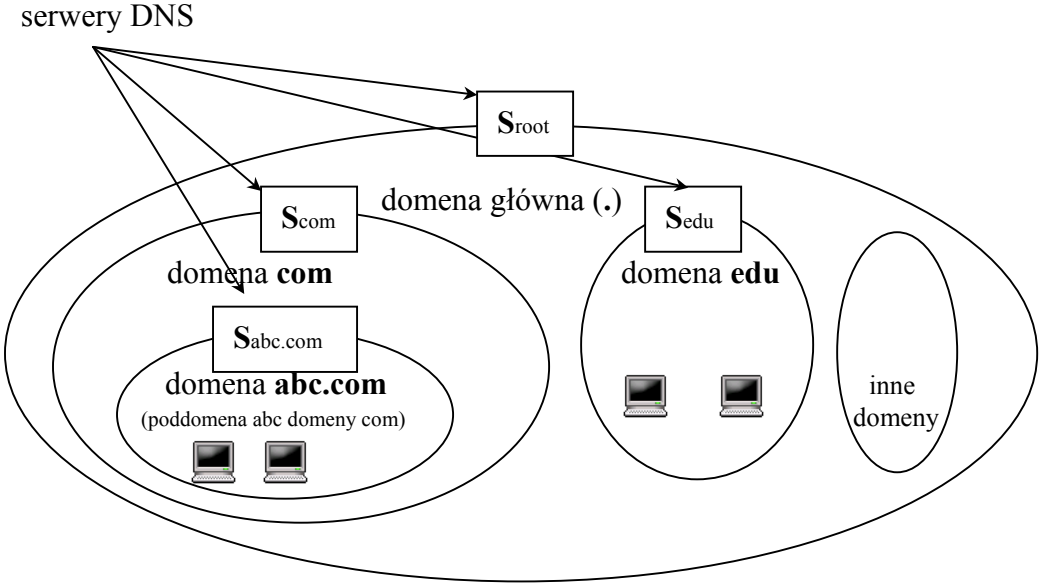
DKonfigurowanie serwera DNS

1 Wprowadzenie

Wymagania wstępne: znajomość podstaw adresacji IP i systemu Linux.
Adres IP nie jest jedynym typem adresu komputera w sieci Internet. Komputer można bowiem adresować (na poziomie warstwy aplikacji) również przez *nazwę*. Ludziom dużo łatwiej jest operować na zrozumiałych nazwach, niż na nieczytelnych adresach numerycznych. Z drugiej strony, komputery preferują liczby. Dlatego aby adresy numeryczne mogły współistnieć z nazwami komputerów, należy umożliwić odwzorowywanie adresów z jednej postaci w drugą. Zadanie to wykonuje system DNS (ang. Domain Name System). Usługa DNS operuje w warstwie aplikacji modelu OSI; została opisana w dokumentach RFC 1034 i 1035.

1.1 Model systemu

Nazwa komputera musi mieć specjalną postać, by można było ją odwzorować w adres IP. Postać ta wynika z przyjętego w systemie DNS modelu, zgodnego z ogólnym modelem klient-serwer. Elementami modelu DNS są: domena oraz serwer DNS. Ilustrację modelu DNS zawiera poniższy rysunek:



W systemie DNS przyjęto hierarchiczny układ domen. Na przykład domeny com i edu są poddomenami domeny głównej, a domena abc.com jest poddomeną domeny com. Hierarchię tę można również przedstawić w postaci drzewa.

Nazwę domeny (od lewej do prawej strony) tworzą nazwy kolejnych naddomen (dokładniej - stref), oddzielone od siebie kropką. Pełna nazwa komputera zaś posiada dodatkowo na początku identyfikator komputera. Na przykład, komputer o identyfikatorze lupus w domenie abc.com ma nazwę lupus.abc.com.
Każda domena posiada swój serwer, przy czym kilka domen może być obsługiwanych przez jeden serwer. Ponadto każda domena ma swojego właściciela i jest przez niego administrowana. W związku z tym aby utworzyć własną domenę, należy ją zarejestrować u właściciela naddomeny (i najczęściej za to zapłacić). Od strony technicznej rejestracja w gruncie rzeczy polega na zapamiętaniu w serwerze naddomeny adresu i nazwy serwera

tworzonej domeny. Serwer danej domeny musi znać lokalizację serwerów wszystkich jej poddomen – jest to jedno z ważniejszych założeń systemu DNS.

