NASK

DNS

Podstawy działania

Krzysztof Olesik • Naukowa i Akademicka Sieć Komputerowa • Dział Domen • Warszawa 17.05.2012

NASK

Agenda

- Co to jest DNS?
- Jak działa DNS?
- Przestrzeń nazw domen
- Rozwiązywanie nazw
- Rodzaje zapytań DNS
- Typy konfiguracji serwerów nazw
- Podstawowe rekordy DNS
- Serwery root
- Anycast w DNS
- Domeny IDN
- Rejestracja domeny

NASK

Co to jest DNS?

NASK

DNS – Domain Name System

- W wolnym tłumaczeniu **system nazw domenowych.**
- DNS zajmuje się odwzorowywaniem (tłumaczeniem) nazw komputerów (hostów) na ich adresy internetowe.
- Z DNS'u korzystamy za każdym razem, kiedy wysyłamy e-mail lub surfujemy po sieci.
- DNS jest podstawą Internetu – z jego usług korzysta wiele protokołów i usług sieciowych.
- DNS jest rozproszoną bazą danych – informacje o komputerach w sieci znajdują się na wielu serwerach DNS rozproszonych po całym świecie.
- DNS cechuje wysoka niezawodność – osiągnięta dzięki nadmiarowości serwerów DNS (minimalnie dwa).
- Doskonała skalowalność.

NASK

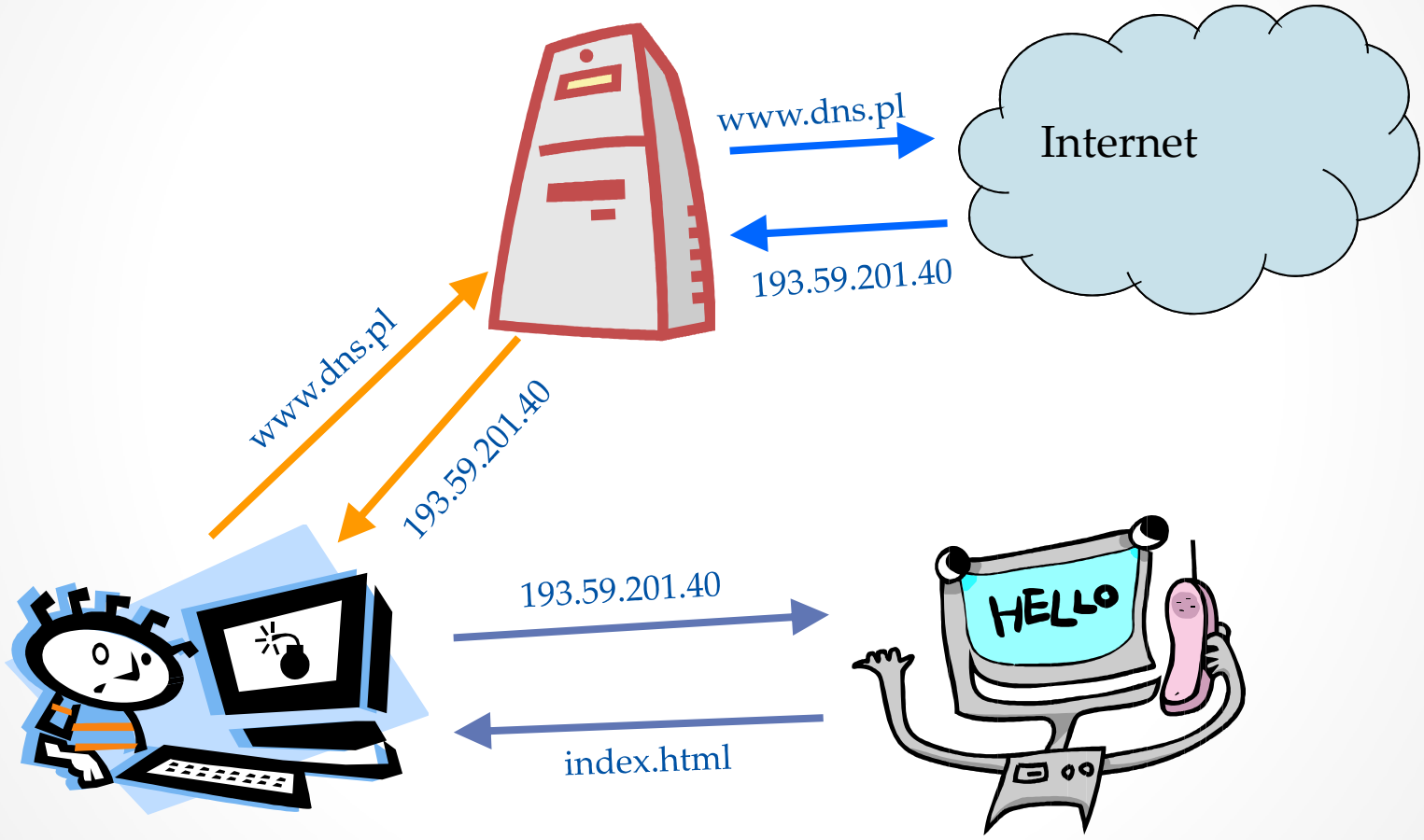
Jak działa DNS?

NASK

Jak działa DNS?

NASK

Jak działa DNS?



NASK

Przestrzeń nazw domen

NASK

Przestrzeń nazw domen

Struktura plików w systemach operacyjnych Windows

Baza danych DNS

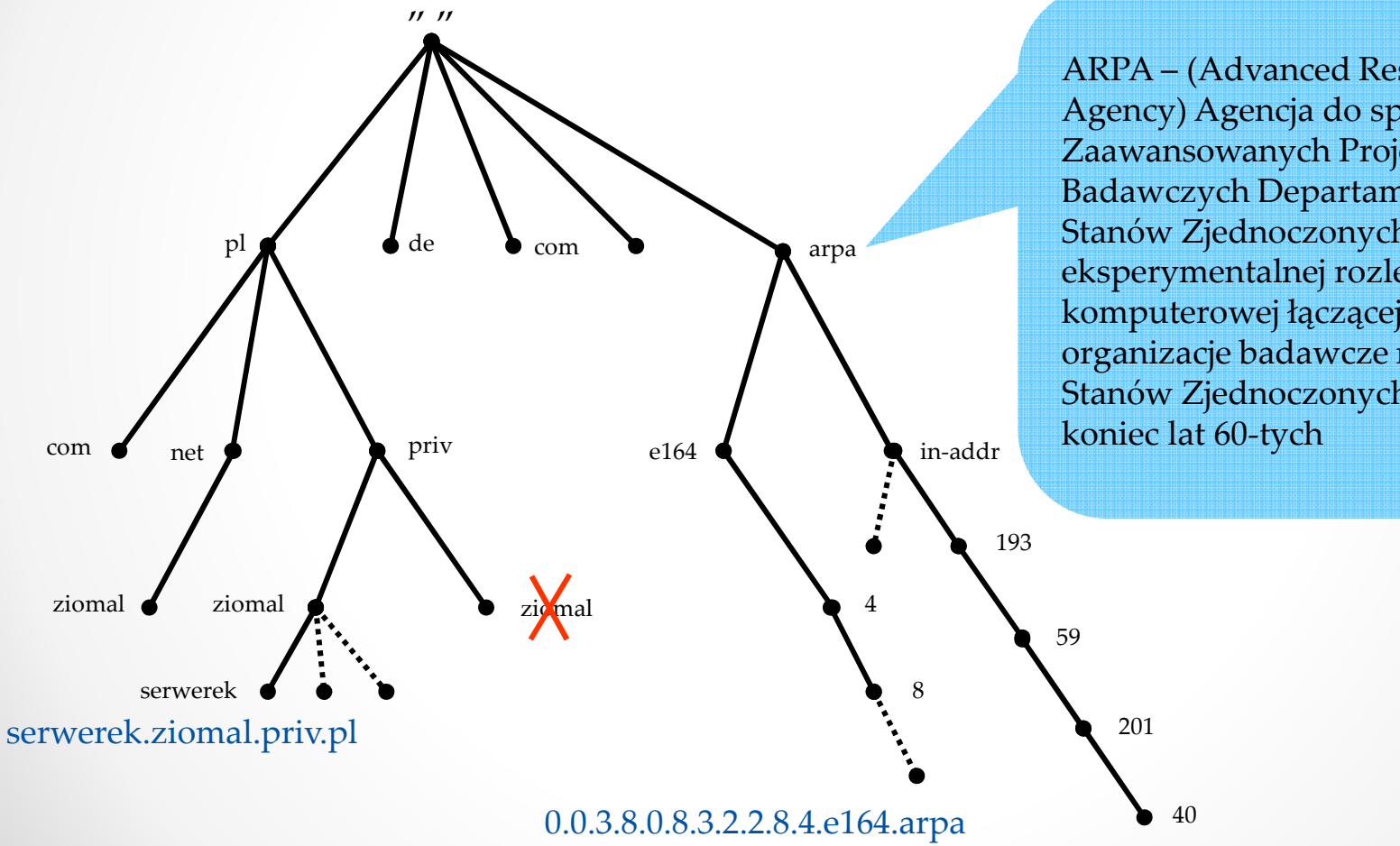
Domena jest poddrzewem przestrzeni nazw domen

C:\Moje dokumenty\Zdjęcia\Ziomal04.jpg serwerek.ziomal.priv.pl

NASK

Przestrzeń nazw domen

Domen prosta, odwrotna, e164



ARPA – (Advanced Research Project Agency) Agencja do spraw Zaawansowanych Projektów Badawczych Departamentu Obrony Stanów Zjednoczonych; twórcy eksperymentalnej rozległej sieci komputerowej łączącej ważne organizacje badawcze na terenie Stanów Zjednoczonych (ARPAnet); koniec lat 60-tych

