

## **Moduł 1: Wprowadzenie do sieci komputerowych**

Aby zrozumieć, jaką rolę odgrywają komputery w systemach sieciowych, rozważmy Internet. Internet jest ważnym zasobem, istotnym w funkcjonowaniu biznesu, przemysłu i szkolnictwa. Tworzenie sieci mającej połączenie z Internetem wymaga starannego planowania. Nawet w przypadku pojedynczego komputera PC, aby podłączyć się do Internetu niezbędne jest sporządzenie planu i podjęcie odpowiednich decyzji. Należy wziąć pod uwagę nie tylko komputer, lecz również urządzenie umożliwiające jego połączenie do Internetu, takie jak karta sieciowa lub modem. Aby uzyskać połączenie z Internetem, należy skonfigurować odpowiednie protokoły, czyli reguły. Równie ważny jest wybór odpowiedniej przeglądarki WWW.

### **1.1 Nawiązywanie połączenia z Internetem    1.1.1 Wymagania dotyczące połączenia z Internetem**

Internet jest największą na Ziemi siecią służącą do przesyłania danych. Składa się on z wielkiej liczby połączonych ze sobą sieci, zarówno dużych, jak i małych. Nadawcami i odbiorcami danych przesyłanych przez Internet są komputery indywidualnych użytkowników. Aby połączyć się przez Internet, wymagane są: połączenie fizyczne, połączenie logiczne oraz odpowiednie aplikacje.

Połączenie fizyczne jest realizowane za pomocą karty rozszerzeń, takiej jak modem lub karta sieciowa, łączącej komputer PC z siecią. Połączenie fizyczne służy do przekazywania sygnałów między komputerami znajdującymi się w sieci lokalnej (LAN) oraz do zdalnych urządzeń znajdujących się w Internecie.

Połączenia logiczne opisywane są przez standardy zwane protokołami. Protokół jest formalnym opisem zestawu reguł i konwencji określających sposób komunikacji między urządzeniami w sieci. Połączenia z Internetem mogą korzystać z wielu protokołów. W Internecie najczęściej wykorzystuje się zestaw protokołów TCP/IP (Transmission Control Protocol/Internet Protocol). Protokoły zestawu TCP/IP współpracują ze sobą w celu zapewnienia transmisji i odbioru danych, czyli informacji.

Ostatnią częścią połączenia są aplikacje, czyli programy, które interpretują dane i prezentują je w formie zrozumiałej dla człowieka. Aplikacje używają protokołów przy wysyłaniu i odbieraniu danych za pośrednictwem Internetu. Przeglądarka internetowa prezentuje dane opisane w języku HTML w formie strony WWW. Przykładami takich przeglądarek są Internet Explorer oraz Netscape. Protokół FTP jest używany do pobierania plików oraz programów z Internetu. Przeglądarki WWW używają również dodatków (plug-in), aby wyświetlić specyficzne typy danych, takie jak filmy lub animacje w formacie Flash. Powyższy opis jest wprowadzeniem do Internetu i może się wydawać zbyt uproszczonym. W miarę zgłębiania tematu stanie się jasne, że przesyłanie danych w Internecie jest skomplikowanym zadaniem.

### **1.1.2 Podstawowe informacje o komputerach PC**

Komputery są ważnymi składnikami sieci. Umiejętność rozpoznawania i nazywania głównych podzespołów komputera PC jest więc bardzo ważna. Wiele urządzeń sieciowych to specjalizowane komputery zawierające w większości takie same podzespoły jak zwykłe komputery PC.

Aby komputer mógł służyć jako niezawodne narzędzie do pobierania informacji, na przykład materiałów szkoleniowych z sieci WWW, musi pracować poprawnie. Aby utrzymać komputer w dobrym stanie, należy od czasu do czasu rozwiązywać pojawiające się problemy sprzętowe i programowe. Z tego powodu ważna jest umiejętność rozpoznawania poszczególnych składników komputera i znajomość ich funkcji:

#### **Niewielkie elementy dyskretne**

**Tranzystor** — element służący do wzmacniania sygnału bądź otwierania i zamykania obwodu.

**Układ scalony** — wykonany z materiału półprzewodnikowego element zawierający wiele tranzystorów i wykonujący określone zadanie.

**Rezystor** — element stosowany do ograniczania lub regulowania przepływu prądu elektrycznego w obwodzie elektronicznym.

**Kondensator** — podzespol elektroniczny złożony z dwóch przewodzących powierzchni metalowych oddzielonych izolatorem, magazynujący energię w postaci pola elektrostatycznego.

**Złącze** — część kabla, która jest wpinana do portu lub interfejsu.

**Dioda LED** — element półprzewodnikowy, który emisję światła, gdy przepływa przezń prąd.

#### **Podsystemy składowe komputera osobistego :**

**-Płytkę obwodu drukowanego (PCB)** — płytka montażowa, która na jednej lub po obu stronach ma nałożone (wydrukowane) ścieżki przewodzące. Może także zawierać wewnętrzne warstwy sygnałów, zasilania i uziemienia. Są na niej montowane mikroprocesory, układy scalone oraz inne podzespoły elektroniczne.

**-Napęd CD-ROM** — napęd dysków kompaktowych przeznaczony tylko do odczytu informacji z płyt CD-ROM.

**-Procesor (CPU)** — element komputera, który steruje działaniem wszystkich innych elementów. Pobiera instrukcje z pamięci i dekoduje je. Wykonuje operacje matematyczne i logiczne, tłumaczy i wykonuje instrukcje.

**-Napęd dyskietek** — napęd w komputerze, który odczytuje i zapisuje dane na dyskietkach, mających postać 3,5-calowych krążków z tworzywa sztucznego, pokrytych warstwą metalu. Standardowe dyskietki pozwalają na zapis około 1 MB danych.

**-Napęd dysku twardego** — urządzenie pamięci masowej w komputerze, które zawiera zestaw wirujących dysków pokrytych warstwą magnetyczną i zwanych talarzami, stosowane do przechowywania danych i programów. Dyski twardy różnią się między sobą pojemnością.

**-Mikroprocesor** — mikroprocesor jest procesorem, który składa się ze specjalnie zaprojektowanych krzemowych układów scalonych i jest bardzo mały. Mikroprocesor wykorzystuje technologię obwodów o bardzo dużej skali integracji (VLSI), co

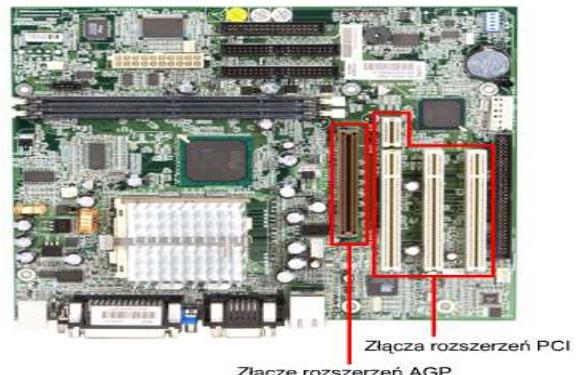
pozwala na integrację pamięci komputera, logiki i sterowania w pojedynczym układzie scalonym. Mikroprocesor zawiera centralną jednostkę wykonawczą (CPU).

**-Płyta główna** — główny obwód drukowany komputera. Płyta główna zawiera magistralę, mikroprocesor i układy scalone stosowane do sterowania wszystkimi wbudowanymi interfejsami urządzeń zewnętrznych, takich jak klawiatura, monitor tekstowy i graficzny, porty szeregowe, joystick i myszka.

**-Magistrala** — zestaw połączeń na płycie głównej, przez które przesyłane są dane i sygnały taktujące między różnymi częściami komputera.

**-Pamięć o dostępie swobodnym (RAM)** — znana również jako pamięć do zapisu i odczytu; można w niej zapisywać nowe dane i odczytywać dane tam przechowywane. Aby móc przechowywać dane, pamięć RAM wymaga zasilania elektrycznego. Jeśli komputer zostanie wyłączony lub nastąpi zanik zasilania, wszystkie dane przechowywane w pamięci RAM zostaną utracone.

**-Pamięć tylko do odczytu (ROM)** — pamięć komputera, w której znajdują się wcześniej zapisane dane. Po zapisaniu danych w układzie pamięci ROM nie można ich stamtąd usunąć, można je jedynie odczytywać.



**Jednostka systemowa** — główna część komputera, w skład której wchodzi obudowa, mikroprocesor, pamięć główna, magistrala i porty. Jednostka systemowa nie obejmuje klawiatury, monitora, ani żadnych innych urządzeń zewnętrznych przyłączanych do komputera.

**Złącze rozszerzeń** — gniazdo na płycie głównej, w którym można umieścić płytę drukowaną zwiększącą funkcjonalność komputera. Rysunek pokazuje gniazda rozszerzeń PCI (Peripheral Component Interconnect) oraz AGP (Accelerated Graphics Port). PCI jest szybkim złączem dla karty sieciowej, modemu wewnętrznego czy karty graficznej. Port AGP zapewnia połaczenie o dużej przepustowości pomiędzy urządzeniem graficznym a pamięcią systemową, w szczególności dostarcza szybkiego połączenia na potrzeby grafiki 3-D.

**Zasilacz** — podzespoł dostarczający energię elektryczną do komputera.

#### Podzespoły na płycie montażowej

**-Płyta montażowa** — płyta drukowana zawierająca obwody i gniazda, do których mogą być włożone dodatkowe urządzenia elektroniczne na innych płytach drukowanych (kartach rozszerzeń); w przypadku komputera określenie to odnosi się do płyty głównej lub jej części.

**-Karta sieciowa** — karta rozszerzeń umieszczana w komputerze w celu umożliwienia połączeń sieciowych.

**-Karta graficzna** — obwód drukowany umieszczany w komputerze w celu umożliwienia wyświetlania danych.

**-Karta dźwiękowa** — karta rozszerzeń umożliwiająca komputerowi przetwarzanie i emitowanie dźwięków.

**-Port równoległy** — interfejs umożliwiający przesyłanie jednocześnie więcej niż jednego bitu danych, używany do połączeń z urządzeniami zewnętrznymi, takimi jak drukarki.

**-Port szeregowy** — interfejs, który może być używany do komunikacji szeregowej, podczas której w danym momencie jest transmitowany tylko jeden bit danych.

**-Port myszy** — port przeznaczony do podłączania myszy do komputera.

**-Port USB (Universal Serial Bus)** — złącze umożliwiające szybkie i łatwe połaczenie do komputera takich urządzeń, jak myszka czy drukarka.

**-Firewire** — standard interfejsu magistrali szeregowej, umożliwiający szybką komunikację i izochroniczne usługi transmisji danych w czasie rzeczywistym.

**-Przewód zasilania** — przewód używany do podłączania urządzenia zasilanego prądem do źródła zasilania. Można przyjąć, że wewnętrzne podzespoły komputera stanowią sieć urządzeń dołączonych do magistrali systemowej. Z tego punktu widzenia komputer stanowi małą sieć komputerową.

**1.1.3 Karta sieciowa**, czyli adapter LAN, umożliwia komputerowi osobistemu nawiązywanie i przyjmowanie połączeń sieciowych. W przypadku komputerów biurkowych (typu desktop) jest to płytką drukowaną, która znajduje się w gnieździe na płycie głównej i udostępnia interfejs do sieci. W komputerach przenośnych (typu laptop) jest zwykle zintegrowana z komputerem lub ma postać karty PCMCIA (Personal Computer Memory Card International Association), inaczej zwanej kartą PC (PC card). Karty PCMCIA są niewielkie, o rozmiarach karty kredytowej. Typ używanej karty musi odpowiadać medium oraz protokołowi stosowanemu w sieci lokalnej.

Karta sieciowa komunikuje się z siecią za pośrednictwem łącza szeregowego, zaś z komputerem poprzez magistralę wewnętrzną komputera. Do współpracy z systemem operacyjnym karta sieciowa wykorzystuje żądanie przerwania (IRQ), adres I/O (wejścia-wyjścia) oraz górny obszar pamięci. Wartość żądania przerwania (IRQ) jest przypisany adresem, gdzie komputer może oczekiwany, że określone urządzenie przerwie mu, kiedy urządzenie to wysyła do komputera sygnały dotyczące jego działania. Na przykład, kiedy drukarka zakończyła drukowanie, wysyła do komputera sygnał przerwania. Sygnał ten chwilowo przerywa działanie komputera, który może podjąć decyzję, co przetwarzać w następnej kolejności. Ponieważ różne sygnały wysłane do komputera na tej samej linii przerwań nie mogłyby być zrozumiane przez komputer, dla każdego urządzenia musi być określona niepowtarzalna wartość oraz ścieżka do komputera. Przed pojawiением się urządzeń typu Plug-and-Play (PnP) użytkownicy często musieli ręcznie ustawać wartości IRQ i znać je, kiedy dodawali do komputera nowe urządzenie.

Podczas wyboru typu karty należy wziąć pod uwagę następujące czynniki:

**Protokoły** — Ethernet, Token Ring lub FDDI

**Typy mediów** — skrętka, kabel koncentryczny, dostęp bezprzewodowy lub światłowód

**Typ magistrali systemowej** — PCI lub ISA

#### 1.1.4 Instalacja karty sieciowej i modemu

Połączenie z Internetem wymaga karty, którą może być modem lub karta sieciowa.

Modem, którego nazwa jest złożeniem słów modulator i demodulator, jest urządzeniem umożliwiającym podłączenie komputera do linii telefonicznej. Modem przekształca (moduluje) dane z postaci cyfrowej na analogową, która jest odpowiednia do przesyłania po zwykłej linii telefonicznej. Po stronie odbiorczej modem demoduluje sygnał, zamieniając go na postać cyfrową. Modemy można instalować wewnątrz komputera lub też na zewnątrz przy pomocy linii telefonicznej. Każde urządzenie, które ma pracować w sieci, powinno być wyposażone w kartę sieciową stanowiącą interfejs między hostem a siecią. Istnieją różne typy kart sieciowych w zależności od konfiguracji poszczególnych urządzeń. Interfejsy sieciowe komputerów typu notebook mogą być wbudowane, bądź też dołączane za pomocą złącza PCMCIA. Na rys. pokazano karty PCMCIA dla połączeń przewodowych i bezprzewodowych oraz adapter (łącznik) USB - Ethernet. W przypadku komputerów stacjonarnych mogą być używane karty sieciowe wewnętrzne lub zewnętrzne, umożliwiające połączenie z siecią poprzez port USB.

**Instalacja karty sieciowej jest niezbędna w następujących sytuacjach:**

Dodanie karty sieciowej do komputera, który jej jeszcze nie posiadał

Wymiana źle funkcjonującej lub uszkodzonej karty sieciowej

Modernizacja polegająca na wymianie karty 10 Mb/s na lepszą kartę 10/100/1000 Mb/s

Wymiana na kartę sieciową innego typu, np. bezprzewodową

Instalacja drugiej karty sieciowej, np. na potrzeby związane z robieniem kopii zapasowych lub bezpieczeństwem sieci

Aby przeprowadzić instalację karty sieciowej lub modemu, mogą być wymagane następujące zasoby:

Wiedza o sposobie konfigurowania karty lub modemu, w tym o ustawieniach zworek i oprogramowaniu plug-and-play

Narzędzia diagnostyczne

Umiejętność rozwiązywania konfliktów sprzętowych związanych z zasobami

#### 1.1.5 Połączenia szybkie i połączenia telefoniczne — przegląd

We wczesnych latach sześćdziesiątych pojawiły się modemy, które służyły do łączenia terminali z komputerem centralnym. Wiele firm dzierżało wówczas czas komputera, gdyż było to bardziej opłacalne niż posiadanie na miejscu niezmiernie drogich maszyn. Prędkość połączenia była bardzo mała i wynosiła 300 bitów na sekundę (b/s), co odpowiada około 30 znakom na sekundę.

Kiedy w latach siedemdziesiątych komputery osobiste stały się tańsze, pojawiły się usługi (biuletyny) BBS (Bulletin Board Systems). Tego typu rozwiązań umożliwiały użytkownikom łączenie się z biuletynami dyskusyjnymi w celu wysyłania lub odczytywania wiadomości. Prędkość 300 b/s była do przyjęcia, ponieważ niewielu ludzi potrafi pisać lub czytać tak szybko. We wczesnych latach osiemdziesiątych liczba użytkowników usług BBS rosła wykładniczo i wkrótce okazało się, że 300 b/s to za mało, aby przesyłać duże pliki i grafikę. W latach dziewięćdziesiątych modemy pracowały z prędkością 9600 b/s i do roku 1998 osiągnęły prędkość 56 kb/s (56 000 b/s), która jest obecnie standardem.

Usługi szybkiego przesyłania danych, takie jak DSL i modemy kablowe, które znalazły początkowo zastosowanie w firmach, zaczęły stopniowo zdobywać rynek użytkowników prywatnych. Usługi te nie wymagają już stosowania drogiego sprzętu lub dodatkowej linii telefonicznej. Są to usługi dostępne przez cały czas, które umożliwiają natychmiastową łączność i nie wymagają nawiązywania połączenia dla każdej sesji. Zwiększa to niezawodność i elastyczność systemu oraz umożliwia współdzielenie połączenia z Internetem przez użytkowników w małych biurach i w sieciach domowych.

#### 1.1.6 Opis i konfiguracja zestawu protokołów TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) jest zestawem protokołów bądź reguł, które zostały utworzone w celu umożliwienia współdzielenia poprzez sieć zasobów współpracujących komputerów. Aby móc korzystać z zestawu protokołów TCP/IP na stacji roboczej, należy go skonfigurować przy użyciu programów narzędziowych zawartych w systemie operacyjnym. W systemach operacyjnych Windows i Mac OS proces ten przebiega bardzo podobnie.

#### 1.1.7 Testowanie połączeń przy użyciu polecenia ping

Ping jest podstawowym programem umożliwiającym sprawdzenie, czy określony adres IP istnieje i może przyjmować żądania. Jego nazwa jest akronimem od angielskiego określenia *Packet Internet (Inter-Network) Groper* (pakietowy poszukiwacz internetowy), który został wymyślony na zasadzie dopasowania do dźwięku towarzyszącego impulsowi sonaru odbitemu od obiektu znajdującego się pod wodą.

