INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ
TENTO PROJEKT JE SPOLUFINANCOVÁN EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY.

Průvodka dokumentem Počítačové sítě 1:
- nadpisy tří úrovní (pomocí stylů Nadpis 1–3), před nimi je znak # OK
- na začátku dokumentu je automatický obsah (#Obsah) OK
- obrázky vynechány, zůstávají pouze původní popisky vložené mezi znaky @...&
- dodatečný komentář editora vložen mezi znaky §...&
- tabulky jsou v textu pouze symetrické, vloženy mezi znaky @...&
- tučné písmo vloženo mezi znaky $...$
- jiné řezy než tučné písmo se v textu nepoužívají
- průvodce studiem a další informace pro studenty: vloženo mezi znaky ~...&
- znakem # je kromě nadpisů označen také začátek korespondenčních úkolů a kontrolních otázek. Taková sekce končí znakem &.
- POZOR: znak & (ampersand) se na několika místech vyskytuje v textu jako významotvorný znak, nikoli jako značka konce sekce (např. tabulky). V těchto případech vždy stojí mezi dvěma alfanumerickými znaky, není tedy bezprostředně před ním ani za ním mezera ani konec řádku.

Tomáš Sochor
Počítačové sítě 1
Studijní opora k inovovanému předmětu: *Počítačové sítě 1*
Ostrava, únor 2013
ISBN 978-80-7464-269-2

#Obsah

~Průvodce studiem

Cíle kurzu:

Cílem tohoto kurzu je seznámit studenta se základními pojmy z oboru počítačových sítí a principy jejich fungování s důrazem na nejrozšířenější přenosové technologie, zejména Ethernet a IEEE 802.11 včetně jejich moderních variant.

Tyto cíle budou splněny prostřednictvím konkrétních cílů specifikovaných v jednotlivých kapitolách.

K jejich splnění Vám pomohou kurzívou psané části označené ikonou kompasu nazvané Průvodce studiem, kde se dozvíte, kolik času budete přibližně potřebovat na zvládnutí jednotlivých kapitol.

Slušelo by se zde na úvod uvést i celkový čas potřebný ke zvládnutí celého modulu. Sečtením časových požadavků jednotlivých kapitol můžete zjistit, že celý modul lze zvládnout přibližně za 16 hodin intenzivního studia. Je však třeba to považovat za údaj s nízkou vypovídací hodnotou. Je nutné brát v úvahu, že především pro ty z Vás, kteří dosud máte s praktickým využíváním počítačových sítí malou nebo žádnou zkušenost, bude látka náročná, a rozhodně nelze plánovat zvládnutí např. jedné kapitoly denně, natož pak více.

Za optimální bych v takovém případě považoval rozvržení studia nejméně do 2- 4 týdnů, pokud možno do delšího období, abyste měli čas na přestávky umožňující lepší promyšlení látky.

Kurz by měl být vždy absolvován za podpory tutora, který je dostatečně erudovaný v oboru počítačových sítí, a který bude nejen hodnotit korespondenční úkoly, ale také bude studentům nápomocen při porozumění obtížnějším pasážím problematiky.

Tomáš Sochor, autor kurzu&

#1 Počítačové sítě – úvod

$Co se dozvíte v této kapitole:$

1. Co je výpočetní model a čím je důležitý pro problematiku počítačových sítí?
2. Jaké jsou hlavní výpočetní modely, které se dnes v počítačových sítích používají?
3. Podle jakých kritérií a na jaké kategorie se počítačové sítě dělí?

$Po prostudování této kapitoly byste měli být schopni:$

1. Charakterizovat nejvýznamnější počítačové modely (host/terminál, pracovní stanice/souborový server, klient/server).
2. Uvést přednosti a nedostatky jednotlivých výpočetních modelů.
3. Znát význam nejdůležitějších kategorií počítačových sítí zejména podle rozsahu (LAN, WAN), podle funkčního postavení uzlů v síti (peer-to-peer, serverová síť).

$Klíčová slova této kapitoly:$

Výpočetní model, host/terminál, pracovní stanice/souborový server, klient/server, síť lokální (LAN), síť rozlehlá (WAN), server, klient, síť peer-to-peer, serverová síť.

~Doba potřebná ke studiu: 2 hodiny&

~Průvodce studiem

Studium této kapitoly je poměrně náročné zejména pro ty z Vás, kteří dosud nemají s prací v počítačových sítích žádnou praxi. V takovém případě Vám zřejmě některé pojmy budou připadat obtížně pochopitelné, ovšem nenechte se tím odradit, potřebné souvislosti vyplynou z látky probírané v dalších kapitolách.
Na studium první části pojednávající o výpočetních modelech si vyhraďte zhruba 2 hodiny. Po jejím prostudování doporučujeme dát si pauzu, třeba do druhého dne, a pak se pusťte do druhé části kapitoly. Její prostudování včetně odpovědí na korespondenční otázky by Vám nemělo trvat déle než 2,5 hodiny, někteří jej zvládnou i za méně než 2 hodiny.&

#1.1 Úvod do počítačových sítí

Na úvod si vymezíme předmět zkoumání, byť se zdá na první pohled zřejmý. Za počítačovou síť budeme považovat takovou množinu samostatných počítačů (tedy počítačů, které mohou fungovat i bez připojení do sítě), které jsou navzájem propojeny, a komunikují spolu (nebo alespoň mohou). Tato komunikace mezi počítači je zásadní charakteristikou, proto ji zdůrazňujeme.

Přitom je vhodné zdůraznit jednu skutečnost: počítače tvořící počítačovou síť, musí být navzájem nezávislé, tedy mohou mít navzájem zcela odlišný hardware, operační systém apod. To, co je spojuje, je komunikace v síti. Přitom nijak nevymezujeme, jakým způsobem mají být počítače propojeny, může se tedy jednat o počítače propojené na krátkou vzdálenost třeba Ethernetovým UTP kabelem, ale i počítače propojené na tisíce kilometrů třeba satelitním propojením.

V dalších částech práce se budeme věnovat různým aspektům počítačových sítí, od způsobu fyzického propojení jednotlivých součástí sítě (počítačů, propojovacích prvků apod.) po síťové aplikace, např. world wide web (www).

#1.2 Klasifikace počítačových sítí

Jak jsme uvedli v předchozí kapitole, potřeba řešení lokálních úloh bez použití jediného ústředního počítače vedla ke vzniku tzv. *počítačových sítí*, které umožňují uživatelům pracovat v síti i samostatně. Rozvoj počítačových sítí umocnilo též prudké nasazení počítačů řady PC v komerční sféře, což se projevilo prudkým rozvojem sítí lokálních sítí (LAN) v této oblasti v nejrůznějších typech organizací (úřady, školy, obchody, podniky).

Abychom mohli počítačové sítě charakterizovat, je nutné mít k dispozici členění podle různých kritérií. Nejobvyklejšími používanými kritérii jsou dosah sítě, architektura sítě, role (postavení) uzlů sítě, účel, kterému síť slouží, vlastnické vztahy k síti a jejím jednotlivým částem, použité přenosové techniky, použité přenosové technologie, použitá přenosová média, mobilita uživatelů apod.

Všechna tato kritéria nemusí být exaktně definována, ani výsledné kategorie nemusí být přesně vymezeny, hranice mezi nimi nemusí být ostré a konkrétní klasifikace může mít i subjektivní složku, neboť výsledné kategorie mnohdy nejsou vzájemně zcela disjunktní. Výsledné kategorie představující dělení podle různých kritérií se mohou vzájemně prolínat, jedna a tatáž síť může patřit do různých kategorií současně (při uvážení různých kritérií). Pokusme se nyní objasnit některá kritéria.

#1.2.1 Dělení sítí dle rozsahu

Počítačové sítě rozdělujeme podle územního rozsahu obvykle do tří skupin :

1. $**WAN$** (Wide Area Network) – obvykle jsou představiteli této kategorie veřejné datové sítě
2. $**LAN$** (Local Area Network) - lokální počítačové sítě

WAN – rozsáhlé sítě nemají definovaný maximální rozsah, přičemž mohou zabírat území měst, států či jejich částí, nebo i celých kontinentů.

LAN - lokální sítě pokrývají území nepřesahující 1 - 2 km. Tedy svým nasazením pokrývají rozsah pracovišť, budov, závodů.

Dříve existoval i jakýsi mezistupeň zvaný městské sítě (MAN – Metropolitan Area Network), ale protože nebyl charakteristický žádným výrazným specifickým rysem a technologie určené pro tento segment se neprosadily, mnozí autoři jej vůbec neuvádějí a zahrnují jej převážně pod sítě WAN.

Máme tedy 2 výrazněji odlišné kategorie sítí, LAN a WAN. Jejich odlišnosti shrnuje následující tabulka 1.

@Tabulka 1: Porovnání LAN a WAN sítí

Charakteristika	LAN	WAN
primární účel	sdílení dat/zařízení	předávání dat aplikacemi (e-mail, IM, www apod.)
topologie	pravidelná (strom, příp. s redundantními spojeními	nepravidelná (polygon), vzniklý jako postupně se doplňující množina ad-hoc 2-bodových spojů
charakter a dostupnost uzlů	převažují stanice – dostupnost dle potřeba, ne trvale	převažují servery – dostupnost trvale
přenosová rychlost	typicky 100 Mb/s, páteřní spoje 1-10 Gb/s	typicky 1 – 100 Mb/s dle požadavků, v páteřních částech více
přenosové zpoždění (latence)	nízká (v řádech do 1 ms)	vyšší (často i stovky ms)

&
Hranice mezi LAN a WAN není ostrá a rozdíly mají tendenci se stále zmenšovat, což se projevuje např. v tom, že sítě LAN se zvětšují a sítě WAN se zrychlují. Je zřetelný trend neustálého zmenšování rozdílu mezi oběma kategoriemi sítí. V blízké budoucnosti bude zřejmě uživateli jedno, zda pracuje v síti LAN či WAN, všude bude mít stejné služby a bude používat stejný styl práce a tím si nebude muset uvědomovat rozdíl mezi LAN a WAN.

Vedle těchto „tradičních" kategorií počítačových sítí v posledních letech vznikal ještě další kategorie počítačových sítí, označovaná jako $**PAN$** (Personal Area Network) neboli osobní sítě. Tyto sítě jsou specifické následujícími rysy:

- Síť PAN propojuje více zařízení majících rysy samostatného počítače (např. PC, notebook, PDA, smartphone neboli mobilní telefon s operačním systémem) apod. na velmi krátkou vzdálenost (do 10 metrů), přičemž všechna zařízení v PAN zpravidla používá stejný uživatel. této síti mohou být i sdílené periferie, např. tiskárny, síťové disky (NAS) apod. Požadavek propojení alespoň 2 autonomních zařízení s vlastním OS je zde uveden proto aby bylo možné opravdu mluvit o skutečné síti počítačů, nikoli jen o síti připojujících k 1 počítači více nesamostatných periferií.
- PAN síť pracuje v režimu ad-hoc, tedy vzniká a zaniká (resp. aktivuje se a dezaktivuje, proto že samotný vznik často vyžaduje nějakou počítační konfiguraci, např. v případě Bluetooth tzv. spárování zařízení) dle potřeby. V případě použití bezdrátové technologie se může PAN aktivovat samotným přiblížením zařízení do vzájemného dosahu signálu.
- V PAN se používají specifické přenosové technologie pro přenos dat, jako Bluetooth, případně IrDA pro bezdrátové propojení, nebo USB či FireWire pro kabelové propojení. Méně často může taková síŤ využívat technologií používaných pro běžné LAN, tedy zejména IEEE802.11 (tzv. WiFi), případně Ethernetu.

Sítě PAN se také někdy označují méně častým termínem *piconet*.

#1.2.2 Dělení dle technologií

Dnes existují přenosové technologie, které jsou buď vhodné jen pro LAN (např. Novell IPX/SPX), nebo vhodné jen pro WAN (např. X.25), ale také technologie vhodné pro LAN i WAN (TCP/IP, ATM). Je tomu proto, že některé technologie vycházejí z určitých předpokladů, např. krátké přenosové zpoždění (IPX/SPX), nebo nespolehlivost přenosových cest (X.25). Vzhledem k tomu, že v dnešní době převládá prakticky ve všech sítích protokolová sada TCP/IP, má dnes používání technologického kritéria spíše okrajový význam, neboť většina sítí je nyní založena na protokolové sadě TCP/IP.

#1.2.3 Dělení sítí dle role uzlů

Jiné kritérium dělení sítí je dle postavení (role) uzlů. Zde jde o to, zda uzel sítě pouze nabízí své vlastní zdroje k využití ostatním uzlům, formou sdílení (chová se jako server), nebo pouze využívá zdroje ostatních uzlů, prostřednictvím sdílení (chová se jako klient), a nebo nabízí vlastní zdroje a současně využívá zdroje jiných uzlů (chová se současně jako klient i server). Pokud v síti převažuje současné využívání i nabízení, jde o síť typu peer-to-peer, kde postavení uzlů je zde symetrické a uzly komunikují jako „rovný s rovným". Pokud existuje ostrá hranice mezi nabízením a využíváním prostředků, jde o síť serverového typu, kde je postavení uzlů asymetrické, některé uzly se chovají pouze či převážně jako klienti, jiné pouze jako servery.

Srovnání je zřejmé z následující tabulky 2.

@Tabulka 2: Porovnání serverových sítí a peer-to-peer.

Charakteristika	síť peer-to-peer	serverová síť
uzly v síti	rovnoprávné postavení	část určena k poskytování služeb

		(servery), zbytek smí služby jen využívat
rozložení sdílených zdrojů v síti	kdekoli v síti	centralizováno na několika málo místech
TCO[1]	nulové náklady na pořízení, základní správa jednoduchá, ale nejsou k dispozici žádné nástroje pro správu. V rozsáhlejší síti obtížné na správu.	Licence serverového OS (obvykle placená). Následná správa je díky nástrojům obsaženým v licenci serverového OS výrazně snazší
Doporučené velikost	5 – 10 počítačů	od cca 5 počítačů výše

&

Uvedené dělení se týká hlavně lokálních sítí, přičemž i zde se rozdíly poněkud zmenšují. Obě tyto kategorie v lokálních sítích často splývají především proto, že častá je kombinace obou přístupů, např. v síti řídí server přihlašování uživatelů, přidělování přístupových oprávnění a přístup k centralizovaným prostředkům, zatímco prostředky pro vytváření sítí peer-to-peer se může řídit např. přístup k méně významným síťovým prostředkům lokálního dosahu. Typickým využitím je např. sdílení malé tiskárny v rámci více uživatelů v jedné místnosti, neboť její sdílení přes centrální tiskový server, ač je v principu také možné, by bylo k mnoha důvodů zbytečně těžkopádné (např. odstavení z nabídky v případě odpojení tiskárny, zabránění odeslání tisku na tuto tiskárnu jiným uživatelem mimo uživatelů dané místnosti apod.

#1.2.4 Dělení sítí dle vlastnictví

Další používaným kritériem klasifikace je vztah k vlastnictví sítě. Zde je třeba uvažovat brát v úvahu, kdo je vlastníkem sítě jako celku, kdo je faktickým provozovatelem sítě, kdo je uživatelem sítě, komu smí být služby sítě poskytovány a jaké služby jsou poskytovány. Z těchto hledisek existují sítě privátní a veřejné, někdy lze též najít sítě tzv. poloprivátní, a lze sem zařadit dále též virtuální privátní sítě.

U $**privátní počítačové sítě**$ je vlastníkem, provozovatelem i uživatelem tentýž subjekt, i když některé části (např. přenosové trasy) mohou být pronajaty od jiných subjektů a ten, kdo síť vybudoval a uvedl do provozu, může být jiný subjekt (např. externí dodavatel).

U $**veřejné sítě**$ je vlastníkem i provozovatelem sítě určitý (stejný) subjekt, který sám není uživatelem své sítě. Vlastními uživateli veřejné sítě mohou být jiné subjekty. Služby sítě jsou poskytovány na komerčním principu, mohou být nabízeny zájemcům bez omezení (skutečně „veřejně“) a nabízené služby mají nejčastěji charakter pouhého přenosu dat. To je případ tzv. veřejných datových sítí, což jsou sítě, které poskytují pouze jistý druh propojení mezi 2 či více body s tím, že vlastník a provozovatel sítě zajistí pro zákazníka jisté specifikované služby této sítě, např. konektivitu pomocí protokolu IP? nebo jen prosté propojení 2 bodů specifikovanou fyzickou přenosovou cestou, např. optickým vláknem.

Lze se setkat i s jistým mezistupněm ve formě $**poloprivátní sítě**$, kdy vlastníkem i provozovatelem sítě je určitý (stejný) subjekt, který sám (typicky) není uživatelem své sítě. Uživateli mohou být jiné subjekty a služby sítě jsou jim poskytovány buď na komerčním principu, avšak jen určitému omezenému okruhu uživatelů (například jen vlastním zákazníkům). Důvodem pro poskytování služeb jen omezenému okruhu zájemců mohou být zejména obchodní strategie a záměr provozovatele, případně obtížnost či nemožnost získání licence či jiného oprávnění k veřejnému poskytování takové služby.

[1] TCO = Total Costs of Ownership (Celkové nákldy na vlastnictví. Jde o termín, který má zahrnovat jak náklady na pořízení, tak na následnou správu a údržbu.

$Virtuální privátní síť (VPN)$ je příbuzný pojem, který k výše uvedeným pojmům logicky patří. Jde o logicky samostatnou podsíť jiné sítě, typicky veřejné (datové) sítě. Technicky a provozně jde o součást „mateřské“ (veřejné) sítě, z pohledu uživatele jde však o samostatnou síť, protože její uživatel si může myslet, že síť (byť jde o podmnožinu rozsáhlejší sítě) je jen jeho a je mu plně k dispozici. Smyslem takového řešení je, že uživatel chce mít vlastní síť, ale nevyplatí se mu ji budovat a provozovat, neboť na to nemá lidi, znalosti, zázemí a je to pro něj takto výhodnější. Často se s tímto termínem setkáváme také jako označením technologických prostředků, které takovou virtuální síť umožňují vytvořit. VPN sítě se v dnešní době obvykle zřizují jako síť tzv. šifrovaných tunelů, které propojují jednotlivá pracoviště uživatele. Šifrování se nejčastěji děje pomocí protokolů IPSec nebo SSL (TLS).

#1.2.5 Dělení sítí dle použité přenosové techniky

Dalším kritériem dělení sítí je dle použité přenosové techniky. Základními (a na rozdíl od jiných klasifikací vzájemně neslučitelnými) přenosovými technikami jsou:

- přenos s přepojováním okruhů
- přenos s přepojováním paketů.

Základní způsoby přenosu lze porovnat se známými komunikačními službami, listovní poštou a telefonní službou. $**Přepojování okruhů (circuit switching)**$ lze přirovnat k běžnému telefonování I zde totiž vzniká mezi příjemcem a odesilatelem přímá, souvislá cesta a komunikace probíhá v reálném čase. Představa je taková, že od odesilatele vede až k příjemci jednolitá nepřerušovaná „roura“, a přenášená data se tedy nikde nehromadí. Výhodou je, že každý přenášený blok dat nemusí být příjemci explicitně adresován. Příjemce dat je totiž jednoznačně určen již vložením datového bloku do příslušného přenosového kanálu (je jím ten, kdo je na druhém konci „roury“). Jedná se o techniku, která existuje již nejméně od doby, kdy se začal používat telefon. Dosud se používá, převážně v telekomunikačních sítích. I přes několik technologických pokusů o jeho zavedení do počítačových sítí se tam nikdy významněji nerozšířil.

$Přepojování paketů (packet switching)$ je mnohem novější technika. Její základy se zrodily spolu se zárodky dnešního Internetu v 60. etech 20. století, a právě ARPANET byla síť, která měla ověřit provozuschopnost této koncepce ve větším měřítku. Přepojování paketů lze přirovnat k běžné listovní poště. Mezi příjemcem a odesilatelem nevzniká žádná souvislá vyhrazená cesta, na cestě od odesilatele k příjemci existují přestupní body, které si zásilku postupně předávají, a jsou schopny ji nakonec dopravit až k příjemci. Data jsou obvykle přenášena podle principu „store&forward“, kdy jednotlivé přestupní uzly nejprve přijmou celý přenášený blok dat, a teprve pak jej předají dál (nejde, a kvůli nutnému rozhodování na přepojovacích uzlech ani nemůže jít o přenos v reálném čase). Přenášená data musí být explicitně adresována (každý blok dat musí obsahovat úplnou a jednoznačnou identifikaci svého příjemce.

Metoda přepojování okruhů pochází ze „světa spojů“ (funguje tak většina telefonních sítí jako pro pevné telefony, tak pro telefony mobilní) a je výhodná pro „rovnoměrné“ přenosy např. pro multimediální formáty (živý zvuk a obraz). Používá se např. v sítích ISDN. Metoda přepojování paketů pochází ze „světa počítačů“ a je výhodná pro „nárazové“ přenosy, např. přenosy souborů a nevhodná pro zvuk a obraz. Takto fungují prakticky všechny sítě LAN i WAN.

#1.2.6 Virtuální lokální sítě (VLAN)

Na závěr první kapitoly se zmíníme o jednom důležitém a frekventovaném pojmu, totiž VLAN (virtuální síť LAN -Virtual LAN). Přestože jde o pojem, který logicky patří do poněkud jiné kategorie než pojmy dosud popsané, považuji za potřebné se o něm již zde zmínit.

Dokud se počítače zařazovaly do samostatných sítí, mezi kterými docházelo ke „směrování“, a příslušnost k dané síti byla dána fyzickým umístěním jednotlivých uzlů ve fyzicky různých sítích, nebylo sítí VLAN třeba. Potřeba pružnějšího uspořádání například (například ve větších kancelářských budovách obývaných více navzájem cizími organizacemi, které však často sdílejí jednu společnou kabeláž a dělí je třeba jen stěny mezi místnostmi) vyvolala potřebu vzniku tzv. virtuálních LAN. Dalším důvodem byl nástup bezdrátových technologií pro připojení do sítě (tzv. WiFi), kdy samozřejmě pojem fyzického napojení přenosového média do určitého síťového prvku nelze využít.

Při zavádění VLAN fyzické umístění počítačů nehraje roli, jejich zařazení do jednotlivých VLAN je logická záležitost a o zařazení do určité sítě rozhoduje správce pomocí nástrojů konfigurace síťových prvků. Představa VLAN je zobrazena na obr. 1, kde je znázorněna jedna fyzická síť v části budovy. Síť je tvořena 1 směrovačem (routerem) na chodbě a 3 přepínači (switchi) v rozích místností A, C a F, k nimž jsou připojeny koncové počítače. Pomocí barevných oválů rozlišených 3 barvami (zelená, červená, fialová) je znázorněna příslušnost počítačů do 3 logických skupin (odpovídajících např. různým firmám nebo oddělením). Takovéhoto rozdělení se dosahuje obvykle (statickým neboli ručním) přiřazením příslušných rozhraní switche do příslušné virtuální LAN. VLAN jsou identifikovány celými kladnými čísly (max. do 4096) a switche zajišťují, aby každý rámec, který se posílá ze switche jinému switchi, byl označen právě tímto číslem (obvykle pomocí tzv. tagování dle IEEE 802.1q). Na základě této identifikace rámce pak přijímající switch ví, že smí předat rámec pouze do takového segmentu, který náleží do stejné VLAN.

Pro mechanismus VLAN je podstatnou skutečností to, že mezi jednotlivými částmi sítě nebo na jejím „okraji“ musí být připojen jeden či více směrovačů (routerů), které zajistí korektní předávání informací mezi jednotlivými virtuálními LAN (kde je komunikace možná jen za splnění určitých podmínek podobně jako mezi zcela nezávislými sítěmi LAN.

