



**AKADEMIA GÓRNICZO-HUTNICZA  
IM. STANISŁAWA STASZICA W KRAKOWIE**

# **Sieci komputerowe**

## **Domain Name System**

**dr inż. Andrzej Opaliński  
andrzej.opalinski@agh.edu.pl**

# Wprowadzenie

- **DNS – Domain Name System – system nazw domenowych**
  - Protokół komunikacyjny
  - Usługa
- **Główne zadanie:**  
„Tłumaczenie nazwy mnemonicznej na odpowiadający jej adres IP”
- **Przykład:**
  - **www.agh.edu.pl -> 149.156.96.52**

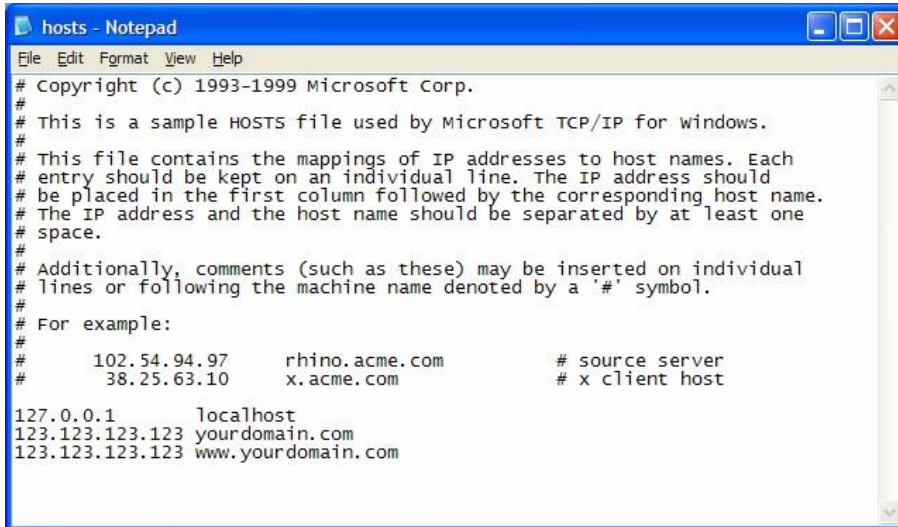


# Historia

- **Opracowany na potrzeby dostarczania poczty w sieci ARPANET**
  - 1982 rok – RFC 819 - podstawy
  - 1983 rok - RFC881, RFC882, RFC883 – oficjalna specyfikacja
  - 1989 rok – RFC1034, RFC1034 – nowa specyfikacja
  - 1996 rok – RFC 1918 – „Internet Best Current Practices”
- **Zastąpił plik hosts.txt**
  - Pozostałość istnieje w większości systemów operacyjnych
    - LINUX/UNIX - /etc/hosts
    - Windows – Windows\system32\drivers\etc\hosts
  - Hosts.txt funkcjonował przez 10 lat
  - Lata 70/80 – znaczny wzrost liczby hostów w ARPANET
  - Duży rozmiar pliku
  - Częste zmiany przypisani (nazwa-adres) wymagały transferu pliku do wszystkich hostów
  - Transfer poczty wymagał specyfikacji hostów pośredniczących
    - utzoo!decvax!harpo!eagle!mhtsa!ihnss!ihuxp!grg
    - user@host

# Plik hosts obecnie

- **Każda linia jest osobnym wpisem**
- **Zawiera:**
  - Adres IP v4 lub v6
  - Nazwę długą i/lub krótką
- **Użycie pliku hosts przez resolver**
  - Linux - /etc/hosts.conf, /etc/nsswitch.conf
  - Windows – wpisy w rejestrach



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com        # x client host

127.0.0.1        localhost
123.123.123.123  yourdomain.com
123.123.123.123  www.yourdomain.com
```

```
127.0.0.1        localhost        #IPv4
255.255.255.255 broadcasthost
fe80::1%lo0     localhost        #MacOSX
149.156.112.55  tempus.metal.agh.edu.pl  tempus
# IPv6
::1             localhost ipv6-localhost ipv6-loopback
fe00::0        ipv6-localnet
ff00::0        ipv6-mcastprefix
ff02::1        ipv6-allnodes
ff02::2        ipv6-allrouters
ff02::3        ipv6-allhosts
```

# Struktura systemu DNS

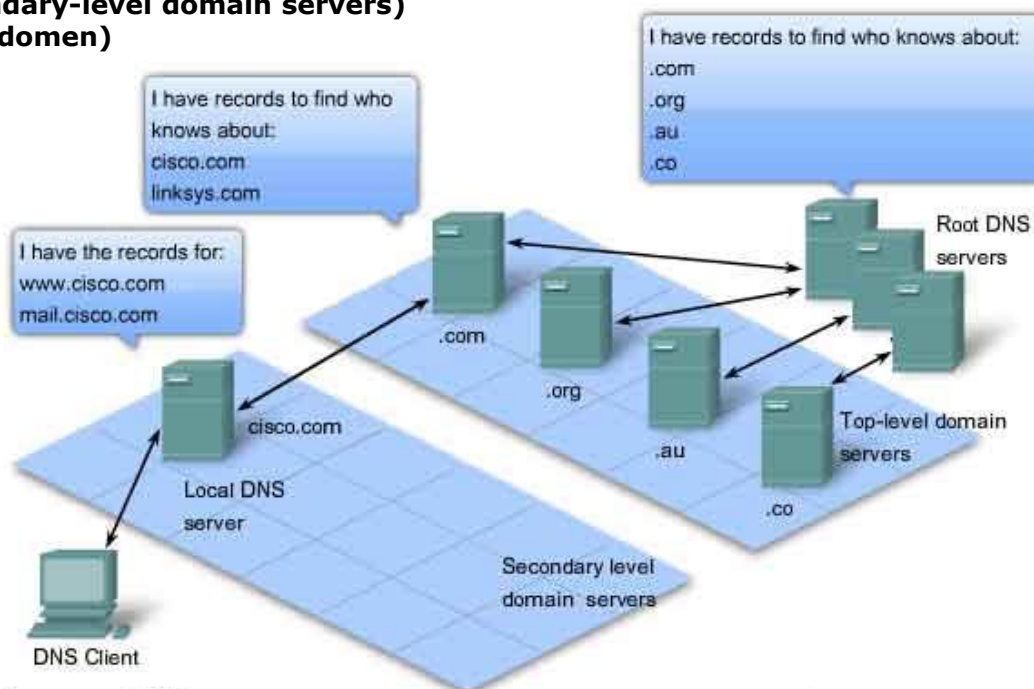
- Ogólnosiwiatowa sieć serwerów (przechowujących informacje na temat adresów domen)
- Drzewiasta struktura
  - 13 „root” serwerów (root servers) - ftp://ftp.rs.internic.net/domain/named.root
  - Serwery główne (top-level domain servers) – domeny krajowe, funkcyjne
  - Serwery niższego rzędu (secondary-level domain servers) (przechowują dane wybranych domen)

## • Serwery „root”

