

40

Przygotowanie do pracy serwera DNS

ZAGADNIENIA

- Funkcje protokołu DNS
- Typy serwerów DNS
- Typy stref przeszukiwania i ich funkcje
- Procedura konfigurowania serwerów buforującego, podstawowego i zapasowego
- Narzędzia do testowania działania serwera DNS

System DNS jest oparty na hierarchicznej i logicznej strukturze drzewa zwanej obszarem nazw domen. Każdy węzeł drzewa DNS reprezentuje nazwę DNS, np. domenę DNS. Domeny DNS mogą zawierać hosty (np. komputery, serwery) oraz inne domeny nazywane poddomenami. Węzły w drzewie domen DNS są identyfikowane przez pełną nazwę domeny FQDN (ang. *Fully Qualified Domain Name*) i wskazują położenie węzła względem domeny głównej.

Serwer DNS pozwala na tłumaczenie nazw w sieciach opartych na TCP/IP na adresy IP odpowiadające nazwom. Dzięki DNS użytkownik może posługiwać się nazwami domen zamiast adresami IP konkretnych serwerów. DNS może być wykorzystany do tłumaczenia nazw w sieci lokalnej lub, po zarejestrowaniu nazwy domeny, również w internecie.

Serwer DNS umożliwia dwa rodzaje przeszukiwania strefy:

- **do przodu** – na podstawie nazwy określamy adres IP;
- **wstecz** – na podstawie adresu IP szukamy odpowiadającej mu nazwy.

Do przeszukiwania stref serwer wykorzystuje rekordy zasobów:

- **A** – mapuje nazwę hosta na adres IPv4;
- **AAAA** – mapuje nazwę hosta na adres IPv6;
- **CNAME** – ustawia alias (inną nazwę) dla nazwy hosta;
- **MX** – określa serwer wymiany poczty dla domeny;
- **NS** – określa serwer nazw dla domeny (DNS);
- **PTR** – tworzy powiązanie adresu IP z nazwą w strefie przeszukiwania wstecz.

SOA jest wymagany dla każdej strefy i określa serwer DNS, który dostarcza autorytatywne informacje dla danej strefy. Istnieją trzy główne sposoby konfigurowania usługi DNS:

- **buforujący serwer nazw** (ang. *caching name server*) – nie przechowuje bazy danych rekordów; gdy otrzyma pytanie o nazwę, o obsłudze żądania poprosi inny serwer nazw i umieści ją w swoim buforze, dzięki czemu będzie ona zawsze dostępna;
- **podstawowy serwer nazw** (ang. *primary name server*) – zawiera główną kopię bazy danych z nazwami wszystkich hostów w strefie oraz rekordy dla wszystkich poddomen;
- **zapasowy serwer nazw** (ang. *secondary name server*) – zawiera kopię bazy danych z rekordami dla domeny i poddomen; zmiany wprowadzane do podstawowego DNS są replikowane do wszystkich serwerów zapasowych.

Jednym z najpopularniejszych serwerów DNS wykorzystywanym w systemach Linux jest **BIND**. Aby zainstalować serwer w dystrybucji Ubuntu, należy wydać polecenie:

sudo apt install bind9.

Pliki konfiguracyjne są przechowywane w katalogu **/etc/bind/**. Podstawowe opcje konfiguracji są przechowywane w plikach **named.conf**, **named.conf.options** i **named.conf.local**. Ponadto dodatkowe pliki wykorzystuje się do przechowywania informacji o strefach.

Dzięki buforującemu serwerowi nazw można przyspieszyć proces tłumaczenia nazw na adresy IP. Serwer umieszczony w sieci lokalnej, np. w szkole, zapisuje w swojej pamięci informacje o nazwach stron internetowych odwiedzonych przez uczniów i odpowiadających im adresach IP. Dostęp do tych informacji w sieci lokalnej jest szybszy, a ponadto można zmniejszyć liczbę zapytań wysyłanych do zewnętrznych serwerów DNS.