@Obrázek 1: Virtuální sítě LAN.&
§Obrázek vynechán, popis obrázku v textu výše&

#Úkol k zamyšlení:

Pokuste se síť, se kterou pracujete v zaměstnání, ve škole či jinde, zařadit do skupin podle všech výše uvedených kritérií (např. síť lokální/rozlehlá, na bázi protokolové sady TCP/IP, serverového typu/peer-to-peer, privátní síť, …).&

#Korespondenční úkoly:

1. Několika (nejvýše 10) větami či heslovitě popište počítačovou síť, s kterou v praxi (ve svém zaměstnání, škole apod.) pracujete. Pokud je takových více, vyberte tu, se kterou pracujete nejčastěji (tu byste měli nejlépe znát). Pokud si nejste jisti svými vědomostmi o Vaší síti a máte možnost konzultace této otázky s Vaším správcem sítě, neváhejte ji využít!
2. Může jedna síť patřit zároveň do více kategorií (z hlediska jednoho kritéria dělení)? Uveďte na podporu svého tvrzení příklad z praxe.&

$Shrnutí obsahu kapitoly$

Úvodní kapitola Vás seznámila s nezbytnými základními pojmy, jejichž osvojení je nezbytné pro pochopení další látky. Z těchto pojmů zdůrazňujeme v následujícím odstavci několik nejdůležitějších. Ke každému pojmy byste měli být schopni přiřadit alespoň stručný popis.

$Pojmy k zapamatování$

- Sítě LAN, WAN, PAN
- Sítě s přepojováním paketů a sítě s přepojováním okruhů;
- Sítě peer-to-peer a sítě serverového typu;
- Sítě veřejné, privátní a VPN;
- Virtuální lokální sítě.

~Průvodce studiem

Pojmy uvedené ve shrnutí kapitoly výše jsou zcela zásadní pro pochopení látky v dalších kapitolách. Po dokončení studia kapitoly doporučujeme udělat si pauzu nejméně do druhého dne, a pak se vrátit ke shrnutí kapitoly. Pokud pocítíte, že jste některému z pojmů zde uvedených zcela neporozuměli, vraťte se k němu ještě předtím, než se pustíte do studia dalších kapitol.&

#2 Funkce sítí LAN

$V této kapitole se dozvíte:$

1. Jaké jsou hlavní důvody zřizování lokálních sítí?
2. Jaké druhy služeb mají uživatelé v sítích LAN k dispozici?

$Po jejím prostudování byste měli být schopni:$

1. Charakterizovat druhy služeb, které sítě LAN uživatelům poskytují.

$Klíčová slova této kapitoly:$

Sdílení dat, sdílení síťových prostředků.

~Doba potřebná ke studiu: 1/2 hodiny&

~Průvodce studiem

Cílem této kapitoly je seznámit studenty s hlavními funkcemi, které lokální sítě mohou poskytovat. Především se jedná o služby umožňující sdílení dat různého druhu, sdílení technických zařízení sítě (nejčastěji tiskáren), a různé komunikační služby.

Studium této kapitoly není příliš náročné. Na její studium by vám měla stačit přibližně 1 hodina, možná i méně.&

#2.1 Sítě LAN - úvod

Síť LAN je vlastně skupina počítačů, které jsou navzájem propojené tak, aby byla možná jejich vzájemná komunikace. Uživatelům mohou poskytovat následující služby:
1. Sdílení technických zařízení (např. síťových tiskáren, skenerů apod.) pomocí sítě.
2. Sdílení společných dat uložených v síti.
3. Obecné služby komunikace mezi uživateli nebo aplikacemi.

Sítě LAN poskytují svým uživatelům nejčastěji první dva druhy služeb. Kromě těchto služeb bývá nejvíc využívanou službou, která spadá do 3. kategorie, *elektronická pošta*, která umožňuje zasílat soubory jednotlivým uživatelům sítě. Její realizace může být v jednotlivých sítích odlišná.

#2.2 Sdílení technických zařízení pomocí sítě

Většina lokálních sítí (LAN) umožňuje používat uživatelům sítě (buď všem, nebo jen těm, kteří mají přiděleno příslušné oprávnění) společná (neboli sdílená) technická zařízení. Obvykle se jedná o velkokapacitní síťové disky (ať již fyzické, nebo logické), tiskárny, případně další speciální hardware. Tyto služby si vynutily především ekonomické důvody, neboť vlastník sítě obvykle usiluje o dosažení vhodného kompromisu mezi vysokou pořizovací cenou některých zařízení a potřebou jejich používání více účastníky.

Pokud je potřeba, aby např. 20 uživatelů v síti používalo velkoformátovou tiskárnu, pak je jak z hlediska pořizovacích nákladů, tak i z hlediska optimalizace provozních nákladů vhodnější pořídit jednu tiskárnu a umožnit její sdílení, namísto pořízení byť o něco levnější tiskárny každému ze 20 uživatelů.

$Příklad$

Na obrázku 2 je vyobrazeno schéma LAN sítě malé organizace. Předpokládejme, že počítač v místnosti E má připojenou tiskárnu, počítače v místnosti A nikoli. Dále nechť počítač v místnosti G má připojeno externí diskové pole. Pokud bude vhodně nakonfigurováno sdílení tiskárny i diskového pole, mohou mít uživatelé vybraných nebo všech počítačů v dané síti k dispozici jak službu tisku na tiskárnu připojenou k počítači v místnosti E, tak přístupu k diskovému poli připojenému k počítači v místnosti G, a v případě diskového pole se uživatelé ani nemusejí dovědět, kde je diskové pole umístěno (v případě tiskárny to z praktických důvodů vědět potřebují, aby si mohli vyzvedávat svoje vytištění dokumenty, neboť zde nepředpokládáme velkou tiskárnu s personalizovanými oddělenými zásobníky.

@Obrázek 2: Ilustrace LAN ke sdílení síťových zdrojů a dat&
§Obrázek vynechán, popis obrázku v textu výše&

#2.3 Sdílení společných dat

Zřejmě ještě důležitějším motivem pro zavedení počítačové sítě, než je úspora nákladů na nákup zařízení zmíněný v předchozí podkapitole, je možnost sdílení dat. Bez nějakého nástroje pro sdílení dat si většina dnešních uživatelů počítačů nedovede svou práci s počítačem představit. V prostředí organizací, ale i domácností hraje roli tento důvod bývá v poslední době nejčastějším důvodem budování počítačových sítí LAN, i když sdílení síťových zdrojů má rovněž velký význam. Všichni uživatelé sítě mohou v síti využívat a zpracovávat společná data. Tato služba se používá, jakmile potřebuje větší počet pracovníků přístup ke stejným datům. Takovýto případ je zmíněn i v příklad v předchozí podkapitole, kde je zmínka o přístupu ke sdílenému diskovému poli. V případě vhodné podpory ze strany operačních systémů lze docílit např. toho, že některé soubory uložené na diskovém poli (například soubory měsíčních účetních závěrek) budou moci číst všichni uživatelé sítě (případně jen jejich podmnožina), zatímco přístup k zápisu do souboru bude mít pouze jeden uživatel (vlastník souboru, např. účetní).

#2.4 Další komunikační služby

Jde o služby, které umožňují výměnu dat, například textových zpráv či přiložených souborů v případě elektronické pošty. Komunikační služby se liší podle jejich určení, například elektronická pošta umožňuje zaslání zprávy uživateli, aniž by adresát v současné době aktivně používal komunikační aplikaci. Jiné komunikační služby (např. aplikace typu Instant messaging, kam patří např. Skype a ICQ) naopak současnou aktivitu obou uživatelů předpokládají či přímo vyžadují. K dalším službám sítí lze zařadit například monitorování činnosti jiných uživatelů v síti, vzdálené řízení jiných počítačů po síti apod.

$Korespondenční úkol:$

Napište, které z funkcí počítačové sítě, které byly popsány v kapitole 2, nejčastěji používáte. Napište také , zda existují také takové funkce, které nevyužíváte vůbec. Pokud ano, proč?

$Shrnutí obsahu kapitoly$

Tato kapitola studenty seznamuje se základními službami, které obvykle poskytují lokální sítě. Z těchto služeb zdůrazňujeme na tomto místě především tyto:

- Sdílení dat, zpravidla ve formě souborů či adresářů;
- Sdílení zařízení, např. tiskáren;
- Komunikační služby různého druhu (elektronická pošta, monitorování jiných účastníků, vzdálené řízení apod.).

$Pojmy k zapamatování$

- server
- klient
- sdílení dat
- sdílení síťových prostředků

~Průvodce studiem

Studium 2. kapitoly nebylo zřejmě příliš náročné. Máte-li chuť a čas, můžete se hned pustit do další kapitoly, která na tuto kapitolu bezprostředně navazuje.&

#3 Aplikace a služby Internetu a TCP/IP

$Obsah kapitoly$

~Průvodce studiem

Tato kapitola popisuje jednotlivé standardní služby aplikační vrstvy protokolové sady TCP/IP. Seznámíte se se službami vzdáleného přihlašování, elektronické pošty, přenos sdílení souborů a služby zprostředkování informací WWW. Na závěr kapitoly se seznámíte s principem fungování systému DNS

Jde o nejnáročnější kapitolu celého kurzu, a osvojení principů v ní popisovaných je klíčem k pochopení fungování většiny služeb sítí TCP/IP a tedy i Internetu. Proto doporučuji vyhradit si na její studium dostatek času a věnovat mu potřebnou pozornost. Časový údaj uvedený níže je spíše minimální dobou, kterou budete na studium potřebovat.&

$V této kapitole se dozvíte:$

1. Jaké jsou vlastnosti aplikační vrstvy protokolové sady TCP/IP?
2. Jaké standardní služby jsou v aplikační vrstvě TCP/IP k dispozici?
3. Jaké jsou principy fungování a základní vlastnosti služby pro vzdálené přihlašování (telnet)?
4. Jaké jsou principy fungování a základní vlastnosti služby pro sdílení souborů (FTP)?
5. Jaké jsou principy fungování a základní vlastnosti služby elektronické pošty?
6. Jaké jsou principy fungování a základní vlastnosti služby WWW?
7. Jak funguje a k čemu slouží systém DNS?

$Po jejím prostudování byste měli být schopni:$

1. Charakterizovat vlastnosti služby telnet;
2. Charakterizovat vlastnosti služby FTP;
3. Charakterizovat vlastnosti služby elektronické pošty;
4. Charakterizovat vlastnosti služby WWW;
5. Charakterizovat účel a funkci systému DNS.

~Klíčová slova této kapitoly:

Vrstva aplikační, telnet, FTP, elektronická pošta, protokol SMTP, protokol POP3, st MIME, služba WWW, jazyk HTML, protokol http, systém DNS.

Doba potřebná ke studiu: 4 hodiny&

#3.1 Aplikace v Internetu, resp. TCP/IP

Aplikace v síťové architektuře TCP/IP jsou založeny na výpočetním modelu klient/server. Znamená to, že jejich funkce je rozdělena mezi klientskou část, která se zpravidla spouští na pracovní stanici, a serverovou část, která je v provozu na určitém konkrétním aplikačním serveru. Součástí aplikační vrstvy jsou pouze ty části aplikací, které jsou nutné pro fungování určité služby, nikoli však uživatelské rozhraní. V případě klientské části pro elektronickou poštu jsou součástí aplikační vrstvy funkce pro odesílání zpráv a jejich příjem, ne však např. funkce pro správu složek apod. Standardizovány jsou pochopitelně jen ty části aplikací, které jsou součástí aplikační vrstvy.

Na počátku vývoje protokolové sady TCP/IP (tedy v dobách počátků Internetu a jeho předchůdce ARPANETu) se používaly především 3 tyto typy aplikačních služeb:

- přenos souborů (pomocí protokolu FTP);
- vzdálené přihlašování (pomocí protokolu telnet);
- elektronická pošta.

Později se objevily i další aplikační služby, z nichž se do dnešní doby udrželo především sdílení souborů pomocí protokolu NFS a zejména dnes nejrozšířenější služba WWW (World Wide Web), často však vznikají další.

#3.2 Protokoly FTP

Pro práci se soubory (pro přenos souborů) ů se v protokolové sadě TCP/IP používá ponejvíce protokol FTP.

#3.2.1 Protokol FTP

Protokol FTP je jedním z nejstarších protokolů v protokolové sadě TCP/IP, neboť pochází dokonce ještě z období před vznikem protokolové sady TCP/IP. Byl používán již nad protokolem NCP, což byl, jak víme z 1. kapitoly, první protokol používaný v ARPANETu.

Vzhledem k tomu, že v době vzniku protokolu FTP byly mezi různými operačními systémy mnohem větší odlišnosti než dnes, se musel se všemi těmito odlišnostmi již od počátku FTP umět vyrovnat. Příkladem takové odlišnosti může být velikost slova nebo reprezentace znaků používaného v daném operačním systému. Dnes se většina takových odlišností eliminovala, odlišnost znázornění znaků (především znaků národních abeced) však přetrvává. Proto také během vývoje protokolu FTP většina schopností vyrovnávat rozdíly mezi platformami vymizela, pouze schopnost konvertovat textové soubory při přenosu mezi různými platformami zůstala zachována.

Protokol FTP definuje 2 základní **režimy** přenosu souborů, **textový** (při něm se provádějí konverze znaků v přenášeném souboru), a **binární** (v něm se konverze neprovádí, je pro přenos zcela transparentní).

FTP podobně jako telnet zavádí pro potřeby přenosu jednotný formát dat. Také u FTP se v případě potřeby mohou komunikující strany dohodnout na přenosu v jiném formátu.

Protokol FTP přenáší soubory bez ohledu na jejich vnitřní strukturu. Soubor je implicitně přenášen jako souvislý proud dat (tzv. stream mode). Alternativně umožňuje protokol FTP použít tzv. blokový režim, při němž se mezi bloky vkládají tzv. zarážky, k nimž je možno se po eventuálním přerušení spojení vrátit. Tím je možno ušetřit čas a přenosovou kapacitu, neboť při přerušení přenosu např. v polovině souboru je možno navázat přenos od poslední zarážky a není nutno začínat přenos znovu od počátku souboru. Pro využití této schopnosti je pochopitelně nutné, aby blokový režim podporoval jak FTP server, tak FTP klient. Ojediněle se používá také tzv. komprimovaný režim přenosu, který eliminuje opakující se znaky.

Protokol FTP je zpravidla implementován tak, že jeho funkce jsou rozděleny mezi 2 aplikační entity:

- Protocol interpreter (interpretr protokolu);
- Data transfer process (proces přenosu dat).

Interpretr protokolu existuje trvale (vytvoří se ihned po spuštění programu, tedy FTP klienta či FTP serveru). Proces přenosu dat se vytváří až na základě požadavku na přenos určitého souboru a po jeho ukončení zaniká.

Pro komunikaci se používají 2 spojení, spojení řídící určené pro přenos příkazů, a spojení datové, jehož prostřednictvím se realizuje přenos souborů. Oddělení datového a řídícího spojení je výhodné především proto, že pomocí řídícího spojení je možno řídit přenos i během přenosu dat (např. je možné předčasně ukončit přenos, pokud se výrazně zpomalí, je možno signalizovat konec souboru apod.).

Řídící spojení přetrvává po celou dobu spojení klienta s určitým serverem. Toto spojení navazuje vždy klient na dobře známý port serveru 21. Datové spojení se ustavuje až na základě požadavku klienta. datové spojení navazuje server, a to bez ohledu na směr přenosu souboru (tedy i v případě, že se bude přenášet soubor z klienta na server). Pro datové spojení používá server dobře známý port 20, případně jiný port, na němž se předem s klientem domluví (pomocí příkazů PORT nebo PASV).

V případě, že to klient požaduje, může navázat datové spojení namísto serveru, musí to však serveru předem oznámit nastavením tzv. pasivního režimu. V případě klienta nacházejícího se za firewallem, který požadavky na otevření FTP spojení zvenčí sítě neakceptuje, je to pro správné fungování FTP protokolu nutné.

Protokol FTP má zabudován mechanismus pro přihlašování uživatelů, tedy server si je vědom toho, který uživatel se přihlašuje, a po korektním přihlášení mu podle jeho oprávnění zpřístupní příslušné soubory a adresáře. K lokálním souborům přistupuje FTP server vždy jménem uživatele, který spustil FTP klienta, který spojení s daným serverem inicioval. Je však nutno poznamenat, že podobně jako protokol telnet ani FTP nijak nechrání uživatelské jméno a heslo před odposlechem při přenosu po síti (nepoužívá tedy např. šifrování hesla).

Tzv. anonymní FTP servery, které se často používají pro zveřejnění souborů, nejsou při vyžadování uživatelského jména a hesla výjimkou. Používá se však konvence pojmenování uživatele anonymous a jako heslo je zpravidla požadována e-mailová adresa.

Pro účely řízení přenosu definuje protokol FTP vlastní řídící jazyk. Příkazy řídícího jazyka jsou pro snazší práci uživatelů v řádkových FTP klientech nahrazeny odpovídajícími, avšak snáze zapamatovatelnými příkazy tzv. uživatelského jazyka. Klient zajistí jejich překlad do řídícího jazyka a jejich zaslání serveru. Podobně je tomu i v případě grafických FTP klientů, ovšem zde uživatel nemusí příkazy vůbec zadávat v textové formě.

Řídící jazyk obsahuje 3 skupiny příkazů, které jsou uvedeny dále spolu s příkladem příkazů uživatelského jazyka:

- Příkazy pro řízení přístupu (např. otevření spojení - příkaz open, zadání hesla - příkaz user, atd.);
- příkazy pro nastavení parametrů (např. nastavení textového režimu - příkaz ascii);
- výkonné příkazy (např. přenos souboru na server - put, přenos souboru ze serveru - get, změnu aktuálního adresáře - cd, vytvoření adresáře, smazání při přejmenování souboru či adresáře apod.).

FTP server na příkazy odpovídá 3-znakovými odpověďmi složenými z číslic. První číslice signalizuje třídu odpovědi (1 - dočasná kladná, 2 - trvalá kladná, 3 - prozatímní, 4 - dočasná záporná, 5 - trvalá záporná odpověď). Další 2 číslice odpověď přesněji specifikují. Klient tyto odpovědi zpravidla vypisuje spolu s jejich textovou interpretací.

Za zmínku stojí i dnes již pomalu ustupující zjednodušená varianta protokolu FTP, která se nazývá TFTP (Trivial FTP). Ta se používá hlavně k zavedení operačního systému do bezdiskových stanic a terminálů. Její omezení spočívají především v tom, že nezná pojem uživatele, nepodporuje tedy přihlašování, a nepodporuje relativní cesty k souborům pomocí aktuálního adresáře, všechny cesty se tedy musí zadávat explicitně celé.

#3.3 Elektronická pošta

Elektronická pošta je služba přenosu zpráv (původně krátkých a pouze textových, to ale dnes již dávno neplatí), která je implementována různými způsoby v mnoha různých prostředích (známé jsou např. systémy X.400, Lotus ccMail a jiné). Je nutno poznamenat, že různé systémy elektronické pošty jsou vzájemně nekompatibilní a k tomu, aby bylo možné mezi různými systémy komunikovat, jsou nutné převodní brány.

Elektronická pošta v rámci protokolové sady TCP/IP je jednou z implementací služeb elektronické pošty, avšak díky rozšíření používání TCP/IP je ze všech systémů elektronické pošty dnes nejpoužívanější. Je založena na protokolu SMTP a na standardu RFC 822.
V dalším textu budeme elektronické poště v rámci protokolové sady TCP/IP hovořit pouze jako o „elektronické poště“, případně „elektronické poště SMTP“pokud nebude explicitně zmíněn jiný význam tohoto výrazu.

Úspěch elektronické pošty obecně a elektronické pošty v Internetu zvlášť spočívá především v jejích vlastnostech. Mezi nejvýznamnější z nich patří rzejména možnost komunikace „off-line“, tedy skutečnost, že odesílatel může zprávy odesílat bez ohledu na to, zda je příjemce právě připojen, a příjemce může zprávy zpracovat až tehdy, když se mu to hodí.

Původní podoba elektronické pošty byla velmi prostá: umožňovala pouze předávání krátkých textových sdělení elektronickou formou. Předávaný text mohl obsahovat pouze znaky základní ASCII sady.

Elektronická pošta vychází podobně jako většina ostatních aplikací v TCP/IP z výpočetního modelu klient/server. Serverem je tzv. poštovní server, který zabezpečuje přenos zpráv na cílový server a shromažďuje přijaté zprávy pro ty uživatele, kteří nejsou momentálně připojeni. Klientem je program, který umožňuje zprávy přijímat a číst, psát a odesílat a provádět s nimi další úkony.

Na fungování elektronické pošty SMTP se podílí několik protokolů. Přenos zpráv z klienta (odesílatele zprávy) na SMTP server odesílající pošty a pak dále na SMTP server příjemce zajišťuje protokol SMTP, práci s doručenými zprávami ve schránce uživatele zajišťují protokoly POP3 a IMAP. Formát zpráv a formát adres je definován doporučením RFC 822. Pozdější rozšíření, především v oblasti formátu zprávy, jsou definována standardem MIME.

Elektronická pošta SMTP prošla poměrně dlouhým vývojem. Původní koncepce počítala s tím, že uživatelé jsou připojeni k poštovnímu serveru prostřednictvím terminálové sítě, čili de facto přímo, takže poštovní server a klient běží na stejném počítači. Proto služba elektronické počítala pouze s přenosem zpráv z poštovního serveru odesílatele (z adresářů určených k odeslání) na jiný poštovní server (případě tentýž) do příslušného adresáře adresáta zprávy. Později se však ukázalo, že častější bude případ, kdy uživatel bude k poštovnímu serveru připojen z jiné stanice prostřednictvím počítačové sítě (zpravidla lokální sítě nebo

pomocí dočasného připojení), tedy že klient poběží na jiném uzlu než server. Proto bylo nutné dodatečně vyvinout prostředky pro komunikaci mezi poštovním klientem a serverem. Pro odesílání zpráv na poštovní server bylo možno použít protokolu SMTP, avšak pro přenos zpráv opačným směrem ze schránky uživatele na serveru do schránky uživatele na stanici byl vyvinut protokol POP, dnes se používá ve verzi POP3.

Poštovní schránka pro přijaté zprávy je vždy umístěna na poštovním serveru, na kterém má uživatel službu elektronické pošty zřízenu. Zpravidla je však schránka rozdělena na 2 části: přijaté zprávy, které si dosud uživatel nevyzvedl, jsou uloženy ve schránce na serveru, zatímco zprávy, které si uživatel již vyzvedl, jsou při vyzvednutí přeneseny na jeho počítač. V takovém případě je nutné nové poštovní zprávy explicitně přenášet neboli „stahovat“ na počítač uživatele. Ke stahování zpráv se používá zpravidla protokol POP3. Toto uspořádání je univerzální, a proto se s ním můžeme setkat ve všech prostředích.

Druhou možností je umístit celou schránku na poštovní server a vyzvednuté zprávy nikam nepřenášet. Tato varianta není vhodná, pokud je klient připojen pouze dočasně nebo sice trvale, ale pomalým připojením. Naproti tomu v prostředí s trvalým rychlým připojením může přinést některé výhody. za nejvýznamnější výhodu se považuje skutečnost, že uživatel má v tomto případě k dispozici všechny zprávy včetně již přečtených z každé stanice připojené k jeho poštovnímu serveru. Znamená to, že uživatel si může prohlížet všechny zprávy např. z kteréhokoli počítače v lokální síti. tato varianta se realizuje zpravidla pomocí protokolu IMAP.

#3.3.1 Formát zprávy

Součástí vývoje elektronické pošty bylo i postupné rozšiřování služeb, především v oblasti možného obsahu zprávy. Z původního omezení na ASCII znaky a striktního omezení velikosti se služba vyvinula do dnešní podoby, kdy je možno do zprávy vkládat znaky národních abeced, formátování, obrázky, přílohy ve formě souborů prakticky libovolného formátu apod. a velikost zprávy je omezena pouze kapacitou poštovní schránky příjemce a případnými omezeními na poštovním serveru odesílatele. O formátu zprávy nyní zmíníme podrobněji.

Každá zpráva obsahuje 2 základní části: hlavičku zprávy a datovou část neboli tělo zprávy. Hlavička obsahuje nejdůležitější údaje, jimiž se řídí poštovní server při práci se zprávou. Její struktura včetně přesné syntaxe adres je definována doporučením RFC 822. Toto doporučení nijak nedefinuje obsah těla zprávy, o němž pouze předpokládá, že je tvořeno ASCII textem. Určitou strukturu do těla zprávy zavedl teprve standard MIME, který tím mimo jiné umožnil zasílání příloh ve zprávách.

