Multicast DNS (mDNS) pojmenování klientů v místní síti

Petr Krčmář

ROOT.CZ_ vpsFree.cz

7. října 2023

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Prezentace už teď na webu

https://www.petrkrcmar.cz

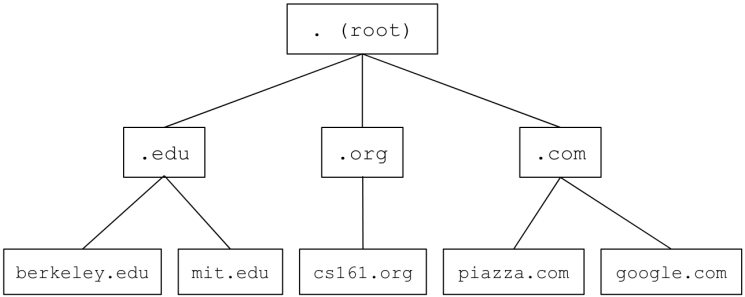
Čísla a názvy

- počítače v sítích mají **číselné** adresy
- člověk si dlouhá čísla špatně pamatuje
  - 37.205.10.41
  - 2a01:430:17:1::ffff:205
- uživatelé mají raději slovní označení
  - www.petrkrcmar.cz
- chceme tedy počítače označovat raději jmény
- problém je starý jako internet samotný
- proto vznikl systém DNS

Pár slov o DNS

- informace jsou rozloženy v globálním **doménovém stromě**
  - každý správce má na starosti jen část
- celé jméno se skládá z domén oddělených tečkami
  - vpravo nejobecnější, vlevo konkrétní
- jméno také popisuje průchod doménovým stromem
  - zájemce o informace postupuje strimem od kořene k listům
- nejprve musíme jít ke kořeni a zjistit delegaci pro .cz
- poté takto postupujeme až ke koncovému uzlu
- hloubka je omezena na 127 úrovní
  - obvykle využíváme maximálně čtyři až pět

Stromová struktura



Role serverů

- autoritativní server drží data našeho zájmu
  - je zodpovědný jen za učritou oblast (zónu)
  - odpovídá na dotazy klientů
- resolver (řešitel) se ptá autoritativních serverů
  - „obchází“ autoritativní servery a ptá se
  - odpovídá klientům a kešuje získané informace
- stub resolver (pahýl) je v operačním systému a vytváří dotazy
  - překládá volání systémového API do protokolu DNS
  - obvykle velmi jednoduchý, jen předá dotaz resolveru

DNS zpráva

- dva typy zpráv: dotazy (query) a odpovědi (answer)
  - obě mají **stejný formát**: hlavička a čtyři sekce
  - výchozím transportním protokolem je UDP (512 bajtů)
- sekce mohou obsahovat zdrojový záznam (RR)
  - ne vždy všechny, u dotazu třeba typicky jen v QUERY
  - nelze se ptát na více jmen či typů najednou

QUERY	hledaná informace: jméno, třída, typ
ANSWER	zdrojové záznamy s odpovědi na dotaz
AUTHORITY	informace o autoritativních serverech
ADDITIONAL	doplňkové informace (třeba A k MX)

ROOT.CZ_ vpsFree.cz

UDP vs. TCP

- DNS je protokol **aplikační vrstvy**
  - musí tedy používat protokoly nižších vrstev
- buď jednoduché nespojové UDP nebo spolehlivé TCP
- při návrhu se počítalo především s použitím UDP
- pouze pro větší objemy dat se přejde na TCP
  - velikost dat v DNS postupně roste
- zároveň má UDP bezpečnostní problémy (odražení)
- statistiky QPS z ODVR od CZ.NIC
  - UDP 7K, DoT 2K, DoH 320, TCP 56

Adresace v místní síti

- v dnešní síťi spousta různých zařízení
  - tiskárny, multimedia, NAS, IoT...
- dynamická adresace (DHCP, SLAAC)
- chceme je nějak lidsky pojmenovávat
- chceme je automaticky vyhledávat
  - objevování zařízení (třeba tiskáren)

