PODSTAWY SIECI KOMPUTEROWYCH

Co-funded by the
Erasmus+ Programme
of the European Union

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

Spis treści

1. Wprowadzenie

Cyberbezpieczeństwo, czym jest? Na czym polega i dlaczego jest tak ważne? W czasach, w których technologia nie odstępuje nas na krok i mamy z nią do czynienia praktycznie wszędzie, nie możemy zapominać o naszym cyberbezpieczeństwie w tym jakże wygodnym cyfrowo świecie. W sieci nie jesteśmy nie widoczni, a nasze aktywności pozostawiają po nas różne ślady bądź informację. Praktycznie codziennie korzystamy z udogodnień Internetu czy to na serwisach społecznościowych, forach czy wszelakich platformach sprzedażowych. Gdzie dzielimy się swoimi danymi osobowymi, finansowymi, przesyłamy numery kont, płacimy za pomocą kart, telefonów, różnych walut cyfrowych. Jakie zagrożenia czyhają w Internecie? Kradzieże tożsamości, klonowanie kart płatniczych, utrata prywatnych plików/danych, wyłudzenia z kont bankowych, oszustwa. W życiu dbamy o swoje bezpieczeństwo, pilnujemy się, kupujemy leki, przewidujemy. Dlaczego nie robimy tego w sieci? Ilu z Was ma zainstalowanego antywirusa na swoim komputerze? Wszyscy? A na swoim telefonie? Ktokolwiek? Tutaj powinniśmy sobie zadać pytanie, czy rzeczywiście większość czasu w sieci spędzamy przed ekranem komputera czy może jednak swojego telefonu? Wg różnego rodzaju statystyk, już ponad 70% wszelkiego ruchu w sieci pochodzi z urządzeń mobilnych, przede wszystkim z naszych smartphonów. Czy nie zdarzyło się Wam kupić czegoś telefonem, bądź za jego pośrednictwem wprowadzać swoje dane rozliczeniowe do różnych transakcji? Właściwie przygotowane urządzenia do korzystania z sieci to tylko połowa sukcesu, drugim czynnikiem gwarantującym względne bezpieczeństwo jest świadomość użytkownika Internetu. Możesz być najlepiej przygotowany i mieć najlepszy sprzęt, ale jednak bez odpowiedniego know-how możesz narobić sobie sporo niepotrzebnych i niemiłych problemów.

1.1. Komunikacja w sieci

Obecnie niewielu potrafi wyobrazić sobie otaczający nas świat bez komputerów, telefonów i wielu innych urządzeń elektroniki użytkowej. Urządzenia te oferują nam mnóstwo funkcji i możliwości ułatwiających wykonywanie codziennych czynności, a także pomocnych w pracy i nauce. Wiele z tych funkcji byłoby bezużytecznych bez ważnego aspektu, możliwości szybkiej komunikacji i wymiany danych.

Dzięki tej możliwości jesteśmy w stanie w kilka sekund dotrzeć do znajomych, którzy aktualnie są na drugim końcu świata, w kilka sekund zapłacić rachunki za prąd, czy kupić nowe trampki bez wychodzenia z domu. Oczywiście nie będę tutaj omawiał wszystkich zalet dostępu do Internetu, ponieważ nie jest to główny temat kursu, ale mam nadzieję, że zdajesz sobie sprawę, że wszystko, co możesz zrobić ze swoim komputerem lub smartfonem, ma jedną wspólną cechę. Tym mianownikiem jest, a właściwie jest, sieć komputerowa, która powstała kilkadziesiąt lat temu i jest fundamentem dzisiejszego Internetu.

Czym jest dziś Internet? To nic innego jak sieć komputerowa, bardzo rozbudowana, z wieloma podłączonymi urządzeniami, ale to wciąż sieć.

2. Podstawowe pojęcia

Zdefiniujmy podstawowe pojęcia związane z sieciami komputerowymi:

Sieć komputerowa - Zbiór urządzeń, takich jak komputery, drukarki, telefony i telewizory, które są ze sobą połączone w celu wymiany danych. W celu połączenia urządzeń wykorzystuje się medium transmisyjne, a do transmisji danych wykorzystywany jest protokół komunikacyjny.

Adres IPv4 - Jest to liczba 32-bitowa, wprowadzana w postaci dziesiętnej dla ułatwienia obsługi (np. 192.168.31.190), umożliwiająca identyfikację urządzeń i adresowanie danych
w sieci.

HOST - Jest to urządzenie o adresie IP, które jest źródłem lub odbiorcą danych przesyłanych przez sieć, czyli odbiera dane z innych urządzeń lub takie dane wysyła. Termin host bywa używany zamiennie z terminem urządzenie końcowe, gdyż zwykle odnosi się do komputera, tabletu lub smartfona, czyli urządzenia, z którym użytkownik sieci ma bezpośredni kontakt.

Klient - Urządzenie, a dokładniej jego oprogramowanie, korzysta z usług świadczonych przez serwer. Najpopularniejszym klientem jest dziś przeglądarka internetowa, która umożliwia przeglądanie zawartości stron internetowych hostowanych przez serwer WWW. Przykładem klienta może być również program FileZilla, który umożliwia wymianę plików przez Internet oraz wszelkiego rodzaju programy pocztowe, ułatwiające korzystanie z poczty. Klientami będą także konsole do gier czy smartfony, o ile oczywiście będą połączeni z Internetem.

Serwer - Jest to komputer z zainstalowanym dedykowanym specjalistycznym oprogramowaniem do obsługi innych komputerów. Usługą, którą może świadczyć serwer, jest na przykład strona internetowa, poczta e-mail lub zasób plików. Serwerem może być dowolny komputer, na którym takie oprogramowanie jest zainstalowane i skonfigurowane, np. APACHE, który służy do utrzymywania i udostępniania stron internetowych, czy MySQL, który jest systemem zarządzania bazami danych. Serwerem jest zazwyczaj dedykowany komputer o dużej mocy obliczeniowej, który jest w stanie obsłużyć wiele połączeń i zapytań jednocześnie.

Medium transmisyjne - Innymi słowy medium będące elementem sieci, za pośrednictwem którego urządzenia komunikują się ze sobą i wymieniają dane. Tym medium może być kabel miedziany, kabel światłowodowy i fale radiowe (WiFi).

Protokół komunikacyjny - Jest to sposób lub język komunikacji i wymiany danych między urządzeniami, który określa reguły i zasady tej komunikacji.

Internet - Jest to zestaw połączonych ze sobą sieci rozległych, które tworzą globalną sieć komputerową. Początki Internetu sięgają powstania sieci ARPANET pod koniec lat sześćdziesiątych, a pierwsze łącze internetowe w Polsce uruchomiono we wrześniu 1990 roku. Internet jest postrzegany przez wielu jako zbiór stron do przeglądania, ale tak nie jest, ponieważ Internet jest zbiorem wielu szerokich sieci rozsianych po całym świecie, a strony internetowe są specyficznymi usługami sieciowymi.

Intranet - To prywatna sieć wewnętrzna, która wykorzystuje dokładnie te same standardy komunikacji (protokoły) co Internet, ale ma dostęp tylko do autoryzowanych użytkowników, takich jak pracownicy danej firmy. W większości przypadków dostęp do intranetu, czyli tej wewnętrznej sieci firmowej, odbywa się za pośrednictwem strony internetowej, dlatego mówi się, że komunikacja wykorzystuje te same standardy co Internet.

Ekstranet - to rozbudowana różnorodność sieci intranetowych, które umożliwiają dostęp do jej zasobów nie tylko pracownikom danej firmy, ale także innym użytkownikom.

DNS (Domain Name System) - Usługa sieciowa, której zadaniem jest zmiana nazwy czytelnej dla człowieka, tzw. nazwy mnemonicznej, na adres IP urządzenia w sieci. Jest to podstawowa usługa internetu, polegająca na zmianie adresów stron internetowych na odpowiadające im adresy IP serwerów, na których te strony są przechowywane, np. zmiana adresu internetowego onet.pl na adres IP 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) - to protokół automatycznej konfiguracji, który przypisuje hostowi adres IP, maskę podsieci lub adres bramy domyślnej. Jest to najczęstsza metoda przypisywania adresów IP komputerom w sieci, ponieważ nie wymaga ręcznej konfiguracji adresu IP na każdym komputerze.

3. Jednostki danych w sieciach

Podstawową jednostką używaną w informatyce do przechowywania danych jest 1 bit [b].
Z drugiej strony w sieciach komputerowych jednostka bitów na sekundę jest używana do określenia przepustowości (szybkości) sieci, wyrażonej w b/s lub bps (bitach na sekundę).

Oczywiście 1 bit/s jest mały, więc aby użyć wielokrotności tej jednostki do określenia rozmiaru pliku, pojemności dysku lub pamięci operacyjnej, niezależnie od bitów, a nie bajtów, te wielokrotności to:

1. Kilobit [Kb],
2. Megabit [Mb],
3. Gigabit [Gb],
4. terabit [Tb].

Ponieważ w sieci komputerowej jednostka jest w bitach, w przeciwieństwie do rozmiaru pliku lub pojemności dysku, gdzie zamiast bitów[b] używane są bajty[B], pojawia się tutaj problem konwersji, czyli konwersji jednostek.

1 bajt[B] równa się 8 bitom[b] Więc jeśli chcemy, aby rozmiar pliku w bajtach był zapisany w bitach, musimy pomnożyć liczbę bajtów przez 8. Na przykład, jeśli chcemy obliczyć, ile megabitów zawiera plik o wielkości 3 MegaBajta, mnożymy jego rozmiar przez 8. Wynik to 24 MB.

3 MB • 8 = 24 MB

W przypadku konwersji odwrotnej, czyli z bitów na bajty, musimy wykonać odwrotność mnożenia, czyli dzielenia. Na przykład: plik o rozmiarze 40 Mb zostanie przekonwertowany na 5 MB.

40 MB ÷ 8 = 5 Mb

Możliwość przeliczania jednostek najlepiej nadaje się do wykonywania obliczeń na konkretnych przykładach. Poniżej opisano dwa rozwiązania.

Przykład 1

Zakładając, że przepustowość naszego łącza jest stała i sięga 300 Mb/s, policzmy, ile danych pobierzemy z Internetu w ciągu dwóch godzin.

dane:

Czas: 2 godziny

Przepustowość łącza: 300 Mb/s

Oblicz:

1. Sekundy minuty mnożymy przez minuty:

120 minut • 60 sekund = 7200 sekund

2. Konwertujemy jednostkę transferu danych z megabitów na megabajty na sekundę:

300MB/s ÷ 8 = 37,5MB/s

3. Mnożymy przepustowość przez czas:

37,5 MB/s • 7200 sekund = 270000 MB ~ 270 GB

Odpowiedź na przykład 1: W ciągu dwóch godzin pobierzemy 270 GB.

Przykład 2

Obliczmy czas potrzebny na pobranie pliku o rozmiarze 5 GB, zakładając, że przepustowość naszego połączenia jest stała i osiąga 300 Mb/s.

dane:

Rozmiar pliku: 5 GB

Przepustowość łącza: 300 Mb/s

Oblicz:

1. Przeliczamy jednostkę transmisji danych z megabitów na megabajty na sekundę:

300 Mb/s ÷ 8 = 37,5 MB/s

2. Konwertuj jednostki zapisywania plików z gigabajtów na megabajty:

5 GB => 5120 MB

3. Dzielimy rozmiar pliku przez przepustowość:

5120 MB ÷ 37,5 MB / s = 136,5 sekundy ~ 2 minuty 16 sekund

Odpowiedź na przykład 2: Ściągniemy plik 5 GB przez łącze 300 Mb/s w około 2 minuty 16 sekund.

ZADANIA DO SAMODZIELNEGO WYKONANIA

Oblicz, kiedy zawartość płyty DVD (4,7 GB) może być przesyłana łączem o przepustowości 50 Mb/s.

Oblicz, ile danych można przesłać łączem 500 Mb/s w 15 minut.

3.1. Media transmisyjne

Media transmisyjne to niezwykle istotna kwestia związana z sieciami komputerowymi. Powodów jest wiele, z których najważniejszą jest to, że wybór odpowiedniego medium jest podstawą i gwarancją normalnego i efektywnego działania sieci komputerowych.

3.2. Medium

Innymi słowy medium będące elementem sieci, za pośrednictwem którego urządzenia komunikują się ze sobą i wymieniają dane. Tym medium może być kabel miedziany, kabel światłowodowy i fale radiowe (Wi-Fi).

PODZIAŁ MEDIÓW TRANSMISYJNYCH

RODZAJ	**KABEL MIEDZIANY**		**KABEL ŚWIATŁOWODOWY**	
TYP	**KABEL KONCENTRYCZNY**	**KABEL TYPU SKRĘTKA**	**ŚWIATŁOWÓD JEDNOMODOWY**	**ŚWIATŁOWÓD WIELOMODOWY**

3.3. Kabel koncentryczny

1. Budowa:

· rdzeń miedziany,

· izolacja z tworzywa sztucznego,

· ekran miedziany,

· Koszulka zewnętrzna.

Kończy się złączem o nazwie BNC. Czasami na końcu kabla koncentrycznego znajdujemy również tzw. terminator BNC, którego zadaniem jest usuwanie odbić z sygnału przesyłanego przez kabel.

2. Rodzaje:

Istnieją dwa rodzaje kabla koncentrycznego: cienki kabel koncentryczny i gruby kabel koncentryczny. Różnice między tymi dwiema odmianami są następujące:

RODZAJ	**GRUBOŚĆ**	**DŁUGOŚĆ MAX**	**STANDARD SIECI**	**MAKSYMALNA PRZEPUSTOWOŚĆ**
CIENKI	5 mm	185 M	10base-2	10 Mb/s
GRUBY	10 mm	500 M	10base-5	10 Mb/s

Warto zauważyć, że kabel koncentryczny nie jest już wykorzystywany przy budowie nowych sieci. Został on zastąpiony bardziej wydajnymi rozwiązaniami, takimi jak skrętka
i światłowody.

3.4. Kabel skrętka

1. Budowa:

· 8 drutów miedzianych splecionych w 4 pary,

· Koszulka zewnętrzna.

Jest zakończony wtykiem RJ45, znanym również jako 8P8C.

W zależności od rodzaju skrętki występują również folie i ekrany ochronne, które chronią kabel przed niepożądanymi elementami mogącymi wpływać na transmisję danych, takimi jak fale elektromagnetyczne.

2. Typy skrętki:

· UTP – skrętka nieekranowana,

· FTP – skrętka ekranowana folią,

· STP – skrętka ekranowana siatką.

W praktyce możemy spotkać się z różnymi wariantami powyższych typów, z których najważniejsze to:

· **U/UTP – skrętka nieekranowa**

· **F/UTP – skrętka foliowana**

· **U/FTP – skrętka z każdą parą w osobnym ekranie z folii,**

· **F/FTP – skrętka z każdą parą w osobnym ekranie z folii i dodatkowo cała wiązka również w ekranie z folii**

· **S/FTP – skrętka z każdą parą w osobnym ekranie z folii i dodatkowo cała wiązka w ekranie z siatki**

Najpopularniejszym materiałem stosowanym w ekranowaniu skrętek jest folia poliestrowa pokryta warstwą aluminium i miedzi.

Rodzaj skrętki, którą należy dobrać do budowy sieci, zależy od miejsca działania sieci oraz poziomu zakłóceń elektromagnetycznych występujących w danej lokalizacji. W małych sieciach lokalnych, czy to w szkole, czy w domu, podstawowy typ UTP jest najczęściej używany, ponieważ jest wystarczający dla tak małej sieci, a także jest najtańszym rodzajem skrętki.

3. Kategorie kabla typu skrętka

Oprócz typów skrętek istnieją klasy, które definiują m.in. standardy sieciowe, w jakich można je stosować.

KATEGORIA	STANDARD SIECI
3	Ethernet 10Base-T
5/5e	FastEthernet 100Base-TX GigabitEthernet 1000Base-T
6	GigabitEthernet 1000Base-T
6a	10-GigabitEthernet 10GBase-T
7	10-GigabitEthernet 10GBase-T

4. Parametry techniczne

· Tłumienie sygnału - to stosunek napięcia wyjściowego do wejściowego, wyrażony w decybelach [dB]

· Propagacja sygnału - Jest to prędkość impulsu elektrycznego w stosunku do prędkości światła, wyrażona w procentach [%]

· Rezystancja - jest to rezystancja przewodu na prąd wyrażona w omach [Ω]

· Near Crosstalk (NEXT) — jest to zakłócenie w danym zestawieniu spowodowane transmisją danych w sąsiednim zestawieniu

Również z punktu widzenia montażu ważnym parametrem jest promień gięcia kabla, który dla większości rozwiązań jest 4-krotnością jego średnicy zewnętrznej.

3.5. Kabel światłowodowy

Zupełnie inny od omówionego wcześniej medium transmisyjnego jest kabel światłowodowy, ze względu na różne materiały użyte do budowy rdzenia. W przypadku kabla koncentrycznego i skrętki, rdzeniem lub drutem jest miedź, a w przypadku kabli światłowodowych mamy do czynienia z włóknem szklanym. Zastosowanie włókna szklanego jako materiału budulcowego rdzenia wymaga również zastosowania różnych rodzajów sygnałów transmisyjnych. W przypadku mediów miedzianych jest to prąd elektryczny,
w przypadku światłowodu światło, najczęściej stosowanym rodzajem jest światło podczerwone.

1. Budowa:

- Rdzeń - ma wyższy współczynnik załamania światła,
- Powłoka - ma niższy współczynnik załamania światła,
- powłoka lakiernicza chroniąca powłokę,
- Powłoka wzmacniająca chroniąca rdzeń podczas montażu,
- powłoka zewnętrzna.

Możemy również znaleźć następujące rodzaje złączy:

- LC
- MT – RJ
- MU
- DIN

2. Rodzaje światłowodów:

Podobnie jak w przypadku miedzi i światłowodu, możemy omówić różne rodzaje tego medium. Najczęstsze podziały to światłowody jednomodowe i wielomodowe.

W przypadku światłowodów jednomodowych przez szklany rdzeń przechodzi tylko jedna wiązka światła, co powoduje tzw. zjawisko rozmycia sygnału, czyli jego osłabienia.

Przy użyciu tego typu światłowodu można przesyłać sygnały na duże odległości bez sprzętu wzmacniającego sygnał.

W światłowodzie wielomodowym większa część wiązki jest przesyłana przez rdzeń, co skutkuje wyższym stopniem rozmycia sygnału w porównaniu do światłowodu jednomodowego. Dzieje się tak, ponieważ każda wiązka wysyłana przez rdzeń musi podróżować inną ścieżką od nadawcy do odbiorcy.

Dlatego światłowód wielomodowy jest używany na krótkich dystansach, do kilku kilometrów.

Kolejną różnicą między światłowodem jednomodowym a wielomodowym jest stosowana średnica rdzenia. W przypadku światłowodu jednomodowego jest to od 8 do 10 mikrometrów [µm], a w przypadku światłowodu wielomodowego jest to 50 lub 62,5 mikrometrów.

3.6. Podsumowanie

Media miedziane

ZALETY	WADY
Tanie w zakupie	**Krótkie odcinki między węzłami sieci**
Prosta diagnostyka i naprawy usterek	**Podatne na zakłócenia elektromagnetyczne**
Bezproblemowy montaż i instalacja	**Wolniejsze niż światłowody**

Media światłowodowe

ZALETY	WADY
Zdecydowanie szybsze	**Skomplikowany montaż i instalacja**
Praktycznie odporne na zakłócenia elektromagnetyczne	**Zdecydowanie droższy w zakupie ze względu na potrzebne sprzęty**
Przesyła dane na długich odcinkach	**Rozmycie sygnału**

Media bezprzewodowe

W przypadku mediów bezprzewodowych stosuje się kilka rozwiązań, ale faktycznie wykorzystuje się tylko jedno z nich, fale radiowe. Znana technologia Wi-Fi wykorzystuje to medium do transmisji danych.

Fale radiowe to promieniowanie elektromagnetyczne w zakresie częstotliwości od 3 Hz do około 3 THz. Źródła fal radiowych mogą być naturalne lub wytworzone przez człowieka, na przykład te emitowane przez komórkowe stacje radiowe. Ich głównym celem jest przesyłanie informacji, aw przypadku telekomunikacji danych. Istnieje kilka rodzajów fal radiowych, przy czym do transmisji danych wykorzystuje się fale długie, średnie, krótkie i ultrakrótkie.

Omawiając fale radiowe, warto wspomnieć o standardach stosowanych w sieciach bezprzewodowych. Są ważne z punktu widzenia wyboru odpowiedniego routera Wi-Fi.

STANDARD	CZĘSTOTLIWOŚĆ	MAKSYMALNA PRZEPUSTOWOŚĆ
802.11a	5 GHz	54 Mb/s
802.11b	2,4 GHz	11 Mb/s
802.11g	2,4 GHz	54 Mb/s
802.11n	2,4 GHz | 5 GHz	150 Mb/s | 600 Mb/s
802.11ac	5 GHz	Kilka Gb/s

4. Rodzaje sieci komputerowych

Sieci komputerowe można podzielić na różne sposoby, biorąc pod uwagę różne kryteria. Podstawowym standardem podziału sieci jest podział według obszaru, na którym działa sieć, a więc podział według obszaru (zasięgu) sieci wygląda następująco:

Sieć lokalna (**LAN -** Local Area Network) **—** sieć obejmująca najmniejszy obszar, na przykład studio, szkoła lub kilka budynków szkolnych. Sieć LAN pojawia się również w Twoim domu, jeśli używasz więcej lub jednego komputera.

Sieć miejska (**MAN –** Metropolitan Area Network) **—** sieć obejmująca obszar większy niż pomieszczenie lub budynek. Sieć MAN jest rozłożona na terenie miasta lub aglomeracji.

Sieć rozległa (**WAN -** Wide Area Network) **—** rozległa sieć łącząca sieci LAN i MAN.

Oprócz standardów regionalnych, sieci można również podzielić według ich architektury. Rozróżniamy sieci o architekturze klient-serwer i peer-to-peer.

W architekturze klient-serwer istnieje co najmniej jeden komputer obsługujący użytkowników sieci (są to serwery) oraz wiele komputerów korzystających z usług serwera (są to klienci). Używamy architektury klient-serwer podczas przeglądania stron internetowych, wysyłania e-maili czy pracy z bazami danych.

Inaczej jest w przypadku architektury peer-to-peer, znanej również jako Peer2Peer (P2P).
W tym przypadku usługa nie jest świadczona przez jeden lub więcej komputerów, ale przez wiele komputerów z tymi samymi prawami. Każdy komputer w sieci może jednocześnie korzystać i udostępniać zasoby. Korzystając z usług udostępniania plików, takich jak BitTorrent, korzystamy z architektury peer-to-peer.

4.1. Topologie sieci

Topologię sieci dzielimy na fizyczną, która definiuje sposób połączenia urządzeń ze sobą,
oraz logiczną, która opisuje sposób przesyłania danych między urządzeniami. Każda, nawet najmniejsza sieć komputerowa, posiada fizyczną i logiczną topologię, która definiuje sposób podłączenia urządzeń oraz sposób przesyłania danych.

Topologia sieci komputerowej

Definiuje relacje między urządzeniami w sieci, połączenia między nimi oraz sposób przepływu danych.

4.2. Topologie fizyczne

Do fizycznych topologii sieci zaliczamy topologię:

- Magistrali (ang. Bus),
- Pierścienia (ang. Ring),
- Gwiazdy (ang. Star).

