Sieci Komputerowe

System DNS

mgr inż. Jerzy Sobczyk

Plan wykładu

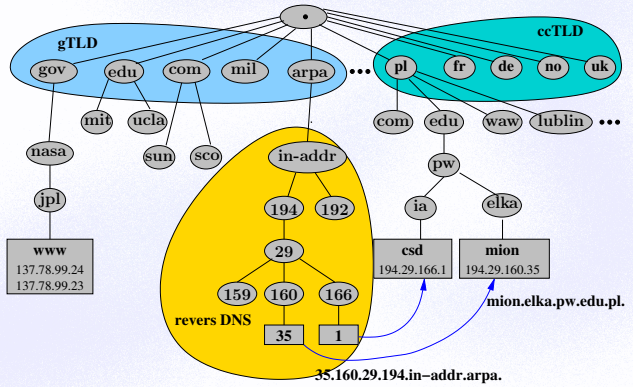
- Usługa DNS.
- Serwery DNS.
- DNS podzielony.
- DNS bezpieczny.
- Konfigurowanie serwera DNS.

Historia

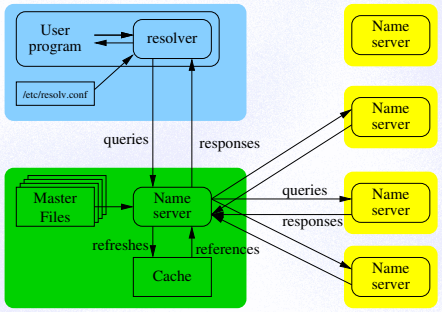
1969	Jonathan Postel edytorem RFC
1983.11	DNS - RFC 882, 883
1984	serwer Bind - Douglas Terry, Mark Painter, David Riggle and Songnian Zhou
1986.06	oficjalna wersja serwera Bind
1988.12	pierwsza wzmianka o IIANA - RFC 1083
1997.01	DNSsec - RFC 2065
1997.04	DDNS - RFC 2136
1997.05	Bind 8 - ISC - Bob Halley, Paul Vixie
1998	Bind - Paul Vixie
1998.09.18	utworzenie ICANN
1998.10.16	śmierć Jonathana Postela
1999.03	poprawki DNSsec - RFC 2535
2000.02	DNS-SD rekord SRV - RFC 2782
2000.09	Bind 9 - ISC
2005.03	poprawki DNSsec - RFC 4033, 4034, 4035
2009	Bind 10 - ISC
2010.04	rezygnacja ISC z Bind 10
2010.07.15	podpisanie domeny głównej (root)
2010.06.30	podpisanie domeny edu.
2011.04.01	podpisanie domeny com.
2012.02.10	podpisanie domeny pl.
2013	wymaganie podpisania domeny dla wszystkich TLD
2013	multicast DNS RFC 6762
2016.09	ostateczne przejęcie funkcji IIANA przez ICANN
2018.02.05	podpisane jest 1385/1514=91% TLD i 4% 2LD; 12% użytkowników weryfikuje podpisy
2023.04.21	podpisane jest 1366/1479=92% TLD i 7% 2LD; 32% użytkowników weryfikuje podpisy

