33. BlueTooth – zastosowania, struktura sieci, wykorzystanie pasma

Zastosowania:

Podłączenie urządzeń o niskim poborze mocy typu telefon komórkowy, mysz słuchawki, drukarka, moduł GPS lub pikosieci o niewielkim zasięgu i ilości węzłów.

Struktura sieci:

- Podstawą działania BT jest pikosieć (piconet)
- 1 węzeł typu master (nadrzędny)
- do 7 aktywnych urządzeń typu slave (podrzędnych)
- do 255 urządzeń w stanie synchronizacji z master (stan niskiego poboru mocy)

Wykorzystanie pasma:

- Bluetooth wykorzystuje FHSS (skakanie po kanałach 1600 razy/sek)
- Sekwencję skoków dyktuje węzeł master
- dane kontrolne (nagłówki) zajmują dużą część pasma ~270kb/s

34. Wersje Blueooth

- **wersja 1.0** – 1Mb/s (efektywnie 721kb/s)
- **wersja 1.1** (802.15.1-2002) – 1Mb/s (efektywnie 721kb/s)
  – poprawiono błędy
  – możliwa transmisja bez szyfrowania
  – wskaźnik mocy sygnału
- **wersja 1.2** (802.15.1-2005) – 1Mb/s (efektywnie 721kb/s)
  – szybsze rozpoznawanie
  – poprawiony algorytm AFH skoków po kanałach
  – poprawiona transmisja synchroniczna audio
  – poprawiony HCI (obsługa UART)
- **wersja 2.0** (różnie wg różnych źródeł)
  – równoważna 1.2 + poprawione błędy
- **wersja 2.0 + EDR** – 3Mb/s (efektywnie 2,1Mb/s)
  – kompatybilna wstecznie z 1.1
  – zwiększona prędkość
  – niższe zużycie energii
- **wersja 2.1 -2007r**
  zwiększono ilość informacji wymienianej przez urządzenia
  – polepszono szyfrowanie danych
  – zwiększono szybkość i bezpieczeństwo parowania
  – zredukowano zużycie energii 3 do 10 razy (szczególnie dla
  – HID – myszy BT itp.)

- **wersja 3.0**
  – zwiększenie szybkości (480Mb/s)
  – zmniejszenie zużycia energii
  – nowe usługi

35. Klasy mocy BT

- Klasa 1 (class 1) – 100mW zasięg do 100m
- Klasa 2 (class 2) – 2,5mW zasięg do ok. 10m
- Klasa 3 (class 3) – 1mW zasięg do 1m

36. Stos protokołów BT

•Podstawowe
- – Baseband – wszystko co się wiąże z obsługą pasma
- – LMP – (Link Management Protokol)
  - » Protokół kontroli i zarządzania łącza
- – L2CAP (Logical Link and Adaptation Protocol)
  - » przeplata dane różnych protokołów
  - » obsługuje segmentacje i scalanie pakietów
  - » QoS
- – BNEP – emulacja sieci
- – SDP – Service Discovery Protocol
  - » wykrywanie usług

• Pozostałe
- – rfcomm – emulacja urządzeń szeregowych
- – Telefoniczne
  - » TCS Binary
  - » AT Commands
- – protokoły aplikacyjne
  - » ppp
  - » IP/TCP/UDP
  - » OBEX
  - » WAP/WAE
  - » vCard/vCal

37. Usługi BT

Discovery – rozpoznawanie sieci
– Audio - transmisja dźwięku
– Control - kontrola
– Rfcomm - emulacja portu szeregowego do podłączania myszy, klawiatury, modemu itp.
– Telephony - umożliwia transmisję dźwięku w czasie rzeczywistym
– LLC - do połączenia sieciowego

38. Informacje udostępniane przez urządzenie BT

• Każde urządzenie przesyła
- – nazwę
- – klasę
- – listę usług
- – informacje techniczne (wersję BT, przesunięcie zegara, producenta ...)