Hlavička zprávy dle RFC 822 je tvořena jednotlivými položkami, které jsou vždy uvozeny klíčovým slovem končícím dvojtečkou. každá z položek hlavičky začíná na novém řádku. Pořadí položek v hlavičce není předepsáno, existuje však doporučené pořadí. Několik položek je povinných, většina jich však je nepovinných. Ty řádky v hlavičce, které nezačínají žádným z klíčových slov, jsou ignorovány. Hlavička je od těla zprávy oddělena prázdným řádkem.

Nejdůležitějšími položkami hlavičky zprávy jsou tyto:

- From: (adresa autora zprávy);
- To: (adresa příjemce);
- Sender: (adresa odesílatele, je-li jím někdo jiný než autor zprávy);
- Cc: (adresa pro zaslání kopie zprávy „na vědomí“);

- Bcc: (adresa pro zaslání „slepé“ kopie zprávy - příjemce v této položce se nezobrazí ostatním příjemcům v položkách To: a Cc:);
- Reply-to: (adresa pro zaslání odpovědi, pokud je jiná než adresa From:);
- Return-Path: (adresa pro vrácení zprávy v případě její nedoručitelnosti, pokud je jiná než adresa From:);
- Date: (datum a čas odeslání zprávy)
- Subject: předmět zprávy.

Všechny výše uvedené položky s výjimkou poslední z nich (Subject:) mají pevně stanovenou syntaxi, neboť smějí obsahovat pouze adresu, případně více adres oddělených čárkami. Výjimkou je pochopitelně předposlední položka Date:, která obsahuje datum a čas v předepsaném formátu, do vyplnění této položky však uživatel prakticky nemůže zasáhnout.

Syntaxe adres je vcelku jednoduchá: adresy smějí obsahovat pouze písmena, číslice a některé další znaky ze základní ASCII sady. Adresa má 2 části, které odděluje znak „@” (tzv. zavináč). Ten se pochopitelně na jiném místě adresy vyskytovat nesmí.

Adresa se může používat rovněž ve formě s komentářem (nejčastěji bývá komentářem skutečné jméno adresáta), a to buď nejprve komentář a pak adresa oddělená lomenými závorkami (např. „Tomáš Sochor <tomas.sochor@osu.cz>”), nebo nejprve adresa a pak komentář v kulatých závorkách (např. „tomas.sochor@osu.cz (Tomáš Sochor)”). Je přitom třeba upozornit, že použití českých znaků či jiných znaků národních abeced umožnil až standard MIME, nebylo jej tedy možno používat ve starších poštovních klientech. Pro účely zapsání adresy ve formě odkazu pro použití v HTML dokumentech se adresa uvozuje příznakem „mailto:“. Příkladem takového odkazu je tedy “mailto:tomas.sochor@osu.cz”.

Vzhledem k tomu, že elektronická pošta SMTP vznikala v době, kdy nebylo možné po sítí běžně zasílat 8-bitová slova (8. bit se často používal jako tzv. paritní), předpokládá elektronická pošta, že všechny znaky tvořící zprávu budou patřit do základní ASCII sady (kódy 0-127). Pro přenos 8-bitových bytů bylo nutno taková data nejprve upravit do 7-bitové formy.

Pro úpravu příloh do 7-bitové podoby se postupně vyvinuto několik způsobů. Nejstarší z nich (UUEncode pocházející z unixu a BinHex pocházející z počítačů Macintosh) jsou poněkud nesystematické, protože řeší pouze přibalování příloh do zpráv a nezabývají se dalšími aspekty, např. rozlišením typu přílohy, formátováním obsahu (těla) poštovních zpráv, použití znaků národních abeced v těle zprávy apod.

Systematičtější řešení přinesl až standard MIME (Multipurpose Internet Multimedia Extensions), který umožňuje bezproblémovou práci s přílohami díky tomu, že definuje nejen způsob úpravy přílohy pro odeslání, ale umožňuje přikládání více příloh do zprávy, definuje typy příloh napomáhající příjemci otevření souboru ve správné aplikaci, umožňuje vkládání 8-bitových znaků (např. češtiny, formátovacích znaků apod.) do těla zprávy, předmětu zprávy i komentářové části adres.

MIME zavádí 2 typy přenosového kódování, konkrétně tzv. Quoted Printable a Base64 (která nahrazují dříve používaná kódování UUencode a BinHex). Kódování zajišťuje převod 8-bitových dat na 7-bitová, což byl postup vyvinutý v důsledku toho, že přenosové mechanismy elektronické pošty (zejména protokol SMTP) garantují pouze přenos tzv. 7-bitových dat (8. bit byl dříve používán ke kontrolním účelům, např. jako paritní bit). Kódování je dodnes nutný krok, který se provádí před odesláním zprávy, a díky němuž je skutečná velikost zprávy přeipavené pro přenos obvykle zhrubě o 10 – 30 % větší než zpráva

uložená v počítači).

Dále se zavádí dvousložkové MIME typy, které definují typ přílohy a způsob zpracování (např. image/gif, application/msword apod.), a především zavádí do hlavičky nové položky, které se použijí především pro předání informací o přílohách, kódování apod. v hlavičce zprávy.

Zavedení nových položek do hlavičky je umožněno již zmíněnou vlastností definice hlavičky dle RFC 822, že totiž položky začínající jiným než klíčových slovem se ignorují. Z důležitých nových položek si uvedeme alespoň položku Content-type určující pomocí MIME typu typ obsahu zprávy a případně i informaci o kódování národních znaků. Díky zavedení této položky bylo například umožněno dnes poměrně rozšířené zasílání zpráv ve formátu HTML.

MIME typy mají 7 základních typů (text, image, audio, video, application, multipart a message) a velké množství podtypů, které není uzavřeno pro tvorbu nových. Uvádí se vždy ve tvaru typ/podtyp a používají se také mimo elektronickou poštu, např. k určení typu stránek, které WWW server zasílá klientovi.

V případě, že uživatel používá klienta, který dosud standard MIME nepodporuje, bude mít některé části zprávy nečitelné, avšak nezpůsobí to nedoručení zprávy.

#3.3.2 Poštovní domény

Často se můžeme setkat s tím, že „serverová“ část adresy elektronické pošty (např. „osu.cz“ v případě adresy uzivatel@osu.cz) neodpovídá žádné IP adrese (tedy pro tuto doménu neexistuje v DNS databázi tzv. A záznam, který určuje IP adresu daného serveru, ve výše uvedeném případě „osu.cz“). Znamená to, že „osu.cz“ není název poštovního serveru. Přesto však na tuto adresu lze doručovat zprávy elektronické pošty, a proto musí existovat nějaký poštovní server, který tuto poštovní doménu „obhospodařuje“.

Tento poštovní server je určen pomocí tzv. MX (Mail eXchange) záznamu, který pro poštovní doménu určuje poštovní server (např. pro doménu „osu.cz“ určuje třeba poštovní server „mailer.osu.cz“).

#3.4 Služba World Wide Web

WWW neboli World Wide Web je dnes nejrozšířenější službou Internetu. Tato služba se však používá k prezentaci dat i mimo Internet, v soukromých sítích (Intranetech) apod.

Služba WWW vznikla v roce 1989 ve středisku CERN v Ženevě, původně jako textová služba. Služba WWW vychází z principu hypertextu. Hypertext je dokument rozdělený na menší stránky, mezi nimiž mohou existovat libovolné vazby pomocí tzv. aktivních odkazů. Hypertext se často používá např. v systémech nápovědy k operačním systémům, zde se však používají pouze odkazy mezi jednotlivými stránkami, případně na jiné dokumenty v rámci daného počítače. Služba WWW obohacuje hypertext především o možnost umísťování odkazů na libovolný soubor kdekoli na síti. Přitom aktivní odkazy mohou být umístěny nejen v samotném textu, ale i na obrázcích nebo jejich částech.

Služba WWW prošla rychlým vývojem od původně textové služby do dnešní podoby, kdy umožňuje začleňování celé řady formátů souborů včetně multimediálních (zvuk, video, animace apod.).

Během vývoje se WWW stal ze služby také platformou pro poskytování jiných služeb. Příkladem je vyhledávání v Internetu, které bylo v počátcích realizováno specializovanými službami (Archie, Veronica, FTP Search apod.), po nástupu služby WWW se začalo

přesouvat pod tuto platformu a dnes se vyhledávání realizuje zpravidla prostřednictvím přístupu přes WWW a mnohé specializované vyhledávací služby prakticky zanikly. Další službou, ke které se často přistupuje prostřednictvím WWW, je elektronická pošta.

Služba WWW je také velmi významná tím, že se jedná prakticky o jedinou službu TCP/IP, která se ve velkém měřítku používá ke komerčním účelům. Právě komerční využití této služby je největším hybatelem jejího prudkého vývoje.

Služba WWW vychází z modelu klient/server. WWW server uchovává a spravuje jednotlivé WWW stránky a na žádost klienta jim je poskytuje (zasílá). WWW klient (většinou nazývaný WWW prohlížeč neboli browser) si vyzvedává stránky od WWW serverů a zobrazuje je pro uživatele.

Pro fungování služby WWW je nutné mít definovaný jednak způsob přenosu stránek mezi serverem a klientem (to definuje protokol HTTP), a také formát stránek (ten je definován jazykem HTML). Filosofie jazyka HTML vychází z toho, že definuje strukturu dokumentu (např. nadpisy, seznamy, obrázky apod.), nikoli to, jak má dokument vypadat na obrazovce (to definuje WWW klient podle svých grafických schopností). V dnešní době je jazyk HTML poměrně komplikovaný, obsahuje velké množství různých možností, např. vkládání částí programového kódu pomocí skriptů nebo appletů, umožňuje pomocí formulářů získávat data od uživatele apod.

WWW klient zobrazuje obdržené HTML soubory a soubory jiných typů podle svých grafických možností, přičemž někdy používá pro zobrazení speciálních formátů externí programy v rámci operačního systému stanice, na které pracuje. V dnešní době je většina WWW klientů schopna fungovat i jako klienti služby FTP, často je jejich součástí i klient elektronické pošty.

Protokol http je jednoduchý přenosový protokol, který využívá služeb protokolu TCP. Data přenáší v textovém tvaru, server očekává požadavky na portu 80. Protokol http funguje bezestavově, pro každý objekt na stránce se navazuje samostatné spojení. Komunikace probíhá tak, že klient zašle požadavek a server na něj odpoví a pak spojení ukončí (v případě protokolu http 1.1 definovaného v RFC 2068 se ukončí spojení až po načtení celé stránky, resp. po přenesení všech souborů z daného serveru, které jsou v daném okamžiku požadovány).

Pro komunikaci je definováno několik jednoduchých příkazů označovaných jako metody. Nejdůležitějšími metodami jsou GET, pomocí které klient žádá o zaslání stránky, a POST, kterou klient odesílá data ve formuláři serveru. Pro získání samotných hlaviček odpovědi (viz dále) se používá též metoda HEAD. Každá metoda (i odpověď na ni) je doplněna o parametry, tzv. hlavičky, kde se uvádní např. adresa požadovaného serveru, MIME typ přenášených dat atd.

$Příklad$

Zkuste si pomocí vhodného nástroje (např. zachycovač paketů Wireshark, nebo specializované nástroje jako je plug-in LiveHttpHeaders pro prohlížeč Firefox) zobrazit požadavek na zaslání souboru z www serveru (metodou GET) a odpověď serveru na tento požadavek a vypište si názvy jednotlivých hlaviček, které jsou součástí požadavku a odpovědi. Všimněte si rozdílů ve struktuře hlaviček mezi požadavkem a odpovědí.

Odpovědi serveru mají podobně jako v případě FTP podobu tříznakových číselných kódů volitelně doplněných krátkým textem. Odpověď začínající číslicí 1 je informační, číslicí 2 začíná kladná odpověď serveru, číslicí 3 začíná upozornění na očekávanou další aktivitu klienta, číslicí 4 začíná oznámení chyby na straně klienta a číslicí 5 začíná oznámení chyby na

straně serveru. Typickým příkladem odpovědi, s níž se může uživatel často setkat, je „404“, jejíž význam je vyjádřen textem „Not Found“, což znamená, že na daném serveru nebyl nalezen požadovaný soubor. Součástí kladné odpovědi pochopitelně je i požadovaný soubor, nejčastěji HTML stránka (v případě metody GET nebo POST).

Dotazy i odpovědi jsou doplněny tzv. „hlavičkami“, což jsou v podstatě parametry upřesňující dotaz či odpověď. V hlavičkách kladné odpovědi bývá uveden MIME typ přenášeného souboru, informace o platnosti souboru apod.

Vzhledem ke skutečnosti, že bezestavový charakter komunikace neumožňuje, aby si server pamatoval například průběh předchozí komunikace s klientem, omezuje to možnost poskytování některých služeb. Jednou z možností, jak to obejít, je vložit tyto informace do adresy (URL) serveru jako parametr, avšak univerzálnější řešení představují tzv. cookies, které byly zavedeny v RFC 2109. Cookies jsou krátké textové údaje, které generuje www server a zasílá je klientovi. Ten si je může uložit na disk pro potřeby další komunikace s tímto serverem. Při další komunikaci s tímto serverem mu klient zašle příslušný cookie a server si jej může podle toho identifikovat. Ukládání cookies na straně klienta je pochopitelně volitelné a je možné jej zakázat. Tím se zvýší bezpečnost klienta, ovšem může se omezit možnost pracovat s některými WWW servery. Cookie se zasílají obvykle rovněž pomocí hlaviček (viz výše).

Přestože se to často tvrdí, není pravda, že by cookie obsahovaly např. údaje o uživateli jako uživatelské jméno, heslo apod. Cookie mohou obsahovat v zásadě cokoli, ale pouze nesprávně napsané www aplikace ukládají do cookie takovéto údaje. Cookie je textový řetězec, u něhož stačí, že má význam pro server, který jej vygeneroval. Skutečnost, že cookie lze využít např. k tzv. trvalému přihlášení na jistý www server, znamená pouze to, že příslušná cookie, kterou má www prohlížeč uživatele uloženu ve svém úložišti[2], je na serveru svázána s určitým uživatelským účtem, a server má u tohoto účtu nastaveno, že po zaslání cookie klientem nemá zaslat přihlašovací stránku, ale přímo stránku zobrazující uživatelův obsah (např. poštovní schránky).

#3.5 Systém DNS

Při práci se službami TCP/IP si mnozí uživatelé ani neuvědomí, že prakticky všechny služby využívají jednou službu pomocnou, totiž DNS (Domain Name System). Služba DNS slouží k tomu, aby si uživatel nemusel pamatovat IP adresy, které jsou zapamatovatelné obtížně, a místo toho si mohl zapamatovat adresu serveru v textové formě. Jistě se snáze pamatuje např. symbolická adresa www.osu.cz než IP adresa 195.113.106.17. Součástí služby DNS jsou pochopitelně i pravidla pro vytváření doménových jmen, správa domén, ale my se zde zaměříme jen na to nejdůležitější pro uživatele, tedy na mechanismus převodu symbolických jmen na IP adresy.

Služba DNS využívá k přenosu svých dotazů a odpovědí obvykle protokol UDP (je pro ni vyhrazen dobře známý port číslo 53). Pouze v případě přenosu většího množství dat, která není možno umístit do jednoho UDP datagramu, lze využít i protokolu TCP (na stejném dobře známém portu 53).

Základním typem záznamu v systému DNS jsou tzv. A záznamy, které určují, že určitému doménovému jménu odpovídá určitá IP adresa (např. že doménovému jménu www.osu.cz odpovídá 195.113.106.10). Během vývoje systému DNS byly do DNS databáze

---

2 Pro zájemce uvádím na doplnění, že cookie obvykle nemají společné úložiště pro celý operační systém, ale každý www klient (prohlížeč) si cookie uchovává ve svém vlastním úložišti (mimo jiné se proto s nimi v různých prohlížečích pracuje různě pohodlně) a toto úložiště není dostupné jiným www klientům používaným na tomto počítači.

doplněny další typy záznamů, z nichž se zmíníme o dvou. Záznam typu AAAA slouží podobně jako záznam typu A k převodu doménového jména na IP adresu, ovšem o případě záznamu AAAA jde o překlad na IP adresu verze 6, tedy na adresu 128-bitovou. Protože 128 bitů je čtyřnásobek délky IP adresy verze 4, nese tento typ záznamu označení čtyřmi „A“.

Dalším důležitým typem záznamu v DNS databázi je tzv. MX záznam, který určuje poštovní server pro tzv. poštovní doménu, tedy pro doménu, pro kterou neexistuje záznam typu A, ale přesto se vyskytuje v adrese elektronické pošty (např. „osu.cz“).

Systém DNS je založen na hierarchické struktuře tzv. domén. Doména je prvek hierarchického jmenného prostoru. Příkladem může být doména osu, která je subdoménou domény cz, a její plně kvalifikovaný zápis je tedy „osu.cz“. Doménám, ale v praxi častěji skupinám domén zvaným zóny, odpovídá systém tzv. DNS serverů, které odpovídají na požadavky klientů. Požadavek na DNS server vygeneruje každý klient každé aplikační služby TCP/IP při obdržení požadavku, v němž se vyskytuje symbolické jméno místo IP adresy. Protože je těchto požadavků velké množství, je systém zefektivněn ukládáním odpovědí na požadavky do cache na každém DNS serveru. Teprve pokud není odpověď na požadavek nalezena v cache, provede se dotaz do hierarchické struktury DNS serverů.

Odpověď z cache se nazývá neautoritativní. Aplikace si však může v případě potřeby vyžádat pouze autoritativní odpověď, tedy odpověď pocházející přímo od DNS serveru obsluhujícího příslušnou doménu.

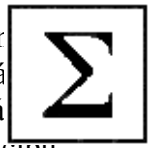
Platí, že každá doména má svůj DNS server, kam ukládá informace o doméně a změnách v ní, který se nazývá primární. Z něho čerpá informace zbytek serverů zapojených do systému DNS. Z důvodů zajištění bezproblémové funkce se obvykle pro každou doménu definuje nejméně jeden server záložní, tzv. sekundární.

Zásadní funkci v celém systému mají domény nejvyšší úrovně neboli TLD (Top Level Domain). Tyto domény obhospodařuje skupina tzv. kořenových („root“) serverů, na jejichž fungování dohlíží organizace ICANN.

Později byly funkce systému DNS rozšířeny tak, aby například umožňoval vyhledávání IP adres verze 6 (záznamy typu AAAA) a zejména o záznamy typu MX, které určují poštovní server pro poštovní domény. Podobně se používají také záznamy typu CNAME, které podobně jako záznamy typu MX „nahrazují“ jedno doménové jméno jiným, ovšem musí být jedinečné, což je rozdíl od MX záznamů, které díky údaji o prioritě v každém MX záznamu mohou být pro jednu doménu duplicitní.

K ověření funkčnosti systému DNS slouží řádková utilita *nslookup*, která je k dispozici na většině dnešních operačních systémů.

$Shrnutí obsahu kapitoly$



V této kapitole jste se seznámili s vlastnostmi aplikační vrstvy a jejich nejvýznamn
službami. K nim patří především služba pro sdílení informací WWW, elektronická
telnet, FTP a NFS, s nimiž jsme se seznámili podrobněji a popsali jsme si jejich zá
vlastnosti důležité pro jejich používání. Všechny tyto služby jsou založeny na princip
komunikace klient/server, což významným způsobem ovlivňuje jejich vlastnosti.

Kromě toho jsme se také seznámili s velmi důležitým podpůrným systémem DNS, který umožňuje, aby uživatelé mohli při používání služeb TCP/IP místo IP adres používat snáze zapamatovatelná symbolická jména.

$Pojmy k zapamatování:$

- FTP
- Protokol SMTP
- Protokol POP3
- Rozšíření formátu zprávy elektronické pošty MIME, MIME typ, přenosové kódování
- Služba WWW
- Jazyk HTML
- Protokol http
- Cookie
- Systém DNS

$Kontrolní otázky$

1. Proč není možné bez úprav přiloženého souboru posílat ve zprávě elektroni podle standardu SMTP přílohy?
2. Proč je při odesílání zpráv vhodnější držet se standardu MIME místo použi UUencode nebo BinHex?
3. Vzpomeňte si, které z protokolů pro vzdálené přihlašování a práci se soubory (telnet, FTP, NFS) používáte v praxi a k jakému účelu.
4. Napište, jaké $**výkonné$** příkazy uživatelského jazyka protokolu FTP znáte (nejvýše 10 příkazů, jen výkonné příkazy, tedy ty, které způsobí přenos dat, ne jen řídícího příkazu!)

$Korespondenční úkoly$

1. Potřebuje Vaše PC, které je připojeno do lokální sítě a používá pouze elektronickou poštu, přímo komunikovat s Internetem (tedy: potřebuje veřejnou IP adresu
2. V čem myslíte, že by mohla spočívat potenciální nebezpečnost cookies pro a němž pracuje klient služby WWW, a pro uživatele tohoto počítače?
3. Pokud provedete změnu hesla svého uživatelského účtu prostřednictvím protokolu telnet na dálku, jakému nebezpečí se vystavujete?
4. Popište použití položky Bcc: (tzv. slepá kopie) v hlavičce zprávy elektronické pošty!
5. Spusťte si z příkazového řádku utilitu nslookup a její pomocí zjistěte nastavení MX záznamů pro Vaši poštovní doménu (pomůcka: je třeba nastavit typ hledaného záznamu pomocí příkazu set). Výstup z programu okomentujte (jaký poštovní server Vaši doménu obsluhuje apod.)
6. V klientském programu pro práci s elektronickou poštou si otevřete poštovní zprávu, která obsahuje v těle zprávy české znaky a nejméně jednu přílohu, a zobrazte si její zdrojový text. Zde si najděte označení MIME typu a typu přenosového kódování jednotlivých částí zprávy a řetězec oddělovače, vše ve zdrojovém textu vyznačte a pošlete tutorovi. Poznámka: pozor, k tomuto cvičení nepoužívejte komerční programy, v některých nejde zdrojový kód zprávy zobrazit (např. MS Outlook).
7. Pomocí programu Wireshark nebo jiného paketového analyzátoru si zachyťte komunikaci Vašeho www prohlížeče s některým www serverem při zobrazování www stránky obsahující např. externí obrázky a jiné dokumenty a do své odpovědi vypište použité dotazovací metody a jejich hlavičky stejně jako hlavičky odpovědí zasílaných serverem. Pokuste se zachytit hlavičku Set-Cookie: nebo Cookie:. Výpis okomentujte tak, aby bylo poznat význam jednotlivých použitých metod a hlaviček. Poznámka: hlavičky lze snadno zachytit pomocí rozšíření LiveHTTPHeaders pro prohlížeč Firefox.

#4 Rodina protokolů TCP/IP, architektura TCP/IP

$Obsah kapitoly$

Průvodce studiem

Studium této úvodní kapitoly je poměrně náročné. Přitom bez jejího dokonalého zv nelze předpokládat úspěšné osvojení poznatků v dalších kapitolách. Doporučuji si vyhradit alespoň 2 hodiny času.

$V této kapitole se dozvíte:$

1. Jak a kdy vznikla protokolová sada TCP/IP?
2. Jaká je základní filosofie fungování TCP/IP?
3. Jakou má strukturu architektura TCP/IP?
4. Jaké jsou nedostatky, omezení a problémy TCP/IP a jaká jsou jejich řešení?

$Po jejím prostudování byste měli být schopni:$

1. Charakterizovat základní přednosti a nedostatky TCP/IP;
2. Popsat základní filosofická východiska vzniku TCP/IP a její vrstevnatou strukturu;
3. Rozumět omezením TCP/IP a znát možnosti jejich eliminace.

~Klíčová slova této kapitoly:

Architektura síťová, protokol, princip maximální snahy, nespolehlivá komunikace, přepojování paketů

Doba potřebná ke studiu: 2 hodiny&

#4.1 Úvod

V dnešní době v počítačových sítích bezkonkurenčně dominuje tzv. rodina protokolů TCP/IP. Jde o sadu protokolů, která v poslední době prakticky vytlačila všechny ostatní sady protokolů pro počítačové sítě. Proto je i tento text věnován výlučně protokolové sadě TCP/IP.

