## PODSTAWOWE POJĘCJA

**DTE** (ang. Data Terminal Equipment) – urządzenia końcowe np. komputer, router
**DCE** (ang. Data Communication Equipment) – urządzenia pośredniczące w transmisji, np. huby, bridge, switche

**Unicast** – adres pojedynczego hosta
**Multicast** – adres grupowy
**Broadcast** – adres rozgłoszeniowy, typ transmisji polegający na wysłaniu przesz jeden port danych do wszystkich hostów dołączonych do tej samej sieci.

**Simplex** – transmisja jest możliwa tylko w jedną stronę (ulica jednokierunkowa)
**half-duplex** – transmisja możliwa jest w obie strony ale w danym czasie tylko w jedną (remontowany most)
**duplex** – równoczesna transmisja w obie strony (ulica dwukierunkowa)

**Szerokość pasma** (ang. bandwidth) – wyraża maksymalną teoretyczną przepustowość sieci.
**Przepustowość** (ang. throughput) – wyraża aktualne możliwości sieci w zakresie przesyłania danych w sieci i jest mniejsza lub równa od teoretycznej.

## WARSTWA 1 - FIZYCZNA

**Przesyła nieprzetworzone bity danych przez fizyczny nośnik (kabel sieciowy lub fale elektromagnetyczne w przypadku sieci radiowych). Ta warstwa przenosi dane generowane przez wszystkie wyższe poziomy.**

**Odmiany sieci Ethernet i ich cechy charakterystyczne:**

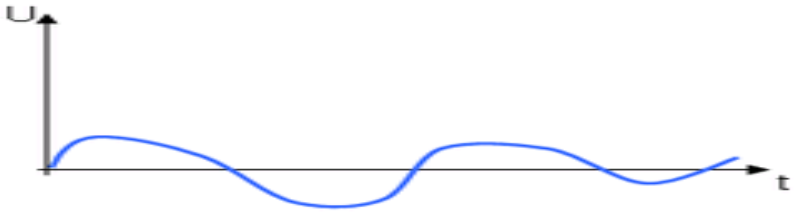
| Typ sieci Ethernet | Przepustowość, MB/s | Transmisja | Długość segmentu, m | Łącze |
|---|---|---|---|---|
| 10Base-5 | 10 | w paśmie podstawowym | 500 | przewód koncentryczny |
| 10Base-2 | 10 | w paśmie podstawowym | 185 | przewód koncentryczny |
| 10Base-T | 10 | w paśmie podstawowym | 100 | skrętka |
| 10Broad-36 | 10 | szerokopasmowa | 3600 | przewód koncentryczny |
| 10Base-F | 10 | w paśmie podstawowym | 4000 | światłowód |
| 100Base-X | 100 | w paśmie podstawowym | | skrętka |
| 100VG-AnyLAN (ang. Video Grade) | 100 | | 100-150 | skrętka czteroprzewodowa |
| 100Base-TX | 100 | w paśmie podstawowym | | skrętka |
| 1000Base-T | 1000 | w paśmie podstawowym | | skrętka |

Warstwa fizyczna opisuje sygnały, napięcia, ich poziomy, sposoby kodowania, media transmisyjne, a także sprzęt sieciowy, opisany w dziale Urządzenia sieciowe.

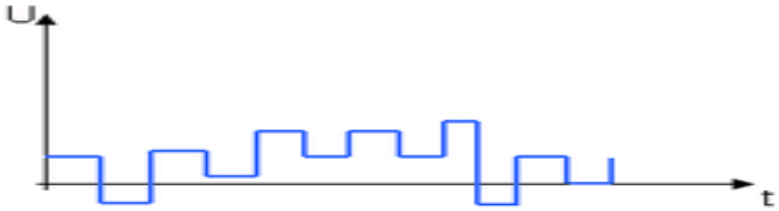
Dane przesyłane są w postaci bitów. Sygnałem może być każda funkcja, której zmienną niezależną jest czas. Poziom napięcia elektrycznego na wyjściu pewnego urządzenia jest funkcją czasu.

