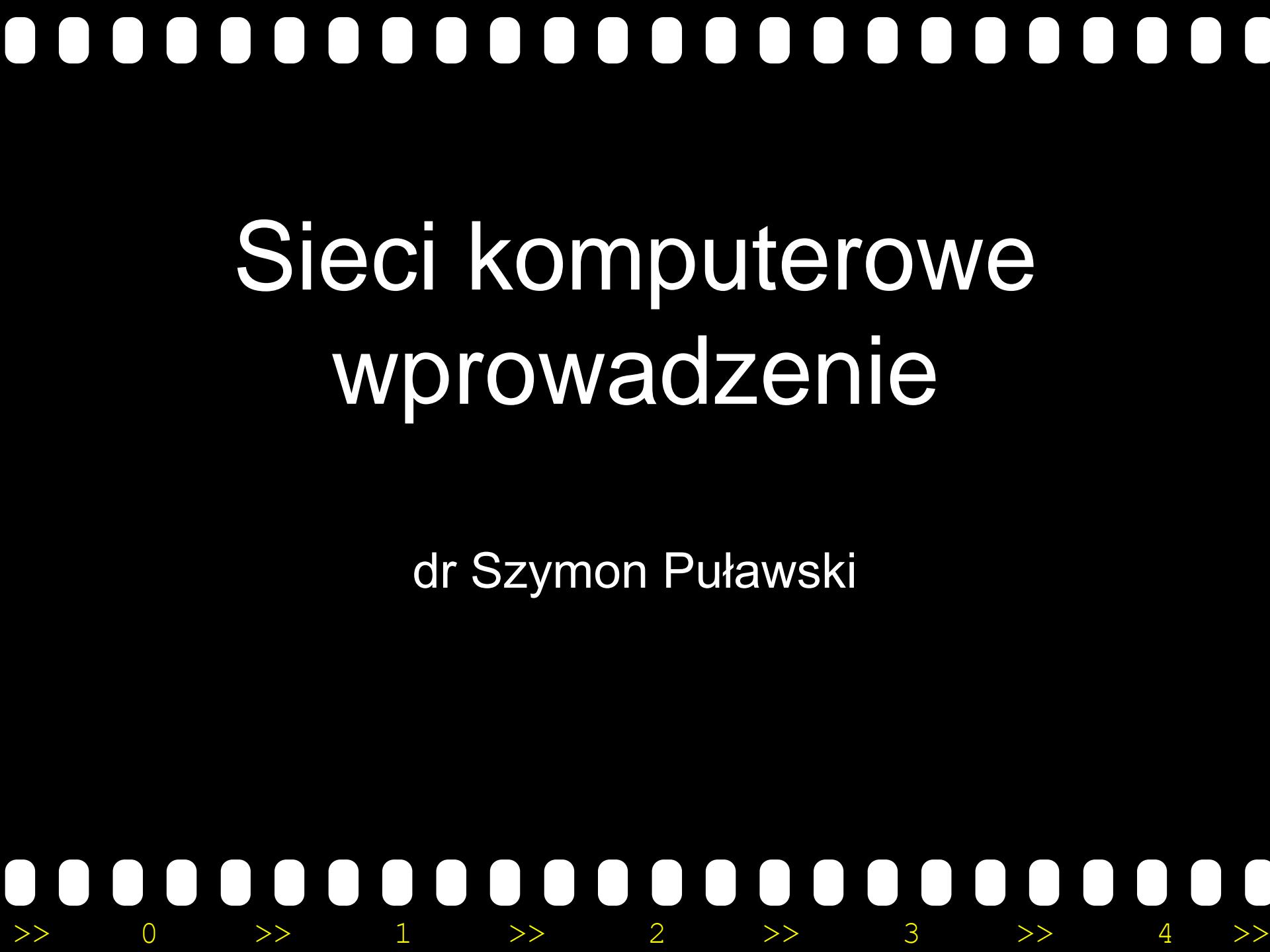


| | |
|-----------|-----|
| Wyklad_1 | 2 |
| Wyklad_2 | 44 |
| Wyklad_3 | 109 |
| Wyklad_4 | 159 |
| Wyklad_5 | 210 |
| Wyklad_6 | 240 |
| Wyklad_7 | 327 |
| Wyklad_8 | 400 |
| Wyklad_9 | 419 |
| wyklad_10 | 447 |



Sieci komputerowe wprowadzenie

dr Szymon Puławski

Plan wykładu

- Wprowadzenie: historia sieci komputerowych, model ISO-OSI, rodzaje i topologie sieci.
- Media transmisyjne i ich parametry, rodzaje okablowania.
- Rozwój standardu Ethernet: podstawy funkcjonowania sieci Ethernet, standardy: Fast Ethernet, Gigabit Ethernet i 10 Gigabit Ethernet, STP.
- WAN - Sieci Frame Relay: budowa sieci, urządzenia komunikacyjne, protokół transmisji, budowa komórki, rodzaje połączeń, klasy ruchu, sygnalizacja, model odniesienia, ILMI, LANE.
- Protokoły z rodziny TCP/IP: IP, ICMP, IGMP.
- Adresacja w sieciach IP: IPv4 i IPv6.
- Uzyskiwanie adresu IP: statyczne, ARP/RARP, BOOTP, DHCP.
- Protokoły warstwy transportowej stosu protokołów TCP/IP: UDP, TCP.
- DNS.
- Routing w sieciach IP: zasady wyboru trasy, tablica routingu, protokoły routingu dynamicznego (RIP/RIP2, OSPF, BGP).
- Sieci bezprzewodowe WLAN.
- Podstawowe usługi sieciowe: poczta elektroniczna (SMTP, IMAP, POP3, autoryzacja, zabezpieczenia), transmisja danych (FTP, SCP), zdalny dostęp (telnet, SSH, usługi terminalowe), serwisy informacyjne (HTTP).
- Ochrona danych w sieci: metody projektowania sieci bezpiecznych, analiza ruchu, firewall, VPN, IDS.
- Programowanie sieciowe



Classroom z wykładami

- Kod zajęć:
 - ce2gfjz





Literatura

- Bradford Russell *PODSTAWY SIECI KOMPUTEROWYCH*
- Krysiak Karol *SIECI KOMPUTEROWE. KOMPEDIA*
- Witold Wrotek *SIECI KOMPUTEROWE. KURS*



Podstawy podstaw



- Sieć komputerowa to medium umożliwiające połączenie dwóch lub więcej urządzeń w celu wzajemnego komunikowania się.

Sieci komputerowe – dlaczego?

- Potrzeba swobodnego, efektywnego i bezpiecznego komunikowania się jest niewątpliwie najważniejszą przyczyną powstania sieci komputerowych.
- Lata 40te XXw. skonstruowano pierwsze komputery - dostęp do nich miała stosunkowo niewielka grupa osób
- Latach 50te XXw. wynalezienie układu scalonego - miniaturyzacja sprzętu, opracowanie systemów wielodostępnych z podziałem czasu i pierwszych systemów operacyjnych oraz języków programowania wysokiego poziomu.
- Dostęp do komputerów możliwy był z poziomu terminali znajdujących się albo bezpośrednio w centrach obliczeniowych, albo w lokalizacjach połączonych z centrum dedykowaną, telefoniczną linią dzierżawioną, albo indywidualnie za pomocą modemu i komutowanej linii telefonicznej.

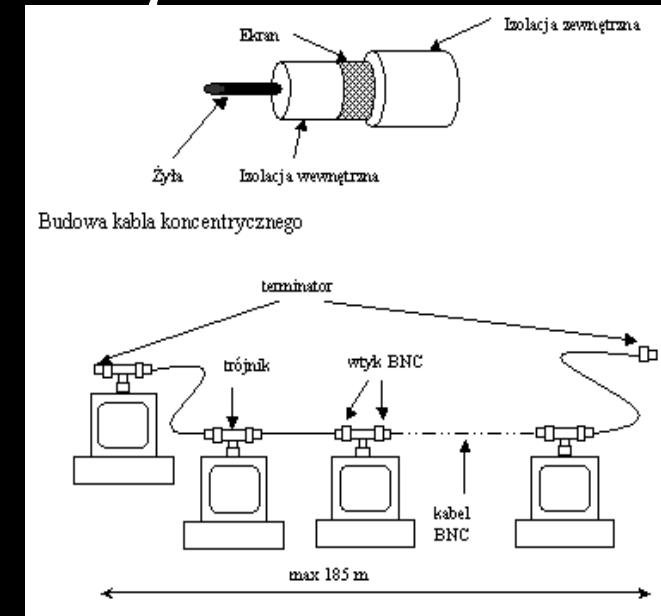


Pierwsze sieci komputerowe

- Wraz z upowszechnieniem się stosowania komputerów pojawiła się potrzeba bardziej efektywnego i szerszego dostępu do ich zasobów oraz potrzeba automatycznej wymiany danych między komputerami.
- Lata 60te XXw. Departament Obrony Stanów Zjednoczonych rozpoczął tworzenie sieci komputerowej (**ARPANET**), której celem było połączenie uniwersytetów oraz innych jednostek realizujących projekty dla armii w celu umożliwienia im wzajemnego dostępu do mocy obliczeniowej komputerów.
- Gdy w późniejszym okresie opracowano rodzinę **protokołów TCP/IP** i zaimplementowano je w systemach UNIX'owych okazało się, że niemal natychmiast sieć ARPANET powiększyła się o wszystkie lokalne sieci komputerowe zainstalowane w uniwersytetach stanowych.
- W podobnym okresie, na Uniwersytecie Hawajskim prowadzone były badania umożliwiające komunikację za pomocą nadajników krótkofalarskich. W wyniku tych prac powstał protokół **ETHERNET**, który z czasem stał się niemal jedynym protokołem komunikacyjnym we wszystkich sieciach lokalnych.

Co dalej z siecią?

- Ponieważ komputery, a dokładniej minikomputery znalazły zastosowanie w firmach komercyjnych, także i tutaj pojawiła się potrzeba wzajemnego komunikowania się, np. między oddziałami tej samej firmy w celu wymiany i synchronizacji danych.
- W tym obszarze stosowano głównie rozwiązania autorskie pochodzące od firm, które były producentami sprzętu komputerowego (Xerox, Intel, DEC, IBM). W zdecydowanej większości protokoły te zostały całkowicie wyparte w sieciach lokalnych przez protokół Ethernet, natomiast ich elementy można znaleźć wśród protokołów stosowanych w centralach telefonicznych.



BBS (Bulletin Boards)

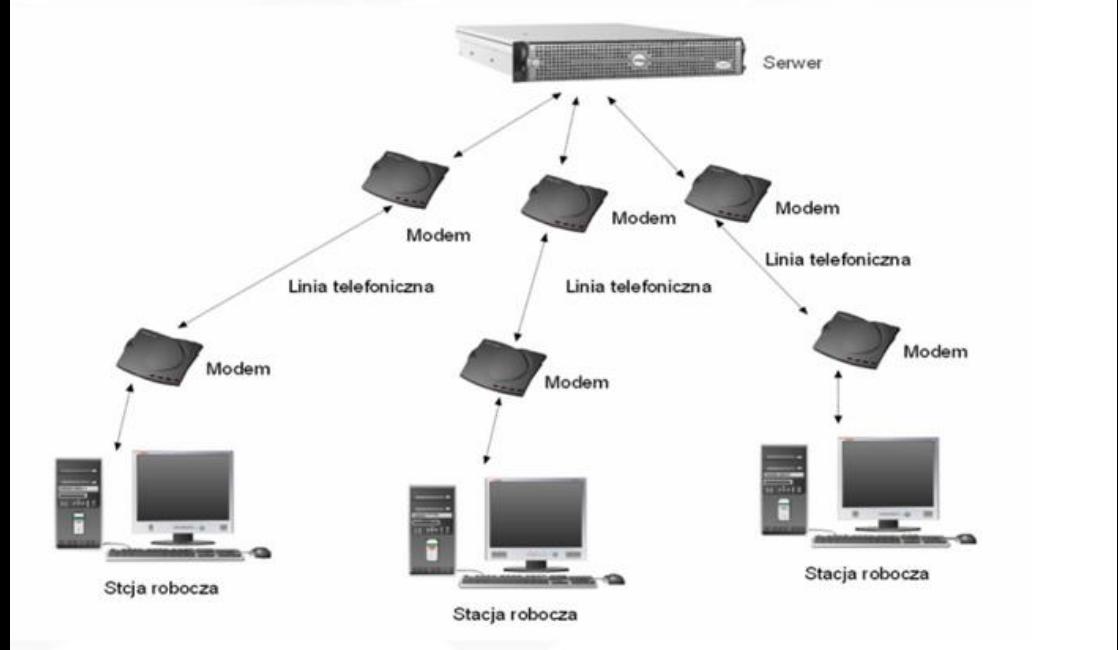
- Komputery dla mas = sieć dla mas?
- W latach 80tych XXw. opracowano sposób komunikacji typu punkt-punkt oparty na łączności modemowej wykorzystującej standardowe, komutowane łącza klasycznej sieci telefonicznej. Stworzono specjalne centra zwane BBS'ami pełniące rolę punktów kontaktowych, za pomocą których można było wymieniać wiadomości i pliki.

- Zaletą BBS'ów były: porównywalnie niższy koszt i istnieniu danego BBS'u oraz znać jego numer.

– Tani koszt dostępu: wiadomości miały jedynie postać tekstową, mały rozmiar plików (transmisji 1200/2400 bps) = krótki czas płatnego połączenia komutowanego.

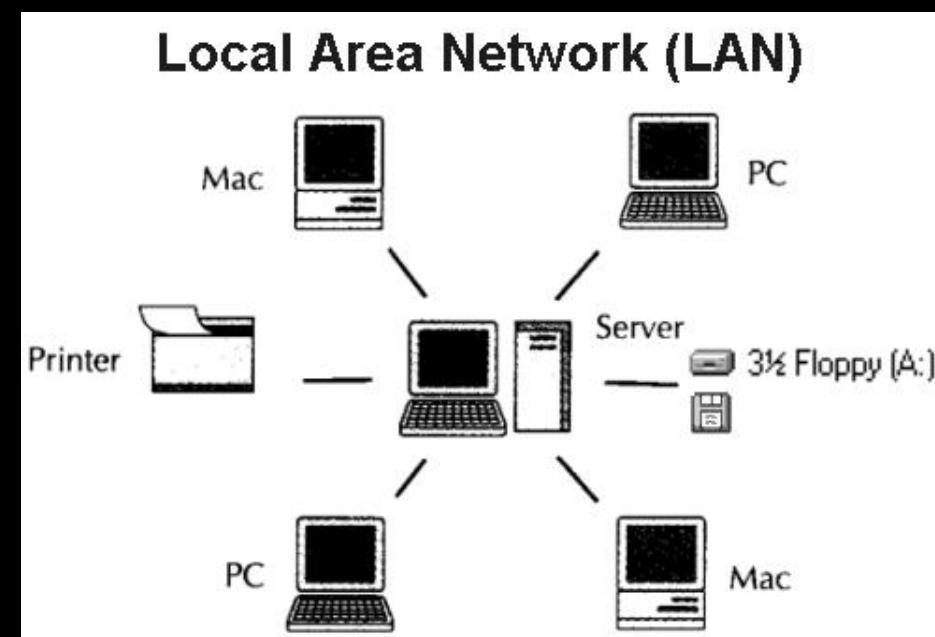
- Wadą BBS'ów było to. Użytkowników tylu ile linii telefonicznych każde połączenie=modem.

– ale jakość sieci nie jest jednolita. BBS'ów brak znanej jego numeru



- Opracowanie standardów dotyczących sieci lokalnych (lata 80).
- Gwarancja kompatybilności sprzętowej.
- Standardem stały się konstrukcje oparte na sieciowym systemie operacyjnym z centralnym serwerem plików, wydruku oraz poczty elektronicznej, zapewniającym autentykację użytkowników i autoryzację dostępu do zasobów

Sieci lokalne



Internet

- W 1990 roku, gdy sieć ARPANET zaczęła się gwałtownie rozrastać zmieniono jej nazwę na Internet.



Internet

- Funkcjonująca obecnie konstrukcja Internetu, zarówno na poziomie globalnym jak i pojedynczej sieci lokalnej oparta jest na tych samych zasadach jakie opracowano i opublikowano na przełomie lat 80tych i 90tych XXw. Zasadnicze zagadnienia, które związane są z budową Internetu dotyczą takich spraw jak:
 - łączenie komputerów w lokalną sieć komputerową,
 - podłączanie do sieci pojedynczych komputerów w sytuacji dużych odległości,
 - rozbudowa lokalnych sieci komputerowych,
 - komunikacja między sieciami lokalnymi,
 - usługi sieciowe,
 - bezpieczeństwo sieci,
 - zarządzanie i monitoringu sieci.

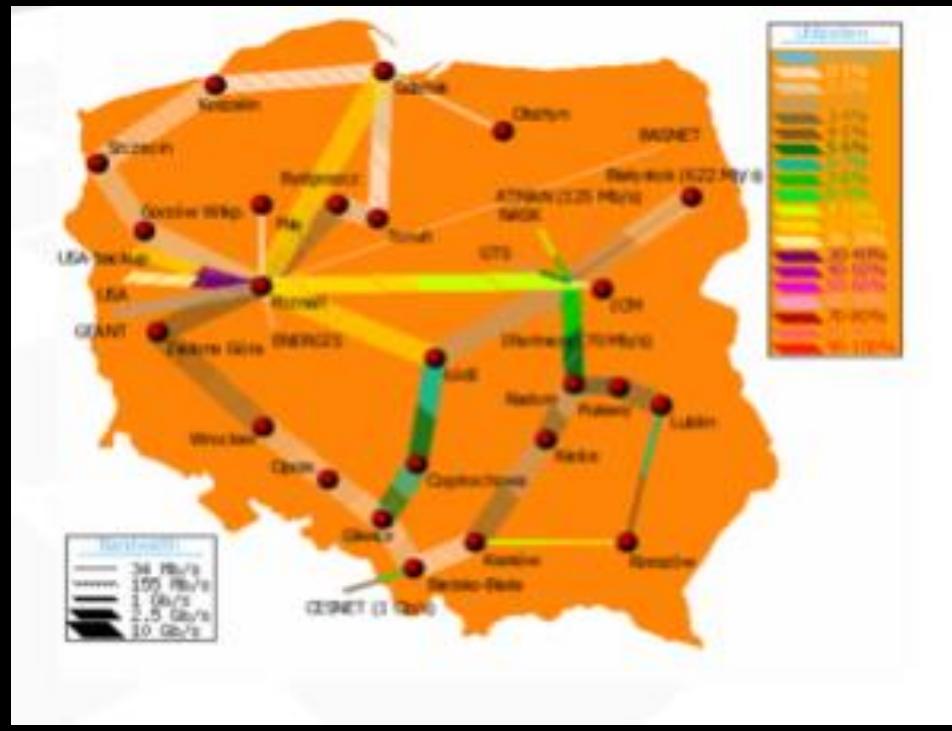
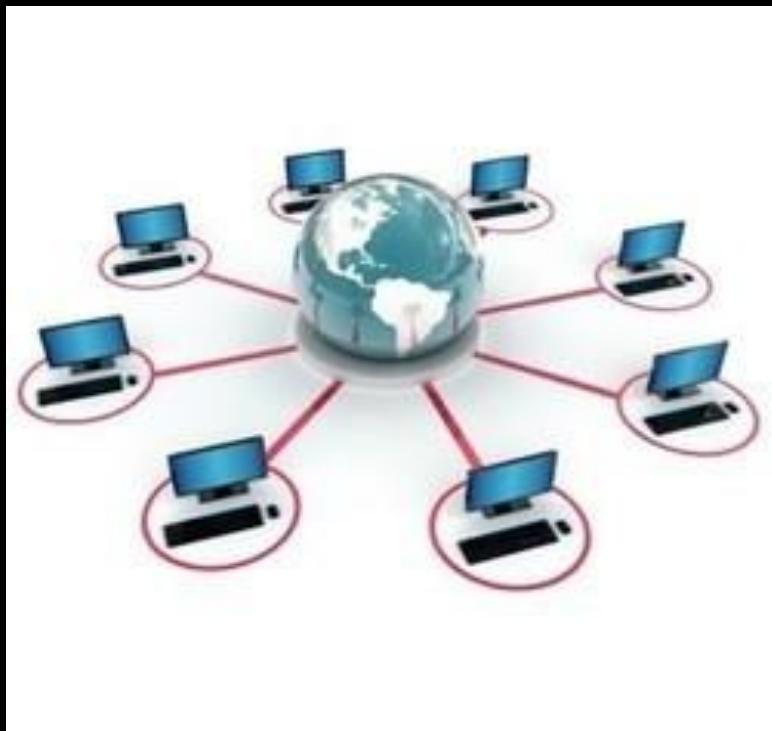


Typy sieci

- WAN (Wide Area Network)
- MAN (Metropolitan Area Network)
- LAN (Local Area Network)
- PAN (Private Area Network)

WAN

- Sieci rozległe charakteryzują przede wszystkim długie połączenia zlokalizowane na stosunkowo dużym obszarze takim jak województwo, kraj, kontynent czy cały glob.



LAN



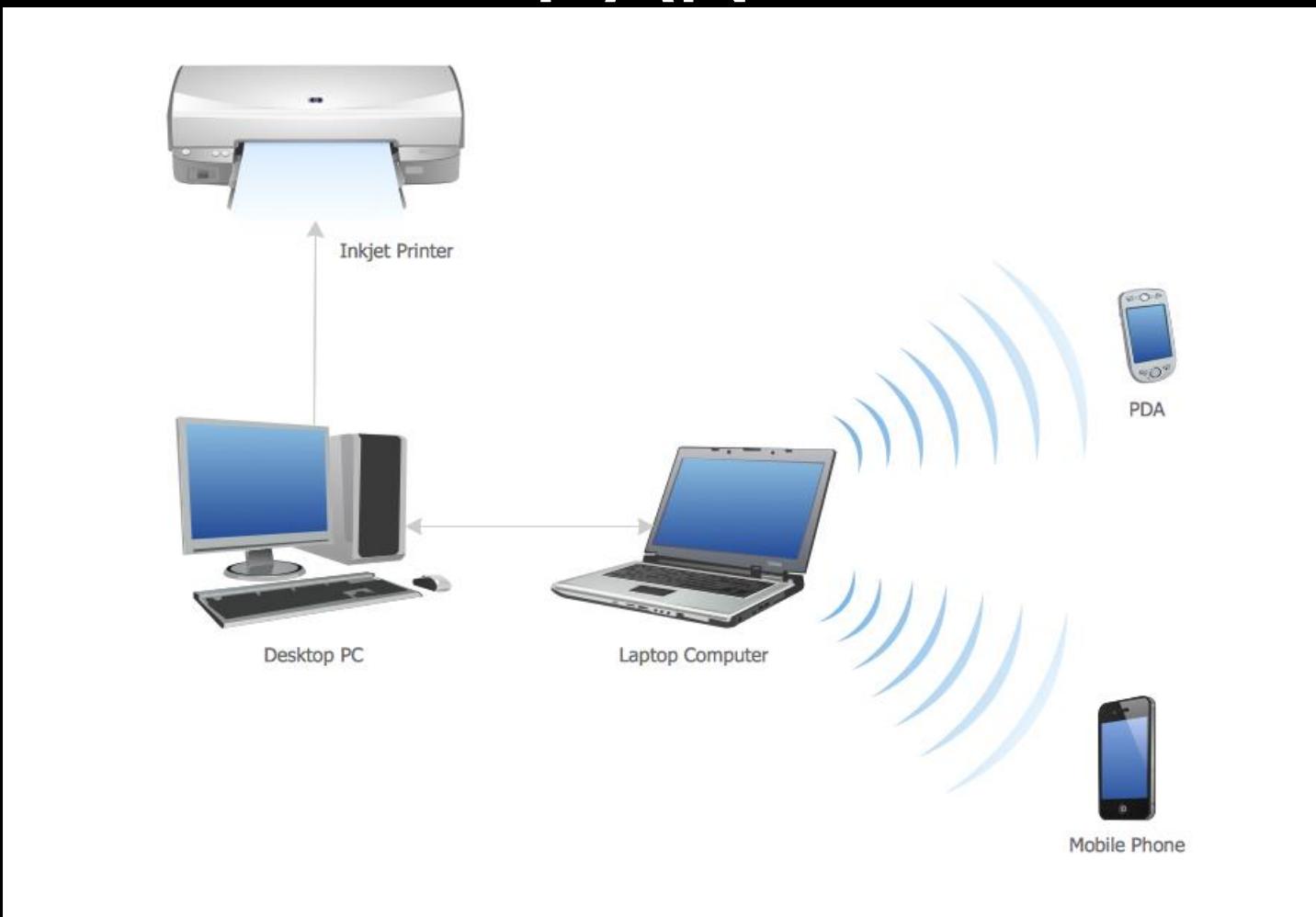
Local Area Network (LAN) - www.certiology.com

- Sieci lokalne dotyczą instalacji zlokalizowanych na stosunkowo niewielkim obszarze. Teoretyczna średnica sieci lokalnej może wynosić nawet kilkaset metrów, jednak po uwzględnieniu geometrii pomieszczeń obszar instalacji ogranicza się do jednego budynku lub jego części, np. piętra.
- W sieciach lokalnych stosuje się krótkie łącza (do ok.. 100m) o wysokiej przepustowości lub rozwiązania oparte na technice radiowej. Sieci lokalne charakteryzuje też wysoka niezawodność działania

MAN



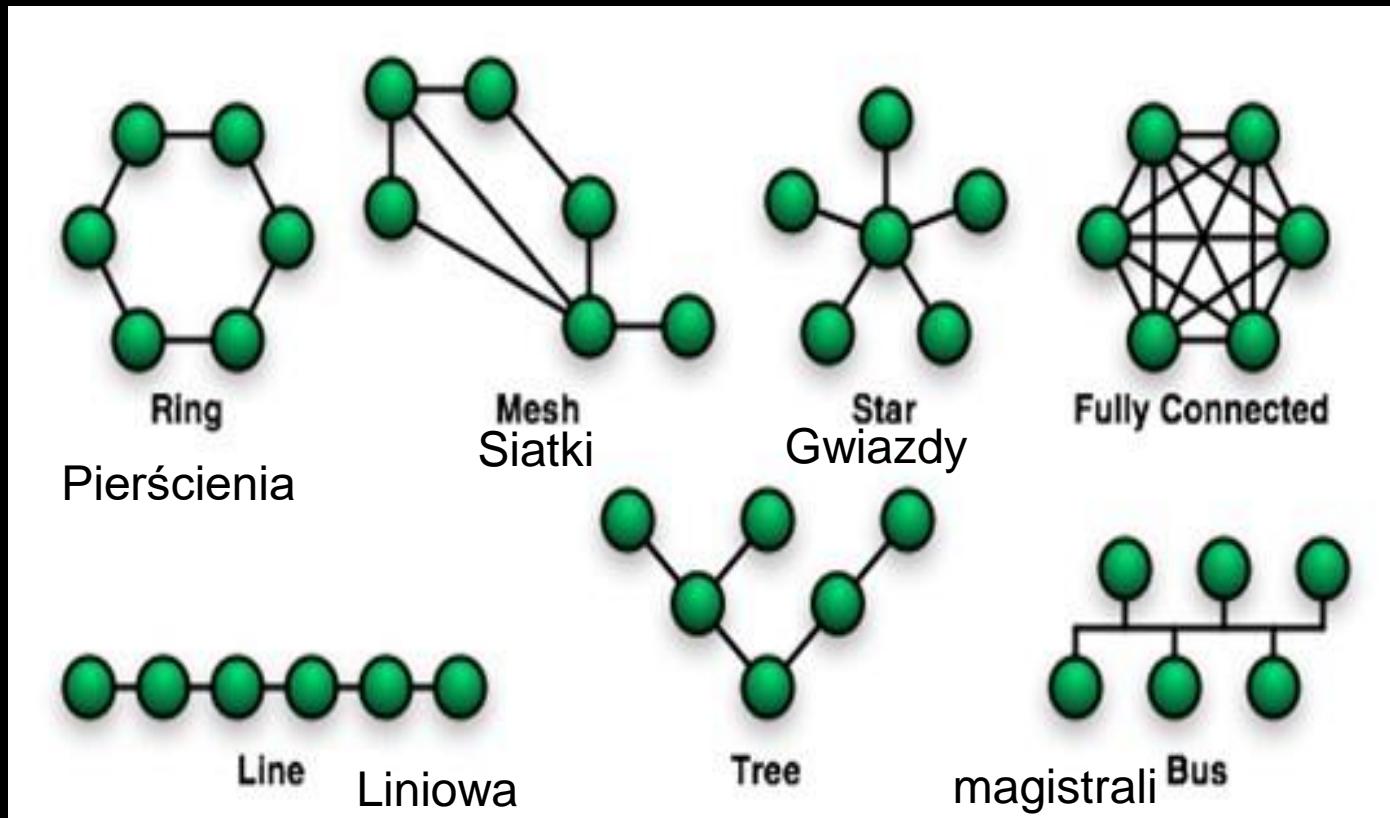
PAN



Topologie sieci

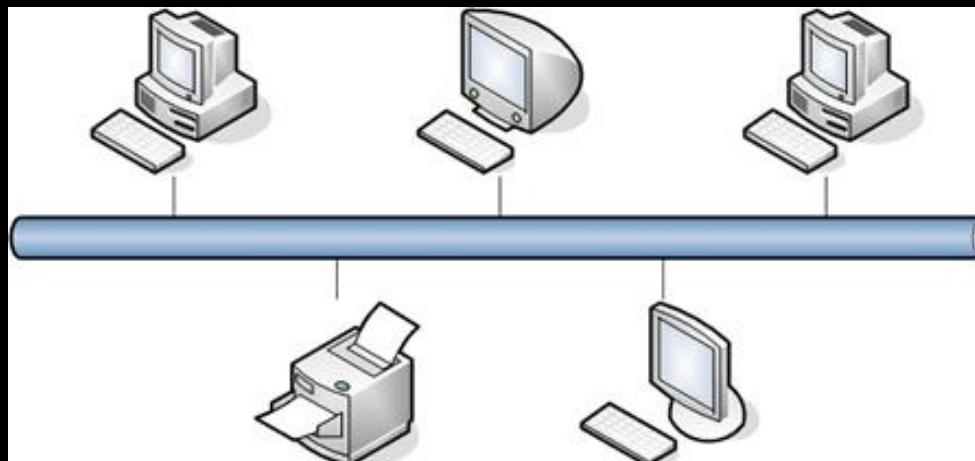
- Topologia jest to rozkład urządzeń i okablowania sieci.
 - Topologia fizyczna
 - Odwzorowanie węzłów w sieci oraz fizycznych połączeń między nimi
 - Topologia logiczna
 - Sposoby komunikowania się w sieci za pomocą urządzeń topologii fizycznej

Fizyczna topologia sieci



Topologia magistrali

- Historyczna





Topologia magistrali

- Typowy skład:
 - Kabel koncentryczny
 - Złącza
- Wampiry – vampire tap
- Złącza BNC w kształcie litery T (trójkąt)
 - Terminatory - oporniki



Topologia magistrali

- Stosowana była do budowy sieci lokalnych
- Komunikacja na wspólnej ścieżce
- Konieczność używania algorytmów Collision Detection -CD oraz Collision Avoidance -CA



Topologia magistrali

Zalety

Prosta instalacja

Niskie koszty

Wady

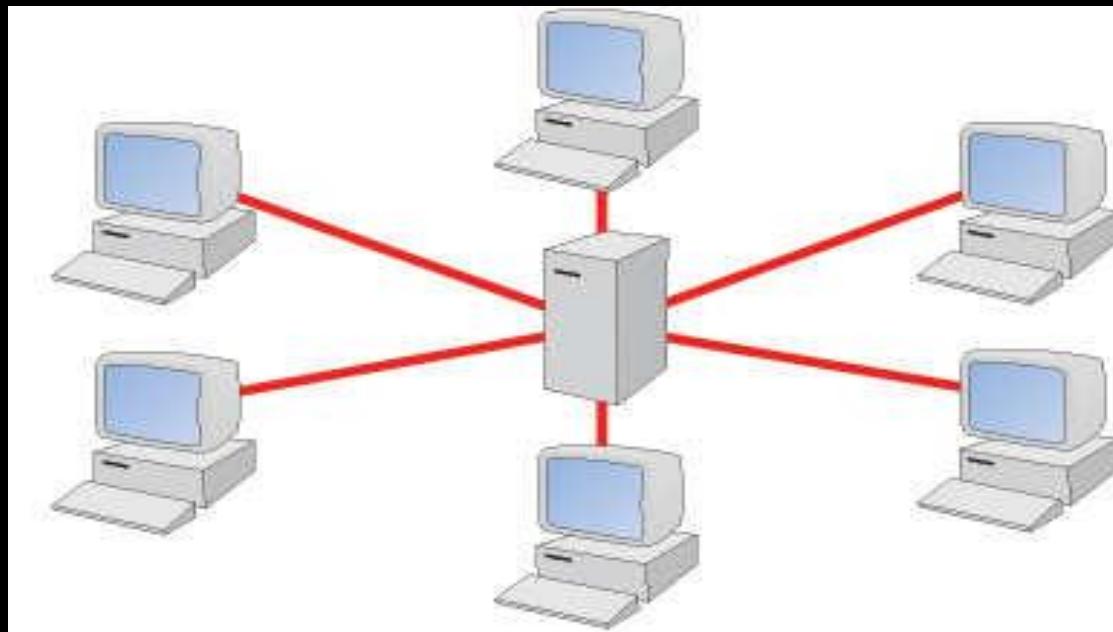
Terminatory na końcach sieci

Uszkodzenie kabla = globalna awaria

Ograniczona rozbudowa
Usterka ciężka do wykrycia

Obecnie właściwie nie stosowana

Topologia gwiazdy





Topologia gwiazdy

- Każdy węzeł sieci podłączony własnym kablem
- Jedno urządzenie „środkowe” - koncentrator lub przełącznik
 - Urządzenia te odpowiednio powielają lub przełączają ruch sieciowy.
- W sieciach lokalnych obecnie najpopularniejsze rozwiązanie.

Topologia gwiazdy

Zalety

Przejrzysta konstrukcja

Duża stabilność

Węzły mogą być dowolnie
przełączne

Przerwanie pojedynczego
kabla nie powoduje większej
awarii

Nie wymaga dodatkowych
urządzeń (np. terminatorów)

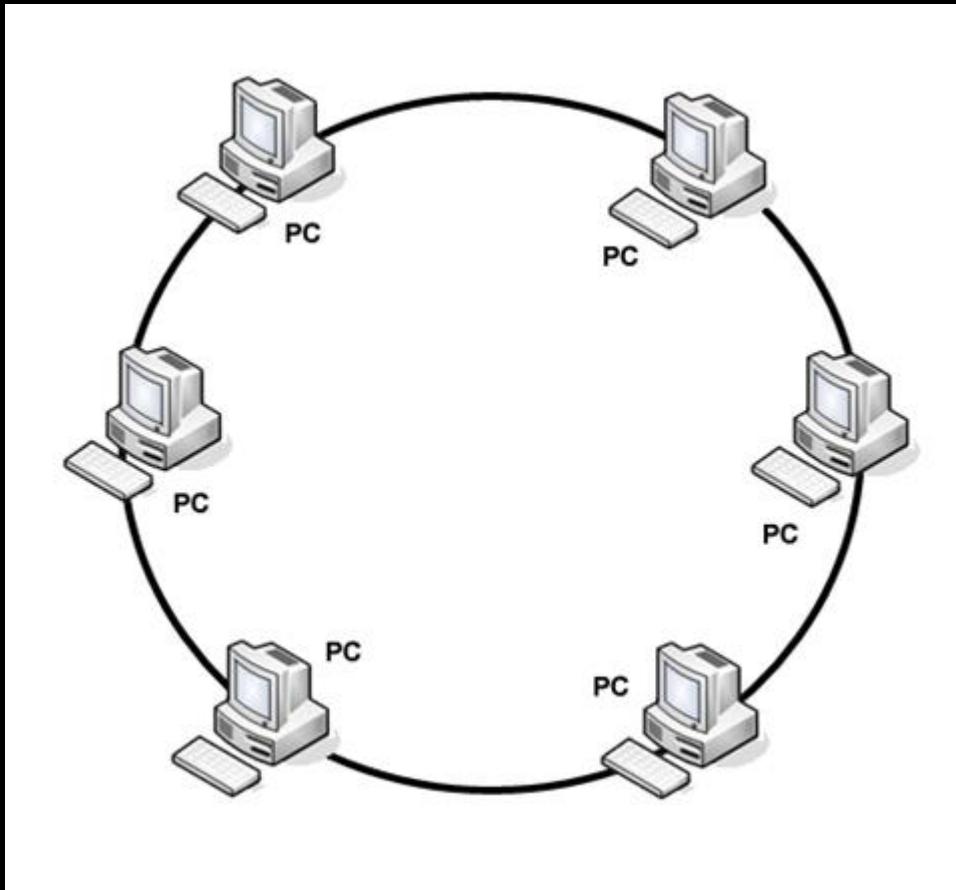
Wady

Awaria
koncentratora/przełącznika =
awaria całej sieci

Koszt urządzeń sieciowych

Duża ilość kabla

Topologia pierścienia





Topologia pierścienia

- Urządzenia podpięte bezpośrednio do siebie
- Każdy węzeł połączony z dwoma sąsiednimi
- Topologia logiczna – przekazywanie żetonu
- Żeton (token) jest sekwencją bitów zawierającą informację kontrolną.

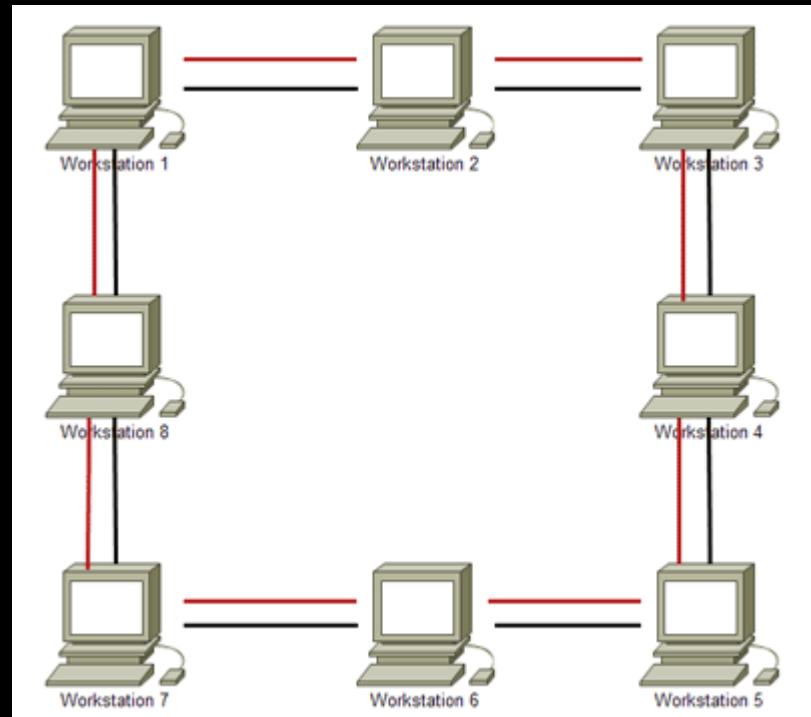
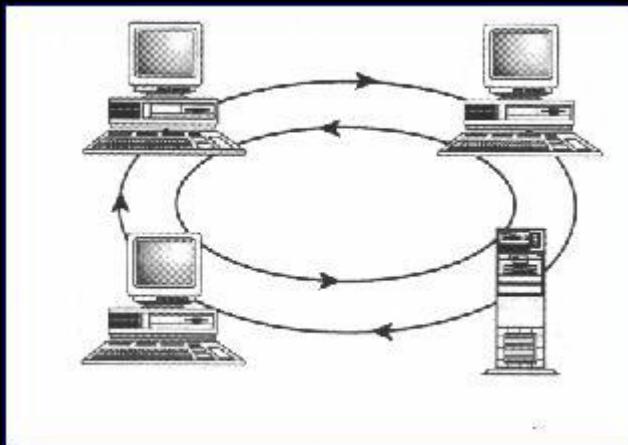
Topologia pierścienia – przekazywanie żetonu

- Tylko urządzenie posiadające żeton może rozpoczęć transmisję.
- Jeden żeton w całej sieci.
- Kolejne komputery przekazują dane dalej aż dotrą one do adresata. Adresat wysyła wiadomość zwrotną do nadawcy.
- Po weryfikacji nadawca generuje nowy żeton i wysyła go w sieć

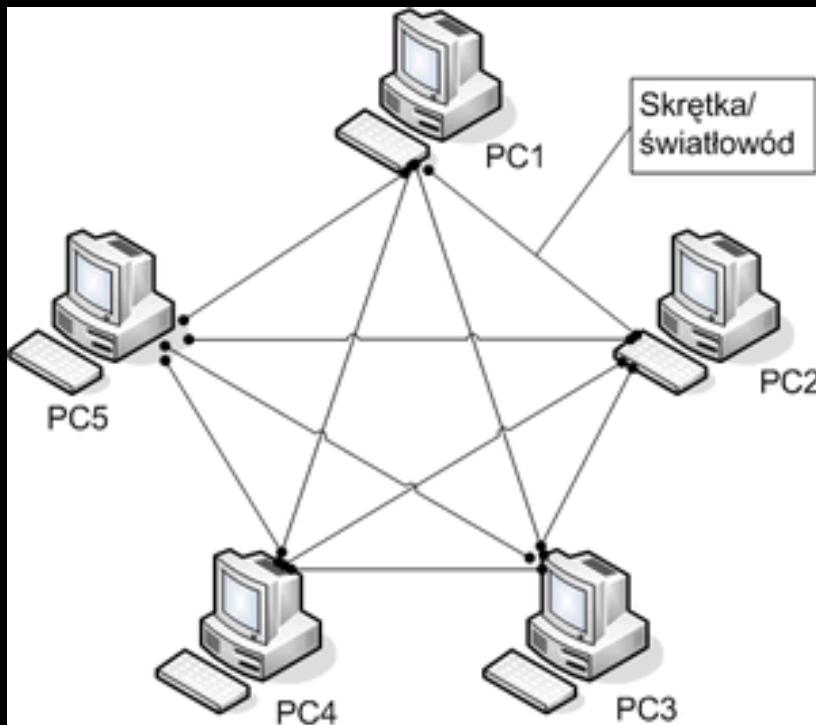


Topologia pierścienia

Topologia podwójnego pierścienia



Topologia siatki



- Dodatkowe redundantne połączenia pomiędzy węzłami
- Sieci metropolitalne i sieci rozległe



Topologia pełnej siatki

- Każdy host ma połączenie z pozostałymi hostami
- Niezawodna – istnieją zapasowe połączenia
- Duża liczba połączeń, skomplikowana rozbudowa.



Siatka częściowa

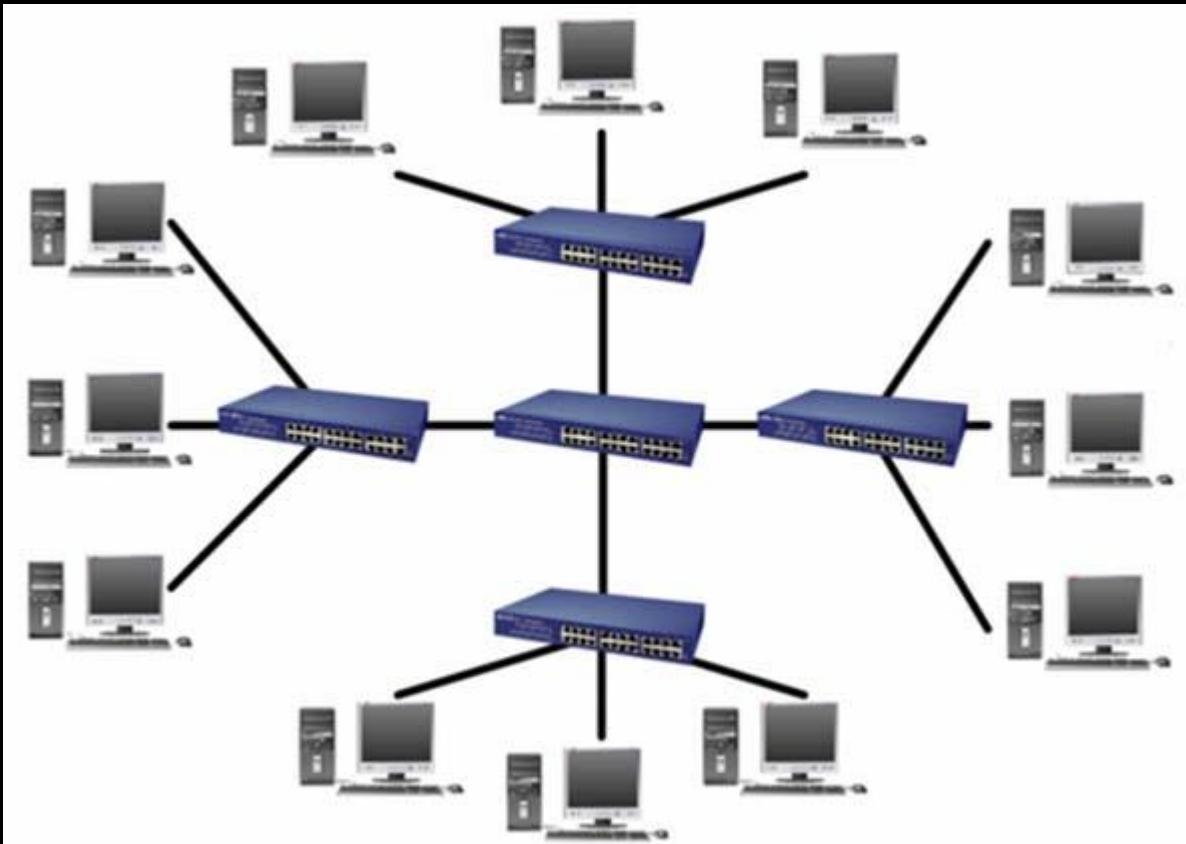
- Hosty połączone na wiele sposobów z innymi hostami (ale nie na każdy z każdym)
- Stosowana w internecie



Topologie mieszane

- Najczęściej spotykane w dużych sieciach.
- Tzw. hybrydy to dwie lub więcej topologii połączonych ze sobą.

Rozszerzona/rozgałęziona gwiazda

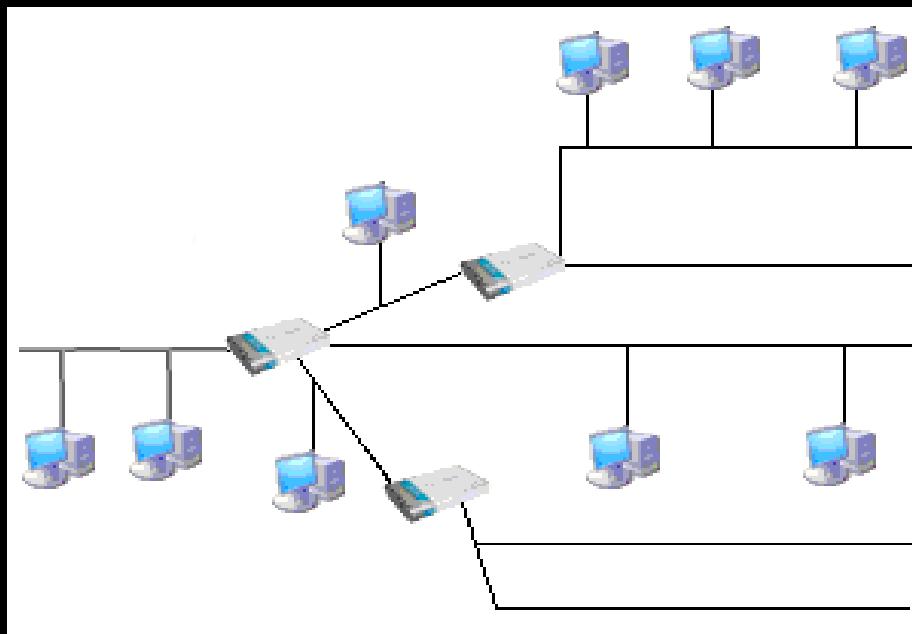




Rozszerzona gwiazda

- Kilka topologii gwiazdy połączonych w topologii gwiazdy
- Topologia hierarchiczna
- Może być skonfigurowana tak by ruch w sieci pozostawał lokalny

Topologia drzewa

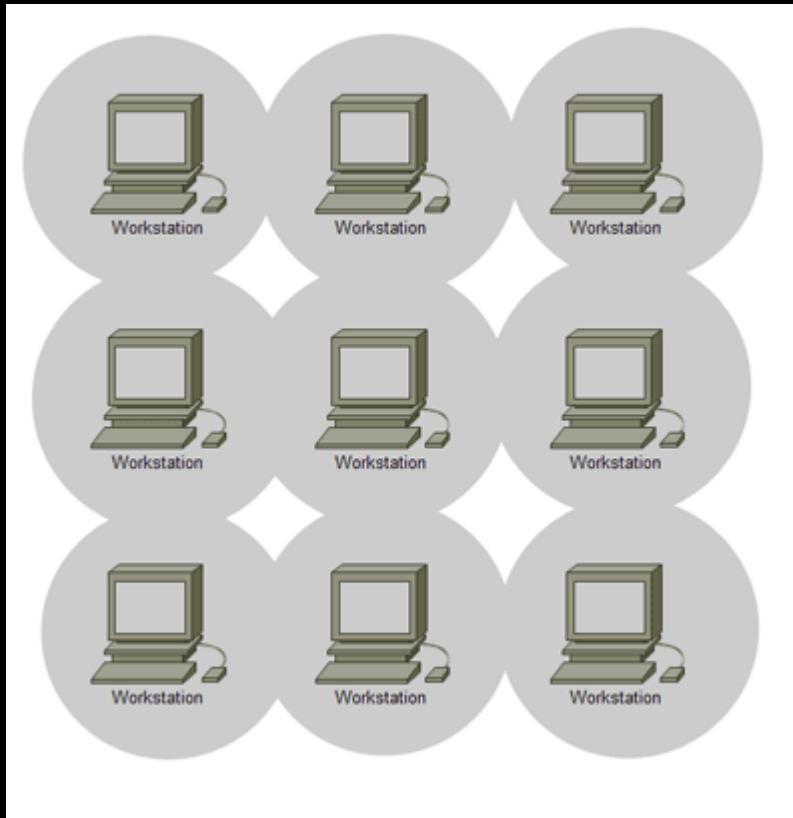


Topologia drzewa

- Wiele magistrali połączonych łańcuchowo
- Z węzła podstawowego rozchodzą się kolejne węzły
- Drzewo binarne:
 - Każdy węzeł ma 2 połączenia
- Drzewo szkieletowe:
 - Pień to przewód z kilkoma rozgałęzieniami.

Przepływ danych jest hierarchiczny

Topologia komórkowa (bezprzewodowa)





Topologie logiczne

- Topografię logiczną określa ścieżka jaką przebywają dane od węzła do węzła.
- Najczęściej wyróżniane na podstawie protokołu sieciowego:
 - Rozgłoszanie (broadcast) – host wysyła dane do wszystkich hostów podłączonych do medium – Ethernet
 - Przekazywanie tokenu – Token passing



A za tydzień?

- Urządzenia sieciowe
- Media sieciowe

Urządzenia i media sieciowe

dr Szymon Puławski

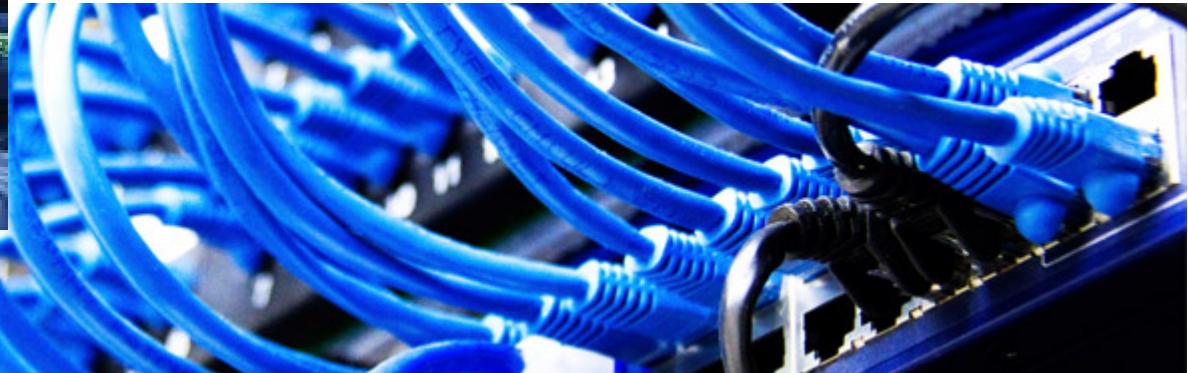
Urządzenia sieciowe

- Urządzenia sieciowe stanowią trzeci element fizycznej budowy sieci.



Urządzenia bierne

- Urządzenia bierne to kable oraz koncentratory.
- W budowie sieci komputerowych wykorzystywane są trzy rodzaje kabli: koncentryczny, skrętka, światłowód.



