Instalacja i konfiguracja serwera DNS

Linux/UNIX - DNS

BIND

BIND (*Berkeley Internet Name Domain*, poprzednio:
Berkeley Internet Name Daemon) jest popularnym serwer (demon) DNS.
Stworzony przez Paula Vixie w 1988.

Wykorzystywany jest w systemach Linux i Unix.

Stanowi składnik zapewniający poprawne działanie systemu nazw w Internecie.

Cechy BIND:
Open source, licencja BSD.

Wersja BIND 9 napisana od zera pod koniec lat 90. XX wieku, ze względu na dużą ilość błędów bezpieczeństwa w poprzedniej wersji BIND 4.

Obsługa ładowania stref z plików, katalogu LDAP, baz danych Berkeley DB, PGSQL, MySQL.
Integracja z serwerem DHCP ISC dla automatycznych uaktualnień DDNS klientów DHCP.

BIND zawarty jest w praktycznie każdej dystrybucji Linuxa.

Podstawy konfiguracji BIND

Instalacja
 # apt-get install bind9 dnsutils

Polecenie startujące usługę
 # /etc/init.d/bind9 start

Katalog z konfiguracją
/etc/bind

Główny plik konfiguracyjny
/etc/bind/named.conf

W Debianie plik ten zawiera polecenia użycia plików:

named.conf.options – konfig. katalogu roboczego, porty nasłuchu, forward

named.conf.local – definicje lokalnych stref

named.conf.default-zones – konfiguracja stref głównych, localhosta i broadcastu

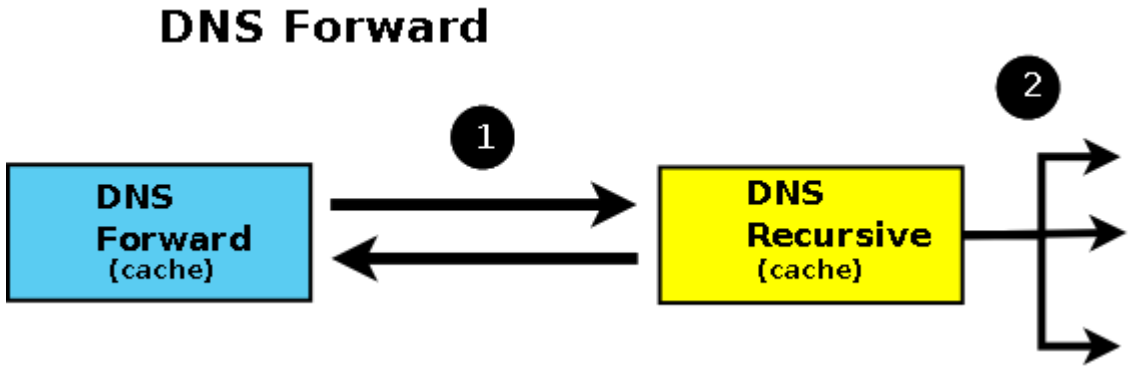
Rodzaje stref DNS

Strefa podstawowa (primary, master) Zawiera dane strefy pobrane bezpośrednio z pliku na hoście

Strefa zapasowa (secondary, slave). Zawiera dane kopiowane podczas procesu replikacji z podstawowego serwera strefy lub z innego serwera zapasowego

Strefa skrótowa (stub zone) Strefa ta zawiera wyłącznie rekordy, które są potrzebne do zidentyfikowania serwera DNS dla tej strefy.

