

1. Modele warstwowe OSI i TCP/IP.

OSI:

7. **aplikacji** -Bezpośredni dostęp sieciowy dla aplikacji
6. **prezentacji** -Reprezentacja danych, szyfrowanie i deszyfrowanie, konwertowanie danych zależnych od platformy sprzętowej do postaci uniwersalnej
5. **sesji** - Komunikacja między hostami
4. **transportowa** - Komunikacja między hostami
3. **sieciowa** -Określanie trasy i adresowanie logiczne
2. **łącza danych** -Adresowanie fizyczne
1. **fizyczna** - Media, sygnały i transmisja binarna

TCP/IP

Aplikacji
Transportowa
Internetu
Łącza

2. Przepustowość i opóźnienie.

Przepustowość:

- 1.W komunikacji elektronicznej – szerokość pasma częstotliwości która może być wykorzystana do przesyłania danych
- 2.W sieciach komp. – utożsamiane z szybkością transferu danych(ilość danych jakie można przenieść z jednego punktu do drugiego w danym czasie)

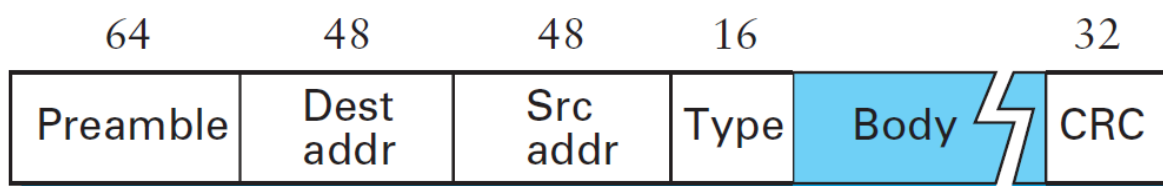
Opóźnienie:

czas potrzebny na dotarcie wiad. Z jednego punktu sieci do drugiego np. 24ms

3. Metody wykrywania błędów w transmisji danych.

1. Parzystość wykrywa wszystkie błędy 1-3 bitowe i większość 4 bitowych
2. Cykliczny Kod Nadmiarowy (CRC)
3. Dzielenie „bitowych” wielomianów
4. Realizacja CRC
5. stop-and-wait
6. sliding window

4. Ethernet: ramka, adresowanie, transmisja i odbiór danych.



- Preambuła – synchronizacja, symbol początku ramki
- 48-bitowe adresowanie
- Typ przenoszonego protokołu wyższej warstwy lub – w standardzie IEEE 802.3 – długość pola danych
- Dane – min. 46 do max. 1500 bajtów
- CRC – 32-bitowe: $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$

ADRESOWANIE:

- Każde urządzenie korzystające z sieci Ethernet powinno mieć swój UNIKALNY adres sprzętowy MAC (ang. media access control)
- Każdy producent posiada własny prefiks adresu
- Adres – 48 bitowy np.

00001000 00000000 00101011 11100100 10110001 00000010

ODBIÓR Każdy interfejs sieciowi odbiera ramki

1. Adresowane do niego
2. Wysłane na adres rozgłoszeniowy
3. Wysłane na adres grupowy
4. Wszystkie jeśli został ustawiony w tryb nasłuchu

5. Algorytm CSMA/CD, technologia AutoMDIX.

- CSMA - metoda rozproszonej koordynacji transmisji : kiedy urządzenie lub węzeł w sieci posiada dane, które chce przesłać - nasłuchuje łącza, sprawdzając czy jakieś inne urządzenie nie przesyła danych w linii transmisyjnej.
- CD - urządzenie wysyłające dane, będzie monitorowało swoją własną transmisję (czy sygnał w kablu jest taki sam jak sygnał przez niego wysyłany), w celu wykrycia kolizji.



- Auto MDIX** funkcja przełącznika sieciowego lub karty sieciowej typu polegająca na automatycznym rozpoznaniu przez to urządzenie, czy podłączony kabel sieciowy jest skrosowany, czy prosty.

6. Gigabit Ethernet – nowe elementy

- Medium - skrętka co najmniej 5 kategorii, zasięg max. 100 m. wykorzystuje wszystkie 4 pary przewodu.
- Czas transmisji ramki 512 ns (poprzednio 51,2 μ s).
- Zastosowane kodowania 8B1Q4 i 4D-PAM5 przetwarzają osiem bitów na jedną serię czterech sygnałów (grup kodowych) o poziomach napięć z pięciowartościowego zbioru $\{2,1,0,-1,-2\}$ V, wysyłanych jednocześnie.
- Nowa ramka posiada minimalny rozmiar 512 B, zawiera w sobie klasyczne ramki ethernetowe.
- Przesyłanie ramek wiązkami (ang. frame bursting, burst) – przesyłanie naraz sekwencji ramek do osiągnięcia ich sumy bajtów równej 8192. Jeśli cała paczka ma mniej niż 512 B, to stosowane jest dodatkowo dopełnienie

7. Adresowanie w IPv4 (klasy, adresy specjalnego przeznaczenia i prywatne, CIDR, podział na podsieci – praktycznie)

Maski podsieci – umożliwiające dodatkowy podział sieci klasy A, B lub C na podsieci o określonym, nie zawsze idealnie dostosowanym do wymagań, rozmiarze

Bezklasowy wybór trasy między domenami (ang. Classless Inter-Domain Routing, w skrócie: CIDR) – zakłada eliminację idei klas i podział całej dostępnej przestrzeni adresowej na podsieci o dokładnie określonej wielkości. Obecnie to dominująca metoda

Maski podsieci – umożliwiające dodatkowy podział sieci klasy A, B lub C na podsieci o określonym, nie zawsze idealnie dostosowanym do wymagań, rozmiarze

Bezklasowy wybór trasy między domenami (ang. Classless Inter-Domain Routing, w skrócie: CIDR) – zakłada eliminację idei klas i podział całej dostępnej przestrzeni adresowej na podsieci o dokładnie określonej wielkości. Obecnie to dominująca metoda

SPECJALNE PRZEZNACZENIE ADRESÓW IP

- Adres sieciowy** – odnosi się do samej sieci, a nie komputera. Sufiks adresu jest wypełniony zerami np. 192.168.10.0.
- Adres rozgłaszania kierunkowego (ang. broadcast)** – odnosi się do wszystkich komputerów w sieci. Sufiks adresu wypełniony jedynekami np. 192.168.10.255 albo zerami (tzw. rozgłaszanie Berkeley-historyczne) np. 192.168.10.0.
- Adres rozgłaszania ograniczonego** – odnosi się do rozgłaszania w lokalnej sieci (używane przy starcie systemu). Prefiks i sufiks wypełniony jedynekami tj. 255.255.255.255.
- Adres bieżącego komputera** – odnosi się do lokalnego komputera (używane przy starcie systemu). Prefiks i sufiks wypełnione zerami tj. 0.0.0.0.
- Adres pętli zwrotnej (ang. loopback)** – identyfikuje lokalną pętlę zwrotną umożliwiającą testowanie/aplikacji/serwerów/ usług. Prefiks 127, sufiks – dowolny. Np. 127.0.0.1

8. Datagram IPv4.

bity											
słowa	0	4	8	12	16	20	24	28	31		
1	Wersja	IHL	Typ usługi		Długość całkowita					Nagłówek	
2	Identyfikator				Flagi	Przesunięcie fragmentacji					
3	Czas życia	Protokół	Suma kontrolna								
4	Adres źródła										
5	Adres przeznaczenia										
6	Opcje						Uzupełnienie				
7	DANE										

