Počítačové sítě 1

Přednáška č.10 – Služby sítě

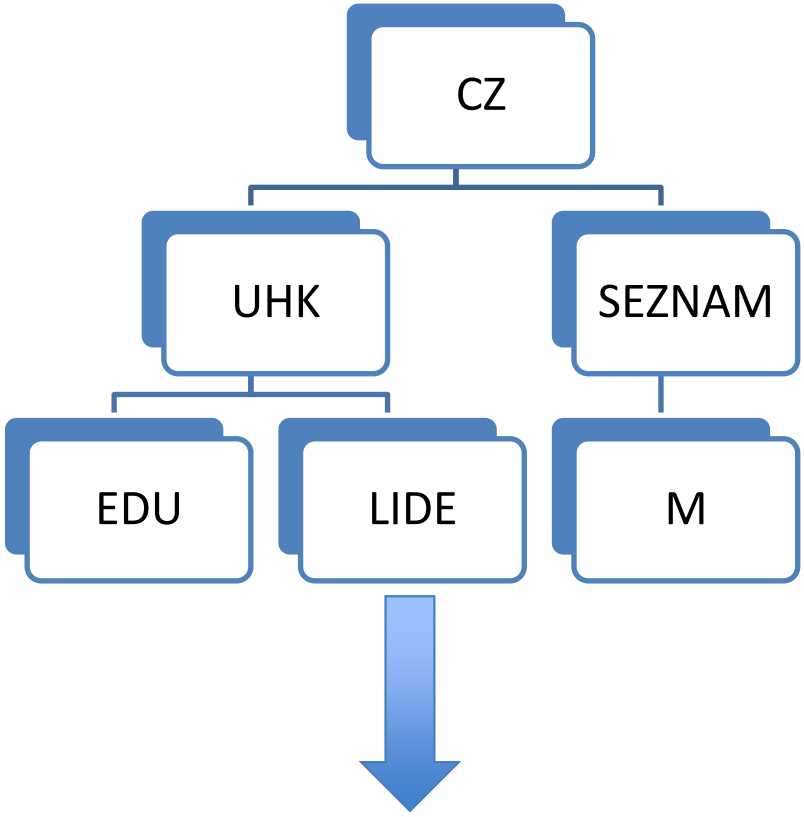
- Služby sítě
  - DNS – Domain Name System
  - DNSSEC – DNS Secure
  - DHCP - Dynamic Host Configuration Protocol
  - DHCP Relay

Služby sítě - DNS

- Komunikace mezi jednotlivými IP uzly probíhá na základě IP adres, které jednoznačně definují každého klienta rozsáhlé počítačové sítě
- Tento přístup je pro člověka nevhodný a těžko zapamatovatelný
- DNS (Domain Name System) je řešení, které umožňuje:
  - využít symbolických adres
  - skrýt nedostatky nebo strukturu sítě
  - rozdělit síť dle logické přehlednosti
  - definovat, vytvářet a spravovat přidělené zóny (rozdělit otevřenou síť do správních oblastí)
  - možnost využití jmen při komunikaci není jediným důsledkem zavedení DNS
- Jmenný systém musí vyřešit problematiku:
  - zásady tvorby, přidělování a správy jmen
  - vytvoření a systematické údržby jmenné databáze
  - zajištění komunikačních a převodních mechanizmů
  - mnoho dalších problémů souvisejících s nasazením DNS

- Internet, respektive otevřená počítačová síť, je rozdělen do tzv. **domén**
  - domény systému DNS zajišťují logické zpřehlednění a rozdělení jednotlivých fyzických částí do jednotného celku
  - d rámci domény je možné vytvářet podskupiny – **subdomény**
  - každá skupina má přiřazeno jméno, z jednotlivých jmen se pak skládá **doménové jméno uzlu**
- **Doménové jméno**:
  - skládá se z řetězců vzájemně oddělených tečkou
  - jméno se zkoumá zprava doleva
  - nejvyšší instancí je tzv. **root doména, vyjadřuje se tečkou zcela vpravo (většinou se vynechává)**
  - V root doméně jsou definovány tzv. **generické domény –TLD**
  - **Top Level Domains:** edu, com, net, org, mil, int, arpa a dvojznakové domény jednotlivých států **(ISO-3166)**
  - jména tvoří stromovou strukturu
  - první řetězec je jméno počítače, další řetězec je jméno nejnižší vnořené domény
  - celé jméno může mít max. 255 znaků, jednotlivé řetězce max. 63 znaků
  - řetězce mohou obsahovat písmena, číslice, pomlčky (nesmí být na začátku nebo na konci)
  - možno používat malá i velká písmena
  - na počítačích uvnitř domény je možné psát pouze jméno počítače bez domény

