pasja-informatyki.pl

Sieci komputerowe – Windows Server #5

DNS & IIS

Damian Stelmach

Spis treści

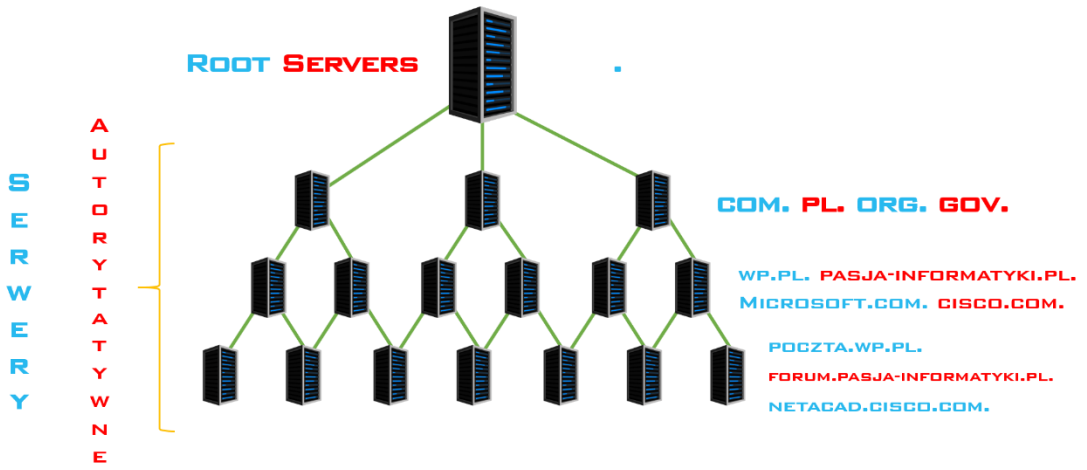
DNS (ang. Domain Name Service/System) to usługa sieciowa zamieniająca nazwy mnemoniczne, słowne, zrozumiałe dla nas ludzi, na adresy IP hostów w sieci i odwrotnie. Urządzenia sieciowe, komputery, tablety czy smartfony nie komunikują się w taki sposób jak my, ludzie za pomocą słów. Komunikują się za pomocą adresów IP. Stąd potrzeba zamiany nazw na te właśnie adresy, które to następnie dalej konwertowane są na ciągi zer i jedynek i w takiej formie transmitowane są przez sieć. Gdyby DNS nie działał to zamiast adresu domenowego, w polu adresu przeglądarki należałoby wpisać adres IP serwera, na którym strona ta jest hostowana, co zwyczajnie jest kłopotliwe i niezbyt intuicyjne.

DNS nie działa tylko w Internecie i nie odpowiada tylko za zwracanie klientom adresów ip serwerów, ma których hostowane są strony WWW. Stosowany jest również do lokalizacji komputerów, serwerów i usług w sieciach lokalnych, zapewnia dostęp aplikacjom do określonych zasobów, czy też pozwala na dostęp do sieci firmowych poprzez VPN. Doskonałym przykładem tego, ze DNS działa nie tylko w Internecie jest usługa Active Directory, która do poprawnego działania wymaga właśnie serwera DNS. Dlatego tak ważne jest, aby komputery, które z domeny Active Directory korzystają, a także kontrolery tych domen miały w swojej konfiguracji przypisane poprawne adresy IP serwerów DNS.

Na samym początku istnienia Internetu odwzorowania nazw na adresy IP zapisywane były w zwykłych plikach tekstowych (plikach hosts). Rozwój technologii informatycznych i sieci spowodował jednak, że sposób ten stał się mało wydajny i niewystarczający. Tak powstał DNS, którego używamy do dzisiaj, a jego bazą są setki tysięcy serwerów, rozsianych po całym świecie, przechowujących w swoich baza rekordy odwzorowań.

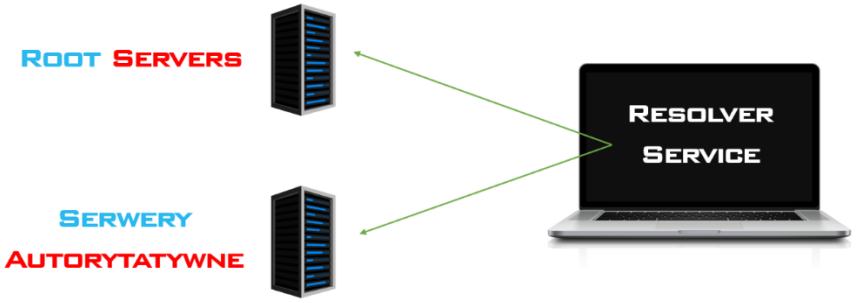
Struktura usługi DNS ma postać odwróconego drzewa, gdzie na szczycie znajdują się serwery główne, tak zwane Root Servers, reprezentowane przez znak kropki, której my nie widzimy, chociaż faktycznie ona tam jest, a poniżej serwery dla poszczególnych domen. Domeny drugiego poziomu to domeny typu com, pl, org czy też gov. Dalej mamy domeny trzeciego poziomu czyli wp.pl, pasja-informatyki.pl,

Microsoft.com, cisco.com itd. Następne w hierarchii są domeny typu poczta.wp.pl, forum.pasja-informatyki.pl czy netacad.cisco.com.

