# 21. Základní principy činnosti protokolů sítě Internet – IP, TCP, UDP. Domain Name System, jeho role a činnost, DNS servery, postup řešení dotazu, reverzní DNS

### Protokol IP (Internet Protocol)

Je datový protokol na síťové vrstvě a tvoří základní protokol dnešnímu internetu. Data se posílají po blocích (datagramy, pakety), putují sítí nezávisle, není zajištěna spolehlivost doručení (to se řeší o vrstvu výš např. TCP). Každerozhraní má svoji IP adresu a v každém datagramu je IP příjemce i odesílatele. Na základě těchto adres probíhá směrování.

**Verze IP:** **IPv4 -** každý datagram má hlavičku (Id, celk. délka, TTL, adresa odesílatele a příjemce, více http://cs.wikipedia.org/wiki/IPv4) adresa 32 bitů, zápis v desítkové soustavě (192.168.56.101), rozdělení na privátní a veřejné adresy (privátní se nesměrují), obsahuje NET ID (část adresy pro sítě) a HOST ID (část adresy konkrétního rozhraní)

**IPv6 -** 128 bitů dlouhé adresy, zápis v šestnáctkové soustavě výhody:

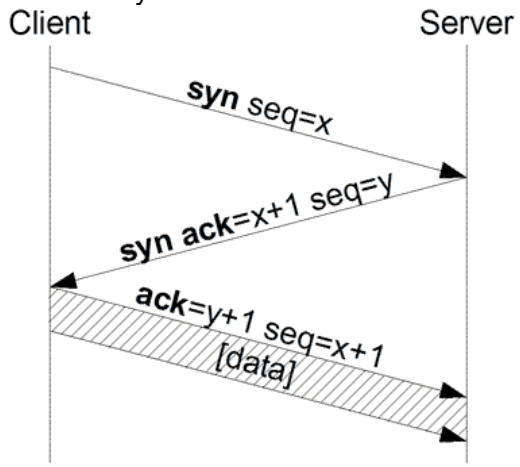
- dostatečně bohatý adresní prostor
- podpora služeb se zaručenou kvalitou
- design odpovídající vysokorychlostním sítím
- bezpečnostní mechanismy přímo v IP
- podpora mobilních zařízení
- automatická konfigurace
- kooperace s IPv4 a co nejhladší přechod ze stávajícího protokolu na nový

(více http://cs.wikipedia.org/wiki/IPv6).

### TCP (Transmisson Control Protocol)

Transportní protokol, zaručuje spolehlivé potvrzení o doručení dat (pomocí sequence a acknowledge čísel), je spojový, kontrolním součtem ověřuje data, udžuje spojení
Je spolehlivý, ale právě kvůli režii spojení je pomalejší než UDP.

**TCP handshake -** 3 kroky




**Port -** slouží k rozlišení komunikujících apllikací, počet je 2^16

**192.168.56.101:12345** - jednoznačné určení IP adresy i komunikujícího portu na síti, některé porty jsou rezervované pro klasické protokoly (HTTP - 80).
(více http://cs.wikipedia.org/wiki/TCP).

### UDP (User Datagram Protocol)

Transportní protokol, není záruka ani o potvrzení ani o doručení datagramu, používá se pro

komunikaci typu otázka - odpověď (DNS, DHCP), rychlejší než TCP. Jeho bezstavovost se využívá u serverů, které obsluhují mnoho klientů a nevadí, že se občas datagram ztratí (VoIP).

**Hlavička UDP -** zdrojový port, cílový port, délka a kontrolní součet

**Rozdíly TCP a UDP:**

TCP:

- spolehlivost – TCP používá potvrzování o přijetí, opětovné posílání a překročení časového limitu. Pokud se jakákoliv data ztratí po cestě, server si je opětovně vyžádá. U TCP nejsou žádná ztracená data, jen pokud několikrát po sobě vyprší časový limit, tak je celé spojení ukončeno.
- zachování pořadí – Pokud pakety dorazí ve špatném pořadí, TCP vrstva příjemce se postará o to, aby se některá data pozdržela a finálně je předala správně seřazená.
- vyšší režie – TCP protokol potřebuje např. tři pakety pro otevření spojení, umožňuje to však zaručit spolehlivost celého spojení.

UDP:

- bez záruky – Protokol neumožňuje ověřit, jestli data došla zamýšlenému příjemci. Datagram se může po cestě ztratit. UDP nemá žádné potvrzování, přeposílání ani časové limity. V případě potřeby musí uvedené problémy řešit vyšší vrstva.
- nezachovává pořadí – Při odeslání dvou zpráv jednomu příjemci nelze předvídat, v jakém pořadí budou doručeny.
- jednoduchost – Nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

(více http://cs.wikipedia.org/wiki/UDP).

## DNS (Domain Name System)

Hiearchický systém pro převod doménového jména na IP adresu a opačně. Prostor doménových jmen tvoří strom. Každý uzel stromu má info o své doméně a odkazy na domény podřízené. Kořenem stromu je kořenová doména (samotná tečka), pod ní jsou domény nejvyšší úrovně (tématické - com, edu, nebo státní - cz, sk). Strom je rozdělen do zón a každou spravují určití správci.

