Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Media transmisyjne **4**
miedziane : 4
światłowody : 6
bezprzewodowe : 6

Urządzenia Sieciowe **7**
Karta sieciowa 7
Router 8
Koncentrator 8
Przełącznik (Switch) 9
Punkt dostępowy 9
Most (bridge) 9
repeater Wi-Fi 10
Adapter PowerLine 10
Serwer wydruku 11
Kamera IP 11
Bramka VoIP 12

Symbole graficzne używane w schematach **13**

Topologie sieci **14**
FIZYCZNA 14
Topologia magistrali (szyna baz) 14
Topologia gwiazdy (star) i gwiazdy rozszerzonej 15
Topologia pierścienia 17
Topologia siatki 18
Topologie bezprzewodowe 19
LOGICZNA 21
Punkt- Punkt 21
w tej topologii przesył danych odbywa się tylko pomiędzy dwoma urządzeniami w sieci 21
Topologia rozgłaszania (broadcaster) 21
Token-passing(przekazywanie tokenu) 21

Metody dostępu do nośnika **22**
CSMA/CD 22
CSMA/CA 22

Rodzaje środowisk sieciowych **23**
Klient - Serwer 23
Każdy z każdym 23

Komunikacja w sieci **23**
Tryb połączeniowy 23
Tryb bezpołączeniowy 23
Rodzaje transmisji ze względu na ilość odbiorców : 25

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Rodzaje transmisji ze względu na kierunek przepływu danych : 26

Modele warstwowe sieci 27
Model ISO/OSI 27
Model TCP/IP 28
Protokoły sieciowe 30
Warstwa aplikacji 30
Warstwa transportowa 31
Warstwa sieciowa (TCP/IP warstwa internetowa) 31
Warstwa łącza danych (TCP/IP warstwa dostępu do sieci) 32
Warstwa fizyczna (TCP/IP warstwa dostępu do sieci) 32
Niezależne : 32
Porty protokołów sieciowych : 33

Budowa ramki Ethernet 34

Budowa nagłówka IP 35

Budowa segmentu TCP 36

Budowa datagramu UDP 37

Polecenia Sieciowe (cmd i terminal) 38
Polecenia diagnostyczne Windows 38
Polecenia diagnostyczne Linux 42
Polecenia Konfiguracyjne Windows 44
Polecenia Konfiguracyjne Linux 45

Adresowanie w sieci komputerowej 46
Fizyczne 46
Logiczne 46
IPV4 46
IPv6 48

Podział Sieci na podsieci 51
Obliczanie Ilości podsieci na podstawie maski 51
Przykład: 51
Ważne! 51
Obliczanie Ilości hostów na podstawie maski 51
Przykład: 51

Zasady projektowania adresacji ip 53
Zasady przy projektowaniu 53
Technika VLSM 53

Model hierarchiczny sieci 54

Zasady projektowania lokalnych sieci komputerowych 55

Struktura dokumentacji projektowej 56
Fazy realizacji projektu 56

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Dokumentacja projektowa zawiera 56

Projektowanie okablowania strukturalnego 57

Elementy okablowania strukturalnego: 57

Punkty dystrybucyjne 58

Normy przy projektowaniu sieci 59

Organizacje standaryzacyjne 59

Normy dotyczące okablowania strukturalnego: 59

Najważniejsze zalecenia wynikające z powyższych norm 59

Zalecenia dotyczące kabli w przebiegach poziomych: 60

Zasady układanie kabla w przebiegach poziomych: 60

Okablowanie Pionowe - wymagania instalacyjne 61

Pozostałe wymagania 61

Najczęściej wykorzystywane końcówki: 62

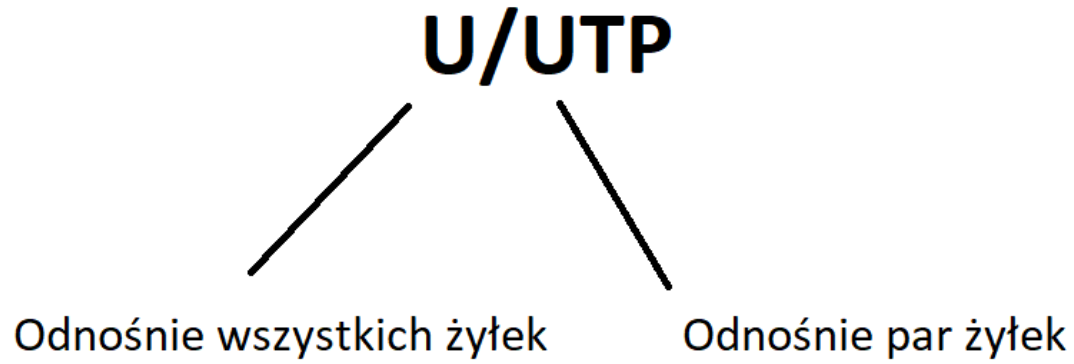
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Media transmisyjne

miedziane :

- kable koncentryczne
- skrętki :

Oznaczenia dla skrętki :



U - nieekranowane
F - ekranowane folią
S - ekranowane siatką
SF - ekranowane siatką i folią

kategoria 5 - 100 Mbit/s
kategoria 5e - 1 Gbit/skategoria 6 - 10 Gbit/s

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

1000BASE-T (IEE 802.3)

1000 - przepustowość łącza (1000Mb/s)
BASE - przesyłanie sygnału w paśmie podstawowym

T - skrętka
LX, LH - jednomodowy światłowód
SX - wielomodowy światłowód

Kolejność żyłek w standardzie A :

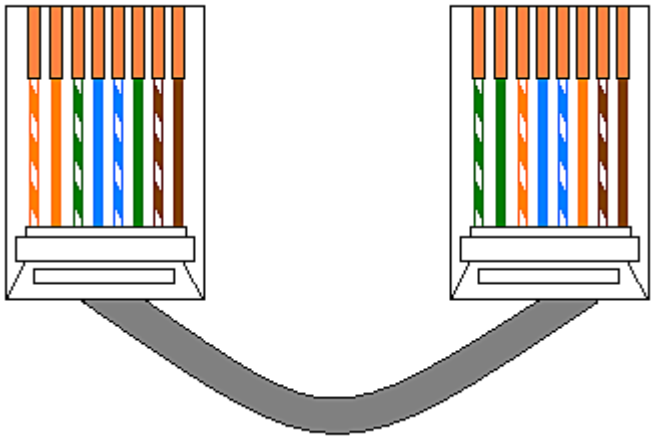
- biało-zielony
- zielony
- biało-pomarańczowy
- niebieski
- biało-niebieski
- pomarańczowy
- biało-brązowy
- brązowy

Kolejność żyłek w standardzie B :

- biało-pomarańczowy
- pomarańczowy
- biało-zielony
- niebieski
- biało-niebieski
- zielony
- biało-brązowy
- brązowy

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Układ żyłek w kablu krosowanym :



światłowody :

jednomodowe - SM - jeden promień światła w przewodzie

wielomodowe - MM - wiele promieni światła w przewodzie

bezprzewodowe :

802.11a - 54 Mbps
802.11b - 11 Mbps
802.11g - 54 Mbps
802.11n - 600 Mbps
802.11ac - 1,3 Gbps
802.11ax - 10 - 12 Gbps

IRDA - fale podczerwone

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Urządzenia Sieciowe

Elementy aktywne	Elementy pasywne
Rutery (ang. Routers)	**Media transmisyjne** (ang. Cables)
Przełączniki (ang. Switches)	**Panele krosownicze** (ang. Patchpanel)
Punkty dostępowe (ang. Access Points)	**Szafy dystrybucyjne** (ang. Rack)
Serwery (ang. Servers)	**Gniazda abonenckie** (ang. Socket)
	Organizatory kabli
	Korytka kablowe

Karta sieciowa

Karta rozszerzeń montowana w gnieździe magistrali PCI, PCI-Express lub jako zewnętrzny adapter USB.

posiada unikatowy adres sprzętowy MAC wykorzystywany do identyfikowania komputera w sieci.

Adres MAC składa się z 48 bitów i zapisywany jest szesnastkowo. Pierwsze 24 bity oznaczają producenta, pozostałe 24 są unikatowe dla danego egzemplarza karty:

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Router

Urządzenie które służy do łączenia sieci komputerowych, na przykład sieci Internet z domową siecią lokalną:

Koncentrator

Działa w topologii gwiazdy

rozsyła zapytania do wszystkich komputerów uruchomionych w sieci. Dane trafiają do każdego aktywnego węzła, jednak odpowiada tylko ta maszyna, dla której przeznaczone są dane pakiety, pozostałe ignorują cudze pakiety:

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Przełącznik (Switch)

Działa w topologii gwiazdy
Urządzenie centralne służące do realizacji połączeń
Przełącznik przechowuje w wewnętrznej pamięci numery MAC interfejsów sieciowych.
Dzięki sprawdzeniu adresu każdej ramki danych switch przesyła pakiety tylko do właściwego komputera:

Punkt dostępowy

Zapewnia bezprzewodowy dostęp do zasobów sieci za pomocą WiFi:

Most (bridge)

Sygnał sieci bezprzewodowej możemy zamienić na połączenie kablowe:

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

repeater Wi-Fi

Służy do poprawienia zasięgu Wi-Fi sieci:

Adapter PowerLine

Pozwalają przesyłać sygnał sieci poprzez istniejącą np. w mieszkaniu instalację elektryczną:

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Serwer wydruku

Serwer udostępniający usługę drukowania, potrafi kolejkować przychodzące do wydruku pliki, formatować odpowiednio ich wygląd, jak również prowadzi statystyki i raporty na temat przetwarzanych plików:

Kamera IP

Urządzenie sieciowe najczęściej wykorzystywane w systemach monitoringu, łączące funkcje kamery i komputera. Urządzenie posiada adres IP i jest podłączone do sieci. Dzięki temu może pełnić rolę serwera lub klienta FTP, może też wysyłać maile, zarządzać alarmami, wysyłać logi na stronę www etc. Kamera IP nie potrzebuje komputera do działania.

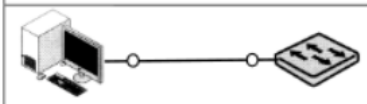
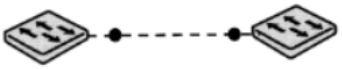
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Bramka VoIP

Urządzenie sieciowe, które służy do wykonywania połączeń tradycyjnym aparatem telefonicznym (podłączonym złączem RJ-11) :

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Symbole graficzne używane w schematach

Symbol	Znaczenie	Symbol	Znaczenie
	modem		AP - punkt dostępowy
	koncentrator		router
	most		stacja robocza
	przełącznik		zapora sieciowa
	kabel Ethernetowy prosty		kabel szeregowy
	kabel Ethernetowy krosowany		kabel światowo-dowy
	internet		printer

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

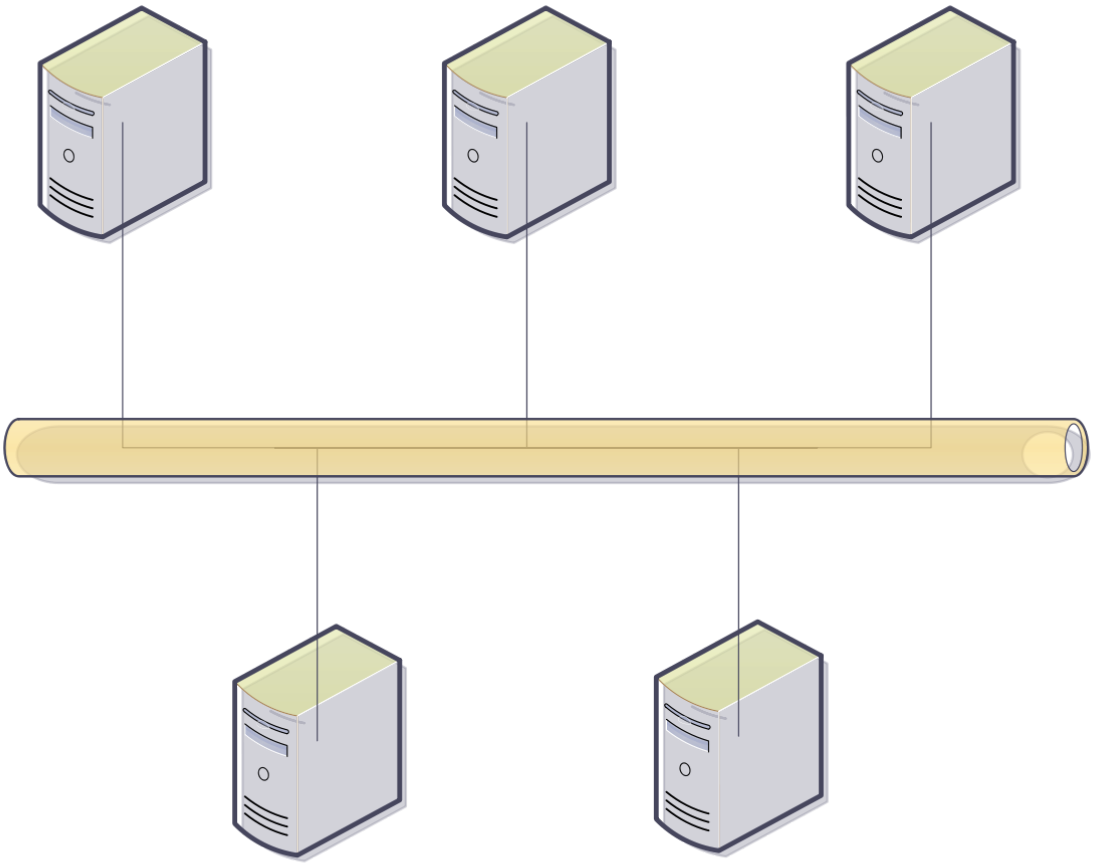
Topologie sieci

Topologia - nauka o budowie urządzeń sieciowych.