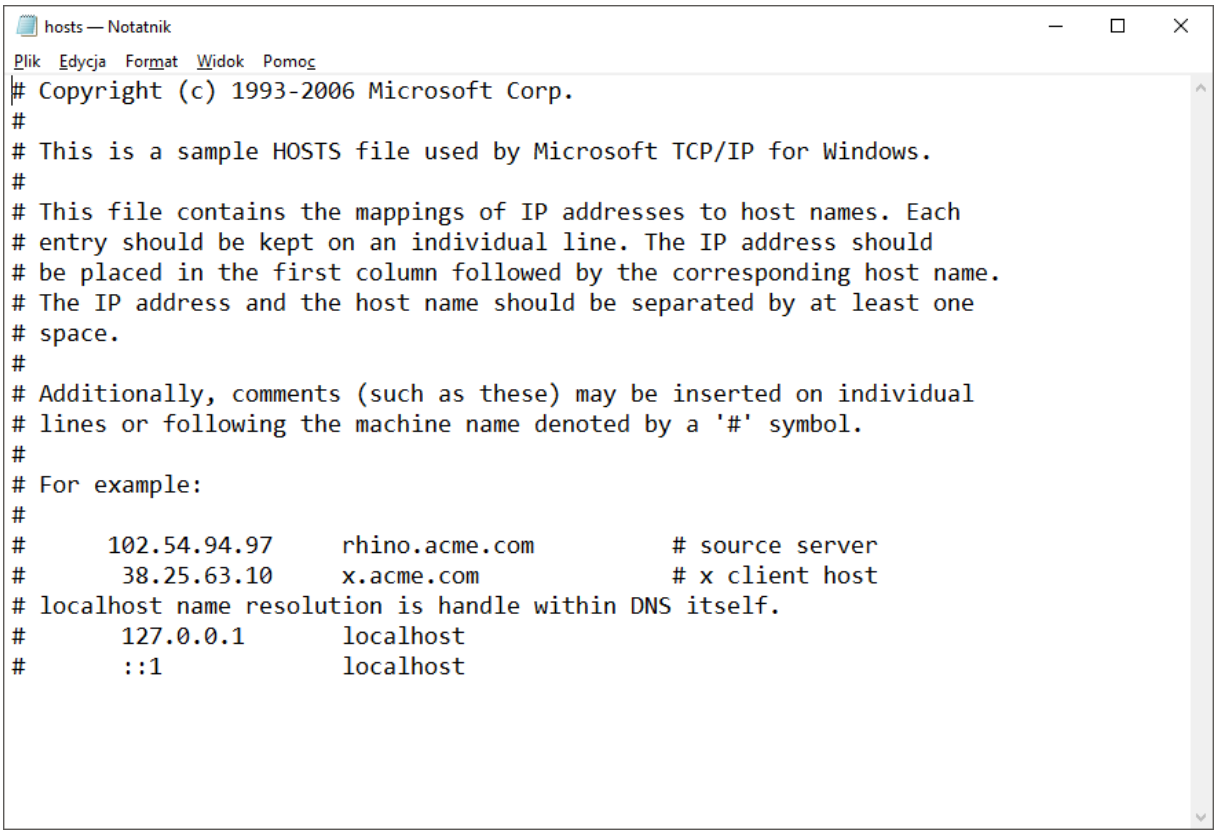


Każda domena, czyli każdy adres internetowy musi posiadać swój własny serwer. Mówi się o nim wówczas, że jest serwerem autorytatywnym dla domeny. Jeśli zakładacie swoją stronę w Internecie, to również ona musi mieć swój autorytatywny serwer DNS. Można sobie taki serwer skonfigurować we własnym zakresie i udostępniać go w sieci, ale najczęściej jest tak, że to operator waszej domeny, wasz usługodawca u którego ją wykupiliście zrobi to za was. Co do serwerów poziomu głównego to jest ich na całym świecie aż 13. To oczywiście nie jest liczba wybitnie duża, a wręcz bardzo mała, natomiast mają one swoje kopie rozlokowane w różnych zakątkach globu. Można ich lokalizację podejrzeć, wystarczy wejść na stronę root-servers.org. Znajdziemy na niej lokalizację serwerów root, a także ich adresy IP oraz nazwy firm, które nimi zarządzają.

Te dwa wymienione typy serwerów czyli serwery domeny głównej oraz serwery autorytatywne dla domen stanowią lwią cześć systemu nazw DNS. Do tego aby system był kompletny brakuje nam jeszcze klientów. Klientem systemu DNS jest usługa systemowa zwana z angielskiego resolver, która implementowana jest w każdym systemie operacyjnym. To właśnie ten resolver, a nie przykładowo przeglądarka internetowa odpowiedzialny jest za komunikację z serwerem DNS.



