PRZESTRZEŃ NAZW DOMEN – DNS

1. DNS – nazwy zamiast liczb

Wszystkie komputery w sieci TCP/IP identyfikowane są za pomocą jednoznacznego adresu IP. Jego postać liczbowa o długości 32 bitów jest skomplikowana i łatwo o błąd podczas wpisywania. Z tego powodu już w roku 1984 utworzono system nazw domen Domain Name System (DNS). To właśnie dzięki niemu można połączyć się z hostem, używając przynależnej nazwy domeny.

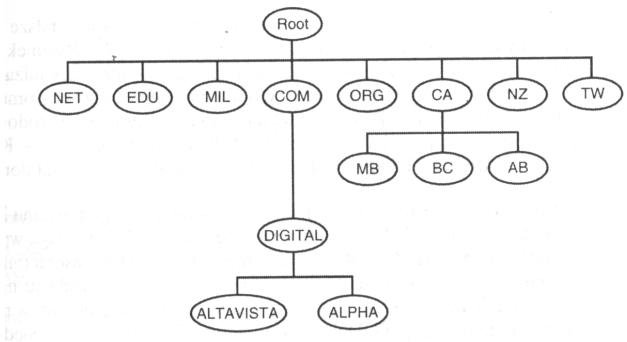
DNS to rozproszona baza danych, której głównymi komponentami są serwery nazw. Zarządzają informacjami o odwzorowaniu, co polega na wzajemnym przyporządkowaniu adresów IP i nazw komputerów.

Gdy jeszcze nie było Internetu obecnej postaci, a ARPAnet łączył kilkaset komputerów, wszystkie informacje o hostach mieściły się w jednym pliku. Plik ten musiał się znajdować w każdym komputerze podłączonym do sieci ARPAnet; zawierał wszystkie informacje związane z odwzorowaniem. System nazw domen usunął podstawowe wady tablic nazw opartych na plikach:

- DNS daje się łatwo rozszerzać
- ma postać rozproszonej bazy danych i gwarantuje, że informacje o nowych komputerach i zmianach w razie potrzeby dotrą do wszystkich użytkowników Internetu

2. Przestrzeń Nazw Domen

Przestrzeń nazw domen jest drzewiastą strukturą obejmującą wszystkie domeny tworzące przestrzeń nazw Internetu. Początkiem drzewa jest domena określana angielskim terminem root, czyli korzeń.



Rys.: DNS

Źródło: Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion, strona 137

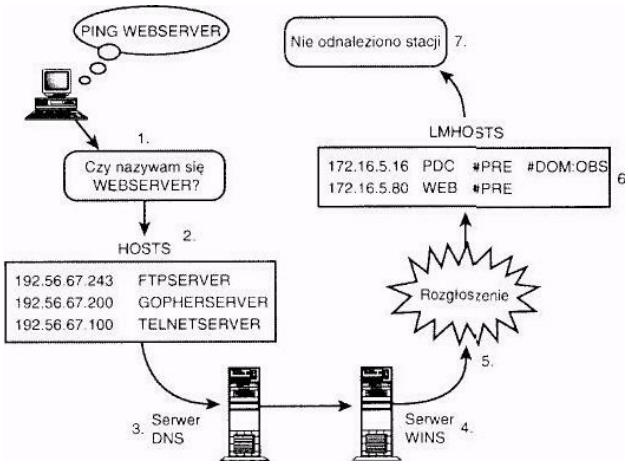
W odróżnieniu od pozostałych domen, domenie root nie odpowiada żadna występująca w nazwach stacji etykieta. Do jej określenia stosuje się czasem znak kropki (.).
Poniżej domeny root znajdują się domeny pierwszego poziomu. Są one dwojakiego rodzaju: pierwsza ich grupa odpowiada typom działalności korzystających z nich organizacji, druga wykorzystuje dwuliterowe oznaczenia krajów, w których poszczególne organizacje się znajdują.

