

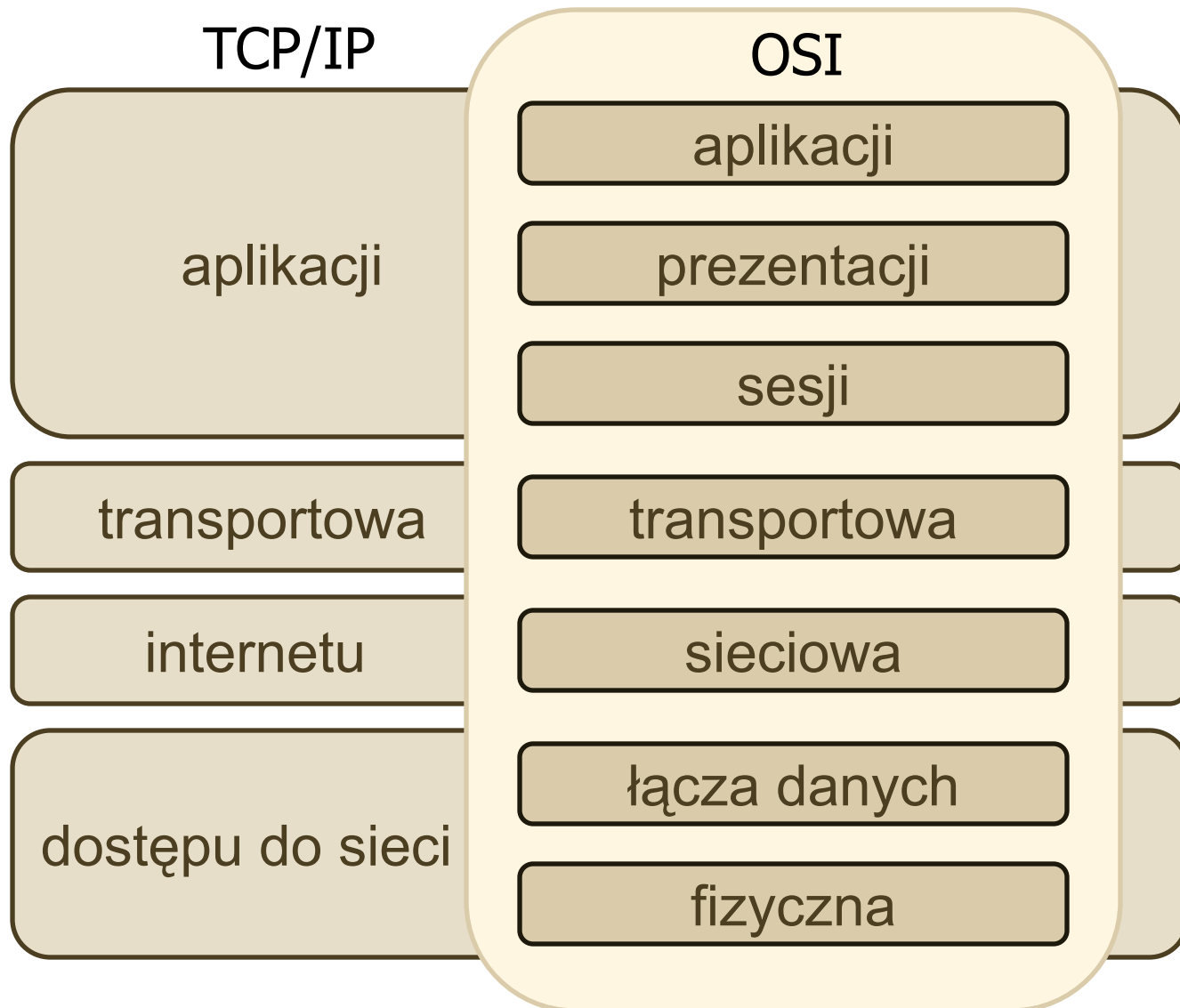


# Usługa nazw domenowych

Domain Name System (DNS)

Krzysztof Boryczko

# Model OSI a TCP/IP



# Warstwy modelu OSI

## 1. Dostępu do sieci

- Zawiera w sobie wszystkie składniki niezbędne do wysyłania i obierania sygnału
- Sygnał może być przesyłany w formie elektrycznej, optycznej, radiowej itp.
- Obejmuje również urządzenia potrzebne do transportu sygnału, a więc okablowanie, karta sieciowa, koncentrator, modem, repeater itp.
- Jest odpowiedzialna za przesyłanie sygnałów dla wszystkich protokołów sieciowych
- Przykładowe standardy: Ethernet 10BASE-T, Ethernet 100BASE-TX, iRDA, Bluetooth, Firewire, USB, ISDN, DSL, GSM itp

# Warstwy modelu OSI c.d.

## 2. Łączy dane

- Odpowiedzialna za transport danych pomiędzy dwoma urządzeniami w tej samej sieci lokalnej
- Upakowuje dane w ramki i w takiej postaci je przesyła
- Protokoły pracujące w tej warstwie, to przykładowo: Ethernet, ARP, ATM, Frame Relay, IEEE 802.11 wireless LAN, itp.
- Urządzenia pracujące w tej warstwie to: przełącznik (switch), most (bridge)

# Warstwy modelu OSI c.d.

## 3. Sieciowa

- Odpowiedzialna za transport danych w postaci datagramów od nadawcy do końcowego odbiorcy
- Musi umieć znaleźć odpowiednią trasę, czyli odpowiedzialna za routing
- Posługuje się adresacją logiczną hostów (nie zależna od sprzętu i sposobu przesyłania danych)
- Podstawowe urządzenie tej warstwy to router
- Wykorzystywane protokoły: IPv4, IPv6, ICMP, IPsec, AppleTalk, IPX, itp.

# Warstwy modelu OSI c.d.

## 4. Transportowa

- Odpowiedzialna za przesyłanie danych pomiędzy odpowiednimi aplikacjami
- Musi umieć podzielić dane na datagramy, ponumerować je i wysłać, tak by trafiły do odpowiedniej aplikacji odbiorcy i mogły zostać złożone w całość
- Może zawierać mechanizmy kontroli przesyłania danych, aby mieć pewność, że dane zostały dostarczone do aplikacji odbiorcy, czy kontroli przepływu danych
- Podstawowe protokoły to: TCP, UDP, SSL, TLS, SCTP

# Warstwy modelu OSI c.d.

## 5. Sesji

- Odpowiedzialna za otwieranie, zamykanie i sterowanie sesją (konwersacją) pomiędzy aplikacjami
- Synchronizuje dane za pomocą punktów kontrolnych (np. strumień audio-video)
- Często wykorzystywana przez aplikacje RPC

## 6. Prezentacji

- Odpowiedzialna za konwersje danych z różnych formatów na standardowe
- Umożliwia szyfrowanie, kompresję
- Protokoły to XML, HTML, ASCII

# Warstwy modelu OSI c.d.

## 7. Aplikacji

- Odpowiedzialna za komunikacje pomiędzy procesami końcowych użytkowników
- Inicjuje i nadzoruje sesje komunikacyjne
- Często zapewnia integralność danych i obsługę błędnych informacji
- Najpopularniejsze protokoły: HTTP, SMTP, POP3, IMAP, NFS, NTP, itp.