Przykładowo, chcąc utworzyć nową domenę def w domenie com, należy najpierw oficjalnie wystąpić do administratora domeny com o rejestrację nowej domeny. Ponadto, domena def.com musi mieć swój serwer, a jego adres i nazwa zostanie zapamiętana w serwerze domeny com.

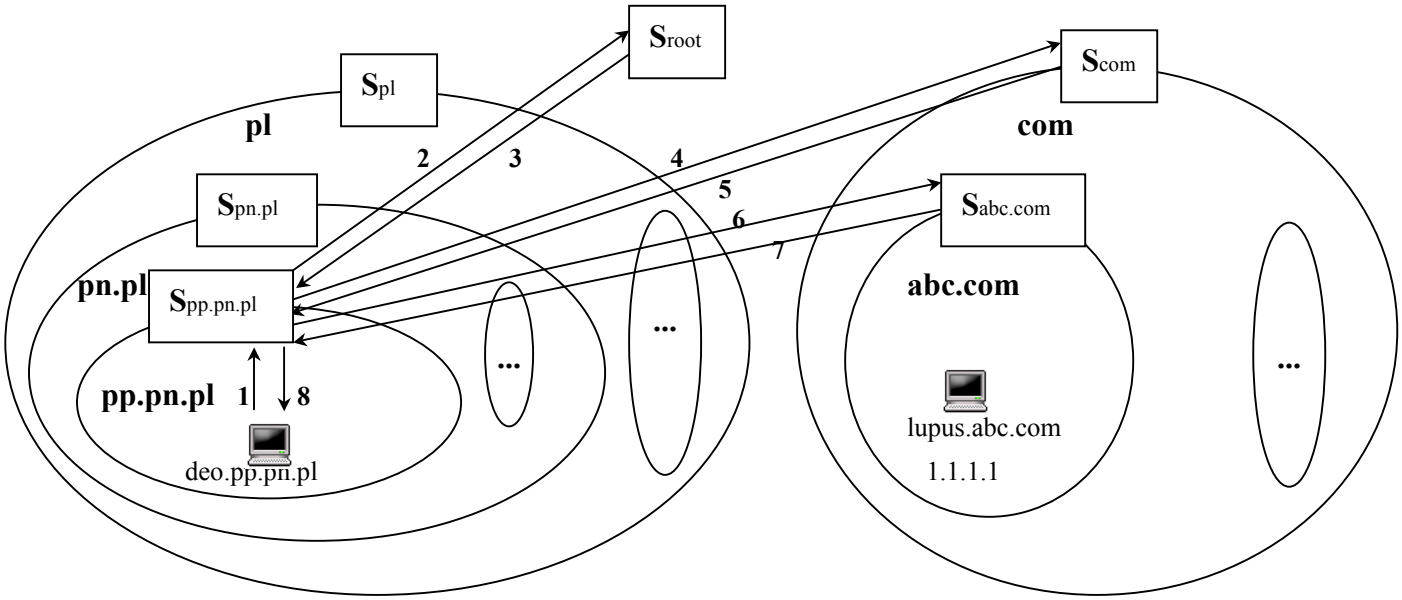
1.2 Typy serwerów DNS

W systemie DNS wyróżnia się dwa główne typy serwerów:

- serwery domeny głównej (ang. root servers) – są to serwery znajdujące się na samym szczycie hierarchii modelu. Obecnie istnieje na świecie około 13 serwerów domeny głównej, z których większość znajduje się w Stanach Zjednoczonych;
- serwery autorytatywne (ang. authoritative servers) – serwerem autorytatywnym danej domeny jest ten, który zawsze posiada aktualne informacje na temat komputerów w tej domenie. Najczęściej serwerem autorytatywnym danej domeny jest jej lokalny serwer. Aby jednak zwiększyć niezawodność systemu, zaleca się, by dla każdej domeny istniały co najmniej dwa serwery autorytatywne.