Huby bierne

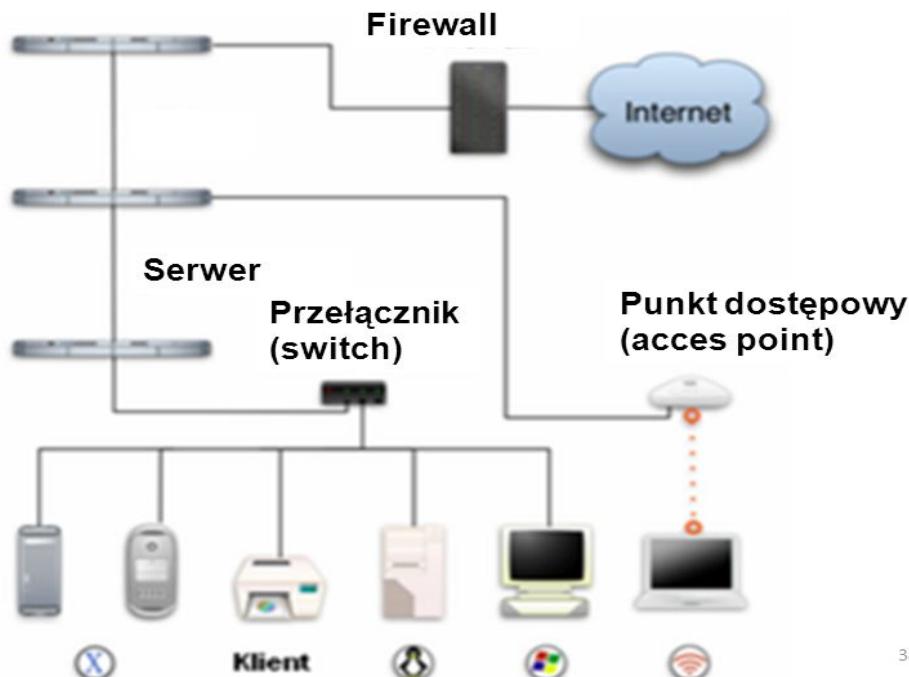
- Koncentratory (hub'y) bierne stosowane były głównie w sieciach zbudowanych w oparciu o kabel koncentryczny. Ze względu na duże ograniczenia związane z dopuszczalną długością połączeń koncentratory wykorzystywano w sieciach o niewielkich rozmiarach.



Urządzenia aktywne

- Podstawowym zadaniem urządzeń aktywnych jest regeneracja sygnału lub łączenie różnych rodzajów mediów (huby, konwertery, modemy)

Urządzenia aktywne



Model DSL



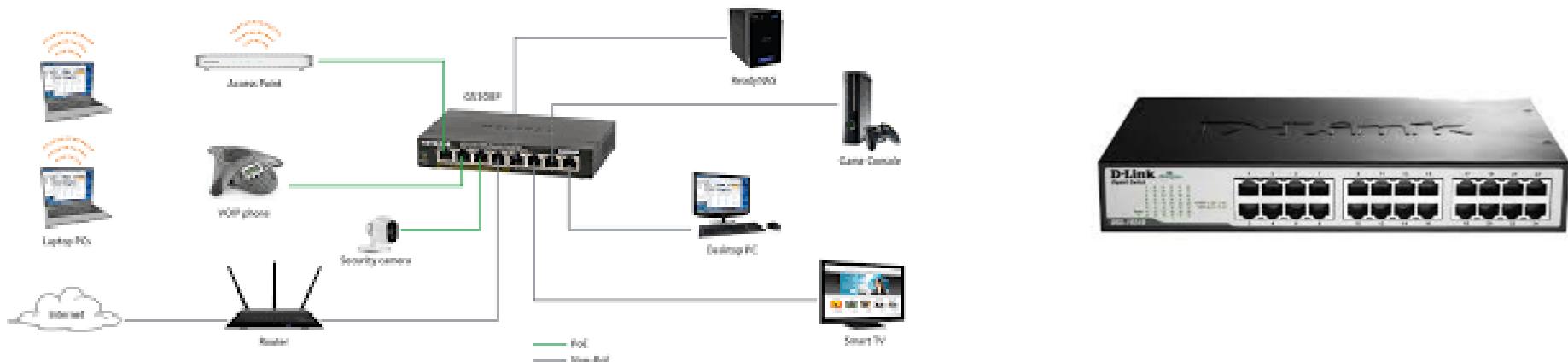
Koncentrator (hub)

- Hub otrzymane dane automatycznie rozsyła na wszystkie swoje porty

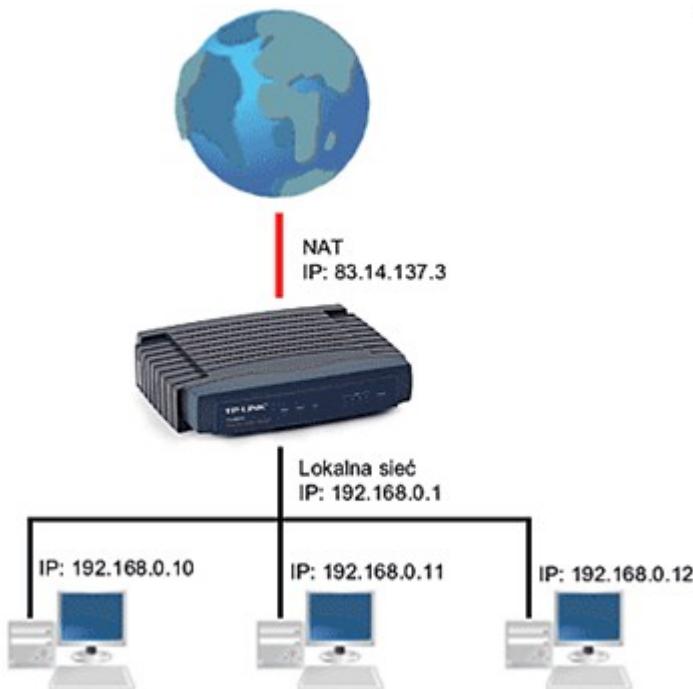


Przełącznik (switch)

- Switch potrafi rozpoznać do kogo adresowane są dane i przekierować je na właściwe złącze



Router



- Służy do łączenia różnych sieci (różne adresy).
- Węzeł komunikacyjny
- Kieruje ruchem (trasowanie, routing)

Punkt dostępowy (Acces point) sieci bezprzewodowych



Urządzenia końcowe



Copyright © StackMob, Inc. All rights reserved.

Karty sieciowe



Media sieciowe/transmisyjne

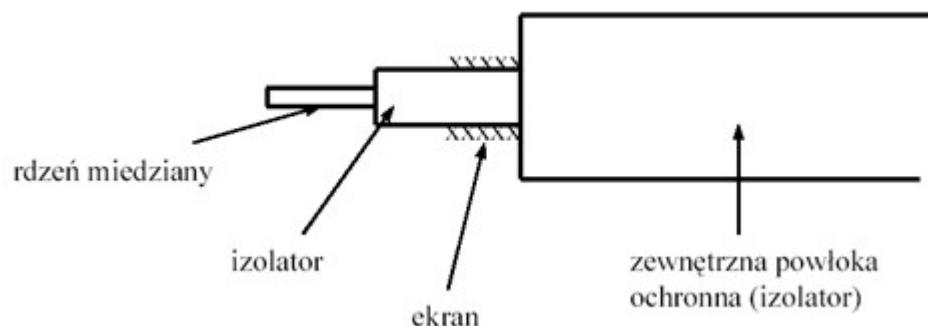
- Kable miedziane
- Media optyczne
- Radiowy kanał łączności
- Kanał satelitarny

Kabel miedziany

- Małe odległości.
- 3 rodzaje:
 - Prosty (historyczne)
 - Koncentryczne
 - skrętka

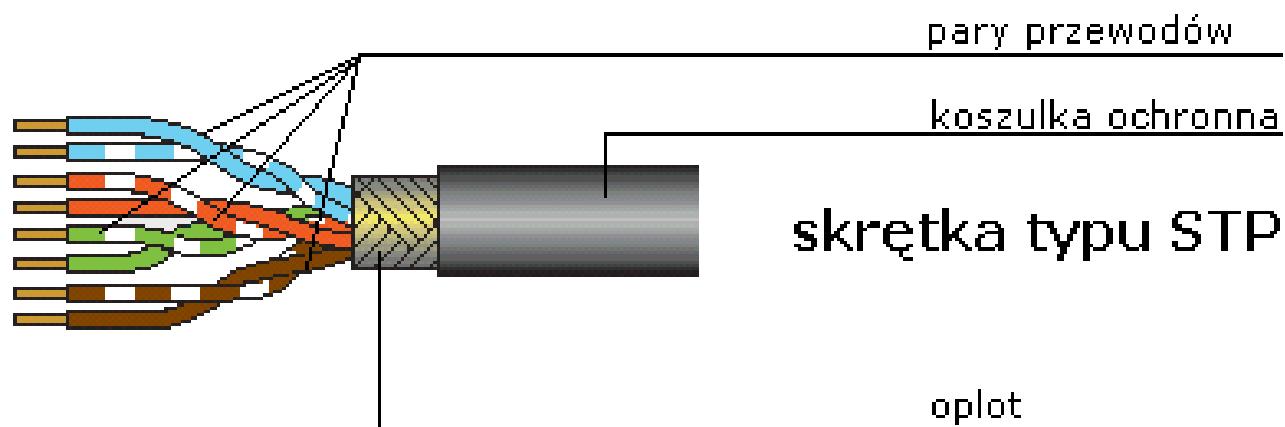
Kabel koncentryczny

- Ekranowany w celu odizolowania od zewnętrznych pól elektromagnetycznych – cienka siatka miedziana
- Odporny na zakłócenia
- Łatwo ulega uszkodzeniom
- Umożliwia podsłuch



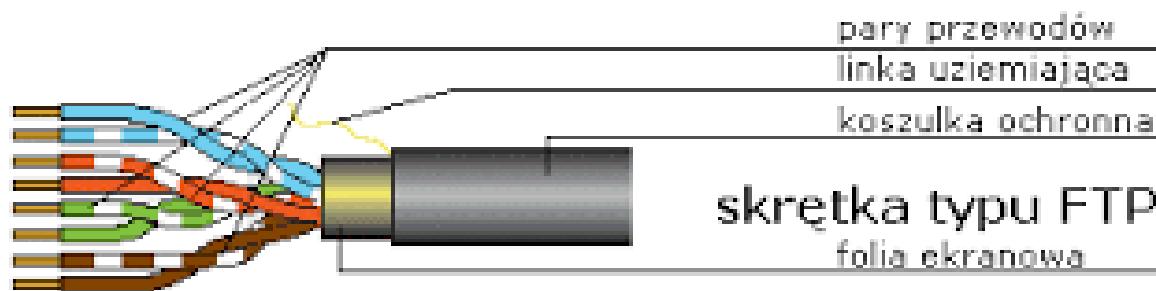
Skrętka ekranowana

- STP (ang. Shielded Twisted Pair) – skrętka ekranowana – klasyczne miedziane medium transportowe sieci komputerowej, wykonane z dwóch skręconych przewodów wraz z ekranem w postaci oplotu. Para ekranowana jest bardziej odporna na zakłócenia impulsowe oraz szkodliwe przesłuchy niż skrętka UTP.



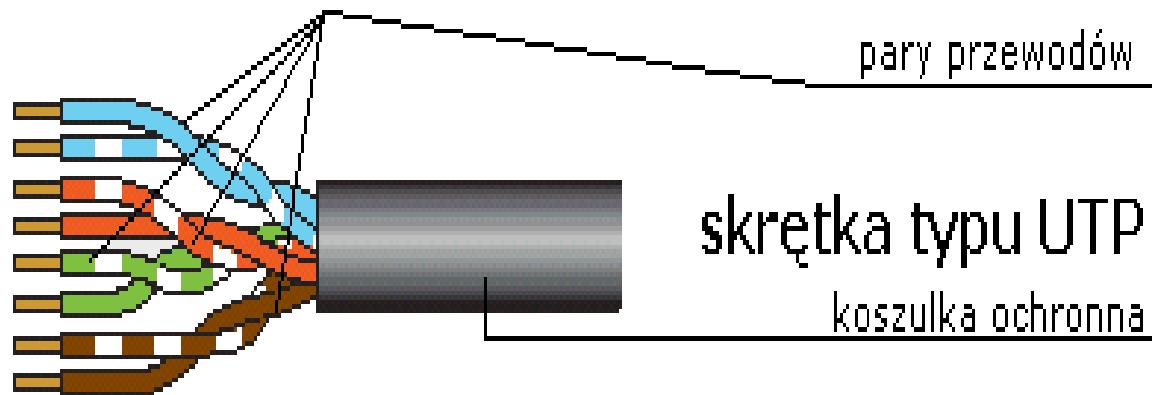
Skrętka foliowana

- FTP (ang. Foiled Twisted Pair) – skrętka foliowana – skrętka miedziana ekranowana za pomocą folii wraz z przewodem uziemiającym. Przeznaczona jest głównie do budowy sieci komputerowych (Ethernet, Token Ring) o długości nawet kilku kilometrów. Stosowana ostatnio również na krótszych dystansach w sieciach standardu Gigabit Ethernet (1 Gb/s) z wykorzystaniem wszystkich czterech par okablowania miedzianego kat. 5.



Skrętka nieekranowana

- UTP (ang. Unshielded Twisted Pair) – skrętka nieekranowana – skrętka wykonana z dwóch przewodów, ze zmiennym splotem (zwykle 1 zwój na 6-10 cm), co chroni transmisję przed oddziaływaniem otoczenia. Skrętka nieekranowana UTP jest powszechnie stosowana w sieciach telefonicznych (jedna, dwie lub cztery pary) i w kablach komputerowych (cztery skrętki w kablu).



Skrętka więcej typów

- F-FTP – każda para przewodów otoczona jest osobnym ekranem z folii, cały kabel jest również pokryty folią,
- S-FTP – każda para przewodów otoczona jest osobnym ekranem z folii, cały kabel pokryty jest opłotem,
- S-STP – każda para przewodów otoczona jest osobnym ekranem (opłotem), cały kabel pokryty jest opłotem.

•Kategorie kabli miedzianych

Kategorie kabli miedzianych zostały ujęte w specyfikacji EIA/TIA w kilka grup:

- kategoria 1 – tradycyjna nieekranowana skrętka telefoniczna przeznaczona do przesyłania głosu, nie przystosowana do transmisji danych
- kategoria 2 – nieekranowana skrętka, szybkość transmisji do 4 MHz. Kabel ma 2 pary skręconych przewodów
- kategoria 3 – skrętka o szybkości transmisji do 10 MHz, stos. w sieciach Token Ring (4 Mb/s) oraz Ethernet 10Base-T (10 Mb/s). Kabel zawiera 4 pary skręconych przewodów
- kategoria 4 – skrętka działająca z szybkością do 16 MHz. Kabel zbudowany jest z czterech par przewodów
- kategoria 5 – skrętka z dopasowaniem rezystancyjnym pozwalająca na transmisję danych z szybkością 100 MHz pod warunkiem poprawnej instalacji kabla (zgodnie z wymaganiami okablowania strukturalnego) na odległość do 100 m
- kategoria 5e – (enhanced) – ulepszona wersja kabla kategorii 5. Jest zalecana do stosowania w przypadku nowych instalacji

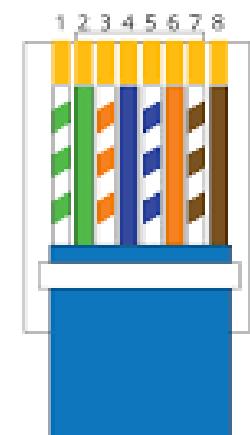
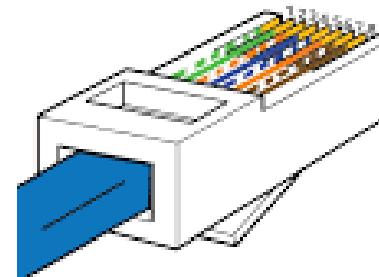
Kategorie kabli miedzianych cd

- kategoria 6 – skrętka umożliwiająca transmisję z częstotliwością do 200 MHz. Kategoria ta obecnie nie jest jeszcze zatwierdzona jako standard, ale prace w tym kierunku trwają
- kategoria 7 – kabel o przepływności do 600 MHz. Będzie wymagać już stosowania nowego typu złączy w miejsce RJ-45 oraz kabli każdą parą ekranowaną oddzielnie. Obecnie nie istnieje.

Wtyczki RJ-45

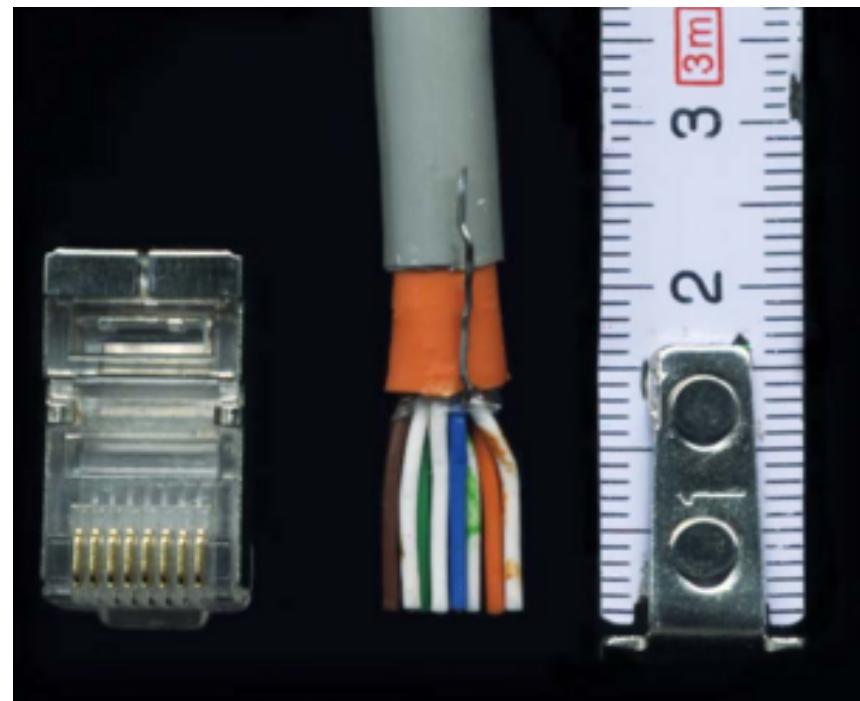


**RJ45 Pinout
T-568A**



- | | |
|-----------------|----------------|
| 1. White Green | 5. White Blue |
| 2. Green | 6. Orange |
| 3. White Orange | 7. White Brown |
| 4. Blue | 8. Brown |

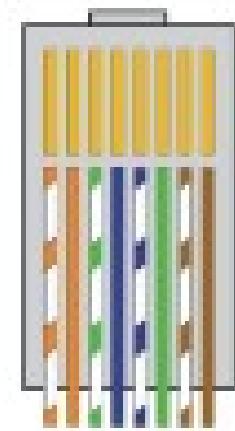
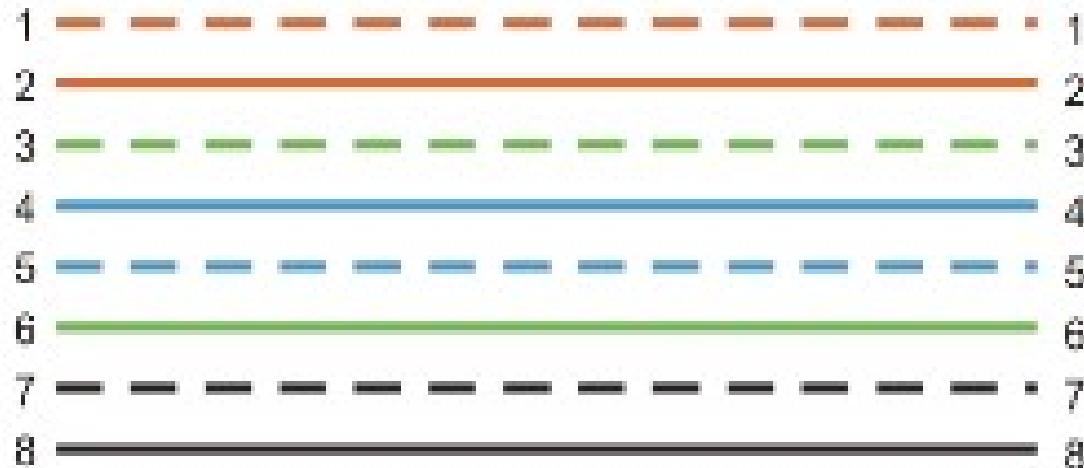
RJ-45 technicznie



Typy przyłączy przewodów

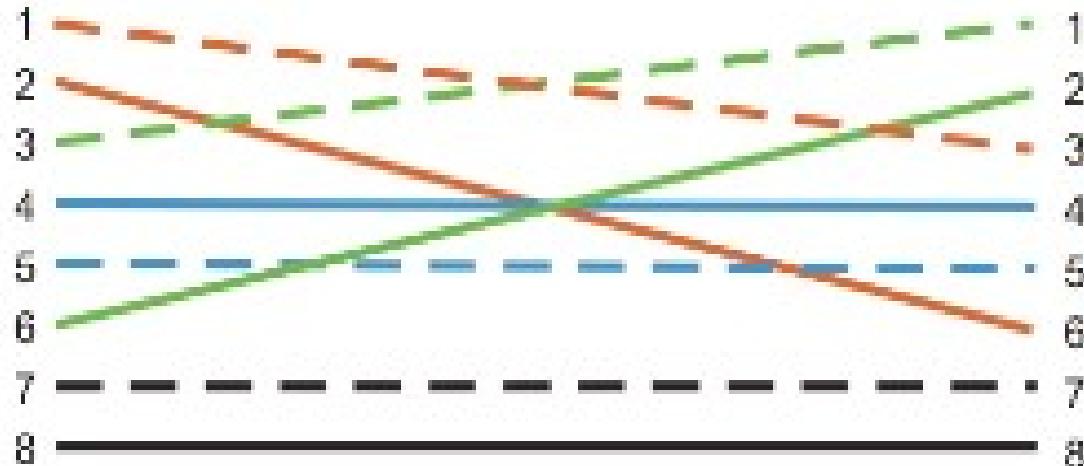
- W sieciach 10Base-T i 100Base-TX stosuje się dwa typy podłączeń końcówek RJ-45:
 - Zgodne (proste) - wszystkie żyły wewnątrz przewodu podłączamy do wtyków w następujący sposób: styk pierwszy we wtyczce pierwszej do styku pierwszego we wtyczce drugiej, 2 do 2, 3 do 3, itd.
 - Krzyżowe - w tym połączeniu dwie pary wewnętrznych przewodów są zamienione ze sobą (1-3, 2-6). Tak powstały kabel nazywa się cross-over.

Połączenie zgodne



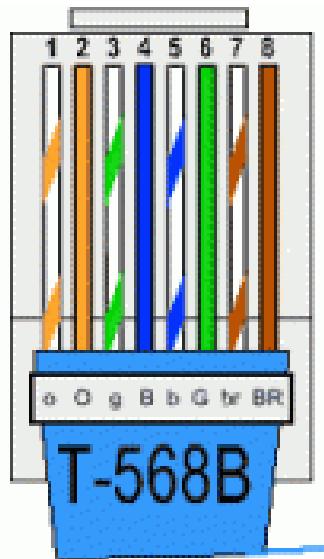
g b w r . p l

Połączenie krzyżowe



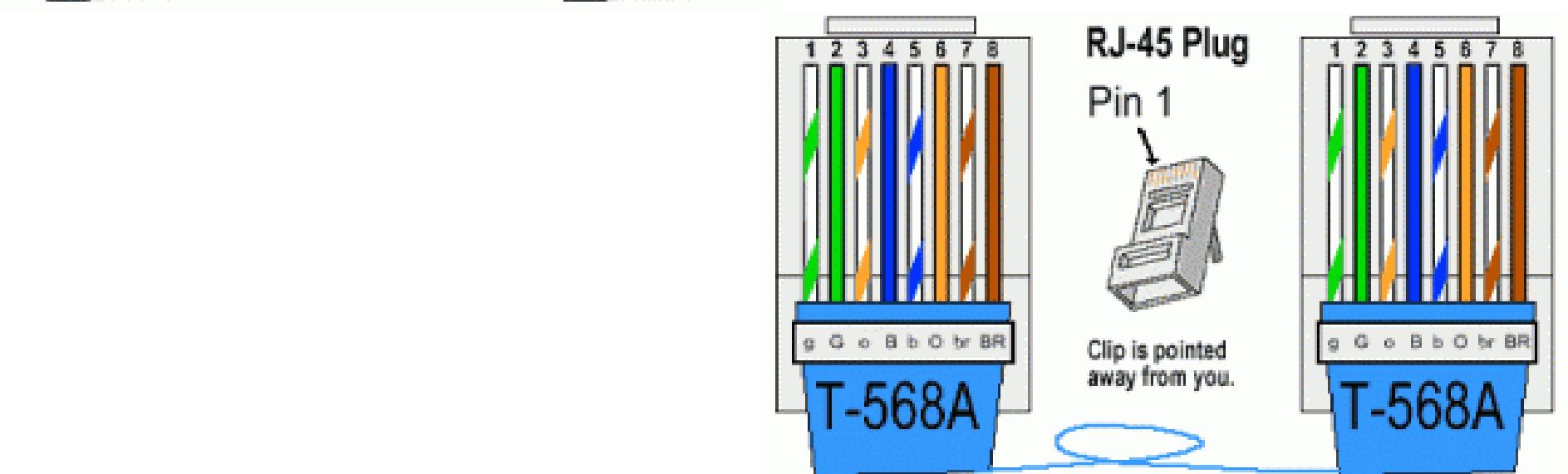
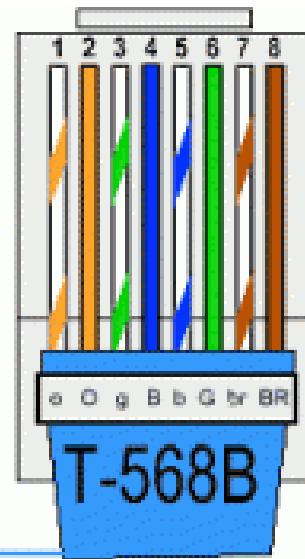
g b w r . p l

Układ prosty - standardy



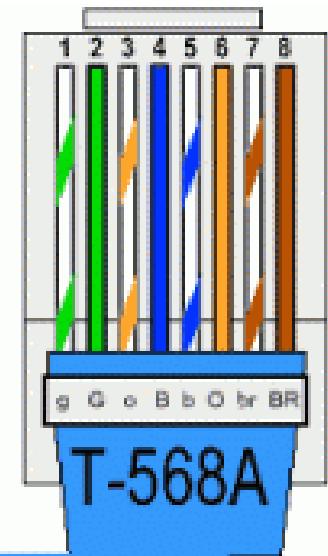
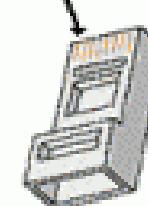
RJ-45 Plug

Pin 1

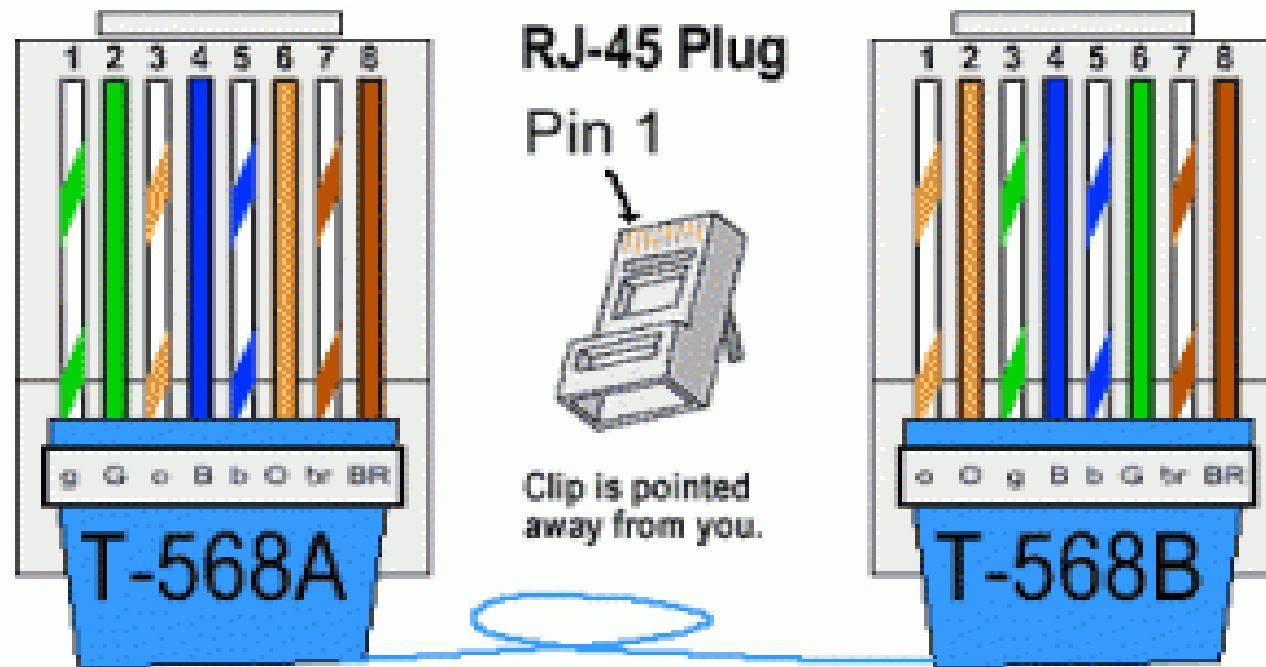


RJ-45 Plug

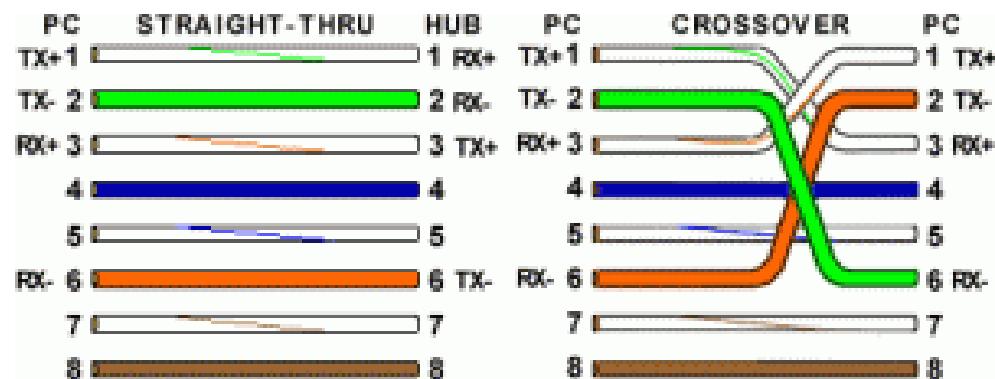
Pin 1



Układ krosowany - standard

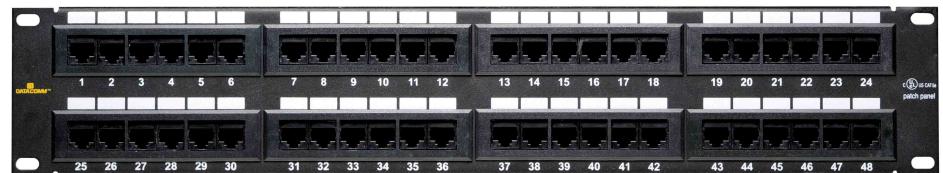
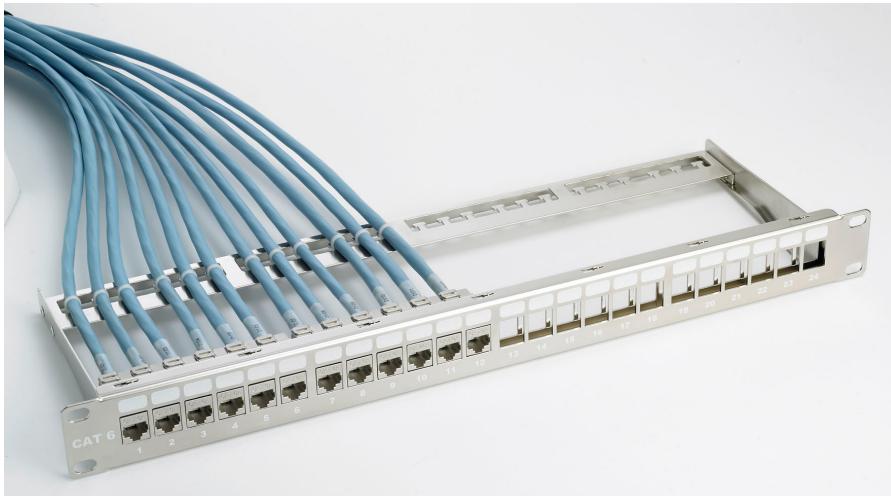


Która para do czego?



Panel krosowniczy

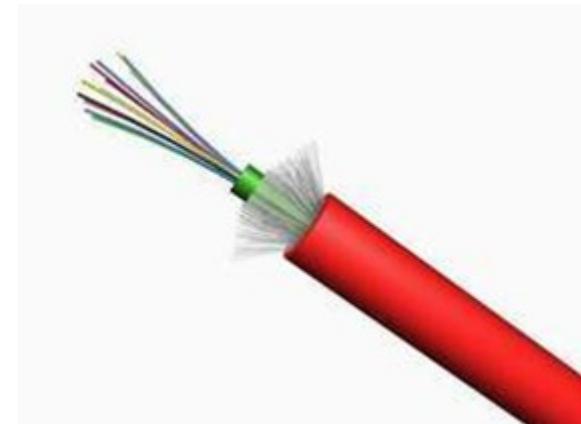
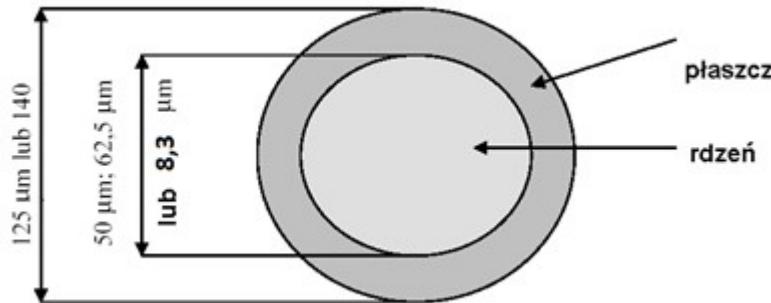
- Panel krosowniczy - (ang. patch panel) to pasywny element sieci komputerowych i telekomunikacyjnych. Montowany jest w szafach krosowniczych. Z jednej strony przyłączane są przewody prowadzące do gniazdek RJ-45.
- Przy pomocy tzw. patch cordów gniazda te (a i przez to urządzenia będące na drugim końcu kabla) przyłączane są do urządzeń sieciowych.



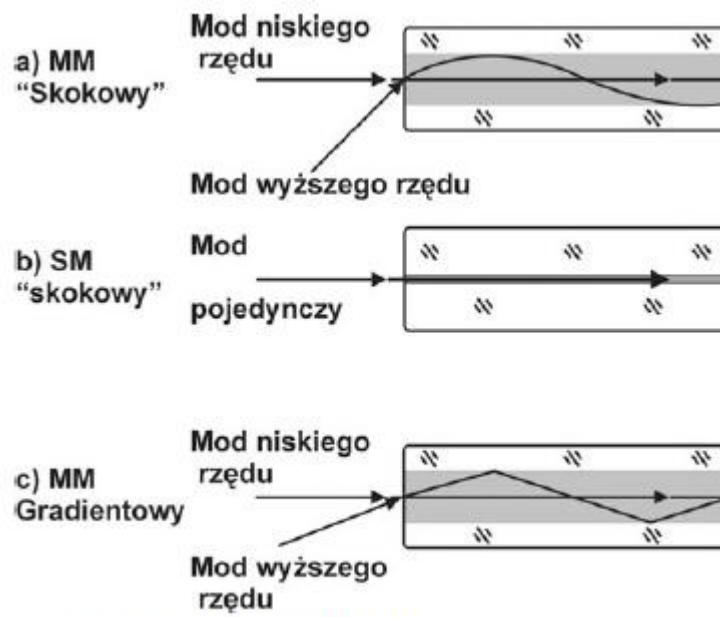
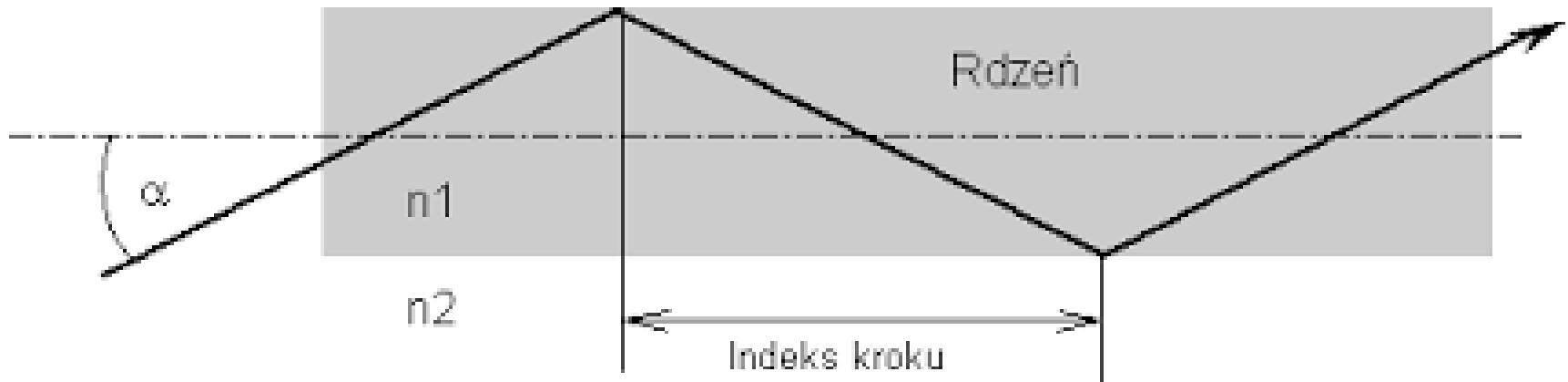
Światłowody

- Transmisja na odległości powyżej 100 m.
- Zbudowane ze szkła kwarocwego o dużej czystości
 - Budowa:
 - Rdzeń
 - Płaszcz
 - Dodatkowo zabezpieczenie z tworzywa sztucznego

Światłowody



Światłowody zasada działania



Rys. 2. Rodzaje światłowodów.

Cechy światłowodu

- Duża szerokość pasma częstotliwości – do 2×10^{14} Hz
- Mała strata mocy spowodowana rozpraszaniem – ok 0,2 dB/km
- Przesył 200 000 km/s
- Odporność na interferencje elektromagnetyczne
- Niska waga, wymiary, dobra giętkość i wytrzymałość

nanometr

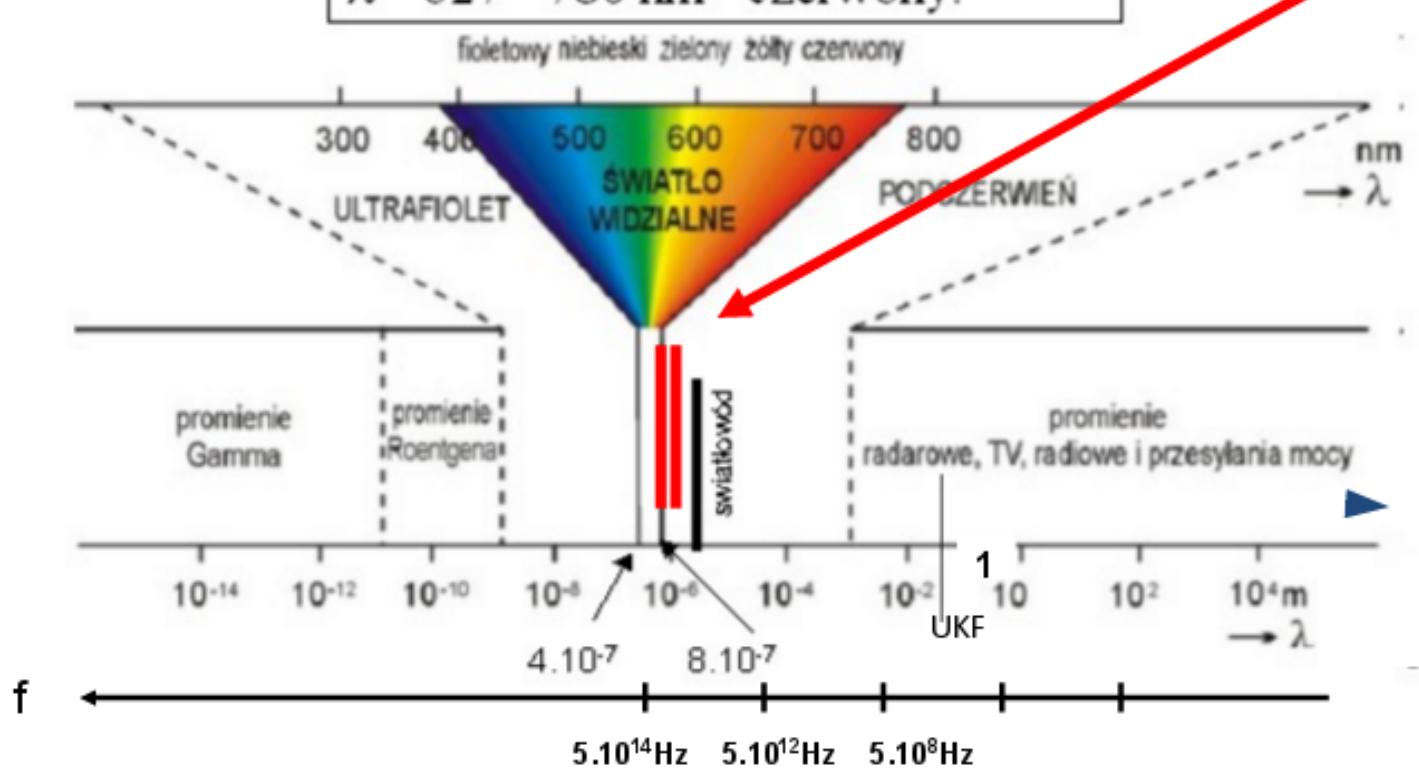
$$1 \text{ nm} = 10^{-9} \text{ m}$$

mikrometr

$$1 \mu\text{m} = 10^{-6} \text{ m}$$

$\lambda = 380 - 436 \text{ nm}$ fiolet,
 $\lambda = 436 - 495 \text{ nm}$ niebieski,
 $\lambda = 495 - 566 \text{ nm}$ zielony,
 $\lambda = 566 - 589 \text{ nm}$ żółty (żółty),
 $\lambda = 589 - 627 \text{ nm}$ pomarańczowy,
 $\lambda = 627 - 780 \text{ nm}$ czerwony.

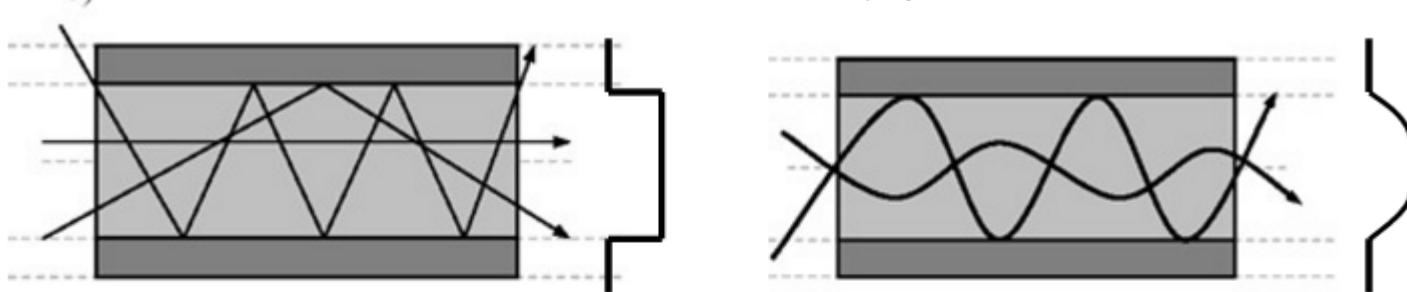
$$f = v/\lambda$$



Wady i zalety

- Zalety:
 - Brak pola elektromagnetycznego – niemożliwe podsłuchanie transmisji
- Wady:
 - Dyspersja – rozmycie impulsu ograniczające częstotliwość sygnału

Wielomodowe – 50 lub 62,5 μm



światłowód **skokowy** - współczynnik załamania światła inny dla rdzenia i płaszcza (duża dyspersja więc niewielkie odległości)

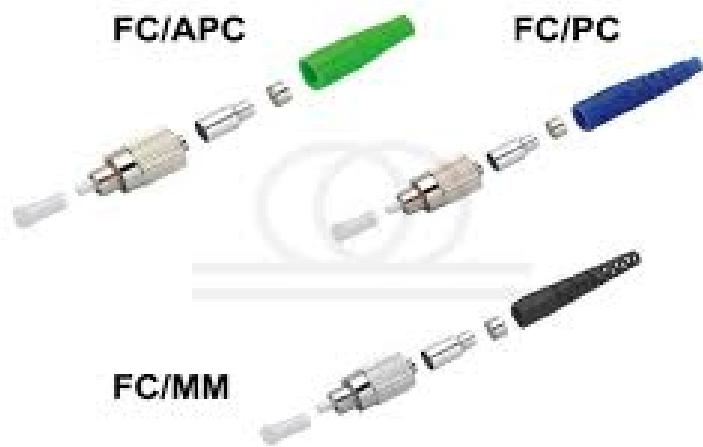
światłowód **gradientowy** – gęstość kwarcu zmienna płynnie, mniejsza droga promienia to mniejsza dyspersja (do 2 km)

Jednomodowe – ~8-10 μm



telekomunikacja – tanie ale światło spójne (laser jest drogi) – duże odległości – do 120 km!!!

Gniazda (końcówki) światłowodowe



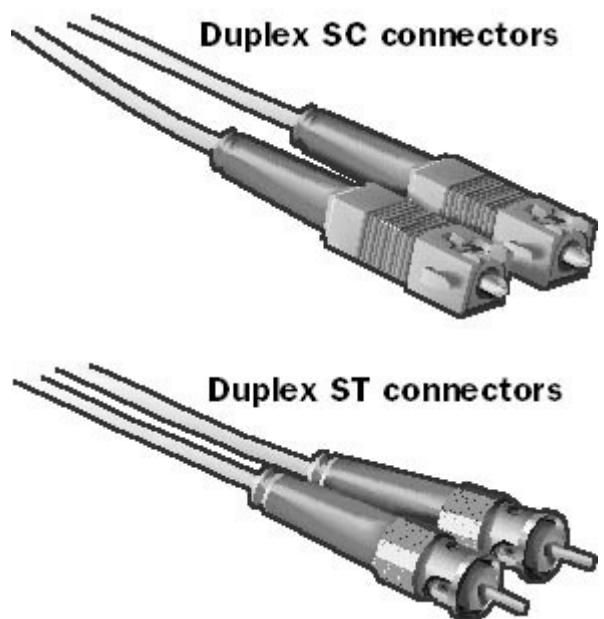
- Złącza FC zostały specjalnie zaprojektowane z myślą o aplikacjach telekomunikacyjnych wymagających stałego i pewnego połączenia. Skręcone, gwintowane zakończenie zapewnia niezawodność połączeń nawet w przypadku częstych przełączeń. Zastosowana w złączu ferrula typu PC (z kontaktem fizycznym bez przerwy powietrznej) zmniejsza odbicie wsteczne. Ferrule wykonywane są z dwutlenku cyrkonu lub stopów nierdzewnej stali. Właściwości: Gwintowany sposób mocowania zwiększający bezpieczeństwo połączenia. Zastosowanie klucza przeciwdziałającego niepożądanym obrotom ferruli wewnątrz wtyku. Dostępne w wersji wielomodowej i jednomodowej.

ST

- W złączu ST umieszczono bagnetowy zatrzask obrotowy z ferrulą o średnicy 2,5mm. Złącza dostępne są w wersji jedno i wielomodowej. Zapewniają one solidność i trwałość wykonanych połączeń. Kształt konektora ST umożliwia trwałe i pewne mocowanie kabla wraz z kevlarem zapobiegając jego wysuwaniu się ze złącza.
- Właściwości: Prosty i szybki sposób mocowania złącza światłowodowego Zgodność wtyku z gniazdem typu Bayonet wyposażonym w metalową sprężynę Dostępne w wersji wielomodowej i jednomodowej



- Jest to jedno z najpopularniejszych typów połączeń światłowodowych. SC jest złączem zatrzaskowym z ferrulą samocentrującą wykonaną z dwutlenku cyrkonu o średnicy 2,5mm. Złącza te są wykonywane w wersjach pojedyńczej (simplex) i podwójnej (duplex). Jego kształt umożliwia łączenie tzw. „push-pull”, dzięki czemu zapewnia szybki i stosunkowo łatwy montaż w przełącznicach. Do połączeń dwóch tego typu złącz stosuje się plastikowe łączniki. Konstrukcja złącza minimalizuje odbicie wsteczne. Zalecane dla łączów jednomodowych w sieciach telekomunikacyjnych. Właściwości: Niska waga wtyku SC, wygoda i pewność połączenia łączów światłowodowych dzięki zastosowaniu mechanizmu zatrzaskowego, wymiary otworów w panelu identyczne jak dla standardu E2000, adaptery światłowodowe montowane w panelach na dwóch śrubach lub na zatrzask, dostępne w wersji wielomodowej i jednomodowej.



SC mini (MU)

- Właściwości: Wygoda i pewność połączenia złączy światłowodowych dzięki zastosowaniu mechanizmu zatrzaskowego, małe wymiary złącza światłowodowego pozwalające na uzyskanie dużej gęstości upakowania, koncepcja oparta na ferruli 1,25mm, dostępne w wersji wielomodowej i jednomodowej.
- Zastosowany w tego typu złączach system blokady zatrzaskowej zabezpiecza połączenie przed przypadkowym wyciągnięciem końcówki. Jego zaletą są niewielkie wymiary co umożliwia zastosowanie go w miejscach dużego zagęszczenia pól przełączeniowych. Złącza te występują w wersjach „simplex” i „duplex”, zaopatrzone w ceramiczną ferrulę o średnicy 1,25mm.
- Właściwości: Wygoda i pewność połączenia złączy światłowodowych dzięki zastosowaniu mechanizmu zatrzaskowego, małe wymiary złącza światłowodowego pozwalające na uzyskanie dużej gęstości upakowania, koncepcja oparta na ferruli 1,25mm, dostępne w wersji wielomodowej i jednomodowej.

MU

- Konstrukcja typu MU łączy cechy złącza SC i LC. Zapewnia wysoką jakość połączeń a zarazem można stosować je w miejscach dużego zagęszczenia pól przełączeniowych.



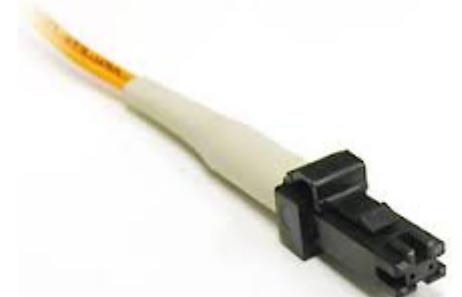
MTP/MPO

„USconec MTP” są złączami zgodnymi z MPO. Umożliwiają łatwe i pewne połączenie jednocześnie do 12-tu włókien. Występują w wersji jedno i wielomodowej. Dostępne są również złącza w wersjach do 4 i do 8 włókien.



MTRJ

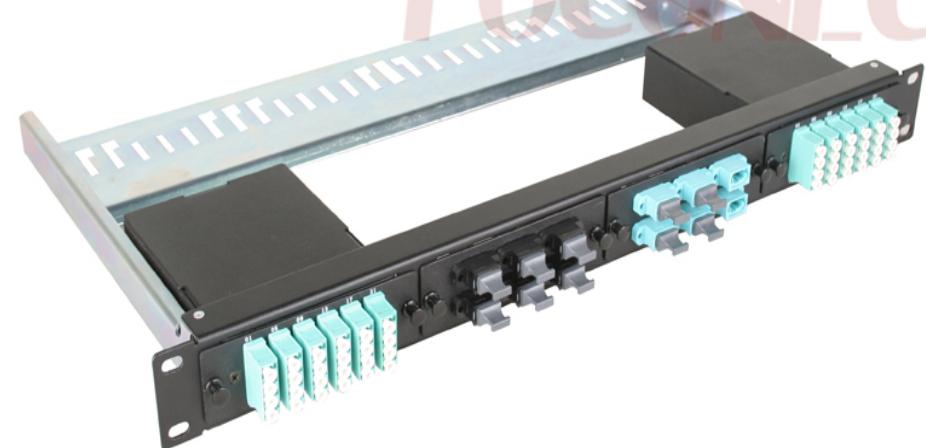
- Złącze MTRJ dzięki swej konstrukcji zapewnia podwójnie zagęszczenie portów w porównaniu ze złączami typu SC. W pojedyńczej, plastikowej ferruli znajdują się dwa włókna oraz mechanizm zatrzaskowy typu RJ-45.
- Właściwości: Dwukrotnie większą gęstość upakowania w stosunku do dupleksowych złączy światłowodowych SC, wymiary otworów w panelu identyczne jak dla standardu SC, posiadają zatrzaskowy mechanizm łączenia, typowo występują w konfiguracji gniazdowyk, przy czym istnieje również możliwość ich łączenia przy pomocy adapterów, analogicznie do złączy światłowodowych innych rodzajów, koncepcja oparta na ferruli MT (ang. Mass Termination). Dostępny w wersji wielomodowej i jednomodowej



Urządzenia sieciowe światłowodowe



FOCONEC



Model ISO-OSI

- Wielość rozwiązań stosowanych w budowie pierwszych sieci komputerowych w sposób istotny utrudniała wzajemną komunikację pomiędzy sieciami działającymi na podstawie różnych specyfikacji. Fakt ten był bezpośrednią przyczyną podjęcia działań w kierunku standaryzacji rozwiązań.
- W wyniku analizy modeli sieciowych, takich jak DECnet (ang. Digital Equipment Corporation net), SNA (ang. Systems Network Architecture) i TCP/IP, organizacja ISO (ang. International Organization for Standardization) opracowała zbiór zasad umożliwiający budowę wzajemnie zgodnych sieci, który został opublikowany w 1984 roku jako model odniesienia OSI (ang. Open System Interconnection). Obecnie, ze względu na ujednolicenie stosowanych technologii zawarte w modelu zasady zdezaktualizowały się ale sam model odniesienia stał się głównym modelem komunikacji sieciowej stosowanym podczas projektowania, wdrażania i użytkowania sieci komputerowych, a przede wszystkim w procesie szkolenia

Model ISO-OSI

- Model odniesienia ISO/OSI przedstawia proces komunikacji w postaci siedmiu warstw.
- Każda warstwa odpowiada konkretnemu fragmentowi procesu komunikacji, który sam w sobie stanowi zamkniętą całość. Dla każdej warstwy zdefiniowano interfejsy do warstw sąsiednich. Przy użyciu tego modelu można wyjaśnić, w jaki sposób pakiet przechodzi przez różne warstwy do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca dysponują różnymi typami medium sieciowego. Dzięki takiemu podejściu uporządkowano reguły konstrukcji i jednocześnie uproszczono proces projektowania sieci, który w pewnym sensie także uległ rozbiciu na „warstwy”. Do najważniejszych zalet modelu ISO/OSI należy zaliczyć:
 - podział procesu komunikacji sieciowej na mniejsze, łatwiejsze do zarządzania elementy składowe;
 - utworzenie standardów składników sieci, dzięki czemu składniki te mogą być rozwijane i obsługiwane przez różnych producentów;
 - umożliwienie wzajemnej komunikacji sprzętu i oprogramowania sieciowego różnych producentów;
 - wyeliminowanie wpływu zmian wprowadzonych w jednej warstwie na inne warstwy;
 - podział procesu komunikacji sieciowej na mniejsze składowe, co pozwala na łatwiejsze jego zrozumienie.

