# Pytania z kolosów

**Kolos 1.**

1. Do czego wykorzystywany jest protokół ICMP?

Protokół ICMP służy do przesyłania komunikatów diagnostycznych między komputerami w sieci IP. ICMP jest często wykorzystywany do przekazywania komunikatów o błędach i problemach z połączeniami lub dostępem do zasobów sieciowych. ICMP może być również wykorzystywany do wykrywania komputerów w sieci, tworzenia map sieci i monitorowania połączeń sieciowych.

2. Rodzaje transmisji wideo pod względem liczby użytkowników.

- Pojedynczy użytkownik: transmisja wideo jedno-do-jednego (1:1) pozwala użytkownikowi oglądać strumieniowo na żywo jeden tylko obraz.
- Wielu użytkowników: transmisja wideo wielu-do-jednego (many-to-one) pozwala wielu użytkownikom oglądać strumieniowo na żywo jeden obraz.
- Wielu użytkowników: transmisja wideo jeden-do-wielu (one-to-many) pozwala jednemu użytkownikowi wysyłać strumieniowo na żywo jeden obraz do wielu użytkowników.

3. Maska, adres rozgłoszeniowy i ich powiązanie.

Maskę adresu IP wykorzystuje się do określenia, które segmenty adresu są przeznaczone do identyfikacji komputera lub sieci. Adres rozgłoszeniowy jest adresem IP, który wskazuje na wszystkie komputery w sieci. Maskę można wykorzystać do wyodrębnienia adresu rozgłoszeniowego z adresu IP i ustalenia, które segmenty adresu są przeznaczone do identyfikacji sieci i komputerów.

4. Funkcjonalność RTCP.

RTCP (Real-Time Control Protocol) to protokół oparty na protokole TCP/IP, który pozwala na monitorowanie w czasie rzeczywistym połączeń sieciowych. Umożliwia także kontrolę jakości strumienia danych, jak również statystyki dotyczące połączeń.

RTCP działa w parach z protokołem RTP (Real-Time Protocol). RTP wysyła dane strumieniowe, natomiast RTCP odpowiada za ich kontrolę. RTCP stanowi ważną część sieci komunikacyjnych, w których wykorzystywane są strumienie danych w czasie rzeczywistym. Dzięki RTCP

5. Na czym polega szyfrowanie asymetryczne.

Szyfrowanie asymetryczne to rodzaj szyfrowania, który wykorzystuje podwójny klucz. Klucz publiczny i prywatny są używane do zaszyfrowania i odszyfrowania danych. Klucz publiczny jest widoczny dla wszystkich, natomiast klucz prywatny jest zachowany w tajemnicy przez właściciela. Dzięki temu, że są używane różne klucze, pozwala to na bezpieczny transfer informacji, ponieważ osoba, która posiada klucz publiczny nie może odszyfrować danych.

6. Główne funkcjonalności protokołu RTCP w mechanizmie transmisji danych.

Protokół RTCP (Real-Time Control Protocol) służy do monitorowania i kontrolowania transmisji danych w sieciach RTSP (Real-Time Streaming Protocol). Główne funkcjonalności protokołu RTCP obejmują:

- Monitorowanie transmisji: RTCP wykorzystuje komunikaty, aby monitorować i kontrolować przepływ danych w sieci.
- Ocena jakości transmisji: komunikaty RTCP są wykorzystywane do oceny jakości usług, które są świadczone w sieci.

- Ustalanie współczynników strumieniowania: protokół RTCP umożliwia ustalenie współczynników strumieniowania, które określają, jak dane są przesyłane w sieci.
- Reagowanie na zmiany w sieci: protokół RTCP umożliwia sieci RTSP reagowanie na zmiany w sieci, takie jak zmiany przepustowości, opóźnień i innych czynników wpływających na jakość transmisji.
- Przesyłanie informacji: protokół RTCP umożliwia przesyłanie informacji o aktualnych i planowanych transmisjach w sieci RTSP.

7. Co to jest tunel wirtualny? Jakie są przesłanki do tworzenia tunelu?

Tunel wirtualny to bezpieczny połączenie pomiędzy dwiema sieciami. Przesłanka do tworzenia tunelu to konieczność bezpiecznego przekazywania danych pomiędzy sieciami. Drugą przesłanką jest potrzeba tworzenia sieci wirtualnych, które umożliwiają przesyłanie danych między sieciami znajdującymi się na różnych serwerach.

8. Rodzaje sieci VPN.

- Sieć VPN IPSec: IPSec jest jednym z najbardziej popularnych rodzajów sieci VPN. Jest zabezpieczony za pomocą protokołu szyfrowania, co zapewnia wysoką bezpieczeństwo.
- Sieć VPN PPTP: PPTP jest najstarszym, najbardziej powszechnym i najtańszym rodzajem sieci VPN. Jest łatwy w konfiguracji i używania, ale ma mniejszą wydajność i mniejszą wydajność szyfrowania niż inne rodzaje sieci VPN.
- Sieć VPN L2TP/IPSec: L2TP/IPSec jest kombinacją protokołu L2TP i IPSec. Jest bardziej wydajny niż PPTP i ma lepszą wydajność szyfrowania niż IPSec.
- Sieć VPN SSL: SSL jest jednym z najnowocześniejszych rodzajów sieci VPN. Jest zabezpieczony za pomocą protokołu szyfrowania SSL, który jest bardzo bezpieczny.
- Sieć VPN OpenVPN: OpenVPN jest rodzajem sieci VPN, która jest łatwa w konfiguracji i prawie wszędzie dostępna. Jest bardzo wydajny i ma wysoki poziom bezpieczeństwa.

9. Scharakteryzuj idealną transmisję danych.

Idealna transmisja danych to proces przesyłania danych między dwoma urządzeniami przy użyciu określonego protokołu sieciowego. Idealna transmisja danych powinna charakteryzować się szybkością, niezawodnością i bezpieczeństwem. Powinna też zapewniać wysoką jakość transmisji, minimalizując ilość błędów i utratę danych. Idealna transmisja danych powinna również zapewniać jak największą wydajność, dzięki czemu możliwe będzie szybsze przesyłanie danych.

10. Co to jest trójstronne potwierdzanie i jak działa?

Trójstronne potwierdzanie to proces weryfikacji, który wymaga udziału trzech stron: pośrednika, strony wysyłającej i strony odbierającej. Proces ten polega na potwierdzeniu, że transakcja została zakończona przez wszystkie strony. Proces ten może się składać z wielu kroków, w których każda ze stron musi potwierdzić swoje uczestnictwo w transakcji. Na przykład, pośrednik może potwierdzić, że strona wysyłająca dokonała zapłaty, następnie strona odbierająca potwierdzi, że otrzymała pieniądze, a w końcu pośrednik potwierdzi, że transakcja została zakończona pomyślnie. Trójstronne potwierdzanie jest często używane do zabezpieczenia transakcji finansowych, aby zapobiec nadużyciom.

11. Na czym polega szyfrowanie symetryczne?

Szyfrowanie symetryczne polega na wykorzystaniu tego samego klucza do zaszyfrowania i odszyfrowania informacji. Klucz jest wspólny dla nadawcy i odbiorcy i używany jest do zamiany informacji na niezrozumiały ciąg znaków. Klucz musi być odpowiednio zabezpieczony, aby uniemożliwić osobom trzecim odczytanie zaszyfrowanych danych.

12. Co to jest TTL w nagłówku IP?

TTL (ang. 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. Jeśli liczba TTL osiągnie zero, pakiet jest odrzucany i wysyłane jest potwierdzenie o odrzuceniu.

13. Zalety stosowania VPN.

- Bezpieczeństwo: szyfrowanie danych i anonimowość użytkownika chronią twoje informacje przed włamaniami lub przechwytywaniem.
- Prywatność: zapobiega śledzeniu użytkowników przez władze, firmy reklamowe lub hakerów.
- Dostęp do zablokowanych stron: umożliwia dostęp do stron internetowych, które są zablokowane w twojej lokalizacji.
- Ochrona połączeń Wi-Fi: chroni twoje połączenia Wi-Fi przed włamaniami.
- Oszczędność czasu i pieniędzy: VPN może umożliwić oszczędność.

14. Czym jest certyfikat cyfrowy?

Certyfikat cyfrowy to elektroniczny dokument, który służy do uwierzytelnienia tożsamości, autentyczności i integralności danych. Certyfikat cyfrowy składa się z klucza publicznego, podpisu cyfrowego i informacji o właścicielu. Certyfikaty cyfrowe są wykorzystywane do uwierzytelniania, szyfrowania i podpisywania danych w wirtualnym środowisku, a także do weryfikacji tożsamości w Internecie.

15. Główne funkcjonalności protokołu SIP w mechanizmie transmisji danych.

Główne funkcjonalności protokołu SIP w mechanizmie transmisji danych to:

- Inicjowanie połączenia - Protokół SIP używa poleceń INVITE, ACK i BYE do inicjowania połączenia.
- Utrzymywanie stanu połączenia - Protokół SIP używa poleceń OPTIONS i UPDATE do utrzymywania stanu połączenia.
- Negocjacja parametrów - Protokół SIP umożliwia negocjację parametrów, takich jak przepływność, szybkość transmisji danych, kodek audio i wideo, które są używane do połączenia.
- Przekazywanie informacji - Protokół SIP używa poleceń REFER i INFO do przesyłania informacji między użytkownikami.
- Uwierzytelnianie i autoryzacja - Protokół SIP używa poleceń REGISTER, INVITE i ACK do uwierzytelniania i autoryzacji połączenia.
- Zwijanie połączenia - Protokół SIP używa poleceń BYE i CANCEL do zwijania połączenia.

16. Wymień i opisz czynniki wpływające na jakość transmisji cyfrowej.

- Przepustowość: Przepustowość jest miarą maksymalnej ilości danych wysyłanych i odbieranych w jednostce czasu. Im wyższa przepustowość, tym wyższa jakość transmisji.
- Interferencja: Interferencja to zakłócenia w sygnale, które mogą być spowodowane przez inne urządzenia wytwarzające fale radiowe w otoczeniu. Im większa jest interferencja, tym niższa jakość transmisji.
- Szybkość łącza: Szybkość łącza mierzy szybkość, z jaką dane są przesyłane. Im szybsze łącze, tym wyższa jakość transmisji.
- Przeplot: Przeplot to stosunek sygnału do szumu w sygnale cyfrowym. Im wyższy jest przeplot, tym wyższa jakość transmisji.
- Kodowanie: Kodowanie to proces kompresji danych, który pozwala na przesyłanie informacji w krótszym czasie. Im lepsze kodowanie, tym wyższa jakość transmisji.

