Počítačové sítě

přednášky

Jan Outrata

říjen–prosinec 2008

Aplikační vrstva

CVIČENÍ: aplikační programové rozhraní BSD Socket/Winsock

Jmenné služby

- aplikace používají pro identifikaci uzlů (síťových rozhraní) v síti síťové (IP) adresy, např. 158.194.80.13
- pro člověka jsou číselné adresy těžko zapamatovatelné a sledují **fyzickou strukturu sítě** – jedna organizace může mít podsítě po celém Internetu

→ **textové označení uzlu** přiřazené k adrese, **strukturované jméno** uzlu sledující **logickou strukturu sítě**

- aplikace používané člověkem používají jména – **jméno se** nejdříve **přeloží na IP adresu** a ta se použije
- použití IP adres pouze nouzově při problémech s překladem
- historický vývoj:
  1. každý uzel udržuje vlastní databázi jmen – s počtem roste náročnost
  2. centrální databáze ve středisku InterNIC – uzké místo, proti duchu internetu
  3. **decentralizovaná distribuovaná databáze** (bez centra) = systém DNS, 1985

Domain Name System (DNS)

- RFC 1035 a další
- strukturované jméno uzlu = symbolické, **doménové jméno**, např. phoenix.inf.upol.cz

= **decentralizovaná distribuovaná databáze** záznamů doménových jmen vs. IP adres (k jedné IP adrese může být přiřazeno více doménových jmen a obráceně)

= **systém překladu doménových jmen** na IP adresy a naopak

= **decentralizovaná distribuovaná (aplikační) služba** modelu (charakteru) klient/server

- záznamy rozmístěny na tzv. **jmenných (DNS) serverech**
- klient, tzv. **řešitel (resolver)**, žádá jmenný server o překlad

Domény

- **stromově hierarchické skupiny** logicky sdružených **doménových jmen** (např. organizace, země, Internet), podskupiny = subdomény (např. oddělení organizace), strukturní jednotky DNS
- **kořenová (root) doména/zóna** – nejvyšší doména/zóna obsahující top-level domény, neuvažuje se, i alternativní (OpenNIC, New.Net aj.)
- **top-level domény (TLD)**:
  - spravované IANA (ICANN), http://www.iana.org/domains/root/db/
  - infrastrukturní (historicky generické): arpa (1985, Address and Routing Parameter Area), např. pro reverzní domény
  - generické (gTLD): otevřené, com (1984, RFC 920), info (2000), net (1984), org (1984), i s omezeními na registraci, biz (2000), name (2000), pro (2000)
  - sponzorované (sTLD, uvažované jako generické): sponzorované s omezeními na registraci, aero (2000), asia (2006), cat (2005), coop (2000), edu (1984), gov (1984), int (1988), jobs (2005), mil (1984), mobi (2005), museum (2000), post (2005, dosud nefunkční), tel (2005), travel (2005), xxx (zamítnutá), od června 2008 jakékoliv (např. msn, google)

Domény

- **top-level domény (TLD)**:
  - národní (country-code, cTLD): dvojznaková jména domén států a unií (ISO 3166), např. cz, sk, eu
  - internacionalizované (IDN): pro testování národních abeced (arabské, cyrilice, čínské, řecké apod.)
  - rezervované: pro speciální účely v neprodukčních sítích
- top-level domény (domény 1. řádu) obsahují domény 2. **řádu** pro organizace (např. upol, google), ty zase domény 3. řádu (např. inf) atd. až po jména uzlů (např. phoenix, mail)
- domény (záznamy pro jména) spravovány jmennými servery

Obrázek: Obrázek průvodce 246

Domény

Doménové jméno

- odráží příslušnost uzlu či subdomény k (sub)doméně, složeno ze jména uzlu v (sub)doméně a jmen nadřazených (sub)domén, např. uzel phoenix v subdoméně inf v subdoméně upol v doméně cz (v kořenové doméně)
- **tečková notace**: (zleva) jména uzlu a nadřazených domén oddělená tečkou, max. 255 B
- jméno uzlu/domény: case-insensitive řetězec znaků, původně pouze ASCII znaky (a-z, 0-9, -, RFC 1034), od 1998 **IDN** (v některých TLD, v testovacím režimu, 2003 IDNA převod na ASCII, algoritmy ToASCII a ToUnicode), max. 63 B
- kořenová doména má prázdné jméno, poslední oddělující tečka se běžně nepíše (relativní jméno), ozn. i s tečnou (absolutní jméno) jako tzv. **plně kvalifikované doménové jméno (FQDN)**
- např. **phoenix.inf.upol.cz.**
- uvnitř domény se obvykle vynechává část jména pro doménu, např. uvnitř inf.upol.cz jen phoenix

