



Wprowadzenie do systemu UNIX

Cz. 5:

Podstawy sieci komputerowych i rodziny protokołów TCP/IP

Krzysztof Boryczko

Krótką historia (1)

- 1957 r. - w strukturze Departamentu Obrony Stanów Zjednoczonych powstaje ARPA (Advanced Research Projects Agency). Głównym zadaniem jest opracowanie nowych technologii informacyjnych oraz adaptacja ich dla celów militarnych.
- 1962 r. - Paul Baran z Rand Corporation tworzy wraz z przyjaciółmi koncepcję sieci opartej na wymianie pakietów - informacja dzielona jest na mniejsze jednostki i partiami przesyłana między nadawcą i odbiorcą. Tzw. packet switching pozwala na wymianę informacji między różnymi maszynami przy użyciu tego samego kabla, gdyż każdy z pakietów zawiera m.in. adres docelowy, zapobiegając ewentualnemu zagubieniu. Sieć taka jest w stanie wytrzymać atak nuklearny, zniszczenie nawet kilku węzłów przy odpowiednim rozmiarze sieci spowoduje dynamiczne "dopasowanie się" do nowych warunków. Jak pokaże bieg wydarzeń, rozwiązanie takie okaże się również idealne dla modelu sieci cywilnej - Internetu, choć oczywiście nie takie były założenia.

Krótką historia (2)

- 1965r. - połączono dwa komputery w Massachusetts (MIT) i w Santa Monica - była to jeszcze sieć bez wymiany pakietów.
- 1967r. - Larry Roberts rozwinął w ARPA pomysł znany z Rand Corp. i w dwa lata później powstaje pierwszy węzeł sieci z wymianą pakietów na uniwersytecie w Los Angeles, do którego dołączają uniwersytety w Santa Barbara i Utah oraz Instytut Stanford. Sieć przyjmuje nazwę ARPANET i jest oparta o IMP (Information Message Processors) - minikomputery Honeywell 516 z 12 KB pamięci operacyjnej.
- 1969r. – początek historii Internetu. DARPA stworzyła pierwsze projekty połączenia ze sobą sieci lokalnych. Zapoczątkowała również badania nad stworzeniem protokołu sieci, czyli zbioru przepisów określających sposób obiegu informacji w sieci.
- Początek lat 80-tych - APARNET podzielił się na dwie odrębne sieci - ARPANET i Milnet (sieć wojskową), jednak zainstalowanie między nimi wielu połączeń pozwoliło kontynuować swobodną wymianę informacji. To połączenie DARPA nazwała Internetem.

Krótką historia (3)

- Również na początku lat 80-tych środowiskom naukowym i akademickim w całych Stanach udostępniono nieco bardziej zharmonizowane połączenia komputerowe - Computer Science Network (CSNET) i BITNET. Nie były one częścią Internetu, jednakże później stworzono specjalne pomosty (bramki) pozwalające na wymianę danych użytkownikowi tych sieci.
- 1982 r. - Amerykański Departament Obrony uznał, konstruowane od połowy lat 70-tych, protokoły TCP/IP za standard w całej sieci należącej do wojska. Prace nad nimi stanowiły część projektu, którego celem było stworzenie odpornej na atak sieci komputerowej.
- 1986 r. – stworzono sieć NFSNET.
- 1990 r. – sieć NFSNET wyparła ARPANET. Ta ostatnia została uroczyście wyłączona.

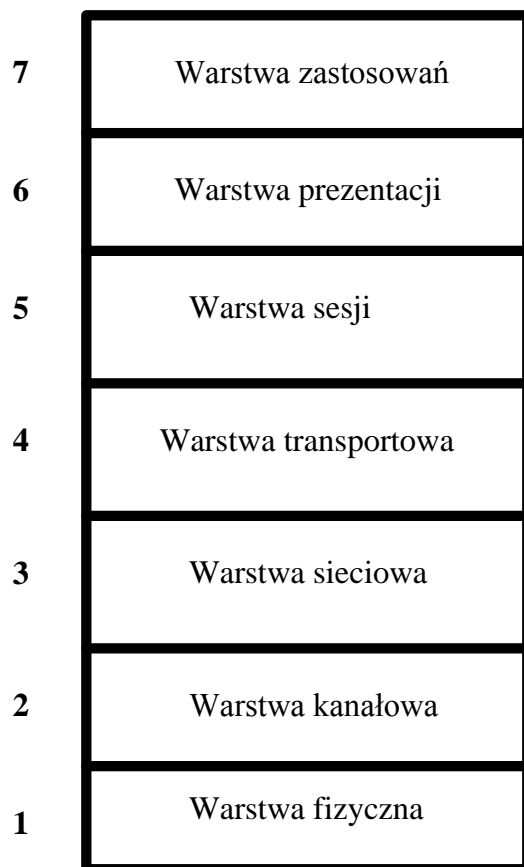
UNIX a sieci

- uucp (Unix-to-Unix copy program) – 1976, SV, program wsadowy do rozprowadzania oprogramowania. Komputery połączone bezpośrednio liniami telefonicznymi.
- cu – łączenie się z odległym systemem przy pomocy linii telefonicznych, 1978. SV.
- tip – odpowiednik cu w systemach 4.3BSD.
- Implementacja protoplasty poczty i usługi zdalnego drukowania na kampusie Uniwersytetu Kalifornijskiego w Berkeley, 1978, rs-232.
- Opracowanie na zlecenie DARPA rodziny protokołów TCP/IP, 1980.
- Opracowanie technologii Ethernet. Włączenie TCP/IP do BSD4.2, 1983.

