

Politechnika Łódzka
Instytut Informatyki Stosowanej

Podstawy działania sieci komputerowych

PIOTR URBANEK

Sieci przewodowe i bezprzewodowe

- URZĄDZENIA DOSTĘPU
- MEDIA PRZEWODOWE
- MEDIA BEZPRZEWODOWE
- SIECI BEZPRZEWODOWE

Komputer

Urządzenia dostępu

odpowiedzialne za: formatowanie danych w celu przesyłania ich w sieci, umieszczanie w sieci sformatowanych danych, odbieranie danych do nich zaadresowanych.

Urządzenia wzmacniania przesyłanych sygnałów

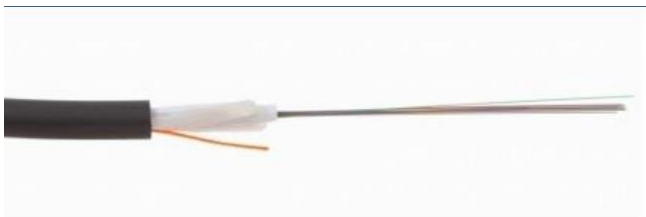
Stosowane w sieciach WAN. Wzmacniają sygnały, umożliwiają podłączenie wielu urządzeń do sieci.



Media przewodowe

Przewodowe media transmisyjne:

- kabel symetryczny (tzw. skrętka)
- kabel współosiowy (kabel koncentryczny)
- kabel światłowodowy (światłowód jednomodowy lub wielomodowy)
- kable energetyczne



Podstawowym nośnikiem jest kabel typu skrętka:

- nieekranowa (UTP)
- ekranowa (STP)

Odległość między urządzeniami dla skrętki UTP wynosi 100m

Odległość między urządzeniami dla skrętki STP wynosi 250m

Kabel ekranowy posiada folię ekranującą, co zapewnia mniejsze straty transmisji



Sieci bezprzewodowe

Elementy wykorzystywane do budowy sieci bezprzewodowej:

- karty sieciowe: najczęściej wmontowane w komputer
- punkty dostępowe (WAP – Wireless Access Point): określane zazwyczaj jako routery bezprzewodowe Wi-Fi
- anteny: wpływają na zasięg sieci
- repeatery (opcjonalne): wpływają na zwiększenie zasięgu sieci

Media bezprzewodowe

- Fale radiowe do transmisji wymagają planowania przydziału częstotliwości
- Obecnie najpopularniejszymi częstotliwościami używanymi do transmisji bezprzewodowej są 2,4 Ghz i wyższe
- Odległości na jakich stosuje się fale radiowe wynoszą do kilkudziesięciu kilometrów przy zastosowaniu specjalnych anten
- Fale elektromagnetyczne w zakresie podczerwieni IR (InfraRed)
- Stosowane na otwartym terenie, bądź w budynkach
- Źródłem promieniowania tych fal są diody elektroluminescencyjne lub diody laserowe
- Przy używaniu łącz bezprzewodowych w podczerwieni nie jest wymagane uzyskanie licencji na ich stosowanie w przeciwieństwie do fal radiowych
- Największym ograniczeniem tego medium jest ograniczony zasięg wynoszący do kilkudziesięciu metrów

Sieci LAN (*Local Area Network*)

TYPY SIECI LAN

ELEMENTY SKŁADOWE SIECI

MODELE POŁĄCZEŃ

Sieć LAN (Local Area Network)

Podstawowe pojęcia:

- Adres IP
- Ethernet
- Karta sieciowa
- Peer to peer
- Transfer danych
- Switch
- Router
- Maska podsieci
- Wireless LAN
- Topologia sieci

