Główne funkcjonalności protokołu RTCP w mechanizmie transmisji danych.
Real Time Transport Control Protocol
- protokół sterujący, wspierający RTP
- nie transportuje danych
- dostarcza zwrotnej info odnośnie poprawności odebranych danych poprzez przesłanie statystyk
- wykorzystane do ewentualnej zmiany parametrów kodowania przez źródło
- przenosi stały identyfikator transportowy źródła protokołu RTP

Wymień i opisz rodzaje transmisji wideo w aspekcie liczby odbiorców.
Transmisja jeden-do-jednego, w których pojedynczy pakiet danych przesyłany jest od nadawcy do jednego odbiorcy, dokładnie pod jeden adres. Transmisja może być zrealizowana np. w oparciu o protokół RTP. Za pomocą tego protokołu klient kontaktuje się z serwerem. Serwer odpowiada klientowi poprzez RTP, przesyłając informację opisującą materiał wideo jako sesję strumieniowania. Sesja strumieniowania może składać się z jednego lub więcej strumieni, np. strumienia audio i strumienia wideo. Serwer przekazuje klientowi informację, jak dużo strumieni powinien on oczekiwać oraz podaje dokładne dane dotyczące m.in. typu przesyłanych danych i zastosowanego kodeka.
Transmisja jeden-do-wielu składa się z pojedynczego pakietu danych, który adresowany jest do grupy odbiorców, przy czym ruter docelowy może wysyłać pakiety nie tylko do użytkowników końcowych, ale także do innych ruterów.
Transmisje rozgłoszeniowe składają się z pojedynczego pakietu danych, kopiowanego i przesyłanego do wszystkich węzłów sieciowych. Pakiet jest adresowany przez węzeł źródłowy specjalnym adresem rozsyłającym, a następnie przesyłany do sieci, która tworzy kopie pakietu i wysyła je do każdego węzła sieci

Co to jest tunel wirtualny jakie są przesłanki do tworzenia tunelu.
Jest to kanał komunikacyjny chroniony przed niepowołanym dostępem przez zastosowanie kryptografii. Umożliwia chronioną transmisję w obszarze publicznej sieci rozległej. Drugą przesłanką jest tworzenie sieci wirtualnych, które umożliwiają przesyłanie danych między sieciami znajdującymi się na różnych serwerach.

Co to jest trójstronne potwierdzenie i jak działa?
- Host inicjujący połączenie wysyła pakiet zawierający segment TCP z ustawioną flagą SYN (synchronize).
- Host odbierający połączenie, jeśli zechce je obsłużyć, odsyła pakiet z ustawionymi flagami SYN i ACK (acknowledge – potwierdzenie).
- Inicjujący host powinien teraz wysłać pierwszą porcję danych, ustawiając już tylko flagę ACK (i gasząc SYN).
- Jeśli host odbierający połączenie nie chce lub nie może odebrać połączenia, powinien odpowiedzieć pakietem z ustawioną flagą RST (reset).

Na czym polega szyfrowanie asymetryczne
Polega na użyciu dwóch kluczy: publicznego (do zaszyfrowywania transmisji oraz weryfikacji podpisu) oraz prywatnego (do rozszyfrowywania danych i tworzenie podpisu elektrycznego), konieczne jest zastosowanie dłuższych ciągów bitów, wymaga większej mocy obliczeniowej, znacznie wygodniejsza w użyciu.

Na czym polega szyfrowanie symetryczne

Polega na szyfrowaniu za pomocą jednego, współdzielonego klucza, jest szybkie, ten sam klucz służy do zaszyfrowywania i rozszyfrowywania danych, podstawowym problemem jest dostarczenie do obu hostów klucza

Scharakteryzuj idealną transmisję danych

+ Brak strat – pakiet dociera do miejsca przeznaczenia
+ Niskie opóźnienia – możliwie szybko dociera do miejsca przeznaczenia
+ Niewielki narzut protokołu – nagłówki dodawane przez protokół są zaniedbywalnie małe w stosunku do danych (payload)
+ Stabilność transmisji – dane są odbierane z tą samą prędkością z jaką są nadawane – brak jitteru

Zalety stosowania VPN

+ zapewnienie poufności poprzez szyfrowanie danych silnymi algorytmami kryptograficznymi,
+ zapewnienie integralności poprzez uniemożliwienie modyfikacji danych w trakcie transmisji,
+ uwierzytelnianie stron poprzez zapewnienie, ze nikt nie podszył się pod żądną ze stron,
+ zapewnienie niezaprzeczalności, które oznacza, że strony nie mogą zaprzeczyć, że nie wysłały danej informacji, o ile informacja ta była podpisana kluczem prywatnym i podpis został poprawnie zweryfikowany.

Rodzaje sieci VPN

- **sieci typu site-to-site:** łączą ze sobą w sposób bezpieczny 2 lub więcej sieci, tunele są zakończone na dedykowanych urządzeniach
- **sieci typu remote-access**: łączą w bezpieczny sposób pojedyncze komputery z sieciami, wymagają instalacji specjalnego oprogramowania
- **oparte na protokole SSL:** nie wymagają instalacji specjalnego oprogramowania, mają mniejszą funkcjonalność
- **oparte na innych protokołach**

Co to certyfikat cyfrowy?

Najbardziej zaufany mechanizm uwierzytelnia, rozumiany jako dane podpisywane cyfrowo przez zaufaną trzecią stronę. Uwierzytelniają strony biorące udział w połączeniu, zapewniają poufność danych, zapewniają integralność danych oraz ich niezaprzeczalność.