PRZYKŁAD 40.1

Konfigurowanie i testowanie buforującego serwera nazw

Aby skonfigurować buforujący serwer nazw, należy:

- W pliku **named.conf.options** usunąć symbol komentarza na początku poniższych linijek i wpisać adresy serwerów DNS dostawcy usług internetowych (rys. 40.1). W tym przykładzie wpisano adresy serwerów OpenDNS – oferujących darmowy dostęp do DNS i dodatkowo możliwość zablokowania dostępu np. do stron pornograficznych lub zawierających sceny przemocy.

```
forwarders {
    208.67.222.222;
    208.67.220.220;
};
```

```
named.conf.options * — Kate
Plik Edycja Widok Projekty Zaktual. Sesje Narzędzia Ustawienia Pomoc
Dokumenty named.conf.options named.conf
options {
    directory "/var/cache/bind";
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses
    // replacing
    // the all-0's placeholder.
    forwarders {
        208.67.222.222;
        208.67.220.220;
    };
    //
    // -----
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/
    // bind-keys
    //
    dnssec-validation auto;
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};

Wiersz 15, Kolumna 19 WSTAW Mяkka tabulacja: 4 UTF-8 Normal Znajdź i zastąp
```

Rys. 40.1 Przykładowy plik **/etc/bind/named.conf.options**

40. PRZYGOTOWANIE DO PRACY SERWERA DNS

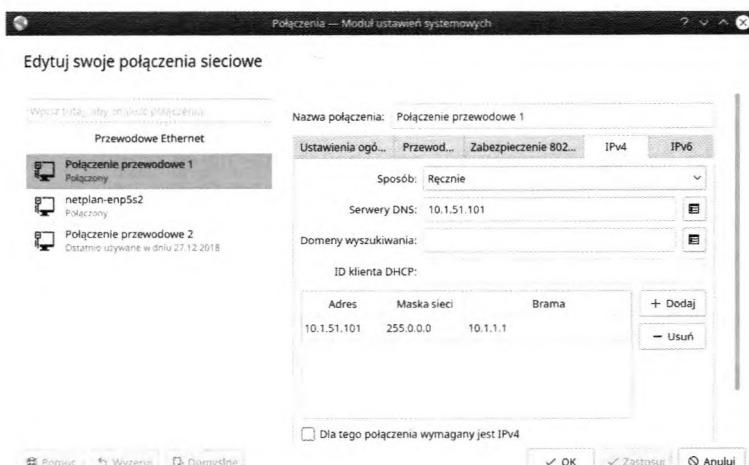
Linux

opcje
i na-
infor-nazw
mięci
idażą-
nadopo-
vych
cych
. do

2. Uruchomić ponownie demona BIND za pomocą polecenia:

```
sudo /etc/init.d/bind9 restart.
```

3. W oknie konfiguracji adresu IPv4 ustawić adres serwera DNS. W polu Serwery DNS należy wpisać adres IP komputera, w którym jest uruchomiony buforujący serwer DNS (rys. 40.2).



Rys. 40.2. Konfiguracja adresu serwera DNS

4. Przetestować działanie serwera. Do testowania serwera DNS w środowisku Linux można użyć polecenia **dig**, np. aby sprawdzić adres IP serwera **onet.pl**, należy wydać polecenie:

```
dig onet.pl.
```

Przykład działania polecenia **dig** zaprezentowano na rys. 40.3. Adres IP serwera **onet.pl** jest pokazany w sekcji „ANSWER SECTION”.

```
uczen: bash — Konsola
Plik Edycja Widok Zakładki Ustawienia Pomoc
:-$ dig onet.pl
; <>> DiG 9.11.3-Ubuntu1.3-Ubuntu <>> onet.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 21999
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 9, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; COOKIE: 29611969fbce@0ea9ef06e15c310983b3e881874cf527@c (good)
;; QUESTION SECTION:
;onet.pl.           IN  A
;; ANSWER SECTION:
onet.pl.          60   IN  A    213.180.141.140
;; AUTHORITY SECTION:
pl.               172197  IN  NS   g-dns.pl.
pl.               172197  IN  NS   h-dns.pl.
pl.               172197  IN  NS   e-dns.pl.
pl.               172197  IN  NS   f-dns.pl.
pl.               172197  IN  NS   b-dns.pl.
pl.               172197  IN  NS   d-dns.pl.
pl.               172197  IN  NS   c-dns.pl.
pl.               172197  IN  NS   a-dns.pl.
pl.               172197  IN  NS   i-dns.pl.
;; Query time: 72 msec
;; SERVER: 10.1.51.101#53(10.1.51.101)
;; WHEN: Sat Jan 05 20:46:11 CET 2019
;; MSG SIZE rcvd: 260
:-$
```