Model ISO/OSI

Warstwa aplikacji

Warstwa prezentacji

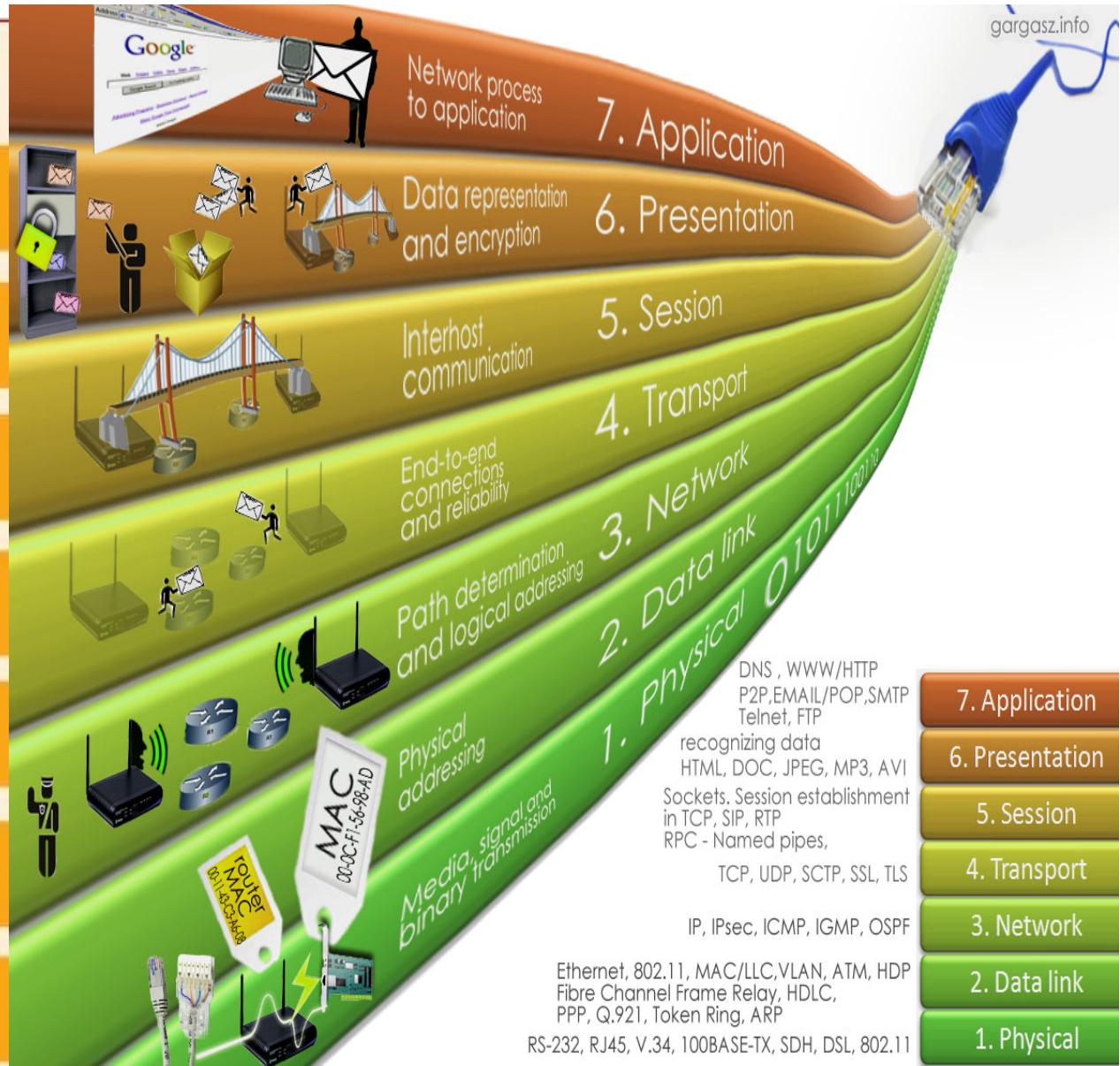
Warstwa sesji

Warstwa transportowa

Warstwa sieciowa

Warstwa łącza danych

Warstwa fizyczna



Warstwa fizyczna – transmisja binarna

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

Zadaniem warstwy fizycznej jest transmitowanie sygnałów cyfrowych pomiędzy urządzeniami sieciowymi. Jednostką informacji na poziomie tej warstwy jest pojedynczy **bit**. Parametry charakteryzujące tę warstwę to właściwości fizyczne łączą takie jak częstotliwości, napięcia, opóźnienie, długość, zniekształcenia, poziom zakłóceń, itp.

Warstwa łącza danych – bezpośrednie sterowanie łączem, dostęp do medium

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 łącza danych |
| 1 Fizyczna |

Warstwa łącza danych odpowiada za komunikację pomiędzy hostami, podłączonymi do tego samego medium. Jej głównym zadaniem jest sterowanie dostępem do medium. Jednostką informacji w tej warstwie jest **ramka** składająca się z bitów o ścisłe określonej strukturze zawierająca adresy nadawcy i adresata. Adresy urządzeń mogą mieć dowolną postać, określoną w specyfikacji zastosowanego standardu komunikacji. **Warstwa wyposażona jest w mechanizm kontroli poprawności transmisji**, w celu zapewnienia niezawodnego przesyłania danych przez medium.

Warstwa sieci – adresacja sieciowa i wybór najlepszej ścieżki

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

Głównym zadaniem warstwy sieci jest umożliwienie komunikacji pomiędzy hostami znajdującymi się w różnych sieciach lokalnych. Realizacja tego zadania możliwa jest dzięki dwóm mechanizmom: jednolitej adresacji urządzeń w całej sieci oraz routingu. Podstawową jednostką informacji w tej warstwie jest **pakiet** o ścisłe określonej strukturze zawierający oprócz danych, adresy: nadawcy i odbiorcy pakietu. **Warstwa ta nie gwarantuje niezawodności transmisji**, natomiast wyposażona jest w mechanizmy monitorowania transmisji, co pozwala m.in. na identyfikację przyczyn uniemożliwiających komunikację.

Warstwa transportowa - połączenie typu end-to-end

| |
|-----------------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

Warstwa transportowa odpowiedzialna jest za niezawodne przesyłanie danych między urządzeniami. Warstwa ta posiada mechanizmy umożliwiające inicjację, utrzymanie i zamykanie połączenia między urządzeniami, sterowanie przepływem danych oraz wykrywanie błędów transmisji.

Warstwa sesji – komunikacja między hostami

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

- Zadaniem warstwy sesji jest zarządzanie komunikacją między aplikacjami działającymi na danym hoście, a aplikacjami działającymi na innych hostach w sieci.
- Ze względu na funkcjonalność systemów operacyjnych zawsze występuje sytuacja, gdy liczba aplikacji korzystających z sieci jest większa od liczby fizycznych interfejsów sieciowych.
- Rola tej warstwy sieci polega na stworzeniu mechanizmu umożliwiającego dostarczanie danych jakie przyszły z sieci oraz wysyłanie danych do sieci do aplikacji, dla której te dane są przeznaczone.

Warstwa prezentacji – reprezentacja danych

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

- Zadaniem warstwy prezentacji jest konwersja danych pod względem formatu oraz struktury aby interpretacja tych danych była jednakowa na obu urządzeniach: wysyłającym i odbierającym.
- Najczęściej konieczność dostosowania danych wynika z różnic między platformami sprzętowymi, na których działają komunikujące się aplikacje.

Warstwa aplikacji – połączenie procesów sieciowych z aplikacjami

| |
|----------------|
| 7 Aplikacji |
| 6 Prezentacji |
| 5 Sesji |
| 4 Transportowa |
| 3 Sieci |
| 2 Łącza danych |
| 1 Fizyczna |

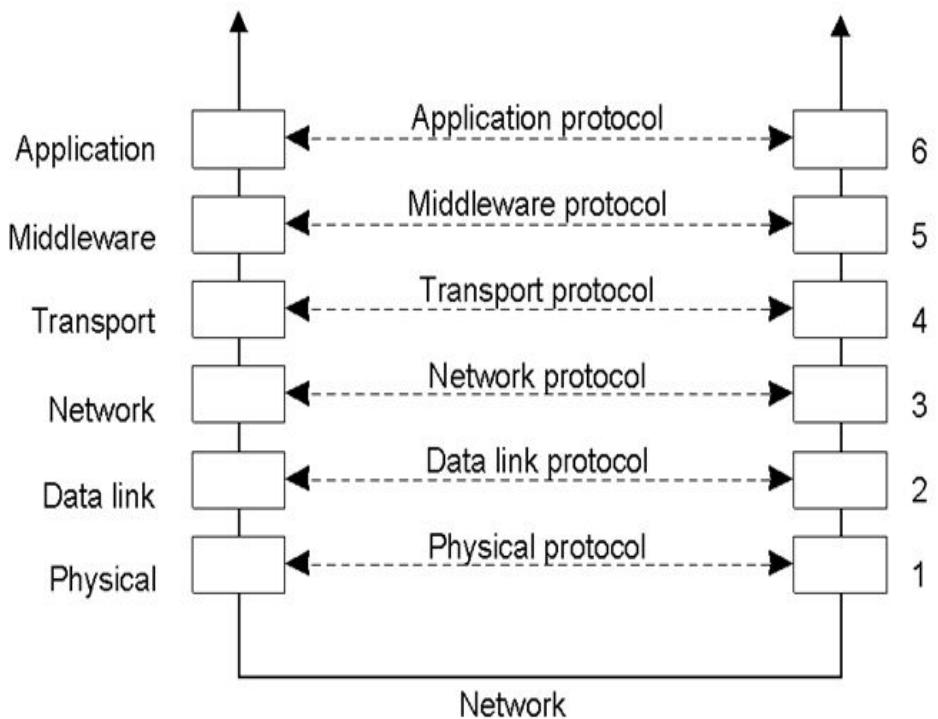
- Zadaniem warstwy aplikacji jest zapewnienie dostępu do usług sieciowych procesom aplikacyjnym, działającym na danym urządzeniu.

Model komunikacji ISO-OSI



- Model komunikacji w sieci komputerowej oparty jest na komunikacji równorzędnej (ang. peer-to-peer).
- W procesie przesyłania danych między dwoma hostami, każda warstwa sieciowa jednego hosta komunikuje się z odpowiadającą jej warstwą drugiego hosta. Komunikacja równorzędnych warstw odbywa się poprzez wymianę ścisłe określonych dla danej warstwy jednostek informacji oznaczanych skrótnie PDU (ang. Protocol Data Unit).

Model komunikacji ISO-OSI



- Aby taka forma komunikacji mogła zostać zrealizowana warstwy wyższe hosta wysyłającego muszą skorzystać z usług świadczonych przez warstwy niższe, natomiast w przypadku hosta odbierającego odwrotnie. Polega to na tym, że warstwa wyższa przekazuje dane do wysłania warstwie niższej, która przekształca dane do odpowiedniej postaci i przekazuje następnej, niższej warstwie. Gdy dane dojdą do warstwy fizycznej zostają przekształcone do postaci ciągu bitów i przekazane za pomocą medium transmisyjnego do warstwy fizycznej hosta odbierającego, na którym zachodzi proces odwrotny.

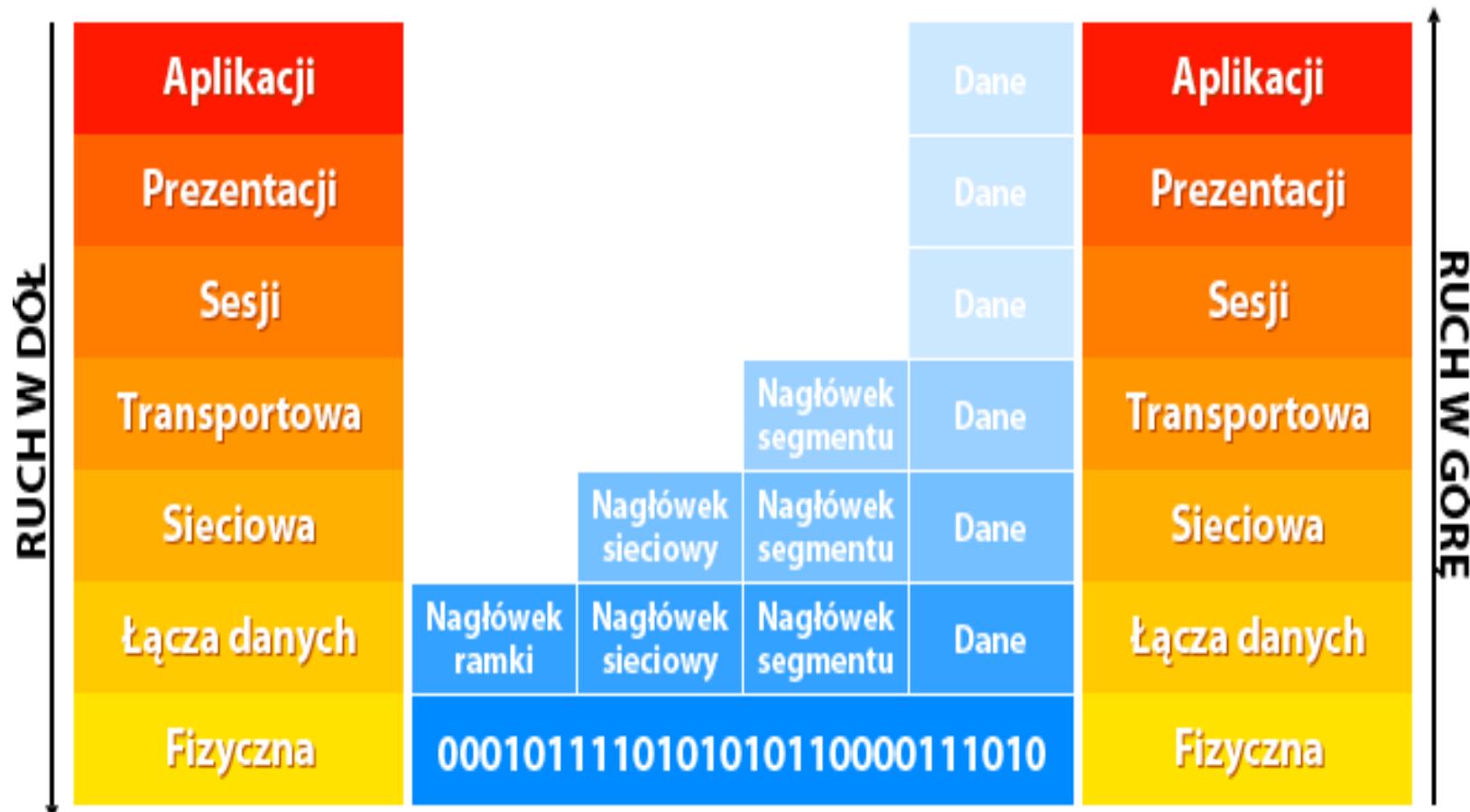
Model komunikacji ISO-OSI

Enkapsulacja

- Wędrowce danych między warstwami modelu odniesienia towarzyszy proces enkapsulacji (opakowania) jeżeli dane przekazywane są w dół stosu oraz proces dekapsulacji (rozpakowania), gdy dane przekazywane są w kierunku przeciwnym.
- Warstwa niższa przekształcając dane do odpowiedniej postaci dodaje niezbędne informacje (enkapsulacja), aby dane te mogły zostać poprawnie przesłane do równorzędnej warstwy hosta odbierającego i poprawnie przez nią zinterpretowane. Następnie, równorzędna warstwa hosta odbierającego dokonuje procesu dekapsulacji i przekazuje dane warstwie wyższej.

Enkapsulacja

Warstwy w modelu odniesienia OSI

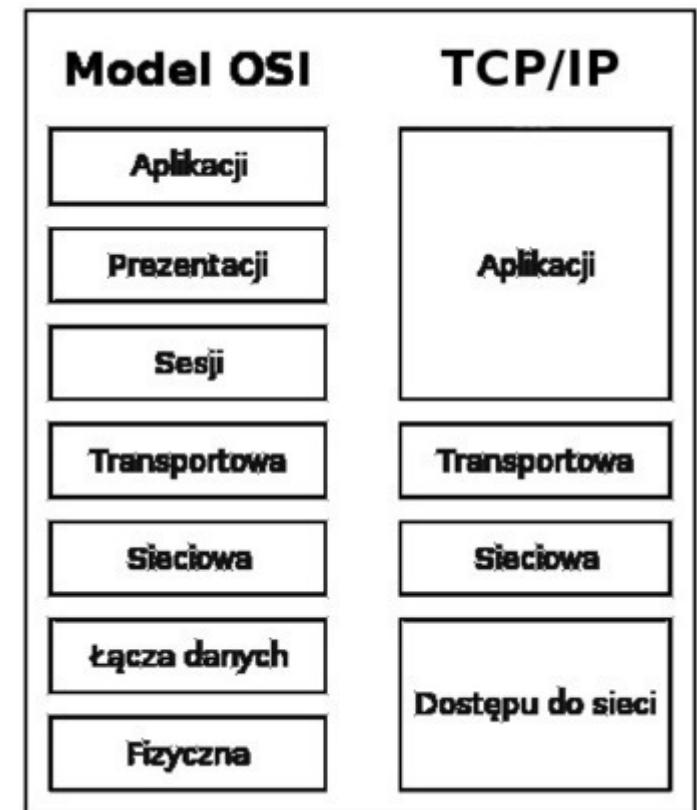


Model TCP/IP

- Zadaniem modelu odniesienia ISO/OSI było uporządkowanie i ujednolicenie procesów związanych z komunikacją w sieci:
- budowa sieci, działanie sieci, zarządzanie siecią. Ze względów praktycznych (stan rozwoju technologii, konkurencja między producentami, preferencje użytkowników, sytuacja polityczna) zaproponowane wraz z modelem ISO/OSI rozwiązania nie przyjęły się, poza samym modelem odniesienia. Weryfikacji rozwiązań dokonał „rynek”. Można zaryzykować stwierdzenie, że momentem decydującym było opracowanie rodziny protokołów TCP/IP, zimplementowanie ich w sieci ARPANET oraz w systemach UNIX'owych. Z czasem, w celu zachowania jednolitego modelu komunikacji w całym Internecie rodzina protokołów TCP/IP stała się także podstawowym standardem wykorzystywanym w sieciach lokalnych.

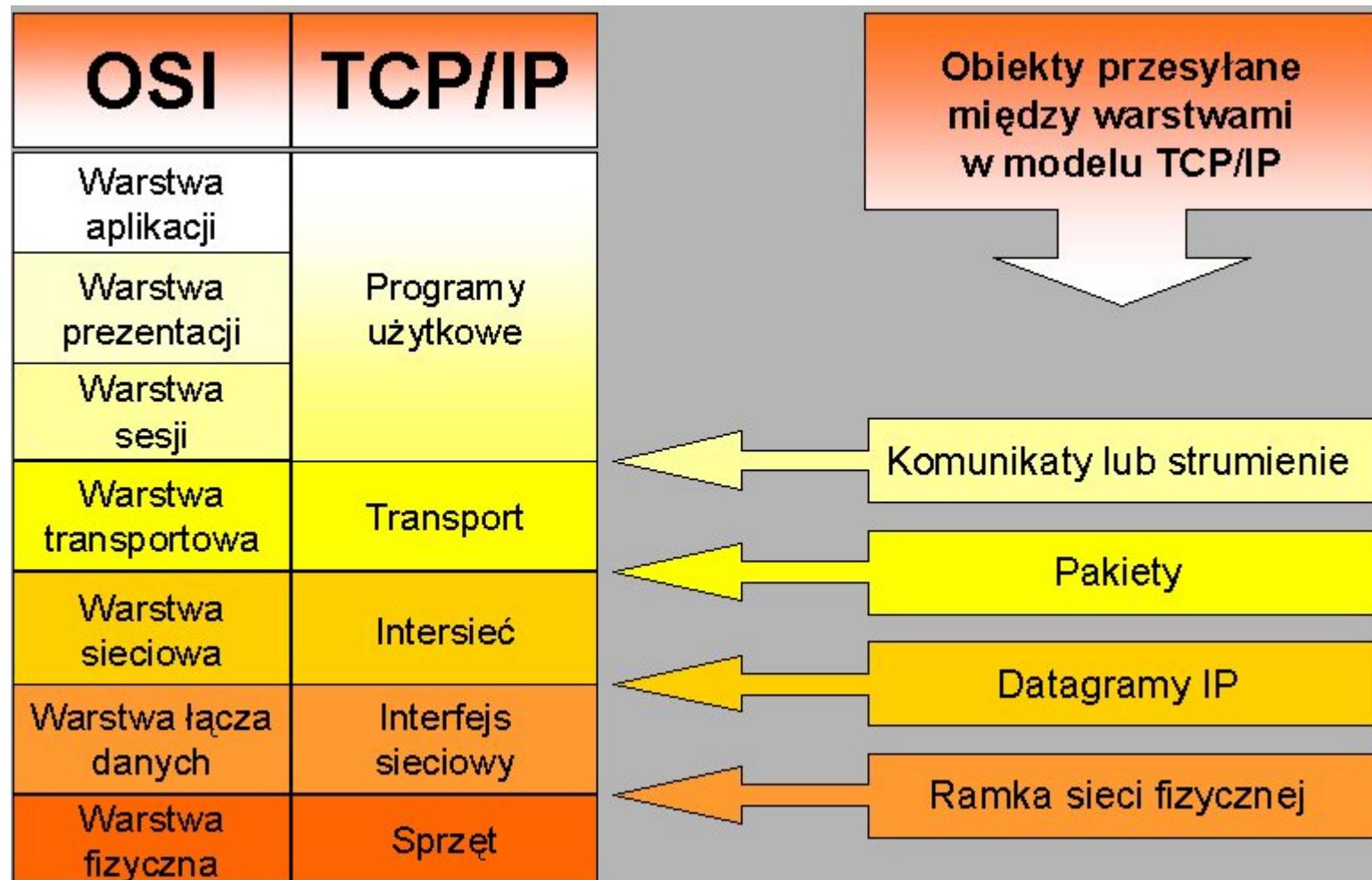
Model TCP/IP

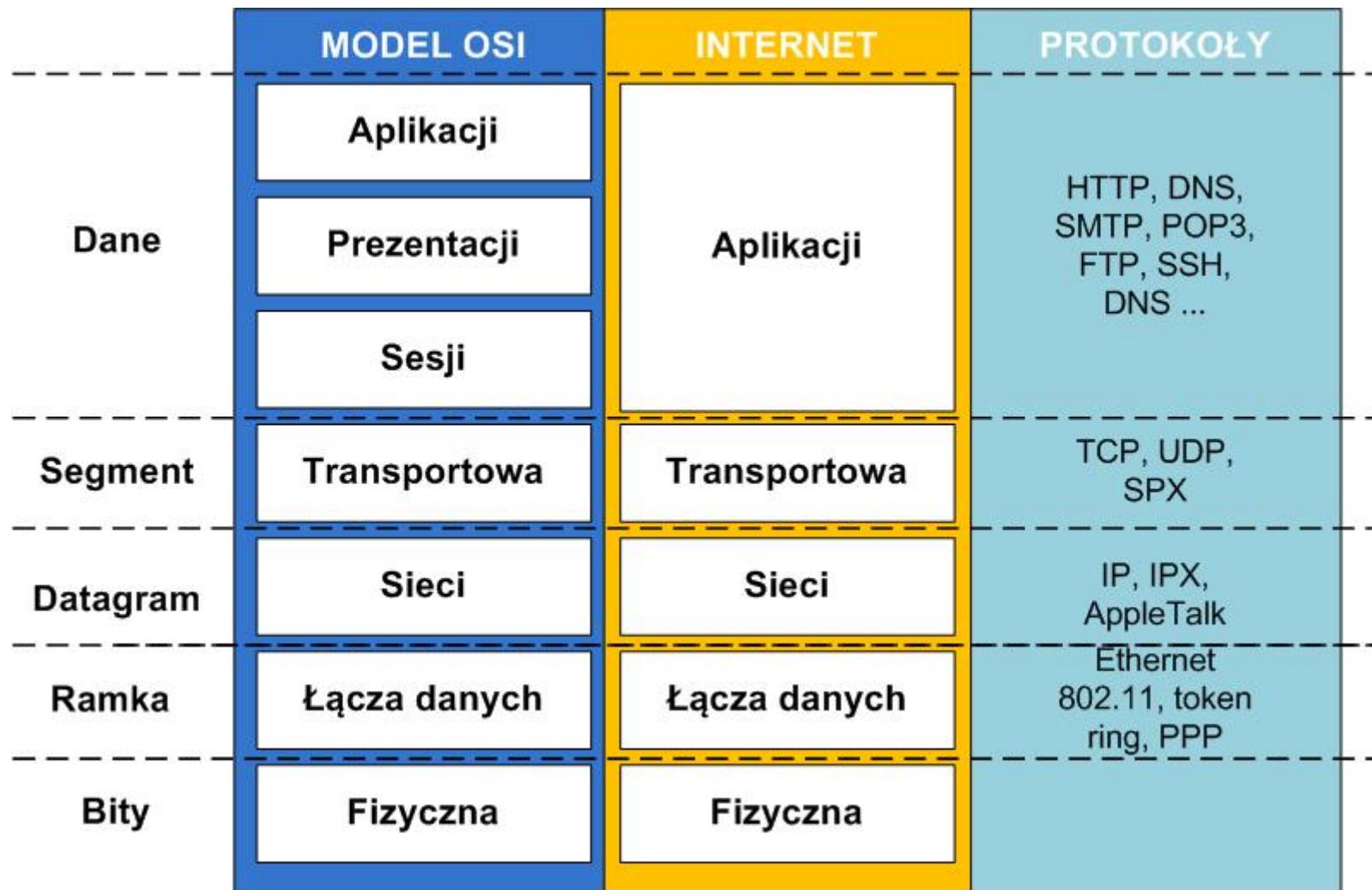
- Model TCP/IP składa się z czterech warstw:
- warstwy dostępu do sieci,
- warstwy internetu,
- warstwy transportowej,
- warstwy aplikacji.



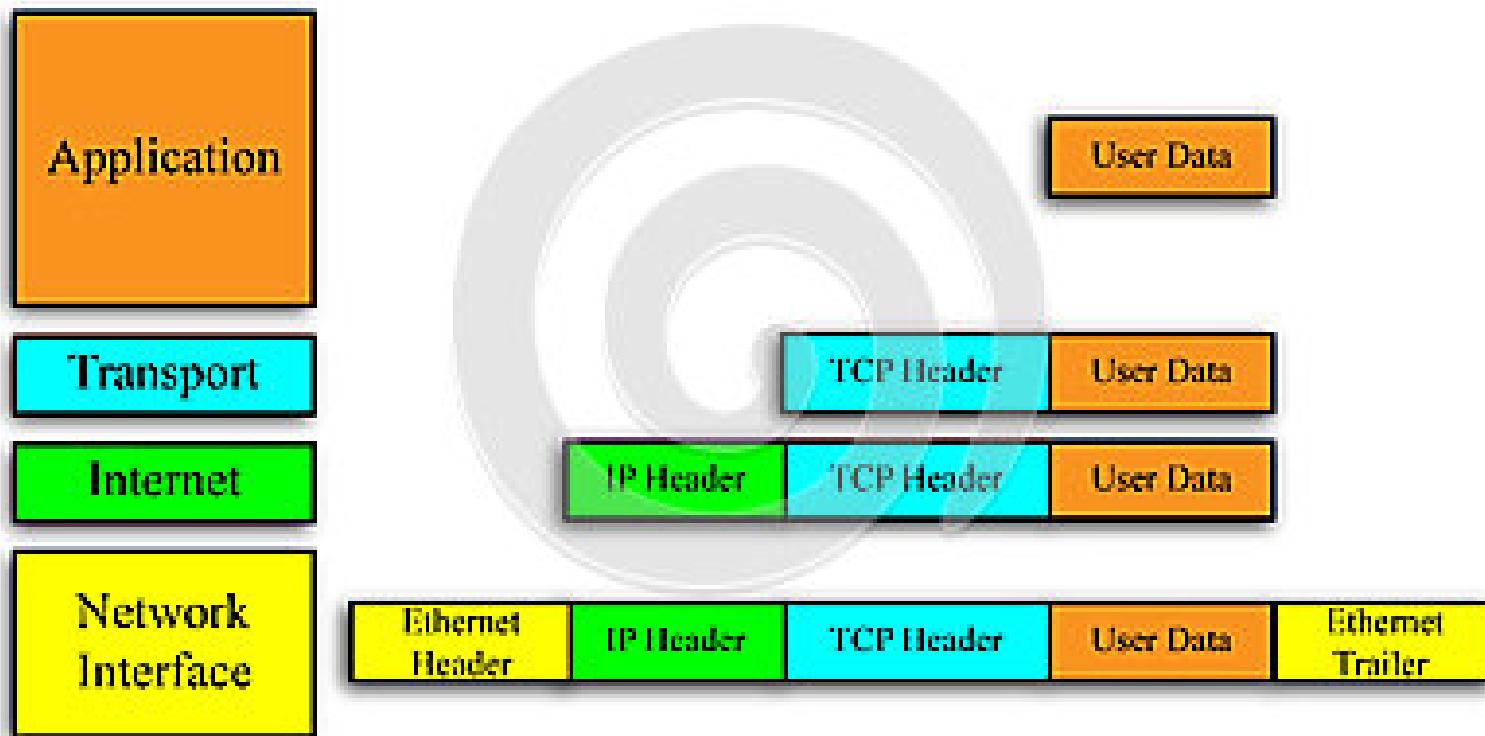
Model TCP/IP

- Ze względu na dużą różnorodność rozwiązań w zakresie fizycznej konstrukcji sieci, jaka istniała w chwili opracowywania, model TCP/IP zapewnia interfejs do warstwy dostępu do sieci traktując ją jako monolit. Warstwa ta odpowiada dwóm najniższym warstwom, fizycznej oraz łącza danych modelu ISO/OSI.
- Warstwa internetu odpowiada warstwie sieci w pełnym zakresie funkcjonalności.
- Warstwa transportowa modelu TCP/IP realizuje te same zadania, co warstwa transportowa modelu ISO/OSI oraz dodatkowo zajmuje się podstawowymi aspektami związanymi z zarządzaniem sesjami aplikacyjnymi.
- Pozostałe zadania warstwy sesji modelu ISO/OSI oraz zadania warstwy prezentacji i aplikacji zostały umieszczone w modelu TCP/IP w warstwie aplikacji. Obecnie rodzina protokołów TCP/IP jest podstawowym modelem komunikacji w Internecie i zdecydowanej większości lokalnych sieci komputerowych nie podpiętych do Internetu.





TCP/IP Network Model Encapsulation



Adresacja w sieciach

Protokół IPv4

- Protokół IPv4 został szczegółowo opisany w dokumencie RFC 791. Sam protokół IP został opracowany do działania w sytuacjach ekstremalnych, np. w trakcie wojny. W normalnych warunkach jego funkcja sprowadza się do wyboru optymalnej trasy i przesyłania nią pakietów. W przypadku wystąpienia awarii, na którymś z połączeń protokół będzie próbował dostarczyć pakiety trasami alternatywnymi (nie zawsze optymalnymi). Protokół IP jest podstawowym protokołem przesyłania pakietów w Internecie.
- Protokół IP jest protokołem bezpołączeniowym. Oznacza to, że w celu przesłania pakietów nie jest nawiązywane połączenie z hostem docelowym. Pakiety mogą być przesyłane różnymi trasami do miejsca przeznaczenia, gdzie są następnie składane w całość. Podobna zasada działa przy przesyłaniu listów tradycyjnym systemem pocztowym. Tutaj również w momencie wysyłania listu adresat nie musi potwierdzać, że przesyłkę odbierze.
- Do przesyłania danych protokół IP używa specjalnego formatu pakietu. Pakiet ten składa się z nagłówka pakietu oraz danych do przesłania. Zgodnie z zasadą przesyłania strumieniowego dane protokołu IP są danymi pochodzącyimi z wyższych warstw modelu ISO/OSI. Dane te są następnie enkapsulowane do postaci pakietu IP. Przy przejściu do warstwy łączącej danych pakiet IP jest enkapsulowany do postaci ramki Ethernetowej.

Pakiet IPv4

| + Bity 0 - 3 | 4 - 7 | 8 - 15 | 16 - 18 | 19 - 31 |
|-----------------------------|--------------------------|------------|---------|-------------------------|
| 0 Wersja | Długość nagłówka | Typ usługi | | Całkowita długość |
| 32 | Numer identyfikacyjny | | Flagi | Kontrola przesunięcia |
| 64 Czas życia pakietu (TTL) | Protokół warstwy wyższej | | | Suma kontrolna nagłówka |
| 96 | Adres źródłowy IP | | | |
| 128 | Adres docelowy IP | | | |
| 160 | Opcje IP | | | Uzupełnienie |
| 192 | Dane | | | |

- Poszczególne pola pakietu mają następujące znaczenie:
- wersja (VERS) - pole 4-bitowe określające typ protokołu IP. Jeśli jest tam wpisana wartość 4 oznacza to wersję czwartą protokołu. Jeśli jest tam wartość 6 oznacza to IPv6..
- długość nagłówka (HLEN) - pole 4 bitowe określające długość datagramu wyrażoną jako wielokrotność słów 32 bitowych.
- typ usługi (TOS ang. Type-of-Service) - 8-bitowe pole określające poziom ważności jaki został nadany przez protokół wyższej warstwy. Znaczenie poszczególnych bitów tego pola jest następujące:
 - pierwsze 3 bity: wartość 0 - stopień normalny, wartość 7 - sterowanie siecią
 - czwarty bit - O - prośba o krótkie czasy oczekiwania
 - piąty bit - S - prośba o przesyłanie danych szybkimi łączami
 - szósty bit P - prośba o dużą pewność przesyłania danych
 - bity 6, 7 nieużywane
- całkowita długość - pole 16-bitowe. Długość całego pakietu wyrażona w bajtach.
 - W celu uzyskania długości pola danych należy odjąć od długości całkowitej długość nagłówka.
 - Wartość minimalna wynosi 576 oktetów zaś maksymalna 65535 oktetów, tzn. 64 kB Identyfikacja - 16 bitowe pole używane do określania numeru sekwencyjnego bieżącego datagramu.
- Znaczniki - 3 bitowe pole. Pierwszy najbardziej znaczący ma zawsze wartość 0. Kolejne znaczące bity sterują fragmentacją
 - 0- oznacza, czy pakiet może zostać podzielony na fragmenty,
 - 1 - nie może być podzielony.

Trzeci bit oznacza: ostatni pakiet powstały w wyniku podzielenia (jeśli ma wartość 1) lub pakiet ze środka 0.

- Przesunięcie fragmentu - 13-bitowe pole służące do składania fragmentów datagramu.
- Czas życia (TTL, ang. Time To Live) - 8-bitowe pole określające liczbę routerów (przeskoków), przez które może być przesłany pakiet. Wartość tego pola jest zmniejszana przy przejściu przez każdy router na ścieżce. Gdy wartość tego pola wynosi 0, wtedy pakiet taki jest odrzucany. Zasada ta pozwala na stosowanie mechanizmów zapobiegających zapętlaniu się tras routingu.
- Protokół - 8-bitowe pole określające, który z protokołów warstwy wyższej odpowiada za przetworzenie pola Dane.
- Suma kontrolna nagłówka - 16-bitowe pole z sumą kontrolną nagłówka pozwalającą stwierdzić, czy nie nastąpiło, naruszenie integralności nagłówka. Ze względu na fakt, że każdy router dokonuje zmian w nagłówku musi ona być przeliczona na każdym z routerów.
- Adres IP nadawcy - 32-bitowe pole z adresem IP nadawcy pakietu
- Adres IP odbiorcy - 32-bitowe pole z adresem IP odbiorcy pakietu
- Opcje - pole to nie występuje we wszystkich pakietach.
- Uzupełnienie (Wypełnienie) - pole to jest wypełnione zerami i jest potrzebne, żeby długość nagłówka była wielokrotnością 32 bitów (patrz-> Długość nagłówka) Dane - pole od długości do 64kB zawierające dane pochodzące z wyższych warstw.

Opcje w IPv4

0 1 2 3 4 5 6 7

| Kopij | Klasa opcji | Numer opcji |
|-------|-------------|-------------|
|-------|-------------|-------------|

Bajt kodu w polu opcje

| Klasa opcji | Numer opcji | Długość | Opis |
|-------------|-------------|---------|--|
| 0 | 0 | - | Koniec listy opcji-używane,gdy opcje nie kończą się wraz z końcem nagłówka |
| 0 | 1 | - | Brak przypisanej funkcji, służy do wyrównania bajtów w liście opcji |
| 0 | 2 | 11 | Ograniczenia związane z bezpieczeństwem i obsługą |
| 0 | 3 | zmienna | Zapisuj trasę - do śledzenia trasy |
| 0 | 7 | zmienna | Identyfikator strumienia - przestarzałe |
| 0 | 8 | 4 | Rigorystyczne trasowanie według nadawcy |
| 0 | 4 | zmienna | Używana do zapisywania czasów wzduż trasy pakietów |

Protokół w IPv4

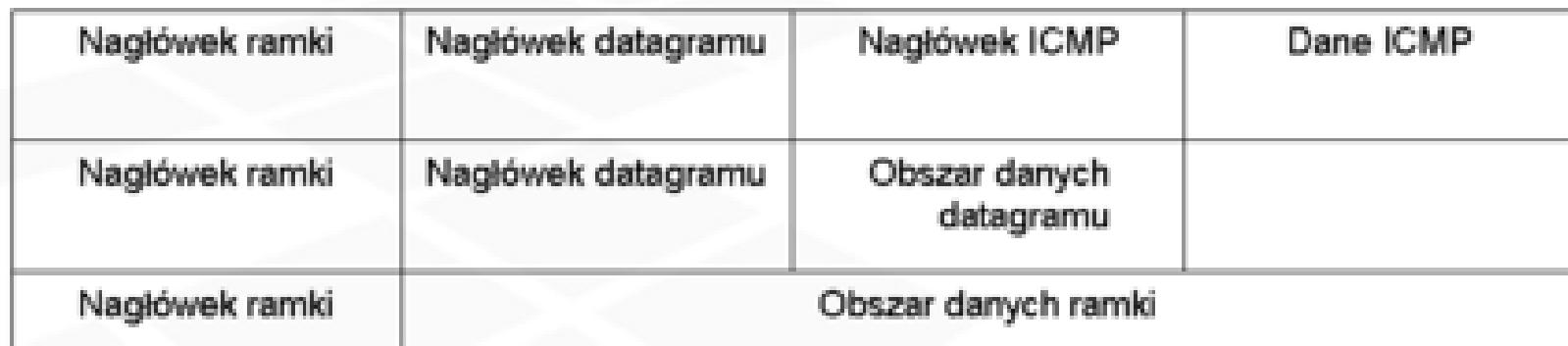
- W zależności od tego jaki protokół uformował pole danych oraz jaki powinien je przetworzyć w nagłówku pakietu musi być to zaznaczone.
- Polem odpowiedzialnym za identyfikację właściwego protokołu jest pole „Protokół”.
- Wartości wpisane w pole „protokół” nagłówka IP mają następujące znaczenie:
 - 1 - ICMP (ang. Internet Control Message Protocol) - protokół komunikacyjny sterowania siecią Internet
 - 2 - IGMP (ang. Internet Group Message Protocol) - protokół zarządzania grupami Internetowymi
 - 6 - TCP - (ang. Transmission Control Protocol) - protokół sterujący transmisją
 - 8 - EGP - (ang. Exterior Gateway Protocol) - zewnętrzny protokół bramowy
 - 17 - UDP - (ang. User Datagram Protocol) - protokół datagramów użytkownika

Protokół ICMP

- protokół IP nie sprawdza, czy dane dotarły do adresata. Rolę sprawdzania, czy pakiety docierają do adresata pełnią protokoły wyższych warstw.
- W ramach warstwy sieciowej sprawdzaniem dostępności sieci docelowej zajmuje się protokół ICMP (ang. Internet Control Message Protocol). Jego zadaniem nie jest rozwiązywanie problemów z zawodnością IP, ale zgłaszanie braku łączności. Protokół ten został zdefiniowany w dokumencie RFC 792.
- Komunikaty ICMP wysyłają zwykle bramy lub hosty. Najczęstsze powody wysyłania tych komunikatów to:
 - zbytnie obciążenie routera lub hosta
 - wysyłany jest komunikat ICMP, że należy zwolnić prędkość przesyłania komunikatów, bo host nie nadaje je przetwarzać
 - router lub host znajduje lepszą trasę - może wtedy wysłać do źródła komunikat o lepszej trasie
 - host docelowy jest nieosiągalny - wtedy ostatnia brama wysyła komunikat ICMP o niedostępności adresata i przesyła go do hosta źródłowego
 - pole TTL pakietu jest równe 0 - wtedy router może wysłać komunikat ICMP do źródła i odrzuca pakiet.

Dostarczanie komunikatu ICMP

- Jak zostało to pokazane na rysunku, sam komunikat ICMP jest przesyłany w datagramie IP. Komunikat ICMP składa się z nagłówka ICMP oraz danych ICMP. Warto przy tym zauważyć, że ze względu na zawodny charakter protokołu IP w momencie zaginięcia datagramu przenoszącego komunikat ICMP nie zostanie to zdiagnozowane. Wysyłanie komunikatów o błędach powodowałoby występowanie znacznego ruchu w sieci.



Format komunikatu ICMP

- Najważniejsze dane przesyłane w komunikacie ICMP zawarte są w polach TYP i KOD. Zatem wszystkie wersje komunikatów ICMP muszą zawierać pola: Typ, Kod, Suma kontrolna. Znaczenie poszczególnych bajtów jest następujące:

Pole Typ: 0 - odpowiedź z echem (ang. Echo Reply) 3 - odbiorca nieosiągalny (ang. Destination Unreachable). 4 - zmniejszenie szybkości nadawania - tłumienie źródła (ang. source quench) 5 - zmiana trasowania - przekierowanie (ang. redirect). 8 - prośba o echo (ang. echo request) 9 - rozgłaszenie routera (ang. router advertisement) 10 - wywołanie routera (ang. router solicitation) 11 - przekroczenie TTL (ang. Time Exceeded) 12 - kłopot z parametrami datagramu 13 - prośba / żądanie o wysłanie znacznika czasu (ang. timestamp request) 14 - odpowiedź na prośbę / żądanie o wysłanie znacznika czasu (ang. timestamp reply) 15 - prośba o informację 16 - odpowiedź z informacją 17 - prośba o maskę adresu 18 - odpowiedź z maską adresu 30 - Traceroute 31 - błąd konwersji datagramu (ang. Datagram Conversion Error) 32 - przekierowanie hosta mobilnego (ang. Mobile Host Redirect) 33 - IPv6 Where-Are-You 34 - IPv6 Here-I-Am 35 - prośba o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Request) 36 - odpowiedź na prośbę o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Reply) 37 - żądanie nazw domeny (ang. Domain Name Request) 38 - zwrot nazwy domeny (ang. Domain Name Reply) 39 - SKIP Algorithm Discovery Protocol 40 - Photuris, Security Failures
- W zależności od wartości występującej w polu Typ, wartość pola Kod może zawierać różne liczby. Najczęściej spotykane wartości par Typ, Komunikat zostaną przedstawione na następnych slajdach.
- Następujące wartości pola Typ są zarezerwowane : 1,2,7,19 (zarezerwowane dla bezpieczeństwa), 20-29, 41-255.

| 0 | 8 | 16 | 31 |
|-------------------|-----|----------------|----|
| Typ | Kod | Suma kontrolna | |
| Identyfikacja | | Numer kolejny | |
| Dane (opcjonalne) | | | |

Nagłówek ICMP

Echo request i echo response

- W przypadku komunikatu ICMP typu żądanie echa (ang. echo request) i odpowiedzi z echem (ang. echo reply) wartości pola typ wynoszą odpowiednio 8 albo 0. Wartość pola Kod w obu przypadkach wynosi 0.
- Tego typu komunikaty ICMP są wykorzystywane przez podstawowe programy testujące, takie jak ping czy traceroute.

| 0 | 8 | 16 | 31 |
|-----------------|---------|-------------------|----|
| Typ (0 lub 8) | Kod (0) | Suma kontrolna | |
| Identyfikator | | Numer sekwencyjny | |
| Dane opcjonalne | | | |

- Przy próbach wysyłania pakietów do miejsca przeznaczenia może wystąpić szereg błędów związanych z np. z uszkodzeniem łącza, błędnym adresem docelowym, nieznaną lokalizacją, itd. W takich przypadkach router, który wykryje problem wysyła komunikat o niedostępny adresacie (ang. destination unreachable) w postaci przedstawionej na rysunku.
- W zależności od przyczyny błędu w polu „Kod” pojawiają się wartości liczbowe powiązane z następującymi usterkami:
 - 0 - sieć niedostępna
 - 1 - host niedostępny
 - 2 - protokół niedostępny
 - 3 - port niedostępny
 - 4 - niezbędna fragmentacja, ustawiona wartość DF
 - 5 - nie powiodło się określenie trasy przez nadawcę (ang. source route)
 - 6 - nieznana sieć docelowa
 - 7 - nieznany host docelowy
 - 8 - host źródłowy odizolowany
 - 9 - komunikacja z siecią docelową zablokowana przez administratora
 - 10 - komunikacja z hostem docelowym zablokowana przez administratora
 - 11 - sieć niedostępna dla tego typu usługi
 - 12 - host niedostępny dla tego typu usługi
- Komunikat o niedostępnym adresie wysyłany jest również w przypadku, gdy przesyłany pakiet musi zostać podzielony na mniejsze datagramy, np. przy przesyłaniu z sieci typu Token Ring do sieci Ethernet, a znacznik w nagłówku pakietu nie pozwala na taką fragmentację. Wysyłany jest wtedy kod błędu o wartości 4.

| 0 | 8 | 16 | 31 |
|---|--------------|----------------|----|
| Typ (3) | Kod (0 - 12) | Suma kontrolna | |
| Nieużywane (musi mieć wartość zero) | | | |
| Nagłówek internetowy + pierwsze 64 bity datagramu | | | |

Inne typy i kody komunikatów ICMP

- Typ 12 Błąd ten oznacza, że jest problem związany z parametrem (ang. parameter problem).
 - Jeśli pole „Kod” ma wartość 0, to wartość w polu „Wskaźnik” wskazuje numer oktetu nagłówka datagramu, w którym występuje błędna wartość parametru.
- Typ 5 – zmiana trasowania / przekierowanie
 - Kod 0 dla sieci
 - Kod 1 dla hosta
 - Kod 2 dla typu usługi i sieci
 - Kod 3 dla typu usługi hosta

Inne typy i kody komunikatów ICMP

- Typ 13 i 14 ICMP żądanie / prośba wysłania znacznika czasowego (ang. timestamp request) o wartości pola Typ równej 13. W odpowiedzi na taką prośbę wysyłany jest komunikat odpowiedzi o wartości pola Typ równej 14. Pola kodu w przypadku obu typów komunikatów są równe 0
- Komunikaty **żądanie / prośba o przesłanie informacji** (ang. information request) oraz odpowiedź na żądanie przesłania informacji (ang. information reply) zostały zaprojektowane z myślą o przesyłaniu numerów IP. W zależności od tego czy jest to prośba o informację, czy też odpowiedź na tę prośbę pole **Typ ma wartości: 15 lub 16**. W przypadku obu typów komunikatów wartości pola „**Kod**” **wynoszą 0**. W praktyce obecnie nie są wykorzystywane, gdyż informacje takie są przesyłane w sposób bardziej dogodny przez protokoły takie jak BOOTP, RARP czy też DHCP. Protokoły służące uzyskiwaniu adresów zostaną omówione w kolejnym module poświęconym automatycznemu uzyskiwaniu adresów IP.

Inne typy i kody komunikatów ICMP

- Komunikat ICMP typu **żądanie maski adresowej** oraz **odpowiedź** na żądanie maski adresowej mają odpowiednio wartości pól **Typ** wypełnione liczbami **17** i **18**. Komunikaty te służą określeniu przez hosta jego maski adresowej.

IRDP: Komunikaty ICMP umożliwiające wykrywanie routera

- ICMP Router Discovery Messages (RFC 1256):
 - Rozgłaszenie routera (ang. router advertisement)

| 0 | 8 | 16 | 31 |
|----------------|------------------------|----------------|----|
| Typ (9) | Kod (0) | Suma kontrolna | |
| Liczba adresów | Rozmiar Pozycji adresu | Czas życia | |
| | Adres routera 1 | | |
| | Poziom preferencji 1 | | |
| | Adres routera 2 | | |
| | Poziom preferencji 2 | | |

- Wywołanie routera (ang. router solicitation)

| 0 | 8 | 16 | 31 |
|---------------|--------|----------------|----|
| Typ(10) | Kod(0) | Suma kontrolna | |
| Zarezerwowany | | | |

Protokół IGMP

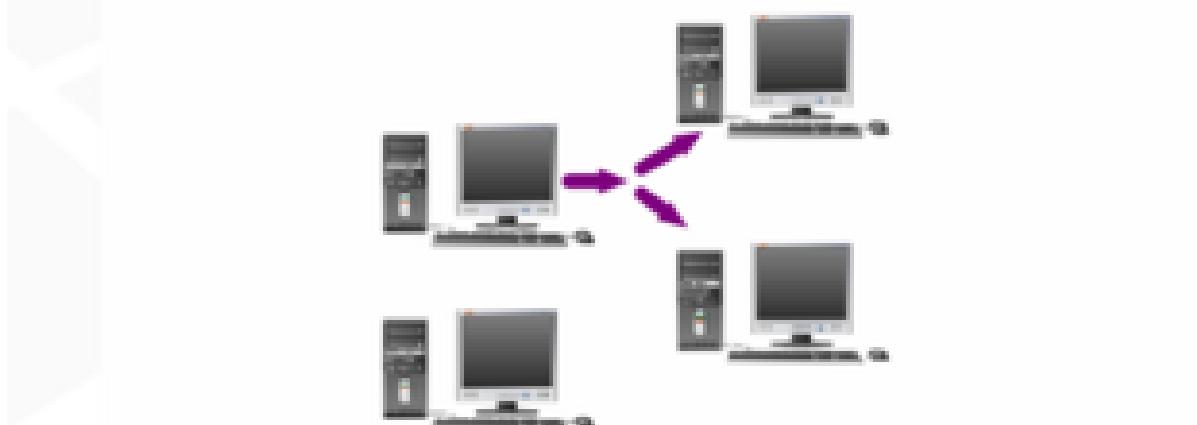
- Protokół zarządzania grupami internetowymi IGMP (ang. Internet Group Management Protocol) został opracowany z myślą o dogodnej komunikacji urządzeń sieciowych przy pomocy transmisji grupowych. Standard tego protokołu został opublikowany w dokumencie RFC 1112 pod koniec lat 90-tych XXw.
- Działanie takie jest możliwe, dzięki transmisjom grupowym (ang. multicasting). W tym typie transmisji pakiety wysyłane są na adres grupowy IP. Routery wiedzą, które komputery znajdują się w grupie obsługiwanej przez daną aplikację. Pozwala to na jednokrotne wysłanie określonych danych do wszystkich hostów z danej grupy. Jest to działanie bardziej efektywne niż transmisje kierowane (ang. unicasting), czy też wysyłanie poprzez adres rozgłoszeniowy (ang. broadcasting).

Typy transmisji danych



Unicast

Broadcast



Multicast

IGMP

- Hosty, które chcą się przyłączyć do danej grupy wysyłają komunikat IGMP Host Membership Report. Przyłączenie się klienta do danej grupy składa się z dwóch procesów:
 - host powiadamia router o tym, że chce się przyłączyć do danej grupy
 - host wiąże w sposób dynamiczny IP z adresem grupowym, który jest zarezerwowany dla danej aplikacji oraz z zarezerwowanym adresem Ethernetowym
- Opuszczenie danej grupy odbywa się poprzez wysłanie komunikatu IGMP Explicit Leave. Host powinien powiadomić lokalne routery o zamiarze opuszczenia grupy poprzez wysłanie właśnie takiego komunikatu.
- Routery okresowo sprawdzają czy w dalszym ciągu istnieje potrzeba przesyłania pakietów na adres grupowy. Kontrola taka odbywa się poprzez wysłanie zapytania przy użyciu adresu grupowego przeznaczonego dla wszystkich hostów (224.0.0.1). Pakiety które są wysyłane pod ten zarezerwowany numer IP mają ustawione pole TTL na wartość jeden, dzięki temu nie są rozsyłane dalej przez inne routery. W odpowiedzi hosty powinny przesłać pakiet raportu z adresem takim jaki jest zarezerwowany dla tej grupy. Po sprawdzeniu, które z grup jeszcze istnieją routery będą przesyłały tylko pakiety dla funkcjonujących grup, natomiast pakiety z adresem grupowym będą odrzucane przez router.