Są to podstawowe topologie, które są podstawą do budowania rozszerzonych topologii gwiazdy i siatki w dużych sieciach.

Fizyczna topologia magistrali

Topologia magistrali charakteryzuje się tym, że wszystkie urządzenia są podłączone do wspólnego medium transmisyjnego. Powszechnym medium transmisyjnym w tej topologii jest kabel koncentryczny. Jedną z wad tej topologii jest niska przepustowość (do 10 Mb/s).

Ta topologia służy do budowy lokalnej sieci komputerowej. Celowo używam tutaj słowa „było", ponieważ nie jest już powszechnie używane. Oprócz niskiej przepustowości jest również bardzo podatny na awarie sieci. W momencie zerwania kabla koncentrycznego cała sieć przestaje działać. Niewątpliwą zaletą zastosowania tej topologii jest niski koszt wdrożenia, gdyż nie ma potrzeby stosowania setek metrów kabla ani żadnego sprzętu pośredniczącego.

Fizyczna topologia pierścienia

W topologii pierścienia każde urządzenie jest połączone z dwoma sąsiadami, tworząc zamknięty okrąg. Podobnie jak w przypadku topologii magistrali, ta konstrukcja nie wykorzystuje dużej liczby kabli i dodatkowego wyposażenia.

Ponadto można stosować różne media transmisyjne, od kabla koncentrycznego przez skrętkę miedzianą po kabel światłowodowy. Wadą tej topologii jest to, że przerwanie medium lub awaria jednego z komputerów może spowodować przerwanie pracy całej sieci. Aby temu zapobiec, stosuje się tzw. podwójne pierścienie, czyli podwojenie liczby połączeń między urządzeniami. Wtedy taka topologia nazywana jest topologią podwójnego pierścienia.

Fizyczna topologia gwiazd

W topologii gwiazdy urządzenia są połączone z centralnym punktem, czyli punktem dostępu do sieci. W przeszłości ten punkt był używany jako koncentrator, ale teraz używany jest przełącznik. Jest to najczęstsza topologia w sieciach lokalnych, ponieważ jest łatwa do projektowania, budowania i skalowania, odporna na awarie i łatwa w zarządzaniu.

Kolejną zaletą jest to, że można go zbudować z wykorzystaniem różnych mediów transmisyjnych, takich jak skrętka miedziana, kabel światłowodowy lub fale radiowe (WLAN). Jednak istotną wadą może być koszt budowy, ponieważ wymagane jest dodatkowe wyposażenie (przełączniki) i wiele metrów kabla.

4.3. Topologie logiczne

Logiczna topologia sieci obejmuje:

- peer to peer,
- przekazać token,
- Wielokrotny dostęp.

Topologia logiczna punkt-punkt

W topologii punkt-punkt dane są przesyłane tylko z jednego urządzenia do drugiego. Urządzenia te można łączyć ze sobą bezpośrednio, np. komputer z przełącznikiem,
lub pośrednio, na duże odległości, za pomocą urządzenia pośredniego, np. łącząc dwa routery oddalone od siebie o kilka kilometrów.

W obu przypadkach możemy mówić o logicznych połączeniach punkt-punkt. Jest to topologia logiczna, często używana w sieciach LAN, które wykorzystują fizyczną topologię gwiazdy.

Logiczna topologia przekazywania tokena

W topologii z przekazywaniem tokena dane są przekazywane sekwencyjnie do urządzeń sieciowych. Urządzenie, które otrzymuje partię danych, analizuje je, aby sprawdzić, czy na nią wskazuje. Jeśli dane nie są dla niego przeznaczone, przekaże je do sąsiedniego urządzenia. W ten sposób wszystkie urządzenia przesyłają dane między urządzeniami źródłowymi i docelowymi.

Topologia logiczna wielokrotnego dostępu

Topologia wielodostępu (czasami nazywana również topologią rozgłoszeniową lub logiczną magistrali) umożliwia urządzeniom w sieci komunikację za pośrednictwem jednego fizycznego medium transmisyjnego. Przeważnie był używany z fizycznymi topologiami magistrali i gwiazdami na wczesnych etapach jego rozwoju, kiedy koncentratory były nadal używane jako punkty dostępu do sieci.

Każde urządzenie w tej topologii widzi dane przesyłane przez sieć, ponieważ są one wysyłane do wszystkich urządzeń, ale tylko określone urządzenie, do którego dane są adresowane, może je zinterpretować. Ponieważ urządzenia w sieci korzystają ze wspólnego medium, konieczne jest wprowadzenie mechanizmów kontroli dostępu do tego medium, są to: CSMA/CD, CSMA/CA oraz token pass.

Metoda dostępu do łącza (sieci)

Metoda CSMA/CD, metoda wykrywania kolizji, polega na monitorowaniu stanu łącza. Jeżeli urządzenie, które ma rozpocząć transmisję, wykryje, że łącze jest nieaktywne, rozpoczyna taką transmisję. Jeśli podczas przesyłania danych wykryje, że inne urządzenie w sieci również wysyła swoje dane, przesyłanie zostanie przerwane. Po chwili ponów próbę transferu. Starsze wersje Ethernetu wykorzystują ten mechanizm.

Metoda CSMA/CA, metoda unikania kolizji, również obejmuje monitorowanie stanu łącza, ale wykrywanie, że nośnik, tj. urządzenie, w którym medium transmisyjne jest bezczynne, zaczyna od wysłania informacji o swoim zamiarze przed rozpoczęciem transmisji. Ten mechanizm istnieje w sieciach bezprzewodowych.

Metoda przekazywania tokena polega na wysłaniu z urządzenia do urządzenia specjalnej części danych zwanej tokenem lub tokenem, której posiadanie rozpoczyna transfer.

5. Modele warstwowe ISO/OSI i TCP/IP

Wzajemna komunikacja urządzeń w sieci komputerowej składa się z kilku etapów, z kilkoma elementami. Każdy z nich jest równie ważny, ponieważ każdy z nich wykonuje zadania wymagane do prawidłowej komunikacji. Kroki te są zdefiniowane przez tzw. model hierarchiczny. Każdy, kto zna model warstwowy, wie, że zrozumienie tego tematu jest podstawą do dalszej wiedzy i umiejętności w dziedzinie sieci komputerowych.

Istnieją dwa modele warstwowe, model protokołu TCP/IP i model referencyjny ISO/OSI.
Z jednej strony są do siebie podobne, a z drugiej każdy model komunikuje się nieco inaczej. Zanim jednak omówimy te dwa modele i wyjaśnimy różnice między nimi, powiemy
Ci, dlaczego i dlaczego powinieneś ich używać, do czego służą i jakie są korzyści z ich używania.

Podział procesu komunikacji sieciowej na warstwy niesie ze sobą wiele korzyści, z których najważniejsze to:

- łatwiejsze definiowanie reguł i zasad komunikacji (są to protokoły komunikacyjne),
- możliwość współpracy ze sprzętem sieciowym i oprogramowaniem różnych producentów,
- łatwiej zrozumieć możliwość całego procesu komunikacji,
- Umiejętność zarządzania procesem komunikacji.

Zanim dane z urządzenia źródłowego trafią do urządzenia końcowego, muszą przebyć długą drogę, podczas której najpierw są odpowiednio oznakowane, otagowane, opisane konkretnymi informacjami pozwalającymi na ich identyfikację, a następnie przesłane pomiędzy wieloma urządzeniami pośredniczącymi, dopóki nie dotrze do odbiorcy, który musi następnie przetłumaczyć.

Bez takiego modelu, który dzieli komunikację na mniejsze, bardziej zrozumiałe i łatwe
w zarządzaniu etapy oraz definiuje zadania, które należy wykonać w poszczególnych warstwach, trudno będzie właściwie zarządzać komunikacją sieciową, ponieważ liczne rozwiązania i technologie tworzą ogromny chaos, niekontrolowany. Wyobraźmy sobie sytuację, w której nie ma takiego nawarstwiania, nie ma reguł opisujących komunikację,
a każdy producent sprzętu i oprogramowania tworzy własny, niezależny system.

Oczywiście w rozwiązaniu jednej firmy komunikacja będzie bardzo sprawna i szybka, ale rozwiązania dwóch oddzielnych firm mogą być ze sobą niekompatybilne. W praktyce wykorzystujemy sprzęt i oprogramowanie sieciowe różnych firm, dzięki podziałowi na osobne warstwy z regułami i zadaniami opisującymi ich działanie. Te zasady i zadania są takie same dla wszystkich, ale każda firma, każdy producent, czy to sprzęt, czy oprogramowanie, może je wdrożyć na swój sposób.

Typowym przykładem są systemy operacyjne. Niektórzy użytkownicy korzystają z systemu Windows, niektórzy pochodzą z dystrybucji Linuksa, a niektórzy z MacOS. Każdy z tych systemów jest inny i każdy wykonuje zadania sieciowe w inny sposób, ale ostatecznie
w każdym z tych systemów strona internetowa lub wiadomość e-mail będą wyglądać tak samo lub przynajmniej podobnie. Dlatego do najważniejszych korzyści wynikających
z zastosowania modelu hierarchicznego należą:

- zarządzanie procesem komunikacji sieciowej,
- określić swoje zasady i zadania,
- możliwość współdziałania na poziomie sprzętowym i programowym produktów sieciowych różnych producentów,
- i kontrolować poprawność komunikacji.

Teraz, gdy znamy już przeznaczenie modeli hierarchicznych, przejdźmy do omówienia najważniejszych ich cech. Oba modele powstały dawno temu w latach siedemdziesiątych, ale nadal są aktualne i używane. Pierwszym z nich jest model TCP/IP, znany jako model protokołu. Każda z jego warstw wykonuje określone zadania przy użyciu określonych protokołów. Z drugiej strony modele ISO/OSI znane jako modele referencyjne są częściej wykorzystywane do analizy w celu lepszego zrozumienia procesów komunikacyjnych zachodzących w sieci i są modelami do projektowania rozwiązań sieciowych, zarówno sprzętowych, jak i programowych.

W przypadku modelu TCP/IP możemy wyróżnić 4 warstwy, są to warstwy: Aplikacja, Transport, Internet i Dostęp do Sieci.

Warstwa aplikacji umożliwia użytkownikom korzystanie z usług sieciowych, takich jak sieć, poczta e-mail, wymiana plików, połączenia terminalowe i wiadomości błyskawiczne. Zawsze mówię moim studentom, że jest to warstwa najbliższa użytkownikowi, ponieważ pozwala nam w pełni korzystać z dobrodziejstw nowoczesnych serwisów internetowych. Na przykład, gdy siedzimy przed komputerem i uruchamiamy przeglądarkę internetową, korzystamy
z sieci na poziomie warstwy aplikacji.

Poniżej znajduje się **warstwa transportowa**, której głównym zadaniem jest sprawna obsługa komunikacji między urządzeniami. Na tej warstwie dane są dzielone na mniejsze części,
a następnie uzupełniane o dodatkowe informacje, co pozwala na ich dystrybucję do odpowiedniej aplikacji na urządzeniu docelowym i montowanie na urządzeniu docelowym
w odpowiedniej kolejności.

Dalej jest **warstwa internetowa**, której głównym zadaniem jest znalezienie najkrótszej
i najszybszej drogi do docelowego urządzenia przez WAN, podobnie jak samochodowy GPS, ale również wykorzystuje adresy logiczne (adresy IP) do adresowania danych.

Wreszcie mamy **warstwę dostępu do sieci**, która koduje dane jako czyste bity (zera
i jedynek) i przekazuje je do medium transmisyjnego i adresuje je, tym razem poprzez adres fizyczny (adres MAC).

Model ISO/OSI składa się z 7 warstw (aplikacji, prezentacji, sesji, transportu, sieci, łącza danych, fizyczna).

W górnej części tego modelu możemy wyróżnić warstwę aplikacji, która działa tutaj bardzo podobnie do modelu TCP/IP w tym, że umożliwia korzystanie z aplikacji sieciowych przez użytkowników końcowych sieci.

Dalej jest warstwa prezentacji, która przekazuje do warstwy aplikacji informacje o używanym formacie danych, np. informuje, jakie typy plików będą przesyłane, a także odpowiada za prawidłowe kodowanie danych na urządzeniu źródłowym i dekodowanie na urządzeniu. Urządzenie docelowe.

Poniżej znajduje się warstwa sesyjna, która zarządza sesjami użytkowników za pomocą
np. strony internetowej lub komunikacji wideo.

Idąc krok dalej, mamy warstwę transportową, która znowu jest dokładnie taka sama jak
w modelu TCP/IP i w obu przypadkach funkcja tej warstwy jest dokładnie taka sama.

Dalej jest warstwa sieciowa, która jest odpowiednikiem warstwy internetowej modelu TCP/IP, czyli bardzo podobnych funkcji, takich jak adresowanie i wyznaczanie najlepszej ścieżki do przesyłania danych.

Dalej mamy warstwę łącza danych, której głównym zadaniem jest kontrola dostępu do medium transmisyjnego oraz adresowanie danych, tym razem jednak w celu ich przetransportowania pomiędzy hostami w sieci LAN.

Wreszcie warstwa fizyczna koduje dane na czyste bity (1s i 0s) i przesyła je przez medium transmisyjne do odpowiedniego urządzenia.

Oba modele są do siebie bardzo podobne. Powstająca różnica widoczna jest w górnych warstwach, w przypadku modelu ISO/OSI jest on podzielony na 3 warstwy, natomiast
w przypadku modelu TCP/IP tę samą funkcję pełni tylko jedna warstwa. Warstwy widać
z podobną różnicą, w modelu ISO/OSI mamy dwie oddzielne warstwy łącza danych i warstwy fizyczne, podczas gdy w przypadku modelu TCP/IP jest tylko jedna warstwa dostępu do sieci.

6. Proces komunikacji

Przyjrzyjmy się teraz procesowi komunikacji z wykorzystaniem modelu TCP/IP. Jak wspomniałem wcześniej, model ten opisuje zestaw protokołów operacyjnych, które tworzą coś, co nazywa się protokołem, czasami nazywanym stosem protokołów. Skąd wzięła się nazwa? Wyjaśniłem, że gdy chcemy wyświetlić stronę internetową, najpierw warstwa aplikacji korzysta z protokołu HTTP, następnie w warstwie transportowej korzystamy z protokołu tej warstwy, takiego jak TCP lub UDP, a następnie w warstwie internetowej protokołu IP, w warstwa dostępu do sieci, na przykład standard Ethernet. Komunikacja opiera się na zestawie protokołów, jeden na drugim. Poprawność można zagwarantować tylko wtedy, gdy do komunikacji używany jest cały stos protokołów.

Najpierw użytkownik sieci tworzy dane w warstwie aplikacji, może to być zapytanie do serwera WWW lub może pisać komunikaty w komunikatorze. Dane są następnie przesyłane w dół stosu, najpierw do warstwy transportowej, gdzie są dzielone na mniejsze części, a następnie do warstwy internetowej, gdzie otrzymują adres, który umożliwia przesyłanie danych przez sieć WAN. Następnie przechodzą do warstwy dostępu do sieci i ponownie przypisują adresy, tym razem do adresów urządzeń w sieci lokalnej. Na koniec dane są wprowadzane do medium transmisyjnego i przesyłane za pośrednictwem pośrednika do urządzenia końcowego, gdzie przechodzą przez stos, ponownie składają i przekazywane są do warstwy aplikacji.

Zapamiętaj

Proces przesyłania danych ze źródła do celu przenosi dane przepływające przez warstwy na urządzeniu źródłowym, które następnie są kodowane i przesyłane za pośrednictwem medium transmisyjnego do urządzenia docelowego, gdzie zamiast tego dane trafiają na stos.

Zanim zagłębimy się w proces komunikacji, musimy zadać jeszcze jedno bardzo ważne pytanie. Aby dane dotarły do odpowiednich hostów i aplikacji oraz pozostały możliwie niezmienione, przekazując im odpowiednie informacje, nazywamy to informacją kontrolną.

Ta informacja jest dodawana w trzech warstwach. Warstwa transportowa dodaje numery portów aplikacji (port aplikacji na hoście źródłowym i port aplikacji na hoście docelowym), warstwę internetową lub sieciową, adres IP (w tym host źródłowy i docelowy), warstwę sieci lub łącza danych, adres MAC (host źródłowy) i router sieci lokalnej). Cały proces przechodzenia warstw w stosie, dzielenia ich na mniejsze części i dodawania informacji kontrolnych (tj. dodatkowych danych) nazywa się enkapsulacją. Oczywiście istnieje odwrotny proces usuwania tych dodatkowych informacji z urządzenia docelowego, zwany procesem dekapsulacji.

Zapamiętaj

Dane przepływają przez warstwy na urządzeniu źródłowym, otaczając je informacjami w celu identyfikacji aplikacji i urządzenia docelowego, podczas gdy proces odwrotny, w którym dane przepływają w górę warstw i usuwają te dodatkowe informacje na hoście docelowym, to dekapsulacja.

Dodanie tych informacji kontrolnych do każdej warstwy z osobna nieznacznie zmieniłoby ich strukturę, co jest logiczne, ponieważ dodajemy pewne informacje do danych, których wcześniej tam nie było. Dlatego zmienia się również nazewnictwo zbiorów danych. Zazwyczaj dane przesyłane przez sieć są nazywane jednostkami danych protokołu (PDU), ale w miarę przemieszczania się między warstwami ich nazwy zmieniają się, więc: W warstwie aplikacji po prostu nazywamy PDU danymi. W dalszej części warstwy transportowej będziemy odnosić się do PDU jako segmentów lub datagramów w zależności od protokołu używanego w tej warstwie. PDU w warstwie internetowej to już pakiet, aw warstwie dostępu do sieci będziemy mieli ramkę. Tę samą nomenklaturę będziemy używać przy analizie komunikacji za pomocą modelu ISO/OSI.

7. Omówienie zastosowania warstw

Nadszedł czas na bardziej szczegółowe zrozumienie procesu komunikacji opartej na warstwach. Omówimy to na przykładzie wysłania e-maila. Pierwotnie internauci tworzyli wiadomości e-mail za pomocą programów pocztowych lub przeglądarek internetowych. Warstwa aplikacji poprawnie koduje te dane i przekazuje je do warstwy transportowej.

Warstwa ta dzieli dane na mniejsze części, segmenty, które są łatwiejsze do przesłania przez sieć. To tak, jakbyśmy chcieli przesunąć ogromny róg z miejsca na miejsce, ciężko przestawić całość, bo nawet nie mieści się w drzwiach, więc rozbieramy go zamiast kombinować z całkowitym przesunięciem. dodaje również informacje kontrolne, które pozwalają później złożyć segmenty na urządzeniu końcowym we właściwej kolejności (choć nie zawsze są one dodawane, w zależności od protokołu używanego w tej warstwie), ale co najważniejsze, dodawany jest również numer portu aplikacji (port aplikacji na serwerze i port na kliencie), czyli informacje, które pozwalają później określić, że jest to wiadomość e-mail, a nie strona internetowa. Więcej o portach aplikacji będziemy mówić, gdy będziemy omawiać funkcje i protokoły warstwy aplikacji i warstwy transportowej.

Następnie segmenty te są transportowane do warstwy internetowej, gdzie przydzielane są adresy IP – urządzenie służące do przesyłania danych oraz urządzenie będące odbiorcą. Ten proces jest używany, aby router (czyli urządzenie pośredniczące między nadawcą a odbiorcą wiadomości) wiedział, gdzie wysłać wiadomość. Od tego momentu nasz segment jest adresowany przez pakiet.

Następnie pakiet trafia do warstwy dostępu do sieci, gdzie tworzona jest ramka i dostarcza fizyczny adres urządzenia wysyłającego oraz fizyczny adres routera, do którego podłączony jest komputer, do którego wysyłamy wiadomość. Dzięki temu adresowi ramki mogą następnie dotrzeć do tego routera, który następnie wysyła je do sieci WAN.

Jednak przed samą transmisją ramka jest kodowana na bity i przekazywana przez router do urządzenia docelowego.

Gdy te bity są odbierane przez hosta docelowego, następuje odwrotny proces enkapsulacji i dekapsulacji, w którym ramki są konwertowane na pakiety, pakiety są konwertowane na segmenty, a warstwa transportowa ponownie składa je we właściwej kolejności. Po zakończeniu tego procesu dane są przesyłane do warstwy aplikacji, w której wyświetlany jest komunikat. Gdy chcemy wyświetlić stronę WWW lub wysłać plik przez Internet, proces komunikacji będzie podobny, z tą różnicą, że zostaną użyte inne protokoły warstwy aplikacji, aby zamiast wysyłania i odbierania e-maili, obsługiwały wysyłanie stron WWW lub plików.

Na koniec ważna informacja - proces komunikacji pomiędzy omawianymi tutaj urządzeniami jest uproszczony i nazywamy to umową. Czemu? Ano dlatego, że pominęliśmy proces przesyłania danych pomiędzy urządzeniami pośredniczącymi (czyli routerami). Proces routingu, czyli przesyłanie danych pomiędzy routerami w sieci rozległej oraz możliwość wykorzystania różnych mediów transmisyjnych w procesie od nadawcy do odbiorcy, to obszerna i złożona kwestia, której nie będziemy teraz omawiać. Oczywiście jest to niezwykle ważna faza komunikacji i na pewno zwrócimy na nią uwagę, ale tylko jeśli pozwoli na to nasza wiedza i umiejętności z zakresu sieci komputerowych.

Cóż, teraz każdy z Was wie, jak wygląda proces komunikacji, gdy jest prezentowany i prezentowany na warstwowym modelu protokołu TCP/IP, który wygląda bardzo podobnie na modelu referencyjnym ISO/OSI. Jeśli więc zostaniesz poproszony (np. nauczyciela o wykonanie testu) o opisanie procesu komunikacji w oparciu o model ISO/OSI, nie powinieneś mieć problemu.

8. Adresowanie w sieci

Wyjaśnijmy teraz bardzo ważną kwestię, a mianowicie adresowanie w sieci. Być może zauważyłeś, że to pytanie pojawia się 3 razy podczas omawiania procesu komunikacji, ponieważ informacje związane z adresami lub numerami są dodawane aż do trzech warstw.

Ale tym razem zacznijmy od dołu stosu i zobaczmy, że w warstwie dostępu do sieci modelu TCP/IP i warstwie łącza danych modelu ISO/OSI pojawiła się koncepcja adresów fizycznych. Pytasz, jaki jest ten adres fizyczny. Żaden adres fizyczny, znany również jako adres MAC, to 48-bitowa liczba zakodowana szesnastkowo na karcie sieciowej urządzenia końcowego, czyli komputera. Adres ten może mieć formę: 28-80-23-D6-BE-14, podawany na etapie tworzenia karty. Składa się z dwóch równych części, pierwsza to identyfikator producenta, a druga to identyfikator karty.

Wszystkie te kody szesnastkowe służą do znalezienia hosta w sieci lokalnej, sieci LAN, jest to ten adres, adres fizyczny hosta źródłowego i routera w sieci lokalnej, brama łącząca naszą sieć lokalną i WAN, w TCP/ Proces enkapsulacji sieci warstwy dostępu modelu IP i warstwy łącza danych modelu ISO/OSI.

Idąc w górę, mamy warstwę internetową modelu TCP/IP i warstwę sieciową modelu ISO/OSI. W tych warstwach adresy IP, zwane również adresami logicznymi, są dodawane podczas procesu enkapsulacji. Adresy te to adres IP komputera nadawcy i adres IP komputera odbiorcy. Nie będę tutaj wdawał się w szczegóły budowy, wykorzystania i obliczania adresów IP, ponieważ w naszym kanale jest już odcinek (kliknij, aby wejść), który jest w całości poświęcony adresom IP, a powiem tylko, że te adresy są zlokalizowane w różnych sieciach do transmisji danych Hosty są zwykle oddalone od siebie geograficznie o setki kilometrów.