Domény

Reverzní domény

- pro **reverzní překlad IP adresy na doménové jméno**, např. z bezpečnostních důvodů (ověření jméno vs. adresa)
- k IP adrese přiřazené doménové jméno v doméně **in-addr.arpa**: (zleva) jména uzlu a reverzních subdomén jako čísla adresy zprava
- např. pro IP adresu 158.194.80.13 jméno 13.80.194.158.in-addr.arpa
- u subsítí (typicky sítí z třídy C) bývají subdomény pro poslední nenulové číslo z adresy subsítě
- jména z reverzních domén překládaná na doménová jména

Obrázek: Obrázek průvodce 248

- reverzní doména **0.0.127.in-addr.arpa**: pro reverzní překlad zpětné smyčky uzlu (127.0.0.1) na jméno localhost, měla by být spravována každým jmenným serverem

Domény

Rezervované domény (RFC 2606)

- example (příklady do dokumentací, 192.0.2.0/24), invalid, localhost, test (také pro testování IDN)

Pseudodomény

- **local** – pro lokální sítě (intranety, 10.0.0.0/8), autokonfigurační protokol Zeroconf (multicast DNS), uzly bez přiděleného doménového jména (169.254.0.0/16, link-local) apod., záznamy pro překlad přímo na uzlu, ne na jmenném serveru
- pro jiné sítě: uucp (síť UUCP, bang notace jména), onion (pro anonymizační síť Tor), bitnet (síť BITNET) aj.

Zóna

Obrázek: Obrázek průvodce 249

- **část** (prostoru jmen) **domény** spravovaná jedním jmenným serverem, kromě subdomén (podřízených zón) delegovaných jiným serverům
- kořenové zóny, speciální zóny – pro implementaci jmenného serveru, stub (seznam jmenných serverů pro subdomény), cache/hint (seznam IP adres kořenových jmenných serverů)

Řešitel (resolver)

- **klient služby DNS** dotazující se jmenného serveru na překlad jména
- vyžaduje od serveru konečnou odpověď, kladnou (výsledek překladu) nebo zápornou (neexistující záznam)
- **komponenta OS**, knihovna nebo knihovní funkce standardní knihovny používané aplikacemi pro jmennou službu
- má v konfiguraci **IP adresy** (!) **jmenných serverů místní domény**, kterých se dotazuje: v unixových OS soubor `/etc/resolv.conf`, v MS Windows záložka DNS v dialogu nastavení protokolu TCP/IP (plus záložka WINS pro systém LAN Manager, protokol NetBIOS a službu WINS poskytující jiný překlad jmen na IP adresy)
- může (dle konfigurace) k zadanému jménu bez koncové tečky (relativnímu jménu) při prvních dotazech přidávat **přednastavené domény** (v MS Windows i domény Windows), při negativních odpovědích znovu bez nich
- konfigurace je možná ručně (staticky) nebo dynamicky pomocí protokolů DHCP nebo PPP

Řešitel (resolver)

- obsahuje **cache se záznamy** z výsledků předchozích dotazů (pozitivní i negativní), bez cache tzv. **pahýlový resolver**, např. v unixových OS (GNU/Linux), pro cache caching-only jmenný server (viz dále, např. pdsnd, dnsmasq) nebo speciální daemon (např. nscd), v MS Windows 2000 a víš resolver s cache při volbě "Klient DNS" (výchozí)
- kromě DNS překladu (před ním) lze využít **lokální soubor** s (ručně zadanými) asociacemi jmen a IP adres

CVIČENÍ: konfigurace resolveru, IP adres jmenných serverů, přednastavené domény, lokální soubor