IGMP: struktura pakietu

| 0 | 4 | 8 | 16 | 32 |
|-------------|-----|-------------|----------------|----|
| Wersja | Typ | Nie używane | Suma kontrolna | |
| Adres grupy | | | | |

W nagłówku pakietu IGMP przesyłane są następujące pola:

Wersja - 4b - wersja pakietu IGMP Typ - 4b - typ komunikatu. Wartości tam zapisane oznaczają odpowiednio;

1 - zapytanie o przynależność hosta

2 - raport o przynależności hosta

Nie używane - 8b - pole nie wykorzystywane

Suma kontrolna - 16b - pole wykorzystywane do przesyłania liczby umożliwiającej sprawdzenie integralności pakietu

Adres grupy - 32b - gdy pakiet jest przesyłany w celu zapytania o przynależność hosta, to pole to jest puste. Gdy host odpowiada raportem o przynależność do grupy, to w polu tym przesyłany jest adres rozsyłania grupowego konkretnej grupy.

Konieczność adresacji

- W przypadku sieci komputerowych, podobnie jak w przypadku tradycyjnych sposobów komunikacji, istnieje potrzeba określenia miejsca przeznaczenia, do którego powinna zostać wysłana porcja danych. Można to przyrównać do wysyłania listu do znanej nam (lub nieznanej) osoby. W obu przypadkach należy określić adres miejsca przeznaczenia. W przypadku tradycyjnego systemu pocztowego na kopercie wpisywane są dane adresata. Zwykle też podawane są dane nadawcy, w celu komunikacji zwrotnej. Oba adresy powinny być unikalne w innym przypadku korespondencja mogłaby nie trafiać do adresatów.
- Również analogicznie jak w tradycyjnej poczcie pakiety transportowane są do określonej sieci, w której router jest odpowiednikiem urzędu pocztowego. Router decyduje również do którego hosta adresuje ramkę z danym pakietem, podobnie jak listonosz, który przynosi przesyłki do konkretnego adresata.

Adresacja w sieciach

- Analogicznie w sieciach komputerowych stosuje się adresację wymaganą przez stosowane protokoły. W zależności od rozpatrywanych warstw modelu ISO/OSI można wyróżnić adresację na poziomie warstwy łącza danych (L2) oraz adresację na poziomie warstwy sieci (L3). Pierwsza z nich dotyczy adresacji fizycznej interfejsu sieciowego, tzw. **adres MAC** (Media Access Control). Druga z nich odnosi się do adresacji logicznej **adres IP**.

Przydzielanie adresów

- Podobnie jak w przypadku rzeczywistych adresów tak samo w przypadku adresów IP musi być zapewniona ich unikalność.
- Przydzielaniem adresów zajmują się powołane do tego celu organizacje:
 - Pierwotnie zajmował się tym Internet Network Information Center (InterNIC). Organizacja ta obecnie nie istnieje.
 - Internet Assigned Numbers Authority (IANA).

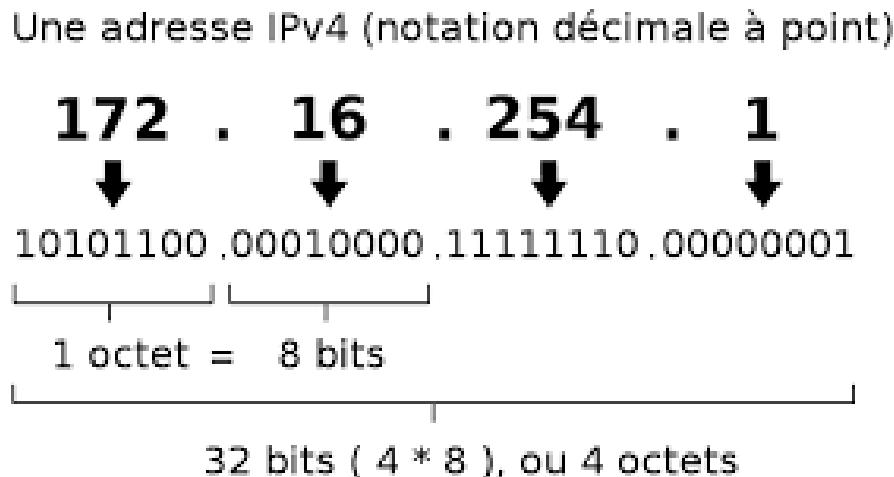
Wersje adresacji

- IPv4 – 32 bity adresu – dostępnych adresów 2^{32}
- IPv6 – 128 bitów adresu – dostępnych adresów 2^{128}

| IPv4 | IPv6 |
|--|--|
| Deployed 1981 | Deployed 1999 |
| Address Size: 32-bit number | Address Size: 128-bit number |
| Address Format: | Address Format: |
| Dotted Decimal Notation: 192.149.252.76 | Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD |
| Prefix Notation: 192.149.0.0/24 | Prefix Notation: 3FFE:F200:0234::/48 |
| Number of Addresses: $2^{32} = \sim 4,294,967,296$ | Number of Addresses: $2^{128} =$ $\sim 340,282,366,920,938,463,463,374,$ $607,431,768,211,456$ |

Struktura adresacji IPv4

- W przypadku adresacji IP adres składa się z części bitów przeznaczonych
 - na identyfikację sieci, do której został przypisany dany interfejs hosta
 - pozostałej liczby bitów przeznaczonych na adresację hosta w danej sieci.



Maska

- W przypadku IPv4 część adresu przeznaczona na identyfikator sieci jest zależna od długości maski sieciowej.
- Maska ta służy do wyznaczania adresu sieciowego, który jest (musi być) taki sam dla wszystkich interfejsów znajdujących się w tej samej podsieci.
- Netmaska podobnie jak adres IPv4 składa się z 32 bitów.

| CIDR | Maska | Liczba dostępnych adresów hostów |
|------|-----------------|----------------------------------|
| /1 | 128.0.0.0 | 2147483646 |
| /2 | 192.0.0.0 | 1073741822 |
| /3 | 224.0.0.0 | 536870910 |
| /4 | 240.0.0.0 | 268435454 |
| /5 | 248.0.0.0 | 134217726 |
| /6 | 252.0.0.0 | 67108862 |
| /7 | 254.0.0.0 | 33554430 |
| /8 | 255.0.0.0 | 16777214 |
| /9 | 255.128.0.0 | 8388606 |
| /10 | 255.192.0.0 | 4194302 |
| /11 | 255.224.0.0 | 2097150 |
| /12 | 255.240.0.0 | 1048574 |
| /13 | 255.248.0.0 | 524286 |
| /14 | 255.252.0.0 | 262142 |
| /15 | 255.254.0.0 | 131070 |
| /16 | 255.255.0.0 | 65534 |
| /17 | 255.255.128.0 | 32766 |
| /18 | 255.255.192.0 | 16382 |
| /19 | 255.255.224.0 | 8190 |
| /20 | 255.255.240.0 | 4094 |
| /21 | 255.255.248.0 | 2046 |
| /22 | 255.255.252.0 | 1022 |
| /23 | 255.255.254.0 | 510 |
| /24 | 255.255.255.0 | 254 |
| /25 | 255.255.255.128 | 126 |
| /26 | 255.255.255.192 | 62 |
| /27 | 255.255.255.224 | 30 |
| /28 | 255.255.255.240 | 14 |
| /29 | 255.255.255.248 | 6 |

Formy adresacji IP

- Adresacja klasowa
- Adresacja bezklasowa
-
-
- Podział na notację klasową i bezklasową wynika ze stosowania numerów IPv4 i odpowiadających im netmasek. W przypadku notacji klasowej numery IP jak i maski mają ścisłe określone zakresy. W przypadku adresacji bezklasowej dozwolonym numerom IPv4 mogą być przypisane dowolne (dozwolone) netmaski.

Podział adresów IPv4 na klasy

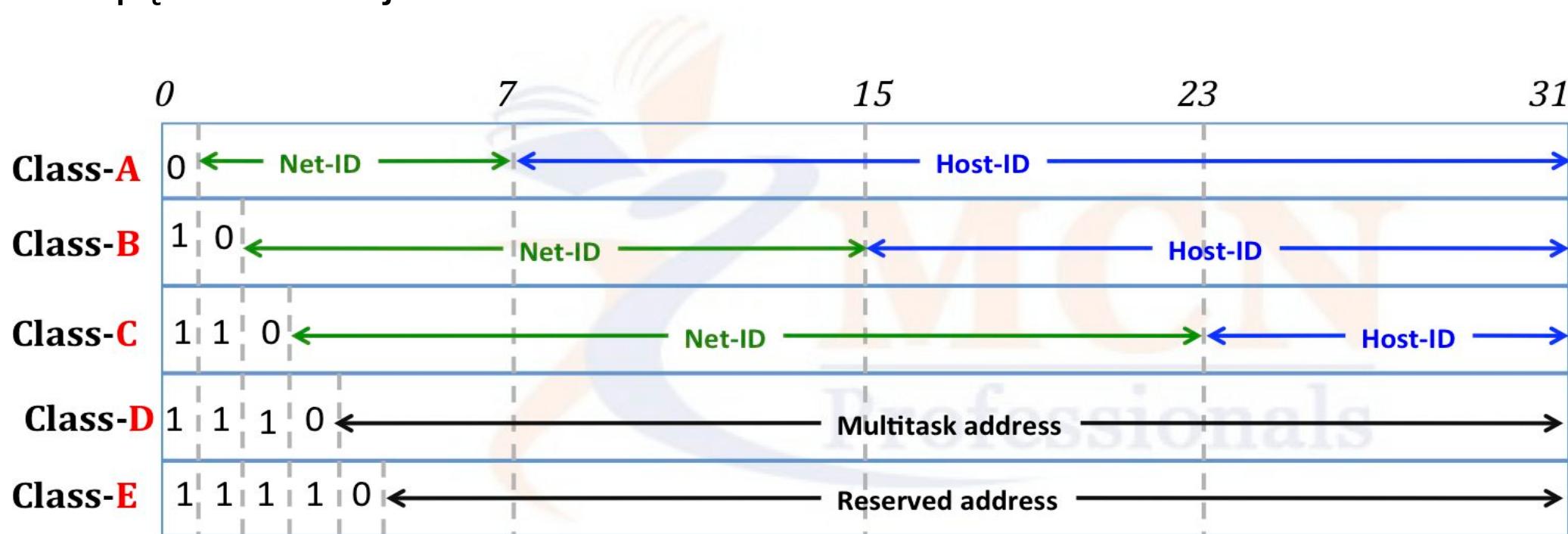
| Bit → 0 | 31 | Address Range: |
|-----------|---------------------------|-----------------------------|
| 0 | Class A Address | 0.0.0 - 127.255.255.255 |
| 1 0 | Class B Address | 128.0.0.0 - 191.255.255.255 |
| 1 1 0 | Class C Address | 192.0.0.0 - 223.255.255.255 |
| 1 1 1 0 | Class D Multicast Address | 224.0.0.0 - 239.255.255.255 |
| 1 1 1 1 0 | Reserved | 240.0.0.0 - 247.255.255.255 |

Klasa IPv4

- Klasa A została przeznaczona dla dużych organizacji z bardzo dużą liczbą hostów. Pula adresowa sieci zawiera się w przedziale 1-126 i stanowi połowę wszystkich dostępnych adresów.
- Klasa B została przeznaczona dla dużej liczby organizacji z dużą liczbą hostów. Numery sieci w tej klasie zawierają adresy od 128 do 191, stąd dostępna liczba adresów stanowi 25 procent całej puli adresowej.
- Klasa C była zaplanowana przede wszystkim dla małych organizacji z liczbą hostów nie przekraczającą kilkuset sztuk.
- Klasa D służy do rozsyłania grupowego pakietów przy pomocy adresów IPv4. Klasa E została zarezerwowana przez IETF dla celów badawczych.
- Jak się później okazało podział ten nie pozwalał na efektywne zarządzanie pulą adresów.

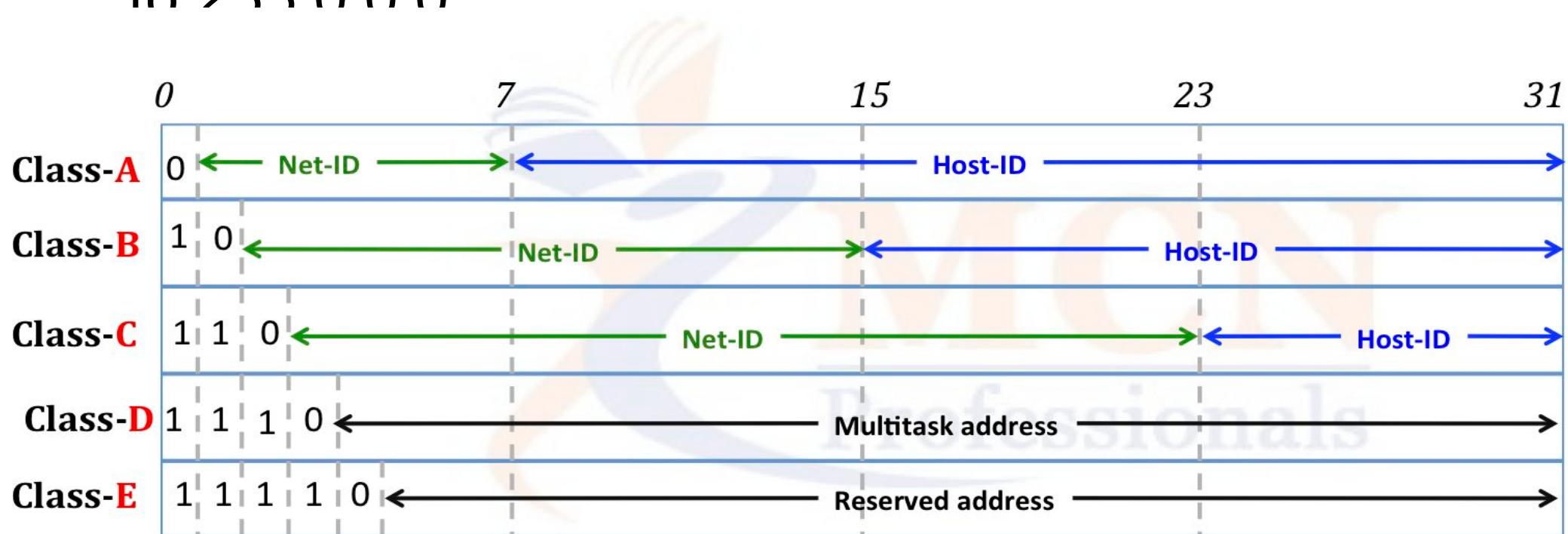
KLASA A

- W klasie A tylko 8 bitów zostało przeznaczone na adresację sieci.
- Pierwszy najbardziej znaczący bit ma zawsze wartość 0, zatem do dyspozycji na numerację sieci klasy A pozostaje 2^7 adresów.
- Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 0 do 126.
- Adres zaczynający się od 127 został zarezerwowany na adres pętli zwrotnej



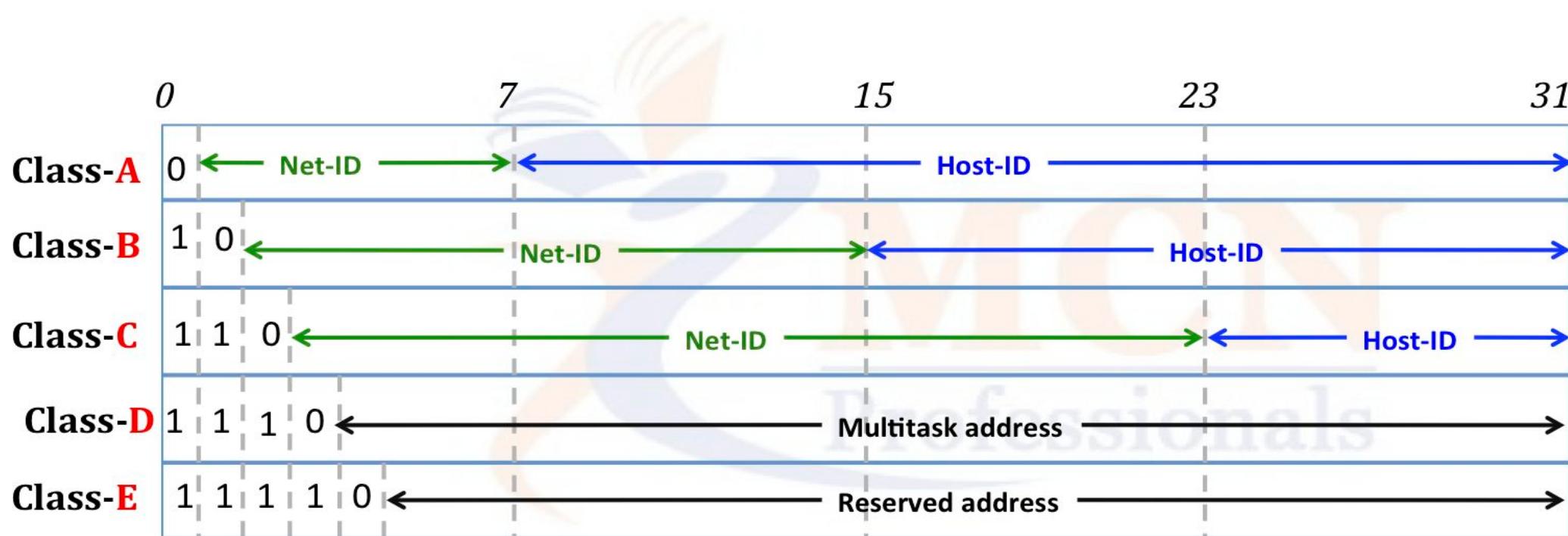
KLASA A

- W sieci tej klasy pozostałe 24 bity są przeznaczone na część identyfikującą hosty.
- Daje to przestrzeń adresową ponad 16 milionową (16.777.216)
- Standardowa (naturalna) maska dla sieci tej klasy to 255.0.0.0



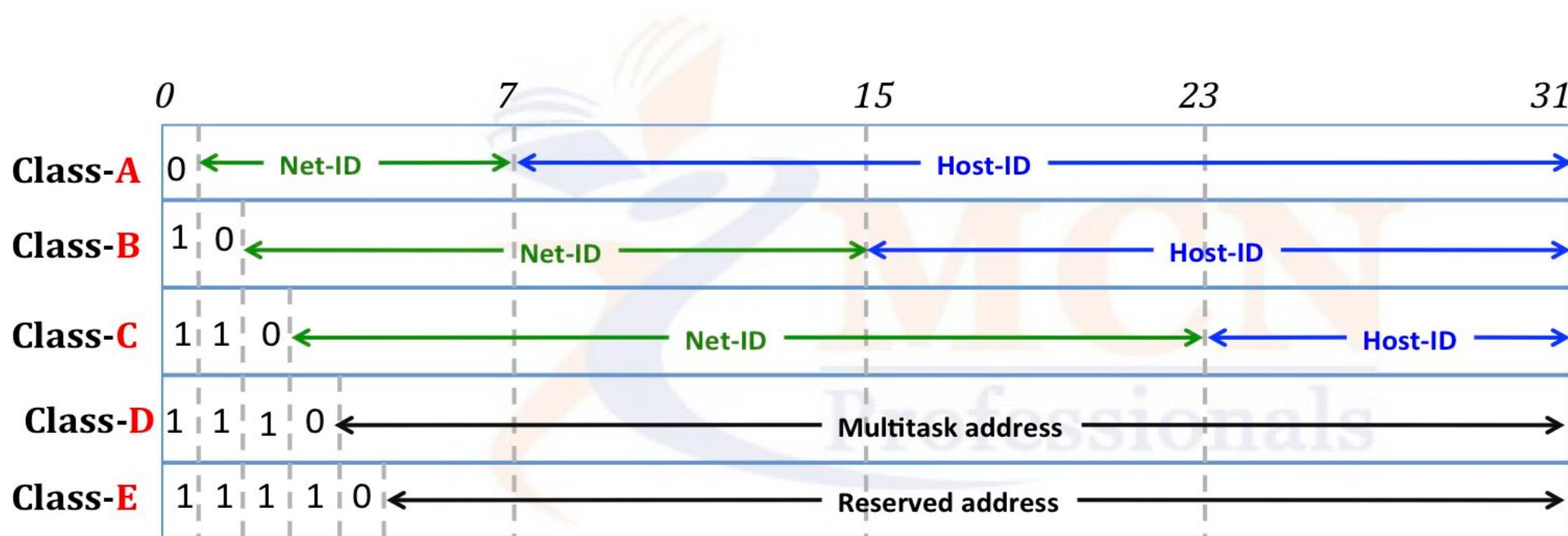
KLASA B

- W klasie B 16 bitów zostało przeznaczone na adresację sieci.
- Pierwsze dwa najbardziej znaczące bity mają wartość 10. Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 128 do 191.
- Zatem na zaadresowanie sieci pozostaje 14 bitów, co daje 16384 (2^{14}) adresów
- W sieci tej klasy pozostałe 16 bitów przeznaczone są na część identyfikującą hosty.
- Daje to przestrzeń adresową umożliwiającą wykorzystanie ponad 65 tysięcy adresów sieciowych (65536).
- Standardowa (naturalna) maska sieciowa dla tej klasy wynosi: 255.255.0.0



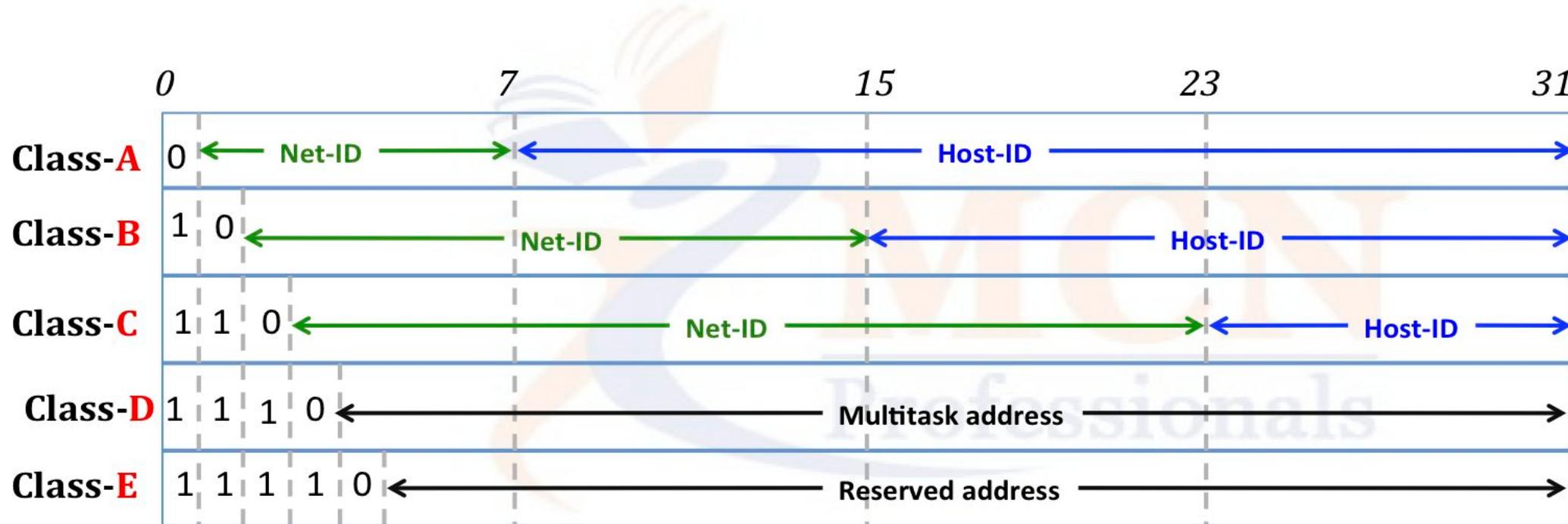
KLASA C

- W klasie C 24 najbardziej znaczące bity zostały przeznaczone na adresację sieci.
- Pierwsze trzy najbardziej znaczące bity mają wartość 110.
- Dzięki temu zakres adresów pierwszego oktetu zawiera się w przedziale od 192 do 223.
- Daje to razem 2097152 (2^{21}) adresów przeznaczonych na identyfikację sieci.
- W sieci tej klasy pozostałe 8 bitów przeznaczone są na część identyfikującą hosty.
- Daje to przestrzeń adresową umożliwiającą zaadresowanie małych sieci składających się z nie więcej niż 256 adresów.
- Standardowa (naturalna) maska sieciowa dla tej klasy wynosi: 255.255.255.0



KLASA D

- Klasa adresów D została zarezerwowana na potrzeby rozsyłania grupowego.
- Jest to bardziej efektywny sposób przesyłania danych do hostów niż rozwijanie poprzez adres 255.255.255.255.
 - Ten ostatni sposób wymaga przetwarzania pakietów przez wszystkie hosty w domenie rozwijanej. Związań jest to z niepotrzebnym nakładem obliczeń. Zamiast tego można wykorzystywać adresację grupową, gdzie tylko określone hosty będą otrzymywać pakiety, które muszą przetworzyć.
- Przykładem takich pakietów są pakiety wysyłane przez protokoły routingu:
 - RIPv2 wysyła aktualnienia na adres 224.0.0.9
 - OSPF wysyła pakiety "Hello" na adres 224.0.0.5



Zasady adresowania IPv4

- Z puli dostępnych wartości adresów część wartości jest wyłączona z adresów, które mogą być nadawane hostom.
- Jednym z takich ograniczeń jest adres postaci 127.x.x.x. Został on zarezerwowany na potrzeby pętli zwrotnej.
- Kolejnym ograniczeniem jest adres, w którym identyfikator hosta składa się z liczb 255. Wynika, to z założenia, że ten rodzaj adresu przeznaczony jest do rozsyłania komunikatów typu broadcast.
- Identyfikator hosta nie może składać się z samych zer, gdyż jest to adres sieci, w której znajduje się host.
- Aby spełniony był warunek unikalności całych adresów IP, identyfikator hosta nie może powtórzyć się w sieci.

Użyteczna liczba hostów

- $2^n - 2$
- Pierwszy adres hosta – zarezerwowany na identyfikator sieci
- Ostatni adres hosta – zarezerwowany na adres rozgłoszeniowy - broadcastowy

Ograniczenia klasowego IPv4

- Protokół IPv4 został zaprojektowany na początku lat 80-tych XX w.
- W tamtym czasie spełniał on w wystarczającym stopniu wymagania co do liczby adresów niezbędnych do obsłużenia połączonych w sieci urządzeń.
- **Jednak wraz z rozwojem sieci komputerowych wzrasta zapotrzebowanie na adresy IP.**
- Potrzeba co raz większej liczby adresów wymusiła potrzebę zarządzania dostępną pulą adresów.
- **Problem ten szczególnie dotyczył adresów klasy C**, która zakładała przydzielanie całej puli składającej się z **255 adresów**. W przypadku, gdy sieć ta posiadała zaledwie kilkanaście hostów pozostałe ponad dwieście było niewykorzystanych.
- „rozrzutność” dotyczyła sieci klasy A, czy też B. Sytuacja odwrotna występowała w przypadku organizacji z dużą liczbą hostów. W tym przypadku istniała potrzeba używania większej puli adresów. W obu przypadkach wiązało się to z nieefektywnym wykorzystaniem przydzielonych adresów.
- Dodatkowym problemem były duże tablice routingu i związane z tym długie czasy przesyłania pakietów w sieciach.

Rozwiążanie problemu niedobory adresów IPv4

- Ze względu na zmniejszającą się pulę dostępnych adresów podejmowane były różne kroki w celu rozwiązania tego problemu.
- Tworzenie podsieci (1985)
- Tworzenie podsieci o zróżnicowanej długości adresów (1987)
- Bezklasowy routing między-domenowy – CIDR (1993)
- Wydzielenie prywatnych adresów sieciowych
- Translacja adresów sieciowych
- Automatyczne przydzielanie adresów.

• Tworzenie podsieci (1985)

- Jednym ze sposobów, zaproponowanym w 1985 roku, było tworzenie podsieci.
- Zakres adresów hostów w danej sieci był dzielony na mniejsze podsieci z mniejszą liczbą hostów, w każdej z nowo utworzonych.
- Metoda ta wymagała „pożyczenia” bitów z części adresu przeznaczonej dla identyfikacji hosta dla zaadresowania podsieci.

- Tworzenie podsieci o zróżnicowanej długości adresów (1987)

- Innym sposobem rozwiązania problemu brakujących adresów było, zaproponowanie w dokumencie RFC 1009 (w 1987 roku), tworzenie podsieci o zróżnicowanej długości masek adresów (ang. Variable Length Subnet Masks (VLSM)).
- Przydzielona danej organizacji pula adresów jest następnie dzielona wewnątrz niej na mniejsze porcje.
- Podział ten jest następnie niewidoczny z zewnątrz sieci danej organizacji.

•Bezklasowy routing międzydomenowy – CIDR (1993)

- Jeszcze inne rozwiązanie polegało na wprowadzeniu bezklasowego routingu międzydomenowego - CIDR (ang. Classless Inter-Domain Routing).
- Metoda CIDR podobnie jak metoda VLSM pozwala na podział puli adresów na mniejsze porcje. Przy czym w odróżnieniu do metody VLSM, metoda CIDR polega na podziale puli dostępnych adresów przez Internet Registry dla dostawcy Internetu (ISP) najwyższego poziomu, poprzez poziom pośredni niski, aż do odbiorcy usług Internetowych.
- W metodzie CIDR informacje na temat masek sieci są przekazywane przez poszczególne routery w trakcie aktualizacji tablic routingu.

• Wydzielenie prywatnych adresów sieciowych

- Kolejnym sposobem, który może być stosowany w sieciach lokalnych jest mechanizm adresów prywatnych.
- Nie wymaga on praktycznie żadnych nakładów poza wyborem numeracji.
- Pakiety pochodzące z takich adresów będą odfiltrowywane przez routery.
- **Dokument RFC 1918 podaje trzy pule adresów prywatnych, po jednej dla poszczególnych klas A,B,C.** Pakiety z adresami prywatnymi nie są przepuszczane przez routery sieciowe.
 - W klasie A są to adresy z zakresu 10.0.0.0 - 10.255.255.255
 - W klasie B do dyspozycji jest pula adresów 172.16.0.0 - 172.31.255.255
 - W klasie C są to adresy 192.168.0.0 192.168.255.255
- Dodatkowo stosując netmaski i zmiennej długości (VLSM) można te pule zmniejszać lub też zwiększać w zależności od potrzeb.

• Translacja adresów sieciowych - NAT

- W przypadku adresów prywatnych, aby była możliwa komunikacja w Internecie, wprowadzono mechanizm tłumaczenia adresów prywatnych na publiczne, tzw. NAT (ang. Network Address Translation).
- Dzięki temu organizacjom wystarczy pojedynczy publiczny adres IP, w przypadku braku serwerów WWW, pocztowych i innych.

Adresacja IPv6

- Protokół IPv4 jest w dalszym ciągu powszechnie wykorzystywany pomimo niedoskonałości tego rozwiązania.
- Prace nad nowszą wersją protokołu IPv6 trwają od kilku lat.
- Jednym z ważniejszych argumentów przemawiających za potrzebą migracji do nowszej wersji protokołu jest zapotrzebowanie na dużą liczbę adresów Internetowych.
- Innym powiązanym z poprzednim, wymaganiem jest potrzeba zapewnienia ustalonych parametrów transmisji dla ruchu multimedialnego. Technologie wprowadzane coraz powszechniej: telefonia IP, telewizja cyfrowa, video na życzenie itp. wymagają stałych parametrów przesyłania.
- Innym, równie istotnym, wymogiem jest kwestia autoryzacji nadawcy, która nie była możliwa w IPv4.
- Te oraz inne niewymienione czynniki bardzo istotnie przemawiają za szybką migracją do IPv6, który również bywa nazywany protokołem następnej generacji IPNG (IP Next Generation).

- Warto podkreślić fakt, że zmiana protokołu warstwy sieciowej modelu ISO (protokołu warstwy Internetowej stosu protokołów TCP/IP) nie powoduje potrzeby dostosowywania protokołów pozostałych. Część z dostawców Internetu (ISP) oferuje już dostęp do IPv6. Ze względu na fakt, że w dalszym ciągu powszechnie używany jest IPv4, to ruch IPv6 jest tunelowany w starszej wersji protokołu (IPv6-in-IPv4). Protokół IPv6 opisują dokumenty RFC 1883 oraz RFC 1884.
- Jedną z podstawowych zalet, chociaż nie najważniejszą, jest liczba dostępnych adresów w nowej wersji protokołu.
- Ze względu na to, że do zapisania adresu w IPv6 użytych jest 128 bitów, to dostępna pula wynosi ok. $3,4 \times 10^{38}$ adresów.
- W przeliczeniu na powierzchnię Ziemi daje to ok. $6,7 \times 10^{17}/\text{mm}^2$. W ten sposób zapotrzebowanie na pulę adresów dla nowych rozwiązań sieciowych powinno zostać spełnione.

Budowa datagramu IPv6

IPv6 – nagłówki rozszerzające

- Ważną cechą, która umożliwia szybsze przesyłanie pakietów przez routery jest możliwość dołączania nagłówków rozszerzających.
- Jest to możliwe, dzięki polu „Następny nagłówek” (ang. Next header). Nagłówek ten jest umieszczany w pakiecie za nagłówkiem podstawowym, a przed nagłówkiem warstwy transportowej. Nagłówki te powinny występować w określonej kolejności natomiast nie ma ograniczenia co do ich liczby. Nagłówki te zastępują pola opcjonalne w IPv4. Dzięki zastosowaniu tego mechanizmu możliwe jest, m.in. uwierzytelnianie pakietów.
- Wśród zdefiniowanych nagłówków dodatkowych można wymienić: Hop-by-hop options header Destinations options header-1 Source routing header Fragmentation header Authentication header IPv6 encryption header Destination option header-2

Adresy IPv6

- Jedną z najważniejszych i bardzo istotną zmianą w stosunku do IPv4 jest przeznaczenie większej liczby bitów na określenie adresu.
- Rozwój metod komunikacji (GPRS, EDGE, UMTS) oraz wprowadzanie na rynek nowych urządzeń z funkcją komunikacji sieciowej wymusza zastosowanie efektywniejszych metod przesyłania datagramów. Jednym z bardziej istotnych elementów jest możliwość nieograniczonego przydzielania adresów IP.
- Zwiększenie przestrzeni adresowej z 2^{32} (IPv4) do 2^{128} (IPv6) oznacza przyrost możliwych do przypisania adresów z ok. $4,3 \times 10^9$ do ok. $3,4 \times 10^{38}$.
- Adres IPv6 zapisywany jest postaci **heksadecymalnej**.
- Preferowany jest zapis, w którym co 16 bitów (4 cyfry heksadecymalne) wstawiany jest separator w postaci dwukropka. 0432:5678:abcd:00ef:0000:0000:1234:4321.
- Notacja pozwala opuszczać wiodące zera, zatem adres ten można zapisać również jako:
432:5678:abcd:ef:::1234:4321
- Specyfikacja pozwala również w przypadku występowania mieszanej infrastruktury (IPv6 z Ipv4) na podkreślenie tego faktu poprzez zapis ostatnich 32 bitów podobnie jak to było zapisywane w wersji IPv4, np.: 0:0:0:0:0:13.1.68.3 0:0:0:0:FFFF:129.144.52.38 lub wersji skróconej: 13.1.68.3 FFFF:129.144.52.38
- Ze względu na fakt, że spora część ruchu odbywa się w dalszym ciągu w oparciu o IPv4 pakiety IPv6 są tunelowane wewnętrz IPv4.

IPv6 typy adresów

- Wartym podkreślenia jest fakt, że w IPv6 nie ma adresów rozgłoszeniowych (ang. broadcastowych). Ich funkcje w pełni zastąpiły adresy rozsyłania grupowego.
- W specyfikacji RFC 1884 wymienione są 3 typy adresów:
 - kierowanego (ang. Unicast) - identyfikator pojedynczego interfejsu. Pakiety wysyłane na ten adres trafiają do określonego w nim hosta
 - uniwersalnego (ang. Anycast) - identyfikator zbioru interfejsów, które zwykle należą do różnych węzłów sieci. Pakiet wysłany na ten adres jest dostarczany tylko na jeden z interfejsów z tego zbioru. Zwykle jest to adres interfejsu najbliższego w rozumieniu metryki
 - grupowego (ang. Multicast) - podobnie jak w przypadku poprzednim: identyfikator jest przypisany do zbioru interfejsów. Pakiet zawierający ten adres jest dostarczany na każdy z interfejsów należących do zbioru.

IPv6 specjalne pule adresów

- Wśród adresów IPv6 są pewne specjalne pule adresów. Część z nich zostanie wymieniona poniżej
- ::/128 – adres zerowy, wykorzystywany tylko w oprogramowaniu.
- ::1/128 – adres pętli zwrotnej, zapisany inaczej: 0:0:0:0:0:0:1 (odpowiednik 127.0.0.1 z IPv4).
- ::/96 – adresy kompatybilne z adresem IPv4 hosta korzystającego z IPv6 i IPv4.
- ::ffff:0:0/96 – adresy kompatybilne z adresem IPv4 hosta korzystającego wyłącznie z IPv4, część adresu (32 najmniej znaczące bity) jest taka sama jak w IPv4
- fe80::/10 – adresy typu "link-local" wykorzystywane wewnątrz sieci lokalnych, w procesie autokonfiguracji.
- ff00::/8 – adresy multicast

Ethernet

Aloha - prekursor

Prekursorem sieci Ethernet była sieć komputerowa Aloha oparta na komunikacji radiowej. Sieć Aloha powstała na Uniwersytecie Hawajskim. Jej twórcą był Norman Abramson wraz z kolegami. Sieć umożliwiała komunikację między wyspami Archipelagu Hawajskiego.

- Komputer podpięty do sieci Aloha mógł w dowolnym momencie rozpocząć nadawanie. Jeżeli po określonym czasie nie było odpowiedzi od adresata, nadawca przyjmował, że nastąpiła kolizja w wyniku jednoczesnego nadawania we współdzielonym medium.
- W takiej sytuacji obaj nadawcy odczekiwali losowy przedział czasu zanim ponawiali nadawanie, co gwarantowało poprawną transmisję. Jednak przy zwiększającej się liczbie komputerów wykorzystanie kanału spadało do 18%, a po wprowadzeniu synchronizacji transmisji do 37%.

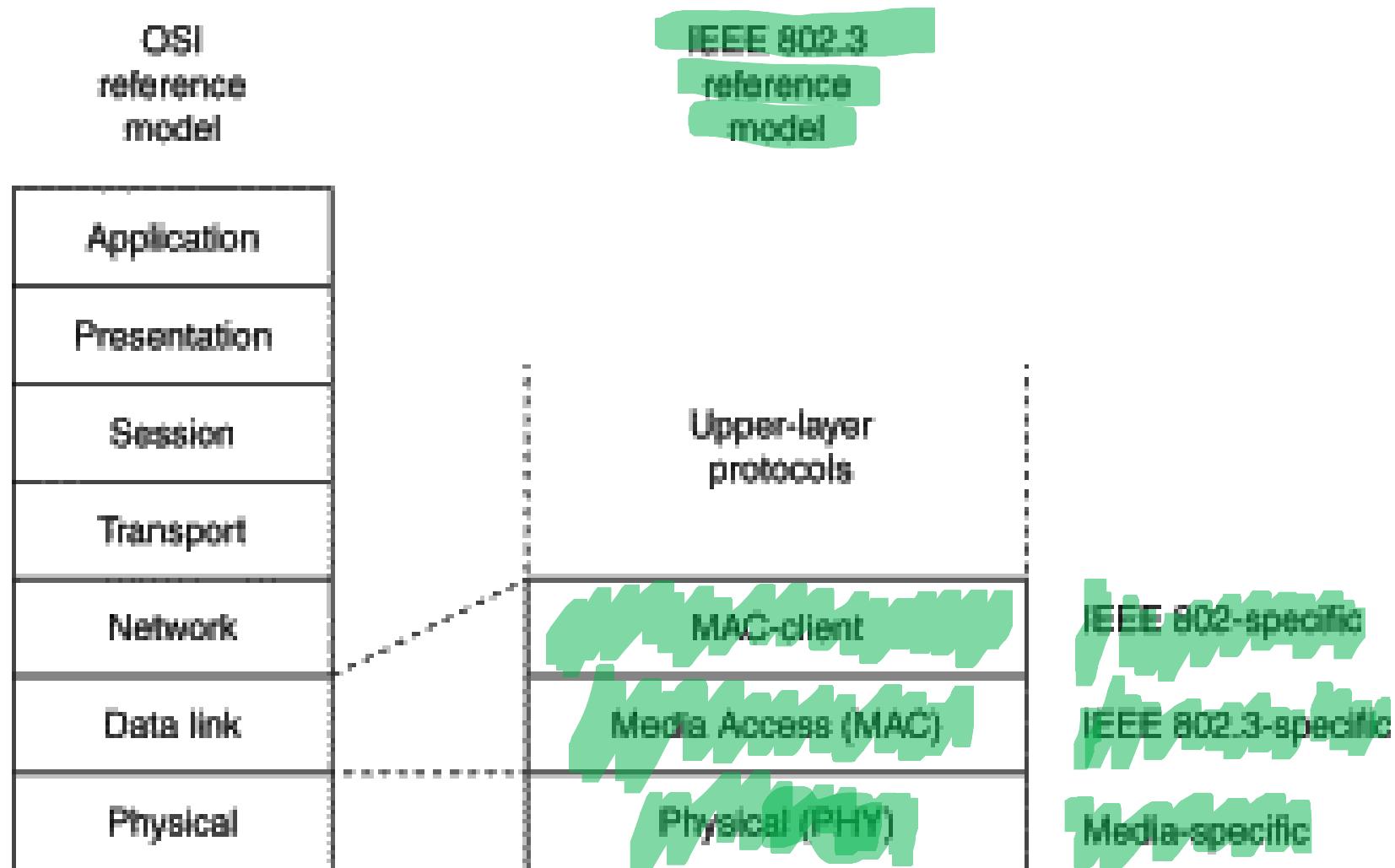
Historia

- Bazując na rozwiązaniach zastosowanych w sieci Aloha, Bob Matcalfe opracował **nowy system**, w którym znalazły się takie mechanizmy jak: **wykrywanie kolizji, wykrywanie zajętości kanału, współdzielony dostęp, co doprowadziło do powstania protokołu CSMA/CD** (Carrier Sense Multiple Access with Collision Detection).
- W wyniku dalszych prac nad siecią Ethernet przeprowadzonych w firmie Xerox PARC powstała pierwsza doświadczalna sieć **komputerowa Alto Aloha Network**.
- Prace zostały uwieńczone publikacją w 1976 roku artykułu w Communication of the Association for Computing Machinery (CACM): Bob Matcalfe, David Boggs – „Ethernet Distributed Packet Switching for Local Computer Networks” oraz uzyskaniem w 1977 roku w Urzędzie Patentowym USA **patentu numer 4063220 pod nazwą: „Multipoint Data Communication System With Collision Detection”**.

Historia

- W 1980 roku konsorcjum **DIX (Digital-Intel-Xerox)** opublikowało **standard Ethernet** pracujący z prędkością **10Mbps** znany pod nazwą **DIX Ethernet**. Ostatnia znana wersja tego standardu to DIX V2.0
- W wyniku prac komisji 802.3, która wykorzystała w swoich pracach standard DIX opublikowano w 1985 roku standard IEEE pod nazwą: „**IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications**”.
- W następnych latach opracowano **całą gamę standardów 802.3** uwzględniających bieżący stan rozwoju technologii w zakresie przesyłania sygnałów.
- Do najważniejszych można zaliczyć standardy o znaczeniu przełomowym dla sieci komputerowych, jak np. **wprowadzenie skrętki, czy kolejnych szybkości ethernetu: 100Mb, 1Gb i obecnie 10Gb**.

Ethernet a model OSI



| Ethernet Standards | | | |
|--------------------|---------|------------------|--------------------------------------|
| Standard | Speed | Segment Length | Cable |
| 10Base5 | 10Mbps | 500m / 164ft. | RG-8 or RG-11 coaxial |
| 10Base2 | 10Mbps | 185m / 606ft. | RG 58 A/U or RG 58 C/U coaxial |
| 10Base-T | 10Mbps | 100m / 328ft. | Category 3 or better UTP |
| 100Base-T | 100Mbps | 100m / 328ft. | Cat 5 UTP or STP |
| 100Base-TX | 100Mbps | 100m / 328ft. | Cat 5 UTP or STP |
| 100Base-FX | 100Mbps | 2 kM | 2-pair 850 nm multimode optic fibers |
| 1000Base-T | 1Gbps | 100m / 328ft. | 4-pair, CAT5 or CAT5e |
| 1000Base-SX | 1Gbps | 550m (multimode) | 2-pair fiber optic |

IEEE 802 Standards

| | |
|---------------|--|
| 802.1 | Bridging & Management |
| 802.2 | Logical Link Control |
| 802.3 | Ethernet - CSMA/CD Access Method |
| 802.4 | Token Passing Bus Access Method |
| 802.5 | Token Ring Access Method |
| 802.6 | Distributed Queue Dual Bus Access Method |
| 802.7 | Broadband LAN |
| 802.8 | Fiber Optic |
| 802.9 | Integrated Services LAN |
| 802.10 | Security |
| 802.11 | Wireless LAN |
| 802.12 | Demand Priority Access |
| 802.14 | Medium Access Control |
| 802.15 | Wireless Personal Area Networks |
| 802.16 | Broadband Wireless Metro Area Networks |
| 802.17 | Resilient Packet Ring |

Wybrane standardy

| Original IEEE | IEEE Shorthand Name | Informal Name(s) | Speed | Typical Cabling |
|---------------|---------------------|-------------------------------|-----------|-----------------|
| 802.3i | 10BASE-T | Ethernet | 10 Mbps | UTP |
| 802.3u | 100BASE-T | Fast Ethernet (Fast E) | 100 Mbps | UTP |
| 802.3z | 1000BASE-X | Gigabit Ethernet (Gig E, GbE) | 1000 Mbps | Fiber |
| 802.3ab | 1000BASE-T | Gigabit Ethernet (Gig E, GbE) | 1000 Mbps | UTP |
| 802.3ae | 10GBASE-X | 10 GbE | 10 Gbps | Fiber |
| 802.3an | 10GBASE-T | 10 GbE | 10 Gbps | UTP |
| 802.3ba | 40GBASE-X | 40GbE (40 GigE) | 40 Gbps | Fiber |
| 802.3ba | 100GBASE-X | 100GbE (100 GigE) | 100 Gbps | Fiber |

Podstawy działania

- Lokalną sieć komputerową (LAN) tworzą różnego rodzaju urządzenia sprzętowo-programowe, które współpracując ze sobą umożliwiają przesyłanie danych między komputerami.
- W celu poprawnej realizacji tego zadania muszą zostać spełnione ścisłe określone warunki, które definiują cztery podstawowe elementy : ramkę, protokół sterujący dostępem do medium, komponenty sygnalizacji, media fizyczne.

Podstawowe elementy

- **Ramka** – ustandaryzowany zestaw bitów umożliwiający przesyłanie danych.
- **Protokół dostępu do medium (MAC protocol)** – zestaw reguł działania każdego interfejsu Ethernet umożliwiający współdzielenie kanału Ethernet
- **Elementy sygnałowe** – standardowe urządzenia do transmisji sygnałów w kanale Ethernet
- **Medium fizyczne** – kable oraz inne elementy wykorzystywane do przesyłania sygnałów między komputerami dołączonymi do sieci Ethernet

Ramka ethernet

| Obliczenie kodu FCS | | | | | | | |
|---|--|-------|----------|---------------|--------------------|-------------|-----------|
| Preambuła 7 | Znacznik SFD 1 | Cel 6 | Źródło 6 | Długość Typ 2 | Dane od 46 do 1500 | Wypełnienie | Kod FCS 4 |
| Pola ramki: Ethernet IEEE 802.3 | | | | | | | |
| Oktety | Opis | | | | | | |
| - 7 | Preambuła | | | | | | |
| - 1 | Znacznik początku ramki (SFD) | | | | | | |
| - 6 | Adres MAC odbiorcy | | | | | | |
| - 6 | Adres MAC nadawcy | | | | | | |
| - 2 | Pole długości/typu (długość, jeśli wartość jest mniejsza od 0800 oznacza DNSR; w przeciwnym razie typ protokołu) | | | | | | |
| - od 46 do 1500 dane (jeśli mniej niż 46 oktetów, to na końcu konieczne jest dodanie wypełnienia) | | | | | | | |
| - 4 | Kod kontrolny ramki FCS (suma kontrolna CRC) | | | | | | |

Ramka ethernet II



Pola ramki Ethernet IEEE 802.3

| Oktety | Opis |
|-----------------|---|
| - 8 | Preambuła (zakończona wzorem 10101011, czyli znacznikiem SFD 802.3) |
| - 6 | Adres MAC odbiorcy |
| - 6 | Adres MAC nadawcy |
| - od 46 do 1500 | dane (jeśli mniej niż 46 oktetów, to na końcu konieczne jest dodanie wypełnienia) |
| - 2 | Pole typu |
| - 4 | Kod kontrolny ramki FCS (suma kontrolna CRC) |

802.3 vs Ethernet II

| IEEE 802.3 | | | | | | |
|------------|--------------------------|----------------|---------------|---------------|-----------------------|---------------------|
| 7 | 1 | 6 | 6 | 2 | 46 do 1500 | 4 |
| Preambuła | Początek znacznika ramki | Adres odbiorcy | Adres nadawcy | Długość / Typ | Dane i nagłówek 802.2 | Kod kontrolny ramki |
| Ethernet | | | | | | |
| 8 | 6 | 6 | 2 | 46 do 1500 | 4 | |
| Preambuła | Adres odbiorcy | Adres nadawcy | Typ | Dane | Kod kontrolny ramki | |

Preambuła

.Preambuła to 7 oktetów składających się z na przemian występujących jedynek i zer. Preambuła **służy do synchronizacji taktowania w systemach Ethernet o szybkości do 10Mb**. Szybsze systemy Ethernet zachowały preambułę w celu zachowania zgodności.

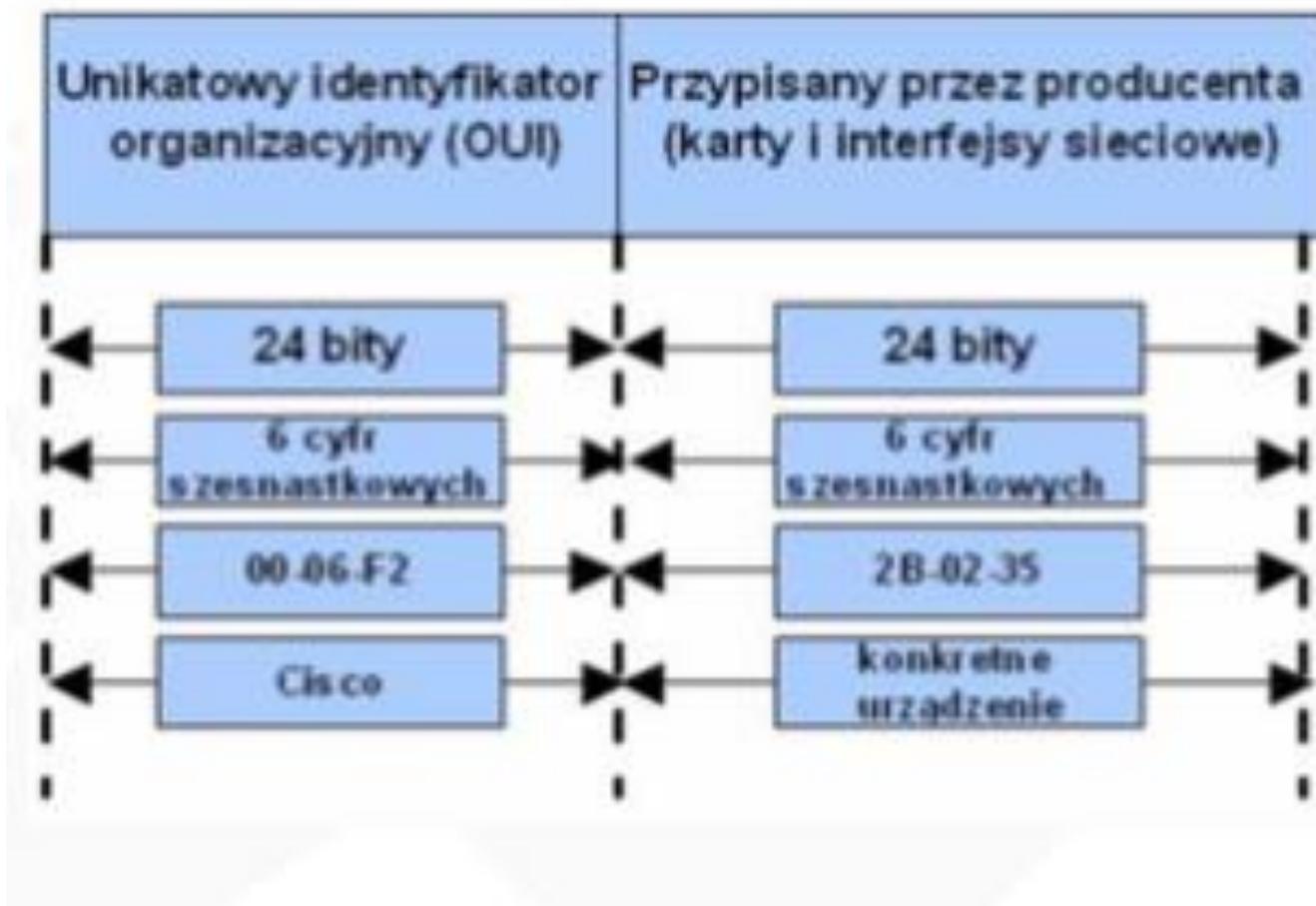
.Znacznik początku ramki (SFD) to jeden oktet bitów w postaci: 10101011, oznaczający **koniec sekwencji synchronizującej**.

.Pole adresata zawiera MAC adres odbiorcy. Adres odbiorcy może być MAC adresem konkretnego urządzenia, adresem grupowym lub rozgłoszeniowym.

.Pole adresu nadawcy zawiera MAC adres nadawcy. Adres nadawcy jest MAC adresem konkretnego urządzenia nadającego, będącego węzłem sieci Ethernet.

.Znacznik VLAN (**Virtual LAN**) został wprowadzony przez standard **IEEE 802.1Q**. Stanowi on czterooktetowy zespół dodatkowych pól w nagłówku ramki Ethernet służących do identyfikacji przynależności ramki do konkretnego VLAN'u w komunikacji między urządzeniami oraz do obsługi priorytetów zgodnie z QoS (Quality of Service).

