Politechnika Łódzka
Instytut Informatyki Stosowanej

Administracja i bezpieczeństwo systemów sieciowych

Laboratorium

Ćwiczenie nr 3.

Usługi DNS w systemie Windows

1. Cel ćwiczenia

Celem ćwiczenia jest zainstalowanie, uruchomienie i skonfigurowanie serwera DNS w systemie Windows.

2. Wstęp

Podstawa technicznego systemu DNS jest ogólnoświatowa sieć serwerów. Przechowują one informacje na temat adresów domen. Każdy wpis zawiera nazwę oraz odpowiadający jej adres IP. Wpisy udostępniane są automatycznie, co pozwala na pracę Internetu. DNS to również protokół komunikacyjny. Opisuje on sposób łączenia się klientów z serwerami DNS. Częścią specyfikacji protokołu jest również zestaw zaleceń, jak aktualizować wpisy w bazach domen internetowych. Po całym świecie rozsiane są serwery DNS, które odpowiadają za obsługę poszczególnych adresów internetowych. Listę 13 głównych serwerów odpowiedzialnych za obsługe poszczególnych domen najwyższego poziomu można pobrać z ftp://ftp.rs.internic.net/domain/named.root.

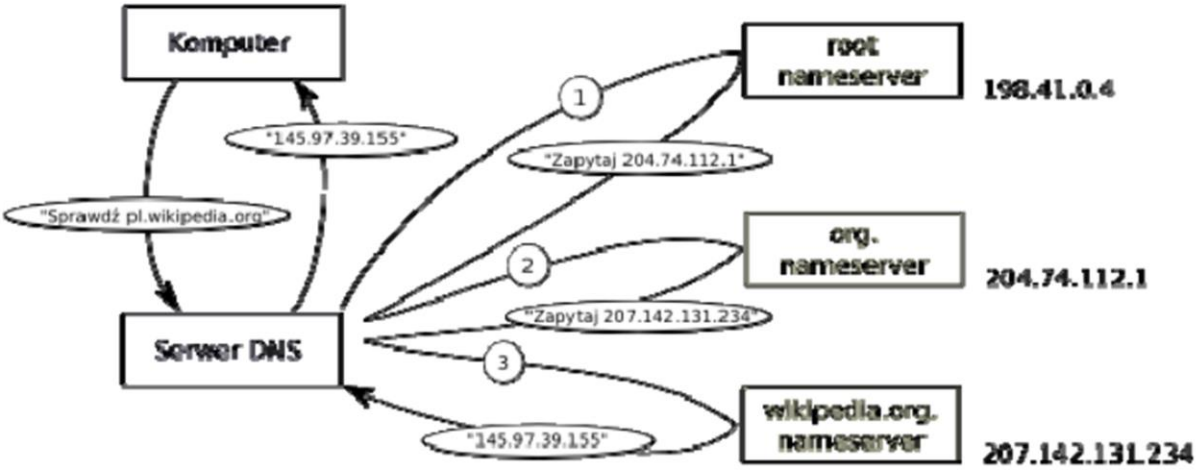
System DNS posiada następujące cechy:

- Nie ma jednej centralnej bazy danych adresów IP i nazw. Najważniejsze jest te 13 serwerów, które są rozrzucone na różnych kontynentach.
- Serwery DNS przechowują dane tylko wybranych domen.
- Każda domena ma co najmniej 2 serwery DNS obsługujące ja, jeśli wiec nawet któryś z nich będzie nieczynny, to drugi może przejąć jego zadanie.
- Serwery DNS przechowują przez pewien czas odpowiedzi z innych serwerów (ang. caching), a wiec proces zamiany nazw na adresy IP jest często krótszy niż w podanym przykładzie.
- Każdy komputer może mieć wiele różnych nazw. Na przykład komputer o adresie IP 207.142.131.245 ma nazwę pl.wikipedia.org oraz de.wikipedia.org.
- Czasami pod jedna nazwa może kryć się więcej niż 1 komputer po to, aby jeśli jeden z nich zawiedzie, inny mógł spełnić jego role.
- Jeśli chcemy przenieść serwer WWW na inny szybszy komputer, z lepszym łączem ale z innym adresem IP, to nie musimy zmieniać adresu WWW strony, a jedynie w serwerze DNS obsługującym domenę poprawiamy odpowiedni wpis.

- Protokół DNS posługuje się do komunikacji głównie protokołem UDP.
- Serwery DNS działają na porcie numer 53.

Przykład działania systemu DNS

Na rysunku nr 1 przedstawiono przykład działania usługi DNS.



Rys. 1. Przykład działania usługi DNS.