- Wersja [4 bity] – numer wersji protokołu IP np. 0100 to IPv4, 0110 i IPv6
- IHL [4 bity] – długość nagłówka (ang. IP Header Length) w 32-bitowych słowach, minimalnie = 5, maksymalnie 15 (czyli 60 bajtów)
- TOS [8 bitów] – typ/jakość usługi (ang. Type of Service) lub tzw. Differentiated Services
- Długość całkowita [16 bitów] – długość całkowita pakietu IP w bajtach (zawiera nagłówek i dane) . Łatwo zatem obliczyć że max. objętość przenoszonych danych to 65535B, rzeczywista zależy od MTU (ang. Maximum Transfer Unit) warstwy łącza – niezbędna jest ich fragmentacja (dzielenie pakietu na mniejsze części).
- Identyfikator [16 bitów] – numer identyfikacyjny pakietu
- Flagi [3 bity] – flagi sterujące fragmentacją:
 - bit nr 0: zarezerwowany, musi mieć wartość zero
 - bit nr 1: (DF) 0 – można, 1 – nie wolno fragmentować
 - bit nr 2: (MF) 0 – ostatni fragment, 1 – będzie więcej
- Przesunięcie fragmentacji [13 bitów] – wskazuje, do którego miejsca pakietu danych należy fragment. Przesunięcie mierzone jest w jednostkach 8 bajtów (64 bitów). Pierwszy fragment ma przesunięcie równe zero.
- Czas życia [8 bitów] – w skrócie TTL (ang. Time-to-Live) , wskazuje maksymalny czas przebywania pakietu w Internecie, mierzony w praktyce liczbą skoków (ang. hops) między routerami, ustawiany początkowo na pewną wartość i stopniowo (przy każdym skoku) zmniejszany, przy TTL=0 pakiet jest odrzucany
- Protokół [8 bitów] – wskazuje oznaczenie protokołu warstwy wyższej, do którego zostaną przekazane dane z pakietu, np.
 - 01h – ICMP, 06h – TCP, 11h – UDP
- Suma kontrolna [16 bitów] – suma kontrolna nagłówka
- Adresy źródła i przeznaczenia [32 + 32 bity]
- Opcje [zmienne] – opcje protokołu
- Uzupełnienie [32bity – długość pola opcji]
- Dane [zmienne]

9. Metody odwzorowywania adresów. ARP – funkcjonalność i zastosowania.

METODY

Tablicowa – odwzorowania są przechowywane w tablicy (zwykle tworzonej dynamicznie), która w razie potrzeby jest przeszukiwana przez oprogramowanie

Obliczeniowe – adres protokołowy przydzielony komputerowi jest wybrany w taki sposób, żeby można było go przekształcić w adres sprzętowy za pomocą ciągu operacji arytmetycznych i logicznych

Sieciowe – w celu odwzorowania adresów komputery przesyłają w sieci komunikaty z zapytaniami (o adres sieciowy węzła) i odpowiedziami (ten adres zawierający)

- ARP to sieciowa metoda odwzorowywania adresów, opracowana pierwotnie dla sieci Ethernet w latach 80-tych XX wieku.
- Klient ARP poza przysyłaniem komunikatów przechowuje tabelę odwzorowywania adresów, z której wpisy usuwane są automatycznie po pewnym, zależnym od implementacji protokołu czasie.
- ARP definiuje 2 rodzaje komunikatów:
 - żądanie (ang. request) – rozgłaszane w sieci lokalnej
 - odpowiedź (ang. reply) – węzła o adresie w żądaniu

W obu przypadkach wiadomość protokołu ARP zawiera adres sprzętowy i IP, zarówno nadawcy, jak i odbiorcy, co pozwala na obustronną aktualizację tablic

10. Algorytm routingu IPv4 .

1. Przeszukać tablicę routingu w poszukiwaniu rekordu, który odpowiada adresowi przeznaczenia IP. Jeśli taki adres został znaleziony – wyślij pakiet do wskazanego rutera będącego ruterem następnego przejścia lub do bezpośrednio

next-hop routing

1. Przeszukać tablicę routingu w poszukiwaniu rekordu, który odpowiada adresowi przeznaczenia IP. Jeśli taki adres został znaleziony – wyślij pakiet do wskazanego rutera będącego ruterem następnego przejścia lub do bezpośrednio dołączonego interfejsu.
2. Przeszukać tablicę routingu w poszukiwaniu rekordu, który odpowiada adresowi sieci. Jeśli taki adres został znaleziony – wyślij pakiet do wskazanego rutera będącego ruterem następnego przejścia lub do bezpośrednio dołączonego interfejsu.
3. Przeszukać tablicę routingu w poszukiwaniu rekordu oznaczonego jako "domyślny" (ang. default). Jeśli zostanie znaleziony, wyślij pakiet do wskazanego rutera następnego przejścia.

Jeśli żaden z tych trzech kroków nie przyniesie rezultatu, datagram zostaje uznany jako taki, którego nie można dostarczyć a do aplikacji wysyłającej datagram wysyłany jest komunikat o błędzie.

Uwaga: w procesie przekazywania pakietów adres adresata pozostaje niezmienny!

Protokoły routingu dynamicznego

Tablice routingu muszą być nieustannie uaktualniane (dostosowywane do bieżącego stanu sieci), w sposób zapewniający efektywne jej wykorzystanie. W tym celu opracowano protokoły routingu dynamicznego, pozwalające na wymianę informacji między routerami.

Podstawowe metody routingu dynamicznego:

- Metoda wektora odległości (ang. distance vector routing), nazywana często algorytmem Bellmana-Forda
- Metoda stanu łącza (ang. link-state routing) nazywana też często algorytmem najkrótszej ścieżki

RIP (Routing Information Protocol) to najbardziej znany protokół routingu dynamicznego oparty o metody wektora odległości. Najnowsze odmiany tego protokołu to RIP-2 i RIPv6 opracowany dla IPv6.

Główne cechy:

- Odległość mierzona w skokach (ang. hops), maksymalna długość trasy to 16 węzłów (odp. Destination unreachable)
- Dwa typy komunikatów
 - zapytanie (ang. request) – wysyłane przez router np. przy jego włączeniu, może dotyczyć całej tabeli bądź jej części
 - odpowiedź (ang. response) – wysyłana w odpowiedzi na zapytanie i stale, co 30 sekund
- Dodatkowe timery usuwające dawno nieaktualizowane wpisy
- Wsparcie domyślnej trasy (oznaczonej 0.0.0.0) i multicasting (w RIP-2)

W metodach stanu łącza każdy router przesyła jedynie dostępne mu informacje dotyczące połączeń do najbliższych mu węzłów tzw. Link-State Packet (LSP). Wybór trasy polega na składaniu tego typu informacji w spójną całość.

Każdy z routerów rozesła tzw. link-state packet zawierający identyfikator oraz listę węzłów do niego przyłączonych wraz z kosztem tych połączeń.

Trasa obliczana jest na podstawie grafowego algorytmu Dijkstry.

11. ICMP – główne zastosowania.

Protokół ICMP (ang. Internet Control Message Protocol) został opracowany jako uzupełnienie protokołu IP w zakresie niezawodności i jakości transmisji. Nie zapewnia on jej bezpośrednio, natomiast pozwala na przesyłanie komunikatów kontrolnych.

Protokół ICMP pracuje w warstwie internetu, a do przekazywania wiadomości wykorzystuje datagramy IP.

Wykrywanie nieosiągalnych miejsc przeznaczenia

Jeśli komputer docelowy nie odpowiada system, który wykrył problem wysyła do nadawcy komunikat *Destination Unreachable* (typ 3). Jeśli komunikat ten jest wysyłany przez router, oznacza, że router nie może wysłać pakietów do danego komputera. Może to nastąpić w dwóch przypadkach:

- adres docelowy IP nie istnieje
- router nie może dostarczyć datagramu do tej sieci

W momencie, gdy komunikat ten jest wysyłany przez host, może to oznaczać, że:

dany komputer nie posiada wsparcia dla któregoś z protokołów warstw wyższych lub port protokołu TCP jest nieosiągalny.