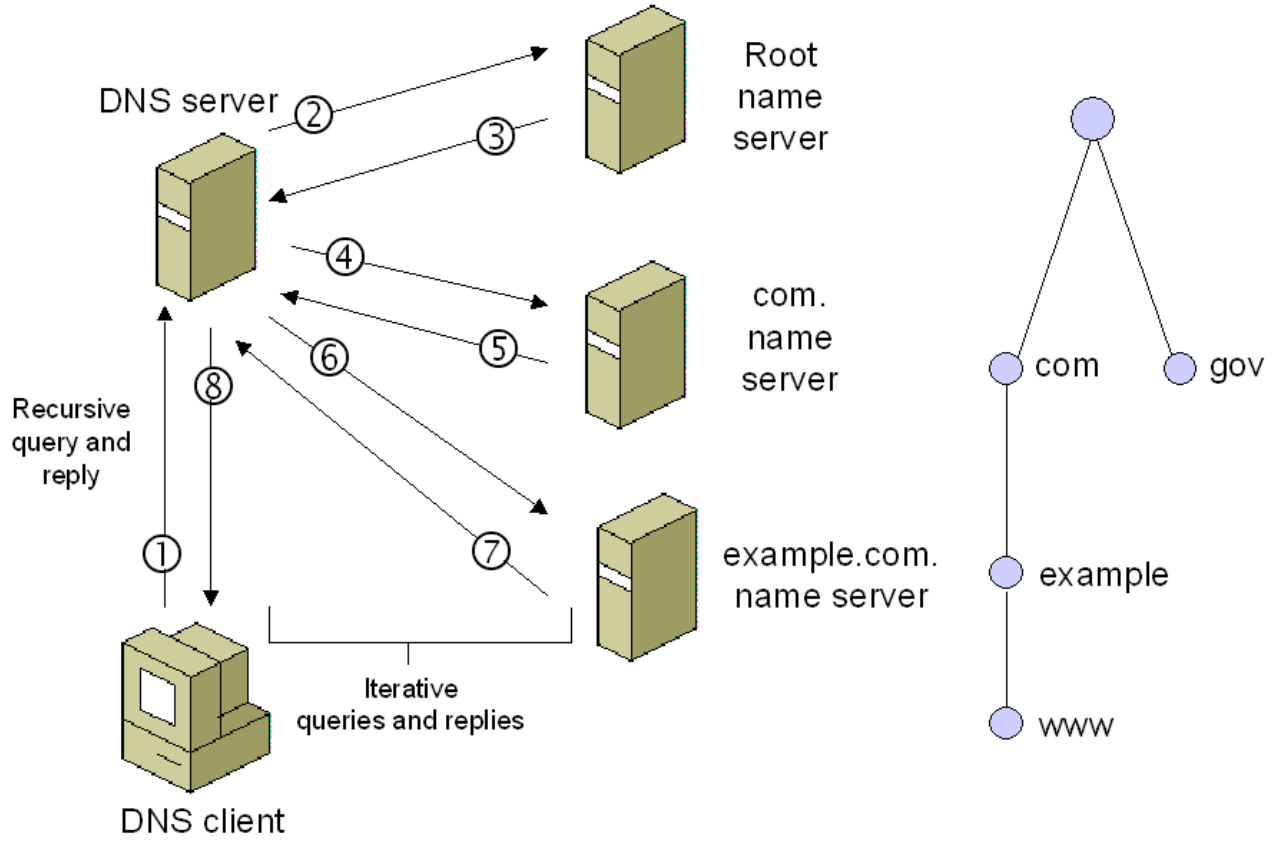
Forwardowanie – przekazywanie zapytań dla konkretnej strefy do innego serwera DNS znajdującego się na liście forwardu



Rodzaje stref DNS

Strefa prosta (forward zone) – strefa przechowująca rekordy do zapytań prostych: adres domenowy -> adres IP