serwerek.ziomal.priv.pl

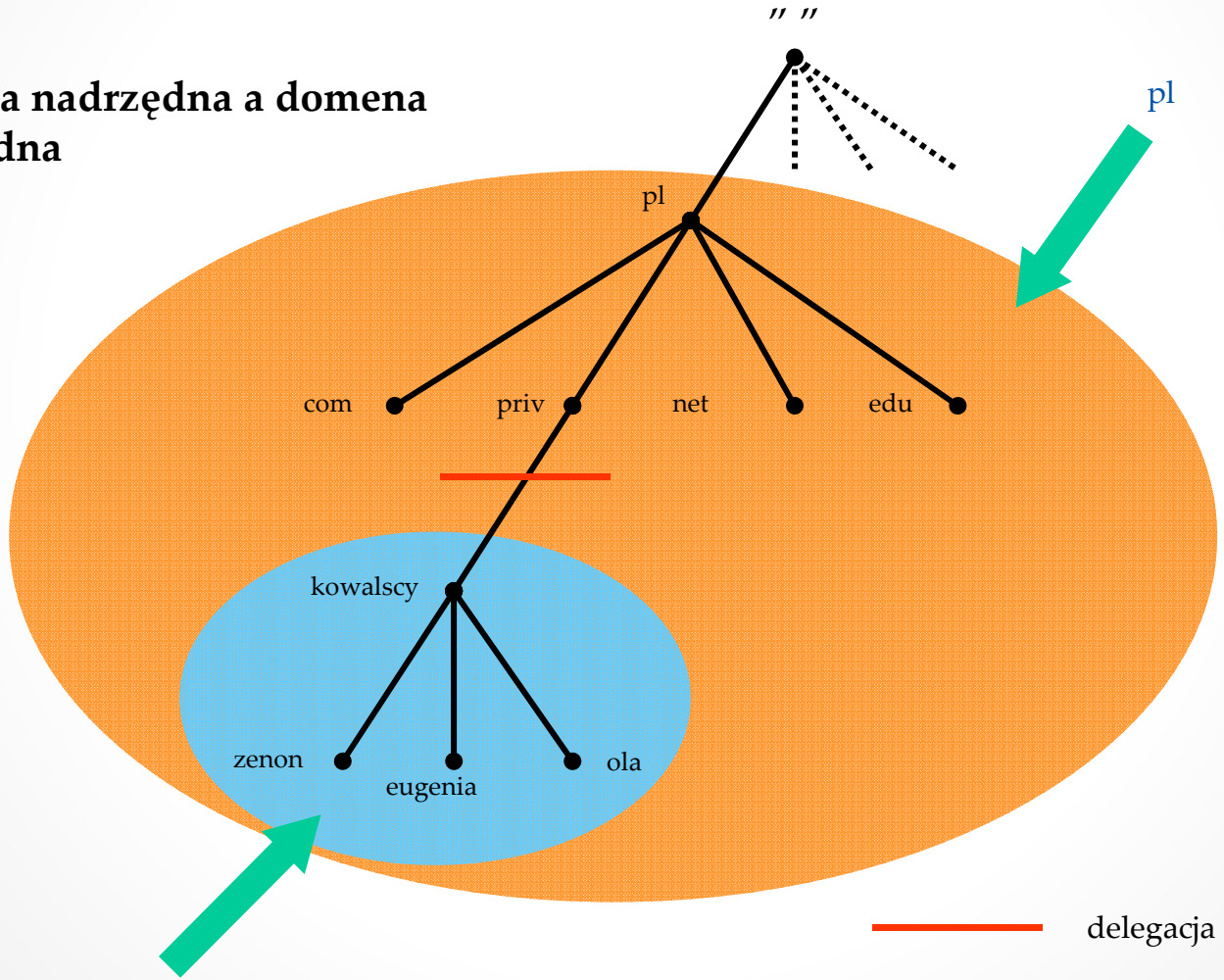
0.0.3.8.0.8.3.2.2.8.4.e164.arpa

40.201.59.193.in-addr.arpa

NASK

Przestrzeń nazw domen

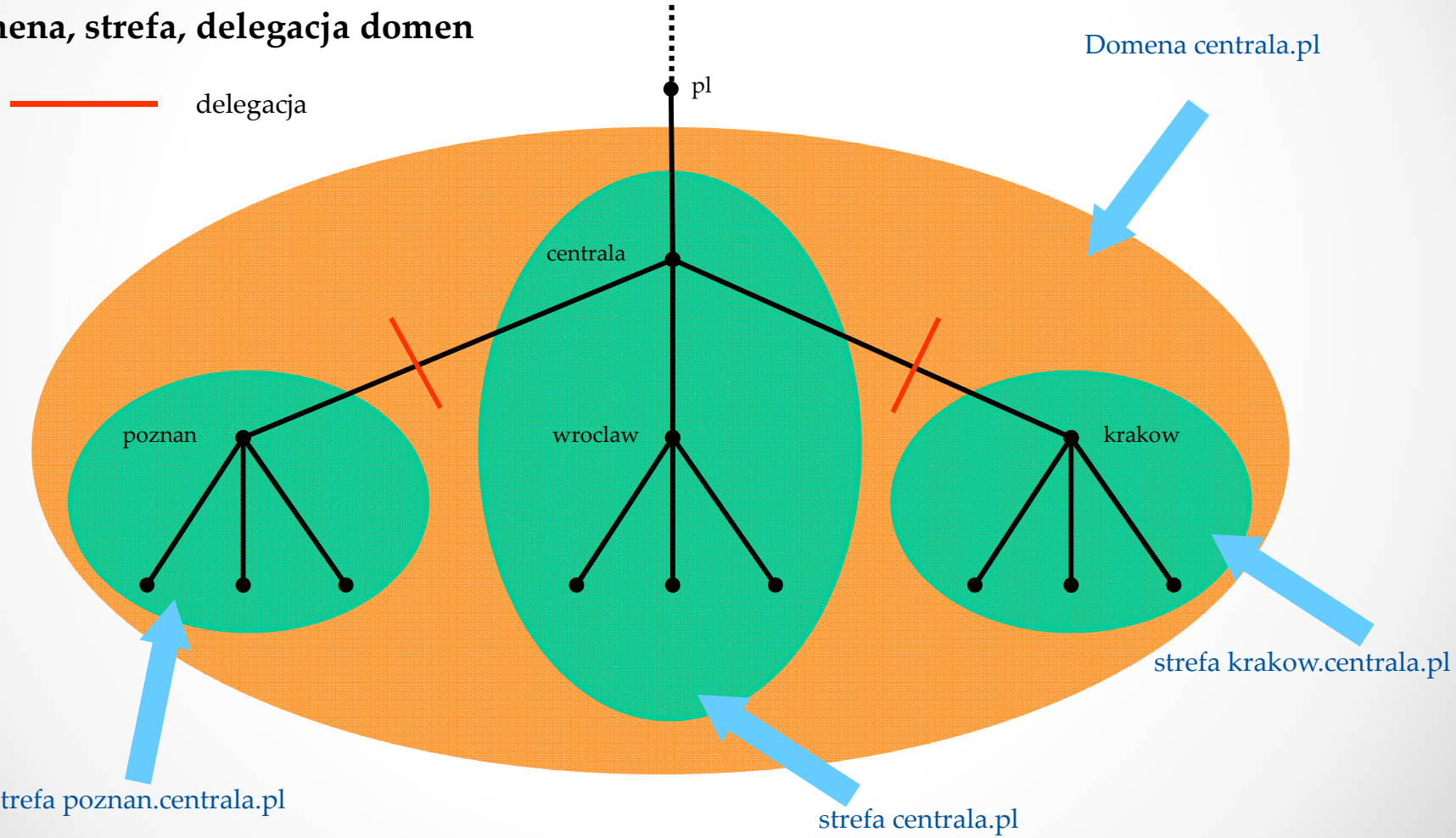
Domena nadrzędna a domena podrzędna



NASK

Przestrzeń nazw domen

Domena, strefa, delegacja domen

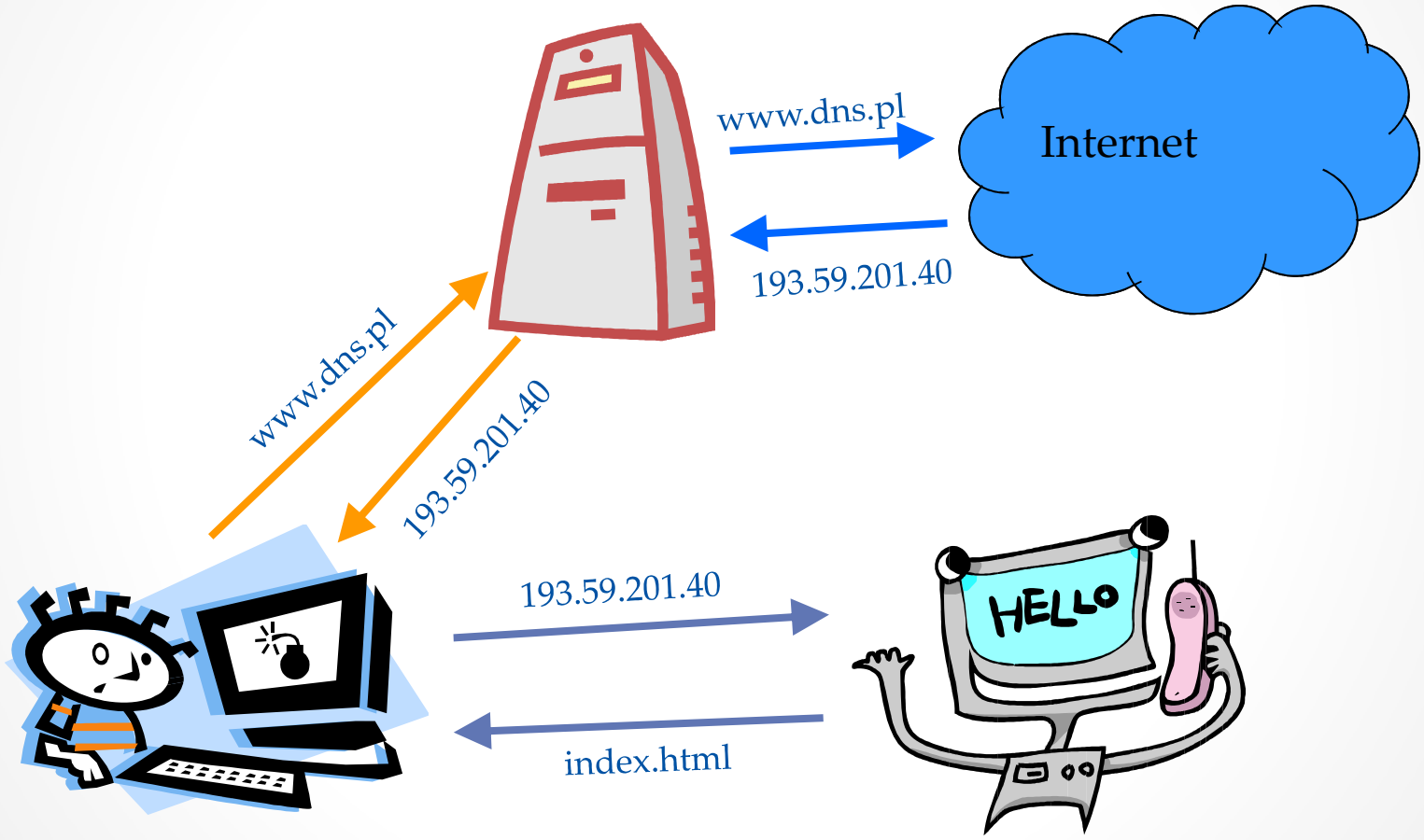


NASK

Rozwiązywanie nazw domenowych

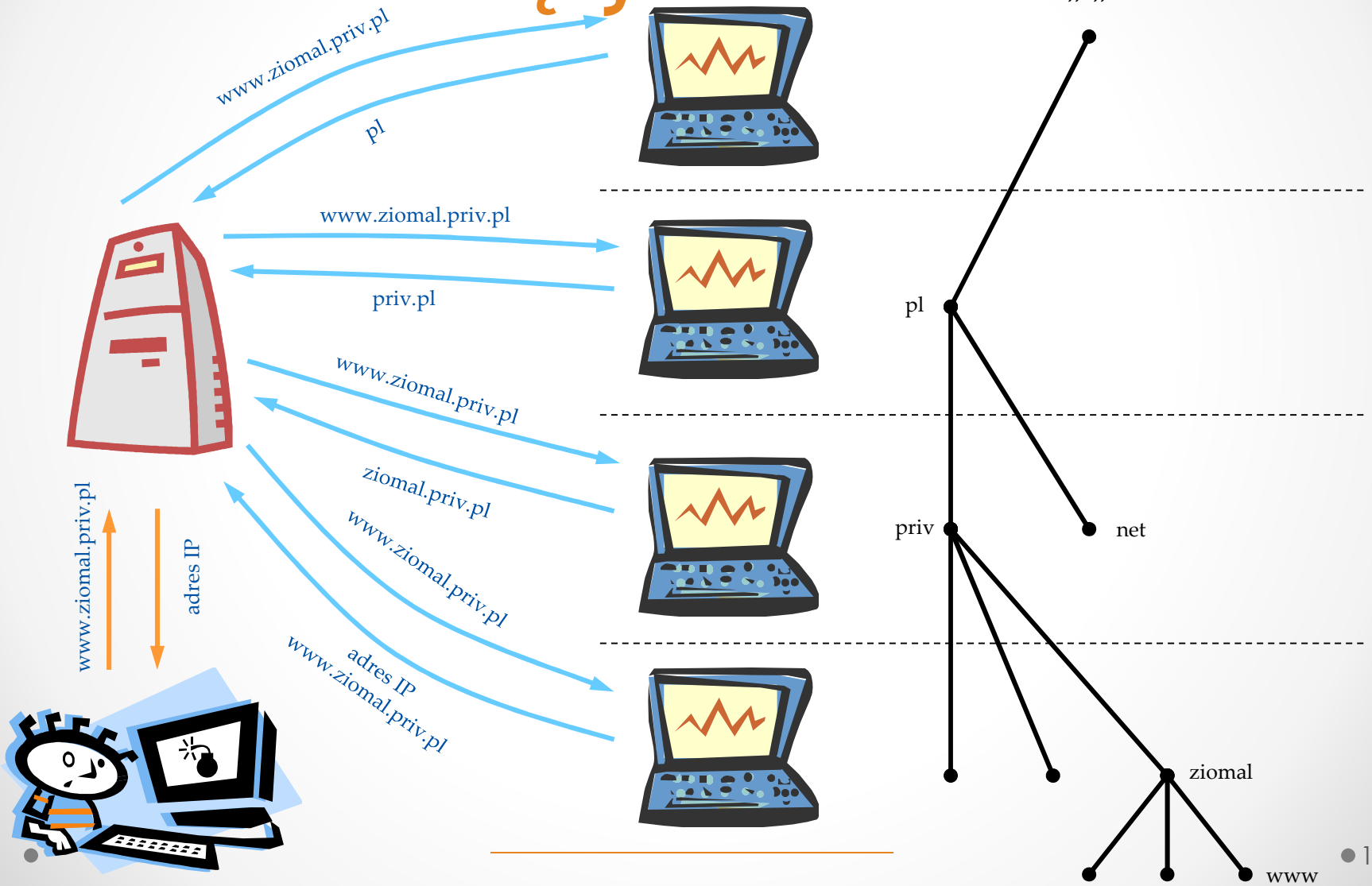
NASK

Rozwiązywanie nazw



NASK

Rozwiązywanie nazw



```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5 <<>> www.dns.pl +trace
;; global options:  printcmd
.                       27477   IN      NS      k.root-servers.net.
.                       27477   IN      NS      f.root-servers.net.
.                       27477   IN      NS      d.root-servers.net.
.                       27477   IN      NS      c.root-servers.net.
.                       27477   IN      NS      h.root-servers.net.
.                       27477   IN      NS      m.root-servers.net.
.                       27477   IN      NS      l.root-servers.net.
.                       27477   IN      NS      j.root-servers.net.
.                       27477   IN      NS      b.root-servers.net.
.                       27477   IN      NS      i.root-servers.net.
.                       27477   IN      NS      a.root-servers.net.
.                       27477   IN      NS      e.root-servers.net.
.                       27477   IN      NS      g.root-servers.net.
;; Received 512 bytes from 195.187.245.51#53(195.187.245.51) in 4 ms

pl.                     172800  IN      NS      a-dns.pl.
pl.                     172800  IN      NS      c-dns.pl.
pl.                     172800  IN      NS      d-dns.pl.
pl.                     172800  IN      NS      e-dns.pl.
pl.                     172800  IN      NS      f-dns.pl.
pl.                     172800  IN      NS      g-dns.pl.
pl.                     172800  IN      NS      h-dns.pl.
pl.                     172800  IN      NS      i-dns.pl.
;; Received 400 bytes from 193.0.14.129#53(k.root-servers.net) in 11 ms

dns.pl.                 86400   IN      NS      bilbo.nask.org.pl.
dns.pl.                 86400   IN      NS      eomer.nask.net.pl.
dns.pl.                 86400   IN      NS      ns.tpnet.pl.
dns.pl.                 86400   IN      NS      kirdan.nask.net.pl.
dns.pl.                 86400   IN      NS      frodo.nask.net.pl.
dns.pl.                 86400   IN      NS      ns1.tpnet.pl.
;; Received 184 bytes from 195.187.245.44#53(a-dns.pl) in 2 ms

www.dns.pl.             28800   IN      A       193.59.201.40
dns.pl.                 28800   IN      NS      kirdan.nask.net.pl.
dns.pl.                 28800   IN      NS      frodo.nask.net.pl.
dns.pl.                 28800   IN      NS      bilbo.nask.org.pl.
dns.pl.                 28800   IN      NS      ns1.tpnet.pl.
dns.pl.                 28800   IN      NS      ns.tpnet.pl.
dns.pl.                 28800   IN      NS      eomer.nask.net.pl.
;; Received 336 bytes from 195.187.245.51#53(bilbo.nask.org.pl) in 3 ms
```

NASK

DNS Explained by CENTR

www.centr.org

NASK

Serwery nazw, resolwery, zasoby rekordów

NASK

Komponenty systemu DNS

- zasobów rekordów (Resource Records); dane zawarte w danej domenie (strefie);
- serwerów nazw
