Politechnika Wrocławska

TCP/IP: DNS, protokoły, gniazda, IP v.6

wer. 39 z drobnymi modyfikacjami!

Wojciech Myszka

2023-04-20 12:04:08 +0200

HR EXCELLENCE IN RESEARCH

Część I

DNS

Domain Name System I

System Nazw Domenowych

1. *System Nazw Domenowych* (częściej Domain Name System, albo DNS) to rozproszona baza danych służąca do zarządzania konwersją adresów IP na (bardziej) czytelne dla ludzi nazwy symboliczne.
2. Kiedyś, gdy tego systemu nie było (to znaczy przed rokiem 1985) wykorzystywano pliki tekstowe do łączenia nazw symbolicznych komputerów z ich adresami IP.
   - Unix and co.: `/etc/hosts`
   - Windows: `%SystemRoot%\System32\drivers\etc\hosts`
   - Apple Macintosh: `/etc/hosts`
3. Jest to całkiem złożony system informatyczny (i bardzo złożony system prawny).

Domain Name System II

System Nazw Domenowych

- z jednej strony wykorzystywany jest do nadawania „osobowości internetowej" nowym podmiotom pojawiającym się w sieci,
- z drugiej — nieodzowny fragment infrastruktury internetu zapewniający realizację usług różnych protokołów najwyższej warstwy.

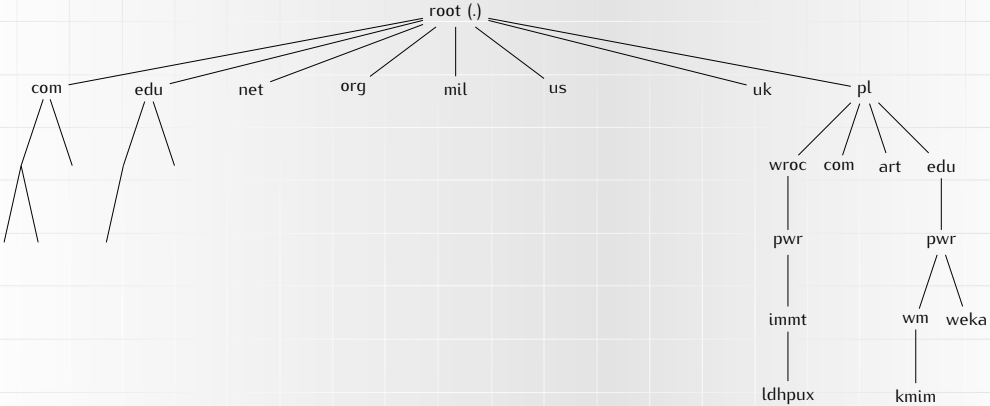
4. Nazwy domenowe tworzą strukturę drzewiastą:
   - korzeniem drzewa jest domena główna *root* oznaczana jako . (kropka)
   - kolejne człony nazw (o długości do 63 znaków każdy), oddzielane są kropkami,
   - domena to poddrzewo hierarchii obejmujące szereg pod-domen o wspólnym przyrostku: **com.pl**, **edu.pl**, **wroc.pl**, **net.pl**, **art.pl**,...

Domain Name System III

System Nazw Domenowych

- nazwy domen mogą zawierć znaki, cyfry i znak minus (kiedyś sugerowano, że nazwa domeny powinna zaczynać się od litery, ale okazało się, że sytuacja, gdy zaczyna się od cyfry nie stanowi żadnego problemu,
- od pewnego czasu można używać nie tylko znaków ASCII, ale również znaków Unicode, ale z różnych, praktycznych względów adresy takie są rzadko stosowane. Choć korzysta z tego bardzo chętnie Wikipedia

DNS



Rysunek: Uproszczony schemat fragmentu drzewa DNS

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

. — nazwa domeny (kropka: domena główna)

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

```
dig soa .
```

```
. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000
1800 900 604800 86400
```

6900 — czas ważności **tego** rekordu

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

```
dig soa .
```

```
. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000
1800 900 604800 86400
```

IN SOA — oznaczenie rekordu Start of Authority

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

```
dig soa .
```

```
. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400
```

a.root-servers.net. — adres serwera głównego (kropka na końcu oznacza pełny adres, bez kropki może być on jeszcze rozszerzany)

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

nstld.verisign-grs.com. — adres odpowiedzialnego (pierwszą kropkę zamieniamy na znak @, ostatnią usuwamy)

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

2023042000 — numer seryjny rekordu

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

1800 — okres odświeżania

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

900 — okres powtarzania (gdy nie uda się odświeżyć)

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

dig soa .

. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000 1800 900 604800 86400

604800 — okres ważności (w sekundach, tydzień)

Serwery DNS

- Z każdą nazwą domenową związany jest serwer przechowujący wszystkie informacje o domenie:
  - adres e-mail osoby odpowiedzialnej,
  - adresy serwerów zapasowych,
  - okres ważności informacji oraz okres odświeżania informacji przez serwery zapasowe,
  - numer seryjny domeny.

,

```
dig soa .
```

```
. 6900 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023042000
1800 900 604800 86400
```

86400 — minimalny okres ważności rekordu (gdy nie podano inaczej, w tym wypadku doba)

Politechnika Wrocławska

dig ns

dig ns .

```
. 83939 IN NS a.root-servers.net.
. 83939 IN NS b.root-servers.net.
. 83939 IN NS c.root-servers.net.
. 83939 IN NS d.root-servers.net.
. 83939 IN NS e.root-servers.net.
. 83939 IN NS f.root-servers.net.
. 83939 IN NS g.root-servers.net.
. 83939 IN NS h.root-servers.net.
. 83939 IN NS i.root-servers.net.
. 83939 IN NS j.root-servers.net.
. 83939 IN NS k.root-servers.net.
. 83939 IN NS l.root-servers.net.
. 83939 IN NS m.root-servers.net.
```

Politechnika Wrocławska

Liczba występująca po nazwie domeny oznacza pozostały okres ważności tej informacji, po przekroczeniu jego — informacja jest kasowana z pamięci podręcznej.

dig ns immt.pwr.wroc.pl

```
immt.pwr.wroc.pl. 86400 IN NS sun2.pwr.wroc.pl.
immt.pwr.wroc.pl. 86400 IN NS ldhpux.immt.pwr.wroc.pl.
immt.pwr.wroc.pl. 86400 IN NS dns1.pwr.wroc.pl.
immt.pwr.wroc.pl. 86400 IN NS dns2.pwr.wroc.pl.
immt.pwr.wroc.pl. 86400 IN NS temisto.immt.pwr.wroc.pl.
```

Rozwiązywanie adresów I

1. Baza danych ma strukturę hierarchiczną
2. Wystarczy znać adres któregokolwiek serwera root, żeby zacząć rozwiązywać adresy.
   Załóżmy, że interesuje mnie numeryczna wartość adresu `ldhpux.immt.pwr.wroc.pl`. Pytam o to serwera głównego.

dig @l.root-servers.net. ldhpux.immt.pwr.wroc.pl

```
;; AUTHORITY SECTION:
pl. 172800 IN NS a-dns.pl.
pl. 172800 IN NS b-dns.pl.
pl. 172800 IN NS c-dns.pl.
...
```

Politechnika Wrocławska

Rozwiązywanie adresów II

dig @a-dns.pl. ldhpux.immt.pwr.wroc.pl

```
;; AUTHORITY SECTION:
wroc.pl. 86400 IN NS bilbo.nask.org.pl.
wroc.pl. 86400 IN NS wask.wask.wroc.pl.
wroc.pl. 86400 IN NS ldhpux.immt.pwr.wroc.pl.
wroc.pl. 86400 IN NS ns1.net.icm.edu.pl.
wroc.pl. 86400 IN NS sun2.pwr.wroc.pl.
wroc.pl. 86400 IN NS kirdan.nask.net.pl.
```

