Spis treści

1. Internet

Internet - ogólnoświatowy system połączeń między komputerami, określany również jako sieć. W znaczeniu informatycznym Internet to przestrzeń adresów IP przydzielonych hostom i serwerom połączonym za pomocą urządzeń sieciowych, takich jak karty sieciowe, modemy i koncentratory, komunikujących się za pomocą protokołu internetowego z wykorzystaniem infrastruktury telekomunikacyjnej.

2. Sieć

Sieć komputerowa – zbiór komputerów i innych urządzeń połączonych z sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane w tej sieci. Umożliwia ona wzajemne przekazywanie informacji oraz udostępnianie zasobów własnych między podłączonymi do niej urządzeniami, zwanymi punktami sieci. Głównym przeznaczeniem sieci komputerowej jest ułatwienie komunikacji między ludźmi. Sieć umożliwia łatwy i szybki dostęp do publikowanych danych, jak również otwiera techniczną możliwość tworzenia i korzystania ze wspólnych zasobów informacji i zasobów danych.

3. Topologie

Topologia sieci komputerowej – model układu połączeń różnych elementów (linki, węzły itd.) sieci komputerowej. Określenie topologia sieci może odnosić się do konstrukcji fizycznej albo logicznej sieci.

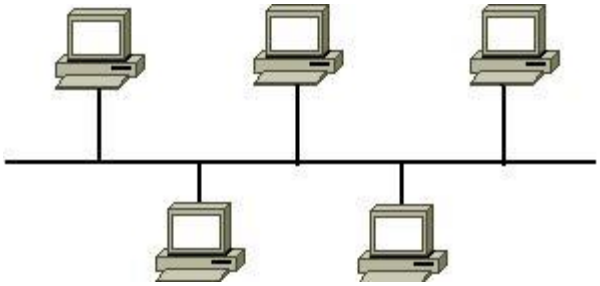
Topologia fizyczna opisuje sposoby fizycznej realizacji sieci komputerowej, jej układu przewodów, medium transmisyjnych. Poza połączeniem fizycznym hostów i ustaleniem standardu komunikacji, topologia fizyczna zapewnia bezbłędną transmisję danych. Topologia fizyczna jest ściśle powiązana z topologią logiczną np. koncentratory, hosty.

Topologia logiczna opisuje sposoby komunikowania się hostów za pomocą urządzeń topologii fizycznej.

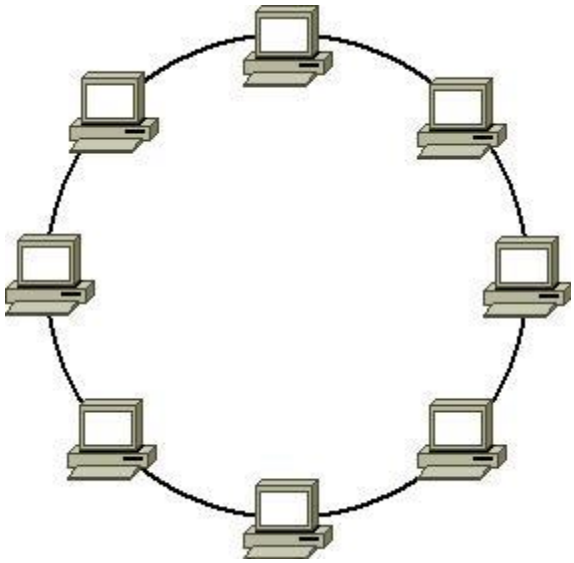
Rodzaje topologie fizyczne:

- Liniowa - wszystkie elementy sieci połączone są z dwoma sąsiadującymi.

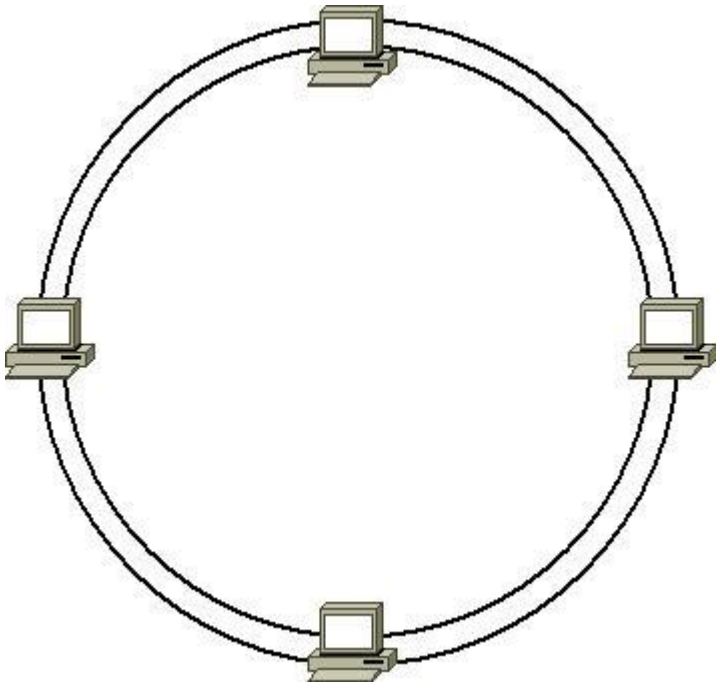
- Magistrali - wszystkie elementy sieci podłączone do jednej magistrali. Obecnie stosowana do łączenia urządzeń w topologii punkt-punkt.



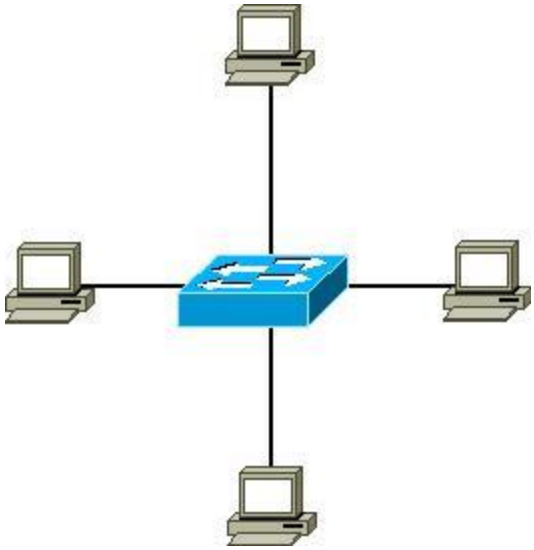
- Pierścienia - poszczególne elementy są połączone pomiędzy sobą odcinkami przewodów tworząc zamknięty pierścień.