1.3 Rodzaje zapytań

Zapytanie DNS ma na celu znalezienie odwzorowania nazwy domenowej w adres IP (lub odwrotnego). Istnieją dwa rodzaje zapytań DNS – iteracyjne i rekurencyjne. Zasadę działania zapytania iteracyjnego ilustruje poniższy rysunek:



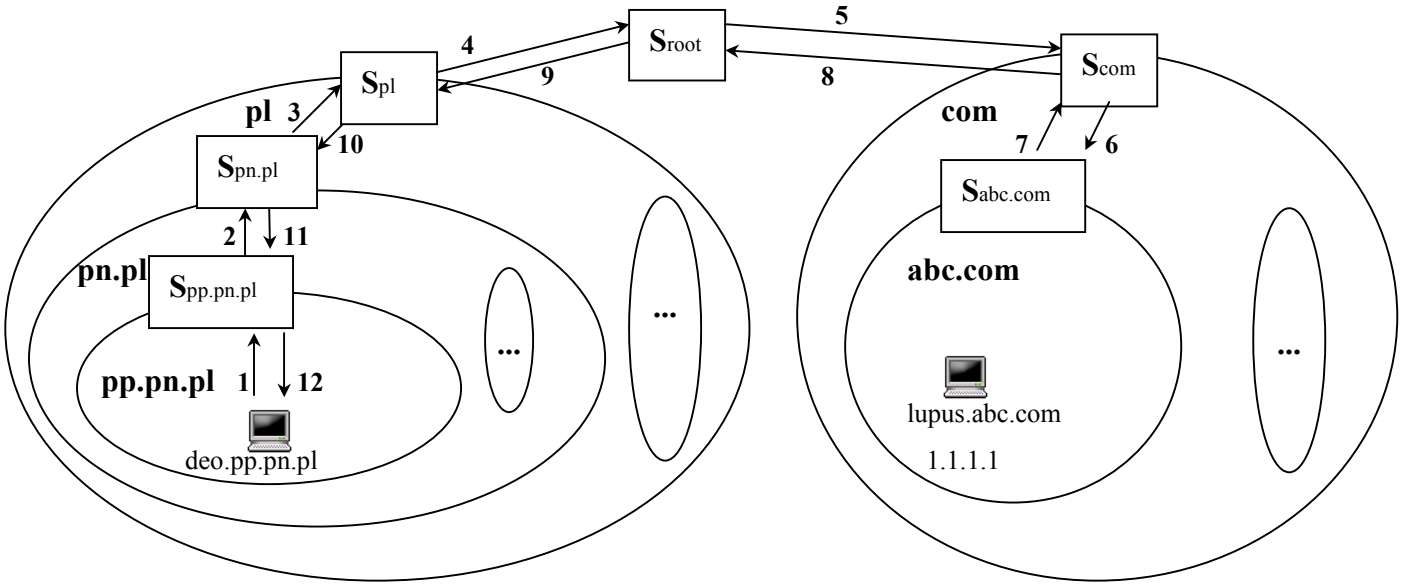
Na rysunku celowo pominięte zostały serwery $S_{pn.pl}$ oraz S_{pl}, aby ilustracja odpowiadała rzeczywistości. Serwer lokalny, nie znając odwzorowania, odwołuje się od razu do serwera domeny głównej.

Kolejne kroki odwzorowywania nazwy lupus.abc.com w adres IP (patrz rysunek):

1. Jaki jest adres IP komputera o nazwie lupus.abc.com?
2. Jaki jest adres IP komputera o nazwie lupus.abc.com?
3. Nie wiem, ale zapytaj serwer domeny com.
4. Jaki jest adres IP komputera o nazwie lupus.abc.com?
5. Nie wiem, ale zapytaj serwer domeny abc.com.