# Budowa ramki IPv4

0 – 3	4 – 7	8 – 15	16 – 18	19 – 31
wersja	IHL	ToS	długość całkowita	
identyfikator			flagi	fragment offset
TTL		protokół	suma kontrolna	
adres źródłowy				
adres docelowy				
opcje (zwykle nieużywane)				
dane				

Ciemniejszym kolorem zaznaczone są najistotniejsze pola z punktu widzenia filtrowania ruchu w sieci

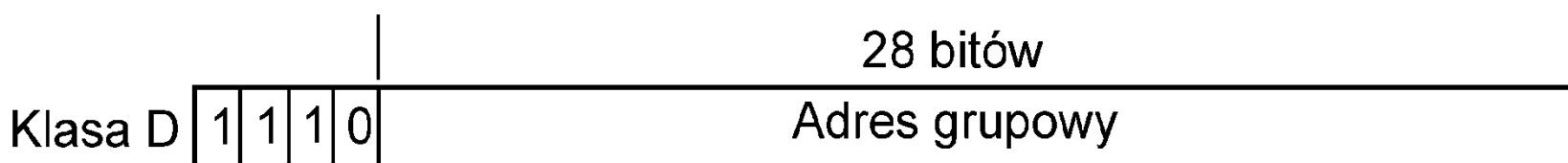
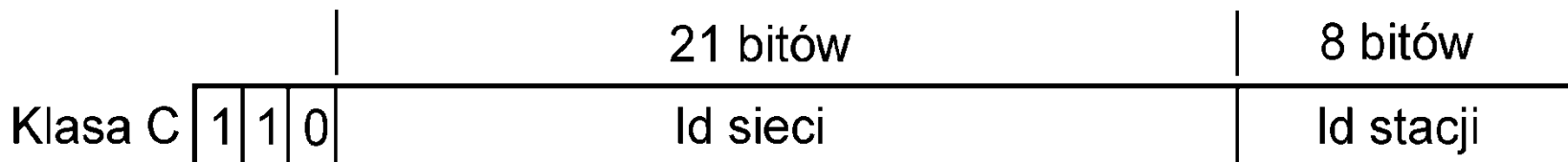
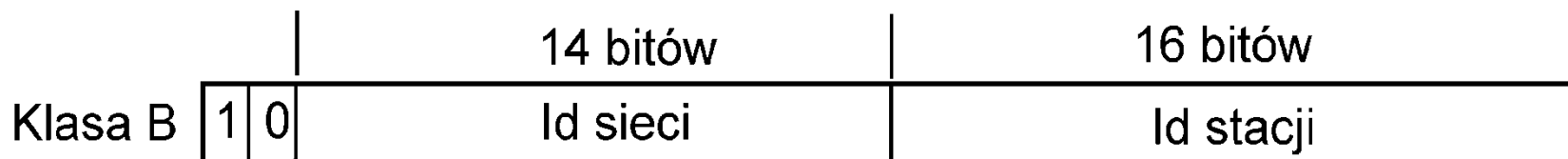
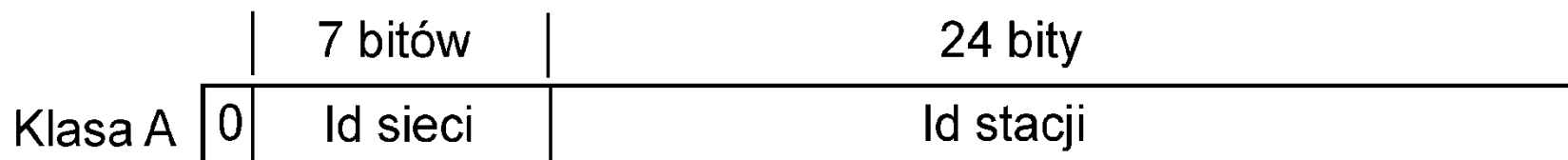
# Budowa pakietu UDP

0 – 15	16 – 31
port źródłowy	port docelowy
długość	suma kontrolna
dane	

# Budowa pakietu TCP

0 – 3	4 – 7	8 – 15	16 – 31
port źródłowy			port docelowy
numer sekwencyjny			
numer potwierdzenia			
offset dan	rezerw	flagi (ACK, SYN...)	rozmiar okna
suma kontrolna			wskaźnik priorytetu
opcje (opcjonalnie)			
dane			

# Adresy IP – klasy (przestarzałe)



# Adresy IP – routing bezklasowy

- Adres IPv4 składa się z 4 oktetów (32 bitów)
- Maska podsieci określa przynależność adresu do sieci
- Maska podsieci – ciąg jedynek i zer
- Przykład: 147.132.90.72/26 (26 bitów maski)  
czyli maska: 255.255.255.192

11111111.11111111.11111111.11	000000	
10010011.10000100.01011010.01	001000	
część adresu sieci	adresu hosta	
10010011.10000100.01011010.01	000000	sieć
10010011.10000100.01011010.01	111111	
bcast		

