Technologie informacyjne

Dr Zbigniew Kozioł -wykład
Mgr Mariusz Woźny - laboratorium

Internet: protokoły, organizacja

Internet i bezpieczeństwo w sieci (II)

0. Co to są protokoły internetowe? RFC.

1. Sposoby adresowania w sieci (IPv4, IPv6). Porty. ICANN. ARIN, RIPE, etc, whois, dig, nslookup
2. TCP/IP
3. Protokoły “usługowe” :
   - telnet (port 20)
   - http (port 80)
   - ftp (port 21, 23)
   - smtp (port 25)
   - protokoły “bezpieczne”:
     - https (port 443)
     - ssh, scp (Putty), sftp (port 22)

4. Kryptografia. Certyfikaty. Przykłady: https i PGP.
   - Dodatkowe zabezpieczenia w e-banking.

5. Społeczności internetowe. Blogi internetowe.

Protokoły internetowe

RFC – jak powstają

TCP/IP
IPv4, IPv6
DNS

telnet
HTTP, HTTPS
SMTP, POP, IMAP
FTP
SSH
etc...

Protokoły internetowe

RFC

(ang. Request for Comments – dosłownie: prośba o komentarze)

– zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum związanych z Internetem oraz sieciami komputerowymi. Każdy z nich ma przypisany unikatowy numer identyfikacyjny, zwykle używany przy wszelkich odniesieniach. Publikacją RFC zajmuje się Internet Engineering Task Force.

Dokumenty nie mają mocy oficjalnej, jednak niektóre z nich zostały później przekształcone w oficjalne standardy sieciowe, np. opis większości popularnych protokołów sieciowych został pierwotnie opisany właśnie w RFC.

RFC

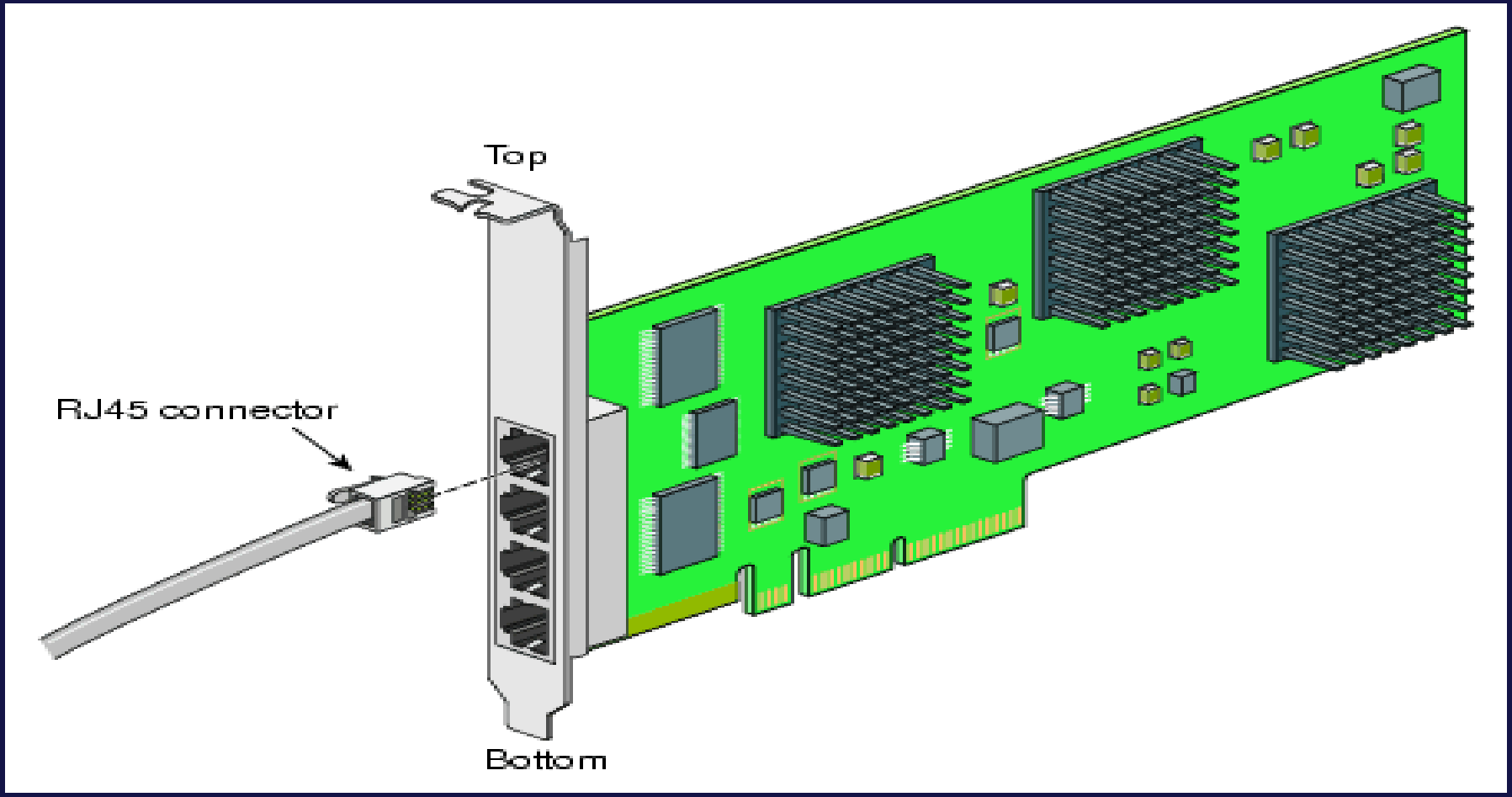
22 czerwca 1973 roku ukazał się pierwszy humorystyczny dokument RFC zatytułowany „ARPAWOCKY” (RFC 527). W późniejszych latach wydano ich jeszcze kilka, natomiast od 1989 roku publikowane są one regularnie w prima aprilis. Praktycznie wszystkie nie mają żadnego zastosowania; zostały napisane dla rozrywki. Oto tytuły niektórych z takich dokumentów:

TELNET – opcja gubienia danych (RFC 748, 1 kwietnia 1978)
Transmisja datagramów IP przez gołębie pocztowe (RFC 1149, 1 kwietnia 1990)
Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0) (RFC 2324, 1 kwietnia 1998)
Transmisja pakietów IP poprzez gołębie pocztowe z QoS (RFC 2549, 1 kwietnia 1999)
Protokół Generowania Liczby PI (RFC 3091, 1 kwietnia 2001)
Etymologia słowa „foo” (RFC 3092, 1 kwietnia 2001)
Electricity over IP (RFC 3251, 1 kwietnia 2002)

RFC (przykłady)

Address Resolution Protocol	RFC 826
Date and Time on the Internet (ISO 8601)	RFC 3339
Domain Name System	RFC 1034, RFC 1035
Dynamic Host Configuration Protocol	RFC 1531, RFC 1541, RFC 2131, RFC 3315 (IPv6)
ECHO protocol	RFC 862
File Transfer Protocol	RFC 114, RFC 172, RFC 265, RFC 354, RFC 765, RFC 959
gzip	RFC 1952
HyperText Transfer Protocol	RFC 1945 (v 1.0), RFC 2616 (v 1.1)
Internet Message Access Protocol	RFC 1176 (v 2), RFC 1730 (v 4), RFC 2060 (v 4r1), RFC 3501 (v 4r1)
Internet Protocol	zobacz IPv4 oraz IPv6
IP over Avian Carriers	RFC 1149, RFC 2549
IPv4	RFC 760, RFC 790, RFC 791
IPv6	RFC 1883, RFC 2460
IPv6 addressing	RFC 2373, RFC 3513
Internet Relay Chat	RFC 1459, RFC 2810, RFC 2811, RFC 2812, RFC 2813
MD5	RFC 1321
Multipurpose Internet Mail Extensions	RFC 2045, RFC 2046, RFC 2047, RFC 2049
Network Address Translation	RFC 2663, RFC 2993, RFC 3022, RFC 3027, RFC 3234, RFC 3489, RFC 4787
Network File System	RFC 1094, RFC 1813 (v.3), RFC 3010 (v.4), RFC 3530 (v.4)
Network News Transfer Protocol	RFC 977 RFC 3977
Network Time Protocol	RFC 1059 (v.1), RFC 1119 (v.2), RFC 1305 (v.3)
Post Office Protocol	RFC 1081 (v.3), RFC 1225 (v.3), RFC 1460 (v.3), RFC 1725 (v.3), RFC 1939 (v.3)
Pretty Good Privacy	RFC 1991, RFC 2440
Secure Shell-2	RFC 4251
Simple Mail Transfer Protocol	RFC 821, RFC 822, RFC 2505, RFC 2821, RFC 2822
TELNET	RFC 854, RFC 855
Uniform Resource Identifier	RFC 3986
UTF-8	RFC 3629

Karta ethernet: łączność między komputerem a siecią



Karta ethernet: łączność między komputerem a siecią

MAC (ang. Media Access Control)

Sprzętowy adres karty sieciowej Ethernet i Token Ring, unikatowy w skali światowej, nadawany przez producenta danej karty podczas produkcji.