Místní síť v DNS

- k adresaci lokální sítě lze použít globální DNS
- informace můžeme vložit do veřejné zóny
  - častěji ale do místního resolveru
- řešení není příliš uživatelsky přívětivé
- vyžaduje místní resolver a není automatizované
  - potřebuje netriviální konfiguraci a údržbu
  - nedovoluje přidávat automaticky nové stroje
- neumožňuje vyhledávat stroje, o kterých nevíme

Cimrman inspirující

mDNS

- koncept mDNS z roku 2000, Bill Woodcock a Bill Manning
  - v roce 2013 vyšlo RFC 6762
- využívá některých základních konceptů DNS
  - princip dotazování a získávání odpovědí
  - způsob zápisu doménových jmen
  - formát DNS zpráv přenášených přes UDP
- nevyužívá ale koncept serverů a doménového stromu
  - mDNS je informačně zcela oddělen od DNS
  - pokrývá adresní informace v **místní síti**
  - odpovídá jen na dotazy z vyhrazené domény `.local`
- klienti spolu komunikují přímo pomocí multicastu

DNS v multicastu

- jednotlivé uzly sítě se vzájemně oslovují na multicastových aresách
  - IPv4 adresa 224.0.0.251 neb IPv6 adresa ff02::fb
  - dosah jen po místní lince – ethernetovém segmentu
- používá se neprivilegovaný port 5353
- zájemce o informaci pošle dotaz na skupinovou adresu
  - držitel informace pošle zpět odpověď
- záznamy jsou dvojího typu: unikátní a sdílené
  - unikátní dotaz je obsluhován jedním uzlem
  - sdílený může být s různými daty na více uzlech

Průběžné dotazování

- některé záznamy má smysl poptávat opakovaně
  - nestačí nám první (nejrychlejší) odpověď, chceme všechny
  - typicky třeba seznam tiskáren v síti
- chceme udržovat aktuální informace o zařízeních
  - zároveň nechceme zbytečně zatěžovat síť
- rozestup mezi prvními dotazy alespoň sekunda
  - další dotazy po nejméně dvojnásobné pauze
  - občerstvování záznamů za polovinou životnosti
- mechanismus potlačování známých odpovědí
  - v dotazu jsou v sekci ANSWER už známé odpovědi
  - odpovídač vrátí jen neznámé záznamy

Vyrovnávací paměť

- stroje poslouchají na multicastové adrese ostatní odpovědi
- plni si informace do své vyrovnávací paměti
  - zbytečně se tak neopakují už odeslané informace
- odpovídači vynechávají stejné záznamy, které poslal někdo jiný
- záznamy lze odstraňovat několika způsoby
  - při ukončení platnosti lze zaslat paket „goodbye“
  - informaci lze přepsat (aktualizovat) bitem cache-flush
  - pokud klient nedostane dvakrát odpověď, sám odstraňuje
    - poslouchají i ostatní, také odstraní
- předcházení kolizím – objevování stejných záznamů
  - třikrát pošlu dotaz na vlastní záznamy
  - pokud někdo odpoví, má přednost a já mlčím

Objevování služeb (DNS-SD)

- DNS-SD (DNS-based Service Discovery) umožňuje objevovat služby
  - popisuje RFC 6763
- vyhledávání služeb podle typu služby
  - formát jména: instance.služba.doména
  - služba určuje aplikační + transportní protokol
  - doména buď .local (mDNS) nebo skutečná v DNS (DHCP)
  - například pracovna._ipp._tcp.local
- objevujeme pomocí reverzních záznamů (PTR)
  - hledáme stroje ve formátu služba.doména
  - odpovědí jsou kompletní jména včetně instancí