Wreszcie mamy warstwę transportową, która nie używa adresowania do wykrywania hostów, jak poprzednio omówione warstwy, ale zamiast tego używa numerów portów do przypisywania danych do określonych aplikacji w systemie operacyjnym. Pamiętaj,
że dzisiejsze komputery umożliwiają jednoczesne uruchamianie wielu aplikacji. Jednocześnie możemy korzystać z przeglądarki do surfowania po Internecie, słuchania radia internetowego, wysyłania i odbierania e-maili, a nawet grania w gry online. Jeśli aplikacje nie są podzielone na partycje, jeśli numery portów nie są przypisane w warstwie transportowej, aby umożliwić identyfikację konkretnych usług sieciowych, możemy doświadczyć, że podczas rozgrywki na ekranie będą pojawiać się przychodzące e-maile w niższych stopniach,
w edytorach tekstowych Będą wiadomości od komunikator w komunikatorze. Zobacz, jak to wszystko jest przemyślane, logicznie ułożone, bez szans, dlatego tak bardzo kocham sieci komputerowe.

8.1. Podsumowanie

W sieciach komputerowych, aby ułatwić opis i kontrolę różnych etapów komunikacji oraz
w celu standaryzacji, stosuje się model warstwowy, aby sprzęt i oprogramowanie różnych producentów były ze sobą kompatybilne. Komunikacja w sieci odbywa się przy użyciu reguł
i zasad znanych jako przyjęcie protokołów komunikacyjnych. Proces komunikacji w sieci polega na przekazywaniu danych w dół stosu na urządzeniu źródłowym, kodowaniu ich na bity i wysyłaniu do urządzenia docelowego, gdzie dane są przesyłane dalej i interpretowane w urządzeniu docelowym. W każdej warstwie dane są dostarczane z informacjami kontrolnymi, numerami portów oraz adresami logicznymi i fizycznymi, które są następnie kodowane i wysyłane do odbiorcy. Proces spływania danych w dół stosu i przesyłania informacji sterujących oraz adresów nazywa się enkapsulacją, natomiast na urządzeniach końcowych, gdy dane wędrują w górę stosu, proces ten nazywa się dekapsulacją.

9. Protokoły warstwy aplikacji

9.1. Protokół HTTP

Kiedy uruchamiamy przeglądarkę internetową, komunikator lub program do udostępniania plików, aplikacje te tworzą interfejs komunikacyjny między siecią komputerową
a użytkownikiem. Oczywiście sam program użytkowy, sam program komputerowy, nie wystarcza do sprawnej komunikacji, ponieważ wymagane są do tego powyższe protokoły komunikacyjne, ale są one w tych programach zaimplementowane. Przykładowy protokół warstwy aplikacji, prawdopodobnie jeden z najpopularniejszych, HTTP, jest zaimplementowany w przeglądarkach internetowych i podobnie jak wszystkie komunikatory i inne programy komunikujące się za pomocą sieci, również implementują odpowiedni protokół.

Gdy wprowadzimy w przeglądarce adres strony internetowej tzw. URL (Uniform Resource Locator), a po naciśnięciu klawisza Enter nasza przeglądarka połączy się z serwerem, na którym przechowywana jest strona i zażąda od niej określonego zasobu – Większość z nich to zazwyczaj pliki zawierające strony z treścią. Jeśli serwer posiada żądany zasób, wysyła jego zawartość do przeglądarki, która interpretuje kod HTML, z którego składa się strona, i wyświetla jej zawartość użytkownikowi. W rzeczywistości proces jest nieco skomplikowany. Jako przykład weźmy adres internetowy:

http://www.cybersecurity.pl/fundamentals.html

Po wprowadzeniu i potwierdzeniu przeglądarka najpierw sprawdza typ protokołu, następnie nazwę domeny internetowej, a na końcu rozważa nazwę konkretnego pliku. Później nasza przeglądarka odwołuje się do serwera DNS w celu zmiany nazwy mnemonicznej
(tj. cybersecurity.pl) na adres IP serwera, na którym przechowywana jest strona.

Przeglądarka znając ten adres wysyła do serwera żądanie dostępu do pliku tomijerry.html znajdującego się w domenie alamakota.pl. Jeśli serwer ma w odpowiedzi dany zasób, wysyła odpowiednią wiadomość wraz z zawartością żądanego pliku. Zawartość tego pliku, kod HTML, jest interpretowana przez przeglądarkę i wyświetlana jako strona internetowa.

Protokół HTTP domyślnie pracuje na porcie 80 i definiuje kilka podstawowych typów komunikatów, czyli żądanie komunikacji między klientem a serwerem WWW, z których najważniejsze to: GET i POST.

9.2. Metoda GET

GET służy do żądania danej strony internetowej z serwera. Jego składnia wygląda tak:

GET /fundamentals.html HTTP/1.1

Oprócz nazwy żądanego zasobu zawiera również używaną wersję protokołu. Gdy serwer otrzyma taką wiadomość, takie żądanie, odpowiada klientowi odpowiednią wiadomością
(z nagłówkami pokazanymi poniżej) i żądanym zasobem:

HTTP/1.1 200 OK/fundamentals.html

Żądanie GET zawiera również następujące informacje: nazwę hosta (np. wp.pl), nazwę przeglądarki, która wysłała żądanie, typy plików akceptowane przez przeglądarkę oraz preferowany język lub kodowanie znaków strony. Odpowiedź serwera zawiera następujące informacje: czas serwera, nazwę aplikacji serwera (np. APACHE) lub czas wygaśnięcia dokumentu.

Jeśli z jakiegoś powodu serwer sieciowy nie może odesłać zasobu, odsyła komunikat
o błędzie, taki jak 404 powiadamiający, że żądany zasób nie został znaleziony lub 403 powiadamiający, że dostęp do zasobu jest zabroniony. Wybrane komunikaty i kody błędów przedstawiono w poniższej tabeli.

[tabelka z wklejki poniżej]

Kod błędu klienta:

Kod Opis Znaczenie

400 Bad Request Serwer nie mógł przetworzyć żądania z powodu błędu klienta

401 Żądania nieautoryzowane Żądania dotyczące zasobów, które wymagają uwierzytelnienia

403 Forbidden Serwer rozumie żądanie, ale konfiguracja zabezpieczeń uniemożliwia
mu zwrócenie żądanego zasobu

404 Not Found Serwer nie znalazł zasobu pod podanym adresem URL

405 Metoda niedozwolona Metoda zawarta w żądaniu jest niedozwolona dla wskazanego zasobu

406 Not Acceptable Żądany zasób nie może zwrócić odpowiedzi, którą klient może obsłużyć

407 Wymagane uwierzytelnienie proxy Wymagane uwierzytelnienie proxy

408 Limit czasu żądania Upłynął czas oczekiwania na żądanie — klient nie wysłał żądania do serwera w określonym czasie

409 Konflikt Żądanie nie mogło zostać zrealizowane z powodu konfliktu z aktualnym stanem zasobu

411 Wymagana długość wymagana długość — serwer odmówił ukończenia zapytania z powodu braku nagłówka Content-Length w zapytaniu

415 Unsupported Media Type Unknown request way — serwer odmówił przyjęcia zapytania, ponieważ jego składnia była niezrozumiała dla serwera

[koniec tabelki]

Kod błędu serwera:

Kod Opis Znaczenie

500 Internal Server Error Wewnętrzny błąd serwera — serwer napotkał problem uniemożliwiający zakończenie żądania

501 Not Implemented Serwer nie ma możliwości wymaganych dla zapytania

502 Błąd nieprawidłowej bramy Brama — serwer — działający jako brama lub pośrednik — otrzymał złą odpowiedź od serwera nadrzędnego i nie mógł spełnić żądania klienta

503 Usługa niedostępna Usługa niedostępna — serwer nie może obecnie wykonać zapytania klienta z powodu przeciążenia

504 Gateway Timeout Przekroczony czas bramy — serwer działający jako brama lub pośrednik nie otrzymał odpowiedzi z określonego serwera HTTP, FTP, LDAP itp. w określonym czasie lub do obsługi żądania wymagany jest serwer DNS

505 HTTP Version Not Supported Nieobsługiwana wersja HTTP — serwer nie obsługuje lub odmawia obsługi wersji HTTP wskazanej przez klienta

9.3. Metoda POST

Innym rodzajem wiadomości jest wiadomość POST, która służy do przesyłania danych na serwer. Na przykład, gdy na stronie znajduje się formularz, który przesyła dane na serwer, taki jak formularz rejestracyjny, dane, które w niej umieszczamy, są przesyłane wiadomością POST.

Chociaż protokół HTTP jest bardzo popularny i prawdopodobnie najczęściej używany ze wszystkich protokołów warstwy aplikacji, nie jest bezpieczny. Metoda POST wysyła dane do serwera w postaci zwykłego tekstu. W przypadku przechwycenia transmisji między klientem a serwerem możliwe jest odczytanie informacji, które chcesz wysłać do serwera.

Jest to bardzo niebezpieczne, dlatego obecnie większość stron internetowych może wysyłać pewne informacje na serwer, np. na tych stronach, które wymagają logowania, już używa protokołu HTTPS, który szyfruje komunikację między klientem a serwerem, działa na porcie 443.

Inne rodzaje wiadomości, które klienci mogą wysyłać na serwer WWW, to:

Dane do tabelki mojej:

Usuń żądanie usunięcia zasobu z serwera

Head żąda zasobów z serwera w postaci nagłówków

Link Request ustanawia relacje między istniejącymi zasobami

OPCJE Żądanie od serwera identyfikacji obsługiwanych metod

Put żąda od serwera otrzymania pliku od klienta

Trace żąda od serwera zwrócenia nagłówków wiadomości wysłanej przez klienta

9.4. Poczta elektroniczna

Poczta e-mail korzysta z dwóch protokołów warstwy aplikacji, które współpracują ze sobą. Jeden służy do wysyłania poczty, co jest protokołem SMTP, a drugi do odbierania wiadomości, czyli POP3. Dziś IMAP może być również używany do odbierania wiadomości e-mail. Protokoły te są ściśle powiązane z aplikacjami, procesami działającymi na komputerach klienckich i serwerach, które tworzą i odbierają wiadomości. Procesy te to MUA (Mail User Agent), MTA (Mail Transfer Agent) i MDA (Mail Delivery Agent).Proces MUA działa na urządzeniu klienckim, a dwa pozostałe procesy na serwerze pocztowym.

Uproszczony proces wysyłania wiadomości e-mail przy użyciu proxy wygląda następująco:

1. Użytkownik tworzy wiadomość e-mail i używa procesu MUA do przekazania jej do serwera pocztowego i procesu MTA działającego na tym serwerze.

2. Ten proces analizuje nagłówki wiadomości, w tym. W celu zdefiniowania odbiorcy wiadomości i sprawdzenia, czy użytkownik, na który wskazuje wiadomość, znajduje się na jego liście użytkowników.

3. Jeśli tak, przekazuje wiadomość do procesu MDA, który odpowiada za dostarczenie jej do odpowiedniego odbiorcy.

4. Jeśli odbiorca wiadomości nie ma konta na tym serwerze, proces MTA przekazuje wiadomość do procesu MTA na innym serwerze, na którym znajduje się konto użytkownika.

5. Serwer przekazuje wiadomość do procesu MDA, który dostarcza wiadomość do zamierzonego odbiorcy.

W poniższej tabeli przedstawiono porty, na których działa protokół poczty elektronicznej.

Protokół	**Numer portu**
IMAP	143
POP3	110
SMTP	25
Szyfrowany IMAP	993
Szyfrowany POP3	995
Szyfrowany SMTP	465 lub 587

9.5. Protokół FTP

Trzecią, równie popularną usługą internetową jest możliwość wysyłania i odbierania plików przez FTP (File Transfer Protocol). Usługa jest również protokołem komunikacyjnym, gdy chcemy przesłać pliki strony internetowej na serwer WWW lub po prostu chcemy przesłać niektóre pliki na serwer i udostępnić innym użytkownikom. Aby wykonać operację wgrywania plików na serwer lub pobierania zasobów z serwera, musimy skorzystać z klienta FTP i oczywiście taka usługa również musi być uruchomiona na serwerze. Klienci FTP są dostępni w każdym systemie operacyjnym, na przykład za pomocą wiersza poleceń, co jest niewygodne, ale działa.

Jeśli używamy FTP tylko do pobierania plików, możemy to zrobić bezpiecznie za pomocą przeglądarki internetowej. Większość, jeśli nie wszystkie, popularne przeglądarki mają wbudowanych klientów FTP.

Jeśli jednak chcemy przesłać pliki na serwer, warto skorzystać z dedykowanych programów, takich jak FileZilla czy WinSCP – są one darmowe i można je łatwo pobrać z sieci.

Klient FTP WinSCP

W przypadku tego protokołu, aby komunikować się poprawnie, należy nawiązać dwa połączenia pomiędzy klientem a serwerem. Pierwsze połączenie jest używane tylko do wysyłania poleceń i wiadomości i nazywa się połączeniem kontrolnym (działa na porcie 21), podczas gdy drugie połączenie działa na porcie 20 i jest używane do przesyłania plików do iz serwera. W celu ochrony dostępu do serwera FTP stosowana jest autoryzacja użytkownika, która jest dokładnie taka sama jak przy logowaniu do profili czy maili w serwisach społecznościowych, ale czasami, gdy zasób jest dostępny dla większej liczby odbiorców, anonimowy dostęp mają tzw. użytkownicy, Dlatego nie jest wymagane żadne zezwolenie.
To rozwiązanie powinno być stosowane tylko wtedy, gdy użytkownik może pobierać dane
z serwera. Wgrywanie plików, czyli umieszczanie ich na serwerze, jest zawsze dostępne tylko dla użytkowników posiadających login i hasło.

powszechnie używanym protokołem warstwy aplikacji jest protokół zdalnego zarządzania hostem, znany jako SSH (Secure Shell). Dla osób niebędących informatykami nazwa ta ma niewielkie znaczenie, ponieważ nie jest protokołem, stroną internetową ani e-mailem używanym przez „zwykłych zjadaczy chleba". Administratorzy używają go do zarządzania serwerami, które często znajdują się w różnych lokalizacjach geograficznych, niekoniecznie w miejscu pracy. Na przykład jest również używany przez osoby, które kupiły serwery VPS i dlatego nimi zarządzają. Protokół ten wywodzi się z innego protokołu dostępu zdalnego, protokołu TELNET, i jest prawdopodobnie lepszą wersją. Czemu? Ponieważ TELNET przy okazji jest prawdopodobnie najstarszym protokołem w warstwie aplikacji, nie szyfruje komunikacji między klientem a serwerem, wiadomości wysyłane są w postaci zwykłego tekstu, dzięki czemu możliwe jest przechwycenie komunikacji i zastanowienie się, w jakiej sesji znajdują się informacje jest wysłany. Jego zdaniem jest to sytuacja niedopuszczalna, dlatego hostem zarządza się zdalnie za pomocą szyfrowanego protokołu SSH.

Domyślnym algorytmem szyfrowania komunikacji jest RSA, ale nieco słabszy algorytm DSA może być również użyty do szyfrowania danych. Podczas instalacji serwera SSH tworzona jest para kluczy – publiczny i prywatny serwera – które służą do szyfrowania i deszyfrowania komunikacji. Gdy klient łączy się z serwerem po raz pierwszy, zapisuje klucz publiczny serwera w pliku known_hosts na dysku.

Następnie tworzy tak zwany klucz sesji, który służy do szyfrowania całej komunikacji. Klucz sesji jest szyfrowany kluczem publicznym wcześniej otrzymanym z serwera i odesłanym do niego. Od tego momentu cała komunikacja jest szyfrowana za pomocą klucza sesji.

Domyślnie SSH działa na porcie 22. PUTTY to jeden z najpopularniejszych programów klienckich do korzystania z SSH, jest bezpłatny, można go pobrać z sieci i nie wymaga instalacji. Aby połączyć się zdalnie z hostem, po prostu uruchom go, wprowadź nazwę hosta lub jego adres IP, wybierz SSH, jeśli nie jest zaznaczone domyślnie, i kliknij Otwórz. Jeśli łączymy się ze zdalnym hostem po raz pierwszy, potwierdzamy, że chcemy się połączyć i możemy nim zarządzać zdalnie.

9.7. Protokół DNS

DNS to protokół, usługa, która tłumaczy czytelne dla człowieka nazwy domen na adresy IP urządzeń w Internecie. Wyobraźmy sobie sytuację, w której DNS nie istnieje, a chcemy wyświetlać w przeglądarce nasze ulubione strony. Musimy wpisać adres IP, a nie nazwę domeny, czyli adres w formie słownej, na przykład: 212.56.93.112. Dla większości z nas to żaden problem, niektóre liczby można zapamiętać. Z drugiej strony w Internecie jest wiele stron internetowych i trudno zapamiętać wiele adresów liczbowych. Co więcej, w takich cyfrowych zapisach łatwo o pomyłkę, a w świecie Internetu tak mały błąd może doprowadzić do innej strony niż się spodziewaliśmy.

To jedna strona medalu, a druga strona jest taka, że adres IP serwera może nie zmieniać się zbyt często. Gdy nasza strona internetowa zmienia adres IP i usługa DNS nie działa, musimy ponownie nauczyć się tego adresu i zapamiętać. DNS rozwiązuje za nas ten problem, ponieważ zmienia ten adres w swojej bazie rekordów i przypisuje go do nazwy domeny. Wtedy dla nas użytkowników nie ma znaczenia, jaki jest adres IP strony, ważne jest to, że znamy jej adres, nazwę domeny i nie ulegają one zmianie.

DNS to usługa działająca w architekturze klient-serwer, ale nie traktujemy tutaj klientów jako programów komputerowych, takich jak przeglądarki czy programy do udostępniania plików. Na tym komputerze działa tylko usługa systemowa o nazwie DNS Resolver, która obsługuje wszystkie aplikacje na komputerach klienckich, których nazwy wymagają zmiany. Ilekroć konfigurujemy urządzenie sieciowe, czy tylko komputer, powinniśmy podać dwa adresy serwerów DNS, aby jeśli jeden z nich się nie komunikował, drugi pełnił funkcję podstawienia nazw.

Serwery DNS przechowują różnego rodzaju rekordy, w tym rekordy A i AAAA zawierające adresy urządzeń końcowych oraz rekordy MX obsługujące wymianę poczty, ponieważ należy pamiętać, że DNS nie tylko tłumaczy adresy domenowe na adresy IP dla stron internetowych, ale także stosuje do serwera poczty e-mail. Zamiana nazw wygląda dla mnie tak:

1. Klient wysyła zapytanie do serwera DNS, który sprawdza, czy dany rekord istnieje w jego bazie danych.

2. Jeśli tak, tłumaczy nazwę na adres IP i odsyła do klienta:

3. Jeśli nie, to kontaktuje się z innymi serwerami, aby dany rekord znalazł się w ich bazie danych:

Wysyłanie zapytań do innych serwerów o serwer DNS, który nie znajduje rekordu w swojej bazie danych, może spowodować duży ruch w sieci, co jest mylącą sytuacją. Aby zapobiec nadmiernemu i niepotrzebnemu ruchowi w sieci, gdy inny serwer odnajdzie dany rekord i prześle go na serwer przypisany do naszego urządzenia, ten ostatni zapisuje rekord w pamięci podręcznej, dzięki czemu w przyszłości nie trzeba odwoływać się do innego serwera w celu ten sam adres. Z pewnością przyspieszy to późniejsze zmiany nazw, ponieważ nasze serwery DNS nie wyszukują już rekordów na innych serwerach, ale natychmiast zastępują nazwy. Podobnie usługi DNS na komputerach osobistych przechowują wcześniej przetłumaczone nazwy. Można to zweryfikować, wprowadzając ipconfig /displaydns na komputerze z systemem Windows. Następnie zobaczymy, które mapowania są przechowywane w pamięci podręcznej usługi DNS naszego komputera.

9.8. Hierarchia DNS

Ta hierarchia serwerów DNS ma postać odwróconego drzewa, z korzeniem, serwerem DNS najwyższego poziomu, na szczycie. Serwer najwyższego poziomu przechowuje informacje
o tym, jak dotrzeć do serwera najwyższego poziomu, który z kolei przechowuje informacje
o tym, jak dotrzeć do serwera drugiego poziomu itp. Domeny najwyższego poziomu określają kraj (.pl.de lub .uk) lub typ organizacji (.org .com lub .gov).

W przykładowym adresie takim jak Pocztowy.wp.pl rozróżniamy domenę najwyższego poziomu (.pl), następnie domenę drugiego poziomu (wp.pl) i wreszcie domenę trzeciego poziomu (Pocztowy.wp.pl Oczywiście nie wszystkie Adresy muszą zawierać jak najwięcej poziomów domen, a nie tylko domeny najwyższego i drugiego poziomu, takie jak wp.pl, pasja-informatyki.pl, Szkola.pl.

9.9. Protokół DHCP

Podobnie jak DNS omówiony wcześniej, DHCP jest protokołem działającym jako usługa, a nie jako program lub aplikacja. DHCP umożliwia komputerom łączącym się z siecią uzyskanie adresów IP, masek podsieci, adresów bram i serwerów DNS oraz innych ustawień z wcześniej skonfigurowanej puli adresów. Serwer DHCP można skonfigurować na osobnym komputerze i będzie on oddzielnym urządzeniem w sieci, które przypisuje adresy IP komputerom klienckim, lub może działać na istniejącym serwerze jako osobna usługa, osobny proces.

Obecnie router w naszym domu również pozwala nam na skonfigurowanie takiej usługi. Przypisywanie adresów komputerom klienckim za pośrednictwem usługi DHCP (tzw. przydzielanie dynamiczne) jest bardzo wygodnym rozwiązaniem dla administratorów, zwłaszcza w dużych sieciach, w których często pojawiają się nowe komputery i ich użytkownicy. W sieci ze 100, 200 lub 500 komputerami i dużą liczbą urządzeń mobilnych sama konfiguracja adresów IP byłaby żmudnym i co najważniejsze czasochłonnym zadaniem.

Oczywiście nie wszystkie urządzenia w sieci mogą w ten sposób uzyskiwać adresy, ponieważ niektóre z nich, takie jak serwery aplikacji, bazy danych, uwierzytelnianie użytkowników, drukarki sieciowe lub routery, powinny i muszą mieć adresy przypisane statycznie, czyli dystrybuowane ręcznie. Czemu? Ponieważ usługa DHCP skonfigurowana na serwerze nie zawsze przypisuje na stałe dany adres IP do komputera. Dzierżawi taki adres tylko na czas określony przy konfiguracji DHCP, może godziny, dni, ale nie na stałe, chociaż są od tego wyjątki, opowiem przy konfiguracji konkretnego serwera DHCP.

Wyłączona maszyna zwraca wydzierżawiony adres, który jest zwracany do puli. Inne urządzenie może wtedy wydzierżawić ten adres. Gdy serwer, router lub drukarka sieciowa wydzierżawi te adresy, mogą być zmuszone do zwrócenia ich do puli po pewnym czasie i nie ma gwarancji, że ponownie otrzymają ten sam adres. Komputery klienckie, które komunikują się z dowolnym serwerem lub innym ważnym urządzeniem działającym w sieci, odnoszą się do niego po jego adresie IP, jeśli adres IP często się zmienia, niektóre usługi dla użytkowników w sieci lokalnej mogą być niedostępne przez pewien czas, zwłaszcza w firma Tym bardziej Niedopuszczalne.

