Výpočetní technika a informatika VTI

Střední Odborná Škola Hořovice

Základy informatiky

Bc.Papavasiliu Vassilis

Počitačové sítě - network

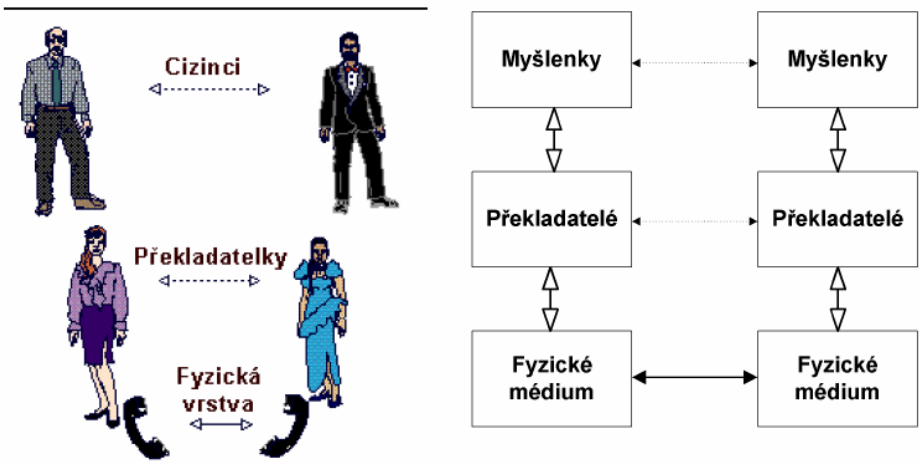
Obsah:

Architekrura sítí.

Síťové protokoly

Podobně jako diplomaté při svých jednáních používají diplomatický protokol, tak i počítače v počítačových sítích používají pro vzájemnou komunikaci síťové protokoly. Síťových protokolů existuje celá řada. V Internetu se používají síťové protokoly TCP/IP.
Síťový protokol je norma napsaná na papíře (resp. textovým editorem na počítači). V Internetu se používají normy nazývané Request For Comments – zkratkou RFC, které se číslují průběžně od jedničky.
V současné době jich jsou necelé tři tisíce. Mnohé však postupem času zastaraly, takže z první tisícovky jich je aktuálních jen několik.
Mezinárodní normalizační úřad (ISO) normalizoval soustavu protokolů označovaných jako ISO OSI.
Další slovutnou organizací vydávající normy v oblasti komunikací je ITU se sídlem v Ženevě (dříve CCITT – nejstarší celosvětová organizace vůbec, založena 1865). Dále se setkáme s normami vydanými sdružením elektrotechnických inženýrů IEEE. Běžný uživatel se však může dostat pouze k normám RFC, protože ostatní organizace neposkytují své normy zdarma. *
Nejprve si musíme objasnit, proč je problematika komunikace mezi počítači vždy rozdělena do více protokolů. OdpověT je velice jednoduchá, celá problematika je velice komplikovaná a pokrývá několik profesí. Většina publikací o síťových protokolech uvádí přirovnání ke komunikaci dvou cizinců (či filozofů, šamanů apod.), kteří umí každý jen svůj jazyk. Aby si vyměnili své myšlenky, musí si každý obstarat překladatelku do společného jazyka – např. do češtiny. Viz obr. 1.1.

Obr. 1.1
Třívrstvá komunikační architektura

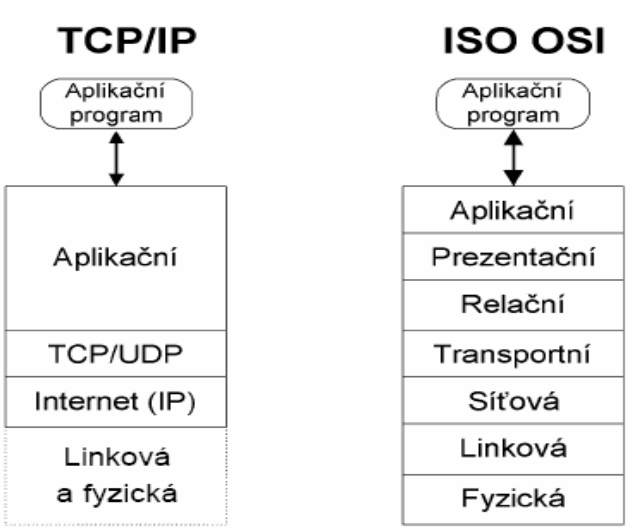


Vzájemně si oba cizinci předávají své myšlenky, tj. komunikují mezi sebou. Jenže mezi sebou komunikují jen pomyslně (virtuálně). Ve skutečnosti oba své informace předávají překladatelkám, a ty pak pomocí svých hlasivek rozvlní vzduch, aby přenesly informace. Nebo jsou obě strany vzdáleny a překladatelé komunikují pomocí telefonu, pak se informace fyzicky přenášejí po telefonních linkách.
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, jak je znázorněno na obr. 1.2.

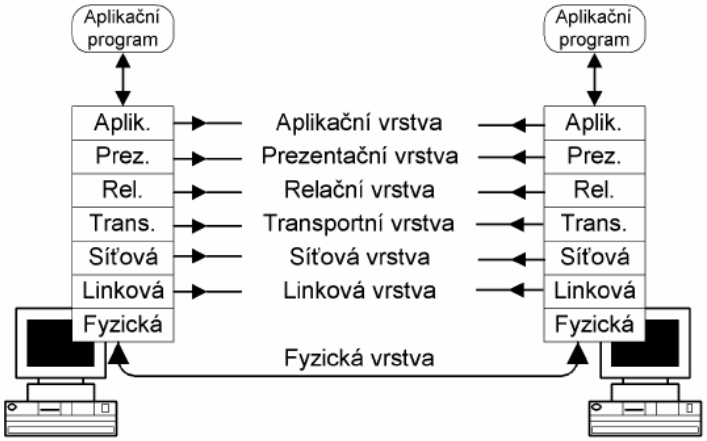
Obr. 1.2
Porovnání síťových modelů TCP/IP a ISO OSI



ISO OSI

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.

Obr. 1.3
Sedmivrstvá architektura ISO OSI

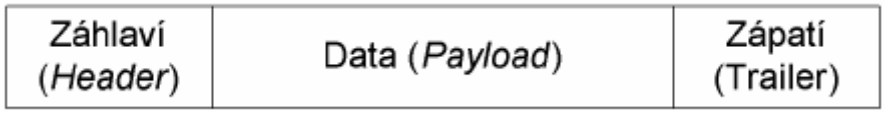


Fyzická vrstva

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.

Linková vrstva

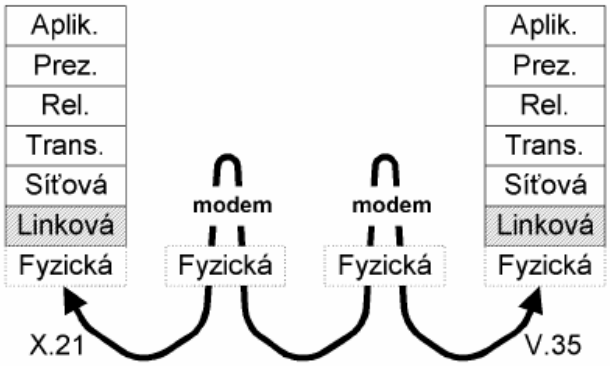
Linková vrstva zajišGuje v případě sériových linek výměnu dat mezi sousedními počítači a v případě lokálních sítí výměnu dat v rámci lokální sítě.



Základní jednotkou pro přenos dat je na linkové vrstvě datový rámec (viz obr. 1.4). Datový rámec se skládá ze záhlaví (*Header*), přenášených dat (*Payload*) a zápatí (*Trailer*).

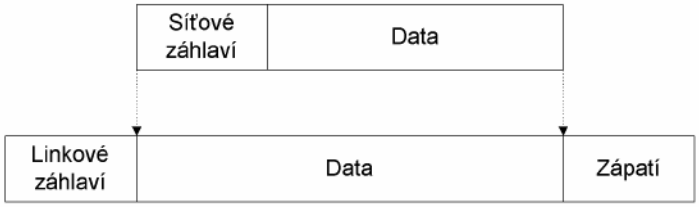
Datový rámec nese v záhlaví linkovou adresu příjemce, linkovou adresu odesílatele a další řídící informace.
V zápatí nese mj. obvykle kontrolní součet z přenášených dat. Pomocí něho lze zjistit, zdali nedošlo při přenosu k porušení dat. V přenášených datech je pak zpravidla nesen paket síťové vrstvy.
Z obr. 1.5 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*), který konvertuje linkové rámce jednoho linkového protokolu na rámce jiného linkového protokolu (např. Ethernet na FDDI), což má pochopitelně za následek i použití jiných protokolů na fyzické vrstvě.

Obr. 1.5 Komunikace na linkové vrstvě

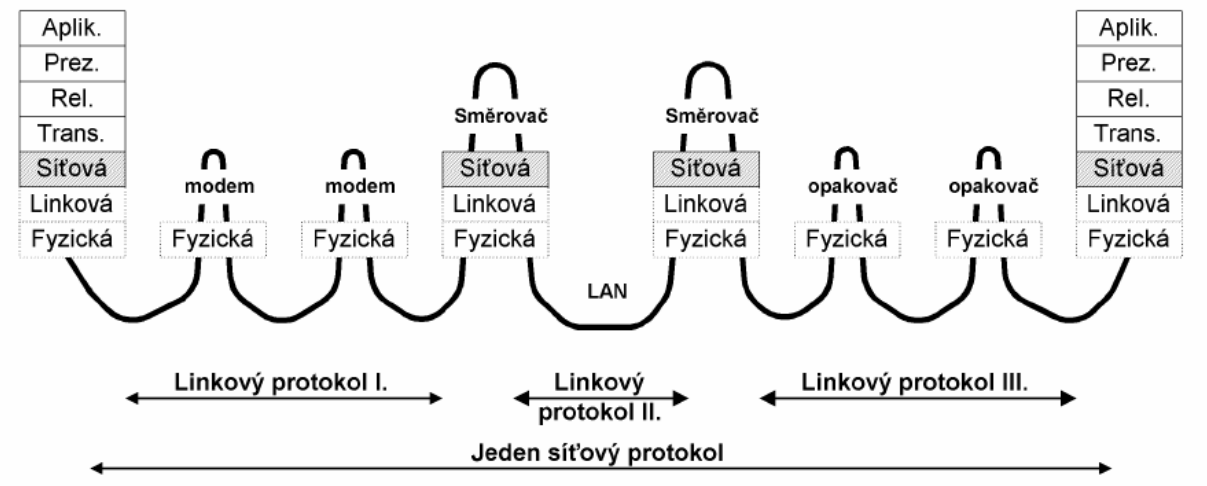


Síťová vrstva
Síťová vrstva zabezpečuje přenos dat mezi vzdálenými počítači WAN. Základní jednotkou řenosu je síťový paket, který se balí do datového rámce. Síťový paket se také skládá ze záhlaví a datového pole.Se zápatím se u síťových protokolů setkáváme jen zřídka.

Obr. 1.6 Síťový paket a jeho vkládání (encapsulation) do linkového rámce



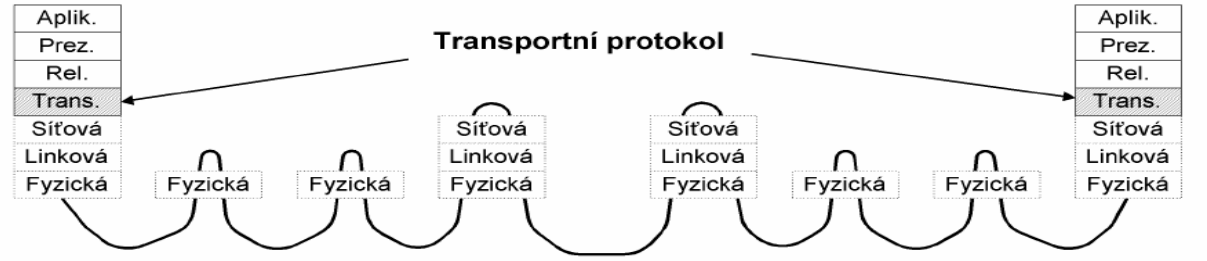
Z obr. 1.6 je patrné, že síťové záhlaví společně s daty síťového paketu tvoří data linkového rámce.
V rozsáhlých sítích (WAN) mezi počítači leží zpravidla jeden nebo více směrovačů. Mezi sousedními směrovači je na linkové vrstvě vždy přímé spojení. Směrovač vybalí síťový paket z datového rámce (jednoho linkového protokolu) a před odesláním do jiné linky jej opět zabalí do jiného datového rámce (obecně jiného linkového protokolu).



Síťovou vrstvu příliš nezajímá jaké jednotlivé linkové protokoly byly na cestě mezi oběma konci spojení použity. Na síťové vrstvě je jednoznačně v celé WAN adresováno síťové rozhraní. Síťovým rozhraním může být např. karta pro Ethernet.

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. Také předpokládá, že spojení mezi počítači je zajištěno, proto se bez zbytečných starostí může věnovat spojení mezi aplikacemi na vzdálených počítačích.



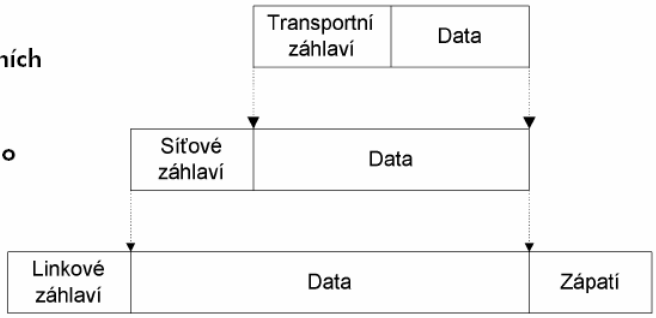
Obr. 1.8 Spojení na transportní vrstvě

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.

Aplikace jsou jednoznačně adresovány v rámci jednoho počítače.

Jednotkou přenosu je transportní paket, který se opět skládá ze záhlaví a datové části. Transportní paket se přenáší v datové části síťového paketu.

Obr. 1.9
Vkládání transportních paketů do síťových paketů, které jsou následně vloženy do linkových rámců



Relační vrstva
Relační vrstva zabezpečuje výměnu dat mezi aplikacemi, tj. provádí tzv. checkpoint, synchronizaci transakcí (*commit*), korektní uzavírání souborů atd. Dobře představitelnou relací je např. sdílení síťového disku. Disk může být sdílen po určitou dobu, avšak pracuje se s ním jen zřídka. Vždy, když je např. třeba pracovat se souborem na síťovém disku, tak se naváže na dobu od otevření souboru až po jeho uzavření spojení na transportní vrstvě. Avšak relace na relační vrstvě existuje po celou dobu sdílení disku.
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.
1.1.6 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.
1.1.7 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.

Obr. 1.10 Některé protokoly z rodiny protokolů 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

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.

Internet Protokol

Internet Protokol (dále jen IP-protokol) prakticky odpovídá síťové vrstvě. IP-protokol přenáší tzv. Ipdatagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese adresu příjemce, což je úplná směrovací informace pro dopravu IP-datagramu k adresátovi. Takže Síť může přenášet každý Ipdatagram 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*.

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 zajišGují spojení mezi aplikacemi běžícími na vzdálených počítačích. Protokoly TCP a UDP mohou zajišGovat 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.

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). Obdobně protokol ASN.1 (včetně kódování BER, resp. DER) byl nejprve využíván protokolem SNMP, avšak je využíván např. i protokolem S/MIME.
Aplikačních protokolů je velké množství. Z praktického hlediska je lze rozdělit na:

- ✓ Uživatelské protokoly, které využívají uživatelské aplikace (např. pro vyhledávání informací v Internetu).