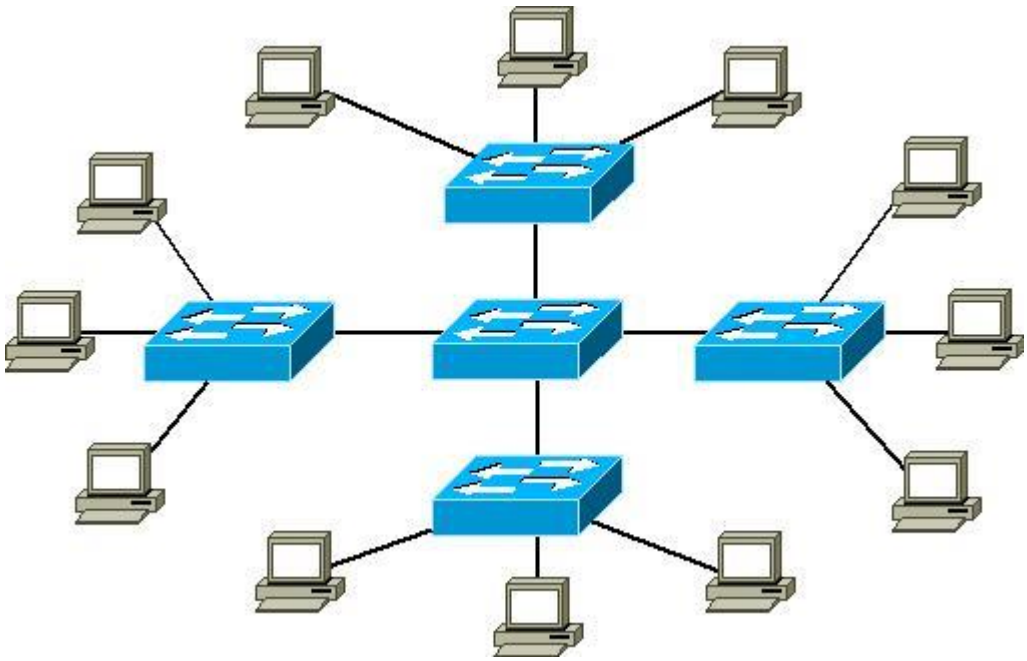
- Podwójnego pierścienia - poszczególne elementy są połączone pomiędzy sobą odcinkami tworząc dwa zamknięte pierścienie.



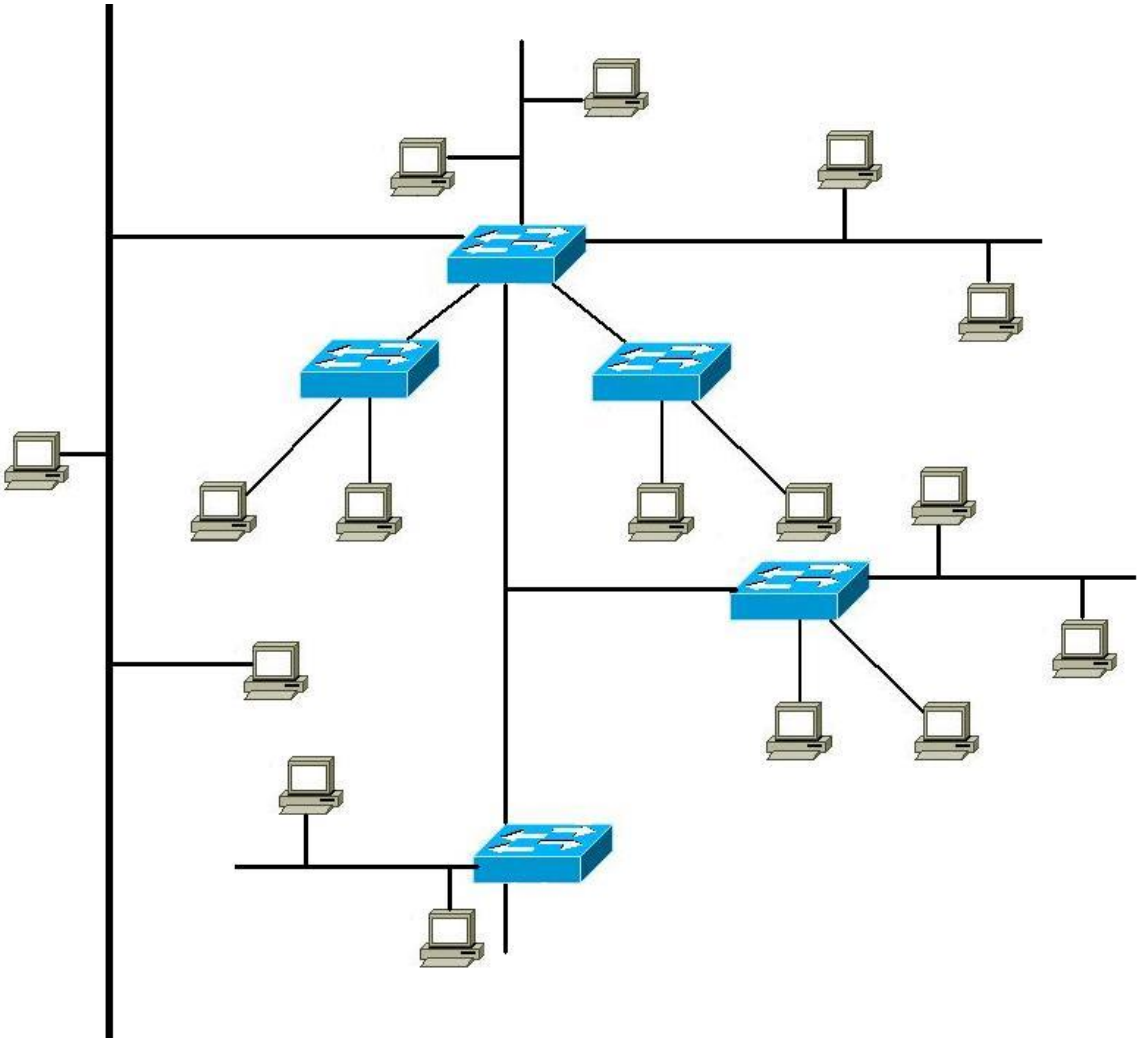
- Gwizdy - komputery są podłączone do jednego punktu centralnego, koncentratora (koncentrator tworzy fizyczną topologię gwiazdy, ale logiczną magistralę) lub przełącznika. Stosowana przy łączeniu urządzeń przy pomocy kabla skrętnego lub światłowodu. Każdy pojedynczy przewód jest stosowany do połączenia z siecią dokładnie jednego urządzenia.



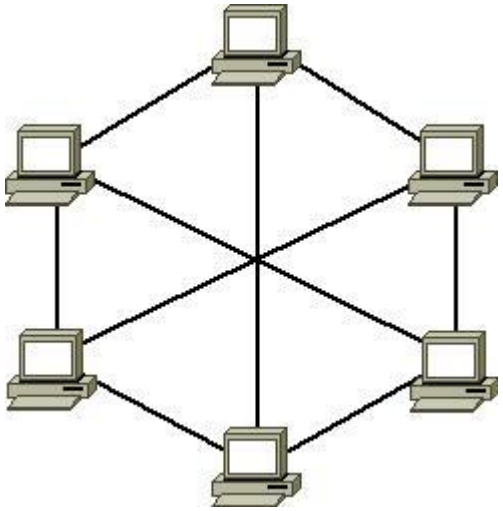
- Gwizdy rozszerzonej - posiada punkt centralny (podobnie do topologii gwiazdy) i punkty poboczne (jedna z częstszych topologii fizycznych Ethernetu).