Aby komputer z systemem Windows mógł uzyskać adres z serwera DHCP, należy w konfiguracji sieci wybrać opcję „Uzyskaj adres IP automatycznie”.

9.10. Zestawienie protokołów

Protokoły warstwy aplikacji opisane w tym odcinku to tylko niewielka część ogólnej listy dostępnych protokołów warstwy aplikacji. W sieci komputerowej istnieje wiele innych usług, z których każda działa na innym protokole. Ciężko je tutaj wymienić, więc wymieniono te najpopularniejsze i najczęściej używane. Dla zainteresowanych zgłębieniem tematu protokołów komunikacyjnych warstwy aplikacji odsyłam do literatury fachowej. Poniższa tabela zawiera zestaw popularnych protokołów warstwy aplikacji i ich numery portów. Z pewnością przydają się do sprawdzania przed egzaminami lub egzaminami zawodowymi.

Protokół	Opis	Port
HTTP	Protokół przesyłania dokumentów hipertekstowych	80
HTTPS	Szyfrowany protokół HTTP korzystający z protokołów SSL lub TLS	443
POP3	Protokół odbierania poczty	110 (szyfrowany 995)
IMAP	Protokół odbierania poczty umożliwiający zarządzanie folderami w skrzynce	143 (szyfrowany 993)
SMTP	Protokół wysyłania poczty	25 (szyfrowany 465 lub 587)
FTP	Protokół przesyłania plików	21 (polecenia) i 20 (pliki)
FTPS	Szyfrowany protokół FTP	990
TELNET	Protokół połączenia terminalowego	23
SSH	Szyfrowany protokół połączenia terminalowego	22
DNS	Protokół zmiany nazw domenowych na adresy IP	53
DHCP	Protokół automatycznej konfiguracji hostów w sieci	67 i 68 (IPv6 – 546 i 547)
LDAP	Protokół usług katalogowych (np. AD w WS)	389 (szyfrowany 639)
SNMP	Protokół konfiguracji urządzeń sieciowych	161
MySQL	System zarządzania bazą danych	3306
PostgreSQL	System zarządzania bazą danych	5432

10. Zadania warstwy transportowej

Warstwa transportowa lub warstwa transportowa (można używać tych nazw zamiennie) jest bardzo ważnym elementem procesu komunikacji. Do najważniejszych zadań tej warstwy należą:

- nawiązywać i obsługiwać połączenia (sesje) pomiędzy hostami,
- śledzić połączenia między hostami,
- Podziel dane na mniejsze kawałki,
- Zidentyfikuj poszczególne aplikacje,
- kontrola przepływu danych,
- Retransmisja w przypadku utraty danych.

Śledzenie połączeń, które są konwersacjami między hostami, umożliwia wielu aplikacjom jednoczesne wysyłanie i odbieranie danych. Na jednym komputerze możemy sprawdzać pocztę, korzystać z bankowości elektronicznej czy komunikować się ze znajomymi. W tej chwili wydaje nam się naturalne, że właściwie trudno wyobrazić sobie sytuację bez tej możliwości, ale warto pamiętać, że jest to możliwe dzięki warstwie transportowej.

Możliwość korzystania z wielu usług jednocześnie, obejmuje również dzielenie danych, czyli rozbijanie ich na mniejsze kawałki. Pozwala to na wydajniejszą komunikację, ponieważ duże ilości danych nie są przesyłane jednocześnie. Gdyby nie segmentacja, tylko jedna aplikacja mogłaby odbierać dane na raz, a pozostałe aplikacje, z których korzystamy, musiałyby czekać na swoją kolej. Jak widać na poniższym obrazku, segmenty są przesyłane naprzemiennie, segmenty strony internetowej, segmenty wiadomości e-mail, segmenty komunikatora itp. są przesyłane naprzemiennie. Cały proces naprzemiennego przesyłania wielu segmentów aplikacji nazywa się multipleksowaniem.

Innym ważnym zadaniem lub funkcją warstwy transportowej jest przekazywanie danych do właściwej aplikacji. Każda aplikacja ma swój własny identyfikator, aby ją jednoznacznie zdefiniować. Ten identyfikator to numer portu aplikacji.

Jest przypisywany do segmentu lub datagramu podczas enkapsulacji na poziomie warstwy transportowej i gwarantuje dostarczenie danych do określonej aplikacji.

Podobnie jak w przypadku adresów IP, numery portów są przydzielane przez urząd IANA (Internet Assigned Numbers Authority), który dzieli numery portów na 3 grupy:

Nazwa grupy portów	Zakres numeracji	Zastosowanie
Dobrze znane (ang. well knows)	0 – 1023	Usługi i aplikacje serwera
Zarejestrowane (ang. registered)	1024 – 49151	Usługi i aplikacje użytkownika
Dynamiczne (ang. dynamic)	49152 – 65535	Losowo wybierane dla aplikacji klienta

Dobrze znane porty, tj. porty od 0 do 1023, są zarejestrowane dla usług i określonych aplikacji serwerowych, np. serwery WWW domyślnie uruchamiane na porcie 80, a serwery POP3 domyślnie uruchamiane na porcie 110. Zestaw aplikacji ze znanymi portami, w tym protokołami warstwy transportowej, jak pokazano poniżej.

Protokół warstwy aplikacji	Numer portu	Protokół warstwy transportowej
HTTP	80	TCP
HTTPS	443	TCP
POP3	110 (szyfrowany 995)	TCP
IMAP	143 (szyfrowany 993)	TCP
SMTP	25 (szyfrowany 465 lub 587)	TCP
FTP	21 (polecenia) i 20 (pliki)	TCP
FTPS	990	TCP

TELNET	23	TCP
SSH	22	TCP
DNS	53	TCP lub UDP
DHCP	67 i 68 (IPv6 – 546 i 547)	UDP
LDAP	389 (szyfrowany 639)	TCP lub UDP
SNMP	161	UDP

Druga grupa, zarejestrowane porty, jest wykorzystywana przez aplikacje zainstalowane na komputerze użytkownika. Na przykład, jeśli zainstalujemy na naszym komputerze aplikację systemu zarządzania bazą danych MySQL, będzie ona działać na porcie 3306. Trzecia i ostatnia grupa, dynamiczny numer portu, jest losowo przypisywana do aplikacji klienckiej, np. gdy klient wysyła do serwera żądanie udostępnienia strony internetowej, serwer domyślnie akceptuje żądanie na porcie 80, ale klient otrzymuje żądanie z serwera. Przychodząca odpowiedź nie zostanie wysłana na port 80, ponieważ jest on zarezerwowany dla procesu serwera WWW, ale na losową liczbę portów przydzielonych z puli portów dynamicznych.

Wiele aplikacji nie może działać na tym samym numerze portu. Gdy dana aplikacja działa na porcie 53 (DNS), niemożliwe jest, aby inna aplikacja nie mogła już działać na tym porcie.

Jeśli już wiemy, czym jest port aplikacji, przedstawmy inną koncepcję. To będzie gniazdo.
Z pojęciem gniazd spotkałeś się już podczas omawiania płyt głównych i procesorów na zajęciach z technologii komputerowych, pojawia się ono również w sieciach komputerowych. Gniazdo to kombinacja adresu IP i numeru portu:

192.168.20.20:80

Gniazdo jednoznacznie identyfikuje dany proces działający na urządzeniu, więc na przykład, gdy nasza przeglądarka będzie odwoływać się do serwera WWW, aby obsłużyć stronę internetową, żądania serwera będą wysyłane do jego gniazda, procesu (aplikacji serwera WWW).

10.1. Nagłówek TCP

TCP to złożony, zorientowany na połączenie protokół, którego celem jest zagwarantowanie niezawodnego przesyłania danych i kontroli przepływu. Podczas enkapsulacji do nagłówka TCP dodawanych jest do 20 bajtów danych kontrolnych, ale jest to wymagane dla niezawodności TCP. Aplikacje korzystające z tego protokołu obejmują przeglądarki internetowe, klienty poczty e-mail i programy do przesyłania plików. Poniżej możesz zobaczyć tryb segmentu TCP. Liczby w nawiasach oznaczają liczbę bitów zarezerwowanych dla danego pola.

<table>
<tr><td colspan="3">BIT (0)</td><td>BIT (15) BIT (16)</td><td>BIT (31)</td></tr>
<tr><td colspan="3">Port źródłowy (16)</td><td colspan="2">Port docelowy (16)</td></tr>
<tr><td colspan="5">Numer sekwencyjny (32)</td></tr>
<tr><td colspan="5">Numer potwierdzenia (32)</td></tr>
<tr><td>Długość nagłówka (4)</td><td>Zarezerwowane (6)</td><td>Bity kodu (flagi) (6)</td><td colspan="2">Okno (16)</td></tr>
<tr><td colspan="3">Suma kontrolna (16)</td><td colspan="2">Wskaźnik pilności (16)</td></tr>
<tr><td colspan="5">Opcje (0 lub 32)</td></tr>
<tr><td colspan="5">Dane warstwy aplikacji (dł. zmienna)</td></tr>
</table>

- Port źródłowy — port aplikacji wysyłającej dane.
- Port docelowy — port aplikacji, do którego wysyłane są dane.
- Numer sekwencji — numer ostatniego bajtu w segmencie.
- Numer potwierdzenia — numer następnego bajtu oczekiwany przez odbiorcę.
- Długość — długość całego segmentu TCP.
- Bity kodu (flagi) — kontroluj informacje o segmencie.
- Okno - Ilość danych, które można przesłać bez potwierdzenia.
- Suma kontrolna — służy do weryfikacji przesłanych danych.
- Wskaźnik awaryjny — używany tylko wtedy, gdy ustawiona jest flaga URG.

10.2. Uzgadnianie? 3-etapowe

TCP jest protokołem połączenia, co oznacza, że zanim host źródłowy będzie mógł wysłać jakiekolwiek dane do hosta docelowego, musi zostać między nimi nawiązane połączenie. Ta kombinacja nazywana jest trójstronnym uściskiem dłoni. Host źródłowy, czyli klient, wysyła segment zawierający flagę SYN (SYN to flaga synchronizacji numeru seryjnego), a segment zawiera również losowy numer seryjny klienta (zwany również numerem ISN, SEQ=100), który służy do kolejnych scalonych fragmentów danych.

Po otrzymaniu tego segmentu host docelowy, czyli serwer, jest informowany, że klient chce nawiązać z nim połączenie. W odpowiedzi serwer wysyła segment z ustawionymi flagami SYN i ACK (flaga ACK informuje klienta, że serwer odebrał poprzedni segment), numer sekwencyjny otrzymany od klienta jest zwiększany o 1 (ACK = 101) i jego losowy numer kolejny (SEQ = 300).

Na koniec klient wysyła segment z powrotem do serwera z ustawioną flagą ACK, potwierdzając odbiór poprzedniej wiadomości z numerem sekwencyjnym serwera zwiększonym o 1 (SEQ=101, ACK=301). To kończy proces połączenia i umożliwia prawidłowe przesyłanie danych. Poniżej przedstawiono trzyetapowy proces uzgadniania.

Dopiero po nawiązaniu połączenia TCP z serwerem klient może przesłać odpowiednie dane, takie jak żądanie strony internetowej lub pliku.

Wreszcie, gdy wszystkie dane zostaną przesłane, sesja musi zostać zamknięta. Klient wysyła następnie segment do serwera z flagą FIN, która informuje serwer o zamiarze zamknięcia sesji, który odpowiada segmentem potwierdzającym z flagą ACK, że otrzymał taki segment. Następnie serwer wysyła również segment z flagą FIN, a klient odpowiada segmentem potwierdzenia z flagą ACK. Spowoduje to zamknięcie sesji TCP.

Flaga	**Zastosowanie**
URG	Informuje o istnieniu pola wskaźnik pilności w nagłówku (urgent)
ACK	Informuje o istnieniu pola numer potwierdzenia w nagłówku (acknowledgment)
PSH	Wymuszenie przesłania pakietu (push)
RST	Ponowne zestawienie połączenia (reset)
SYN	Synchornizacja numerów sekwencyjnych
FIN	Koniec danych od nadawcy

10.3. Okno TCP

Niezawodność dostarczenia danych w ramach sesji z wykorzystaniem protokołu TCP polega na przesłaniu przez klienta potwierdzenia odebrania wcześniej przesłanych danych. Zanim serwer będzie mógł wysłać kolejną porcję danych do klienta, musi otrzymać takie potwierdzenie odbioru. Czasami powoduje to opóźnienia w dostarczaniu segmentów, ponieważ nie są one wysyłane w sposób ciągły. Jednak te problemy są dopuszczalne, gdy wymagana jest niezawodność komunikacji.

Zakładając, że w segmencie o numerze sekwencyjnym 1 zostanie wysłanych 1000 bajtów danych, gdy klient odbierze 1 część danych, wyśle segment z numerem potwierdzenia 1001 do serwera. Następny bajt, zaczynając od bajtu 1001. Gdy serwer wyśle jeszcze 1000 bajtów, otrzymanym numerem potwierdzenia będzie 2001, następna liczba to 3001, następna 4001
i tak dalej.

Oczywiście w rzeczywistości, gdy host musi każdorazowo potwierdzać otrzymanie tak małej ilości danych, może to spowodować duże przeciążenie łącza, np. czas ładowania strony może być długi. W związku z tym przesyłanych jest więcej danych, które są potwierdzane informacją zwrotną. Ilość danych, które serwer może wysłać przed otrzymaniem potwierdzenia od klienta, nazywana jest rozmiarem okna, w tym przypadku 3000 bajtów.

Rozmiar ten jest określony w nagłówku segmentu TCP i oprócz określania, ile danych można przesłać bez potwierdzenia, pozwala kontrolować przepływ danych między urządzeniami. Jeśli klient napotka blokowanie podczas odbierania danych i dany segment zostanie utracony, urządzenie może wysłać informacje do serwera, aby zmniejszyć rozmiar tego okna, ilość danych, które można odebrać bez potwierdzenia, spowalniając transfer,
ale zapobiegając utracie segmentu. Po pewnym czasie rozmiar okna powraca do swojego pierwotnego rozmiaru. Zmiana rozmiaru okna podczas transferu nazywana jest oknem dynamicznym lub oknem przesuwnym.

10.4. Protokół UDP

Innym protokołem, który realizuje niektóre funkcje warstwy transportowej, jest protokół UDP. W tym przypadku jest to jednak znacznie prostsze, ponieważ protokół nie implementuje żadnego mechanizmu gwarantującego niezawodność dostarczania danych czy kontrolę przepływu.

Protokół UDP jest prostym protokołem bezpołączeniowym, a jego największą zaletą jest niski narzut danych sterujących dodawanych w procesie enkapsulacji. UDP w datagramie dodaje tylko 8 bajtów danych kontrolnych. Nagłówek datagramu UDP wygląda tak:

BIT (0)	**BIT (15) BIT (16)**	**BIT (31)**
Port źródłowy (16)	Port docelowy (16)	
Długość (16)	Suma kontrolna (16)	
Długość warstwy aplikacji (dł. zmienna)		

· Port źródłowy — określa port aplikacji, z którego mają być wysyłane dane.

· Port docelowy — określa port aplikacji, do którego wysyłane są dane.

· Długość - 16-bitowe pole określające długość całego datagramu UDP

· Suma kontrolna — 16-bitowe pole używane do sprawdzania poprawności wysyłanych danych.

Bezpołączeniowy UDP oznacza, że host źródłowy nie wysyła żadnych informacji w celu ustanowienia połączenia z hostem docelowym przed rozpoczęciem procesu komunikacji. Ogólna zasada jest taka, że jeśli urządzenie źródłowe chce rozpocząć transfer, chce wysłać dane, które właśnie zakończyło, bez wcześniejszego uzgodnienia.

Jeśli porównamy to do komunikacji międzyludzkiej, to w przypadku protokołu TCP byłoby to coś w stylu: Hej Tomek, skup się, bo zaraz będę z tobą rozmawiał i dopiero jak dostanę ten komunikat Rozpocznie się normalna rozmowa, oczywiście tylko wtedy, gdy Tomek odpowie: OK, zacznę słuchać. W przypadku UDP nie powiadomił Toma, że mam zamiar zacząć komunikować mu coś ważnego, po prostu zacząłem rozmowę.

Aplikacje lub usługi korzystające z tego protokołu transportowego obejmują DNS, DHCP, telefonię VoIP i strumieniowe przesyłanie wideo.

Dlaczego te? Cóż, odpowiedź jest prosta, aplikacje te cenią szybkość nad niezawodność komunikacji, a właściwie konieczność odbierania wszystkich przesyłanych danych. Wyobraź sobie sytuację, w której oglądamy transmisję wideo lub gramy ze znajomymi, jak CS. Trudno jest rywalizować w grze lub oglądać cokolwiek, gdy pakiety się spóźniają.

Ktoś mógłby zapytać: ale skąd to opóźnienie? Cóż, na przykład segmenty TCP są znacznie większe niż datagramy UDP, a TCP musi potwierdzać dostarczone dane, więc są przesyłane przez sieć w dużych ilościach, więcej niż w UDP.

W przypadku aplikacji korzystających z tego konkretnego protokołu można tolerować,
że czasami pakiety mogą zostać utracone lub uszkodzone. W przypadku usług DNS, jeśli datagram zostanie utracony, zapytanie jest po prostu ponownie wysyłane do serwera DNS
i nie byłoby tragedią, gdyby datagram nie dotarł podczas sesji, ponieważ komunikaty zawsze mogą się powtórzyć. W przypadku aplikacji korzystających z protokołu TCP strata lub pomyłka nie jest już akceptowalna. Datagramy odbierane są w kolejności, w jakiej są odbierane, a jeśli jest ich wiele, za ich prawidłowy montaż odpowiada konkretna aplikacja.

10.5. Polecenie NETSTAT

Jak mogę wyświetlić połączone połączenia naszego komputera z różnymi serwerami
w systemie Windows? W tym celu można skorzystać z programu Wireshark, dzięki któremu mogliśmy sprawdzić wszystko, co przechodzi przez naszą kartę sieciową, a także skorzystać
z polecenia NETSTAT w konsoli Windows. Po wprowadzeniu możemy śledzić, jakie mamy aktywne połączenia. Dane wyjściowe tego polecenia pokazują typ protokołu warstwy transportowej używanego do połączenia, gniazdo mojego komputera, czyli adres IP
z numerem portu, gniazdo serwera, z którym jesteśmy połączeni, oraz stan połączenia.

Programy można wywoływać z różnymi argumentami, a ich lista i opis zostaną wyświetlone po wpisaniu polecenia netstat /help.

Jak widać na powyższym obrazku, tych połączeń jest bardzo dużo, a to dlatego, że przede wszystkim używam Windowsa 10, o którym wiadomo, że prawie cały czas coś wysyła na serwery Microsoftu, a poza tym ja skonfigurowałem synchronizację z usługami w chmurze
i istnieje program antywirusowy, który również łączy się ze swoimi serwerami. Jak więc sprawdzić, do jakich usług podłączony jest nasz komputer? Wystarczy uruchomić polecenie netstat -f i skopiować nazwę domeny (PPM -> Tag -> Select Domain Name -> CTRL + C lub PPM -> Copy).

Możemy zobaczyć właściciela domeny poprzez stronę whois.domaintools.com i jej wyszukiwarkę. Wystarczy wkleić skopiowaną nazwę domeny. Jak widać, właścicielem tej domeny jest Google.

11. Zadania i protokoły warstwy sieciowej

Warstwa sieciowa (model ISO/OSI – warstwa 3), znana również jako warstwa internetowa, odbiera pofragmentowane dane z warstwy transportowej, a następnie wykonuje operacje umożliwiające przesyłanie pakietów przez sieć. Działania te obejmują:

- Adresowanie danych z wykorzystaniem adresów IP;
- Enkapsulacja danych, czyli przypisanie dodatkowych informacji wymaganych przez używany protokół warstwy sieciowej;
- Routing, czyli wybór najlepszej trasy dla paczki;
- Dekapsulacja, która usuwa te dodatkowe informacje, gdy pakiet dotrze do miejsca docelowego.

Wiemy, że komunikacja sieciowa rządzi się pewnymi regułami, protokołem komunikacyjnym. Wiemy również, że każda warstwa korzysta z własnego protokołu, niezależnego od drugiej. Warstwa sieciowa, w której również się pojawiają, nie różni się. Najpopularniejszym protokołem komunikacyjnym dla tej warstwy jest IPv4. Najważniejszym powodem, dla którego warto go używać, jest to, że jest to protokół otwarty. Oznacza to, że nie należy do żadnej firmy ani firmy, więc może komunikować się między urządzeniami różnych producentów. Już teraz śledzi IPv6, który jest również protokołem otwartym.

Obecnie wielu producentów urządzeń i oprogramowania korzysta z tych protokołów równolegle. Może w przyszłości IPv6 całkowicie zastąpi IPv4, ale nie sądzę, że to za wcześnie. Oczywiście istnieją również protokoły zastrzeżone dla konkretnych firm, takie jak protokół IPX należący do firmy Novell, która specjalizuje się w tworzeniu sieciowych systemów operacyjnych, czy protokół AppleTalk opracowany przez firmę Apple. Można jednak śmiało powiedzieć, że protokół IPv4 jest zdecydowanie najczęściej używanym protokołem warstwy sieciowej.

11.1. Protokół IPv4

Protokół IPv4 został zaprojektowany w taki sposób, że nie ma potrzeby dodawania dużej ilości danych kontrolnych podczas procesu enkapsulacji. Zapewnia tylko podstawową funkcjonalność wymaganą do przesyłania pakietów ze źródła do miejsca docelowego. Jest bezpołączeniowy, co oznacza, że nie nawiązuje połączenia przed wysłaniem danych i działa na zasadzie „najlepszego wysiłku", co oznacza, że nie używa kontroli przepływu ani żadnych potwierdzeń dostarczenia danych, jak robi to protokół TCP, ale robi wszystko, co w jego mocy aby komunikacja była skuteczna. Jest to również protokół niezależny od medium, co oznacza, że dane mogą być przesyłane między hostami niezależnie od używanego medium.

Wszak w jednej sieci możemy używać skrętki, w innej światłowody, aw trzeciej fale radiowe. Protokół IP działa dokładnie tak samo w każdej sieci. Problemem, który może się pojawić przy przesyłaniu danych na różnych nośnikach jest maksymalny rozmiar pakietu, który jest wartością MTU (Maximum Transmission Unit), jeśli pakiet będzie zbyt duży, routery podłączone do sieci podzielą go na mniejsze części. Proces ten nazywamy fragmentacją, co jest kolejnym terminem z naszego słownika internetowego.

Aby ułatwić zrozumienie działania protokołu IPv4 i sposobu przesyłania pakietów przez Internet, posłużę się przykładem paczki wysłanej przez moją ciotkę ze Stanów Zjednoczonych do wyjaśnienia jej działania. Opakowanie składa się z 3 kartonów połączonych w jedną całość. Ciociu napisała adres na prezent i wysłała go do firmy kurierskiej. Wysyłając paczkę, rezygnuje z dodatkowych opcji, takich jak potwierdzenie odbioru czy śledzenie przesyłki. Pracownik firmy przed wydaniem paczki oznacza karton miejscem docelowym i adresem zwrotnym. Został przewieziony samochodem do portu wraz z dziesiątkami innych paczek, gdzie został zapakowany w kontener, a następnie przepłynął przez ocean.