Rozróżniamy sygnały:

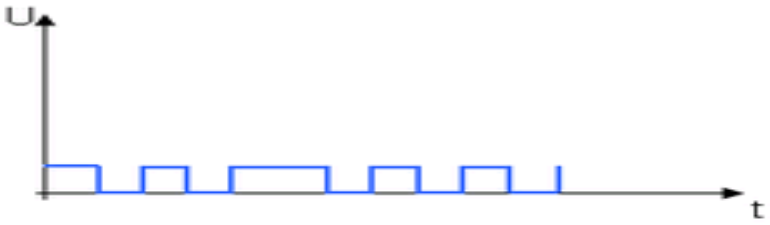
- **analogowy**- ciągła funkcja czasu,




- **dyskretny**- przyjmuje co najwyżej przeliczalny zbiór wartości,




- **cyfrowy** (binarny)- szczególny przypadek sygnału dyskretnego. Przyjmować może tylko 2 wartości.




**Nadajnik**- urządzenie wytwarzające sygnał.

**Odbiornik**- urządzenie wykorzystujące sygnał.

**Tor transmisji**- droga, którą przebywa sygnał od nadajnika do odbiornika.

Transmisja przebiega w pewnym medium transmisyjnym, którym może być kabel miedziany, światłowód, powietrze lub też próżnia. Podczas transmisji mają miejsce straty energii sygnału i zakłócenia. Wówczas sygnał podlega opóźnieniu i zniekształceniu. Powstaje tzw. widmo sygnału. Widmo pasma o skończonej mocy, powyżej pewnej częstotliwości staje się bardzo małe. Zakres częstotliwości, w jakim widmo uważamy za niezerowe, nazywamy **pasmem sygnału**, a jego długość nazywamy **szerokością pasma**.

Każdy tor transmisji posiada swoją charakterystykę częstotliwościową, czyli zależność przewodzenia składowej sygnału od częstotliwości tej składowej. Dla rzeczywistych mediów ich charakterystyki częstotliwościowe powyżej pewnej częstotliwości stają się bliskie zeru, tzn, że składowe sygnałów o wyższych częstotliwościach są prawie całkowicie tłumione. Mówimy wówczas o paśmie przenoszenia danego toru transmisji.

Gdy pasmo sygnału zawiera się w paśmie przenoszenia toru transmisji, a ponadto pasmo przenoszenia jest funkcją stałą w zakresie pasma sygnału, sygnał po przebiegu przez tor transmisji jest stłumiony i opóźniony, ale jego kształt nie ulega zmianie.

Jeżeli pasmo przenoszenia pewnego toru transmisji jest dużo szersze, niż pasmo wykorzystywane przez pojedynczy sygnał, można przez ten tor transmisji przesyłać wiele sygnałów jednocześnie. W takim przypadku mamy do czynienia z pojęciem **modulacji**.

Rozróżniamy modulację:

- amplitudy,
- częstotliwości,
- fazy.

Wzór ogólny równania fali nośnej:

**A * cos(2 * Π * f * t + Φ)**, gdzie

A- amplituda
f- częstotliwość
Φ - faza

Zmieniając jeden z tych parametrów uzyskujemy odpowiedni rodzaj modulacji (amplitudy, częstotliwości lub fazy).

Dla przykładu modulacja amplitudy będzie wyglądała następująco:

sygnał s(t) * nośna = sygnał zmodulowany, czyli odpowiednio:

**s(t) * cos(2 * Π * f * t + Φ)**.

Generowanie wielu nośnych, odległych od siebie na osi częstotliwości o więcej niż podwojona szerokość pasma sygnału użytecznego i modulowaniu każdej z nośnych innym sygnałem użytecznym nazywamy **zwielokrotnieniem**.

Suma zmodulowanych sygnałów jest przepuszczana przez łącze, a następnie poszczególne sygnały użyteczne są odfiltrowane i rozdzielone.

**Kodowanie sygnałów**

W warstwie fizycznej dane są przekazywane w postaci bitów. Sygnał cyfrowy przesyłany przez łącze może napotkać na znaczące problemy (zniekształcenia, ważność bitów, synchronizacja przesyłania danych itp.)

Wobec tego stosuje się kodowanie bitów. Sposobów jest kilka, a najczęściej stosowane to:

- <!--
  google_ad_client = "ca-pub-8415325888459429";
  /* sieci_srodek */
  google_ad_slot = "0844597726";
  google_ad_width = 250;
  google_ad_height = 250;
  //-->**NRZ** (*ang. Non Return to Zero*),
- **NRZI** (*ang. Non Return to Zero Inverted*),
- **Menchester**,
- **Menchester różnicowy**.