6. Jaki jest adres IP komputera o nazwie lupus.abc.com?
7. Odpowiedź: 1.1.1.1
8. Odpowiedź: 1.1.1.1

Zasadę działania zapytania rekurencyjnego przedstawia poniższy rysunek:



Kolejne kroki odwzorowywania nazwy lupus.abc.com w adres IP (patrz rysunek):

1. Jaki jest adres IP komputera o nazwie lupus.abc.com?
2. Jaki jest adres IP komputera o nazwie lupus.abc.com?
3. Jaki jest adres IP komputera o nazwie lupus.abc.com?
4. Jaki jest adres IP komputera o nazwie lupus.abc.com?
5. Jaki jest adres IP komputera o nazwie lupus.abc.com?
6. Jaki jest adres IP komputera o nazwie lupus.abc.com?
7. Odpowiedź: 1.1.1.1
8. Odpowiedź: 1.1.1.1
9. Odpowiedź: 1.1.1.1
10. Odpowiedź: 1.1.1.1
11. Odpowiedź: 1.1.1.1
12. Odpowiedź: 1.1.1.1

Należy zaznaczyć, że powyższy rysunek służy wyłącznie jako ilustracja koncepcji zapytań rekurencyjnych. W rzeczywistości serwery łączą obydwa rodzaje zapytań. Jeżeli serwer lokalny domeny nie posiada odwzorowania, wysyła zapytanie do jednego z serwerów domeny głównej. Jeśli ten nie odpowiada, pytany jest kolejny serwer domeny głównej, i tak dalej. Serwery domeny głównej są więc odpytywane w sposób iteracyjny. Reszta zapytań zaś ma najczęściej charakter rekurencyjny.

Wykonywanie zapytań rekurencyjnych pozwala wszystkim uczestniczącym serwerom zapamiętać odwzorowanie (ang. DNS caching), co podnosi efektywności systemu.

Jak już wspomniano, system DNS umożliwia również wykonywanie zapytań odwrotnych, znajdujących nazwę komputera o znanym adresie IP.

1.4 Rekordy zasobowe

Opis domeny dokonywany jest przy użyciu tzw. rekordów zasobowych DNS (ang. DNS resource records).
Do najważniejszych wśród nich należą:

- rekord SOA (ang. Start of Authority) – wskazuje, że dany serwer jest najlepszym źródłem informacji o swojej domenie oraz definiuje zachowanie serwerów głównych (ang. Primary) i zapasowych (ang. secondary). Rekord SOA jest obecny jako pierwszy rekord w każdym pliku strefowym;
- rekord A – zawiera odwzorowanie nazwy domenowej w adres IP;
- rekord NS – określa nazwę komputera będącego serwerem DNS dla danej domeny. UWAGA: Dla tej nazwy musi również istnieć rekord A, wiążący ją z adresem IP serwera. Uwaga ta obowiązuje również dla kolejnych rekordów zasobowych;
- rekord CNAME – wiąże dwie nazwy danego komputera: nazwę, pod którą komputer ten występuje w sieci Internet, z faktyczną (tzw. kanoniczną) nazwą tego komputera. Rekord ten umożliwia tworzenie wielu nazw dla jednego komputera;
- rekord MX (ang. Mail eXchanger) – określa nazwę kanoniczną komputera będącego serwerem poczty elektronicznej w danej domenie. Serwery SMTP odczytują jego wartość, aby wiedzieć, do którego komputera należy wysyłać pocztę adresowaną do danej domeny;
- rekord PTR – definiuje odwzorowanie odwrotne (adresu IP w nazwę komputera).

To właśnie wartości rekordów zasobowych przesyłane są w zapytaniach i odpowiedziach DNS. Na przykład serwer poczty elektronicznej odczytuje wartości rekordów MX, z kolei serwer DNS – najczęściej wartości rekordów A i NS.

1.5 Narzędzia systemu Linux

Istnieją dwie implementacje usługi DNS: wykorzystywana w laboratorium - BIND (ang. Berkeley Internet Name Domain) oraz djbdns (nazwa od nazwiska twórcy D. J. Bernstein).
W systemie Linux rolę serwera pełni proces **named**. Jego parametry konfiguracyjne znajdują się w pliku **/etc/named.conf**. Zawiera on między innymi: definicje domen (bez rekordów zasobowych opisujących domenę), opcje rejestrowania zdarzeń w dzienniku systemu (w logu) oraz opcje bezpieczeństwa. Daną domenę opisują rekordy zasobowe, zawarte w tzw. pliku strefowym (ang. zone file), którego nazwa wskazana jest w pliku /etc/named.conf.
Wznowienie pracy serwera można wywołać poleceniem **/etc/rc.d/named restart**.