Informowanie o „zaginionych datagramach”

Jeśli jakiś datagram, podczas przechodzenia przez ruter osiągnie zerowy limit „czasu życia” (*Time-to-Live*) jest usuwany. Do komputera źródłowego danego datagramu wysyłany jest komunikat ICMP *Time-exceeded* (typ 11, kod 0).

Sprawdzanie zdalnego hosta

Odbywa się m.in. poprzez wywołanie komendy ping. Wysyłany jest komunikat ICMP *Echo Message* (typ 8, kod 0), po otrzymaniu którego komputer docelowy musi odpowiedzieć komunikatem *Echo Reply* (typ 0, kod 0). Jeśli tego nie zrobi, uznawany jest za nieosiągalny

Sterowanie przepływem danych

W przypadku, gdy komputer docelowy transmisji IP nie nadąża za obróbką przychodzących datagramów IP, ICMP wysyła komunikat *Source Quench* (typ 4, kod 0), po którym nadawca czasowo wstrzymuje transmisję.

Przekierowywanie ścieżek

Jeśli komputer, do którego dotarł datagram IP uzna, że właściwszą bramką będzie inny komputer z tej samej sieci, wysyła komunikat *Redirect* (typ 5, kody różnorakie) wskazujący na ten właśnie komputer (musi znajdować się w tej samej sieci). Po otrzymaniu takiego komunikatu nadawca aktualizuje swoją tablicę routingu.

Inne przykłady: Rozgłaszanie routerów, maski podsieci itp.

12. UDP – własności i pola wiadomości.

UDP jest bardzo prostym protokołem warstwy transportowej opracowanym na początku lat 80.

UDP implementuje przesyłanie danych pomiędzy dwoma procesami odległych węzłów

UDP nie zapewnia:

- połączenia (wiadomości są po prostu „wypychane” przez łącze) i wykrywania zagubionych komunikatów
- potwierdzeń i gwarancji dostarczenia wiadomości
- kontroli przepływności oraz właściwej kolejności dostarczenia wiadomości

WIADOMOSC UDP

Bity 0-15 Bity 0-15

PORT ŹRÓDŁOWY PORT PRZEZNACZENIA

DŁUGOŚĆ SUMA KONTROLNA

DANE

13. TCP – główne cechy, pola segmentu i flagi, nawiązanie i zakończenie połączenia.

Protokół TCP jest powiązany wspólną historią z protokołem IP, początkowo stanowiły one jeden spójny protokół sieciowy

Cechy:

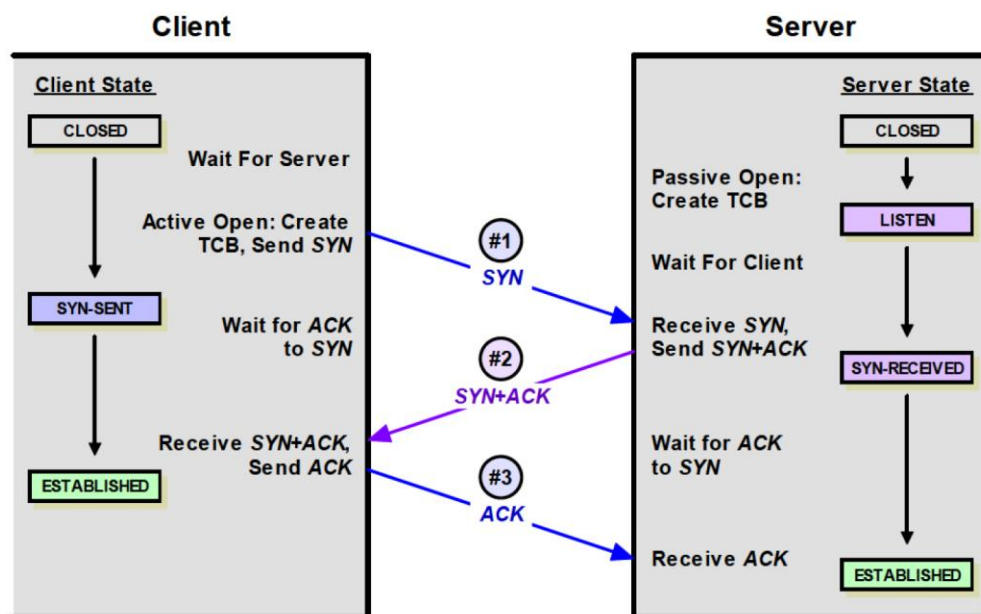
- Zorientowany na połączenie – obie strony je nawiązują i obie strony mogą przysyłać do siebie dane (dwukierunkowy)
- Obsługa wielu połączeń równocześnie
- Niezawodny – sprawdza integralność danych, zapewnia ich retransmisję w przypadku błędu, definiuje potwierdzenia
- Strumieniowy – pozwala na transmisję strumienia danych, sam dzieląc je na segmenty w zależności od potrzeb, zapewnia także kontrolę przepływności

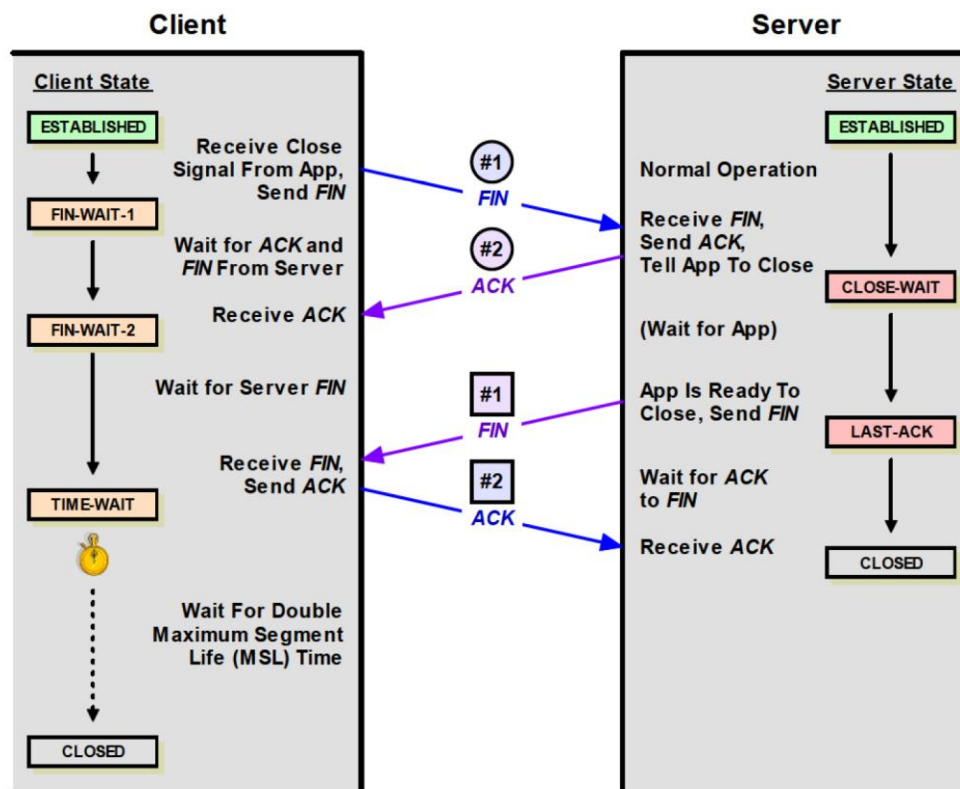
W TCP w celu efektywnego i niezawodnego przesyłania danych między węzłami nawiązywane są połączenia.