Rys. 40.3. Testowanie DNS za pomocą polecenia **dig**

Każdy host w domenie ma adres IP i nazwę domenową. Rekordy odwzorowania adresów (A) odwzorowują nazwę hosta na przypisany mu adres IP. Dzięki tym rekordom inne hosty w sieci mogą uzyskać od serwera DNS odpowiedź na zapytania o adres IP przypisany do określonej nazwy hosta. Rekordy wskaźników wyszukiwania odwrotnego (PTR) odwzorowują adresy IP poszczególnych hostów na przypisane im nazwy – pozwalają innym hostom w sieci uzyskać od serwera DNS informacje o nazwach odpowiadających adresom IP. Administrator serwera DNS musi zdefiniować dane strefy DNS i utworzyć rekordy zasobów. Serwer DNS obsługuje również inne typy rekordów zasobów, np. rekordy serwerów poczty elektronicznej (MX) lub innych serwerów nazw (NS).

Każdy serwer nazw zawiera dane o pewnej części całej przestrzeni adresowej DNS. Dane z każdej domeny powinny być przechowywane na co najmniej dwóch serwerach. Jeden z nich, tzw. podstawowy serwer nazw, jest autorytatywnym źródłem informacji o danej domenie. Pozostałe serwery przechowują kopię zawartości serwera podstawowego. Serwery zapasowe zwiększą niezawodność i odporność całego systemu na awarie i są używane w przypadku awarii lub wyłączenia serwera podstawowego albo w celu rozłożenia obciążenia na kilka serwerów.

PRZYKŁAD 40.2

Konfigurowanie podstawowego serwera nazw

W tym przykładzie zostanie skonfigurowany podstawowy serwer DNS dla domeny **zsp.local**. Ponieważ nazwa tej domeny nie została zarejestrowana, dostępna będzie tylko w sieci lokalnej. Aby skonfigurować podstawowy serwer nazw, należy:

1. W pliku **named.conf.local** dodać strefę przeszukiwania „w przód”. W tym przykładzie dodano opis strefy **zsp.local**. W opisie strefy „type master” oznacza typ strefy podstawowej, natomiast **file** opisuje ścieżkę do pliku zawierającego bazę danych strefy. Przykładowy plik **named.conf.local**, zawierający strefę przeszukiwania „w przód” i „wstecz”, pokazano na rys. 40.6.

```
zone „zsp.local” IN {  
    type master;  
    file „/etc/bind/db.zsp.local”;  
};
```

2. Utworzyć plik konfiguracji strefy. W katalogu **/etc/bind** są umieszczone przykładowe pliki konfiguracji stref. Można skopiować plik, np. **db.local**, i podać go modyfikacji. Na rys. 40.4 pokazano przykładowy plik konfiguracji strefy przeszukiwania „w przód”. W pliku w obszarze SOA wprowadzono nazwę serwera DNS **ns1.zsp.local** i **root.zsp.local**. (zwróć uwagę na kropkę na końcu nazwy). Pozostałe parametry można pozostawić bez zmian. Ponadto w pliku wprowadzono cztery rekordy typu A (brama, jas, franek, ania) wraz z odpowiadającymi im adresami IP. Po każdym wprowadzeniu zmian w pliku konfiguracyjnym strefy należy zwiększyć wartość **numeru konfiguracji (serial)** – opcja ta pozwala na określenie, który z plików konfiguracji stref ma najbardziej aktualne dane.
3. W pliku **named.conf.local** dodać strefę przeszukiwania „wstecz”. W tym przykładzie dodano opis strefy **10.in-addr.arpa**. W opisie strefy opcja **notify** no oznacza, że serwer nie będzie wysyłał powiadomień o zmianach w strefie do innych serwerów, pozostałe opcje mają takie samo znaczenie jak w strefie „w przód”.