statystyki na podstawie http://rick.eng.br/dnssecstat/

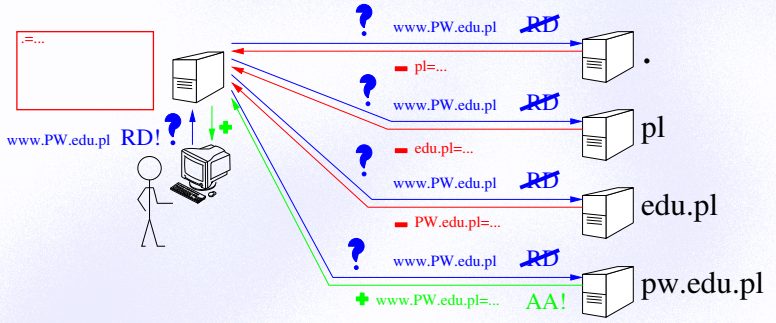
Struktura domen DNS



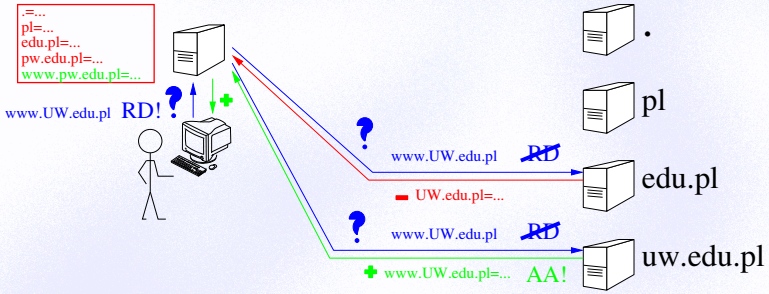
Rekursywny serwer DNS



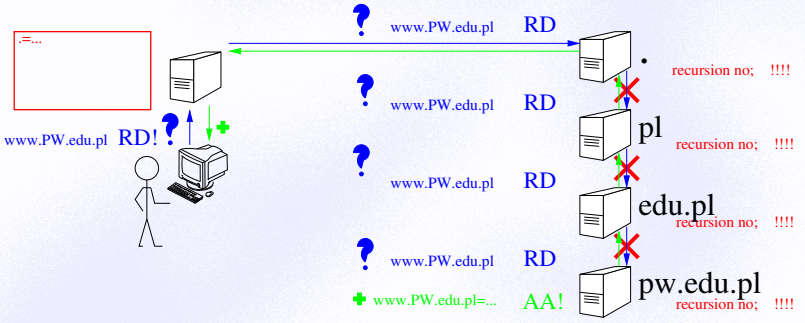
DNS - sekwencja zapytań



DNS - sekwencja zapytań - cache



DNS - sekwencja zapytań - rekursja?



Budowa rekordu

nazwa	*czas życia*	*klasa*	*typ*	*wartość*
mion	86400	IN	A	194.29.160.35

Pole	Opis
nazwa	Nazwa rekordu. Jedną nazwę może mieć klika rekordów nawet jeśli sa tego samego typu.
czas życia (TTL)	Wyrażony w sekundach maksymalny czas przechowywania w serwerach buforujacych.
klasa	Klasa rekordu (IN - Internet, CH - Chaos, HS - Hesiod, ??).
typ	Typ rekordu.
wartość	Wartość rekordu zależna od jego typu.

Typy rekordów

Typ	Przeznaczenie	Przykład		
SOA	początek opisu domeny	elka.pw.edu.pl.	IN SOA	proton.elka.pw.edu.pl. ...
NS	serwer obsługujący domenę	elka.pw.edu.pl.	IN NS	dns1.elka.pw.edu.pl.
A	adres IP v.4	mion.elka.pw.edu.pl.	IN A	194.29.160.35
AAAA	adres IP v.6	C.root-servers.net.	IN AAAA	2001:500:2::c
PTR	odsyłacz do innego rekordu	35.160.29.194.in-addr.arpa.	IN PTR	mion.elka.pw.edu.pl.
CNAME	nazwa alternatywna	www.elka.pw.edu.pl.	IN CNAME	moon.elka.pw.edu.pl.
MX	serwer pocztowy	elka.pw.edu.pl.	IN MX	10 elektron.elka.pw.edu.pl.
TXT	dowolny tekst	elka.pw.edu.pl.	IN TXT	v=spf1 ip4:194.29.160.103 -all
SRV	serwer usługi	_imap._tcp.elka.pw.edu.pl.	IN SRV	0 0 993 elektron.elka.pw.edu.pl.
DNSKEY	klucz serwera	pl.	IN DNSKEY	257 3 8 AwEAAd85/h2y+oC .....
RRSIG	podpis rekordu	pl.	IN RRSIG	DS 8 1 86400 202312110500 .....
HINFO	informacje o komputerze	pc.abc.com.	IN HINFO	"Cray-3" "CrayOS"
WKS	oferowane usługi	csd.ia.pw.edu.pl.	IN WKS	TCP (22 25 80 143 443 568 993)
...	... ...			