Vyhledání tiskáren

```
$ dig -p 5353 -t ptr _ipp._tcp.local @224.0.0.251
```

Získání parametrů služby

- získání parametrů služby z DNS: buď běžné DNS nebo mDNS
  - ze získaných záznamů zjistíme, jak služba funguje
  - SRV obsahuje adresu a port služby
  - TXT pak další informace klíč-hodnota
- obsah záznamů je závislý na poskytované službě

Příklad

```
pracovna._ipp._tcp.local. 10 IN SRV 0 0 631 pracovna.local.
pracovna._ipp._tcp.local. 10 IN TXT "txtvers=1" "qtotal=1" "pdl=…
```

ROOT.CZ_ vpsFree.cz

Implementace u klientů

- Apple Bonjour na macOS, iOS a MS Windows
  - v roce 2002 jako Rendezvous, v roce 2005 přejmenováno
  - využívá iTunes, iPhoto, iChat, Safari, Bonjour Browser a další
- Avahi v Linuxu a BSD
  - implementace klienta i odpovídače
  - navázání na aplikace přes D-Bus API
  - integrováno do KDE a GNOME
- Resolver v systemd-resolved
  - stačí zapnout v `/etc/systemd/resolved.conf`
- Android od roku 2021
  - rozšíření knihovní funkce `getaddrinfo()`
  - transparentní přístup k mDNS pro aplikace

ROOT.CZ_ vpsFree.cz

Implementace u síťových prvků

- tiskárny používají `_ipp._tcp.local.`
- HomeAssistant používá `_home-assistant._tcp.local`
- Chromecast používá `_googlecast._tcp.local.`
- AirTunes používá `_raop._tcp.local`
- SSH používá `_ssh._tcp.local`
- NFS používá `_nfs._tcp.local`
- další najdete v registru organizace IANA nebo v `/etc/services`

Hrátky s příkazem dig

Vyhledání tiskáren

```
$ dig -p 5353 -t ptr +short _printer._tcp.local @224.0.0.251
```

Vyhledání IPP

```
$ dig -p 5353 -t ptr _ipp._tcp.local @224.0.0.251
```

Vyhledání Chromecastů

```
$ dig -p 5353 -t ptr _googlecast._tcp.local @224.0.0.251
```

Odposlech zpráv mDNS

```
$ tcpdump -n host 224.0.0.251 and port 5353
```

Démon Avahi

- implementuje odpovídač na DNS-SD
- balíček i služba `avahi-daemon`
- konfigurace služeb v jednoduchém XML

/etc/avahi/services/ssh.service

```
<?xml version="1.0" standalone='no'?>
  <!DOCTYPE service-group SYSTEM "avahi-service.dtd">
    <service-group>
      <name replace-wildcards="yes">Server</name>
        <service>
           <type>_ssh._tcp</type>
           <port>22</port>
        </service>
    </service-group>
```

ROOT.CZ_ vpsFree.cz

Utility Avahi

- balíčky `avahi-utils`, `avahi-ui-utils` a `avahi-discover`
- `avahi-browse` objevuje služby v síti
- `avahi-discover` klikací objevitel služeb
- `bssh` prochází servery SSH
- `bvnc` prochází servery VNC

Prohlédání všech zařízení

```
$ avahi-browse --all
```

Výhody a nevýhody

- **výhody**
  - nepotřebuje centrální DNS server
  - nevyžaduje instalaci ani správu
  - nepotřebuje žádnou infrastrukturu
  - nevyžaduje publikaci ve veřejném DNS
  - pokrývá libovolný aplikační protokol
  - implementačně velmi jednoduché, široká podpora
- **nevýhody**
  - ve velkých sítích způsobuje multicast velký provoz
    - zároveň vytváří velké množství dotazů
  - nefunguje napříč různými podsítěmi
  - chybí jakékoliv zabezpečení
    - kdokoliv může vysílat cokoliv
    - je nutné používat autentizaci a šifrovat

ROOT.CZ_ vpsFree.cz

Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ_ vpsFree.cz