  - Serwer nazw może obsługiwać wiele domen. Dane domen zdefiniowane przez zasoby rekordów są zorganizowane w plikach stref (ang. zone files) tworzących bazę danych serwera nazw.
  - Format plików stref zdefiniowany jest przez RFC 1035.
- resolwerów
  - Resolwer jest to program lub biblioteka systemowa, która odpowiada za komunikację z serwerami nazw.
  - Na systemach operacyjnych zazwyczaj rezyduje stub resolwer. Jest to minimalna implementacja resolwera, która wspiera tylko zapytania rekurencyjne, tzn. nie potrafi sam rozwiązywać nazw, polega na odpowiedzi serwera nazw wskazanego w konfiguracji danego hosta.

NASK

Rodzaje zapytań DNS

- Rekurencyjne (ang. recursive)
  - Zadanie rozwiązania nazwy przeniesione jest na serwer nazw, do którego zostało wysłane takie zapytanie. Na takie zapytanie resolwer otrzyma pełną odpowiedź lub błąd.
- Iteracyjne (ang. Iterative)
  - Takim zapytaniem pytamy się co serwer wie o danej domenie. Na takie zapytanie otrzymamy pełną odpowiedź lub wskazanie na inne serwery (ang. referral).

NASK

Typy konfiguracji serwerów nazw

- Master/Primary server
- Slave/Secondary server
- Caching server
- Forwarding server
- Stealth (Hidden Primary)
- Authoritative
- Split Horizon

NASK

Master server

- Na serwerze master (podstawowym) wprowadzamy zmiany w danej strefie, np. ręcznie lub za pomocą mechanizmu dynamicznych aktualizacji (ang. dynamic updates).
- Serwer master wysyła powiadomienia (ang. notify) do serwerów slave jeśli strefa uległa aktualizacji.
- Jest serwerem autorytatywnym dla skonfigurowanych dla nim domen.

NASK

Slave server

- Serwer slave (zapasowy) pobiera strefę z serwera master za pomocą mechanizmu transferu stref (AXFR lub IXFR).
- Tak samo jak master udziela informacji autorytatywnych dla stref, które obsługuje.
- Serwer nazw może być jednocześnie serwerem slave i master zależnie od sposobu konfiguracji domen.

NASK

Caching server

- Caching server zapamiętuje wyniki rozwiązywania nazw.
- Zapisuje w pamięci podręcznej tylko wyniki odpowiedzi ze źródeł autorytatywnych na czas równy wartości TTL (ang. time to live) strefy lub indywidualnego rekordu.
- Może być również serwerem master lub slave dla skonfigurowanych na nim domen.
- Tak samo jak master i slave udziela informacji autorytatywnych dla stref, które obsługuje. Jeżeli odpowiada z informacjami zapamiętanymi wówczas takie odpowiedzi są nieautorytatywne.
- Typowym zachowaniem BIND przy włączonej rekurencji jest keszowanie odpowiedzi.

NASK

Forwarding server

- Forwarding server działa analogicznie jak proxy, przekazuje wszystkie zapytania do innego serwera DNS (wskazanego w pliku konfiguracyjnym) i zapamiętuje zwrócone odpowiedzi.

NASK

Stealth server

- Stealth server nie występuje w delegacji domeny i nie jest wskazany przez rekordy NS w danej domenie.

NASK

Authoritative only server

- Jest to serwer master lub slave z wyłączoną rekurencją i keszowaniem.
- W serwerze BIND samej funkcji keszowania nie można wyłączyć, takie zachowanie BIND'a kontrolujemy przez włączanie lub wyłączenie rekurencji.

NASK

Split horizon server

- Jest to serwer nazw, który udziela różnych informacji w zależności od adresu źródłowego zapytania DNS zgodnie z konfiguracją.
  - Taką funkcjonalność można uzyskać korzystając z dyrektywy widoków w serwerze BIND (ang. view clouse).

