

Sieci komputerowe – zajęcia, klasa 1

Spis treści

Urządzenia w sieci	2
Rodzaje sieci	6
Aplikacje sieciowe	6
Technologie w LAN/WAN	7
Działanie sieci komputerowej	7
Specyfikacje sieci	8
Topologie sieciowe	9
Domena kolizyjna/rozgłoszeniowa	10
Model ISO/OSI	12
Warstwy	13
NAT/ARP	29
Sieć WLAN	31
Kontrolery sieci	34
Programy do diagnozowania sieci/sniffery	37

Sieć komputerowa – zespół urządzeń i komputerów połączonych za pomocą medium.

Urządzenia:

Stacja robocza – komputery, które są podłączone do sieci; na nich zainstalowane są aplikacje sieciowe. Komputery pracują na wszystkich warstwach ISO/OSI.

Karta sieciowa – (NIC) Network Interface Controller, urządzenie umożliwiające podłączenie się do sieci. Jeśli karta podpięta jest od płyty głównej to komunikuje się z nią poprzez połączenie równoległe. Karta w PC zawiera 2 interfejsy:

- a) Interfejs do skrętki/koncentryka/powietrza
- b) Interfejs do połączenia z komputerem: ISA, PCI, USB.

Jak sprawdzić, w jakim trybie pracuje karta sieciowa?: menadżer urządzeń -> karty sieciowe -> właściwości -> speed and duplex -> autonegotiation. Full duplex – transmisja odbywa się w obu kierunkach, half – tylko naprzemiennie co powoduje spadek transferu. Obecnie karty sieciowe mają własny procesor i RAM pełniący funkcję buforu, gdy nie jest w stanie przetworzyć napływających danych.

Karty sieciowe w konfiguracji routerów to tak naprawdę interfejsy, za pomocą których łączymy urządzenia sieciowe. Karty sieciowe zawierają 48 bitów po to by uniknąć błędów w transmisji danych.

Poniżej karta sieciowa dla światłowodów:

Na rysunku przedstawiona jest karta

- A. kontrolera RAID
- B. kontrolera SCSI
- C. sieciowa Token Ring
- D. sieciowa Fibre Channel



Adres MAC – jest zapisany na stałe w chipie urządzenia (ROM) tj. w karcie sieciowej, routerze, PC, switchu, serwerze i telefonie. MAC jest jak adres na kartce pocztowej. Adres ten zawiera 48 bitów, pierwsze 24 to nazwa producenta a kolejne 24 to unikatowy numer karty. Gdyby mogłyby pojawiły się 2 karty sieciowe o takim MAC-u spowodowałoby to błędy w transmisji. Jak sprawdzić adres MAC – ipconfig/all w CMD. Producenta karty sieciowej można sprawdzić na: www.standards.ieee.org/regauth/oui/oui.txt. do zmiany adres MAC na karcie służy program Etherchange.

Modem – wyodrębnia dane internetowe dla użytkownika sieci. Służy do połączenia komputerów przez sieć telefoniczną bądź kable miedziane. Modem zamienia sygnał analogowy od dostawcy Internetu na sygnał cyfrowy dla użytkownika. Modemy stosuje się w sieciach telewizji kablowej i telefonii komórkowej np. 3G, 4G. Dawniej, połączenie następowało poprzez wybranie odpowiedniego numeru telefonicznego i zalogowanie się do usługi przy użyciu protokołu PPP. Klient otrzymywał tymczasowy adres IP.

Most (bridge) – urządzenie o 2 portach, mające za zadanie łączenie ze sobą domen kolizyjnych. Umożliwia zwiększenie rozpiętości sieci lokalnych. Działa w warstwie fizycznej, lecz zapamiętuje adresy MAC - na podstawie adresu MAC most podejmuje decyzję czy przesłać go do innego segmentu sieci czy go zablokować. Mosty są urządzeniami przełączającymi – od przełącznika różnią się mechanizmem przełączania ramki. Most robi to programowo a przełącznik sprzętowo.

Serwer – komputer, który udostępnia zasoby w sieci. Powinien mieć dużą moc obliczeniową, bo jest duża liczba użytkowników. Wiele serwerów ma swoje backup serwery, bo w przypadku dużego przedsiębiorstwa brak komunikacji byłaby dotkliwa finansowo. Serwer nie zmienia ilości domen kolizyjnych w sieci. Wyróżniamy:

- serwery plików (w tym serwery bazodanowe i serwery aplikacji), gdzie klienci mają przestrzeń dysków twardych,
- serwery wydruków udostępniające drukarki do wspólnego użytkowania w sieci (wydruk następuje albo na zasadzie kto pierwszy ten lepszy lub wg ustalonego priorytetu),
- serwery komunikacyjne, które umożliwiają komunikację z innymi sieciami jak DNS, DHCP,
- serwery poczty (email),
- serwery webowe, na którym „stoją” strony internetowe,
- serwery bazodanowe.

Istnieją także serwery pośredniczące proxy, które pozwalają na przyspieszenie pobierania danych z Internetu a są one skonfigurowane na komputerze w sieci lokalnej. Zadaniem tego serwera jest buforowanie na dysku lokalnym stron WWW odwiedzanych wcześniej. Jeśli przeglądarka znajdzie uprzednio odwiedzone strony, nie wymaga to pobrania danych z Internetu. Jeśli strony nie ma w buforze, serwer proxy pobiera ją, zapisuje w buforze i udostępnia klientom w sieci, co skraca czas oczekiwania na dane. Mamy też możliwość ukrycia przed serwerem stron internetowych, adresu IP klienta. By skonfigurować serwer proxy na Edge należy: wejść w ustawienia -> system, otwórz ustawienia serwera proxy -> użyj serwera proxy (wpisz adres i nr portu)-> nie używaj serwera dla adresów lokalnych -> zapisz.

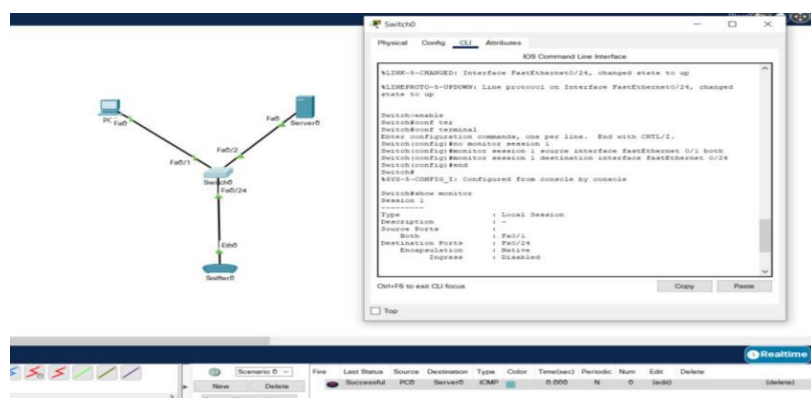
Switch/przełącznik– odpowiedzialny za przełączanie ramek z 1 stacji roboczej do 2, które umożliwiają komunikację w lokalnej sieci LAN. Stosowane są w topologii gwiazdy, głównie opartej na skrajce. Zwiększają rozpiętość sieci, bo mają więcej portów niż router. Przełączniki tworzą VLAN’y, by ograniczyć domenę rozgłoszeniową – separujemy wtedy np. działy w firmie, by łatwiej tym zarządzać.

Przełączniki filtrują też ruch w sieci. Trzy tryby pracy:

- cut-through gdzie ramka jest dzielona na porcie wchodzącym i składana w poprawnej kolejności na porcie wychodzącym,
 - straightforward, gdzie cała ramka jest przesyłana na raz co powoduje spadek przepustowości
- Przełączniki zarządzalne mają własny system operacyjny, którego pracę i parametry możemy konfigurować. Nowe przełączniki działają w warstwie 3 jak routery, definiują reguły ruchu sieciowego (ACL), load balancing, QOS, Spanning Tree (nadmiarowe połączenia pomiędzy przełącznikami).

Jeśli administrator chce monitorować cały ruch w sieci może na przełączniku skonfigurować usługę port mirroring, który może dotyczyć wybranych portów przełącznika lub wybranych sieci wirtualnych.

Poniżej schemat monitorowania portów na przełączniku:



Hub – przekazuje sygnał na swoje porty, nie ma możliwości przeglądania otrzymywanych treści, nie dzieli na odrębne domeny kolizji, lecz ogranicza do 1, co sprawia, że sieć jest niestabilna. Warstwa pierwsza ISO/OSI.

Koncentrator to wieloportowy wzmacniacz i rozdzielacz sygnału. Są koncentratory aktywne (regenerują sygnał) i pasywne (nie regenerują sygnału). Regeneruje kształt sygnału np. amplitudy przed transmitowaniem go dalej. Wymiana koncentratorów na przełączniki w sieci Ethernet spowoduje zmniejszanie ilości kolizji.

Router (warstwa 3, 2 i 1) – to swego rodzaju komputer posiadający procesor, pamięć operacyjną i system. Router ma 4 rodzaje pamięci: RAM (pliki bieżącej konfiguracji, tablica routingu, bufor ARP), ROM (instrukcje rozruchowe, instrukcje diagnostyczne, uproszczona wersja systemu Lite IOS), NVRAM (przechowuje plik konfiguracji startowej), Flash (obraz systemu, który podczas startu kopiowany jest do RAM-u).

Routery tworzą sieci i umożliwiają komunikację w sieci lokalnej i rozległej. Jego zadanie to odnajdywanie najlepszych tras. Łączą one niezależne sieci i przesyłają pakiety lub datagramy. Router jest oknem na świat tj. **bramą domyślną** WAN z LAN. Router służy też do obrony LAN przed atakami sieci WAN (m.in. jako zaporą) oraz poprzez NAT – mechanizm, który ukrywa nasz adres IP i zamienia go na publiczny. Jest urządzeniem pozwalającym na sterowanie przepustowością sieci, oddziela domeny kolizji i domeny rozgłoszeniowe – router tworzy tyle domen rozgłoszeniowych, ile posiada interfejsów. Zapewnia zestawienie bezpiecznych kanałów połączeń (VPN) poprzez Internet – kanał jest szyfrowany i zapewnia prywatność komunikacji. Router posiada 5 interfejsów wirtualnych.

Routery zawierają porty konsolowe do konfiguracji, port aux jako pomocniczy, porty jako interfejsy oraz serialowe porty WAN jako kabel serialowy DB60 (karta WIC oraz HWIC, HWIC2). Kable serialowe do wyboru to DTE (urządzenia zamieniające sygnał po stronie klienta (routery), zamieniają sygnał usługodawcy na sygnał w naszej sieci LAN) i DCE, który zamienia sygnał z naszego routera na odpowiednią technologię, którą oferuje nam dostawca sieci WAN.



Routery zawierają tablice routingu tj. informacje o sieciach podpiętych bezpośrednio do routera (oznaczone literą C w CLI) oraz o sieciach zdalnych, które nie są do niego podłączone, ale router zna ich trasy (literka R w CLI), oraz S jako sieć zdalna wskazana przez nas statycznie/ręcznie wpisana. Tablica routingu jest uzupełniania ręcznie lub dynamiczny z wykorzystaniem protokołu routingu statycznego lub dynamicznego.

Regenerator/repeater – urządzenie aktywne służące do wzmacniania i naprawiania zniekształceń sygnałów w sieci. Nie wprowadza żadnych zmian logicznych w przesyłane sygnały. Działa na poziomie warstwy fizycznej.

Rodzaje sieci:

LAN – budowana w większości na switchach, mały zasięg geograficzny, router brzegowy łączy z WAN. Grupa PC połączona w jednym pokoju lub budynku.

WAN – rozległa sieć, budowana na routerach, duży zasięg geograficzny, łączy wiele sieci LAN w jedną całość. Technologie w WAN to frame relay, ISDN (dane i głos), DSL.

MAN – Metropolitan Area Network, sieć miejska, łącząca LAN na obszarze 1 miasta. Sieci te umożliwiają połączenia między sieciami lokalnymi uczelni, organów administracji.

PAN – sieć prywatna, do 10m, głównie oparta na bluetooth.

Intranet – sieć w obrębie 1 przedsiębiorstwa.

Domowa sieć komputerowa (SOHO) – działają jako lokalne sieci komputerowe dla małych firm i domowych biur, umożliwiające urządzeniom komunikację i współdzielenie zasobów, takich jak drukarki, skanery czy dostęp do internetu. Zazwyczaj wykorzystują centralny router lub koncentrator do łączenia urządzeń przewodowych lub bezprzewodowych

Ze względu na rodzaj komunikacji sieci możemy podzielić na peer to peer (brak scentralizowanego serwera administratora, każdy jest jednocześnie klientem i serwerem) oraz klient-serwer, gdzie rolę nadrzędną odgrywa 1 serwer.

Aplikacje sieciowe:

- przeglądarka internetowa, - email, - gry komputerowe, - wymiana plików (FTP, TFTP),
- skype, google meet, teams

Dokumenty RFC (request for comment) – informacje o urządzeniach i protokołach sieciowych. Bazę wszystkich dokumentów RFC znajdziesz pod adresem <https://www.rfc-editor.org>.

Technologie stosowane w sieciach komputerowych:

- **Ethernet:** opiera się o metodę CSMA/CD opartą o rywalizację o dostęp do nośnika, mogą występować kolizje wtedy, gdy stacje nadają w tym samym czasie,
- **Token Ring:** stacje sieciowe tworzą jeden pierścień, stacja robocza uzyskuje dostęp tylko wtedy, gdy ma pierścień. Jeśli ramka jest uszkodzona to jest usuwana – nie próbuje się jej retransmitować, a jeśli już to robią to urządzenia końcowe (komunikacja bank->klient)
- **FDDI:** podwójny pierścień oparty na światłowodzie.
- **Frame Relay** – działa poprzez dzielenie danych na ramki i przesyłanie ich przez sieć opartą na wirtualnych obwodach, gdzie przełączniki wybierają dynamicznie ścieżkę.
- **DSL** – Digital Subscriber Line, cyfrowa linia abonencka wykorzystująca sieci telefoniczne i kable miedziane do 80 Mb/s. Symetria łącza – użytkownik generuje większy ruch u siebie (downstream) niż od siebie (upstream). Technologie te zapewniają też większe pasmo przy pobieraniu danych z Internetu a mniejsze przy wysyłaniu.
DSL ma wiele podgrup np. ADSL, ADSL-1, ADSL-2+ (zapewnia dostęp do Internetu oraz odbiór cyfrowych kanałów telewizyjnych), ADSL -3, RADSL. Ważną funkcją jest użycie tzw. splittera, który jest filtrem rozdzielającym pasmo na częstotliwości poniżej i powyżej 4 kHz.
- ATM** – szerokopasmowa technologia używana do transmisji głosu i sygnału, w dużych sieciach MAN i WAN. Nie bazuje na 1 warstwie ISO/OSI więc wykorzystuje sieci oparte na wszystkich nośnikach/mediach transmisyjnych. Komórki (dane w ATM) wysyłane są bez ustalonego porządku i mogą mieć różną szybkość. Połączenia są tylko logiczne. Sieci ATM nie dokonują poprawności przesyłania danych. Sieci ATM trasują wykorzystując routery rozproszone oraz protokół OSPF (open shortest path first).
- **HFC** jest technologią służącą do wykorzystywania Internetu wraz z telewizją kablową, gdzie wykorzystywany jest kabel światłowodowy lub koncentryk.

Działanie sieci komputerowej

Podstawą sieci komputerowych również jest system binarny – przesyłane odbywa się przy użyciu różnych technologii, np. światłowodowo lub radiowo, lecz zawsze na samym końcu swojej drogi zamieniane na 0 i 1. Pojedynczy znak to 1 bajt informacji (wielkość pliku), 1 bajt to 8 bitów, znak „C” to 8 bitów informacji, słowo CISCO to 5 bajtów (40 bitów), kilobajt to 1024. Prędkość sieci mierzy się w kilobitach i megabitach. Jeśli dla przykładu chcesz zamienić np. 20 kB/s na 20 kb/s, wystarczy 20 kB/s pomnożyć przez 8. Wynik to 160 kb/s.

Ćwiczenie: 4500 MB, ile to GB? **Odpowiedź** 4500 MB/1024 = 4,39 GB

Ćwiczenie: 6 GB, ile to MB? **Odpowiedź** 6 GB×1024 = 6144 MB

Przesyłanie danych w sieci

W transmisji biorą udział cztery urządzenia sieciowe (dwie karty sieciowe, przewód, przełącznik), mimo to sieć charakteryzuje pięć istotnych parametrów, które mają bezpośrednio wpływ na przesyłanie danych. Oto one:

- pasmo, max. ilość informacji jaką można przesłać przez medium sieciowe, kabel miedziany 100Mb/s, światłowód 10Gb/s.
- przepustowość, jaką ilość info możemy przesłać przez sieć w danym momencie,
- transfer, ile czasu potrwa przesłanie danych przez łącze (Mb/s),
- opóźnienie, ile będziemy czekać aż dane dotrą (milisekundy),
- dostępność, czy użytkownik może korzystać z zasobów.

Sieci posiadają łącza symetryczne, gdzie przepustowość wysyłania i pobierania jest jednakowa oraz łącza asymetryczne, gdzie przepustowość kanału pobierania jest większa.

Transfer:

Istotną sprawą jest użycie odpowiednich jednostek miary. Pamiętaj, że pasmo mierzone jest np. w megabitach (Mb), a rozmiar pliku w większości przypadków podawany jest w megabajtach (MB). Przed rozpoczęciem obliczeń zamień megabajty na megabity, mnożąc liczbę megabajtów przez 8 (np. $2 \text{ MB} \times 8 = 16 \text{ Mb}$). Aby obliczyć czas transferu, skorzystaj z następującego wzoru: $T = RP / P$, gdzie: T — to czas transferu, RP — to rozmiar pliku, P — to pasmo.

Założmy, że chcesz przesłać plik wielkości 2 MB przez łącze o paśmie 1,54 Mb/s. Najpierw należy zamienić MB na Mb. Mnożę więc $2 \text{ MB} \times 8$. Otrzymuję 16 Mb. $T = 16 \text{ Mb} / 1,54 \text{ Mb}$
Zaokrąglając otrzymuję czas 10 sek.