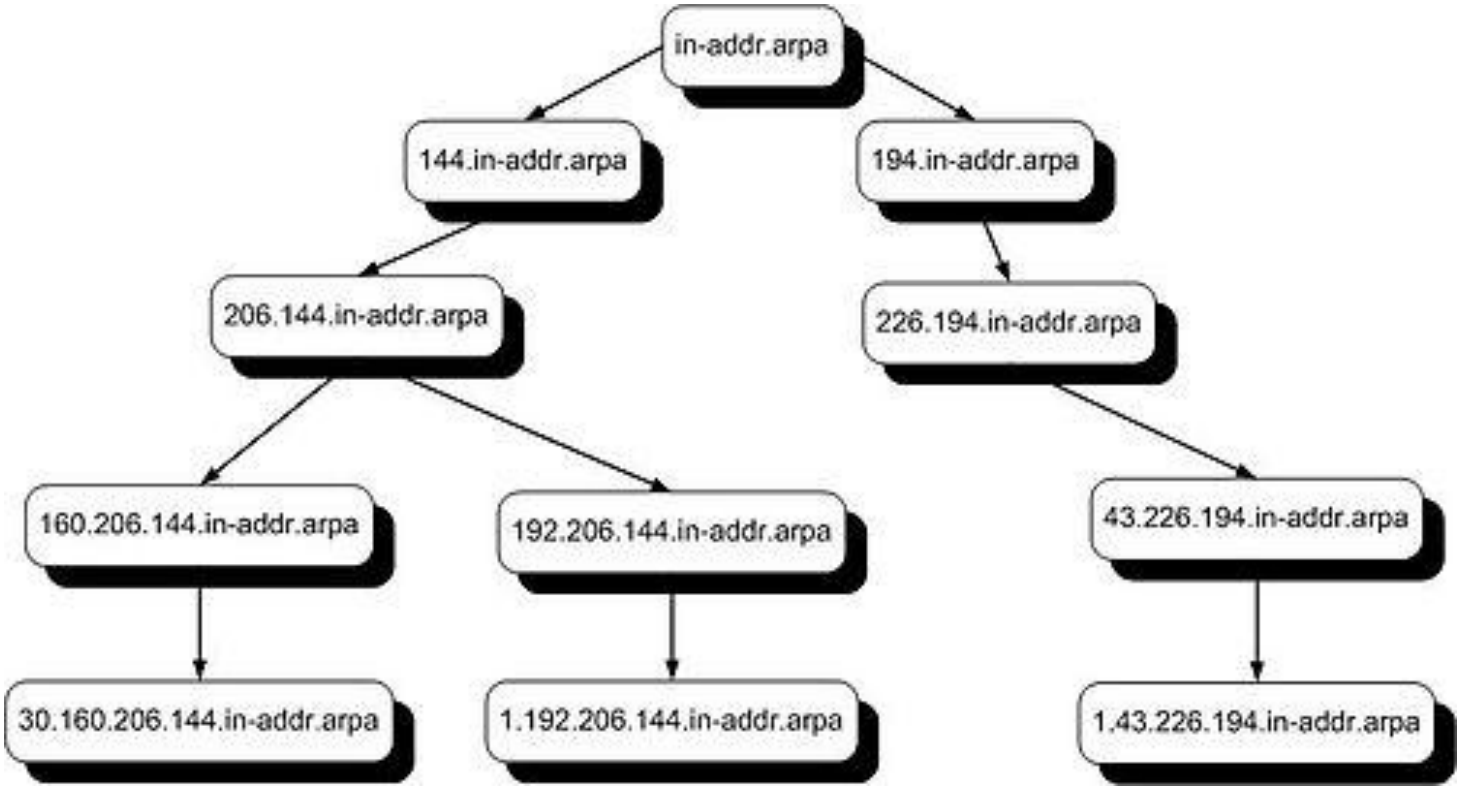
```
zone "test.debian.org.pl" {
  type master;
  file "/etc/bind/db.test.debian.org.pl";
};
```



Rodzaje stref DNS

Strefa odwrotna (reverse zone) – strefa przechowująca rekordy do zapytań odwrotnych: adres IP - >nazwa domenowa

```
zone "194.122.212.in-addr.arpa" {
  type master;
  file "/etc/bind/db.194.122.212.in-addr.arpa";
};
```



Przykładowa konfiguracja serwera BIND

Plik **named.conf.options**

```
options {
        directory "/var/cache/bind";
        listen-on { any; };
        listen-on-v6 { any; };
        auth-nxdomain yes;
        query-source address * port 53;
        transfer-source * port 53;
        notify-source * port 53;
        version "Mój serwer DNS";
        forwarders { 192.168.1.1; 192.168.1.4; };
};
```

Serwer DNS będzie pracował jako serwer cache'ujący i ustawimy forwarding do DNS'ów dostawcy. Wcześniej ustaw statyczną konfigurację IP.

