

Předložená disciplína Vás tedy postupně seznámí s problematikou služeb DNS a DHCP, včetně jejich uplatnění v počítačových sítích. Rozsah témat je voleb 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:

- vysvětlit pojem DNS a orientovat se v problematice domén a subdomén,
- charakterizovat funkci protokolu DHCP,
- popsat jednotlivé síťové prvky a objasnit jejich účel.

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 ❶, ❷ 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	Služba DNS (Domain Name System) - Teoretický základ kapitoly (domény a subdomény, syntaxe jména, reverzní domény, doména 0.0.127.in-addr.arpa, zóna, doména a autonomní systém, rezervované domény a pseudodomény, dotazy (překlady)) - Úkol 1 – analýza pojmu DNS - Úkol 2 – orientace v problematice domén a subdomén - Úkol 3 – vysvětlení významu klienta revolver - Shrnutí kapitoly a kontrolní otázky a úkoly
Kapitola 2	Služba DHCP (Dynamic Host Configuration Protocol) - Teoretický základ kapitoly (funkce DHCP, výhody protokolu DHCP, autokonfigurace protokolu IP, proces zápůjčky DHCP, stavy klienta DHCP v procesu zápůjčky)

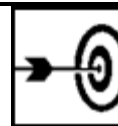
	- Úkol 1 – vysvětlení pojmu protokol DHCP - Úkol 2 – charakterizování funkce protokolu DHCP - Úkol 3 – popis stavů klienta DHCP v procesu zápůjčky - Shrnutí kapitoly a kontrolní otázky a úkoly
Kapitola 3	Aktivní a pasivní síťové prvky - Teoretický základ lekce (typy aktivních prvků, typy pasivních prvků) - Úkol 1 – rozčlenění síťových prvků - Úkol 2 – popis jednotlivých aktivních a pasivních síťových prvků - Úkol 3 – objasnění účelu jednotlivých síťových prvků - Shrnutí kapitoly a kontrolní otázky a úkoly

1 Služba DNS (Domain Name System)

Cíle

Po prostudování této kapitoly byste měli být schopni:

- vysvětlit pojem DNS,
- orientovat se v problematice domén a subdomén,
- vysvětlit význam klienta resolver.



Průvodce studiem

Víte co je to mnemotechnická pomůcka? Tak se říká každému slovnímu prostředku (může jich být i několik), který nějakým výstižným způsobem zastupuje to, co si máme ve skutečnosti zapamatovat. Jistě jste této techniky využívali např. při učení vyjmenovaných slov.

Proč o tom hovoříme? A proč zrovna v souvislosti s DNS? Odpověď je jednoduchá. Již jsme v předchozích kapitolách hovořili nesčetněkrát o IP-adresách. Je to způsobeno tím, že všechny aplikace, které zajišťují komunikaci mezi počítači, používají k identifikaci komunikujících uzlů IP-adresu. Zde ovšem musíme brát ohled na uživatele.

Jen stěží by jste si uživatelé byli schopni zapamatovat všechny potřebné IP-adresy v číselném tvaru (např. 194.149.104.203). Daleko výhodnější je pamatovat si jméno uzlu na který se chci připojit (např. info.pvt.net). A právě o tom, jak to všechno funguje, bude řeč v následující kapitole.

Vstupní znalosti:

- v této kapitole budeme navazovat na problematiku IP adres, proto je dobré, aby jste ji ovládali.

Potřebný čas pro studium kapitoly:

- 60 minut



1.1 Obecně o DNS

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



DNS (Domain Name System)

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

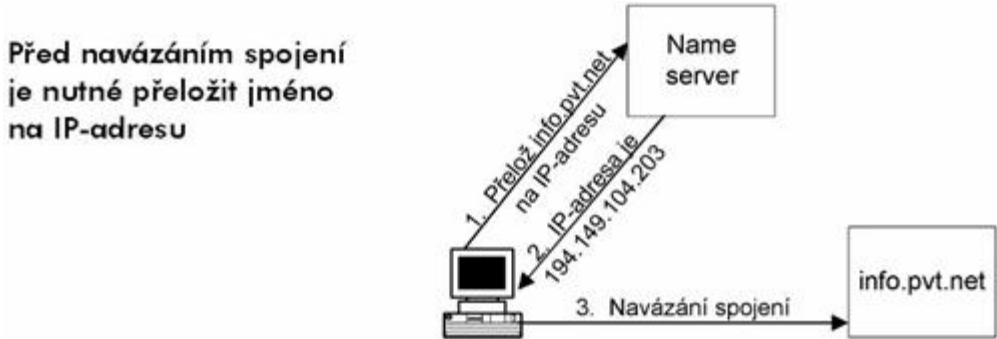
Příklad:

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

`telnet info.pvt.net.`

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

```
telnet 194.149.104.203
```



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

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

1.2 Domény a subdomény



Domény a subdomény

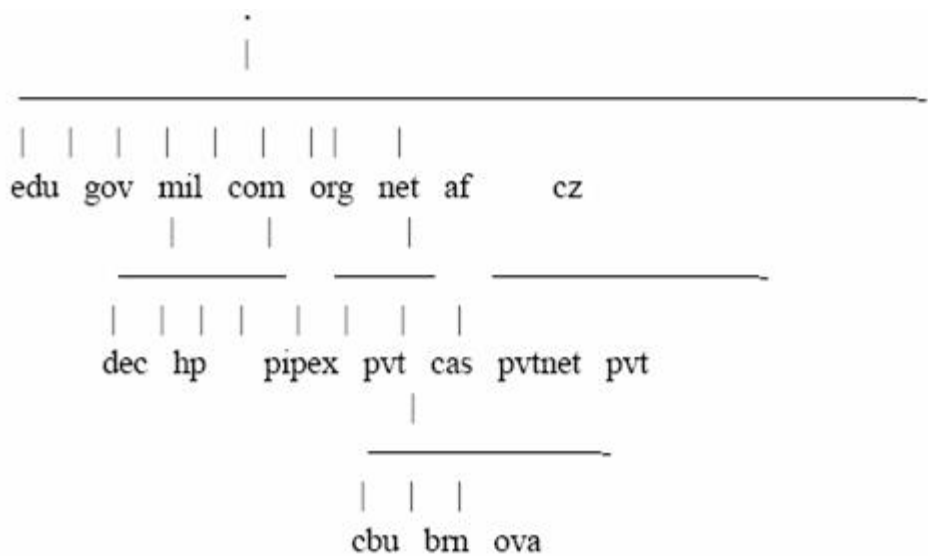
Celý Internet je rozdělen do tzv. domén, tj. skupin jmen, která k sobě logicky patří. Domény specifikují, patří-li jména jedné firmě, jedné zemi apod. V rámci domény je možné vytvářet podskupiny, tzv. subdomény, např. doméně firmy lze vytvořit subdomény pro oddělení.

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

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

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

Jména tvoří stromovou strukturu:



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

Úkol 1.2 (krátký úkol)

Pro Českou republiku je vyhrazena doména?



1.3 Syntaxe jména domény

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

řetězec.řetězec.řetězec....řetězec.



Syntaxe jména

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

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

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

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

Je možné vynechat:

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

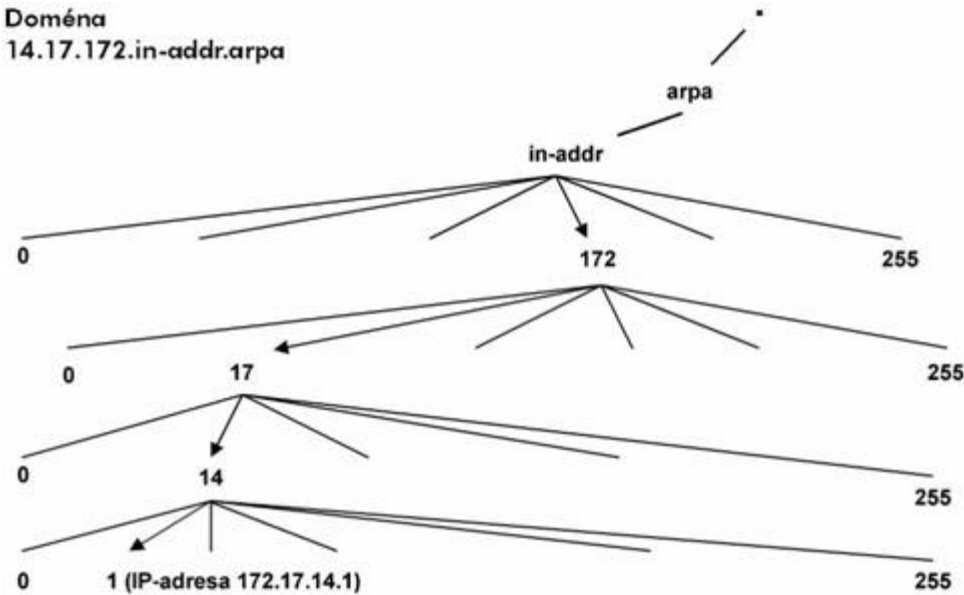
Úkol 1.3 (krátký úkol)

Jaký je maximální počet znaků v názvu domény?