Format adresu MAC



Znacznik VLAN

. W skład znacznika wchodzą następujące pola:

- .TPID (Tag Protocol Identifier),
- .TCI (Tag Control Information): Priority,

.CFI (Canonical Format Indicator), pole używane do zachowania kompatybilności między przełącznikami Ethernet a Token Ring. Dla przełączników Ethernet wartość tego pola ustawiana jest na 0.

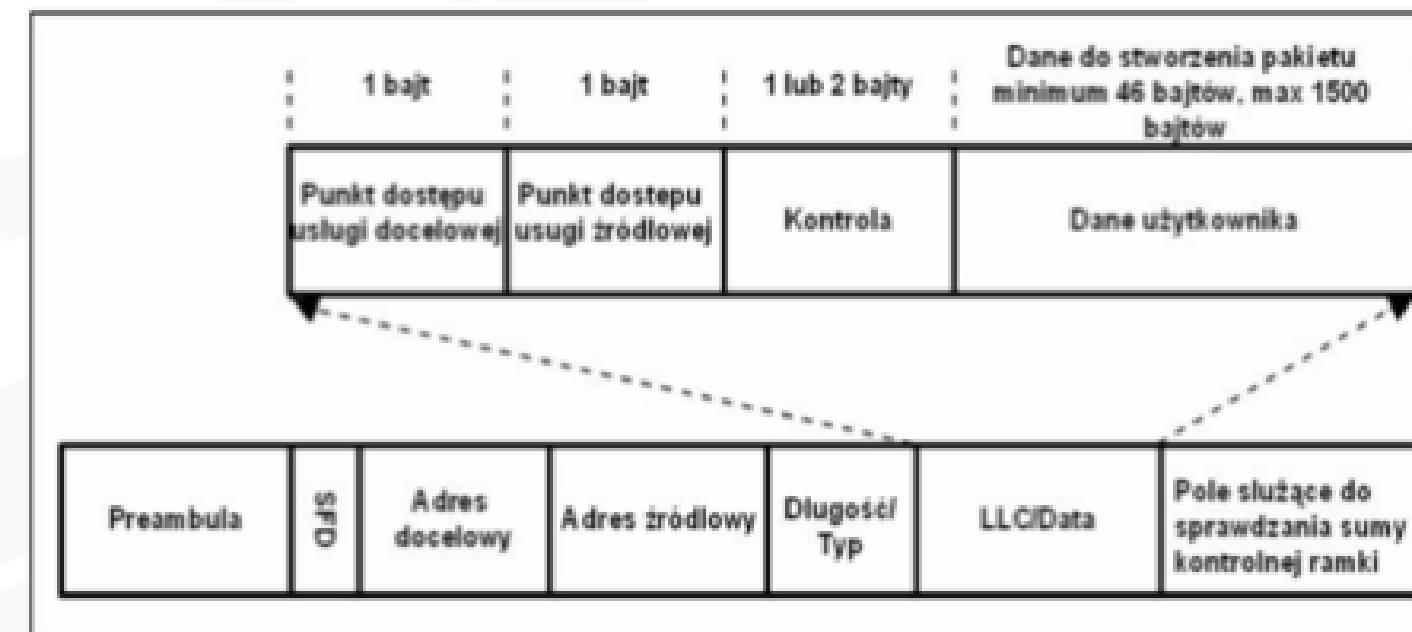
.VID (VLAN ID). Numer identyfikujący VLAN zgodnie z IEEE 802.1Q. **Numery VLAN'ów mogą przyjmować wartości od 1 do 4094.** Wartość 0 oznacza ramkę priorytetową, wartość 4095 jest zarezerwowana. W standardzie DIX pole to oznaczało typ protokołu warstwy wyższej, natomiast w pierwszej wersji standardu IEEE długość ramki. W celu zapewnienia jednoznacznej interpretacji tego pola, w kolejnym wydaniu standardu IEEE wprowadzono interpretację kontekstową. Jeżeli wartość pola jest mniejsza niż 1536 (0x0600), to wartość określa długość ramki, a identyfikację protokołu warstwy wyższej zapewnia warstwa LLC. W przeciwnym wypadku wartość pola należy interpretować jako numer protokołu warstwy wyższej. Maksymalny rozmiar pola danych wynosi 1500 oktetów, co stanowi wartość maksymalnej jednostki transmisji (MTU – Maximum Transmision Unit) dla sieci Ethernet. Jeżeli całkowita długość ramki jest mniejsza niż 64 oktety, to zawartość pola danych uzupełniana jest dodatkowymi oktetami aż do osiągnięcia przez ramkę minimalnej długości.

.TPID – zajmuje miejsce przeznaczone w podstawowym standardzie dla pola typ/długość i jego wartość ustawiona jest na 0x8100, co jednoznacznie identyfikuje typ ramki jako IEEE 802.1Q/802.1P. Priority – trzy pierwsze bity pola TCI pozwalają na zdefiniowanie 8 poziomowego priorytetu zgodnie z IEEE 802.1P.

LLC

- Warstwa LLC służy do przenoszenia informacji dotyczącej typu ramki. Sytuacja taka występuje wtedy, gdy pole typ/długość zawiera długość ramki, albo gdy do budowy sieci LAN wykorzystano inny protokół niż Ethernet.
- Dane warstwy LLC zgodnie z IEEE 802.2 zajmują kilka pierwszych bitów pola danych. DSAP (Destination Service Access Point) – identyfikuje protokół warstwy wyższej SSAP (Source Service Access Point) Dane kontrolne

LLC



Protokół MAC

- Drugim niezwykle istotnym elementem systemu LAN są zasady dostępu do medium. Określają one reguły działania urządzeń nadawczych podczas transmisji sygnałów.
- Wyróżniamy dwa podstawowe rodzaje protokołów **deterministyczne** i **niedeterministyczne**.

Protokoły deterministyczne

- Typowymi protokołami deterministycznymi stosowanymi w sieciach LAN są rozwiązania obecne w systemach Token Ring oraz FDDI.
- Komputery w tych systemach połączone są za pomocą topologii pierścienia, w którym krąży znaczek (token), przekazywany między komputerami. Komputer, będący w posiadaniu znacznika, może nadawać przez określony czas, po czym przekazuje znaczek następnemu komputerowi. Dzięki temu w sieci nie występują kolizje, gdyż w danym momencie tylko jeden komputer wysyła dane do sieci.

Protokoły niedeterministyczne

.System Ethernet dla odmiany jest systemem niedeterministycznym.

- Obowiązuje tu **zasada rywalizacji o dostęp do medium**. W takim środowisku zjawiskiem normalnym **są częste kolizje** wynikające stąd, że w danym momencie dwa lub więcej urządzeń, współdzielących medium, może rozpoczęć transmisję danych.
- W związku z tym, **wprowadzono mechanizm umożliwiający rozwiązywanie sytuacji kolizyjnych w postaci protokołu CSMA/CD** (Carrier Sense Multiple Access with Collision Detection).
- Protokół CSMA/CD opiera się na **trzech prostych mechanizmach: wykrywania kanału, rozpoznawania kolizji, wyznaczania czasu po którym nastąpi próba retransmisji**.

Minimalna długość ramki

- . Mechanizm wykrywania kolizji w protokole CSMA/CD zakłada, że wszystkie urządzenia sieciowe zostaną poinformowane o wystąpieniu kolizji.
- . Przyjmując skrajny przypadek, w którym kolizja wystąpiła na jednym krańcu sieci, to stacja nadawcza, znajdująca się na drugim krańcu otrzyma informację o kolizji z pewnym opóźnieniem, równym czasowi propagacji sygnału w medium o długości dwukrotnie większej niż maksymalny rozmiar sieci.
- . Do celów projektowych przyjęto z pewną nadwyżką czas propagacji sygnału przez całą sieć na poziomie 25,6us.
- . W związku z tym stacja nadająca otrzyma sygnał o wystąpieniu kolizji nie później niż 51,2us. Ponieważ projekt dotyczył sieci o szybkości 10Mbps, oznacza to że sygnał o wystąpieniu kolizji powinien dotrzeć do nadawcy nie później niż podczas wysyłania maksimum pierwszych 512 bitów (64 oktety).
- . Zatem jeżeli nadawca wyśle pierwsze 64 oktety ramki i nie otrzyma sygnału kolizji kontynuuje wysyłanie pozostałej części ramki. Jeżeli długość ramki byłaby mniejsza niż 64 oktety nadawca nie mógłby wiedzieć, czy transmisja zakończona została sukcesem, czy nie.
- . Dlatego przyjęto, że minimalnym rozmiarem ramki gwarantującym pewność poprawności transmisji jest rozmiar równy **64 oktetom**.

Przerwa międzyramkowa

| Szybkość | Przerwa międzyramkowa | Wymagany czas |
|----------|-----------------------|-------------------|
| 10 Mbps | 96 bit-times | 9.6 micro sec. |
| 100 Mbps | 96 bit-times | 0.96 micro sec. |
| 1 Gbps | 96 bit-times | 0.096 micro sec. |
| 10 Gbps | 96 bit-times | 0.0096 micro sec. |

Czas transmisji 1 bitu

| Szybkość sieci Ethernet | Czas transmisji 1 bitu |
|-------------------------|------------------------|
| 10 Mbps | 100 ns |
| 100 Mbps | 10 ns |
| 1000 Mbps = 1 Gbps | 1 ns |
| 10,000 Mbps = 10 Gbps | .1ns |

Parametry szczeliny czasowej

• Wersje technologii Ethernet pracujące z **szbkością 10 Mb/s i wolniejsze są asynchroniczne.**

Asynchroniczność oznacza, że każda **stacja odbierająca wykorzystuje osiem oktetów informacji taktowania do zsynchronizowania obwodu odbiorczego dla nadchodzących danych, po czym odrzuca je.**

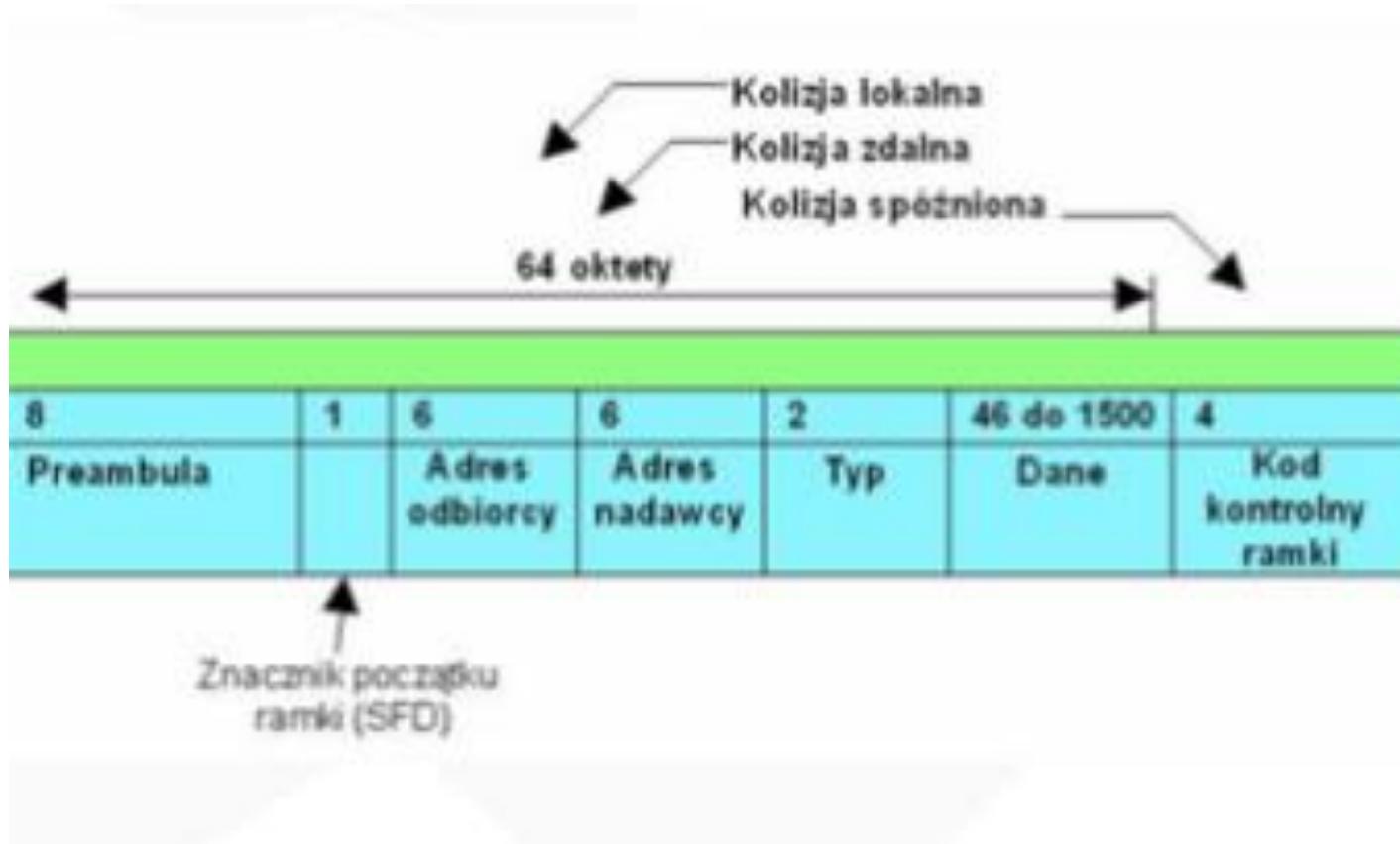
• Implementacje technologii Ethernet pracujące z **szbkością 100 Mb/s i szybsze są synchroniczne.** Synchroniczność oznacza, że **informacja taktowania nie jest wymagana, lecz dla utrzymania zgodności pole preambuły i znacznik początku ramki (SFD) są obecne.**

Szczelina czasowa

- We wszystkich odmianach technologii Ethernet o szybkości transmisji nieprzekraczającej 1000 Mb/s standard wyznacza minimalny czas pojedynczej transmisji nie krótszy niż szczelina czasowa.

| Szybkość | Szczelina czasowa | Odstęp czasu |
|----------|-------------------|------------------|
| 10 Mbps | 512 bit-times | 512 micro sec. |
| 100 Mbps | 512 bit-times | 5.12 micro sec. |
| 1 Gbps | 4096 bit-times | 4.096 micro sec. |
| 10 Gbps | nie dotyczy | nie dotyczy |

Błędy transmisji



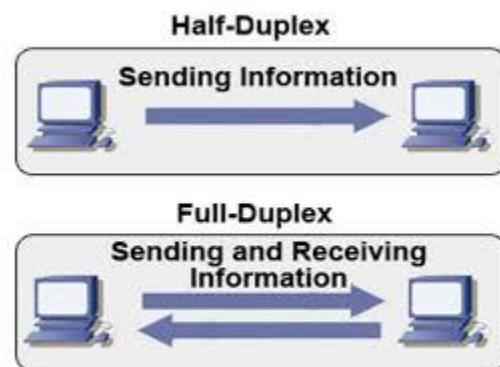
Błędy transmisji

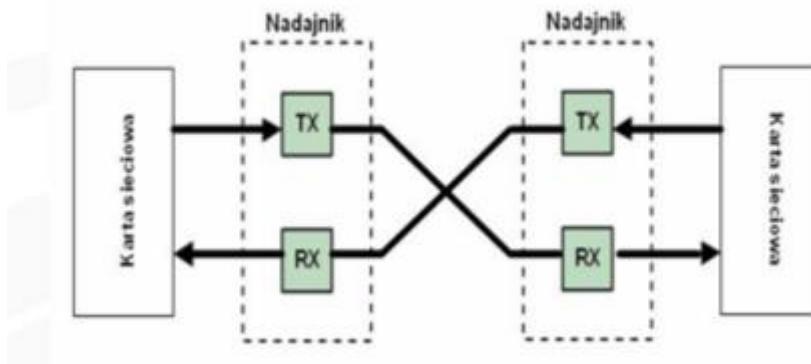
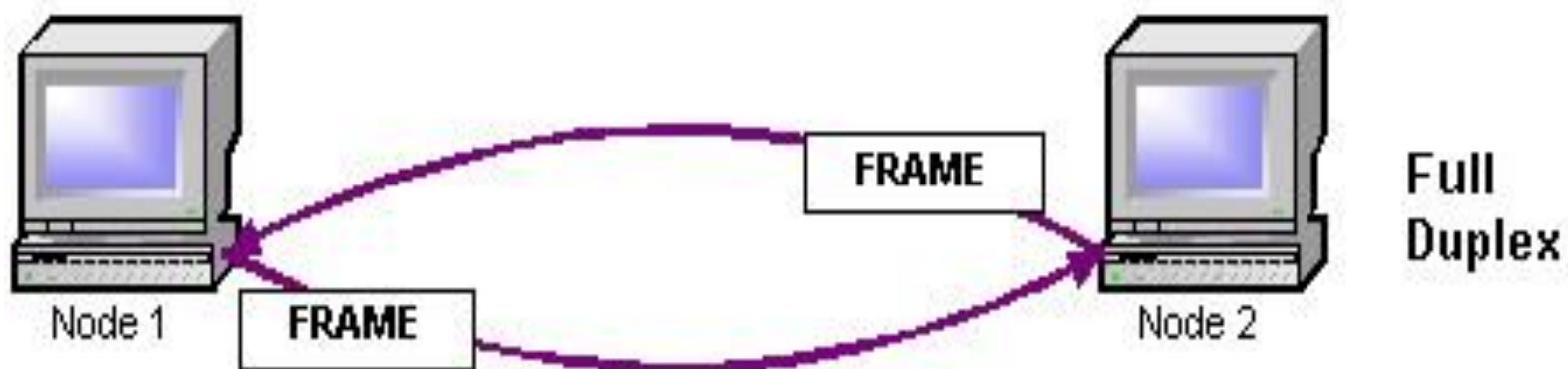
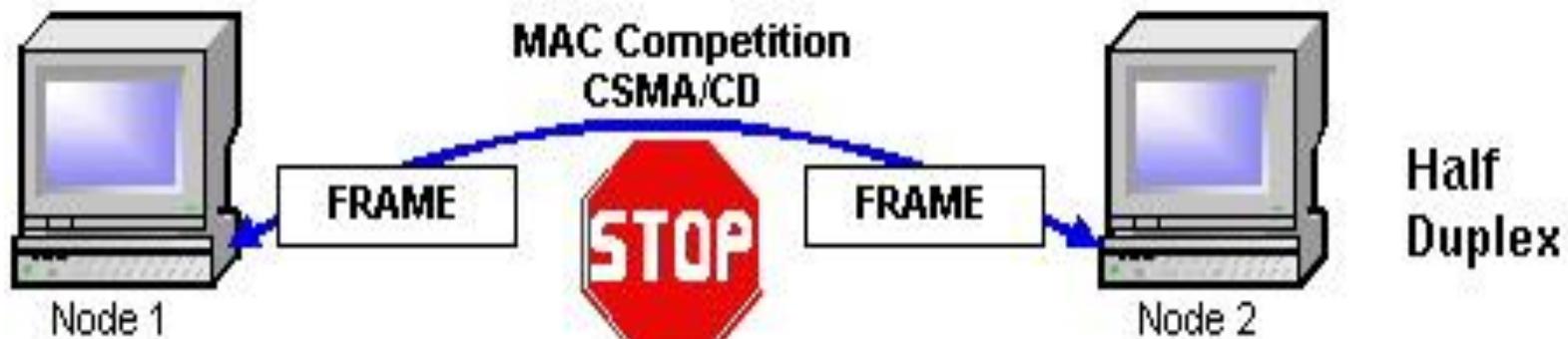
. Podczas transmisji danych w sieci mogą zdarzyć się różnego rodzaju sytuacje, które nie zostały przewidziane w standardzie. Tego typu przypadki traktowane są jako błędy transmisji. Należą do nich:

- Kolizja lub runt – jednoczesna transmisja więcej niż jednego urządzenia przed upływem szczeliny czasowej
- Późna kolizja – jednoczesna transmisja więcej niż jednego urządzenia po upływie szczeliny czasowej
- Jabber, długa ramka, błędy zakresu – niedopuszczalnie długa transmisja
- Krótka ramka, fragment kolizji lub runt – niedopuszczalnie krótka transmisja
- Błąd FCS – uszkodzona ramka
- Błąd wyrównania – zbyt duża albo zbyt mała liczba wysyłanych bitów
- Błąd zakresu – liczba otrzymanych bitów różna od liczby zadeklarowanej
- Ghost lub jabber – niedopuszczalnie długa preambuła lub zakłócenie.

Half-/Full Duplex

- Half Duplex – tryb pracy, w którym urządzenie w danej chwili może tylko wysyłać lub odbierać dane.
- Full Duplex – urządzenie może zarówno wysyłać jak i odbierać dane w tym samym czasie.

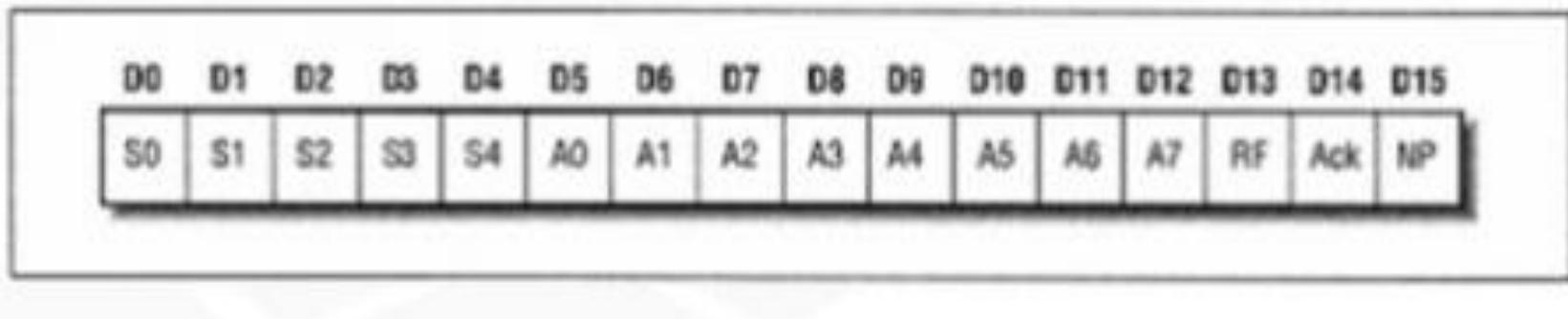




Auto negocjacja

- Procedura Ethernetu pozwalająca dwóm urządzeniom w sieci wybrać wspólne parametry pracy:
 - Prędkość
 - Full/Half-Duplex
- Działa w warstwie 1 modelu OSI

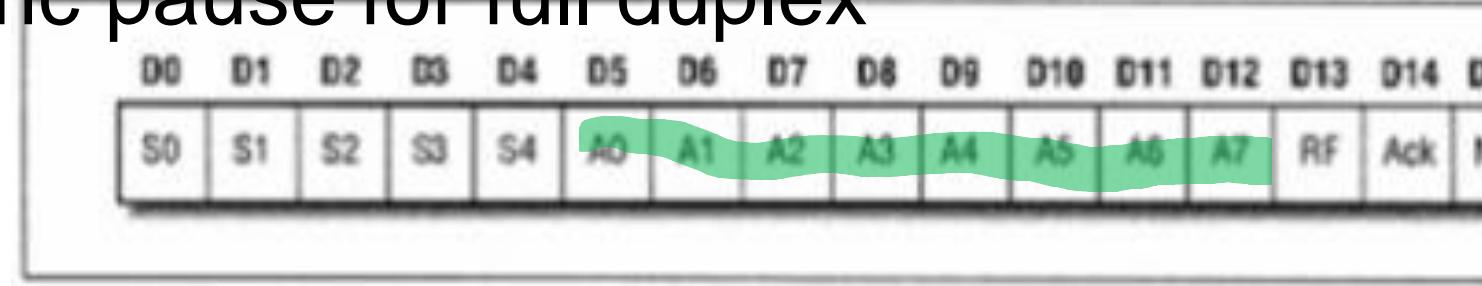
FLP (Fast Link Pulse)



- .D0 – D4 – identyfikator technologii LAN
- .D5 – D12 – identyfikator technologii sieciowych
- .D13 – wskaźnik błędu
- .D14 – bity potwierdzenia odbioru wiadomości
- .D15 – Sygnalizator kontynuacji w następnej wiadomości

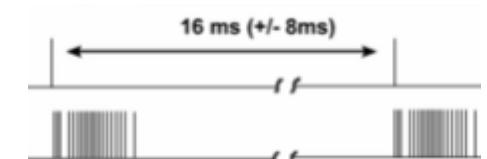
FLP – identyfikatory technologii

- A0: device supports 10BASE-T
- A1: device supports 10BASE-T in full duplex
- A2: device supports 100BASE-TX
- A3: device supports 100BASE-TX in full duplex
- A4: device supports 100BASE-T4
- A5: pause
- A6: asymmetric pause for full duplex
- A7: reserved



NLP

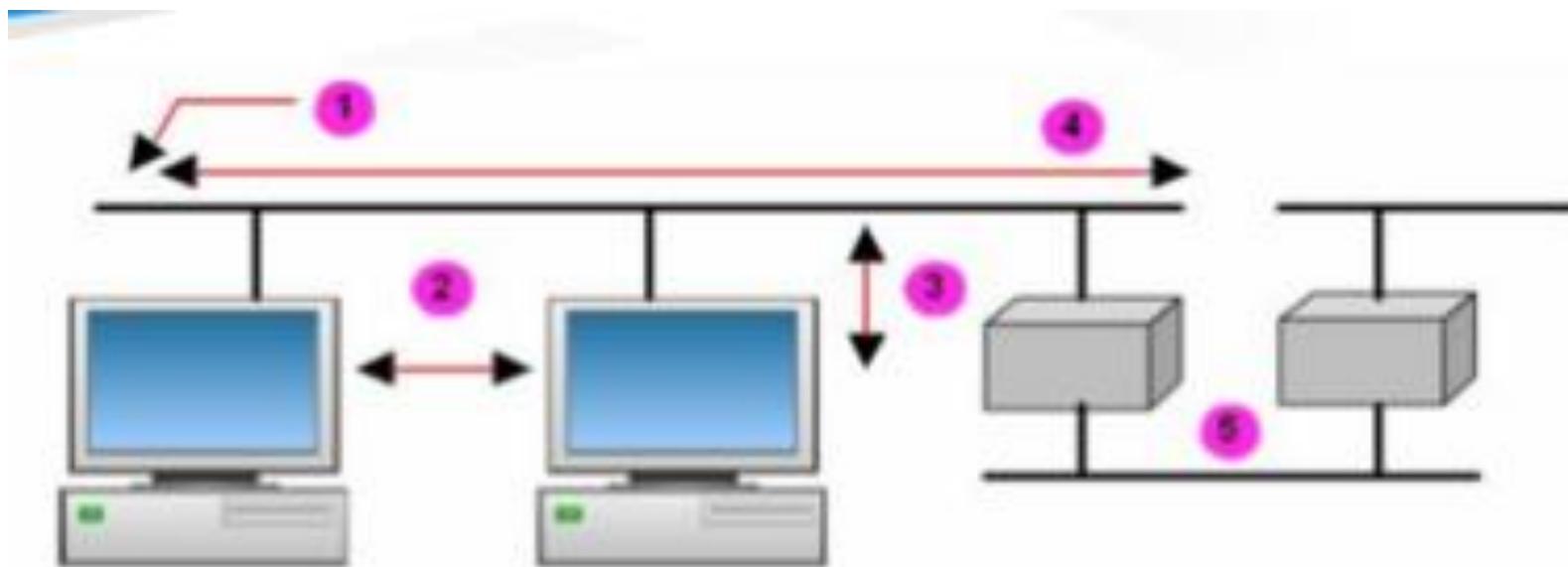
- .Sygnalizacji NLP (Normal Link Pulse) używanej w standardzie 10BASE-T do sprawdzania integralności łącza.
- .Standard 10BASE-T wymaga, aby każde urządzenie wysyłało co ok. 16ms ciąg impulsów.
- .Protokół auto-negocjacji NLP/FLP zaadoptował ten mechanizm do ogłaszanego pełnej funkcjonalności danego interfejsu.
- .W tym celu wysyłane jest tyle 16-bitowych wiadomości ile potrzeba do opisania możliwości interfejsu.



Historia standardu ETHERNET

- Pierwotna specyfikacja systemu Ethernet przewidyszała łączenie komputerów do współdzielonego medium, którym był kabel koncentryczny.
- Zgodnie z zasadami budowy segmentu sieci w oparciu o ten typ kabla: Oba końce kabla powinny być zakończone terminatorami o oporności 50ohm,
- Minimalna odległość między punktami przyłączenia urządzeń wynosi 0.5m
- Każda stacja powinna być bezpośrednio podłączona do trójnika BNC,
- Maksymalna długość segmentu wynosi 185m.

- Standard przewidywał rozbudowę sieci lokalnej w systemie Ethernet poprzez łączenie segmentów pod następującymi warunkami:
- Łączenie segmentów dokonuje się przy pomocy wzmacniaczy dwustronnych, tzw. repeater'ów
- Maksymalna liczba repeater'ów między dowolnymi dwoma stacjami w sieci wynosi 4
- Do segmentów parzystych mogą być podłączone jedynie dwa urządzenia, którymi są repeater'y.

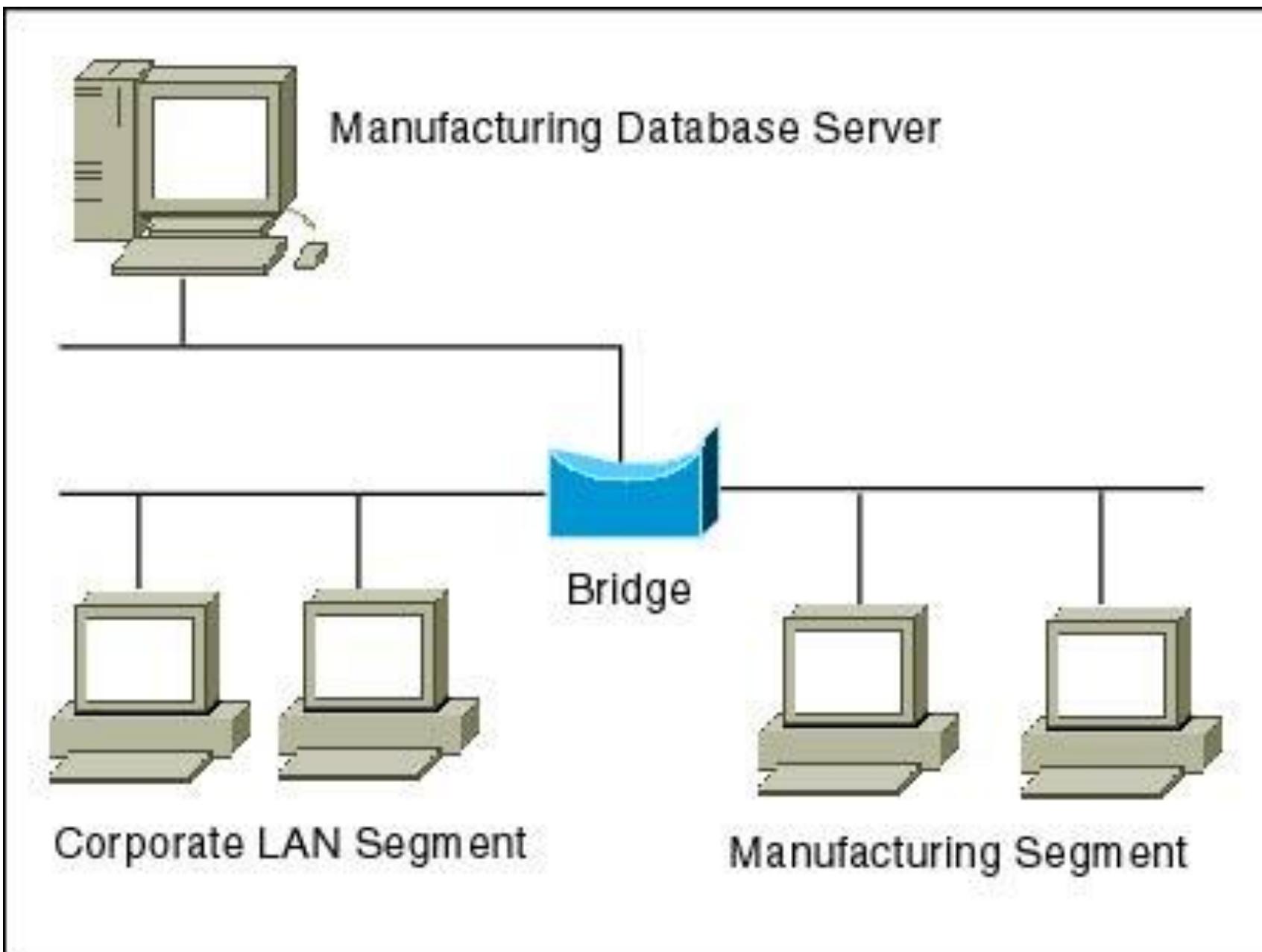


1. Oba końce kabla koncentrycznego powinny być zakończone terminatorem o impedancji falowej 50 ohmów.
2. Minimalna odległość między punktami wpiecia urządzeń do kabla wynosi 0,5 metra.
3. Każda stacja musi być bezpośrednio połączona z trójkątem BNC wpisującym do kabla koncentrycznego.
4. Maksymalna długość segmentu wynosi 185 metrów.
5. Do segmentów sieci pomiędzy wtermikami mogą być dołączone tylko 2 urządzenia, którymi są te wtermiki.

- Wraz z opracowaniem standardu umożliwiającego wykorzystanie skrętki czteroparowej pojawiły się koncentratory (repeater'y wieloportowe), umożliwiające podłączanie do sieci urządzeń w topologii gwiazdy.
- Zasady łączenia tego typu segmentów w celu rozbudowy sieci ograniczają się jedynie do ograniczenia liczby koncentratorów do 4 między dwoma dowolnymi urządzeniami.
- Maksymalna długość kabla łączącego urządzenie z koncentratorem wynosi 100m.
- W przypadku sieci pracujących z szybkością 100Mb (FastEthernet) standard dopuszcza jedynie dwa koncentratory oraz ogranicza maksymalną długość połączeń między dwoma dowolnymi stacjami do 205m.

- Stosowane dotychczas urządzenia pracowały w warstwie 1 modelu ISO/OSI i poza regeneracją sygnałów nie wnosiły żadnych innych funkcjonalności do budowy sieci.
- Dalsza rozbudowa sieci przy pomocy koncentratorów i wzmacniaczy oznaczałaby przekroczenie maksymalnej wartości opóźnienia w sieci, co spowodowałoby wadliwe działanie protokołu CSMA/CD.
- Wraz z rozwojem technologii, do sieci podłączano coraz większą liczbę urządzeń, co doprowadzało nawet poprawnie skonstruowane sieci do załamania komunikacji z powodu nadmiernego wzrostu kolizji.
- Segment sieci, w którym wszystkie połączenia zostały zrealizowane za pomocą urządzeń biernych i aktywnych warstwy 1 modelu ISO/OSI nazwano domeną kolizyjną.

- W celu umożliwienia dalszej rozbudowy oraz podniesienia wydajności sieci lokalnej opracowano urządzenie o nazwie most (ang. Bridge), wyposażone w dodatkową funkcjonalność w stosunku do zwykłych regeneratorów sygnałów.
- Funkcjonalność ta polega na umiejętności rozpoznawania urządzeń pod kątem przynależności do domen kolizyjnych bezpośrednio podłączonych do mostu.
- Most tworzy i przechowuje tablicę pozwalającą skojarzyć MAC adres urządzenia z odpowiednim portem mostu.
- Ponieważ most przetwarza ramki Ethernet zaliczany jest do urządzeń aktywnych warstwy 2 modelu ISO/OSI.



Urządzenia wykorzystywane obecnie

- Mosty
- Routery
- Switche

- Tryb pracy przełączników możemy podzielić ze względu na sposób w jaki przełącznik podejmuje decyzję o przekierowaniu ramki na dany port.
 - Cat-through
 - Store-and-forward
 - Fragment-free
 - Hybrid

Cut-through

- Przełączaniem symetrycznym (wszystkie porty przełącznika pracują z tą samą szybkością) stosowany jest tryb cat-through.
- Tryb ten polega na podejmowaniu decyzji o przekierowaniu ramki na podstawie adresu docelowego, znajdującego się w pierwszych 6 oktetach ramki Ethernet.

Store-and-forward

- Drugi sposób stosowany bywa zazwyczaj w trybie przełączania niesymetrycznego (porty przełącznika pracują z różnymi szybkościami, co głównie występuje w przełącznikach z portami 10/100/1000Mb) i określany jest jako stor-and-forward.
- Jak sama nazwa wskazuje decyzja o przekierowaniu ramki podejmowana jest dopiero wtedy, gdy przełącznik otrzyma całą ramkę i ewentualnie sprawdzi jej poprawność na podstawie pola FCS.

Fragment-free

• W przypadku gdy do portów przełącznika podłączone są segmenty sieci w postaci domen kolizyjnych, niezależnie od sposobu przełączania stosowany bywa pośredni tryb fragment-free, w którym decyzja o przekierowaniu ramki podejmowana jest po otrzymaniu przez przełącznik pierwszych 64oktetów ramki, co pozwala upewnić się, że podczas transmisji ramki nie doszło do kolizji.

Hybrid

- W niektórych przełącznikach stosowana jest czwarta metoda, hybrydowa.
- Jeżeli poziom błędów w sieci nie przekracza pewnej wartości (ok. 10%), przełącznik stosuje tryb cat-through.
- Jeżeli poziom błędów wzrośnie ponad założoną wartość, to przełącznik przechodzi do trybu store-and-forward.

Redundancja

- .Jednym z istotnych aspektów pracy sieci jest jej niezawodność (stabilność, dostępność).
- .W celu osiągnięcia możliwe wysokiego poziomu niezawodności stosuje się urządzenia o wysokim współczynniku bezawaryjności, najczęściej wyposażone w podwójne układy zasilające oraz **redundantny system połączeń sieciowych** umożliwiających zachowanie komunikacji w sieci pomimo awarii części urządzeń.

Protokół STP

- Obecnie jedyną techniką umożliwiającą konfigurację połączeń redundantnych kontrolowanych automatycznie przez same urządzenia jest zastosowanie protokołu STP (Spanning Tree Protocol).
- Działanie tego protokołu polega na wzajemnym informowaniu się urządzeń o bieżącym stanie połączeń za pomocą komunikatów BPDU (Bridge Protocol Data Units).
- W wyniku wymiany informacji nt. konfiguracji połączeń każdy port przełącznika może

Protokół STP

- Blocking
 - Listening
 - Learning
 - Forwarding
 - Disabled
- From initialization to blocking
 - From blocking to listening or to disabled
 - From listening to learning or to disabled
 - From learning to forwarding or to disabled
 - From forwarding to disabled

Koniec



Routing

Protokół trasowania

- Protokół trasowania (routing, routujący, ang. routing protocol) – używany jest do wymiany informacji o trasach pomiędzy sieciami komputerowymi, co pozwala na dynamiczną budowę tablic trasowania.
- Tradycyjne trasowanie jest bardzo proste, bo polega na wykorzystaniu tylko informacji o następnym "przeskoku" (ang. hop).
- W tym przypadku router kieruje pakiet do następnego routera, bez uwzględnienia na przykład zbyt wielkiego obciążenia czy awarii na dalszej części trasy.

Metryka trasowania

- Metryka trasowania jest wartością używaną 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.

Sieć typu Ad-Hoc

- bezprzewodowa sieć o zdecentralizowanej strukturze, w której przyłączone mobilne urządzenia mogą pełnić funkcje zarówno klienta (terminala końcowego), jak i punktu dostępu.
- Do przekazywania danych nie jest wymagane istnienie żadnej infrastruktury sieciowej (brak punktów zarządzających), gdyż komunikacja między poszczególnymi jednostkami podsieci następuje w sposób bezpośredni: pakiety dostarczane są do odbiorcy bez potrzeby istnienia dodatkowych węzłów kierujących ruchem.
- Do zabezpieczenia sieci przed osobami niepożądanymi oraz do ustanowienia komunikacji tylko pomiędzy wybranymi stacjami używany jest identyfikator domeny (Wireless Domain ID). Każda maszyna przynależąca do danej podsieci ma ustawiony ten sam identyfikator.
- Maksymalna odległość między poszczególnymi stacjami wynosi od 30 m do 60m.

Zastosowania sieci AD-Hoc

- .komercyjne rozwiązania w małych, przenośnych urządzeniach takich jak:
- .telefony komórkowe z modułem Bluetooth i GPRS (w przyszłości UMTS)
- .komputery PDA
- .PSP
- .aparaty cyfrowe
- .publiczne terminale dostępowe bazujące na standardzie WLAN IEEE 802.11
- .medyczne, mobilne urządzenia pomiarowe
- .sieci o małym zasięgu PAN (Personal Area Network)
- .wojskowe techniki łączności

Protokoły trasowania w sieciach ad-hoc

- proaktywne:

- OLSR

- reaktywne:

- AODV

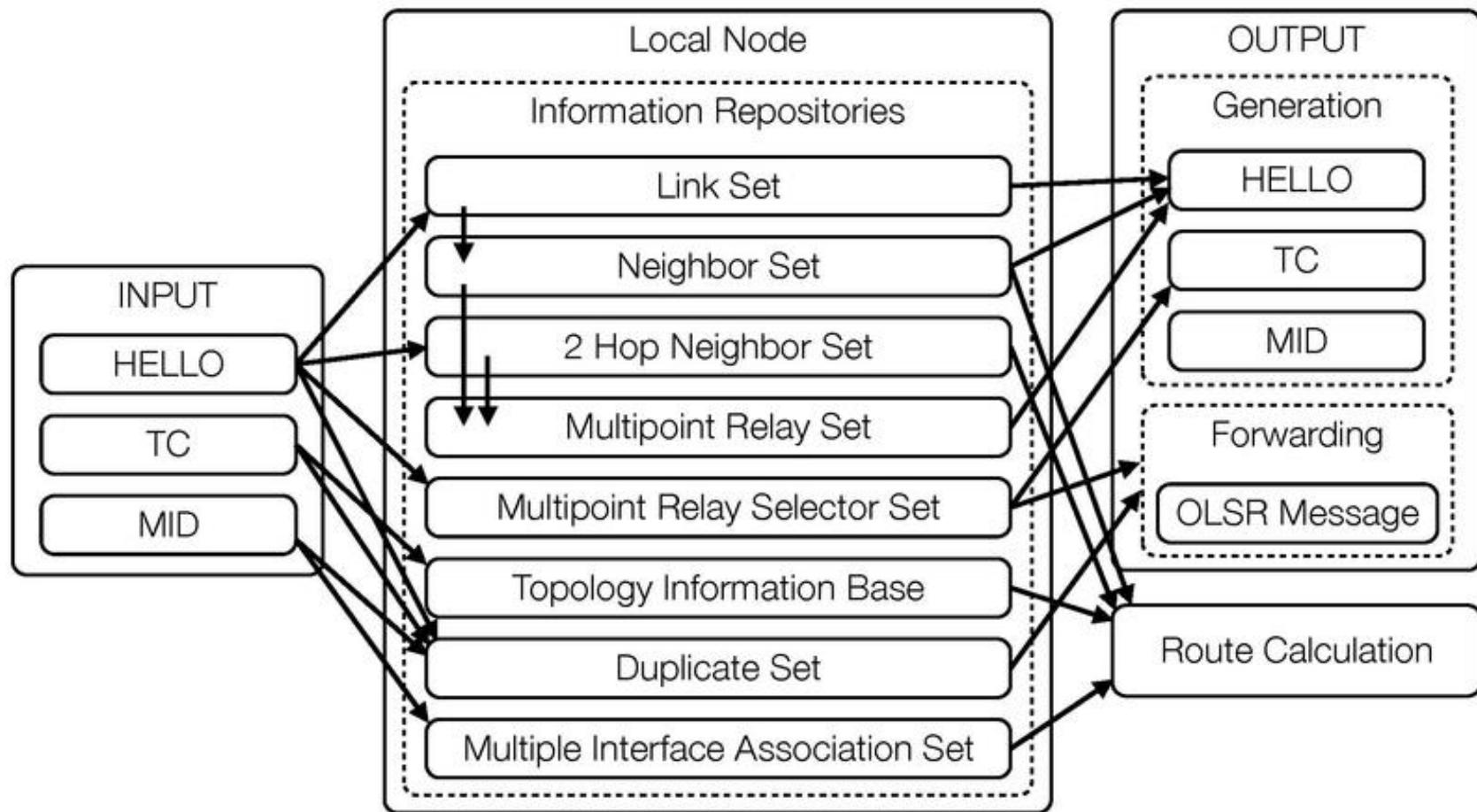
- DYMO

- DSR

OLSR

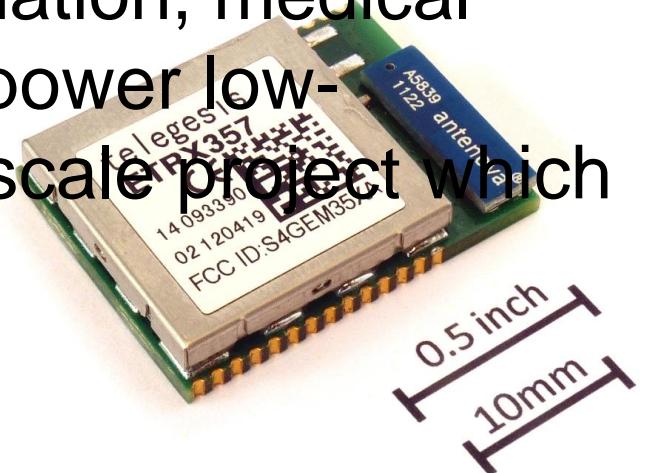
- Optimized Link State Routing Protocol (OLSR) jest protokołem routowania IP zoptymalizowanym do pracy w sieciach ad-hoc.
- Tworzy proaktywną tablicę routingu wykorzystując hello and topology control (TC)
- Na podstawie tych informacji każdy element sieci określa następny przeskok (next hop) tak by wykorzystać najkrótszą drogę.

OLSR



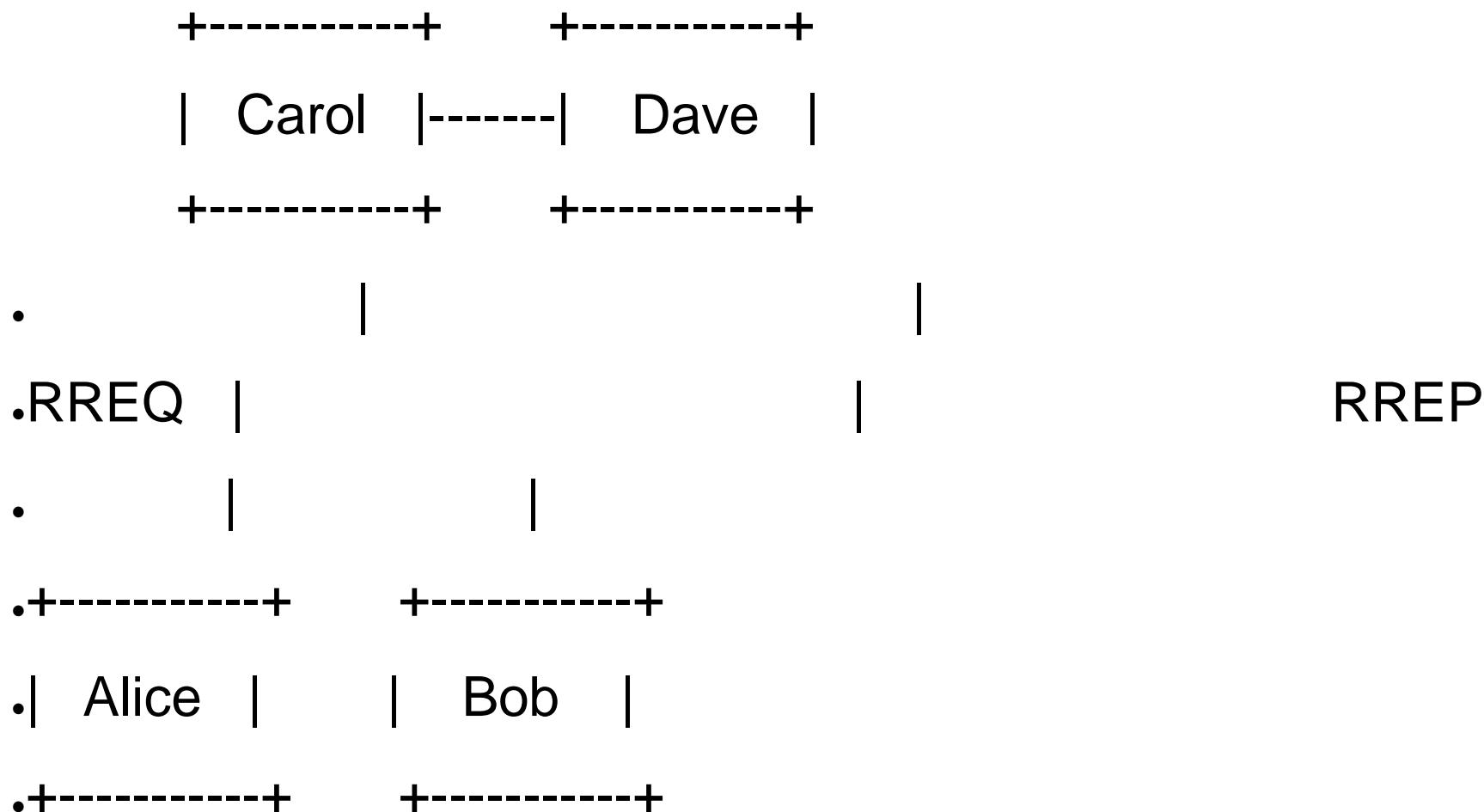
AODV

- Ad hoc On-Demand Distance Vector (AODV) Routing
- July 2003 in Nokia Research Center, University of California, Santa Barbara and University of Cincinnati
- ZigBee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection.



DYMO

- DYMO routing protocol jest następcą AODV Routing protocol
- DYMO może działać jako protokół proaktywny jak i reaktywny np:



DSR

- Dynamic Source Routing
- Używa tablic routingu do źródła a nie informacji z każdego urządzenia po drodze.

Wewnętrzne protokoły trasowania

.IGP, (ang. Interior Gateway Protocol) – używane do wymiany informacji o trasach w pojedynczym systemie autonomicznym.

- IGRP/EIGRP (Interior Gateway Routing Protocol / Enhanced IGRP)
- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- IS-IS (Intermediate System to Intermediate System)

IGRP/EIGRP

Whereas RIP uses the metric of hops, IGRP uses the following metrics:

- **Internetwork Delay** - this represents the delay on the medium in units of 10 microseconds e.g. for Ethernet this value is 100 microseconds i.e. 1ms, so the value of Delay is $100/10 = 10$.
- **Bandwidth (Bw)** - this represents the speed of the link where the speed can range from 1200bps to 10Gbps. The value used is actually the inverse of the Bandwidth (in Kb/s) multiplied by 10^7 e.g. for a 64Kb/s link the value of Bw is $10^7/64 = 156250$.
- **Reliability** - fractions of 255 where 255 means totally reliable.
- **Administrative Distance** - can take a value between 1 and 255 and creates a **Load** or weighting on that particular link, the higher the number the less attractive the link is.