Rodzaje topologii:

FIZYCZNA

- **Topologia magistrali (szyna baz)**
  Wykorzystuje kabel koncentryczny



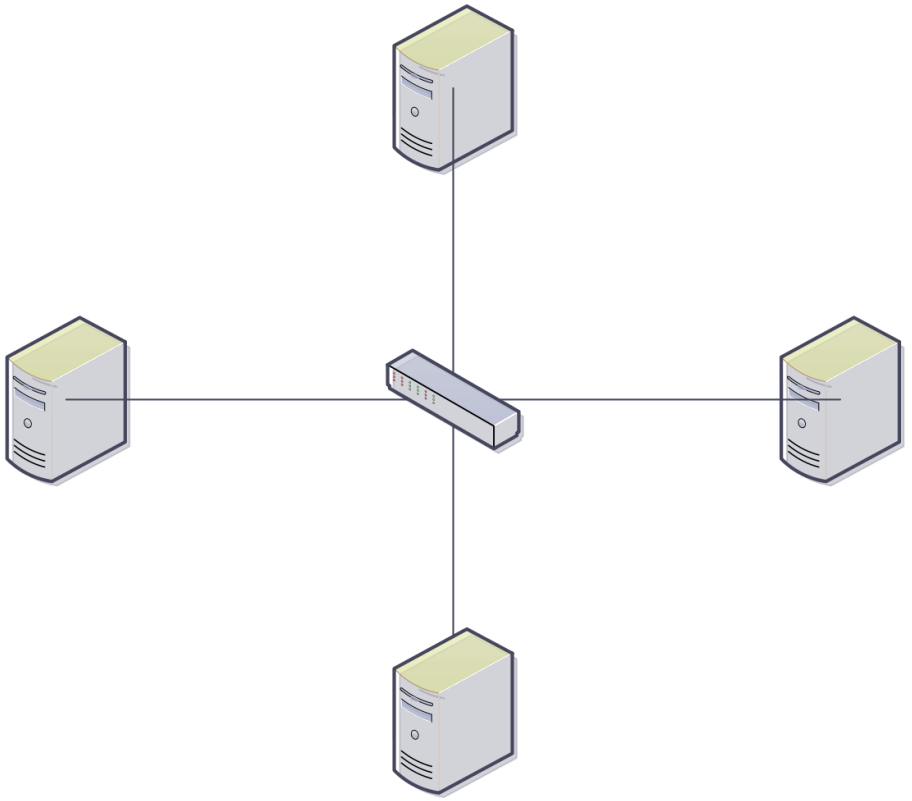
Zalety:
-niewielkie zużycie kabla
-łatwa instalacja
-niewielkie cena instalacji
-łatwa rozbudowa

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

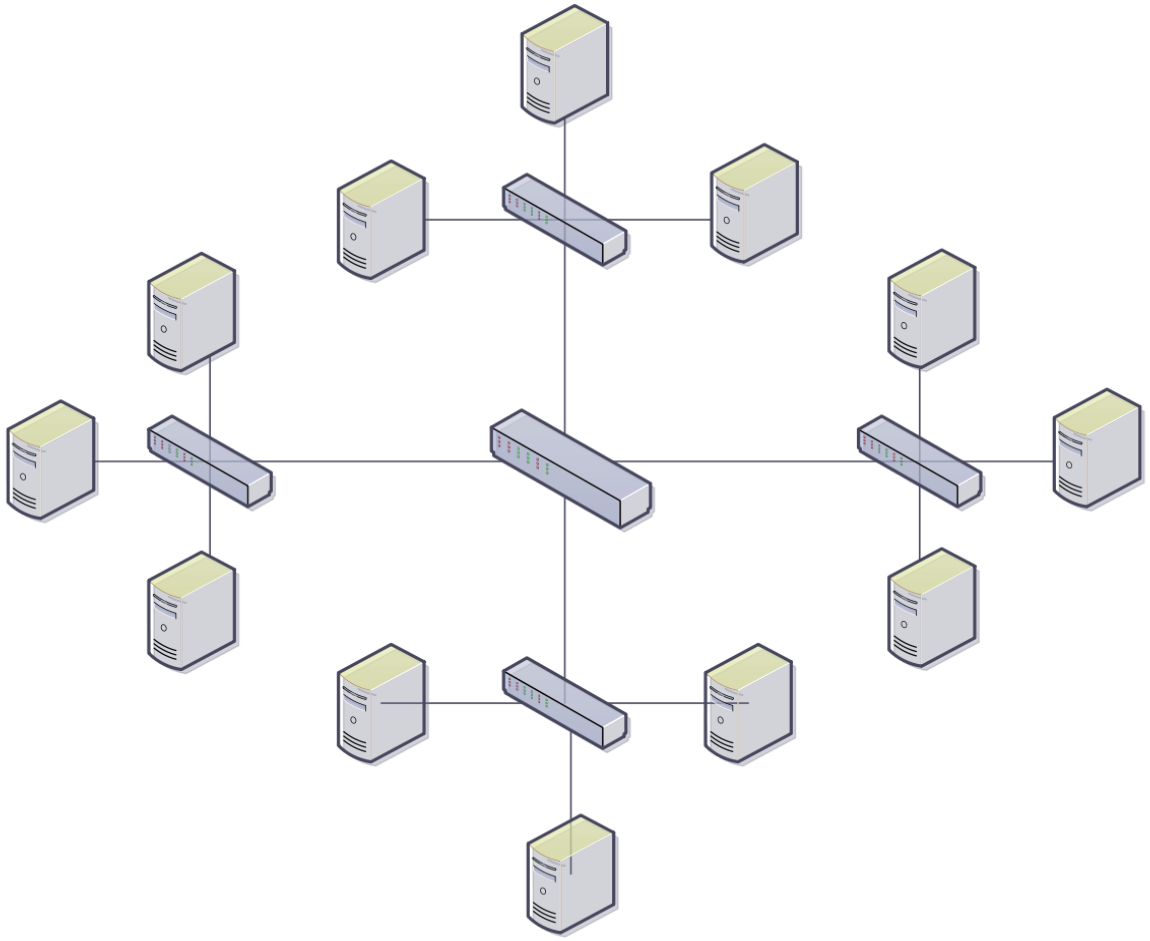
Wady

- wszystkie urządzenia korzystają z jednego kabla
- dużo kolizji
- małe bezpieczeństwo

- **Topologia gwiazdy (star) i gwiazdy rozszerzonej**



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021



Zalety

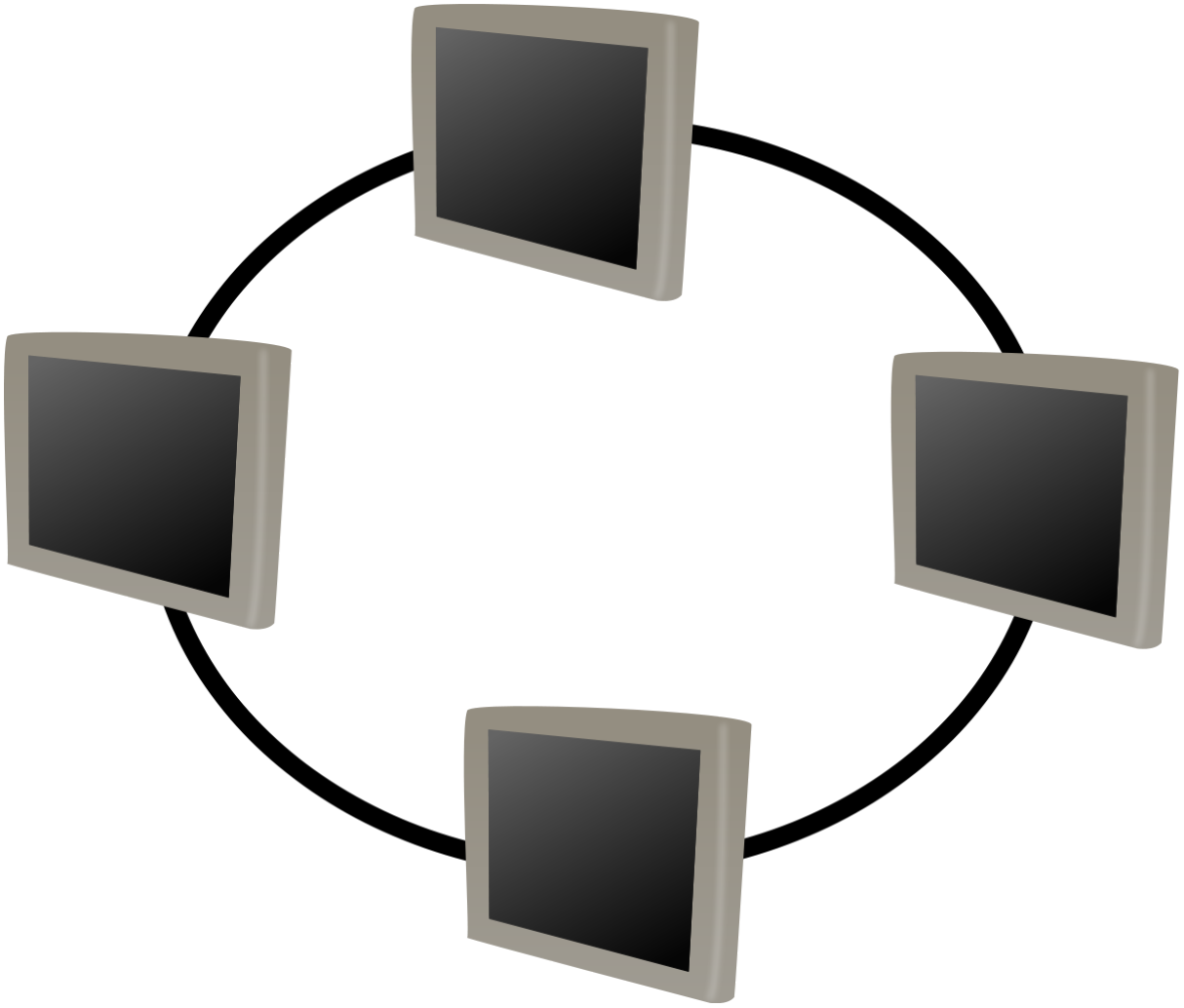
- Łatwa lokalizacja uszkodzeń
- Łatwa rozbudowa
- Awaria komputera nie ma wpływu na sieć

Wady

- Duża ilość kolizji
- Awaria switcha to brak sieci

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Topologia pierścienia



Zalety

- małe zużycie kabla

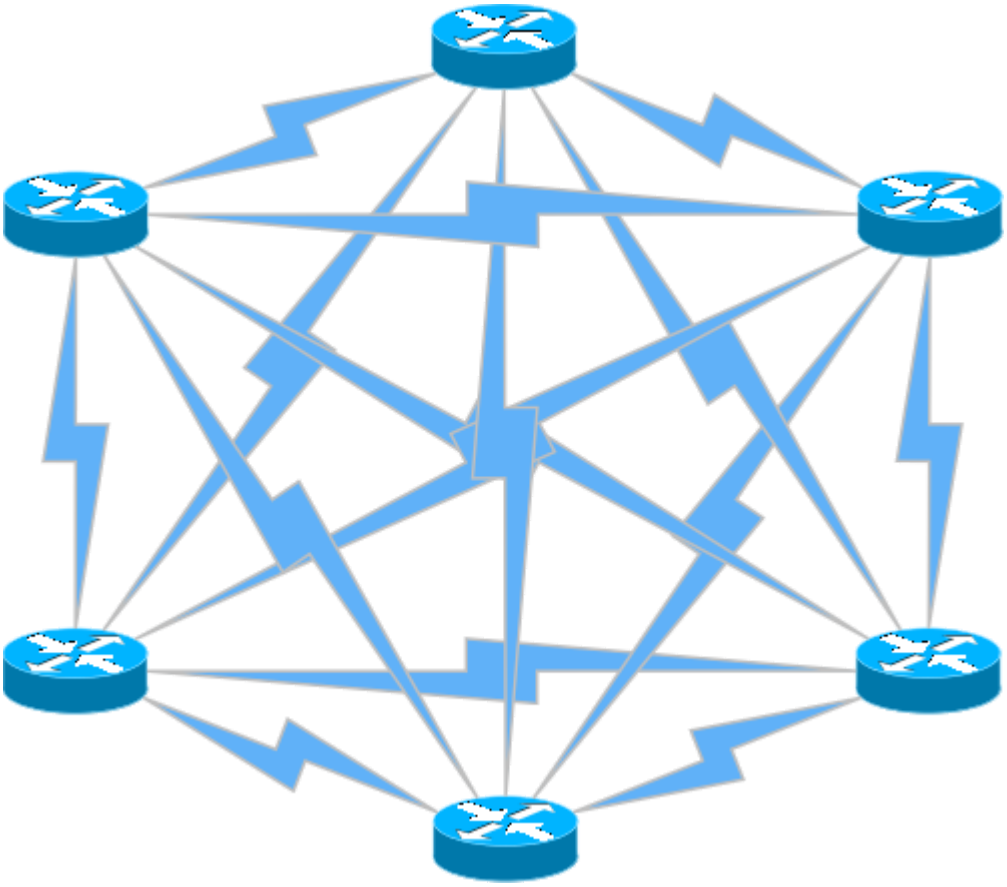
Wady

- trudna lokalizacja awarii
- przerwanie kabla = wszystko się zepsuje

Istnieje również topologia podwójnego pierścienia która polega na wstawieniu drugiego pierścienia