**Kolos 2.**

1. Omówić mechanizm MIMO.

MIMO (Multiple Input Multiple Output) to 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.

2. Jak zmieniają się stany hostów w mechanizmie Three way handshake?

Three way handshake to mechanizm używany do ustanowienia połączenia między dwoma hostami. To protokół sieciowy, który umożliwia obustronną wymianę danych między dwoma hostami. Stany hostów zmieniają się w następujący sposób:

- Pierwszy stan: Host A wysyła do hosta B pakiet SYN (synchronizacja).
- Drugi stan: Host B odbiera pakiet SYN i wysyła do hosta A pakiet SYN-ACK (synchronizacja + potwierdzenie).
- Trzeci stan: Host A odbiera pakiet SYN-ACK i wysyła do hosta B pakiet ACK (potwierdzenie).

Po trzecim kroku połączenie jest ustanowione i hosty A i B mogą wymieniać dane.

3. Wymień i krótko opisz 2 typy wiadomości wysłane przy użyciu protokołu ICMP.

- Echo Request – wiadomość przesyłana do komputera docelowego, aby potwierdzić czy komputer jest dostępny w sieci. Komputer docelowy odpowiada wysyłając Echo Reply.
- Destination Unreachable – wiadomość wysyłana w celu poinformowania komputera żądającego, że żądany cel nie jest dostępny. Wiadomość ta może być wysłana, gdy cel jest niedostępny lub gdy nie ma dostępnego połączenia fizycznego do celu.

4. Jakie są różnice pomiędzy algorytmami link state i distance vector.

Algorytmy link state i distance vector to dwa rodzaje algorytmów routingu, które służą do wyznaczania optymalnych ścieżek w sieciach komputerowych. Różnice między nimi:

- Algorytm link state wykorzystuje protokół link state routing (LSR), który wykorzystuje algorytm Dijkstry do wyznaczania optymalnych ścieżek. Natomiast algorytm distance vector używa algorytmu Bellmana-Forda do wyznaczania optymalnych ścieżek.
- Algorytm link state wymaga, aby węzły w sieci posiadały pełny zaktualizowany obraz sieci, w tym informacje o sąsiadach, ich szybkości połączeń, koszcie połączeń i innych parametrach. Natomiast w algorytmie distance vector wystarczy, aby węzły w sieci posiadały informacje o odległości do wszystkich węzłów w sieci.
- Algorytm link state wymaga, aby wszystkie węzły w sieci wymieniały informacje o sieci między sobą. Natomiast algorytm distance vector wymaga, aby każdy węzeł wymieniał jedynie informacje o odległościach do wszystkich węzłów w sieci z jego bezpośrednimi sąsiadami.
- Algorytm link state jest bardziej wydajny niż algorytm distance vector, ponieważ wymaga mniej ruchu w sieci.

5. Opisz protokoły trasowania RIP (v1 i v2).

Protokół trasowania RIP (Routing Information Protocol) jest jednym z najstarszych i najczęściej stosowanych protokołów trasowania opierających się na algorytmie znajdowania najkrótszej ścieżki (ang. Distance Vector Routing Protocol).

RIP v1:

- jest protokołem trasowania opartym na algorytmie znajdowania najkrótszej ścieżki;
- obsługuje do 15 sąsiednich sieci;
- używa długości trasy jako miary odległości;
- nie obsługuje autoryzacji;
- używa protokołu UDP;
- używa portu 320.

RIP v2:

- jest protokołem trasowania opartym na algorytmie znajdowania najkrótszej ścieżki;
- obsługuje do 15 sąsiednich sieci;
- używa długości trasy jako miary odległości;
- obsługuje autoryzację;
- używa protokołu UDP;
- używa portu 520.

6. Opisz protokół trasowania IGRP.

Interior Gateway Routing Protocol (IGRP) jest protokołem trasowania stosowanym w sieciach komputerowych, który umożliwia routerom wymianę informacji o trasowaniu. Jest on znacznie bardziej zaawansowany niż protokół trasowania RIP, który jest często stosowany w małych sieciach.

IGRP wykorzystuje algorytm trasowania zwany algorytmem wielokryterialnym, który jest znacznie bardziej zaawansowany niż algorytm trasowania stosowany w RIP. Algorytm ten określa nie tylko najkrótszą ścieżkę do węzła docelowego, ale również wybiera najbardziej odpowiednią ścieżkę, biorąc pod uwagę wiele innych czynników, takich jak szybkość sieci, niezawodność i poziom zatłoczenia.

IGRP jest dość prosty w konfiguracji i zarządzaniu. Wymaga jedynie, aby wszystkie routery w sieci były skonfigurowane z tymi samymi parametrami, takimi jak czas życia do indeksu, czas wygaśnięcia, czas odświeżania itp.

IGRP ma również zdolność do rozpoznawania problemów w sieci i odpowiedniego reagowania na nie. Jeśli router wykryje problem, będzie on informował pozostałe routery w sieci i wszystkie routery będą aktualizować swoje tabele trasowania, aby ominąć problem.

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

Routing statyczny jest zazwyczaj zdefiniowany przez system administracyjny, a jego informacje są stałe i nie zmieniają się automatycznie. Routing dynamiczny jest zautomatyzowany i jego informacje są aktualizowane w czasie rzeczywistym przez protokoły routingu dynamicznego, takie jak OSPF, EIGRP i RIP.

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

**SYN**: skrót od angielskiego słowa "synchronize" (zsynchronizuj), jest to flaga sieciowa protokołu TCP, która jest wykorzystywana przez klienta, aby poprosić serwer o nawiązanie połączenia.

**ACK**: skrót od angielskiego słowa "acknowledge" (potwierdź), jest to flaga sieciowa protokołu TCP, która jest wykorzystywana przez serwer, aby potwierdzić otrzymanie danych.

**FIN**: skrót od angielskiego słowa "finish" (zakończ), jest to flaga sieciowa protokołu TCP, która jest wykorzystywana przez klienta, aby wyświadczyć serwerowi prośbę o zakończenie połączenia.

Pojęcia te są wykorzystywane w protokole TCP i służą do nawiązywania, utrzymywania i zamykania połączenia sieciowego.

9. Wymień najważniejsze cechy protokołu TCP.

- połączenie orientowane (zachodzące połączenie musi zostać potwierdzone przez obiema strony),
- dzielenie danych na segmenty, - kontrola błędów za pomocą sumy kontrolnej, - nagłówki w każdym segmencie,
- potwierdzenia danych,
- porządkowanie danych,
- kontrola przepływu.

10. Rola bramki Beacon w WiFi.

Bramka Beacon jest podstawowym elementem konfiguracji sieci WiFi. Jest odpowiedzialna za wysyłanie sygnałów beacona, które informują innym urządzeniom o dostępnej sieci. Sygnały te są wysyłane regularnie i umożliwiają innym urządzeniom łatwe wykrywanie i połączenie się z siecią Wi-Fi. Bramka Beacon jest niezbędnym elementem wszystkich sieci WiFi.

11. Wymień i opisz tryby współpracy urządzeń w sieciach WiFi.

**Ad-hoc** – w tym trybie urządzenia łączą się bezpośrednio ze sobą. Jest to typ sieci bezpośredniej, w której każde urządzenie jest równorzędnym uczestnikiem sieci i może wysyłać i odbierać dane.

**Infrastructure** – sieci tego typu składają się z routera lub punktu dostępowego, który jest centrum sieci i wszystkie pozostałe urządzenia są połączone z tym routerem. Router lub punkt dostępowy przekazuje dane między innymi urządzeniami.

**Wi-Fi Direct** – jest to technologia umożliwiająca bezpośrednią komunikację między urządzeniami bez konieczności korzystania z routera lub punktu dostępowego. Urządzenia mogą wymieniać dane bezpośrednio ze sobą.

12. Definicja IBSS.

IBSS (Independent Basic Service Set) - jest to rodzaj sieci, w której komputery pracują w trybie ad-hoc, czyli bez zewnętrznego punktu dostępu. Komputery w tej sieci są połączone za pomocą bezprzewodowej sieci komputerowej. IBSS służy do tworzenia sieci bezprzewodowych, które nie są połączone z punktem dostępu.

13. Uwierzytelnianie 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.

**Kolos 3.**

1. Opisz architekturę sieci bluetooth.

Architektura sieci Bluetooth składa się z trzech warstw:

- Warstwa fizyczna - obejmuje interfejs radiowy, który jest używany do bezprzewodowego przesyłania danych między urządzeniami przy użyciu fal radiowych o częstotliwości 2,4 GHz.
- Warstwa dostępu do medium (MAC) - zapewnia szyfrowanie i kontrolę przepustowości, umożliwiając bezpieczne przesyłanie danych między urządzeniami.
- Warstwa usług - zapewnia standardowe protokoły i usługi, umożliwiając urządzeniom wymianę danych i współpracę.
- Każde urządzenie w sieci Bluetooth ma swój własny adres fizyczny, który jest używany do identyfikacji.

2. Co to jest pikosieć i jak działa?

Pikosieć to rodzaj sieci komputerowej, która wykorzystuje technologię Wi-Fi do tworzenia krótkich zasięgów sieci. Technologia ta zapewnia znacznie szybszą prędkość transmisji danych niż tradycyjne sieci Wi-Fi, a także mniejsze opóźnienia. Używa ona szerokopasmowych częstotliwości radiowych do przesyłania danych, dzięki czemu może uzyskać wyższą szybkość transmisji. Pikosieć działa poprzez podzielenie sieci na mniejsze segmenty, a następnie podłączenie ich do pojedynczego punktu.

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

- Bluetooth v2.0 + EDR – wersja 2.0 dostarcza szybszy transfer danych (do 3 Mbps) dzięki Enhanced Data Rate, który pozwala na skrócenie czasu potrzebnego do przesyłania dużych plików.
- Bluetooth v3.0 + HS – ta wersja dostarcza transfer danych na poziomie 24 Mbps dzięki technologii High Speed.
- Bluetooth 4.0 – ta wersja dostarcza szybką transmisję danych za pomocą technologii Bluetooth Low Energy, która zmniejsza zużycie energii przez urządzenia.
- Bluetooth 5.0 – ta wersja dostarcza szybszy transfer danych (do 2 Mbps) i ma zasięg do 4 razy większy niż poprzednie wersje.

