Instytut Teleinformatyki
Wydział Fizyki, Matematyki i Informatyki
Politechnika Krakowska

Laboratorium Administrowania Systemami Komputerowymi

„Usługi nazw domenowych DNS”

ćwiczenie numer: 4

Spis treści

INSTYTUT TELEINFORMATYKI....1
SPIS TREŚCI....2
1. WSTĘPNE INFORMACJE....3
Temat ćwiczenia....4
Zagadnienia do przygotowania....4
Cel ćwiczenia....4
Wymagany sprzęt oraz oprogramowanie....5
2. PRZEBIEG ĆWICZENIA....11
Przygotowanie ćwiczenia....12
Zadanie nr 1 - Rejestrowanie zdarzeń....14
Zadanie nr 2 - Serwer nazw z pamięcią podręczną....15
Zadanie nr 3 - Konfiguracja serwera nadrzędnego dla strefy iti.pk....17
Zadanie nr 4 - Konfiguracja serwera nadrzędnego dla strefy 112.168.192.in-addr.arpa...21
Zadanie nr 5 - Konfiguracja serwera podrzędnego....23
Zadanie nr 6 - Transfer stref....25
Zadanie nr 7 - Dynamiczna aktualizacja....27
Zakończenie ćwiczenia....29
Opracowanie ćwiczenia i sprawozdanie....30

1. Wstępne informacje

TEMAT ĆWICZENIA

Tematem ćwiczenia jest udostępnianie nazw domenowych DNS. DNS (ang. *Domain Name Service)* jest jedną z najważniejszych usług Internetowych. Podstawową funkcjonalność DNS stanowi mechanizm translacji adresów w postaci kanonicznej do postaci kropkowo – dziesiętnej.

ZAGADNIENIA DO PRZYGOTOWANIA

Przed przystąpieniem do ćwiczenia należy zapoznać się z następującymi zagadnieniami:

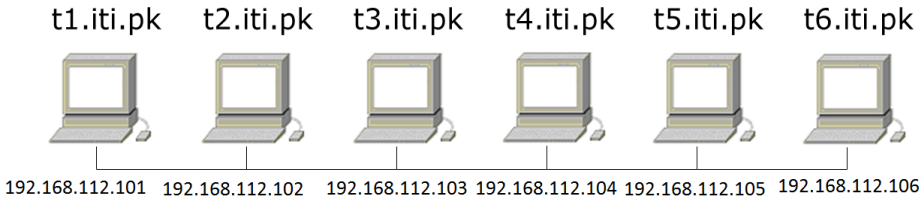
- Architektura mechanizmu DNS;
- Konfiguracja oprogramowania DNS dla systemu Linux RedHat

Większość informacji zawartych w tym ćwiczeniu została zasięgnięta z książki:

- "DNS i BIND" autorzy: Paul Albitz i Cricket Liu, wyd. O'Reilly
- w sieci istnieje wiele linków, które opisują system DNS

CEL ĆWICZENIA

Celem ćwiczenia jest skonfigurowanie serwerów nazw dla niewielkiej sieci przedstawionej na poniższym rysunku.



Komputery znajdują się w sieci 192.168.112.0, ich domeną jest iti.pk. Serwery nazw działają na komputerze „t5". Wymiennikami poczty dla iti.pk są hosty t1.iti.pk oraz t2.iti.pk.

WYMAGANY SPRZĘT ORAZ OPROGRAMOWANIE

Do wykonania ćwiczenia niezbędny jest komputer z systemem operacyjnym Linux z zainstalowanym pakietami: **bind9, dnsutils**, oraz skrypt **lab-dns**.

Wybrane informacje o oprogramowaniu wykorzystywanym w ćwiczeniu

Implementacja **BIND**

BIND (Berkeley Internet Name Domain) początkowo został napisany dla systemu operacyjnego Unix 4.3 BSD. Obecnie jest najpopularniejszą implementacja DNS. Został przeniesiony do większości odmian Unixa i jest dostarczany jako standardowa część dystrybucji tego systemu operacyjnego.

Aby uruchomić serwer nazw wystarczy użyć polecenia:

```
# /usr/sbin/named
```

named może być uruchomiony z różnymi parametrami, oto niektóre z nich:

Nazwa	Opis
`-c plik_konfiguracyjny`	zamiast /etc/bind/named.conf zostanie użyty plik_konfiguracyjny
`-t katalog`	named zostanie “uwięziony” w katalogu katalog
`-u użytkownik`	named będzie działał z prawami użytkownika

Plik konfiguracyjny

Plikiem konfiguracyjnym, z którego domyślnie korzysta named jest **/etc/bind/named.conf**. Składnia tego pliku przypomina język C, każda instrukcja i podinstrukcja kończy się średnikiem. Dozwolone są trzy rodzaje komentarzy:

```
# w stylu powłoki
/* w stylu C */
// w stylu C++
```

