6.3 DNS – Domain Name System

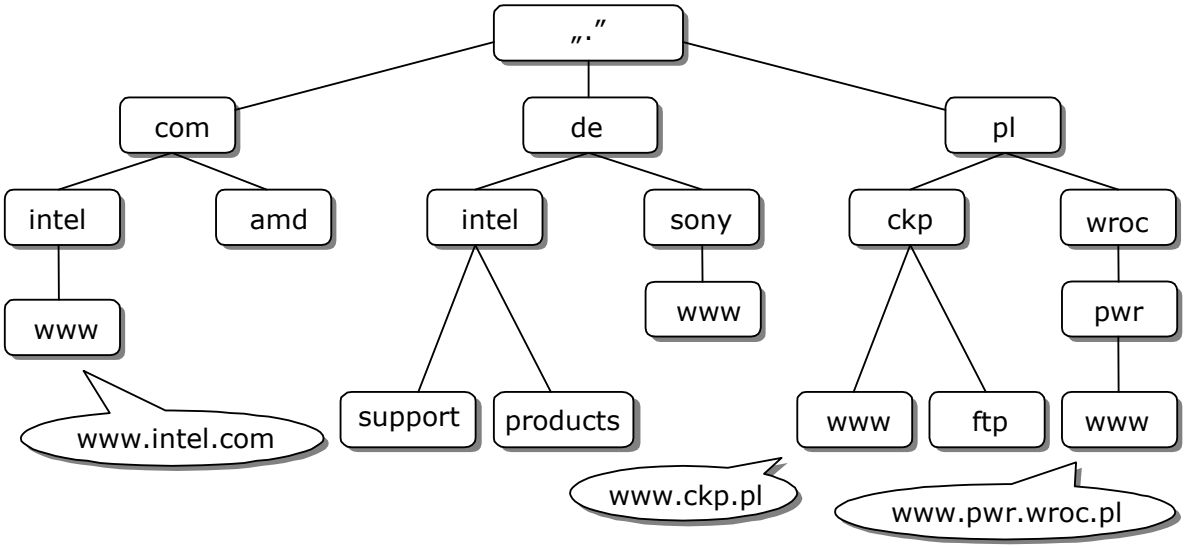
6.3.a Wstęp

DNS jest rozproszoną bazą danych, używaną w sieciach TCP/IP do tłumaczenia nazw komputerów na ich adresy IP. DNS wykorzystywany jest przede wszystkim w Internecie, ale także sieci prywatne (intranety) często korzystają z DNS. W Windows 2000/2003 DNS jest podstawowym systemem rozpoznawania nazw, a usługa Active Directory Windows 2000/2003 Server jest ściśle powiązana z DNS.

DNS tworzy hierarchiczną strukturę przypominającą odwrócone drzewo. Każdy węzeł w drzewie DNS może być identyfikowany przez pełną nazwę domeny (FQDN, Full Qualified Domain Name). Składa się ona z nazw domen węzłów rozdzielanych znakiem kropki. Z prawej strony znajduje się domena najwyższego poziomu np. www.ckp.pl. Nazwy domen mogą składać się ze znaków a-z, A-Z, 0-9, (-) (maksymalnie 63, FQDN to maksymalnie 255 znaków, nie jest rozróżniana wielkość liter).

Na samej górze znajduje się domena katalogu głównego oznaczana znakiem „.” Internetowa domena katalogu głównego zarządzana jest przez kilka organizacji, w tym Network Solutions Inc. Pod domeną katalogu głównego znajduje się domena najwyższego poziomu, zwana domeną pierwszego poziomu. Istnieją trzy rodzaje domen wysokiego poziomu:

- *Domeny organizacji* - są skrótami typu organizacji np. com – komercyjne, edu – edukacyjne, gov – rządowe, org – niekomercyjne, int – międzynarodowe, mil – wojskowe, net – operatorów sieciowych. Domeny organizacyjne najwyższego poziomu dotyczą organizacji znajdujących się w Stanach Zjednoczonych lub o zasięgu ogólnoświatowym.
- *Domeny geograficzne* - są dwuliterowymi skrótami państw np. pl – to Polska, ru – Rosja, de – Niemcy, uk – Wielka Brytania. Tylko Stany Zjednoczone nie korzystają z domeny geograficznej pierwszego poziomu.
- *Domena wsteczna* - in-addr.arpa jest specjalnym typem domeny używanym do odwzorowywania adresów IP na nazwy, nazywanym odwzorowaniem wstecznym.