SOA – parametry buforowania informacji o domenie

```
@ IN SOA   csd.ia.pw.edu.pl.   root.ia.pw.edu.pl.  (
                2001090500     ;Serial
                10800          ;Refresh
                3600           ;Retry
                432000         ;Expire
                86400 )        ;Minimum
```

Nazwa	Przykład	Opis
Master	csd.ia.pw.edu.pl	Nazwa serwera głównego (master).
Admin	root.ia.pw.edu.pl	Adres e-mail administratora domeny (znak @ zastąpiony kropką - np.: root@ia.pw.edu.pl).
Serial	2001090500	Numer sekwencyjny - zawsze musi rosnąć!
Refresh	10800	Co ile sekund należy sprawdzać aktualność danych.
Retry	3600	Co ile sekund należy ponawiać nieudaną próbę.
Expire	432000	Po ilu sekundach dane należy uznać za nieaktualne.
Minimum	86400	Minimalny czas przechowywania.

SOA – numer sekwencyjny

Przy każdej zmianie zawartości domeny numer sekwencyjny MUSI rosnąć!

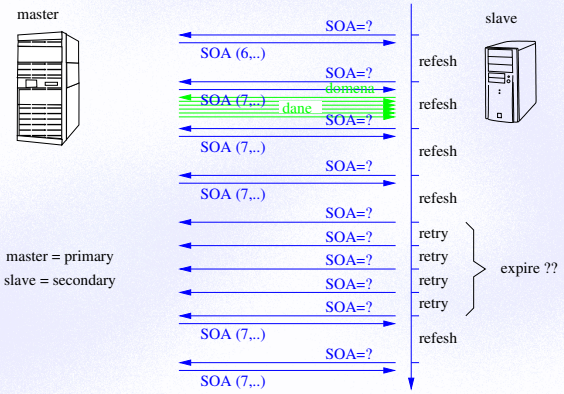
Zalecany format: YYYYMMDDnn	
Zapis	Uwagi
2011081101	11 sierpnia 2011 wersja 1
4294123199	bez problemów do roku 4294

Dawniej dopuszczalny był zapis: n.m

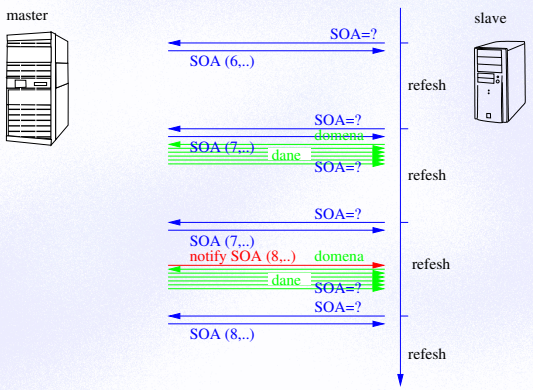
$$n.m = n \times 10^{3+int(0.9+log_{10}m)} + m$$

Zapis	Wartość	Uwagi
13.1	13001	
13.2	130002	
13.11	130011	
13.13	1300013	
13.15	1300015	
14.1	14001	numer zmalał!!!
14.12	140012	
14.13	1400013	dopiero teraz większy

DNS - aktualizacja danych



DNS - notyfikacja



DNS dla IP v.4 i v.6

IP v4 DNS record

yxz IN A 1.2.3.4

revers DNS for IP v4

4.3.2.1.IN-ADDR.ARPA.

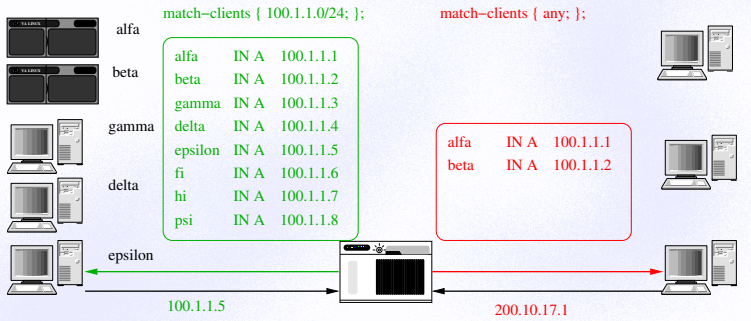
IP v6 DNS record

xyz IN AAAA 1080:0000:0000:0000:0008:0800:200C:417A
xyz IN AAAA 1080::8:800:200C:417A