Główne funkcjonalności protokołu SIP w mechanizmie transmisji danych

SIP (Session Initiation Protocol) - Protokół komunikacyjny wykorzystywany do sygnalizacji i kontrolowania podczas sesji wymiany danych multimedialnych
· Negocjacja kodeków
· Wykorzystywany w VoIP, serwisach streamingowych
· Format wiadomości jak w HTTP
· Dostępne szyfrowanie payloadu

Wymień i opisz czynniki wpływające na jakość transmisji cyfrowej

- **kompresja** – obecnie największy wpływ na jakość sygnału mulitmedialnego
- **opóźnienie transmisji** – na opóźnienie wpływają: kodeki, prędkość transmisji, odległość od nadajnika a odbiornika
- **jitter** – zjawisko polegające na błędach w czasie odebrania transmitowanych danych, powszechnie w sieciach IP
- **utrata pakietów** – w sieciach IP nie wszystkie pakiety docierają do adresata, powodem może być przeciążenie łącza, zbyt duża liczba kolizji, w przypadku transmisji multimedialnej skutkuje to przerwami w sygnale audio video

Jakie są różnice pomiędzy algorytmami link state i distance vector

Link state (Shortet path first):
- rozsyła info routingu do wszystkich węzłów obsługujących połączenia międzysieciowe.
- każdy router wysyła jednak tylko część tabeli routingu,
- skomplikowany, trudny do skonfigurowania,
- wymaga obecności silniejszego procesora CPU,
- odnotowuje szybciej wszelkie zmiany

Distance Vector (Bellmana-Forda):
- rozsyła całą tabelę routingu, ale tylko do sąsiadujących z nimi routerów,
- nie pracuje tak stabilnie,
- łatwiejszy do implementowania,
- sprawuje się dobrze w dużych sieciach

Opisz protokół trasowania IGRP – Interior Gateway Routing Protocol

Protokół trasowania bramy wewnętrznej. Algortym typu distance vector, metryka wykorzystywana przez routery do wyboru ścieżki, rozgłaszanie info o dostępności trasf (cykliczne lub po zmianie stanu sieci), protokół własnościowy, brak wparcia dla VLSM.

Opisz protokoły trasowania RIP (v1 i v2)

RIP v1 (Routing Information Protocol)
- protokół bram wewnętrznych, rodzina protokołów opartych o wektor odległości. Aktualizacja tras (rozgłaszana przez adres broadcastowy, wysyłana co 30s), max liczba przeskoków na trasie -15. Wady: nie wysyła info o masce podsieci, nie obsługuje VLSM i CIDR, nie obsługuje uwierzytelniania

RIP v2:
- obsługuje routing bezklasowy, przesyła info o masce podsieci i info uwierzytelniające, info przesyła na adres mulicastowy, przenosi info uzyskane za pomocą innych protokołów z sieci zewnętrznej

Czym różni się routing statyczny od dynamicznego i w oparciu o co działają.

Routing statyczny – mapa połączeń sieciowych jest programowana w routerze „ręcznie”przez administratora. W razie, gdy jakaś ścieka zostanie przerwana, administrator musi przeprogramować router, aby odpowiednie pakiety mogły dotrze do celu. W systemach sieciowych o kluczowym znaczeniu taki sposób trasowania jest niemożliwy do zaakceptowania. Stosuje się więc dynamiczne routery, które automatycznie diagnozują stan połączeń i wyznaczają połączenia alternatywne. Zalety: brak komunikacji w sieci związanej z dynamiczną konfiguracją routingu, wady: konieczność ręcznej ingerencji w przypadku awarii lub modyfikacji sieci

Routing dynamiczny – trasy ustalane w oparciu o protokoły routingu: otwarte i własnościowe. „System autonomiczny”– zbiór adresów sieci IP pod wspólną kontrolą administracyjną, w którym utrzymywany jest spójny schemat trasowania. Protokoły wewnętrzne (IGP), zewnętrzne (EGP).
Podział ze wzgedu na sposób wyznaczania trasy:
- distance vector,
- link state
- protokoły hybrydowe
- protokoły path-vector (opisują trasy przy użyciu atrybutów)

SYN, ACK, FIN – co oznaczają te pojęcia, w jakim protokole są wykorzystywane i jakie jest ich zastosowanie?

Są stosowane w protokole TCP, three-way handshake jako flagi
• SYN – synchronizuje kolejne numery sekwencyjne
• FIN – oznacza zakończenie przekazu danych
• ACK – informuje o istotności pola "Numer potwierdzenia

Rola ramki Beacon w WiFi

Ramka beacon jest ramką zarządzającą cyklicznie, rozgłaszaną przez punkt dostępowy w celu sygnalizowania jego obecności. Karty sieci bezprzewodowej 802.11 okresowo skanują wszystkie kanały radiowe i nasłuchują ramek beacon. Dzięki temu użytkownik wie, w zasięgu jakich sieci się znajduje, a wypadku sieci z roamingiem jest automatycznie przełączany między punktami dostępowymi. Z reguły punkt dostępowy ma opcję wyłączenia rozgłaszania identyfikatora SSID, jednak błędem jest identyfikowanie tej opcji z wyłączaniem rozgłaszania ramki beacon, gdyż identyfikator jest jednym z wielu jej składników.
11. Wymień i opisz tryby współpracy urządzeń w sieciach WiFi

Definicja IBSS – Independent Basic Service Set

Pracuje w trybie ad-hoc. Służy do tworzenia sieci bezprzewodowych, które nie są połączone z pkt dostępu.

Uwierzytelnienie Opensystem i SharedKey

Uwierzytelnianie OpenSystem i SharedKey są dwoma typami uwierzytelniania sieci bezprzewodowych.
OpenSystem jest najbardziej popularnym typem uwierzytelniania i pozwala wszystkim urządzeniom bezprzewodowym na dostęp do sieci bez wzajemnego uwierzytelniania. Jest to najprostszy typ uwierzytelniania, nie wymaga żadnych kluczy ani haseł.
SharedKey jest mniej popularnym typem uwierzytelniania i wymaga od obu stron wzajemnego uwierzytelniania za pomocą wspólnego klucza lub hasła. Jest to bardziej bezpieczny typ uwierzytelniania, ponieważ wymaga, aby obie strony wprowadziły swój klucz lub hasło. Jest to szczególnie ważne, gdy urządzenia końcowe są używane do przesyłania informacji poufnych.