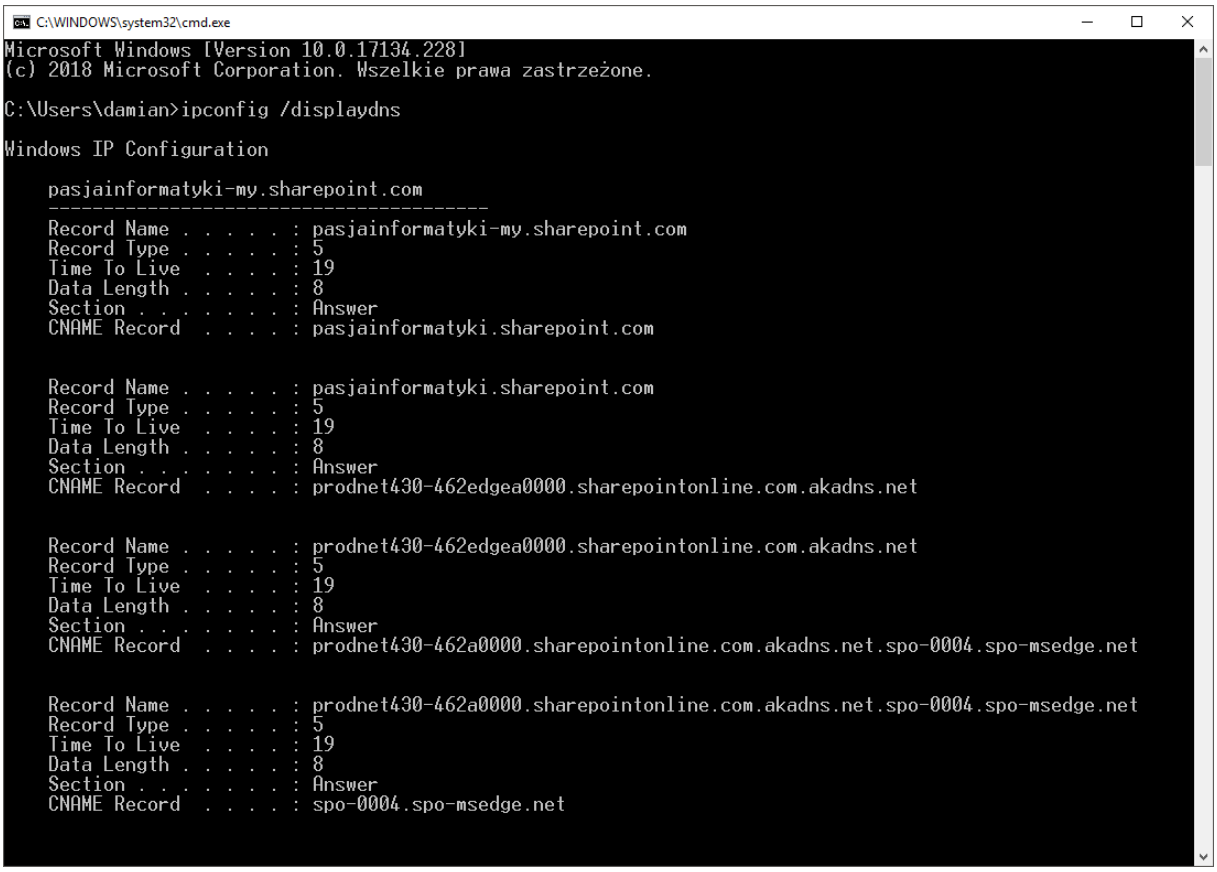
Każdy komputer czy też inny host, jeśli chce komunikować się z innymi hostami w sieci powinien mieć w swojej konfiguracji przypisany adres IP serwera DNS, który będzie tego hosta obsługiwał. W większości systemów operacyjnych podaje się go razem z konfiguracją adresacji. Najczęściej adresem serwera DNS na komputerze domowym będzie adres rutera dostępowego do Internetu lub też adres serwera, który przydzielił usługodawca internetowy. W przypadku komputerów firmowych no to już wszystko zależy od struktury sieci i liczby serwerów DNS jakie w firmie pracują. Bez względu na to czy korzystacie z komputera w domu czy też w corpo robocie to zanim resolver systemu operacyjnego, wyśle zapytanie do przypisanego serwera DNS przeszuka komputer w celu odnalezienie informacji na dysku twardym. A co będzie sprawdzał? No najpierw prześwietli plik hosts, który zawiera rozwiązania nazw przypisane na sztywno. Plik ten w Windowsach zapisany jest w takiej lokalizacji: **C:\Windows\System32\drivers\etc\hosts**



Jeśli chcecie się pobawić możecie tutaj podać adresy IP najczęściej odwiedzanych przez was stron, wówczas wasz komputer nie będzie musiał komunikować się z serwerem DNS w celu uzyskania informacji o adresie danej strony, weźmie ją sobie zwyczajnie z tego pliku. Oczywiście w rzeczywistości mało kto chce się w to bawić i raczej nie korzysta się z tej opcji, z wyłączeniem dużych sieci

korporacyjnych, gdzie czasami dodaje się wpisy w tych plikach z informacjami o adresach IP urządzeń sieciowych w nich pracujących.

Jeśli resolver nie odnajdzie intersującego go wpisu w pliku hosts, przeszuka własny cache, czyli pamięć podręczną, w której zapisał sobie wcześniejsze rozwiązania nazw. Do tej pamięci możemy sobie zajrzeć, wydając w konsoli polecenie ***ipconfig /displaydns***.