- Hierarchiczna - zwana także topologią drzewa, jest kombinacją topologii gwiazdy i magistrali, budowa podobna do drzewa binarnego.



- Siatki - oprócz koniecznych połączeń sieć zawiera połączenia nadmiarowe; rozwiązanie często stosowane w sieciach, w których wymagana jest bezawaryjność.



4. Kable

Jakie są rodzaje przewodów do Internetu?

Istnieje kilka wariantów kabli sieciowych, a ich poszczególne wersje różnią się pod względem parametrów. Przewód do Internetu bywa nazywany skrętką i może występować w poniższych wariantach:

- Kabel sieciowy nieekranowany (UTP) – kabel ten tworzy symetryczną linię. Składa się ze skręconych ze sobą par przewodów. Kabel internetowy tego typu jest powszechnie stosowany w połączeniach informatycznych. Istnieją różne kategorie skrętki tego typu. Przykładowo: kategoria 3 pozwala na transmisję danych z prędkością do 10 Mb/s, a kategoria 5 do 100 Mb/s.
- Kabel sieciowy ekranowany (STP) – skrętka posiada ekran z uziemieniem oraz oplot. Przewody z ekranem oraz oplotem są zgodne z normami europejskimi EMC w zakresie emisji EMI (Electro Magnetic Interference).
- Kabel sieciowy foliowany (FTP) – skrętka posiada ekran foliowy z uziemieniem. To rodzaj przewodu, który jest rekomendowany do zastosowania w sieciach komputerowych, które są narażone na liczne zakłócenia elektromagnetyczne.

To podstawowe wersje przewodów internetowych, które są najczęściej wybierane i stosowane w praktyce. Istnieją również kable hybrydowe, które posiadają dodatkowe zabezpieczenia ekranowe i foliowe.

Kable hybrydowe do Internetu

- Kabel internetowy F/FFTP – oddzielna folia pokrywa każdą parę przewodów. Oprócz tego wszystkie przewody są pokryte wspólną warstwą foliowego ekranu.
- Kabel internetowy U/FTP – każda para przewodów jest pokryta ekranem z folii.
- Kabel do Internetu S/FTP – każda para przewodów foliowana, dodatkowo wszystkie przewody znajdują się we wspólnym oplocie.
- Kabel do Internetu SF/FTP – każda para przewodów jest foliowana, a wszystkie przewody znajdują się we wspólnym ekranie z folii i siatki.

To kilka z wielu wariantów hybrydowych przewodów internetowych. Kabel RJ45 hybrydowy, z uwagi na skutecznie zabezpieczenia, może być dobrym rozwiązaniem do stosowania w miejscach szczególnie narażonych na zakłócenia elektromagnetyczne.

Jakie są rodzaje zakończeń w kablach do Internetu?

Wariantów kabli do Internetu jest wiele. Wybór odpowiedniego przewodu komplikuje również dwojaki sposób zarabiania końcówek. Można spotkać się z kablami sieciowymi typu A oraz typu B, które różnią się pomiędzy sobą sposobem zakończenia:

- Kabel Ethernet typu A – przewody w kablu są ułożone parami (biało-zielony, zielony, biało-pomarańczowy, niebieski, biało-niebieski, pomarańczowy, biało-brązowy, brązowy).

- Kabel Ethernet typu B – przewody w kablu są ułożone parami (biało-pomarańczowy, pomarańczowy, biało-zielony, niebieski, biało-niebieski, zielony, biało-brązowy, brązowy).

Kabel światłowodowy

Kabel światłowodowy (ang. Optical fiber cable) – kabel zawierający jedno lub więcej włókien szklanych prowadzących impulsy światła. Najlepszy kabel światłowodowy jest z pojedynczą wiązką/włóknem ze względu na to iż jest mniej odbić sygnałów dzięki czemu mniejsza strata na jakości.

W telekomunikacji wykorzystuje się zwykle światło podczerwone. Kable utworzone z włókien szklanych są odporne na zakłócenia elektromagnetyczne i mają dużą przepustowość. Przy ich użyciu można osiągać szybkości przesyłania do 100 Gb/s (ok. 12,5 GB/s); najszybsze systemy światłowodowe mogą prowadzić sygnał rzędu kilku Tb/s. Kłopot konstrukcyjny sprawia tylko stosunkowo duży promień zgięcia światłowodu. Musi wynosić on kilka centymetrów, aby było możliwe właściwe wewnętrzne odbijanie i rozchodzenie się światła, a samo włókno nie uległo uszkodzeniu.

Budowa kabla światłowodowego

Struktura kabla światłowodowego zależy od planowanego rejonu instalacji, zasięgu i występujących zagrożeń.

- (a) Zewnętrzna warstwa ochronna kabla mająca na celu ochronę przed warunkami zewnętrznymi, wykonana z tworzywa PVC pod tą warstwą możemy także spotkać warstwę z metalu/ołowiu, chroniącą kabel przed uszkodzeniami,
- (b) Warstwa kevlarowych "nitek" wzmacniająca konstrukcje kabla,
- (c) Kolejna warstwa ochronna, wewnątrz której umieszczony jest żel,
- (d) Żel w którym umieszczone są światłowody. Żelu używa się w przypadku kabli uniwersalnych które mogą być kładzione pod ziemią w kanałach telekomunikacyjnych,
- (e) Ostatnia warstwa, która otacza pojedyncze włókno światłowodowe. Warstwa ta chroni delikatne włókno szklane przed złamaniem i innymi uszkodzeniami. Światłowód umieszczony wewnątrz tej warstwy można wyginać niemal pod dowolnym kątem (nie powinno się wyginać zbyt mocno). W celu poprawnego podłączenia wtyczek po obu końcach światłowodu warstwa ta każdego światłowodu posiada inny kolor,
- (f) Włókno światłowodowe przez które przebiega sygnał w postaci światła (światłowód).

5. Wi-Fi

Wi-fi – potoczne określenie zestawu standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem wi-fi jest budowanie sieci lokalnych (LAN) opartych na komunikacji radiowej, czyli WLAN. Zasięg od kilku metrów do kilku kilometrów i rzeczywistej przepustowości sięgającej 900 Mb/s, przy transmisji w standardzie 802.11ac na

trzech kanałach o szerokości 80 MHz jednocześnie. Produkty zgodne z wi-fi mają na sobie odpowiednie logo, które świadczy o zdolności do współpracy z innymi produktami tego typu.

