

Předložená disciplína Vás tedy postupně seznámí s problematikou adresace a směrování v počítačových sítích. Rozsah témat je volem tak, aby Vám umožnil orientovat se v oblasti počítačových sítí. Pokud tedy budete společně s námi sledovat následující výklad, získáte mnoho teoretických i praktických znalostí a dovedností, které Vám umožní rychlou a efektivní obsluhu výpočetní techniky.

Po prostudování tohoto materiálu budete schopni:

- prezentovat poznatky z oblasti počítačových sítí,
- vysvětlit problematiku IP adres,
- objasnit pojem směrování,
- charakterizovat protokol TCP a UDP,
- charakterizovat aplikační vrstvu.

A nyní několik pokynů ke studiu.

Budeme s Vámi rozmlouvat prostřednictvím tzv. průvodce studiem. Odborné poznatkové penzum najdete v teoretických pasážích, ale nabídneme Vám také cvičení, pasáže pro zájemce, kontrolní úkoly, klíče k řešení úkolů (**najdete je na konci studijního materiálu**), shrnutí, pojmy k zapamatování a studijní literaturu. Je vhodné, ale ne nezbytně nutné, abyste tento text studovali především u Vašeho osobního počítače a všechny popsané postupy ihned aplikovali. Také jsme pro vás připravili mnoho kontrolních úkolů, na kterých si ihned ověříte, zda jste nastudovanou problematiku pochopili a zda jste schopni ji aplikovat.

Proto je v textu umístěno mnoho obrázků, které Vám umožní rychlou a snadnou orientaci ve výkladu. Tyto obrázky obsahují skutečné zobrazení počítače, počítačových komponent, uživatelských rozhraní aplikací apod. Každý obrázek je navíc doplněn o orientační značky (tzn.: ikony čísel 1, 2 apod.), které určují pozici nejdůležitějších prvků. U každého takového obrázku je potom umístěna příslušná legenda (zpravidla ihned pod obrázkem), která daný označený objekt nebo prvek popisuje a vysvětluje také jak je možné jej ovládat. Proto je vhodné nejprve daný obrázek (který vždy vysvětluje danou problematiku) prohlédnout, podle orientační značky identifikovat popisované prvky nebo objekty a poté si přečíst příslušnou legendu.

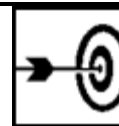
Obsah kapitol disciplíny:

Kapitola 1	IP adresa a její části - Teoretický základ kapitoly (třída A, B, C, speciální IP adresy, maska sítě, IP adresa i Intranetu, nečíslované sítě, adresní plán) - Úkol 1 – vysvětlení pojmu IP adresa - Úkol 2 – rozlišení tříd IP adres, - Úkol 3 – analýza aplikace IP adres v intranetu - Úkol 4 – tvorba adresního plánu - Shrnutí kapitoly a kontrolní otázky a úkoly
Kapitola 2	Směrování v síti

	- Teoretický základ kapitoly (předávání a filtrace, zpracování směrování, manipulace se směrovacími tabulkami, směrovací protokoly) - Úkol 1 – objasnění principu směrování - Úkol 2 – vysvětlení procesu předávání a filtrace - Úkol 3 – základní manipulace se směrovacími tabulkami - Úkol 4 – popis směrovacích protokolů - Shrnutí kapitoly a kontrolní otázky a úkoly
Kapitola 3	Přenosové protokoly TCP a UDP - Teoretický základ kapitoly (TCP segment, navázání a ukončení spojení navázaného protokolem TCP, protokol UDP) - Úkol 1 – vysvětlení pojmů protokol TCP a UDP - Úkol 2 – popis TCP segmentů - Úkol 3 – objasnění principu navázání a ukončení spojení protokolem TCP - Úkol 4 – analýza zjištění stavu spojení - Shrnutí kapitoly a kontrolní otázky a úkoly
Kapitola 4	Aplikační vrstva počítačové sítě - Teoretický základ kapitoly (klasifikace služeb aplikační vrstvy, typy serverů aplikační vrstvy, služby aplikační vrstvy) - Úkol 1 – analýza pojmu aplikační vrstva - Úkol 2 – klasifikace služeb aplikační vrstvy - Úkol 3 – popis jednotlivých serverů aplikační vrstvy - Úkol 4 – charakteristika služeb aplikační vrstvy - Shrnutí kapitoly a kontrolní otázky a úkoly

1 IP adresa a její části

Cíle



Po prostudování této kapitoly byste měli být schopni:

- vysvětlit pojem IP adresa,
- rozlišit třídy IP adres,
- chápat princip síťové masky,
- objasnit problematiku IP adres v intranetu,
- vytvořit adresní plán.

Průvodce studiem



Zapomněli jste základní poznatky z kapitoly o síťových protokolech? Nic se neděje. Můžete se kdykoliv vrátit a vše potřebné si připomenout a nebo Vám za tímto účelem nabízíme následujících pár řádků:

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

V této kapitole se podrobněji zaměříme a IP adresy. Podrobněji si vysvětlíme pojem IP adresa a provedeme rozdělení do tříd. Dále se budeme věnovat IP adresám v intranetu a nečíslovaným sítím.

V závěru se naučíme vytvářet adresní plány, které využijete, budete-li chtít Vaši firmu připojit k Internetu.

Vstupní znalosti:

- pro studium této kapitoly by jste měli mít osvojeny základní poznatky o síťových protokolech.

Potřebný čas pro studium kapitoly:

- 65 minut

1.1 IP adresa obecně



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

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

V praxi se však využívání sekundárních IP-adres pro WWW-servery považuje za plýtvání – používají se tzv. virtuální WWW-servery, kdy mnoha WWW-serverům stačí jedna společná IP-adresa. Specifikace

IP adresa

serveru se pak provádí na aplikační úrovni v protokolu http (pomocí hlavičky *host*).

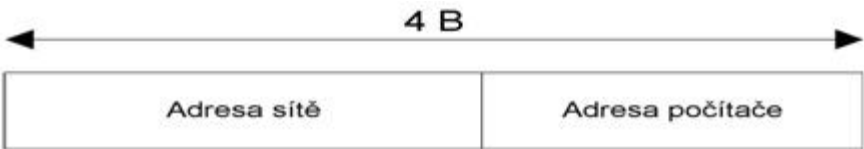
Jelikož má většina počítačů jedno síťové rozhraní, tak se přeneseně místo IP-adresa rozhraní říká IP-adresa počítače. IP-adresa je tvořena čtyřmi bajty. IP-adresa se zapisuje notací, kde jednotlivé bajty se mezi sebou oddělují tečkou. Rozeznáváme:

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

Složení IP adresy

IP-adresa se skládá ze dvou částí:

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



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

- Třída A. V třídě A máme 126 sítí (0 a 127 mají zvláštní význam).
V každé síti je 2^{24} - 2 adres pro počítače (adresy tvořené samými nulami a samými jedničkami mají zvláštní význam).
- Třída B. Můžeme mít celkem 214 sítí a v každé síti 216 - 2 počítačů.
- Třída C. Můžeme mít 2^{22} sítí a v každé síti 128 - 2 počítačů.
- Třída D, kde nejvyšší čtyři bity prvního bajtu mají hodnotu 1110₂.
Zbytek IP-adresy se pak už nedělí na adresu sítě a adresu počítače.
Zbytek IP-adresy tvoří adresný oběžník (*multicast*).
- Třída E tvořící zbytek adres je tč. rezervou.

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

Úkol 1.1 (krátký úkol)

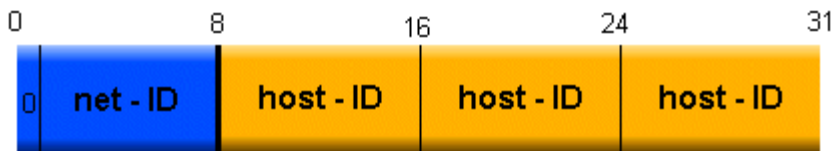
Kolik tříd IP adres existuje?



1.2 Třída adres A



Třída A



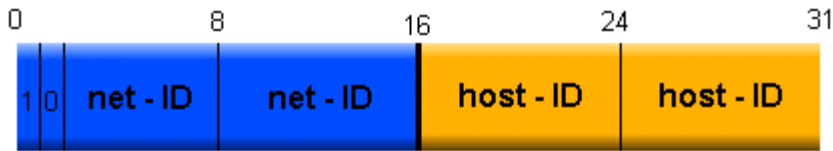
IP adresu třídy A v České republice nikdo nemá. Mají ji hlavně nadnárodní společnosti, vládní organizace USA atp. Dovoluje adresování jen 128 sítí, ale v každé z nich může být až 16 miliónů počítačů. První byte může v desítkové soustavě nabývat hodnot od 1 do 126.



1.3 Třída adres B



Třída B



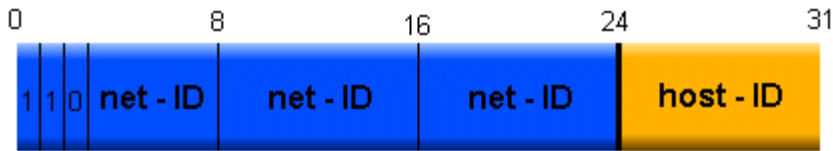
Třída B umožňuje adresovat už 16 tisíc sítí a 65 tisíc počítačů. V Čechách ji mají významné organizace. První byte v desítkové soustavě nabývá hodnot od 128 - 191. Například:



1.4 Třída adres C



Třída C



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

Úkol 1.4 (krátký úkol)



Kolik sítí obsahuje třída adres C?

1.5 Speciální IP-adresy



IP-adresa je obecně tvaru: síť.počítač

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

Speciální IP-
adresy

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

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

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

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

ping 192.168.6.255

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

Úkol 1.5 (krátký úkol)

Kterou IP adresu má každý počítač?



1.6 Síťová maska

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



Síťová maska

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

11111111.00000000.00000000.00000000

což vyjádřeno v desítkové soustavě je:

255 . 0 . 0 . 0 (šestnáctkově ff.00.00.00)

Obdobně standardní síťová maska pro třídu B je desítkově:

255 . 255 . 0 . 0 (šestnáctkově ff.ff.00.00)

Konečně pro třídu C:

255 . 255 . 255 . 0 (šestnáctkově ff.ff.ff.00).

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

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

170 . 85 . 255 . 248, tj. dvojkově
10101010 . 01010101 . 11111111 . 11111000

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

11111111 . 11111111 . 00000000 . 00000000

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

10101010 . 01010101 . 11111111 . 11111000
11111111 . 11111111 . 00000000 . 00000000

10101010 . 01010101 . 00000000 . 00000000

Výsledek převedeme do desítkové soustavy a zjistíme, že počítač leží na síti 170 . 85 . 0 . 0.

Úkol 1.6 (krátký úkol)

Kolik bajtů má maska sítě?



1.7 IP-adresy v intranetu

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

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



IP-adresy
v intranetu

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

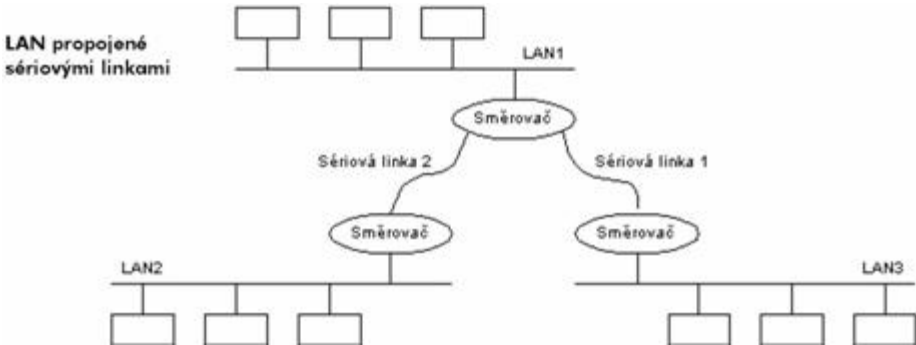
Pro uzavřené podnikové sítě si zvolte IP-adresy sítí podle RFC1918 uvedené v tabulce.