The formula used to calculate the metric is $[K_1 * Bw + K_2 * Bw/(256-Load) + K_3 * Delay] * [K_5 / (Reliability + K_4)]$. Be aware that the MTU is NOT used in the calculation of the metric, however the MTU is tracked through the path to find the smallest MTU.

| Media | Bandwidth (Kb/s) | Bw | Delay (uS) | Delay |
|---------------------|-------------------------|-----------|-------------------|--------------|
| ATM 155Mb/s | 155000 | 65 | 100 | 10 |
| Fast Ethernet | 100000 | 100 | 100 | 10 |
| FDDI | 100000 | 100 | 100 | 10 |
| HSSI | 45045 | 222 | 20000 | 2000 |
| Token Ring (16Mb/s) | 16000 | 625 | 630 | 63 |
| Ethernet | 10000 | 1000 | 1000 | 100 |
| T1 | 1544 | 6476 | 20000 | 2000 |
| E1 | 2048 | 5000 | 20000 | 2000 |
| DS0 | 64 | 156250 | 20000 | 2000 |
| 56Kb/s | 56 | 178571 | 20000 | 2000 |
| Tunnel | 9 | 1111111 | 500000 | 50000 |

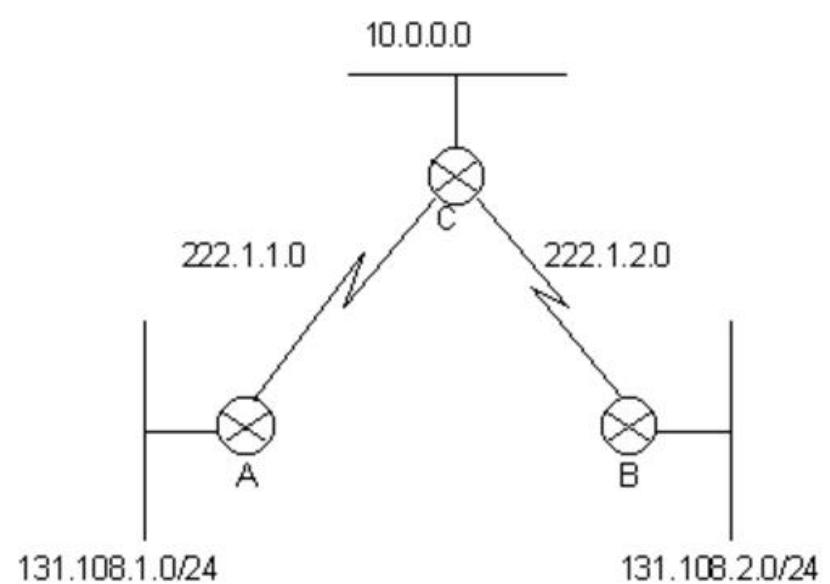
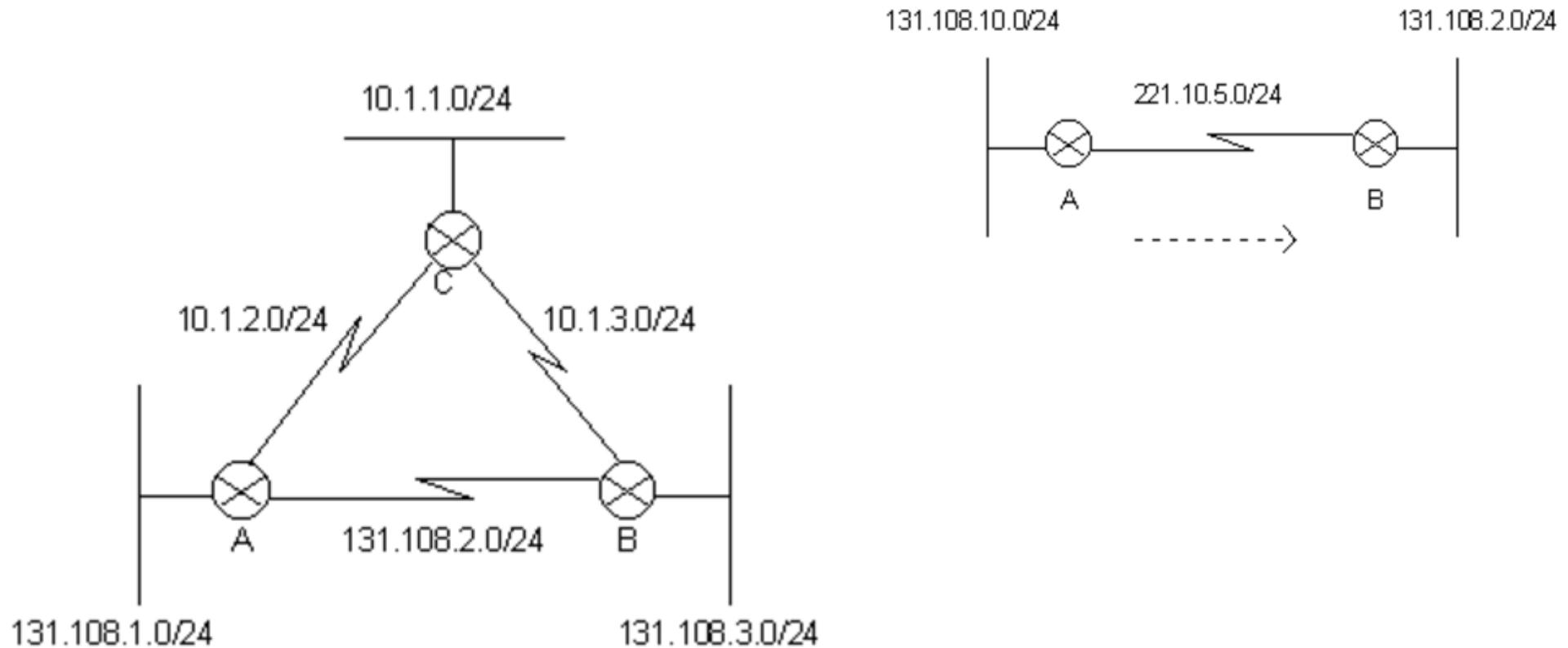
IGRP Packet Format

| Bits | 4 | 4 | 8 | 16 | 16 | 16 | 16 | Variable | |
|------|-------------|--------|-----------|-----------|------------------------|----------------------|------------------------|--------------|---------------|
| | Version | Opcode | Edition | AS Number | No. of interior routes | No. of system routes | No. of exterior routes | Checksum | Route entries |
| Bits | 24 | 24 | 24 | 16 | 8 | 8 | 8 | other routes | |
| | Destination | Delay | Bandwidth | MTU | Reliability | Load | Hop Count | | |

RIP

.RIP was originally developed by Xerox and was called Gateway Info (GWInfo) it then developed into Routed which you will within the Unix environment. RIP v1 is described in RFC 1058.

.In a RIP v1 environment all subnet masks throughout the network must be the same therefore limiting addressing schemes somewhat. This is because RIP v1 is a Classful routing protocol, it does not have the ability to transmit the subnet mask within its updates. RIP v1 imposes the subnet mask on the inbound interface and this is normally defined by the engineer. Learned routes are entered into the routing table with their natural mask. As a result there can be a great waste of internet host addresses. This can be rectified by using RIP v2 (see later) or OSPF which are able to implement Variable Length Subnet Masks (VLSM). They can do this because they can transmit the subnet mask within their routing updates and these protocols are known as Classless routing protocols.



• RIP v1 uses UDP port 520 for sending and receiving broadcast messages.

| Bytes | 1 | 1 | 2 | 2 | 2 | 4 | 4 | 4 | 4 |
|-------|---------|---------|--------|---------------------------|--------|------------|--------|--------|--------|
| | Command | Version | Unused | Address Family Identifier | Unused | IP Address | Unused | Unused | Metric |

RIP v1

;

• Request

• Response

• Traceon (no longer used)

• Traceoff (no longer used)

• Reserved (used by Sun Microsystems)

IPv2

- The latest RFC for RIP v2 is RFC 1723 and replaces RFC 1388.
- The following features are additional to those found within RIP v1:
 - Authentication: A simple password of up to 128 characters can be used to verify legal IP datagrams between RIP v2 configured router interfaces.
 - Route Tags
 - Subnet Mask: Each network entry within the RIP update has its subnet mask included so accurate routing information can be included within the routing tables and a RIP v2 router advertises all known subnetworks out an interface not belonging to that subnetwork.
 - Multicasting: RIP v2 updates are multicast to 224.0.0.9 (class D) so RIP v2 routers share information independently from other routers.

| Bytes | 1 | 1 | 2 | 2 | 2 | 4 | 4 | 4 | |
|-------|---------|---------|--------|---------------------------|-----------|------------|-------------|----------|--------|
| | Command | Version | Unused | Address Family Identifier | Route Tag | IP Address | Subnet Mask | Next Hop | Metric |

RIP v2

OSPF

- .Open Shortest Path First (OSPF) routing protocol is a Link State protocol based on cost rather than hops or ticks (i.e. it is not a vector based routing protocol).
- .As with RIPv2 different sized subnet masks can be used within the same network thereby allowing more efficient utilisation of available address space.
- .OSPF supports unnumbered point to point links and equal cost multipath (or load balancing for up to 6 paths; meaning balancing the distribution of IP datagrams down parallel routes to the same destination router using a round robin or a direct addressing option).

.The Link State Database (LSDB) contains the link state advertisements sent around the 'Area' and each router holds an identical copy of this LSDB. The router then creates a Shortest Path First (SPF) tree using Dijkstra's algorithm on the LSDB and a routing table can be derived from the SPF tree which now contains the best route to each router.

.Within OSPF there can be Point-to-Point networks or Multi-Access networks. The Multi-Access networks could be one of the following:

- Broadcast Network: A single message can be sent to all routers
- Non-Broadcast Multi-Access (NBMA) Network: Has no broadcast ability, ISDN, ATM, Frame Relay and X.25 are examples of NBMA networks.
- Point to Multipoint Network: Used in group mode Frame Relay networks.

- .Point-to-Point and Point-to-Multipoint links do not require a Designated Router (DR) or a Backup Designated Router (BDR) because adjacencies have to form with each other anyway.
- .On a Point-to-Point and Point-to-Multipoint networks adjacencies are always formed between the two routers so there is no requirement for a DR or BDR,
- .whilst on a multi-access network a router will form an adjacency with the Designated Router (DR) and the Backup Designated Router (BDR).
- .In a broadcast or NBMA network it is not feasible for every router to form a full mesh of adjacencies with all the other routers. The Designated Router forms adjacencies with each of the other routers and performs the link-state information exchange thereby minimising the traffic load and making sure that the information is consistent across the network.

.The Retransmit Interval is the number of seconds between LSAs across an adjacency. The following settings are often recommended:

| | |
|-----------------------------|------------|
| Broadcast network | 5 seconds |
| Point-to-Point network | 10 seconds |
| NBMA network | 10 seconds |
| Point-to Multipoint network | 10 seconds |

- .The Hello Interval must be the same on each end of the adjacency otherwise the adjacency will not form.
- .In a Point-to-Point network this value is 10 seconds whereas in a Non Broadcast Multiaccess Network (NBMA) the Hello Interval is 30 seconds.
- .The Dead Interval is 40 seconds in a Point-to-Point network and 120 seconds in a Non Broadcast Multiaccess Network (NBMA).

.The Metric Cost

| Network Type | Cost |
|---------------------|-------------|
| FDDI/Fast Ethernet | 1 |
| Token Ring (16Mbps) | 6 |
| Ethernet | 10 |
| E1 | 48 |
| T1 | 64 |
| 64 kb/s | 1562 |
| 56 kb/s | 1785 |

- These costs are used to calculate the metric for a line and thus determine the best route for traffic. The lowest cost to a destination is calculated using Dijkstras Algorithm. The lowest cost link is used unless there are multiple equally low cost links in which case load balancing takes place between up to 6 route entries.
- RFC 2328 describes Dijkstras Algorithm (also called the Shortest Path First (SPF) algorithm.

Koniec

.Za tydzień bezpieczeństwo sieci.

Usługi i protokoły bezpieczeństwa

- Zabezpieczanie sieci
- Rodzaje ataków i exploity
- Ochrona systemów
- Metody szyfrowania
- System bezpieczeństwa sieciowego Kerberos

- Sieć jest atakowana na coraz bardziej wyrafinowane sposoby, które nieustannie są rozwijane.
- Wydaje się, że bieżące wiadomości zawsze mogą zawierać najnowszego wirusa, konia trojańskiego lub robaka, a w wiadomości e-mail z banku może znajdować się ostrzeżenie dla danego klienta, że ktoś przechwycił informacje związane z jego kartą kredytową.
- Jeżeli funkcjonowanie sieci wydaje się dziwne lub działa w niej jakiś system, to użytkownik jest usprawiedliwiony, kiedy zachowuje się jak paranoik.
- Żyjemy w niepewnych czasach, ale zawsze istnieje możliwość zniechęcenia potencjalnych atakujących przez lepsze zabezpieczenie sieci, a tym samym zmuszenie ich do poszukania łatwiejszego celu ataku.

- Nie ma jednej skutecznej metody ochrony sieci.
- Każdy system bezpieczeństwa może zostać złamany, jeżeli nie z zewnątrz, to z wewnętrz.
- Najlepszym sposobem zapewnienia bezpieczeństwa sieci jest stosowanie różnych warstw zabezpieczeń. W takim przypadku, zanim atakujący uzyska dostęp, będzie musiał pokonać co najmniej dwa systemy zabezpieczeń.
- Regularna zmiana parametrów bezpieczeństwa, na przykład haseł, oraz podział sieci na części to dwie kolejne metody, które są nieocenione.

Luki w zabezpieczeniach sieci

- Luki w zabezpieczeniach sieci to słabe punkty, które można wykorzystać w celu uzyskania dostępu do danego systemu.
- Przyczyny złamania zabezpieczeń mogą być różne:
 - stosowanie słabych haseł przez użytkowników,
 - wirusy i konie trojańskie,
 - błędy w oprogramowaniu,
 - pliki wykonywalne lub skrypty uruchomione w systemie, a także umieszczenie fragmentów kodu w systemie.
- Kiedy luka w zabezpieczeniach staje się znana, są tworzone programy, które ją wykorzystują. Programy takie określa się exploitami, rozpowszechniają się równie szybko jak wirusy.

- Każdy program zawiera jakieś błędy bądź procedury, które można złamać.
- Aktualizacje regularnie dostarczane przez firmy, na przykład infrastruktura Microsoft Update, mają za zadanie usuwać odkryte luki.
- Ujawnienie luki w systemie przed opracowaniem aktualizacji poprawiającej dany błąd naraża system na ataki z wykorzystaniem tej luki.
- Ataki tego rodzaju są nazywane Zero Day Exploit. Można w to wierzyć bądź nie, ale istnieją firmy dostarczające usługi subskrypcji, która informuje klientów o sposobie wykorzystania Zero Day

- Exploit do atakowania systemów. Oczywiście istnieją też inne firmy, które z kolei informują klientów, jak się bronić przed tego rodzaju atakami.
- Jesteśmy więc świadkami nieustannego wyścigu między atakującymi i atakowanymi.

- Najlepszym zaleceniem dotyczącym Zero Day Exploit jest stosowanie we wszystkich systemach uaktualnień tuż po ich wydaniu.
- Wielu administratorów wzdraga się przed traktowaniem tej sugestii jako przykładu najlepszego rozwiązania, ponieważ aktualizacje mogą wyeliminować pewne błędy, ale jednocześnie wprowadzić nowe.
- Automatyczne uaktualnianie systemów produkcyjnych wprowadza element niepewności, który by nie występował, gdyby oprogramowanie systemowe nie ulegało zmianom.

- Jedną z metod stosowanych do wykrywania luk w zabezpieczeniach sieci jest próbkowanie sieci za pomocą narzędzia analizy ryzyka — skanera luk w zabezpieczeniach.
- Tego rodzaju skanery działają w ten sposób, że skanują sieć dla wszystkich przypisanych adresów IP, określają otwarte porty, a następnie budują listę programów i systemów operacyjnych, które funkcjonują w różnych systemach.
- Skanerami tego typu są skanery portów, skanery sieciowe, skanery witryn internetowych oraz dedykowane narzędzia znajdujące się w platformach struktur przeznaczonych do zarządzania.
- Po zakończeniu badania początkowego skaner może zbudować mapę sieci albo utworzyć raport. Jeżeli skaner używa SNMP, WMI lub innego protokołu zarządzania, to ma możliwość sprawdzania systemów i aplikacji w celu określenia nie tylko ich rodzaju, ale także numerów wersji i poziomu aktualizacji.
- Mogą być stosowane oznaczenia poziomów zagrożenia oraz listy zaleceń i działań, które administratorzy powinni podjąć w celu dalszego zabezpieczenia sieci.

- Przemysłowy standard określania podatności systemu komputerowego na luki w zabezpieczeniach ma nazwę Common Vulnerability Scoring System (CVSS).
- Ocena bazuje na zestawie pomiarów i dotyczy podstawowych lub poważnych luk w zabezpieczeniach, wskazuje zagrożenia oraz uwzględnia czynniki związane z implementacją bądź środowiskiem.
- CVSS FIRST (ang. Forum of Incident Response and Security Teams),
 - Standard ten (obecnie w wersji 2.) został opracowany przez grupę CVSS Special Interest Group — SIG.
 - Do kalkulatora online dostarczanego przez bazę danych National Vulnerability Database w sekcji SVSS Scoring można wprowadzić różne dane w celu otrzymania określonych ocen

- Powszechnie dostępne są również inne narzędzia.
 - Jednym z przykładów jest Microsoft Baseline Security Analyzer. Narzędzie MBSA używa infrastruktury Microsoft Update oraz agenta lokalnego w celu określenia, czy system Windows jest bezpieczny i uaktualniony.
 - Według firmy Microsoft ta bazująca na internecie usługa przeprowadza tygodniowo sprawdzanie trzech milionów systemów pod kątem istnienia luk w zabezpieczeniach.
 - MBSA może skanować systemy nie tylko takie jak Windows 10, ale również Windows CE i Embedded, serwery Microsoft SQL Server oraz Microsoft Internet Information Server.

- Skanowanie pod kątem luk w zabezpieczeniach oraz rozpoznawanie sieci to techniki stosowane również przez **atakujących**, którzy próbują uzyskać dostęp do sieci, a także funkcje niektórych robaków.

Baza danych National Vulnerability Database

- CVE (ang. Common Vulnerabilities and Exposures) — słownik zagrożeń bezpieczeństwa obsługiwany przez MITRE Corporation dla wydziału National Cyber Security Division Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych.
- CVE używa systemu identyfikatorów, które unikalnie identyfikują znane zagrożenia. Czynniki zagrożenia są czasami określane jako identyfikatory CVE, nazwy, numery, identyfikatory lub po prostu CVE.
- Umieszcza się je w bazie danych po zidentyfikowaniu ich przez firmy trzecie jako potencjalnych czynników zagrożenia.
- Czynnik taki otrzymuje numer CAN (ang. Candidate Number), następnie jest analizowany oraz potwierdzany i staje się oficjalnym wpisem na liście CVE.

- Funkcją MITRE Corporation w obsłudze tej bazy danych jest opisywanie zagrożeń, nadawanie im numerów CAN oraz publiczne udostępnianie zebranych informacji.
- Baza danych CVE zawiera znane zagrożenia zebrane z całego świata i jest dostępna bezpłatnie.
- Z punktu widzenia CVE luka w zabezpieczeniach jest błędem w oprogramowaniu, który umożliwia uzyskanie nieuprawnionego dostępu do systemu bądź sieci.
- Błąd w prawidłowym stosowaniu oprogramowania lub pozostawienie systemu otwartego nie jest uznawany za lukę w zabezpieczeniach, a tym samym nie znajduje się w bazie danych.
- Jeżeli na przykład sieciowy system operacyjny pozwala na ustalanie silnych haseł, ale użytkownik nie jest zmuszany do ich stosowania lub w ogóle nie musi stosować hasła, to w takim przypadku nie mówimy o luce w zabezpieczeniach.

- Luka w zabezpieczeniach występuje, gdy:
- atakujący może uzyskać dostęp do danych, do których nie ma uprawnień,
- atakujący może podszyć się pod innego użytkownika,
- atakujący może doprowadzić do sytuacji, w której usługa będzie niedostępna dla innych użytkowników.

- Istnieje możliwość przeszukania listy CVE w bazie danych National Vulnerability Database (NVD) przy wykorzystaniu witryny internetowej <http://nvd.nist.gov/>.
- Obecnie baza danych zawiera informacje o ponad 50 tys znanych lukach w zabezpieczeniach i może zostać pobrać w celu jej przeglądania online.
- Dane znajdujące się w bazie obsługują program ISAP (ang. U.S. Information Security Program) oraz działają w charakterze repozytorium dla protokołu Security Content Automation Protocol, używanego do monitorowania bezpieczeństwa sieci i szacowania poziomu zagrożenia.

- Baza danych NVD wykorzystuje strukturalny system nazw dla różnych typów systemów informatycznych, oprogramowania oraz innych pakietów.
- System ten ma składnię podobną do używanej w adresach URI (ang. Uniform Resource Identifiers) stosowanych w internecie; ma nazwę Common Product Enumeration (CPE) (katalog produktów) i jest dostarczany w formacie możliwego do pobrania pliku XML jako część bazy danych.

Miejsca ataku

- Bezpieczeństwo sieci najczęściej jest naruszane z zewnątrz.
- Typowy atak dotyczy luk w zabezpieczeniach, w oprogramowaniu bądź sprzęcie.
- Jednak luki w bezpieczeństwie, które pozwalają na dostanie się do wewnętrz sieci, bardzo często są najskuteczniejsze, ponieważ mogą działać niewykryte.

- Najczęstszymi obszarami ataków są:
- Zewnętrzne — dostępność systemu. System może być przeciążony przez rozgłoszenie w sieci z dużą liczbą komputerów sfałszowanego pakietu ICMP, w którym zmieniono adres źródła na adres atakowanego systemu, co skutkuje dużą ilością odpowiedzi ECHO do atakowanego systemu. W takim przypadku mamy do czynienia z **tzw. atakiem smerfów (ang. Smurf Attack)**.
- Zewnętrzne — odmowa usług (DoS, Denial of Service). Atak, w którym usługa sieciowa jest zasypana żądaniami, nazywa się odmową usług (DoS). Najbardziej znany przykładem ataku **DoS** jest atak na serwer nazw domeny (DNS). Kiedy taki atak się powiedzie, to dla systemów obsługiwanych przez zaatakowany DNS adresy innych systemów w internecie lub intranecie będą niemożliwe do ustalenia, a tym samym niedostępne.
 - Atak Distributed Denial of Service (**DDoS**) oznacza atak przeprowadzony przez ogromną liczbę złamanych systemów, które działają jak tzw. komputery zombies i mogą być zamienione w botnety, czyli „roboty sieciowe”.

- Zewnętrzne lub wewnętrzne — uwierzytelnianie. Atakujący podszywa się pod tożsamość innego użytkownika.
- Dane w trakcie transportu. Ruch sieciowy jest przechwytywany w trakcie transmisji, modyfikowany, a następnie wysyłany do miejsca przeznaczenia. Taki atak nazywa się „**atakiem z osobą pośrodku**” (ang. man-in-the-middle attack); jego efektem może być podsłuchanie danych.
- Wewnętrzne — robaki, konie trojańskie oraz inne programy otwierające tylne drzwi. Wymienione programy dostarczają atakującemu metod kontrolowania systemów wewnętrz sieci oraz możliwość zmiany komputerów na zombies. Tylne drzwi mogą być programami wykonywalnymi lub algorytmami, które mogą omijać mechanizm uwierzytelniania sieciowego, przeprowadzać różne operacje i pozostawać w ukryciu.
 - Rootkit to rodzaj programu otwierającego tylne drzwi — potrafi ukrywać się jako sterownik niskiego poziomu lub moduł jądra. Rootkit nie pojawia się w systemie plików, a na liście procesów może widnieć jako zwykły proces systemowy.
- Bezpośredni dostęp wewnętrz. Atak może nastąpić z nośnika takiego jak dysk optyczny, pamięć USB, napęd przenośny itp.

- W trakcie opracowywania oprogramowania firma Microsoft używa modelu szacowania zagrożenia, który został nazwany podejściem STRIDE. Skrót STRIDE oznacza:
 - Spoofing Identity (authentication), czyli podszywanie się pod inną osobę (uwierzytelnianie) — atakujący może podszyć się pod innego użytkownika. Użytkownicy i systemy muszą stosować uwierzytelnianie za pomocą haseł, certyfikatów cyfrowych bądź innych metod.□
 - Tampering with Data (integrity), czyli złośliwa modyfikacja danych (spójność)- atakujący modyfikuje dane. Metody stosowane do zapewnienia spójności danych obejmują między innymi procedury sprawdzania błędów w danych.
 - Repudiation (non-repudiation), czyli wyparcie się (brak możliwości wyparcia się) - poszczególne osoby odrzucają odpowiedzialność za przeprowadzane operacje.
 - Information Disclosure (confidentiality), czyli dotarcie do informacji przez osobę niemającą odpowiednich uprawnień (zapewnienie poufności). W tym przypadku atakujący zyskuje dostęp do informacji poufnych. Sieci stosują ograniczenia dostępu za pomocą list dostępu, domen, usług katalogowych oraz innych funkcji sieciowych systemów operacyjnych, aby dostęp mogły uzyskać tylko te osoby, które mają do tego uprawnienia.

- Denial of Service (availability), czyli odmowa usług (dostępność). Atak typu DoS może doprowadzić do tego, że określona usługa stanie się niedostępna. Użytkownicy i systemy muszą być w niezawodny sposób połączeni z inicjowanymi zdarzeniami. Istnieje możliwość stosowania dzienników rejestrujących wszelkie zdarzenia, dołączenia danych uwierzytelniających użytkownika i systemu do danych, a także zapewnienia bezpiecznych kanałów komunikacji w celu transferu danych. W przypadku ważnych systemów powinny istnieć kopie bezpieczeństwa, które zapewniają możliwość działania po wystąpieniu awarii.
- Elevation of Privilege (authorization), czyli nieautoryzowane zwiększenie uprawnień (uwierzytelnianie). W tej sytuacji użytkownik systemu zyskuje większe uprawnienia, niż powinien mieć. Zasoby muszą być dostępne, kiedy jest to wymagane. Systemy odpowiedzialne za zarządzanie dostępem do zasobów muszą być bezpieczne. Natomiast użytkownicy powinni mieć najmniejszy poziom uprawnień, który pozwoli im na wykonywanie pracy.

Reguły tworzenia bezpiecznej sieci

- Środki bezpieczeństwa powinny koncentrować się na trzech oddzielnych poziomach:
 - Szacowanie ryzyka i ochrona przed zagrożeniem. Do najefektywniejszych technologii ochrony przed zagrożeniami zalicza się kontrolę dostępu użytkownika, szyfrowanie i zapory sieciowe.
 - Wykrywanie zagrożeń. Systemy wykrywania zagrożeń obejmują skanery antywirusowe i antyspyware'owe, systemy wykrywania włamań (ang. Intrusion Detection System, IDS), badanie zdarzeń oraz heurystyczną analizę zdarzeń w dziennikach zdarzeń.
 - Odpowiedź. Odpowiedzią na wykrycie włamania do systemu może być kwarantanna systemu bądź podsieci, przywrócenie stanu z ostatniej dobrej kopii zapasowej, naprawa i uaktualnienie mechanizmu ochrony.

- Z punktu widzenia kosztów i trudności implementacji każdy z trzech wymienionych poziomów bezpieczeństwa jest zwykle o rząd wielkości droższy niż poziom niższy.
- Dlatego wykrywanie zagrożeń może kosztować dziesięciokrotnie więcej niż szacowanie zagrożenia, natomiast odpowiedź może być już stukrotnie droższa od ochrony przed zagrożeniem.
- Warto zastanowić się nad kosztem instalacji oprogramowania skanowania antywirusowego i antyspyware'owego lub zapory sieciowej w stosunku do ilości czasu i kosztu związanego z naprawą wielu systemów, które padły ofiarą ataku.

- Jedną z najważniejszych reguł bezpiecznego projektu sieci jest minimalizacja „obszaru ataku” w systemie lub sieci. Obszar ataku to ujawniony profil systemu, który jest dostępny do przeglądania przez użytkownika bądź atakującego, zawierający na przykład następujące informacje:
 - protokoły działające w danej sieci bądź systemie,
 - interfejsy sieciowe, które mogą odpowiadać na zapytania lub wiadomości,
 - otwarte porty,
 - usługi działające w dostępnym systemie,
 - pola danych wejściowych użytkownika.

- Im mniejsza liczba dróg, którymi atakujący może spenetrować system, tym większe bezpieczeństwo.
- Jednak kiedy atakujący dostanie się do systemu, to mniejszy obszar ataku wcale nie ogranicza ilości zniszczeń, których intruz może dokonać.

- 14 najlepszych wskazówek dotyczących bezpieczeństwa sieci:
 - 1)Używaj zapory sieciowej. Zawsze należy pracować za zaporą sieciową. Warto wybierać sprzętową zaporę sieciową zamiast programowej i upewnić się, że oferuje ona izolację zarówno fizyczną, jak i protokołu. System połączony z internetem i pozbawiony zapory sieciowej może być złamany w ciągu kilku minut.
 - 2)Wymuszaj stosowanie silnych haseł. Zawsze trzeba zmieniać każde hasło domyślne. Należy stosować hasła o długości minimum ośmiu znaków, łączące małe i duże litery, cyfry oraz znaki w ciągi tekstowe, które nie występują w słowniku.
 - 3)Zainstaluj oprogramowanie antywirusowe i antyspyware'owe. Szczególnie dotyczy to bram sieci.
 - 4)Stosuj niezawodną politykę tworzenia kopii zapasowej systemu. Obrazy systemu należy przechowywać dla wszystkich systemów.
 - 5)Aktualizuj oprogramowanie. Zawsze należy aktualizować oprogramowanie tuż po wydaniu aktualizacji, ale warto mieć kopię zapasową na wypadek wystąpienia jakichkolwiek problemów związanych z aktualizacją. Szczególną uwagę trzeba poświęcić każdemu programowi, który ma styczność z siecią publiczną. Bardzo ważne jest aktualizowanie na przykład serwera WWW i przeglądarki internetowej.
 - 6)Podziel sieć na podsieci. To zapewnia fizyczną izolację sieci dzięki adresom IP.
 - 7)Szyfruj poufne dane i używaj bezpiecznych protokołów podczas transmisji danych. Danych, których nigdy nie opublikowalibyśmy w dzienniku ogólnokrajowym, nie należy wysyłać w postaci zwykłego tekstu.

- 8) Uważaj na pobieraną treść, łącza internetowe oraz niechciane wiadomości e-mail. Należy wyłączyć domyślne wykonywanie skryptów.
- 9) Zminimalizuj liczbę sposobów ataku na system. Trzeba zamknąć wszystkie niepotrzebne porty i wyłączyć wszystkie nieużywane protokoły sieciowe.
- 10) Uważaj na udziały sieciowe i na udzielanie pełnych praw dostępu do współdzielonych zasobów. Udziały stanowią potencjalny mechanizm rozprzestrzenienia w sieci wirusów, robaków, koni trojańskich i innego złośliwego oprogramowania. Należy stosować silną politykę list kontroli dostępu w sieciowym systemie operacyjnym.
- 11) Uważaj na systemy mobilne i nośniki. Trzeba izolować laptopy, które są używane poza firmą, do chwili, gdy zostaną dokładnie sprawdzone. Należy się upewnić, że systemy poufne mają zablokowaną możliwość obsługi nośników, na przykład pamięci USB.
- 12) Bezpieczny oznacza bezpieczny. Trzeba się upewnić, że połączenia w trakcie używania formularzy bądź połączenia HTTPS są bezpieczne. Należy weryfikować połączenia przez sprawdzanie certyfikatów bezpieczeństwa na witrynach internetowych. Trzeba zamykać przeglądarkę internetową po zakończeniu sesji; nie wystarczy jedynie zamknięcie karty bądź okna przeglądarki.
- 13) Poświęć czas na opracowanie polityki bezpieczeństwa. Należy we właściwy sposób wykorzystywać polityki bezpieczeństwa oferowane przez używany sieciowy system operacyjny.

- Gdy wszystkie wymienione powyżej wskazówki będą przestrzegane, sieć będzie dla intruzów trudniejszym celem.

- Polityki bezpieczeństwa w Windows Server mogą
 - blokować dostęp do zasobów na podstawie użytkowników lub grup,
 - uniemożliwiać instalację oprogramowania bądź sterowników urządzeń,
 - uniemożliwiać wykorzystywanie różnych klas urządzeń, blokować pulpit i przeglądarki internetowe,
 - Kontrolować dostęp do załączników poczty elektronicznej,
 - uniemożliwiać zapisywania płyt DVD,
 - przeprowadzać kwarantannę sieciową,
 - ustalać działania związane z ochroną konta użytkownika
 - oraz przeprowadzać inne operacje.
- Prawdopodobnie około 40% z 2400 ustawień polityk w Windows Server dotyczy bezpieczeństwa. Inne sieciowe systemy operacyjne i produkty związane z politykami bezpieczeństwa, takie jak Novell ZenWare, także oferują szerokie możliwości konfiguracji.

Technologie NLA oraz NAP

- Istnieje tak wiele sposobów, na które sieć może zostać zaatakowana, że tym, co tak naprawdę trzeba mieć przygotowane do obrony przed zagrożeniami, jest adaptacyjna strategia sieciowa.
- Firma Microsoft opracowała kilka takich strategii i dostarcza je wraz z systemami Windows Server.
 - Pierwsza technologia to Network Location Awareness (NLA)- powoduje ona, że Windows Server ma możliwość wykrywania systemów, połączeń i stanu sesji oraz odpowiedniego zastosowania właściwej polityki względem klienta.

- W wielu przypadkach klient sieciowy używa polecenia ping albo wysyła pakiet ICMP w celu sprawdzenia, czy po drugiej stronie znajduje się zasób sieciowy, z którym można się połączyć.
- Kiedy laptop nawiązuje połączenie z domeną Windows, używając polecenia ping, to stanowi ono mechanizm, który domena wykorzysta w celu określenia stanu klienta.
- Dlatego jeżeli działanie polecenia ping zakończy się niepowodzeniem, domena nie będzie mogła zastosować swojej polityki grupy.
- Reagowanie na pakiet ICMP jest często wyłączane w zaporze sieciowej, więc ten mechanizm również nie będzie niezawodny w modyfikacji połączenia klienta.
- W celu rozwiązania tych problemów opracowano technologię NLA, a informacje klienta są wymieniane za pomocą połączenia VPN. W trakcie każdego odświeżania połączenia VPN odświeżeniu ulega również polityka grupy zarówno dla użytkowników, jak i komputerów.

- Wykorzystując technologię Network Location Awareness, w systemie klienta można wprowadzić następujące zmiany:
- Opcje mogą być ustawiane automatycznie na etapie PXE (ang. Pre-Execution Environment).
- Polityka grupy klienta może być uaktualniana automatycznie, kiedy nawiązuje on połączenie z domeną. Inne zdarzenia, na przykład połączenie urządzenia mobilnego, nawiązanie sesji VPN, wybudzenie klienta ze stanu hibernacji bądź wstrzymania lub przeniesienie systemu odizolowanego w kwarantannie do sieci produkcyjnej, również powoduje odświeżenie polityki grupy.
- Istnieje możliwość konfiguracji klientów na podstawie wykrytych zasobów. Jeśli karta interfejsu sieciowego nie zostanie wykryta, to sterownik dla tej karty nie będzie automatycznie wczytany. Zawieszenie wczytywania niepotrzebnych sterowników urządzeń powoduje skrócenie czasu rozruchu.
- Przepustowość łącza do klienta również może być częścią polityki, która jest stosowana, gdy klient nawiązuje połączenie z domeną.

- Istnieje także drugie podejście do ochrony sieci — Network Access Protection (NAP). Ono także opiera się na zarządzaniu zasobami na podstawie zdefiniowanych polityk. Mechanizm NAP sprawdza stan dostępnych klientów, kiedy próbują zalogować się do domeny. Zanim klient zostanie uwierzytelniony i otrzyma dostęp do połączenia sieciowego, mechanizm NAP próbuje określić, czy nastąpiło złamanie którejkolwiek z wymienionych poniżej polityk:
 - zapora sieciowa klienta jest włączona;
 - oprogramowanie antywirusowe i antyspyware'owe działa, jego definicje są aktualne, a skanowanie było przeprowadzone niedawno;
 - zainstalowane zostały wszystkie aktualizacje udostępniane przez Microsoft;
 - inne polityki charakterystyczne dla danej sieci.

- Niespełnienie tych warunków powoduje poddanie systemu kwarantannie aż do jego naprawienia i spełnienia przez niego wszystkich wymagań.
- NAP dostarcza dodatkowych kryteriów, których spełnienie jest wymagane do zagwarantowania, że bezpieczeństwo nie będzie naruszone z wewnątrz sieci.
- Technologia ta przedstawia nowy kierunek, który wiele sieciowych systemów operacyjnych zaadaptuje, aby sieci stały się bezpieczniejsze.

- Tego typu mechanizmy mogą być zmodyfikowane jako polityki systemowe stosowane następnie do określonych konfiguracji sieciowych.
- W poprawnie skonfigurowanej usłudze NAP oprogramowanie odpowiedzialne za politykę NAP jest obsługiwane przez serwery Health Requirement oraz Trusted Health Registration Authority.
- Obsługą identyfikacji i uwierzytelniania klientów zajmują się serwery usług katalogowych i certyfikatów. Kiedy klient NAP nie spełni wymagań polityki dotyczącej jego kondycji, zostanie zalogowany do oddzielnej podsieci, gdzie będzie zarządzany przez serwer naprawczy, który zajmie się jego mankamentami.

Bezpieczne protokoły w internecie

- Internet to niewątpliwie niebezpieczne środowisko. W większości przypadków każdy odbywający się w nim ruch sieciowy może być przechwycony i buforowany.
- W celu zagwarantowania poufności danych wysyłanych przez internet opracowano kilka różnych protokołów komunikacyjnych, dzięki którym można chronić dane.
 - IPsec,
 - Transport Layer Security (poprzednio Secure Sockets Layer),
 - HTTPS.

IPsec

- Internet Protocol Security (IPsec) to metoda szyfrowania i weryfikowania ruchu sieciowego wysyłanego przez sieci TCP/IP będąca standardem otwartym, zdefiniowanym w dokumencie IETF RFC 2401
- Zestaw protokołów zawiera bazujący na kluczu mechanizm szyfrujący do ustanawiania unikalnej identyfikacji punktów końcowych połączenia.
- W celu użycia IPsec oba węzły muszą mieć lokalnie uruchomiony ten protokół. Za pomocą protokołu IPsec można korzystać z emisji pojedynczej lub multiemisji.
- W trakcie multiemisji wszystkie węzły docelowe muszą współdzielić te same informacje bezpieczeństwa.

- IPsec może operować w dwóch trybach:
 - transportowym,
 - Tunelu.
- W trybie transportowym w pakiecie pozostaje oryginalny nagłówek IP w przeciwieństwie do trybu tunelu, gdzie nagłówek ten jest zamieniany na nowy, a oryginalny jest enkapsulowany.
- Tryb transportowy jest zazwyczaj stosowany w komunikacji pomiędzy urządzeniami końcowymi,
- tryb tunelu jest głównie stosowany do łączenia dwóch sieci. Tryb tunelu jest często używany w tworzeniu sieci VPN (ang. Virtual Private Network — wirtualna sieć prywatna).

- Istnieje również możliwość używania IPsec, kiedy tylko jeden punkt końcowy połączenia obsługuje protokół IPsec.
- W takim przypadku pakiet IPsec jest szyfrowany i enkapsulowany w routerze brzegowym (lub w innym zewnętrznym), a następnie deszyfrowany i wyodrębniany w routerze granicznym dla systemu docelowego.
- Po skonfigurowaniu IPsec w taki właśnie sposób ruch sieciowy jest widoczny dla obu punktów końcowych w sieci, ale bezpieczny po opuszczeniu podsieci, w której znajduje się system wysyłający pakiet.

- W modelu OSI IPsec jest protokołem warstwy sieciowej (poziom 3.), natomiast w modelu TCP/IP protokołem warstwy internetu.
- W zestawie protokołu IPsec najważniejsze są trzy protokoły:
- Authentication Header (AH). Protokół AH dostarcza mechanizm gwarantujący uwierzytelnianie i integralność pakietów IP w IPsec. W tym celu stosuje wartość kontrolną ICV (ang. Integrity Check Value), której wartość protokół AH oblicza, używając algorytmu kodującego oraz współdzielonego klucza. Wartość kontrolna ICV pełni taką samą funkcję jak sprawdzanie danych CRC. Odbiorca pakietu deszyfruje dane, uruchamia te same algorytmy i sprawdza, czy obliczona wartość kontrolna ICV jest taka sama jak w datagramie, co zapewnia uwierzytelnienie nadawcy.

- Encapsulating Security Payload (ESP). Protokół ESP szyfruje dane używane w komunikacji IPsec i zapewnia formę uwierzytelniania, integralności danych (wartość kontrolna ICV) oraz ochrony treści danych IPv4 lub IPv6. ESP można stosować w trybie tylko szyfrowania albo tylko uwierzytelniania, ale najczęściej włączone są obie funkcje. ESP w przeciwieństwie do AH nie zapewnia integralnej ochrony nagłówka IP.
- Internet Key Exchange (IKE) v1 oraz v2. Protokół IKE dostarcza mechanizm współpracy między dwoma punktami końcowymi połączenia, ustala dostępne protokoły bezpieczeństwa i określa, które z nich będą używane. Następnie przeprowadza szyfrowanie i tworzy klucze uwierzytelnienia wysyłane do systemu docelowego, aby wysyłany pakiet mógł być poprawnie zidentyfikowany i odszyfrowany. Protokół IKE został zdefiniowany w dokumencie IETF RFC 2409

- Do wymiany danych i negocjacji parametrów bezpieczeństwa (SA, ang. Security Association) IKE używa protokołu Internet Security Association and Key Management Protocol (ISCAPM).
- ISCAPM pozwala na obsługę różnych metod wymiany kluczy. Dwa najczęściej stosowane protokoły wymiany kluczy to OAKLEY i SKEME. Ten pierwszy jest najczęściej używany jako technologia wymiany kluczy w IKE, natomiast od drugiego (SKEME) IKE „pożyczca” pewne funkcje, na przykład technologię szyfrowania klucza publicznego.

- Ponieważ IPsec operuje na tym samym poziomie co sam protokół IP, pozostaje niezależny od aplikacji i może być używany do bezpiecznego wysyłania pakietów z dowolnej aplikacji.
- Taka sytuacja nie ma miejsca w przypadku innych protokołów bezpieczeństwa, na przykład SSL, które operują na wyższych poziomach i wymagają od aplikacji wbudowania ich obsługi.

- IPsec negocjuje metodę stosowaną do przekazywania datagramów w danym formacie między punktami końcowymi.
- Dwa punkty końcowe wraz z wynegociowaną polityką bezpieczeństwa są przechowywane w SA.
- Polityka bezpieczeństwa określa, które pakiety są zabezpieczane i kiedy wykorzystują protokół AH lub ESP.
- Algorytmy używane do szyfrowania oraz do uwierzytelniania są wybierane z listy, a następnie współdzielone, podobnie jak klucze niezbędne do odszyfrowania danych w obu procesach.
- Polityki są przechowywane lokalnie w bazie danych SPD (ang. Security Policy Database) każdego urządzenia.
- Natomiast SA są przechowywane w bazie danych SAD (ang. Security Association Database) każdego urządzenia.

- Wprawdzie IPsec jest komponentem opcjonalnym w komunikacji IPv4, jest jednak wymagany i stanowi zintegrowaną część IPv6

Zestaw protokołów Transport Layer Security

- Transport Layer Security (TLS) to zestaw protokołów kryptograficznych wykorzystywanych do szyfrowania danych wysyłanych na poziomie warstwy transportowej w sieci TCP/IP.
- Ten rozwijany standard został zdefiniowany w dokumencie IETF RFC 5246.
- TLS obsługuje nadzbiór doskonale znanego protokołu SSL (ang. Secure Socket Layer), opracowanego przez firmę Netscape i używanego przez wiele lat.
- Protokół SSL 3.0 był pierwszym protokołem sieciowym wybranym przez firmy obsługujące płatności przeprowadzane za pomocą kart internetowych do bezpiecznej obsługi transakcji w internecie.

- Protokół TLS zarówno szyfruje, jak i uwierzytelnia dane wysyłane z serwera do uwierzytelnionego klienta, tak więc zapewniane jest bezpieczeństwo komunikacji.
- Protokół ten jest najczęściej wykorzystywany w celu umożliwienia serwerom WWW komunikacji z klientami, na przykład przeglądarkami internetowymi.
- Jednak może być też stosowany w przypadku ruchu sieciowego TCP/IP, generowanego przez dowolne aplikacje.

- W swojej najprostszej postaci TLS używa serwera uwierzytelnionego oraz klienta nieuwierzytelnionego.
- Jeżeli została zainstalowana infrastruktura klucza publicznego (ang. Public Key Infrastructure — PKI), TLS można skonfigurować w taki sposób, aby oba punkty końcowe połączenia mogły być wzajemnie uwierzytelniane.

- Proces ten opiera się na trzech krokach:
 - 1)Obsługa negocjacji protokołu. Klient wysyła do serwera TLS listę obsługiwanych metod szyfrowania oraz funkcji kodujących, serwer wybiera najmocniejszą. Krok ten określa się „uściskiem dłoni TLS” (ang. TLS handshake); może on być prostym procesem bez uwierzytelniania klienta.

- 2) Wymiana klucza i system pojedynczego bądź wzajemnego uwierzytelniania. Serwer zwraca klientowi certyfikat cyfrowy zawierający nazwę serwera oraz dane uwierzytelniające z centrum certyfikacji (ang. Certificate Authority, CA). Klient może zweryfikować te informacje w serwerze centrum certyfikacji.
- 3) Szyfrowanie symetryczne i uwierzytelnianie wiadomości. Klient szyfruje losowo wybraną liczbę za pomocą klucza publicznego serwera i wysyła ten klucz sesji serwerowi, gdzie będzie odszyfrowany za pomocą klucza prywatnego. Zarówno serwer, jak i klient powinny wygenerować losowe liczby, które następnie będą użyte przez różne algorytmy do wygenerowania odpowiednich kluczy.

- TLS obsługuje pewną liczbę różnych algorytmów kryptograficznych zarówno w celu tworzenia i wymiany klucza, jak i uwierzytelniania.
- Kiedy dwa punkty końcowe prowadzą negocjacje, dochodzi do wyboru algorytmu wymiany klucza oraz algorytmu uwierzytelniania.
- Uwierzytelnianie wiadomości obejmuje także użycie kodów uwierzytelniania wiadomości (ang. Message Authentication Code, MAC), które są tworzone za pomocą funkcji kryptograficznych.
- Z kolei SSL do utworzenia swoich kodów MAC wykorzystuje pseudolosową funkcję.
- Ogólnie rzecz ujmując, negocjacje TLS polegają na wyborze algorytmów z pakietu kryptograficznego.

- Aby aplikacja mogła używać TLS, musi mieć wbudowaną obsługę protokołu TLS.
- Wprawdzie protokół TLS jest stosowany przede wszystkim dla ruchu HTTP podczas transportu przez TCP, ale jest wykorzystywany również do zabezpieczania ruchu SMTP, FTP, NNTP oraz XMPP. OpenVPN.
- Innym obszarem, na którym TLS jest szeroko wykorzystywany, jest ruch VoIP (ang. Voice over IP), gdzie protokół sygnalizacyjny SIP (ang. Session Initiation Protocol) jest szyfrowany i uwierzytelniany.

- Dla wielu aplikacji pozbawionych obsługi TLS istnieją produkty firm trzecich enkapsulujące ruch TLS i transportujące go między punktami końcowymi.
- Jeden z takich programów to stunnel. Jest to działająca na wielu platformach bezpłatna (typu open source) aplikacja tunelowania TLS/SSL.
- Działa na zasadzie enkapsulacji danych do TLS i może używać infrastruktury PKI do tworzenia bezpiecznych połączeń.

Protokół HTTPS

- HyperText Transfer Protocol Secure (HTTPS) łączy w sobie protokół HyperText Transfer Protocol (HTTP) z protokołami Transport Layer Security (TLS) albo Secure Sockets Layer (SSL).
- Uwierzytelniony serwer WWW używa HTTPS w celu nawiązania bezpiecznego połączenia z przeglądarką internetową klienta.
- Podczas nawiązywania połączenia w pasku adresu URL zamiast standardowego prefiksu `http://` podaje się `https://`.
- O ile nie zostanie to zmodyfikowane, domyślnie ruch sieciowy HTTP będzie używał portu numer 443.

- Certyfikaty stosowane przez serwery WWW są certyfikatami klucza publicznego, które zostały utworzone przez oprogramowanie i wysłane do centrum certyfikacji w celu ich weryfikacji.
- Taki certyfikat jest cyfrowo podpisywany przez centrum certyfikacji, co oznacza, że każdemu zainteresowanemu dostarcza klucza publicznego niezbędnego do weryfikacji i sprawdzenia, czy informacje podawane przez serwer WWW są prawidłowe.
- Aby przeglądarka internetowa mogła zweryfikować certyfikat, musi dysponować podpisany certyfikatem centrum autoryzacji. Ponieważ taka funkcja będzie bezużyteczna bez certyfikatów, certyfikaty większości głównych centrów certyfikacji są dostępne we wszystkich najważniejszych przeglądarkach internetowych.

- Firmy i użytkownicy prywatni mogą ustanawiać własne centra certyfikacji, ale będą one nadawały się jedynie do szyfrowania ruchu sieciowego, tak aby inni nie mogli podglądać danych.
- Certyfikat prywatny lub firmowy nie uwierzytelnia nadawcy. Jednak jeżeli firma wysyła dane ze swojego serwera WWW do swoich przeglądarek internetowych, to w takim przypadku certyfikat tej firmy potwierdzi prawdziwość nadawcy.
- Oprócz certyfikatów dla serwerów firmy mogą tworzyć certyfikaty dla klientów i umieszczać je w przeglądarkach internetowych poszczególnych użytkowników.
- Certyfikat klienta może zweryfikować w serwerze dane użytkownika bez konieczności jego logowania i pozwala serwerowi na sprawdzenie tej informacji podczas każdego połączenia z klientem.

Szyfrowanie i kryptografia

- Kryptografia to nauka o metodach szyfrowania (ukrywania) informacji.
- Związane z nią zagadnienia mieszczą się w obrębie zarówno informatyki, jak i matematyki.
- Istnieje wiele metod kryptograficznego zabezpieczania informacji, między innymi używanie haseł, biometryk lub innych urządzeń, szyfrowanie danych za pomocą algorytmów, używanie kluczy itp.

- Szyfrowanie oznacza proces przekształcania informacji na postać danych, które tracą swój kontekst.
- Deszyfrowanie to proces całkowicie odwrotny, to znaczy przekształcanie danych z powrotem na postać informacji, które mogą być odczytane i zrozumiane.
- Oba procesy, tj. dwa algorytmy odpowiedzialne za szyfrowanie i deszyfrowanie, nazywamy kodowaniem.
- Niektóre systemy kodowania wymagają używania klucza, który stanowi informację wykorzystywaną do modyfikacji operacji kodowania.
 - W takich przypadkach nadawca i odbiorca mogą współdzielić klucz publiczny, ale nie wymieniają kluczy prywatnych koniecznych do przeprowadzenia procesu kodowania. Aby zachować pełną poufność, klucz powinien być zmienny (to znaczy generowany na nowo w trakcie każdego użycia), w przeciwnym razie traci swoją możliwość ochrony kodu przed osobami z zewnątrz.
- Wszystkie wymienione elementy komunikacji — kodowanie, klucze i zaszyfrowane dane — są przedmiotem działania dla metod uwierzytelniających, które weryfikują, czy informacje zostały dostarczone prawidłowo, i ustalają źródło ich pochodzenia.

- Nowoczesne metody kodowania są wyjątkowo dobre i bardzo trudne do złamania. Trzy najlepiej znane algorytmy kryptograficzne stosowane w informatyce to:
 - Data Encryption Standard (DES)
 - Algorytm Diffie-Hellman Key Agreement
 - Algorytm klucza publicznego RSA

Kerberos

- Protokół Kerberos to system uwierzytelniania sieciowego, który bazuje na infrastrukturze klucza symetrycznego oraz zaufanym systemie firmy trzeciej.
- Na tej podstawie ustala tożsamość stron komunikacji i gwarantuje, że dane zostaną dostarczone bez ingerencji lub przejęcia.
- System Kerberos został utworzony w celu umożliwienia wysyłania danych przez niezabezpieczone połączenia (na przykład internet) przy jednoczesnym zagwarantowaniu, że nie zostaną podejrzane lub ponownie przetransmitowane jako część ataku z osobą pośrodku (ang. man-in-the-middle attack) lub ataku powtórzeniowego (ang. replay attack).
- Od chwili opracowania na uczelni MIT Kerberos został rozszerzony na wiele sposobów i zawiera uwierzytelnianie z użyciem algorytmu klucza asymetrycznego.

- Kerberos podczas uwierzytelniania działa w następujący sposób:
 - 1) Klient loguje się do sieci, a informacje logowania są wysyłane do systemu lokalnego centrum bezpieczeństwa (ang. Local Security Authority, LSA).
 - 2) System LSA przekazuje żądanie do usługi uwierzytelniania wraz z żądaniem uwierzytelnienia klienta przez LSA.
 - 3) Żądanie jest przekazywane do polecenia Pobranie danych uwierzytelniających z systemu LSA, a system LSA wysyła klientowi odpowiednie dane uwierzytelniające.
 - 4) Klient rozpoczyna sesję.
 - 5) Bilet żądania dla danej aplikacji, sesji lub operacji jest przekazywany do LSA przez klienta, a następnie przesyłany dalej do serwera przyznającego bilety (ang. Ticket Granting Service, TGS). Bilet utworzony w TGS jest zwracany klientowi.
 - 6) Żądanie jest przekazywane do serwera WWW w celu bezpiecznego pobrania informacji z systemu e-commerce.
 - 7) Serwer WWW może przekazać żądanie do serwera E-Commerce, a następnie wysłać polecenie Pobranie danych uwierzytelniających do systemu LSA, który z kolei przekazuje żądanie do usługi certyfikatu (ang. Certificate Service).
 - 8) Usługa certyfikatu wysyła dane uwierzytelniające do systemu LSA, który następnie wykonuje polecenie Zezwolenie na sesję.
 - 9) Serwer WWW wysyła informacje żądane przez klienta.

- Nazwa „Kerberos” pochodzi od Cerbera (Cerberus), mitycznego trzygłowego psa, który strzegł Hadesu.
- Kerberos został opracowany jako część projektu Athena na uczelni MIT i po raz pierwszy pojawił się w wersji 4. w roku 1988.
- Wersja 5. pojawiła się w roku 1993 i została opublikowana przez IETF jako dokument RFC 1510.
- Standard MIT Kerberos jest dostępny bezpłatnie i wielu ważnych graczy w internecie, między innymi Sun Microsystems, Microsoft, Google, Apple oraz inne firmy, utworzyło konsorcjum Kerberos Consortium w celu kontynuowania prac w MIT nad tym standardem.
- Kerberos jest używany w wielu sieciowych systemach operacyjnych, takich jak Solaris, BSD UNIX, sieci Windows (od wersji 2000 wzwyż), Mac OS X czy Red Hat Linux (v.4 i późniejsze).

- Kerberos pierwotnie używało szyfrowania DES, co doprowadziło do tego, że władze Stanów Zjednoczonych zakazały eksportu tej technologii do innych krajów w ramach przepisów o zakazie eksportu uzbrojenia, obowiązujących do roku 2000.
- Windows Server 2000 to pierwszy ważniejszy sieciowy system operacyjny, który zawierał technologię Kerberos wraz z DES-56.
- Od tej chwili Microsoft korzysta z algorytmu RC4 w swoim szyfrowaniu Kerberos.
- Poza Stanami Zjednoczonymi opracowano inne wersje systemu Kerberos, które nie stosowały algorytmu DES. Do najbardziej znanych implementacji zaliczają się eBones i Heimdal.

- Kerberos używa dwóch protokołów komunikacji opracowanych przez Rogera Needhama i Michaela Schroedera.
 - Protokół Symmetric Key Protocol wykorzystuje algorytm szyfrowania symetrycznego w celu utworzenia klucza sesji między punktami końcowymi połączenia.
 - Protokół Public Key Protocol stosowany w systemie Kerberos służy do ustanowienia wspólnego uwierzytelnienia między punktami końcowymi.
- Zaufaną firmę trzecią w systemie Kerberos określa się mianem centrum dystrybucji kluczy (ang. Key Distribution Center, KDC);
 - jest ona umieszczona w dwóch oddzielnych usługach: serwerze uwierzytelniania (AS) oraz
 - serwerze przyznającym bilety (TGS).