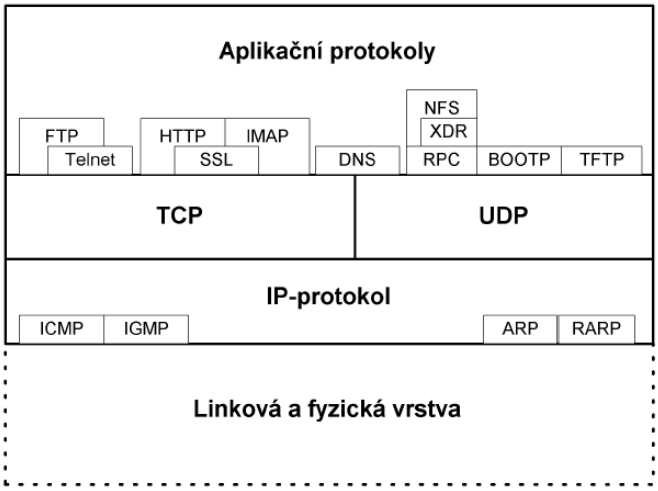
Příkladem takových protokolů jsou protokoly: HTTP, SMTP, Telnet, FTP, IMAP, POP3 atd.

- ✓ 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.

V této publikaci se blíže věnujeme pouze jedinému aplikačnímu protokolu – protokolu DNS. Protokol DNS je zvláštní v tom, že jej nelze snadno zařadit ani do jedné z uvedených kategorií. Běžný uživatel jej pravděpodobně zařadí mezi služební protokoly. Tento názor mu však vydrží pouze po dobu, kdy uživatelův počítač pracuje správně. Jakmile uživatel začne mít potíže s protokolem DNS, pak obratem zjistí, že jej velice nutně ke své práci potřebuje, že jej používá v téměř každém svém příkazu.

Obr. 1.11
Některé protokoly z rodiny protokolů TCP/IP

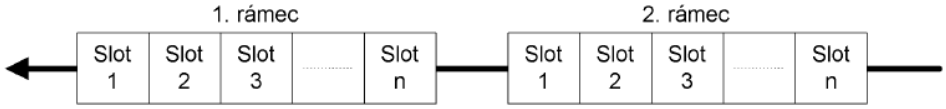


Způsoby přenosů informací

Síťových protokolů je velké množství, dokonce na jedné vrstvě máme často k dispozici několik protokolů.
Zejména u protokolů nižších vrstev rozlišujeme jaký typ přenosu protokol zabezpečuje a zdali zabezpečuje službu spojovanou nebo nespojovanou, zdali protokol používá virtuální okruhy atd.
Rozeznáváme přenos **synchronní, paketový a asynchronní**.

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.

Obr. 1.12
Rozdělení rámců na sloty u synchronního přenosu

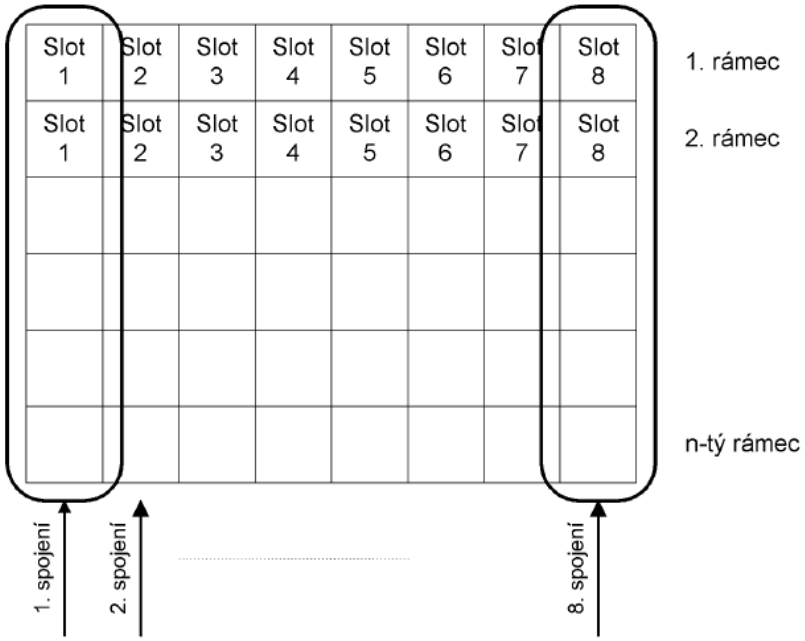


Synchronní přenos používá rámce konstantní délky, které jsou přenášeny sítí konstantní rychlostí.

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, viz obr. 1.12. Představíme-li si, že v každém rámci je např. slot číslo 1 vyhrazen pro naše spojení, pak jelikož rámce stejnoměrně plynou sítí za sebou, tak naše aplikace má garantovánu šíři pásma, která je dána tím, kolik slotů číslo jedna přenese Síť za vteřinu.
Podstatu pochopíme, když si několik rámců nakreslíme pod sebe do tzv. super-rámce, viz obr.

Sloty pod sebou patří témuž spojení.

Obr. 1.13
Super-rámec



Se synchronním přenosem se setkáváme např. u připojení podnikové telefonní ústředny k ústředně Telecomu.
Ta bývá připojena např. linkou E1, která obsahuje 32 slotů, každý o šířce pásma 64 kb/s. Slot lze využít pro telefonní hovor. Současně je tak teoreticky garantováno 32 hovorů (některé sloty se však používají jako služební).
Internet nepoužívá synchronní přenos, tj. negarantuje šíři přenášeného pásma. Kvalitní přenos zvuku či videa se v Internetu zpravidla dociluje předimenzováním přenosových linek.

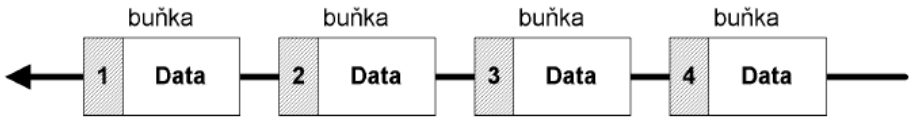
Paketový přenos
Paketový přenos je výhodný zejména pro přenos dat. Pakety nesou data obecně různé délky.

Obr. 1.14
Paketový přenos dat

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.

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

Obr. 1.15
Asynchronní přenos dat

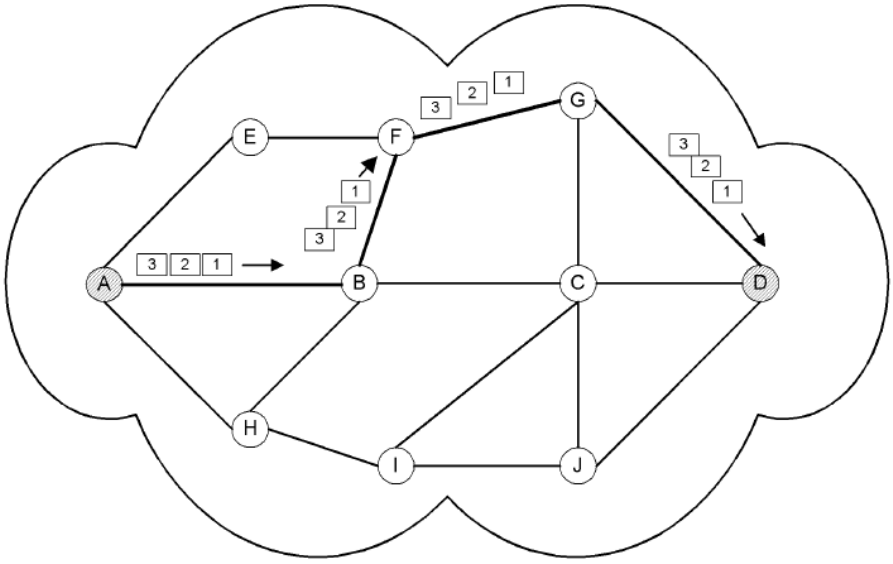


Podobně jako u paketového přenosu jsou u asynchronního přenosu data přenášena v malých paktech, které se však nazývají buňky. Obdobně jako u paketového přenosu se v jedné buňce přenáší data jedné aplikace (jednoho spojení). Avšak buňky mají stejnou délku, takže garantuje-li se, že každá x-tá buňka bude k dispozici konkrétní aplikaci (konkrétnímu spojení), pak se tím garantuje i šířka pásma. Navíc, pokud aplikace buňku neodešle – nevadí, může být odeslána buňka jiné aplikace.

Virtuální okruh

Některé Síťové protokoly vytváří v síti virtuální okruh (*Virtual Circuit*). Virtuální okruh je vedený sítí a všechny pakety spojení pak prochází tímto okruhem. V případě, že se okruh někde přeruší, tak se spojení přeruší, vytvoří se nový okruh a poté se opět mohou přenášet data.

Obr. 1.16
Virtuální okruh



Na obr. 1.16 je vytvořen virtuální okruh mezi uzly A a D přes uzly B, F a G. Všechny pakety musí procházet tímto okruhem.

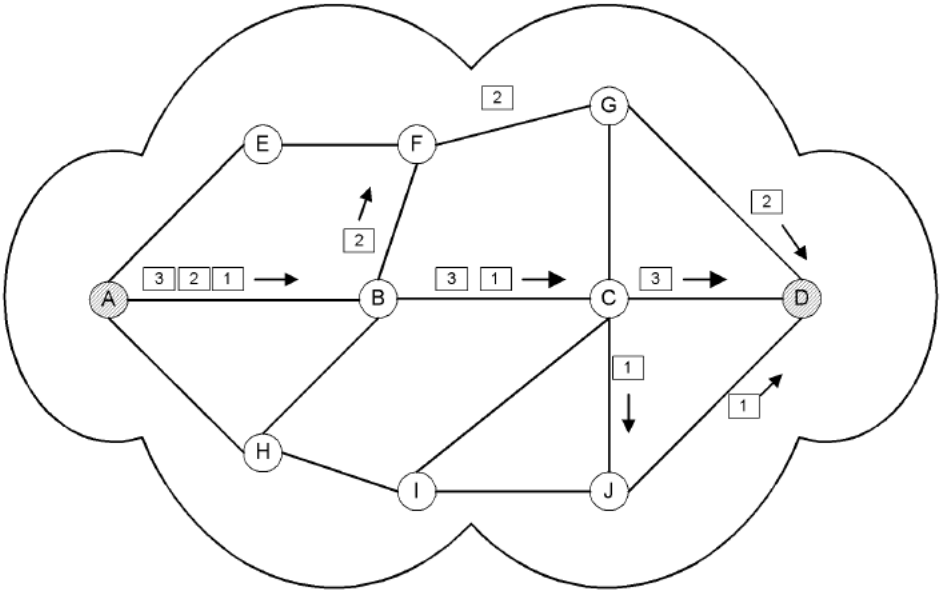
Na virtuálním okruhu je možné buT přenášet datagramy, kdy okruh negarantuje doručení datagramu příjemci (tj. v případě zahlcení sítě může datagram i zahodit), takovýmto protokolem je např. protokol Frame Relay. Nebo naopak virtuální okruh může navázat spojení a doručení dat garantovat, tj. přenášená data čísluje a příjemce potvrzuje příjem dat. Pokud by se nějaká data ztratila, pak je dožádáno jejich opakování. Tento mechanismus používá např. protokol X.25.

Výhodou virtuálního okruhu je, že je nejprve sestaven (pomocí signalizace) a teprve do sestaveného okruhu se vkládají data. Každý paket obecně nemusí ve svém záhlaví nést globálně jednoznačnou adresu příjemce, ale pouze identifikaci okruhu.

V Internetu se mechanismus virtuálních okruhů nepoužívá, protože zničení uzlu ve virtuálním okruhu znamená přerušení spojení, což nevyhovovalo tvůrcům rodiny protokolů TCP/IP, která byla prvotně vytvořena pro ministerstvo obrany USA. Z tohoto důvodu IP-protokol nepoužívá virtuální okruhy. Každý IP-datagram nese IP-adresu příjemce (tj. úplnou směrovací informaci) a je proto dopravován samostatně.

Zničení uzlu sítě může zničit pouze IP-datagram právě procházející zničeným uzlem v okamžiku zničení uzlu. Další IP-datagramy jsou směrovány přes jiné uzly.

Obr. 1.17
IP-protokol nepoužívá virtuální okruhy



Z obr. 1.17 je vidět, že IP-datagramy 1, 2 a 3 odešly z uzlu A společně na uzel B, ale z tohoto uzlu jsou již datagramy 1 a 3 směrovány jinou cestou než datagram 2. Do cílového uzlu D pak každý z našich datagramů dorazí jinou cestou. Obecně IP-datagramy mohou dorazit i v jiném pořadí než byly odeslány, tj. např. v pořadí 2, 1 a 3.
Nad nespojovaným IP-protokolem se v Internetu používá protokol TCP (protokol vyšší vrstvy), který spojení naváže a který garantuje doručení dat. Tj. pokud zjistí, že se některá data ztratila, vyžádá si jejich opakování. Pokud byla data ztracena díky zničení některého uzlu sítě a v síti existuje ještě jiná cesta, pak opakování dat již automaticky proběhne po této záložní cestě.
Abychom byli objektivní, tak na obranu protokolu X.25 musíme uvést, že to je protokol popisující pouze rozhraní mezi uživatelem a sítí X.25. Uvnitř sítě X.25 (kam uživatel nevidí), mohou být pak data přenášena obdobně jako v Internetu (tj. nikoliv protokolem X.25 samotným).

Pevné a komutované virtuální okruhy
Virtuální okruhy rozeznáváme:
- ✓ Pevné (*Permanent Virtual Circuit – PVC*), tj. virtuální okruhy pevně sestavené administrátorem

sítě.
- ✓ Komutované (*Switched Virtual Circuit – SVC*), tj. virtuální okruhy dynamicky vznikající podle okamžité potřeby. SVC se vytváří pomocí tzv. signalizačních protokolů, což jsou protokoly pomocí kterých spolu mohou komunikovat uživatel a samotná Síť. Síť signalizuje uživateli různé mimořádné stavy, pomocí kterých lze spravovat i monitorovat Síť, ale právě i vytvářet okruhy.

Na SVC se tak komunikace skládá ze dvou kroků: z vytvoření virtuálního okruhu a z jeho vlastního využití ke komunikaci.
PVC je obdobou pevných linek a SVC je obdobou komutovaných (vytáčených) linek v telefonní síti.
Poznámka: Protokoly využívající virtuální okruhy se anglicky nazývají *Connection Oriented Network Services* (CONS) a protokoly dopravující své pakety bez sestavení virtuálních okruhů se anglicky nazývají *Connection-Less Network Services* (CLNS), tj. spojované a nespojované Síťové služby. V této publikaci spojovanou službou míníme službu, kdy je navázáno spojení, kterým jsou potvrzována přijatá data, v případě ztráty dat je pak dožadováno zopakování vysílání.

Základní dělění sítí

Dělení počítačových sítí podle rozlehlosti

WAN - Wide Area Network.

Síť spojující jendnotlivé prvky sítě na vzdálenosti desítek kilometrů a výše. Pro spojení se většinou používají telekomunikační linky. Nejrozsáhlejší sítí typu WAN je dnes síť Internet..

MAN - Metropolitan Area Network

Síť rozprostřená na území města. Většinou slouží k propojení LAN..

LAN - Local Area Network.

Síť sloužící většinou jedné organizaci nebo její čáati. Vzdálenost propojených prvků se většinou počítá ve stovkách metrů nebo jednotkách kilometrů..

Služby poskytované v sítích LAN.

- sdílení nákladných zařízení (laserové tiskárny, plotry, disky ...)
- Komunikace mezi uživateli
- sdílení dat

Služby poskytované v sítích WAN.

- přenos zpráv
- elektronická pošta
- práce na vzdálených počítačích
- využití informačních databází, konference, diskusní kluby, ...

Dělení lokálních počítačových sítí podle hierarchie uzlů

Peer-to-peer

Každý počítač v síti peer-topeer může poskytovat služby ostatním počítačům v síti. V této síti není vyhrazen žádný hlavní počítač. Pojem peer-to-peer lze volně přeložit jako “rovný s rovným”..

Konfigurace sítě spočívá v izolovaném nastavení jednotlivých počítačů. Z toho vyplývá, že správa není centralizována. Pro praxi to přináší menší efektivitu při správě sítě. Sítě peer-to-peer se budují většinou v menším rozsahu. Pořizovací cena je relativně nízká..

Server-client

Uzly v síti srver-client vykonávají dvě rozdílné funkce. “Obslužná stanice” (server) je vyhrazena pro poskytování služeb. Těchto služeb využívají ostatní “pracovní stanice” (workstation)..

Správa celé sítě spočívá buď v konfiguraci jednotlivých serverů nebo je celá správa centralizována do jednoho bodu. To napomáhá k efektivnější správě síťových prostředků Síťe server-client mohou být velmi rozsáhlé. Cena na jejich vybudování bývá vyšší..