- = DNS funguje **hierarchicky**
- = Na internetu jsou rozmístěné tzv. **kořenové servery** –servery, které zajišťují kořenovou zónu (pro doménu .xxx)
- = Mají tedy přehled o **delegaci top-level domén**, jako je COM, EDU, DE nebo CZ
- = Každá doména nižší úrovně **musí mít server**, který zajišťuje funkčnost a propojení v systému DNS
- = Servery v hierarchii na sebe **navzájem odkazují** a společně tak vyřeší jakýkoli dotaz

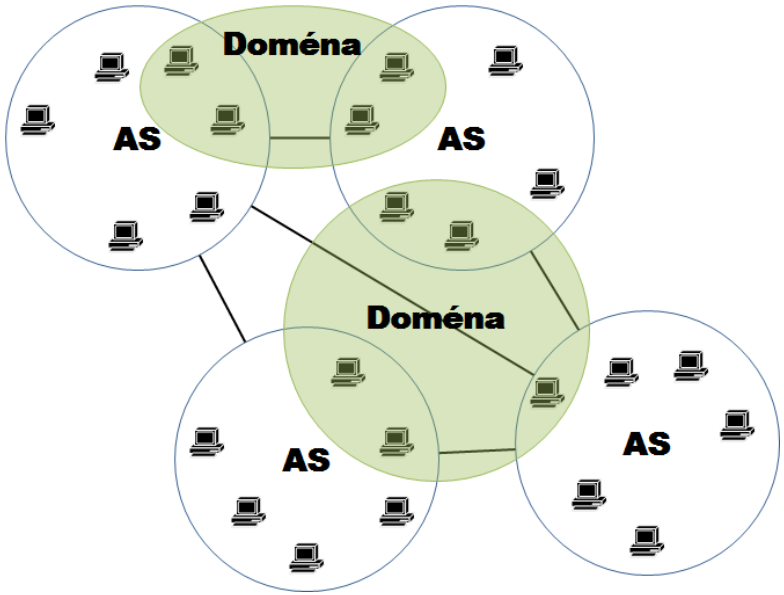


= LIDE.UHK.CZ

- Reverzní překlad je překlad IP adresy na doménové jméno
  - záznam definující vazbu IP adresy na doménové jméno je záznam PTR
  - reverzní překlad využívají některé programy (ftp, traceroute,...)
  - pokud není v DNS zaveden reverzní záznam pro doménové jméno, mohou některé služby nesprávně pracovat
  - záznamy PTR, respektive reverzní domény jsou důležité (ne každý poskytovatel tento princip zodpovědně realizuje)
- Reverzní doména je vždy vytvářena a delegována pro síť IP adres
  - pro síť 194.149.177 musí být v DNS vytvořena a delegována reverzní doména 177.149.194.in-addr.arpa
- Reverzní doména tedy nijak nesouvisí s klasickou doménou
- V jedné reverzní doméně se mohou vyskytovat doménová jména z různých domén

- Typy reverzních domén se odvíjejí od rozsahu používané sítě
- Příkladem může být použití rozsah 256 IP adres – síť třídy C
- O delegaci reverzních domén pro sítě třídy B a C se nestarají **národní sdružení NIC**, ale mezinárodní organizace přidělující IP adresy.
  - v Evropě delegaci reverzních domén zajišťuje **organizace RIPE**
  - na jmenný server RIPE **ns.ripe.net** jsou delegovány reverzní domény pro sítě IP adres, které RIPE přiděluje
  - poskytovatelům, tedy např.: 200.in-addr.arpa, 201.in-addr.arpa, 202.in-addr.arpa
  - RIPE deleguje reverzní domény pro menší intervaly IP adres –sítě třídy C na jmenné servery poskytovatelů nebo koncových uživatelů