Kodowania NRZ i Menchester to tzw. kody proste. NRZI i Menchester różnicowy to kody różnicowe. Sygnały w kodach NRZ i NRZI zachowują stały poziom napięcia w ciągu jednego okresu sygnalizacji. Mogą go zachowywać przez dowolnie długi czas. Grozi to desynchronizacją nadajnika i odbiornika.

Sygnały w kodach Manchester i Manchester różnicowy zawsze zmieniają poziom napięcia w połowie okresu. Są to kody samosynchronizujące.

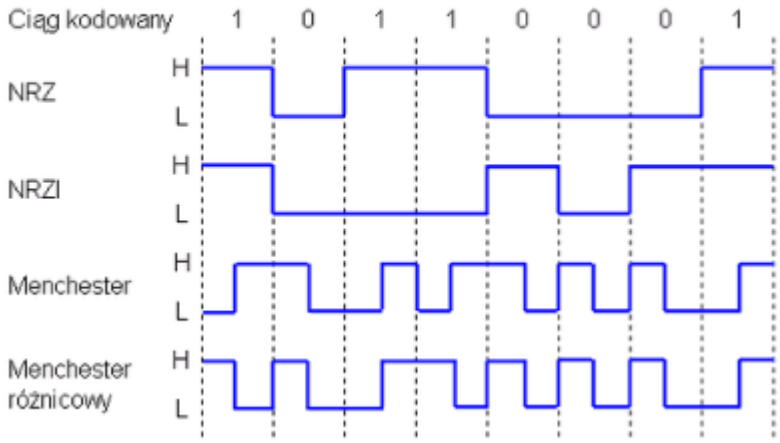
Sygnały w kodzie NRZ i NRZI w przypadku przewagi zer nad jedynkami (lub na odwrót) wprowadzają składową stałą sygnału. Średni poziom napięcia w łączu może odbiegać od średniej arytmetycznej wysokiego (H) i niskiego (L) poziomu napięcia. Może to być niekorzystne w przypadku niektórych rozwiązań technicznych. Dla sygnałów w kodzie Manchester i Manchester różnicowy średnia wartość napięcia zawsze wynosi **(H+L)/2**.

Kody różnicowe są bardziej odporne na przypadkowe zakłócenia i przypadkową zmianę polaryzacji

sygnału (zamianę końcówek kabli).

| Kodowanie | Informacja źródłowa | Poziom sygnału zakodowanego w czasie | | |
|---|---|---|---|---|
| | | -0,5T - 0 | 0 - 0,5T | 0,5T - T |
| NRZ | 1 | nieistotny | H | H |
| | 0 | nieistotny | L | L |
| NRZI | 1 | H | H | H |
| | | L | L | L |
| | 0 | H | L | L |
| | | L | H | H |
| Menchester | 1 | nieistotny | L | H |
| | 0 | nieistotny | H | L |
| Menchester różnicowy | 1 | H | H | L |
| | | L | L | H |
| | 0 | H | L | H |
| | | L | H | L |

Przykłady kodowania:




FDDI (ang. Fiber Distributed Data Interface)

- protokół oparty na przekazywaniu tokenu
- postać ramki podobne do Token Ring
- światłowód jako medium transmisji
- duża niezawodność

## WARSTWA 2 – ŁĄCZE DANYCH

**Zajmuje się pakietami logicznymi (lub ramkami) danych. Pakuje nieprzetworzone bity danych z warstwy fizycznej w ramki, których format zależy od typu sieci: Ethernet lub Token Ring. Ramki używane przez tę warstw zawieraj fizyczne adresy nadawcy i odbiorcy danych. Protokoły dostępu do medium**

### Niedeterministyczny

- stacja nadaje, gdy łącze jest wolne
- każda stacja jest równouprawniona
- rywalizacyjny
- problem z wielodostępem do medium
- dobry do zastosowań biurowych
- Ethernet

**Deterministyczny**

- stacja nadaje, gdy nadejdzie kolejność
- można wprowadzać priorytety
- np. tokenowy
- problem z zarządzaniem tokenem
- dobry do zastosowań przemysłowych
- token Ring, Token Bus, FDDI

**CSMA/CD** (ang. **Carrier Sense Multiple Access with Collision Detection**)

**Carrier Sense**

- każda stacja monitoruje medium
- gdy medium jest zajęte nie może nadawać
- gdy medium jest wolne odczekuje pewien czas (IFG ang. Inter-frame Gap)