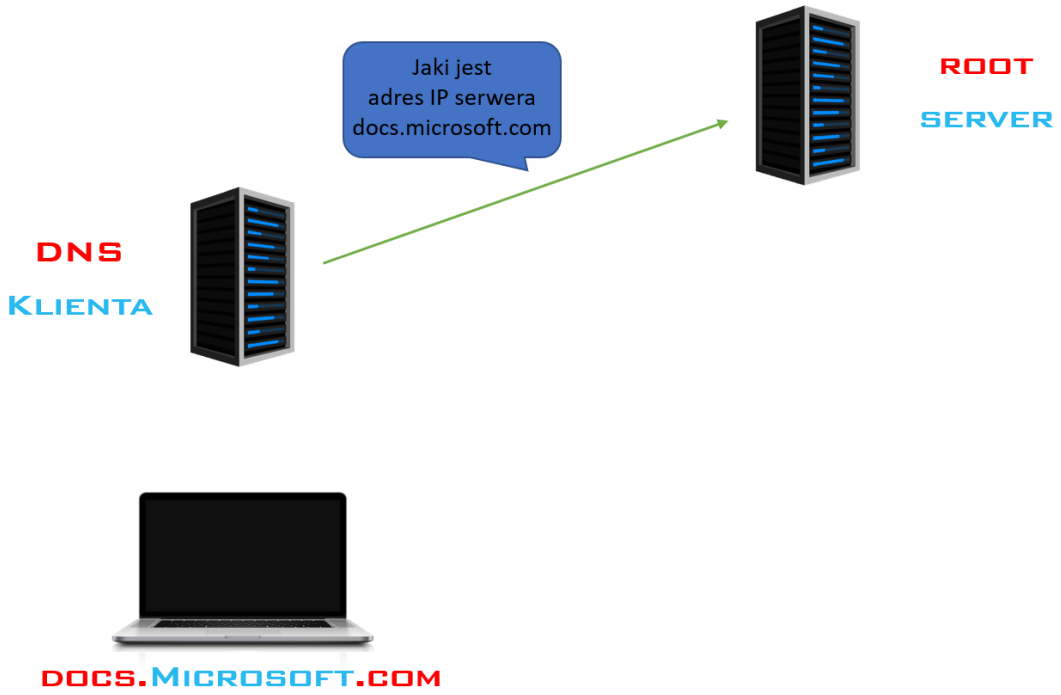
Widzimy tutaj rozwiązania, które zostały już wcześniej zrealizowane i zapisane po to aby nie korzystać z serwera DNS, jeśli nazwa została już wcześniej rozwiązana. Cache czyszczony jest po każdym restarcie komputera, natomiast można go też wyczyścić ręcznie, wykonując polecenie ***ipconfig /flushdns***. Jeśli i w cache'u resolver nie odnajdzie intersującego go wpisu, czyli rozwiązania nazwy dopiero następuje komunikacja z zewnętrznym serwerem DNS.

Zapytania do serwerów DNS mogą być zapytaniami rekurencyjnymi lub też iteracyjnymi. Rekurencja wymaga od serwera podania adresu IP, którego żąda klient lub też zwrócenia komunikatu o błędzie, np. niepoprawnej nazwie domenowej. W przypadku iteracji, zapytania iteracyjnego, serwer zobligowany jest do podania najlepszej możliwej informacji jaką obecnie posiada, z tym że może to być, ale wcale nie musi adres serwera, o którego jest odpytywany, może to być np. informacja gdzie dalej wysłać zapytanie aby otrzymać stosowną odpowiedź.

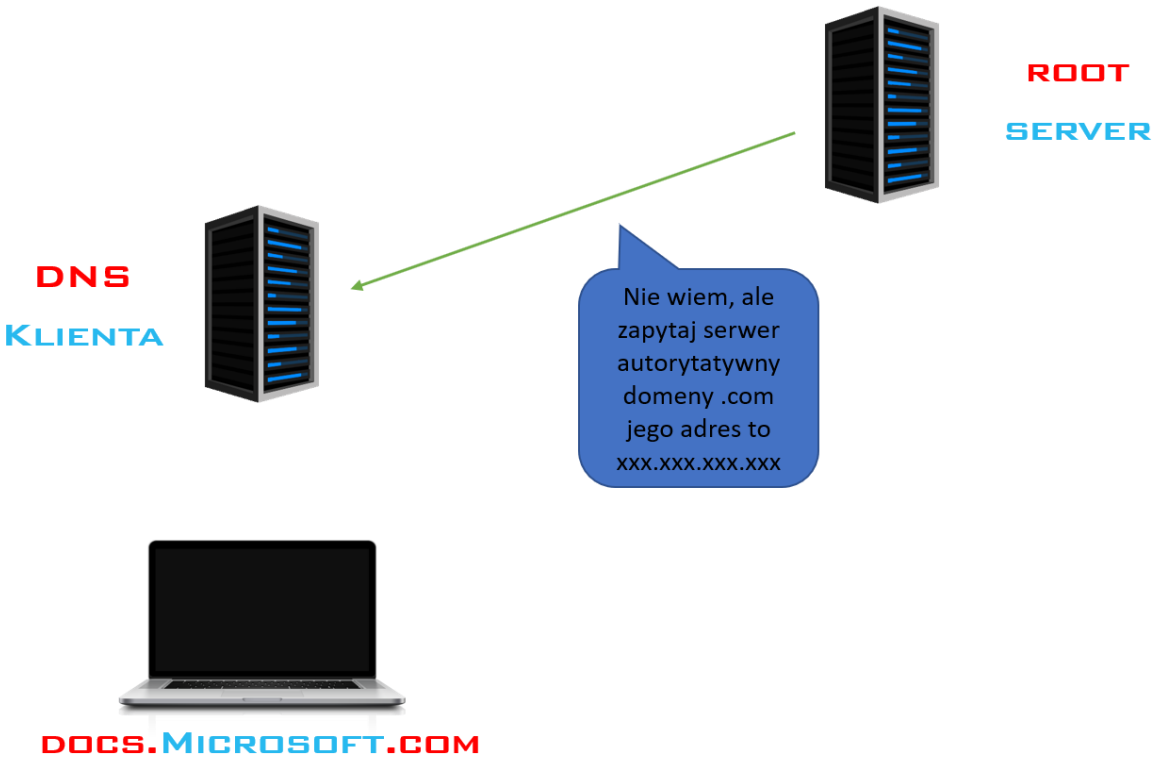
Załóżmy, że chcemy wejść na stronę **docs.microsoft.com**. Resolver wysyła zapytanie rekurencyjne zamiany nazwy do serwera, który jest do niego przypisany w konfiguracji.