Przykład adresu MAC:

zbych@orion:~$ /sbin/ifconfig

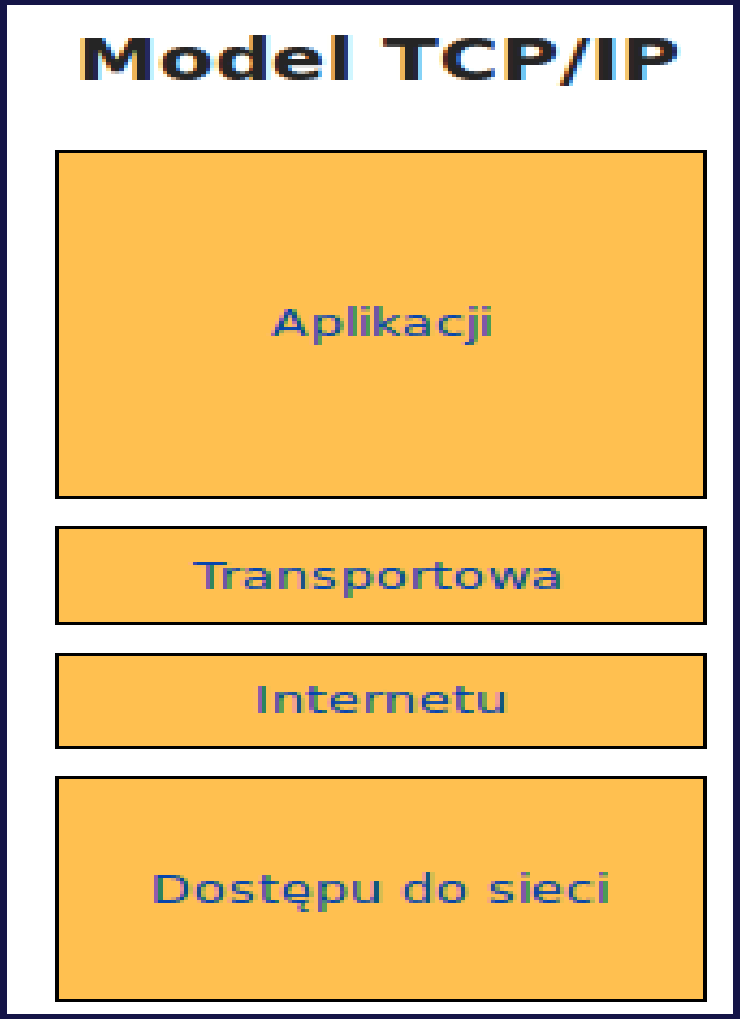
eth0 Link encap:Ethernet **HWaddr 78:45:c4:a1:ef:c2** inet addr:**192.168.1.102** Bcast:192.168.1.255 Mask:255.255.255.0 inet6 addr: fe80::7a45:c4ff:fea1:efc2/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:2624284 errors:0 dropped:0 overruns:0 frame:0 TX packets:1796530 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:3215777605 (3.2 GB) TX bytes:269737680 (269.7 MB)

Pierwsze 3 bajty adresu **78:45:c4:a1:ef:c2** identyfikują producenta karty. Następne trzy bajty są unikatowe.

Protokół TCP/IP

Model TCP/IP (ang. Transmission Control Protocol/Internet Protocol) – teoretyczny model warstwowej struktury protokołów komunikacyjnych. Model TCP/IP został stworzony w latach 70. XX wieku w DARPA, aby pomóc w tworzeniu odpornych na atak sieci komputerowych. Potem stał się podstawą struktury Internetu.

- niezawodny transfer danych,
- dużą przepustowość,
- krótki czas reakcji.