Model ISO-OSI - idea

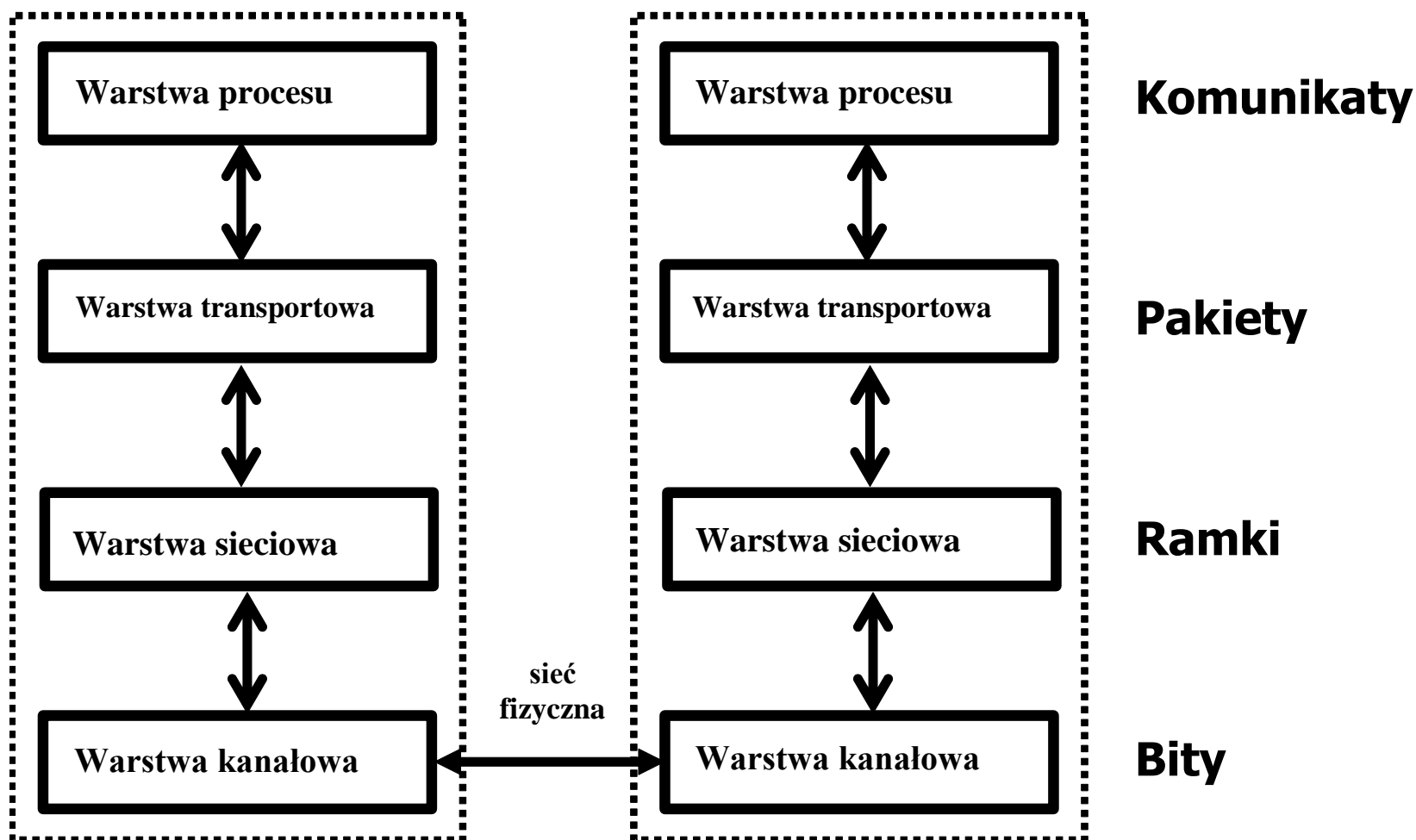
- Duża liczba rozwiązań sieciowych wprowadziła konieczność unifikacji.
- Międzynarodowa Organizacja ds. Standaryzacji wprowadziła model, który dzieli „aspekty” komunikacji sieciowej na warstwy.
- Idea polega na określeniu zadań poszczególnych warstw oraz standaryzacji interfejsów między warstwami, co ułatwia tworzenie aplikacji sieciowych.
- Zastosowanie się do modelu gwarantuje iż zaproponowane rozwiązania (sprzęt, oprogramowanie) będą mogły współpracować z rozwiązaniami innych producentów.

Warstwy modelu ISO-OSI



- Podstawowy model składa się z siedmiu warstw.
- Każda rodzina protokołów działających w sieci Internet wpisuje się w model.
- Do popularnych protokołów należy zaliczyć:
 - Rodzinę TCP/IP (DARPA)
 - Rodzinę XNS (Xerox)
 - Rodzinę SNA (IBM)