Ćwiczenie: Ile czasu potrzeba na wysłanie pliku o wielkości 12 MB, jeśli pasmo sieci wynosi 2 Mb/s? **Odpowiedź** $12 \text{ MB} \times 8 = 96 \text{ Mb/s}$, $96 \text{ Mb/s} : 2 \text{ Mb/s} = 48$ (sekund).

Ćwiczenie: Jaką ilość danych można przesłać w czasie 1s przez łącze synchroniczne o przepustowości 512 kbps, bez sprzętowej i programowej kompresji? Około 55 kB.

Specyfikacje sieci komputerowych:

IEEE 802.3 - 10Mb Ethernet

IEEE 802.3u – 100 Mb Ethernet

IEEE 802.3x – Full Duplex Ethernet

IEEE 802.3z – 1Gb Ethernet

IEEE 802.5 – Token Ring

IEEE 802.11 – Wireless LAN

IEEE 802.12 - 100 VG-AnyLAN

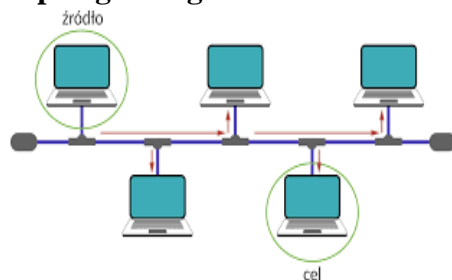
IEEE 802.14 – Cable Modem

Topologie sieciowe

Topologia fizyczna zwykle określa sposób rozmieszczania kabli, urządzeń sieciowych i innych urządzeń sieci (geometryczna organizacja sieci). Po stworzeniu, sieć LAN powinna mieć dokumentację zawierającą plan połączeń nałożony na plan budynku wraz z numeracją gniazdek sieciowych oraz protokół z pomiarów dokonanych na wszystkich gniazdkach.

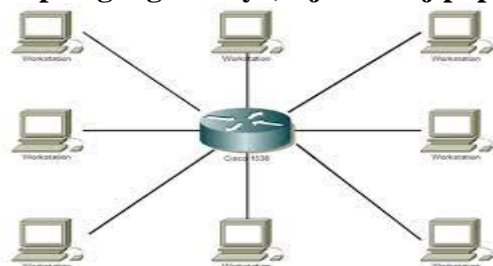
Topologia logiczna prezentuje sposób działania sieci na poziomie logiki. Pokazuje więc, w jaki sposób urządzenia pracujące w sieci będą się ze sobą komunikować, jakie dane wysyłać i za pomocą jakiej technologii.

Topologia magistrali



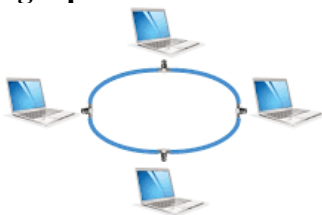
W tej topologii wszystkie urządzenia połączone są ze sobą przy użyciu kabla (najczęściej koncentrycznego). W topologii tej można zauważyć główny przewód, do którego podłączone są pozostałe komputery (węzły dołącza się do wspólnej magistrali za pomocą trójników). Ten przewód zwany jest magistralą. Topologia magistrali (*bus topology*) wymaga ograniczonej ilości kabla; jest dość prosta w instalacji i późniejszej rozbudowie, nie wymaga montowania przełączników. Jej wadą jest to, że podczas awarii kabla trudno zdiagnozować problem. Oba końce magistrali muszą być zakończone elementami ograniczającymi, tzw. terminatorami – chroniącymi przed odbiciami sygnału.

Topologia gwiazdy (najbardziej popularna)



W topologii gwiazdy każdy komputer podłączony jest do głównego punktu, jakim może być przełącznik, koncentrator lub inne urządzenie sieciowe. Sieci oparte na topologii gwiazdy są bardzo łatwo skalowalne. Zaletą topologii gwiazdy jest możliwość szybkiego zdiagnozowania uszkodzenia, np. kabla lub komputera. Zarówno uszkodzenie pojedynczego komputera, jak i dołączenie nowego nie mają wpływu na pracę innych urządzeń pracujących w sieci. Wadą stosowania topologii gwiazdy jest centralne miejsce, do którego podłączane są komputery. W przypadku jego awarii cała sieć nie może pracować. Najczęściej w tej topologii używany jest kabel dwużyłowy – skrętka.

Topologia pierścienia

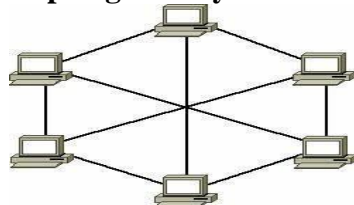


W topologii pierścienia każdy komputer połączony jest z kolejnym, tworząc tzw. pierścień. Komunikacja w sieciach tego typu polega na przekazywaniu pakietu tylko w jednym kierunku. W topologii pierścienia wszystkie komputery mają równy dostęp do nośnika, mogą nadawać wyłącznie w momencie otrzymania znacznika. Niweluje to powstawanie kolizji pakietów w sieci. Wyróżniamy pierścień pojedynczy i pierścień podwójny. Najczęściej

wykorzystywany jest tu światłowód. Przykładem topologii pierścienia jest technologia token ring – przekazywany żeton jest od stacji do stacji (jak ma żeton to wtedy nadaje), w 1 chwili może nadawać tylko 1 stacja – nie występują więc kolizje. Żeton pełni swego rodzaju funkcję przekazywanej ramki.

Technologia FDDI również mieści się w obrębie topologii pierścienia. Są to 2 pierścienie światłowodowe, ruch odbywa się w przeciwnych kierunkach. Jednocześnie używany jest tylko 1 z pierścieni, a 2 odgrywa rolę połączenia awaryjnego. Rozpiętość do 200km.

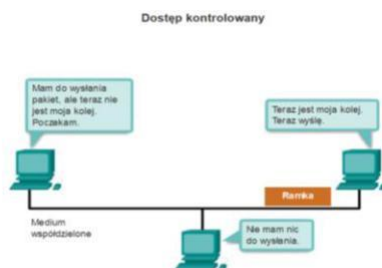
Topologia kraty



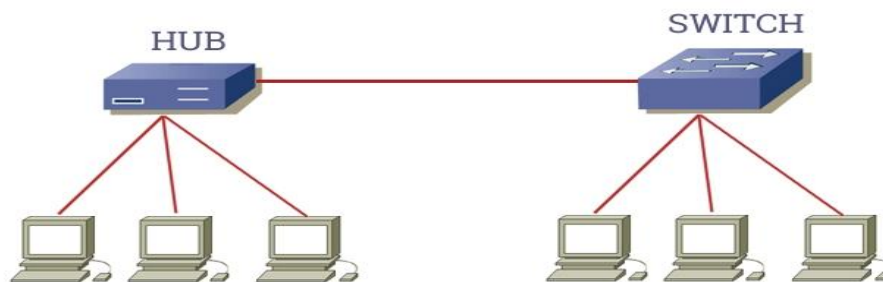
Topologia kraty (*grid topology*) oparta jest na wykorzystaniu łączy nadmiarowych. Każdy komputer pracujący w topologii kraty połączony jest z każdym innym. Takie rozwiązanie ma kilka zalet, z których najważniejszą jest duża odporność sieci na awarię. Wadą stosowania tego typu rozwiązania jest duży koszt, związany z zakupem kabla oraz urządzeń sieciowych.

Domena kolizyjna

Domena kolizyjna to logiczny obszar sieci komputerowej, w którym może dojść do kolizji pakietów danych nadawanych współbieżnie przez różne stacje. Aby zapobiec całkowitemu chaosowi w medium, stosowana jest metoda Carrier Sense Multiple Access (CSMA), która najpierw wykrywa, czy medium aktualnie przenosi sygnał. Jeżeli wykryty zostanie sygnał przesyłany przez medium, to oznacza, że inne urządzenie przesyła dane. Wtedy urządzenie chcące wysłać dane stwierdzi, że medium jest zajęte i odczeka ono pewien krótki przedział czasu zanim ponowi próbę wysłania danych. Jeżeli urządzenie nie wykryje sygnału, to rozpocznie przesyłanie danych. Ethernet i sieci bezprzewodowe używają metody dostępu do medium opartej na rywalizacji. Domenę kolizyjną eliminuje full-duplex. Możliwe jest, że proces CSMA nie zadziała i dwa urządzenia będą jednocześnie transmitować dane, co spowoduje kolizję. Jeśli to nastąpi, to dane przesyłane przez oba urządzenia wzajemnie się zakłócą i będą wymagały ponownego przesłania.



Poniżej schemat sieci gdzie występują 4 domeny kolizyjne:



Metoda CSMA w połączeniu z metodą rozwiązywania konfliktów połączenia z medium to metoda, która jest najczęściej stosowana. Obecnie stosowane są te dwie metody:

- **Wielodostęp z wykrywaniem nośnej i wykrywaniem kolizji (CSMA/CD):**
Urządzenie końcowe monitoruje medium w celu wykrycia obecności sygnału danych. Jeżeli medium jest wolne (nie wykryto obecności sygnału danych), to urządzenie zaczyna transmitować dane. Jeżeli podczas nadawania urządzenie wykryje sygnał, który jest

nadawany przez inne urządzenie, to wszystkie nadające urządzenia zaprzestają transmitować i próbują wysłać ramkę później. Metoda ta jest używana w sieciach Ethernet.

- **Wielodostęp z wykrywaniem nośnej i unikaniem kolizji - (CSMA/CA):** Urządzenie końcowe sprawdza medium w celu wykrycia obecności sygnału danych. Jeżeli medium jest wolne, to urządzenie chcące nadawać wysyła krótką informację do medium, że chciałoby użyć tego medium. Po otrzymaniu potwierdzenia o braku zajętości medium urządzenie wysyła dane. Metoda ta jest używana w sieciach bezprzewodowych 802.11.

Media Access Control

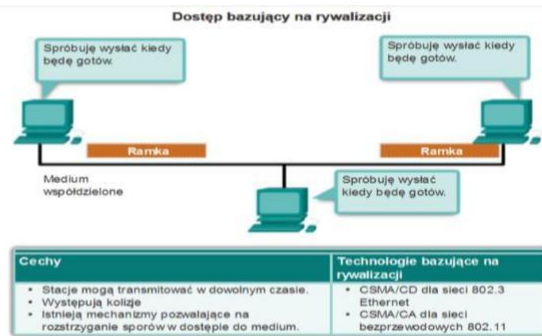
Topologie LAN

obecności sygnału danych. Jeżeli medium jest wolne (nie wykryto obecności sygnału danych), to urządzenie zaczyna transmitować dane. Jeżeli podczas nadawania urządzenie wykryje sygnał, który jest nadawany przez inne urządzenie, to wszystkie nadające urządzenia zaprzestają transmitować i próbują wysłać ramkę później. Metoda ta jest używana w sieciach Ethernet.

- **Wielodostęp z wykrywaniem nośnej i unikaniem kolizji - (CSMA/CA):** Urządzenie końcowe sprawdza medium w celu wykrycia obecności sygnału danych. Jeżeli medium jest wolne, to urządzenie chcące nadawać wysyła krótką informację do medium, że chciałoby użyć tego medium. Po otrzymaniu potwierdzenia o braku zajętości medium urządzenie wysyła dane. Metoda ta jest używana w sieciach bezprzewodowych 802.11.

Na rysunku przedstawiono:

- Jak działają metody dostępu oparte na rywalizacji.
- Właściwości metod dostępu wykorzystujące rywalizację
- Przykłady metod dostępu wykorzystujące rywalizację

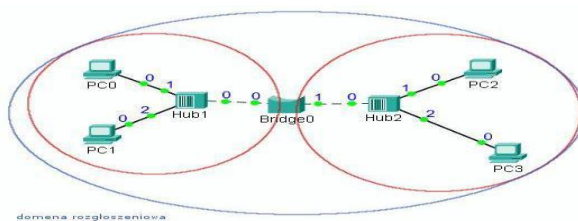


Kontrola dostępu – CSMA/CA.

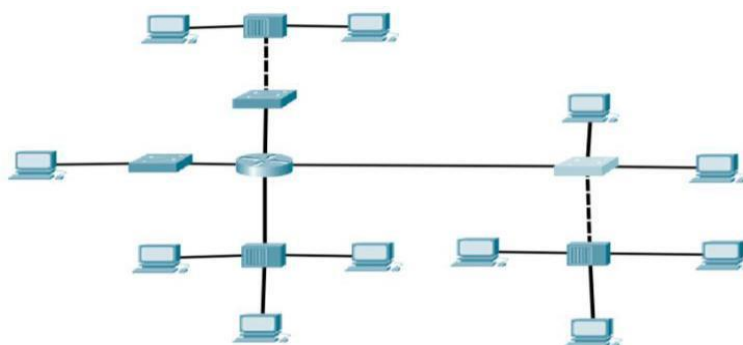
W sieciach WLAN nie jest możliwe stosowanie CSMA/CD (stosowanego w sieciach Ethernet) - stacja nie może równocześnie prowadzić nasłuchu, gdyż jej własny sygnał mógłby je zagłuszyć.

CSMA/CA – stacja prowadzi nasłuch pasma -> jeśli nie wykryje transmisji przełącza się w tryb gotowości do nadawania i czeka -> jeśli nikt nie nadaje stacja rozpoczyna transmisję. Dla każdej przesłanej ramki do nadawcy musi dotrzeć potwierdzenie poprawności otrzymania ACK.

Domena rozgłoszeniowa - (broadcast domain) - logiczny obszar sieci komputerowej, w którym dowolne urządzenie podłączone do sieci może bezpośrednio dokonać transmisji danych do dowolnego innego urządzenia w obrębie domeny bez routera. Domenę rozgłoszeniową można ograniczyć tworząc vlan na switchu co sprawi, że ruch sieciowy będzie zawężony to konkretnego VLAN-u.



Poniższy schemat zawiera 4 domeny rozgłoszeniowe i 9 domen kolizyjnych:



Model OSI/ISO – model referencyjny, składający się z 7 warstw (poniżej), międzynarodowy standard, pozwala nam zrozumieć proces przesyłania i otrzymywania danych w sieci, ale również do tego by gdy zajdzie błąd w komunikacji urządzeń w sieci go zidentyfikować i usunąć. Z punktu widzenia sieci komputerowych warstwy aplikacji, prezentacji oraz sesji są w zasadzie nieistotne i nie mają wpływu na komunikację sieciową.

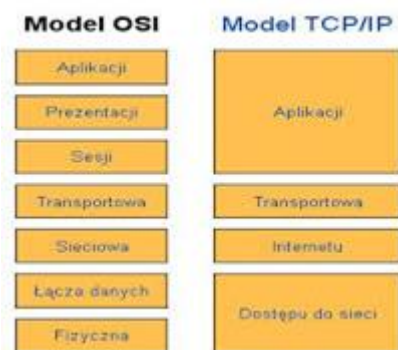
Model TCP/IP nie jest tylko modelem i pojedynczym protokołem, lecz pakietem protokołów. Dodatkowe informacje możesz odszukać w RFC1180. Składa się z czterech warstw, z których każdą można powiązać z modelem ISO/OSI (poniżej).

Proces przechodzenia danych od klienta do serwera przez poszczególne warstwy od 7 do 1 nazywa się enkapsulacją. Proces, który odbywa się po drugiej stronie, czyli w tym przypadku po stronie serwera, nazywa się dekapulacją. Oznacza on przejście danych z warstwy 1 w górę do warstwy 7.

Najważniejsze momenty procesu enkapsulacji (od warstwy 7 do 1):

1. Utworzenie segmentu z numerami portów (TCP lub UDP) — WARSTWA 4.
2. Utworzenie pakietu, przypisanie adresów IP do pakietu — WARSTWA 3.
3. Utworzenie ramki z adresami MAC źródłowym i docelowym — WARSTWA 2.
4. Przesłanie danych przez fizyczne medium w postaci 0 i 1 — WARSTWA 1.

Poniżej opis warstw uczestniczących w procesie enkapsulacji i dekapulacji.



Opis problemów typowych dla warstw:

WARSTWA

OPIS PROBLEMU

APLIKACJI

niska przepustowość, nakładanie się czytania i zapisu plików, obciążenie klienta i serwera z powodu dużego przeszukiwania plików,

PREZENTACJI

różne odmiany tego samego protokołu

SESIJ

ponowne ustanawianie połączenia, problem DNS

TRANSPORTOWA

ponowne transmisje, zgubione fragmenty,

SIECIOWA

błędy nagłówka IP, sumy danych, problem z adresowaniem, zgubione pakiety, sztormy rozgłoszeniowe

ŁĄCZA DANYCH

błędy CRC ramek, kolizje i krótkie pakiety, uszkodzenie danych w przełącznikach, sztormy rozgłoszeniowe

FIZYCZNA

złe okablowanie, zewnętrzne zakłócenia RFI

Warstwa aplikacji

Warstwa aplikacji (*application layer*) jest najbliższa użytkownikowi i dostarcza wszystkie te usługi, które może on zobaczyć. Odpowiada za usługi sieciowe, aplikacje użytkownika (drukowanie, edytory itd.) i przeglądarki internetowe. Warstwa aplikacji odpowiedzialna jest za interfejs użytkownika. Konfigurację interfejsu sieciowego w systemie Linux można wykonać, edytując plik `/etc/network/interfaces`

FTP lub SFTP (*File Transfer Protocol*) (RFC959) — umożliwia przesyłanie oraz odbieranie plików ze zdalnych komputerów, na których została zainstalowana usługa FTP oraz np. zmianę praw dostępu – możliwy jest anonimowy dostęp. Protokół FTP używa portów o numerach 20 oraz 21. W praktyce możesz uruchomić usługę serwera FTP i za jej pomocą udostępnić określone foldery lub pliki. Użytkownik pracujący w innym miejscu sieci, używając **klienta FTP**, czyli oprogramowania, które umożliwia połączenie się z serwerem FTP, pobiera udostępnione pliki. FTP pracuje w tryb pracy aktywnym i pasywnym (pasywny jest prawie zawsze używany przez przeglądarki WWW, połączenia nawiązywane od klienta do serwera, co rozwiązuje problem ochrony klientów przez firewall). Problem z trybem aktywnym – firewall klientów uniemożliwia kontakt z FTP oraz problem z przechodzeniem takich połączeń przez NAT. Tryb pasywny jest gorszy ze względów bezpieczeństwa – musi on otworzyć wszystkie porty zamiast tylko tych używanych. Popularnym klientem FTP jest program FILEZILLA. FTP transmituje pliki w trybie tekstowym i binarnym.