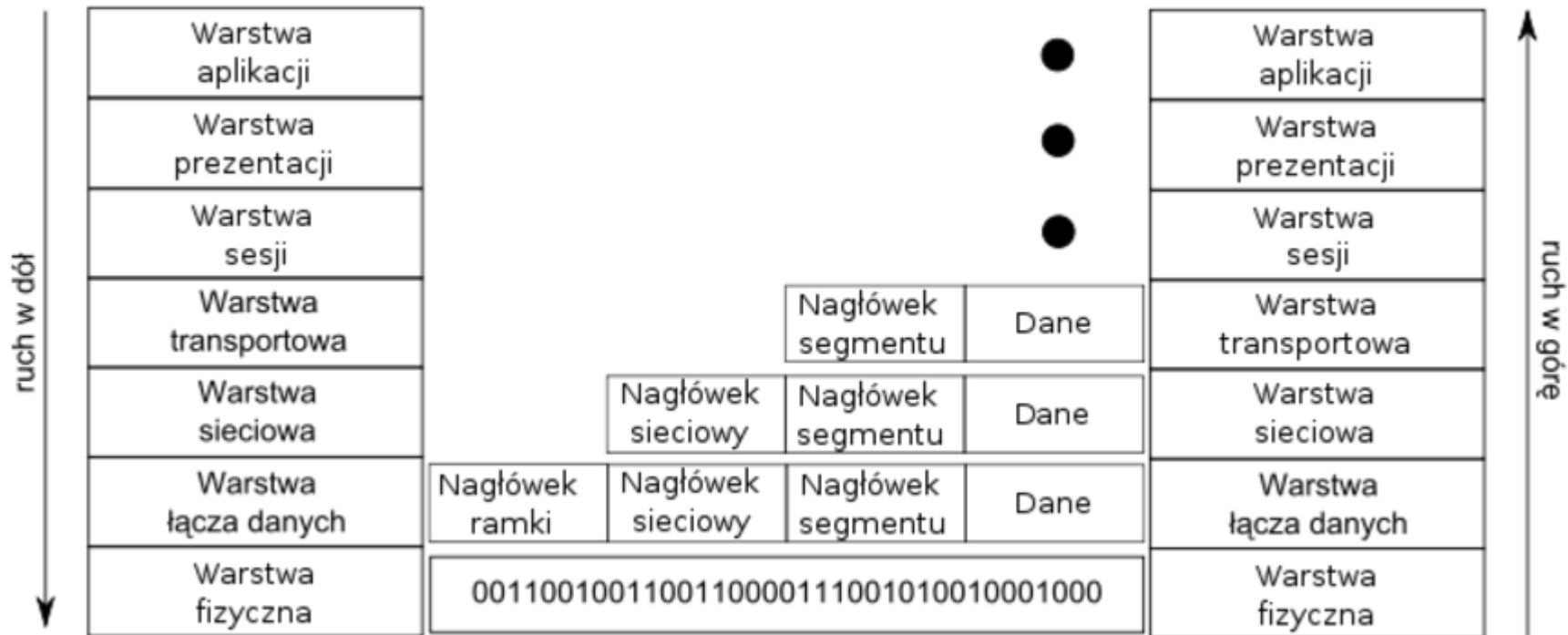
Sieć komputerowa – wszystko, co umożliwia dwóm, lub więcej komputerom komunikowanie się pomiędzy sobą, lub z innymi urządzeniami.

Sieci składają się ze sprzętu i oprogramowania

Podzielone są na dwie kategorie:

- Sieci lokalne (LAN)
- Sieci rozległe (WAN)

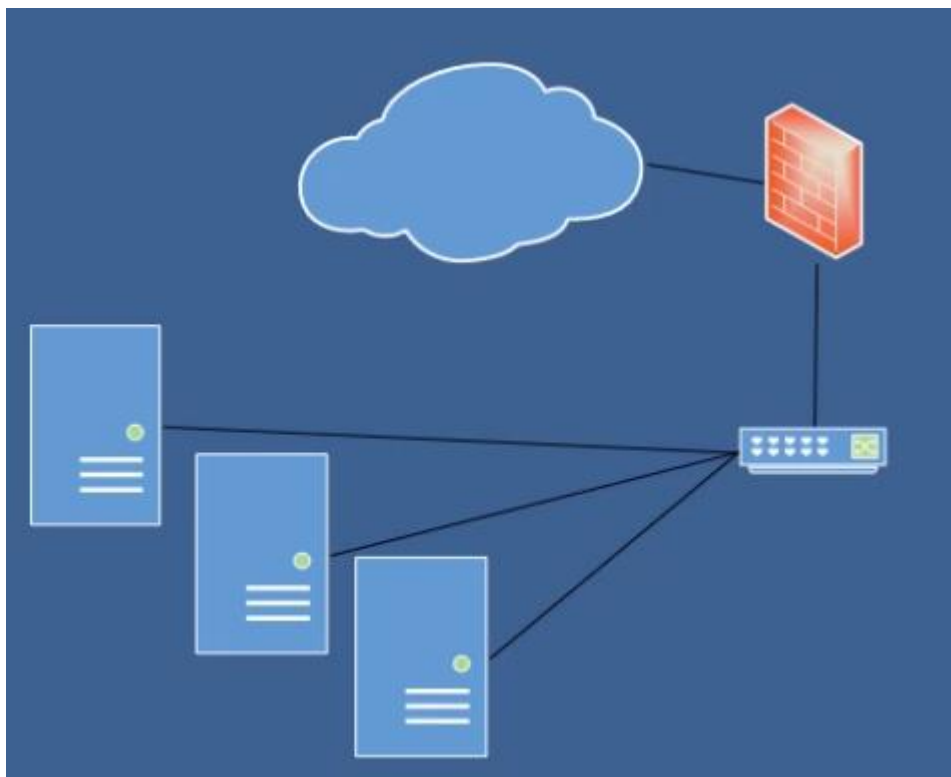
Warstwy modelu OSI



Warstwy modelu OSI

Layer	Defines
Warstwa 7 – Aplikacji	Umożliwia użytkownikom i aplikacjom dostęp do sieci
Warstwa 6 – Prezentacji	Przetwarza dane na wspólny format, zrozumiały dla niższych warstw
Warstwa 5 – Sesji	Odpowiada za synchronizację połączenia między nadawcą i odbiorcą
Warstwa 4 – Transportowa	Segmentuje dane i rozkłada je na tzw. Strumień. Zapewnia całościowe połączenie między stacjami: źródłową oraz docelową
Warstwa 3 - Sieciowa	Dysponuje wiedzą na temat fizycznej topologii sieci. Rozpoznaje, jakie drogi łączą poszczególne komputery
Warstwa 2 – Łączy danych	Rozpoznaje błędy związane z pominięciem pakietu oraz uszkodzeniem ramek i zajmuje się ich naprawą
Warstwa 1 – Fizyczna	Określa wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego, radiowego wysyłania i dobierania sygnałów