Rozwiązywanie adresów III

dig @bilbo.nask.org.pl. ldhpux.immt.pwr.wroc.pl

```
;; AUTHORITY SECTION:
pwr.wroc.pl. 10800 IN NS sun2.pwr.wroc.pl.
pwr.wroc.pl. 10800 IN NS dns2.pwr.wroc.pl.
pwr.wroc.pl. 10800 IN NS dns.pwr.wroc.pl.
pwr.wroc.pl. 10800 IN NS wask.wask.wroc.pl.
pwr.wroc.pl. 10800 IN NS ns2.net.icm.edu.pl.
pwr.wroc.pl. 10800 IN NS ns1.net.icm.edu.pl.
```

Rozwiązywanie adresów IV

dig @ns2.net.icm.edu.pl. ldhpux.immt.pwr.wroc.pl

```
;; AUTHORITY SECTION:
immt.pwr.wroc.pl. 300 IN NS ldhpux.immt.pwr.wroc.pl.
immt.pwr.wroc.pl. 300 IN NS sun2.pwr.wroc.pl.
immt.pwr.wroc.pl. 300 IN NS dns2.pwr.wroc.pl.
```

dig @sun2.pwr.wroc.pl. ldhpux.immt.pwr.wroc.pl

```
;; ANSWER SECTION:
ldhpux.immt.pwr.wroc.pl. 259200 IN A 156.17.8.1
```

3. Proces przeprowadziłem ręcznie, ale normalnie odbywa się on automatycznie.

Rozwiązywanie adresów V

4. Każdy komputer (na ogół) ma pamięć podręczną, w której przechowuje „zdobyte” dotychczas informacje. Przyśpiesza to proces rozwiązywania adresów.
   Z drugiej strony jeżeli jakaś informacja jest w pamięci podręcznej (i jest błędna)...
5. Przed opracowaniem systemu rozproszonej bazy danych używano pliku. Nazywa się on `hosts` i znajduje się w kartotece `/etc/`.
6. Jest on obecny również w systemie Windows: `%SystemRoot%\System32\drivers\etc\hosts`.

Politechnika Wrocławska

Adresy „odwrotne”

- Wcześniej opisałem sposób translacji adresu symbolicznego na adres numeryczny.
- Istnieje równiez procedura odwrotna — translacji adresu numerycznego na symboliczny,
- W tym celu utworzno „sztuczną” domenę `in-addr.arpa`.
- Jej poddomeny to kolejne części numeryczne adresu IP w kolejnosci **odwrotnej**.
- Chcąc uzyskać nazwę internetową węzła o adresie numerycznym 156.17.8.1 odpytujemy o `1.8.17.156.in-addr.arpa`.

```
nslookup 156.17.8.1
1.8.17.156.in-addr.arpa name = ldhpux.immt.pwr.wroc.pl.
```

Albo inaczej

```
dig -x 156.17.8.1
;; ANSWER SECTION:
1.8.17.156.in-addr.arpa. 86400 IN PTR ldhpux.immt.pwr.wroc.pl.
```

Sekcja 3

Protokoły, porty i gniazdka

Politechnika Wrocławska

Porty

- Jednym z bardzo ważnych zadań stosu sieciowego jest zapewnienie dostarczania przekazywanych przez sieć informacji do właściwych aplikacji.
- Jest tylko jedno[1] gniazdko sieciowe oraz wiele aplikacji i wielu użytkowników z niego korzystających.
- Zapewniają to dodatkowe informacje przesyłane z każdym pakietem. Są to:
  - deklaracja protokołu (TCP, UDP,...),
  - gniazdo (*socket*),
  - port,
  - adresy IP (źródłowy i docelowy).

[1] Mnóstwo zastrzeżeń tu!

Politechnika Wrocławska

Kilka definicji (1)

Definicja (Port protokołu)

Port (protokołu) to szesnastobitowa liczba całkowita bez znaku używana w komunikacji sieciowej do definicji procesu z niego korzystającego.
Porty dzielą się na:

- ogólnie znane (*well known*) (liczby z zakresu od 0 do 1023), oraz
- dynamiczne (przydzielane w miarę potrzeby).

Port jest jednym z atrybutów gniazda.

Porty ogólnie znane...