Działanie polecenia ping polega na wysyłaniu pod podany adres pakietów IP szczególnego rodzaju, zwanych datagramami ICMP (*Internet Control Message Protocol*) typu „prośba o echo” (*Echo Request*). Każdy wysłany pakiet zawiera żądanie wysłania odpowiedzi. Dane uzyskane po odebraniu odpowiedzi ukazują liczbę operacji zakończonych pomyślnie oraz czas przesyłania pakietów w obie strony. Na podstawie tych informacji można określić, czy istnieje połączenie z adresem docelowym. Polecenie ping jest używane do testowania funkcji wysyłania/odbierania danych przez kartę sieciową, konfiguracji zestawu protokołów TCP/IP oraz połączeń sieciowych. Poniżej podano kilka przykładowych testów przy użyciu polecenia ping:

**ping 127.0.0.1** — test specjalny, zwany wewnętrznym testem pętli zwrotnej. Sprawdzana jest dzięki niemu poprawność działania konfiguracji TCP/IP.

**ping lokalny adres IP** — polecenie ping dla hosta PC sprawdza poprawność konfiguracji adresu TCP/IP dla lokalnego hosta.

**ping adres IP domyślnej bramy** — polecenie ping dla domyślnej bramy sprawdza, czy router łączący sieć lokalną z innymi sieciami jest osiągalny.

**ping zdalny docelowy adres IP** — polecenie ping dla zdalnego adresu sprawdza połączenie z hostem zdalnym.

## 1.1.8 Przeglądarka WWW i dodatki (plug-in)

Przeglądarka WWW spełnia następujące funkcje:

Łączy się z serwerem WWW

Żąda przesłania informacji

Pobiera informacje

Wyświetla wyniki na ekranie

Przeglądarka WWW jest oprogramowaniem, które interpretuje język HTML (*Hypertext Markup Language*) — jeden z języków używanych do zapisywania zawartości strony WWW. Inne języki o zwiększonej funkcjonalności stają się częścią właśnie powstających technologii. HTML jest najbardziej znanym językiem znaczników, umożliwiającym wyświetlanie grafiki, odtwarzanie dźwięków, filmów oraz innych plików multimedialnych. Hiperłącza umieszczone na stronie WWW umożliwiają sprawne przemieszczanie się do innych lokalizacji na tej samej lub innej stronie WWW.

Dwie najpopularniejsze przeglądarki są Internet Explorer (IE) i Netscape Communicator. Chociaż zadania wykonywane przez nie są takie same, to jednak istnieją między nimi pewne różnice. Niektóre witryny mogą nie obsługiwać jednej z tych przeglądarek, zatem zaleca się zainstalowanie na komputerze obu programów.

### Netscape Navigator:

Pierwsza powszechnie używana przeglądarka

Zajmuje mniej miejsca na dysku

Wyświetla pliki HTML, obsługuje pocztę elektroniczną i przesyłanie plików oraz wiele innych funkcji

### Internet Explorer (IE):

Silnie zintegrowana z innymi produktami firmy Microsoft

Zajmuje więcej miejsca na dysku

Wyświetla pliki HTML, obsługuje pocztę elektroniczną i przesyłanie plików oraz wiele innych funkcji

Istnieje wiele specyficznych typów plików, które nie mogą być wyświetlane przez standardowe przeglądarki. Aby wyświetlić zawartość tych plików w przeglądarce, należy tak ją skonfigurować, aby korzystała z dodatków (plug-in).

Aplikacje te współpracują z przeglądarką i uruchamiają programy wyświetlające zawartość specjalnych plików:

**Flash** — odtwarza pliki multimedialne utworzone za pomocą programu Macromedia Flash

**Quicktime** — odtwarza pliki wideo (program firmy Apple)

**Real Player** — odtwarza pliki audio

Aby zainstalować dodatek plug-in Flash, wykonaj następujące czynności:

Przejdź do witryny firmy Macromedia.

Pobierz najnowszy plik instalacyjny.

Uruchom go i zainstaluj w przeglądarce Netscape lub IE.

Sprawdź instalację i poprawność działania aplikacji, przechodząc na stronę Cisco Academy.

Oprócz wyświetlania materiałów szkoleniowych Cisco Academy komputery mogą wykonywać wiele innych użytkowych zadań. W zastosowaniach biurowych pracownicy często używają pakietów oprogramowania biurowego, takich jak Microsoft Office. Aplikacje biurowe najczęściej składają się z następujących programów:

**Arkusze kalkulacyjne**, w których dane są przechowywane w tabelach składających się z kolumn i wierszy, często używane do przetwarzania i analizowania danych przy użyciu formuł.

**Edytory tekstów**, które są aplikacjami służącymi do tworzenia i edycji dokumentów tekstowych.

**Nowoczesne edytory tekstów** umożliwiają użytkownikowi tworzenie skomplikowanych dokumentów zawierających grafikę oraz bogato formatowany tekst.

**Oprogramowanie zarządzające** bazami danych jest używane do przechowywania, utrzymywania, organizowania, sortowania i filtrowania rekordów. Rekord jest zestawem informacji, który jest identyfikowany przez pewien wspólny element, na przykład przez nazwę klienta.

**Oprogramowanie prezentacyjne** jest używane do przygotowywania i wykonywania prezentacji używanych podczas spotkań, lekcji czy pokazów.

**Menedżer informacji** osobistych zawiera narzędzie do obsługi poczty

elektronicznej, listę kontaktów,

kalendarz oraz listę zadań do wykonania.

**Aplikacje biurowe** stanowią dziś powszechnie używane narzędzie pracy, tak jak niegdyś, przed nadaniem ery komputerów, maszyny do pisania.

## 1.1.9 Rozwiązywanie problemów z połączeniem z Internetem

Podczas tych zajęć będą rozwiązywane problemy pojawiające się w konfiguracji sprzętu, oprogramowania i sieci. Celem zajęć jest zidentyfikowanie i rozwiązanie w określonym czasie problemów, dzięki czemu będzie możliwe uzyskanie dostępu do materiałów szkoleniowych. Zademonstrowana zostanie złożoność konfiguracji

1. Zdefiniuj problem
2. Zbierz fakty
3. Rozważ wszystkie rozwiązania
4. Utwórz plan działania
5. Wykonaj plan
6. Zaobserwuj efekty
7. Udokumentuj efekty
8. Wywołaj problemy i rozwiąż je

nawet tak prostego procesu jak dostęp do sieci WWW. W ramach zajęć zostaną zaprezentowane procesy i procedury związane z rozwiązywaniem problemów sprzętowych, programowych i sieciowych.

## 1.2 Elementy matematyki

Wartość odpowiadająca pozycji	1000    100    10    1
Podstawa Wykładnik	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Liczba symboli	10
Symbol	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Uzasadnienie	10 = liczba palców u rąk

używane do przedstawiania symboli wprowadzanych z klawiatury. Gdy komputer wysyła przez sieć informacje o stanie włączonym lub wyłączonym, są one zamieniane na sygnały elektryczne, świetlne lub radiowe, reprezentujące zera i jedynki. Należy zauważyć, że każdemu znakowi jest przypisany unikalny wzór złożony z ośmiu cyfr dwójkowych.

Ponieważ komputery są skonstruowane przy wykorzystaniu przełączników dwustanowych (włączony/wyłączony), cyfry i liczby dwójkowe są dla nich czymś naturalnym. Ludzie używają systemu dziesiętnego, który wygląda prosto w porównaniu z długimi seriami zer i jedynek używanych przez komputery. Liczby dwójkowe używane przez komputer są zamieniane na łatwiej czytelne liczby dziesiętne.

Niekiedy liczby dwójkowe są zamieniane na cyfry szesnastkowe (heksadecymalne), które są krótsze od odpowiadających im liczb dwójkowych dzięki zastosowaniu znaków szesnastkowych. Dzięki temu łatwiej je zapamiętać i operować na nich.

### 1.2.2 Bity i bajty

Dwójkowa cyfra 0 może być reprezentowana przez napięcie 0 woltów ( $0 = 0$  woltów).

Dwójkowa cyfra 1 może być reprezentowana przez napięcie +5 woltów ( $1 = +5$  woltów).

Komputery są tak skonstruowane, że korzystają z grup składających się z ośmiu bitów. Taka grupa ośmiu bitów nosi nazwę bajtu. W komputerze jeden bajt reprezentuje najmniejszy możliwy do zaadresowania obszar pamięci.

Obszary te reprezentują wartość lub pojedynczy znak danych, taki jak znak kodu ASCII. Liczba kombinacji stanów ośmiu przełączników, z których każdy może być niezależnie włączony lub wyłączony, wynosi 256. Dlatego bajt może przyjmować wartości liczbowe z zakresu od 0 do 255. Bajt jest ważnym pojęciem, służącym do wyjaśnienia zasad pracy komputerów i sieci.

### 1.2.3 System liczbowy o podstavie 10

Wartość odpowiadająca pozycji	1000    100    10    1
Podstawa Wykładnik	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Liczba symboli	10
Symbol	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Uzasadnienie	10 = liczba palców u rąk

pozycja reprezentuje  $10^6$  ( $10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1\ 000\ 000$ ). Analogicznie określa się wartość reprezentowaną przez dalsze pozycje.

Przykład:  $2134 = (2 \times 10^3) + (1 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$

Cyfra 4 znajduje się na pozycji jedności, 3 na pozycji dziesiątek, 1 na pozycji setek i 2 na pozycji tysięcy. Ten przykład wydaje się oczywisty, gdy mamy do czynienia z systemem dziesiętnym. Jednak dokładne zrozumienie zasad systemu dziesiętnego jest ważne, gdyż umożliwia zrozumienie systemu dwójkowego i szesnastkowego. W obu tych systemach używane są takie same metody jak w systemie dziesiętnym.

### 1.2.1 Dwójkowa reprezentacja danych

Dane są przechowywane i przetwarzane w komputerach za pomocą swoistych elektronicznych przełączników, które mogą być włączone albo wyłączone. Komputery mogą przetwarzać tylko takie dane, które są w formacie dwustanowym, zwany również binarnym. Cyfry 1 i 0 są reprezentowane przez dwa możliwe stany elementów elektronicznych w komputerze: cyfra 1 przez stan włączony, zaś cyfra 0 przez stan wyłączony. Są one znane pod nazwą cyfr binarnych, dwójkowych lub bitów.

Najczęściej używanym standardem służącym do reprezentacji danych alfanumerycznych w komputerze jest ASCII (*American Standard Code for Information Interchange*). W standardzie ASCII cyfry dwójkowe są

Jednostki	Definicja	Ilość bajtów*	Ilość bitów*	Przykłady
Bit (b)	Cyfra dwójkowa, 1 albo 0	1	1	Włączony/wyłączony; Otwarty/zamknięty; +5 woltów lub 0 woltów
Bajt (B)	8 bitów	1	8	Reprezentacja litery X w kodzie ASCII
Kilobajt (KB)	1 kilobajt = 1024 bajty	1000	8,000	Typowy list e-mail = 2 KB 10-stronicowy raport = 10 KB Wczesne komputery PC = 64 KB pamięci RAM
Megabajt (MB)	1 megabajt = 1024 kilobajty = 1 048 576 bajtów	1 milion	8 milionów	Dyskietka = 1,44 MB Typowa pamięć RAM = 32 MB CDROM = 650 MB
Gigabajt (GB)	1 gigabajt = 1024 megabajtów = 1 073 741 824 bajty	1 miliard	8 miliardów	Typowy dysk twardy = 40 GB (lub więcej)
Terabajt (TB)	1 terabajt = 1024 gigabajty = 1 099 511 627 778 bajtów	1 bilion	8 bilionów	Ilość danych, które teoretycznie można przesyłać w światłowodzie w ciągu jednej sekundy

Systemy liczbowe składają się z symboli oraz reguł ich używania.

Najczęściej używanym systemem liczbowym jest system dziesiętny, zwany również systemem o podstavie 10. W systemie tym używa się dziesięciu symboli — 0, 1, 2, 3, 4, 5, 6, 7, 8 i 9. Symbole te można łączyć ze sobą w celu przedstawienia wszystkich możliwych wartości liczbowych.

System dziesiętny jest oparty na potęgach liczby 10. Każda kolejna cyfra, od prawej do lewej, jest mnożona przez liczbę 10 (podstavę) podniesioną do potęgi (wykładnika). Potega, do której podnoszona jest liczba 10, zależy od pozycji cyfry w stosunku do przecinka dziesiętnego. Gdy liczba dziesiętna jest odczytywana od prawej do lewej, pierwsza, czyli skrajnie prawa pozycja reprezentuje  $10^0$  (1), druga pozycja reprezentuje  $10^1$  ( $10 \times 1 = 10$ ). Trzecia pozycja reprezentuje  $10^2$  ( $10 \times 10 = 100$ ). Siódma

pozycja reprezentuje  $10^6$  ( $10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1\ 000\ 000$ ). Analogicznie określa się wartość reprezentowaną przez dalsze pozycje.

Przykład:  $2134 = (2 \times 10^3) + (1 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$

Cyfra 4 znajduje się na pozycji jedności, 3 na pozycji dziesiątek, 1 na pozycji setek i 2 na pozycji tysięcy. Ten przykład wydaje się oczywisty, gdy mamy do czynienia z systemem dziesiętnym. Jednak dokładne zrozumienie zasad systemu dwójkowego i szesnastkowego. W obu tych systemach używane są takie same metody jak w systemie dziesiętnym.

## **1.2.4 System liczbowy o podstawie 2**

Komputery rozpoznają i przetwarzają dane w systemie liczbowym o podstawie 2, czyli binarnym lub dwójkowym. System dwójkowy używa tylko dwóch symboli, 0 i 1, zamiast dziesięciu symboli używanych w dziesiętnym systemie liczbowym. Pozycja lub miejsce każdej cyfry dwójkowej, od strony prawej do lewej, reprezentuje liczbę 2 (cyfrę podstawową) podniesioną do potegi (wykładnika), począwszy od 0. Wartościami dla tych pozycji są, od prawej do lewej,  $2^0$ ,  $2^1$ ,  $2^2$ ,  $2^3$ ,  $2^4$ ,  $2^5$ ,  $2^6$  i  $2^7$ , czyli odpowiednio 1, 2, 4, 8, 16, 32, 64 i 128.

Przykład:  $10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22$  (16+0+4+2+0) Jeżeli liczba dwójkowa ( $10110_2$ ) jest odczytywana od strony lewej do prawej, to na pozycji szesnastek znajduje się 1, na pozycji ósemek — 0, na pozycji czwórek — 1, na pozycji dwójek — 1 i 0 na pozycji jedynek. Po dodaniu tych wartości otrzymujemy liczbę 22.

Wartość odpowiadająca pozycji	128	64	32	16	8	4	2	1
Podstawa Wykładnik	$2^7 = 128$	$2^3 = 8$						
	$2^6 = 64$	$2^2 = 4$						
	$2^5 = 32$	$2^1 = 2$						
	$2^4 = 16$	$2^0 = 1$						
Liczba symboli	2							
Symbole	0, 1							
Uzasadnienie	Dwustanowe (dyskretne binarne) systemy napięciowe utworzone z tranzystorów są niewielkie, tanie i odporne na zakłócenia zewnętrzne. Posiadają wiele różnorodnych zastosowań.							

(6+0+4+2+0) – Jeżeli liczba dwuścigowa (10110...) jest odczytywana od

## **1.2.7 Reprezentacja dwójkowych liczb 32-bitowych za pomocą czterech oktetów oddzielanych kropkami**

Obecnie adresy przypisywane komputerom w Internecie są 32-bitowymi liczbami dwójkowymi. Aby ułatwić posługiwanie się takimi adresami, 32-bitowa liczba dwójkowa jest rozbijana na liczby dziesiętne. W tym celu dzieli się taką liczbę na cztery grupy, z których każda jest ośmiobitową liczbą dwójkową. Następnie każdą grupę ośmiu bitów, zwaną też oktetem, należy zamienić na jej odpowiednik dziesiętny. Taką konwersję należy przeprowadzić w taki sam sposób, jaki przedstawiono na poprzedniej stronie, gdzie omówiono konwersję liczby dwójkowej na dziesiętną.

Następnie całą 32-bitową liczbę dwójkową zapisuje się jako cztery grupy cyfr dziesiętnych oddzielone kropkami. Ta notacja znana jest pod nazwą notacji kropkowo-dziesiętnej; umożliwia ona zwarty, łatwy do zapamiętania zapis przedstawiający 32-bitowy adres. Reprezentacja ta będzie często używana w dalszej części kursu, zatem konieczne jest jej zrozumienie. Podczas zamiany z postaci kropkowo-dziesiętnej na dwójkową należy pamiętać, że każda grupa składa się z jednej, dwóch lub trzech cyfr dziesiętnych reprezentujących osiem cyfr dwójkowych. Jeśli liczba dziesiętna zamieniana na postać dwójkową jest mniejsza niż 128, konieczne jest uzupełnienie postaci dwójkowej zerami z lewej strony, tak aby łączna liczba cyfr binarnych wynosiła osiem. Przykład: Zamień zapis 200.114.6.51 na jego 32-bitowy odpowiednik dwójkowy. Zamień liczbę 10000000 01011101 00001111 10101010 na jej odpowiednik w notacji kropkowo-dziesiętnej.

<b>Dwójkowo</b>	11001000	01110010	00000110	00110011			
<b>Dziesiętnie</b>	200	.	114	.	6	.	51
	liczba	kropka	liczba	kropka	liczba	kropka	liczba

### 1.2.8. Liczby szesnastkowe

### Konwersja liczby dwójkowej na liczbę szesnastkową

100100100010111110111110111001001

**Przekształcamy na:**

0001 0010 0100 0101 1111 0111 1101 1100 1001

**Przekształcamy na:**

1 2 4 5 F 7 D C 9

A zatem:

1001001000101111011110111001001 dwójkowo

= 1245F7DC9 szesnastkowo

dwójkowej liczbie 0010000100000010 odpowiada szesnastkowa liczba 2102. Słowo „szesnastkowy” jest często zastępowane przez skrót 0x występujący obok wartości liczby: 0x2102. Podobnie jak system dwójkowy i dziesiętny, system szesnastkowy opiera się na odpowiednim zastosowaniu symboli, potęg i pozycji cyfr. Symbolami używanymi w układzie szesnastkowym są cyfry: 0-9, A, B, C, D, E, F.