#4.2 Vznik rodiny protokolů TCP/IP

Historie protokolové sady TCP/IP začíná v 60. letech 20. století, kdy na několika výzkumných pracovištích v USA vznikla koncepce „přepojování paketů“. Vznikla jako alternativa dosud převládající koncepce „přepojování okruhů“ převzaté z telekomunikačních sítí, a motivem pro její vznik byla především snaha o vytvoření počítačové sítě, která by byla odolná vůči výpadkům jednotlivých částí sítě.

Princip **přepojování paketů**, který byl stručně popsán např. v předchozí kapitole, je vcelku prostý, avšak pro jeho důležitost jej zde znovu připomeneme. Místo toho, aby byl před zahájením přenosu dat vytvořen okruh (zpravidla virtuální), po němž se data posléze posílají, se při využití koncepce přepojování paketů data v blocích (tzv. paketech) předávají síti, která

se podle adresy příjemce postará o jejich doručení, a odesílatel se nezabývá tím, jak a kudy síť data doručí příjemci. Princip přepojování paketů byl pro provoz datových sítí navržen až v 60. letech 20. století. Do té doby se používal výlučně princip přepojování okruhů běžný v tehdejších telekomunikačních sítích, kde převažuje dodnes.

Výzkumem v té době převratné koncepce přepojování paketů se věnovalo několik akademických pracovišť především v USA, která získala pro praktické ověření výsledků tohoto výzkumu finanční podporu agentury ARPA. Tak vznikla síť ARPANET, která byla po ukončení výzkumných úkolů předána do užívání akademickým pracovištím (nejen těm, která se podílela na výzkumu).

V síti ARPANET se zpočátku používal protokol NCP, což byl experimentální protokol, ten se však příliš nehodil pro rutinní používání. Proto byly brzy zahájeny práce na jeho nahrazení protokolovou sadou TCP/IP. Její vývoj byl opět financován agenturou ARPA. V průběhu 70. let 20. století byla protokolová sada TCP/IP z větší části vyvinuta a implementována do některých operačních systémů, především Unixu. Protože velká část těchto prací byla financována vládou USA (prostřednictvím vládních agentur), musel být jejich výsledek (protokolová sada TCP/IP a její implementace) dán k dispozici veřejnosti. Celý Internet (ve který se původní síť ARPANET mezitím přeměnila) přešel na používání protokolů TCP/IP na počátku roku 1983.

#4.3 Architektura TCP/IP

Architektura TCP/IP je determinována následujícími především snahou přizpůsobit se předpokládaným výpadkům částí sítě a jejich nespolehlivosti. Přitom byla především eliminována potřeba existence centrálního prvku sítě (síť byla navržena tak, aby byla schopna provozu i při výpadku kteréhokoli prvku nebo části sítě). Přitom celá síťová architektura TCP/IP byla budována jako maximálně otevřená s důrazem na praktické používání. To se projevuje zejména tím, že se nejprve vytvářejí funkční protokoly, a ty se teprve následně po ověření funkčnosti začleňují do struktury celé architektury. Díky této filosofii z TCP/IP vznikla funkční síťová architektury rychleji než z referenčního modelu ISO/OSI, který začal vznikat prakticky souběžně. Otevřenost TCP/IP se projevuje zejména tím, že architektura TCP/IP je schopna akceptovat i protokoly vzniklé původně mimo její rámec, pokud se v praxi osvědčí.

Z výše uvedených výchozích odlišností pak vyplývají vlastnosti, kterými je celá architektura TCP/IP specifická:

- co nejnižší počet vrstev daný především tím, že většina aplikačně orientovaných funkcí byla v TCP/IP začleněna jako volitelná do aplikační vrstvy;
- ponechání co největší možnosti volby na všech vrstvách (to se projevuje nejvíce na transportní vrstvě);
- přednost má nespojovaná a nespolehlivá komunikace, při uplatnění principu „**best effort**“ (maximální snahy).

Z výše uvedených důvodů se architektura TCP/IP ustálila na 4 vrstvách, jak potvrzuje tabulka 1. V tabulce se zmiňuje porovnání s referenčním modelem ISO/OSI, který se v tomto kurzu neprobírá, avšak protože se často používá jako zdroj terminologie, uvádíme zde toto porovnání.

@Tabulka 3. Porovnání vrstev TCP/IP a ISO/OSI

TCP/IP	ISO/OSI
aplikační vrstva	aplikační vrstva

	prezentační v. relační v.
transportní vrstva	transportní vrstva
síťová vrstva (IP vrstva)	síťová v.
vrstva síťového rozhraní	linková (spojová) v. fyzická v.

&

#4.3.1 Nespojovaná a nespolehlivá komunikace

Nejprve si vymezíme několik důležitých pojmů. **Spojově orientovanou komunikací** či službou rozumíme komunikaci, kdy se před zahájením přenosu vytvoří virtuální kanál od odesílatele k příjemci, ten se využije pro přenos datových paketů, a po ukončení přenosu se virtuální kanál zruší. **Nespojová komunikace** či služba je taková služba, která pro odeslání dat žádný přenosový kanál nevytváří.

Spolehlivou komunikací či službou rozumíme takovou službu, kdy odesílatel dostane informaci o doručení odeslaných dat příjemci (případně o nemožnosti jejich doručení. **Nespolehlivá komunikace** je taková služba, která tuto vlastnost nemá.

Naproti tomu v TCP/IP se v hojné míře (dále uvidíme, že především na síťové vrstvě) uplatňuje pravý opak, **nespojová komunikace**. Důvod je nasnadě. Vzpomeňte si, že v úvodu jsme uvedli, že při návrhu protokolů se počítalo s výpadky a nespolehlivostí různých částí sítě. Pokud by se používala spojově orientovaná komunikace, bylo by nutné při každém výpadku spojení obnovovat, a obnovení je spojeno s nezanedbatelným **režijním provozem** (tedy přenosem dat, která neslouží k doručení příjemci, ale pouze pro potřeby provozu sítě). Totéž platí při změnách v síti (např. její topologie). V případě nespojové komunikace taková režie nevzniká.

Je zřejmé, že to má svá omezení: nespojová komunikace se hodí pro tzv. shlukové přenosy s nízkou průměrnou přenosovou rychlostí, kdy se občas přenášejí větší objemy dat, nicméně po většinu času se nepřenášejí téměř žádná data. Nehodí se však určitě pro případ trvalých toků většího množství dat.

Protože se na nižších vrstvách TCP/IP používá nespojovaná komunikace, je zřejmé, že by nemělo smysl nespojovanou komunikaci kombinovat se spolehlivou službou, proto se dává přednost nespolehlivé komunikaci. Dalším důvodem pro využití nespolehlivé služby je skutečnost, že zajištění spolehlivosti vyžaduje nezanedbatelnou režii, a pokud by touto režií byla zatížena např. síťová vrstva, nemohla by se jí vyšší vrstva vyhnout, i pokud by spolehlivý přenos nevyžadovala. Navíc vzhledem ke skutečnosti, že je prakticky velmi obtížné docílit 100% spolehlivosti, mohlo by se stát, že nabízená úroveň spolehlivosti je pro některou aplikaci i tak nedostatečná, a tak by si musela spolehlivost zajistit sama, čímž by docházelo k dalšímu zvyšování režie a plýtvání přenosovou kapacitou. Je nutné upozornit, že i přesto, že nižší vrstvy fungují nespojovaně a nespolehlivě, mohou nad nimi vyšší vrstvy fungovat spolehlivě a v případě potřeby i spojovaně. Mechanismy, jimiž to lze zajistit, jsou popsány v kapitole 4.

Z důvodů shrnutých výše bylo v TCP/IP zvoleno řešení, které umožňuje si aplikaci zvolit, zda spolehlivost vyžaduje či nikoli. Pokud ano, použije spolehlivou spojovanou službu transportní vrstvy, reprezentovanou protokolem TCP, v opačném případě použije nespolehlivou nespojovanou službu protokolu UDP.

Rozhodnutí tvůrců protokolové sady TCP/IP nabídnout dvě alternativní služby přenosu dat až na transportní vrstvě a ponechat služby síťové vrstvy pouze nespolehlivé a nespojované

znamená, že spolehlivost se bude zajišťovat pouze na koncových uzlech. Na mezilehlých uzlech (nejčastěji směrovačích), které zahrnují pouze funkce vrstvy sítového rozhraní a vrstvy síťové, bude jedinou možnou službou nespolehlivý a nespojovaný přenos. Toto rozhodnutí je dosti zásadní pro celou koncepci budování TCP/IP sítí, protože to znamená, že síťová infrastruktura včetně mezilehlých uzlů (směrovačů) bude pracovat co nejjednodušeji a zároveň s maximálním omezením režie. Veškeré dodatečné služby (mezi něž zajištění spolehlivosti patří) budou implementovány pouze na koncových uzlech.

Toto rozhodnutí je koncepčního charakteru zejména pro další rozvoj služeb TCP/IP sítí. Pokud totiž například nějaká budoucí verze protokolu TCP zdokonalí mechanismus zajištění spolehlivosti (či dokonce nahradí protokol TCP jiným), nebude nutné kvůli tomu provádět žádné změny na síťové infrastruktuře, postačí pouze změny v samotných koncových uzlech, kde se díky častější obměně hardware i operačních systémů provádějí snáze.

Řečeno jinými slovy to znamená, že složitější softwarové funkce (neboli „inteligence“) potřebné k provádění složitějších operací (k nimž zajištění spolehlivosti patří) a spolu s nimi potřebný výpočetní výkon jsou umístěny především na koncových uzlech a nikoli v mezilehlých uzlech v síti. Zde spočívá jeden z důležitých rozdílů proti telekomunikačním sítím, které umísťují inteligenci naopak především do sítě (do ústředen apod.).

Princip maximální snahy zmíněný výše ovšem znamená, že v případě požadavků přesahujících kapacitu některé části sítě může přetížená část sítě (například směrovač) požadavky krátit, a to buď pozdržením jejich vyřízení, nebo i úplným zahozením některých paketů. Je přitom důležité si uvědomit, že protokolová sada TCP/IP nemá v sobě zabudovány žádné mechanismy pro rozlišení datových toků podle priority, takže při krácení požadavků jsou všechny požadavky kráceny stejnou měrou. Není tedy možné např. při zahazování paket; nejdříve zahazovat pakety elektronické pošty nebo FTP a tak omezit třeba opožďování datového toku u služeb, které jsou na jeho pravidelnosti více závislé (třeba webové vysílání TV signálu, Real audio apod.). Je zřejmé, že tato vlastnost TCP/IP poněkud brání rozvoji především multimediálních služeb. Naproti tomu lze ukázat, že síť fungující na principu „best effort“ je mnohem efektivnější pro veškeré datové přenosy. Je třeba si uvědomit i skutečnost, že právě tato efektivnost pomohla Internetu k tak rychlému rozvoji.

Při vzniku protokolové sady TCP/IP se počítalo s tím, že jednotlivé dílčí sítě budou propojeny pomocí směrovačů, přičemž z požadavku robustnosti (zachování funkce při výpadku některé části sítě) vyplývá, že jsou přípustná (a dokonce žádoucí) redundantní propojení. Pochopitelně nutno podmínkou provozuschopnosti sítě je souvislost grafu sítě, tedy existence neméně jednoho spojení mezi každými 2 uzly. Hlavní zásadou budování Internetu je to, že každá síť má svou množinu adres, které se používají pouze uvnitř této sítě, a nelze je použít mimo ni. Tyto sítě, které jsou pomocí konkrétních rozsahů adres takto vymezeny, jsou pak mezi sebou propojeny zásadně pomocí směrovačů.

Jak již bylo zmíněno výše, jsou IP sítě tvořeny dvěma druhy uzlů. Na jedné straně většina uzlů jsou koncové uzly neboli podle původní terminologie TCP/IP $**hostitelské počítače$** (host computers), což jsou nejčastěji pracovní stanice, servery, ale i tiskárny či faxy se síťovou kartou apod. Společným rysem těchto uzlů je $**připojení právě do jedné sítě$.** Zpravidla v početní menšině pak jsou uzly druhého typu, totiž $**směrovače$** (routery, dříve se pro ně používal termín gateway), které zajišťují propojení mezi 2 nebo více sítěmi.

Platí určitá pravidla pro nesměšování těchto typů uzlů, která sice nejsou závazná, avšak představují prakticky ověřená doporučení hodná následování. Podobně jako v lokálních sítích pravidlo, že server by neměl sloužit jako zároveň pracovní stanice, protože jeho funkci serveru (která je přirozeně důležitější, protože obsluhuje více uživatelů) to může ohrožovat, tak i v IP sítích platí, že směrovač by neměl plnit další funkce, a to z podobného důvodu.

Nejspíše by připadala v úvahu funkce serveru, neboť zejména v menších sítích se můžeme často setkat se směrovači postavenými na bázi PC (nejčastěji s OS Linux). Přesto se s takovým uspořádáním (nazývá se „multihomed host“) někdy setkáváme. U specializovaných směrovačů vestavěných typicky do stojanového modulu současné využití pro jiné funkce pochopitelně zpravidla nepřichází v úvahu, neboť zpravidla pracují se speciálním operačním systémem, který něco takového neumožňuje.

#4.4 Rozdělení TCP/IP do vrstev

#4.4.1 Vrstva síťového rozhraní a síťová vrstva

Koncepce nižších vrstev protokolové sady TCP/IP pramení ze stavu při vzniku ARPANETu, kdy bylo nutné propojit technologicky naprosto různé sítě. Proto bylo přijato rozhodnutí, že síťová vrstva vytvoří jednotné rozhraní mezi nejrůznějšími technologiemi používanými ve vrstvě síťového rozhraní a vyššími vrstvami TCP/IP. Architektura TCP/IP se nesnaží vytvořit své vlastní řešení i pro vlastní přenos dat, ale spoléhá na existující standardizovaná řešení (např. Ethernet, ATM, TokenRing, FDDI, ISDN, Frame Relay apod.).

Aby bylo možné překrýt různé přenosové technologie jednotnou síťovou vrstvou, musí nutně síťová vrstva využívat pouze těch služeb různých technologií ve vrstvě síťového rozhraní, které jsou schopny nabídnout všechny existující technologie. Z těchto důvodů není např. možné využít spolehlivého přenosu těch technologií, které to nabízejí (např. ATM). Ze stejných důvodů dokonce některé technologie působí při spolupráci s TCP/IP problémy, protože v TCP/IP se pro určité činnosti počítá s možností všesměrového vysílání na vrstvě síťového rozhraní, což některé technologie (opět např. ATM) nenabízejí. Z důvodů uvedených výše se na síťové vrstvě používá přenosový protokol, který je nespolehlivý a nespojovaný. Z týchž důvodů se zavádí jednotné adresování pomocí 32-bitových adres, které v sobě zahrnují část identifikující síť, a část identifikující uzel v rámci sítě. Vzhledem k tomu, že jsou použity virtuální IP adresy, které neobsahují žádnou informaci o adresách z vrstvy síťového rozhraní, bylo nutné vytvořit převodní mechanismy mezi adresami fyzickými (linkovými) a virtuálními IP adresami. Síťová vrstva musí také mít k dispozici některé další informace o vlastnostech vrstvy síťového rozhraní, která pracuje pod ní. Jde především o parametr MTU (Maximum Transfer Unit), který určuje maximální velikost rámce, který může vrstva síťového rozhraní přenést.

Jak již bylo uvedeno výše, protokolová sada TCP/IP nedefinuje protokoly síťového rozhraní, ale pouze to, jak navázat službu síťové vrstvy na služby vrstvy síťového rozhraní, kde mohou být používány různé protokoly (též označované jako přenosové technologie), např. Ethernet, IEEE 802.11 (tzv. WiFi) atd. Tyto technologie samotné však nejsou protokolovou sadou TCP/IP definovány.

Určitou výjimku představují protokoly SLIP a PPP určené pro provoz na dvoubodových spojích. Důvod jejich vzniku je nasnadě: uživatelé potřebovali jednoduché protokoly pro provoz na dvoubodových spojích (často využívaných pro připojení malých sítí nebo jednotlivých počítačů k TCP/IP sítím), a tyto protokoly nebyly v době vzniku SLIP k dispozici.

#4.4.2 Vyšší vrstvy - transportní a aplikační

Funkce transportní vrstvy v TCP/IP jsou podobné jako v referenčním modelu ISO/OSI, odlišné je však uspořádání vrstev nad ní. Na rozdíl od 3 vrstev ISO/OSI je zde pouze jediná vrstva, totiž aplikační. Znamená to, že všechny funkce, které jsou v referenčním modelu ISO/OSI svěřeny 3 aplikačně orientovaným vrstvám (vrstvě aplikační, prezentační a relační), musí v TCP/IP zajistit samotná aplikační vrstva. Je to ostatně v souladu s filosofií TCP/IP, která se snaží zatěžovat režií jen ty entity, které využívají služby tuto režii vyžadující.

Znamená to tedy, že zatímco v ISO/OSI musí např. služby prezentační vrstvy, která zabezpečuje mimo jiné konverze dat, využívat všechny aplikace, v TCP/IP si tyto služby zajišťuje aplikace sama, proto ta, která tyto služby nepotřebuje, nenese jejich režii.

Na druhé straně má tento přístup nevýhodu v tom, že některé služby (např. právě již zmiňované konverze dat) se musí programovat vícekrát. Ovšem to plně platilo jen do doby začlenění protokolu NFS mezi aplikační protokoly sady TCP/IP. Jeho samostatně použitelnou součástí totiž byly také protokoly RPC (Remote Procedure Call) a XDR (eXternal Data Representation), které volitelně nabízejí opakovatelně použitelné funkce, které by v rámci referenčního modelu byly zřejmě zařazeny právě do relační a prezentační vrstvy.

Mezi nejdůležitější aplikace v aplikační vrstvě (bývají často označovány jako služby) patřila původně elektronická pošta (protokoly SMTP, POP, později IMAP), přenos souborů (protokol FTP) a vzdálené přihlašování (telnet). Původním aplikacím plně vyhovoval princip maximální snahy, protože nutně nevyžadují žádné garantované parametry přenosu. Později k nim přibyly další aplikace (např. sdílení souborů pomocí protokolu NFS, prezentace obsahu stránek pomocí WWW, chat apod.), pro něž již princip maximální snahy již představoval určité omezení funkčnosti, ne však zásadního charakteru. V případě dostatečné přenosové kapacity i tyto aplikace fungují bez problémů.

Je nutno si uvědomit, že všechny aplikace v TCP/IP jsou založeny na výpočetním modelu klient/server, tedy na jedné straně stojí klientský program poskytující dané služby (např. WWW server), proti němu stojí na druhé straně příslušný klient (v uvedeném příkladě web prohlížeč).

#4.5 Omezení architektury TCP/IP

Během vývoje TCP/IP se objevily i aplikace, pro které je fungování aplikační vrstvy v TCP/IP nevhodné. Jedná se jednak o aplikace vyžadující distribuci identických dat od jednoho zdroje k více příjemcům (např. hromadný přenos rozhlasového, televizního či video signálu apod.). Je zřejmé, že distribuce většího množství dat pomocí dvoubodových spojení klient-server je neefektivní, při větším množství klientů dokonce může být i technicky nemožná.

Některé z výše zmíněných aplikací narážejí v TCP/IP na další problém, kterým je neexistující podpora tzv. Quality of Services (QoS) neboli kvality služeb, což znamená, že v TCP/IP není bez dalších technických nebo organizačních opatření (z nichž některá se postupně stávají i standardy) možné garantovat např. omezenou velikost přenosového zpoždění, jeho omezené kolísání apod. To představuje zásadní omezení především pro aplikace, které potřebují přenášet v reálném čase např. videosignál, zvuk apod.

Zřejmě nejčastěji zmiňovaným problémem TCP/IP je nedostatečná bezpečnost. Zde se však jedná spíše o nepochopení, než o skutečný problém. Autoři TCP/IP neměli v úmyslu žádné důmyslnější bezpečnostní mechanismy vytvořit, neboť vycházeli z toho, že pokud nějaká aplikace bude zabezpečení požadovat, musí si je zabezpečit sama. Důvodem k tomuto přístupu byla mimo jiné již zmiňovaná filosofie minimalizace režie, tedy snaha neklást režii za zabezpečovací mechanismy na ty uživatele, kteří je nevyžadují. Navíc v době vzniku TCP/IP se nepočítalo s jeho hromadným rozšířením do komerční sféry, kde jsou požadavky na bezpečnostní mechanismy typicky vyšší.

Problém nastal v okamžiku, kdy běžné aplikace TCP/IP (např. elektronickou poštu) začali používat uživatelé bez dostatečných informací i pro přenos citlivých dat. Nebyli si přitom vědomi skutečnosti, že svěřit obchodní dopis běžnému e-mailu je z hlediska zabezpečení obsahu před přečtením nepovolanou osobou totéž jako jej poslat na korespondenčním lístku, což by jistě učinil málokdo. Na rozdíl od výše zmiňovaných

problémů s distribučními aplikacemi či chybějící podporou QoS lze však bezpečnostní mechanismy do aplikací na aplikační vrstvě poměrně snadno začlenit.

#4.6 Další aspekty TCP/IP

#4.6.1 Standardizace v TCP/IP

V počátcích vývoje protokolové sady TCP/IP se jako víceméně univerzální komunikační nástroj vyvinuly dokumenty RFC pojmenované podle původního určení Request for Comment (žádost o komentář).

Dokumenty RFC, jakmile jsou oficiálně vydány, se nikdy nemění. Při vydání je každému RFC dokumentu trvale přiděleno pořadové číslo. Dokumenty RFC jsou volně dostupné, jejich přehled je k dispozici např. na adrese http://www.ietf.org/iesg/1rfc_index.txt. Dokumenty RFC se dělí na 2 skupiny:

- standard (dokumenty popisující standardy TCP/IP)
- off-track (ostatní dokumenty, zejména informativní, experimentální, prototypové, historické apod.)

V případě, že je třeba popsat určitou skutečnost novým (např. v definici nové verze některého protokolu), se původní RFC dokument označí jako zastaralý (obsolete), avšak zůstává v původní podobě. Nový text je vydán v novém RFC dokumentu. Vzhledem k tomu, že RFC dokumentů je velké množství (početně výrazně převažují off-track dokumenty), je orientace v nich např. při vyhledávání určitého standardu poněkud obtížná. Proto vznikly tzv. dokumenty STD, které obsahují vždy aktuální RFC dokument popisující příslušný standard. Ten však přitom však zůstává součástí řady RFC dokumentů.

Standardizace je řízena standardizačními orgány zastřešenými organizací ISOC (Internet Society Nejdůležitější výkonnou roli v tomto procesu hraje organizace Internet Engineering Task Force (IETF). Zájemci mohou úplné informace nalézt např. na stránce Internet Architecture Board (IAB) na adrese http://www.iab.org

Samotný proces a standardizace má 3 fáze, kterými musí projít každý normotvorný dokument RFC. Tyto fáze se označují:

- Proposed Standard (návrh standardu), jehož podmínkou jsou dvě nezávislé implementace;
- Draft Standard (vyžadují se provozní zkušenosti);
- Internet Standard (konečná podoba standardu).

Faktické vytváření návrhů standardů bylo dříve zajišťováno pracovními skupinami ustavovanými IETF, dnes jsou pracovní skupiny ustavovány převážně jen pro dohled nad samotným procesem standardizace, zatímco vytváření a předkládání návrhů je plně v režii soukromých firem, neboť mnohé z nich považují skutečnost, že se některá technologie vyvinutá původně jako proprietární řešení (pouze pro zákazníky dané firmy či uživatele jejích výrobků) stane součástí veřejných standardů RFC, za zvýšení vlastní prestiže.

#4.6.2 Dohled nad fungováním Internetu

K tématu TCP/IP nepochybně patří i dohled nad fungováním Internetu, neboť způsob fungování Internetu ovlivňuje také fungování jiných TCP/IP sítí, zejména těch, které jsou nebo později budou s Internetem propojeny. Subjektem, který má fungování Internetu na starost, je organizace ICANN. Jde o sdružení podnikatelských, akademických i jiných subjektů z celého světa, převážně organizací, které v roce 1998 nahradilo organizaci IANA a převzalo její činnost.