Sieć LAN



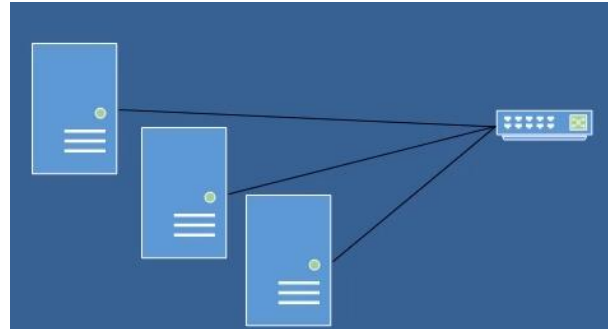
- Niewielka odległość między komputerami
- Jedno medium komunikacyjne, np. przewodowe lub bezprzewodowe

Programowe elementy składowe sieci

- **Programy poziomu sprzętowego (sterowniki):** zapewniają działanie urządzeń, takich, jak karta sieciowa, w której zapewniają komunikację komputera z siecią. Złącza RJ45, BNC, AUI.
- **Protokoły:** określają sposób i parametry komunikowania się urządzeń w sieci. Odpowiadają za standaryzację komunikacji urządzeń w sieci.
W sensie logicznym w sieciach LAN zawierają karty sieciowe – architektura LAN.
- **Oprogramowanie komunikacyjne**
 - Programy „mapowania dysków”
 - Protokół HTTP
 - Programy przesyłania plików
 - Poczta elektroniczna

Typy sieci LAN

- Sieci przewodowe
- Sieci bezprzewodowe
- Sieci wirtualne



Host – każde urządzenie podłączone do sieci i posiadające unikatowy adres IP (komputer, router, drukarka)

Adres IP

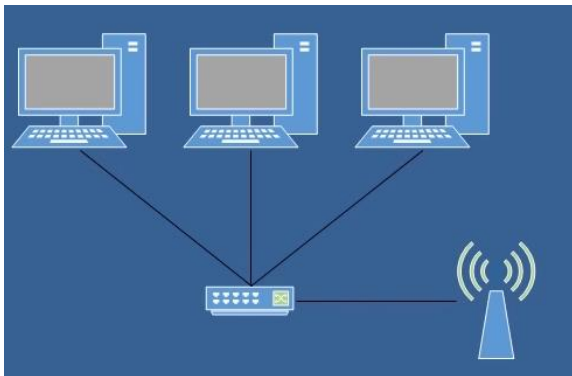
Identyfikuje urządzenie w sieci

Podzielony na dwie części:

Adres sieci: 192.168.1

Adres hosta: 1

Czyli **192.168.1.1**



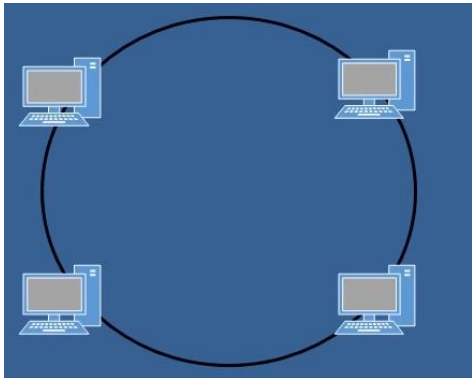
Topologie sieci LAN

Topologia logiczna – możliwe połączenia między punktami sieci.

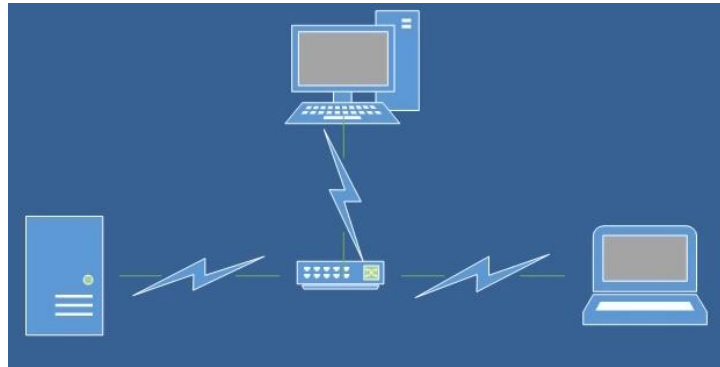
Topologia fizyczna – określa geometryczną organizację sieci lokalnych.