**Multiple Access**

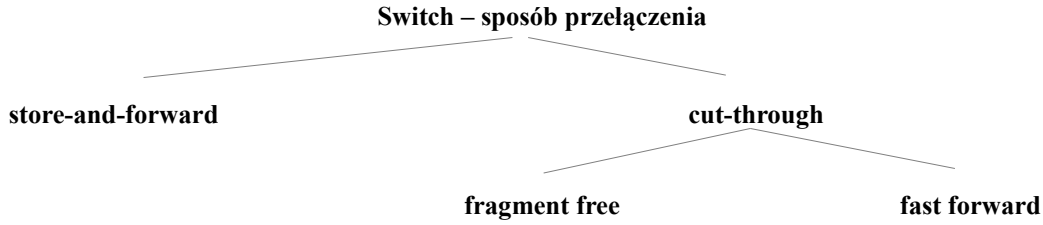
- każda stacja która stwierdzi, że łącze jest wolne może rozpocząć transmisję
- jest możliwość, że wiele stacji może nadawać równocześnie
- występują kolizje

**Collision Detection**

- stacje nadając równocześnie nasłuchują medium
- jeśli stacja wykryje kolizję, nie wstrzymuje wysyłania lecz wysyła jeszcze sekwencję zagłuszającą o czasie 32 bit co powoduje zauważenie kolizji przez inne stacje, następnie przestaje nadawać.
- Kiedy kolizja jest zauważona przy wysyłaniu preambuły, to jest ona nadal wysyłana a dopiero po niej sekwencja zagłuszająca.
- Po odczekaniu losowego czasu (algorytm exponential Backoff) stacja próbuje ponownie wysłać ramkę
- w poprawnej sieci nie może zdarzyć się kolizja po wysłaniu 64 bit ramki (szczelina czasowa)

**Ramka Ethernet**

Preambuła (7B) → Znacznik początku ramki (1B) → Adres docelowy (6B) → Adres źródłowy (6B) → Typ albo Długość ( długość gdy wartość<1518 typ gdy 1536 <wartość) (2B) → Dane (46-1500B) → FCS - Suma kontrolna (4B)




**Store and forward** – jest odbierana cała ramka i sprawdzana czy suma kontrolna się zgadza, jeśli tak jest wysyłana dalej.
**Cut-through** – ramka jest wysyłana dalej nawet zanim jeszcze zostanie odebrana cała ramka.
**Fragment free** – jest wysyłany natychmiast po przeczytaniu adresu MAC
fast forward -

**STP** (ang. **Spanning Tree Protocol**)

- Protokół drzewa opinającego ustanawia węzeł główny, który jest nazywany mostem głównym.
- Protokół drzewa opinającego konstruuje topologię, w której do każdego węzła w sieci prowadzi dokładnie jedna ścieżka.
- Połączenia nadmiarowe, które nie są częścią drzewa o najkrótszych ścieżkach, są blokowane.
- Połączenia, które powodują powstanie pętli, przechodzą do stanu blokowania.
- Stany portów

- **Blokowania** (ang. blocking) – porty mogą jedynie odbierać jednostki BPDU.
- **Nasłuchiwania** (ang. listening) – przełączniki ustalają, czy istnieją inne ścieżki do mostu głównego. Ścieżka, która nie jest ścieżką o najniższym koszcie prowadzącą do mostu głównego, przechodzi z powrotem do stanu blokowania. W stanie nasłuchiwania nie są przesyłane dane i nie są zapamiętywane adresy MAC
- **Zapamiętywania** (ang. learning) – W tym stanie dane nie są przekazywane, ale adresy MAC są odbierane i zapamiętywane.
- **Przekazywania** (ang. forwarding) – W tym stanie dane użytkowe są przekazywane, a adresy MAC są w dalszym ciągu zapamiętywane.
- **Wyłączenia** (ang. disabled) – Stan wyłączenia może wystąpić, gdy port zostanie wyłączony przez administratora lub ulegnie awarii.

**BPDU (ang. Bridge Protocol Date Unit)** – komunikaty za pomocą których jest tworzona topologia.

- Jednostki BPDU są odbierane nawet na zablokowanych portach.
- Zadaniami BPDU jest
  - Wybrać jeden przełącznik główny, który będzie pełnił rolę korzenia drzewa opinającego.
  - Obliczyć najkrótszą ścieżkę od danego przełącznika do przełącznika głównego.