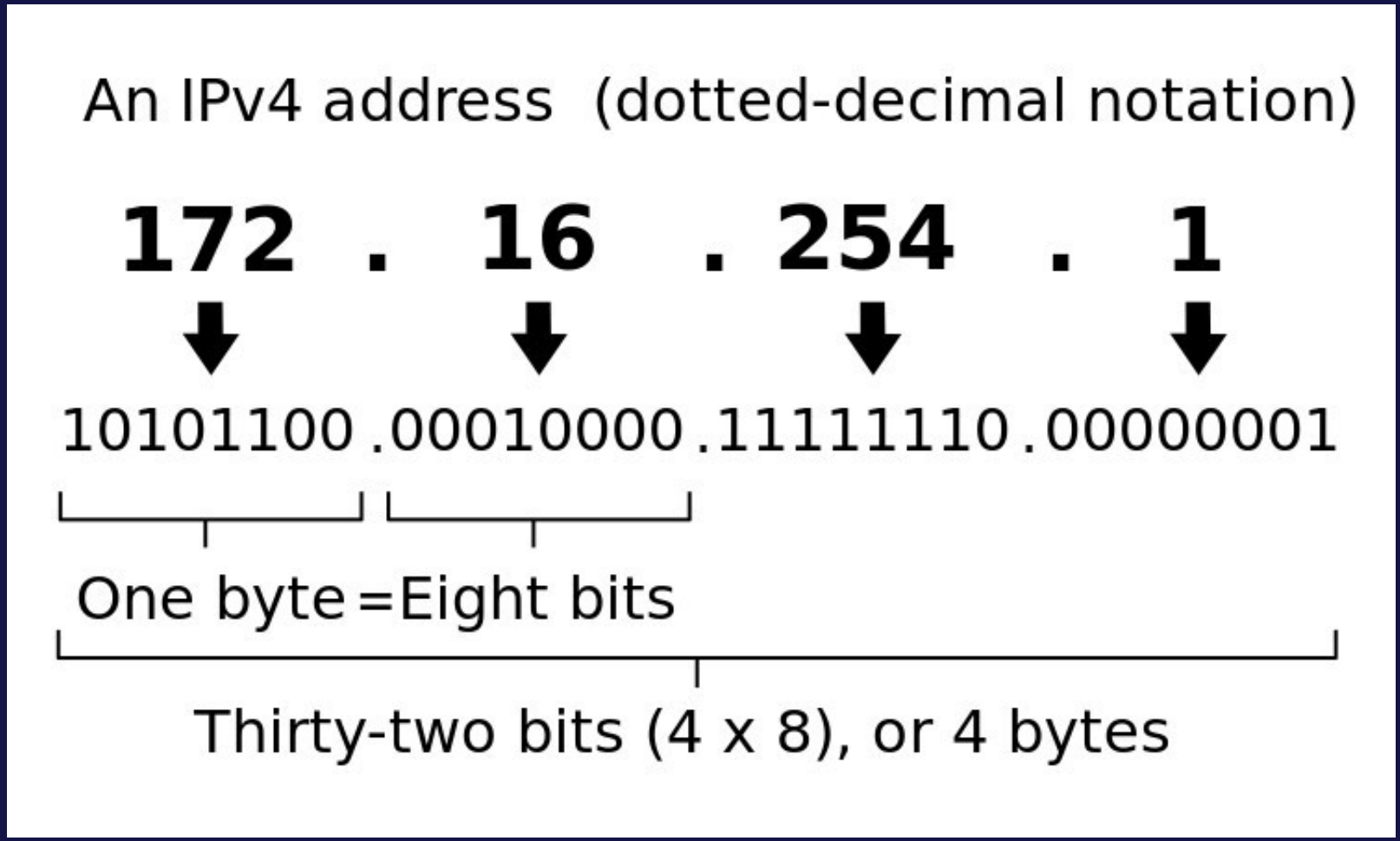


Protokół IP

IP Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

Protokół IP: adresowanie (IPv4)



Protokół IP: adresowanie (IPv4)

WAN (Wide Area Network) – zwykle sieć zewnętrzna Internet
LAN (Local Area Network) – lokalna sieć wewnętrzna, zwykle za firewall (ścianą bezpieczeństwa)

127.0.0.0/8 – zarezerwowane dla lokalnego komputera

IANA-reserved private IPv4 network ranges

	Start	End	No. of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16 777 216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1 048 576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65 536

Protokół IP: adresowanie (IPv6)

IPv6 (ang. Internet Protocol version 6) – protokół komunikacyjny,
- następca protokołu IPv4

Podstawowymi zadaniami nowej wersji protokołu jest zwiększenie przestrzeni dostępnych adresów poprzez zwiększenie długości adresu z 32-bitów do 128-bitów

Uproszczony nagłówek protokołu
Wprowadzenie rozszerzeń

Protokół DNS Domain Name System (pol. „system nazw domenowych”)

nanophysics.pl <==> 88.198.20.90

– system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.232

DNS to złożony system komputerowy oraz prawny. Zapewnia z jednej strony rejestrację nazw domen internetowych i ich powiązanie z numerami IP. Z drugiej strony realizuje bieżącą obsługę komputerów odnajdujących adresy IP odpowiadające poszczególnym nazwom. Jest nieodzowny do działania prawie wszystkich usług sieci Internet

Ale komputer wcale nie musi korzystać z internetowej sieci DNS. Może korzystać z sieci autonomicznej DNS.

Ale może też korzystać wyłącznie z adresów IP (nie zawsze).

DNS AS System autonomiczny (ang. Autonomous System, AS)

- zbiór prefiksów (adresów sieci IP) pod wspólną administracyjną kontrolą, w którym utrzymywany jest spójny schemat trasowania (ang. routing policy).

Kto tym zarządza?

- ICANN Internet Corporation for Assigned Names and Numbers

- IANA Internet Assigned Numbers Authority
- RIR Regional Internet Registers
  - - ARIN
  - - RIPE
  - - etc...