Hlavní činnosti, které ICANN zajišťuje, jsou:

- koordinace technické správy systému doménových jmen Internetu (DNS);
- koordinace přidělování IP adres z adresního prostoru;
- koordinace přiřazování čísel protokolů (tzv. dobře známých portů);
- správa systému kořenových DNS serverů.

Kromě těchto úkolů se ICANN zabývá i jinými otázkami a problémy dlouhodobějších charakteru s cílem zachování a zlepšování svobodné konkurence na Internetu při zachování jeho provozní stability.

#4.6.3 Vztah TCP/IP a Internetu

Vztah protokolové sady TCP/IP a Internetu je mnohostranný, avšak pro správné pochopení procesů, které se v oblasti TCP/IP a Internetu odehrávají, je tento vztah důležité pochopit. Protokolová sada TCP/IP je „technologie“, která vznikla v Internetu či přesněji spolu s ním, jak bylo popsáno výše. Přitom však použití TCP/IP není vázáno na Internet, dnes existuje mnoho sítí používajících technologie TCP/IP, které k Internetu nejsou připojeny. Protože však je Internet největší světovou sítí využívající TCP/IP, určuje vývoj v Internetu vývoj celé architektury TCP/IP.

$Shrnutí obsahu kapitoly$

V této úvodní kapitole jsme se seznámili se vznikem protokolové sady TCP/IP, s jej filosofií (otevřenost, snaha o jednoduchost), a dále s vrstevnatým uspořádáním TC 4 vrstev (vrstva síťového rozhraní, vrstva síťová, transportní v., aplikační v.) a jejic funkcemi. Jistě jste si zapamatovali, že v TCP/IP, především na síťové vrstvě, se uplatňuje princip přepojování paketů, jehož důsledkem je, že služby poskytované síťovou vrstvou nemají žádnou garantovanou kvalitu, a jsou poskytovány na bázi principu maximální snahy (best effort). Rovněž již víme, jakým způsobem vznikají standardy TCP/IP a jakou mají formu, a kdo se stará o každodenní fungování Internetu.

$Pojmy k zapamatování:$

- Princip přepojování paketů
- Princip maximální snahy (best effort)
- Nespolehlivá nespojová komunikace
- 4 vrstvy TCP/IP
- RFC
- IETF, IAB
- ICANN

$Kontrolní otázky:$

1. Co znamená princip „best effort“ a na jaké vrstvě se princip „best effort“ uplat
2. Jaké jsou hlavní přednosti TCP/IP?
3. Jaké má TCP/IP nedostatky?

$Korespondenční úkoly:$

1. Napište, k čemu ve své práci či studiu používáte služby sítí na bázi TCP/IP.
2. Najděte na Internetu webové stránky všech organizací a orgánů jmenovaných v vyhledejte si tam seznam RFC dokumentů a ustavující dokumenty ISOC. Nalezené URL pošlete tutorovi.

#5 Protokoly transportní vrstvy

$Obsah kapitoly$

~Průvodce studiem

Tato kapitola se zabývá problematikou fungování transportní vrstvy protokolové sad TCP/IP. Seznámí Vás s protokoly TCP a UDP, z nichž si mohou aplikace vybrat ten, lépe vyhovuje jejich požadavkům, a s rozdíly mezi nimi.&

$V této kapitole se dozvíte:$

1. Jaké jsou vlastnosti transportní vrstvy protokolové sady TCP/IP?
2. Jaké protokoly se používají pro přenos dat v transportní vrstvě TCP/IP?
3. Jaké jsou vlastnosti protokolů TCP a UDP?

$Po jejím prostudování byste měli být schopni:$

1. Specifikovat funkce protokolu TCP a uvést hlavní položky jeho paketu (segmentu);
2. Specifikovat funkce protokolu UDP a uvést hlavní položky jeho paketu;
3. Charakterizovat odlišnosti protokolů TCP a UDP a uvést případy, kdy je pro aplikací výhodné použít protokol TCP a kdy UDP.

~Klíčová slova této kapitoly:

Vrstva transportní, protokol TCP, spolehlivá přenosová služba, bytová roura, protok

Doba potřebná ke studiu: 1,5 hodiny&

#5.1 Funkce transportní vrstvy

Obecnou funkcí transportní vrstvy je přizpůsobovat možnosti vrstev nižších (reprezentovaných službami síťové vrstvy) požadavkům vrstev vyšších. Konkrétně v TCP/IP jde především o přizpůsobení nespolehlivé a nespojované služby protokolu IP (síťové vrstvy) častému požadavku mnoha aplikací na spolehlivý spojovaný přenos. Těmto požadavkům se umí transportní vrstva TCP/IP přizpůsobit, přitom však dává aplikacím možnost volby, takže ty aplikace, které požadují spolehlivost, použijí protokol TCP, kdežto ty, které preferují rychlost a spolehlivou službu nepotřebují, použití protokol UDP.

Naopak požadavku na garanci určitého maximálního zpoždění přenosu či garanci jiného parametru přenosu dosud transportní vrstva TCP/IP vyhovět neumí. Přitom tyto požadavky se stále častěji objevují spolu s rostoucími požadavky uživatelů a aplikací na přenosy multimediálních dat. Na řešení tohoto problému se pracuje, avšak protože jde o značný zásah do filosofie TCP/IP, uspokojivé řešení zachovávající výhody TCP/IP dosud neexistuje.

Vedle přizpůsobení je další funkcí transportní vrstvy rozlišování paketů či datových toků podle jejich příslušnosti k určitým procesům v aplikační vrstvě. Tato funkce se nazývá multiplexování a demultiplexování. Bez ní by nebylo možné například provozovat (mít spuštěný) na stanici současně program pro práci s elektronickou poštou a prohlížeč WWW, což by dnes, v době nadvlády víceúlohových operačních systémů na stanicích bylo jistě nepohodlné. Ještě horší by bylo, že na jednom fyzickém serveru by nemohl běžet proces sloužící jako WWW server zároveň např. s FTP serverem, a dokonce by ani jeden WWW

server nemohl zároveň komunikovat s více uživateli. K tomuto rozlišení se na transportní vrstvě TCP/IP používají tzv. $**porty$.**

Port je přechodovým bodem mezi aplikační vrstvou a transportní vrstvou, k nimž se mohou aplikace podle potřeby asociovat. Přitom jedna aplikace může využívat více portů, ale pochopitelně jeden port nesmí být současně používán více aplikacemi.

Porty jsou identifikovány svými čísly, jejichž tvar je nezávislý na platformě (vždy se jedná o celá kladná čísla). Tato čísla představují relativní adresu v rámci uzlu. Programy obvykle přistupují k portům prostřednictvím tzv. socketů, které jsou součástí příslušného programátorského rozhraní (API).

Význam některých portů je pevně dán, neboť je přidělila IANA (předchůdce ICANN) příslušným aplikacím. Jde o tzv. dobře známé porty (v rozsahu 1-1023), na nichž jsou poskytovány standardní služby. Jejich přidělení je uvedeno v RFC 1700, později je přidělení aktualizováno pouze on-line. Smyslem existence tzv. dobře známých portů je tedy to, aby klientský program věděl, na jakém portu bude server očekávat jeho požadavky pro určitou službu a aby tedy uživatel nemusel číslo portu na serveru zadávat do URL (např. www klient si automaticky doplní číslo portu 80 k URL zadané uživatelem, pokud ovšem uživatel nezadal jiné číslo portu).

Z výše uvedeného tedy vyplývá, že spojení mezi aplikacemi na dvou uzlech je definováno pěticí údajů, tedy:

- transportní protokol (TCP nebo UDP);
- IP adresa odesílatele;
- port odesílatele;
- IP adresa příjemce;
- port příjemce.

#5.2 Služby transportní vrstvy

Jak bylo uvedeno výše, transportní vrstva umožňuje aplikaci, aby si zvolila, který typ služby bude používat. Proto jsou na transportní vrstvě definovány 2 odpovídající typy služby a navíc ještě jeden typ speciální. Konkrétně se jedná o tyto typy:

- **$stream$**, kdy transportní vrstva vytváří iluzi bytového proudu. V tomto případě jsou data přijímána a vydávána po bytech, členění na bloky je pro aplikaci transparentní, tedy se provádí pouze interně pro potřeby přenosu. Přenos je spolehlivý, je garantováno pořadí dat, do služby je začleněno řízení toku. Tuto službu nabízí protokol TCP.
- **$datagram$**, kdy transportní služba vytváří iluzi blokového přenosu. Data jsou členěna do bloků (datagramů), přenášena jsou nespolehlivě, bez garance pořadí, ztrát či duplicit. Tato služba neobsahuje řízení toku. Tuto službu nabízí protokol UDP.
- **raw**, což je speciální režim umožňující přímý přístup ke službám nižších vrstev. Používá se pro testovací účely, pro utility typu PING apod.

#5.3 Protokoly transportní vrstvy

#5.3.1 Protokol UDP

Protokol UDP představuje prakticky pouze jednoduchou nadstavbu nad protokolem IP. Nemění charakter jeho služeb, neboť UDP poskytuje nespolehlivou a nespojovou službu. Navíc zajišťuje pouze multiplexing a demultiplexing v rámci uzlu. Definice protokolu UDP zahrnuje možnost vytváření kontrolního součtu celého paketu, avšak jedinou reakcí tohoto

protokolu při doručení paketu s kontrolním součtem je zahození paketu. Vytváření kontrolního součtu lze vypnout.

Protokol UDP používají ty aplikace, které potřebují co nejrychlejší doručení dat a nejsou přitom závislé na tom, zda data budou doručena všechna. Vyšší rychlost UDP proti TCP je dána tím, že UDP není zatížen režií spojenou s vytvářením a rušením spojení, potvrzování doručení a dalšími mechanismy zabezpečení.

Vlastnosti UDP již byly zmíněny výše, proto jen zopakujeme. Jde o protokol:

- nespolehlivý;
- nespojový;
- vytvářející iluzi blokového přenosu (maximální velikost bloku je 2^{16}-20-8 bytů; první údaj je max. velikost IP paketu, 20 je minimální délka hlavičky IP paketu a 8 je délka hlavičky UDP datagramu, jak uvidíme později).

Protokol UDP může být použit i pro rozesílání všesměrových (broadcast) paketů nebo paketů pro více příjemců (multicast), což u TCP není možné (protože vytváří spojení, které nemůže spojovat více než 2 body). Komunikace pomocí protokolu UDP je bezestavová, takže si komunikující strany nemusí pamatovat předchozí historii komunikace a mohou kdykoli (přesněji řečeno po odeslání nebo přijetí kteréhokoli UDP datagramu) komunikaci přerušit nebo v ní znovu pokračovat.

UDP datagram je velmi jednoduchý. Zahrnuje pouze 8-bytovou hlavičku obsahující zdrojový port, cílový port, délku datagramu a kontrolní součet. Jak bylo zmíněno výše, generování kontrolního součtu je volitelné. Kontrolní součet se zde generuje z celého UDP datagramu (hlavičky i dat) a navíc ještě z tzv. $**pseudohlavičky$**. Pseudohlavička je virtuální struktura, která nikde reálně neexistuje, a používá se právě jen pro generování kontrolního součtu. Obsahuje ve 12 bytech nejdůležitější údaje z hlavičky IP paketu, především zdrojovou a cílovou IP adresu. Pokud se kontrolní součet generuje, kontroluje se při doručení datagramu a v případě neshody vypočteného součtu s údajem v hlavičce se datagram zahodí bez jakéhokoli oznámení odesílateli (na rozdíl od IP protokolu).

#5.3.2 Protokol TCP

Protokol TCP poskytuje službu spojovaného charakteru. Znamená to, že pro přenos dat se nejprve ustaví spojení mezi odesílatelem a příjemcem (vždy jedinými, tedy vždy se jedná o dvoubodové spojení), po něm se přenesou data a po přenosu dat se spojení ukončí. Standardně jde o spojení duplexní, tedy obousměrné. Služba protokolu TCP vytváří pro aplikace iluzi bytového toku. Zajišťuje plnou spolehlivost a řízení toku paketů, při kterém se odesílatel snaží přizpůsobit schopnostem příjemce.

Spojovaná služba protokolu TCP je pouze iluzí pro aplikaci, protože IP protokol na síťové vrstvě funguje pochopitelně stále nespojovaně. Proto musí protokol TCP ošetřit všechny stavy, k nimž může na síťové vrstvě dojít, jako např. restart uzlu, ztrátu dat způsobenou nespolehlivostí přenosové infrastruktury, změnu pořadí dat apod. Mezilehlé uzly (směrovače) o protokolu TCP nevědí, protože funguje až na transportní vrstvě.

Spojení se vytváří pomocí tzv. $**3-fázového handshakingu$**, což je způsob, jimž se v protokolu TCP navazuje (a též ruší) spojení. Postup je následující:

1. Uzel, který iniciuje navázání spojení, pošle TCP segment s nastaveným bitovým příznakem SYN (synchronize);
2. Druhá strana odpoví TCP segmentem, který má nastaven příznak SYN a ACK (Acknowledge), přičemž zároveň potvrdí v poli Acknowledgement Number číslo, které v poli Sequence Number předchozího segmentu zaslal iniciátor spojení jako počátek

číslování dat. V poli Sequence Number tohoto druhého segmentu bude navržený počátek číslování pro opačný směr.

3. Uzel, který inicioval navázání spojení, pošle druhé straně TCP segment s nastaveným příznakem ACK.

Spolehlivost v protokolu TCP je zajišťována především pomocí techniky tzv. kontinuálního potvrzování. Příjemce generuje po přijetí TCP paketu (který se obvykle nazývá **$TCP segment$**) kladná potvrzení. Odesílatel monitoruje dobu obrátky (tedy dobu od odeslání TCP segmentu do přijetí potvrzení) a podle váženého průměru doby obrátky a jejího rozptylu počítá dobu, po kterou čeká na potvrzení. Výsledkem je, že doba, po kterou se čeká na potvrzení, je o něco vyšší než průměrná doba obrátky, přičemž velikost zvýšení čekací doby nad průměrnou dobu obrátky je úměrná rozptylu doby obrátky.

Tento postup vcelku uspokojivě reaguje jak na prodlužování doby obrátky, tak na její zkracování, a to bez ohledu na skutečnou velikost průměrné doby obrátky, která je pochopitelně vyšší v rozlehlých sítích a výrazně nižší naopak v lokálních sítích.

Protokol TCP používá nesamostatného potvrzování, což znamená, že údaj potvrzující přijetí dat (číslo bytu, který byl jako poslední správně přijat), je vložen do určeného pole (Acknowledgement Number) v hlavičce protisměrného TCP segmentu. Tento způsob potvrzování se nazývá piggybacking.

Jak bylo uvedeno dříve, vytváří služba protokolu TCP pro aplikaci iluzi bytového proudu, tedy aplikace předává data protokolu TCP po bytech. TCP protokol si tato data sám „bufferuje“ neboli seskupuje do skupin odpovídajících množství volného místa a po naplnění velikosti bufferu (jehož velikost závisí na parametru MTU). Aby bylo možné data odeslat v případě potřeby okamžitě (např. při předávání dat ve formě souboru po dosažení jeho konce), má aplikace možnost vyžádat si okamžité odeslání obsahu bufferu i před jeho úplným naplněním.

Vzhledem k tomu, že protokol TCP nepracuje s bloky, musí zajistit číslování pozice v bytovém proudu. K tomu se používá 32-bitové číslo. Počáteční hodnota se volí náhodně (přesněji řečeno tak, aby se brzy po sobě neopakovala stejná čísla), tedy neplatí, že pozice prvního byte má číslo 1.

Protokol TCP řídí tok dat tak, aby odesílatel nezahlcoval příjemce a nedocházelo kvůli tomu ke ztrátě dat. Toho se dosahuje použitím tzv. metody okénka. Okénko udává velikost volného místa pro příjem dat. Tato velikost okénka je signalizována spolu s každým potvrzením o přijetí TCP segmentu. Odesílatel vysílá jen tolik dat, kolik odpovídá aktuálně volnému okénku, a vysílání obnoví až tehdy, když mu bude příjemce signalizovat zvětšení volného okénka.

V případě, že během zasílání řady TCP segmentů dojde ke ztrátě některého ze segmentů, a tedy odesílatel neobdrží potvrzení doručení tohoto segmentu, přejde odesílatel z kontinuálního potvrzování na potvrzování jednotlivých segmentů. To znamená, že odesílatel odesílá jednotlivé segmenty až po obdržení potvrzení doručení předchozího segmentu, namísto aby odesílal tolik segmentů, kolik odpovídá velikosti volného okénka. Ke kontinuálnímu potvrzování přechází odesílatel postupným zdvojnásobováním množství odesílaných dat a v případě včasného doručení potvrzení se takto pokračuje až do dosažení velikosti volného okénka.

$Shrnutí obsahu kapitoly$

V této kapitole jste se seznámili s vlastnostmi transportní vrstvy. Zejména je důležité zapamatovat, že zde jsou k dispozici dva alternativní přenosové protokoly, TCP a

se liší svými vlastnostmi. Protokol TCP poskytuje spolehlivé spojové služby, zatímco protokol UDP služby nespolehlivé nespojové. Mezi protokoly TCP a UDP si mohou aplikace vybírat ten, který lépe vyhovuje jejich potřebám a požadavkům na přenosové služby. Oba tyto protokoly přitom využívají služeb nespolehlivého protokolu IP na síťové vrstvě.

$Pojmy k zapamatování:$

- Protokol TCP
- Protokol UDP

#Kontrolní otázky

1. Proč je nutné pro různé služby použít různé porty transportní vrstvy?
2. Na jakém principu pracuje protokol TCP?
3. Jaké mechanismy používá TCP protokol k zajištění spolehlivosti?
4. Co znamená použití 3-fázového handshake protokolem TCP?&

#Korespondenční úkoly

1. Posuďte na základě vlastností, které byste očekávali od služby přenosu souboru měla používat protokol TCP nebo UDP. Svou úvahu si můžete později ověřit v vlastnostech protokolu FTP.
2. Pomocí vhodného programu pro zachycování paketů (např. Wireshark) zachyťte libovolnou komunikaci se serverem, ke které se používá protokol TCP (např. zobrazení www stránky) a zjistěte, jaké údaje se zasílají mezi klientem (stranou inciující navázání spojení) a serverem při navázání spojení. Nápověda: při 3 krocích navázání spojení se používají 1-bitové příznaky SYN a ACK.
3. Podobně jako v případě navázání spojení zjistěte, kolik kroků má ukončení spojení, jaké jsou jeho druhy (jaké příznaky se používají) a jaké informace se při něm předávají.&

#6 IP adresy

$Obsah kapitoly$

~Průvodce studiem

Na studium této kapitoly doporučuji si vyhradit alespoň 1,5 až 2 hodiny času. V rám doby byste měli stihnout zpracovat i korespondenční úkol. Nevynechávejte ani řešen příklady, jejich prostudování umožní lepší pochopení práce s IP adresami.&

$V této kapitole se dozvíte:$

1. Jaké adresy se používají v protokolové sadě TCP/IP?
2. Jaké existují třídy IP adres a k čemu slouží?
3. Proč se dnes již mechanismus tříd nepoužívá a co jej nahrazuje?
4. Jaké existují způsoby řešení nedostatku nových IP adres?

$Po jejím prostudování byste měli být schopni:$

1. Definovat jednotlivé třídy IP adres;
2. Popsat využití maskyů
3. Uvést, kdo a jakým způsobem dohlíží na přidělování IP adres;
4. Charakterizovat příčiny nedostatku IP adres a mechanismy jeho řešení.

~Klíčová slova této kapitoly:

IP adresa, vrstva síťová, subnetting, maska podsítě, CIDR, supernetting, privátní IP a ICANN.

Doba potřebná ke studiu: 2 hodiny&

#6.1 Struktura IP adres, třídy IP adres, distribuce adres

IP adresy jsou adresy, které se používají na síťové vrstvě a vyšších vrstvách protokolové sady TCP/IP. Aby mohly sloužit svému účelu, kterým je identifikace uzlů v rámci celé sítě TCP/IP (např. celého Internetu), musí být zajištěna jedinečnost přidělených adres v rámci celé této sítě.

IP adresy v sobě přitom nenesou žádnou explicitní informaci o adrese fyzické neboli linkové a proto se nijak navzájem neliší IP adresy, které patří uzlům připojenými k sítích s odlišnou přenosovou technologií. Velikost IP adresy je 32 bitů.

IP adresy jsou fyzicky jednosložkové, přestože obsahují část označující adresu sítě, a část identifikující uzel v dané síti. Hranici mezi oběma částmi adresy tvoří určitá bi pozice. Je přitom zřejmé, že pokud by bylo umístění této hranice pevně stanoveno, by k velkému plýtvání adresami, neboť hranice by zřejmě musela být nastavena tal vyhovovala i velkým sítím, a proto by malé sítě, kterých je početně jistě velká větš adresami velmi plýtvaly. Vzhledem ke koncepci IP adres totiž není možné, aby měly dvě různé sítě síťovou část adresy shodnou.

$Příklad$

Například při pevném rozdělení IP adresy na polovinu (16 bitů pro adresu sítě a 16 bitů pro adresu uzlu) by v síti o 1000 uzlech zůstalo nevyužito přes 64 tisíc adres (přesně 64 536), což je přes 98 procent.

$Úkol k textu$

Zkuste si sami spočítat, jak velká je ztráta počtu IP adres při 500 uzlech v síti, pok
použita pevná velikost síťové části adresy 16 bitů.

Z výše uvedeného vyplývá, že hranice mezi síťovou částí a uzlovou částí IP adresy musí být do jisté míry pohyblivá. Původní koncepce IP adres počítala s tím, že informace o tom, kde se zmíněná hranice mezi síťovou a uzlovou částí adresy nachází, ponese adresa určitým způsobem v sobě, a proto byly definovány 3 tzv. třídy adres:

- Adresy třídy A, které mají síťovou část dlouhou 8 bitů a uzlovou část 24 bitů, jsou určeny pro největší sítě. Rozlišovacím znakem je, že jejich první bit je nulový.
- Adresy třídy B, které mají síťovou část dlouhou 16 bitů a uzlovou část rovněž 16 bitů, jsou určeny pro středně velké sítě. Rozlišovacím znakem je, že jejich první bit má hodnotu 1 a druhý bit 0.
- Adresy třídy C, které mají síťovou část dlouhou 24 bitů a uzlovou část 8 bitů, jsou určeny pro malé sítě. Rozlišovacím znakem je, že jejich první dva bity mají hodnotu 1 a třetí bit 0.

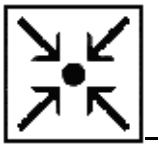
Upozorňujeme zde na to, že vzhledem k tomu, co bylo uvedeno výše, se IP adresy přidělují po celých blocích, a proto se často pod pojmem „adresa třídy ...“ míní celý blok adres se stejnou síťovou částí, tedy např. v případě adresy třídy C všech 256 možných adres, přestože jednotné číslo by naznačovalo, že se jedná o jednotlivou adresu.

$Úkol k zamyšlení$

Zkuste si spočítat, jak velkou část adresového prostoru IP adres zabírají adresy tříd
třídy B a adresy třídy C. Proč myslíte, že je rozdělení určeno tak, že se všechny 3 t
adresní prostor nedělí rovnoměrně?

Pro snazší práci lidí s IP adresami (pro účely různých úkonů spojených s konfigurací sítě apod.) je třeba, aby si IP adresy bylo možné zapamatovat. Binární vyjádření není pro lidské vnímání (na rozdíl od počítačové paměti) vhodné, proto se obvykle používá jiný způsoby zápisu IP adres. Ten je založen na tom, že se IP adresa rozdělí na 4 byty (skupiny po 8 bitech) a ty se převedou na desítkové číslo. Takto vzniklá 4 desítková čísla se zapíší vedle sebe oddělené tečkami.

$Příklad$



IP adresa binárně vyjádřená číslem **11000000101010001111111100000001** má sy
vyjádření **192.168.255.1.**

$Úkol k textu$

Převeďte binární IP adresu **00001010000000010000000100110111** na symbolický
využívající desítkových čísel.