Przykładowy plik named.conf:

```
options {

        directory "/var/named";
        listen-on port 53 {127.0.0.1;};
        transfer-source 127.0.0.1;
        allow-transfer {192.168.112.105;};
};

zone "iti.pk" {
        type master;
        file "iti.pk";
        allow-update {127.0.0.1;};
};

zone "112.168.192.in-addr.arpa" {
        type slave;
        masters {192.168.112.105;};
         File "112.168.192";
};

include \"/etc/bind/rndc.key\";

controls{
         inet 127.0.0.1 port 953 allow {127.0.0.1;}
         keys{rndc-key;};
};
```

Instrukcja **`options`** konfiguruje opcje globalne:

Nazwa	Opis
`directory "/var/named"`	definiuje katalog zawierający pliki danych strefowych
`listen-on port 53 {127.0.0.1;}`	określa adres IP oraz port, na którym serwer nazw będzie oczekiwał na zapytania
`transfer-source 127.0.0.1`	określa adres IP, który będzie używany jako źródłowy podczas transferów stref
`allow-transfer {192.168.112.105;}`	transfery stref są dozwolone tylko z adresu 192.168.112.105

Instrukcja **zone** konfiguruje strefy obsługiwane przez serwer:

Nazwa	Opis
`"iti.pk"`	nazwa domenowa
`type master`	serwer nazw jest serwerem nadrzędnym dla tej strefy
`file "iti.pk"`	nazwa pliku w którym przechowywane są dane o strefie
`allow-update {127.0.0.1;}`	dynamiczna aktualizacja dla tej strefy dozwolona jest tylko z adresu 127.0.0.1
`"112.168.192.in-addr.arpa"`	nazwa domenowa
`type slave`	serwer nazw jest serwerem podrzędnym dla tej strefy
`masters {192.168.112.105;}`	adresy serwerów z których będą pobierane dane o strefie
`file "112.168.192"`	nazwa pliku, w którym będą przechowywane dane o strefie

Linia **`include \"/etc/bind/rndc.key\";`** załącza plik z kluczami pozwalającymi na dostęp zdalny do serwera nazw.

Plik rndc.key jest generowany dla naszego serwera DNS poleceniem

```
# rndc-confgen -a -u bind -t /lab-dns/dns1
```


Nazwa	Opis
`-a`	tworzenie pliku z kluczem dla serwera DNS w zmienionym katalogu roota
`-t katalog`	Katalog domowy serwera DNS, dla którego generujemy pliki
`-u użytkownik`	użytkownik, dla którego generujemy klucz

Instrukcja **`controls`** konfiguruje dostęp zdalny do naszego serwera:

Nazwa	Opis
inet 127.0.0.1 port 953	adres oraz port, na którym nasłuchiwane będą połączenia zdalne do serwera nazw
allow {127.0.0.1;}	adres, z którego akceptowane będą połączenia zdalne
keys{rndc-key;};	nazwa klucza potrzebnego do autoryzacji połączenia zdalnego

Pliki danych strefowych

Każdy rekord zapisany w pliku danych strefowych ma następujący format:


```
nazwa TTL klasa typ dane
```

Nazwa	Opis
nazwa	zawiera nazwę domenową, do której odnosi się wpis. Pole nazwy może być puste wtedy za nazwę domenową przyjmuje się domyślnie nazwę z poprzedniej pozycji. Nazwy domenowe zakończone kropką są nazywane bezwzględnymi i uważane za kompletne. Nazwy domenowe nie zakończone kropką są nazywane względnymi, rzeczywista nazwa domenowa jest złożeniem nazwy względnej oraz źródła
TTL	Time To Live - czas życia. Czas, przez który serwery mogą buforować dane. Jeśli zostawi się to pole puste, zostanie przyjęty domyślny TTL (ustawiony instrukcją $TTL na początku pliku)
klasa	pole określa klasę adresową. Zdefiniowane są klasy: IN – klasa Internet CS – klasa CSNET CH – klasa CHAOS HS – klasa Hesiod
Typ	pole to określa typ rekordu. Oto niektóre typy: A – adres CNAME – nazwa kanoniczna HINFO – informacje o hoście MX – wymiennik poczty NS – serwer nazw PTR – wskaźnik SOA – początek autorytatywnych danych TXT – tekst
Dane	zawartość tego pola zależy od typu rekordu

Przykładowy plik:

```
$TTL 1h
iti.pk.  IN  SOA  dns1.iti.pk. root.dns1.iti.pk. (
                1   ; numer seryjny
                1h  ; okres odświeżania
                1h  ; okres ponownej próby
                1d  ; czas wygasania
                1d ); czas buforowania negatywnego
iti.pk.         1h      IN NS   dns1.iti.pk.
iti.pk.         1h      IN NS   dns2.iti.pk.
dns1.iti.pk.    1h      IN A    127.0.0.1
dns2.iti.pk.    1h      IN A    192.168.112.105
t1.iti.pk.      1h      IN A    192.168.112.101
t2.iti.pk.      1h      IN A    192.168.112.102
t3.iti.pk.      1h      IN A    192.168.112.103
t4.iti.pk.      1h      IN A    192.168.112.104
t5.iti.pk.      1h      IN CNAME dns2.iti.pk.
iti.pk.         1h      IN MX  10  t1.iti.pk.
iti.pk.         1h      IN MX  20  t2.iti.pk.
```