Tworzymy własną strefę podstawową

Plik **/etc/bind/named.conf.local**

```
zone „i.sobczak.edu.pl" {
        type master;
        file "/etc/bind/i.sobczak.edu.pl";
        allow-transfer { any; };
        notify yes;
};
```

type (master/slave) mówi o tym, że to serwer jest podstawowy lub zapasowy
file wskazuje na ścieżkę do pliku ze strefą
allow-transfer to adresy IP serwerów, które mogą transferować całą zawartość strefy. Zazwyczaj są to adresy IP zapasowych serwerów DNS dla danej domeny.
notify ustawia, czy zapasowe serwery mają być informowane o zmianach w strefie. Opcja ta znacznie przyspiesza aktualizowanie informacji o strefach.

Tworzymy własną strefę podstawową

Edytujemy plik **`/etc/bind/i.sobczak.edu.pl`**

```
$TTL 2d
@ IN SOA ns1.i.sobczak.edu.pl. root.i.sobczak.edu.pl.(
2012110810          ; Serial
10800               ; Refresh
180                 ; Retry
604800              ; Expire - 1 week
60 )                ; Minimum
  NS ns1. i.sobczak.edu.pl.
@ IN A 192.167.0.15
ns1 IN A 192.167.0.15
pserver IN A 192.167.0.18
pserver2 IN A 192.167.0.19
irek IN A 192.167.0.22
irek2 IN A 192.167.0.23
```

Zauważ, że wszystkie nazwy domenowe są zakończone kropką.

Gdyby tych kropek nie było, serwer potraktowałby tą nazwę jako cześć domeny utrzymywanej w tej strefie!

Objaśnienia do pliku strefy

$TTL to czas, przez jaki poszczególne wpisy są buforowane na serwerach DNS

$ORIGIN to nazwa utrzymywanej strefy.

ns1.twoj.server.pl to adres Twojego serwera nazw

root.twoj.server.pl to Twój adres email, gdzie pierwsza kropka oznacza znak @.

Serial to numer seryjny. Zaleca się aby był on w formacie RRRRMMDDNN. (data ostatniej modyfikacji plus numer poprawki)

Objaśnienia do pliku strefy

Refresh – Częstość odświeżania. Decyduje o tym, jak często serwery dodatkowe będą sprawdzać, czy ich dane na temat strefy są aktualne.

Retry – Częstość powtórek. Jeśli serwerowi dodatkowemu nie uda się skontaktować z serwerem podstawowym po czasie odświeżania, to próbuje co jakiś tu zdefiniowany czas.