Należy zauważać, że każdej z możliwych kombinacji czterech cyfr dwójkowych odpowiada jeden symbol szesnastkowy, podczas gdy w systemie dziesiętnym wymagałoby to jednej lub dwóch cyfr. Dwie cyfry szesnastkowe z powodzeniem mogą zatem reprezentować dowolną kombinację ośmiu cyfr dwójkowych. Reprezentacja dziesiętna 8-bitowej liczby wymagałaby użycia dwóch lub trzech cyfr. Z tego powodu właśnie, symbole szesnastkowe używa się częściej do przedstawiania dużych liczb binarnych. Poza tym używanie szesnastkowej notacji ułatwia czytanie i zapisywanie długich ciągów cyfr binarnych. Należy pamiętać, że oznaczenie  $0x$  wskazuje na użycie wartości szesnastkowej. Przykładowa liczba

Liczby szesnastkowe (heksadecymalne) są często używane podczas pracy z komputerem, ponieważ pozwalają przedstawiać liczby dwójkowe w bardziej czytelnej postaci. Komputer wykonuje obliczenia w systemie dwójkowym, ale często zdarza się, że wyjściowe dane dwójkowe są przedstawiane w postaci szesnastkowej w celu zwiększenia ich czytelności. Zamiana liczb szesnastkowych na dwójkowe i odwrotnie jest często wykonywanym zadaniem podczas pracy z rejestrem konfiguracyjnym routerów Cisco. Rejestry konfiguracyjne routerów Cisco mają długość 16 bitów. Taka 16-bitowa liczba dwójkowa może być przedstawiona w postaci czterocyfrowej liczby szesnastkowej. Na przykład

5D może zostać zapisana jako 0x5D. Aby zamienić liczbę szesnastkową na dwójkową, należy zamienić każdą jej cyfrę na jej czterobitowy równoważnik dwójkowy.

Dwójkowo	Szesnastkowo	Dziesiętnie	Dwójkowo	Szesnastkowo	Dziesiętnie
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	A	10
0011	3	3	1011	B	11
0100	4	4	1100	C	12
0101	5	5	1101	D	13
0110	6	6	1110	E	14
0111	7	7	1111	F	15

### Konwersja liczby szesnastkowej na liczbę dwójkową

0x2102

Przekształcamy na:

2 1 0 2  
0010 0001 0000 0010

A zatem:

2102 w zapisie szesnastkowym odpowiada: 0010 0001 0000 0010 w zapisie dwójkowym

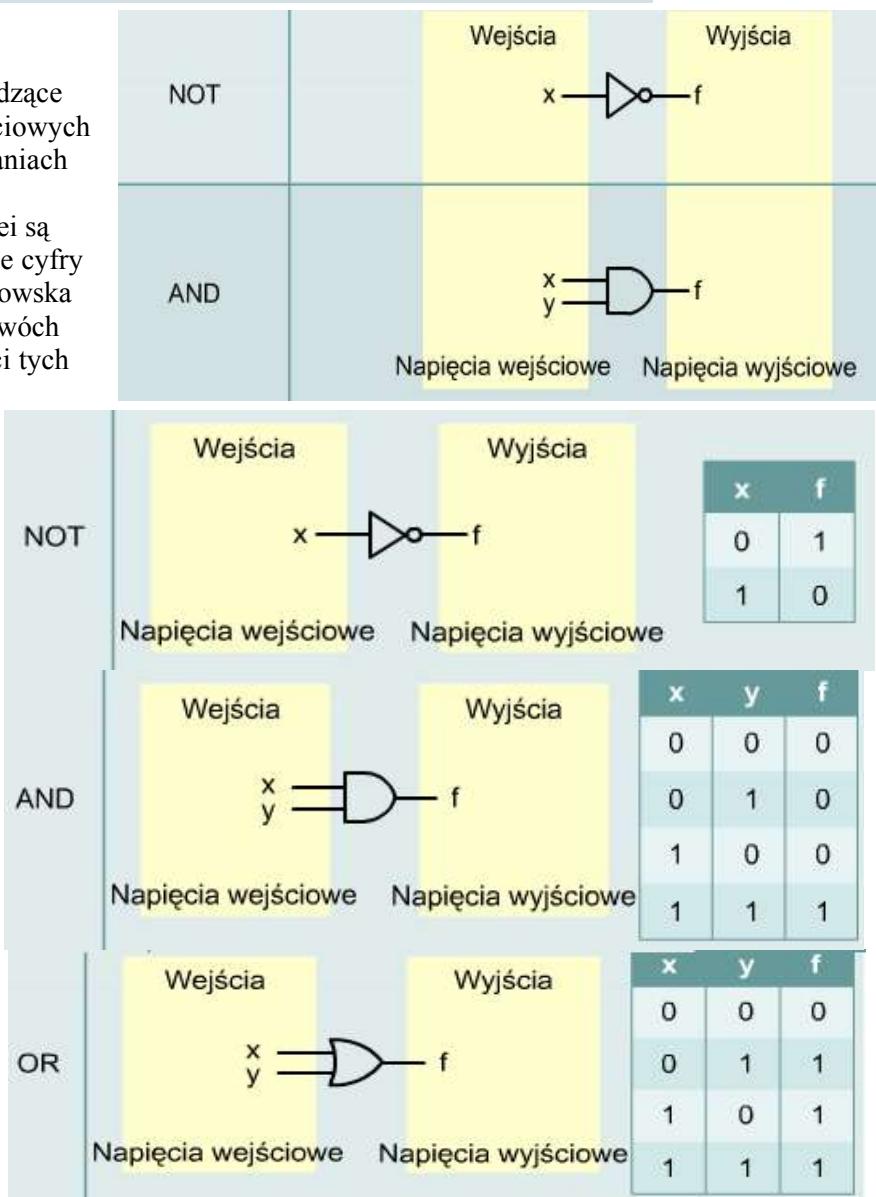
### 1.2.9 Logika boole'owska (binarna)

Logika boole'owska opisuje działanie układów cyfrowych, które przyjmują jeden lub dwa nadchodzące sygnały napięciowe. W zależności od napięć wejściowych generowane jest napięcie wyjściowe. W zastosowaniach komputerowych napięcie jest powiązane z dwoma stanami,łączonym i wyłączonym. Te stany z kolei są skojarzone z wartościami 0 i 1, które stanowią dwie cyfry w dwójkowym układzie liczbowym. Logika boole'owska jest logiką binarną, która umożliwia porównanie dwóch liczb oraz określenie wyniku na podstawie wartości tych liczb. Wynik jest określany przy użyciu funkcji logicznych AND, OR i NOT. Z wyjątkiem operacji NOT logiczne operacje boole'owskie są funkcjonalnie podobne. Przyjmują dwie liczby, które mają wartości 0 lub 1, po czym generują wynik na podstawie odpowiedniej reguły logicznej.

**Operacja NOT** (logiczne „nie”) pobiera dowolną wartość, 0 lub 1, i zmienia ją na przeciwną. Jedynka staje się zerem, a zero — jedynką. Należy zapamiętać, że bramki logiczne są urządzeniami elektronicznymi służącymi wyłącznie do tego celu. Reguła logiczna, zgodnie z którą działają, polega na wygenerowaniu na wyjściu wartości przeciwej do wejściowej.

**Operacja AND** (logiczne „i”) przyjmuje dwie wartości wejściowe. Jeśli obie są równe 1, bramka logiczna generuje na wyjściu wartość 1. W innych przypadkach wartością wyjściową jest 0. Istnieją cztery kombinacje wartości wejściowych. Trzy z tych kombinacji generują 0, zaś jedna generuje 1.

**Operacja OR** (logiczne „lub”) również ma dwie wartości wejściowe. Jeśli co najmniej jedna z wartości wejściowych jest równa 1, wartością wyjściową jest 1. Ponownie mamy do czynienia z czterema kombinacjami wartości wejściowych. Tym razem trzy kombinacje generują 1, zaś czwarta generuje 0. Dwiema używanymi w sieci operacjami, w których używana jest logika boole'owska, są maskowanie podsieci oraz maskowanie szablonowe. Operacje maskowania umożliwiają filtrowanie adresów. Adresy służą do identyfikowania



urządzeń w sieci; można je grupować lub kontrolować przy użyciu innych operacji sieciowych. Funkcje te zostaną dokładnie opisane w dalszej części szkolenia.

## 1.2.10 Adresy IP i maski sieci

32-bitowe adresy binarne używane w Internecie są znane pod nazwą adresów IP (*Internet Protocol*). W tej sekcji zostanie omówiony związek między adresami IP a maskami sieci.

W adresach, które zostały przypisane komputerom, część bitów znajdująca się z lewej strony 32-bitowego adresu IP identyfikuje sieć. Liczba tych bitów zależy od tzw. klasy adresu. Pozostałe bity w 32-bitowym adresie IP identyfikują konkretny komputer znajdujący się w tej sieci. Taki komputer nazywany jest hostem. Adres IP komputera składa się z części sieciowej i części hosta, które reprezentują konkretny komputer znajdujący się w konkretnej sieci. Aby poinformować komputer o sposobie podziału na części 32-bitowego adresu IP, używana jest druga 32-bitowa liczba, zwana maską podsieci. Maska ta wskazuje, w jaki sposób powinien być interpretowany adres IP, określając liczbę bitów używanych do identyfikacji sieci, do której jest podłączony komputer. Maska podsieci jest wypełniana kolejnymi jedynkami wpisywanymi od lewej strony maski. Maska podsieci będzie zawierała jedynki w tych miejscach, które mają być interpretowane jako adres sieci, a pozostałe bity maski aż do skrajnego prawego bitu będą równe 0. Bitы w masce podsieci równe 0 identyfikują komputer lub hosta znajdującego się w tej sieci. Przykłady masek podsieci:

11111111000000000000000000000000 zapisana w notacji kropkowo-dziesiętnej jako 255.0.0.0

lub

11111111111111111111111111111111 zapisana w notacji kropkowo-dziesiętnej jako 255.255.0.0

W pierwszym przykładzie pierwsze osiem bitów od lewej strony reprezentuje część sieciową adresu, natomiast pozostałe 24 bity reprezentują część adresu identyfikującą hosta. W drugim przykładzie pierwsze 16 bitów reprezentuje część sieciową adresu, a pozostałe 16 bitów reprezentuje część adresu identyfikującą hosta.

Zamiana adresu IP 10.34.23.134 na postać dwójkową daje w wyniku:

00001010.00100010.00010111.10000110

Wykonanie boole'owskiej operacji AND na adresie IP 10.34.23.134 i masce podsieci 255.0.0.0 prowadzi do utworzenia adresu sieciowego hosta:

00001010.00100010.00010111.10000110

11111111.00000000.00000000.00000000

00001010.00000000.00000000.00000000

00001010.00100010.00010111.10000110

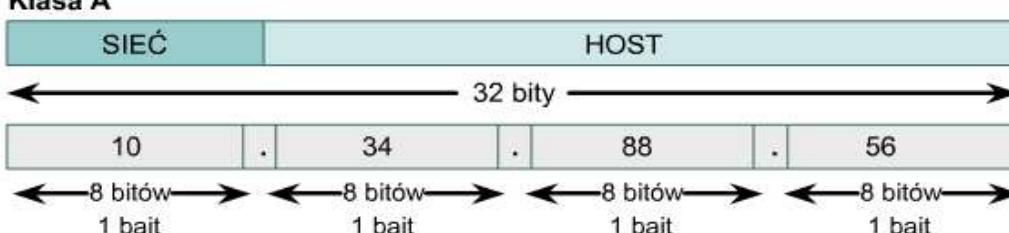
11111111.11111111.00000000.00000000

00001010.00100010.00000000.00000000

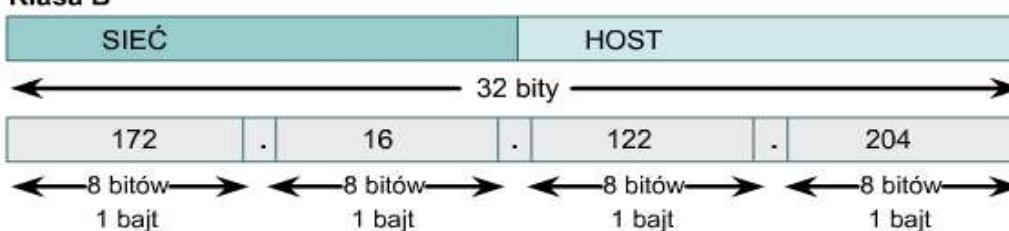
Po zamianie wyniku na postać kropkowo-dziesiętną otrzymujemy sieciową część adresu IP — 10.0.0.0 (jeśli zastosujemy maskę 255.0.0.0). Po wykonaniu boole'owskiej operacji AND na adresie IP 10.34.23.134 i masce podsieci 255.255.0.0 otrzymujemy adres sieciowy hosta: Po zamianie wyniku na postać kropkowo-dziesiętną otrzymujemy sieciową część adresu IP — 10.34.0.0 (jeśli zastosujemy maskę 255.255.0.0). Jest to krótki przykład wpływu maski sieci na adres IP.

Istotność operacji maskowania można sobie lepiej uświadomić w miarę wykonywania dalszych działań na adresach IP. W chwili obecnej ważne jest tylko zrozumienie pojęcia maski.

Klasa A



Klasa B



- Trzema warunkami nawiązania połączenia z siecią Internet są: połączenie fizyczne, połączenie logiczne i przeglądarka WWW.
- Komputery rozpoznają i przetwarzają dane, używając dwójkowego systemu liczbowego.
- Najczęściej używanym systemem liczbowym jest system dziesiętny.
- System szesnastkowy jest używany podczas pracy z komputerami, ponieważ umożliwia prezentację liczb dwójkowych w bardziej czytelnej postaci.

## **Moduł 2: Podstawy działania sieci komputerowych Wprowadzenie**

Szerokość pasma ma zasadnicze znaczenie dla działania sieci komputerowej. Decyzje dotyczące szerokości pasma są jednymi z najważniejszych, które trzeba podjąć podczas projektowania sieci. W niniejszym module omówiono znaczenie szerokości pasma, wyjaśniono sposoby jego obliczania oraz pomiaru.

Funkcje sieci są opisywane przy użyciu modeli warstwowych. W module 2 omówiono dwa najważniejsze modele, tj. model OSI (ang. *Open System Interconnection*) i model TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*).

Przedstawiono także różnice i podobieństwa między nimi.

### **2.1 Terminologia sieciowa**

#### **2.1.1 Sieci danych**

Rozwój sieci danych zawdzięczamy faktowi stosowania na mikrokomputerach aplikacji biznesowych. Z początku, mikrokomputery nie były ze sobą połączone, podobnie jak terminale komputerów klasy mainframe, nie istniała więc wygodna metoda wymiany danych między wieloma mikrokomputerami. Stało się oczywiste, że przenoszenie danych przy użyciu dyskietek (stosowanie sieci Sneakernet) nie jest ani na tyle wydajne, ani oszczędne, aby nadawało się do zastosowań w biznesie. Taki sposób przenoszenia danych sprawiał, że były one przechowywane w wielu kopiiach. Każda modyfikacja pliku pociągała za sobą konieczność jego ponownego rozpowszechnienia wśród pracowników, którym był potrzebny. W przypadku jednoczesnego zmodyfikowania pliku przez dwie osoby próba rozpowszechnienia zmian mogła powodować utratę jednego zbioru modyfikacji. Przedsiębiorstwa potrzebowały dobrego rozwiązywanie trzech następujących problemów:

Jak uniknąć powielania urządzeń i zasobów? Jak wydajnie się komunikować? Jak zbudować sieć i zarządzać nią?

Zorientowano się, że technika sieciowa może zwiększyć wydajność przy jednoczesnym obniżeniu kosztów. Prędkość wdrażania i upowszechniania się sieci zaczęła dorównywać tempu wprowadzania nowych technologii i produktów sieciowych na rynek. We wczesnych latach 80. XX w. nastąpiło masowe upowszechnienie sieci komputerowych, pomimo tego, że początkowo ich rozwój nie był zorganizowany.

W połowie lat 80. pojawiające się technologie sieciowe były tworzone na bazie różnego sprzętu i oprogramowania. Każda firma produkująca urządzenia i oprogramowanie sieciowe stosowała własne standardy. Tworzenie indywidualnych standardów wynikało z panującej na rynku konkurencji. W wyniku tego wiele technologii sieciowych było ze sobą niezgodnych. Wzajemna komunikacja sieci opartych na różnych specyfikacjach stawała się coraz bardziej trudna. Wdrożenie nowego sprzętu często powodowało konieczność wymiany starych urządzeń sieciowych.

Jednym z wczesnych rozwiązań tych problemów było utworzenie standardów sieci lokalnych LAN. Ze względu na to, że standardy LAN zawierały otwarty zbiór wytycznych dotyczących projektowania sprzętu i oprogramowania sieciowego, urządzenia produkowane przez różne firmy mogły stać się zgodne z systemami konkurencji. Pozwoliło to na ustabilizowanie się implementacji sieci LAN.

W systemie LAN każdy dział firmy jest rodzajem elektronicznej wyspy. Wraz ze wzrostem znaczenia komputerów dla przedsiębiorstw stało się jasne, że sieci LAN nie są rozwiązaniem wystarczającym.

Pojawiła się potrzeba opracowania sposobu szybkiej i wydajnej wymiany informacji nie tylko w ramach jednej firmy, ale także między przedsiębiorstwami. Rozwiązaniem stało się utworzenie sieci miejskich MAN (ang. *metropolitan-area network*) i sieci rozległych WAN (ang. *wide-area network*). Ponieważ sieci WAN pozwalały na łączenie użytkowników rozproszonych na dużych obszarach geograficznych, możliwa stała się wzajemna komunikacja na duże odległości.

#### **2.1.2 Historia sieci komputerowych**

Historia sieci komputerowych jest złożona. W rozwój sieci w ciągu ostatnich 35 lat było zaangażowanych wielu ludzi z całego świata. W tym miejscu przedstawiono skrócony opis rozwoju Internetu. Procesy tworzenia nowych rozwiązań i ich wprowadzania na rynek są daleko bardziej skomplikowane, ale spojrzenie na podstawy rozwoju jest bardzo pomocne.