4. Na czym poelga i czemu służy architektura CIDR?

CIDR (Classless Inter-Domain Routing) jest architekturą sieciową, która służy do optymalizacji routingu w Internecie. Umożliwia przydzielanie adresów IP w sposób elastyczny oraz zmniejszenie liczby wpisów tablic routingu. Pozwala również na tworzenie dużych sieci, podzielonych na mniejsze podsieci. Umożliwia to operatorom sieciowym zmniejszenie zużycia zasobów sieciowych, zwiększenie wydajności sieci i zmniejszenie kosztów związanych z zarządzaniem siecią.

5. Budowa adresu IPv4 – opisz i podaj przykład.

Adres IPv4 składa się z 4 liczb oddzielonych kropkami (czyli 32 bity). Każda z liczb może mieć wartość od 0 do 255. Przykładowy adres IPv4 to: 192.168.0.1. Każda liczba odpowiada określonemu segmentowi sieci. Pierwsza liczba określa klasę sieci, która determinuje zasięg sieci (np. 192.168 oznacza klasę C, co oznacza sieć lokalną). Pozostałe trzy liczby określają adres hosta, czyli konkretny komputer w sieci.

6. Czym jest sieć TOR?

Sieć TOR (The Onion Router) jest siecią anonimizującą, która wykorzystuje wielopoziomowe szyfrowanie do ochrony danych użytkowników i umożliwia im bezpieczny i anonimowy dostęp do sieci. Pozwala zachować anonimowość użytkowników, chronić dane przed wyciekiem i umożliwia prywatny dostęp do stron i usług, które w innym przypadku byłyby niedostępne.

7. Typy węzłów w sieci TOR – wymień i krótko opisz.

- Wyjście – węzeł, który jest połączony z Internetem i pozwala na połączenie z innymi sieciami.
- Wejście – węzeł, który jest połączony z Internetem i pozwala na połączenie do sieci TOR.
- Dzielnik – węzeł, który jest połączony z Internetem i kieruje ruch w sieci TOR.
- Złośliwy – węzeł, który jest połączony z Internetem i ma za zadanie zapisywanie informacji o ruchu w sieci TOR.
- Śledczy – węzeł, który jest połączony z Internetem i ma za zadanie monitorowanie ruchu w sieci TOR.

**Pytania**

**Grupa A**

1. Ramka Beacon

Bramka Beacon jest podstawowym elementem konfiguracji sieci WiFi. Jest odpowiedzialna za wysyłanie sygnałów beacona, które informują innym urządzeniom o dostępnej sieci. Sygnały te są wysyłane regularnie i umożliwiają innym urządzeniom łatwe wykrywanie i połączenie się z siecią Wi-Fi. Bramka Beacon jest niezbędnym elementem wszystkich sieci WiFi.

2. CSMA/CD

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) jest techniką kontroli dostępu do medium transmisyjnego w sieciach komputerowych. CSMA/CD jest stosowane w sieciach Ethernet, w których komputery komunikują się korzystając z kabla, lub innego medium transmisyjnego.

Idea działania CSMA/CD jest prosta. Wszystkie komputery w sieci mają możliwość wykrywania że kabel jest w użyciu (tzw. Carrier Sense). 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 (Collision). Wszystkie komputery w sieci są zaprogramowane do wykrywania tych kolizji (Collision Detection). W przypadku wykrycia kolizji, wszystkie komputery przerywają wysyłanie danych i wykonują procedurę Backoff, czyli losowe przesuwanie czasu oczekiwania przed ponownym wysłaniem danych.

3. Co może zawierać tabela w routingu

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

4. Reverse DNS.

Reverse DNS to inna nazwa dla odwrotnego konwertowania numeru IP na nazwę hosta. Jest to proces w którym numer IP jest konwertowany na nazwę domeny. Proces ten jest używany do identyfikacji witryn internetowych i systemów informatycznych.

**Grupa B**

1. Co to jest maska i adres broadcast, podać zależności. Opisać różnice między adresem multicast, a broadcast.

Maska sieci jest 32 bitową liczbą reprezentującą rozkład adresów IP w sieci. Używa się jej do określenia, które bity określają numer sieci, a które bity określają numer hosta. Adres broadcast jest specjalnym adresem IP, który jest używany do wysyłania pakietów do wszystkich hostów w sieci.

Adres multicast jest klasy adresu IP, który jest używany do wysyłania pakietów do wielu hostów w sieci. Pakiety multicast są wysyłane do grup hostów, które zostały zdefiniowane przez użytkowników.

Adres broadcast jest używany do wysyłania pakietów do wszystkich hostów w sieci. Różnica polega na tym, że pakiety multicast są wysyłane tylko do określonej grupy hostów, podczas gdy pakiety broadcast są wysyłane do wszystkich hostów.

2. Scharakteryzować protokół ICMP, do czego służy?

Protokół ICMP służy do przesyłania komunikatów diagnostycznych między komputerami w sieci IP. ICMP jest często wykorzystywany do przekazywania komunikatów o błędach i problemach z połączeniami lub dostępem do zasobów sieciowych. ICMP może być również wykorzystywany do wykrywania komputerów w sieci, tworzenia map sieci i monitorowania połączeń sieciowych.

3. Opisać rodzaje połączeń włókien światłowodowych.

Połączenia włókien światłowodowych można podzielić na trzy rodzaje: połączenia przewodowe, połączenia bezprzewodowe i połączenia radiowe.

- Połączenia przewodowe: polegają na przesyłaniu sygnału światłowodowego za pomocą kabli światłowodowych, które są podłączone bezpośrednio do urządzeń.
- Połączenia bezprzewodowe: tego rodzaju połączenia wykorzystują technologie radiowe, takie jak Wi-Fi, Bluetooth czy LTE, do przesyłania sygnałów światłowodowych między dwoma urządzeniami.
- Połączenia radiowe: w tym przypadku sygnał światłowodowy jest przesyłany za pomocą fal radiowych, które są przesyłane za pośrednictwem anten lub innych urządzeń nadawczych i odbiorczych.

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

Ataki typu Man in the Middle (MitM) w DNS polegają na tym, że złośliwy podmiot śledzi i modyfikuje komunikację pomiędzy klientem i serwerem DNS. Atakujący może wykorzystać tę technikę, aby wyciągnąć informacje lub podszyć się pod stronę internetową. Atakujący może również przekierować ruch do nieautoryzowanych stron internetowych, które mogą zawierać malware lub inne szkodliwe oprogramowanie. Ataki te mogą być szczególnie niebezpieczne w przypadku korzystania z bezpiecznych połączeń HTTPS, ponieważ złośliwy podmiot może uzyskać dostęp do danych użytkownika, które zostały zaszyfrowane.

**Grupa A**

1. Wymień i opisz główne tryby współpracy z WIFi.

**Ad-hoc** – w tym trybie urządzenia łączą się bezpośrednio ze sobą. Jest to typ sieci bezpośredniej, w której każde urządzenie jest równorzędnym uczestnikiem sieci i może wysyłać i odbierać dane.

**Infrastructure** – sieci tego typu składają się z routera lub punktu dostępowego, który jest centrum sieci i wszystkie pozostałe urządzenia są połączone z tym routerem. Router lub punkt dostępowy przekazuje dane między innymi urządzeniami.

**Wi-Fi Direct** – jest to technologia umożliwiająca bezpośrednią komunikację między urządzeniami bez konieczności korzystania z routera lub punktu dostępowego. Urządzenia mogą wymieniać dane bezpośrednio ze sobą.

2. Mechanizm Three-way-shake – opisz.

Three way handshake to mechanizm używany do ustanowienia połączenia między dwoma hostami. To protokół sieciowy, który umożliwia obustronną wymianę danych między dwoma hostami. Stany hostów zmieniają się w następujący sposób:

- Pierwszy stan: Host A wysyła do hosta B pakiet SYN (synchronizacja).
- Drugi stan: Host B odbiera pakiet SYN i wysyła do hosta A pakiet SYN-ACK (synchronizacja + potwierdzenie).
- Trzeci stan: Host A odbiera pakiet SYN-ACK i wysyła do hosta B pakiet ACK (potwierdzenie).

3. Wymień i krótko scharakteryzuj klasy i kategorie skrętki.

**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 – Skrętka kategorii 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 – Skrętka kategorii 6 jest wyjątkowo odporna na zakłócenia. Jest odporna na wiele rodzajów zanieczyszczeń i może przesyłać dane z szybkością do 10 Gb/s.

Kategoria 6a – Skrętka kategorii 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.

4. Model OSI-ISO – wymień i krótko opisz warstwy.

Model OSI-ISO (ang. Open Systems Interconnection - International Organization for Standardization) to model połączenia systemów otwartych, zaproponowany w 1977 roku przez organizację ISO. Model składa się z siedmiu warstw:

- **Warstwa fizyczna** (ang. Physical Layer) – odpowiada za dostarczanie fizycznych środków transportu danych pomiędzy komputerami.
- **Warstwa dostępu do medium** (ang. Data Link Layer) – odpowiada za dostarczanie środków technicznych do przesyłania danych, które zostały zapisane w warstwie fizycznej.
- **Warstwa sieciowa** (ang. Network Layer) – odpowiada za organizację danych w różnych sieciach, np. routowanie, łączenie sieci i adresowanie.
- **Warstwa transportowa** (ang. Transport Layer) – odpowiada za dostarczanie środków transportu danych między komputerami.
- **Warstwa sesji** (ang. Session Layer) – odpowiada za kontrolę sesji między komputerami, takich jak synchronizacja, kontrola błędów i komunikacja.
- **Warstwa prezentacji** (ang. Presentation Layer) – odpowiada za dostarczanie środków prezentacji danych, takich jak kompresja, szyfrowanie i konwersja danych.
- **Warstwa aplikacji** (ang. Application Layer) – odpowiada za dostarczanie środków aplikacji danych, takich jak protokoły sieciowe, przeglądarki internetowe i e-mail.

