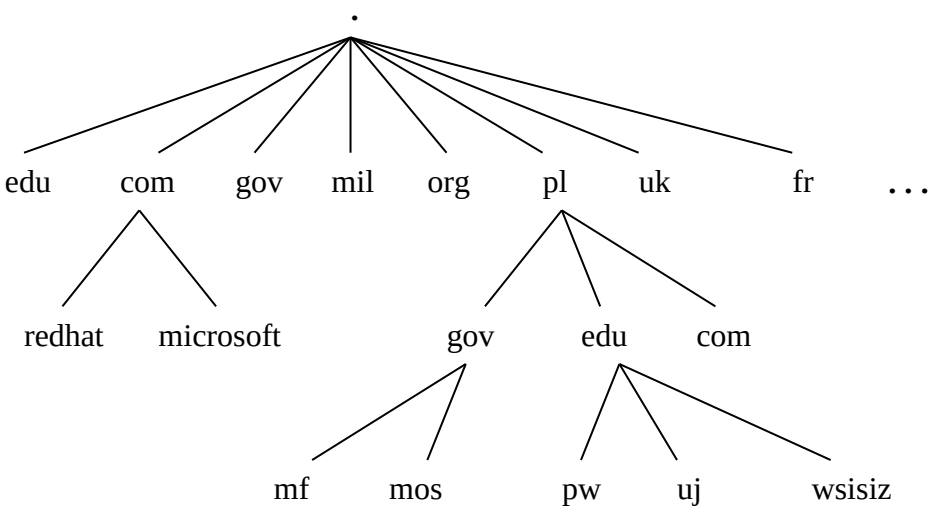
**Usługa DNS**

Zadaniem usługi DNS (Domain Name Service) jest ustalenie adresu IP maszyny na podstawie jej nazwy domenowej, albo operacja odwrotna – ustalenie nazwy domenowej maszyny na podstawie jej adresu IP. Usługa ta działa w oparciu o protokół transportowy UDP, a jej serwery używają portu o numerze 53.

Przestrzeń nazw DNS

Nazwa domenowa jest elementem hierarchicznej struktury zwanej przestrzenią nazw DNS. Najwyższym elementem przestrzeni nazw DNS jest domena główna (root domain) oznaczana samą kropką. Na pierwszym poziomie umiejscowione są domeny organizacji edukacyjnych, komercyjnych, rządowych, wojskowych, itd. mających swoje siedziby w Stanach Zjednoczonych (historycznie, system DNS wywodzi się z USA), oraz 224 domeny krajowe. W nomenklaturze angielskojęzycznej nazywane są one „top level domains", czyli domenami pierwszego poziomu.




Budowa drzewa nazw DNS

Pełna nazwa domenowa (ang. Fully Qualified Domain Name, w skrócie FQDN) składa się z nazwy maszyny oraz tzw. prefiksu DNS, jednoznacznie określającego położenie domeny, do której maszyna ta należy. W skład prefiksu DNS wchodzi nazwa domeny, oraz nazwy wszystkich domen położonych nad nią. Formalnie, prefiks powinien być zakończony kropką, jednak często jest ona opuszczana. Przykładowo, sz123**.**wsisiz**.**edu**.**pl**.** jest pełną nazwą domenową (FQDN) komputera o nazwie sz123 należącego do domeny wsisiz będącej pod-domeną domeny edu, która z kolei jest pod-domeną domeny pl. Domena pl, znajdująca się na pierwszym poziomie hierarchii DNS, jest pod-domeną domeny głównej.

Strefy i delegacje

Usługa DNS działa w oparciu o rozproszoną bazę danych, której fragmenty umiejscowione są na wielu serwerach DNS rozlokowanych po całym świecie. Przestrzeń nazw DNS podzielona jest na obszary zwane strefami. Strefą nazywamy zbiór domen posiadających wspólną domenę nadrzędną, również należącą do tej strefy. Domena taka