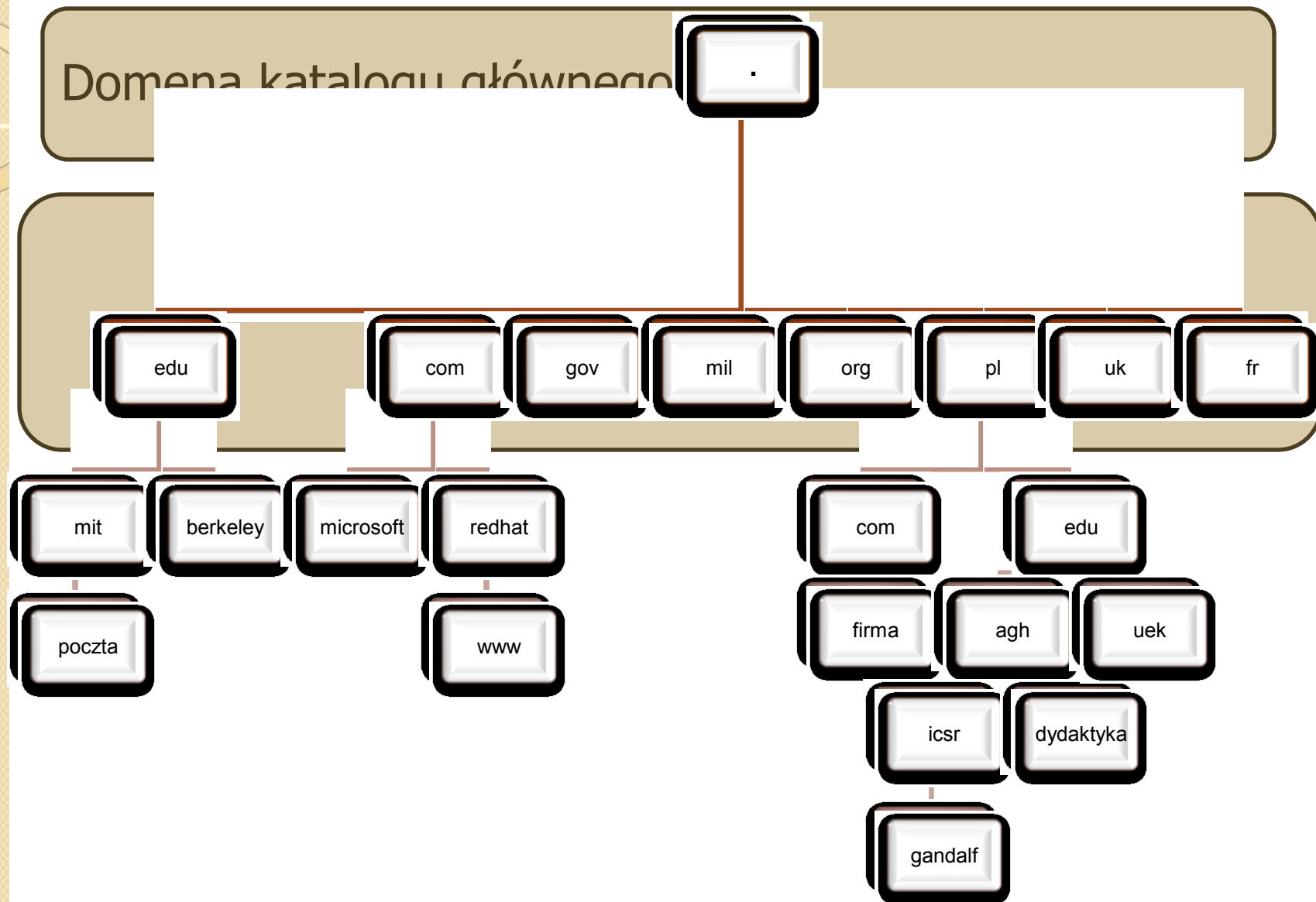
147.132.90.64 – adres sieci

147.132.90.127 – adres rozgłoszeniowy

# 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 unikalną nazwę
- Nazwa domeny określa jej pozycję w hierarchii
- Nazwa domeny jest dodawana do nazwy jej domeny podrzędnej (subdomeny)

# Hierarchia nazw domen



# Struktura hierarchiczna

- Domena katalogu głównego znajduje się na szczycie i jest przedstawiana znakiem „.” Zarządzana przez *Internet Assigned Numbers Authority* (IANA) podległą *Internet Corporation for Assigned Names and Numbers* (ICANN)
- Domeny najwyższego poziomu (Top-Level Domain – TLD) – dwu lub trzy literowe kody nazw wg:
  - położenia geograficznego (kod kraju); np. .pl, .fr, .fm
  - typów organizacji (domyślnie znajdujących się w Stanach Zjednoczonych); np. .gov, .mil, .edu, .com, .at
- Domeny drugiego poziomu – przyznawane przez odpowiednie organizacje nimi zarządzające na potrzeby organizacji, instytucji, osób fizycznych czy nazw regionalnych. Mogą zawierać hosty oraz subdomeny
- Domena .pl zarządzana jest przez *NASK*



# Nazewnictwo domen

- Pełną nazwę domeny określa się jako Fully Qualified Domain Name (FQDN); np. *agh.edu.pl*
- 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) za pomocą których definiuje się nazwy zawierające diakrytyczne znaki narodowe (Internationalized Domain Name)

# Strefy

- Strefa to ciągła część przestrzeni nazw domeny, może odnosić się do całej domeny lub subdomeny.
- Mapowanie nazw na adresy IP jest przechowywane w bazie danych strefy serwera DNS.
- Serwer przechowujący strefę jest dla niej autorytatywny.
- Strefy umożliwiają podzielenie przestrzeni nazw domeny na łatwo zarządzane sekcje
- Nie każda subdomena musi być wydzieloną strefą; np. *dydaktyka.agh.edu.pl* może być nową strefą, a *it.agh.edu.pl* pozostaje w strefie *agh.edu.pl*
- Konieczne jest zdefiniowanie delegacji dla strefy w strefie domeny nadrzędnej; czyli *agh.edu.pl* musi zawierać delegację dla *dydaktyka.agh.edu.pl*

# Rodzaje stref

- Każda definiowana strefa ma swój określony rodzaj, który określany jest podczas jej definicji.
- Typy stref są następujące:
  - **master** – serwer ma u siebie bazę związaną z tą strefą i jest dla niej autorytatywny
  - **slave** – posiada ją drugorzędny serwer dla danej strefy; odpowiada jako autorytatywny o ile ma aktualną wersję strefy
  - **stub** – podobna jak „slave”, z tym że zawiera jedynie replikę rekordów NS strefy, a nie całą jej zawartość
  - **forward** – umożliwia konfigurowanie przekierowania strefy do innych serwerów
  - **hint** – zawiera listę serwerów najwyższego poziomu (root-servers) od których rozpoczyna się rozwiązywanie kwerendy.

# Serwery nazw

- Serwer nazw przechowuje bazę danych strefy.
- Serwery nazw mogą przechowywać dane dla jednej lub więcej stref, które nie muszą być powiązane; np. *agh.edu.pl* i *pewnafirma.com.pl* mogą mieć wspólny DNS.
- Strefa musi posiadać co najmniej jeden serwer nazw, choć zalecane jest by obsługiwały ją co najmniej dwa.
- Jeden z serwerów obsługujących strefę jest podstawowym, a reszta to drugorzędne serwery DNS (wyjątek serwery w Active Directory – może być kilka podstawowych).
- Główny serwer DNS przesyła swą bazę do drugorzędnych serwerów (transfer strefy); zapewnia to nadmiarowość, zmniejszenie obciążenia i zwiększenie szybkości dostępu do danych.