W latach 40. XX w. komputery były łatwo psującymi się, ogólnymi urządzeniami elektromechanicznymi. Wynalezienie w 1947 roku tranzystora półprzewodnikowego otworzyło wiele możliwości budowania mniejszych i bardziej niezawodnych komputerów. W latach pięćdziesiątych komputery klasy mainframe, które wykonywały programy zapisane na kartach perforowanych, zaczęły być wykorzystywane przez duże instytucje. W późnych latach pięćdziesiątych wynaleziono układ scalony, który składał się z kilku, później wielu, a obecnie z milionów tranzystorów umieszczonych na małym kawałku półprzewodnika. W latach 60. komputery mainframe z terminalami nie były niczym niezwykłym i upowszechniły się układy scalone. W późnych latach 60. i w trakcie następnej dekady powstały mniejsze komputery nazywane minikomputerami.

Jednak nawet tamte minikomputery były ogromne według współczesnych standardów. W roku 1977 firma Apple Computer Company przedstawiła mikrokomputer nazywany także komputerem osobistym. W roku 1981 firma IBM zaprezentowała swój pierwszy komputer osobisty. Przyjazny użytkownikowi komputer Mac, otwarta architektura komputera IBM PC i dalsza miniaturyzacja układów scalonych doprowadziły do rozpowszechnienia się komputerów osobistych w domu i w biznesie. W połowie lat 80. XX w. użytkownicy autonomicznych komputerów zaczęli wykorzystywać modemy do łączenia się z innymi komputerami i wymiany plików. Nazywano to komunikacją punkt-punkt lub komunikacją komutowaną (dial-up). Pomysł ten rozwinięto, wykorzystując komputery jako centralne punkty komunikacji w połączeniach komutowanych. Komputery te nazywano białymi BBS (ang. *bulletin boards*). Użytkownicy mogli połączyć się z białym BBS i pozostawić tam lub pobrać stamtąd wiadomości bądź pliki. Wadą takiego systemu było to, że komunikacja bezpośrednią była ograniczona i dotyczyła tylko tych, którzy wiedzieli o danym białym BBS. Inne ograniczenie stanowił fakt, że komputer BBS wymagał jednego modemu do każdego połączenia. Tak więc jednoczesne połączenie pięciu użytkowników wymagało pięciu modemów podłączonych do pięciu odrębnych linii telefonicznych. Wraz ze wzrostem liczby osób chcących korzystać z systemu obsługiwanego wszystkimi zgłoszeniami stawało się niemożliwe. Wystarczy wyobrazić sobie sytuację, w której 500 osób chce połączyć się w tej samej chwili. W latach 60. XX w. Departament Obrony USA rozpoczął

tworzenie dużych i niezawodnych sieci WAN do celów wojskowych i naukowych. Ich rozwój był kontynuowany przez trzy następne dekady. Ta technologia różniła się od komunikacji punkt-punkt wykorzystywanej w biuletynach BBS. Umożliwiała wspólne połączenie wielu komputerów przy użyciu różnych ścieżek. Sposób przenoszenia danych między komputerami był określany przez sieć. Wprowadzono możliwość komunikacji między wieloma komputerami przy użyciu tego samego połączenia, podczas gdy wcześniej możliwa była komunikacja z zaledwie jednym komputerem w danej chwili. Sieć WAN Departamentu Obrony USA ostatecznie przekształciła się w Internet.

### 2.1.3 Urządzenia sieciowe

Urządzenia przyłączane bezpośrednio do segmentu sieci dzielą się na dwie klasy. Pierwszą klasę stanowią urządzenia końcowe. Są to komputery, drukarki, skanery i inne urządzenia, które wykonują usługi bezpośrednio dla użytkownika. Drugą klasę stanowią urządzenia sieciowe. Są to wszystkie urządzenia, które łączą urządzenia końcowe, umożliwiając komunikację między nimi.

Urządzenia końcowe, które umożliwiają użytkownikom połączenie z siecią, są również nazywane hostami. Urządzenia takie pozwalają użytkownikom na współdzielenie, tworzenie i uzyskiwanie informacji. Hosty mogą istnieć bez sieci, ale wtedy ich możliwości są znacznie ograniczone. Hosty są fizycznie przyłączone do mediów sieciowych przy użyciu karty sieciowej. Połączenie to jest wykorzystywane do wykonywania takich zadań, jak wysyłanie poczty elektronicznej, drukowanie dokumentów, skanowanie obrazów i uzyskiwanie dostępu do bazy danych. Karta sieciowa może mieć postać płytka z obwodem drukowanym, który pasuje do złącza rozszerzeń na magistrali płyty głównej komputera, może także występować w postaci urządzenia peryferyjnego. Inna nazwa karty sieciowej to adapter sieciowy. Karty sieciowe komputerów przenośnych mają zwykle rozmiar karty PCMCIA. Do każdej karty sieciowej jest przypisany unikatowy kod nazywany adresem MAC. Jest on używany do sterowania komunikacją hosta w sieci. Więcej informacji o adresie MAC zostanie przedstawionych później. Jak sama nazwa wskazuje, karta sieciowa steruje dostępem hosta do medium.

W przemyśle sieciowym nie zostały ustalone zestandardyzowane oznaczenia **urządzeń końcowych**. Przypominają one kształtem rzeczywiste urządzenia, aby można je było szybko rozpoznać.

**Urządzenia sieciowe** zapewniają transmisję danych przeznaczonych do przesłania między urządzeniami końcowymi. Urządzenia sieciowe umożliwiają rozszerzenie skali możliwych połączeń kablowych, koncentrację połączeń, konwersję formatu danych i zarządzanie przesyłem informacji. Przykładami urządzeń spełniających takie funkcje są: wtórnik, koncentratory, mosty, przełączniki i routery. Wszystkie wymienione urządzenia sieciowe będą szczegółowo opisane w dalszej części kursu. W tym miejscu zostaną one omówione w skrócie.

Wtórnik jest urządzeniem sieciowym używanym do regenerowania sygnału. Wtórnik regenerują sygnał analogowy lub cyfrowy zniekształcony przez straty transmisji powstałe w wyniku tłumienia. Wtórnik nie podejmuje decyzji odnośnie przekazywania pakietów, jak router lub most.

Koncentratory służą do koncentrowania połączeń. Innymi słowy, dzięki nim grupa hostów jest postrzegana od strony sieci jako pojedyncza jednostka. Koncentracja jest wykonywana pasywnie i nie ma żadnego innego wpływu na transmisję danych. Koncentratory aktywne nie tylko koncentrują hosty, lecz także regenerują sygnał. Mosty przekształcają formaty sieciowej transmisji danych oraz realizują podstawowe funkcje zarządzania nią. Mosty, jak sugeruje nazwa, stanowią połączenie między sieciami LAN. Nie tylko łączą one sieci LAN, ale także sprawdzają dane w celu określenia, czy powinny one zostać przesłane na drugą stronę mostu, czy też nie. Dzięki temu poszczególne części sieci funkcjonują wydajniej.

Przełączniki grup roboczych wykonują bardziej zaawansowane funkcje zarządzania przesyaniem danych. Nie tylko określają, czy informacje powinny pozostać w danej sieci LAN, czy nie, ale także mogą przesyłać dane tylko do tego połączenia, w którym są one potrzebne. Inną różnicę między mostem a przełącznikiem stanowi fakt, że przełącznik nie przekształca formatów transmisji danych.

Routery dysponują wszystkimi wymienionymi wcześniej możliwościami. Mogą one regenerować sygnały, koncentrować wiele połączeń, przekształcać formaty transmisji danych i zarządzać transferem danych. Umożliwiają również połączenie z siecią WAN, co pozwala na łączenie znacznie od siebie oddalonych sieci lokalnych. Żadne z pozostałych urządzeń nie zapewnia takiego połączenia.

Urządzenia końcowe	
Komputer PC	Drukarka
Apple Macintosh	Serwer plików
Komputer przenośny	Komputer mainframe
Urządzenia sieciowe	
Wtórnik	Most
Koncentrator 10BASE-T	Przełącznik grupy roboczej
Koncentrator (100BASE-T Hub)	Router
Koncentrator	Chmura obrazująca sieć

## 2.1.4 Topologia sieci

Topologia sieci określa jej strukturę. Jedną częścią definicji topologii jest topologia fizyczna, która stanowi rzeczywisty układ przewodów lub medium transmisyjnego. Drugą częścią jest topologia logiczna, która określa sposób dostępu hosta do medium w celu wysłania danych. Powszechnie stosowane są następujące odmiany topologii fizycznej:

**Topologia magistrali**, w której wykorzystywany jest pojedynczy kabel szkieletowy na obu końcach wyposażony w terminatory. Wszystkie hosty są podłączone bezpośrednio do tego szkieletu.

**Topologia pierścienia**, w której każdy host jest podłączony do następnego, a ostatni host jest podłączony do pierwszego. W ten sposób tworzony jest pierścień okablowania.

**Topologia gwiazdy**, w której wszystkie kable łączą się w jednym punkcie centralnym.

**Topologia gwiazdy rozszerzonej**, w której pojedyncze gwiazdy są powiązane poprzez połączenie koncentratorów lub przełączników. Ta topologia umożliwia rozszerzenie zasięgu i obszaru sieci.

**Topologia hierarchiczna** jest podobna do rozszerzonej gwiazdy. Jednak zamiast łączyć razem koncentratory lub przełączniki, system jest podłączony do komputera, który steruje ruchem w tej topologii.

**Topologia siatki** w możliwie największym stopniu zabezpiecza przed przerwami w dostępie do usług. Świetnym przykładem może być zastosowanie topologii siatki w sieciowym systemie sterowania elektrownią atomową. Jak widać na rysunku, każdy host dysponuje połączeniami z wszystkimi innymi hostami. Chociaż w Internecie istnieje wiele ścieżek do każdego miejsca, nie mamy w nim do czynienia z pełną topologią siatki.

**Topologia logiczna** sieci to sposób, w jaki hosty komunikują się ze sobą za pośrednictwem medium. Dwie najpowszechniejsze topologie logiczne to rozgłaszanie i przekazywanie tokenu.

**Topologia rozgłaszania** oznacza po prostu, że każdy host wysyła przekazywane dane do wszystkich hostów podłączonych do medium sieciowego. Nie ma określonej kolejności korzystania z sieci przez poszczególne stacje. Host, który jako pierwszy wyśle dane, jest obsługiwany jako pierwszy (ang. *first come, first serve*). W ten sposób działa sieć Ethernet, co zostanie omówione w dalszej części kursu.

Drugą odmianą topologii logicznej jest przekazywanie tokenu. W tej topologii dostęp do sieci jest kontrolowany przez przekazywanie elektronicznego tokenu kolejno do każdego hosta. Gdy host odbierze token, może wysyłać dane przez sieć. Jeśli nie ma danych do wysłania, przekazuje token do następnego hosta i proces się powtarza. Przykładami sieci, w których jest wykorzystywane przekazywanie tokenu, są Token Ring i FDDI. Odmianą sieci Token Ring i FDDI jest sieć Arcnet. W sieci Arcnet token jest przekazywany w ramach topologii magistrali.

Diagram na rysunku przedstawia wiele różnych topologii w połączeniu z urządzeniami sieciowymi. Prezentuje on typową dla szkoły lub małej firmy sieć o średnim stopniu złożoności. Znajduje się na nim wiele symboli i wiele rozwiązań sieciowych, których poznanie będzie wymagało czasu.

## 2.1.5 Protokoły sieciowe

Zestawy protokołów są to zbiory protokołów, które umożliwiają sieciową komunikację między hostami. Protokół jest formalnym opisem zestawu reguł i konwencji regulujących szczególny aspekt komunikacji między urządzeniami w sieci. Protokoły określają format informacji, zależności czasowe, kolejność transmisji i sposób wykrywania oraz reagowania na błędy występujące podczas komunikacji. Bez znajomości protokołów komputer nie mógłby przywrócić początkowej postaci strumienia bitów przychodzących z innego komputera.

Protokoły regulują wszystkie aspekty komunikacji danych. Należą do nich:

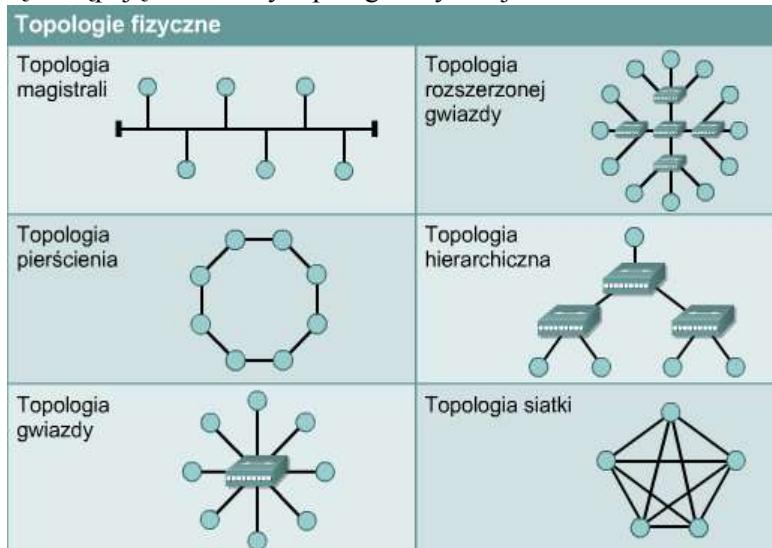
- budowa sieci fizycznej,
- sposoby łączenia komputerów z siecią,
- sposoby formatowania danych do transmisji,
- sposoby wysyłania danych,
- sposoby obsługi błędów.

Reguły funkcjonowania sieci są opracowywane i nadzorowane przez wiele różnych organizacji i komitetów. Należą do nich: Institute of Electrical and Electronic Engineers (IEEE), American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA) i International Telecommunications Union (ITU), dawniej znana pod nazwą Comité Consultatif International Téléphonique et Télégraphique (CCITT).

## 2.1.6 Sieci LAN

składają się z następujących elementów:

- komputery,
- urządzenia peryferyjne,
- urządzenia sieciowe.
- karty sieciowe,
- media sieciowe,



Sieci LAN umożliwiają efektywne wykorzystanie technologii komputerowych w biznesie do lokalnego współdzielenia plików i zapewnienia wewnętrznej komunikacji. Dobrym przykładem takiego rozwiązania jest poczta elektroniczna. Sieci LAN wiążą razem dane, lokalną komunikację i urządzenia komputerowe. Najpowszechniej stosowanymi technologiami sieci LAN są:

Ethernet                  Token  
RingFDDI

### 2.1.7 Sieci WAN

Sieci WAN łączą sieci LAN, co umożliwia dostęp do komputerów lub serwerów plików znajdujących się w innych miejscach. Ze względu na to, że sieci WAN łączą sieci na dużych obszarach geograficznych, umożliwiają komunikację między firmami na duże odległości. Sieci WAN umożliwiają współdzielenie komputerów, drukarek i innych urządzeń znajdujących się w sieci LAN z maszynami znajdującymi się w odległych miejscach. Pozwalają one na szybką komunikację na dużych obszarach geograficznych. Oprogramowanie do pracy zespołowej umożliwia dostęp do informacji i zasobów w czasie rzeczywistym, co pozwala na zdalne uczestnictwo w spotkaniach, które

wcześniej wymagały fizycznej obecności uczestników. Sieci rozległe spowodowały powstanie nowej klasy pracowników zwanych telepracownikami, którzy nie muszą wychodzić z domu, aby wykonywać swą pracę.

Zadania sieci WAN prezentują się następująco:

- działanie na dużych, odległych geograficznie obszarach;
- umożliwienie użytkownikom komunikacji w czasie rzeczywistym;
- udostępnienie stałego połączenia zdalnych zasobów i lokalnych usług; dostęp do poczty elektronicznej, sieci WWW, usług przesyłania plików i handlu elektronicznego.

Najpowszechniej stosowanymi technologiami WAN są:

sieci komutowane  
sieci ISDN (ang. *Integrated Services Digital Network*)  
linie DSL (ang. *Digital Subscriber Line*)  
sieci Frame Relay  
sieci Carrier Series w USA (T) i w Europie (E): sieci T1, E1, T3 i E3  
sieci SONET (ang. *Synchronous Optical Network*)

### 2.1.8 Sieci MAN

Sieć MAN obejmuje swoim zasięgiem obszar miejski, taki jak centrum miasta lub przedmieście. Sieć MAN zwykle składa się z dwóch lub więcej sieci LAN znajdujących się na wspólnym obszarze geograficznym. Sieć MAN może być na przykład wykorzystywana przez bank mający kilka oddziałów. Zwykle dostawca usług łączy dwie lub więcej sieci LAN przy użyciu własnych linii komunikacyjnych lub usług światłowodowych. Sieć MAN można także utworzyć przy użyciu bezprzewodowych mostów, przesyłając sygnały przez obszary publiczne.

### 2.1.9 Sieci SAN

Sieć SAN jest wydzieloną, wysoko wydajną siecią używaną do przenoszenia danych między serwerami i zasobami służącymi do przechowywania informacji. Ponieważ jest to odrębna, wydzielona sieć, nie występują w jej przypadku kolizje w ruchu między serwerami i klientami.

Technika SAN umożliwia szybką łączność serwer-pamięć, pamięć-pamięć i serwer-serwer. Metoda ta polega na wykorzystaniu odrębnej infrastruktury sieci, co wyklucza problemy związane z łącznością w istniejącej sieci. Sieci SAN mają następujące cechy:

**Wydajność:** Sieci SAN umożliwiają współbieżny szybki dostęp dwóch lub więcej serwerów do macierzy dyskowych lub taśmowych, zapewniając większą wydajność systemu.

**Dostępność:** Sieci SAN mają wbudowaną odporność na awarie, ponieważ pozwalają na utworzenie lustrzanej kopii danych przy użyciu sieci SAN w odległości do 10 km.

#### Sieci LAN:

- Działają na ograniczonym obszarze geograficznym.
- Umożliwiają jednoczesny dostęp wielu urządzeń do medium o dużej szerokości pasma.
- Pozwalają na lokalne administrowanie siecią.
- Zapewniają stały dostęp do lokalnych usług.
- Zapewniają połączenie fizyczne sąsiadujących urządzeń.