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Topologia siatki



Zalety

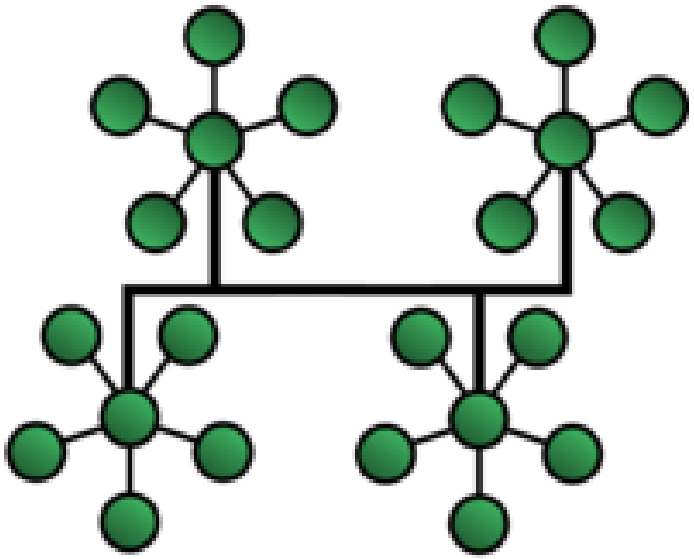
- duża niezawodność
- duża przepustowość
- brak kolizji

Wady

- wysoki koszt
- dużo kabla
- skomplikowana budowa

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Topologia drzewa (hierarchiczna)

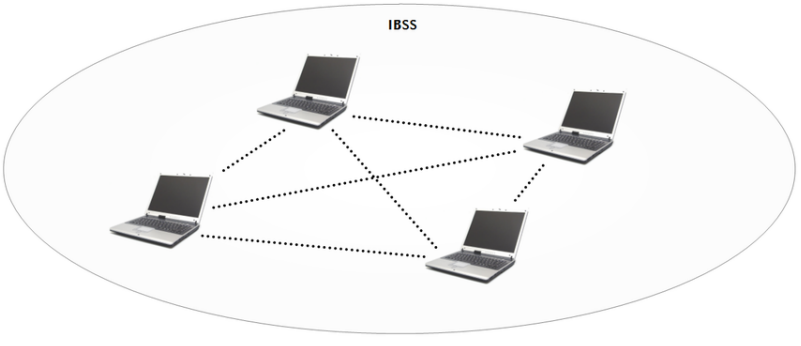


Zalety
- łatwa lokalizacja uszkodzeń
- łatwa rozbudowa

Wady
- główna magistrala upada = wszystko się psuje

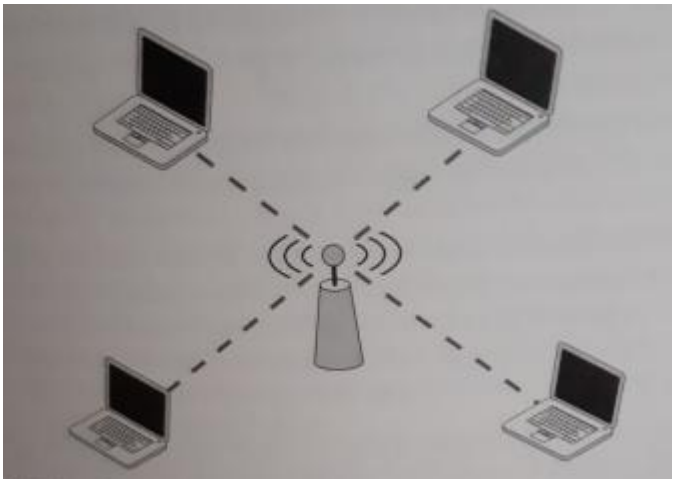
Topologie bezprzewodowe

- **Ad-hoc** - krótkoterminowe połączenie urządzeń (np w celu przesłania pliku), sieć demontowana po zakończeniu połączenia, nie wymaga infrastruktury sieciowej



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

- **Infrastruktury -** wykorzystuje punkty dostępowe (Access Pointy - AP); wszystkie urządzenia komunikują się tylko z AP, który spełnia funkcję bramy (do sieci przewodowej) i pośredniczy w komunikacji pomiędzy urządzeniami sieci bezprzewodowej.



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

LOGICZNA

Punkt- Punkt

w tej topologii przesył danych odbywa się tylko pomiędzy dwoma urządzeniami w sieci

Topologia rozgłaszania (broadcaster)

Host wysyła dane do wszystkich hostów podłączonych do mediów transmisyjnych
“Kto pierwszy ten lepszy”.

Token-passing(przekazywanie tokenu)

Host posiada token, który jest przekazywany kolejnym urządzeniom w sieci dopóki nie trafi na właściwego adresata.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Metody dostępu do nośnika

Mechanizm regulacji dostępu do nośnika realizowany był i jest przez warstwę 2 modelu referencyjnego OSI, czyli warstwę danych.
I tak w sieciach LAN dostęp do nośnika regulowany może być na jeden z czterech różnych sposobów:

- rywalizacji,
- przesyłania tokenu (żetonu),
- priorytetu żądań,
- przełączania.

CSMA/CD

(ang. Carrier Sense Multiple Access with Collision Detection) – protokół wielodostępu CSMA z badaniem stanu kanału i wykrywaniem kolizji.

Kiedy urządzenie lub węzeł w sieci chce przesłać jakieś dane - nasłuchuje łącza, sprawdzając czy jakieś inne urządzenie nie przesyła danych w linii transmisyjnej.
Dane będą wysyłane wtedy kiedy żadne inne urządzenie w sieci nie wysyła danych

CSMA/CA

(ang. Carrier Sense Multiple Access with Collision Avoidance) – protokół wielodostępu do łącza ze śledzeniem stanu nośnika i unikaniem kolizji.

Jest to rozszerzona wersja CSMA.
Gdy kilka urządzeń próbuje wysyłać informacje na tym samym łączu w tym samym czasie, każde urządzenie przed próbą wejścia na linię wysyła sygnał próbny (pilot) i jeżeli nie zaszła kolizja z sygnałem innego urządzenia – uzyskuje zgodę na nadawanie. Znaczącą wadą tego rozwiązania jest fakt, że w przypadku zapełnienia łącza protokół ten generuje duże straty czasowe.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Rodzaje środowisk sieciowych

Klient - Serwer

Klient - komputer korzystający z zasobów udostępnionych w sieci przez serwer
Serwer - jeden lub kilka komputerów z zainstalowanym serwerowym systemem operacyjnym.

Każdy z każdym

Nie ma uprzywilejowanego komputera, każdy klient może udostępniać zasoby oraz korzystać ze wszystkich zasobów udostępnianych przez innych klientów. Każdy użytkownik sam zarządza dostępem innych użytkowników do swoich zasobów.

Komunikacja w sieci

Komunikacja może odbywać się w dwóch trybach (nierównocześnie)

Tryb połączeniowy

Polega na nawiązywaniu sesji (połączenia logicznego) i może odbywać się w ramach jednej maszyny, a nawet jednego procesu. Aby rozpocząć komunikację, należy najpierw nawiązać połączenie. Po nawiązaniu sesji, przydzielany jest jej unikatowy numer.
Dane przesyłane są w sposób niezawodny (jeżeli adresat nie odbierze wiadomości, nadawca zostanie o tym poinformowany).
Maksymalny rozmiar wiadomości to ok. 64kB. Jeżeli podczas wysyłania wiadomości wystąpi błąd, nastąpi zamknięcie sesji.

Wyróżniamy 3 fazy:

- budowa połączenia
- przesyłanie danych
- likwidacja połączenia

W trybie połączeniowym działa protokół TCP

Tryb bezpołączeniowy

Komunikaty są przekazywane niezależnie np. podczas przekazywania wiadomości poprzez pocztę elektroniczną. W komunikacji biorą udział co najmniej dwa urządzenia.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

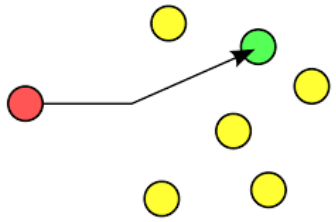
Adresat nie posiada gwarancji, że odbierze wiadomość.
Nadawca nie otrzymuje potwierdzenia oraz informacji dotyczącej wysłanej wiadomości.
Wiadomości są odbierane jeżeli adresat oczekuje na datagram. Rozmiar datagramu
to około 500B. Przeważnie wiadomości są adresowane do wszystkich odbiorców za pomocą
rozgłaszania.

W trybie bezpołączeniowym działa protokół UDP

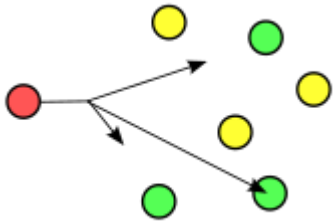
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Rodzaje transmisji ze względu na ilość odbiorców :

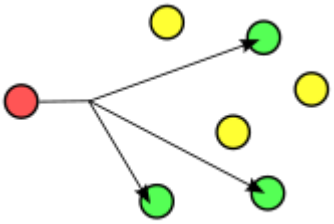
unicast - pakiety są wysyłane do dokładnie jednego punktu



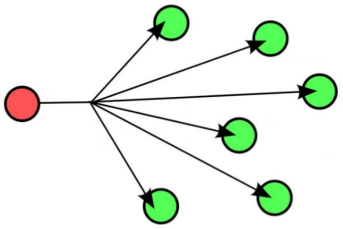
anycast - pakiety są wysyłane do najbliższego punktu



multicast - pakiety wysyłane są do określonej grupy odbiorców



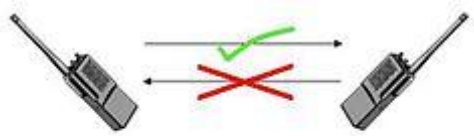
broadcast - pakiety są wysyłane do wszystkich możliwych odbiorców



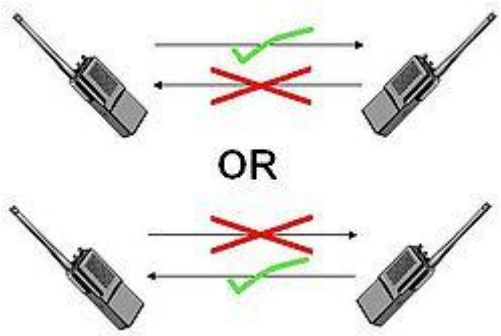
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Rodzaje transmisji ze względu na kierunek przepływu danych :

Simplex (ang. duplex) - transmisja odbywa się jednostronnie (jeden nadajnik i jeden odbiornik)



Półduplex (ang. half duplex) - transmisja dwukierunkowa naprzemienna.

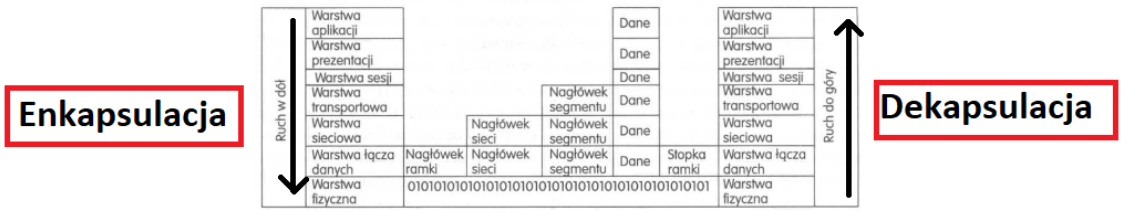


Duplex (ang. full duplex) - transmisja dwukierunkowa jednoczesna.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Modele warstwowe sieci

Proces podziału strumienia danych na jednostki danych i opatrywania ich nagłówkami nazywamy **enkapsulacją**. Proces odwrotny, realizowany podczas odbierania informacji i przesyłania danych do górnych warstw nazywamy **dekapsulacją**.



Model ISO/OSI

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Warstwa modelu ISO/OSI	**Zadania**
Aplikacji	Zajmuje się specyfikacją interfejsu, który wykorzystują aplikacje. Świadczy usługi końcowe dla aplikacji
Prezentacji	Przetwarza dane z warstwy aplikacji do postaci standardowej, wymaganej przez warstwy niższe. W przypadku dekapsulacji - warstwa ta tłumaczy dane na format zgodny z aplikacją. **Odpowiada też za kompresję i szyfrowanie danych**
Sesji	Zarządzanie przebiegiem komunikacji podczas połączenia. Nadzoruje połączenie i kontroluje, która aplikacja łączy się z inną. Gdy połączenie zostanie przerwane, nawiązuje ją ponownie. Określa kierunek komunikacji (możliwa jest dwukierunkowa).
Transportu	Dzieli dane na **segmenty** i wysyła je do stacji docelowej. Zapewnia poprawną kolejność otrzymywanych segmentów. W przypadku uszkodzenia segmentu, zarządza jego retransmisji. Może wysyłać potwierdzenie otrzymania segmentu
Sieci	Rozpoznaje trasy łączące komputery i sieci na podstawie topologii i wybiera najlepszą z nich. Jednostka danych to **pakiet.** Odpowiada za adresowanie logiczne węzłów sieci (np. adresy IP)
Łącza danych	Nadzoruje warstwę fizyczną i steruje wymianą bitów. Definiuje mechanizmy kontroli błędów CRC. Zapewnia dostarczenie ramek informacji na podstawie MAC karty sieciowej. Jednostką danych jest **ramka.**
Fizyczna	Przesyłanie strumieni bitów. Ustala sposób przesyłania oraz odległości przerw między nimi.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Model TCP/IP

Warstwa	Zadania
Aplikacji	Wysyłają lub odbierają dane w postaci pojedynczych komunikatów lub strumienia bajtów.
Transportu	Zapewnienie komunikacji między programami użytkownika. Zarządza przepływem informacji oraz zapewnia niezawodność przesyłania dzięki porządkowaniu segmentów danych i retransmisję ich w przypadku uszkodzenia.
Internetowa	Wysyła pakiety i dostarcza je do miejsca przeznaczenia. Dzieli się na pakiety i dodaje nagłówek zawierający IP nadawcy i odbiorcy. Warstwa ta wysyła też komunikaty o błędach oraz komunikaty kontrolne
Dostępu do sieci	Zapewnia interfejs z siecią fizyczną i przekazuje dane poprzez fizyczne połączenie. Formatuje dane do transmisji przez nośnik oraz adresuje dane do podsieci. Zapewnia sprawdzenie błędów przesyłu danych za pomocą sumy kontrolnej ramki.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Protokoły sieciowe

