

# DNS: podsumowanie

- Hosty i routery w Internecie są jednoznacznie identyfikowane przez tzw. adres IP
- Taka metoda identyfikacji nie byłaby wygodna w użyciu kiedy np.
  - adres IP musi ulec zmianie
  - jedna usługa (z punktu widzenia użytkownika) jest realizowana przez wiele serwerów
  - jeden serwer realizuje różne usługi

*Rozwiązaniem tego problemu jest wykorzystanie bardziej czytelnej dla człowieka nazwy zamiast adresu IP (np. [www.pjwstk.edu.pl](http://www.pjwstk.edu.pl))*

# DNS: podsumowanie

- DNS (Domain Name System) “tłumaczy” nazwy na konkretne adresy IP
- Usługa związana jest z portem 53 UDP (przede wszystkim)
- DNS działa jak rozproszona baza danych implementowana przez hierarchię wielu serwerów nazw

*Żaden serwer nie zna wszystkich odwzorowań!*

# DNS: podsumowanie

- **Autorytatywny serwer nazw dla hosta/domeny**

*Odpowiedzialny za przechowywanie odwzorowań DNS dla danego hosta/domeny*

- **Lokalny serwer nazw**

*Serwer przypisany do konkretnej organizacji. Zwykle do niego w pierwszej kolejności kierowane są zapytania!*

- **Serwery u korzenia**

*Z nimi kontaktują się lokalne serwery DNS, kiedy nie potrafią przetłumaczyć nazwy.*

*Jeśli serwer u korzenia nie zna odwzorowania, zwraca listę serwerów autorytatywnych dla odpowiedniej domeny.*

# DNS: podsumowanie

- Rodzaje zapytań

## Zapytania rekurencyjne

Jeśli pytany serwer nie zna odwzorowania, sam wyśle zapytanie do kolejnego serwera DNS przed odesłaniem odpowiedzi do klienta.

*Zwykle tak działają serwery lokalne*

## Zapytania iterowane

Jeśli pytany serwer nie zna odwzorowania, w odpowiedzi odeśle nazwę kolejnego serwera, który należy spytać. Klient musi wysłać zapytanie do serwera sam.

*Tak działają np. serwery u korzenia*

Serwer nie musi obsługiwać zapytań rekurencyjnie!

# DNS: podsumowanie

- Kiedy serwer pozna odwzorowanie, zachowuje je w schowku
  - Potencjalne zagrożenie atakiem DNS cache poisoning
  - Te informacje są po pewnym czasie usuwane

Odpowiedzi autorytatywne	Odpowiedzi nieautorytatywne
Pochodzą od serwera autorytatywnego dla danej domeny	Odpowiedzi na podstawie danych ze schowka – nie pochodzą bezpośrednio od serwera autorytatywnego dla danej domeny

# DNS: podsumowanie

- Wybrane typy rekordów DNS

<b>A</b>	Wartość to adres IP hosta o podanej nazwie
<b>NS</b>	Wartość to nazwa autorytatywnego serwera nazw dla danej domeny
<b>CNAME</b>	Wartość jest nazwą kanoniczną* serwera o podanym aliasie
<b>MX</b>	Nazwa serwera poczty związanego z podaną nazwą