Plik ten można również zapisać tak (korzystając ze skrótów):

```
$TTL 1h
@ SOA  dns1 root.dns1 1 1h 1h 1d 1d
        NS   dns1
        NS   dns2
dns1    A    127.0.0.1
dns2    A    192.168.112.105
t1      A    192.168.112.101
t2      A    192.168.112.102
t3      A    192.168.112.103
t4      A    192.168.112.104
t5      CNAME dns2
@       MX  10  t1
        MX  20  t2
```

Polecenie **dig**

W celu wysłania zapytania do serwera nazw można użyć programu **dig** (Domain Information Groper – Wyszukiwacz Informacji Domenowych).

Najczęściej polecenia **dig** używa się w następującej formie:

dig @serwer nazwa typ

Nazwa	Opis
serwer	nazwa lub adres IP serwera nazw, który chcemy zapytać
nazwa	nazwa hosta lub adres IP, jeśli użyto opcji -x
Typ	typ zapytania (SOA,NS,A,MX,CNAME,PTR,AXFR ...), domyślnym typem jest A

Program **nsupdate**

Program **nsupdate** wchodzący w skład standardowej dystrybucji BIND służy do dynamicznej aktualizacji. Program czyta jednowierszowe polecenia i tłumaczy je na komunikaty

aktualizacji. Polecenia można podawać ze standardowego wejścia lub pliku, którego nazwę należy podać jako argument nsupdate. Pusty wiersz powoduje wysłanie uaktualnienia.

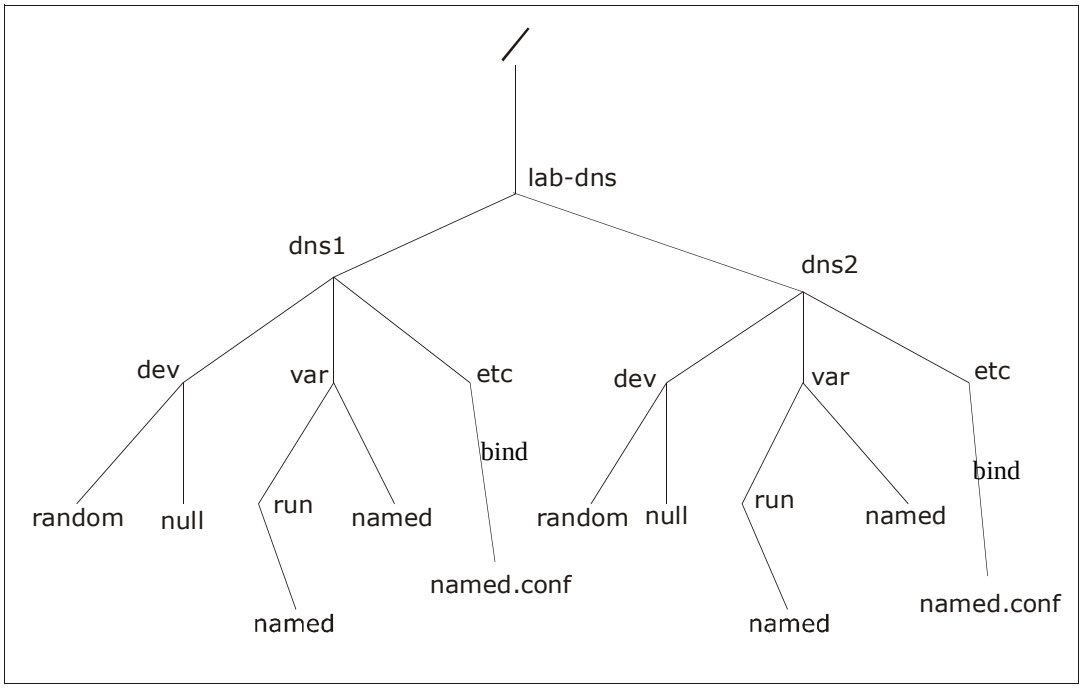
Program **nsupdate** interpretuje między innymi następujące polecenia:

Nazwa	Opis
`- prereq yxdomain nazwa_domenowa`	istnienie określonej `nazwy_domenowej` jest warunkiem aktualizacji
`- prereq nxdomain nazwa_domenowa`	brak określonej `nazwy_domenowej` jest warunkiem aktualizacji
`- update delete nazwa_domenowa`	usuwa określoną `nazwę_domenową`
`- update add nazwa_domenowa TTL klasa typ dane_rekordu`	dodaje do strefy

2. Przebieg ćwiczenia

PRZYGOTOWANIE ĆWICZENIA

Do wykonania ćwiczenia niezbędne są następujące pliki i katalogi:



Plik named.conf dla serwera DNS1 (**/lab-dns/dns1/etc/bind/named.conf**) powinien zawierać:

```
options {
        directory "/var/named";
        listen-on port 53 {127.0.0.1;};
        transfer-source 127.0.0.1;
};

include "/etc/bind/rndc.key";

controls{
       inet 127.0.0.1 port 953 allow {127.0.0.1;}
       keys{rndc-key;};
};
```

Nazwa	Opis
`directory "/var/named"`	definiuje katalog zawierający pliki danych strefowych
`listen-on port 53 {127.0.0.1;}`	określa adres IP oraz port, na którym serwer nazw będzie oczekiwał na zapytania
`transfer-source 127.0.0.1`	określa adres IP, który będzie używany jako źródłowy podczas transferów stref

Podobnie plik named.conf dla serwera DNS2 (**/lab-dns/dns2/etc/bind/named.conf**) powinien zawierać:

```
options {
        directory "/var/named";
        listen-on port 53 {192.168.112.numer_komputera;};
        transfer-source 192.168.112.numer_komputera;
};

include "/etc/bind/rndc.key";

controls{
       inet 192.168.112.numer_komputera port 953 allow
{127.0.0.1;}
       keys{rndc-key;};
};
```

Aby utworzyć niezbędną strukturę plików i katalogów wystarczy uruchomić skrypt:

```
# /root/lab-dns/lab-dns start
```

Po wykonaniu się skryptu należy zmienić w pilikach konfiguracyjnych napisy **`numer_komputera`** tak aby adres zgadzał się z adresem IP maszyny, na której pracujemy oraz należy zwracać uwagę w kolejnych zadaniach aby podczas korygowania plików konfiguracyjnych wpisywać poprawny adres swojego komputera.

Kiedy mamy już gotowe drzewo katalogów i plików zatrzymujemy działanie demona programu named oraz generujemy pliki z kluczami rndc.

```
# /etc/init.d/bind9 stop
# rndc-confgen -a -u bind -t /lab-dns/dns1
# rndc-confgen -a -u bind -t /lab-dns/dns2
```


ZADANIE NR 1 - REJESTROWANIE ZDARZEŃ

BIND jest wyposażony w system rejestracji zdarzeń. Konfiguruje się go przy użyciu instrukcji logging. W plikach konfiguracyjnych serwerów nazw (**/lab-dns/dns1/etc/bind/named.conf oraz /lab-dns/dns2/etc/bind/named.conf**) należy dopisać:

```
logging {
       channel log {
       file “file.log”;
       severity info;
       print-time yes;
       print-category yes;
       };
       category default { log; };
       category queries { log; };
       category update {log; };
};
```

instrukcja channel definiuje kanał:

Nazwa	Opis
`file “file.log”`	w pliku file.log będą zapisywane komunikaty
`severity info`	określa ważność zapisywanych komunikatów
`print-time yes`	daty będą zapisywane w komunikacie
`print-category yes`	kategorie będą zapisywane w komunikacie
`category default { log; }`	określa kanał dla kategorii default
`category queries { log; }`	określa kanał dla kategorii queries (zapytania
`category update {log; }`	określa kanał dla kategorii update (dynamiczne aktualizacje)

ZADANIE NR 2 - SERWER NAZW Z PAMIĘCIĄ PODRĘCZNĄ

Serwer nazw z pamięcią podręczną szuka odpowiedzi na zapytania o nazwy i pamięta odpowiedź, więc przy kolejnych zapytaniach o tę samą nazwę czas odpowiedzi jest znacznie krótszy.

Serwer nazw musi wiedzieć, gdzie znajdują się serwery nazw strefy głównej. Odpowiada za to wpis w named.conf:

```
zone "." {
        type hint;
        file "root";
};
```

Plik **`root`** zawiera wskazania do głównych serwerów nazw.

Ponieważ BIND9 ma wbudowaną strefę hints, nie musisz umieszczać instrukcji zone dla tej strefy w pliku named.conf.

Aby sprawdzić działanie serwera nazw z pamięcią podręczną uruchom serwery nazw DNS1 i DNS2:

```
# /usr/sbin/named -u bind -t /lab-dns/dns1
# /usr/sbin/named -u bind -t /lab-dns/dns2
```

Teraz korzystając z polecenia **`dig`** zapytaj serwer nazw o dowolny adres np.:

```
# dig @127.0.0.1 www.onet.pl
```

Zrób to jeszcze raz i porównaj czasy odpowiedzi(Query time).

Następnie obejrzyj komunikaty w pliku **/lab-dns/dns1/var/named/file.log**. Powinny tam znajdować się komunikaty podobne do tych:


```
13-Nov-2010 10:20:16.277 general: running
13-Nov-2010 10:22:55.223 queries: client 127.0.0.1#40188:
      query:      www.onet.pl IN A + (127.0.0.
13-Nov-2010 10:24:00.188 queries: client 127.0.0.1#44199:
      query:      www.onet.pl IN A + (127.0.0.1)
```

Każda linia w pliku zawiera jeden komunikat. Na początku znajduje się data oraz kategoria a następnie treść komunikatu. Pierwszy komunikat oznacza uruchomienie serwera nazw. Kolejne dwa to komunikaty dotyczące zapytań. 127.0.0.1#32780 to adres IP i port z którego nastąpiło zapytanie, natomiast www.onet.pl IN A oznacza, że pytano o adres IP hosta www.onet.pl.

