síťové karty** (NIC - network interface card) jsou elektronické komponenty, které se zasunují do volných slotů počítačů. Podle druhu sběrnice počítače mohou být karty ISA, EISA, PCI, PCMCIA nebo USB (obvykle u počítačů typu notebook). Na síťové kartě je umístěn konektor, který zprostředkuje propojení síťové karty s kabeláží. Konektory rozlišujeme BNC (koaxiální kabeláž), RJ-45 (twisted pair) nebo SC a ST (optická kabeláž).
- **HUBy a SWITCHE** jsou zařízení určená k propojení počítačů. HUB zajišťuje jednoduché propojení. Na všech jeho vstupech a výstupech (tzv. portech) se objevuje stejný signál (stejná informace). Oproti HUBu, Switch je už chytřejší. Ví, která zpráva je komu určena (ví, které počítače jsou připojeny ke kterému portu) a jinému ji prostě nepošle. Komunikace dvou účastníků sítě přes SWITCH tedy neblokuje komunikaci ostatních účastníků, tak jako komunikace přes HUB.
- **Síťový operační systém** řídí provoz a práci celé počítačové sítě. Operačních systémů je obrovská řada. Vyrábí je firmy jako Microsoft, Novell, Unix, Banyan"s VINES a řada dalších. Přesto existují v zásadě pouze dva základní typy - ***cliet/server*** (zákazník/služba) a ***peer-to-peer*** (rovný s rovným).
- **Síť typu CLIENT/SERVER** je obvykle řízena jedním výkonným počítačem-SERVERem. Ten mívá více pevných disků, které jsou sdíleny jednotlivými účastníky sítě- pracovními stanicemi (workstation). Rozlišení, zda-li jde o server nebo stanici je v těchto sítích velice jednoduché. Jinými slovy - počítač je vždy server nebo stanice, nikdy ne oba. Stanice mohou komunikovat pouze se serverem (a i spolu tedy pouze přes server). V sítích často bývá více serverů. Obvykle platí ,

že počet serverů je nižší než počet pracovních stanic. Tento typ sítí je především určen pro větší sítě v průmyslovém nasazení.

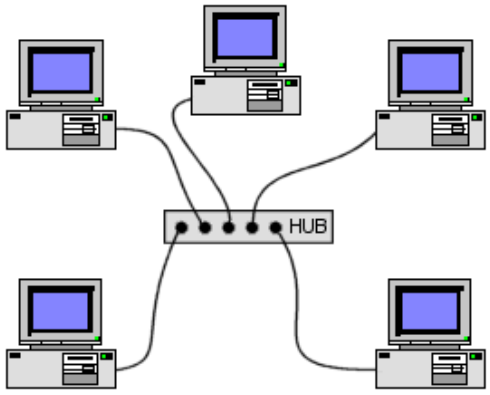
- **Síť typu peer-to-peer** se vyznačuje tím, že počítač může být i pracovní stanicí i serverem. Takže všichni uživatelé spolu navzájem komunikují. Tento typ sítí je především určen pro malé sítě zajišťující komunikaci v kancelářích. Jsou podstatně levnější než sítě client/server.
- **Výběr síťového protokolu.** ***V zásadě rozlišujeme 4 druhy: Ethernet, ARCNET, Token Ring a ATM.*** Každý z nich má svůj vlastní síťový hardware a pravidla. Pravidla určují, jaká kabeláž se může použít, jaké mohou být délky propojovacích kabelů, jak se přenášejí data a řadu dalších.

    - Protokol Token Ring je velmi stabilní proti poruchám kabeláže. Je však velmi drahý. Používá se zejména v bankovnictví.
    - Protokol ATM je vhodný zejména do podniků, kde se využívá multimedií, například Videokonferencí. Zatím nejdražší.
    - ARCNET se dnes již téměř nepoužívá z důvodu malé rychlosti. V současné době je nejobvyklejším síťovým protokolem Ethernet. Je levnější než Token Ring nebo ATM a výkonnější než ARCNET.
    - Ethernet může teoreticky přenášet data rychlostí 10 milionů bitů za vteřinu (10Mbps). Jelikož byte má 8 bitů, je rychlost teoreticky 1.2 milionu bytů za vteřinu. Tato rychlost však nemůže být dosažena, neboť data se přenáší ve skupinách zvaných pakety, které mohou být nejvýše 1500 bytů veliké. Například 150 000 bytů dlouhý soubor se musí rozdělit na 100 packetů. A to zabere nějaký čas.
    - Fast Ethernet je novější verzí Ethernetu. Přenáší data desetkrát větší rychlostí (1 000 Mbps). Gigabit Ethernet je nejnovější verzí Ethernetu. Přenáší data stokrát větší rychlostí než Ethernet. Tento standard je však zatím drahý a jeho dosah je pouze asi cca 100 m (data z počátku roku 2016).

1.2 Topologie počítačových sítí

1.2.1 Hvězdicová topologie (strom)

Ve hvězdicové topologii jsou počítače propojeny pomocí kabelových segmentů k centrálnímu prvku sítě, nazývanému rozbočovač. Signály se přenáší z vysílacího počítače přes rozbočovače do všech počítačů v síti. Tato topologie pochází z počátků používání výpočetní techniky, kdy bývaly počítače připojeny k centrálnímu počítači mainframe. Mezi každými dvěma stanicemi musí existovat jen jedna cesta!



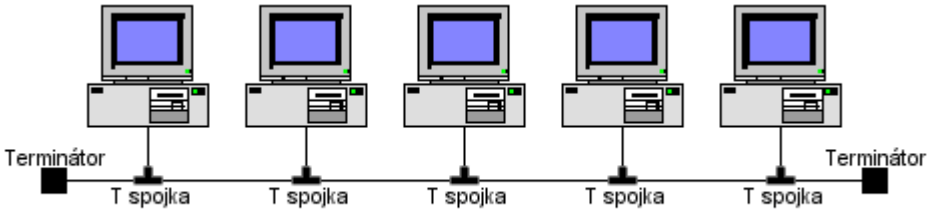
Síť s hvězdicovou topologií

Hvězdicová topologie nabízí centralizované zdroje a správu. Protože jsou však všechny počítače připojeny k centrálnímu bodu, vyžaduje tato topologie při instalaci velké sítě velké množství kabelů. Kromě toho, selže-li centrální bod, přestane fungovat celá síť.

Pokud ve hvězdicové síti selže jeden počítač nebo kabel, který ho připojuje k rozbočovači, pouze tento nefunkční počítač nebude moci posílat nebo přijímat data ze sítě. Zbývající část sítě bude i nadále fungovat normálně.

1.2.2 Sběrnicová topologie

Sběrnicová topologie je také známa jako lineární sběrnice. Jde o nejjednodušší a nejčastější způsob zapojení počítačů do sítě. Skládá se z jediného kabelu nazývaného hlavní kabel (také páteř nebo segment), který v jedné řadě propojuje všechny počítače v síti.



Síť se sběrnicovou topologií

Komunikace ve sběrnicové topologii
Počítače v síti se sběrnicovou topologií komunikují tak, že adresují data konkrétnímu počítači a posílají tato data po kabelu ve formě elektrických signálů. Abyste pochopili, jak počítače ve sběrnicové topologii komunikují, musíte se seznámit se třemi pojmy:

- posílání signálu
- vracející se signál
- terminátor

Posílání signálu
Data v síti ve formě elektrických signálů jsou posílána všem počítačům v síti, nicméně informaci přijme pouze ten počítač, jehož adresa odpovídá adrese zakódované v počátečním signálu. V daný okamžik může zprávy odesílat vždy pouze jeden počítač.

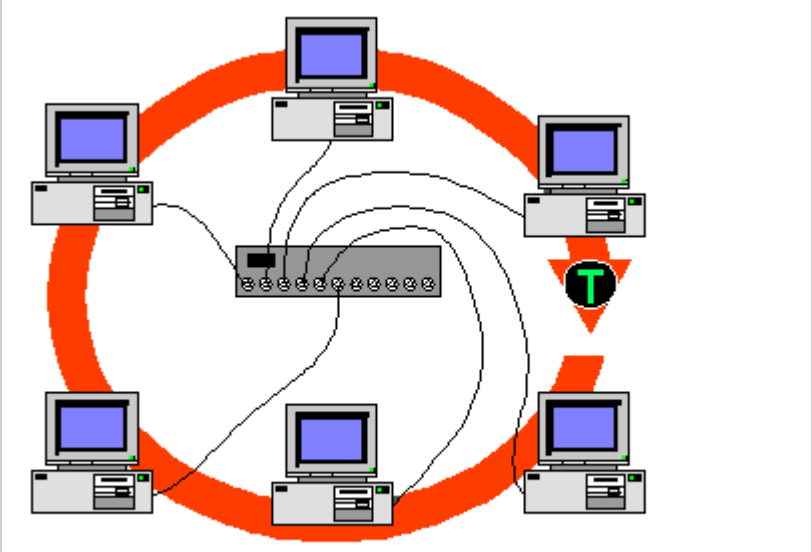
Protože ve sběrnicové síti může v daném okamžiku data posílat vždy pouze jeden počítač, závisí výkon sítě na počtu počítačů připojených ke sběrnici. Čím více počítačů je ke sběrnici připojených, tím více počítačů bude čekat, aby mohly poslat data po sběrnici, a tím bude síť pomalejší.
Sběrnicová topologie je pasivní topologií. Počítače ve sběrnicové síti pouze poslouchají, zda jsou v síti posílána nějaká data. Neodpovídají na přesun dat z jednoho počítače na druhý. Pokud jeden počítač selže, neovlivní to zbytek sítě. V aktivní topologii počítače obnovují signály a přesunují data dále po síti.

Vracející se signál
Protože data, neboli elektrický signál, jsou posílána po celé síti, cestují z jednoho konce kabelu na druhý. Kdyby mohl signál pokračovat bez přerušení, neustále by se vracel tam a zpět podél kabelu a zabránil by tak ostatním počítačům v odesílání jejich signálů. Proto je potřeba signál, co měl možnost dosáhnout cílové adresy, zastavit.

Terminátor
Aby se zastavilo vracení signálu, umístí se na oba konce kabelu terminátor, který pohlcuje volné signály. Pohlcování vyčistí kabel tak, aby mohly data posílat i další počítače.

1.2.3 Prstencová topologie (kruh)

Prstencová topologie propojuje počítače pomocí kabelu v jediném okruhu. Neexistují žádné zakončené konce. Signál postupuje po smyčce v jednom směru a prochází všemi počítači. Narozdíl od pasivní sběrnicové topologie funguje každý počítač jako opakovač, tzn. že zesiluje signál a posílá ho do dalšího počítače. Protože signál prochází všemi počítači, může mít selhání jednoho počítače dopad na celou síť.



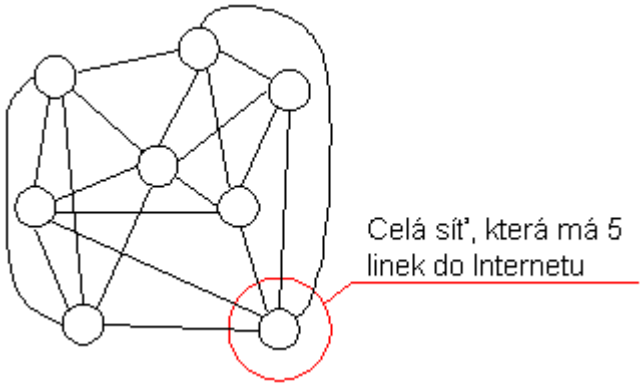
Síť s prstencovou topologií

Předávání známky

Jeden způsob přenosu dat po kruhu se nazývá předávání známky. Známka (token) se posílá z jednoho počítače na druhý, dokud se nedostane do počítače, který má data k odeslání. Vysílající počítač známku pozmění, přiřadí datům elektronickou adresu a pošle ji dál po okruhu.
Data procházejí všemi počítači, dokud nenaleznou počítač s adresou, která odpovídá jim přiřazené adrese.
Přijímací počítač vrátí vysílacímu počítači zprávu, že data byla přijata. Po ověření vytvoří vysílací počítač novou známku a uvolní ji do sítě.
Může se zdát, že oběh známky trvá dlouho, ale ve skutečnosti se přenáší přibližně rychlostí světla. Známka proběhne kruhem o průměru 200m asi 10 000krát za sekundu.

1.2.4 Neomezená topologie

Segmenty sítě jsou zapojeny libovolně mezi sebou. Nejedná se o samostatné počítače, ale o navzájem propojené sítě. Například pro připojení do Internetu.

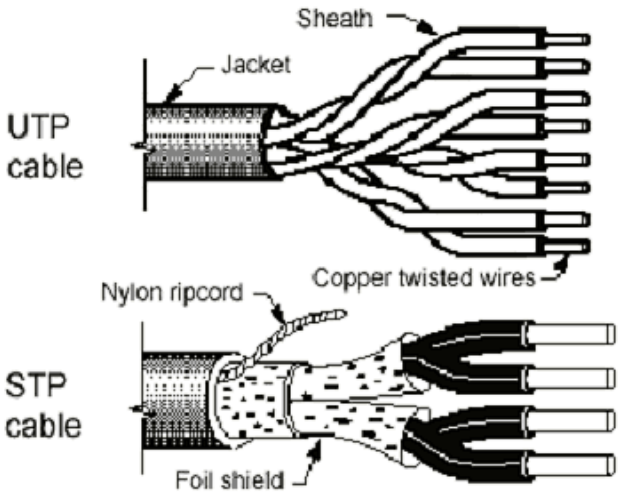


1.3 Komunikační média (kabeláž)

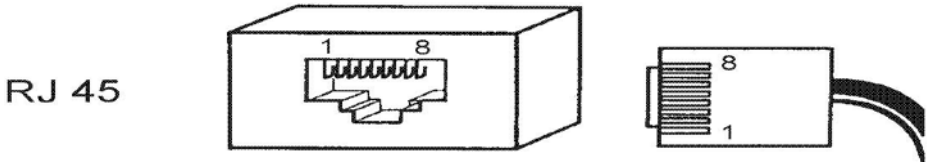
1.3.1 Měděné vodiče (kroucená dvoulinka)

- 8 žil, několik druhů CAT3 – připojení telefonu (10 Mb/s), CAT5, CAT6 (100 Mb/s)
- proud ve vodiči teče oběma směry – tam i zpět ⇒ eliminace rušivých vlivů

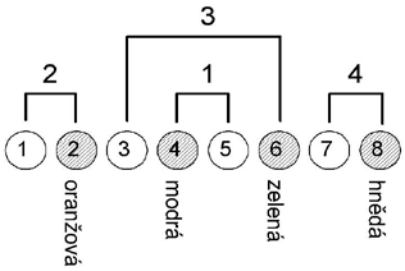
V současné době je v LAN nejpoužívanějším přenosovým médiem **kroucený dvoupár** označovaný jako UTP (Unshelded Twisted Pair). Základním parametrem tohoto kabelu je impedance 100 ohmů. V Evropě je ovšem používanější stíněná STP (Shielded Twisted Pair) nebo FTP (Foiled Twisted Pair). UTP kabely lze používat pro celé spektrum současně používaných technologií – Ethernet Fast Ethernet, Gigabit Ethernet, Token Ring i ATM. Topologií, která je krouceným dvoupárem vytvořena je hvězda. Běžné označení pro sítě tvořené krouceným dvoupárem je **strukturovaná kabeláž**.



Jednotlivé místnosti se opatřují zásuvkami pro konektor RJ 45



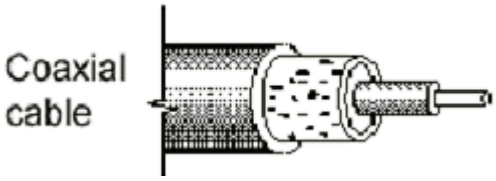
Konektor RJ 45 („kostka cukru“) obsahuje 8 vývodů pro 4 páry. Nejčastěji se používá zapojení dle EIA 568B. Toto zapojení umožňuje např. pár číslo 1 použít pro telefon (analogový) a páry 2 a 3 např. pro Ethernet (pár 4 zůstává v tomto případě volný).



1.3.2 Koaxiální kabel

Signál je veden vnitřním vodičem, opředení funguje jako uzemnění ⇒ stínění vnitřního vodiče.

Ještě před nedávnou dobou byl nejpoužívanějším přenosovým médiem v Ethernet LAN sítích **koaxiální kabel** (v Token Ring sítích s modifikací twinax). Výhodou byla cena a jednoduchost provedení. Nevýhodami jsou náchylnost k poruchovosti a technologická omezení (počet uzlů, rychlost). Typickou topologií tvořenou koaxiálním kabelem je sběrnice.

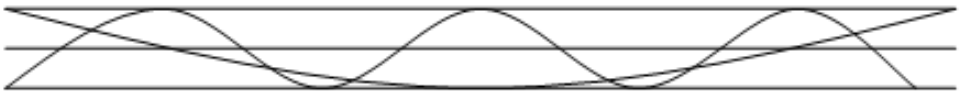


1.3.3 Optická vlákna

Výroba tažením ze speciálního skla, průměr 50 μm, délka až 1 km.

Konstantní index lomu

- skleněné vlákno je obaleno teflonem, který má jiný index lomu



- paprsky jsou vysílány pod různým úhlem
- každý paprsek tak letí jinak dlouhou cestu, potřebují k tomu jiné množství času⇒ omezení šířky pásma kvůli slévání ⇒ omezeno na 10 Mb/s

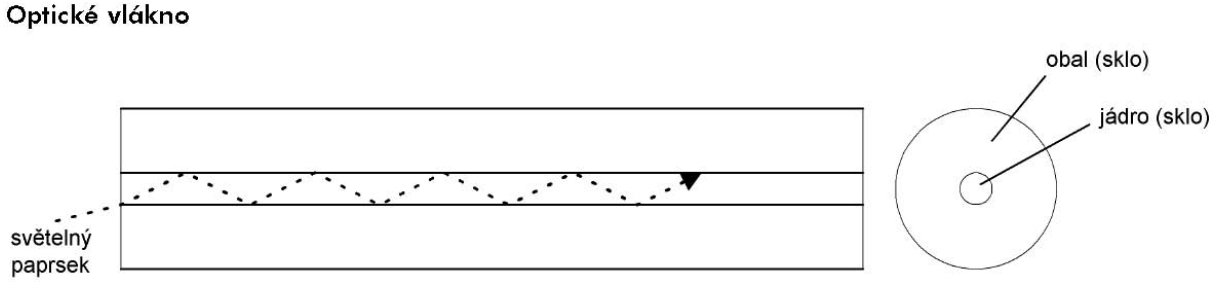
Vlákno s proměnným indexem lomu

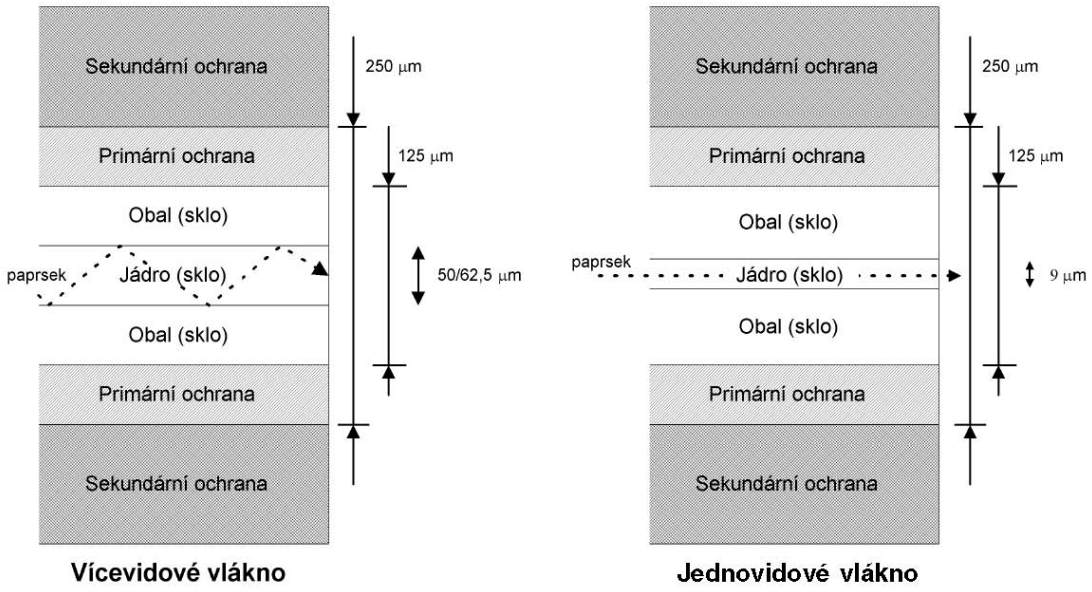
- při okrajích je vlákno „řidší“ ⇒ paprsek při okrajích letí rychleji, u středu pomaleji ⇒ celková dráha jednotlivých paprsků je různá ale čas je stejný
- omezení až na 10 Gb/s

Jednovidová vlákna

- průměr 2 μm, signál se šíří pouze středem
- rychlost až několik Gb/s
- výhodou je menší útlum signálu ⇒ možnost vedení na větší vzdálenosti (20-30 km)

V LAN sítích se pro překlenutí delších vzdáleností používají optické kabely. Pro kratší vzdálenosti (cca 260 m až 2 km v závislosti na technologii) multimodové (neboli mnohovidové) pro větší vzdálenosti singlemodové (neboli jednovidové). Optické kabely se používají i pro spojování budov tam, kde je nutné realizovat spoj venkovním prostředím a to i na poměrně krátké vzdálenosti. Typickou topologií tvořenou koaxiálním kabelem je hvězda.





Jednovidová vlákna mají již tak úzké jádro, že paprsek se šíří jádrem vlákna rovnoběžně, tj. neodráží se od rozhraní mezi oběma druhy skel. Jednovidová vlákna se zásadně budí laserem. Jednovidová vlákna jsou určena pro spoje na velké vzdálenosti.

1.3.4 Radiové spoje

Všesměrové

- rozhlasové a televizní spoje
- nevýhodou je zabrání celého frekvenčního pásma

Směrové (Wi-Fi, BrezzeNet)

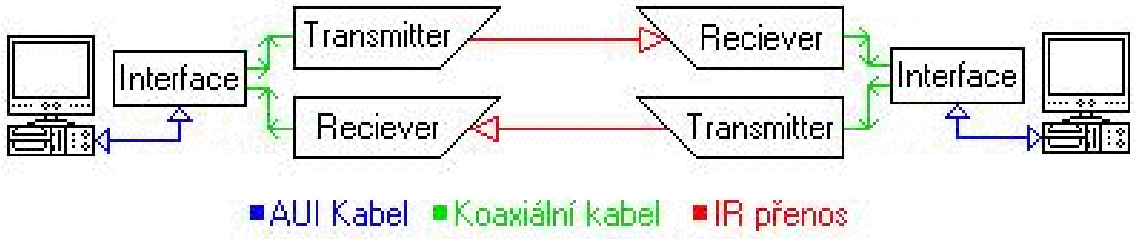
- signál se šíří v daném směru na vzdálenost až 30 km
- u počítačových sítí zejména toto použití ⇒ minimální výkon a maximální kapacita, minimální investiční náklady
- 2,5 GHz ⇒ 1 až 10 Mb/s, 3 GHz ⇒ 10 až 52 Mb/s, 5 GHz ⇒ 10 až 100 Mb/s

Družicové

- vyšší přenosové frekvence asi 11 000 GHz
- využití geostacionárních družic (telefon, televize a počítačové sítě) – nevýhodou je veliká vzdálenost 40 000 km ⇒ zpoždění tedy 270 milisekund
- využití družic nízké oběžné dráhy – nevýhodou je nenulová rychlost oběhu družic nad zemí a natáčení parabol na povrchu zemském a výhodou malá vzdálenost, např. program IRIDIUM = systém 78 družic – použití u telefonních hovorů

1.3.5 Optické (laserové) spoje

Uvedené systémy pro přenos využívají světelného paprsku, který produkují LED diody. Zařízení je možné s PC propojit buď pomocí AUI rozhraní (Attachment Unit Interface) anebo při požití modulu twister i přes používanější rozhraní TP. To umožňuje zapojit zařízení například i do switche. Obě sběrnice podporují rychlost přenosu 10Mbit za sekundu využívají rozhraní Full Duplex.



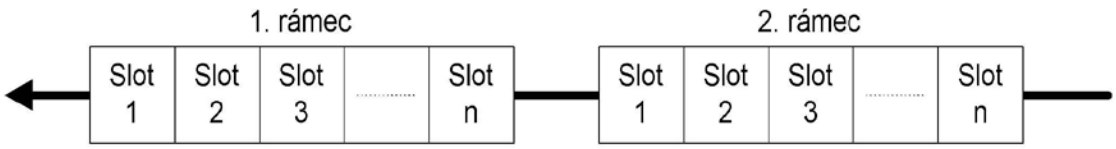
1.3.6 Velikosti segmentů kabeláže

Typ kabeláže	Délka kabelu (m)	Průměr sítě (m)
TP	100	500
Optika FOIRL	1000	5000
Optika 10BASE-FL	2000	10000
Tenký koax	185	925
Tlustý koax	500	2500
AUI	50	-

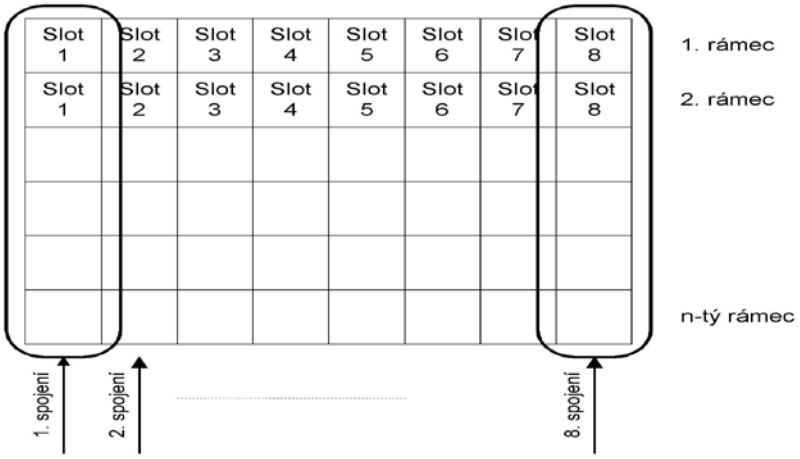
1.4 Způsoby přenosu informací

1.4.1 Synchronní přenos

Synchronní přenos je vyžadován např. pro zvuk a video, tj. v případě, kdy je třeba stejnoměrně po dobu přenosu zajistit požadovanou šíři pásma. Stane-li se, že odesílatel nevyužije zajištěné pásmo, pak pásmo zůstává nevyužito.



Synchronní přenos používá rámce konstantní délky, které jsou přenášeny sítí konstantní rychlostí. Garance šíře přenosového pásma se u synchronního přenosu provádí rozdělením přenášených rámců na sloty. Pro dané spojení se pak v každém přenášeném rámci vyhradí jeden (či více) slotů.

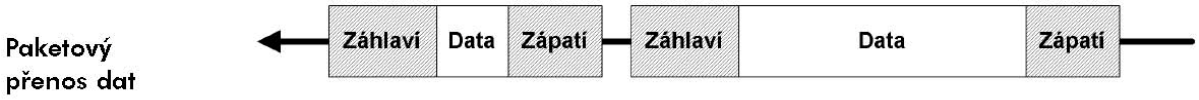


Se synchronním přenosem se setkáváme např. u připojení podnikové telefonní ústředny k ústředně Telecomu.

Internet nepoužívá synchronní přenos, tj. negarantuje šíři přenášeného pásma. Kvalitní přenos zvuku či videa se v Internetu zpravidla dociluje předimenzováním přenosových linek.

1.4.2 Paketový přenos

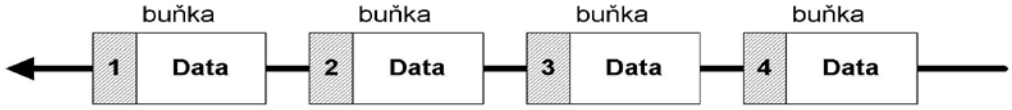
Paketový přenos je výhodný zejména pro přenos dat. Pakety nesou data obecně různé délky.



Paket nese data vždy jedné aplikace (jednoho spojení). Jelikož jsou pakety různé délky, nelze garantovat šíři pásma. Výhodou je efektivní využití pásma, protože v případě, že aplikace nepotřebuje přenášet data, pak pásmo mohou využít jiné aplikace.

1.4.3 Asynchronní přenos

Asynchronní přenos používá protokol ATM. Tento typ přenosu kombinuje paketový přenos se synchronním přenosem.



Podobně jako u paketového přenosu jsou u asynchronního přenosu data přenášena v malých paktech, které se však nazývají buňky. Obdobně jako u paketového přenosu se v jedné buňce přenáší data jedné aplikace (jednoho spojení). Avšak buňky mají stejnou délku.

2. Síťové protokoly

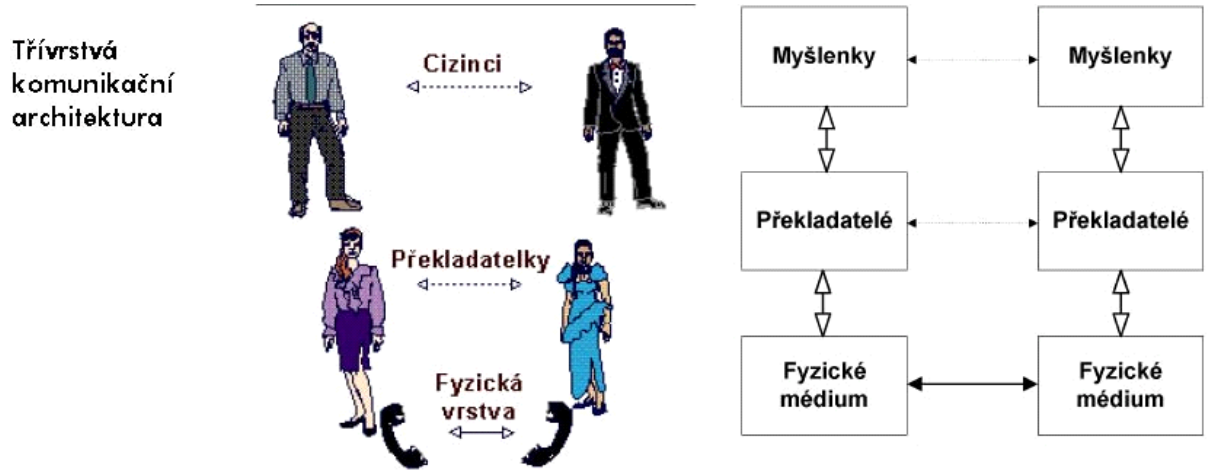
Protokoly jsou:

- pravidla, podle kterých sítové komponenty vzájemně komunikují
- definují formáty vyměňovaných zpráv a akce spojené s přenosem zpráv mezi entitami
- protokoly známé z běžného života: řízení dopravy, komunikace lidí, problémy souběžného přístupu apod.
- telekomunikační společnost CCITT vytvořila nejprve protokoly v telekomunikačních sítích a poté se věnovala tvorbě protokolů v sítě počítačové

2.1 Typy protokolů

Rozeznáváme virtuální komunikaci ve vodorovném směru (filozofickou, společným jazykem mezi překladatelkami a elektrickými signály po telefonním vedení) a skutečnou komunikaci ve svislém směru, tj. cizinec – překladatel a překladatel – telefon. Rozlišujeme tedy celkem tři vrstvy komunikace:

- Komunikace mezi cizinci
- Komunikace mezi překladatelkami
- Fyzický přenos informací po médiu (např. telefonní vedení, zvukové vlny atp.)

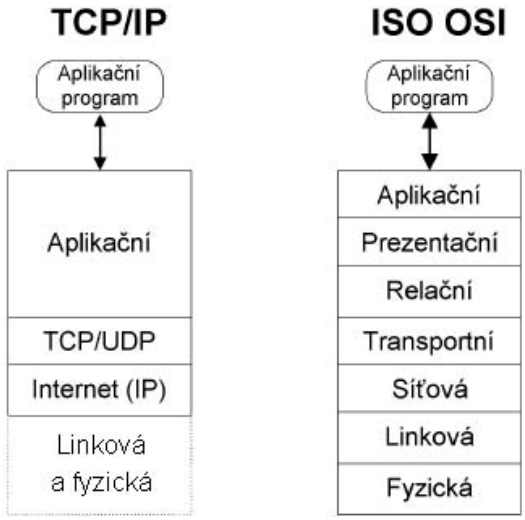


Komunikace cizinec – cizinec a překladatel – překladatel je pouze pomyslná (virtuální). Ve skutečnosti (reálně) komunikuje cizinec s překladatelem. V počítačových sítích používáme ještě více vrstev.

Počet vrstev závisí na tom, jakou soustavu síťových protokolů použijeme. Místo o soustavě síťových protokolů někdy též mluvíme o tzv. síťovém modelu. Nejčastěji se budeme setkávat s modelem, který používá Internet, tento model se též nazývá rodinou protokolů TCP/IP. Kromě protokolů TCP/IP se setkáme ještě s modelem ISO OSI, který standardizoval mezinárodní standardizační úřad (ISO).

Rodina protokolů TCP/IP využívá čtyři vrstvy a protokoly ISO OSI používají vrstev dokonce sedm.

Porovnání síťových modelů TCP/IP a ISO OSI



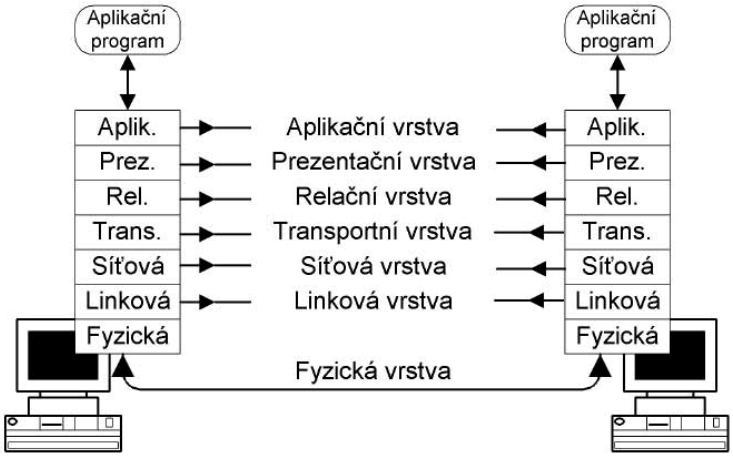
Soustavy síťových protokolů TCP/IP a ISO OSI se od sebe liší – jsou vzájemně neporovnatelné. Z obrázku je však patrné, že na síťové a transportní vrstvě jsou si velmi blízké.

Rodina síťových protokolů TCP/IP neřeší (až na výjimky, jako je protokol SLIP) linkovou a fyzickou vrstvu, proto se i v Internetu setkáváme s linkovými a fyzickými protokoly z modelu ISO OSI.

2.2 Protokol ISO OSI

- ISO - zkratka Mezinárodní organizace pro standardizaci.
- OSI - Open Systems Interconection (architektura pro propojování otevřených systémů).
- Komunikace mezi dvěma počítači je schématicky znázorněna na obrázku.

Sedmivrstvá architektura ISO OSI



2.2.1 Fyzická vrstva

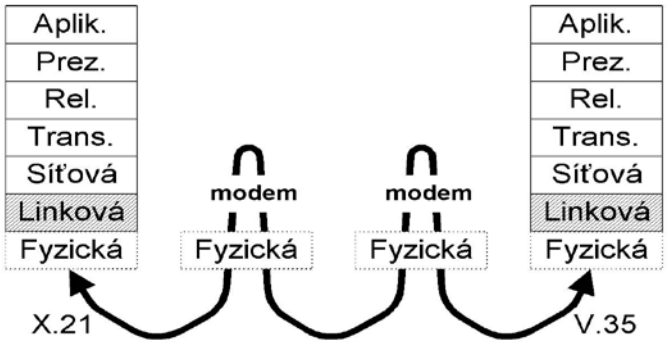
Fyzická vrstva popisuje elektrické či optické signály používané při komunikaci mezi počítači. Na fyzické vrstvě je vytvořen tzv. fyzický okruh. Na fyzický okruh mezi dva počítače bývají často vkládána další zařízení, např. modemy, které modulují signál na telefonní vedení atp.

2.2.2 Linková vrstva

Linková vrstva zajišťuje v případě sériových linek výměnu dat mezi sousedními počítači a v případě lokálních sítí výměnu dat v rámci lokální sítě.

Základní jednotkou pro přenos dat je na linkové vrstvě datový rámec. Datový rámec se skládá ze záhlaví (*Header*), přenášených dat (*Payload*) a zápatí (*Trailer*). Datový rámec nese v záhlaví linkovou adresu příjemce, linkovou adresu odesílatele a další řídící informace. V zápatí nese mj. obvykle kontrolní součet z přenášených dat. Pomocí něho lze zjistit, zdali nedošlo při přenosu k porušení dat. V přenášených datech je pak zpravidla nesen paket síťové vrstvy.

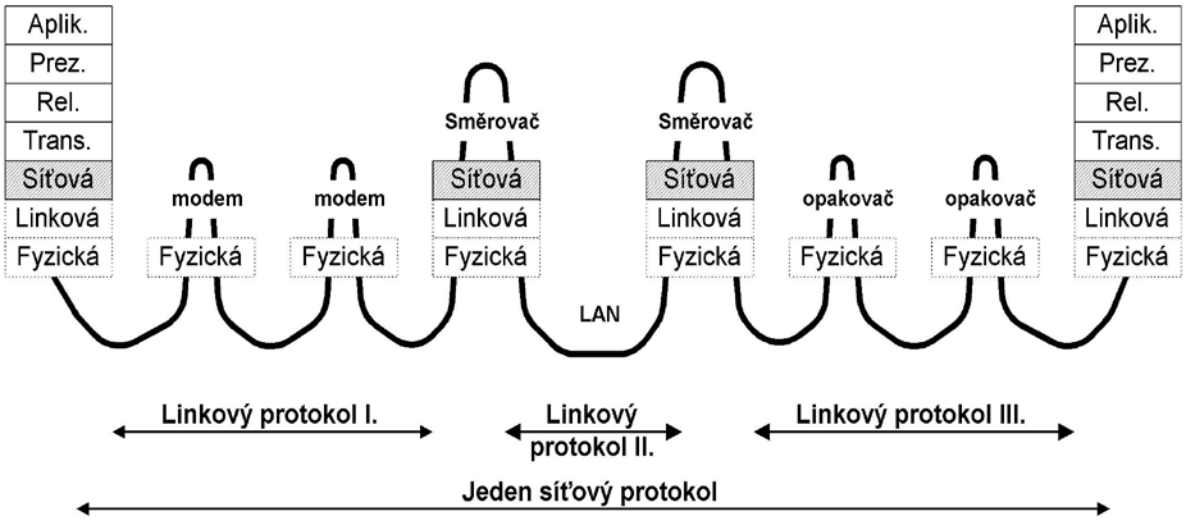
Z obrázku je vidět, že na fyzické vrstvě mohou být pro každý konec spojení použity jiné protokoly. V našem případě jeden konec používá protokol X.21 a druhý konec používá protokol V.35. Tento fakt neplatí jen pro sériové linky, ale i pro lokální sítě. U lokálních sítí se ale spíše setkáváme s komplikovanějším případem, kdy mezi oba konce spojení je vložen např. přepínač (*Switch*).



2.2.3 Síťová vrstva

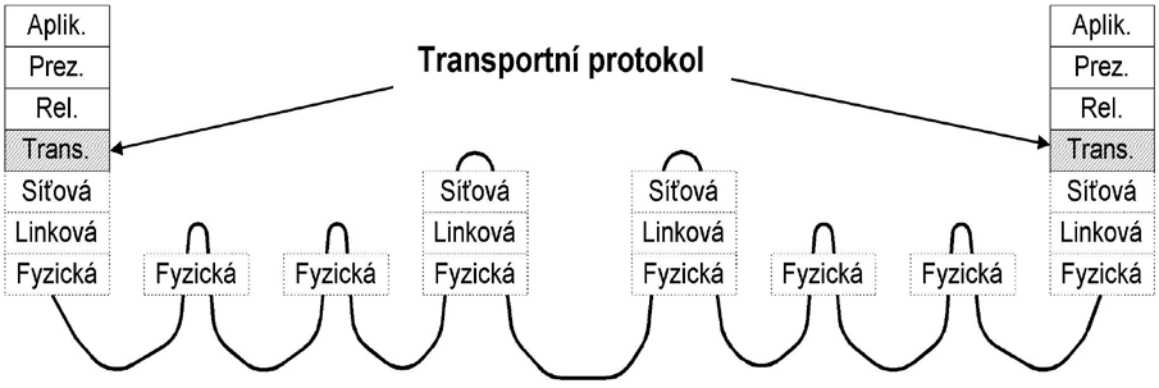
Síťová vrstva zabezpečuje přenos dat mezi vzdálenými počítači WAN. Základní jednotkou přenosu je síťový paket, který se balí do datového rámce. Síťový paket se také skládá ze záhlaví a datového pole. Se zápatím se u síťových protokolů setkáváme jen zřídka.

Z obrázku je patrné, že síťové záhlaví společně s daty síťového paketu tvoří data linkového rámce. V rozsáhlých sítích (WAN) mezi počítači leží zpravidla jeden nebo více směšovačů (routerů). Směrovač vybalí síťový paket z datového rámce (jednoho linkového protokolu) a před odesláním do jiné linky jej opět zabalí do jiného datového rámce (obecně jiného linkového protokolu).

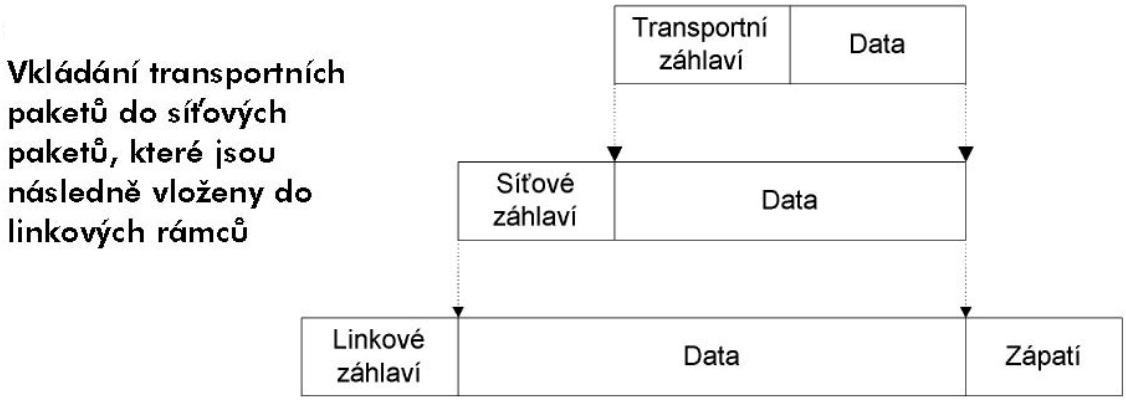


2.2.4 Transportní vrstva

Síťová vrstva zabezpečí spojení mezi vzdálenými počítači, takže transportní vrstvě se jeví jakoby žádné modemy, opakovače, mosty či směrovače na cestě nebyly. Transportní vrstva se zcela spoléhá na služby nižších vrstev.