• Użycie usługi może wymagać „parowania”
• Niektóre urządzeni mogą nie odpowiadać kiedy są już podłączone (np słuchawka BT)

39. Zabezpieczenie transmisjii Bluethooth

– Bezpieczeństwo danych
- • Ustanowienie połączenia szyfrowanego bazuje na PIN
- • przy pomocy algorytmu E22 generuje się ciąg szyfrujący E0 używany do szyfrowania transmisji

– Uwagi co do bezpieczeństwa
- • klucz pin można odtworzyć przez wymuszenie przez trzecie urządzenie ponownego parowania
  - – PIN o długości 4 znaków można odtworzyć w 6 sekund!
  - – powinno stosować się PINy > 6 znaków
  - – wyłączać BT kiedy jest nie potrzebny
  - – zmieniać domyślną politykę akceptowania połączeń

40. Zasada działania sieci GSM/UMTS, pasma częstotliwości

GSM jest siecią komórkową
– urządzenie przenośne szuka komórek (nadajników)
– nawiązuje połączenie ze stacją bazową o najlepszych warunkach transmisji

GSM działanie sieci:

- Wykorzystuje CDMA
- w strukturze sieci znajdują się cyfrowe centrale telefoniczne SS7
- głos o częstotliwości 300-3400Hz jest kodowany cyfrowo, szyfrowany i przesyłany do sieci
- definiowane są usługi zintegrowane z siecią
  – fax
  – SMS
  – poczta głosowa
  – identyfikacja numeru
  – itp
- telefon łączy się z siecią za pomocą stacji bazowej
- transmisja odbywa się na wielu częstotliwościach
- dla każdej częstotliwości jest 8 szczelin czasowych
  – rozmowa może zajmować 1 lub 0,5 szczeliny z pogorszeniem jakości (do 16 rozmów na jednej częstotliwości)

GSM częstotliwości:
cecha/system GSM400 GSM850 GSM900 GSM1800 GSM1900
liczba częst. 35 124 174 374 299

- pasmo 900 MHz ma mniejszą ilość częstotliwości (równoczesnych rozmów) ale większy zasięg
- pasmo 1800 stosuje się w miejscach o dużej gęstości telefonów

UMTS (Universal Mobile Telecommunications System)
- system 3G
  – używa W-CDMA (poszerzone pasmo do 5MHz)
  – usługi Video
  – nowy interfejs radiowy
    » polepszony został znacznie transfer danych pomiędzy abonentem a siecią, co zaowocowało poprawą jakości oferowanych usług

41. Transmisja danych w sieciach GSM/UMTS/LTE

– Usługi szybkiej transmisji danych(UMTS)
– HSPA High Speed Packet Access
» od 144kbps do 2Mbps W-CDMA 5MHz pasmo
– HSPA+, I-HSPA, HSPA Evolution – Wersja 7 HSPA
» 42/22Mb/s z MIMO
– HSDPA High Speed Downlink Packet Access (2006)
» do 14,4Mb/s modulacja QPSK i 16QAM
– HSUPA High Speed Uplink Packet Access (Nokia) EUL Enhances UpLink do 11,5Mb/s
– HSOPA/LTE High Speed OFDM Packet Access do 100Mb/s downlink i 50Mb/s uplink
» zmienne pasmo 1,25 do 20MHz

– Usługi szybkiej transmisji danych(UMTS rev 8 (pre 4G))

- wykorzystuje OFDM i MIMO
- transmisja pakietowa - HSOPA/LTE
- pełna integracja z IP
- usługi głosowe VOIP
- przepustowość 1 – 100Mb/s
- Streaming HDTV/DVB
- SDR – Software Defined Radio
  – dla zapewnienia zgodności z dotychczasowymi rozwiązaniami

Interfejs radiowy **LTE** używa technologii OFDM do transmisji danych od stacji bazowej do telefonu. Transmisja w kierunku przeciwnym (od telefonu w górę) wykorzystuje SC-FDMA (DFTS-FDMA). Jest to jedna z najbardziej widocznych różnic w stosunku do UMTS, który bazuje na WCDMA.

42. Adresowanie w sieci IPv4, klasy, zasady adresowania

Adresowanie:

W IPv4, czyli obecnym standardzie adresowania internetu, adres IP to liczba 32-bitowa (od 0 do 4294967295), zapisywana w porządku big endian. Liczby w adresie IP nazywają się oktetami, ponieważ w postaci binarnej mają one osiem bitów. Te osiem bitów daje w sumie 256 kombinacji, więc każdy oktet przedstawia liczbę od 0 do 255.