Aby móc kontrolować na bieżąco zapisy dokonywane w plikach logowania możemy w osobnych terminalach wprowadzić następujące polecenie:

```
# tail -f /lab-dns/dns1/var/named/file.log
```

oraz analogiczny wpis dla drugiego serwera DNS.

ZADANIE NR 3 - KONFIGURACJA SERWERA NADRZĘDNEGO DLA STREFY ITI.PK

Załóżmy, że serwery nazw mają obsługiwać fikcyjną strefę iti.pk. Serwer DNS1 to serwer nadrzędny dla tej strefy, a serwer DNS2 podrzędny. Do pliku named.conf dla serwera DNS1 (**/lab-dns/dns1/etc/bind/named.conf**) dodaj wpis odpowiedzialny za strefę iti.pk:

```
zone "iti.pk" {
        type master;
        file "iti.pk";
};
```

Nazwa	Opis
`"iti.pk"`	nazwa strefy
`type master`	serwer nazw jest serwerem nadrzędnym dla tej strefy
`file "iti.pk"`	nazwa pliku, w którym przechowywane są dane o strefie

Następnie utwórz plik danych strefowych iti.pk:

```
# touch /lab-dns/dns1/var/named/iti.pk
```

i otwórz go używając dowolnego edytora.

Pierwszy wpis w pliku danych strefowych dotyczy domyślnego TTL dla strefy. TTL jest to "czas życia", czyli okres, przez który inne serwery mogą buforować dane. Gdy ten czas upłynie, serwer musi usunąć buforowane dane i pobrać nowe z autorytatywnego źródła. Domyślny TTL ustawia się za pomocą instrukcji $TTL. Aby ustawić domyślny TTL na 1 godzinę wystarczy na początku pliku dodać instrukcje:

```
$TTL 1h
```

Drugim wpisem jest rekord SOA (Start Of Authority – początek autorytatywnych danych), który wskazuje na zwierzchność nad strefą. Rekord SOA dla strefy iti.pk wygląda tak:


```
iti.pk.  IN  SOA  dns1.iti.pk. root.dns1.iti.pk. (
            1     ; numer seryjny
            1h    ; okres odświeżania
            1h    ; okres ponownej próby
            1d    ; czas wygasania
            1d )  ; czas buforowania negatywnego
```

Nazwa	Opis
"iti.pk"	nazwa strefy
IN	klasa danych, jest to skrót od Internetu
SOA	typ rekordu (Start Of Authority – początek autorytatywnych danych)
dns1.iti.pk.	nazwa podstawowego nadrzędnego serwera nazw dla strefy iti.pk
root.dns1.iti.pk.	adres e-mail osoby odpowiedzialnej za strefę (“@” zastąpiono “.”)

Dane w nawiasie związane są z serwerem podrzędnym:

Nazwa	Opis
numer seryjny	numer ten należy zwiększać po każdej modyfikacji pliku strefy, ponieważ serwer podrzędny próbując pobrać dane strefowe najpierw sprawdza numer seryjny i pobiera nową kopie strefy tylko wtedy, gdy numer strefy w serwerze podrzędnym jest mniejszy niż w nadrzędnym
okres odświeżania	określa jak często serwer podrzędny powinien sprawdzać, czy dane strefowe są aktualne(1h – oznacza 1 godzinę, 3d4h30m – oznacza 3 dni, 4 godziny i 30 minut)
okres ponownej próby	jest to czas, po którym serwer spróbuje się ponownie połączyć z serwerem nadrzędnym, gdy nie udało się z nim skontaktować po upływie okresu odświeżania
Czas wygasania	po jego upływie serwer podrzędny uznaje strefę za wygasłą i przestaje udzielać odpowiedzi na zapytania, które jej dotyczą
Czas buforowania negatywnego	przez ten czas serwery mogą buforować odpowiedzi negatywne

Następne wpisy to rekordy NS, dotyczące serwerów nazw. Każdy autorytatywny dla strefy iti.pk serwer nazw będzie miał jeden taki rekord:

```
iti.pk.          1h      IN NS   dns1.iti.pk.
iti.pk.          1h      IN NS   dns2.iti.pk.
```

Nazwa	Opis
`iti.pk.`	nazwa strefy
`1h`	TTL
`IN`	klasa danych
`NS`	typ rekordu (Name Server – serwer nazw)
`dns1.iti.pk.`	nazwa hosta, na którym działa serwer nazw