W porcie przeznaczenia kontenery są rozpakowywane, paczki sortowane, a następnie przewożone samochodem do różnych miast i lokalnych punktów odbioru. Z punktu odbioru samochodem paczka ma być dostarczona pod wskazany adres, ale okazuje się, że trzy połączone kartony są zbyt duże, aby można je było przewieźć na wózku, więc kurier rozdziela je na poszczególne kartony i dostarcza do ty jako taki. Ponieważ ciocia nie wybrała opcji dodatkowych, firma kurierska nie dostarczyła jej potwierdzenia odbioru. Możesz to zrobić sam, np. zadzwoń do cioci, aby podziękować 🙂

Przekształcenie tego na komunikację za pomocą protokołu IP wyglądałoby tak:

· Paczka wysyłana jest bez uprzedniego powiadomienia odbiorcy - mamy tryb bezpołączeniowy;

· Podczas procesu enkapsulacji przydzielany jest adres źródłowy i docelowy
– w naszym przypadku adres domowy odbiorcy jest adresem docelowym, a adres domowy ciotki jest adresem zwrotnym;

· Przesyłka nie zawierała zbyt wielu danych kontrolnych, które mogłyby spowolnić komunikację - za to ciocia zrezygnowała z dodatkowej opcji, potwierdzenia i śledzenia przesyłki;

· Paczki docierają do miejsca przeznaczenia za pośrednictwem światłowodów, skrętek
i fal radiowych - ponieważ paczki dostarczane są różnymi środkami transportu: łodziami, dużymi samochodami, małymi samochodami;

· Paczka jest zbyt duża, aby wysłać ją w całości przez jedną z sieci, przez co jest rozdrobniona – tzn. paczka jest w pewnym momencie rozdzielona, aby można ją było przewieźć małym samochodem;

· Protokół IP nie wysłał potwierdzenia otrzymania paczki - tak jak firma nie zapewniła cioci, że paczka dotarła.

Jak każdy protokół komunikacyjny, IPv4 ma również ustandaryzowane nagłówki, które umożliwiają dodawanie informacji kontrolnych. Poniżej przedstawiono przykład typowego nagłówka IPv4.

<table>
<tr><td>Wersja</td><td>IHL</td><td>Typ usługi</td><td colspan="2">Długość pakietu</td></tr>
<tr><td colspan="3">Identyfikacja</td><td>Flaga</td><td>Przesunięcie fragmentu</td></tr>
<tr><td>TTL</td><td colspan="2">Protokół</td><td colspan="2">Suma kontrolna nagłówka</td></tr>
<tr><td colspan="5">Adres źródłowy</td></tr>
<tr><td colspan="5">Adres docelowy</td></tr>
<tr><td colspan="3">Opcje</td><td colspan="2">Wypełnienie</td></tr>
</table>

· docelowy adres IP – adres IP urządzenia, do którego kierowane są dane;

· źródłowy adres IP – adres IP urządzenia będącego nadawcą danych;

· Czas życia (TTL) — 8-bitowe pole określające pozostały czas życia pakietu. Wartość TTL zmniejsza się o co najmniej 1 za każdym razem, gdy pakiet przechodzi przez router (to znaczy po każdym przeskoku). Gdy wartość osiągnie 0, router odrzuca pakiet i usuwa go z przepływu danych w sieci. Mechanizm ten zapobiega nieskończonemu przesyłaniu pakietów, które nie mogą dotrzeć do celu, między tak zwanymi routerami. pętle routingu. Jeśli pętle routingu są dozwolone, sieć zostanie przeciążona pakietami, które nigdy nie dotrą do celu. Zmniejszenie wartości TTL przy każdym przeskoku zapewnia, że ostatecznie osiągnie ona 0, a pakiety z polem TTL równym 0 zostaną odrzucone.

· Protokół — ta 8-bitowa wartość określa używany protokół warstwy wyższej (transportowej), taki jak UDP lub TCP.

· Type of Service (ToS) — zawiera 8-bitową wartość, która określa priorytet każdego pakietu.

· Fragment Offset - Pole używane podczas rekonstrukcji pakietów podzielonych przez routery. Wskazuje kolejność, w jakiej każdy pakiet powinien być ułożony podczas rekonstrukcji.

· Flaga More Fragments (MF) - Pojedynczy bit używany z polem Fragment Offset do partycjonowania i rekonstrukcji pakietów. Ustawienie flagi MF oznacza, że dany fragment nie jest ostatnim fragmentem pakietu. Gdy host odbierający zauważy przychodzący pakiet z ustawionym MF = 1, sprawdza pole przesunięcia fragmentu, aby umieścić fragment podczas rekonstrukcji pakietu. Gdy host odbierający zauważy, że przychodzący pakiet ma ustawione MF = 0 i ma niezerową wartość w polu przesunięcia fragmentu, użyje tego fragmentu jako ostatniego bloku zrekonstruowanego pakietu.

· Flaga DF (Don't Fragment) — Pojedynczy bit, który, jeśli jest ustawiony, oznacza, że fragmentacja pakietów jest niedozwolona. Fragmentacja pakietu nie jest dozwolona, jeśli ustawiona jest flaga DF.

· Wersja — zawiera numer wersji protokołu IP (w tym przypadku IPv4).

· Długość nagłówka (IHL) — określa rozmiar nagłówka pakietu.

· Długość pakietu — to pole podaje całkowity rozmiar pakietu w bajtach, łącznie z nagłówkiem i danymi.

· Identyfikacja — to pole służy do jednoznacznej identyfikacji fragmentu podzielonego pakietu IP.

· Suma kontrolna nagłówka — to pole służy do sprawdzania błędów nagłówka pakietu.

· OPCJE — jest to miejsce w nagłówku IPv4 na dodatkowe pola do obsługi innych usług. Jednak jest rzadko używany.

11.2. Adresowanie IPv4

Jednym z kluczowych zadań warstwy sieciowej jest adresowanie. Adresowanie w sieciach IP jest bardzo podobne do adresowania, którego używamy my, ludzie. Oczywiście tylko na poziomie logicznym mechanizm adresowania jest inny. Hosty w sieci są pogrupowane w celu łatwego zarządzania i adresowania.

Podobnie jak ludzie mieszkamy na konkretnych ulicach miast. Dzięki temu powyższa przesyłka mojej amerykańskiej ciotki bez problemu dotrze do odbiorcy. Najpierw promem do Polski, potem ciężarówką do Twojego miasta, a potem mniejszym samochodem na ulicę
i numer domu. Jest to bardzo podobne do adresowania hosta. Pakiety wysyłane między sieciami najpierw docierają do sieci, do której należy host, a następnie są wysyłane do określonego hosta. Ten rodzaj adresowania nazywa się adresowaniem hierarchicznym, ponieważ najpierw odczytywana jest informacja ogólna, czyli w przypadku przesyłania danych, adres sieciowy, a następnie informacje szczegółowe, czyli adres IP konkretnego hosta.

[Rozbudowany tutorial dotyczący adresowania IP, wraz z omówieniem jak wykonywać obliczenia na adresach IPv4, znajdziesz na naszym kanale:

]

W sieci komputerowej hosty mogą komunikować się ze sobą na trzy sposoby:

· użyj transmisji pojedynczej;

· za pośrednictwem multiemisji;

· za pośrednictwem transmisji.

Transmisja unicast jest najbardziej powszechna i jest używana do typowego połączenia między dwoma hostami. Na przykład, gdy klient wysyła żądanie do serwera, używa do tego transportu emisji pojedynczej.

Korzystanie z transmisji multicast może znacznie zmniejszyć zużycie przepustowości w sieci, ponieważ pojedynczy pakiet nie jest wysyłany do wielu hostów, tak jak transmisja unicast, ale wysyłany jest jeden pakiet, który może dotrzeć do wielu odbiorców jednocześnie.

Routery mogą używać multiemisji do wymiany informacji o routingu i dystrybucji oprogramowania. W transmisji multicastowej wykorzystywana jest specjalna pula adresów, zwana adresami grupowymi, a w protokole IPv4 jest to zakres pokazany poniżej:

od **224.0.0.0** do **239.255.255.255**

Broadcast z kolei wysyła pakiet do wszystkich hostów w danej sieci. Używany jest do tego specjalny adres, adres rozgłoszeniowy, dzięki czemu adresy wszystkich hostów w sieci nie są przechowywane w pakietach IP. Jest to technicznie niemożliwe, wtedy użycie jednej i dwóch emisji, na przykład, gdy adres konkretnego urządzenia jest nieznany. Ten rodzaj transportu jest najczęściej używany w sieciach lokalnych, a rozgłaszanie jest rzadko używane do komunikowania się z hostami poza daną siecią lokalną.

W całej puli adresów IPv4 występują różne grupy adresów, tzw. specjalnego przeznaczenia. Są to adresy, które nie są używane do komunikacji WAN. Wśród tych specjalnych adresów znajdują się tak zwane adresy pętli zwrotnej. Adres pętli zwrotnej to nic innego jak własny adres.Oprócz prawidłowego adresu IP używanego do komunikacji, każdy komputer w sieci ma również przypisany własny adres, najczęściej jest to adres 127.0.0.1. Ponadto każdy adres w puli służy do weryfikacji konfiguracji IPv4 na hoście.

Innym specjalnym rodzajem adresu jest adres lokalny łącza. Te typy adresów są używane, gdy host powinien uzyskać adres IP z serwera DHCP, ale z jakiegoś powodu adres jest niedostępny. Host otrzyma wtedy adres z lokalnej puli adresów łącza. Transfery danych przy użyciu takich adresów mogą odbywać się tylko w sieci lokalnej, w której działają dane hosta. Istnieje również ostateczny zestaw adresów specjalnych, adresy TEST-NET. Podobnie jak w przypadku adresów połączonych lokalnie, są one wykorzystywane wyłącznie do komunikacji w sieci lokalnej, w celach edukacyjnych. Można ich używać w dokumentacji lub przykładach, takich jak kursy online. Nie należy ich jednak używać na stałe. Specjalne zakresy adresów przedstawiono w poniższej tabeli:

Zakres adresów	**Nazwa**
127.0.0.1 – 127.255.255.254	Pętla zwrotna (Loopback)
169.254.0.1 – 169.254.255.254	Łącze lokalne (Local-Link)
192.0.2.0 – 192.0.2.254	Edukacyjne (Test-Net)

11.3. Testowanie warstwy sieciowej

Każdy system operacyjny implementuje programy, które pozwalają nam przetestować warstwę sieciową. Jednym z nich jest program PING, który służy do testowania łączności między hostami. Ta nazwa jest dostępna w systemie Windows i różnych dystrybucjach systemu Linux. Drugi to program TRACERT, który służy do testowania routingu między hostem źródłowym a hostem docelowym. W systemach opartych na jądrze Linux ten sam program nazywa się TRACEROUTE.

PING używa innego protokołu warstwy sieci, ICMP, do wysyłania datagramu z żądaniem echa i oczekiwania na odpowiedź. Po otrzymaniu odpowiedzi pokazuje nam czas, jaki upłynął od wysłania prośby do otrzymania informacji zwrotnej. PING może być używany do testowania:

· Tak zwany stos lokalny, czyli aby zweryfikować poprawność instalacji protokołu IP na komputerze wystarczy wpisać w konsoli Windows komendę PING, korzystając z jednego z adresów sprzężenia zwrotnego, czyli z zakresu 127.0.0.1 do 127.255.255.254:

· Nawiązywane jest połączenie z hostem w sieci lokalnej, następnie zamiast adresu pętli zwrotnej wpisujemy adres hosta w sieci lokalnej (np. 192.168.0.1):

· Połącz się z hostem w sieci zdalnej. Tutaj, jeśli chcesz sprawdzić komunikację z serwerem, na którym przechowywana jest strona, możesz zamiast adresu IP wpisać nazwę domeny, czyli facebook.com:

Czasami możemy nie otrzymać odpowiedzi na żądanie echa wysłane przez program PING, nawet jeśli sieć zdalna działa i komunikuje się poprawnie. Dzieje się tak, ponieważ niektórzy administratorzy sieci ograniczają lub całkowicie uniemożliwiają wstawianie datagramów ICMP do swoich sieci ze względów bezpieczeństwa.

Inną częścią testowania warstwy sieciowej jest badanie routingu pakietów od hosta źródłowego do hosta docelowego. W sieci rozległej pracują tysiące routerów, tworząc tzw. Internet, połączenia między sieciami lokalnymi rozsianymi po całym świecie.

Aby sprawdzić przez jakie routery przesyłany jest pakiet, np. z komputera na serwer WWW, posłużymy się programem TRACERT dla systemów Windows lub TRACEROUTE dla systemów Linux. Działają dokładnie w ten sam sposób i podobnie jak PING, używają protokołu ICMP i komunikatów echa. Aby wykonać test, po prostu wpisz TRACERT w konsoli wraz z adresem hosta docelowego. Może to być adres IP, lub adres domeny, jeśli chcemy przetestować routing do konkretnego hosta, np. wp.pl.

Poniżej możesz zobaczyć test routingu do serwera, na którym przechowywana jest strona Wirtualnej Polski.

12. Zadania warstwy łącza danych

Główną i zasadniczą rolą warstwy łącza danych jest zapewnienie wyższym warstwom dostępu do medium transmisyjnego. Dane przemieszczające się w dół stosu podczas przechodzenia przez warstwy muszą w pewnym momencie zostać dostarczone do nośnika danych, przez który docierają do miejsca docelowego, hosta odbiorczego. Jest to podstawowa funkcja warstwy łącza danych: przechowuje dane z wyższych warstw na nośniku.

Warstwa sieciowa omówiona w poprzednim odcinku tego kursu obejmowała segmenty
z adresami IP otrzymanymi z warstwy transportowej podczas procesu enkapsulacji w celu tworzenia pakietów. Pakiety te docierają do warstwy łącza danych przed wysłaniem do hosta docelowego, a następnie przechodzą przez warstwę łącza danych do medium transmisyjnego. Wcześniej jednak pakiety otrzymywały dalsze informacje kontrolne, tym razem były to fizyczny adres urządzenia, 48-bitowy adres MAC.

Pakiety stają się wtedy ramkami i to właśnie te ramki trafiają do nośnika w celu dalszej transmisji do hosta docelowego. Adres MAC jest przypisywany podczas produkcji karty
i przechowywany w pamięci ROM. ROM jest tylko do odczytu, więc nie ma możliwości zmiany przypisanych adresów na poziomie karty i na poziomie sprzętu. Jednak takie adresy można zmienić na poziomie systemu urządzenia, na przykład w systemie operacyjnym. Czasami administratorzy wprowadzają takie zmiany na poziomie systemu, np. gdy nie chcą rekonfigurować sprzętu sieciowego, np. gdy w sieci pojawia się nowy komputer.

Sama warstwa łącza danych jest pośrednikiem między medium transmisyjnym,
a oprogramowaniem sieciowym. W przypadku urządzeń końcowych, tj. komputerów, serwerów czy telefonów, jest to jedyna warstwa zaimplementowana nie tylko w domenie programowej, ale również sprzętowej. Fizycznym odzwierciedleniem warstwy łącza danych jest karta sieciowa, którą instalujemy w naszym komputerze. Karty te stanowią interfejs między oprogramowaniem sieciowym a medium transmisyjnym. Ponieważ warstwa łącza danych działa na dwóch poziomach, na poziomie sprzętu i oprogramowania, jej funkcje
i zadania są również podzielone na dwie mniejsze podwarstwy:

- LLC (Kontrola łączy logicznych),
- MAC (kontrola dostępu do mediów).

Podwarstwa LLC ramkuje informacje o używanym protokole warstwy sieciowej, dzięki czemu różne protokoły warstwy sieci, takie jak IPv4, IPv6 lub IPX, mogą korzystać z tego samego medium transmisyjnego i karty sieciowej, a jej funkcje w komputerze są wykonywane przez sterownik karty sieciowej. Z drugiej strony podwarstwa MAC określa zasady dostępu do medium i wykonuje funkcje adresowania. Metoda MAC została omówiona w pierwszym odcinku tej serii.

Podsumowując – warstwa łącza danych:

- odbierać dane z warstwy sieciowej,
- tworzyć ramki, które można przesyłać za pośrednictwem medium,
- podaje fizyczny adres ramki,
- Odpowiada za kontrolę dostępu do medium.

Warstwa ta jest implementowana na urządzeniach końcowych takich jak komputery,
ale także na routerach i przełącznikach.

Ramka warstwy łącza danych i komunikacja

Istnieje wiele rozwiązań i wiele standardów sieciowych do implementacji funkcjonalności warstwy 2. Mamy standardy Ethernet, mamy sieci bezprzewodowe, w końcu mamy wiele protokołów sieciowych działających w sieciach WAN, takich jak Frame Relay. Nie ma więc czegoś takiego jak uniwersalna ramka. Każdy standard sieciowy ma własną strukturę, specyficzną dla konkretnego rozwiązania. Podsumowując temat, możemy założyć, że typowy framework drugiego poziomu składa się z 3 głównych części:

Nagłówek	Dane	Stopka
adresy MAC źródłowy i docelowy **sygnał początku ramki**	pakiety warstwy sieciowej / internetowej	sygnał końca ramki **suma kontrolna**

Prześledźmy teraz proces komunikacji między urządzeniami, skupiając się na funkcjach warstwy łącza danych. Załóżmy, że nasz komputer wysyła żądanie do serwera WWW w sieci zdalnej.

Dane do wysłania takiego zapytania są już enkapsulowane w jeden pakiet z numerem portu aplikacji i adresem logicznym, czyli adresem IP komputera i serwera.

Zanim pakiet wejdzie do medium transmisyjnego, warstwa łącza danych musi skonstruować ramkę z odpowiednimi adresami MAC nadawcy i odbiorcy ramki. W przypadku adresu MAC nadawcy rzecz jest oczywista, to tylko adres MAC komputera, ale co z adresem hosta docelowego? Jeśli komputer i serwer WWW nie znajdują się w tej samej sieci i nie można ustalić adresu MAC jego karty sieciowej, nie ma takiej możliwości, co jest technicznie niewykonalne. Czemu? Ponieważ adresy MAC są używane tylko do komunikacji w danej sieci i nigdy poza jej obszarem. Dlatego w polu ramki zawierającej docelowy adres MAC zostanie zapisany adres MAC interfejsu routera, do którego podłączony jest nasz komputer.

Ramka jest wysyłana przez medium transmisyjne do pierwszego routera. Ten ostatni po odebraniu ramki dekapsuluje ją tak, aby mógł odczytać adres IP urządzenia, do którego zmierza pakiet. Adresy IP nie mogą być odczytywane bezpośrednio z ramek warstwy 2, dlatego wymagana jest dekapsulacja. Po odczytaniu adresu IP z pakietu (po dekapsulacji ramki dane stają się ponownie pakietem), porównaj go z wpisem w tablicy routingu i znajdź wpis, który wskazuje, że sieć serwerów jest trasowana przez inne routery.

Następnie utworzy nową ramkę, w której adresem źródłowym będzie adres MAC interfejsu, który łączy z drugim routerem, oraz docelowy adres MAC tego routera.

Ramka następnie przechodzi przez nośnik do drugiego routera, który ponownie hermetyzuje ramkę w celu odczytania adresu IP z pakietu. Stwierdza, że odbiorcą danych jest urządzenie pracujące w sieci, bezpośrednio z nią połączone, więc proces enkapsulacji wykonywany przez drugi router dzieje się ponownie, tym razem w polu adresu MAC wpisuje adres MAC swojego drugiego routera. interfejs jest używany jako adres źródłowy, a adres MAC serwera adresowego jest używany jako adres docelowy.

Tak przygotowane ramki trafiają na serwer, który również je dekapsuluje. Tym razem jednak jest to urządzenie, na które wskazują dane, więc dekapsuluje je całkowicie, czyli dodatkowo odczytuje numer portu aplikacji w celu przesłania danych do odpowiedniej konkretnej aplikacji, w tym przypadku serwisu WWW.

Następnie usługa sieciowa przygotowuje dane odpowiedzi. Dane trafiają najpierw do warstwy transportowej, gdzie nadawany jest numer portu aplikacji, następnie do warstwy sieciowej, tworząc pakiet z odpowiednim adresem IP, a na końcu do warstwy łącza danych, gdzie z pakietu przygotowywana jest ramka, zaznaczona z adresami MAC serwera i routera dla podłączonego serwera.

Odpowiedź jest następnie przekazywana do mediów, która jest następnie wysyłana do klienta. Podczas tego procesu przechodzi przez dwa routery, które wykonują proces dekapsulacji i rekapsulacji, a ponieważ muszą odczytać adres IP, mogą przekazać odpowiedź. W końcu odpowiedź należy do klienta. Spowoduje to rozpakowanie danych, umożliwiając przeglądarce wyświetlenie strony internetowej.

12.1. Protokół ARP

Jako użytkownicy sieci, gdy przesyłamy dane z jednego urządzenia na drugie, znamy jego adres IP lub nazwę domeny, dzięki czemu możemy wykonywać takie transfery. Jeszcze gorsze są adresy MAC, na ich podstawie my użytkownicy sieci nie określamy odbiorcy danych, dzieje się to poza nami. W sieciach komputerowych opartych na protokole IPv4 do uzyskania informacji o adresie MAC danego urządzenia wykorzystywany jest protokół zwany ARP (Address Resolution Protocol).

ARP to mechanizm, który umożliwia mapowanie adresów logicznych (tj. IP) na adresy fizyczne (tj. MAC). Załóżmy, że komputer, który chce wysłać dane do innego urządzenia, zna swój adres IP, ale nie zna swojego adresu MAC. Aby poznać ten adres, komputer wysyłający dane utworzy ramkę rozgłoszeniową ARP i wyemituje ją do wszystkich urządzeń w tej samej sieci przed wysłaniem określonych danych. W polu adresu źródłowego ramki zapisywany jest adres komputera, który przygotował ramkę, a w polu adresu docelowego rozgłoszeniowy adres MAC: FF-FF-FF-FF-FF-FF.

Każde urządzenie, które odbiera ramkę, dekapsuluje ją do pakietu i sprawdza, czy adres IP pola docelowego jest jego adresem. Jeśli docelowy adres IP jest inny niż jego, zignoruje pakiet, jeśli jest to jego adres IP, utworzy nową ramkę, w której zostanie zapisany jego adres MAC i wyśle go do transmisji.

Komputer wysyłający ramkę rozgłoszeniową zna teraz fizyczny adres urządzenia, z którym chce się komunikować, i może rozpocząć tę komunikację. Informacje o mapowaniu IP na MAC są przechowywane w tabeli ARP każdego urządzenia do późniejszego wykorzystania. Domyślnie w systemach Windows takie wpisy trwają do 10 minut, a następnie są usuwane. Aby wyświetlić tabelę ARP, uruchom arp -a z konsoli. Jak widać, jest tu kilka wpisów, co oznacza, że w ciągu ostatnich 10 minut była komunikacja między moim komputerem a innym urządzeniem.

12.2. Ethernet

Prace nad tym standardem sięgają lat 70-tych, kiedy Xerox, jedna z największych firm technologicznych, postanowiła zaprojektować otwarty standard komunikacji sieciowej, który służyłby ludziom przez lata. Pod koniec lat 70. opracował standard dla lokalnych sieci komputerowych i stał się prototypem Ethernetu. Obecnie Ethernet jest standardem, który można znaleźć w większości lokalnych sieci komputerowych na świecie, a ze względu na swoje liczne zalety stał się również standardem dla sieci miejskich, aw niektórych przypadkach nawet sieci rozległych.