1.4 Reverzní domény

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

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



Pod doménou in-addr.arpa jsou domény jmenující se jako první číslo z IP-adresy sítě.

Např. síť 194.149.101.0 patří do domény 194.in-addr.arpa. Síť 172.17 patří do domény 172.in-addr.arpa. Dále doména 172.in-addr.arpa se dělí na subdomény, takže síť 172.17 tvoří subdoménu 17.172.in-addr.arpa. Je-li síť 172.17 rozdělena pomocí síťové masky na subsítě, pak každá subsíť tvoří ještě vlastní subdoménu.

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

Příklad:

Reverzní doména pro subsíť 194.149.150.16/28 je 16.150.149.194.in-



Reverzní domény

addr.arpa

Pasáž pro zájemce

Doména 0.0.127.in-addr.arpa

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

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

Úkol 1.4 (krátký úkol)

Pro účely reverzního překladu byla definována pseudodoména s názvem?

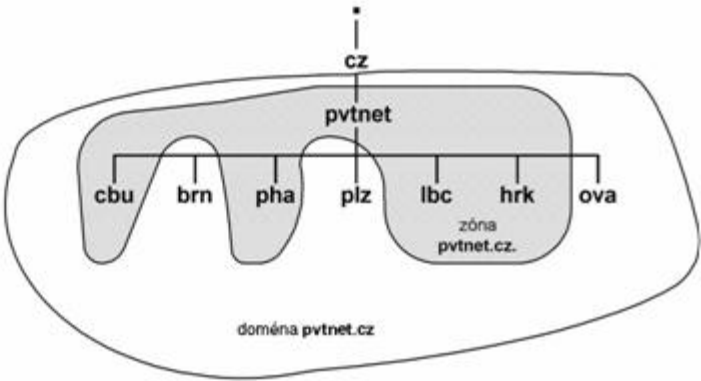
1.5 Zóny

Často se setkáváme s otázkou: „Co je to zóna?“ „Jaký je vztah mezi doménou a zónou?“.

Jak jsme již uvedli, **doména je skupina počítačů, které mají společnou pravou část svého doménového jména**. Doména je např. skupina počítačů, jejichž jméno končí *cz*. Doména *cz* je však velká. Dělí se dále na subdomény např. *pvt.cz*, *eunet.cz* a tisíce dalších. Každou z domén druhé úrovně si většinou spravuje na svých name serverech majitel domény nebo jeho poskytovatel Internetu.

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

Zóna pvtnet.cz



Úkol 1.5 (krátký úkol)

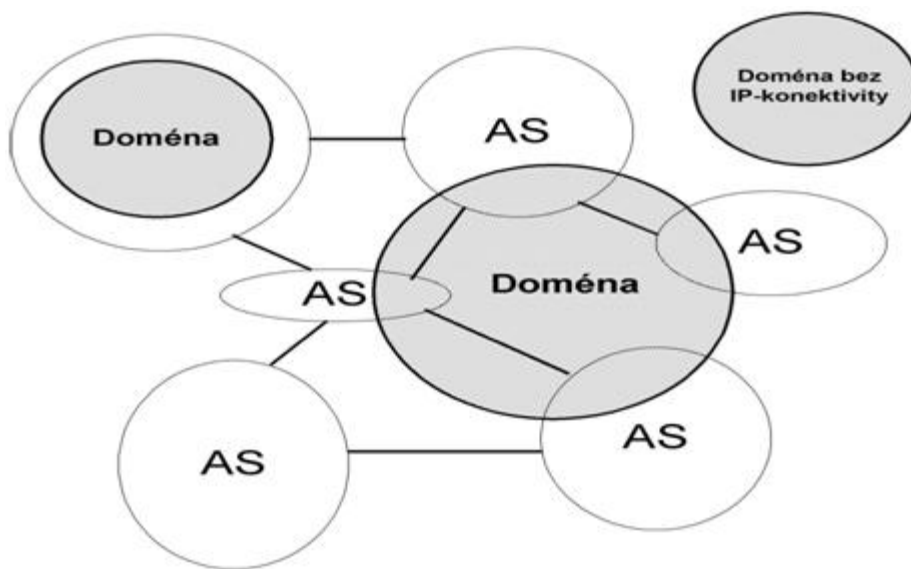
Data o doméně uložená na name serveru jsou nazývána jako?

1.6 Domény a autonomní systémy

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



*Doména
a autonomní
systém*



Autonomní systémy dělí Internet z hlediska IP-adres (směrování), naproti tomu domény dělí Internet z hlediska jmen počítačů.

1.7 Rezervované domény a pseudodomény

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

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

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

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

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



1.8 Dotazy a jejich překlady



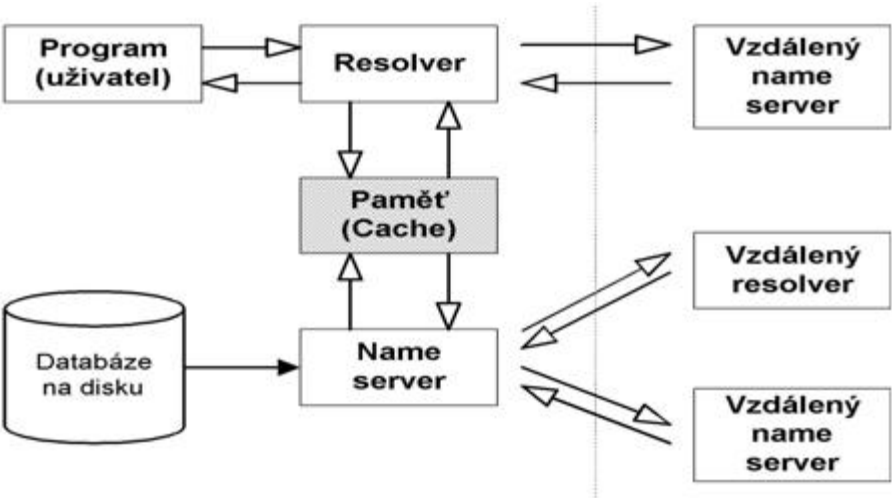
Dotazy
(překlady)

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

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

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

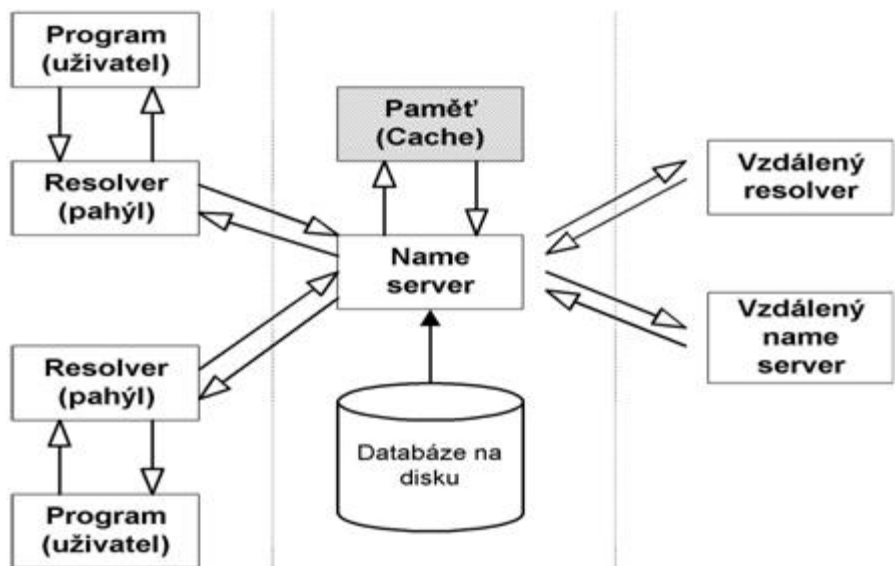
Name server i resolver společně sdílejí paměť cache. Během práce do ní ukládají kladné odpovědi na dotazy, které provedly jiné name servery, tj. ke kterým jsou jiné name servery authority. Ale z hlediska našeho name serveru jsou tato data opět neautoritativní – pouze šetří čas při opětovných dotazech.