Jmenný server

- spravuje **záznamy pro svou zónu**, včetně seznamu jmenných serverů pro subdomény/podřízené zóny – tzv. autoritativní záznamy
- obsahuje **cache** se seznamem **IP adres serverů spravujících kořenovou zónu** (z konfigurace) a záznamy z výsledků předchozích dotazů na jiné servery (pozitivní i negativní, neautoritativní záznamy)
- program poskytující klientům (resolver nebo jiný server) odpověď na dotaz, tj. **řeší dotaz** - přeložení jména, např. v unixových OS program BIND
- typy:
  - **primární** – jediný "hlavní", autoritativní, server pro doménu/zónu (záznamy zóny v konfiguraci), poskytuje tzv. **autoritativní odpověď** pro autoritativní záznamy ze své zóny a neautoritativní odpověď pro záznamy z cache (podobně i resolver)
  - **sekundární** – "vedlejší", autoritativní, server pro doménu, pravidelně kopíruje záznamy zóny dotazem (**zone transfer**) z primárního serveru (problém při aktualizaci), poskytuje stejné odpovědi jako primární

Jmenný server

- typy:
  - **caching only** – neautoritativní server pro žádnou doménu nebo zónu, poskytuje pouze **neautoritativní odpovědi**
  - **kořenový** – primární server pro kořenovou doménu/zónu, je jich víc
  - **forwarder** – server provádějící překlad pro jiný server (vystupující jako resolver)
- pro každou doménu vždy **minimálně dva** (nezávislé) jmenné servery, primární a sekundární, v **konfiguraci jmenného serveru nadřízené domény** – pravidlo Internetu
- jeden jmenný server může být primárním pro jednu doménu/zónu a zároveň sekundárním pro jiné domény/zóny
- **round robin**: při více IP adresách (různých strojů) k jednomu jménu cyklické vracení různých adres na dotazy, použití pro rovnoměrné vyrovnávání zátěže strojů (load balancing)

Překlad (vyřešení dotazu)

= překlad doménového jména z dotazu na IP adresu nebo IP adresy (reverzního doménového jména z dotazu) na doménové jméno

- požaduje resolver nebo jmenný server, poskytuje (řeší) jmenný server
- dotaz:
  - **rekurzivní** – vyžaduje se a server vrací konečnou odpověď (autoritativní nebo neautoritativní), typicky požaduje resolver
  - **nerekurzivní** – server vrací seznam IP adres jiných jmenných serverů, typicky požaduje jmenný server (v roli klienta)

Obrázek: Obrázek (kombinace průvodce 253, 260 a 262

Překlad (vyřešení dotazu)

1. aplikace žádá resolver o překlad
2. resolver prohledá cache (pokud ji má)
3. resolver vznese **dotaz na jmenný server** (pro **místní doménu**, první z konfigurace) – pokud nedojde v časovém intervalu odpověď, opakuje dotaz na cyklicky další nebo stejný (pokud je v konfiguraci jen jeden) do vypršení celkového časového intervalu na překlad
4. server prohledá cache
5. server vznese **dotaz na jiný jmenný server** (DNS databáze je distribuovaná) – opakovaně v časových intervalech do vypršení celkového
   - **kořenový** (ze seznamu) – vrací **seznam IP adres jmenných serverů** pro doménu (TLD), náš server vznese dotaz na nějaký z nich, ten v případě nerekurzivního dotazu vrátí seznam IP adres serverů pro subdoménu vyššího řádu atd. až do konečné odpovědi – **proces iterace, rekurzivní překlad**

Překlad (vyřešení dotazu)

5.

- **nadřazený** v rámci domény (pro nadřazenou zónu) nebo **forwarder server** – vrací konečnou odpověď, tj. náš server se chová jako resolver a vznáší rekurzivní dotaz, ale po vypršení časového intervalu provede překlad sám (pokud není tzv. **forwarder only**, v uzavřených sítích)

CVIČENÍ: vysvětlení úplného postupu rekurzivního překladu konkrétního jména (např. www.seznam.cz) z uzlu v konkrétní doméně (např. inf.upol.cz)

- kořenové servery a servery pro TLD obsluhují **pouze** nerekurzivní dotazy (kvůli zátěži, kritické místo systému DNS!), caching only server předává dotaz autoritativnímu serveru domény/zóny
- manuální překlad/diagnostika DNS: nástroje **nslookup, dig**