```

;
.
A.ROOT-SERVERS.NET. 3600000 NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.
B.ROOT-SERVERS.NET. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 192.228.79.201
B.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:84::b
;
; FORMERLY C.PSI.NET
;
.
C.ROOT-SERVERS.NET. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
C.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.
D.ROOT-SERVERS.NET. 3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 199.7.91.13
D.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.
E.ROOT-SERVERS.NET. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
;
; FORMERLY NS.ISC.ORG

```

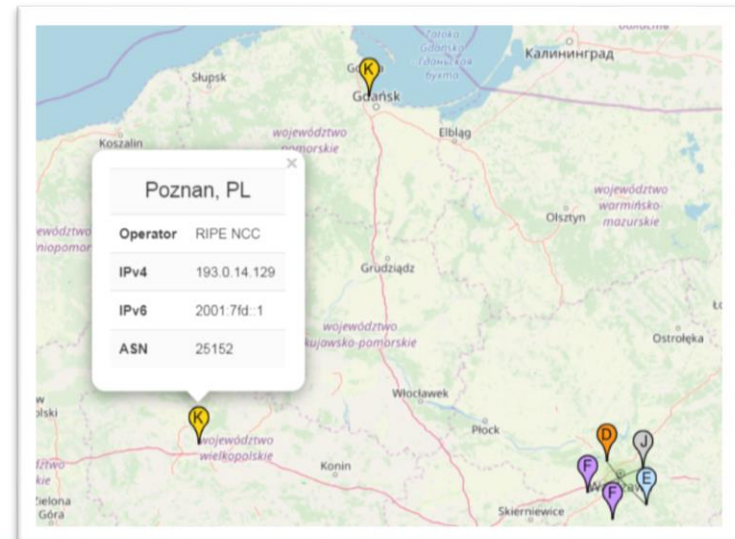


A hierarchy of DNS servers contains the resource records that match names with addresses.

# Root serwery DNS

- **ftp://ftp.rs.internic.net/domain/named.root**
- **https://www.iana.org/domains/root/servers**
- **Fizycznie każdy root serwer ma kilkadziesiąt kopii rozmieszczonych po całym świecie**
- **Aktualnie (listopad 2019) działa 1019 egzemplarzy root serwerów obsługiwanych przez 12 niezależnych operatorów**

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project



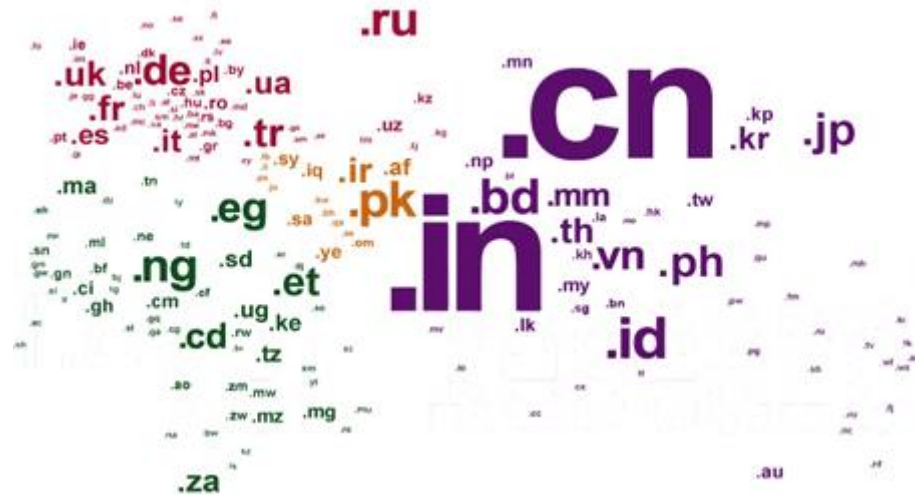
# Domeny najwyższego poziomu

- **Top Level Domains (TLD)**
  - Tworzone i zarządzane przez
    - IANA – Internet Assigned Numbers Authority
    - ICANN – The Internet Corporation for Assigned Names and Numbers
- **typy domen TLD**
  - Funkcjonalne (gTLD – generic TLD)
    - Niesponsorowane
      - .com – komercyjne
      - .org – organizacje
      - .net – internetowe
      - .int – organizacje międzynarodowe
      - .edu – uczelnie wyższe w USA
      - .gov – organizacje rządowe w USA
      - .mil – organizacje wojskowe w USA
    - Sponsorowane
      - .aero – transport lotniczy
      - .mobi – telefonia komórkowa
    - Infrastrukturalne
      - .arpa – infrastruktura sieciowa internetu (Reverse DNS)
      - .root – niektóre główne serwery DNS
    - Usługowe (.post, .tel)
    - Inne (.kids, .xxx, .eco)
  - Krajowe (ccTLD – country code TLD)



# Krajowe domeny najwyższego poziomu

- **ccTLD – (country code TLD)**
  - zawsze dwuliterowe
  - Odpowiadają kodom krajów ze standardu ISO 3166-1
  - Przyporządkowane także do odrębnych obszarów geograficznych
    - Hongkong (.hk)
    - Antyle Holenderskie (.an)
- **Przykłady**
  - .at – Austria
  - .dk – Dania
  - .ee – Estonia
  - .es – Hiszpania
  - .fm - Mikronezja
  - .it – Włochy
  - .pl – Polska
  - .se – Szwecja
  - .tv – Tuvalu
  - .uk – Wielka Brytania
  - .us – Stany Zjednoczone





# Domeny drugiego poziomu

- **W strukturze poniżej domeny najwyższego poziomu**
- **Subdomena TLD**
- **Rodzaje domen (Przykład dla domeny TLD .pl)**
  - Regionalne
    - krakow.pl,
    - malopolska.pl
  - Funkcjonalne
    - com.pl - biznesowe
    - gov.pl – rządowe
    - org.pl – organizacje pozarządowe
  - Należące do firm lub osób prywatnych
    - zus.pl
    - kazik.pl
    - filmweb.pl



# Nazwy domen

- **Węzły - Etykiety tekstowe o długości od 1 do 63 znaków**
- **Oddzielane kropką „.”**
- **Dozwolone znaki**
  - Standardowo
    - Litery
    - Cyfry
    - Znak „-”
  - Znaki narodowe (IDN) – Internationalized Domain Name
    - Zawierają znaki spoza kodu ASCII
    - W języku polskim: ą, ć, ę, ł, ń, ó, ś, ź, ż
    - Przekształcanie do 7bitowych znaków - Punycode (RFC 3490)
    - Technicznie: prefix „xn—” przed nazwą domeny
    - Obecnie standardowo obsługiwane przez wszystkie przeglądarki i programy pocztowe

Unicode form of IDN

[www.róźyczka.pl](http://www.róźyczka.pl)

ASCII form (called as well ACE form) of IDN stored in DNS resources

ACE - ASCII Compatible Encoding

prefiks ACE

etykieta ACE

[www.xn--ryczka-bxa01i.pl](http://www.xn--ryczka-bxa01i.pl)

- **Dwie instytucje zarządzająco-nadzorcze**
  - IANA – Internet Assigned Numbers Authority
    - zarządzanie domenami najwyższego poziomu
    - Ogólny nadzór nad działaniem mechanizmu DN
  - ICANN – The Internet Corporation for Assigned Names and Numbers
    - Przyznawanie nazw domen internetowych
    - Ustalanie struktury domen
    - Administrowanie adresami IP
    - Przyznawanie parametrów protokołom internetowym
- **Rozdzielają domeny najwyższego poziomu (TLD) pomiędzy:**
  - Kraje
  - Organizacje(z przekazaniem praw do zarządzania)
- **Polska - rząd przekazał nadzór nad domeną .pl Naukowej i Akademickiej Sieci Komputerowej (NASK)**  
(także gov.pl, com.pl, biz.pl, org.pl, net.pl, waw.pl, ...)



- **Naukowa i Akademicka Sieć Komputerowa (NASK)**  
instytut badawczy znajdujący się przy ul. Kolskiej 12 w Warszawie.