#### Wykorzystanie:



#### Sieci WAN:

- Działają na dużych obszarach geograficznych.
- Umożliwiają dostęp przez relatywnie wolne interfejsy szeregowe.
- Zapewniają łączność w pełnym lub ograniczonym wymiarze czasowym.
- Łączą urządzenia znacznie od siebie oddalone, które mogą się znajdować w różnych częściach globu.

#### Wykorzystanie:



**Skalowalność:** Jak w przypadku sieci LAN i WAN, tak i tu można korzystać z różnych technologii sieciowych. Pozwala to na łatwe przenoszenie kopii zapasowych i plików, realizowanie różnych operacji i replikację danych między systemami.

## 2.1.10 Sieć VPN

Sieć VPN to prywatna sieć utworzona w ramach infrastruktury sieci publicznej, takiej jak światowa sieć Internet. Przy użyciu sieci VPN telepracownik może za pośrednictwem Internetu uzyskać dostęp do sieci komputerowej znajdującej się w centrali firmy, tworząc zabezpieczony tunel między własnym komputerem a routerem VPN w siedzibie firmy

## 2.1.11 Zalety sieci VPN

Produkty firmy Cisco obsługują najnowsze rozwiązania z zakresu technologii VPN. Sieć VPN jest usługą, która zapewnia bezpieczną i niezawodną komunikację poprzez wspólną sieć publiczną, taką jak Internet. Reguły zabezpieczeń i zarządzania w sieciach VPN są takie same jak w sieci prywatnej. Sieci te są najbardziej wydajną metodą nawiązywania połączeń punkt-punkt między zdalnymi użytkownikami i siecią klienta firmy.

Wyróżnia się trzy główne typy sieci VPN:

**Dostępowe sieci VPN:** Dostępowe sieci VPN zapewniają łączność zdalnych pracowników i małych biur z centralą intranetu lub ekstranetu za pośrednictwem wspólnej infrastruktury. W przypadku dostępowych sieci VPN do bezpiecznej komunikacji przemieszczających się pracowników, telepracowników i biur terenowych używane są techniki analogowe, komutowane, ISDN, DSL, mobile IP i kablowe.

**Intranetowe sieci VPN:** Intranetowe sieci VPN łączą regionalne i zdalne biura z centralą sieci wewnętrznej za pośrednictwem wspólnej infrastruktury korzystającej z dedykowanych połączeń. Intranetowe sieci VPN różnią się od ekstranetowych sieci VPN tym, że umożliwiają dostęp tylko pracownikom danej firmy.

**Ekstranetowe sieci VPN:** Ekstranetowe sieci VPN łączą partnerów firmy z centralą sieci za pośrednictwem wspólnej infrastruktury korzystającej z dedykowanych połączeń. Ekstranetowe sieci VPN różnią się od intranetowych sieci VPN tym, że umożliwiają dostęp użytkownikom spoza firmy

## 2.1.12 Intranety i ekstranety

Jedną z powszechnie stosowanych konfiguracji sieci LAN jest Intranet. Intranetowe serwery WWW różnią się tym od publicznych serwerów WWW, że aby uzyskać dostęp z zewnątrz do Intranetu danej organizacji trzeba mieć odpowiednie uprawnienia i hasła. Intranety są projektowane w taki sposób, aby umożliwiały dostęp tym użytkownikom, którzy mają uprawnienia dostępu do wewnętrznej sieci LAN firmy. W intrancie są instalowane serwery WWW. Przeglądarki są wykorzystywane jako wspólny mechanizm dostępu (fronton) do informacji przechowywanych na tych serwerach, takich jak dane lub wykresy finansowe bądź dane tekstowe.

Terminem „ekstranet” określa się aplikacje i usługi oparte na intrancie i korzystające z rozszerzonego, zabezpieczonego dostępu do zewnętrznych użytkowników lub firm. Dostęp ten zwykle uzyskuje się przy użyciu haseł, identyfikatorów i innych zabezpieczeń na poziomie aplikacji. Tak więc ekstranet jest rozszerzeniem dwóch lub kilku intranetów z zapewnieniem bezpiecznej interakcji między współpracującymi firmami i ich intranetami

## 2.2 Przepustowość

### 2.2.1 Znaczenie szerokości pasma

Szerokość pasma jest zdefiniowana jako ilość informacji, które można przesłać siecią w określonym czasie. Zrozumienie istoty szerokości pasma podczas poznawania zagadnień sieciowych jest bardzo ważne z następujących powodów:

**Szerokość pasma jest skończona.** Innymi słowy, niezależnie od medium użytego do budowy sieci ilość informacji przenoszonych przez tę sieć jest ograniczona. Szerokość pasma jest ograniczona prawami fizyki i technologiami umieszczania informacji w medium. Szerokość pasma zwykłego modemu jest na przykład ograniczona do około 56 kb/s przez fizyczne właściwości skrętki telefonicznej i technologię modemu. Ta sama skrętka telefoniczna jest wykorzystywana przez urządzenia technologii DSL, która zapewnia znacznie większą szerokość pasma. Czasami nawet ograniczenia wynikające z praw fizyki trudno jest opisać.

Światłowód daje fizyczną możliwość uzyskania praktycznie nieograniczonej szerokości pasma. Pomimo tego nie jesteśmy w stanie w pełni wykorzystać możliwości światłowodu, ponieważ technologie, które pozwoliłyby na wykorzystanie całego jego potencjału, nie zostały jeszcze opracowane.

**Im większa szerokość pasma, tym większy koszt.** Można kupić sprzęt dla sieci LAN, który zapewni niemal nieograniczoną szerokość pasma przez długi czas. W przypadku połączeń WAN prawie zawsze trzeba kupić szerokość pasma od dostawcy usług. W obu przypadkach zrozumienie, czym jest szerokość pasma i skąd biorą się zmiany zapotrzebowania na szerokość pasma w danej chwili, może pozwolić danej osobie lub firmie na znaczące oszczędności. Menedżer sieci musi podejmować właściwe decyzje dotyczące tego, które urządzenia i usługi zakupić.

**Szerokość pasma ma kluczowe znaczenie dla analizy wydajności sieci, projektowania nowych sieci i zrozumienia zasad działania Internetu.** Osoba zawodowo zajmująca się sieciami komputerowymi musi rozumieć ogromny wpływ, jaki na wydajność i projekt sieci ma przepustowość i szerokość pasma. Informacje są przesyłane między komputerami na całym świecie jako ciągi bitów. Bity te reprezentują ogromne ilości

informacji przepływających przez kulę ziemską w ciągu pojedynczych sekund lub jeszcze szybciej. W pewnym sensie można powiedzieć, że Internet to pasmo.

**Popyt na szerokość pasma nieustannie rośnie.** Wraz z powstaniem technologii i infrastruktur sieciowych zapewniających szersze pasmo tworzone są aplikacje korzystające z tych możliwości. Przesyłanie siecią bogatych treści medialnych, w tym strumieni wideo i audio, wymaga bardzo szerokiego pasma. Zamiast tradycyjnych systemów głosowych instaluje się obecnie często systemy telefonii IP, co dodatkowo zwiększa zapotrzebowanie na szerokość pasma. Dla specjalistów w dziedzinie sieci komputerowych kluczem do sukcesu jest przewidywanie zwiększającego się zapotrzebowania na szerokość pasma i podejmowanie zgodnych z tą tendencją działań.

## 2.2.2 Pulpit

Szerokość pasma jest zdefiniowana jako ilość informacji, które można przesyłać siecią w określonym czasie. Idea przepływu informacji sugeruje dwie analogie, które ułatwiają zobrazowanie szerokości pasma sieci. Ponieważ pojęcie przepływu opisuje zarówno wodę, jak i ruch uliczny, należy rozważyć następujące analogie:

**Szerokość pasma jest jak liczba pasm autostrady.**

Sieć dróg funkcjonuje w każdym dużym mieście lub miejscowości.

Ogromne wielopasmowe autostrady są połączone mniejszymi drogami o mniejszej liczbie pasm. Drogi te prowadzą do jeszcze mniejszych, węższych dróg, które w końcu łączą się z dojazdami do domów i firm. Gdy systemem dróg porusza się mało samochodów, każdy pojazd może jechać bez ograniczeń prędkości. Gdy ruch jest większy, pojazdy poruszają się wolniej. Dzieje się tak szczególnie na drogach o mniejszej liczbie pasm dla samochodów. Gdy natężenie ruchu w systemie dróg zwiększy się jeszcze bardziej, nawet wielopasmowe

autostrady staną się zatłoczone i powolne. Sieć danych bardzo przypomina system dróg. Pakiety danych można porównać do pojazdów, a szerokość pasma do liczby pasm autostrady. Gdy na sieć danych patrzy się jak na sieć dróg, można łatwo zaobserwować, w jaki sposób połączenia o wąskim paśmie powodują przeciążenia ruchu w całej sieci.

## 2.2.3 Pomiary

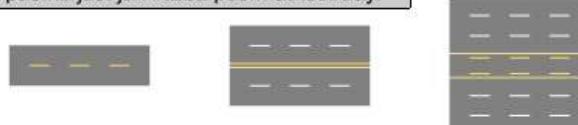
W systemach cyfrowych podstawową jednostką szerokości pasma są bity na sekundę (b/s). Szerokość pasma jest miarą tego, jaka ilość informacji lub bitów może przepływać z jednego miejsca do innego w danym czasie. Chociaż szerokość pasma można określić w bitach na sekundę, zwykle używana jest wielokrotność tej jednostki. Innymi słowy, pasmo

sieciowe jest zwykle opisane przy użyciu tysięcy bitów na sekundę (kb/s), milionów bitów na sekundę (Mb/s), miliardów bitów na sekundę (Gb/s) i bilionów bitów na sekundę (Tb/s). Chociaż pojęcia szerokości pasma i szybkości są często używane zamiennie, nie oznaczają one tego samego. Ktoś może na przykład powiedzieć, że połączenie T3 o paśmie 45 Mb/s działa szybciej niż połączenie T1 o paśmie 1,544 Mb/s. Jeśli jednak wykorzystywana jest tylko niewielka część ich możliwości, oba typy połączeń będą przesyłały dane z mniej więcej tą samą szybkością. Na przykład, niewielka ilość wody będzie przepływać z tą samą szybkością zarówno przez rurę o dużej, jak i o malej średnicy. A więc bardziej scisłe jest stwierdzenie, że połączenie T3 ma szersze pasmo niż połączenie T1. Jest to spowodowane tym, że połączenie T3 może przenieść więcej informacji w tym samym czasie, a nie tym, że jest szybsze.

## 2.2.4 Ograniczenia

Szerokość pasma zależy od typu użytego medium oraz od użytej technologii sieci LAN lub WAN. Niektóre różnice wynikają z fizycznych właściwości medium. Sygnały są przesyłane miedzianą skrętką, kablem koncentrycznym, światłowodem lub za pomocą łączą bezprzewodowego. Fizyczne różnice w sposobie przesyłania sygnału są źródłem

Szerokość pasma jest jak liczba pasm autostrady.



Urządzenia sieciowe można porównać do bramek, sygnalizacji świetlnej, znaków i map.



Pakiety są jak samochody.



Jednostka szerokości pasma	Skrót	Odpowiednik
Bity na sekundę	bps	1 b/s = podstawowa jednostka szerokości pasma
Kilobity na sekundę	kbps	1 kbps = 1,000 bps = $10^3$ bps
Megabity na sekundę	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabity na sekundę	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
Terabity na sekundę	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

podstawowych ograniczeń przepustowości danego medium. Rzeczywista szerokość pasma sieci jest jednak zależna od dwóch czynników: rodzaju medium fizycznego oraz technologii służących do sygnalizacji i wykrywania sygnałów sieciowych. Na przykład aktualna wiedza dotycząca fizycznych właściwości miedzianej skrętki nieekranowanej (UTP) wyznacza teoretyczną granicę szerokości pasma równą jednemu gigabitowi na sekundę (Gb/s). Jednak w praktyce szerokość pasma zależy od tego, czy zostanie użyta sieć Ethernet typu 10BASE-T, 100BASE-TX czy 1000BASE-TX. Innymi słowy, rzeczywiste szerokość pasma jest określana poprzez wybrane metody sygnalizacji, rodzaje kart sieciowych i inne elementy sieci. Szerokość pasma nie wynika więc wyłącznie z ograniczeń medium.

## 2.2.5 Przepustowość

Szerokość pasma jest miarą ilości informacji, które można przesyłać siecią w danym czasie. Z tego powodu szerokość dostępnego pasma jest jednym z najważniejszych elementów specyfikacji sieci komputerowej. Typowa sieć LAN może być tak skonstruowana, aby zapewniała pasmo 100 Mb/s dla każdej stacji roboczej, ale to nie znaczy, że dowolny użytkownik będzie mógł w rzeczywistości przesyłać siecią sto megabitów danych w każdej sekundzie korzystania z niej. Byłoby to możliwe tylko w warunkach idealnych. Pojęcie przepustowości może pomóc w wyjaśnieniu powodu takiego stanu rzeczy. Przepustowość oznacza rzeczywistą szerokość pasma zmierzona o określonej porze dnia, przy użyciu określonych tras internetowych i podczas transmisji siecią określonych zbiorów danych. Niestety z wielu powodów przepustowość jest często znacznie mniejsza niż maksymalna możliwa szerokość pasma cyfrowego używanego medium. Niektórymi spośród czynników mających wpływ na przepustowość są:

- urządzenia intersieciowe
- typ przesyłanych danych
- topologia sieci
- liczba użytkowników sieci
- komputer użytkownika
- komputer pracujący jako serwer
- warunki zasilania

Teoretyczna szerokość pasma jest ważnym czynnikiem podczas projektowania sieci, ponieważ nigdy nie przekroczy ona wartości granicznych związanych z wyborem medium i technologii sieciowych. Jednak równie ważne dla projektanta sieci i administratora jest wzięcie pod uwagę czynników, które mogą wpływać na rzeczywistą przepustowość. Dzięki okresowym pomiarom przepustowości administrator sieci będzie miał świadomość zmian wydajności sieci i potrzeb jej użytkowników. Sieć można dzięki temu dostosowywać do aktualnych wymagań.

## 2.2.6 Obliczanie parametrów przesyłania danych

Projektanci i administratorzy sieci muszą często podejmować decyzje dotyczące szerokości pasma. Przykładem takiej decyzji może być podwyższenie parametrów połączenia WAN w celu obsługi ruchu związanego z nową bazą danych. Inna decyzja może być związana z okresem, czy aktualna sieć szkieletowa LAN ma szerokość pasma wystarczającą dla szkoleniowego programu video. Odpowiedzi na takie pytania nie zawsze są łatwe, ale analizę należy zacząć od prostego obliczenia parametrów przesyłania danych. Korzystając ze wzoru: czas przesyłania = rozmiar pliku / szerokość pasma (C=R/P), administrator sieci może oszacować kilka ważnych elementów składowych wydajności sieci. Jeśli typowy rozmiar pliku dla danej aplikacji jest znany, podzielenie tej wartości przez szerokość pasma sieci daje dobre przybliżenie najkrótszego czasu przesyłania takiego pliku. Wykonując takie obliczenia, należy wziąć pod uwagę dwie sprawy.

- Wynik jest tylko przybliżeniem, ponieważ rozmiar pliku nie obejmuje dodatkowych danych dołączonych podczas enkapsulacji.
- Wynik będzie najprawdopodobniej dotyczyć najbardziej korzystnego przypadku, ponieważ dostępna szerokość pasma najczęściej nie jest równa maksymalnej szerokości pasma dla sieci danego typu.

Dokładniejsze oszacowanie można otrzymać, podstawiając we wzorze przepustowość w miejsce szerokości pasma. Chociaż obliczenie transferu danych jest całkiem proste, należy zwrócić uwagę na to, by w równaniu posługiwać się tymi samymi jednostkami. Innymi słowy, jeśli szerokość pasma jest mierzona w megabitach na sekundę (Mb/s), rozmiar pliku należy podać w megabitach (Mb), a nie w megabajtach (MB). Ponieważ rozmiary plików są zwykle podawane w megabajtach, może być konieczne przemnożenie liczby megabajtów przez osiem, aby przekształcić je w megabit.

Najlepszy czas pobierania $T = \frac{S}{BW}$	Typowy czas pobierania $T = \frac{S}{P}$	BW	Maksymalna teoretyczna szerokość pasma najwolniejszego łącza między hostem źródłowym i docelowym (mierzona w bitach na sekundę)
P	Rzeczywista przepustowość w momencie przesyłania (mierzona w bitach na sekundę)		
T	Czas przesyłania pliku (mierzony w sekundach)		
S	Rozmiar pliku w bitach		

## 2.2.7 Transmisja cyfrowa a analogowa

Sygnały radiowe, telewizyjne i telefoniczne były do niedawna przesyłane drogą radiową oraz za pomocą transmisji przewodowej przy użyciu fal elektromagnetycznych. Fale te są nazywane analogowymi, ponieważ mają taki sam kształt jak fale świetlne i dźwiękowe wytwarzane przez nadajniki. Sygnał elektryczny przenoszący informacje zmienia się proporcjonalnie do zmian natężenia i kształtu transmitowanych fal świetlnych i dźwiękowych. Innymi słowy, fale elektromagnetyczne są analogią fal świetlnych i dźwiękowych.

Pasmo analogowe jest mierzone poprzez określenie, jaką część widma elektromagnetycznego zajmuje każdy sygnał. Podstawową jednostką pasma analogowego jest herc (Hz) lub liczba cykli na sekundę. Najczęściej używane są

wielokrotności jednostki podstawowej, jak dzieje się to w przypadku pasma cyfrowego. Powszechnie używanymi jednostkami są: kiloherc (kHz), megaherc (MHz) i gigaherc (GHz). Są to jednostki używane do opisania częstotliwości telefonów bezprzewodowych, które zwykle działają w zakresie 900 MHz lub 2,4 GHz. Są to także jednostki używane do opisu częstotliwości sieci bezprzewodowych 802.11a i 802.11b, wynoszących odpowiednio 5 GHz i 2,4 GHz.