  CVIČENÍ: manuální překlad jména a IP adresy (reverzní), rekurzivní i nerekurzivní, programem nslookup (dig nebo host)
- veškerá komunikace (dotazy a odpovědi) pomocí **protokolu DNS**

Protokol DNS

- **aplikační protokol** pracující způsobem (stylem) **dotaz-odpověď** poskytující službu typu **klient/server**: klient pošle dotaz, server odpověď
- **operace DNS query** pro získání informací z DNS databáze na serveru, typicky překlad doménového jména na IP adresu
- další operace DNS, např. update, notify, aj.
- používá pro přenos dat transportní protokoly **UDP i TCP**, pro oba **port 53** (tj. 53/udp i 53/tcp)
  - stejný protokol jako u dotazu i pro odpověď
  - pro běžné dotazy, např. překlad jména, nejprve UDP (kvůli režii TCP, časovým intervalům při nedostupnosti serveru), odpověď případně zkrácena na 512 B (velikost UDP datagramu, kvůli IP fragmentaci)
  - pro kompletní odpověď nebo zone transfer dotaz přes TCP
  - protokol DNS (jmenná služba) **není zcela spolehlivý** – časový interval pro odpověď, datagramový protokol UDP
- pro různé operace různé **DNS pakety** – neobsahují kontrolní součet! $\longrightarrow$ měl by obsahovat UDP datagram

DNS query

- základní operace protokolu DNS: **dotaz** (klienta) a **odpověď** (serveru) s **informacemi (záznamy) podle požadavků** v dotazu (pro doménové jméno, typ záznamu) nebo negativní (záznam podle požadavků neexistuje)
- stejný formát DNS paketu pro dotaz i odpověď

Obrázek: Obrázek průvodce 266

- 5 sekcí: záhlaví (povinná), dotazy, odpovědi, autoritativní jmenné servery a doplňující informace (nepovinné)
- sekce **záhlaví (HEADER)**: v dotazu i odpovědi
  - ID: identifikátor, stejný v dotazu i odpovědi pro spárování
  - QR: 0 pro dotaz, 1 pro odpověď
  - Opcode: typ dotazu (stejné v odpovědi), 0 pro standardní, 1 pro inverzní, 2 pro status, 4 pro operaci notify, 5 pro operaci update

DNS query

- sekce **záhlaví (HEADER)**:
  - **AA**: 1 pro autoritativní odpověď
  - **TC**: 1 pro odpověď zkrácenou na 512 B
  - **RD, RA**: 1 pro požadavek (u dotazu) a možnosti (u odpovědi) rekurzivního překladu
  - **Rcode**: kód odpovědi, 0 (NoError) pro bez chyby, 1 (FormErr) pro chybu formátu dotazu, 2 (ServFail) pro neschopnost odpovědi, 3 (NXDomain) pro negativní odpověď (záznam pro jméno z dotazu neexistuje), 5 (Refused) pro odmítnutí odpovědi atd.
  - další: počet záznamů v dalších sekcích, při 1 formát odpovědi "one-answer", při více "many-answer", záleží na implementaci serveru
- sekce dotazů (QUESTION): většinou jediná s jedním záznamem, v dotazu i odpovědi (zopakovaná)
- ostatní sekce (ANSWER, AUTHORITY, ADDITIONAL): odpověď s požadovanými záznamy, autoritativní jmenné servery pro subdomény a jejich IP adresy

DNS query

- **komprese DNS paketu**: další výskyty (části) jména v datech jsou nahrazeny odkazem na první výskyt, oddělovací byte ve jméně (viz dále) je ≥ 192, tj. první dva bity 1, ostatní a další byte = pořadové číslo bytu prvního výskytu od začátku paketu (od 0)
- **inverzní dotaz** (Opcode = 1): jako reverzní, ale pro odpověď se místo vět typu PTR použijí věty typu A (viz DNS záznamy/věty RR), nemusí být podporován

CVIČENÍ: zachytávání a inspekce (záhlaví) DNS query paketů

DNS záznamy/RR věty

- **zdrojové věty (resource records, RR)** – forma dat záznamů v DNS paketech operací, např. u query v dotazu a odpovědi
- forma uložení záznamů o doménových jménech vs. IP adresách a všech ostatních informací DNS v databázi na jmenném serveru (v textové podobě)