40. PRZYGOTOWANIE DO PRACY SERWERA DNS

```

db.zsp.local * — Kate
Plik Edycja Widok Projekty Zakładki Sesje Narzędzia Ustawienia Pomoc
Dokumenty db.zsp.local named.conf.local
;
; BIND data file for local loopback interface
$TTL 604800
@ IN SOA ns1.zsp.local. root.zsp.local. (
        2 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
@ IN A 127.0.0.1
@ IN AAAA ::1
brama IN A 10.1.1.1
jas IN A 10.1.51.101
franek IN A 10.1.51.102
ania IN A 10.1.51.103

```

Wiersz 20, Kolumna 1 WSTAW Miękka tabulacja: 4 UTF-8 Normal

Q Znajdź i zastąp

Rys. 40.4. Plik konfiguracji strefy przeszukiwania „w przód”

```

zone „10.in-addr.arpa” {
    type master;
    notify no;
    file „/etc/bind/db.10.in-addr.arpa”;
}

```

4. Utworzyć plik konfiguracji strefy. Można skopiować przykładowy plik, np. **db.255**, i poddać go modyfikacji. Na rys. 40.5 pokazano przykładowy plik konfiguracji strefy przeszukiwania „wstecz”. W pliku w obszarze SOA wprowadzono nazwę serwera DNS **ns1.zsp.local.** i **root.zsp.local.** (zwróć uwagę na kropkę na końcu nazwy). Pozostałe parametry można pozostawić bez zmian. Ponadto w pliku wprowadzono cztery wskaźniki przeszukiwania wstecz dla rekordów brama, jas, franek, ania wraz z odpowiadającymi im adresami IP. Po każdym wprowadzeniu zmian w pliku konfiguracyjnym strefy należy zwiększyć wartość numeru konfiguracji (**serial**).

```

db.10.in-addr.arpa * — Kate
Plik Edycja Widok Projekty Zakładki Sesje Narzędzia Ustawienia Pomoc
Dokumenty db.10.in-addr.arpa
;
; BIND reverse data file for broadcast zone
$TTL 604800
@ IN SOA ns1.zsp.local. root.zsp.local. (
        1 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
$ORIGIN 1.10.in-addr.arpa.
1 IN PTR brama.zsp.local.
$ORIGIN 51.10.in-addr.arpa.
101 IN PTR jas.zsp.local.
102 IN PTR franek.zsp.local.
103 IN PTR ania.zsp.local.

```

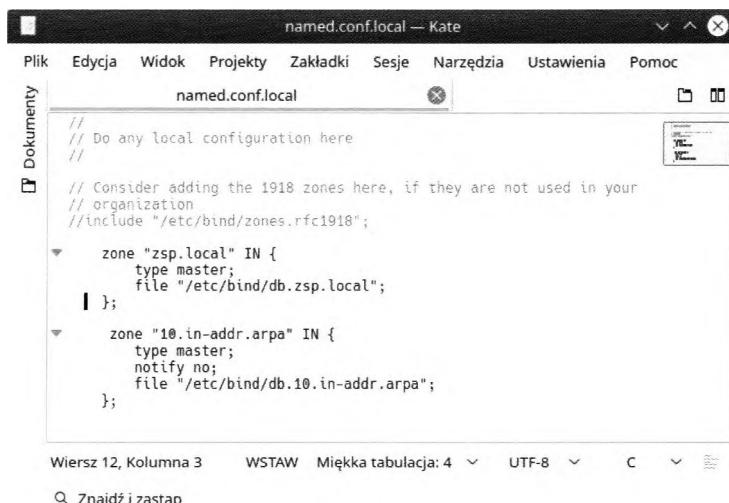
Wiersz 19, Kolumna 36 WSTAW Miękka tabulacja: 4 UTF-8 Normal