Chociaż sygnały analogowe mogą przenosić zróżnicowane informacje, mają one pewne znaczące wady w porównaniu z transmisją cyfrową. Analogowego sygnału wideo, którego transmisja wymaga szerokiego zakresu częstotliwości, nie można przesyłać w węższym paśmie. Z tego powodu, jeśli wymagane pasmo analogowe nie jest dostępne, sygnału nie można wysłać. W przypadku sygnału cyfrowego wszystkie dane są przesyłane w postaci bitów niezależnie od rodzaju informacji.

Głos, sygnał wideo i dane przygotowane do transmisji w medium cyfrowym stają się strumieniami bitów. Taki sposób transmisji zapewnia istotną przewagę pasma cyfrowego nad analogowym. Kanałem cyfrowym o najwęższym nawet paśmie można przesyłać nieograniczone ilości informacji. Niezależnie od tego, ile czasu trwa przesyłanie informacji cyfrowej do miejsca docelowego i jej ponowne złożenie, może ona zostać wyświetlona, odsłuchana, odczytana lub przetworzona w oryginalnej postaci.

Zrozumienie różnic i podobieństw między pasmem cyfrowym i analogowym jest bardzo ważne. Oba typy pasm bardzo często występują w dziedzinie technik informacyjnych. Ponieważ jednak ten kurs dotyczy głównie cyfrowych sieci komputerowych, termin „pasmo” będzie odnosił się do pasma cyfrowego.

## 2.3 Modele działania sieci komputerowych

### 2.3.1 Używanie warstw do analizy problemów związanych z przepływem informacji

W celu opisania komunikacji między komputerami stosuje się koncepcję warstw. Na rysunku (obok) przedstawiono zbiór zagadnień związanych z przepływem, który jest zdefiniowany jako ruch fizycznych lub logicznych obiektów w systemie. Zagadnienia te ilustrują, w jaki sposób koncepcja warstw pomaga w opisie szczegółów procesu przepływu. Proces ten może być przepływem dowolnego rodzaju, od ruchu ulicznego w systemie dróg do przepływu danych w sieci komputerowej.

Rozmowa między dwiema osobami jest dobrą okazją do przedstawienia podejścia warstwowego w celu analizy przepływu informacji. Podczas rozmowy każda osoba, która chce coś powiedzieć, rozpoczyna od stworzenia myśli. Następnie podejmowana jest decyzja, w jaki sposób prawidłowo tę myśl przekazać. Można na przykład mówić, śpiewać lub krzyczeć oraz użyć określonego języka. W końcu myśl jest przekazywana. Osoba wydaje dźwięk, który przenosi wiadomość. Proces ten można podzielić na kilka odrębnych warstw, które mają zastosowanie do wszystkich rozmów. Góra warstwa jest myślą, która będzie przekazywana. Warstwa środkowa to decyzja dotycząca sposobu przekazania myśli.

Warstwa najniższa odpowiada za wytworzenie dźwięku, który przenosi informację. Ta sama metoda dzielenia na warstwy wyjaśnia, w jaki sposób sieć komputerowa przekazuje informacje od źródła do miejsca docelowego. Gdy komputery wysyłają informacje poprzez sieć, cała komunikacja rozpoczyna się u źródła, a kończy w miejscu docelowym. Informacje przenoszone w sieci są zwykle nazywane danymi lub pakietami. Pakiet jest logiczną grupą informacji, która przemieszcza się między systemami komputerowymi. Gdy dane są przekazywane między warstwami, każda warstwa dodaje do nich informacje, które umożliwiają efektywną komunikację z odpowiadającą jej warstwą na drugim komputerze. Sposób przesyłania danych między komputerami można wyjaśnić przy użyciu warstw modeli OSI i TCP/IP. Modele te różnią się liczbą i funkcjami warstw. Mimo to, każdego z nich można użyć do opisu i przedstawienia szczegółów przepływu informacji od źródła do celu.

### 2.3.2 Wykorzystanie warstw do opisu komunikacji danych

Aby możliwe było przesyłanie pakietów danych z miejsca źródłowego do docelowego, wszystkie urządzenia w sieci muszą używać tego samego języka lub protokołu. Protokół jest zestawem reguł, które komunikację w sieci czynią bardziej efektywną. Na przykład podczas lotu samolotem piloci stosują się do specjalnych zasad komunikacji z innymi samolotami i kontrolą lotów.

Protokół komunikacji danych jest zestawem reguł lub umową, która określa format i zasady transmisji danych.

Warstwa 4 w komputerze źródłowym komunikuje się z warstwą 4 w komputerze docelowym. Reguły i konwencje używane w tej warstwie są nazywane protokołami warstwy 4. Należy pamiętać o tym, że protokoły przygotowują dane liniowo.

Szerokość pasma (cyfrowego) jest podobna do szerokości pasma analogowego.



Urządzenia sieciowe są jak telefony, radioodbiorniki AM/FM i odtwarzacze płyt CD.



Pakietów są jak muzyka.



Protokół w jednej warstwie, przygotowując dane do przesłania siecią, wykonuje na danych pewien zestaw operacji. Dane te są następnie przekazywane do kolejnej warstwy, w której następny protokół wykonuje inny zestaw operacji. Gdy pakiet dotrze do miejsca docelowego, protokoły dokonują dekonstrukcji pakietu, który został zbudowany po stronie źródłowej. Wykonywane jest to w odwrotnej kolejności. Protokoły każdej warstwy w komputerze docelowym przywracają oryginalną postać informacji, aby aplikacja mogła je we właściwy sposób odczytać.

### 2.3.3 Model OSI

Wczesny rozwój sieci komputerowych był pod wieloma względami niezorganizowany. We wczesnych latach 80. XX w. nastąpił ogromny wzrost liczby i rozmiarów sieci. Gdy tylko w firmach zdano sobie sprawę z korzyści wynikających ze stosowania technologii sieciowych, prędkość wdrażania i rozpowszechniania się sieci dorównała tempu wprowadzania nowych technologii i produktów sieciowych na rynek. W połowie lat 80. w firmy zaczęły odczuwać problemy wynikające z tak gwałtownego rozwoju. Podobnie jak dzieje się to w przypadku ludzi, którzy mają problemy z porozumiewaniem się, ponieważ nie mówią tym samym językiem, w sieciach komputerowych zbudowanych na podstawie różnych specyfikacji i implementacji wystąpiły problemy z wymianą informacji. Te same problemy dotyczyły firm, które rozwijały prywatne lub zastrzeżone technologie sieciowe. Słowo „zastrzeżone” oznacza, że tylko jedna firma lub grupa firm miały kontrolę nad wykorzystaniem określonej technologii. Wzajemna komunikacja systemów opartych na ścisłej realizacji własnych, zastrzeżonych zasad nie była możliwa. W celu rozwiązywania problemu niezgodności sieci organizacja ISO (ang. International Organization for Standardization) zbadała modele sieciowe, takie jak DECnet (ang. Digital Equipment Corporation net), SNA (ang. Systems Network Architecture) i TCP/IP, aby określić możliwy do ogólnego zastosowania zestaw zasad dla wszystkich sieci. Wykorzystując te badania, organizacja ISO utworzyła model sieciowy, który umożliwił producentom wytwarzanie wzajemnie zgodnych sieci. Model odniesienia OSI (ang. Open System Interconnection) wydany w roku 1984 był opisowym modelem sieci, który powstał w organizacji ISO. Zawierał on zestaw standardów przeznaczonych dla producentów, które zapewniły większą zgodność i możliwość współdziałania różnych technologii sieciowych wytwarzanych przez firmy na całym świecie. Model odniesienia OSI stał się głównym modelem komunikacji sieciowej. Chociaż istnieją inne modele, większość producentów sieci wykorzystuje w swoich produktach model odniesienia OSI. Dzieje się tak szczególnie w przypadku szkolenia użytkowników ich produktów. Model ten jest uważany za najlepsze dostępne narzędzie służące do nauczania zagadnień związanych z wysyłaniem i odbieraniem danych w sieci.

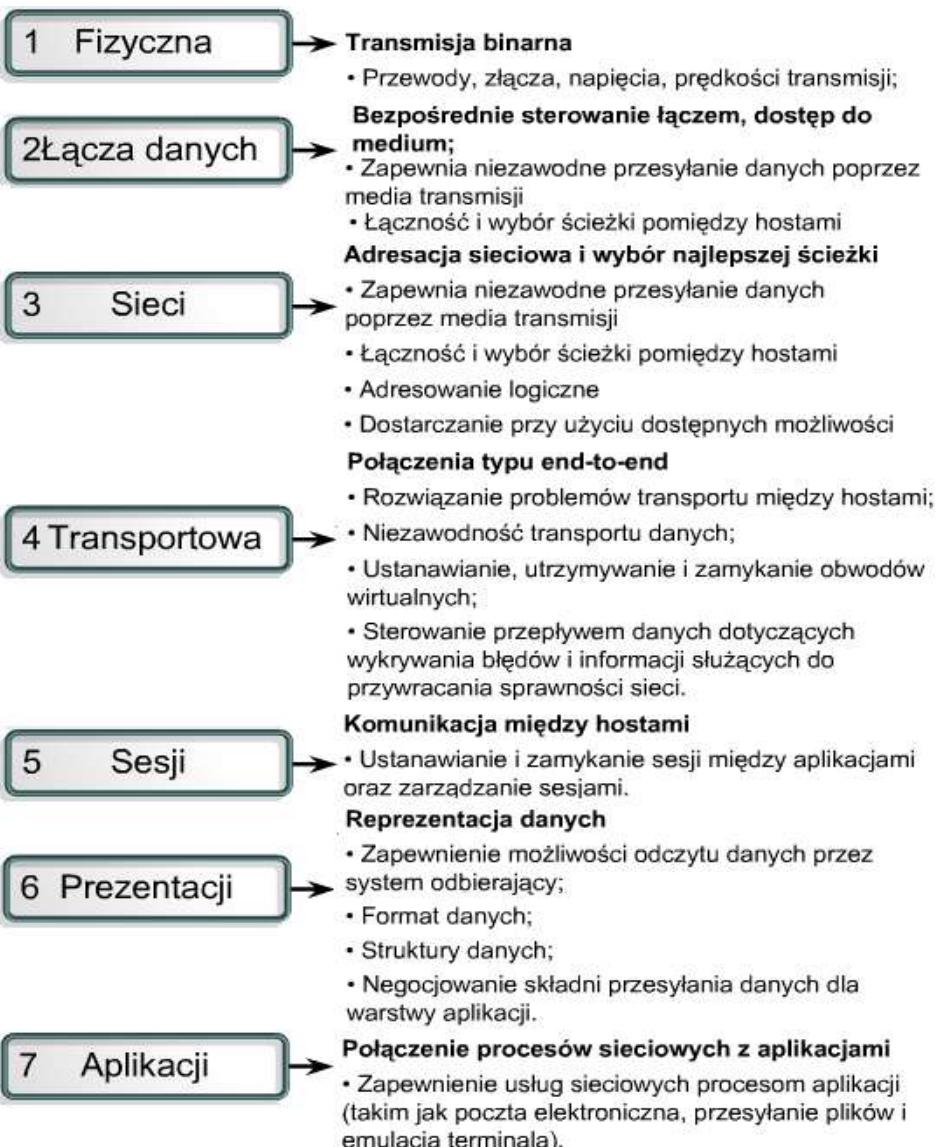
### 2.3.4 Warstwy OSI

Model odniesienia OSI jest szkieletem używanym do poznania mechanizmów przesyłania informacji w sieci. Przy użyciu tego modelu można wyjaśnić, w jaki sposób pakiet przechodzi przez różne warstwy do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca dysponują różnymi typami medium sieciowego. W modelu odniesienia OSI jest siedem warstw, z których każda dotyczy pewnej funkcji sieci. – Podział sieci na warstwy przynosi następujące korzyści:

dzieli proces komunikacji sieciowej na mniejsze, łatwiejsze do zarządzania elementy składowe; tworzy standardy składników sieci, dzięki czemu składniki te mogą być rozwijane i obsługiwane przez różnych producentów; umożliwia wzajemną komunikację sprzętu i oprogramowania sieciowego różnych rodzajów; zmiany wprowadzone w jednej warstwie nie dotyczą innych warstw; dzieli proces komunikacji sieciowej na mniejsze składowe, co pozwala na łatwiejsze jego zrozumienie.

#### Korzyści ze stosowania modelu OSI:

- Mniejsza złożoność
- Ustandaryzowanie interfejsów
- Projektowanie modułowe
- Zapewnienie współdziałania technologii
- Przyspieszony rozwój
- Uproszczenie procesu nauczania



### **2.3.5 Komunikacja węzłów równorzędnych**

Aby dane mogły zostać przesłane ze źródła do miejsca docelowego, każda warstwa modelu OSI w miejscu źródłowym musi porozumieć się z równorzędną jej warstwą w miejscu docelowym. Taka forma komunikacji jest nazywana komunikacją równorzędną (ang. *peer-to-peer*). Podczas tego procesu protokoły każdej warstwy wymieniają informacje nazywane jednostkami danych protokołu (ang. *protocol data unit, PDU*). Każda warstwa komunikacyjna w komputerze źródłowym komunikuje się przy użyciu określonych jednostek PDU z równorzędną jej warstwą w komputerze docelowym, co przedstawiono na rysunku.

Pakiety danych w sieci są wysyłane ze źródła i trafiają do miejsca docelowego. Każda warstwa zależy od funkcji usługowej realizowanej przez warstwę OSI znajdującą się poniżej. W warstwie niższej następuje enkapsulacja jednostek PDU wyższej warstwy w polu danych warstwy niższej, po czym dodawane są nagłówki i stopki wymagane do wykonania funkcji tej warstwy. Następnie do danych

przesyłanych w dół przez kolejne warstwy modelu OSI dodawane są kolejne nagłówki i stopki. Po dodaniu informacji w warstwach 7, 6 i 5 kolejne informacje zostaną dodane w warstwie 4. Taka grupa danych, jednostka PDU warstwy 4, jest nazywana segmentem. Warstwa sieciowa świadczy usługi warstwie transportowej, która dostarcza dane do podsystemu intersieci. Zadaniem warstwy sieciowej jest przesyłanie danych intersiecią. Zadanie to jest wykonywane poprzez enkapsulację danych i dodanie nagłówka, co powoduje utworzenie pakietu (jednostka PDU warstwy 3). Nagłówek zawiera informacje wymagane do realizacji przesłania, takie jak źródłowy i docelowy adres logiczny. Warstwa łącza danych świadczy usługi warstwie sieciowej. Umieszcza informacje pochodzące z warstwy sieciowej w ramce (jednostka PDU warstwy 2). Nagłówek ramki zawiera informacje (na przykład adresy fizyczne) wymagane do realizacji funkcji łącza danych. Warstwa łącza danych świadczy usługi warstwie sieciowej, umieszczając informacje pochodzące z tej warstwy w ramce. Warstwa fizyczna z kolei świadczy usługi warstwie łącza danych. W warstwie fizycznej następuje kodowanie ramki łącza danych na ciąg zer i jedynek (bitów) w celu przesłania ich przez medium (zwykle kabel) w warstwie 1.

### **2.3.6 Model TCP/IP**

Model TCP/IP jest historycznym i technicznym standardem sieci Internet. Model odniesienia TCP/IP został utworzony w Departamencie Obrony USA jako projekt sieci, która przetrwałyby w każdych warunkach, nawet podczas wojny nuklearnej. W departamencie sformułowano wymaganie, aby transmisja pakietów była możliwa zawsze i w każdych warunkach przy wykorzystaniu różnych mediów komunikacyjnych, takich jak przewody miedziane, mikrofale, światłowody i łączna satelitarne. Postawienie tego trudnego problemu zaowocowało utworzeniem modelu TCP/IP. W przeciwieństwie do zastrzeżonych technologii sieciowych opisanych wcześniej, model TCP/IP został opracowany jako ogólnodostępny standard otwarty. Oznaczało to, że każdy mógł korzystać z modelu TCP/IP. Pozwoliło to na przyspieszenie rozwoju modelu TCP/IP jako standardu. Model TCP/IP składa się z następujących czterech warstw:

### **warstwa aplikacji**

## **warstwa transportowa**

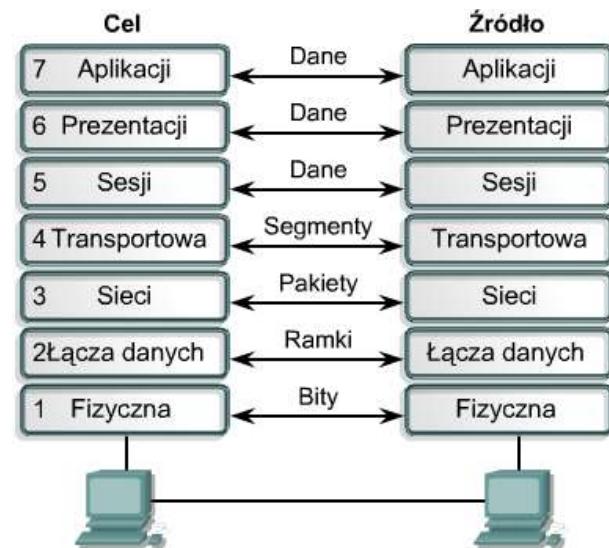
### **warstwa internetowa**

### **warstwa dostępu do sieci**

Chociaż niektóre warstwy modelu TCP/IP nazywają się tak samo jak warstwy modelu OSI, oba modele nie do końca sobie odpowiadają. Największa różnica polega na tym, że warstwy aplikacji obu modeli realizują inne funkcje. Projektanci modelu TCP/IP uważali, że warstwa aplikacji powinna obejmować warstwy sesji i prezentacji modelu OSI. Stworzyli warstwę aplikacji, która obsługuje prezentację, kodowanie i sterowanie konwersacją. **Warstwa transportowa** jest odpowiedzialna za sprawy związane z jakością usług, co obejmuje niezawodność transmisji, sterowanie przepływem i korekcję błędów. Jeden z jej protokołów, protokół TCP, posiada efektywne i elastyczne sposoby realizowania niezawodnej komunikacji sieciowej o niskiej stopie błędów i wysokiej przepustowości. **Protokół TCP** jest protokołem zorientowanym połączeniowo. Obsługuje on konwersację między miejscem źródłowym a docelowym, pakując informacje pochodzące z warstwy aplikacji w jednostki nazywane segmentami. Nazwa „zorientowany połączeniowo” nie oznacza, że między komunikującymi się komputerami istnieje obwód. Oznacza to, że segmenty warstwy 4 są przenoszone tam i z powrotem między hostami, potwierdzając logiczne istnienie połączenia przez określony czas. Zadaniem warstwy internetowej jest podzielenie segmentów TCP na pakiety i przesłanie ich dowolną siecią. Pakiety trafiają do sieci docelowej niezależnie od przebytej drogi. Protokołem, który zarządza tą warstwą, jest protokół IP. W tej warstwie następuje określenie najlepszej ścieżki i przełączanie pakietów. Związek między protokołem IP i protokołem TCP jest bardzo istotny. Protokół IP określa drogę dla pakietów, a protokół TCP zapewnia niezawodny transport. Pojęcie warstwy dostępu do sieci jest szerokie i w pewnym stopniu myjące. Jest ona także nazywana warstwą łączą host-sieć. W warstwie tej są obsługiwane wszystkie fizyczne i logiczne składniki potrzebne do utworzenia fizycznego łączka. Obejmuje ona szczegółowe rozwiązania dotyczące technologii sieciowej, łącznie ze szczegółami warstwy fizycznej i łączą danych modelu OSI.