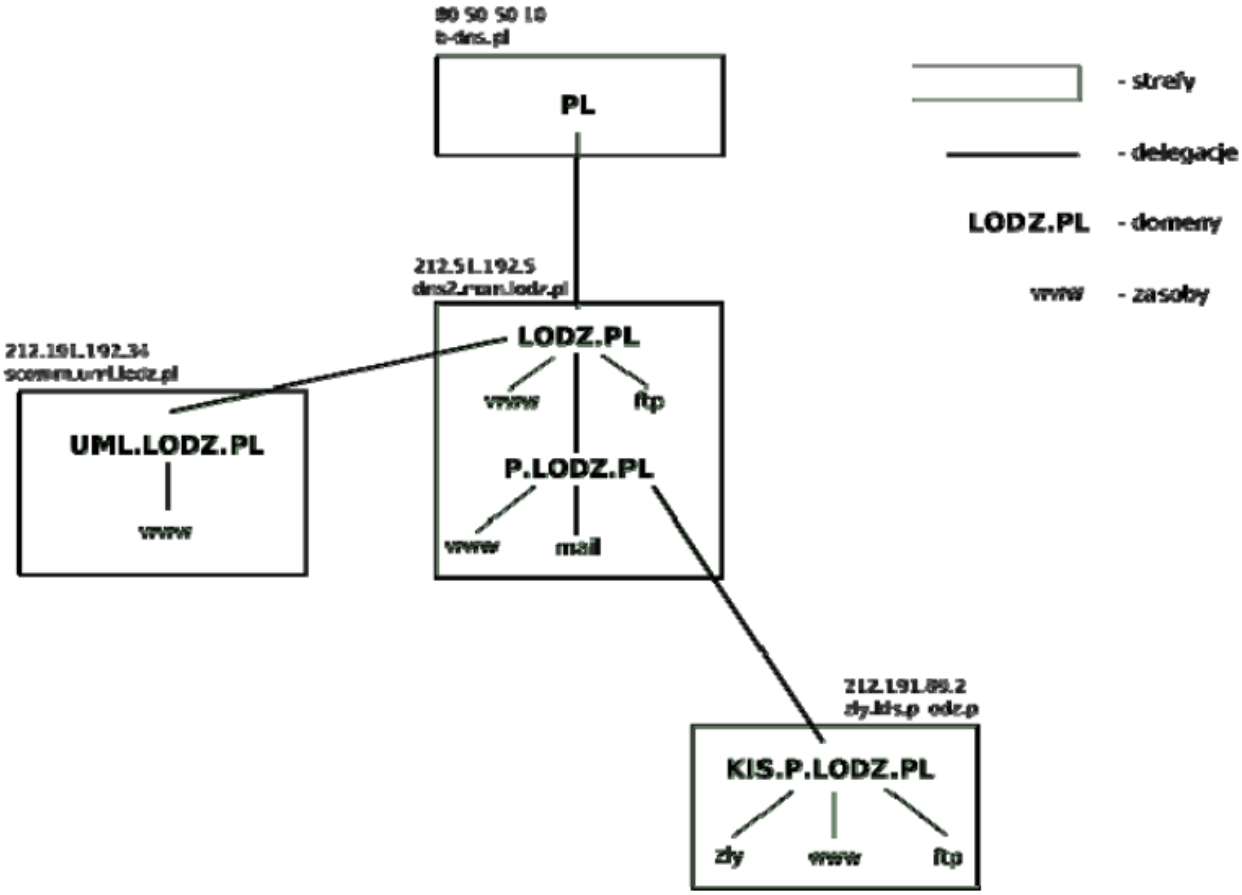
Składowe systemu DNS

Strefa DNS jest zbiorem plików lub rekordów (mówiąc precyzyjniej, bazą danych wpisów rekordów zasobów), które odpowiadają fragmentom hierarchicznej przestrzeni nazw DNS. Strefy DNS są wykorzystywane do określania tych serwerów DNS, które są odpowiedzialne (autorytatywne) za udzielanie odpowiedzi na zapytania o rozwiązanie nazwy dotyczącej danej części hierarchii DNS. Strefy DNS różnią się od domeny tym, że strefy mogą obejmować jedną lub wiele domen DNS. Strefa rozpoczyna się jako baza danych dla jednej nazwy domeny DNS. Jeśli poniżej domeny użytej do utworzenia strefy są dodane inne domeny, mogą one być się częścią tej samej strefy lub mogą należeć do innej strefy. Po dodaniu poddomeny może ona być:

- Zarządzana i dołączona jako część pierwotnych rekordów strefy, lub
- Delegowana do innej strefy utworzonej w celu obsługi poddomeny

Na przykład na rysunku 2 przedstawiono fragment domeny lodz.pl, która zawiera nazwy domen na obszarze Łodzi. Kiedy domena lodz.pl jest po raz pierwszy tworzona na jednym serwerze, jest konfigurowana jako pojedyncza strefa dla całego obszaru nazw DNS sieci komputerowej w Łodzi. Jeśli jednak w domenie p.lodz.pl wystąpi potrzeba użycia poddomen,

musza one zostać dołączone do tej strefy albo delegowane do innej strefy. W tym przykładzie domena p.lodz.pl ma nową poddomenę uml.p.lodz.pl, delegowaną ze strefy p.lodz.pl i zarządzaną w swojej własnej strefie. Jednak strefa p.lodz.pl musi zawierać kilka rekordów zasobów, aby zapewnić informacje o delegowaniu, które odwołują się do serwerów DNS autorytatywnych dla delegowanej poddomeny uml.p.lodz.pl. Jeśli w strefie p.lodz.pl nie będzie stosowane delegowanie do poddomeny, wszelkie dane dotyczące tej poddomeny pozostaną częścią strefy p.lodz.pl. Na przykład poddomena p.lodz.pl nie jest delegowana, lecz jest zarządzana przez strefę lodz.pl.



Rys. 2. Strefy i domeny.

Serwer podstawowy jest autorytatywnym dla strefy serwerem nazw. Wszystkie zadania administracyjne związane z ta strefą (takie jak tworzenie poddomen wewnątrz strefy lub inne podobne zadania administracyjne) muszą być wykonane na serwerze podstawowym. Dodatkowo zmiany związane ze strefą lub modyfikacje czy dodawanie kolejnych rekordów zasobów w pliku tej strefy musi być przeprowadzone na serwerze podstawowym. Dla każdej strefy istnieje serwer podstawowy.

Serwer pomocniczy jest zapasowym serwerem DNS. Odbiera on od serwera podstawowego wszystkie swoje pliki stref w czasie transferu stref. Może istnieć wiele serwerów pomocniczych dla danej strefy – tyle, ile jest konieczne, aby zapewnić zrównoważenie obciążenia, odporność na uszkodzenia i zredukowanie ruchu w sieci. Ponadto każdy serwer DNS może być serwerem pomocniczym dla jednej lub więcej stref.

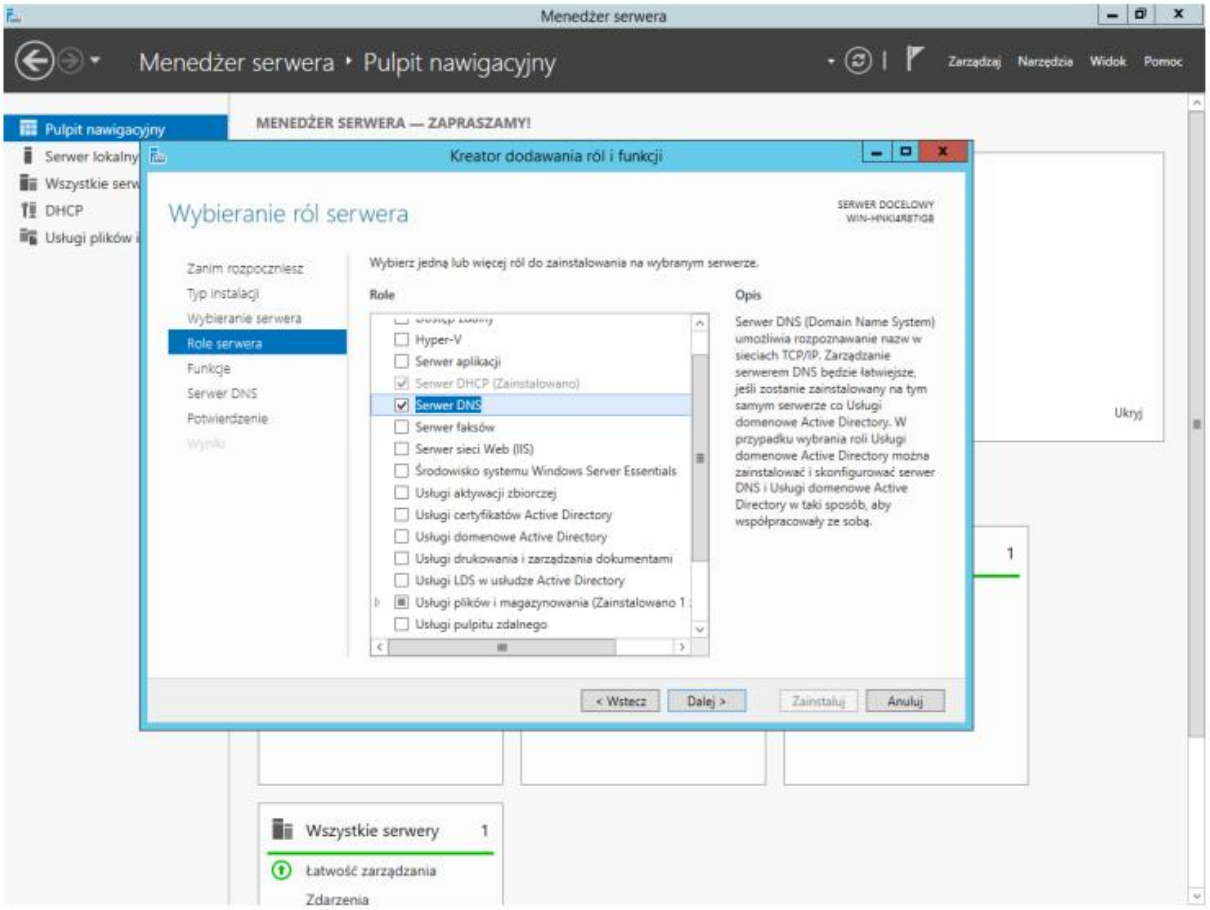
Najważniejsze typy rekordów DNS oraz ich znaczenie:

- **rekord A -** rekord adresu (ang. address record) przypisuje do nazwy domeny DNS 32bitowy adres IPv4.
- **rekord AAAA -** rekord adresu IPv6 (ang. IPv6 address record) mapuje nazwę domeny DNS na jej 128 bitowy adres IPv6.
- **rekord CNAME -** rekord nazwy kanonicznej (ang. canonical name record) ustanawia alias nazwy domeny. Wszystkie wpisy DNS oraz poddomeny są poprawne także dla aliasu.
- **rekord MX -** rekord wymiany poczty (ang. mail exchange record) mapuje nazwę domeny DNS na nazwę serwera poczty.
- **rekord PTR -** rekord wskaźnika (ang. pointer record) tworzy powiązanie pomiędzy adresem IP i nazwa hosta w strefach wyszukiwania wstecznego. (ang. reverse DNS lookup).
- **rekord NS -** rekord serwera nazw (ang. name server record) mapuje nazwę domenowa na listę serwerów DNS dla tej domeny. Każdy serwer DNS, zarówno podstawowy, jak i pomocniczy, powinien zostać zadeklarowany przy pomocy tego rekordu.
- **rekord SOA -** rekord adresu startowego uwierzytelnienia (ang. start of authority record) ustala serwer DNS dostarczający autorytatywne informacje o domenie internetowej.
- **rekord SRV -** rekord usługi (ang. service record) pozwala na zawarcie dodatkowych informacji dotyczacych lokalizacji danej usługi, która udostepnia serwer wskazywany przez adres DNS.
- **rekord TXT** - rekord ten pozwala dołączyć dowolny tekst do rekordu DNS. Rekord ten może być użyty np. do implementacji specyfikacji Sender Policy Framework.
- inne typy rekordów dostarczają informacje o położeniu hosta (np. rekord LOC) lub o danych eksperymentalnych.

Serwery podstawowe powinny zawierać strefy wyszukiwania do przodu oraz strefy wyszukiwania wstecznego dla danej domeny. Wyszukiwanie do przodu umożliwia zmianę nazw domen na adresy IP. Wyszukiwanie wsteczne pozwala potwierdzić zapytania DNS poprzez znalezienie nazw odpowiadających podanym adresom IP.

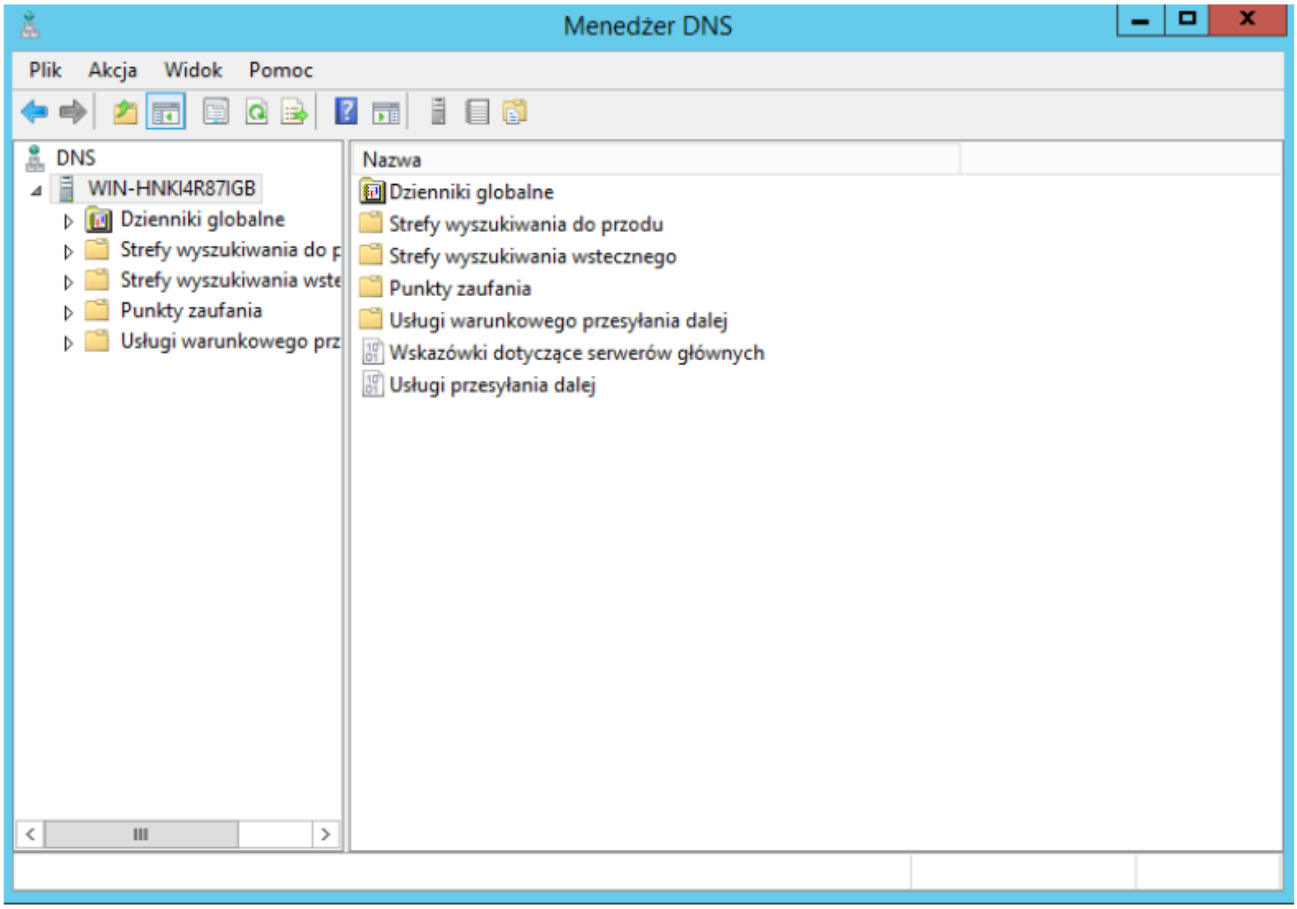
3. Instalacja i konfiguracja serwera

W celu instalacji usługi DNS w Menedżerze serwera zaznacz rolę Serwer DNS (rys. 3).



Rys. 3. Dodanie roli serwera DNS.