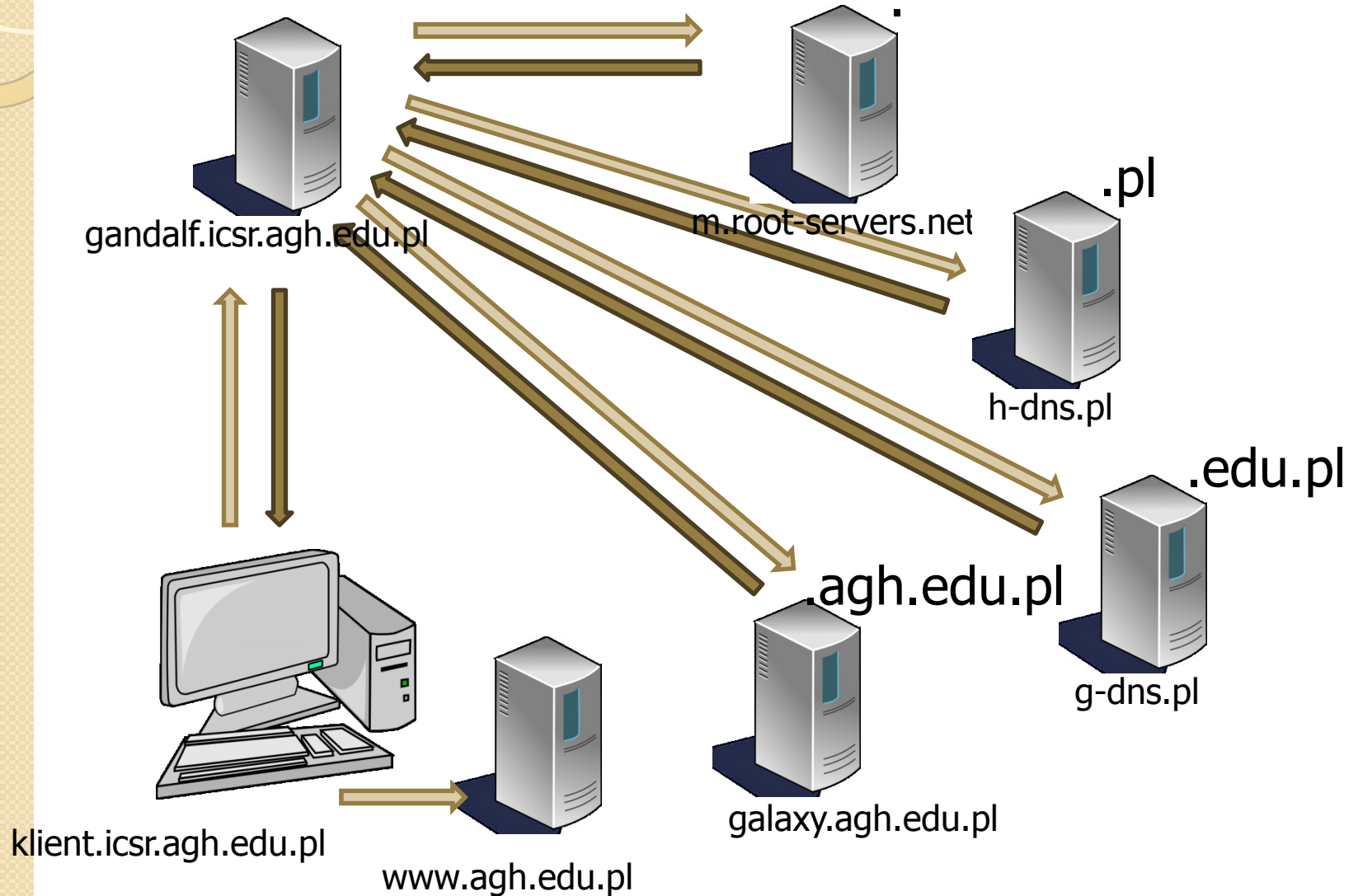
# Transfer strefy

- Każda strefa ma swój numer sekwencyjny.
- Podstawowy serwer DNS informuje o zmianie numeru.
- Drugorzędny serwer DNS uaktualnia swą wersję strefy gdy jej numer sekwencyjny nie jest aktualny.
- Podstawowy transfer strefy – drugorzędny serwer żąda kopii całej strefy (opisany w RFC 1034).
- Przyrostowy transfer strefy – drugorzędny serwer żąda tylko zmian od ostatniej aktualizacji (zdefiniowany w RFC 1995). Podstawowy serwer DNS musi utrzymywać historię zmian.
- Transfer strefy w Active Directory – wszystkie kontrolery domeny są podstawowymi serwerami DNS. Spójność ich baz zapewnia mechanizm replikacji AD.

# Proces rozpoznawania nazw

- Rozwiązywanie nazw na adres IP – wyszukiwanie do przodu lub adresu IP na nazwę – wyszukiwanie wstecz
- Serwer DNS otrzymawszy kwerendę od klienta rozwiązuje ją wykonując następujące czynności:
  - Szuka rozwiązania w swej bazie, w strefach którymi zarządza. Jeśli znajdzie odpowiedź wysyła ją jako pochodzącą od autorytatywnego serwera DNS.
  - Jeśli nie znalazł odpowiedzi we własnych strefach, to przeszukuje swoją bazę zbudowaną na podstawie zebranych odpowiedzi z wcześniejszych zapytań (cache) i wysyła odpowiedź klientowi (nie autorytatywną).
  - Jeśli nie był w stanie znaleźć u siebie rozwiązania, to może odpytywać inne serwery w celu uzyskania odpowiedzi i po jej otrzymaniu odsyła ją klientowi. Czyni to wtedy, gdy obsługuje zapytania rekursywne. Jeśli nie, to nie wysyła rozwiązania kwerendy klientowi.

# Rekursywne wyszukiwanie do przodu



# Rekursywne wyszukiwanie do przodu

1. Klient wysyła kwerendę do lokalnego serwera nazw (np. *gandalf.icsr.agh.edu.pl*) pytając przykładowo o *www.agh.edu.pl*
2. Gdy serwer DNS nie znajdzie u siebie rozwiązania kwerendy i obsługuje wyszukiwanie rekurencyjne wtedy:
  - a) Odpytuje jeden z głównych serwerów (root servers) obsługujących domenę „.” (np. *M.ROOT-SERVERS.NET*) o domenę .pl i otrzymuje adres jednego z serwerów DNS (np. *h-dns.pl*)
  - b) Pyta serwer *h-dns.pl* o domenę .edu.pl i otrzymuje adres serwera autorytatywnego dla niej (np. *g-dns.pl*)
  - c) Pyta *g-dns.pl* o *agh.edu.pl* i otrzymuje adres *galaxy.uci.agh.edu.pl*
  - d) Wreszcie pyta *galaxy.uci.agh.edu.pl* i otrzymuje ostateczną odpowiedź: *www.agh.edu.pl* to *149.156.96.2*
  - e) Odsyła tę odpowiedź klientowi



# Iteracyjne wyszukiwanie do przodu

1. Klient wysyła kwerendę do lokalnego serwera nazw (np. *gandalf.icsr.agh.edu.pl*) pytając przykładowo o *www.agh.edu.pl*
2. Gdy serwer DNS nie znajdzie u siebie rozwiązania kwerendy i **nie** obsługuje wyszukiwanie rekurencyjnego wtedy odsyła klientowi informację o braku rozwiązania.
3. Klient odpytuje więc inny serwer DNS wysyłając tę samą kwerendę.
4. Powtarza tę operację dopóki nie otrzyma rozwiązania nazwy lub gdy odpyta wszystkie serwery DNS, które ma u siebie zdefiniowane.

