1. Omówić mechanizm MIMO

MIMO- (Multiple Input Multiple Output) Wiele wejść wiele wyjść, umożlwia osiąganie prędkości 540Mb/s i zasięgu 110m(w terenie otwartym) użycie wielu anten w odpowiednich odległościach dzięki temu każda odbiera sygnał z innymi zakłóceniami, wykorzystanie odbić wielodrożnych (które zakłócały starsze technologie) do odzyskiwania sygnału. Stosowanie kilku aten rozmieszczonych w różnych miejscach w przestrzeni. Nie jest konieczne kupowanie u dostawy łącza o większej przepustowości.

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

Mechanizm nawiązania połączenia

Jedną z najważniejszych cech protokołu sterowania transmisją jest obecność mechanizmów nawiązania i zakończenia połączenia. Nawiązanie połączenia jest opartę o procedurę zwaną *three-way handshake*. Ustanowienia połączenia wygląda następująco:

1. Klient wysyła segment SYN wraz z inicjującym numerem sekwencji np. liczbą 100 (symbol A)
2. Serwer odpowiada wysyłając segment SYN ze swoim numerem sekwencji (symbol B), a także potwierdza otrzymanie segmentu od klienta wysyłając ACK z numerem A+1.
3. Klient wysyła potwierdzenie ACK z numerem B+1 odebrania segmentu SYN od serwera.

CO MÓWI WIKIPEDIA…

Stany połączenia [edytuj | edytuj kod]

Połączenie TCP może znajdować się w jednym z następujących stanów:

LISTEN
Gotowość do przyjęcia połączenia na określonym porcie przez serwer.

SYN-SENT
Pierwsza faza nawiązywania połączenia przez klienta. Wysłano pakiet z flagą SYN. Oczekiwanie na pakiet SYN+ACK.

SYN-RECEIVED
Otrzymano pakiet SYN, wysłano SYN+ACK. Trwa oczekiwanie na ACK. Połączenie jest w połowie otwarte (ang. *half-open*).

ESTABLISHED
Połączenie zostało prawidłowo nawiązane. Prawdopodobnie trwa transmisja.

FIN-WAIT-1
Wysłano pakiet FIN. Dane wciąż mogą być odbierane ale wysyłanie jest już niemożliwe.

FIN-WAIT-2
Otrzymano potwierdzenie własnego pakietu FIN. Oczekuje na przesłanie FIN od serwera.

CLOSE-WAIT
Otrzymano pakiet FIN, wysłano ACK. Oczekiwanie na przesłanie własnego pakietu FIN (gdy aplikacja skończy nadawanie).

CLOSING
Połączenie jest zamykane.

LAST-ACK
Otrzymano i wysłano FIN. Trwa oczekiwanie na ostatni pakiet ACK.

TIME-WAIT
Oczekiwanie w celu upewnienia się, że druga strona otrzymała potwierdzenie rozłączenia. Zgodnie z RFC 793 ↓ połączenie może być w stanie TIME-WAIT najdłużej przez 4 minuty.

CLOSED
Połączenie jest zamknięte.

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

Wybrane typy wiadomości:
0 – Echo Reply (odpowiedź na ping)
3 – Destintation Unreachable
8 – Echo Request (ping)
9 – Router Advertisement
11 – Time Exceeded
17 – Address Mask Request (żądanie maski adresowej)
18 – Address Mask Reply (zwrot maski adresowej)
30 – Traceroute

0-7	8-15	16-23	24-31
Typ	Kod	Suma kontrolna	
Identyfikator		Numer sekwencji	
Dane (opcjonalnie)			

Budowa pakietu ICMP Echo Request i Echo Reply

W przypadku pakietów ICMP Echo Request i Echo Reply w sekcji Dane dodatkowo pojawiają się dodatkowe wartość: identyfikator (16 bitów) i numer sekwencji (16 bitów). Służą one do oznaczania żądań w przypadku, gdy nadawca wysyła kilka pakietów Echo Request.