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

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

1.8 Nečíslované sítě

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

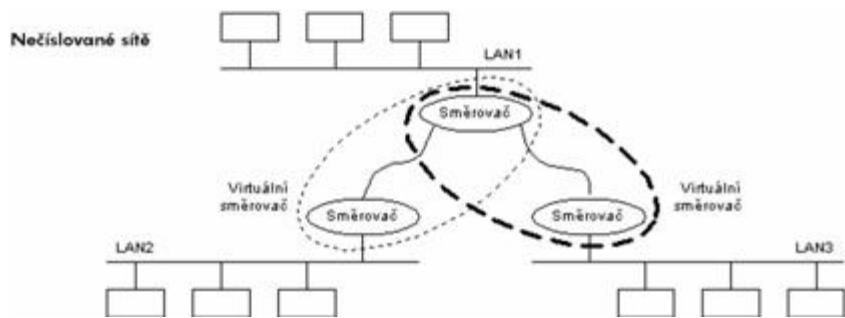


Z obrázku je patrné, že kromě tří intervalů IP-adres pro lokální sítě budeme potřebovat další adresy pro sítě tvořené sériovými linkami. Na první pohled je vidět, že by bylo efektivní pro sériové linky nepotřebovat další adresu sítě.

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



Nečíslované sítě



*Dynamicky
přidělované
adresy*

Pro sériové linky tak není třeba plýtvat IP-adresami.

1.8.1 Dynamicky přidělované adresy

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

Jsou dvě možnosti:

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

Dynamické přidělování přináší výhodu i v tom, že je potřeba jen tolik IP-adres, kolik je současně přihlášených uživatelů. Dynamické přidělování adres řeší aplikační protokol DHCP. Protokol DHCP vychází ze zkušeností

a částečně v sobě zahrnuje i podporu starších protokolů z této oblasti, tj. protokolů RARP, DRARP a BOOTP. Blíže viz RFC-1531.

V protokolu DHCP žádá klient DHCP-server o přidělení IP-adresy (případně o další služby). DHCP-server může být realizován jako proces na počítači s operačním systémem UNIX, Windows NT atp. Nebo DHCP-server může být realizován i jako součást směrovače.

Zatímco přidělování IP-adres na LAN je v současné době doménou protokolu DHCP, pro přidělování IP-adres počítačům za komutovanou linkou (např. zákazníkům poskytovatele Internetu) se zpravidla přidělují IP-adresy pomocí protokolu PPP.

NAT

Protokol PPP je linkovým protokolem používaným na asynchronních sériových linkách. Neumožňuje takové služby jako protokol DHCP, avšak přidělit IP-adresu stanici umí. Více stejně pro připojení uživatele k Internetu nebývá třeba.

1.8.2 NAT

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

Když počítač z lokální sítě odesílá paket do vnější sítě (např. internetu), odešle jej se svou zdrojovou IP adresou a portem. Při průchodu NATem jsou však zdrojové IP adresy v paketech přepsány na veřejnou IP

adresu NATu. Také je přepsáno číslo zdrojového portu na port, který NAT odesílajícímu počítači přidělil. NAT si zároveň uloží toto přidělení do své převodní tabulky (v které jsou uloženy veškeré informace o vzájemném mapování jednotlivých adres).

Když pak následně dorazí odpověď od vzdáleného počítače, hlavičky paketů jsou znovu přepsány – tentokrát je cílová adresa a port přepsána příslušnými informacemi z převodní tabulky (lokální IP adresou a portem příslušného počítače) a paket je předán dál k doručení do lokální sítě.

NAT je ovšem "velkým zlem", jelikož s počítači za NATem nelze z venku přímo navázat spojení a jsou tak narušeny základní principy internetu (všechny počítače mají být jednoznačně adresovány a kdokoliv s kýmkoliv má mít možnost komunikovat přímo).

NAT je také těžko slučitelný s některými protokoly vyšších vrstev (jako např. FTP, H.323, SIP, atd.) a příslušné služby pak za NATem nemusí dobře fungovat (respektive aby fungovaly, musí být na NATu použit connection tracking rozumějící daným vyšším protokolům).

Úkol 1.8 (krátký úkol)

Pomocí jakého serveru se dynamicky přidělují IP adresy?



1.9 Adresní plán

Každá firma, která se chce připojit k Internetu, si musí nejprve udělat adresní plán. Ten se obvykle skládá ze dvou částí.

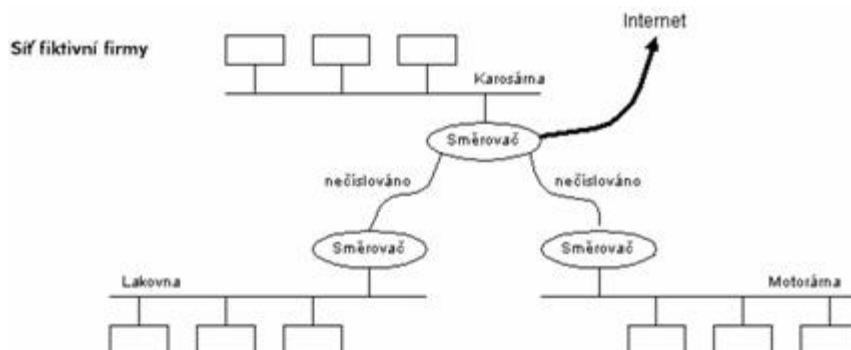
Jednak ze schematického znázornění propojení jednotlivých LAN do WAN a jednak ze seznamu jednotlivých LAN s odhadovaným počtem síťových rozhraní na LAN.



Adresní plán

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

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



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

počítačů.

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

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

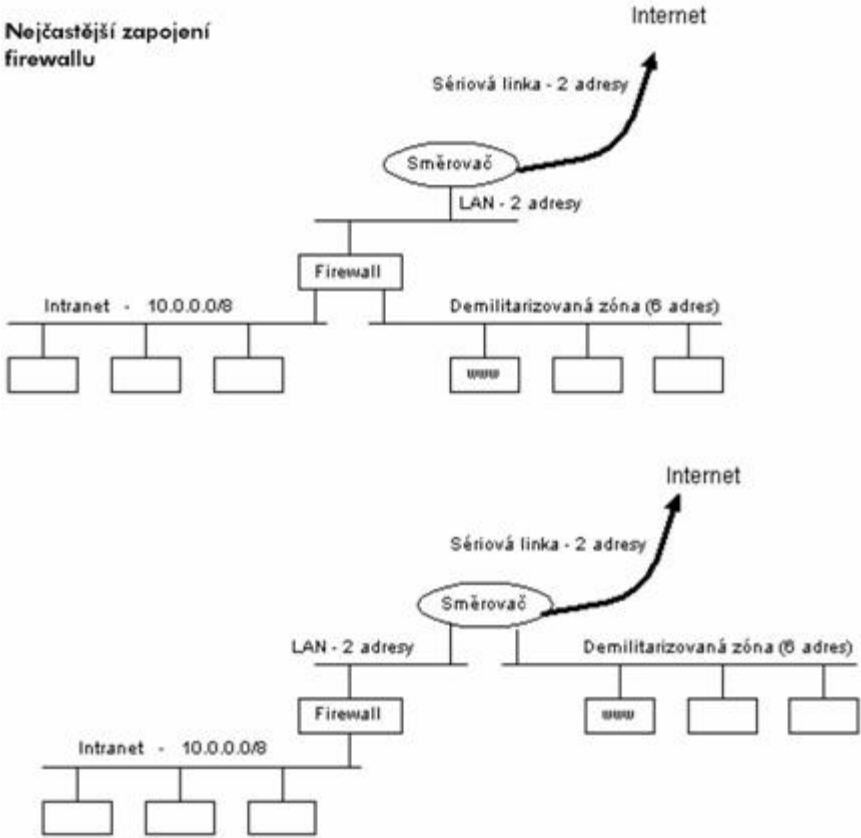
To aby všechny LAN z hlediska poskytovatele tvořily jeden celek (“supersít”), je vyžadováno zejména v případě, kdy firma využívá pro připojení k Internetu komutovaný spoj. Přitom komutovaným spojem může být zálohována i pevná linka (*dialup backup*).

Příklad neřešil problém sériové linky propojující firmu s Internetem. To je třeba projednat vždy s poskytovatelem. Možná, že se vám zdá, proč připojovat jednotlivé provozy do Internetu. Větší a velké firmy se vyznačují tím, že nepotřebují více jak 16 IP-adres. Většinou si vyberou z některého ze zapojení firewallu znázorněného na obrázku:

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

Nejvýše je tedy třeba IP-adresy pro:

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



Úkol 1.9 (krátký úkol)

V jakou velikost má rezerva v adresném plánu?



Shrnutí kapitoly

- Protokol IP verze 4 používá IP-adresu o délce čtyři bajty. IP-adresa adresuje jednoznačně síťové rozhraní systému. Anglicky se takováto jednoznačná adresa nazývá *unicast*. Pokud má systém více síťových karet (více síťových rozhraní) a na všech je provozován protokol IP, pak každé rozhraní má svou IP adresu.
- Je možná i opačná varianta, kdy na jedné síťové kartě (fyzicky jednom síťovém rozhraní) podporujeme několik IP-adres. První adresa se obvykle nazývá primární a další adresy pak sekundární nebo aliasy. Využití sekundárních IP-adres je běžné např. pro WWW-servery
- Jelikož má většina počítačů jedno síťové rozhraní, tak se přeneseně místo IP-adresa rozhraní říká IP-adresa počítače. IP-adresa je tvořena čtyřmi bajty. IP-adresa se zapisuje notací, kde jednotlivé bajty se mezi sebou oddělují tečkou.
- IP-adresa se skládá ze dvou částí: adresy (lokální) sítě a adresy počítače v (lokální) síti.
- IP adresu třídy A v České republice nikdo nemá. Mají ji hlavně nadnárodní společnosti, vládní organizace USA atp. Dovoluje adresování jen 128 sítí, ale v každé z nich může být až 16 miliónů počítačů.
- Třída B umožňuje adresovat už 16 tisíc sítí a 65 tisíc počítačů. V Čechách ji mají významné organizace.
- IP adresou třídy C dokážeme adresovat až 2 milióny sítí. V každé



- síť může být 255 počítačů.
- Síťová maska se používá pro určení adresy sítě. Adresa sítě je částí IP adresy. Síťová maska určuje, které bity v IP-adrese tvoří adresu sítě.
 - Každá firma, která se chce připojit k Internetu, si musí nejprve udělat adresní plán. Ten se obvykle skládá ze dvou částí. Jednak ze schematického znázornění propojení jednotlivých LAN do WAN a jednak ze seznamu jednotlivých LAN s odhadovaným počtem síťových rozhraní na LAN.

Kontrolní otázky

- 1) Vysvětlíte pojem IP adresa. (odpověď naleznete [zde](#))
- 2) Uveďte do jakých tříd se dělí IP adresy a stručně tyto IP adresy charakterizujte. (odpověď naleznete [zde](#))
- 3) Vysvětlíte význam síťové masky. (odpověď naleznete [zde](#))
- 4) Objasněte problematiku IP adres v intranetu. (odpověď naleznete [zde](#))
- 5) Popište řešení problematiky IP adres v síti LAN propojené sériovými linkami. (odpověď naleznete [zde](#))
- 6) Uveďte postup tvorby adresního plánu pro připojení firmy k Internetu. (odpověď naleznete [zde](#))



Pojmy k zapamatování

IP adresa, síťová maska, IP adresy v intranetu, NAT, adresní plán.