<table>
<tr><th>Model OSI</th><th>Model TCP/IP</th><th colspan="3">Protokoły</th></tr>
<tr><td>Warstwa aplikacji</td><td rowspan="3">Warstwa aplikacji</td><td rowspan="3">telnet, ssh, http, smtp, pop3, ftp</td><td rowspan="3">tftp, dns</td><td></td></tr>
<tr><td>Warstwa prezentacji</td><td></td></tr>
<tr><td>Warstwa sesji</td><td></td></tr>
<tr><td>Warstwa transportowa</td><td>Warstwa transportowa</td><td>TCP</td><td>UDP</td><td></td></tr>
<tr><td>Warstwa sieciowa</td><td>Warstwa internetowa</td><td colspan="2">IP, ICMP IGMP, RIP, OSPF, BGP</td><td rowspan="2">ARP</td></tr>
<tr><td>Warstwa łącza danych</td><td rowspan="2">Warstwa dostępu do sieci</td><td colspan="2" rowspan="2">Ethernet</td></tr>
<tr><td>Warstwa fizyczna</td><td></td></tr>
</table>

Warstwa aplikacji

Telnet – standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala w architekturze klient-serwer. Korzysta z portu 23

ssh - to protokół zdalnego zarządzania hostami. Zazwyczaj korzysta z portu 22

http - Protokół przesyłania dokumentów hipertekstowych, protokół sieci WWW korzysta z portu 80.

smtp - protokół komunikacyjny poczty elektronicznej w internecie, określa się w nim co najmniej jednego odbiorcę wiadomości. Działa na porcie 25.

pop3 - protokół poczty elektronicznej umożliwia pobieranie i kasowanie poczty. Działa na porcie 110 (z ssl na 996)

IMAP - następca pop3, umożliwia zarządzanie wieloma folderami pocztowymi i operowanie na listach na zdalnym serwerze. IMAP pozwala na ściągnięcie nagłówków wiadomości i wybranie, które z wiadomości chcemy ściągnąć na komputer lokalny. Działa na porcie 143.

ftp - protokół komunikacyjny, umożliwiający dwukierunkowy transfer plików w układzie serwer-klient. Działa na portach 21 (dla poleceń) i 20 (do przesyłania danych).

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

tftp - prosty protokół wykorzystywany do przesyłania plików.
Nie posiada większości funkcji protokołu FTP – np. nie może wyświetlać katalogów, ani uwierzytelniać użytkowników, a jego jedynym zadaniem jest odczytywanie plików z komputera zdalnego i transmitowanie do niego plików. Korzysta z portu 69.

dns - DNS to protokół, usługa, zamieniająca nazwy domenowe, zrozumiałe dla człowieka na adresy IP urządzeń w sieci. Korzysta z portu 53.

Warstwa transportowa

TCP - (transmission control protocol) - połączeniowy, niezawodny, strumieniowy protokół stosowany do przesyłania danych między maszynami. Korzysta z protokołu IP do wysłania i odbierania danych i ich fragmentacji

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.

UDP - (user datagram protocol) - jeden z protokołów internetowych, nie gwarantuje dostarczenia datagramu. Jest to protokół bezpołączeniowy - więć nie ma konieczności nawiązania połączenia.

Korzyścią płynącą z takiego uproszczenia budowy jest szybsza transmisja danych i brak dodatkowych zadań.

Warstwa sieciowa (TCP/IP warstwa internetowa)

IP - protokół komunikacyjny warstwy sieciowej OSI, Protokół internetowy to zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia w celu nawiązania łączności i wymiany danych. Używany powszechnie w Internecie i lokalnych sieciach komputerowych.

ICMP - (internet control message protocol)Pełni przede wszystkim funkcję kontroli transmisji w sieci. Jest wykorzystywany w programach ping oraz traceroute.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

IGMP - (internet group management protocol) IGMP służy do zarządzania grupami multicastowymi w sieciach opartych na protokole IP. Komputery wykorzystują komunikaty IGMP do powiadamiania routerów w swojej sieci o chęci przyłączenia się do lub odejścia z określonej grupy multicastowej.

RIP (routing information protocol) - protokół bram wewnętrznych oparty na zestawie algorytmów wektorowych, służących do obliczania najlepszej trasy do celu. Działa na podstawie wektora odległości, do utworzenia metryki stosuje się jedynie liczbę przeskoków, jeżeli liczba przeskoków osiągnie 15 pakiety na następnym routerze są odrzucane.

OSPF (open shortest path first) - protokół trasowania oparty na analizie stanu łącza (ang. *link-state*). Cechami protokołu OSPF są: trasowanie wielościeżkowe, trasowanie najmniejszym kosztem i równoważenie obciążenia. Wykorzystuje algorytm SPF (algorytm Djikstry)

W przeciwieństwie do protokołu RIP, charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek, przyspieszoną zbieżnością i brakiem ograniczenia skoków powyżej 15.

BGP (border gateway protocol)- Jest protokołem wektora ścieżki umożliwiającym tworzenie nie zapętlonych ścieżek pomiędzy różnymi systemami autonomicznymi. Protokół ten nie używa tradycyjnych metryk – analogiczną funkcję (determinanty wyboru trasy) pełnią atrybuty i algorytm wyboru. BGP pozwala na pełną redundancję w połączeniu z Internetem. (port TCP o numerze 179)

Warstwa łącza danych (TCP/IP warstwa dostępu do sieci)

ARP (address resolution protocol) - Protokół ten nie ogranicza się tylko do kojarzenia adresów IP z adresami MAC stosowanymi w sieciach Ethernet, lecz jest także wykorzystywany do odpytywania o adresy fizyczne stosowane w technologiach Token ring czy FDDI. Zarządza tzw. tablicą ARP.

RARP - (reverse address resolution protocol) - protokół komunikacyjny pozwalający na przekształcanie 48-bitowych fizycznych adresów MAC na 32-bitowe adresy IP.

Warstwa fizyczna (TCP/IP warstwa dostępu do sieci)

ETHERNET - Protokół Ethernet jest typową technologią LAN. Nowe karty Ethernet, znane jako Fast Ethernet, reprezentują technologię szybkich sieci LAN, ponieważ mogą zapewnić szybkość przesyłania danych do 100 Mb / s. Dwa nowe standardy Ethernet, które są obecnie opracowywane, to Gigabit Ethernet (do 1000 Mb / s) i 10 Gigabit Ethernet (z szybkością przesyłania danych 10 000 Mb / s).

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Niezależne :

DHCP (ang. *Dynamic Host Configuration Protocol* – protokół dynamicznego konfigurowania hostów) – protokół komunikacyjny umożliwiający hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci..

W sieci opartej na protokole TCP/IP każdy komputer ma co najmniej jeden adres IP i jedną maskę podsieci; dzięki temu może się komunikować z innymi urządzeniami w sieci.

port źródłowy 67 i port docelowy 68.

Porty protokołów sieciowych :

Port	Protokół
53	DNS
20	FTP - przesyłanie oraz pobieranie plików i folderów
21	FTP – przesyłanie poleceń
67	DHCP - serwer
68	DHCP – klient
80	HTTP
443	HTTPS (HTTP na SSL)
143	IMAP
220	IMAP3
110	POP3
995	POP3S (POP3 na SSL)
25	SMTP
22	SSH
23	Telnet
69	TFTP

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Budowa ramki Ethernet

Rozmiar pola w bajtach	7	1	6	6	2	46 - 1500	4
Nazwa pola	Preambuła	Znacznik początku ramki	Adres MAC odbiorcy	Adres MAC nadawcy	Długość/Typ	Dane i wypełnienie	Kod kontrolny ramki (FCS)

- **Preambuła** oraz **znacznik początku ramki** – te pola służą do poinformowania urządzenia docelowego, aby przygotował się na odbiór ramki;
- **Docelowy adres MAC**, czyli adres fizyczny odbiorcy ramki;
- **Źródłowy adres MAC**, czyli adres fizyczny hosta wysyłającego dane;
- **Długość / Typ** – pole długość określa wielkość ramki, natomiast **typ** określa, jaki został wykorzystany **protokół warstwy wyższej**, najczęściej jest to **IPv4**;
- **Dane** – to pakiet, który odebrany został z **warstwy sieciowej**. Minimalna wielkość tego pola to **46**, a maksymalna **1500 bajtów**. Jeśli pakiet jest mniejszy niż **46 bajtów**, to dopełnia się
  go, losowymi danymi, tak aby rozmiar całej ramki został zwiększony do wymaganego minimum, czyli do **64 bajtów**.
- **Kod kontrolny ramki** – pole zawierające **sumę kontrolną ramki**, służącą do wykrywania **ewentualnych błędów ramki**. Urządzenie wysyłające dane **oblicza sumę kontrolną** i umieszcza ją w ramce, odbiorca danych, po jej otrzymaniu **również taką sumę oblicza, jeśli obydwie sumy się zgadzają ramka jest akceptowana, jeśli się różnią, ramkę traktuje się jako uszkodzoną i odrzuca**.

Całkowita wielkość ramki może wynieść maksymalnie **1518 bajtów** (przy obliczaniu jej wielkości, **nie brana jest pod uwagę preambuła i sygnał początku ramki**).

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Budowa nagłówka IP

1 bajt		2 bajt	3 bajt	4 bajt
Wersja	Długość nagrania	Typ usług	Całkowita długość pakietu	
Identyfikacja			Flagi	Przesunięcie fragmentu
Czas życia		Protokół	Suma kontrolna	
Adres źródłowy				
Adres docelowy				
Opcje				
Dane				

Czas życia TTL - określa maksymalny czas przebywania pakietów w sieci. Gdy pakiet przechodzi przez router, zmniejsza się jego wartość o 1. Maksymalna liczba routerów wynosi 255.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Budowa segmentu TCP

<table>
<tr><th colspan="3">BIT (0)</th><th colspan="2">BIT (15) BIT (16)</th><th>BIT (31)</th></tr>
<tr><td colspan="3">Port źródłowy (16)</td><td colspan="3">Port docelowy (16)</td></tr>
<tr><td colspan="6">Numer sekwencyjny (32)</td></tr>
<tr><td colspan="6">Numer potwierdzenia (32)</td></tr>
<tr><td>Długość nagłówka (4)</td><td>Zarezerwowane (6)</td><td>Bity kodu (flagi) (6)</td><td colspan="3">Okno (16)</td></tr>
<tr><td colspan="3">Suma kontrolna (16)</td><td colspan="3">Wskaźnik pilności (16)</td></tr>
<tr><td colspan="6">Opcje (0 lub 32 – jeśli istnieją)</td></tr>
<tr><td colspan="6">Dane warstwy aplikacji (dł. zmienna)</td></tr>
</table>

- **Port źródłowy** – port aplikacji, z której wysłano dane.
- **Port docelowy** – port aplikacji, do której wysłano dane.
- **Numer sekwencyjny** – numer ostatniego bajtu w segmencie.
- **Numer potwierdzenia** – numer następnego bajtu oczekiwanego przez odbiorcę.
- **Długość** – długość całego segmentu TCP.
- **Bity kodu (flagi)** – informacje kontrolne dotyczące segmentu.
- **Okno** – ilość danych jaka może zostać przesłana bez potwierdzenia.
- **Suma kontrolna** – używana do sprawdzania poprawności przesłanych danych.
- **Wskaźnik pilności** – używany tylko kiedy ustawiona jest flaga URG.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Budowa datagramu UDP

BIT (0)	BIT (15) BIT (16)	BIT (31)
Port źródłowy (16)	Port docelowy (16)	
Długość (16)	Suma kontrolna (16)	
Dane warstwy aplikacji (dł. zmienna)		

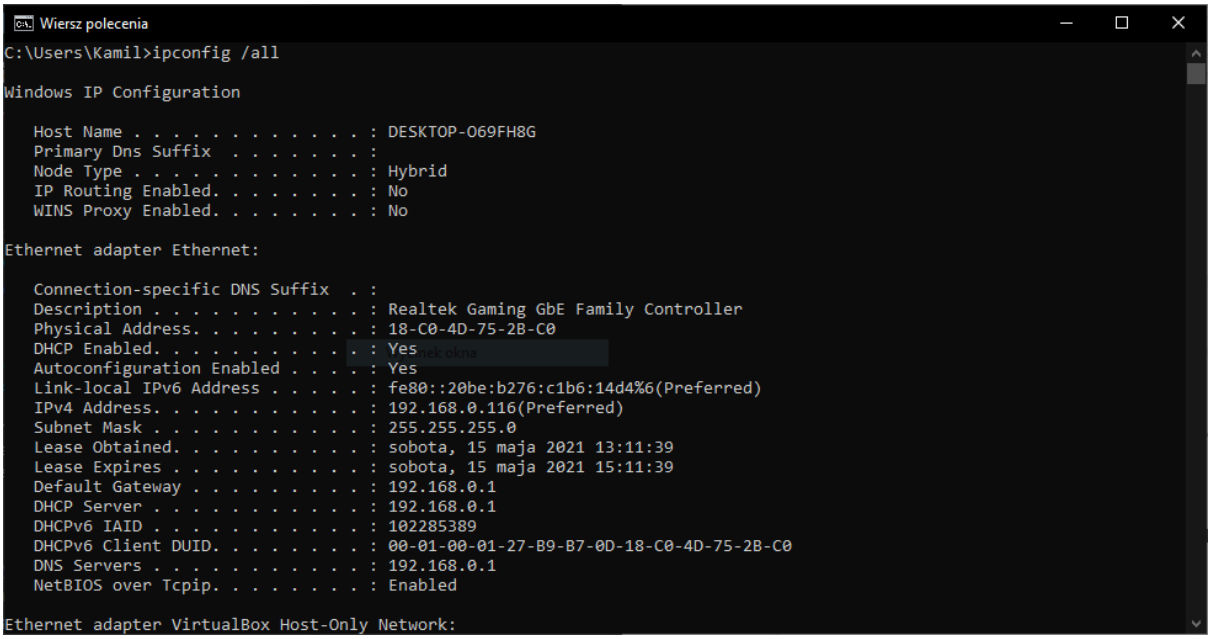
- **Port źródłowy** – określa port aplikacji, z której wysłano dane.
- **Port docelowy** – określa port aplikacji, do której wysłano dane.
- **Długość** – 16 – bitowe pole określające długość całego datagramu UDP
- **Suma kontrolna** – 16 – bitowe pole służące do sprawdzania poprawności przesłanych danych.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