- Data o doméně uložené na name serveru jsou nazývány **zónou**
- Zóna obsahuje jen **část domény**. Doména je skupina počítačů, které mají **společnou pravou část svého doménového jména**
- Autonomní systémy dělí Internet z **hlediska IP-adres** (směrování), naproti tomu domény dělí Internet z hlediska jmen počítačů. Reverzní domény kopírují strukturu poskytovatelů Internetu



- Jmenný server **udržuje informace pro překlad** jmen počítačů na IP-adresy (resp. pro reverzní překlad)
  - obhospodařuje nějakou část z prostoru jmen všech počítačů – **zónu**
  - name server 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
- Primární name server
  - udržuje data o své zóně v databázích na disku
  - na primárním name serveru **má smysl editovat databázi**
- Sekundární name server
  - **kopíruje databáze** v pravidelných časových intervalech z primárního name serveru
- Primární i sekundární name servery jsou tzv. autoritou pro své domény, jejich informace se považují za nezvratná (autoritativní)
- Caching only server
  - **není autoritou** –využívá obecné vlastnosti name serveru, tj. data, která jím prochází, **ukládá ve své paměti**
  - tato data se označují jako **neautoritativní**, každý server je caching server, ale slovy caching only zdůrazňujeme, že pro žádnou zónu není **ani primárním, ani sekundárním** name serverem
- Root name server
  - name server obsluhující root doménu
  - root name server je primárním serverem – rozdílné od ostatních name serverů

- Jeden name server může být pro nějakou zónu **primárním** name serverem, pro jinou **sekundárním**
  - **Z hlediska klienta** není mezi primárním a sekundárním name serverem rozdíl
  - Pro správnou činnost musí name server **znát root name servery** (není pro ně však autoritou)
- Forwarding a slave servery
  - nesouvisí s tím, zda jsou primárními nebo sekundárními servery pro nějakou zónu, ale souvisí se **způsobem jejich překladu**
- Předávání dotazů
  - 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 zpět **forwarding serveru konečný výsledek**
  - pro forwarding je praktické použít name server poskytovatele Internetu
- Slave server
  - slave servery se používají v **uzavřených podnikových sítích** (za firewallem), **kde není možný kontakt s root name servery**
  - slave server pak **kontaktuje forwardera**, který je součástí firewallu
  - slave server **musí být forwarding server**
  - oba mohou být caching only servery
  - oba mohou být primární nebo sekundární name servery pro určitou zónu

- Doménová služba je realizována jednoduchým **protokolem DNS**
  - tento protokol pracuje způsobem **dotaz – odpověď**
  - **klient pošle dotaz** serveru a server na dotaz odpoví
  - jistou komplikací je **komprese jmen**, která se provádí proto, aby byly DNS pakety co nejúspornější
  - DNS je **protokol aplikační vrstvy**, neřeší tedy otázku vlastního přenosu paketů
  - využívá DNS jako transportní protokoly **UDP i TCP**
  - dotaz i odpověď jsou přenášeny vždy stejným transportním protokolem.U dotazů na překlad (tj. žádosti o RR record) je dávána **přednost protokolu UDP**
- V případě, že je DNS odpověď delší než 512 B, vloží se do odpovědi pouze část informací nepřesahující 512 B
- Bit TC v záhlaví specifikuje o neúplnou odpověď
- Klient si může **kompletní odpověď** vyžádat protokolem **TCP**
- U přenosu zón např. mezi primárním a sekundárním name serverem se používá protokol TCP
- Name server standardně očekává dotazy jak na portu **53/udp**, tak na portu **53/tcp**