FTP serwer sprawdza tożsamość klienta za pomocą loginu i hasła przesłanego otwartym tekstem. FTP nie przysyła poszczególnych bitów, ale od razu operuje na całych plikach, które można usuwać, zmieniać nazwy, zmieniać bieżące katalogi.

Do kopiowania plików między urządzeniem a komputerem służy także protokół TFTP. By zainstalować serwer TFTP należy go pobrać ze strony: http://tftpd32.jounin.net/tftpd32_download.html Później pobieramy plik instalacyjny serwera: `Tftpd64-4.62-setup.exe`. Po instalacji uruchamiamy program i wybieramy „server interfaces”, -> settings -> global (pozostawić tylko TFTP) -> w zakładce TFTP wskazać katalog główny usługi (do tego katalogu będą kopiowane pliki).

HTTP (*Hyper Text Transfer Protocol*) (RFC2616) — dzięki współpracy z siecią WWW (*World Wide Web*) umożliwia przeglądanie stron internetowych. Klient wyposażony w przeglądarkę internetową może połączyć się z serwerem i przeglądać zawartość strony www. Popularnymi serwerami http jest Apache i Microsoft IIS. Apache działa na licencji opensource, obsługuje SSL, można zarządzać pasmem, śledzić sesję przez cookies, moduł proxy.

DHCP (*Dynamic Host Configuration Protocol*) (RFC2131) — służy do automatycznej konfiguracji protokołu TCP/IP w systemie operacyjnym. Przydziela automatycznie adresy IP oraz inne ustawienia pracującym w sieci komputerom. Serwer DHCP działa na porcie 67. i przydziela automatycznie ustawienia klientowi działającemu na porcie o numerze 68. DHCP to protokół klient-serwer zapewniający automatyczną konfigurację parametrów sieciowych (adres IP, maska, adres bramki) stacji roboczej, na podstawie adresu MAC każdej stacji. DHCP może przydzielać adresy przez określony czas, a w momencie, gdy adres zostanie zwolniony, otrzyma go kolejny klient. DHCP umożliwia hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP bramy sieciowej.

Proces uzyskiwania konfiguracji: klient przechodzi przez kilka etapów:

- DHCPDISCOVER – odkrywanie istniejących serwerów, pakiet rozgłoszeniowy,
- DHCPOFFER – serwer odpowiada, oferując konfigurację w wysłanym pakiecie, zawarty jest w tym czasie dzierżawy przydzielonego adresu IP,
- DHCPREQUEST – przyjęcie oferty serwera, zapamiętanie serwera, odnawianie czasu dzierżawy,
- DHCPACK – potwierdzenie wpisania klienta do bazy serwera,
- DHCPRELEASE – zwolnienie adresu IP.

W sieciach dążymy do zminimalizowania adresów IP: np. pracownia w szkole ma 1 adres a tam pula adresów jest przydzielana dynamicznie na inne hosty.

SMTP (*Simple Mail Transport Protocol*) (RFC2821) — służy do przesyłania poczty elektronicznej, wyłącznie w postaci tekstowej. Najczęściej działa razem z protokołem POP3.

Do komunikacji wykorzystuje port numer 25. Określany jest często jako serwer poczty wychodzącej. Protokół ten umożliwia wysyłanie i odbieranie poczty przez różne środowiska systemowe. Klient wysyła zapytanie do serwera, odpowiada najpierw serwer domenowy DNS a potem serwer SMTP. Przykładem spełniającym funkcje serwera SMTP jest Exchange firmy Microsoft – służy on często do pracy grupowej i wysyłania poczty, zawiera system przechowywania danych, ma możliwość telekonferencji. Do korzystania z Exchange potrzebny jest dedykowany, płatny system.

POP3 (*Post Office Protocol*) (RFC1939) — używa portu 110. i jest odpowiedzialny za odbieranie poczty elektronicznej. Odebranie poczty wymaga zalogowania się do serwera, podania nazwy użytkownika i hasła – w przeciwieństwie do SMTP. Do sprawdzania serwera POP3 służy telnet.

IMAP – port 143, protokół dzięki któremu odbieramy pocztę z serwera, ma bardziej rozbudowane możliwości niż POP3. Umożliwia przechowywanie wiadomości na serwerze i podzielenie ich na różne foldery, dzięki czemu użytkownik logując się ma dostęp do całej swojej skrzynki pocztowej (ma ją skopiowaną lokalnie). Do sprawdzenia komunikacji z serwerem również służy telnet.

SSL (*Secure Sockets Layer*) — umożliwia korzystanie z szyfrowanej komunikacji pomiędzy klientem a serwerem. Wykorzystuje port 443. Jest to zestaw algorytmów wykorzystywanych do bezpieczeństwa. Algorytmy szyfrowania dzielą się na symetryczne (używany jest ten sam klucz szyfrujący) i asymetryczne (używane są różne klucze publiczne, znając klucz nie możemy odszyfrować wiadomości). SSL jest kojarzony z http, Telnetem, SMTP, POP i IMAP.

Telnet – protokół terminalu sieciowego, służy do zalogowania się i zdalnej pracy na odległym komputerze z wykorzystaniem konsoli tekstowej. Telnetu nie należy używać na naszych systemach, bo transmisja odbywa się bez żadnego kodowania. Jeśli ktoś podsłucha transmisję, to uzyska login i hasło do naszego serwera. Lepszy jest SSH. Do czego praktycznie potrzebujemy telnet? Z chwilą, gdy nie mamy fizycznie routera przy sobie, możemy się do niego dostać z hosta. Telnet służy więc do zarządzania przełącznikami i routerami.

SSH – jest bezpiecznym protokołem udostępniającym usługi szyfrowania i pracującym na porcie 22. SSH dostarcza technologię TCP/IP port forwarding technologii przekierowywania niechronionych połączeń przez chroniony kanał, jak w SSL – możemy stworzyć kodowany kanał pomiędzy dowolnymi komputerami w Internecie, transportujący dane, które chcemy chronić.

SNMP – służy do zarządzania i monitorowania urządzeń sieciowych (przełączniki, routery, serwery, modemy, drukarki). Jest to protokół typu klient-serwer, definiowany jako protokół menadżer-agent. Agent (serwer) działa na obsługiwanym urządzeniu i monitoruje stan urządzenia. Menedżer (klient) wysyła zapytania do agenta oraz odbiera od niego odpowiedzi. Wymieniane są tutaj informacje kontrolne pomiędzy urządzeniami sieciowymi.

DNS (*Domain Name System*) (RFC1034) — umożliwia odwzorowywanie nazwy na adres IP. Najważniejsza warstwa z punktu widzenia użytkownika, odwzorowuje nazwy hostów na adresy IP. **DNS** sprawia, że nie musimy zapamiętywać adresów IP tylko wpisujemy adres. System operacyjny najpierw sprawdza wpisy dokonane w plikach (katalog etc) a gdy ich nie znajdzie wysyła zapytanie do serwera świadczącego usługę DNS. DNS to baza danych, która także posiada informacje przekazywaniu poczty. Określa także format pakietów, pozwalających na komunikację między serwerami nazw oraz odpytywanie tych serwerów przez klientów. By wyczyścić bufor nazw domenowych w Windows należy zastosować polecenie ipconfig/ flushdns.

Polecenie: **netsh advfirewall firewall add rule name="Open" dir=in action=deny protocol=TCPlocalport =53** służy do blokowania usługi DNS opartej na protokole TCP.

Popularne serwery DNS to BIND oraz djbdns – można je pobrać ze stron twórcy. Jak sprawdzić adresy serwerów DNS – poprzez nslookup w CMD lub np. nslookup www.onet.pl:



```
Wiersz polecenia - nslookup
Microsoft Windows [Version 10.0.19042.685]
(c) 2020 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\user>nslookup
Default Server: funbox.home
Address: 192.168.1.1

> google.com.pl
Server: funbox.home
Address: 192.168.1.1

*** No Internet type for both IPv4 and IPv6 Addresses (AAAA) records available for google.com.pl
> google.com.pl
Server: funbox.home
Address: 192.168.1.1
```

ISDN – zintegrowane usługi sieci cyfrowej korzystającym ze struktury telefonicznej. Zawiera kanał B (dane klienta, umożliwia jednocześnie rozmowy telefoniczne i przeglądanie Internetu) i kanał D (informacje kontrolne).

PPP – Point to Point Protocol – zapewnia komutowane połączenia modemowe czyli wdzwanianego dostępu do Internetu oraz na łączach stałych. Jest to protokół bezpołączeniowy - nie potrzeba zatwierdzenia poprawności przesyłania danych. Spaja np. 2 routery – wspiera pracę warstwy łącza danych. Zapewnia synchronizację i asynchronizację, dokonuje autentykacji hasła routera, grupuje interfejsy WAN w jeden – razem z load balance, dzięki czemu przepustowość łącza wzrasta. PPP kompresuje dane, można ustawić procentową tolerancję błędów – jeśli próg zostanie przekroczony interfejs będzie zamknięty. PPP umożliwia komunikację 2 różnych protokołów np. IPV4 i IPV6. PPP służy też do spięcia routera CISCO z routerem innej firmy niż CISCO.

Warstwa prezentacji

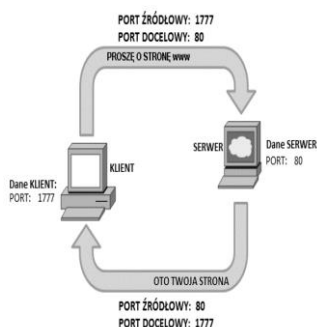
Warstwa prezentacji — jak sama nazwa wskazuje — odpowiada za prezentowanie danych w sieci. Pobiera dane z warstwy aplikacji i tłumaczy je na odpowiedni format. Jeśli to konieczne, dokonuje również szyfrowania lub kompresji. Jej celem jest doprowadzenie do tego, aby przekazywane dane miały wspólny format. Przykładowo w warstwie aplikacji ustala się, że w połączeniu dane zostaną przesłane w postaci plików jpg.

Warstwa sesji

Warstwa sesji jest odpowiedzialna za tworzenie sesji pomiędzy komputerami pracującymi w sieci oraz za zarządzanie sesją, jeśli zostanie nawiązana. Warstwa sesji kontroluje nawiązywanie i zrywanie połączenia przez aplikację. Warstwa sesji — poprzez wykorzystanie odpowiednich protokołów — udostępnia dwa rodzaje komunikacji: komunikację połączeniową oraz bezpołączeniową. W warstwie sesji występuje pewnego rodzaju ochrona przed koniecznością ponownej transmisji danych. Ochrona realizowana jest przez umieszczenie punktów kontrolnych. Podczas utraty sesji dane nie muszą być transmitowane od początku, ale od miejsca, w którym połączenie zostało zerwane.

Warstwa transportu

Warstwa transportu jest jedną z najważniejszych warstw całego modelu ISO/OSI. W warstwie transportu komunikacja przebiega na podstawie numerów portów. Każda aplikacja lub usługa sieciowa posiadają podczas działania swój unikatowy numer portu. Port źródłowy ma inny port niż docelowy, http ma 80.



Na rysunku można zobaczyć, że warstwa transportu wybrała port 80. jako docelowy oraz port 1777. jako źródłowy. Jeśli serwer odbierze „prośbę” o przesłanie strony www, wyśle ją do portu docelowego 1777., umieszczając w nagłówku również port źródłowy, czyli 80.

Zauważ, że jest już podany port docelowy, czyli wysłane dane mogą w tej postaci trafić do celu, jednak po jego osiągnięciu nie będą mogły wrócić, ponieważ nie został podany port źródłowy. Serwer może wysłać dane z powrotem do portu 80., ale co by się stało, gdybyś otworzył kilka stron www. Dane nie zawierają informacji, do jakiej przeglądarki mają wrócić. Port źródłowy musi więc być inny. Warstwa transportu wybiera port źródłowy z puli wolnych portów przeznaczonych do tego celu i umieszcza porty źródłowy oraz docelowy w nagłówku, następnie przesyła dane do niższej warstwy.

W warstwie transportowej mamy do czynienia z tzw. segmentem. Segment to coś w rodzaju pudełeczka, do którego są wrzucane przesyłane dane. Następnie pudełeczko jest adresowane, czyli opatrywane numerami portu źródłowego (nadawcy) oraz docelowego (odbiorca). Na końcu jest wysyłane do warstwy niżej, czyli warstwy sieci (warstwy 3).

W tej warstwie jest podejmowana decyzja, w jaki sposób dane zostaną wysłane, czyli czy jako TCP czy UDP. Wybór następuje pomiędzy dwoma protokołami **TCP** oraz **UDP**.

TCP (*Transmission Control Protocol*) jest protokołem niezawodnym i pewnym, co oznacza, że dane po każdym wysłaniu muszą zostać odebrane i potwierdzone. Jeśli zostały potwierdzone, oznacza to, że trafiły do adresata. W tej warstwie funkcjonuje mechanizm CRC – sprawdza poprawność przesyłania pakietów. Dodatkowo dzielone są tutaj dane na bloki podczas wysyłania i ich złożenie w całość po odbiorze. Warstwa ta zawiera kontrolę przepływu – to dzięki niej sieci przeciążone mogą wciąż funkcjonować.

TCP jest protokołem połączeniowym, przed rozpoczęciem transmisji stosuje tzw. trójstopniowe uzgodnienie (*three-way handshake*). W skrócie jest to prośba o nawiązanie połączenia przed rozpoczęciem transmisji danych. Oto przykładowe rozpoczęcie rozmowy:

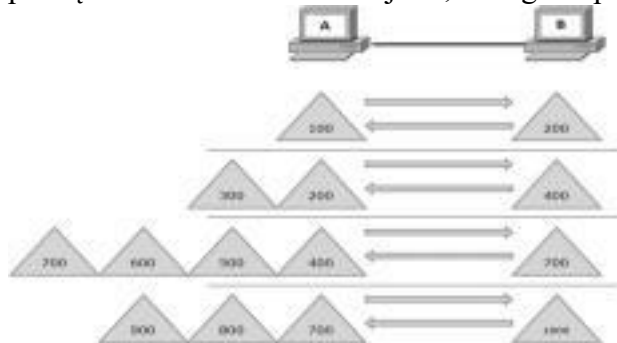
1. Przepraszam Panią, czy możemy porozmawiać?
2. Tak, oczywiście, mam chwilkę czasu.
3. Cieszę się.

Komputer po lewej stronie wysyła wiadomość SYN (*SYN*chronization – 32 bity), można ją porównać do „Przepraszam Panią, czy możemy porozmawiać?”. Komputer proponuje rozpoczęcie połączenia (synchronizacji), wysyłając wiadomość SYN. Ponieważ zawsze dane przesyłane za pośrednictwem protokołu TCP muszą zostać potwierdzone, komputer odpowiada i potwierdza poprzednie dane, wysyłając SYN-ACK (numer potwierdzenia, 32 bity).

Wiarygodność tego protokołu polega na tym, że każde wysłane dane muszą zostać potwierdzone. Komputer źródłowy nie prześle następnych danych bez potwierdzenia wcześniejszych. W przypadku gdy dane dotrą uszkodzone lub niepełne, TCP może rozpocząć proces retransmisji. TCP jest protokołem połączeniowym; oznacza to otwieranie połączenia za każdym razem, kiedy przesyłane są dane.

Protokół TCP umożliwi odbiorcy sterownie szybkością wysyłania danych przez nadawcę. Funkcja ta nosi nazwę kontroli przepływu (*flow control*). Jest przydatna, gdy nadawca chce jednocześnie wysłać bardzo dużą ilość danych do odbiorcy, który nie nadąża z ich przetwarzaniem. Aby wówczas nie doszło do przepełnienia pamięci, odbiorca może żądać od nadawcy spowolnienia transmisji danych. Suma kontrolna sprawdza poprawność przesłania danych.

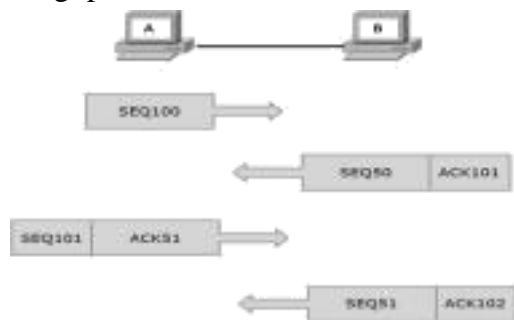
Na poniższym rysunku mamy dwa komputery. W pierwszej fazie komputer A zaczyna transmisję od ustalenia rozmiaru okna na 100 bajtów. Dane zostają przesłane do komputera B i — oczywiście — potwierdzone. Komputer B wysyła potwierdzenie i zezwala na powiększenie okna do 200 bajtów, dlatego w potwierdzeniu (trójkąt) widać liczbę 200.



W kolejnej transmisji komputer A zwiększa rozmiar okna do 200 bajtów, ale w potwierdzeniu otrzymuje 400. Jest to zezwolenie na wysłanie następnym razem okna o wielkości 400 bajtów. Podczas kolejnej transmisji następuje błędny przesył okna numer 700. Jak widać w potwierdzeniu, stacja B żąda przesłania okna 700, dlatego w następnej transmisji dołączone jest okno 3. o numerze 700. Wysłane potwierdzenie o numerze 1000 jest znakiem dla komputera A, że tym razem transmisja została przeprowadzona prawidłowo. Druga forma,

czyli kontrola przepływu za pomocą wstrzymywania potwierżeń (*buffering*), polega na wstrzymaniu potwierdzenia przez host odbierający, aż do czasu, kiedy wszystkie dane zostaną przetworzone. Jeśli host wysyłający nie otrzyma potwierdzenia, nie może wysłać dalszych danych. Chroni tym samym host odbierający przed zalaniem danymi i zapełnieniem pamięci (*congestion voidance*). Ważną funkcją protokołu TCP jest segmentacja. Segmentacja to ważna funkcjonalność ze względu na rozległość sieci Internet i dróg, jakimi mogą być przekazywane pakiety przesyłane przez sieć. Dane muszą być segmentowane, gdyż nie ma możliwości, aby wysłać wszystkie dane w paczce np. 100 GB. Muszą one zostać podzielone na mniejsze porcje, maksymalnie po 1500 bajtów.