Kolejne rekordy będą dotyczyły odwzorowania nazw na adresy. Rekordem realizującym odwzorowanie nazwy na adres jest rekord A. W strefie iti.pk są następujące hosty:

```
dns1.iti.pk.     1h      IN A    127.0.0.1
dns2.iti.pk.     1h      IN A    192.168.112. numer_komputera
t1.iti.pk.       1h      IN A    192.168.112.101
t2.iti.pk.       1h      IN A    192.168.112.102
t3.iti.pk.       1h      IN A    192.168.112.103
t4.iti.pk.       1h      IN A    192.168.112.104
```

Do tworzenia aliasów służy rekord CNAME (Canonical Name), który odwzorowuje alias na nazwę kanoniczną :

```
t5.iti.pk.       1h      IN CNAME dns2.iti.pk.
```

Do realizacji trasowania poczty DNS używa rekordu zasobu MX (Mail Exchanger – wymiennik poczty). Rekord ten określa wymiennik poczty dla danej domeny. Oprócz

nazwy domenowej rekord MX ma dodatkowy parametr, nazywany wartością preferencji, który określa priorytet wymiennika poczty. Program pocztowy próbuje skontaktować się z wymiennikiem poczty o najmniejszej wartości preferencji. Dla strefy iti.pk mamy dwa wymienniki poczty:

```
iti.pk.      IN  MX  10  t1.iti.pk.
iti.pk.      IN  MX  20  t2.iti.pk.
```

Po utworzeniu pliku z danymi strefy konieczne jest przeładowanie serwerów nazw. Wydaj polecenia:

```
# kill -HUP `cat /lab-dns/dns1/var/run/named/named.pid`
# kill -HUP `cat /lab-dns/dns2/var/run/named/named.pid`
```

lub skorzystaj ze skryptu:

```
# /root/lab-dns/lab-dns reload
```

Korzystając z polecenia dig sprawdź poprawność powyższej konfiguracji:

```
# dig @127.0.0.1 t1.iti.pk
# dig @127.0.0.1 t5.iti.pk
# dig @127.0.0.1 iti.pk ns
# dig @127.0.0.1 iti.pk mx
```

W pliku **/lab-dns/dns1/var/named/file.log** powinny pojawić się nowe wpisy:

```
13-Nov-2010 10:26:11.230 general: zone iti.pk/IN: loaded
      serial 1
13-Nov-2010 10:26:11.231 notify: zone iti.pk/IN: sending
      notifies (serial 1)
13-Nov-2010 10:26:13.981 queries: client 127.0.0.1#48252:
      query: t1.iti.pk IN A + (127.0.0.1)
13-Nov-2010 10:26:19.412 queries: client 127.0.0.1#42122:
      query: t5.iti.pk IN A + (127.0.0.1)
13-Nov-2010 10:26:28.826 queries: client 127.0.0.1#43564:
      query: iti.pk IN NS + (127.0.0.1)
13-Nov-2010 10:26:32.542 queries: client 127.0.0.1#33642:
      query: iti.pk IN MX + (127.0.0.1)
```


Pierwszy wpis informuje, że została załadowana strefa iti.pk i jej numer seryjny to jeden. Drugi to informacja, że zostały wysłane powiadomienia o zmianie danych w strefie iti.pk. Kolejne to zapytania, które wysłałeś do serwera nazw przy użyciu programu **dig**.

ZADANIE NR 4 - KONFIGURACJA SERWERA NADRZĘDNEGO DLA STREFY 112.168.192.IN-ADDR.ARPA

Serwerem nadrzędnym dla strefy 112.168.192.in-addr.arpa będzie serwer DNS2. Do pliku named.conf dla serwera DNS2 (**/lab-dns/dns2/etc/bind/named.conf**)dodaj wpis odpowiedzialny za strefę 112.168.192.in-addr.arpa:

```
zone "112.168.192.in-addr.arpa" {
        type master;
        file "112.168.192";
};
```

Nazwa	Opis
`"112.168.192.in-addr.arpa"`	nazwa strefy
`type master`	serwer nazw jest serwerem nadrzędnym dla tej strefy
`file "112.168.192"`	nazwa pliku, w którym przechowywane są dane o strefie

Następnie utwórz plik danych strefowych 112.168.192:

```
# touch /lab-dns/dns2/var/named/112.168.192
```

i używając dowolnego edytora zapisz w nim:

```
$TTL 1h
112.168.192.in-addr.arpa. IN SOA  dns2.iti.pk. root.dns2.iti.pk. (
                                        1
                                        1h
                                        1h
                                        1d
                                        1d )
112.168.192.in-addr.arpa.       1h      IN NS   dns1.iti.pk.
112.168.192.in-addr.arpa.       1h      IN NS   dns2.iti.pk.
numer_komputera.112.168.192.in-addr.arpa.     1h      IN PTR  dns2.iti.pk.
101.112.168.192.in-addr.arpa.     1h      IN PTR  t1.iti.pk.
102.112.168.192.in-addr.arpa.     1h      IN PTR  t2.iti.pk.
103.112.168.192.in-addr.arpa.     1h      IN PTR  t3.iti.pk.
104.112.168.192.in-addr.arpa.     1h      IN PTR  t4.iti.pk.
```


Rekordy PTR (Pointer – wskaźnik) odwzorowują adresy na nazwy.