Standardy w sieciach bezprzewodowych

Główne standardy w sieciach bezprzewodowych:

- 802.11a – do 54 Mb/s częstotliwość 5 GHz;
- 802.11b – 11 Mb/s częstotliwość 2,4 GHz ma zasięg ok. 30 m w pomieszczeniu i 120 m w otwartej przestrzeni; w praktyce można osiągnąć transfery rzędu 5,5 Mb/s. Materiały takie jak woda, metal, czy beton obniżają znacznie jakość sygnału; standard 802.11b podzielony jest na 14 kanałów o szerokości 22 MHz które częściowo się pokrywają, Polska wykorzystuje tylko pasma od 2400 do 2483,5 MHz – kanał od 1 do 13;
- 802.11g – 54 Mb/s częstotliwość 2,4 GHz, standard wi-fi, który powstał w czerwcu 2003 roku, w praktyce osiągalne są transfery do 20-22Mbit/s przy transmisji w jedną stronę, wykorzystanie starszych urządzeń w tym standardzie powoduje zmniejszenie prędkości do 11 Mb/s, jest bardziej podatna na zakłócanie i wymaga silniejszego i stabilniejszego sygnału niż 802.11b;
- 802.11n – 300 Mb/s częstotliwość 5 GHz oraz 150Mb/s w częstotliwości 2,4 GHz, obecnie najpopularniejszy, który został wprowadzony na rynek w 2007 roku jako „draft", choć urządzenia „pre-N" pojawiały się już od 2002 roku. W dniu 4.09.2009 „draft-N" został ratyfikowany jako standard, w praktyce osiągalne są transfery rzędu 150Mbit/s w jedną stronę, jednak wymaga on bardzo silnego i stabilnego sygnału do działania.
- 802.11ac – do 1 Gb/s, zaprezentowany w 2012 roku.
- 802.11ax – do 10 Gb/s, zaprezentowany w 2017 roku.

oraz:

- 802.11c
- 802.11d
- 802.11e
- 802.11f
- 802.11h (w Europie odpowiednikiem jest 802.11a na częstotliwości 5 GHz)
- 802.11i (w tym systemie wprowadzono nowe zabezpieczenia za pomocą szyfrowania)
- 802.11j (powstał ze standardu 802.11a na potrzeby Japonii)
- 802.11r (dość szybki roaming)

6. Protokoły

Protocol data unit inaczej **PDU** dzielimy na modele **ISO OSI** oraz **TCP/IP**.

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

Dane, segmenty, pakiety, ramki, bity

W poszczególnych warstwach w modelu odniesienia ISO/OSI przechodzące dane noszą nazwę jednostek danych protokołu PDU (ang. Protocol Data Unit). Jednostki te mają różne nazwy w zależności od protokołu. I tak w trzech górnych warstwach mamy do czynienia ze strumieniem danych, w warstwie transportu są segmenty, w warstwie sieci są pakiety, w warstwie łącza danych – ramki, a w warstwie fizycznej – bity (zera i jedynki). Jednostki te w poszczególnych warstwach różnią się częścią nagłówkową.

Model OSI

Model OSI (pełna nazwa ISO OSI RM, ang. ISO Open Systems Interconnection Reference Model – model odniesienia łączenia systemów otwartych) lub OSI – standard zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej. Model ISO OSI RM jest traktowany jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Podstawowym założeniem modelu jest podział systemów sieciowych na 7 warstw (ang. layers) współpracujących ze sobą w ściśle określony sposób. Został przyjęty przez ISO w 1984 roku a najbardziej interesującym organem jest wspólny komitet powołany przez ISO/IEC, zwany Joint Technical Committee 1- Information Technology (JTC1). Formalnie dzieli się jeszcze na podkomitety SC.

Warstwy wyższe

- **Warstwa 7: aplikacji**
  Warstwa aplikacji jest warstwą najwyższą, zajmuje się specyfikacją interfejsu, który wykorzystują aplikacje do przesyłania danych do sieci (poprzez kolejne warstwy modelu ISO/OSI). W przypadku sieci komputerowych aplikacje są zwykle procesami uruchomionymi na odległych hostach. Interfejs udostępniający programistom usługi dostarczane przez warstwę aplikacji opiera się na obiektach nazywanych gniazdami (ang. socket).
  Jeżeli użytkownik posługuje się oprogramowaniem działającym w architekturze klient-serwer, zwykle po jego stronie znajduje się klient, a serwer działa na maszynie

podłączonej do sieci świadczącej usługi równocześnie wielu klientom. Zarówno serwer, jak i klient znajdują się w warstwie aplikacji. Komunikacja nigdy nie odbywa się bezpośrednio między tymi programami. Kiedy klient chce przesłać żądanie do serwera, przekazuje komunikat w dół do warstw niższych, które fizycznie przesyłają go do odpowiedniej maszyny, gdzie informacje ponownie wędrują w górę i są ostatecznie odbierane przez serwer. Jednocześnie zapewnia interfejs między aplikacjami, których używamy, a siecią (umożliwia komunikację).

- **Warstwa 6: prezentacji**
  Podczas ruchu w dół zadaniem warstwy prezentacji jest przetworzenie danych od aplikacji do postaci kanonicznej (ang. canonical representation) zgodnej ze specyfikacją OSI-RM, dzięki czemu niższe warstwy zawsze otrzymują dane w tym samym formacie. Kiedy informacje płyną w górę, warstwa prezentacji tłumaczy format otrzymywanych danych na zgodny z wewnętrzną reprezentacją systemu docelowego. Wynika to ze zróżnicowania systemów komputerowych, które mogą w różny sposób interpretować te same dane. Dla przykładu bity w bajcie danych w niektórych procesorach są interpretowane w odwrotnej kolejności niż w innych. Warstwa ta odpowiada za kodowanie i konwersję danych oraz za kompresję / dekompresję; szyfrowanie / deszyfrowanie. Warstwa prezentacji obsługuje np. MPEG, JPG, GIF itp.

- **Warstwa 5: sesji**
  Warstwa sesji otrzymuje od różnych aplikacji dane, które muszą zostać odpowiednio zsynchronizowane. Synchronizacja występuje między warstwami sesji systemu nadawcy i odbiorcy. Warstwa sesji „wie", która aplikacja łączy się z którą, dzięki czemu może zapewnić właściwy kierunek przepływu danych – nadzoruje połączenie. Wznawia je po przerwaniu.