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

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

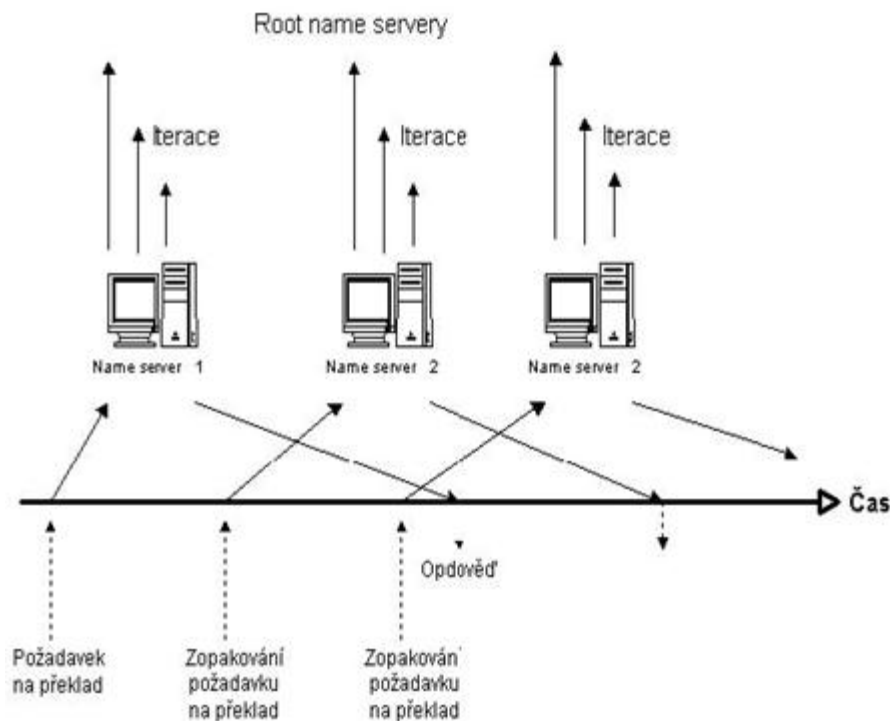
Resolver předává všechny dotazy na lokální name server. Od name serveru pak očekává konečnou (rekurzivní) odpověď. Name server buď odpoví přímo, nebo sám kontaktuje další name servery, tj. name server rekurzivně řeší dotaz a klientovi zašle až výsledek.



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

Dotazy, kterými se přenášejí data o zóně (*zone transfer*) např. mezi primárním a sekundárním name serverem, se přenáší protokolem TCP. Běžné dotazy (např. překlad jména na IP-adresu a naopak) se provádí pomocí datagramů protokolu UDP.

V Internetu platí pravidlo, že databáze s daty nutnými pro překlad jsou vždy uloženy alespoň na dvou nezávislých počítačích (nezávislých name serverech). Je-li jeden nedostupný, pak se překlad může provést na druhém počítači.



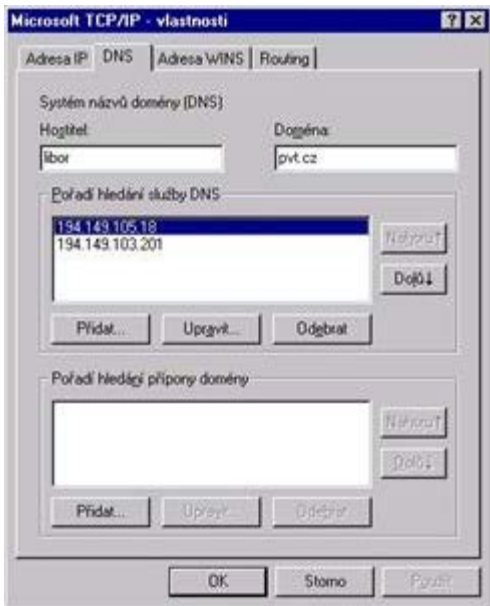
1.8.1 Resolver

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

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

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

Name server



1.8.2 Name server

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

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

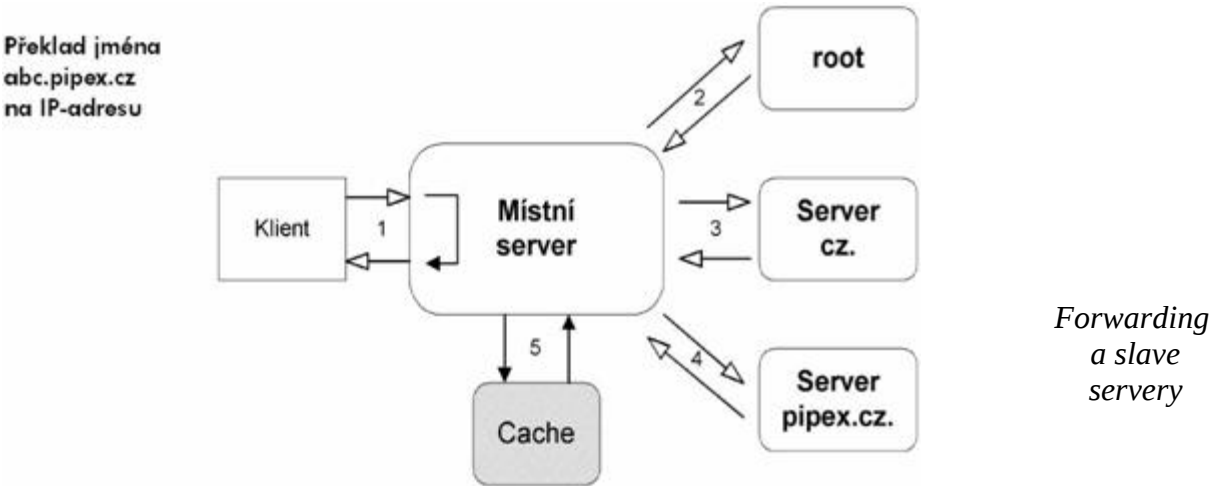
Podle uložení dat rozlišujeme následující typy name serverů:

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

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

provést překlad, pak kontaktuje autoritativní server pro danou zónu.

Autoritativní data pocházejí z databází na disku. Je zde pouze jedna výjimka. Pro správnou činnost name serveru musí name server znát root name servery. Pro ty však není autoritou, přesto každý name server má na disku databázi informací o root serverech, kterou ale zavádí příkazem cache do sekundární paměti (není k nim autorita).



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

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

1.8.3 Forwarding a slave servery

Ještě existují dva typy serverů: forwarding a slave servery. Tato vlastnost serveru nesouvisí s tím, zda jsou primárními nebo sekundárními servery pro nějakou zónu, ale souvisí se způsobem jejich překladu.

Je-li podniková síť připojena k Internetu pomalou linkou, pak místní name server zatěžuje linku svými překlady. V takovém případě je výhodné si name server konfigurovat jako **forwarding server** (viz obr). Forwarding server vezme požadavek od klienta a předá jej forwarderovi na rychlé síti jako rekurzivní dotaz. Forwarder je server v Internetu, který je připojen rychlejšími linkami. Dotaz rekurzivně vyřeší a pošle mému forwarding serveru konečný výsledek.

Nemá-li forwarding server kontaktovat root name servery, ale pouze čekat na odpověď od forwardera, pak je nutné označit takový server navíc jako **slave server**. Slave servery se používají v uzavřených podnikových sítích (za firewalllem), kde není možný kontakt s root name servery. Slave server pak kontaktuje forwardera, který je součástí firewallu.



Úkol 1.8 (krátký úkol)

Přeložení jména na IP-adresu zprostředkovává tzv.?

Shrnutí kapitoly

- Všechny aplikace, které zajišťují komunikaci mezi počítači, používají k identifikaci komunikujících uzlů IP-adresu. Pro člověka jako uživatele jsou však IP-adresy těžko zapamatovatelné. Proto se používá místo IP-adresy název síťového rozhraní. Pro každou IP-adresu máme zavedeno jméno síťového rozhraní (počítače), přesněji řečeno doménové jméno.
- Jedna IP-adresa může mít přiřazeno i několik doménových jmen.
- Vazba mezi jménem počítače a IP adresou je definována v DNS databázi. DNS (*Domain Name System*) je celosvětově distribuovaná databáze. Jednotlivé části této databáze jsou umístěny na tzv. name serverech.
- Celý Internet je rozdělen do tzv. domén, tj. skupin jmen, která k sobě logicky patří. Domény specifikují, patří-li jména jedné firmě, jedné zemi apod.
- V rámci domény je možné vytvářet podskupiny, tzv. subdomény, např. doméně firmy lze vytvořit subdomény pro oddělení.
- Doménové jméno se skládá z řetězců vzájemně oddělených tečkou. Jméno se zkoumá zprava doleva. Nejvyšší instancí je tzv. root doména, která se vyjadřuje tečkou zcela vpravo (tato tečka bývá často vypouštěna). Celé jméno může mít maximálně 255 znaků, řetězec pak maximálně 63 znaky.
- Některé aplikace potřebují k IP-adrese nalézt jméno, tj. nalézt tzv. reverzní záznam. Jedná se tedy o překlad IP-adresy na doménové jméno. Tento překlad se často nazývá zpětným (reverzním) překladem.
- Přeložení jména na IP-adresu zprostředkovává tzv. resolver. Resolver je klient, který se dotazuje name serveru.

Kontrolní otázky

- 1) Vysvětlíte pojem DNS. (odpověď naleznete [zde](#))
- 2) Objasněte problematiku domén a subdomén v Internetu. (odpověď naleznete [zde](#))
- 3) Popište princip překladu IP-adresy na doménové jméno. (odpověď naleznete [zde](#))

- 4) Vysvětlíte, k jakému účelu slouží klient resolver. (odpověď naleznete [zde](#))
- 5) Objasněte význam name Serveru. (odpověď naleznete [zde](#))
- 6) Analyzujte možnosti využití forwarding a slave serverů. (odpověď naleznete [zde](#))

Pojmy k zapamatování

DNS, doména, subdoména, syntaxe jména, reverzní doména, zóna, pseudodoména, resolver, name server, forwarding, slave server.