  - **pełni funkcję rejestru domen internetowych (DNS) .pl,**
  - **domen ENUM (dla +48)**
  - **oferuje usługi teleinformatyczne**  
(IP transit, dostęp do Internetu, sieci VPN, VoIP, WiMAX).
- Powstał wiosną 1991 roku przy Uniwersytecie Warszawskim  
(17 sierpnia 1991 – pierwsza łączność IP z uniwersytetem w Kopenhadze)
- Rejestr domen internetowych .pl
  - Mechanizm automatyczny w oparciu o protokół EPP (Extensible Provisioning Protocol)
  - Model registry-registrar (NASK-partnerzy) (większość Home.pl i NetArt)
  - Ponad 2,46mln aktywnych nazw w domenie .pl na koniec 2020 roku  
(spadek o ok. 59 tys w porównaniu do roku poprzedniego)
  - 1,21% domen z polskimi znakami diaktrycznymi
  - 79% - w domenie .pl
  - 16% - w domenach funkcjonalnych
  - 5% - w domenach regionalnych
  - 2155 rejestracji dziennie
  - 65% odnowień

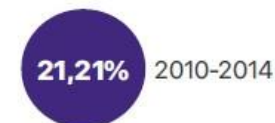
- **Raport NASK z 1 kwartału 2020**

- 2 451 047 aktywnych nazw w DNS
- Z czego 1 915 145 w domenie .pl
- 425 746 w domenach funkcjonalnych
- 110 183 w domenach regionalnych

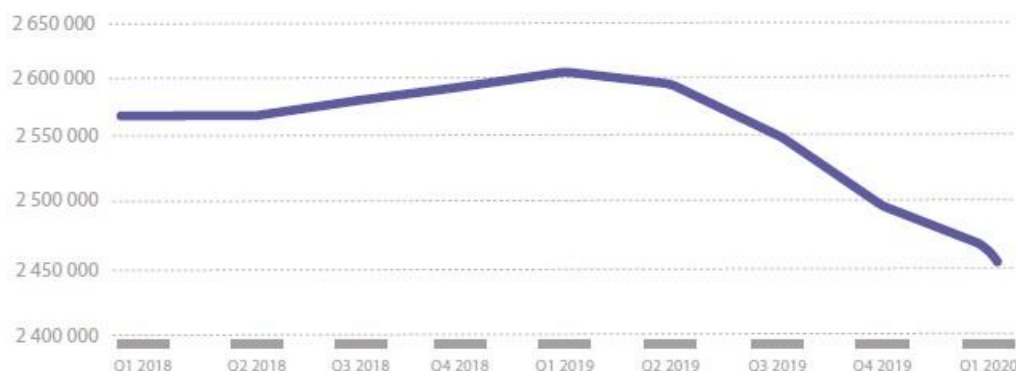
- **Transfery domen**

- 341 transferów dziennie

Rok rejestracji nazw  
domeny .pl  
aktywnych w DNS



Liczba nazw domeny .pl w DNS

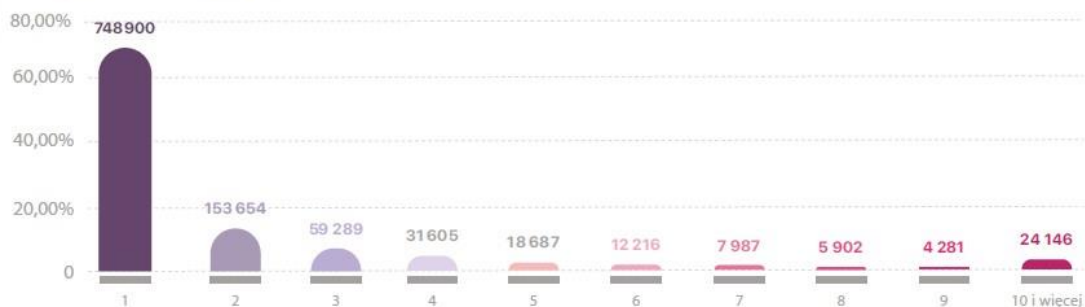


# NASK – struktura abonentów

## • Stan na koniec marca 2020

- 1 066 668 wpisów dotyczących unikalnych abonentów
- Mniej o 5 920 w porównaniu z rokiem poprzednim

Podział abonentów ze względu na utrzymywaną liczbę nazw domeny .pl, Q1 2020



Na jednego abonenta przypadają średnio **2,3** nazwy domeny .pl.



Od początku stycznia do końca marca 2020 roku wykonano **25 037** zmian abonentów nazwy domeny .pl.

Copyright by NASK

Struktura abonentów nazw domeny .pl, Q1 2020



Copyright by NASK

Aktywne w DNS nazwy domeny .pl podzielone na typ abonenta, Q1 2020



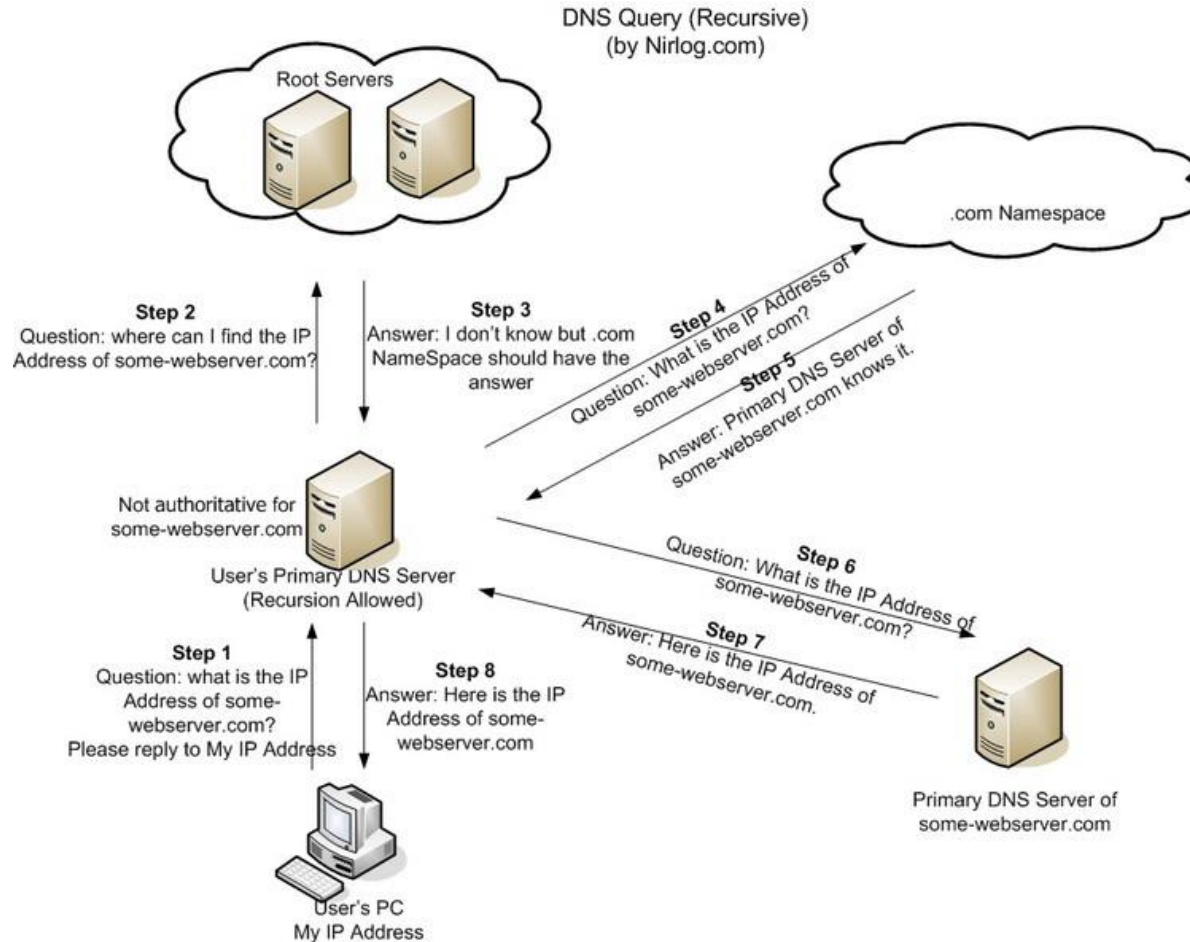
Copyright by NASK

Rejestracje nazw domeny .pl podzielone na typ abonenta, Q1 2020



Copyright by NASK

# Przykład zapytania DNS

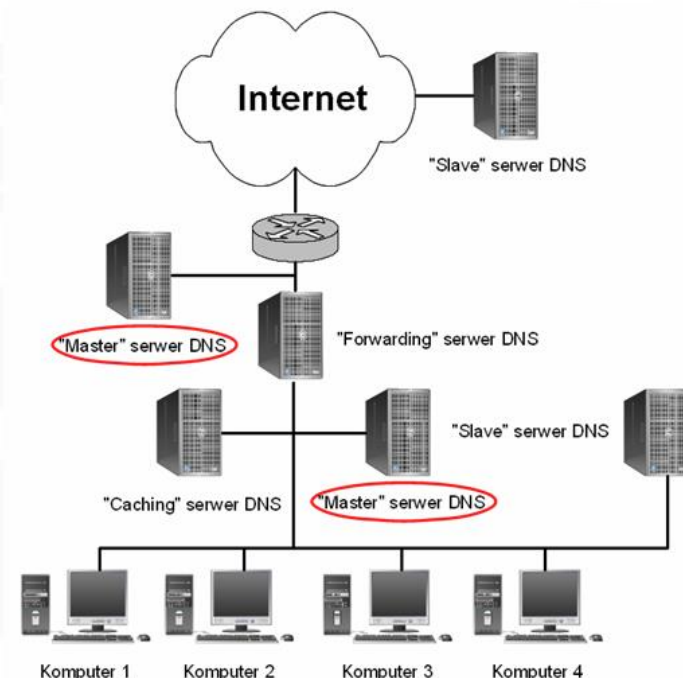




AGH

## Rodzaje serwerów DNS

- DNS Master Server
  - Na każdym poziomie systemu DNS
  - Przechowują dane źródłowe dla konkretnego poddrzewa danego poziomu
  - Funkcjonalności:
    - Transfer pełnych danych do serwerów slave
    - Odpowiedzi dot. domen zależnych
  - 5- liczba oficjalnych serwerów Master i Slave
- DNS Slave Server
  - Odpowiedzi o równym priorytecie co Master
  - Synchronizacja danych z serwerem Master (po zmianach, lub gdy nie ma pełnych danych)
  - Nieoficjalne serwery slave – do obsługi konkretnych segmentów sieci
- DNS Cache Server
  - Nie przechowuje informacji o systemie DNS jako Master lub Slave
  - Obsługuje segment sieci którego jest członkiem
  - Buforowanie informacji uzyskanych w wyniku wyszukiwania
- DNS Forward Server
  - Przeznaczony do komunikacji z serwerami spoza DMZ (Master, Slave, Cache)





# Zapytania DNS

- **Pomiędzy klientem (resolverem) a serwerem DNS**

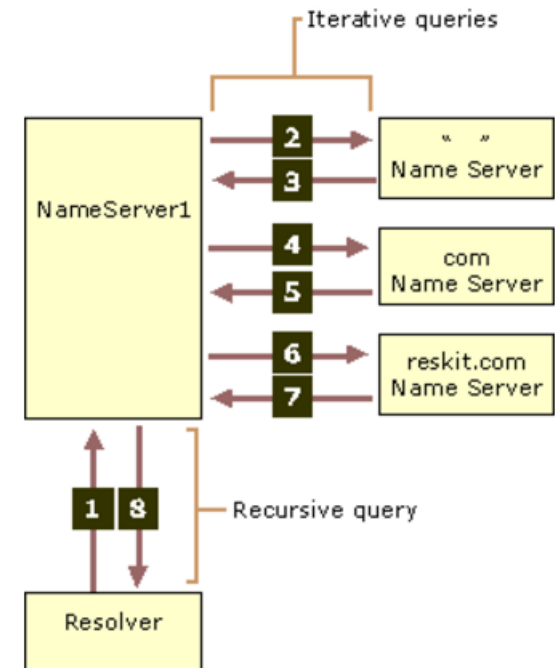
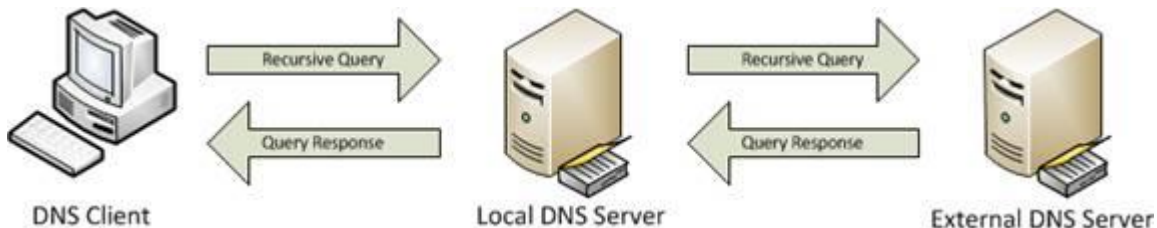
- **Rekurencyjne**

- Odpytywany serwer musi odnaleźć informacje o domenie lub zwrócić wiadomość o błędzie.
- Odpytywany serwer nie znając zapytania, odpytuje inne serwery DNS
- Umożliwia zapamiętanie odwzorowania w pamięci serwera (DNS caching)
- Realizowane jedynie przez:
  - serwery lokalne dla lokalnych hostów (resolverów) (realizowane później iteracyjnie)
  - Serwery forwardujące

- **Iteracyjne**

- Odpytywany serwer odpowiada najlepszą znaną mu odpowiedzią (np. adresem serwerów autorytatywnych dla danej domeny)
- Odpytywany serwer nie łączy się z innymi serwerami

- Przykład dla domeny noam.reskit.com



# Odpowiedzi DNS

## • Autorytatywne

- Dotyczą domen w strefie na którą dany serwer ma zarząd
- Pochodzą bezpośrednio z bazy danych serwera
- Zawiera ustawiony bit uwierzytelniania (AA – authoritative answer)

## • Nieautorytatywne

- Dane pochodzą spoza strefy zarządzanej przez dany serwer
- Odpowiedzi nieautorytatywne są na serwerze buforowane przez określony czas, po czym są usuwane

### ▣ Answers

- ▣ www.google.com: type A, class IN, addr 74.125.131.147  
Name: www.google.com  
Type: A (Host address)  
Class: IN (0x0001)  
Time to live: 5 minutes  
Data length: 4  
Addr: 74.125.131.147 (74.125.131.147)
- ▣ www.google.com: type A, class IN, addr 74.125.131.103
- ▣ www.google.com: type A, class IN, addr 74.125.131.104
- ▣ www.google.com: type A, class IN, addr 74.125.131.106
- ▣ www.google.com: type A, class IN, addr 74.125.131.99
- ▣ www.google.com: type A, class IN, addr 74.125.131.105