- DNS nejčastěji využívá **UDP**
  - datagram se vyšle prvnímu serveru
  - nepřijde-li odpověď do krátkého časového okamžiku, pošle se datagram s žádostí dalšímu
  - zkusí se další, pak se kolečko opakuje do vypršení časového intervalu
  - tento přístup maximalizuje rychlost z důvodu existence více name serverů
- Přeložení jména na IP-adresu zprostředkovává tzv. **resolver**
- Resolver je **klient**, který se dotazuje name serveru
- Databáze je celosvětově distribuována
  - Nejbližší name server nemusí znát odpověď, proto tento name server může žádat o překlad další name servery
  - Veškerá komunikace se skládá z dotazů a odpovědí
- Name server po startu načte do paměti data pro zónu, kterou spravuje:
  - **Primární** name server načte data z lokálního disku
  - **Sekundární** name server dotazem zone transfer získá data z primárního name serveru
- Name server i resolver společně sdílejí paměť **cache**
  - Do ní ukládají **kladné odpovědi** na dotazy, které provedly jiné name servery
  - **Šetří čas** při opětovných dotazech

- Resolver **zformuluje požadavek** na name server a očekává **jednoznačnou odpověď**
- Odpověď hledá ve své **cache paměti**, zde se nacházejí data získaná při předešlých řešeních (autoritativní i neautoritativní)
  - nezná-li odpověď, pak **kontaktuje další servery** (name server musí znát IP-adresy root name serverů)
  - není-li dostupný žádný root name server, pak pokus o překlad zkolabuje
- Root name server zjistí, že informace o doméně cz **delegoval** větou typu NS na name server nižší úrovně
- Dotazujícímu se name serveru vrátí IP-adresu separujícího **domény cz**
- Name server se obrátí na server pro doménu cz, který zjistí, že informace o doméně delegovala větou NS na nižší úroveň
- Vrátí tedy **IP-adresu** serveru spravujícího doménu uhk.cz
- Server se obrátí na **server spravující doménu uhk.cz**, který požadavek vyřeší (nebo ne) a výsledek vrátí klientovi
- Informace, které server obdržel, si **uloží do cache**

- **„A“** – pro převod doménového jména na **IPv4 adresu**
  - **„AAAA“** – pro převod doménového jména na **IPv6 adresu**
- **„CNAME“** – alias doménového jména na jiné doménové jméno
  - jeden počítač může mít **více logických jmen** pro různé služby (www.fim.cz, ftp.fim.cz)
  - může provozovat jednu službu pro více domén (www.uhk.cz, www.fim.cz atd.)
- **„MX“** – na jaké doménové jméno se má směrovat pošta pro nějakou doménu
  - může, ale nemusí být doménovým jménem konkrétního počítače
  - jeden počítač může přijímat poštu pro více domén
  - změnou v DNS lze směrovat poštu jinam, třeba na centrální podnikový mailserver
- **„NS“** – který počítač slouží jako DNS server pro danou doménu
- **„PTR“** – reverzní záznam
  - jaké je doménové jméno pro konkrétní IP adresu (192.168.1.1.in-addr.arpa PTR lide.uhk.cz)
- **„SOA“** - zajišťuje určitou část režijních informací
  - označuje DNS server pro danou doménu jako primární (Start Of Authority)

- Existují určitá pravidla pro **formální čistotu DNS**
  - nemělo by být zapsáno **více A (AAAA) záznamů** (doménových jmen) na jedinou IP adresu
  - **aliasy** lze vytvořit **pomocí CNAME**
  - záznamy MX, NS, CNAME, PTR a SOA by **měly ukazovat zásadně na A záznam** (FQDN – hlavní a jedinečné doménové jméno)
  - příslušný reverzní záznam **musí přesně odpovídat**
  - V případě nedodržení pravidel je pravděpodobná **nefunkčnost některých služeb** a síťových programů
  - A a PTR záznamy můžou způsobovat nemožnost připojení se na anonymní FTP servery
  - Některé další servery v rámci své bezpečnostní politiky považují rozdílnost záznamů, respektive chyby v DNS jako nebezpečnou činnost, které se snaží zamezit (obrana před potenciálním útokem)