**Identyfikacja sieci VLAN**

Aby pomiędzy przełącznikami jednym łączem przesyłać ramki z różnych sieci VLAN, należy na tym łączu umożliwić przesyłanie ramek w ramach różnych sieci VLAN. Takie łącze określane jest mianem **łącza trunk** (ang. VLAN trunk). Komunikację w ramach jednej sieci VLAN wykorzystującej łącza trunk (czyli sieci VLAN obejmującej więcej niż jeden przełącznik) umożliwia technika oznaczania ramek sieciowych identyfikatorem sieci VLAN (ang. VLAN ID). Technika ta polega na dodawaniu do ramki 12-bitowej liczby identyfikującej sieć VLAN nadawcy. Tak zmodyfikowana ramka przesyłana jest łączami trunk tak długo, aż dotrze do docelowego przełącznika. Ten zaś przed przekazaniem ramki na właściwy port usuwa z niej nadmiarową informację, wprowadzoną przez przełącznik źródłowy. Jest to nazwane etykietowaniem ramek (ang. frame tagging).

## WARSTWA 3 - SIECIOWA

**Kojarzy logiczne adresy sieciowe i ma możliwość zamiany adresów logicznych na fizyczne. U nadawcy warstwa sieciowa zamienia duże pakiety logiczne w małe fizyczne ramki danych, zaś u odbiorcy składa ramki danych w pierwotną logiczną struktur danych.**

**Trasowanie na podstawie wektora odległości –** jest oparty na algorytmach wektora odległości

- Wysyłana cała tablica do najbliższych sąsiadów (tzw. routing poprzez plotkowanie).
- Stosowana komunikacją jest komunikacja rozgłoszeniową (ang. **broadcast**),
- niektóre protokoły wykorzystują (ang. **multicast**).
- Tablice zawierają adres i odległość
- zastosowanie w małych sieciach
- problemem jest zbieżność (wolna reakcja na zmiany topologii)
- cykliczne wysyłanie danych o tablicach
- powstawanie pętli między routerami
- protokoły RIP, IGRP

**Trasowanie na podstawie stanu łącza** – utrzymują złożoną bazę danych opisującą topologię sieci.

- Rozsyłane są pakiety LSA (ang. **Link-state advertisement**)
- Routery wysyłają informację do wszystkich o swoich sąsiadach oraz o ich stanie (on, off)
- każdy posiada całą mapę sieci, tworząc drzewo najkrótszych ścieżek SPF (ang. **shortest path first**)
- aktualizacja następuje tylko przy zmianie topologi.
- Zastosowanie w dużych sieciach
- protokoły OSPF

**liczenia do nieskończoności**

- Pętle routingu: Pojawiają się gdy zbieżność protokołu routingu jest zbyt wolna.
- Liczenie do nieskończoności: występuje na skutek pojawienia się pętli routingu. Każde przejście pakietu przez kolejny router powoduje zwiększenie wektora odległości. Jeśli sieć sieć docelowa jest niedostępna i pojawiła się pętla routingu, pakiet może krążyć w sieci w nieskończoność a wartość wektora odległości będzie rosła do nieskończoności.

**Zapobieganie zapętlaniu**

- **Dzielony horyzont** (ang **split horizon**)
  - informacje otrzymane są wysyłane dalej, oprucz interfejsu od którego dostał te informacje (tzw. nie ucz nauczyciela swego)
- **Aktualizacja wymuszona (ang. triggered update)**
  - router wysyła natychmiast informację o zmianach i jest wysyłana tylko informacja o zmianie nie cała tablica rutingu.
- **Wstrzymanie** (**ang. path holddown**)
  - po otrzymaniu, że sieć nie istnieje, jest włączany licznik (ang. hold-down timer)
  - jeśli dostanie od tego samego routera, że trasa jest ok, przerywa liczenie
  - jeśli otrzyma komunikat od innego routera ogłaszającą lepszą trasę, przerwie liczenie
  - jeśli otrzyma gorszą trasę, ignoruje ją
  - po upłynięciu licznika, kasowana jest ścieszka.