```
> metal.agh.edu.pl
Server: galaxy.agh.edu.pl
Address: 149.156.96.9

-----
Got answer:
HEADER:
  opcode = QUERY, id = 31, rcode = NOERROR
  header flags: response, auth. answer, want recursion, recursion avail.
  questions = 1, answers = 6, authority records = 0, additional = 8

QUESTIONS:
  metal.agh.edu.pl, type = ANY, class = IN
ANSWERS:
-> metal.agh.edu.pl
   ttl = 86400 (1 day)
   primary name server = sendzimir.metal.agh.edu.pl
   responsible mail addr = root@sendzimir.metal.agh.edu.pl
   serial = 20170208
   refresh = 10800 (3 hours)
   retry = 3600 (1 hour)
   expire = 604800 (7 days)
   default TTL = 86400 (1 day)
-> metal.agh.edu.pl
   nameserver = sendzimir.metal.agh.edu.pl
   ttl = 86400 (1 day)
```

```
> nokia.com
Server: galaxy.agh.edu.pl
Address: 149.156.96.9

-----
Got answer:
HEADER:
  opcode = QUERY, id = 30, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 7, authority records = 6, additional = 9

QUESTIONS:
  nokia.com, type = ANY, class = IN
ANSWERS:
-> nokia.com
   nameserver = ns.nokia.com
   ttl = 81616 (22 hours 40 mins 16 secs)
-> nokia.com
   nameserver = ns6.nokia.com
   ttl = 81616 (22 hours 40 mins 16 secs)
```



AGH

## Typy rekordów DNS

- SOA (start of authority record) – rekord adresu startowego uwierzytelniania  
(ustala serwer DNS dostarczający autorytatywne informacje o domenie wraz z parametrami)
- A (address record) – rekord adresu  
(mapuje nazwę domeny na adres IPv4)
- AAAA (IPv6 address record) – rekord adresu IPv6  
(mapuje nazwę domeny na adres IPv6)
- CNAME (canonical name record) – rekord nazwy kanonicznej  
(ustawia alias domeny)
- NS (name server record) – rekord serwera nazw  
(mapuje nazwę domenową na listę serwerów DNS dla tej domeny)
- MX (mail exchange record) – rekord wymiany poczty  
(mapuje nazwę domeny na nazwę serwera pocztowego oraz priorytet)
- PTR (pointer record) – rekord wskaźnika  
(mapuje adres IP (v4/6) na nazwę kanoniczną hosta)  
(pozwala na odwrotną translację adresów)
- SRV (service record) - rekord usługi  
(dodatkowe informacje dotyczące usługi udostępnianej przez serwer)
- TXT (text record) – rekord tekstowy  
(dodatkowe informacje tekstowe, np. specyfikacja SPF – Sender Policy Framework – zabezpieczenia pocztowe)

Typ	Dane
A	91.219.122.70
NS	ns1.webio.pl
NS	ns2.webio.pl
MX	[10], mail3.webio.pl
MX	[10], mail1.webio.pl
MX	[10], mail2.webio.pl
MX	[90], mailoffsite.webio.pl
TXT	v=spf1 a mx ip4:194.88.154.129/26 ip4:78.131.153.11 -all
SPF	v=spf1 a mx ip4:194.88.154.129/26 ip4:78.131.153.11 -all
A	91.219.122.70
CNAME	poczta.webio.pl
A	91.219.122.70
A	91.219.122.70
SRV	[443], poczta.webio.pl

# Uproszczony wpis konfiguracyjny serwera DNS

