KOLOS III

1. **Opisz architekturę sieci bluetooth, co to jest pikosieć i jak działa?**

Bluetooth pozwala na szybkie skonstruowanie bezprzewodowych, radiowych sieci łączących odpowiednie urządzenia wyposażone w moduły nadawczo-odbiorcze Bluetooth. Takie połączenia realizowane są zawsze w relacjach master-slave. Jest możliwość zestawienia dwóch rodzajów łączy
między urządzeniami typu master i slave:
• łącze typu point-to-point – jest połączeniem 2 urządzeń Bluetooth z których jedno pełni rolę urządzenia nadrzędnego (master) natomiast drugie podrzędnego (slave);
• łącze typu point-to-multipoint tworzy sieć składającą się z maksymalnie ośmiu urządzeń, które określa się pikonetem. Kilka pikonetów dzięki jednemu z urządzeń wchodzących w skład sieci,może współpracować ze sobą, tworząc większy konglomerat (scatternet)
Podstawową jednostką standardu Bluetooth jest pikosieć, która zawiera węzeł typu master oraz maksymalnie 7 węzłów typu slave oraz w jednej pikosieci może pracować do 255 węzłów pozostających w stanie synchronizacji z urządzeniem typu master.Podział węzłów na master i slave to minimalizacja kosztów technologii. Wiele pikosiecie może być w jednym pomieszczeniu, a nawet mogą być ze sobą połączone za pomocą węzła typu bride, a połączone pikosieci nazywamy scatternet. Pikosieć jest scentralizowanym systemem TDM,
urządzenie master kontroluje zegar i określa, które urządzenie i w którym slocie czasowym może się z nim komunikować. Wymiana danych może nastąpić tylko pomiędzy węzłem master i slave. Komunikacja slave – slave nie jest możliwa.

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

a. Bluetooth 1.0 – 21 kb/s
b. Bluetooth 1.1 – 124 kb/s
c. Bluetooth 1.2 – 328 kb/s
d. Bluetooth 2.0 – 2,1 Mb/s,
e. Bluetooth 2.0 + EDR (Enhanced Data Rate) - 3,1 Mb/s
f. Bluetooth 3.0 + HS (High Speed) – 24 Mb/s (3 MB/s)
g. Bluetooth 3.1 + HS (High Speed) – 40 Mb/s (5 MB/s)
h. Bluetooth 4.0 + LE (Low Energy) – 200 kb/s, niższe zużycie energii, mniejszy transfer, większy zasięg (do100m)
i. Bluetooth 4.1 – standard opracowany do zastosowania w tzw. „internecie rzeczy", umożliwiający bezpośrednią łączność przedmiotów z internetem
j. Bluetooth 4.2 – w stosunku do poprzednich wersji: szybszy transfer, wyższy poziom bezpieczeństwa, nawiązanie łączności z przedmiotami – łatwiejsze
k. 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.

3. **Na czym polega i czemu służy architektura CIDR?**

Polega na dowolnym definiowaniu długości maski podsieci. Wykorzystuje maskę podsieci do ustalenia zmiennej części 32 bitowego adresu IP sieci. CIDR pozwala na efektywniejsze wykorzystywanie puli adresów IP oraz zmniejszenie tablic routingu.

Aby poprawność efektywność wykorzystania adresów IPv4, wprowadzono architekturę CIDR (ang Classless Inter-Domain Routing). Głównym zadaniem tej architektury było spowolnienie wzrostu rozmiaru tablic routingu w routerach oraz spowolnienie procesu wyczerpywania puli adresów IPv4. W

maski. Przy okazji wprowadzenia architektury CIDR wprowadzono również nowy sposób zapisu maski, tzw. zapis skrócony lub zapis CIDR. Od tej pory zamiast podawać pełną maskę zapisaną w postaci czterech oktetów (255.255.255.0) wystarczy podać liczbę bitów maski o wartości 1 (255.255.255.0 => 11111111.11111111.11111111.0 => /24).