Ethernet to kompletny zestaw rozwiązań sieciowych zaimplementowanych zarówno w warstwie łącza danych, jak iw warstwie fizycznej. Rozwój tej technologii jest obecnie nadzorowany przez organizację IEEE (Instytut Inżynierów Elektryków i Elektroników), która opublikowała swój standard w 1985 roku i opisuje go pod numerami 802.2 i 802.3. Standard 802.2 obejmuje funkcje związane z podwarstwą LLC, która jest powiązana z podwarstwą MAC i warstwą fizyczną modelu OSI.

Na sukces rozwiązań opartych na sieci Ethernet składa się wiele czynników, w tym:

- łatwe do wdrożenia,
- niezawodność,
- umiejętność adaptacji nowych technologii,
- Koszty wdrożenia są stosunkowo niskie.

12.3. Rozwój Ethernetu

Omówmy teraz ewolucję Ethernetu. Początkowe wersje standardu, zwane grubymi sieciami (tzw. grubym Ethernetem) i cienkimi sieciami (tzw. cienkimi sieciami ethernetowymi), miały niewiele możliwości w porównaniu do tego, co mamy obecnie. Starsze wersje działają na miedzianym medium transmisyjnym (kabel koncentryczny). Wykorzystują fizyczną topologię magistrali, która charakteryzuje się tym, że wszystkie urządzenia są podłączone do wspólnego medium. Rozwiązanie wymaga kontroli dostępu do mediów, która realizowana jest w podejściu CSMA/CD

Po wielu latach stosowania jako medium transmisyjnego rozwiązań opartych na topologii magistrali okazuje się, że to rozwiązanie nie jest już wystarczająco efektywne. Szybki rozwój sieci doprowadził do coraz wyższych wymagań użytkowników dotyczących jej przepustowości i niezawodności. W miejsce kabli koncentrycznych szeroko stosowane są skrętki dwużyłowe, kable UTP i nowa topologia. Pojawiły się topologie gwiazdy, te same używane dzisiaj, ale wykorzystujące koncentratory zamiast przełączników jako centralny punkt sieci. Nikt wtedy nie słyszał o przełącznikach.

Zastosowanie koncentratorów w pewnym stopniu poprawiło działanie sieci komputerowych, ale szybko okazało się, że i to rozwiązanie nie jest idealne. Podstawową cechą koncentratora jest to, że przesyła dane do wszystkich podłączonych do niego urządzeń. Działa to tak,
że komputer, który chce przesłać dane do innego urządzenia, wykonuje tę komunikację przez koncentrator. Ten drugi z kolei nie jest tak sprytny, aby przenieść dane do odpowiedniego urządzenia, po prostu wysyła dane do wszystkich podłączonych do niego osób.

Tylko urządzenia, do których przesyłane są dane, analizują adresowanie w celu określenia, czy są odbiorcami. Jeśli nie są odbiorcami, ignorują dane, a jeśli tak, interpretują je.

Tego typu rozwiązanie oznacza, że chociaż fizyczna topologia jest topologią gwiazdy, jest logicznie podobna do tej, która była używana w poprzedniej generacji Ethernetu. Również tutaj stosowana jest metoda dostępu do łącza oparta na CSMA/CD, która stała się nieefektywna ze względu na szybki rozwój sieci. Ponadto każdy koncentrator tworzy tak zwaną domenę kolizyjną.

Im więcej urządzeń podłączonych do koncentratora, tym większa domena kolizyjna,
a im większa domena kolizyjna, tym większe prawdopodobieństwo kolizji, ograniczającej przepustowość i tworzących wymagania dotyczące częstych retransmisji danych. Więcej kolizji to nie jedyny problem związany z używaniem koncentratorów. Inne wady takich urządzeń to ograniczona skalowalność i zwiększone opóźnienia w przesyłaniu danych, między innymi przez wspomniane wcześniej wstrząsy.

Przez lata kontynuowano wysiłki mające na celu wyeliminowanie słabości Ethernetu opartego na koncentratorach, dopóki nie wynaleziono inteligentnego urządzenia sieciowego zwanego przełącznikiem, które rozwiązało problemy, które nękały wcześniejsze wersje Ethernetu.

Przełączniki w sieciach komputerowych działają do dziś i nic nie wskazuje na to, by miało się to zmienić w najbliższym czasie. Dlaczego te urządzenia są tak popularne i dlaczego są tak inteligentne? Cóż, w przeciwieństwie do koncentratora, przełącznik nie wysyła danych do wszystkich podłączonych do niego urządzeń, ale tylko do konkretnego urządzenia, dla którego dane są przeznaczone, oczywiście z pominięciem transmisji rozgłoszeniowych, takich jak omawiana wcześniej transmisja ARP. Pomiędzy portem przełącznika, do którego jest podłączone urządzenie, a samym urządzeniem istnieje logiczna topologia typu punkt-punkt. Dane wysyłane do konkretnego urządzenia są przesyłane do niego i tylko do niego.

Zastosowanie przełącznika prawie całkowicie eliminuje ryzyko kolizji, ponieważ urządzenia nie muszą rywalizować ze sobą o dostęp do medium. Jednocześnie rozmiar domeny kolizyjnej jest ograniczony, ponieważ taka domena składa się wyłącznie z portów przełącznika i podłączonych do niej urządzeń. Zalet przełączników jest znacznie więcej. Każde urządzenie podłączone do portu przełącznika ma dostępną dedykowaną przepustowość. Na przykład, jeśli przełącznik oferuje prędkość transferu 100 Mb/s, ta przepustowość będzie dostępna dla każdego podłączonego do niego urządzenia.

W przypadku koncentratora ta przepustowość jest dzielona między wszystkie urządzenia. Dzięki zastosowaniu przełącznika dane mogą być przesyłane również w trybie full-duplex,
co oznacza, że podłączone do niego urządzenia mogą jednocześnie odbierać i wysyłać dane.

Obecnie w użyciu jest kilka wersji standardu Ethernet. Najpopularniejszym z nich jest standard oferujący nominalne przepustowości do 100 Mb/s, znany jako standard FastEthernet. Transmisja w tym standardzie odbywa się tylko po 2 parach miedzi, a nie 4 skrętkach. Jest to powszechne rozwiązanie stosowane w wielu sieciach komputerowych.
W większości przypadków spełnia wymagania sieci komputerowych.

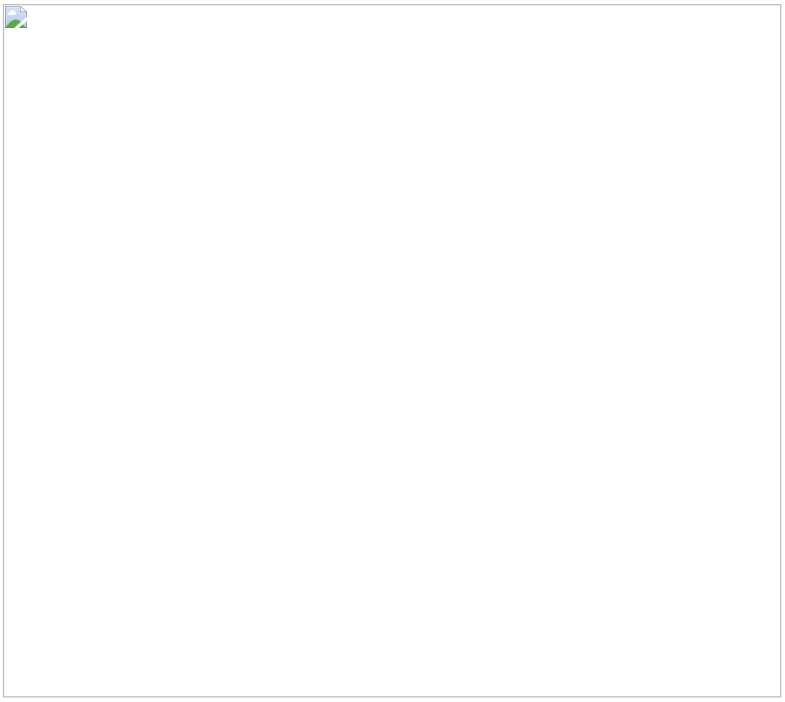
Standard Gigabit Ethernet może być stosowany, gdy zapotrzebowanie na przepustowość sieci wzrasta wraz z ilością przesyłanych danych. Nominalnie zapewnia przepustowość
1 Gb/s. Jeśli używany jest standard 1000BASE-T, do transmisji wykorzystywane są wszystkie skrętki miedziane. Z tej wersji Ethernetu korzystają duże sieci lokalne, które korzystają
z telefonii internetowej VoIP i przesyłają duże ilości różnego rodzaju multimediów.

Wykorzystując standard Ethernet, dane mogą być również przesyłane łączami światłowodowymi, w tym przypadku standard Gigabit Ethernet nazywa się 1000BASE-SX lub LX. Istnieją również standardy Ethernet, które zapewniają komunikację z przepustowością 10, a nawet 100 Gb/s. Stosowane są głównie w sieciach miejskich i rozległych, ponieważ są bardzo, bardzo drogie w realizacji i niewiele osób może sobie pozwolić na korzystanie z tego typu rozwiązań w sieci lokalnej. Poniższa tabela przedstawia najpopularniejsze wersje standardów Ethernet oraz wykorzystywane przez nie medium transmisyjne:

Standard Ethernet	Maksymalna przepustowość	Stosowane medium transmisyjne	Maksymalna odległość
100BASE-TX (fastEthernet)	100 Mb/s	UTP (kat. 5/5e)	100 metrów
100BASE-FX (fastEthernet)	100 Mb/s	Światłowód (jedno/wielomodowy)	400/2000 metrów

100BASE-T (gigabitEthernet)	1 Gb/s	UTP (kat. 5e)	100 metrów
100BASE-TX (gigabitEthernet)	1 Gb/s	UTP (kat. 6)	100 metrów
100BASE-SX (gigabitEthernet)	1 Gb/s	Światłowód wielodomowy	550 metrów
100BASE-LX (gigabitEthernet)	1 Gb/s	Światłowód jednomodowy	2000 metrów
10GBASE-T (10gigabitEthernet)	10 Gb/s	UTP (kat. 6/7)	100 metrów
10GBASE-LX4 (10gigabitEthernet)	10 Gb/s	Światłowód jednomodyw/wielomodowy	300/10000 metrów

Opisane powyżej przełączniki wykorzystują adresy MAC do przesyłania danych między urządzeniami podłączonymi do portów przełącznika. Każdy przełącznik ma coś, co nazywa się tabelą adresów MAC. To nic innego jak zbiór informacji, które określają, które urządzenie,
a właściwie jaki adres MAC urządzenia jest podłączone do konkretnego portu. Zrzut ekranu przykładowej tabeli adresów MAC dla przełącznika CISCO pokazano poniżej:



Wpisy w takiej tabeli są dodawane dynamicznie, a nie przez administratora. Przełącznik pobiera informacje przechowywane na tablicy podczas procesu uczenia. Z odebranej ramki przełącznik odczytuje źródłowy adres MAC i dodaje go do swojej tabeli, przypisując numer portu, na którym odebrał ramkę. Z kolei jeśli nie wie, do kogo wysłać taką ramkę, ponieważ w tabeli nie ma wpisu adresu MAC odbiorcy, następuje proces zwany floodingiem.

Można to porównać do rozgłaszania, ponieważ ramka jest wysyłana do wszystkich urządzeń oprócz nadawcy. Urządzenie, do którego ramka nie została zaadresowana, odrzuca ją, podczas gdy urządzenie odbierające odpowiada i wysyła ramkę do przełącznika. Przełącznik odczyta adres MAC nadawcy z ramki i zapisze go w swojej tabeli. Cały proces uczenia się
i zalewania jest przedstawiony w samouczku wideo.

Ramka Ethernet

Ponieważ standard Ethernet działa na drugiej warstwie modelu OSI, można się domyślić,
że również tworzy swoje ramki. Oczywiście tak, Ethernet hermetyzuje własną ramkę, zwaną ramką Ethernet. Poniżej możesz zobaczyć przykładową ramkę:

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)

· Preambuła i Znacznik początku ramki — te pola służą do poinformowania urządzenia docelowego, że jest ono gotowe do odbierania ramek;

· Docelowy adres MAC, czyli fizyczny adres odbiorcy ramki;

· Źródłowy adres MAC, czyli fizyczny adres hosta wysyłającego;

· Długość/Typ — pole długość określa rozmiar ramki, natomiast typ określa protokół używany przez wyższe warstwy, z których najpopularniejszym jest IPv4;

· Dane — jest to pakiet odebrany z warstwy sieciowej. Minimalny rozmiar tego pola musi wynosić 46 bajtów, a maksymalny 1500 bajtów. Jeśli pakiet jest mniejszy niż 46 bajtów, jest uzupełniany losowymi danymi w celu zwiększenia rozmiaru całej ramki do wymaganego minimum, czyli maksymalnie 64 bajtów.

· Kod kontrolny ramki — pole zawierające sumę kontrolną ramki, używane do wykrywania możliwych błędów ramek. Urządzenie wysyłające dane wylicza sumę kontrolną i umieszcza ją w ramce, odbiorca danych również taką sumę wylicza po jej odebraniu, jeśli obie sumy są poprawne, ramka jest akceptowana, jeśli są różne, ramka jest uznawana za uszkodzoną i odrzuconą .

Całkowity rozmiar ramki może wynosić do 1518 bajtów (przy obliczaniu rozmiaru ramki nie uwzględnia się preambuły i początku sygnału ramki). Istnieje również ramka Ethernet
o maksymalnej długości 1522 bajtów. Takie ramki są używane w wirtualnych sieciach LAN,
w tzw. sieciach VLAN.

13. Podstawowe zagadnienia z komunikacji VoIP

Najważniejsze definicje

- VoIP - https://pl.wikipedia.org/wiki/Voice_over_Internet_Protocol
- PBX - https://pl.wikipedia.org/wiki/PBX
- Kodek - https://pl.wikipedia.org/wiki/Kodek
- SIP - https://pl.wikipedia.org/wiki/Session_Initiation_Protocol

Co to jest VoIP?

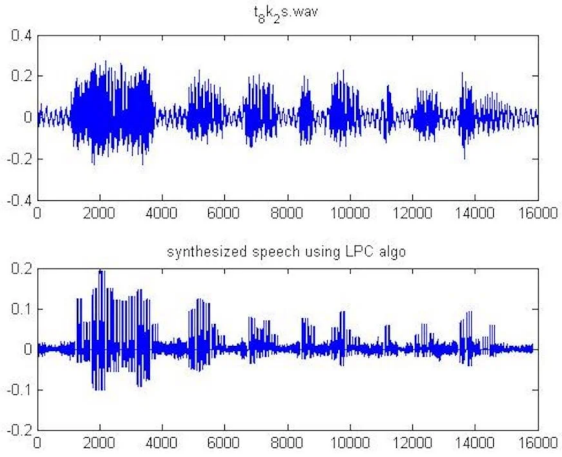
VoIP jest skrótem od słów Voice over Internet Protocol. Jest to technologia pozwalająca nadawać i odbierać dźwięk przez sieć komputerową, technologia ta służy do prowadzenia rozmów „telefonicznych" w czasie rzeczywistym.

Mimo, że technologia VoIP stała się bardzo popularna w ciągu ostatniej dekady to historia VoIP zaczyna się blisko 100 lat temu w instytucie badawczym Bell Labs.

W roku 1938 Homer Dudley, inżynier Bell Labs, stworzył pierwszy elektroniczny syntezator mowy, znany jako Vocoder. Koncepcja działania była podobna do dzisiejszej transmisji pakietowej (IP), która rejestruje próbki głosu na jednym telefonie i odtwarza je na innym. Obecnie ta sama technologia jest wykorzystywana nie tylko w telefonii VoIP, ale także w implantach ślimakowych.

Nie można prowadzić rozmów przez Internet bez sieci komputerowej. Historia sieci komputerowej zaczyna się w 1969 roku w Advanced Research Project Agency – rządowej agencji USA. W wyniku prac agencji powstał protokół sieciowy TCP/IP oraz uruchomiono pierwszą sieć komputerową – ARPANET. Sieć ta działała formalnie do 1990 roku.

W roku 1973 w MIT Bob McAuley, Ed Hofstetter i Charlie Radar opracowali pierwszy pakiet głosowy przekazywany przez ARPANET.

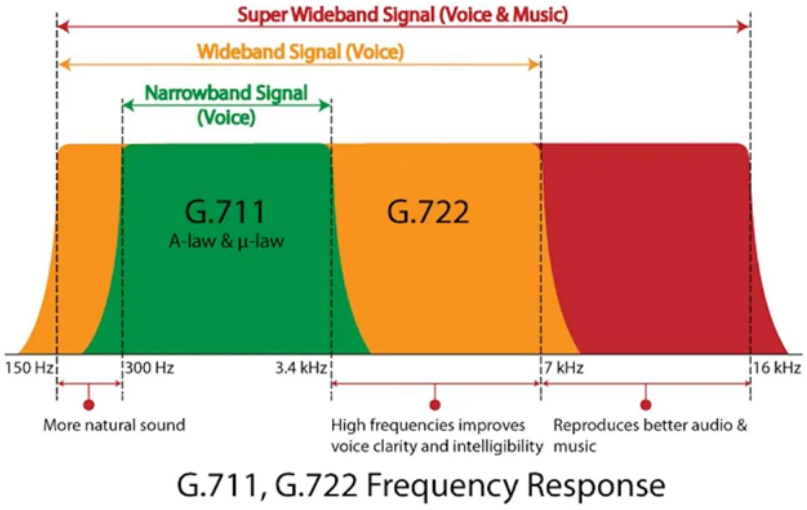


(Źródło: https://www.mathworks.com/matlabcentral/fileexchange/13529-speech-compression-using-linear-predictive-coding)

Ta transmisja głosu była możliwa dzięki LPC, czyli Linear Predictive Coding - fundamentowi nowoczesnej technologii VoIP. LPC to technika analizy mowy, która opiera się na liniowym modelu predykcyjnym do przetwarzania i ponownej syntezy skompresowanych cyfrowych form sygnałów głosowych i mowy.

W tym czasie nie można było używać sieci ARPANET do celów prywatnych. Pierwszy "techniczny" cyberprzestępca to Leonard Kleinrock, który w 1973 r. wysłał wiadomość przez ARPANET dotyczącą jego zaginionej elektrycznej maszynki do golenia.

W 1974 r. Lincoln Lab i Culler Harrison Inc. pomyślnie przesłały między sobą testowe pakiety danych głosowych. W 1976 roku Culler Harrison i Lincoln Labs przeprowadzili telekonferencję przez LPC. W 1982 r. osiągnęli znaczący postęp, wykorzystując LPC do łączenia się przez lokalną sieć kablową, mobilną sieć pakietową i interfejs z PSTN (Public Switched Telephone Network).



Rysunek 2: Pierwszy szerokopasmowy kodek audio

(Źródło rysunku: https://www.gl.com/newsletter/g722-wideband-audio-codec-support-across-tdm-voip-platforms-newsletter.html)

W 1988 roku ITU-T zatwierdził szerokopasmowy kodek audio G.722, czyli program, który umożliwia zamianę dźwięku na język „cyfrowy" oraz, po przesłaniu przez sieć, zamianę z powrotem na sygnał dźwiękowy. Kodek G.722 oferował znacznie lepszą jakość mowy w porównaniu do swoich poprzedników. G.722 oferuje szybkość transmisji danych do 64 kb/s, czyni go idealnym do komunikacji VoIP — zwłaszcza w sieciach lokalnych (LAN).

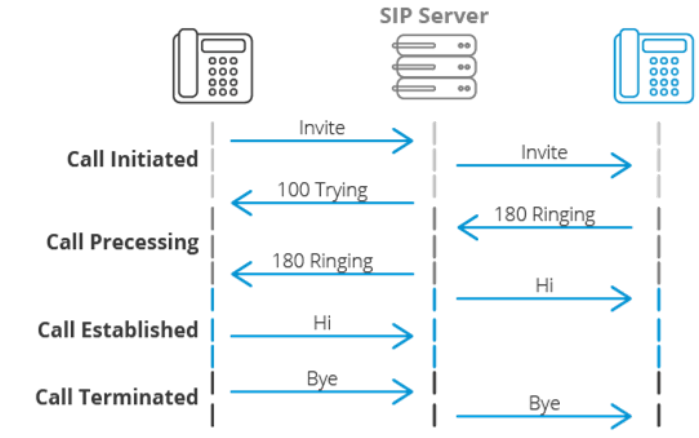
W 1989 roku deweloper Brian C. Wiles stworzył RASCAL, pierwszy system, który z powodzeniem przesyłał głos przez sieci Ethernet — pierwsza aplikacja VoIP.

W 1991 roku John Walker z firmy Autodesk napisał i udostępnił program NetFone, później znany jako Speak Freely, to pierwszy telefon VoIP oparty na oprogramowaniu.

Rok 1993 przyniósł pierwszy system wideo konferencyjny – Teleport. Twórcami Teleport byli David Allen i Herold Williams, którzy sprzedali swój produkt hotelom Hilton.

Pierwszą komercyjną aplikacją VoIP stał się w roku 1995 program VocalTec Internet Phone. Program wykorzystywał protokół H.323, wymagania to: procesor 486, 8 MB pamięci RAM, 16-bitowej karty dźwiękowej i połączenia internetowego SLLP lub PPP. VocalTec był tańszy od tradycyjnych połączeń telefonicznych w połączeniach międzynarodowych i międzymiastowych.

W 1996 roku opracowano SIP (Session Initiation Protocol). Pierwsza wersja SIP miał tylko jedno polecenie – „nawiąż połączenie", ale już w 1999 r. rozwinięto możliwości SIP do 6 poleceń.

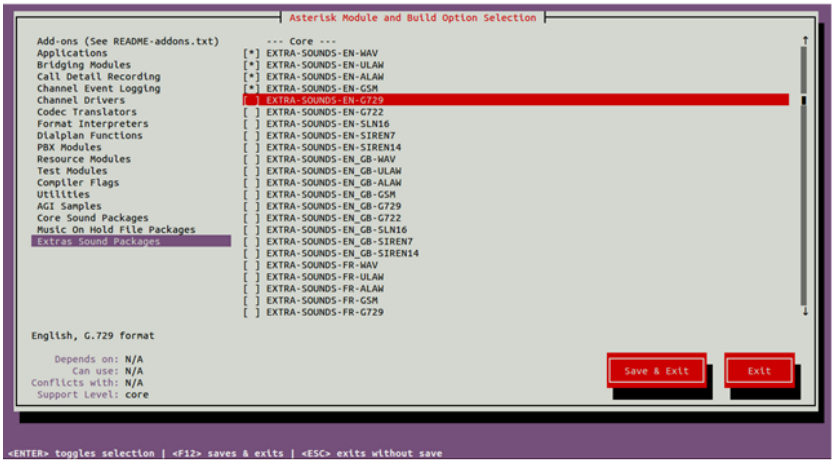


Rysunek 3: Protokół SIP

(Źródło rysunku: https://www.3cx.pl/voip-sip/sip/)

SIP stał się preferowanym protokołem mobilnej telefonii VoIP.

W 1999 roku Mark Spencer postanowił zaprogramować własny system IP-PBX, czyli program pełniący funkcję centrali telefonicznej, i nazwać go Asterisk. Asterisk jest programem open source, który szybko zyskał popularność i jest rozwijany i ulepszany do dziś przez tysiące programistów.