Studijní literatura

Základní:

KLEMENT, M. *Výpočetní technika - software a hardware*. 1. vyd. Olomouc: Vydavatelství UP Olomouc, 2002. 178 s. ISBN 80-244-4012-6.

Rozšířená (pro hlubší pochopení):

HORÁK, J. *Hardware*. 2. vyd. Brno: Computer Press, 1998, 331 s. ISBN 80-7226-122-3.



Průvodce studiem

Problematika sítě je náročná a při jejím studiu vyžaduje více, než-li jedno přečtení. Budete-li číst tuto kapitulu podruhé, sami si začnete uvědomovat, že jednotlivé poznatky vzájemně zapadají do souvislého celku.

Nenechte se proto při studiu odradit tím, že něčemu napoprvé neporozumíte.



2 Směrování v síti

Cíle

Po prostudování této kapitoly byste měli být schopni:

- objasnit princip směrování,
- vysvětlit proces předávání a filtrace,
- popsat základní manipulace se směrovacími tabulkami,
- popsat směrovací protokoly.



Průvodce studiem

V tomto okamžiku jste se určitě, jako mnoho studujících před Vámi, podívali na nadpis této kapitoly a „zděsili jste se“. Jistě se ptáte: Jaké směrování? Co to je?...

Uznáváme, že tato kapitola bude operovat s pojmy abstraktnějšího rázu a proto budeme, pokud to je jen trochu možné, využívat názorných analogií z běžného života.

Tak např. *směrování* si představte jako třídění dopisů na poště. Dopisy jsou adresovány do různých míst a k tomu, aby je bylo možné doručit, je nutné jejich roztřídění. Jsou tříděny do pytlů s označeními měst, kam je nutné dopisy doručit.

Toho, kdo dopisy třídí je zase možné přirovnat ke směrovači. *Směrovač* o kterém hovoříme v souvislosti se sítěmi však netřídí dopisy, ale IP-datagramy.

Vidíte jak je to snadné!

Vstupní znalosti:

- pro studium této kapitoly by jste měli mít osvojeny základní poznatky o IP adresách.

Potřebný čas pro studium kapitoly:

- 60 minut



2.1 Obecně o směrování

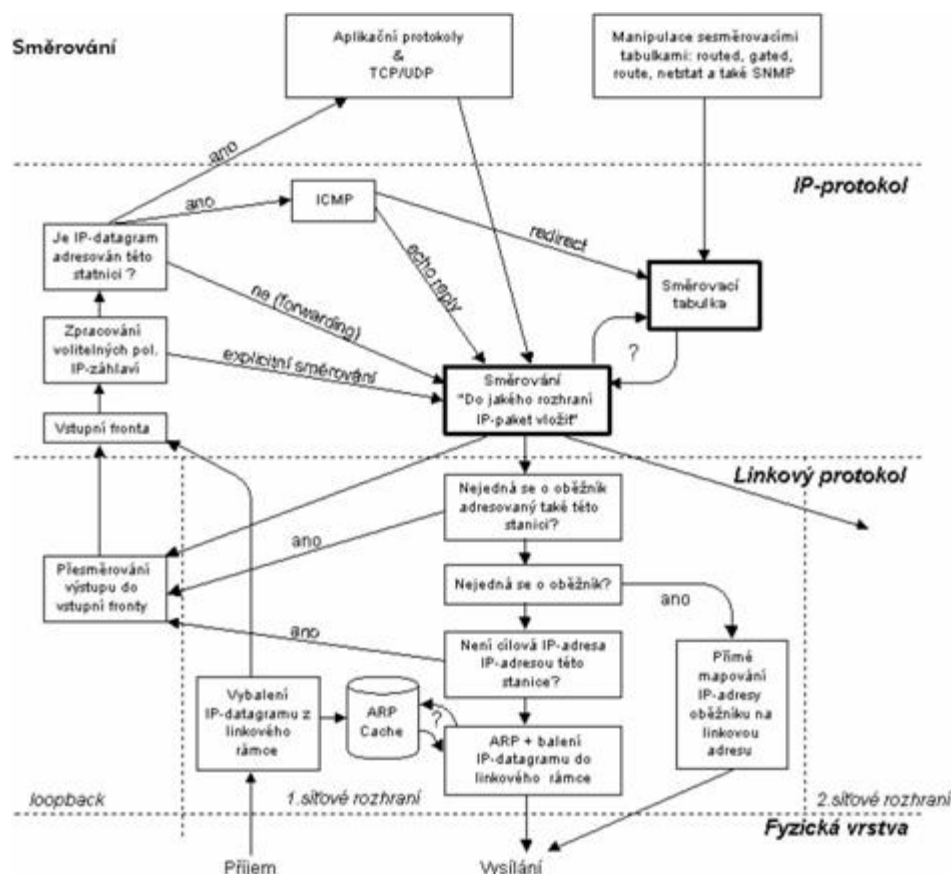
Směrování IP-datagramů (*IP routing*) a předávání IP-datagramů (*IP forwarding*) jsou dva procesy, na kterých Internet stojí. Základní schéma směrování je zobrazeno na níže uvedeném obrázku.

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

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



*Směrování
obecně*



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

2.2 Předávání a filtrace datagramů

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

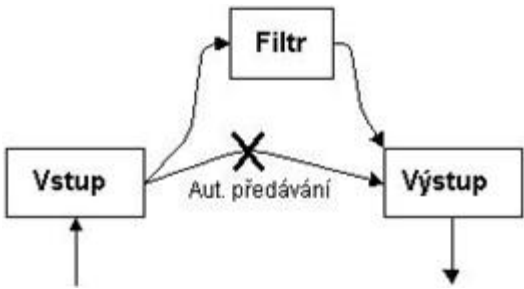
Zajímavou vlastností mnohých operačních systémů je, že IP-datagramy nepředávají mechanicky, ale provádějí filtraci (*screening*), tj. nepředávají všechny pakety, ale jen některé – prolustrované. Většinou filtrace pracuje tak, že před tím, než je IP-datagram předán, tak se celý proces předávání pozastaví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

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

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



Předávání
a filtrace



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

Úkol 2.2 (krátký úkol)

Jakým anglickým slovem se označuje filtrace?



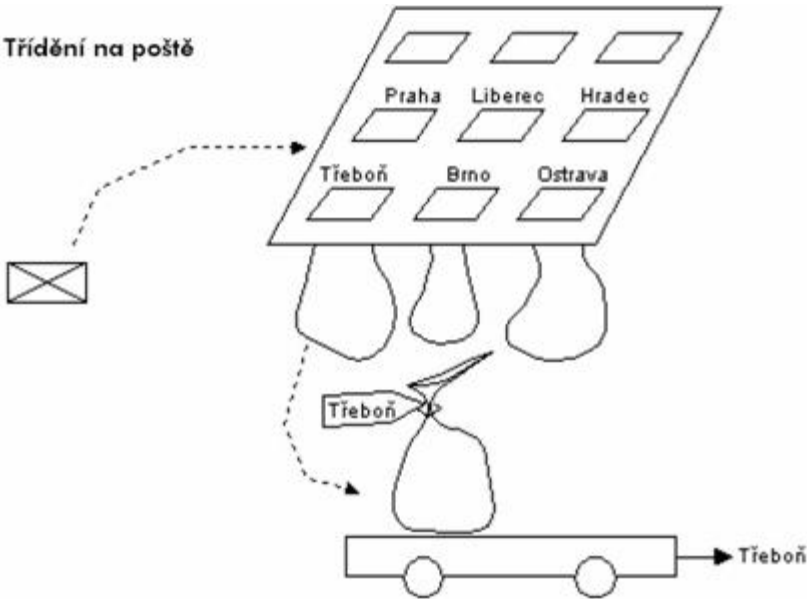
2.3 Směrování datagramů



Směrování

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

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

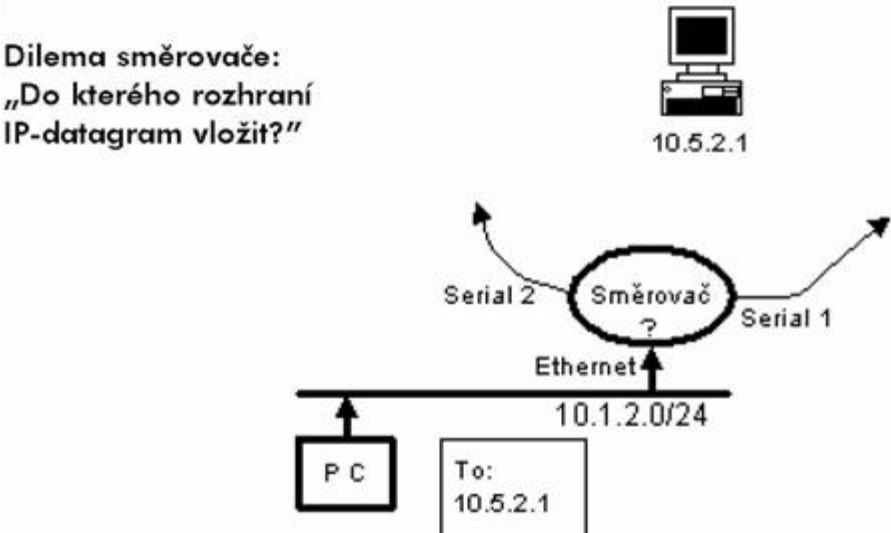


Směrovač netřídí dopisy, ale IP-datagramy. Tento proces se nazývá směrováním.

Směrovač obdrží IP-datagram a musí rozhodnout, do kterého svého

rozhraní jej má vhodit, kterému svému sousedovi (*next hop*) jej má poslat. Zjednodušeně řečeno směrovač je zařízení, které předává IP-datagramy z jednoho svého rozhraní do jiného rozhraní. Směrovač umí předat IP-datagram i do téhož rozhraní, ze kterého IP-datagram přišel. Považuje to však ze výstřednost, takže o tom odesílatele IP-datagramu upozorní ICMP-paketem „*redirect*”.

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



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

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

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

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

Zpracování

2.3.1 Zpracování

V případě, že jsou řádky směrovací tabulky sestupně tříděny, pak stačí

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

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

1. Řádek:

192.168.1.0	255.255.255.0	192.168.254.5	Seriál 1	4
-------------	---------------	---------------	----------	---

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

2. Řádek:

10.1.2.0	255.255.255.0	Lokální rozhraní	Ethernet	0
----------	---------------	------------------	----------	---

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

3. Řádek:

10.5.1.0	255.255.255.0	10.10.10.2	Seriál 2	3
----------	---------------	------------	----------	---

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

4. Řádek:

10.5.0.0	255.255.0.0	10.5.5.5	Seriál 1	2
----------	-------------	----------	----------	---

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

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

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

Úkol 2.3 (krátký úkol)



Co slouží směrovači k rozhodování při směrování datagramů?

2.4 Směrovací tabulky a manipulace s nimi

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

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

2.4.1 Výpis obsahu směrovací tabulky v NT

Příkaz *netstat* vypisuje obsah směrovací tabulky seřazen vzestupně, takže pokud chcete vyhodnocovat tabulku, pak ji musíte procházet zdola nahoru. Trochu nezvyklé je, že rozhraní (*interface*) se jmenují svou IP-adresou. Avšak když se podíváte na první sloupec, tak IP-datagramy adresované adresátovi 194.149.104.121 se mají vkládat do rozhraní 127.0.0.1. Je to správně, protože se jedná o adresu lokálního síťového rozhraní.