Przykładem iteracyjnego wyszukiwania jest również sposób w jaki serwer DNS obsługuje rekursywne uzyskiwanie rozwiązania kwerendy klienta. W sposób iteracyjny odpytuje kolejne serwery DNS, aż do uzyskania ostatecznej odpowiedzi.

# Buforowanie serwera nazw

- Rozwiązanie nazwy może generować kilka kwerend prowadzących do „poznania” nowych serwerów nazw
- Wyniki kwerend są buforowane lokalnie (cache), co zmniejsza ruch sieciowy (istotny czas buforowania)
- Po rozwiązaniu serwer nazw:
  - Buforuje wynik przez czas określony przez TTL danego rekordu.
  - 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. polecenia *nslookup*, *host*)
- Pewne aplikacje wdrażają zabezpieczenie polegające na możliwości łączenia się przez adresy symboliczne  
Przykładowo większość serwerów pocztowych sprawdza zgodność adresu IP serwera z jego nazwą, zanim wyśle do niego pocztę.
- 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 (najczęściej spotykana)
  2. CS – Klasa CSNET (przestarzała)
  3. CH – Klasa CHAOS
  4. HS – Klasa HESIOD

# Rekordy zasobów - SOA

- Adres startowy uwierzytelnienia Start of Authority (SOA) (TTL=3600 s) pierwszy w bazie. Określa:
  - serwer nazw będący podstawowym źródłem informacji o domenie
  - adres e-mail administratora strefy
  - numer seryjny strefy
  - czas odświeżenia co jaki serwer drugorzędny sprawdza czy nie zmienił się numer seryjny strefy na nowszy
  - czas przerwy do podjęcia ponownej próby odświeżenia informacji o strefie po poprzedniej nieudanej próbie
  - czas po jakim będą kasowane informacje o strefie z drugorzędnych serwerów DNS w przypadku gdy nie uda im się skomunikować z podstawowym serwerem DNS
  - minimalny czas ważności wszystkich rekordów w bazie, jeśli nie został ustawiony inny dla poszczególnych rekordów. Istotne przy buforowaniu odpowiedzi w cache'u

# Rekordy zasobów – SOA c.d.

- Wartość rekordu SOA dla strefy *agh.edu.pl*:

```
[root@localhost ~]# dig -t soa agh.edu.pl
```

```
...
```

```
:: ANSWER SECTION:
```

```
agh.edu.pl.      7200   IN      SOA     ns.agh.edu.pl.  
hostmaster.agh.edu.pl. 2010020900 28800 7200 604800 86400
```

- Odpowiadająca jej definicja w pliku strefy (BIND)

```
$TTL 7200
```

```
@ IN SOA ns.agh.edu.pl. hostmaster.agh.edu.pl. (  
                2010020900 ;   serial YYYYMMDDnn  
                        8H;    refresh (8 godzin)  
                        2H;    retry (2 godziny)  
                        1W;    expire (1 tydzień)  
                        1D );   minimum (1 dzień)
```

# Rekordy zasobów c.d.

- NS (name server record) – adres serwera DNS dla danej strefy
- A (address record) – adres IPv4 hosta
- AAAA (IPv6 address record) – adres IPv6 hosta
- CNAME (canonical name record) – alias adresu
- TXT (text record) – opis rekordu (często są tu dane dla komputerów związanych z szyfrowaniem itp.)
- Dokumenty: RFC1034, RFC1464, RFC2052, RFC2065



# Rekord MX (mail exchanger)

- Rekordy MX określają wymienniki poczty (ang. mail exchanger) dla danej nazwy domenowej.
- Jest to host, który przetwarza lub przekazuje (np. przez firewall) pocztę adresowaną do danej nazwy domenowej
- Przekazywanie poczty oznacza wysyłanie poczty do końcowego miejsca przeznaczenia, albo do innego wymiennika poczty znajdującego się bliżej adresata za pośrednictwem protokołu SMTP.
- Wartość rekordu MX zawiera priorytet – niższy, to wyższy priorytet serwera pocztowego RFC5321, RFC974.
- Wartość rekordu MX dla domeny *agh.edu.pl*

```
[root@localhost ~]# dig -t mx agh.edu.pl
```

```
...
```

```
:: ANSWER SECTION:
```

```
agh.edu.pl.      3600    IN      MX      0 poczta.agh.edu.pl.
```

# Rekord SRV

- Rekord SRV, wprowadzony w RFC 2052, to uniwersalny mechanizm lokalizowania usług.
- Postać definicji rekordu SRV:  
\_usługa.\_protokół.nazwa TTL klasa SRV priorytet waga port cel  
gdzie:
  - usługa – nazwa usługi (np. kerberos, ldap)
  - nazwa – pełna nazwa domeny (FQDN), w której jest usługa
  - TTL – czas życia rekordu,
  - klasa – głównie IN (Internet),
  - priorytet – im niższa wartość, tym wyższy (jak dla MX),
  - waga – rozróżnia ważność dla rekordów mających ten sam priorytet,
  - port – określa port, na którym pracuje usługa,
  - cel – nazwa FQDN hosta świadczącego usługę

# Rekord SRV - przykład

- Przykładowa wartość rekordu SRV dla lokalizacji usługi LDAP w domenie *krakow.agh.edu.pl*

```
[root@localhost ~]# dig -t srv _ldap._tcp.agh.edu.pl
```

```
...
```

```
:: ANSWER SECTION:
```

```
_ldap._tcp.krakow.agh.edu.pl. 600 IN SRV 0 100 389  
dns1.krakow.agh.edu.pl
```

```
:: ADDITIONAL SECTION:
```

```
dns1.agh.edu.pl. 3600 IN A      172.31.1.10
```

# Rekord LOC

- LOC – Location Record określony przez RFC1876
- Umożliwia zdefiniowanie lokalizacji hosta według zapisanych współrzędnych geograficznych
- Rekord LOC zawiera:
  - szerokość geograficzną w st min s
  - długość geograficzną w st min s
  - wysokość w m
  - rozmiar w m
  - dokładność położenia i wysokości w m

```
[root@localhost ~]# dig -t loc ckdhr.com
```

```
...
```

```
:: ANSWER SECTION:
```

```
ckdhr.com.          259200 IN      LOC   42 21 43.528 N 71 5  
6.284 W -25.00m 1m 3000m 10m
```

# Rekord PTR

- PTR – Pointer Record określony przez RFC1035
- Jest to rekord dla wyszukiwania wstecznego.
- Wskazuje na nazwę FQDN dla danego adresu IP
- W definicji podawana jest tylko część adresu IP hosta; adres sieci jest w nazwie domeny in-addr.arpa
- Przykład zapytania:

```
[root@localhost ~]# dig -x 217.96.89.184
```

```
...
```

```
:: ANSWER SECTION:
```

```
184.89.96.217.in-addr.arpa. 86400 IN   PTR    poczta.agh.edu.pl.
```