Mezi dvěma počítači může být několik transportních spojení současně, jedno např. pro virtuální terminál a druhé pro elektronickou poštu. Z hlediska síťové vrstvy jsou pakety adresovány adresou počítače (resp. jeho síťového rozhraní). Z hlediska transportní vrstvy jsou adresovány jednotlivé aplikace.



2.2.5 Relační vrstva

Relační vrstva zabezpečuje výměnu dat mezi aplikacemi, tj. provádí tzv. checkpoint, synchronizaci transakcí (*commit*), korektní uzavírání souborů atd.

Základní jednotkou je relační paket, který se opět vkládá do transportního paketu. V literatuře se můžeme často sekat s obrázkem, jak se relační paket skládá z relačního záhlaví a relačních dat a celý relační paket se vkládá do transportního paketu. Od transportní vrstvy výše tomu tak být nemusí. Informace relační vrstvy mohou být přenášeny uvnitř dat. Ještě markantnější je tato situace u prezentační vrstvy, která data např. zašifruje, takže změní celý obsah paketu.

2.2.6 Prezentační vrstva

Prezentační vrstva je zodpovědná za reprezentaci a zabezpečení dat. Reprezentace dat může být na různých počítačích různá. Např. se jedná o problém, zdali je nejvyšší bit v bajtu zcela vlevo nebo vpravo atp. Zabezpečením se rozumí šifrování, zabezpečení integrity dat, digitální podepisování atd.

2.2.7 Aplikační vrstva

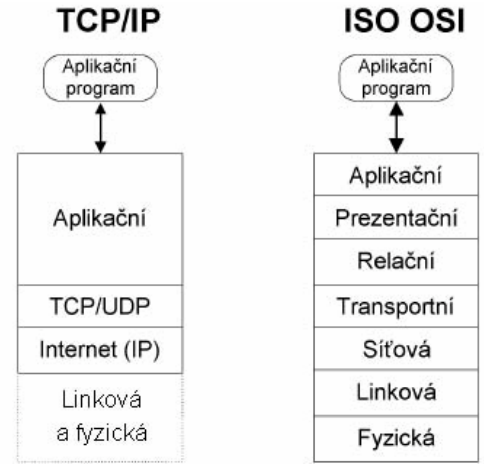
Aplikační vrstva předepisuje, v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů. Např. protokol Virtuální terminál popisuje, jak mají být data formátována, ale i dialog mezi oběma konci spojení.

Na následujícím obrázku vidíme některé protokoly jednotlivých vrstev relačního modelu ISO OSI.

Aplikační	X.400, FTAM, CMIP
Prezentační	X.226, X.216, ASN.1
Relační	X.225, X.215
Transportní	TP 0-4, TP nespoj.
Síťová	X.25, X.75, ISDN
Linková	HDLC, LAPB, ISDN
Fyzická	V.24, V.35, X.21, ISDN

2.3 Protokol TCP/IP

Rodina protokolů TCP/IP se nezabývá (až na výjimky) fyzickou a linkovou vrstvou. V praxi se i v Internetu používají pro fyzickou a linkovou vrstvu často protokoly vyhovující normám ISO OSI, které standardizoval ITU.
Jaký je vztah mezi protokoly ISO OSI a TCP/IP? Každá skupina má vlastní definici svých vrstev i protokolů jednotlivých vrstev. Proto jsou protokoly ISO OSI a TCP/IP obecně nesouměřitelné. V praxi však je třeba využívat komunikační zařízení vyhovující ISO OSI pro přenos IP-paketů nebo např. naopak realizovat služby podle ISO OSI přes Internet.



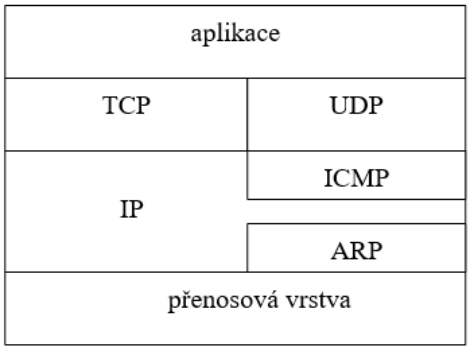
Vývoj protokolu TCP/IP je možné shrnout do těchto bodů:

- byla velká snaha uvést sedmiúrovňový model v život, jenže bylo mnoho proti: nutnost celé řady protokolů, vysoké náklady, malá používanost
- americké ministerstvo obrany zadalo projekty univerzitám (zač 70. let), aby vymysleli systém pro posílení armády, jedním z úkolů byla také počítačová síť
- došlo k vytvoření modelu přenosu dat přepínáním paketů (rozdělení, posílání samostatně, opětovné spojování)
- koncem 70. let představení tohoto modelu veřejnosti $\Rightarrow$ velký zájem univerzit podílet se na tomto projektu

- začátkem 80. let je už dost přípojných bodů, dochází k oddělení vojenské části
- počátkem 90. let komercionalizace ⇒ vznik Internetu

Internet je tedy postaven na přenosových protokolech ze 70. let: TCP/IP

- TCP……Transport Control Protocol ……. 4. úroveň
- IP……Internet Protocol……3. úroveň
- Internet – celosvětová síť
- intranet – propojení sítí s TCP/IP
- architektura TCP/IP:



fyzická + linková úroveň

přenosová vrstva – spolupráce se současnými schopnostmi, přenos informací z jednoho uzlu do druhého

síťová úroveň

ICMP……Internet Control Message Protocol – přenos řídících zpráv
ARP……..Adress Resolution Protocol – převod síťové adresy na fyzickou

transportní úroveň

UDP……..User Datagram Protocol – datagramové služby
TCP……..Transport Control Protocol – přenos pomocí segmentů

2.3.1 Internet Protokol

Internet Protokol (dále jen IP-protokol) prakticky odpovídá síťové vrstvě. IP-protokol přenáší tzv. IP-datagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese adresu příjemce, což je úplná směrovací informace pro dopravu IP-datagramu k adresátovi. Takže se může přenášet každý IP-datagram samostatně. IP-datagramy tak mohou k adresátovi dorazit v jiném pořadí, než byly odeslány.

Každé síťové rozhraní v rozsáhlé síti Internet má svou celosvětově jednoznačnou IP-adresu (jedno síťové rozhraní může mít více IP-adres, avšak jednu IP-adresu nesmí používat více síťových rozhraní). Internet je tvořen jednotlivými sítěmi, které jsou propojeny pomocí směrovačů. Směrovač se anglicky nazývá *router*, ve starších publikacích se však označuje jako *gateway*.

2.3.2 Protokoly TCP a UDP

Protokoly TCP a UDP odpovídají transportní vrstvě. Protokol TCP dopravuje data pomocí TCP segmentů, které jsou adresovány jednotlivým aplikacím. Protokol UDP dopravuje data pomocí tzv. UDP datagramů.
Protokoly TCP a UDP zajišťují spojení mezi aplikacemi běžícími na vzdálených počítačích. Protokoly TCP a UDP mohou zajišťovat i komunikaci mezi procesy běžícími na témže počítači, to je však z našeho pohledu nepříliš zajímavé.

Rozdíl mezi protokoly TCP a UDP spočívá v tom, že protokol TCP je tzv. spojovanou službou, tj. příjemce potvrzuje přijímaná data. V případě ztráty dat (ztráty TCP segmentu) si příjemce vyžádá zopakování přenosu. Protokol UDP přenáší data pomocí datagramů (obdoba telegramu), tj. odesílatel odešle datagram a už se nezajímá o to, zdali byl doručen.

Adresou je tzv. port. Pro pochopení rozdílu mezi IP-adresou a portem se používá srovnání s poštovní adresou. IP-adresa odpovídá adrese domu a port jménu a příjmení osoby, které má být dopis doručen.

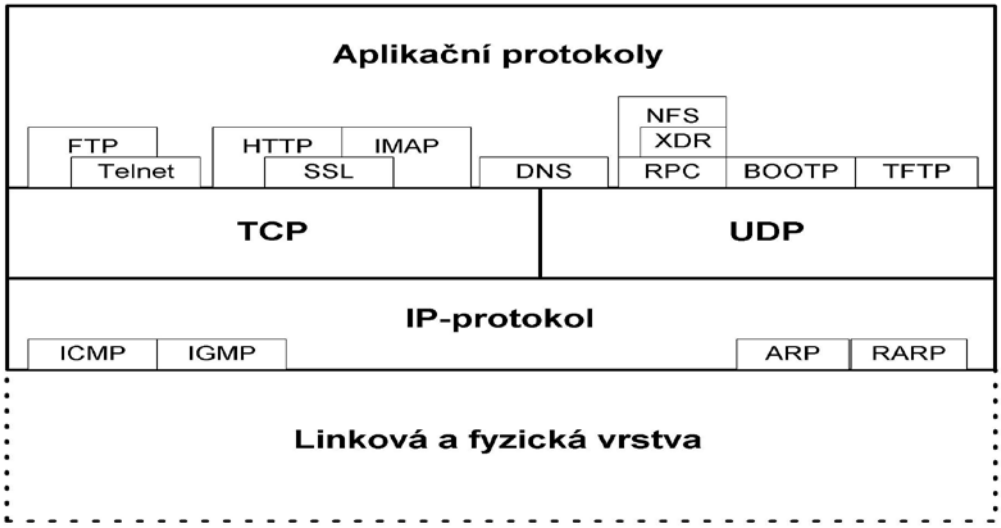
2.3.3 Aplikační protokoly

Aplikační protokoly odpovídají několika vrstvám ISO OSI. Relační, prezentační a aplikační vrstva ISO OSI je zredukována do jedné aplikační vrstvy TCP/IP. Absence prezentační vrstvy se řeší zavedením specializovaných „prezentačních-aplikačních“ protokolů, jako jsou protokoly SSL a S/MIME specializující se na zabezpečení dat. Nebo protokoly Virtuální terminál a ASN.1 určené pro prezentaci dat. Protokol Virtuální terminál (nezaměňovat se stejnojmenným protokolem v ISO OSI) specifikuje prezentaci dat v síti pro protokol Telnet, avšak využívají jej i další protokoly (FTP, SMTP a částečně i HTTP).

Aplikačních protokolů je velké množství. Z praktického hlediska je lze rozdělit na:

- Uživatelské protokoly, které využívají uživatelské aplikace (např. pro vyhledávání informací v Internetu). Příkladem takových protokolů jsou protokoly: HTTP, SMTP, Telnet, FTP, IMAP, POP3 atd.
- Služební protokoly, tj. protokoly se kterými se běžní uživatelé Internetu nesetkají. Tyto protokoly slouží pro správnou funkci Internetu. Jedná se např. o směrovací protokoly, které používají směrovače mezi sebou, aby si správně nastavily směrovací tabulky. Dalším příkladem je protokol SNMP, který slouží ke správě sítí.

Přehled protokolů využívající relační model TCP/IP je uveden na dalším obrázku:


Aplikační protokoly
FTP
Telnet
HTTP
SSL
IMAP
DNS
NFS
XDR
RPC
BOOTP
TFTP
TCP
UDP
IP-protokol
ICMP
IGMP
ARP
RARP
Linková a fyzická vrstva

3. Fyzická vrstva

Pro drtivou většinu uživatelů jsou protokoly na fyzické vrstvě „ty naprosto odtažité protokoly, které popisují signály na konektorech (uživatelé říkají zástrčkách) na zadní straně počítače, na které je připoje-na šňůra propojující počítač s počítačovou sítí“.

V zásadě rozlišujeme dva typy počítačových sítí: lokální sítě (LAN) a rozsáhlé sítě (WAN). Z hlediska fyzické vrstvy jsou v podstatě protokoly pro LAN jednou skupinou protokolů a protokoly pro WAN druhou skupinou. Kromě toho dnes populární protokol ATM smazávající rozdíl mezi LAN a WAN používá nejen nové protokoly, ale je zejména schopen využít stávající linky pro WAN včetně jejich protokolů (např. linky E1). Na druhou stranu ATM i emuluje protokoly pro LAN.

WAN
Rozsáhlé sítě pokrývají velkou škálu situací. Od připojení domácího PC k Internetu pomocí sériové asynchronní linky rychlostmi uváděnými v kb/s až po mezikontinentální linky realizované podmořský-mi kabely či družicovými spoji o rychlostech uváděných v Gb/s.

LAN
Lokální sítě jsou středně rychlé sítě. Základní vlastností LAN je, že na lokální síti spolu zpravidla komunikuje několik stanic na sdíleném médiu. Na LAN je běžné použití oběžníků. V rámci jedné LAN se používá stejný linkový protokol (např. Ethernet). Dnes se však pod pojmem LAN často myslí tzv. rozšířené LAN, které mohou obsahovat mosty a přepínače, které mají síťová rozhraní pro více linkových protokolů a umí konvertovat rámce jednoho linkového protokolu na rámce jiného linkového protokolu. Z hlediska fyzické vrstvy nás však budou zajímat pouze klasické LAN, protože na rozšířené LAN se fyzická vrstva dívá jako na soustavu jednotlivých LAN.
Pro připojení LAN k rozsáhlé síti (WAN) se využívají směrovače. Směrovač je zařízení předávající IP-datagramy z jednoho síťového rozhraní na jiné své síťové rozhraní, přitom každé rozhraní může být na jiné LAN, nebo může být rozhraním do WAN.

Přenosové rychlosti na dnešních LAN se pohybují od 10 Mb/s až po Gb/s.

3.1 Sériové linky

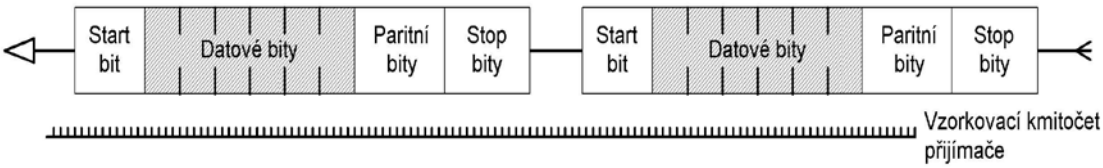
Sériové výstupy PC používají signály specifikované normou ITU V.24 (v USA analogická norma RS232). Jedná se o rozhraní pro sériový asynchronní arytmický přenos dat. V praxi se běžně používá do 64 kb/s, ale modem si doma na něj nejspíše připojíte rychlostí 115 200 b/s a ono to kupodivu bude také pracovat.

Chcete-li se s někým např. telefonem o něčem domluvit, pak musíte mluvit tak rychle, aby on byl schopen vám rozumět. Např. budete-li mluvit desetkrát rychleji, pak vám stěží porozumí. Tj. ten kdo poslouchá se musí synchronizovat s tím kdo mluví.

Z hlediska synchronizace rozeznáváme přenos:

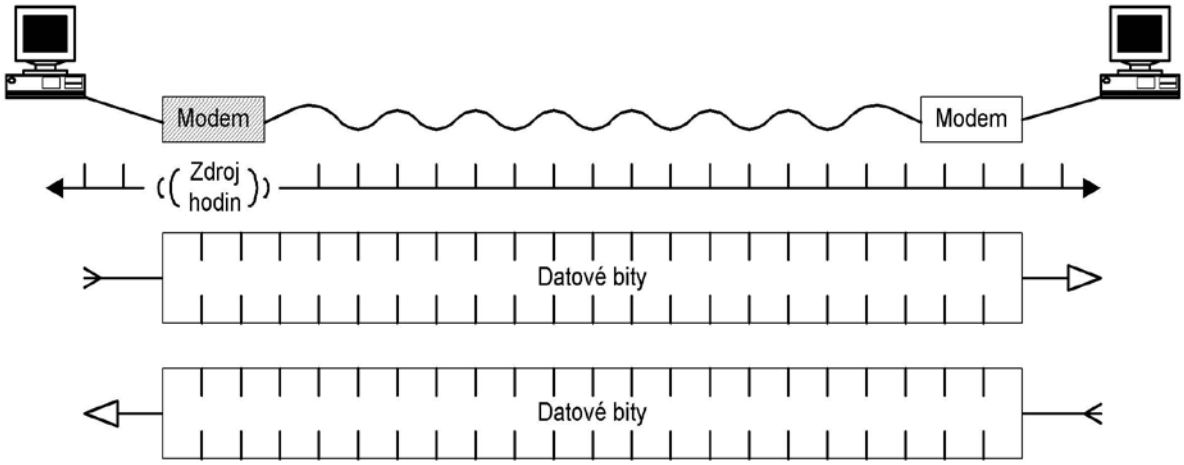
- Synchronní, kdy se informace přenášejí po jednotlivých bitech. Okamžiky přechodu od přeno-su jednoho přenášeného bitu k přenosu dalšího bitu jsou vždy stejně vzdáleny.
- Asynchronní, kdy okamžiky přechodu od přenosu jednoho bitu k přenosu dalšího bitu nejsou stejně vzdáleny. Zvláštním případem asynchronního přenosu dat je tzv. arytmický přenos.

Při asynchronním arytmickém přenosu je odesílaný znak obalen obálkou tvořenou startovacím bitem, paritními bity a stop bity (viz obr.).



Přijímač generuje vzorkovací kmitočet o řád vyšší frekvence než je maximální možná frekvence přenosu jednoho bitu. Přijímač touto frekvencí testuje vzorky přijímaného signálu. Pokud vzorek odpovídá s jistou pravděpodobností startovacímu bitu, předpokládá, že narazil na přenášený znak. Pokračuje ve vzorkování, vše až do stop bitů považuje za bity přenášeného znaku. Mezi start bitem a stop bity jsou datové bity přenášeného znaku, navíc tam může být ještě paritní bit zabezpečující jednoduchý kontrolní součet přenášeného znaku.

Dnes je však běžnější zcela jiný princip. Kromě přenášených dat se přenáší ještě synchronizační signál (hodiny). Na obr. 3.2 se na komunikaci podílí čtyři zařízení (dva modemy a dva počítače).

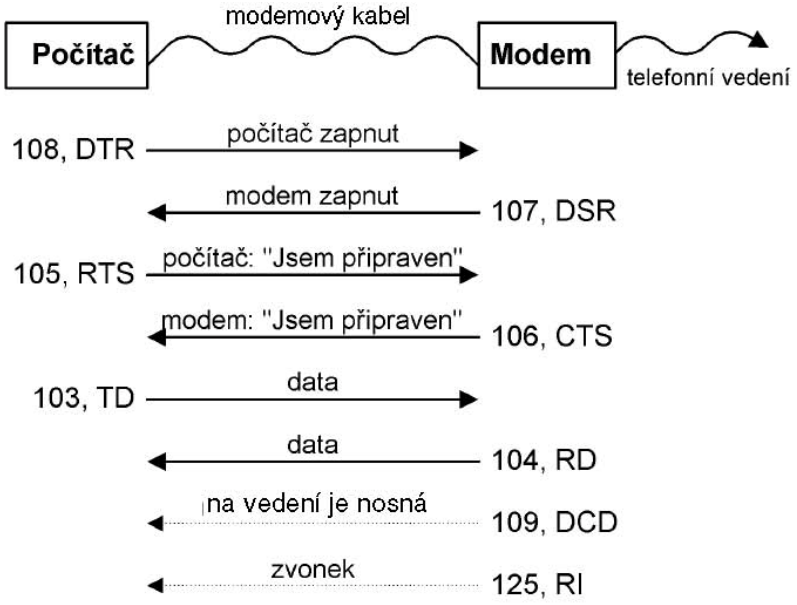


Podobně jako v orchestru může být jen jeden dirigent, tak zdrojem hodin může být jen jedno z těchto čtyř zařízení. Zpravidla to bývá jeden z modemů (*originator*). Ostatní zařízení si přizpůsobí takt svých obvodů tomuto dirigentovi. Jelikož všechna čtyři zařízení jsou synchronizována, tak mohou mezi sebou přímo komunikovat (bez vzorkování).
Na fyzické úrovni se pro sériová rozhraní nejčastěji používají normy V.35, X.21 a u PC oblíbená norma V.24. Pochopitelně existují i jiné normy, s těmi se však setkáváme méně často.

Dialog mezi počítačem a modemem je schématicky vyjádřen na obr. Signály DTR a DSR signalizují svému protějšku, že zařízení je zapnuto. V praxi se tyto signály někdy nepoužívají (vývody se nezapojují nebo naopak přímo v konektoru jsou vývody DTR a DSR propojeny).

Význam signálů RTS a CTS spočívá v řízení toku dat. V případě, že modem má svou vyrovnávací paměť plnou, pak shodí signál CTS a počítač tak signalizuje svému protějšku, aby pozastavil odesílání dat.

Schématické znázornění dialogu mezi počítačem a modemem



Hovoříme-li o přenosové rychlosti modemu, pak máme na mysli přenosová rychlost po telefonním vedení. Přenosová rychlost je dána doporučeními ITU, která modem podporuje.

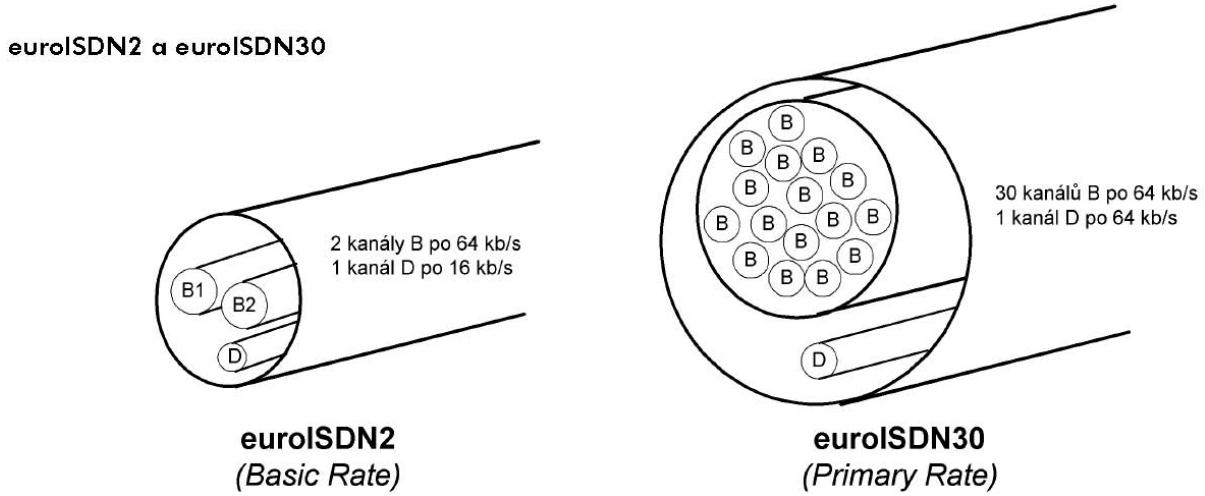
Doporučení ITU	Rychlost v Kb/kb/s
V.32	9,6
V.32bis	14,4
V.34	28, 8
V.34+	33,6
V.90	56 (od ústředny k modemu) 33,6 (od modemu k ústředně)

3.2 Digitální okruhy

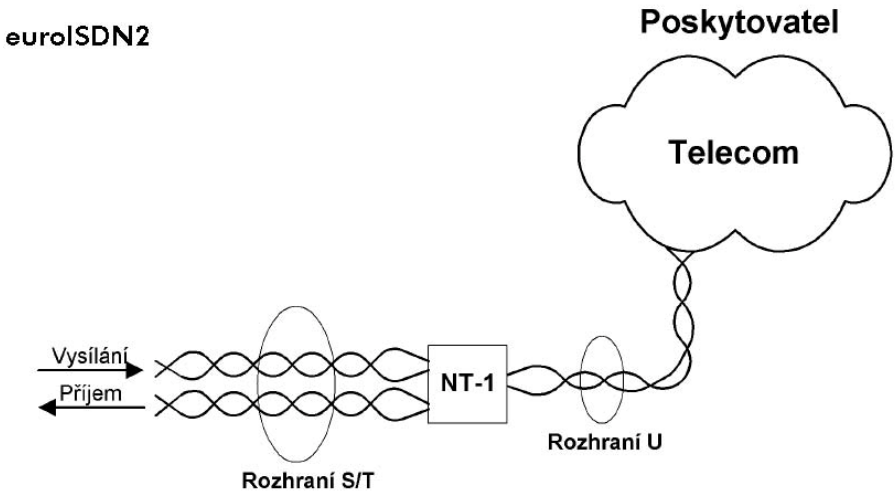
Doposud jsme popisovali analogové okruhy. Život však jde dále a analogové rozvody jsou nahrazovány digitálními. Nejprve se tak dělo uvnitř telekomunikačních firem. Dnes však i uživatelé mohou používat digitální okruhy – ISDN.

Telekomunikační firmy u nás nabízí připojení euroISDN2 a euroISDN30. To jsou spíše obchodní označení, v literatuře se spíše setkáme s anglickými názvy:

- *Basic Rate* pro euroISDN2, což je typ připojení, kdy ve fyzicky jednom vedení (jedné kroucené dvojlince) jsou dva datové kanály B každý o kapacitě 64 kb/s a jeden signalizační kanál D o kapacitě 16 kb/s.
- *Primary Rate* pro euroISDN30, což je typ připojení, kdy ve fyzicky jednom vedení (např. lince E1) je třicet datových kanálů B, každý o kapacitě 64 kb/s a jeden signalizační kanál D o kapacitě 64 kb/s.



euroISDN2 využívá stávající telefonní rozvody kroucenou dvoulinkou. Tj. většinou lze využít pro rozvod euroISDN2 i stávající metalické rozvody pro analogové telefony. Připojení ISDN popisuje norma V.110.



Jak je znázorněno na obr., jednotlivá zařízení se na rozhraní S/T připojují jako na sběrnici. Jelikož euroISDN2 má k dispozici dva datové kanály B, tak v jednom okamžiku mohou komunikovat současně dvě zařízení (např. digitální telefon a digitální modem nebo dva digitální telefony atd.).

Základem je linka o přenosové rychlosti 64 kb/s (v tabulce označena jako E0). Linka E1 pojme 32 takových základních linek. Linka E2 pojme 4x E1. Používanější je však E3, která pojme 16x E1 (resp. 4x E2) atd.

Linka	Přenosová rychlost kb/s
(E0)	64
E1	2 048
E2	8 448
E3	34 368
E4	139 264

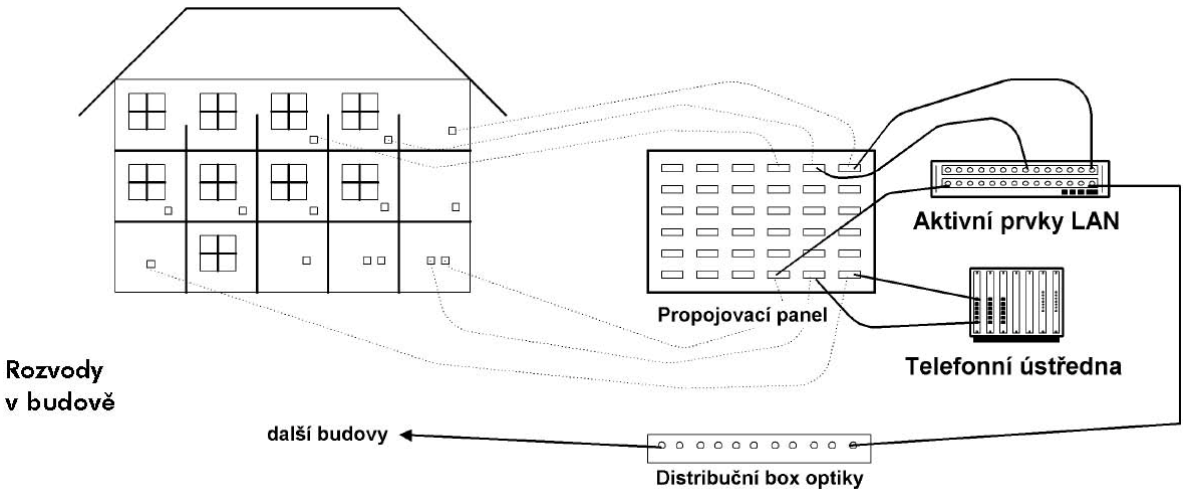
3.3 LAN

Lokální sítě jsou určeny pro propojení počítačů na kratší vzdálenosti (stovky metrů až kilometry). U lokálních sítí závisí volba fyzického rozhraní na volbě linkového protokolu. V dnešní době přicházejí v úvahu zejména čtyři typy linkových protokolů: Ethernet, Fast Ethernet, Gigabitový Ethernet a FDDI. Protokoly Arcnet a Token Ring jsou v praxi málo běžné.

3.3.1 Strukturovaná kabeláž

Strukturovanou kabeláží se rozumí komplexní řešení nízkonapěťových rozvodů v budově. Zahrnuje zejména telefonní rozvody a rozvody pro LAN. Většinou zahrnuje i další rozvody jako jsou bezpečnostní a jiné signalizace.

V jednotlivých místnostech budovy jsou umístěny telefonní zásuvky, zásuvky LAN a jiné vývody.



Propojovací panel a distribuční box optiky bývají uzavřeny v jedné skříni (*RackMount*) spolu s aktivními prvky LAN či dokonce i s telefonní ústřednou. Propojení mezi propojovacím panelem a aktivními prvky se provádí propojovacími kabely (*Patch Cord*).

Rozvod od zásuvek na propojovací panel je poměrně drahou záležitostí, protože se mnohdy jedná i o stavební úpravy. Snahou je proto rozvod provést maximálně kvalitně, aby se rozvody nemusely často předělávat. Základní filozofií nových protokolů je pak v maximální míře využít stávající kabeláže. Proto také kvalitním rozvodům původně vytvořeným pro Ethernet 10Base-T nedělal problémy přechod na 100Base-TX.

Existují normy pro rozvody – tzv. kategorie. Dnes jsou aktuální kategorie:

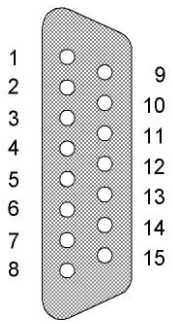
- Kategorie 5, kdy dodavatel garantuje práci v šířce pásma do 100 MHz nezávisle na použitém protokolu (Etherent, Token Ring, CDDI atd.).
- Rozšířená kategorie 5 (nebo také 5+), pracuje rovněž v šířce pásma do 100 MHz, avšak vyžaduje nové způsoby měření parametrů a v některých parametrech je přísnější. Cílem je provozovat Gigabitový Ethernet.
- Kategorie 6 s šířkou pásma do 200 MHz.
- Kategorie 7 s šířkou pásma do 600 MHz.
- Dříve existovaly i kategorie 3 a 4. Rozvody dle těchto kategorii je dnes většinou nutné předělat.

3.3.2 Ethernet (10 Mb/s)

Ethernet používá čtyři typy rozhraní: **AUI, BNC, TP** nebo **optický spoj**.

AUI (označované též jako 10BASE-5) je rozhraní (konektor CANNON 15), na které se připojuje kabel propojující počítač s tzv. *transceiverem*. Transceiver je zařízení, které vysílá/přijímá původně na tlustý koaxiální kabel rozvodu LAN. Existují však i transceivery pro rozvod tenkým koaxiálním kabelem („redukce AUI/BNC“) i transceivery pro kroucenou dvojlinku („redukce AUI/TP“).

Obr. 3.27
Zapojení rozhraní AUI



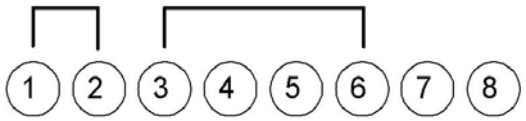
AUI

BNC (označované též jako 10BASE-2) je rozhraní pro připojení na tenký koaxiální kabel. Koaxiální kabel je v místě připojení přerušen. Na oba konce přerušení se speciálními kleštěmi

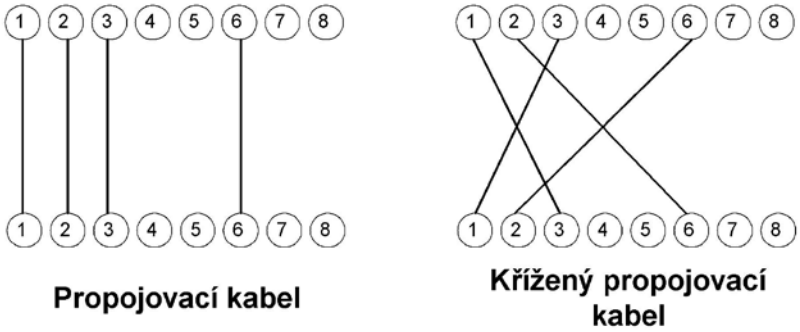
připevní BNC-konektory. Oba BNC-konektory se připojí na BNC T-konektor, který je připojen do počítače.

Kroucená dvojlinka (zkratkou TP, označovaná též jako 10BASE-T) se připojuje konektorem RJ45 („kostka cukru“). Kroucená dvojlinka vede zpravidla společně s telefonním rozvodem na centrální propojovací panel.

TP používá dva páry v konektoru RJ45, jak je znázorněno na obrázku. (Všimněte si, že vývody 4 a 5 zůstávají volné, takže je lze použít pro telefon (analogový).



V konektoru RJ45 se používají pro Ethernet dva páry. Jeden pár pro vysílání, druhý pár pro příjem. V případě, že ethernetový segment sdílejí pouze dvě stanice, které jsou propojeny přímo propojovacím kabelem, pak musí být páry překříženy (tj. překřížen příjem s vysíláním).



Ethernet na optických vláknech se označuje též jako 10BASE-F. Zásadně se vždy používá pár optických vláken – pro každý směr komunikace jedno vlákno.

3.3.3 Fast Ethernet (100 Mb/s)

Fast Ethernet se připojuje kroucenou dvojlinkou (označení **100BASE-TX**) nebo optickým spojem (označení **100BASE-FX**). Rozdíl oproti klasickému Ethernetu je pouze v kvalitě vedení. Současné rozvody se většinou staví minimálně kategorie 5, takže nasazení Fast Ethernetu jim nečiní potíže.

3.3.4 Gigabitový Ethernet (1 Gb/s)

Gigabitový Ethernet je standardizován pro optické spoje a pro kroucenou dvojlinku (4 páry). Pro jednovidová vlákna je určen standard pod označením **1000BASE-LX** buzený laserem o frekvenci 1300 nm s maximální délkou segmentu do 2 km (jednovidová vlákna na plně duplexních segmentech až do 40 km). Pro vícevidová vlákna může týž standard (1000BASE-LX)

pracovat až do vzdálenosti 450 m. Pouze pro vícevidová vlákna je určen standard 1000BASE-SX, který je buzen laserem o frekvenci 850 nm a je určen pro vzdálenosti do 250 m.

Standard pro metalické spoje **1000BASE-CX** může využívat současných rozvodů kategorie 5+ (100 MHz), avšak využije všechny čtyři páry kroucené dvojlinky (tj. všech 8 vývodů konektoru RJ 45).

3.3.5 FDDI

FDDI existují dvě varianty: na optickém vlákně (**FDDI**) nebo na kroucené dvoulince (**CDDI**). Na jedné LAN je možné obě eventuality i kombinovat. Přednost se dává kroucené dvojlince a pro připojení vzdálenějších uzlů se použije světelné vlákno. Vývody opět zpravidla vedou na distribuční box optiky v případě optických rozvodů a na propojovací panel v případě měděných rozvodů.

4. Linková vrstva LAN

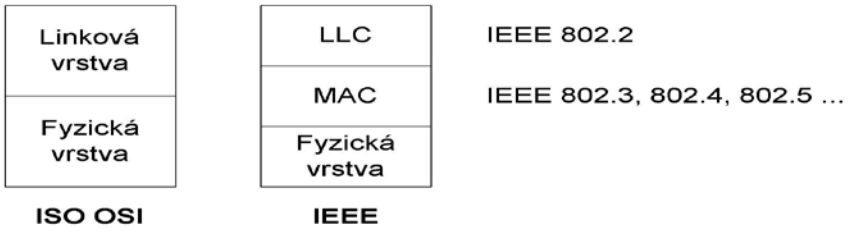
V uplynulých deseti letech byla vyvinuta celá řada systémů LAN. Masového rozšíření se však dočkaly jen dva: Ethernet a v menším rozsahu FDDI. (Někdy se ještě setkáváme se systémem Token Ring firmy IBM, ale to spíše v případech, že uživatel je kompletně vybaven systémy firmy IBM.)

Pro připojení stanice na LAN je nutné do stanice vložit příslušnou síťovou kartu. Linkové protokoly LAN jsou realizovány z části přímo v síťové kartě. Problematika LAN se vždy skládá z:

- Problematiky kabeláže, která patří do fyzické vrstvy.
- Problematiky síťových karet, které se vkládají do počítačů a ostatních zařízení. To je součást jak fyzické vrstvy, tak i linkové vrstvy, protože část softwaru pro obsluhu linkové vrstvy je realizována přímo na síťové kartě.
- Problematiky samotného linkového protokolu (včetně obsahu linkových rámců) a jeho realizace programy v počítači (ovladači).

Instituce IEEE před dvaceti lety předložila projekt, jehož cílem bylo vypracovat normy pro jednotlivé typy LAN (např. Ethernet, Arcnet, Token Ring atd.). Tyto normy popisovaly pro každý typ LAN vrstvu MAC. Vznikla tak norma IEEE 802.3 pro Ethernet, IEEE 802.4 pro Token Bus, IEEE 802.5 pro Token Ring atd.

Pro všechny systémy pak byla vypracována společná norma pro vrstvu LLC pod označením IEEE 802.2, což schématicky vyjadřuje obrázek.



Problematika linkové vrstvy pro LAN tak byla rozdělena do dvou podvrstev:

- Spodní vrstva Medium Access Control (MAC) částečně zasahující do fyzické vrstvy se zabývá přístupem na přenosové médium.
- Horní vrstva Logical Link Control (LLC) umožňuje navazovat, spravovat a ukončovat logická spojení mezi jednotlivými stanicemi LAN.

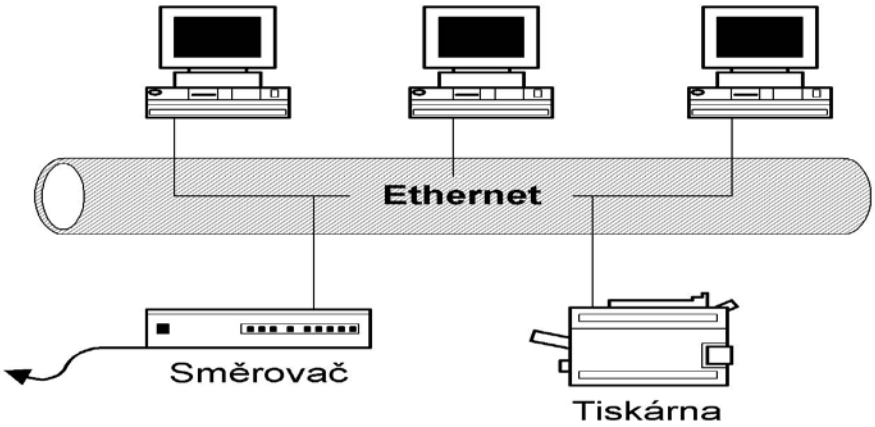
Uvedené normy IEEE byly převzaty později ISO. Z normy IEEE 802.2 tak vznikla norma ISO 8802-3, z normy IEEE 802.3 vznikla norma ISO 8802-3 atd.

4.1 Ethernet

Protokol Ethernet byl původně vyvinut firmami DEC, Intel a Xerox. Jeho varianta 600 MHz se označuje jako Ethernet II. Později byl Ethernet normalizován institutem IEEE jako norma

802.3. Tato norma byla převzata ISO a publikována jako ISO 8802-3. Formát rámců podle normy Ethernet II se mírně odlišuje od formátu ISO 8802-3. Postupem času vznikla norma IEEE 802.3u pro Ethernet na frekvenci 100 MHz (Fast Ethernet) a norma IEEE 802.3z pro frekvenci 1 GHz (gigabitový Ethernet).

Původní rozvod Ethernetu by prováděn tzv. tlustým koaxiálním kabelem označovaným 10BASE5. Koaxiální kabel, který mohl být dlouhý maximálně 500 metrů, tvořil jeden segment lokální sítě. Segment tlustého Ethernetu (jak se tomuto rozvodu často říkalo) byl většinou tvořen jedním kusem koaxiálního kabelu. Na koaxiální kabel byly napichovány transceivery, které se propojovaly kabelem na AUI-port ethernetové přídavné karty v počítači. AUI-port zpravidla používá konektor CANNON-15.
Označení 10BASE5 vyjadřuje, že se jedná o síť používající přenosovou frekvenci 10 MHz (ta je v případě Ethernetu rovná i teoretické přenosové rychlosti sítě).



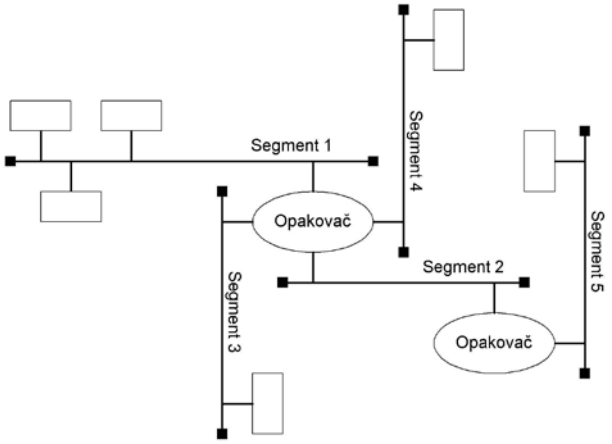
Masově se Ethernet rozšířil na tzv. tenkém koaxiálním kabelu. Tenký koaxiální kabel je u každé stanice přerušen a na oba konce přerušení je buď napájen nebo speciálními kleštěmi namáčknut BNC-konektor. Mezi dva BNC-konektory se vloží BNC-T-konektor – "odbočka k počítači". Třetí vývod BNC-konektoru se nasadí přímo na ethernetovou síťovou kartu v počítači (na její BNC-konektor). Existují však i transceivery pro tenký Ethernet, pak se BNC-T-konektor připojí na transceiver pro tenký Ethernet a kabel z transceiveru se připojí na AUI-port počítače.