Rys. 6.9 Hierarchiczna struktura domen

Pod domeną najwyższego poziomu znajduje się domena drugiego poziomu. Jeżeli pierwszym poziomem jest domena geograficzna, wówczas drugi poziom tworzy domena organizacji lub domena regionalna np. wroc – Wrocław, waw – Warszawa. W tej sytuacji drugi poziom nie jest jednak obowiązkowy.

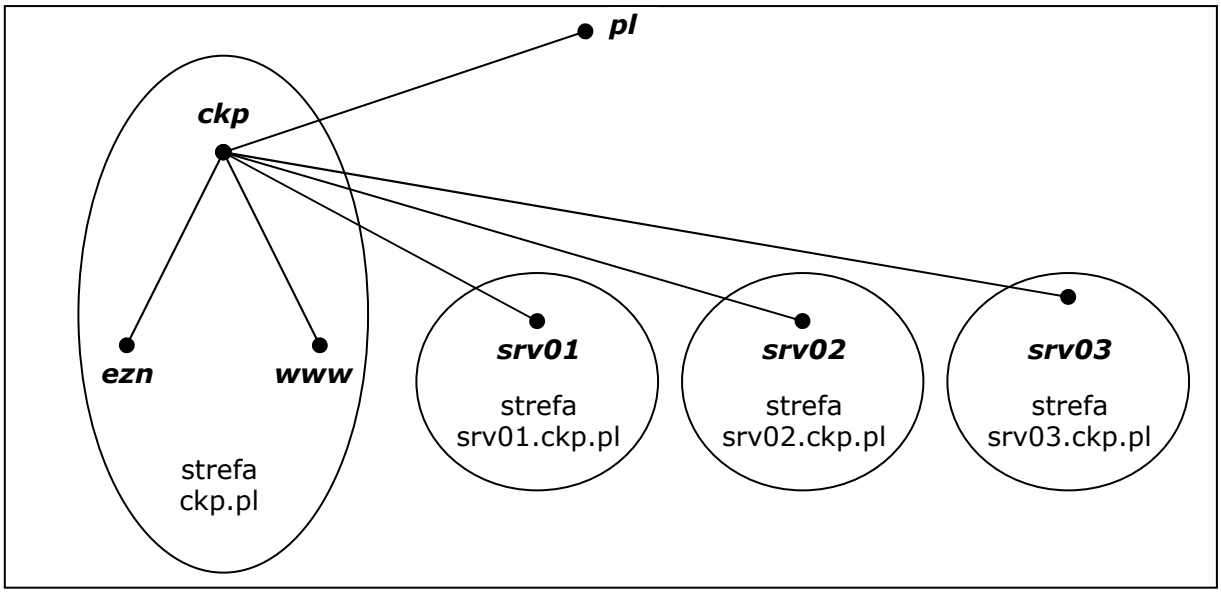
Domenę można zarejestrować u operatora wybranej domeny pierwszego lub drugiego poziomu. W Polsce za obsługę domeny pl odpowiedzialny jest NASK (Naukowa Akademicka Sieć Komputerowa), a za obsługę domeny wroc.pl WCSS (Wrocławskie Centrum Sieciowo-Superkomputerowe przy Politechnice Wrocławskiej).

W domenie mogą znajdować się nazwy hostów, odnoszące się do konkretnych komputerów lub inne domeny, zwane poddomenami.

Podczas zarządzania systemem DNS korzysta się ze stref. Strefa jest częścią obszaru nazw domeny zakotwiczoną w konkretnym węźle domeny, w przeciwieństwie do domeny, którą jest cała gałąź domeny. Domena może zostać podzielona na wiele części (strefy) każda z nich może być zarządzana przez inny serwer DNS.

Oprócz strefy podstawowej istnieje strefa pomocnicza stanowiąca kopie strefy z serwera głównego. Dla każdej domeny tylko jeden serwer DNS może zarządzać strefą podstawową. Natomiast strefa zapasowa może znajdować się na wielu serwerach. Jeden serwer DNS może przechowywać bazę wielu stref podstawowych i pomocniczych. Strefa musi posiadać przynajmniej jeden serwer podstawowy i zapasowy.

Poniższy rysunek przedstawia domenę ckp.pl i podział na strefy wykorzystywane podczas tego ćwiczenia.



Rys. 6.10 Podział na strefy domeny ckp.pl

Zapytania do serwera DNS nazywane są kwerendami. DNS może rozwiązywać kwerendy wyszukiwania do przodu, odwzorowujące nazwę na adres IP i kwerendy wyszukiwania wstecznego, odwzorowujące adres IP na nazwę.