nazywana jest domeną główną strefy. Zgodnie z powyższą definicją, zbiór składający się z jednej domeny również jest strefą. Za każdą strefę odpowiedzialny jest co najmniej jeden serwer DNS będący tzw. serwerem autorytatywnym tej strefy. Serwer autorytatywny przechowuje pliki zawierające m.in. odwzorowania nazw DNS na adresy IP dla wszystkich maszyn należących do domen strefy, oraz inne istotne informacje. W celu zapewnienia niezawodnego działania usługi DNS, wymaga się, aby pliki te były przechowywane na więcej niż jednym serwerze, zatem oprócz podstawowego serwera strefy powinien istnieć co najmniej jeden serwer zapasowy, który przejmuje funkcje serwera podstawowego w przypadku awarii bądź planowego wyłączenia. Informacja przechowywana na serwerach zapasowych jest uaktualniana za pomocą tzw. transferów strefy. Transfery strefy mogą być pełne (AXFR) lub przyrostowe (IXFR). Transfery przyrostowe uwzględniają tylko zmiany, które zaszły od ostatniej zmiany numeru seryjnego (patrz opis rekordu SOA).

Kluczowe dla działania systemu DNS są serwery strefy „**.**” która składa się z samej domeny głównej. Obecnie strefa ta jest obsługiwana przez 13 serwerów o następujących nazwach domenowych A**.**ROOT-SERVERS**.**NET**.** , B**.**ROOT-SERVERS**.**NET**.** ,..., M**.**ROOT-SERVERS**.**NET. .Należy zwrócić uwagę na fakt, że serwery strefy „**.**” nie należą do domeny głównej, ale do domeny ROOT-SERVERS**.**NET**.**

Domena główna każdej strefy jest zarazem korzeniem poddrzewa DNS. Zbiór domen należących do tego poddrzewa może być zbyt liczny, aby tworzył jedną strefę, a to ze względu na rozmiar plików bazy DNS dla takiej strefy. W związku z powyższym stosuje się tzw. delegowanie stref. Strefa delegowana to taka, której domena główna znajduje się bezpośrednio pod jedną z domen strefy delegującej. Przykładowo, wszystkie domeny pierwszego poziomu są domenami głównymi stref delegowanych ze strefy „**.**”.

Rekordy zasobów

Pliki bazy DNS składają się z rekordów zasobów (ang. Resource Record, w skrócie RR). Istnieje ok. 20 typów tych rekordów, z których najważniejsze to:

| Nazwa typu | Skrót nazwy | Funkcja |
|---|---|---|
| Adres (Address) | A | Odwzorowanie nazwy domenowej maszyny na adres IPv4 (obsługa zapytań prostych) |
| Adres (Address) | AAAA | Odwzorowanie nazwy domenowej maszyny na adres IPv6 (obsługa zapytań prostych) |
| Serwer nazw (Name Sertver) | NS | Odwzorowanie nazwy DNS strefy na nazwę DNS jednego z serwerów strefy (podstawowego lub jednego z zapasowych) |
| Początek autorytatywnej informacji (Start of Authority) | SOA | Odwzorowanie nazwy DNS strefy na nazwę DNS **podstawowego** serwera strefy, adres e-mail administratora strefy, oraz parametry określające harmonogram transferów strefy |
| Wskaźnik (Pointer) | PTR | Odwzorowanie adresu IP maszyny na jej nazwę DNS (obsługa zapytań odwrotnych) |
| Nazwa kanoniczna(Canonical Name) | CNAME | Odwzorowanie innej nazwy DNS (alias) maszyny, której podstawowa nazwa jest podana w rekordzie typu A. |
| Wymiennik poczty (Mail Exchange) | MX | Odwzorowanie nazwy DNS strefy na nazwę DNS serwera pocztowego (SMTP) tej strefy |
| Informacja o sprzęcie (Hardware Information) | HINFO | Określenie platformy sprzętowej i systemu operacyjnego maszyny |

Rekord zasobów składa się z następujących pól:

Owner: nazwa maszyny lub pełna nazwa DNSdomeny; informacja wiodąca według której wyszukiwany jest potrzebny rekord
TTL: data i czas określające do kiedy informacja w danym rekordzie jest aktualna; po upływie tego czasu klient albo serwer działający w trybie rekurencyjnym, który pobrał tę informację powinien usunąć ją z pamięci podręcznej
Class: klasa rekordu; najczęściej używaną klasą jest IN (Internet)
Type: typ rekordu
Record-specific data: informacja podawana w rekordzie

Rekord SOA:

Rekord SOA musi być pierwszym rekordem każdego pliku strefy. Pole „Owner" zawiera nazwę DNS strefy, dla której dany serwer jest autorytatywny. Informacja podawana w rekordzie: pełna nazwa domenowa **podstawowego** serwera strefy (Primary DNS Server),

adres e-mail administratora strefy (Zone Admin e-mail), numer seryjny sterujący transferami strefy (Serial Number), okres odświeżania (refresh interval), czas do ponownej próby połączenia z serwerem podstawowym (Retry Interval), czas przez jaki informacja na serwerze wtórnym pozostaje aktualna (Expire Interval), minimalny czas życia (Minimum TTL).
**Uwaga!** W rekordzie SOA znak „@” w adresie pocztowym administratora strefy jest zamieniany na „**.**”, a każdy znak „**.**” występujący przed @ – na „**\.**”. Przykładowo, adres zone.master@firma.com jest zamieniany na zone**\.**master.firma.com. Jeśli zapis w rekordzie SOA ma być zamieniony na standardowy adres pocztowy, to znaki „\.” są zamieniane na „.”, a pierwszy znak „.” na „@”.

Przykład rekordu SOA:
wsisiz.edu.pl. 86400 IN SOA see-you-later.wsisiz.edu.pl. admin.wsisiz.edu.pl. 2021100603 28800 7200 1814400 86400

Rekord typu A:

Pole „Owner” zawiera nazwę domenową maszyny. Informacja podawana przez rekord to adres IPv4 maszyny. Jest to informacja podawana w odpowiedzi na zapytanie proste.

Przykład rekordu A:
sz022.wsisiz.edu.pl. 86400 IN A 213.135.47.132

Rekord typu AAAA:

Pole „Owner” zawiera nazwę domenową maszyny. Informacja podawana przez rekord to adres IPv6 maszyny. Jest to informacja podawana w odpowiedzi na zapytanie proste.

Przykład rekordu AAAA:
oceanic.wsisiz.edu.pl. 86400 IN AAAA 2001:1a68:a::33

Rekord typu NS

Pole „Owner” zawiera nazwę DNS strefy. Informacja podawana przez rekord to pełna nazwa domenowa jednego z serwerów danej strefy. Uwaga: jeden z rekordów NS zawiera nazwę serwera podstawowego, ale nie ma tam informacji, że jest to serwer podstawowy.

Przykład rekordu NS:
wsisiz.edu.pl. 86400 IN NS see-you-later.wsisiz.edu.pl.

Rekord typu PTR:

Pole "Owner" zawiera nazwę DNS składającą się z adresu IP zapisanego "na odwrót" oraz prefiksu in-addr.arpa . Informacja podawana przez rekord to pełna nazwa domenowa maszyny, której adres IP jest zapisany "na odwrót" w polu "Owner". Jest to informacja podawana w odpowiedzi na zapytanie odwrotne.

Przykład rekordu PTR:
132.47.135.213.in-addr.arpa. 86400 IN PTR sz022.wsisiz.edu.pl.

Delegowanie stref przy użyciu rekordów zasobów

Jak już wcześniej wspomniano, delegowanie strefy jest zabiegiem mającym na celu utrzymanie rozmiarów plików bazy DNS w rozsądnych granicach. Aby delegowanie strefy powiodło się, w plikach strefy delegującej muszą się znaleźć następujące informacje: nazwa strefy delegowanej, oraz nazwa DNS i adres IP serwera autorytatywnego dla strefy delegowanej. Pierwsze dwa parametry są określane przy pomocy rekordu NS wiążącego nazwę strefy delegowanej z nazwą serwera tej strefy, natomiast trzeci – przy pomocy rekordu A wiążącego nazwę serwera strefy delegowanej z jego adresem IP. Oczywiście, w pliku strefy delegowanej musi znajdować się rekord SOA, wiążący nazwę strefy delegowanej z nazwą DNS podstawowego serwera tej strefy. Istotne jest, aby nazwa serwera strefy delegowanej w tym rekordzie była zgodna z nazwą serwera w odpowiednim rekordzie NS pliku strefy delegującej. Do zilustrowania powyższych warunków niech posłuży następujący przykład:

Załóżmy, że z hipotetycznej strefy mojafirma.com.pl. delegowana jest strefa wawa.mojafirma.com.pl. . Plik strefy mojafirma.com.pl. musi zawierać następujące rekordy:

| | | | |
|---|---|---|---|
| wawa.mojafirma.com.pl. | IN | NS | dns.wawa.mojafirma.com.pl. |
| dns.wawa.mojafirma.com.pl. | IN | A | 193.0.0.1 |