**Na rysunku** przedstawiono niektóre spośród popularnych protokołów zdefiniowanych przy użyciu warstw modelu odniesienia TCP/IP. Najczęściej stosowane protokoły warstwy aplikacji to:

protokół FTP (ang. *File Transfer Protocol*)



protokół HTTP (ang. *Hypertext Transfer Protocol*)  
 protokół SMTP (ang. *Simple Mail Transfer Protocol*)  
 protokół DNS (ang. *Domain Name System*)  
 protokół TFTP (ang. *Trivial File Transfer Protocol*)

Najczęściej stosowane protokoły warstwy transportowej to:

protokół TCP (ang. *Transport Control Protocol*)  
 protokół UDP (ang. *User Datagram Protocol*)

Główny protokół warstwy internetowej to

protokół IP (ang. *Internet Protocol*)

Warstwa dostępu do sieci dotyczy określonej technologii używanej w danej sieci. Niezależnie od dostępnych usług aplikacji sieciowej i używanego protokołu istnieje tylko jeden protokół internetowy — protokół IP. Jest to świadoma decyzja projektowa. Protokół IP jest uniwersalnym protokołem umożliwiającym dowolnemu komputerowi komunikację w dowolnej chwili i w dowolnym miejscu.

### **Porównanie modeli OSI i TCP/IP wykaże niektóre podobieństwa i różnice.**

**Podobieństwa są następujące:**

- Obydwa modele mają budowę warstwową.
- Oba protokoły mają warstwy aplikacji, chociaż świadczą one bardzo różne usługi.
- Oba mają porównywalne warstwy sieciowe i transportowe.
- Oba modele muszą być znane osobom zawodowo zajmującym się sieciami komputerowymi.
- W obu protokołach założeniem jest przełączanie pakietów. Oznacza to, że poszczególne pakiety mogą do tego samego miejsca docelowego trafić różnymi ścieżkami. Inaczej niż w sieci z komutacją łączy, gdzie wszystkie pakiety pokonują tę samą ścieżkę.

**Różnice są następujące:**

- W protokole TCP/IP zadania warstwy prezentacji i sesji są realizowane w warstwie aplikacji.
- W warstwie dostępu do sieci protokołu TCP/IP połączono funkcje warstw łączą danych i fizycznej modelu OSI.

**Protokół TCP/IP wydaje się prostszy, bo ma mniej warstw.** Protokoły TCP/IP są standardem, wokół którego powstał Internet, więc model TCP/IP zyskał na znaczeniu właśnie dzięki tym protokołom. W przeciwieństwie do modelu TCP/IP model OSI nie jest zwykle bazą do tworzenia sieci, pomimo tego, że jest on używany jako podstawa teoretyczna. Chociaż protokoły TCP/IP są standardami, które przyczyniły się do rozwoju Internetu, w programie szkolenia będzie używany model OSI. Powody tego są następujące:

Jest to podstawowy, niezależny od protokołów standard.

Jest bardziej szczegółowy, co sprawia, że jest bardziej pomocny w nauce.

Większa szczegółowość może być pomocna w przypadku rozwiązywania problemów.

Osoby zawodowo zajmujące się sieciami komputerowymi różnią się w opiniach, który model powinien być używany. W związku z naturą tej gałęzi przemysłu trzeba dobrze znać oba modele. Zarówno model OSI, jak i model TCP/IP będą przywoływane w trakcie trwania całego kursu. Nacisk zostanie położony na:

protokół TCP jako protokół warstwy 4 modelu OSI;

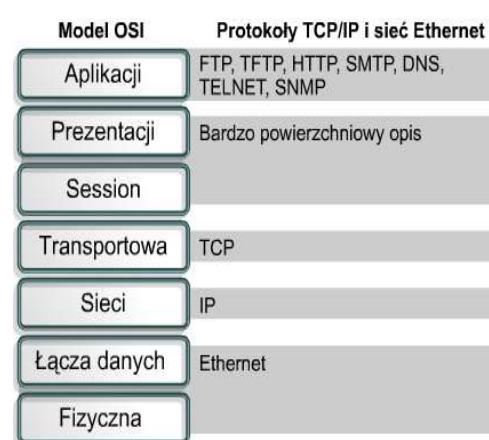
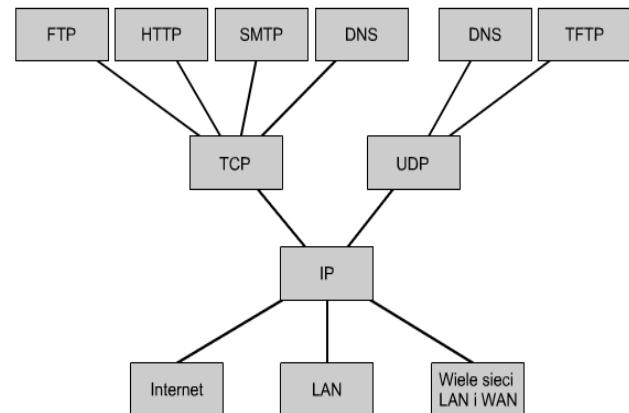
protokół IP jako protokół warstwy 3 modelu OSI;

sieć Ethernet jako technologię obejmującą warstwy 2 i 1.

Należy pamiętać o tym, że między modelem a rzeczywistym protokołem używanym w sieci jest różnica. Model OSI będzie używany do opisu protokołów TCP/IP.

### **2.3.7 Szczegóły procesu enkapsulacji**

Dane w komunikacji sieciowej są wysyłane ze źródła i trafiają do miejsca docelowego. Informacje przesyłane siecią są nazywane danymi lub pakietami danych. Jeśli dane mają być przesłane z jednego komputera (host A) do drugiego komputera (host B), muszą najpierw zostać opakowane w procesie zwanym enkapsulacją. W procesie enkapsulacji dane przed przesaniem siecią są uzupełniane o potrzebne informacje związane z używanymi protokołami. Dlatego do pakietu danych przekazywanego w dół przez warstwy modelu OSI dodawane są nagłówki, stopki i inne informacje. Sposób przeprowadzania enkapsulacji można zaobserwować, patrząc na wędrówkę danych przez poszczególne warstwy, co przedstawiono na rysunku . Dane wysłane ze źródła przechodzą przez warstwę aplikacji w dół do kolejnych warstw. Opakowanie i przepływ wymienianych danych zmienia się, w miarę jak w kolejnych warstwach realizowane są usługi dla użytkowników końcowych. Jak przedstawiono to na rysunku , sieć musi przeprowadzić pięć następujących etapów konwersji, aby dokonać enkapsulacji danych:



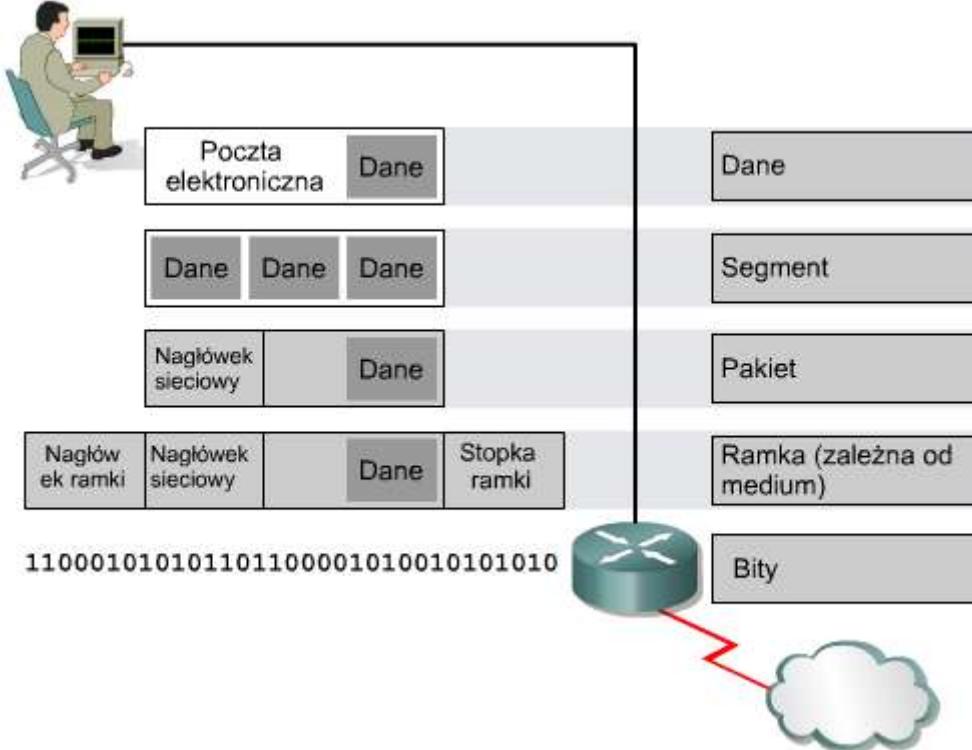
**Utworzenie danych.** Gdy użytkownik wysyła wiadomość e-mail, znaki alfanumeryczne są przekształcane w dane, które można przesyłać intersiecią.

**Opakowanie danych do transportu end-to-end.** Dane są opakowywane w celu przesłania ich w intersieci. Funkcja transportowa dzięki użyciu segmentów zapewnia niezawodną komunikację hostów wiadomości po obu stronach systemu poczty elektronicznej.

**Dodanie sieciowego adresu IP do nagłówka.** Dane są umieszczane w pakiecie lub datagramie, który zawiera nagłówki z logicznym adresem źródłowym i docelowym. Adresy te umożliwiają urządzeniom sieciowym przesyłanie pakietów siecią wzdłuż wybranej ścieżki.

**Dodanie nagłówka i stopki warstwy łącza danych.** Każde urządzenie sieciowe musi umieścić pakiet w ramce. Ramka umożliwia połączenie z najbliższym bezpośrednio połączonym urządzeniem sieciowym na łączu. Każde urządzenie znajdujące się na wybranej ścieżce sieciowej musi obsługiwać ramki, aby możliwe było połączenie z kolejnym urządzeniem.

**Przekształcenie na bity w celu ich transmisji.** Ramkę trzeba przekształcić w ciąg zer i jedynek (bitów) w celu ich transmisji poprzez medium. Funkcja taktowania umożliwia urządzeniom rozróżnienie bitów przesyłanych przez medium. Medium w intersieci fizycznej może zmieniać się wzdłuż używanej ścieżki. Na przykład wiadomość e-mail może zostać wysłana z sieci LAN, przejść przez sieć szkieletową kampusu i zostać wprowadzona do sieci WAN, aż osiągnie miejsce docelowe w innej oddalonej sieci LAN.



### Podsumowanie

- Karty sieciowe, węzły, koncentratory, mosty, przełączniki i routery są powszechnie stosowanymi urządzeniami sieciowymi.
- Niektóre spośród popularnych typów sieci to: sieci LAN, WAN, MAN, SAN i VPN.
- Szerokość pasma jest zdefiniowana jako ilość informacji, która można przesyłać siecią w określonym czasie.
- Dwa najbardziej znane modele sieci to: model odniesienia OSI i model TCP/IP.

## Moduł 3: Media transmisyjne używane w sieciach. Wprowadzenie

Kable miedziane są wykorzystywane praktycznie w każdej sieci LAN. Dostępne są różne typy kabli miedzianych, z których każdy ma swoje wady i zalety. Prawidłowy wybór okablowania ma istotne znaczenie dla efektywnej pracy sieci. Ponieważ informacje są przenoszone w miedzi za pośrednictwem prądu elektrycznego, podczas planowania i instalowania sieci ważne jest poznanie niektórych zasad rządzących elektrycznością. Światłowód jest medium najczęściej wykorzystywany na długich odcinkach szerokopasmowej transmisji danych punkt-punkt, stosowanych w szkieletowych sieciach LAN i w sieciach WAN. W mediach optycznych do transmisji danych poprzez włókno szklane lub plastikowe wykorzystywane jest światło. Sygnały elektryczne powodują generowanie przez nadajnik światłowodowy sygnałów świetlnych wysyłanych przez światłowód. Host odbiorczy otrzymuje sygnały świetlne i przekształca je na sygnały elektryczne na odległym końcu światłowodu. Przez sam kabel światłowodowy nie przepływa jednak prąd elektryczny. W rzeczywistości użyte w kablu światłowodowym szkło jest bardzo dobrym izolatorem elektryczności. Fizyczne połączenie urządzeń umożliwia zwiększenie produktywności dzięki temu, że pozwala na udostępnianie drukarek, serwerów i oprogramowania. Tradycyjne systemy sieciowe wymagają, aby stacja robocza cały czas pozostawała w tym samym miejscu, zezwalając na ruch jedynie w granicach narzuconych przez długość kabla przyłączniowego. Wprowadzenie technologii bezprzewodowych usuwa te ograniczenia i umożliwia prawdziwą mobilność w świecie komputerów. Obecnie technika bezprzewodowa nie oferuje szybkiej transmisji danych ani takich zabezpieczeń czy niezawodności pracy jak w przypadku sieci kablowych. Jednak elastyczność techniki bezprzewodowej stanowi wystarczającą rekompensatę. Podczas instalowania nowej sieci lub modernizacji istniejącej administratorzy często biorą pod uwagę technikę bezprzewodową. Prosta sieć bezprzewodowa może działać już w kilka minut połączenie z Internetem następuje poprzez połączenie kablowe, router, modem kablowy lub DSL i bezprzewodowy punkt dostępu, który pełni rolę koncentratora węzłów bezprzewodowych. W zastosowaniach domowych lub biurowych te wszystkie funkcje są często spełniane przez jedno urządzenie.

### 3.1 Media miedziane

#### 3.1.1 Atomy i elektrony

Cała materia złożona jest z atomów. Układ okresowy pierwiastków obejmuje wszystkie znane typy atomów i ich własności. Na atom składają się następujące elementy:

**elektrony** – cząstki naładowane ujemnie, które poruszają się po orbitach wokół jądra,

**protony** – cząstki naładowane dodatnio,

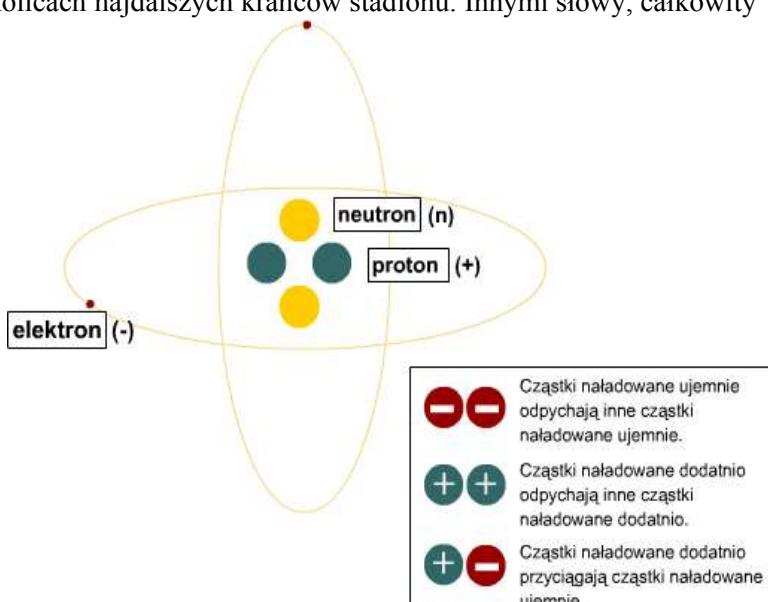
**neutrony** – cząstki bez ładunku (obojętne).

Protony i neutrony tworzą centralną część atomu zwaną jądrem. Aby lepiej zrozumieć elektryczne właściwości pierwiastków/substancji, należy odnaleźć hel (He) w układzie okresowym pierwiastków. Liczba atomowa helu to 2, co oznacza, że składa się on z 2 protonów i 2 elektronów. Jego masa atomowa to 4. Odejmując liczbę atomową (2) od masy atomowej (4), można się przekonać, że hel ma również 2 neutrony. Duński fizyk Niels Bohr opracował uproszczony model atomu. Ilustracja przedstawia model atomu helu. Gdyby protony i neutrony w atomie miały takie rozmiary, że razem tworzyłyby bryłę o wielkości piłki futbolowej znajdującej się na środku boiska, jedynymi mniejszymi elementami byłyby elektrony. Miałoby one rozmiar wiśni i orbitowałyby w okolicach najdalszych krańców stadionu. Innymi słowy, całkowity rozmiar tego atomu, z uwzględnieniem orbit elektronów, byłby zbliżony do rozmiaru stadionu. Natomiast samo jądro atomu, w którym znajdują się protony i neutrony, miałoby rozmiar piłki. Jedno z praw przyrody, zwane prawem Coulomba, mówi, że ładunki różnoimienne (przeciwne) oddziałują na siebie siłą, która powoduje, że wzajemnie się przyciągają. Ładunki jednoimienne (podobne) oddziałują na siebie siłą, która powoduje, że się odpychają. Zarówno w przypadku ładunków różnoimiennych, jak i jednoimiennych, siła zwiększa się w miarę zbliżania się ładunków do siebie i jest odwrotnie proporcjonalna do kwadratu odległości między nimi. Gdy cząsteczki znajdują się bardzo blisko siebie, siły jądrowe równoważą odpychającą siłę elektrostatyczną, sprawiając, że nukleony w jądrze utrzymują się razem. Właśnie dlatego jądra nie rozpadają się. Przyjrzyjmy się modelowi atomu helu proponowanemu przez Bohra. Jeśli prawo Coulomba jest prawdziwe, a model Bohra opisuje atomy helu jako stabilne, to działać muszą jeszcze jakieś inne prawa przyrody. W jaki sposób zarówno prawo Coulomba, jak i model Bohra mogą być jednocześnie prawdziwe?