Jeśli ten serwer posiada w swojej bazie lub buforze żądane rozwiązanie nazwy na IP, odpowiada stosownym komunikatem, zawierającymi adres IP tego szukanego serwera. Serwer posiadał adres, no to go klientowi przekazał.

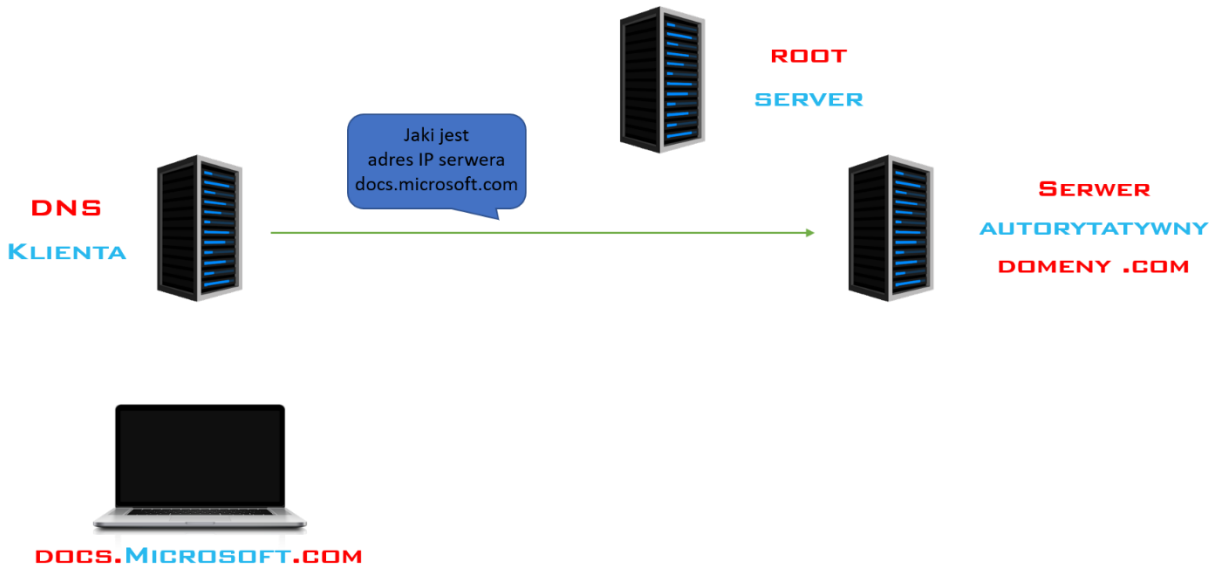
Jeśli rozwiązania natomiast nie posiada, to przesyła żądanie dalej, do jednego z serwerów głównych.



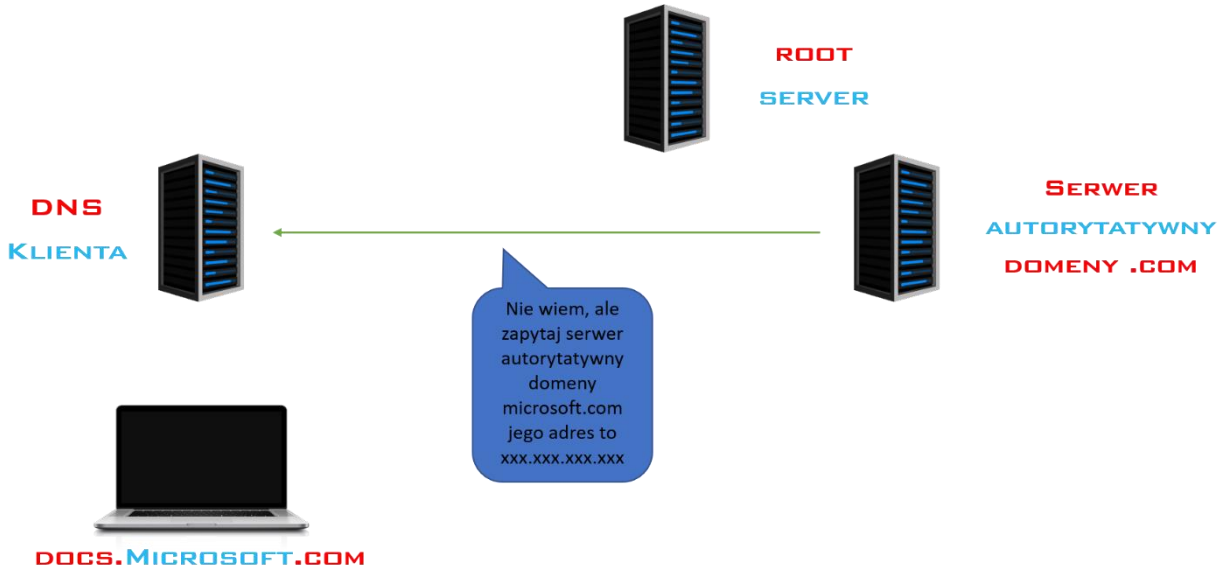
Serwer główny takiego rozwiązania posiadać nie musi, więc odeśle komunikat z informacją, jaki jest adres serwera dla domeny com.



