1. Co to jest sieć bezprzewodowa?

- Bezprzewodowa sieć WiFi jest systemem komunikacji zaprojektowanym jako alternatywa lub uzupełnienie sieci tradycyjnej (kablowej). Wykorzystuje ona do transmisji danych fal radiowych o odpowiedniej częstotliwości, minimalizując tym samym konieczność użycia połączeń kablowych. Sieć bezprzewodowa łączy w sobie mobilność użytkowania oraz transmisję danych.

2. Cym charakteryzuje się standard 802.11g?

- Standard ten pracuje w paśmie 2.4 GHz, jednak w odróżnieniu od 802.11b posiada przepustowość rzędu 54 Mb/s. Wykorzystuje on technologię ODM(Orthogonal Frequency Division Multiplexing). Urządzenia wspierające standard 802.11g, dzięki pracy w zakresie częstotliwości takim samym jak urządzenia 802.11b, mają możliwość współpracowania z urządzeniami w standardzie 802.11b.

3. Co to jest topologia sieci oraz jakie znasz jej przykłady w nawiązaniu do sieci bezprzewodowych?

- Topologia jest to fizyczne lub logiczne rozmieszczenie elementów sieci, czyli węzłów za pomocą których łączymy komputery w sieć. W sieciach przewodowych można wyróżnić pięć głównych typów topologii: magistrali, pierścienia, gwiazdy, drzewa i kraty. Obecnie w sieciach bezprzewodowych możemy zastosować tylko dwa spośród typów topologii, a mianowicie topologia gwiazdy oraz topologia kraty.

4. Na czym polega zjawisko ukrytej stacji?

- Zjawisko to może wystąpić jeżeli nie wszystkie stacje mają ze sobą łączność. Stacja jest ukryta jeżeli znajduje się w zasięgu stacji odbierającej dane, ale jest poza zasięgiem stacji nadawczej. Podczas tego zjawiska możemy wyróżnić zjawisko ukrytego odbiornika i nadajnika. Rozróżniamy te zjawiska gdy przesyłanie danych poprzedzone jest informacją sterującą. Zamiar nadawania realizowany jest przez wysyłanie ramki RTS (Request To Send), natomiast jeżeli adresat tej ramki może odebrać dane, sygnalizuje nadawcy za pomocą ramki CTS (Clear To Send). Kolizje wywołane tym zjawiskiem mogą spowodować ogólny spadek przepustowości sieci wskutek konieczności retransmisji.

5. Na czym polega zjowisko odkrytej stacji?

- Podczas gdy nie wszystkie stacje się widzą nawzajem, może wystąpić również zjawisko odkrytej stacji. Zjawisko to występuje gdy stacja znajduje się w zasięgu stacji nadawczej, ale poza zasięgiem stacji odbiorczej. Tutaj również wyróżniamy dwa zjawiska: odkryty nadajnik oraz odkryty odbiornik. Rozróżnia się je również poprzez wymianę ramek RTS i CTS. Kolizje wywołane tym zjawiskiem mogą spowodować ogólny spadek przepustowości łącza ponieważ zbędnie wstrzymana jest transmisja danych.

6. Na czym polega zjawisko interferencji?

- Interferencje, czyli zakłócenia transmisji, powstają gdy stacja jest poza zasięgiem zarówno odbiornika jak i nadajnika, jednak wystarczająco blisko aby móc zakłócić przesyłanie informacji między nimi. Stacje które zakłócają transmisje powinny wstrzymać nadawanie podczas gdy inna transmisja jest realizowana, jednak ani nadajnik ani odbiornik nie może poinformować stacji interferującej o tym, że zakłóca ona przebieg transmisji.

7. Na czym polega efekt przechwytywania?

- Efekt ten występuje gdy do odbiornika docierają dwa sygnały o różnej mocy. W tym momencie tylko jeden z sygnałów może zostać odebrany bezbłędnie, sygnał słabszy może zostać zagłuszony. Poprawia to zatem wykorzystanie kanału transmisyjnego, niemożna natomiast nasłuchiwać łącza podczas nadawania. Powoduje to iż niemożna wykryć kolizji podczas nadawania. W celu wykrycia tych kolizji stosuje się systemy potwierdzeń.