**Grupa B**

1. Ramka Beacon.

Bramka Beacon jest podstawowym elementem konfiguracji sieci WiFi. Jest odpowiedzialna za wysyłanie sygnałów beacona, które informują innym urządzeniom o dostępnej sieci. Sygnały te są wysyłane regularnie i umożliwiają innym urządzeniom łatwe wykrywanie i połączenie się z siecią Wi-Fi. Bramka Beacon jest niezbędnym elementem wszystkich sieci WiFi.

2. Co to jest maska i adres broadcast, podać zależności. Opisać różnice między adresem multicast, a broadcast.

Maska sieci jest 32 bitową liczbą reprezentującą rozkład adresów IP w sieci. Używa się jej do określenia, które bity określają numer sieci, a które bity określają numer hosta. Adres broadcast jest specjalnym adresem IP, który jest używany do wysyłania pakietów do wszystkich hostów w sieci.

Adres multicast jest klasy adresu IP, który jest używany do wysyłania pakietów do wielu hostów w sieci. Pakiety multicast są wysyłane do grup hostów, które zostały zdefiniowane przez użytkowników.

Adres broadcast jest używany do wysyłania pakietów do wszystkich hostów w sieci. Różnica polega na tym, że pakiety multicast są wysyłane tylko do określonej grupy hostów, podczas gdy pakiety broadcast są wysyłane do wszystkich hostów.

3. Podaj i scharakteryzuj systemy rozproszone ze względu na sposób realizacji rozproszenia.

Systemy rozproszone dzielą się na cztery kategorie ze względu na sposób realizacji rozproszenia:

Systemy o **strukturze centralnej**: są to systemy, w których jeden element jest głównym sterownikiem i odpowiada za wszystkie komunikacje między innymi elementami w systemie. Elementy te są zależne od centralnego elementu i nie mogą wykonywać żadnych zadań bez jego zgody. Przykładem takiego systemu jest system bankowy, w którym bank jest centrum danych, a wszystkie transakcje są przesyłane przez bank.

Systemy o **strukturze klient-serwer**: są to systemy, w których istnieją różne rodzaje komputerów, które wykonują zadania w ramach tego samego systemu. Klient wykonuje zadania, w których serwer odpowiada za wykonanie danego zadania. Przykładem takiego systemu jest system internetowy, w którym klient wysyła dane do serwera, a serwer odpowiada za ich przetworzenie.

Systemy **decentralizowane**: są to systemy, w których wszystkie elementy są niezależne od siebie i współdziałają ze sobą. Każdy element systemu ma własny zestaw danych i jest w stanie wykonywać zadania bez zgody innych elementów. Przykładem takiego systemu jest system kryptowalut, w którym wszystkie elementy są niezależne od siebie i współdziałają ze sobą.

Systemy **hybrydowe**: są to systemy, które łączą cechy systemów centralnego, klient-serwer i decentralizowanego. Cechą charakterystyczną systemu hybrydowego jest to, że posiada on elementy obu poprzednich systemów. Przykładem takiego systemu jest system chmury obliczeniowej, w którym serwery są centralnym elementem, a pozostałe elementy są zależne od serwera.

4. CSMA/CA – krótka charakterystyka i zasada działania.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – jest to protokół sieciowy stosowany w sieciach bezprzewodowych. Umożliwia on użytkownikom komunikowanie się bez wykorzystania kontrolowanych łączy. Zasada działania tego protokołu opiera się na następującym założeniu: wszystkie urządzenia w sieci mogą wysyłać i odbierać informacje, jednak przed wysłaniem

wiadomości muszą one sprawdzić, czy pasmo jest wolne. Jeśli wszystkie urządzenia w sieci będą postępować zgodnie z tym założeniem, zmniejszy się ryzyko wystąpienia kolizji i przeładowania sieci.

**Grupa A**

1. Rodzaje skrętki.

- Sieci lokalne (LAN): sieci lokalne są sieciami komputerowymi, które łączą komputery w ramach jednej lokalizacji. Mogą one obejmować małą sieć domową lub sieć w dużym biurze.
- Sieci rozległe (WAN): sieci rozległe są sieciami komputerowymi, które łączą komputery w różnych lokalizacjach. Mogą obejmować sieci telefonii komórkowej, sieci szerokopasmowe oraz sieci satelitarną.
- Sieci bezprzewodowe (WLAN): sieci bezprzewodowe są sieciami komputerowymi, które łączą komputery za pośrednictwem radiowego połączenia bezprzewodowego. WLAN są często wykorzystywane w miejscach publicznych, takich jak hotele, lotniska, kawiarnie i biblioteki.
- Sieci komórkowe (WWAN): sieci komórkowe są sieciami komputerowymi, które łączą komputery za pośrednictwem sieci komórkowych. WWAN obejmuje sieci GSM, CDMA i LTE.
- Sieci hybrydowe (HAN): sieci hybrydowe są sieciami komputerowymi, które łączą komputery za pośrednictwem zarówno bezprzewodowego, jak i przewodowego połączenia. HAN obejmuje sieci Ethernet, Wi-Fi i Bluetooth.

2. Ramka TCP.

Ramka TCP (Transmission Control Protocol) jest protokołem komunikacji, używanym w sieciach komputerowych do zapewnienia prawidłowego wewnętrznego przesyłania danych. Jest to protokół pochodzący z warstwy transportowej modelu OSI i jest często używany przez protokoły warstwy aplikacji, takie jak HTTP, SMTP i FTP.

Ramka TCP składa się z nagłówka, który jest odpowiedzialny za przesyłanie informacji potrzebnych do przesyłania danych, takich jak numer identyfikacji, numer 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. Nagłówek zawiera również informacje o potencjalnych opcjach, których używają aplikacje, takie jak SMTP i FTP.

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.

3. Rodzaje uwierzytelniania WIFI.

Istnieje wiele rodzajów uwierzytelniania WIFI:

- WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key): to popularny typ uwierzytelniania WIFI, który wymaga wprowadzenia długiego hasła.

- WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key): 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 (Wired Equivalent Privacy): jest to starszy typ uwierzytelniania WIFI, który działa na zasadzie klucza szyfrującego.
- WPS (Wi-Fi Protected Setup): jest to nowoczesny typ uwierzytelniania WIFI, który wymaga wprowadzenia krótkiego kodu PIN.

4. Domena kolizyjna.

Domena kolizyjna to część sieci komputerowej, w której wszystkie urządzenia muszą komunikować się za pośrednictwem jednego łącza sieciowego. Domena kolizyjna działa w oparciu o protokół Ethernet, w którym wszystkie urządzenia wysyłają i odbierają dane jednocześnie, bez zastosowania żadnego układu kontroli dostępu. Z tego powodu, gdy kilka urządzeń wysyła jednocześnie informacje, występuje kolizja i dane są odrzucane. Aby temu zaradzić, systemy sieciowe stosują algorytmy, które obliczają, które urządzenie powinno być pierwsze w kolejce, aby uniknąć kolizji danych.

**Grupa B**

1. Co to jest adres MAC i jak jest zbudowany?

Adres MAC (ang. Media Access Control) to unikalny identyfikator sprzętowy, służący do identyfikacji komputerów w sieci komputerowej. Jest zbudowany z 48-bitowego ciągu znaków. Każdy znak składa się z dwóch zmiennoprzecinkowych cyfr szesnastkowych, oznaczonych od 0 do 9 i od A do F. Przykładowy adres MAC to 0A-3F-3B-1F-E3-6F.

2. Mechanizm MIMO.

MIMO (Multiple Input Multiple Output) to 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.

Tunel VPN (Virtual Private Network) jest rodzajem sieci, która tworzy bezpieczne połączenie między użytkownikiem a zdalnym serwerem za pośrednictwem szyfrowanych protokołów. Zabezpiecza ona dane przed nieautoryzowanym dostępem i umożliwia użytkownikowi zdalne połączenie z siecią prywatną.

Tunel natomiast jest połączeniem między dwoma sieciami, które umożliwia przekazywanie danych wykorzystując protokoły szyfrowania. Tunelowanie pozwala na przesyłanie danych pomiędzy dwoma sieciami, bez konieczności wykorzystywania publicznego adresu IP. Jest to bardzo przydatne, gdy dane mają być wysyłane przez Internet, ale nie chcemy, aby były one widoczne dla innych użytkowników.

4. Dwa rodzaje kabli światłowodowych.

Single-Mode i Multi-Mode. Single-Mode używa pojedynczego włókna i ma mały promień zakrzywienia, co umożliwia szybkie przesyłanie danych przez duże odległości. Multi-Mode używa wielu

włókien i ma większy promień zakrzywienia, co pozwala na szybsze przesyłanie danych na krótszych dystansach.

**Grupa A**

1. Mechanizm Three-Way-Handshake – opisz zasadę działania oraz zmiany stanów

Three way handshake to mechanizm używany do ustanowienia połączenia między dwoma hostami. To protokół sieciowy, który umożliwia obustronną wymianę danych między dwoma hostami. Stany hostów zmieniają się w następujący sposób:

- Pierwszy stan: Host A wysyła do hosta B pakiet SYN (synchronizacja).
- Drugi stan: Host B odbiera pakiet SYN i wysyła do hosta A pakiet SYN-ACK (synchronizacja + potwierdzenie).
- Trzeci stan: Host A odbiera pakiet SYN-ACK i wysyła do hosta B pakiet ACK (potwierdzenie).

2. Wymień i porównaj dwa rodzaje kabla światłowodowego.

Single-Mode i Multi-Mode. Single-Mode używa pojedynczego włókna i ma mały promień zakrzywienia, co umożliwia szybkie przesyłanie danych przez duże odległości. Multi-Mode używa wielu włókien i ma większy promień zakrzywienia, co pozwala na szybsze przesyłanie danych na krótszych dystansach.