Klient wysyła kwerendę do swojego serwera DNS. Jeżeli pytanie dotyczy stref zarządzanych przez dany serwer, to uzyskuje natychmiast odpowiedź. W przeciwnym wypadku, jego zapytanie kierowane jest do innych serwerów DNS, wg hierarchii domeny, zaczynając od serwera katalogu głównego. Serwer DNS buforuje wszystkie kwerendy, zanim wyśle zapytanie do innego serwera, sprawdza czy odpowiedzi nie ma w buforze.

Dla rozwiązywania zapytań wstecznych, została utworzona specjalna domena in-addr.arpa. Wykorzystuje ona także hierarchiczny system nazewniczy, ale w połączeniu z adresami IP zapisywanymi od końca w notacji kropkowo dziesiętnej, np. dla klasy C 212.160.198.x domena odwrotna to 198.160.212.in-addr.arpa. Organizacje administrują subdomenami, w oparciu o przyznane im adres IP i maskę podsieci.

Odwrotną domenę można stworzyć zatem dla podsieci przynajmniej 256 adresów. Często jednak ISP przydziela mniejszą ilość adresów, wówczas to ISP jest odpowiedzialny za administrowanie domeną odwrotną. W takiej sytuacji można stworzyć bezklasową strefę odwrotną, jednak nie wszyscy ISP zezwalają na delegowanie strefy bezklasowej.

6.3.b Rekordy zasobów i strefy

Pliki stref w serwerze DNS zbudowane są z rekordów, które wiążą informacje o zasobach z nazwami domen DNS.

Rekordy zasobów mają następującą składnię:

- ***Właściciel*** – wskazuje nazwę domeny DNS, która jest właścicielem rekordu zasobu. Znak <@> oznacza nazwę strefy.
- ***Czas wygasania TTL*** – 32-bitowa liczba całkowita, reprezentująca w sekundach czas, przez jaki serwer lub przelicznik (lokalny bufor) ma przechowywać dany rekord w buforze, zanim go odrzuci. Pole to jest opcjonalne i jeśli nie jest określone, to klient decyduje o minimalnym czasie.
- ***Klasa*** – określa używaną rodzinę protokołów. Dla Internetu jest to IN.
- ***Typ*** – określa typ rekordu.
- ***Dane*** – specyficzne dane rekordu zasobu. Typ zależy od przechowywanych informacji.

System DNS korzysta z kilku typów rekordów:

- ***SOA*** – znajduje się na początku każdej strefy. Jest rekordem adresu startowego. Posiada złożone pole danych. Znajduje się w nim:

- ***Serwer autorytatywny*** – podstawowy serwer DNS dla strefy,
- ***Osoba odpowiedzialna*** – zawiera adres e-mail administratora odpowiedzialnego za strefę. UWAGA: zamiast znaku <@> występuje <.>
- ***Numer seryjny*** – zawiera informacje o aktualizacji strefy, zazwyczaj podaje się w formacie rrrrmmddnn, gdzie rrrr – to rok, mm – miesiąc, dd – dzień, nn – numer aktualizacji w dniu. Po każdej zmianie strefy, numer seryjny powinien być aktualizowany. Serwer pomocniczy, na postawie numeru, określa konieczność transferu strefy z serwera głównego.
- ***Interwał odświeżania*** – określa w sekundach, jak często serwer pomocniczy ma sprawdzać, czy strefa została zaktualizowana. Zazwyczaj ustawiany na 8 godz. – 28800 sek.
- ***Interwał ponawiania*** – określa jak długo po wysłaniu żądania transferu stref serwer pomocniczy ma czekać na odpowiedź serwera głównego, zanim wyśle powtórzenie żądania. Zazwyczaj ustawiany na 1 godz. – 3600 sek.
- ***Interwał wygasania*** – określa jak długo, po ostatnim transferze stref serwer, pomocniczy odpowiada na zapytania dotyczące danej strefy, zanim uzna ją za nieważną. Zazwyczaj ustawiany na 1 tydzień – 604800 sek.
- ***Minimalny TTL*** – minimalny TTL dla wszystkich rekordów strefy, które nie mają własnego pola TTL. Zazwyczaj ustawiany na kilka, kilkanaście godzin. 24 godz. – 86400 sek.

Przykładowy rekord ***SOA***:

```
@       IN      SOA     k211-01.srv01.ckp.pl.               ; serwer strefy
                        administrator.k211-01.srv01.ckp.pl. ;e-mail administratora strefy
                        (2002051501                         ; numer seryjny
                        28800                               ; interwał odświeżania
                        3600                                ; interwał ponawiania
                        604800                              ; interwał wygasania
                        86400                               ; domyślny TTL
                        )
```

UWAGA: nazwy domen w pliku strefy muszą zawierać kropkę katalogu głównego, np. k211-01.srv01.ckp.pl.