Q Znajdź i zastąp

Rys. 40.5. Plik konfiguracji strefy przeszukiwania „wstecz”

5. Uruchomić ponownie demona BIND za pomocą polecenia:

```
sudo /etc/init.d/bind9 restart.
```

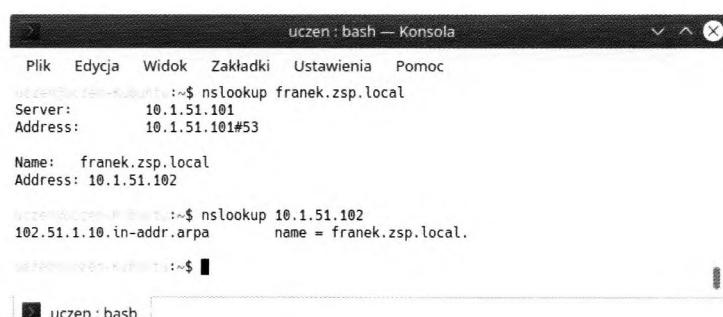


Rys. 40.6. Plik konfiguracji stref przeszukiwania

6. Przetestować działanie serwera. Do testowania serwera DNS w środowisku Linux można użyć polecenia **nslookup**, np. aby sprawdzić adres IP komputera **franek.zsp.local**, należy wydać polecenie:

```
nslookup franek.zsp.local.
```

Narzędzie może być wykorzystane do testowania strefy „w przód” – jako argument polecenia podaje się nazwę, a serwer DNS zwraca adres IP, lub do testowania strefy „wstecz” – podaje się adres IP, a otrzymuje nazwę. Przykład działania polecenia **nslookup** pokazano na rys. 40.7.



Serwery zapasowe pobierają dane strefy z serwera autorytatywnego. Aktualizowanie tych danych odbywa się w wyniku przesyłania strefy z serwera autorytatywnego. Podczas uruchamiania serwer zapasowy wysyła do podstawowego serwera nazw żądanie przesłania wszystkich danych dla określonej domeny. Strefa jest transferowana tylko w przypadku,

gdy numer konfiguracji (*serial*) strefy serwera podstawowego jest wyższy niż numer konfiguracji (*serial*) strefy serwera zapasowego. Serwer zapasowy może zażądać zaktualizowanych danych z podstawowego serwera nazw, gdy zostanie powiadomiony o zmianach przez podstawowy serwer nazw (jeśli włączona jest opcja *notify*) lub gdy na podstawie zapytań kierowanych do podstawowego serwera nazw wykryje zmianę danych. Do dobrej praktyki administratora należy skonfigurowanie przynajmniej jednego serwera zapasowego dla każdej strefy.

PRZYKŁAD 40.3

Konfigurowanie zapasowego serwera nazw

W tym przykładzie zostanie skonfigurowany zapasowy serwer DNS dla domeny **zsp.local**. Aby skonfigurować zapasowy serwer nazw, należy:

1. Skonfigurować serwer podstawowy tak, aby zezwalał na transfer stref. W pliku **named.conf.local** w konfiguracji stref dodać wpis **allow-transfer** (rys. 40.8). Opcja ta określa adresy IP serwerów, do których będą wysyłane dane stref.

```
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "zsp.local" IN {
    type master;
    notify yes;
    file "/etc/bind/db.zsp.local";
    allow transfer { 10.1.51.102; };
};

zone "10.in-addr.arpa" IN {
    type master;
    notify yes;
    file "/etc/bind/db.10.in-addr.arpa";
    allow transfer { 10.1.51.102; };
};
```

Rys. 40.8. Plik konfiguracyjny podstawowego serwera DNS z możliwością transferu stref