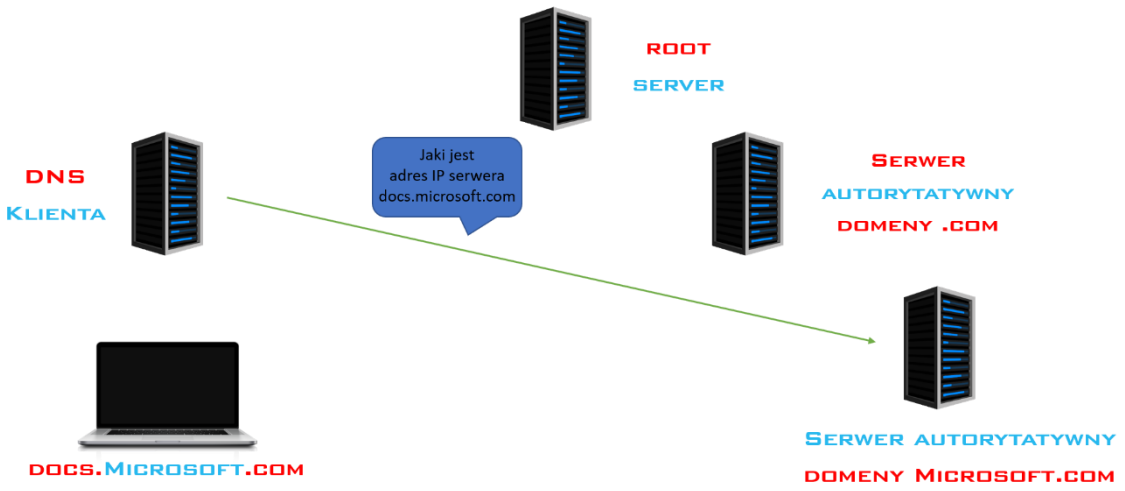
Następnie przypisany do komputera serwer DNS wyśle zapytanie do serwera autorytatywnego dla domeny com.



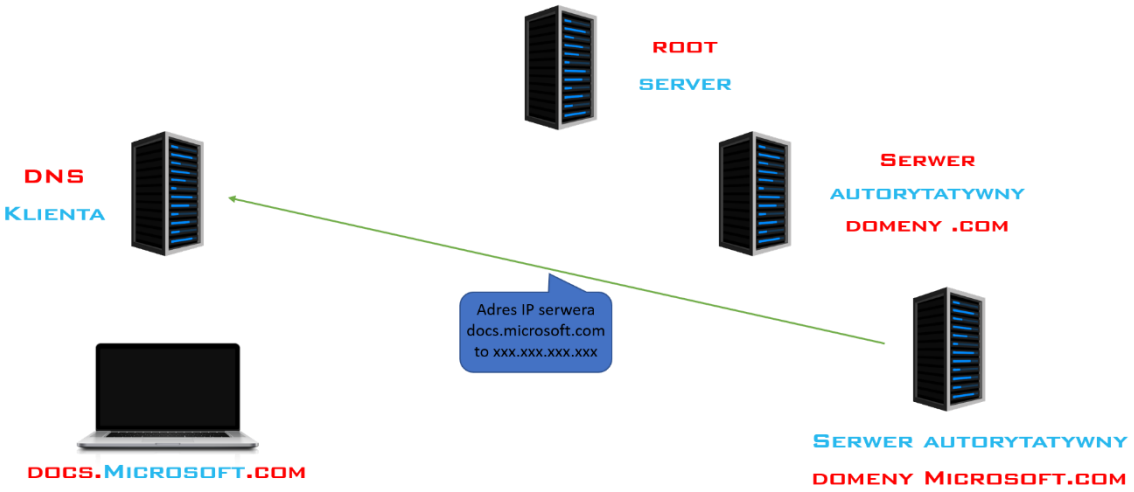
Ten również może nie mieć w swojej pamięci i bazie informacji jaki jest adres IP domeny docs.microsoft.com, ale odeśle do naszego serwera informacje z adresem IP serwera autorytatywnego dla domeny microsoft.com.



Wówczas nasz serwer wyśle zapytanie do serwera autorytatywnego dla domeny microsoft.com