NASK

Podstawowe typy rekordów DNS

- A - przypisuje adres IPv4 do domeny lub subdomeny (RFC 1035)
  - `www.example.com. IN A 69.9.64.11`
- AAAA - przypisuje adres IPv6 do domeny lub subdomeny (RFC 3596)
  - `example.com. IN AAAA 2001:db8::3`
- NS – Name Server, wskazuje na autorytatywny serwer domeny (RFC 1035); Występuje w pliku strefy autorytatywnego serwera oraz w tzw. punkcie delegacji w domenie nadrzędnej. Rekordy występujące w punkcie delegacji nie są rekordami autorytatywnymi.
- MX – Mail exchanger, wskazuje nazwe serwera pocztowago w danej domenie (RFC 1035)
  - `example.com. IN MX 10 mail1.example.com.`
  - `example.com. IN MX 20 mail2.example.com.`

NASK

Podstawowe typy rekordów DNS

- SOA - Start of Authority, rekord wskazuje na master serwer domeny, podaje e-mail kontaktowy do administratora oraz ważne parametry strefy jak: numer seryjny, czasy ekspiracji, ponowienia aktualizacji, odświeżanie danych strefy, negatywnego TTL (RFC 1035).

```
$ORIGIN example.com.
@       IN      SOA   ns1.example.com. hostmaster.example.com. (
                      2011022501 ; serial number
                      1d12h      ; refresh =  1 day 12 hours
                      15M        ; update retry = 15 minutes
                      3W12h      ; expiry = 3 weeks + 12 hours
                      2h20M      ; minimum = 2 hours + 20 minutes
                      )
        IN      NS    ns1.example.com.
        IN      NS    ns2.example.com.
```

NASK

Podstawowe typy rekordów DNS

- TXT – Text, zawiera informację tekstową skojarzaną z daną nazwą (RFC 1035);
  - `ziomal IN TXT „Super bezpieczny serwer”`
- CNAME – alias „kanonicznej” nazwy hosta (RFC 1035)
  - `ftp IN CNAME www.example.com.`
- SRV – Service, wskazuje na hosta świadczącego daną usługę, np.:ldap, imap, http, ftp. (RFC 2872)
  - `_http._tcp.example.com. IN SRV 0 5 80 www.example.com.`
- PTR – pointer występuje w domenie odwrotnej, mapuje adres IP na nazwę hosta (RFC 1035)
  - `11 IN PTR www.example.com.`
- Lista wszystkich zasobów rekordów DNS: http://www.iana.org/assignments/dns-parameters

NASK

DNS - komunikacja

- protokół wymiany komunikatów DNS wykorzystuje TCP bądź UDP, port 53
- brak szyfrowania
- wykorzystanie TCP
  - połączeniowy, mało wydajny dla potrzeb DNS (zestawienie, RTT),
  - rzadko wykorzystywany (0,10 % ruchu)
- wykorzystanie UDP
  - bezpołączeniowy i bezstanowy,
  - przeważnie wykorzystywany
- rozszerzenie EDNS0 pozwala na obsługę wiadomości dłuższych niż 512 bajtów (domyślnie 4kB).

NASK

DNS - sepcyfikacja [1]

1. RFC 952 DOD INTERNET HOST TABLE SPECIFICATION
2. RFC 1032 DOMAIN ADMINISTRATORS GUIDE
3. RFC 1033 DOMAIN ADMINISTRATORS OPERATIONS GUIDE
4. RFC 1034 DOMAIN NAMES - CONCEPTS AND FACILITIES
5. RFC 1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
6. RFC 1101 DNS Encoding of Network Names and Other Types
7. RFC 1122 Requirements for Internet Hosts -- Communication Layers
8. RFC 1123 Requirements for Internet Hosts -- Application and Support
9. RFC 1183 New DNS RR Definitions
10. RFC 1348 DNS NSAP RRs
11. RFC 1535 A Security Problem and Proposed Correction With Widely Deployed DNS Software
12. RFC 1536 Common DNS Implementation Errors and Suggested Fixes
13. RFC 1537 Common DNS Data File Configuration Errors
14. RFC 1591 Domain Name System Structure and Delegation (Informational)
15. RFC 1611 DNS Server MIB Extensions
16. RFC 1612 DNS Resolver MIB Extensions
17. RFC 1706 DNS NSAP Resource Records
18. RFC 1712 DNS Encoding of Geographical Location
19. RFC 1750 Randomness Recommendations for Security
20. RFC 1876 A Means for Expressing Location Information in the Domain Name System

NASK

DNS - sepcyfikacja [2]

21. RFC 1886 DNS Extensions to support IP version 6
22. RFC 1982 Serial Number Arithmetic
23. RFC 1995 Incremental Zone Transfer in DNS
24. RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
25. RFC 2052 A DNS RR for specifying the location of services (DNS SRV)
26. RFC 2104 HMAC: Keyed-Hashing for Message Authentication
27. RFC 2119 Key words for use in RFCs to Indicate Requirement Levels
28. RFC 2133 Basic Socket Interface Extensions for IPv6
29. RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
30. RFC 2137 Secure Domain Name System Dynamic Update
31. RFC 2163 Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)
32. RFC 2168 Resolution of Uniform Resource Identifiers using the Domain Name System
33. RFC 2181 Clarifications to the DNS Specification
34. RFC 2230 Key Exchange Delegation Record for the DNS
35. RFC 2308 Negative Caching of DNS Queries (DNS NCACHE)
36. RFC 2317 Classless IN-ADDR.ARPA delegation
37. RFC 2373 IP Version 6 Addressing Architecture
38. RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
39. RFC 2535 Domain Name System Security Extensions
40. RFC 2536 DSA KEYs and SIGs in the Domain Name System (DNS)

NASK

DNS - sepcyfikacja [3]

41. RFC 2537 RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
42. RFC 2538 Storing Certificates in the Domain Name System (DNS)
43. RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
44. RFC 2540 Detached Domain Name System (DNS) Information
45. RFC 2541 DNS Security Operational Considerations
46. RFC 2553 Basic Socket Interface Extensions for IPv6
47. RFC 2671 Extension Mechanisms for DNS (EDNS0)
48. RFC 2672 Non-Terminal DNS Name Redirection
49. RFC 2673 Binary Labels in the Domain Name System
50. RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
51. RFC 2825 A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols
52. RFC 2826 IAB Technical Comment on the Unique DNS Root
53. RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)
54. RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering
55. RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record
56. RFC 2929 Domain Name System (DNS) IANA Considerations
57. RFC 2930 Secret Key Establishment for DNS (TKEY RR)
58. RFC 2931 DNS Request and Transaction Signatures (SIG(0)s)
59. RFC 3007 Secure Domain Name System (DNS) Dynamic Update
60. RFC 3008 Domain Name System Security (DNSSEC) Signing Authority

NASK

DNS – sepcyfikacja [4]

61. RFC 3071 Reflections on the DNS, RFC 1591, and Categories of Domains
62. RFC 3090 DNS Security Extension Clarification on Zone Status
63. RFC 3110 RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS
64. RFC 3123 A DNS RR Type for Lists of Address Prefixes (APL RR)
65. RFC 3152 Delegation of IP6.ARPA
66. RFC 3197 Applicability Statement for DNS MIB Extensions
67. RFC 3225 Indicating Resolver Support of DNSSEC
68. RFC 3226 DNSSEC and IPv6 A6 aware server/resolver message size requirements
69. RFC 3258 Distributing Authoritative Name Servers via Shared Unicast Addresses
70. RFC 3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
71. RFC 3364 Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)
72. RFC 3425 Obsoleting IQUERY
73. RFC 3445 Limiting the Scope of the KEY Resource Record (RR)
74. RFC 3467 Role of the Domain Name System (DNS)
75. RFC 3490 Internationalizing Domain Names In Applications (IDNA)
76. RFC 3491 Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)
77. RFC 3492 Punycode:A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
78. RFC 3493 Basic Socket Interface Extensions for IPv6
79. RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
80. RFC 3596 DNS Extensions to Support IP Version

NASK

DNS – sepcyfikacja [5]

81. RFC 3597 Handling of Unknown DNS Resource Record (RR) Types
82. RFC 3645 Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
83. RFC 3655 Redefinition of DNS Authenticated Data (AD) bit
84. RFC 3658 Delegation Signer (DS) Resource Record (RR)
85. RFC 3757 Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag
86. RFC 3833 Threat Analysis of the Domain Name System (DNS)
87. RFC 3845 DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format
88. RFC 3901 DNS IPv6 Transport Operational Guidelines
89. RFC 4025 A Method for Storing IPsec Keying Material in DNS
90. RFC 4033 DNS Security Introduction and Requirements
91. RFC 4034 Resource Records for the DNS Security Extensions
92. RFC 4035 Protocol Modifications for the DNS Security Extensions
93. RFC 4074 Common Misbehavior Against DNS Queries for IPv6 Addresses
94. RFC 4159 Deprecation of "ip6.int"
95. RFC 4193 Unique Local IPv6 Unicast Addresses
96. RFC 4255 Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
97. RFC 4343 Domain Name System (DNS) Case Insensitivity Clarification
98. RFC 4367 What's in a Name: False Assumptions about DNS Names
99. RFC 4398 Storing Certificates in the Domain Name System (DNS)
100. RFC 4408 The DNSSEC Lookaside Validation (DLV) DNS Resource Record

NASK

DNS – sepcyfikacja [6]

101. RFC 4431 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1
102. RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line Signing
103. RFC 4634 US Secure Hash Algorithms (SHA and HMAC-SHA)
104. RFC 4641 DNSSEC Operational Practices

Źródło: http://www.isc.org/community/reference/RFCs/DNS

NASK

DNS – sepcyfikacja [7]

105. RFC 6106 IPv6 Router Advertisement Options for DNS Configuration
106. RFC 6014 Cryptographic Algorithm Identifier Allocation for DNSSEC
107. RFC 5966 DNS Transport over TCP - Implementation Requirements
108. RFC 5936 DNS Zone Transfer Protocol (AXFR)
109. RFC 5933 Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
110. RFC 5864 DNS SRV Resource Records for AFS
111. RFC 5855 Nameservers for IPv4 and IPv6 Reverse Zones
112. RFC 5782 DNS Blacklists and Whitelists
113. RFC 5702 Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
114. RFC 5625 DNS Proxy Implementation Guidelines
115. RFC 5507 Design Choices When Expanding the DNS
116. RFC 5452 Measures for Making DNS More Resilient against Forged Answers
117. RFC 5395 Domain Name System (DNS) IANA Considerations
118. RFC 5358 Preventing Use of Recursive Nameservers in Reflector Attacks
119. RFC 5158 6to4 Reverse DNS Delegation Specification
120. RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
121. RFC 5074 DNSSEC Lookaside Validation (DLV)
122. RFC 5011 Automated Updates of DNS Security (DNSSEC) Trust Anchors
123. RFC 5006 IPv6 Router Advertisement Option for DNS Configuration
124. RFC 5001 DNS Name Server Identifier (NSID) Option
125. RFC 4986 Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover

Źródło: http://www.bind9.net/rfc

NASK

DNS – sepcyfikacja [8]

126. RFC 4956 DNS Security (DNSSEC) Opt-In
127. RFC 4955 DNS Security (DNSSEC) Experiments
128. RFC 4892 Requirements for a Mechanism Identifying a Name Server Instance
129. RFC 4848 Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)
130. RFC 4701 A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)
131. RFC 4697 Observed DNS Resolution Misbehavior
132. RFC 4690 Review and Recommendations for Internationalized Domain Names (IDNs)

Źródło: http://www.bind9.net/rfc

NASK

Root

NASK

Strefa root

- Zarządzana jest przez organizację IANA (The Internet Assigned Numbers Authority, www.iana.org)
- Baza danych strefy root http://www.iana.org/domains/root/db/
- Whois http://www.iana.org/whois
- Do pobrania:
  - Strefa root http://www.internic.net/zones/root.zone
  - Lista serwerów root http://www.internic.net/zones/named.root

NASK

Serwery root

- Informacje o serwerach root:
  www.root-servers.org
- **13** serwerów: **a**,b,**c**,d,e,**f**,**g**,**h**,**i**,**j**,**k**,l,**m**
- Serwery unicast i **anycast**
- Łącznie **301** serwerów
- serwery root w Polsce
  - j.root-servers.net – dwie lokalizacje w Warszawie (jedna w NASK)
  - k.root-servers.net – Poznań
  - l.root-servers.net - Warszawa
- L.root-servers.net – serwer anycast; ponad 70 lokalizacji na całym świecie.