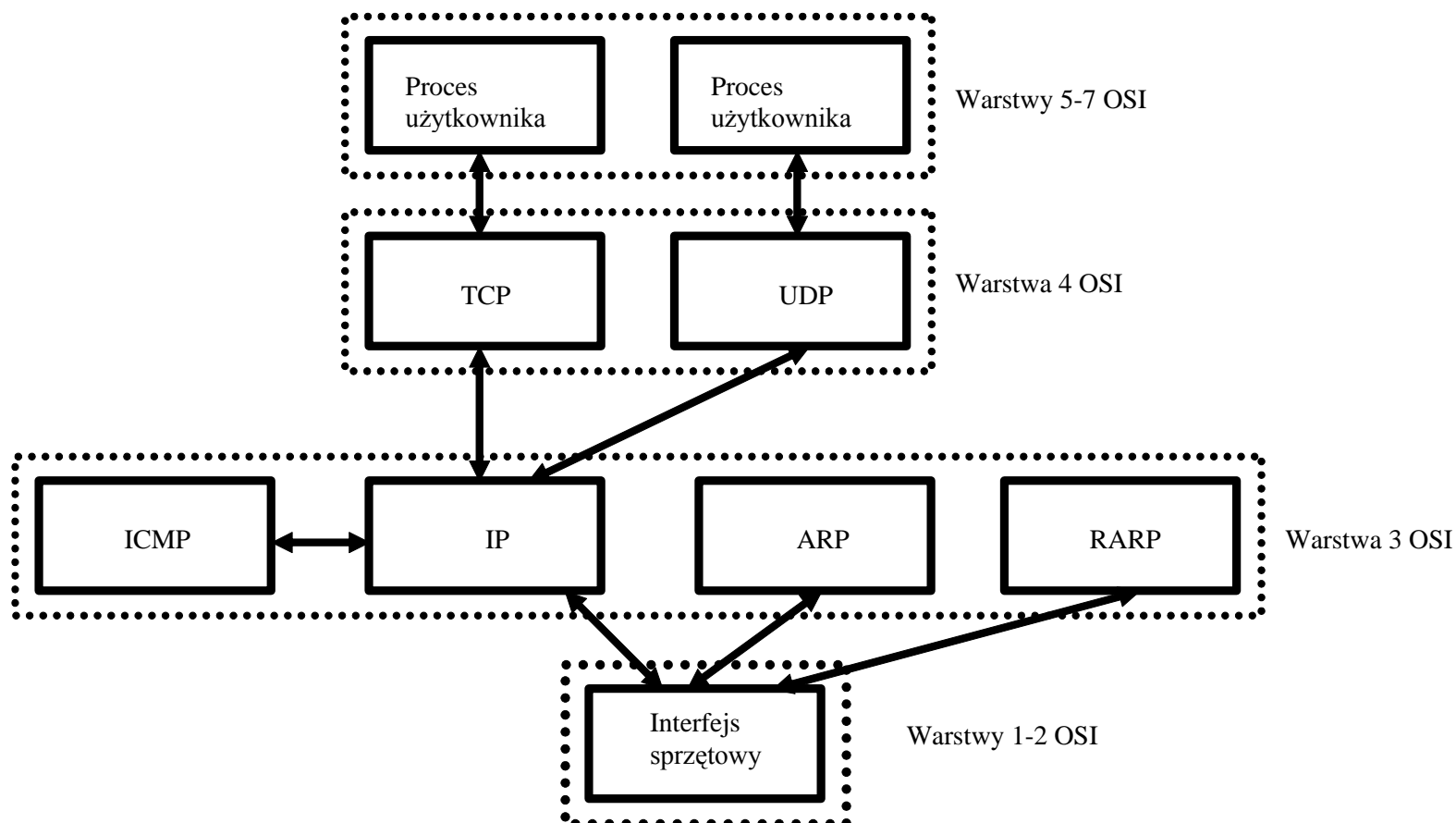
Uproszczony model ISO-OSI



Rodzina protokołów TCP/IP

- Najpopularniejsza w zastosowaniu w sieci Internet ze względu na otwartość kodu (nie jest rozwiązaniem komercyjnym).
- Łatwa w implementacji.
- Nie obciąża szczególnie pamięci operacyjnej systemu.

Rodzina protokołów TCP/IP w modelu ISO-OSI



Interfejs sprzętowy

- Tu odbywa się właściwa komunikacja na poziomie pojedynczych bitów.
- W warstwie tej zdefiniowane są parametry fizyczne transmisji takie jak właściwości medium transmisyjnego, poziomy oraz czasy trwania sygnałów, itd.
- W tej warstwie zdefiniowany jest adres sprzętowy (MAC), który jest przypisany do interfejsu:
 - Długość – 48 bitów.
 - Powinien być unikatowy w skali świata.
 - Producenci interfejsów dzielą pulę adresową między siebie.
 - Kupując interfejsy do komputerów sieci możemy być pewni, że przypisane im adresy nie będą tworzyły ciągłej przestrzeni adresowej – problemy w administrowaniu i konieczność znalezienia adresacji „lepszey” do administracji.

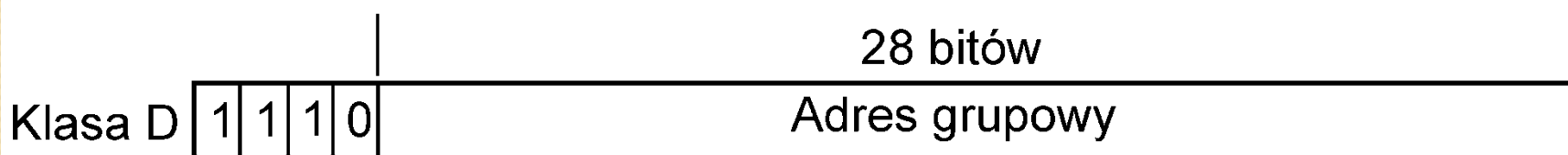
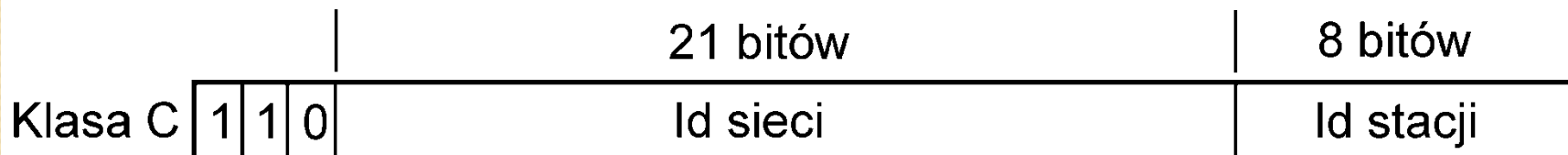
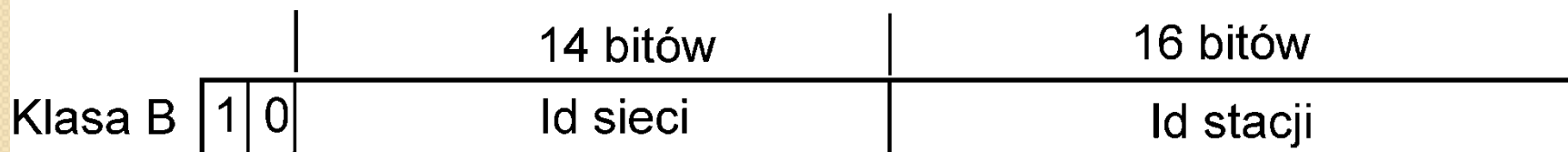
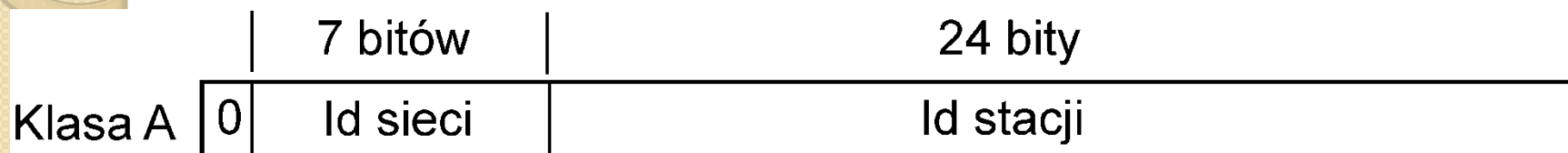
Warstwa Internetu

- W niej zdefiniowane są protokoły umożliwiające dostęp do Internetu:
- Protokół IP – zapewniający ciągłą adresację hostów oraz obsługę zaadresowanych ramek.
- Protokół ARP – pozwalający na znalezienie adresu MAC w oparciu o adres IP w celu fizycznego przesłania informacji.
- Protokół RARP – umożliwiający znalezienie adresu MAC na podstawie adresu IP.
- Protokół ICMP – protokół wykorzystywany w diagnostyce oraz trasowaniu.