#6.1.1 Distribuce adres

Vzhledem k požadavku jedinečnosti IP adres v celé IP síti je nutno ve velkých sítích zajistit distribuci nově přidělovaných IP adres. Tento problém je nejzávažnější v Internetu, neboť se jedná o nejrozsáhlejší IP síť obepínající dnes již prakticky celý svět. Musí proto existovat organizace, která bude přidělování IP adres řídit. Touto organizací je ICANN zmíněná v lekci 1. ICANN přiděluje IP adresy hierarchicky prostřednictvím pověřených regionálních organizací. Pro Evropu jde o organizaci RIPE. RIPE přiděluje bloky IP adres buď přímo (zpravidla nadnárodním poskytovatelům služeb Internetu, tzv. ISP), nebo prostřednictvím národních organizací s působností v určitém státě.

Je třeba si také uvědomit skutečnost, že ne všechny číselné kombinace, které vypadají jako IP adresy, lze skutečně použít k adresování konkrétního uzlu. Pokud pomineme adresy z rozsahu mimo třídy A, B a C (kde jsou vymezeny další třídy D a E, ale adresy třídy D se přidělují pouze pro použití multicastingu (to je mechanismus pro rozesílání IP paketů více příjemcům současně, jímž se v tomto textu nezabýváme), a adresy třídy E se nepřidělují prakticky vůbec), pak i z adresního rozsahu tříd A, B a C musíme některé adresy odstranit. Jednak jsou to adresy vyhrazené jako privátní, které nejsou nikomu přiděleny (jejich rozsahy jsou uvedeny dále), pak jde o adresy mající v prvním bytu hodnotu 127 (to je tzv. loopback neboli smyčka sloužící např. k testování programů), a některé další.

Ale i z každého přiděleného bloku adres musíme vždy 2 krajní (nejvyšší a nejnižší) odečíst. Adresa, která má v uzlové části samé nuly, je symbolická adresa celé sítě, naproti tomu adresa, která má v uzlové části samé jedničky (binárně), je adresou oběžníku pro danou síť (tedy pokud pošleme paket na tuto adresu, obdrží ho všechny uzly v dané síti, tedy všechny uzly se stejným síťovým prefixem). Tyto speciální adresy samozřejmě nelze využít pro adresování běžných uzlů v žádné síti.

#6.1.2 Adresní prostor IP adres

V důsledku nečekaně prudkého nárůstu uživatelů Internetu od počátku 90. let došlo k tomu, že počet IP adres se začal rychle vyčerpávat. Je zřejmé, že celkový počet možných kombinací IP adres (přes 4 miliardy) by byl ještě dlouho dostatečný, ale způsob distribuce a přidělování adres byl i přes rozdělení IP adres do tříd poměrně neefektivní a nebyl připraven na tak vysoký počet uživatelů sítě. Proto byla hledána různá řešení tohoto problému.

Principiálním řešením by zřejmě byl přechod na IP protokol verze 6, který kromě jiných zlepšení přináší prodloužení adresy na 128 bitů a tím mnohonásobné rozšíření adresního prostoru. Přechod na IP protokol verze 6 již probíhá, avšak kvůli poměrně velkému množství potřebných změn probíhá přechod dosti pomalu a zejména formou budování paralelní „překryvné“ sítě na bázi IP verze 6, proto se budeme s protokolem IP stávající verze 4 jistě ještě několik let setkávat.

Z výše uvedených důvodů se dosud používají především dočasná řešení orientovaná na zefektivnění využívání stávajícího adresního prostoru.

#6.1.3 Subnetting

Jedním z takových řešení, které se používá zejména pro malé sítě, je vytváření tzv. podsítí (**subnetting**). Princip subnettingu spočívá v tom, že se hranice mezi síťovou a uzlovou částí adresy v určité konkrétní síti (bloku IP adres) posune směrem k nižším bitům (neboli se zvětší síťová část všech IP adresy v daném bloku na úkor jejich uzlové části), a díky tomu se může jedna síť (blok adres) rozdělit na několik menších sítí. Vzhledem k mechanismu rozdělení na podsítě založeném na posunu hranice mezi oběma částmi adresy není možné provádět dělení libovolně, ale pouze po mocninách čísla 2, neboť posun hranice mezi síťovou a uzlovou částí IP adresy musí být učiněn vždy o celočíselný počet bitů. Protože ne všechny mechanismy pro práci s IP adresami nejsou na subnetting připraveny, bylo nutné pro tento účel zavést tzv.

masky.

Maska je podobně jako IP adresa 32-bitové číslo, nese však jedinou informaci: počet bitů, který je v příslušné IP adrese vyhrazen pro identifikací sítě (tedy délka tzv. síťového prefixu). Tato informace se v masce vyjadřuje tak, že maska obsahuje (v binárním vyjádření) od počátku (od nejvyšších bitů) souvislý blok jedniček o počtu rovném počtu bitů síťového prefixu, a zbývající bity jsou doplněny nulami.

Maska se stala natolik univerzálním mechanismem popisujícím délku síťové části adresy (prefixu), že se dnes uvádí maska prakticky spolu s každou IP adresou, jejíž se stala nedílnou součástí. Navíc se dnes často (a možná vhodněji) místo termínu „maska podsítě“ používá pouze termín „maska“, čímž se vyjadřuje, že maska neslouží vždy jen k rozdělení jedné sítě na více podsítí.

Dělení na podsítě se provádí izolovaně, tedy tak, že informace o něm nejsou šířeny do zbytku sítě, jehož se toto rozdělení netýká. Schéma vytváření podsítí je zobrazeno na obr. 4.2.

$Příklad$

Maska příslušející k IP adrese **192.168.255.1** bude mít tvar **255.255.255.0**, protože uvedená IP adresa je třídy C, tedy délka síťového prefixu je 24 bitů. Maska vyjádřená binárně tedy bude mít hodnotu **11111111111111111111111100000000**. Pokud provedeme rozdělení takovéhoto bloku adres na dvě podsítě, musíme o jeden bit (jímž se budou tyto dvě podsítě rozlišovat) zvětšit délku síťové části adresy, tedy potom bude mít maska 25 bitů jedničkových, a její hodnota po převodu na dekadický tvar bude 255.255.255.128.

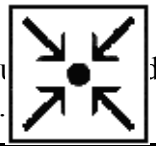
Vhodnou pomůckou pro procvičení práce s podsítěmi, maskami a prováděí výpočtů jsou různé tzv. subnet kalkulátory. Lze jich nalézt velké množství, dokonce jsou součástí některých operačních systémů. Jeden z takových kalkulátorů je uveden v seznamu odkazů po č. [12].

$Úkol k textu$

Určete masku příslušející IP adrese **126.0.0.5**.

Smysl subnettingu spočívá v tom, že umožňuje využití jedné síťové adresy (přesněji řečeno jedné skupiny adres určité třídy) pro více menších sítí. Bez subnettingu by bylo nutné pro každou takovou síť použít samostatnou adresu příslušné třídy, čímž by docházelo k plýtvání.

$Příklad$



Například pro 4 sítě po 50 uzlech je možno využít díky subnettingu celkem jednu adresu třídy C rozdělenou na čtvrtiny. Bez subnettingu by bylo nutné použít 4 adresy třídy C.

Je však nutno poznamenat, že subnetting lze použít pouze pro sítě navzájem blízké v tom smyslu, že mají $**jediný společný vstupní bod$**, který je propojuje se zbytkem sítě. Je to vynuceno tím, že informace o rozdělení do podsítí je lokalizována (není šířena dále do sítě). V případě více vstupních bodů by nebylo možné rozhodnout o tom, který se má použít.

#6.1.4 Privátní IP adresy

Dalším řešením je využití privátních IP adres. Privátní adresy se používají pro ty uzly v IP sítích, které nepotřebují přímo komunikovat s uzly mimo síť. Na první pohled se může zdát, že ve většině sítí takových uzlů mnoho nebude, neboť např. elektronickou poštou s obchodními partnery komunikuje dnes i mnoho řadových zaměstnanců v mnoha podnicích. Právě pro práci s elektronickou poštou a službou WWW jako zřejmě nejpoužívanějšími

službami Internetu však stanice přímou komunikaci se stanicemi mimo lokální síť nepotřebují, neboť komunikují pouze s poštovním serverem, který je zpravidla umístěn uvnitř téže lokální sítě a veškerou komunikaci mimo síť realizuje sám. V případě služby WWW tomu tak není, ovšem zde lze zase snadno použít tzv. proxy serveru, který pro pracovní stanice uvnitř sítě službu zprostředkuje. Toto uspořádání se velmi často používá, protože mimo jiné umožňuje do jisté míry kontrolovat využívání služby WWW, a také v menší míře přispívá ke zvýšení bezpečnosti sítě zneviditelněním jejích stanic zvenčí.

Privátní IP adresy se tedy mohou používat mnoha i poměrně rozsáhlých IP sítích, které pak vystačí s přidělením běžných (veřejných) IP adres pro několik málo uzlů. Je zřejmé, že základní podmínkou fungování privátních adres je zamezení šíření směrovacích informací ven ze sítě používající privátní adresy na jejích hranicích. Potom lze v takové síti jako privátní adresy použít adresy v zásadě libovolné. Přesto vzniklo doporučení, které rozsahy adres se mají používat jako privátní. Jedná se o tyto adresy:

- 1 adresu třídy A, konkrétně o adresy 10.0.0.0 - 10.255.255.255;
- 16 adres třídy B, konkrétně o adresy 172.16.0.0 - 172.31.255.255
- 256 adres třídy C, konkrétně o adresy 192.168.0.0 - 192.168.255.255

Důvodem vzniku tohoto doporučení byla skutečnost, že ne vždy musí být zajištěno skutečné zamezení šíření směrovacích informací o vnitřku sítě s privátními adresami hned na hranici sítě (například kvůli nesprávně nakonfigurovanému směrovači). Pokud bude použito privátních adres z výše uvedených doporučených rozsahů, zastaví šíření nesprávně zaslaných paketů každý další směrovač, neboť má informaci o tom, že jde o privátní IP adresy, které nemá směrovat. V případě použití jiných adres jako privátních to pochopitelně neplatí.

#6.1.5 Network Address Translation (NAT)

Spolu s privátními adresami se často používá mechanismu NAT, který za chodu překládá adresy používané uvnitř sítě na adresy používané mimo síť. Je popsán v dokumentu RFC 3022. Při překladu je možno s výhodou využít toho, že lze obvykle vystačit s překladem výrazně většího počtu privátních adres na menší počet adres veřejných. Přitom se využívá skutečnosti, že se na hraničním směrovači překládají nikoli samotné IP adresy, ale vždy dvojice IP adresa – port.

Použití privátních adres však naráží také na některé problémy. jejich rozbor je nad rámec tohoto textu, proto jen jako několik příkladů uvádím problémy s případným uváděním IP adresy v datové části paketu, se šifrováním apod.

#6.1.6 Classless InterDomain Routing (CIDR)

Dalším mechanismem pomáhajícím zpomalit úbytek IP adres, je mechanismus CIDR. Jde v zásadě o komplementární postup k subnettingu (z tohoto důvodu se také někdy označuje jako supernetting), který umožňuje, aby se sítím přidělovaly vždy vhodně velké rozsahy adres, neboť umožňuje posun hranice mezi síťovou částí adresy (nyní označovanou jako „prefix“) a uzlovou částí adresy. Prakticky tedy CIDR spolu s maskami nahrazuje systém rozdělení IP adres do tříd A, B a C.

CIDR je založen na agregaci sousedních adres sítí (ve smyslu podobnosti čísel, přesněji shodnosti nejnižších bitů síťové části adresy) ve směrovacích tabulkách. Nutnou podmínkou pro použití mechanismu CIDR je, aby sousední adresy byly přiděleny sousedním sítím ve smyslu hierarchie připojení. To si vynucuje, aby se do přidělování adres zapojili poskytovatelé připojení, kteří jedině jsou schopni toto zajistit.

V souvislosti s mechanismem CIDR se ujalo označování bloků adres ve formě tzv. CIDR bloků, které se zapisují jako IP adresa a za ní lomítko a za lomítkem počet bitů síťové části

adresy (prefixu). Tedy např. označení 198.199.200.0/23 znamená, že máme k dispozici všechny IP adresy, které mají prvních 23 bitů shodných s uvedenou IP adresou. Pro adresování uzlů nám tedy zbývá 9 bitů, celkový počet číselných kombinací je tedy 2^9, celkový počet použitelných IP adres je $2^9 - 2$. Důvod odečtení dvou krajních adres je vysvětlen v části pojednávající o speciálních IP adresách, jde totiž o IP adresu sítě a broadcastovou adresu.

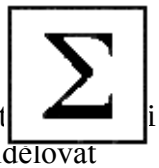
$Příklad$

Mějme 2 CIDR bloky 192.168.2.0/24 a 192.168.3.0/24. Ty lze sdružit do bloku 192.168.2.0/23, protože do 23. bitu včetně mají oba bloky stejné síťové prefixy a c slučované bloky dohromady pokrývají stejný rozsah jako nový blok (tato podmínka je nutná, aby byla obě vyjádření ekvivalentní!).
Naproti tomu třeba bloky 192.168.3.0/24 a 192.168.1.0/24 sdružit nelze, protože se liší již na 23. bitu. Bylo by však možné sdružit bloky 192.168.0.0/24 a 192.168.1.0/24 a 192.168.2.0/24 a 192.168.3.0/24 do bloku 192.168.0.0/22.

$Úkol k textu$

Jaká je maska pro podsítě vzniklé rozdělením bloku 172.16.100.0/16 na 2 stejně ve podsítě?

$Shrnutí obsahu kapitoly$



V této lekci jsme se seznámili se základními vlastnostmi IP adres. Jde o 32-bitové adresy, které neobsahují žádnou informaci o fyzické adrese uzlu. Proto je nutné tut i získávat jiným způsobem, s nímž se seznámíme v kapitole 3. IP adresy je třeba přidělovat v celých blocích, nikoli samostatně, proto došlo k rozdělení do tříd A, B a C. Seznámili jsme se i s prostředky dočasného omezení rychlého vyčerpávání volných IP adres, především pak subnettingu a mechanismu CIDR, a s perspektivou přechodu na IP protokol verze 6, který tento problém řeší systematicky.

$Řešení úkolů k textu:$

1. **$Ztráta počtu IP adres$** při 500 uzlech v síti, pokud by byla použita pevná velikost síťové části adresy 16 bitů: množství vyplýtvaných adres je rovna $2^{16} - 500$.
2. **$Převod binární IP adresy$** 00001010000000010000000100110111 na symbolický dekadický tvar: 10.1.1.55.
3. **$Maska pro IP adresu 126.0.0.5:$** je 255.0.0.0, protože jde o adresu třídy A s délkou prefixu 8 bitů. Proto bude maska mít binární hodnotu 11111111000000000000000000000000.
4. **$Maska pro podsítě$** je 255.255.128.0. Zdůvodnění:
   Číslo 16 za lomítkem udává vždy počet bitů prefixu (síťové části adresy), tedy zde 16. (Ekvivalentní zápis by byl zapsat tuto adresu a k ní masku 255.255.0.0). Je-li tento blok se 16-bitovým prexifem rozdělen na 2 stejně velké podsítě, pak pro identifikaci podsítí se využije jeden bit (pro 1. podsíť =0, pro druhou =1), který se tedy z hlediska těchto podsítí stane pevným bitem a tedy součástí síťového prefixu. Pro identifikaci podsítí se vždy používají nejvyšší bity uzlové části adresy, zde tedy pouze jeden bit, tedy bit číslo 17 (počítáno od nejvyššího bitu zleva). Proto bude maska číslo složené ze 17 jedniček a 15 nul, tedy 255.255.128.0.

$Pojmy k zapamatování:$

- IP adresa

- Adresa třídy A, B, C
- Privátní IP adresa
- Maska podsítě
- CIDR

$Korespondenční úkoly$

1. Napište libovolnou IP adresu třídy A.
2. Napište masku pro IP adresu třídy C.
3. Zjistěte si (při aktivním připojení k Internetu) IP adresu svého počítače (Windows 9x/ME – utilita winipcfg, Windows NT/2000/XP – řádková utilita ipconfig), napište ji a zařaďte ji do příslušné třídy adres.
4. Kolik možných číselných kombinací a kolik použitelných IP adres máme k dispozici, pokud můžeme využívat CIDR blok 198.197.196.128/25?
5. Rozdělte blok adres 172.16.20.0/23 na 4 stejně velké podsítě (subnety). Pro každý subnet určete IP adresu podsítě, broadcastovou adresu, nejnižší a nejvyšší IP adresu pro přidělení uzlům a masku.

#7 IP protokol, vlastnosti síťové vrstvy

$Obsah kapitoly$

~Průvodce studiem

Tato kapitola se zabývá principy fungování síťové vrstvy protokolové sady TCP/IP, k přenosového protokolu IP a s ním souvisejících služebních protokolů. Seznámíte se t s principy směrování a rozpoznávání adres a způsobem signalizace chybových stavů vrstvě. Porozumění fungování síťové vrstvy je podstatné pro pochopení funkce služeb vyšších vrstev, proto mu věnujte odpovídající pozornost.&

$V této kapitole se dozvíte:$

1. Jaké jsou vlastnosti síťové vrstvy protokolové sady TCP/IP?
2. Jaký protokol se používá pro přenos dat v síťové vrstvě TCP/IP?
3. Jaké jsou vlastnosti protokolu IP a pomocného protokolu ICMP?
4. Jak se zjišťuje fyzická adresa uzlu?

$Po jejím prostudování byste měli být schopni:$

1. Specifikovat klíčové položky hlavičky IP datagramu;
2. Popsat účel a funkci protokolu ICMP;
3. Popsat účel a mechanismy směrování;
4. Charakterizovat účel rozpoznávání adres a mechanismy, které se k němu využívají.

~Klíčová slova této kapitoly:

Vrstva síťová, protokol IP, protokol ICMP, rozpoznávání adres, ARP.

Doba potřebná ke studiu: 2 hodiny&

#7.1 IP protokol

IP protokol je jediný přenosový protokol síťové vrstvy v architektuře TCP/IP. Jedná se totiž o přenosový protokol univerzální, který je schopen fungovat nad téměř libovolnou přenosovou technologií používanou ve vrstvě síťového rozhraní. Proto nevyužívá specifika jednotlivých přenosových technologií a požaduje od nich pouze služby na společné minimální úrovni kvality, tedy nespojové a nespolehlivé.

Protokol IP je tedy nespolehlivý a nespojovaný. Pracuje s proměnlivou délkou paketu (používá se též termínu „datagram“). Protože jde o univerzální přenosový protokol síťové vrstvy, je implementován ve všech uzlech, tedy ve směrovačích i v hostitelských počítačích.V současné době se používá jeho verze 4. Existuje návrh verze 6, o němž jsme se zmínili v předchozím textu v souvislosti s rozšířením adresního prostoru, ten se však dosud nepoužívá, přestože má již formu standardu.

Protokol IP v rámci svého fungování rozhoduje o volbě směru pro další zaslání paketu, zajišťuje předávání paketů vrstvě síťového rozhraní pro odeslání.

#7.1.1 Formát IP paketu (IP datagramu)

Jak již bylo zmíněno výše, délka datagramu je proměnná. Maximální délka je 64 kB, tedy 65536 bytů. Tuto maximální hodnotu si většina sítí snižuje podle toho, jakou maximální velikost rámce jim umožňuje zasílat vrstva síťového rozhraní. Minimální hodnota velikosti paketu je 576 bytů, což odpovídá nejméně 512 bytům dat přenášeným v paketu.

Paket obsahuje hlavičku, která má rovněž proměnlivou délku, její minimální délka však je 20 bytů. Nejvýznamnější položky hlavičky jsou:

- údaj o délce hlavičky a délce paketu (v prvních 4 bytech);
- identifikační číslo paketu (slouží pro potřeby fragmentace , nikoli pro číslování pořadí paketů), a příznaky pro fragmentaci. O fragmentaci se dozvíme dále.
- životnost paketu (položka TTL), označení přenášeného protokolu, kontrolní součet hlavičky
- IP adresu odesílatele a IP adresu příjemce

Hlavička může být doplněna o další nepovinné položky a vždy je doplněna tzv. výplní na délku dělitelnou 32 bity.

Zde se stručně zmíním o kontrolním součtu hlavičky, který je zmíněn výše jako jedna z položek hlavičky IP paketu. Co je to kontrolní součet, to si většina z Vás snad ještě pamatuje z kurzu Architektura počítačů, přesto to připomenu a upřesním význam, který tomuto pojmu budeme přisuzovat v tomto textu. Kontrolní součet v původním slova smyslu je opravdu prostý součet hodnot všech bytů paketu (resp. pokud zde mluvíme o kontrolním součtu hlavičky, pak součet všech bytů hlavičky). Ten se prostě ořízne na velikost položky, která je pro něj vyhrazena, a vloží se do ní. Smyslem kontrolního součtu není nést jakoukoli samostatnou informaci, ale chránit paket (resp. zde jen hlavičku) před změnou po cestě. Nejde o samoopravný kód, ale ve velké většině případů umožní detekovat, zda mezi odesláním paketu a jeho přijetím došlo ke změně (a to tak, že příjemce si z přijatého paketu vypočte kontrolní součet znovu a porovná s hodnotou v paketu. Rozdíl signalizuje změnu během doručování (ta je samozřejmě nežádoucí), a protože zde je chráněna hlavička, kde jsou především IP adresy (citlivé na změnu byť i jen jediného bytu, neboť tím se změní objekt, na který ukazují), přijatý paket s nesprávným kontrolním součtem se zpravidla dále nezpracovává a zahodí se.

Prostý součet hodnot bytů použitý jako kontrolní součet má výhodu v tom, že jej lze vygenerovat)spočítat) velmi rychle jak při odeslání, tak při přijetí paketu (v obou případech je jakékoli zdržení nežádoucí), nicméně má i své nevýhody.

#Úkol k zamyšlení

Jistě by každý z Vás dovedl snadno představit situaci, kdy dojde ke změně hlavičky, a její kontrolní součet (počítaný jako prostý součet hodnot bytů) se nezmění. Zkuste si zachytit IP paket a takovou změnu na reálném paketu navrhnout.&

Z výše uvedených důvodů se brzy začaly používat složitější algoritmy pro ochranu integrity přenášených dat, kdy se namísto prostého součtu používá složitější výpočet. V počátcích vývoje počítačů však nesměl být tento výpočet příliš složitý, neboť nesměl trvat dlouho. Takto vynikl např. kód CRC32, který vykazuje i při zachování nízké výpočetní složitosti vyšší spolehlivost než prostý součet. Ještě mnohem později se začaly používat i kontrolní součty s pokročilejšími vlastnostmi, např. s jistými kryptografickými vlastnostmi (tzv. hash funkce). My se v tomto textu však nebudeme zabývat tím, jak se konkrétní kontrolní součet počítá, a všechny kódy sloužící v popisovaných protokolech pro ochranu integrity

přenášených dat budeme označovat výrazem „kontrolní součet.“ Musíme však přitom mít na paměti, že nemusí vždy jít jen o prostý součet.

Pro úplnost zde uvádím, že v nové verzi IP protokolu, IPv6, se již kontrolní součet hlavičky nepoužívá. Nicméně s různými kontrolními součty se ještě setkáme na transportní vrstvě (u protokolů TCP i UDP), a pak na vrstvě linkové (např. v Ethernetovém rámci).

#7.1.2 Fragmentace

Po odbočení ke kontrolním součtům se nyní vrátíme k IP paketu. Jak již bylo uvedeno výše, je délka IP paketu proměnlivá. maximální možná délka IP paketu je 65536 bytů, což je ovšem mnohem více, než je typická maximální přípustná délka přenášeného souvislého bloku dat na linkové vrstvě, která se v dané síti používá. Tento parametr je důležitý pro IP protokol při odesílání paketu, proto jej pod označením MTU (Maximal Transfer Unit) inzeruje linkové vrstva, a IP protokol nevytváří delší pakety. Proto se délka IP paketů může v různých sítích lišit, a může dokonce dojít k situaci, kdy na směrovač přijde paket o velikosti, která je větší než maximální velikost, kterou je možno poslat přes síť určenou směrovačem jako odchozí. V takovém případě má směrovač dvě možnosti: buď paket rozdělit na části (tzv. fragmentovat), nebo jej zahodit (to učiní pouze tehdy, pokud je příznakem v hlavičce zakázána fragmentace daného paketu).