NASK

Serwery root

Serwer	Operator	Lokalizacje
A	VeriSign, Inc.	6
B	Information Sciences Institute	1
C	Cogent Communications	6
D	University of Maryland	1
E	NASA Ames Research Center	1
F	Internet Systems Consortium, Inc.	49
G	U.S. DOD Network Information Center	6
H	U.S. Army Research Lab	2
I	Netnod (formerly Autonomica)	38
J	VeriSign, Inc.	70
K	RIPE NCC	18
L	ICANN	97
M	WIDE Project	6

Źródło: www.root-servers.org

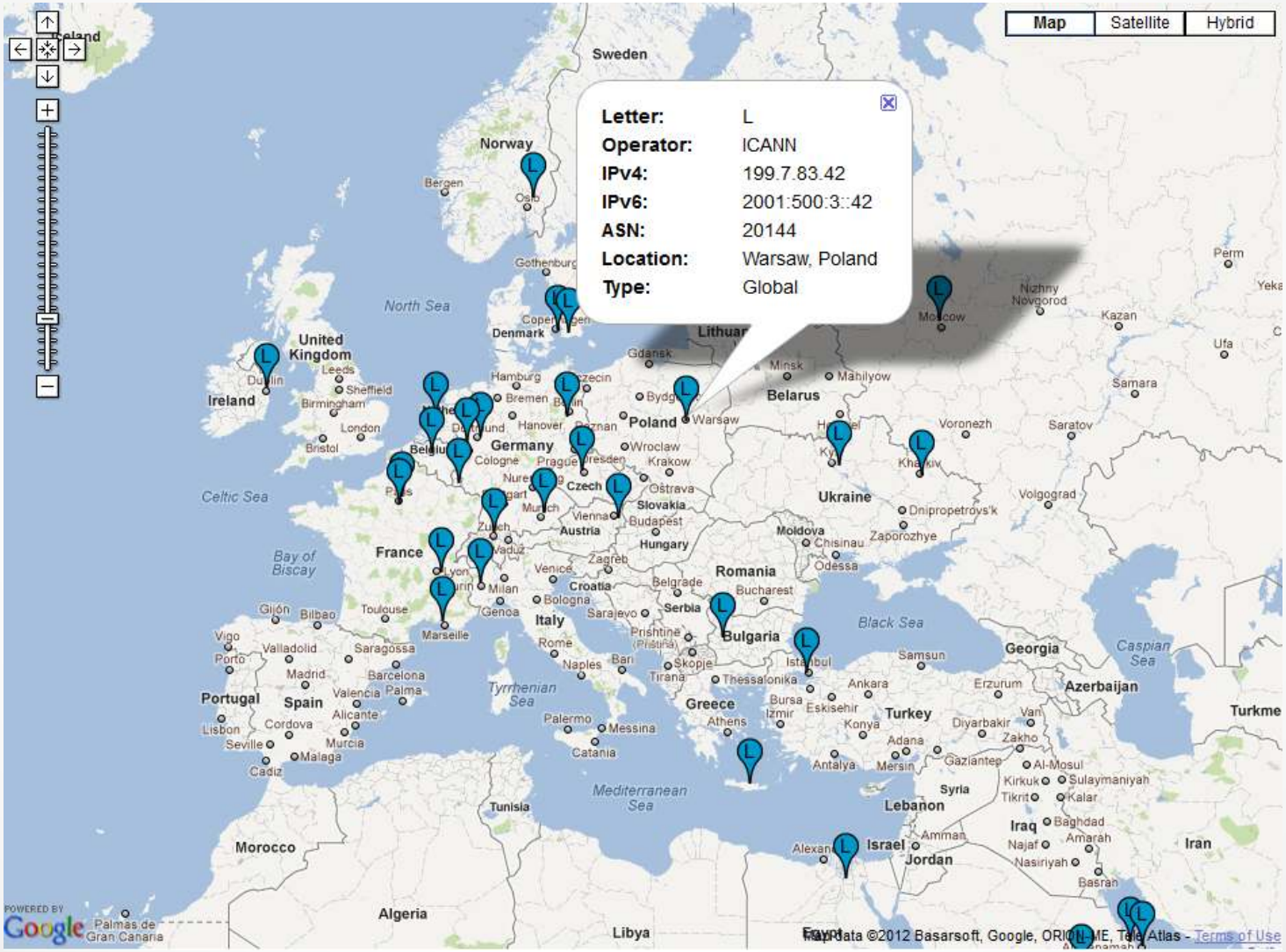
NASK

Lokalizacja serwerów root

www.root-servers.org

NASK

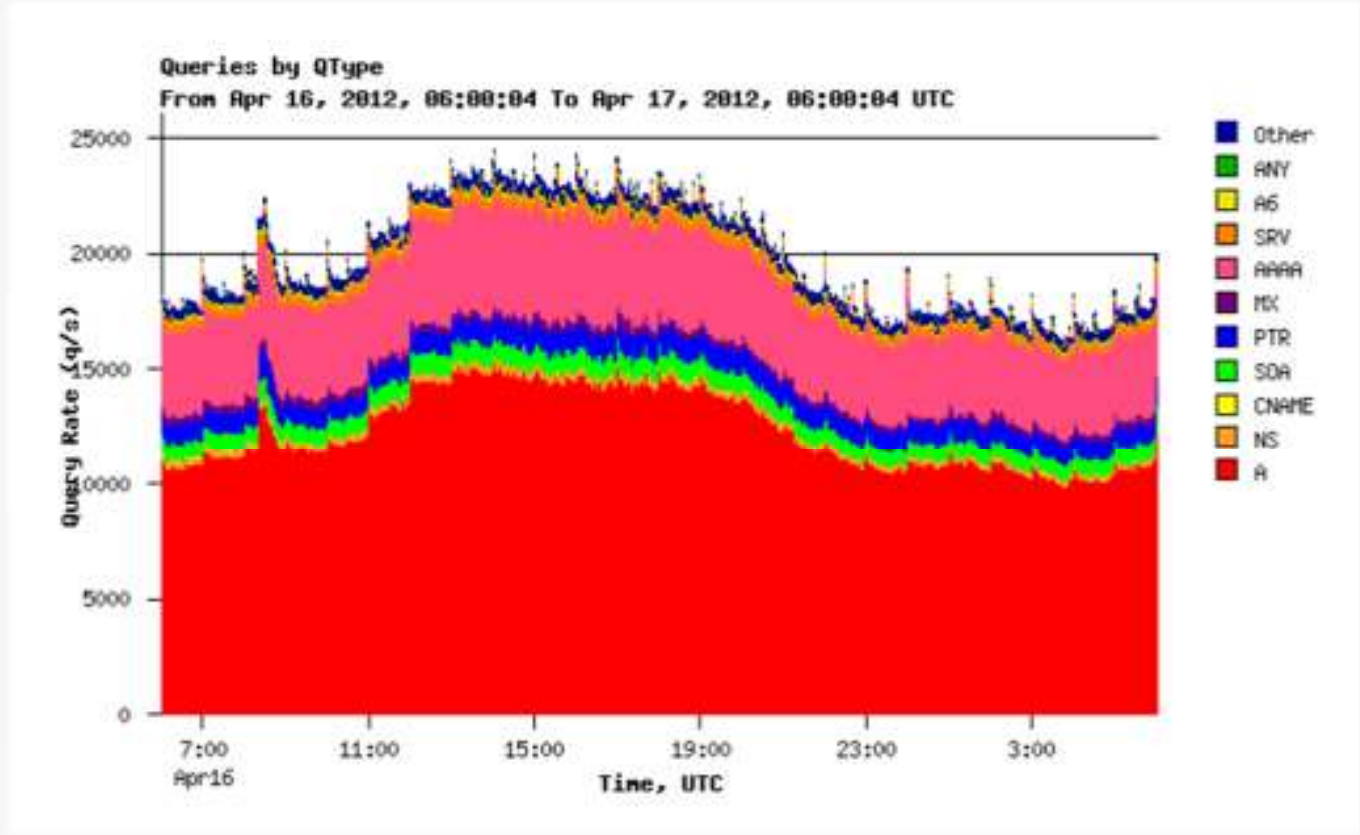
L-root



Źródło: http://dns.icann.org/lroot/locations/

NASK

L-root - Statyski

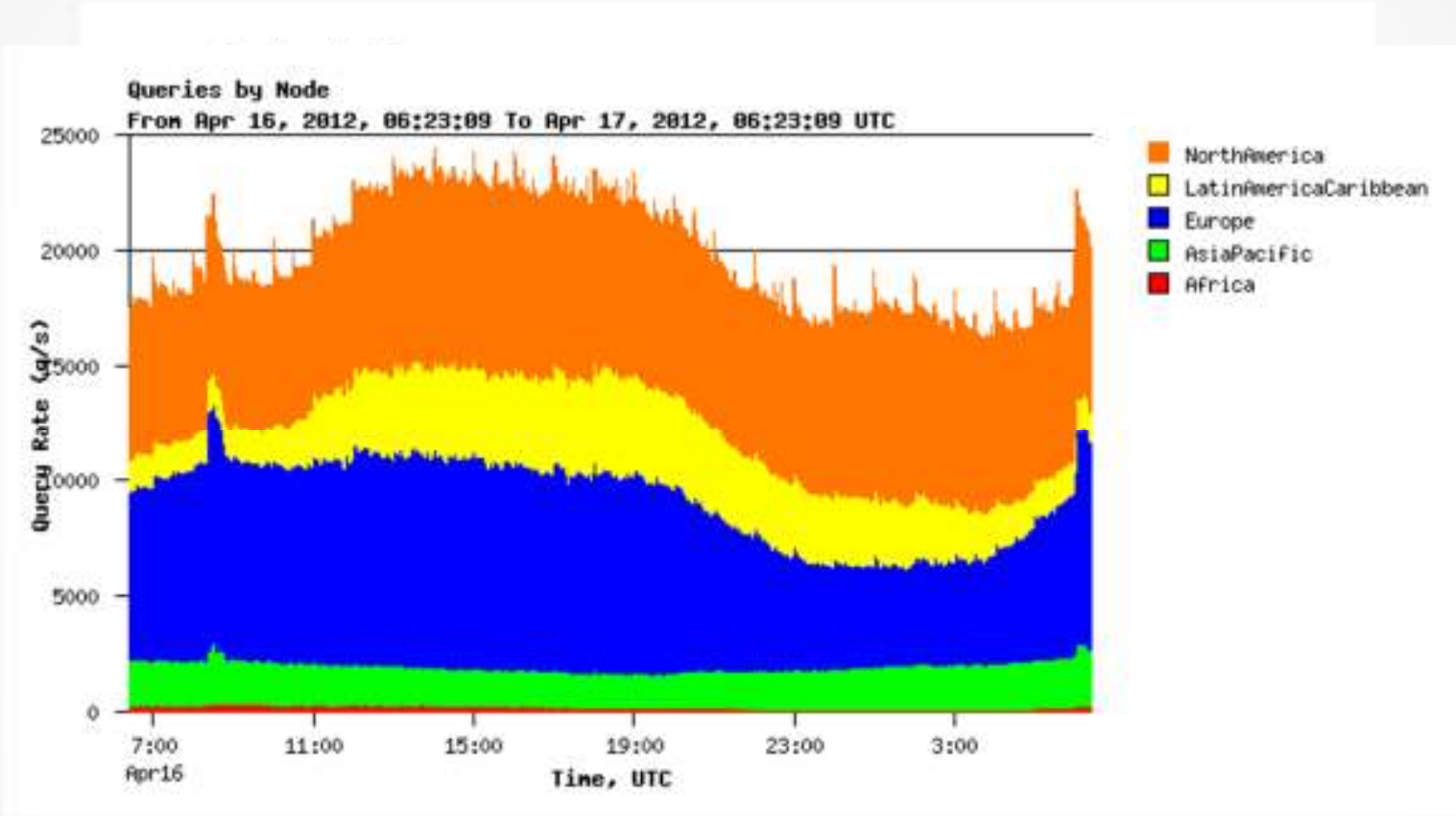


L-Root Queries per Second

Źródło: http://dns.icann.org/lroot/stats/

NASK

L-root - Statyski



L-Root Queries per Second

Źródło: http://dns.icann.org/lroot/stats/

NASK

.pl

NASK

Serwery nazw .pl

- a-dns.pl internet address = 195.187.245.44
- c-dns.pl internet address = 195.47.235.226
- d-dns.pl internet address = 213.172.174.70
- e-dns.pl internet address = 195.80.237.162
- f-dns.pl internet address = 217.17.46.189
- f-dns.pl AAAA IPv6 address = 2001:1a68:0:10::189
- g-dns.pl internet address = 149.156.1.6
- g-dns.pl AAAA IPv6 address = 2001:6d8:0:1::a:6
- **h-dns.pl internet address = 194.0.1.2**
- **h-dns.pl AAAA IPv6 address = 2001:678:4::2**
- **i-dns.pl internet address = 156.154.100.15**

NASK

Lokalizacja serwerów .pl

NASK

Serwery root – ataki DDoS

- DDoS – Distributed Denial of Service
  - rozproszona odmowa usługi,
  - atak przeprowadzony równocześnie z wielu komputerów na określoną usługę mający na celu uniemożliwienie jej działania poprzez wysycenie jej zasobów.
- 21.10.2002 – jednoczesny atak na 13 serwerów root
  - fakty: http://www.isc.org/f-root-denial-of-service-21-oct-2002
- 6.02.2007 – zaatakowano 6 serwerów, w tym dwa skutecznie
  - fakty: http://www.icann.org/en/news/announcements/announcement-08mar07-en.htm

NASK

Serwery root – ataki DDoS

„At least six root servers were attacked but only two of them were noticeably affected: the "g-root", which is run by the U.S. Department of Defense, and the "l-root" run the Internet Corporation for Assigned Names and Numbers (ICANN), based in California.

*The reason why these **two were particularly badly affected** was because they are **the only root servers attacked that have yet to install Anycast** (a further three root servers without Anycast were not attacked this time)."*

Źródło: ICANN, Factsheet, Root server attack on 6 February 2007

NASK

Anycast w DNS

NASK

Anycast