Są 3 rodzaje topologii fizycznej:

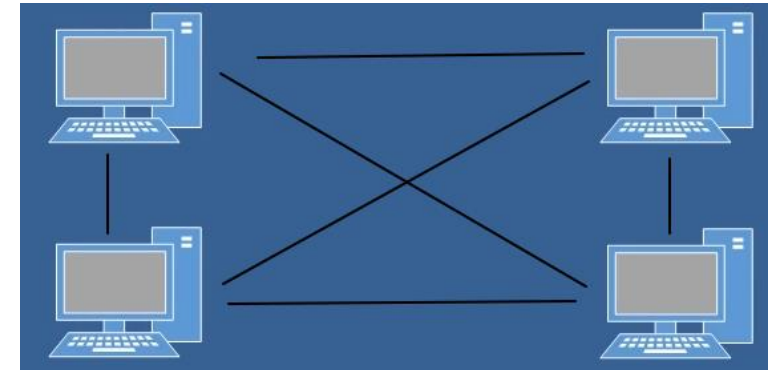
Topologia pierścienia



Topologia gwiazdy



Topologia siatki



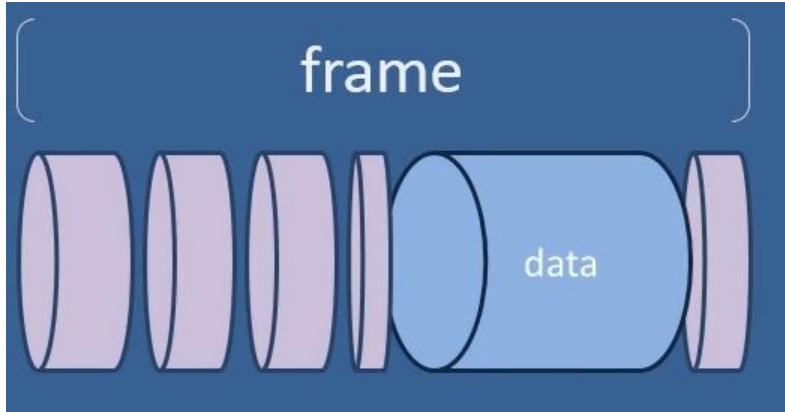
Technologia Ethernet

- Definiuje, w jaki sposób informacja jest wysyłana i odbierana przez urządzenia sieciowe
- Opisuje format ramek i protokoły z dwóch najniższych warstw modeli OSI
- Bazuje na schemacie węzłów podłączanych do wspólnego medium wysyłających i odbierających za jego pomocą specjalne komunikaty (ramki)
- Klasyczne sieci Ethernet charakteryzują się parametrami:
 - Czasowymi
 - Format ramki
 - Proces transmisji
 - Podstawowymi regułami ich tworzenia
- Standardy (10 MB/s, 100 MB/s, 1 GB/s, 10 GB/s)
- Urządzenia w sieci Ethernet wykorzystują standard CSMA/CD (Carrier Sense Multiple Access/ Collision Detect).

Ramki sieci Ethernet

Komputery w sieci Ethernet komunikują się za pomocą ramek. Jest to sekwencja bitów zawierających wykrywalny początek i koniec pakietów w strumieniu

Ramka jest zaliczana do drugiej warstwy modelu OSI.

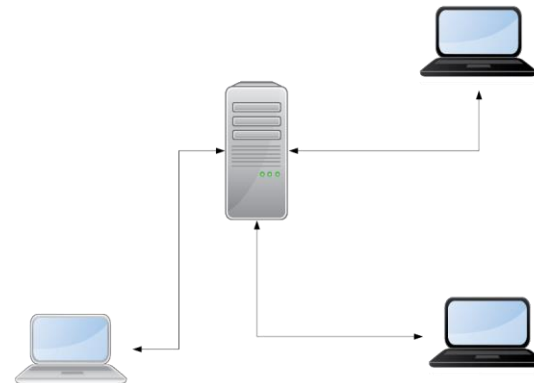


Model Klient - Serwer

- Architektura dotycząca podziału ról w sieci.
- Serwer zapewnia usługi dla klientów, zgłaszających do serwera żądania obsługi (service request).
- Z usług serwera może korzystać wielu klientów.
- Jeden klient może korzystać z wielu serwerów.
- Przykłady serwerów działających w oparciu o model klient – serwer
 - Serwer www
 - Serwer poczty elektronicznej

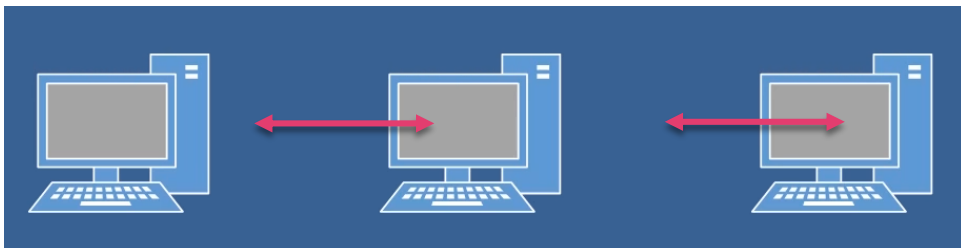
Model Klient - Serwer

- Klient jest stroną żądającą dostępu do danej usługi lub zasobu.
- Tryb pracy klienta jest aktywny – wysyła żądanie i oczekuje na odpowiedź
- Tryb pracy serwera jest pasywny – czeka on na żądania od klientów
- Serwer przetwarza zapytania od klientów i wysyła odpowiedzi
- Ze względu na podział wykonywanych zadań są trzy typy architektury „Klient – Serwer”:
 - Architektura dwuwarstwowa,
 - Architektura trójwarstwowa,
 - Architektura wielowarstwowa.