Protokół IP v IV

- Nie posiadał mechanizmów bezpieczeństwa. Dopiero w wersji IPSec pojawił się nagłówek autentykacji (Authentication Header – AH) oraz szyfrowanie (Encapsulating Security Payload - ESP).
- Adres ma postać 4 bajtów oddzielonych kropkami, czyli 32 bitów.
- Adres składa się z części adresującej sieć i części adresującej hosta. Gdzie przebiega granica? Wstępny podział na klasy adresowe zakładał granice występujące na kropkach.

Adresy IP – klasy (przestarzałe)



Nowe mechanizmy adresacji w IP v IV

- Wyczerpywanie się puli adresowej IP v IV spowodowało konieczność poszukiwania bardziej oszczędnych mechanizmów gospodarowania nimi. Stąd:
 - Network Address Translation (NAT).
 - Tzw routing bezklasowy – wymagający podania maski podsieci wskazującej na granicę w adresie między częścią adresującą sieć i częścią adresującą hosta.
- Pula adresów klasy C jest już wyczerpana.

Adresy IP – routing bezklasowy

- Maska podsieci – ciąg jedynek i zer.
Np. 255.255.255.192
11111111.11111111.11111111.11000000
- Adres hosta:
Np. 147.132.90.72/26 (26 bitów maski)
10010011.10000100.01011010.01001000
10010011.10000100.01011010.01000000 sieć
10010011.10000100.01011010.01111111 bcast
147.132.90.64 – adres sieci
147.132.90.127 – adres rozgłoszeniowy

Przypisywanie adresów IP hostom

- Poleceniami: *ifconfig*, *route*
- Statycznie – polega na zdefiniowaniu atrybutów protokołu IP w plikach konfiguracyjnych. Niestety ich nazwy i format są różne w różnych dystrybucjach.

```
#RedHat linux
#/etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.3.127
IPADDR=192.168.3.116
NETMASK=255.255.255.128
NETWORK=192.168.3.0
ONBOOT=yes
```

```
#FreeBSD
#/etc/rc.conf
ifconfig_ed0="inet 192.168.1.116 netmask 255.255.255.128"
```

- Dynamicznie - z wykorzystaniem protokołu DHCP.

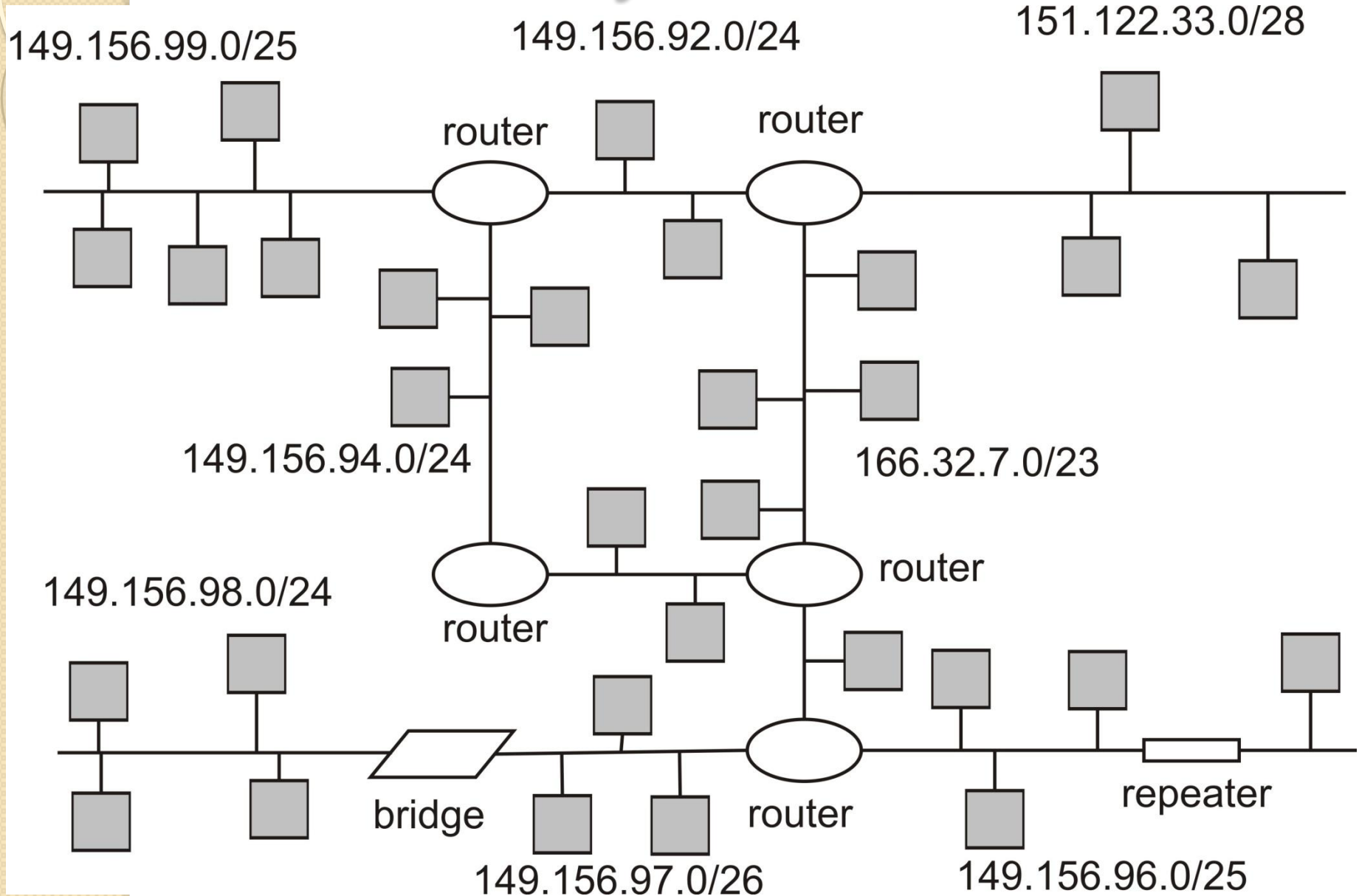
Protokół DHCP - podstawy

- Wymaga istnienia co najmniej jednego serwera DHCP w sieci lokalnej.
- Każdy serwer musi posiadać zdefiniowaną pulę adresów IP „do rozdania”. W przypadku kilku serwerów w jednej sieci ich pule muszą być rozłączne.
- Po stronie klienta wymagane jest jedynie zdefiniowanie tej metody przydzielania adresów.