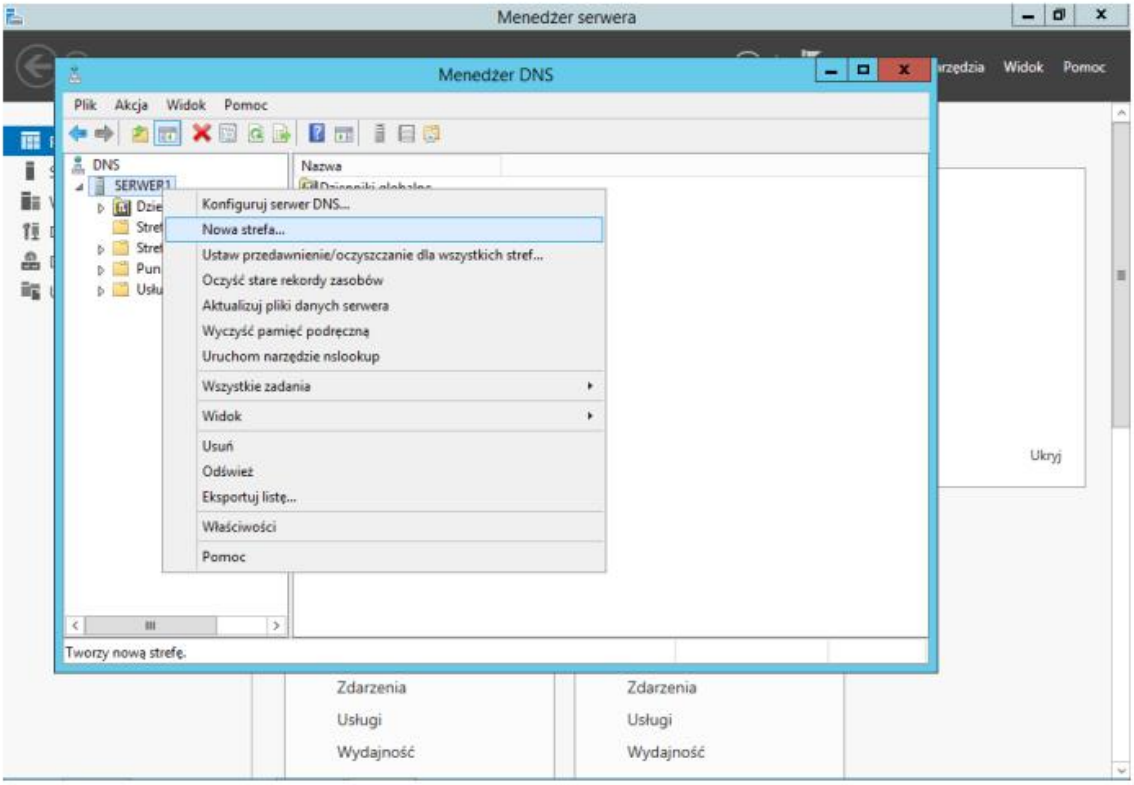
W celu konfiguracji serwera należy uruchomić konsolę Menedżer DNS, dostępną m.in. w menu Narzędzia Menedżera serwera (rys. 4).



Rys. 4. Konsola zarządzania usługą DNS.

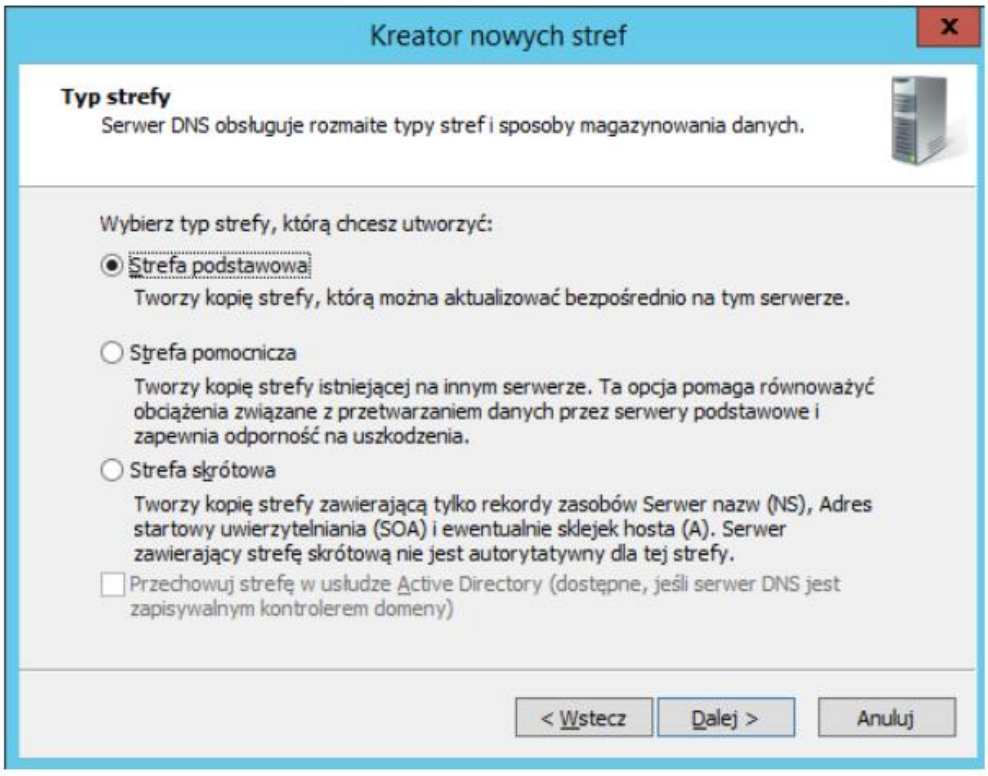
3.1. Utworzenie nowej strefy.

Aby utworzyć nową strefę należy w menu kontekstowym serwera DNS wybrać opcję Nowa strefa (rys. 5).



Rys. 5. Tworzenie nowej strefy.

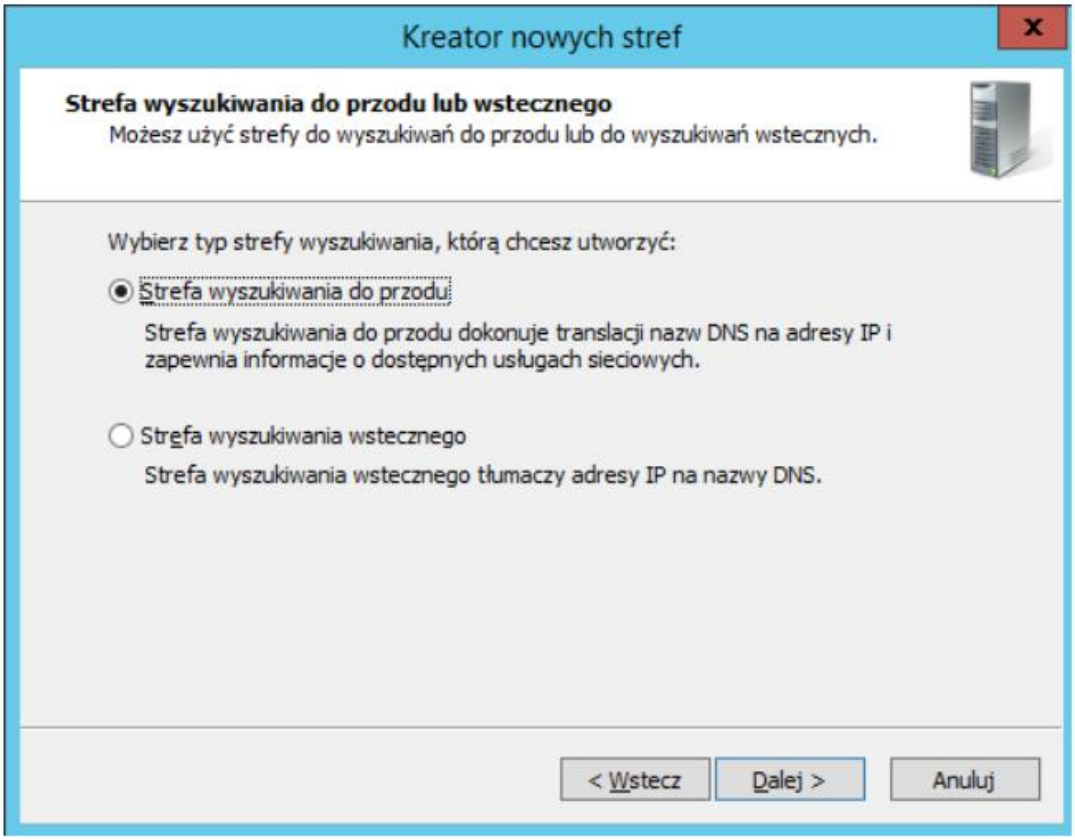
Uruchomiony zostanie kreator nowych stref (rys. 6).



