Piotr Kowalski
KAiTI

Sieci komputerowe
- Protokoły DHCP i DNS

Plan i problematyka wykładu

1. DHCP
   - Wprowadzenie, główne cechy, metody przydziału adresów.
   - Cykl pracy klienta DHCP
   - Format wiadomości DHCP
2. DNS
   - Wprowadzenie, przestrzeń domen – struktura i zarządzanie
   - Tłumaczenie nazw domenowych
   - Format wiadomości DNS (zarys)

DHCP – wprowadzenie

- Dynamic Host Configuration Protocol (DHCP) został opracowany na początku lat 90 jako rozwinięcie protokołu BOOTP
- DHCP pozwala na autokonfigurację interfejsów sieciowych węzłów w sieci TCP/IP, z możliwością realizacji przydziału dynamicznego z dostępnej puli adresów
- DHCP pracuje w architekturze klient/serwer i definiuje zestaw wiadomości i odpowiedzi na nie

Metody przydziału adresów w DHCP

- **Przydział ręczny** – adres IP jest przydzielany przez administratora każdemu urządzeniu, zadaniem serwera DHCP jest jedynie jego zakomunikowanie
- **Przydział automatyczny** – serwer DHCP przydziela adres automatycznie włączonemu do sieci urządzeniu, na stałe, wybierając adres z dostępnej puli
- **Przydział dynamiczny** – serwer DHCP przydziela adres węzłowi z puli dostępnych adresów na określony czas tzw. czas dzierżawy adresu (ang. lease time) lub do czasu gdy klient zakomunikuje że adresu już nie wymaga

Cykl dzierżawy adresu (ang. lease life cycle)

Cykl procesu dzierżawy adresu obejmuje:

1. Alokację adresu (ang. address allocation)
2. Realokację adresu (ang. address reallocation)
3. Normalną pracę tj. klient w stanie przydzielonej dzierżawy (ang. bound)
4. Odnowę dzierżawy (ang. lease renewal)
5. Ponowne nawiązanie dzierżawy (ang. rebind), korzystając z usług innego serwera DHCP
6. Zwolnienie dzierżawy (ang. release)

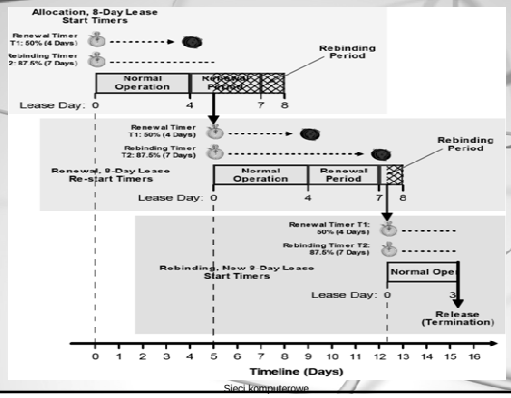
Odliczanie czasu w procesie dzierżawienia adresu

Klient DHCP wykorzystuje dwa liczniki czasu (timery), zliczające w dół co pozwala na wznowienie dzierżawy bez utraty w międzyczasie funkcjonalności węzła sieciowego:

- **Timer odnowy dzierżawy** (ang. renewal timer) – ustawiony początkowo domyślnie na 50% czasu dzierżawy przesłanego przez serwer DHCP i oznaczany jako T1
- **Timer ponownej dzierżawy** (ang. rebinding timer) – ustawiony początkowo domyślnie na 87,5% czasu dzierżawy i oznaczany jako T2

Po pomyślnej odnowie lub ponowieniu dzierżawy timery T1 i T2 są resetowane do stanu początkowego. Gdy T1 lub T2 osiągną zero to realizowana jest odnowa lub ponowna dzierżawa adresu.