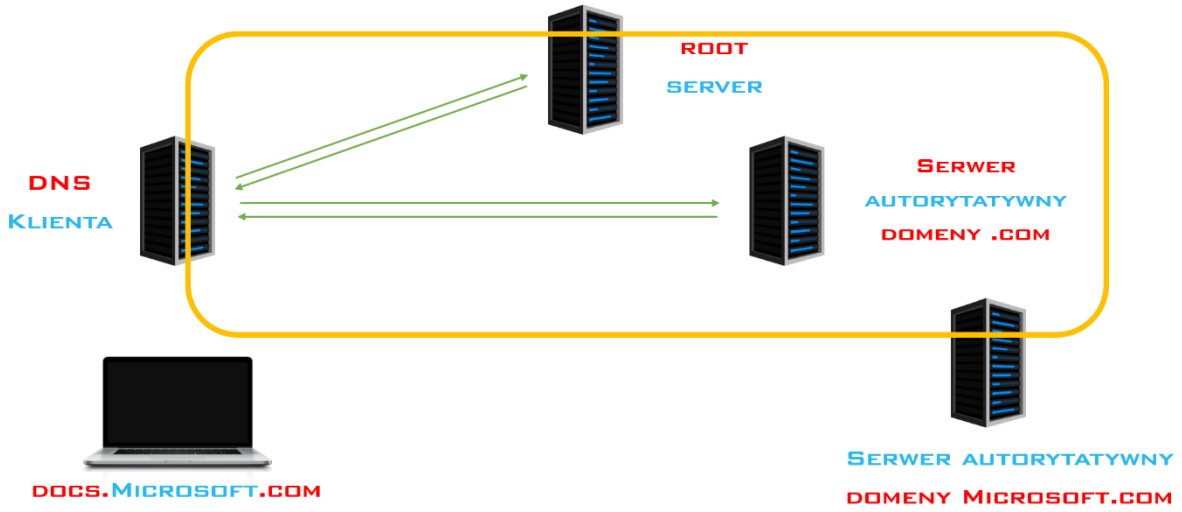


Załóżmy, że ten posiada w swojej bazie odpowiedni rekord, odpowiednie rozwiązanie nazwy, także w odpowiedzi prześle adres IP serwera na którym jest hostowana szukana strona.



Ten adres zostanie przekazany z serwera DNS do naszego komputera i to zakończy proces rozwiązywania nazwy dla domeny docs.microsoft.com.

To co się wydarzyło tutaj:



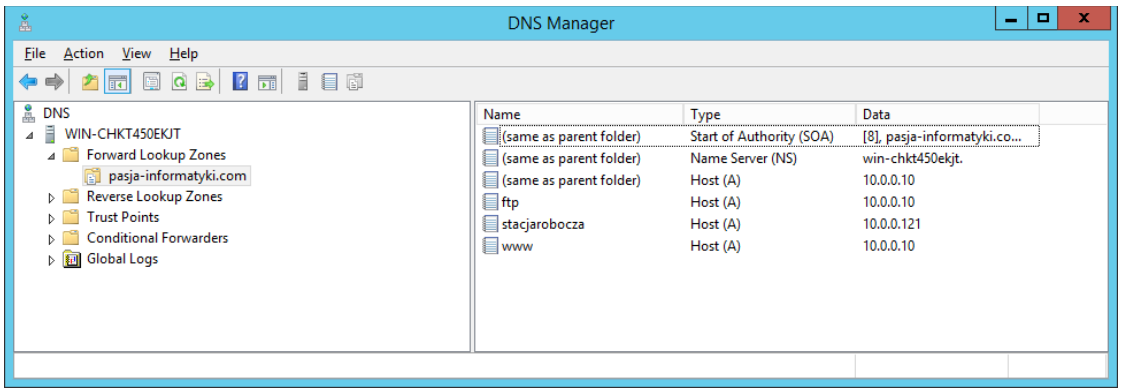
to były już zapytania iteracyjne, ponieważ te serwery nie wysyłały w odpowiedziach adresu IP domeny docs.microsoft.com, ale informacje, gdzie tej domeny szukać. Tak więc jak widzicie, stosuje się w procesie rozwiązywania nazw zarówno zapytania iteracyjne jak i rekurencyjne.

Tak to wygląda w teorii, jeśli chodzi o metody zapytań. Musicie jeszcze wiedzieć o tym, że na każdym z wymienionych etapów występuje proces cache'owania, czyli zapisywania już wcześniej zrealizowanych zapytań do bufora. Zdecydowanie przyspiesza to działanie systemu DNS na świecie. Gdyby za każdym razem, pojedyncze zapytanie DNS było przesyłane od serwera do serwera, jak zostało to pokazane, strasznie obciążyłoby cała sieć Internet, dlatego też w rzeczywistości proces ten nie składa się z aż tylu etapów, ponieważ poszczególne serwery zapisują rozwiązane już żądania w swoich pamięciach podręcznych.

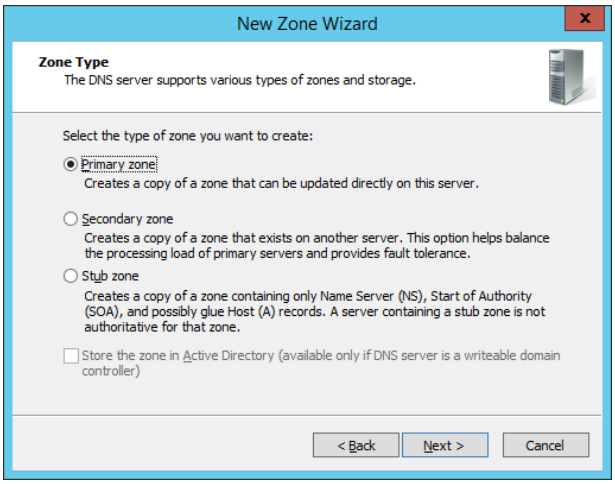
Dane na serwerach DNS, jak w każdej bazie danych, przechowywane są w tak zwanych rekordach. Każde odwzorowanie nazwy na IP i nie tylko zapisane jest w postaci pojedynczego rekordu. Typów rekordów DNS jest mnóstwo, najważniejsze z nich znajdziecie w tabeli poniżej:

Rodzaj rekordu	Opis
A	Mapowanie nazwy na IPv4
AAAA	Mapowanie nazwy na IPv6
CNAME	Alias nazwy rekordu, pozwala używać kilku rekordów odnoszących się do jednego hosta
MX	Mapowanie nazwy domeny na nazwę serwera mejlowego
PTR	Mapowanie adresu IP na nazwę hosta
NS	Rekord określający adres serwera dla domeny/strefy
SOA	Rekord określający serwer autorytatywny dla domeny/strefy
SRV	Rekord zawierający informację o lokalizacji określonej usługi
ISDN	Mapowanie nazwy hosta na numer telefonu
KEY	Identyfikacja klucza publicznego dla domeny
SIG	Rekord podpisu kryptograficznego