Rys. 6. Kreator nowych stref.

Kreator umożliwia wybór typu stref. Jeśli konfigurowany serwer ma być podstawowym serwerem, należy wybrać opcje Strefa podstawowa. Ponieważ na serwerze nie jest uruchomiona usługa Active Directory, pole wyboru Przechowuj strefę w usłudze Active Directory jest niedostępne. Następnie należy kliknąć Dalej.

Następnie należy określić rodzaj tworzonej strefy (rys. 7).



Rys. 7. Wybór rodzaju tworzonej strefy.

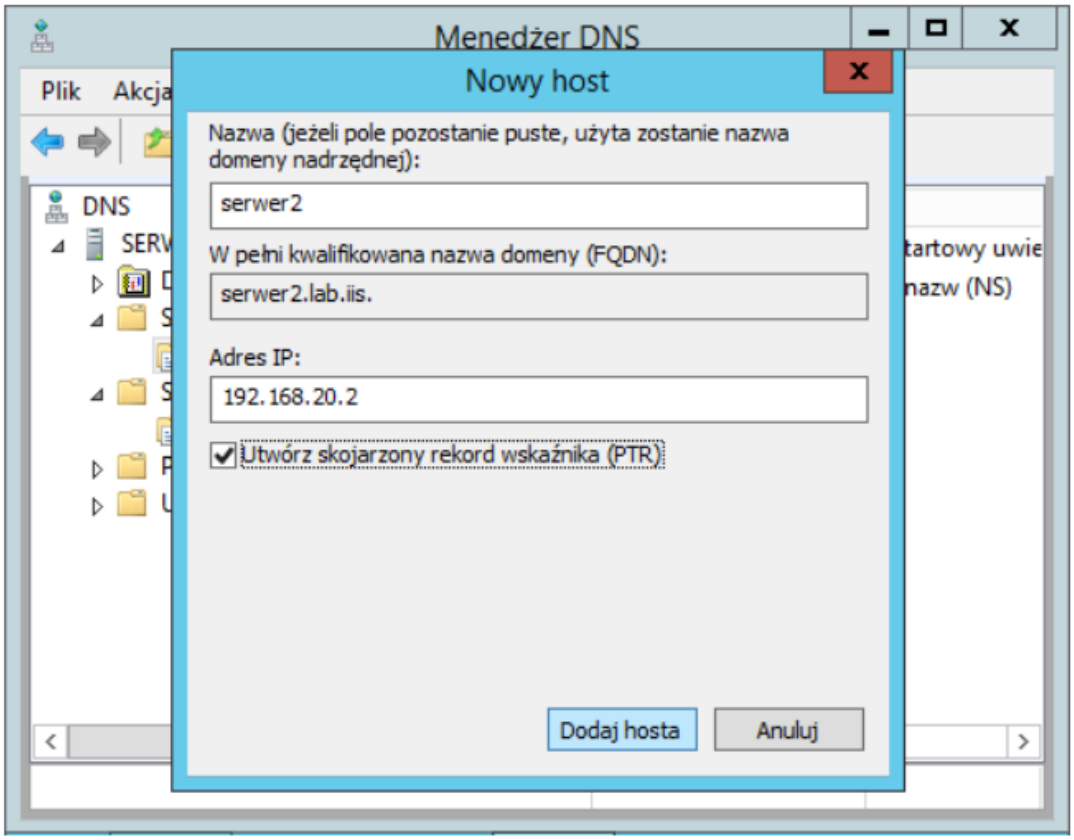
3.2. Dodawanie rekordów adresów i wskaźników

Rekordy adresów i wskaźników definiują przypisania hostów do adresów IP i odwrotnie. Rekordy te mogą być tworzone równocześnie lub oddzielnie. W celu utworzenia nowego wpisu hosta z rekordami A i PTR należy wykonać następującą procedurę:

- Rozwinąć gałąź Strefy wyszukiwania do przodu dla wybranego serwera w konsoli DNS.
- Kliknąć prawym klawiszem myszy nazwę domeny, w której zostanie utworzony nowy host, po czym wybrać polecenie Nowy host z menu podręcznego. Wyświetlone zostanie okno dialogowe przedstawione na rysunku (Rys. 8).

- Wpisać jednoczęściową nazwę komputera (np. test) w polu Nazwa i należący do niego adres w polu Adres IP.
- Zaznaczyć pole wyboru Utwórz skojarzony rekord wskaźnika (PTR).
- Kliknąć Dodaj hosta. Czynności należy powtórzyć w celu dodania rekordów dla innych komputerów.
- Po zakończeniu dodawania hostów kliknąć Gotowe.

Uwaga: Rekord wskaźnika PTR może zostać utworzony jedynie w przypadku, gdy istnieje odpowiednia strefa wyszukiwania wstecznego. Jeśli taka strefa dla odpowiedniej podsieci nie istnieje, należy ja utworzyć.



Rys. 8. Dodawanie wpisów do bazy DNS.

Dodawanie rekordu PTR

Jeśli rekord PTR nie został utworzony przy tworzeniu wpisu hosta w strefie wyszukiwania do przodu, można dodać go wykonując następującą procedurę:

- Rozwinąć gałąź Strefy wyszukiwania wstecznego dla wybranego serwera w konsoli Menedżera DNS.

- Kliknąć prawym klawiszem myszy nazwę podsieci, która ma być uaktualniona, po czym wybrać z menu podręcznego polecenie Nowy wskaźnik (PTR).
- W polu Numer IP hosta wpisać końcówkę numeru IP, po czym w polu Nazwa hosta wpisać nazwę odpowiedniego komputera, np. serwer.grupaX.kis. Kliknąć OK., aby utworzyć rekord.

