Politechnika Łódzka
Instytut Informatyki Stosowanej

Administracja i bezpieczeństwo systemów sieciowych

Laboratorium

Ćwiczenie nr 3.

Usługi DNS w systemie Linux

1. Cel ćwiczenia

Celem ćwiczenia jest zainstalowanie, uruchomienie i skonfigurowanie serwera DNS w systemie Linux.

2. Wstęp

Podstawa technicznego systemu DNS jest ogólnoświatowa sieć serwerów. Przechowują one informacje na temat adresów domen. Każdy wpis zawiera nazwę oraz odpowiadający jej adres IP. Wpisy udostępniane są automatycznie, co pozwala na pracę Internetu. DNS to również protokół komunikacyjny. Opisuje on sposób łączenia się klientów z serwerami DNS. Częścią specyfikacji protokołu jest również zestaw zaleceń, jak aktualizować wpisy w bazach domen internetowych. Po całym świecie rozsiane są serwery DNS, które odpowiadają za obsługę poszczególnych adresów internetowych. Listę 13 głównych serwerów odpowiedzialnych za obsługe poszczególnych domen najwyższego poziomu można pobrać z ftp://ftp.rs.internic.net/domain/named.root.

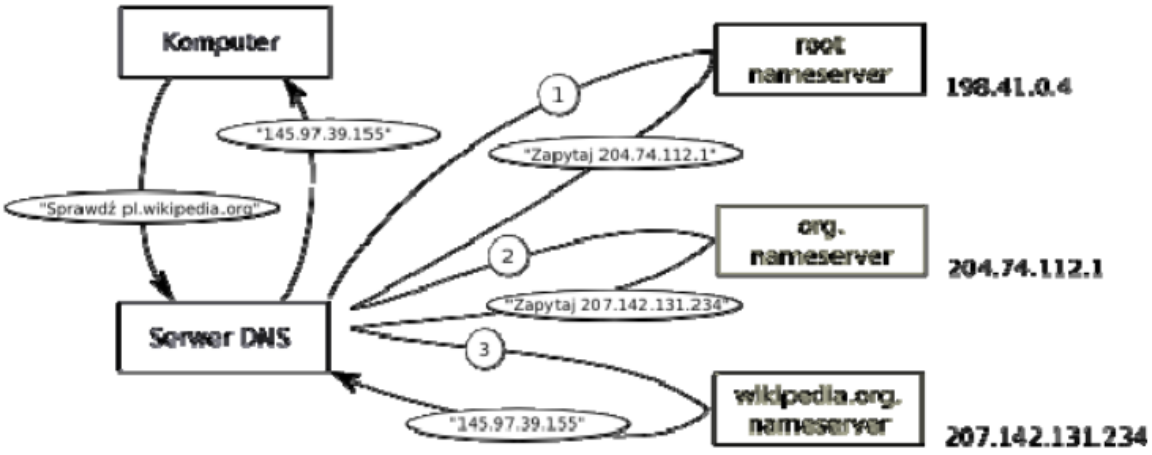
System DNS posiada następujące cechy:

- Nie ma jednej centralnej bazy danych adresów IP i nazw. Najważniejsze jest te 13 serwerów, które są rozrzucone na różnych kontynentach.
- Serwery DNS przechowują dane tylko wybranych domen.
- Każda domena ma co najmniej 2 serwery DNS obsługujące ja, jeśli wiec nawet któryś z nich będzie nieczynny, to drugi może przejąć jego zadanie.
- Serwery DNS przechowują przez pewien czas odpowiedzi z innych serwerów (ang. caching), a wiec proces zamiany nazw na adresy IP jest często krótszy niż w podanym przykładzie.
- Każdy komputer może mieć wiele różnych nazw. Na przykład komputer o adresie IP 207.142.131.245 ma nazwę pl.wikipedia.org oraz de.wikipedia.org.
- Czasami pod jedna nazwa może kryć się więcej niż 1 komputer po to, aby jeśli jeden z nich zawiedzie, inny mógł spełnić jego role.
- Jeśli chcemy przenieść serwer WWW na inny szybszy komputer, z lepszym łączem ale z innym adresem IP, to nie musimy zmieniać adresu WWW strony, a jedynie w serwerze DNS obsługującym domenę poprawiamy odpowiedni wpis.

- Protokół DNS posługuje się do komunikacji głównie protokołem UDP.
- Serwery DNS działają na porcie numer 53.

Przykład działania systemu DNS

Na rysunku nr 1 przedstawiono przykład działania usługi DNS.



Rys. 1. Przykład działania usługi DNS.