Działanie protokołu DHCP

- Uzyskanie adresu IP składa się z 4 faz:
 1. DHCPDISCOVER – klient do wszystkich serwerów DHCP w sieci (co 2, 4, 8, 16 sec. 5 min) wysyła zapytanie.
 2. DHCPOFFER wszystkie serwery DHCP do klienta od którego otrzymały zapytanie z propozycją adresu.
 3. DHCPREQUEST – klient do wybranego serwera DHCP z informacją o wybraniu adresu.
 4. DHCPACK – serwer DHCP do klienta, któremu wydłuża adres ze swojej puli.
- Po upływie połowy czasu dzierżawy klient występuje o przedłużenie czasu dzierżawy.
- W przypadku braku odpowiedzi od serwera klient przydziela sobie adres z puli klasy B 169.254.0.0 z maską 255.255.0.0.

Przykład sieci



Trasowanie pakietów IP v IV

- Na podstawie jej zawartości podejmowana jest decyzja, w „którą stronę” kierowany jest pakiet.
- Znajduje się tablicy routowania systemu operacyjnego oraz w routerach łączących segmenty sieci.

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
149.156.99.0	0.0.0.0	255.255.255.128	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	149.156.99.17	0.0.0.0	UG	0	0	0	eth0

Śledzenie drogi pakietów (1)

C:\Program Files\Windows Resource Kits\Tools>ipconfig
Konfiguracja IP systemu Windows

Karta Ethernet Połączenie lokalne:

Sufiks DNS konkretnego połączenia : csg.agh.edu.pl
Adres IP. : 172.19.5.147
Maska podsieci. : 255.255.255.0
Brama domyślna. : 172.19.5.254

C:\Program Files\Windows Resource Kits\Tools>tracert 149.156.96.9

Trasa śledzenia do galaxy.agh.edu.pl [149.156.96.9]
przewyższa maksymalną liczbę przeskoków 30

1	<1 ms	<1 ms	<1 ms	172.19.5.254
2	<1 ms	<1 ms	<1 ms	149.156.119.58
3	7 ms	1 ms	<1 ms	149.156.119.57
4	<1 ms	<1 ms	<1 ms	marvin.uci.agh.edu.pl [149.156.96.134]
5	<1 ms	<1 ms	<1 ms	galaxy.agh.edu.pl [149.156.96.9]

Śledzenie zakończone.

Śledzenie drogi pakietów (2)

C:\Program Files\Windows Resource Kits\Tools>tracert 8.8.8.8

Trasa śledzenia do google-public-dns-a.google.com [8.8.8.8]
przewyższa maksymalną liczbę przeskoków 30

1	<1 ms	<1 ms	<1 ms	172.19.5.254
2	<1 ms	<1 ms	<1 ms	149.156.119.58
3	1 ms	<1 ms	1 ms	149.156.119.57
4	1 ms	3 ms	<1 ms	149.156.6.222
5	<1 ms	<1 ms	<1 ms	193.193.64.25
6	9 ms	9 ms	9 ms	z-krakowa.poznan-gw3.10Gb.rtr.pionier.gov.pl [212.191.224.69]
7	25 ms	25 ms	28 ms	dk-ore.nordu.net [109.105.98.49]
8	36 ms	65 ms	36 ms	nl-sar.nordu.net [109.105.97.25]
9	36 ms	36 ms	36 ms	core2.ams.net.google.com [195.69.145.100]
10	36 ms	36 ms	36 ms	209.85.254.90
11	38 ms	36 ms	85 ms	209.85.255.70
12	40 ms	40 ms	40 ms	216.239.49.38
13	*	*	*	Upłynął limit czasu żądania.
14	40 ms	40 ms	40 ms	google-public-dns-a.google.com [8.8.8.8]

Śledzenie zakończone.

IP v VI – podstawowe założenia

- Adres ma 128 bitów, z czego 3 pierwsze wykorzystywane są zarezerwowane do wskazania, że jest to adres klasy VI. Do dyspozycji mamy 125 bitów co daje ok. 10^{38} adresów.
- Wbudowane mechanizmy bezpieczeństwa – AH oraz ESP.
- Wdrażanie poprzez tworzenie sieci – „wysp” oraz ich łączenie. Technologia czasochłonna i kosztowna.

Warstwa transportowa

- Zawiera dwa protokoły:
 1. TCP (Transmission Control Protocol) – protokół połączeniowy. Przed przesłaniem pakietu zestawiany jest obwód wirtualny. Przesłanie pakietu wymaga potwierdzenia – jego brak implikuje kolejne próby przesłania. Protokół wolny, stosowany w sieciach rozległych.
 2. UDP (User Datagram Protocol) – protokół bezpołączeniowy. Przesyłane są datagramy, bez potwierdzenia i ew. retransmisji. Protokół szybki, ale stosowany w sieciach lokalnych.

Usługi i numery portów

- W sieci wykorzystywany jest model klient-serwer.
- Stroną czynną jest klient, który żąda od serwera udostępniania usług.
- Żądanie wysyłane do klienta jest parą adresu IP oraz numeru usługi.
- Usługi posiadają zdefiniowane numery.
- Serwer, aby rozpoznać połączenia z tego samego klienta nadaje im numer z przedziału 49152 do 65535.