```
$TTL 86400
@ IN SOA ns1.test1.com.
postmaster.test1.com. (
    2001031102
    10800
    3600
    604800
    86400
) ;
IN      NS      ns1.test1.com.
IN      NS      ns2.test1.com.
IN      MX 1    mail.test1.com.
ns1     IN      A      192.168.1.4
ns2     IN      A      192.168.1.5
www     IN      A      192.168.1.6
www1    IN      CNAME   www
mail    IN      A      192.168.1.7
```

```
; example.com [448369]
$TTL 86400
@          IN  SOA ns1.linode.com.
admin.example.com. 2013062147 14400 14400
1209600 86400
@          NS  ns1.linode.com.
@          NS  ns2.linode.com.
@          NS  ns3.linode.com.
@          NS  ns4.linode.com.
@          NS  ns5.linode.com.
@          MX  10 mail.example.com.
@          A   12.34.56.78
mail       A   12.34.56.78
www        A   12.34.56.78
```

- TTL (Time To Live) – czas (w sekundach) przez który można przechowywać wpis w pamięci cache (później należy go odświeżyć)
- Standardowo wartości między 3600 (1h) a 86400 (1d)

- **Start of Authority (SOA) – rekord adresu startowego uwierzytelniania**
  - Ustala serwer DNS dostarczający autorytatywne informacje o domenie
  - Pola
    - MNAME (ns.icann.org) – główny serwer nazw dla tej domeny
    - RNAME (noc.dns.ican.org) – mailowy kontakt administracyjny (@ zamiast pierwszej kropki, dot escape - \.)
    - SERIAL – numer seryjny domeny (jego zwiększenie oznacza konieczność aktualizacji u serw. SLAVE)
    - REFRESH – co ile sekund serwer SLAVE powinien sprawdzać aktualizację SOA/serial
    - RETRY – co ile sekund serwer SLAVE powinien odpytać MASTER po braku odpowiedzi
    - EXPIRE – liczba sekund po jakiej SLAVE powinien przestać udzielać odpowiedzi, jeśli MASTER nie odpowiada (> REFRESH + RETRY)
    - TTL (minimum) – czas przez jaki resolver może przechowywać odpowiedź NXDOMAIN

```
$TTL 86400
@   IN  SOA      ns.icann.org. noc.dns.icann.org. (
      2020080302 ;Serial
      7200       ;Refresh
      3600       ;Retry
      1209600    ;Expire
      3600       ;Minimum TTL
)
```

## A oraz AAAA

- **A**
  - Przekierowują nazwę domeny na adres IPv4
  - Możliwość przekierowania różnych domen na różne adresy IP
  - Możliwość agregacji przekierowania subdomen za pomocą znaku (\*)
- **AAAA**
  - Przekierowują nazwę domeny na adres IPv6

example.com	A	12.34.56.70
test.example.com	A	12.34.56.80
hello.example.com	A	12.34.56.90
*.example.com	A	12.34.56.70
example.com	AAAA	0123:4567:89ab:cdef:0123:4567:89ab:cdef

# CNAME oraz MX

- **CNAME**

- Canonical Name record
- Przekierowanie domeny lub subdomeny na inną domenę – alias (nigdy nie na adres IP)
- Przykład:
  - Alias zmapowany na example
  - Example zmapowane na adres IPv4

- **MX**

- Mail exchanger record
- Ustawienie serwera obsługi poczty dla danej domeny
- Dodatkowo liczbowe pole priorytetu

alias.com	CNAME	example.com.
example.com	A	12.34.56.78
example.com	MX	10 mail.example.com.
mail.example.com	A	12.34.56.78
example.com	MX	10 mail_1.example.com
example.com	MX	20 mail_2.example.com
example.com	MX	30 mail_3.example.co

- **NS – Name Server**
  - Delegacja domeny (strefy) do konkretnych autorytatywnych serwerów nazw (DNS)
  - Przekierowanie na nazwę kanoniczną (a nie na adres IP)
- **PTR – Reverse-lookup Pointer**
  - Rekord wskaźnika
  - Mapuje adres IPv4/IPv6 na nazwę kanoniczną hosta (w domenie .arpa)
  - Umożliwia wsteczne wyszukiwanie nazw (w oparciu o adres IP)

@	IN	NS	ns1.example.com.
@	IN	NS	ns2.example.com
ns1	IN	A	198.51.100.2
ns2	IN	A	198.51.100.3
131.28.12.202.in-addr.arpa.	IN	PTR	svc00.example.com



- **SRV – Service Locator**

- Lokalizacja usług na serwerach w ramach strefy DNS
  - PRI – priorytety hosta (niższe wartości są bardziej preferowane)
  - WT – waga – względna waga dla wpisów o tym samym priorytecie (wyższe wartości są bardziej preferowane)
  - PORT – numer portu TCP lub UDP na którym znajduje się usługa
  - TARGET – kanoniczna nazwa serwera na którym znajduje się usługa

- **TXT – Rekord tekstowy**

- Przechowuje tekst w dowolnej formie
- Początkowo były to informacje o lokalizacji serwera lub centrów danych
- Aktualnie głównie przechowuje informacje na temat
  - SPF (Sender Policy Framework) – autoryzacja serwerów pocztowych dla danej domeny
  - DKIM (DomainKeys Identified Mail) – sygnatury wiadomości pocztowych

DOMAIN	TTL	TYPE	PRI	WT	PORT	TARGET
sip.g33k.fun.com	86400 IN	SRV	0	5	5060	sipserver.g33k.fun.com
g33k.fun.com	14400 IN	TXT	"v=spf1 +a +mx +ip4:67.257.187.136 ~all,"			
test-mail.dk.fun.com	IN	TXT	"v=DKIM1;k=rsa; p=MICSqGS...Gf9WZPcL86oSRmt4mwIDAQAB"			

# Klienci - resolvery

- **Resolvery**
  - zaimplementowane ramach systemu operacyjnego
  - Niewidoczne dla użytkownika
- **Programy dedykowane**
  - Nslookup
  - Host
  - Dig

```
> ?
Commands:  (identifiers are shown in uppercase, [] means optional)
NAME       - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ?  - print info on common commands
set OPTION - set an option
all        - print options, current server and host
[no]debug  - print debugging information
[no]d2     - print exhaustive debugging information
[no]defname - append domain name to each query
[no]recurse - ask for recursive answer to query
[no]search - use domain search list
[no]vc     - always use a virtual circuit
domain=NAME - set default domain name to NAME
srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
root=NAME  - set root server to NAME
retry=X    - set number of retries to X
timeout=X  - set initial time-out interval to X seconds
type=X     - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
querytype=X - same as type
class=X    - set query class (ex. IN (Internet), ANY)
[no]msxfr  - use MS fast zone transfer
ixfrver=X  - current version to use in IXFR transfer request
server NAME - set default server to NAME, using current default server
!server NAME - set default server to NAME, using initial server
root       - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
-a        - list canonical names and aliases
-d        - list all records
-t TYPE   - list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.)
view FILE - sort an 'ls' output file and view it with pg
exit     - exit the program

> agh.edu.pl
Server: [8.8.8.8]
Address: 8.8.8.8

Non-authoritative answer:
Name:      agh.edu.pl
Addresses: 2001:6d8:10:1060::6034
           149.156.96.52

>
```

# Resolver - nslookup

- Uruchamiany z linii komend

- Tryb prosty

```
> krakow.pl
Serwer: galaxy.agh.edu.pl
Address: 149.156.96.9

Nieautorytatywna odpowiedź:
Nazwa: krakow.pl
Address: 149.156.2.195
```

- Tryb debug

```
> set debug
> krakow.pl
Serwer: galaxy.agh.edu.pl
Address: 149.156.96.9

DNS request timed out.
  timeout was 2 seconds.
timeout (2 secs)
-----
Got answer:
HEADER:
  opcode = QUERY, id = 23, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
  krakow.pl, type = AAAA, class = IN
AUTHORITY RECORDS:
-> krakow.pl
  ttl = 10639 (2 hours 57 mins 19 secs)
  primary name server = nms.cyf-kr.edu.pl
  responsible mail addr = hostmaster.cyf-kr.edu.pl
  serial = 2017042501
  refresh = 28800 (8 hours)
  retry = 7200 (2 hours)
  expire = 604800 (7 days)
  default TTL = 86400 (1 day)

-----
Got answer:
HEADER:
  opcode = QUERY, id = 24, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 1, authority records = 4, additional = 6