(193.0.0.1 jest oczywiście tylko przykładowym publicznym adresem IP), natomiast plik strefy wawa.mojafirma.com.pl. – następujące rekordy:

| | | | |
|---|---|---|---|
| wawa.mojafirma.com.pl. | IN | SOA | dns.wawa.mojafirma.com.pl. |
| dns.wawa.mojafirma.com.pl. | IN | A | 193.0.0.1 |

Zakładamy tu, że podstawowy serwer strefy wawa.mojafirma.com.pl. należy do domeny głównej tej strefy, ale **w ogólnym przypadku nie jest wymagane, aby serwer autorytatywny dla strefy należał do domeny głównej tej strefy**.

Zasady działania usługi DNS

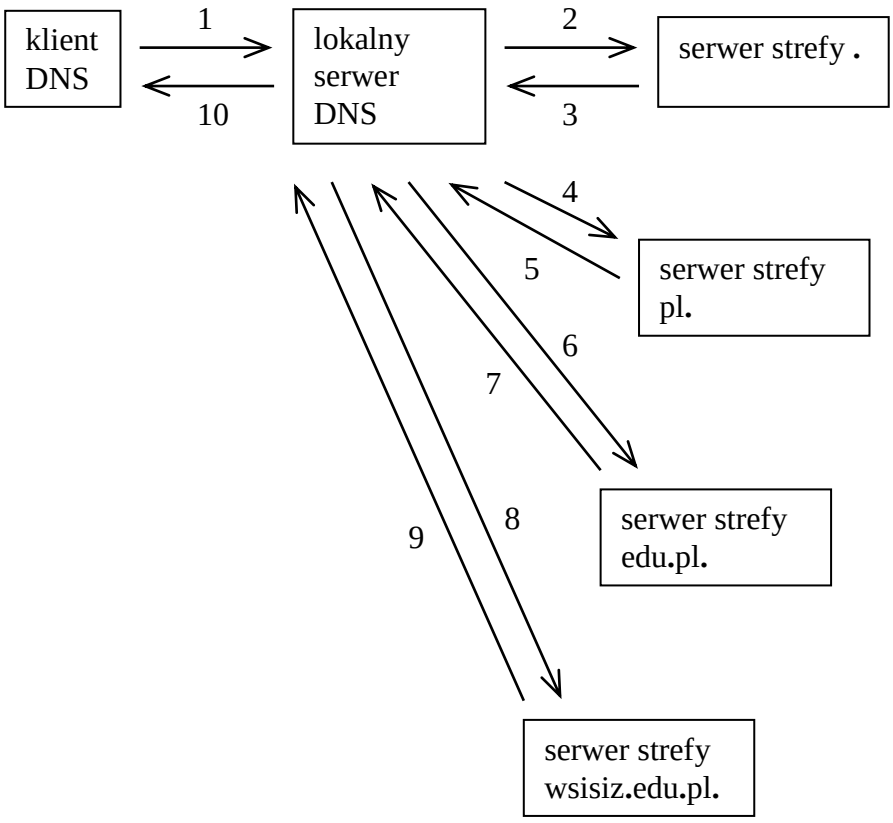
Klientem DNS może być dowolny komputer pracujący w oparciu o protokół TCP/IP. Użycie nazwy domenowej w poleceniu uruchamiającym aplikację sieciową, np. telnet sz123.wsisiz.edu.pl, albo wpisanie nazwy domenowej w polu adresu przeglądarki internetowej powoduje, w sposób niewidoczny dla klienta, wysłanie zapytania DNS do lokalnego serwera tej usługi. Serwer lokalny udziela odpowiedzi klientowi, w oparciu o własne zasoby, bądź zasoby innych serwerów. Istnieją dwa rodzaje zapytań DNS - zapytania proste, czyli o adres IP maszyny o podanej nazwie domenowej, oraz zapytania odwrotne, czyli o nazwę domenową maszyny o podanym adresie IP. Te drugie używane są zazwyczaj w celu wyeliminowania tzw. "DNS spoofing", czyli zabiegu polegającego na udzielaniu przez podstawiony serwer DNS fałszywych odpowiedzi na zapytania proste, aby umożliwić innej maszynie udawanie maszyny o określonej nazwie domenowej.