Klasy:

klasa A: zakres bitów na pierwszym bajcie 00000000 do 01111111, czyli adresy IP od 0.0.0.0 do 127.255.255.255, przy czym adresy od 127.0.0.0 do 127.255.255.255 są wykorzystywane dla programowej pętli testowej - loopback. Maska sieciowa 8-mio bitowa: 255.0.0.0, inny zapis maski: /8;

klasa B: zakres bitów na pierwszym bajcie 10000000 do 10111111, czyli adresy IP od 128.0.0.0 do 191.255.255.255. Maska sieciowa 16-to bitowa: 255.255.0.0; inny zapis maski: /16;

klasa C: zakres bitów na pierwszym bajcie 11000000 do 11011111, czyli adresy IP od 192.0.0.0 do 223.255.255.255. Maska sieciowa 24-ro bitowa: 255.255.255.0; inny zapis maski: /24;

klasa D: zakres bitów na pierwszym bajcie 11100000 do 11101111, czyli adresy IP od 224.0.0.0 do 239.255.255.255. Przeznaczona dla multicastu.

klasa E: zakres bitów na pierwszym bajcie 11110000 do 11111111, czyli adresy IP od 240.0.0.0 do 255.255.255.255. Zarezerwowana dla celów badawczych

43. Adres IP/maska/numer sieci/adres broadcast – obliczanie

44. Adresy nieroutowalne

Dla sieci LAN przyznano pewne nieroutowalne adresy (tzn. służące tylko do komunikacji w wewnętrznej sieci, bez dostępu do Internetu). Są to

Klasa adresów	Maska podsieci	Zakres adresów IP (od)		(do)
Klasa A	255.0.0.0	10.0.0.0	-	10.255.255.255
Klasa B	255.255.0.0	172.16.0.0	-	172.31.255.255
Klasa C	255.255.255.0	192.168.0.0	-	192.168.255.255

Powyższe adresy służą tylko i wyłącznie do komunikacji w LAN-ie.

45. Adresy klasy D

Adresy klasy D to tzw. adresy grupowe, wykorzystywane przy przesyłaniu wiadomości do grupy komputerów w Internecie. Tego typu system umożliwia znaczne zmniejszenie ruchu w sieci w stosunku do systemu nawiązywania oddzielnych połączeń z każdym z użytkowników. Obecnie istnieją jednak lepsze techniki rozgłaszania wiadomości grupowych w sieci.

46. porty w połączeniu TDP/UDP

TCP jest protokołem działającym w trybie klient-serwer. Serwer oczekuje na nawiązanie połączenia na określonym porcie. Klient inicjuje połączenie do serwera.

W przeciwieństwie do UDP, TCP gwarantuje wyższym warstwom komunikacyjnym dostarczenie wszystkich pakietów w całości, z zachowaniem kolejności i bez duplikatów. Zapewnia to wiarygodne połączenie kosztem większego narzutu w postaci nagłówka i większej liczby przesyłanych pakietów. Chociaż protokół definiuje pakiet TCP, to z punktu widzenia wyższej warstwy oprogramowania, dane płynące połączeniem TCP należy traktować jako ciąg oktetów. W szczególności – jednemu wywołaniu funkcji API (np. send()) nie musi odpowiadać wysłanie jednego pakietu. Dane z jednego wywołania mogą zostać podzielone na kilka pakietów lub odwrotnie – dane z kilku wywołań mogą zostać połączone i wysłane jako jeden pakiet (dzięki użyciu algorytmu Nagle'a). Również funkcje odbierające dane (recv()) w praktyce odbierają nie konkretne pakiety, ale zawartość bufora stosu TCP/IP, wypełnianego sukcesywnie danymi z przychodzących pakietów.

Port nadawcy – 16-bitowy numer identyfikujący port nadawcy.

Port odbiorcy – 16-bitowy numer identyfikujący port odbiorcy.

Numer sekwencyjny – 32-bitowy identyfikator określający miejsce pakietu danych w pliku przed fragmentacją (dzięki niemu, można "poskładać" plik z poszczególnych pakietów).

Numer potwierdzenia – 32-bitowy numer będący potwierdzeniem otrzymania pakietu przez odbiorcę, co pozwala na synchronizację nadawanie-potwierdzenie.

Długość nagłówka – 4-bitowa liczba, która oznacza liczbę 32-bitowych wierszy nagłówka, co jest niezbędne przy określaniu miejsca rozpoczęcia danych. Dlatego też nagłówek może mieć tylko taką długość, która jest wielokrotnością 32 bitów.

Zarezerwowane – 4-bitowy ciąg zer, zarezerwowany dla ewentualnego przyszłego użytku.