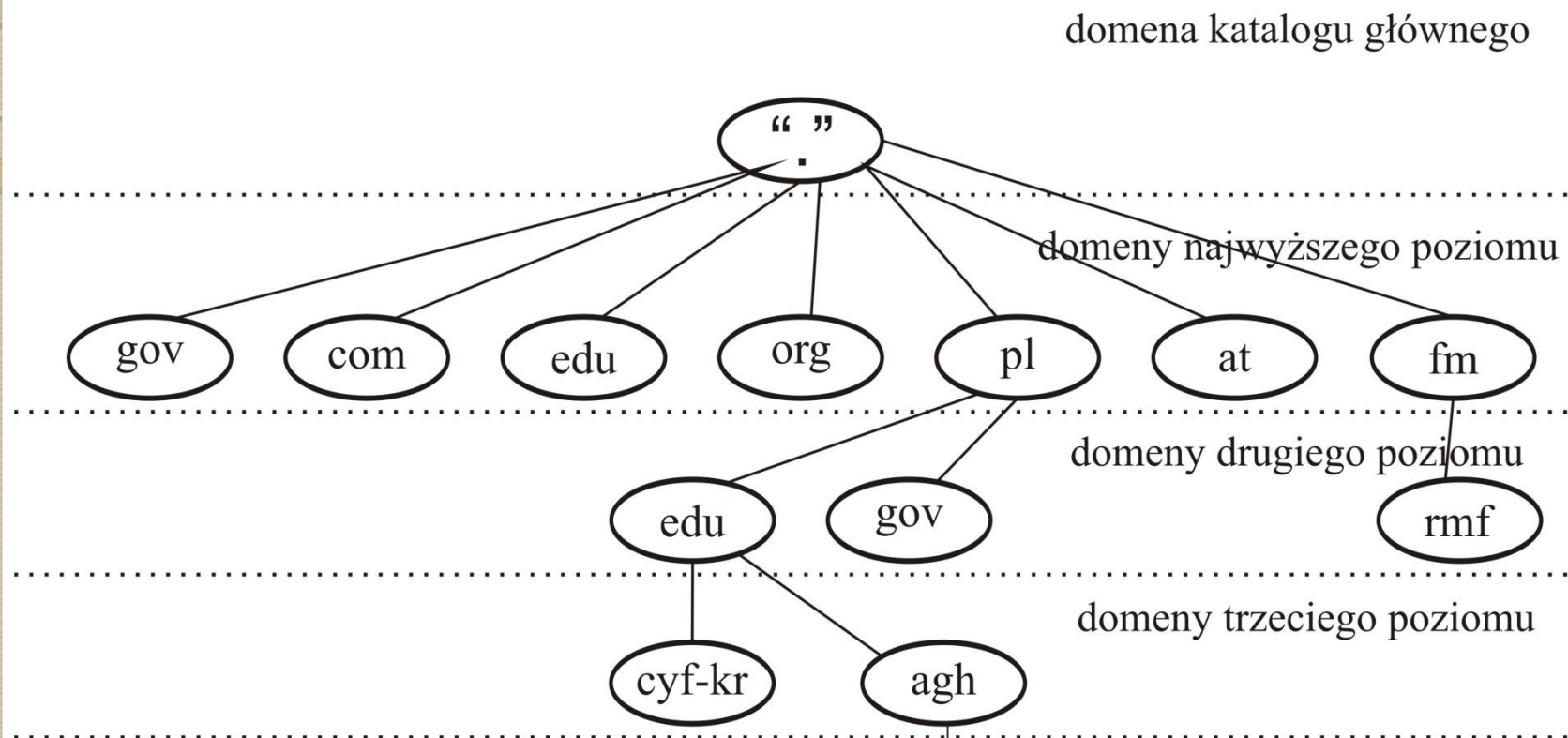
Plik /etc/services

```
#
# WELL KNOWN PORT NUMBERS
#
rtmp      1/ddp   #Routing Table Maintenance Protocol
tcpmux    1/tcp   #TCP Port Service Multiplexer
tcpmux    1/udp   #TCP Port Service Multiplexer
nbp       2/ddp   #Name Binding Protocol
compressnet 2/tcp   #Management Utility
compressnet 2/udp   #Management Utility
compressnet 3/tcp   #Compression Process
compressnet 3/udp   #Compression Process
echo      4/ddp   #AppleTalk Echo Protocol
rje       5/tcp   #Remote Job Entry
rje       5/udp   #Remote Job Entry
zip       6/ddp   #Zone Information Protocol
echo      7/tcp
echo      7/udp
discard   9/tcp   sink null
discard   9/udp   sink null
systat    11/tcp   users    #Active Users
systat    11/udp   users    #Active Users
daytime   13/tcp
daytime   13/udp
qotd      17/tcp   quote    #Quote of the Day
qotd      17/udp   quote    #Quote of the Day
msp       18/tcp   #Message Send Protocol
msp       18/udp   #Message Send Protocol
chargen   19/tcp   ttytst source #Character Generator
chargen   19/udp   ttytst source #Character Generator
ftp-data  20/tcp   #File Transfer [Default Data]
ftp-data  20/udp   #File Transfer [Default Data]
ftp       21/tcp   #File Transfer [Control]
ftp       21/udp   #File Transfer [Control]
ssh       22/tcp   #Secure Shell Login
ssh       22/udp   #Secure Shell Login
telnet    23/tcp
telnet    23/udp
#         24/tcp   any private mail system
#         24/udp   any private mail system
smtp      25/tcp   mail     #Simple Mail Transfer
smtp      25/udp   mail     #Simple Mail Transfer
```

Domain Name System

- Rozproszona baza danych używana w sieciach TCP/IP do tłumaczenia nazw komputerów na adresy IP (RFC 1034, RFC 1035).
- Przestrzeń nazw domeny jest schematem nazewniczym udostępniającym hierarchiczną strukturę dla bazy danych DNS.
- Baza danych DNS jest indeksowana po nazwie stąd każda domena musi mieć nazwę.
- Nazwa domeny określa jej pozycję w hierarchii.
- Nazwa domeny podrzędnej jest dodawana do nazwy jej domeny nadrzędnej (subdomeny).

Struktura przestrzeni nazw domeny



student.agh.edu.pl



Struktura hierarchiczna

- Domena katalogu głównego – znajduje się na szczycie i jest przedstawiana znakiem „.” (kropki). Zarządzana przez kilka organizacji (np. Network Solutions).
- Domeny najwyższego poziomu – dwu lub trzy literowe kody nazw wg typów organizacji lub położenia geograficznego (np. .gov, .mil, .at).
- Domeny drugiego poziomu – przyznawane przez organizacje na potrzeby organizacji i osób fizycznych. Mogą zawierać hosty oraz subdomeny.

Nazewnictwo domen

- Konieczność ograniczania liczby poziomów domen (3-4 poziomy).
- Nazwy unikalne, proste i strukturalne.
- Długość nazw domen do 63 znaków (z kropkami). Całkowita długość nazwy do 255 znaków.
- Stosuje się standardowe znaki DNS (A-Z a-z 0-9 -) (RFC 1035) oraz znaki Unicodu (RFC 2044).

Strefy

- Strefa reprezentuje nieciągłą część przestrzeni nazw domeny.
- Strefy umożliwiają podzielenie przestrzeni nazw domeny na łatwo zarządzane sekcje.
- Strefa musi obejmować ciągłą przestrzeń nazw domeny.
- Mapowanie nazw na adresy IP jest przechowywane w bazie danych strefy. Każda strefa jest zdefiniowana w określonej domenie.