Software	OS	Poznámka
BIND	UNIX, Solaris, BSD, Linux, Windows, MAC OS X	Prakticky nejrozšířenější open-source SW pro realizaci DNS. Stabilita. De facto standard.
MS DNS Server	Windows Server (NT 4.0+)	Komerční produkt MS dodávaný spolu se serverovým OS Windows Server s jádrem NT 4.0+
PowerDNS	Linux, Windows	Open-source, web interface, pokročilé funkce, IPv6
Cisco Network Registar	Solaris, Linux, Windows	Komerční produkt Cisco Systems, kromě DNS poskytuje také DHCP, Cloud ready
Velké množství dalších komerčních, free i open-source implementací ….		

- Registrace domény je v současné době jednoduchá
  - proces registrace je do značné míry **automatizován**
  - existuje **větší množství poskytovatelů**, respektive delegovaných registrátorů
  - delegace domény a konfigurace vlastního serveru je daleko složitějším problémem pro správce sítě
- Delegace domény – obvykle z příčiny změny poskytovatele
  - zprovoznění **primárního name server** pro doménu
  - konfigurujeme sekundárního name server pro doménu, případně požádáme o jeho konfiguraci svého poskytovatele Internetu
  - žádost o delegaci domény v doméně vyšší úrovně
  - pokud se jedná o doménu druhé úrovně, je třeba ještě registrovat **doménu v databázi domén**
  - změna delegace domény **v doméně vyšší úrovně**
- Po provedení změny delegace **je vhodné** nechat běžet alespoň původní sekundární name server (s novými daty) několik dní
- V paměti name serverů po celém světě je ještě IP adresa původních serverů
- Okamžité zastavení primárního i sekundárních name serverů by mohlo způsobit problémy

Služby sítě - DNSSEC

- Jedná se o bezpečnostní rozšíření systému DNS
  - Zajišťuje **důvěryhodnost údajů** z DNS
- Poskytuje uživatelům jistotu, že informace, které z DNS získal
  - Byly poskytnuty **správným zdrojem**
  - **Jsou úplné**
  - Při přenosu nebyla narušena jejich **integrita**
- DNSSEC je definován v dokumentech RFC
  - **RFC 4033** – základní pojmy a jeho principy
  - **RFC 4034** – definice nových záznamů, jež DNSSEC používá
  - **RFC 4035** – popisuje příslušné změny v DNS

Proč je potřeba DNSSEC?

- Většina internetových služeb (e-mail, webové stránky, instant messaging, VoIP) většinou sama o sobě nějaké zabezpečení má
- Ale všechny tyto služby **používají** v nějaké formě službu DNS
- Pokud jsme schopni **podvrhnout službu DNS**, jsme schopni narušit fungování většiny dalších internetových služeb, které ji využívají

- Poskytuje ověřené informace, včetně těch negativních (kdy hledaný záznam neexistuje)
- Vychází z **digitálního podpisu**
  - Každá sada záznamů (záznamy stejného typu pro stejné jméno) **je podepsána**
    - Přidá se k ní záznam **RRSIG s podpisem**
  - Pro podpis se používá běžných kryptografických metod s **veřejným a privátním klíčem**
  - Privátní klíč je použitý **k vytvoření podpisů** a je držen **v tajnosti** (zcela mimo DNS, ideálně i mimo síť jako takovou)
  - Jemu odpovídající veřejný klíč je uložen přímo do zónového souboru dané domény prostřednictvím záznamu **DNSKEY**
  - Aby bylo možné ověřit pravost veřejného klíče, jeho otisk (diggest, záznam **DS**) je vložen do **nadřazené domény** v hierarchii DNS
  - Uložení otisků se **rekurzivně opakuje** až ke kořenovému serveru
  - Pokud má klient **důvěryhodný veřejný klíč ke kořenové doméně** (root), je od něj poté schopen rozvinout **řetězec důvěry** až ke zkoumanému záznamu ☺