- ***NS*** - serwer nazw. Rekordy NS określają serwer podstawowy i pomocniczy dla strefy. Każda strefa musi zawierać przynajmniej jeden rekord NS. Wskazują także delegowanie określonej strefy na inny serwer.

Przykładowe rekordy ***NS***:

```
@               IN      NS      k211-01.srv01.ckp.pl.       ; serwer strefy
poddomena       IN      NS      k211-01.srv01.ckp.pl.       ; delegacja domeny
```

- ***A*** – adres hosta, odwzorowuje pełną nazwę domeny na adres IP.

Przykładowy rekord ***A:***

```
k211-01         IN      A       10.0.10.1
```

- ***PTR*** – odwzorowuje adres IP na nazwę. Wykorzystywany w strefach odwrotnych.

Przykładowy rekord ***PTR*** dla strefy 10.0.10.in-addr.arpa.

```
1               IN      PTR     k211-01.srv01.ckp.pl.
```

- ***CNAME*** – tworzy nazwę kanoniczną (alias) dla podanej nazwy FQDN. Dzięki rekordowi CNAME można tworzyć wirtualne serwery. Wiele nazw skojarzonych z jednym adresem IP.

Przykładowe rekordy ***CNAME***:

```
www             IN      CNAME       k211-01.srv01.ckp.pl.
ftp             IN      CNAME       k211-01.srv01.ckp.pl.
```

- ***MX*** – określa serwer poczty dla nazwy domeny. Aby serwer pocztowy mógł działać, musi mieć zdefiniowany rekord MX. Domena może korzystać z kilku serwerów pocztowych. Wówczas, po typie rekordu, należy podać priorytet. Preferowane są serwery z niższym priorytetem. Jeżeli będzie niedostępny serwer z najniższym priorytetem, wówczas wykorzystywany jest serwer z wyższym priorytetem.

Przykładowe rekordy ***MX:***

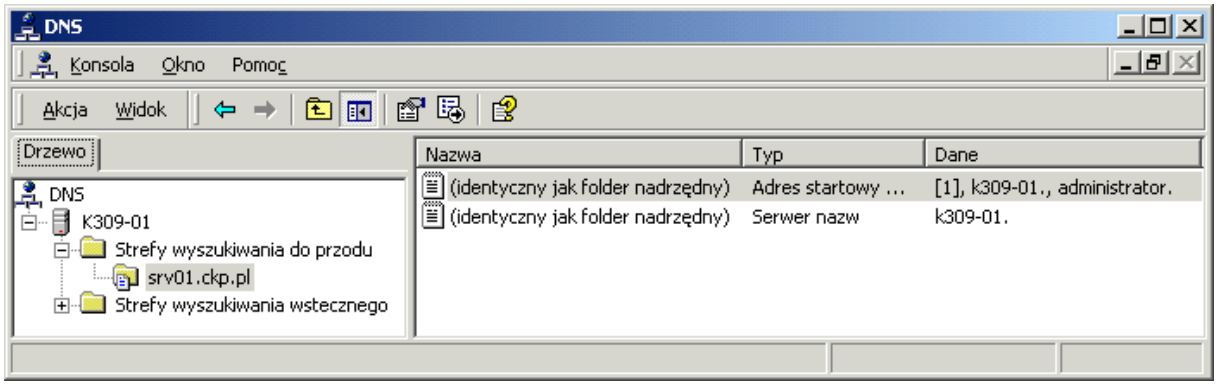
```
srv01.ckp.pl    IN      MX      0       k211-01.srv01.ckp.pl.
srv01.ckp.pl    IN      MX      10      k211-01a.srv01.ckp.pl.
```

- ***SRV –*** umożliwia lokalizację innych usług w domenie. Korzysta z niego usługa Active Directory do lokalizacji serwera domeny.
- ***TXT*** – tekst opisowy dla domeny

6.3.c Instalowanie usługi DNS

Przed instalacją, serwer musi mieć skonfigurowany statyczny adres IP i ustawienia DNS tak, aby wskazywały z powrotem na serwer. Serwer DNS jest usługą sieciową i można zainstalować ją przez ***Dodaj/Usuń programy -> Dodaj/Usuń składniki systemu Windows -> Usługi sieciowe -> System DNS***.

Po instalacji, folder <%SystemRoot%\System32\DNS> zawierać będzie pliki bazy danych DNS. W ***Narzędziach administracyjnych*** pojawi się skrót do przystawki ***DNS***, za pomocą której można konfigurować serwer.