Chcąc ustalić adres IP maszyny o znanej nazwie domenowej, przykładowo - sz123.wsisiz.edu.pl. , klient DNS wysyła zapytanie do lokalnego serwera DNS (Adres lokalnego serwera jest jednym z parametrów konfiguracyjnych klienta DNS). Serwer lokalny wysyła zapytanie do serwera strefy . . Serwer strefy . udziela tzw. odpowiedzi referencyjnej (ang. Referral Answer), podając adres serwera strefy pl. (delegowanej ze strefy . ). W następnym kroku serwer lokalny wysyła zapytanie do serwera strefy pl. , który również udziela odpowiedzi referencyjnej, podając adres serwera strefy edu.pl. (zakładamy, że strefa

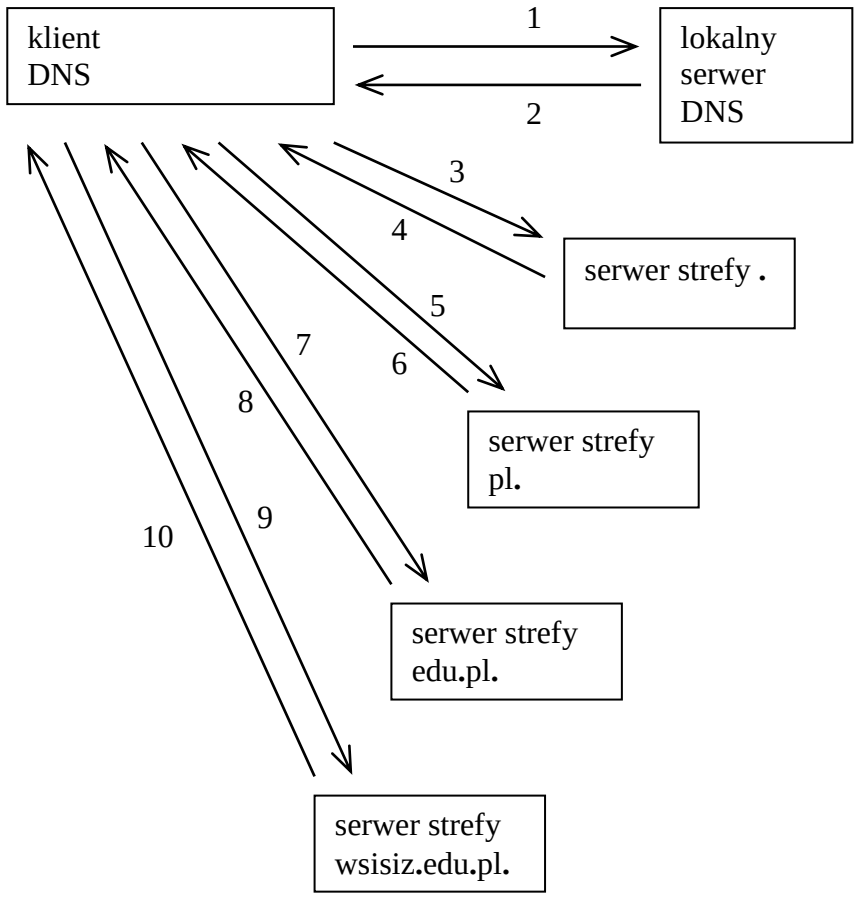
edu.pl. jest delegowana ze strefy pl. ). W kolejnym etapie serwer lokalny wysyła zapytanie do serwera strefy edu.pl. , który też udziela odpowiedzi referencyjnej, podając adres serwera strefy wsisiz.edu.pl. (zakładamy, że strefa wsisiz.edu.pl. jest delegowana ze strefy edu.pl. ). W ostatnim kroku serwer lokalny wysyła zapytanie do serwera strefy wsisiz.edu.pl. , który podaje adres IP maszyny sz123.wsisiz.edu.pl. udzielając tzw. odpowiedzi autorytatywnej (ang. Authoritative Answer). Po uzyskaniu adresu IP maszyny sz123.wsisiz.edu.pl.., lokalny serwer DNS przesyła go klientowi.