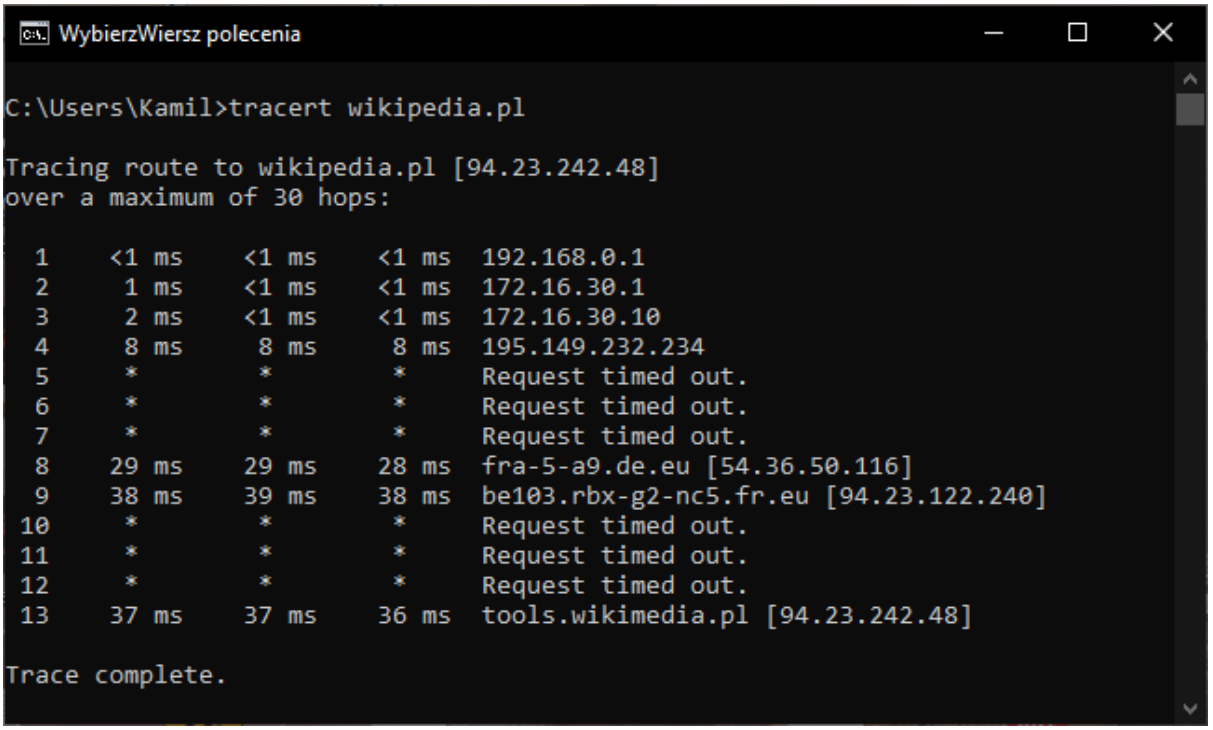
Polecenia Sieciowe (cmd i terminal)

Polecenia diagnostyczne Windows

ipconfig /all - wyświetla wszystkie informacje o kartach sieciowych

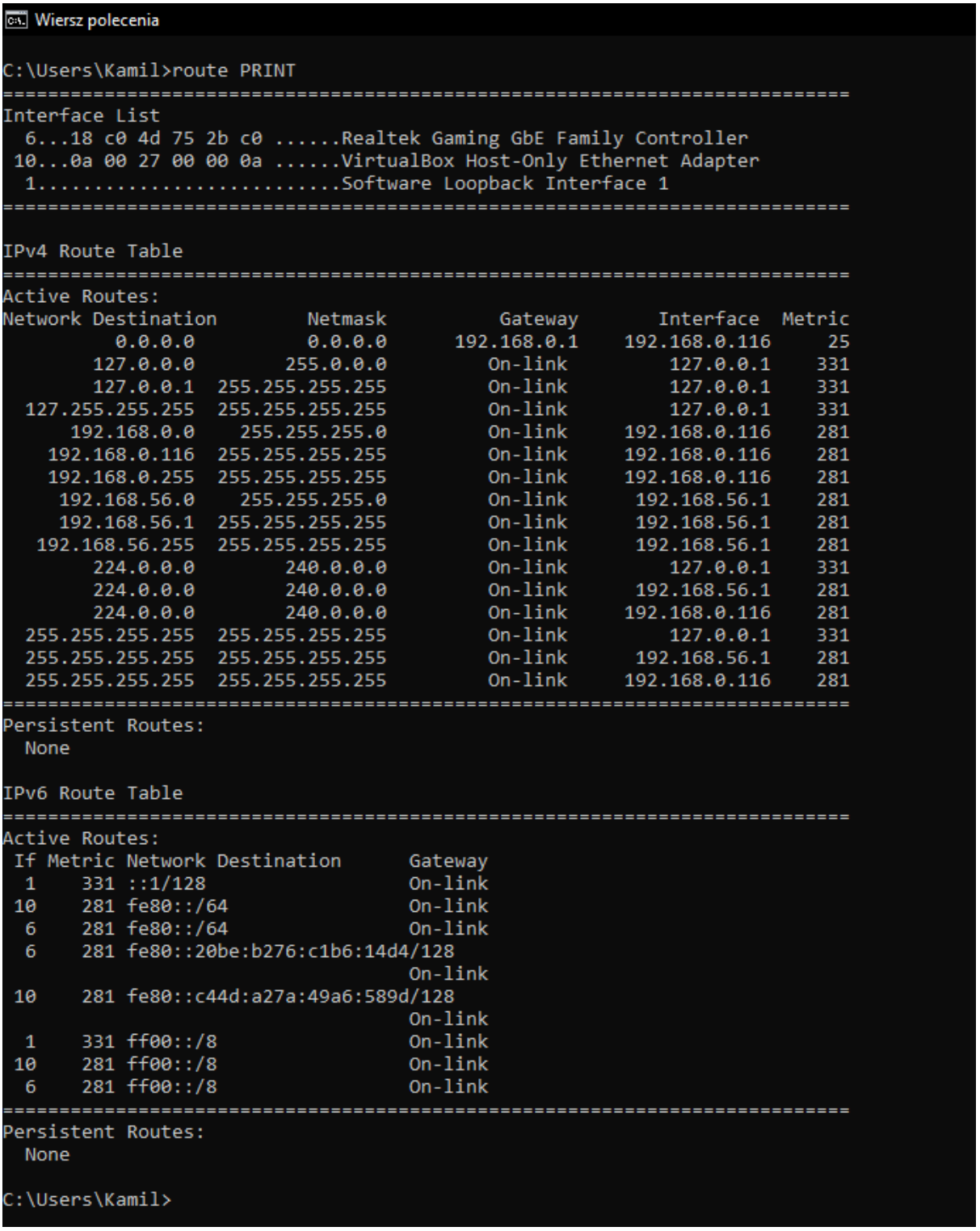


tracert - wyświetla poszczególne skoki pakietów w drodze do celu



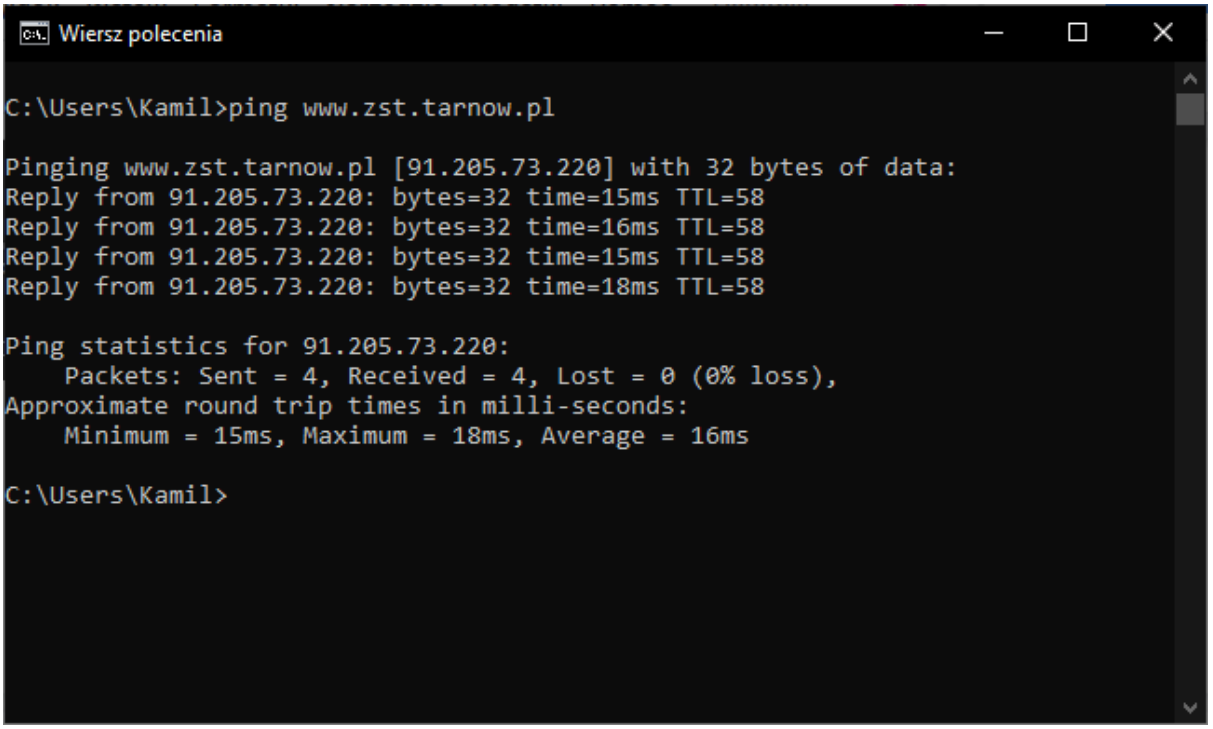
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

route print - wyświetla tablice routingu :



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

ping - służy do sprawdzania połączenia między komputerami. Wysłany pakiet ICMP, mierzone opóźnienie

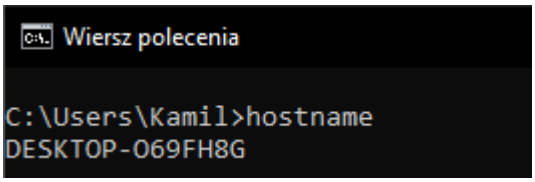


netstat - pokazuje aktywne połączenia i wykorzystywane porty (-o dla pokazania id procesu)

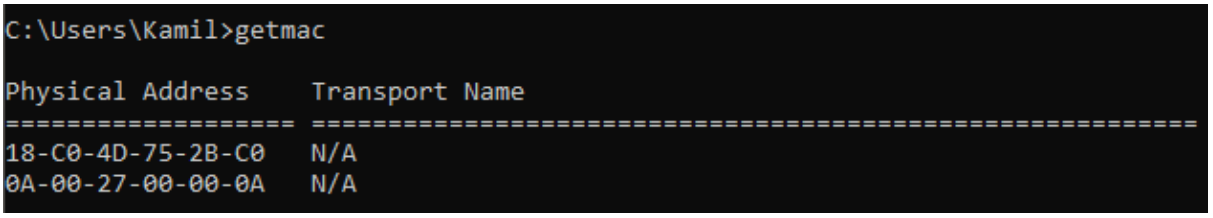
```
C:\Users\Kamil>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49831        DESKTOP-O69FH8G:49832  ESTABLISHED     9432
  TCP    127.0.0.1:49832        DESKTOP-O69FH8G:49831  ESTABLISHED     9432
  TCP    127.0.0.1:49838        DESKTOP-O69FH8G:49839  ESTABLISHED     9032
  TCP    127.0.0.1:49839        DESKTOP-O69FH8G:49838  ESTABLISHED     9032
  TCP    127.0.0.1:49845        DESKTOP-O69FH8G:49846  ESTABLISHED     8884
  TCP    127.0.0.1:49846        DESKTOP-O69FH8G:49845  ESTABLISHED     8884
  TCP    127.0.0.1:49849        DESKTOP-O69FH8G:49850  ESTABLISHED     8144
  TCP    127.0.0.1:49850        DESKTOP-O69FH8G:49849  ESTABLISHED     8144
  TCP    127.0.0.1:49892        DESKTOP-O69FH8G:49893  ESTABLISHED     12644
  TCP    127.0.0.1:49893        DESKTOP-O69FH8G:49892  ESTABLISHED     12644
  TCP    127.0.0.1:49961        DESKTOP-O69FH8G:49962  ESTABLISHED     12876
  TCP    127.0.0.1:49962        DESKTOP-O69FH8G:49961  ESTABLISHED     12876
  TCP    127.0.0.1:50141        DESKTOP-O69FH8G:50142  ESTABLISHED     5284
  TCP    127.0.0.1:50142        DESKTOP-O69FH8G:50141  ESTABLISHED     5284
  TCP    192.168.0.116:49707    51.103.5.186:https     ESTABLISHED     3400
  TCP    192.168.0.116:49734    162.159.136.234:https  ESTABLISHED     8856
  TCP    192.168.0.116:49740    a92-123-16-61:https    ESTABLISHED     9140
  TCP    192.168.0.116:49760    183:4070               ESTABLISHED     9972
  TCP    192.168.0.116:49769    25:https               ESTABLISHED     10044
```