Tworzenie aliasów DNS przy pomocy rekordu CNAME

Aliasy umożliwiają pojedynczemu komputerowi występowanie pod wieloma rożnymi nazwami. Typowym zastosowaniem tego mechanizmu jest przypisanie hostowi nazw związanych z pełna funkcja. Na przykład serwer gamma.microsoft.com może posiadać aliasy www.microsoft.com i ftp.microsoft.com.

W celu utworzenia rekordu CNAME należy wykonać następujące czynności:

- Rozwinąć gałąź Strefy wyszukiwania do przodu w konsoli Menedżera DNS.
- Kliknąć prawym klawiszem nazwę domeny, w której zostanie utworzony alias, po czym wybrać polecenie Nowy alias (CNAME) w menu podręcznym.
- W polu Nazwa aliasu wpisać jednoczęściową nazwę hosta, taką jak www lub ftp. Nazwa ta zostanie automatycznie uzupełniona nazwa FQDN wybranej domeny.
- W polu W pełni kwalifikowana nazwa domeny (FQDN) dla hosta docelowego należy wpisać pełna nazwę komputera, którego ma dotyczyć tworzony alias.
- Kliknąć OK.

4. Budowanie struktury DNS

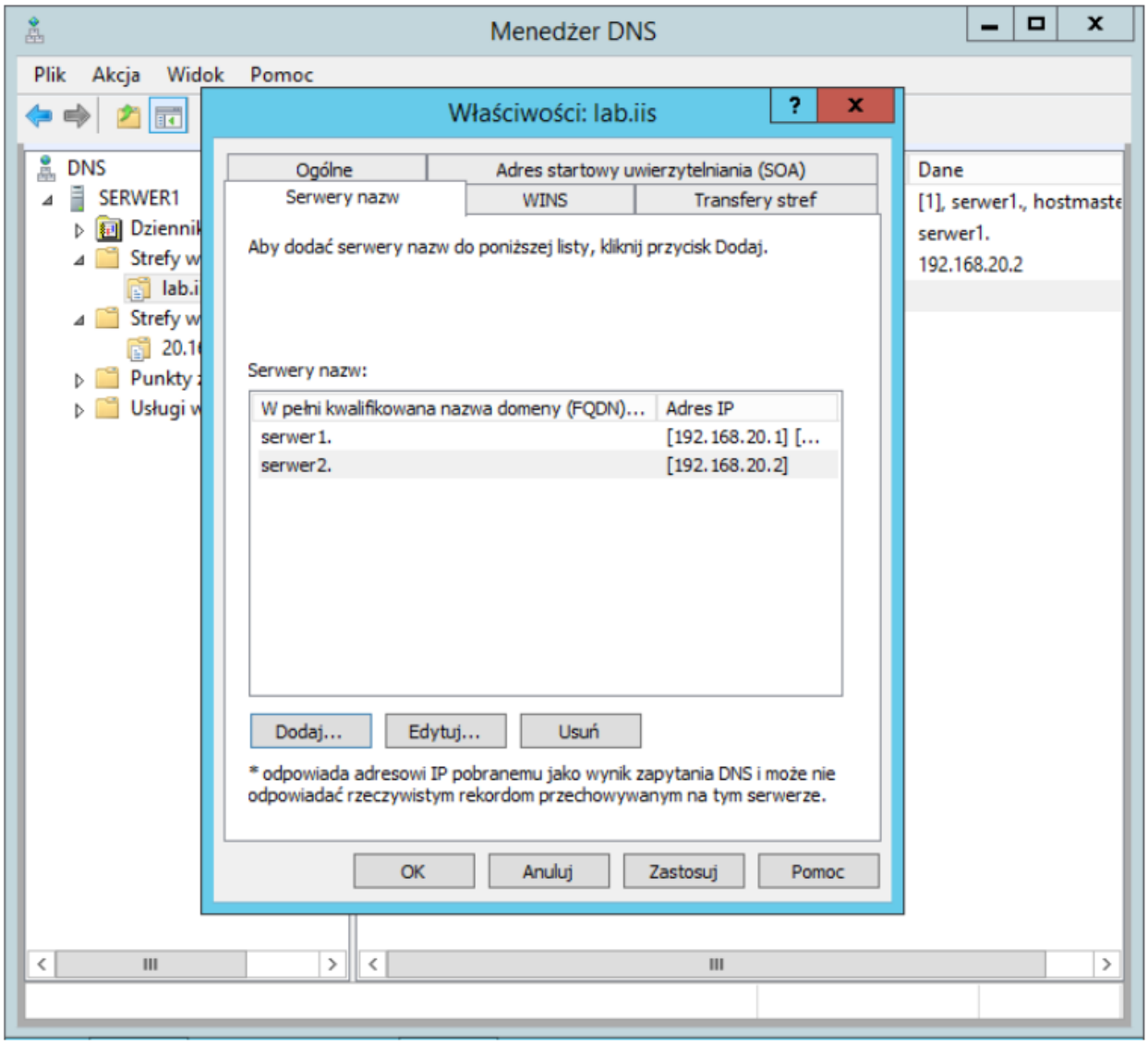
4.1. Dodawanie serwerów nazw

Rekord NS definiuje serwer nazw dla wybranej domeny. Każdemu podstawowemu i pomocniczemu serwerowi DNS musi odpowiadać rekord NS zawierający odpowiednią deklarację. Jeśli pomocnicze serwery DNS są administrowane przez inna organizacje (na przykład przez dostawce usług internetowych), należy upewnić się, że własny serwer DNS zawiera odpowiednie rekordy NS wskazujące na te serwery.

W celu utworzenia rekordu NS należy wykonać następujące czynności:

- Rozwinąć gałąź Strefy wyszukiwania do przodu dla wybranego serwera w konsoli DNS.
- Wyświetlić rekordy DNS dla domeny, zaznaczając nazwę domeny w drzewie konsoli.

- Kliknąć prawym klawiszem myszy istniejący rekord Serwer nazw (NS) w panelu widoku, po czym wybrać polecenie Właściwości. Wyświetlone zostanie okno Właściwości dla wybranej domeny z zaznaczoną zakładką Serwery nazw, przedstawione na rysunku (rys. 9).



Rys. 9. Definiowanie serwerów nazw.