W miarę możliwości, lokalny serwer zapisuje do pamięci podręcznej (ang. DNS cache) uzyskiwane z innych serwerów informacje, aby przy kolejnych zapytaniach klientów nie musiał powtarzać procedury uzyskiwania adresów IP serwerów niektórych stref. Przechowywanie odpowiedzi DNS w pamięci podręcznej serwerów przyspiesza działanie usługi DNS, oraz zmniejsza obciążenie serwerów, a zwłaszcza serwerów strefy . i stref pierwszego poziomu. Ze swojej strony, klienci DNS zapisują w pamięci podręcznej informacje uzyskane z lokalnego serwera DNS, co zmniejsza ruch w sieci lokalnej, jak również obciążenie serwera lokalnego.

Opisany powyżej schemat działania usługi DNS nosi nazwę trybu rekurencyjnego. Polega on na tym, że lokalny serwer DNS otrzymuje od klienta zadanie ustalenia adresu IP maszyny o podanej nazwie domenowej (zapytanie proste), albo nazwy domenowej maszyny o podanym adresie IP (zapytanie odwrotne) i po wykonaniu tego zadania przesyła klientowi żądaną informację. W przypadku, gdy serwer DNS odmawia działania w trybie rekurencyjnym, usługa DNS działa w trybie iteracyjnym. Polega on na tym, że, zadanie odpytywania kolejnych serwerów DNS spoczywa na kliencie, a serwer lokalny przesyła klientowi tylko adres następnego serwera, z którym klient ma się komunikować (odpowiedź referencyjna). Administrator serwera DNS ma możliwość wyłączenia trybu rekurencyjnego i zastąpienia go trybem iteracyjnym. Należy zauważyć, że w podanym przykładzie, lokalny serwer DNS uzyskuje końcową odpowiedź w trybie iteracyjnym, gdyż właśnie na nim spoczywa zadanie odpytywania kolejnych serwerów DNS. Przyjęto tu założenie, że w celu uniknięcia zbyt dużego obciążenia, serwery stref . , pl. i edu.pl. najprawdopodobniej odmówią działania w trybie rekurencyjnym.




Schemat działania DNS w trybie rekurencyjnym




Schemat działania DNS w trybie iteracyjnym

Strefa wyszukiwania odwrotnego in-addr.arpa.

Specjalna strefa in-addr.arpa. została utworzona w przestrzeni DNS w celu dostarczenia informacji, w oparciu o którą serwery DNS mogą odpowiadać na zapytania odwrotne, tj. zapytania o nazwę domenową maszyny o podanym adresie IP. Nazwy DNS stref delegowanych z in-addr.arpa są to adresy zarejestrowanych sieci IP zapisane w porządku odwrotnym, do których dodany jest prefiks in-addr.arpa. . Jeśli, na przykład, jakiejś organizacji przyznano sieć klasy A o adresie 20.0.0.0, to odpowiada jej strefa 20.in-addr.arpa. Załóżmy, że sieć tę podzielono maską 16-bitową na 256 podsieci (każda podsieć ma rozmiar sieci klasy B) i dla każdej z nich ze strefy 20.in-addr.arpa. delegowano osobną strefę. Nazwy DNS delegowanych stref będą wówczas następujące: 0.20.in-addr.arpa. , 1.20.in-addr.arpa. , 2.20.in-addr.arpa. ,..., 255.20.in-addr.arpa. Jeśli sieć 20.1.0.0/16 zostanie następnie podzielona maską 24-bitową na 256 podsieci i dla każdej z nich ze strefy 1.20.in-addr.arpa. będzie delegowana osobna strefa, to powstaną w ten sposób strefy 0.1.20.in-addr.arpa. , 1.1.20.in-addr.arpa. , 2.1.20.in-addr.arpa. ,..., 255.1.20.in-addr.arpa.

Pliki bazy DNS znajdujące się w serwerach stref delegowanych z in-addr.arpa. muszą składać się m.in. z rekordów typu PTR. Rekordy PTR zawierają informację, na podstawie której wspomniane wyżej serwery udzielają odpowiedzi na zapytania odwrotne.