Na każdym serwerze DNS można utworzyć dwa rodzaje stref przeszukiwań rekordów: **strefę wyszukiwania wprzód** (ang. forward lookup zone) oraz **strefę wyszukiwania wstecz** (ang. reverse lookup zone). Zadaniem stref wyszukiwania wprzód jest generalnie mapowanie nazw domenowych na adresy IP, np. jan.firma.com -> 192.168.12.30. Strefy wsteczne, wykonują jak można się domyśleć zadania odwrotne, czyli zajmują się mapowaniem adresów IP hostów na ich nazwy, np. 10.0.0.10 -> dns.pasja-informatyki.com (z tego korzysta m.in. Active Directory). Strefy wsteczne, wykorzystują rekordy typu PTR (ang. pointer record), inaczej niż strefy wprzód, które to wykorzystują rekordy typy A, AAAA, MX czy CNAME. Nazwa strefy to zaznaczaj nazwa domeny, którą dany serwer ma obsługiwać, dla której ma być serwerem autorytatywnym. Rekordy w tej strefie, to zbiór nazw hostów i ich adresów IP, działających w ramach danej domeny.



Tworząc strefy na serwerze DNS (zarówno strefy wyszukiwania wprzód jak i wstecz) możemy wybrać jedne z trzech dostępnych typów stref:



- Strefę główną
- Strefę pomocniczą
- Strefę skrótową

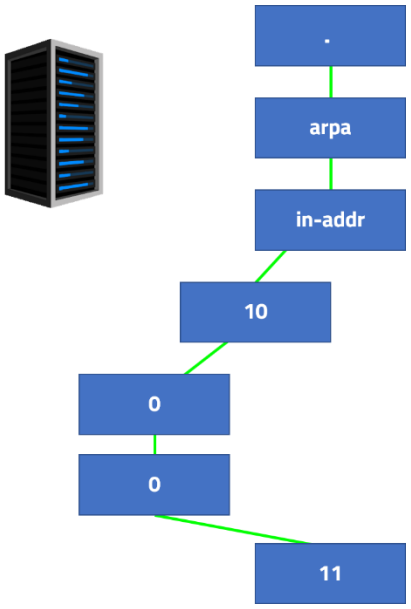
Różne strefy, tworzone są na osobnych maszynach, w celu zagwarantowania dostępności tej usługi dla klientów. **Strefa główna** to strefa zawierająca rekordy dla domeny, w niej te rekordy można tworzyć i dodawać. **Strefa pomocnicza** tworzona jest na osobnej maszynie i zawiera ona kopie rekordów ze strefy głównej. Do niej rekordów dodawać nie można, jest to tak zwana strefa tylko do odczytu. Strefa skrótowa natomiast, to strefa nieposiadająca w bazie rekordów, jej zadaniem jest tylko przekazywanie żądań od klientów DNS do strefy głównej oraz

pomocniczej. Na serwerach Windowsowych, można jeszcze tworzyć strefy powiązane z usługą Active Directory, jeśli ta na serwerze jest zainstalowana i skonfigurowana.

Wyszukiwanie wstecz stosuje inną metodę mapowania aniżeli wyszukiwanie w przód. Zamiast przestrzeni nazw, stosuje się przestrzeń adresów IP. W cały Internecie służy do tego specjalna domena o nazwie **.in-addr.arpa**. Każda strefa wyszukiwania wstecznego tworzona jest w oparciu o domenę .in-addr.arpa i adres IP sieci, w jakiej DNS pracuje. Sieć w jakiej konfigurowany był nasz DNS ma adres 10.0.0.0 z maską 24 bitową, dlatego też strefa wsteczna będzie miała nazwę **0.0.10.in-addr.arpa**. Przykłady nazw stref wstecznych, stosujących inna adresację sieci widać poniżej:

ADRES SIECI	NAZWA STREFY
10.0.0.0/24	0.0.10.IN-ADDR.ARPA
10.0.0.0/16	0.10.IN-ADDR.ARPA
172.16.0.0/24	0.16.172.IN-ADDR.ARPA
192.168.1.0/24	1.168.192.IN-ADDR.ARPA

Każdy pojedynczy oktet adresu IP (w tym przypadku IPv4) stanowi domenę podrzędną dla domeny .in-addr.arpa. Dla przykładowego adresu IP 10.0.0.11, domeną pierwszego poziomu będzie 10.in-addr.arpa. Domena taka zwierać może do 256 (2^8) domen podrzędnych. Dla naszego przykładu domeną podrzędną dla 10.in-addr.arpa, będzie domena 0.10.in-addr.arpa, która również może zawierać do 256 domen podrzędnych, a dla naszego przykładu będzie to domena 0.0.10.in-addr.arpa i to jest nazwa naszej strefy wyszukiwania wstecznego, w której znajdują się rekordy PTR hostów w naszej sieci.



ipconfig /all – wyświetla rozszerzoną konfigurację IP hosta, w tym adres serwera DNS

ipconfig /displaydns – wyświetla zawartość pamięci podręcznej resolver'a

ipconfig /registerdns – rejestruje klienta w domenie DNS

nslookup – wyświetla informacje związane z serwerem DNS obsługującym klienta