**Zbieżność** – jest to czas w którym routery będą mieć jednakowy obraz sieci po zmianie topologi lub awarii.

**Podział Protokołów Routingu**

- **Statyczny**
- **Dynamiczny**
  - **Wewnętrzny**
    - IGP
      - Z wektorem odległości
        - RIP
        - IGRP
      - Stanu łącza
        - OSPF
        - IS-IS
  - **Zewnętrzny**
    - EGP
      - Z wektorem odległości
        - BGP
      - Stanu łącza

**Routing statyczny i Dynamiczny**

- Statyczny
  1. przewidywalny – znamy sieć, łatwo konfigurowalny
  2. łącza nie obciążone routowaniem
  3. łatwa konfiguracja w małych sieciach
  4. brak obsługi redundantnych połączeń
  5. brak dynamicznej zmian konfiguracji
- Dynamiczny
  1. Skalowalność
  2. Dostosowanie się do zmian topologi

3. łatwa konfiguracja
4. większy stopień zawiłość działania sieci
5. synchroniczna aktualizacja obciąża sieć

**Protokoły Routingu**

- Wewnętrzny
  1. stosowany wewnątrz jednej domeny administracyinej
  2. proste, w małym stopniu obciążają routery
  3. mało skalowalne
  4. RIP (ang. Routing Information Protocol)
  5. IGRP (ang. Interior Gateway Routing Protocol)
  6. OSPF (ang. Open Shortest Path First)
- Zewnętrzny
  1. odpowiadają za komunikację  między dwiema niezależnymi administracyjnie sieciami
  2. dają się skalować, łatwa obsługa dużych sieci
  3. są skaplikowane większa liczba informacja może blokować małe i średnie sieci
  4. EGP (ang. Exterior Gateway Protocol )
  5. BGP (ang. Border Gateway Protocol)

IP (ang. Internet Protocol)

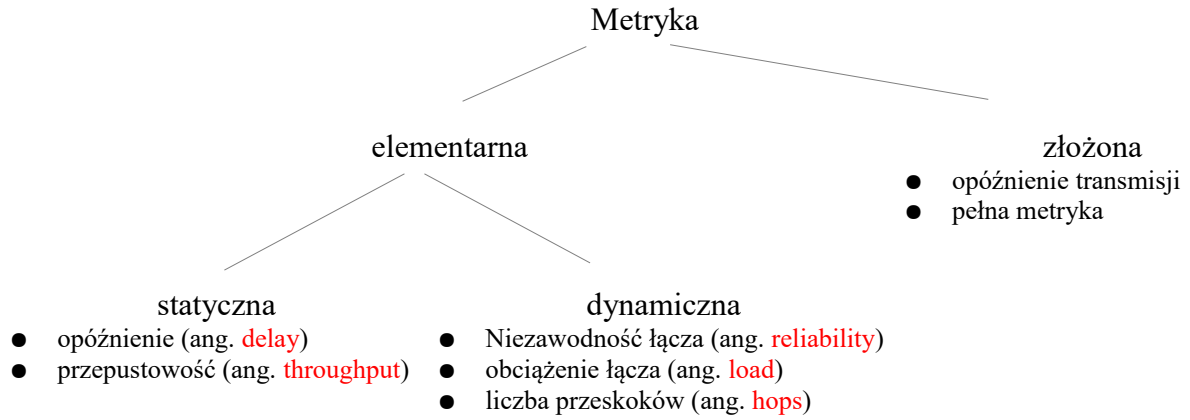
- jest protokołem bezpołączeniowym

**RIP** (ang. Routing Information Protocol) – protokół informowania o transporcie

1. aktualizacja co 30 s
2. synchroniczny spadek wydajności.
3. pakiety są wysyłane broadcast-em
4. wysyłana jest cała tablica do sąsiadów
5. Metryka jest liczbą przeskoków
6. po 180 s nie odświeżona droga zostaje usuwana
7. liczenie do nieskończoności
8. po 16 przeskokach pakiet zostanie odrzucony
9. aktualizacje przenoszone są przez UDP na porcie 520

**IGRP** (ang. Interior Gateway Routing Protocol)

1. wykorzystuje wyszukiwanie drogi przez wektor odległości
2. aktualizacja co 90 sekund
3. liczba przeskoków do 255
4. metryka →