- K ověření **negativních** záznamů slouží záznamy **NSEC**
- Ke každému jménu v doméně je přiřazen jeden záznam typu NSEC
- Přináší celkem dvě informace:
  - Seznam typů záznamů pro dotazované doménové jménu
  - Následující jméno v doméně

- V případě dotazu na **neexistující jméno**
  - Server pošle NSEC **záznam jeho předchůdce**, z nějž je patrné, že požadované jméno v doméně není
- V případě dotazu na **neexistující typ záznamu**
  - Server odešle **jeho NSEC** ověřující, že požadovaný typ záznamu pro toto jméno chybí

- Předpokladem pro implementaci DNSSEC nad DNS je, že použitý software zajišťující službu DNS **podporuje DNSSEC**

- Rozšíření je pak možné obecně provést v těchto krocích
  - Je nutné **přidat veřejný klíč** (**DNSKEY**) domény použitý k podepsání záznamů
  - Ke každému jménu v doméně je potřebné **přidat NSEC záznam** se seznamem typů záznamů pro toto jméno a s následujícím jménem
  - Pro každou dvojici jméno-typ záznamu je potřebné **přidat záznam RRSIG** obsahující podpis celé sady, včetně záznamů přidaných v předchozích krocích

Služby sítě - DHCP

- DHCP (Dynamic Host Configuration Protocol) je aplikační protokol z rodiny TCP/IP
- DHCP definován v roce 1993 –standard RFC 2131 z roku zajišťuje poslední definici DHCPv6
- Používá se pro automatické přidělování IP adres koncovým stanicím v síti
- DHCP protokol je rozšířením staršího BOOTP protokolu, který přiděloval IP adresy na neomezenou dobu
- DHCP je s BOOTP obousměrně kompatibilní
- Současně s IP adresou posílá server klientům další nastavení:
  - adresa nejbližšího směrovače
  - masku sítě
  - adresy DNS serverů
  - možnost zasílat adresy doporučených NTP, WINS, SMTP serverů, stárnutí ARP,...
  - definovat lze i uživatelské parametry – neznámé parametry jsou ignorovány

- DHCP protokol přináší několik výhod:
  - uživatelé si na počítači v souvislosti s připojením k síti nemusí **nic nastavovat**
  - zaručuje, že se na síti nevyskytne **konflikt IP adres**
  - správce sítě může **"přečíslovat" síť** nebo **změnit vlastnosti** sítě s minimálním zásahem do práce uživatelů