- model trasowania, gdzie dane są kierowane do najbliższego lub najlepszego hosta docelowego z punktu widzenia topologii sieci i polityk trasowania,
- model komunikacji jeden do jeden z wielu,
- wiele hostów posiada ten sam adres IP,
- zastosowanie podstawowych protokołów bez żadnych modyfikacji,
- najczęściej stosowany przez usługi wykorzystujące do transportu protokoły bezstanowe, np. UDP,
- najpopularniejsze zastosowanie: DNS.

NASK

Internet

- **Internet** – globalna sieć połączonych i wymieniający ze sobą dane mniejszych sieci
  - na stykach sieci znajdują się routery
- **router** – urządzenie odpowiadające za wyznaczanie trasy i przesyłanie pakietów do celu
  - routery informują się wzajemnie jakie sieci są dostępne za ich pośrednictwem – rozgłaszanie prefiksów np. 192.168.1.0/24
  - za wyznaczanie optymalnej trasy pakietu odpowiadają protokoły trasowania (IGP wewnątrz sieci i BGP na zewnątrz sieci)
- **system autonomiczny** - grupa połączonych ze sobą sieci będąca pod kontrolą jednego bądź wielu operatorów, w obrębie której stosowana jest wspólna i jasno określona polityka trasowania – RFC 1930
  - taka sieć jest identyfikowana za pomocą specjalnego numeru określanego jako ASN (Autonomous System Number).

NASK

Internet

- **protokoły trasowania** – realizują wymianę informacji o trasach pomiędzy sieciami
  - informacje zapisywane w tablicach trasowania, w najprostszej postaci są to informacje o następnym przeskoku (ang. hop)
  - wewnętrzne protokoły trasowania IGP (Interior Gateway Protocols) - używane do wymiany informacji o trasach w systemie autonomicznym np. OSPF, IS-IS, RIP, IGRP
  - zewnętrzne protokoły trasowania EGP (Exterior Gateway Protocols) – wykorzystywane do wymiany informacji między systemami autonomicznymi, np. BGP (Border Gateway Protocol), EGP (przestarzały)
- **metryki trasowania** – wartości pozwalające określić, która trasa jest najlepsza
  - mogą uwzględniać: szerokość pasma, opóźnienie, liczba przeskoków, koszt ścieżki, obciążenie, MTU (maksymalny rozmiar datagramu), niezawodność, koszt komunikacji.

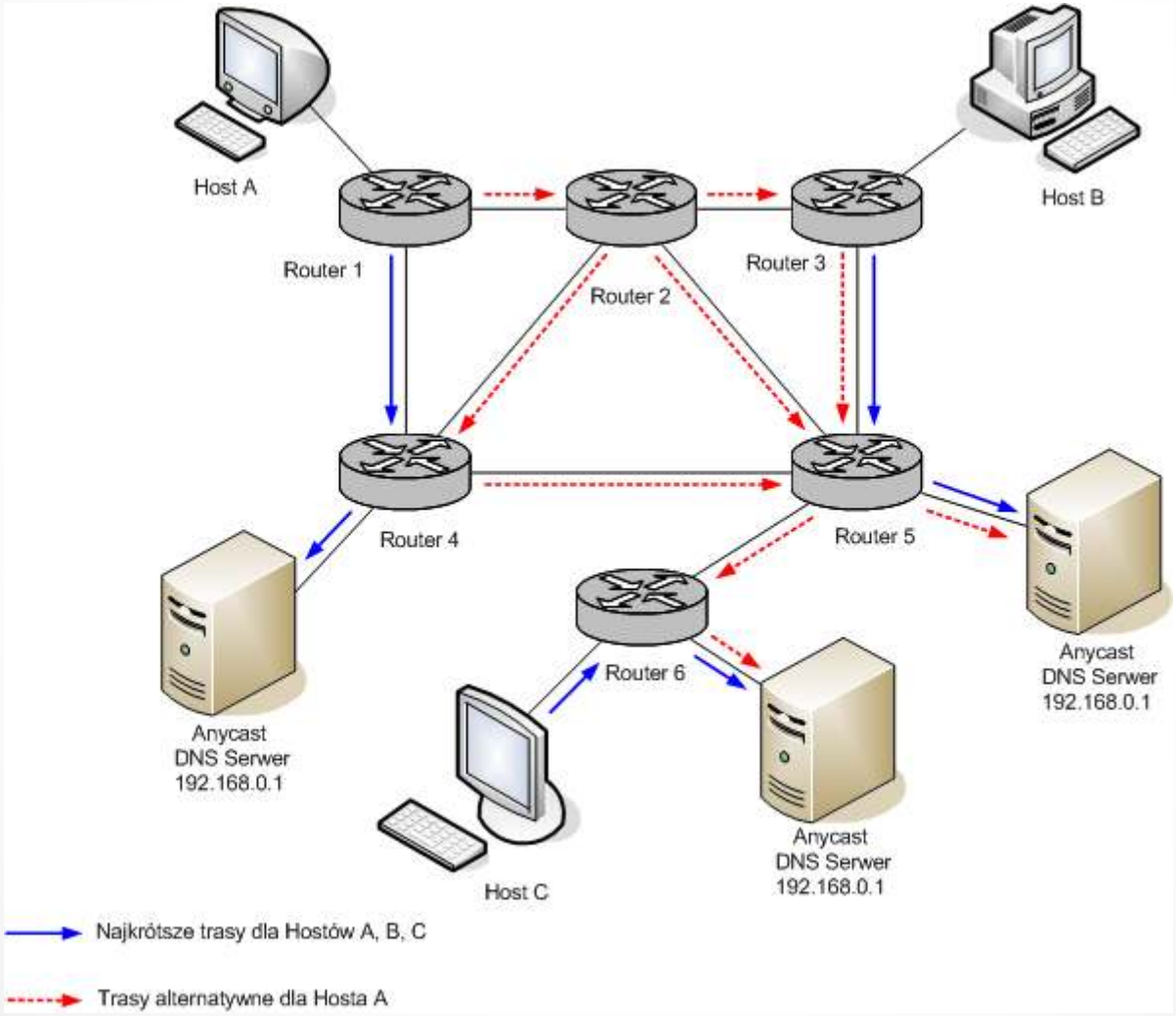
NASK

Anycast – globalny i lokalny

- **lokalny anycast** - jego zasięg (widoczność) jest ograniczony do danego autonomicznego systemu
  - do trasowania stosowane głównie protokoły IGP (np. OSPF, EIGRP, IS-IS)
- **globalny anycast** – węzły klastra anycast rozmieszczone w sieciach różnych operatorów i widoczne z całego świata
  - do trasowania wykorzystany jest protokoły BGP
- serwery root systemu DNS korzystają zarówno z lokalnych jak i globalnych węzłów anycast.