W Polsce nadrzędną organizacją zarządzająca adresami IP i nazwami domen jest NASK (Naukowa i Akademicka Sieć Komputerowa)

Nawiązanie po raz pierwszy łączności przy użyciu protokołu IP pomiędzy Instytutem Fizyki Uniwersytetu Warszawskiego a Centrum Komputerowym Uniwersytetu w Kopenhadze nastąpiło 17 sierpnia 1991 r.

ICANN

Internet Corporation for Assigned Names and Numbers

Internetowa Korporacja ds. Nadanych Nazw i Numerów) to instytucja odpowiedzialna obecnie za przyznawanie nazw domen internetowych, ustalanie ich struktury oraz za ogólny nadzór nad działaniem serwerów DNS na całym świecie. Została powołana do życia 18 września 1998 r. w celu przejęcia od rządu USA funkcji nadzorowania technicznych aspektów Internetu.

Formalnie ICANN jest prywatną organizacją non-profit, faktycznie organizacją rządową USA: rząd USA przekazał czasowo prawo nadzoru nad systemem DNS, przydziałem puli adresów IPv4 oraz IPv6 dla tzw. Regional Internet Registries RIR oraz rejestracją numerów portów.

Rada Dyrektorów raz do roku wybierana przez potencjalnie wszystkich użytkowników Internetu (tzn. że każdy kto ma dostęp do sieci może oddać swój głos). W praktyce jednak na Dyrektorów ICANN głosuje średnio ok 100 000 osób, głównie "świadomych" członków Internet Society i IETF, a więc niewielki ułamek wszystkich internautów. Głosowanie odbywa się za pomocą e-maili.