Każdy wysłany pakiet posiada swój numer sekwencyjny. Jeśli komputer A wysła pakiet z numerem sekwencyjnym 100, po odebraniu zostaje on potwierdzony i A może przesyłać drugi pakiet o numerze 101.



Warstwa transportu czuwa nad tym, aby dane z komputera wysyłającego trafiły do celu nienaruszone, w odpowiedniej kolejności oraz odpowiedniej wielkości. Mechanizm ten zapobiega zalaniu komputera docelowego zbyt dużą ilością informacji. Mogłoby to doprowadzić do przepełnienia bufora, co z kolei wiąże się z utratą przesyłanych danych. Aby przesyłanym informacjom zapewnić odpowiednią kolejność oraz wielkość, warstwa transportu wykorzystuje segmentację danych. Dane przesyłane są w segmentach i obsługiwane na zasadzie **FIFO**, czyli pierwsze przyszło, pierwsze wyszło (ang. *First In First Out*). Otrzymane dane, w zależności od wykorzystywanego protokołu, muszą zostać potwierdzone bądź nie. W momencie gdy bufor zostanie zapchany, pakiety zostają odrzucone do czasu aż zwolni się miejsce.

Protokół UDP (*User Datagram Protocol*) jest protokołem zawodnym i niepewnym. Oznacza to, że dane po każdym wysłaniu nie są potwierdzane. Może to powodować, że niektóre dane nie dotrą do adresata, a nadawca nigdy się o tym nie dowie. DHCP, DNS, TFTP czy SNMP wykorzystują protokół UDP.

TCP wykorzystywane jest przez http, WWW, FTP, Telnet.

UDP nie ma segmentacji danych jak TCP, jest niewiarygodny, dane mogą docierać w różnej kolejności, przykładem jest VOiP. Po prostu wysyła paczkę i nie sprawdza, czy dotarła do celu – dzięki temu zmniejszona jest ilość przesyłanych informacji kontrolnych. UDP sprawdza się, gdy ilość przesyłanych danych w poszczególnych pakietach jest niewielka.

Sprawdzanie aktualnie używanych portów

Aby sprawdzić, które porty są aktualnie używane, posłuż się poleceniem netstat dostępnym w systemach Windows. W wierszu poleceń wpisz netstat i naciśnij *Enter*. Po chwili pojawi się lista wszystkich aktualnie wykorzystywanych portów. W kolumnie *Adres lokalny* znajdziesz adresy IP oraz numery lokalnie używanych portów. W kolumnie *Obcy adres* zobaczysz nazwę lub adres urządzenia docelowego. Po znaku: widocznym po adresie IP w kolumnie *Adres lokalny* znajduje się również numer portu lub podana nazwa usługi, np. *http*. Zbyt duża liczna połączeń ze stronami http może świadczyć o konie trojańskim.

Polecenie netstat służy tu do wypisywania informacji dot. stanu podsystemu sieciowego. Polecenie netstat -r wyświetla tablicę routingu a „netstat -se” do obejrzenia statystyk protokołów IP, ICMP, TCP i UDP, netstat -e, liczbę pakietów wysłanych a nbtstat -n, wyświetla statystykę protokołu netBIOS, netstat -n, listę aktywnych połączeń.

Często, gdy mówimy o warstwie transportowej to mówimy o ACL (listy dostępowe – np.

blokujemy adres IP lub port dla hosta).

Przydatną komendą w CMD jest ipconfig /all gdzie możemy sprawdzić adresy kart sieciowych, adresy IP i bramę.

Poniżej przykład działania programu netstat z opcją -b (wymaga uprawnień administratora):

Proto	Local Address	Foreign Address	State
TCP	10.100.2.21:59446	db5sch101102019:https	ESTABLISHED
TCP	10.100.2.21:59752	162.125.18.133:https	ESTABLISHED
TCP	10.100.2.21:59789	db5sch101101914:https	ESTABLISHED

```

Interface List
10...ec Be b5 9f 18 7a .....Intel(R) Ethernet Connection I219-LM
13...e4 b3 18 5c df 01 .....Microsoft Wi-Fi Direct Virtual Adapter
8...e6 b3 18 5c df 00 .....Microsoft Wi-Fi Direct Virtual Adapter #2
14...e4 b3 18 5c df 00 .....Intel(R) Dual Band Wireless-AC 8260
12...e4 b3 18 5c df 04 .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====
IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface Metric
0.0.0.0                0.0.0.0          192.168.1.1      192.168.1.5    40
127.0.0.0              255.0.0.0        On-link          127.0.0.1      331
127.0.0.1              255.255.255.255 On-link          127.0.0.1      331
127.255.255.255       255.255.255.255 On-link          127.0.0.1      331
192.168.1.0            255.255.255.0   On-link          192.168.1.5    296
192.168.1.5            255.255.255.255 On-link          192.168.1.5    296
192.168.1.255         255.255.255.255 On-link          192.168.1.5    296
224.0.0.0              240.0.0.0        On-link          127.0.0.1      331
224.0.0.0              240.0.0.0        On-link          192.168.1.5    296
255.255.255.255       255.255.255.255 On-link          127.0.0.1      331
255.255.255.255       255.255.255.255 On-link          192.168.1.5    296
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1         331 ::1/128                  On-link
14        296 fe80::64                  On-link
14        296 fe80::dff:fc20:bf58:27c/128 On-link
1         331 ff00::8                   On-link
14        296 ff00::8                   On-link
=====
Persistent Routes:
None

```

TCP	192.168.0.13:51614	bud02s23-in-f8:https	ESTABLISHED
TCP	192.168.0.13:51615	edge-star-mini-shv-01-ams3:https	ESTABLISHED
TCP	192.168.0.13:51617	93.184.220.29:http	ESTABLISHED
TCP	192.168.0.13:51618	93.184.220.29:http	ESTABLISHED
TCP	192.168.0.13:51619	93.184.220.29:http	TIME_WAIT
TCP	192.168.0.13:51621	bud02s23-in-f206:https	TIME_WAIT
TCP	192.168.0.13:51622	xx-fbcdn-shv-01-ams3:https	ESTABLISHED
TCP	192.168.0.13:51623	108.161.188.192:https	ESTABLISHED
TCP	192.168.0.13:51626	23.111.9.32:https	TIME_WAIT
TCP	192.168.0.13:51628	lg-in-f155:https	ESTABLISHED
TCP	192.168.0.13:51629	waw02s06-in-f68:https	ESTABLISHED

Na jednym komputerze mającym 1 adres IP może jednocześnie działać wiele aplikacji, do ich identyfikacji wykorzystuje się porty. W konfiguracji urządzeń sieciowych ważne jest wyłączenie aktualnie nieużywanych portów na switchach. Porty na switchu są w różnych stanach, m.in. porty nasłuchują i uczą się ruchu sieciowego po to by nie tworzyły się pętle w sieci/nie dublowały adresy IP.

Port protokołu – pojęcie związane z protokołami używanymi w Internecie do identyfikowania procesów działających na odległych systemach. Jest to jeden z parametrów gniazda.

Gniazdo w telekomunikacji (*socket*) – pojęcie abstrakcyjne reprezentujące dwukierunkowy punkt końcowy połączenia. Dwukierunkowość oznacza możliwość wysyłania i odbierania danych. Wykorzystywane jest przez aplikacje do komunikowania się przez sieć w ramach komunikacji międzyprocesowej. Gniazdo posiada trzy główne właściwości:

1. typ gniazda identyfikujący protokół wymiany danych
2. lokalny adres (np. adres IP, IPX, czy Ethernet)
3. opcjonalny lokalny numer portu identyfikujący proces, który wymienia dane przez gniazdo (jeśli typ gniazda pozwala używać portów).

Gniazdo może posiadać (na czas trwania komunikacji) dwa dodatkowe atrybuty:

1. adres zdalny (np. adres IP, IPX, czy Ethernet)
2. opcjonalny numer portu identyfikujący zdalny proces (jeśli typ gniazda pozwala używać portów).

Adres IP wyznacza węzeł w sieci, numer portu określa proces w węźle, a typ gniazda determinuje sposób wymiany danych.

Różne usługi mogą używać tego samego numeru portów, pod warunkiem, że korzystają z innego protokołu (TCP lub UDP), chociaż istnieją także usługi korzystające jednocześnie z jednego numeru portu i obu protokołów. Przykładem takiej usługi jest DNS – korzysta z portu 53 za pomocą TCP i UDP jednocześnie. Zdarza się także, że jedna usługa może korzystać z dwóch różnych portów używanych do innych zadań, jak to jest w przypadku FTP czy SNMP. Poszczególne numery portów przydzielone są przez IANA.

Grupy portów:

Do dyspozycji jest ogółem 65 535 portów TCP i UDP. Aby zachować nad nimi kontrolę, a także by móc przydzielać aplikacjom stałe numery, podzielono je na trzy grupy.

- **Dobrze znane porty (well known ports)** – zarezerwowane, standardowe numery portów od 1 do 1023. Ułatwiają nawiązanie połączenia, ponieważ zarówno nadawca, jak i odbiorca z góry wiedzą, że dane muszą być przesłane dla określonego procesu pod określony numer portu. Dzięki tym portom można identyfikować nie tylko procesy, ale również usługi działające na odległych systemach. Serwery Telnetu używają na przykład portu nr 23. Dobrze znane porty umożliwiają klientom nawiązywanie połączeń z serwerami bez dodatkowej konfiguracji. Zarządzaniem tymi portami zajmuje się Internet Assigned Numbers Authority (IANA). Listę aktualnie przydzielonych numerów portów można znaleźć pod adresem <https://www.iana.org/assignments/port-numbers>. Do roku 1992 dobrze znane porty ograniczały się do zakresu 1 do 255. Porty o numerach od 256 do 1023 były stosowane do usług uniksowych. Porty dobrze znane służą do komunikacji np. pomiędzy klientem a serwerem i są to porty na stałe przypisane do usługi. I tak port 80. obsługuje ruch związany z HTTP. Dzieje się tak, ponieważ klient wykorzystujący zasoby serwera musi wcześniej znać port, którego ma użyć w celu przesłania danych poprzez

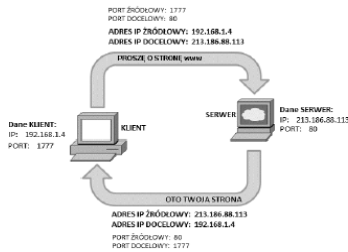
określoną usługę. Na serwerze może być uruchomionych kilkadziesiąt usług TCP, dlatego klient musi znać port, aby dane zostały poprawnie przesłane oraz zinterpretowane. Porty dobrze znane z reguły wykorzystywane są przez takie usługi jak wspomniane HTTP, FTP lub pocztę elektroniczną. Ich pełna lista znajduje się pod adresem <http://www.iana.org/assignments/port-numbers>.

- **Zarejestrowane porty (registered ports)** – porty o numerach od 1024 do 49151 przewidziane są dla usług, które zwyczajowo korzystają z określonych portów. Przykładem może być port 3128, często wykorzystywany przez serwery proxy jako alternatywny port HTTP.
- **Porty przydzielane dynamicznie (dynamically allocated ports, również ephemeral ports)** – jak wskazuje nazwa, zawsze przydzielane dynamicznie. Są to porty o numerach od 49152 do 65535. Każdy klient może korzystać z nich tak długo, jak długo kombinacja protokołu transportowego, adresu IP i numeru portu jest jednoznaczna. Proces, który potrzebuje dostępu do portu, żąda go od swojego hosta.

Port	Protokół
53	DNS
20	FTP – przesyłanie danych
21	FTP – przesyłanie poleceń
67	BOOTP – serwer
68	BOOTP – klient
80	HTTP , dodatkowe serwery, np. proxy , sa najczęściej umieszczane na porcie 8080
443	HTTPS (HTTP na SSL)
143	IMAP
220	IMAP3
5222	XMPP – dla serwera sieci Jabber
3306	MySQL
119	NNTP
110	POP3
995	POP3S (POP3 na SSL)
25	SMTP
22	SSH
514	Syslog
23	Telnet
69	TFTP
161	SNMP

W systemach uniksopodobnych lista portów i nazw odpowiadających im usług znajduje się w pliku /etc/services. Przykład: za pomocą przeglądarki internetowej łączymy się ze stroną <http://www.pg.edu.pl>. Przeglądarka utworzy połączenie z adresem IP 153.19.40.170. Na serwerze zostanie użyty port TCP numer 80, dobrze znany port serwerów WWW (internetowych). Klient wykorzysta dynamicznie przydzielany port np. 29867.

Warstwa sieci

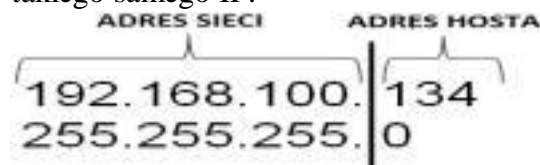


Warstwa sieci (*network layer*) odpowiedzialna jest m.in. za **routing**. Tu jest dodawany adres IP. Tworzy logiczną ścieżkę pomiędzy komunikującymi się hostami. Routing (ang. *routing*) to odnajdowanie najlepszych tras dla pakietów danych. W warstwie sieci występuje kilka rodzajów protokołów, najważniejsze to **IP**, **ARP** (na podstawie IP ustalamy MAC lub odwrotnie) oraz **ICMP**. W warstwie sieci dane przesyłane są w pakiecie. W segmencie adresami były porty (docelowy i źródłowy), w pakiecie adresem jest adres IP. Każdy pakiet musi posiadać adres IP (źródłowy oraz docelowy). W warstwie sieci działają routery. Jednym z zadań routerów jest odnajdowanie najlepszej trasy dla pakietów danych. Trasy są wyszukiwane na podstawie adresów IP. W tej warstwie określane są błędy w komunikacji. Każdy PC w sieci musi posiadać unikatowy adres IP. Sprawdzanie adresu IP komputera w oknie wiersza poleceń wpisz ipconfig i naciśnij *Enter*. Warstwa internetowa/sieci odpowiada za znalezienie najlepszej drogi do celu, wykorzystuje przy tym tabele routingu. W warstwie internetowej pracują routery, które mają za zadanie odnajdywanie najlepszych tras dla pakietów danych.

Protokół IP (*Internet Protocol*) (RFC791) to protokół komunikacyjny umożliwiający tworzenie, wysyłanie oraz otrzymywanie danych w postaci tzw. pakietów. Pakiet IP to dane wysyłane przez protokół IP poprzedzone tzw. nagłówkiem IP. Oczywiście, każdy pakiet posiada numer zwany adresem IP (*IP address*). Adres IP to niepowtarzalny identyfikator komputera w sieci. Jest to 32-bitowa liczba podzielona na cztery oktety. Każdy oktet to 8 bitów.

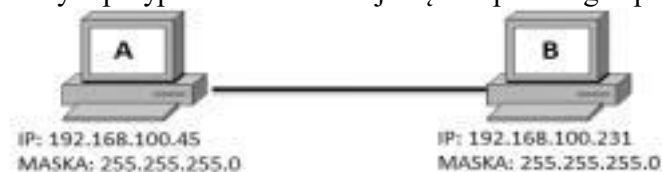
192	168	100	21
1 OKTET	2 OKTET	3 OKTET	4 OKTET
8 BITÓW	8 BITÓW	8 BITÓW	8 BITÓW

Podczas komunikacji w sieci napotkasz na trzy najważniejsze adresy. Pierwszy to adres IP. Drugim adresem jest maska służąca do wyodrębnienia z adresu IP adresu sieci oraz adresu hosta. Maska opisuje, która część adresu IP jest odpowiedzialna za adresację sieci, a która adresuje hosty. Ostatnim, trzecim adresem jest adres domyślnej bramy (*default gateway*). Zanim zacznę omawianie poszczególnych adresów, jeszcze raz przejdź do linii komend i wpisz polecenie ipconfig oraz naciśnij *Enter*. Nikt inny w sieci lokalnej nie może mieć takiego samego IP.

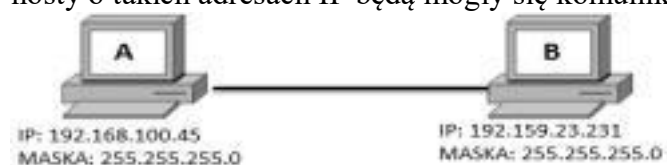


255.255.255.0 – maska podsieci. Zauważ, że pod liczbami 192.168.100 znajdują się liczby 255.255.255. Dlatego w tym przypadku sieć to 192.168.100. Jeśli w adresie maski podsieci znajduje się 0, wówczas reprezentuje ona adres hosta. W naszym przykładzie pod liczbą 134 znajduje się 0, dlatego liczba 134 to adres hosta. Załóżmy, że posiadasz adres 172.161.100.200

oraz maskę podsieci 255.255.0.0. W tym przypadku liczby 255 znajdują się pod 172.161, natomiast pod 100.200 znajdują się zera. Dlatego 100.200 to adres hosta w sieci numer 172.161. Aby dwa komputery mogły się ze sobą komunikować, muszą znajdować się w tej samej sieci, ale posiadać różne adresy hosta. Na rysunku poniżej znajdują się dwa komputery bezpośrednio podłączone, dlatego muszą znajdować się w tej samej sieci. Znajdują się w sieci 192.168.100, ponieważ maska wynosi 255.255.255.0. Posiadają również różne adresy hosta. W tym przypadku komunikacja będzie przebiegać prawidłowo.



Na poniższym rysunku komunikacji pomiędzy dwoma hostami nie będzie, gdyż komputery znajdują się w zupełnie różnych sieciach. Oczywiście, istnieją technologie, które sprawiają, że hosty o takich adresach IP będą mogły się komunikować:



Protokół IP zapewnia przenoszenie danych pomiędzy komputerami w Internecie, definiuje format datagram/pakietu, określa schemat adresowania, wybiera trasowanie, dzieli dane na fragmenty (fragmentacja). Jest niepewny (nie zapewnia korekcji błędów transmisji) i bezpołączeniowym (nie ustanawia połączenia i nie sprawdza gotowości odległego komputera).

Budowa pakietu:

- wersja, numer wersji IP,
- IHL, (Internet Header Length) – długość nagłówka,
- TOS, typ usługi – zapewnia jakość ruchu, określa sposób przekazywania pakietu w węzle sieci,
- długość pakietu,
- identyfikator – służy do odróżniania pakietów tworzących całość.