**Doménové jméno:**

Celé jméno se skládá z několika částí oddělených tečkami. Na jeho konci se nacházejí domény nejobecnější, směrem doleva se postupně konkretizuje.

- část nejvíce vpravo je doména nejvyšší úrovně, např. *wikipedia.org* má nejvýšší org.
- jednotlivé části (subdomény) mohou mít až 63 znaků a skládat se mohou až do celkové délky doménového jména 255 znaků.

## DNS server

DNS server má jednu ze tří rolí::

- **Primární server** je ten, na němž data vznikají. Pokud je třeba provést v doméně změnu, musí se editovat data na jejím primárním serveru. Každá doména má právě jeden primární server.
- **Sekundární server** je automatickou kopií primárního. Průběžně si aktualizuje data a slouží jednak jako záloha pro případ výpadku primárního serveru, jednak pro rozkládání zátěže u frekventovaných domén. Každá doména musí mít alespoň jeden sekundární server.
- **Pomocný (caching only) server** slouží jako vyrovnávací paměť pro snížení zátěže celého systému. Uchovává si odpovědi a poskytuje je při opakování dotazů, dokud nevyprší jejich životnost.

Téměř každý DNS server funguje zároveň jako DNS cache. Při opakovaných dotazech pak nedochází k rekurzivnímu prohledávání stromu, ale odpověď je získána lokálně. V DNS

záznamech je totiž uložena i informace jak dlouho lze záznam používat (TTL) a lze také zjistit, zda byl záznam změněn. Po vypršení platnosti je záznam z DNS cache odstraněn.

## Postup řešení dotazu

Každé PC má ve své konfiguraci síťových parametrů obsaženu i adresu lokálního DNS serveru, na nějž se má obracet s dotazy.Adresu lokálního serveru počítač typicky obdrží prostřednictvím DHCP.
Pokud počítač hledá určitou informaci v DNS, obrátí se s dotazem na tento lokální server. Každý DNS server má ve své konfiguraci uvedeny IP adresy kořenových serverů. Obrátí se tedy s dotazem na některý z nich. Kořenové servery mají autoritativní informace o kořenové doméně. Konkrétně znají všechny existující domény nejvyšší úrovně a jejich autoritativní servery. Dotaz je tedy následně směrován na některý z autoritativních serverů domény nejvyšší úrovně, v níž se nachází cílové jméno. Ten je opět schopen poskytnout informace o své doméně a posunout řešení o jedno patro dolů v doménovém stromě. Tímto způsobem řešení postupuje po jednotlivých patrech doménové hierarchie směrem k cíli, až se dostane k serveru autoritativnímu pro hledané jméno, který pošle definitivní odpověď.
Získávání informací z takového systému probíhá rekurzí. Resolver (program zajišťující překlad) postupuje od kořene postupně stromem směrem dolů dokud nenalezne autoritativní záznam o hledané doméně. Jednotlivé DNS servery jej postupně odkazují na autoritativní DNS pro jednotlivé části jména.

Postup řešení dotazu pro “*www.wikipedia.org”*

## Reverzní DNS

Úkolem DNS je poskytnout informace (nejčastěji IP adresu) pro zadané doménové jméno. Dovede ale i opak – sdělit jméno, pod kterým je daná IP adresa zaregistrována. Při vkládání dat pro zpětné dotazy bylo ale třeba vyřešit problém s opačným uspořádáním IP adresy a doménového jména. Zatímco IP adresa má na začátku obecné informace (adresu sítě), které se směrem doprava zpřesňují až k adrese počítače, doménové jméno má pořadí přesně opačné. Instituce připojená k Internetu typicky má přidělen začátek svých IP adres a konec svých doménových jmen.
Tento nesoulad řeší DNS tak, že při reverzních dotazech obrací pořadí bajtů v adrese. K obrácené adrese pak připojí doménu *in-addr.arpa* a výsledné „jméno“ pak vyhledává standardním postupem. Hledá-li například jméno k IP adrese 145.97.39.155, vytvoří dotaz na *155.39.97.145.in-addr.arpa*. Obrácení IP adresy umožňuje delegovat správu reverzních domén odpovídajících sítím a podsítím správcům dotyčných sítí a podsítí. Je dobré mít na paměti, že na data z reverzních domén nelze zcela spoléhat. Do reverzní domény se v principu dají zapsat téměř libovolná jména. Nikdo například nemůže zabránit SURFnetu, aby o počítači 145.97.1.1 prohlásil v reverzní zóně, že se jedná třeba o *www.seznam.cz*. Pokud na tom záleží, je záhodno si poskytnutou informaci ověřit normálním dotazem (zde nalézt IP adresu k *www.seznam.cz* a porovnat ji s 145.97.1.1). Jestliže odpovědí na něj bude původní IP adresa, jsou data důvěryhodná – správce klasické i reverzní domény tvrdí totéž. Pokud se liší, znamená to, že data v reverzní doméně jsou nekorektní.