IANA

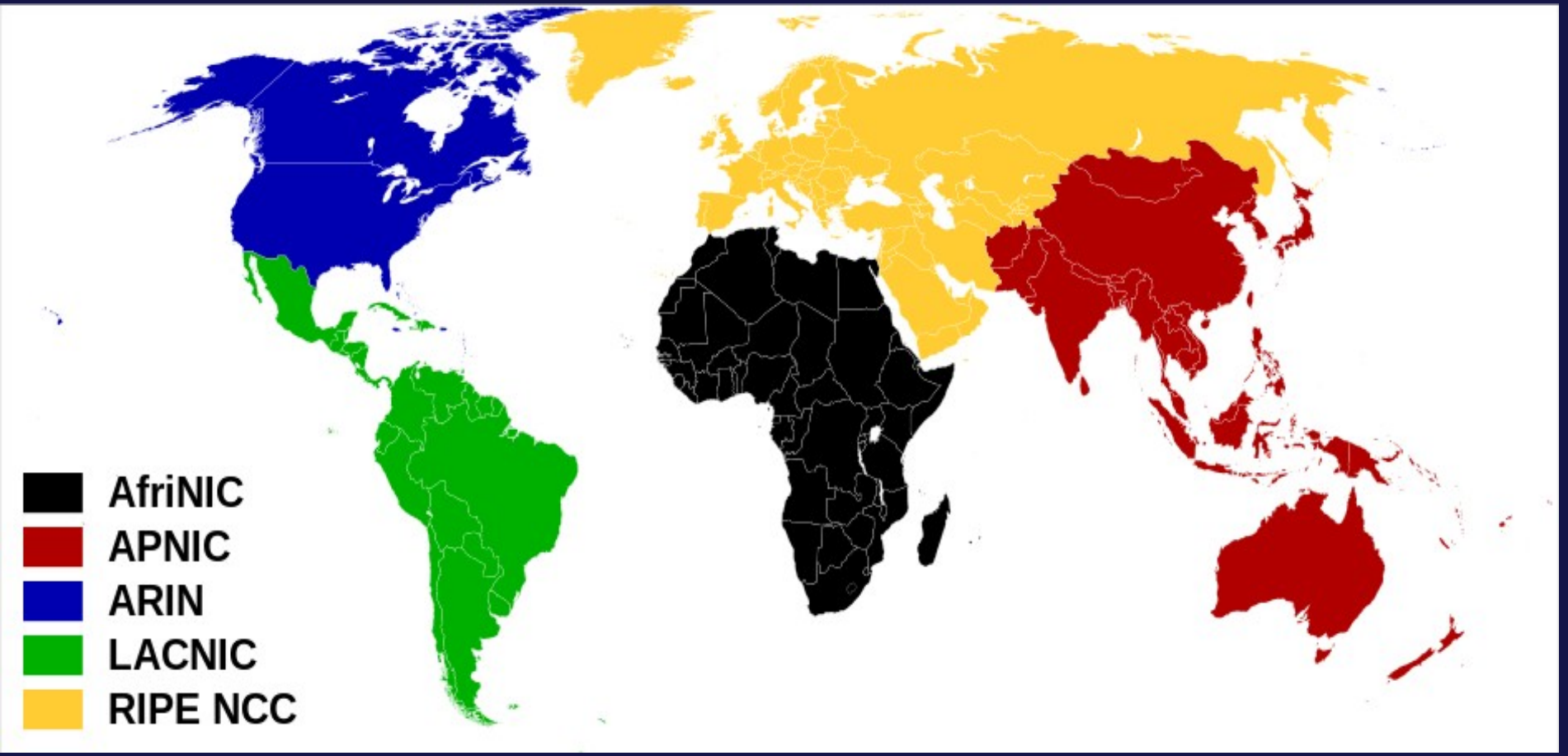
Internet Assigned Numbers Authority

organizacja, która wyłoniła się z Internet Engineering Task Force w celu zaprowadzenia porządku w nazwach domen i adresach IP komputerów przyłączonych do Internetu.

Początkowo IANA była jedną z grup roboczych IETF, która zajmowała się ustaleniem standardów przyznawania numerów IP. Później jednak powstała konieczność powstania instytucji, która będzie na co dzień zarządzała zasadami przyznawania numerów IP i nazw domen kolejnym użytkownikom. To zadanie spełniała długi czas właśnie IANA, która mimo że nie była od strony prawnej sformalizowana, dostała od rządu USA uprawnienia do zarządzania domenami, bo nikt inny nie był wtedy w stanie tego robić.

Na podstawie umowy z rządem USA obowiązującej do roku 2006 (zapewne będzie przedłużana sukcesywnie na kolejne lata) większość codziennej pracy przy przyznawaniu numerów IP oraz zarządzaniu domenami najwyższego poziomu została ostatecznie przekazana ICANN której autonomiczną częścią jest właśnie IANA. Do zadań IANA należy obecnie tylko zarządzanie domenami najwyższego poziomu oraz ogólny nadzór nad działaniem mechanizmu DNS.

Regional Internet Registries



A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers.

RIPE (Réseaux IP Européens Network Coordination Centre)

– niezależna i niedochodowa organizacja wspierająca infrastrukturę sieci Internet. Jej siedziba znajduje się w Amsterdamie. RIPE NCC pełni rolę między innymi Regionalnego Rejestru Internetowego (ang. RIR) przechowując i przydzielając takie dane jak adresy IPv4 i IPv6. Rejonem w jakim działa RIPE są: Europa, Bliski Wschód i część Azji Środkowej.

http://ripe.org

ARIN (American Registry for Internet Numbers)

Regional Internet Registry (RIR) for Canada, the United States, and many Caribbean and North Atlantic islands. ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers. ARIN opened its doors for business on December 22, 1997 after incorporating on April 18, 1997. ARIN is a nonprofit corporation with headquarters in Chantilly, Virginia, USA.

Like the other RIRs, ARIN:

Provides services related to the technical coordination and management of Internet number resources
Facilitates policy development by its members and stakeholders
Participates in the international Internet community
Is a nonprofit, community-based organization
Is governed by an executive board elected by its membership

http://arin.net

Domena najwyższego poziomu (ang. TLD – Top-Level Domain) – domena internetowa, powyżej której nie istnieją żadne inne domeny w systemie DNS. Są one tworzone i zarządzane przez IANA i ICANN.

Każda domena w Internecie składa się z pewnej liczby nazw, oddzielonych kropkami. Ostatnia z tych nazw jest domeną najwyższego poziomu. Na przykład w "pl.wikipedia.org" domeną najwyższego poziomu jest "org".

Domeny najwyższego poziomu są używane w protokole DNS zamieniającym nazwy komputerów na ich adresy IP.

Istnieją 2 typy domen najwyższego poziomu:

krajowe (ang. ccTLD – country code TLD) – zawsze dwuliterowe np. Polska – .pl
funkcjonalne (ang. gTLD – generic TLD) np. .com, .org, .net, .biz, .info

Narzędzia:

- traceroute
- whois
- dig lub nslookup
- ping

traceroute (trasowanie)

```
zbych@orion:~$ traceroute nanophysics.pl
traceroute to nanophysics.pl (88.198.20.90), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  4.258 ms  4.290 ms  4.285 ms
 2  * * *
 3  brt1.ostnet.pl (62.133.128.1)  221.944 ms  222.174 ms  222.874 ms
 4  88.220.127.221 (88.220.127.221)  41.110 ms  41.131 ms  45.178 ms
 5  213.172.188.49 (213.172.188.49)  54.368 ms  56.807 ms  59.298 ms
 6  init7.plix.pl (195.182.218.171)  60.477 ms  36.582 ms  38.806 ms
 7  r1nue1.core.init7.net (77.109.140.30)  58.557 ms  58.637 ms  61.187 ms
 8  gw-hetzner.init7.net (77.109.135.102)  113.689 ms  62.572 ms  106.019 ms
 9  core11.hetzner.de (213.239.203.137)  60.554 ms  62.135 ms  54.977 ms
10  core22.hetzner.de (213.239.245.226)  57.397 ms  56.136 ms  58.359 ms
11  juniper2.rz13.hetzner.de (213.239.245.122)  58.384 ms juniper1.rz13.hetzner.de (213.239.245.82)  64.350
ms  61.545 ms
12  hos-tr4.ex3k3.rz13.hetzner.de (213.239.224.100)  57.016 ms hos-tr3.ex3k3.rz13.hetzner.de
(213.239.224.68)  57.699 ms hos-tr1.ex3k3.rz13.hetzner.de (213.239.224.4)  57.977 ms
13  * * *
...
```

whois

zbych@orion:~$ whois nanophysics.pl

```
DOMAIN NAME:          nanophysics.pl
registrant type:      individual
nameservers:          dns7.linuxpl.com.   ns7.linuxpl.com.
created:              2014.09.01 18:42:17
last modified:        2014.09.01 18:42:24
renewal date:         2015.09.01 18:42:17
no option
dnssec:               Unsigned

REGISTRAR:
Consulting Service Sp. z o.o.
ul. Domaniewska 35A lok.1B
02-672 Warszawa
Polska/Poland
+48.22 8538888
domeny@ConsultingService.pl
```

dig

zbych@orion:~$ dig nanophysics.pl

```
; <<>> DiG 9.9.5-3-Ubuntu <<>> nanophysics.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23377
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
nanophysics.pl.         14400 IN      A       88.198.20.90

;; AUTHORITY SECTION:
nanophysics.pl.         14400 IN      NS      ns7.linuxpl.com.
nanophysics.pl.         14400 IN      NS      dns7.linuxpl.com.

;; ADDITIONAL SECTION:
ns7.linuxpl.com.    4446  IN      A       88.198.69.134
dns7.linuxpl.com.   4446  IN      A       88.198.23.35

;; Query time: 70 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Nov 02 16:05:51 CET 2014
;; MSG SIZE  rcvd: 139
```

Ping (służy do diagnozowania połączeń sieciowych)

zbych@orion:~$ ping nanophysics.pl

```
PING nanophysics.pl (88.198.20.90) 56(84) bytes of data.
64 bytes from server.second.vdl.pl (88.198.20.90): icmp_seq=1 ttl=53 time=64.1 ms
64 bytes from server.second.vdl.pl (88.198.20.90): icmp_seq=2 ttl=53 time=66.1 ms
64 bytes from server.second.vdl.pl (88.198.20.90): icmp_seq=3 ttl=53 time=64.1 ms
^C
--- nanophysics.pl ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 64.114/64.821/66.197/0.973 ms
```

HTTP (HyperText Transfer Protocol)

```
zbych@orion:~$ telnet nanophysics.pl 80
Trying 88.198.20.90...
Connected to nanophysics.pl.
Escape character is '^]'.
GET / HTTP/1.1
host: nanophysics.pl

HTTP/1.1 200 OK
Date: Mon, 03 Nov 2014 15:24:50 GMT
Server: Apache
Vary: Accept-Encoding,User-Agent
Transfer-Encoding: chunked
Content-Type: text/html

1259

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3c.org/TR/1999/REC-html401-
19991224/loose.dtd">
...
<p class="text">Nanophysics is just physics but at micro- and nano-scale. Surprisingly or not it is observed that at
these subscales compared to our everyday life experience new physical phenomena are found, that are not known or
are insignificant ar macro-scale. </P>
...
</body></html>

0

Connection closed by foreign host.
```

SMTP (Simple Mail Transfer Protocol)

telnet: > telnet mx1.example.com smtp
telnet: Trying 192.0.2.2...
telnet: Connected to mx1.example.com.
telnet: Escape character is '^]'.
server: 220 mx1.example.com ESMTP server ready Tue, 20 Jan 2004 22:33:36 +0200
client: HELO client.example.com
server: 250 mx1.example.com
client: MAIL from: <sender@example.com>
server: 250 Sender <sender@example.com> Ok
client: RCPT to: <recipient@example.com>
server: 250 Recipient <recipient@example.com> Ok
client: DATA
server: 354 Ok Send data ending with <CRLF>.<CRLF>
client: From: sender@example.com
client: To: recipient@example.com
client: Subject: Test message
client:
client: This is a test message.
client: .
server: 250 Message received: 20040120203404.CCCC18555.mx1.example.com@client.example.com
client: QUIT
server: 221 mx1.example.com ESMTP server closing connection