Po przeładowaniu serwerów nazw sprawdź poprawność powyższej konfiguracji:

```
# dig @192.168.112.numer_komputera -x 192.168.112.101
```

Obejrzyj plik **/lab-dns/dns2/var/named/file.log**. Jego zawartość powinna być podobna do pliku pokazanego w poprzednich punktach.

ZADANIE NR 5 - KONFIGURACJA SERWERA PODRZĘDNEGO

Serwer DNS2 będzie serwerem podrzędnym dla stref iti.pk a serwer DNS1 dla strefy 112.168.192.in-addr.arpa. Do pliku konfiguracyjnego (named.conf) serwera DNS2 dodaj:

```
zone "iti.pk" {
        type slave;
        masters {127.0.0.1;};
        file "iti.pk";
};
```

Nazwa	Opis
`"iti.pk"`	nazwa strefy
`type slave`	serwer nazw jest serwerem podrzędnym dla tej strefy
`masters {127.0.0.1;}`	adres IP serwera nadrzędnego dla tej strefy
`file "iti.pk"`	nazwa pliku, w którym będą przechowywane dane o strefie

Natomiast do pliku konfiguracyjnego serwera DNS1 dodaj:

```
zone "112.168.192.in-addr.arpa" {
        type slave;
        masters {192.168.112.numer_komputera;};
        file "112.168.192";
};
```

Nazwa	Opis
`"112.168.192.in-addr.arpa"`	nazwa strefy
`type slave`	serwer nazw jest serwerem podrzędnym dla tej strefy
`masters {192.168.112.numer_komputera;}`	adres IP serwera nadrzędnego dla tej strefy
`file "112.168.192"`	nazwa pliku, w którym będą przechowywane dane o strefie

Po przeładowaniu serwerów sprawdź działanie serwera podrzędnego:

```
# dig @192.168.112.numer_komputera t5.iti.pk
# dig @127.0.0.1 -x 192.168.112.101
```

W pliku **/lab-dns/dns1/var/named/file.log** powinny pojawić się wpisy:

```
13-Nov-2010 11:28:30.170 xfer-in: transfer of
      '112.168.192.in-addr.arpa/IN' from 192.168.112.5#53:
      connected using 127.0.0.1#58359
13-Nov-2010 11:28:30.171 general: zone 112.168.192.in-
      addr.arpa/IN: transferred serial 1
13-Nov-2010 11:28:30.171 xfer-in: transfer of
      '112.168.192.in-addr.arpa/IN' from 192.168.112.5#53:
      Transfer completed: 1 messages, 9 records, 255 bytes,
      0.001 secs (255000 bytes/sec)
13-Nov-2010 11:28:30.212 xfer-out: client
      192.168.112.5#39754: transfer of 'iti.pk/IN': AXFR
      started
13-Nov-2010 11:28:30.212 xfer-out: client
      192.168.112.5#39754: transfer of 'iti.pk/IN': AXFR
      ended
```

Pierwszy oznacza pobranie przez serwer nazw strefy 112.168.192.in-addr.arpa, natomiast drugi informuje, że z serwera nazw została pobrana strefa iti.pk.
Plik **/lab-dns/dns2/var/named/file.log** zawiera analogiczne wpisy.

ZADANIE NR 6 - TRANSFER STREF

Wykonaj polecenia:

```
# dig @127.0.0.1 iti.pk axfr
# dig @192.168.112.numer_komputera 112.168.192.in-addr.arpa axfr
```

W wyniku ich działania powinieneś otrzymać całą strefę iti.pk i 112.168.192.in-addr.arpa. Takie działanie serwera nazw nie jest zbyt bezpieczne, ponieważ każdy może dokonać transferu strefy. Podinstrukcja allow-transfer pozwala zapobiegać nieautoryzowanym transferom stref. Aby transferu stref mógł dokonać tylko serwer podrzędny do plików konfiguracyjnych serwerów nazw dodaj w instrukcji options następujące linie:

- dla serwera DNS1

  ```
  allow-transfer {192.168.112.numer_komputera;};
  ```

- dla serwera DNS2

  ```
  allow-transfer {127.0.0.1;};
  ```

Przeładuj serwery nazw. Teraz używając polecenia:

```
# dig @127.0.0.1 iti.pk axfr
```

nie otrzymasz transferu strefy, ponieważ transfer strefy iti.pk może być dokonany tylko z adresu 192.168.112.numer_komputera.