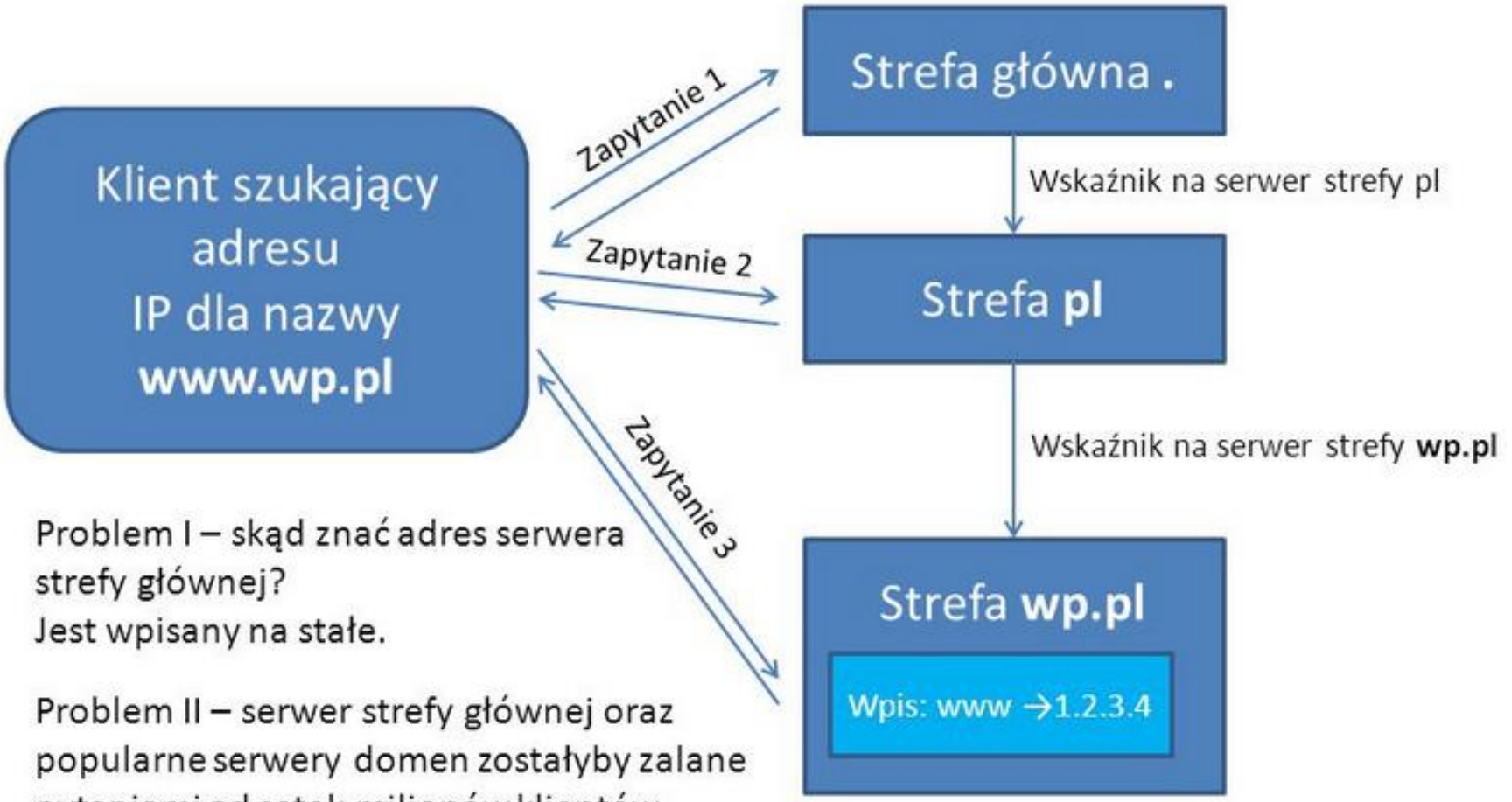
Expire – Czas wygaśnięcia. Jeśli serwerowi dodatkowemu nie uda się skontaktować z serwerem podstawowym przez czas wygaśnięcia, to zaczyna usuwać stare dane. Czas wygaśnięcia zawsze powinien być znacznie większy od częstości odświeżania i powtórek (na przykład 30 dni).

Tworzymy własną strefę podstawową

Edytujemy plik **`/etc/resolv.conf`**

```
domain i.sobczak.edu.pl
search i.sobczak.edu.pl
nameserver 192.167.0.15
```