Przesyłanie dalej

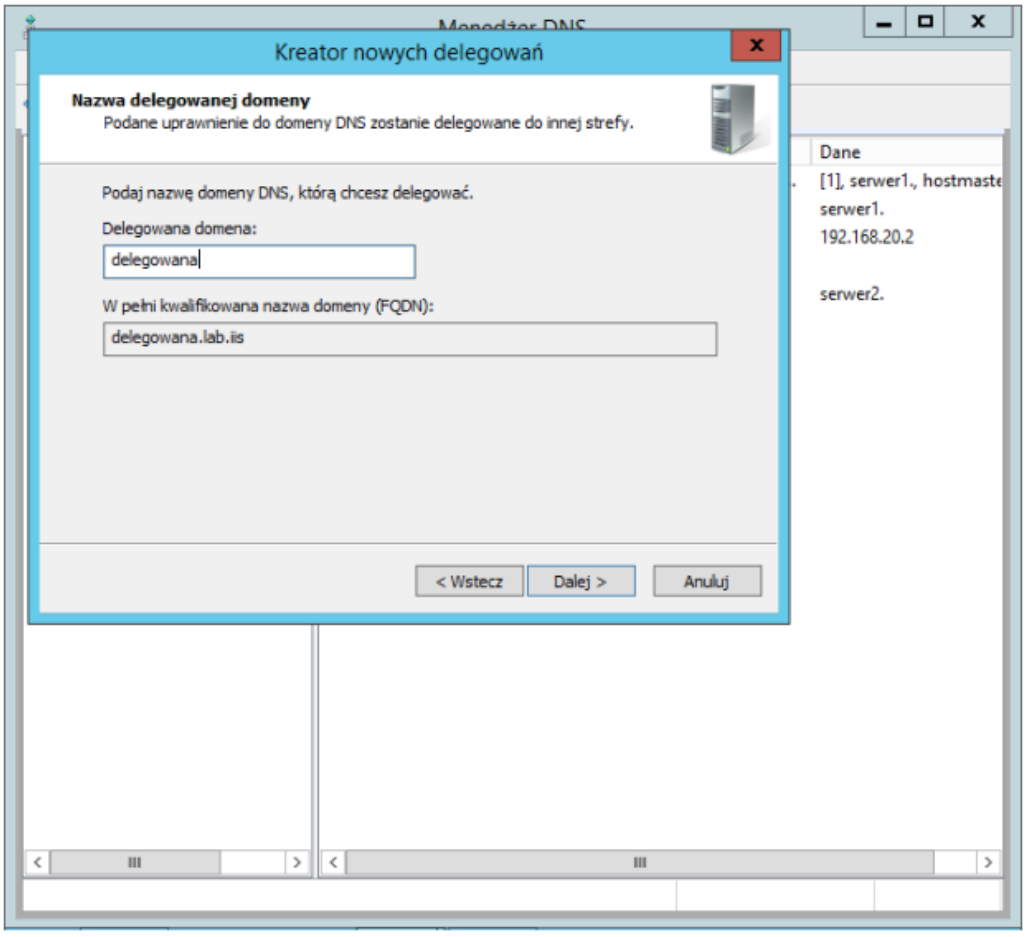
W sytuacji gdy serwer DNS nie może rozwiązać nazwy, przesyła zapytanie do innego serwera. W typowych domenach jest to jeden z serwerów głównych. W sieciach wewnętrznych wskazanym może być przesyłanie zapytanie do innego serwera wewnątrz sieci. Aby skonfigurować serwer DNS w taki sposób, by zapytanie, których nie może rozwiązać, przesyłał do innych serwerów należy zastosować następującą procedurę:

- Otwórz konsolę DNS.
- W drzewie konsoli kliknij odpowiedni serwer DNS.
- W menu Akcja kliknij polecenie Właściwości.
- Na karcie Usługi przesyłania dalej kliknij Edytuj.
- wpisz adres IP usługi przesyłania dalej i kliknij przycisk OK.

Tworzenie delegacji

Aby utworzyć delegację należy zastosować poniższa procedurę:

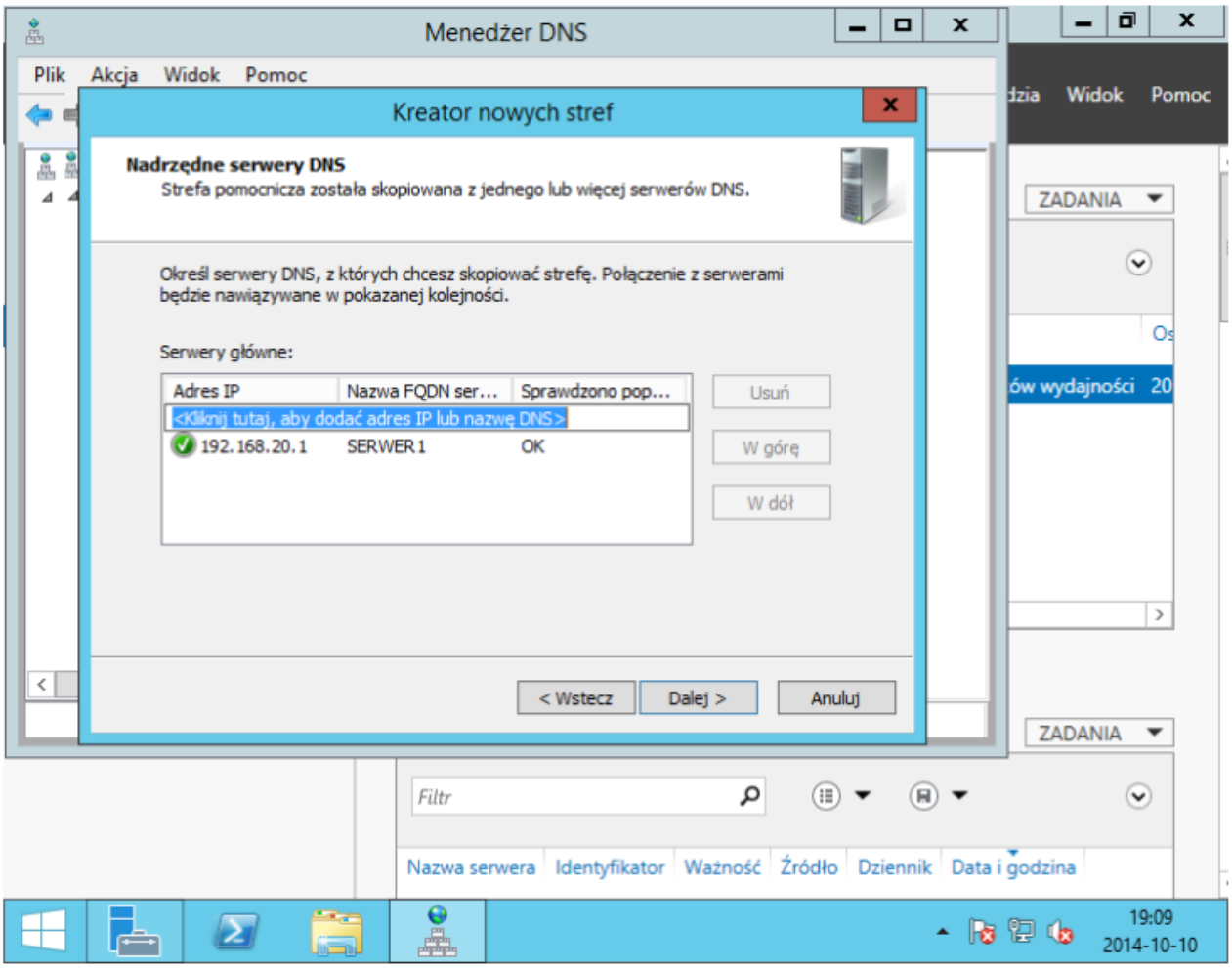
- Otwórz konsolę DNS.
- W drzewie konsoli kliknij prawym przyciskiem myszy odpowiednią domenę, a następnie kliknij polecenie Nowe delegowanie.
- Postępuj według instrukcji Kreatora nowych delegowań, aby ukończyć tworzenie nowej domeny delegowanej (Rys.10).



Rys. 10. Tworzenie delegowanej domeny DNS.