Każdy z pakietów ma określony rozmiar MTU (Maximum Transmission Unit). Jeśli rozmiar datagramu jest zbyt duży to dzielony jest na fragmenty a później przez odbiorcę łączony jest w całość (defragmentacja). Adres IP jest adresem logicznym interfejsu sieciowego hosta (przykład interfejsu to karta sieciowa). Czy urządzenie pracujące w sieci może mieć więcej niż 1 adres IP? Może, np. serwer z 2 kartami sieciowymi, ma adres IP WAN i LAN. Podobnie działają routery w naszych domach. Adres publiczny (od providera, może być tylko 1 na świecie) i adres prywatny w LAN – mogą się dublować. NAT tłumaczy adresy publiczne na prywatne i odwrotnie – możemy to skonfigurować na routerze.

Maska podsieci (też jest 32 bitowa), 4 oktetowa albo /24 (24 jedynek w binarnym zapisie maski, jedynek w masce to adres sieci a 0 to adres hosta). Ćwiczenie na przekształcenie dziesiętnych na binarną:

$$192.168.1.120 = 11000000.10101000.00000001.01111000$$

Adresowanie klasowe (np. A, B, C, D, E) na sztywno określa ilość hostów i sieci. Adresowanie bezklasowe – elastyczne adresowania sieci, my decydujemy ile hostów i ile sieci.

Dzięki masce podzielimy sieć na podsieć!

Obliczanie adresu sieci, adresu maski, broadcast, zakresu sieci.

192.168.1.145 a maska 255.255.255.128 /25

Aby obliczyć adres sieci zamieniamy adres IP na postać binarną:

11000000 10101000 00000001 10010001

Potem konwertujemy maskę:

11111111 11111111 11111111 10000000

Potem wykonujemy operację “and - mnożenie” – tak na prawdę konwertujemy tylko ostatni oktet:

11000000 10101000 00000001 10010001

11111111 11111111 11111111 10000000

= 11000000 10101000 00000001 10000000

Teraz konwertujemy na postać dziesiętną, czyli: 192.168.1.128 – to jest nasz adres sieci.

Teraz obliczamy adres rozgłoszeniowy, czyli zamieniamy binarnie maskę przez bramkę not – 0 zamieniamy na 1:

11111111 11111111 11111111 10000000

not 00000000 00000000 00000000 01111111

a teraz postać dziesiętna: 0.0.0.127 a potem dodajemy tą wartość do adresu sieci:

0.0.0.127+192.168.1.128 = 192.168.1.255 (to jest adres rozgłoszeniowy naszej sieci).

Teraz obliczamy liczbę hostów w naszej sieci:

2 (liczba bitów adresu IP – skrócony zapis maski) -2 = ilość hostów:

$2(32 \text{ bity} - 25) - 2 = 2^7 - 2 = 128 - 2 = 126$ hostów.

Adres IPV4 1-go i ostatniego hosta w sieci: Adres sieci: 192.168.1.128 1 host: 192.168.1.129

Adres broadcast: 192.168.1.255 to ostatni host 192.168.1.254

Ćwiczenie: Wskaż adres sieci, do której należy host o adresie 172.16.0.123/27

A. 172.16.0.16

B. 172.16.0.96 (zamieniamy na binarkę, stosujemy AND)

C. 172.16.0.112

D. 172.16.0.224

Ćwiczenie do obliczania adresu klasy B. Oblicz adres sieci, broadcast, liczbę hostów oraz adres 1 hosta i ostatniego adresu: 172.16.160.200 o masce 255.255.192.0.

obliczamy adres sieci

krok 1

```

172.16.160.200  1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 1 0 0 0
255.255.192.0   1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  
```

krok 2

```

      128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1 128 64 32 16 8 4 2 1
AND (-) 1 0 1 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
      128 + 32 + 8 + 4 = 172          16          128          0
  
```

krok 3

172.16.128.0

obliczamy adres rozgłoszeniowy

krok 1

```

255.255.192.0  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
NOT            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
  
```

krok 2

```

      + 0 . 0 . 63 . 255
      + 0 . 0 . 63 . 255
  
```

krok 3

```

adres sieci: 172 . 16 . 128 . 0
              + 0 . 0 . 63 . 255
              -----
              = 172 . 16 . 191 . 255
  
```

IPv4

obliczamy liczbę hostów

Adres IP: 172.16.160.200
jak to adres IPv4, składa się z 32 bitów

Maska: 255.255.192.0
maska w zapisie skróconym: /18

2 (liczba bitów adresu IP - skrócony zapis maski) - **2**

po podstawieniu do wzoru:

$2^{(32 - 18)} - 2 = 2^{14} - 2 = 16384 - 2 = 16382$

adres pierwszego i ostatniego hosta

adres sieci: **172.16.128.0** +1

adres pierwszego hosta: **172.16.128.1**

adres rozgłoszeniowy: **172.16.191.255** -1

adres ostatniego hosta: **172.16.191.254**

Zatem: Jeżeli adres IP stacji roboczej ma postać 176.16.50.10/26 to adres rozgłoszeniowy oraz maksymalna liczba hostów w sieci wynoszą 176.16.50.63; 62 hosty. Adresem pętli zwrotnej jest 127.0.0.0 a w wersji IPV6 jest to: ::1/128.

Ćwiczenie: Określ do jakiej podsieci należy komputer o adresie 192.168.0.123 i masce 255.255.255.224. Do obliczenia zamieniamy adresy na postać binarną a potem stosujemy iloczyn logiczny.

```

11000000.10101000.00000000.011111011
11111111.11111111.11111111.11100000
11000000.10101000.00000000.01100000
  
```

Ten komputer należy do podsieci o adresie: 192.168.0.96.

Obliczanie ilości podsieci.

Liczba możliwych do utworzenia podsieci zależy od liczby bitów z części hosta przeznaczonych do utworzenia podsieci. W sieci o adresie powyżej 192.168.0.123 i masce

10.10.1.1	192.181.230.176
192.255.255.254	194.181.230.33

Użytkownik systemu operacyjnego Linux chcąc przypisać adres IP 152.168.1.200 255.255.0.0 interfejsowi sieciowemu wpisuje polecenie (mając uprawnienia root):
ip addr add 152.168.1.200/16 dev eth1. W wyniku polecenia route add 192.168.35.0 MASK 255.255.255.0 192.168.0.2 można ustawić adres docelowej sieci na 192.168.35.0.

TTL – czas życia datagramu w Internecie. TTL powstał, aby dane nie były rozpropagowywane do serwerów posiadających w buforze wpisy o stanie poprzednim. Po tym czasie serwer musi usunąć dane z bufora. TTL zwiększa obciążenie serwera, bo musi odpowiadać na zapytania innych serwerów odświeżających swoje dane. TTL jest zmniejszany o wartość 1 gdy przejdzie przez kolejny router. Gdy TTL osiągnie wartość 0, to router odrzuca pakiet i wysyła do jego nadawcy pakiet ICMP informujący o przedawnieniu. Sprawdzając pakiet IP za pomocą analizatora nie zorientujesz się, ile przeszedł on routerów, dopóki nie będziesz znał początkowego TTL ustanowionego przez źródło.

CIDR – bezklasowe routowanie międzydomenowe wraz z którym powstało pojęcie maski podsieci. Teraz adres sieci i komputera określa się za pomocą maski. Powstało to dlatego, że kończyły się możliwości podłączenia komputerów np. więcej niż 254. Jeśli form chciała to zrobić musiała otrzymać adres klasy B – można zaadresować 65 tysięcy komputerów a oznaczało to stratę 65 tysięcy adresów. Klasy adresów zaczęły się kurczyć. Zapisem CIDR jest np. 10.10.1.22/16 (bo jest to maska 255.255.0.0, czyli 2x 8 bitów więc 16).

VLSM – dopuszczanie masek podsieci o różnych długościach. Można połączyć 2 podsieci tworząc jedną większą. Wtedy zmniejsza się maska, bo ona definiuje rozmiar podsieci.

IPV6

Adres IPV6 - 128 bitów (2 do 128 potęgi, 8x16 bitów).

- unicast (indywidualne adresy w sieci),
- multicast (adresy grupy),
- anycast (adresy grupy).

Przykładowy IPV6:

2001:0db8:0000:0001:0000:0000:0000:0001

-> 2001:db8:0:1:0:0:0:1

-> 2001:db8:0:1:::1

Jest to ciąg ośmiu szesnastobitowych liczb w systemie szesnastkowym, oddzielonych dwukropkiem. Zera są pomijane np.: FF01:0:0:0:456:FEDC:0:88 -> FF01::456:FEDC:0:88. W adresacji IPv6 adres np. ff00::/8 określa pulę adresową używaną do komunikacji multicast.

Wpisywanie do przeglądarki adresu IPV6: [http://\[2001:db8:0:1:::1\]](http://[2001:db8:0:1:::1])

Wyodrębnianie części sieciowej od części hostowej w adresie IPV6:

Najczęściej dzielimy adres na pół tzn. 64 bit należą do sieci a drugie 64 bity należą do hosta.

2001:4070:11:204:0212:34FF:FE56:789A

Kolor zielony – prefix operatora, kolor czerwony – dostawca Internetu

Kolor niebieski – prefix sieci, kolor czarny – identyfikator hosta

IPv6 to nowy typ adresów „anycast” – odbiorcą adresu jest jeden host z grupy, stosowane, gdy kilka routerów łączy sieć lokalną z Internetem. Wystarczy, że datagram dotrze do 1 z nich i w przypadku awarii któregośkolwiek dane zostaną przejęte przez pozostałe grupy. W IPV6 przyjęto nowe mechanizmy szyfrowania.

Zadanie egzaminacyjne: odpowiedź B:

Który adres IPv6 jest prawidłowy?

- A. 1234:9ABC::123::DEF4
- B. 1234:9ABC::123:DEF4
- C. 1234-9ABC-123-DEF4
- D. 1234.9ABC.123.DEF4

Do IPv6 dodano nową wersję protokołu dynamicznej konfiguracji hostów DHCPv6, dzięki czemu hosty otrzymają od serwera dane takie jak IP hosta, IP bramy sieciowej, adres serwera DNS, maski podsieci. W IPv6 nie występuje pojęcie komunikacji broadcastowej a zamiast tego stosowany jest link-local (routery nie przekazują tych adresów do WAN).

W tym protokole zdefiniowano adresy specjalne:

::128 – adres nieokreślony, same 0,

::0 – adres globalny trasy domyślnej w routingu,

::1/128 – adres pętli zwrotnej (odpowiednik 127.0.0.1),

2000::/ - adresy unicastowe,

FC00::/7 – adres lokalny, odpowiednik adresów IPv4: 10.0.0.0, 172.16.0.0, 192.168.0.0/24.

FE80::/10 – adres lokalny autokonfiguracji łącza,

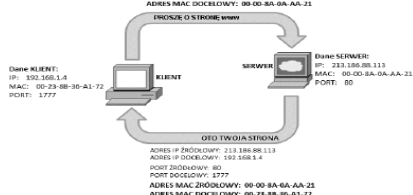
FF00::/8 – adresu multicastowe, pełniące funkcje „broadcastu”.

Jeżeli twój host ma przydzielony adres IPv6 to możemy sprawdzić czy odpowiada poprzez wpisanie ping -6 ::1 lub gdy chcemy spingować innego hosta w sieci: ping -6 <adresIPv6>.

Identyfikacja ruchu dla IPV6 jest inna niż w wersji 4. Zamiast Type of Service jest Flow Label. Fragmentacja pakietu następuje tylko przez hosta a nie jak w przypadku IPV4 – hosta i router. Brak ARP (zamiast tego mechanizm neighbor solicitation) i NAT. ICMPv6 jest odpowiednikiem starszego protokołu.

Warstwa łącza danych

Warstwa łącza danych (*data link layer*) umieszcza pakiety w ramach oraz przesyła je do punktu docelowego na podstawie adresów **MAC**. Na warstwę łącza danych składają się dwie podwarstwy: podwarstwa kontroli dostępu do medium (**MAC**) oraz podwarstwa kontroli łącza logicznego (**LLC**). Pierwsza określa sposób przesłania danych przez medium sieciowe i jest oparta na adresacji fizycznej. Druga identyfikuje protokoły oraz występującą w nich enkapsulację danych. Komunikacja w warstwie łącza danych odbywa się na podstawie adresów MAC. Przybywający z warstwy wyższej pakiet zostanie opakowany w ramkę zawierającą adresy MAC nadawcy i odbiorcy. Następnie ramka jest wysyłana przez łącze fizyczne. Warstwa ta zajmuje się kompresją danych. W jej skład wchodzi sterowniki kart sieciowych czy switche.



Każdy interfejs routera, przełącznika, jak i karty sieciowej posiadają swój unikatowy adres MAC. Teraz już widzisz, dlaczego ważne jest, aby każda karta sieciowa na świecie posiadała unikatowe adresy MAC.

Budowa ramki: Preambuła (7 bajtów, pozwala na synchronizację odbiorników), SFD (znacznik początkowy ramki 1 bajtowy), MAC odbiorcy (6 bajtów), MAC nadawcy (6 bajtów), typ ramki/długość (2 bajty), dane (46-1500 bajtów), FCS (wykrywa błędy, 4 bajty).

Rozmiar pola w bajtach	7	1	6	6	2	46 - 1500	4
Nazwa pola	Preambuła	Znacznik początku ramki	Adres MAC odbiorcy	Adres MAC nadawcy	Długość/Typ	Dane i wypełnienie	Kod kontrolny ramki (FCS)

Protokół kontroli MAC (MAC Control) – w momencie, gdy zagubi się ramka lub zostanie odrzucona, protokół ten ją odnajdzie. Jest to mechanizm sterowania przepływu danych w czasie rzeczywistym dla full duplex. Stacja wysyłająca ramkę nie musi pamiętać adresu stacji odbierającej.

VLAN (802.1q) – wyodrębnianie sieci w ramach sieci LAN. Jest to rozdzielanie komputerów za pomocą przełącznika.

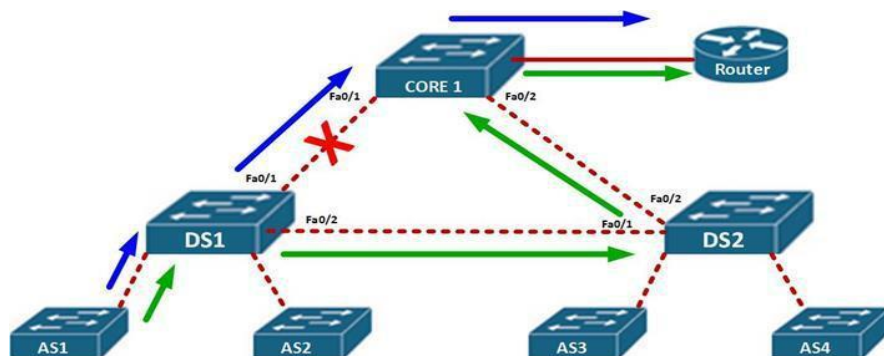
QOS (802.1p) – zarządzanie jakością ruchu – quality of service. Mechanizm umożliwiający priorytetyzację ruchu sieciowego, np. głos lub wideo będą miały pierwszeństwo nad mailami (eliminuje zbędny multicast poprzez przełączniki). Ruch ważniejszy będzie miał więc pierwszeństwo przed tym nieistotnym - ramki o niższym priorytecie nie będą wysyłane, dopóki ramki o wyższym priorytecie nie zostaną wysłane. Aby priorytetowanie miało sens wszystkie urządzenia w sieci muszą mieć to wdrożone. Sprawdza to się m.in. przy telefonach VOIP gdzie głos jest stawiany jako priorytet kosztem Internetu.

W QOS ustalamy również górną granicę opóźnień, wymaganą przepływność i dopuszczalny procent utraty pakietów.

STP (802.1d) – Spanning Tree Protocol, protokół zapobiegający powstawaniu połączeń nadmiarowych czy pętli. Problemem może być broadcast storm – ramki rozgłoszeniowe zaczynają krążyć bez końca. STP zwiększa poziom odporności sieci na awarie. STP wybiera więc najkrótszą ścieżkę w głównym przełączniku uwzględniając tzw. skumulowany koszt połączenia np. 10Gb/s – koszt 2, 1Gb/s – koszt 4, 100 Mb/s – koszt 19, 10Mb/s – koszt 100.

Każdy z portów przełącznika, na którym działa STP może mieć 1/5 stanów:

- disabled – wyłączony port lub uszkodzony,
- blocking – nasłuchiwanie ramek BPDU (bridge), wszystkie inne są blokowane,
- listening – przełącznik sprawdza czy są inne ścieżki do przełącznika głównego,
- learning – przełączniki uczą się adresów MAC,
- forwarding – normalna praca przełącznika.

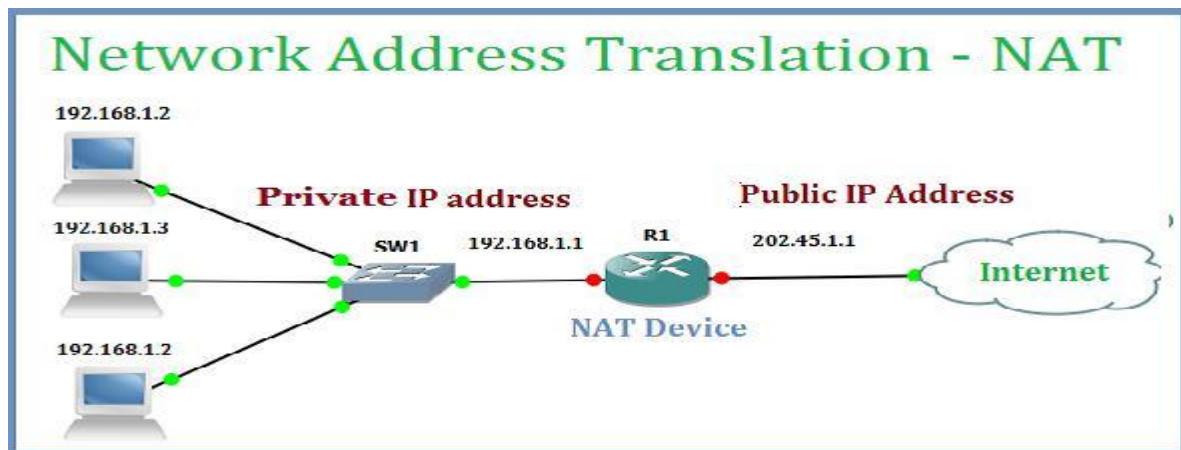


RSTP (Rapid – 802.1w) – blocking i listening połączone w discarding, szybsze przełączenie na ścieżkę zapasową w przypadku awarii.