Warstwy niższe

- **Warstwa 4: transportowa**
  Warstwa transportowa segmentuje dane oraz składa je w tzw. strumień. Warstwa ta zapewnia całościowe połączenie między stacjami: źródłową oraz docelową, które obejmuje całą drogę transmisji. Następuje tutaj podział danych na części, które są kolejno indeksowane i wysyłane do docelowej stacji. Na poziomie tej warstwy do transmisji danych wykorzystuje się dwa protokoły TCP (ang. Transmission Control Protocol) oraz UDP (ang. User Datagram Protocol). W przypadku gdy do transmisji danych wykorzystany jest protokół TCP stacja docelowa po odebraniu segmentu wysyła potwierdzenie odbioru. W wyniku niedotarcia któregoś z segmentów stacja docelowa ma prawo zlecić ponowną jego wysyłkę (kontrola błędów transportu). W przeciwieństwie do protokołu TCP w protokole UDP nie stosuje się potwierdzeń. Protokół UDP z racji konieczności transmisji mniejszej ilości danych zazwyczaj jest szybszy od protokołu TCP, jednakże nie gwarantuje dostarczenia pakietu. Oba protokoły warstwy transportowej stosują kontrolę integralności pakietów, a pakiety zawierające błędy są odrzucane.

- **Warstwa 3: sieciowa**
  Warstwa sieciowa jako jedyna dysponuje wiedzą dotyczącą fizycznej topologii sieci. Rozpoznaje, jakie drogi łączą poszczególne komputery (trasowanie) i decyduje, ile informacji należy przesłać jednym z połączeń, a ile innym. Jeżeli danych do przesłania jest zbyt wiele, to warstwa sieciowa po prostu je ignoruje. Nie musi zapewniać pewności transmisji, więc w razie błędu pomija niepoprawne pakiety danych. Standardowa paczka danych czasami oznaczana jest jako NPDU (ang. Network Protocol Data Unit). Nie znajdują się w nim żadne użyteczne dla użytkowników dane. Jedyne jego zadanie, to zapewnienie sprawnej łączności między bardzo odległymi punktami sieci. Routery są podstawą budowy rozległych sieci informatycznych takich jak Internet, bo potrafią odnaleźć najlepszą drogę do przekazania informacji. Warstwa sieciowa podczas ruchu w dół umieszcza dane wewnątrz pakietów zrozumiałych dla warstw niższych (kapsułkowanie). Jednocześnie warstwa sieci używa czterech procesów (adresowanie, enkapsulacja, routing, dekapsulacja). Protokoły warstwy sieci to: (IPv4, IPv6, ICMP, NOVELL IPX, APPLE TALK, CLNS/DECN itd.).

- **Warstwa 2: łącza danych**
  Warstwa łącza danych jest czasami nazywana warstwą liniową lub kanałową. Ma ona nadzorować jakość przekazywanych informacji. Nadzór ten dotyczy wyłącznie warstwy niższej. Warstwa łącza danych ma możliwość zmiany parametrów pracy warstwy fizycznej, tak aby obniżyć liczbę pojawiających się podczas przekazu błędów. Zajmuje się pakowaniem danych w ramki i wysyłaniem do warstwy fizycznej. Rozpoznaje błędy związane z gubieniem pakietów oraz uszkodzeniem ramek i zajmuje się ich naprawą. Podczas ruchu w dół w warstwie łącza danych zachodzi enkapsulacja pakietów z warstwy sieciowej tak, aby uzyskać ramki zgodne ze standardem. Czasami są one oznaczane jako LPDU (ang. data Link Protocol Data Unit).
  Ramka danych przeważnie składa się z:
    - ID odbiorcy – najczęściej adres MAC stacji docelowej lub bramy domyślnej,
    - ID nadawcy – najczęściej adres MAC stacji źródłowej,
    - informacja sterująca – zawiera dane o typie ramki, trasowaniu, segmentacji itp.,
    - CRC (ang. Cyclic Redundancy Check) – kod kontroli cyklicznej – odpowiada za korekcję błędów i weryfikację poprawności danych otrzymywanych przez stację docelową.

  Warstwa łącza danych dzieli się na dwie podwarstwy:
    - LLC (ang. logical link control) – sterowania łączem danych – kontroluje poprawność transmisji i współpracuje przede wszystkim z warstwą sieciową w obsłudze usług połączeniowych i bezpołączeniowych.
    - MAC (ang. media access control) – sterowania dostępem do nośnika – zapewnia dostęp do nośnika sieci lokalnej i współpracuje przede wszystkim z warstwą fizyczną.
    - Urządzenia działające w tej warstwie to: most i przełącznik.

- **Warstwa 1: fizyczna**
  Fundamentem, na którym zbudowany jest model referencyjny OSI, jest jego warstwa fizyczna. Określa ona wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego, radiowego wysyłania i odbierania sygnałów. Warstwa fizyczna składa się z czterech obszarów funkcjonalnych:
    - mechanicznego,
    - elektrycznego,
    - funkcjonalnego,
    - proceduralnego.

  Wspólnie obejmują one wszystkie mechanizmy potrzebne do obsługi transmisji danych, takie jak techniki sygnalizacyjne, napięcie elektryczne powodujące przepływ prądu elektrycznego przenoszącego sygnał, rodzaje nośników i odpowiadające im właściwości impedancji, elektroniczne składniki kart sieciowych, a nawet fizyczny kształt złącza używanego do terminacji nośnika.
  Warstwa fizyczna przesyła i odbiera sygnały zaadresowane dla wszystkich protokołów jej stosu oraz aplikacji, które je wykorzystują. Musi ona więc wykonywać kilka istotnych funkcji – w szczególności:
    - Aby móc nadawać dane, musi ona:
      - zamieniać dane znajdujące się w ramkach na strumienie binarne,
      - wykonywać taką metodę dostępu do nośnika, jakiej żąda warstwa łącza danych,
      - przesyłać ramki danych szeregowo (czyli bit po bicie) w postaci strumieni binarnych.
    - W celu odbierania danych konieczne jest natomiast:
      - oczekiwanie na transmisje przychodzące do urządzenia hosta i do niego zaadresowane,
      - odbiór odpowiednio zaadresowanych strumieni,
      - przesyłanie binarnych strumieni do warstwy łącza danych w celu złożenia ich z powrotem w ramki.

Model TCP/IP

Model TCP/IP (ang. Transmission Control Protocol/Internet Protocol) – teoretyczny model warstwowej struktury protokołów komunikacyjnych. Model TCP/IP został stworzony w latach 70. XX wieku w DARPA, aby pomóc w tworzeniu odpornych na atak sieci komputerowych. Potem stał się podstawą struktury Internetu.

- **Warstwa aplikacji**
  Warstwa procesowa czy warstwa aplikacji (ang. process layer) to najwyższy poziom, w którym pracują użyteczne dla człowieka aplikacje takie jak np. serwer WWW czy przeglądarka internetowa. Obejmuje ona zestaw gotowych protokołów, które aplikacje wykorzystują do przesyłania różnego typu informacji w sieci. Wykorzystywane protokoły to m.in.: HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Window.