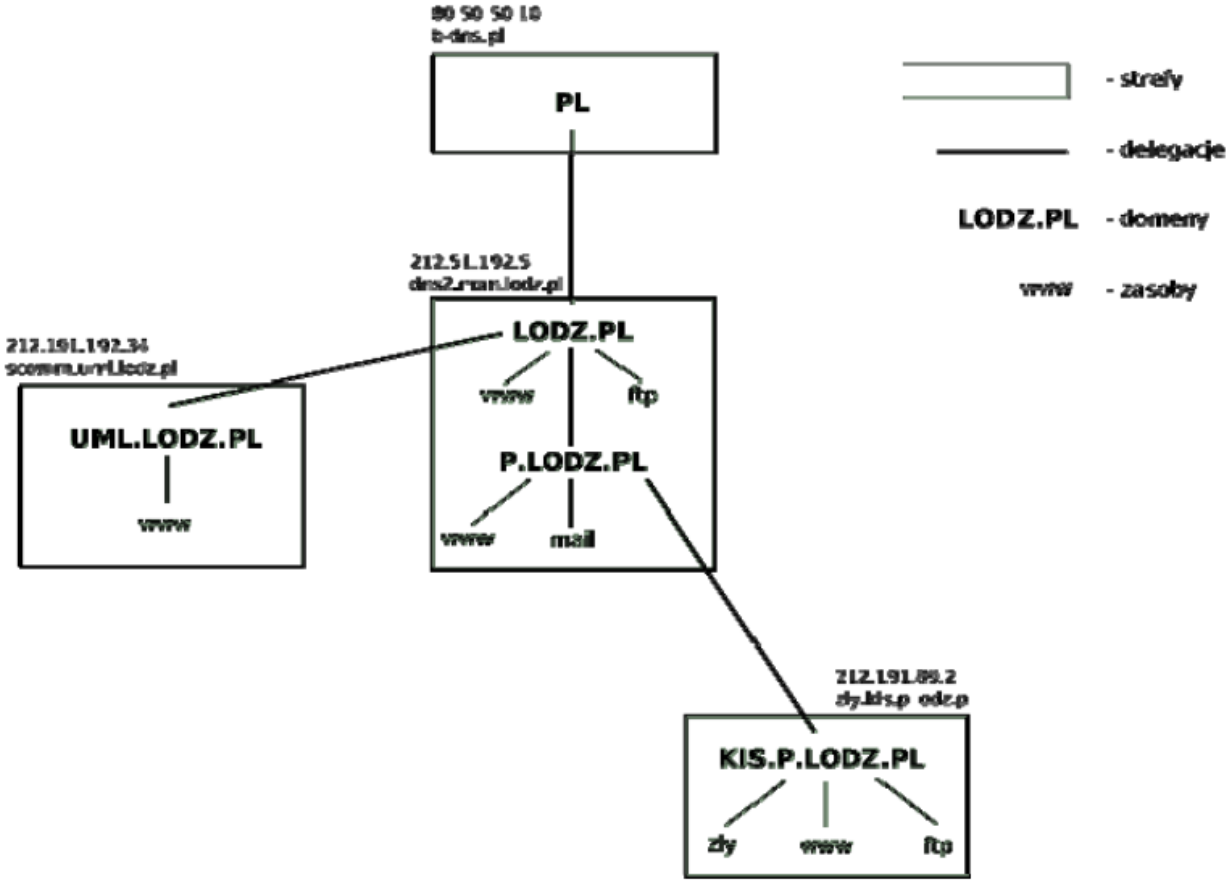
Składowe systemu DNS

Strefa DNS jest zbiorem plików lub rekordów (mówiąc precyzyjniej, bazą danych wpisów rekordów zasobów), które odpowiadają fragmentom hierarchicznej przestrzeni nazw DNS. Strefy DNS są wykorzystywane do określania tych serwerów DNS, które są odpowiedzialne (autorytatywne) za udzielanie odpowiedzi na zapytania o rozwiązanie nazwy dotyczącej danej części hierarchii DNS. Strefy DNS różnią się od domeny tym, że strefy mogą obejmować jedną lub wiele domen DNS. Strefa rozpoczyna się jako baza danych dla jednej nazwy domeny DNS. Jeśli poniżej domeny użytej do utworzenia strefy są dodane inne domeny, mogą one być się częścią tej samej strefy lub mogą należeć do innej strefy. Po dodaniu poddomeny może ona być:

- Zarządzana i dołączona jako część pierwotnych rekordów strefy, lub
- Delegowana do innej strefy utworzonej w celu obsługi poddomeny