2.1. Domeny wysokiego poziomu wykorzystywane obecnie

- com organizacje komercyjne
- edu instytucje edukacyjne, w szczególności uniwersytety
- org organizacje niekomercyjne
- net organizacje związane z siecią
- gov pozamilitarne organizacje rządowe
- mil wojskowe organizacje rządowe
- num numery telefonów
- arpa domeny wyszukiwania odwrotnego
- xx dwuliterowe kody krajów (jak pl dla polski, de dla niemiec)
- biz przedsiębiorstwa i spółki
- info jednostki prowadzące usługi informacyjne
- aero przedsiębiorstwa związane z lotnictwem
- pro osoby samodzielnie prowadzące działalność gospodarczą
- coop spółdzielnie
- name domeny personalne
- museum muzea

Kolejny poziom hierarchii, zawierający konkretne stacje i dalsze poddomeny, tworzą domeny drugiego poziomu. „Microsoft" jest przykładem organizacji, która zarejestrowała domenę drugiego poziomu w domenie pierwszego poziomu COM.
Frazy MB, BC i AB przedstawiają jedną z technik podziału domeny narodowej – odpowiadaj poszczególnym prowincjom Kanady: MB to Manitoba, BC – Kolumbia Brytyjska, a AB – Alberta. W ten sposób powstaje geograficzny podział domeny kraju.

3. Proces odwzorowywania nazw stacji



Rys.: Proces odwzorowywania hostnames

Źródło: Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion, strona 139

Proces ten przebiega w kilku etapach:

- Czy przedmiotowa nazwa jest nazwą stacji, na której aktualnie pracujesz?
- Czy przedmiotowa nazwa występuje w pliku HOSTS?
- Czy serwer DNS posiada wpis odpowiadający poszukiwanej stacji?
- Czy nazwa stacji została zarejestrowana na serwerze WINS?
- Czy nazwa stacji może zostać odwzorowana za pośrednictwem lokalnego rozgłoszenia?
- Czy nazwa stacji została zapisana w pliku LMHOSTS?

Kiedy żadna z tych metod określania adresu IP stacji docelowej nie zakończy się powodzeniem, aplikacja zwraca komunikat informujący, że nazwa stacji nie została odnaleziona.

4. Podział ról w systemie DNS

W procesie odwzorowania nazwy, jaki zachodzi w systemie przestrzeni nazw domen, biorą udział trzy rodzaje podstawowych elementów:

- przestrzeń nazw domen
- klienty odwzorowania
- serwery nazw

4.1. Przestrzeń nazw domen

Zapewnia rozproszoną, hierarchiczną bazę danych, która zawiera wszystkie przyporządkowania nazw stacji do adresów IP w Internecie. Pozwala więc odwzorować dowolną nazwę stacji na jej adres IP.

4.2. Klienty odwzorowania

Jest to oprogramowanie klienckie, które wymaga odwzorowania nazwy na adres IP. Funkcje klienta odwzorowania są albo częścią aplikacji wywołującej, albo też uruchomione są w systemie operacyjnym stacji jako część stosu protokołu TCP/IP.

4.3. Serwery nazw

To obecne w sieci stacje przyjmujące zapytania od klientów odwzorowania i zwracające adresy IP poszukiwanych stacji. W zależności od konfiguracji i przyjętego zapytania serwer nazw może zwracać adres IP odpowiadający nazwie stacji, nazwę odpowiadającą adresowi IP, odpowiedź informującą o tym, że nazwa stacji nie została odnaleziona lub wskazanie innego serwera nazw, który może zrealizować zapytanie.

Każdy z serwerów nazw może występować jako:

- Podstawowy serwer nazw
- Pomocniczy serwer nazw
- Główny serwer nazw
- Serwer nazw buforujący

4.3.1. Podstawowy serwer nazw

Podstawowy serwer naw zarządza strefą danych. Termin strefa oznacza część przestrzeni nazw domen, za który odpowiedzialny jest konkretny serwer nazw. Pliki danych dla strefy są przechowywane lokalnie na podstawowym serwerze nazw. Wszystkie modyfikacje w tych plikach mogą być przeprowadzane wyłącznie na tym serwerze. Strefa obsługiwana przez podstawowy serwer nazw może obejmować więcej niż jedną domenę. Może on zarządzać poddomenami w określonej domenie albo też przechowywać pliki związane z kilkoma różnymi domenami drugiego poziomu.

4.3.2. Pomocniczy serwer nazw

Pomocniczy serwer nazw uzyskuje informacje o strefie z innego serwera posiadającego plik strefy; owym „innym serwerem" może być jakiś serwer pomocniczy lub też serwer podstawowy. Operacja przesłania informacji o strefie jest zwięźle określana terminem przesłanie strefy.