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

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

2.4.2 Výpis obsahu směrovací tabulky v UNIXu

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

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



Manipulace se směrovacími tabulkami

Výpis obsahu směrovací tabulky v NT

Výpis obsahu směrovací tabulky v UNIXu

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

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

Sloupec Refs ukazuje kolik je tímto směrem navázáno spojení protokolem TCP. Sloupec Use indikuje, kolik IP-paketů bylo tímto směrem odesláno (zpravidla od startu systému).

Nejzajímavějším sloupcem je sloupec s příznaky (*Flags*). Příznaky mají následující významy:

- U (up). Směr je dostupný.
- G (gateway). Příznak G určuje, že cesta k cílové síti vede přes směrovač. Tj. next hop je směrovač. Linková vrstva bude hledat linkovou adresu uvedeného směrovače, nikoliv přímo adresáta (ten není přímo dostupný).
- H (host). Příznak H určuje, že se jedná o adresu rozhraní (počítače) nikoliv adresu sítě, tj. maska je 255.255.255.255.
- D. Položka byla vytvořena na základě ICMP-zprávy redirect.
- M. Položka byla modifikována na základě zprávy redirect.
- S (static). Jedná se o statickou položku vytvořenou příkazem route.
- R (reject). Tato položka byla rovněž vytvořena příkazem route.

*Naplnění
tabulky
a rušení položek*

2.4.3 Naplnění tabulky a rušení položek

Směrovací tabulka se plní:

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

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

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

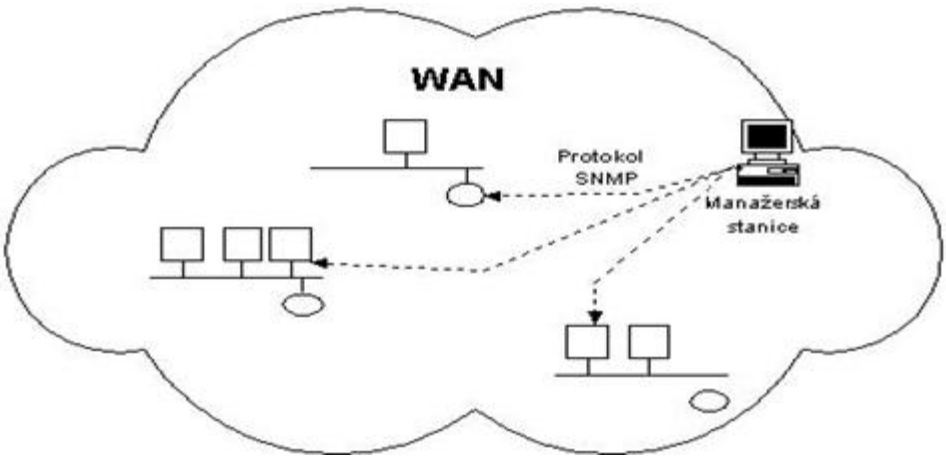
-f          Vymaže nejprve obsah směrovací tabulky.
-p          U příkazu ADD zajistí, aby takto přidaná
            položka zůstala ve směrovací tabulce i po
            restartu PC, tj. stala se trvalou položkou. U
            příkazu PRINT způsobí, že se vypíše trvalé
            položky.
command     Určuje příkaz pro manipulaci se směrovací
            tabulkou, nabývá následujících hodnot:
            PRINT      Vypiš obsah směrovací tabulky
            ADD        Přidej položku do směrovací
                       tabulky.
```

DELETE	Zruš položku ve směrovací tabulce.
CHANGE	Změň položku
destination	Specifikuje cílovou síť.
netmask	Specifikuje síťovou masku
gateway	Specifikuje next hop.
METRIC	Specifikuje metriku.

Manipulace se směrovací tabulkou protokolem SNMP

2.4.4 Manipulace se směrovací tabulkou protokolem SNMP

Pokud ovšem nespravujeme jeden počítač, ale rozsáhlou síť počítačů, pak je velice náročné se postupně přihlašovat na jednotlivé systémy a tam dávat příkaz route. Zpravidla máme k dispozici manažerskou stanici a na všech aktivních prvcích sítě (počítače, směrovače, HUBy, modemy, databáze atd.) běží SNMP agenti, kteří jsou k dispozici manažerské stanici. Z manažerské stanice je možné provádět dotazy na nejrůznější parametry jednotlivých systémů. Mj. je takovým parametrem i položka směrovací tabulky. Takže z manažerské stanice můžeme vypisovat obsah směrovacích tabulek, ale i směrovací tabulky modifikovat. Nesmíte si jen zmodifikovat směrovací tabulky tak, abyste ztratili spojení s manažerskou stanicí ...



Úkol 2.4 (krátký úkol)

Směrovací tabulka se ručně (staticky) plní pomocí příkazu?



2.5 Směrovací protokoly

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

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



Směrovací protokoly

2.5.1 LSP a RVP

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

Nesmím zapomenout u takto doplněné položky zvýšit metriku. Tyto protokoly jsou jednoduché a snadno se implementují. Jejich nevýhodou je, že ve větších rozsáhlých sítích může výměna vektorů oscilovat a pak některé vzdálenější sítě mohou být chvíli dostupné a za okamžik již nikoliv. Většími sítěmi se rozumí sítě o více jak 10 LAN.

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

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

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

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

Protokoly LSP jsou oproti protokolům RVP nesrovnatelně stabilnější a lze je aplikovat i u velmi rozsáhlých sítí. Nevýhodou je, že návrh sítě, tj. rozdělení sítě na oblasti musí provést zkušený odborník, rovněž konfigurace je netriviální. Pokud se použije protokol typu LSP bez větších zkušeností, tak je také možné, že některými linkami data prostě nepotečou a jiné budou přetížené.

2.5.2 IGP a EGP

Protokoly IGP jsou určeny pro činnost v rámci autonomního systému. Již zmíněné protokoly RIP, RIP2, OSPF i IS-IS jsou vesměs protokoly IGP. Ovšem poskytovatelé Internetu si mezi sebou potřebují také vyměňovat směrovací informace. Poskytovatelé Internetu pro výměnu směrovacích informací mezi autonomními systémy používají protokoly

IGP a EGP

Agregace

EGP. V dnešní době používají protokol BGP (*Border Gateway Protocol*) verze 4.

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

2.5.3 Agregace

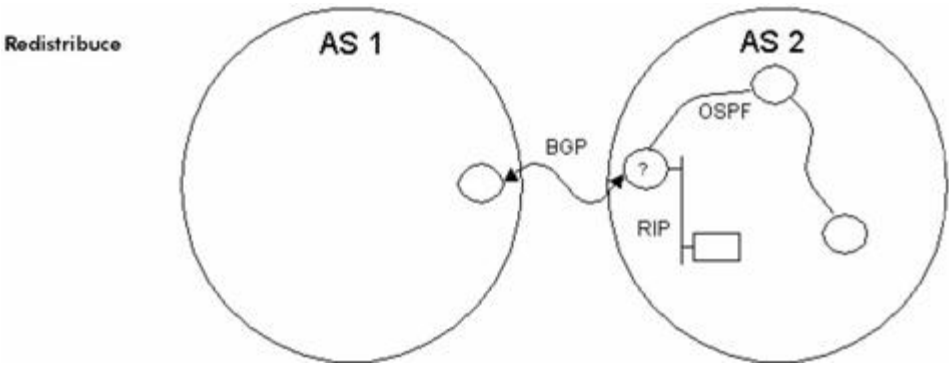
Agregace je proces, kdy se z několika položek směrovací tabulky udělá jedna položka. Tento proces je žádoucí např. při propagaci sítí vně autonomního systému. Jednu položku můžeme z více udělat tehdy, když sítě slučované do jedné položky vytvoří supersít'.

Automatická agregace je spíše přání než realita. Poskytovateli většinou vypadnou z jeho supersítí některé adresy, které ještě nikomu nepřidělil, takže nelze automaticky agregovat všechny IP-adresy autonomního systému do jedné nebo několika málo položek. Prakticky se agregace provede ručně tak, že se vně autonomního systému propagují všechny IP-adresy, které jsou přiděleny.

Redistribuce

2.5.4 Redistribuce

Na obrázku je otazníkem označen směrovač, který si vyměňuje současně směrovací informace protokoly BGP, OSPF, RIP a k tomu možná má ve směrovací tabulce několik statických položek. Otázka je, zdali se mají informace (položky směrovací tabulky) získané jedním směrovacím protokolem propagovat do ostatních směrovacích protokolů, tj. má-li se provést redistribuce.



Položka ve směrovací tabulce musí v sobě nést tedy také informaci, jakým protokolem byla vytvořena.

Úkol 2.5 (krátký úkol)

Příkladem protokolů RVP jsou protokoly?



Shrnutí kapitoly

- Směrování IP-datagramů (*IP routing*) a předávání IP-datagramů (*IP forwarding*) jsou dva procesy, na kterých Internet stojí.
- že při zpracování vstupů v některých případech operační systém informace automaticky předává na výstup (do procesu směrování), tj. aplikační programy do tohoto předávání nezasahují. Jedná se



zejména o: explicitní směrování, předávání, požadavek o echo, přesměrování.

- Předávání umožňuje stanici pracovat jako směrovač. Pokud stanice zjistí, že IP-datagram není adresován pro ni, pak se jej pokouší předat dále, tj. odeslat jako odesílá své IP-datagramy.
- Předávaný IP-datagram se předá filtračnímu procesu, který buď předání schválí, nebo zamítne.
- Směrování IP-datagramů je velice podobné třídění dopisů na poště.
- Směrovač obdrží IP-datagram a musí rozhodnout, do kterého svého rozhraní jej má vhodit, kterému svému sousedovi (*next hop*) jej má poslat.
- Směrovací tabulku je třeba jednotlivými položkami naplnit. Položky jsou pak v tabulce trvale, dokud je někdo nezruší nebo nevypne systém.
- Směrovací protokoly jsou aplikační protokoly, které neslouží uživatelům (osobám), ale směrovačům, aby si vzájemnou komunikaci mezi sebou automaticky naplnily směrovací tabulky.

Kontrolní otázky

- 1) Vysvětlíte princip směrování. (odpověď naleznete [zde](#))
- 2) Objasněte princip předávání a filtrace. (odpověď naleznete [zde](#))
- 3) Uveďte, k jakému účelu se užívá příkazu *netstat*. (odpověď naleznete [zde](#))
- 4) Popište směrovací protokoly LSP a RVP. (odpověď naleznete [zde](#))
- 5) Popište směrovací protokoly IGP a EGP. (odpověď naleznete [zde](#))
- 6) Vysvětlíte pojem směrovací tabulka. (odpověď naleznete [zde](#))

Pojmy k zapamatování

Směrování, předávání a filtrace, směrovací tabulka, směrovací protokol.

Studijní literatura

Základní:

KLEMENT, M. *Výpočetní technika - software a hardware*. 1. vyd. Olomouc: Vydavatelství UP Olomouc, 2002. 178 s. ISBN 80-244-4012-6.

Rozšířená (pro hlubší pochopení):

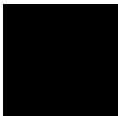
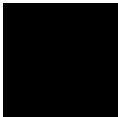
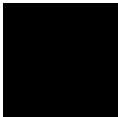
HORÁK, J. *Hardware*. 2. vyd. Brno: Computer Press, 1998, 331 s. ISBN 80-7226-122-3.

Průvodce studiem

Pokud jste zvládli nastudovat obsah této kapitoly, musíme Vás pochválit. Nebyla příliš jednoduchá, i když jsme se Vám učení pomocí analogií snažili maximálně zjednodušit.

Nicméně, i když jste nepochopili vše na 100 %, tak si udělejte delší přestávku spojenou s pohybem či činností jiného charakteru a potom pokračujte ve studiu.

V další lekci se budeme zabývat protokoly TCP a UDP.



3 Přenosové protokoly TCP a UDP

Cíle



Po prostudování této kapitoly byste měli být schopni:

- vysvětlit pojem protokol TCP,
- vysvětlit pojem protokol UDP,
- popsat TCP segment,
- objasnit princip navázání a ukončení spojení protokolem TCP,
- zjistit stav spojení.

Průvodce studiem

V předchozích kapitolách jsme již několikrát s různých souvislostech pojednávali o IP protokolu. Oproti němu je protokol TCP, o němž bude řeč v této kapitole, protokolem vyšší vrstvy. Již jsme si vysvětlili, že protokol IP přepravuje data mezi libovolnými počítači v Internetu. Protokol TCP se odlišuje od IP protokolu tím, dopravuje data mezi dvěma konkrétními aplikacemi běžícími na těchto počítačích. Více se již ale dozvíte v následujícím textu.