Warstwa fizyczna

Ostatnią warstwą modelu ISO/OSI jest warstwa fizyczna, która przesyła dane w postaci bitów przez medium sieciowe, takie jak kabel miedziany lub światłowód. Warstwa fizyczna działa tylko na zasadzie przyjmowania binarnych 0 lub 1 i przekazywania ich przez łącze. Warstwa fizyczna obsługuje elektryczny, optyczny oraz radiowy sposób wysyłania i odbierania danych. Rozpoznaje i potrafi interpretować takie technologie jak napięcie elektryczne, światło i fale radiowe. W warstwie fizycznej działają m.in. takie urządzenia jak karty sieciowe i koncentratory. Warstwa ta określa też sposób połączenia mechanicznego (wtyczki, skrętki), elektrycznego (poziom napięcia, prądu).

NAT polega na zamianie jednego adresu IP na inny adres. Zmiany adresów dokonuje router, na którym wcześniej skonfigurowano usługę NAT. Aby możliwe było tłumaczenie adresów, na routerze musi zostać skonfigurowana tablica translacji. Translacja może odbywać się na trzy sposoby. Pierwszym jest sposób statyczny (*static translation*), polegający na wpisaniu do tablicy NAT adresów lokalnych, które mają zostać tłumaczone na adres publiczny (rysunek poniżej). Drugim sposobem jest translacja dynamiczna (*dynamic translation*). Trzecim jest translacja z przeciążeniem, zwana inaczej PAT (*Port Address Translation*). Zaletą technologii NAT jest wyższy poziom bezpieczeństwa sieci prywatnej, ponieważ routery ukrywają komputery pracujące w tej sieci. Inną zaletą jest to, że posiadając jeden publiczny adres, można zapewnić wielu komputerom dostęp do sieci publicznej.



Protokół ARP

Aby poprawnie przesłać dane przez sieć, urządzenie nadawcze musi znać adres MAC urządzenia docelowego. Protokół ARP (RFC826) służy do poznawania tego adresu przed wysłaniem ramki. Aby poznać adres MAC odbiorcy, nadawca wysyła tzw. żądanie ARP (żądanie ma format rozgłoszeniowy — *broadcast* — czyli jest wysyłane do wszystkich) zawierające adres IP odbiorcy. Komunikat ARP jest zawsze wysyłany do wszystkich członków sieci, ale tylko jedna stacja odpowie na taki komunikat, wysyłając w odpowiedzi swój adres MAC. Tworzy w tym celu tzw. odpowiedź ARP zawierającą, oprócz jego adresu IP, również jego adres MAC. Dane o adresie MAC odbiorcy są przechowywane w specjalnej tablicy nazywanej tablicą ARP. Jest tworzona po to, aby za każdym razem nie było konieczne pytanie o adres MAC, bo nadawca szuka najpierw danych o adresie MAC odbiorcy w swojej tablicy. Aby wyświetlić tablicę ARP na Twoim komputerze (z systemem Windows), wpisz w wierszu poleceń „arp -a”.

Protokół ARP umożliwia przekształcenie adresów protokołów sieciowych (IP) na 48 bitowy adres ethernetowy MAC. W momencie, gdy protokół warstwy sieci chce przekazać datagram do warstwy dostępu do sieci, warstwa ta musi określić adres docelowy MAC komputera. ARP to swego rodzaju tablica z adresami MAC wszystkich urządzeń w sieci LAN. Gdy raz zostanie podany adres MAC, tablica trzyma go swojej pamięci. ARP jest przydatny w momencie, gdy mogą zdublować się adresy IP w sieci lokalnej.

Domena rozgłoszeniowa – w sieciach lokalnych, tworzą je wszystkie komputery które otrzymują wysłaną ramkę typu broadcast. Podziału dokonuje router. Domeny kolizji są dzielone przez przełączniki.

Założmy, że komputer o adresie IP 192.168.1.5 wysyła plik muzyczny mp3 do komputera o adresie IP 192.168.1.10. Pamiętaj, że urządzenia sieciowe nigdy nie komunikują się przy użyciu bezpośrednio adresów IP, zawsze dokonują tego za pomocą adresów MAC. Dlatego w tym przypadku komputer 192.168.1.5 wyśle żądanie ARP dotyczące adresu komputera

192.168.1.10, które trafi do wszystkich urządzeń w danej sieci lokalnej, również do routera. Router po odebraniu żądania stwierdzi, że nie posiada adresu 192.168.1.10, więc na przesłane żądanie nie odpowie. Nie przekaże również żądania dalej, ponieważ routery nie przesyłają rozgłoszeń. Na żądanie odpowie jednak komputer 192.168.1.10, który w odpowiedzi wyśle swój adres MAC. Komputer 192.168.1.5 odbierze odpowiedź i zapisze adres MAC w swojej lokalnej tablicy ARP, aby na przyszłość nie wysyłać żądania ARP. Następnie komputer 192.168.1.5 utworzy ramkę, gdzie w polu adresu MAC odbiorcy będzie widoczny adres 00-01-21-21-A1-A1, natomiast w polu adresu MAC nadawcy będzie adres 00-00-01-23-A1-01. Na tej podstawie prześle plik mp3, który zostanie umieszczony wewnątrz utworzonej ramki.

Protokół ICMP (*Internet Control Message Protocol*) (RFC792) to protokół bezpołączeniowy, posiada mechanizm informowania o błędach. Umożliwia przesyłanie informacji o błędach występujących w funkcjonowaniu sieci IP między urządzeniami aktywnymi pracującymi w tejże sieci. ICMP powiadamia m.in. o braku możliwości dostarczenia pakietu do miejsca przeznaczenia, o zmianie wcześniej wyznaczonej trasy przez jeden z pośredniczących routerów. Informacje przesyłane przez ICMP noszą nazwę komunikatów i są przesyłane wewnątrz pakietów IP. Protokół ICMP posługuje się dwunastoma komunikatami, które są wymieniane pomiędzy urządzeniami pracującymi w sieci, np. routerami lub stacjami roboczymi. Dotyczą one m.in:

- przekroczenia czasu życia datagramu (*Time to Live — TTL*); komunikat jest wysyłany, jeśli po wykonaniu odpowiednich obliczeń wartość pola czasu życia datagramu IP osiągnie zero, wykrycia nieosiągalnych miejsc przeznaczenia,
- chwilowego wstrzymania nadawania, gdy datagramy przybywają do komputera lub pośredniczącego routera szybciej, niż można je przetworzyć, i brakuje wolnej pamięci buforowej do ich zapamiętania,
- sprawdzenia zasobów sieciowych; w tym celu wysyłany jest sygnał echa; system po otrzymaniu tego komunikatu musi natychmiast odesłać go do nadawcy; brak odpowiedzi oznacza, że komunikacja w danej chwili jest niemożliwa.

PING lub TRACERT informuje nas, gdzie datagramy zostały zgubione w sieci – jest praktycznym przykładem wykorzystania ICMP. Tracert służy także do śledzenia pakietów do serwera strony internetowej.

Co należy wpisać w miejscu kropek, aby w systemie Linux zwiększyć domyślny odstęp czasowy między kolejnymi transmisjami pakietów przy użyciu polecenia ping?

```
ping ..... 192.168.11.3
```

Odpowiedź: -i 3

Gdy na pingu zobaczymy odpowiedź: „sieć docelowa jest nieosiągalna” to oznacza że nie istnieje trasa prowadząca do miejsca docelowego. Odpowiedź: „Upłynął limit czasu żądania” oznacza, że w domyślnym czasie 1s nie nadeszła odpowiedź na polecenie ping.

POE – (Power over Ethernet 802.3af) – standard, który umożliwia doprowadzenie zasilania do urządzeń sieciowych poprzez skrętkę. Wykorzystuje on albo przełącznik (end-span) lub patch-panel (mid-span) albo można stosować zasilanie wykorzystujące obydwa urządzenia. Dzięki temu zaoszczędzimy na UPS-ach i będziemy korzystać z zasilania urządzeń wpiętych.

Sygnały i kodowanie

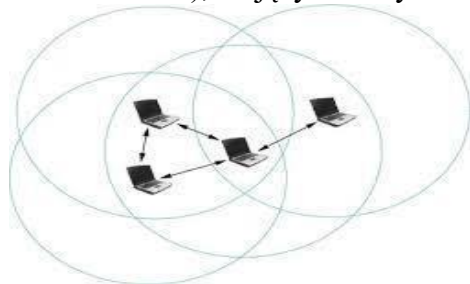
10Mb/s (10BASE-T) – tu działa kodowanie Manchester:

- 0 - sygnał o wysokiej wartości w 1 połowie okresu i niskiej w drugiej,
- 1 – sygnał o niskiej wartości w pierwszej połowie okresu i wysokiej w drugiej. Sygnały są sprawdzane za pomocą testu łącza.

100Mb/s (100BASE-T) – opiera się na kodowaniu blokowym, 4 bitowy blok danych jest kodowany za pomocą 5 bitowego sygnału. Pozostałe wartości służą do sygnalizacji startu ramki czy błędów.

1Gb/s (1000BASE-LX) – w światłowodzie stacja sprawdza braki transmisji wysyłając sygnały IDLE. W skrętce sygnały są wysyłane i odbierane wszystkimi parami.

Sieć WLAN – komputery łączą się za pomocą bezprzewodowych kart sieciowych, każdy użytkownik pełni rolę klienta i serwera, w instalacjach tymczasowych typu ad hoc (czyli bez Access Pointa), mających mały zasięg:



By zwiększyć zasięg w sieci ad hoc (topologia oparta na wykorzystaniu fali radiowych), można zainstalować access point – odpowiednik koncentratora w sieci Ethernet. Strukturę taką określamy jako tryb infrastrukturalny.

Często WLAN jest uzupełnieniem kablowej LAN, dzięki właśnie access point. Połączenie tych 2 typów sieci nazywa się ESS - Extended Service Set. Filtrowanie adresów MAC jest skutecznym sposobem zabezpieczającym sieć bezprzewodową.

Tworzenie sieci ad hoc w Windows 10.

W CMD wpisz: `netsh wlan set hostednetwork mode=allow ssid=ad hoc key=Qwerty123` (SSID: ad hoc, hasło: Qwerty123).

Włączanie sieci ad hoc: `netsh wlan start hostednetwork`. W centrum sieci i udostępniania można sprawdzić czy zostało utworzone połączenie sieciowe. W oknie połączenia sieciowe kliknąć prawym: właściwości -> udostępnianie -> zezwalaj innym użytkownikom sieci na łączenie się poprzez połączenie internetowe tego komputera, z listy wybrać ad hoc i ok. Za pomocą innego urządzenia np. laptopa znaleźć sieć ad hoc w SSID i połączyć.

Protokół 802.11 w WLAN – stacja bezprzewodowa może znajdować się w 3 stanach:

- stan początkowy – nieskojarzony z żadnym punktem dostępowym,
- uwierzytelniony (wiarygodność punktu dostępowego),
- uwierzytelniony i skojarzony z danym punktem dostępowym.

Aby stacja mogła wykryć sieć WLAN musi rozpocząć skanowanie – każdy punkt dostępowy ma obowiązek wysyłania ramek informacyjnych Beacon, które dostarczają informację dzięki którym nasłuchująca stacja może podjąć decyzję o dokonaniu próby podłączenia do sieci typu ad hoc. W przypadku wielu access pointów, stacja wybiera ten punkt, gdzie sygnał jest najmocniejszy.

W sieciach 802.11 nie istnieje kontrola MAC adresów więc możliwe jest podszywanie się pod wybraną stację. Dodatkowym problemem jest uruchomienie przez agresora fałszywego punktu dostępowego.

Roaming – proces przemieszczania się stacji bezprzewodowej pomiędzy kolejnymi punktami dostępowymi z zachowaniem ciągłości transmisji. Stacja wysyła próbkę w poszukiwaniu silnego sygnału – po określeniu, wysyła do niego ramkę – punkt dostępowy potwierdza wpisanie tej stacji na listę użytkowników (proces kojarzenia).

Transmisja radiowa

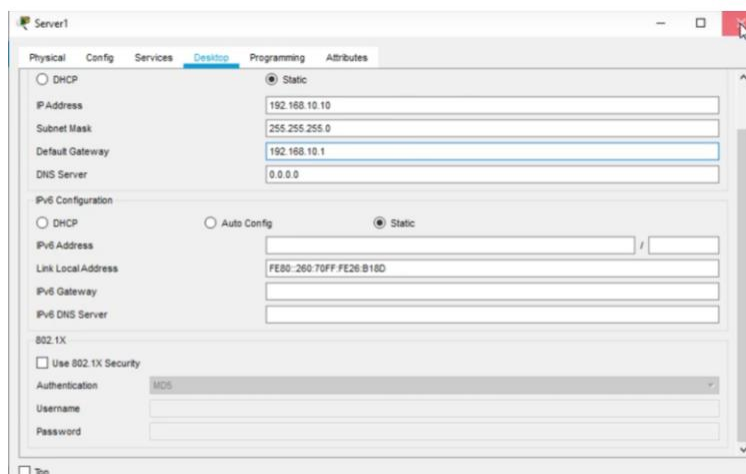
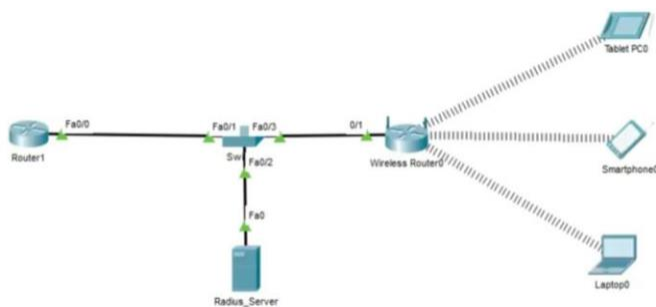
Stosowane są 2 metody:

- a) DSSS (direct sequence spread spectrum) – rozpraszanie widma w sekwencji bezpośredniej
- b) FHSS (frequency hopping...) – rozpraszanie widma z przeskokiem częstotliwości, odporna na zakłócenia.

WEP – (**wire equivalent privacy**), wykorzystuje zawodny do szyfrowania algorytm o długości 40 lub 104 bitów: *shared key* – wymagające odesłania klucza i *open system* – niewymagający uwierzytelnienia. Każdy z użytkowników sieci WLAN może podsłuchiwać innych transmitujących z tym samym kluczem WEP. WEP nie zabezpiecza przed podsłuchaniem transmisji sąsiada traktując wszystkich użytkowników sieci bezprzewodowej jako rodzinę. Niemniej jednak należy korzystać z WEP, najlepiej z maksymalną długością klucza. Warto wyłączyć rozgłaszanie ESSID (nazwy sieci) przez punkty dostępowe. WEP wykorzystuje klucz symetryczny w oparciu o algorytm RC4.

Radius jest protokołem uwierzytelniającym użytkowników małych i miejskich na linii klient-serwer, wykorzystuje porty 1812 i 1813. Najczęściej punkt dostępowy pełni funkcję klienta Radius. Po otrzymaniu danych od użytkownika wysyła jego identyfikator wraz z zakodowanym hasłem do serwera Radius. Po sprawdzeniu danych, serwer albo ustala *accept* lub *reject*. Zadanie Packet tracer z Radius:

Zbuduj sieć z laptopa z WiFi, który będzie połączony z routerem WRT300N, później kablem z Switchem i na końcu z serwerem i innym routerem. Na laptopie, smart phonie i tablecie wpisz adres IP statyczny i bramę a w zakładce config: nazwę SSID, WPA2, hasło, i adresację. Na routerze podobnie.



Radius_Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

AAA

Service On Off Radius Port 1645

Network Configuration

Client Name Home Client IP 192.168.10.1

Secret password ServerType Radius

Client Name	Client IP	Server Type	Key
1 Home	192.168.10.1	Radius	password

User Setup

Username Password

Username	Password
1 User	User
2 user1	user1

Wireless Router0

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Wireless

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): Home

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: Enabled Disabled

Wireless Router0

Physical Config **GUI** Attributes

Wireless Security

Security Mode: WPA2 Enterprise

Encryption: AES

RADIUS Server: 192 . 168 . 10 . 10

RADIUS Port: 1645

Shared Secret: password

Key Renewal: 3600 seconds

Tablet PC0

Physical **Config** Desktop Programming Attributes

Wireless0

Port Status On

Bandwidth 300 Mbps

MAC Address 00E0-A311-7AD3

SSID Home

Authentication

Disabled

WPA-PSK

WPA

802.1X

WPA2

Method: WPA2-PSK

WEP Key

PSK Pass Phrase

User ID User

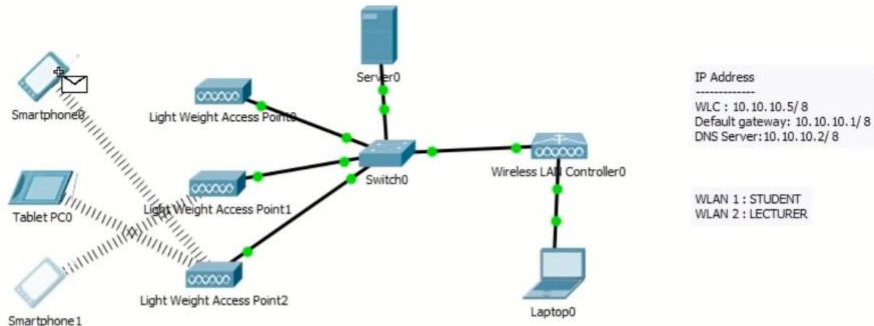
Password Use

Encryption Type AES

IP Configuration DHCP

Kontrolery sieci

W dużych sieciach za zarządzanie i udostępnianie sieci WiFi odpowiedzialne są kontrolery sieci.