Ilustracja



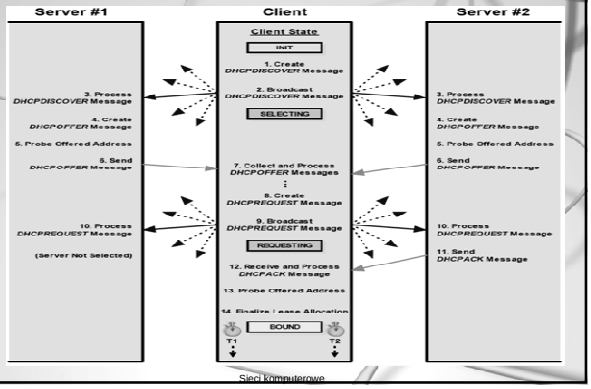
Cykl pracy klienta DHCP

- **INIT** – klient bez dzierżawy adresu, wysyła wiadomość DHCPDISCOVER by ją uzyskać, przechodzi po jej wysłaniu do stanu SELECTING
- **SELECTING** – oczekiwanie na jedną lub więcej wiadomości DHCPOFFER, po ich otrzymaniu następuje wybór jednej i odesłanie do serwerów wiadomości DHCPREQUEST potem przejście do stanu REQUESTING
- **REQUESTING** – po przesłaniu prośby o dzierżawę, istnieją 3 możliwe sytuacje po odpowiedzi serwera:
  a) odpowiedź serwera to DHCPACK, wysłany adres jest wolny – ustawia się timery T1 i T2 i przechodzi do BOUND
  b) odpowiedź serwera to DHCPACK, wysłany adres jest zajęty, do serwera wysyła się DHCPDECLINE i wraca do INIT
  c) odpowiedź serwera to DHCPNAK – wycofanie oferty dzierżawy, należy wrócić do INIT

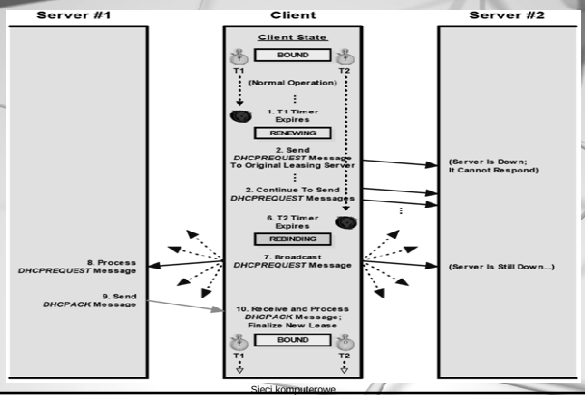
Cykl pracy klienta DHCP (cd.)

- **INIT-REBOOT** – klient z aktualną dzierżawą po restarcie przechodzi w ten stan, wysyła DHCPREQUEST i czeka na potwierdzenie dzierżawy, przechodząc do REBOOTING
- **REBOOTING** –jak w REQUESTING czeka się na odpowiedź serwera i po jej otrzymaniu albo przechodzi do BOUND, albo INIT
- **BOUND** – klient z przypisaną dzierżawą, gdy timer T1 osiąga zero klient przechodzi do RENEWING, gdy klient chce zerwać dzierżawę wysyła DHCPRELEASE i przechodzi do INIT
- **RENEWING** – klient chce odnowić dzierżawę, wysyła do dotychczasowego serwera dzierżawy DHCPREQUEST, trzy warianty: otrzymanie DHCPACK, odnowa dzierżawy i przejście do BOUND, otrzymanie DHCPNAK – odmowa dzierżawy i przejście do INIT, osiągnięcie przez timer T2 zera – przejście do REBINDING
- **REBINDING** – wysyłany okresowo DHCPREQUEST – prośba o nową dzierżawę, 3 warianty: otrzymanie DHCPACK i przejście do BOUND, DHCNAK i do INIT, brak odpowiedzi – do INIT

Proces uzyskania dzierżawy



Proces odnowy dzierżawy



Wiadomości w DHCP

- DHCP definiuje kilka rodzajów komunikatów (o tym za chwilę)
- DHCP przesyła informacje wykorzystując 67 port UDP, przy czym często stosuje adres rozgłaszania lub opiera się jedynie na warstwie drugiej TCP/IP
- DHCP w celu ograniczenia ilości transmitowanych komunikatów w przypadku braku odpowiedzi na żądanie ponawia je stosując strategie wykładniczego losowego oczekiwania tzn. czas pierwszej retransmisji to 4±1sek, drugiej: 8±1sek, trzeciej: 16±1sek, aż do 64±1sek.