W pliku **/lab-dns/dns1/var/named/file.log** wyraźnie widać działanie podinstrukcji allow-transfer:

Przed dodaniem wpisu można było dokonać transferu strefy z adresu 127.0.0.1


```
13-Nov-2010 10:40:56.559 queries: client 127.0.0.1#59144:
      query: iti.pk IN AXFR -T (127.0.0.1)
13-Nov-2010 10:40:56.560 xfer-out: client 127.0.0.1#59144:
      transfer of 'iti.pk/IN': AXFR started
13-Nov-2010 10:40:56.560 xfer-out: client 127.0.0.1#59144:
      transfer of 'iti.pk/IN': AXFR ended
```

natomiast po dodaniu allow-transfer {192.168.112.numer_komputera;}; transfer nie jest już możliwy z adresu 127.0.0.1.

```
13-Nov-2010 10:48:04.829 queries: client 127.0.0.1#57100:
      query: iti.pk IN AXFR -T (127.0.0.1)
13-Nov-2010 10:48:04.829 security: client 127.0.0.1#57100:
      zone transfer 'iti.pk/AXFR/IN' denied
```


ZADANIE NR 7 - DYNAMICZNA AKTUALIZACJA

Wszystkie zmiany, jakich dokonywałeś w tym ćwiczeniu wymagały przeładowania serwera nazw. Dynamiczne aktualizacje pozwalają na aktualizacje danych strefowych podczas pracy serwera nazw. Aby zezwolić na dynamiczne aktualizacje z localhost'a dodaj w plikach konfiguracyjnych serwerów DNS1 i DNS2 następujące linie:

- w instrukcji zone “iti.pk”pliku konfiguracyjnego serwera DNS1

```
allow-update {127.0.0.1;};
```

- a w instrukcji zone “112.168.192.in-addr-arpa” pliku konfiguracyjnego serwera DNS2 :

```
allow-update {192.168.112.numer_komputera;};
```

Następnie, po przeładowaniu serwerów nazw, uruchom program nsupdate:

```
# nsupdate
> server 127.0.0.1
> prereq nxdomain t6.iti.pk.
> update add t6.iti.pk. 3600 A 192.168.112.6
>
>server 192.168.112.numer_komputera
>prereq nxdomain 6.112.168.192.in-addr.arpa.
>update add 6.112.168.192.in-addr.arpa. 3600 PTR t6.iti.pk.
>
>quit
```

Teraz poleceniem **dig** sprawdź czy dane strefowe zostały zaktualizowane:

```
# dig @127.0.0.1 t6.iti.pk.
# dig @192.168.112.numer_komputera -x 192.168.112.6
```

Zobacz także, jakie zmiany zostały wprowadzone w plikach iti.pk i 112.168.192.in-addr.arpa.

W pliku **/lab-dns/dns1/var/named/file.log** powinny znaleźć się podobne wpisy:

```
13-Nov-2010 11:34:53.600 update: client  127.0.0.1#36606:
      updating zone 'iti.pk/IN':   adding an RR at
      't6.iti.pk' A
13-Nov-2010 11:34:53.604 notify: zone iti.pk/IN:
      sending notifies (serial 2)
```

Pierwszy wpis informuje, że został dodany rekord zasobów do strefy iti.pk. Drugi natomiast – wysłanie powiadomień o zmianie danych strefy iti.pk. Plik **/lab-dns/dns2/var/named/file.log** zawiera analogiczne wpisy.

ZAKOŃCZENIE ĆWICZENIA

Po zakończeniu ćwiczenia należy uruchomić:

```
# /root/lab-dns/lab-dns stop
```

w celu przywrócenia stanu wyjściowego systemu.

OPRACOWANIE ĆWICZENIA I SPRAWOZDANIE

Wykonanie ćwiczenia polega na praktycznej realizacji wszystkich zadań **Rozdziału 2** niniejszej instrukcji zatytułowanego „**Przebieg Ćwiczenia**". Należy sporządzić sprawozdanie z wykonania ćwiczenia (w formie dokumentu elektronicznego) i w ciągu najdalej dwóch tygodni od dnia wykonania ćwiczenia oddać je prowadzącemu zajęcia.

Kompletne opracowanie ćwiczenia powinno zawierać:

- ✓ Część opisową odnoszącą się do teorii przerabianego ćwiczenia. Ta część sprawozdania powinna wykazać dobrą ogólną znajomość zagadnień leżących u podstaw przerabianego tematu, znajomość odnośnej literatury, samodzielność myślenia i umiejętność pisania opracowań o charakterze technicznym.

- ✓ Wnioski praktyczne wynikające z wykonania ćwiczenia, a w tym:

  - uwagi odnoszące się do przebiegu ćwiczenia (np. czy dane ćwiczenie może być wykonane z pełnym rozumieniem zawartych w nim czynności i problemów, czy ćwiczenie jest możliwe do wykonania w czasie przeznaczonym na zajęcia, czy ćwiczenie jest zbyt trudne/ zbyt łatwe, itp.,
  - uwagi odnoszące się do sposobu przygotowania i jakości (waloru dydaktycznego) instrukcji do ćwiczenia,
  - uwagi odnoszące się do ewentualnych utrudnień technicznych lub organizacyjnych pojawiających się w trakcie wykonywania ćwiczenia,
  - postulaty merytoryczne i techniczne dotyczące usprawnienia/ulepszenia jakości wykonywanego ćwiczenia,
  - inne

  Wnioski z drugiej części sprawozdania posłużą do usprawnienia i poprawy zajęć laboratoryjnych w latach następnych.