...to porty, pod którymi nasłuchują najważniejsze usługi sieci Internet:

80	serwery WWW (protokól http),
443	serwery WWW (protokół https),
25	serwery SMTP (poczty elektronicznej)
20, 21	ftp
53	Domain Name System
631	drukarki (IPP)
143, 993	IMAP (poczta elektroniczna — klient)

Plik `/etc/services` zawiera większość definicji portów i związanych z nimi usług.

Wiele z portów ma identyczne znaczenie dla protokołu TCP i UDP (usługi mogą być dostępne w obu protokołach).

Przydziałem numerów portów zajmuje się IANA (http://www.iana.org/assignments/port-numbers)

Kilka definicji (2)

Definicja (Gniazdo)

Gniazdo to abstrakcyjny dwukierunkowy punkt końcowy połączenia. Dwukierunkowość oznacza, że można dane odbierać i wysyłać. Podstawowe atrybuty gniazda:

- typ gniazda (protokół przesyłu informacji),
- lokalny adres (na przykład IP, Ethernet,...),
- opcjonalnie lokalny numer portu definiujący proces wymieniający dane przez gniazdo.

Dodatkowo może to być:

- zdalny adres,
- opcjonalnie zdalny numer portu definiujący zdalny proces z niego korzystający.

Politechnika Wrocławska

Plik /etc/protocols zawiera zakodowane numerycznie nazwy protokołów:

```
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers
# and other sources.

ip      0       IP              # internet protocol, pseudo protocol number
hopopt  0       HOPOPT          # IPv6 Hop-by-Hop Option [RFC1883]
icmp    1       ICMP            # internet control message protocol
igmp    2       IGMP            # Internet Group Management
ggp     3       GGP             # gateway-gateway protocol
ipencap 4       IP-ENCAP        # IP encapsulated in IP (officially ‘‘IP’’)
st      5       ST              # ST datagram mode
tcp     6       TCP             # transmission control protocol
egp     8       EGP             # exterior gateway protocol
igp     9       IGP             # any private interior gateway (Cisco)
pup     12      PUP             # PARC universal packet protocol
udp     17      UDP             # user datagram protocol
hmp     20      HMP             # host monitoring protocol
```

Przykład I

Poniżej dosyć długi przykład opisujący (w przybliżeniu) co się dzieje podczas komunikacji.

1. Uruchamiamy przeglądarkę i wpisujemy adres strony: `http://pwr.edu.pl/`.
2. Otwierany jest port do komunikacji (system operacyjny tworzy go i nadaje mu numer), na przykład 35898.
3. Przeglądarka z całego adresu wydobywa adres serwera (wszystko to co jest za dwiema ukośnymi kreskami, a przed jedną ukośną) i wysyła do serwera (czyli pod adres pwr.edu.pl) zapytanie, które wygląda jakoś tak:

```
GET / HTTP/1.1
Host: pwr.edu.pl
```

Przykład II

(powyższe, to są dane informacje wysyłane do serwera).
Wszystko odbywa się w warstwie aplikacji.

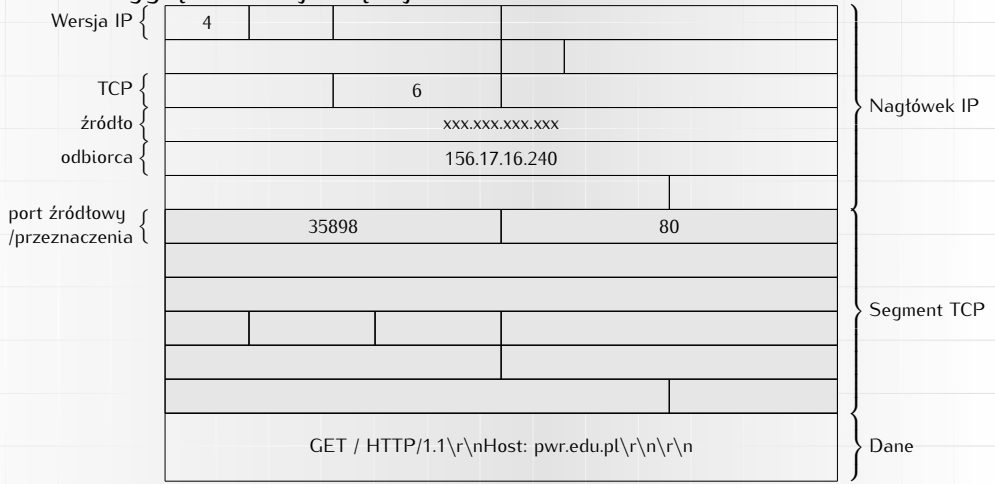
4. Najpierw dokonywana jest translacja adresu symbolicznego (pwr.edu.pl) na adres numeryczny (156.17.16.240)
5. Sprawdzane jest, czy adres znajduje się w „naszej” sieci (NIE).
6. Ustalany jest adres IP najlepszej bramy.
7. Ustalany jest adres fizyczny bramy (ARP).