Tenký Ethernet, označovaný jako 10BASE2 může být tvořen segmentem o maximální délce 185 metrů. Použijí-li se na segmentu stejné síťové přídavné karty, pak v případě některých karet je možné segment zvětšit až na 300-400 metrů.

4.1.1 Opakovač (receiver)

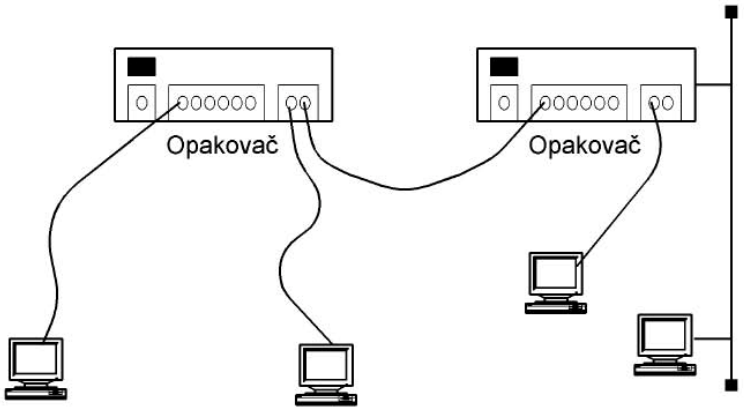
Délka segmentu LAN je tedy 500 (resp. 185 – 300) metrů. Rozsah LAN je možné zvětšit tím, že použijeme více segmentů, které mezi sebou propojíme tzv. **opakovači**. Opakovač je tvořen dvěma nebo více síťovými kartami, které jsou vzájemně propojeny. Objeví-li se nějaký datový rámec na jednom rozhraní, pak je automaticky zopakován na všechny ostatní. Opakovač může být osazen AUI i BNC porty, takže některé segmenty mohou používat tlustý a jiné tenký Ethernet.

Mezi dvěma opakovači může být použita i dvojice optických kabelů, tento typ Ethernetu se někdy označuje jako 10BASE-F. Délka optického propojení dvou opakovačů může být 1 km. Nyní si řekneme, že opakovač může být osazen i porty pro kroucenou dvojlinku. V případě kroucené dvojlinky je situace trochu odlišná. Kroucená dvojlinka (přesněji řečeno dva páry vodičů) je rozhraní mezi opakovačem a počítačem.

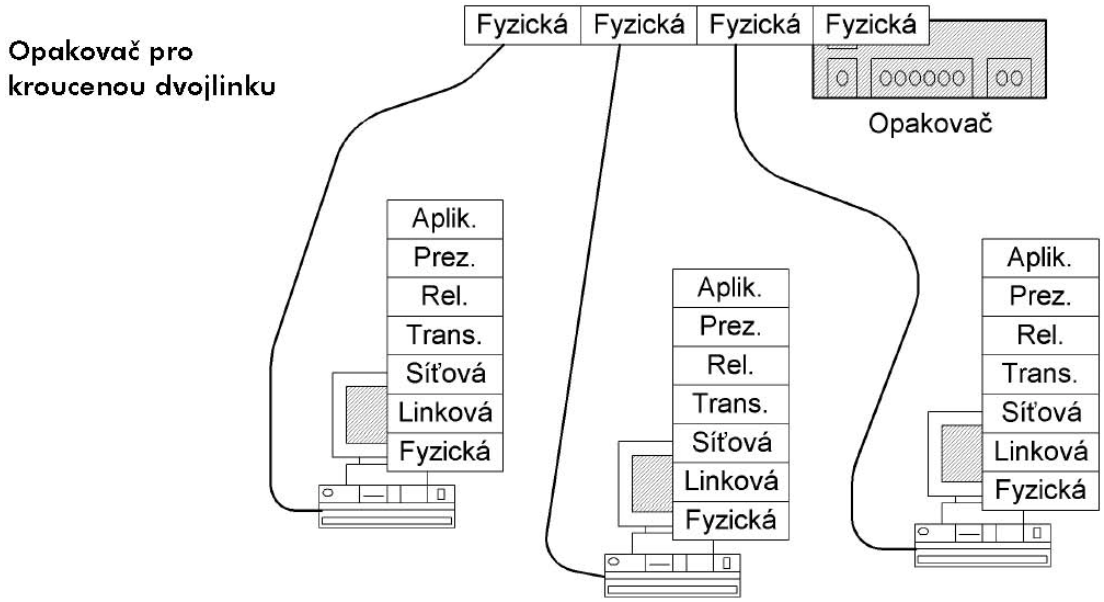


Spíše toto rozhraní připomíná rozhraní mezi transceiverem a AUI-konektorem (neobsahuje však napájení). V případě kroucené dvojlinky je jádrem sítě opakovač (na rozdíl od koaxiálního kabelu). Z opakovače se hvězdicovitě rozbíhají kroucené dvojlinky k jednotlivým počítačům. Opakovač pro kroucenou dvojlinku se označuje jako HUB (označení HUB se používalo pro aktivní prvek u sítí s hvězdicovou topologií). HUB může mít pochopitelně i BNC nebo AUI-porty.

Opakovač pro kroucenou dvojlinku (HUB)



Spoj mezi opakovačem a počítačem je tvořen dvěma páry kroucené dvoulinky (4 vodiče). Jedná se o duplexní spoj, kde pro každý kanál je určen jeden pár. Z hlediska počítače je tedy jeden pár "vysílání" a druhý pár "příjem". HUBy pro kroucenou dvojlinku je možné mezi sebou vzájemně propojovat. Ale pozor, co je pro jeden "vysílání", je pro druhý "příjem", takže v propojovací šňůře musí být páry překřížené (jako např. v případě nulových modemů). Většinou se však dodávají HUBy, kde jeden port je osazen přepínačem, který právě způsobí překřížení párů, takže stačí použít „normální" propojovací šňůru a připojit ji do portu s přepínačem a ten přepnout do vhodné polohy.



Ethernet na kroucené dvojlince se označuje jako 10BASE-T. Existuje i verze desetkrát rychlejšího Ethernetu označovaná 100BASE-TX a gigabitový Ethernet označovaný 1000BASE-CX. Pomocí opakovačů nelze kombinovat 10BASE-T, 100BASE-TX a 1000BASE-CX – propojit je lze až pomocí přepínače. Délka dvojlinky mezi opakovačem a stanicí je standardně do 100 metrů.

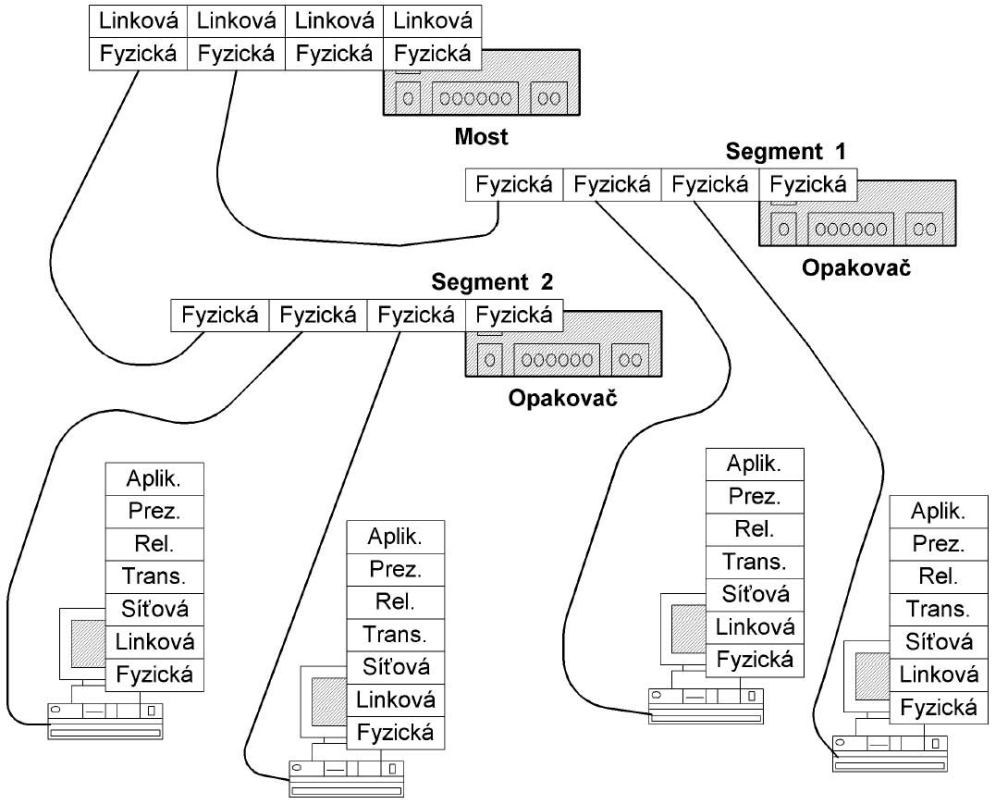
Z hlediska síťového modelu pracuje opakovač (HUB) na fyzické úrovni. Komunikace mezi počítači je v LAN osazené opakovači transparentní (průhledná), tj. počítače na LAN spolu komunikují, aniž by o opakovači věděly.

4.1.2 Most (bridge)

Oproti opakovači **most** také spojuje mezi sebou jednotlivé segmenty LAN, ale neopakuje mechanicky všechny rámce, které se na nějakém z jeho portů objeví. Most je realizován specializovaným počítačem, který má předávací tabulku. V tabulce je seznam všech linkových adres všech síťových rozhraní LAN. U každé adresy má poznamenáno, za kterým síťovým rozhraním mostu se nachází. Objeví-li se datový rámec na nějakém síťovém rozhraní mostu, pak se most podívá do datového rámce na adresu příjemce a z předávací tabulky zjistí, za jakým rozhraním se adresát nachází. Rámec pak zopakuje pouze do rozhraní, za kterým je adresát. V případě, že se adresát nachází za stejným rozhraním, pak jej neopakuje vůbec. Oběžníky se pochopitelně opakují do všech rozhraní.

Důležitým parametrem mostu je, jak velkou může mít předávací tabulku, tj. kolik na ní má paměti. Avšak kardinální otázkou je, jak takovou tabulku naplnit správnými údaji. Naskýtá se odpověď, že data do ní může pořídit správce LAN ručně. Možná, že vám to připadá jako směšné řešení, ale toto řešení je oblíbené v případě sítí, kde se klade velký důraz na bezpečnost. Pak správce LAN takovou tabulku přesně nastaví. Dnes se mosty doplňují i o další tabulku, která je obdobou předávací tabulky a která vyjadřuje, kdo kam nemůže.
Jak se ale předávací tabulka naplní automaticky? Algoritmus je velice jednoduchý. Most pracuje po zapnutí v podstatě jako opakovač, tj. opakuje vše na všechna rozhraní. Avšak každému příchozímu rámci se podívá na adresu odesílatele. Most ví, z jakého rozhraní rámec

přišel, takže si může jako novou položku do předávací tabulky uložit adresu odesílatele a příslušné rozhraní.



V lokální síti můžeme mít i více mostů. Předávání rámců mezi jednotlivými rozhraními mostu nemusí být tak rychlé jako u opakovače (může být delší doba odezvy). To otevírá cestu k tomu, aby dva mosty sítě byly propojeny např. sériovou linkou s modemy nebo radioreleovým spojem.

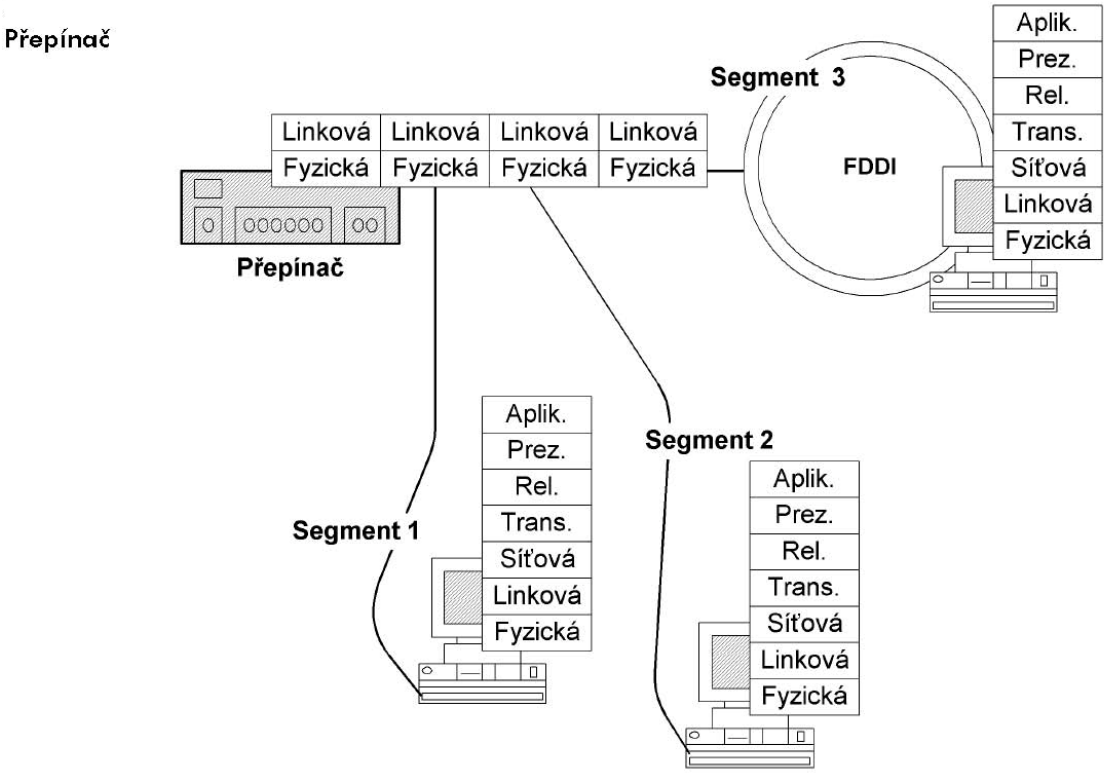
Jádrem jednotlivých segmentů LAN je opakovač. Jednotlivé segmenty jsou propojeny pomocí mostu. Na segment se pak umísťují počítače, které spolu více komunikují. Např. počítače jednoho oddělení. Na port mostu je užitečné připojit např. směrovač směřující do Internetu nebo na centrální server atp. Pomocí mostu lze tedy oddělit provoz mezi segmenty.

Jiným řešením je použít most s velkým počtem portů a nepoužít již opakovače pro jednotlivé segmenty sítě. Takovéto řešení se někdy nazývá přepínaný Ethernet. Jádrem přepínaného Ethernetu je inteligentní most, který v okamžiku, kdy zjistí, na které rozhraní má rámec opakovat, paralelně již začíná zpracovávat další rámec. Takovýto most se již označuje jako

4.1.3 Přepínač (switch)

Přepínačem se označují výkonnější mosty, které umí opakovat rámce nejen mezi jednotlivými segmenty Ethernetu, ale i např. mezi Ethernetem a Fast Ethernetem, mezi Ethernetem a FDDI atd. Přepínač musí umět nejenom změnit tvar rámce např. z Ethernetu na FDDI, ale i pokusit se překlenout rozdíl mezi přenosovými rychlostmi. Problém je totiž při přenosu dat mezi

rychlým segmentem (FDDI) a např. Ethernetem, kdy se musí směrovat na Ethernet takové množství dat, aby jej Ethernet dokázal odebírat.

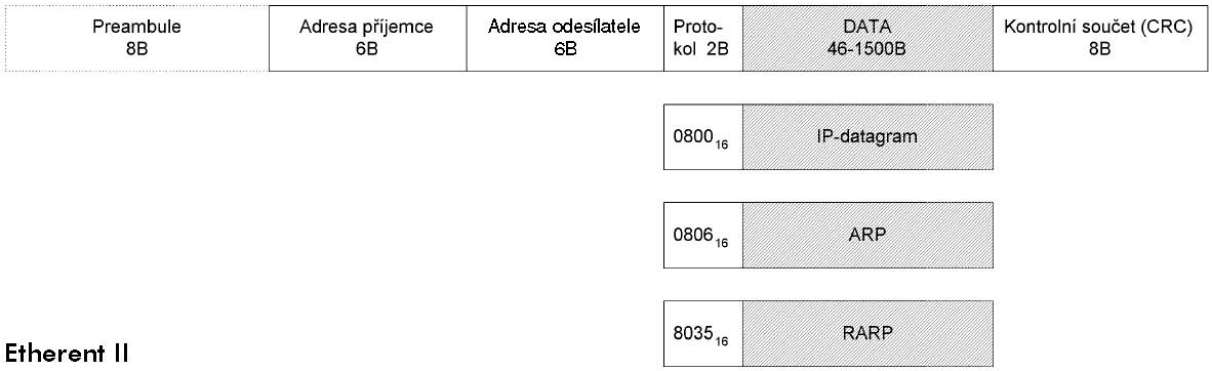


Rámce se musí ukládat do vyrovnávací paměti přepínače atd. Pro výměnu rámců mezi stanicemi se používá protokol CSMA/CD. V tomto protokolu jsou si všechny stanice na LAN rovny. Potřebuje-li nějaká stanice vysílat, pak si poslechne, zdali jiná stanice právě nevysílá. V případě, že médium není používáno (jiná stanice nevysílá), pak může stanice začít vysílat. Jenže v přibližně stejném okamžiku to mohlo napadnout dvě stanice najednou. Takže kromě toho, že stanice vysílá data, tak ještě připoslouchává, jestli nezačal vysílat současně někdo jiný. V případě, že současně začala vysílat jiná stanice, dochází ke kolizi. Při kolizi nemohou obě stanice okamžitě přestat vy sílat (aby kolize byla i ostatními detekovatelná), tak ještě nějakou dobu vysílají bezvýznamné znaky a pak se na náhodně zvolený časový interval odmlčí. Čím je na Ethernetu větší provoz, tím je větší pravděpodobnost vzniku kolizí. Rozumnou zátěží je využití sítě asi na 20 %. Takže u varianty Ethernetu s frekvencí 10 MHz kalkulujeme propustnost sítě asi na 2 Mb/s (tj. 256 KB/s. Pro ilustraci u FDDI (100 MHz) je výtěžnost 80-90 %, takže lze kalkulovat 90 Mb/s, tj. asi 11 MB/s.

Pokud ale máme segment, kde jsou pouze dvě stanice, tak na koaxiálním kabelu může dojít na takovémto segmentu také ke kolizi. Jiná je situace v případě, že segment o dvou stanicích je na kroucené dvoulince, která má samostatný pár pro vysílání a samostatný pár pro příjem. Síťové karty se pak na takovýchto segmentech přepnou do plně duplexního provozu, ve kterém může stanice současně přijímat i vysílat data. Takovýto segment se nazývá bezkolizním segmentem. Na bezkolizním segmentu můžeme dosahovat praktických přenosových rychlostí blížících se až k teoretickému maximu. Pokud jádrem LAN není opakovač, ale přepínač a jednotlivé stanice jsou připojeny bezkolizním segmentem, pak hovoříme o přepínaném Ethernetu. Bezkolizní segment je tvořen z jedné strany počítačem a z druhé strany rozhraním přepínače.

4.2 Ethernet II

Struktrura rámce protokolu Ethernet závisí na použité normě. Struktura rámce protokolu Ethernet II je znázorněna na obrázku.



Etherent II

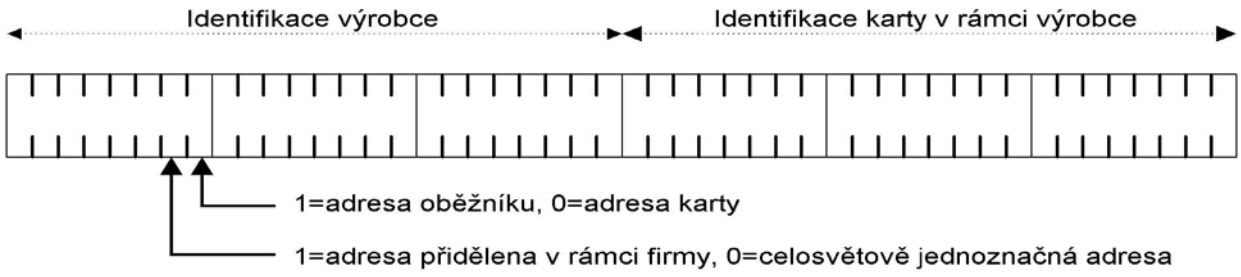
Ethernet II má na počátku synchronizační preambuli (součást fyzické vrstvy), při které se synchronizují všechny stanice přijímající rámec. Na konci rámce je kontrolní součet, ze kterého lze zjistit, nebyl-li rámec přenosem poškozen. Dále obsahuje šestibajtovou linkovou adresu příjemce a odesílatele, pole specifikující protokol vyšší vrstvy (tj. síťové vrstvy) a vlastní přenášená data (specifikace protokolů: IP verze 4, ARP a RARP je patrná z obrázku).

Datové pole musí být minimálně 46 bajtů dlouhé, takže v případě, že je potřeba přenášet méně dat, tak se datové pole zprava doplní bezvýznamnou výplní.

Fyzická adresa je šestibajtová. První tři bajty specifikují výrobce síťové karty a zbylé tři bajty kartu v rámci výrobce, takže adresy jsou celosvětově unikátní. Toto platí pouze pro tzv. globální adresy, které jsou celosvětově jednoznačné. Tyto adresy jsou uloženy v permanentní paměti síťové karty. Při inicializaci karty ovladačem lze kartě sdělit, aby nepoužívala tuto adresu, ale adresu jinou. V rámci firmy tak lze používat vlastní systém linkových adres. Tento mechanismus využíval např. protokol DECnet fáze IV.

Síťová karta může používat globálně jednoznačnou adresu nebo jednoznačnou adresu v rámci firmy. Kromě těchto jednoznačných adres existují ještě oběžníky. Všeobecný oběžník (adresa se skládá z 48 jedniček) je určen pro všechny stanice na LAN. Adresný oběžník (má nastaven nejnižší bit prvního bajtu na jedničku) je určen pouze některým stanicím na LAN, stanicím, které akceptují uvedenou adresu.

Nultý a první bit prvního bajtu linkové adresy mají specifický význam (viz obr.):



- Nultý bit specifikuje, zdali se jedná o jednoznačnou adresu nebo adresu oběžníku.
- První bit specifikuje, zdali se jedná o globálně jednoznačnou adresu.

Uveďme si příklad výpisu rámce protokolu Ethernet II z MS Network Monitoru:

```
+ FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
      ETHERNET: Destination address : 00000C31D211
            ETHERNET: .......0 = Individual address
            ETHERNET: ......0. = Universally administered address
      ETHERNET: Source address : 0010A4F18B3E
            ETHERNET: .......0 = No routing information present
            ETHERNET: ......0. = Universally administered address
      ETHERNET: Frame Length : 74 (0x004A)
      ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
      ETHERNET: Ethernet Data: Number of data bytes remaining = 60 (0x003C)
+ IP: ID = 0xAB06; Proto = ICMP; Len: 60
+ ICMP: Echo, From 195.47.37.200 To 194.149.105.18

00000: 00 00 0C 31 D2 11 00 10 A4 F1 8B 3E 08 00 45 00     ...1.......>..E.
00010: 00 3C AB 06 00 00 20 01 DB 1B C3 2F 25 C8 C2 95     .<.... ..../%...
00020: 69 12 08 00 42 5C 01 00 0A 00 61 62 63 64 65 66     i...B\....abcdef
00030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76     ghijklmnopqrstuv
00040: 77 61 62 63 64 65 66 67 68 69                       wabcdefghi
```

Preambule 8B	Adresa příjemce 6B	Adresa odesílatele 6B	Délka 2B	DATA 46-1500B	Kontrolní součet (CRC) 8B

Situace u protokolu ISO 8802-3 je poněkud složitější. Datový rámec protokolu ISO 8802-3 se liší pouze v jednom poli proti protokolu Ethernet II.

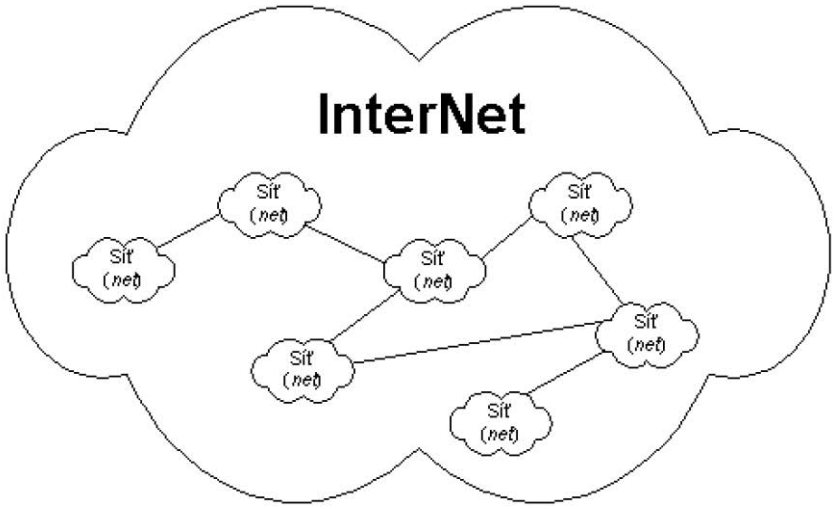
5. IP Protokol

Některé linkové protokoly jsou určeny pro dopravu dat v rámci lokální sítě, jiné linkové protokoly dopravují data mezi sousedními směrovači rozsáhlé sítě. IP-protokol na rozdíl od linkových protokolů dopravuje data mezi dvěma libovolnými počítači v Internetu, tj. i přes mnohé LAN.

Data jsou od odesílatele k příjemci dopravována (směrována) přes směrovače (*router*). Na cestě od odesílatele k příjemci se může vyskytnout cela řada směrovačů. Každý směrovač řeší samostatně směrování k následujícímu směrovači. Data jsou tak předávána od směrovače k směrovači. Z angličtiny se počeštil v tomto kontextu termín následující hop (*next hop*), jako následující uzel kam se data předávají. Hopem se rozumí buď následující směrovač, nebo cílový stroj.

IP-protokol je protokol, umožňující spojit jednotlivé lokální sítě do celosvětového Internetu. Od protokolu IP dostal také Internet své jméno. Zkratka IP totiž znamená InterNet Protocol, tj. protokol spojující jednotlivé sítě. Později, se místo InterNet začalo psát Internet a Internet byl na světě.

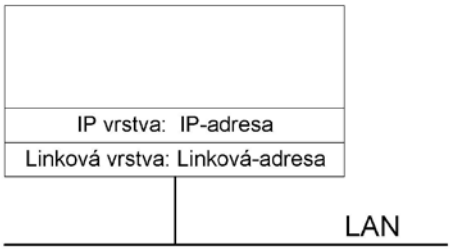
Obr. 5.1
InterNet



IP-protokol je tvořen několika dílčími protokoly:

- Vlastním protokolem IP.
- Služebním protokolem ICMP sloužícím zejména k signalizaci mimořádných stavů.
- Služebním protokolem IGMP sloužícím pro dopravu adresných oběžníků.
- Služebními protokoly ARP a RARP, které jsou často vyčleňovány jako samostatné, na IP nezávislé protokoly, protože jejich rámce nejsou předcházeny IP-záhlavím.

Zatímco v linkovém protokolu mělo každé síťové rozhraní (*network interface*) svou fyzickou (tj. linkovou) adresu, která je v případě LAN zpravidla šestibajtová, tak v IP-protokolu má každé síťové rozhraní alespoň jednu IP-adresu, která je v případě IP-protokolu verze 4 čtyřbajtová, a v případě IP-protokolu verze 6 šestnáctibajtová.

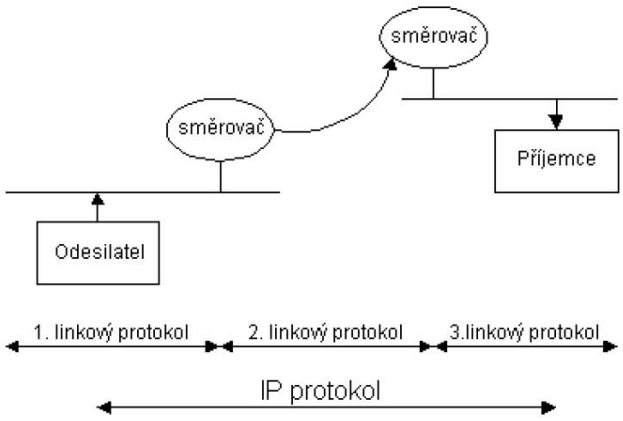


Základním stavebním prvkem WAN je směrovač (anglicky *router*), kterým se vzájemně propojují jednotlivé LAN do rozsáhlé sítě. Jako směrovač může sloužit běžný počítač s více síťovými rozhraními a běžným operačním systémem nebo specializovaná skříňka (*box*), do které nebývá běžně zapojen ani monitor ani klávesnice. Tyto specializované skříňky se u nás v Česku mezi odbornou veřejností nazývají routery a v tiskovinách směrovače.

Schopnost předávat datové pakety mezi síťovými rozhraními směrovače se nazývá jako předávání (*forwarding).* Zatímco u směrovačů je tato funkce požadována, tak u počítačů s klasickým operačním systémem (UNIX, OpenVMS, NT apod.) je někdy dotazováno, jak přinutit jádro operačního systému předávání zakázat.

Základní otázkou je: „Proč jsou třeba dva protokoly: linkový protokol a protokol IP? Proč nestačí pouze linkový protokol?“. Linkový protokol slouží pouze k dopravě dat v rámci LAN. Tj. k dopravě dat k nejbližšímu směrovači, ten z linkového rámce data „vybalí“ a „přebalí“ je do jiného linkového rámce.

Obr. 5.3
Linkové protokoly
a IP protokol

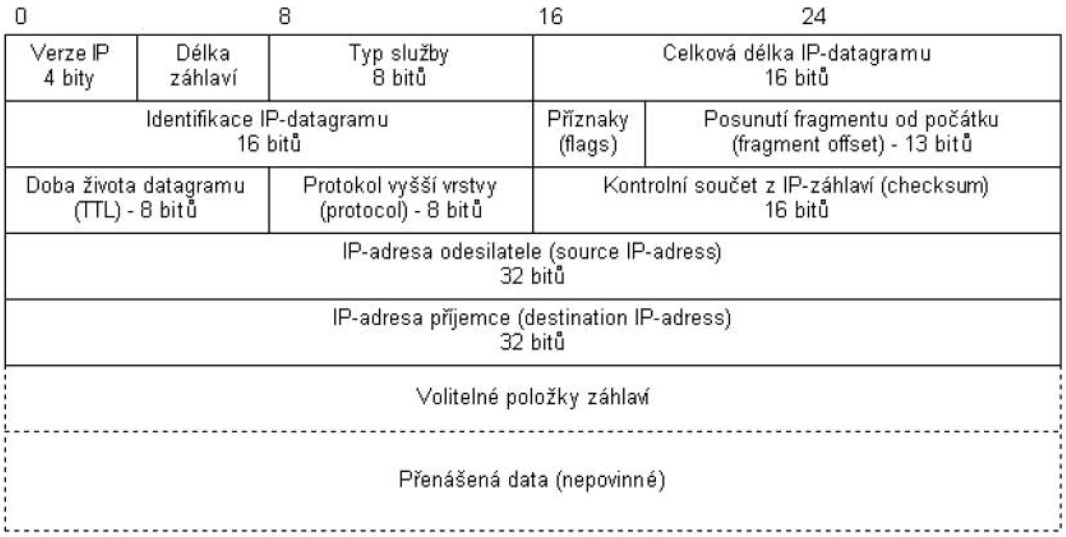


Obrázek znázorňuje, že linkový protokol dopravuje datové rámce pouze k následujícímu směrovači, kdežto IP-protokol dopravuje data mezi dvěma vzdálenými počítači rozsáhlé sítě (WAN). Zatímco obálka, kterou jsou na linkové vrstvě data obalena je na každém směrovači vždy zahozena a vytvořena nová, tak IP-datagram není směrovačem změněn. Směrovač nesmí změnit obsah IP-datagramu. Výjimkou je pouze položka TTL ze záhlaví IP-datagramu, kterou je každý směrovač povinen zmenšit alespoň o jedničku a v případě změny na nulu se IP-datagram zahazuje. Tímto mechanismem se Internet snaží zabránit nekonečnému toulání paketů Internetem.

Zatímco u linkových protokolů jsme základní přenášené kvantum dat označovali jako linkový rámec, tak u IP-protokolu je základní jednotkou přenášených dat IP-datagram.

5.1 IP-datagram

IP-datagram se skládá ze záhlaví a přenášených dat. Záhlaví má zpravidla 20 bajtů. Záhlaví však může obsahovat i volitelné položky a v takovém případě je záhlaví o ně delší.



- **Délka záhlaví** (*header length*) obsahuje délku záhlaví IP-datagramu. Maximální délka záhlaví IP-datagramu je tedy omezena tím, že položka délka záhlaví má k dispozici pouze 4 bity.
- **Typ služby** (*type of service – TOS*) je položka, která v praxi nenašla svého naplnění. Záměr spočíval v jistém nedostatku IP-protokolu jehož podstatou, je skutečnost, že v Internetu není zaručena šíře přenosového pásma mezi účastníky.
- **Celková délka** IP-datagramu (*total length*) obsahuje celkovou délku IP-datagramu v bajtech. Jelikož je tato položka pouze dvojbajtová, tak maximální délka IP-datagramu je 65535 bajtů. **Identifikace IP-datagramu** (*identification*) obsahuje identifikaci IP-datagramu, kterou do IP-datagramu vkládá operační systém odesílatele. Tato položka se společně s položkami **příznaky** (*flags*) a **posunutí fragmentu** (*fragment offset*) využívá mechanismem fragmentace datagramu.
- **Doba života datagramu** (*time to live – TTL*) slouží k zamezení nekonečného toulání IP-datagramu Internetem. Každý směrovač kladnou položku TTL snižuje alespoň o jedničku. Není-li už možné hodnotu snížit, IP-datagram se zahazuje a odesílateli IP-datagramu je tato situace signalizována protokolem ICMP.
- **Protokol vyšší vrstvy** (*protocol*) obsahuje číselnou identifikaci protokolu vyšší vrstvy, který využívá IP-datagram ke svému transportu. V praxi se nesetkáváme s případem, že by se komunikovalo přímo IP-protokolem. Vždy je použit protokol vyšší vrstvy (TCP nebo UDP) nebo jeden ze služebních protokolů ICMP či IGMP.
- **Kontrolní součet z IP-záhlaví** (*header checksum*) obsahuje kontrolní součet, avšak pouze ze záhlaví IP-datagramu a nikoliv z datagramu celého. Jeho význam je tedy omezený. Problém s kontrolním součtem spočívá v tom, že když směrovač změní nějakou položku v záhlaví IPdatagramu (např. TTL změnit musí), tak musí změnit i hodnotu kontrolního součtu, což vyžaduje jistou režii směrovače.

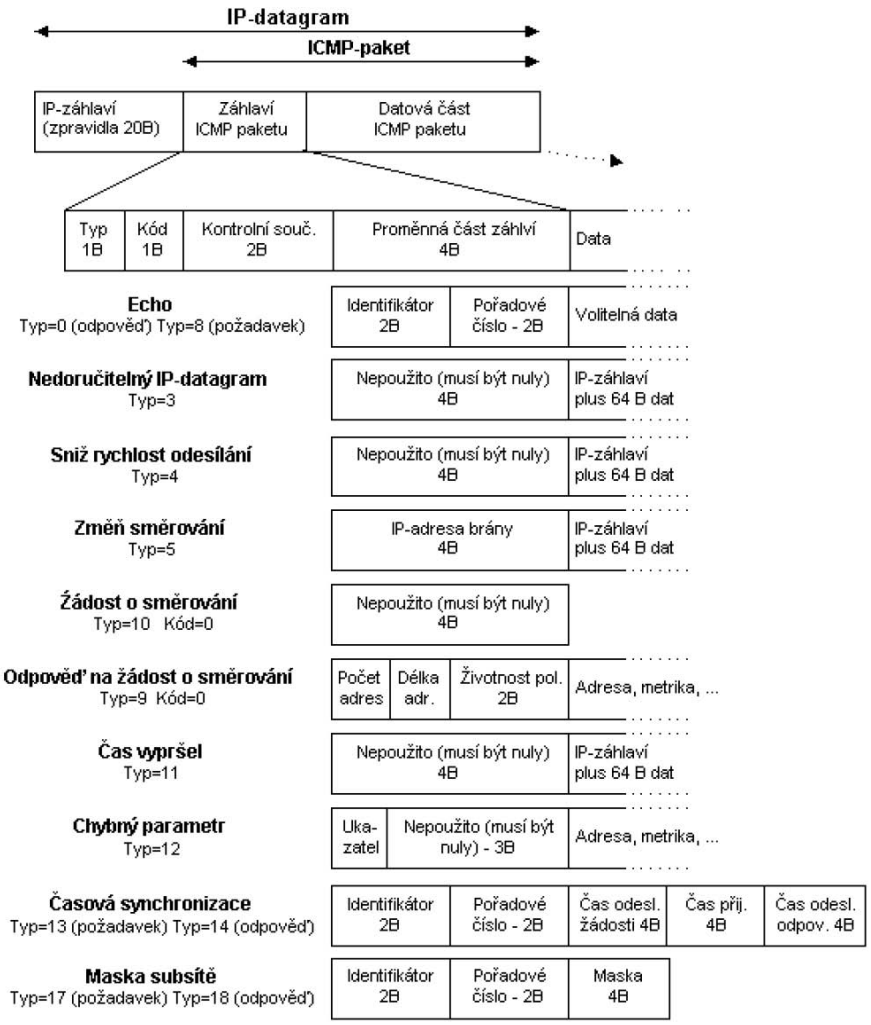
- **IP-adresa odesílatele** a **IP-adresa příjemce** (*source* and *destination adress*) obsahuje čtyřbajtovou IP adresu odesílatele a příjemce IP-datagramu.
- **Volitelné položky** jsou využívány ojediněle a zpravidla směrovače bývají nakonfigurovány tak, aby IP-datagramy s použitými volitelnými položkami byly bez okolků zahozeny.

5.2 ICMP Protokol

Protokol ICMP je služební protokol, který je součástí IP-protokolu. Protokol ICMP slouží k signalizaci mimořádných událostí v sítích postavených na IP-protokolu. Protokol ICMP svoje datové pakety balí do IP-protokolu, tj. pokud budeme prohlížet přenášené datagramy, pak v nich najdeme za linkovým záhlavím záhlaví IP-protokolu následované záhlavím ICMP paketu.

Protokolem ICMP je možné signalizovat nejrůznější situace, skutečnost je však taková, že konkrétní implementace TCP/IP podporují vždy jen jistou část těchto signalizací, a navíc z bezpečnostních důvodů mohou být na směrovačích mnohé ICMP signalizace zahazovány.

Obr. 5.10
ICMP-paket



5.2.1 Echo

Je jednoduchý nástroj protokolu ICMP, kterým můžeme testovat dosažitelnost jednotlivých uzlů v Internetu. Žadatel vysílá ICMP-paket „Žádost o echo“ a cílový uzel je povinen odpovědět ICMP-paketem „*Echo*“.
Všechny operační systémy podporující protokol TCP/IP obsahují program ping, kterým uživatel může na cílový uzel odeslat žádost o echo. Program ping pak zobrazuje odpověď.

5.2.2 Nedoručitelný IP-datagram

Nemůže-li být IP-datagram předán dále směrem k adresátovi, pak je zahozen a odesílatel je protokolem ICMP o tom uvědomen zprávou „Nedoručitelný IP-datagram“.

5.2.3 Sniž rychlost odesílání

Jestliže je síť mezi odesílatelem a příjemcem v některém místě přetížena, pak směrovač, který není schopen předávat dále všechny IP-datagramy, signalizuje odesílateli „Sniž rychlost odesílání“.

5.2.4 Změň směrování *(Redirect)*

Pomocí tohoto ICMP-paketu se provádí dynamické změny ve směrovací tabulce.

5.2.5 Žádost o směrování

Jedná se o poměrně novou záležitost, pomocí které nemusíme do směrovací tabulky počítačů na LAN ručně konfigurovat vůbec žádnou položku *default*. Počítač po svém startu vyšle oběžníkem „Žádost o směrování“ a směrovač mu odpoví ICMP-paketem.

5.2.6 Čas vypršel *(time exceeded)*

Tento typ zahrnuje dva velmi odlišné případy.
Pro kód=0 signalizuje, že položka TTL by byla na směrovači snížena na nulu, tj. že je podezření, že IP-datagram v Internetu zabloudil, proto bude zlikvidován.
Pro kód=1 signalizuje, že počítač adresáta není schopen v daném čase sestavit z fragmentů celý IP-datagram

5.2.7 Žádost o masku

Tímto ICMP-paketem může bezdisková stanice žádat o masku své sítě poté, co protokolem RARP obdržela svou IP-adresu. Tento mechanismus je v praxi dnes již málo běžný.

5.2.8 Časová synchronizace

Tímto ICMP-paketem se žádá cílový počítač o čas.

5.3 IGMP Protokol

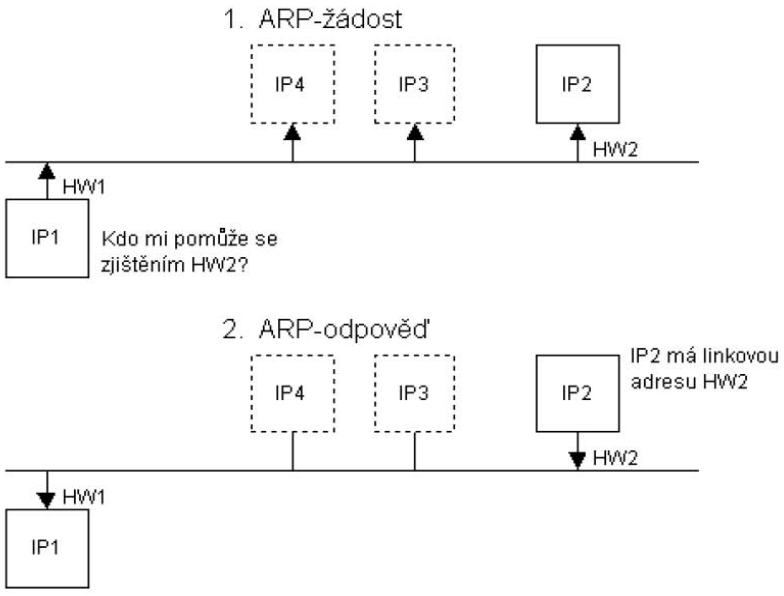
Protokol IGMP je podobně jako protokol ICMP služebním protokolem (podmnožinou) protokolu IP. Pakety IGMP-protokolu jsou baleny do IP-datagramů.