Tworzenie strefy pomocniczej

Zadaniem strefy pomocniczej jest utrzymywanie bieżącej kopii strefy. Aby utworzyć strefę pomocniczą postępujemy podobnie jak w przypadku strefy podstawowej, z tą różnicą, iż w pierwszym oknie kreatora wybieramy opcję "Strefa pomocnicza" zamiast "Strefa podstawowa". Spowoduje to, że w dalszej części pracy kreatora zostaniemy zapytani o określenie serwera nadrzędnego (rys.11).



Rys. 11. Definiowanie nadrzędnego serwer DNS.

Aby replikacja zadziałała poprawnie serwer podstawowy musi wyrazić na nią zgodę. Domyślnie serwer DNS pozwala na replikację jedynie serwerom znajdującym się na jego liście serwerów nazw. Zatem musimy nowy serwer dodać do tej listy. W tym celu wybieramy "Właściwości" z menu kontekstowego strefy i dodajemy nowy wpis na zakładce "Serwery nazw" (rys. 9).

5. Diagnostyka DNS.

Podstawowym narzędziem diagnostycznym DNS w systemie Windows jest Nslookup.exe. Jest to narzędzie administracyjne wiersza poleceń, umożliwiające testowanie i rozwiązywanie problemów z serwerami DNS. Pozwala na łączenie się z serwerami DNS i pobieranie z nich informacji dotyczących nazw przez nie obsługiwanych. Narzędzie Nslookup jest programem interaktywnym. Istnieje także możliwość wykonania polecenia Nslookup z poziomu linii poleceń CMD.

Składnia polecenia: *nslookup [-podpolecenie ...] [{host| [-serwer]}]*

Komendy interpretowane przez Nslookup:

- help lub ? - drukuje opis najważniejszych poleceń
- NAZWA - wyświetla informacje o hoście/domenie NAZWA używając serwera domyślnego DNS
- NAZWA1 NAZWA2 - jak powyżej, lecz NAZWA2 oznacza serwer DNS
- set OPCJA - ustawia opcje. Najważniejsze z opcji to:
    - all - wyświetla opcje, informacje o bieżącym serwerze i hoście
    - [no]debug oraz [no]d2 - wyświetla informacje debugera
    - [no]recurse - ustawia rekursywne odpytywanie serwerów DNS
    - domain=NAZWA - ustawia domyślną nazwę domeny na NAZWA
    - root=NAZWA - ustawia serwer główny (root server) od którego rozpoczynane są zapytania.
    - retry=X - ustawia liczbę ponawianych prób na X
    - timeout=X - ustawia początkowy limit czasu na X sekund
    - type=X lub querytype=X - ustawia typ kwerendy (np. A, ANY, CNAME, MX, NS, PTR, SOA, SRV)
- server NAZWA - ustawia domyślny serwer z którego będą pobierane dane (do rozwiązania nazwy serwera używa serwera bieżącego)
- lserver NAZWA - ustawia domyślny serwer z którego będą pobierane dane (do rozwiązania nazwy serwera używa serwera początkowego)
- ls [opt] DOMENA [> PLIK] - wyświetla adresy w DOMENIE (opcjonalne: kieruje wyniki do PLIKU). Opcje polecenia:
    - -a - wyświetla kanoniczne nazwy i aliasy
    - -d - wyświetla wszystkie rekordy

    - -t TYP - wyświetla rekordy określonego typu (np. A, CNAME, MX, NS, PTR itd.)
- view PLIK - sortuje plik wynikowy polecenia ls i wyświetla go używając pg
- exit - kończy pracę programu

Przykład: Proste zapytanie nazwę:

C:\>nslookup
Default Server: plusmx1.polkomtel.com.pl
Address: 212.2.96.51

> www.p.lodz.pl
Server: plusmx1.polkomtel.com.pl
Address: 212.2.96.51

Non-authoritative answer:
Name: ck.p.lodz.pl
Address: 212.51.207.68
Aliases: www.p.lodz.pl

Ponieważ informacje są dość ubogie ustawiamy zapytanie o wszystkie rekordy:

> set querytype=any
> www.p.lodz.pl
Server: plusmx1.polkomtel.com.pl
Address: 212.2.96.51

Non-authoritative answer:
www.p.lodz.pl canonical name = ck.p.lodz.pl

p.lodz.pl nameserver = cc1.p.lodz.pl
p.lodz.pl nameserver = dns5.man.lodz.pl
cc1.p.lodz.pl internet address = 212.51.207.67
dns5.man.lodz.pl internet address = 212.51.192.10

W ten sposób poznajemy serwery przechowujące informacje o domenie p.lodz.pl. Po zmianie serwera odpytywanego na jeden z nich można uzyskać bardziej szczegółowe informacje:

> server cc1.p.lodz.pl
Default Server: cc1.p.lodz.pl
Address: 212.51.207.67

> p.lodz.pl
Server: cc1.p.lodz.pl

```
Address:  212.51.207.67

p.lodz.pl
        primary name server = cc1.p.lodz.pl
        responsible mail addr = dns.p.lodz.pl
        serial  = 2007020202
        refresh = 10800 (3 hours)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
p.lodz.pl       nameserver = dns5.man.lodz.pl
p.lodz.pl       nameserver = cc1.p.lodz.pl
p.lodz.pl       MX preference = 10, mail exchanger = mail.p.lodz.pl
cc1.p.lodz.pl   internet address = 212.51.207.67
dns5.man.lodz.pl        internet address = 212.51.192.10
mail.p.lodz.pl  internet address = 212.51.207.70
```

Niektóre serwery DNS pozwalają na pobranie informacji o wszystkich zarejestrowanych nazwach:

```
> ls p.lodz.pl
[cc1.p.lodz.pl]
 p.lodz.pl.              NS    server = cc1.p.lodz.pl
 p.lodz.pl.              NS    server = dns5.man.lodz.pl
 pc-212.51.217.130       A     212.51.217.130
 4ds                     NS    server = czworka.p.lodz.pl
 abw-virt                A     212.51.207.57
 adamus                  A     212.51.207.51
 adm                     NS    server = cc1.p.lodz.pl
 adm                     NS    server = sir2.adm.p.lodz.pl
 sir2.adm                A     212.51.208.189
 sirmail.adm             A     212.51.208.187
 albert                  A     212.191.78.69
 .......
 .......
```

... i jeszcze kilkadziesiąt podobnych wpisów.

6. Zadania

1. Uruchom serwer DNS w na obu maszynach wirtualnych Windows 2012.
2. Skonfiguruj na komputerze A domenę DNS "komputer.iis" (komputer - numer podany przez prowadzącego).
3. Dodaj kilka hostów do domeny.

Uwaga: Komputer kliencki buforuje przypisania DNS. Po każdej zmianie konfiguracji serwera należy wyczyścić pamięć nazw (patrz: polecenie ipconfig).

4. Skonfiguruj na serwerze A poddomenę DNS "testowa.komputer.iis"
5. Wydeleguj poddomenę "poddomena" na serwer B
6. Na komputerze B skonfiguruj serwer pomocniczy dla domeny komputer.iis
7. Sprawdź serwer nazw domeny wp.pl
8. Sprawdź komputery zarejestrowane w domenie wpk.p.lodz.pl oraz kis.p.lodz.pl (wskazówka: NS użyty w przykładzie jest serwerem pomocniczym dla powyższych domen)