Rys. 6.11 Przystawka DNS

6.3.d Tworzenie stref i rekordów

Aby usługa DNS mogła działać na serwerze, należy utworzyć przynajmniej jedną strefę wyszukiwania do przodu.

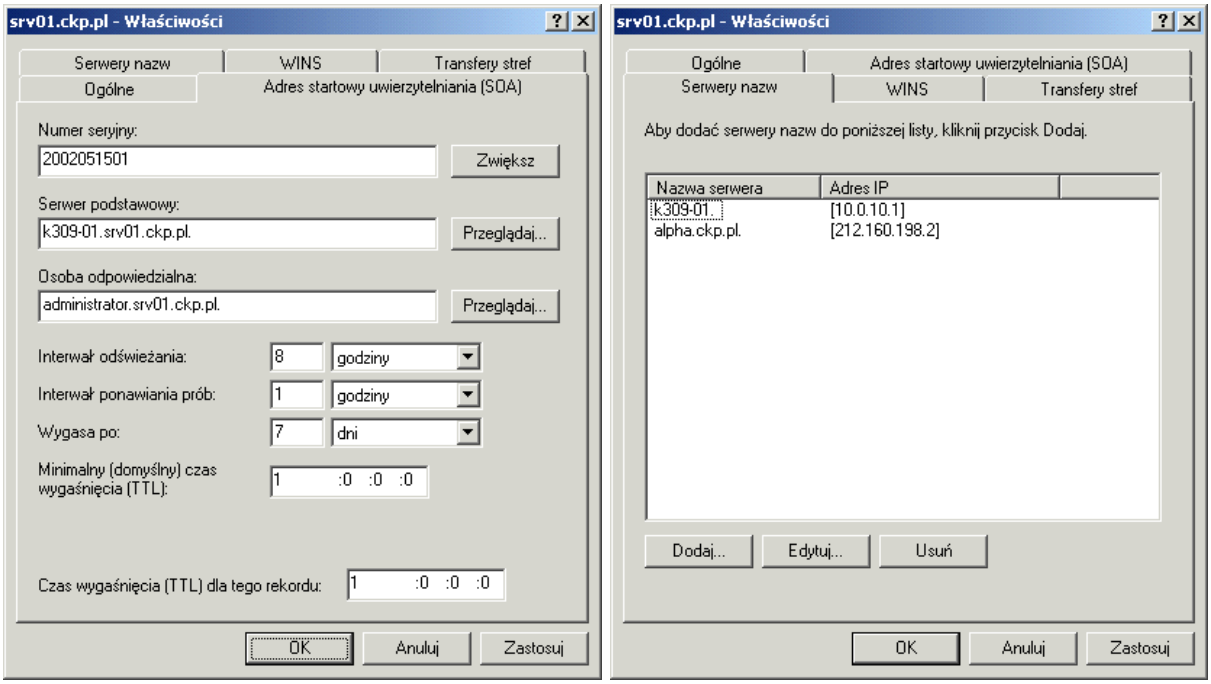
Aby utworzyć nową strefę, należy wskazać nazwę serwera i po kliknięciu prawym przyciskiem myszy wybrać ***Nowa strefa***. Wywołany zostanie w ten sposób kreator, który szybko przeprowadzi przez proces konfiguracji.

1. Na początku należy określić ***Typ strefy***. Dostępna jest ***Podstawowa standardowa***. Przy korzystaniu z Active Directory można wybrać ***Zintegrowana usługa AD***. Jeżeli serwer DNS ma być serwerem pomocniczym wówczas ***Pomocnicza standardowa***.
2. Następnie należy określić, czy kreator ma stworzyć ***strefę wyszukiwania do przodu,*** czy ***wyszukiwania wstecznego***. Strefy wyszukiwania wstecznego można tworzyć jedynie dla pełnych sieci klas A, B, C. Zatem jeżeli dysponuje się jedynie podsiecią IP, wówczas za obsługę strefy odwrotnej odpowiedzialny jest operator Internetu.
3. Kolejne okno, to podanie nazwy strefy (np. twoja domena internetowa)
4. W przed ostatnim kroku należy określić ***nazwę pliku strefy***. Domyślna nazwa pliku, to nazwa strefy z rozszerzeniem dns.
5. W ostatnim kroku określa się opcje ***Aktualizacji dynamicznej***. Dla stref wykorzystywanych w Internecie, ze względów bezpieczeństwa najlepiej wybrać ***Nie zezwalaj na aktualizacje dynamiczne***. Natomiast dla stref wykorzystywanych lokalnie dobrze jest korzystać z ***aktualizacji dynamicznych***, ale jedynie ***zabezpieczonych***.