Kryptografia

– przekazywanie informacji w sposób zabezpieczony przed niepowołanym dostępem:

- hasła komputerowe, karty bankowe, handel elektroniczny

- wojsko, szpiedzy, dyplomacja

Kryptografia w komputerze? https, ssh, pgp (ale i mnóstwo innych sposobów o których nawet nie zdajemy sobie sprawy)

Kryptografia

Najstarsze sposoby:

- przestawianie lub podstawianie w tekście znaków lub słów. Np. Używamy następnej w alfabecie litery:

Kryptografia →Lszruphsbgjb ← sposób prosty, dawniej czasem użyteczny, ale do komunikacji komputerowej nie nadaje się zupełnie. Dlaczego?

- komputer jest w stanie odszyfrować tak proste schematy szyfrowania “natychmiast”

- hasła komputerowe: powinne być długie (>8 znaków), przypadkowe, składać się z wszelkich możliwych znaków

Kryptografia: PGP – pretty good privacy

- służy do ukrycia przesyłanej informacji przed osobami trzecimi
- może służyć jako podpis elektroniczny (uwierzytelnienie)

Użytkownicy generują dwa klucze elektroniczne: prywatny i publiczny;
wymieniają się kluczami publicznymi.

Nadawca szyfruje wiadomość własnym kluczem prywatnym i publicznym kluczem odbiorcy.
Odbiorca odczytuje wiadomość własnym kluczem prywatnym I kluczem publicznym nadawcy.

Kryptografia: PGP – pretty good privacy

PGP można używać do korespondencji email.

Klucz własny uwierzytelniamy na spotkaniu z osobą, która już posiada klucz PGP: organizowane są nawet spotkania grupowe przy piwie i kiełbaskach służace temu. Wymagane jest przedstawienie dowodu tożsamości.

Dlaczego metoda stosowana szeroko nie jest?
- jest niewygodna
- władzom nie zależy na ochronie prywatności korespondencji, gdyż … utrudniałoby to inwigilację!

Kryptografia: HTTPS

Jest odmianą metody PGP.

Generacja kluczy odbywa się automatycznie na komputerze użytkownika w czasie sesji https

Na serwerze istnieje fizycznie certyfikat bezpieczeństwa, zwykle podpisany przez bank lub inną instytucję upoważnioną

W przeglądarce internetowej są zainstalowane klucze publiczne najczęściej używanych instytucji wydających uwierzytelnienia kluczy.

Certyfikat może utworzyć administrator serwera, ale nieuwierzytelniony.

Certyfikat zawsze posiada ograniczony termin ważności.

Kryptografia: SSH

Jest odmianą metody PGP.

Służy do szyfrowanej komunikacji z okna terminala z odległym komputerem (na Windows można korzystać z PuTTy).

Przykład klucza publicznego:

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCcTfthH6CcQ9N74o6pZ0oxGZw
q9L2dQwdZQVgxDJlFvfXokTB4QygPHtR7rguunF/JTcGXCQ0OIah929VLRvE
T50R8U2VdnZlId+R5fNrMb+5TPT/XkppiKrjbqmaGssvCSs8LUMGJNaJlBtGS
b/hOkmsVDK1lKX9XeqPGOudY47OXZxaIz23ILu8ZHBpHj4c4+OGLNH3DrX
zkctUNcTAWdJCUWsx4bJA2AfHMWkV73gmi2fW/vTxxqvtyzzGQvu3OgilNok
q6KrVbFAqFLdMEL2HMZRqb75EwhG/xalc0fpAo65kxlNyjvu4bo0L9b3fGsOD
uR8+0xzh4OTXG2mND zbych@orion

Kryptografia: steganografia

Ukrywanie informacji w powszechnie dostępnym przekazie w sposób taki, iż domyśleć się tego może jedynie odbiorca, dla którego jest ona przeznaczona.

Np. Herodot opisuje przypadek niewolnika z tatuażem na głowie ukrytym pod włosami. Albo ukryjmy informacje w pliku muzycznym. Lub w obrazku...

Następne wykłady:

4. Systemy operacyjne.
- historia
- świat Unixów
- Windows
- Linux
- Linux z okna terminala. Przykłady. Web serwer.

5. Operacje na bitach. Grafika rastrowa a wektorowa.

6. Przetwarzanie tekstów. Formuły matematyczne w MS Word. LaTeX – historia i przykłady. Bazy danych. SQL. Arkusze kalkulacyjne.

7. BHP pracy z komputerem. Komputer a zdrowie. Prawa autorskie.