- **Warstwa transportowa**
  Warstwa transportowa (ang. host-to-host layer) gwarantuje pewność przesyłania danych oraz kieruje właściwe informacje do odpowiednich aplikacji. Opiera się to na wykorzystaniu

portów określonych dla każdego połączenia. W jednym komputerze może istnieć wiele aplikacji wymieniających dane z tym samym komputerem w sieci i nie nastąpi wymieszanie się przesyłanych przez nie danych. To właśnie ta warstwa nawiązuje i zrywa połączenia między komputerami oraz zapewnia pewność transmisji.

- **Warstwa Internetu**
  Warstwa Internetu lub warstwa protokołu internetowego (ang. internet protocol layer) to sedno działania Internetu. W tej warstwie przetwarzane są datagramy posiadające adresy IP. Ustalana jest odpowiednia droga do docelowego komputera w sieci. Niektóre urządzenia sieciowe posiadają tę warstwę jako najwyższą. Są to routery, które zajmują się kierowaniem ruchu w Internecie, bo znają topologię sieci. Proces odnajdywania przez routery właściwej drogi określa się jako trasowanie.

- **Warstwa dostępu do sieci**
  Warstwa dostępu do sieci lub warstwa fizyczna (ang. network access layer) jest najniższą warstwą i to ona zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi. Najczęściej są to karty sieciowe lub modemy. Dodatkowo warstwa ta jest czasami wyposażona w protokoły do dynamicznego określania adresów IP.

7. RFC

RFC (ang. Request for Comments – dosłownie: prośba o komentarze) – zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum związanych z Internetem oraz sieciami komputerowymi. Każdy z nich ma przypisany unikatowy numer identyfikacyjny, zwykle używany przy wszelkich odniesieniach. Publikacją RFC zajmuje się Internet Engineering Task Force.

Dokumenty nie mają mocy oficjalnej, jednak niektóre z nich zostały później przekształcone w oficjalne standardy sieciowe, np. opis większości popularnych protokołów sieciowych został pierwotnie opisany właśnie w RFC.

8. Enkapsulacja i dekapsulacja

Enkapsulacja (dekapsulacja) danych jest procesem zachodzącym w kolejnych warstwach modelu ISO/OSI.

Proces enkapsulacji oznacza dokładanie dodatkowej informacji (nagłówka) związanej z działającym protokołem danej warstwy i przekazywaniu tej informacji warstwie niższej do kolejnego procesu enkapsulacji.

Proces dekapsulacji polega na zdejmowaniu dodatkowej informacji w kolejnych warstwach modelu ISO/OSI.

9. LAN

Lokalna sieć komputerowa, LAN (od ang. local area network) – sieć komputerowa łącząca komputery na określonym obszarze (blok, szkoła, laboratorium, biuro). Sieć LAN może być wydzielona zarówno fizycznie, jak i logicznie w ramach innej sieci. Główne różnice LAN w porównaniu z WAN to wyższy wskaźnik transferu danych i mniejszy obszar geograficzny.

10. WLAN

Bezprzewodowa sieć lokalna, WLAN (od ang. wireless local area network) – sieć lokalna, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów. W Polsce termin Wi-Fi (chociaż pierwotnie był nazwą tylko jednego produktu używającego określonego standardu WLAN) używany jest jako synonim określenia WLAN.

11. VLAN

Wirtualna sieć lokalna, VLAN (od ang. virtual local area network) – sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

Do tworzenia VLAN-ów wykorzystuje się konfigurowalne lub zarządzalne przełączniki, umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych, przez separację ruchu między określonymi grupami portów. Komunikacja między VLAN-ami jest możliwa, gdy w VLAN-ach tych partycypuje port należący do routera lub z wykorzystaniem przełączników warstwy trzeciej. W przełącznikach konfigurowalnych zwykle spotyka się tylko najprostszą formę VLAN-ów, wykorzystującą separację grup portów.

W przełącznikach zarządzalnych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (tagowanie) poprzez doklejenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (trunking). W przypadku urządzeń zgodnych z ISL ramki są kapsułkowane w całości.

Niektóre nowe karty sieciowe komputerów klasy PC (w tym również interfejsy sieciowe laptopów) umożliwiają skonfigurowanie trybu pracy na tryb zgodny z IEEE 802.1Q. Możliwe jest wtedy bezpośrednie podłączenie komputera do portu przełącznika, na którym jest skonfigurowana sieć VLAN. Na takiej karcie można również ustawić korzystanie z wielu VLAN-ów jednocześnie (tzw. trunku).

Protokoły: IEEE 802.1Q, Inter-Switch Link (ISL), rozwiązanie Cisco.

Generacje sieci wirtualnych

- Pierwszą generacją są sieci wirtualne tworzone jako grupy portów czy grupy określonych adresów fizycznych MAC. Możliwości tworzenia tego typu sieci są udostępniane przez większość obecnych na rynku przełączników.
- Drugą generacją są sieci wirtualne tworzone na podstawie protokołu lub adresu użytkowników, wykorzystujących do komunikacji protokół warstwy trzeciej modelu OSI. Sieci wirtualne tej generacji, jako jedyne mają możliwość łączenia się ze sobą dzięki zastosowaniu

wspomnianej wcześniej techniki routingu. Generacja ta, bardziej skomplikowana niż pierwsza, jest skutecznie wprowadzona tylko w niewielkiej liczbie przełączników.

- Trzecią generacją są sieci wirtualne określone na podstawie wykorzystywanej przez użytkowników aplikacji lub kryteriów wybranych przez użytkownika, a zdefiniowanych w formacie ramki danego protokołu sieciowego. Sieci VLAN tej generacji można tworzyć opierając się na nielicznych typach przełączników obecnie dostępnych na rynku.

Rodzaje sieci wirtualnych

- Sieci wirtualne określone jako grupy portów
- Sieci wirtualne jako grupy adresów fizycznych MAC
- Sieci wirtualne definiowane przez wykorzystywany protokół warstw wyższych modelu OSI
- Sieci wirtualne określone przez adresy logiczne urządzeń (adresy warstwy trzeciej modelu OSI)
- Sieci wirtualne określone jako grupa multicast
- Sieci wirtualne określone na podstawie własnych kryteriów użytkownika
- Sieci wirtualne określone na podstawie parametrów przekazanych przez serwer uwierzytelniania

12. AAA (Authentication, Authorization, Accounting)

Systemy AAA (ang. authentication, authorization and accounting) umożliwiają zmniejszenie tego typu zagrożeń przez:

- budowę unikalnych i niemożliwych do odkrycia cech charakterystycznych każdego użytkownika systemu IT (tzw. credentiali),
- jednoznaczną identyfikację użytkownika (tzw. autentykację) na podstawie tych cech,
- po poprawnej autentykacji nadanie mu w systemie IT, odpowiednich zdefiniowanych wcześniej praw dostępu (tzw. autoryzacja),
- rejestrowanie jego aktywności w systemie (za pomocą dzienników zdarzeń tzw. logów),
- zarządzanie regułami prawami dostępu – czyli administrację.