Flagi 8-bitowa informacja/polecenie dotyczące bieżącego pakietu. Poszczególne flagi oznaczają:

- **CWR** – (ang. Congestion Window Reduced) flaga potwierdzająca odebranie powiadomienia przez nadawcę, umożliwia odbiorcy zaprzestanie wysyłania echa.
- **ECE** – (ang. ECN-Echo) flaga ustawiana przez odbiorcę w momencie otrzymania pakietu z ustawioną flagą CE
- **URG** – informuje o istotności pola "Priorytet"
- **ACK** – informuje o istotności pola "Numer potwierdzenia"
- **PSH** – wymusza przesłanie pakietu
- **RST** – resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)
- **SYN** – synchronizuje kolejne numery sekwencyjne
- **FIN** – oznacza zakończenie przekazu danych

Szerokość okna – 16-bitowa informacja o tym, ile danych może aktualnie przyjąć odbiorca. Wartość 0 wskazuje na oczekiwanie na segment z innym numerem tego pola. Jest to mechanizm zabezpieczający komputer nadawcy przed zbyt dużym napływem danych.

Suma kontrolna – 16-bitowa liczba, będąca wynikiem działań na bitach całego pakietu, pozwalająca na sprawdzenie tego pakietu pod względem poprawności danych.

Wskaźnik priorytetu – jeżeli flaga URG jest włączona, informuje o ważności pakietu.

Opcje – czyli ewentualne dodatkowe informacje i polecenia:

- **0** – koniec listy opcji
- **1** – brak działania
- **2** – ustawia maksymalna długość segmentu

W przypadku opcji **2** to tzw. **Uzupełnienie**, które dopełnia zerami długość segmentu do wielokrotności 32 bitów (patrz: informacja o polu "Długość nagłówka")

Porty w połączeniu UDP:

Port nadawcy

identyfikuje port, z którego została wysłana wiadomość, kiedy znaczący to wskazuje port wysyłającego procesu i może zostać przyjęty jako port, do którego powinna zostać zwrócona wiadomość zwrotna w przypadku braku innej informacji. Port nadawcy jest polem opcjonalnym. Gdy pole to nie jest używane przyjmuje wartość zero.

Port odbiorcy

identyfikuje port odbiorcy i jest polem wymaganym.

Długość

16-bitowe pola specyfikują długość w bajtach całego datagramu: nagłówek i dane. Minimalna długość to 8 bajtów i jest to długość nagłówka. Wielkość pola ustala teoretyczny limit 65,527 bajtów, dla danych przenoszonych przez pojedynczy datagram UDP.

Suma kontrolna

16 bitowe pole, które jest użyte do sprawdzania poprawności nagłówka oraz danych. Pole jest opcjonalne. Ponieważ IP nie wylicza sumy kontrolnej dla danych, suma kontrolna UDP jest jedyną gwarancją, że dane nie zostały uszkodzone.

47. Stos protokołów TCP/IP vs modele OSI, protokoły poszczególnych warstw ARP, IP, ICMP, IGMP, TCP, UDP

48. ICMP i jego rola w diagnostyce

ICMP (ang. Internet Control Message Protocol, internetowy protokół komunikatów kontrolnych) – opisany w RFC 792 protokół warstwy sieciowej OSI/TCP/IP wykorzystywany w diagnostyce sieci oraz trasowaniu. Pełni przede wszystkim funkcję kontroli transmisji w sieci. Jest wykorzystywany w programach ping oraz traceroute..

Zastosowania:

Poniższa lista zawiera kilka sytuacji, z powodu których bramy lub hosty mogą wysyłać komunikaty ICMP:

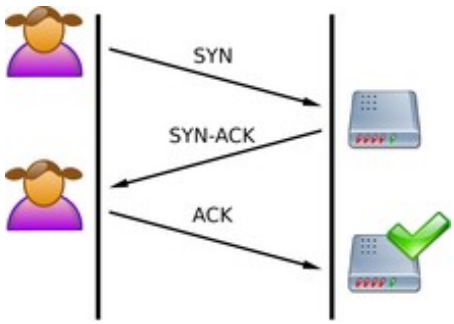
- Gdy ruter lub host jest zbyt obciążony, by móc przyjąć do buforów kolejne datagramy, komunikaty ICMP służą do zwolnienia szybkości napływania datagramów do danego rutera.
- Gdy ruter lub host znajduje lepsza trasę do miejsca przeznaczenia, może wysłać do hosta źródłowego komunikat ICMP, powiadamiający o krótszej trasie.
- Gdy host docelowy jest nieosiągalny, ostatnia brama wysyła komunikat ICMP z powrotem do hosta źródłowego, informując o niedostępności adresata.
- Gdy host lub brama przetwarza pakiet o TTL równym 0 hopów, wówczas odrzuca ten pakiet i ewentualnie wysyła komunikat ICMP do hosta źródłowego.