Model Peer – to – Peer (P2P – „Równy z Równym”)

- Model komunikacji sieciowej zapewniający wszystkim hostom te same uprawnienia (nie ma centralnego komputera).
- Każdy host może pełnić rolę serwera i klienta
- Zmienna struktura sieci P2P jest uzależniona od liczby podłączonych użytkowników, co niesie ryzyko odłączenia danego hosta od sieci, jeśli komputery sąsiednie się rozłączą. Zachowanie się sieci po utracie połączenia dzielimy na:
 - Model pasywny (sieć nie podejmuje żadnych działań).
 - Model aktywny (sieć próbuje zastąpić utracone połączenie nowym)



Różnice między modelami „P2P” a „Klient-Serwer”

Klient-serwer to system, w którym serwer świadczy usługi dołączonym stacjom roboczym. W systemie tym programy wykonywane są częściowo lub w całości po stronie klienta.

- Peer-to-Peer (równy z równym) jest modelem komunikacji w sieci komputerowej, który gwarantuje obydwu stacjom równorzędne prawa
- Wymiana danych w sieci P2P jest prowadzona bez pośrednictwa centralnego serwera

Protokół internetowy

- PRACA Z IPV4
- ADRES IP
- ADRESY I MASKI
- BRAMY DOMYŚLNE I SERWERY DNS
- PRACA Z IPV6
- MAPOWANIE ADRESÓW IPV4 NA IPV6

Protokół IPv4

- IPv4 jest czwartą wersją protokołu komunikacyjnego IP przeznaczonego dla Internetu
- Identyfikacja hostów w IPv4 opiera się na adresach IP
- Dane przesyłane są w formie standardowych datagramów
- Wykorzystanie IPv4 jest możliwe niezależnie od technologii łączącej urządzenia sieciowe: sieć telefoniczna, radiowa itp.
- W modelu TCP/IP protokół IPv4 znajduje się w warstwie sieciowej
- Komunikacja jest możliwa w protokole IP poprzez nadanie każdemu z hostów unikatowego identyfikatora - adresu

Adres IP

- Adresy IP składa się z czterech oktetów (liczb 8 bitowych), każdy pomiędzy 0 a 255.

Przykłady:

- 12.5.24.2
 - 127.0.0.1
 - 192.168.3.54
 - 208.32.56.232
- Adres 207.142.131.236 zapisujemy binarnie:
11001111 10001110 10000011 11101100
 - Komputery traktują adresy IP jako liczby 32-bitowe

Adresy i maski

Dana jest sieć składająca się z trzech komputerów:

-komputer 1: 192.168.1.1

-komputer 2: 192.168.1.2 Początek adresu wszystkich z nich jest ten sam, zmienia się tylko końcówka

-komputer 3: 192.168.1.3

W celu ścisłego zdefiniowania adresów przynależnych do danej sieci wymyślono pojęcie **maski** – liczba pierwszych bitów adresu jest taka sama

Maskę zapisuje się jak adres IP:

255.255.255.0 co binarnie daje: 11111111 11111111 11111111 00000000

Klasy adresów IP

Adresy IP zostały podzielone na cztery klasy: A, B, C i D

- W adresach klasy A tylko pierwszy oktet wskazuje adres sieci, pozostałe trzy oktety opisują unikatowy adres węzła w sieci – 255.0.0.0
- Adresy klasy B używają pierwszych dwóch oktetów do wskazywania adresu sieci i ostatnich dwóch jako unikalnego węzła sieci – 255.255.0.0
- W adresach klasy C używa się pierwszych trzech oktetów jako adresu sieciowego i tylko ostatniego oktetu jako adresu węzła – 255.255.255.0

Oznacza to, że adresy klasy C mogą być użyte do adresowania tylko do 254 węzłów

Publiczne i prywatne adresy IP

Adresy IPv4 są podzielone na publiczne i prywatne

- Publiczne adresy IP są widoczne dla innych hostów w Internecie
- Prywatne adresy IP są ukryte przed siecią Internet oraz innymi sieciami
- Adresy prywatne można wykorzystywać za pomocą lokalnych routerów w sieciach lokalnych.
Nie działają w publicznej części Internetu

Przykłady prywatnych adresów IP:

Klasa	Zakres początkowy	Zakres końcowy
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