3. Wymień i krótko scharakteryzuj warstwy modelu IOS-OSI

Model OSI-ISO (ang. Open Systems Interconnection - International Organization for Standardization) to model połączenia systemów otwartych, zaproponowany w 1977 roku przez organizację ISO. Model składa się z siedmiu warstw:

- **Warstwa fizyczna** (ang. Physical Layer) – odpowiada za dostarczanie fizycznych środków transportu danych pomiędzy komputerami.
- **Warstwa dostępu do medium** (ang. Data Link Layer) – odpowiada za dostarczanie środków technicznych do przesyłania danych, które zostały zapisane w warstwie fizycznej.
- **Warstwa sieciowa** (ang. Network Layer) – odpowiada za organizację danych w różnych sieciach, np. routowanie, łączenie sieci i adresowanie.
- **Warstwa transportowa** (ang. Transport Layer) – odpowiada za dostarczanie środków transportu danych między komputerami.
- **Warstwa sesji** (ang. Session Layer) – odpowiada za kontrolę sesji między komputerami, takich jak synchronizacja, kontrola błędów i komunikacja.
- **Warstwa prezentacji** (ang. Presentation Layer) – odpowiada za dostarczanie środków prezentacji danych, takich jak kompresja, szyfrowanie i konwersja danych.
- **Warstwa aplikacji** (ang. Application Layer) – odpowiada za dostarczanie środków aplikacji danych, takich jak protokoły sieciowe, przeglądarki internetowe i e-mail.

4. Wymień i opisz rodzaje uwierzytelniania Wi-Fi

Istnieje wiele rodzajów uwierzytelniania WIFI:

- WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key): to popularny typ uwierzytelniania WIFI, który wymaga wprowadzenia długiego hasła.

- WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key): 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 (Wired Equivalent Privacy): jest to starszy typ uwierzytelniania WIFI, który działa na zasadzie klucza szyfrującego.
- WPS (Wi-Fi Protected Setup): jest to nowoczesny typ uwierzytelniania WIFI, który wymaga wprowadzenia krótkiego kodu PIN.

**Grupa B**

1. Opisać strukturę sieci bluetooth

Bluetooth to bezprzewodowa technologia komunikacyjna, która pozwala na komunikację między urządzeniami za pomocą krótkiej odległości. Struktura sieci Bluetooth składa się z dwóch części: mastera i uczestników. Master jest urządzeniem, które zarządza siecią. Może to być telefon, laptop, tablet lub inne urządzenie. Uczestnicy są podłączone do mastera, a komunikacja między nimi następuje przez połączenie Bluetooth. Każde urządzenie w sieci ma swój własny adres, który pozwala innym urządzeniom na identyfikację. Połączenie jest zabezpieczone przy użyciu różnych protokołów i algorytmów szyfrowania. Sieć Bluetooth może być stosowana do wymiany danych między urządzeniami, takimi jak pliki, zdjęcia, muzyka i wiele innych.

2. Three-way-handshake

Three way handshake to mechanizm używany do ustanowienia połączenia między dwoma hostami. To protokół sieciowy, który umożliwia obustronną wymianę danych między dwoma hostami. Stany hostów zmieniają się w następujący sposób:

- Pierwszy stan: Host A wysyła do hosta B pakiet SYN (synchronizacja).
- Drugi stan: Host B odbiera pakiet SYN i wysyła do hosta A pakiet SYN-ACK (synchronizacja + potwierdzenie).
- Trzeci stan: Host A odbiera pakiet SYN-ACK i wysyła do hosta B pakiet ACK (potwierdzenie).

3. Co to VLAN, sposób działania, dlaczego jest stosowany?

VLAN (Virtual Local Area Network) to wirtualna sieć lokalna, która służy do logicznego grupowania stacji roboczych w określonych przestrzeniach sieciowych. Wirtualna sieć lokalna może być używana do określania dostępu do zasobów sieciowych, zabezpieczeń i kontroli ruchu sieciowego. Struktura VLAN pozwala administratorom sieci wydzielić określone strefy sieciowe, zapewniając tym samym zwiększoną elastyczność w zarządzaniu siecią.

VLAN działa poprzez tworzenie wirtualnych komputerów na istniejącej sieci LAN. Każdy wirtualny komputer może być używany do przechowywania i przesyłania danych, tak jak zwykły komputer. VLAN jest stosowany, ponieważ pozwala administratorom tworzyć wirtualne sieci lokalne na istniejącej fizycznej sieci, co zapewnia lepszą kontrolę nad przepływem danych. Ponadto, zastosowanie VLAN umożliwia administratorom sieci tworzenie sieci, które są odizolowane od innych sieci, co pozwala na lepsze zarządzanie dostępem do zasobów sieciowych.

4. Czym są protokoły Routujące i routowalne. Podać przykłady.

Protokoły routujące to protokoły sieciowe, które pozwalają routerom na wykrywanie innych sieci i wybór najbardziej optymalnych ścieżek (tras) docelowych. Przykłady to protokoły głównie z rodziny TCP/IP, takie jak: RIP, OSPF, EIGRP, BGP, IS-IS.

Protokoły routowalne to protokoły, które umożliwiają wymianę informacji pomiędzy routerami, aby umożliwić im odpowiednie routowanie pakietów. Przykłady to protokoły z rodziny TCP/IP, takie jak: ICMP, ARP, RARP, DHCP, PPP.

**Grupa A**

1. CSMA/CA

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – jest to protokół sieciowy stosowany w sieciach bezprzewodowych. Umożliwia on użytkownikom komunikowanie się bez wykorzystania kontrolowanych łączy. Zasada działania tego protokołu opiera się na następującym założeniu: wszystkie urządzenia w sieci mogą wysyłać i odbierać informacje, jednak przed wysłaniem wiadomości muszą one sprawdzić, czy pasmo jest wolne. Jeśli wszystkie urządzenia w sieci będą postępować zgodnie z tym założeniem, zmniejszy się ryzyko wystąpienia kolizji i przeładowania sieci.

2. Model IOS-OSI

Model OSI-ISO (ang. Open Systems Interconnection - International Organization for Standardization) to model połączenia systemów otwartych, zaproponowany w 1977 roku przez organizację ISO. Model składa się z siedmiu warstw:

- **Warstwa fizyczna** (ang. Physical Layer) – odpowiada za dostarczanie fizycznych środków transportu danych pomiędzy komputerami.
- **Warstwa dostępu do medium** (ang. Data Link Layer) – odpowiada za dostarczanie środków technicznych do przesyłania danych, które zostały zapisane w warstwie fizycznej.
- **Warstwa sieciowa** (ang. Network Layer) – odpowiada za organizację danych w różnych sieciach, np. routowanie, łączenie sieci i adresowanie.
- **Warstwa transportowa** (ang. Transport Layer) – odpowiada za dostarczanie środków transportu danych między komputerami.
- **Warstwa sesji** (ang. Session Layer) – odpowiada za kontrolę sesji między komputerami, takich jak synchronizacja, kontrola błędów i komunikacja.
- **Warstwa prezentacji** (ang. Presentation Layer) – odpowiada za dostarczanie środków prezentacji danych, takich jak kompresja, szyfrowanie i konwersja danych.
- **Warstwa aplikacji** (ang. Application Layer) – odpowiada za dostarczanie środków aplikacji danych, takich jak protokoły sieciowe, przeglądarki internetowe i e-mail.

3. Dwa rodzaje światłowodów – wymień i opisz

Single-Mode i Multi-Mode. Single-Mode używa pojedynczego włókna i ma mały promień zakrzywienia, co umożliwia szybkie przesyłanie danych przez duże odległości. Multi-Mode używa wielu włókien i ma większy promień zakrzywienia, co pozwala na szybsze przesyłanie danych na krótszych dystansach.

4. Zapytania i odpowiedzi w DNS – wymień i opisz.

- Rekord A – służy do mapowania nazw domenowych na adresy IP. Przykładowo, komputer z adresem IP 192.168.0.1 może mieć nazwę hosta "www.example.com".
- Rekord NS – określa, który serwer DNS jest autorytatywny dla danej domeny.
- Rekord CNAME – służy do tworzenia aliasów dla danej domeny. Na przykład, możesz użyć CNAME, aby "www.example.com" było równoważne "example.com".
- Rekord MX – służy do wskazania serwera poczty, który będzie odbierał wiadomości dla danej domeny.
- Rekord PTR – mapuje adresy IP na nazwy domenowe. Jest to używane w protokole odwrotnego DNS, który służy do wyszukiwania nazw domenowych na podstawie adresów IP.

**Grupa B**

1. Rodzaje skrętki:

- Sieci lokalne (LAN): sieci lokalne są sieciami komputerowymi, które łączą komputery w ramach jednej lokalizacji. Mogą one obejmować małą sieć domową lub sieć w dużym biurze.
- Sieci rozległe (WAN): sieci rozległe są sieciami komputerowymi, które łączą komputery w różnych lokalizacjach. Mogą obejmować sieci telefonii komórkowej, sieci szerokopasmowe oraz sieci satelitarną.
- Sieci bezprzewodowe (WLAN): sieci bezprzewodowe są sieciami komputerowymi, które łączą komputery za pośrednictwem radiowego połączenia bezprzewodowego. WLAN są często wykorzystywane w miejscach publicznych, takich jak hotele, lotniska, kawiarnie i biblioteki.
- Sieci komórkowe (WWAN): sieci komórkowe są sieciami komputerowymi, które łączą komputery za pośrednictwem sieci komórkowych. WWAN obejmuje sieci GSM, CDMA i LTE.
- Sieci hybrydowe (HAN): sieci hybrydowe są sieciami komputerowymi, które łączą komputery za pośrednictwem zarówno bezprzewodowego, jak i przewodowego połączenia. HAN obejmuje sieci Ethernet, Wi-Fi i Bluetooth.

2. Ramka beacon

Bramka Beacon jest podstawowym elementem konfiguracji sieci WiFi. Jest odpowiedzialna za wysyłanie sygnałów beacona, które informują innym urządzeniom o dostępnej sieci. Sygnały te są wysyłane regularnie i umożliwiają innym urządzeniom łatwe wykrywanie i połączenie się z siecią Wi-Fi. Bramka Beacon jest niezbędnym elementem wszystkich sieci WiFi.

3. Protokół ARP i RARP

Protokół adresów MAC i IP w sieci Ethernet nazywa się protokołem ARP (ang. Address Resolution Protocol). Jest to protokół służący do automatycznego przypisywania adresów IP do adresów MAC w sieci Ethernet. W tym celu wykorzystuje się wysyłanie pakietów ARP, które służą do wymiany informacji o adresach IP i MAC.

Protokół RARP (ang. Reverse Address Resolution Protocol) jest podobny do protokołu ARP, ale działa w odwrotnym kierunku. Jest to protokół służący do automatycznego przypisywania adresów MAC do adresów IP w sieci Ethernet. W tym celu wykorzystuje się wysyłanie pakietów RARP, które służą do wymiany informacji o adresach MAC i IP.