Protokol IGMP slouží k šíření adresných oběžníků (*multicasts*).

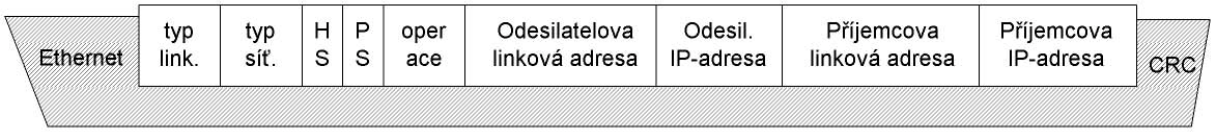
- **Pole MRT** (*Maximum response time*) se používá pouze v dotazu směrovače a specifikuje v desetinách sekundy čas do kterého musí členové skupiny opakovat požadavky na členství ve skupině. Ve všech ostatních případech má pole MRT hodnotu 0.
- **Kontrolní součet** se počítá stejně jako u protokolu ICMP.
- **Pole IP-adresa** adresného oběžníku je nulové u všeobecného dotazu, v ostatních případech specifikuje konkrétní IP-adresu adresného oběžníku.

5.4. Protokol ARP

Protokol ARP (*Address Resolution Protocol*) řeší problém zjištění linkové adresy protější stanice ze znalosti její IP-adresy. Řešení je jednoduché, do LAN vyšle linkový oběžník (linková adresa FF:FF:FF:FF:FF:FF) s prosbou: „Já stanice o linkové adrese HW1, IP-adrese IP1, chci komunikovat se stanicí o IP-adrese IP2, kdo mi pomůže s nalezením linkové adresy stanice o IP-adrese IP2? Stanice IP2 takovou žádost uslyší a odpoví. V odpovědi uvede svou linkovou adresu HW2.



ARP-paket je balen přímo do Ethernetu, tj. nepředchází mu žádné IP-záhlaví. Protokol ARP je vlastně samostatný, na IP nezávislý protokol. Proto jej mohou používat i jiné protokoly, které s protokoly TCP/IP nemají nic společného.



Žádost je posílána linkovým oběžníkem a v poli příjemcova linková adresa má vyplněny nuly. Odpověď pak má již vyplněna všechny pole a nemusí být odesílána oběžníkem. Je třeba zdůraznit, že v odpovědi je odesílatelem dotazovaný a příjemce tazatel (došlo k výměně příjemce a odesílatele).

ARP cache můžeme vypsat příkazem:

```
D:\> arp –a
Interface: 194.149.104.121
Internet Address Physical ADRESS Type
194.149.104.126 00-60-3e-1d-90-01 dynamic
10.1.1.1 00-01-11-11-ff-08 static
```

V ARP cache mohou být položky získané ARP dotazem, ty jsou typu dynamic. Do ARP cache můžeme také zapsat položky explicitně příkazem arp. Takové položky jsou typu static. Rovněž je možné položky ARP cache příkazem arp rušit.

Příklad vložení statické položky:

```
D:\> arp –s 10.1.1.1 00-01-11-11-ff-08
```

Příklad zrušení položky

```
D:\> arp –d 10.1.1.1
```

Jak dlouho zůstávají dynamické položky v ARP cache? Tento interval je parametrem jádra operačního systému. Nejčastěji mají položky dobu života 20 minut.

5.5 RARP

Protokolem ARP je také možné odeslat žádost s vyplněnou IP-adresou odesílatele i příjemce a také s oběma vyplněnými linkovými adresami. Takovou žádost je možné chápat jako: „Neexistuje náhodou na LAN ještě jiná stanice, která používá stejnou IP-adresu jako já?". V případě, že se obdrží odpověď, tak se uživateli signalizuje zpráva „*Duplicate IP address sent from Ethernet address xx:xx:xx:xx:xx:xx*". To pochopitelně signalizuje chybu v konfiguraci jedné ze stanic používajících tuto adresu.

Zatímco protokol ARP slouží k překladu IP-adres na linkové adresy reverzní ARP označované jako RARP slouží k překladu linkové adresy na IP-adresu. Avšak proč takový překlad provádět?

Smysl protokolu RARP je u bezdiskových stanic. Bezdisková stanice (tenký klient) po svém zapnutí nezná nic jiného než svou linkovou adresu (tu má uloženu výrobcem v paměti ROM). Po svém zapnutí se potřebuje dozvědět svou IP-adresu. Proto do LAN vyšle oběžník s prosbou: „Já mám linkovou adresu HW1, kdo mi řekne, jakou mám IP-adresu". Protokol RARP se v praxi téměř nepoužívá, nahradil jej protokol DHCP, který je komplexnější.

6. IP adresa

Protokol IP verze 4 (dnes nejrozšířenější) používá IP-adresu o délce čtyři bajty. IP-adresa adresuje jednoznačně síťové rozhraní systému. Anglicky se takováto jednoznačná adresa nazývá *unicast*. Pokud má systém více síťových karet (více síťových rozhraní) a na všech je provozován protokol IP, pak každé rozhraní má svou IP adresu.

Je možná i opačná varianta, kdy na jedné síťové kartě (fyzicky jednom síťovém rozhraní) podporujeme několik IP-adres. První adresa se obvykle nazývá primární a další adresy pak sekundární nebo aliasy. Využití sekundárních IP-adres je běžné např. pro WWW-servery, kdy na jednom počítači běží WWW servery několika firem a každý se má tvářit jako samostatný WWW-server.

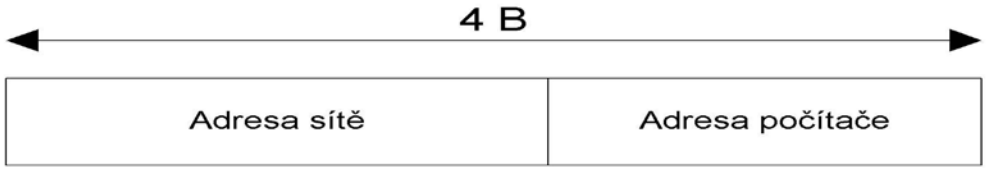
V praxi se však využívání sekundárních IP-adres pro WWW-servery považuje za plýtvání – používají se tzv. virtuální WWW-servery, kdy mnoha WWW-serverům stačí jedna společná IP-adresa. Specifikace serveru se pak provádí na aplikační úrovni v protokolu http (pomocí hlavičky *host*).

Jelikož má většina počítačů jedno síťové rozhraní, tak se přeneseně místo IP-adresa rozhraní říká IP-adresa počítače. IP-adresa je tvořena čtyřmi bajty. IP-adresa se zapisuje notací, kde jednotlivé bajty se mezi sebou oddělují tečkou. Rozeznáváme:

- Dvojkovou notaci, kde jednotlivé bity každého bajtu se vyjádří jako dvojkové číslo, např.: 10101010.01010101.11111111.11111000
- Desítkovou notaci – čtyři osmiciferná dvojková čísla se převedou do desítkové soustavy, tj. pro náš příklad: 170.85.255.248
- Šestnáctkovou notaci – jednotlivé bajty IP-adresy se vyjádří šestnáctkově (hexadecimálně), tj. náš příklad: AA.55.FF.F8

IP-adresa se skládá ze dvou částí:

- Adresy (lokální) sítě.
- Adresy počítače v (lokální) síti.



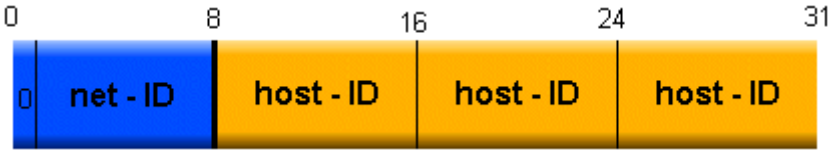
Kolik bajtů z IP-adresy tvoří adresu sítě, určují počáteční bity prvního bajtu IP-adresy. IP-adresy se dělí do pěti tříd:

- Třída A. V třídě A máme 126 sítí (0 a 127 mají zvláštní význam). V každé síti je 2^{24} - 2 adres pro počítače (adresy tvořené samými nulami a samými jedničkami mají zvláštní význam).
- Třída B. Můžeme mít celkem 2^{14} sítí a v každé síti 256 - 2 počítačů.
- Třída C. Můžeme mít 2^{22} sítí a v každé síti 128 - 2 počítačů.

- Třída D, kde nejvyšší čtyři bity prvního bajtu mají hodnotu 1110_2. Zbytek IP-adresy se pak už nedělí na adresu sítě a adresu počítače. Zbytek IP-adresy tvoří adresný oběžník (*multicast).*
- Třída E tvořící zbytek adres je tč. rezervou.

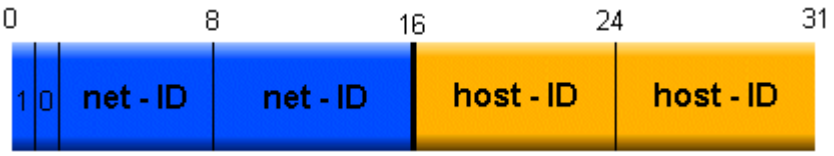
Třída	1. bajt IP-adresy	2. bajt IP-adresy	3. bajt IP-adresy	4. bajt IP-adresy
A	0sssssss 1-127$_{10}$	adresa počítače		
B	10ssssss 128-191$_{10}$	ssssssss	adresa počítače	
C	110sssss 192-223$_{10}$	ssssssss	ssssssss	adresa počítače
D	1110mmmm 224-239$_{10}$	mmmmmmmm	mmmmmmmm	mmmmmmmm
E	>239$_{10}$			

6.1Třída A



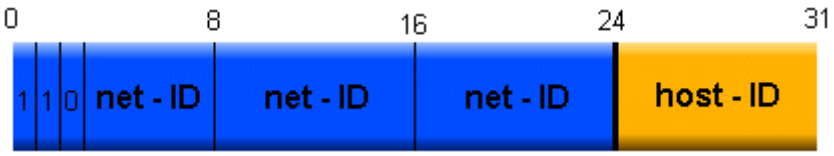
IP adresu třídy A v České republice nikdo nemá. Mají ji hlavně nadnárodní společnosti, vládní organizace USA atp. Dovoluje adresování jen 128 sítí, ale v každé z nich může být až 16 miliónů počítačů. První byte může v desítkové soustavě nabývat hodnot od 1 do 126.

6.2 Třída B



Třída B umožňuje adresovat už 16 tisíc sítí a 65 tisíc počítačů. V Čechách ji mají významné organizace. První byte v desítkové soustavě nabývá hodnot od 128 - 191. Například:

6.3 Třída C



IP adresou třídy C dokážeme adresovat až 2 milióny sítí. V každé síti může být 255 počítačů. IP adresa třídy C je v Čechách nejpoužívanější.

6.4 Speciální IP-adresy

IP-adresa je obecně tvaru:

síť.počítač

kde síť je v případě třídy A tvořena jedním bajtem, v případě třídy B tvořena dvěma bajty a v případě třídy C tvořena třemi bajty.

Jsou–li na místě sítě nebo počítače binárně samé nuly (00…0), pak se to vyjadřuje slovem „tento". Jsou-li tam naopak samé jedničky (11…1), pak se to vyjadřuje slovem „všichni" (či oběžník).

Typ adresy	**Význam**
0.0.0.0	Tento počítač na této síti.
00…0.počítač	Počítač na této síti
síť.00…0	Adresa sítě jako takové
síť.11…1 (samé jedničky na místě adresy počítače)	Všeobecný oběžník *(broadcast)* zasílaný do sítě síť – možno poslat i na vzdálenou síť
11…1 (samé jedničky, tj. desítkově 255.255.255.255)	Všeobecný oběžník na lokální síti *(limited broadcast)* – směrovače jej nepředávají dále
127.cokoliv	Programová smyčka *(loopback)* – nikdy neopouští počítač, zpravidla se používá adresa 127.0.0.1

Každé síťové rozhraní (*interface*) má alespoň jednu jednoznačnou adresu (*unicast*), kromě toho celý systém má jednu adresu programové smyčky 127.0.0.1. Adresa 127.0.0.1 není v Internetu jednoznačná, protože ji má každý počítač (*host*).

Příklad: Síť 192.168.6.0 je síť třídy C. Jaké jsou všechny běžící počítače na této síti? Řešení je jednoduché. Všeobecný oběžník (*broadcast*) na této síti má IP-adresu 192.168.6.255. Po vydání příkazu:

```
ping 192.168.6.255
```

všechny běžící počítače na této síti odpoví ICMP-paketem echo. Implementace příkazu ping firmou Microsoft bohužel nezobrazí všechny odpovědi, většina ostatních implementací nám všechny odpovědi zobrazí, takže zjistíme, které počítače na síti běží.

6.5 Síťová maska

Síťová maska se používá pro určení adresy sítě. Adresa sítě je částí IP adresy. Síťová maska určuje, které bity v IP-adrese tvoří adresu sítě. Síťová maska je opět čtyřbajtové číslo. Toto číslo vyjádřené v dvojkové soustavě má v bitech určujících adresu sítě jedničky a v ostatních bitech nuly.

Princip síťové masky se dobře pochopí, používáme-li dvojkovou notaci. Jednotlivé třídy sítí používají jako adresu sítě různě dlouhou část IP adresy. Třída A používá pro adresu sítě první bajt. Čili standardní síťová maska pro adresy třídy A má v prvním bajtu samé jedničky a ve zbylých třech bajtech samé nuly:

`11111111.00000000.00000000.00000000`

což vyjádřeno v desítkové soustavě je:

`255.0.0.0` (šestnáctkově ff.00.00.00)

Obdobně standardní síťová maska pro třídu B je desítkově:

`255.255.0.0` (šestnáctkově ff.ff.00.00)

Konečně pro třídu C:

`255.255.255.0` (šestnáctkově ff.ff.ff.00).

Síťové masky odpovídající třídám A, B a C se nazývají standardní síťové masky.

Síťová maska slouží k řešení úlohy: Jak určit adresu sítě, na které leží počítač o IP adrese:

`170.85.255.248`, tj. dvojkově `10101010.01010101.11111111.11111000`

Řešení je jednoduché: Nejprve se podíváme do tabulky tříd IP-adres a zjistíme, že naše adresa je třídy B. Používáme standardní síťovou masku, pak maska pro třídu B je:

```
11111111.11111111.00000000.00000000
```

Vynásobíme-li nyní IP-adresu bit po bitu se síťovou maskou, pak získáme adresu sítě:

```
10101010.01010101.11111111.11111000
11111111.11111111.00000000.00000000
_____________________________________
10101010.01010101.00000000.00000000
```

Výsledek převedeme do desítkové soustavy a zjistíme, že počítač leží na síti `170.85.0.0`.

6.6 IP-adresy v intranetu

Použití technologie Internetu uvnitř uzavřené firemní sítě se nejprve označovalo internet (s malým i), později se objevilo slovo intranet, které se uchytilo.

IP-adresy musí být v Internetu přidělovány celosvětově jednoznačně. Ještě před časem mnohé podniky budovaly svou uzavřenou podnikovou síť na bázi protokolu TCP/IP a ani ve snu je nenapadlo, že by se někdy připojovaly k Internetu. I zvolili si naprosto libovolné adresy vlastních sítí. Dnes chtějí tyto sítě propojit přes firewall do Internetu a zjišťují, že stejné adresy už v Internetu někdo používá. Jsou nuceni své sítě přečíslovat, což je velice nepříjemná operace.

Většinou firmy používající v intranetu adresy, které kolidují s adresami v Internetu, z počátku hledají nějaká netradiční řešení jak se vyhnout přečíslování intranetu. Takovým řešením je např. NAT (*Network Address Translator*), avšak tato řešení přinášejí jiná negativa, proto po zbytečně vynaloženém úsilí firmy stejně nakonec přistoupí k přeadresování celého intranetu.

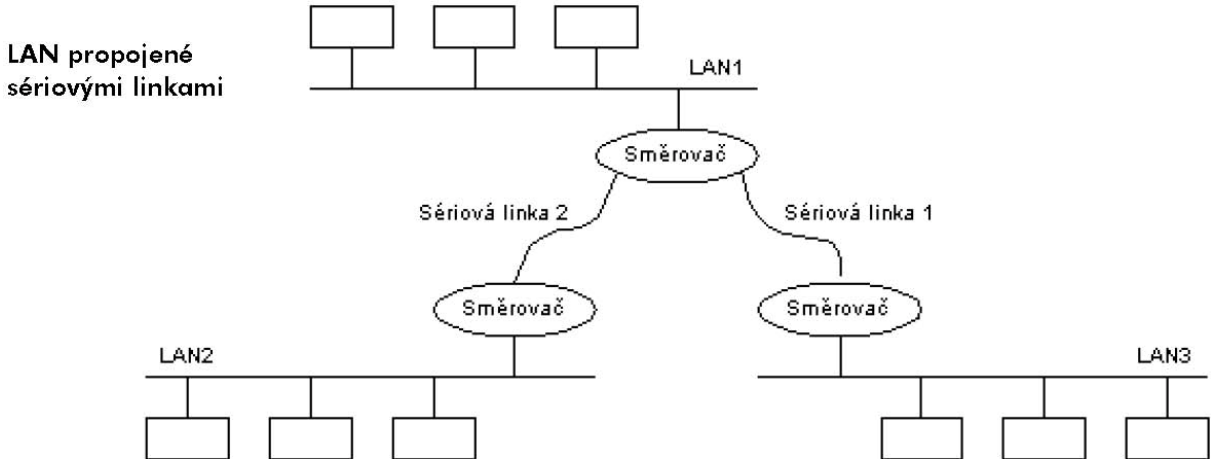
Pro uzavřené podnikové sítě si zvolte IP-adresy sítí podle RFC1918 uvedené v tabulce.

Třída A	10.0.0.0/8	10.0.0.0 až 10.255.255.255
Třída B	172.16.0.0/12	172.16.0.0 až 172.31.255.255
Třída C	192.168.0.0/16	192.168.0.0 až 192.168.255.255

Použití těchto adres navíc zvyšuje bezpečnost, protože v Internetu jsou nepoužitelné (stovky podniků je používají na svých uzavřených sítích). O přidělení adres v těchto rozsazích není třeba nikoho žádat. Častou otázkou je jak to poskytovatelé Internetu dělají, že tyto adresy nelze použít, oni je nějak filtrují? Filtrace není třeba, oni je prostě jen nemají ve směrovacích tabulkách, takže je nemohou dopravovat.

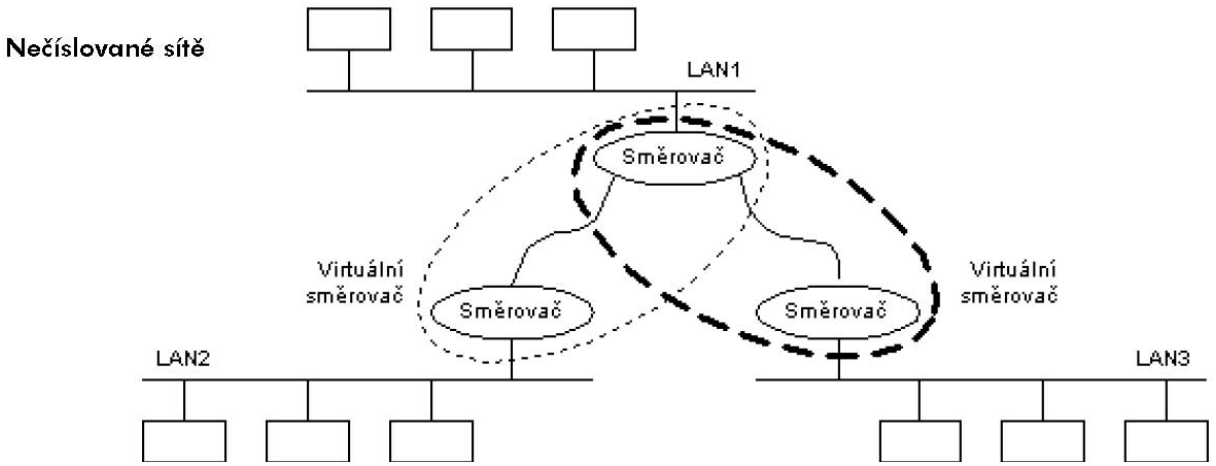
6.7 Nečíslované sítě

Zamysleme se nyní nad sériovými linkami spojujícími LAN. Pro každou linku potřebujeme subsíť o minimálně čtyřech IP-adresách (adresa sítě, oběžník na síti a dvě adresy pro síťová rozhraní na směrovačích).



Z obrázku je patrné, že kromě tří intervalů IP-adres pro lokální sítě budeme potřebovat další adresy pro sítě tvořené sériovými linkami. Na první pohled je vidět, že by bylo efektivní pro sériové linky nepotřebovat další adresu sítě.

Současné směrovače umí na sériových linkách vytvořit „nečíslovanou“ síť (*unnumbered interface*), tj. protější směrovače se chovají jako jeden virtuální směrovač. Každý fyzický směrovač pak tvoří polovinu virtuálního směrovače. Virtuální směrovač má pouze dvě rozhraní – jedno pro každou LAN.



Pro sériové linky tak není třeba plýtvat IP-adresami.

6.7.1 Dynamicky přidělované adresy

Má-li síť již interval IP-adres přidělen, pak můžeme začít s přidělováním adres jednotlivým síťovým rozhraním na této síti.

Jsou dvě možnosti:

- Staticky (trvale) přidělit IP-adresu (pomocí nastavení síťového rozhraní).
- Dynamicky (na dobu připojení) přidělit IP-adresu (pomocí DHCP serveru).

Dynamické přidělování přináší výhodu i v tom, že je potřeba jen tolik IP-adres, kolik je současně přihlášených uživatelů. Dynamické přidělování adres řeší aplikační protokol DHCP. Protokol DHCP vychází ze zkušeností a částečně v sobě zahrnuje i podporu starších protokolů z této oblasti, tj. protokolů RARP, DRARP a BOOTP. Blíže viz RFC-1531.
V protokolu DHCP žádá klient DHCP-server o přidělení IP-adresy (případně o další služby). DHCP-server může být realizován jako proces na počítači s operačním systémem UNIX, Windows NT atp. Nebo DHCP-server může být realizován i jako součást směrovače.

6.7.2 NAT

Zkratka pro **N**etwork **A**ddress **T**ranslation, tedy překlad IP adres (někdy nazývaný také jako IP maškaráda). Používá se k úspoře IP adres v současném internetu. Většinou je realizován například na směrovači (routeru) připojujícím lokální síť k síti poskytovatele připojení. V lokální síti mohou pak být použity libovolné adresy (nejčastěji se jedná o adresy z neveřejného rozsahu).

Když počítač z lokální sítě odesílá paket do vnější sítě (např. internetu), odešle jej se svou zdrojovou IP adresou a portem. Při průchodu NATem jsou však zdrojové IP adresy v paketech přepsány na veřejnou IP adresu NATu. Také je přepsáno číslo zdrojového portu na port, který NAT odesílajícímu počítači přidělil. NAT si zároveň uloží toto přidělení do své převodní tabulky (v které jsou uloženy veškeré informace o vzájemném mapování jednotlivých adres).
Když pak následně dorazí odpověď od vzdáleného počítače, hlavičky paketů jsou znovu přepsány – tentokrát je cílová adresa a port přepsána příslušnými informacemi z převodní tabulky (lokální IP adresou a portem příslušného počítače) a paket je předán dál k doručení do lokální sítě.

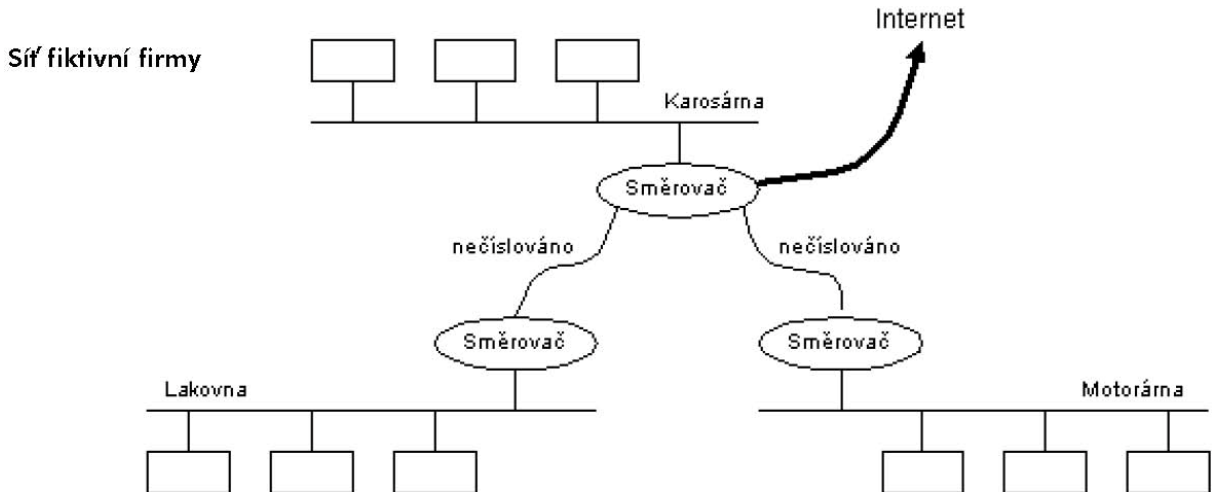
NAT je ovšem "velkým zlem", jelikož s počítači za NATem nelze z venku přímo navázat spojení a jsou tak narušeny základní principy internetu (všechny počítače mají být jednoznačně adresovány a kdokoliv s kýmkoliv má mít možnost komunikovat přímo).
NAT je také těžko slučitelný s některými protokoly vyšších vrstev (jako např. FTP, H.323, SIP, atd.) a příslušné služby pak za NATem nemusí dobře fungovat (respektive aby fungovaly, musí být na NATu použit connection tracking rozumějící daným vyšším protokolům).

6.8 Adresní plán

Každá firma, která se chce připojit k Internetu, si musí nejprve udělat adresní plán. Ten se obvykle skládá ze dvou částí.
Jednak ze schematického znázornění propojení jednotlivých LAN do WAN a jednak ze seznamu jednotlivých LAN s odhadovaným počtem síťových rozhraní na LAN.

Adresní plán by měl obsahovat rezervu s výhledem na příští a přespříští rok. Jako rezerva se běžně bere dvojnásobek současného stavu. Adresní plán se pak zasílá jako požadavek poskytovateli Internetu, kterého tím žádáme o příslušný počet IP-adres.

Příklad: Máme připojit k Internetu firmu používající 3 lokální sítě: karosárna, lakovna a motorárna (nikdy se poskytovatel nespokojí s žádostí typu: tři sítě A, B a C – vždy se musí jednat o konkrétní požadavek).



V karosárně máme 8 počítačů s výhledem na 16, v motorárně 9 počítačů s výhledem na 18 a v lakovně je 20 počítačů s výhledem na 40 počítačů.

LAN	Současný stav	Příští rok	Za 2 roky	Nejbližší možnost pro LAN	Požadováno
Karosárna	8	10	16	32 (16 nelze, protože je třeba adresa pro subsíť a oběžník)	32
Lakovna	9	15	18	32	32
Motorárna	20	35	40	64	64

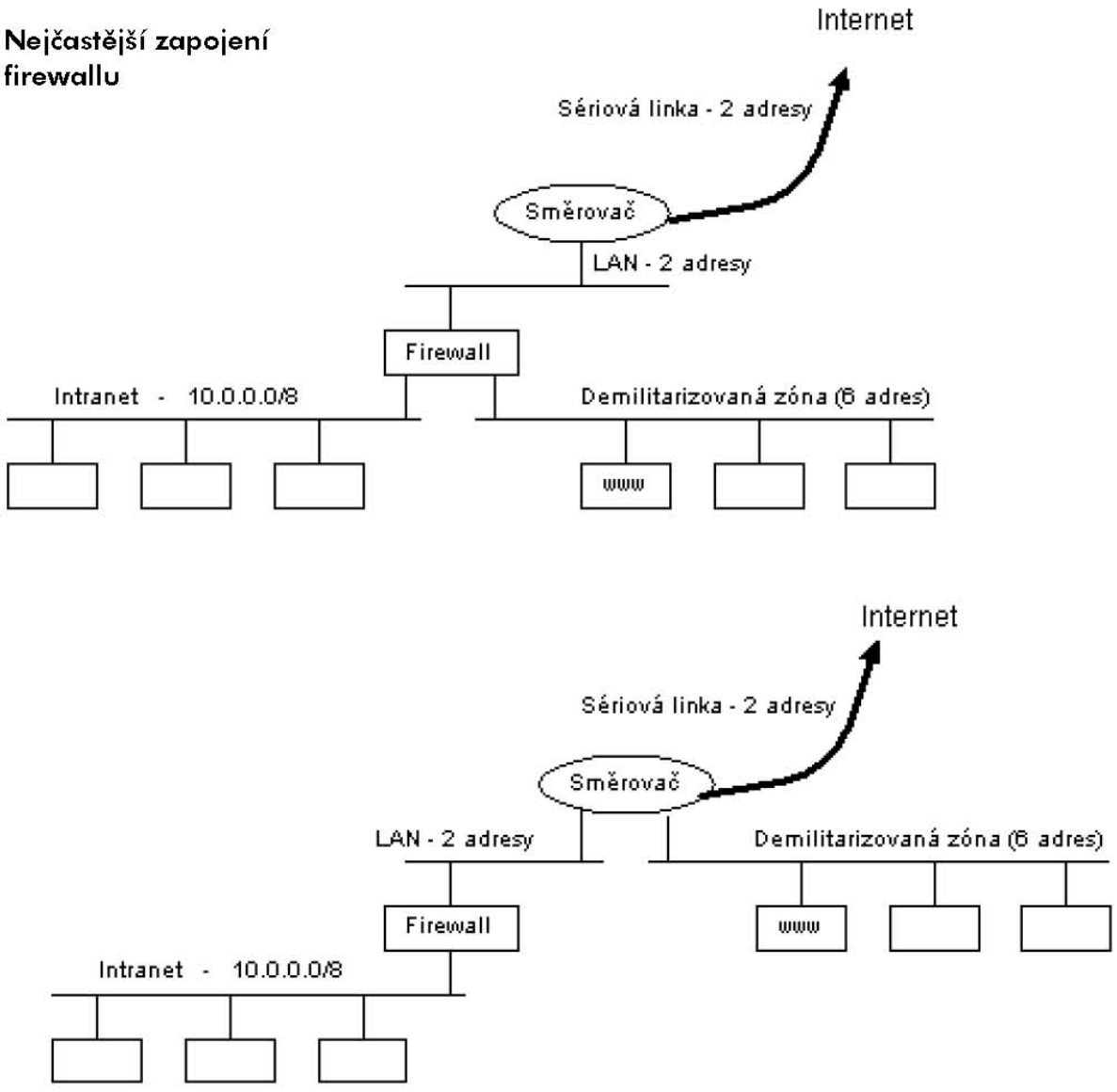
Požadujeme na poskytovateli přidělit 128 IP-adres pro tři subsítě. V případě, že by těchto 128 adres mělo tvořit jeden celek – „supersíť", pak nemůžeme požadovat supersíť o 128 adresách, protože jedna LAN by využívala nejednoznačnou subsíť sítě C, v takovém případě je třeba žádat celou síť třídy C, tj. 256 IP-adres.

To aby všechny LAN z hlediska poskytovatele tvořily jeden celek ("supersíť"), je vyžadováno zejména v případě, kdy firma využívá pro připojení k Internetu komutovaný spoj. Přitom komutovaným spojem může být zálohována i pevná linka (*dialup backup*).
Příklad neřešil problém sériové linky propojující firmu s Internetem. To je třeba projednat vždy s poskytovatelem. Možná, že se vám zdá, proč připojovat jednotlivé provozy do Internetu. Větší a velké firmy se vyznačují tím, že nepotřebují více jak 16 IP-adres. Většinou si vyberou z některého ze zapojení firewallu znázorněného na obrázku:

Demilitarizovaná zóna je LAN, která je přístupná z Internetu, proto musí mít i oficiální IP-adresy. Demilitarizovaná zóna má tu výsadu, že je to jediná síť v Internetu, která je alespoň částečně dostupná z intranetu.

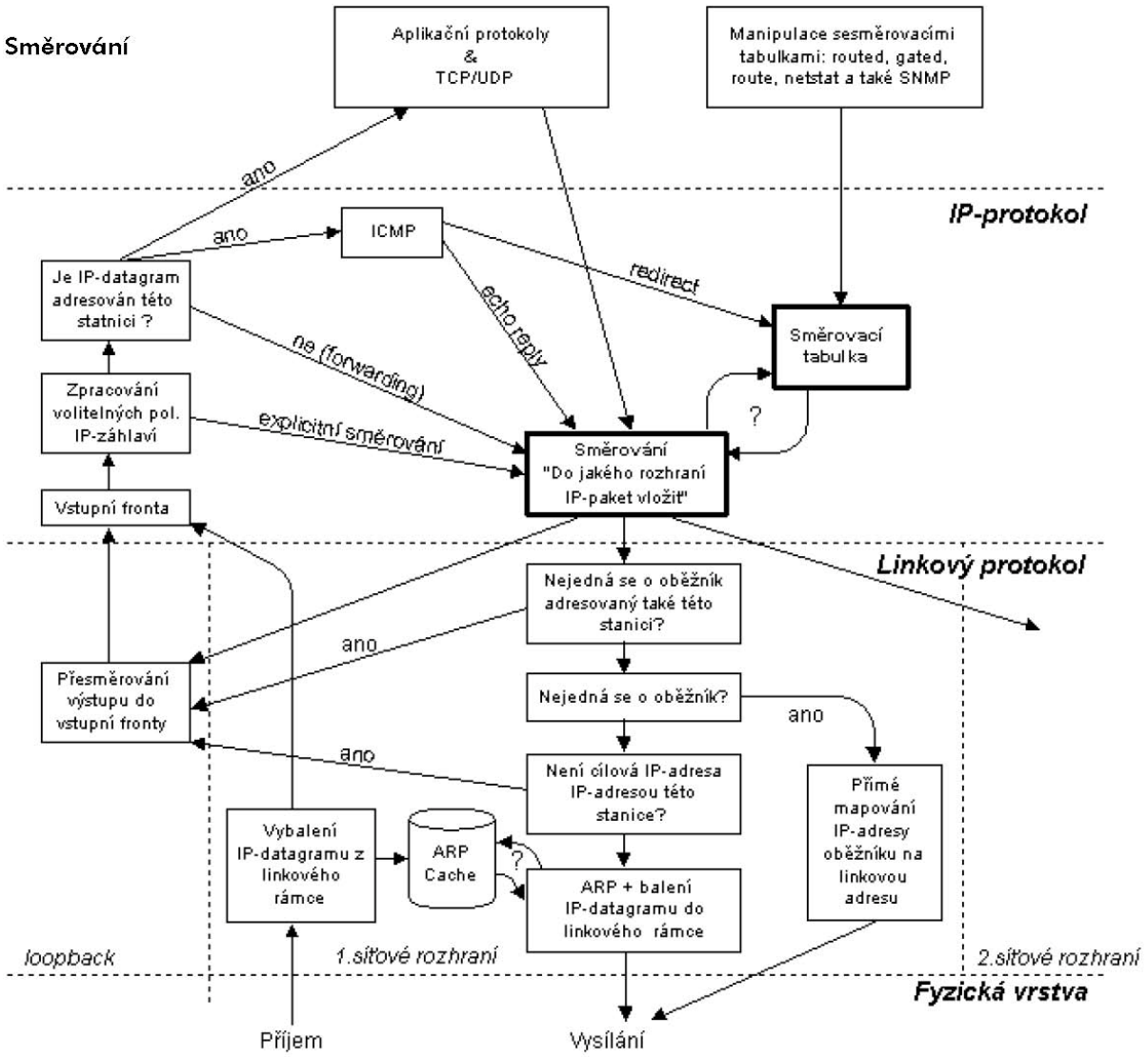
Nejvýše je tedy třeba IP-adresy pro:

- Síť o čtyřech IP-adresách pro sériovou linku vedoucí do Internetu (může se i jednat o nečíslovanou síť).
- Síť pro „internetovskou" stranu firewallu též stačí o čtyřech adresách.
- Síť pro demilitarizovanou zónu, kde je např. firemní WWW-server. Nezažil jsem, aby na demilitarizované zóně bylo více jak 10 počítačů.



7. Směrování

Směrování IP-datagramů (*IP routing*) a předávání IP-datagramů (*IP forwarding*) jsou dva procesy, na kterých Internet stojí. Základní schéma směrování je zobrazeno na obrázku.



Z obrázku je také patrné, že při zpracování vstupů v některých případech operační systém informace automaticky předává na výstup (do procesu směrování), tj. aplikační programy do tohoto předávání nezasahují. Jedná se zejména o:

- Explicitní směrování (*source routing*).
- Předávání (*forwarding*).
- Požadavek o echo (*echo request*).
- Přesměrování (*redirect*).

Operační systémy mají v jádře vždy nějaké parametry, kterými lze takováto automatické zpracování IP-datagramů zakázat. Velice častý je např. zákaz explicitního směrování, naopak zpracování požadavku o echo se zakazuje zřídka.

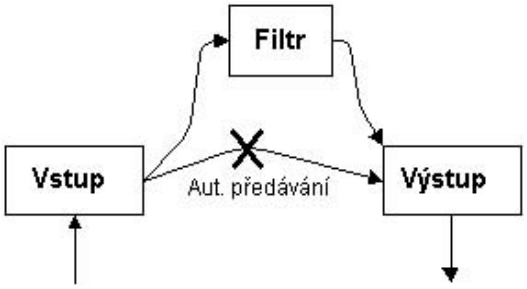
7.1 Předávání a filtrace

Předávání umožňuje stanici pracovat jako směrovač. Pokud stanice zjistí, že IP-datagram není adresován pro ni, pak se jej pokouší předat dále, tj. odeslat jako odesílá své IP-datagramy. Předávání lze i zakázat – to bývá volba jádra operačního systému. U starších systémů bylo nutné pro takový zákaz znovu sestavit jádro operačního systému. U dnešních systémů je to možné provádět dynamicky (např. Windows NT a většina systémů UNIX). Někdy je však nutné systém po takové změně restartovat.

Zajímavou vlastností mnohých operačních systémů je, že IP-datagramy nepředávají mechanicky, ale provádějí filtraci (*screening*), tj. nepředávají všechny pakety, ale jen některé – prolustrované. Většinou filtrace pracuje tak, že před tím, než je IP-datagram předán, tak se celý proces předávání pozastaví a rozhodnutí, zdali IP-datagram předat se ponechá na procesu (službě) běžícím na pozadí.

Předávaný IP-datagram se předá filtračnímu procesu, který buď předání schválí, nebo zamítne. Filtrační proces se rozhoduje, buď na základě informací v:

- IP-záhlaví, např. není-li adresát nebo příjemce na černé listině.
- TCP-záhlaví, např. podle čísel portu a nastavených příznaků ACK či SYN.
- Aplikačního protokolu, což používají některé firewally.

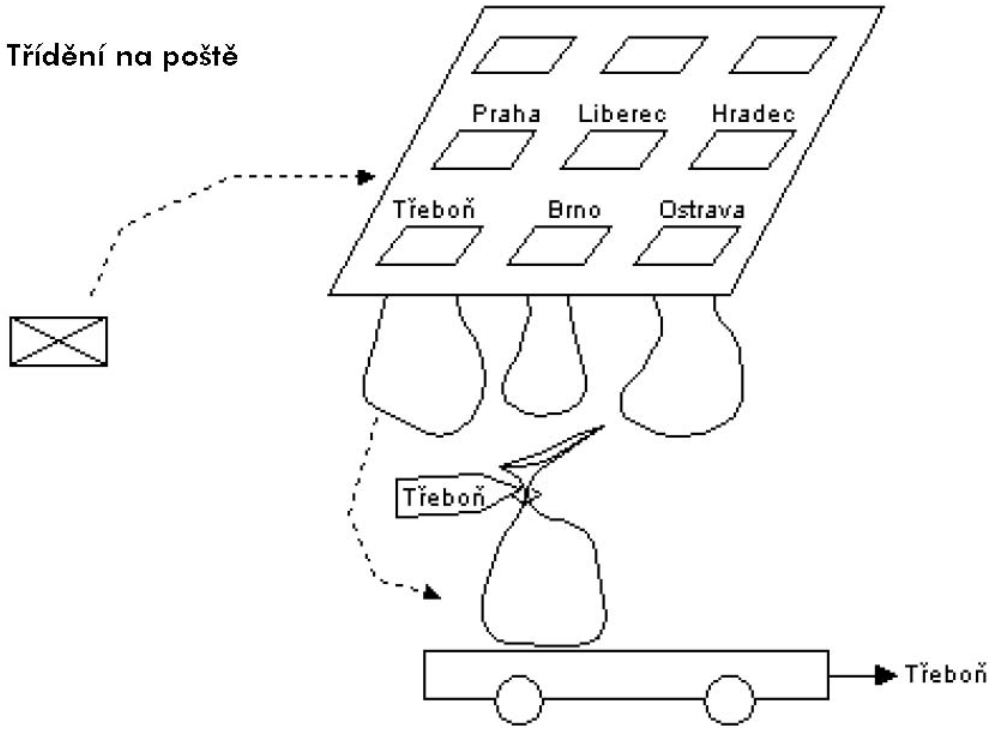


První dva typy filtrace jsou běžně implementovány na směrovačích. Třetí typ je záležitostí firewallů pracujících na principu filtrace (na rozdíl od firewallů pracujících na principu proxy).