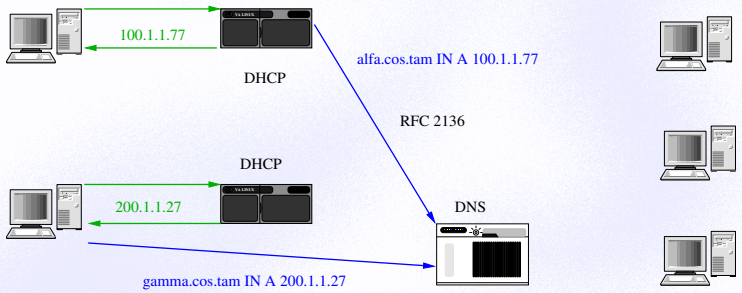
revers DNS for IP v6

A.7.1.4.C.0.0.2.0.0.8.0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.1.IP6.ARPA.

DNS - widoki



DNS - dynamiczny - DDNS



DNS-SD - wykrywanie usług - RFC 2782

```
_service._protocol.domain.name ttl class SRV priority weight port target
_service._protocol.domain.name ttl class TXT parameters
```

_service	nazwa usługi
_protocol	nazwa protokołu np: _tcp, _udp
domain.name	nazwa domeny
ttl	czas przechowania rekordu w serwerach buforujących DNS
class	klasa rekordy DNS zazwyczaj IN
priority	pierwszeństwo - preferowane są niższe wartości
weight	waga - wyższa wartość oznacza większe prawdopodbieństwo wyboru, 0 oznacza brak usługi
port	numer portu
target	nazwa serwera (ale nie CNAME)
parameters	dodatkowe parametry specyficzne dla danej usługi

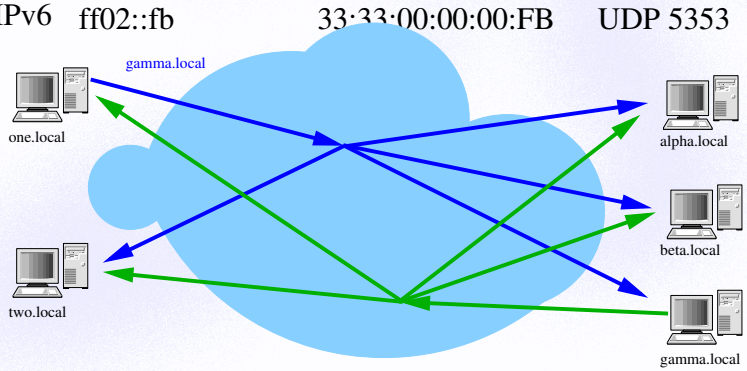
Przykład:

```
_ldap._tcp.cos.tam IN SRV 0 1 389 ldap1.cos.tam
_ldap._tcp.cos.tam IN SRV 0 3 389 ldap2.cos.tam
_ldap._tcp.cos.tam IN SRV 1 1 389 ldap3.cos.tam
_ldap._tcp.cos.tam IN SRV 1 3 389 ldap4.cos.tam
```

Multicast DNS

RFC 6762

IPv4 224.0.0.251 01:00:5E:00:00:FB UDP 5353
IPv6 ff02::fb 33:33:00:00:00:FB UDP 5353