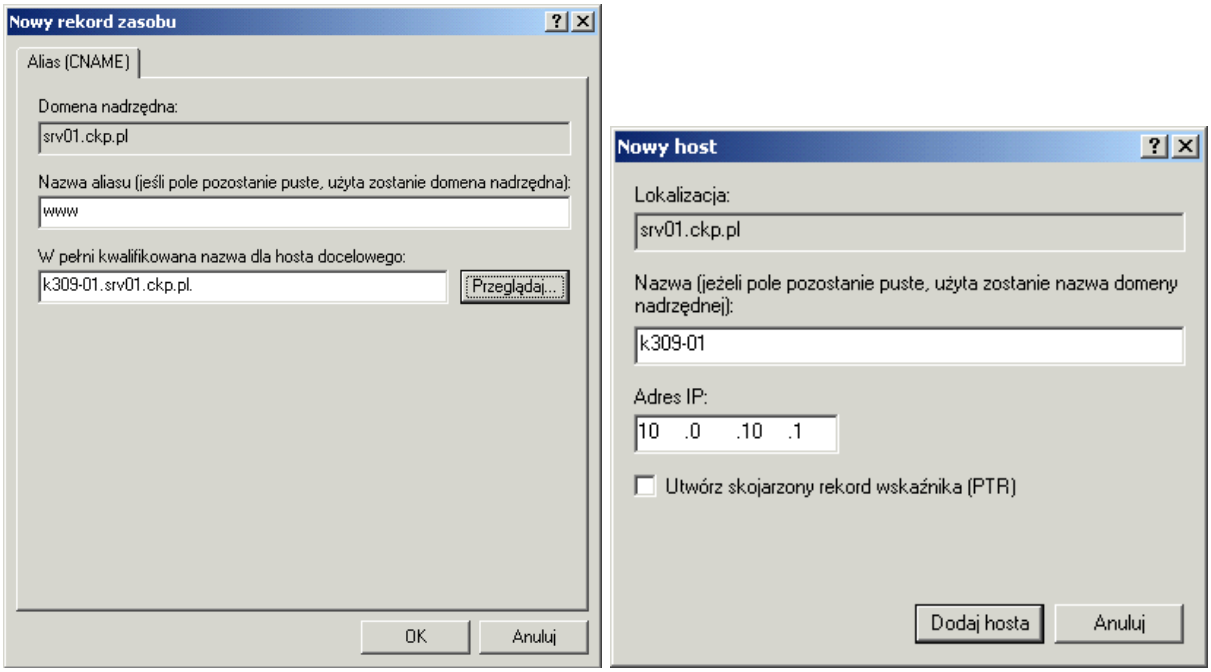
Kreator tworzy strefę z rekordami ***SOA*** i ***NS***. Rekordy te można modyfikować przez wybranie ***Właściwości*** danej strefy.

Rekordy ***A*** i ***CNAME*** można zdefiniować przez wybór ***Nowy host*** lub ***Nowy alias*** z menu podręcznego danej strefy. Natomiast rekord ***MX*** za pomocą opcji ***Nowa usługa wymiany poczty***. Inne rekordy definiuje się, po wybraniu ***Inne nowe rekordy***.

Jeżeli zachodzi potrzeba utworzenia poddomeny, wówczas należy wybrać opcję ***Nowa domena***. Dla delegacji należy wybrać ***Nowe pełnomocnictwo***.



Rys. 6.12 Modyfikacja rekordów SOA i NS



Rys. 6.13 Dodanie nowych rekordów A i CNAME

6.3.e Nslookup

W systemie Windows 2000/2003 znajduje się narzędzie diagnostyczne dla usług DNS. Jest nim program ***nslookup***. Program ten może pracować w trybie interakcyjnym i nieinterkacyjnym (wywołanie programu z parametrami).

Poniżej znajduje się lista najważniejszych poleceń trybu interakcyjnego:

- ***nazwa*** - drukuje informacje o hoście/domenie ***nazwa,*** używając serwera domyślnego,
- ***help*** lub ***?*** - drukuje informacje o najczęściej używanych poleceniach,
- ***set type=X*** lub ***set querytype=X*** - ustawia typ kwerendy na określony rekord, ***all*** oznacza wszystkie,
- ***server nazwa*** - ustawia domyślny serwer na ***nazwa***, używając bieżącego serwera domyślnego,
- ***ls [opt] domena [> plik]*** - wyświetla adresy w domenie (opcjonalnie: kieruje wyniki do pliku) ***–a*** (wyświetla kanoniczne nazwy i aliasy), ***-d*** (wyświetla wszystkie rekordy), ***-t*** typ (wyświetla rekordy określonego typu, all oznacza wszystkie),
- ***exit*** - kończy pracę programu.