4. Budowa adresu IPv4 - opisz i podaj przykład

Jest to liczba 32 bitowa która jest zapisywana jako 4 osobne bity oddzielone kropką. Może być zapisywana w systemie dziesiętnym lub dwójkowym. Maska sieci to liczba 32 bitowa złożona z 1 oraz 0. Zadaniem maski sieci jest wydzielenie z adresu IP części identyfikującej sieć (lub podsieć) i części identyfikującej host.

Obliczanie adresu sieci

W celu obliczenia adresu (pod) sieci, do której należy podane adres IP, należy wykonać iloczyn binarny (operacja AND) adresu i maski:

Obliczanie adresu rozgłoszeniowego (broadcast)

Aby obliczyć adres rozgłoszeniowy (pod)sieci należy najpierw przeprowadzić negację maski (operacja NOT)

Obliczanie liczby adresów hosta w danej (pod)sieci

Aby obliczyć liczbę hostów, które można zaadresować w sieci o danej masce należy wykorzystać następujący wzór:

$$N = 2^{32-CIDR} - 2$$

gdzie: CIDR – skrócony zapis maski (pod)sieci

Obliczanie pierwszego i ostatniego adresu hosta

Aby wyznaczyć pierwszy adres hosta, należy do adresu (pod)sieci dodać 1 (czyli zamienić ostatni bit z 0 na 1):

```
Adres sieci:       192.168.100.0 => 11000000.10101000.01100100.00000000
Pierwszy adres hosta: 192.168.100.1 => 11000000.10101000.01100100.00000001
```

Aby wyznaczyć ostatni adres hosta należy od adresu rozgłoszeniowego odjąć 1 (czyli zamienić ostatni bit z 1 na 0):

```
Adres rozgłoszeniowy: 192.168.100.255 => 11000000.10101000.01100100.11111111
Ostatni adres hosta:  192.168.100.254 => 11000000.10101000.01100100.11111110
```

5. Czym jest sieć TOR?

TOR jest 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. Szyfrowanie ruchu uniemożliwia podsłuchiwanie przez ISP. Przekazywanie pakietów następuje ustaloną przed wysłaniem trasą za pomocą łańcucha węzłów. Ze względu na to, że w przypadku ukrytej usługi Tor ukrywa również IP serwera użycie tej technologii pozwala ominąć cenzurę niektórych usług w sieci. Z drugiej strony jednak wiele usług, których działanie opiera się na pozyskiwaniu i przetwarzaniu danych użytkowników stara się blokować anonimizowany ruch z sieci Tor. Tor i usługi przezeń działające używane są więc m. in. do anonimowej komunikacji, obchodzenia cenzury, zgłaszania wycieków, ukrywania zawartości pakietów przed głęboką analizą czy ochrony przed inwigilacją. Każda informacja wprowadzona równolegle do sieci Tor i sieci otwartej może zdemaskować wprowadzającego.

6. Typy węzłów w sieci TOR - wymień i krótko opisz

Typy węzłów

W strukturze sieci wyróżniamy trzy rodzaje komputerów-przekaźników:

- Guard relay (**Entry node**) - punkt wejścia do sieci, z którymi łączy się komputer kliencki.
- **Middle relay** - punkty, między którymi wymieniane są zaszyfrowane pakiety. Węzły te nie mają informacji o zawartości pakietów - każdy ma tylko informację gdzie przekazać pakiet.
- **Exit node** - Węzły wyjściowe - odszyfrowują ruch i kierują go do docelowego miejsca, np. usługi w "jawnej" sieci WWW. Są one uruchamiane zazwyczaj w miejscach o wysokiej wolności cyfrowej i niskim poziomie rządowej inwigilacji bądź na preferencyjnych warunkach. IP węzła wyjściowego to IP widziane przez docelowy serwer, najczęściej pod sporym nadzorem. Węzeł taki „bierze na siebie” cały ruch wynikowy. Dopóki więc nie jesteśmy w jakimś bezpiecznym pod względem Internetu kraju lub nie przejęliśmy cudzego serwera, nie uruchamiajmy węzła wyjściowego na swoim serwerze.