/etc/hosts

- Plik zawiera adresy IP i nazwy najczęściej „odwiedzanych” hostów.
- Jest pierwszym miejscem, w którym poszukiwany jest adres IP. Jeśli zostanie on znaleziony, to poszukiwanie zostaje przerwane.
- Musi zawierać aktualne dane.
- Format: IP adres_symboliczny lista_aliasów

```
127.0.0.1 localhost.localdomain localhost
```

```
# Auto-generated hostname. Please do not remove this comment.
```

```
149.156.96.9 galaxy.agh.edu.pl galaxy galaxy
```

```
149.156.98.60 student.agh.edu.pl student stud
```

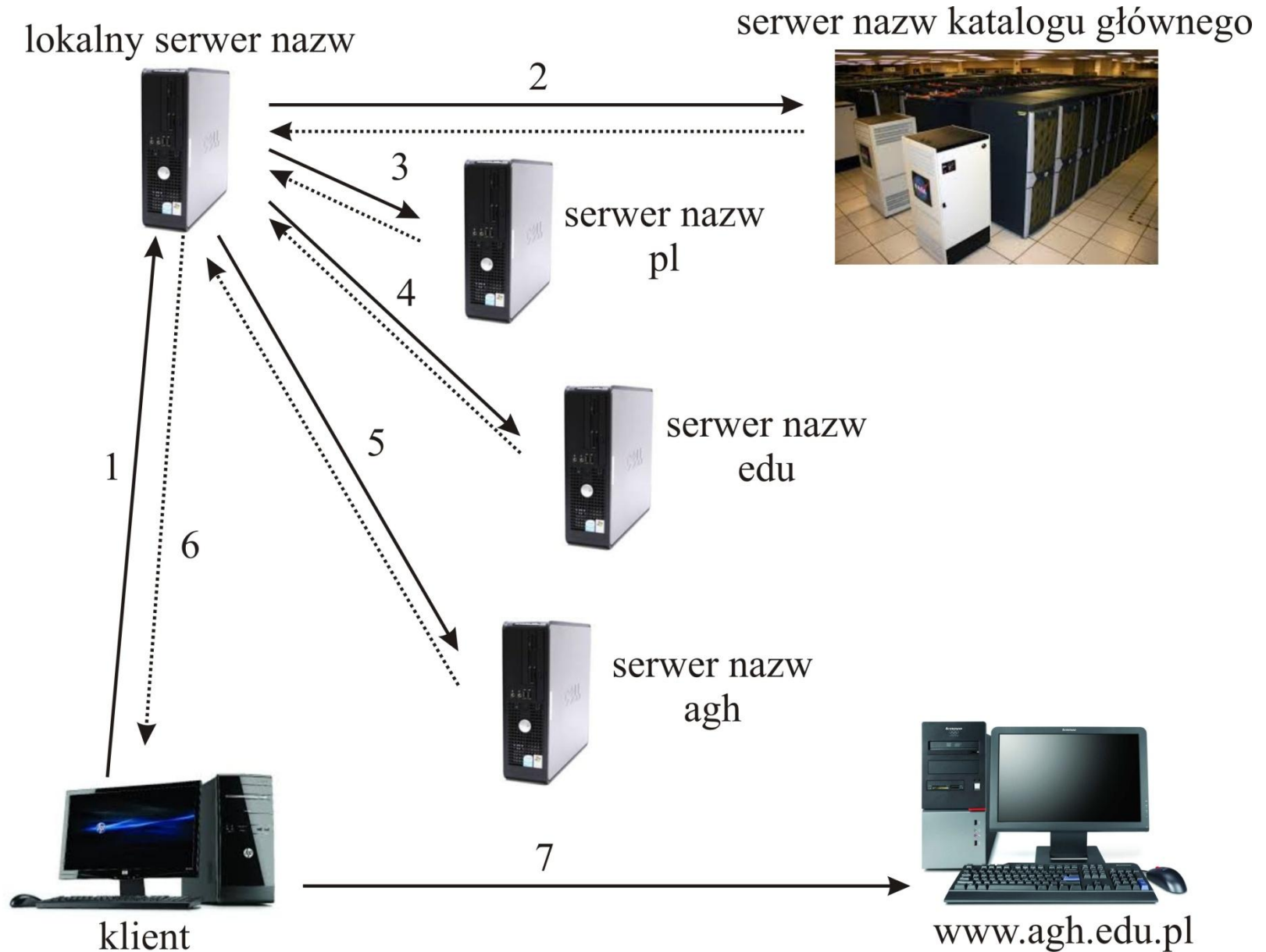
Serwery nazw

- Serwer nazw przechowuje bazę danych strefy.
- Serwery nazw mogą przechowywać dane dla jednej lub więcej stref.
- Strefa musi posiadać co najmniej jeden serwer nazw, przy czym jeden jest zawsze podstawowym (transfer strefy – przesyłanie bazy danych do hostów pomocniczych, nadmiarowość, zmniejszenie obciążenia i poprawa szybkości dostępu do lokalizacji zdalnych).

Proces rozpoznawania nazw

- Rozwiązywanie nazw na adres IP – wyszukiwanie do przodu lub adresu IP na nazwę – wyszukiwanie wstecz.
- Serwer nazw rozwiązuje kwerendy jedynie dla strefy, dla której ma uprawnienia.
- W przypadku niemożności rozwiązania nazwy, kwerenda przesyłana jest do innych serwerów.
- Wyniki kwerend są buforowane dla zmniejszenia ruchu w sieci.

Proces rozpoznawania nazw (przykład)



Kwerenda wyszukiwania do przodu (1)

1. Przekazanie kwerendy do lokalnego serwera nazw (np. `icsr.agh.edu.pl`).
2. Lokalny serwer sprawdza swoją bazę strefy. Jeśli nie ma uprawnień do danej domeny, przekazuje ją do jednego z serwerów katalogu głównego. Serwer katalogu głównego odsyła odnośnik do serwerów nazw (`pl`).
3. Lokalny serwer wysyła żądanie do serwera nazw `pl`. Otrzymuje adres serwera nazw domeny `edu`.