Obrázek: Obrázek průvodce 264

- NAME: **doménové jméno** uzlu nebo subdomény, řetězec proměnné délky – před řetězci mezi tečkami v tečkové notaci jmen byte s délkou řetězce a nulový byte na konci, např. 7phoenix3inf4upol2cz0
- TYPE: **typ věty**, určuje význam pole RDATA (v odpovědi serveru):

DNS záznamy/RR věty

- **A** (1): IPv4 adresa (4B, v poli RDATA) k uzlu NAME
- **NS** (2): jméno autoritativního jmenného serveru pro subdoménu NAME (na serveru nadřazené domény) nebo pro doménu z věty SOA (na serveru domény), pro jmenný server by měla být i věta A (tzv. glue záznam)
- CNAME (5): jméno jako alias k NAME
- SOA (6): informace o autoritativním (primárním) jmenném serveru pro doménu NAME (jeho jméno, časový interval pro zone transfer, výchozí hodnota TTL aj.)
- **PTR** (12): jméno k NAME pro reverzní překlad, domény z NAME postupně delegovány od kořenových serverů stromem domén dolů
- **MX** (15): preference (2B číslo) a jméno e-mailového serveru pro doménu NAME
- WKS (11), SRV (33): informace o počítači (jméno, adresa, port, priorita, váha) s aplikační službou (aplikační a transportní protokol) pro doménu NAME
- HINFO (13), TXT (16): informativní, info o HW a SW uzlu NAME, lib. text
- AXFR (252), IXFR: požadavek transferu zóny (celé zóny nebo inkrementálního)
- * (255): požadavek na všechny věty
- další: pro IPv6, DNSsec (zabezpečení DNS) aj.

DNS záznamy/RR věty

- CLASS: třída věty, IN (1) pro Internet, * (255) pro všechny
- **TTL**: time to live, doba platnosti záznamu v cache jiných serverů a resolveru (0 zabraňuje uchovávání v cache)
- RDLENGTH: délka pole RDATA
- RDATA: data (určená typem věty) jako řetězce proměnné délky
- v dotazu operace query jen položky NAME, TYPE a CLASS
- v konfiguraci serveru zadané textově, se syntaxí doménových jmen a pole oddělena bílými znaky

CVIČENÍ: inspekce záznamů (RR vět) z jednotlivých sekcí DNS paketů z následujícího cvičení, rozpoznání komprese jména v paketu

CVIČENÍ: překlady programem nslookup (nebo dig): získání DNS záznamů (RR vět) pro dané jméno neexistujících, daných typů (A, NS, SOA, PTR, MX), ze serveru mimo naši doménu, všech a inspekce TCP segmentů u delší odpovědi, s ladícím výstupem (úroveň debug)

DNS Update

- RFC 3007
- operace DNS protokolu pro **dynamickou aktualizaci DNS záznamů** (vět) v konfiguraci primárního jmenného serveru (jiné přepošlou)
- dotaz + odpověď, formát paketu podobný operaci query: sekce zóny, předpokladů (ne/existující věty), update (přidávané nebo rušené věty) a doplňkových informací
- změny jsou na serveru ukládány do zónových **žurnálových souborů** pravidelně ukládaných do zónových souborů konfigurace
- zabezpečení: Secure DNS Update, update dotazy pouze z dané IP adresy apod.
- klient nsupdate

DNS Notify a zone transfer

DNS Notify (RFC 1996)

- operace DNS protokolu pro **informování** sekundárních a podřízených jmenných serverů (tzv. notify set) **o změně záznamů** na primárním (dříve než vyprší interval aktualizace)
- zprávu periodicky (různým serverům s různým zpožděním) zasílá primární server (formát paketu podobný operaci query), sekundární nebo podřízený potvrdí a požádá o transfer zóny

Zone transfer

- celé zóny = **AXFR**
- inkrementální = **IXFR**: z (primárního) serveru přenos pouze změněných záznamů (operací update, udržuje se historie stavů databáze, při příliš starém stavu nebo rozsáhlém IXFR se provede AXFR)