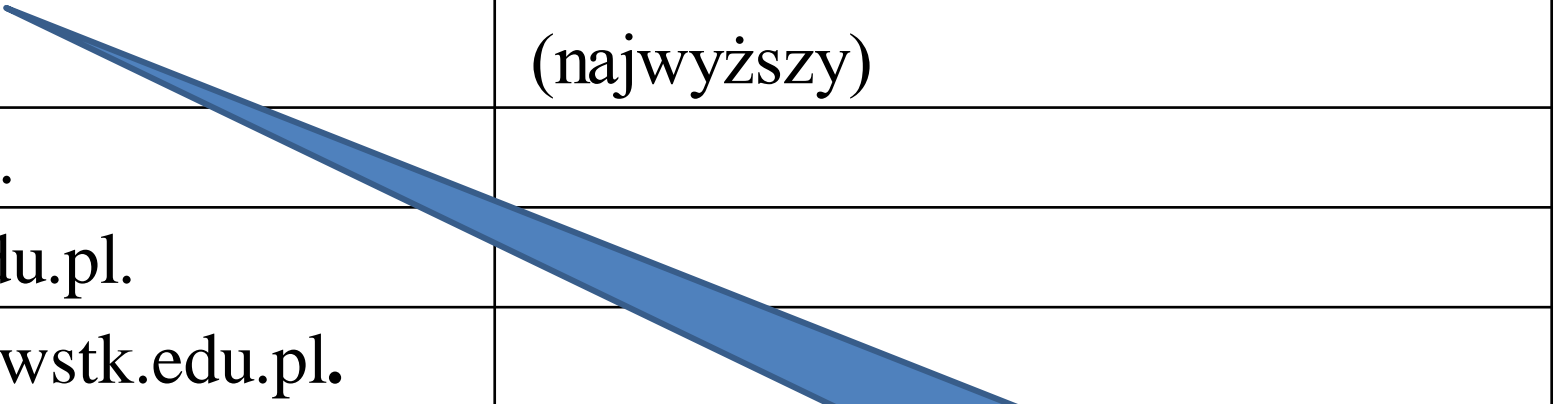
\* *Nazwa kanoniczna to właściwa nazwa serwera, który ma zdefiniowany określony alias  
(tak jak prawdziwe imię i nazwisko)*

# DNS: podsumowanie

- Struktura domen w DNS na przykładzie domeny pjwtst.edu.pl

*a tak naprawdę domeny pjwtst.edu.pl.*

.	Poziom serwerów u korzenia (najwyższy)
pl.	
edu.pl.	
pjwtst.edu.pl.	



*Nie musimy pisać ostatniej kropki...*

# DNS: podsumowanie

- Polecenie 'dig' pozwala na wykonywanie zapytań DNS (w systemie Linux)
  - Wykorzystamy je do zobrazowania działania DNS

*Wykorzystajmy polecenie 'dig', żeby sprawdzić, jaka jest właściwa (kanoniczna) nazwa serwerów translate.google.pl...*



# DNS: podsumowanie

*Polecenie...*

```
tiia@fluorite:~$ dig -t CNAME translate.google.pl

; <<>> DiG 9.7.1-P2 <<>> -t CNAME translate.google.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46208
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;translate.google.pl.                IN      CNAME

;; ANSWER SECTION:
translate.google.pl.                71234 IN      CNAME translate.google.com.
```

*Szukana odpowiedź...*

# DNS: podsumowanie

*Nazwy serwerów autorytatywnych dla danej domeny*

:: AUTHORITY SECTION:

google.pl.	53990	IN	NS	ns2.google.com.
google.pl.	53990	IN	NS	ns1.google.com.

:: ADDITIONAL SECTION:

ns1.google.com.	1213	IN	A	216.239.32.10
ns2.google.com.	1209	IN	A	216.239.34.10

*Adresy serwerów DNS dla danej domeny*

:: Query time: 30 msec

:: SERVER: 212.76.34.49#53(212.76.34.49)

:: WHEN: Wed Mar 2 12:27:56 2011

:: MSG SIZE rcvd: 139

# DNS: podsumowanie

*Sprawdźmy jeszcze ile jest na świecie serwerów u korzenia i jakie są ich nazwy oraz adresy IP...*

# DNS: podsumowanie

*Polecenie...*

```
tiia@fluorite:~$ dig -t NS .
```

```
; <<>> DiG 9.7.1-P2 <<>> -t NS .
```

```
:: global options: +cmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2306
```

```
:: flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 15
```

```
:: QUESTION SECTION:
```

```
;;                               IN      NS
```

# DNS: podsumowanie

:: ANSWER SECTION:

.	73598	IN	NS	e.root-servers.net.
.	73598	IN	NS	g.root-servers.net.
.	73598	IN	NS	l.root-servers.net.
.	73598	IN	NS	j.root-servers.net.
.	73598	IN	NS	c.root-servers.net.
.	73598	IN	NS	d.root-servers.net.
.	73598	IN	NS	i.root-servers.net.
.	73598	IN	NS	k.root-servers.net.
.	73598	IN	NS	m.root-servers.net.
.	73598	IN	NS	h.root-servers.net.
.	73598	IN	NS	b.root-servers.net.
.	73598	IN	NS	a.root-servers.net.
.	73598	IN	NS	f.root-servers.net.