Fragmentace probíhá tak, že směrovač paket rozdělí do více paketů, které budou mít stejné identifikační číslo, a lišit se budou pouze datovou částí a údajem v hlavičce, který se nazývá OFFSET a stanoví posun počátku datové části paketu od počátku datové části původního paketu. Kromě toho bude v hlavičce všech fragmentů kromě posledního fragmentu nastaven příznak MORE FRAGMENTS označující, že paket je fragmentován a že ještě následují další fragmenty.

Skládání fragmentů do paketu pak provádí až cílová stanice. Proto nelze vyloučit situaci, kdy bude potřeba již fragmentovaný paket dále fragmentovat. Jak je vidět z popisu fragmentace v předchozím odstavci, nemělo by to způsobit žádné problémy. Jediným problémem, který je třeba ošetřit, je situace, kdy na cílový uzel některý fragment nedorazí (resp. nedorazí včas). V takovém případě uzel zahodí všechny fragmenty (a vygeneruje zprávu ICMP - viz dále).

#7.2 Protokol ICMP

Protokol IP může v některých případech (např. při přetížení směrovače apod.) některé pakety zahodit. Přestože je definován jako nespolehlivý, snaží se o této situaci zpravidla informovat odesílatele. K tomu slouží protokol ICMP (Internet Control Message Protocol). Protože je IP protokol univerzálním přenosovým protokolem síťové vrstvy, přenášejí se zprávy protokolu ICMP vložené do IP paketů.

ICMP protokol umožňuje efektivně signalizovat různé chybové a abnormální stavy na síťové vrstvě. Protože však jej lze poměrně snadno zneužít k získávání informací potenciálními útočníky, existuje mnoho sítí, kde je jeho šíření poměrně striktně omezeno. Tímto bezpečnostním omezením šíření ICMP paketů se však dále nezabýváme.

Zahození paketů nesoucích ICMP zprávu se však již nesignalizuje, protože by hrozilo zahlcení sítě oznámeními o zahození. Obecné pravidlo přitom zní, že ICMP zprávy se negenerují v případě, že je zahozen paket z důvodu chybného kontrolního součtu hlavičky. Důvod je prostý: adresa odesílatele paketu (a tedy příjemce případně vygenerovaného ICMP paketu), která je součástí hlavičky, v tomto případě nemusí být spolehlivá, neboť chybný kontrolní součet mohla způsobit právě její změna, ke které cestou došlo.

Protokol ICMP definuje vlastní paket, který se vkládá do IP paketu. Jeho formát je jednoduchý: 4 bytová hlavička, která obsahuje v položce TYPE typ ICMP zprávy (jeden

z předdefinovaných označených určeným číslem), upřesňující položku CODE a kontrolní součet paketu. Dále následuje datová část, která obvykle nese část původního paketu.

Nejvýznamnější situace, které jsou protokolem ICMP signalizovány, jsou popsány v následujících odstavcích.

#7.2.1 Time exceeded

Zpráva ICMP Time exceeded označuje zacyklení paketu. To je zjištěno podle položky životnosti (TTL) v hlavičce paketu, která se snižuje o 1 při každém průchodu přes směrovač (u odesílatele je TTL nastavena na implicitní hodnotu, která bývá 64, 128, případně i jiná). Pokud hodnota položky TTL na některém směrovači dosáhne nuly, paket se zahodí a směrovač vygeneruje zprávu ICMP Time exceeded, kterou odešle odesílateli zahozeného paketu. V tomto případě má položka TYPE hodnotu 11 a CODE hodnotu 0.

Druhou situací, kdy se signalizuje paketem ICMP Time exceeded, je situace, kdy během nastavené prodlevy pro čekání na všechny fragmenty některý fragment fragmentovaného paketu nedorazil k příjemci. Pak se zahodí všechny fragmenty a uzel vygeneruje zprávu ICMP Time exceeded, kterou odešle odesílateli zahozeného paketu. V tomto případě má položka TYPE hodnotu 11 a CODE hodnotu 1.

Pomocí zpráv ICMP Time exceeded je zpravidla realizována i utilita $**traceroute$**, která se používá ke zjištění aktuálně používané cesty k určitému uzlu. Využívá zasílání paketu s ICMP zprávou s TYPE=30 a TTL, kterou postupně zvyšuje od jedné až do dosažení cílového uzlu.

#7.2.2 Destination unreachable

Zpráva ICMP Destination unreachable signalizuje další situace, kdy byl zahozen paket. Zejména jde o situace nedostupné sítě, nedostupného uzlu, neexistující adresy či portu, překročení maximální velikosti paketu při zakázané fragmentaci atd. Tyto situace se opět odlišují různými hodnotami položky CODE.

#7.2.3 Další typy ICMP zpráv

Další situací, kdy je signalizováno zahazování paketů, je zpráva ICMP **$Source quench$**. Touto zprávou signalizuje směrovač odesílateli, že je zahlcen a musí proto zahazovat jeho pakety.

Dalším typem ICMP zprávy je dvojice ICMP $**Echo request$** a ICMP $**Echo reply$**. Ty se používají k diagnostickým účelům (zejména ke zjištění doby odezvy určitého uzlu a počtu přechodů přes směrovače na cestě k němu). Využívá jich například utilita ping.

S dalšími druhy ICMP paketů se seznámíme v následující části věnované směrování.

#7.3 Rozpoznávání adres

Protože IP adresy jsou abstraktní, tedy nemají žádnou souvislost s fyzickými adresami používanými na vrstvě síťového rozhraní, je nutné mít k dispozici mechanismus, který umožňuje tyto 2 druhy adres mezi sebou převádět. Především je nutný převod z IP adresy na adresu fyzickou, neboť ten je třeba při každém odeslání paketu. Vrstva síťového rozhraní totiž musí dostat požadavek k zaslání paketu na určitý uzel identifikovaný fyzickou adresou, neboť s IP adresami neumí pracovat. Opačný převod je třeba pouze v některých speciálních případech.

Způsob, který se v dané (lokální) síti použije pro rozpoznávání adres, závisí na vlastnostech vrstvy síťového rozhraní, tedy na použité přenosové technologii. Nejčastěji se používá decentralizované zjišťování pomocí dotazu. Protože se však dotaz musí zaslat všem stanicím na síti, musí mít vrstva síťového rozhraní možnost zasílat všesměrové rámce (tzv. broadcasty).Pro sítě využívající Ethernet se používá protokolu ARP, který používá právě

distribuovaného dotazování. Funguje tak, že dotazující uzel vloží do všesměrového rámce (takový rámec se zasílá na MAC adresu FF:FF:FF:FF:FF:FF) dotaz (ve formátu ARP) na fyzickou (MAC) adresu uzlu, který má IP adresu uvedenou v dotazu. Ten uzel v síti (obvykle lokální), který svou IP adresu pozná (jeho IP adresa je shodná s IP adresou uvedenou v ARP dotazu), odpoví vložením své MAC adresy do rámce a jeho odesláním zpět, tentokrát již pouze dotazující stanici.

Vzhledem k tomu, že překlad adres je třeba při každém odeslání paketu, není efektivní pokaždé provádět skutečné dotazování. Proto je do protokolu ARP zabudováno cacheování. Znamená to, že výsledky ARP dotazů jsou po určenou dobu na uzlech uloženy do vyrovnávací paměti (cache) a při každém požadavku na překlad adresy se nejprve ověří, zda není informace o adrese z předchozích dotazů uložena zde. Teprve v případě, že zde není adresa nalezena, se provede skutečný dotaz. Doba uložení vazby do cache může být různá, např. v OS Windows XP cca tato doba činí 2 - 10 minut, v jiných OS může být doba jiná, ale pravidlem je, že doba vždy bývá z řádu minut až desítek minut.

#7.4 Směrování

Směrování je činnost, při níž je třeba určit nejvhodnější cestu po síti od odesílatele k příjemci podle předem určeného kritéria. Jeho součástí kromě výpočtu optimální cesty je i získávání, šíření a uchovávání směrovacích informací nutných k určení cesty.

Dva základní druhy směrování jsou:

- směrování $**statické$**, kdy se směrovací informace mění pouze ručně, nikoli automaticky;
- směrování $**dynamické$**, kdy je zajištěna automatická aktualizace informací potřebných k určení trasy.

Podle kritéria způsobu určení trasy rozlišujeme:

- směrování zdrojové (celou trasu určuje odesílatel);
- směrování skokové (trasa se určuje průběžně, na každém směrovači se upřesňuje).

V TCP/IP sítích se převážně používá skokové dynamické směrování, pouze ve speciálních případech též směrování statické, obvykle jako doplněk dynamického pro ošetření speciálních případů.

Existují 2 základní algoritmy dynamického směrování:

- směrování na základě vektoru vzdáleností ($**vector-distance routing$**);
- směrování na základě stavu linky ($**link-state routing$**).

Směrování provádějí všechny uzly v síti, tedy hostitelské počítače (stanice, servery apod.) i směrovače. Odlišnost v jejich činnosti spočívá pouze v tom, že směrovače se aktivně účastní i aktualizace směrovacích informací, kdežto hostitelské počítače pouze pasivně (tyto informace pouze přijímají).

Směrování se musí provést při každém odeslání paketu ještě před předáním požadavku na odeslání paketu vrstvě síťového rozhraní. Prvním rozhodnutím, které se přitom musí provést, je rozlišení, zda se jedná o přímé nebo nepřímé doručení paketu.

O $**přímé doručení$** se jedná tehdy, když je odesílatel i příjemce paketu ve stejné síti. O přenos v rámci stejné sítě se jedná tehdy, pokud mají příjemce i odesílatel shodnou síťovou část IP adresy (prefix). V takovém případě není třeba rozhodovat o volbě směru, stačí pouze požádat vrstvu síťového rozhraní o doručení paketu na odpovídající fyzickou adresu zjištěnou pomocí mechanismu rozpoznávání adres.

V případě, že je paket určen příjemci v jiné síti, než kde se nachází odesílatel, jedná se o $**nepřímé doručení$**. V tom případě již je nutné určit odchozí směr, přesněji řečeno IP adresu odchozího směrovače. Tento směrovač (resp. jeho jedno síťové rozhraní) se nachází ve stejné síti jako odesílatel, a tím se případ nepřímého směrování převede opět na směrování přímé.

#7.4.1 Směrovací tabulky

Původní koncepce směrovacích tabulek byla taková, že každý směrovač bude mít (nejméně) jeden záznam pro každou síť, do které posílá pakety (v praxi to jsou většinou všechny připojené sítě, protože jen těžko lze a priori vyloučit komunikaci s některou ze sítí). To by ovšem vedlo k nutnosti práce s obrovským množstvím dat na každém směrovači, nehledě na jejich údržbu. Vzhledem k tomu, že ve směrovací tabulce se vždy nachází pouze odchozí směr pro každou síť, lze nutný objem směrovací tabulky výrazně zmenšit.

O jednom ze způsobů optimalizace směrovacích tabulek jsme se již zmínili v předchozí kapitole. Jde o mechanismus CIDR, který umožňuje sdružování sousedních adres do bloků. Nejefektivnější a zřejmě nejčastěji používaný způsob je však definice implicitního odchozího směru. V případě, že určíme, že pakety pro všechny sítě s výjimkou některých konkrétních sítí, které jsou z hlediska připojení zpravidla „blízko“, mají být posílány přes jeden směrovač (zpravidla ten, který má nejpřímější spojení s nadřízenými směrovači až k páteřním spojům v Internetu), stačí ve směrovacích tabulkách definovat explicitně těch několik výjimek a ostatní záznamy sdružit pod implicitní cestu (**default route**).

@Tabulka 4: Směrování s implicitní cestou – směrovací tabulka

cílová síť/prefix	**posílej přes**
192.168.0/24	směruj přímo
192.168.1/24	192.168.0.3
192.168.3/24	192.168.0.5
všechny ostatní pakety	192.168.0.4

&

Existuje i opačná možnost definovat pro určitý konkrétní uzel specifickou cestu (tzv. host-specific route), to se však používá pouze ve speciálních případech. Díky algoritmu výběru směrovacích informací z tabulky, kdy přednost má vždy informace s nejvyšším počtem shodných bitů (odleva, tedy od nejvyšších bitů) mezi cílovou adresou a prefixem uvedeným ve směrovací tabulce se takové host-specific route uplatní, i když je pro ostatní uzly v téže síti definována třeba jiná cesta. V případě, že není definována implicitní cesta a v tabulce se nenajde odpovídající záznam, skončí směrování chybou a vygeneruje se hlášení ICMP Destination unreachable.

Další ICMP zprávy, které se směrováním úzce souvisejí, jsou:

- **$ICMP Router solicitation$** (dotaz na všechny směrovače, zasílá se IP broadcastem do celé sítě);
- **$ICMP Router advertisement$** (směrovač jím oznamuje svou existenci, buď jako odpověď na ICMP Router solicitation, nebo samostatně);
- **$ICMP Redirect$**, které se zasílá odesílateli paketu, pokud směrovač zjistí, že existuje vhodnější cesta pro daný paket, než kterou ji odesílatel zaslal. Odesílatel by si pak měl příslušným způsobem upravit odpovídající záznam ve své směrovací tabulce. Samotný paket se samozřejmě nevrací odesílateli, ale předá se dalšímu směrovači,

který je pro odeslání vhodnější.

Správné směrování závisí na šíření směrovacích informací, což je při dnešním rozsahu Internetu značně obtížný problém. Vzhledem k tomu, že vnitřní směrovací informace o samostatných částech sítě s jedním vstupním bodem není třeba do zbytku sítě předávat, došlo na základě této myšlenky k rozdělení Internetu na větší množství tzv. $**autonomních systémů$**. Tím došlo k výraznému zmenšení objemu směrovacích informací, které je třeba po síti přenášet. Později bylo umožněno i to, aby autonomní systémy měly i více než jeden vstupní bod, takže jejich topologie může být i nestromovitá.

Touto změnou byl umožněn tzv. peering, neboli propojení sítí různých poskytovatelů připojení (nebo obecněji libovolných provozovatelů sítí) mezi sebou na úrovni nižší než přes páteřní spoje Internetu. V důsledku toho již nedochází k tomu, že např. paket zasílaný ze sítě jednoho poskytovatele v Ostravě do sítě jiného poskytovatele rovněž v Ostravě putoval až do páteřní sítě a pak zpět, jak tomu často bývalo v minulosti.

$Shrnutí obsahu kapitoly$

V této kapitole jste se seznámili s vlastnostmi síťové vrstvy TCP/IP. Zejména je dů zapamatovat, že zde pracuje jediný přenosový protokol IP, který zakrývá specifika přenosových technologií pracujících na vrstvě síťového rozhraní. Dále je třeba si u význam protokolu ICMP především pro signalizaci chybových a jiných abnormálních stavů na síťové vrstvě a rovněž klíčový význam směrování pro fungování rozsáhlých sítí na bázi TCP/IP. Pro praktické fungování protokolu IP nad různými přenosovými technologiemi vrstvy rozhraní je velmi zásadní mechanismus rozpoznávání adres, který je zde také popsán. Především je třeba se dobře seznámit s protokolem ARP, který realizuje rozpoznávání adres v sítích na bázi Ethernetu.

$Pojmy k zapamatování:$

- Protokol IP
- IP datagram
- Fragmentace
- Protokol ICMP
- Přímé doručení
- Nepřímé doručení
- Směrovací tabulka
- Autonomní systém

#Kontrolní otázky

1. Jaké jsou základní vlastnosti protokolu IP?
2. K jakému účelu se používá protokolu ICMP?
3. Co je to fragmentace paketů?
4. Jak pracuje protokol ARP?
5. Jaký je rozdíl mezi směrováním, které provádí uzel (stanice), a tím, které provádí směrovač?
6. Jaké druhý ICMP paketů mohou generovat směrovače a při jaké činnosti?&

#Korespondenční úkoly$

1. Při aktivním připojení k síti vypište směrovací tabulku na své stanici (pod V v příkazovém řádku např. příkazem „route print“) a pokuste se ke každému tabulky napsat, k čemu tento řádek slouží. Ke směrovací tabulce připojte v

aktivních rozhraní počítače a jejich IP adres (např. ipconfig pod Windows). Pokud je ve Vašem počítači více síťových rozhraní s přidělenou IP adresou. omezte svůj popis pouze na směrovací záznamy, které se vztahují k aktuálně používanému síťovému rozhraní. Doporučení: před analýzou si směrovací tabulku seřaďte od nejspecifičtějších záznamů k nejobecnějším, tedy sestupně podle masky.

2. Představte si IP síť tvořenou navzájem propojenými zhruba stejně velkých sítí (do 250 uzlů), kterých je celkem 1000. Vypočtěte, kolik záznamů by musela mít směrovací tabulka v každém směrovači v této síti, pokud by nebyla použita žádná optimalizace směrovacích tabulek (. Na topologii sice v tomto případě nezáleží, ale předpokládejte, že každá síť je připojena ke dvěma dalším sítím (tedy má dva odchozí směrovače se dvěma síťovými rozhraními), přičemž „páteřní sítě“ můžete zanedbat.
3. Pomocí vhodného programu pro zachycování paketů (např. Wireshark) zachyťte komunikaci Vašeho počítače s Vámi zvoleným serverem po spuštění příkazu traceroute (ve Windows jde o řádkovou utilitu nazvanou "tracert") a zjistěte, jakým způsobem tento příkaz zajišťuje odpověď od všech směrovačů na cestě. Nápověda: všímejte si hodnoty TTL (Time To Live) v hlavičkách jednotlivých IP paketů.&

#8 Základy Ethernetu

$V této kapitole se dozvíte:$

- Jaké jsou základní principy technologie Ethernet.
- Kde se Ethernet používá.
- Jak se chová switch (přepínač) v Ethernetové síti.

$Po jejím prostudování byste měli být schopni:$

- Charakterizovat základní principy technologie Ethernet.
- Znát princip fungování přepínačů v Ethernetu.

~Klíčová slova této kapitoly:

- Ethernet, přepínač (switch), opakovač (hub), 100Base-TX, 10Base-T

Doba potřebná ke studiu: 2 hodiny&

~Průvodce studiem

Cílem této kapitoly je seznámit studenty s technologií Ethernet jakožto převládajíc technologií používané v lokálních sítích.&

#8.1 Technologie počítačových sítí

K zapojení počítače do počítačové sítě musíme mít k dispozici následující technické a programové komponenty:

- přenosové médium (kabel, bezdrátové pojítko apod.);
- síťovou kartu (tzv. adaptér) pro práci v síti;
- obslužný program pro adaptér (tzv. ovladač neboli driver);
- operační systém s podporou práce v daném typu sítě.

Většina výrobců se snaží o vzájemnou kompatibilitu svých síťových produktů v různých typech sítí, to znamená schopnost spolupracovat s produkty jiných výrobců. Z tohoto důvodu dochází ke snaze vytvořit síť pokud možno modulárně, aby byla možná zaměnitelnost jednotlivých komponent různých výrobců.

Dříve, než objasníme jednotlivé technologie počítačových sítí, vysvětleme si způsob označování nejběžnějších technologií (na bázi Ethernetu). Obvykle se Ethernetové sítě označují trojsložkovým označení jako je např. 100BaseT. První část tohoto označení (zde číslovka 100) označuje jmenovitou přenosovou rychlost, jakou se v dané síti zasílají datové rámce. Druhá část tohoto označení (slovo „Base“) označuje přenos v základním pásmu. S jiným způsobem přenosu dat se v dnešních počítačových sítích prakticky nesetkáváme. Poslední částí označení (zde písmeno „T“) označuje typ přenosového média. Zde písmeno T obvykle označuje kroucenou dvojlinku, což je odvozeno od anglického označení Twisted pair. Pokud je poslední čásr tvořena číslovkou (nejčastěji 2 nebo 5), jedná se o označení starší normy pro koaxiální kabely a tato číslovka znamená maximální délku kabelového segmentu ve stovkách metrů.
Toto označení se používá u většiny dnešních síťových technologií používajících k přenosu dat kabel. U bezdrátových sítí, kterými se tento text nezbývá, se používá jiné označení.

Sítě typu Ethernet se obecně dělí na:
„Klasický“ Ethernet (přenosová rychlost 10 Mb/s)

10Base-5 Tlustý koaxiál – dosah max. 500 m – již se nepoužívá

10Base-2 Tenký koaxiál – max. 185 m – dnes již ojedinělý
10Base-T Kroucená dvojlinka – max. 100 m
10Base-FL Mnohavidové optické kabely – max. 2 km

Fast Ethernet (přenosová rychlost 100 Mb/s)

100Base-TX Kroucená dvojlinka – max. 100 m
100Base-T4 Nižší kategorie kroucené dvojlinky – již se nepoužívá
100Base-FX Mnohavidové optické kabely – max 2 km

Gigabitový Ethernet (přenosová rychlost 1Gb/s)

1000Base-SX Mnohavidové optické kabely – až 550 m
1000Base-LX Jednovidové optické kabely – až 5 km
1000Base-CX Stíněné kabely TP – dosah 25 m
1000Base-T Nestíněné kabely TP – dosah 100 m

#8.1.1 Technologie sítě Ethernet (IEEE 802.3)

Základy technologie, známé jako Ethernet, byly položeny začátkem 70. let. V roce 1980 byl standardizován konsorciem DEC, Intel a Xerox, standard je známý pod zkratkou DIX. Později v tomto roce byl organizací IEEE vytvořen standard IEEE 802.3 s velmi podobnými vlastnosti a ten se stal základem pro další rozvoj, zejména byl rozšiřován o další média a nové způsoby provozu. Ethernet je přenosovou technologií zajišťující skutečný přenos dat.
V referenčním modelu ISO/OSI pokrývá fyzickou a linkovou vrstvu, v rámci TCP/IP spadá do vrstvy síťového rozhraní. Ethernet může používat různá přenosová média (koaxiální kabely, kroucenou dvojlinku, optická vlákna). Předpokládá logicky sběrnicovou topologii, tj. má „sdílenou“ povahu. Teprve později se díky přepínání (switchingu) mění zčásti na „nesdílenou“ přenosovou technologii. Jeho chování je „statistické“, tj. nezaručuje právo vysílat a funguje dobře jen s „rozumnou“ pravděpodobností. Dále se vyvíjel ve stomegabitový a gigabitový Ethernet.

K základním vlastnostem všech specifikací Ethernetu patří použití metody CSMA/CD pro přístup k médiu, použití 48-bitových MAC adres pro identifikaci uzlů a pohyblivá délka rámce.

MAC adresa je 48-bitové číslo, které přiděluje danému rozhraní výrobce a nelze jej bez zásahu do hardware změnit. MAC adresy jsou přidělovány tak, aby byly celosvětově jednoznačné. Toho je dosaženo tak, že každému výrobci je přiděleno 3-bytový prefix, který tvoří prvních 24 bitů MAC adresy každého síťového rozhraní, jemuž tento výrobce přiděluje MAC adresu, zatímco zbývající část adresy přiděluje výrobce podle svého uvážení.

V Ethernetu se používají rámce různých typů, přičemž nejčastější jsou typy Ethernet II a IEEE 802.3. Tyto 2 typy rámců se liší pouze interpretací 2-bytové položky hlavičky rámce, která je uložena va 13. a 14. bytu rámce. Zatímco v případě rámce typu Ethernet II je tato položka interpretována jako typ přenášecých dat, v případě rámce typu IEEE 802.3 se interpretuje jako délka přenášených dat. Maximální velikost rámce je ve většině případů rovna 1518 bytům (1500 bytů dat, 14 bytů hlavička, 4 byty zakončení, tzv. Frame Check Sequence), minimální velikost rámce původně činila 64 bytů. Tato hodnota byla zachována i v novějších specifikacích Ethernetu používajících vyšší přenosové rychlosti, i když, jak uvidíme později, přece jen došlo v souvislosti s minimální délkou rámce k určitým změnám.