- Równoważna postać zapytania

```
[root@localhost ~]# dig -t ptr 184.89.96.217.in-addr.arpa
```

# Przykład opisu strefy – linux

\$TTL 7200

@ IN SOA dns1.krakow.filemon.agh.edu.pl. hostmaster.krakow.filemon.agh.edu.pl.(

2010020900 ; serial  
8H; refresh  
2H; retry  
1W; expire  
1D ); minimum

NS dns1.krakow.filemon.agh.edu.pl.  
MX 10 poczta.krakow.filemon.agh.edu.pl.

dns1 A 172.31.1.10  
poczta A 172.31.1.12  
klient A 172.31.1.13  
TXT „Serwer testowy”  
www CNAME klient

# HESIOD

- Hesiod dostarcza informacji o użytkownikach, grupach, systemach plikowych dostępnych w sieci, zasobach drukarek i rodzajach używanych usług poczty elektronicznej.
- Hesiod wykorzystuje DNS jako dostęp do bazy danych zawierającej te odpowiednie informacje
- 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.
- Raczej zbyt mało wykorzystywany; częstsze zastosowanie ma przykładowo LDAP

# Spam

- Istnieje wiele baz danych które gromadzą adresy IP, informacje o domenach rozsyłających spam
- Przykładem takiej strony, która przechowuje informacje o nadawcach spamu jest [dnsbl.info](http://dnsbl.info)
- Wykorzystanie DNS polega na wysłaniu zapytania do serwera z odwróconym adresem IP, jeśli zostanie zwrócony rekord A wskazujący na ten adres, to serwer pocztowy jest podejrzany o rozsyłanie spamu



# Spam - przykład

```
[root@localhost ~]# dig 159.238.3.24.dnsbl.sorbs.net
```

```
...
```

```
:: 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.	86400	IN	NS	rbldns12.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns1.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns8.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns7.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns3.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns4.sorbs.net.
dnsbl.sorbs.net.	86400	IN	NS	rbldns6.sorbs.net.