Rozšíření DNS pro IPv6

- RFC 1886, 2874
- IPv4 používá pro překlad doménového jména na IP adresu záznam (větu) typu A
- pro IPv6 nejdříve věta typu AAAA s 128bitovou IPv6 adresou
- nahrazen větou typu **A6**: počet bin. jedniček v síťové masce (např. 64), část IPv6 adresy pro uzel, doménové jméno domény uzlu
- jedna IPv6 adresa uložena pomoví několika A6 vět, po částech adresy – resolver musí sestavit = A6 record chains
- reverzní doména: nejprve ip6.int (nibble formát, subdomény odzadu IPv6 adresy pro jednotlivé šestnáctkové cifry), pak **ip6.arpa** (bitstring formát, subdomény tvaru \[xcifry/bitů])
- věta typu **DNAME**: analogie CNAME, pojmenování podstromu doménových jmen, posloupnost vět DNAME pro delegaci reverzních domén (místo NS u IPv4)

Zabezpečení DNS

DNSsec

- původní rozšíření DNS, RFC 2535, 2538, dnes novější RFC 4033–5
- zabezpečení ve stromu domén od určité domény níže (ideálně od kořenové, ale prostor jmen rozdělen na zóny)
- použití **asymetrické kryptografie**: veřejný klíč subsomény/zóny ve větě typu KEY (nově **DNSKEY**) podepsaný soukromým klíčem nadřízené domény (obdoba certifikace klíče), podpis ve větě typu SIG (nově **RRSIG**), veřejné klíče nejvyšší (zabezpečené) domény v konfiguraci resolveru
- soukromým klíčem subdomény/zóny podepisovány všechny její záznamy (kromě SIG), pospojované do posloupnosti (podepsanými) větami typu NXT (nově **NSEC**) pro ověření negativních odpovědí, poslední speciální věta SIG podepíše celou DNS query odpověď včetně sekce dotazu (možno i dotaz)
- uložení certifikátů (X.509 aj.) pro aplikace pomocí vět typu CERT
- nevýhody: podepisování náročné, soukromý klíč je potřeba pro podpis každé DNS query odpovědi

Zabezpečení DNS

TSIG (Transaction Signatures)

- autorizace komunikace mezi dvěma systémy, RFC 2845
- **MD5 hash přenášených dat** a sdíleného tajemství ve větě typu **TSIG**
- sdílené tajemství vyměňováno Diffie-Hellmanovým algoritmem pomocí vět typu **TKEY**, nebo asymetrickou šifrou (tajemství zašifrováno zaslaným veřejným klíčem)
- použití u DNS Update – může jen autorizovaný systém

Implementace jmenného serveru

Systém BIND (verze 4)

- DNS věty v textovém tvaru (formát BIND) udržovány v souborech na primárním serveru (část DNS databáze)
- udržovaná data: autoritativní záznamy zóny, záznamy zóny cache/hint (seznam IP adres kořenových jmenných serverů), záznamy delegující subdomény na jiné jmenné servery
- program **named** na unixových systémech, služba **Server DNS** na MS Windows 2000 (může být součástí Active Directory)

BIND nové generace (verze 8 a 9)

- podpora dynamické aktualizace (DNS Update ve spolupráci s DHCP serverem), DNS Notify, IXFR, negativní caching, DNSsec, virtuální jmenné servery, propojení s MS Windows 2000, IPv6
- oproti BIND 4: protokolování zpráv, ACL, master/slave místo primární/sekundární/atd., vícevláknový, implementace i pro MS Windows (Professional, XP)
- **lightweight resolver**: knihovna + (lokální) daemon jako caching-only jmenný server

Testování a ladění DNS

- chybně nastavené DNS: nefungující aplikace, výrazně pomalejší OS (zvláště s firewallem), RFC 1537
- nejdříve ověřit **fungování sítě** (Internetu) pomocí ping
- testování jmenného serveru (jako resolver), ladění a administrace DNS – kontrola konfigurace serveru podle pravidel DNS (nástroje implementace serveru, např. rndc u BIND 9, signály na unixových systémech)
- nástroje (RFC 1713):
  - **nslookup** – posílá (rekurzivní i nerekurzivní) dotazy jako resolver, volba typů záznamů a jmenného serveru aj., interaktivní, ladicí výstup (úrovně debug a d2)
  - **dnswalk** – kontrola konfigurace domény (i reverzních) podle pravidel DNS, z transferu zóny
  - **dig** – posílá dotaz jako resolver, volba typu záznamů a jmenného serveru aj., formát BIND odpovědi