Kwerenda wyszukiwania do przodu (2)

4. Lokalny serwer wysyła żądanie do serwera nazw domeny .edu. Serwer domeny edu odsyła adres IP serwera nazw domeny agh.
5. Lokalny serwer nazw wysyła zapytanie do serwera nazw domeny AGH i odsyła adres IP hosta www.agh.edu.pl klientowi.
6. Klient uzyskuje dostęp do hosta www.agh.edu.pl na podstawie uzyskanego adresu IP.

Buforowanie serwera nazw

- Rozwiązanie nazwy może generować kilka kwerend prowadzących do „poznania” nowych serwerów nazw.
- Wyniki kwerend są buforowane co zmniejsza ruch sieciowy (istotny czas buforowania).
- Po rozwiązaniu serwer nazw:
 - Buforuje wynik przez czas określony przez TTL.
 - Zmniejszanie TTL rozpoczyna się w chwili umieszczenia kwerendy w buforze.
 - Po wygaśnięciu TTL serwer nazw usuwa kwerendę z bufora.

Kwerenda wyszukiwania wstecznego

- Wykorzystywane w celu zgłaszania nazw hostów (np. polecenie *nslookup*).
- Pewne aplikacje wdrażają zabezpieczenie polegające na możliwości łączenia się przez adresy symboliczne.
- Baza danych DNS indeksowana jest wg nazwy, więc kwerendy wyszukiwania wstecznego przeszukiwałyby całość bazy.
- Stworzono specjalną domenę drugiego rzędu o nazwie **in-addr.arpa**.

in-addr.arpa

- Ten sam hierarchiczny schemat nazewniczy co pozostałe domeny.
 - Bazuje na adresach IP:
 - Nazwy subdomen występują po adresach IP, przedstawionych jako liczby dziesiętne oddzielone kropkami.
 - Oktety adresu IP występują w odwróconej kolejności.
 - Organizacje administrują subdomenami domeny in-addr.arpa w oparciu o przyznane adresy IP i maskę podsieci.
- Np. właściciel sieci 169.254.16.0 z maską 255.255.255.0 ma uprawnienia do domeny: 16.254.169.in-addr.arpa.

Rekordy zasobów

- Wpisy w pliku bazy danych strefy.
- Dziela się na klasy z których każdy odnosi się do typu sieci lub oprogramowania.
- W rekordach zasobów występuje pole klasy:
 1. IN – Internet
 2. CS – Klasa CSNET (przestarzała)
 3. CH – Klasa CHAOS
 4. HS – Klasa HESIOD

Rekordy zasobów

- Adres startowy uwierzytelnienia (SOA) (TTL=60 min) pierwszy w bazie. Określa serwer nazw będący podstawowym źródłem informacji o domenie.
- Serwer nazw (NS) – serwery nazw związane z daną domeną.
- Nazwa Hosta (A).
- Nazwa kanoniczna (alias) (CNAME).
- Dokumenty: RFC1034, RFC2052, RFC2065.

Rekordy zasobów - przykład

The screenshot shows the Windows DNS console. The left pane displays a tree view of the DNS hierarchy. The right pane shows a list of resource records for the selected zone.

Tree View:

- DNS
 - SERVER
 - Forward Lookup Zones
 - krakow.filemon.wszib.edu.pl
 - Reverse Lookup Zones
 - 0.in-addr.arpa
 - 127.in-addr.arpa
 - 255.in-addr.arpa
 - 1.31.172.in-addr.arpa
 - Cached Lookups

Resource Records:

Name	Type	Data
(same as parent folder)	NS	galaxy.uci.agh.edu.pl.
(same as parent folder)	NS	ns.icm.edu.pl.
(same as parent folder)	NS	nms.cyf-kr.edu.pl.
(same as parent folder)	NS	arrow.uci.agh.edu.pl.
arax	A	149.156.96.21
arrow	A	149.156.96.12
galaxy	A	149.156.96.9
noc	A	149.156.96.8
www	CNAME	arax.uci.agh.edu.pl.

MX (mail exchanger)

- Rekordy MX określają wymiennik poczty (ang. mail exchanger) dla danej nazwy domenowej.
- Jest to host, który przetwarza lub przekazuje (np. przez firewall) pocztę adresowaną do danej nazwy domenowej.
- Przetwarzanie poczty oznacza dostarczenie jej do adresata albo przekształcenie w inny format transportowy.
- Przekazywanie poczty oznacza wysyłanie poczty do końcowego miejsca przeznaczenia albo do innego wymiennika poczty znajdującego się bliżej adresata za pośrednictwem SMTP.

SRV

- Rekord SRV, wprowadzony w RFC 2052, to uniwersalny mechanizm lokalizowania usług.
- Rekord SRV ma też specjalne opcje, dzięki którym można rozkładać obciążenie i zapewniać usługi rezerwowe, podobnie jak rekord MX.

HESIOD

- Hesiod dostarcza informacji o użytkownikach, grupach, systemach plikowych dostępnych w sieci, zasobach drukarek i rodzajach używanych usług poczty elektronicznej.
- Nie jest to system bazodanowy do obsługi zaawansowanych zapytań, lub też magazyn danych które zmieniają się często. Implementacja nie posiada specjalnej aplikacji udostępniającej możliwość aktualizacji danych w bazie Hesiod.

Spam

- Istnieje wiele baz danych które gromadzą adresy IP, informacje o domenach rozsyłających spam
- Przykładem takiej strony, która przechowuje informacje o nadawcach spamu jest ordb.org.

Spam - przykład

dig 159.238.3.24.dnsbl.sorbs.net

```
; <<>> DiG 9.2.1 <<>> 159.238.3.24.dnsbl.sorbs.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59654
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 10, ADDITIONAL: 6

;; QUESTION SECTION:
;159.238.3.24.dnsbl.sorbs.net.      IN      A

;; ANSWER SECTION:
159.238.3.24.dnsbl.sorbs.net. 3560 IN      A      127.0.0.10

;; AUTHORITY SECTION:
dnsbl.sorbs.NET.      86360      IN      NS      rblDNS0.sorbs.NET.

;; ADDITIONAL SECTION:
rblDNS0.sorbs.NET.      7160      IN      A      203.15.51.34

;; Query time: 2 msec
;; SERVER: 149.156.99.9#53(149.156.99.9)
;; WHEN: Mon Feb 28 12:57:49 2005
;; MSG SIZE rcvd: 422
```

host

- Lokalizacja hosta według zapisanych współrzędnych geograficznych:

```
[bory@messy bory]$ host -t loc yahoo.com  
yahoo.com LOC 37 23 30.900 N 121 59 19.000 W 7.00m 100m 100m 2m
```