QUESTIONS:
  krakow.pl, type = A, class = IN
ANSWERS:
-> krakow.pl
  internet address = 149.156.2.195
```

```
-> krakow.pl
  nameserver = nms.cyf-kr.edu.pl
  ttl = 81065 (22 hours 31 mins 5 secs)
ADDITIONAL RECORDS:
-> dns.fuw.edu.pl
  internet address = 193.0.80.11
  ttl = 1028 (17 mins 8 secs)
-> nms.cyf-kr.edu.pl
  internet address = 149.156.1.3
  ttl = 28479 (7 hours 54 mins 39 secs)
-> info.cyf-kr.edu.pl
  internet address = 149.156.4.11
  ttl = 28074 (7 hours 47 mins 54 secs)
-> bilbo.nask.org.pl
  internet address = 195.187.245.51
  ttl = 28465 (7 hours 54 mins 25 secs)
-> nms.cyf-kr.edu.pl
  AAAA IPu6 address = 2001:6d8:0:1::a:3
  ttl = 28479 (7 hours 54 mins 39 secs)
-> info.cyf-kr.edu.pl
  AAAA IPu6 address = 2001:6d8:0:4::11
  ttl = 28074 (7 hours 47 mins 54 secs)
```

-----  
Nieautorytatywna odpowiedź:  
-----

```
Got answer:
HEADER:
  opcode = QUERY, id = 25, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
  krakow.pl, type = AAAA, class = IN
AUTHORITY RECORDS:
-> krakow.pl
  ttl = 10639 (2 hours 57 mins 19 secs)
  primary name server = nms.cyf-kr.edu.pl
  responsible mail addr = hostmaster.cyf-kr.edu.pl
  serial = 2017042501
  refresh = 28800 (8 hours)
  retry = 7200 (2 hours)
  expire = 604800 (7 days)
  default TTL = 86400 (1 day)
```

```
-----
Nazwa: krakow.pl
Address: 149.156.2.195
```

- Klient linuxowy

```
opal@galaxy:~$ dig sendzimir.metal.agh.edu.pl

;<<> DiG 9.11.22 <<> sendzimir.metal.agh.edu.pl
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 2837
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sendzimir.metal.agh.edu.pl.      IN      A

;; ANSWER SECTION:
sendzimir.metal.agh.edu.pl. 2838 IN      A      149.156.111.10

;; AUTHORITY SECTION:
metal.agh.edu.pl.           70902 IN      NS      nms.cyf-kr.edu.pl.
metal.agh.edu.pl.           70902 IN      NS      sendzimir.metal.agh.edu.pl.
metal.agh.edu.pl.           70902 IN      NS      ns1.agh.edu.pl.
metal.agh.edu.pl.           70902 IN      NS      ns2.agh.edu.pl.

;; ADDITIONAL SECTION:
nms.cyf-kr.edu.pl.          5653  IN      A      149.156.1.3
nms.cyf-kr.edu.pl.          5653  IN      AAAA   2001:6d8:0:1::a:3
ns1.agh.edu.pl.             65674 IN      A      149.156.96.9
ns1.agh.edu.pl.             65674 IN      AAAA   2001:6d8:10:1060::6009
ns2.agh.edu.pl.             68680 IN      A      149.156.119.130
ns2.agh.edu.pl.             68680 IN      AAAA   2001:6d8:10:4036::7782

;; Query time: 0 msec
;; SERVER: 149.156.96.8#53(149.156.96.8)
;; WHEN: Tue Dec 15 13:21:50 CET 2020
;; MSG SIZE rcvd: 278
```

```
opal@galaxy:~$ dig nokia.com

;<<> DiG 9.11.22 <<> nokia.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 27921
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;nokia.com.                    IN      A

;; ANSWER SECTION:
nokia.com.                    432000 IN      A      162.13.40.196

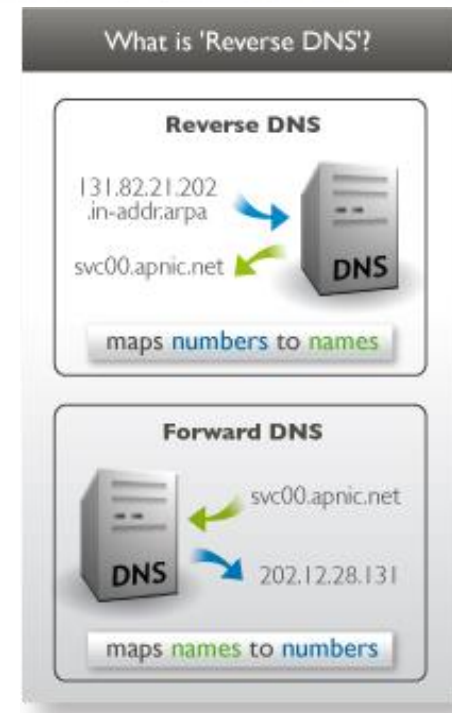
;; AUTHORITY SECTION:
nokia.com.                    13924  IN      NS      ns4.nokia.com.
nokia.com.                    13924  IN      NS      ns.nokia.com.
nokia.com.                    13924  IN      NS      ns2.nokia.com.
nokia.com.                    13924  IN      NS      ns3.nokia.com.
nokia.com.                    13924  IN      NS      ns6.nokia.com.
nokia.com.                    13924  IN      NS      ns5.nokia.com.

;; ADDITIONAL SECTION:
ns.nokia.com.                 85253  IN      A      208.78.70.55
ns.nokia.com.                 68992  IN      AAAA   2001:500:90:1::55
ns2.nokia.com.                68992  IN      A      204.13.250.55
ns3.nokia.com.                68992  IN      A      208.78.71.55
ns3.nokia.com.                68992  IN      AAAA   2001:500:94:1::55
ns4.nokia.com.                68992  IN      A      204.13.251.55
ns5.nokia.com.                68992  IN      A      208.78.70.55
ns5.nokia.com.                68992  IN      AAAA   2001:500:90:1::55
ns6.nokia.com.                13924  IN      A      204.13.250.55

;; Query time: 28 msec
;; SERVER: 149.156.96.8#53(149.156.96.8)
;; WHEN: Tue Dec 15 13:24:37 CET 2020
;; MSG SIZE rcvd: 341
```

# Reverse DNS

- **System serwerów pełniących funkcję odwrotną do DNS**
- **Mapowanie adresów IP na nazwy domenowe**
- **Realizowane w oparciu o domenę in-addr.arpa**
- **Wykorzystuje wpis (pointer) PTR w tablicy DNS**

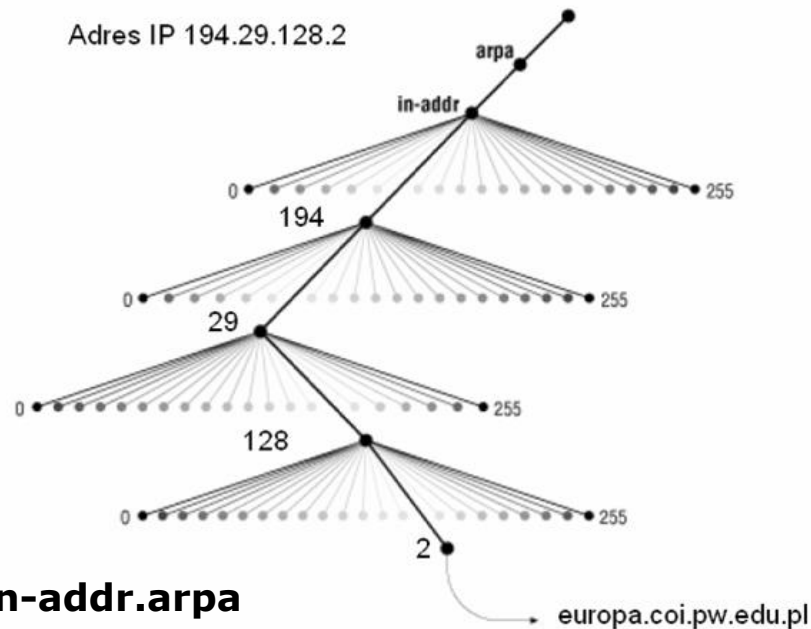


Example 1 – PTR record for the 192.168.1.0/27 block (addresses 192.168.1.1 – 192.168.1.30) and the reverse DNS for 192.168.1.10. This PTR record is created in the “27/1.168.192.in-addr.arpa” zone.

NAME	TTL	TYPE	DATA/SYSTEM
10.27/1.168.192.in-addr.arpa.	1800	PTR	mail.example.com.

# Domena .arpa

- Domena TLD przeznaczona do obsługi infrastruktury sieciowej Internetu
- W ramach domeny zdefiniowano:
  - in-addr.arpa – mapowanie Ipv4 na nazwy
  - ip6.arpa – mapowanie IPv6 na nazwy
  - e164.arpa – mapowanie numerów telefonicznych zgodnych z E.164 na URI
- Przestrzeń mapowania odwrotnego IPv4 i położenie domeny .arpa



**2.128.29.194.in-addr.arpa**

# Reverse dns w resolverze

- Przykład w oparciu o
  - Nslookup, dig
  - Adres ip: 149.156.111.10 (przypisany do serwera sendzimir)