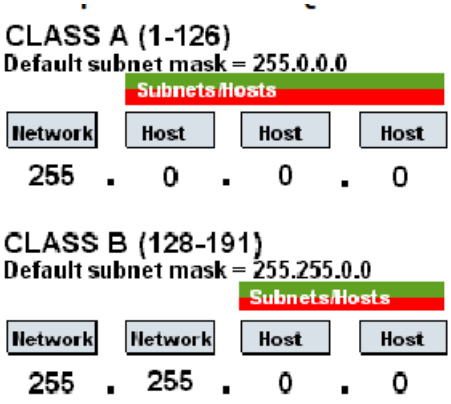
Standardy bluetooth – wymień (min. 4) i je opisz.

Bluetooth 4.0 + LE (Low Energy) – 200 kb/s, niższe zużycie energii, mniejszy transfer, większy zasięg (do100m)
iBluetooth 4.1 – standard opracowany do zastosowania w tzw. „internecie rzeczy”,

umożliwiający bezpośrednią łączność przedmiotów z internetem
Bluetooth 4.2 – w stosunku do poprzednich wersji: szybszy transfer, wyższy poziom bezpieczeństwa, nawiązanie łączności z przedmiotami – łatwiejsze
Bluetooth 5.0 – ujednolicenie wersji, szybszy transfer – 2 Mb/s dla urządzeń typu „wearables" i 50 Mb/s do normalnych, realny zasięg działania do 140 m.

Na czym polega i czemu służy architektura CIDR (Classless Inter-Domain Routing)
Bezklasowy routing międzydomenowy, długość maski dostosowana do potrzeb podsieci, działanie wielu podsieci w ramach jednej domeny trasowania. Agreguje trasy w tablicach routing (jedna trasa dla wielu sieci)

Budowa adresu IPv4 - opisz i podaj przykład
Jest to 32 bitowa liczba, podzielona na równe 4 bajty, oddzielone od siebie kropką. Najbardziej znaczący bit na początku – Big Endian . Przeznaczona na adresy sieci, hostów i adresy specjalne. Są 2 rodzaje pul adresowych: klasowa(5 klas adresowych ze stał ymi maskami) i bezklasowa (w opraciu o maskę wyznaczoną przez administratora sieci



Czym jest sieć TOR – The Onion Routing
Usługą działającą w sieci Internet zapewniającą wyższą anonimowość niż w przypadku zwykłej sieci. Zastosowanie TOR ukrywa adres IP klienta i serwera, a dodatkowo utrudnia namierzenie tych elementów przez analizę ruchu sieciowego.

Typy węzłów w sieci TOR - wymień i krótko opisz
- Guard relay (Entry node)- pkt wejścia do sieci, z którymi łączy się komputer kliencki
- Middle relay – pkt między którymi wymieniane są zaszyfrowane pakiety, węzły nie mają info o zawartości pakietów
- Exit node – odszyfrowują ruch kierują go do docelowego miejsca
Wymień i opisz główne tryby współpracy z Wi-Fi ???

Wymień i krótko scharakteryzuj klasy i kategorie skrętki.
- Klasa – parametry/przydatność transmisji
- Kategoria – przydatność do aplikacji

Klasy skrętki:
Klasa 1 – Skrętka klasy 1 jest przeznaczona do zastosowań w domach i małych firmach, gdzie wymagane jest długoterminowe zapewnienie wydajności i niezawodności. Jest najtańszą i najprostszą skrętką oferowaną, dlatego jest często stosowana w budynkach mieszkalnych.
Klasa 2 – Skrętka klasy 2 jest idealna do środowisk sieciowych, w których wymagana jest wyższa wydajność, a także przemysłowych, gdzie bardziej wymagające środowisko może stanowić wyzwanie dla niższej jakości skrętek.
Klasa 3 – Skrętka klasy 3 jest wysoce wytrzymała, dlatego jest często stosowana w środowiskach, w których wymagana jest wysoka wydajność. Jest odporna na zakłócenia i zapewnia wysoką jakość sygnału.

Kategorie skrętki:

Kategoria 5 – jest wysoce wytrzymała i jest odporna na zakłócenia. Jest to najczęściej stosowana skrętka, ponieważ może ona przesyłać dane z szybkością do 1 Gb/s.
Kategoria 6 – jest wyjątkowo odporna na zakłócenia. Jest odporna na wiele rodzajów zanieczyszczeń i może przesyłać dane z szybkością do 10 Gb/s.
Kategoria 6a –jest wysoce wytrzymała i odporna na zakłócenia. Jest w stanie przesyłać dane z szybkością do 10 Gb/s i może być używana w sieciach gigabitowych.

Podaj i scharakteryzuj systemów rozproszonych ze względu na sposób realizacji rozproszenia

Rozproszony system operacyjny - rozproszenie realizowane jest na poziomie jądra systemu operacyjnego, każda poprawnie napisana wielozadaniowa aplikacja może podlegać migracji (migruje w całości lub wybrane jej podprocesy), rozproszenie jest przeźroczyste dla aplikacji
maszyna wirtualna – uwspólniane są wybrane zasoby np. pamięć i moc obliczeniowa – implementacja odbywa zwykle przez użycie specjalistycznych bibliotek programistycznych
aplikacja rozproszona – poszczególne funkcje aplikacji dzielone są pomiędzy różne komputery np. tzw architektura trójwarstwowa (warstwa składowania danych – serwery baz danych plików – filery, warstwa logiki biznesowej, warstwa prezentacji danych)

Mechanizm MIMO (Mulitple Input Multiple Output)

Technika bezprzewodowej transmisji danych wykorzystująca wiele odbiorników i nadajników. Jest to zaawansowana technika dostępna w sprzęcie sieciowym, która wykorzystuje wiele ścieżek do przesyłania danych, co pozwala na zwiększenie wydajności i przepustowości. MIMO jest szeroko stosowane w sieciach bezprzewodowych, takich jak Wi-Fi, aby poprawić jakość transmisji. Technika ta może również być wykorzystywana do wzmocnienia sygnału w celu redukcji zakłóceń. MIMO wykorzystuje wiele nadajników i odbiorników w celu wielokrotnego przesyłania tych samych danych, co pozwala na zwiększenie szybkości transmisji.

