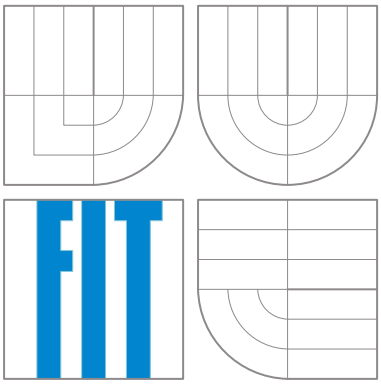
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



Manuál k aplikaci

Proxy DNS generující statistiky dotazů

19. října 2012

Peter Lacko

Obsah

1 Popis činnosti aplikace DNS proxy

DNS proxy je terminálová aplikace sloužící na shromáždování statistik DNS dotazů přicházejících od klientů a jejich zobrazení. Statistiky se zobrazí po výzvě (zaslání signálu `SIGUSR1` procesu „`dns_stat`“), nebo automaticky při ukončení aplikace (signály `SIGTERM` a `SIGINT`). Aplikace implicitně počítá jenom počet dotazů od klientů a odpovědí od DNS serveru. Dále umožňuje zbírat statistiky o typech dotazů, dotazujících se klientech, dotazech (na co se dotazovali), a taktéž zobrazit statistiky za poslední hodinu a hodinový průměr. Pracuje pouze nad protokolem UDP. To jaké statistiky se budou sbírat (a zobrazovat), záleží na parametrech, s jakými byla aplikace spuštěna, viz sekce 3.

Aplikace se pro klienty tváří jako DNS server a pro DNS server jako klient. Pro její plnou funkčnost, je nutné ji spustit jako *root* a to kvůli možnosti naslouchávaní dotazům na portu 53 (tj, standardní port DNS pro naslouchání), který je pro běžné uživatele v unixových systémech nedostupný. Je možné zadat více adres DNS serverů, maximálně ale `MAXNS` (definováno v hlavičkovém souboru `resolv.h`, obvykle 3).

Princip její činnosti je velice jednoduchý. Zde jsou jednotlivé kroky, nutné pro úspěšnou obsluhu jednoho klienta:

1. příjem dotazu od klienta
2. zpracování dotazu, aktualizace statistik
3. přeposlání dotazu DNS serveru
4. čekání na odpověď
5. příjem odpovědi, aktualizace statistik (pouze počet odpovědí)
6. odeslání odpovědi zpátky klientovi

Chybové stavy jsou korektně obslouženy, příslušné chybové hlášení je vypsáno na standardní chybový výstup.

2 Implementace programu

Z hlediska implementace se jedná o síťovou aplikaci operující nad BSD sockety. Po spuštění programu a úspěšném zpracování parametrů, se vytvoří sockety a inicializují se struktury pro komunici s klientem a serverem. Následně se zahájí samotná komunikace, implemntována jako smyčka, kde jeden cyklus = zpracování jedné požadavky.

2.1 Výběr DNS serveru

Jako výchozí DNS server se vybere ten, který byl na příkazové řádce zadán jako první v pořadí. V případe vypršení timeoutu při čekání na odpověď od serveru, se použije server, který byl zadán jako další v pořadí.

2.2 Obsluha signálů

2.2.1 SIGUSR1

Při obdržení signálu `SIGUSR1` se zavolá funkce `printStats()`, která vypíše požadované statistiky na standardní výstup. Pokud byl signál `SIGUSR1` obdržen po dobu čekání na funkci `select()`, pak se znova nastaví file descriptory přísluchající daným socketům a v případě čekání na odpověď od serveru také timeout funkce `select()`.

2.2.2 SIGTERM, SIGINT

Když během čekání na dotaz (blokující `select()`) obdrží program ukončující signál, z funkce obsluhy přerušení se pomocí funkce `siglongjmp()` „vyskočí“ ven ze smyčky, vypíší se požadované statistiky, uzavřou se sockety, uvolní dynamicky přidělená paměť a program se ukončí s návratovou hodnotou 0. Při čekání na odpověď od serveru se navíc dokončí aktuálně zpracovávaný požadavek.

2.3 Uchovávaní statistik za poslední hodinu

Za zmínku stojí také datová struktura použitá pro uložení statistik získaných za poslední hodinu. Zatímco u celkové statistiky stačí pouze inkrementovat počet dotazů (celkově, od každýho klienta, pro každé doménové jméno), u statistik za poslední hodinu je potřeba udržovat také časovou značku, kdy dotaz dorazil.

Z tohoto důvodu byla vytvořena struktura `entry`, obsahující časové razítko příchozího dotazu, typ dotazu, a také iterátory ukazující na příslušnou dvojici v daném asociativním poli (kontajneru) - pole klientů a pole doménových jmen. Vektor těchto struktur je z důvodu úspory paměti aktualizován při každém došlém dotazu a před tiskem statistik.

3 Popis parametrů a ukázky použití

3.1 Popis parametrů

Aplikaci je možné spustit s těmito parametry (viz také nápověda):

povinné:

-s <IP> IP adresa DNS serveru, na kterou budou přeposílany požadavky od klientů, je nutné zadat alespoň jeden parametr -s s adresou, maximálně MAXNS (systémově závislé, obvykle 3)

nepovinné:

<bez parametrů> vytiskne nápovědu

-l <IP> IP adresa rozhraní, na kterém bude aplikace naslouchat defaultně INADDR_ANY

-p <celé číslo> číslo portu, na kterém bude naslouchat, defaultně 53 pro čísla portů < 1024 je nutné aplikaci spustit jako root

-type statistiky o typech dotazů a jejich počtu

-source statistiky podle klientů - kdo se kolikrát ptal

-destination statistiky podle dotazů - kolikrát se na co ptali

-hour statistiky získané za poslední hodinu

-average průměr statistik za hodinu

Při chybně zadaných parametrech se aplikace ukončí s návratovou hodhotou 1.

3.2 Ukázka použití

Na následující ukázce program naslouchá na všech adresách, portu 53 a se dvěma zadanýma DNS serverama - první nevalidní. Po vypršení timeoutu se změní adresa serveru a požadavek je poslán na tento nový DNS server.

```
[root]$ dns_stat -s 123.123.123.221 -s 147.229.190.143 -destination -hour
Timeout vyprsel, novy DNS server: 147.229.190.143

Runtime: 00:00:15

>>>>>>>>>>>> Per last hour statistics >>>>>>>>>>>>

domainname : number of queries
---------------------------------
www.dnssec-validator.cz : 2
www.fit.vutbr.cz : 5
```

```
www4.fit.vutbr.cz : 2

Queries per last hour: 9
Responses per past hour: 9

>>>>>>>>>>>>>>> Overall statistics >>>>>>>>>>>>>>>

domainname : number of queries
---------------------------------
www.dnssec-validator.cz : 2
www.fit.vutbr.cz : 5
www4.fit.vutbr.cz : 2

Total queries: 9
Total responses: 9
-------------------------------------------------
```

4 Literatura

- Studijní opora kurzu ISA
- http://www.ietf.org/rfc/rfc1035.txt