Przykład III

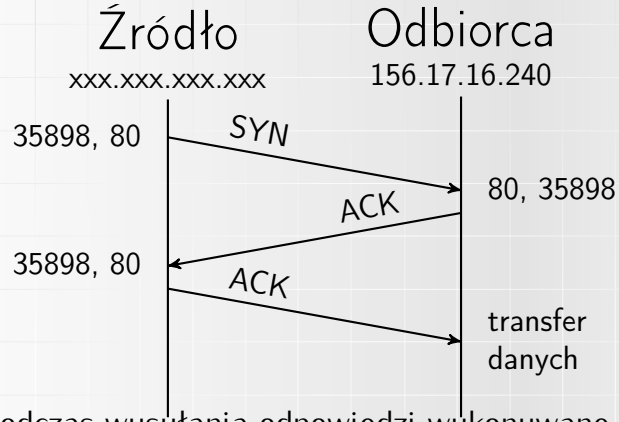
8. Wysyłany jest pakiet otwierający połączenie TCP (SYN) ze zdalnym serwerem WWW, ale wysyłany jest on do lokalnego węzła pełniącego rolę bramy. Kolejne bramy będą w sposób przezroczysty przekazywały pakiet przepakowując go odpowiednio do użytego medium komunikacyjnego).
   Używany jest adres IP serwera WWW i numer portu docelowego 80 (WWW).

Przykład IV

Pakiet wygląda mniej, więcej tak:



Przykład V

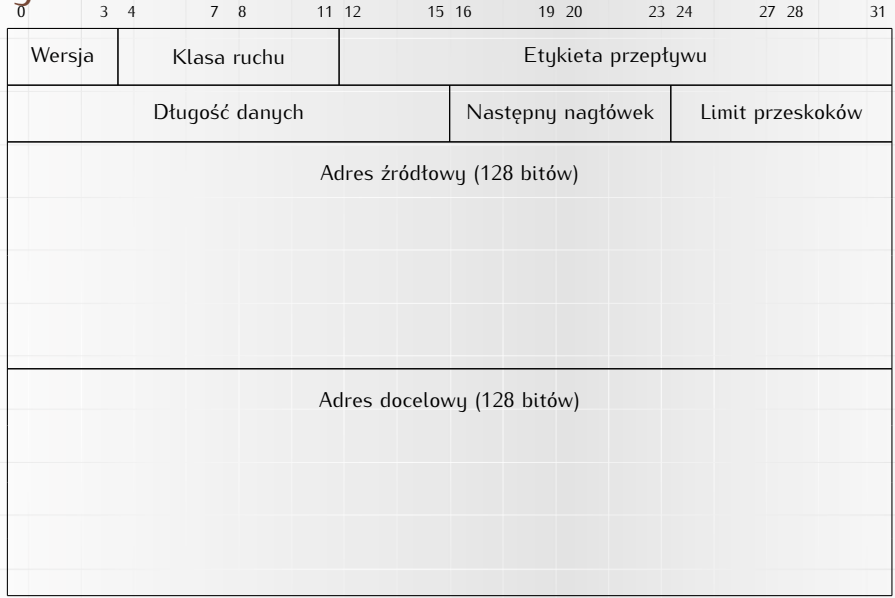


9. Podczas wysyłania odpowiedzi wykonywane są czynności podobne do tych opisanych w punktach 5, 6, 7.
(Serwer zazwyczaj korzysta z informacji zawartych w pamięci podręcznej.)