3. różnica tunel vs VPN

Dwa rodzaje kabli światłowodowych

- jednomodowy: źródło światła to laser, większe pasmo przenoszenia, średnica włókna 9um
- wielomodowy: źródło światła to dioda LED, średnica 50um, promień światła może być wprowadzany pod różnym kątem, niższy koszt

Wymień i opisz rodzaje uwierzytelniania Wi-Fi

- WPA2-PSK: to popularny typ uwierzytelniania WIFI, który wymaga wprowadzenia długiego hasła.
- WPA-PSK: jest to starszy typ uwierzytelniania WIFI, który wymaga wprowadzenia długiego hasła.
- WPA-Enterprise: jest to bardziej zaawansowany typ uwierzytelniania WIFI, który wymaga użycia uwierzytelniania EAP (Extensible Authentication Protocol).
- WEP: jest to starszy typ uwierzytelniania WIFI, który działa na zasadzie klucza szyfrującego.
- WPS: jest to nowoczesny typ uwierzytelniania WIFI, który wymaga wprowadzenia krótkiego kodu Pin

Opisać strukturę sieci Bluetooth

Podstawową jednostką sieci Bluetooth jest pikosieć, która ma 1 węzeł master oraz do 7 węzłów typu slave i do 255 urządzeń w trybie uśpienia. Scatternet łączenie pikosieci, współdzielenie jednego kanału komunikacyjnego, możliwość komunikacji 8 urządzeń jednocześnie

CSMA/CD(Carrier Sense Multiple Access / with Collision Detection)
- Carrier Sense: nasłuchiwanie przed wysłaniem
- Multiple Access: wszystkie węzły mają dostęp do medium transmisyjnego
- Collision Detection: istnieje mechanizm wykrywania kolizji
Wszystkie komputery w sieci mają możliwość wykrywania że kabel jest w użyciu. Gdy jeden komputer chce wysłać dane, musi najpierw sprawdzić czy kabel jest wolny. Jeśli jest wolny, może wysłać dane, jeśli nie, musi poczekać. Jeśli dwa komputery wysyłają dane jednocześnie, może dojść do kolizji. Wszystkie komputery w sieci są zaprogramowane do wykrywania tych kolizji. W przypadku wykrycia kolizji, wszystkie komputery przerywają wysyłanie danych i wykonują procedurę Backoff, czyli losowe przesuwanie czasu oczekiwania przed ponownym wysłaniem danych. Maksymalnie 16 prób.

Co może zawierać tabela routingu
Tabela routingu może zawierać informacje o adresach IP, sieciach, maskach podsieci, interfejsach sieciowych, wirtualnych sieciach VPN, trasowaniu, algorytmach routingu, protokołach routingu, dostawcach usług routingu i innych informacjach

Co to jest maska i adres broadcast, podać zależności. Opisać różnice między adresem multicast, a broadcast.
Maska jest to 32 bitowa liczba która dzieli adres IP na numer hosta i numer sieci. Adres broadcast jest klasy adresu IP, który używany jest do wysyłania pakietu do wielu hostów w sieci. Pakiety multicast są wysyłane do grupy hostów, które zostały zdefiniowane przez użytkowników.

3.Opisać rodzaje połączeń włókien światłowodowych (nie mylić z rodzajami światłowodów).???
Dwa rodzaje światłowodów wymień i opisz

rodzaje skrętki
• UTP (U/UTP) – skrętka nieekranowana (unshielded twisted pair) 4 pary skręconych, zaizolowanych przewodów we wspólnej izolacji
• FTP (F/UTP) – skrętka foliowana (foiled twisted pair) - dodatkowo ekranowana foliowym płaszczem z przewodem uziemiającym
• STP (S/UTP) – skrętka ekranowana (shielded twisted pair) ekran wykonany w postaci oplotu i zewnętrznej koszulki ochronnej
• SFTP (S/FTP) – skrętka foliowana ekranowana (shielded foiled twisted pair) każda para przewodów otoczona osobnym ekranem z folii, cały kabel pokryty oplotem

Protokół ARP i RARP
Uzyskiwanie w sposób dynamiczny adresów IP

RARP(Reverse Address Resolution Protocol) – protokół wstecznego rozwiązywania adresów, może zapytać o adresy IP innych hostów, brak pamięci nieulotnej, brak możliwości zapisania adresu IP hosta

ARP (Address Resolution Protocol) odwzorowuje znany adres IP na adres sprzętowy MAC, adres IP w sieci lokalnej -> adres MAC hosta

Spoza siecie lokalnej -> adres MAC routera

Wykorzystuje tablicę ARP, zapytanie ARP rozsyłane na adres broadcast,

Wady: działa tylko dla IPv4, brak możliwości przesyłania maski sieci, identyfikacja hosta jednynie po adresie MAC

Model ISO-OSI (International Oragnization of Standarization – Open System Interconnection)

Model przedstawia proces komunikacji w postaci 7 warstw,

- podział procesu na mniejsze procesy składowe
- utworzenie standardów składnikami sieci
- komunikacja sprzętu różnych producentów
- brak wpływu zmian w jednej warstwie na inne warstwy
- łatwiejsze zrozumienie procesu komunikacji po podziale na mniejsze składowe

- Warstwa fizyczna-kable, sygnały radiowe
- Warstwa dostępu do medium - nadzoruje przekazywanie danych, pakuje dane w ramki
- Warstwa sieciowa - odpowiada za wybranie odpowiedniej ścieżki międzykomputeram
- Warstwa transportowa - segreguje dane i składa je w strumień
- Warstwa sesji – otrzymane od różnych aplikacji dane synchronizuje
- Warstwa prezentacji - odpowiada za przesyłanie w dolne warstwy, danych kanonicznych wg. Modelu osiRM
- Warstwa aplikacji - zajmuje się specyfikacją interfejsu, który wykorzystują programy, do komunikacji w sieci.