Rysunek 4: Instalacja asterix w systemie Linux

(źródło rysunku: https://www.howtoforge.com/how-to-install-asterisk-17-on-ubuntu-2004/)

W 2003 roku powstał Skype i wkrótce stał się najczęściej używanym komunikatorem głosowym. Z biegiem czasu Skype rozwinął się do poziomu komunikatora wideo z możliwościami przesyłanie plików. Dziś jest w posiadaniu firmy Microsoft.

W 2006 roku Truphone, pierwsza mobilna aplikacja VoIP, została uruchomiona dla użytkowników telefonów Nokia, iPhone'ów, Androidów i Blackberry. Aplikacja wykorzystuje SIP do wykonywania połączeń przez połączenie internetowe, a nie przez sieci komórkowe.

W latach 2011-2015 w USA nastąpił wielki wzrost popularność telefonii VoIP. Na świecie nastąpił wzrost liczby dostawców VoIP, który sprzyjał konkurencyjności i prowadzi lub już doprowadził do wyparcia starszych systemów telefonicznych.

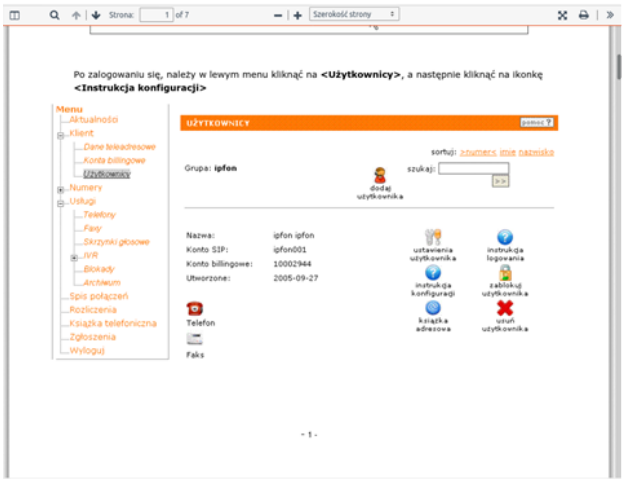
Pandemia COVID z roku 2020 w wielu sektorach gospodarki z dnia na dzień zmieniła charakter pracy na zdalną. Ujednolicona komunikacja oparta na technologii VoIP pozwala pracować zespołowo zdalnie i kontaktować się z klientami za pomocą wielu kanałów, w tym: rozmów wideo, aplikacji mobilnych, połączeń konferencyjnych, zespołowych wiadomości tekstowych, poczty głosowej.

Do najpopularniejszych programów wykorzystujących technologię VoIP należą: Microsoft Teams (domyślny komunikator systemu operacyjnego MS Windiows11), Google Meet, Zoom.

VoIP w domu, VoIP dla biznesu

Rozwiązania VoIP dla użytkowników domowych

Użytkownicy domowi to tacy, którzy potrzebują z reguły jednego numeru telefonu.
W celu uruchomienia publicznego numeru telefonu PSTN z prefixem państwa i obszaru (miasta) należy zarejestrować się u dostawcy usług VoIP. Dostawca telefonii VoIP w procesie rejestracji utworzy konto SIP – login i hasło, oraz poda sposób konfiguracji SIP. Posiadając informacje o koncie możemy logować się do centrali i używać telefonii VoIP w aplikacjach dla telefonów komórkowych, aplikacjach instalowanych w systemach operacyjnych Microsoft, Apple, Linux, czy wreszcie telefonach VoIP.



Rysunek 5: Przykład uzyskania danych logowania do konta SIP

(źródło rysunku: https://docplayer.pl/64633184-Uzyskanie-nazwy-i-hasla-konta-sip.html)

Rozwiązania VoIP dla firm

Aby zarządzać wieloma telefonami VoIP w firmie należny uruchomić centralę abonencką (PBX). Centrala może występować zarówno jako fizyczne urządzenie zainstalowane w siedzicie przedsiębiorstwa jak i w postaci wirtualnej (oprogramowania dostarczonego przez firmę sprzedająca usługi telefoniczne).

Stacjonarne aparaty telefoniczne pracowników firmy w przypadku wirtualnej centrali muszą obsługiwać VoIP. Koszt telefonu VoIP jest porównywalny do tradycyjnego tak więc przy nowych siedzibach firm telefon VoIP wydaję się najlepszym wyborem.

Przedsiębiorstwa posiadające tradycyjne linie PSTN oraz aparaty mogą pozostać przy przydzielonych numerach telefonów na dwa sposoby:

- zakup centrali VoIP z modułami PSTN/ISDN bez wymiany telefonów,
- przeniesienie numerów do wirtualnej PBX i wymiana aparatów telefonicznych na obsługujące VoIP

Przegląd aplikacji VoIP

Aplikacje związane z VoIP możemy podzielić na:

- klienckie – instalowane na aparatach telefonicznych/komputerach końcowego użytkownika VoIP
- serwerowe – instalowane na zwykłych serwerach, czy dedykowanych centralach

Aplikacje klienckie

Współczesna technologia telefonii komórkowej opiera się na technologii cyfrowej, a więc dźwięk przekazywany jest za pośrednictwem kodeka.

W obecnie używanych smartfonach dodanie numeru VoIP jest możliwe bez instalowania dodatkowego oprogramowania. W ustawieniach systemu Android czy iOS możemy wprowadzić dane konta SIP i używać telefonii VoIP. Istnieje też wiele aplikacji VoIP, które dają dodatkowe funkcjonalności (np. wspólna książka adresowa, itp.). Wybierając w jaki sposób chcemy korzystać z telefonii VoIP najlepiej kierować się zaleceniami dostawcy usługi VoIP. Dostawcy usługi często posiadają własną aplikację dedykowaną do używania usług VoIP.

Na komputerach stacjonarnych, laptopach czy tabletach bez możliwości podłączenia się do sieci komórkowej możemy używać VoIP za pośrednictwem sieci Internet. Tak więc wystarczy podłączyć laptop do WiFi oraz zainstalować aplikację VoIP aby móc wykonywać połączenia telefoniczne.

Istnieje wiele popularnych aplikacji, które umożliwiają połączenia telefonii VoIP z publiczną komutowaną siecią telefoniczną (PSTN) : Microsoft Teams, ZOIPER, Blink, Zoom itp. Listę aplikacji klienckich VoIP możemy śledzić na stronie: https://en.wikipedia.org/wiki/List_of_SIP_software

Aplikacje serwerowe

Serwer SIP zarządza połączeniami w sieci, odbiera żądania od klientów VoIP w celu nawiązania i kończenia połączeń.

Najpopularniejszy serwer SIP Open Source to Asterix (https://www.asterisk.org). Aby uruchomić Asterix w firmie należy posiadać serwer z zainstalowanym systemem operacyjnym Linux. W dystrybucjach Linuxa istnieją dedukowane pakiety oprogramowania zawierające serwer Asterix. Najlepszym sposobem instalacji serwera Asterix jest pobranie specjalnie przygotowanej dystrybucji Linuxa – freePBX (https://www.freepbx.org/downloads/). Asterix posada wiele możliwości nowoczesnej telefonii w tym, m. in.: SMS, muzykę przy oczekiwaniu / łączeniu, pocztę głosową.

14. Wydajność sieci. Zapoznanie z metodami ograniczania ruchu sieciowego.

Czynniki wpływające na wydajność sieci komputerowej

Na wydajność sieci komputerowej mają wpływ:

1. **Części pasywne sieci** komputerowej, czyli części sieci komputerowej, które służą jedynie przekazywaniu danych między aktywnymi urządzeniami sieci. Do części pasywnych sieci komputerowej zaliczmy: przewody miedziane, przewody światłowodowe, gniazda sieciowe, oraz pathpanele.
2. **Urządzenia aktywne**, to części sieci komputerowej, które nadają/odbierają informację lub służą do przekazania/wzmacniania danych w sieci komputerowej. Do urządzeń aktywnych zaliczamy: karty sieciowe, przełączniki, wzmacniacze/repetery sieci.
3. **Zakłócenia elektromagnetyczne**, które to wpływają na transmisję bezprzewodową oraz kablami miedzianymi (typu skrętka).

14.1. Jakość kabla typu skrętka

Kable typu skrętka przenoszą informację w postaci impulsów elektrycznych. Skrętka zwiera 8 żył (drutów) miedzianych powlekanych izolacją. Żyły skręcone są w pary w celu zapewnienia lepszej transmisji danych. Na prędkość i jakość przesyłania danych w postaci impulsów elektrycznych największy wpływ mają zakłócenia elektromagnetyczne.

Na jakość wykonania kabli typy skrętka mają wpływ:

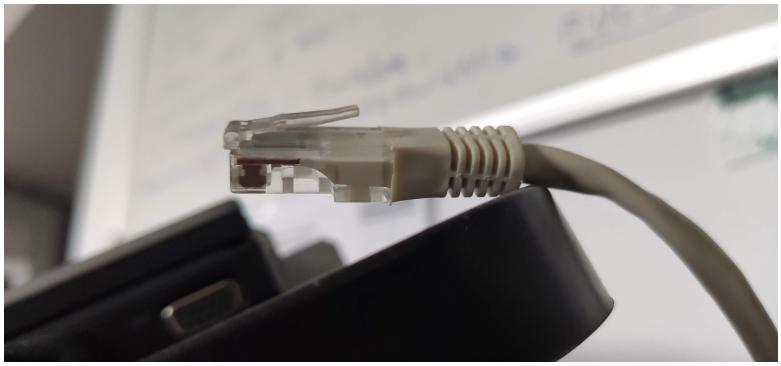
- jakość wykonania żyły miedzianej, tj. czystość metalu, zachowane rozmiary profilu
- jakość i ilość izolacji

W zależności od ilości izolacji oraz użytych sposobów ekranowania (zabezpieczenia przed zakłóceniami) kable typu skrętka określamy kategorią od 1 do 8 oraz typem ekranu: U – nieekranowane, F – ekranowane folią, S – ekranowane siatką, SF – ekranowane folią i siatką. Wyższa kategoria kabla zapewnia szybsza transmisję danych, dla przykładu: kategoria 5 UTP, ScTP, STP zapewnia przesył do 1 Gb/s; kategoria 6 UTP, ScTP, STP - 10 Gb/s.

Kable sieciowe zakończone są końcówkami RJ45. Jakość użytego materiału oraz ekranowanie RJ45 ma oczywiście wpływ na transmisję danych.

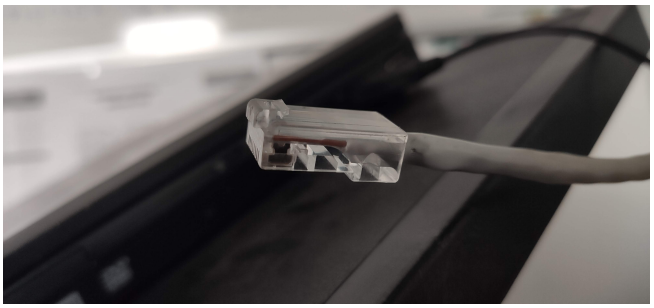
Przykłady uszkodzeń kabli typu skrętka

Na filmie nr 1 widzimy kabel kategorii 6 wykonany w fabryce przy użyciu specjalistycznej linii produkcyjnej. Kabel wkładany w gniazdo zachowuje swoje własności a końcówka RJ45 działa prawidłowo po wielokrotnym podłączaniu komputera. Zabezpieczenie przed niepożądanym wypadaniem kabla działa prawidłowo - słychać charakterystyczne kliknięcie. Nie można też wyciągnąć kabla bez zwolnienia zabezpieczenia. Taki stan kabla gwarantuje prawidłową transmisję danych.



Zadęcie przedstawia dobrej jakości kabel sieciowy z prawidłową wtyczką RJ45.

Film nr 2 prezentuje kabe wykonany samodzielnie przy użyciu słabej wtyczki RJ45. Niska jakość plastiku prowadzi do złamania zabezpieczenia. To uszkodzenie powoduje, że kabel może wypaść z gniazda - transmisja danych zostanie przerwana



Zdjęcie uszkodzonej wtyczki RJ45

Film 3 - dobrej jakości kabel sieciowy

0:00

Film 4 - kabel typu skrętka ze słabej jakości izolacją. Cienka izolacja nie chroni dostatecznie skrętki przed uszkodzeniem mechanicznym.

Film 5 i 6 – Kabel kategorii 5e. Izolacja zewnętrzna wypadła z wtyczki RJ45. Odpowiednie pary żył drutów muszę być skręcone aby niwelować zakłócenia transferu sygnału. W tym przypadku nie jest zapewnione prawidłowe skręcenie par.

14.2. Światłowody

Wstęp

Światłowody przenoszą informację w postaci impulsów świetlnych. Dzięki zjawisku całkowitego wewnętrznego odbicia światło biegnące wewnątrz światłowodu zostaje tam uwięzione. Można więc przesyłać bezstratnie informację na znacznie większą odległość niż w przypadku kabli miedzianych.

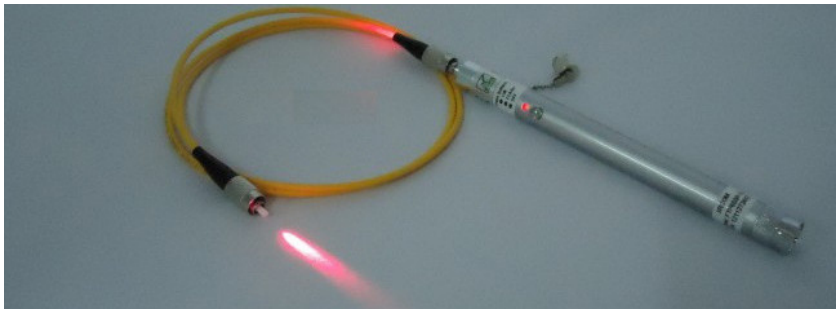
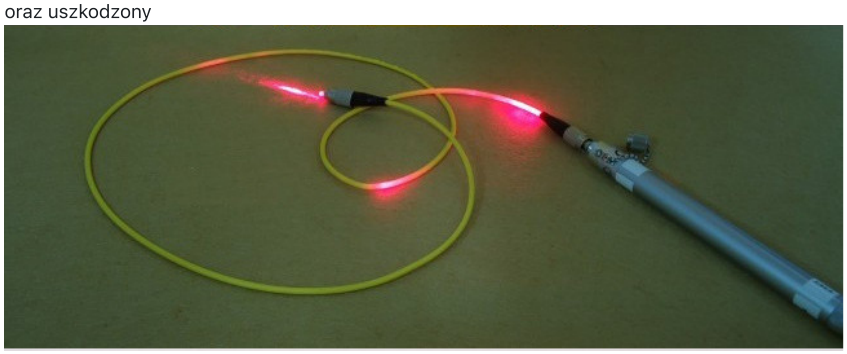
Światło, które porusza się wewnątrz światłowodu, ulega tłumieniu. Ponieważ nie wynaleziono metody wytworzenie idealnie odbijającego światłowodu pojawia się zjawisko utraty mocy optycznej. Obecnie kable światłowodowe potrafią przenosić bezstratnie informację na maksymalną odległość około 100 km. Dzięki zastosowaniu co pewien odcinek wzmacniaczy optycznych siecią światłowodową możemy łączyć bardzo odległe lokalizacje.

Na jakość sieci światłowodowych ma wpływ przede wszystkim jakość robót wykonywanych podczas jego układania. Należy zwrócić uwagę na:

- maksymalny promień gięcia przewodu – w zależności od standardu promień gięcia wynosi: 30, 10 7,5 mm,
- jakość urządzeń tnących – po cięciu krawędź światłowodu nie może być postrzępiona,
- jakość spawarki

Przykłady uszkodzeń

Jednym ze sposobów testowania światłowodu jest użycie lokalizatora uszkodzeń wizualnych:

- Światłowód prawidłowy

- oraz uszkodzony


Powyższa uszkodzenie nastąpiło najprawdopodobniej przez przekroczenie promienia gięcia światłowodu.

14.3. Przełączniki sieciowe, karty sieciowe

Przełącznik sieciowy (switch) to urządzenie odpowiedzialne za przekazywanie danych miedzy hostami w sieciach komputerowych. Host to dowolne urządzenie podłączone do sieci komputerowej - laptop, drukarka, telewizor itd.

Na wydajność sieci największy wpływ ma switch. Przepustowość portów wyrażona w bitach na sekundę (100Mbit/s, 10 Gbit/s), czyli ile danych maksymalnie możemy przesłać do switcha w jednostce czasu, to najważniejszy czynnik określający wydajność sieci komputerowej.

Switch obsługuje wiele połączeń między hostami jednocześnie dlatego należy zwrócić uwagę na parametry takie jak ilość pamięci, szybkość procesora oraz przepustowość. (System Switching Capacity, System Throughput Capacity).

Karty sieciowe są to urządzenia pozwalające podłączyć host do sieci komputerowej. Podstawowym parametrem karty sieciowej jest prędkość wysyłania i odbierania danych wyrażona w bitach na sekundę (100Mbit/s, 1Gbit/s, itp.). Łącząc hosta ze switchem należy pamiętać, o tym że wydajność sieci będzie taka jak urządzanie z najmniejszą przepustowością - przykład switch 100 Mb/s + karta sieciowa 1000 Mb/s daje przepustowość maksymalną 100 Mb/s

14.4. Testy wydajności sieci

Zakłócenia działania sieci

Utrata danych w wyniku zakłóceń elektromagnetycznych może wystąpić zarówno w sieciach bezprzewodowych jak i w sieciach wykorzystujących kable miedziane. Sieci elektryczne, urządzania zasilane dużymi prądami wytwarzają promieniowanie elektromagnetyczne.

Kiedy jakaś część sieć WiFi znajduje się w pobliżu urządzeń takich, jak np. w pociąg trakcji elektrycznej czy tramwaj można spodziewać się zakłóceń w przekazie danych.

Podobnie promieniowanie elektromagnetyczne wpływa na kable sieciowe wykonane z miedzi. Sieci, w których kable UTP położone są zbyt blisko przewodów elektrycznych mogą być narażone na zakłócenia elektromagnetyczne.

Jeżeli spodziewamy się w danej lokalizacji występowania zakłóceń elektromagnetycznych użyjmy jako nośnika danych światłowodów, są one odporne na promieniowanie elektromagnetyczne.

Testy wydajności sieci komputerowej

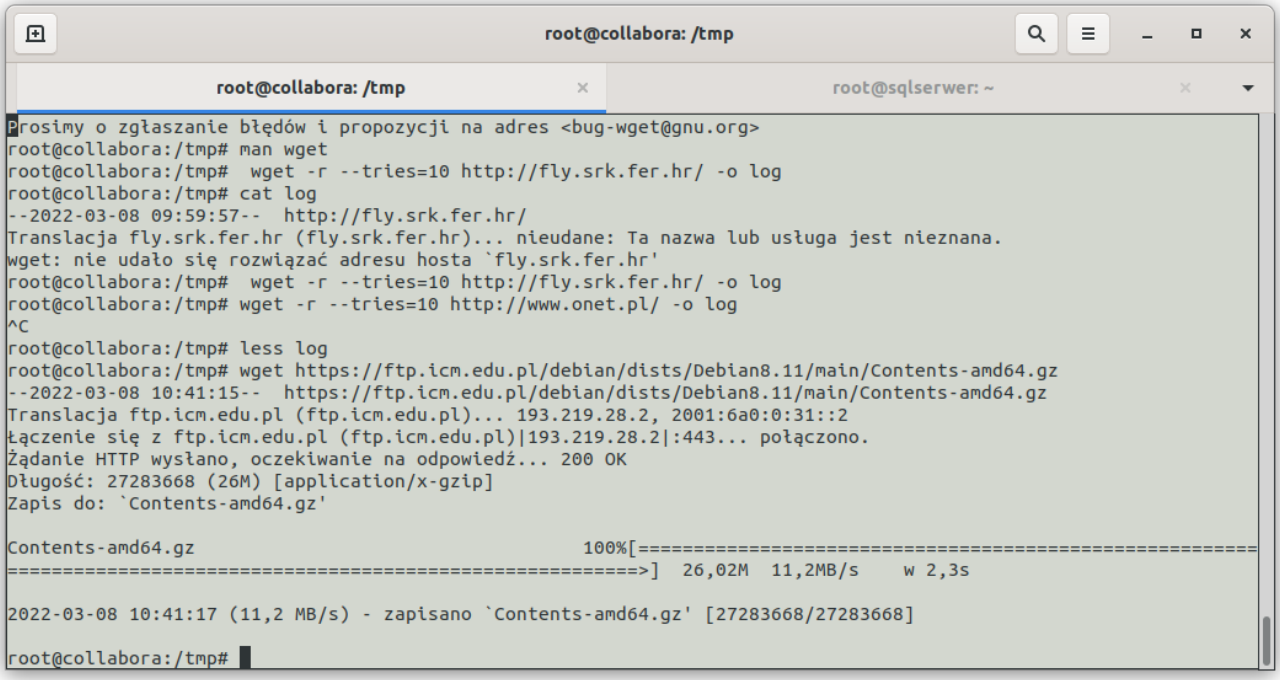
Wydajności sieci komputerowej sprowadza się do określenia przepustowości, czyli ilości informacji jakie w określonym czasie możemy przesłać przez badaną sieć. Najprostszym sposobem określenia wydajności sieci jest więc pobranie/wysłanie pewnej ilości danych i zmierzenie czasu jaki zajmie nam ta czynność.

Wyniki testu wydajności sieci mogą być zniekształcone przez inne czynniki nie będące bezpośrednio elementami sieci komputerowej. Wysyłając lub pobierając dane należy pamiętać o tym, że muszą one być odczytane i zapisane na dysku. Jeżeli dysk twardy komputera ma maksymalną prędkość zapisu/odczytu niższą niż szybkość sieci wynik testu przepustowości nie będzie pokazywał wydajności sieci a jedynie wynik zapisu/odczytu danych na dysku twardym. W takim przypadku możemy powiedzieć że tzw. "wąskim gardłem" naszego systemu komputerowego jest dysk twardy. Kolejnym, często występującym, czynnikiem przekłamującym wydajność sieci są ograniczania prędkości pobierania plików stosowane na serwerach udostępniających pliki. Ponieważ dostawcy usług pobierania plików muszą zapewnić dostęp do pobierania plików jak największej ilości klientów nie mogą przy pobieraniu dopuścić do osiągania maksymalnej prędkość pobierania przez tylko jednego klienta. Na serwerach plików dzieli się maksymalną prędkość wysyłania danych od serwera do klienta przez spodziewana liczbę klientów w nadym okresie czasu dlatego pobierając plik przez Internet o przepustowości np 300 Mb/s maksymalny transfer to np. 10Mb/s.

Do testowania przepustowości sieci możemy posłużyć się dowolnym programem, który pobiera/wysyła dane. Aby uzyskać wiarygodne wyniki należy jednak powtórzyć je wiele razy w różnych dniach i godzinach. Test wydajności możemy przeprowadzić za pomocą programów takich jak: wget, ping lub też za pomocą dedykowanych do tego celu stron www: speeedtest.net, www.nperf.com.

wget

Program **wget** to program konsolowy używany najczęściej w środowisku Linux. W systemie operacyjnym MS Windows od wersji 10 istnieje łatwa możliwości "instalacji" systemu Linux za pomocą technologi WSL (Windows Subsystem for Linux). Aby przeprowadzać test przepustowości sieci za pomocą programu wget - w tym celu w konsoli (terminal tekstowy) wydajemy polecenie: **wget https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz** , polecenie to uruchamia pobieranie pliki z adresu internetowego: https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz. Jak widzimy na poniższym obrazie otrzymujemy informacje: pobrano 26 MB z prędkością 11,2 MB/s w 2,3 sekundy.