49. Różnice pomiędzy protokołami warstwy transportowej budowa pakietów TCP i UDP.

1. TCP –połączeniowy
2. UDP – bezpołączeniowy

50. Nawiązywanie połączenia w protokole TCP

Nawiązywanie połączenia



three-way handshake

Charakterystyczny dla TCP jest moment nawiązania połączenia, nazywany *three-way handshake*. Host inicjujący połączenie wysyła pakiet zawierający segment TCP z ustawioną flagą SYN (*synchronize*). Host odbierający połączenie, jeśli zechce je obsłużyć, odsyła pakiet z ustawionymi flagami SYN i ACK (*acknowledge* – potwierdzenie). Inicjujący host powinien teraz wysłać pierwszą porcję danych, ustawiając już tylko flagę ACK (i gasząc SYN). Jeśli host odbierający połączenie nie chce lub nie może odebrać połączenia, powinien odpowiedzieć pakietem z ustawioną flagą RST (*reset*).

Transmisja danych

W celu weryfikacji wysyłki i odbioru TCP wykorzystuje sumy kontrolne i numery sekwencyjne pakietów. Odbiorca potwierdza otrzymanie pakietów o określonych numerach sekwencyjnych ustawiając flagę ACK. Brakujące pakiety są retransmitowane. Host odbierający pakiety TCP defragmentuje je i porządkuje je według numerów sekwencyjnych tak, by przekazać wyższym warstwom modelu OSI pełen złożony segment.

Zakończenie połączenia

Prawidłowe zakończenie połączenia może być zainicjowane przez dowolną stronę. Polega ono na wysłaniu pakietu z ustawioną flagą FIN (*finished*). Pakiet taki wymaga potwierdzenia flagą ACK. Najczęściej po otrzymaniu pakietu z flagą FIN, druga strona również kończy komunikację wysyłając pakiet z flagami FIN i ACK. Pakiet taki również wymaga potwierdzenia przez przesłanie ACK.

Dopuszcza się również awaryjne przerwanie połączenia poprzez przesłanie pakietu z flagą RST (*reset*). Pakiet taki nie wymaga potwierdzenia.

51. Stany połączenia serwera i klienta TCP.

Połączenie TCP może znajdować się w jednym z następujących stanów:

LISTEN
Gotowość do przyjęcia połączenia na określonym porcie przez serwer.
SYN-SENT
Pierwsza faza nawiązywania połączenia przez klienta. Wysłano pakiet z flagą SYN. Oczekiwanie na pakiet SYN+ACK.
SYN-RECEIVED
Otrzymano pakiet SYN, wysłano SYN+ACK. Trwa oczekiwanie na ACK. Połączenie jest w połowie otwarte (ang. half-open).
ESTABLISHED
Połączenie zostało prawidłowo nawiązane. Prawdopodobnie trwa transmisja.
FIN-WAIT-1
Wysłano pakiet FIN. Dane wciąż mogą być odbierane ale wysyłanie jest już niemożliwe.
FIN-WAIT-2
Otrzymano potwierdzenie własnego pakietu FIN. Oczekuje na przesłanie FIN od serwera.
CLOSE-WAIT
Otrzymano pakiet FIN, wysłano ACK. Oczekiwanie na przesłanie własnego pakietu FIN (gdy aplikacja skończy nadawanie).
CLOSING
Połączenie jest zamykane.

LAST-ACK
Otrzymano i wysłano FIN. Trwa oczekiwanie na ostatni pakiet ACK.
TIME-WAIT
Oczekiwanie w celu upewnienia się, że druga strona otrzymała potwierdzenie rozłączenia. Zgodnie z RFC 793 połączenie może być w stanie TIME-WAIT najdłużej przez 4 minuty.
CLOSED
Połączenie jest zamknięte.