.

Typy serverů:.

- ✓ souborový srver - poskytuje diskový prostor
- ✓ tiskový server - umožňuje používání tiskárny více pracovním stanicím najednou
- ✓ databázový server - poskytuje výpočetní výkon pro zpracování databázových úloh
- ✓ komunikační server - zajišťuje propojení sítě s dalšími sítěmi

Topologie počítačových sítí

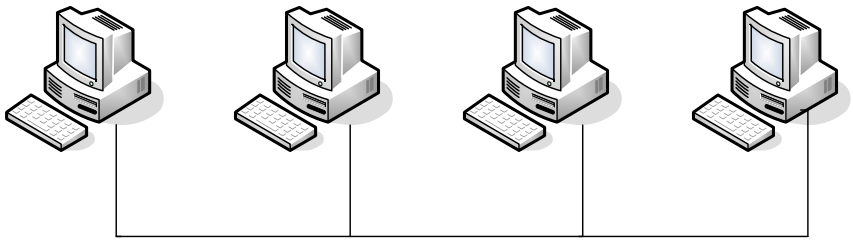
Topologií počítačových sítí rozumíme fyzické uspořádání všech zařízení v síti. Základními typy topologií jsou:.

Sběrnice.

Sítě s topologií sběrnice připojují jednotlivé uzly na společný vodič. V této topologii vysílá signál v jednom okamžiku pouze jeden uzel. Signál se šíří po celém vodiči a zaniká na jeho koncích. Oba konce vodiče jsou zakončeny odporem - **terminátorem**..

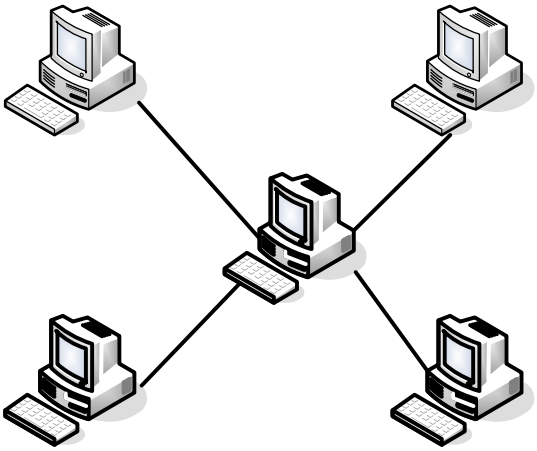
Při poruše libovolného počtu stanic je funkčnost sítě zachována. Porucha vodiče v jednom.

místě znemožní jakoukoli komunikaci..



Hvězda.

Hlavním prvkem je centrální uzel. Tento uzle může být počítač nebo propojovací prvek (hub...). K centrálnímu uzlu jsou připojeny ostatní uzly. Pro chod sítě je rozhodující spolehlivost centrálního uzlu..



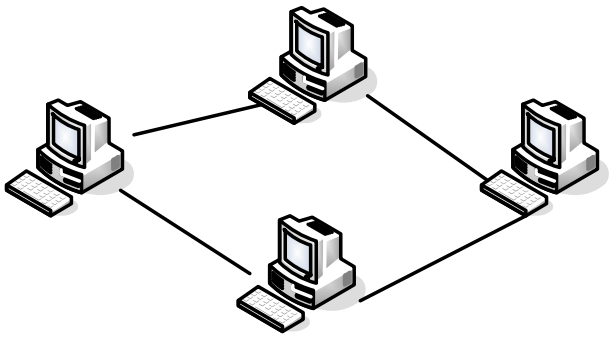
.

Strom.

Vychází z topologie hvězda. Několik hvězd propojíme tak, že koncový uzel jedné hvězdy je centrálním uzlem druhé hvězdy..

Kruh.

Uzly v této síti jsou propojeny postupně od "prvního k poslednímu". Spojením krajních uzlů vznikne kruh. Výpadku jakékoli stanice nebo propojení vede k poruše celé sítě..



.

Token Ring

Sít Token Ring se dostala na trh v roce 1985. Token Ring je označována jako IEEE 802.5. Tento standart specifikuje topologii fyzický kruh, protokol Token Ring (Passing), klasicky přenosovou rychslost 4 Mb/s a definuje speciální kabelové spojení pomocí stíněné kroucené dvoulinky pro oba směry přenosu (je možné i spojení pomocí optického kabelu). V současné době se používá v síti Token Ring rychlost 16 Mb/s..

Charakteristika Token Ring:

Pro síť tohoto typu je charakteristická kruhová topologie s přístupovou metodou Token Passing. Kruhová topologie se vyznačuje tím, že jednotlivé počítače sítě jsou spojené přenosovým médiem fyzicky do kruhu, takže signál přechází postupně přes všechny počítače sítě. Nevýhodou je podstatně horší instalace sítě a skutečnost, že porucha libovolného počítače, ale i porucha některé větve sítě může způsobit její neprůchodnost. Výhodou je vyšší rychlos a více uzlů sítě..

Lepší vlastnosti se dosahují úpravou fyzického kruhu pomocí zvláštních koncentraátorů MAU na logicku hvězdu. Nevýhodou této topologie je omezený počet stanic v kruhu. Na zpoždění

přenášeného rámce se podílí jednak druh kabelu se svou charakteristickou rychlostí šíření signálu a jednak zpoždění dané adaptérem. Pro dosažení zpoždění odpovídajícího rychlosti 4 Mb/s byl stanoven maximální počet 260 uzlů v jedné síti. Čím více bude stanic v síti, tím déle bude trvat cyklus odevzdání práva Token pro vysílání..

Na sběrnici se zachovává jeden směr přenosu. Změna směru znamená problémy s výměnou vstupního konektoru za výstupní na každém uzlu. Kruh musí být za každých okolností uzavřený, takže i při odpojení uzlu z kruhu se na místo uzlu kruh přepojí speciálním konektorem. V každém okamžiku se přenáší v uzavřeném kruhu buď právo Token nebo údaje vysílané některým uzlem.

Rámce podvrstvy MAC:.

V síti Token Ring se rozlišují tři typy rámců. Je to rámec Token, Rušící omezovač a Datový.

1. Token - je rámec, který představuje právo vysílat. Je krátký v délce 3B.

2. Rušící omezovač (Abort Delimiter) - je durhý typ rámce, který při detekci chyby umožňuje předčasně ukončit vysílání rámce. Myslí se tím interní chyba vysílání uzlu nebo chyba ve vysílání některého pole rámce. Každý uzel musí být schopný rozeznat rušící omezovač kdeli v proudu dat.

3. Datový rámec (Frame) - je nejdůležitější z typů rámců sítě. Obsahuje v sobě informace odevzdané vrstvou LLC a služební rámce podvrstvy MAC. Tenhle rámec obsahuje rámec Token. Celková délka rámce je 32B až 16 kB.

Typicky koluje v síti Token s nejnižší prioritou 000. V případě, že uzel požaduje Token přednostně, vyžádá si rezervaci priority rezervačními bity pole AC (bity RRR) v právě procházejícím rámci stanicí. V dalším cyklu Token prochází uzly s nižší priorito, čímž se značně urychlí obsluha příslušného uzlu. Po vykonání činnosti, uzel vráti rezervační i prioritní bity na hodnotu 000..

Pole DA určuje adresu cílové adresy. Norma dovoluje délku 2 až 6 B. Stanovená délka musí být závaznou v celé síti. V síti IBM Token Ring je stanovená na 6B. Individuální, skupinové, globální, nebo lokální adresování se rozlišuje stejně jako v sítích Ethernet. Pole dovoluje definovat univerzální adresu (všechny bity logická 1) pro všechny stanice v kruhu, adresa bez určení (všechny bity logická 0), při které rámec projde sítí bez toho, aby vyl přijatý. Zvláštností v sítích IBM je adresa C000 FFF FFF, jako univerzální. Pak jsou ve skupinových adresách vyhrazeny funkční adresy pro jednoduché adresování přechodových zařízeí určitého typu, jako jsou mosty, servery, atd..

Pole zdrojové adresy SA je individuální adresa uzlu, která rámec vyslala. Na rozdíl od normy IEEE802.5 v IBM sítích nejvyšší bit logická 1 vyjadřuje, že rámec má být přenesen do jiného okruhu odděleného mostem. Mluvíme o tzv. zdrojovém směrování (Source Routing). Při hodnotě logická 0 zůstává rámec v lokálním okruhu..

Pole dat v sítích IBM obsahuje směrovací informace - část RI. Toto pole existuje v případě, že se cílová adresa vyskytuje v jiném okruhu než zdrojový uzel. Pak obsahuje pole směrování 2B a proměnného počtu 16-ti bitových směrovacích polože, které představují čísla okruhů a mostů, přes které bude rámec procházet. Tento mechanismus se označuje jako zdrojové směrování..

V okruhu sítě je vždy jeden uzel označován jako aktivní monitor, který vykonává speciální řídící a kontrolní funkce. Ostatní uzly jsou schopny převzít při výpadku monitoru tyto funkce automaticky. Jedná se o:

1. funkce generování nadřízeného hodinového signálu, synchronizaci, sledování ztráty Tokenu (stanice při ztrátě vynuluje okruh)
2. vygenerování nového Tokenu
3. odstraňování bloudících rámců a Tokenu
4. vyrovnávaní frekvenčních odchylek
5. pravidelná informace o přitomnosti monitoru ostatním uzlům.

V síti Token Ring se mezi užitečnými rámci neustále vysílá proud libovolných bitů typu logická 0, 1. U všech uzlů v síti je frekvence neustále fázově synchronizovaná ze strany monitoru, a proto v rámcích opdadá úvodní synchronizační posloupnost..

Přístupová metoda Token Passing:.

Přístupová metoda Token Passing představuje nekolízní motodu (tedy deterministickou - lze zaručit v časovém intervalu přístup k médiu) s odevzdáváním vysílacího práva Token. Ve stavu klidu, když žádný uzel nevyžaduje právo na vysílání, cyklicky putuje mezi uzly rámec Token (vysílací právo). Libovolný počítač sítě může začít s vysíláním údjaů až když získá toto vysílací právo. Tato metoda má podle použité topologie dvě varianty. Metoda se váže k fyzickému kruhu (Token Ring), nebo ke sběrnici (Token Bus)..

U metody Token Ring adaptér každého uzlu přenáší všechny data ze vstupu na výstup a přitom testuje, zda přijatý rámec je Token nebo jemu adresovaný datový rámec. Doba odezvy při této síti je definovatelná a není kritická při rychlosti 4 Mb/s ani při velkém zatížení v síti. Při výpočtu se vychází z počtu N uzlů (podle normy maximálne 260) a ze zpoždění Ts adapteru jednoho uzlu. Orientačně se maximální zpoždění pohybuje v devítkách mikrosekund. Jednotlivé uzly jsou uspořádané fyzicky nebo logicky do kruhu (Ring) tzn. po poslední m uzlu, který dostl povolení k vysílání, získává oprávnění opět první uzel. Token putuje vždy ve stejném pořadí v jednom směru k sousednímu uzlu. Když uzel o nemá zájem o vysílání, odevzdá Token dalšímu uzlu, která následuje v pořadí. Když ho získá, můůže začít vysílat datové rámce, což je část vysílací zprávy. Když je zpráva delší než je přípustná délka rámce vysílají se postupně rámce za sebou. Po odvysílání datových rámců vyšle Token, když už nechce vysílat data. .

Výhodou této metody je, že každý počítač má zaručeno získání vysílacího práva do určitého časového limitu. Protože údaje jsou přenášena jen jedním směrem, nedojde ke kolizi jak to je u metody CSMA/CD. Tyto sítě jsou proto vhodné pro řízení technologických procesů, kde se vyžaduje řízení v reálném čase..

Přístupová metoda ETR:.

Firma Proteon dosáhla rychlosti do 10 Mb/s a firma IBM až 16 Mb/s díky využití metody ETR (Early Token Relaise - předčasně uvolněný Token), která efektivněji využívá původní přístupovou metodu Token Rlng..

V okruhu je přenášeno více datových rámců současně..

Specifikace fyzické vrstvy v síti Token Ring:.

Dnes se klasické kruhové sítě nebudují. Místo nich se tvoří zvláštní kabelové propojení s charakterem hvězdicové sítě. IBM vyvinula zyfickou hvězdu propojením zpětného vedení logické kruhové sítě. V této síti nejsou počítače propojeny mezi sebou přími, ale prostřednictvím

rozdělovačů kruhového vedení. Pojmenování je Wire Center, nebo MAU (Multiple Access Unit) - vícenásobný přípojný bod..

Každý uzel je připojený k síti dvěmi vedeními k příjimači a vysíči s automatickým testováním je-li uzel v bezporuchovém stavu, nebo jestli má poruchu, nebo je ve vypnutém stavu. Přípojné vedení se realizuje dvojicí klasických koaxiálních kabelů nebo zvláštním dvouvodičovým stíněným krouceným párem v podobě jednoho koaxiálního kabelu pro oba směry toku dat. V obou případech MAU automaticky uzavírá releovým kontaktem požadovaný kruh v místech nepřipojených uzlů. Technicky je to řešeno tak, že každá aktivní stanice pomocí adapteru napájí relé umístěné v MAU, a které svojím kontaktem připojuje uzel do kruhu. Kromě hlavního vedení je v MAU taky náhradní vedení pro případ poškození hlavního okruhu. Váhoda tohoto uspořádání je v centralizaci a v jednodužší opravě a údržbě, ale za cenu větší spotřeby kabelů a vedení. Obvykle je koncentrátor MAU konstruovaný pro 8 uzlů, ale dovoluje libovolné rozšíření. Pro rozšíření má koncentrátor zvláštní svorky RO (Ring Out), RI (Ring In), které je potřeba správně propojit podle směru komunikace. Odpojením tohoto konektoru se pomocí náhradního vedení opět automaticky obnoví uzavřený kruh. Firma Proteon vyvinula MAU s vyšší inteligencí se zabudovaným mikroprocesorem a příslušným programem..

Stíněné kable s krouceným párem se třídí na typy 1, 2, 3, 6 a 8:

1. Typ 1 - je určen pro spojení mezi koncetrátorem a zásuvkou, nebo mezi koncentrátory
2. Typ 2 - odpovídá typu 1, ale kromě hlavního páru a stínění obsahuje navíc 8 vodičů, (použitím tohoto kabelu firma Proteon vytváří diagnostické propojení v síti Token Ring)
3. Typ 3 - nedoporučeje se, když se předpokládá perspektivní zvyšování přenosové rychlosti
4. Typy 6,8 - jsou shodné s typem 3 (typ 8 je mechanicky plošší) a používají se na propojení mezi počítači a koncentrátorem nebo zásuvkou na stěně.

Token Bus

Sítě Token Bus IEEE 802.4 jsou výhodné pro technologické a průmyslové aplikace hlavně pro svou deterministickou motodou přístupu k médiu, která zaručuje čas odezvy pod 20 ms. Důležitou schopností linkové vrstvy pro řízení výroby je zabezpečení prioritního přístupu k médiu. Tato vlastnost umožňuje hierarchizovat jednotlivé uzly podle stupně důležitosti v procesu řízení..

Rámce sítí Token Bus:

Síť IEEE 802.4 podobně jako Token Ring vyžaduje použití speciálních řídících rámců sloužících na zřízení a udržování logického kruhu. Rolišujeme dva druhy řídících a jeden druh informačních rámců. Řídící rámce se odlišují od informačních na zákaldě prvních dvou bitů pole FC (Typ rámce)..

Přístupová metoda Token Bus:.

Linková vrstva využívá ve vrstvě MAC deterministickou přístupovou metodu s odevzdáním přístupového práva po sběrnici, proto má taky označení Token Bus. Metoda zabezpečuje přístup každého uzlu na síť nejpozději po uplynutí určitého přesně definovaného intervalu, poskytuje možnost dynamického přídávání nových uzlů do sítě a řeší poruchy vyvolané uzly sítě..