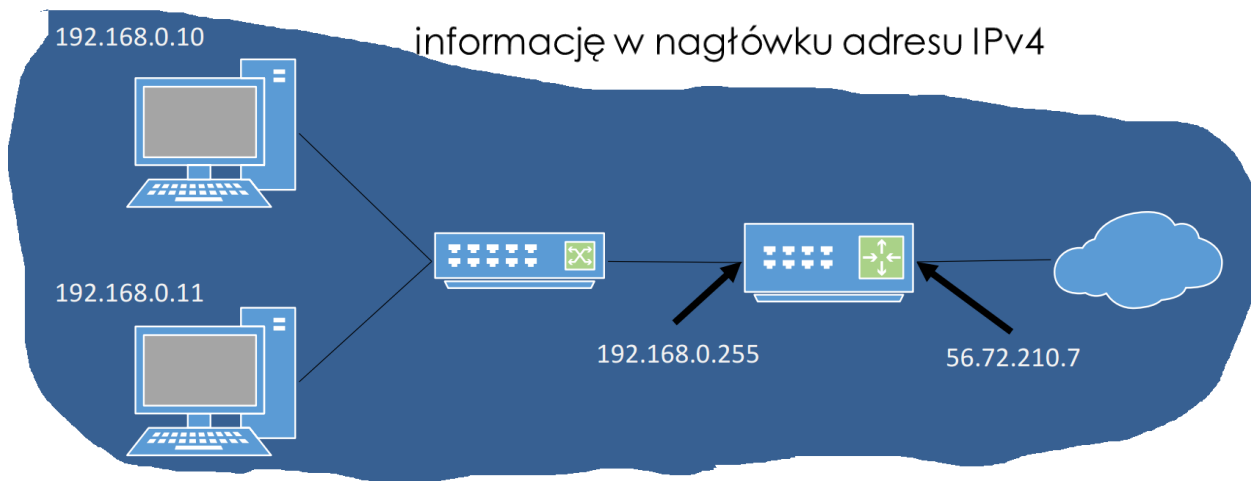
Bramy domyślne i serwery DNS

- Urządzenie chcąc nawiązać połączenie z Internetem musi mieć przypisaną bramę domyślną oraz serwer DNS
- Brama domyślna (Default gateway): Zapewnia domyślną trasę dla hostów protokołu TCP/IP w celu wzajemnej komunikacji w sieci
- Adres bramy domyślnej będzie pierwszym w kolejce, kiedy urządzenie będzie próbowało nawiązać połączenie z hostem na zewnątrz sieci lokalnej
- Serwer DNS pozwala na rozpoznawanie nazw domen i ich translację na adresy IP

Network Address Translation (NAT)

- Jest to technika przesyłania ruchu sieciowego przez router (urządzenie dostępne)
- Zapewnia metodę tłumaczenia adresu urządzenia w jednej sieci dla urządzeń działających w innej sieci
- Pozwala na komunikację hostów z sieci lokalnej z hostami w sieci Internet

Podczas przesyłania danych przez urządzenie do trasowania (router) NAT odpowiednio modyfikuje informację w nagłówku adresu IPv4



Subnetting

- **Subnetting** jest procesem dzielenia sieci na mniejsze logiczne podsieci
- Odbywa się poprzez transformację domyślnej maski podsieci w inne jednostki za pomocą pożyczania bitów
- Podsiecią nazywamy logiczny podział sieci IP

Protokół IPv6

- Następca protokołu IPv4
- Powstał z powodu wyczerpującej się liczby adresów IPv4
- Zwiększa przestrzeń dostępnych adresów IP poprzez zwiększenie długości adresu z 32 do 128 bitów
- IPv6 nie jest wstecznie kompatybilny z IPv4
- Przykładowy adres IPV6: 2001:4860:0000:2001:0000:0000:0000:0068

IPv6 – Typy adresów

- Adres **unicast**: identyfikuje pojedynczy interfejs; pakiety które są kierowane na ten typ adresu dostarczane są tylko do odbiorcy
- Adres **multicast**: identyfikuje grupę interfejsów (mogą należeć do różnych węzłów); pakiety wysyłane na ten adres są dostarczane do wszystkich członków grupy
- Adres **anycast**: podobnie jak adresy **multicast**, identyfikuje grupę interfejsów, jednak pakiet wysyłany na ten adres dostarczany jest tylko do najbliższego węzła

Mapowanie adresów IPv4 na IPv6

- Możliwe jest reprezentowanie adresów IPv4 jako adresów IPv6
- Jedną z możliwości jest stworzenie adresu IPv6, którego młodsze 32 bity zawierają adres IPv4, natomiast starsze 96 bitów jest wypełnione specjalnym wzorcem bitów: `::ffff`
- Tak skonstruowany adres ma postać: `::ffff:127.0.0.1` (za 127.0.0.1 można podstawić dowolny adres IP)
- W protokole IPv6 nie występuje pojęcie komunikacji broadcastowej (dane wysyłane są do wszystkich węzłów w danej podsieci)
- Aby wysłać dane do wielu odbiorców jednocześnie, należy skorzystać z komunikacji multicast

Praca z usługami sieciowymi

- PRZYDZIELANIE ADRESÓW IP
- USŁUGI TERMINALOWE
- DOSTĘP ZDALNY

Protokół DHCP

- Dynamic Host Configuration Protocol: protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych (w tym adresu IP)
- W sieci opartej na protokole TCP/IP każdy komputer ma co najmniej jeden adres IP i jedną maskę podsieci
- Pozwala na odciążenie administratora sieci poprzez dynamiczne przydzielanie adresów dla hostów w sieci

Przydzielanie adresów IP w protokole DHCP

- Przydzielanie ręczne: oparte jest na tablicy adresów MAC, oraz odpowiednich dla nich adresów IP. Jest ona tworzona przez administratora serwera DHCP. Prawo do pracy w sieci mają tylko zarejestrowane wcześniej komputery.
- Przydzielanie automatyczne: wolne adresy IP z zakresu ustalonego przez administratora są przydzielane kolejnym zgłaszającym się po nie klientom.
- Przydzielanie dynamiczne: pozwala na ponowne użycie adresów IP. Administrator sieci nadaje zakres adresów IP do rozdzielenia. Wszyscy klienci mają tak skonfigurowane interfejsy sieciowe, że po starcie systemu automatycznie pobierają swoje adresy.

