Počítačové sítě

přednášky

Jan Outrata

říjen–prosinec 2010 (aktualizace září–prosinec 2013)

Tyto slajdy byly jako výukové a studijní materiály vytvořeny za podpory grantu FRVŠ 1358/2010/F1a.

Aplikační vrstva

CVIČENÍ: aplikační programové rozhraní BSD Socket/Winsock

Jmenné služby

- aplikace používají pro identifikaci uzlů (síťových rozhraní) v síti **číselné** síťové (IP) adresy, např. 158.194.80.13
- pro člověka jsou číselné adresy těžko zapamatovatelné a sledují **fyzickou strukturu sítě** (na síťové vrstvě) – 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** – 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 klient/server

- záznamy rozmístěny na tzv. **jmenných (DNS) serverech**
- klient, tzv. **řešitel (resolver)**, žádá jmenný server o překlad doménového jména na IP adresu, popř. naopak

Domény

= pojmenované, **stromově hierarchické skupiny** logicky sdružených **uzlů** v síti (např. organizace, země, Internetu), podskupiny = **subdomény** (např. oddělení organizace), strukturní jednotky DNS

- **kořenová (root) doména** – nejvyšší doména stromu obsahující top-level domény, běžně se neuvažuje, existují i alternativní (OpenNIC, New.Net aj.)
- **top-level domény (TLD)**:
  - spravované IANA (ICANN), www.iana.org/domains/root/db/
  - infrastrukturní (historicky generické): jméno **arpa** (1985, Address and Routing Parameter Area), např. pro reverzní domény
  - **generické (gTLD)**: otevřené, jména 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): s omezeními na registraci, jména aero (2000), asia (2006), cat (2005), coop (2000), edu (1984), gov (1984), int (1988), jobs (2005), mil (1984), mobi (2005), museum (2000), post (2005), tel (2005), travel (2005), xxx (původně zamítnutá), od června 2008 jakákoliv (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. jména upol, google), ty zase domény 3. řádu (např. inf) atd. až po jména uzlů (např. phoenix, mail)

– domény spravovány jmennými servery – uloženy a poskytovány záznamy doménových jmen vs. IP adres

Obrázek: Obrázek průvodce 246→257(5)

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 postupně 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), i s tečnou (absolutní jméno) je 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 IP adresy ke jménu)

= k IP adrese přiřazené doménové jméno v doméně **in-addr.arpa**: (standardně) zleva jména uzlu a reverzních subdomén jako čísla v IP adrese zprava

- např. pro IP adresu 158.194.80.13 jméno **13.80.194.158.in-addr.arpa**
- jména reverzních domén překládaná na doménová jména (stejným způsobem jako překlad na IP adresy)

Obrázek: Obrázek průvodce 248→258(5)

- 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: **onion** (pro anonymizační síť Tor), uucp (stará síť UUCP, bang notace jména), bitnet (síť BITNET) aj.

Zóna

Obrázek: Obrázek průvodce 249→259(5)

= **část** (prostoru jmen) **domény** spravovaná jedním jmenným serverem, kromě subdomén (podřízených zón) delegovaných jiným serverům

- **kořenové zóny** (= části kořenové domény), speciální zóny – pro implementaci jmenného serveru, např. stub (seznam jmenných serverů pro subdomény), cache/hint (seznam IP adres jmenných serverů pro kořenovou doménu/zóny)

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 systémové 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) přidávat **přednastavené domény** (v MS Windows i domény Windows), při negativních odpovědích dotazy postupně 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 je pak 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 (stub) – tzv. **autoritativní záznamy**
- obsahuje **seznam IP adres serverů spravujících kořenovou zónu** (z konfigurace, cache/hint) a cache se záznamy z výsledků předchozích dotazů na jiné servery (pozitivní i negativní) – neautoritativní záznamy

= program poskytující klientům (resolver nebo jiný server v roli klienta) **odpověď na dotaz** = výsledek překladu 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
  - **sekundární** – „vedlejší“, autoritativní, server pro doménu/zónu, pravidelně kopíruje záznamy zóny dotazem (**zone transfer**) z primárního serveru, 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 (v roli klienta)
- **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 na jméno, 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 (v roli klienta), poskytuje jmenný server

– dotaz:

- **rekurzivní** – klient vyžaduje 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 – běžně označovaný jako **resolvující jmenný server**, **„resolver“**

Obrázek: Obrázek kombinace průvodce 253, 260 a 262→263 a 269(5)

Překlad (vyřešení dotazu)

1. aplikace žádá resolver o překlad
2. resolver prohledá cache (pokud ji má), v případě cache miss
3. resolver vznese (rekurzivní) **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, v případě cache miss
5. server vznese **dotaz na jiný jmenný server** (DNS databáze je distribuovaná) – opakovaně v časových intervalech do vypršení celkového
   - defaultně **kořenový** (ze seznamu) – na nerekurzivní dotaz vrací **seznam IP adres jmenných serverů pro top-level doménu**, náš server vznese **dotaz na některý 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. • **výjimečně nadřazený** pro nadřazenou domény (zónu) nebo **forwarder** – vrací konečnou odpověď, náš server se chová jako resolver a vznáší rekurzivní dotaz, ale po vypršení časového intervalu provede překlad sám (pokud není tzv. **forwarder only**, např. 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 **dotaz-odpověď** poskytující službu typu **klient/server**: klient pošle dotaz, server odpověď

– základní **operace DNS Query** pro získání informací z DNS databáze na serveru, typicky překlad doménového jména na IP adresu

– další operace DNS, např. Update, Notify, Zone transfer aj.

– používá pro přenos dat transportní protokoly **UDP i TCP**, pro oba **port 53** (tj. 53/udp i 53/tcp)

  – stejný protokol pro dotaz i 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!** → 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→294(5)

– 5 sekcí paketu: záhlaví (povinné), 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, aj.

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
  - **AD**: 1 pro požadavek (u dotazu) a vyznačení (u odpovědi) zabezpečené (podepsané) odpovědi (DNSSec)
  - **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 jeden záznam (**doménové jméno a typ**), v dotazu i odpovědi (zopakovaný)
- ostatní sekce (**ANSWER, AUTHORITY, ADDITIONAL**): odpověď s požadovanými záznamy (ANSWER), jména autoritativních jmenných serverů pro doménu (příp. subdomény, AUTHORITY) a jejich IP adresy (příp. poštovní servery, ADDITIONAL)

DNS Query

- **komprese DNS paketu**: další výskyty (části) doménového jména v paketu jsou nahrazeny odkazem na první výskyt – oddělovací byte ve jméně (viz dále) je ≥ 192, tj. první dva bity 1, ostatní bity a další byte = pořadové číslo bytu prvního výskytu od začátku paketu (od 0)
- **inverzní dotaz** (Opcode = 1): jako reverzní, ale pro odpověď se místo záznamů typu PTR použijí záznamy typu A (viz DNS záznamy/věty RR dále), nemusí být servery 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→272(5)

- **NAME**: **doménové jméno** uzlu nebo subdomény, řetězec proměnné délky – před řetězci mezi tečkami v tečkové notaci jmen je oddělovací byte s délkou řetězce (místo tečky) 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) ke jménu NAME
- **NS** (2): **jméno autoritativního jmenného serveru pro subdoménu** NAME (**na serveru nadřazené domény**) nebo pro doménu z věty SOA (na serveru domény), typicky primárního a sekundárního, pro jmenný server by měla být i věta A (tzv. **glue záznam**), domény z NAME postupně delegovány na servery od kořenových serverů stromem domén dolů
- CNAME (5): jméno jako alias k NAME
- SOA (6): informace o autoritativním (primárním) jmenném serveru pro doménu NAME (jeho jméno, email správce, časový interval pro zone transfer, výchozí hodnota TTL aj.)
- **PTR** (12): (FQDN) **jméno** k NAME **pro reverzní překlad**, reverzní domény z NAME postupně delegovány na servery od kořenových serverů stromem domén dolů
- **MX** (15): preference (2B číslo) a **jméno e-mailového serveru pro doménu** NAME

DNS záznamy/RR věty

- WKS (11), SRV (33): informace o počítači (jméno/IP adresa, port, priorita, váha) s aplikační službou (aplikační a transportní protokol, např. _http._tcp) 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), v DNS paketech operace Zone transfer
- * (255): požadavek na všechny věty, v DNS paketech
- další: pro IPv6, DNSSec (zabezpečení DNS) aj., viz dále