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

Můžeme Vám opět blahopřát!!!. Znovu jste postoupili po pomyslném žebříčku odborníků přes počítačové sítě na další příčku. Počítačové sítě nejsou vůbec jednoduchou záležitostí.

Proto, budete-li chtít v budoucnu v této oblasti pracovat na špičkové úrovni, nevyhnete se studiu další literatury. Již nyní, chcete-li si prohloubit Vaše poznání, neváhejte a navštivte knihkupectví s odbornou počítačovou literaturou, či zapátrejte v knihovnách.



2 Služba DHCP (Dynamic Host Configuration Protocol)

Cíle

Po prostudování této kapitoly byste měli být schopni:

- vysvětlit pojem protokol DHCP,
- charakterizovat funkci protokolu DHCP,
- popsat stavy klienta DHCP v procesu zápůjčky.



Průvodce studiem

Stejně jako u předešlé kapitoly i v této půjde především o teorii. Kapitola opět není nejkratší, ale obsahuje celou řadu nezbytných informací.

Budeme se v ní zabývat protokolem DHCP (z angl. Dynamic Host Configuration Protocol). Již nyní Vám prozradíme pár maličkostí:

Jedná se o z působ dynamického (tj. okamžitého) přiřazování adres IP počítačům v lokální síti. Spočívá v tom, že jakmile se uživatel připojí do této sítě, je mu okamžitě přiřazena adresa IP – tato však není vytvořena libovolně, ale je vybrána ze seznamu.

Vstupní znalosti:

- v této kapitole budeme navazovat na problematiku IP adres, proto je dobré, aby jste ji ovládali,

Potřebný čas pro studium kapitoly:

- 60 minut



2.1 Obecně o službě DHCP

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

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



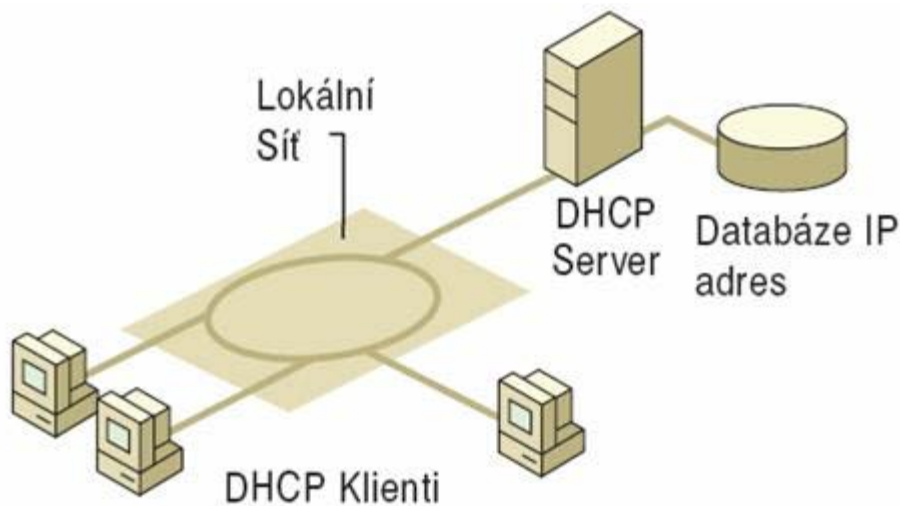
DHCP

2.2 Funkce služby DHCP

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



Funkce DHCP



Základní model protokolu DHCP

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

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

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

Klient podporující službu DHCP při přijetí nabídky zápůjčky obdrží:

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

Úkol 2.2 (krátký úkol)

Protokol DHCP je založen na síťovém modelu?



2.3 Výhody použití služby DHCP

Instalací protokolu DHCP na svou rozlehlou síť získáte následující výhody:

- Bezpečnou a spolehlivou konfiguraci. Protokol DHCP minimalizuje chyby v konfiguraci způsobené manuální konfigurací adres IP, například chyby v psaní, stejně jako minimalizuje konflikty adres



*Výhody
protokolu
DHCP*

způsobené přiřazením již aktuálně používané adresy IP dalšímu počítači.

- Sníženou správu sítě.
- Konfigurace protokolu TCP/IP je centralizovaná a automatizovaná.
- Správci sítě mohou centrálně definovat konfigurace protokolu TCP/IP jak obecně, tak pro konkrétní podsít'.
- Klientům lze automaticky přiřazovat plný rozsah dalších konfiguračních hodnot protokolu TCP/IP pomocí možností DHCP.
- Změny adres pro konfigurace klienta, které musí být často aktualizovány, například klienti se vzdáleným přístupem, kteří se neustále pohybují, lze provádět efektivně a automaticky při spuštění klienta ze svého nového umístění.
- Většina směrovačů může předat požadavky na konfiguraci pomocí služby DHCP, čímž se omezují požadavky na nastavení serveru DHCP na každé podsíti, pokud k tomu není důvod.

2.4 Automatická konfigurace protokolu IP



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

Při autokonfiguraci klienta DHCP probíhá následující proces:

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

Jestliže již dříve klient DHCP obdržel zápůjčku serveru DHCP:

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

- Jestliže je provedení příkazu ping neúspěšné, klient DHCP předpokládá, že byl přesunut na síť, kde nejsou služby DHCP dostupné. Klient pak provede autokonfiguraci své adresy IP.

2.5 Proces zápůjčky IP adresy službou DHCP

Klient podporující službu DHCP obdrží od serveru DHCP zápůjčku na adresy IP. Před vypršením časového omezení zápůjčky musí server DHCP tuto zápůjčku klientovi obnovit nebo klient musí získat novou zápůjčku. Zápůjčky jsou v databázi serveru DHCP uchovávány přibližně jeden den po vypršení. Tato poskytnutá lhůta chrání zápůjčku klienta v případě, že klient a server jsou v různých časových pásmech, jejich interní hodiny nejsou synchronizovány nebo klient je v době vypršení zápůjčky mimo síť.

2.5.1 Zprávy DHCP

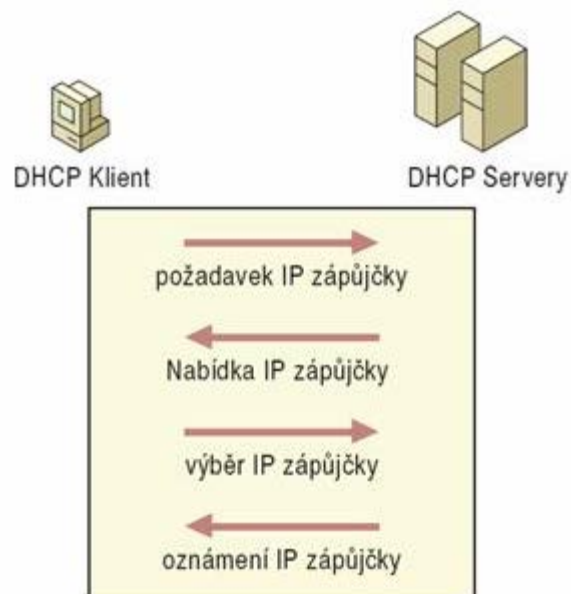
Tabulka popisuje zprávy DHCP vyměňované mezi klientem a serverem.

Typ zprávy	Popis
DHCPDiscover	Požadavek na přidělení IP adresy s DHCP serveru. Jelikož se jedná o první přihlášení (klient ještě nemá IP adresu) je zdrojová adresa IP paketu 0.0.0.0.
DHCPOffer	Pokud server obdrží paket DHCPDiscover odpoví paketem DHCPOffer obsahující nezapůjčenou IP adresu a další informace o nastavení protokolu TCP/IP.
DHCPRequest	Pokud klient obdrží paket DHCPOffer, odpoví serveru paketem DHCPRequest a tím potvrdí obdržení IP adresy.
DHCPAcknowledge (DHCPAck)	Tímto paketem potvrdí klientovi doručení paketu DHCPRequest a dodá i další informace nezbytné pro dokončení konfigurace TCP/IP protokolu.
DHCPNak	Pokud přidělaná IP adresa již není platná, nebo byla přidělena jinému klientovi, odpoví server paketem DHCPNak a proces zápůjčky započne znovu.
DHCPDecline	Jestliže klient zjistí, že nabízené parametry konfigurace TCP/IP protokolu jsou neplatné, pošle serveru paket DHCPDecline.
DHCPRelease	Klient zašle paket DHCPRelease serveru, aby uvolnil a zrušil jakoukoliv zápůjčku, která pro něj byla vytvořena.