Cechami charakterystycznymi użytkownika mogą być:

- elementy stałe, np. podane hasło, PIN, smartkarta,
- generowane dynamicznie w czasie (np. numer z tokenu czy telefonu GSM),
- dane biometryczne np. odcisk palca, obraz siatkówki oka itp.

System autoryzacji i uwierzytelniania, aby wzmocnić odporność na potencjalne włamanie, mogą wykorzystywać następujące rozwiązania:

- autentykację przy użyciu 2-3 cech charakterystycznych (2-factor authenthication),
- jedno silne hasło zamiast 5 słabych poprzez użycie jednego wspólnego, silnego systemu uwierzytelniania do wszystkich aplikacji (tzw SSO – Single Sign On),

- w wypadku braku uwierzytelnienia natychmiastowe odcięcie od warstwy fizycznej sieci LAN (tzw. NAC – Network Access Control).

a. **Authentication** inaczej uwierzytelnianie. Uwierzytelnianie służy nam do określania czy dana osoba jest faktycznie osobą za jaką się podaje. Jest to więc operacja weryfikowania tożsamości.
b. **Authorization** jest to autoryzacja polega na sprawdzeniu czy osoba logująca się mam prawo dostępu do danego zasobu.
c. **Accounting** jest procesem zbierania informacji i logów dotyczących poprzednich dwóch etapów – czyli kto uzyskał dostęp, do czego i kiedy. Dane te są zbierane przede wszystkim w celu przeprowadzania audytów bezpieczeństwa.

13. Cechy protokołu SSH

- Działa w warstwie sesji modelu ISO/OSI oraz w warstwie aplikacji modelu TCP/IP
- Opiera się na protokole transportu strumienia (TCP)
- Zapewnia dodatkową kompresję
- Zapewnia tunelowe sesji terminala
- Zapewnia tunelowy protokołu X11 oraz innych
- Zapewnia negocjację algorytmu kryptograficznej

14. Szyfrowanie w OSI

- Typ 0 jawny tekst hasła widoczne dla wszystkich użytkowników
  switch(config)# line vty 0 15
  switch(config-line)# password cisco
  switch(config-line)# login
- Typ 5 zaszyfrowany hasła są nieodwracalnie zaszyfrowane algorytmem MD5
  switch(config)# usename *uzytkownik* **secret** *haslo*
- Typ 7 ukryty (wydaje mi się że jest to najlepsze rozwiązanie) hasła są kodowane algorytmem Cisco i możliwe jest ich odkodowanie (www, key chain)
  switch(config)# service password-encryption
- Typ 4 zaszyfrowany wykorzystywany do tego celu jest algorytm SHA256 z solą (salt)

15. VLAN

- Natywny VLAN zwany czasem VLANem pierwotnym jest to rodzaj sieci wirtualnej, która obsługuje tak zwany ruch nieoznakowany, czyli przesyła ramki, które nie mają identyfikatora VLAN. Łącza trunkowe, czasami nazywane magistralami 802.1Q, potrafią obsługiwać ruch pochodzący właśnie z różnych sieci VLAN, ruch oznakowany, otagowany, ale również ruch z poza sieci VLAN.
- VLAN zarządzający to rodzaj sieci wirtualnej, która utworzona jest na przełącznikach sieciowych po to aby odseparować ruch, tak zwany zarządzający (ang. management traffic), od faktycznego ruchu sieciowego, który generują komputery użytkowników. W pierwszym odcinku pokazałem jak konfigurować urządzenia za pomocą fizycznego

połączenia z wykorzystaniem kabla konsolowego. To oczywiście jest dobra, skuteczna i zarazem bezpieczna metoda konfiguracji urządzeń sieciowych, ale oczywiście nie jedyna.

- VLAN czarna dziura biorąc pod uwagę fakt, że w sieciach komputerowych jako cel nadrzędny powinniśmy obierać siebie bezpieczeństwo, coś musimy teraz zrobić z naszymi nieużywanymi portami. Te nieaktywne, nieużywane porty możemy dodać do jakiegoś fałszywego VLANu, w którym nie pracują żadne maszyny. Dzięki temu nawet jeśli jakiś intruz się do niego dostał, nie będzie mógł za wiele namieszać.

16. DHCP snooping

Funkcjonalność DHCP snooping, polega na przypisaniu do konkretnego portu zaufanego serwera DHCP, a co za tym idzie, uniemożliwi podłączenie „lewego" serwera, do któregoś z innych portów. Dodatkowo funkcjonalność pozwala na ograniczenie ilości możliwych do wysłania z inny portów komunikatów – żądań DHCP Discover, co uniemożliwi wykonanie ataku.

17. Tryby portów na switchu

- Switchport mode access - W tym trybie przełącznik akceptuje zwykle wszystkie nietagowane ramki i nadaje im znacznik z góry zdefiniowany za pomocą pola PVID. Jeśli dane mają zostać wysłane na port w trybie ACCESS – znacznik zostaje usunięty. Warto tutaj zaznaczyć, że w przypadku trybu ACCESS przypisać możemy tylko jeden wybrany VLAN.
- Switchport mode trunk - Ten tryb w zależności od producenta przełącznika zwykle definiowany jest jako pory którym „przepychane" są wszystkie VLANy jakie znajdują się w obrębie przełącznika.
- Switchport mode dynamic auto - Sprawia, że port Ethernet jest gotowy do konwersji łącza do łącza dalekosiężnego. Port staje się portem trunkingowym, jeśli sąsiedni port jest ustawiony na tryb trunk lub dynamiczny . Jest to tryb domyślny dla niektórych przełączników.
- Switchport mode dynamic desirable - Sprawia, że port aktywnie próbuje przekonwertować łącze na łącze trunkingowe. Port staje się portem trunk, jeśli sąsiedni port Ethernet jest ustawiony na tryb trunk, dynamiczny pożądany lub dynamiczny tryb automatyczny.
- Switchport nonnegotiable - wyłącza DTP. Port nie będzie wysyłać ramek DTP lub będzie podlegać wpływom jakichkolwiek przychodzących ramek DTP. Jeśli chcesz ustawić łącze między dwoma przełącznikami, gdy funkcja DTP jest wyłączona, musisz ręcznie skonfigurować trunking za pomocą polecenia (switch trunk trunk) po obu stronach.

18. Port-security

Port Security to rodzaj zabezpieczenia, które pozwala przekazywać ramki, tylko zaufanych urządzeń, a nie każdego, które do przełącznika podłączymy. Dzięki odpowiedniej konfiguracji

tej funkcjonalności, zabezpieczymy sieć w taki sposób, że tylko jeden komputer będzie mógł korzystać z danego portu.

Kiedy jakiś intruz będzie chciał dostać się do naszej sieci, np. poprzez próbę podłączenia swojego komputera, przełącznik zareaguje i zablokuje ruch na tym porcie. Zablokuje ponieważ adres MAC urządzenia intruza, nie będzie zaufany dla naszego przełącznika.