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), v sekundách
- RDLENGTH: délka pole RDATA
- **RDATA**: **data (určená typem věty)**, jména jako řetězce proměnné délky
  - v dotazu operace Query jen položky NAME, TYPE a CLASS
  - **v konfiguraci serveru** (tzv. **zónových souborech**) zadané **v textové podobě**, jména v syntaxi doménových jmen, položky zadaná svým textovým označením, oddělené 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 (A, NS, SOA, PTR, MX) a všech typů, ze serveru mimo místní doménu, inspekce TCP segmentů u delší odpovědi, s ladícím výstupem (úroveň debug)

DNS Update

- RFC 3007
- = operace DNS protokolu pro **dynamickou aktualizaci DNS záznamů** (RR vět) v konfiguraci primárního jmenného serveru (jiné na něj přepošlou)
- dotaz + odpověď, formát paketu podobný operaci Query: sekce zóny, předpokladů (na 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 povolené pouze z dané IP adresy aj.
- 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 serveru (dříve než vyprší interval aktualizace)

– zprávu periodicky (různým serverům s různým zpožděním) zasílá primární server (formát paketu podobný operaci Query), sekundární nebo podřízený server potvrdí a požádá o transfer zóny

Zone transfer

= operace DNS protokolu pro **přenos záznamů zóny** z (typicky) primárního serveru

- **AXFR** = přenos všech záznamů
- **IXFR** = **inkrementální** – přenos pouze změněných záznamů (ručně v konfiguraci nebo operací Update), udržuje se historie stavů databáze, při příliš starém stavu nebo rozsáhlém IXFR se provede AXFR

Rozšíření DNS pro IPv6

- RFC 1886, 2874 aj.
- pro překlad doménového jména na IPv4 adresu se používá záznam (RR věta) typu A
- pro IPv6 adresu nejdříve a nyní záznam typu **AAAA** s 16B **IPv6 adresou**
- dříve dočasně záznam typu A6: počet bin. 1 v síťové masce, část IPv6 adresy pro uzel a doménové jméno domény uzlu, jedna IPv6 adresa volitelně uložena pomocí několika A6 záznamů, po doménách, na různých serverech – resolver musel sestavit tzv. A6 record chain
- **jméno pro reverzní překlad**: nejdříve a nyní jména uzlu a reverzních subdomén jako jednotlivé šestnáctkové cifry v IPv6 adrese (tzv. nibble formát), nejdříve v doméně ip6.int, nyní v doméně **ip6.arpa**, např. pro IPv6 adresu ??? jméno ???, dříve dočasně jména tvaru \[xcifry/bitů] (tzv. bitstring formát)
- záznam typu DNAME: analogie CNAME, jméno jako alias části doménového jména, např. pro postupnou delegaci reverzních subdomén místo záznamů typu NS

Zabezpečení DNS

DNSSec

- dřívější RFC 2535, 2538, dnes novější RFC 4033–5
- = **zabezpečení záznamů na jmenných serverech a v DNS paketech**, dříve od vybraných (top-level) domén/zón ve stromu domén níže, dnes od kořenové domény
- použití **el. podpisu**: soukromým klíčem subdomény/zóny podepsány všechny její záznamy (kromě RRSIG), podpisy v záznamech typu **RRSIG** (dříve SIG), pro ověření **integrity DNS paketu** (např. odpovědi DNS Query) záznamy pospojované do posloupnosti pomocí (podepsaných) záznamů typu **NSEC** (dříve NXT), plus poslední speciální záznam RRSIG podepisující celý paket
- ověření podpisů: veřejný klíč subdomény/zóny v (podepsaném) záznamu typu **DNSKEY** (dříve KEY), podepsaný (certifikovaný) soukromým klíčem **nadřízené domény**, veřejný klíč kořenové domény (self-signed, popř. vyšších zabezpečených domén) v konfiguraci resolveru

Zabezpečení DNS

DNSSec

- možnost uložení certifikátů (X.509 aj.) pro aplikace pomocí záznamů typu CERT
- nevýhody: soukromý klíč je potřeba pro podpis každého DNS paketu se záznamy (podpisy spojujících NSEC záznamů + celého paketu, podpisy jednotlivých záznamů již v podepsané konfiguraci zóny nebo cache)