Segment TCP zawiera specjalne pole definiujące flagi, określające typ komunikatu przez ten segment przenoszonego, flagi te będą opisane później, na razie ograniczmy się do scharakteryzowania następujących:

- **URG** – segment priorytetowy (pole Urgent Pointer wskazuje koniec danych o priorytetowej „wartości”)
- **ACK** – segment potwierdzenia
- **PSH** – dane powinny być natychmiast przekazane do wyższej warstwy
- **RST** – funkcja resetująca połączenie („delta mamy problem”)
- **SYN** – segment synchronizacji numerów sekwencji
- **FIN** – segment sygnalizujący chęć zakończenia połączenia

Three-way handshake (nawiązanie połączenia TCP)





14. Metody przydziału adresów IPv4 w DHCP. Cykl dzierżawy, odliczanie czasu w procesie odnowy dzierżawy, wiadomości w DHCP (w tym przesyłane przez nie opcje konfiguracyjne).

DHCP pozwala na auto konfigurację 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

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)							

- 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
- 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 strategię wykładniczego losowego oczekiwania tzn. czas pierwszej retransmisji to 4 ± 1 sek, drugiej: 8 ± 1 sek, trzeciej: 16 ± 1 sek, aż do 64 ± 1 sek.

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

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 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.

15. System nazw – domena, nazwa domenowa, funkcje serwerów DNS, metody rozwiązywania nazw.

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

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

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

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.

OPIS DNS

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, równowagę obciążenia i zwiększenie efektywności „rozwiązywania” nazw

Dla domeny serwer istnieje serwer master którego wpisy są propagowane do serwerów podrzędnych

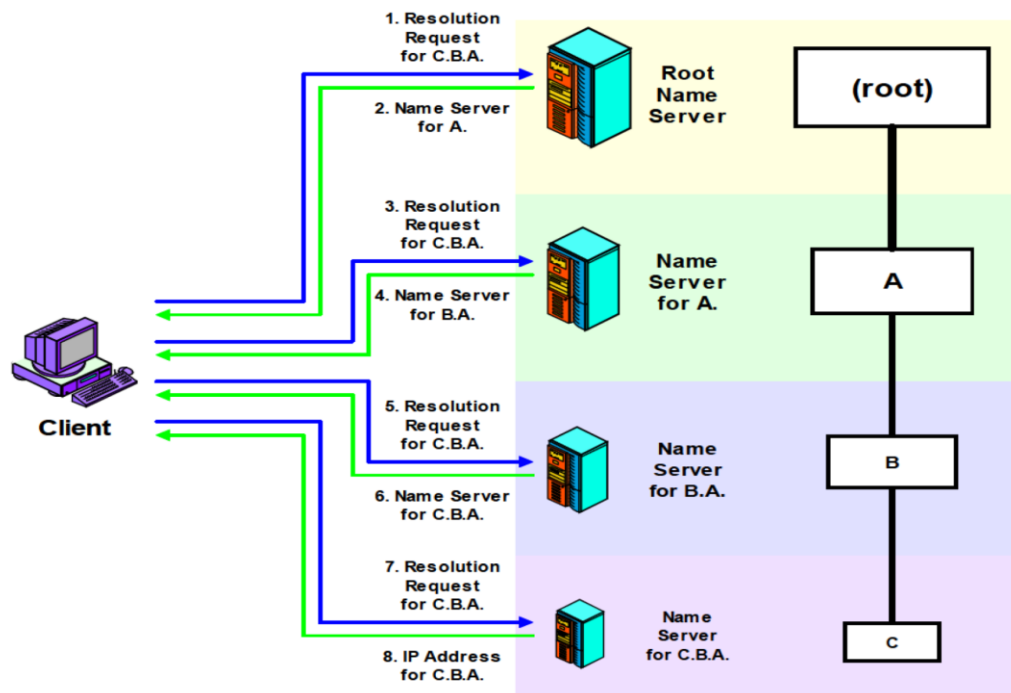
Serwery Caching-DNS – buforują odpowiedzi na zapytania DNS co pozwala na szybsze ich przesłanie w przyszłości

Funkcje DNS

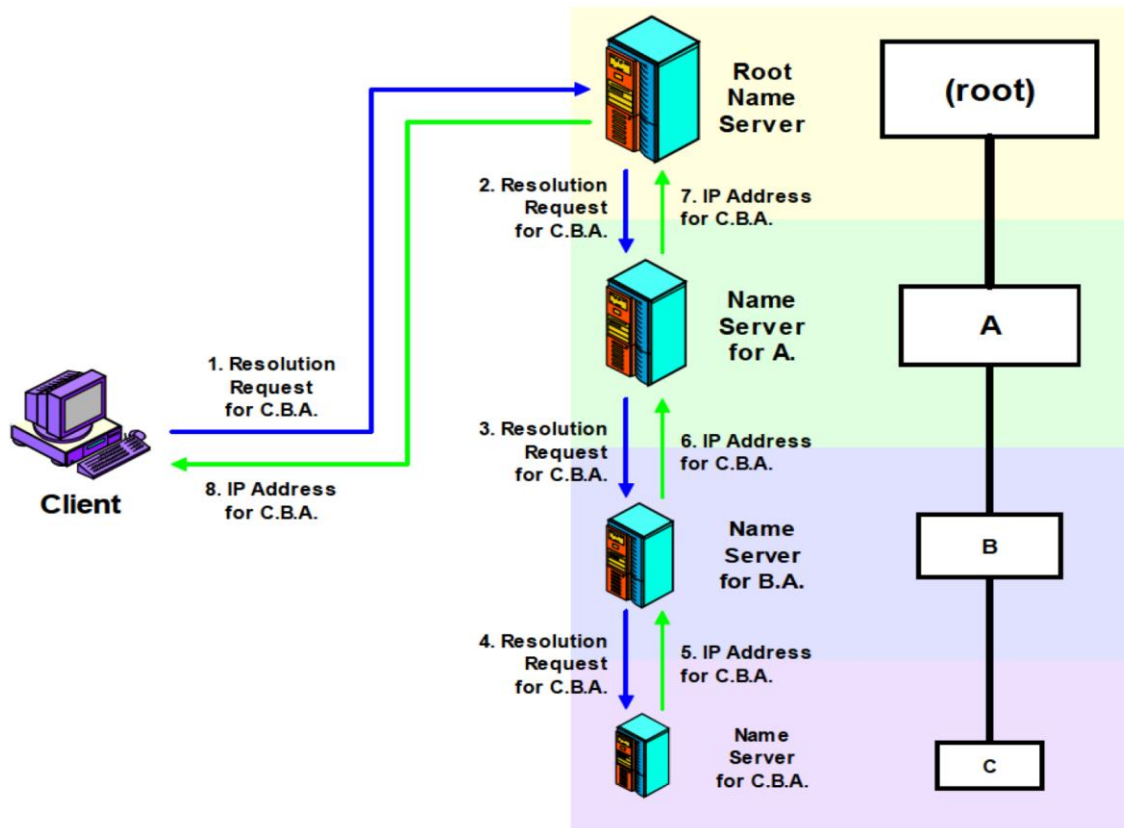
- Typowe tłumaczenie nazw – tj. nazwy do adresu IP
- Odwrotne tłumaczenie nazw – tj. adres IP do nazwy
- Tłumaczenie adresu poczty elektronicznej

Dwie metody rozwiązywania nazw:

- Iteracyjna



- Rekursywna



16. Protokół HTTP - identyfikatory zasobów, obsługiwane metody.

Początki protokołu HTTP (ang. Hypertext Transfer Protocol) sięgają 1990 roku. Od wersji 1.0 pozwala on na przesyłanie poza czystym tekstem także różnego rodzaju danych o charakterze binarnym (obrazy, dźwięki, animacje). Obecnie obowiązuje wersja HTTP/1.1