- Bilety są rozpowszechniane w celu umożliwienia klientowi samoidentyfikacji w sesji.
- Centrum dystrybucji kluczy ma zbiór tajnych kluczy zapisanych w magazynie danych dla każdego węzła sieciowego.
- Tajny klucz jest znany tylko węzłowi oraz centrum dystrybucji kluczy, nikt inny go nie zna.
- Kiedy nawiązywane jest połączenie, centrum dystrybucji kluczy generuje klucz sesji używany do uwierzytelnienia punktów końcowych połączenia.

- Wprawdzie mechanizm Kerberos angażuje co najmniej osiem różnych wiadomości między klientem, serwerem przyznającym bilety i usługą serwera, ale wiadomości te pozwalają każdemu węzłowi w systemie zarówno na samoidentyfikację, jak i weryfikację wiadomości pochodzących z innego węzła.

- Sukces każdej operacji
 - logowania klienta,
 - uwierzytelniania klienta,
 - autoryzacji usługi klienta,
 - żądania usługi klienta
- zależy zarówno od dwóch wiadomości wymieniających bilety, jak i dopasowania kluczy sesji.
- Żadna wiadomość nie zawiera obu tych informacji. Kerberos powoduje obciążenie sieci, ale system jest bezpieczny.

- Kerberos jednak nie jest pozbawiony problemów. Jeden z nich to serwer przyznający bilety — to pojedynczy punkt systemu, który w przypadku awarii powoduje błędne działanie całości.
- Dlatego też trzeba umożliwić mu funkcjonowanie w przypadku awarii.

- Ponadto Kerberos zależy od znaczników czasu umieszczanych w wiadomościach na każdym etapie, więc wszystkie systemy muszą pozostać zsynchronizowane za pomocą usługi takiej jak NTP (ang. Network Time Protocol) lub WTS (ang. Windows Time Service).
- Kerberos może tolerować drobny brak synchronizacji, zwykle do około dziesięciu minut. Większa asynchroniczność prowadzi do tego, że bilety stają się nieważne.
- Wymienione czynniki można dostosować jako część polityk domeny oraz w ustawieniach mechanizmu Kerberos.

- Ostatnia niedogodność wiąże się z faktem, że serwer uwierzytelniania przechowuje wszystkie tajne klucze.
- Jeżeli ktoś uzyska dostęp do tego serwera, to bezpieczeństwo całej sieci będzie zagrożone.
- Na poziomie poszczególnych klientów złamanie systemu może doprowadzić do ujawnienia hasła klienta.
- Mimo to Kerberos jest obecnie najnowocześniejszą technologią uwierzytelniania sieciowego i usługą identyfikacji.

Zapory sieciowe

- W sieci komputerowej odpowiednikiem ściany przeciwpożarowej jest zapora sieciowa — bariera ochronna, którą stanowi zbiór procedur bezpieczeństwa izolujących i chroniących systemy danej sieci przed podejrzanaą aktywnością.
- Może to być oddzielenie sieci za pomocą odrębnych urządzeń sprzętowych (fizycznych interfejsów sieciowych), zawierających wiele połączeń z siecią. Taki mechanizm nazywa się izolacją fizyczną.
- Zapora sieciowa może kontaktować się z siecią zewnętrzną, używając jednego protokołu sieciowego, natomiast z siecią wewnętrzną — za pomocą innego protokołu sieciowego. Określa się to izolacją protokołu.
- W dzisiejszych czasach posiadanie systemów połączonych z internetem bez żadnej zapory sieciowej jest bardzo nieroważne.

- Zapora sieciowa może być zarówno bardzo prosta, jak i niezwykle skomplikowana.
- Może być zaimplementowana w oprogramowaniu lub być oprogramowaniem zainstalowanym na dedykowanych serwerach i urządzeniach.
- Może działać w ramach używanego systemu operacyjnego, na przykład Linuksa, Uniksa lub Windows, albo być rodzajem „czarnego pudełka”, czyli samodzielną jednostką działającą pod kontrolą własnego systemu operacyjnego.

- Zapory sieciowe mogą być podzielone na następujące kategorie:
 - osobiste zapory sieciowe takie jak zapora sieciowa w systemie Windows, ZoneAlarm i inne,
 - zapory sieciowe w routerach,
 - sprzętowe zapory sieciowe zarówno proste, jak i bardzo skomplikowane,
 - zapory sieciowe w postaci proxy,
 - zapory sieciowe w postaci serwerów

- Zapora sieciowa najczęściej oferuje funkcje, które można zaliczyć do więcej niż tylko jednej z wymienionych kategorii.
- Podczas porównywania zapór sieciowych trzeba wziąć pod uwagę trzy czynniki: oferowane funkcje, wydajność (mierzoną przepustowością) oraz cenę.
- Zapory sieciowe to urządzenia sieciowe, dla których nie istnieją standaryzowane testy wydajności.
- Producenci wiedzą, że klienci używają zapór sieciowych na wiele różnych sposobów, i nie znoszą przedstawiania testów wydajności potencjalnym nabywcom.

Funkcje zapory sieciowej

- Niezależnie od natury zaimplementowanej zapory sieciowej jej działanie polega na stosowaniu zestawu filtrów ruchu sieciowego przechodzącego przez tę zaporę sieciową.
- Zapora sieciowa może przekazać dalej albo odrzucić dany ruch sieciowy.
- W modelu OSI zapora sieciowa może być filtrem warstwy sieci (warstwa 3.) bądź aplikacji (warstwa 7.) lub dowolnej warstwy między trzecią i siódmą.

- Wybrane funkcje, na które warto zwrócić uwagę podczas porównywania zapór sieciowych:
 - Filtrowanie pakietów. Operacja filtrowania pakietów odczytuje pola nagłówka pakietu IP i używa zdefiniowanych reguł w celu zezwolenia na ruch przychodzący do systemu lub zablokowania tego ruchu. Filtrowanie pakietów można również zastosować wobec ruchu wychodzącego.

- Filtry danych wejściowych interfejsu sieciowego. Filtry te blokują ruch sieciowy na podstawie parametrów takich jak źródłowy adres IP lub zakres adresów, numer portu czy użyty protokół.
- Mechanizm tłumaczenia adresów sieciowych (NAT). NAT to system konwersji, którego zadaniem jest zmiana źródłowych lub docelowych adresów IP, zazwyczaj również portów TCP/UDP w przepływających pakietach. Mechanizm NAT wykorzystuje tablice translacji i współpracuje z nieroutowalnymi w sieci publicznej sieciami prywatnymi. Mechanizm NAT to nie jest, ścisłe rzecz biorąc, funkcja zapory sieciowej — znacznie częściej jest powiązany z routerami i serwerami proxy — jednak dostarcza technologię pozwalającą na ukrycie adresu IP systemów sieci prywatnej, co jest cenną funkcją.

- Stateful Inspection. Filtry typu Stateful Inspection przeprowadzają analizę wszystkich pakietów wychodzących i rejestrują ich adresy docelowe w tabeli stanu. Kiedy ruch sieciowy jest wysyłany z powrotem z systemu zewnętrznego, zapora sieciowa używa tabeli stanu w celu określenia, czy pakiety powinny być przekazywane. Ogólna reguła jest taka, że filtry typu Stateful Inspection są o wiele większym obciążeniem dla zapory sieciowej i działają znacznie wolniej niż statyczne filtrowanie pakietów.

- Analiza połączeń. W filtrze tego typu sesje są zarządzane, zamiast po prostu odwoływać się do pakietów lub połączenia w tabeli stanu. Sesje wymagają żądań pochodzącego z systemu znajdującego się za zaporą sieciową i mogą obsługiwać aplikacje tworzące wiele połączeń. Protokoły z wieloma połączeniami obejmują między innymi sesje HTTP przeglądarki internetowej, pobieranie plików za pomocą FTP oraz strumieniowanie multimedialnych.
- Funkcja analizy połączeń znacznie utrudnia przeprowadzenie udanego ataku typu IP spoofing (fałszowanie źródłowego adresu IP), DoS (ang. Denial of Service — odmowa usług) i prób rozpoznania sieci. Filtry powiązane z funkcją analizy połączeń stanowią mniej efektywną ochronę przed atakami typu DoS.

- Zapora sieciowa w postaci proxy. Zapora sieciowa w postaci proxy działa w charakterze pośrednika między klientem znajdującym się wewnętrz zapory sieciowej i systemem lub serwerem na zewnątrz. Między obiema stronami nie ma bezpośredniego połączenia przez zaporę sieciową. Zapora sieciowa w postaci proxy tworzy dwa oddzielne połączenia, po jednym dla każdej strony zapory sieciowej. Klient wewnętrz komunikuje się jedynie z proxy, które z perspektywy klienta jest jego punktem docelowym. Serwer proxy może zwiększyć wydajność działania przez buforowanie najczęściej lub ostatnio używanych danych. Ma również możliwość weryfikacji protokołów przekazywanych przez zaporę sieciową. Pozwala także na zarządzanie w taki sposób, aby żądania były przekazywane na bazie identyfikatora użytkownika i (lub) członków grupy.

- Filtrowanie aplikacji. Filtrowanie na poziomie aplikacji to technologia tzw. Głębokiej analizy pakietów (ang. deep packet inspection). Metoda ta jest najbardziej skomplikowana i najwolniejsza z wymienionych na tej liście. Filtry tej metody analizują pakiety pod kątem zawartych w nich danych, a następnie modyfikują je, jeśli zachodzi taka potrzeba.

Bramy bezpieczeństwa

- Brama jest urządzeniem warstwy aplikacji (warstwa 7.) działającym w charakterze interfejsu między sieciami.
- Bramy mogą być zaimplementowane jako urządzenia sprzętowe bądź jako oprogramowanie.
- Pojęcie „brama” jest ogólne i generalnie oznacza występowanie pewnego rodzaju konwersji protokołów.
- W warstwie aplikacji brama musi przekształcać jeden rodzaj pliku na inny, w warstwie prezentacji konwersja może zastępować dany rodzaj szyfrowania innym lub wykonywać inne funkcje.
- Bramy mogą przeprowadzać konwersje na poziomie transportowym (warstwa sieci) z IP na AppleTalk.
- Ogólnie rzecz ujmując, brama to urządzenie, które może działać na dowolnym poziomie modelu OSI. W wyniku tego bardzo często można się spotkać z bramami opisywanymi jako „brama pocztowa”, „brama WWW” lub nawet „brama bezpieczeństwa”.

- Aby brama mogła funkcjonować między sieciami, bardzo często musi mieć możliwość działania jako router dostarczający funkcji mapowania adresów.
- Bardzo często bramy pełnią funkcję serwera proxy lub zapory sieciowej.

Domyślnie odmawiaj

- Standardową regułą używaną przez każdą technologię zapewniającą wysoki poziom bezpieczeństwa jest inicjalizacja urządzenia wraz ze stanem domyślnie odmawiaj.
- Wiele zapór sieciowych, serwerów proxy oraz innych systemów bezpieczeństwa jest standardowo dostarczanych w postaci całkowicie zamkniętej.
- Może to wywołać zdziwienie u kogoś, kto wcześniej nie spotkał się z taką sytuacją. W przypadku całkowicie zamkniętego systemu zaleca się, aby administrator włączał jednorazowo po jednej wymaganej usłudze.

- Typowe jest stosowanie poniższej sekwencji reguł:
 - **Odrzucaj każdy ruch sieciowy, chyba że istnieje odpowiednia reguła, która dopuszcza ten rodzaj ruchu.** To jest właśnie stan domyślnie odmawiaj.
 - **Zablokuj wszystkie pakiety przychodzące z adresami sieci wewnętrznej oraz wszystkie pakiety wychodzące z adresami zewnętrznymi.** Wymienione pakiety zwykle pochodzą od atakujących bądź są błędne.
 - **Skonfiguruj ruch sieciowy DNS odpowiednio dla zapytań DNS bazujących zarówno na UDP, jak i TCP.** Bez usługi rozpoznawania adresów większość innych funkcji sieci nie będzie działała.

- Należy zezwalać na ruch sieciowy HTTP i prawdopodobnie na HTTPS przez otworzenie portu numer 80 oraz odpowiednie przekierowanie tego ruchu.
 - Jeżeli używane są serwery poczty, to należy włączyć SMTP i (lub) POP3 przez otworzenie ich portów.
 - Należy odpowiadać na prośby o pomoc kierowane przez otwieranie poszczególnych portów lub tras po sprawdzeniu tych próśb i upewnieniu się, że funkcje sieciowe wymagają tego rodzaju dostępu
- Wymienione reguły są stosowane w kolejności od początku listy.

Sieciowe systemy operacyjne oraz usługi katalogowe i domeny

Sieciowe systemy operacyjne

- Network operating system to system który został zoptymalizowany w celu dostarczania usług sieciowych.
- System musi:
 - Obsługiwać sprzęt sieciowy
 - Obsługiwać protokoły i usługi sieciowe
 - Dostarczać te usługi klientom.

Sieciowe systemy operacyjne

- Ponadto może/powinien:
 - Posiadać narzędzia administracyjne i zarządzające
 - Usługi katalogowe oraz nazw
 - Serwery plików
 - Serwery wydruku
 - Tworzenie kopii zapasowej
 - Gwarantować bezpieczeństwo
 - Routing sieciowy

Sieciowe systemy operacyjne

- Platformy:
 - Unix
 - Linux
 - Microsoft Windows
 - Cisco IOS

LANtastic

- Opracowany przez Artisoft (najnowszy 8.0)
- Połączenie klientów MS-DOS, Nowell NetWare oraz OS/2
- Współdzielony dostęp do aplikacji, plików, drukarek i napędów optycznych.

NetWare

- Firma Novell – 1983 rok
- Pierwszy sieciowy system operacyjny
- Nacisk na współdzielenie plików
- Administracja dostępem do plików
- TSR (Terminate and Stay resident)
- Mapowanie woluminów do liter dysków lokalnych
- Lider rynku aż do Windows NT (nawet Windows 95 nie pokonał rywala)
- Protokół IPX firmy Novell wyparty przez TCP/IP

Obecne systemy sieciowe

- Trzy podstawowe warunki:
 - Dostarczać system operacyjny obsługujący sprzęt komputerowy
 - Udostępniać różne protokoły sieciowe i usługi, takie jak adresowanie
 - Uruchamiać aplikacje serwerowe i umożliwiać do nich dostęp klientom lub w przypadku sieci równorzędnych dostęp innym systemom operacyjnym

Po za tym

- Zarządzanie i administrowanie siecią
- Nazwy oraz inne usługi katalogowe
- Współdzielenie plików i drukarek
- Usługi sieciowe
- Tworzenie kopii zapasowych
- Usługi replikacji
- Bezpieczeństwo (potrójne A – authentication, authorization i accounting)
- Routing sieciowy i firewall
- Odporność na awarie
- Możliwość skalowalności

Obecnie?

- Wiele firm udostępnia systemy operacyjne z tym samym jądrem dla klienta i serwera.
- Dodają tylko dodatkowe ograniczenia (np. windows XP i Windows Server 2003)
- Kilka dystrybucji Linuxa podobnie jak Windows.
- Solaris nie rozróżnia pomiędzy komputerami klientów a serverami

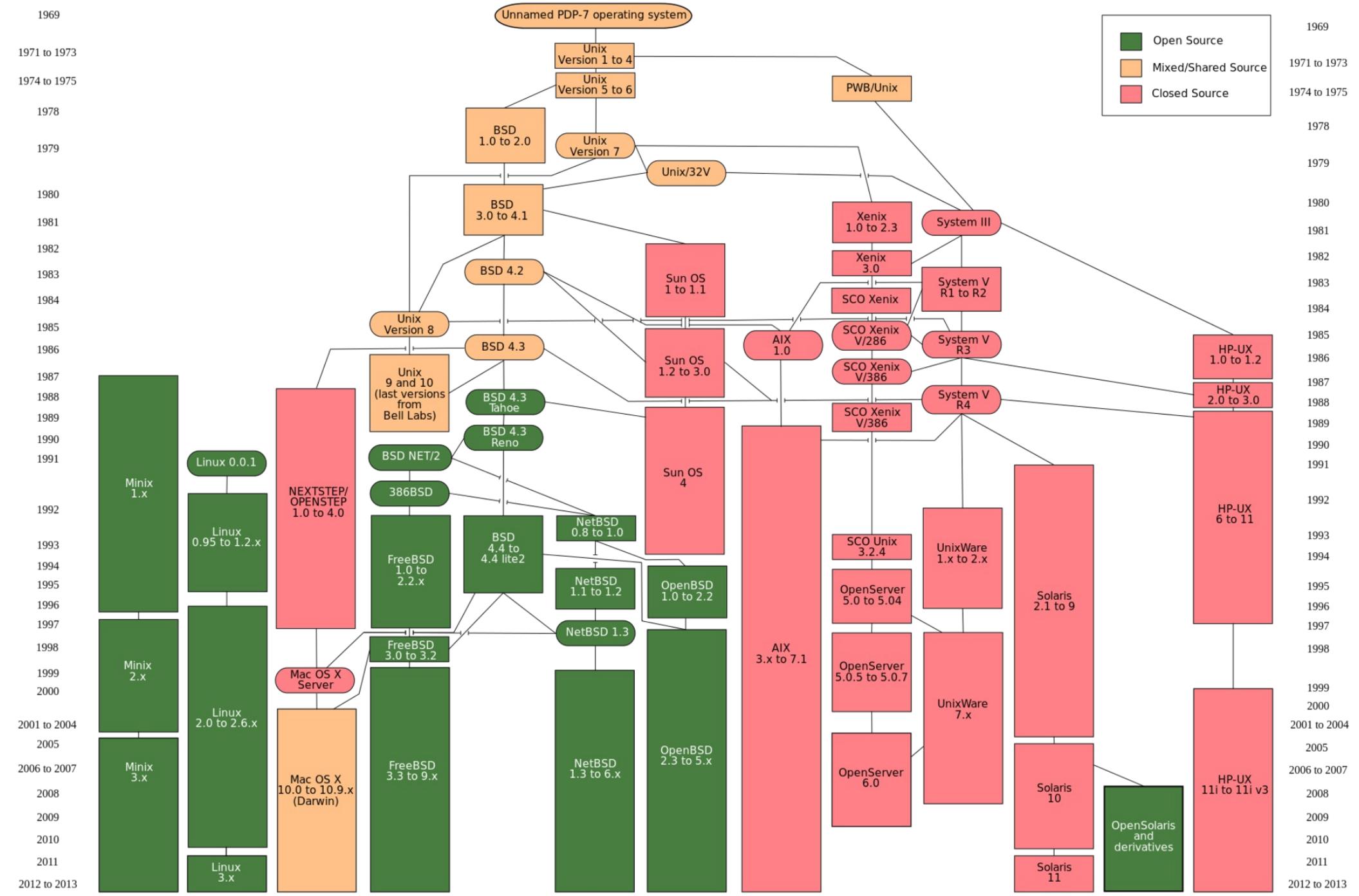
Powszechnie używane platformy

Tabela 20.1. Powszechnie używane platformy sieciowych systemów operacyjnych

| Nazwa systemu NOS | Właściciel | Wersja bieżąca | Obsługiwany sprzęt |
|--------------------------------|---------------------------------------|--------------------------------|--|
| AIX | IBM | 7.1 | 64-bitowe systemy RISC |
| BSD | Projekt FreeBSD, NetBSD i OpenBSD | 8.1, 5.1, 4.8 | Alpha, ARM, x86, IA64, MIPS, PPC, SPARC64, SunOS4 oraz Xbox |
| Digital Unix (TruUnix) | Hewlett-Packard (pomimo przejęcia) | 5.1B-5 | Alpha (do 2012 roku) |
| HP-UX | Hewlett-Packard | UNIX System V Release 4 | IA64, PA-RISC (do 2012 roku) |
| IOS | Cisco Systems | 15 | Routery i przełączniki sieciowe firmy Cisco |
| IRIX | Silicon Graphics | 6.5.30 | Systemy SGI, procesory PowerPC |
| Mac OS X | Apple Computer | 10.6.6 | x86, PowerPC oraz ARM v6 |
| NetWare (wyparty przez OES) | Novell | 6.5 SP8 (odpowiednik OES 2) | x86 |
| Open Enterprise Server | Novell | OES 2 SP3 | x86 |
| OpenVMS | Hewlett-Packard (pomimo przejęcia) | 8.4 | Alpha, VAX, IA64 (Itanium) |
| Red Hat Linux | Red Hat | 6 | x86, IA64 |
| SCO Open Server 6 | The SCO Group | 6 | x86 |
| Solaris | Oracle | 11 | SPARC, x86, IA64 |
| Ubuntu | Canonical | 10.10 | x86, IA64 |
| Windows | Microsoft | 2008 R2 | x86, IA64 |
| z/OS (poprzednio MVS) | IBM | 1.12 | IBM zSeries (MVS działa na komputerach Mainframe System 360/390) |

Unix

- Wielozadaniowy, wielużytkownikowy sieciowy system operacyjny z funkcją podziału czasu.
- Zbudowany na bazie jądra które łatwo dostosowuje się do różnej architektury.
- Oddziela operacje jądra od funkcji użytkownika.
- Opracowany w Bell Labs dla AT&T w latach 60.
- W 1972 na jego potrzebny opracowana język C
- Standard przemysłowy.

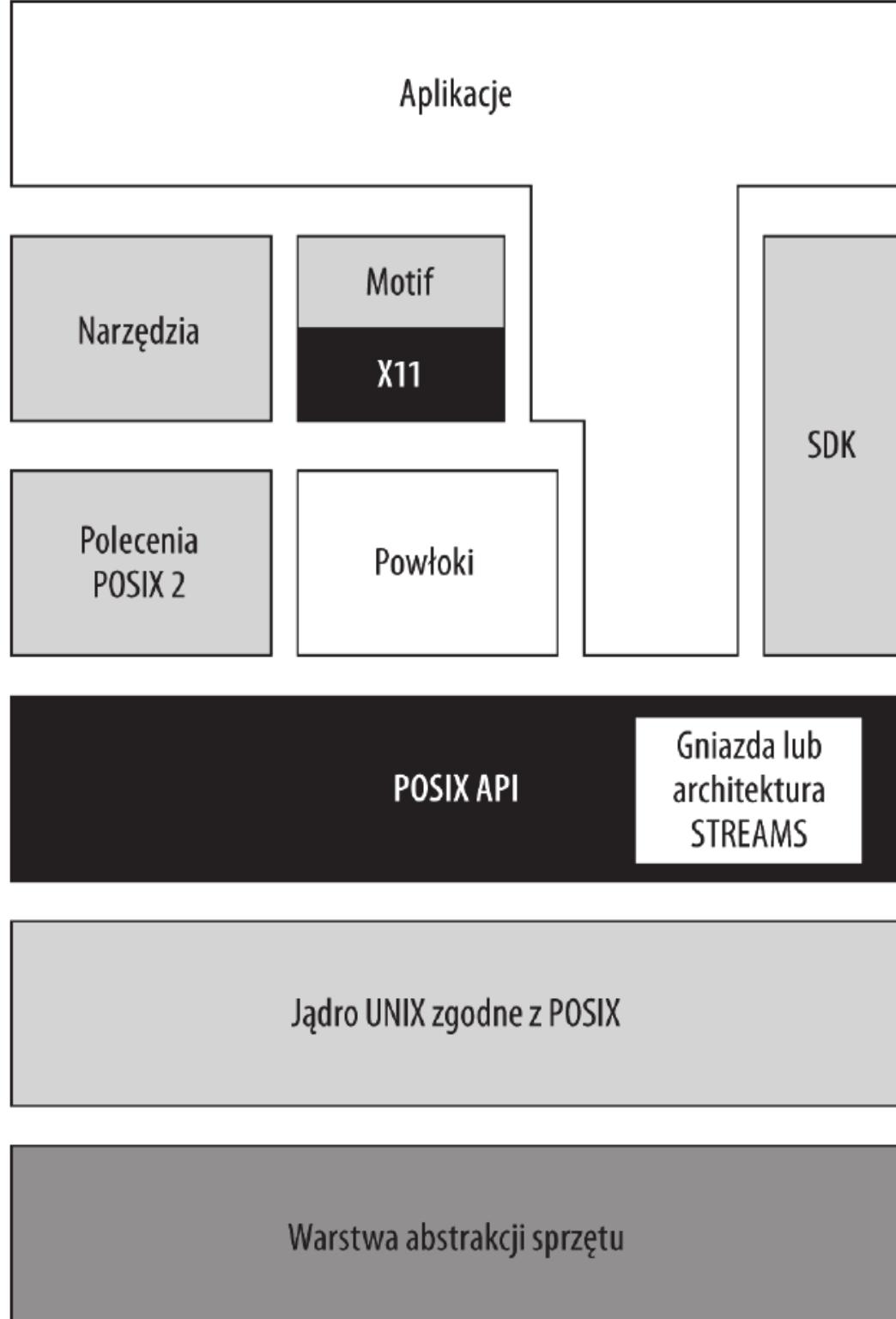


POSIX

- Interfejs systemu Unix oraz standaryzacja wokół języka C ostatecznie doprowadziły do powstania zestawu wskazówek projektowych i API, które stały się architekturą modelu sieciowego systemu operacyjnego. POSIX (ang. Portable Operating System Interface for Unix to API (ang. Application Programming Interface)) zdefiniowane przez standardy IEEE 1003 i ISO/IEC9945.
- POSIX zapewnia systemom sieciowym standaryzację interfejsów programistycznych, użytkownika i właściwości powłok systemów i dlatego został niemal powszechnie zaadaptowany

POSIX

- Funkcje nowoczesnego systemu sieciowego — takie jak hierarchiczny system plików, prze-chowywanie zwykłego tekstu, interpreter wiersza poleceń, komunikacja między aplikacjami i komunikacja między procesami (ang. Inter-Process Communication, IPC), koncepcjapamięci współdzielonej, wiadomości i zapytań, semaforów, gniazd itp. — są wynalazkami wyrastającymi z systemu Unix, chociaż nie stanowiły części oryginalnego systemu Unix



Architektura STREAMS i gniazda

- Architektura STREAMS i gniazda to dwie metody używane przez Unix do ustanowienia interfejsu sieciowego. Ponadto odgrywają one główną rolę w tworzeniu usług sieciowych.

Gniazda

- Gniazdo to punkt końcowy połączenia sieciowego. Kiedy gniazdo pozwala na dwukierun-kowy przepływ danych IP, jest określone mianem gniazda internetowego.
- Gdy gniazdo używa innych typów protokołów, nosi nazwę gniazda sieciowego lub jeszcze prościej — gniazda.
- Gniazda internetowe mają określone właściwości, takie jak używany protokół, przypisany adres IP, numer portu, numer usługi oraz (po nawiązaniu połączenia) zdalny adres IP i zdalny numer portu.
- Wymienione cechy charakterystyczne nadają gniazdom unikalną identyfikację.
- Sieciowe systemy operacyjne wykorzystują koncepcję gniazda jako interfejsu między procesem aplikacji i stosem sieciowym, pozwalając na przepływ danych pomiędzy nimi.

Gniazda

- Prawdopodobnie najbardziej znaną architekturą gniazda sieciowego jest architektura Berkeley Sockets API, która została wprowadzona wraz z BSD UNIX v4.2.
- Obecnie architektura Berkeley Sockets jest uznawana za standardowy model projektu gniazda sieciowego.

Architektura STREAMS

- Architektura STREAMS jest alternatywą dla Berkeley Sockets.
- Po raz pierwszy pojawiła się w UNIX System V używana dla operacji wejścia-wyjścia w celu umożliwienia urządzeniu bądź plikowi specjalnemu systemu na komunikację z urządzeniem za pomocą sterownika tego urządzenia z użyciem standardowych systemowych wywołań wejścia-wyjścia.
- Architektura STREAMS ma konstrukcję modułową i pozwala na łączenie sterowników (które są modułami).
- Obciążenie powodowane przez architekturę STREAMS jest większe niż w przypadku gniazd. W wszystkich systemach operacyjnych używających architektury STREAMS dołączane jest również Sockets API.
- W początkowej specyfikacji Single UNIX Specification architektura STREAMS była komponentem obowiązkowym, natomiast w bieżącej specyfikacji SUS v3 stanowi komponent opcjonalny.

Single Unix specification

- Specyfikacja SUS jest wynikiem wysiłków w celu utworzenia standardu systemu Unix, które zostały zapoczątkowane przez IEEE oraz The Open Group w latach osiemdziesiątych.
- Skutkiem tych działań był standard POSIX.1 (skrót od Portable Operating System Interface for Unix), który wpływał na prace prowadzone nad wieloma systemami sieciowymi w latach osiemdziesiątych i dziewięćdziesiątych w celu utworzenia zestawu standardów Unix.
- Okres ten był znany jako „wojny Unix” i doprowadził niektórych z głównych producentów systemu Unix do założenia COSE (ang. Common Open Software Environment). Największym osiągnięciem COSE było utworzenie środowiska CDE (ang. Common Desktop Environment), które łączyło środowisko X11 z interfejsem użytkownika OSF Motif oraz pakietem narzędziowym.

Specyfikacji SUS

- Specyfikacja SUS dostarczyła zestawu interfejsów użytkownika oraz oprogramowania, które stanowiły standard programowania w powłoce POSIX.
- Ponadto opracowana została pewna liczba systemowych narzędzi i usług, włączając w nie plik, terminal oraz usługi sieciowe.

Linux

- Linux jest systemem operacyjnym z rodziny Unix, używającym jądra Linux dostępnego jako open source.
- Obecnie pod kontrolą systemu Linux działa największa liczba serwerów internetowych, jak wynika z danych statystycznych dotyczących wykorzystywania internetu.
 - połowa serwerów WWW działa pod kontrolą różnych wersji systemu Linux,
 - FreeBSD to około 30%,
 - natomiast pozostałe 20% należy do Windows Server.
 - Inne badania, przeprowadzane na podstawie sprzedaży sprzętu i uwzględniające cały rynek serwerowy, wskazują, że Linux ma w nim około piętnastoprocentowy udział.

- Linux jest zainstalowany na 91,8% najpotężniejszych superkomputerów, wymienionych na liście Top 500 Supercomputer Sites
- Przy użyciu systemów Linux zbudowana jest duża liczba ważnych witryn internetowych, łącznie z czterema największymi: Amazon, eBay, Google oraz Yahoo!.
- W niektórych krajach Linux stał się standardowym systemem operacyjnym dla rządów. Przykładami takich krajów są Brazylia, Rosja, Indie, Chiny, Niemcy oraz Francja.



debian **ubuntu**
linux for human beings



redhat



CentOS



fedora



Mandriva



slackware
linux



FreeBSD



PCBSD



opensolaris



suse

LAMP

- Linux jest często instalowany na sprzęcie przemysłowym i pozwala na osiągnięcie dużej skalowalności przez skalowanie poziome.
- Wiele serwerów Linux ma zainstalowane oprogramowanie nazywane LAMP.
- Pakiet LAMP składa się z następujących komponentów:
 - Linux — system operacyjny;
 - Apache — serwer WWW;
 - MySQL — serwer bazy danych;
 - P — jeden z języków programowania lub języków skryptowych: PHP, Perl lub Python.

Solaris

- System operacyjny Solaris firmy Oracle (dawniej Sun2) to obecnie najczęściej używany sieciowy system operacyjny Unix.
- Solaris został zaprezentowany w roku 1992 w celu zastąpienia systemu operacyjnego SunOS i wprowadził zaawansowany stos sieciowy obsługujący sieci TCP/IP.
- Solaris istnieje w dwóch wersjach:
 - działającej w systemach komputerowych bazujących na procesorach SPARC firmy Oracle
 - w wersji x86 działającej na standardowej architekturze Intel.
- Firma Sun uznała Solaris za jeden z podstawowych sieciowych systemów operacyjnych dla dużych przedsiębiorstw, jak również za preferowaną platformę dla sieci pamięci masowej.

Solaris

- Dostępny bezpłatnie docelów testowych i niekomercyjnych.
- Solaris można zainstalować w postaci serwera lub stacji roboczej.
- Istnieje możliwość instalacji wyłącznie podstawowych usług sieciowych, użytkownika, programisty bądź też instalacji całego pakietu, zawierającego oprogramowanie niezbędne do zarządzania siecią oraz narzędzia do zarządzania jej polityką.

- Oryginalny stos sieciowy w systemie Solaris 1.x bazował na wersji BSD.
- Aby poprawić wydajność Solarisa, w wersji Solaris 2.x stos sieciowy przeniesiono na architekturę AT&T SVR4.
- Różne wersje 2.x kontynuowały przejście w kierunku stosu sieciowego STREAMS, który stał się podstawą dla funkcji sieciowych w UNIX System V.
 - Architektura STREAMS jest znana zarówno ze względu na swoją modułową naturę, jak i możliwość przekazywania komunikatów między modułami.
 - Tworzenie połączenia w architekturze STREAM wiąże się ze znaczącym obciążeniem, ale w przypadku długich sesji powiązanych z protokołami takimi jak FTP i NFS obciążenie to nie stanowi problemu.

- Do późnych lat dziewięćdziesiątych serwery i stacje robocze Sun były najczęściej stosowaną platformą zarówno do routingu, jak i w przypadku aplikacji serwerowych, na których działało oprogramowanie serwerów WWW.
- Protokoły internetowe, w szczególności HTTP, są krótkotrwałymi połączeniami, a architektura STREAM pokazuje tutaj swoje wady.
- Podczas prac nad systemem Solaris 10 firma Sun dokonała przebudowania swojego stosu sieciowego.

- Stos sieciowy w systemie operacyjnym Solaris 10 został przebudowany z użyciem architektury „FireEngine”, która połączyła wszystkie warstwy protokołów w pojedynczy moduł STREAM wraz z pełną obsługą wątkowania.
- Mechanizm określany jako Vertical perimeters pozwala na synchronizację per-procesor w module TCP/IP, co jest wdrożone przy użyciu queue.
- Obsługuje system plików NFS 4.0 i został zaprojektowany w celu obsługi sieci o przepustowości do 10 Gb/s.

- Solaris ma również możliwość dołączania systemu plików ZFS (jego początkowa nazwa kodowa to Zettabyte File System), który oferuje kilka unikalnych funkcji przemysłowych.
- ZFS obsługuje bardzo duże wielkości woluminów oraz integruje system plików wraz z zarządzaniem woluminami.
- Oprócz wbudowanych funkcji tworzenia kopii migawkowych i pełnych system ZFS zawiera także schemat replikacji o nazwie RAID-Z.
 - Technologia ta traktowana jako całość ma pewne unikalne możliwości w zakresie automatycznej naprawy

- System Solaris jest dostarczany wraz z narzędziem o nazwie DTrace (ang. Dynamic Tracing), które diagnozuje wydajność aplikacji sieciowych oraz wykrywa miejsca występowania potencjalnych wąskich gardeł.
- Informacja ta może być przekazana do podsystemu zarządzającego awariami, odpowiedzialnego za usunięcie problemu, optymalizację i (lub) zgłoszenie administratorom systemu.

Novell NetWare oraz Open Enterprise Server

- Oprogramowanie NetWare firmy Novell miało bardzo ważną pozycję w czasie opracowywania sieciowych systemów operacyjnych.
- Przez niemal dekadę NetWare był najważniejszym systemem sieciowym dla komputerów PC, w szczególności dla serwerów plików i wydruku oraz sieci heterogenicznych zawierających różne typy klientów.

- Kiedy Microsoft Windows Server i serwery Linux stały się popularniejsze firma Novell skoncentrowała swoje wysiłki programistyczne
 - na narzędziach zarządzania siecią (ZenWorks),
 - usługach katalogowych klasy przemysłowej (eDirectory)
 - oraz innych produktach, które reprezentowały aktualny stan rozwoju w tej dziedzinie.
- Oprogramowanie NetWare 6.5 zostało zastąpione przez Open Enterprise Server (OES), które w wersji 2 SP1 bazuje na jądrze NetWare 6.5 SP8.
 - System OES 1 pojawił się w marcu 2005 roku, natomiast wersja OES 2 SP3 została wydana w grudniu 2010 roku.

- OES 2 to system sieciowy, który może działać na bazie jądra NetWare albo Linux.
- Novell umieścił OES jako rozwiązanie przemysłowe do obsługi serwera plików, serwera wydruku, usług katalogowych oraz aplikacji sieciowych.
- Na bazie jądra NetWare - OES-NetWare i umożliwia dodanie modułów NLM (ang. NetWare Loadable Modules).
- NLM = różne aplikacje: Apache, eDirectory, GroupWise, iPrint, NSS, OpenSSH, Tomcat oraz innych.

Windows Server

- Windows Server jest uznawany za serwer ogólnego przeznaczenia, który oferuje najlepszą i najszerszą obsługę aplikacji sieciowych ze wszystkich.
- Ogromną liczbą cennych funkcji, takich jak zautomatyzowana implementacja, zarządzanie polityką (ang. policy engine) sieciowego systemu operacyjnego oraz inne dostępne funkcje.

- Pod marką Microsoft Server firma Microsoft sprzedaje także rozbudowany zestaw aplikacji serwerowych.
- Przykłady produktów Microsoft Server to między innymi:
 - Biz Talk Server,
 - Commerce Server,
 - Exchange Server,
 - Internet Information Server (dołączony do Windows Server),
 - ISA Server,
 - SQL Server,
 - Windows Storage Server (w postaci oddzielnego wydania Windows) itp.

- Różne wersje Windows Server obejmują produkty od Windows Home Server,
 - przez Windows Small Business Server,
 - aż do Windows Datacenter Edition.
- Spośród wszystkich produktów
 - Microsoft Exchange osiągnął najwyższą pozycję na rynku poczty korporacyjnej,
 - SQL Server to najlepiej sprzedający się komercyjny serwer bazy danych klasy przemysłowej.

Usługi katalogowe i domeny

- Usługi katalogowe odgrywają ważną rolę w bieżącej architekturze klient-serwer sieciowych systemów operacyjnych.
- Zapewniają
 - usługi nazw,
 - przechowują informacje na temat obiektów w sieci
 - pozwalają na przekazywanie tych informacji dalej, do innych serwerów i aplikacji.
- Obecnie w użyciu jest wiele usług katalogowych, a nowoczesne sieci bardzo intensywnie z nich korzystają.

Domena

- Najmniejszą podstawową jednostką w usłudze katalogowej jest domena.
- Domena to zbiór systemów współdzielących tę samą bazę danych bezpieczeństwa.
- Domeny mogą być różnych typów i zawierać takie elementy, jak jednostki organizacyjne, konta użytkowników i komputerów, a także inne obiekty, do których można uzyskać dostęp za pomocą unikalnej nazwy.

Usługi katalogowe i domeny

- Duże sieci komputerowe stanowią problem dla projektantów sieciowych systemów operacyjnych działających w modelu klient-serwer.
 - W jaki sposób zarządzać ogromną liczbą systemów, użytkowników, urządzeń peryferyjnych oraz innymi elementami znajdującymi się w sieci?
 - Rozwiązanie sprowadza się do takiego przechowywania informacji w bazie danych położonej w pewnym miejscu sieci, aby dostęp do tych informacji był szybki i niezawodny.
 - Oprogramowanie zarządzające takimi informacjami nosi nazwę usługi katalogowej, a podstawowa jednostka używana do przechowywania informacji sieciowych nosi nazwę domeny. Domena jest zwykle powiązana z własną bazą danych bezpieczeństwa.
-

- Sieciowe bazy danych, które zostały zaimplementowane jako usługi katalogowe, działają na zasadzie podobnej do słownika. Są one bliskie idei książki telefonicznej; w wielu ogromnych projektach baz danych słowo katalog zostało zastosowane w latach siedemdziesiątych.
- Ponieważ katalog ten opracowano w celu dostarczania usługi sieciowej, ostatecznie zaczęto stosować pojęcie usługi katalogowe. Standaryzacja usług katalogowych w postaci kilku modeli przemysłowych doprowadziła do rozprzestrzenienia się usług katalogowych we wszystkich sieciowych systemach operacyjnych.
- Ponadto spowodowała zastosowanie ich w ogromnych aplikacjach przemysłowych, służących do zarządzania przechowywanymi danymi różnych rodzajów.

- Ponieważ informacje przechowywane w centralnych sieciowych bazach danych niewątpliwie są poufne, muszą być odpowiednio chronione, a ochrona tych danych musi być w pełni powiązana z centralnym magazynem informacji i za jego pośrednictwem zarządzana.
- Niektóre usługi katalogowe traktują bezpieczeństwo sieci jako jedną całość, podczas gdy inne współpracują z zewnętrznymi systemami bezpieczeństwa.

- Usługa katalogowa może być zbudowana za pomocą dowolnego rodzaju bazy danych:
 - pliku jednorodnego, relacyjnie, hierarchicznie, na zasadzie „równy z równym” itd.
- Najpopularniejsze usługi katalogowe to takie, które są półrelacyjne, hierarchiczne, wysoce skalowalne i przechowują obiekty danych.
- Skalowalność jest ważnym czynnikiem, ponieważ zawsze występuje potrzeba zachowania wszystkich informacji wraz z rozwojem.

- Wprawdzie usługa katalogowa jest podobna do bazy danych, ale istnieją pewne istotne różnice.
 - Informacje usługi katalogowej są odczytywane znacznie częściej, niż są w niej zapisywane. Dlatego też nie jest konieczne stosowanie mechanizmów takich jak wycofywanie transakcji.
 - Poza tym usługi katalogowe nie mają takich samych wymagań w zakresie wydajności i normalizacji (optymalizacji) jak w przypadku relacyjnych baz danych. Można się przekonać, że wiele usług katalogowych tworzy w wielu miejscach powtarzające się zbiory danych, o ile może to przyczynić się do zwiększenia wydajności. Relacyjna baza danych może
 - Usługa katalogowa może być wykorzystywana do przechowywania różnorodnych danych, powiązanych ze sobą w losowy sposób, a więc wymaga mniej strukturalnego schematu.

Banyan VINES

- Obszar usług katalogowych zawdzięcza bardzo wiele opracowaniu Banyan VINES, powstałemu we wczesnych latach osiemdziesiątych. VINES to skrót od Virtual Integrated NEtwork Service; był to sieciowy system operacyjny bazujący na systemie Unix.
- W swoim stosie sieciowym system VINES używał bardzo popularnego w tamtych czasach zestawu protokołów XNS (ang. Xerox Network Services) i miał wbudowany wariant o nazwie VIP (ang. VINES Internetwork Protocol).
- Sieci VINES bazowały na pakietach, używały automatycznego adresowania klientów oraz miały protokół routingu i protokół kontroli internetu.
- Protokoły warstwy górnej aplikacji zawierały standardowe usługi plików oraz wydruku.
- Żadna z tych technologii nie jest szczególnie interesująca. Jednak system VINES był unikalny dzięki StreetTalk, usłudze nazw wysokiego poziomu.

- Większość nowoczesnych usług katalogowych bazuje na standardzie X.500.
 - Wersja LDAP dla X.500 została utworzona dla sieci TCP/IP i jest używana w większości obecnie dostępnych produktów.
- Microsoft Active Directory (AD) to najlepiej znana i najczęściej używana usługa katalogowa.
 - Technologię AD zbudowano w celu przechowywania obiektów różnego typu z uwzględnieniem aspektów bezpieczeństwa.

- Usługa StreetTalk była jedną z wczesnych usług katalogowych.
- W rozproszonej, replikowanej bazie danych tworzyła przestrzeń nazw dla całej sieci i pozwalała różnym sieciom na współdzielenie zasobów.
- W technologii StreetTalk adres był tworzony na podstawie hierarchicznego schematu nazw, odwzorowującego hierarchię obiektu, i miał postać obiekt@grupa@organizacja.
- Obiekt mógł być udziałem sieciowym, drukarką sieciową bądź kontem użytkownika.
- W tamtym czasie oprogramowanie klientów działało w systemach MS-DOS i Windows 3.x. W sieci VINES nie występowały domeny.

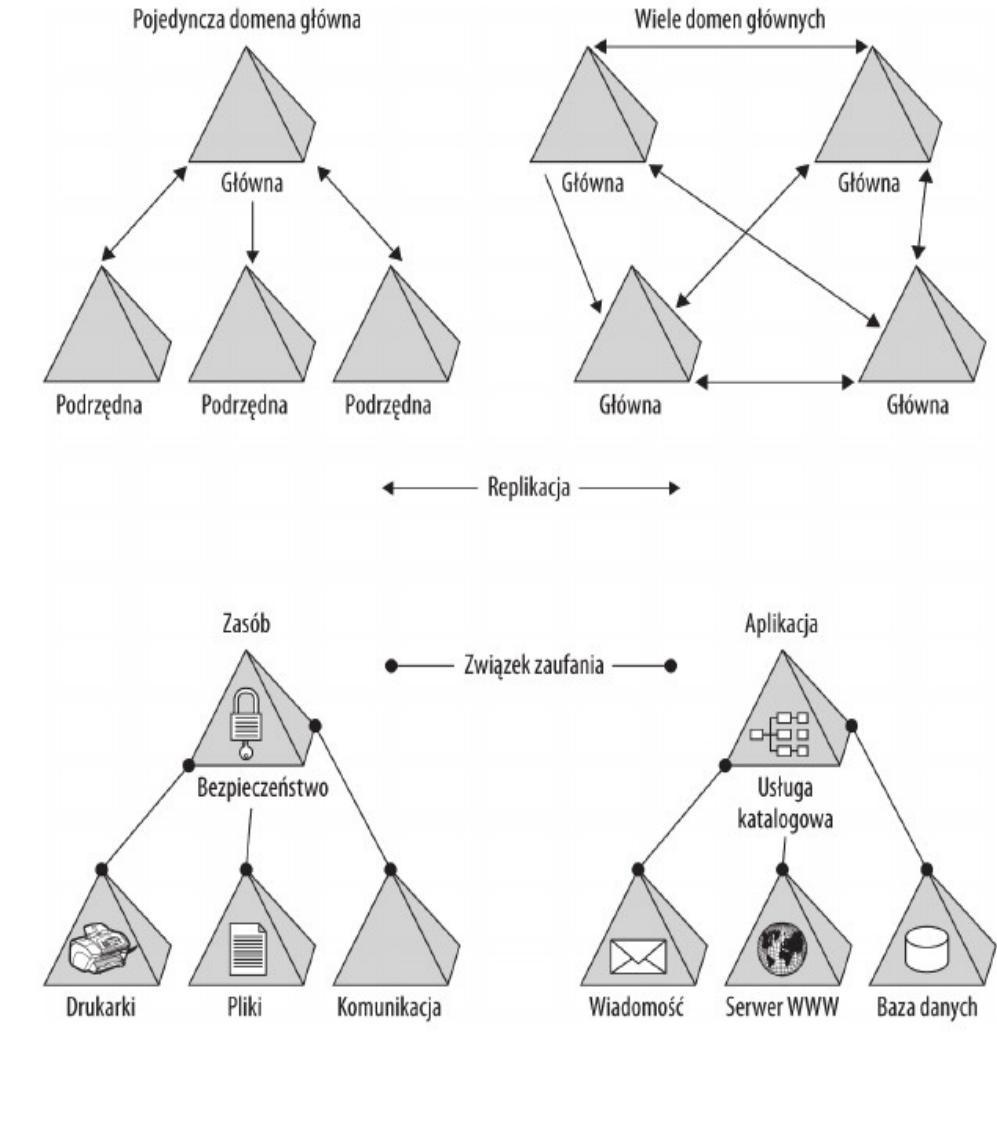
Domena

- Każdy system informacji jest zorganizowany wokół jednostki podstawowej.
- W usłudze katalogowej będzie to domena.
- Domena sieciowa opisuje grupę systemów i powiązanych z nimi zasobów, które są zorganizowane przez usługę katalogową i współdzielą bazę danych bezpieczeństwa oraz model bezpieczeństwa.

Typy domen

Istnieje wiele różnych schematów używanych do organizowania typów domen. Wśród najczęściej spotykanych można napotkać:

- centralna domena główna zorganizowana z domenami podrzędnymi w strukturę
- drzewa, hubu bądź gwiazdy, tzw. „pojedyncza domena główna”;
- struktura wielu domen głównych;
- domeny zasobów;
- domeny zdalne, gdzie łącza przedstawiają zaufane związki i (lub) replikacje, są połączone siecią WAN;
- domeny charakterystyczne dla aplikacji.



Wzajemna współpraca

- Migracja usługi katalogowej utworzonej dla dużej sieci do innej usługi katalogowej to jedno z najboleśniejszych zadań dla zespołu IT organizacji, które musi być wykonane.
- Z dwóch powodów zadanie to okazuje się znacznie trudniejsze niż przeniesienie danych z jednej, przemysłowej bazy danych do innej.
 - Pierwszy — większość baz danych jest dostarczana z funkcjami eksportu i importu albo istnieją dla nich narzędzia firm trzecich, pozwalające na wykonanie tego rodzaju operacji.
 - Drugi — usługi katalogowe są powiązane z funkcjami bezpieczeństwa oraz strukturami własnościowymi, co znacznie utrudnia rozgryzienie i wyodrębnienie danych znajdujących się w usługach katalogowych.

- Heterogeniczna usługa katalogowa przechowuje informacje o systemach działających podkontrolą różnych systemów operacyjnych, co jest funkcją cenną z wielu powodów.
- Sposób, w jaki obce systemy są przedstawiane w usłudze katalogowej, pokazuje, ile producent tego systemu katalogowego włożył pracy, aby osiągnąć dany efekt.
- W przypadku wielu usług katalogowych heterogeniczność niekoniecznie będzie zaletą, a preferowana będzie homogeniczność.

- Wcale nie tak rzadko można się spotkać z sytuacją, w której wiele usług katalogowych działa na różnych serwerach znajdujących się w całej sieci.
- Usługa katalogowa istnieje dla każdego ważniejszego sieciowego systemu operacyjnego.
- Wiele z nich może być powiązanych z serwerami WWW, na przykład Apache, podczas gdy inne mogą być częścią korporacyjnego programu do obsługi poczty elektronicznej.

Serwery domen

- System komputerowy, w którego ramach działa usługa katalogowa, jest nazywany serwerem domen sieci lub kontrolerem domen.
- Ze względów bezpieczeństwa niemal wszystkie usługi katalogowe przechowują swoje dane oraz powiązane z nimi informacje bezpieczeństwa w tym samym serwerze domen.

- W małych sieciach serwery domen poza usługą katalogową mogą oferować także kilka innych usług.
- Przykładem tego rodzaju systemu jest Microsoft Small Business Server (SBS): usługi katalogu AD, DHCP, DNS, Exchange Server, IIS Web Server, ISA (Microsoft Internet Security and Acceleration) oraz SQL Server.

- W zależności od natury domeny i usługi katalogowej, a także przeprowadzanych zadań, domena może mieć jeden serwer domen dla dwóch lub trzech systemów.
- W przypadku tej wielkości sieci wprowadza się na rynek wiele serwerów domowych bazujących na systemie Linux.
- W ogromnych sieciach serwer domen może obsługiwać od 50 do 500 systemów.
- Inne serwery w domenie, które nie są serwerami domen, są nazywane serwerami zasobów i aplikacji.
 - Mogą mieć także inne określenia w zależności od wykonywanych zadań: serwer plików i wydruku, serwer tworzenia kopii zapasowej, serwer odpowiedzialny za bezpieczeństwo lub jakikolwiek inny wymagany przez serwer usługi katalogowej.

Usługi katalogowe

- Usługi katalogowe przechowują metadane, czyli dane dotyczące danych.
- W obiektowej bazie danych przechowującej dane sieciowe metadane dostarczają kontekstu pozwalającego systemowi na określenie sposobu organizacji danych.
- Schemat katalogu definiuje zestaw klas obiektu, do których są przypisane zestawy atrybutów wymaganych bądź opcjonalnych.
- Kiedy to tylko możliwe, większość usług katalogowych używa klas obiektu, atrybutów i numerów identyfikacyjnych, które są zarejestrowane przez IANA (ang. Internet Assigned Numbers Authority) jako standardy.
- Każdy obiekt będący zasobem chronionym jest dołączony do listy ACL (ang. Access Control List), która określa, kto może używać tego obiektu.

- Usługa katalogowa staje się konieczna, kiedy względem sieci zostają wysunięte następujące wymagania:
 - scentralizowane zarządzanie usługami sieciowymi;
 - zdefiniowana polityka bezpieczeństwa wraz z odpowiednio dobranymi uprawnieniami;
 - możliwość przydzielenia różnym osobom odpowiedzialności za określone zasoby;
 - możliwość skalowania sieci w celu obsługi większej liczby użytkowników, niż jest obsługiwana w modelu „równy z równym”;
 - możliwość obsługi różnorodnych klientów oraz systemów operacyjnych;
 - możliwość przeprowadzania nadzoru zdarzeń sieciowych.