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

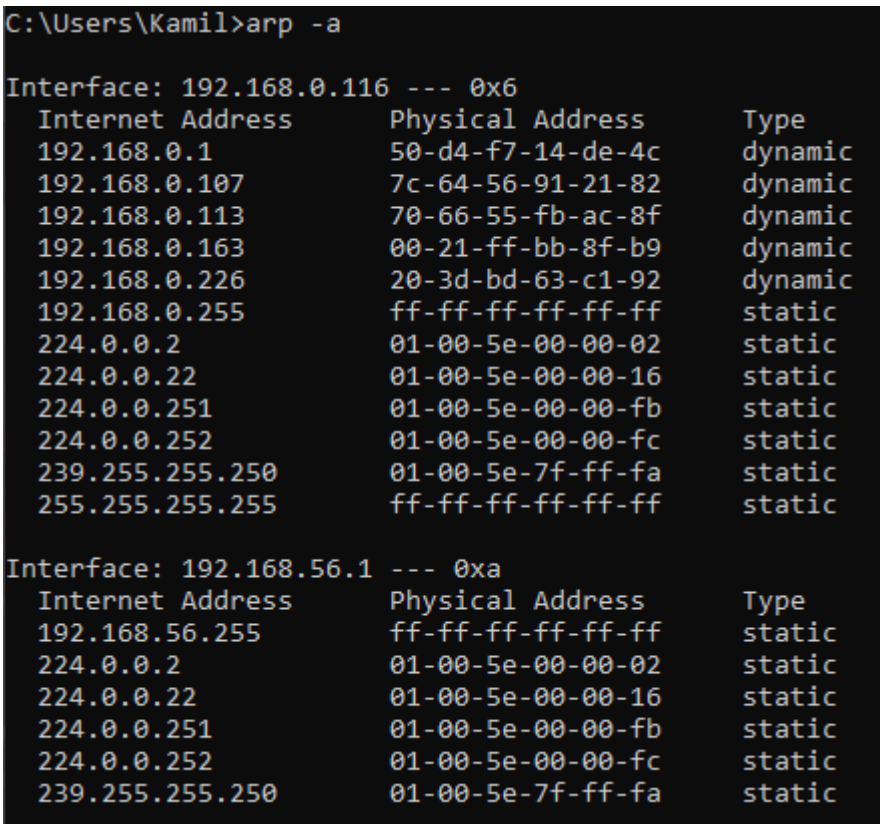
hostname - wyświetla nazwę tego komputera w sieci



getmac - Podaje adres fizyczny karty sieciowej.



arp - a - Znane odwzorowania adresów fizycznych na adresy sieciowe przechowywane są w tak zwanej tablicy ARP.



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

nslookup - wyświetla adres IP powiązany z daną domeną (i na odwrót)

```
C:\Users\Kamil>nslookup wikipedia.pl
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    wikipedia.pl
Addresses:  2001:41d0:2:7530::1001
          94.23.242.48
```

Polecenia diagnostyczne Linux

ifconfig -a (lub ip a) - pokazuje wszystkie dostępne interfejsy

```
root@kamil:/home/kamil_wolak# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe13:a87d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:13:a8:7d  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 97  bytes 9982 (9.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

hostname - wyświetla nazwę hosta

```
kamil_wolak@kamil:~$ hostname
kamil
```

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

netstat - pokazuje aktywne połączenia i informacje na ich temat

```
kamil_wolak@kamil:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 kamil:34046             65.9.66.57:https        TIME_WAIT
tcp        0      0 kamil:58130             waw02s13-in-f3.1e1:http ESTABLISHED
tcp        0      0 kamil:52168             82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 kamil:47326             waw02s16-in-f2.1e:https ESTABLISHED
tcp        0      0 kamil:59082             ec2-44-236-191-53:https ESTABLISHED
tcp        0      0 kamil:59714             65.9.66.52:https        TIME_WAIT
tcp        0      0 kamil:41006             server-13-32-25-6:https ESTABLISHED
tcp        0    849 kamil:57530             ec2-52-39-144-189:https ESTABLISHED
tcp        0      0 kamil:53418             93.184.220.29:http      ESTABLISHED
tcp        0      0 kamil:47230             server-13-32-25-2:https TIME_WAIT
tcp        0      0 kamil:46274             ec2-34-216-198-14:https TIME_WAIT
tcp        0      0 kamil:57524             ec2-52-39-144-189:https ESTABLISHED
tcp        0      0 kamil:58124             waw02s13-in-f3.1e1:http TIME_WAIT
tcp        0      0 kamil:52170             82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 kamil:59718             mil02s06-in-f2.1e:https ESTABLISHED
tcp        0      0 kamil:52074             waw02s17-in-f14.1:https ESTABLISHED
tcp        0      0 kamil:54218             waw02s07-in-f14.1:https ESTABLISHED
tcp        0      0 kamil:59706             65.9.66.52:https        TIME_WAIT
tcp        0      0 kamil:53828             65.9.66.58:https        TIME_WAIT
tcp        0      0 kamil:40274             waw02s16-in-f4.1e:https ESTABLISHED
tcp        0      0 kamil:33114             waw07s03-in-f3.1e:https ESTABLISHED
```

route -n - wyświetla tablicę routingu

```
kamil_wolak@kamil:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    0      0        0 enp0s3
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 enp0s8
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
192.168.0.1     0.0.0.0         255.255.255.255 UH    100    0        0 enp0s8
```

arp - wyświetla odwzorowania adresów fizycznych na adresy sieciowe przechowywane w tak zwanej tablicy ARP.

```
kamil_wolak@kamil:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
? (192.168.0.202) at <incomplete> on enp0s8
_gateway (192.168.0.1) at 50:d4:f7:14:de:4c [ether] on enp0s8
```

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

traceroute - wyświetla poszczególne skoki pakietów w drodze do celu

```
kamil_wolak@kamil:~$ traceroute www.onet.pl
traceroute to www.onet.pl (75.2.92.173), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  0.261 ms  0.341 ms  0.416 ms
 2  172.16.30.1 (172.16.30.1)  1.916 ms  1.911 ms  1.910 ms
 3  110.56.126.176.ip4.epix.net.pl (176.126.56.110)  5.731 ms  5.776 ms  5.730 m
s
 4  do-epix.pl-ktw01a-rd3.aorta.net (94.75.97.221)  6.290 ms  6.527 ms  6.526 ms
 5  pl-waw26b-rc1-ae-57-1422.aorta.net (84.116.253.89)  12.943 ms  12.924 ms  12
.936 ms
 6  pl-waw02a-ri1-ae-0-0.aorta.net (84.116.138.94)  12.097 ms  10.587 ms  11.054
 ms
 7  99.82.176.210 (99.82.176.210)  12.172 ms  12.382 ms  12.341 ms
 8  52.93.18.132 (52.93.18.132)  19.968 ms 52.93.18.36 (52.93.18.36)  19.239 ms
52.93.18.84 (52.93.18.84)  13.857 ms
```

nslookup - wyświetla adres IP powiązany z daną domeną (i na odwrót)

```
kamil_wolak@kamil:~$ nslookup wikipedia.pl
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   wikipedia.pl
Address: 94.23.242.48
Name:   wikipedia.pl
Address: 2001:41d0:2:7530::1001
```

Polecenia Konfiguracyjne Windows

Adresowanie interfejsu sieciowego Ethernet, na 192.168.0.10 , z maską /24 i bramą 192.168.0.1

```
C:\Windows\system32>netsh interface ipv4 set address "Ethernet" static 192.168.0.10 255.255.255.0 192.168.0.1
```

Dodaje serwer DNS do konfiguracji

```
C:\Windows\system32>netsh interface ipv4 set dnsservers "Ethernet" static 8.8.8.8
```

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

ipconfig

/all - wyświetla dodatkowe dane
/renew - odnawia wszystkie dzierżawy adresów z DHCP,
/relase - zwalnia wszystkie dzierżawy adresy z DHCP,
/flushdns - czyści bufor systemu rozpoznawania nazw DNS,
/displaydns - wyświetla zapamiętane nazwy systemu DNS (bufor DNS).

Dodawanie metryki :

```
route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
      destination^      ^mask      ^gateway     metric^    ^
                                                  Interface^
```

Polecenia Konfiguracyjne Linux

Adresowanie interfejsu sieciowego (enp0s8), adres ip i maska, up - uruchamiamy interfejs.

```
root@kamil:/home/kamil_wolak# ifconfig enp0s8 10.10.10.1 netmask 255.255.255.0 up
```

Dodawanie metryki