Istotą WWW jest struktura hipertekstowa. Hipertekst rozumiany jest jako tekst z możliwością tworzenia odnośników do innych treści/dokumentów

Na WWW składają się, poza protokołem HTTP, który służy do przesyłania informacji także: HTML (ang. Hypertext Markup Language) czyli język tworzenia dokumentów oraz URI (ang. Universal Resource Identifier) czyli sposób jednoznacznej identyfikowania zasobów (w HTTP używane są URL – UR Locators)

HTTP pracuje w architekturze klient-serwer, definiując żądania i odpowiedzi na nie

HTTP wykorzystuje do przesyłania wiadomości protokół TCP z nawiązywaniem indywidualnych połączeń. HTTP/1.1 podtrzymuje połączenia tworząc sesje

- **url-path** – identyfikator zasobu na serwerze HTTP; ma tu znaczenie wielkość liter

Ogólny schemat internetowego URL:

`<scheme>://<user>:<password>@<host>:<port>/<url-path>;<params>?<query>#<fragment>`

Składnia URL w HTTP:

`http://<user>:<password>@<host>:<port>/<url-path>?<query>#<bookmark>`

Metody http:

Podstawowe:

- GET – pobierz zasób
- HEAD – to samo co GET ale bez właściwej treści (używana np. po to by sprawdzić czy zasób istnieje)
- POST – przesłanie danych do serwera, URL określa np. nazwę programu który dane ma przetworzyć

Rzadko spotykane:

- OPTIONS – prośba o informacje o dostępnych opcjach transmisji
- PUT – umieszczanie informacji na serwerze pod adresem URL
- DELETE i TRACE – skasuj zasób (genialne!), prośba o przesłanie kopii żądania (dla celów diagnostycznych)

17. Poczta elektroniczna – struktura wiadomości, elementy systemu (funkcje protokołów).

Poczta elektroniczna w protokole TCP/IP nie stanowi pojedynczego protokołu a raczej ich zestaw, wraz z dodatkowymi komponentami takimi jak np. sposób właściwego adresowania

Elementy systemu poczty elektronicznej: standard wiadomości e-mail, przesyłanie poczty (do serwera pocztowego odbiorcy), jej ew. przetworzenie i odbiór przez adresata

Protokoły: transport poczty – Simple Mail Transfer Protocol (SMTP), odbiór poczty – Post Office Protocol (POP) lub Internet Message Access Protocol (IMAP)

Struktura wiadomości e-mail

- Nagłówek

Date (data wysłania)

To, CC (kopia), Bcc (tajna kopia)

Reply-to (odpowiedź ślij pod adres)

In-reply-to, References (identyfikator pierwotnej wiadomości na którą odpowiadamy i wiadomości powiązanych)

Message-ID (unikalny identyfikator)

Subject (temat)

Received (otrzymano od – dodawane przez serwery na ścieżce wiadomości)

Content-type – pozwala na przesyłanie treści o różnorodnym charakterze zgodnie ze standardem MIME (ang. Multipurpose Internet Mail Extensions)

- Pusta linia
- Treść wiadomości

18. Elementy sieci P2P BitTorrent.

- Peer (ang. pośrednik) - użytkownik, który w danym momencie pobiera lub udostępnia dany plik
- Seeder (ang. obsiewacz) - użytkownik, który posiada kompletny plik i udostępnia go innym osobom
- Chunk (ang. kawałek) – fragment pliku (zwykle 64kb-4MB) na który dzielony jest plik celem zwiększenia efektywności współdzielenia
- Tracker (ang. tropiciel) - serwer przekazujący informacje (adresy IP) o innych użytkownikach pobierających dany plik i posiadanych przez nich kawałkach
- Plik .torrent - metaplik zawierający niezbędne informacje (między innymi zawartość archiwum i adres trackera, sumy kontrolne plików) do rozpoczęcia pobierania pliku.
- Info hash - 160-bitowa wartość zakodowana algorytmem SHA1 i zapisana w metapliku .torrent. Służy do identyfikacji przez trackera pliku .torrent oraz użytkowników ściągających te same dane.
- Share ratio (ang. współczynnik dzielenia się) - wyliczany przez wielu klientów BitTorrent stosunek ilości danych wysłanych do pobranych.
- Leecher (ang. pijawka) - w większości przypadków rozumiany jest jako użytkownik, który w danym momencie pobiera dany plik i udostępnia posiadane jego fragmenty (gdy zakończy pomyślnie pobieranie stanie się Seederem). Czasami pojęciem tym jest określana osoba mająca niskie Share ratio.

19. IPv6 – główne cechy, adresowanie (od typów adresów do adresów specjalnego przeznaczenia), bezstanowa autokonfiguracja, datagram – ogólne informacje.

Główne cechy

128-bitowe adresy, z hierarchicznym podziałem ich przestrzeni

Rozwinięte mechanizmy transmisji grupowej

Sprawną autokonfigurację hostów

Nowy format datagramów, z rozszerzalnymi nagłówkami dla różnych typów informacji

Rozwinięte mechanizmy QoS (ang. quality of service) i bezpieczeństwa danych

Zmodernizowane techniki fragmentacji i routingu

Zgodność (współdziałanie) z sieciami pracującymi z IPv4

IP w wersji 6 definiuje następujące typy adresów:

- **Adres jednostkowy** (ang. unicast address) – taki adres odpowiada pojedynczemu węzłowi sieci
- **Adres rozsyłania grupowego** (ang. multicast address) – taki adres odpowiada zbiorowi węzłów znajdujących się być może w różnych miejscach (członkostwo można zmieniać), datagram przesłany pod ten adres jest dostarczany do każdego członka grupy
- **Adres grona** (ang. anycast address) – taki adres odpowiada zbiorowi komputerów o wspólnym prefiksie adresu (zwykle w jednej lokalizacji). Datagram dostarczany jest do jednego węzła, do którego np. ścieżka jest najkrótsza.

Podział przestrzeni adresów

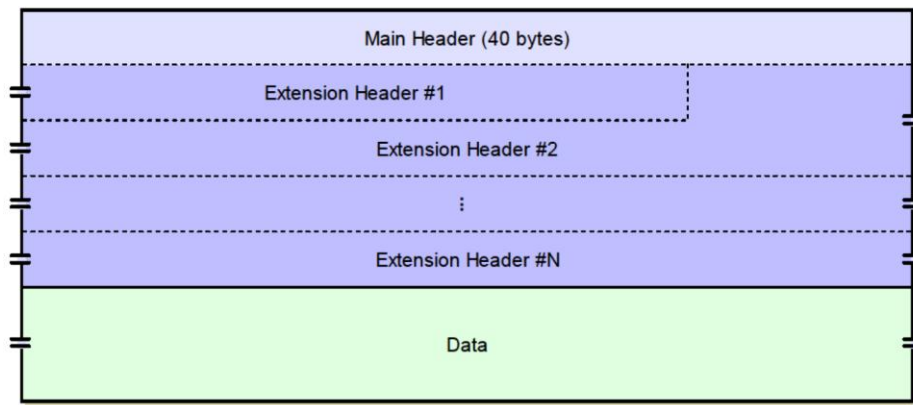
- Paradoksalnie w IPv6 powrócono do koncepcji podziału przestrzeni adresów podobnej do klas z IPv4.
- W IPv6 występują prefiksy adresów o zmiennej długości (pierwotnie od 3 do 10 bitów, zmienne) które określają grupę adresów, przykładowo:
 - 0000 0000 to prefiks adresów specjalnego przeznaczenia takich jak: adres pętli zwrotnej, adres nieokreślony, adres IPv4
 - 1111 1111 to prefiks adresów rozsyłania grupowego, zatem każdy adres zaczynający się od FF jest adresem typu multicast
 - 001 to prefiks adresów jednostkowych – czyli tych najbardziej nas interesujących