- MTU

| RIP (ang. Routing Information Protocol) | OSPF (ang. Open Shortest Path First) |
|---|---|
| Protokół routingu<br>wektor odległości (ang. vector-distance) | Protokół routingu<br>stanu łącza (ang. Link State) |
| Zbieżność<br>wolna zbieżność<br>aktualizacje domyślne co 30 s<br>aktualizacje po zmianie topologi<br>synchroniczne obciążanie sieci | Zbieżność<br>szybka reakcja na zmiany topologi |
| Skalowalność<br>zastosowanie w małych sieciach<br>tylko do 15 routerów | Skalowalność<br>zastosowanie w dużych sieciach<br>rozszerzenie do 500 routerów |
| Metryka<br>liczba przeskoków (ang. hops) | Metryka<br>minimalny koszt<br>stopień pewności dotarcia pakietu do celu<br>przepustowość (ang. troughput)<br>minimalne opóźnienie (ang. delay) |
| Mechanizm<br>Dzielony horyzont (ang split horizon)<br>Aktualizacja wymuszona (ang. triggered update)<br>Wstrzymanie (ang. path holddown) | Mechanizm<br>SPF (ang. shortest path first) |

## EIGRP (ang. Enhanced Interior Gateway Routing Protocol)

Automatyczne dopasowanie metryk wcześniejszych. Minimalne zużycie pasma gdy sieć jest stabilna. Propaguje zmiany w tablicach routingu a nie całe tablice. Niezależność od rutowanych protokołów

## ARP (ang. Address Resolution Protocol)

### Fazy działania ARP

### W tej samej sieci:

1. Jest wysyłane Zapytanie ARP które zawiera adres IP hosta odbiorcy i żądanie „Jeśli jesteś właścicielem tego adresu IP, odeślij mi swój adres sprzętowy”. Zapytanie ARP jest wysyłane do wszystkich w sieci z użyciem adresu broadcast.
2. Host rozpoznaje swój adres IP i wysyła Odpowiedź ARP ze swoim adresem sprzętowym bezpośrednio do nadawcy Zapytania ARP.

### Host jest w innej sieci:

1. Host przed wysłaniem datagramu IP musi zdecydować do kogo go wysyła
   - bezpośrednio czy do routera?
   - Porównuje numery sieci: swój i odbiorcy
2. Host A wysyła zapytanie ARP o adres sprzętowy routera.
3. Router wysyła odpowiedź ARP hostowi A przedstawiając swój adres sprzętowy.
4. Host A uzupełnia datagram IP o adres sprzętowy
   - Host A wysyła datagram IP skierowany do Hosta B routerowi, aby ten przekazał go dalej
5. Router odbiera ramkę Ethernet zdejmuje nagłówek warstwy drugiej i analizuje datagram IP.
   - Na podstawie części sieciowej adresu odbiorcy stwierdza, że odbiorca znajduje się w tej samej sieci
   - Router formuje ramkę warstwy drugiej i przekazuje ją dalej
6. Host B otrzymuje datagram IP

## WARSTWA 4 - TRANSPORTOWA

**Jest odpowiedzialna za dostawę wiadomości, które pochodzą z warstwy aplikacyjnej. U nadawcy**

**warstwa transportu dzieli długie wiadomości na kilka pakietów, natomiast u odbiorcy odtwarza je i wysyła potwierdzenie odbioru. Sprawdza także, czy dane zostały przekazane we właściwej kolejności i na czas. W przypadku pojawienia się błędów warstwa żąda powtórzenia transmisji danych.**

**Porty efemeryczne —** Ustawiane porty na czas połączenia, krótkotrwałe

## Rodzaje protokołów

**Połączeniowy** - Większe możliwości (zapewnienie, że dane dotrą do celu itp.)
- nawiązywanie połączenia
- transmisja danych
- zamykanie połączenia

**Bezpołączeniowy** - Mniejsze narzuty na informacje kontrolne
- **tylko transmisja...**

## TCP (ang. Transmission Control Protocol)
- warstwa 4 - Transportowa
- protokół połączeniowy
- nawiązuje połączenie między dwoma hostami (ang. three-way handshake)
- Niezawodny
  - potwierdzenia odbioru (ang. **positive acknowledgement**)
  - retransmisja
- Nie pozwala na transmisję grupową (ang. **multicasting**)
- Przesyłanie danych wrażliwych na gubienie pakietów (np. Telnet, SSH, FTP, Mail)