```
...
```

# DNS – wymagania instalacyjne

- Host musi posiadać skonfigurowany, statyczny adres IP
- Konieczność takiego skonfigurowania właściwości TCP/IP, aby ustawienia DNS wskazywały z powrotem na serwer
- W przypadku systemów z rodziny Microsoft Windows konieczna jest wersja serwerowa systemu
- Musi być wykonana delegacja dla tworzonej strefy w domenę nadrzędnej

# Instalacja DNS – Linux RH

- Instalacja pakietu *bind* i związanych z nim bibliotek
- W nowszych dystrybucjach instalacja pakietu *bind-chroot* ograniczającego środowisko pracy serwera DNS do katalogu */var/named/chroot*
- Plik konfiguracyjny serwera: */etc/named.conf*
- Katalogi zawierający pliki strefowe: */var/named*
- W przypadku pracy serwera DNS w ograniczonym środowisku (chroot) pliki i katalogi serwera znajdują się w podkatalogach: */var/named/chroot*
- Wszystkie pliki są to pliki tekstowe, a więc zarządzanie serwerem z poziomu dowolnego edytora.

# DNS – protokoły sieciowe

- Standardowo DNS do wymiany informacji wykorzystuje port 53 protokołu UDP oraz TCP.
- Wysyłanie odpowiedzi na kwerendę klienta odbywa się zasadniczo poprzez protokół UDP.
- W przypadku gdy odpowiedź jest za długa, serwer DNS może wykorzystać protokół TCP uprzednio informując o tym klienta (bardzo rzadkie).
- Transfer strefy pomiędzy głównym serwerem a drugorzędnym – protokół TCP.
- W przypadku transferu przyrostowego może być użyty protokół UDP (w wypadku małych zmian).
- Synchronizacja serwerów DNS w AD wykorzystuje mechanizm replikacji AD i specyficzne dlań protokoły.

# Konfiguracja klienta DNS

- Wpis w pliku */etc/resolv.conf*.
  - Wartość atrybutu *nameserver* po jednej definicji w linii.
  - Adresy co najmniej 2 serwerów DNS.
  - Kolejność od „najbliższego czasowo”.
- Możliwość zdefiniowania nazw często odwiedzanych domen (atrybut *search*).

nameserver 172.19.99.9

nameserver 149.156.96.9

search dydaktyka.icsr.agh.edu.pl icsr.agh.edu.pl agh.edu.pl



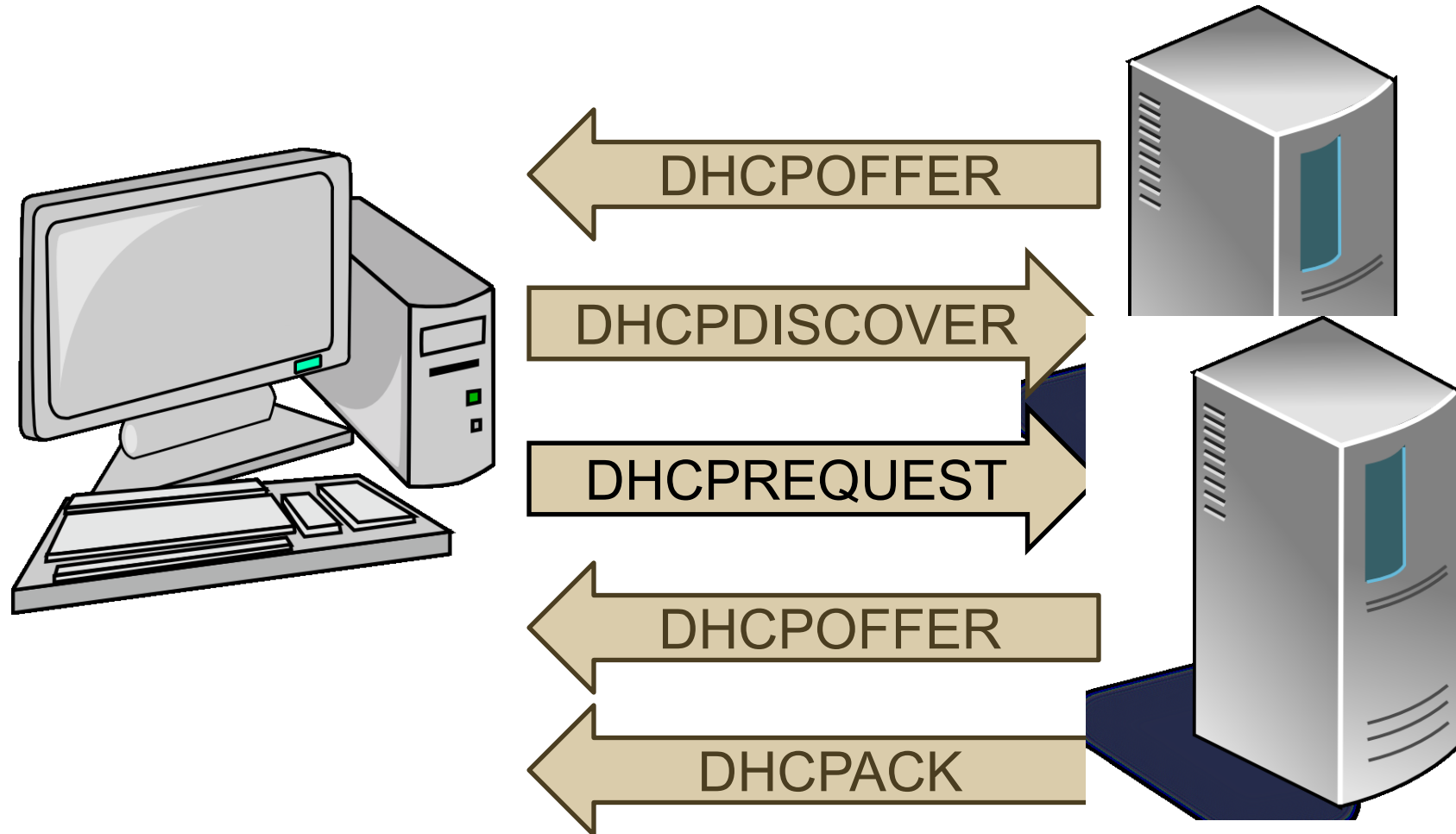
# Protokół dynamicznej konfiguracji hostów

Dynamic Host Configuration Protocol  
(DHCP)

# Protokół DHCP

- Opracowany dla uproszczenia zarządzania konfiguracją IPv4; zdefiniowany w RFC2131.
- Stanowi rozszerzenie protokołu ładowania początkowego BOOTP (BOOTstrap Protocol) opisanego przez RFC951 – możliwe zdalne uruchamianie hosta i jego konfiguracja.
- Protokół DHCP współpracuje również z adresami IPv6, wersja ta (DHCPv6) zdefiniowana jest przez RFC 3315.
- Dostarcza:
  - Adres IP, maskę podsieci
  - Wartości opcjonalne: adres bramy, adresy serwerów DNS, nazwa domeny DNS, adres serwera czasu, adres serwera WINS itd.

# Proces dzierżawienia DHCP





# DHCP – pozyskiwanie konfig.

- DHCPDISCOVER

- wysyłany do wszystkich w sieci (broadcast) z prośbą o otrzymanie adresu IP. Może zawierać ostatnio używany przez klienta adres IP w celu odnowienia go (co serwer może zignorować).

- DHCPOFFER

- wysyłany do wszystkich, ale z adresem sprzętowym klienta z oferowanym adresem, opcjami oraz z czasem ważności dzierżawy

- DHCPREQUEST

- wysyłany do wszystkich, ale z informacją dla konkretnego serwera DHCP o potwierdzeniu otrzymania dzierżawy. Może być kilka serwerów, więc istotne jest by wszystkie otrzymały tę informację.

- DHCPACK

- wysyłane przez serwer potwierdzenie dla klienta (też broadcast). To kończy wymianę informacji i klient może już używać adresu.

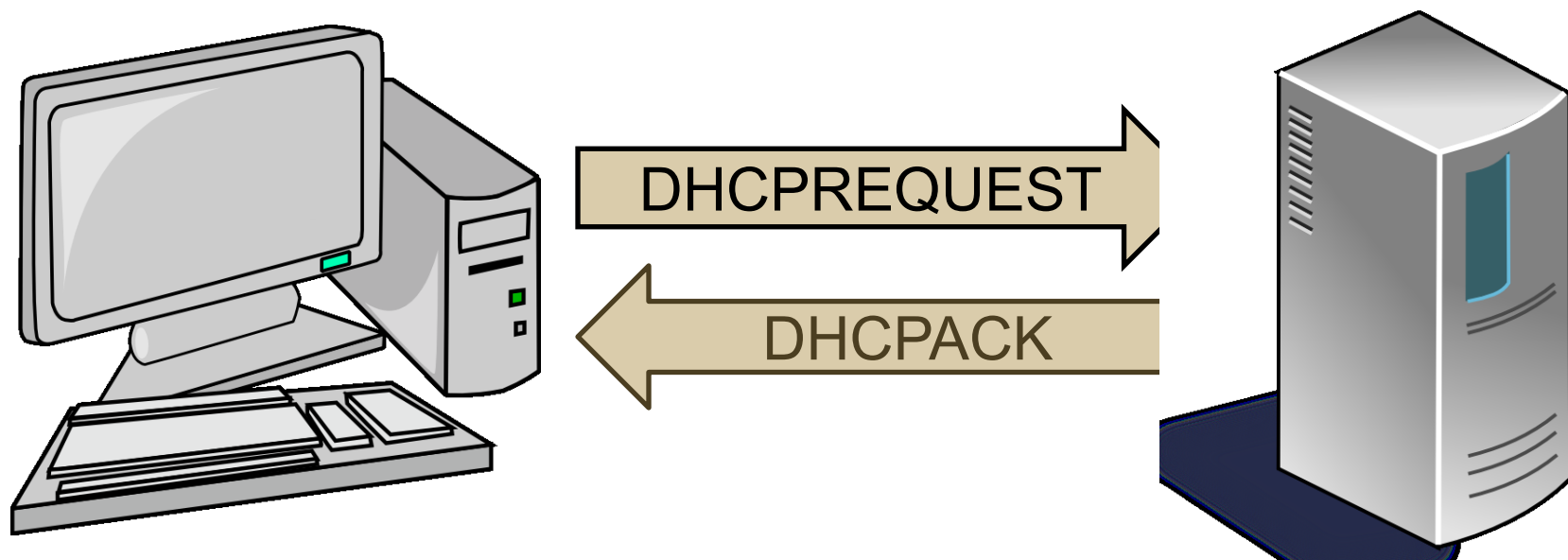
# Pozyskiwanie dzierżawy

- Proces uzyskiwania dzierżawy przez klienta – zapis w pliku dziennika */var/log/messages* systemu Linux:

```
Jan 28 14:17:52 localhost dhcpd: DHCPDISCOVER from  
00:02:e3:53:31:94 via eth1  
Jan 28 14:17:53 localhost dhcpd: DHCPOFFER on 192.168.6.20 to  
00:02:e3:53:31:94 via eth1  
Jan 28 14:17:53 localhost dhcpd: DHCPREQUEST for 192.168.6.20  
(192.168.6.17) from 00:02:e3:53:31:94 via eth1  
Jan 28 14:17:53 localhost dhcpd: DHCPACK on 192.168.6.20 to  
00:02:e3:53:31:94 via eth1
```

- Klient wystąpił o adres *192.168.6.17* lecz otrzymał *192.168.6.20*.

# Odnawianie dzierżawy c.d



- Jeśli po czasie  $T_1$  serwer nie odpowiedział, to klient ponawia próby aż do czasu  $T_2$ , a później występuje o nową konfigurację.
- W przypadku gdy klient przestaje wykorzystywać adres IP informuje o tym serwer (np. wyłączenie interfejsu).

# Odnawianie dzierżawy

- Przesyłana klientowi konfiguracja ma określony czas życia zwany czasem dzierżawy.
- Z czasem ważności dzierżawy związane są dwa parametry – czas T1 i czas T2
- Standardowo T1 to 50%, a T2 – 87,5% czasu dzierżawy, jednak czasem mogą być konfigurowalne.
- Klient po upływie czasu T1 wysyła do serwera od którego otrzymał konfigurację, prośbę o odnowienie dzierżawy – komunikat DHCPREQUEST ze swoim adresem IP
- Serwer zwykle odpowiada komunikatem DHCPACK i resetowane są zegary T1 i T2, itd.

# Przykładowy plik dzierżawy

- Plik znajduje się w katalogu

*/var/lib/dhclient/dhclient-eth\*.leases*