Proces zápůjčky DHCP

Zprávy DHCP



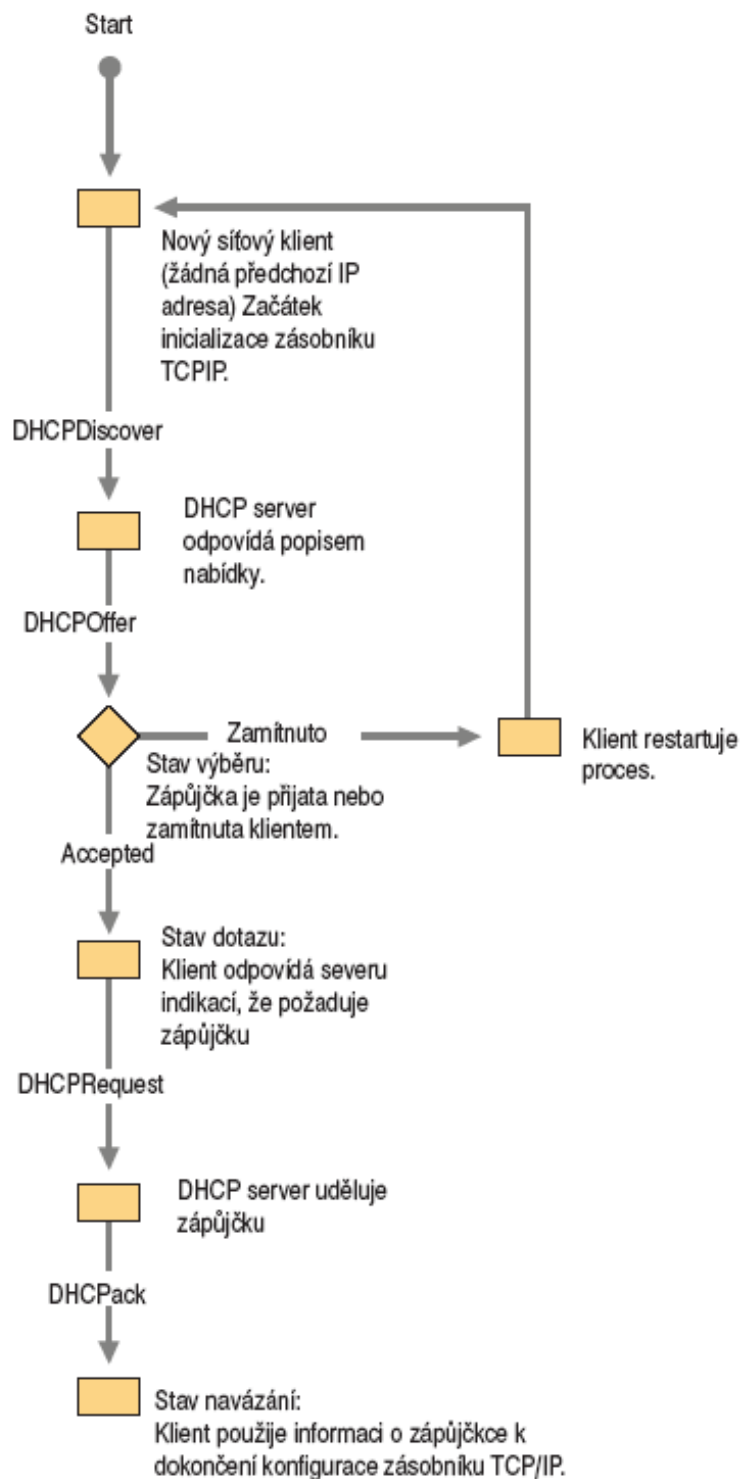
*Funkce procesu
zápůjčky*

2.5.2 Funkce procesu zápůjčky

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

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

*Stavy klienta
DHCP během
procesu
zápůjčky*



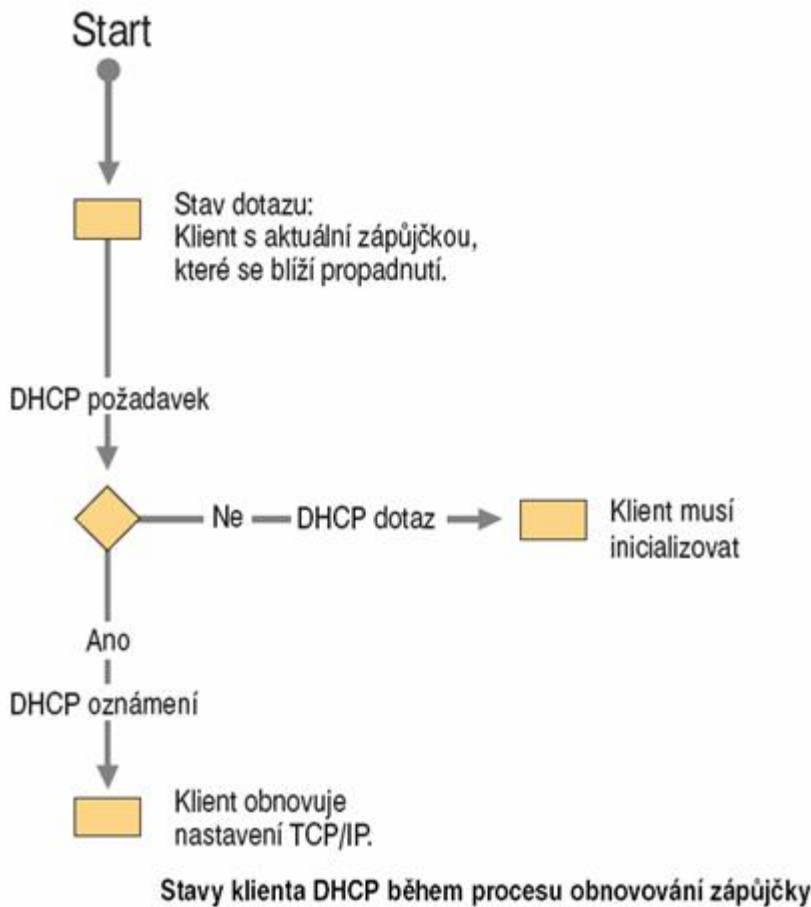
Stavy klienta DHCP během procesu zápůjčky

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

Stavy klienta
DHCP během
procesu
obnovování
zápůjčky

Ve vzácných případech může server DHCP vrátit klientovi negativní

potvrzení. To se může stát, jestliže klient žádá neplatnou nebo duplikovanou adresu. Jestliže klient obdrží negativní potvrzení (DHCPNak) musí klient začít celý proces zápůjčky znovu.



Úkol 2.5 (krátký úkol)

Požadavek na přidělení IP adresy z DHCP serveru je reprezentováno zprávou?



2.6 Stavy klienta služby DHCP v procesu zápůjčky

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

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



*Stavy klienta
DHCP
v procesu
zápůjčky*

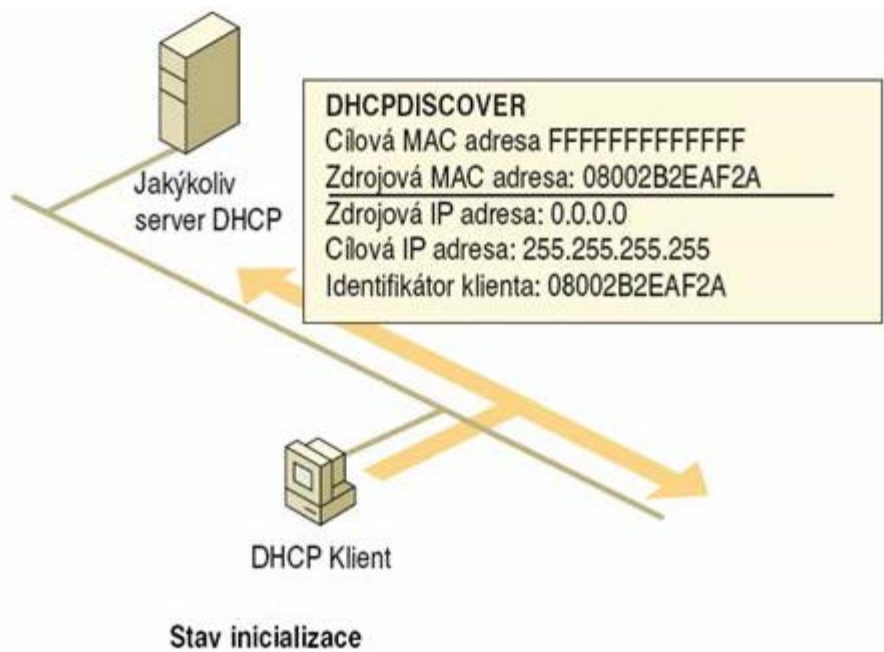
2.6.1 Inicializace

Tento stav nastane při první inicializaci zásobníku protokolu TCP/IP na počítači klienta DHCP. Klient ještě nemá od serveru DHCP vyžádanou adresu IP. Tento stav také nastane, pokud je klientovi odepřena adresa IP,

Inicializace

kteou požaduje, nebo pokud adresa IP, kteou původně měl, byla uvolněna. Stav inicializace je znázorněn na obrázku.