Ramka PAUSE

Pozwalają na czasowe przerwanie transmisji. Schemat:

- stacja A nadaje
- zapełnienie bufora stacji B
- stacja B wysyła ramkę PAUSE do stacji A określając czas wstrzymania transmisji
- stacja A wstrzymuje transmisje na określony czas

Techniki złączeń światłowodów

Złącza mechaniczne: niski koszt, większa tłumienność połączeń

Spawanie światłowodów: łuk elektryczny, mała tłumienność połączeń, drogi sprzęt, wymaga wprawy

CSMA/CA - rozwiń skrót i opisz zasadę działania

Carrier Sense Multiple Access with Collision Avoidance, protokół dostępu do łącza. polegający na nasłuchiwaniu łącza w
celu badania jego stanu aktywności: wolne lub zajęte. Jeżeli komputer wykryje że w danym momencie inna maszyna wykorzystuje łącze, czeka na jego zwolnienie kontynuując nasłuch, w przeciwnym przypadku, czyli jeśli łącze jest wolne komputer rozpoczyna transmisję.

Zalety:
- wszystkie stacje o równych priorytetach
- prostota protokołu
- kolizje jako zdarzenie normalne
- zakłócenia rozpatrywane jako kolizje

Wady:
- niedetermistyczny czas dostępu do łącza
- wzrost liczby kolizji ze wzrostem obciążenia sieci
- wymagane dodatkowe potwierdzenia
- dodatkowe ramki
- mała efektywność wykorzystania łącza

Światłowód - omów zasadę działania i budowę

Kabel telekomunikacyjny umożliwiający przesyłanie sygnału optycznego. Nośnikiem info jest włókno światłowodowe. Głównym elementem światłowodu jest środowisko przewodzące - włókno optyczne. Składa się ono z dwóch warstw: warstwy dielektrycznej i warstwy światłowodowej. Warstwa dielektryczna chroni włókno optyczne przed wpływem zewnętrznych czynników, zabezpieczając je przed uszkodzeniem. Warstwa światłowodowa odbija światło i przewodzi sygnały. Światłowody działają w oparciu o zasadę refleksji. Sygnał jest wysyłany i odbijany przez warstwę światłowodową, tworząc w ten sposób efekt odbić. Sygnał jest wysyłany i odbijany w kierunku przeciwnym, dzięki czemu może być przesłany na duże odległości. Światłowody są w stanie przesłać dane z dużą prędkością i z wysoką jakością sygnału. Mogą one przesyłać dane na odległość do 100 km bez żadnych zakłóceń.

Wady:
- możliwość zaszumienia sygnału poprzez wibracje przewodu
- stosunkowo mało odporne na uszkodzenia
- bardziej skomplikowany proces łączenia
- stosunkowo wysoka cena

Zalety:
- duża przepustowość
- małe straty
- nie generują zakłóceń elektrycznych
- duża niezawodność

Co to są well-known-ports? Podać 4 przykłady.

Porty zarezerwowane dla konkretnych usług
Port 21 - protokół FTP (File Transfer Protocol).
- Port 25 - protokół SMTP (Simple Mail Transfer Protocol).
- Port 80 - protokół HTTP (HyperText Transfer Protocol).
- Port 443 - protokół HTTPS (HyperText Transfer Protocol over SSL).

Opisać, podać zastosowanie, wady i zalety: skrętki i kabla koncentrycznego.

Skrętka – jest to kabel, który jest stosowany do łączenia różnych urządzeń i elementów sieci komputerowej. Składa się z dwóch lub więcej par drutów, które są zwinięte wspólnie. Skrętka jest zazwyczaj zaprojektowana tak, aby zapewnić szybki i niezawodny transfer danych między urządzeniami.

Zastosowanie: Skrętka jest stosowana w wielu różnych sieciach, w tym w sieciach LAN, WAN

i SAN. Jest to szczególnie przydatne w miejscach, gdzie musi istnieć szybkie i niezawodne połączenie między urządzeniami, takimi jak serwery, routery, komputery, drukarki i inne elementy sieci.
Wady: Jedną z głównych wad skrętki jest to, że jest ona podatna na uszkodzenia mechaniczne. Ma tendencję do złamania lub przerwania, jeśli jest źle użytkowana lub jeśli jest uszkodzona. Ponadto skrętka nie jest tak odporna na zakłócenia jak inne typy kabli, takie jak kabel koncentryczny.
Zalety: Skrętka jest bardzo łatwa w instalacji i można ją zamontować w ciągu kilku minut. Ponadto jest to stosunkowo tani typ kabla, dlatego jest bardzo popularny w sieciach komputerowych. Jest również bardzo elastyczny i można go łatwo dostosować do różnych zastosowań.
Kabel koncentryczny – jest to rodzaj kabla, który składa się z zewnętrznej izolacji, warstwy, która otacza wewnętrzną żyłę. Jest to rodzaj kabla, który jest szeroko stosowany w sieciach komputerowych, aby zapewnić szybki i niezawodny transfer danych między urządzeniami.
Zastosowanie: Kabel koncentryczny jest szczególnie przydatny w aplikacjach, które wymagają wyższego poziomu przepustowości i odporności na zakłócenia. Jest to popularny wybór w sieciach telewizji kablowej, sieciach szerokopasmowych, sieciach alarmowych i innych aplikacjach wymagających wyższego poziomu przepustowości.
Wady: Kabel koncentryczny jest zazwyczaj droższy niż skrętka, a jego instalacja może być bardziej skomplikowana. Ponadto może być trudny w przeciąganiu w trudno dostępnych miejscach.
Zalety: Kabel koncentryczny jest bardzo odporny na zakłócenia i oferuje wyższy poziom przepustowości niż skrętka. Ponadto jest on bardziej trwały i odporny na uszkodzenia mechaniczne niż skrętka. Jest to szczególnie ważne w aplikacjach, w których musi istnieć szybkie i niezawodne połączenie.