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

Algorytmy link state i distance vector
Algorytm link state (znany jako shortest path first) rozsyła informacje routingu do wszystkich węzłów obsługujących połączenia międzysieciowe. Każdy router wysyła jednak tylko tę część tabeli routingu, która opisuje stan jego własnych łączy. Algorytm distance vector (znany te pod nazwą Bellman-Ford) wysyła w sieć całą tabelę routingu, ale tylko do sąsiadujących z nim routerów. Mówiąc inaczej, algorytm link state rozsyła wszędzie, ale za to niewielkie, wybrane porcje informacji, podczas gdy distance vector rozsyła komplet informacji, ale tylko do najbliższych węzłów sieci. Każdy z algorytmów ma swoje wady i zalety. Link state jest skomplikowany i trudny do konfigurowania oraz wymaga obecności silniejszego procesora CPU. Odnotowuje za to szybciej wszelkie zmiany zachodzące w topologii sieci. Distance vector nie pracuje może tak stabilnie, ale jest za to łatwiejszy do implementowania i sprawuje się dobrze w dużych sieciach składających się z kilkudziesięciu czy nawet kilkuset routerów.

5. Opisz protokoły trasowania RIP (v1 i v2)

????

6. Opisz protokół trasowania IGRP

Protokół IGRP
Protokół IGRP (*ang. Interior Gateway Routing Protocol*) został zaprojektowany, aby wyeliminować pewne mankamenty protokołu RIP oraz poprawić obsługę większych sieci o różnych przepustowościach łączy. IGRP, podobnie jak RIP, używa trybu rozgłoszeniowego do przekazywania informacji o routingu sąsiednim routerem. Jednak IGRP ma własny protokół warstwy transportu. Nie wykorzystuje UDP ani TCP do przekazywania informacji na temat trasy sieciowej. Oferuje on trzy główne rozszerzenia względem protokołu RIP. Po pierwsze może obsługiwać sieć do 255 skoków miedzy routerami. Po drugie potrafi rozróżniać odmienne rodzaje nośników połączeń i związane z nimi koszty. Po trzecie oferuje szybszą konwergencję , dzięki użyciu aktualizacji typu flash.

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

Routing statyczny

Routing statyczny używany jest wówczas, gdy mapa połączeń sieciowych jest programowana w routerze „ręcznie" przez administratora. W razie, gdy jakaś ścieka zostanie przerwana, administrator musi przeprogramować router, aby odpowiednie pakiety mogły dotrze do celu. W systemach sieciowych o kluczowym znaczeniu taki sposób trasowania jest niemożliwy do zaakceptowania. Stosuje się więc dynamiczne routery, które automatycznie diagnozują stan połączeń i wyznaczają połączenia alternatywne.

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

Flagi:

- NS – (ang. Nonce Sum) jednobitowa suma wartości flag ECN (ECN Echo, Congestion Window Reduced, Nonce Sum) weryfikująca ich integralność
- CWR – (ang. Congestion Window Reduced) flaga potwierdzająca odebranie powiadomienia przez nadawcę, umożliwia odbiorcy zaprzestanie wysyłania echa.
- ECE – (ang. ECN-Echo) flaga ustawiana przez odbiorcę w momencie otrzymania pakietu z ustawioną flagą CE
- URG – informuje o istotności pola "Priorytet"
- ACK – informuje o istotności pola "Numer potwierdzenia"
- PSH – wymusza przesłanie pakietu
- RST – resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)
- SYN – synchronizuje kolejne numery sekwencyjne
- FIN – oznacza zakończenie przekazu danych

Protokół TCP

Zastosowanie: Three-way handshake

9. Wymień najważniejsze cechy protokołu TCP

Najważniejsze cechy protokołu:

- działa w trybie klient-serwer
- wykorzystuje procedury do nawiązania i zakończenia połączenia
- połączenie sterowane jest przy pomocy flag
- gwarantuje dostarczenie wszystkich pakietów z zachowaniem kolejności, bez duplikatów

10. Rola ramki Beacon w WiFi

Najważniejszą ramką zarządzającą w sieciach 802.11 jest ramka Beacon rozsyłana jest w stałych odstępach czasu przez punkt dostępowy (AP) lub w sieci „Ad Hoc" przez stację która w pewnym przedziale czasowym wylosuje najkrótszy offset. Losowanie ponawiane jest za każdym razem kiedy przychodzi czas na wysłanie ramki Beacon.