Na przykład na rysunku 2 przedstawiono fragment domeny lodz.pl, która zawiera nazwy domen na obszarze Łodzi. Kiedy domena lodz.pl jest po raz pierwszy tworzona na jednym serwerze, jest konfigurowana jako pojedyncza strefa dla całego obszaru nazw DNS sieci komputerowej w Łodzi. Jeśli jednak w domenie p.lodz.pl wystąpi potrzeba użycia poddomen,

musza one zostać dołączone do tej strefy albo delegowane do innej strefy. W tym przykładzie domena p.lodz.pl ma nową poddomenę uml.p.lodz.pl, delegowaną ze strefy p.lodz.pl i zarządzaną w swojej własnej strefie. Jednak strefa p.lodz.pl musi zawierać kilka rekordów zasobów, aby zapewnić informacje o delegowaniu, które odwołują się do serwerów DNS autorytatywnych dla delegowanej poddomeny uml.p.lodz.pl. Jeśli w strefie p.lodz.pl nie będzie stosowane delegowanie do poddomeny, wszelkie dane dotyczące tej poddomeny pozostaną częścią strefy p.lodz.pl. Na przykład poddomena p.lodz.pl nie jest delegowana, lecz jest zarządzana przez strefę lodz.pl.



Rys. 2. Strefy i domeny.

Serwer podstawowy jest autorytatywnym dla strefy serwerem nazw. Wszystkie zadania administracyjne związane z ta strefą (takie jak tworzenie poddomen wewnątrz strefy lub inne podobne zadania administracyjne) muszą być wykonane na serwerze podstawowym. Dodatkowo zmiany związane ze strefą lub modyfikacje czy dodawanie kolejnych rekordów zasobów w pliku tej strefy musi być przeprowadzone na serwerze podstawowym. Dla każdej strefy istnieje serwer podstawowy.

Serwer pomocniczy jest zapasowym serwerem DNS. Odbiera on od serwera podstawowego wszystkie swoje pliki stref w czasie transferu stref. Może istnieć wiele serwerów pomocniczych dla danej strefy – tyle, ile jest konieczne, aby zapewnić zrównoważenie obciążenia, odporność na uszkodzenia i zredukowanie ruchu w sieci. Ponadto każdy serwer DNS może być serwerem pomocniczym dla jednej lub więcej stref.

Najważniejsze typy rekordów DNS oraz ich znaczenie:

- **rekord A -** rekord adresu (ang. address record) przypisuje do nazwy domeny DNS 32bitowy adres IPv4.
- **rekord AAAA -** rekord adresu IPv6 (ang. IPv6 address record) mapuje nazwę domeny DNS na jej 128 bitowy adres IPv6.
- **rekord CNAME -** rekord nazwy kanonicznej (ang. canonical name record) ustanawia alias nazwy domeny. Wszystkie wpisy DNS oraz poddomeny są poprawne także dla aliasu.
- **rekord MX -** rekord wymiany poczty (ang. mail exchange record) mapuje nazwę domeny DNS na nazwę serwera poczty.
- **rekord PTR -** rekord wskaźnika (ang. pointer record) tworzy powiązanie pomiędzy adresem IP i nazwa hosta w strefach wyszukiwania wstecznego. (ang. reverse DNS lookup).
- **rekord NS -** rekord serwera nazw (ang. name server record) mapuje nazwę domenowa na listę serwerów DNS dla tej domeny. Każdy serwer DNS, zarówno podstawowy, jak i pomocniczy, powinien zostać zadeklarowany przy pomocy tego rekordu.
- **rekord SOA -** rekord adresu startowego uwierzytelnienia (ang. start of authority record) ustala serwer DNS dostarczający autorytatywne informacje o domenie internetowej.
- **rekord SRV -** rekord usługi (ang. service record) pozwala na zawarcie dodatkowych informacji dotyczacych lokalizacji danej usługi, która udostepnia serwer wskazywany przez adres DNS.
- **rekord TXT** - rekord ten pozwala dołączyć dowolny tekst do rekordu DNS. Rekord ten może być użyty np. do implementacji specyfikacji Sender Policy Framework.
- inne typy rekordów dostarczają informacje o położeniu hosta (np. rekord LOC) lub o danych eksperymentalnych.

Serwery podstawowe powinny zawierać strefy wyszukiwania do przodu oraz strefy wyszukiwania wstecznego dla danej domeny. Wyszukiwanie do przodu umożliwia zmianę nazw domen na adresy IP. Wyszukiwanie wsteczne pozwala potwierdzić zapytania DNS poprzez znalezienie nazw odpowiadających podanym adresom IP.

3. Instalacja i uruchomienie serwera DNS – Bind

Aby zainstalować serwer Bind należy użyć polecenia:

apt-get install bind9

Aby uruchomić serwer DNS w Ubuntu Linux można skorzystać ze skryptu startowego:

service bind9 start

Restart serwera wykonuje sie analogicznie:

service bind9 restart

Polecenie to jest bardzo istotne, gdyż po każdej zmianie konfiguracji należy dokonać restartu serwera.