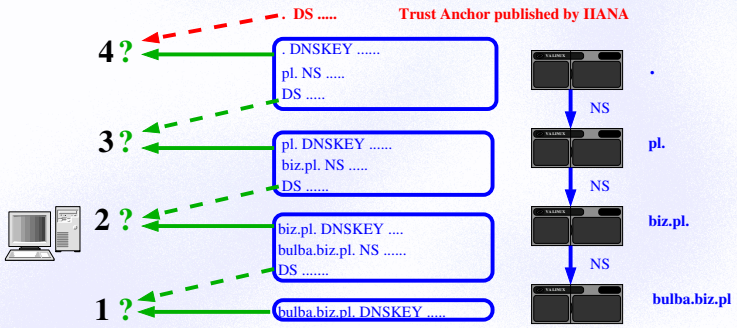


DNSsec - podpisane rekordy - RFC 4035

```
example.    3600 IN SOA ns1.example. bugs.x.w.example. (
                        1081539377
                        3600
                        300
                        3600000
                        3600
                        )
            3600 RRSIG  SOA 5 1 3600 20040509183619 (
                        20040409183619 38519 example.
                        ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                        7TSJaHCqbhE67Sr6aH2xDUGcqQWu/nOUVzrF
                        vkgO9ebarZOGWDKcuwlM6eNB5SiX2K7415LW
                        DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rjkB
                        jV7j86HyQgM5e7+miRAz8V01b0I= )


            3600 NS     ns1.example.
            3600 NS     ns2.example.
            3600 RRSIG  NS 5 1 3600 20040509183619 (
                        20040409183619 38519 example.
                        gl13FO0f2UOR+SWiXXLHwsMY+qStYy5k6zfd
                        EuivWc+wd1fmbNCyqlOTk71HTX6UOxc8AgNf
                        4ISFve8XqF4q+o9qlnqIzmppU3LiNeKT4FZ8
                        RO5urFOvoMRTbQxW3UOhXWuggE4g3ZpsHv48
                        OHjMeRaZB/FRPGfJPajngcq6Kwg= )
```

DNS - łańcuch zaufania



DNS – konfiguracja resolvera

```
;-----------------------------------------
;
;  csd.ia.pw.edu.pl.        /etc/resolv.conf
;
search ia.pw.edu.pl elka.pw.edu.pl
nameserver      148.81.31.1
nameserver      148.81.63.254
nameserver      127.0.0.1
;-----------------------------------------
```

DNS – plik konfiguracyjny (stary typ)

```
;-------------------------------------------------
;
; csd.ia.pw.edu.pl.     /etc/named.boot
;
; type      domain                  source file or host
directory   /var/named
cache       .                       root.dns
primary     ia.pw.edu.pl            ia.dns
primary     31.81.148.in-addr.arpa  ia.rdns
secondary   elka.pw.edu.pl          148.81.63.254 ELKA.DNS
secondary   63.81.148.in-addr.arpa  148.81.63.254 ELKA.RDNS
primary     0.0.127.in-addr.arpa    local.dns
```

DNS – główny plik konfiguracyjny

```
#-------------------------------------------
# csd.ia.pw.edu.pl.     /etc/named.conf
options {
          directory  "/var/named";
          pid-file   "/var/named/named.pid";
          auth-nxdomain yes;
#          forwarders       { 148.81.63.22; 148.81.128.1; };
};
logging {
        category lame-servers  { null; };
        category cname  { null; };
};
```

DNS – główny plik konfiguracyjny cd.

```
zone "." in {
        type hint;
        file "root.dns";
};
zone "ia.pw.edu.pl" in {
        type master;
        file "ia.dns";
};
zone "31.81.148.in-addr.arpa" in {
        type master;
        file "ia.rdns";
};
```

DNS – główny plik konfiguracyjny cd.

```
zone "elka.pw.edu.pl" in {
        type slave;
        file "ELKA.DNS";
        masters { 148.81.63.254; };
};
zone "63.81.148.in-addr.arpa" in {
       type slave;
       file "ELKA.RDNS";
       masters { 148.81.63.254; };
};
```

DNS – pamięć notatnikowa

```
;------------------------------------------------------------
;
; csd.ia.pw.edu.pl.     /var/named/root.dns
;
ia.pw.edu.pl.   99999999  IN NS   csd.ia.pw.edu.pl.
ia.pw.edu.pl.   99999999  IN NS   proton.elka.pw.edu.pl.
pw.edu.pl.      99999999  IN NS   csd.ia.pw.edu.pl.
edu.pl.         99999999  IN NS   cocos.fuw.edu.pl.
; ftp://FTP.RS.INTERNIC.NET/domain/named.root
.                3600000  IN NS   A.ROOT-SERVERS.NET.
                 3600000  IN NS   B.ROOT-SERVERS.NET.
                 3600000  IN NS   C.ROOT-SERVERS.NET.
                 3600000  IN NS   D.ROOT-SERVERS.NET.
                 3600000  IN NS   E.ROOT-SERVERS.NET.
```