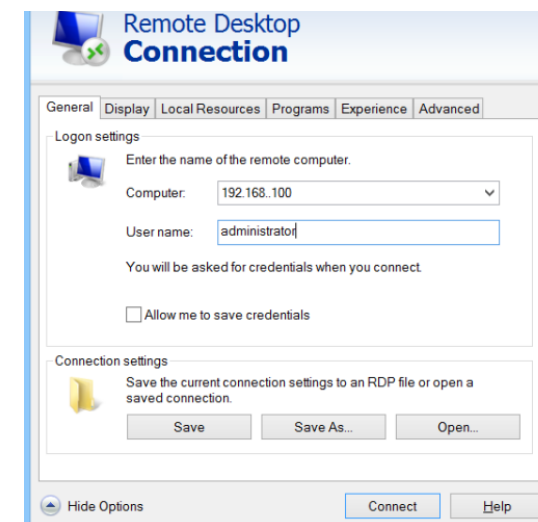
Serwer DHCP

Serwer może przyznawać adresy zgłaszającym się klientom po następującej konfiguracji:

- instalacji serwisu DHCP
- ustaleniu zakresu nadawanych adresów IP
- aktywowaniu zakresu adresów
- autoryzacji serwera

Usługi terminalowe

- Usługi terminalowe umożliwiają wydajne wdrażanie oprogramowania i jego obsługę w środowisku przedsiębiorstwa
- Usługi terminalowe w systemie Windows Server udostępniają technologie pozwalające użytkownikom uzyskać zdalny dostęp do programów zainstalowanych na serwerze terminali lub do pełnego pulpitu systemu Windows



Internet Protocol Security (IPsec)

Jest to protokół zestawu TCP/IP, który zapewnia szyfrowanie i autentykację pakietów IP.

Wyróżnia się trzy typy protokołu IPsec:

- Security association (**SA**): Generuje klucze szyfrowania i autentykacji
- Authentication Header (**AH**): Zapewniający integralność i autentykację danych
- Encapsulation security payload (**ESP**): Zapewnia te same usługi co AH, oraz dodatkowo poufność podczas przesyłania danych

Definiowanie DNS

Domain Name System (DNS – system nazw domenowych): 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

Jest niezbędny do funkcjonowania prawie wszystkich usług sieci Internet

Domain Name System należy do warstwy aplikacji modelu TCP/IP

Definiowanie WINS

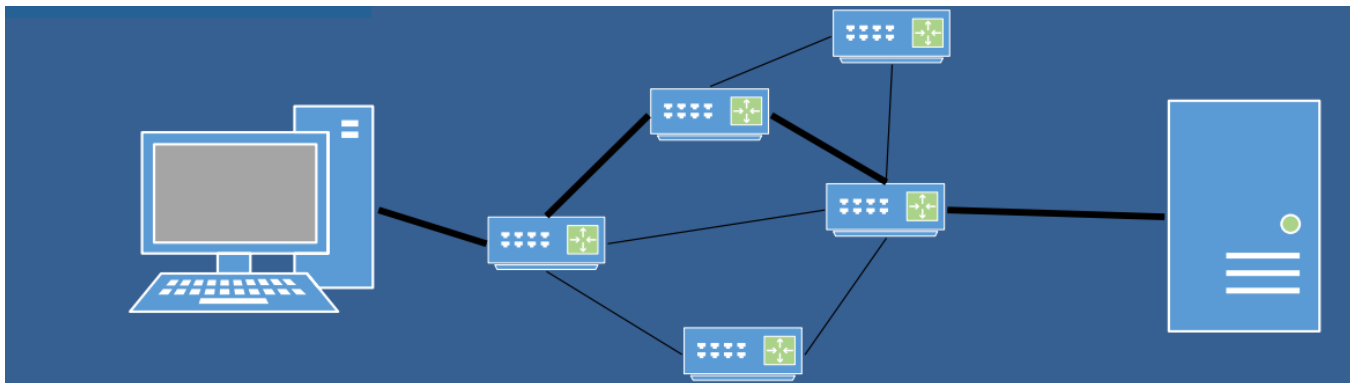
- Windows Internet Name Service (WINS): usługa stworzona przez Microsoft, umożliwiająca tłumaczenie nazw komputerów na adresy internetowe
- Użytkownik korzystający z WINS może odwoływać się do komputerów w sposób bardziej intuicyjny np. SEKRETARIAT – nazwa ta zostanie zamieniona na adres IP tego komputera
- Usługa jest przeznaczona dla niewielkich sieci

Sieć WAN (World Area Network)