4. Zabacułem (?????)

**Grupa A**

1. Model ISO-OSI

Model OSI-ISO (ang. Open Systems Interconnection - International Organization for Standardization) to model połączenia systemów otwartych, zaproponowany w 1977 roku przez organizację ISO. Model składa się z siedmiu warstw:

- **Warstwa fizyczna** (ang. Physical Layer) – odpowiada za dostarczanie fizycznych środków transportu danych pomiędzy komputerami.
- **Warstwa dostępu do medium** (ang. Data Link Layer) – odpowiada za dostarczanie środków technicznych do przesyłania danych, które zostały zapisane w warstwie fizycznej.
- **Warstwa sieciowa** (ang. Network Layer) – odpowiada za organizację danych w różnych sieciach, np. routowanie, łączenie sieci i adresowanie.
- **Warstwa transportowa** (ang. Transport Layer) – odpowiada za dostarczanie środków transportu danych między komputerami.
- **Warstwa sesji** (ang. Session Layer) – odpowiada za kontrolę sesji między komputerami, takich jak synchronizacja, kontrola błędów i komunikacja.
- **Warstwa prezentacji** (ang. Presentation Layer) – odpowiada za dostarczanie środków prezentacji danych, takich jak kompresja, szyfrowanie i konwersja danych.
- **Warstwa aplikacji** (ang. Application Layer) – odpowiada za dostarczanie środków aplikacji danych, takich jak protokoły sieciowe, przeglądarki internetowe i e-mail.

2. Zapytania i odpowiedzi w DNS – wymień i opisz

- Rekord A – służy do mapowania nazw domenowych na adresy IP. Przykładowo, komputer z adresem IP 192.168.0.1 może mieć nazwę hosta "www.example.com".
- Rekord NS – określa, który serwer DNS jest autorytatywny dla danej domeny.
- Rekord CNAME – służy do tworzenia aliasów dla danej domeny. Na przykład, możesz użyć CNAME, aby "www.example.com" było równoważne "example.com".
- Rekord MX – służy do wskazania serwera poczty, który będzie odbierał wiadomości dla danej domeny.
- Rekord PTR – mapuje adresy IP na nazwy domenowe. Jest to używane w protokole odwrotnego DNS, który służy do wyszukiwania nazw domenowych na podstawie adresów IP.

3. Co to jest VLAN – do czego służy i jak działa?

VLAN (Virtual Local Area Network) to wirtualna sieć lokalna, która służy do logicznego grupowania stacji roboczych w określonych przestrzeniach sieciowych. Wirtualna sieć lokalna może być używana do określania dostępu do zasobów sieciowych, zabezpieczeń i kontroli ruchu sieciowego. Struktura VLAN pozwala administratorom sieci wydzielić określone strefy sieciowe, zapewniając tym samym zwiększoną elastyczność w zarządzaniu siecią.

VLAN działa poprzez tworzenie wirtualnych komputerów na istniejącej sieci LAN. Każdy wirtualny komputer może być używany do przechowywania i przesyłania danych, tak jak zwykły komputer. VLAN jest stosowany, ponieważ pozwala administratorom tworzyć wirtualne sieci lokalne na istniejącej fizycznej sieci, co zapewnia lepszą kontrolę nad przepływem danych. Ponadto, zastosowanie VLAN umożliwia administratorom sieci tworzenie sieci, które są odizolowane od innych sieci, co pozwala na lepsze zarządzanie dostępem do zasobów sieciowych.

4. Ramka PAUSE

Ramka PAUSE jest ostatnią ramką wprowadzaną do środowiska Ethernet. Służy do wstrzymywania transmisji danych. Ramka ta jest wysyłana do innych urządzeń w sieci, aby zatrzymać przesyłanie

danych. Ramka PAUSE jest wykorzystywana do zarządzania zasobami sieciowymi, takimi jak przepustowość, w celu zapobiegania zakłóceniom w sieci.

**Grupa B**

1. CSMA/CD

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) jest techniką kontroli dostępu do medium transmisyjnego w sieciach komputerowych. CSMA/CD jest stosowane w sieciach Ethernet, w których komputery komunikują się korzystając z kabla, lub innego medium transmisyjnego.

Idea działania CSMA/CD jest prosta. Wszystkie komputery w sieci mają możliwość wykrywania że kabel jest w użyciu (tzw. Carrier Sense). 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 (Collision). Wszystkie komputery w sieci są zaprogramowane do wykrywania tych kolizji (Collision Detection). W przypadku wykrycia kolizji, wszystkie komputery przerywają wysyłanie danych i wykonują procedurę Backoff, czyli losowe przesuwanie czasu oczekiwania przed ponownym wysłaniem danych.

2. Techniki złączeń światłowodowych + krótki opis

Techniki złączeń światłowodowych to sposoby łączenia włókien światłowodowych, aby umożliwić przesyłanie danych. Do wykonania tego typu połączeń stosuje się specjalny sprzęt, taki jak narzędzia do cięcia, klejenia i polerowania.

- Złącze mechaniczne: Jest to technika łączenia, w której włókna są złączone za pomocą złączy mechanicznych. Złącza te są szczelne i trwałe, dzięki czemu stosuje się je w szerokim zakresie aplikacji.
- Złącze fusion splice: Fusion splice jest to technika łączenia, w której włókna są połączone przez łączenie ich końców. Używa się fali elektromagnetycznej lub lasera do łączenia włókien, co pozwala na uzyskanie wyjątkowo wysokiej jakości połączenia.
- Złącze typu connect-and-go: Jest to technika łączenia, w której końce włókien są połączone za pomocą złączy typu connect-and-go. Połączenia te są zarówno trwałe, jak i szybkie w instalacji, co czyni je bardzo praktycznymi w aplikacjach, w których potrzebne jest szybkie wykonanie połączenia.

3. Protokół ICMP – opisz

Protokół ICMP służy do przesyłania komunikatów diagnostycznych między komputerami w sieci IP. ICMP jest często wykorzystywany do przekazywania komunikatów o błędach i problemach z połączeniami lub dostępem do zasobów sieciowych. ICMP może być również wykorzystywany do wykrywania komputerów w sieci, tworzenia map sieci i monitorowania połączeń sieciowych.

4. Odpowiedzi i zapytania DNS

- Rekord A – służy do mapowania nazw domenowych na adresy IP. Przykładowo, komputer z adresem IP 192.168.0.1 może mieć nazwę hosta "www.example.com".
- Rekord NS – określa, który serwer DNS jest autorytatywny dla danej domeny.
- Rekord CNAME – służy do tworzenia aliasów dla danej domeny. Na przykład, możesz użyć CNAME, aby "www.example.com" było równoważne "example.com".
- Rekord MX – służy do wskazania serwera poczty, który będzie odbierał wiadomości dla danej domeny.

- Rekord PTR – mapuje adresy IP na nazwy domenowe. Jest to używane w protokole odwrotnego DNS, który służy do wyszukiwania nazw domenowych na podstawie adresów IP.

**Grupa A**

1. Czym jest modulacja sygnału? Podaj 3 klasyczne techniki modulacji.

Modulacja sygnału to proces zmiany cech sygnału w celu wyrażenia informacji zawartej w innym sygnale. To technika pozwalająca na przesyłanie informacji za pośrednictwem sygnału nośnego. Klasyczne techniki modulacji to:

- Amplitudowa modulacja składowej stałej (AM)
- Modulacja częstotliwości (FM)
- Modulacja częstotliwości składowej stałej (FSK)

2. CSMA/CA – rozwiń skrót i opisz zasadę działania

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – jest to protokół sieciowy stosowany w sieciach bezprzewodowych. Umożliwia on użytkownikom komunikowanie się bez wykorzystania kontrolowanych łączy. Zasada działania tego protokołu opiera się na następującym założeniu: wszystkie urządzenia w sieci mogą wysyłać i odbierać informacje, jednak przed wysłaniem wiadomości muszą one sprawdzić, czy pasmo jest wolne. Jeśli wszystkie urządzenia w sieci będą postępować zgodnie z tym założeniem, zmniejszy się ryzyko wystąpienia kolizji i przeładowania sieci.

3. Światłowód – omów zasadę działania i budowę

Światłowód to przewód światłowy służący do transmisji sygnałów. Głównym elementem światłowodu jest środowisko przewodzące - włókno optyczne. Składa się ono z dwóch warstw: warstwy dielektrycznej (powłoka z polietylenu) i warstwy światłowodowej (kryształ światłowodowy). 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.

4. Three-way-handshake – na czym polega, opisz kroki oraz stany w każdym z nich.

Three way handshake to mechanizm używany do ustanowienia połączenia między dwoma hostami. To protokół sieciowy, który umożliwia obustronną wymianę danych między dwoma hostami. Stany hostów zmieniają się w następujący sposób:

- Pierwszy stan: Host A wysyła do hosta B pakiet SYN (synchronizacja).
- Drugi stan: Host B odbiera pakiet SYN i wysyła do hosta A pakiet SYN-ACK (synchronizacja + potwierdzenie).
- Trzeci stan: Host A odbiera pakiet SYN-ACK i wysyła do hosta B pakiet ACK (potwierdzenie).

**Dla IS:**

1. Co to są well-known-ports? Podaj 4 przykłady.

Well-known-ports to zakresy portów w systemie IP, które są zazwyczaj używane do odpowiednich zastosowań. Przykłady to:

- 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).

2. Co to jest reverse DNS

Reverse DNS to inna nazwa dla odwrotnego konwertowania numeru IP na nazwę hosta. Jest to proces w którym numer IP jest konwertowany na nazwę domeny. Proces ten jest używany do identyfikacji witryn internetowych i systemów informatycznych.

3. Opisać, podać zastosowanie, wady i zalety: skrętki i kabla koncentracyjnego.

**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.

4. Co to jest VLAN i dlaczego się go stosuje?

VLAN (Virtual Local Area Network) to wirtualna sieć lokalna, która służy do logicznego grupowania stacji roboczych w określonych przestrzeniach sieciowych. Wirtualna sieć lokalna może być używana do określania dostępu do zasobów sieciowych, zabezpieczeń i kontroli ruchu sieciowego. Struktura

VLAN pozwala administratorom sieci wydzielić określone strefy sieciowe, zapewniając tym samym zwiększoną elastyczność w zarządzaniu siecią.