52. Flagi w TCP

1. SYN- synchronizacja
2. ACK- aktywny
3. RST- reset
4. ECE- ustawiana przez odbiorcę gdy otrzyma flage CE
5. URG- informuje o istotności pola priorytet

53. Przykłady protokołów w aplikacji (porty i wykorzystanie prot w warstwie transportowej)

SSH, POP3, SMTP, FTP

SSH (ang. secure shell) to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer.

Post Office Protocol version 3 (POP3) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP. Ogromna większość współczesnych internautów korzysta z POP3 do odbioru poczty.

SMTP (ang. Simple Mail Transfer Protocol) – protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie. Standard został zdefiniowany w dokumencie RFC 821 a następnie zaktualizowany w 2008 roku w dokumencie RFC 5321

SMTP zaczęło być szeroko używane we wczesnych latach osiemdziesiątych dwudziestego wieku. W tamtym okresie było to uzupełnienie UUCP, który lepiej sprawdzał się przy przekazywaniu poczty między maszynami posiadającymi jedynie okresowe połączenie. SMTP natomiast lepiej działa, gdy zarówno maszyna nadająca jak odbierająca są na stałe przyłączone do sieci.

FTP (ang. File Transfer Protocol – Protokół Transferu Plików) – protokół typu klient-serwer, który umożliwia przesyłanie plików z serwera i na serwer poprzez sieć TCP/IP. Protokół ten jest zdefiniowany przez IETF w RFC 959. **FTP** jest protokołem 8-bitowym, dlatego nie wymaga specjalnego kodowania danych na postać 7-bitową, tak jak ma to miejsce w przypadku poczty elektronicznej

54. Enkapsulacja protokołów

Enkapsulacja protokołów, logicznie odseparowane funkcje są poddawane abstrakci poprzez ukrywanie ich w obiektach wyższego poziomu.

55. IPv6 , IPv4 porównanie

Funkcja	IPv4	IPv6
Adresy	32 bity	128
Wsparcie dla IPSec	Opcjonalnie	Wymagane
Fragmentacja	Przez nadającego hosta i routery	Przez nadającego hosta
Suma kontrolna w nagłówku	Obecna	Brak
Opcje	W nagłówku	W nagłówkach dodatkowych
Ramki zgłoszeń	ARP	Ramki zgłoszeń ARP Wielopoziomowe

		wiadomości typu Neighbor Solicitation
Przydzielanie adresu	Ręcznie lub dhcp	Nie wymaga nic

56. Routing, reguła routowania, rodzaje, teblice routingu

1. reguła routowania – jeśli adres nie znajduje się w sieci lokalnej, to ruch kierowany jest do bramy domyślnej
2. rodzaje
- statyczne, przesyłane są pakiety przez z góry określone porty
- dynamiczne- porty są dynamicznie wybierane
3. tablica routingu – tablica na podstawie której routery kierują pakiety do docelowych stacji

57. Protokół HTTP, porty, metody żądań

1. Porty 80 dla WWW, 8080 dla Proxy
2. metody żądań
i. Options – żądanie informacji o połączeniu
ii. Get żądanie zasobów
iii. HEAD jak Get, ale w odp. Nie może być treści
iv. POST żądanie nie widoczne w url
v. Put stosowany do umieszczania np. pliku na serwerze

58. DNS co to jest, wykorzystane porty i protokół w transportowej, funkcjonowanie resolvera w systemie operacyjnym

DNS (ang. Domain Name System, system nazw domenowych) to system serwerów, protokół komunikacyjny oraz usługa zapewniające zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki wykorzystaniu DNS nazwa mnemoniczna, np. pl.wikipedia.org, może zostać zamieniona na odpowiadający jej adres IP, czyli 91.198.174.232 Usługa DNS warstwy aplikacji modelu TCP/IP, jest związana z portem 53 TCP/UDP.

59. Struktura DNS serwery root, rodzaje serwerów DNS

1. serwery Root podstawowe DNS, rozwiązuje podstawowe domeny np. pl.org
2. rodzaje serwerów DNS
i. primary – zawiera strefę dla której jest podstawowym źródłem rekordów
ii. secondary pobiera plik serwera podstawowego
iii. caching odpowiada na zapytania klientów i przechowuje odpowiedzi przez czas TT

Struktura domen:

Wewnątrz każdej domeny można tworzyć tzw. subdomeny – stąd mówimy, że system domen jest 'hierarchiczny'. Przykładowo wewnątrz domeny .pl utworzono wiele domen:

- regionalnych jak 'opole.pl', 'dzi erzoniow.pl' czy 'warmia.pl'
- funkcjonalnych jak 'com.pl', 'gov.pl' czy 'org.pl'
- należących do firm, organizacji lub osób prywatnych jak 'wp.pl', 'zus.pl', 'porady-domowe.pl'

Nazwy domen i poszczególnych komputerów składają się z pewnej liczby nazw, oddzielonych kropkami. Ostatnia z tych nazw jest domeną najwyższego poziomu. Każda z tych nazw może zawierać litery, cyfry lub znak '-'. Od niedawna w nazwach niektórych domen można używać znaków narodowych (IDN) takich jak 'ą' czy 'ż'. Trwają prace nad nowymi standardami odpowiadającymi DNS, które będą obsługiwać kodowanie Unicode, co pozwoli na umieszczanie w nazwach domen dowolnych znaków np. polskich albo chińskich równocześnie. W Polsce domeny zawierające znaki diakrytyczne praktycznie nie występują. Wewnątrz każdej z poddomen można tworzyć dalsze poddomeny, np. w domenie 'wikipedia.org' można utworzyć domenę pl.wikipedia.org.

Root „.”

- Stanowią podstawowe serwery DNS zawierające wskazania dla domen podstawowych
- Aktualna lista znajduję się pod adresem
  - http://www.iana.org/about/popular-links/
  - A listę operatorów na http://www.root-servers.org/
  - Obecnie (5.01.2009) zawiera 13 serwerów root
    - Ograniczenie ustalono na na limit defragmentacji pakietu
      Ipv4 (576B) - co daje maks. 15 rekordów (IPv6 jest więcej)

Serwery root:

DNS to również protokół komunikacyjny opisujący sposób łączenia się klientów z serwerami DNS. Częścią specyfikacji protokołu jest również zestaw zaleceń, jak aktualizować wpisy w bazach domen internetowych. Na świecie jest wiele serwerów DNS, które odpowiadają za obsługę poszczególnych domen internetowych. Domeny mają strukturę drzewiastą, na szczycie znajduje się **13 głównych serwerów (root servers)** obsługujących domeny najwyższego poziomu (TLD – top level domains)

60. Tryby zapytań DNS

1. Rekursywne
2. Nie rekursywne

61. Domeny struktura i nazewnictwo domen DNS

Od końca.

62. Typy rekordów DNS

Najważniejsze typy rekordów DNS, oraz ich znaczenie:

- **rekord A** lub **rekord adresu (ang. address record)** mapuje nazwę domeny DNS na jej 32-bitowy adres IPv4.
- **rekord AAAA** lub **rekord adresu IPv6 (ang. IPv6 address record)** mapuje nazwę domeny DNS na jej 128-bitowy adres IPv6.
- **rekord CNAME** lub **rekord nazwy kanonicznej (ang. canonical name record)** ustanawia alias nazwy domeny. Wszystkie wpisy DNS oraz poddomeny są poprawne także dla aliasu.
- **rekord MX**lub **rekord wymiany poczty (ang. mail exchange record)** mapuje nazwę domeny DNS na nazwę serwera poczty oraz jego priorytet.
- **rekord PTR** lub **rekord wskaźnika (ang. pointer record)** mapuje adres IPv4 lub Ipv6 na nazwę kanoniczną hosta. Określenie rekordu PTR dla nazwy hosta (ang. *hostname*) w domenie `in-addr.arpa` (IPv4), bądź `ip6.arpa` (IPv6), który odpowiada adresowi IP, pozwala na implementację odwrotnej translacji adresów DNS (ang. *reverse DNS lookup*).
- **rekord NS** lub **rekord serwera nazw (ang. name server record)** mapuje nazwę domenową na listę serwerów DNS dla tej domeny.
- **rekord SOA** lub **rekord adresu startowego uwierzytelnienia (ang. start of authority record)** ustala serwer DNS dostarczający *autorytatywne* informacje o domenie internetowej, łącznie z jej parametrami (np. TTL).
- **rekord SRV** lub **rekord usługi (ang. service record)** pozwala na zawarcie dodatkowych informacji dotyczących lokalizacji danej usługi, którą udostępnia serwer wskazywany przez adres DNS. (mało istotne)
- **TXT** – rekord ten pozwala dołączyć dowolny tekst do rekordu DNS. Rekord ten może być użyty np. do implementacji specyfikacji Sender Policy Framework.