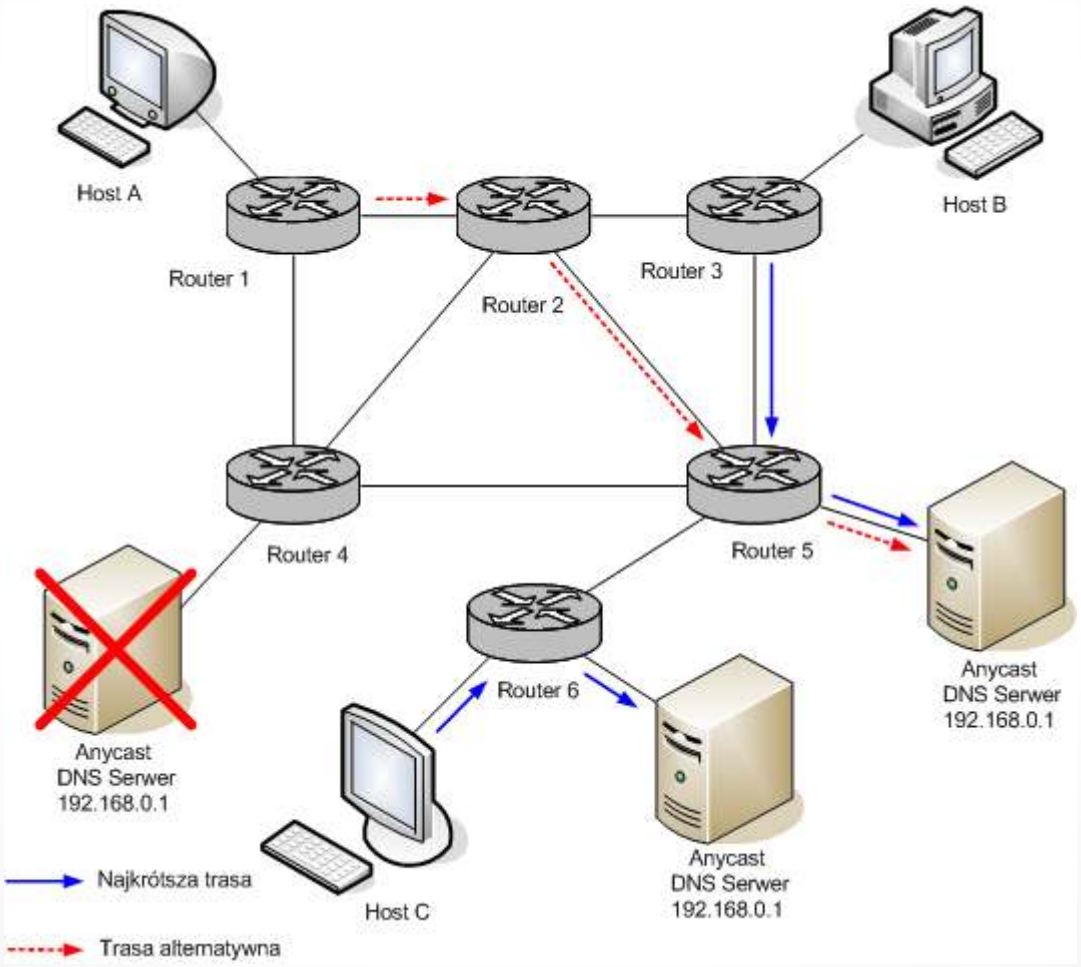
NASK

Anycast – podstawy działania



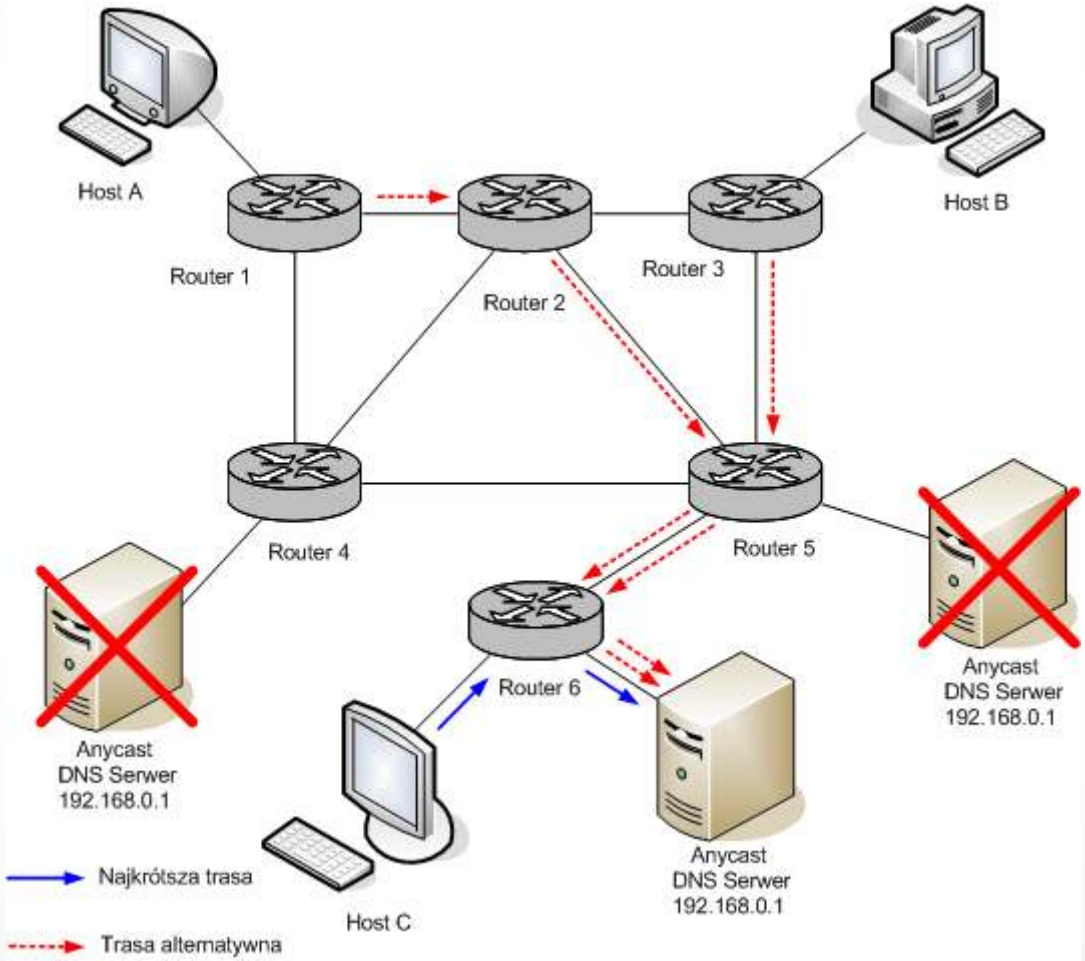
NASK

Anycast – podstawy działania



NASK

Anycast – podstawy działania



NASK

Adresacja anycast

- w anycast stosowane są zwykłe adresy unicast w przeciwieństwie do multicast
  - IANA nie ma wydzielonej przestrzeni adresów IPv4 dla zastosowań anycast w przeciwieństwie do wydzielenia w adresacji IPv6
  - na potrzeby multicast wydzielona jest specjalna klasa adresów 224.0.0.0/4
- rozgłaszana przestrzeń adresów anycast w ramach danego systemu autonomicznego może być ograniczona do jednego adresu hosta (/32)
- RIPE przydziela specjalną klasę adresów (/24) PI - Provider Independent
  - http://www.ripe.net/ripe/docs/ripe-530#---anycasting-tld-and-tier-0/1-enum-nameservers

NASK

Anycast - zalety

- zwiększona niezawodność usługi DNS
  - dowolna liczba lokalizacji i serwerów
  - automatyczne wykluczenie z trasowania węzłów, które uległy awarii
- zwiększona pojemność usługi
  - dowolna liczba lokalizacji i serwerów
- poprawiona skalowalność
  - dowolna liczba węzłów i serwerów
- szybkość działania usługi
  - komunikacja z najbliższym hostem docelowym
- potwierdzona odporność na ataki DDoS
  - lokalne utylizowanie złośliwego ruchu
- jeden serwer w delegacji domeny – dowolna liczba fizycznych instancji (łatwość konfiguracji).

NASK

Anycast - wyzwania

- wprowadza dodatkową złożoność w infrastrukturę DNS
- trudniejszy w utrzymaniu
  - wiele urządzeń,
- trudniejsze wykrywanie i rozwiązywanie problemów
  - identyfikacja problematycznej instancji anycast lub powiązanych z nią elementów,
- wymaga większych kompetencji w administracji niż zwykły DNS
  - wymagana bardzo dobra znajomość zagadnień sieciowych zwłaszcza do diagnostyki i usuwania awarii,
- propagacja danych w chmurze anycast DNS
  - wymaga dobrego zaprojektowania zwłaszcza w kontekście dynamicznego DNSu- często zmieniające się strefy (np. strefa .pl aktualizowana jest co 5 minut),
- utrudnione monitorowania usługi
  - rozproszona usługa wymaga także rozproszonego monitoringu,
- utrudnione wykrywanie zagrożeń
  - przejęcia routingu (RFC 4593 - Generic Threats to Routing Protocols).

NASK

Anycast – zastosowania

- najczęściej stosowany dla usług wykorzystujących protokoły bezstanowe:
  - np. DNS, RP (multicast rendezvous points),
  - inne możliwe zastosowania: Radious, Kerberos, NTP,
- anycast może być także stosowny dla co najmniej wybranych usług wykorzystujących protokół TCP
  - Anycast-aware transport for content delivery networks http://dl.acm.org/citation.cfm?id=1526750
  - TCP Anycast - Don't believe the FUD, Operational experience with TCP and Anycast. NANOG #37 http://www.nanog.org/meetings/nanog37/abstracts.php?pt=Mzg0Jm5hbm9nMzc=&nm=nanog37
  - Anycast-Aware Transport for Content Delivery Networks http://www.cs.ucsb.edu/~almeroth/classes/W10.290F/papers/www-09.pdf
  - Anycast CDNs Revisited http://www2.research.att.com/~slee/pubs/www2008-anycast.pdf
  - OASIS: Anycast for Any Service http://www.cs.berkeley.edu/~karthik/research/papers/oasis/

NASK

IDN

Internationalized Domain NAmes

NASK

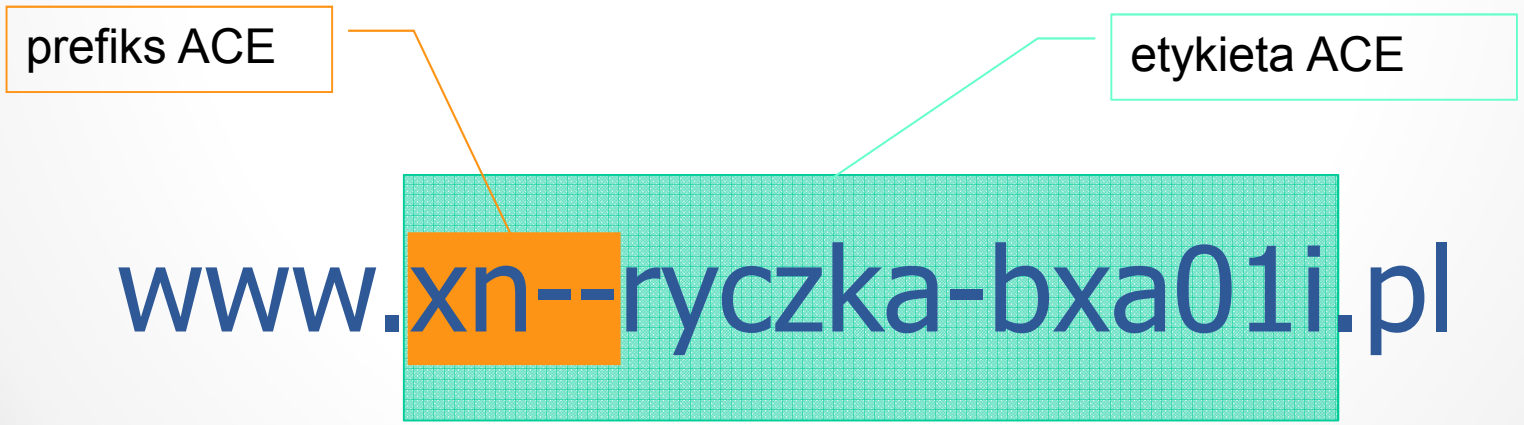
Domeny IDN

Forma unikodowa domeny IDN:

www.różyczka.pl

Forma ACE domeny IDN (przechowywana w zasobach DNSu):