7.2 Směrování

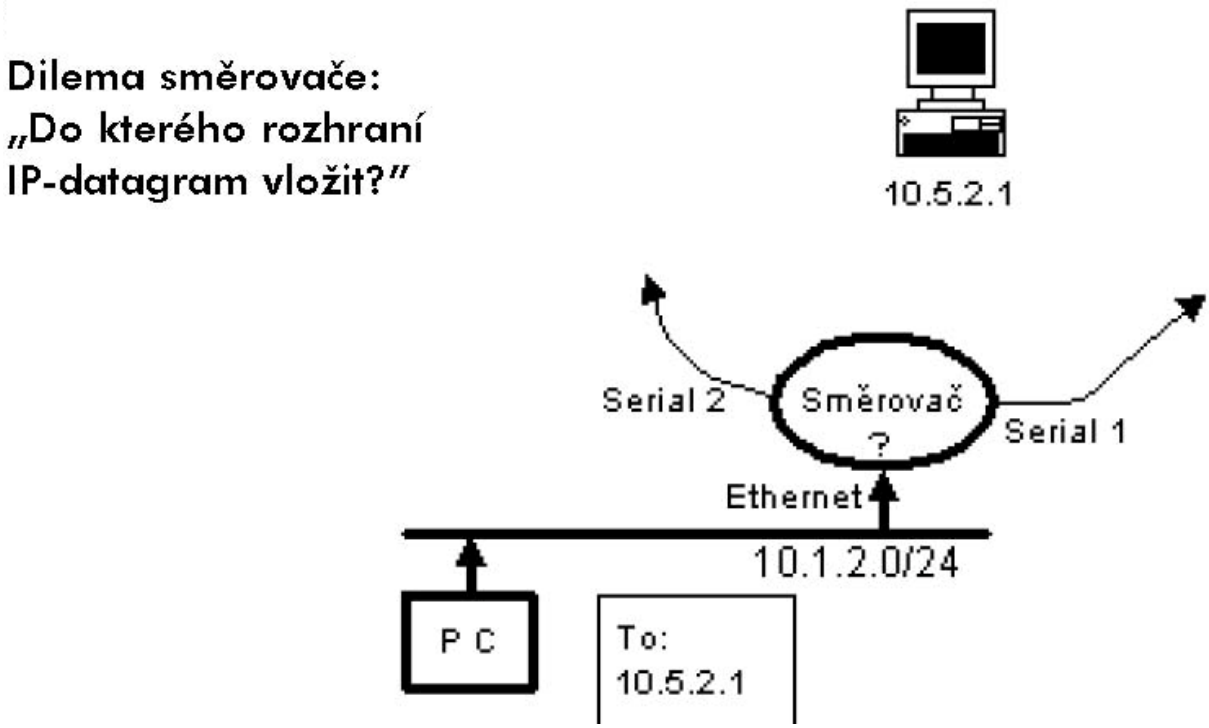
Směrování IP-datagramů je velice podobné třídění dopisů na poště. Na poště mají třídící stůl s vyřezanými otvory. Pod každým otvorem je přivázán poštovní pytel. Nad otvorem jsou napsány názvy měst, kam je z místní pošty přímé poštovní spojení.

Třídění probíhá tak, že poštovní úředník bere dopis za dopisem. Na každém dopisu si prohlédne adresu. Je-li adresát z Brna, pak dopis vhodí do otvoru Brno. Je-li adresát z Roztok u Prahy, pak dopis vhodí do otvoru Praha (protože do Roztok není přímé poštovní spojení, to je nejblíže Roztokům do Prahy). Až poštovní úředník vytřídí všechny dopisy, pak pytel po pytli odváže z třídícího stolu. Každý pytel zaváže a přiváže k němu visačku, na kterou napíše název města, kam se má pytel odeslat. Poté se pytel naloží …



Směrovač netřídí dopisy, ale IP-datagramy. Tento proces se nazývá směrováním.
Směrovač obdrží IP-datagram a musí rozhodnout, do kterého svého rozhraní jej má vhodit, kterému svému sousedovi (*next hop*) jej má poslat. Zjednodušeně řečeno směrovač je zařízení, které předává IP-datagramy z jednoho svého rozhraní do jiného rozhraní. Směrovač umí předat IP-datagram i do téhož rozhraní, ze kterého IP-datagram přišel. Považuje to však ze výstřednost, takže o tom odesílatele IP-datagramu upozorní ICMP-paketem „*redirect*".

Na následujícím obrázku směrovač obdržel IP-datagram adresovaný stanici 10.5.2.1 a musí rozhodnou, zdali jej vložit do rozhraní Serial1, Serial2 nebo snad zpět do rozhraní Ethernet?



Směrovači k rozhodování slouží směrovací tabulka (obdoba třídícího stolu na poště). Náš směrovač má tabulku:

Síť	Maska	Next Hop	Síťové rozhraní	Metrika
192.168.1.0	255.255.255.0	192.168.254.5	Seriál 1	4
10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0
10.5.1.0	255.255.255.0	10.10.10.2	Seriál 2	3
10.5.0.0	255.255.0.0	10.5.5.5	Seriál 1	2
…				
0.0.0.0	0.0.0.0	10.10.10.2	Seriál 2	1

Směrovací tabulka má v prvním sloupci IP-adresu cílové sítě. Představme si pro jednoduchost, že směrovací tabulka je podle prvního sloupce sestupně tříděna. To nám umožní snadno aplikovat základní pravidlo směrování:

Více specifická adresa cílové sítě má přednost před méně specifickou.

Více specifickou adresou sítě se rozumí adresa, která má v síťové masce více jedniček. V případě, že by se ve směrovací tabulce našly dvě či více cest k cíli, pak se zvolí více specifická cesta. V případě, že se najdou dvě stejně specifické cesty, pak se zvolí cesta s nejnižší metrikou (cenou).

7.2.1 Zpracování

V případě, že jsou řádky směrovací tabulky sestupně tříděny, pak stačí směrovací tabulku procházet od shora dolů. Na každém řádku se vezme síťová maska, kterou se bit po bitu vynásobí IP-adresa příjemce IP-datagramu. Výsledek se porovná s prvním sloupcem. Pokud se výsledek nerovná IP-adrese sítě v prvním sloupci, pak se přejde na zpracování následujícího řádku. Pokud se výsledek shoduje s IP-adresou v prvním sloupci, pak se ještě otestuje následující řádek, zdali ve směrovací tabulce neexistuje ještě k cíli jiná cesta, (pak by vstoupila do hry metrika).

Vraťme se k příkladu. Směrovač je postaven před rozhodnutí kterým svým síťovým rozhraním IP-datagram o adrese 10.5.2.1 odeslat. Prochází směrovací tabulku:

1. Řádek:

192.168.1.0	255.255.255.0	192.168.254.5	Seriál 1	4

Vynásobením bit po bitu cílové adresy 10.5.2.1 s maskou 255.255.255.0 obdržíme 10.5.2.0, což se nerovná IP-adrese sítě v prvním sloupci (ta je 192.168.1.0). Přecházíme na vyhodnocení následujícího řádku.

2. Řádek:

10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0

Vynásobením bit po bitu cílové adresy 10.5.2.1 s maskou 255.255.255.0 obdržíme 10.5.2.0, což se nerovná IP-adrese sítě v prvním sloupci (ta je 10.1.2.0). Přecházíme na vyhodnocení následujícího řádku.

3. Řádek:

10.5.1.0	255.255.255.0	10.10.10.2	Seriál 2	3

Vynásobením bit po bitu cílové adresy 10.5.2.1 s maskou 255.255.255.0 obdržíme 10.5.2.0, což se nerovná IP-adrese sítě v prvním sloupci (ta je 10.5.1.0). Přecházíme na vyhodnocení následujícího řádku.

4. Řádek:

10.5.0.0	255.255.0.0	10.5.5.5	Seriál 1	2

Vynásobením bit po bitu cílové adresy 10.5.2.1 s maskou 255.255.0.0 obdržíme 10.5.0.0, což **se rovná** IP-adrese sítě v prvním sloupci (ta je 10.5.0.0). Budeme proto náš IP-datagram vkládat do rozhraní Serial 1 a předávat jej dalšímu směrovači o IP-adrese 10.5.5.5. Pokud by se nejednalo o sériovou linku, ale např. o Ethernet, pak by bylo třeba zjistit linkovou adresu směrovače o IPadrese 10.5.5.5 protokolem ARP.

Poslední řádek obsahující v prvním sloupci 0.0.0.0 s maskou 0.0.0.0 se nazývá *default*. Tímto implicitním směrem jsou pak odesílány všechny IP-datagramy, pro které nevyhovoval žádný jiný řádek směrovací tabulky (všimněte si, že vyhovuje každé IP-adrese: nula krát nula je nula).

Implicitní směr ve směrovací tabulce může a nemusí být – závisí to na správci, jak tabulku naplnil. Implicitní směr používají např. firmy pro cestu do Internetu.

7.3 Manipulace se směrovacími tabulkami

Směrovací tabulku je třeba jednotlivými položkami naplnit. Položky jsou pak v tabulce trvale, dokud je někdo nezruší nebo nevypne systém. Pokud je plní směrovací aplikační protokoly, pak je sledována doba jejich života, po které jsou z tabulky vypuštěny.

V příkazech se anglicky často nepoužívá slovo *router*, ale *gateway*. S čímž se setkáváme zejména ve starší literatuře. Ve směrovací tabulce se tím rozumí následující směrovač (*next hop*).

7.3.1 Výpis obsahu směrovací tabulky v NT

Příkaz *netstat* vypisuje obsah směrovací tabulky setříděn vzestupně, takže pokud chcete vyhodnocovat tabulku, pak ji musíte procházet zdola nahoru. Trochu nezvyklé je, že rozhraní

(*interface*) se jmenují svou IP-adresou. Avšak když se podíváte na první sloupec, tak IP-datagramy adresované adresátovi 194.149.104.121 se mají vkládat do rozhraní 127.0.0.1. Je to správně, protože se jedná o adresu lokálního síťového rozhraní.

```
C:\> netstat
Route Table
Active Routes:
  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0  194.149.104.126  194.149.104.121       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
   194.149.104.64  255.255.255.192  194.149.104.121  194.149.104.121       1
  194.149.104.121  255.255.255.255        127.0.0.1        127.0.0.1       1
  194.149.104.255  255.255.255.255  194.149.104.121  194.149.104.121       1
        224.0.0.0        224.0.0.0  194.149.104.121  194.149.104.121       1
  255.255.255.255  255.255.255.255  194.149.104.121  194.149.104.121       1
```

Síť 224.0.0.0 s maskou 224.0.0.0 označuje všechny adresné oběžníky (včetně rezervy IP-adres, tj. IP-adresy tříd D a E).

7.3.2 Výpis obsahu směrovací tabulky v LINUXu

Položky směrovací tabulky jsou opět vypisovány vzestupně, tzn. směrovací tabulku procházíme opět od spodu nahoru. LINUX je podstatně starší operační systém. Na rozdíl od NT starší verze operačních systémů LINUX nevypisovaly síťovou masku – předpokládaly standardní síťovou masku, což při použití jiných masek vedlo k nepřehlednému výpisu.

Novější verze vypisují síťovou masku ve tvaru lomeno a počet jedniček masky. Navíc ještě před výpis směrovací tabulky vypíší všechny síťové masky, které se ve směrovací tabulce vyskytují.

```
$ netstat -rn
Routing tables
Destination      Gateway            Flags     Refs     Use  Interface
Netmasks:
Inet             255.0.0.0
Inet             255.255.0.0
Inet             255.255.255.224

Route Tree for Protocol Family 2:
default          195.47.37.193      UGS          8    25686  tu0
10/8             195.47.37.193      UGS          0     4916  tu0
127.0.0.1        127.0.0.1          UH           1        0  lo0
172.17/16        195.47.37.193      UGS          2    21306  tu0
195.47.37.192/27 195.47.37.194      U           17    30404  tu0
```

Sloupec Refs ukazuje kolik je tímto směrem navázáno spojení protokolem TCP. Sloupec Use indikuje, kolik IP-paketů bylo tímto směrem odesláno (zpravidla od startu systému). Nejzajímavějším sloupcem je sloupec s příznaky (*Flags*). Příznaky mají následující významy:

7.3.3 Naplnění tabulky a rušení položek

Směrovací tabulka se plní:

- Při konfiguraci síťového rozhraní, kdy říkáme, jakou má síťové rozhraní adresu a masku. V operačním systému LINUX se jedná o příkaz *ifconfig*.
- Staticky (ručně) příkazem *route*.
- Dynamicky ze ICMP-zpráv *redirect*.
- Dynamicky směrovacími (tj. aplikačními) protokoly.

Staticky se směrovací tabulka plní pomocí příkazu route. V operačním systému NT má příkaz route následující syntaxi:

```
ROUTE [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]
```

`-f`	Vymaže nejprve obsah směrovací tabulky.
`-p`	U příkazu ADD zajistí, aby takto přidaná položka zůstala ve směrovací tabulce i po restartu PC, tj. stala se trvalou položkou. U příkazu PRINT způsobí, že se vypíší trvalé položky.
`command`	Určuje příkaz pro manipulaci se směrovací tabulkou, nabývá následujících hodnot:
	`PRINT` Vypiš obsah směrovací tabulky
	`ADD` Přidej položku do směrovací tabulky.
	`DELETE` Zruš položku ve směrovací tabulce.
	`CHANGE` Změň položku
`destination`	Specifikuje cílovou síť.
`netmask`	Specifikuje síťovou masku
`gateway`	Specifikuje next hop.
`METRIC`	Specifikuje metriku.

7.4 Směrovací protokoly

Směrovací protokoly jsou aplikační protokoly, které neslouží uživatelům (osobám), ale směrovačům, aby si vzájemnou komunikací mezi sebou automaticky naplnily směrovací tabulky. Je dvojí na sobě nezávislé dělení směrovacích protokolů:

- Na *Link State Protocols* (LSP) a na *Routing Vector Protocols* (RVP).
- Na IGP a EGP.

7.4.1 LSP a RVP

Protokoly RVP (*Routing Vector Protocols*) pracují tak, že si sousední směrovače mezi sebou vyměňují obsahy směrovacích tabulek (vektorem se míní jedna položka směrovací tabulky). Obdržím-li jednotlivé vektory ze směrovací tabulky svého souseda, pak si z nich mohu vybrat vektory, které ve vlastní směrovací tabulce nemám a doplnit je do vlastní směrovací tabulky.

Příkladem protokolů RVP jsou protokoly RIP a RIP 2. V operačním systému UNIX je protokol RIP implementován programem *routed*. Protokolem RIP si sousední směrovače vyměňují pomocí všeobecných oběžníků (*broadcast*) obsahy svých směrovacích tabulek. Nevýhodou je, že v tomto protokolu není v položce směrovací tabulky uváděna síťová maska. Proto lze protokol RIP použít jen tehdy, když v síti používáme pouze sítě se standardní maskou. Protokol RIP 2 tuto nevýhodu odstraňuje. RIP 2 šíří obsahy směrovacích tabulek zpravidla pomocí adresného oběžníku (*broadcast*) o IP-adrese 224.0.0.9. Nevýhodou protokolu RIP 2 je, že je jen zřídka implementován.

Protokoly LSP pracují na zcela odlišném principu. Každý směrovač si zjistí, jaké směrovače má za své sousedy a v pravidelných intervalech testuje jejich dostupnost. Celou síť pak zaplavuje svými oběžníky o tom, koho má za své sousedy. Takže každý směrovač má od všech ostatních směrovačů zprávu o tom jaké mají sousedy.

Takže každý směrovač má seznam všech cest v síti. Na tento seznam se pustí algoritmus nejkratší cesty, kterým se zjišťuje směr kam se má IP-datagram odeslat. Tj. položky směrovací tabulky se počítají algoritmem nejkratší cesty z dat obdržených od ostatních směrovačů.

U rozsáhlých sítí je problematické zaplavovat je velkým množstvím informací ze směrovačů, proto se takové sítě rozdělí na oblasti a zmíněný postup se aplikuje pouze v rámci této oblasti. Na hranicích se sousedními oblastmi jsou hraniční směrovače, které si pak vyměňují informace o celých oblastech.

7.4.2 IGP a EGP

Protokoly IGP jsou určeny pro činnost v rámci autonomního systému. Již zmíněné protokoly RIP, RIP2, OSPF i IS-IS jsou vesměs protokoly IGP. Ovšem poskytovatelé Internetu si mezi sebou potřebují také vyměňovat směrovací informace. Poskytovatelé Internetu pro výměnu směrovacích informací mezi autonomními systémy používají protokoly EGP. V dnešní době používají protokol BGP (*Border Gateway Protocol*) verze 6.

Protokoly EGP se liší od protokolů IGP zejména tím, že ve směrování umožňují zohlednit směrovací politiku (tj. kdo komu platí).

8. Protokol TCP a UDP

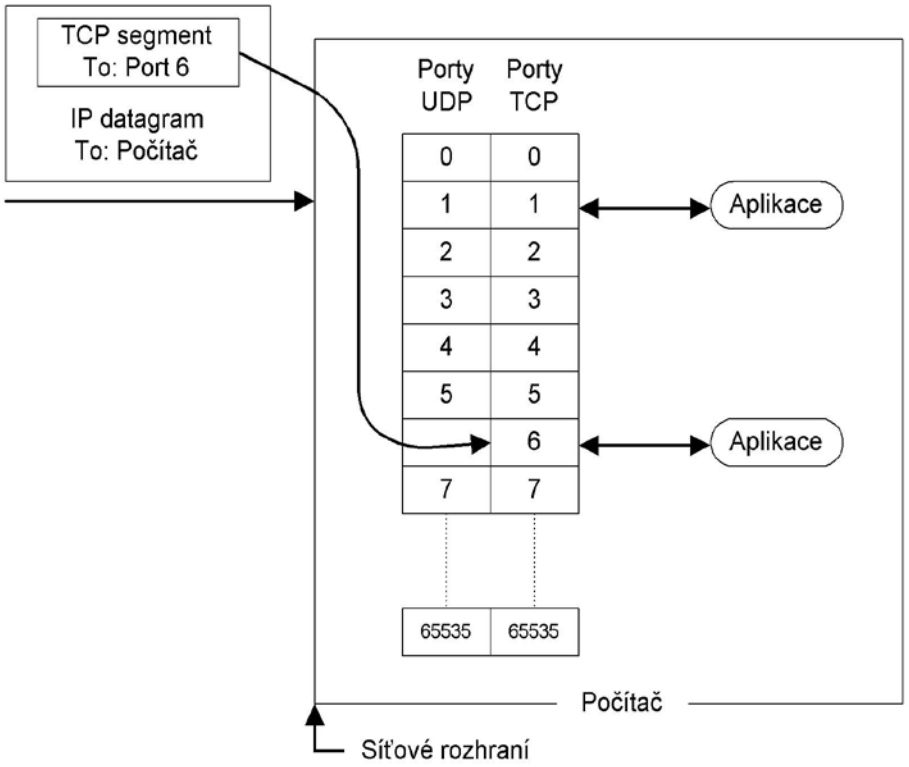
Protokol TCP je proti protokolu IP protokolem vyšší vrstvy. Zatímco protokol IP přepravuje data mezi libovolnými počítači v Internetu, tak protokol TCP dopravuje data mezi dvěma konkrétními aplikacemi běžícími na těchto počítačích.

Pro dopravu dat mezi počítači se využívá protokol IP. Protokol IP adresuje IP-adresou pouze síťové rozhraní počítače. Pokud bychom použili přirovnání k běžnému poštovnímu styku, pak IP-adresa odpovídá adrese domu a port (adresa v protokolu TCP) pak odpovídá jménu konkrétního obyvatele domu.

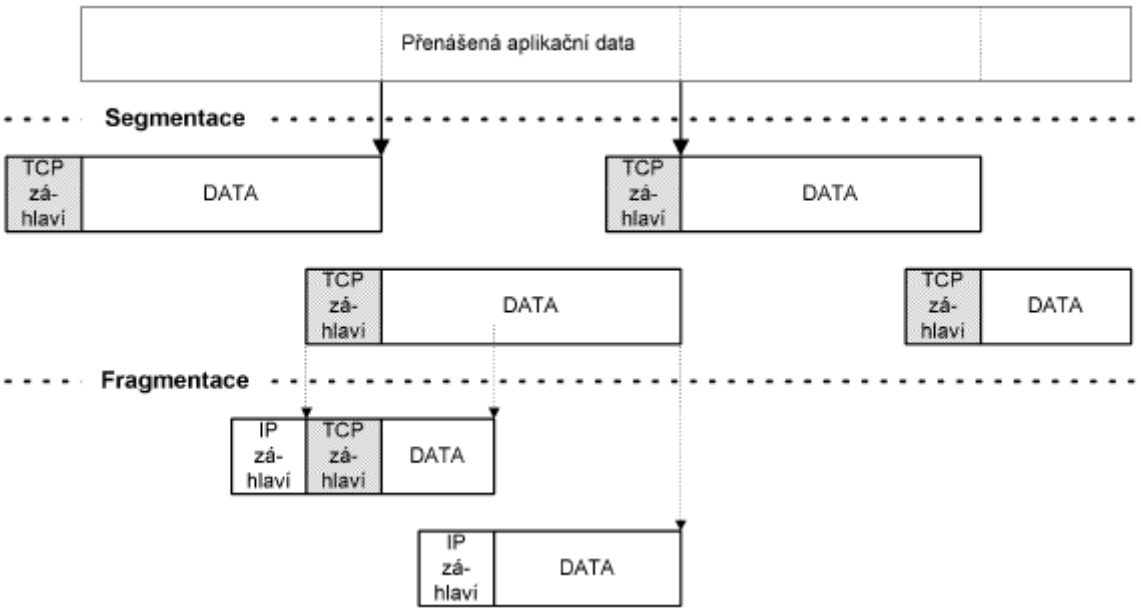
Protokol TCP je spojovanou službou (*connection oriented*), tj. službou která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášené bajty jsou číslovány. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena kontrolním součtem.

Konce spojení ("odesílatel" a „adresát") jsou určeny tzv. číslem portu. Toto číslo je dvojbajtové, takže může nabývat hodnot 0 až 65535. U čísel portů se často vyjadřuje okolnost, že se jedná o porty protokolu TCP tím, že se za číslo napíše lomítko a název protokolu (tcp). Pro protokol UDP je jiná sada portů než pro protokol TCP (též 0 až 65535), tj. např. port 53/tcp nemá nic společného s portem 53/udp.

Cílová aplikace je v Internetu adresována (jednoznačně určena) IP-adresou, číslem portu a použitým protokolem (TCP nebo UDP). Protokol IP dopraví IP-datagram na konkrétní počítač. Na tomto počítači běží jednotlivé aplikace. Podle čísla cílového portu operační systém pozná které aplikaci má TCP-segment doručit.



Základní jednotkou přenosu v protokolu TCP je TCP segment. Někdy se také říká TCP paket. TCP segment se vkládá do IP-datagramu. IP-datagram se vkládá do linkového rámce. Použije-li se příliš velký TCP-segment, který se celý vloží do velkého IP-datagramu, který je větší než maximální velikost přenášeného linkového rámce (MTU), pak IP protokol musí provést fragmentaci IP-datagramu.

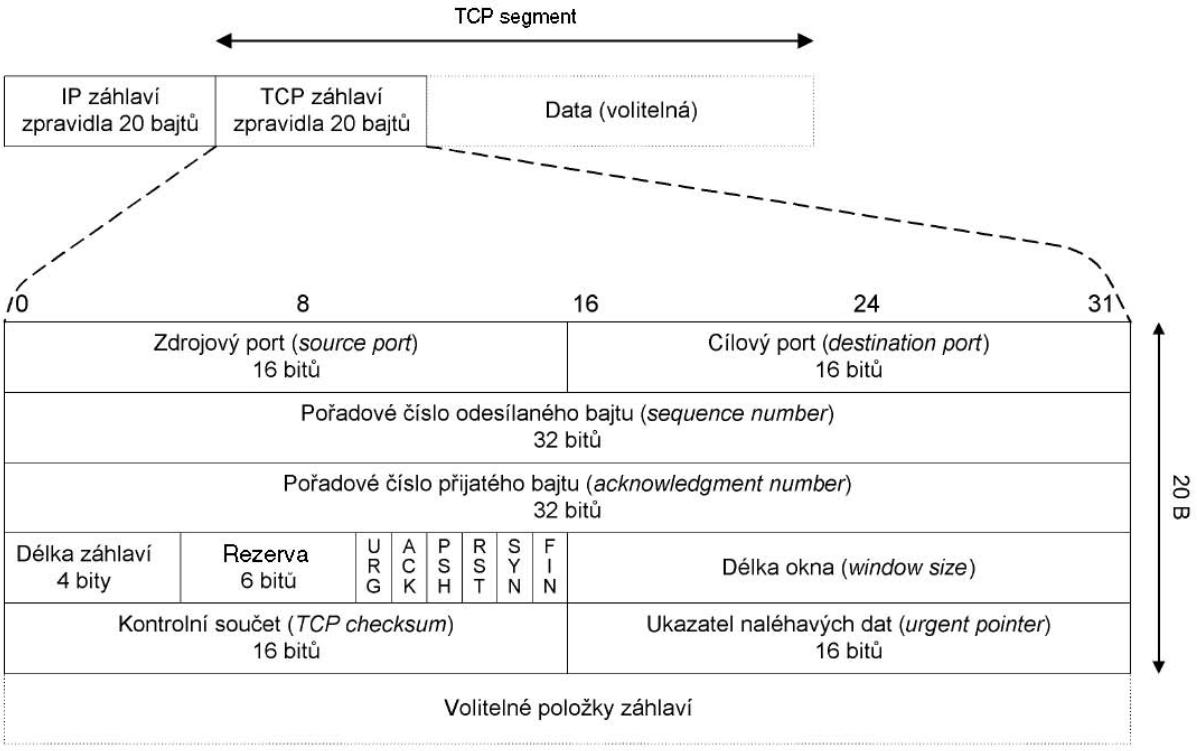


Fragmentace zvyšuje režii, proto je cílem vytvářet segmenty takové velikosti, aby fragmentace nebyla nutná.

8.1 TCP segment

Zdrojový port (*source port*) je port odesílatele TCP segmentu, **cílový port** (*destination port*) je portem adresáta TCP segmentu. Pětice: zdrojový port, cílový port, zdrojová IP-adresa, cílová IP-adresa a protokol (TCP) jednoznačně identifikuje v daném okamžiku spojení v Internetu.

TCP segment je část z toku dat tekoucích od odesílatele k příjemci. **Pořadové číslo odesílaného bajtu** je pořadové číslo prvního bajtu TCP segmentu v toku dat od odesílatele k příjemci (TCP segment nese bajty od **pořadového čísla odesílaného bajtu** až do délky segmentu). Tok dat v opačném směru má samostatné (jiné) číslování svých dat.



TCP segment

Délka záhlaví vyjadřuje délku záhlaví TCP segmentu v násobcích 32 bitů (4 bajtů) – podobně jako u IP-záhlaví.

Délka okna vyjadřuje přírůstek pořadového čísla přijatého bajtu, který bude příjemcem ještě akceptován.

Ukazatel naléhavých dat může být nastaven pouze v případě, že je nastaven příznak URG. Přičte-li se tento ukazatel k pořadovému číslu odesílaného bajtu, pak ukazuje na konec úseku naléhavých dat. Odesílatel si přeje, aby příjemce tato naléhavá data přednostně zpracoval.
V poli příznaků mohou být nastaveny následující příznaky:

- **URG** – TCP segment nese naléhavá data.
- **ACK** – TCP segment má platné pole „Pořadové číslo přijatého bajtu" (nastaven ve všech segmentech kromě prvního segmentu, kterým klient navazuje spojení).
- **PSH** – Zpravidla se používá k signalizaci, že TCP segment nese aplikační data, příjemce má tato data předávat aplikaci. Použití tohoto příznaku není ustáleno.
- **RST** – Odmítnutí TCP spojení.
- **SYN** – Odesílatel začíná s novou sekvencí číslování, tj. TCP segment nese pořadové číslo prvního odesílaného bajtu (ISN).
- **FIN** – odesílatel ukončil odesílání dat. Pokud bychom použili přirovnání k práci se souborem, pak příznak FIN odpovídá konci souboru (EOF). Přijetí TCP segmentu s příznakem FIN neznamená, že v opačném směru není dále možný přenos dat.

Kontrolní součet IP-záhlaví se počítá pouze ze samotného IP-záhlaví. Z hlediska zabezpečení integrity přenášených dat je důležitý kontrolní součet v záhlaví TCP-segmentu počítaný i z přenášených dat.

Volitelné položky TCP záhlaví Povinné položky TCP záhlaví tvoří 20 B. Za povinnými položkami následují volitelné položky. Volitelná položka se skládá z typu volitelné položky, délky volitelné položky a hodnoty. Délka TCP záhlaví musí být dělitelná čtyřmi. V případě, že délka záhlaví by nebyla dělitelná čtyřmi, pak se záhlaví doplňuje prázdnou volitelnou položkou – NOP.

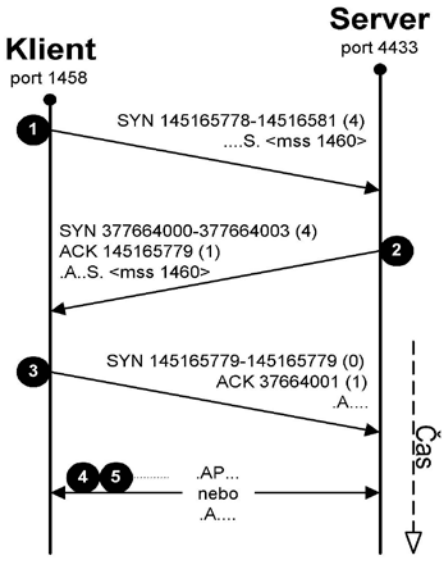
8.2 Navázání a ukončení spojení protokolem TCP

Protokol TCP využívá k transportu dat Internetem protokol IP, avšak nad tímto protokolem zřizuje spojovanou službu. Musí řešit problémy navázání a ukončení spojení, potvrzování přijatých dat, vyžádání ztracených dat, ale také problémy průchodnosti přenosové cesty.

8.2.1 Navazování spojení

Protokol TCP umožňuje jedné straně navazovat spojení. Druhá stana spojení buď akceptuje, nebo odmítne. Z hlediska aplikační vrstvy bude stranou navazující spojení klient a server ta strana, která spojení očekává.

Klient vygeneruje náhodné číslo v intervalu 0 až 2^{32}-1, které použije jako startovací pořadové číslo odesílaného bajtu (tzv. ISN). Skutečnost, že klient právě vytvořil startovací pořadové číslo odesílaného bajtu vyznačí v TCP segmentu nastavením příznaku SYN (….S.). TCP segment s nastaveným příznakem SYN a nenastaveným příznakem ACK je velice zvláštním segmentem. Tato kombinace nastaveného příznaku SYN a nenastaveného příznaku ACK je specifická pro první TCP segment spojení. Pokud se chce klientům zamezit v navázání spojení nějakým směrem, pak stačí v tomto směru odfiltrovat všechny TCP segmenty s nastaveným příznakem SYN a klient (útočník) nemá šanci. Tento mechanismus se též často využívá pro ochranu intranetů od Internetu.



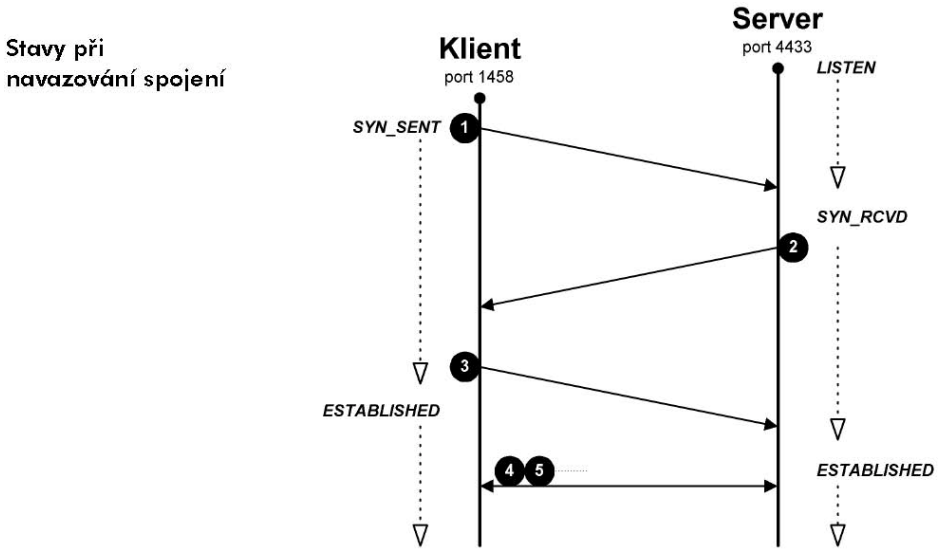
Ne všechny TCP segmenty musí nutně nést aplikační data, tj. mít nastaven příznak PSH (.AP…). Může se stát, že jeden konec spojení odesílá data, avšak druhý konec nemá momentálně žádná data k odeslání. I když druhý konec nemá co posílat, tak musí potvrzovat

přijatá data. Takové potvrzování provádí TCP segmenty s nenastaveným příznakem PSH (.A….), tj. segmenty bez dat.

V každém okamžiku spojení je spojení v tzv. stavu. Při navazování spojení může být:

- Server ve stavu:
  - LISTEN – server je připraven na spojení s klienty.
  - SYN_RCVD – server přijal od klienta první TCP segment, tj. segment s příznakem SYN.
- Klient ve stavu:
  - SYN_SEND – klient odeslal první TCP segment, tj. segment s příznakem SYN.

Pokud se spojení naváže, pak klient i server přecházejí do stavu ESTABLISHED, tj. spojení navázáno. V tomto stavu si mohou oba konce současně předávat data.

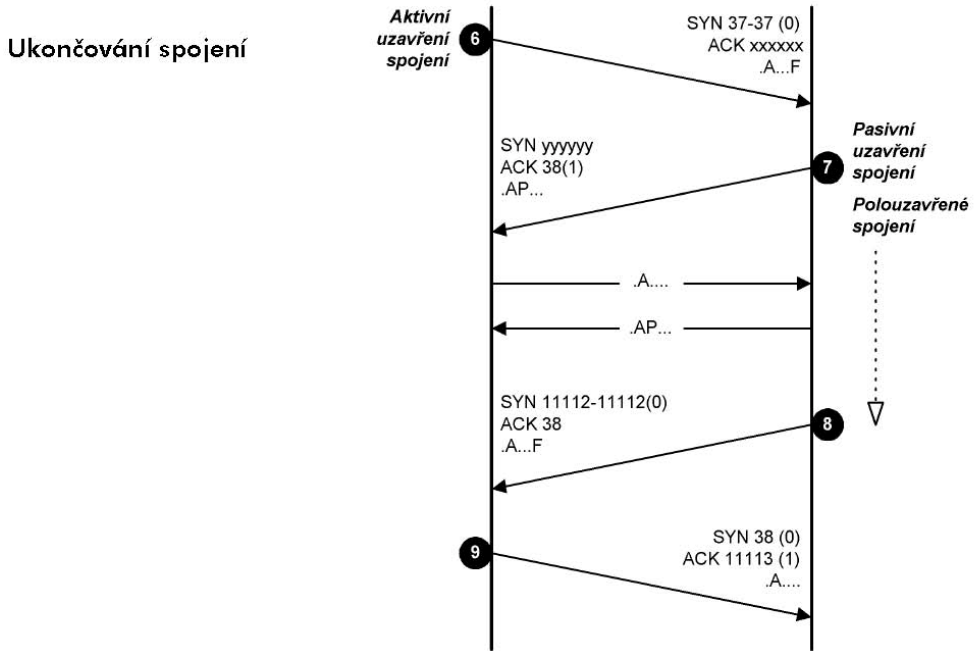


8.2.2 Ukončování spojení

Zatímco spojení navazoval v architektuře klient/server zpravidla klient, tak ukončit spojení může libovolná strana. Strana, která první odešle TCP segment s příznakem FIN (ukončení spojení) provádí tzv. aktivní ukončení spojení (*active close*), druhé straně nezbývá než provést pasivní ukončení spojení *(pasive close*).

Provede-li jedna strana aktivní ukončení spojení, pak již nemůže odesílat data (nemůže odeslat TCP segment s příznakem PSH). Druhá strana však může v odesílání dat pokračovat až do té doby, dokud neprovede sama ukončení spojení. Mezidobí od aktivního ukončení spojení do ukončení spojení nazýváme polouzavřeným spojením (*half close*). TCP segment s příznakem FIN je obdobou konce souboru (EOF).

Pro řádné uzavření spojení jsou nutné čtyři TCP segmenty. Příznak FIN se opět jako příznak SYN při navazování spojení potvrzuje jako by zabíral 1 B dat.

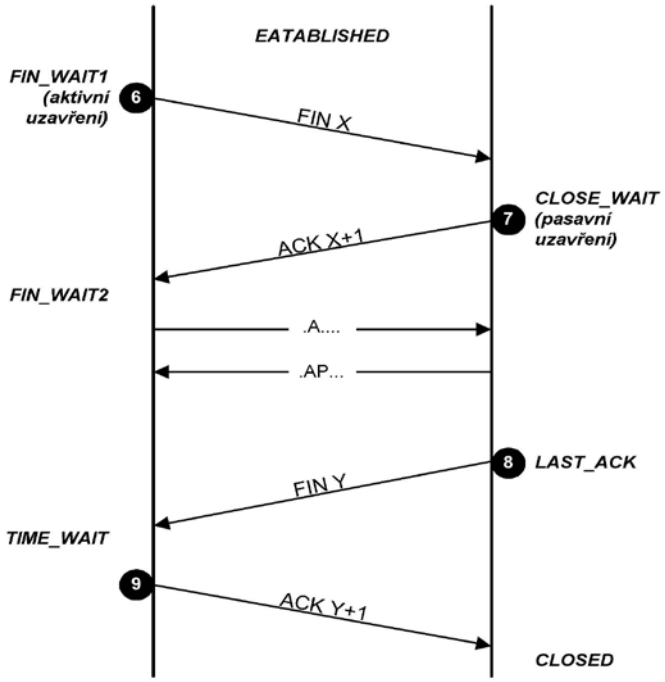


Strana, která spojení uzavřela, již nemůže odesílat žádná data (jí odesílané segmenty nemohou obsahovat příznak PSH).
Stavy při ukončování spojení:

- FIN_WAIT1 – strana zjistila, že již všechna data odeslala (a potřebuje signalizovat konec souboru – EOF), tak v TCP segmentu nastaví příznak FIN, čímž signalizuje aktivní uzavření spojení segmentem 6.
- CLOSE_WAIT – druhá strana obdržela aktivní uzavření spojení a nezbývá jí nic jiného než potvrdit segmentem 7 přechod do pasivního uzavření spojení, kterému odpovídá stav CLOSE_WAIT.
- FIN_WAIT2 je stav poté, co strana obdrží potvrzení segmentem 7 aktivního uzavření spojení od protějšku. Ve stavu FIN_WAIT2 strana zůstává do té doby, dokud protějšek nezašle TCP segment s příznakem FIN, tj. do přechodu do stavu TIME_WAIT.
- LAST_ACK – druhá strana již odeslala všechna data a signalizuje úplné ukončení spojení segmentem 8.
- TIME_WAIT – všechna data oběma směry již byla přenesena. Je nutné pouze potvrdit úplné uzavření spojení. Odesláním TCP segmentu 9 je potvrzeno úplné ukončení spojení.
- CLOSED – druhá strana obdržela potvrzení úplného uzavření spojení a přechází do stavu CLOSED. Strana, která odeslala segment 9 přechází do stavu CLOSED.

8.2.3 Odmítnutí spojení

Spojení se odmítá nastavením příznaku RST (*Reset*) v záhlaví TCP segmentu.



Spojení je odmítáno v zásadě ve dvou případech:

- Klient požaduje spojení se serverem na portu, na kterém žádný server neběží. To je rozdíl oproti protokolu UDP. Pokud je zaslán UDP datagram na port, kde neběží žádný server, pak systém odpoví ICMP zprávou nedosažitelný port.
- Druhým případem je situace, kdy je odmítnuto dále pokračovat v již navázaném spojení. Zde lze rozlišit také dva případy:
  - Řádné ukončení spojení je poměrně dlouhou záležitostí (např. aplikace je nucena posečkávat ve stavu TIME_WAIT). Aplikace si po odeslání všech dat přeje ukončit spojení rychleji – použije odmítnutí spojení. V praxi se setkáváme s tím, že buď místo segmentu 9 je odeslán segment s nastaveným příznakem RST. Nebo po segmentu 9 následuje ještě potvrzení segmentu 9 pomocí TCP segmentu s nastaveným příznakem RST.
  - Jedna z komunikujících stran zjistí, že protějšek je nedůvěryhodný, pak okamžitě ukončuje spojení. To je případ například protokolu SSL.

8.2.4 Zjištění stavu spojení

Výpis všech spojení protokoly TCP a UDP lze získat pomocí příkazu netstat s parametrem –a.

```
$ netstat -a
```

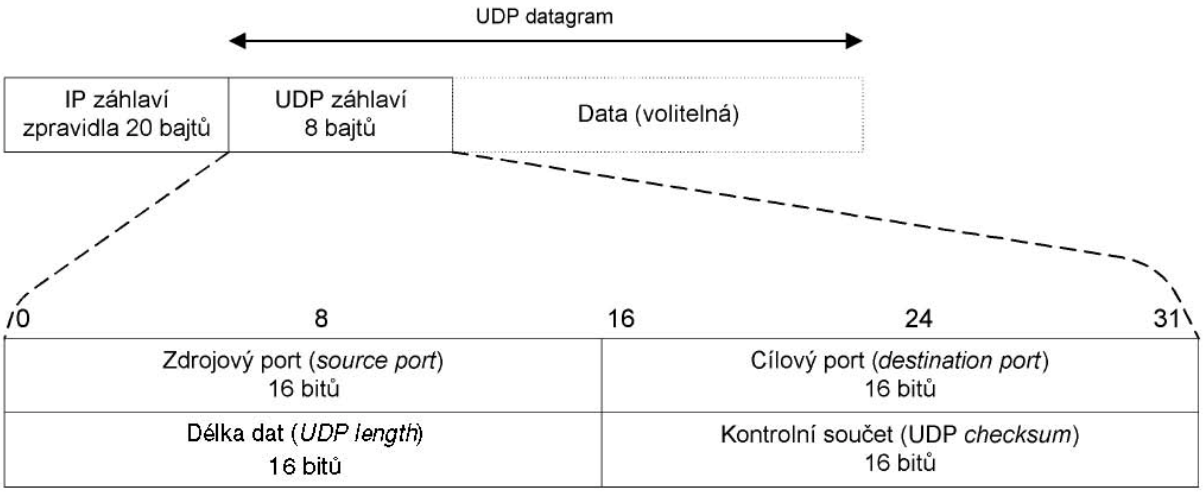
```
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)

tcp        0      0  194.149.105.18.22      194.149.103.204.24695  TIME_WAIT
tcp        0      0  194.149.105.18.3099    194.108.145.128.25     SYN_SENT
tcp        0  34472  194.149.105.18.3079    195.47.32.245.25       ESTABLISHED
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  *.25                   *.*                    LISTEN
tcp        0      0  *.53                   *.*                    LISTEN
udp        0      0  *.53                   *.*
udp        0      0  127.0.0.1.53           *.*
```

První dva řádky tvoří záhlaví výpisu. Význam jednotlivých sloupců:

- Sloupec **Proto** obsahuje název použitého protokolu (TCP nebo UDP).
- Sloupec **Recv-Q** vyjadřuje počet bajtů ve vstupní frontě spojení (čekajících na zpracování aplikací).
- Sloupec **Send-Q** vyjadřuje počet bajtů ve výstupní frontě (čekajících na odeslání).
- Sloupec **Local Address** obsahuje adresu lokálního síťového rozhraní tečkou odděleného od čísla lokálního portu. Servery čekající na spojení mohou mít na místo IP-adresy uvedenu hvězdičku. Hvězdička označuje, že server očekává spojení na všech svých síťových rozhraních.
- Sloupec **Foregin Address** obsahuje IP-adresu a port vzdáleného konce spojení. Hvězdičky vyznačují, že server očekává spojení z libovolné IP-adresy a libovolného portu.
- Sloupec **(state)** obsahuje stav spojení.