```
C:\Windows\System32>nslookup
Serwer domylny: galaxy.agh.edu.pl
Address: 149.156.96.9

> set type=ptr
> 10.111.156.149.in-addr.arpa
Serwer: galaxy.agh.edu.pl
Address: 149.156.96.9

10.111.156.149.in-addr.arpa name = sendzimir.metal.agh.edu.pl
111.156.149.in-addr.arpa nameserver = sendzimir.metal.agh.edu.pl
111.156.149.in-addr.arpa nameserver = galaxy.uci.agh.edu.pl
111.156.149.in-addr.arpa nameserver = nms.cyf-kr.edu.pl
111.156.149.in-addr.arpa nameserver = deenes.uci.agh.edu.pl
nms.cyf-kr.edu.pl internet address = 149.156.1.3
deenes.uci.agh.edu.pl internet address = 149.156.119.130
galaxy.uci.agh.edu.pl internet address = 149.156.96.9
sendzimir.metal.agh.edu.pl internet address = 149.156.111.10
nms.cyf-kr.edu.pl AAAA IPv6 address = 2001:6d8:0:1::a:3
deenes.uci.agh.edu.pl AAAA IPv6 address = 2001:6d8:10:4036::7782
galaxy.uci.agh.edu.pl AAAA IPv6 address = 2001:6d8:10:1060::6009
>
```

```
opal@galaxy:~$ dig -x 149.156.111.10

; <<>> DiG 9.11.22 <<>> -x 149.156.111.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43642
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.111.156.149.in-addr.arpa. IN PTR

;; ANSWER SECTION:
10.111.156.149.in-addr.arpa. 4187 IN PTR sendzimir.metal.agh.edu.pl.

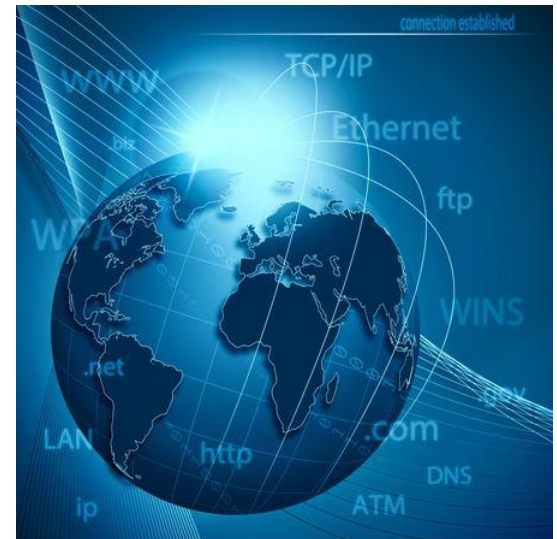
;; AUTHORITY SECTION:
111.156.149.in-addr.arpa. 22827 IN NS ns2.agh.edu.pl.
111.156.149.in-addr.arpa. 22827 IN NS ns1.agh.edu.pl.
111.156.149.in-addr.arpa. 22827 IN NS nms.cyf-kr.edu.pl.
111.156.149.in-addr.arpa. 22827 IN NS sendzimir.metal.agh.edu.pl.

;; ADDITIONAL SECTION:
nms.cyf-kr.edu.pl. 5284 IN A 149.156.1.3
nms.cyf-kr.edu.pl. 5284 IN AAAA 2001:6d8:0:1::a:3
ns1.agh.edu.pl. 65305 IN A 149.156.96.9
ns1.agh.edu.pl. 65305 IN AAAA 2001:6d8:10:1060::6009
ns2.agh.edu.pl. 68311 IN A 149.156.119.130
ns2.agh.edu.pl. 68311 IN AAAA 2001:6d8:10:4036::7782
sendzimir.metal.agh.edu.pl. 2469 IN A 149.156.111.10

;; Query time: 0 msec
;; SERVER: 149.156.96.8#53(149.156.96.8)
;; WHEN: Tue Dec 15 13:27:59 CET 2020
;; MSG SIZE rcvd: 319
```

# DNS jako protokół komunikacyjny

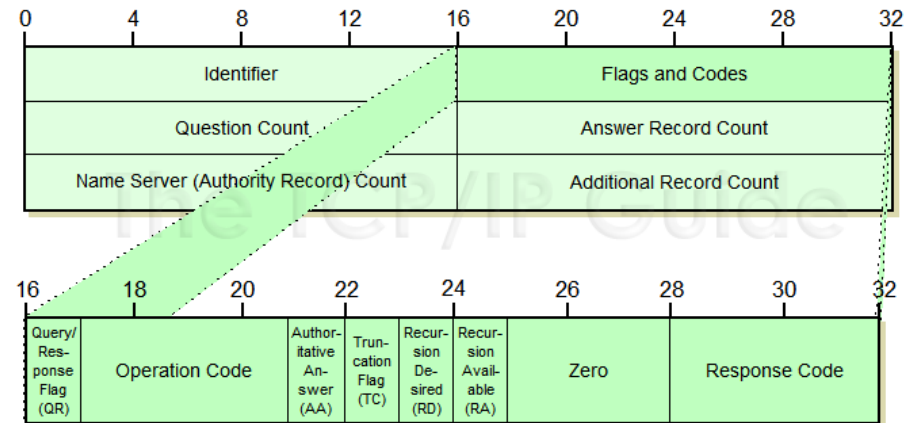
- sposób łączenia się klientów z serwerami DNS
- zestaw zaleceń dotyczących aktualizacji wpisów w bazach domen internetowych
- **Typy i protokoły komunikacji**
  - klient - server - protokół UDP, port 53
  - server master - server slave - protokół TCP, port 53
- **Dla UDP**
  - Wielkość pakietu - do 512 bajtów
- **Dla TCP**
  - Pakiety większe niż 512 bajtów - dodatkowe pole - długość zapytania/odpowiedzi
- **Okresowa aktualizacja wpisów DNS**
  - propagacja informacji do kilkudziesięciu godzin





# Struktura komunikatu DNS

- **Identyfikator**  
(powiązanie zapytania z odp.)
- **Nagłówek**
- **Zapytanie**
- **Odpowiedź**
- **Zwierzchność**  
(serwery zwierzchnie)
- **Dodatkowa**  
(sekcja informacji dodatkowych)
- **Nagłówek**
  - QR – określa czy komunikat jest zapytaniem czy odpowiedzią
  - OPCODE – rodzaj zapytania (standardowe, zwrotne, o stan serwera, zarezerwowane)
  - AA – odpowiedź autorytatywna
  - TC – odpowiedź nie zmieściła się w jednym pakiecie UDP
  - RD – klient żąda rekurencji
  - RA – serwer obsługuje rekurencje
  - Zero – zarezerwowane na przyszłość
  - RCODE – kod odpowiedzi (brak błędu, błąd formatu/serwera/nazwy, odrzucono, zarezerwowane)



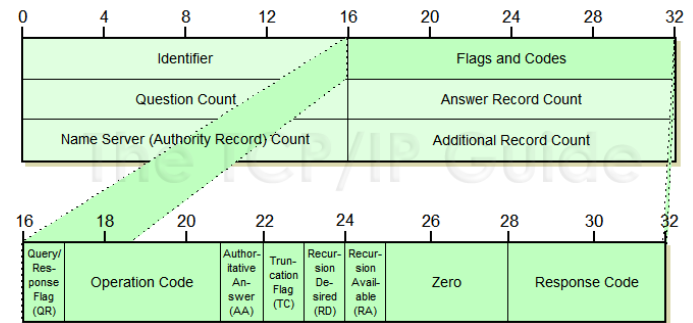
# Zapytanie DNS

No.	Time	Source	Destination	Protocol	Length	Info
5346	104.088004	192.168.1.102	192.168.1.1	DNS	69	Standard query 0x4723 A nokia.com
5348	104.116944	192.168.1.1	192.168.1.102	DNS	372	Standard query response 0x4723 A nokia.com A 162.13.46

> Frame 5346: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF\_{E80965AB-60E1-403A-B3EF-ACA50C9A738B}, id 0  
 > Ethernet II, Src: IntelCor\_07:aa:94 (dc:53:60:07:aa:94), Dst: Tp-LinkT\_01:1b:f8 (0c:80:63:01:1b:f8)  
 > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.1  
 > User Datagram Protocol, Src Port: 53014, Dst Port: 53

▼ Domain Name System (query)  
 Transaction ID: 0x4723  
 > Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 ▼ Queries  
 ▼ nokia.com: type A, class IN  
 Name: nokia.com  
 [Name Length: 9]  
 [Label Count: 2]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)

[Response In: 5348]