19. Protokół

- DTP - jest zastrzeżonym protokołem sieciowym opracowanym przez firmę Cisco Systems w celu negocjowania trunkingu na łączu między dwoma przełącznikami VLAN oraz w celu negocjowania rodzaju enkapsulacji trunkingowej, która ma być używana.
- VTP - (ang. VLAN Trunking Protocol) jego zadaniem jest przekazywanie informacji przełącznikom o sieci VLAN

20. Port Monitor (Port Mirroring)

Port mirroring (w przypadku urządzeń CISCO Port Monitor) jest funkcją, która pozwala na kopiowanie danych z danego, konkretnego portu lub grupy portów na inny. Chodzi o to, że dane, które transmitowane są np. z i do portu 1 mogą być kopiowane na np. port 7. Funkcja te może być wykorzystywana w celach diagnostycznych, np. jeśli chcemy analizować ruch sieciowych maszyn w naszej sieci. Wówczas wszystkie dane z portu źródłowego trafiają do naszego komputera dzięki temu możemy je analizować (wykorzystując np. program Wireshark) i szukać przyczyn błędnego działania usług sieciowych.

21. Ether Channel (Link Aggregation)

Agregacja łączy - technika, polegająca na łączeniu przełączników kilkoma połączeniami równocześnie, co pozwala na utworzenie za pomocą wielu fizycznych połączeń jednego połączenia logicznego (wirtualnego kanału) charakteryzującego się większą przepustowością oraz większą niezawodnością. Najlepiej łączyć w parzystą liczbę aby przepustowość była po równo rozdzielana.

22. IPv4

Opis

Czwarta wersja protokołu komunikacyjnego IP przeznaczonego dla Internetu. Identyfikacja hostów w IPv4 opiera się na adresach IP. Dane przesyłane są w postaci standardowych datagramów. Wykorzystanie IPv4 jest możliwe niezależnie od technologii łączącej urządzenia sieciowe – sieć telefoniczna, kablowa, radiowa, itp. IPv4 znajduje się obecnie w powszechnym użyciu.

Automatyczne przydzielanie adresów IPv4 może być realizowane poprzez zastosowanie protokołów DHCP, RARP, BOOTP, PPP.

W przypadku braku serwera DHCP w sieci, adres IP przydzielany jest z puli 169.254.0.1 – 169.254.255.254 z domyślną maską 255.255.0.0 przez mechanizm APIPA.

Prywatne adresy IP

Istnieje pula prywatnych adresów IP. Mogą być one wykorzystane tylko w sieciach lokalnych. Infrastruktura Internetu ignoruje te adresy IP. IANA (Internet Assigned Numbers Authority) zarezerwował następujące trzy bloki przestrzeni adresów IP dla prywatnych sieci:

- 10.0.0.0 - 10.255.255.255 – dla sieci prywatnych dawniej z klasy A (maska zakresu: 255.0.0.0)
- 172.16.0.0 - 172.31.255.255 – dla sieci prywatnych dawniej z klasy B (maska zakresu: 255.240.0.0)
- 192.168.0.0 - 192.168.255.255 – dla sieci prywatnych dawniej z klasy C (maska zakresu: 255.255.0.0)

Klasy

- **Klasa A /1-8 (maska)**
  Klasa A została stworzona do obsługi bardzo dużych sieci. Wstępnie zakładano, że zapotrzebowanie na tego typu sieci będzie stosunkowo niskie, dlatego też architektura klasy A zakłada małą liczbę sieci klasy A przy bardzo dużej liczbie hostów. Zakres rozpoczyna się od 1.0.0.1 kończy na 126.255.255.254. Adres 127.0.0.1 teoretycznie powinien zawierać się w sieci klasy A, praktycznie jednak został on przypisany do localhost i służy do testowania. Komunikacja z adresem 127.0.0.1 oznacza wymianę informacji wewnątrz jednego hosta.
- **Klasa B /9-16**
  Klasa B została stworzona do obsługi średnich i dużych sieci. W adresie IP sieci klasy B, adres sieci zajmuje pierwsze dwa oktety, natomiast pozostałe dwa określają adresy hostów. Zakres adresów IP sieci klasy B rozpoczyna się od 128.0.0.0 a kończy 191.255.255.255. Oznacza to, że sieć może obsłużyć maksymalnie 65 534 hosty a maksymalna ilość sieci klasy B wynosi 16 382.
- **Klasa C /17-24**
  Klasa C została stworzona do obsługi dużej liczby małych sieci. Pierwsze trzy oktety określają adres sieci natomiast oktet ostatni definiuje hosty. Dopuszczalny zakres

adresacji sieci klasy C rozpoczyna się od adresu IP 192.0.0.0 a kończy 223.255.255.255. Pojedyncza sieć klasy C pozwala obsłużyć 254 hosty, natomiast maksymalna ilość sieci klasy C wynosi 2 097 150.

- **Klasa D**
  Klasa D została stworzona do multiemisji (multicast). Adres multicast jest unikalnym adresem sieci, który kieruje pakiety do grup adresów IP. Takie rozwiązanie jest dużo wydajniejsze od tworzenie oddzielnego strumienia do poszczególnych odbiorców. Dopuszczalny zakres adresów IP hostów sięga od 224.0.0.0 do 239.255.255.254
- **Klasa E**
  Zdefiniowano klasę E, lecz jej adresy zostały zarezerwowane przez Internet Engineering Task Force (IETF) na potrzeby badawcze i klasa ta nie może być używana w Internecie. Adresy IP sieci klasy E zawarte są w zakresie od 240.0.0.0 do 255.255.255.255

23. NAT

Network Address Translation (translacja adresów sieciowych) – technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP.

24. DHCP

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

25. RARP

Reverse Address Resolution Protocol - protokół komunikacyjny przekształcania 48-bitowych fizycznych adresów MAC na 32-bitowe adresy IP w komputerowych sieciach typu Ethernet.

26. BOOTP

Bootstrap Protocol – protokół komunikacyjny typu UDP umożliwiający komputerom w sieci uzyskanie od serwera danych konfiguracyjnych, np. adresu IP.

27. PPP

Point-to-Point Protocol (protokół połączenia punkt-punkt) – protokół komunikacyjny warstwy łącza danych używany przy bezpośrednich połączeniach pomiędzy dwoma węzłami sieci. PPP może być również skonfigurowany na interfejsie szeregowym asynchronicznym i synchronicznym.

28. DNS

Domain Name System - system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.192.

29. APIPA

Automatic Private IP Addressing – metoda, która umożliwia komputerowi przypisanie sobie adresu IP wówczas, gdy serwer DHCP jest niedostępny lub nie istnieje w danej sieci. Metoda ta znacznie ułatwia konfigurowanie i obsługę niewielkiej, prostej sieci lokalnej (LAN, Local Area Network), w której jest używany protokół TCP/IP.