Základem metody odevzdávání vysílacího práva po sběrnici je tzv. logický kruh, který je virtuálně vytvořený na fyzické sběrnici sítě. Logický kruh je sestaven z posloupnosti uzlů uspořádaných vzestupně podle MAC adres sítě. Uzel sítě vždy odesílá vysílací právo tomu uzlu, kerý má nejbližší vyšší MAC adresu. Každý uzel proto musí znát nejen adresu nejbližšího uzlu v logickém kruhu, ale taky adresu předcházejícího uzlu, od kterého přijímá vysílací právo Token. Logický kruh je tak vlastně tvořený obousměrně. V případě připojení dalšího uzlu do sítě, musí být kruh rekonfigurován, protože se musí vzestupná posloupnost adres uzlů aktualizovat podle nové MAC adresy stanice. Rozlišujeme přitom následující stavy logického kruhu:

1. Začlenění uzlu do kruhu - tento proces probíhá tak, že uzel, který disponuje vysílacím právem, vysípá před jeho odevzdáním na síť periodicky výzvu určenou stanicím, jejichž adresy leží mezi jeho adresou a adresou následujícího uzlu v logickém kruhu. Jak na danou výzvu odpoví některý z uzlů, je automaticky začleněn do kruhu a je mu odesláno vysílací právo. V případě, že na výzvu odpoví několik uzlů současně, hodnotí se tento stav jako kolize a nastartuje se algoritmus binárního vyhledávání nejbližšího uzlu. Naopak, když na výzvu neodpoví žádný uzel, pokračuje se s odevzdáváním práva podle existujícího kruhu.

2. Odebrání uzlu z kruhu - v tomto případě informuje aktivní uzel, který ukončuje činnos v kurhu předcházející uzel a odevzdá řízení následujícímu uzlu. Pro případ, když uzel následkem poruchy nebo z jiných příčin neodpovídá na vysílané pověření do stanoveného časového limitu (response window), odevzdá pověření nejbližšímu vyššímu uzlu v kruhu. Neodpovídající uzel je přitom automaticky vyloučen z logického kruhu.

3. Reinicializace logického kruhu - se vykonává při vytváření, krespektive přerušení logického kruhu. Realizována je vysíláním pověření libovolným uzlem, která delší dobu detekuje nečinnost sítě. V tomto případě se to hodnotí jako kolize a začne probíhat algoritmus binárního vyhledávání adres podle vzestupného pořadí, přičemž se vytvoří nový logický kruh.

Vyjmenované služby zabezpečuje speciální služba MAC - ACM (Access Control Mechanics), která zabezpečuje:

1. řízení přístupu k využívaném médiu
2. detekci chyb a obnovu provozu sítě při chybách přenosu
3. inicializaci a udržování logického kruhu
4. připojování a odpojování uzlů ze sítě

Fyzická vrstva sítě Token Bus:.

Fyzická vrstva je specifikovaná hvězdicovou topologií s optickou kabeláží, případně sběrnicovou topologií s koaxiálním kabelem CAT (Cable Antenna Television) s impedancí 75 Ohmů. U optických vláken se využívá přenos v základním pásmu (metoda FO). Pro přenos bitů po koaxiální sběrnic se využívají tři rozdílné signální techniky (PFSK, SFSK, FB), lišící se kódováním a přenosovou rychlostí. Norma povoluje následující signální schémata:

1. Carrierband PFSK (Phase Continous Frequency Shift Keying) - je metoda přenosu signálu frekvenční modulací se spojitou změnou fáze, při které se dosahuje přenosová rychlost 1 Mb/s.

2. Carrierband SFSK (Single Channel Phase-Coherent Frequency Shift Keying) - je frekvenční modulace s koherentní fází, která dovoluje přenosovou rychlost 5 a 10 Mb/s.

3. Broadband FB (Full Broanbandbus) - je režim přenosu s amplitudo-fázovou modulací PSK v proloženém pásmu s přenosovými rychlostmi 1, 5, 10 Mb/s. V tomto případě je topologie stromová. Na rozdíl od metod Carrierband není celé přenosové pásmo přiděleno jediné přenosové cestě pro analogový signál, ale využívá se frekvenční multiplex.

4. Baseband FO (Fiber Optic) - je přenosová metoda v základním pásmu (270nm) s použitím optických vláken a frekvenční středem v oblasti 800-900 nm. Topologie je ve formě aktivní nebo pasivní optické hvězdy s podobnou funkcí jako je u opakovačů 802.3.

Celkový dosah sítě závisí na použitém signálním schématu, které určuje maximální délku segmentů a počet opakovačů u multisegmentové sítě. Například pro metodu PFSK se doporučuje maximální vzdálenost 7600m a při použití méně kvalitní kabeláže se nedoporučuje překročení délky segmentu nad 1280m. Propojovací kabel uzlu ke sběrnici by neměl přesáhnout 30 cm. V současnosti se upřednostňuje varianta sítě FB s modulací PSK, která má nejvyšší přenosovou kapacitu. V této variantě se využívá úplná širokopásmová sběrnice, s možností použití rozbočovačů (Splitters) pro hvězdicové řešení. .

100VG - AnyLAN

Síť 100VG-AnyLAN IEEE802.12 byla vyvinuta firmou Hewlett Packard. Tato síť patří k vysokorychlostním sítím LAN, přičemž na rozdíl od Ethernetu poskytuje deterministickou metodu přístupu..

Charakteristika sitě 100VG-AnyLAN:.

Tato síť je založena na přístupové metodě DPP s prioritním přístupem k médiu. Umožňuje přenosy támců sítí Ethernet a Token Ring po klasické UTP a STP kabeláži rychlostí 100 Mb/s. Využití kabeláže UTP třídy 3 při přenosové rychlosti 100 Mb/s se odrazilo i v názvu sítě, kde písmeno A (Any) naznačuje funkčnost sítě na libovolných hlasových linkách z kroucených párů VG (Voice Grade). Topologie sítě je hvězdicová a je založenána aktivních prvcích, opakovačích 100VG-AnyLAN Hub..

Linková vrstva MAC sítě 100VG-AnyLAN:.

Podvrstva MAN linkové vrstvy, předepisuje formát a typy používaných rámců dané sítě a způsob přístupu ke společně využívanému médiu..

Sítě 100VG-AnyLAN používají na úrovni podvrstvy MAC tři typy rámců:

1. rámce Ehternet 802.3

2. rámce Token Ring 802.5

3. testovací rámce

Na přenos dat se z důvodu kompatibility s nejrozšířenějšími sítěmi LAN používají osvědčené rámce sití Ethernet a Token Ring. V jedné síti 100VG-AnyLAN však není možné současně použíi oba typy rámců. Na komunikaci se vždy používá jen jeden z nich. Zachovaný je nejen systém adresování koncových uzlů sítě, ale i typové označení a způsob kontroly přenosu rámců

prostřednictvím cyklického kódu CRC. Mimo datových rámců se u sítí 100VG-AnyLAN používají i speciální rámce, sloužící na testování koncových zařízení sítě a identifikaci jeji funkce, během sestavování spojení..

Příprava spojení:

Procedura přípravy spojení (Link Training) zabezpečuje inicializaci spojení mezi koncovým zařízením a kativním prvkem sítě 100VG-AnyLAN. Během procedury se vyhodnotí integrita linky testovacím signálem "klidový stav", následuje výměna testovacích rámců, ze kterých zjistí opakovač typ a MAC adresu připojeného koncového zařízení. Po inicializaci spojení je koncový uzel zařazený do režímu cyklické kontroly přístupové metody DPP, když je buď v klidovém stavu nebo zasílá na port opakovače požadavek na vyslání rámce..

Přístupová metoda MAC 100VG-AnyLAN DPP (Demand Priority Protocol):.

Sítě 100VG-AnyLAN používají úplně novou přístupovou metodu, která eliminuje negativní vlastnosti existujících přístupových metod CSMA/CD a Token Ring. Metoda DPP pracuje deterministicky protože nepoužívá kolizní metodu a eliminuje zpoždění přenosu kolizí Ethernetu nebo oběhu Tokenu mezi uzly sítě Token Ring. Metoda DPP je založena na prioritě vysílání koncových uzlů. Každý uzel má přidělenou dvouúrovňovou prioritu skládající se z čísla portu a přiřazené úrovně priority (0, 1). Aktivní prvek obslouží jednotlivé požadavky na vyslání rámce, v pořadí podle stupně přidělené priority. Vlastní činnost DPP se vykonává prostřdnictvím tzv. cyklů DPP:

1. cyklické testování portů opakovače, zda koncové zařízení neodeslalo požadavek na vysílání
2. test priority jednotlivých požadavků
3. obsluha požadavků podle úrovně priority (přepnutí rámce na port s odpovídající cílovou MAC adresou)
4. nastavení priority "1" u požadavnků neobsloužených do 200ms.

Metoda zabezpečuje vyslání jednoho rámce s maximálním zpožděním 200 až 300 ms. Jedná se o deterministickou přístupovou metodu, která specifikuje dobu potřebnou na přenos rámce. V rámci jednoho cyklu metody DPP může koncový zařízení odeslat maximálně jeden rámce, takže při vyslání následujícího rámce se postup cyklicky opakuje. U zřetězených opakovačů je motoda DPP identická s tím, že rozlišujeme opakovač vyšší a nižší úrovně. Oba opakovače samostaně vykonávají cyklus DPP. Během cyklu DPP odevzdá vyšší opakovač dočasn ěřízení nižšímu opakovači, který uskuteční vlastní cyklus DPP a odešle v příslušném pořadí na port vyššího opakovače rámce těch uzlů, kteří požadují komunikaci s uzly vyššího opakovače. Pro vyšší opakovač se celý proces jeví transparentně, jako by komunikoval přímo s koncovými uzly nižšího opakovače. Nastavení dané priority koncových uzlů vykonává správce sítě, konkrétní aplikace, resp. samotná metoda u překročení časového limitu na spracování rámce..

Fyzická vrstva sití 100VG-AnyLAN:.

Fyzická vrstva sítí 100VG-AnyLAN je založena, podobně jako u Ethernetu na vrstveném principu, který umožňuje použití různých přenosových médií..

PMI (Physical Medium Independent) je podvrstva nezávislá od použitého přenosového média. PMI rozděluje jednotlivé bity rámce do čtyřech samostatných kanálů pro jejich další spracování a způsob přenosu. Do její funkce patří konverze oktenů (8bitů) MAC rámce na kvintety (5bitů), jejich překódování a převod na sexteny (6bitů) kódem 5B6B. Kód 5B6B zaručuje mezi jednotlivými šesticemi Hammingovu vzdálenost d=4 s detekcí 3 bitových chyb, což je nutné při

použití méně kvalitní kabeláže a při vysokých rychlostech. Mimo to vytváří PMI pro každý kanál fyzický rámec s preambulí, úvodním a koconým omezovačem..

MII (Physical Media Dependent) je standartní rozhraní nezávislé od média, kterým odevzdává podvrstva PMI fyzické rámce podvrstvě PMD..

PMD (Physical Media Dependent) vykonává převod fyzického rámce na elektrický signál prostřednictvím kódování NRZ (Non Return to Zero) a multiplex kanálů podle použitého typu kabeláže. U kabelových rozvodů UTP se používají na přenos všechny čtyři páry, přes které se přenášejí fyzické rámce jednotlivých kanálů. Signál NRZ je časovaný frekvencí 30 MHz o šířce pásma 15 MHz, čemuž vyhovuje i kabeláž třídy 3. U kebelových rozvodů STP se používá dvoupárový přenos a u optiky dvojice vláken pro každý směr přenosu. V těchto případech se rámce jednotlivých kanálů přenášejí časovým multiplexem na jediný kanál s přenosovou rychlostí 120 Mb/s (místo 5 bitů se přenáší 6)..

MDI (Media Dependent Interface) je rozhraní mezi vrstvou PMD a vlastním médiem. Jde vlastně o použitý konektor. U UTP káblů se používá konektor RJ45..

Konfigurace sítě 100VG-AnyLAN:.

Síť 100VG-AnyLAN na rozdíl od 100BaseT není vhodná pro tvorbu vysokorychlostních páteřních sítí. Její použití se předpokládá spíše v menších pracovních skupinách s aplikačními požadavky na velkou šířku pásma a citlivost na zpoždění (multimedia, interaktivní vide). Propojení vysokorychlostních pracovních skupin se ponechává na sítě FDDI, nebo páteřní řešení na základě přepínačů ATM..

Toplogie sítě je výhradně hvězdicová. Opakovače 100VG-AnyLAN Hub jsou vybavené výstupními porty (Down-Link Port) pro připojení koncových zažízení a propojovacích portů (Up-Link Port), sloužících na připojení k vyššímu 100VG-AnyLAN Hub v kaskádě. Porty můžou být konfigurovány jako privátní a promiskuitní. Privátní porty přijimají jen rámce s odpovídající MAC adresou, zatimco promiskuitní přijimají všechny vyslané rámce, což je nutné například u přepojovacích prvků 10/100 Bridge, který umožňuje připojení na klasické sítě Ethernet..

FDDI

Síť FDDI (Fiber Distribute Data Interface) ANSI X3T12 nepatří ke standartům. Původním záměrem tvůrců bylo vytvořit komunikační rozhraní, které umožňuje propojení počítačů s distribuovanými periferními zařízeními prostřednictvím optických vláken. Později s rozvojem počítačových sítí, se sítě FDDI začaly díky svému výkonu 100 Mb/s a deterministickému přístupu k médiu, využívat jako propojovací vysokorychlostní páteřní sítě. Intergaci se sítěmi LAN 802.3, 802.5 umožnila zejména dobře implementovaná podpora podvrstvy LLC. Síť FDDI byla začátkem devadesátých let jediným standartem u vysokorychlostní páteřní sítě, což se projevilo v budování těchto sítí u větších podnikových a univerzitních tzv. CAMPUS sítí. Síť FDDI pak byla propracována na síť FDDI-II s izochronním režimem přenosu, podporou multimédií, videokonferencí..

Charakteristika FDDI:.

Jsou charakteristické zdvojenou kruhovou topologií, ve které jsou jednotlivé uzly propojené oběma kruhy protisměrně. Propojení uzlů do kruhu je realizované optickými vlákny. Později byly využity i metalické média s názvem sítě CDDI (Copper Distributed Data Interface)..

Linková vrstva sítí FDDI.

Sítě FDDI mají linkovou vrstvu rozdělenou na dvě podvrstvy LLC a MAC..

Na přenos dat po sítí FDDI se využívají dva typy MAC rámců. Rámce Token a datové rámce. Rámce FDDI dosahují maximální délku 4500 B, minimální délku 9 B a povolený interval mezi dvěma následnými rámci 8 B. .

Přístupová netoda Token Passing:.

Síť FDDI využívá deterministickou přístupovou metodu s odevzdáváním přístupového práva po kruhu tzv. Token Passing, která je obdovou specifikace Token Ring. Na rozdíl od sítě Token Ring dokáže síť FDDI přenášet rámce od několika uzlů současně. V případě FDDI uzel vysílá Token hned po odvysílání posledního rámce z dávky rámců uvolněným přijetím předchozího Tokenu. Metoda je podobná jako ETR. Poskytuje vyšší propustnost a eliminované je i opoždění dané oběhem Tokenu..

Fyzická vrstva sítí FDDI:.

Fyzická vrstva FDDI vykonává podobné funkce jako fyzické vrstvy sítí LAN - kódování, synchronizaci, přiřazení symbolů, atd. Vlastní architektura fyzické vrstvy je modulární v podobě vrstev z důvodu přispůsobení u různých přenosových médí, konektorů, vysílačů a příjimačů..

Topologie sítě:.

Síť FDDI využívá výhradně kruhovou topologii, ve které jsou jednotlivé uzly propojené prostřednictvím protisměrných kruhů. Oba kruhy pracují s přenosovou rychlostí 100 Mb/s, přičemž je jeden kruh aktivní (Active Ring), přenášejí se po něm rámce komunikujících uzlů, zatímco druhý slouží jako záložní (Standby Ring). Při poruše, například při přerušení optického vlákna nebo při poškození uzlu, může být vytvořený rekongifurovaný kruh a tak zachována funkčnost sítě. Rekonfigurovaný kruh je vytvořený přepojením primárního a sekundárního kruhu. V síti FDDI se používají následující typy uzlů

1. mosty (Bridge)
2. koncové stanice DAS, SAS (Dual/Single Attachment Station)
3. koncentrátory DAC, SAC (Dual/Single Attachment Concentrator)

Mosty - se využívají na připojení jiných typů sítí LAAN na síť FDDI a jejich vzájemnou komunikaci. Pracují na úrovni LCC jako heterogenní mosty, protože umožňují nejen přispůsobení rychlosti (Token Ring/FDDI 4,16/100 Mb/s. Ethernet/FDDI 10/100 Mb/s), ale i konverzi jednotlivých typů rámců a při¨ístupových metod. Jsou dodávány jako zařízení DAS se dvěma LAN porty (Ethernet). Dnes se dodávají i víceportové mosty označované jako FDDI přepínače..