8.3 Protokol UDP (*User Datagram Protocol*)

Protokol UDP je jednoduchou alternativou protokolu TCP. Protokol UDP je nespojovaná služba (na rozdíl od protokolu TCP), tj. nenavazuje spojení. Odesílatel odešle UDP datagram příjemci a už se nestará o to, zdali se datagram náhodou neztratil (o to se musí postarat aplikační protokol).



Záhlaví UDP datagramu

Z předchozího obrázku je patrné, že záhlaví UDP protokolu je velice jednoduché. Obsahuje čísla zdrojového a cílového portu – což je zcela analogické protokolu TCP. Opět je třeba dodat, že čísla portů protokolu UDP nesouvisí s čísly portů protokolu TCP. Protokol UDP má svou nezávislou sadu čísel portů.

Pole délka dat obsahuje délku UDP datagramu (délku záhlaví + délku dat). Minimální délka je tedy 8, tj. UDP datagram obsahující pouze záhlaví a žádná data. Zajímavé je že pole kontrolní součet nemusí být povinně vyplněné. Výpočet kontrolního součtu je tak v protokolu UDP nepovinný.

V minulosti bylo u některých počítačů zvykem výpočet kontrolního součtu vypínat – zejména se jednalo o počítače s instalovaným systémem NFS (*Network File System*). Důvodem bylo zrychlení odezvy počítače.

8.4.1 Fragmentace

I u UDP datagramů je možná fragmentace v IP-protokolu. Avšak u UDP protokolu se zásadně snažíme fragmentaci vyhýbat. Typickým případem je DNS. DNS klient položí dotaz protokolem UDP. Pakliže odpověď serveru by přesáhla 512 B, pak server odešle jen tolik informací, aby nepřekročil hranici 512 B a navíc v aplikačních datech nastaví příznak TC (Truncation) specifikující, že odpověď byla zkrácena. Pakliže klientovi taková odpověď nestačí, pak ji zopakuje protokolem TCP, kterým mu server vrátí kompletní odpověď.

8.4.2 Oběžníky

Zvláštností protokolu UDP je skutečnost, že adresátem UDP datagramu nemusí být pouze jednoznačná IP-adresa, tj. síťové rozhraní konkrétního počítače. Adresátem může být skupina stanic – adresovat lze i oběžník.

Adresovat lze všeobecné oběžníky (*broadcast*), ale podstatně zajímavějším případem je adresování adresných oběžníků (*multicast*). Např. u aplikací typu RealAudio navazuje každý klient spojení se serverem. Kdežto u ProgresiveRealAudio se šíří data pomocí adresných oběžníků, tj. dochází k ohromné úspoře kapacity přenosových cest. A právě to je příležitost pro UDP.

9. Aplikační vrstva

Aplikační vrstva je poslední vrstvou referenčního modelu. Koncoví uživatelé využívají počítačové sítě prostřednictvím nejrůznějších síťových aplikací (softwarových serverů) - systémů elektronické pošty, přenosů souborů, vzdáleného přihlašování (remote login) a podobně.

Začleňovat všechny tyto různorodé aplikace přímo do aplikační vrstvy by nebylo rozumné. Proto se do aplikační vrstvy zahrnují jen části těchto aplikací, které realizují společně respektive obecně použitelné mechanismy.

Aplikační vrstva tedy zajišťuje jednotlivé služby, specifické pro určité konkrétní aplikace nebo jejich skupiny. Obsahuje služby zvenku viditelné uživatelem (elektronická pošta, vzdálený terminálový přístup, přenos a vzdálené sdílení souborů).

Služby aplikační vrstvy:

- ověření přípustnosti komunikujících partnerů (stejný druh služby)
- identifikace parametrů komunikujících (jména, hesla,...)
- zjištění stupně připravenosti komunikujících partnerů
- ověření pověření pro komunikaci
- určení přiměřenosti prostředků
- parametry služby
- tarify
- mechanismus ochrany zpráv
- synchronizace aplikací
- způsob dialogu
- postup při zahájení a ukončení spojení
- dohoda o syntaxi zpráv(kódy, struktura, abecedy,...)
- přenos zpráv

9.1 Klasifikace služeb aplikační vrstvy

- **Podle síťového modelu:**
  - model server/klient
  - model peer-to-peer ⇒ rovnoprávný (stejná funkce na všech komponentách)

- **Podle služeb:**
  - *datagramové* – pro aplikace jednotného charakteru, např. jmenné služby, čas apod.
  - *virtuální okruhy* – při přenášení velkého množství dat, kde záleží na bezchybném přenesení

- **Podle způsobu práce:**
  - *interaktivní* – v jednu chvíli obhospodařují 1 požadavek
  - *procesně orientované* – vytvoření spec. procesu na uspokojení našeho požadavku a poté zrušení tohoto procesu; počet procesů je omezen (u ftp, gopher atd.)

- **Podle zapamatování stavu:**
  - *stavový*
  - *bezstavový* – pamatují si stav rozpracovaní ⇒ pokračování práce tam, kde došlo k přerušení; server si nemusí nic pamatovat, informace o úplnosti posílá na hostitelský počítač

9.2 Typy serverů aplikační vrstvy

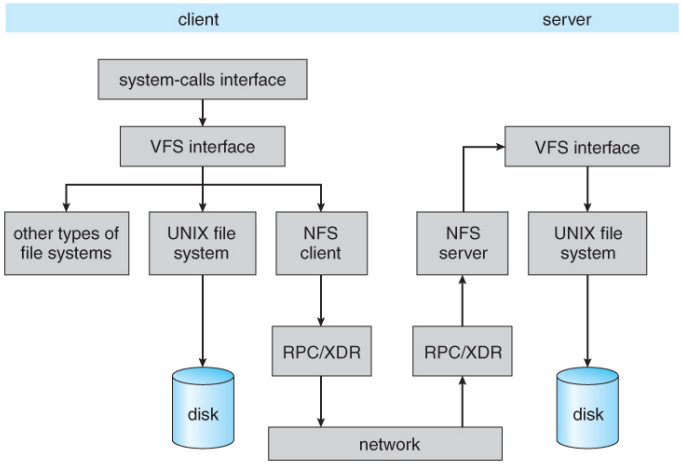
Servery (obslužné stanice) - poskytují některé své prostředky (disky, tiskárny...), zajišťují vlastní chod sítě a realizují jednotlivé síťové funkce. Jsou na ně kladeny vysoké požadavky co se týče spolehlivosti a rychlosti. V síti může být jeden nebo více serverů.

Pracovní stanice (workstations) - slouží uživatelům k provádění jejich prací. Tyto stanice do sítě nic nenabízejí, naopak umožňují přístup ke sdíleným síťovým prostředkům.

9.2.1 Diskový server

Diskový server (disc server) umožňuje uživatelům sdílet rozsáhlý disk, rozdělený na několik tzv. virtuálních disků, s nimiž pracují uživatelé (resp. jejich software) shodně jako s disky svých pracovních stanic (tzn. na fyzické úrovni). Diskový server lze snadno implementovat a je velmi efektivní, ovšem používán je mnohem méně než server souborový.

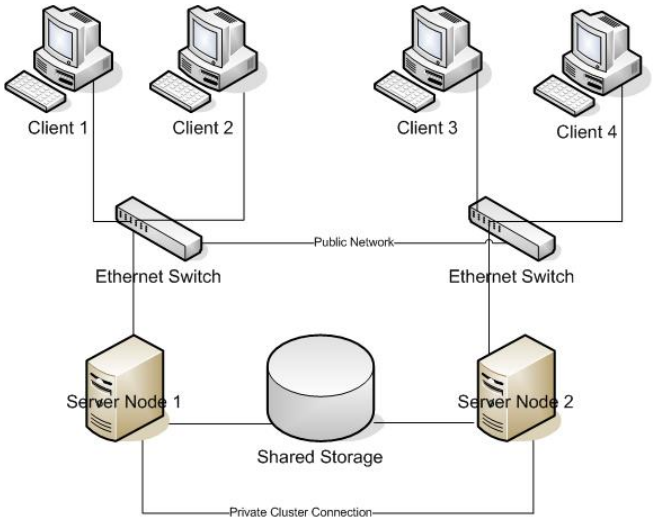
- přístup je pouze k celému disku, ne pouze např. k jednomu souboru
- uživatelé tedy přistupují k disku jako celku
- výhodou větší jednoduchost přístupu
- nevýhodou je vytažení přístupových práv pouze na celý disk
- sdílené disky jsou pouze pro čtení, každý uživatel má pak pro čtení a zápis svůj vlastní disk



9.2.2 Souborový server

Souborový server (file server) rovněž umožňuje sdílet uživatelům vysokokapacitní disk, avšak nikoli na fyzické úrovni, nýbrž na úrovni logické. Tento server může na rozdíl od předchozího implementovat různé způsoby ochrany souborů či vět proti současnému přístupu více uživatelů.
Ochrana dat před neoprávněným použitím je obvykle realizována pomocí hesel, popřípadě pomocí přístupových práv jednotlivých uživatelů. Realizace souborového serveru je sice složitější než u serveru diskového, přesto je prvně jmenovaný typ serveru používán mnohem častěji.

- slouží k ukládání souborů na vybraném PC
- souborový systém se dělí na: svazky, adresáře, soubory
- možnost sdílení dat, ale nutnost vytvoření ověřovacích mechanismů uživatele a mechanismus přístupových práv k souborům: R……čtení; W…...zápis; X……spuštění programu
- využití mapování disků k ztotožňování svazku s nějakou částí adresářového stromu disku na souborovém serveru



9.2.3 Tiskový server

Tiskový server (print server) umožňuje uživatelům počítačové sítě provádět tisky sestav na tiskárnách k tomuto serveru připojených. Server obvykle pracuje s frontou požadavků na tisk, přičemž uživatel může většinou svému požadavku specifikovat typ výstupního formuláře, počet potřebných kopií atd. Velice často bývá funkce tiskového serveru sdružována s funkcí serveru souborového.

- realizování disků na společné tiskárně ⇒ síťové tiskárny
- text, který chceme vytisknout se nejprve převede do jazyka tiskárny a poté až je vytištěn
- síťový server obsluhuje více klientů současně ⇒ vznik *fronty*
- požadavky na tisk se řadí tedy do fronty, kde existují následující stavy: vytváří se, připraven k tisku, tiskne se
- existují také příkazy např. na upřednostňování ve frontě, mazání z fronty apod.

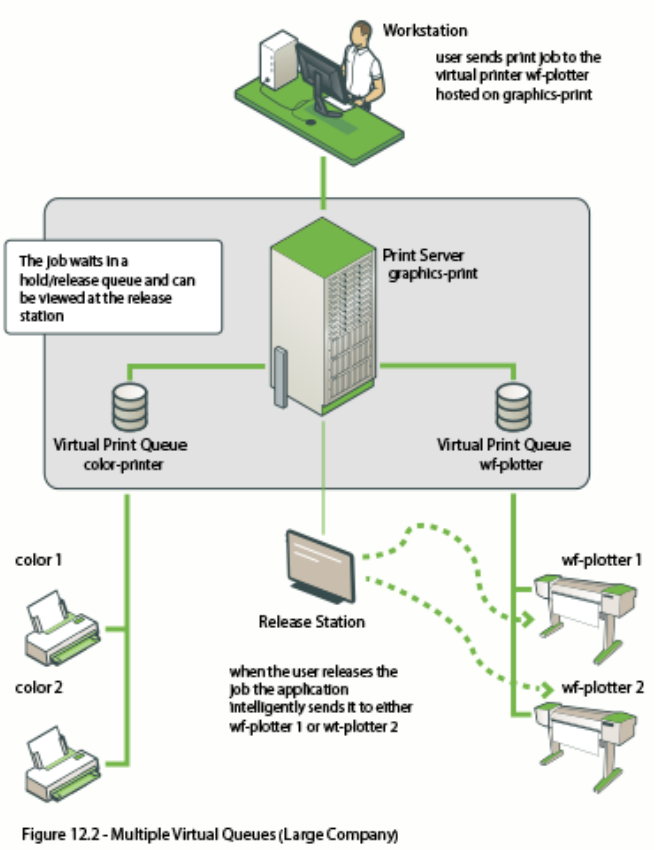


Figure 12.2 - Multiple Virtual Queues (Large Company)

9.2.4 Poštovní server a elektronická pošta

Slouží k přenosu zpráv v datovém režimu a přenáší se:

- text (původně) – ASCII znaky
- formátované dokumenty (text) – např. .pdf (portable data formular)
- zvuk ⇒ voicemail
- obraz
- video
- data (programy) – binární data

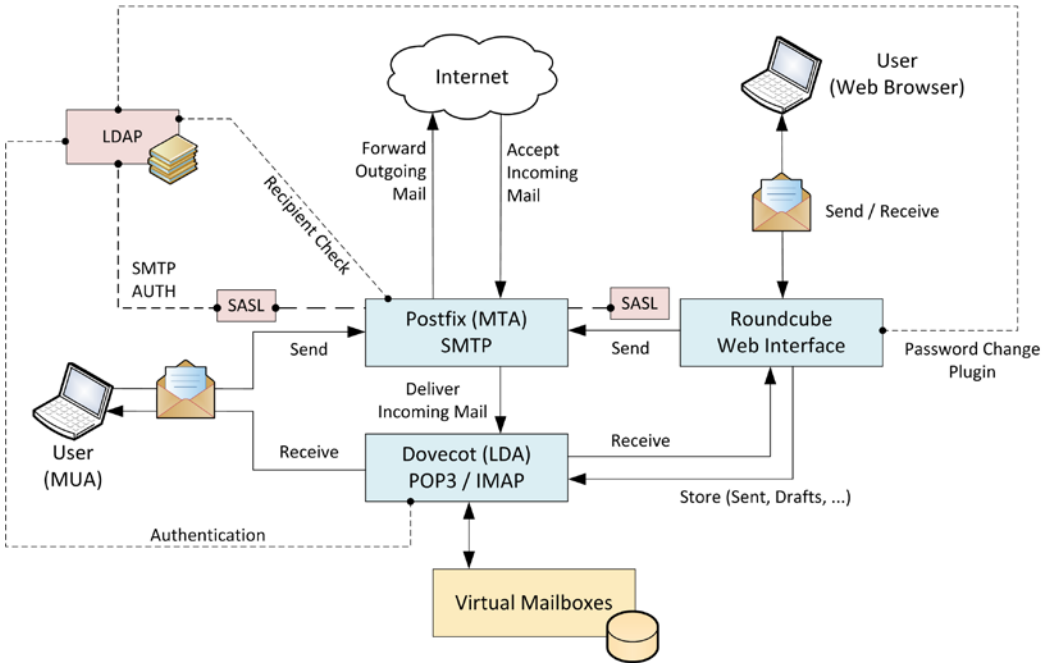
formát přenášených zpráv:

- dvě základní části: záhlaví, data
- adresy vypadají následovně: adresa@počítač.subdoména.doména
- poštovní servery umí pracovat s aliasy (přezdívkami)

vzdálený přístup k elektronické poště:

- *POP – Post Office Protocol*
  - na PC běží tzv. POP klient
  - název POP servru MVSO je pop.mvso.cz

- IMAP – Internet Mail Access Protocol
  - funguje obdobně, ale umožňuje pracovat s poštou i částečně: přenesení autorů zpráv, věcí apod.



9.2.5 List server - Elektronická konference

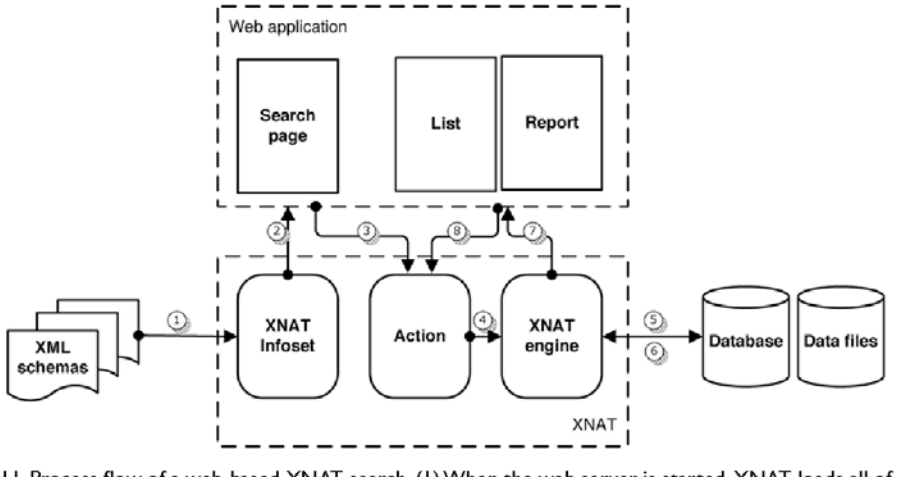
Program, který obsluhuje konference a diskusní skupiny po emailu. Rozesílá příspěvky jednotlivým účastníkům diskuse a také poskytuje administraci s diskusí spojené: přihlášení do skupiny, odhlášení, přesměrování atp.

vytvoření zájmových skupin a těmto pak rozesílání zpráv (příspěvků) od různých členů ⇒ např. server list.mvso.cz

- *uzavřené*
- *otevřené*

druhé členění na:

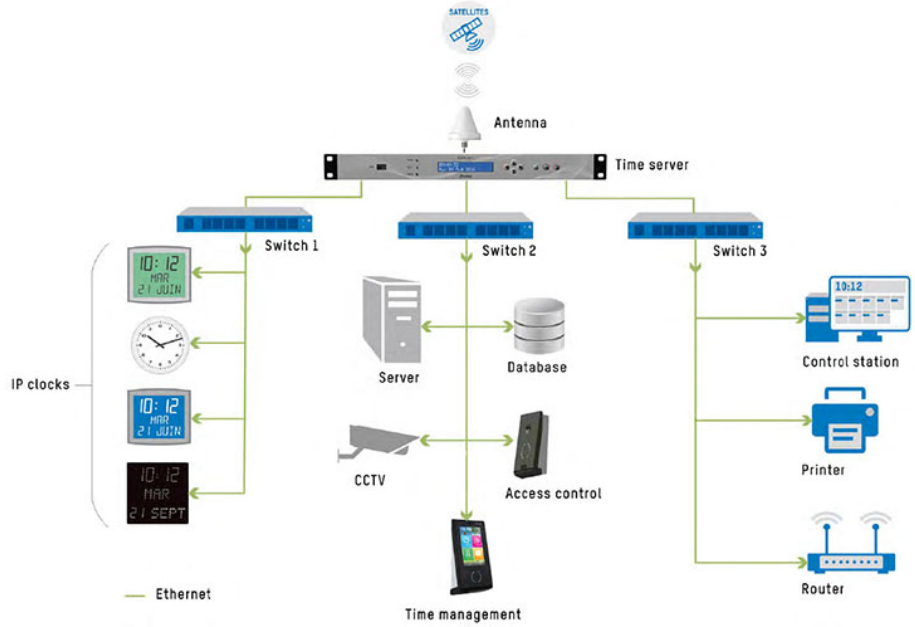
- *moderované*
- *nemoderované*



9.2.7 Časový server

Server, který periodicky synchronizuje čas ve všech počítačích v rámci sítě. Tím je zajištěna shodnost času používaného síťovými službami a místními funkcemi.
Potvrzení od důvěryhodné třetí strany o existenci určité zprávy v určitý časový okamžik. V digitálním kontextu důvěryhodná třetí strana vygeneruje pro danou zprávu důvěryhodné časové razítko tak, že pomocí služby časového razítka doplní do zprávy příslušnou časovou hodnotu a pak výsledek digitálně podepíše.

- pro připojení do počítačové sítě dochází k synchronizaci času mezi naším počítačem a serverem, ke kterému se připojujeme
- u rozsáhlých sítí je to složitější ⇒ existují časové servery, které poskytují přesný čas (buď získaný z jiného časového serveru, nebo přímo z časového etalonu – atomové hodiny, signál šířený dlouhými radiovými vlnami)



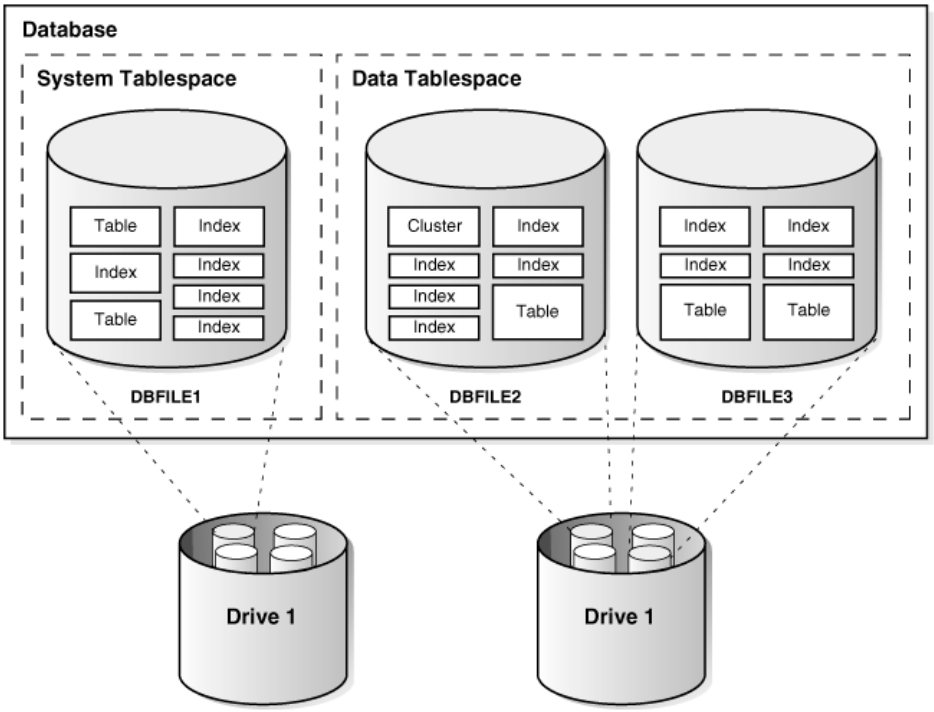
9.2.8 Databázový server

Databázový server (database server) umožňuje uživatelům sdílet data ve společné databázi a poskytuje jim možnost přístupu k ní. Dále zabezpečuje udržení integrity sdílené databáze. Přístup k databázi pomocí databázového serveru (na rozdíl od souborového) výrazně snižuje tok dat sítí, čímž přispívá ke zvýšení jejího výkonu.

Jazykem pro přístup k databázím je ***SQL- Structure Query Language***

Z hlediska způsobu ukládání dat a vazeb mezi nimi můžeme rozdělit databáze do základních typů:

- Hierarchická databáze
- Síťová databáze
- Relační databáze
- Objektová databáze
- Objektově relační databáze



9.2.9 WWW server

Počítač, který je spravován správcem systému nebo poskytovatelem služeb sítě Internet (ISP) a který reaguje na požadavky prohlížeče uživatele. *Internet Information Server*. Server vyvinutý firmou Microsoft pro jejich operační systém Windows NT Server. Obsahuje FTP a WWW server.

- TCP port 80
- hypertextové spojení s dokumenty
- přenos textu, souborů, obrazů, zvuků, videa apod.
- systém dotazovacích serverů

Základní pojmy:

HTTP – Hypertext Transfer Protocol

- kromě zobrazitelných znaků obsahuje i další odkazy na související text

HTML – Hypertext Markup Language

- obsahuje řídící znaky a texty
- obsahuje formáty a odkazy

URL – Uniform Resource Locator

- *schéma: //jméno:heslo@počítač:port-cesta k souboru?parametr*
- schéma: http, shttp, ftp, telnet, gopher, news, mailto, file
- parametr: parametry předávané úloze běžící na serveru
- URL může být lokální (do téhož dokumentu…#), nebo globální; může také být absolutní nebo relativní (obsah se doplňuje automaticky, není vázáno k určitému paměťovému médiu)

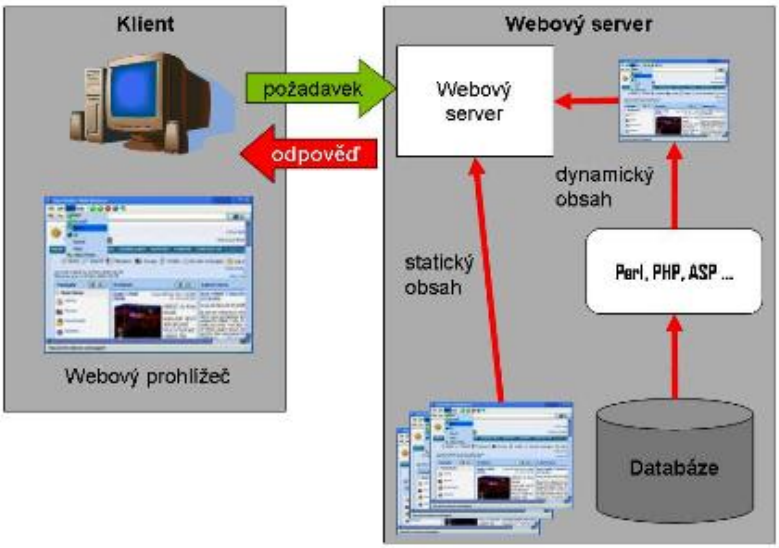
Formát přenášených dat:

```
<HTML>
  <HEAD>          záhlaví…autorská práva, vypršení platnosti, kódování
  </HEAD>
  <BODY>
  </BODY>         vlastní tělo….vlastní stránka
</HTML>
```

značky v dokumentu (tagy) buď párové nebo nepárové (např. <p>)

Dokumenty (html stránky):

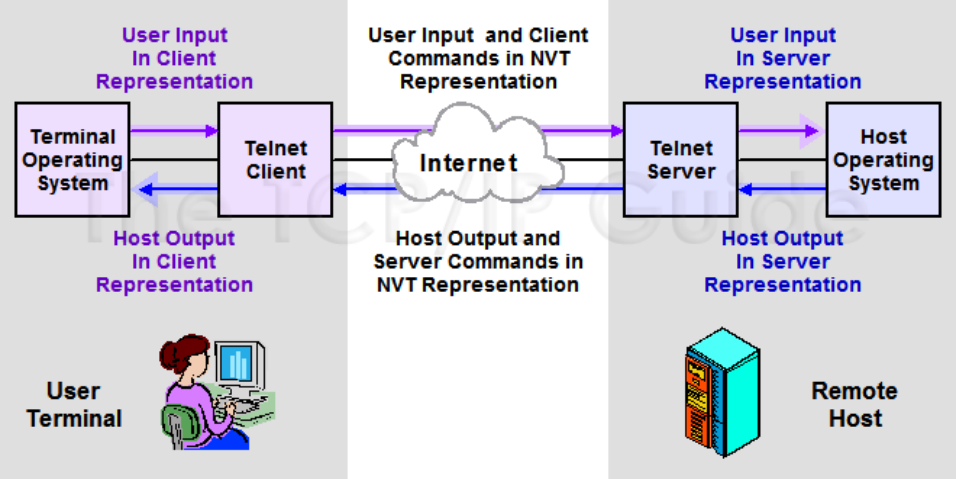
- statické – soubory předem vytvořené přenášené do počítače
- dynamicky vytvářené – podle aktuálního požadavku uživatele
  - vyžadují existenci programu pro vytvoření té podoby stránky jak na straně serveru, tak i na straně klienta
  - používání CGI skriptu „Common Gateway Interface“ – jazyk vyšší úrovně (většinou interpretační) – PHP, Perl, DHTML, Java



9.3 Služby aplikační vrstvy

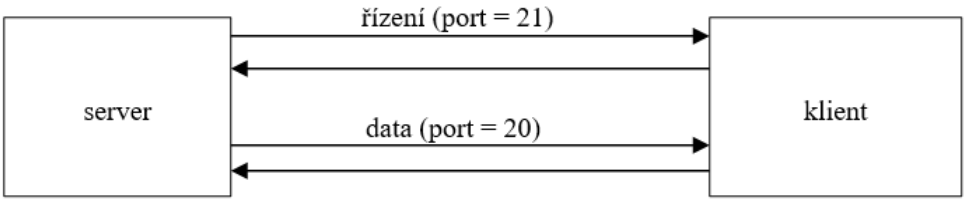
9.3.1 TELNET – vzdálený terminál

- historicky různé typy terminálů: VT100, VT320… (čím větší číslo tím dokonalejší)
- služba telnetu je implicitně přístupná přes port = 23
- znaky na telnet klientovi se zobrazují na obrazovce až po vrácení z telnet serveru
- proti odzírání ve formě otevřené podoby se používá ***ssh –secured shell*** ⇒ prostředek umožňující normální funkce, ale v šifrované podobě; použití port = 22



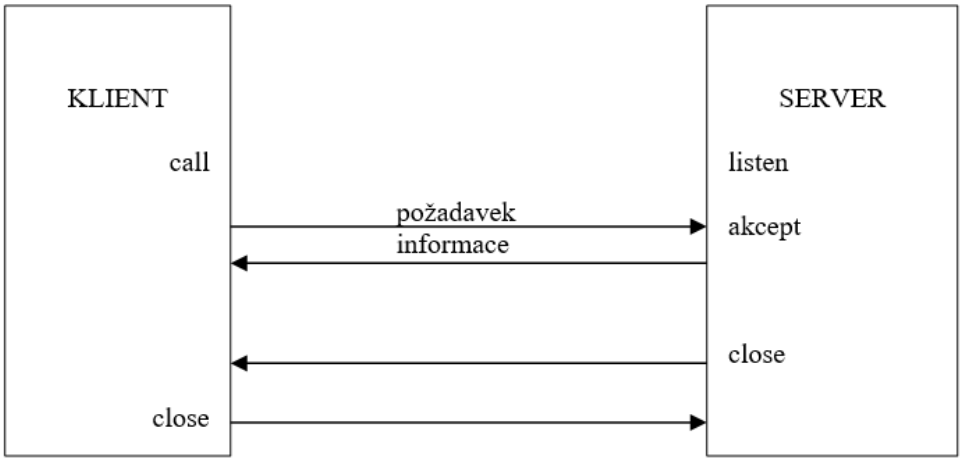
9.3.2 FTP – File Transfer protocol

- ftp serverů je ve světě hodně
- zajišťují binární přenos dat
- zvláštní formou jsou pak indexové servery ⇒ *archie servery* (jméno programu a místo uložení)



9.3.3 FINGER

- získávání informací o uživatelích vzdáleného systému
- textově orientovaný protokol
- protokol TCP port = 79
- architektura server/klient

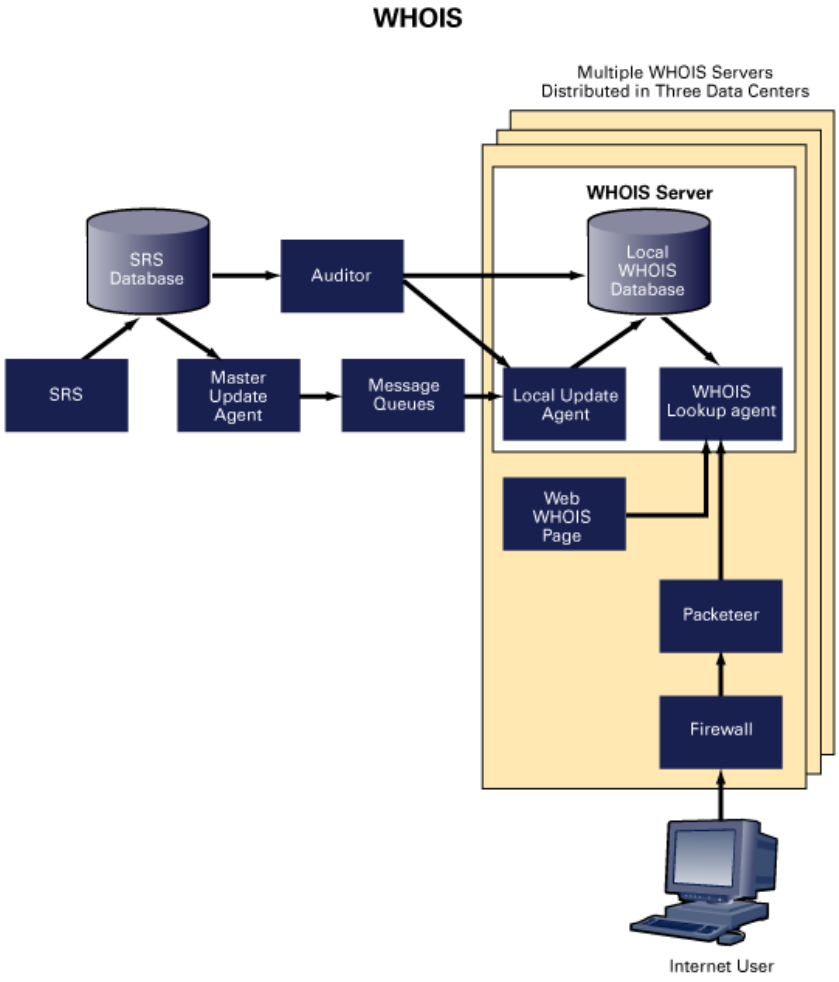


9.3.4 NETFIND

- získávání informací o uživatelích nějaké domény
- ve světě několik serverů, které podporují tudle službu (většinou podle pro jednotlivé státy, např. u nás: netfind.vslib.cz
- přístup k této službě pomocí telnetu nebo bránou přes http protokol

9.3.5 WHOIS

- prostřednictvím centralizované databáze poskytuje tato služba informace o zaregistrovaných uživatelích
- interaktivní prostředí, ve kterém pak pomocí dotazů získáváme informaci o nějakém člověku



10. DNS (Domain Name System)

Všechny aplikace, které zajišťují komunikaci mezi počítači, používají k identifikaci komunikujících uzlů IP-adresu. Pro člověka jako uživatele jsou však IP-adresy těžko zapamatovatelné. Proto se používá místo IP-adresy název síťového rozhraní. Pro každou IP-adresu máme zavedeno jméno síťového rozhraní (počítače), přesněji řečeno doménové jméno.

Jedna IP-adresa může mít přiřazeno i několik doménových jmen. Vazba mezi jménem počítače a IP adresou je definována v DNS databázi. DNS (*Domain Name System*) je celosvětově distribuovaná databáze. Jednotlivé části této databáze jsou umístěny na tzv. name serverech.

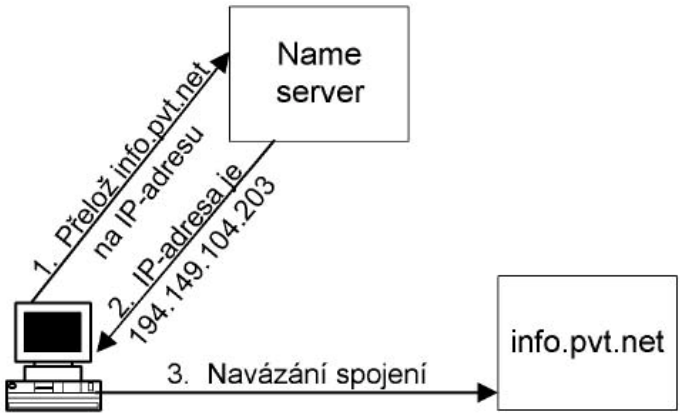
Příklad:
Chci-li se přihlásit na uzel info.pvt.net s IP adresou 194.149.104.203, použiji příkaz:

```
telnet info.pvt.net.
```

Ještě předtím, než se vlastní příkaz provede, přeloží se DNS jméno info.pvt.net na IP adresu a teprve poté se provede příkaz:

```
telnet 194.149.104.203
```

Před navázáním spojení je nutné přeložit jméno na IP-adresu



Použití IP-adres místo doménových jmen je praktické vždy, když máme podezření, že DNS nám na počítači nepracuje korektně. Pak, ač to vypadá nezvykle, můžeme napsat např:

```
ping 194.149.104.203
http://194.149.104.203
```

10.1 Domény a subdomény

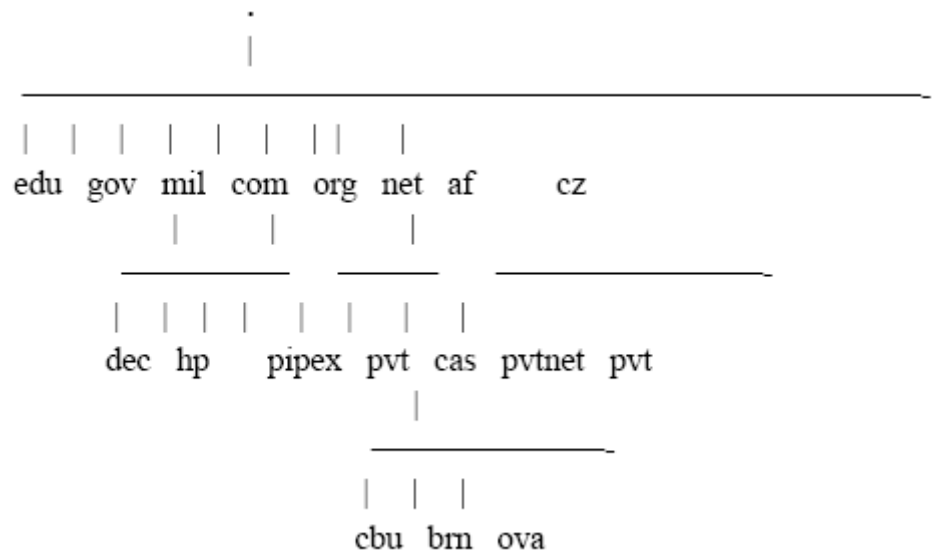
Celý Internet je rozdělen do tzv. domén, tj. skupin jmen, která k sobě logicky patří. Domény specifikují, patří-li jména jedné firmě, jedné zemi apod. V rámci domény je možné vytvářet podskupiny, tzv. subdomény, např. doméně firmy lze vytvořit subdomény pro oddělení.

Doménové jméno odráží příslušnost uzlu do skupiny a podskupiny. Každá skupina má přiřazeno jméno. Z jednotlivých jmen skupin je pak složeno doménové jméno uzlu. Např. uzel se jménem **jakub.firma.cz** je uzel se jménem **jakub** v subdoméně **firma** domény **cz**.

Doménové jméno se skládá z řetězců vzájemně oddělených tečkou. **Jméno se zkoumá zprava doleva**. Nejvyšší instancí je tzv. **root doména**, která se vyjadřuje tečkou zcela vpravo (tato tečka bývá často vypouštěna). V root doméně jsou definované generické domény (*Top Level Domains – TLD*): **edu, com, net, org, mil, int** a **arpa**, které se používají převážně v USA, a dále podle normy ISO-3166 dvojznakové domény jednotlivých států. **Pro Českou republiku je vyhrazena doména cz**.

Doména cz se dělí na subdomény pro jednotlivé organizace: mvso.cz (pro MVŠO o.p.s), cas.cz (pro Českou Akademii Věd), cvut.cz (pro ČVUT) atd. Subdomény se mohou dělit na subdomény nižší úrovně. Např. entu.cas.cz (Entomologický ústav ČAV) atd. Subdomény obsluhují jako prvky počítače.

Jména tvoří stromovou strukturu:



Doména cz obsahuje doménu pvtnet. Doména pvtnet.cz obsahuje krajské subdomény: **pha, cbu, plz, unl, hrk, brn a ova**. Teoreticky by mohly být prvky těchto subdomén i subdomény ještě nižší úrovně atd.

10.2 Syntaxe jména

Jméno je uváděno v tečkové notaci. Např. abc.cbu.pipex.cz. Jméno má obecně syntaxi:

```
řetězec.řetěžěc.řetězec....řetězec.
```

kde první řetězec je jméno počítače, další jméno nejnižší vnořené domény, další vyšší domény atd. Pro jednoznačnost se na konci uvádí také tečka, vyjadřující root doménu. **Celé jméno může mít maximálně 255 znaků**, **řetězec pak maximálně 63 znaky**. Řetězec se může skládat z písmen, číslic a pomlčky. Pomlčka nesmí být na začátku ani na konci řetězce.

Mohou se použít velká i malá písmena, ale není to zase tak jednoduché. Z hlediska uložení a zpracování v databázi jmen (databázi DNS) se velká a malá písmena nerozlišují. Tj. jméno *newyork.com* bude uloženo v databázi na stejné místo jako *NewYork.com* nebo *NEWYORK.com* atp.

Tedy při překladu jména na IP-adresu je jedno, kde uživatel zadá velká a kde malá písmena. Avšak v databázi je jméno uloženo s velkými a malými písmeny, tj. byloli tam uloženo např. *NewYork.com*, pak při dotazu databáze vrátí *NewYork.com*. Poslední tečka je součástí jména.

V některých případech se může část jména zprava vynechat. Téměř vždy můžeme koncovou část doménového jména vynechat v aplikačních programech. V databázích popisujících domény je však situace složitější.