8. Wymień protokoły dostępowe do sieci WiFi?

- Aloha, S-Alocha, BTMA, SRMA, MACA, MACAW, BAPU

9. Co to jest CSMA/CA?

- Protokół CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) Stacja nadawcza po skompletowaniu ramki sprawdza stan łącza. Jeśli jest ono wolne rozpoczyna nadawanie, a jeśli zajęte transmisja jest wstrzymywana do czasu zwolnienia łącza. Protokół ten wykorzystuje potwierdzanie odbioru do wykrywania kolizji. Wykorzystywany jest w niektórych

bezprzewodowych sieciach LAN oraz w sieci Packet Radio.

10. Jak zbudwany jest protokół BAPU?

- Protokół BAPU ma na celu sprawniejsze niż w protokołach MACA eliminowanie zjawiska ukrytej i odkrytej stacji. Rozdzielono tu fizycznie kanał danych i kanał sterujący, przy czym ten drugi ma większy zasięg transmisji. Dzięki temu eliminuje się możliwość interferencji stacji w kanale danych. W protokole używa się pięciu typów ramek sterujących:
    - RTS (Request To Send) czyli zgłoszenie gotowości do nadawania
    - CTS (Ciear To Send) czyli zgłoszenie gotowości do odbioru
    - DS (Data Sending) poprzedzająca rozpoczęcie nadawania danych
    - NCTS (Not Ciear To Send) zgłoszenie braku gotowości do odbioru, np. wysyłana wtedy, gdy stacja jest w zasięgu innej transmisji danych
    - ACK (Acknowledge) potwierdzająca poprawny odbiór ramki danych

11. Wymień sposoby zabezpieczeń sieci WiFi?

- ukrycie ESSID, Filtracja MAC, szyfrowanie WEP, IEEE 802.1x, WPA, 802.11i
VPN

12. Czym charakteryzuje się się szyfrowanie WEP?

- Szyfrowanie WEP (ang. Wired Equivalent Privacy) jest następnym zabezpieczeniem, które zostało wprowadzone do sieci bezprzewodowych. WEP jest to pierwsze zabezpieczenie, które dość dobrze chroni nas przed włamaniami. W porównaniu do wcześniejszych zabezpieczeń można powiedzieć, że WEP jest rewolucją w zabezpieczeniach. WEP jest szyfrem, który jest najczęściej stosowany do dziś. To zabezpieczenie jest dostępne, w każdym AP, lecz powoduje obniżenie wydajności takiego połączenia. WEP w dzisiejszych czasach jest standardem i radzi sobie całkiem nieźle. Protokół WEP odziała na zasadzie współdzielonego klucza szyfrującego o długości 40 lub 104 bitów oraz 24-bitowym wektorze inicjującym IV (ang. Initialization Vector). Często mówi się o nich, że są to klucze 64 i 128 bitowe ale takie stwierdzenie jest niepoprawne technicznie. Choć to zabezpieczenie jest często stosowane to jednak nie jest idealnym ze względu na słabość wektora inicjującego oraz klucza. Dziś już powstały narzędzia , które w łatwy i szybki sposób mogą złamać taki klucz. Więc takie szyfrowanie również nie daje żadnej pewności przed hakerami. Jednak to zabezpieczenie powoduje iż wydłuża czas osoby, która chce się natychmiast dostać do sieci i odstrasza pewną grupę włamywaczy. WEP zabezpiecza sieć przed przypadkowym podsłuchaniem danych krążących w eterze czyli teoretycznie chroni naszą prywatność w sieci.