DNS – pamięć notatnikowa cd.

```
;
;  Prep the cache (hotwire the addresses).
;
cocos.fuw.edu.pl.       99999999  IN A  148.81.4.6
proton.elka.pw.edu.pl.  99999999  IN A  148.81.63.254
; ftp://FTP.RS.INTERNIC.NET/domain/named.root
A.ROOT-SERVERS.NET.      3600000  IN A  198.41.0.4
B.ROOT-SERVERS.NET.      3600000  IN A  128.9.0.107
C.ROOT-SERVERS.NET.      3600000  IN A  192.33.4.12
D.ROOT-SERVERS.NET.      3600000  IN A  128.8.10.90
E.ROOT-SERVERS.NET.      3600000  IN A  192.203.230.10
;------------------------------------------------------------
```

DNS – konfiguracja domeny lokalnej

```
;------------------------------------------------
; csd.ia.pw.edu.pl.     /var/named/local.dns
;
$TTL    86400
@ IN SOA   csd.ia.pw.edu.pl.    root.csd.ia.pw.edu.pl.  (
                2001041500      ;Serial
                10800           ;Refresh
                3600            ;Retry
                432000          ;Expire
                86400 )         ;Minimum

                IN      NS      csd.ia.pw.edu.pl.
1               IN      PTR     csd.ia.pw.edu.pl.
```

DNS – konfiguracja domeny IA

```
;------------------------------------------------
; csd.ia.pw.edu.pl.     /var/named/ia.dns
;
$TTL    86400
@ IN SOA   csd.ia.pw.edu.pl.    root.csd.ia.pw.edu.pl.  (
                2001090500      ;Serial
                10800           ;Refresh
                3600            ;Retry
                432000          ;Expire
                86400 )         ;Minimum

                IN      NS      csd.ia.pw.edu.pl.
                IN      NS      proton.elka.pw.edu.pl.
                IN      MX      10      csd.ia.pw.edu.pl.
```

DNS – konfiguracja domeny IA

```
csd             IN      A       148.81.31.1
loghost         IN      CNAME   csd.ia.pw.edu.pl.
;
ftp             IN      CNAME   csd.ia.pw.edu.pl.
www             IN      CNAME   csd.ia.pw.edu.pl.
mailsrv         IN      CNAME   csd.ia.pw.edu.pl.
csd1            IN      A       148.81.31.2
                IN      MX      10      csd.ia.pw.edu.pl.
netlab          IN      NS      net-s.netlab.ia.pw.edu.pl,
net-s.netlab.ia.pw.edu.pl,      IN      A       148.81.31.22
```

DNS – konfiguracja domeny odwrotnej

```
;------------------------------------------------
; csd.ia.pw.edu.pl.     /var/named/ia.rdns
;
@ IN SOA   csd.ia.pw.edu.pl.    root.csd.ia.pw.edu.pl. (
                2001090500      ;Serial
                10800           ;Refresh
                3600            ;Retry
                432000          ;Expire
                86400 )         ;Minimum

        IN      NS      csd.ia.pw.edu.pl.
1       IN      PTR     csd.ia.pw.edu.pl.
2       IN      PTR     csd1.ia.pw.edu.pl.
```

DNS – Sprawdzenia poprawności

```
# Sprawdzenie pliku konfiguracyjnego
named-checkconf /etc/named.conf

# Sprawdzenia plików strefowych
named-checkzone -i local ia.pw.edu.pl /var/named/ia.dns
named-checkzone elka.pw.edu.pl /var/named/elka.dns
named-checkzone 31.81.148.in-addr.arpa /var/named/ia.rdns
named-checkzone 63.81.148.in-addr.arpa /var/named/elka.rdns
```

Dziękuję za uwagę

mgr inż. Jerzy Sobczyk