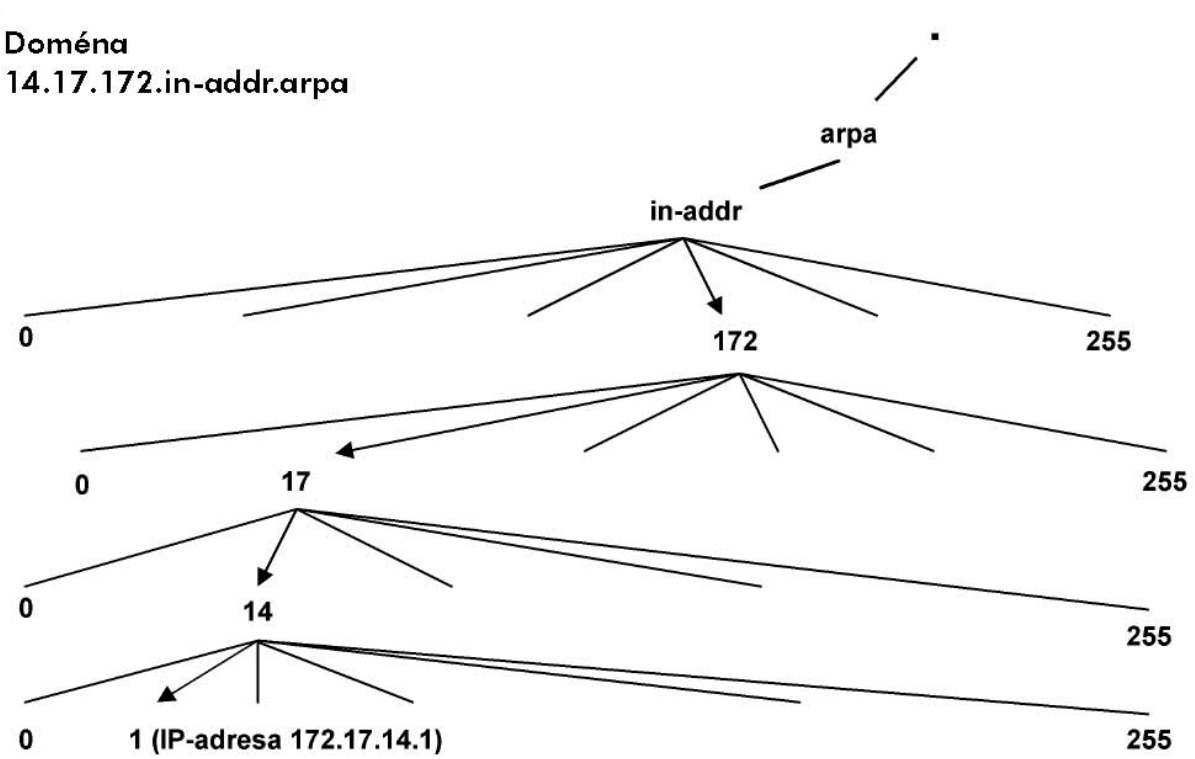
Je možné vynechat:

- Poslední tečku téměř vždy.
- Na počítačích uvnitř domény se zpravidla může vynechat konec jména, který je shodný s názvem domény. Např. uvnitř domény pipex.cz, je možné psát místo počítač.abc.pipex.cz jen počítač.abc (nesmí se ale uvést tečka na konci!).

10.3 Reverzní domény

Některé aplikace naopak **potřebují k IP-adrese nalézt jméno**, tj. nalézt tzv. reverzní záznam. Jedná se tedy o překlad IP-adresy na doménové jméno. Tento překlad se často nazývá **zpětným (reverzním) překladem**.

Pro účely reverzního překladu byla definována pseudodoména „in-addr.arpa“. Jméno této pseudo domény má historický původ, jde o zkratku „*inverse addresses in the Arpanet*“.



Pod doménou in-addr.arpa jsou domény jmenující se jako první číslo z IP-adresy sítě.
Např. síť 194.149.101.0 patří do domény 194.in-addr.arpa. Síť 172.17 patří do domény 172.in-addr.arpa. Dále doména 172.in-addr.arpa se dělí na subdomény, takže síť 172.17 tvoří subdoménu 17.172.in-addr.arpa. Je-li síť 172.17 rozdělena pomocí síťové masky na subsítě, pak každá subsíť tvoří ještě vlastní subdoménu.

Reverzní domény pro subsítě adres třídy C jsou tvořeny podle metodiky classless in-addr.arpa. Přestože IP-adresa má pouze 4 bajty a klasická reverzní doména má tedy maximálně 3 čísla, jsou reverzní domény pro subsítě třídy C tvořeny 4 čísly.

Příklad:
Reverzní doména pro subsíť 194.149.150.16/28 je 16.150.149.194.in-addr.arpa

10.4 Doména 0.0.127.in-addr.arpa

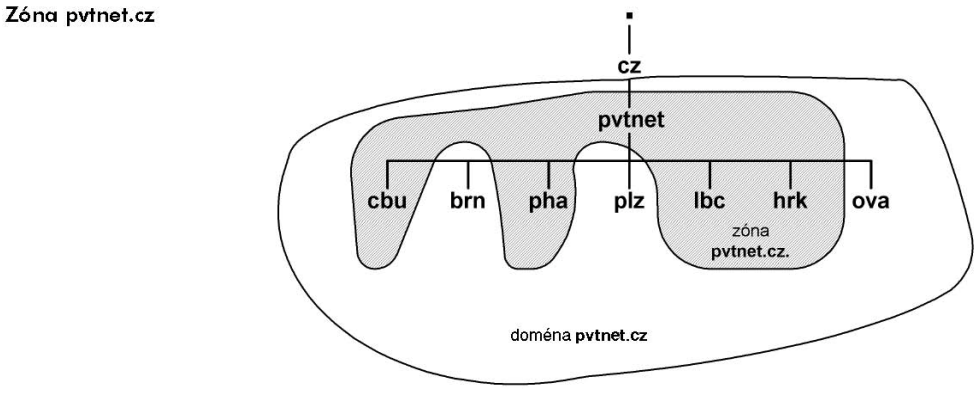
Jistou komplikací (zvláštností) je adresa sítě 127.0.0.1. Síť 127 je totiž určena pro *loopback*, tj. softwarovou smyčku na každém počítači. Zatímco ostatní IP-adresy jsou v Internetu jednoznačné, adresa 127.0.0.1 se vyskytuje na každém počítači.

Každý name server je autoritou nejen „obyčejných“ domén, ale ještě autoritou (primárním name serverem) k doméně **0.0.127.in-adr.arpa**. V dalším textu budeme tento fakt považovat za samozřejmost a v tabulkách jej pro přehlednost nebudeme uvádět, ale nikdy na něj nesmíte zapomenout.

10.5 Zóna

Často se setkáváme s otázkou: „Co je to zóna?“ „Jaký je vztah mezi doménou a zónou?“.
Jak jsme již uvedli, **doména je skupina počítačů, které mají společnou pravou část svého doménového jména**. Doména je např. skupina počítačů, jejichž jméno končí cz. Doména cz je však velká. Dělí se dále na subdomény např. pvt.cz, eunet.cz a tisíce dalších. Každou z domén druhé úrovně si většinou spravuje na svých name serverech majitel domény nebo jeho poskytovatel Internetu.

Data pro doménu druhé úrovně např. pvt.cz nejsou na stejném name serveru jako doména cz. Jsou rozložena na mnoho name serverů. Data o doméně uložená na name serveru jsou nazývána zónou. Zóna tedy obsahuje jen část domény. **Zóna je část prostoru jmen, kterou obhospodařuje jeden name server.**



10.6 Rezervované domény a pseudodomény

Později se ukázalo, že jako TLD je možné využít i jiné domény. Některé další TLD byly rezervovány RFC-2606:

- doména **.test** pro testování.
- doména **.expample** pro vytváření dokumentace a příkladů.
- doména **.invalid** pro navozování chybových stavů.
- doména **.localhost** pro softwarovou smyčku

Obdobně byla rezervována doména **.local** pro intranety. Význam této domény je obdobný jako význam sítě 10.0.0.0/8. V intranetu je tak možné využívat nejednoznačnou doménu, čímž si ulehčíme práci se dvěma různými doménami stejného jména *firma.cz* – jednou v Internetu a druhou v intranetu.

Z výše uvedeného obrázku je patrné, že mohou existovat i domény, které nejsou přímo připojeny k Internetu, tj. jejichž počítače ani nepoužívají síťový protokol TCP/IP – tedy nemají ani IP-adresu. Takovéto domény se někdy označují jako pseudodomény. Mají význam zejména pro elektronickou poštu.

Pomocí pseudodomény lze řešit problém posílání elektronické pošty do jiných sítí než Internet (např. DECnet či MS Exchange).

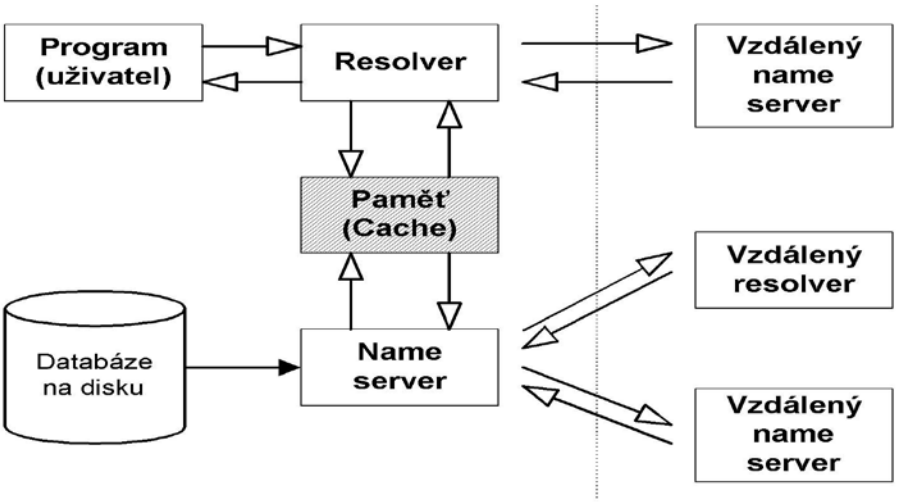
10.7 Dotazy (překlady)

Přeložení jména na IP-adresu zprostředkovává tzv. resolver. **Resolver je klient, který se dotazuje name serveru**. Jelikož je databáze celosvětově distribuována, nemusí nejbližší name server znát odpověď, proto může tento name server požádat o pomoc další name servery. Získaný překlad pak name server vrátí jako odpověď resolveru. Veškerá komunikace se skládá z dotazů a odpovědí.

Name server po svém startu načte do paměti data pro zónu, kterou spravuje. **Primární name server** načte data z lokálního disku, **sekundární name server dotazem zone transfer** získá pro spravované zóny data z primárního name serveru a rovněž je uloží do paměti. Tato **data primárního a sekundárního name serveru se označují jako autoritativní (nezvratná)**.

Dále name server načte z lokálního disku do paměti data, která nejsou součástí dat jeho spravované zóny, ale umožní mu spojení s **root name servery** a případně s name servery, kterým delegoval pravomoc pro spravování subdomén. **Tato data se označují jako neautoritativní.**

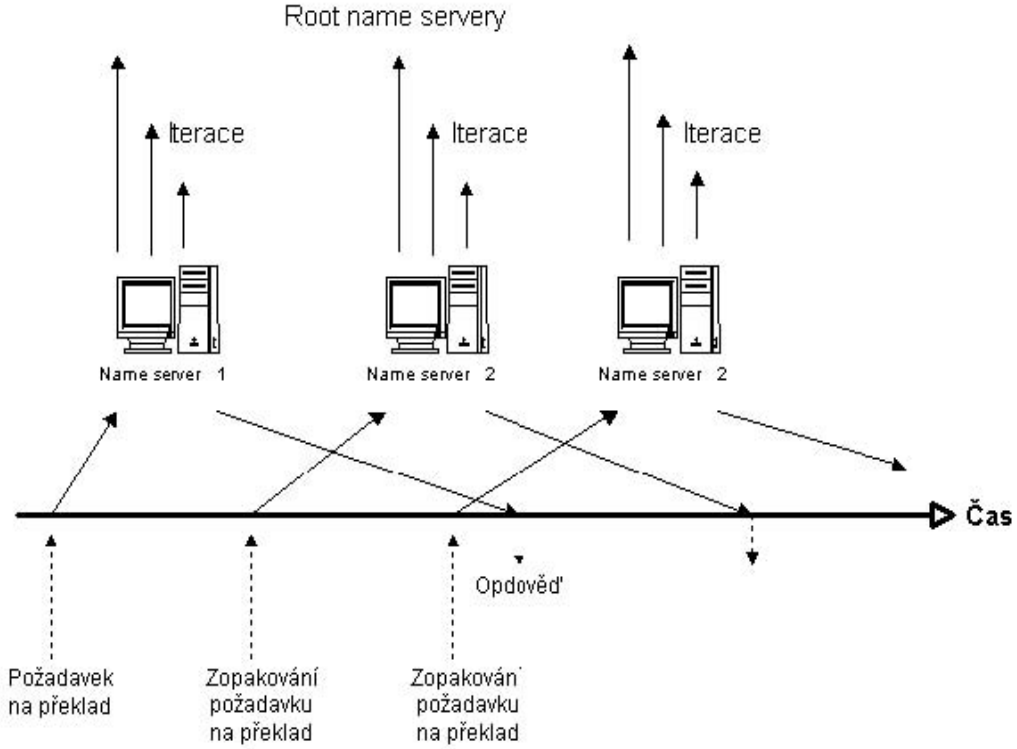
Name server i resolver společně sdílejí paměť cache. Během práce do ní ukládají kladné odpovědi na dotazy, které provedly jiné name servery, tj. ke kterým jsou jiné name servery autority. Ale z hlediska našeho name serveru jsou tato data opět neautoritativní – pouze šetří čas při opětovných dotazech.



Do paměti se ukládají jen kladné odpovědi. Provoz by byl podstatně zrychlen, kdyby se tam **ukládaly i negativní odpovědi (negativní caching)**, avšak to je podstatně složitější problém. Podpora negativního cachingu je záležitostí posledních několika let.

Takto pracuje DNS na serverech (např. s operačním systémem NT nebo UNIX). Avšak např. **PC nemívají realizovány servery**. V takovém případě se celý mechanismus redukuje na tzv. **pahýlový resolv**er. Tj. z celého mechanismu zůstane pouze resolver.

DNS používá jak protokol UDP, tak i protokol TCP. Pro oba protokoly používají port 53 (tj. porty 53/udp a 53/tcp). Běžné dotazy, jako je překlad jména na IP-adresu a naopak, se provádějí přes protokol UDP. Délka přenášených dat protokolem UDP je implicitně omezena na 512 B.

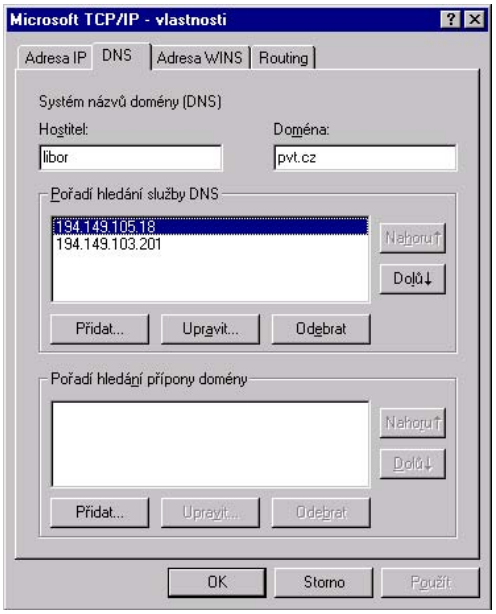


10.8.1 Resolver

Resolver je komponenta systému zabývající se překladem IP-adresy. Resolver je klient. Resolver není konkrétní program. Je to soustava knihovních funkcí, která se sestavuje (linkuje) s aplikačními programy, požadujícími tyto služby (např. telnet, ftp, WWW-prohlížeč atd.). Tj. potřebuje-li např. telnet převést jméno počítače na jeho IP-adresu, pak zavolá příslušné knihovní funkce.

Klient (např. zmíněný telnet) zavolá knihovní funkce, které zformulují dotaz a vyšlou jej na server. Server je v UNIXu realizován programem *named*. Server buď překlad provede sám, nebo si sám vyžádá pomoc od dalších serverů, nebo zjistí, že překlad není možný.

V systému NT se resolver konfiguruje pomocí okna. Do pole doména vyplníme lokální doménu, která se bude doplňovat ke jménům v případě, že neuvedeme na konci tečku. Pakliže překlad s touto doplněnou doménou i bez ní selže, pak se systém pokusí ještě doplňovat domény z okna „Pořadí hledání přípony domény“.



10.8.2 Name server

Name server udržuje informace pro překlad jmen počítačů na IP-adresy (resp. pro reverzní překlad). Name server obhospodařuje nějakou část z prostoru jmen všech počítačů. Tato část se nazývá zóna.

Zóna je tvořena doménou nebo její částí. Name server totiž může pomocí věty typu NS ve své konfiguraci delegovat spravování subdomény na name server nižší úrovně. Name server je program, který provádí na žádost resolveru překlad. V UNIXu je name server realizován programem *named*.

Podle uložení dat rozlišujeme následující typy name serverů:

- **Primární name server** udržuje data o své zóně v databázích na disku. Pouze na primárním name serveru má smysl editovat tyto databáze.
- **Sekundární name server** si kopíruje databáze v pravidelných časových intervalech z primárního name serveru. Tyto databáze nemá smysl na sekundárním name serveru editovat, nebo budou při dalším kopírování přepsány. Primární i sekundární name servery jsou tzv. autoritou pro své domény, tj. jejich data pro příslušnou zónu se považují za nezvratná (autoritativní).
- **Caching only server** není pro žádnou doménu ani primárním, ani sekundárním name serverem (není žádnou autoritou). Avšak využívá obecné vlastnosti name serveru, tj. data, která jím prochází, ukládá ve své paměti. Tato data se označují jako neautoritativní.
- **Root name server** je name server obsluhující root doménu. Každý root name server je primárním serverem, což jej odlišuje od ostatních name serverů.

Z hlediska klienta není žádný rozdíl mezi primárním a sekundárním name serverem. Oba mají data stejné důležitosti – oba jsou pro danou zónu autoritami. Klient nemusí ani vědět, který server pro zónu je primární a který sekundární. Naproti tomu caching server není autoritou, tj. nedokáže-li provést překlad, pak kontaktuje autoritativní server pro danou zónu.

Program *nslookup* je užitečný program pro správce name serveru. Chcete-li programem nslookup provádět dotazy jakoby name serverem, pak zakažte rekurence a přidávání doménových jmen příkazy:

```
$ nslookup
set norecurse
set nosearch
```

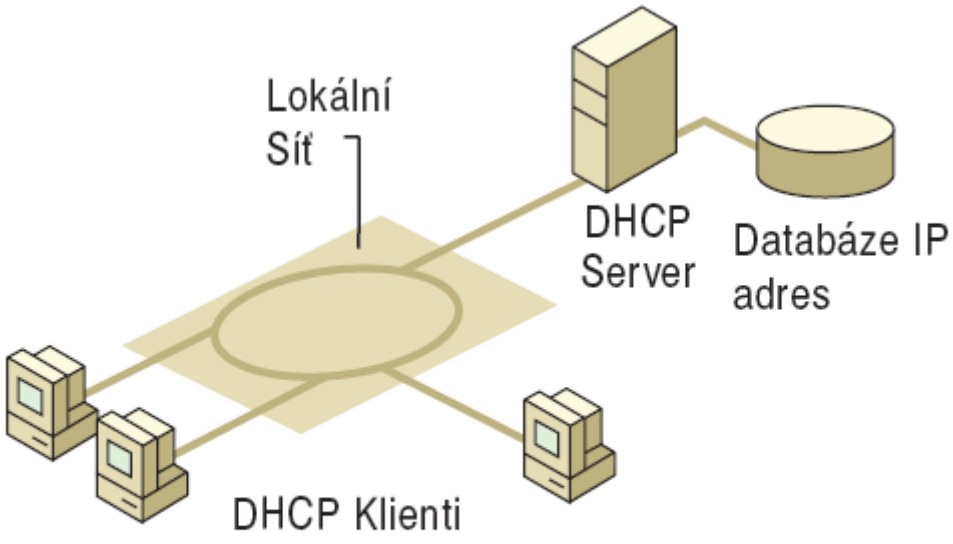
11. DHCP

Protokol DHCP zjednodušuje správu konfigurace adresy IP pomocí automatického konfigurování adres pro síťové klienty. Standard protokolu DHCP zajišťuje používání serverů DHCP, které jsou definovány jako jakýkoli počítač, na němž běží služba DHCP. Server DHCP automaticky přiřazuje adresy IP a podobná nastavení konfigurace protokolu TCP/IP počítačů na síti podporujících protokol DHCP.

Každé zařízení na síti založené na protokolu TCP/IP musí mít jedinečnou adresu IP, aby bylo schopno přistupovat k síti a jejím prostředkům. Bez protokolu DHCP je nutno provést nakonfigurování protokolu IP ručně u nových počítačů, počítačů přesunovaných z jedné podsítě na jinou a počítače odebírané ze sítě.

11.1 Funkce DHCP

Protokol DHCP je založen na modelu klient/server, jak je znázorněno na obrázku.



Základní model protokolu DHCP

Správce sítě zakládá jeden nebo více serverů DHCP, které udržují informace o konfiguraci protokolu TCP/IP a poskytují konfiguraci adres klientům podporujícím službu DHCP ve formě nabídky zápůjčky.

Server DHCP uchovává informace o konfiguraci v databázi, která zahrnuje:

- Parametry konfigurace protokolu TCP/IP platné pro všechny klienty na síti.
- Platné adresy IP udržované ve fondu adres pro přiřazení klientům, stejně jako adresy vyhrazené pro ruční přiřazení.
- Doba trvání zápůjčky nabízená serverem – doba, po kterou může být adresa IP používána před nutností obnovení zápůjčky.

Klient podporující službu DHCP při přijetí nabídky zápůjčky obdrží:

- Platnou adresu IP pro síť, ke které se připojuje.
- Další parametry konfigurace protokolu TCP/IP, které se označují jako možnosti DHCP.

11.2 Výhody protokolu DHCP

Instalací protokolu DHCP na svou rozlehlou síť získáte následující výhody:

- Bezpečnou a spolehlivou konfiguraci. Protokol DHCP minimalizuje chyby v konfiguraci způsobené manuální konfigurací adres IP, například chyby v psaní, stejně jako minimalizuje konflikty adres způsobené přiřazením již aktuálně používané adresy IP dalšímu počítači.
- Sníženou správu sítě.
- Konfigurace protokolu TCP/IP je centralizovaná a automatizovaná.
- Správci sítě mohou centrálně definovat konfigurace protokolu TCP/IP jak obecně, tak pro konkrétní podsíť.
- Klientům lze automaticky přiřazovat plný rozsah dalších konfiguračních hodnot protokolu TCP/IP pomocí možností DHCP.
- Změny adres pro konfigurace klienta, které musí být často aktualizovány, například klienti se vzdáleným přístupem, kteří se neustále pohybují, lze provádět efektivně a automaticky při spuštění klienta ze svého nového umístění.
- Většina směrovačů může předat požadavky na konfiguraci pomocí služby DHCP, čímž se omezují požadavky na nastavení serveru DHCP na každé podsíti, pokud k tomu není důvod.

11.3 Autokonfigurace protokolu IP

Klienti na platformě Windows si mohou automaticky nakonfigurovat adresu IP a masku podsítě v případě, že je server DHCP v okamžiku spuštění systému nedostupný. Tato vlastnost nazvaná APIPA (Automatic Private IP Addressing) je užitečná pro klienty na malých soukromých sítích.

Při autokonfiguraci klienta DHCP probíhá následující proces:

1. Klient DHCP se snaží lokalizovat server DHCP a získat adresu a konfiguraci.
2. Jestliže nelze server DHCP nalézt, případně neodpovídá, klient DHCP si sám nakonfiguruje adresu IP a masku podsítě za použití vybrané adresy ze sítě třídy B rezervované pro Microsoft, 169.254.0.0 s maskou podsítě 255.255.0.0. Klient DHCP hledá konflikty adres, aby se ujistil, že vybraná adresa již není na příslušné síti používána. Pokud je nalezen konflikt, klient vybere jinou adresu IP: Klient se pokusí o autokonfiguraci až do 10 adres.
3. Jakmile klient DHCP uspěje při samostatném výběru adresy, nakonfiguruje s touto adresou IP své síťové rozhraní. Klient pak na pozadí pokračuje v intervalech 5 minut v hledání serveru DHCP. Jestliže klient najde server DHCP později, opustí

svou autokonfiguraci. Klient DHCP pak použije adresu nabídnutou serverem DHCP (a jakékoli další informace možností DHCP) a zaktualizuje své nastavení konfigurace protokolu IP.

Jestliže již dříve klient DHCP obdržel zápůjčku serveru DHCP:

1. Jestliže je zápůjčka klientovi během spouštění systému stále platná (nevypršela), klient se pokusí obnovit tuto zápůjčku.
2. Jestliže během snahy obnovit zápůjčku klient neuspěje při lokalizaci serveru DHCP, bude se snažit provést příkaz ping na přednastavenou bránu uvedenou v zápůjčce a bude pokračovat jedním z následujících způsobů:
   - Jestliže je provedení příkazu ping úspěšné, klient DHCP předpokládá, že je stále umístěn na stejné síti, odkud získal svou aktuální zápůjčku a pokračuje v jejím užívání.
   - Jestliže je provedení příkazu ping neúspěšné, klient DHCP předpokládá, že byl přesunut na síť, kde nejsou služby DHCP dostupné. Klient pak provede autokonfiguraci své adresy IP.

11.4 Proces zápůjčky DHCP

Klient podporující službu DHCP obdrží od serveru DHCP zápůjčku na adresy IP. Před vypršením časového omezení zápůjčky musí server DHCP tuto zápůjčku klientovi obnovit nebo klient musí získat novou zápůjčku.

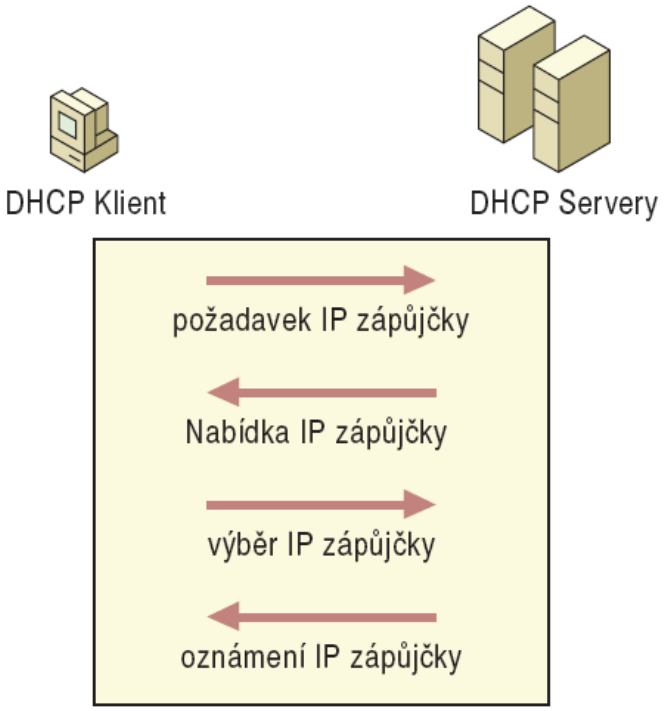
Zápůjčky jsou v databázi serveru DHCP uchovávány přibližně jeden den po vypršení. Tato poskytnutá lhůta chrání zápůjčku klienta v případě, že klient a server jsou v různých časových pásmech, jejich interní hodiny nejsou synchronizovány nebo klient je v době vypršení zápůjčky mimo síť.

11.4.1 Zprávy DHCP

Tabulka popisuje zprávy DHCP vyměňované mezi klientem a serverem.

Typ zprávy	Popis
DHCPDiscover	Požadavek na přidělení IP adresy s DHCP serveru. Jelikož se jedná o první přihlášení (klient ještě nemá IP adresu) je zdrojová adresa IP paketu 0.0.0.0.
DHCPOffer	Pokud server obdrží paket DHCPDiscover odpoví paketem DHCPOffer obsahující nezapůjčenou IP adresu a další informace o nastavení protokolu TCP/IP.
DHCPRequest	Pokud klient obdrží paket DHCPOffer, odpoví serveru paketem DHCPRequest a tím potvrdí obdržení IP adresy.
DHCPAcknowkedge (DHCPAck)	Tímto paketem potvrdí klientovi doručení paketu DHCPRequest a dodá i další informace nezbytné pro dokončení konfigurace TCP/IP protokolu.
DHCPNak	Pokud přidělaná IP adresa již není platná, nebo byla přidělena jinému klientovi, odpoví server paketem DHCPNak a proces zápůjčky započne znovu.

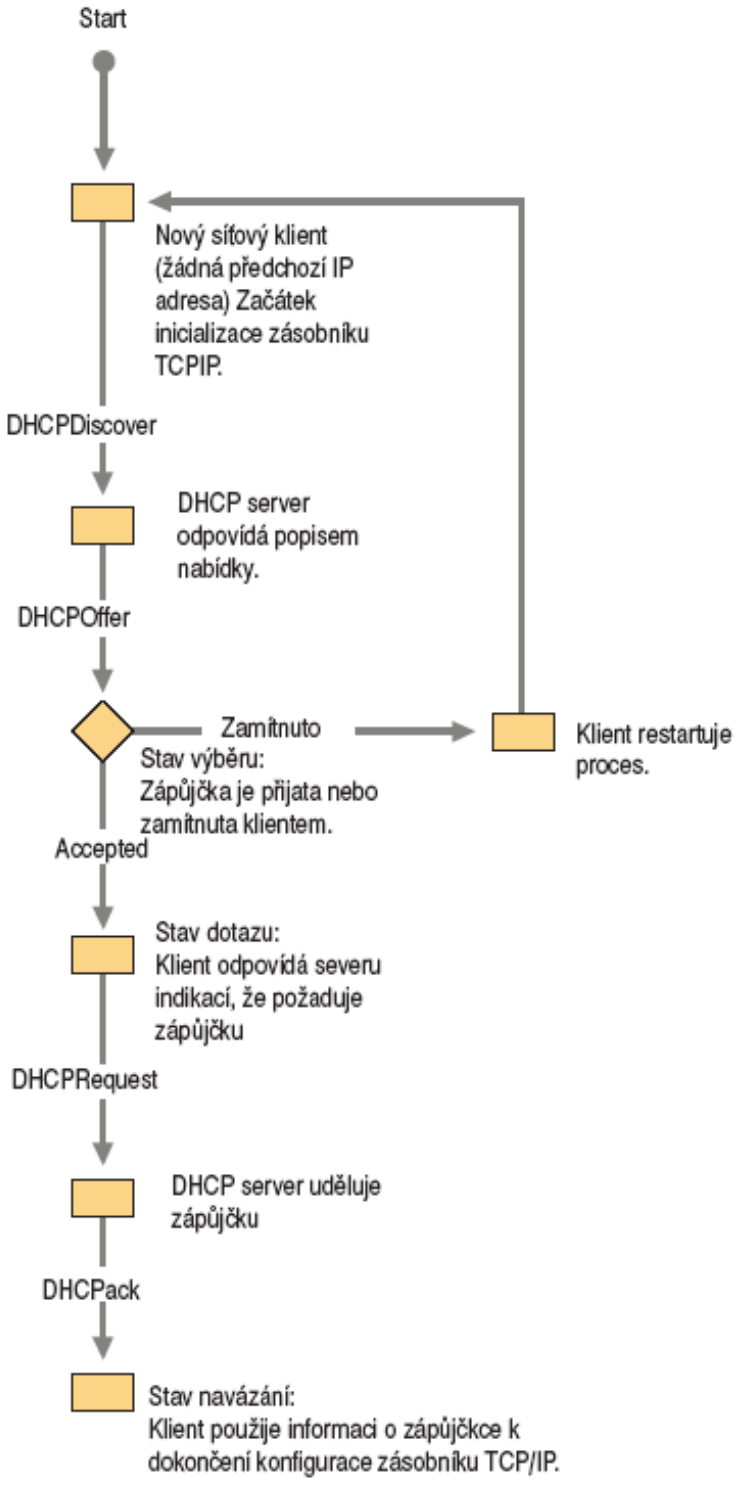
DHCPDecline	Jestliže klient zjistí, že nabízené parametry konfigurace TCP/IP protokolu jsou neplatné, pošle serveru paket DHCPDecline.
DHCPRelease	Klient zašle paket DHCPRelease serveru, aby uvolnil a zrušil jakoukoliv zápůjčku, která pro něj byla vytvořena.



11.4.2 Funkce procesu zápůjčky

Jakmile se poprvé spustí klient podporující DHCP a pokusí se připojit k síti, automaticky následuje inicializační proces k získání zápůjčky od serveru DHCP.

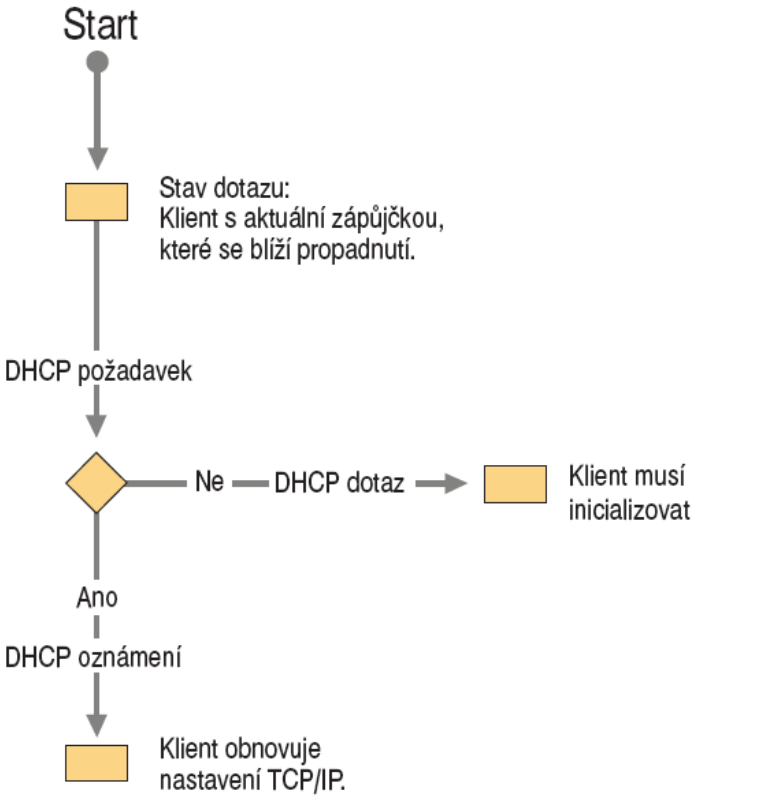
1. Klient DHCP požaduje adresu IP prostřednictvím všesměrového vysílání zprávy DHCPDiscover na lokální podsíti.
2. Klientovi je nabídnuta adresa, když server DHCP reaguje zprávou DHCPOffer obsahující adresu IP a informace o konfiguraci pro zápůjčku.



Stavy klienta DHCP během procesu zápůjčky

3. Klient sdělí přijetí nabídky výběrem nabízené adresy a odpovědí serveru pomocí zprávy DHCPRequest.
4. Klientovi je přiřazena adresa a server DHCP mu pošle zprávu DHCPAck potvrzující zápůjčku. Ve zprávě mohou být obsaženy i informace o dalších možnostech DHCP.
5. Poté, co klient obdrží potvrzení, nakonfiguruje si vlastnosti protokolu TCP/IP za použití jakékoli informace o možnosti DHCP obsažené v odpovědi a připojí se k síti.

Ve vzácných případech může server DHCP vrátit klientovi negativní potvrzení. To se může stát, jestliže klient žádá neplatnou nebo duplikovanou adresu. Jestliže klient obdrží negativní potvrzení (DHCPNak) musí klient začít celý proces zápůjčky znovu.



Stavy klienta DHCP během procesu obnovování zápůjčky

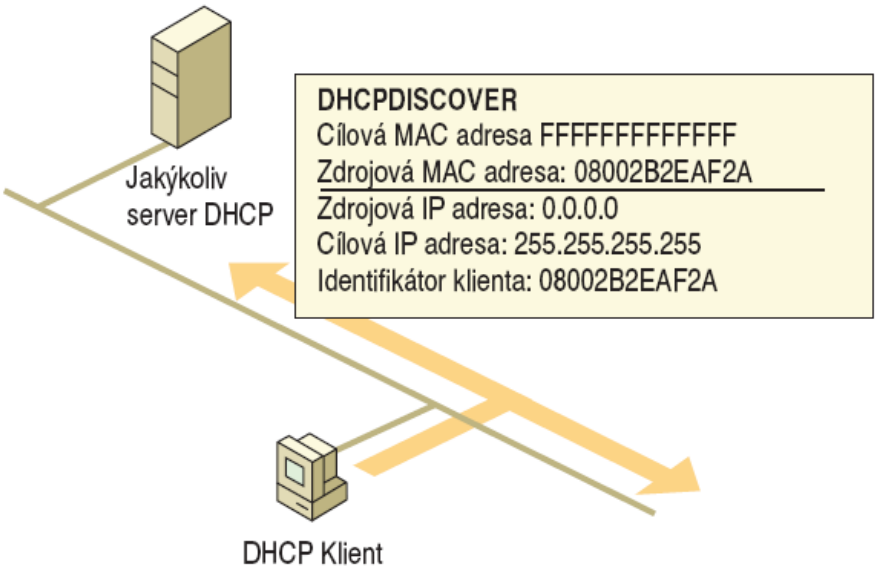
11.5 Stavy klienta DHCP v procesu zápůjčky

Cyklus klienta DHCP přes šest různých stavů klienta během procesu zápůjčky DHCP. Když je klient DHCP a server DHCP na stejné podsíti, zprávy DHCPDiscover, DHCPOffer, DHCPRequest a DHCPAck jsou posílány přes všesměrové vysílání na úrovni MAC a IP.

Aby klienti DHCP mohli komunikovat se serverem DHCP na vzdálené síti, musí připojující směrovač nebo směrovače podporovat předávání zpráv DHCP mezi klientem DHCP a serverem DHCP za použití služby BOOTP/DHCP Relay Agent.

11.5.1 Inicializace

Tento stav nastane při první inicializaci zásobníku protokolu TCP/IP na počítači klienta DHCP. Klient ještě nemá od serveru DHCP vyžádanou adresu IP. Tento stav také nastane, pokud je klientovi odepřena adresa IP, kterou požaduje, nebo pokud adresa IP, kterou původně měl, byla uvolněna. Stav inicializace je znázorněn na obrázku.



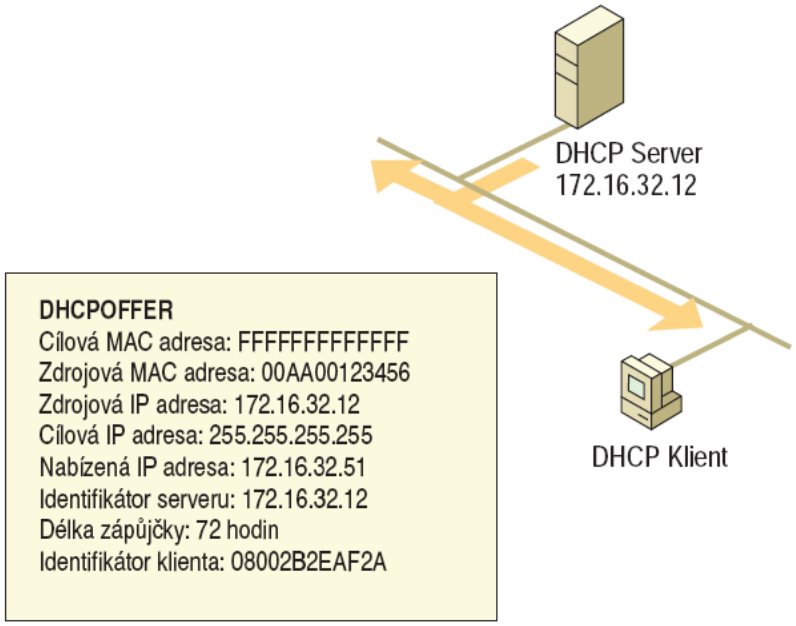
Stav inicializace

Když je klient DHCP v tomto stavu, jeho adresa IP je 0.0.0.0. Při získávání platné adresy klient prostřednictvím všesměrového vysílání pošle zprávu DHCPDiscover z portu UDP 68 na port UDP 67 se zdrojovou adresou 0.0.0.0 a cílovým umístěním 255.255.255.255 (klient dosud nezná adresu serverů DHCP). Zpráva DHCPDiscover obsahuje adresu MAC klienta DHCP a název počítače.

11.5.2 Výběr

Pak se klient přesune do stádia výběru, kdy vybírá odpověď serveru DHCP, DHCPOffer. Všechny servery DHCP, které obdržely zprávu DHCPDiscover a mohou klientovi DHCP nabídnout platné adresy IP, reagují zprávou DHCPOffer odesílanou z portu UDP 68 na port UDP 67. Zpráva DHCPOffer je poslána prostřednictvím všesměrového vysílání MAC a IP, protože klient DHCP ještě nemá platnou adresu IP, kterou lze použít jako cílové umístění.

Server DHCP rezervuje adresu IP, aby nebyla nabízena jinému klientovi DHCP:
Zpráva DHCPOffer obsahuje adresu IP a odpovídající masku podsítě, identifikátor serveru DHCP (adresu IP nabízejícího serveru DHCP) a dobu trvání zápůjčky. Stav výběru je znázorněn na obrázku.

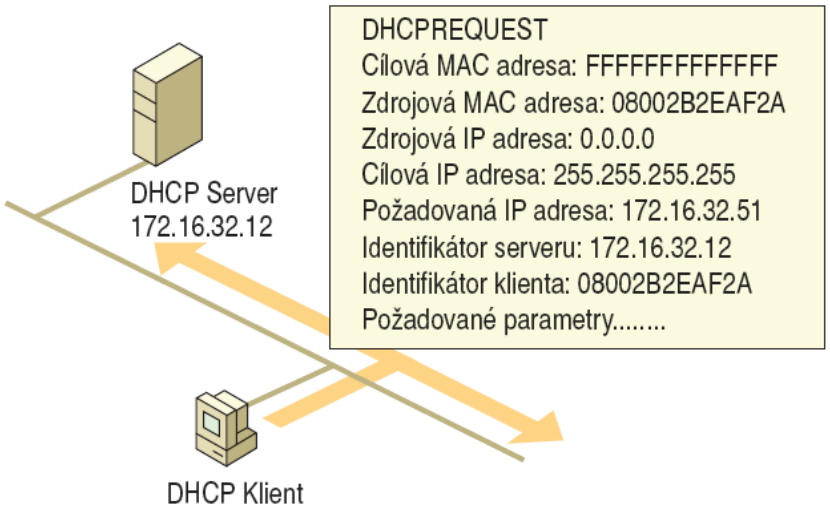


Stav výběru

Klient DHCP čeká na zprávu DHCPOffer. Neobdrží-li zprávu DHCPOffer od serveru DHCP při spouštění systému, pokusí se o to znovu čtyřikrát (v intervalech 2, 4, 8 a 16 sekund plus náhodný čas mezi 0 a 1000 milisekund). Jestliže klient DHCP neobdrží zprávu DHCPOffer po čtyřech pokusech, počká 5 minut a pak se pokouší znovu, vždy v 5minutových intervalech.

11.5.3 Požadavek

Poté, co klient DHCP obdrží ze serveru zprávu DHCPOffer, klient se přesune do stavu požadavku. Klient DHCP zná adresu IP, kterou chce zapůjčit, takže pošle prostřednictvím všesměrového vysílání zprávu DHCPRequest na všechny servery DHCP. Klient musí použít všesměrové vysílání, protože stále nemá přiřazenou adresu IP. Stav požadavku je znázorněn na obrázku.