Co to jest VLAN i dlaczego się go stosuje?

VLAN (Virtual Local Area Networ) jest to wirtualna sieć lokalna, pozwala w ramach jednej sieci fizycznej tworzyć wiele sieci logicznych, zwanych sieciami wirtualnymi, technologia ta działa w 2. warstwie modelu OSI
– Dodatkowy znacznik w ramce Ethernet identyfikujący wirtualny LAN
– Tworzenie dodatkowych logicznych grup, poprzez: Przydzielanie ramek, ułatwienie zarządzania siecią, zwiększenie bezpieczeństwa sieciowego, ograniczenie domen broadcastowych

Co to jest TTL – Time To Live – w nagłówku IP jest liczbą określającą maksymalny czas życia pakietu w sieci. Przy każdym przeskoku pakietu oczekującego na potwierdzenie, liczba TTL zmniejsza się o jeden. Gdy osiągnie zero, pakiet jest odrzucany i wysyłane jest potwierdzenie o odrzuceniu.

Protokół TCP (Transmission Control Protocol)

Protokół kontroli transmisji jest to połączeniowy i niezawodny protokół komunikacyjny warstwy OSI. Większy rozmiar nagłówka(obciążenie sieci). Protokół TCP jest odpowiedzialny za utrzymanie połączenia między dwoma hostami i zapewnia mechanizmy potwierdzania, porządkowania i retransmisji danych, jeśli zostaną one utracone w trakcie transmisji.
Najważniejsze cechy protokołu:
• działa w trybie klient-serwer

• wykorzystuje procedury do nawiązania i zakończenia połączenia
• połączenie sterowane jest przy pomocy flag
• gwarantuje dostarczenie wszystkich pakietów z zachowaniem kolejności, bez duplikatów

Ramka TCP:

Ramka TCP składa się z nagłówka (5x32bity), który jest odpowiedzialny za przesyłanie informacji potrzebnych do przesyłania danych, takich jak nr identyfikacji, nr sekwencji i długość ramki. Nagłówek zawiera również informacje, które umożliwiają kontrolę przepływu danych, takie jak numer ostatniego zaakceptowanego bajtu, zmienna określająca przesunięcie w sekwencji i wskaźnik surowych danych.
Ramka TCP działa jako pośrednik między dwiema komputerami, które wysyłają i odbierają dane. Jeśli dane są przesyłane z jednego komputera do drugiego, ramka TCP zapewnia, że dane zostaną wysłane w odpowiedniej kolejności i są dostarczane bez błędów. Ramka TCP zapewnia również nadmiarowe informacje w celu weryfikacji poprawności danych i umożliwia wycofanie danych, jeśli są one niekompletne lub błędne.

Struktura DNS – Domain Name System – ogólnoświatowa sieć serwerów

- drzewiasta struktura
- (13) serwery root – rozwiązujących podstawowe domeny np.: .pl, .org, każdy z serwerów posiada kilkadziesiąt kopii na całym świecie
- Serwery główne z ang. Top-level domain
- domeny krajowe oraz funkcyjne: Local Domain oraz serwery niższego rzędu: Secondary-level domain servers; przechowują dane wybranych domen

Odpowiedzi i zapytania DNS

Zapytania:

Rekurencyjne: odpytywany serwer musi odnaleźć info o domenie lub zwrócić wiadomość o błędzie, odpytywany serwer nie znając zapytanie odpytuje inne serwery DNS, umożliwia zapamiętywanie odwzorowania w pamięci serwera, realizowane przez sieci lokalne
Iteracyjne: odpytywany serwer odpowiada najlepszą znaną mu odpowiedzią, nie łączy się z innymi serwerami

Odpowiedzi :

Autorytatywne: dotyczą domen w strefie na którą dany serwer ma zarząd, pochodzą bezpośrednio z bazy danych serwera, zawierają ustalony bit uwierzytelniania
Nieautorytatywne: dane pochodzą spoza strefy zarządzanej przez dany serwer, są na serwerze buforowane przez określony czas po czym usuwane

Opisać na czym polegają ataki typu Man in the middle w DNS.