VLAN działa poprzez tworzenie wirtualnych komputerów na istniejącej sieci LAN. Każdy wirtualny komputer może być używany do przechowywania i przesyłania danych, tak jak zwykły komputer. VLAN jest stosowany, ponieważ pozwala administratorom tworzyć wirtualne sieci lokalne na istniejącej fizycznej sieci, co zapewnia lepszą kontrolę nad przepływem danych. Ponadto, zastosowanie VLAN umożliwia administratorom sieci tworzenie sieci, które są odizolowane od innych sieci, co pozwala na lepsze zarządzanie dostępem do zasobów sieciowych.

**Dla IO:**

1. Co to jest TTL?

TTL (ang. 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. Jeśli liczba TTL osiągnie zero, pakiet jest odrzucany i wysyłane jest potwierdzenie o odrzuceniu.

2. Protokół TCP

Protokół TCP (Transmission Control Protocol) jest protokołem warstwy transportowej w modelu OSI. Jest to protokół połączeniowy, który zapewnia niezawodne przesyłanie danych pomiędzy dwoma hostami działającymi w sieci TCP/IP. 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. Protokół TCP jest używany do obsługi wielu usług sieciowych, w tym protokołu WWW, SSH, FTP, Telnet i wiele innych.

3. Domena kolizyjna i sposoby jej separacji.

Domena kolizyjna to miejsce w sieci, w którym dwa lub więcej urządzeń komunikuje się z tą samą siecią w tym samym czasie. Domeny kolizyjne powstają, gdy dwa lub więcej urządzeń wysyła jednocześnie dane do tej samej sieci. Aby zapobiec zakłóceniom w przepływie danych, wymagana jest separacja domeny kolizyjnej. Sposoby separacji domeny kolizyjnej obejmują:

- Użycie przełączników lub routerów: Przełączniki i routery są urządzeniami do przesyłania danych między sieciami. Rozdzielają one domenę kolizyjną i dostarczają skrótów dla sieci, w których przesyłają dane.
- Użycie protokołu CSMA/CD: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to protokół sieciowy, który umożliwia wiele urządzeń do komunikowania się za pomocą jednej sieci. Protokół ten pozwala urządzeniom wykrywać zakłócenia w sieci i zapobiegać występowaniu kolizji.
- Użycie algorytmu dystrybucji czasu: Algorytm dystrybucji czasu (TDMA) jest stosowany do podziału czasu w sieci na okresy. Urządzenia w sieci mogą wysyłać dane tylko w okresach, które są przydzielone specjalnie dla nich, dzięki czemu nie ma konfliktów.

4. Co wpłynęło na wzrost przepustowości 802.3?

Większa przepustowość sieci 802.3 wynika przede wszystkim z wprowadzenia i stosowania szybszych standardów transmisji danych. W miarę jak technologia postępowała, można było uzyskać wyższą przepustowość za pomocą szybszych standardów technologicznych, takich jak 10 Gb / s, 40 Gb / s i 100 Gb / s. Ponadto nowe technologie, takie jak Power over Ethernet (PoE), Gigabit Ethernet (GbE) i 10-Gigabit Ethernet (10 GbE) wpłynęły również na wzrost przepustowości sieci 802.3. Wzrost

przepustowości sieci 802.3 osiągnięto również dzięki wprowadzeniu nowych standardów kabli, takich jak kategorie 5, 5e i 6, które znacznie zwiększyły prędkości transmisji danych.

5. Opisać fizyczne struktury DNS.

Fizyczna struktura DNS polega na rozproszeniu serwerów nazw domen po całym świecie. Serwery DNS zlokalizowane są na serwerach fizycznych, które mogą znajdować się w różnych lokalizacjach. Serwery te tworzą sieć serwerów DNS, która jest wykorzystywana do przetwarzania zapytań związanych z nazwami domen. Serwery te służą również do przechowywania informacji dotyczących domen, takich jak adresy IP, informacje o hostach i inne informacje, które są potrzebne do prawidłowego działania sieci.

6. Podzielić sieci ze względu na tryb nadawania.

Sieci mogą być podzielone ze względu na typ nadawania na sieci:

- Sieci wymiany danych: sieci wymiany danych służą do przesyłania danych między urządzeniami, takimi jak komputery i serwery. Przykładami sieci tego typu są LAN, WAN i MAN.
- Sieci transmisji wideo: sieci transmisji wideo są wykorzystywane do przesyłania strumieniowego wideo między urządzeniami. Przykładami sieci tego typu są sieci telewizji kablowej, satelitarnej i naziemnej.
- Sieci transmisji głosu: sieci transmisji głosu są wykorzystywane do przesyłania głosu między urządzeniami. Przykładami sieci tego typu są sieci telefonii stacjonarnej i komórkowej.
- Sieci bezprzewodowe: sieci bezprzewodowe są wykorzystywane do przesyłania danych między urządzeniami bez kabli. Przykładami sieci tego typu są sieci Wi-Fi, Bluetooth.

7. ICMP – rozwinąć skrót, krótko opisać, zastosowanie.

Protokół ICMP (Internet Control Message Protocol) służy do przesyłania komunikatów diagnostycznych między komputerami w sieci IP. ICMP jest często wykorzystywany do przekazywania komunikatów o błędach i problemach z połączeniami lub dostępem do zasobów sieciowych. ICMP może być również wykorzystywany do wykrywania komputerów w sieci, tworzenia map sieci i monitorowania połączeń sieciowych.

8. DHCP – krótko scharakteryzować i opisać algorytm.

DHCP (Dynamic Host Configuration Protocol) to protokół komunikacji sieciowej używany do automatycznego przydzielania adresów IP i innych parametrów sieciowych do komputerów i innych urządzeń w sieci. Algorytm DHCP jest podobny do serwera wydzierżawiania, w którym przydzielane są adresy IP (lub inne informacje sieciowe), a następnie po odpowiednim czasie zwracane do serwera. 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.

9. Co to jest i jak działa reverse DNS.

Reverse DNS to inna nazwa dla odwrotnego konwertowania numeru IP na nazwę hosta. Jest to proces w którym numer IP jest konwertowany na nazwę domeny. Proces ten jest używany do identyfikacji witryn internetowych i systemów informatycznych.

10. 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.

Przełącznik sieciowy jest urządzeniem sieciowym, 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.

11. Opisać TCP w transmisji

**Grupa A**

1. Co to jest metryka? Jakie informacje może zawierać i na co może mieć wpływ?

Metryka to szczegółowe i dokładne opisanie danych. Może zawierać informacje, takie jak typ danych, wielkość, jakość, kontekst i lokalizacja. Metryka może wpływać na to, jak sieci i administracja danych są zarządzane. Pozwala administratorom danych określić, jakie dane są przechowywane i jak są one wykorzystywane. Metryka może również pomóc w ocenie jakości danych i w ustaleniu, czy dane są wystarczająco dokładne i aktualne.

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

FTP (File Transfer Protocol) to protokół sieciowy, który służy do przesyłania plików pomiędzy dwoma komputerami. Został stworzony w celu dostarczenia szybkiego i bezpiecznego sposobu wymiany danych. Protokół FTP wykorzystuje TCP/IP jako podstawowy protokół transportowy i w celu bezpieczeństwa używa autentykacji użytkowników oraz szyfrowania danych.

TFTP (Trivial File Transfer Protocol) jest podobny do protokołu FTP, ponieważ również służy do przesyłania plików między dwoma komputerami. Różni się jednak od protokołu FTP, ponieważ jest to bardzo prosty, niezabezpieczony protokół, który nie wymaga autentykacji użytkowników ani szyfrowania danych. TFTP jest przydatny do przesyłania małych plików, ponieważ ma bardzo małe wymagania dotyczące zasobów systemowych. Główne różnice pomiędzy protokołami FTP i TFTP to:

- FTP jest zabezpieczony i wymaga autentykacji użytkowników, podczas gdy TFTP nie posiada żadnych zabezpieczeń.
- FTP wymaga dużo mocy obliczeniowej, ponieważ jest zabezpieczony, podczas gdy TFTP jest bardzo prostym protokołem, który ma niskie wymagania systemowe.
- FTP używa TCP/IP jako podstawowego protokołu transportowego, podczas gdy TFTP używa UDP.

3. Co to jest VLSM? Rozwiń skrót i opisz technologię, gdzie jest stosowana?

VLSM (Variable Length Subnet Mask) to technologia sieciowa stosowana w celu optymalizacji adresów IP. Pozwala ona na podział jednej sieci na mniejsze podsieci o różnych długościach maski podsieci. Technologia VLSM jest stosowana w sieciach, które wymagają zwiększenia liczby adresów IP, ale nie korzystają z wirtualnych sieci wirtualnych. Umożliwia to administratorom sieci użycie mniejszych masek podsieci, aby lepiej wykorzystać dostępną ilość adresów IP. Technologia VLSM jest szeroko stosowana w sieciach LAN i WAN, szczególnie w sieciach wielopoziomowych.

4. Co to jest domena .arpa i gdzie jest wykorzystywana?

Domena .arpa to domena specjalnego przeznaczenia wykorzystywana głównie w systemach komunikacyjnych i usługach sieciowych. Jest wykorzystywana do śledzenia adresów IP i adresów sieciowych, do przypisywania nazw hostom, do identyfikacji serwerów DNS oraz do tworzenia środowisk testowych.

**Grupa B**

1. Jakie są cele kodowania w sieciach komputerowych. (Powiedział, że nie chodzi ani o kompresję, ani o szyfrowanie).

Cele kodowania w sieciach komputerowych to:

- 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.

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

Protokoły routujące to protokoły sieciowe, które pozwalają routerom na wykrywanie innych sieci i wybór najbardziej optymalnych ścieżek (tras) docelowych. Przykłady to protokoły głównie z rodziny TCP/IP, takie jak: RIP, OSPF, EIGRP, BGP, IS-IS.

Protokoły routowalne to protokoły, które umożliwiają wymianę informacji pomiędzy routerami, aby umożliwić im odpowiednie routowanie pakietów. Przykłady to protokoły z rodziny TCP/IP, takie jak: ICMP, ARP, RARP, DHCP, PPP.