## UDP (ang. User Datagram Protocol) – protokół pakietów użytkownika
- warstwa 4 – Transportowa
- protokół bezpołączeniowy
- szybki (małe ilości danych)
- zawodny (nie posiada żadnych kontroli dostarczenia)
- Zastosowanie
  - transmisje grupowe
  - transmisje w czasie rzeczywistym
  - przesyłanie w sieciach LAN
  - wideokonferencje

| TCP (ang. Transmission Control Protocol) | UDP (ang. User Datagram Protocol) |
|---|---|
| Zalety:<br>protokół połączeniowy – three-way handshake<br>niezawodny<br>potwierdzenie odbioru<br>retransmisja<br>szeregowanie danych | Zalety:<br>szybki (małe ilości danych)<br>transmisje w czasie rzeczywistym<br>transmisje grupowe (ang. multicasting) |
| Wady:<br>brak transmisji grupowej (ang. multicasting)<br>jest wolny | Wady:<br>zawodny<br>brak gwarancji dostarczenia przesyłki<br>brak potwierdzenia odbioru<br>brak szeregowania |
| Użycie:<br>FTP (ang. File Transfer Protocol)<br>HTTP (ang. HyperText Transfer Protocol)<br>SSH (ang. secure shell) | Użycie:<br>transmisja dźwięku / wideo<br>DNS (ang. Domain Name System)<br>RIP (ang. Routing Information Protocol)<br>SNMP (ang. Simple Network Management Protocol) |

**Segment TCP** – nazywany jednostkową porciąt danych wysyłanych między oprogramowanie TCP na różnych maszynach

**Przesuwane okno**
- Zapobiega przeciążeniu odbiorcy

- odbiorca określa ile jest w stanie danych przyjąć
- szybki nadawcza czeka aż odbiorca stworzy dla niego okno

**Syndrom głupiego okna**

- problemy
  - Odbiorca odczytuje bufor bajt po bajcie (małymi blokami)
  - Odbiorca ogłasza niewielkie okna zamiast poczekać na opróżnienie bufora
  - Nadawca wysyła niewielkie segmenty, zamiast większych bloków danych danych
- Rozwiązanie
  - Odbiorca czeka z otwarciem okna, aż możliwe będzie powiększenie go o MSS lub o połowę rozmiaru bufora odbiorcy

## WARSTWA 7 - APLIKACJI

**Jest bramą , przez którą procesy aplikacji dostaj się do usług sieciowych. Ta warstwa prezentuje usługi, które s realizowane przez aplikacje (przesyłanie plików, dostęp do baz danych, poczta elektroniczna itp.)**

**NAT** (ang. **Network Adress Translation**) **–** Technologia NAT umożliwia ograniczenie liczby publicznych adresów IP i wykorzystanie prywatnych adresów IP w sieciach wewnętrznych. Powoduje to zwiększenie poziomu bezpieczeństwa w sieci. Ponieważ w wypadku sieci prywatnej nie są rozgłaszane wewnętrzne adresy ani informacje o wewnętrznej topologii, sieć taka pozostaje wystarczająco zabezpieczona, gdy dostęp zewnętrzny odbywa się z wykorzystaniem translacji NAT.

- **Wewnętrzny adres lokalny –** adres IP przypisany do hosta w sieci wewnerznej.
- **Wewnętrzny adres globalny** – legalny adres IP przypisany przez dostawcę usług. Adres ten reprezentuje dla sieci zewnętrznych jeden lub więcej wewnętrznych, lokalnych adresów IP
- **Zewnętrzny adres lokalny** – adres IP zewnętznego hosta, który znamy jest hostom znajdującym się w sieci wewnętrznej.
- **Zewnętrzny adres globalny** – adres IP przypisany do hosta w sieci zewnętrznej. Ten adres przypisany jest przez właściciela hosta.

### Cechy NAT

- Statyczna translacja NAT umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi
- Dynamiczna translacja NAT umożliwia mapowanie adresu prywatnego na adres publiczny.

**PAT (ang. Port Address Translation**) polega na tym, że komputer pełniący funkcję bramy zajmuje się takim modyfikowaniem ramek pakietów wchodzących i wychodzących z sieci lokalnej, aby możliwy był dostęp poprzez pojedynczy publiczny adres IP, a pakiety przychodzące docierały do właściwych komputerów w sieci lokalnej.

**Cechy PAT**

- W technologii PAT tłumaczone adresy są rozróżniane przy użyciu unikatowych numerów portów źródłowych powiązanych z globalnym adresem IP