Fałszywe odpowiedzi DNS dla komputera ofiary, połączenie komputera ze sfałszowanym serwerem docelowym

Typy rekordów DNS:

- SOA – rekord adresu startowego uwierzytelniania
- A – rekord adresu
- AAAA – rekord adresu IPv6
- CNAME – rekord nazwy kanonicznej
- NS – rekord serwera nazw
- TXT – rekord tekstowy

Co to i jak działa Reverse DNS
System serwerów pełniących funkcję odwrotną do DNS. Mapowanie adresów IP na nazwy domenowe

Rodzaje serwerów DNS
- **DNS Master Server** - Przechowują dane źródłowe dla konkretnego poddrzewa danego poziomu
- **DNS Slave Server** - Synchronizacja danych z serwerem Master
- **DNS Cache Server** - Nie przechowuje informacji o systemie DNS jako Master lub Slave, obsługuje segment sieci którego jest członkiem
- **DNS Forward Server** – przeznaczony do komunikacji z serwerem spoza DMZ

DHCP krótko scharakteryzowaać i opisać algorytm (Dynamic Host Configuration Protocol)
Protokół zarządzania siecią w stosie TCP/IP, model bezpołączeniowy, protokół UDP. Służy do automatycznego przydzielania adresów IP i innych parametrów sieciowych do komputerów i innych urządzeń w sieć. Tryby przydzielania adresów IP: alokacja ręczna, alokacja dynamiczna, dzierżawa.
W przypadku DHCP adres IP jest przydzielany na czas określony, zazwyczaj kilka godzin lub dni, po czym zwracany jest serwerowi. Gdy adres IP jest zwracany, może być ponownie wykorzystany przez inne urządzenie. Gdy adres IP jest wykorzystywany przez dane urządzenie, serwer DHCP wysyła informacje sieciowe do urządzenia, w tym adres IP, maskę podsieci, adres bramy domyślnej i adres serwera DNS. Wszystkie te informacje są niezbędne do skonfigurowania połączenia sieciowego.

Różnice między koncentratorem a przełącznikiem
Koncentrator to urządzenie sieciowe, które służy do połączenia wielu urządzeń sieciowych w jednej sieci. Koncentrator wykorzystuje porty do łączenia urządzeń sieciowych i jest zazwyczaj umieszczany w centrum sieci, aby upraszczać połączenia. Urządzenie pasywne.
Przełącznik sieciowy jest urządzeniem sieciowym, wielopoziomowy most, które umożliwia wymianę informacji między komputerami w ramach sieci. Przełącznik sieciowy wykorzystuje porty, takie jak koncentrator, ale przełącznik służy do przesyłania informacji między komputerami, a nie tylko do łączenia ich w jedną sieć. Przełącznik sieciowy jest zazwyczaj umieszczany na końcu sieci, aby zapewnić szybkie i skuteczne przesyłanie informacji .
Przekazuje ramki pomiędzy segmentami sieci

Co to jest metryka? Jakie informacje może zawierać i na co mieć wpływ.
Metryka routingu, zwana też metryką trasowania jest wartością pozwalającą określić, która z tras routingu jest lepsza, wykorzystywana jest przez algorytmy trasowania. Miarą opisująca „koszt" przesłania pakietu daną trasą. Innymi słowy jest to abstrakcyjna ilościowa wartość wskazująca odległość do danej sieci, która może składać się z następujących wartości: Wartość liczbowa – zgodnie z zasadą „im mniej tym lepiej", Szerokość pasma, Opóźnienie, Obciążenie Niezawodność

Co to jest vlsm? Rozwiń skrót i opisz tę technologię, gdzie jest stosowana.

Variable Lenght Subnet Mask podsieć o zmiennej długości maski, która powstała jako rozwiązanie problemu niewystarczającej puli adresów IPv4, VLSM zakłada podział klasy adresowej wewnątrz organizacji na mniejsze podsieci, routery muszą przesyłać pełną informacje o sieciach, łącznie z maskami. Podsieć wspierana przez Protokół **EIGRP** (Enhanced Interior Gateway Routing Protocol) hybrydowy protokół trasowania operujący na algorytme wektora odległości.

Opisz protokół FTP i TFTP. Wskaż główne różnice pomiędzy nimi.

FTP – File Transfer Protocol – protokół transferu plików, protokół typu klient – serwer, wykorzystuje 2 połączenia TCP, może działać w 2 trybach: aktywny i pasywny, tryby dostępu: anonimowy, autoryzowany
TFTP – Trivial File Transfer Protocol – mniej funkcjonalności w porównaniu do FTP, implementowany na protokole UDP, gwarancja niezawodności transmisji

cecha	FTP	TFTP
Autentyfikacja	W oparciu o login i hasło	Brak autentyfikacji
Połączenie	Oparte na TCP. Retransmisja w oparciu o mechanizmy zapewnione w TCP	Oparte na UDP. Błędy (utracone pakiety, sumy kontrolne) oparte o mechanizmy TFTP.
Algorytm protokołu	W oparciu o mechanizmy zapewniana w TCP. (kontrola przepływu (okno przesuwne, bufory) i przeciążeń)	Oparty na potwierdzeniach przesyłanych pakietów (pojedynczych, ograniczona przepustowość).
Złożoność	Nieco bardziej skomplikowany od TFTP. Czasami niezalecany do bootloaderów przechowywanych w pamięci EEPROM.	Bardzo prosty, z bardzo małym narzutem (oparty o równie prosty UDP). Może być wykorzystywany w bootloaderach.
Kanały transmisji danych	Dwa oddzielne kanały transmisji. Jeden do kontroli drugi do przesyłania danych w oparciu o dwa oddzielne połączenia TCP	Dane i informacje kontrolne przesyłane w oparciu o jedno połączenie TCP.

Co to jest domena .arpa i gdzie jest wykorzystywana.

Domena TLD przeznaczona do obsługi infrastruktury sieciowej Internetu. W ramach domeny zdefiniowano mapowanie numerów telefonicznych na URI oraz IPv4 oraz IPv6 na nazwy. Wykorzystywaną przy reverse DNS w infrastrukturze sieciowej internetu.