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

- Sieci lokalne (LAN): sieci wykorzystywane do komunikacji pomiędzy urządzeniami znajdującymi się w miejscu ograniczonym geograficznie, np. biuro, szkoła lub dom.
- Sieci rozległe (WAN): sieci wykorzystywane do komunikacji pomiędzy urządzeniami w odległych lokalizacjach, takich jak różne miasta, kraje lub kontynenty.
- Sieci metropolitalne (MAN): sieci wykorzystywane do komunikacji pomiędzy urządzeniami znajdującymi się w dużym obszarze, takim jak duże miasto lub region.
- Sieci kampusowe (CAN): sieci wykorzystywane do komunikacji pomiędzy urządzeniami znajdującymi się na terenie danego obiektu, np. szkoły, szpitala lub fabryki.

4. Opisz protokół ICMP

Protokół ICMP służy do przesyłania komunikatów diagnostycznych między komputerami w sieci IP. ICMP jest często wykorzystywany do przekazywania komunikatów o błędach i problemach z połączeniami lub dostępem do zasobów sieciowych. ICMP może być również wykorzystywany do wykrywania komputerów w sieci, tworzenia map sieci i monitorowania połączeń sieciowych.

**Grupa A**

1. WCM

WCM (Web Content Management) to system zarządzania treścią, pozwalający tworzyć, edytować i zarządzać treścią stron internetowych. WCM zapewnia zintegrowane narzędzia i procesy, które pozwalają użytkownikom tworzyć, aktualizować i zarządzać treścią w sieci.

2. Socket

Socket to interfejs programowy używany do tworzenia aplikacji sieciowych. Socket pozwala aplikacjom komunikować się pomiędzy sobą w celu wymiany danych. Socket umożliwia aplikacjom nawiązywanie połączeń i komunikowanie się za pośrednictwem protokołów sieciowych, takich jak TCP/IP, UDP i innych.

3. Tablica routingu

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

4. Podaj 4 aktywne urządzenia z 2 lub 3 warsty ISO-OSI

- Routery
- Switche
- Brama VoIP
- Kontroler bezprzewodowy

**Grupa B**

1. Domena kolizyjna i sposoby jej separacji.

Domena kolizyjna to miejsce w sieci, w którym dwa lub więcej urządzeń komunikuje się z tą samą siecią w tym samym czasie. Domeny kolizyjne powstają, gdy dwa lub więcej urządzeń wysyła jednocześnie dane do tej samej sieci. Aby zapobiec zakłóceniom w przepływie danych, wymagana jest separacja domeny kolizyjnej. Sposoby separacji domeny kolizyjnej obejmują:

- Użycie przełączników lub routerów: Przełączniki i routery są urządzeniami do przesyłania danych między sieciami. Rozdzielają one domenę kolizyjną i dostarczają skrótów dla sieci, w których przesyłają dane.
- Użycie protokołu CSMA/CD: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to protokół sieciowy, który umożliwia wiele urządzeń do komunikowania się za pomocą jednej sieci. Protokół ten pozwala urządzeniom wykrywać zakłócenia w sieci i zapobiegać występowaniu kolizji.
- Użycie algorytmu dystrybucji czasu: Algorytm dystrybucji czasu (TDMA) jest stosowany do podziału czasu w sieci na okresy. Urządzenia w sieci mogą wysyłać dane tylko w okresach, które są przydzielone specjalnie dla nich, dzięki czemu nie ma konfliktów.

2. Struktura DNS

DNS (Domain Name System, sieć nazw domenowych) jest hierarchicznym systemem informacji składającym się z serwerów, które mapują nazwy domen na adresy IP. Struktura DNS składa się z następujących elementów:

- Serwery główne (Root Servers): Są to serwery główne, które są odpowiedzialne za rozdzielanie domen na różne serwery.

- Serwery TLD (Top Level Domain): Są to serwery, które są odpowiedzialne za wyświetlanie i przesyłanie informacji o domenach na najwyższym poziomie.
- Serwery autorytatywne: Są odpowiedzialne za zarządzanie informacjami o domenach na niższym poziomie, takich jak domeny drugiego poziomu.
- Serwery rekurencyjne: Są odpowiedzialne za przekazywanie informacji o domenach innym serwerom.
- Serwery poczty: Są to serwery, które są odpowiedzialne za przechowywanie i przesyłanie wiadomości e-mail. 6. Serwery WWW: Są one odpowiedzialne za wyświetlanie stron internetowych.

3. Wymień i opisać techniki łączenia światłowodów.

Techniki złączeń światłowodowych to sposoby łączenia włókien światłowodowych, aby umożliwić przesyłanie danych. Do wykonania tego typu połączeń stosuje się specjalny sprzęt, taki jak narzędzia do cięcia, klejenia i polerowania.

- Złącze mechaniczne: Jest to technika łączenia, w której włókna są złączone za pomocą złączy mechanicznych. Złącza te są szczelne i trwałe, dzięki czemu stosuje się je w szerokim zakresie aplikacji.
- Złącze fusion splice: Fusion splice jest to technika łączenia, w której włókna są połączone przez łączenie ich końców. Używa się fali elektromagnetycznej lub lasera do łączenia włókien, co pozwala na uzyskanie wyjątkowo wysokiej jakości połączenia.
- Złącze typu connect-and-go: Jest to technika łączenia, w której końce włókien są połączone za pomocą złączy typu connect-and-go. Połączenia te są zarówno trwałe, jak i szybkie w instalacji, co czyni je bardzo praktycznymi w aplikacjach, w których potrzebne jest szybkie wykonanie połączenia.

4. Co wpłynęło na wzrost przepustowości sieci 802.3?

Większa przepustowość sieci 802.3 wynika przede wszystkim z wprowadzenia i stosowania szybszych standardów transmisji danych. W miarę jak technologia postępowała, można było uzyskać wyższą przepustowość za pomocą szybszych standardów technologicznych, takich jak 10 Gb / s, 40 Gb / s i 100 Gb / s. Ponadto nowe technologie, takie jak Power over Ethernet (PoE), Gigabit Ethernet (GbE) i 10-Gigabit Ethernet (10 GbE) wpłynęły również na wzrost przepustowości sieci 802.3. Wzrost przepustowości sieci 802.3 osiągnięto również dzięki wprowadzeniu nowych standardów kabli, takich jak kategorie 5, 5e i 6, które znacznie zwiększyły prędkości transmisji danych.

**Grupa A**

1. Podział sieci ze względu na typ nadawania.

Sieci mogą być podzielone ze względu na typ nadawania na sieci:

- Sieci wymiany danych: sieci wymiany danych służą do przesyłania danych między urządzeniami, takimi jak komputery i serwery. Przykładami sieci tego typu są LAN, WAN i MAN.
- Sieci transmisji wideo: sieci transmisji wideo są wykorzystywane do przesyłania strumieniowego wideo między urządzeniami. Przykładami sieci tego typu są sieci telewizji kablowej, satelitarnej i naziemnej.
- Sieci transmisji głosu: sieci transmisji głosu są wykorzystywane do przesyłania głosu między urządzeniami. Przykładami sieci tego typu są sieci telefonii stacjonarnej i komórkowej.

- Sieci bezprzewodowe: sieci bezprzewodowe są wykorzystywane do przesyłania danych między urządzeniami bez kabli. Przykładami sieci tego typu są sieci Wi-Fi, Bluetooth.

2. Jakie funkcje pełni TCP w warstwie transportowej.
3. Co to jest adres MAC i jak jest zbudowany?

Adres MAC (ang. Media Access Control) to unikalny identyfikator sprzętowy, służący do identyfikacji komputerów w sieci komputerowej. Jest zbudowany z 48-bitowego ciągu znaków. Każdy znak składa się z dwóch zmiennoprzecinkowych cyfr szesnastkowych, oznaczonych od 0 do 9 i od A do F. Przykładowy adres MAC to 0A-3F-3B-1F-E3-6F.

4. TTL w nagłówku IP.

TTL (ang. 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. Jeśli liczba TTL osiągnie zero, pakiet jest odrzucany i wysyłane jest potwierdzenie o odrzuceniu.

**Grupa B**

1. Co wpłynęło na wzrost przepustowości sieci 802.3?

Większa przepustowość sieci 802.3 wynika przede wszystkim z wprowadzenia i stosowania szybszych standardów transmisji danych. W miarę jak technologia postępowała, można było uzyskać wyższą przepustowość za pomocą szybszych standardów technologicznych, takich jak 10 Gb / s, 40 Gb / s i 100 Gb / s. Ponadto nowe technologie, takie jak Power over Ethernet (PoE), Gigabit Ethernet (GbE) i 10-Gigabit Ethernet (10 GbE) wpłynęły również na wzrost przepustowości sieci 802.3. Wzrost przepustowości sieci 802.3 osiągnięto również dzięki wprowadzeniu nowych standardów kabli, takich jak kategorie 5, 5e i 6, które znacznie zwiększyły prędkości transmisji danych.

2. Co to jest WDM? Rozwiń skrót i opisz technologię.

WDM (ang. Wave Division Multiplexing) to technologia łączności optycznej, która pozwala na przesyłanie kilku sygnałów światłowodowych poprzez jeden światłowód. WDM jest zazwyczaj wykorzystywany do łączenia kilku sieci różnych typów w jedną sieć optyczną. Technologia ta pozwala na przesyłanie szerokopasmowych sygnałów optycznych za pomocą jednego światłowodu. WDM dzieli pasmo radiowe na wiele mniejszych pasm i pozwala je przesyłać jednocześnie. Technologia ta jest często wykorzystywana do przesyłania sygnałów szerokopasmowych, takich jak sygnały telewizyjne, sygnały dźwiękowe, sygnały danych i sygnały telefoniczne.

3. Cele kodowania w sieciach komputerowych.

Cele kodowania w sieciach komputerowych to:

- 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.

4. Modulacja, co to jest + 3 klasyczne sposoby.

Modulacja sygnału to proces zmiany cech sygnału w celu wyrażenia informacji zawartej w innym sygnale. To technika pozwalająca na przesyłanie informacji za pośrednictwem sygnału nośnego. Klasyczne techniki modulacji to:

- Amplitudowa modulacja składowej stałej (AM)
- Modulacja częstotliwości (FM)
- Modulacja częstotliwości składowej stałej (FSK)