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



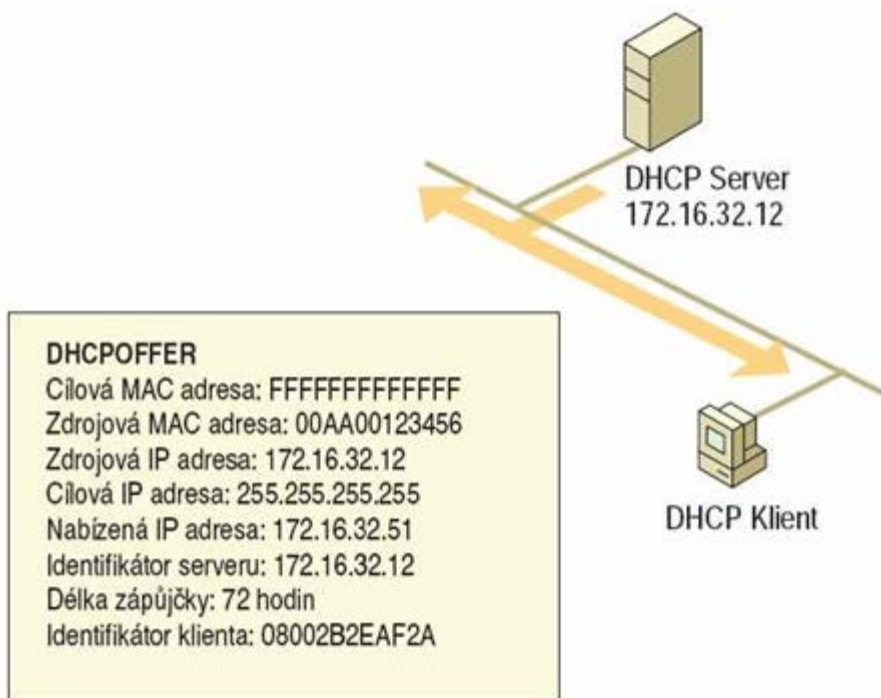
Výběr

2.6.2 Výběr

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

Server DHCP rezervuje adresu IP, aby nebyla nabízena jinému klientovi DHCP:

Zpráva DHCPOffer obsahuje adresu IP a odpovídající masku podsítě, identifikátor serveru DHCP (adresu IP nabízejícího serveru DHCP) a dobu trvání zápůjčky. Stav výběru je znázorněn na obrázku.



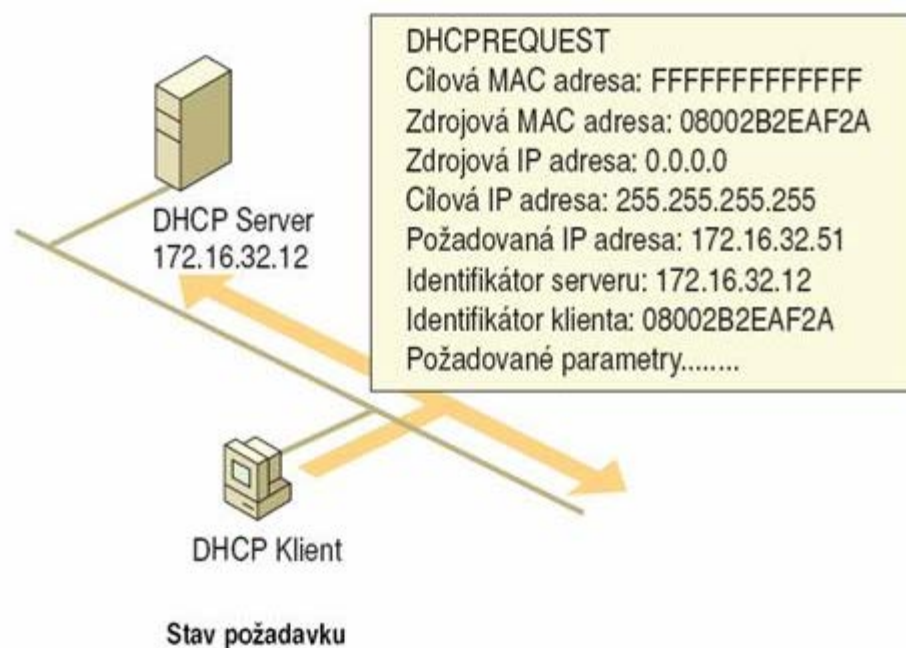
Stav výběru

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

Požadavek

2.6.3 Požadavek

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

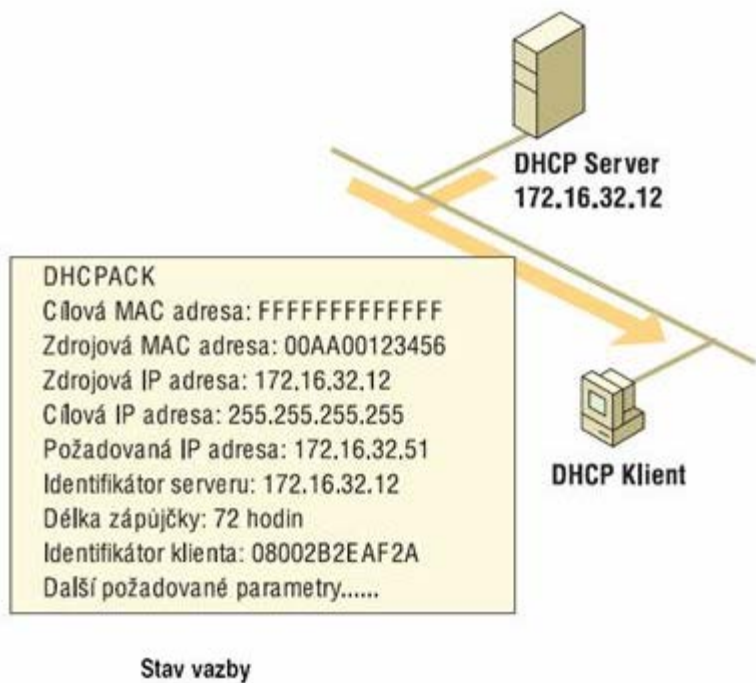


Jestliže byla adresa IP klienta známa (tzn. že počítač byl restartován a snaží se zapůjčit si původní adresu), všesměrové vysílání sledují všechny servery DHCP. Server DHCP, který může zapůjčit požadovanou adresu IP, odpoví buď úspěšným potvrzením (DHCPAck) nebo neúspěšným potvrzením (DHCPNak). Zpráva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

Vazba

2.6.4 Vazba

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



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

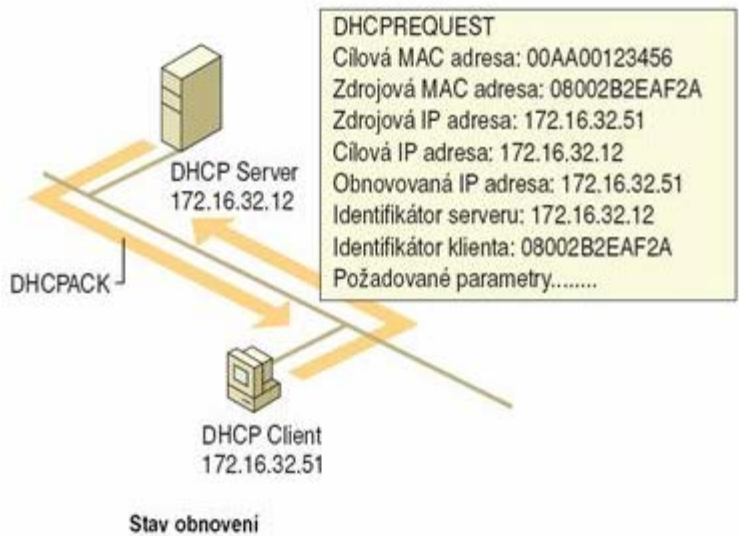
Obnovení

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

2.6.5 Obnovení

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

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



Obnovení vazeb

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

2.6.6 Obnovení vazeb

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



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

Úkol 2.6 (krátký úkol)

Server DHCP reaguje na zprávu DHCPRequest prostřednictvím zprávy?

Shrnutí kapitoly

- Protokol DHCP zjednodušuje správu konfigurace adresy IP pomocí automatického konfigurování adres pro síťové klienty.
- Server DHCP automaticky přiřazuje adresy IP a podobná nastavení konfigurace protokolu TCP/IP počítačů na síti podporujících protokol DHCP.
- Každé zařízení na síti založené na protokolu TCP/IP musí mít jedinečnou adresu IP, aby bylo schopno přistupovat k síti a jejím prostředkům. Bez protokolu DHCP je nutno provést nakonfigurování protokolu IP ručně u nových počítačů, počítačů přesunovaných z jedné podsítě na jinou a počítače odebírané ze sítě.
- Správce sítě zakládá jeden nebo více serverů DHCP, které udržují informace o konfiguraci protokolu TCP/IP a poskytují konfiguraci adres klientům podporujícím službu DHCP ve formě nabídky zápůjčky.
- Klient podporující službu DHCP obdrží od serveru DHCP zápůjčku na adresy IP. Před vypršením časového omezení zápůjčky musí server DHCP tuto zápůjčku klientovi obnovit nebo klient musí získat novou zápůjčku.
- Cyklus klienta DHCP přes šest různých stavů klienta během procesu zápůjčky DHCP. Když je klient DHCP a server DHCP na stejné podsíti, zprávy DHCPDiscover, DHCPOffer, DHCPRequest a DHCPACK jsou posílány přes všesměrové vysílání na úrovni MAC a IP.
- Aby klienti DHCP mohli komunikovat se serverem DHCP na vzdálené síti, musí připojující směrovač nebo směrovače podporovat předávání zpráv DHCP mezi klientem DHCP a serverem DHCP za použití služby BOOTP/DHCP Relay Agent.