#8.1.1.1 Technologie 10Base-T

Kabely původně určené pro přenos telefonních hovorů od místní ústředny k telefonnímu přístroji uživatele, které předpokládá standard 10Base-T, jsou typu tzv. kroucená dvojlinka (Twisted pair). Pro každý uzel (počítač) se používají 2 páry vodičů, jejichž kvalita je tzv. voice grade („hlasové“) - dnes se tyto kabely označují jako kategorie 3. Běžná (nestíněná) kroucená dvojlinka se též označuje zkratkou UTP (unshielded twisted pair).

Na kroucené dvojlince nelze dělat odbočky, proto je potřebné rozvětvení (rozbočení) nutné dělat elektronickou cestou, a kvůli tomu se používají rozbočovače (huby). Rozbočení (rozvětvení) může logicky fungovat na úrovni fyzické vrstvy, pak se hub chová jako opakovač. To je nejobvyklejší případ, proto se po pojmem hub často rozumí víceportový opakovač. Hub může pracovat i na úrovni linkové vrstvy, pak se hub chová jako most nebo switch. Více informací o fungování těchto prvků najdete dále v této kapitole.

Ze čtyř vodičových párů kabelu UTP jsou využity dva, jeden pár přenáší signál od stanice k opakovači, druhý přenáší signál ve směru opačném. Kabel UTP musí splňovat podmínky na šířku pásma, charakteristickou impedanci a přeslech. Podmínky splňují kabely UTP kategorie 3 a s rezervou dnes běžnější UTP kategorie 5. Jako konektor slouží plochý konektor EIA RJ-45, který je 8-pólový. Využity jsou jen 4 piny:
pin č. 1: TransmitData (TD)+
pin č. 2: TD-
pin č. 3: Receive Data (RD)+
pin č. 6: RD-
ostatní: nevyužité

@Obr 3: Zástrčka RJ 45&
§obrázek – fotografie zástrčky se UTP zapojeným kabelem - vynechán&

@Obr 4: Zásuvka RJ 45&
§obrázek – fotografie zástrčky se UTP zapojeným kabelem – vynechán&

Opakovač předává signál přijatý od jedné ze stanic po úpravě (regeneraci a zesílení) ostatním stanicím, kromě stanice nebo opakovače, od nichž je přijímán. Stará se tak o vytvoření sdíleného kanálu propojujícího všechny uzly v síti. Příjem signálu při vlastním vysílání je pro stanici indikací kolize. Opakovače lze mezi sebou propojovat, buď opět kabely UTP, nebo optickými spoji. Často se setkáváme s tzv. stohovatelnými (stackable) huby, které umožňují pomocí proprietárního (obvykle velmi rychlého) propojení mezi nimi vznik skupiny hubů, která se v síti chová jako jediný hub s více porty.

Sdílený kanál vytvářený vícevstupovým opakovačem 10Base-T nebo strukturou složenou z více stohovaných hubů přináší proti sběrnicovému propojení počítačů podstatnou výhodu: fyzické odpojení stanice neovlivní chod zbytku sítě. Logika opakovačů 10Base-T dovolí odizolovat i stanici, která by u sběrnicovému Ethernetu svou poruchou narušila funkci celé sítě (např. trvalým vysíláním signálu).

Pro propojení hub-uzel je třeba tzv. patch kabel zapojený jako kabel 1:1 kde jsou vzájemně propojeny piny stejných čísel. V singulárních případech lze přímo propojit i dva koncové uzly mezi sebou, tj. bez použití hubu, ale je na to potřeba tzv. překřížený (cross-over) kabel.

#8.1.1.2 Zapojení kabelu UTP v konektoru RJ45 pro Ethernet

Zapojení standardního propojovacího kabelu pro použití v Ethernetových sítích znázorňuje následující tabulka. Prosím povšimněte si, že ačkoli se obvykle využívají pouze dva páry, je třeba mít ve všech kabelech zapojeny všechny 4 páry. Je to z důvodu předcházení případným možným problémům při budoucím přechodu na použití jiných technologií.

V případě standardního kabelu je zapojení na obou koncích totožné (viz obrázek 8.1). Tabulka níže znázorňuje též zapojení překříženého kabelu, který se používá pro propojení dvou síťových rozhraní bez použití rozbočovače či jiného propojovacího prvku (tedy obvykle pro přímé propojení 2 počítačů do miniaturní sítě). Překřížený kabel má překřížený 1 pár s druhým.

Tabulka zapojení kříženého kabelu:

Standardní kabel	Překřížený (cross-over) kabel
1 – Oranžovo-bílý	1 – Zeleno-bílý
2 – Oranžový	2 – Zelený
3 – Zeleno-bílý	3 – Oranžovo-bílý
4 – Modrý	4 – Modrý
5 – Modro-bílý	5 – Modro-bílý
6 – Zelený	6 – Oranžový
7 – Hnědo-bílý	7 – Hnědo-bílý
8 – Hnědý	8 – Hnědý

$Technologie 100Base-TX$

Výraznou technologickou modifikací hvězdicového Ethernetu *10Base-T* je standard označovaný jako *100Base-T* a zvyšující přenos na 100 Mb/s na kabelovém rozvodu UTP Cat. 5 nebo kabelech STP či optických vláknech.

Standard 100Base-T je označován jako Fast Ethernet a oproti 10Mb/s verzi je 10x rychlejší a je zaveden mechanismus pro detekci rychlosti (tzv. auto-negotiation of media speed – automatická negociace rychlosti přenosu dat). Beze změny zůstal formát linkových rámců, přístupová metoda a adresy. Fast Ethernet (100Base-T a jiné standardy pro rychlost 100 Mb/s) dosáhl desetinásobného zrychlení desetinásobným zkrácením bitového intervalu a zkrácením maximálního dosahu kabelových segmentů. Toto zkrácení je dáno nutností včasné signalizace kolize vysílajícímu uzlu (ještě před ukončením vysílání rámce). Byla zavedena možnost používání různých druhů kabeláže tj. dvojlinky kategorie 5, dvojlinky kategorie 3 a optických vláken.

Technologie Fast Ethernetu je založena na efektivnějším využití přenosového média. Kódování *Manchester* je nahrazeno efektivnějším kódováním *4B5B*. To dovolí dosáhnout efektivní přenosové rychlosti 100 Mb/s (na médiu až 125 Mb/s). Maximální vzdálenost mezi stanicí a rozbočovačem zůstala 100 m při použití kroucené dvojlinky, optické vlákno dovolí dosáhnout až přes 400 m.

Zvýšení rychlosti při zachování ostatních vlastností Ethernetu si však vyžádalo snížení maximální vzdálenosti.

Omezení dosahu sítě Fast Ethernet je dáno obecnými zásadami tj.:

- žádný segment z kroucené dvojlinky nesmí být delší než 100 metrů
- žádný optický segment nesmí být delší než 412 metrů

a dalším omezením uplatňujícím se při použití opakovačů

- nelze mechanicky sčítat délky segmentů;
- konkrétní hodnoty je třeba najít ve standardu.

Pro řadu aplikací může stačit dvoubodové připojení pracovišť kanály o rychlosti 10 Mb/s k přepínači (mikrosegmentace), přičemž k přepínači jsou rychlejšími kanály připojeny servery a další části sítě. Pro náročné aplikace je k dispozici možnost sdílení rychlého kanálu 100 Mb/s, nebo mikrosegmentace s plným vyhrazením kanálů 100 Mb/s.

Kombinace zařízení se standardní rychlostí 10 Mb/s a zařízení pracujících se 100 Mb/s a navíc s odlišným využitím média (100Base-TX a 100Base-T4) a režimem provozu (poloduplex, plný duplex) může přinést problémy se správou a konfigurací. Pro usnadnění konfigurace jsou zařízení umožňující práci oběma rychlostmi vybavena obvody dovolujícími automatickou konfiguraci při zahájení provozu (tzv. autonegociaci – viz výše). Mechanismus respektuje i fakt, že jedno ze zařízení nemusí být obvody pro automatickou konfiguraci vybaveno.

#8.1.1.3 Gigabitový Ethernet – technologie 1000 Base-X

Ethernet jako bezpochyby nejrozšířenější současná síťová přenosová technologii se i nadále vyvíjí. Jeho nejnovější verze dosahuje přenosové rychlosti 1000 Mb/s (1 Gb/s), což je stokrát více, než šířka pásma původní verze Ethernetu. Přitom i tento nový gigabitový Ethernet zůstává kompatibilní s existujícími „starými“ verzemi Ethernetu, používá stejnou přístupovou metodu CSMA/CD a MAC adresy.

V roce 1995 došlo přijetím standardu Fast Ethernet k podstatnému nárůstu přenosového pásma (100 Mb/s) a zdálo se, že možnosti dalšího zvyšování jsou již plně vyčerpány. Přesto se podařilo dále zvýšit rychlost, ovšem za cenu omezení poloduplexního provozu. Při plně duplexním provozu se eliminuje vliv metody CSMA/CD, resp. detekce kolizí, a tedy nestojí dále v cestě zvyšování přenosové rychlosti.

Standardy gigabitového Ethernetu byly vyhlášeny v letech 1998 1999. Gigabitový standard je zpětně kompatibilní s existujícími instalacemi Ethernetu. Jako přístupovou metodu zachovává CSMA/CD (i když v případě plně duplexního provozu ji de facto eliminuje). Použití gigabitového Ethernetu je nejčastější pro páteřní spoje lokálních sítí - propojení serverů a přepínačů Fast Ethernet.

Na fyzické vrstvě se používá (vzhledem k převažujícímu použití optických vláken) specifikace Fibre Channel. Existují celkem 4 specifikace gigabitového Ethernetu.

Specifikace 1000Base-SX (zde písmeno S jako Short) je určena pro levná mnohavidová vlákna pro kratší horizontální vedení nebo páteřní aplikace. Pro překlenutí větších vzdáleností (L jako Long) jednovidovými vlákny je pak určena specifikace 1000Base-LX.

Na metalickou kabeláž jsou zaměřeny dvě specifikace. První z nich, 1000Base-CX je určena pro krátká propojení (do 25 m) stíněným kabelem typu twinax, např. propojení serverů a přepínačů v serverových farmách.Tato technologie má spíše omezený význam.

Druhá specifikace pro metalickou kabeláž, 1000Base-T, využívá UTP kabeláž kategorie 5 standardních horizontálních rozvodů budov (do 100 m). V tomto případě se však využívají všechny 4 páry vodičů pro jeden směr přenosu a vylepšené kódování (2 bitové místo 1-bitového) umožnilo dosáhnout přenosu 1 Gb dat za sekundu, ačkoli na každém páru se přenášejí data rychlostí výrazně nižší.

Jak bylo vůbec dosaženo toho, že se omezení kladená na síť (vyjma požadavků na vyšší kvalitu kabeláže) prakticky nezměnily? Odpověď je třeba najít v principech Ethernetu.

Minimální velikost rámce Ethernetu je 64 bajtů. Ta je právě dána standardem 802.3 pro zajištění toho, aby stanice neskončila svoje vysílání dříve, než první bit rámce dosáhne vzdáleného konce kabelu, kde může nastat kolize s jiným rámcem, a případný interferenční signál kolize se nevrátí zpět k vysílající (a zároveň poslouchající) stanici. Pokud by toto omezení neexistovalo, mohlo by se stát, že stanice vyšle velmi krátký rámec, který se ve vzdálené části sítě dostane do kolize, avšak protože vysílající stanice skončí vysílání dříve, než se o kolizi dozví, nespojí si tuto kolizi s již odeslaným rámcem, který považuje za správně odeslaný a tedy i správně doručený. Tento rámec však nebyl doručen a došlo k jeho ztrátě.

Zmíněná minimální velikost rámce se nazývá slot size (a pro Ethernet je uvedených 64 bajtů), odvozenou hodnotou je tzv. slot time, minimální čas, po který stanice musí vysílat.

Max. vzdálenost mezi dvěma uzly standardního Ethernetu je v případě žlutého koaxiálního kabelu 2,5 km (při max. počtu čtyř opakovačů). Zvýšení přenosové rychlosti musí být vykoupeno:

- buď zachováním slot time (tj. zachováním min. velikosti rámce) a zmenšením rámce, nebo
- zvětšením slot time (tj. zvětšením min. velikosti rámce) při nezměněné velikosti rámce, nebo

- kombinací obou způsobů.

Standard Fast Ethernet vyřešil tento problém prvním z uvedených způsobů, tj. redukcí délky rámců. Maximální velikost kolizní domény se zmenšila v případě UTP kabelů na 200 m, resp. 210 m.

V případě gigabitového Ethernetu se tvůrci specifikace nutně dostali ke stejnému rozhodování. Gigabitový Ethernet je opět desetkrát rychlejší (než Fast Ethernet). Při zachování stejné slot size (min. velikosti rámce) by došlo k redukci segmentů na pouhých 10 m. To je však již příliš málo, aby šlo o použitelné řešení.

Autoři specifikace přesto zachovali jak min. a max. velikost rámců standardního Ethernetu, tak rozumnou délku segmentů. Jak toho dosáhli? Zvláštním procesem, zvaným Carrier Extension. Gigabitový Ethernet používá sice stejný minimální rámec o velikosti 64 bajtů, ale zvětšenou hodnotu slot size na 512 bajtů. Že by tyto dvě hodnoty měly být stejné, jak jsme si uvedli o několik odstavců výše? Nemusí, uvědomíme-li si, že slot time je doba vysílání paketů minimální délky, potřebná k zajištění detekce kolizí všemi zúčastněnými uzly. Potřebujeme-li zachovat zpětnou kompatibilitu, tedy stejnou velikost min. rámce, musíme tento rámec vysílat delší dobu. Jak? Jednoduchým doplněním o neplatná data na požadovanou velikost.

V praxi uvedené řešení funguje tedy tak, že je-li rámec menší než 512 bajtů, je doplněn na velikost 512 bajtů neplatnými speciálními symboly, tzv. Carrier Extension. Každý vysílaný rámec tak má min. velikost 512 bajtů a je splněna podmínka dostatečného slot time, doby pro vysílání a detekci kolizí i těch nejmenších rámců.

Doplnění rámce do dostatečné délky zvláštními neplatnými znaky je sice jednoduché řešení, bystřejšího čtenáře již jistě ale napadlo, že je to také značné plýtvání šířkou pásma. Při nejmenším paketu je doplněno „zbytečných“ 448 doplňujících bajtů.

Dalo by se sice namítnout, že při rychlosti 1 Gb/s nám na pár bajtech nemusí až tak záležet, není to však úplně pravda. Při větším množství malých paketů by přeci jen mohlo docházet k významnému poklesu výkonu sítě (při vysílání pouze 64 bajtových rámců by klesla efektivní přenosová rychlost na pouhých 120 Mb/s!). Samozřejmě jde o extrémní případ, běžný průměr rámců je někde mezi 200 až 500 bajty, i tak by to ale znamenalo datovou propustnost „pouze“ 300 až 400 Mb/s.

Proto bylo řešení s rozšířením malých rámců doplněno o tzv. Packet Bursting, čili posílání rámců ve shlucích. Chce-li stanice poslat více rámců, první rámec je (je-li to nutné) doplněn na potřebnou velikost užitím Carrier Extension. Následující rámce jsou ale vysílány jeden po druhém hned za sebou, s minimální odstupem IPG (Inter-packet gap, mezera mezi jednotlivými vysílanými rámci). Tak jsou ve shluku odvysílány i malé rámce bez nutnosti jejich doplňování na minimálních 512 bajtů, což by bylo nutné při jejich samostatném odvysílání. Vysílání shluku rámců pokračuje až do vyčerpání času (burst timer) potřebného pro odvysílání plného rámce - 1500 bajtů. Tímto způsobem je velice efektivně sníženo ono „plýtvání“ přenosovým pásmem.

Přesto ani shlukování rámců nepředstavuje nijak oslnivé řešení. Řešením je zřejmě pouze přechod na plně duplexní provoz, který se nejen díky výše zmíněným důvodům v gigabitovém Ethernetu používá velmi často. Díky duplexnímu provozu odpadá možnost vzniku kolizí , a tedy není nutno ani respektovat omezení vyplývající z nutnosti kolize detekovat, jejichž nejvíce viditelným důsledkem je právě prodloužení minimální délky vysílaného bloku dat. Síť využívající pouze plně duplexní spoje totiž přestává být sítí se sdíleným médiem, neboť všechny spoje jsou vyhrazené pouze pro jeden směr provozu mezi 2 uzly.

#8.2 Technické vybavení sítí LAN

Technické vybavení sítí je tvořené přenosovým médiem, síťovým adaptérem případně opakovači, mosty a přepínači. V standardním případě je technickým vybavením realizovaná úroveň první a část druhé vrstvy. Tyto vrstvy vlastně určují topologii a přístupovou metodu sítě.

#8.2.1 Přenosové médium

Zajišťuje přenos dat mezi počítači sítě. Nejčastěji se používají tyto druhy přenosových medií:

- **$stíněný symetrický kabel STP$** - složený z měděných vodičů, které jsou obklopené izolačním nevodivým materiálem;
- **$nestíněný symetrický kabel UTP$** - složený s dvou, čtyř, 22, 24 nebo 26 vodičů, kde páry jsou navzájem obtočené, použití je podle kategorie (Cat. 3 - Cat. 5);

$Členění:$

•kategorie 1: telefonní pro přenos řeči, v datových sítích se nepoužívá
•kategorie 2: přenosová rychlost do 4 Mb/s - 4 páry, v datových sítích se nepoužívá
•kategorie 3: přenosová rychlost do 16 Mb/s - 4 páry s 9 závity/1m, použití v sítích dnes již spíše ojedinělé ve starších instalacích
•kategorie 4: přenosová rychlost do 20 Mb/s, díky rychlému nástupu kategorie 5 se příliš neprosadila
•kategorie 5: přenosová rychlost do 100 Mb/s
•kategorie 6: přenosová rychlost do 200 Mb/s

$Poznámka:$ Existují také kategorie 5+ a 5E, které jsou používané některými výrobci. Specifikace kabelů těchto kategorií klade přísnější limity především na přeslech, ale maximální přenosová rychlost je shodná s kategorií 5, proto tyto kategorie v našem výčtu explicitně neuvádíme).

- **$optický kabel$** - pro své výborné přenosové vlastnosti je čím dál více perspektivnější, hlavně při propojování vzdálenějších sítí, je však stále poměrně drahý. Existují dva základní navzájem nekompatibilní typy optických kabelů (resp. vláken) podle jejich konstrukce (levnější mnohavidová a kvalitnější jednovidová vlákna.

$Pojmy k zapamatování:$

- Ethernet
- MAC adresa
- Rámec Ethernet II
- Rámec IEEE 802.3
- 10Base-T, 100Base-TX, 1000Base-T
- Autonegociace

#Kontrolní otázky

1. Proč je při zvýšení přenosové rychlosti v Ethernetové síti nutné zmenšit při velikost kolizní domény?
2. Jak je možné zajistit, ay v jedné síti používaly některé segmenty standardu a jiné 100Base-TX?&

#Korespondenční úkoly

1. Jak souvisí přípustná (maximální) velikost (délka) kolizní domény v Ethernetové síti s přenosovou rychlostí?
2. Pomocí paketového analyzátoru (např. program Wireshark) zachyťte rámec II a popište délku a význam jednotlivých polí hlavičky rámce. Totéž prove

rámec IEEE 802.3. Napište, jak se od sebe oba typy rámce dají rozlišit, pokud se používají současně na stejné síti.&

~Průvodce studiem

Zde končí kurz zaměřený na poskytnutí úvodních informací o problematice počítačových sítí. Pro mnohé z Vás se zřejmě jedná o problematiku, se kterou se setkáváte poprvé. Proto je velmi důležité, abyste si ještě před zakončením kurzu zrekapitulovali nově nabyté znalosti, případně si osvěžili ty, které nemáte ještě dostatečně fixované. S rychle rostoucím praktických významem počítačových sítí se zřejmě i v praxi alespoň někteří z vás setkají s možností prakticky si ověřit některé z poznatků, které Vám měl tento kurz předat.&

$Literatura$

1. **Základní:** Klimeš, C., Sochor, T. *Počítačové sítě 1. Text pro distanční studium.*. Ostrava: Ostravská univerzita, 2003. ISBN 80-7042-853-8. Původní text pro adaptaci, předchozí vydání
2. **Rozšiřující:** Heather Osterloh. *TCP/IP - Kompletní průvodce.*. Softpress Praha, 2003. ISBN 80-86497-34-8. **Není k dispozici**
3. **Rozšiřující:** Dostálek, L. *Velký průvodce protokoly TCP/IP: bezpečnost.*. Computer Press, Praha, 2003. ISBN 80-7226-849-X. **Je k dispozici v centr. katalogu UK (černotisk)**
4. **Rozšiřující:** Angela Orebaugh, Gilbert Ramirez, Josh Burke, Greg Morris, Larry Pesce, Joshua Wright. *Wireshark a Ethereal*. Computer Press Praha, 2008. ISBN 978-80-251-2048-4. **Není k dispozici**
5. Tanenbaum, A.S., Steen, M. van: Distributed systems. Principles and paradigms. Prentice hall. New Jersey 2002. ISBN 0-13-088893-1 **Je k dispozici v centr. katalogu UK (černotisk)**

6. **Doporučená:** Dostálek, L., Kabelová A. *Velký průvodce protokoly TCP/IP a systémem DNS.*. Computer Press Praha, 2008. ISBN 978-80-251-2236-5. **Je k dispozici v centr. katalogu UK (černotisk)**

$Náhradní literatura dostupná z Knihovní brány pro zdravotně postižené$ (http://seth.ics.muni.cz/usr/portal/)

Sosinsky B. Mistrovství - počítačové sítě : vše, co potřebujete vědět o správě sítí. Computer Press, Brno 2010, 1. vyd, ISBN 9788025133637

Shinder Debra Littlejohn. Počítačové sítě : nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí. Praha : Softpress, 2003. 1. vyd. ISBN 8086497550

Kállay F., Peniak P. Počítačové sítě a jejich aplikace : LAN/MAN/WAN.Grada, Praha 2003. ISBN 8024705451

Spurná I. Počítačové sítě : praktická příručka správce sítě. Kralice na Hané : Computer Media, 2010. Vyd. 1 ISBN 9788074020360

$Knihy v hmatovém písmu:$
Název: Počítačové sítě a jejich aplikace : PA 159 Typ dokumentu: hmatové písmo Autor: Luděk Matyska, Eva Hladká, Petr Holub Rok vydání: 2004 Pochází z knihovny: Teiresiás MU

Název: Soudobé počítačové sítě : PA 151 Typ dokumentu: hmatové písmo Autor: Jan Staudek. Rok vydání: 2007 Pochází z knihovny: Teiresiás MU

$Důležité odkazy na www$

- Program Wireshark je k dispozici na www.wireshark.org
- *IP Subnet Calculator*. on-line dostupné z http://www.subnet-calculator.com/ [2010-05-03]
- Peterka, J.: *Počítačové sítě, verze 3.5*. [on-line] dostupné na http://earchiv.cz/l222/index.php3 [2011-03-25]
- Peterka J.: *Rodina protokolů TCP/IP, verze 2.7.* [on-line] dostupné na http://earchiv.cz/l223/index.php3 [2011-03-25]

Doplňující informace (tiráž)

Studijní opora je jedním z výstupu projektu ESF OP VK.

@

Číslo Prioritní osy	7.2
Oblast podpory	7.2.2 – Vysokoškolské vzdělávání
Příjemce	Ostravská univerzita v Ostravě
Název projektu	Podpora terciárního vzdělávání studentů se specifickými vzdělávacími potřebami na Ostravské univerzitě v Ostravě
Registrační číslo projektu	CZ.1.07/2.2.00/29.0006
Délka realizace	6. 2. 2012 – 31. 1. 2015
Řešitel	PhDr. Mgr. Martin Kaleja, Ph.D.

&

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.
Název: Počítačové sítě 1
Autor: Tomáš Sochor
Studijní opora pro kurz: Počítačové sítě 1
Recenzent: jméno a působiště recenzenta
Jazyková korektura nebyla provedena, za jazykovou stránku odpovídá autor.