Format wiadomości DHCP

00 – 07bit	08 – 15bit	16 – 23bit	24 – 31bit
OPERACJA	TYP ADRESU SPRZĘTOWEGO	DŁUGOŚĆ ADRESU SPRZĘTOWEGO	LICZBA SKOKÓW
XID (IDENTYFIKATOR TRANSAKCJI)			
SEKUND		FLAGI	
ADRES IP KLIENTA			
PRZYDZIELONY ADRES IP KLIENTA			
ADRES IP SERWERA			
ADRES IP ROUTERA			
ADRES SPRZĘTOWY KLIENTA			
NAZWA SERWERA (64 OKTETY)			
PLIK STARTOWY (128 OKTETÓW)			
OPCJE PRODUCENTA (DŁUGOŚĆ ZMIENNA)			

Opis pól

- OPERACJA – kod operacji: żądanie lub odpowiedź
- TYP ADRESU SPRZĘTOWEGO – np. 1 to Ethernet
- LICZBA SKOKÓW – klient ustawia na 0, ogranicza ilość routerów przez które wiadomość może wędrować
- XID – unikalny identyfikator komunikacji serwer-klient
- SEKUND – czas który upłynął od rozpoczęcia starań przez klienta w celu odnowy bądź uzyskania dzierżawy
- FLAGI – przede wszystkim B, która jest ustawiana przez klienta który nie ma swojego adresu IP i wymaga odpowiedzi przez rozgłoszenie
- ADRES IP KLIENTA – własny adres klienta lub zero
- PRZYDZIELONY ADRES IP
- ADRES IP SERWERA
- OPCJE – rozbudowane pole w którym kryje się moc możliwości DHCP

Pole opcji

Pole opcji umożliwia przesłanie m.in. :

- Maski podsieci, routerów w sieci lokalnej,
- Serwerów czasu, DNS, drukarek,
- Nazwę węzła i domeny,
- Ścieżki do głównego drzewa katalogów klienta w protokole NFS
- Domyślnego TTL, MTU, adresu rozgłaszania, tras, domeny NIS, serwerów rozmaitych usług…
- I co najważniejsze: rozmaitych opcji samego przydziału adresów

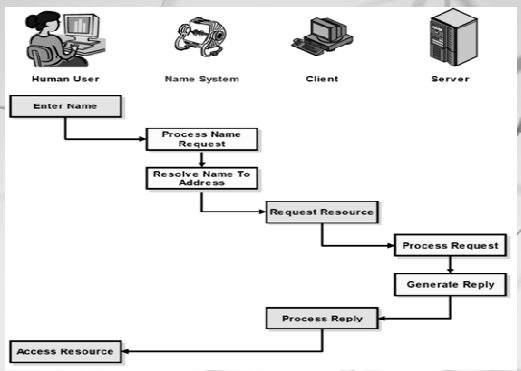
Opcje przydziału adresów

Code Value	Data Length (bytes)	Name and Description
50	4	***Requested IP Address:*** Used in a client's *DHCPDISCOVER* message to request a particular IP address assignment.
51	4	***IP Address Lease Time:*** Used in a client request to ask a server for a particular DHCP lease duration, or in a server reply to tell the client the offered lease time. It is specified in units of seconds.
52	1	***Option Overload:*** Used to tell the recipient of a DHCP message that the message's *SName* and/or *File* fields are being used to carry options, instead having their normal meanings. This option implements the option overload feature. There are three possible values for this single-byte option: *Option* Value: 1 — Option Overload Method: The *File* field is carrying option data. 2 — The *SName* field is carrying option data. 3 — Both fields are carrying option data.
53	1	***DHCP Message Type:*** Indicates the specific type of DHCP message: Option Value: 1 — DHCP Message Type: *DHCPDISCOVER* 2 — *DHCPOFFER* 3 — *DHCPREQUEST* 4 — *DHCPDECLINE* 5 — *DHCPACK* 6 — *DHCPNAK* 7 — *DHCPRELEASE* 8 — *DHCPINFORM*
54	4	***Server Identifier:*** The IP address of a particular DHCP server. The option is included in messages sent by DHCP servers to identify themselves as the source of the message. It is also used by a client in a *DHCPREQUEST* message to specify which server's lease it is accepting.
55	Variable	***Parameter Request List:*** Used by a DHCP client to request a list of particular configuration parameter values from a DHCP server.
56	Variable	***Message:*** Used by a server or client to indicate an error or other message.
57	2	***Maximum DHCP Message Size:*** Used by a DHCP client or server to specify the maximum size of DHCP message it is willing to accept. The minimum legal value is 576 bytes.
58	4	***Renewal (T1) Time Value:*** Tells the client the value to use for its renewal timer.
59	4	***Rebinding (T2) Time Value:*** Tells the client what value to use for its rebinding timer.