Jakie są protokoły routowalne i routujące? Opisz i podaj parę przykładów każdego

Protokoły routowalne zawierają informacje identyfikujące nadawcę i adresata, przykładami są: IP, Apple Talk, IPX
Protokoły routujące obsługują proces przesyłu pakietu między urządzeniami sieciowymi, wybór odpowiedniej trasy dla pakietu, komunikacja między routerami oraz wymiana informacji o trasach

Wymień podział sieci ze względu na obsługiwany przez nie obszar oraz opisz każdy typ

- **WAN (Wide Area Network)–** połączenia na stosunkowo dużym obszarze, wykorzystanie usług operatorów telekomunikacyjnych, różnego typu transmisji szeregowej, sieć PIONER
- **MAN (Metropolitan Area Network)** - łączenie wielu sieci w aglomeracji miejskiej, oparta na sieci szkieletowej
- **Sieci kampusowe** – połączenie sieci wewnętrznych łaczami charakterystycznymi dla sieci lokalnych, względy prktyczne i ekonomiczne

- LAN (Local Area Network) – instalacje na niewielkim obszarze, krótkie łącza o wysokiej przepustowości, rozwiązanie oparte na technice radiowej lub przewodowej
- **PAN (Personal Area Network)** – stosowana w domach lub niewielkich biurach, niewielki zasięg, różnorodne media

Opisz protokół ICMP – Internet Control Message Protocol – jest to internetowy protokół komunikatów kontrolnych służący do przesyłania informacji o błędzie lub problemie połączenia. Wysyłanie komunikatów ICMP najczęściej odbywa się przez bramy lub hosty, zapewniając lepszą trasę dla pakietów, komunikat o lepszej trasie wysyłany przez router do źródła, gdy host docelowy jest nieosiągalny, brama wysyła komunikat o niedostępności adresata.

Wymień i krótko opisz 2 typy wiadomości wysyłane przy użyciu protokołu ICMP
- **Echo request:** typ 0 lub 8, kod zawsze 0, identyfikator i nr seryjny (unikalne wartości w celu połączenia żądania i odpowiedzi)
- Destination unreachable: uszkodzenie łącza, błędny adres docelowy, nieznana lokalizacja, wysyłane przez router

WDM – Wavelenght Division Multiplexing – zwielokrotnianie w dziedzinie długości fali realizowane za pomocą światła laserowego, transmisja sygnału cyfrowego w formie analogowej, podział światła laserowego na wiele fal o różnych długościach, fale przesyłane w tym samym czasie każda długość fali tworzy osobny kanał, który może przenosić informację, przesyłanie kilku sygnałów światłowodowych przez jeden światłowód. Multipleksja z podziałem długości fali, przesyłany sygnał pochodzi z oddzielnych źródeł, każdemu jest przypisana jego własna długość fali.

Socket (pol. Gniazdo) abstrakcyjna reprezentacja 2-kierunkowego zakończenia połączenia. Charakteryzowane przez typ/protokół(TCP lub UDP), adres lokalny (najczęściej IP), nr portu identyfikujący proces

Tablica routingu- tablica na podstawie której routery kierują pakiety do docelowej stacji

Podaj 4 aktywne urządzenia z 2 lub 3 warstwy iso-osi: Routery, Switche, Brama VoI, Kontroler bezprzewodowy

Domena kolizyjna i sposoby jej separacji – jest to fragment sieci połączony za pomocą urządzeń biernych, most, przełącznik (most wieloportowy), tablica skojarzeniowa(Max/port)

Wymienić i opisać techniki łączenia światłowodów:
- łącza mechaniczne: niski koszt utrzymania, większa tłumienność połączeń,
- spawanie światłowodów: łuk elektryczny, mała tłumienność połączeń, drogi sprzęt, wymaga wprawy

Co wpłynęło na wzrost przepustowości sieci 802.3?
- nowe standardy kabli
- wprowadzenie i stosowanie szybszych standardów transmisji danych
- nowe technologie takie jak: PoE czy GbE

Podział sieci ze względu na typ nadawania

- **kolizyjne** - Węzeł przed nadawaniem sprawdza czy linia jest wolna i rozpoczyna wysyłanie pakietu. Może dojść do kolizji. Wady: spadek wydajności sieci wraz ze wzrostem obciążenia, Zalety: rozwiązanie tanie i powszechne;
- **krążącego żetonu** – posiada zezwolenie na wysyłanie danych gdy otrzyma od poprzedzającego go węzła żeton (token). Następnie przekazuje go dalej.
- **z wykorzystaniem slotów czasowych** - Każde urządzenie ma przydzielony czas, w którym może nadawać

Jakie funkcje pełni TCP w warstwie transportowej

- gwarancja przesyłania danych
- kierowanie właściwych info do odpowiednich aplikacji
- opiera się na wykorzystaniu portów określonych dla każdego połączenia

Co to jest adres MAC i jak jest zbudowany – Media Access Control

Sprzętowy adres karty sieciowej, 48 bitowa liczba , pierwsze 24 bity oznaczają kod producenta a kolejne 24 nr seryjny

Cele kodowania w sieciach komputerowych

- Zabezpieczenie danych przed nieautoryzowanym dostępem.
- Umożliwienie bezpiecznej transmisji danych przez sieć.
- Ochrona poufnych informacji.
- Umożliwienie szyfrowania komunikatów między urządzeniami w sieci.
- Zapewnienie integralności danych przesyłanych przez sieć.
- Zapobieganie podsłuchiwaniu i modyfikowaniu przesyłanych informacji

Modulacja, co to jest + 3 klasyczne sposoby

Modulacja jest to zmiana 1 lub więcej parametrów sygnału w celu umożliwienia wydajniejszego wykorzystania sygnału, umożliwienia wielokrotnego wykorzystania kanału częstotliwości, uodpornienia sygnału na wpływ szumów czy zmniejszenia wzgl szerokości pasma

1) Modulacja FHSS
2) Modulacja DSSS
3) Modulacja OFDM

MPLS, Wymień i opisz tryby współpracy urządzeń w sieciach WiFi

Multi Protocol Label Switching – technika transmisji pakietów w sieciach rozległych, protokół zarządzania siecią, działa na styku warstwy drugiej i trzeciej, zastępuje proces routowania przez przełączanie etykiet.

Tryby współpracy???