13. Czym charakteryzuje się się szyfrowanie WPA?

- WPA (ang. WiFi Protected Access) jest to szyfrowanie stosowane w sieciach bezprzewodowych standardu 802.11.Standard WPA został przedstawiony i wprowadzony przez organizacje WiFi. WPA jest następcą mniej bezpiecznego standardu WEP. WPA sam w sobie wykorzystuje protokoły TKIP, 802.1x i uwierzytelnienie EAP.WPA jest dobrze zobrazowany za pomocą tego wzoru:

WPA=802.1x+EAP+TKIP+MIC

WPA jest to standard przejściowy pomiędzy WEP a zabezpieczeniem 802.11i czyli WPA2. WPA jest to zabezpieczenie, które dzieli się na:
Personal – opierający się na kluczu PSK do zastosowań domowych,
Enterprise – służy do zastosowań profesjonalnych i korzysta z serwera RADIUS.
Zabezpieczenie WPA i 802.11i różnią się tym, że mają inne metody szyfrowania. W WPA zastosowano również algorytm Michael (MIC), który jest odpowiedzialny za uniemożliwienie ataków z odwracalnością klucza.

14. Czym charakteryzuje się standard 802.11i?

- Standard 802.11i (oznaczany często jako WPA2) został wprowadzony w 2004 roku. Protokół ten zawiera w sobie 802.1x i CCMP. Wykorzystuje klucze 128-bitowe i automatycznie je dystrybuuje. Klucze te są dynamiczne na poziomie sesji, użytkownika i klucza pakietów. WPA2 zostały poprawione wszystkie złamane zabezpieczenia z WEP jak i również zostało wzmocnione

bezpieczeństwo autoryzacji użytkownika. Teraz można by powiedzieć, że to zabezpieczenie będzie dobrze chroniło nasze sieci bezprzewodowe lecz naprawdę jest inaczej, bo i to zabezpieczenie zostało złamane przez hakerów.

15. Na czym polega metoda zabezpieczenia zwana filtracją MAC?

- Działa to na zasadzie przypisania adresów fizycznych kart bezprzewodowych użytkowników, którzy mają mieć dostęp do sieci Ethernetu. Jeśli jakiś użytkownik nie ma przypisanego adresu MAC w AP to połączy się z siecią ale nie będzie miał dostępu do Internetu.

16. Co to jest VPN?

- VPN (Virtual Private Network) jest to metoda, która pozwala zabezpieczyć transmisje. Opiera się ona na technologii tunelowania. W takim tunelu płynie ruch w ramach sieci prywatnej, między klientami końcowymi, za pośrednictwem publicznej sieci np. Internetu, w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Dane przesyłane dzięki takim tunelom mogą być szyfrowane i kompresowane a to powoduje, że cechują się bezpieczeństwem i wydajnością.

17. Co to jest ESSID?

- Jest to nazwa rozsyłana przez Access Point. W celu nawiązania połączenia z siecią udostępnioną poprzez dany AP należy znać jego nazwę dostępową.

18. W jaki sposób można ukryć ESSID?

- AP ma możliwość zablokowania rozgłaszania swojej nazwy dostępowej. Wystarczy jedynie w konfiguracji AP odznaczyć pole odpowiedzialne za rozgłaszanie nazwy ESSID. W tym momencie nazwa dostępowa AP będzie nie widoczna dla otoczenia co tym samym utrudni dołączenie się do sieci osobom nieporządanym. Jest to najsłabsza forma zabezpieczenia sieci bezprzewodowych.

19. Czym charakteryzuje się protokół Aloha?

- Był to pierwszy protokół obsługujący sieci bezprzewodowe. W tym protokole stacja może nadawać w dowolnym czasie, w związku z czym występuje wiele kolizji między ramkami wysyłanymi przez różne stacje. Kolizje są wykrywane poprzez potwierdzanie poprawnego odebrania ramki. Podczas kolizji ramka jest wysyłana ponownie po upływie losowo wybranego czasu.

20. Wymień kilka zalet sieci bezprzewodowych

Przenośność - czyli łatwa zmiana lokalizacji np. w firmach
Brak okablowania strukturalnego
Szybkość i prostota instalacji
Elastyczność instalacji
Redukcja kosztów eksploatacji
Skalowalność - łatwe dostosowanie do różnych systemów informatycznych
Mobilność dla użytkownika
Szybka i łatwa zmiana konfiguracji
Bezprzewodowy monitoring