ACE - ang. ASCII Compatible Encoding



NASK

Domeny IDN

- **IDN** - czyli Internationalized Domain Name; jest to nazwa domenowa, którą możemy zapisać używając znaków zaczerpniętych z repertuaru znaków Unikodu.
- **IDNA** - czyli Internationalizing Domain Names in Application; jest to mechanizm odpowiadający za utrzymanie i używanie IDN w „standardowym stylu" (RFC 3490). RFC 5890 jest nową wersją protokołu IDNA.
- **Unikod** - (ang. Unicode) przypisuje każdemu znakowi unikalny numer (kod numeryczny, ang. code point), niezależny od używanej platformy, programu czy języka. Unikod jest nowoczesnym sposobem kodowania obejmującym znaki używane na całym świecie (np. polskie ogonki, hieroglify, cyrylicę), symbole muzyczne, techniczne, fonetyczne i inne często spotykane. Ważną cechą Unikodu jest fakt, że pierwsze 128 znaków odpowiada kodom ASCII (zakres 00..7F). (www.unicode.org)
  - Unicode IDNA Compatibility Processing (Unicode Technical Standard #46) http://www.unicode.org/reports/tr46/tr46-5.html

NASK

Cechy IDNA

- Pozwala na używanie w nazwach domen internetowych znaków „non-ASCII” reprezentowanych za pomocą znaków ASCII.
- IDNA nie wprowadza żadnych zmian do infrastruktury Internetu. Żaden z istniejących protokołów nie musi być modyfikowany aby móc używać IDN.
- Protokoły niższych warstw nie musza być „świadome” użycia IDN w aplikacji.
- IDNA ma zastosowanie tylko do aplikacji użytkownika (IDNA ingeruje tylko w warstwę aplikacji modelu ISO OSI), np.: przeglądarki internetowe, klienci poczty elektronicznej, klienci FTP itp.

NASK

Możliwe problemy i komplikacje

- Użytkownik IDNA musi wiedzieć jak dokładnie wprowadzić daną domenę (literka po literce).
- Wprowadzenie dużego repertuaru znaków może powodować dużą ilość błędów (literówek) w pisaniu nazw domen.
- Możliwość błędnego odczytania domeny ze względu na podobieństwo niektórych znaków.
- Problemy we wprowadzeniu poprawnej nazwy domeny w oparciu o wizualną albo oralną informację (np. billboard i radio).
- Może powstać wiele podobnie wyglądających lub brzmiących nazw.

NASK

Co „piszczy” w środku?

- IDNA zawiera się tylko w aplikacji.
- Wykonywane są dwie operacje:
  - ToASCII – jest wykonywana przed wysłaniem IDN do czegoś, co oczekuje nazw w kodzie ASCII (np. resolwer) lub zapisuje IDN w miejsce, gdzie oczekiwana jest nazwa w kodzie ASCII (np. plik konfiguracyjny serwera DNS).
  - ToUnicode – jest wykonywana przed wyświetleniem IDN użytkownikowi.
- IDNA wymaga zaimplementowania Nameprep’a, który jest profilem Stringprep’a, i Punycode’a.

NASK

Stringprep, Nameprep, Punycode

- **Stringprep** (RFC 3454) - ogólny algorytm przygotowania tekstu Unikodowego przed zamianą go na ciąg znaków ASCII (tzn. algorytm, który może być profilowany - dostosowywany do rożnych potrzeb). Draft określa kilkanaście tabel (mapowania, znaki zakazane, tablice "dwukierunkowe"), które mogą być zastosowane w algorytmach opartych na stringprep'ie (m.in. nameprep).
- **Nameprep** (RFC 3491) jest profilem stringprep'a (w drafcie określono dokładnie, które z tabel mapowania, znaków zakazanych etc., są zastosowane). Reguły przetwarzania zostały wybrane na potrzeby kodowania nazw domenowych, a nie zwykłego tekstu (=> dozwolone znaki zgodne z RFC1035 [a-zA-Z0-9-]).
- **Punycode** (RFC 3492) to instancja algorytmu Bootstring (ma inne wartości parametrów inicjalizujących). Algorytm pozwala jednoznacznie odwzorować ciągi znaków stworzone z większego zbioru znaków w ciągi złożone z mniejszego zbioru znaków.

NASK

Podobieństwo znaków i spoofing

Single-script spoofing

pepsi.pl	xn--e1avb8ff.pl
cocacola.pl	xn--l-7sbb7cbpbb.pl
paypal.pl	xn--payl-73d9g.pl
paypal.pl	xn--l-7sba6dbr.pl
paypal.pl	xn--apl-7cd1fta.pl
mbank.pl	xn--mbnk-63d.pl

Latin script

Cyrillic script

Mixed-script spoofing

http://en.wikipedia.org/wiki/IDN_homograph_attack

NASK

Podobieństwo znaków i spoofing

Latin			Cyrillic			Greek			Hebrew	According to confusables
glyph	code point	character name	glyph	code point	character name	glyph	code point	character name		
6	0036	DIGIT SIX	б	0431	CYRILLIC SMALL LETTER BE					X
a	0061	LATIN SMALL LETTER A	а	0430	CYRILLIC SMALL LETTER A					X
c	0063	LATIN SMALL LETTER C	с	0441	CYRILLIC SMALL LETTER ES					X
e	0065	LATIN SMALL LETTER E	е	0435	CYRILLIC SMALL LETTER IE					X
i	0069	LATIN SMALL LETTER I	і	0456	CYRILLIC SMALL LETTER BYELORUSSIAN-UKRAINIAN I	ι	03B9	GREEK SMALL LETTER IOTA		X[8] X[3]
j	006A	LATIN SMALL LETTER J	ј	0458	CYRILLIC SMALL LETTER JE					X
o	006F	LATIN SMALL LETTER O	о	043E	CYRILLIC SMALL LETTER O	ο	03BF	GREEK SMALL LETTER OMRICON		X[2]
p	0070	LATIN SMALL LETTER P	р	0440	CYRILLIC SMALL LETTER ER	ρ	03C1	GREEK SMALL LETTER RHO		X (L2C, G2C)
r	0072	LATIN SMALL LETTER R	г	0433	CYRILLIC SMALL LETTER GHE					X
s	0073	LATIN SMALL LETTER S	ѕ	0455	CYRILLIC SMALL LETTER DZE					X
u	0075	LATIN SMALL LETTER U				υ	03C5	GREEK SMALL LETTER UPSILON		X
v	0076	LATIN SMALL LETTER V				ν	03BD	GREEK SMALL LETTER NU		X[1]
x	0078	LATIN SMALL LETTER X	х	0445	CYRILLIC SMALL LETTER HA					X
y	0079	LATIN SMALL LETTER Y	у	0443	CYRILLIC SMALL LETTER U					X[5]
è	00E8	LATIN SMALL LETTER E WITH GRAVE	ѐ	0450	CYRILLIC SMALL LETTER IE WITH GRAVE					X[6]
ë	00EB	LATIN SMALL LETTER E WITH DIAERESIS	ё	0451	CYRILLIC SMALL LETTER IO					X[7]
ï	00EF	LATIN SMALL LETTER I WITH DIAERESIS	ї	0457	CYRILLIC SMALL LETTER YI	ϊ	03CA	GREEK SMALL LETTER IOTA WITH DIALYKTIKA		X[3]
ó	00F3	LATIN SMALL LETTER O WITH ACUTE				ό	03CC	GREEK SMALL LETTER OMICRON WITH TONOS		X[4]
ħ	0127	LATIN SMALL LETTER H WITH STROKE	ћ	045B	CYRILLIC SMALL LETTER TSHE					X
ı	0131	LATIN SMALL LETTER DOTLES I	і	0456	CYRILLIC SMALL LETTER BYELORUSSIAN-UKRAINIAN I	ι	03B9	GREEK SMALL LETTER IOTA		X
κ	0138	LATIN SMALL LETTER KRA	к	043A	CYRILLIC SMALL LETTER KA	κ	03BA	GREEK SMALL LETTER KAPPA		X (L2G, C2G)
			п	043F	CYRILLIC SMALL LETTER PE	π	03C0	GREEK SMALL LETTER PI		X
			ф	0444	CYRILLIC SMALL LETTER EF	φ	03C6	GREEK SMALL LETTER PHI		X
			є	0454	CYRILLIC SMALL LETTER UKRAINIAN IE	ε	03B5	GREEK SMALL LETTER EPSILON		X

NASK

www.polska.pl

www.πολωνία.pl	www.xn--kxae2aiif9d.pl
www.بولندا.pl	www.xn--mgbbv7fkk.pl
www.פולין.pl	www.xn--9dbiinv.pl

NASK

Domeny IDN w NASK

http://www.dns.pl/IDN

- Zasady rejestracji
- Zbiory znaków dopuszczonych do rejestracji
- Narzędzia do konwersji domen IDN
- Dokumenty RFC

NASK

Rejestracja domen

NASK

Rejestracja domen w NASK

- Rejestracja dowolnego ciągu znaków spełniających kryteria techniczne dla nazw domen internetowych.
- Nie jest możliwa rejestracja nazw domen będących nazwami usług sieciowych jak www, http, ftp itp.
- Rejestrowana domena musi być wydelegowana na min. dwa serwery nazw.
- Serwery nazw nie muszą być skonfigurowane do obsługi domeny.
- FAQ na temat rejestracji domen w NASK: http://www.dns.pl/rejestracja-domen.html

NASK

Rejestracja domen w NASK

Domeny funkcjonalne NASK

http://www.dns.pl/dns-funk.html

aid.pl
agro.pl
atm.pl
auto.pl
biz.pl
com.pl
edu.pl
gmina.pl
gsm.pl
info.pl
mail.pl
miasta.pl
media.pl
mil.pl
net.pl
nieruchomosci.pl
nom.pl
org.pl
pc.pl
powiat.pl
priv.pl
realestate.pl
rel.pl
sex.pl
shop.pl
sklep.pl
sos.pl
szkola.pl
targi.pl
tm.pl
tourism.pl
travel.pl
turystyka.pl

NASK

Rejestracja domen w NASK

Domeny regionalne NASK

http://www.dns.pl/dns-regiony.html

A
augustow.pl
B
babia-gora.pl
bedzin.pl
beskidy.pl
bialowieza.pl
bialystok.pl
bielawa.pl
bieszczady.pl
boleslawiec.pl
bydgoszcz.pl
bytom.pl
C
cieszyn.pl
czeladz.pl
czest.pl

D
dlugoleka.pl
E
elblag.pl
elk.pl
G
glogow.pl
gniezno.pl
gorlice.pl
grajewo.pl
I
ilawa.pl
J
jaworzno.pl
jelenia-gora.pl
…

Rejestracja domeny w programie partnerskim

- Domena może zostać zarejestrowana za pośrednictwem partnera NASK.
- Lista partnerów NASK – Registrars: http://www.dns.pl/porozumienie/uslugobiorcy.html

NASK

Dziękuję za uwagę.