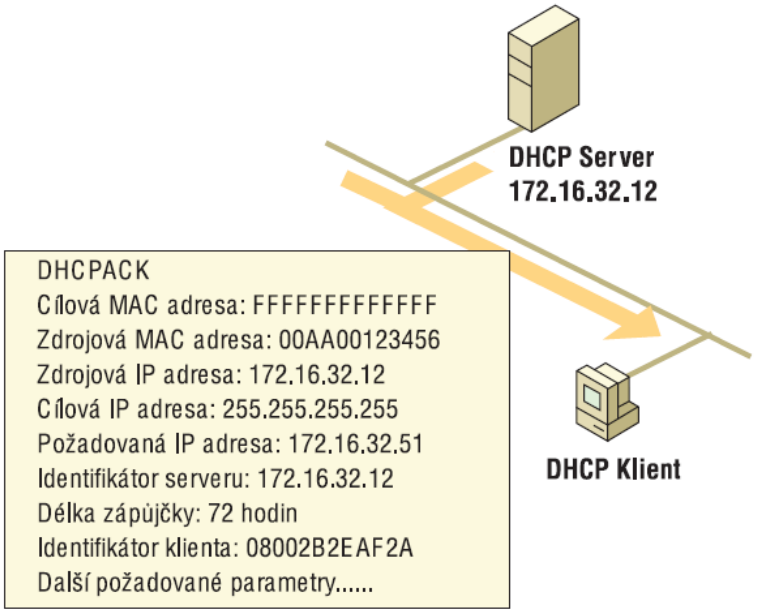


Stav požadavku

Jestliže byla adresa IP klienta známa (tzn. že počítač byl restartován a snaží se zapůjčit si původní adresu), všesměrové vysílání sledují všechny servery DHCP. Server DHCP, který může zapůjčit požadovanou adresu IP, odpoví buď úspěšným potvrzením (DHCPAck) nebo neúspěšným potvrzením (DHCPNak). Zpráva DHCPNak je použita v případě, že požadovaná adresa IP není dostupná nebo klient se fyzicky přesunul na jinou podsíť, která požaduje jinou adresu IP. Po obdržení zprávy DHCPNak se klient vrací do stavu inicializace a začíná proces zápůjčky znovu.

11.5.4 Vazba

Server DHCP reaguje na zprávu DHCPRequest prostřednictvím zprávy DHCPAck. Tato zpráva obsahuje platnou zápůjčku na vyjednanou adresu IP a jakékoli možnosti DHCP nakonfigurované správcem serveru DHCP. Stav vazby je znázorněn na obrázku.



Stav vazby

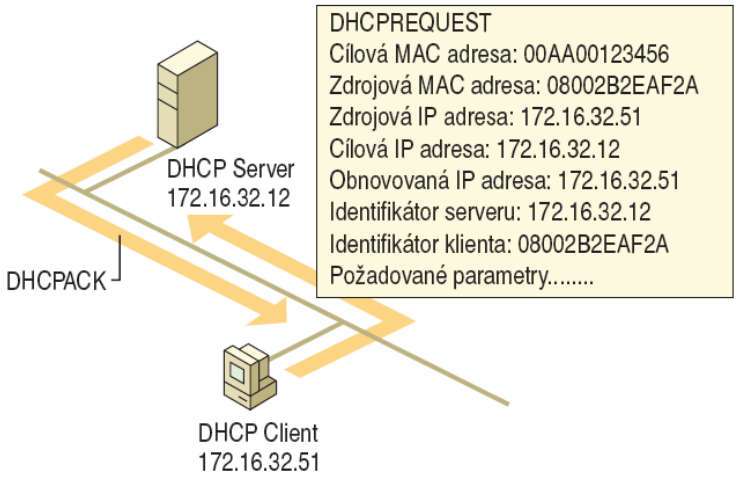
Server DHCP pošle zprávu DHCPAck prostřednictvím všesměrového vysílání IP. Poté, co klient DHCP obdrží zprávu DHCPAck, dokončí inicializaci zásobníku protokolu TCP/IP. Je nyní považován za vázaného klienta DHCP, který může používat protokol TCP/IP ke komunikaci na síti.

Adresa IP zůstává přiřazena klientovi až do ručního uvolnění adresy klientem nebo do vypršení doby zápůjčky a odmítnutí zápůjčky serverem DHCP.

11.5.5 Obnovení

Informace o adresování IP jsou zapůjčeny klientovi a klient je zodpovědný za obnovování zápůjčky. Dle výchozího nastavení se klient DHCP snaží obnovit svou zápůjčku po uplynutí 50 procent doby trvání zápůjčky. Kvůli obnovení zápůjčky posílá klient DHCP zprávu DHCPRequest serveru DHCP, od kterého původně zápůjčku obdržel.

Server DHCP automaticky zápůjčku obnoví prostřednictvím zprávy DHCPAck. Tato zpráva DHCPAck obsahuje novou zápůjčku a parametry možností DHCP. To zajišťuje, že klient DHCP může aktualizovat svá nastavení protokolu TCP/IP v případě, že správce sítě změnil některá nastavení serveru DHCP. Stav obnovení je znázorněn na obrázku.

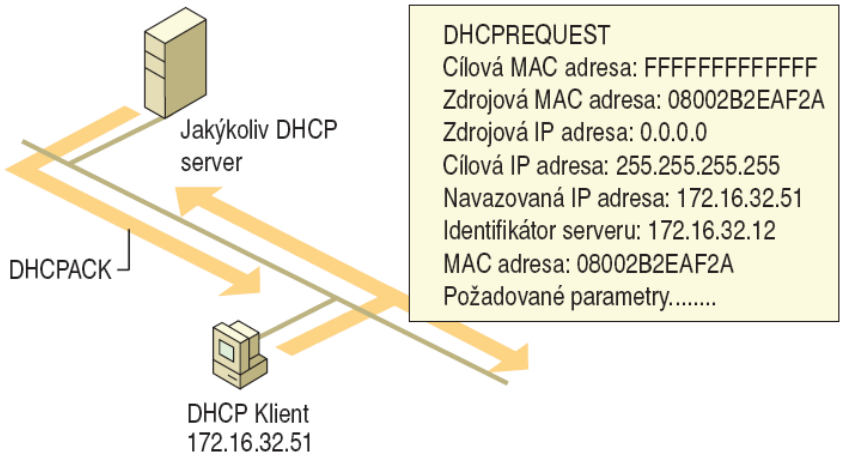


Stav obnovení

Jakmile klient DHCP obnoví zápůjčku, navrátí se do stavu vazby. Zprávy o obnovení (DHCPRequest a DHCPAck) jsou posílány jednosměrným provozem na úrovni IP a MAC.

11.5.6 Obnovení vazeb

Jestliže klient DHCP není schopen komunikovat se serverem DHCP, od kterého získal svou zápůjčku, a vypršelo již 87,5 procenta doby trvání zápůjčky, bude se snažit kontaktovat jakýkoli dostupný server DHCP pomocí zpráv DHCPRequest odesílaných prostřednictvím všesměrového vysílání. Jakýkoli server DHCP může reagovat zprávou DHCPAck a obnovit zápůjčku, případně zprávou DHCPNak, kterou donutí klienta DHCP k inicializaci a novému začátku procesu zápůjčky. Stav obnovení vazeb je znázorněn na obrázku.



Stav obnovení vazeb

Jestliže doba zápůjčky vyprší, nebo klient obdrží zprávu DHCPNak, musí klient DHCP okamžitě přestat užívat svou aktuální adresu IP. Jakmile k tomuto dojde, je komunikace přes protokol TCP/IP přerušena až doby, kdy klient získá novou adresu IP.

12. Síťové Prvky

Aktivní síťové prvky:

- **síťový adaptér** (NIC - Network Interface Card) - slouží k připojení zařízení do sítě - často integrováno na základní desce počítače nebo se připojuje pře standardní sloty (PCI, ISA, PC card,…),
- **HUB** (čti „hab“ - rozbočovač) - prosté propojení zařízení,
- **bridge** (čti „bridž“ - most) - odděluje provoz v lokálních sítích,
- **switch** (čti „svič“ - přepínač) - umožňuje rozdělení LAN do podsítí, vykonává také funkci bridge,
- **router** (čti „rauter“ - směrovač) - umožňuje směrovýní datagramů v rozlehlých sítích,
- **repeater** (čti „ripítr“ - opakovač) - zesilovač signálu,
- **transceiver** (čti „transívr“ - převodník) - převádí signál z jednoho druhu média na jiný (FO/TP, AUI/FO,…),
- **gateway** (čti „gejtvej“ - brána) - propojuje sítě.

Pasívní síťové prvky:

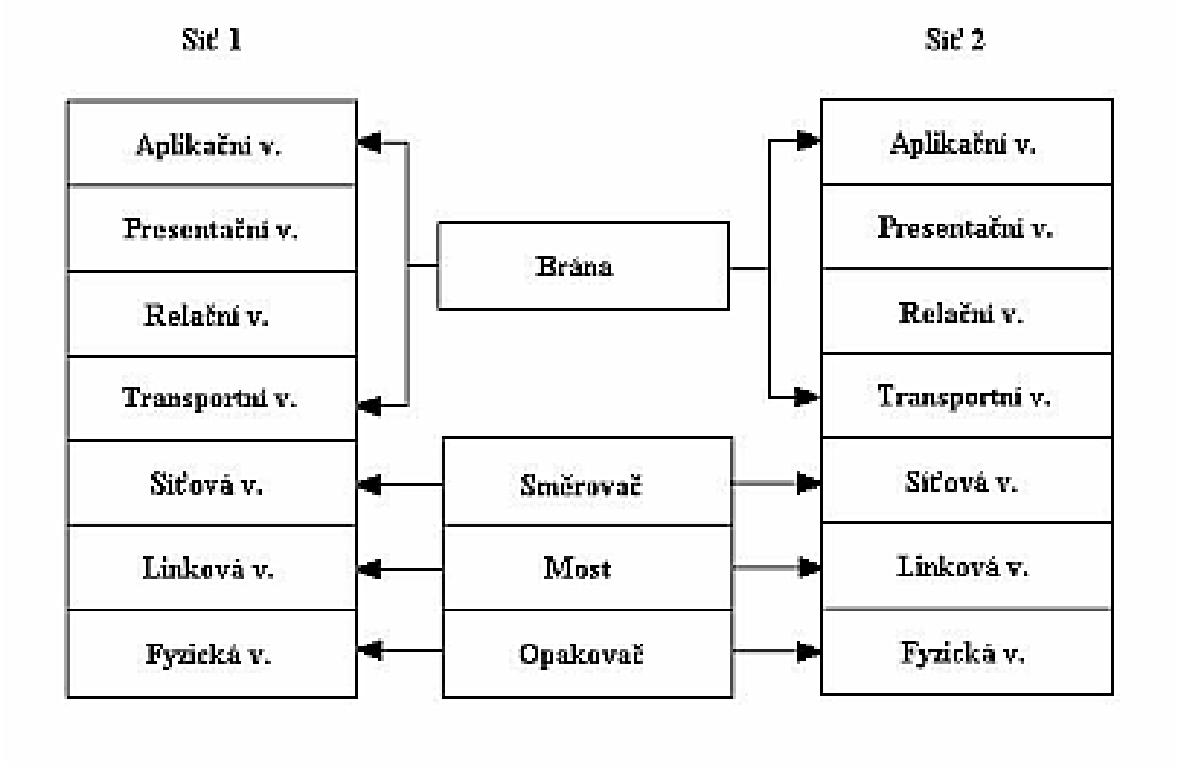
- **fyzické propojení počítačů** (kabeláž - metalická, optická, bezdrátové - infračervené, mikrovlnné, GSM, laser),
- **počítačové zásuvky**,
- **patch panely** (propojovací panely, ve kterých končí přípojky z počítačových zásuvek),
- **racky** (rozvodné skříně, v nichž jsou umístěny patch panely a některé aktivní prvky sítě),
- **propojovací kabely** (metalické, optické),

Základní rozdělení aktivních prvků:

- **Hardwarové síťové prvky**. Jsou specializovaná jednoúčelová zařízení, které se zpravidla osahují do Racků (speciální skříně).
- **Softwarové síťové prvky**. Odvedou stejnou práci jako hardwarové. Je to v podstatě normální počítač, na kterém běží program, který provádí určitou činnost související s provozem sítě.

Hlavní rozdíly souvisí s vrstvovým modelem, ze kterého vychází dnešní sítě - ať již se pohybujeme v rámci (spíše akademického) modelu ISO/OSI či v praxi používaného modelu TCP/IP, směrovače fungují na úrovni vrstvy síťové (třetí vrstvy počítáno odspodu), zatímco přepínače na úrovni bezprostředně nižší vrstvy linkové (resp. vrstvy síťového rozhraní, v terminologii TCP/IP)

Vztah aktivních síťových prvků k modelu OSI.



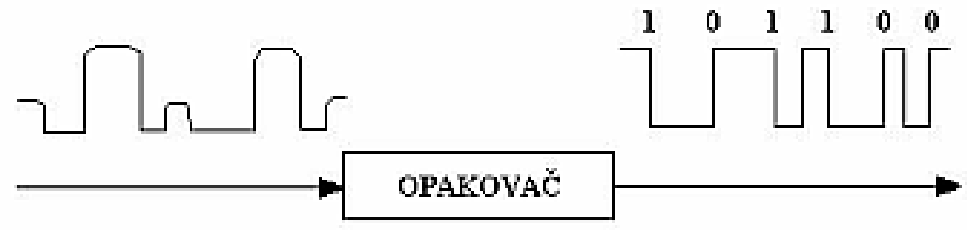
12.1 Typy aktivní prvků

12.1.1 Opakovače (repeatery)

Opakovač není ve své podstatě nic jiného, než obousměrný číslicový zesilovač. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, jíž jsme schopni lokální síti obsáhnout. Nejedná se tedy v pravém smyslu slova o propojení dvou různých lokálních sítí, ale o tvorbu jedné větší lokální sítě z menších částí.

Další možnou funkcí opakovače je propojení dvou částí lokální sítě, pracující s různými kabely. V případě Ethernetu tak můžeme například propojit segment pracující s tenkým koaxiálním kabelem (10BASE2) se segmentem pracujícím s tlustým koaxiálním kabelem (10BASE5).

Opakovač navíc regeneruje rámce putující po síti a je pro obě části sítě (oba segmenty), které spojuje, "průhledný".

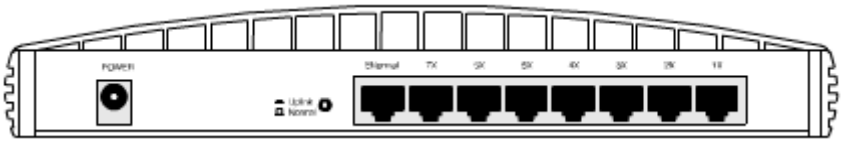


Připomeneme-li si funkce jednotlivých vrstev OSI Modelu, je zřejmé, že opakovače pracují v nejnižší, tj. fyzické vrstvě OSI Modelu. Kromě právě popsaných jednoduchých opakovačů existují také opakovače s více porty (tzv. multi-port repeaters), umožňující současné připojení více ethernetovských segmentů.

12.1.2 Rozbočovače (huby)

Hub je rozbočovací zařízení, které větví přenášený signál a tím umožňuje rozšiřování sítě o další pracovní stanice. Vše co mu přijde na jeho vstupy, ihned odesílá na všechny výstupy.

Je určen pro vytváření sítí s topologií hvězda. Na přední straně jsou zásuvky (porty), které jsou uvnitř vzájemně elektricky propojeny. Tyto zásuvky jsou u malých hubů většinou zezadu. Do těchto zásuvek se připojují kabely které vedou od počítačů.



Dále bývá na přední straně několik indikačních LED diod. Tyto LEDky nám dávají základní informace o tom zda počítač připojený k hubu je aktivní a v jaké rychlosti komunikuje se serverem (10/100 Mbps). Některé huby mají také indikátor zatížení v procentech. Pokud se zatížení neustále pohybuje přes 50% měli bychom přemýšlet o rozdělení sítě na více oddělených segmentů.

Huby jsou už nyní výhradně aktivní. To znamená, že přenášený signál je také zesílen a hrany signálu jsou upraveny do pravoúhlého stavu. Tím je možné dosáhnout větší délky kabelů.

Asi nejčastěji sledovaným údajem u hubů je kolik má portů. Počet portů se může pohybovat od 8 do 48. Osmi portové huby jsou určeny pro malé sítě, nebo jako doplnění když pár portů chybí. Většinou jsou to malé krabičky které se vejdou všude (na stůl, za stůl atd). 24 a více portové se už většinou prodávají ve standardní velikosti pro zamontování do 19 palcového racku.

Datová rychlost hubu je dalším parametrem. Dnes nejčastěji narazíme na dualspeed huby, které podporují rychlost 100/1000 Mbps. Lze se ale také setkat se staršími 10 Mbps huby.

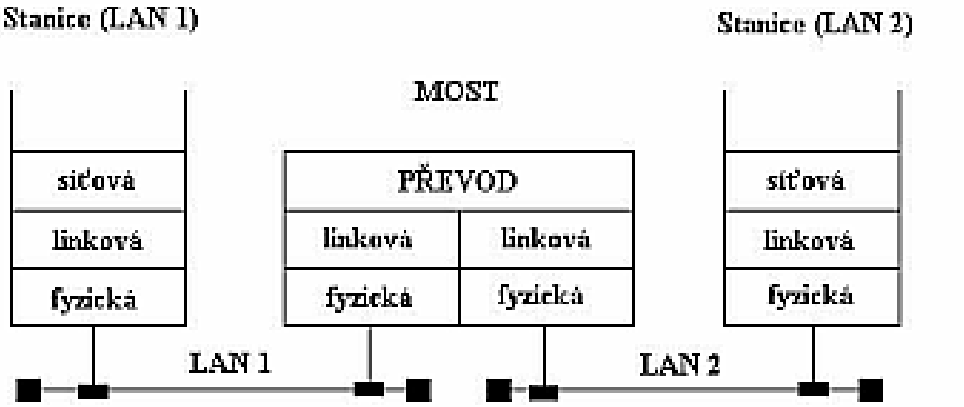
12.1.3 Mosty (bridge)

Mosty pracují na rozdíl od opakovačů na zcela jiném principu a jsou používány pro spojení dvou různých lokálních sítí, lišících se ve dvou nejnižších vrstvách OSI Modelu, tj. ve fyzické a linkové vrstvě. V případě lokálních sítí půjde o odlišnost až po tzv. MAC podvrstvu linkové

vrstvy. Pro potřeby standardizace lokálních počítačových sítí je výhodné rozdělit linkovou vrstvu na dvě další podvrstvy:

- na vrstvu řízení přístupu k síťovému médiu MAC - Media Acces Control,
- na vrstvu řízení logického spojení LLC - Logical Link Control).

Most sám o sobě je zařízení, které je součástí obou propojovaných sítí, z nichž obsahuje ty části (ty vrstvy OSI Modelu), kterými se tyto sítě liší. Data jsou z každé z propojených sítí v mostu převedena až do té vrstvy, kde se obě sítě neliší, a tam je proveden přenos dat do druhé se sítí. V tomto smyslu se dá tudíž říci, že mosty operují nad linkovou vrstvou OSI Modelu (to ale neznamená, že operují v síťové vrstvě, znamená to pouze, že využívají informace z linkové vrstvy).



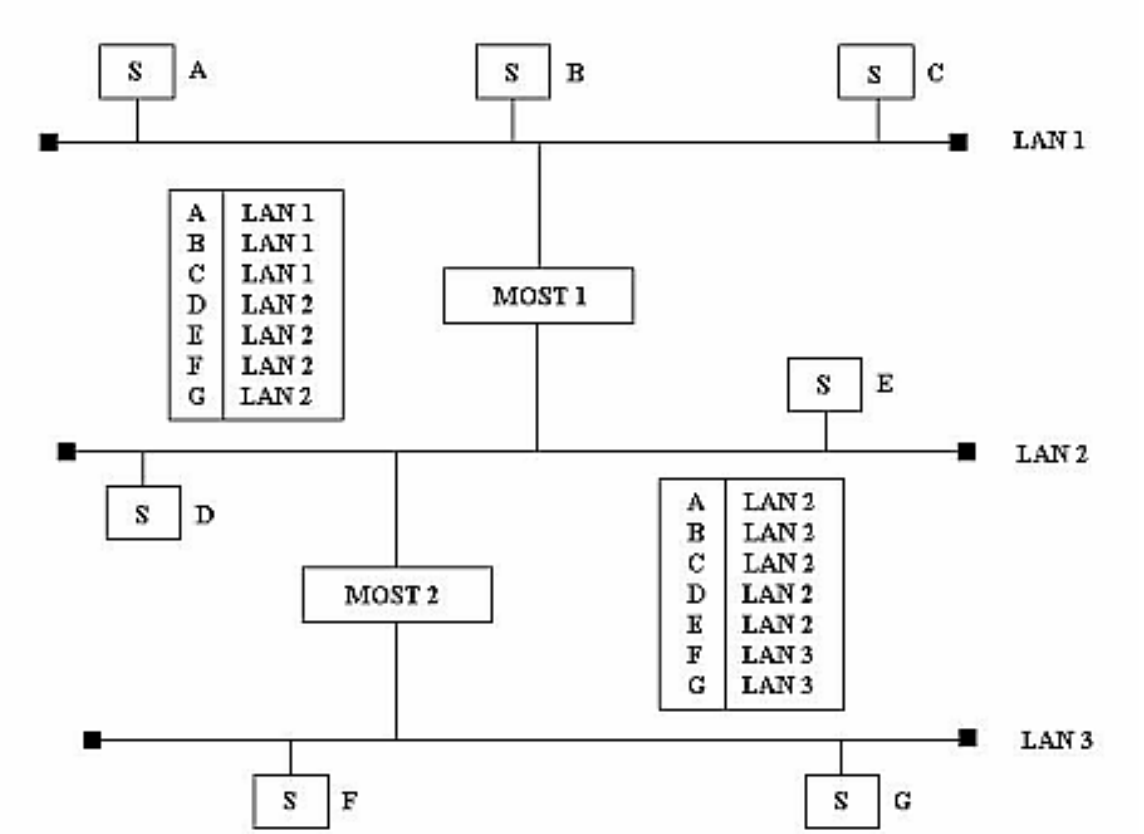
Mosty nejsou, na rozdíl od opakovačů, pro spojované sítě průhledné v tom smyslu, že přes mosty nepřejdou všechna data (rámce), která některá ze spojovaných sítí vyprodukuje. Projdou pouze ta data, která jsou určena stanicím nacházejícím se na "druhé straně mostu". To má jeden velice podstatný důsledek. Vede to totiž k celkovému snížení provozu na systému pospojovaných lokálních sítí. Lokální data zůstanou lokální a "nepřekáží" v dalších částech sítě.

V případě, že bychom na místě mostů použili opakovače, měli bychom celý systém doslova přeplněný daty, protože i cestě lokální data, jejichž vysílající i cílová stanice leží na stejné "podsíti" (v případě Ethernetu na stejném segmentu), by díky průhlednosti opakovačů bloudila po celém systému.

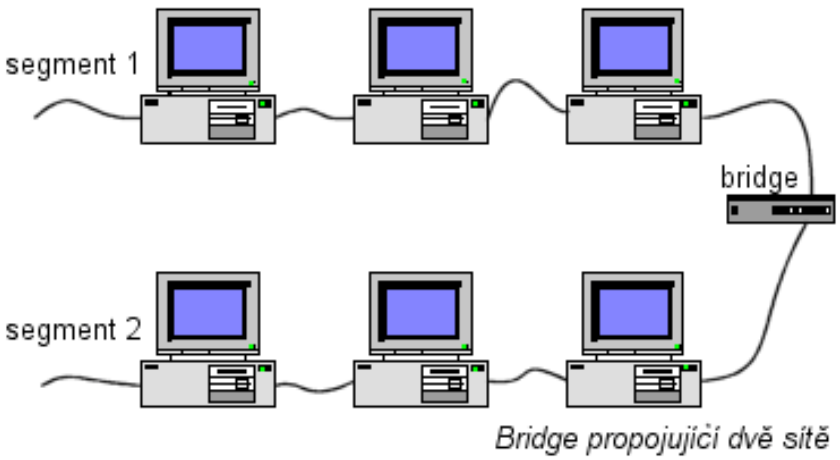
Mostem může být například normální osobní počítač, stejný jako v případě běžných síťových pracovních stanic, vybavený ale v tomto případě dvěma síťovými adaptéry (pro každou připojenou lokální síť jedna) a příslušném programovým vybavením. Most bude sledovat provoz na každé k němu připojené síti, ale přenášet bude pouze ty rámce, které rozpozná (podle cílové adresy) jako rámce určené druhé síti, než je síť, ze které přišly.

Použití mostu vede ve svých důsledcích také ke zvýšení výkonnosti (celkové kapacity) a spolehlivosti systému. Oddělením provozu v jednotlivých částech sítě totiž snižuje nebezpečí "zahlcení" celého systému. To je zvlášť důležité zejména u sítí Ethernet, které jsou díky použité přístupové metodě (CSMA/CD) na přetížení sítě zvláště citlivé. Pokud jde o zvýšení spolehlivosti, zde působí to, že mosty jsou díky své funkci schopny oddělit od zbytku sítě ty

její části, na nichž došlo k poruše. Mosty mohou sloužit také pro spojení lokálních sítí používajících odlišné typy síťových kabelů.



Most někdy zvaný brouter rozděluje síť na dvě kolizní domény. Umožňuje stanicím v kterékoliv síti přistupovat na zdroje v druhé síti. Pomocí mostů je možné prodlužovat délku, počet uzlů v síti a redukovat úzké profily vzniklé z přílišného počtu připojených počítačů.



Bridge propojující dvě sítě

12.1.4 Směrovače (routery)

Směrovače pracují na podobných principech jako mosty, pouze s tím rozdílem, že využívají informace ze třetí, tj. ze síťové vrstvy OSI Modelu, což je vrstva, která se stará o nalezení optimální cesty k cílové stanici.

Směrovače můžeme tudíž chápat jako mosty doplněné o možnost volby směru. Síťová vrstva pracuje kromě adres vlastních síťových stanic také se symbolickými adresami jednotlivých lokálních sítí jako takových. Jak pracovní stanice, tak směrovače mají nyní vytvořeny směrovací tabulky, v nichž jsou každé síti přiřazeny směrovače, které mohou zprostředkovat spojení.

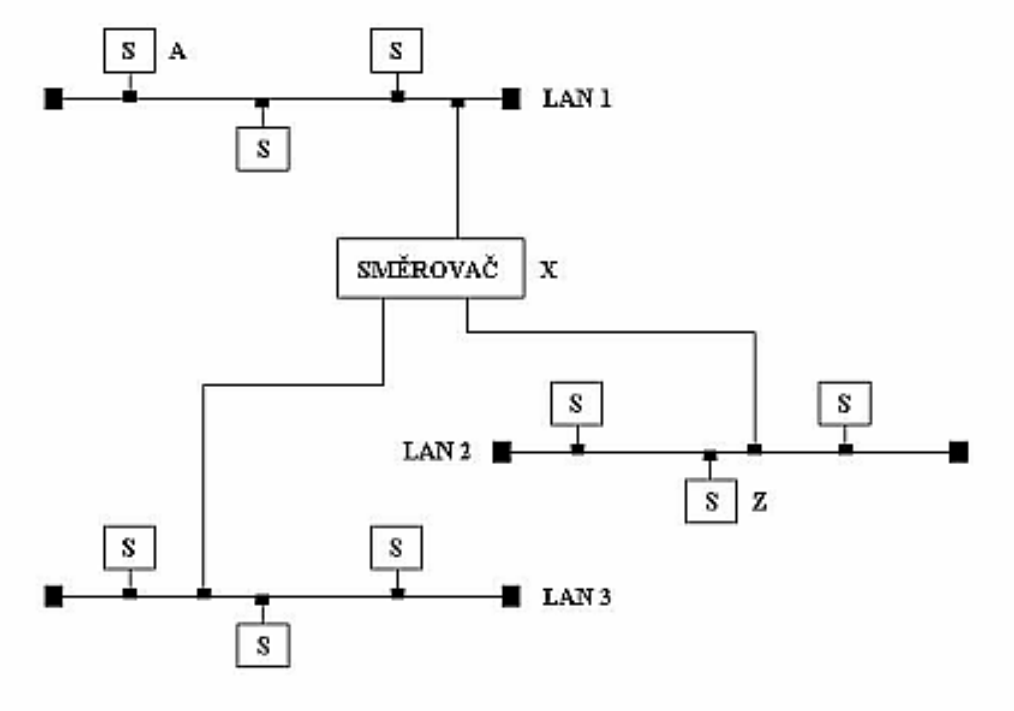
Adresu skutečné cílové stanice umístí do hlavičky paketu síťové vrstvy. Směrovač, který zprávu přijme, oddělí hlavičku linkové vrstvy a v hlavičce síťové vrstvy najde skutečnou cílovou adresu. Pak opět použije svou směrovací tabulku a zjistí adresu dalšího směrovače a tuto adresu opět předá linkové vrstvě pro vytvoření dalšího rámce. Obsah paketu síťové vrstvy zůstane nezměněn.

V případě, že cílová stanice i směrovač jsou součástí stejné lokální sítě, předá směrovač linkové vrstvě místo adresy dalšího směrovač přímo adresu cílové stanice. Tak například, chce-li stanice "A" poslat nějaká data stanici "Z", vyšle rámec:

Kde symbol "X" přestavuje adresu směrovače v síti číslo 1 a symbol "Z" adresu cílové stanice. Symbol na prvním místě představuje "aktuální" adresu (tj. adresu MAC podvrstvy) v dané síti, kdežto symbol na druhém místě představuje konečnou cílovou adresu. Směrovač tento rámec přijme, zpracuje (až do úrovně síťové vrstvy) a vygeneruje a vyšle na síť číslo 2 nový rámec, který bude vypadat takto:

Jistou výhodou směrovače proti mostu je to, že nemusí zpracovávat všechny v síti si pohybující rámce. Zpracovává pouze ty, které jsou mu na úrovni linkové vrstvy (respektive MAC podvrstvy linkové vrstvy) přímo adresovány. Dochází tedy u směrovače k jeho menšímu zatížení. Naproti tomu vzhledem k tomu, že u směrovačů musí být každý paket zpracován komplexněji, bude zpoždění zprávy pří průchodu směrovačem větší než při průchodu mostem.

Směrovače mohou díky své funkci podporovat složitější síťové topologie, zahrnující celou řadu nadbytečných spojení, a mohou přitom brát v úvahu celou řadu dodatečných informací, týkajících se například cen přenosu rámce po jednotlivých cestách atp.



Je zřejmé, že směrovače budou použity místo mostů zejména tam, kde půjde o komplikovanější sítě, skládající se například z menších lokálních sítí vybudovaných na základě různých IEEE standardů.

V posledních letech se můžeme setkat při spojování sítí s nový pojmem brouter jedná se v podstatě o kombinaci mostu a směrovače. V případě neznámého protokolu se chovají jako mosty, v případě daného, předem určeného protokolu jako směrovače.

12.1.5 Přepínače (switche)

Ve výkladu pojmu přepínač (switch) je určitá nejednoznačnost.

Podle klasické definice pracují přepínače na linkové vrstvě, a to do značné míry podobným způsobem jako mosty. Při této definici je jediný rozdílem mezi mostem a přepínačem to, že most pracuje jako zařízení pro ukládání a odesílání rámců, zatímco přepínač nikoli.

Moderní definice přepínače je poněkud odlišná, a to zejména v souvislosti s Internetem. Dnešní přepínač již není pouze přepínačem v lokální síti LAN; provádí také přepínání v sítích WAN. Přepínač je nicméně i nadále zařízením, které pracuje především na linkové vrstvě, jeden stejný přepínač však provádí také určité omezené funkce na síťové vrstvě. Díky této širší množině funkcí můžeme dnešní přepínače přirovnávat spíše ke směrovači než k mostu.

Switch se rozhoduje pouze na základě linkových adres (tedy například na základě Ethernetových adres, jde-li o ethernetové rámce). Přitom vystačí jen se znalostí struktury linkových rámců (aby věděl, kde v nich najít adresy příjemce a odesilatele), a se znalostí svého bezprostředního okolí (svých bezprostředních sousedů). Tuto znalost získává v zásadě sám (samoučením), tím že monitoruje odkud mu přichází jaké rámce. Přepínače jsou tedy zařízeními typu plug&play, které stačí zapnout a fungují „samy“. Je pro ně charakteristické také to, že jsou optimalizovány na rychlost, té se typicky dosahuje "zadrátováním"

příslušných přepojovacích funkcí (neboli: jejich implementací přímo v hardwaru, dnes prostřednictvím integrovaných obvodů ASIC).

Inteligence přepínačů (switchů) je také přizpůsobena jejich rychlosti - řečeno velmi lapidárně a s určitou mírou nadsázky, přepínače nejsou stavěny na žádné velké přemýšlení (ale na rychlost).

12.1.6 Brány (gateways)

Brána (gateway) je obvykle kombinací softwaru a hardwaru, který propojuje dvě různé sítě pracující pod různými protokoly.

Brány pracují zpravidla na síťové vrstvě nebo ještě výše. Některé brány kromě vlastního přenosu dat z jedné sítě do jiné zabezpečují současně s přenosem také převod do jiného protokolu; takovýmto branám se říká aplikační brány. Příkladem může být e-mailová brána, která převádí elektronickou poštu z podoby definované jedním protokolem do jiného protokolu.

Někdy se pojem brána používá i v situacích, kdy se neprovádí žádný převod mezi protokoly, ale kdy se data pouze přenesou z jedné sítě do jiné. Takovouto bránu tvoří software a hardware, který propojuje dvě různé sítě. Jednou z možných charakteristik brány mohou být dvě různé adresy pro síťovou vrstvu, například více různých IP adres.

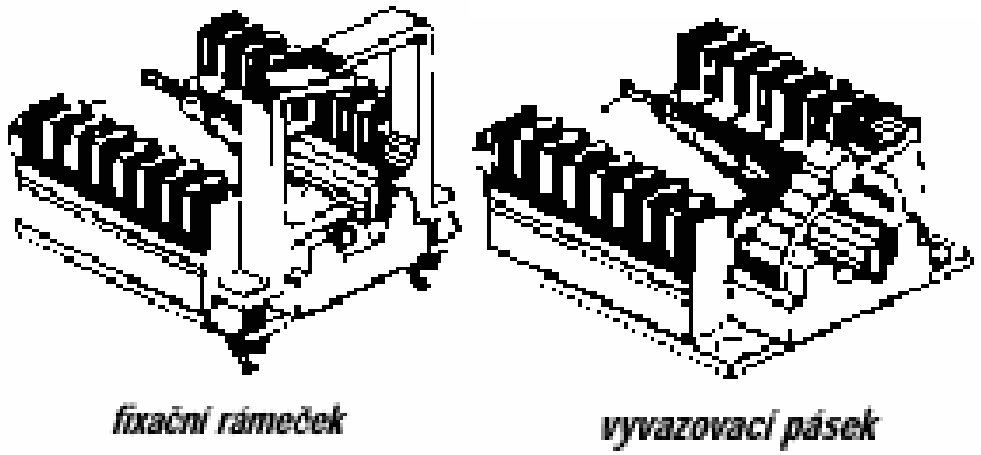
12.2 Typy pasivních prvků

12.2.1 Patch panely

Používají se k ukončení horizontální nebo páteřní kabeláže a k uspořádání rozhraní do rozličných síťových zařízení. Jsou vesměs umístěny v rozvaděči. Zajišťují jednoduchý servis, administraci a údržbu.

Patch panely jsou osazeny speciálně konstruovanými zásuvkovými bloky. Všechny patch panely mají standardně rozteč uchycování otvorů 19“ a jsou v CAT 5E. Pro lepší orientaci jsou vyráběny v různém barevném provedení.

Vodiče lze upevnit na svorkovnici pomocí vyvazovacího pásku. Vodiče se vyvazují pomocí fixačního rámečku. Každý blok má jeden fixační rámeček. Oba uchycovací systémy jsou obsaženy u každého modulu.



12.2.2 Racky

Racky mají standardizovanou šířku 19'', výška a hloubka je volitelná. Podle velikosti jsou racky samostatně stojící nebo montované na zeď. V definici rozměrů zařízení určených k instalaci do racku se používá jednotky 1U, která odpovídá velikosti 1,5'' – běžné výšky zařízení jsou 1U, 2U, 3U, 5U.

Připojení racku k napájení je většinou realizováno standardní síťovou zástrčkou. Uvnitř racku je zpravidla jeden napájecí panel s přepěťovou ochranou - většinou se umisťuje na zadní straně racku. V dolní části racku je umístěn zdroj nepřerušitelného napájení UPS. Napájí se z napájecího panelu v zadní části racku a výstup je vyveden do chráněného napájecího panelu v přední části racku.

Další zařízení se už potom zpravidla montují podle systému nejtěžší do nižších poloh, důvodem je stabilita racku. Všechny komponenty se připevňují do racku do připravených otvorů v palcové rozteči speciálními čtvercovými maticemi. V nejvyšších polohách bývají vyvedeny patch panely, pod nimi se většinou montují kabelové organizery, pro zpřehlednění propojování.

Dále pak následují aktivní prvky a telefonní ústředny, do nižších pater se pak montují servery. K racku existuje celá řada příslušenství, z nichž za zmínku stojí ventilační jednotky s termostatem a prachovým filtrem – napájí se z nechráněného panelu, osvětlení racku – rovněž se napájí z nechráněného panelu, a celý sortiment organizérů, polic a úchytů.

Technologie počítačových sítí

UKÁZKOVÝ ZKOUŠKOVÝ TEST

Prosím vyplňte (velkým tiskacím písmem)!!!	
Příjmení:	…….
Jméno:	…….
Ročník:	…….
Typ studia (P/K):	…….
Datum konání:	…….

Prosím nevyplňujte!!!	
Počet bodů:	…….
Klasifikace:	…….

Návod na vyplnění testu

Nejprve vyplňte titulní stránku testu, kde uveďte všechny požadované údaje. Během testu neopisujte, ani nijak nespolupracujte se svými sousedy a ostatními kolegy. Pokud toto porušíte, bude Vám test odebrán a budete klasifikováni jako nevyhovující!!! Test nejprve vyplňte „nanečisto“ (obyčejnou tužkou), budete totiž moci odpovědi opravovat pouze jednou!!!

Jednotlivé správné odpovědi (VŽDY JEN JEDNA JE SPRÁVNĚ) označujte křížkem např.:

Základní jednotkou pro přenos dat je na síťové vrstvě je?

a) Síťový rámec
~~b)~~ Síťový paket
c) Datagram

Pokud chcete změnit svou odpověď, tak špatnou odpověď zakroužkujte nebo napište že NEPLATÍ např.:

Základní jednotkou pro přenos dat je na síťové vrstvě je?

~~a)~~ Síťový rámec - NEPLATÍ
~~b)~~ Síťový paket
c) Datagram

Klasifikace testu:

Za každou správně zodpovězenou otázku získáte jeden bod (celkový počet bodů je 24).

0 – 12 bodů	F (opravný termín)
13 – 15 bodů	E
16 – 17 bodů	D
18 – 19 bodů	C
20 – 21 bodů	B
22 – 24 bodů	A

V současné době je v LAN nejpoužívanějším přenosovým médiem kroucený dvoupár označovaný jako?

a) AUI

b) UTP

c) BNC

Součásti koaxiálního kabelu není?

a) izolace

b) Konektor RJ-45

c) jádro

Mezi vrstvy síťového modelu TCP/IP patří?

a) Linková a fyzická

b) TCP/UDP

c) Transakční

Mezi služební protokoly IP protokolu patří?

a) ICMP

b) DHCP

c) DNS

Chceme-li použít telefonní vedení pro počítačovou komunikaci, pak se musí datové informace na telefonní vedení?

a) modulovat a na druhé straně demodulovat

b) na obou stranách pouze modulovat

c) na obou stranách pouze demodulovat

Strukturovanou kabeláží se rozumí komplexní řešení?

a) signalizačních rozvodů v budově

b) vysokonapěťových rozvodů v budově

c) nízkonapěťových rozvodů v budově

Jak se označuje 100 MHz varianta Ethernetu?

a) Ethernet I

b) Ethernet II

c) Ethernet III

Mezi systémy LAN na linkové vrstvě patří?

a) TCP/UDP

b) IP adresace

c) Ethernet

IP-adresa má v případě IP-protokolu verze 4 velikost?

a) Čtyřbajtová

b) Osmibajtová

c) Šestnáctibajtová

Protokol IGMP je služební protokol, který je součástí?

a) IP protokolu

b) TCP protokolu

c) UDP protokolu

IP adresa počítače zapsaná v desítkové notaci má tvar?

a) 10101010.01010101.11111111.11111000

b) 170.85.255.248

c) AA.55.FF.F8

Síťová maska se používá pro určení?

a) Adresy sítě

b) Jména sítě

c) MAC adresy počítače

Který příkaz vypisuje obsah směrovací tabulky?

a) Netstat

b) Ping

c) Delete

Filtrační proces při filtraci IP-datagramů se rozhoduje na základě informací v?

a) Záznamu v DNS

b) Hesla

c) Aplikačního protokolu

Kolik portů existuje pro službu UDP?

a) 16 640

b) 32 128

c) 65 535

Ukončení spojení se provádí pomocí TCP segmentu s příznakem?

a) SYN

b) FIN

c) ACK

Klasifikace aplikační vrstvy se podle způsobu práce dělí na?

a) Hybridní, Nehybridní

b) Interaktivní, Procesně orientované

c) Synchronní, Asynchronní

Který port standardně používá služba FTP serveru?

a) 21

b) 53

c) 80

Pro Českou republiku je vyhrazena doména ve tvaru?

a) eu

b) cz

c) czech

Resolver je klient, který se dotazuje?

a) Print serveru

b) Disc serveru

c) Name serveru

Server DHCP uchovává informace o konfiguraci v databázi, která zahrnuje?

a) Parametry MAC adres

b) Platné adresy IP udržované ve fondu adres pro přiřazení klientům

c) Záznamy DNS

Servery DHCP udržují informace o konfiguraci protokolu?

a) TCP/IP

b) ARP

c) ICMP

Mezi pasivní síťové prvky patří?

a) Hardwarový firewall

b) Počítačové zásuvky (např.: RJ – 45)

c) Switch

Mezi aktivní síťové prvky patří?

a) Patch panel

b) Rack

c) Router