- CO TO JEST ROUTING?
- ROUTING STATYCZNY
- PROTOKOŁY ROUTINGU
- TECHNOLOGIE I POŁĄCZENIA STOSOWANE W WAN

Routing

- Routing jest procesem zarządzania przepływem danych między segmentami sieci oraz między hostami lub routerami
- Zarządzanie przepływem danych może być realizowane dynamicznie przez router lub ustalone statycznie przez administratora sieci.
- W pamięci routera zapisane są tabele z informacjami dotyczącymi innych routerów w sieci



Routing statyczny oraz dynamiczny

- Routing jest procesem, w którym router używając poprzednich pakietów przesyła dane do miejsca przeznaczenia
- Routing statyczny: jest konfigurowany i zarządzany ręcznie, najczęściej przez administratora sieci. Każda zmiana w topologii sieci wymaga dokonania zmian w konfiguracji routingu
- Routing dynamiczny: jest dynamicznie konfigurowany oraz zarządzany przy użyciu specjalnych protokołów routingu. Router ustala trasę pakietów do odległej sieci na podstawie informacji od innych routerów.

Protokoły routingu

- Protokół routingu służy do komunikacji między routerami
- Pozwala jednemu routerowi dzielić się informacjami z innymi routerami, które są razem w jednej sieci
- Za pomocą protokołów routingu router zbiera informacje od innych routerów, budując swoją tablicę routingu

Protokoły routingu:

- Routing Information Protocol (**RIP**)
- Interior Gateway Routing Protocol (**IGRP**)
- Enhanced Interior Gateway Routing Protocol (**EIGRP**)
- Open Shortest Path First (**OSPF**)

Protokół routowalny

Protokół routowalny jest stosowany do bezpośredniego połączenia użytkowników

Protokoły routowalne:

- Internet Protocol (**IP**)
- Internetwork Packet Exchange (**IPX**)

Identyfikacja klas routingu dynamicznego

- Distance-vector: algorytm kopiujący okresowo tablicę routingu z jednego routera na inny. Regularne uaktualnienia między routerami komunikują zmiany w topologii sieci.
- Link-state: (zwany algorytmem Dijkstras): protokoły tego typu zachowują dokładną wiedzę na temat topologii sieci. W przeciwieństwie do algorytmów distance-vector posiadają dokładne informacje na temat odległych routerów oraz sieci.

Metryka routingu obejmuje następujące elementy:

- opóźnienie sieci
- przepustowość łącza
- niezawodność łącza
- maksymalną liczbę pakietów obsługiwanych przez komunikujące się interfejsy

Routing Information Protocol (RIP)

Protokół oparty na algorytmie distance-vector

- Metryki wyboru ścieżki są ustalane przy obliczaniu liczby skoków
- Jeśli liczba skoków przekracza 15 pakiet jest porzucany
- Uaktualnienia są domyślnie pobierane co 30 sekund

Interior Gateway Routing Protocol (IGRP)

Prawnie zastrzeżony i używany przez firmę CISCO

- Protokół typu distance-vector
- Jako metryk routingu używa przepustowości pasma, obciążenia pasma, opóźnienia i niezawodności pasma
- Pakiety uaktualniające są automatycznie rozsyłane co 90 sekund

Open Shortest Path First (OSPF)

Prawnie zastrzeżony i używany przez firmę CISCO

- Protokół oparty na algorytmie link-state
- Używa algorytmu SPF (Shortest Path First) do wyliczenia ścieżki o najmniejszym koszcie
- Uaktualnienia są automatycznie rozsyłane jeśli nastąpi zmiana w topologii sieci

Enhanced Interior Gateway Routing Protocol (EIGRP)

Protokół używający kombinacji obydwu algorytmów, distance-vector oraz link-state

- Używa zasady load balancingu (równoważenia obciążenia)
- Do wyliczenia najkrótszej ścieżki używa Diffused Update Algorithm (DUAL)
- Pakiety uaktualniające są rozsyłane co 90 sekund, lub gdy zmieni się topologia sieci

Definiowanie przesyłania pakietów

- Przesyłanie pakietów oznacza sposób, w jaki pakiety danych przemieszczają się i przesyłają w sieciach rozległych
- Do najważniejszych z nich należy standard X.25 oraz Frame Relay

Standard protokołu komunikacyjnego X.25

- Definiuje interfejs połączenia między terminalem danych DTE (Data Terminal Equipment) a urządzeniem transmisji danych DCE (Data Communications Equipment), dla terminali pracujących w trybie pakietowym, podłączonych do sieci publicznych
- X.25 definiuje warstwę fizyczną, warstwę łącza danych oraz warstwę sieci modelu OSI
- Używany w sieciach WAN



Modem (DCE)

X.25 Network

Standard protokołu komunikacyjnego Frame Delay

Frame Delay jest siecią z komutacją pakietów

- Używana jest do łączenia odległych sieci lokalnych (LAN)
- Służy do przesyłania danych, obrazu i głosu oraz dostępu do Internetu
- Sieć Frame Delay jest szybsza od sieci opartych na standardzie X.25
- Protokół funkcjonuje w dwóch pierwszych warstwach modelu OSI

Inne technologie WAN oraz łączności internetowej

- Asynchronous Transfer Mode (ATM)
- SONET
- Fiber Distributed Data Interface
- Digital Subscriber Line (DSL)
- BroadBand Cable