Poniżej przedstawiono powody przemawiające za wprowadzeniem serwera pomocniczego:

- potrzeba rozłożenia obsługi ruchu sieciowego na dodatkowy serwer z tymi samymi danymi strefy
- potrzeba przyspieszenia odwzorowywania w ośrodku odległym przez utworzenie w nim dodatkowego serwera nazw
- potrzeba zmniejszenia awaryjności układu przez utworzenie dodatkowego serwera zapewniającego utrzymanie możliwości odwzorowywania nawet w przypadku utraty funkcjonalności przez jeden z serwerów nazw
- utworzenie serwera pomocniczego jest warunkiem zarejestrowania domeny w InterNIC

Pliki stref przechowywane na serwerach pomocniczych nie są nigdy aktualizowane bezpośrednio – są jedynie kopiami plików przechowywanych na serwerach podstawowych. Stąd też stosowane jest niekiedy określenie serwer podległy.

4.3.3. Główny serwer nazw

Główny serwer nazw to serwer nazw, który przesyła swoje pliki stref do serwera pomocniczego. Chociaż mogłoby się wydawać, że jedynie podstawowe serwery nazw pracują jako serwery główne, również serwer pomocniczy może pełnić tę rolę. Sytuacja taka może wyniknąć z właściwości wykorzystywanych łączy sieciowych.
W konfiguracji serwera pomocniczego wskazywany jest adres IP serwera głównego. Podczas inicjalizacji komunikuje się on ze wskazanym serwerem głównym i inicjuje przesyłanie danych DNS strefy.

4.3.4. Buforujące serwery nazw

Buforujący serwer nazw nie przechowuje informacji strefowej na lokalnych nośnikach danych. Kiedy stacja przesyła zapytanie do serwera buforującego, ten przekazuje je dalej „w imieniu" tej stacji, buforuje wynik i zwraca klientowi adres IP poszukiwanej stacji. Kiedy później odbiera takie samo zapytanie od innej stacji, odpowiedź jest przekazywana na podstawie danych wciąż przechowywanych w buforze.
Tego rodzaju rozwiązanie staje się użyteczne, gdy łącza sieci rozległej posiadają stosunkowo niewielką przepustowość. Zamiast serwera pomocniczego, który wymaga regularnego przesyłania pełnej informacji o strefie, może zostać utworzony jedynie serwer buforujący. Przesyłane są wówczas jedynie faktycznie użyteczne dane. W buforze przechowywane są wtedy informacje o najczęściej odwiedzanych miejscach i skorzystanie z nich nie wymaga żadnego ruchu na łączach sieci WAN.

5. Rodzaje zapytań DNS

Klient odwzorowania może kierować do serwera nazw następujące rodzaje zapytań:

- Rekurencyjne
- Iteracyjne
- Odwrotne

5.1. Zapytania rekurencyjne

W przypadku zapytania rekurencyjnego serwer nazw może zwrócić wyłącznie adres IP odpowiadający wskazanej stacji albo informację o błędzie. Często wymaga to pełnienia przezeń roli klienta odwzorowania i przekazania zapytania do dalszego, wskazanego w konfiguracji, serwera nazw.

Przykład odwzorowywania do adresu IP nazwy www.yahoo.com:

- Klient DNS przesyła zapytanie rekurencyjne do wewnętrznego serwera DNS, żądając adresu IP stacji www.yahoo.com
- Wewnętrzny serwer DNS, nie znając odpowiedzi na otrzymane zapytanie, generuje kolejne zapytanie rekurencyjne do serwera ISP (usługodawcy

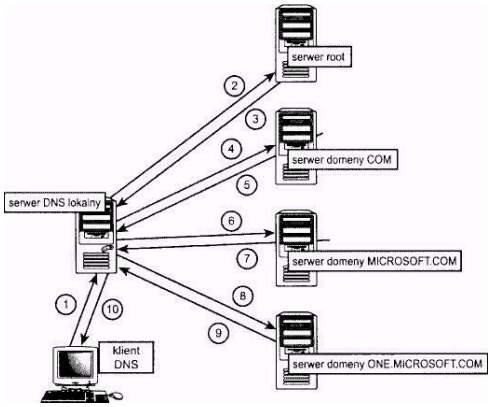
internetowego). Adres serwera ISP jest zapisany w konfiguracji serwera wewnętrznego

- Serwer DNS usługodawcy internetowego przekazuje wewnętrznemu serwerowi DNS adres IP stacji www.yahoo.com. Powiązanie adresu z nazwą zostaje zapisane w buforze (pamięci podręcznej) serwera
- Wewnętrzny serwer DNS zwraca adres IP klientowi