Działanie serwera kończy polecenie:

service bind9 stop

Aby sprawdzić, czy serwer uruchomił się poprawnie (lub zrestartował) należy odczytać ostatnie wpisy z logu systemowego. Można to zrobić poleceniem:

tail /var/log/syslog

4. Konfiguracja serwera Bind

4.1. Plik konfiguracji named.conf

Zanim przystąpimy do konfiguracji własnej domeny przyjrzyjmy się domyślnemu plikowi konfiguracyjnemu /etc/bind/named.conf. Ma on postać (po usunięciu komentarzy):

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

Jak widać, konfiguracja serwera DNS bazuje na trzech plikach:

/etc/bind/named.conf.options - zawierającego ustawienia konfiguracyjne serwera

/etc/bind/named.conf.local - zawierającego deklaracje stref

/etc/bind/named.conf.default-zones - zawierającego deklaracje domyślnych stref oraz odwołanie do listy 13 głównych serwerów DNS odpowiedzialnych za obsługę domen najwyższego poziomu

4.2. Plik konfiguracji named.conf.options

```
options {
 directory "/var/bind";
 listen-on-v6 { none; };
 listen-on { 127.0.0.1; };
 pid-file "/var/run/named/named.pid";
 forwarders {
        234.234.12.12;
        123.213.14.14;
};
};
```

W pierwszej linii określony jest roboczy katalog serwera named. Kolejne dwie linie mówią pod jakimi adresami dostępny będzie serwer (pierwsza dotyczy adresowania IPv6, które jest wyłączone). Znak ; (średnik) na końcu pełni rolę ogranicznika dla poszczególnych opcji umieszczonych w sekcji. Przyczyną ewentualnych błędów często jest brak średnika w odpowiednim miejscu. W przypadku pracy serwera Bind w trybie cache, opcja forwarders umożliwia wskazanie serwerów DNS, z których nasz serwer będzie pobierał translacje nieznanych nazw domenowych.

4.3. Plik konfiguracji named.conf.default-zones

```
zone "." {
   type hint;
   file "/etc/bind/db.root";
};
zone "localhost" {
   type master;
   file "/etc/bind/db.local";
};
```

```
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

Jak widać poszczególne wpisy w tym pliku podzielone są na sekcje. Początek i koniec każdej sekcji wyznaczają klamry. Znak ; (średnik) na końcu pełni dwie role: pierwsza rola to ogranicznik dla poszczególnych opcji umieszczonych w sekcji, a druga to ogranicznik dla całej sekcji. Przyczyną ewentualnych błędów często jest właśnie brak średnika w odpowiednim miejscu.

Kolejne sekcje zawierają definicję obsługiwanych stref. Pierwsza nakazuje serwerowi, w przypadku otrzymania zapytania nie objętego innymi definicjami, wykorzystanie pliku /etc/bind/db.root. Plik ten zawiera definicje głównych serwerów DNS, stanowiących początek światowego systemu nazw. Dzięki temu wpisowi nasz serwer DNS jest w stanie odnaleźć adres dowolnego hosta w internecie. Kolejne dwie sekcje definiują strefy wyszukiwania adresów oraz wyszukiwania wstecznego dla sieci zwrotnej (localhost, 127.x.x.x).

4.4 Plik konfiguracji named.conf.local

W pliku tym należy umieszczać deklaracje lokalnych stref. Pojedynczy wpis strefy określa zazwyczaj:

- nazwę strefy
- klasę strefy
- type - rodzaj strefy (master - główna; slave - pomocnicza)
- file - plik, w którym przechowywana jest definicja strefy
- allow-update - listę serwerów, które mogą aktualizować definicję strefy
- notify - możliwość powiadamiania innych serwerów o zmianach definicji strefy

Uwaga: W pakiecie bind bezwzględne nazwy stref kończą się kropką np.: "www.wp.pl." (kropka po nazwie domeny!!!).

Znając te informacje możemy przygotować sekcję dla domeny "nasza domena":

```
zone "nasza.domena" {
 type master;
 file "/etc/bind/db.nasza.domena";
 allow-update { none; };
 notify no;
 forwarders { };
};
```

4.5. Pliki konfiguracji stref

W systemie Ubuntu Linux pliki stref znajdują się w katalogu /etc/bind. Nazwy plików stref rozpoczynają się ciągiem db.* (aczkolwiek jest to tylko umowa - nazwę definiuje plik konfiguracji serwera).
Na początek przyjrzyjmy się domyślnemu plikowi db.local:

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

Na tej podstawie możemy przygotować plik dla naszej domeny db.domena.zone:

```
$TTL 86400
```

```
@     IN     SOA     ns1.nasza.domena. root.nasza.domena. (
      2010082000 ; serial
      28800      ; refresh
      14400      ; retry
      604800     ; expire
      86400      ; TTL
      )
@           IN     NS     ns1.nasza.domena.
@           IN     NS     ns2.nasza.domena.

ns1.nasza.domena.       IN     A      192.168.1.1
ns2.nasza.domena.       IN     A      192.168.1.24
test1.nasza.domena.     IN     A      192.168.1.8

mail.nasza.domena. IN CNAME test1.nasza.domena.
```

Pierwsza linia pliku (TTL) określa domyślny czas ważności informacji. Wartość podaje się w sekundach, ale dopuszczalny jest zapis uproszczony: xxH - liczba godzin, xxD - liczba dni, xxW - liczba tygodni.

Pierwszy wpis dotyczy definicji strefy - Rekord SOA (Start Of Authorihy). Definicja SOA zawarta jest pomiędzy ( ). Bardzo ważne jest, aby pamiętać o poprawnym zamknięciu tych nawiasów. Jeśli o tym zapomnimy pozostałe wpisy zostaną zinterpretowane jako rekord SOA. Wpis ma następujące składniki:

- @ - nazwa domeny, dla której jesteśmy serwerem. W tym przypadku jest to główna domena strefy - o nazwie strefy. Oznaczono to znakiem „@. W przypadku innej domeny należy tu podać bezwzględna jej nazwę np.: „domena.pl.. Proszę zwrócić uwagę na kropkę kończącą nazwę!
- IN - klasa rekordu (podana wartość dla sieci TCP/IP)
- SOA - typ rekordu
- ns1.nasza.domena. - nazwa podstawowego serwera DNS dla domeny
- root.nasza.domena. - adres kontaktowy email do osoby odpowiedzialnej za strefę (pierwsza kropkę należy traktować jako znak @ (at), czyli root@nasza.domena)

- Serial - wartość dla zapasowego serwera DNS. Przy każdej zmianie w strefie w serwerze podstawowym należy zwiększać tę wartość, gdyż sprawdzając aktualność swoich danych serwer podstawowy porównuje numer, którym obecnie dysponuje z numerem, który właśnie pobrał. W momencie, gdy pobrany numer jest większy zostaje rozpoczęty transfer całej strefy. Przyjmuje się, iż najlepszy format numeru seryjnego to taki, jaki podano w przykładzie YYYYMMDDNN, gdzie YYYY - rok, MM - miesiąc, DD - dzień, NN - numer modyfikacji danego dnia.
- Refresh - informacja dla serwera zapasowego co jaki czas ma sprawdzać aktualność swoich danych strefowych
- Retry - jeżeli nie udało się połączyć z serwerem podstawowym po upływie czasu odświeżania (np. awaria łącza w sieci, w której pracuje serwer podstawowy), to w tym polu znajduje się informacja dla serwera zapasowego co ile ma ponawiać próbę nawiązania połączenia
- Expire - czas, po jakim serwer zapasowy uzna dane w strefie za nie aktualne, jeżeli nie zdoła się połączyć z serwerem podstawowym po okresie czasu zdefiniowanym w polu RETRY
- Minimum - jest to czas, przez jaki serwery będą przechowywały wszelkie negatywne odpowiedzi.

Parametry Refresh, Retry, Expire oraz Minimum można również podać w wersji uproszczonej (xH - liczba godzin, xxD - liczba dni, xxW - liczba tygodni). Starsze implementacje aplikacji bind mogą nie obsługiwać zapisu uproszczonego. Znak ; (średnik) oznacza komentarz.

Składnia dalszej części pliku stref ma stałą postać. Każdy wpis ma następująca składnię:
nazwa_domenowa [ttl] [klasa] typ_rekordu dane_rekordu
Pod rekordem SOA należy zdefiniować, które serwery DNS będą obsługiwały nasz domenę. Należy tutaj pamiętać o umieszczeniu kropki na końcu. Pominięcie kropki spowoduje, że bind dopisze na końcu nazwę domeny. W naszym przykładzie, pominięcie kropki po ns1.nasza.domena' spowodowałoby, że bind zrobiłby wpis ns1.nasza.domena.nasza.domena.

Aby zdefiniować adresu serwerów DNS dla naszej domeny należy posłużyć się wpisami typu IN NS.