```
lease {  
  interface "eth0";  
  fixed-address 192.168.6.20;  
  option subnet-mask 255.255.255.240;  
  option routers 192.168.6.17;  
  option dhcp-lease-time 600;  
  option dhcp-message-type 5;  
  option domain-name-servers 217.96.89.150,149.156.96.9;  
  option dhcp-server-identifier 192.168.6.17;  
  option broadcast-address 192.168.6.31;  
  option domain-name "wroclaw.filemon.agh.edu.pl";  
  renew 4 2010/01/28 13:26:29;  
  rebind 4 2010/01/28 13:31:25;  
  expire 4 2010/01/28 13:32:40;  
}
```

# Inne komunikaty DHCP

- DHCPNAK

- wysyłany do klienta przez serwer DHCP jako odmowna odpowiedź gdy np. klient nie może dostać adresu, lub przeniósł się do innej sieci, itp.

- DHCPDECLINE

- wysyłany do serwera z informacją, że proponowany adres jest już używany przez inny host

- DHCPRELEASE

- wysyłane przez klienta do serwera DHCP zwolnienie zajmowanego adresu IP i przerwanie dzierżawy

- DHCPINFORM

- wysyłane przez klienta do serwera DHCP żądanie dodatkowych ustawień. Klient już posiada skonfigurowany adres IP.

# Tworzenie zakresu DHCP

- Jest to pula prawidłowych adresów IP, które mogą być dzierżawione klientom DHCP
- Zakres określony jest przez adres podsieci (wraz z maską) dla której jest definiowany oraz przez początkowy i końcowy adres w tej podsieci
- Dla każdego serwera musi być utworzony co najmniej jeden zakres
- Możliwe jest tworzenie wielu zakresów na jednym serwerze DHCP (najczęściej różne podsieci na serwerze mają swe zakresy)
- Z zakresu należy wyłączyć pulę adresów statycznych
- Każdy zakres może mieć oddzielną konfigurację parametrów przekazywanych klientom

# Tryby przydzielania adresów

- Dynamiczna alokacja
  - Na serwerze DHCP określona jest pula adresów IP, które są automatycznie przydzielane klientom.
  - Adresy te nie są odnawiane, lecz serwer DHCP zmienia je pomiędzy hostami.
- Automatyczna alokacja
  - Podobna jak dynamiczna, ale serwer pamięta adresy IP jakie przydziela klientom
  - Hosty odnawiają dzierżawę i wykorzystują te same adresy
- Statyczna alokacja
  - Serwer DHCP przydziela adresy IP według adresów sprzętowych MAC jakie ma w swojej konfiguracji.
  - Zapisana jest para adres IP / adres MAC dzięki czemu klient zawsze otrzymuje ten sam adres.
  - Tylko Ci klienci którzy są zarejestrowani otrzymują adresy IP



# Zakres i rezerwacja – Linux

- Konfiguracja zakresu od *192.168.6.20* do *192.168.6.30* dla podsieci *192.168.6.16/28*

```
subnet 192.168.6.16 netmask 255.255.255.240 {  
    range 192.168.6.20 192.168.6.30;  
    ...  
    option ...  
}
```

- Konfiguracja rezerwacji adresu IP wg adresu sprzętowego

```
host nazwa_rezerwacji {  
    option host-name „nazwa_hosta”;  
    hardware ethernet 00:02:e3:53:31:94;  
    fixed-address 192.168.6.20;  
}
```

# Przykład konfiguracji – Linux

```
subnet 192.168.6.16 netmask 255.255.255.240 {  
    range 192.168.6.20 192.168.6.30;  
    option routers 192.168.6.17;  
    option broadcast-address 192.168.6.31;  
    option domain-name-servers 217.96.89.150,149.156.96.9;  
    option domain-name "wroclaw.filemon.agh.edu.pl";  
  
    default-lease-time 600;  
    max-lease-time 7200;  
    ddns-updates off;  
  
    host klient {  
        option host-name "klient";  
        hardware ethernet 00:02:e3:53:31:94;  
        fixed-address 192.168.6.20;  
    }  
}
```

# DHCP – wymagania instalacyjne

- Musi posiadać ręcznie skonfigurowany adres IP, maskę podsieci, bramę domyślną oraz inne parametry protokołu IP – nie może być klientem DHCP
- W przypadku systemów z rodziny Microsoft Windows konieczna jest wersja serwerowa systemu
- Musi posiadać uaktywniony zakres DHCP
- W przypadku instalacji serwera DHCP w domenie Active Directory konieczna jest jego autoryzacja w usłudze AD

# Instalacja DHCP – Linux RH

- Instalacja pakietu *dhcp* i związanych z nim bibliotek
- Plik konfiguracyjny serwera: */etc/dhcp/dhcpd.conf*  
w starszych wersjach systemu: */etc/dhcpd.conf*
- Plik konfiguracyjny serwera, to plik tekstowe, a więc zarządzanie serwerem z poziomu dowolnego edytora.

# DHCP – protokoły sieciowe

- Do przesyłania danych pomiędzy stacją kliencką a serwerem DHCP zasadniczo wykorzystywany jest protokół UDP
- W szczególnym przypadku, gdy wysyłane dane będą za duże możliwe jest wykorzystanie protokołu TCP, co jest niezmiernie rzadkie
- Do komunikacji wykorzystywane są dwa porty – 67 na którym nasłuchuje serwer DHCP i 68 po stronie klienta
- Prawie cała komunikacja wysyłana jest na adres rozgłoszeniowy podsieci

# Klient DHCP – Linux RH

- Konfiguracja interfejsu sieciowego o nazwie *eth0* w systemie Linux RH znajduje się w pliku */etc/sysconfig/network-scripts/ifcfg-eth0*
- Ustawienie dynamicznej (DHCP) konfiguracji sieci:

```
# Networking Interface  
DEVICE=eth0  
HWADDR=00:1B:38:6A:C2:E5  
BOOTPROTO=dhcp  
TYPE=Ethernet  
ONBOOT=yes
```