Vstupní znalosti:

- pro studium této kapitoly nepotřebujete žádné odborné znalosti.

Potřebný čas pro studium kapitoly:

- 50 minut

3.1 Obecně o protokolech TCP a UDP



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

*Protokol TCP
a UDP*

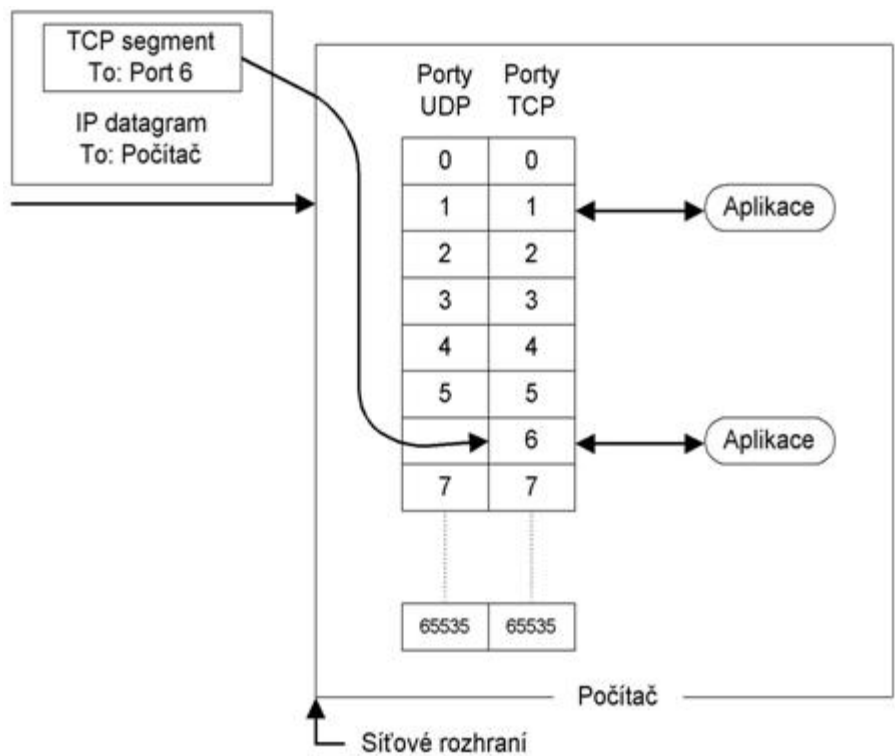
Pro dopravu dat mezi počítači se využívá protokol IP. Protokol IP adresuje IP-adresou pouze síťové rozhraní počítače. Pokud bychom použili přirovnání k běžnému poštovnímu styku, pak IP-adresa odpovídá adrese domu a port (adresa v protokolu TCP) pak odpovídá jménu konkrétního obyvatele domu.

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

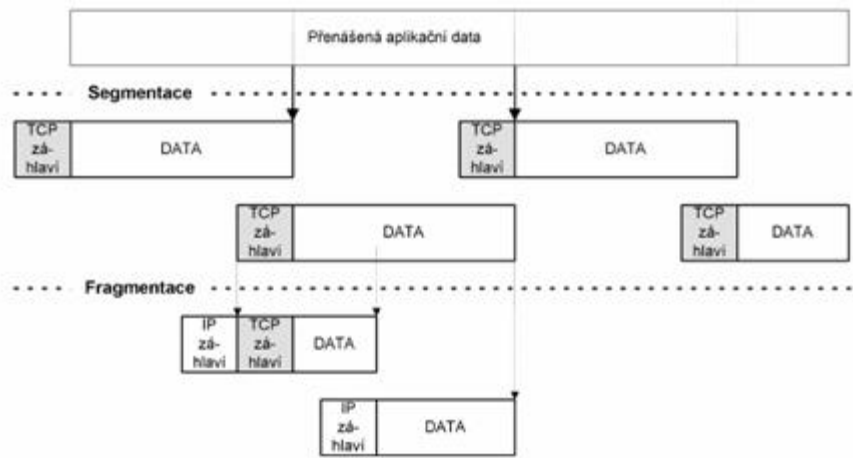
Konce spojení („odesílatel” a „adresát”) jsou určeny tzv. číslem portu. Toto číslo je dvojbajtové, takže může nabývat hodnot 0 až 65535. U čísel portů se často vyjadřuje okolnost, že se jedná o porty protokolu TCP tím, že se za číslo napíše lomítko a název protokolu (tcp). Pro protokol UDP je jiná sada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

nemá nic společného s portem 53/udp.

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



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



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

Úkol 3.1 (krátký úkol)

Protokol TCP je proti protokolu IP protokolem jaké vrstvy? Nižší nebo vyšší?



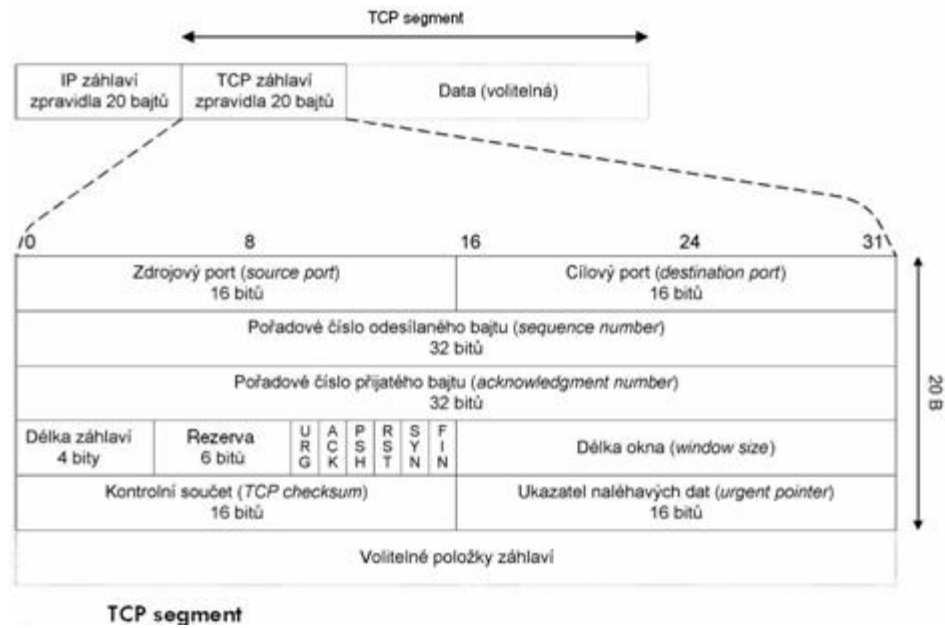
3.2 TCP segment



TCP segment

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

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



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

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

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

V poli příznaků mohou být nastaveny následující příznaky:

- **URG** – TCP segment nese naléhavá data.
- **ACK** – TCP segment má platné pole „Pořadové číslo přijatého bajtu” (nastaven ve všech segmentech kromě prvního segmentu, kterým klient navazuje spojení).
- **PSH** – Zpravidla se používá k signalizaci, že TCP segment nese aplikační data, příjemce má tato data předávat aplikaci. Použití tohoto příznaku není ustáleno.

- **RST** – Odmítnutí TCP spojení.
- **SYN** – Odesílatel začíná s novou sekvencí číslování, tj. TCP segment nese pořadové číslo prvního odesílaného bajtu (ISN).
- **FIN** – odesílatel ukončil odesílání dat. Pokud bychom použili přirovnání k práci se souborem, pak příznak FIN odpovídá konci souboru (EOF). Přijetí TCP segmentu s příznakem FIN neznámá, že v opačném směru není dále možný přenos dat.

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

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

Úkol 3.2 (krátký úkol)

Ukazatel naléhavých dat je reprezentován příznakem?



3.3 Navázání a ukončení spojení protokolem TCP

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



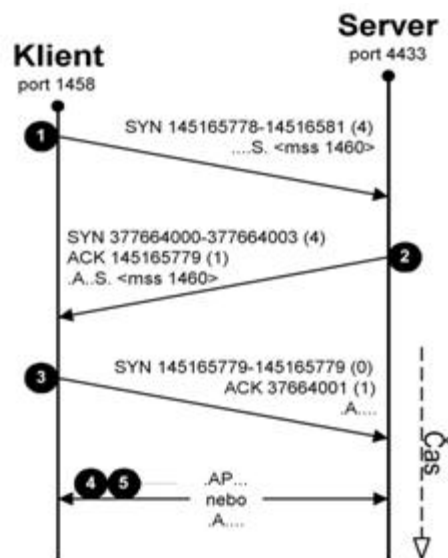
*Navázání
a ukončení
spojení
protokolem TCP*

3.3.1 Navazování spojení

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

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

*Navazování
spojení*

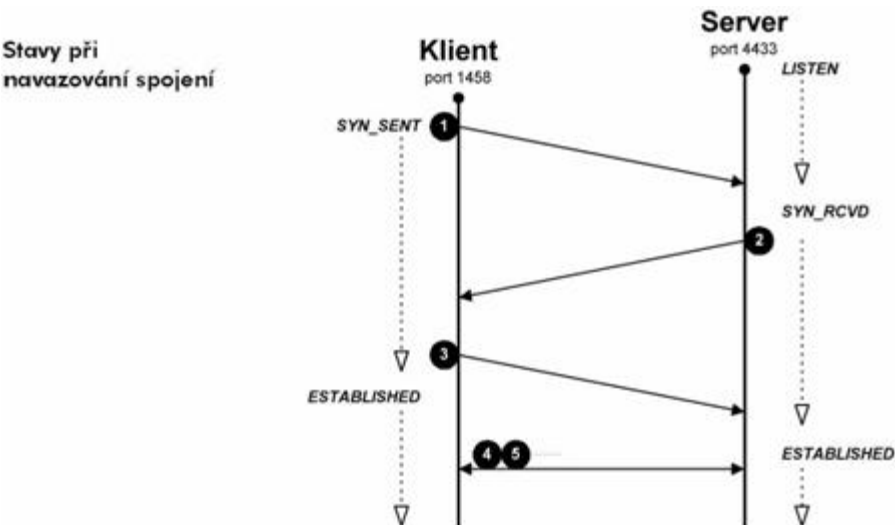


Ne všechny TCP segmenty musí nutně nést aplikační data, tj. mít nastaven příznak PSH (.AP...). Může se stát, že jeden konec spojení odesílá data, avšak druhý konec nemá momentálně žádná data k odeslání. I když druhý konec nemá co posílat, tak musí potvrzovat přijatá data. Takové potvrzování provádí TCP segmenty s nenastaveným příznakem PSH (.A....), tj. segmenty bez dat.

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

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

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



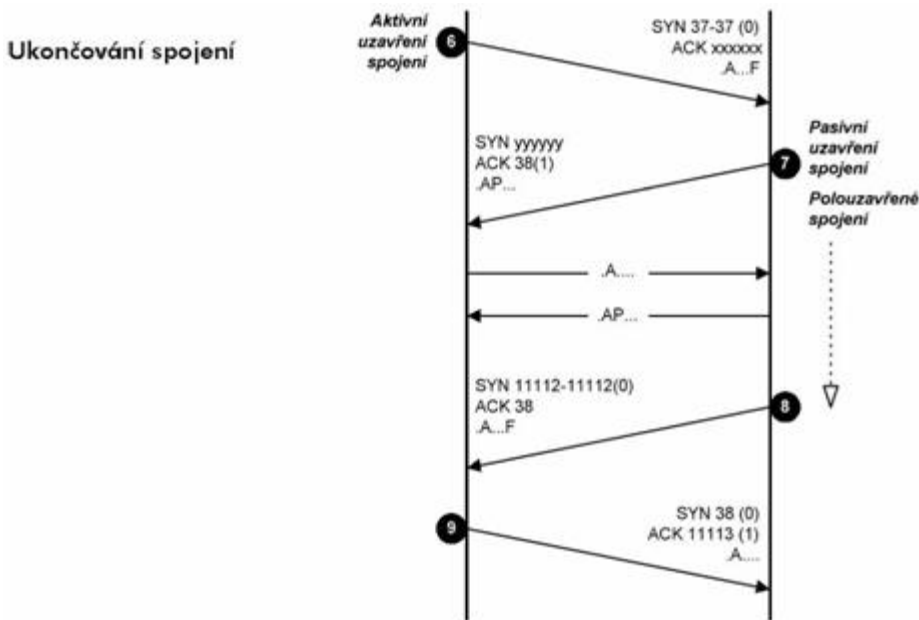
Ukončování spojení

3.3.2 Ukončování spojení

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

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

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



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

Stavy při ukončování spojení:

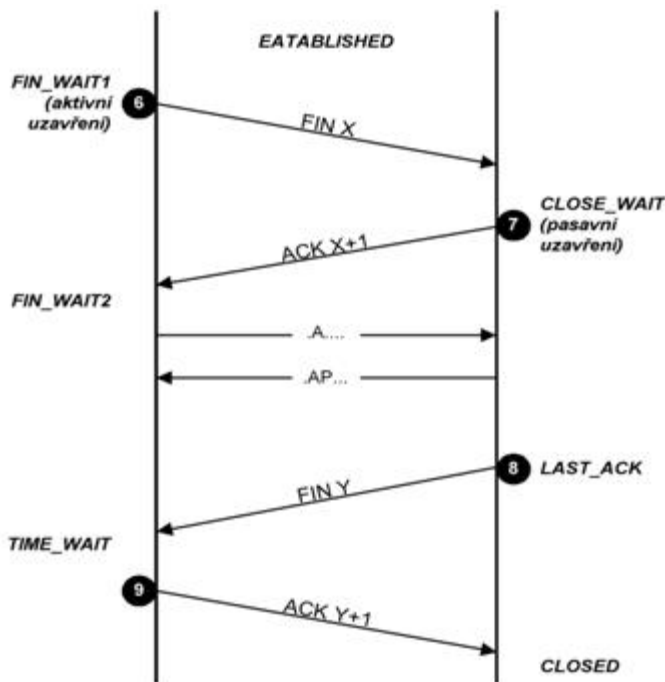
- **FIN_WAIT1** – strana zjistila, že již všechna data odeslala (a potřebuje signalizovat konec souboru – EOF), tak v TCP segmentu nastaví příznak FIN, čímž signalizuje aktivní uzavření spojení segmentem 6.
- **CLOSE_WAIT** – druhá strana obdržela aktivní uzavření spojení a nezbyvá jí nic jiného než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

Odmítnutí
spojení

segment 9 přechází do stavu CLOSED.

3.3.3 Odmítnutí spojení

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



Spojení je odmítáno v zásadě ve dvou případech:

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

Zjištění stavu spojení

3.3.4 Zjištění stavu spojení

Výpis všech spojení protokoly TCP a UDP lze získat pomocí příkazu netstat s parametrem -a.
\$ netstat -a

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp	0	0	194.149.105.18.22	194.149.103.204.24695	TIME_WAIT
tcp	0	0	194.149.105.18.3099	194.108.145.128.25	SYN_SENT
tcp	0	34472	194.149.105.18.3079	195.47.32.245.25	ESTABLISHED
tcp	0	0	*.22	*,*	LISTEN
tcp	0	0	*.25	*,*	LISTEN
tcp	0	0	*.53	*,*	LISTEN
udp	0	0	*.53	*,*	
udp	0	0	127.0.0.1.53	*,*	

První dva řádky tvoří záhlaví výpisu. Význam jednotlivých sloupců:

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

Úkol 3.3 (krátký úkol)

Pokud se spojení naváže, pak klient i server přecházejí do stavu?

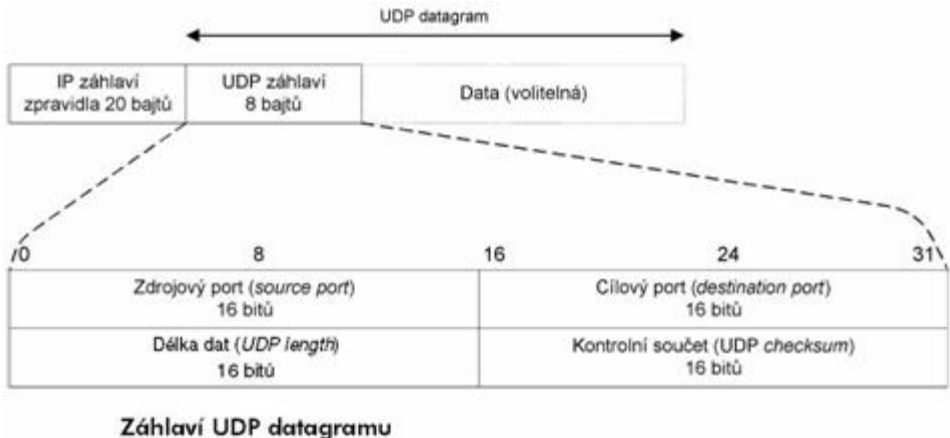


3.4 Protokol UDP

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



Protokol UDP
(User Datagram Protocol)



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

nezávislou sadu čísel portů.

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

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

Fragmentace

3.4.1 Fragmentace

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

Oběžníky

3.4.2 Oběžníky

Na první pohled by se zdálo, že protokol UDP je chudým příbuzným protokolu TCP. Může však existovat něco, co umí protokol UDP a nelze to udělat protokolem TCP? Právě zvláštností protokolu UDP je skutečnost, že adresátem UDP datagramu nemusí být pouze jednoznačná IP-adresa, tj. síťové rozhraní konkrétního počítače. Adresátem může být skupina stanic – adresovat lze i oběžník.

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

Úkol 3.4 (krátký úkol)

Protokol UDP je spojová nebo nespojová služba?



Shrnutí kapitoly

- Protokol TCP je proti protokolu IP protokolem vyšší vrstvy. Zatímco protokol IP přepravuje data mezi libovolnými počítači v Internetu, tak protokol TCP dopravuje data mezi dvěma konkrétními aplikacemi běžícími na těchto počítačích.
- Protokol TCP je spojovanou službou (*connection oriented*), tj. službou která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry).
- Konce spojení (“odesílatel” a „adresát”) jsou určeny tzv. číslem portu. Toto číslo je dvojbajtové, takže může nabývat hodnot 0 až 65535.



- **Zdrojový port** (*source port*) je port odesílatele TCP segmentu, **cílový port** (*destination port*) je portem adresáta TCP segmentu. Pětice: zdrojový port, cílový port, zdrojová IP-adresa, cílová IP-adresa a protokol (TCP) jednoznačně identifikuje v daném okamžiku spojení v Internetu.
- TCP segment je část z toku dat tekoucích od odesílatele k příjemci.
- Protokol TCP využívá k transportu dat Internetem protokol IP, avšak nad tímto protokolem zřizuje spojovanou službu. Musí řešit problémy navázání a ukončení spojení, potvrzování přijatých dat, vyžádání ztracených dat, ale také problémy průchodnosti přenosové cesty.
- Protokol UDP je jednoduchou alternativou protokolu TCP. Protokol UDP je nespojovaná služba (na rozdíl od protokolu TCP), tj. nenavazuje spojení. Odesílatel odešle UDP datagram příjemci a už se nestará o to, zdali se datagram náhodou neztratil (o to se musí postarat aplikační protokol).

Kontrolní otázky

- 1) Vymezte rozdíl mezi IP protokolem a protokolem TCP. (odpověď naleznete [zde](#))