2. Skonfigurować serwer zapasowy tak, aby zezwalał na odbieranie transferu stref z serwera podstawowego. W pliku **named.conf.local** w konfiguracji stref dodać wpis **masters** (rys. 40.9). Opcja ta określa adresy IP serwerów, z których będą wysyłane dane stref. Ze względu na bezpieczeństwo systemu pliki zawierające kopie bazy danych stref są umieszczane w katalogu **/var/cache/bind**.
3. Na obu serwerach uruchomić ponownie demona BIND polecienniem:
sudo /etc/init.d/bind9 restart.
4. Sprawdzić w katalogu **/var/cache/bind**, czy zostały utworzone pliki stref i czy zawierają opisy stref.
5. W systemie Windows w oknie konfiguracji protokołu TCP/IP ustawić adres preferowanego i alternatywnego serwera DNS, wpisać adres IP komputerów, odgrywających rolę serwera DNS (rys. 40.10).

```

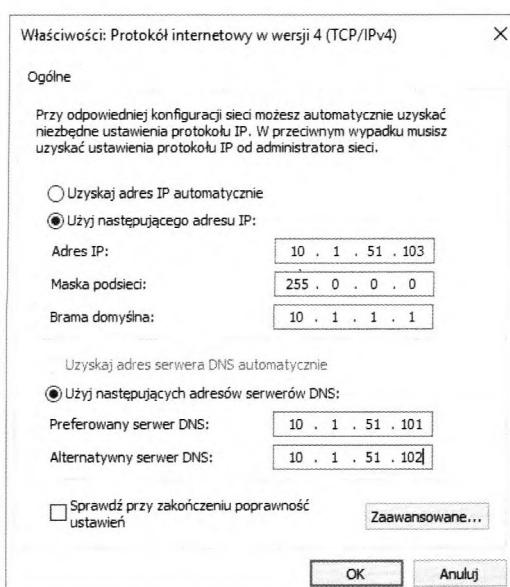
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "zsp.local" IN {
    type slave;
    file "/etc/bind/db.zsp.local";
    masters { 10.1.51.101; };
};

zone "10.in-addr.arpa" IN {
    type slave;
    file "/etc/bind/db.10.in-addr.arpa";
    masters { 10.1.51.101; };
};

```

Rys. 40.9. Plik konfiguracji zapasowego serwera DNS z możliwością odbierania transferu stref



Rys. 40.10. Konfiguracja adresu serwerów DNS w systemie Windows

- Przetestować działanie serwera. Program nslookup może pracować w trybie interaktywnym (rys. 40.11). W pierwszym poleceniu uruchomiono tryb interaktywny programu. W wierszu drugim za pomocą polecenia **server** wybrano preferowany serwer (do tego serwera będą wysyłane zapytania). Wprowadzenie nazwy powoduje wysłanie do serwera DNS zapytania o adres IP, natomiast wprowadzenia adresu IP wysyła zapytanie o nazwę. Poprawne wykonanie obu zapytań pozwala na przetestowanie obu stref wyszukiwania. Program zakończono poleciением **exit**.

```
C:\Users\kp-dell>nslookup
Default Server: jas.zsp.local
Address: 10.1.51.101

> server 10.1.51.101
Default Server: jas.zsp.local
Address: 10.1.51.101

> franek.zsp.local
Server: jas.zsp.local
Address: 10.1.51.101

Name:   franek.zsp.local
Address: 10.1.51.102

> 10.1.51.102
Server: jas.zsp.local
Address: 10.1.51.101

Name:   franek.zsp.local
Address: 10.1.51.102

> exit
C:\Users\kp-dell>
```

Rys. 40.11. Testowanie serwera DNS za pomocą nslookup w trybie interaktywnym

🎯 SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer buforujący, obsługujący sieć szkolną.
2. Wykonaj konfigurację i testowanie działania podstawowego i zapasowego serwera DNS dla sieci w twojej szkole.

🎯 SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij, jakie typy rekordów są używane do opisywania zasobów w systemie DNS.
2. Wyjaśnij, jaka jest różnica między serwerami DNS buforującym i podstawowym.
3. Wyjaśnij, dlaczego w sieci powinien być więcej niż jeden serwer DNS.