IPv6 używa tzw. **bezstanowej autokonfiguracji** węzła (tj. przypisania mu adresu IP), kolejne kroki tej procedury to:

- Przypisanie węzłowi adresu prywatnego (odpowiedni prefiks tj. 1111 1110 10 + 54 zera + zmodyfikowany EUI-64)
- Test jednoznaczności adresu (tj. czy któryś z węzłów w sieci nie używa identycznego adresu) z użyciem protokołu wykrywania sąsiadów (ang. IPv6 Neighbour Discovery), gdy jest konflikt generujemy nowy adres, gdy nie ma – możemy go używać do komunikacji w sieci lokalnej
- Kontakt z najbliższym routerem który informuje czy węzeł może użyć bezstanowej konfiguracji tj. do prefiksu sieci dodać swój identyfikator czy też użyć DHCP dla konfiguracji adresu

Datagram protokołu IPv6 w sposób oczywisty różni się od datagramu IP w wersji 4. Podstawowe jego cechy w zestawieniu z IPv4 to:

- „wielonagłówkowość” (nagłówek główny + nagłówki dodatkowe)
- zmniejszenie ilości pól (np. brak długości nagłówka – stała wartość i sumy kontrolnej), zmiana nazw itp.
- lepsze wsparcie dla mechanizmów priorytetowego przesyłania danych (QoS)



20. Standardy sieci bezprzewodowych. Ogólna architektura sieci 802.11 w trybie infrastructure, typy ramek. Proces skanowania. Dostęp do nośnika: problem ukrytego węzła, mechanizm CSMA/CA.

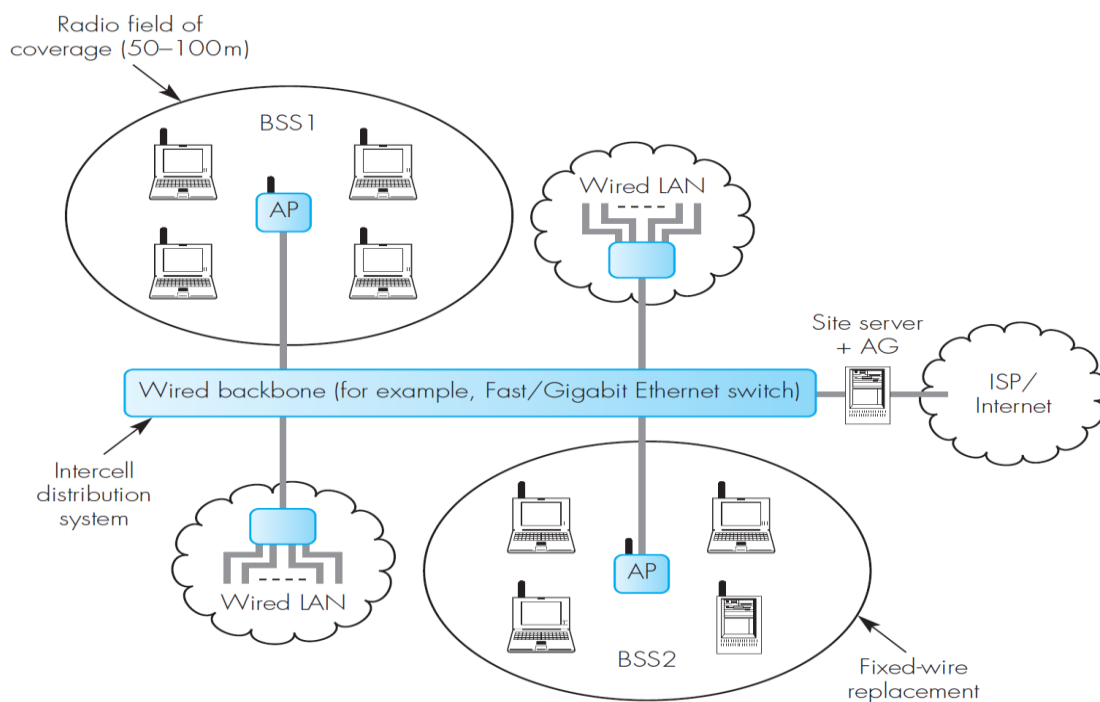
Podstawowe typy technologii stosowanych w sieciach bezprzewodowych, z podziałem ze względu na zasięg działania:

- **Sieci osobiste o niewielkim zasięgu** (ang. wireless personal area network, WPAN) – sieci standardu IEEE 802.15, np. Bluetooth
- **Bezprzewodowe sieci lokalne** (ang. wireless local area networks, WLAN) – sieci standardu IEEE 802.11, opatrzone znakiem towarowym Wi-Fi (tj. wireless fidelity)
- **Bezprzewodowe sieci o dużym zasięgu** (ang. wireless wide area networks, WWAN) – sieci standardów radiowej komunikacji komórkowej np. GSM, GPRS, UMTS, HSDPA, IEEE 802.16 (WI-MAX)

Ogólna architektura sieci 802.11 – tryb infrastructure

AP – Access point (punkt dostępowy);

Wszystkie urządzenia komunikują się tylko z AP, który spełnia funkcję bramy (do sieci przewodowej) i pośredniczy w komunikacji pomiędzy urządzeniami sieci



W sieciach 802.11 występują następujące typy ramek:

- Ramki kontrolne (ang. Control Frames)
- Ramki zarządzające (ang. Management Frames)

- Ramki danych (ang. Data Frames)

Wieloramkowość wynika z dodatkowych czynności jakie muszą być zrealizowane na wstępie (przed dokonaniem transmisji)
np. oczyszczenie kanału, ustalenie fizycznego dostępu, uwierzytelnienie oraz przerywanie połączeń

Ramki w sieciach 802.11 są formatowane wg określonego ogólnego schematu.

Skanowanie pasywne - polega na przeglądaniu przez stację wszystkich kanałów w poszukiwaniu wysyłanych okresowo ramek zarządzających typu *beacon* – odebranie takiej ramki pozwala na ustalenie identyfikatora SSID, kanału pracy, obsługiwanych prędkości oraz poziomu sygnału radiowego dostępnej sieci bezprzewodowej.