```
# ip route add 172.10.1.0/24 via 10.0.0.100 dev eth0
```

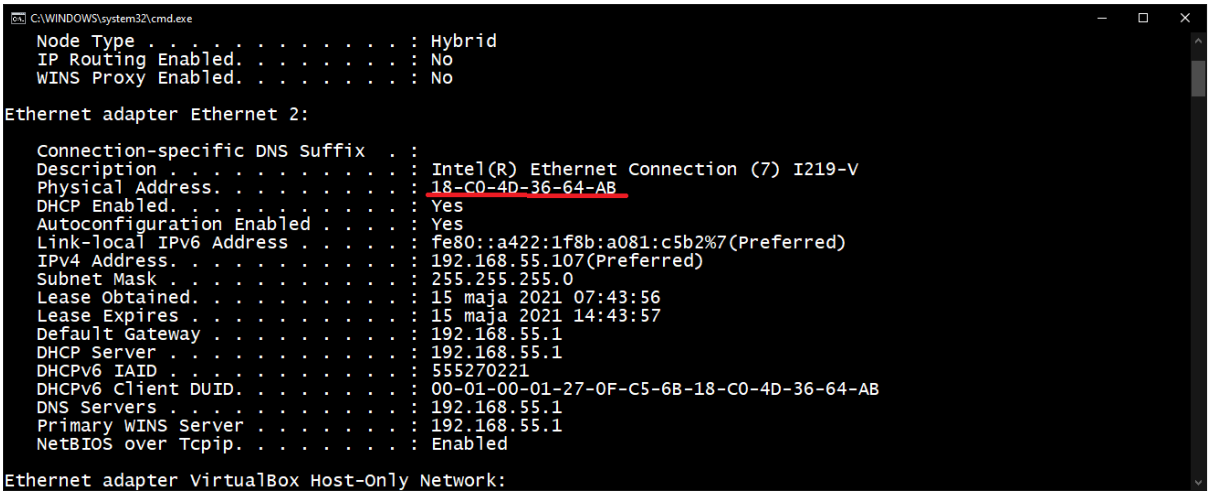
Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Adresowanie w sieci komputerowej

Rozróżniamy adresy:

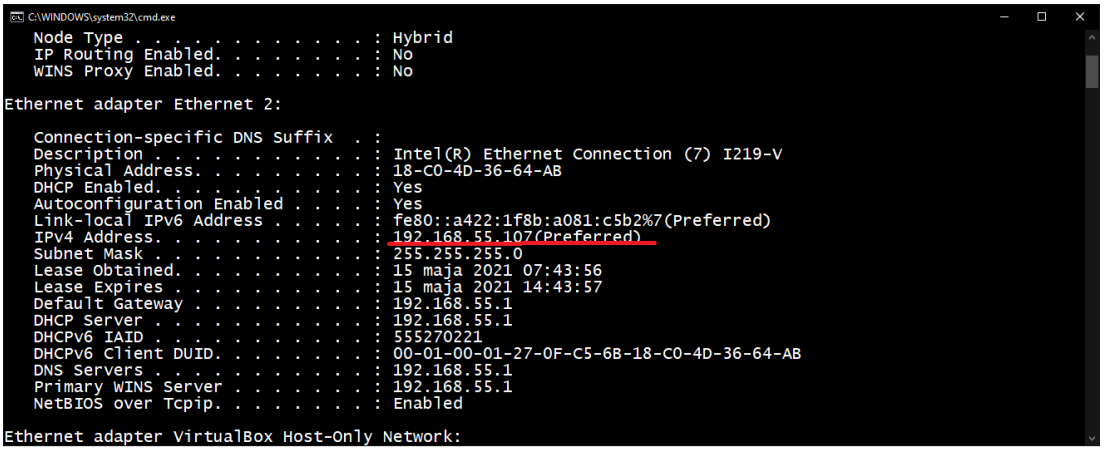
- ## Fizyczne

  Adres fizyczny jest nadawany przez producenta w każdej karcie sieciowej. Każdy z tych adresów jest unikalny, jego długość wynosi 48 bitów, a przedstawienie go jest w postaci szesnastkowej.



- ## Logiczne

  Jest to adres przydzielany podczas podłączenia do sieci. Każdy interfejs w komputerze otrzymuje adres IP. Adres ten jest unikalny w każdej podsieci. Każde urządzenie w sieci potrzebuje adresu IP aby komunikować się w sieci.



Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

IPV4

W adresacji IPv4 wyróżniamy kilka klas o różnych zakresach

Klasa A

Adresy IPv4 klasy A to wszystkie adresy zaczynające się od binarnego 0. Są to zatem adresy od 0.0.0.0 do 127.255.255.255. W adresach klasy A, pierwszy oktet jest adresem sieciowym, a pozostałe trzy oktety pełnią rolę adresu hosta. Maska sieciowa adresów klasy A ma więc formę 255.0.0.0 (/8 w notacji CIDR).

Mamy zatem do dyspozycji 8 bitów na adres sieciowy i 24 bity na adres hosta. W tej konwencji zaadresujemy więc 128 sieci. Dlaczego 128? W części sieciowej, która ma 8 bitów, pierwszy bit jest zawsze zerem – jest on "zafiksowany". Pozostaje nam zatem 7 bitów, którymi możemy manipulować. Mamy więc do dyspozycji 2^7 kombinacji – czyli 128.

Analogicznie w części adresowej hosta, pozostają nam 24 bity, którymi możemy manipulować. Mamy zatem do dyspozycji 2^24 adresów – 16 777 216. Całkiem sporo, co nie?

Klasa B

Adresy IPv4 klasy B to wszystkie adresy zaczynające się od binarnego 10. Są to zatem adresy od 128.0.0.0 do 191.255.255.255. W adresach klasy B, pierwsze dwa oktety są adresem sieciowym, a pozostałe dwa oktety pełnią rolę adresu hosta. Maska sieciowa adresów klasy B ma więc formę 255.255.0.0 (/16 w notacji CIDR).

Mamy zatem do dyspozycji 16 bitów na adres sieciowy oraz 16 bitów na adres hosta. W tej konwencji zaadresujemy więc 16 384 sieci. Dlaczego właśnie tyle? W części sieciowej, która ma 16 bitów, pierwszy dwa bity są zawsze ustawione na 01. Pozostaje nam zatem 14 bitów, którymi możemy manipulować. Mamy więc do dyspozycji 2^14 kombinacji – czyli 16 384.

Analogicznie w części adresowej hosta, pozostaje nam 16 bitów, którymi możemy manipulować. Mamy zatem do dyspozycji 2^16 adresów – 65 536. Nadal dużo, ale jednak już znacznie mniej niż w przypadku klasy A.

Klasa C

Adresy IPv4 klasy C to wszystkie adresy zaczynające się od binarnego 110. Są to zatem adresy od 192.0.0.0 do 223.255.255.255. W adresach klasy C, pierwsze trzy oktety są adresem sieciowym, a ostatni, czwarty oktet pełni rolę adresu hosta. Maska sieciowa adresów klasy C ma więc formę 255.255.255.0 (/24 w notacji CIDR).

Mamy zatem do dyspozycji 24 bity na adres sieciowy oraz 8 bitów na adres hosta. W tej konwencji zaadresujemy więc aż 2 097 152 sieci. Dlaczego właśnie tyle? W części sieciowej, która ma 24 bity, pierwsze trzy bity są zawsze ustawione na 110. Pozostaje nam zatem 21 bitów, którymi możemy manipulować. Mamy więc do dyspozycji 2^21 kombinacji – czyli 2 097 152.

Analogicznie w części adresowej hosta, pozostaje nam 8 bitów, którymi możemy manipulować. Mamy zatem do dyspozycji 2^8 adresów – 256. Widzimy więc, że adresy klasy C pozwalają na zaadresowanie ogromnej liczby sieci, składających się ze stosunkowo małej liczby hostów.

Klasa D

Adresy IPv4 klasy D to wszystkie adresy zaczynające się od binarnego 1110. Są to zatem adresy od 224.0.0.0 do 239.255.255.255. W adresach klasy D nie dokonujemy już podziału na adres sieci oraz hosta. Nie mamy tu zatem również wyróżnionej maski. Są to adresy przeznaczone do specjalnego użytku – tzw. adresy multicast. Czym są adresy multicast? To już jest temat na zupełnie osobny artykuł.

Klasa E

Ostatnia klasa z jaką mamy do czynienia to klasa E. Adresy IPv4 klasy E to wszystkie adresy zaczynające się od binarnego 1111. Są to zatem adresy od 240.0.0.0 do 255.255.255.255. W adresach klasy E również nie dokonujemy już podziału na adres sieci oraz hosta i nie mamy wyróżnionej maski. Co więcej – w ogóle nie wykorzystujemy tych adresów. Zakres ten został zarezerwowany przez organizację odpowiedzialną za standard IPv4 (IANA) na potrzeby przyszłych zastosowań. Jest to tzw. zakres eksperymentalny.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Adres sieci - adres w którym w części przeznaczonej dla hosta znajdują się same zera
Adres rozgłoszeniowy (broadcast) - adres w którym w części przeznaczonej dla hosta znajdują się same jedynki.

W przypadku braku połączenia z siecią komputer otrzymuje adres poprzez usługę APIPA.

Zakres APIPA: 169.254.0.1 - 169.254.255.254

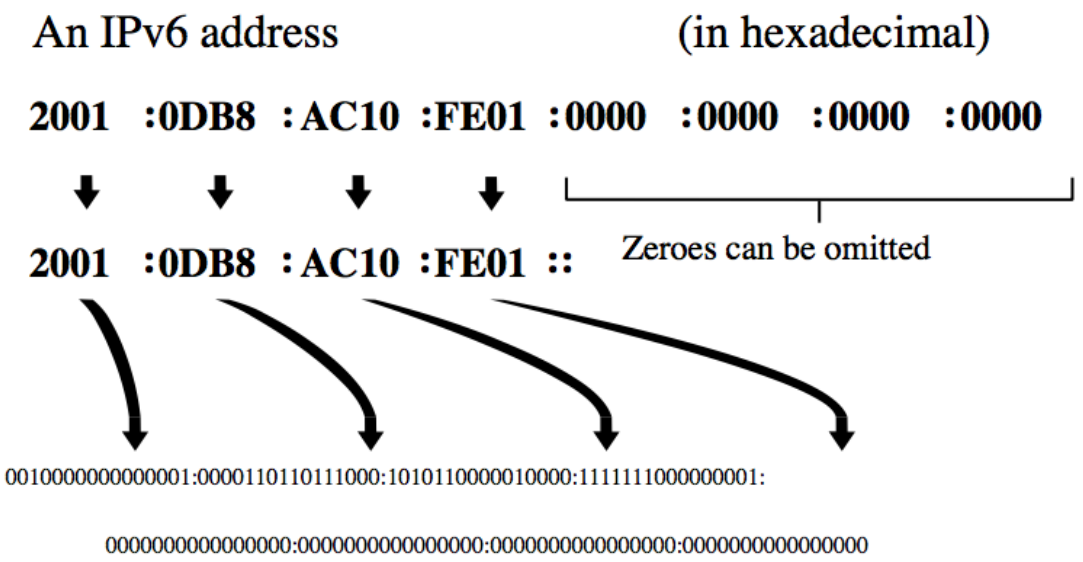
Adresy prywatne:

- 10.0.0.0 – 10.255.255.255 – dla sieci prywatnych klasy A (maska: 255.0.0.0/8)
- 172.16.0.0 – 172.31.255.255 – dla sieci prywatnych klasy B (maska: 255.240.0.0/12)
- 192.168.0.0 – 192.168.255.255 – dla sieci prywatnych klasy C (maska: 255.255.0.0/16)

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

IPv6

W IPv6 występują trzy typy adresów:
- unicast
- multicast
- anycast



Adres IPv6 składa się z 128 bitów. Dopuszczalny jest **tylko jeden** podwójny dwukropek.

Adresy specjalne:

Prefiks	Zasięg	Opis
`::/128`	nieokreślony	Adres nieokreślony
`::/0`	globalny	Adres trasy domyślnej w routingu (ang. *default*)
`::1/128`	interfejsu	Adres loopback. Odpowiednik adresu IPv4 127.0.0.1
`2000::/3`	globalny	Adresu unicastowe
`FC00::/7`	lokalny	Nieroutowalne adresy prywatne. Odpowiednik adresów IPv4 10.0.0.0/8, 172.16.0.0/13, 192.168.0.0/16
`FE80::/10`	lokalny	Adresy autokonfiguracji łącza
`FF00::/8`	określony w adresie	Adresy multicastowe

FE80::/10 - APIPA

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Opis pól nagłówka protokołu IPv6[5]

Bity	0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
0	Wersja	Klasa ruchu		Etykieta przepływu				
32	Długość danych				Następny nagłówek		Limit przeskoków	
64	Adres źródłowy (128 bitów)							
96								
128								
160								
192	Adres docelowy (128 bitów)							
224								
256								
288								

Podstawowy nagłówek protokołu składa się z następujących pól:

- Wersja (4 bity) – definiująca wersję protokołu, w przypadku IPv6 pole to zawiera wartość 6 (bitowo 0110)
- Klasa ruchu (8 bitów) – określa sposób w jaki ma zostać potraktowany pakiet danych. W poprzedniej wersji protokołu pole to nazywało się Type of Service, jednak ze względu na to, że w IPv6 stosowane są inne mechanizmy priorytetowania danych, nazwę tego pola zmieniono
- Etykieta przepływu (20 bitów) – pomagające odróżnić pakiety, które wymagają takiego samego traktowania (ich pole klasy ruchu ma tę samą wartość)
- Długość danych (16 bitów) – wielkość pakietu, nie wliczając długości podstawowego nagłówka (wliczając jednak nagłówki rozszerzające)
- Następny nagłówek (8 bitów) – identyfikuje typ następnego nagłówka, pozwalając określić czy jest to nagłówek rozszerzający czy nagłówek warstwy wyższej. W przypadku tego drugiego, wartość pola jest identyczna z wartością pola w protokole IPv4
- Limit przeskoków (8 bitów) – określa ilość węzłów, po odwiedzeniu których pakiet zostaje porzucony. W poprzedniej wersji protokołu pole to nosiło nazwę time to live i zawierało liczbę skoków, która była zmniejszana przez każdy odwiedzony węzeł
- Adres źródłowy (128 bitów) – adres węzła, który wysłał pakiet
- Adres docelowy (128 bitów) – adres węzła do którego adresowany jest pakiet

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Podział Sieci na podsieci

Obliczanie Ilości podsieci na podstawie maski

p - ilość podsieci
b - ilość bitów przeznaczonych dla podsieci
m - maska
mk - maska klasy
wzory:
b = m - mk <------- obliczanie bitów przeznaczonych dla podsieci
p = 2^b <------- obliczanie ilości podsieci

Przykład:

maska: 255.255.255.192(/26)
ip sieci : 192.168.0.0

Obliczanie:
mk = 24 (klasa c ma maskę /24)
26 - 24
2^2 = 4 (ilość podsieci)

Ważne!

Przy tworzeniu podsieci wyróżnia się podsieci efektywne:
są to takie które mają własne adresy rozgłoszeniowe i podsieci. Dlatego od ilości podsieci odejmuje się 2 aby wyodrębnić “podsieci efektywne”. Według powyższego przykładu są 4 podsieci, co oznacza że 2 będą efektywne. Pierwsza ma adres podsieci taki sam jak adres sieci, a ostatnia ma adres rozgłoszeniowy podsieci taki sam jak adres rozgłoszeniowy sieci, więc nie są one efektywne.

Obliczanie Ilości hostów na podstawie maski

h - ilość bitów przeznaczona na hosta
n - ilość hostów w podsieci
m - maska
wzory:
h = 32 - m <------- obliczanie bitów przeznaczonych dla hosta
n(h) = 2^h - 2 <------- obliczanie ilości hostów w podsieci

Odejmujemy 2 ze względu na adres rozgłoszeniowy i podsieci.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Przykład:

maska: 255.255.255.192(/26)
ip sieci : 192.168.0.0

Obliczanie:
32 - 26 = 6 (ilość bitów dla hosta)
2^6 - 2 = 64 - 2 = 62 (ilość hostów w podsieci)

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Zasady projektowania adresacji ip

Zasady przy projektowaniu

1. Wszystkie urządzenia w danej sieci/podsieci powinny mieć ten sam adres sieci/podsieci (Wtedy wiadomo że są w jednej sieci/podsieci)
2. Każde urządzenie powinno mieć unikatowy adres ip możliwy do nadania w danej sieci. (Nie wolno nadawać 2 identycznych adresów ip dla urządzeń w jednej sieci)
3. Nie można korzystać z adresów 255.255.255.255 i 0.0.0.0 ponieważ jest to adres rozgłoszeniowy całej sieci oraz adres używany do oznaczenia trasy domyślnej.
4. Nie można nadawać urządzeniom w sieci adresów rozgłoszeniowych i sieci/podsieci.
5. Maskę dobieramy tak aby zapewnić wystarczającą liczbę możliwych do zaadresowania hostów(np. jeśli potrzeba 25 hostów to wybieramy maskę dającą 30 hostów)

Technika VLSM

Pozwala na przydzieleniu podsiecią odpowiednio długiej maski. Dzięki takiemu rozwiązaniu możemy przydzielić odpowiednią ilość hostów i sprawić aby nasza sieć była odpowiednio wykorzystana i efektywna.

Praktyczne zastosowanie:
Mamy podzielić sieć tak aby zapewnić adresy dla kolejnych liczb urządzeń i jak najlepiej wykorzystać naszą sieć o adresie 192.168.5.0/24..
Szkoła A - 56 urządzeń
Szkoła B - 26 urządzeń
Szkoła C - 16 urządzeń

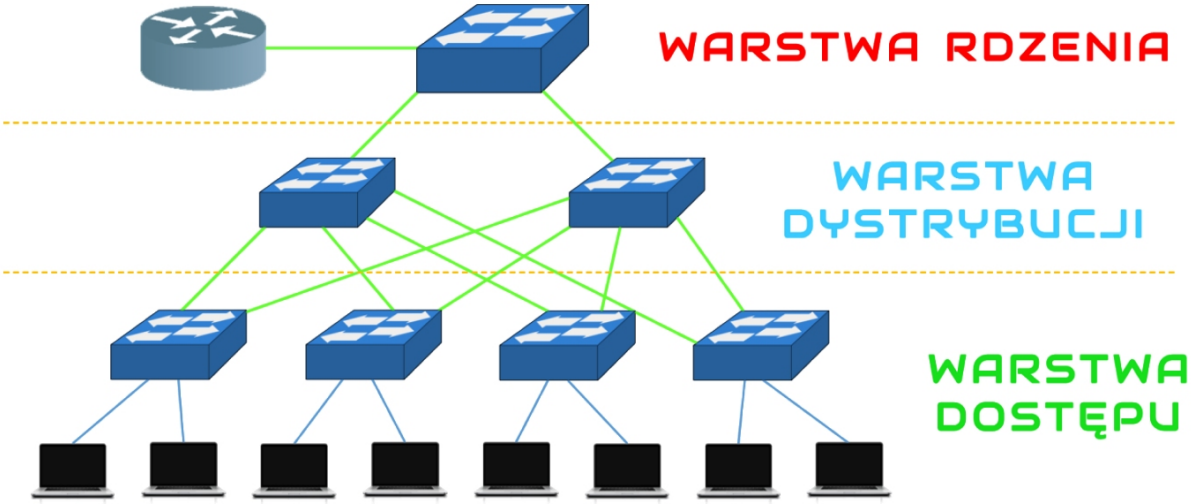
Numer podsieci	Adres podsieci	Adres podpodsieci	liczba hostów	Maska podsieci	Zastosowanie(cel)
1	192.168.5.0				Posiada adres całej sieci
2	192.168.5.64		64	/26	Szkoła A
3	192.168.5.128	192.168.5.128	32	/27	Szkoła B
		192.168.5.160	32	/27	Szkoła C
4	192.168.5.194				Posiada adres rozgłoszeniowy całej sieci

Należy pamiętać że nasze szkoły są umieszczone w różnych miejscach więc nie będą mogły pracować w jednej podsieci. W przykładzie widać że podzieliliśmy naszą podsieć na 2 kolejne aby wykorzystać odpowiednie dostępne adresy.