*Nazwy serwerów DNS u korzenia*

# DNS: podsumowanie

:: ADDITIONAL SECTION:

a.root-servers.net.80607 IN  
a.root-servers.net.70781 IN  
b.root-servers.net.82638 IN  
c.root-servers.net.82638 IN  
d.root-servers.net.82638 IN  
e.root-servers.net.82638 IN  
f.root-servers.net.82638 IN  
g.root-servers.net.75011 IN  
h.root-servers.net.82638 IN  
i.root-servers.net.82638 IN  
i.root-servers.net.35555 IN  
j.root-servers.net.84709 IN  
k.root-servers.net.85858 IN  
k.root-servers.net.73664 IN  
l.root-servers.net.16802 IN

A	198.41.0.4
AAAA	2001:503:ba3e::2:30
A	192.228.79.201
A	192.33.4.12
A	128.8.10.90
A	192.203.230.10
A	192.5.5.241
A	192.112.36.4
A	128.63.2.53
A	192.36.148.17
AAAA	2001:7fe::53
A	192.58.128.30
A	193.0.14.129
AAAA	2001:7fd::1
A	199.7.83.42

*Adresy IP serwerów DNS u korzenia*

# DNS: podsumowanie

*Co oznacza zaznaczony adres na końcu odpowiedzi?*

```
:: Query time: 10 msec
:: SERVER: 212.76.34.49#53(212.76.34.49)
:: WHEN: Wed Mar  2 12:56:36 2011
:: MSG SIZE rcvd: 504
```

*Jakieś pomysły?*

# DNS: podsumowanie

*Co oznacza zaznaczony adres na końcu odpowiedzi?*

```
:: Query time: 10 msec  
:: SERVER: 212.76.34.49#53(212.76.34.49)  
:: WHEN: Wed Mar  2 12:56:36 2011  
:: MSG SIZE rcvd: 504
```

*To jest adres **lokalnego serwera DNS**, który udzielił nam odpowiedzi...*



# DNS: podsumowanie

*W poniższym przykładzie wysyłamy zapytanie bezpośrednio do serwera a.root-servers.net.*

Polecenie...

```
tiia@fluorite:~$ dig -t CNAME translate.google.se @a.root-servers.net.  
; <<>> DiG 9.7.1-P2 <<>> -t CNAME translate.google.se @a.root-servers.net.  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23406  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 13
```

# DNS: podsumowanie

```
:: WARNING: recursion requested but not available
```

```
:: QUESTION SECTION:
```

```
:translate.google.se.      IN      CNAME
```

```
:: AUTHORITY SECTION:
```

se.	172800 IN	NS	a.ns.se.
se.	172800 IN	NS	b.ns.se.
se.	172800 IN	NS	c.ns.se.
se.	172800 IN	NS	d.ns.se.
se.	172800 IN	NS	e.ns.se.
se.	172800 IN	NS	f.ns.se.
se.	172800 IN	NS	g.ns.se.
se.	172800 IN	NS	h.ns.se.
se.	172800 IN	NS	i.ns.se.
se.	172800 IN	NS	j.ns.se.

```
:: ADDITIONAL SECTION:
```

a.ns.se.	172800 IN	AAAA	2a01:3f0:0:301::53
----------	-----------	------	--------------------

*Serwery u korzenia nie obsługują rekurencji!*

*W odpowiedzi na zapytanie otrzymaliśmy listę serwerów autorytatywnych dla domeny se. ale zapytanie do któregoś z nich musimy wysłać sami.*

# DNS: podsumowanie

- Odpowiednikiem polecenia „dig” w systemie Windows jest program „nslookup”
- Ręczne modyfikacje listy serwerów DNS w systemie Linux
  - /etc/resolv.conf

```
nameserver 202.54.1.10

nameserver 202.54.1.11
```
- Lokalna konfiguracja odwzorowań ip->nazwa
  - /etc/hosts

IPAddress	Hostname	Alias
127.0.0.1	localhost	deep.openna.com
208.164.186.1	deep.openna.com	deep
208.164.186.2	mail.openna.com	mail
208.164.186.3	web.openna.com	web

- Szczegółowe informacje na temat DNS

<http://pl.wikipedia.org/wiki/DNS>