Załóżmy że chcemy włączyć strefę x w globalny system DNS. Procedura ta polega m.in. na rejestracji domeny głównej strefy x, w wyniku czego staje się ona strefą delegowaną z innej strefy, już włączonej w globalny DNS. Oprócz tego, dla x należy zarejestrować strefę

wyszukiwania odwrotnego, czyli strefę ois(x)**.**in-addr**.**arpa**.** , gdzie ois(x) oznacza odwrócony identyfikator (pod)sieci IP przydzielonej organizacji, która chce zarejestrować domenę x. Wówczas strefa ois(x)**.**in-addr**.**arpa**.** stanie się strefą delegowaną, pośrednio lub bezpośrednio, ze strefy in-addr.arpa**.** Zagwarantuje to dotarcie do serwera strefy ois(x)**.**in-addr**.**arpa**.** przez serwery stref położonych wyżej w hierarchii DNS, a tym samym umożliwi uzyskiwanie odpowiedzi na zapytania odwrotne dotyczące maszyn ze strefy x.

Klient DNS w systemie Red Hat Linux

Funkcje klienta DNS realizuje program o angielskiej nazwie „resolver". Działanie tego programu zależy od zawartości dwóch plików konfiguracyjnych - /etc/host.conf i /etc/resolv.conf . Pierwszy z tych plików podaje ustawienia opcji programu resolver. Oto niektóre z nich:

order: kolejność stosowania różnych metod odwzorowywania nazw
- hosts: ustalenie adresu IP na podstawie wpisu w /etc/hosts
- bind: ustalenie adresu IP w oparciu o usługę DNS
- nis: ustalenie adresu IP w oparciu o usługę NIS

trim: usunięcie nazwy domeny przy sprawdzaniu pliku /etc/hosts

multi: możliwość związania kilku adresów IP z jedną nazwą DNS w /etc/hosts

Przykładowa zawartość /etc/host.conf :

```
order hosts, bind
multi off
```

Plik /etc/resolv conf zawiera pewne ustawienia domyślne programu resolver:

domain: nazwa DNS domeny lokalnej

search: lista nazw DNS automatycznie dołączanych do przekazywanej programowi resolver nazwy maszyny

nameserver: adres IP lokalnego serwera DNS; może być więcej niż jeden taki wpis

Przykładowa zawartość pliku /etc/resolv.conf :

```
domain  wsisiz.edu.pl
search  wsisiz.edu.pl  ibspan.waw.pl
nameserver  213.135.44.40
nameserver  213.135.34.24
nameserver  217.17.34.10
nameserver  212.87.0.37
```

Polecenia diagnostyczne nslookup, host i dig

Polecenie host służy do uzyskiwania informacji z serwerów stref. Domyślnie, tzn. bez wskazania serwera strefy, informacja pobierana jest z serwera strefy lokalnej. Przykłady działania polecenia host:

host ns.icm.edu.pl : wypisuje adres IP maszyny o podanej nazwie DNS (ns.icm.edu.pl)

host –v ns.icm.edu.pl : wypisuje w formacie plików strefy informacje dotyczące maszyny ns.icm.edu.pl, m.in. zawartość rekordu typu A, na podstawie którego ustalany jest adres IP. Dodatkowo wypisywane są nazwy DNS serwerów autorytatywnych strefy icm.edu.pl

host –t ns redhat.com : wypisuje nazwy DNS serwerów autorytatywnych strefy redhat.com

host –t soa redhat.com : wypisuje nazwę DNS serwera podstawowego strefy redhat.com, oraz inne informacje zawarte w rekordzie SOA tej strefy

host 66.187.233.210 : wypisuje nazwę DNS maszyny o podanym adresie IP (66.187.233.210)

host –v 66.187.233.210 : wypisuje w formacie plików strefy informacje dotyczące maszyny o adresie 66.187.233.210, m.in. zawartość rekordu typu PTR, na podstawie którego ustalana jest nazwa DNS. Dodatkowo wypisywane są nazwy DNS serwerów autorytatywnych strefy wyszukiwania odwrotnego 233.187.66.in-addr.arpa , oraz adres IP serwera podstawowego tej strefy.

host –l wsisiz.edu.pl : wypisuje pełną zawartość plików wskazanej strefy (wsisiz.edu.pl). Polecenie to korzysta z pełnego transferu strefy (AXFR). Należy mieć na uwadze, że serwer strefy może odmówić jej pełnego transferu dla nieuprawnionego klienta.

host –l –v wsisiz.edu.pl : wypisuje pełną zawartość plików strefy, zachowując oryginalny format.