Koncové stanice - jsou určeny na přímé připojení uzlů k síti FDDI. Jsou to uzly, který vyžadují vysokou propustnost a šířku pásma jako například různé servery, výkonné pracovní stanice. Koncové stanice se můžou použí ve formě DAS jako uzes se dvěma vstupními a výstupními porty pro oba kruhy, nebo SAS jenom s jedním portem pro jednodušší topologie a bez možnosti rekonfigurace. V úloze koncových stanic SAS a DAS můžou vystupovat rovněž samotné směrovače a mosty s připojením na jité typy sítí..

Koncentrátory - mají několik portů. Umožňují připojení několika stanic DAS, SAS v mítě jednoho přímo připojeného aktivního prvku sítě FDDI. Používají se na připojení koncových uzlů (pracovní stanice, servery) osazenými rozhraním FDDI většinou ve formě SAS..

Omezení sítě FDDI vzhledem na topologii a dosah:

1. maximální dosah sítě 1max = 100 km
2. celková délka optických vláken 1c = 200 km, při dvojitém kruhu

3. maximálně překlenutelná vzdálenost mezi sousedními uzly 1umax = 2 km
4. maximální počet uzlů v síti FDDI nmax = 1000

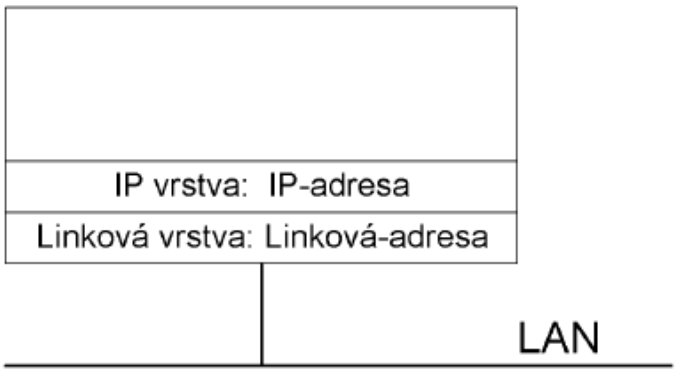
IP protokol - Internet protocol

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 bu1 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.
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.

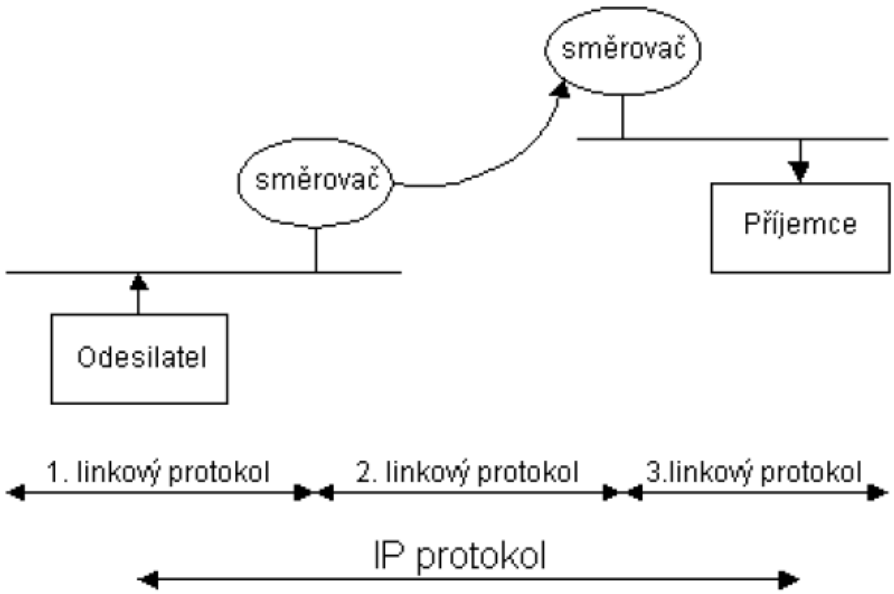
Obr. 5.2
Linková adresa a IP-adresa



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. Slovo směrovač má tedy dva významy. V prvním obecném významu se směrovačem míní funkce počítače (a; klasického počítače nebo specializované skříňky) předávat datové pakety mezi dvěma síťovými

rozhraními a v druhém a to praktickém smyslu se jím označuje specializovaná skříňka pracující jako směrovač.
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. Na každém rozhraní směrovače může být použit jiný linkový protokol. A nenechte se mýlit případem, kdy směrovač na svých rozhraních používá stejný linkový protokol – např. Ethernet. I v tomto případě dochází k „přebalování“ – stačí si uvědomit, že ethernetový rámec používá před přebalením jiné fyzické adresy než po přebalení.
Avšak pádným argumentem na otázku „proč dva protokoly“ jsou až vlastnosti protokolů, které používají k dopravě dat pouze linkovou vrstvu, tj. jednotliví účastníci komunikace mají pouze linkové (šestibajtové) adresy. Takovými protokoly jsou např. NetBEUI (Microsoft) či LAT (Digital). Tyto protokoly 120 Velký průvodce protokoly TCP/IP a systémem DNS
Obr. 5.2 Linková adresa a IP-adresa jsou jednoduché a opravdu asi rychlejší při tvorbě a zpracování svých paketů. Avšak díky tomu, že lze příjemce adresovat pouze v rámci LAN, tak nelze odeslat data příjemci za směrovačem – tj. ve WAN.
Proto se tyto protokoly označují jako nesměrovatelné. Jsou použitelné pouze v rámci lokální sítě, nikoliv mimo ni.

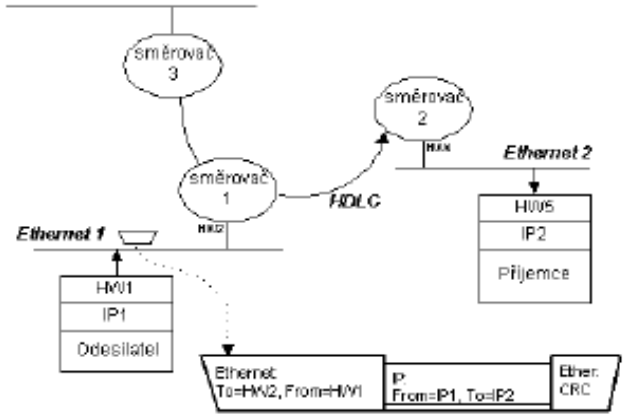
Obr. 5.3
Linkové protokoly
a IP protokol



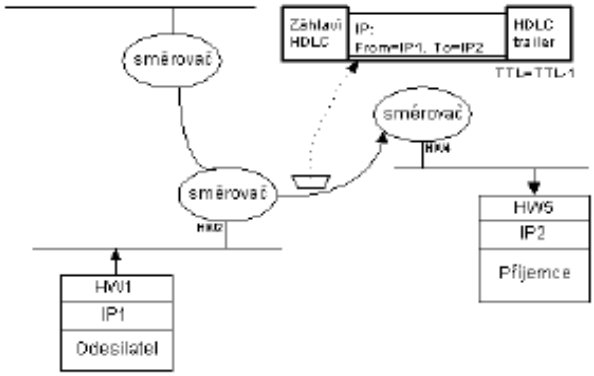
Obrázek 5.3 znázorňuje, že linkový protokol dopravuje datové rámce pouze k následujícímu směrovači, kdežto IP-protokol dopravuje data mezi dvěma vzdálenými počítači rozsáhlé sítě (WAN). Zatímco obálka, kterou jsou na linkové vrstvě data obalena je na každém směrovači vždy zahozena a vytvořena nová, tak 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. Existují i další výjimky, ke kterým se také později dostaneme (např. fragmentace).
Zatímco u linkových protokolů jsme základní přenášené kvantum dat označovali jako linkový rámec, tak u IP-protokolu je základní jednotkou přenášených dat IP-datagram.
Proberme si případ z obr. 5.4, kdy odesílatel z lokální sítě **Ethernet 1** odesílá IP-datagram příjemci na síti **Ethernet 2.** IP-adresu odesílatele a příjemce jsme na obrázku 5.4 pro

jednoduchost označili slovy **From** a **To** jak je zvykem u elektronické pošty. Obdobně jsme označili i linkové adresy. Např. odesílatel má na obrázku linkovou adresu HW1.
Odesílatel chce odeslat IP-datagram příjemci o IP-adrese IP2. Vytvoří IP-datagram, ale aby jej mohl vložit do lokální sítě, tak jej musí vložit do linkového rámce (v našem případě Ethernet). Docela výstižné je přirovnání, že „IP-datagram byl naložen na lo1 Ethernet 1". Linkovým protokolem však mohou tato data putovat jen na **směrovač 1**, který IP-datagram vybalí z ethernetového rámce a podívá se na Ipadresu příjemce. Podle IP-adresy příjmce se rozhodne kterým svým rozhraním pošle IP-datagram dále – tj. „na jaký linkový protokol se provede překládka IP-datagramu".
Rozhodování to však není jednoduché, směrovač se rozhoduje na základě svých směrovacích tabulek (*routing table*), kterým se budeme také podrobně věnovat. Předpokládejme, že směrovač se rozhodl pro linku **HDLC**.

Obr. 5.4
Odesílatel odesílá IP-datagram v rámci protokolu Ethernet

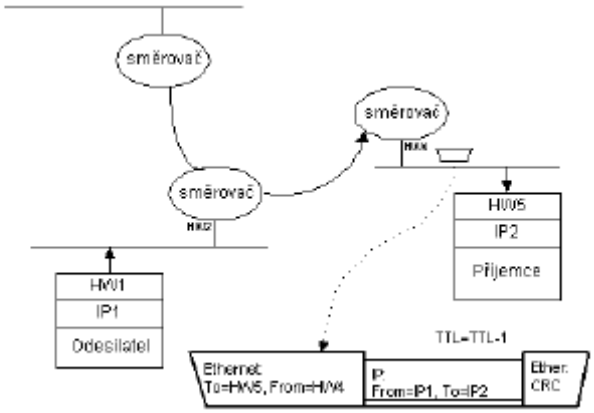


Obr. 5.5
IP-datagram byl vložen do rámce protokolu HDLC



Směrovač sníží hodnotu položky TTL alespoň o jedničku a vloží náš IP-datagram do jiného linkového protokolu, kterým je v tomto případě protokol HDLC – viz obr. 5.5. Přirovnáme-li protokol HDLC ke kontejnerové dopravě, pak „náš IP-datagram byl přeložen z lodi Ethernet 1 do kontejneru společnosti HDLC".
Protokolem HDLC je náš IP-datagram dopraven na následující směrovač, který opět IP-datagram vybalí z HDLC-obálky, sníží hodnotu položky TTL a po obalení ethernetovou obálkou jej vloží do cílové LAN.

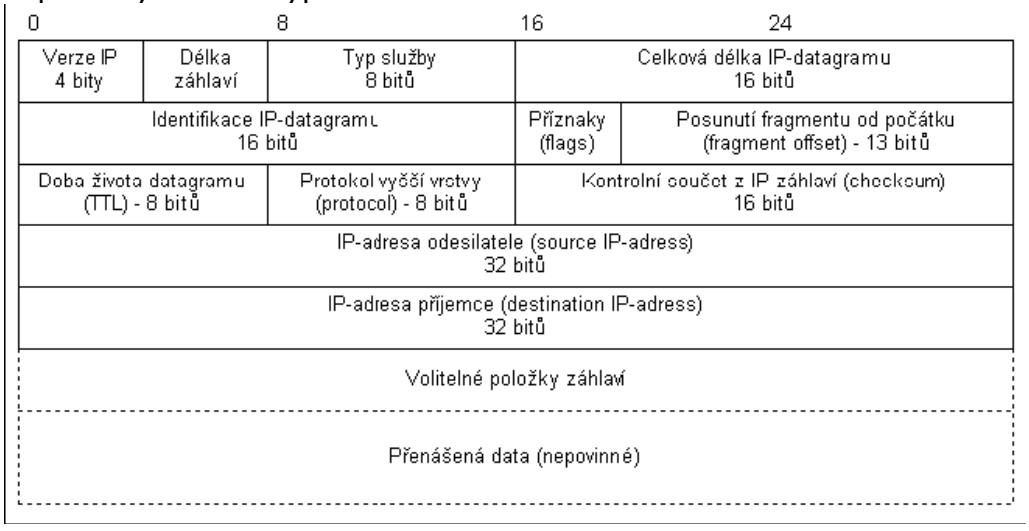
Obr. 5.6
IP-datagram je opět vložen do rámce protokolu Ethernet



Záměrně jsem si na obou LAN vybral stejný linkový protokol (Ethernet). Aby bylo vidět, že pokaždé se jedná o zcela jiný linkový rámec. Na LAN odesílatele má ethernetový rámec adresu příjemce HW2 a odesílatel HW1, kdežto na LAN příjemce se sice také jedná o Ethernet, ale linková adresa příjemce je HW5 a odesílatele HW4.

IP Datagram

Při výkladu protokolů TCP/IP je zvykem vše znázorňovat v tabulce jejíž řádek má 4 bajty, tj. bity 0 až 31. I my budeme často používat toto znázornění.
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.
Struktura IP-datagramu je na obrázku 5.7. Ještě než začneme popisovat jednotlivé položky záhlaví, tak si nějaký IP-datagram odchytneme pomocí MS Network Monitoru (viz obr. 5.8).
A tak bude okamžitě vidět, zdali sítí chodí opravdu to, co popisujeme. Nyní již můžeme začít s popisováním významu jednotlivých položek záhlaví IP-datagramu.
Verze (*version*) je první položkou záhlaví IP-datagramu. Tato položka dlouhá 4 bity (půl bajtu) obsahuje verzi IP-protokolu. V této kapitole hovoříme o IP-protokolu verze 4, tudíž tato položka je v našem případě rovná hodnotě 4. **Délka záhlaví** (*header length*) obsahuje délku záhlaví IP-datagramu. V případě odchyceného IP-datagramu na obr. 5.8 je délka záhlaví 20, ale jak je vidět z hexadecimálního výpisu z MS Network Monitoru, tak položka délka záhlaví nabývá hodnoty 5 (nikoliv 20). Vysvětlení je prosté. Délka není uváděna v bajtech, ale v čtyřbajtech a 5x4=20. Délka záhlaví musí tak být i v případě použití volitelných položek násobkem čtyř. V případě, že by záhlaví nevyšlo na násobek čtyř, pak se na násobek čtyř doplní nevýznamnou výplní.



Obr. 5.8 IP-datagram odchycený pomocí MS Network Monitoru

Maximální délka záhlaví IP-datagramu je tedy omezena tím, že položka délka záhlaví má k dispozici pouze 4 bity (11112=F16=1510). Délka záhlaví IP-datagramu je tedy maximálně 60 B (=15x4). Jelikož povinné položky mají 20 B, tak na volitelné položky zbývá maximálně 40 B.

Typ služby (*type of service – TOS*) je položka, která v praxi nenašla svého naplnění. V normách RFC-791 a RFC-1349 lze nalézt konkrétní návrhy využití. Záměr spočíval v jistém nedostatku IP-protokolu jehož podstatou je skutečnost, že v Internetu není zaručena šíře přenosového pásma mezi účastníky.

Jistého vylepšení se mělo dosáhnout právě touto položkou, pomocí které je možné označit některé Ipdatagramy tak, aby byly dopravovány přednostně či aby byla zaručena rychlá odezva atp.

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.

Síťové služby

Každý počítač začleněný do sítě má možnost využívat tkz. Síťové služby. Pod tímto pojem si můžeme představit různé služby, jako např. E-mailové služby, Fileserver služby atd. My se zaměříme na hlavní a jedny z nejdůležitějších služeb, které většina uživatelů vyžadují.