Wady

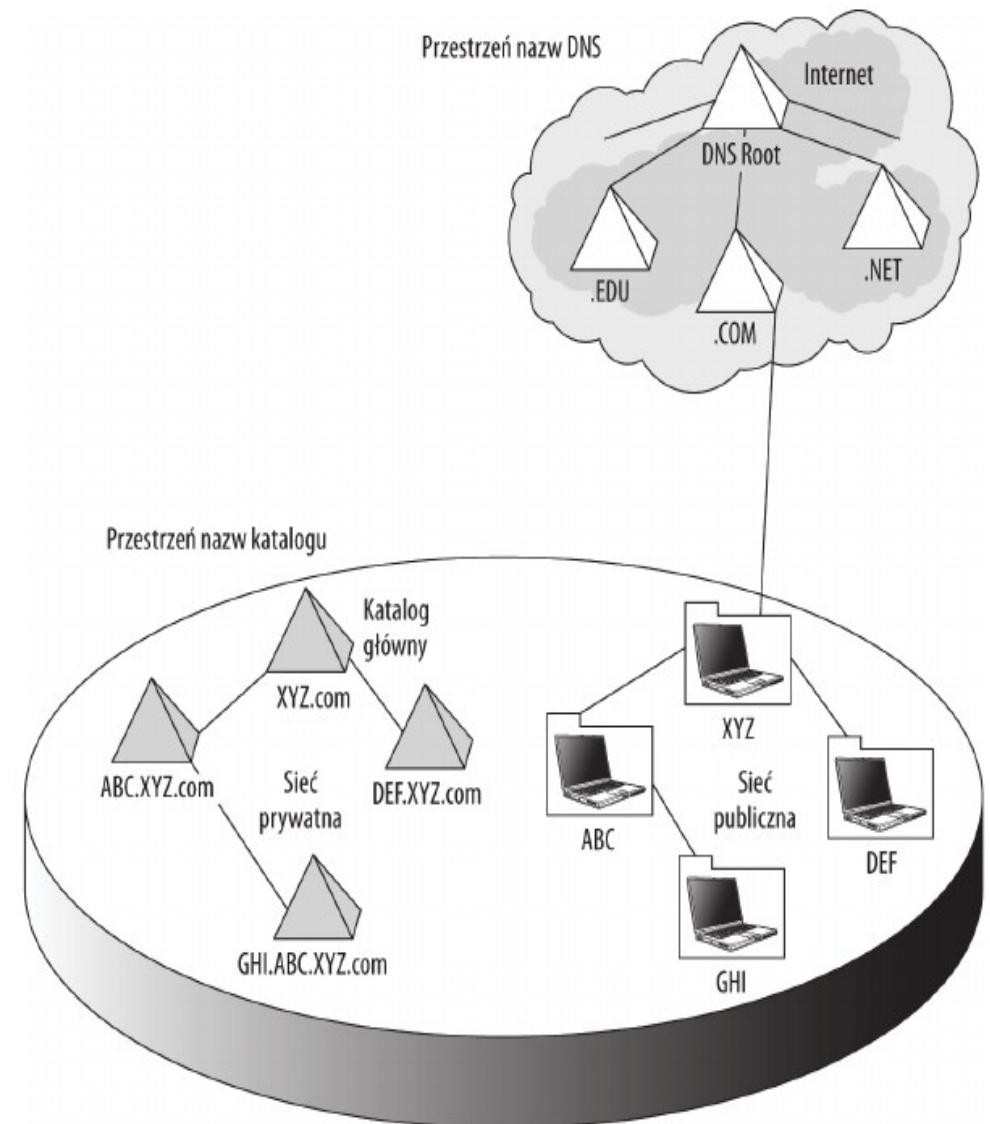
- Usługi katalogowe mają nie tylko zalety, lecz także pewne wady.
- Oprócz dodatkowego kosztu i zwiększenia stopnia skomplikowania sieci do prawidłowego funkcjonowania usługi katalogowe wymagają również usług domeny, które zawsze powinny być dostępne w sieci.
- W większości przypadków te dodatkowe wymagania ograniczają wykorzystanie domen w sieciach domowych i małych biurach, gdzie podłączonych jest mniej niż 20 systemów.

Przestrzeń nazw

- Usługa katalogowa definiuje przestrzeń nazw dla wszystkich przechowywanych obiektów.
- Aby zapewnić efektywność, przestrzeń nazw musi tworzyć unikalne oznaczenie, które powinno być logicznym połączeniem różnych gałęzi drzewa.
 - W przypadku DNS będzie to URI (ang. Uniform Resource Identifier).

- Wiele organizacji zastosowało dla domen schemat nazw odpowiadający sposobowi, w jaki DNS oznacza strukturę katalogów witryny internetowej.

- możliwość późniejszego udostępnienia w internecie struktury domeny bez konieczności wprowadzania znaczących zmian w nazewnictwie.



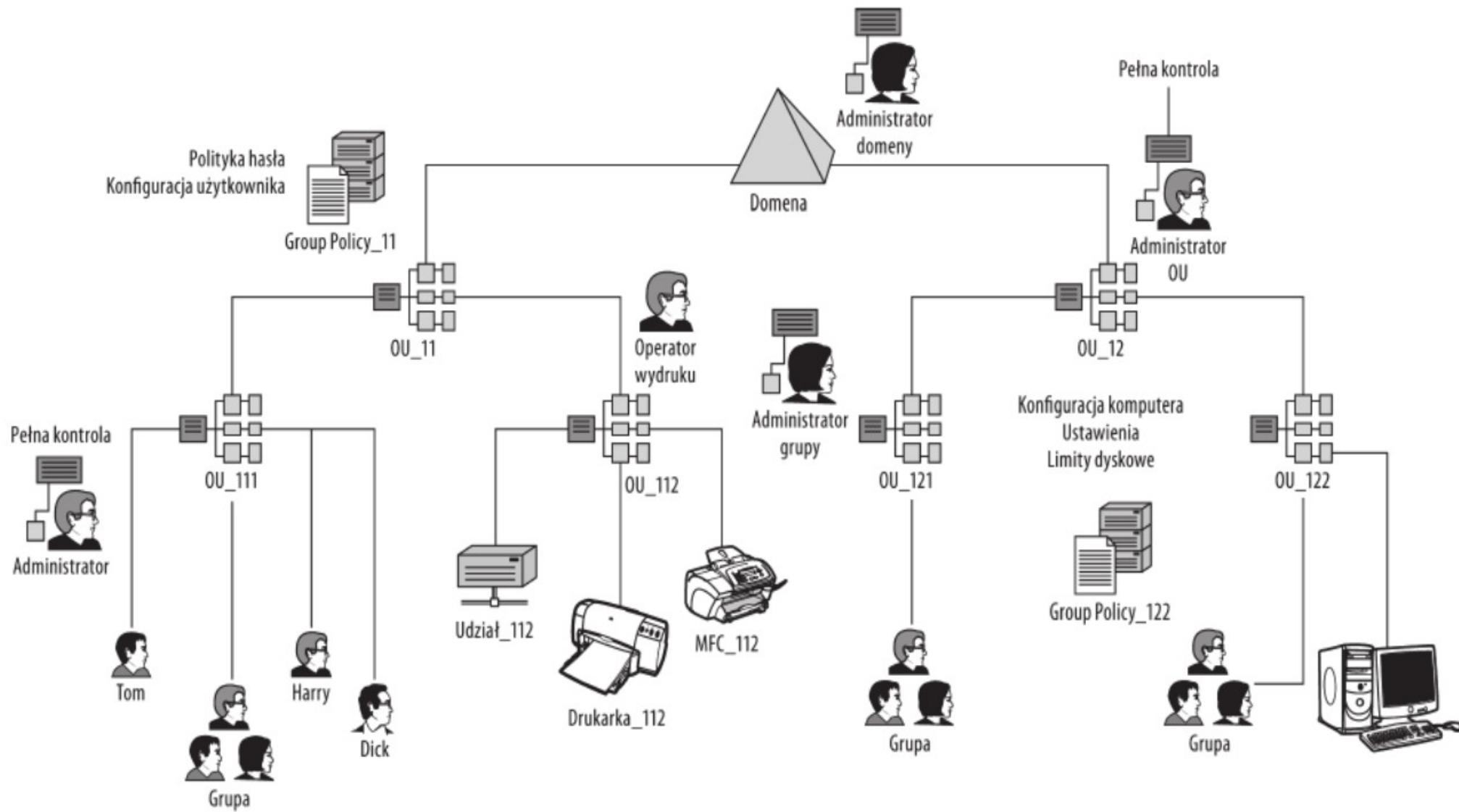
- Jeżeli w sieci prywatnej ma być używana publiczna przestrzeń nazw DNS,
 - na przykład .com, .gov lub .edu,
- to trzeba się upewnić, że wewnętrzne i zewnętrzne nazwy domen nie kolidują ze sobą.
- Publiczny serwer DNS powinien być skonfigurowany w celu przekazywania żądań adresów do wewnętrznego serwera DNS sieci prywatnej.

Polityka

- Podczas przechowywania w bazie danych obiektów z informacjami sieciowymi możliwe jest utworzenie zestawu reguł, które będą określały sposób używania tych obiektów.
- Wspomniane reguły są przechowywane oddzielnie od mechanizmu bezpieczeństwa wykorzystywanego przez sieciowy system operacyjny, choć niektóre reguły mogą się wzajemnie nakładać.

- Polityka będzie definiowała pewne zachowanie sieciowe, włączając w to między innymi:
 - konfigurację systemu klienta;
 - częstotliwość przeprowadzania aktualnień i instalacji poprawek;
 - zachowanie mechanizmu nadzoru;
 - stopień skomplikowania haseł;
 - zadania przeprowadzane w trakcie operacji logowania i wylogowania.

- Najbardziej znaną usługą zarządzania polityką jest Group Policies firmy Microsoft (przechowywana w Active Directory).
- SRM (ang. Solaris Resource Manager) firmy Sun oferuje zarządzanie polityką ustawiania ograniczeń zasobów.
 - Za pomocą SRM można określić maksymalną liczbę dozwolonych procesów, połączonych użytkowników, liczbę operacji logowania itp.
 - Za pomocą skryptów SRM może wprowadzać nowe zasady polityki tuż po uruchomieniu systemu operacyjnego.
 - Każdy sieciowy system operacyjny implementuje pewną formę zarządzania polityką.
- Po rozpoczęciu przeglądania usług zarządzania polityką oferowanych przez firmy trzecie można się przekonać o dostępności ogromnej ilości rozwiązań.



Server IDA

Serwer IDA (ang. Identity and Access) musi funkcjonować w różnych systemach sieciowych, aby mógł być użyteczny.

- W przypadku serwera IDA może być konieczne zapewnienie obsługi następujących funkcji:
 - Zarządzanie certyfikatami oraz kartami smart card, a także połączeniami z różnymi usługami certyfikacji.
 - Zapewnienie federacyjnej usługi wśród wielu usług katalogowych znajdujących się w sieci; zadaniem tej usługi będzie przekazywanie tożsamości między nimi.
 - Najważniejsze usługi katalogowe, których obsługę należy zapewnić, to Microsoft Active Directory, Sun Directory Server, Novell eDirectory oraz IBM Tivoli Directory Server.
- Praca z usługami tożsamości poczty elektronicznej i komunikatorów internetowych oraz zapewnienie ich synchronizacji, jeśli to konieczne.
 - Lotus Notes i Microsoft Exchange to przykłady dwóch serwerów przechowujących tożsamości, które często współpracują z tożsamościami innych usług katalogowych.
- Zarządzanie tożsamościami sieciowej bazy danych tak, aby użytkownik nie mógł się do niej zalogować bez ważnej tożsamości.
 - Oracle, IBM DB2 oraz Microsoft SQL Server to przykłady systemów zarządzania bazami danych, które mogą przechowywać własne konta użytkowników.
- Praca z aplikacjami korporacyjnymi, takimi jak SAP, aplikacje telefoniczne itd.

X500

- Przemysł telekomunikacyjny utworzył standard w celu umożliwienia współpracy różnych katalogów.
- Standard ten nosi nazwę X.500 Directory Access Protocol (DAP). Protokół ten jest akceptowany przez sieć dowolnego rodzaju. Standard DAP może przechowywać informacje o obiektach dowolnej z siedmiu warstw modelu ISO/OSI.
- W protokole X.500 klient może wykonać zapytanie do serwera w usłudze katalogowej, używając DAP do komunikacji.
- Następnie DSA (ang. Directory System Agent), czyli baza danych przechowująca informacje, udziela odpowiedzi na to żądanu. Bazy danych DSA są hierarchiczne i połączone ze sobą za pomocą drzewa DIT (ang. Directory Information Tree).
- Z kolei DUA (ang. Directory User Agent) to program taki jak whois, finger bądź polecenie GUI uzyskujące dostęp do DSA

NIS

- NIS (ang. Network Information Service) to bazujący na RPC system katalogowy klient-serwer przechowujący w bazie danych nazwy użytkowników i systemów dla komputerów w sieci.
- Ponadto NIS definiuje zestaw procesów używanych w celu zarządzania i uzyskiwania dostępu do usługi katalogowej.
- Za pomocą NIS administrator może zdefiniować domenę NIS współdzielącą zestaw powszechnie używanych plików konfiguracyjnych.
- Operacje dodawania tych plików konfiguracyjnych do nowych systemów lub ich modyfikacja mogą być przeprowadzane zdalnie i są względnie łatwe.

Serwery LDAP

- Obecnie niemal wszystkie nowoczesne usługi katalogowe bazują na protokole LDAP, który zapewnia możliwość współdziałania.
- Dwoma wyjątkami, o których trzeba tutaj wspomnieć, są DNS (ang. Domain Name System) i NIS (ang. Network Information System), opracowane przed powstaniem standardu X.500 i LDAP.
- Lista kilku z wielu usług katalogowych bazujących na LDAP:
 - Microsoft Active Directory
 - Novell eDirectory (wcześniej NDS, czyli NetWare Directory Services);
 - Fedora Directory Server;
 - OpenDS;
 - Oracle Directory Server Service Plus;
 - IBM Tivoli Directory Server;
 - Apple Open Directory;
 - ApacheDS.

LDAP – nazwy wyróżniające

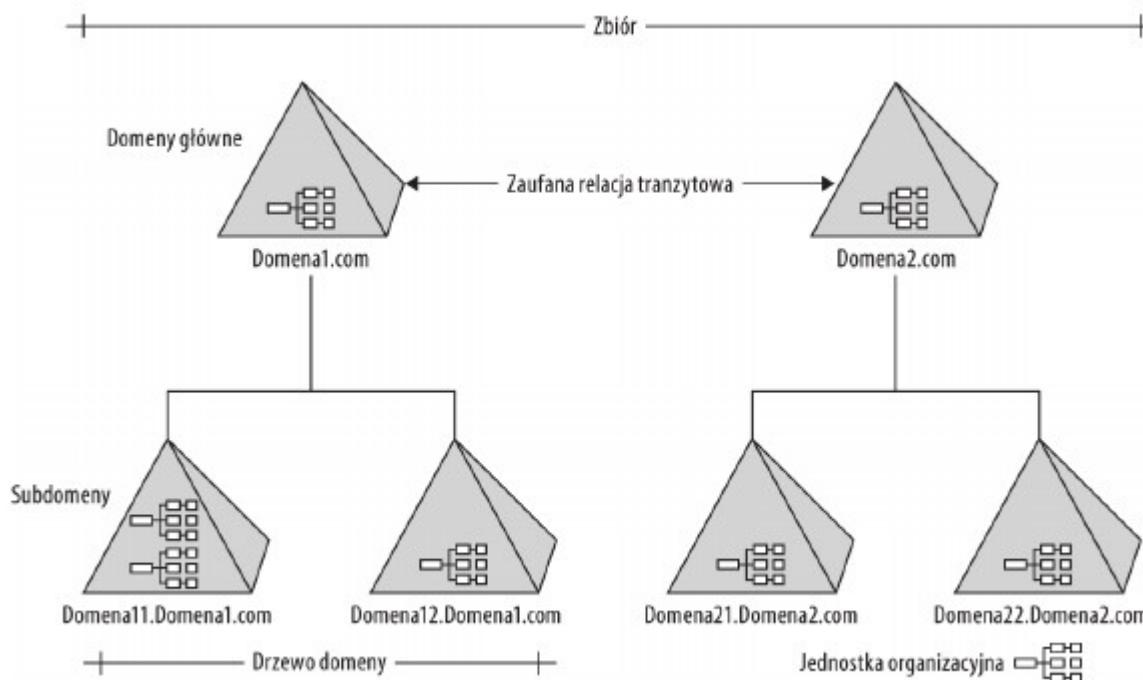
Wszystkie katalogi LDAP współdzielą zestaw zdefiniowanych obiektów oraz powszechnych metod adresowania, które tworzą nazwę wyróżniającą (ang. Distinguished Name, DN) dla obiektu. Funkcje katalogu LDAP to:

- **Drzewo katalogu.** Hierarchiczne drzewo wraz z obiekta katalogu jako węzłami.
- **Węzły.** Węzły to nazwane obiekty pojemników bądź jednostek, którym przypisano zestaw właściwości lub atrybutów. LDAP pozwala na to, aby obiekty miały możliwości rozszerzania, czyli definiowania dodatkowych właściwości.
- **Atrybuty.** Atrybut jest właściwością, której nazwa jest uznawana jako typ lub opis. Atrybuty mogą mieć jedną lub wiele wartości.
- **Wpisy.** Wpis stanowi unikalny egzemplarz typu obiektu. Obiekt może mieć przypisaną nazwę wyróżniającą i przez porównanie z jego węzłem nadziednym może mieć przypisany RDN (ang. Relative Distinguished Node).

LDAP – nazwy wyróżniające

- Nazwa wyróżniająca jest bardzo ważna, ponieważ pozwala systemowi na wyszukanie i pobranie informacji.
- Dzięki nazwie wyróżniającej wiadomo, w jaki sposób obiekt jest powiązany z wieloma innymi obiektami.
- Ogólnie rzecz biorąc, to sposób zapewnienia relacji „jeden do wielu”, która nie jest bezpośrednio obsługiwana w usługach katalogowych.

- Kolekcja domen może być ze sobą połączona w postać zbioru — każda domena będzie miała własną bazę danych bezpieczeństwa.
- Aby w sieci możliwa była komunikacja użytkowników i systemów w różnych domenach, trzeba nawiązać zaufaną relację.
- **Kontrolery domen w zbiorze** zawierają informacje o innych domenach w zbiorze dzięki użyciu **replikacji**.
- Zaufana **relacja tranzytowa** spełnia następujący warunek: jeśli automatyczna zaufana relacja istnieje między domenami A i B oraz B i C, to zaufana relacja istnieje również między domenami A i C.



[MEMYTUTAJ.PL](#)

DZIĘKUJĘ ZA UWAGĘ

**WSZYSTKIM KTÓRZY NIE
ZASNĘLI :)**

Tworzenie narzędzi sieciowych z wykorzystaniem Python, C/C++

- Python posiada wbudowany moduł o nazwie **socket**, który zawiera wszystkie niezbędne definicje i funkcje pozwalające na otwieranie gniazd i komunikację sieciową z ich wykorzystaniem.

Czym są sockety (gniazda)?

- Jest to pewien mechanizm umożliwiający otwarcie kanału komunikacji pomiędzy hostami. Każde gniazdo posiada adres IP oraz numer portu i może przesyłać trzy rodzaje pakietów

datagramy

- datagramy (pakiety UDP) — są to tzw. „datagram sockets” — ten kanał komunikacji wykorzystuje protokół UDP, czyli połączenie jest bezstanowe. Gniazdko wysyła pakiet UDP do docelowego hosta/portu i nie sprawdza, czy komunikacja zakończyła się powodzeniem. Przykładem usługi działającej z użyciem UDP jest DNS (Domain Name Server, port 53);

strumienie

- strumienie (pakiety TCP) — czyli „stream sockets” — te gniazdko wysyłają dane za pomocą protokołu TCP, a zatem otwierają kanał komunikacji na określonym porcie, dane wysyłane są w pakietach TCP, gniazdko (socket) nie zamyka połączenia i oczekuje na odpowiedź od hosta docelowego. Przykładem usługi korzystającej z TCP jest HTTP (HyperText Transfer Protocol, port 80 — gdy przeglądarka internetowa chce pobrać zasób z serwera WWW, robi to właśnie poprzez zestawienie kanału komunikacji TCP na porcie 80);

Raw sockets

- raw sockets (IP sockets) — ostatni rodzaj to gniazdko, które są w stanie wysyłać pakiety IP z pominięciem obu przedstawionych powyżej rodzajów pakietów, które są niejako opakowaniem dla danych (UDP i TCP). Raw IP sockets pozwalają na zdefiniowanie pakietu IP z dowolnym nagłówkiem i przesłanie go dowolnie zdefiniowanym protokołem (np. ICMP).

```
1 #!/usr/bin/python
2 #
3 # uzycie:
4 # ./host.py domena
5 #
6
7 import socket, sys # [1]
8
9 def getHostIP(domain_name):
10     ip_addr = socket.gethostbyname(domain_name) # [2]
11     return ip_addr
12
13 if __name__ == '__main__':
14     domain = sys.argv[1]
15     print "Adres IP dla domeny %s to %s" % (domain, getHostIP(domain))
```

Architektura klient-serwer

```
1 #!/usr/bin/python
2 #
3 # Klient
4 #
5 import socket
6
7 def sendPacket():
8     proto = socket.getprotobynumber('tcp')                      # [1]
9     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM, proto) # [2]
10    try:
11        s.connect(("127.0.0.1", 2222))                          # [3]
12        s.send("Hello world")                                  # [4]
13
14        resp = s.recv(1024)                                    # [5]
15        print resp
16    except socket.error:
17        pass
18    finally:
19        s.close()
20
21 if __name__ == '__main__':
22     sendPacket()
```

```
1 #!/usr/bin/python
2 #
3 # SERWER
4 #
5
6 import socket
7
8 def server():
9     proto = socket.getprotobynumber('tcp')                      # [1]
10    serv = socket.socket(socket.AF_INET, socket.SOCK_STREAM, proto)
11
12    serv.bind(("localhost", 2222))                                # [2]
13    serv.listen(1)                                                 # [3]
14
15    return serv
16
17 serv = server()
18
19 while 1:
20     conn, addr = serv.accept()                                    # [4]
21     while 1:
22         message = conn.recv(64)                                  # [5]
23         if message:
24             conn.send('Hi, I am a server, I received: ' + message)
25         else:
26             break
27     conn.close()
```

```
1 #!/usr/bin/python
2
3 import socket,sys
4
5 def main(dest_name):
6     dest_addr = socket.gethostbyname(dest_name) # [1]
7     port = 33434
8     max_hops = 30
9     icmp = socket.getprotobynumber('icmp')
10    udp = socket.getprotobynumber('udp')
11    ttl = 1
12    while True:
13        recv_socket = socket.socket(socket.AF_INET, socket.SOCK_RAW, icmp) # [2]
14        send_socket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM, udp)
15        send_socket.setsockopt(socket.SOL_IP, socket.IP_TTL, ttl) # [3]
16        recv_socket.bind(("", port)) # [4]
17        send_socket.sendto("", (dest_name, port)) # [5]
18        curr_addr = None
19        curr_name = None
20        try:
21            _, curr_addr = recv_socket.recvfrom(512)
22            curr_addr = curr_addr[0]
23            try:
24                curr_name = socket.gethostbyaddr(curr_addr)[0]
25            except socket.error:
26                curr_name = curr_addr
27            except socket.error:
28                pass
29            finally:
30                send_socket.close()
31                recv_socket.close()
32
33            if curr_addr is not None:
34                curr_host = "%s (%s)" % (curr_name, curr_addr)
35            else:
36                curr_host = "*"
37            print "%d\t%s" % (ttl, curr_host)
38
39            ttl += 1
40            if curr_addr == dest_addr or ttl > max_hops:
41                break
42
43 if __name__ == "__main__":
44     host = sys.argv[1]
45     main(host)
```

C/C++

- można wykorzystać moduł **SFML Network** który daje prosty i wygodny dostęp do komunikacji między komputerami.

Połączenie TCP

Tworzenie gniazda klienta

C/C++

```
// klient

sf::TcpSocket socket; // tworzymy gniazdo klienta
sf::IpAddress ip = "adres.ip.serwera.do.ktorego.sie.chcesz.polaczyc";
unsigned int port = 54000 // port na którym nasłuchuje serwer

if( socket.connect( ip, port ) != sf::Socket::Done ) // łączymy się z adresem 'ip' na porcie 'port'
// jeśli funkcja connect zwróci sf::Socket::Done oznacza to, że wszystko poszło dobrze
{
    cerr << "Nie można połączyć się z " << ip.toString() << endl;
    exit( 1 );
}
```

getLocalAddress() zwraca lokalne IP.
getLocalPort() zwraca lokalny port.
getRemoteAddress() zwraca zdalne IP.
getRemotePort() zwraca zdalny port.

Tworzenie gniazda serwera TCP

C/C++

```
// serwer

sf::TcpListener listener; // tworzymy gniazdo nasłuchujące
unsigned int port = 54000; // port, na którym będziemy nasłuchiwać

if( listener.listen( port ) != sf::Socket::Done ) // rozpoczynamy nasłuchiwanie na porcie 'port'
{
    cerr << "Nie mogę rozpoczęć nasłuchiwania na porcie " << port << endl;
    exit( 1 );
}

//...
```

C/C++

```
// serwer

while( /*...*/ )
{
    sf::TcpSocket client; // tworzymy gniazdo, dzięki któremu będziemy mogli się komunikować z klientem
    listener.accept( client );

    // wysyłanie/odbieranie danych od/do klienta
}
```

Komunikacja między połączonymi gniazdzami TCP

C/C++

```
// sposób działa dla klienta i dla serwera

const int datasize = 100; // rozmiar bloku danych
char data[ 100 ] = "..."; // tworzymy blok danych

//...

// wysyłanie danych
if( socket.send( data, datasize ) != sf::Socket::Done ) // i wysyłamy...
{
    // nie można wysłać danych (prawdopodobnie klient/serwer się rozłączył)
    cerr << "Nie można wysłać danych!\n";
    exit( 1 );
}

//...

// odbieranie danych
unsigned int received; // do tej zmiennej zostanie zapisana ilość odebranych danych
if( socket.receive( data, datasize, received ) != sf::Socket::Done ) // i wysyłamy...
{
    // nie można odebrać danych (prawdopodobnie klient/serwer się rozłączył)
    cerr << "Nie można odebrać danych!\n";
    exit( 1 );
}
else
    cout << "Odebrano " << received << " bajtów\n";
```

Komunikacja za pomocą UDP

C/C++

```
sf::UdpSocket sock; // tworzymy gniazdo

const int datasize = 100; // rozmiar danych do wysłania/odebrania
char data[ datasize ] = "..."; // dane

// wysyłanie
sf::IpAddress ip( "adres.komputera.do.którego.chcesz.wysłać.dane" );
unsigned int port = 56000; // port, na który chcesz wysłać dane
if( sock.send( data, datasize, ip, port ) != sf::Socket::Done )
{
    cerr << "Nie można wysłać danych!\n";
    exit( 1 );
}

// odbieranie
sf::IpAddress ip( "adres.komputera.od.którego.chcesz.odebrać.dane" );
unsigned int port = 56000; // port, na którym chcesz odbierać dane
unsigned int senderport = 54000; // port, z którego zostanły wysłane dane
unsigned int received;
sock.bind( port );
if( sock.receive( data, datasize, received, ip, senderport ) != sf::Socket::Done )
{
    cerr << "Nie można odebrać danych!\n";
    exit( 1 );
}
cout << "Odebrano bajtów: " << received << endl;
```

Problem blokujących gniazd

C/C++

```
// dobrze

sf::TcpListener server; // gniazdo nasłuchujące
vector< sf::TcpSocket *> clients; // tutaj przechowujemy klientów

sf::SocketSelector sel; // selektor
sel.add( server ); // dodajemy gniazdo nasłuchujące
//...
while( true )
// pętla główna serwera
{
    if( sel.wait( sf::seconds( 2 ) )  // jeśli metoda wait() zwróci true, to znaczy, że ktoś z dodanych gniazd jest gotowe do odbioru
    // jako argument podajemy czas, przez który ma czekać na dane
    {
        if( sel.isReady( server ) )  // metoda isReady() sprawdza, czy dane gniazdo ma dane do odebrania
        // jeśli do metody isReady() przekażemy gniazdo nasłuchujące, true oznacza, że ktoś chce się do niego połączyć
        {
            TcpSocket * tmp = new sf::TcpSocket;
            server.accept( * tmp ); // skoro ktoś chce się do nas połączyć, to go akceptujemy
            clients.push_back( tmp ); // i dodajemy go do listy
            sel.add( * tmp ); // oraz do selektora, żeby można było od niego odbierać dane
            // nie zapomnij, by usunąć(za pomocą delete) gniazdo, kiedy się rozłączy
        }

        // pętla przechodząca po kontenerze gniazd (zależy od typu kontenera)
        for( int i = 0; i < clients.size(); i++ )  // u nas to jest for i indeks i
        {
            if( sel.isReady( * clients[ i ] ) )  // *clients[i] coś nam wysłał
            {
                const int datasize = 100; // rozmiar danych do odebrania
                char data[ datasize ]; // dane
                unsigned int received; // odebrane
                clients[ i ]->receive( data, datasize, received );
                cout << "Odebrano " << received << " bajtów od " << clients[ i ]->getRemoteAddress() << endl;
                // tutaj robimy coś z odebranymi danymi
                //...
            }
        }
    }
    // reszta kodu serwera
}
```

Pakiety

- 1) Jeśli wyślesz np. 1kB danych to dotrą one (prawdopodobnie) podzielone na kilka części. Serwer odbierze pierwszą serię danych, a później nie będzie wiedział, czy ma oczekiwany na następną, czy to już wszystko.
- 2) Kiedy wysydasz dane do jakieś maszyny, nie wiesz, czy ma ona np. ten sam rozmiar typu int, albo czy używa ona konwencji little-endian (bajty "bardziej znaczące" są na początku), czy big-endian (na końcu).

Jak odbierać dane za pomocą pakietów:

- 1)Tworzymy zmienną typu sf::Packet
- 2)Odbieramy dane za pomocą metody receive()
- 3)Wyciągamy dane z pakietu jak ze strumienia istream z biblioteki standardowej

C/C++

```
sf::Packet pak; // 1
someSocket.receive( pak ); // 2

float x;
int y;
string z;
pak >> x >> y >> z; // 3
```

Jak wysyłać dane z pomocą pakietów:

- 1)Tworzymy zmienną typu sf::Packet
- 2)Zapisujemy dane do pakietu jak do strumienia ostream z biblioteki standardowej
- 3)Wysyłamy dane za pomocą metody send()

C/C++

```
sf::Packet pak; // 1

float x = 3.14f;
int y = 64;
string z = "hello!";
pak << x << y << z; // 2
someSocket.send( pak ); // 3
```

Darknet

zagrożenie czy przyszłość

Internet czy to cała sieć?

- Ze względu na ograniczenia prawne wprowadzane w sieci internet od lat rozwija się szara strefa mająca na celu wprowadzenie pełnej wolności – wolności absolutnej.

Rozmiary

- Szacuje się, że Darknet jest o kilka rządów wielkości większy, niż powszechnie znane strony na powierzchni sieci. Według niektórych szacunków, nawet 96% wszystkich danych znajduje się w szeroko rozumianej Deep Web (Głęboka sieć).

Realizacja

- ANts P2P – system wymiany plików P2P anonimizujący i szyfrujący ruch, obsługuje publikacje HTTP.
- Azureus – klient BitTorrent z dodatkową opcją użycia I2P lub Tor (open source, napisany w Javie)
- Freenet – odporny na cenzurę rozproszony system plików do anonimowej publikacji (open source, napisany w Javie)
- GUNet – P2P framework, zawiera program do wymiany plików jako najważniejsza aplikację (projekt GNU, napisany w C)
- I2P – anonimizująca powłoka sieciowa na której mogą być budowane aplikacje (open source, napisany w języku Java)
- Imule – modyfikacja emule działająca w sieci I2P
- MUTE – anonimizujący program do wymiany plików.
- Nodezilla – anonimizująca powłoka sieciowa o zamkniętym kodzie, na której można budować aplikacje (napisany w językach C++ oraz Java)
- Tor – Jest to jeden z największych projektów badawczych sieci anonimowych nastawiony na anonimowe przeglądanie internetu. Tor nie jest klientem P2P sam w sobie, tzn nie świadczy usług innym użytkownikom sieci.
- Winny – Klient P2P bardzo popularny w Japonii (freeware, napisany w C++ dla Windows)

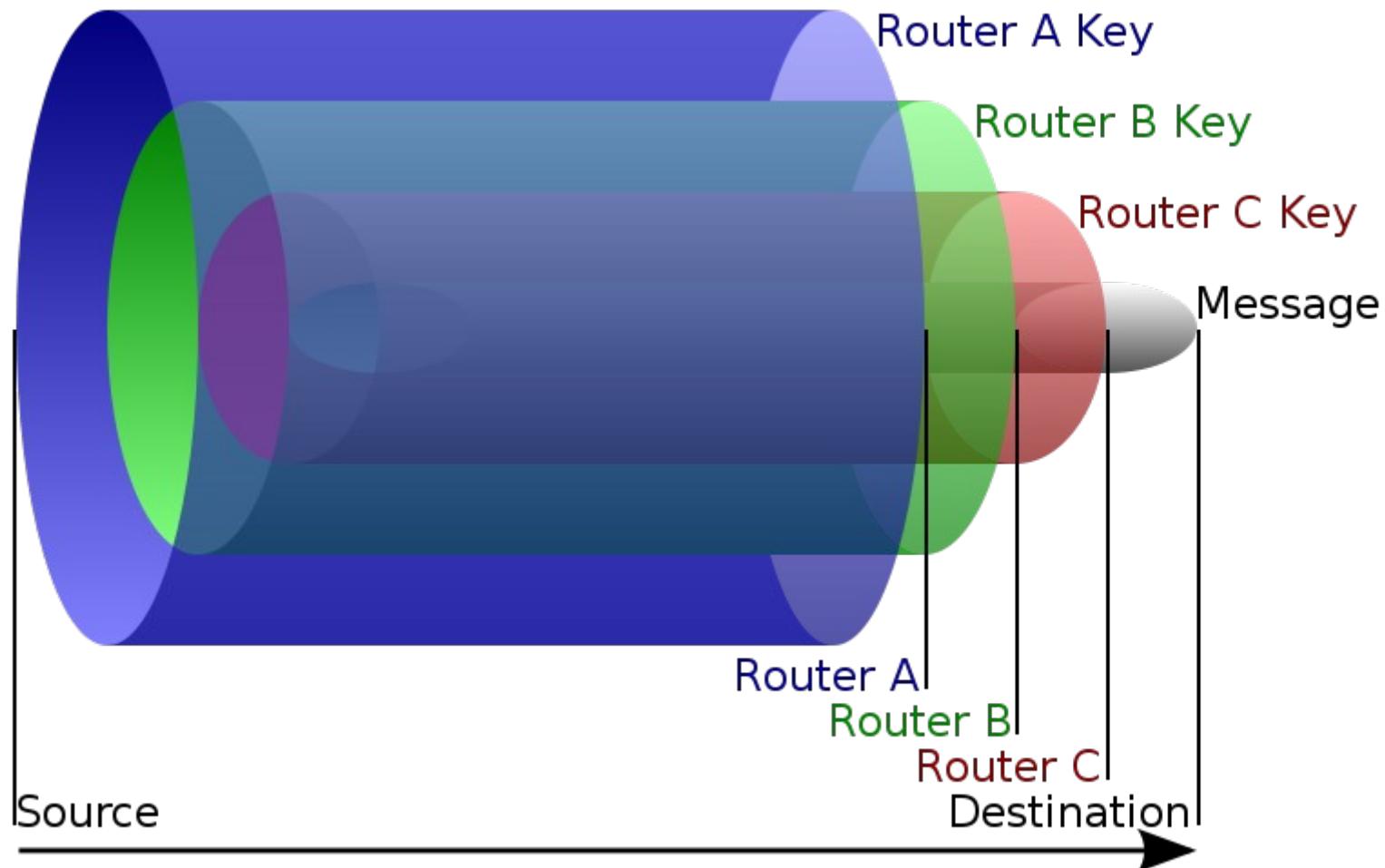
Zasada działania

- Wszystkie te sieci oparte są na zasadzie wymiany peer2peer oraz by zagwarantować anonimowość głównie wykorzystują trasowanie cebulowe.

Trasowanie cebulowe

- Trasowanie cebulowe (ang. onion routing) - technika służąca anonimowej komunikacji w sieci komputerowej.
- Polega ona na wielokrotnym szyfrowaniu wiadomości, a następnie przesyłaniu jej przez szereg węzłów zwanych routerami cebulowymi (ang. onion routers). Każdy z nich usuwa warstwę szyfrowania w celu uzyskania informacji o dalszym trasowaniu i przesyła dane do następnego routera. Takie działanie zapobiega ujawnieniu węzłom pośredniczącym pochodzenia, odbiorcy oraz treści wiadomości. Trasowanie cebulowe opracowane zostało przez Davida Goldschлага, Michaela Reeda oraz Paula Syversona.
- Począwszy od 2008 r. sieć Tor dominuje w wykorzystywaniu tej technologii

Trasowanie cebulowe



- Tor chroni tożsamość użytkowników oraz ich działalność w sieci przed analizą ruchu. Operatorzy utrzymują wirtualną sieć złożoną z ruterów cebulowych, zapewniającą anonimowość zarówno w sensie ukrycia lokalizacji użytkownika, jak też możliwości udostępniania anonimowych ukrytych usług.
- Wykorzystuje kryptografię, wielowarstwowo szyfrując przesyłane komunikaty (stąd określenie „trasowanie cebulowe”), zapewniając w ten sposób poufność przesyłania danych pomiędzy ruterami. Użytkownik musi mieć uruchomiony na swoim komputerze program, który łączy się z serwerem pośredniczącym sieci Tor[4]. Takie serwery, zwane węzłami, może uruchomić u siebie każdy, kto chce wspomóc rozwój Tora. Oprogramowanie łączące się z internetem może korzystać z Tora poprzez interfejs SOCKS.

- Tor nie oferuje całkowitej anonimowości i przy założeniu dostępu do odpowiednio dużych środków technicznych możliwe jest wytropienie danego użytkownika tej sieci[5]. Tor nie może i nie próbuje chronić przed monitorowaniem ruchu na granicach sieci, tzn. pakietów wchodzących i opuszczających sieć[6]. Na przykład rząd Stanów Zjednoczonych ma możliwość monitorowania dowolnego szerokopasmowego połączenia z Internetem dzięki urządzeniom wprowadzonym na podstawie Communications Assistance for Law Enforcement Act (CALEA) i dlatego może kontrolować oba punkty końcowe połączeń Tora, wykonywanych na terytorium USA. O ile Tor chroni przed analizą ruchu, nie może zapobiec potwierdzeniu komunikacji[6].

Historia

- Początkowo sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych, pod koniec 2004 r. stał się projektem firmowanym przez Electronic Frontier Foundation (EFF), która wspierała go finansowo aż do listopada 2005[7]. Obecnie rozwojem oprogramowania Tor zajmuje się Tor Project – organizacja non-profit (niedochodowa) o charakterze badawczo-edukacyjnym, z siedzibą w Stanach Zjednoczonych, otrzymująca wsparcie finansowe z różnych źróde

Trasa pakietu

- Użytkownicy uruchamiają na swoich komputerach oprogramowanie klienckie sieci Tor, które okresowo tworzy wirtualne obwody w sieci.
- Tor wielowarstwo szyfruje przesyłane komunikaty (stąd nazwa „trasowanie cebulowe”), zapewniając doskonałą poufność przesyłania pomiędzy ruterami. Jednocześnie oprogramowanie udostępnia interfejs SOCKS klientom. Aplikacje potrafiące obsługiwać protokół SOCKS mogą być skonfigurowane tak, by łączyły się z internetem za pośrednictwem oprogramowania klienckiego Tor, pełniącego w tym wypadku funkcję proxy, które następnie multipleksuje ruch sieciowy przez wirtualny obwód sieci Tor.
- Wewnątrz sieci Tor ruch jest przekazywany pomiędzy ruterami, osiągając w końcu węzeł wyjściowy, z którego niezaszyfrowany pakiet jest przekazywany do miejsca przeznaczenia. Z punktu widzenia docelowego komputera, ruch wydaje się pochodzić z wyjściowego węzła sieci Tor.
- Schemat połączenia wygląda w następujący sposób.
Użytkownik → węzeł1 → węzeł2 → węzeł3 → Serwer docelowy

- Sieć Tor działa na poziomie protokołu TCP i – inaczej niż większość pozostałych sieci anonimowych – nie narzuca ograniczeń co do możliwych zastosowań. Anonimizacji przy użyciu Tora poddawane są często takie aplikacje, jak IRC, komunikatory internetowe czy przeglądanie stron WWW. W przypadku WWW Tor na ogół stosuje się w parze z Privoxy, filtrującym serwerem pośredniczącym, mającym za zadanie ochronę prywatności na poziomie aplikacji.

Etykieta

- Nieodłącznie towarzysząca sieci Tor anonimowość sprawia, że tradycyjne praktyki administracyjne, zmierzające do przeciwdziałania nadużyciom, mogą być niewystarczające dla połączeń z niej wychodzących. Tor posiada funkcję, pozwalającą zredukować ten problem zarówno z perspektywy operatorów węzłów wyjściowych, jak i witryn osób trzecich.
- Węzły wyjściowe definiują swoją „politykę wyjściową”, która określa, jaki ruch jest, a jaki nie jest dopuszczalny przez ten węzeł. Większości najważniejszych nadużyć dotyczących sieci Tor można zapobiec, używając kombinacji adresu i portu. Potencjalne nadużycia obejmują:
 - Zapychanie łączy - Społeczność Tora uważa za niestosowne przesyłanie wielkich ilości danych przez sieć – rutery cebulowe są utrzymywane przez ochotników na własny koszt.
 - BitTorrent Protokół BitTorrent nie powinien być używany z siecią Tor ze względu na duże ilości przesyłanych danych. Domyślna polityka węzłów wyjściowych blokuje standardowe porty BitTorrent.
 - Spam Domyślna polityka wyjściowa blokuje połączenia z portem 25, zapobiegając rozsyłaniu spamu bezpośrednio z sieci Tor.
 - Anonimowi użytkownicy Serwisy, które chcą odmiennie traktować użytkowników odwiedzających je poprzez Tor, mają taką możliwość.

TOR

- TOR (Tor's Onion Router Network) jest prawdopodobnie najprostszą i najpopularniejszą implementacją Darknetu.
- Technologia ta została opracowana przez wojska amerykańskie w celu umożliwienia anonimowego przesyłu informacji i do dziś nie znaleziono sposobu, aby ją złamać (niektoří informatycy są przekonani, že nigdy to nie będzie możliwe).

TOR

- Występująca w niej domena .onion nie jest częścią rejestru ICANN i nie da się z nią połączyć bez użycia programu
- Ze względu na sposób działania routingu TOR, zarówno host obsługujący odwiedzaną stronę internetową, jak i klient zwracający, są ukryci i ich identyfikacja jest praktycznie niemożliwa.

- Kombinacja ta powoduje, że taka forma Internetu znajduje się daleko poza kontrolą jakiegokolwiek rządu lub regulacji.
- Użytkownik musi tylko kliknąć przycisk „Nowa tożsamość” („New Identity”), a program wybierze nowy węzeł, przez który będzie wysyłać zapytania – operacja ta nadaje ci nowy adres IP i całkowicie nową tożsamość, nawet w zwykłym Internecie.

- Dla systemu operacyjnego Windows istnieje też bardzo wygodna wersja Tora, która nie wymaga instalacji i zawiera w sobie skonfigurowaną przeglądarkę Firefox. Dzięki temu Tora możesz mieć zawsze przy sobie, np. na pendrive i odpalać go gdziekolwiek jesteś.

- Mając zainstalowanego TOR-a może uzyskać dostęp do wszystkich domen .onion, takich jak Hidden Wiki (adresy w domenie .onion wyglądają dosyć niekonwencjonalnie i mają niestety nieprzyjemną dla użytkownika formę);
- Hidden Wiki <http://www.kpvz7ki2v5agwt35.onion/wiki/> która powie ci dużo o tym jak odnaleźć się w Darknecie i od czego zacząć.
- Własny hosting na Freedom Hosting (<http://www.xqz3u5drneuzhaeo.onion/>),
- blog na blog.masked (<http://www.ms4kc75hlvnfcxgz.onion/>)

- Tor to nieprzebrane bogactwo stron i informacji, po których z czasem nauczysz się swobodnie poruszać. W sieci będziesz mógł prowadzić własną pocztę e-mail, udzielać się na rozmaitych forach, przesyłać pliki, czy dokonywać transakcji handlowych z innymi użytkownikami z całego świata.

Nielegalne zastosowania

- Sieć Tor może być wykorzystywana do celów uznawanych za nielegalne w niektórych jurysdykcjach, jak na przykład krytykowanie przywódców państwowych, wymiana materiałów chronionych prawem autorskim bądź dystrybucja pornografii dziecięcej[20][21][22]. We wrześniu 2006 r. władze niemieckie, w trakcie operacji wymierzonej przeciwko pornografii dziecięcej, skonfiskowały sprzęt jednego z centrów danych, na którym uruchomione było oprogramowanie Tor

Słabości TOR

- Wycieki zapytań DNS

- Podobnie jak w przypadku wielu innych systemów do anonimowego surfowania po internecie, część aplikacji nadal wykonuje bezpośrednie zapytania do serwerów domenowych (DNS), pomijając serwer pośredniczący Tor. Wykorzystanie Privoxy bądź polecenia „torify”, dystrybuowanego wraz z Torem, to jedne z możliwych rozwiązań tego problemu. Ponadto aplikacje używające protokołu SOCKS5, który obsługuje żądania proxy oparte na nazwach, mogą przesyłać przez Tora zapytania DNS, które zrealizuje węzeł wyjściowy, zapewniając w ten sposób anonimowość analogiczną jak dla innych danych przesyłanych przez sieć Tor

Słabości

- Analiza ruchu
 - Jak wszystkie współczesne sieci anonimowe z niewielkimi opóźnieniami (ang. low latency), Tor jest podatny na analizę ruchu przez adwersarzy, którzy mogą obserwować oba końce połączenia użytkownika
- Podsłuchiwanie przez węzły wyjściowe

Niebezpieczeństwa

- Tor może być niebezpieczny, jeśli jest niewłaściwie użyty, podobnie jak każda inna rzecz. Z Daknetu korzystają wszyscy: politycy, aktywiści, uciekinierzy, szpiedzy, detektywi, służby specjalne, rebelianci, hakerzy, spiskowcy, handlarze bronią, narkotykami, płatni mordercy, pedofile, alfonsi, złodzieje, oszuści... a także zwykli, przeciętni ludzie, którzy z jakiegoś powodu chcą skorzystać ze swojego naturalnego prawa do zachowanie prywatności i anonimowości.

- W Torze można znaleźć różne plugastwa, ale pamiętaj też, że nikt cię nie zmusza, aby tam wchodzić (dla własnego zdrowia psychicznego odradzam korzystanie z hostingów ze zdjęciami, oraz z niemoderowanych for, takich ja chany) – przy odrobinie zdrowego rozsądku, można tego wszystkiego uniknąć i cieszyć się wolnością poważnych i rzeczowych informacji, jakie można tam znaleźć.

I2P2 Network and .i2p Domains

- Inna forma Darknetu znajduje się w sieci I2P2. I2P działa w bardzo podobny sposób do Tora, choć jest nieco bardziej elastyczna i może być używana dla wielu różnych typów protokołów i różnych aplikacji, włączając w to Web access, email, IRC Chat i inne.
- Oprogramowanie to pozwala na dostęp do domeny I2P, która jest inną formą Darknetu.

Domeny namecoin .bit i alternatywny DNS

- Wiele podobnych wielkich projektów jest obecnie w fazie rozwoju.
- Namecoin jest zdecentralizowanym, rozpowszechnionym systemem DNS, zaopatrzonym w domenę najwyższego poziomu .bit, opartą na tej samej strukturze co Bitcoin (wirtualna waluta).
- Zasadniczo, należąc do „kopalni” Namecoin, w ten sama sposób można wydobywać bitcoiny.
- Jest to zatem wymienialne dla nazwy domeny .bit.
- Co ciekawe, ICANN zgłosił również niedawno zwiększenie liczby dozwolonych sufiksów internetowych.

Inne formy Darknet i Dark Web

- Należy też zauważyc, że Deep Web (Głęboka sieć) jest wszechogarniającym pojęciem, które obejmuje wszelkiego rodzaju treści, które nie są zwykle dostępne (albo ze względu na użycie niestandardowych DNS, jak Dark Internet lub podobne, nie są po prostu indeksowana i nie można ich znaleźć za pomocą zwykłej, nieskonfigurowanej przeglądarki), wyszukiwane, lub po prostu linki do tych stron są nieznane.
- Darknet jednak, zazwyczaj odnosi się do udostępniania plików na stronach (włączając w to metodę peer-to-peer), jak również do przekaźników IRC chat, z których większość nie jest typowo indeksowana.
- Dark Internet najprawdopodobniej jest naturalną i nieuniknioną odpowiedzią na rządowe próby coraz większej kontroli, prowadzącej do zniszczenia tej wspaniałej idei.
- Można przewidzieć, że w najbliższych latach zauważymy gwałtowny wzrost i rozwój ciemnej strony Internetu.

Przydatne linki

- [https://pl.wikipedia.org/wiki/Tor_\(sie%C4%87_anonimowa\)](https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa))
- <http://libertarianin.org/co-to-jest-darknet/>

Email

Szymon Pulawski

E-mail

- Poczta elektroniczna, e-poczta, e-mail usługa internetowa, w nomenklaturze prawnej określana zwrotem świadczenie usługi drogą elektroniczną, służąca do przesyłania wiadomości tekstowych, jak i multimedialnych, tzw. listów elektronicznych – stąd zwyczajowa nazwa tej usługi.
- Od kwietnia 2009 roku, na podstawie dyrektywy Unii Europejskiej, dostawcy usług internetowych muszą rejestrować kontakty swoich klientów w sieci, w tym również e-maile, podobnie do billingu.

Zarządzanie email

- Klienci
- Webmail

SMTP

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

Simple Mail Transfer Protocol

- SMTP to względnie prosty, tekstowy protokół, w którym określa się co najmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości. [Demon](#) SMTP działa najczęściej na porcie 25.

- sesja SMTP (z serwerem [exim](#)), w której klient kolejno:
 - rozpoczyna połączenie z serwerem (polecamie **helo**),
 - podaje adres nadawcy (polecamie **mail from**),
 - podaje adres odbiorcy (polecamie **rcpt to**),
 - wpisuje wiadomość (polecamie **data**),
 - kończy sesję (polecamie **quit**).

- Jednym z ograniczeń pierwotnego SMTP jest brak mechanizmu weryfikacji nadawcy, co ułatwia rozpowszechnianie niepożądanych treści poprzez pocztę elektroniczną ([wirusy komputerowe](#), [spam](#)).
Żeby temu zaradzić stworzono rozszerzenie [SMTP-AUTH](#).

Odbieranie poczty – POP3

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

- Kiedy użytkownik połączy się z siecią, to korzystając z POP3 może pobrać czekające na niego listy do lokalnego komputera. Jednak protokół ten ma wiele ograniczeń:
 - połączenie jest realizowane tylko na czas kiedy użytkownik pobiera pocztę, nie może zostać uśpione,
 - każdy list musi być pobierany razem z załącznikami i żadnej jego części nie można w łatwy sposób pominąć – istnieje co prawda komenda **top**, ale pozwala ona jedynie określić przesyłaną liczbę linii od początku wiadomości,
 - wszystkie odbierane listy trafiają do jednej skrzynki, nie da się utworzyć ich kilku,
 - serwer POP3 nie potrafi sam przeszukiwać czekających w kolejce listów.

- Przykładowa sesja POP3 w której klient kolejno:
 - podaje identyfikator użytkownika, którego poczta będzie ściągana (polecenie **user**),
 - podaje hasło (polecenie **pass**),
 - prosi o listę wiadomości oczekujących na ściągnięcie (polecenie **list**),
 - ściąga pierwszą (i akurat w tym przypadku ostatnią) z wiadomości (polecenie **retr**),
 - kasuje wiadomość po jej ściągnięciu (polecenie **dele**),
 - kończy sesję (polecenie **quit**).

Internet Message Access Protocol

- **IMAP** (ang. *Internet Message Access Protocol*) – internetowy protokół pocztowy zaprojektowany jako następca POP3
- W przeciwieństwie do POP3, który umożliwia jedynie pobieranie i kasowanie poczty, IMAP pozwala na zarządzanie wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze.

- IMAP pozwala na dwa tryby działania: połączeniowy i bezpołączeniowy. W przypadku protokołu POP, [klient](#) zazwyczaj podłączony jest do serwera na tyle długo, na ile trwa pobieranie wiadomości. W przypadku IMAP klient często utrzymuje połączenie dopóki [interfejs użytkownika](#) jest uruchomiony, żeby móc pobierać wiadomości na żądanie. W przypadku kont pocztowych posiadających wiele bądź duże wiadomości, tego rodzaju strategia może skutkować niższym czasem reakcji.

- Protokół POP wymaga, aby w tym samym czasie do danego konta pocztowego podłączony był jeden klient. IMAP pozwala równocześnie podłączać się wielu klientom. Dostarcza mechanizmy pozwalające wykryć zmiany dokonane przez inne podłączone w tym samym czasie stacje klientów.
- Dzięki IMAP IDLE wiadomości mogą być przesyłane do klientów bezpośrednio po dostarczeniu na serwer, bez konieczności ręcznego odpytywania serwera ([push e-mail](#)).

- W protokole IMAP fragmenty wiadomości elektronicznej są opisane za pomocą standardu MIME. IMAP umożliwia pobieranie wskazanych części wiadomości elektronicznej, niekoniecznie całej wiadomości. Tak więc można pobrać jedynie tekst bez konieczności pobierania załączników (zdjęć, dokumentów, które opisane są każde z osobna przez standard [MIME](#), jako osobne części wiadomości). Możliwe jest też częściowe pobieranie określonych przez MIME fragmentów wiadomości.

- Protokół IMAP implementuje system flag określających status wiadomości w taki sposób, że każdy z podłączonych klientów widzi zmiany statusów dokonane przez innych klientów. Flagi określają m.in.: czy wiadomość została przeczytana, skasowana, czy udzielona została na nią odpowiedź. Status flag zapisywany jest na serwerze.
- Niektóre z serwerów IMAP pozwalają na przyporządkowanie do wiadomości jednego, bądź większej ilości predefiniowanych znaczników (tags), których znaczenie interpretowane jest przez klienty pocztowe. Dodawanie znaczników (tagów) wiadomościom jest wspierane przez niektórych dostawców poczty oferujących dostęp z poziomu przeglądarki, np. gmail.

- IMAP pozwala na posiadanie wielu folderów na jednym koncie pocztowym. Klienty IMAP są w stanie tworzyć, zmieniać nazwę oraz kasować foldery w skrzynkach pocztowych na serwerze. Mogą też przenosić wiadomości między folderami. Możliwy jest również dostęp do folderów publicznych i współdzielonych.
- IMAP pozwala wykonywać przeszukiwanie skrzynki pocztowej po stronie serwera. Zatem zadanie wyszukiwania może być przetwarzane przez serwer pocztowy, nie przez klienta. Działanie takie nie wymusza pobierania wszystkich wiadomości.
- Korzystając z doświadczeń wcześniej rozwijanych protokołów, IMAP jasno definiuje sposoby dzięki którym może być rozszerzany.