Stronę klienta realizuje program **dig** (lub jego poprzednik **nslookup**). Konfiguracja klienta pamiętana jest w pliku **/etc/resolv.conf**; wymienia się tam adresy IP jego serwerów DNS.

2. Organizacja, wymagany sprzęt i oprogramowanie

- zadanie wykonuje grupa 2-osobowa;
- sprzęt: 2 komputery PC;
- oprogramowanie: system Linux.

3. Zadania

1. W domenie pro.pl utworzona została poddomena pp.pro.pl. Serwer domeny pro.pl przechowuje rekordy NS oraz A wskazujące, że serwerem domeny pp.pro.pl jest komputer o adresie 150.254.17.101. W tym komputerze należy skonfigurować i uruchomić serwer DNS dla domeny pp.pro.pl. Ponadto nowa domena powinna zawierać komputer o nazwie host.pp.pro.pl z prywatnym adresem IP w sieci 192.168.1.0. Poprawna konfiguracja obydwu komputerów umożliwi odwzorowywanie nazwy host.pp.pro.pl we właściwy adres IP.
   UWAGA – parametr TTL na początku pliku strefowego określa, jak długo serwery DNS odczytujące rekordy danego serwera powinny je zapamiętywać. Ponieważ w warunkach laboratoryjnych zdarza się popełniać błędy konfiguracyjne, serwery długo pamiętałyby błędne rekordy. Dlatego parametr ten powinien mieć małą wartość, na przykład jedną minutę ($TTL 1M lub $TTL 60).
2. Porównać czasy wykonania dwóch zapytań DNS o tę samą nazwę komputera (polecenie **dig** <nazwa_komputera>); wyjaśnić różnicę wyników.

4. Pytania sprawdzające

1. Jaka jest funkcja i zasada działania systemu DNS?
2. Jakie są rodzaje: a) serwerów DNS; b) zapytań DNS; c) rekodrów zasobowych DNS?
3. Jak wykonywane są rekurencyjne oraz iteracyjne zapytania DNS?
4. Opisz kolejne kroki przy konfiguracji serwera DNS.
5. Co to jest odwrócone zapytanie DNS (ang. DNS reverse lookup)? Jakie warunki muszą zostać spełnione, aby możliwe było wykonywanie zapytań odwróconych?
6. Na czym polega transfer strefy (ang. zone transfer) w systemie DNS ?
7. Jak działa serwer DNS typu forwarder ?

5. Literatura

1. Opis systemu DNS: książki A. S. Tanenbaum „Computer Networks” oraz J. F. Kurose, F. Ross „Computer Networking – A Top-Down Approach Featuring the Internet”.
2. Konfiguracja serwera BIND: dokument DNS HOWTO: http://www.langfeldt.net/DNS-HOWTO/BIND-8/DNS-HOWTO.html#toc7,
   Książka „Pro DNS and BIND”: http://www.zytrax.com/books/dns/.
3. Informacje o rekordzie zasobowym SOA: http://support.microsoft.com/kb/163971

FRAGMENT PRZYKŁADOWEGO PLIKU /etc/named.conf

```
options {

        # The directory statement defines the name server's
        # working directory

        directory "/var/lib/named";

        # If notify is set to yes (default), notify messages are
        # sent to other name servers when the the zone data is
        # changed. Instead of setting a global 'notify' statement
        # in the 'options' section, a separate 'notify' can be
        # added to each zone definition.

        notify no;
};

# plik opisujący domenę główną
zone "." in {
        type hint;
        file "root.hint";
};

# plik opisujący lokalny komputer (domena localhost)
zone "localhost" in {
        type master;
        file "localhost.zone";
};

# plik dla zapytań odwróconych
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};
# You can insert further zone records for your own domains below.
```

FRAGMENT PRZYKŁADOWEGO PLIKU STREFOWEGO /var/lib/named/abc.com

```
$TTL 1M
abc.com.        IN SOA      abc.com.   root (
                            42              ; serial (d. adams)
                            2M              ; refresh
                            4M              ; retry
                            6M              ; expiry
                            1M )            ; minimum
abc.com.        IN NS       ns1
host1           IN A        192.168.1.2
host2           IN A        192.168.1.3
ns1             IN A        120.120.1.1
```