

Laboratorium - Obserwacja procesu tłumaczenia nazw DNS

Cele

Część 1: Obserwacja konwersji DNS nazwy URL na adres IP.

Część 2: Obserwacja procesu przeszukiwania nazw DNS, przy pomocy polecenia Nslookup dla strony WWW.

Część 3: Obserwacja procesu przeszukiwania DNS, przy pomocy polecenia Nslookup dla serwerów e-mail.

Scenariusz

System nazw domenowych (DNS) jest uruchamiany wtedy, gdy w polu adresu przeglądarki WWW wpisujemy adres URL, np. <http://www.cisco.com>. Pierwsza część adresu URL określa jaki protokół będzie używany. Najczęściej spotykane protokoły to: Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) i File Transfer Protocol (FTP).

DNS zajmuje się drugą częścią adresu URL, którą w podanym przykładzie jest www.cisco.com. System DNS tłumaczy nazwę domeny (www.cisco.com) na adres IP w celu umożliwienia hostowi źródłowemu połączenia z hostem docelowym. W tym laboratorium zobaczysz jak działa DNS, a także użyjesz polecenia **nslookup** (name server lookup) by uzyskać więcej informacji o DNS. Wykonuj to laboratorium wraz z innym uczestnikiem zajęć.

Wymagane wyposażenie

- 1 PC (Windows 7, Vista or XP z dostępem do Internetu i wiersza poleceń)

Część 1: Obserwacja konwersji DNS nazwy URL na adres IP.

- Kliknij przycisk **Start** systemu Windows, w polu "Wyszukaj programy i pliki" wpisz **cmd** i naciśnij Enter. Po zatwierdzeniu polecenia pojawi się okno wiersza poleceń.
- W oknie wiersza poleceń wprowadź komendę ping oraz adres URL organizacji ICANN (ang. Internet Corporation for Assigned Names and Numbers) w postaci **www.icann.net**. ICANN jest organizacją odpowiedzialną za przyznawanie nazw domen internetowych, administrację adresów IP, a także za zarządzanie domenami i serwerami DNS najwyższego poziomu (root). Komputer musi przetłumaczyć ciąg znaków www.icann.net na adres IP, dzięki czemu będzie wiedział, gdzie przesłać pakiety ICMP (Internet Control Message Protocol).
- Pierwsza linia odpowiedzi pokazuje adres www.icann.net przetłumaczony przez DNS na adres IP. Powinieneś być w stanie zobaczyć efekt działania DNS nawet, jeśli twoja organizacja posiada zaporę ogniową, która blokuje pakiety wysyłane przez program ping lub jeśli serwer docelowy uniemożliwia "pingowanie" swojego serwera WWW.

```
C:\>ping www.icann.net

Pinging www.icann.net [192.0.43.22] with 32 bytes of data:
Reply from 192.0.43.22: bytes=32 time=112ms TTL=241
Reply from 192.0.43.22: bytes=32 time=119ms TTL=241
Reply from 192.0.43.22: bytes=32 time=113ms TTL=241
Reply from 192.0.43.22: bytes=32 time=115ms TTL=241

Ping statistics for 192.0.43.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 112ms, Maximum = 119ms, Average = 114ms
```

Zanotuj adres IP strony www.icann.net. _____

- d. Wpisz adres IP zamiast URL otrzymany w **kroku c** w pole adresu przeglądarki WWW. Zauważ, iż wyświetlona została strona domowa organizacji ICANN.



Większości ludzi dużo łatwiej przychodzi zapamiętywanie słów niż liczb. Jeśli powiesz komuś, aby udał się na stronę **www.icann.net**, istnieje duża szansa, że ta osoba ją zapamięta. Natomiast jeśli poprosisz ją o odwiedzenie strony o adresie 192.0.43.22, zapamiętanie takiego ciągu cyfr będzie kłopotliwe. Jednakże komputery przetwarzają liczby, a nie słowa. DNS jest procesem tłumaczenia słów na postać liczbową. Dodatkowo, zachodzi jeszcze drugi proces tłumaczenia. Ludzie operują na liczbach w systemie dziesiętnym. Komputery natomiast, operują liczbami w systemie binarnym (dwójkowym). Adres IP w systemie dziesiętnym w postaci 192.0.43.22, w systemie binarnym zapiszemy jako: 11000000.00000000.00101011.00010110. Co się stanie, jeżeli skopiujesz adres IP w systemie binarnym w pole adresu przeglądarki WWW?