Kontrolní otázky

- 1) Vysvětlíte pojem DHCP. (odpověď naleznete [zde](#))
- 2) Objasněte funkci protokolu DHCP. (odpověď naleznete [zde](#))
- 3) Proveďte rozbor výhod protokolu DHCP. (odpověď naleznete [zde](#))
- 4) Popište proces autokonfigurace protokolu DHCP. (odpověď naleznete [zde](#))
- 5) Vysvětlíte proces zápůjčky DHCP. (odpověď naleznete [zde](#))
- 6) Analyzujte stavy klienta DHCP v procesu zápůjčky. (odpověď naleznete [zde](#))

Pojmy k zapamatování

DHCP, zápůjčka, DHCPDiscover, DHCPOffer, DHCPRequest, DHCPACKnowledge, DHCPNak, DHCPDecline, DHCPRelease.

Studijní literatura

Základní:

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

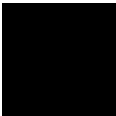
Rozšířená (pro hlubší pochopení):

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



Průvodce studiem

Pokud jste dokázali správně odpovědět na všechny kontrolní otázky, tak si nyní udělejte delší přestávku na odpočinek. Po ní se společně podíváme na poslední kapitolu této disciplíny, která je teoretičtějšího charakteru.



3 Aktivní a pasivní síťové prvky

Cíle

Po prostudování této kapitoly byste měli být schopni:

- uvést aktivní a pasivní síťové prvky,
- popsat jednotlivé aktivní síťové prvky,
- popsat jednotlivé pasivní síťové prvky,
- objasnit účel jednotlivých síťových prvků.



Průvodce studiem

Jakou funkci plní protokol DHCP? Nebojte, nyní Vás nezkoušíme, jelikož jsme přesvědčeni, že vše perfektně ovládáte. Zeptáme se Vás až u zkoušky.

V této poslední kapitole se společně podíváme na síťové prvky. Hned na začátku uvedeme jejich výčet včetně rozdělení a potom si jednotlivé síťové prvky podrobněji popíšeme.

Vstupní znalosti:

- ke studiu této kapitoly nepotřebujete žádné speciální znalosti.

Potřebný čas pro studium kapitoly:

- 90 minut



3.1 Obecně o síťových prvcích

Aktivní síťové prvky:

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



Síťové prvky

Pasivní síťové prvky:

- **fyzické propojení počítačů** (kabeláž - metalická, optická,

bezdrátové - infračervené, mikrovlnné, GSM, laser),

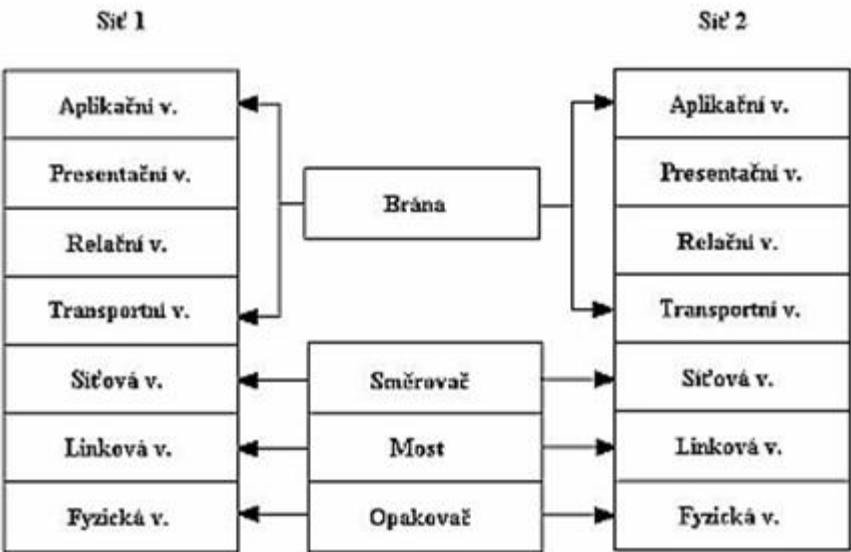
- **počítačové zásuvky**,
- **patch panely** (propojovací panely, ve kterých končí přípojky z počítačových zásuvek),
- **racky** (rozvodné skříně, v nichž jsou umístěny patch panely a některé aktivní prvky sítě),
- **propojovací kabely** (metalické, optické),

Základní rozdělení aktivních prvků:

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

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

Vztah aktivních síťových prvků k modelu OSI.



3.2 Typy a dělení aktivních síťových prvků

3.2.1 Opakovače (repeatery)

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



*Opakovače
(repeatery)*

menších částí.

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

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



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

3.2.2 Rozbočovače (huby)

*Rozbočovače
(huby)*

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

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



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

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

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

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

Mosty (bridge)

3.2.3 Mosty (bridge)

Mosty pracují na rozdíl od opakovačů na zcela jiném principu a jsou používány pro spojení dvou různých lokálních sítí, lišících se ve dvou nejnižších vrstvách OSI Modelu, tj. ve fyzické a linkové vrstvě. V případě lokálních sítí půjde o odlišnost až po tzv. MAC podvrstvu linkové vrstvy. Pro potřeby standardizace lokálních počítačových sítí je výhodné rozdělit linkovou vrstvu na dvě další podvrstvy:

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

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



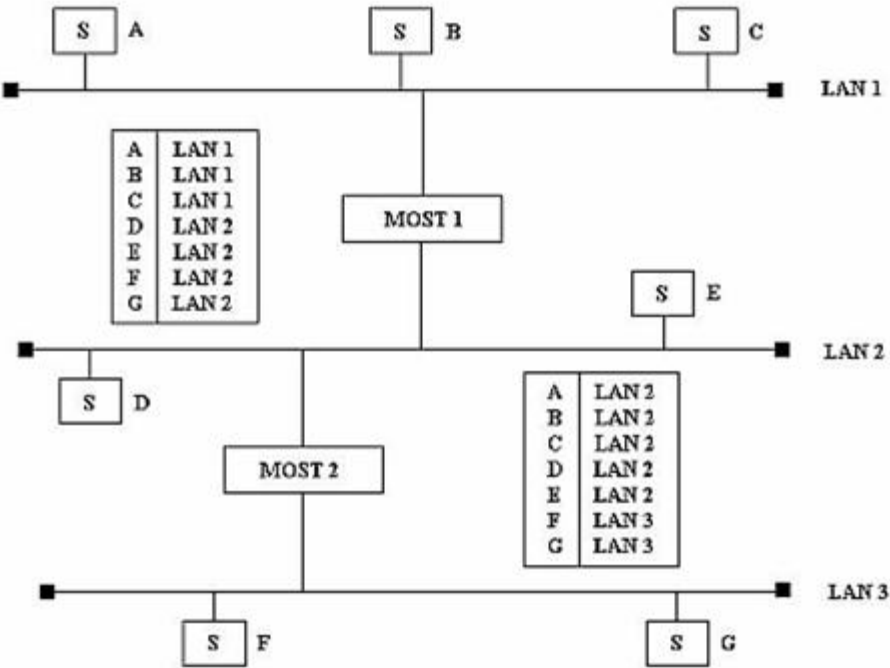
Mosty nejsou, na rozdíl od opakovačů, pro spojované sítě průhledné v tom smyslu, že přes mosty nepřejdou všechna data (rámce), která některá ze spojovaných sítí vyprodukuje. Projdou pouze ta data, která jsou určena stanicím nacházejícím se na "druhé straně mostu". To má jeden velice podstatný důsledek.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

V případě, že bychom na místě mostů použili opakovače, měli bychom

celý systém doslova přepíněný daty, protože i cestě lokální data, jejichž vysílající i cílová stanice leží na stejné "podsíti" (v případě Ethernetu na stejném segmentu), by díky průhlednosti opakovačů bloudila po celém systému.