```

0000  0c 80 63 01 1b f8 dc 53 60 07 aa 94 08 00 45 00  ..c...S `.....E-
0010  00 37 3a 5f 00 00 80 11 7c 9f c0 a8 01 66 c0 a8  -7:_....|....f..
0020  01 01 cf 16 00 35 00 23 11 75 47 23 01 00 00 01  .....5.#.uG#....
0030  00 00 00 00 00 00 05 6e 6f 6b 69 61 03 63 6f 6d  .....nokia.com
0040  00 00 01 00 01  .....
```

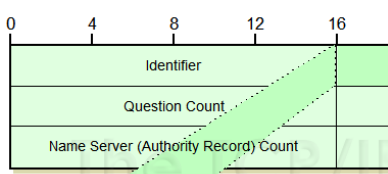
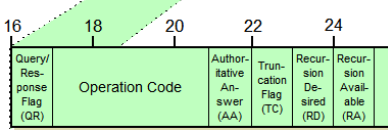
# Odpowiedź DNS

dns.resp.name == nokia.com

No.	Time	Source	Destination	Protocol	Length	Info
5348	104.116944	192.168.1.1	192.168.1.102	DNS	372	Standard query response 0x4723 A nokia.com

```

> Frame 5348: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface \Device\NPF_{E80965AB-60E1-403A-B3EF-ACA50C9A}
> Ethernet II, Src: Tp-LinkT_01:1b:f8 (0c:80:63:01:1b:f8), Dst: IntelCor_07:aa:94 (dc:53:60:07:aa:94)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.102
> User Datagram Protocol, Src Port: 53, Dst Port: 53014
v Domain Name System (response)
  Transaction ID: 0x4723
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 6
  Additional RRs: 9
v Queries
  > nokia.com: type A, class IN
v Answers
  v nokia.com: type A, class IN, addr 162.13.40.196
    Name: nokia.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 432000 (5 days)
    Data length: 4
    Address: 162.13.40.196
  v Authoritative nameservers
    > nokia.com: type NS, class IN, ns ns3.nokia.com
    > nokia.com: type NS, class IN, ns ns.nokia.com
    > nokia.com: type NS, class IN, ns ns6.nokia.com
    > nokia.com: type NS, class IN, ns ns2.nokia.com
    > nokia.com: type NS, class IN, ns ns4.nokia.com
    > nokia.com: type NS, class IN, ns ns5.nokia.com
  v Additional records
    > ns.nokia.com: type A, class IN, addr 208.78.70.55
    > ns.nokia.com: type AAAA, class IN, addr 2001:500:90:1::55
    > ns2.nokia.com: type A, class IN, addr 204.13.250.55
    > ns3.nokia.com: type A, class IN, addr 208.78.71.55
    > ns3.nokia.com: type AAAA, class IN, addr 2001:500:94:1::55
    > ns4.nokia.com: type A, class IN, addr 204.13.251.55
    > ns5.nokia.com: type A, class IN, addr 208.78.70.55
    > ns5.nokia.com: type AAAA, class IN, addr 2001:500:90:1::55
    > ns6.nokia.com: type A, class IN, addr 204.13.250.55
  [Request In: 5346]
  [Time: 0.028940000 seconds]
  
```

0	4	8	12	16	20	24	28	32
Identifier				Flags and Codes				
Question Count				Answer Record Count				
Name Server (Authority Record) Count				Additional Record Count				

16	18	20	22	24	26	28	30	32
Query/Response Flag (QR)	Operation Code		Authoritative Answer (AA)	Truncation Flag (TC)	Recursion Desired (RD)	Recursion Available (RA)	Zero	Response Code

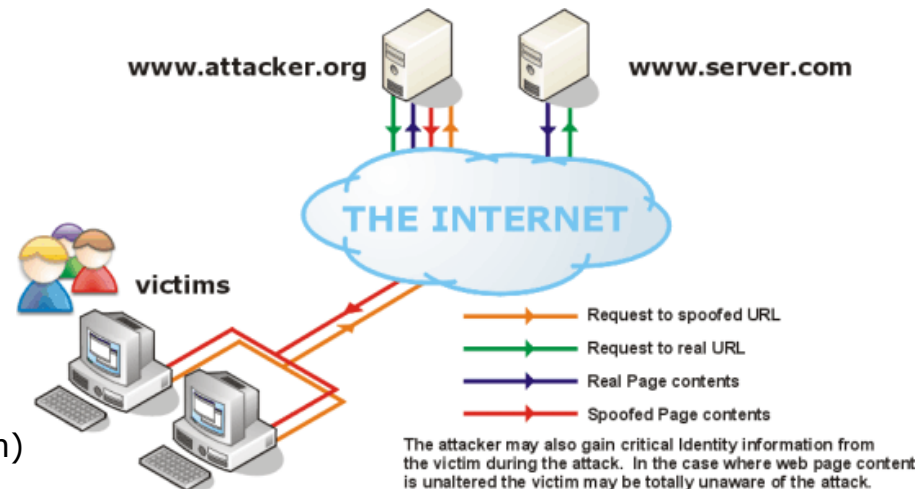
```

0020 01 66 00 35 cf 16 01 52 ff 28 47 23 81 80 00 01 .f.5...R.(G#....
0030 00 01 00 06 00 09 05 6e 6f 6b 69 61 03 63 6f 6d .....nokia.com
  
```

Domain Name System (dns), 330 byte(s)

# Bezpieczeństwo w DNS

- **Wykorzystanie protokołu UDP (bezpołączeniowy)**
- **Ataki DDoS (Distributed Denial of Service)**
  - Spreparowanie zapytań z fałszywym adresem źródłowym (ofiary)
  - Rozesłanie zapytań do wielu serwerów DNS
  - Rozmiar odpowiedzi - 10 x zapytanie
- **Ataki Man in the middle**
  - Fałszywe odpowiedzi DNS dla komputera ofiary
  - Połączenie komputera ofiary ze sfałszowanym serwerem docelowym
  - (banki, wyłudzenia haseł)
- **Rozwiązanie – system DNSSEC**
  - Rozszerzenie systemu DNS
  - uwierzytelnianie źródeł danych
  - Oparte o mechanizmy podpisów cyfrowych (kryptografia asymetryczna)
  - Brak powszechnego wsparcia przez
    - Społeczność
    - Aplikacje
    - Urządzenia
  - Praktycznie nieużywany  
(w Polsce zabezpieczone 0,46 na 2,4 mln domen)



Paul Albirz, Cricket Liu: *DNS i BIND*. Warszawa: Wydawnictwo RM, 1999, s. 9.

J.Durak, „DNS” Pracownia Informatyki, 2009

Nirlog.com „DNS Amplification Attack” <http://nirlog.com/2006/03/28/dns-amplification-attack/>

Webio.pl „Zarządzanie strefą DNS”

Highteck.net „Application Layer ISO OSI Functionality and Protocol”

Charles M. Kozierok, „The TCP/IP Guide”, 2005

W.Graniszewski, E.Grochocki, G.Świątek – DNS – Sieci Komputerowe, <http://ważniak.mimów.edu.pl/>

WikiBooks, Communication Networks/DNS

„.PL DOMAIN NAME MARKET” NASK’s Report for the fourth quarter of 2016

Linode „DNS Records: An Introduction”

„Rynek nazw domeny .pl, Szczegółowy raport NASK za pierwszy kwartał 2020 roku” NASK