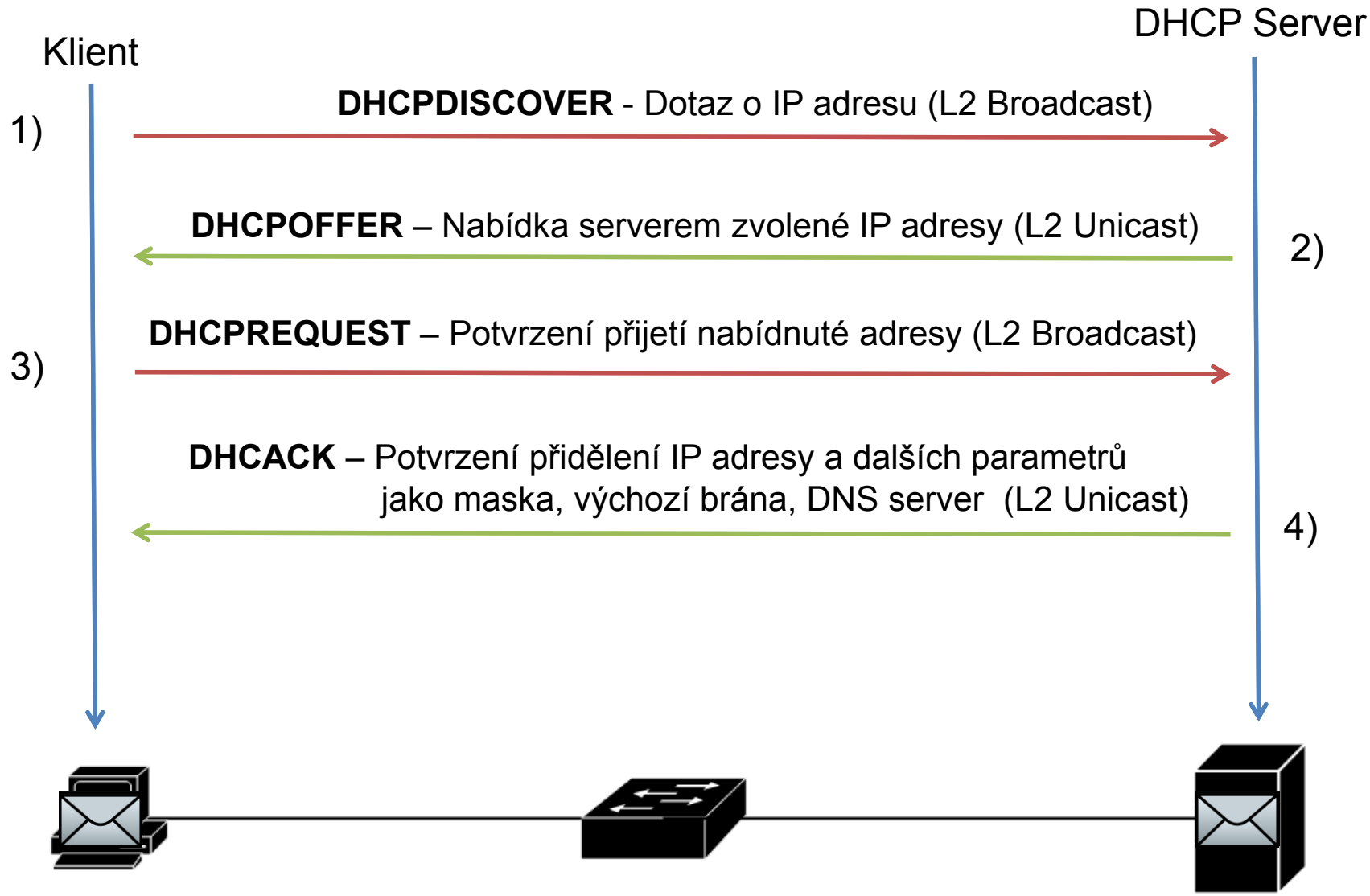
- DHCP je možné realizovat na **HW či SW platformě**
- V závislosti na implementaci využívá DHCP server tři metody alokace IP adres:
  - **Manuální alokace**
  - **Automatická alokace**
  - **Dynamická alokace**

- **Manuální alokace**
  - alokace založena na principu využití tabulky MAC adres
  - IP adresy jsou manuálně definovány administrátorem sítě
  - pouze dotazy klientů s odpovídající hodnotou MAC v záznamech DHCP serveru mohou získat IP adresu a další informace
- **Automatická alokace**
  - DHCP permanentně přiřazuje požadavky klientů
  - adresy jsou volně přidělovány z rozsahu daným serverem
  - rozsah případně rezervace adres pro přidělení definuje administrátor sítě
- **Dynamická alokace**
  - metoda, která zajišťuje dynamické znovupoužití IP adres
  - adresy jsou volně přidělovány z rozsahu daným serverem
  - rozsah případně rezervace adres pro přidělení definuje administrátor sítě
  - každý klient obsahuje speciální SW pro konfiguraci a zasílání požadavků k DHCP serveru
  - proces požadavků a garance zajišťuje spojení v určitém časovém intervalu
  - jedná se o jednoduchý a efektivní koncept dynamického přidělování adres

8	16	24	32
OP Code (1)	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction Identifier			
Seconds – 2 bytes		Flags – 2 bytes	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) – 16 bytes			
Server name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