Część II

Internet Protocol v.6

Datagram IP ver. 6



Politechnika Wrocławska

Datagram IP ver. 6 I

- **Wersja** (4 bity) — definiująca wersję protokołu, w przypadku IPv6 pole to zawiera wartość 6 (bitowo 0110)
- **Klasa ruchu** (8 bitów) — określa sposób w jaki ma zostać potraktowany pakiet danych. W poprzedniej wersji protokołu pole to nazywało się **Type of Service**, jednak ze względu na to, że w IPv6 stosowane są inne mechanizmy priorytetowania danych, nazwę tego pola zmieniono
- **Etykieta przepływu** (20 bitów) — pomagające odróżnić pakiety, które wymagają takiego samego traktowania (ich pole klasy ruchu ma tę samą wartość)
- **Długość danych** (16 bitów) — wielkość pakietu, nie wliczając długości podstawowego nagłówka (wliczając jednak nagłówki rozszerzające)

Datagram IP ver. 6 II

- **Następny nagłówek** (8 bitów) — identyfikuje typ następnego nagłówka, pozwalając określić czy jest to nagłówek rozszerzający czy nagłówek warstwy wyższej. W przypadku tego drugiego, wartość pola jest identyczna z wartością pola w protokole IPv4
- **Limit przeskoków** (8 bitów) — określa ilość węzłów, po odwiedzeniu których pakiet zostaje porzucony. W poprzedniej wersji protokołu pole to nosiło nazwę time to live i zawierało liczbę skoków, która była zmniejszana przez każdy odwiedzony węzeł
- **Adres źródłowy** (128 bitów) — adres węzła, który wysłał pakiet
- **Adres docelowy** (128 bitów) — adres węzła do którego adresowany jest pakiet

Politechnika Wrocławska

Adresy IPv6

- 128 bitów (340 282 366 920 938 463 463 374 607 431 768 211 456) $3{,}4028210^{38}$
- Adresy zapisywane są w postaci:
  `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` gdzie każdy znak x to cyfra szesnastkowa reprezentująca 4 bity adresu.
- W wersji tekstowej adresu może pojawić się (jeden raz) podwójny dwukropek `::`. Oznacza on ciągłe pole złożone z samych zer.
- Adres IPv6 mojego laptopa (w czasie pisania tych słów) to:
  2a02:a317:e341:6780:8be8:c8a:b8db:c349 albo
  `fe80::7ca9:2b76:d4b6:5a8c`