```
@       IN    NS    ns1.nasza.domena
```

Jeżeli obie nazwy dotyczą komputerów, które wcześniej nie pełniły roli serwerów DNS, należy dodać wpisy takie jak poniżej:

ns1.nasza.domena. *IN* *A* *192.168.1.1*

ns2.nasza.domena. *IN* *A* *192.168.1.24*

Wpis ns1 wskazuje na adres serwera DNS, który aktualnie konfigurujemy, natomiast ns2 powinien wskazywać na podrzędny (secondary) serwer DNS. Zrobiliśmy to posługując się wpisami typu IN A. Należy pamiętać o umieszczeniu kropki na końcu.

Oznaczenia typów to:

- A - rekord ten wiąże adres IP z nazwa hosta. Może istnieć tylko jeden rekord dla danego hosta, ponieważ nazwa ta jest uznawana za kanoniczną (oficjalną). Reszta nazw tego hosta musi zostać zdefiniowana jako alias za pomocą rekordu CNAME. Pole dane_rekordu powinno zawierać adres IP w notacji kropkowej.
- CNAME - rekord ten odwzorowuje alias na kanoniczną nazwę hosta. Dzięki temu rekordowi możliwe jest utworzenie wielu nazw tego samego hosta. Pole dane_rekordu powinno zawierać kanoniczna nazwę hosta. Niektórzy administratorzy zalecają, ze względów bezpieczeństwa, zastępowanie tego wpisu, wpisem A.
- NS - rekordy te określają wszystkie serwery (master i slave) dla danej domeny. Pole dane_rekordu powinno zawierać kanoniczną nazwę hosta, który jest serwerem strefy.

Plik dla własnej domeny mógłby mieć postać (używając nazw bezwzględnych):

```
$ttl 3h
;poczatek rekordu SOA
grupa1.kis. IN SOA ns1.grupa1.kis. hostmaster.grupa1.kis. (
        2006032601
        3H
        15M
        1W
        1D )
;Serwery nazw dla domeny grupa1.kis
grupa1.kis. IN NS ns1.grupa1.kis.
```

```
;Rekordy zasobów strefy grupa1.kis
test1.grupa1.kis. IN A 10.1.1.2
test2.grupa1.kis. IN A 10.1.1.4
test3.grupa1.kis. IN A 10.1.1.8

;Definicje aliasów
mail.grupa1.kis. IN CNAME test1.grupa1.kis.
ns1.grupa1.kis. IN CNAME test1.grupa1.kis.
```

lub stosując nazwy względne:

```
$ttl 3h
;poczatek rekordu SOA
@ IN SOA ns1.grupa1.kis. hostmaster.grupa1.kis. (
        2006032601
        3H
        15M
        1W
        1D )

;Serwery nazw dla domeny sso.pl
IN NS ns1

;Rekordy zasobów strefy grupa1.kis
test1 IN A 10.1.1.2
test2 IN A 10.1.1.4
test3 IN A 10.1.1.8

;Definicje aliasów
mail IN CNAME test1
ns1 IN CNAME test1
```

4.6. Pliki konfiguracji stref wyszukiwania wstecznego

Wyszukiwanie wsteczne często traktowane jest jako "niekonieczny dodatek". Rzeczywiście, brak wstecznego wyszukiwania nie powoduje łatwych do zauważenia problemów. Niestety okazuje się, że wiele współczesnych serwisów (www, mail, irc, itd.) dokonuje weryfikacji nazwy domenowej hosta. Zatem brak wstecznego wyszukiwania może powodować sporadyczne, lecz trudne do wykrycia problemy.

Niestety bind został zaprojektowany do pracy z klasowym przydziałem adresów (z dokładnością do oktetu). Konfiguracja serwera wyszukiwania wstecznego dla masek nie będących wielokrotnością ósemki jest skomplikowana i bardzo pracochłonna. Ta instrukcja pokazuje tylko zarys konfiguracji strefy wstecznego wyszukiwania. Mechanizm wstecznego wyszukiwania działa analogiczne do wyszukiwania adresów. Adres IP hosta (np. a.b.c.d) zostaje przedstawiony w postaci d.c.b.a.in-addr.arpa. (kropka na końcu). Zatem zostaje dopasowany do struktury nazw DNS. Domyślną strefą wyszukiwania wstecznego w Ubuntu Linux jest strefa 127.in-addr.arpa. (kropka na końcu). Jej plik konfiguracyjny ma postać:

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                                1         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

Jak widać struktura pliku jest identyczna jak w przypadku pliku strefy wyszukiwania do przodu. Jedyną różnicą jest zastąpienie wpisu "A" wpisem "PTR".

Przykładowy plik strefy wyszukiwania wstecznego może mieć postać:

```
$ttl 3h ;domyslny ttl dla strefy
```

;rekord SOA

1.1.10.in-addr.arpa. IN SOA ns1.grupa1.kis. hostmaster.grupa1.kis. (

02030202

3h

1h

1w

1h);koniec rekordu SOA

;Serwer dla strefy 0.168.192.in-addr.arpa.

1.1.10.in-addr.arpa. IN NS test1.grupa1.kis.

;Rekordy zasobów

2.1.1.10.in-addr.arpa. IN PTR test1.grupa1.kis.

4.1.1.10.in-addr.arpa. IN PTR test2.grupa1.kis.

8.1.1.10.in-addr.arpa. IN PTR test3.grupa1.kis.

5. Narzędzia DNS w systemie Linux

5.1. nslookup

Program jest najstarszym narzędziem pozwalającym na testowanie serwerów DNS. Przeznaczony jest głównie do pracy w trybie interaktywnym, niemniej jednak pozwala wykonać większość operacji po uruchomianiu z linii poleceń. Składnia jest następująca:

nslookup [-option...] [host | -] [serwer]

gdzie:

- -options - pozwala na wykonanie dowolnych poleceń.
- host - nazwa hosta o który pytamy. Zastąpienie nazwy znakiem „-" powoduje odpytanie server nazw.
- server - adres pytanego serwera nazw.

Po uruchomieniu bez parametrów przechodzi w tryb interaktywny. Najważniejsze z poleceń dostępnych tym trybie to:

- host [server] - pobiera informacje o nazwie używając aktualnego serwera lub innego, jeśli go podano

- server domain - określa domyślny serwer. Od tej chwili będą kierowane do niego zapytania
- lserver domain - podobnie jak powyżej, lecz korzysta z serwera początkowego zamiast domyślnego
- set - pozwala na ustawienie parametrów (wybrane):
    - class=value - określa klasę rekordów:
        - IN - Internet
        - CH - Chaos (sieć z początków rozwoju ARPANETu)
        - HS - Hesiod (j.w.)
        - ANY - wszystkie
    - querytype=value - określa jakie rekordy mają byś wyświetlane (ANY, NS, A,...)
    - [no]debug - powoduje wyświetlanie większej liczby informacji o procesie zapytań
    - i inne...

Polecenie jest obecnie rzadko używane. Zaleca się używanie polecenia host

5.2. Host

Host wyszukuje informacje o hostach w Internecie. Pobiera te informacje z sieci połączonych ze sobą serwerów, które są rozrzucone po całym kraju. Standardowo przekształca on nazwy hostów w adresy internetowe. Składnia polecenia jest następująca:

host [-opcje] [-c class] [-N ndots] [-t type] [-W timeout] [-R retries] hostname [server]

- hostname - określa nazwę lub adres, o których chcemy uzyskać informacje
- server - określa pytany serwer
- -c class - określa klasę rekordu (ANY, IN, CH, HS)
- -t type - określa jakie rekordy mają byś wyświetlane (ANY, NS, A,...)
- -W timeout - określa czas oczekiwania na odpowiedź
- -R retries - określa liczbę prób
- -opcje (wybrane)
    - -a - pobiera wszystkie informacje (-v -t *)
    - -r - blokuje odpytywanie rekursywne

- -v - włącza szczegółowe informacje
- inne

5.3. Dig

Program jest zaawansowanym narzędziem odpytującym serwery DNS. Pracuje podobnie jak uruchamiany z linii poleceń. Pozwala na zadanie wielu zapytań w tym samym czasie. Składnia programu jest następująca (wybrane parametry):

dig [@global-server] [domain] [q-type] [q-class] {q-opt} {global d-opts} host [@local-server] {local d-opts} [host[@local-server] {local-d-opt} [...]]

- @global-server & @local-server - odpytywane serwery
- domain - nazwa domeny
- q-class - określa klasę (in,hs,ch,...; domyślnie: in)
- q-type - określa rodzaj rekordu (a,any,mx,ns,soa,hinfo,axfr,txt,...; domyślnie:a)
- q-opt - lista parametrów określających zawartość zapytania (wybrane):
  - -f filename - plik z listą zapytań
  - -p port - port serwera
  - -t type - rodzaj rekordu
  - -c class - klasa rekordu
- d-opt - lista parametrów określających działanie programu (wybrane):
  - +time=czas - czas oczekiwania na odpowiedź
  - +[no]search - ignoruje kolejność poszukiwań (resolv.conf)
  - +[no]recurse - wyłącza tryb rekursywnego odpytywania
  - +[no]trace - śledzi kolejne delegacje, zaczynając od roota („.")
- global d-opts & servers - parametry dotyczące wszystkich zapytań
- local d-opts & servers - parametry dotyczące następnego zapytania

6. Budowanie struktury DNS

6.1. Konfiguracja serwera pomocniczego

Konfiguracja serwera pomocniczego jest znacznie prostsza od konfiguracji serwera głównego. Niezbędny jest tylko jeden wpis do pliku /etc/bind/named.conf.local:

```
zone "sso.pl" {
  type slave;
  masters { 10.1.1.2; };
  file "/var/cache/bind/db.sso.pl";
};
```

Należy pamiętać o umożliwieniu transferu danych strefy z serwera głównego do pomocniczego. W tym celu na serwerze głównym w pliku /etc/bind/named.conf.local należy użyć opcji allow-transfer { adres_IP_serwera_pomocniczego; };

Kopiowanie zawartości strefy powinno następować automatycznie. W przypadku stosowania serwera pomocniczego należy pamiętać o modyfikacji pola Serial w definicji strefy na serwerze głównym. Należy inkrementować tą wartość przy każdej modyfikacji definicji strefy.

6.2. Delegacja poddomeny DNS

Delegacja domeny polega na przekazaniu "odpowiedzialności" za cześć domeny innemu serwerowi DNS. Konfiguracja delegacji w systemie bind nie powinna przysporzyć problemów. Serwer delegujący powinien mieć dodane wpisy określające serwery nazw odpowiedzialne z obsługę poddomeny. Poniżej znajdują się przykładowe wpisy:

```
poddomena.grupa1.kis. IN NS ns1.instytucja_a.pl.
poddomena.grupa1.kis. IN NS ns2.instytucja_b.pl.
```

W momencie gdy do serwera przyjdzie zapytanie dotyczące hosta o domenie poddomena.sso.pl, zostanie ono przekierowane do jednego z serwerów utrzymujących tą domenę. Proszę zwrócić uwagę, że serwery nazw znajdują się poza domeną. W przypadku gdy serwer nazw znajduje się w poddomenie, niezbędne jest zupełnie pliku rekordami typu „A:

poddomena.grupa1.kis. IN NS ns1.poddomena.grupa1.kis.
poddomena.grupa1.kis. IN NS ns2.poddomena.grupa1.kis.
ns1.poddomena.grupa1.kis. IN A 10.1.1.21
ns2.poddomena.grupa1.kis. IN A 10.1.1.22

Dwa rekordy A noszą nazwę rekordów spajających (glue records). Dlaczego są konieczne? Otóż odpowiedź jest następująca: serwer szukający nazwy w domenie poddomena.sso.pl najpierw odpytałby nasz serwer o rekordy NS dla tej strefy. Nasz serwer oczywiście udzieliłby odpowiedzi podając ns1.poddomena.sso.pl oraz ns2.poddomena.sso.pl. Problem w tym, że nazwy te znajdują się w strefie, o którą zdalny serwer pytał, co oznacza, że nie ma możliwości poznania ich adresów IP... Gdyby nie rekordy klejące, tak właśnie by było. Dzięki nim nasz serwer DNS zna adresy IP serwerów, do których oddelegowano poddomenę i to właśnie je zwraca pytającemu.
Konfiguracja serwera utrzymującego poddomenę jest analogiczna od konfiguracji serwera nadrzędnego. Uwaga: Proszę pamiętać, że serwer poddomeny musi odpowiadać na adresie karty sieciowej - należy ustawić odpowiednie opcje.

6.3. Współpraca z DNS w Windows Server

System DNS jest kompatybilny we wszystkich systemach operacyjnych. Istniej możliwość delegowania stref zarówno do systemów uniksowych z systemów Windows jak i odwrotnie. Także serwery Windows mogą funkcjonować jako serwery pomocnicze dla serwerów w systemach Unix.

7. Zadania

1. Na pierwszym komputerze z systemem Linux uruchom główny serwer domeny DNS grupaX.iis.
2. Dodaj do domeny kilka hostów (np.: host1.grupaX.iis, host2.grupaX.iis) - sprawdź poleceniem host i ping czy działa poprawnie
3. Skonfiguruj na głównym serwerze DNS strefę wyszukiwania wstecznego (podsieć 192.168.30.0).
4. Na drugim komputerze z systemem Linux uruchom pomocniczy serwer DNS.

5. Dołącz do sieci wewnętrznej VirtualBox o nazwie lanlin drugi z serwerów Windows (zadbaj o wyłączenie usług uruchomionych na Windows Server, które mogą zakłócić pracę sieci lanlin).
6. Dokonaj delegacji strefy z głównego serwera DNS w systemie Linux do serwera Windows (np. strefy poddomena.grupaX.iis). Wskazówka: nie zapomnij o wyłączeniu forwardowania stref, dla których serwer główny DNS jest autorytatywny (w pliku named.conf.local).