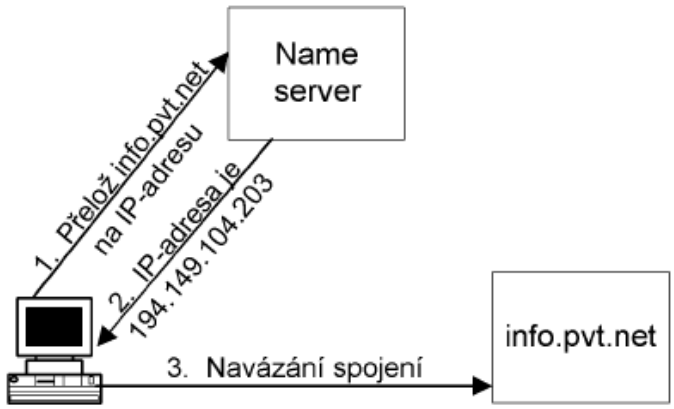
- ✓ Network Disk Service je služba, která umožňuje uživateli ukládat své data na disk a adresář, který je na serveru.
- ✓ AntiVirus Shield Service se často používá v síťích jako ochrana uživatelů před napadením viru.
- ✓ ADS – Active Domain Service je služba, která je poskytována se serverovými produkty firmy Microsoft. Pomocí této služby se uživatel přihlašuje na server a má určitá práva provádět určité úkony a operace.
- ✓ E-Mail Service je poštovní služba, která umožňuje uživatelům přijímat a odesílat elektronickou poštu.

Služeb je tedy celá řada počínaje bežícími službami v PC uživatele až po ICQ.

DNS

Všechny aplikace, které zajiš_ují 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 sí_ového rozhraní. Pro každou IP-adresu máme zavedeno jméno sí_ového rozhraní (počítače), přesněji řečeno doménové jméno. Toto doménové jméno můžeme používat ve všech příkazech, kde je možné použít IP adresu. Výjimkou, kdy se musí použít IP-adresa, je identifikace samotného name serveru.
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.

Obr. 11.1
Před navázáním spojení je nutné přeložit jméno na IP-adresu

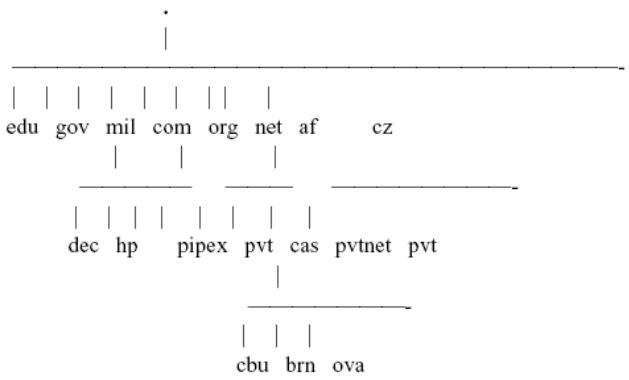


Použití IP-adres místo doménových jmen je praktické vždy, když máme podezření, že DNS nám na počítači nepracuje korektně. Pak, ač to vypadá nezvykle, můžeme napsat např:
ping 194.149.104.203
http://194.149.104.203

či odeslat mail na: dostalek@[194.149.104.203]
Reakce však může být neočekávaná zejména pro poštu, protokol HTTP a protokol HTTPS. Poštovní server totiž nemusí podporovat dopravu na servery uvedené v hranatých závorkách. Protokol http nám vrátí primární webovou stránku a protokol HTTPS se bude rozčilovat, že jméno serveru neodpovídá položce CN v jedinečném jméně certifikátu serveru.

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 přižazeno 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: pvt.cz (pro PVT, a.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.

Syntaxe jména

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

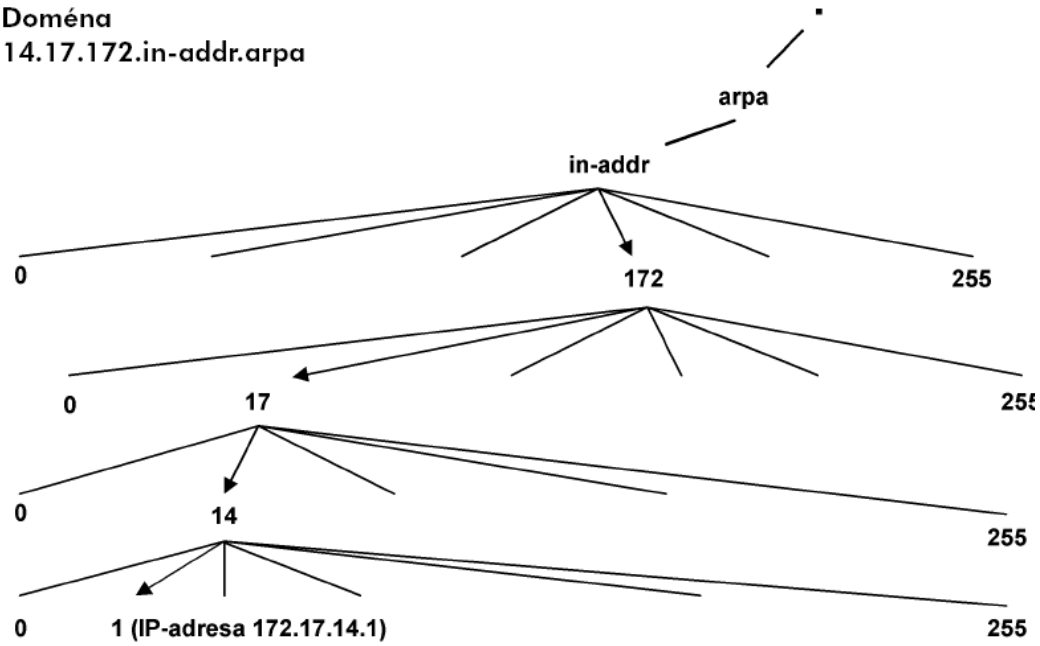
Existují i rozšíření specifikující bohatší repertoár znaků použitelných pro tvorbu jmen. Zásadně se však těmto dalším znakům vyhýbáme, protože jen některé aplikace toto rozšíření podporují. Mohou se použít velká i malá písmena, ale není to zase tak jednoduché. Z hlediska uložení a zpracování v databázi 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. bylo-li 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!). Do kterých domén počítač patří se definuje příkazy domain
a search v konfiguračním souboru resolveru.
Upozornění
Netvořte jména subdomén v kolizi se jmény Top Level Domén. Např. chcete-li rozdělit doménu *pipex.cz* na subdomény podle krajských měst a použijete dvojznakové řetězce, vznikne problém. Pro Liberec byste si vybrali např. *lb.pipex.cz*.
Uživatel z domény *cbu.pipex.cz* bude psát mail uživateli Alois v doméně *lb.pipex.cz* a napíše podle předchozího pravidla příkaz:
mail Alois@lb
(oba jsou přece v doméně pipex.cz). No a milý mail dojde klidně do Libanonu. Důvodem je to, že neexistuje přesná specifikace „místní domény“. To, co se doplňuje zprava v případě, že uživatel nezadal tečku na konci, je zcela v kompetenci místního správce.
Uvedenému problému předejdete, zvolíte-li si pro Liberec např. doménu *lbc.pipex.cz*.

Reverzní domény
Již jsme uvedli, že komunikace mezi uzly probíhá na základě IP adres, nikoli doménových jmen. 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.
Podobně jako domény tvoří i IP-adresy stromovou strukturu. Domény tvořené IP-adresami se pak často nazývají reverzní domény. Pro účely reverzního překladu byla definována pseudodoména „inaddr. arpa“. Jméno této pseudo domény má historický původ, jde o zkratku „*inverse addresses in the Arpanet*“.

Obr. 11.2
Doména
14.17.172.in-addr.arpa



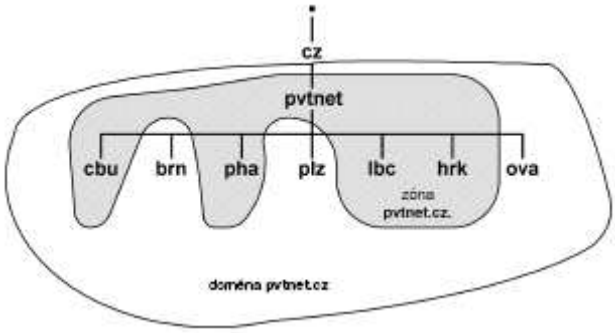
Pod doménou in-addr.arpa jsou domény jmenující se jako první číslo z IP-adresy sítě. Např. sí_ 194.149.101.0 patří do domény 194.in-addr.arpa. Sí_ 172.17 patří do domény 172.in-addr.arpa. Dále doména 172.in-addr.arpa se dělí na subdomény, takže sí_ 172.17 tvoří subdoménu 17.172.in-addr.arpa.
Je-li sí_ 172.17 rozdělena pomocí sí_ové masky na subsítě, pak každá subsí_ tvoří ještě vlastní subdoménu.
Všimněte si, že domény jsou zde tvořeny jakoby IP-adresami sítí psanými ale pozpátku.
Reverzní domény pro subsítě adres třídy C jsou tvořeny podle metodiky classless in-addr.arpa. Přesto že 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 subsí_ 194.149.150.16/28 je 16.150.149.194.in-addr.arpa
Opět i tyto reverzní subdomény sítí třídy C tvoří stromovou strukturu.

Doména 0.0.127.in-addr.arpa
Jistou komplikací (zvláštností) je adresa sítě 127.0.0.1. Sí_ 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.

Zóna
Často se setkáváme s otázkou: „Co je to zóna?“ „Jaký je vztah mezi doménou a zónou?“. Vysvětleme si tedy vztah těchto pojmů na doméně cz.
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.

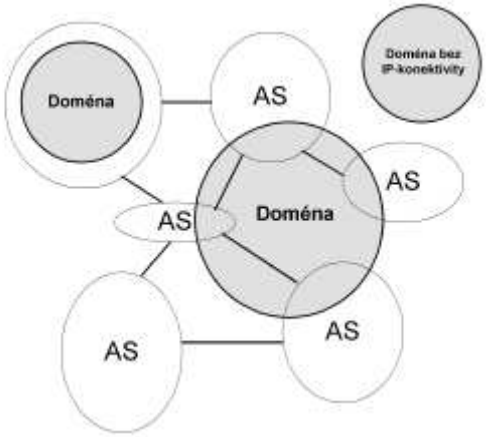
Obr. 11.3
Zóna pvtnet.cz



Na obrázku 11.3 je znázorněno, jak může být (hypoteticky) v doméně *pvtnet.cz* pomocí vět typu NS decentralizována kompetence na nižší správní celky. Takže doména *pvtnet.cz* obsahuje v sobě všechny subdomény, ale zóna *pvtnet.cz* delegovala na jiné name servery pravomoci na zóny *brn.pvtnet.cz*, *plz.pvtnet.cz* a *ova.pvtnet.cz*. Takže zóna *pvtnet.cz* obsahuje doménu pvtnet.cz až na tři uvedené výjimky.

Doména a autonomní systém
Na tomto místě musíme zdůraznit, že rozdělení sítě na autonomní systémy nesouvisí s rozdělením na domény (nebo snad na zóny). Tzn. je-li podniku přiděleno jméno domény a IP-adresy sítí jedním poskytovatelem, pak při přechodu k jinému poskytovateli zůstanou podniku jména domén, ale Ipadresy dostane od nového poskytovatele nové. Musí se tedy přečíslovat jednotlivé LAN, ale jména počítačů a adresy elektronické pošty zůstanou beze změn.

Obr. 11.4
Domény
a autonomní
systémy



Autonomní systémy dělí Internet z hlediska IP-adres (směrování), naproti tomu domény dělí Internet z hlediska jmen počítačů.
Jiná je situace u reverzních domén, které kopírují strukturu poskytovatelů Internetu.

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 obrázku 11.4 je patrné, že mohou existovat i domény, které nejsou přímo připojeny k Internetu, tj. jejichž počítače ani nepoužívají sí_ový protokol TCP/IP – tedy nemají ani IP-adresu. Takovéto doményse 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).

Firma ve své vnitřní síti používá jednak sí_ový protokol TCP/IP a jednak protokol DECnet. Z Internetu je adresován uživatel používající ve vnitřní síti protokol TCP/IP např. *Alois@počítač.firma.cz*. Ale jak adresovat uživatele na počítačích pracujících v protokolu DECnet?

Pro tento případ se vsune do adresy pseudodoména *dnet*. Takže uživatel je adresován *uživatel@počítač.*

dnet.firma.cz. Pomocí DNS je veškerý mail adresovaný do domény *dnet.firma.cz* přesměrován na bránu do protokolu DECnet (brána domény firma.cz), která provede transformaci z protokolu TCP/IP (resp. SMTP) do protokolu DECnet (resp. Mail-11).

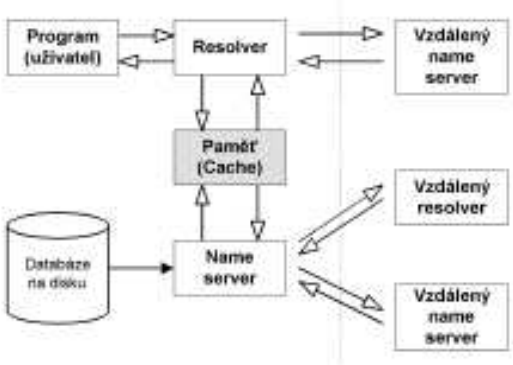
11.8 Dotazy (překlady) Přeložení jména na IP-adresu zprostředkovává tzv. resolver. Resolver je klient, který se dotazuje name serveru. Jelikož je databáze celosvětově distribuována, nemusí nejbližší name server znát odpověď, proto může tento name server požádat o pomoc další name servery. Získaný překlad 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 pamě_ 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.

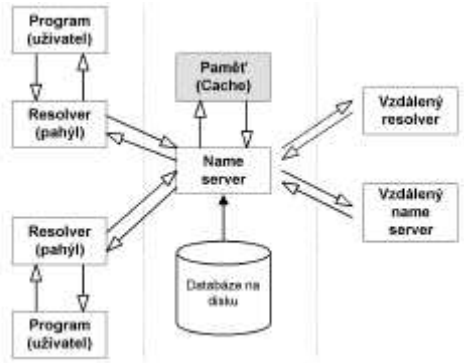
Představme si, že přijde dotaz (např. požadavek na překlad jména na IP-adresu) na name server. Je-li server pro daný dotaz autoritou (autoritativní name server) a nemá požadované jméno v databázi, odpoví negativně (jméno nelze přeložit na IP-adresu). Není-li name server pro daný dotaz autoritou, pak odpoví, že neví a doporučí name server, který by autoritou mohl být.

Obr. 11.5
DNS na serveru

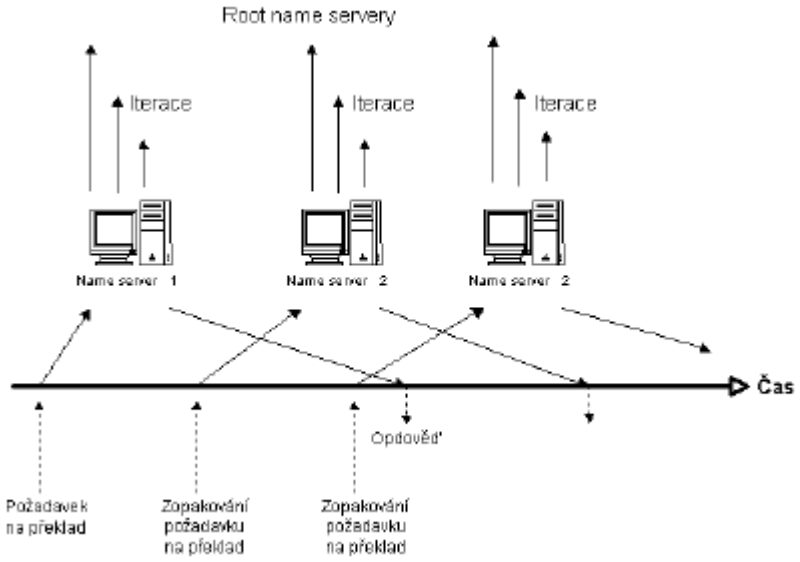


Do paměti se ukládají jen kladné odpovědi. Provoz by byl podstatně zrychlen, kdyby se tam ukládaly i negativní odpovědi (negativní caching), avšak to je podstatně složitější problém. Podpora negativního cachingu je záležitostí posledních několika let.
Takto pracuje DNS na serverech (např. s operačním systémem NT nebo UNIX). Avšak např. PC nemívají realizovány servery. V takovém případě se celý mechanismus redukuje na tzv. pahýlový resolver.
Tj. z celého mechanismu zůstane pouze resolver.
Resolver předává všechny dotazy na lokální name server. Od name serveru pak očekává konečnou (rekurzivní) odpověď. Name server buU odpoví přímo, nebo sám kontaktuje další name servery, tj. name server rekurzivně řeší dotaz a klientovi zašle až výsledek.
Lokální name server udržuje společnou cache pro všechny lokální počítače.