(Rysunek 1. Test prędkości sieci za pomocą programu wget)

Za pomocą programu wget możemy wykonać wiele prób jednocześnie, przykład:

wget -r --tries=10 http://www.onet.pl/ -o log

Wykonujemy tu pobieranie **rekursywne** (-r) zawartości strony www.onet.pl , próby pobierania powtórzymy **10** razy, wyniki zapiszmy w pliku **log.** Wyniki zapisane w pliku log przedstawiają czas oraz prędkość transferu dany ze strony www.

ping

Kolejnym programem konsolowym dostępnym w róznych systemach operacyjnych jest program ping.

Przykład testu wydajności sieci za pomocą programu ping:

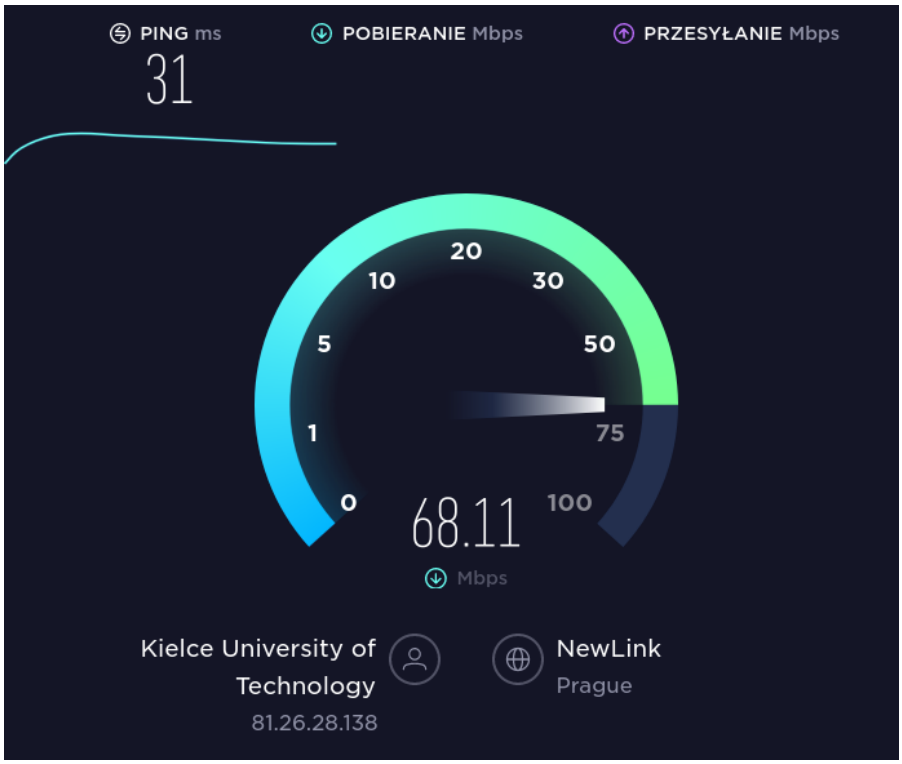
```
ping wp.pl
PING wp.pl (212.77.98.9) 56(84) bytes of data.
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=1 ttl=55 time=16.0 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=2 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=3 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=4 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=5 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=6 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=7 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=8 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=9 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=10 ttl=55 time=15.3 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=11 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=12 ttl=55 time=15.2 ms
64 bytes from www.wp.pl (212.77.98.9): icmp_seq=13 ttl=55 time=15.2 ms

--- wp.pl ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12015ms
rtt min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms
```

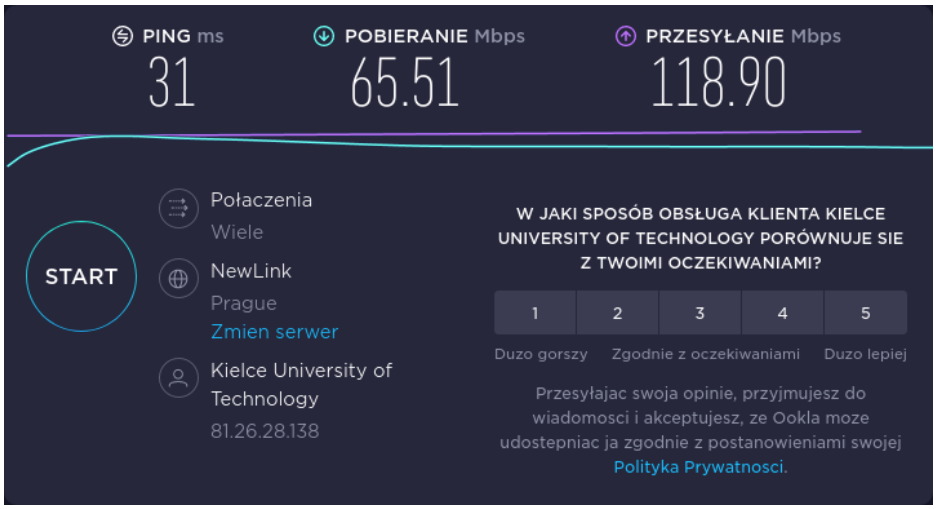
W powyższym przykładzie wysłano wo serwera o adresie www.wp.pl 13 razy pakiet *ICMP Echo Request* i odebrano tyle samo odpowiedzi (*ICMP Echo Reply)*. Ostatnia linia przykłądu (min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms) zawiera wynik testu prędkości przesyłania pakietu prze sieć - im mniejsze czasy odpowiedzi tym nasza sieć jest wydajniejsza.

speedtest.net

Do testowania predkości wysyałania/pobierania służą też aplikacje internetowe. Pod adresem https://www.speedtest.net możemy wykonać test pokazyjacy zarówno wartość PING jak i również prędkośc pobierania i wysyałania. Poniższe rysunki przedstawiają zrzuty ekranu testu wysyłania danych przez Internet pomiedzi sięcią w Kielcach (Polska) a siecią w Pradze (Czechy).



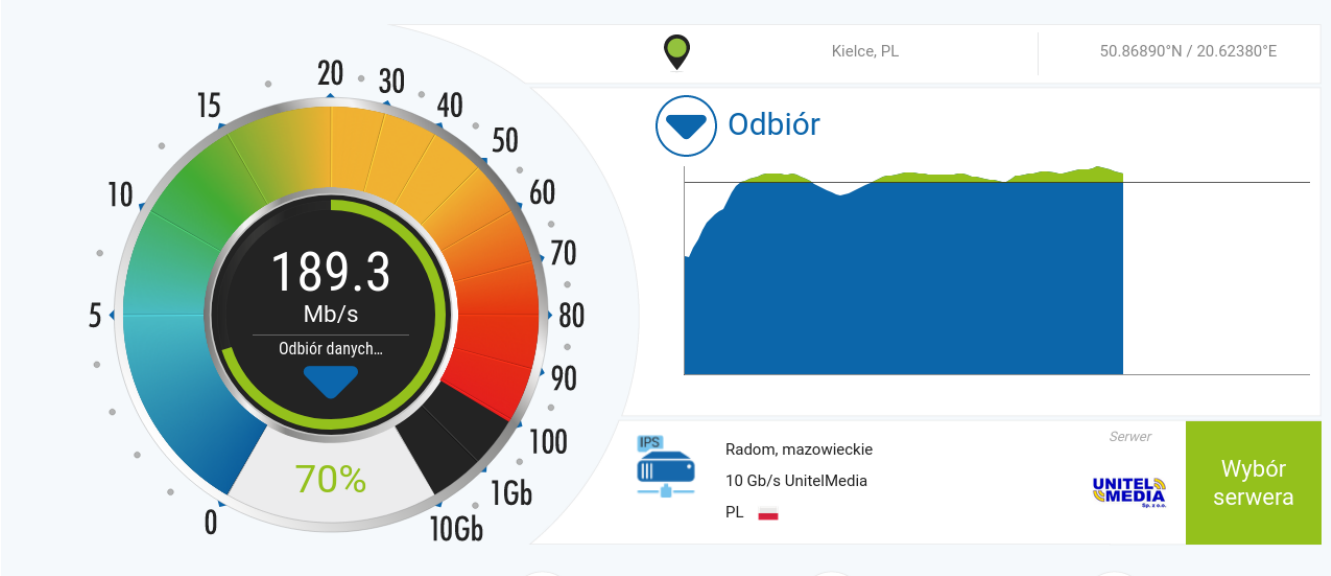
(Rysunek 2. Test prędkości sieci za pomocą programu speedtest.net)



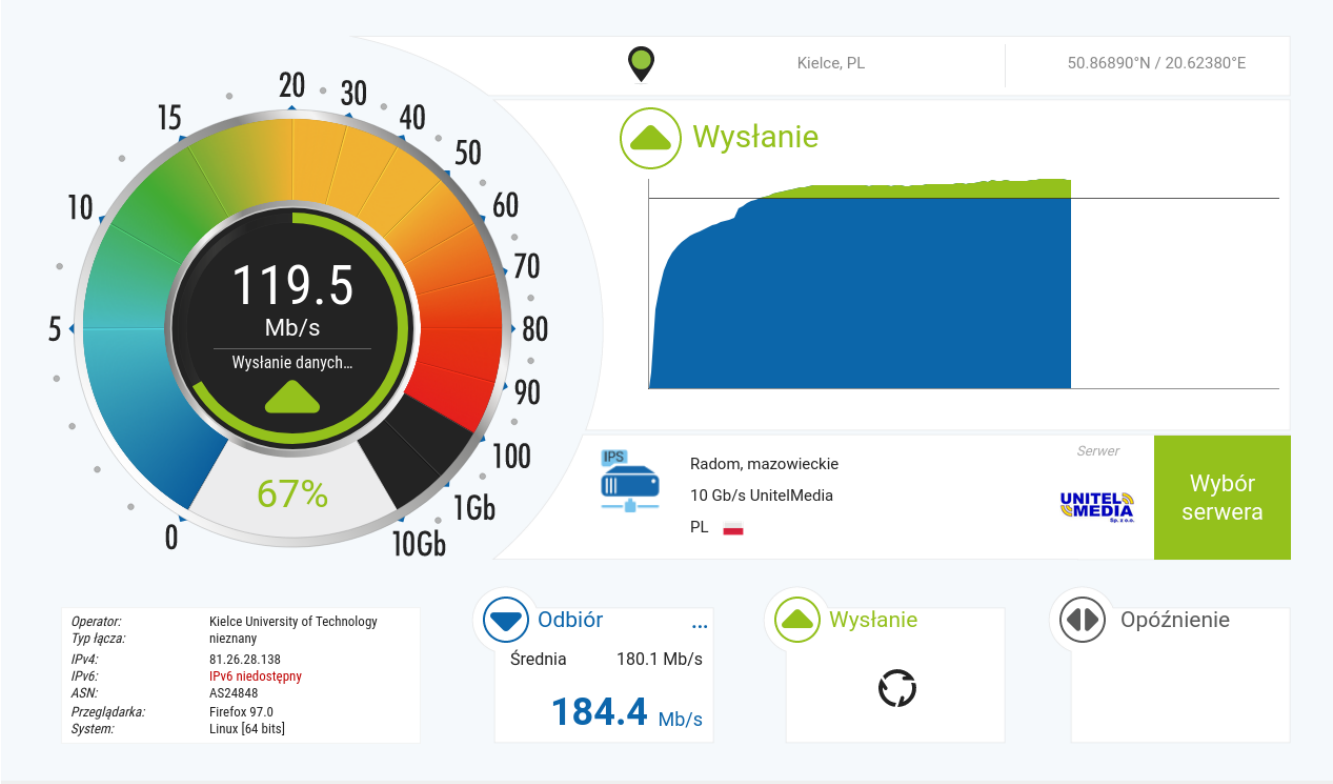
(Rysunek 3. Wynik testu sieci za pomocą programu speedtest.net)

www.nperf.com

Aplikacja internetowa npref.com jest podobna do speedtes.net. Wyniki przedstawione są również w atracyjnej formie graficznej.



(Rysunek 4. Test prędkości sieci programem www.nperf.com)



(Rysunek 5. Test prędkości sieci programem www.nperf.com)

14.5. Ograniczanie ruchu sieciowego na przykładzie routera klasy "domowej"

Router łączy sieć domową (firmową) z Internetem. Na routerze możemy ograniczać prędkość, wyłączać dostęp do internetu lokalnym hostom. Wyłącznie i ograniczenia ruchu mogą być stałe jak i uruchamiana na określony czas.

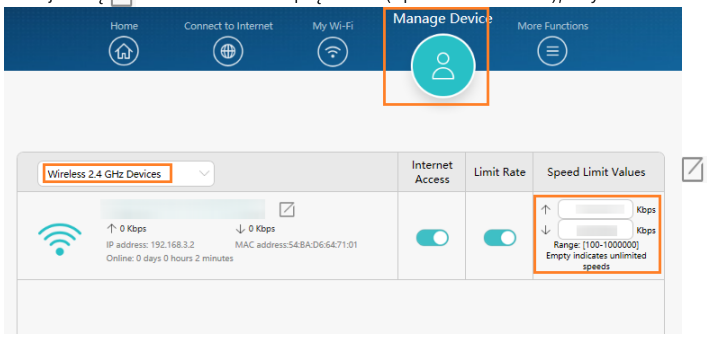
W routerze "domowym", czyli tanim urządzeniu zaprojektowanym do obsługi sieci składającej się z od kilku do kilkudziesięciu hostów, możemy wyłączyć dostęp oraz ograniczać prędkość pobierania i wysyłania danych. Możliwości ograniczania ruchu sieciowego zależą oczywiście od modelu routera.

Celem wprowadzania ograniczenia prędkości transferu jest zabezpieczenie się przed spadkiem prędkości pobierania lub wysyłania na kluczowych hostach naszej sieci domowej. Na przykład: jeżeli zakładamy, że nasz laptop, na którym wykonujemy prace zdalną jma miec stabilne połaczanie z Internetem podczas telekonferencji wszytkim innym urządzeniom wprowadzimy limity prędkości.

Przykład włączenia ograniczeń prędkości w routerze Wi-Fi Huawey:

1. Podłącz komputer/telefon do routera Wi-Fi (sprawdź na tabliczce znamionowej na spodzie routera domyślną nazwę Wi-Fi, bez hasła) lub podłącz komputer do portu LAN routera za pomocą kabla Ethernet. Wprowadź domyślny adres IP w pasku adresu przeglądarki i zaloguj się do internetowej strony zarządzania (sprawdź domyślny adres IP na tabliczce znamionowej na dole routera).

2. Kliknij Zarządzaj urządzeniem (Manage Device), wybierz telefon lub komputer, dla którego chcesz ustawić limit, włącz opcję Prędkość limitu i kliknij ikonę ✎ w Wartości limitu prędkości (Speed limit Values), aby ustawić maksymalną prędkość wysyłania i pobierania.



(Rysunek - ekran konfiguracji urządzeń, źródło: https://consumer.huawei.com/en/support/content/en-us15806295/)

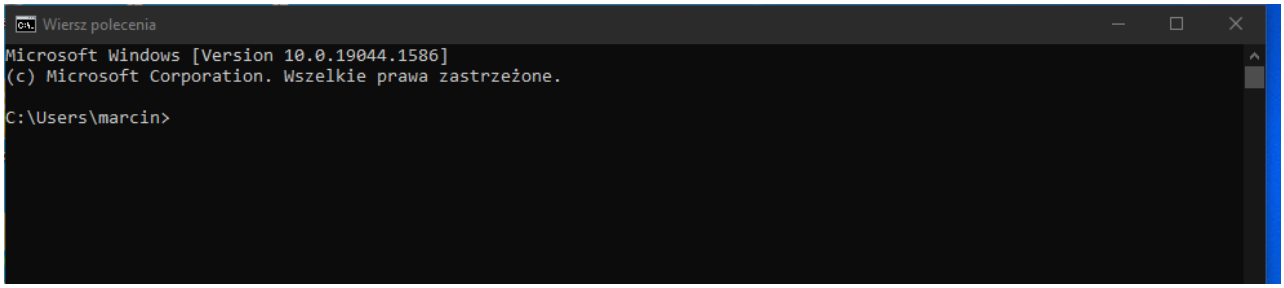
15. Podstawowe testy sieci komputerowych

Testy sieci komputerowej w środowisku MS Windows oraz UNIX-Like za pomocą programów:

- ping
- tracert
- telnet
- nc
- wget

Wszystkie powyższe programy uruchamiamy wpisując polecenie w terminalu / wierszu poleceń.
W systemie operacyjnym Linux z uruchomionym środowiskiem graficznym / macOS aby wykonać polecenie wpisywane z klawiatury należy uruchomić terminal. Polecenia wpisujemy w oknie terminala.

W systemie operacyjnym MS Windows aby wykonać polecenie wpisywane z klawiatury należy należy uruchomić wiersz poleceń. Aby uruchomić wiersz poleceń w Windows 10/11 klikamy "Start" i w oknie wyszukiwania wpisujemy cmd



15.1. ping

Opis programu ping

Program ping służy do diagnozy połączeń sieciowych. Sprawdzamy nim jakość połączenia między komputerami wysyłającym zapytania a odsyłającym odpowiedź.
Ping odpowie nam na pytania:

- Czy istnieje połączenie miedzy komputerami?
- Jaki jest czas odpowiedzi na wysłany pakiet?

Program uruchamiamy w wierszu poleceń MS Windows (terminal Linux/Mac). W wierszu poleceń wpisujemy: ping [IP lub nazwa] oraz zatwierdzamy przez Enter.

Przykład działania programu ping w Linuxie:

```
ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.364 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.274 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.433 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.545 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=0.380 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=64 time=0.284 ms
64 bytes from 10.10.10.1: icmp_seq=7 ttl=64 time=0.477 ms
64 bytes from 10.10.10.1: icmp_seq=8 ttl=64 time=0.257 ms
^C
--- 10.10.10.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7154ms
rtt min/avg/max/mdev = 0.257/0.376/0.545/0.099 ms
```

W powyższym przykładzie wysłano 8 razy pakiet *ICMP Echo Request* i odebrano tyle samo odpowiedzi (*ICMP Echo Reply)*. Pakiety wysyłano z komputera o IP 10.10.10.2 do komputera o IP 10.10.10.1. Średni czas odpowiedzi to 0,376 milisekundy.

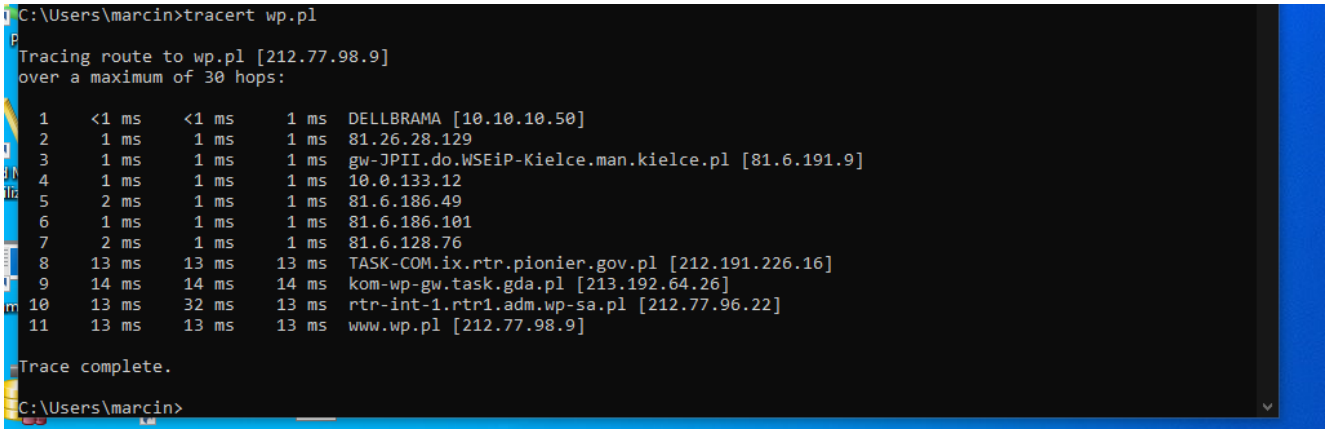
15.2. tracert

Tracert to program do określania marszruty (trasy) pakietów w sieci IP to tracert (MS Windows) / traceroute (Linux/macOS)

Tracert/traceroute zwraca listę kolejnych routerów na trasie do docelowego komputera w sieci.

Im dłuższa trasa - większa ilość routerów, tym komunikacja z badanym komputerem w sieci jest trudniejsza. Jeżeli na naszej trasie wystąpi źle skonfigurowany router będziemy mieć utrudniony dostęp do danego komputera (wolno ładująca się strona www, błędy przy pobieraniu plików, zła jakość radia internetowego, itp.)

Przykład zbadania trasu od siedziby uczelni do serwera wp.pl:



W powyższym przykładzie widzimy 11 węzłów (routerów)

15.3. telnet

Telnet jest to program używany po połącznia się ze zdalnym serwerem. Serwer telnet instalowany jest na komputerach klasy serwerowej ale także szeroko wykorzystywany jest we wszelkiego rodzaju urządzeniach sieciowych (np. switch, AccessPoint)

Programu telnet możemy użyć w celu sprawdzania czy na zdalnym komputerze działa dana usługa, np. usługa SMTP, HTTP.

W celu sprawdzania łączności między komputerem klienta a serwerem w wierszu poleceń (terminalu) wydajmy polecenie:

telnet [adres serwera badanego] [port usługi podanej]

Jeżeli chcemy sprawdzić czy na komputerze www.nasa.gov jest działający serwer STMP i z naszego komputera będziemy mogli się z mim połączyć i wysłać pocztę to wydajemy polecenie:

telnet www.nasa.gov 25

gdzie 25 to numer portu TCP, na którym nasłuchuje usługa SMTP (wysyłanie poczty).

15.4. nc

Netcat (nc) jest to polecenie wykonywane w terminalu. Jest dostępne w systemach Linux i macOS Testować nim można jednocześnie działanie wielu portów TCP na zdalnym serwerze.

Przykład:

w trminalu linuxa wpisuję:

nc -z -v 10.10.10.1 22

Polecenie zwraca wynik:

Connection to 10.10.10.1 22 port [tcp/ssh] succeeded!

Oznacza to udane połączenie do hosta 10.10.10.1 na porcie TCP 22

15.5. wget

Wget to program konsolowy, który służy do pobierania plików. Wget zwraca prędkość pobierania dzięki czemu uzyskujemy informację o wydajności pobierania naszego łącza internetowego.

Przykład:

W terminalu wpisuję:

wget https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz -O moodle-latest-311.tgz

Oznacza to że będę pobierał plik z serwera **https://download.moodle.org**, pobrany plik zapiszę pod nazwą **moodle-latest-311.tgz**

Po wydaniu polecenie w terminalu wget zwraca następujące informacje:

--2022-03-31 11:31:57-- https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz
Resolving download.moodle.org (download.moodle.org)... 104.22.64.81, 104.22.65.81, 172.67.26.233, ...
Connecting to download.moodle.org (download.moodle.org)|104.22.64.81|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60212386 (57M) [application/g-zip]
Saving to: 'moodle-latest-311.tgz'

moodle-latest-311.tgz 100%
[===>]
57,42M 11,0MB/s in 5,2s

2022-03-31 11:32:03 (11,1 MB/s) - 'moodle-latest-311.tgz' saved [60212386/60212386]

Widzimy prędkość z jaką pobrał się plik - 11,0 MB/s