!!!. W przykładzie nie zostały uwzględnione adresy dla routerów które będą potrzebne aby rozdzielać nasze ip do odpowiednich szkół. (Chodzi, aby pokazać działanie maski o różnych długościach.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Model hierarchiczny sieci



Warstwa dostępu - Umożliwia połączenia urządzeń z siecią oraz sprawuje kontrolę nad komunikowaniem się urządzeń w sieci

Warstwa dystrybucji - gromadzi dane otrzymane od przełączników z warstwy dostępu przed ich transmisją do warstwy rdzenia. Warstwa ta kontroluje przepływ danych w sieci oraz wyznacza domeny rozgłoszeniowe. **Realizuje również routing między VLAN.**

Warstwa rdzenia - gromadzi ruch sieciowy ze wszystkich urządzeń warstwy dystrybucji. Warstwa ta może być połączona z zasobami internetowymi.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Zasady projektowania lokalnych sieci komputerowych

Cechy sieci:

- **Skalowalność**

O skalowalności sieci możemy mówić wówczas, kiedy np. bez ingerencji w jej logikę możemy podłączyć kolejnych użytkowników. Praktycznym przykładem skalowalności sieci jest np. użycie przełączników posiadających większą liczbę portów niż wymagane to jest na etapie projektowania sieci.

- **Nadmiarowość**

Zakłada wykorzystanie większej liczby urządzeń aktywnych niż jest to na daną chwilę wymagane. Zamiast jednego przełącznika w danym segmencie, można zainstalować dwa i odpowiednio je skonfigurować tak, aby w momencie awarii jednego z nich, drugi przejął jego funkcję bez ingerencji administratora.

- **Wydajność**

Zakłada wykorzystanie sprzętu, który pozwoli na szybkie i sprawne jej działanie. Wydajność zależy głównie od zastosowanego sprzętu, a także mediów transmisyjnych. Projektując sieć należy uwzględnić w jakim zakresie użytkownicy będą z niej korzystać i jaki standard sieciowy będzie do tego odpowiedni.

- **Bezpieczeństwo**

Sieć musi zostać tak wykonana, aby postronne osoby nie miały dostępu do sprzętu sieciowego, zarówno w rozumieniu fizycznym, sprzęty po prostu muszą usytuowane być w miejscu niedostępnym dla osób postronnych, jak również w sensie logicznym,

- **Łatwość utrzymania i zarządzania siecią**

Odpowiednie umiejscowienie elementów sieci, dokładny ich opis i dokumentacja, pozwolą na łatwą konserwację sieci, a także na szybkie odnajdywanie potencjalnych usterek.

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Struktura dokumentacji projektowej

Fazy realizacji projektu

- audyt - rozpoznawanie
- projektowanie systemu
- impedancja systemu
- instalacja, testowanie, usuwanie błędów
- serwisowanie i dalszy rozwój systemu

Dokumentacja projektowa zawiera

- nazwa firmy, tytuł projektu, data wykonania
- wykaz używa skrótów
- spis treści
- opis projektu
- cel projektu
- zakres dokumentacji (wymagania dotyczące elementów sieci)
- dokumentację techniczną
    - plany budynków
    - karty katalogowe
    - schemat logiczny
    - dokumentacja centralnego punktu sieci i punktów rozdzielczych
    - dokumentacja rejonów okablowania
    - projekt koncepcyjny sieci i innych wyspecjalizowanych
    - numeracja gniazd w panelu krosowym
    - opis procedur odbioru okablowania
    - wyniki testów i pomiarów
    - spis komponentów i ich rozmieszczenie
    - protokół odbioru
    - kosztorys

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Projektowanie okablowania strukturalnego

Elementy okablowania strukturalnego:

- typ nośnika danych (typ przewodu)
- okablowanie pionowe
- punkty rozdzielcze
- okablowanie poziome
- gniazda abonenckie
- połączenia systemowe
- połączenia telekomunikacyjne budynków

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Punkty dystrybucyjne

- PCS - punkt centralny sieci

Obsługuje grupę budynków w wielkich kompleksach
Punkt Centralny Sieci. Zawiera farm serwerów, punkt dostpu do Internetu oraz Centralny Punkt Dystrybucyjny okablowania. Jest to strategiczne i główne pomieszczenie sieci LAN. Stanowi ono serce całej infrastruktury teleinformatycznej.

- CPD - centralny punkt dystrybucyjny

  Tutaj zbiega si całe okablowanie pionowe i międzybudynkowe`. W tym miejscu umieszczona jest take 19- calowa szafa dystrybucyjna (1x42U lub z podwójnym stelaem 2x42U). Jest to najważniejszy element systemu okablowania strukturalnego.

- BPD - budynkowy punkt dystrybucyjny

  Sprzęga on całe okablowanie z obszaru podległego sobie budynku z CPD. Do tego punktu zbiegaj si take wszystkie kable z kondygnacyjnych punktów dystrybucyjnych.

- ICPD - kondygnacyjny punkt dystrybucyjny

  Swoim zasięgiem obejmuje jedynie pojedyncze piętra lub skrzydła budynku. W mniej rozległych systemach okablowania hierarchia na tym elemencie si koczy.

- LPD - lokalny punkt dystrybucyjny

  Najczęściej jest to fizycznie mała 19- calowa wisząca szafka, której zadaniem jest przedłużenie segmentu sieci. W dużych obszarowo kondygnacjach możemy mieć problem z utrzymaniem stosownej odległości kabla między punktem abonenckich a KPD. W takim przypadku zachodzi konieczno zainstalowania LPD, który przedłuży segment sieci. Dla standardu sieci Ethernet 100Base-TX maksymalna długo kabla wynosi 100 m.

Główny punkt rozdzielczy MDF (ang. Main Distribution Frame) to punkt centralny okablowania w topologii gwiazdy. Zbiegaj si w nim kable z sąsiednich budynków, piter i miejskiej centrali telefonicznej oraz odchodź przebiegi pionowe (do pośrednich punktów dystrybucyjnych IDF w obiekcie) i poziome do punktów abonenckich zlokalizowanych w pobliżu MDF (do 90m). Często umieszczony jest na parterze lub na środkowej kondygnacji budynku (np. 2 piętro budynku 4 piętrowego), w jego pobliżu znajduje się centrala telefoniczna, serwer lub inny sprzęt aktywny.

• Pośredni punkt rozdzielczy IDF (ang. Intermediate Distribution Frame) lub inaczej SDF (ang. Sub-Distribution Frame) to lokalny punkt dystrybucyjny obsługujący najczęściej dany obszar roboczy lub pitro. Jest obszarem przejściowym między okablowaniem pionowym i poziomym. Jest to miejsce, którego mona dokonywa o poszerzenia sieci poprzez rozbudowywanie przebiegów poziomych o zarządza wykorzystaniem tych przebiegów poprzez organizowanie ich połączeń o przeprowadza ich testowanie

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Normy przy projektowaniu sieci

Organizacje standaryzacyjne

- **ANSI** - American National Standards Institute
- **IEEE** - The institute of Electrical and Electronics Engineers
- **ISO** - International Organization for Standardization
- **IETF** - Internet Engineering Task Force
- **Unia Europejska** - publikuje normy europejskie
- **EIA/TIA** - Electronics Industry Association/Telecommunications Industry Association

Normy dotyczące okablowania strukturalnego:

ISO 11801 - podstawowa norma
EN 50173 - europejska norma
PL-EN 50174-1 - polska norma - projektowanie i montaż okablowania
PL-EN 50174-2 - instalacja okablowania wewnątrz budynku
PL-EN 50174-3 - instalacja okablowania na zewnątrz budynku

Najważniejsze zalecenia wynikające z powyższych norm

- Okablowanie poziome powinno tworzyć nieprzerwane połączenie od punktu dystrybucyjnego do punktu abonenckiego
- Należy umieścić jeden punkt abonencki 2x RJ-45 na każde $10m^2$ powierzchni biurowej .
- Na każdym piętrze budynku powinien być punkt dystrybucyjny.
- Wszystkie kable muszą być zakończone w gniazdach abonenckich, i szafach dystrybucyjnych.
- W obrębie całej sieci powinno się stosować jednakowe przewody (kable miedziane o jednakowej impedancji i średnicy, a kable światłowodowe o jednakowych włóknach)
- Rozplot kabla UTP nie powinien być większy niż 13 mm
- Każdy element systemu powinien być czytelnie oznaczony.
- Sieć musi posiadać pełną dokumentację

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Zalecenia dotyczące kabli w przebiegach poziomych:

Norma zaleca stosowanie 4-parowego kabla STP lub UTP kategorii co najmniej 5e.
Parametry kabla:
- średnica przewodów: 0,45/0,65 mm
- nominalna impedancja: 100V ± 15%
- tłumienność: dla kategorii 5 przy f = 100 MHz - 24,0 dB, dla kategorii 6 przy f = 100 MHz - 21,1 dB

- Długość kabla nie może przekraczać 100m.
- Maksymalna długość przebiegu kabla poziomego między punktem abonenckim, a punktem dystrybucyjnym w panelu krosowym wynosi 90m.
- Maksymalna długość kabli krosowych między panelem krosowym, a przełącznikiem wynosi 5m.
- Łączna długość kabla stacyjnego i krosowego wynosi 10m.

Zasady układanie kabla w przebiegach poziomych:

- kable biegnące ponad sufitem podwieszonym nie powinny być mocowane do konstrukcji sufitu
- Odległość między punktami mocowania kabli poziomych nie powinny być większe niż 1,2 - 1,5 m
- Należy kable prowadzić prostopadle lub równolegle do korytarza
- Kable wchodzące i wychodzące do/z pomieszczenia (pod kątem 90°) powinny skręcać łagodnie **(minimalny promień skrętu = 8 średnic kabla)**
- Należy sprawdzić czy kable nie są naprężone na końcach i na swoim przebiegu. Nie wolno owijać kabli dookoła rur, kolumn itp.
- Kable na całej swojej długości od gniazda abonenckiego do punkt dystrybucyjnego, muszą być wolne od sztukowań, zagnieceń i nacięć lub złamań
- Nie można rozdzielać par przewodów na dwa kanały komunikacyjne
- Promień zgięcia:
  dla skrętki UTP - 4 średnice kabla
  dla skrętki STP - 6 średnic kabla

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

dla kabla światłowodowego - od 10 do 20 średnic kabla (w zależności od sposobu wykorzystania)

Odległości od źródeł zasilania:

- 30 cm od wysokonapięciowego oświetlenia (świetlówki)
- 90 cm od przewodów elektrycznych 5 KVA lub więcej
- 100 cm od transformatorów i silników

Okablowanie Pionowe - wymagania instalacyjne

Połączenia wykonywane :

- kablem ekranowanym (Kat 6)
- światłowód

Maksymalna odległość 90 m - skrętka FastEthernet / GigabitEthernet
Maksymalna odległość światłowód 1,5 km

10 GigabitEthernet → 55 metrów

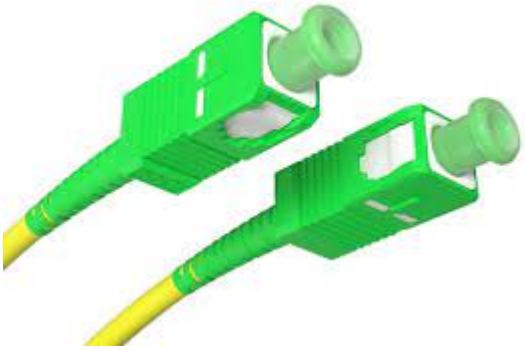
Pozostałe wymagania

- Po rozszyciu kabla w gnieździe przewody nie mogą wystawać więcej niż 25 mm poza płaszcz, a pary nie mogą być rozkręcone na długości większej niż 13 mm
- Instalując gniazda należy pamiętać o zapasie kabla
- Kable doprowadzone do punktów dystrybucyjnych powinny być logicznie pogrupowane
- Lokalizacja punktów dystrybucyjnych powinna być taka, aby przebiegi poziome nie przekraczały 90 m
- IDF należy podzielić na logiczne sekcje, grupując połączenia o podobnej funkcji

Dokument made by Jakub Ziewacz && Kamil Wolak © 2021

Najczęściej wykorzystywane końcówki:

- SC - plastikowa obudowa i pewne połączenie



- LC - mniejsze od poprzedniego, dość popularne ze względu na małe gabaryty i na użycie go w modułach SFP

- ST - metalowe, przypominające elektryczne złącze BNC, stosowane częściej w sieciach wielomodowych.