- e. Wpisz ping www.cisco.com.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.144.170] with 32 bytes of data:
Reply from 23.1.144.170: bytes=32 time=51ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58

Ping statistics for 23.1.144.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 51ms, Average = 50ms
```

- f. Jeżeli, wykonasz polecenie ping www.cisco.com, uzyskasz adres IP taki jak w przykładzie, czy może będzie on inny? Odpowiedź uzasadnij.

- g. Wpisz w przeglądarce internetowej adres IP, który uzyskałeś podczas wysłania żądania ping do strony www.cisco.com. Czy strona WWW została wyświetlona? Uzasadnij swoją odpowiedź.

Część 2: Obserwacja procesu przeszukiwania DNS, przy pomocy polecenia Nslookup dla strony WWW.

- a. W wierszu poleceń wpisz komendę **nslookup**.

```
C:\>nslookup
Default Server:  dslrouter.westell.com
Address:  192.168.1.1
>
```

Podaj jaki jest domyślny, wykorzystywany serwer DNS?

Zwróć uwagę na zmianę znaku zachęty do postaci > . To jest znak zachęty polecenia **nslookup**. W tym trybie możesz wprowadzać polecenia związane z DNS.

Wprowadź ?, aby zobaczyć listę możliwych poleceń, które możesz używać w trybie **nslookup**.

- b. W trybie **nslookup**, za znakiem zachęty wpisz **www.cisco.com**.

```
> www.cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: e144.dscb.akamaiedge.net
Addresses: 2600:1408:7:1:9300::90
           2600:1408:7:1:8000::90
           2600:1408:7:1:9800::90
           23.1.144.170
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Jaki adres IP został wyświetlony? _____

Czy jest to ten sam adres IP uzyskany za pomocą polecenia **ping** ? _____

Pod polem Addresses (oprócz adresu IP 23.1.144.170), wypisane są następujące liczby: 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9800::90. Do czego one służą?

- c. W wierszu poleceń wpisz adres IP znalezionej serwera WWW firmy Cisco. Kiedy nie znasz URL, możesz użyć polecenia **nslookup** by na podstawie adresu IP otrzymać nazwę domeny internetowej.

```
> 23.1.144.170
Server: dslrouter.westell.com
Address: 192.168.1.1

Name: a23-1-144-170.deploy.akamaitechnologies.com
Address: 23.1.144.170
```

Możesz użyć narzędzia **nslookup** do tłumaczenia nazw domen internetowych na adresy IP. Możesz również używać go do tłumaczenia adresów IP na nazwy domen.

Korzystając z narzędzia **nslookup**, zapisz adresy IP powiązane z www.google.com.

```
> www.google.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400c:c01::93
           173.194.75.147
           173.194.75.105
           173.194.75.99
           173.194.75.103
           173.194.75.106
           173.194.75.104
```

Część 3: Obserwacja procesu przeszukiwania DNS, przy pomocy polecenia Nslookup dla serwerów e-mail.

- a. Za znakiem zachęty, wpisz `set type=mx` by `nslookup` identyfikował serwery pocztowe.

```
> set type=mx
```

- b. Za znakiem zachęty, wpisz `cisco.com`.

```
> cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
cisco.com      MX preference = 10, mail exchanger = rcdn-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = alln-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = ams-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = rtp-mx-01.cisco.com

ams-mx-01.cisco.com  internet address = 64.103.36.169
rcdn-mx-01.cisco.com internet address = 72.163.7.166
```

Podstawową regułą przy projektowaniu sieci jest nadmiarowość (skonfigurowanych jest więcej niż jeden serwer pocztowy). W ten sposób, jeśli jeden z serwerów pocztowych jest niedostępny, komputer próbuje skontaktować się z kolejnym. Administratorzy poczty przy pomocy parametru **MX preference** określają, który serwer pocztowy ma być używany jako pierwszy (spójrz na rysunek powyżej). Serwer pocztowy z najniższą wartością **MX preference** jest używany jako pierwszy. Bazując na powyższych danych, wskaż który serwer pocztowy zostanie użyty jako pierwszy, przy wysłaniu wiadomości e-mail do `cisco.com`?

-
- c. Za znakiem zachęty `nslookup`, wpisz `exit`, by powrócić do standardowego wiersza poleceń.
- d. W wierszu poleceń wpisz `ipconfig /all`.
- e. Wypisz adresy wszystkich serwerów DNS, których używa twoja szkoła.
-

Do przemyślenia

Jaki jest główny cel systemu DNS?