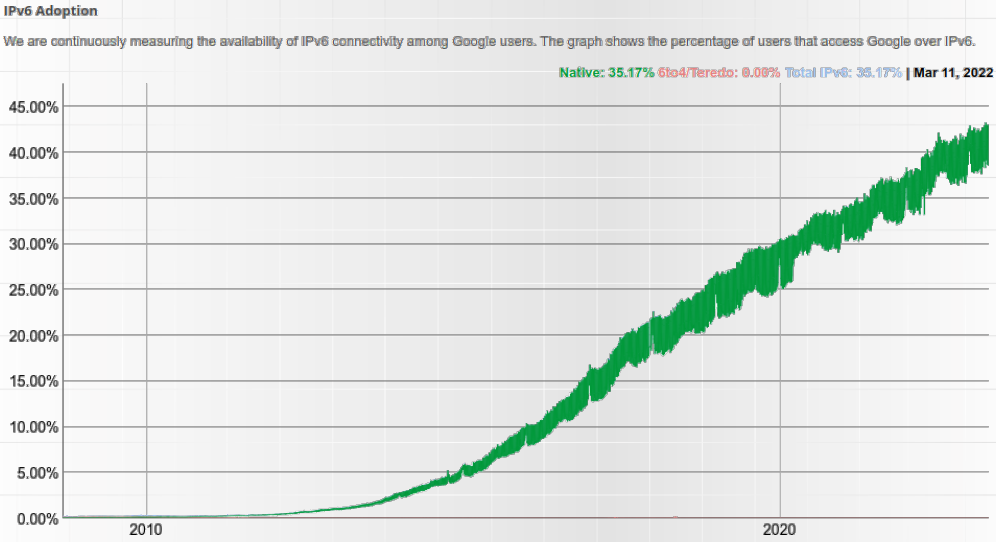
Politechnika Wrocławska

Najważniejsze różnice

- Liczba dostępnych adresów i różne tego konsekwencje:
  - własny adres IP dla (praktycznie) każdego sensownego gadżetu elektronicznego.
  - (teoretyczna) możliwość połączenia każdego węzła z każdym bez uciążliwych pośredników (typu NAT),
- Szyfrowanie w standardzie.
- Prostszy nagłówek IP.
- W IPv4 konfiguracja adrsu ręczna lub automatyczna (specjalne oprogramowanie zainstalowane w sieci) w przypadku IPv6 — ma się to odbywać „samoistnie” (ale prace są w początkowej fazie)

Politechnika Wrocławska

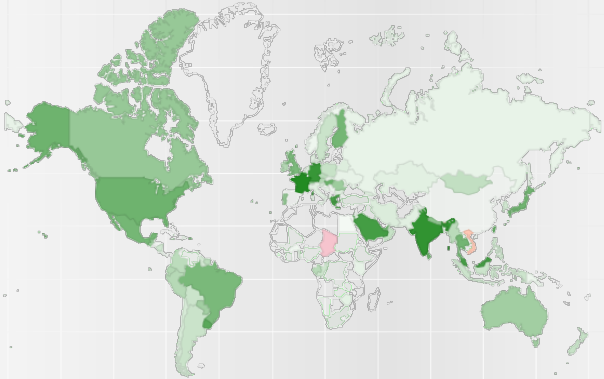
Zasięg IP v6



Politechnika Wrocławska

Zasięg IP v6 kraje

Per-Country IPv6 adoption



World | Africa | Asia | Europe | Oceania | North America | Central America | Caribbean | South America

The chart above shows the availability of IPv6 connectivity around the world.

- Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
- Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
- Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.

Część III

Przydział adresów IP

Przydział adresów IP

IP v4

1. Ręczna
2. Automatyczna — serwer DHCP.
   Na podstawie adresu MAC karty przydzielany jest adres IP o ograniczonym czasie ważności.
   Administrator sieci konfiguruje serwer DHCP.
3. Serwer DHCP może współpracować z serwerami DNS.

IP v6

1. Automatyczna.
   Podstawowym identyfikatorem komputera jest EUI64 tworzony automatycznie na podstawie adresu MAC karty sieciowej przez wstawienie w środek adresu MAC ciągu 0xFFFE i zanegowanie siódmego najstarszego bitu adresu. Ale generuje to przewidywalne adresy.
   Stąd zazwyczaj generowane są one inaczej.

W obu przypadkach mogą być również przydzielane adresu *link-local* z zakresu 169.254.0.0/16 (IPv4) i FE80::/10 (IPv6).

Adresy IP v6

1. „Górne” 64 bity ustalane są w sposób ułatwiający routing w sieci globalnej.
2. Dla WASK jest to 2001:a48::/32
3. Kolejne bity mogą być „standaryzowane” na potrzeby routingu wewnątrz organizacji.
4. Specjalna kategoria to adresy postaci: FE80::/10 (1111 1110 10). Są to, tak zwane *link local addresses* nieroutowalne adresy węzłów podłączonych do medium lokalnego. Przydzielane są one automatycznie. Pozwalają one na komunikację między komputerami podłączonymi do tego medium.

Routing w sieci Internet

Polecam stronę BGPView, zaczynając, na przykład, od Sieci WASK

Strona whois.ipip.net zawiera wiele interesujących informacji.

Pozwala zamienić adres IP na numer systemu autonomicznego: 156.17.8.1