Typowo ramka Beacon jest rozsyłana 10 razy na sekundę

11. Wymień i opisz tryby współpracy urządzeń w sieciach WiF

5. Budowa sieci 802.11 i tryby współpracy urządzeń

- **IBSS (Independent Basic Service Set)** – niezależne stacje łączące się w trybie „ad hoc" (w razie potrzeby/ z doskoku) na zasadzie peer-to-peer (każdy z każdym) tworząc pełną lub częściową siatkę (mesh). Ramka Beacon wysyłana jest przez stację, która wylosowała najmniejszy offset w oknie rywalizacji do wysłanie tej ramki. Otrzymując ją inne stacje zaprzestają przygotowań do wysłania tej ramki aż do następnego cyklu.
- **BSS (tryb zarządzany - 1 AP**) – punkt dostępowy pełni rolę zarządzającą wysyłając ramki Beacon i decyduje czy dana stacja zostanie podłączona czy nie. Wspomaga zarządzanie energią stacji buforując pakiety. Cały ruch pomiędzy stacjami bezprzewodowymi i stacjami bezprzewodowymi a siecią przewodową odbywa się za pośrednictwem AP
- **ESS (Extended SS - infrastruktura - wiele AP)** – jw ale wchodzące w skład ESS AP mogą pracować na jednym bądź kilku kanałach dla zwiększenia przepustowości. Funkcje autoryzacji są często scentralizowane i realizowane przez jeden AP lub wydzielone urządzenie (serwer dystrybucji kluczy np radius; DHCP). Punkty komunikują się ze sobą za pomocą protokołu IAP (Inter AccessPoint Protocol). Stacja może być skojarzona tylko z jednym punktem dostępowym.

Punkt dostępowy może spełniać różne funkcje:

- **bridge AP** funkcja mostu pomiędzy siecią przewodową (802.3) a 802.11 stacje za pośrednictwem WiFi łączą się z siecią szkieletową
- **bridge WDS (Wireless Distant Service)** funkcja mostu bezprzewodowego, w którym jeden AP nie ma dostępu do sieci strukturalnej (połowa pasma jest rezerwowana na funkcje mostu) umożliwia przedłużenie zasięgu sieci bez konieczności bodowy przewodowej sieci szkieletowej
- **client** funkcja mostu w której AP nie może obsługiwać stacji bezprzewodowych tylko przewodowe

12. Definicja IBSS- wyżej

13. Uwierzytelnienie Opensystem i SharedKey

Uwierzytelnienie
OpenSystem (otwarty system) – krótka sekwencja, każda stacja jest akceptowana. Jest to jedyny typ uwierzytelnienia wymagany standardem. Mimo iż metoda może być używana w połączeniu z WEP w celu poprawy bezpieczeństwa połączenia, ramki odpowiedzialne za autentykacje przesyłane są nieszyfrowanym tekstem.

SharedKey (klucz współdzielony)
Pierwsze implementacja zakładała użycie klucza WEP (Wired Equivalent Privacy).
Stacja aby została zaakceptowana musi zaszyfrować przy pomocy algorytmu RC4 z użyciem otrzymanego inną drogą klucza ciągu znaków „ChalangeText" jeżeli punkt dostępowy odtworzy tekst źródłowy przy pomocy klucza przechowywanego u siebie stacja jest akceptowana. WEP zapewnia zarówno poufność jak i autoryzację Obecnie Standard 802.11i oddziela autoryzację od zapewnienia poufności:

- Autoryzacja: np WPA - TKIP MIC; WPA2 – CCMP(AES), EAP/PEAP
- Poufność np TLS