Obr. 11.6
Pahýlový resolver



Z obrázku 1.6 je patrné, že lokální name server udržuje společnou cache pro všechny lokální počítače s pahýlovým resolverem.
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 (příznakem *truncation* může být signalizováno, že se odpověď nevešla do 512 B a pro přídanou kompletní odpověď je nutné použít protokol TCP). Délka UDP paketu je omezena na 512 B, protože u větších IP-datagramů by mohlo dojít k fragmentaci. Fragmentaci UDP datagramu DNS nepovažuje za rozumnou.
Dotazy, kterými se přenášejí data o zóně (*zone transfer*) např. mezi primárním a sekundárním name serverem, se přenáší protokolem TCP.
Běžné dotazy (např. překlad jména na IP-adresu a naopak) se provádí pomocí datagramů protokolu UDP. Překlad požaduje klient (resolver) na name serveru. Neví-li si name server rady, může požádat o překlad (o pomoc) jiný name server prostřednictvím root name serveru.
V Internetu platí pravidlo, že databáze s daty nutnými pro překlad jsou vždy uloženy alespoň na dvou nezávislých počítačích (nezávislých name serverech). Je-li jeden nedostupný, pak se překlad může provést na druhém počítači.
Obecně se nepředpokládá, že by byly všechny name servery dostupné. V případě, že by se pro překlad použil protokol TCP, pak by navazování spojení na nedostupný počítač znamenalo přečkat časové intervaly protokolu TCP pro navázání spojení a teprve poté by bylo možno se pokusit navázat spojení s dalším name serverem.
Řešení pomocí protokolu UDP je elegantnější: Datagramem se vyšle žádost prvnímu serveru, nepřijde-li se odpověď do krátkého časového intervalu, pak se pošle datagramem žádost dalšímu (záložnímu name serveru), nepřijde-li se opět odpověď, pak se pošle dalšímu atd. V případě, že se vyčerpají všechny možné name servery, pak se opět začne prvním a celý kolotoč se zopakuje, dokud nepřijde odpověď nebo nevyprší stanovený časový interval.



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 buU překlad provede sám, nebo si sám vyžádá pomoc od dalších serverů, nebo zjistí, že překlad není možný.

Do hry ještě vstupují časová omezení. Může se totiž stát, že na položený dotaz nedostane resolver odpověď, ale další stejný dotaz již bude korektně zodpovězen (serveru se mezitím podařilo získat odpověď a první dotaz nebyl zodpovězen proto, že odpověď z jiného name serveru dlouho nepřicházela). Z hlediska uživatele se to jeví tak, že napoprvé se překlad nepovede a při dalším zadání téhož příkazu už ano.

Podobný efekt způsobuje i použití protokolu UDP. Může se totiž také stát, že server vůbec žádost o překlad neobdrží, protože je sí_ přetížená a UDP-datagram se prostě někde ztratil.

Klient může sice mít v konfiguračním souboru uvedeno více name serverů, ale použije se vždy jen odpověď, která přišla první. Tj. když jako první přijde negativní odpověď (např., že k danému jménu neexistuje IP-adresa), nepokusí se resolver kontaktovat další name server, který by jméno snad přeložil (jak si mnozí představují), ale oznámí, že překlad k danému jménu neexistuje. Konfigurační soubor pro resolver se v operačním systému UNIX jmenuje /etc/resolv.conf. Zpravidla obsahuje dva typy řádků (druhý se může několikrát opakovat):

domain jméno_místní_domény nameserver IP-adresa_name_serveru

V případě, že uživatel zadal jméno bez tečky na konci, pak resolver za zadané jméno přidá jméno domény z příkazu *domain* a pokusí se jméno předat name serveru k přeložení. V případě, že se překlad neprovede (negativní odpověď name serveru), pak se resolver pokusí ještě přeložit jméno samotné, tj. bez přípony z příkazu *domain*.

Některé resolvery umožňují zadat příkazem *search* více jmen místních domén.

Příkazem *nameserver* se specifikuje IP-adresa name serveru, který má resolver kontaktovat. Je možné uvést i další příkazy nameserver pro případ, že některé name servery jsou nedostupné. Musí se zde uvést IP-adresa name serveru – nikoliv doménové jméno name serveru!

V případě konfigurace resolveru na name serveru může příkaz nameserver ukazovat na místní name server 127.0.0.1 (nemusí to však být pravidlem).

Další parametry resolveru (např. maximální počet příkazů nameserver) lze nastavit v konfiguračním souboru jádra. Tento soubor se často jmenuje */usr/include/resolv.h*. Musí pak pochopitelně následovat sestavení jádra operačního systému.
Obecně je možné konfigurovat všechny počítače též bez použití DNS. Pak se veškeré dotazy na překlady adres provádějí lokálně pomocí souboru */etc/hosts*. Je možné obě metody i kombinovat (nejčastější případ), pak však je třeba být opatrný na obsah databáze */etc/hosts*. Většinou je možné i nastavit v jakém pořadí se mají databáze prohlížet. Zpravidla se prohlíží nejprve soubor */etc/hosts* a posléze DNS. V DEC OSF/1 slouží pro konfiguraci pořadí prohledávání soubor */etc/svc.conf*.
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".

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

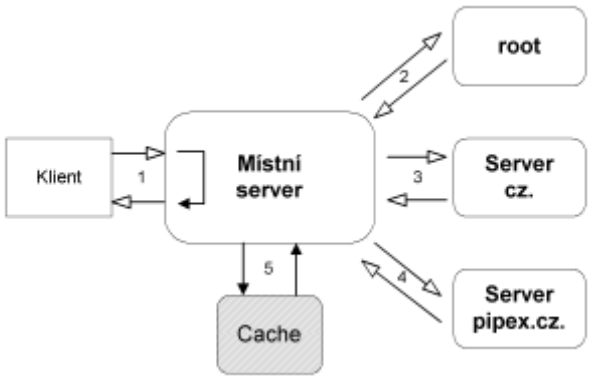
(není žádnou autoritou). Avšak využívá obecné vlastnosti name serveru, tj. data, která jím prochází, ukládá ve své paměti. Tato data se označují jako neautoritativní. Každý server je caching server, ale slovy caching only zdůrazňujeme, že pro žádnou zónu není ani primárním, ani sekundárním name serverem. (Pochopitelně i caching only server je primárním name serverem pro zónu 0.0.127.in-addr.arpa, ale to se nepočítá.)

- **Root name server** je name server obsluhující root doménu. Každý root name server je primárním serverem, což jej odlišuje od ostatních name serverů.

Jeden name server může být pro nějakou zónu primárním serverem, pro jiné sekundárním serverem.
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.
Takže přidá-li správce zóny (*hostmaster*) do databáze na primárním name serveru další počítač, pak po době stanovené parametrem ve větě SOA se tato databáze automaticky opraví i na sekundárních name serverech (opravil-li by ručně jen databázi na sekundárním name serveru, pak by po stejné době oprava zmizela!). Problém nastane v případě, že

uživatel v době, kdy ještě není sekundární name server aktualizován, dostane první odpověď od sekundárního name serveru. Ta je negativní, tj. takový počítač v databázi není.
Klasickou chybou je, že primární name server pracuje korektně, ale na sekundárním name serveru z nějakého důvodu nejsou data pro zónu. Klienti náhodně dostávají autoritativní odpovědi ze sekundárního name serveru či z primárního name serveru. Odpovědi z primárního name serveru správně překládají, kdežto odpovědi ze sekundárního name serveru jsou negativní (uživatelé pak říkají:
„jednou to jde a podruhé ne“).
Autoritativní data pocházejí z databází na disku. Je zde pouze jedna výjimka. Pro správnou činnost name serveru musí name server znát root name servery. Pro ty však není autoritou, přesto každý name server má na disku databázi informací o root serverech, kterou ale zavádí příkazem cache do sekundární paměti (není k nim autorita).
Na obr. 11.9 je překlad jména *abc.pipex.cz* na IP-adresu (nejedná se o forwarder nebo slave server):

Obr. 11.9
Překlad jména
abc.pipex.cz
na IP-adresu



Resolver zformuluje požadavek na name server a očekává jednoznačnou odpověď. Umí-li nameserver odpovědět, pak obratem zašle odpověď. Odpověď hledá ve své cache paměti (*5*). Tam jsou, jak autoritativní data z databází na disku, tak i neautoritativní data získaná při předešlých řešeních. Nezná-li server odpověď, pak kontaktuje další servery. Vždy začíná root name serverem.
Nezná-li name server přímo odpověď, pak kontaktuje root name server, proto každý name server musí znát IP-adresy root name serverů. Není-li však žádný root server dostupný (to je např. případ všech uzavřených sítí), pak po několika neúspěšných pokusech celý proces překladu zkolabuje.
Root name server zjistí, že informace o doméně cz delegoval větou typu NS name serveru nižší úrovně a zašle našemu name serveru IP-adresy serverů spravujících domény cz.
2. Name server se obrátí na server pro doménu cz, který však zjistí, že informace o doméně delegoval větou typu NS name serveru nižší úrovně a zašle našemu name serveru IP-adresy serverů spravujících doménu pipex.cz.
3. Náš server se tedy obrátí na server spravující doménu pipex.cz, který mu požadavek vyřeší (nebo ne). Výsledek předá klientovi.
4. Informace které postupně získal si též uloží do cache.
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

IP adresa

Protokol IP verze 4 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 IPadresu.
Je to podobné jako s adresou domu. Pokud má dům vchod ze dvou ulic, pak má i dům dvě adresy.
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 WWWservery 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:
1. Adresy (lokální) sítě.
2. Adresy počítače v (lokální) síti.

Problém je v tom jak zjistit, která část IP-adresy je adresou sítě a která adresou počítače. Není ani zcela jasné co to znamená slovo síť, protože jeho význam se postupně měnil a kromě slova síť se zavedly pojmy subsíť a supersíť. K tomu však musíme dospět postupně.
IP-adresa se dělí na adresu sítě a adresu počítače v rámci této sítě (viz obr. 6.1).
Kolik bajtů z IP-adresy tvoří adresu sítě určují počáteční bity prvního bajtu IP-adresy. IP-adresy se dělí do pěti tříd:

- ✓ **Třída A**, kde nevyšší bit prvního bajtu má hodnotu 0. Zbylých 7 bitů prvního bajtu tvoří adresu sítě a zbytek je určen pro adresu počítače v rámci sítě. V třídě A máme 126 sítí (0 a 127 mají zvláštní význam. V každé síti je 224-2 adres pro počítače (adresy tvořené samými nulami a samými jedničkami mají zvláštní význam).
- ✓ **Třída B**, kde nejvyšší dva bity prvního bajtu mají hodnotu 102. Zbylých 6 bitů a následující druhý bajt je určen pro adresy sítí. Můžeme tedy mít celkem 214 sítí a v každé síti 216-2 počítačů.
- ✓ **Třída C**, kde nevyšší tři bity prvního bajtu mají hodnotu 1102. Zbylých 5 bitů a následující dva bajty jsou určeny pro adresu sítě. Můžeme tedy mít 222 sítí a v každé síti 128-2 počítačů.
- ✓ **Třída D**, kde nejvyšší čtyři bity prvního bajtu mají hodnotu 11102. 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.

Jednotlivé třídy adres jsou shrnuty v tab. 6.1, kde s vyznačuje bity používané pro adresu sítě a

Tab. 6.1 Třídy IP-adres

Třída	1. bajt IP-adresy	2. bajt IP-adresy	3. bajt IP-adresy	4. bajt IP-adresy
A	0ssssss 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$_{10}$			

m bity používané pro adresný oběžník.
Z tabulky je dále patrné, že sítí třídy A může být celkem 128 – 2 = 126 a v každé může být 28+8+8= 16 M adres. Obdobně třídy B může být 14 K a každá může obsahovat až 64 K adres. A konečně sítí třídy C může být 2 M a každá může obsahovat až 256 adres. Některé adresy jsou však vyhrazeny pro speciální účely.
6.1.1 Speciální IP-adresy IP-adresa je obecně tvaru:
sí5.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". Jsouli tam naopak samé jedničky (11…1), pak se to vyjadřuje slovem „všichni" (či oběžník).Přehled speciálních adres ve dvojkové notaci je uveden v tab. 6.2.

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

Tab. 6.2 Speciální IP-adresy

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.

Obdobně lze příkazem ping (s TTL=1) zjistit, které počítače na LAN zpracovávají které adresné oběžníky.
Např:
ping 224.0.0.1

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
x 11111111.11111111.00000000.00000000

10101010.01010101.00000000.00000000

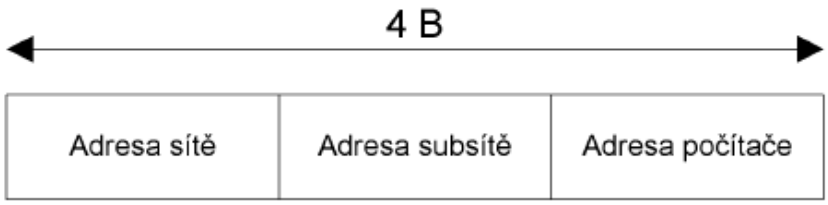
Výsledek převedeme do desítkové soustavy a zjistíme, že počítač leží na síti 170.85.0.0.
Tato metoda určení adresy sítě se může zdát až příliš komplikovanou v případě, že se používají standardní síťové masky. Může se zdát, že síťová maska je důležitá tak pro tvůrce operačního systému, nikoliv však pro správce. Význam síťové masky doceníme v následující historické epoše.

Síť – historická epocha II

V roce 1993 vyšly normy RFC-1517 až 1520. Tyto dnes již málo citované normy od základu změnily pohled na slovo síť jak je chápáno v Internetu. Přestalo se na sítě hledět přes třídy, ale výhradně přes sí-
;ové masky.
Jenže ono úplně nejde abstrahovat od sítí, takže v podstatě dělení IP-adresy na adresu sítě a adresu počítače
zůstalo, pouze část IP-adresy dříve odpovídající adrese počítače se rozdělila na dvě části: na adresu

subsítě a adresu počítače.

Obr 6.2
Struktura IP-adresy



Z hlediska síťové masky je adresa sítě i subsítě jeden celek. Ta část IP-adresy, kde jsou v masce jedničky je prostě síť. Jenže nyní dochází k nejednoznačnosti v terminologii. Jednou slovo síť označuje ve smyslu třídy (A, B, nebo C) a podruhé je sítí myšleno obecně část IP-adresy, kde v odpovídající masce jsou jedničky. Pokud na čas zapomeneme na třídy a budeme používat libovolné masky, pak už nestačí mluvit o síti např. 192.168.0.0 ale vždy k ní musíme dopsat masku, abychom vyjádřili co touto sítí míníme. Pokud bychom uvažovali třídně, pak se pro tuto síť použije vždy maska 255.255.255.0, protože se jedná o síť třídy C. Maska 255.255.255.0 pro síť 192.168.0.0 se nazývá standardní síťovou maskou.
Kromě subsítí se používají i supersítě, u kterých je počet jedniček masky menší než u standardní síťové masky.
Jako příklad je v tab. 6.3 uvedeno dělení sítě 192.168.0.0 na subsítě s různými maskami (standardní maska je zobrazena tučně).
Adresy s maskami majícími méně jedniček než je standardní maska se nazývají adresy supersítí (v tabulce nahoře) a adresy s maskami o více jedničkách než má standardní maska se nazývají adresy subsítí (dolní část tabulky).
Jelikož dvojkové vyjádření síťové masky je tvořeno zprava souvislou řadou jedniček, tak se místo vyjádření „síť 192.168.0.0 s maskou 255.255.255.252" častěji zkrácuje na 192.168.0.0/30, kde číslo 30 vyjadřuje počet jedniček masky.
Už slyším jak se čtenář čílí, proč je maska tvořena souvislou řadou jedniček. Ano teoreticky to tak být nemusí, je to jen nepsané pravidlo, ale docela dobré pravidlo.
Vezměte si např. sí5 192.168.0.0 s maskou 255.255.255.95. 95 je binárně 01011111, tj. k dispozici jsou změny na místech x1x11111, takže adresa sítě je 00000000 (desítkově 0), adresy pro počítače jsou 00100000 (desítkově 32) a 10000000 (desítkově 128) a oběžník je 10100000 což je desítkově 160. Těžko řešitelným problémem je pak mezi tyto adresy vložit další subsítě.
Myslíte, že byste takovou sí5 chtěli spravovat? Pointa spočívá v tom, že většina softwaru takové sítě i podporuje.