Tego rodzaju konfiguracja sprawdza się w przypadku sieci lokalnej oddzielonej od Internetu zaporą firewall. Wówczas należy zadbać o odpowiednie skonfigurowanie zapory – musi ona dopuszczać wymianę danych pomiędzy wewnętrznym serwerem DNS, a serwerem DNS usługodawcy. Serwer DNS powinien być wówczas jedynym komputerem, który może przekazywać zapytania DNS do sieci zewnętrznej. Użycie zapytania rekurencyjnego pozwala wewnętrznemu serwerowi DNS przekazać je do wskazanego w konfiguracji serwera nazw, po czym zwrócić odpowiedź w postaci adresu IP do stacji inicjującej.

5.2. Zapytanie iteracyjne

Zapytanie iteracyjne nakłada na serwer nazw wymóg podania klientowi jedynie najlepszej z możliwych odpowiedzi. Odpowiedzią może być zarówno adres IP poszukiwanej stacji (lub informacja o braku możliwości odwzorowania), jak i wskazanie innego serwera DNS, który może dostarczyć adres IP odpowiadający poszukiwanej nazwie.



Rys.: Iteracyjne zapytanie DNS

Źródło: Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion, strona 146

W celu odwzorowania nazwy altavista.digilal.com wykonane zostały następujące kroki:

- Klient DNS wysyła do swojego serwera DNS rekurencyjne zapytanie o adres IP odpowiadający nazwie altavista.digital.com
- Serwer DNS nie ma odpowiedzi w swoim buforze ani też wskazania w konfiguracji, pozwalającego kontynuować zapytanie rekurencyjne. Wysyła więc do serwera root zapytanie iteracyjne o adres odpowiadający nazwie altavistu.digital.com
- Serwer root zwraca lokalnemu serwerowi DNS adres IP serwera domeny wysokiego poziomu com.
- Lokalny serwer DNS wysyła do serwera nazw domeny com kolejne zapytanie iteracyjne, również o nazwę altavista.digital.com.
- Serwer nazw domeny com zwraca w odpowiedzi adres IP autorytatywnego serwera nazw domeny digital.com.
- Lokalny serwer DNS ponawia zapytanie o adres stacji altavistu.digital.com, kierując je do serwera nazw domeny digital.com.
- Jeżeli dane dotyczące poddomeny altavisla.digital.com są przechowywane w osobnym pliku strefy, na osobnym serwerze nazw, serwer DNS domeny digital.com zwróci adres serwera nazw odpowiadającego za domenę altavista.digital.com.
- Lokalny serwer nazw wysyła do serwera nazw domeny one.microsoft.com zapytanie o partnering.one.microsoft.com.
- Serwer one.microsoff.com zwraca adres IP stacji purlnering.one.microsoft.com, a jeżeli nazwa taka nie istnieje w tej domenie – informację o nieprawidłowej nazwie stacji.
- Lokalny serwer nazw przede wszystkim zapisuje adres IP stacji partnering. one.microsoft.com w swojej pamięci podręcznej. Po utworzeniu odpowiedniego wpisu przekazuje adres IP do klienta, który zainicjował procedurę.

5.3. Zapytanie odwrotne

Zapytanie odwrotne służy do odnalezienia pełnej kwalifikowanej nazwy domeny (FQDN) odpowiadającej określonemu adresowi IP. Zamiast określania adresu na

podstawie nazwy stacji wyszukujemy więc nazwę stacji odpowiadającą znanemu adresowi IP.

Jest to czynność powszechnie wykonywana przez osoby analizujące bezpieczeństwo sieci, kiedy próbują odwzorować adres IP stacji zapisanej w dzienniku bezpieczeństwa na jej internetową nazwę.

Jest również wykorzystywane przy ustalaniu reguł ograniczających dostęp do określonych ośrodków dla zapory firewall. Jeżeli zostało ustalone, że użytkownicy nie powinni uzyskiwać dostępu do ośrodka www.strony.com, zapora może zostać dodatkowo skonfigurowana do przeprowadzania wyszukiwań odwrotnych. Zabezpieczy to przed omijaniem przez użytkowników wprowadzonego ograniczenia przez bezpośrednie wpisanie adresu IP, jak np.: 192.168.5.67

6. Literatura

6.1. Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion.

6.2. Sportack, M. (1999). Sieci komputerowe – księga eksperta. Gliwice: Helion.

6.3. „PC World Komputer PRO”. Nr 3/2003.