Wireless LAN Controller0

Physical Config Attributes

GLOBAL Settings

INTERFACE

GigabitEthernet1

GigabitEthernet2

GigabitEthernet3

GigabitEthernet4

Management

Management

IP Configuration

IP Address 10.10.10.5

Subnet Mask 255.0.0.0

Default Gateway 10.10.10.1

DNS Server 10.10.10.2

IP Address

WLC : 10.10.10.5/8

Default gateway: 10.10.10.1/8

DNS Server: 10.10.10.2/8

WLAN 1 : STUDENT

WLAN 2 : LECTURER

Server0

Physical Config Services Desktop Programming Attributes

GLOBAL Settings

Algorithm Settings

INTERFACE

FastEthernet0

Port Status On

Bandwidth 100 Mbps 10 Mbps Auto

Duplex Half Duplex Full Duplex Auto

MAC Address 000A-4107-4E79

IP Configuration

DHCP

Static

IP Address 10.10.10.3

Subnet Mask 255.0.0.0

IPv6 Configuration

DHCP

Auto Config

Server0

Physical Config Services Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

DHCP

Interface FastEthernet0 Service On Off

Pool Name serverPool

Default Gateway 10.10.10.1

DNS Server 10.10.10.2

Start IP Address : 10 10 10 100

Subnet Mask: 255 0 0 0

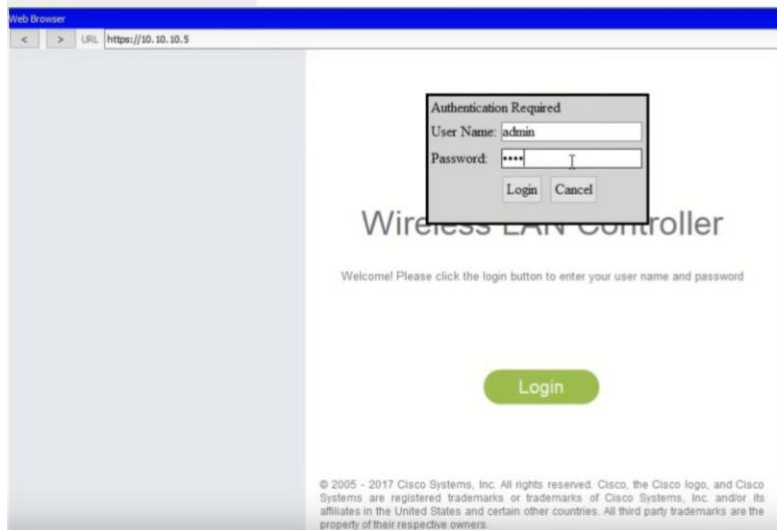
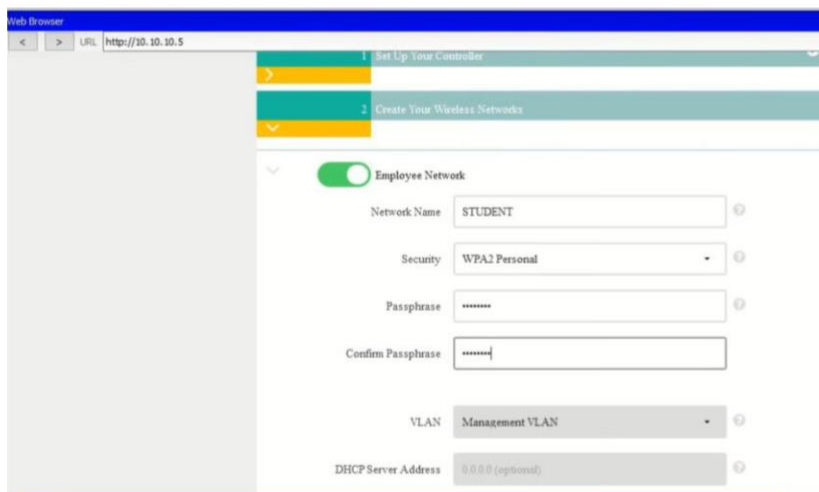
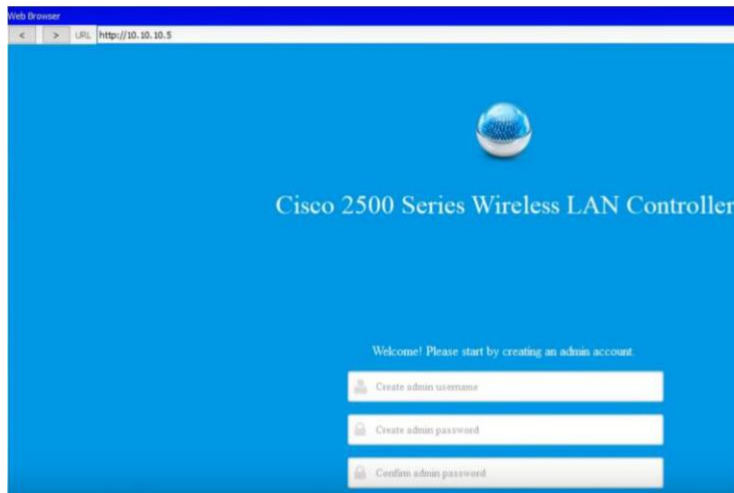
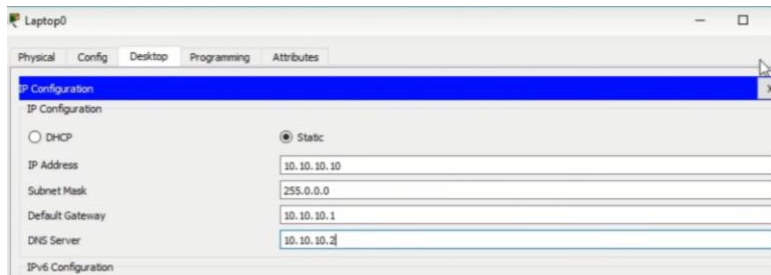
Maximum Number of Users : 100

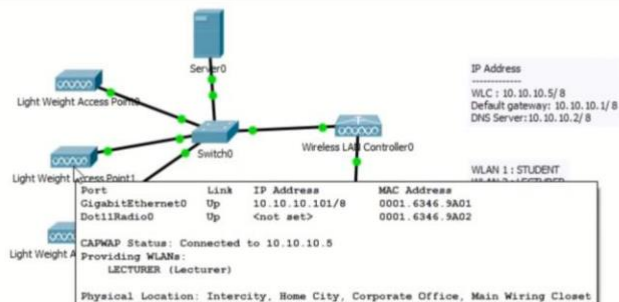
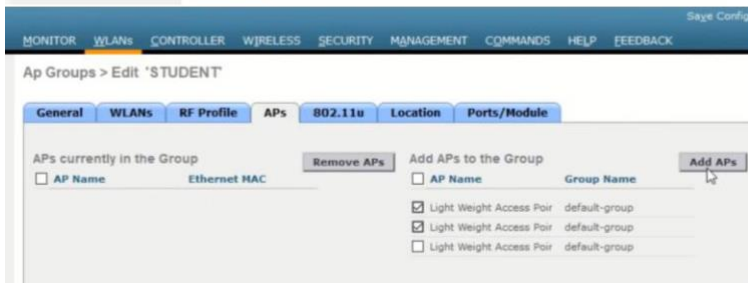
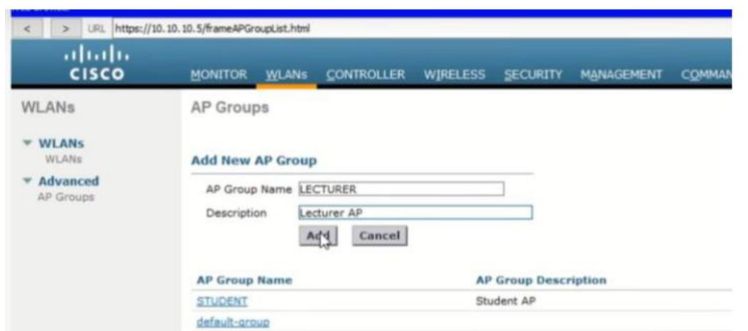
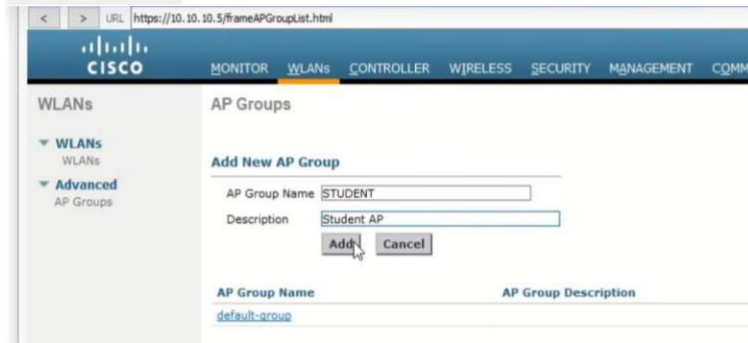
TFTP Server: 0.0.0.0

WLC Address: 10.10.10.5

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	10.10.10.1	10.10.10.2	10.10.10.100	255.0.0.0	100	0.0.0.0	10.10.10.5





Punkt dostępowy – konfiguracja jest możliwa za pomocą:

- Łączy szeregowo, uruchamiamy na komputerze emulator i podłączamy do portów COM do AP,
- Telnetu – połączenie konsolowe
- SNMP – protokół – instalujemy program do zarządzania,
- WWW – wchodzimy w przeglądarkę

Ważna jest zmiana domyślnego hasła punktu dostępowego administratora.

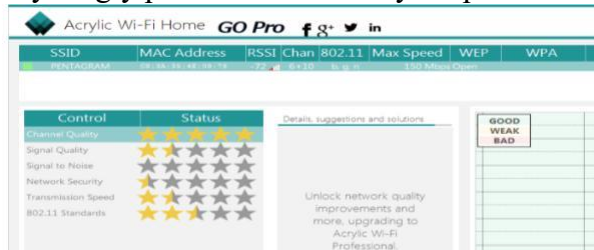
Programy do diagnozowania stanu sieci

Microsoft Network Monitor – sniffer zawarty w systemie operacyjnym Windows 2000 server i wyższych. Oferuje on najważniejsze statystyki sieciowe oraz możliwość przejrzenia przechwyconych ramek.

CommView – program idealny do tworzenie sieciowych statystyk. Możemy obejrzeć listę połączeń sieciowych i dokonać analizy pakietów. Można tu podejrzeć np. treść plików przesyłanych przez WWW.

KISMET – darmowy program wykrywający sieci WLAN i dostarczającym wiele informacji o nich np. moc sygnału czy listę klientów.

WIMAX - wireless MAN. IEEE 802.16, transmisja punkt-wielopunkt lub tworzenia topologii siatki by mogły powstawać struktury bezprzewodowych sieci. Przepływność – 100Mb/s.



Za pomocą programu Acrylic Wi-Fi Home wykonano test, którego wyniki przedstawiono na zrzucie. Na ich podstawie można stwierdzić, że dostępna sieć bezprzewodowa

A. jest nieszyfrowana.

Analizatory sieci

Analizatory są to programy do analizy statystycznej ruchu w sieci, wykonują różnorodne wykresy. Na podstawie rozkładu zajętości pasma przez stacje, protokoły czy też usługi możesz podjąć odpowiednie decyzje dotyczące optymalizacji pracy sieci – podział domen kolizji za pomocą przełączników, zastosowania dodatkowych routerów w celu podziału domen broadcastowych.

Anasil Windows

Zapewnia wgląd m.in. w statystyki błędów transmisji, ilości wolnego miejsca na dyskach, otwartych portów TCP/UDP. Możemy testować point-to-point dzięki czemu poznany opóźnienia i straty pakietów.

LanExplorer Windows - analizuje ruch, w tym obciążenie najbardziej aktywnych hostów.

Podaje kto łączył się z jakimi stronami internetowymi.

Inne przydatne programy: Visual Route (rysuje trasę datagramów IP podając ich położenie geograficzne), VNC (tightvnc.com), który umożliwia przejmowanie pulpitu dowolną stacją w sieci, na której został uruchomiony serwer VNC, Netwox – wykrywa adresy MAC, podsłuchuje ruch sieciowy, testuje router. Advanced IP Scanner – analizuje sieć LAN, wyświetla listę aktywnych urządzeń w sieci.

Programy do robienia kosztorysów i projektów sieci: RODOS, AutoCAD, Zuzia, Norma Pro, Winbud.