Obr 6.2

Struktura IP-adresy

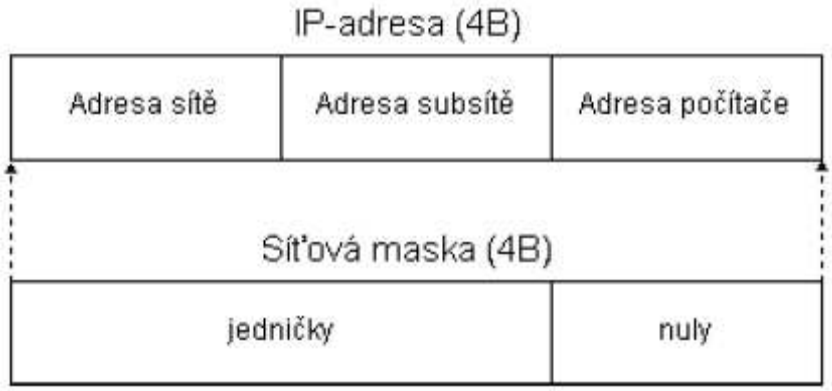
Maska	Počet jedniček v masce (zleva)	Síť je tvořena intervalem IP-adres	Zkrácený zápis sítě (včetně masky)
255.248.0.0	13	192.168.0.0 až 192.175.255.255	192.168.0.0/13
255.252.0.0	14	192.168.0.0 až 192.171.255.255	192.168.0.0/14
255.254.0.0	15	192.168.0.0 až 192.169.255.255	192.168.0.0/15
255.255.0.0	16	192.168.0.0 až 192.168.255.255	192.168.0.0/16
255.255.248.0	21	192.168.0.0 až 192.168.7.255	192.168.0.0/21
255.255.252.0	22	192.168.0.0 až 192.168.3.255	192.168.0.0/22
255.255.254.0	23	192.168.0.0 až 192.168.1.255	192.168.0.0/23
255.255.255.0	24	192.168.0.0 až 192.168.0.255	192.168.0.0/24
255.255.255.128	25	192.168.0.0 až 192.168.0.127	192.168.0.0/25
255.255.255.192	26	192.168.0.0 až 192.168.0.63	192.168.0.0/26
255.255.255.224	27	192.168.0.0 až 192.168.0.31	192.168.0.0/27
255.255.255.240	28	192.168.0.0 až 192.168.0.15	192.168.0.0/28
255.255.255.248	29	192.168.0.0 až 192.168.0.7	192.168.0.0/29
255.255.255.252	30	192.168.0.0 až 192.168.0.3	192.168.0.0/30
255.255.255.254	31	192.168.0.0 až 192.168.0.1 Pozor, takováto síť je nesmysl, protože má jen dvě IP-adresy, tedy adresu sítě samotné a adresu oběžníku, nedostávají se už adresy pro počítače na této síti.	192.168.0.0/31
255.255.255.255	32	Adresa samostatného počítače (host address) 192.168.0.0	192.168.0.0/32

Tab. 6.3 Příklad dělení sítě 192.168.0.0 na subsítě

Subsítě

Síťová maska nerozlišuje mezi částí IP-adresy určené pro síť a pro subsíť.

Obr. 6.3 IP-adresa a její síťová maska



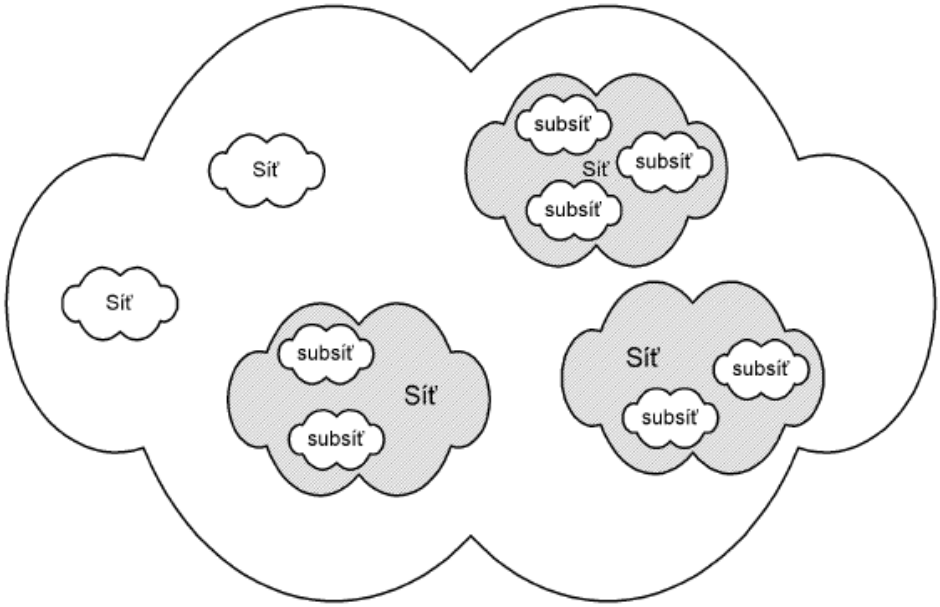
Používají se také vyhrazené adresy – viz tab. 6.4.

síť.subsíť.00…0	Adresa subsítě jako takové
síť.00…0.00…0	Adresa sítě
síť.subsíť.11…1	Oběžník na subsíti
síť.11…1.11…1	Pozor, toto je oběžník pro všechny subsítě dané sítě

Tab. 6.4 Speciální adresy

Problém je pochopitelně se subsítí, která má na místě pro subsíť nuly, pak se těžko rozlišuje mezi adresou sítě a subsítě. Rovněž u případu, kdy na místě pro subsíť jsou samé jedničky je nejednoznačnost, zdali oběžník je oběžníkem na subsíť nebo na všechny subsítě. Proto se tyto subsítě snažíme nepoužívat.
Mnohý software takové subsítě vůbec nepodporuje, jiný software je v případě použití takovýchto subsítí třeba speciálně konfigurovat.
Avšak oběžník na všechny subsítě dané sítě je stejně jen teorie. Nesetkal jsem se s případem, že by to šlo využít, protože směrovač nemá informaci na jaké subsítě je vzdálená síť dělena.
Subsítě se používají v rámci firem na konfiguraci jednotlivých lokálních sítí. Vzhledem k nedostatku IP adres má dnes většina firmem přidělenu jen subsíť sítě třídy C. Tuto subsíť si pak dělí na ještě menší subsítě. Dokonce se firmám přidělují jen subsítě sítě třídy C a ty si firmy drobí na menší subsítě.
Subsíť je část Internetu odpovídající jedné firmě nebo části firmy.

Obr. 6.4
Internet je tvořen sítěmi, sítě se mohou dělit na subsítě



Prakticky: Mám za úkol připojit firmu k Internetu. Získal jsem adresu třídy C (např. 194.149.115.0 desítkově,
tj. 11000010.10010101.1110011.00000000 dvojkově), která má standardní síťovou masku 255.255.255.0. Měl jsem tedy štěstí, že jsem dostal celou adresu třídy C. Problém je v tom, že můj podnik má složitější strukturu – jeho síť se skládá z řady menších lokálních sítí (LAN) a řady sériových linek propojujících tyto LAN. Je tedy nutné rozdělit přidělenou síť na subsítě.
Navenek se pochopitelně bude celý podnik tvářit jako jedna síť se standardní maskou.
Vzhledem k tomu, že první tři bajty přidělené IP-adresy zůstávají stále stejné, budu v dalších úvahách psát jen posledním bajt v IP-adrese (první tři bajty jsou konstantně např. 194.149.115).
Pro rozdělení sítě na subsítě se na první pohled naskýtá možnost nepoužít standardní síťovou masku pro adresu třídy C, tj. 255.255.255.0, ale např. nestandardní ale **konstantní sí3ovou masku**
255.255.255.240 (dvojkově 11111111.11111111.11111111.11110000 – všimněte si, že první polovina posledního bajtu slouží pro adresu subsítě), která nám umožní rozdělit přidělenou adresu třídy C na 16 subsítí a každá subsíť může mít 16 adres.

Subsíť dvojkově (poslední bajt z IP-adresy 194.149.115.0)	Síťová maska (dvojkově)	Adresa subsítě (desítkově)	Síťová maska (desítkově)	Max. počet počítačů v subsíti (bez adresy subsítě a oběžníku)
00000000 až 00001111	11110000	.0	.240	0 (nejednoznačná subsíť)
00010000 až 00011111		.16		14
00100000 až 00101111		.32		14
00110000 až 00111111		.48		14
01000000 až 01001111		.64		14
01010000 až 01011111		.80		14
01100000 až 01100000		.96		14
01110000 až 01111111		.112		14
10000000 až 10001111		.128		14
10010000 až 10011111		.144		14
10100000 až 10101111		.160		14
10110000 až 10111111		.176		14
11000000 až 11001111		.192		14
11010000 až 11011111		.208		14
11100000 až 11101111		.224		14
11110000 až 11111111		.240		0 (nejednoznačná subsíť)

Tab. 6.5 Konstantní síťová maska

Každá subsíť má 16 adres, ale použitelných je pouze 14, protože dvě adresy mají speciální význam. Samé nuly označují adresu subsítě a samé jedničky oběžník na subsíti. Např. adresa 194.149.115.32 označuje „třetí“ subsíť jako takovou a adresa 194.149.115.47 oběžník na této subsíti (194.149.115.255 je oběžník na síti 194.149.155.0 jako takové). Přidělovat je tedy možné na subsíti 194.149.115.32 pouze adresy 194.149.155.33 až 46.
Druhým problémem je, že není jednoznačně určeno, zdali 194.149.155.255 je oběžník pro všechny subsítě sítě 194.149.155.0 nebo jen na subsíti 194.149.115.240. Proto se poslední subsíť zpravidla nepoužívá. Podobným problémem je kolize při určení adresy sítě a subsítě 194.149.115.0. Proto se též první subsíť zpravidla nepoužívá.
V praxi často nepotřebujeme rozdělit přidělenou adresu na stejné části. Např. pro sériové linky je 14 adres na subsíť zbytečný luxus a naopak pro mnohé LAN je to nedostatečné. Pro rozdělení sítě na různě dlouhé subsítě používáme **variabilní síťovou masku**. Např. viz tab.

6.6.

Subsíť dvojkově (poslední bajt)	Síťová maska (dvojkově)	Adresa subsítě (desítkově) 194.149.115.	Síťová maska (desítkově)	Max. počet počítačů v subsíti (bez adresy subsítě a oběžníku)
00000000 až 00000011	11111100	.0	.252	0 (nejednoznačná subsíť)
00000100 až 00000111	11111100	.4/30	.252	2
00001000 až 00001111	11111000	.8/29	.248	6
00010000 až 00011111	11110000	.16/28	.240	14
00100000 až 00111111	11100000	.32/27	.224	30
01000000 až 01111111	11000000	.64/26	.192	62
10000000 až 10111111	11000000	.128/26	.192	62
11000000 až 11011111	11100000	.192/27	.224	30
11100000 až 11101111	11110000	.224/28	.240	14
11110000 až 11100011	11111000	.240/29	.248	6
11111000 až 11111011	11111100	.248/30	.252	2
11111100 až 11111111	11111100	.252/30	.252	0 (nejednoznačná subsíť)

Tab. 6.6 Variabilní síťová maska

Z předchozí tabulky je vidět, že nejdelší subsíť má 64 prvků, potřebujeme-li na jednu LAN více jak 62 rozhraní, pak je dobré použít celou adresu třídy C.
Nyní si můžeme dát nový příklad. Určete adresu sítě, na které leží počítač o IP-adrese 10.0.0.239 používámeli síťovou masku 255.255.255.240.
IP-adresu i masku převedeme do dvojkové soustavy a bit po bitu vynásobíme:

```
        00001010.00000000.00000000.11101111 tj. 10.0.0.239
x       11111111.11111111.11111111.11110000 tj. 255.255.255.240
        -----------------------------------
        00001010.00000000.00000000.11100000 - 10.0.0.224
```

Adresa leží na síti 10.0.0.224. Ale může to být adresa počítače? Ne. Proč? Oddělíme adresu sítě a adresu počítače:

```
00001010.00000000.0000000.1110|1111
          <-------síť------->|<poč>
```

adresa je tvaru síť.jedničky, nejedná se tedy o adresu počítače, ale o adresu oběžníku na síti 10.0.0.224.
Podobně jako u sítí je možné poslat příkazem ping všeobecný oběžník, tak i v našem případě:
ping 10.0.0.224
zjistí zdali na subsíti je nějaký počítač „živý" a UNIXové implementace příkazu ping nám sdělí které počítače na subsíti jsou „živé".

Supersítě, autonomní systémy
Zatímco subsítě se používají na LAN, tj. používají se v konfiguraci jednotlivých síťových rozhraní (síťových karet), tak supersítě se používají pro agregace IP-adres. Agregace IP-adres je výhodná pro směrování a pro administrativu při přidělování IP-adres.
V současné době je při pohledu z velké vzdálenosti (z Měsíce) Internet soustavou vzájemně propojených poskytovatelů Internetu. Poskytovatel Internetu (*provider*) poskytuje připojení k Internetu bu1 pro komerční nebo nekomerční účely. Kromě poskytovatelů tvoří Internet ještě několik organizací, které se zabývají správou a vývojem v této oblasti, avšak ze síťového hlediska se od poskytovatelů neliší.
Poskytovatelé dopravují IP-datagramy bu1 v rámci sebe nebo mezi sebou. Dva poskytovatelé si mohou vyměňovat IP-datagramy mezi sebou, existují však i tranzitní poskytovatelé, kteří přes sebe IP-datagramy tranzitují.

Neříká se, že se Internet dělí na poskytovatele, ale z hlediska dopravy IP-datagramů se Internet dělí na autonomní systémy. Každý poskytovatel má pak přidělen jeden nebo více autonomních systémů. Autonomní systém je reprezentován dvoubajtovým číslem.
Internet je tedy z hlediska směrování (tj. dopravy IP-paketů) rozdělen na autonomní systémy (AS). Pro směrování mezi AS se dříve používal protokol EGP, nyní se však masově přechází k protokolu BGP verze 4.
Poskytovatelé Internetu jsou správci autonomního systému. Správci AS žádají o intervaly IP-adres, které přidělují sobě a svým zákazníkům. Jednotliví poskytovatelé jsou pak i se svými zákazníky součástí konkrétního AS. V kapitole o administrativní stránce věci se dozvíme, že problém je ještě složitější, že o přidělení IP-adresy žádají tzv. lokální Internet Registry, kteří mohou mít svůj vlastní AS nebo mohou sdílet AS s někým dalším.
Proč je snaha v rámci autonomního systému používat intervaly adres? Důvod je prostý. Interval adres je možné agregovat do jedné adresy supersítě. Ve směrových tabulkách směrovačů vzdálených autonomních systémů může celý interval adres vystupovat jako jedna položka, čímž se šetří pamě; směrovače a zjednodušuje se správa.
Agregace je jednoduchá. Např. je-li přidělen interval adres sítí 194.149.96.0 až 194.149.128.0, pak je možné jej agregovat na adresu supersítě 194.149.96.0 se síťovou maskou 255.255.224.0. Častěji se však píše adresa 194.149.96.0/19 (maska 255.255.224.0 je tvořena 19 jedničkami).
Zatímco při dělení sítě na subsítě obsahovala maska více jedniček, tak při agregaci je tomu naopak, ale princip je týž. O agregovaných sítích se hovoří jako o supersítích. Z pohledu vzdáleného AS se supersí ; jeví jako jeden celek. Pro správce AS je síť jeden celek. A pro správce sítě jsou zase jednotlivými celky subsítě.
Problém ale spočívá v tom, když firma přejde od jednoho poskytovatele Internetu k jinému, který je navíc v jiném autonomním systému. Pak musí od nového poskytovatele získat nové IP-adresy a následně všechny používané sítě přečíslovat. Jména počítačů (tj. i e-mailová adresa) však mohou zůstat zachovány.

VP strana 173