Przykład użycia hierarchii w DNS



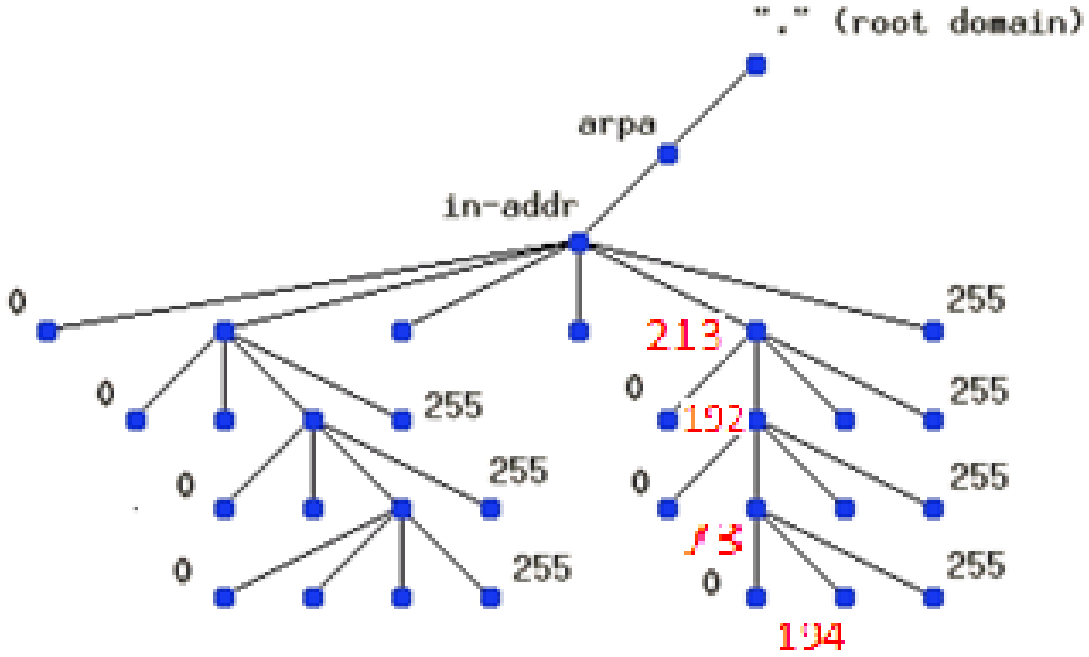
Problem I – skąd znać adres serwera strefy głównej?
Jest wpisany na stałe.

Problem II – serwer strefy głównej oraz popularne serwery domen zostałyby zalane pytaniami od setek milionów klientów

Strefa odwrotna RevDNS

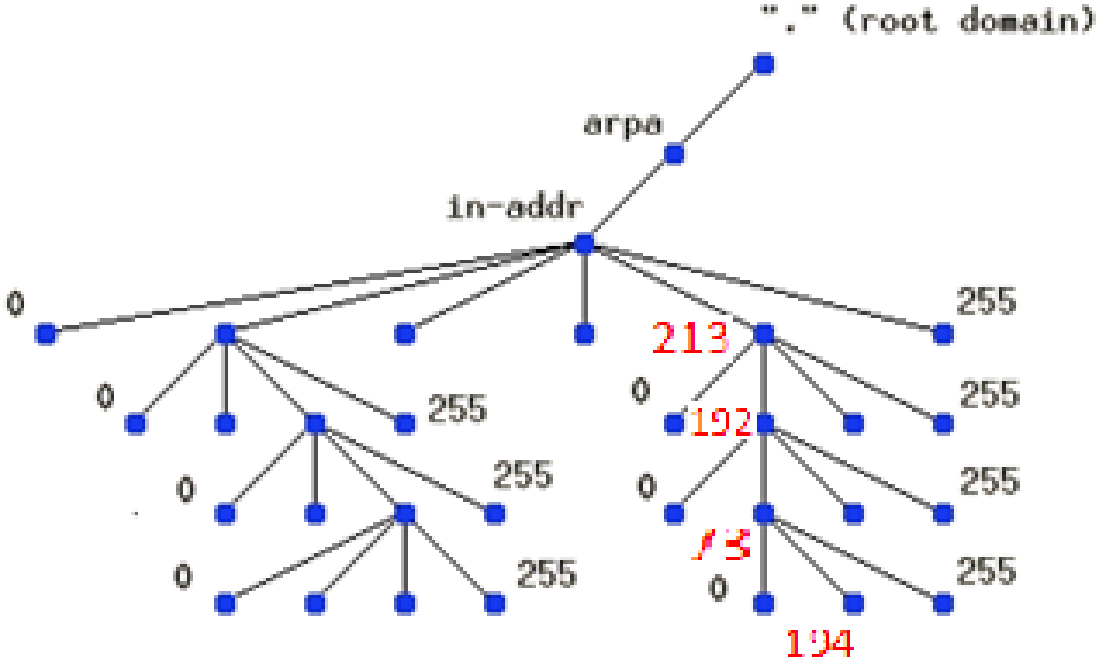
RevDNS to odwzorowywanie adresów IP na nazwy.
W przestrzeni nazw domenowych istnieje domena in-addr.arpa, węzły w tej domenie są etykietowane wg. liczb w kropkowej notacji adresu IP.