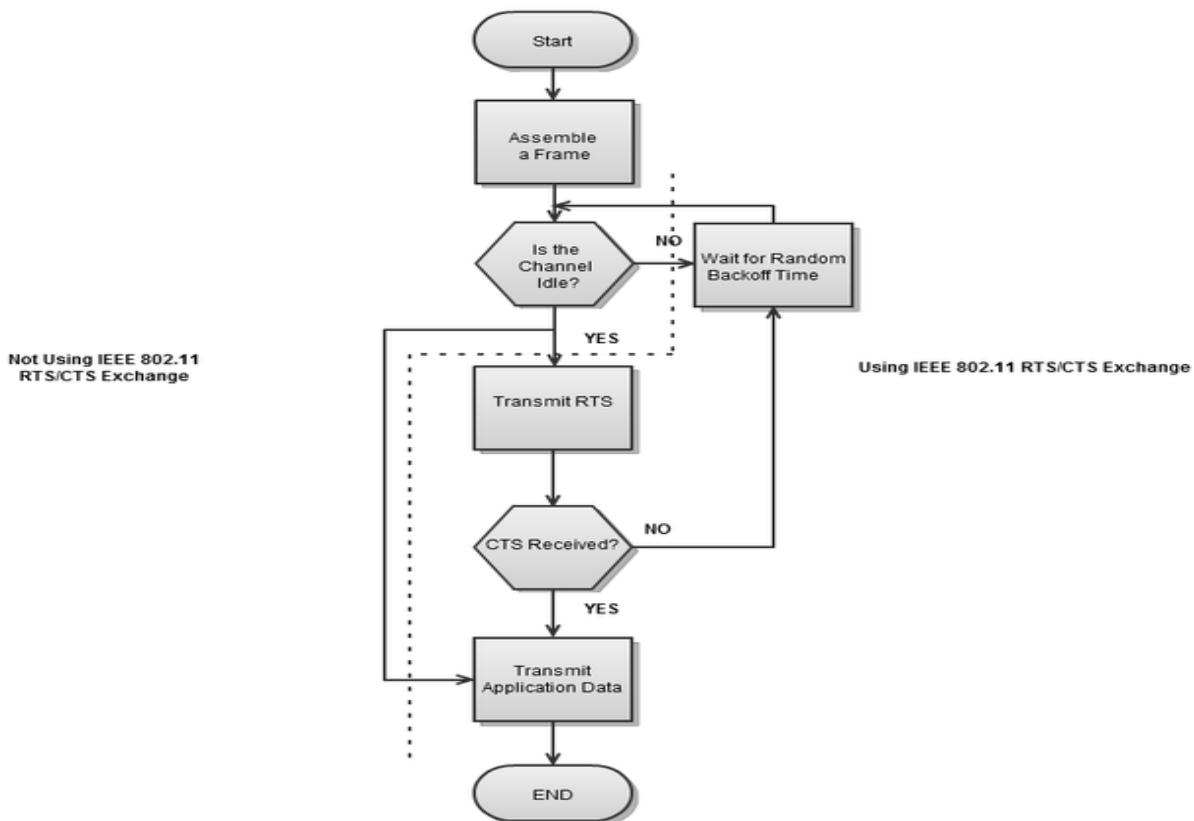
Skanowanie aktywne –

1. Próbkowanie – wysyłanie *probe request* na każdym kanale
2. Odebranie odpowiedzi – *probe response* – od każdego dostępnego AP

Dostęp do nośnika:

- Sieć standardu 802.11 realizuje funkcje rozproszonej koordynacji transmisji (ang. distributed control function, DCF). Główną techniką DCF wykorzystywaną w tych sieciach jest CSMA/CA czyli wielodostęp do łącza z wykrywaniem nośnej i unikaniem kolizji (ang. carrier sense multiple access/collision avoidance)
- Mechanizm CSMA/CA może być dodatkowo uzupełniony o potwierdzenia RTS i CTS (ang. *request to send* i *clear to send*)
- Zastosowanie RTS i CTS pozwala częściowo uniknąć problemu węzła ukrytego tj. sytuacji gdy dwie stacje nie będące w zasięgu transmisji radiowej usiłują równocześnie nadać informację do trzeciej

Mechanizm CSMA/CA



21. Routing statyczny a dynamiczny – różnice oraz wady i zalety.

#Zalety Statycznego:

- Router przesyła pakiety przez z góry ustalone interfejsy bez konieczności każdorazowego obliczania tras, co zmniejsza zajętość cykli procesora i pamięci.
- Informacja statyczna nie jest narażona na deformację spowodowaną zanikiem działania dynamicznego routingu na routerach sąsiednich.
- Dodatkowo zmniejsza się zajętość pasma transmisji, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego. Zapewnia również konfigurację tras domyślnych, nazywanych bramkami ostatniej szansy (gateway of the last resort). Jeżeli router uzna, iż żadna pozycja w tablicy routingu nie odpowiada poszukiwanemu adresowi sieci docelowej, korzysta ze statycznego wpisu, który spowoduje odesłanie pakietu w inne miejsce sieci

#Wady Statycznego:

Routing statyczny wymaga jednak od administratora sporego nakładu pracy w początkowej fazie konfiguracji sieci, nie jest również w stanie reagować na awarie poszczególnych tras.

#Zalety Dynamicznego:

Adaptacja do zmiennych warunków w sieci. Oznacza to, że routery reagują na wszelkie nieprawidłowości oraz zmiany parametrów podczas pracy sieci, a więc informacje przechowywane w węzłach są bardziej adekwatne i ściślej opisują bieżącą topologię w sieci.

#Wady Dynamicznego:

wymagania stawiane sprzętowym konfiguracjom węzłów sieci – mocy obliczeniowej oraz ilości pamięci, jak również dodatkowy ruch generowany w sieci na skutek wymiany informacji pomiędzy węzłami.

22. Pojęcie metryki routingu oraz dystansu administracyjnego.

Metryka trasowania - wartość używana przez algorytmy trasowania do określenia, która trasa jest lepsza.

Brane są pod uwagę: szerokość pasma, opóźnienie, liczba przeskoków, koszt ścieżki, obciążenie, MTU, niezawodność, koszt komunikacji. Tylko najlepsze trasy przechowywane są w tablicach trasowania, podczas gdy inne mogą być przechowywane w bazach danych. Jeśli router korzysta z mechanizmów równoważenia obciążenia (ang. load balancing), w tablicy trasowania może wystąpić kilka najlepszych tras. Router będzie je wykorzystywał równolegle, rozpraszając obciążenie równomiernie pomiędzy trasami.

- i – miara używana przez routery Cisco (i nie tylko), będąca liczbą naturalną z przedziału od 0 do 255, reprezentującą poziom zaufania (wiarygodności) w odniesieniu do źródła informacji o danej trasie. Zasada działania jest dość prosta – im mniejszy dystans administracyjny (mniejsza liczba), tym źródło danych o trasie jest bardziej godne zaufania.

23. Urządzenia sieciowe: hub, bridge, switch oraz router – charakterystyka działania.

Koncentrator (hub) – urządzenie łączące wiele urządzeń sieciowych w sieci komputerowej o topologii gwiazdy. Koncentrator pracuje w warstwie pierwszej modelu ISO/OSI (warstwie fizycznej), przesyłając sygnał z jednego portu na wszystkie pozostałe. Nie analizuje ramki pod kątem adresu MAC oraz IP. Ponieważ koncentrator powtarza każdy sygnał elektroniczny, tworzy jedną domenę kolizyjną. Koncentrator przenosi sygnał z portu wejściowego na wszystkie porty wyjściowe bit po bicie, przełącznik (switch) natomiast ramka po ramce, co jest powodem wprowadzania dużych opóźnień (także dodatkowych, zmiennych, w zależności od długości ramki). Jeżeli przesyłane mają być dane, dla których wspomniane zmienne opóźnienie jest niepożądane (np. streaming), koncentrator okaże się lepszym rozwiązaniem od przełącznika.

Przełącznik (switch) - urządzenie które łączy oddzielne sieci LAN oraz zapewnia filtrowanie pakietów między nimi. Switch LAN jest urządzeniem z pewną liczbą portów, z których każdy może współpracować z siecią Ethernet lub Token Ring. Chociaż zapewniają one takie same możliwości łączenia za pomocą kabli sieciowych jak koncentratory, to jednak przyczyniają się do zwiększenia wydajności całej sieci. Dzieje się tak wskutek rozszerzenia pasma transmisji danych (czyli maksymalnej pojemności sieci transmisji danych). Zamiast współdzielenia całego dostępnego pasma pomiędzy wszystkich użytkowników, tak jak w przypadku koncentratora, przełącznik przydziela każdemu podłączonemu urządzeniu sieciowemu określoną część pasma transmisyjnego. Na przykład, każdy koncentrator 10 Mb/s udostępni całe pasmo transmisyjne 10 Mb/s wszystkim podłączonym urządzeniom. Odpowiedni przełącznik przydzieli takie pasmo każdemu urządzeniu z osobna, co znacznie zwiększy wydajność. Dalsze zwiększenie wydajności można uzyskać przez wprowadzenie przełączników pozwalających na obsługę połączeń dwukierunkowych. Działanie przełączników jest możliwe dzięki zapamiętaniu jednoznacznych adresów MAC każdego urządzenia pracującego w lokalnej sieci komputerowej i informacjom o tym, z którym portem komunikuje się dane urządzenie.