Zadanie poniżej – skaner portów:

```
CA\Windows\system32\cmd.exe
C:\Users\sebastian> nmap localhost
Starting Nmap 7.00 (https://nmap.org) at 2019-11-26 20:23 from kowoc.europa.jaki.c
scan stand.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
145/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIOP
1026/tcp  open  i50-or-ntera
1027/tcp  open  IIS
1029/tcp  open  ms-lsa
1030/tcp  open  iad1
1031/tcp  open  iad2
1044/tcp  open  doulliey
1234/tcp  open  hotline
2062/tcp  open  ioclap
16992/tcp open  ant-map-http
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

Przedstawione narzędzie służące do monitorowania sieci LAN to

- A. konfigurator IP.
- B. skaner portów.
- C. zapora sieciowa.
- D. konfigurator sieci.

Sniffery – programy służące do analizy ruchu sieciowego a przede wszystkim pakietów.

Analiza pakietów pozwala:

- zrozumieć charakterystykę sieci,
- sprawdzić kto znajduje się w sieci, w tym zlokalizować punkty końcowe (hosty),
- określić co powoduje wykorzystanie dostępności sieci, co spowalnia aplikacje,
- określenie godzin, w których sieć jest maksymalnie wykorzystywana,
- identyfikacja ataków i zagrożeń, ktoś może przechwytywać image i tekst,
- administrator może sprawdzać czy jakiś pracownik firmy albo uczeń nie gra w grę komputerową (gapnie się po protokole),
- wykrywanie złośliwych lub nadmiernie rozbudowanych aplikacji.

Przykładami takich programów jest Wireshark, TCPDUMP czy OmniPeek.

W Linuxie do monitorowania połączeń sieciowych służy **iftop**.

Sniffery analizują wszystkie protokoły sieciowe (IP, ICMP), protokoły warstwy transportowej (TCP/UDP), protokoły warstwy aplikacji (HTTP, DNS). Większość administratorów bierze odpowiedzialność za 1 (kable, karta sieciowa), 2 (switch) i 3 warstwę (router). Warstwa 4 jest niestety błędnie przemilczana, a tym zajmuje się głównie Wireshark. Serwer pracuje na 7 warstwie i też jest często pomijany. Warstwa 4 nie musi być problemem sama w sobie, ta warstwa poprzez TCP/UDP mówi nam by iść w górę warstw albo w dół. Wielu użytkowników zgłasza problemy z siecią a tak naprawdę nie ma to nic z tym wspólnego, problemem może być np. obciążenie serwera.

Sniffer zbiera dane binarne z sieci, karta sieciowa nasłuchuje cały ruch w segmencie sieci a nie tylko ruch, który jest kierowany do karty. Później następuje konwersja danych binarnych na postać łatwą do odczytu dla człowieka. Na końcu jest weryfikacja protokołu i danych.

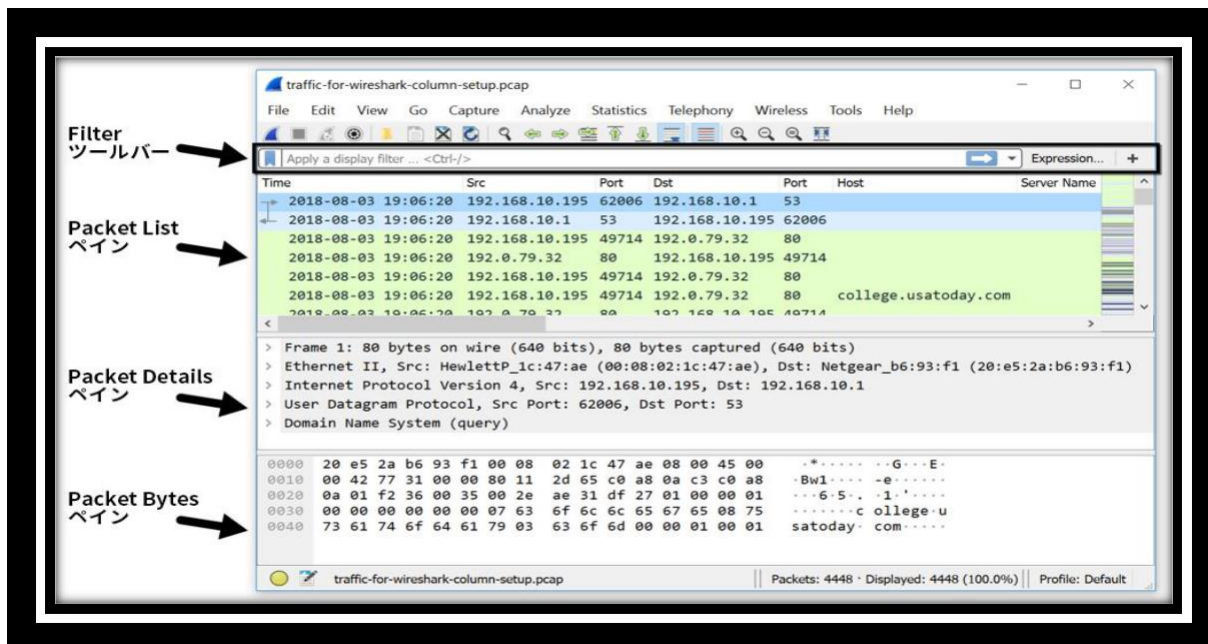
Sniffery pozwalają nam zrozumieć:

- kto rozpoczyna transmisję pakietów: klient czy serwer?
- czy protokół szyfruje komunikację?
- jaka jest kolejność danych w pakiecie?
- ile routerów musi pokonać pakiet? (po TTL, każdy router zmniejsza wartość o 1),
- co się stanie, gdy pakiet zbyt długo podróżuje do miejsca docelowego? (wykrywanie błędów),
- jak host ma zasignalizować zakończenie komunikacji?

Sniffery pozwalają zlokalizować błędy w złej adresacji routerów np. PC z sieci A chce wysłać pakiet do sieci D. Router jest źle skonfigurowane i pakiety nie docierają. Sniffer pomoże nam więc zlokalizować błąd. Sniffery analizują ruch sieci WIFI, ale również możemy je fizycznie podpiąć (PC z Wireshark) do portu przełącznika, koncentratora, routera.

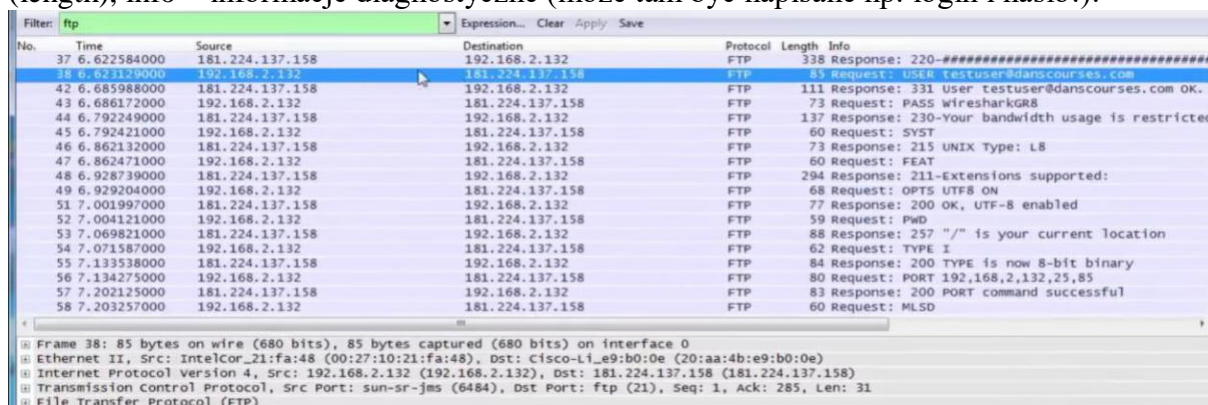
Po wpisaniu przez użytkownika sieci „google.com” następuje enkapsulacja tj. podróż pakietu od warstwy 7 do 1 a później dekapulacja do serwera google – to jest komunikacja typu unicast -1 wysyła do 1. Natomiast protokół ARP wkracza, gdy 1 PC chce nawiązać komunikację z innym: wysyła komunikaty do wszystkich (broadcast) tj. do komputerów inne niż docelowe, by odnaleźć właściwy adres MAC w domenie rozgłoszeniowej. Komputery, które nie zawierają adresu IP rozgłoszone przez ARP po prostu ignorują komunikat. ARP zapisze sobie w pamięci komu ma co wysyłać. Właściwy PC odpowiada więc: „Cześć ARP, to ja jestem PC, którego szukasz, to mój IP i MAC – wysyłaj do mnie pliki”. ARP jest ważny, bo PC w sieci często zmieniają adresy IP, ARP ma za zadanie je aktualizować a wie kto jest kto bo ma adresy fizyczne urządzeń. Gdy to nie jest robione mogłoby to doprowadzić do błędów w komunikacji. Czasem hakerzy wysyłają fałszywie zaadresowane pakiety do komputerów w celu przechwycenia ruchu lub zamulenia sieci (ataki dos).

Co to jest WinPcap w Wireshark? – to jest przełączenie karty sieciowej na tryb mieszany. W tym trybie mamy gwarancję analizy całego ruchu sieciowego. Dzięki temu sterownikowi możemy również filtrować pakiety. Każdy pakiet danego protokołu wyświetlany jest w innym kolorze (menu -> widok -> reguły kolorowania).

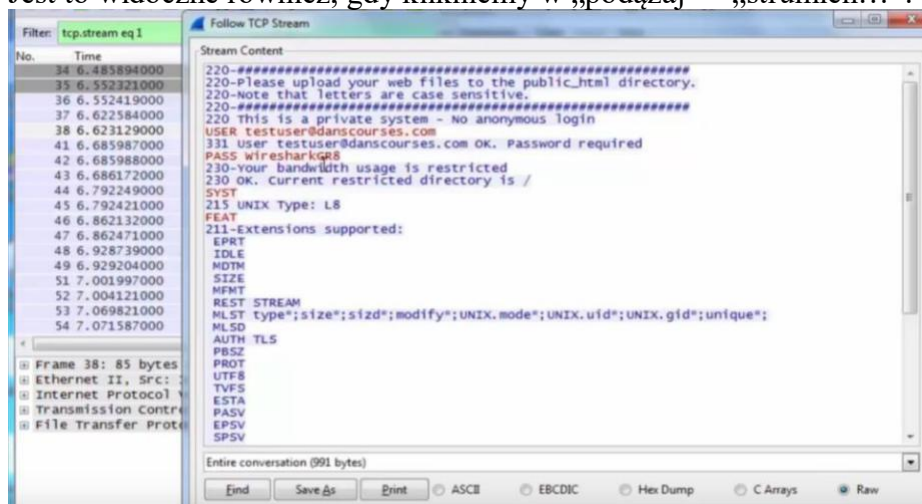


Filter – filtrowanie pakietów

Packet List – okno, które zawiera wszystkie przechwycone pakiety, mamy tam m.in. czas przechwycenia pakietu (importowany z systemu PC, również czas od momentu przechwycenia jednego pakietu do następnego), IP nadawcy, IP odbiorcy, ilość danych (length), info – informacje diagnostyczne (może tam być napisane np. login i hasło!):



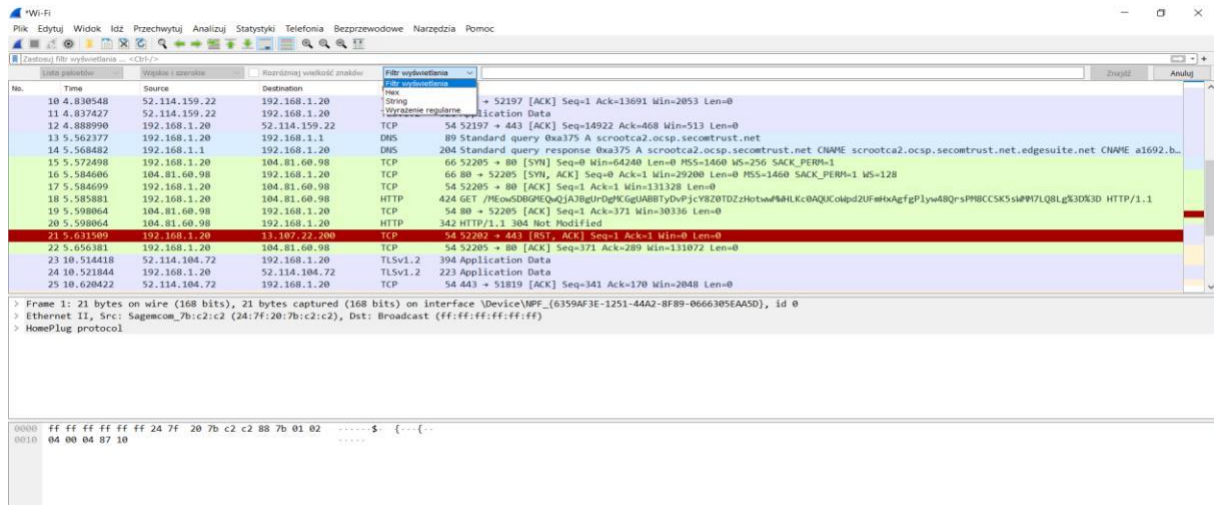
Jest to widoczne również, gdy klikniemy w „podążaj” – „strumień...”:



Packet details – środkowy panel zawiera hierarchiczną analizę zaznaczonego pakietu.

Packet bytes – wyświetla dane pakietu w postaci nieprzetworzonej.

U góry mamy również sposób filtrowania (hex oznacza zapis szesnastkowy, który powinien być oddzielony dwukropkami, string – tekstowy).



Filtrowanie w Wireshark jest korzystne pod kątem odciążenia pracy procesora. Mniej pakietów będzie filtrowanych – mniej mocy obliczeniowej będzie potrzebne, np. gdy przechwytyjemy pakiety z serwera o wielu rolach a interesuje nas tylko usługa na porcie 262. Możemy filtrować adres MAC urządzenia czy IP, możemy się dowiedzieć jaki ruch sieciowy przepływa przez dany PC wpisując w filtrze polecenie np.: host 192.168.0.5. Klikamy w „opcje przechwytywania u góry po lewej, potem wybieramy adapter (interfejs) w filtrze wpisujemy host...).

Filtrowanie w Wireshark

Filtrowanie względem DNS może pozwolić nam na odnajdowanie nazwy komputera.

Filtrowanie pakietów wychodzących i przychodzących do IP: „ip.addr”, „ip.src”, „ip.dst”, „ip.addr == 192.168.1.20”

Filtrowanie względem protokołów: „http” albo 2 „dns and http”.

Filtrowanie portów TCP albo UDP: np. „tcp.port == 443”.

Filtrowanie w przypadku utraty pakietów, problemy z TCP: „tcp.analysis.flags” – wyświetla tylko problemy (np. retransmission, packet loss). Flaga zajmuje się oznaczaniem segmentów pakietu, czyli jeśli pakiet zostanie podzielony na 100 części to każda będzie oznaczona by się nic nie zgubiło.

Filtrowanie tekstu w pakiecie, np. „TCP contains facebook” (ten „facebook powinno być widać w buforze na dole po prawej (w sekcji packet bytes) albo „udp contains facebook”.

Wykluczanie w filtrach to np. „! ARP”, „! IP”

Możemy filtrować pakiety mniejszy niż 128 bajtów – „frame.len <= 128”

Możemy np. filtrować ruch tylko do 1 adresu ip lub 2.

Operator	Opis
==	równość
!=	nierówność
>	wiekszy niż
<	mniejszy niż
>=	wiekszy lub równy
<=	mniejszy lub równy

```
ip.addr==192.168.0.1 or ip.addr==192.168.0.2
```

Statystyki -> Endpoint – pokazuje jakie urządzenia są podpięte do naszej sieci. **Sprawdzić i porównać z ipconfig /all!!!!**

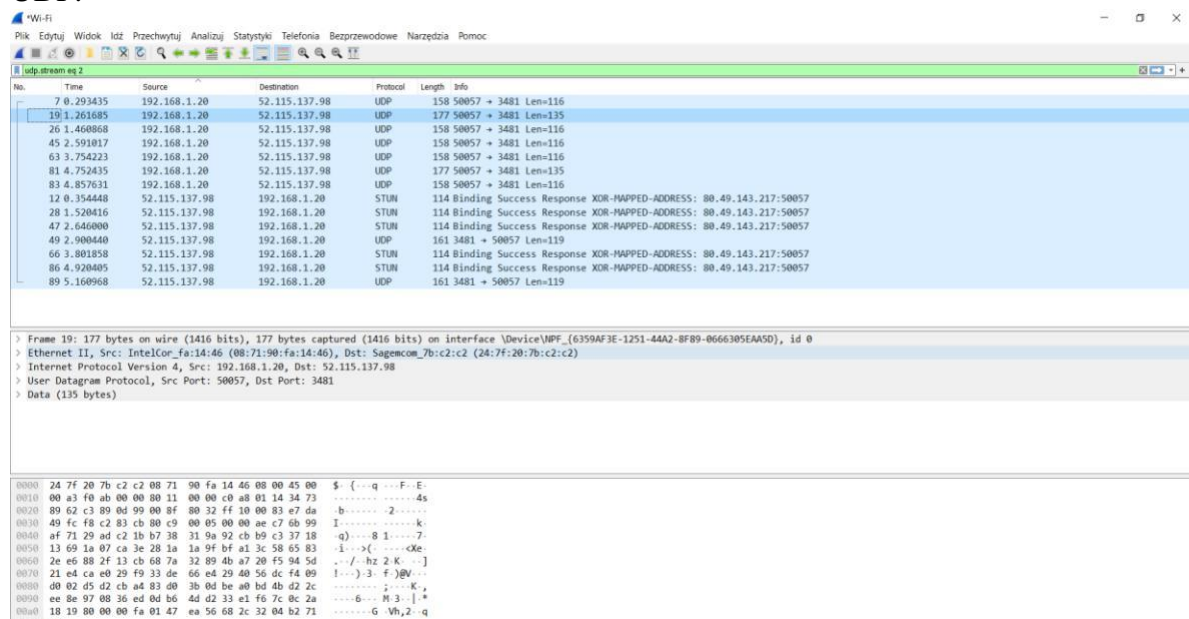
Statystyki -> Conversations -> ipv4 – pokazuje które urządzenie końcowe zużywa najwięcej bajtów.

Statystyki --> hierarchia protokołów. Sprawdza które protokoły statystycznie wykorzystują najwięcej protokołów, np. gdy zwyczajowo mamy wykorzystywany ARP w 10% a jednego dnia wyskoczy nam 60% to znaczy, że dzieje się coś niepokojącego.

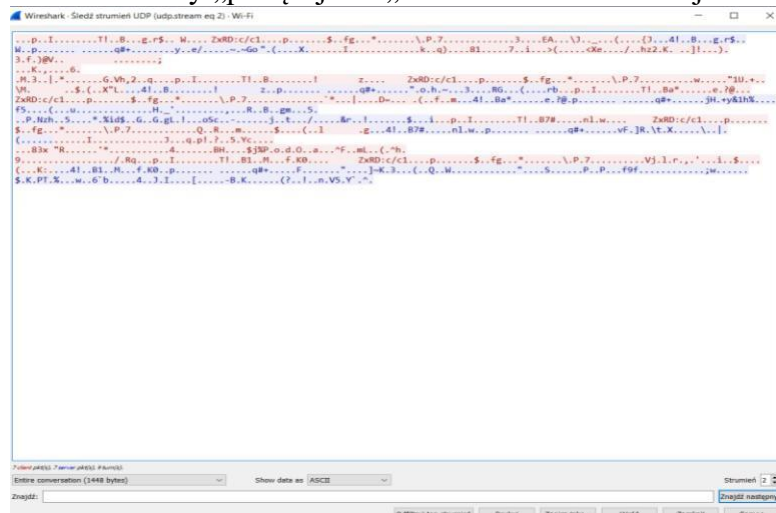
W routerze mamy 2 główne rodzaje komunikacji (wchodzimy przez Putty):

- SSL to komunikacja zaszyfrowana pomiędzy komputerami, jeśli część jest odsłonięta to znaczy, że zabezpieczenia nie działają dobrze.

- Telnet – niezasyfrowana komunikacja pomiędzy komputerami, jeśli nie ma tego protokołu to dobrze, to narzędzie nasłuchuje niezabezpieczone hasła i loginy do routera. Spójrzmy na przykład poniżej. Prawym kliknięciem myszy otworzyliśmy pakiet protokołu UDP.



Potem klikamy „podążaj” -> „strumień UDP”. Tekst jest zaszyfrowany.



W Telnetcie zarówno hasło jak i login byłoby widoczne. Tekst na czerwono powyżej to ruch ze źródła do celu a na niebiesko odwrotnie. Kolor zależy kto zainicjował komunikację.

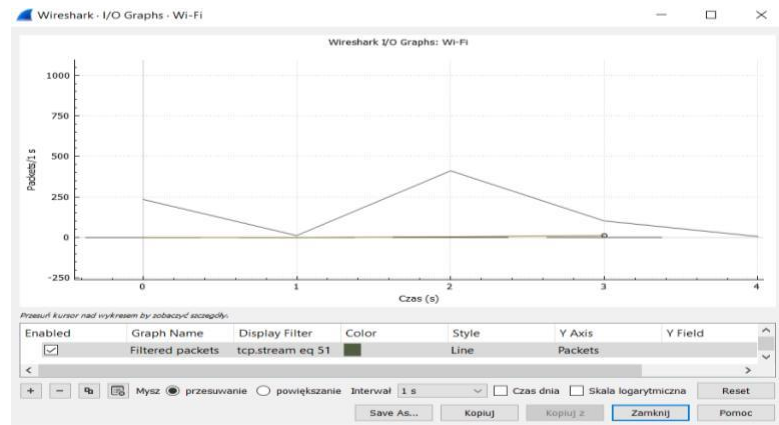
Większość komunikacji to 2 urządzenia, zaczynające się od GET aż do komendy 200 OK serwera (oznacza powodzenie żądania).

Długość pakietu, duże pakiety oznaczają po prostu transfer danych („statystyki” -> „długość pakietu”, małe pakiety to tylko polecenia kontrolne - do 1460 bajtów oznacza brak transmisji plików, do 54 bajtów mają pakiety kontrolne TCP takie jak ACK, SYN (1 pakiet wysłany przez klienta do serwera), RST, FIN:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	766	395,52	54	1514	0,1867	100%	1,5300	2,891
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	355	56,83	54	78	0,0865	46,34%	0,9000	2,894
80-159	72	109,33	82	157	0,0175	9,40%	0,2800	0,000
160-319	46	209,39	161	312	0,0112	6,01%	0,1400	0,079
320-639	139	479,32	322	625	0,0339	18,15%	0,3600	0,000
640-1279	66	1028,86	659	1273	0,0161	8,62%	0,2200	2,922
1280-2559	88	1485,85	1316	1514	0,0214	11,49%	0,2100	2,921
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

Po co nam ta wiedza? By sprawdzać np. czy pracownicy nie siedzą na Netflixie lub czy ktoś nie podpiął się pod sieć.

Okno I/O graphs (w panelu statystyki) bada przepustowość sieci. Jest do najlepsze do analizy podczas pobierania jakiegoś pliku.



Graf przepływu analizuje czas od momentu zapytania klienta do czasu otrzymania pliku. Czas do zaakceptowania to 0,05 sekundy, poniżej mamy 0,012 sekundy.

The packet list window shows a list of captured packets. The first few packets are SYN and SYN-ACK. The packet list includes columns for Time, Source, Destination, Protocol, Length, and Info. The info column shows details for each packet, such as 'Ethernet II, Src: Intel(R) Dual Band Wireless-AC, Dst: 192.168.1.100, Protocol: TCP, Seq: 3399, Win: 0, Len: 0' for the SYN packet and 'Ethernet II, Src: Intel(R) Dual Band Wireless-AC, Dst: 192.168.1.100, Protocol: TCP, Seq: 3399, Win: 0, Len: 0' for the SYN-ACK packet.

W Wireshark musimy zwracać szczególną uwagę na pakiety zaznaczone na kolor czarny z tekstem na czerwono – często są to opóźnienia w komunikacji na linii klient-serwer.

Jak zbadać, czy serwer jest obciążony? Klikamy w pakiet SYNC (żądanie klienta to serwera, patrzemy w IPV4 (Packet Details) jaki jest Time to Live), potem klikamy w kolejny pakiet tj w odpowiedź serwera (SYNC-ACK) i porównujemy w IPV4 (Packet details) jaki jest Time to live. Analiza TTL jest ważna, ponieważ TTL wędruje on od routera do routera – gdzieś może się po drodze zgubić.