- 2) Vysvětlíte pojem *protokol TCP*. (odpověď naleznete [zde](#))
- 3) Popište TCP segment. (odpověď naleznete [zde](#))
- 4) Objasněte princip navázání a ukončení spojení protokolem TCP. (odpověď naleznete [zde](#))
- 5) Vysvětlíte pojem *protokol UDP*. (odpověď naleznete [zde](#))



Pojmy k zapamatování

Protokol TCP, protokol UDP, TCP segment.



Studijní literatura

Základní:

KLEMENT, M. *Výpočetní technika - software a hardware*. 1. vyd. Olomouc: Vydavatelství UP Olomouc, 2002. 178 s. ISBN 80-244-4012-6.

Rozšířená (pro hlubší pochopení):

HORÁK, J. *Hardware*. 2. vyd. Brno: Computer Press, 1998, 331 s. ISBN 80-7226-122-3.



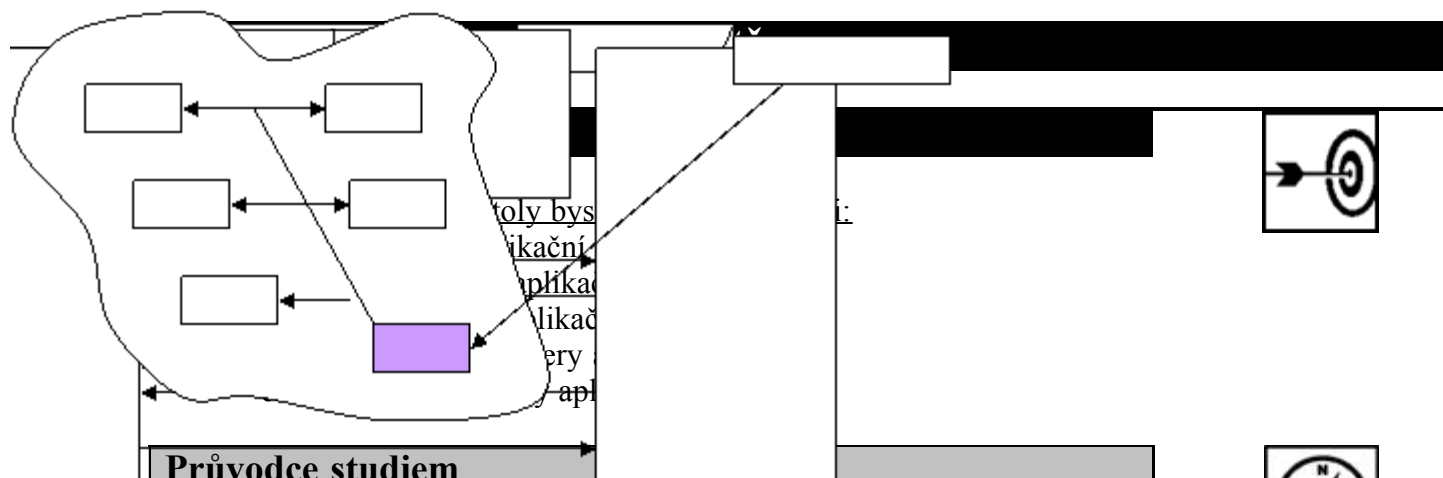
Průvodce studiem

Pokud se Vám zdá, že zapomínáte to, co jste se naučili v předchozích kapitolách tak nezafrčte. To je normální průvodní jev při učení. Jak se sami přesvědčíte, ke zopakování Vám však bude tentokrát stačit mnoho méně času.

Doporučujeme Vám nepodceňovat kontrolní otázky uvedené vždy v závěrech kapitol. Dotazují se na základní učivo, které je potřebné znát.

Nepodceňujte význam relaxace a odpočinku. Rychlé memorování nelze považovat za efektivní metodu učení a vědomosti nejsou trvalé. To jistě ale víte a proto se učíte průběžně.





Průvodce studiem

V této poslední kapitole disciplíny se budeme společně zabývat aplikační vrstvou. Aplikační vrstva je poslední vrstvou referenčního modelu. Koncoví uživatelé využívají počítačové sítě prostřednictvím nejrůznějších síťových aplikací (softwarových serverů) - systémů elektronické pošty, přenosů souborů, vzdáleného přihlašování (remote login) a podobně.

Začleňovat všechny tyto různorodé aplikace přímo do aplikační vrstvy by nebylo rozumné. Proto se do aplikační vrstvy zahrnují jen části těchto aplikací, které realizují společně respektive obecně použitelné mechanismy. O tom se již ale více dozvíte v následujícím textu.

Vstupní znalosti:

- pro studium této kapitoly nepotřebujete žádné odborné znalosti.

Potřebný čas pro studium kapitoly:

- 70 minut

4.1 Aplikační vrstva obecně

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

Služby aplikační vrstvy:

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



Aplikační vrstva

4.2 Klasifikace služeb aplikační vrstvy

- **Podle síťového modelu:**
 - model server/klient
 - model peer-to-peer – rovnoprávný (stejná funkce na všech komponentách)
- **Podle služeb:**
 - *datagramové* – pro aplikace jednotného charakteru, např. jmenné služby, čas apod.
 - *virtuální okruhy* – při přenášení velkého množství dat, kde záleží na bezchybném přenesení
- **Podle způsobu práce:**
 - *interaktivní* – v jednu chvíli obhospodařují 1 požadavek
 - *procesně orientované* – vytvoření spec. procesu na uspokojení našeho požadavku a poté zrušení tohoto procesu; počet procesů je omezen (u ftp, gopher atd.)
- **Podle zapamatování stavu:**
 - *stavový*
 - *bezstavový* – pamatují si stav rozpracování a pokračování práce tam, kde došlo k přerušení; server si nemusí nic pamatovat, informace o úplnosti posílá na hostitelský počítač



*Klasifikace
služeb aplikační
vrstvy*

Úkol 4.2 (krátký úkol)

Podle síťového modulu můžeme služby aplikační vrstvy klasifikovat na sítě typu?



4.3 Typy serverů aplikační vrstvy

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

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



*Typy serverů
aplikační vrstvy*

4.3.1 Diskový server

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

Diskový server

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

Souborový server

4.3.2 Souborový server

Souborový server (file server) rovněž umožňuje sdílet uživatelům vysokokapacitní disk, avšak nikoli na fyzické úrovni, nýbrž na úrovni logické. Tento server může na rozdíl od předchozího implementovat různé způsoby ochrany souborů či vět proti současnému přístupu více uživatelů.

Ochrana dat před neoprávněným použitím je obvykle realizována pomocí hesel, popřípadě pomocí přístupových práv jednotlivých uživatelů. Realizace souborového serveru je sice složitější než u serveru diskového, přesto je prvně jmenovaný typ serveru používán mnohem častěji.

- slouží k ukládání souborů na vybraném PC
- souborový systém se dělí na: svazky, adresáře, soubory
- možnost sdílení dat, ale nutnost vytvoření ověřovacích mechanismů uživatele a mechanismus přístupových práv k souborům

R.....čtení

W.....zápis

X.....spuštění programu

....

- využití mapování disků k ztotožňování svazku s nějakou částí adresářového stromu disku na souborovém serveru
- typy: NOVEL v 5.x (Dos)
NFS – Network File System (Unix)
NTFS – NT File System (NT Server)
AFS – Andrew File System (Orion)

Tiskový server

4.3.3 Tiskový server

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

- realizování disků na společné tiskárně a síťové tiskárny

Lokální tisk

- text, který chceme vytisknout se nejprve převede do jazyka tiskárny a poté až je vytištěn

Sít'ový tisk

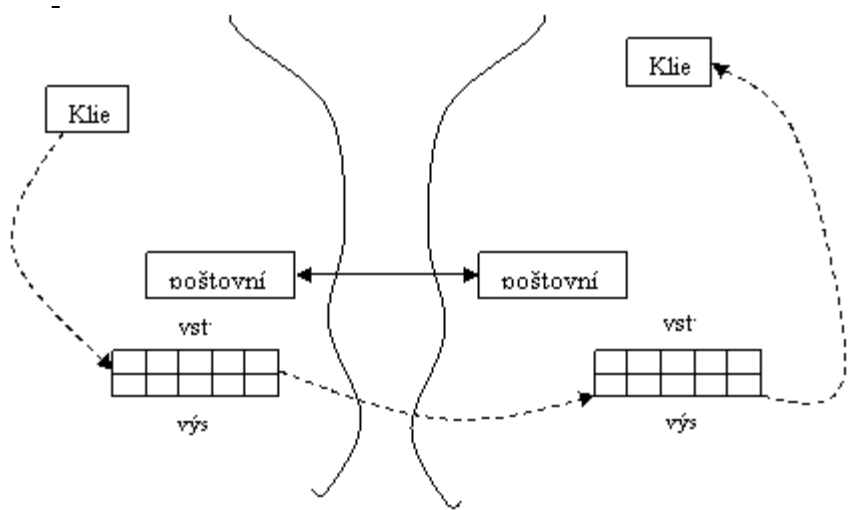
- sít'ový server obsluhuje více klientů současně & vznik *fronty*
- požadavky na tisk se řadí tedy do fronty, kde existují následující stavy: vytváří se, připraven k tisku, tiskne se
- existují také příkazy např. na upřednostňování ve frontě, mazání z fronty apod.
- přístup k tiskovému serveru:
 - ✓ *přesměrováním* – převedení tisku na sít'ovou tiskárnu; v Novelu příkazy „capture, endcap“
 - ✓ *tisk souboru* – a) uložení tiskové sestavy do souboru
b) kopírování souboru na tiskárnu (copy/b soubor.prn lpt2)

Poštovní server
a elektronická
pošta

4.3.4 Poštovní server a elektronická pošta

- slouží k přenosu zpráv v datovém režimu
- přenáší se :
 - text (původně) – ASCII znaky
 - formátované dokumenty (text) – např. .pdf (portable data formular)
 - zvuk & voicemail
 - obraz
 - video
 - data (programy) – binární data

funkce elektronické pošty:



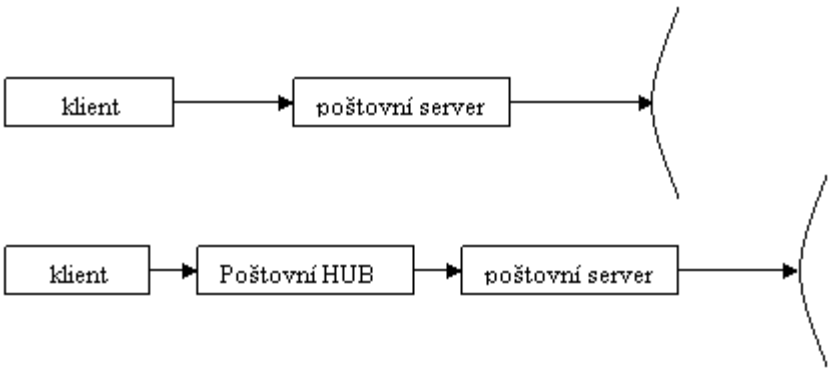
- k chybě může dojít např. přeplněním poštovního serveru

formát přenášených zpráv:

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

prostředky pro přístup k elektronické poště:

- odesílání pošty



- přijímání pošty

poštovní přihrádka (mail)

.....programy: pine, elmumí manipulovat se soubory
v pošt. adresáři

vzdálený přístup k elektronické poště:

- **POP – Post Office Protocol**
 - na PC běží tzv. POP klient
 - název POP serveru MVSO je pop.mvso.cz
- **IMAP – Internet Mail Access Protocol**
 - funguje obdobně, ale umožňuje pracovat s poštou i částečně: přenesení autorů zpráv, věcí apod.

*List server -
Elektronická
konference*

4.3.5 List server - Elektronická konference

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

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

- uzavřené
- otevřené

druhé členění na:

- moderované
- nemoderované

komunikace:

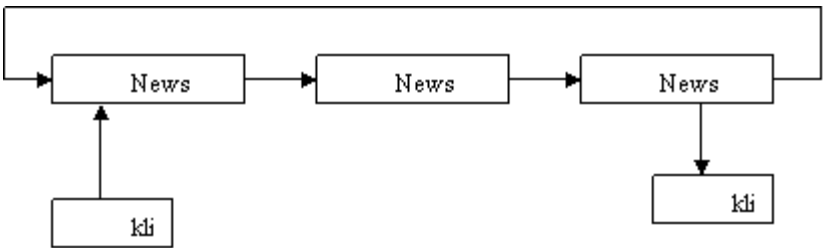
- administrativní (řídící) kanál
 - umožňuje přihlášení, odhlášení, pozastavení a obnovení členství, výpis seznamu konferencí, seznamu členů, help
 - např. listserv@list.zcu.cz, majordomo@..., název konference-request@....
- datový kanál
 - samotný přenos zpráv
 - např. webnet@list.zcu.cz

News server -
Elektronické
news

4.3.6 News server - Elektronické news

Veřejně přístupná síť na internetu, která organizuje veřejné diskusní skupiny a skupinové poštovní schránky. Diskusní skupiny neboli USENET slouží k diskuzím uživatelů na určitá témata, která většinou vystihují názvy jednotlivých skupin. Skupiny jsou uloženy na tzv. **newsserveru**. Pro připojení se k newsserveru je potřeba mít nainstalován klient (součást např. balíku Mozilla Suite).

- zaslané příspěvky se pouze ukládají na servery, na kterých je možné si je přečíst & nedochází k odesílání klientům



Časový server

4.3.7 Časový server

Server, který periodicky synchronizuje čas ve všech počítačích v rámci sítě. Tím je zajištěna shodnost času používaného síťovými službami a místními funkcemi.

Potvrzení od důvěryhodné třetí strany o existenci určité zprávy v určitý časový okamžik. V digitálním kontextu důvěryhodná třetí strana vygeneruje pro danou zprávu důvěryhodné časové razítko tak, že pomocí služby časového razítka doplní do zprávy příslušnou časovou hodnotu a pak výsledek digitálně podepíše.