DNS – wprowadzenie

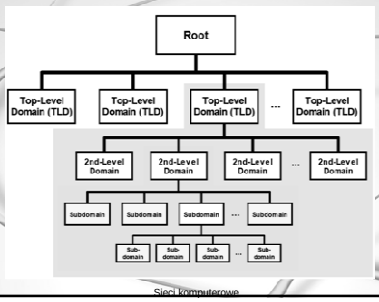
- Motywacja – adresy IP (zwłaszcza IPv6) są dla przeciętnego użytkownika intersieci nieczytelne
- Adresy domenowe to abstrakcja – zupełnie niepotrzebna z punktu widzenia funkcjonowania samej sieci Internet
- Historia DNS sięga początku lat 80-tych choć sam problem nazw węzłów sieci został zauważony już w latach 70-tych
- Główne cechy DNS to: skalowalny światowy system nazw, lokalna kontrola nad lokalnymi nazwami, rozproszona struktura, uniwersalność i niezależność od sprzętu
- DNS jako system nazw domenowych zapewnia 3 najważniejsze funkcjonalności: zdefiniowanie przestrzeni nazw, metod ich rejestrowania i tłumaczenia

Idea DNS



Przestrzeń domen – struktura hierarchiczna

Domena (ang. Domain) Słowny lub literowy element adresu DNS wykorzystywany do nazywania urządzeń (najczęściej komputerów) w Internecie.



Elementy struktury

- Domeny najwyższego poziomu to np. domeny funkcjonalne (.gov – rządowe, polityczne) czy krajowe (.pl)
- Nazwa domeny powinna spełniać następujące kryteria:
  - Długość max. 63 znaki
  - Brak symboli (poza -)
  - Brak dużych liter (a właściwie – nie są one po prostu rozróżniane)
- Nazwa domeny musi być unikalna w ramach domeny nadrzędnej
- Nazwa domenowa to ciąg nazw domen do których dany węzeł należy od domeny najniższego poziomu do najwyższego, oddzielony kropkami (max. 255 znaków)
- Identyfikator zasobu – następuje po nazwie domenowej, slash jako identyfikator katalogu w ramach węzła

Zarządzanie domenami

- Struktura hierarchiczna determinuje hierarchiczną strukturę zarządzania.
- Domenami najwyższego poziomu administrują IANA (ang. Internet Assigned Numbers Authority) i ICANN (ang. The Internet Corporation for Assigned Names and Numbers)
- W Polsce NASK – nadzór nad domeną .pl jako całością, oraz obsługa rejestrowania domen: .com.pl, .biz.pl, .org.pl, .net.pl oraz kilkudziesięciu innych domen "funkcjonalnych" oraz części domen lokalnych, np. .waw.pl. Co ciekawe domeną gov.pl zawiaduje IPPT PAN.

Serwery DNS – wprowadzenie

- Rozproszenie – brak centralnej bazy danych wszystkich domen
- Podział na strefy – zwykle tożsamy z podziałem na domeny ale nie zawsze
- Każda strefa winna posiadać 2 synchronizujące się serwery DNS: główny (ang. primary) i dodatkowy (ang. secondary), które zapewniają redundancję, równoważenie obciążenia i zwiększenie efektywności „rozwiązywania” nazw
- Dla domeny serwer istnieje serwer master którego wpisy są propagowane do serwerów podrzędnych
- Serwery Caching-DNS – buforują odpowiedzi na zapytania DNS co pozwala na szybsze ich przesłanie w przyszłości

Serwery nadrzędne DNS

Funkcje serwerów DNS

Pomijamy oczywiste aspekty związane z utrzymaniem funkcjonującej struktury systemu nazw

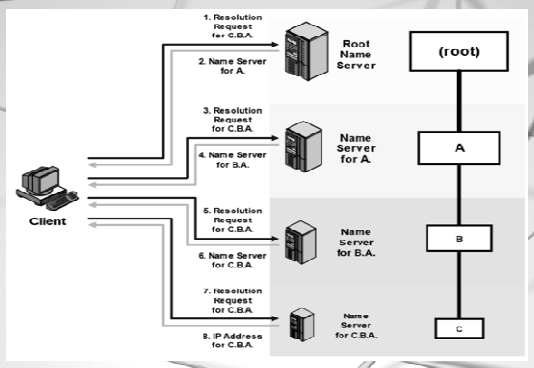
Skupmy się na:

- Typowe tłumaczenie nazw – tj. nazwy do adresu IP
- Odwrotne tłumaczenie nazw – tj. adres IP do nazwy
- Tłumaczenie adresu poczty elektronicznej