- Umieszczone w pobliżu szkieletu sieci likwidują "wąskie gardła" systemu transmisji danych i zwiększają przepustowość sieci;
- Mogą zwiększyć zasięg sieci, w której zainstalowano maksymalną dozwoloną liczbę połączonych szeregowo koncentratorów; używane jako urządzenia do podłączenia komputerów biurowych, zapewniają ich użytkownikom najwyższą możliwą wydajność pracy.

Mostek (bridge) - urządzenie, które analizuje pakiety na poziomie warstwy łącza danych (ang. Data Link Layer – DLL) modelu OSI/ISO. W trakcie pracy analizuje stworzoną przez siebie tablicę forwardingu (ang. Forwarding DataBase – FDB lub MAC DataBase), zawierającą numery portów (interfejs E0/0, E0/1, itd...), do których przyłączone są urządzenia oraz adresy sprzętowe MAC. Mosty działają w trybie nasłuchu (ang. promiscuous mode) i odbierają dane krążące w medium transmisyjnym. Aby określić, jakie urządzenia znajdują się w poszczególnych segmentach sieci (skojarzonych z poszczególnymi portami), mosty odczytują źródłowe adresy MAC z ramek danych. Na tej podstawie tworzona jest tablica forwardingu (w wolnym tłumaczeniu "tablica mostowania"). Mosty, w przeciwieństwie do przełączników, mają oprogramowanie w formie programowej a nie sprzętowej, są więc od przełączników wolniejsze (przełącznik używa układu scalonego ASIC wspomagającego podejmowanie decyzji o filtrowaniu). Mosty mogą mieć tylko jedną instancję drzewa rozpinającego przypadającą na jeden port, przełączniki mogą mieć ich wiele. Podobnie mosty mogą mieć tylko do 16 portów, zaś przełączniki mogą mieć ich setki.

Ruter (router) – urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Na podstawie informacji zawartych w pakietach TCP/IP jest w stanie przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci. Proces kierowania ruchem nosi nazwę trasowania, routingu lub rutowania. Trasowanie musi zachodzić między co najmniej dwiema podsieciami, które można wydzielić w ramach jednej sieci komputerowej. Urządzenie tworzy i utrzymuje tablicę trasowania, która przechowuje ścieżki do konkretnych obszarów sieci oraz metryki z nimi związane (odległości od siebie licząc kolejne routery). Skuteczne działanie routera wymaga wiedzy na temat otaczających go urządzeń, przede wszystkim innych routerów oraz przełączników. Może być ona dostarczona w sposób statyczny przez administratora, wówczas nosi ona nazwę tablicy statycznej lub może być pozyskana przez sam router od sąsiadujących urządzeń pracujących w trzeciej warstwie, tablice tak konstruowane nazywane są dynamicznymi. Podczas wyznaczania tras dynamicznych router korzysta z różnego rodzaju protokołów trasowania i polega przede wszystkim na odpytywaniu sąsiednich urządzeń o ich tablice trasowania, a następnie kolejnych w zależności od zapotrzebowań ruchu, który urządzenie obsługuje.

24. Idea wirtualnej sieci (VLAN).

Sieć VLAN (ang. Virtual LAN) to wydzielona logicznie sieć urządzeń w ramach innej, większej sieci fizycznej. Urządzenia tworzące sieć VLAN, niezależnie od swojej fizycznej lokalizacji (przełącznika do którego są podłączone), mogą się swobodnie komunikować ze sobą, a jednocześnie są odseparowane od innych sieci VLAN, co oznacza, że na poziomie przełącznika nie ma żadnej możliwości skomunikowania urządzeń należących do dwóch różnych sieci VLAN (dotyczy to także ramek rozgłoszeniowych). Sieci VLAN konfiguruje się w przełącznikach, urządzeniach sieciowych warstwy 2 modelu ISO/OSI. Jedna sieć VLAN może swym zasięgiem obejmować wiele przełączników, a w najprostszym przypadku tworzona jest w jednym przełączniku. Sieć VLAN identyfikowana jest poprzez liczbę całkowitą. Ze stosowaniem sieci VLAN wiąże się kilka korzyści. Pozwalają one ograniczyć ruch rozgłoszeniowy, gdyż rozgłaszane ramki trafiają tylko do komputerów w obrębie danej sieci VLAN, nie „zalewają” całej sieci LAN. Ponadto, stosując sieci VLAN łatwo jest dostosować strukturę sieci do zmian w organizacji, ponieważ administrator może dokonać zmian topologii sieci programowo, a nie sprzętowo. Na przykład jeśli użytkownik należący do danej sieci VLAN zmienia stanowisko pracy, administrator po prostu konfiguruje przełącznik tak, by nowe stanowisko należało do odpowiedniej sieci VLAN. Do odzwierciedlenia zmiany administrator używa oprogramowania, a nie sprzętu (okablowania). Taka elastyczność jest szczególnie ceniona w dużych sieciach, w których często zachodzą zmiany w fizycznej topologii sieci. I wreszcie, podział sieci fizycznej na wiele sieci VLAN zwiększa bezpieczeństwo sieci komputerowej już z racji samej tylko separacji ruchu sieciowego w różnych sieciach VLAN

- Dzieli sieć przełączane na segmenty logicznie niezależnie od fizycznego rozmieszczenia użytkowników
- Pełnione funkcje, oddziały, zespoły projektowe
- Konfigurowane programowo
- Brak konieczności fizycznego przenoszenia sprzętu
- Usprawniają administrowanie grupami urządzeń
- Dodawanie, usuwanie i przenoszenie elementów grup
- Zwiększają skalowalność i bezpieczeństwo w sieci definiując, które węzły mogą się komunikować
- Zmniejszają domenę rozgłoszeniową

25. Połączenie typu TRUNK.

Gdy do sieci VLAN należą porty z różnych przełączników, konieczne jest skonfigurowanie specjalnego połączenia między przełącznikami (trunk), poprzez które przekazuje się informacje o sieciach VLAN - jest ono ustanawiane przez interfejsy Fast-Ethernet (100 Mb/s). Połączenia typu trunk między przełącznikami realizowane są z wykorzystaniem specjalnego protokołu, np. ISL (Inter-Switch Link) firmy Cisco, dostępnego między innymi na przełącznikach Catalyst 1900 (przełącznik 1900 faktycznie obsługuje protokół Dynamic ISL). ISL pracuje w warstwie drugiej modelu OSI, wymaga interfejsów FastEthernet i może być stosowany na połączeniach punkt-punkt między dwoma przełącznikami, między przełącznikiem a routerem, a także między przełącznikiem a serwerem wyposażonym w specjalną kartę sieciową

obsługującą protokół ISL (np. firmy Intel). Protokół ISL hermetyzuje standardowe ramki Ethernet, dodając własny 26-bajtowy nagłówek oraz sumę kontrolną CRC. Protokół ten musi być obsługiwany przez obydwie końce połączenia, w przeciwnym razie taka ramka będzie nieczytelna dla strony odbiorczej. Jednym z podstawowych pól nagłówkowych jest 15-bitowe pole VLAN ID, w którym umieszczany jest identyfikator sieci VLAN (kolor). Dzięki temu możliwe jest identyfikowanie i przesyłanie ramek różnych sieci VLAN przez pojedyncze łącze trunk (p. rys.). Tylko 10 bitów pola VLAN ID jest w praktyce wykorzystywane, co pozwala obsługiwać maksymalnie 1024 sieci VLAN.