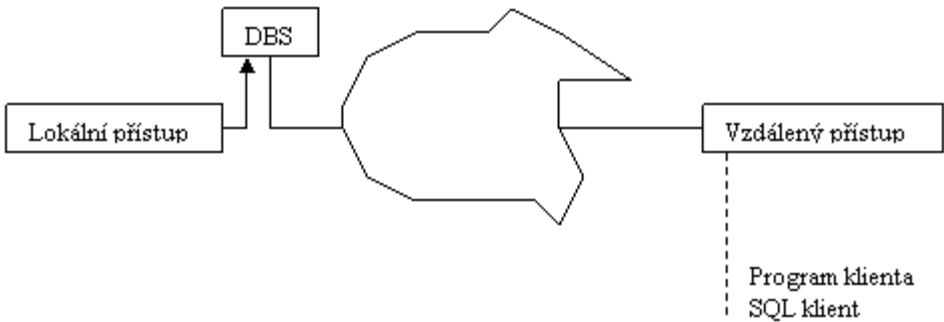
- pro připojení do počítačové sítě dochází k synchronizaci času mezi naším počítačem a serverem, ke kterému se připojujeme
- u rozsáhlých sítí je to složitější a existují časové servery, které poskytují přesný čas (buď získaný z jiného časového serveru, nebo přímo z časového etalonu – atomové hodiny,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

Databázový server

4.3.8 Databázový server

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

- jazykem pro přístup k databázím je *SQL- Structure Query Language*
- unifikovaný přístup



WWW server

4.3.9 WWW server

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

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

Základní pojmy:

HTTP – Hypertext Transfer Protocol

- kromě zobrazitelných znaků obsahuje i další odkazy na související text

HTML – Hypertext Markup Language

- obsahuje řídící znaky a texty
- obsahuje formáty a odkazy

URL – Uniform Resource Locator

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

SERVER – http server b relativně jednoduchý (například IIS)

KLIENT – relativně složitý, univerzální (například prohlížeč Internet Explorer)

Formát přenášených dat:

<HTML>

<HEAD> záhlaví...autorská práva, vypršení

</HEAD> platnosti, kódování

<BODY>

</BODY> vlastní tělo...vlastní stránka

</HTML>

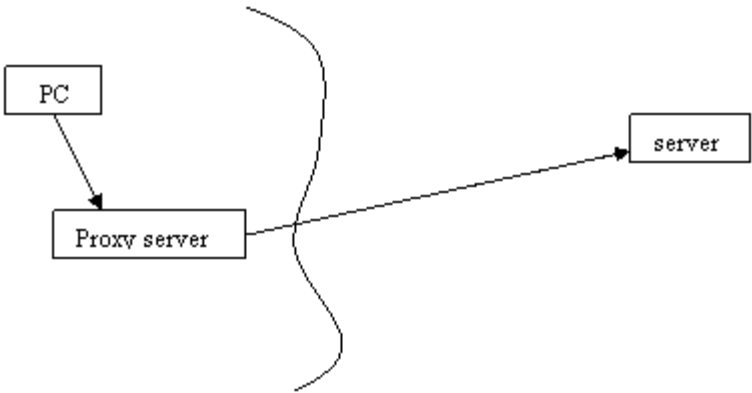
..... značky v dokumentu buď párové nebo nepárové (např. <p>)

Dokumenty (html stránky):

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

Problémy:

- vyžaduje přenos velkého objemu dat a zavedení vyrovnávacích pamětí (cache)
- tyto vyrovnávací paměti jsou uloženy v mezilehlých uzlech a proxy servery (zástupné)
- možnost filtrace, a kontroly práce na síti (problémem např. v bankovníctví)



Brány:

- umožnění komunikace, překlad do html a přesun klientům
- např. netfind, whois, protokoly

Úkol 4.3 (krátký úkol)

Jaký port TCP používá WWW server?



4.4 Služby aplikační vrstvy

4.4.1 TELNET – vzdálený terminál

- historicky různé typy terminálů: VT100, VT320... (čím větší číslo tím dokonalejší)
- služba telnetu je implicitně přístupná přes port = 23
- znaky na telnet klientovi se zobrazují na obrazovce až po vrácení z telnet serveru

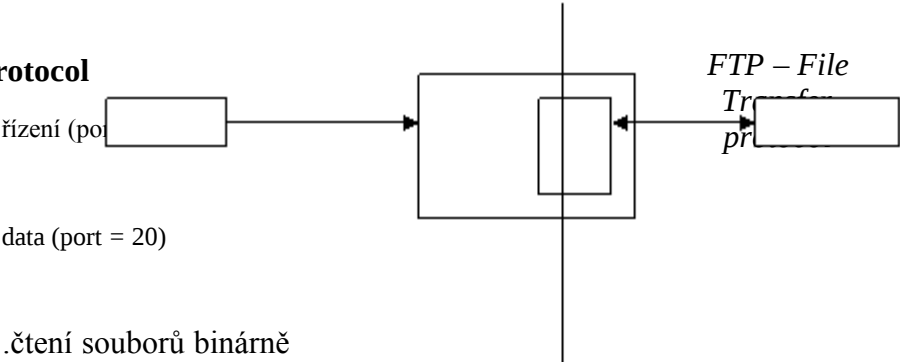


*TELNET –
vzdálený
terminál*

Otevřená podoba

- proti odzírání ve formě otevřené podoby se používá **ssh** – **secured shell** ▶ prostředek umožňující normální funkce, ale v šifrované podobě; použití port = 22

4.4.2 FTP – File Transfer protocol



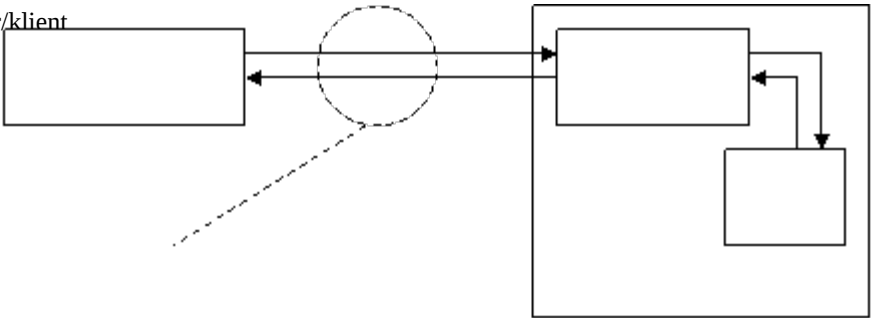
- bin.....čtení souborů binárně
- ascii.....čtení textových souborů
- prompt.....přepínač, zapíná/vypínání dotazů
- hash.....zobrazování křížku za každý přenesený kb
- !.....ovládání v našem vlastním adresáři
- lcd.....změna domácího adresáře

- ftp serverů je ve světě hodně
- zvláštní formou jsou pak indexové servery ▶ *archie servery* (jméno programu a místo uložení)

4.4.3 FINGER

FINGER

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



požadavek
informace

požadavek:

- ✓ jméno uživatele + @jméno hosta
- ✓ přihlašovací jméno uživatele

informace:

- ✓ výpis informací o uživateli
- ✓ výpis informací o přihlášených uživateli

NETFIND

4.4.4 NETFIND

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

WHOIS

4.4.5 WHOIS

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

4.4.6 Videokonference

Videokonference

- přenos obrazu a zvuku
- internetové rádio, internetová televize, videokonference

zobrazování (zpracování informace) – obraz, zvuk

- např. *Net Meeting* – výměna informací mezi 2 účastníky p obraz, zvuk, obrázky (white board), textová informace

požadavky na přenosové kapacity:

- zvuk v kvalitě audio CD, stereo 44,1 KHz $\rightarrow$ 1,411 Mb/s
- obraz 768x576 b, 25 frames, 24 b/na 1 bod $\rightarrow$ 33 MB/s

komprese dat:

- ***Motion Picture Expert Group***
- MPEG1 – 352x288 b, 25 frames $\rightarrow$ 1,5 Mb/s
- MPEG 2 – 768x576 b, 25 frames $\rightarrow$ 2-10 Mb/s (komprese 1:30 - 1:200)
- MPEG 4 – 176x144 b, 10 frames $\rightarrow$ 64 kb/s

infrastruktura:

- pro přenos multimediálních dat je nutná kvalitní infrastruktura
- přenos obrazové a zvukové informace se realizuje pomocí tzv. **skupinového adresování** $\rightarrow$ skupina počítačů má stejnou skupinovou adresu dochází tak k přenosu 1:N

- využívání tzv. **MBONE** – páteřních sítí pro přenos skupinových dat (dat na skupinové adresy)
- realizováno nad sítí Internet
- nutná celá řada směrovačů $\rightarrow$ nutnost tedy dovybavit síť prostředky pro skupinové směrování
- výhodou je možnost využití již stávající infrastruktury
- nutností je také zajistit synchronní přenos dat $\rightarrow$ vysílací rychlost musí být stejná jako rychlost přijímací (např. řešeno pomocí načítání do „bufferů“)
- přijatelné je pouze zpoždění

Úkol 4.5 (krátký úkol)

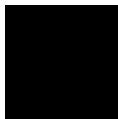
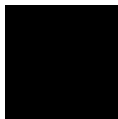
Jaký port využívá FTP protokol?

Shrnutí kapitoly

- Koncoví uživatelé využívají počítačové sítě prostřednictvím nejrůznějších síťových aplikací (softwarových serverů) - systémů elektronické pošty, přenosů souborů, vzdáleného přihlašování (remote login) a podobně.
- Aplikační vrstva tedy zajišťuje jednotlivé služby, specifické pro určité konkrétní aplikace nebo jejich skupiny. Obsahuje služby zvenku viditelné uživatelem (elektronická pošta, vzdálený terminálový přístup, přenos a vzdálené sdílení souborů).
- Diskový server (disc server) umožňuje uživatelům sdílet rozsáhlý disk, rozdělený na několik tzv. virtuálních disků, s nimiž pracují uživatelé (resp. jejich software) shodně jako s disky svých pracovních stanic (tzn. na fyzické úrovni).
- Souborový server (file server) rovněž umožňuje sdílet uživatelům vysokokapacitní disk, avšak nikoli na fyzické úrovni, nýbrž na úrovni logické.
- Tiskový server (print server) umožňuje uživatelům počítačové sítě provádět tisky sestav na tiskárnách k tomuto serveru připojených.
- Poštovní server slouží k přenosu zpráv v datovém režimu.
- Databázový server (database server) umožňuje uživatelům sdílet data ve společné databázi a poskytuje jim možnost přístupu k ní. Dále zabezpečuje udržení integrity sdílené databáze.
- WWW server je počítač, který je spravován správcem systému nebo poskytovatelem služeb sítě Internet (ISP) a který reaguje na požadavky prohlížeče uživatele.

Kontrolní otázky

- 1) Charakterizujte aplikační vrstvu a uveďte její služby. (odpověď naleznete [zde](#))



- 2) Klasifikujte služby aplikační vrstvy podle vhodných kritérií. (odpověď naleznete [zde](#))
- 3) Vyjmenujte typy serverů aplikační vrstvy. (odpověď naleznete [zde](#))
- 4) Popište diskový a souborový server. (odpověď naleznete [zde](#))
- 5) Popište tiskový a poštovní server. (odpověď naleznete [zde](#))
- 6) Popište List server a News server. (odpověď naleznete [zde](#))
- 7) Popište časový a databázový server. (odpověď naleznete [zde](#))
- 8) Popište www server. (odpověď naleznete [zde](#))
- 9) Charakterizujte služby aplikační vrstvy. (odpověď naleznete [zde](#))

Pojmy k zapamatování

Aplikační vrstva, služby aplikační vrstvy, diskový server, souborový server, tiskový server, poštovní server, List server, News server, časový server, databázový server, www server, TELNET, FTP, FINGER, NETFIND, WHOIS, videokonference.

Studijní literatura

Základní:

KLEMENT, M. *Výpočetní technika - software a hardware*. 1. vyd. Olomouc: Vydavatelství UP Olomouc, 2002. 178 s. ISBN 80-244-4012-6.

Rozšířená (pro hlubší pochopení):

HORÁK, J. *Hardware*. 2. vyd. Brno: Computer Press, 1998, 331 s. ISBN 80-7226-122-3.

Průvodce studiem

Víme, že jste studiu věnovali hodně úsilí a trpělivosti. Odměnou Vám však může být to, že jste si odnášíte mnoho poznatků a dovedností, které jistě využijete ve svém osobním a pracovním životě.

Budu se na Vás těšit při studiu další disciplíny tohoto modulu.