TSIG (Transaction Signatures)

= **autorizace komunikace DNS serverů**, RFC 2845

- MD5 hash přenášených záznamů a sdíleného tajemství v záznamu typu **TSIG**
- sdílené tajemství vyměňováno Diffie-Hellmanovým algoritmem pomocí záznamů typu **TKEY**, nebo asymetrickou šifrou (tajemství zašifrováno zaslaným veřejným klíčem)
- použití u DNS Update – může jen autorizovaný server

Implementace jmenného serveru

Systém BIND (verze 4)

- DNS záznamy v textovém tvaru (**formát BIND**) udržovány v zónových souborech na primárním serveru
- udržovaná data: autoritativní záznamy zóny vč. záznamů delegujících správu části domény na jiné (podřízené) jmenné servery, záznamy zóny cache/hint (seznam IP adres kořenových jmenných serverů)

= 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
- **lightweight resolver** = knihovna + (lokální) server jako caching-only jmenný server

Testování a ladění DNS

- chybně nastavené DNS $\Rightarrow$ **prodlevy** v aplikacích a OS kvůli časovému intervalu na překlad $\rightarrow$
  1. ověřit **fungování sítě**, např. pomocí ping
  2. ověřit **konfiguraci resolveru** – místní DNS servery, doména
  3. **testování** (místních) **jmenných serverů – dotazy** jako resolver i jako server v roli klienta
  4. kontrola a ladění konfigurace serveru – podle pravidel DNS (nástroje implementace serveru, např. rndc u BIND 9)
- nástroje (RFC 1713):
  - **nslookup** – rekurzivní i nerekurzivní dotazy, volba typů záznamů a jmenného serveru aj., interaktivní, ladicí výstup (úrovně debug a d2)
  - **dig** – rekurzivní i nerekurzivní dotazy, volba typu záznamů a jmenného serveru aj., formát BIND odpovědi
  - **dnswalk** – kontrola záznamů pro doménu (i reverzních) podle pravidel DNS, z transferu zóny

CVIČENÍ: testování DNS (dotazy) programy nslookup a dig (viz minulé cvičení), kontrola záznamů pro doménu programem dnswalk

Delegace a registrace domén

Delegace domény na vlastní jmenné servery

1. vytvoření **primárního jmenného serveru** pro doménu – připojení k Internetu by mělo být pevnou linkou (pravidlo Internetu)
2. vytvoření **sekundárního jmenného serveru** pro doménu – případně u poskytovatele Internetu
3. **delegace domény v nadřazené doméně** = záznamy typu NS v nadřazené doméně a typu PTR v nadřazené reverzní doméně pro jmenné servery delegované domény (plus glue záznamy typu A)

Delegace a registrace domén

Registrace domény 2. úrovně

1. **registrace domény** – v databázi (lokálního) **Internet Registry (IR)** pro TLD (= nadřazená doména, např. pro cTLD cz národní sdružení CZ.NIC), prostřednictvím **registrátora** (často poskytovatel připojení k Internetu), doména musí být **volná**
2. **registrace reverzní domény** – pro rozsah IP adres z bloku adres (= nadřazená reverzní doména), v databázi poskytovatele připojení k Internetu nebo regionálního IR (např. RIPE NCC), prostřednictvím registrátora

Příklad průvodce 370–372

Internet Registry (IR)

= organizace přidělující v Internetu IP adresy (RFC 1466), čísla autonomních systémů, jména domén (TLD a 2. řádu) aj.

- **IANA** (The Internet Assigned Numbers Authority) – nejvyšší, rozděluje mezi regionální IR
- **regionální** – spravují větší geografické oblasti Internetu rozdělené mezi lokální IR
  - **RIPE NCC** – Evropa, Blízký východ a Rusko (a bývalé sovětské republiky)
  - **ARIN** – Severní Amerika
  - **APNIC** – asijsko-pacifická oblast
  - **LACNIC** – Latinská Ameriku
  - **AfriNIC** – Afriku
- **lokální** – národní IR a poskytovatelé připojení k Internetu, sponzorují regionální IR, např. **CZ.NIC**, DE.NIC, **ICANN** (USA, gTLD, sTLD) atd.

Internet Registry (IR)

RIPE (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