CVIČENÍ: testování DNS (překlady) programy nslookup a dig (viz minulé cvičení), kontrola konfigurace domény programem dnswalk

DNS v intranetu

- uzavřený (bez spojení do Internetu) nebo bez překladu jmen v Internetu: není možné kontaktovat kořenové jmenné servery nutné pro překlad jmen mimo doménu intranetu $\longrightarrow$ **kořenový jmenný server** (pro doménu .) v intranetu vracející negativní odpovědi
- pseudodoména **local** pro intranet – bezpečné, ale nepraktické
- společná doména pro Internet i intranet – nevýhody: v Internetu případně jména uzlů s privátními IP adresami, zveřejnění jmen a IP adres uzlů v intranetu, problematické směrování Internetu v intranetu (filtrace) popř. transparentní aplikační proxy
- **dva pohledy** na doménu (BIND 9) nebo **dvě zóny pro doménu**: dva (primární) jmenné servery, pro Internet (jeho resolver nasměrován na server intranetu) a intranet (forwarduje požadavky mimo zónu na server pro Internet)
- sekundární jmenný server v intranetu forwarduje požadavky mimo doménu/zónu na primární – na firewallu

DNS v intranetu

- **duální DNS**: oba primární jmenné servery na firewallu na různých portech a **DNS proxy** – případně odpovídá negativně za kořenový jmenný server

CVIČENÍ: zprovoznění jmenných serverů, popř. DNS proxy, na intranetu pro pokusnou doménu (viditelnou pouze v intranetu)

Delegace a registrace domén

1. zprovoznění **primárního jmenného serveru** pro delegovanou doménu: připojení k Internetu musí být pevnou linkou
2. konfigurace **sekundárního jmenného serveru**: případně u poskytovatele Internetu
3. žádost o **delegaci domény v nadřazené doméně**: záznamy typu NS pro jmenné servery domény (plus glue záznamy typu A a záznamy typu PTR pro reverzní domény)
4. **registrace domény** v případě domény 2. úrovně: v databázi lokálního Internet Registry (IR) pro TLD (např. pro cTLD národní sdružení NIC) prostřednictvím nějakého **registrátora**, placená služba, doména musí být volná
5. **registrace reverzní domény** pro IP adresu třídy C nebo bloku adres: v databázi regionálního IR (např. RIPE)

Příklad průvodce 370–372

Delegace a registrace domén

- domény 2. úrovně pod cTLD cz spravuje sdružení **CZ.NIC**
- reverzní domény delegovány pro rozsah IP adres:
  - 255 adres třídy C ("adresa" třídy B): pro poskytovatele
  - jedna nebo více adres třídy C: pro organizace, může spravovat i poskytovatel bloku adres
  - interval v jedné adrese třídy C (subsítě, RFC 2317): v rámci organizace, záznamy typu CNAME na jmenném serveru sítě C jako aliasy na záznamy na jmenném serveru pro subsíť

Příklad průvodce 376–379

Internet Registry (IR)

- mezinárodní organizace jednoznačně přidělující v Internetu IP adresy (RFC 1466), čísla autonomních systémů, jména domén (TLD a 2. řádu) aj. uložená v databázích
- **The Internet Assigned Numbers Authority (IANA)** – nejvyšší, rozděluje intervaly mezi regionální IR
- spravují větší geografické oblasti Internetu rozdělené mezi lokální IR, vytváří pro ně normy
- **RIPE NCC** pro Evropu, Rusko (a bývalé sovětské republiky) a severní Afriku, **ARIN** pro Ameriku a jižní Afriku, **APNIC** pro Asijsko-Pacifickou oblast
- lokální IR – národní IR a poskytovatelé Internetu, sponzorují regionální IR
- národní IR: CZ.NIC, DE.NIC, **ICANN** (USA, gTLD, sTLD) atd.

Internet Registry (IR)

RIPE (http://www.ripe.net)

- **objekty databáze** = přidělená čísla a jména (inetnum, domain, aut-num), informace o zodpovědných osobách (správcích sítí, person, role, autorizovaných ke změnám, mntner), směrování (route) aj.
- databáze veřejně přístupná, čtení pomocí programu **whois** nebo služby WWW, editace e-mailem (robot, člověk, okno IP adres přidělované poskytovatelům)