Wynika z tego, że domena in-addr.arpa posiada 256 węzłów, których etykietą jest pierwszy oktet adresu IP.



Każdy z tych węzłów rozgałęzia się na kolejne 256 węzłów których etykietą jest już drugi oktet adresu IP.

Strefa odwrotna RevDNS



Tworzy się w ten sposób drzewo posiadające cztery poziomy (tyle ile jest oktetów w adresie IP).
W ten sposób domena in-addr.arpa w rzeczywistości może pomieścić wszystkie adresy IP Internetu.
Adresy w nazwie domenowej zapisywane są od tylu - adresowi IP 213.192.73.194 odpowiada węzeł w domenie in-addr.arpa 194.73.192.213.in-addr.arpa.
Taka struktura umożliwia delegowanie domen w strefie odwzorowywanie odwrotnego.

Tworzymy strefę odwrotną

Plik strefy **/etc/bind/db.87.190.211.in-addr.arpa**

```
@ IN SOA debian1.oke.local. root.oke.local. (
2007040301          ;serial
14400               ;refresh
3600                ;retry
604800              ;expire
10800               ;minimum
)

87.190.211.in-addr.arpa.  IN  NS  debian1.oke.local.
87.190.211.in-addr.arpa.  IN  NS  debian2.oke.local.

77  IN  PTR  debian1.oke.local.
78  IN  PTR  debian2.oke.local.
79  IN  PTR  debian3.oke.local.
80  IN  PTR  debian4.oke.local.
```

Tworzymy strefę odwrotną

Opis pliku strefy
Podobnie jak dla strefy prostej pierwszy wpis stanowi domyślny **ttl**, potem rekord **SOA**, następnie rekordy zasobów dotyczące serwerów strefy odwzorowywania odwrotnego i na końcu rekordy zasobów dla konkretnej strefy.
Jednakże w pliku tym wykorzystuje się do tego celu jeden rekord **PTR**.
Rekord ten służy do powiązania nazw w domenie in-addr.arpa z nazwami hostów.
Pole musi zawierać kanoniczną nazwę hosta.

wpis w pliku **/etc/bind/named.conf.local**

```
zone "87.190.211.in-addr.arpa" {
  type master;
  file "/etc/bind/db.87.190.211.in-addr.arpa";
  allow-transfer { any; };
  notify yes;
};
```

Tworzymy zapasowy serwer DNS

Ponownie edytujemy plik **/etc/bind/i.sobczak.edu.pl**
Dodajemy modyfikacje o secondary DNS

```
$TTL 2d
@ IN SOA ns1.i.sobczak.edu.pl.
root.i.sobczak.edu.pl.(
2012110810              ; Serial
10800                   ; Refresh
180                     ; Retry
604800                  ; Expire - 1 week
60 )                    ; Minimum
  NS ns1.i.sobczak.edu.pl.
@ IN A 192.167.0.15
ns1 IN A 192.167.0.15
ns2 IN A 192.167.0.16
pserver IN A 192.167.0.18
pserver2 IN A 192.167.0.19
irek IN A 192.167.0.22
irek2 IN A 192.167.0.23
```

Tworzymy zapasowy serwer DNS

Edytujemy plik **named.conf.local**
Pozwalamy na transfer stref

```
zone "i.sobczak.edu.pl" {
        type master;
        file "/etc/bind/ i.sobczak.edu.pl ";
        allow-transfer { 192.167.0.16 };
        notify yes;
};
```

Serwer zapasowy DNS

Konfigurujemy DNS na drugim serwerze
Edytujemy plik **named.conf.local**

```
zone " i.sobczak.edu.pl " {
        type slave;
        file "/etc/bind/slave/ i.sobczak.edu.pl ";
        masters { 192.167.0.15 };
};
```

należy utworzyć katalog /etc/bind/slave i zmienić właściciela na bind

 # mkdir /etc/bind/slave
 # chown bind.bind /etc/bind/slave

Poprawność konfiguracji sprawdzamy w pliku
/var/log/daemon.log

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;

Rekordy zasobowe

• 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 od czytują 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.

Lokalizacja serwerów dns

http://www.dns.pl/map.html