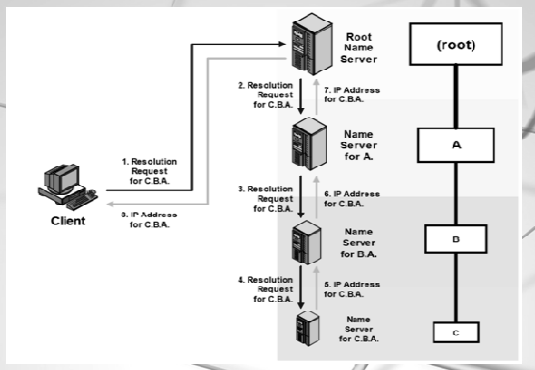
Dwie metody rozwiązywania nazw:

- Iteracyjna
- Rekursywna

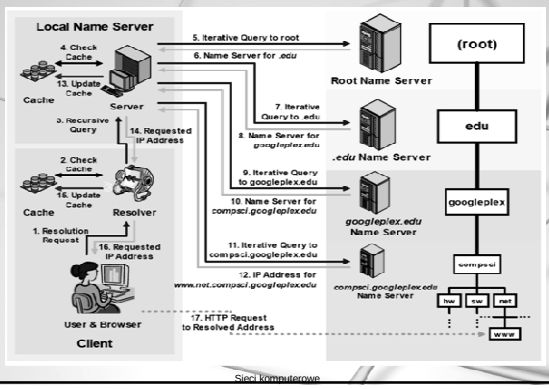
Iteracyjne tłumaczenie nazwy domenowej



Rekursywne tłumaczenie nazwy domenowej



Tłumaczenie nazw – przebieg operacji



DNS – zarys komunikacji

- Protokół DNS posługuje się do komunikacji serwer-klient głównie protokołem UDP, serwer pracuje na porcie numer 53, przesyłanie nazw domenowych pomiędzy serwerami master i slave odbywa się protokołem TCP na porcie 53.
- TCP jest używany w przypadku gdy UDP zawodzi bądź gdy komunikat jest zbyt długi
- Format komunikatu DNS:
  - NAGŁÓWEK – (ang. Header)
  - ZAPYTANIE – (ang. Question) do serwera nazw
  - ODPOWIEDŹ – (ang. Answer) zawiera rekordy będące odpowiedzią
  - ZWIERZCHNOŚĆ – (ang. Authority) wskazuje serwery zwierzchnie dla domeny
  - DODATKOWA – (ang. Additional) sekcja informacji dodatkowych

Nagłówek wiadomości DNS

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	OPCODE				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

ID – identyfikator tworzony przez program wysyłający zapytanie; serwer używa tego identyfikatora w odpowiedzi

QR – określa, czy komunikat jest zapytaniem (0) czy odpowiedzią (1)

Pola nagłówka

- **OPCODE** – określa rodzaj zapytania wysyłanego od klienta, jest przypisywany przez serwer do odpowiedzi. Wartości:
  0 – QUERY – standardowe zapytanie, 1 – IQUERY – zapytanie zwrotne, 2 – STATUS – pytanie o stan serwera,
- **AA** (Authoritative Answer) – oznacza, że odpowiedź jest autorytatywna.
- **TC** (TrunCation) – oznacza, że odpowiedź nie zmieściła się w jednym pakiecie UDP i została obcięta.
- **RD** (Recursion Desired) – oznacza, że klient żąda rekurencji – pole to jest kopiowane do odpowiedzi
- **RA** (Recursion Available) – serwer obsługuje zapytania rekurencyjne
- **RCODE (Response CODE)** kod odpowiedzi. Wartości:
  0 – brak błędu, 1 – błąd formatu – serwer nie potrafił zinterpretować zapytania, 2 – błąd serwera – wewnętrzny błąd serwera, 3 – błąd nazwy – nazwa domenowa podana w zapytaniu nie istnieje, 4 – nie zaimplementowano – serwer nie obsługuje typu otrzymanego zapytania, 5 – odrzucono – serwer odmawia wykonania określonej operacji, np. transferu strefy
- **QDCOUNT , ANCOUNT, NSCOUNT, ARCOUNT** – określają liczbę wpisów w sekcji zapytania, odpowiedzi, zwierzchności, dodatkowej


DZIĘKUJĘ ZA UWAGĘ!
ZAPRASZAM NA EGZAMIN ☺
Sieci komputerowe