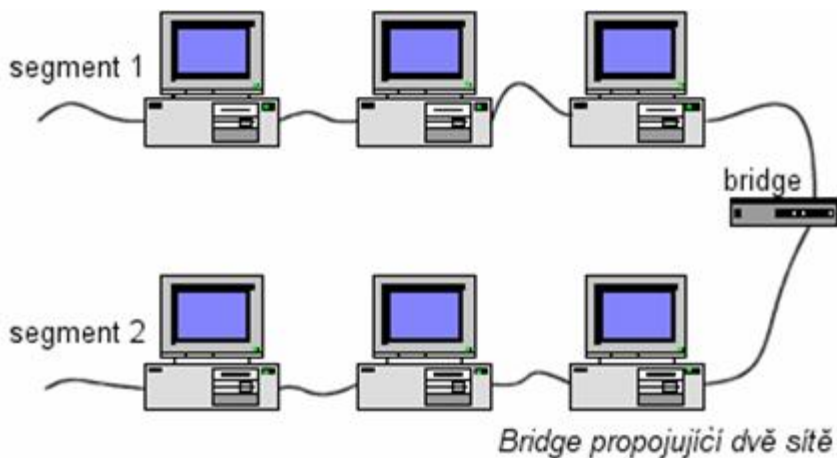
Mostem může být například normální osobní počítač, stejný jako v případě běžných síťových pracovních stanic, vybavený ale v tomto případě dvěma síťovými adaptéry (pro každou připojenou lokální síť jedna) a příslušném programovým vybavením. Most bude sledovat provoz na každé k němu připojené síti, ale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

Použití mostu vede ve svých důsledcích také ke zvýšení výkonnosti (celkové kapacity) a spolehlivosti systému. Oddělením provozu v jednotlivých částech sítě totiž snižuje nebezpečí "zahlcení" celého systému. To je zvlášť důležité zejména u sítí Ethernet, které jsou díky použité přístupové metodě (CSMA/CD) na přetížení sítě zvláště citlivé. Pokud jde o zvýšení spolehlivosti, zde působí to, že mosty jsou díky své funkci schopny oddělit od zbytku sítě ty její části, na nichž došlo k poruše. Mosty mohou sloužit také pro spojení lokálních sítí používajících odlišné typy síťových kabelů.



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

Směrovače
(routery)



3.2.4 Směrovače (routery)

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

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

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

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

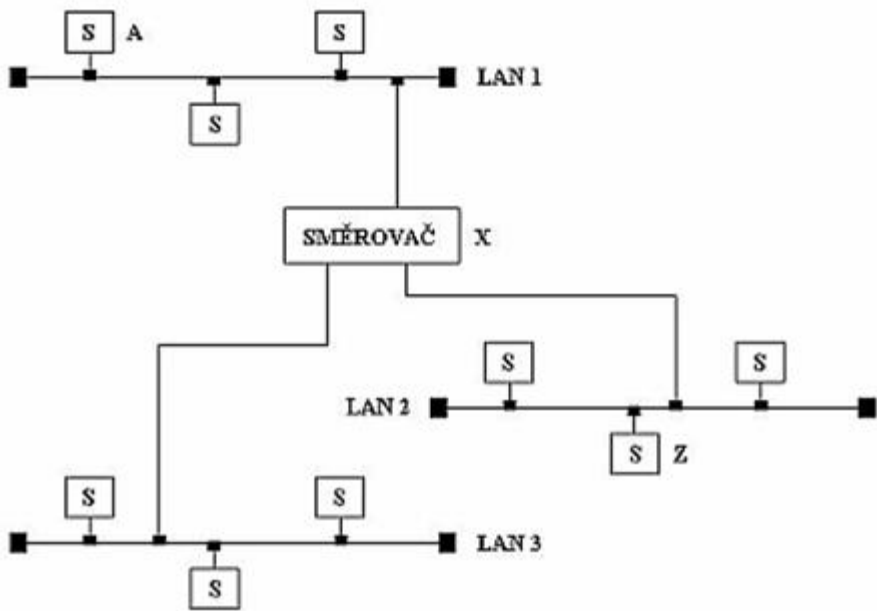


Kde symbol "X" představuje adresu směrovače v síti číslo 1 a symbol "Z" adresu cílové stanice. Symbol na prvním místě představuje "aktuální" adresu (tj. adresu MAC podvrstvy) v dané síti, kdežto symbol na druhém místě představuje konečnou cílovou adresu. Směrovač tento rámec přijme, zpracuje (až do úrovně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



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

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



Přepínače
(switche)

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

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

3.2.5 Přepínače (switche)

Ve výkladu pojmu přepínač (switch) je určitá nejednoznačnost.

Podle klasické definice pracují přepínače na linkové vrstvě, a to do značné míry podobným způsobem jako mosty. Při této definici je jediný

Brány

rozdílem mezi mostem a přepínačem to, že most pracuje jako zařízení pro ukládání a odesílání rámců, zatímco přepínač nikoli.

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

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

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

3.2.6 Brány (gateways)

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

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

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

Úkol 3.2 (krátký úkol)



Most (někdy zvaný brouter) rozděluje síť na dvě?

3.3 Typy a dělení pasivních síťových prvků



3.3.1 Patch panely

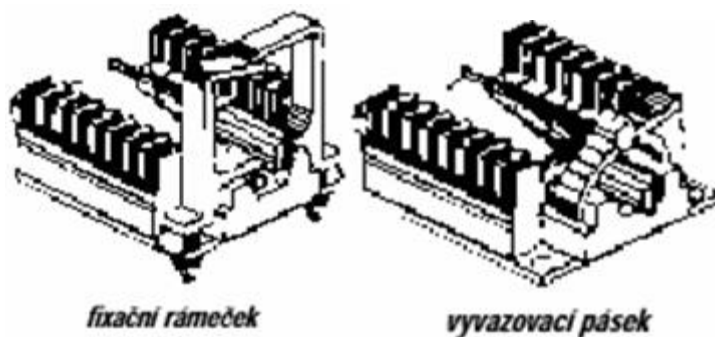
Používají se k ukončení horizontální nebo páteřní kabeláže a k uspořádání rozhraní do rozličných síťových zařízení. Jsou vesměs umístěny v rozvaděči. Zajišťují jednoduchý servis, administraci a údržbu.

Patch panely

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



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



Racky

3.3.2 Racky

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

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

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

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

Úkol 4.3 (krátký úkol)

Všechny patch panely mají standardně rozteč uchycování otvorů o velikosti?



Shrnutí kapitoly

- Mezi aktivní síťové prvky řadíme: síťový adaptér, HUB, bridže, switch, routek, repeater, transceiver, gateway.
- Mezi pasivní síťové prvky řadíme: fyzické propojení počítačů, počítačové zásuvky, patch panely, racky, propojovací kabely.
- Opakovač není ve své podstatě nic jiného, než obousměrný číslicový zesilovač. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, již jsme schopni lokální sítě obsáhnout.
- Hub je rozbočovací zařízení, které větví přenášený signál a tím umožňuje rozšiřování sítě o další pracovní stanice. Vše co mu přijde na jeho vstupy, ihned odesílá na všechny výstupy.
- Mosty pracují na rozdíl od opakovačů na zcela jiném principu a jsou používány pro spojení dvou různých lokálních sítí, lišících se ve dvou nejnižších vrstvách OSI Modelu, tj. ve fyzické a linkové vrstvě.
- Směrovače pracují na podobných principech jako mosty, pouze s tím rozdílem, že využívají informace ze třetí, tj. ze síťové vrstvy OSI Modelu, což je vrstva, která se stará o nalezení optimální cesty k cílové stanici.
- Dnešní přepínač již není pouze přepínačem v lokální síti LAN; provádí také přepínání v sítích WAN. Přepínač je nicméně i nadále zařízením, které pracuje především na linkové vrstvě, jeden stejný přepínač však provádí také určité omezené funkce na síťové vrstvě.
- Brána (gateway) je obvykle kombinací softwaru a hardwaru, který propojuje dvě různé sítě pracující pod různými protokoly.
- Patch panely se používají se k ukončení horizontální nebo páteřní kabeláže a k uspořádání rozhraní do rozličných síťových zařízení.
- Racky mají standardizovanou šířku 19", výška a hloubka je volitelná. Podle velikosti jsou racky samostatně stojící nebo montované na zeď.



Kontrolní otázky

- 1) Rozdělte síťové prvky do dvou základních skupin. (odpověď naleznete [zde](#))



- 2) Popište opakovač. (odpověď naleznete [zde](#))
- 3) Popište rozbočovač (HUB). (odpověď naleznete [zde](#))
- 4) Popište most. (odpověď naleznete [zde](#))
- 5) Vysvětlete, k jakému účelu slouží směrovač. (odpověď naleznete [zde](#))
- 6) Vysvětlete, k jakému účelu slouží přepínač. (odpověď naleznete [zde](#))
- 7) Popište bránu (gateways). (odpověď naleznete [zde](#))
- 8) Vysvětlete, k jakému účelu se používají Patch panely. (odpověď naleznete [zde](#))
- 9) Popište rack. (odpověď naleznete [zde](#))

Pojmy k zapamatování

Opakovač, rozbočovač, most, směrovač, přepínač, brána, Patch panel, rack.

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

Gratulujeme! Z učiva o sítích jste právě zvládli teoretickou část. A nyní můžeme tyto poznatky směle využívat v praxi.