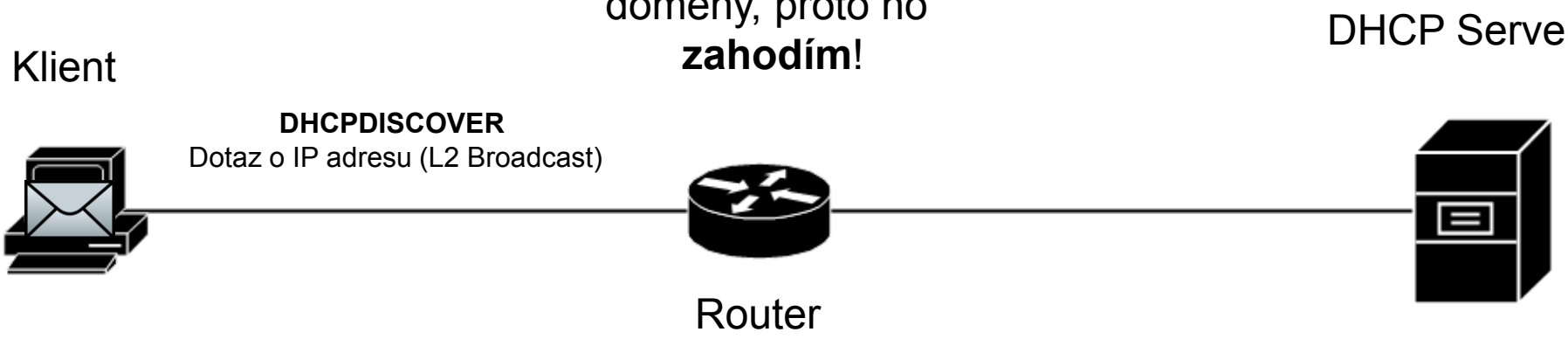
- **DHCPDISCOVER**
  - vysílaný broadcast klientem pro nalezení dostupných DHCP serverů v síti
- **DHCPOFFER**
  - odpověď z DHCHP serveru na DHCPDISCOVER nabízející IP adresu a další související parametry
- **DHCPREQUEST**
  - je zpráva vysílaná od klienta zahrnující níže uvedené parametry
  - požadavek parametrů nabízených jedním ze DHCP serverů a odmítnutí jiných nabídek
  - verifikace a alokace nabídnutých adres v rámci systémové změny
  - požadavek na rozšíření či změna adresy
- **DHCPACK**
  - potvrzení klienta a jeho parametrů serverem
- **DHCPNACK**
  - negativní potvrzovací zpráva klientovi od serveru, indikuje expiraci adresy klienta či jeho odmítnutí

- **DHCPDECLINE**
  - zpráva klientovi, signalizující obsazení dané adresy
- **DHCPRELEASE**
  - zpráva klienta serveru o uvolnění či odevzdání adresy
- **DHCPINFORM**
  - zpráva klienta, který je manuálně nastaven s žádostí o další parametry nastavení


Klient
DHCP Server
1)
DHCPDISCOVER - Dotaz o IP adresu (L2 Broadcast)
DHCPOFFER – Nabídka serverem zvolené IP adresy (L2 Unicast)
2)
3)
DHCPREQUEST – Potvrzení přijetí nabídnuté adresy (L2 Broadcast)
DHCACK – Potvrzení přidělení IP adresy a dalších parametrů
jako maska, výchozí brána, DNS server (L2 Unicast)
4)

- **Problém:**
  - Většina DHCP komunikace probíhá na druhé vrstvě, pomocí L2 Broadcastu a Unicastu
  - Takováto komunikace je možná pouze v jedné broadcastové doméně
  - Pokud se DHCP server nachází v jiné IP síti než klient (tzn. mimo broadcastovou doménu) nelze komunikaci mezi klientem a DHCP serverem uskutečnit

A hele **Broadcast**!
Já jsem směrovač.
Dělím broadcastové domény, proto ho **zahodím**!



- **Řešení je DHCP Relay**
  - DHCP Relay je služba běžící na směrovači, která ví jak vypadá DHCP komunikace a dokáže ji překládat DHCP serveru do jiné sítě, pokud zná jeho IP adresu
  - Pokud router zná IP adresu DHCP serveru a má potřebné směrovací informace k jeho dosažení nahradí MAC adresu v přijatém rámci za MAC adresu svého rozhraní a odešle rámec příslušným rozhraním

Děkuji za pozornost