Zadanie 6.3 – Instalacja i konfiguracja DNS

UWAGA: jeżeli w czasie ćwiczenia skorygujesz swój błąd będziesz musiał ***wyczyścić pamięć podręczną*** w serwerze DNS i podatkowo pamięć podręczną systemu poleceniem ***ipconfig /flushdns***

1. Zainstaluj serwer DNS.
2. Dla domeny ***srvxx.ckp.pl*** utwórz strefę wyszukiwania do przodu, gdzie xx to numer twojego serwera.
3. Dodaj rekord A (host) dla twojej głównej nazwy serwera to ***k211-xx***. Sprawdź, za pomocą polecenia ***ping*** działanie twojego serwera. UWAGA: w strefie musi pozostać tylko jeden rekord wskazujący na twoją główną nazwę.
4. Zmodyfikuj rekord SOA (adres startowy uwierzytelniania): ustaw odpowiednio numer seryjny, serwer podstawowy, e-mail osoby odpowiedzialnej, interwały, TTL (patrz punkt 6.3.b).
5. Zmodyfikuj rekordy NS (serwer nazw). Musi pozostać rekord z główną nazwą i adresem internetowym serwera, a także rekordy z nazwami i adresami serwerów zapasowych (serwer sąsiada będzie dla ciebie serwerem zapasowym).
6. Dodaj rekord A (host) dla nazw ***www***, ***ftp***. Sprawdź, za pomocą polecenia ***ping***, działanie twojego serwera.
7. Dodaj rekord MX (usługa wymiany poczty) dla twojej domeny. Twój serwer w przyszłości będzie serwerem pocztowym.
8. Dodaj rekord TXT (tekst) dla twojej domeny.
9. Usuń poddomenę ***lanxx***.
10. Utwórz nową strefę ***lanxx.srvxx.ckp.pl***. Zezwól na aktualizacje dynamiczne.
11. Skontroluj czy w nowej strefie jest tylko jeden rekord powiązany z główną nazwą serwera i wskazujący na adres lokalny serwera.
12. Przeglądnij rekord SOA i NS nowo utworzonej strefy. Dla strefy lokalnej mogą pozostać domyślne ustawienia.

13. Sprawdź ze stacji roboczej, za pomocą polecenia ***ping***, działanie twojego serwera DNS.
14. Utwórz strefę pomocniczą dla twojego sąsiada.
15. Pobierz strefę z serwera głównego – z menu podręcznego należy wybrać ***Transferuj z wzorca***.
16. Utwórz strefę wyszukiwania wstecznego dla twojej domeny lokalnej. Zezwól na aktualizacje dynamiczne.
17. Dodaj rekord PTR dla adresu IP twojego serwera.
18. Sprawdź ze stacji roboczej, za pomocą polecenia ***tracert***, działanie twojego serwera DNS.
19. We właściwościach serwera DNS załącz usługi przesyłania dalej. Jako adres serwera DNS podaj adres twojego operatora Internetu, w czasie ćwiczenia to 212.160.198.2

6.3.f Dynamiczne aktualizacje

Serwer DNS Windows 2000/2003 udostępnia dynamiczną aktualizację zwaną DDNS. Klienci mogą automatycznie przekazywać do serwera zmiany nazwy. Przekazują serwerowi rekordy A i PTR. Serwer DNS może także współpracować z serwerem DHCP, który odświeżać będzie informacje o hostach.

Odpowiednie opcje konfiguracyjne znajdują się we właściwościach strefy, na zakładce ***Ogólne.***

6.4 WINS – Windows Internet Name Service

6.4.a Wstęp

Klienci Windows 9x/ME i NT do komunikowania używają nazw NetBIOS. Dlatego też sieć wykorzystująca Windows 2000/XP/2003, współpracująca z Windows 9x/ME/NT, potrzebuje środowiska do rozwiązywania nazw NetBIOS na adresy IP. W tej sytuacji można skorzystać z mechanizmu rozgłaszania nazw. Jest to jednak metoda mało efektywna
i w większych sieciach powoduje generowanie znacznego ruchu. Lepszym rozwiązaniem jest instalacja serwera nazw NetBIOS – WINS. Rejestruje on dynamicznie nazwy komputerów i dostarcza adresy IP.

Przy każdym uruchomieniu klienta WINS, rejestruje on swoją nazwę i adres IP na serwerze WINS. A gdy klient inicjuje połączenie NetBIOS, wysyła do serwera WINS żądanie z pytaniem, zamiast emitować ją w sieci lokalnej.

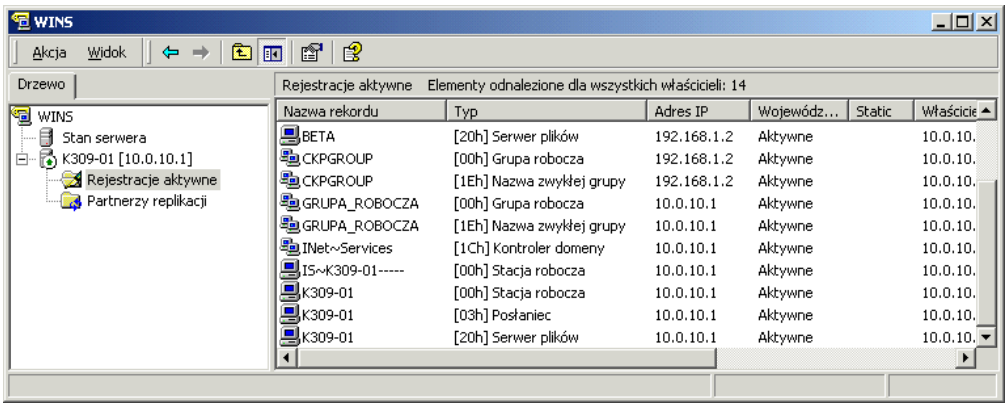
6.4.b Instalacja i zarządzanie WINS

Serwer WINS jest usługą sieciową, zatem można zainstalować ją przez ***Dodaj/Usuń programy -> Dodaj/Usuń składniki systemu Windows -> Usługi sieciowe -> WINS***.

Po instalacji w ***Narzędziach administracyjnych,*** dostępna będzie przystawka ***WINS,*** za pomocą której można zarządzać serwerem.

Aby zobaczyć zarejestrowane nazwy, po kliknięciu na ***Rejestracje aktywne,*** należy wybrać z menu podręcznego ***Wyświetl rekordy.***

Aby ręcznie zarejestrować nazwę z menu podręcznego, należy wybrać opcję ***Nowe mapowanie statyczne***.



Rys. 6.14 Przystawka WINS

Zadanie 6.4 – Instalacja WINS

1. Zainstaluj serwer WINS.
2. W konfiguracji TCP/IP serwera (dla połączenia ***LAN)*** i stacji roboczej ustaw korzystanie z serwera WINS. Podaj odpowiedni adres.
3. Sprawdź w serwerze WINS, czy zostały automatycznie zarejestrowane nazwy.

6.5 Routing

6.5.a Wstęp do routingu

Routing jest procesem polegającym na przekazaniu danych przez zespół sieci, z systemu źródłowego do docelowego. Proces ten jest dwuetapowy. Na początku odbywa się routing w systemie końcowym, następnie dane przekazywane są do routera.

Host, przed wysłaniem pakietu, porównuje adres docelowy z adresem swojej sieci i na tej podstawie określa, czy pakiet należy przekazać bezpośrednio do systemu końcowego, czy użyć routera.

Po decyzji, iż pakiet należy przesłać do routera, host musi określić adres pierwszego przeskoku. Korzysta przy tym z kilku technik:

- Trasa domyślna – w celu uproszczenia konfiguracji hostów, definiuje się trasę domyślną dla adresów z poza lokalnej podsieci, przez podanie bramy domyślnej.
- Tabela routingu hosta – w systemie można zdefiniować statyczną tabelę routingu.
- Dynamiczne uaktualnienie tabeli routingu – jeżeli w sieci znajduje się klika routerów, mogą one za pomocą protokołu ICMP, informować o lepszych trasach dla hosta docelowego.
- Monitorowanie – hosty są w stanie monitorować ruch generowany przez routery z informacjami o trasach sieciowych. Routery korzystają przy tym ze specjalnego protokołu (np. RIP).

Router, po otrzymaniu pakietu, który nie jest dla niego przeznaczony, musi przesłać go dalej, do docelowego hosta lub do kolejnego routera. Jeżeli pakiet kierowany jest do sieci, do których podłączony jest router, przekazuje go do docelowego hosta, dostarczając pakiet bezpośrednio. W przeciwnym wypadku przekazuje pakiet do kolejnego pośredniczącego routera, wybierając go na podstawie tabeli routingu. Router może korzystać ze statycznej tabeli routingu lub dynamicznej. Tabele dynamiczne tworzone są na postawie komunikacji między routerami. Routery korzystają przy tym ze specjalnych protokołów np. RIP.