**Prawo Coulomba** – ładunki jednoimienne odpychają się, a różnoimienne przyciągają.

**Model Bohra** – protony mają ładunki dodatnie, a elektrony ładunki ujemne. W jądrze znajduje się kilka protonów.

**Elektrony** pozostają na orbitach, mimo iż protony je przyciągają. Elektrony mają wystarczającą prędkość, aby utrzymywać się na orbicie i nie zostać wciągnięte na jądro, podobnie jak dzieje się to w wypadku Księżyca krążącego wokół Ziemi.



**Protony** nie oddalają od siebie z powodu sił jądrowych, które związane są z neutronami. Siły jądrowe to niewiarygodnie duże siły, które działają jak klej, utrzymując protony blisko siebie. **Protony i neutrony** są ze sobą związane bardzo wielką siłą, natomiast elektrony są utrzymywane na orbicie wokół jądra przez siłę znacznie mniejszą. Tak więc elektrony niektórych atomów, na przykład atomów metali, mogą zostać odciągnięte od atomu i zmuszone do przepływu. Właśnie dzięki temu morzu elektronów, w niewielkim stopniu związanych z atomami, możliwa jest elektryczność. Elektryczność to swobodny przepływ elektronów. **Uwolnione elektrony**, które pozostają w jednym miejscu bez ruchu i mają ładunek ujemny, nazywane są elektrycznością statyczną. Jeśli te statyczne elektrony będą miały możliwość przeskoczenia na przewodnik, może dojść do wyładowania elektrostatycznego (ESD). Przewodniki zostaną omówione w dalszej części tego rozdziału. **Wyładowanie elektrostatyczne**, które jest zazwyczaj bezpieczne dla ludzi, może być niebezpieczne dla wrażliwego sprzętu elektronicznego. Wyładowanie statyczne może uszkodzić układy scalone komputera, przechowywane na nim dane lub jedno i drugie. Obwody logiczne układów scalonych komputera są bardzo wrażliwe na wyładowania elektrostatyczne. Podczas wykonywania czynności wewnętrz komputera, routera lub innych urządzeń należy zachować w związku z tym ostrożność. Substancje zbudowane z atomów lub grup atomów, zwane cząsteczkami, często określa się terminem „materiały”. Materiały klasyfikuje się pod względem przynależności do jednej z trzech grup w zależności od tego, z jaką łatwością może przez nie przepływać prąd elektryczny, czyli wolne elektrony. Wiedza, w jaki sposób izolatory, przewodniki i półprzewodniki kontrolują przepływ elektronów i pracują ze sobą w różnych kombinacjach, ma zasadnicze znaczenie, jeżeli chodzi o wszystkie urządzenia elektroniczne.

### 3.1.2 Napięcie

Napięcie jest czasami nazywane siłą elektromotoryczną (EMF, ang. electromotive force; w języku polskim stosowany jest też skrót SEM). Siła elektromotoryczna jest siłą elektryczną lub ciśnieniem, które ujawnia się, gdy elektrony i protony zostaną rozdzielone. Wytworzona siła przyciąga ładunki przeciwnie i odpycha ładunki podobne. Proces taki zachodzi w baterii, w której reakcje chemiczne doprowadzają do uwolnienia elektronów z ujemnego bieguna baterii. Elektrony wędrują następnie przez obwód ZEWNĘTRZNY w kierunku przeciwnego, czyli dodatniego, bieguna. Elektrony nie przemieszczają się przez samą baterię. Należy pamiętać, że przepływ prądu elektrycznego jest w rzeczywistości przepływem elektronów. Napięcie może być również wytworzone na trzy inne sposoby. Po pierwsze, przez tarcie (elektryczność statyczna). Po drugie, przez magnetyzm (generator elektryczny). I wreszcie napięcie można wytworzyć za pomocą światła (ogniwo słoneczne). Napięcie oznacza się literą U lub literą E, jeśli mowa jest o sile elektromotorycznej. Jednostką pomiaru napięcia jest wolt (V) Volt jest definiowany jako ilość pracy wykonanej nad ładunkiem jednostkowym, potrzebna do rozdzielenia ładunków.

### 3.1.3 Opór i impedancja

Materiały, przez które przepływa prąd, stawiają różny opór (rezystancję) przepływającym elektronom.

Materiały, które mają bardzo małą rezystancję lub nie mają jej wcale, są nazywane przewodnikami. Te materiały, które nie przewodzą prądu lub przewodzą go w bardzo małym stopniu, nazywane są izolatorami.

Wielkość rezystancji zależy od chemicznego składu

materiału. Wszystkie materiały przewodzące prąd elektryczny charakteryzują się mierzalną wielkością opisującą rezystancję dla przepływających przez nie elektronów. Materiały te charakteryzują się również pojemnością i indukcyjnością, które związane są z przepływem elektronów. Te trzy charakterystyki składają się na impedancję, która jest podobna do rezystancji i stanowi jej uogólnienie. **Tłumienność** jest ważnym pojęciem w nauce o sieciach. Odnosi się do oporu stawianego przepływowi elektronów, który powoduje pogorszenie sygnału podczas przechodzenia przez przewodnik. Litera R oznacza rezystancję. Jednostką pomiaru rezystancji jest om ( $\Omega$ ). Symbol pochodzi od greckiej litery omega,  $\Omega$ .

**Izolatory elektryczne**, nazywane zazwyczaj izolatorami, to materiały, przez które elektrony przepływają z trudem lub w ogóle nie przepływają. Przykładami izolatorów elektrycznych jest plastik, szkło, powietrze, suche drewno, papier, guma i hel. Materiały te mają bardzo stabilną strukturę chemiczną, a orbitujące elektrony są silnie związane z atomami.

**Przewodniki elektryczne**, nazywane zazwyczaj przewodnikami, to materiały, przez które elektrony przepływają z dużą łatwością. Plyną one bez przeszkodek, ponieważ elektrony zewnętrzne są bardzo słabo związane z jądem i łatwo można je uwolnić. W temperaturze pokojowej materiały te mają bardzo dużą liczbę wolnych elektronów, które mogą umożliwić przewodzenie. Przyłożenie napięcia powoduje przemieszczanie się wolnych elektronów, co z kolei wywołuje przepływ prądu. W układzie okresowym niektóre grupy atomów są łączone w kategorie rozmieszczone w kolumnach. Atomy każdej kolumny należą do określonej rodziny chemicznej. Mimo iż mogą mieć one różną liczbę protonów, neutronów i elektronów, ich elektrony zewnętrzne mają podobne orbity i zachowują się w podobny sposób podczas oddziaływanego z innymi atomami i cząsteczkami. Najlepszymi przewodnikami są metale takie jak miedź (Cu), srebro (Ag) i złoto (Au), ponieważ ich elektrony mogą zostać łatwo uwolnione. Inne przewodniki to stop lutowniczy, będący mieszaniną ołowiu (Pb) i cyny (Sn), oraz woda zawierająca jony. Jon to atom mający więcej lub mniej elektronów niż protonów w jądrze atomu. Ludzkie ciało składa się w około 70% z wody zawierającej jony, co oznacza, że ludzkie ciało jest przewodnikiem.

**Półprzewodniki** to materiały, w których można precyzyjnie kontrolować wielkość przewodzonego prądu elektrycznego. Materiały te są umieszczone w tej samej kolumnie układu okresowego. Przykładem jest węgiel (C), german (Ge) oraz arsenek galu (GaAs). Najważniejszym półprzewodnikiem, z którego wykonuje się najlepsze miniaturowe obwody elektroniczne, jest krzem (Si). Krzem występuje powszechnie i można go znaleźć w piasku, szkle i w wielu typach skał.

Izolatory	Przewodniki	Półprzewodniki
Elektrony przepływają z trudem	Elektrony przepływają z łatwością	Przepływ elektronów może być precyzyjnie kontrolowany
Plastik Guma Powietrze Papier Suche drewno Szkło	Miedź (Cu) Srebro (Ag) Złoto (Au) Stop lutowniczy Woda z jonami Ludzie	Węgiel (C) German (Ge) Arsenek galu (GaAs) Krzem (Si)

Obszar wokół San Jose w Kalifornii jest znany jako Dolina Krzemowa, ponieważ powstał tam przemysł komputerowy, który opiera się na krzemowych układach scalonych

### 3.1.4 Prąd

Prąd elektryczny to przepływ ładunków wywołany ruchem elektronów. W obwodach elektrycznych prąd jest wywołyany przepływem swobodnych elektronów. Gdy przyłożone zostanie napięcie (ciśnienie elektryczne) i powstanie ścieżka dla prądu, elektrony będą się poruszać od ujemnego bieguna do bieguna dodatniego. Biegun ujemny odpycha elektrony, a biegun dodatni przyciąga je. Prąd jest oznaczany literą „I”. Jednostką pomiaru prądu jest amper (A). Definiowany jest on jako liczba ładunków przepływających w ciągu sekundy przez punkt wzduł ścieżki. Jeśli przyjmiemy, że natężenie lub prąd to ilość lub objętość ruchu elektronów, to napięcie będzie szybkością, z jaką przepływają elektrony. Z połączenia natężenia i napięcia powstaje moc elektryczna. Moc urządzeń elektrycznych, takich jak żarówki, silniki i zasilacze

komputerowe, jest podawana w watach. Liczba watów określa, ile mocy dane urządzenie zużywa lub wytwarza. Całą pracę w obwodzie elektrycznym wykonuje prąd lub natężenie. Przykładowo, elektryczność statyczna charakteryzuje się bardzo wysokim napięciem, tak wysokim, że może spowodować przeskok iskry przez lukę wielkości kilku centymetrów. Jednak ma ona bardzo małe natężenie i może wywołać szok, ale nie trwałe obrażenia. Rozrusznik w samochodzie pracuje z bardzo niskim napięciem rzędu 12 woltów, ale wymaga bardzo dużego natężenia do wytworzenia energii, która wystarczyłaby do obrócenia wału silnika. Piorun ma zarówno bardzo wysokie napięcie, jak i natężenie, w wyniku czego może spowodować poważne uszkodzenia lub obrażenia.

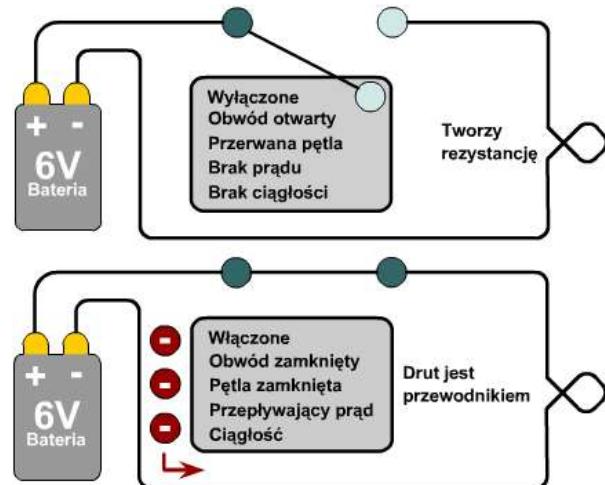
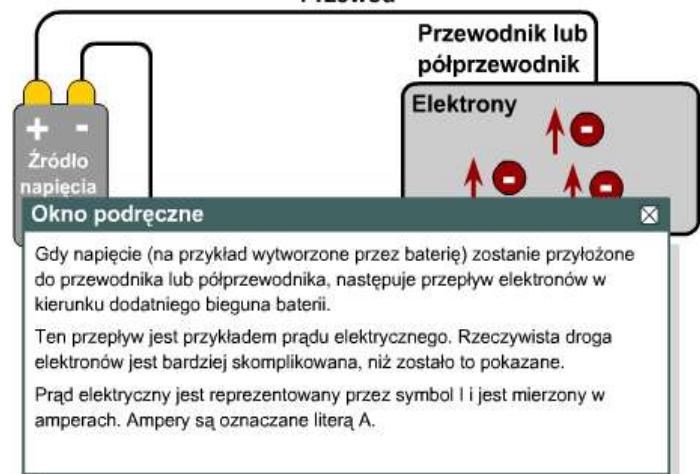
### 3.1.5 Obwody

Prąd przepływa w zamkniętych pętlach zwanych obwodami. Obwody te muszą składać się z przewodników i muszą zawierać źródła napięcia. Napięcie powoduje przepływ prądu, natomiast rezystancja i impedancja utrudniają ten przepływ. Prąd złożony jest z elektronów przepływających od biegunów ujemnych w kierunku biegunów dodatnich. Znajomość tych faktów umożliwia ludziom kontrolowanie przepływu prądu. W najczęstszym przypadku prąd elektryczny będzie się starał popływać ku ziemi, jeśli tylko znajdzie do niej ścieżkę. Prąd również płynie ścieżką o najmniejszej rezystancji. Tak więc, jeśli ludzkie ciało stanowić będzie ścieżkę o najmniejszej rezystancji, prąd popływie przez nie. W gniazdku elektrycznym z wystającym bolcem, bolec ten działa jako uziemienie o napięciu zero woltów. Uziemienie tworzy dla elektronów ścieżkę prowadzącą bezpośrednio do ziemi. Podczas wykonywania pomiarów elektrycznych uziemienie oznacza, że pomiar napięcia musi być wykonany pomiędzy dwoma punktami. Analogia z przepływem wody pomaga wyjaśnić pojęcie elektryczności. Im wyższe są poziom wody i ciśnienie, tym więcej wody popłynie. Strumień wody zależy również od rozmiaru przestrzeni, przez którą musi on płynąć. Podobnie, im wyższe jest napięcie i ciśnienie elektryczne, tym większy prąd zostanie wytworzony. Prąd elektryczny napotyka rezystancję, która podobnie jak zawór wodny, zmniejsza przepływ. Jeśli prąd elektryczny znajduje się w obwodzie prądu zmiennego, to ilość prądu będzie zależeć od wielkości impedancji. Jeśli prąd elektryczny znajduje się w obwodzie prądu stałego, to ilość prądu będzie zależeć od wielkości rezystancji. Pompa pełni rolę baterii. Wytwarza ona ciśnienie umożliwiające przepływ. **Zależność pomiędzy napięciem, rezystancją a prądem jest następująca: napięcie ( $U$ ) = prąd ( $I$ ) pomnożony przez rezystancję ( $R$ ). Innymi słowy,  $U=I \cdot R$ . Jest to prawo Ohma, nazwane tak od nazwiska naukowca badającego te zagadnienia.**

Prąd może płynąć na dwa sposoby, jako prąd zmienny (AC) i jako prąd stały (DC). Prąd zmienny (AC) i napięcie zmieniają się w czasie, jednocześnie zmieniając swój kierunek (polaryzację).

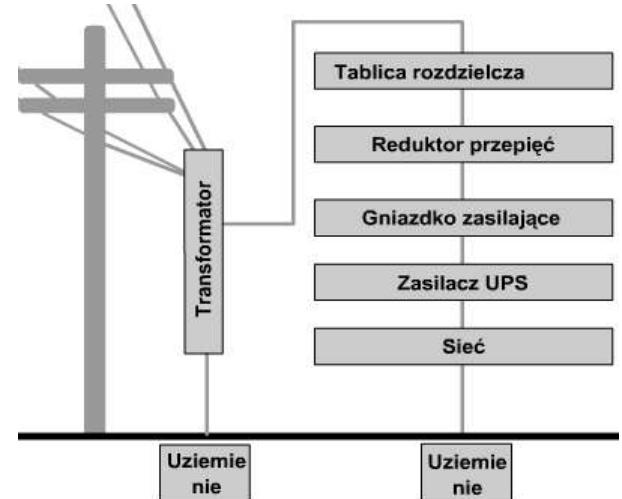
Prąd zmienny płynie w jednym kierunku, po czym zmienia go na przeciwny i płynie tak do momentu kolejnej zmiany.

Proces się powtarza. Napięcie zmienne jest dodatnie na jednym bieguncie i ujemne na drugim. Napięcie zmienne zmienia polaryzację, więc biegun dodatni staje się ujemnym, a biegun ujemny staje się dodatnim. Ten proces powtarza się ciągle. Prąd stały zawsze płynie w tym samym kierunku, a napięcie stałe ma zawsze tę samą polaryzację. Jeden biegun jest zawsze dodatni, a drugi jest zawsze ujemny. Nie zmieniają się one ani nie zamieniają miejscami. **Oscyloskop** to urządzenie elektroniczne używane do badania przebiegu sygnałów elektrycznych w czasie. Wyświetla on wykresy fal i impulsów, umożliwiając obserwowanie ich zależności w czasie. Na ekranie oscyloskopu widoczna jest oś x oznaczająca czas oraz oś y oznaczająca napięcie. Zazwyczaj oś y umożliwia wyświetlanie dwóch kanałów wejściowych, można więc obserwować dwa przebiegi elektryczne jednocześnie. **Linie elektryczne** przenoszą elektryczność w postaci prądu zmiennego, ponieważ w ten sposób można ją efektywnie dostarczać na duże odległości. Prąd stały znajduje



zastosowanie w bateriach latarek, akumulatorach samochodowych i w zasilaniu układów scalonych na płycie głównej komputera, gdy wymagane jest dostarczenie prądu na krótkich odcinkach.

**Elektryny** przepływają w obwodach zamkniętych lub pętlach zamkniętych. **Rysunek (poprzednia strona)** przedstawia prosty obwód. Procesy chemiczne zachodzące w baterii powodują wytworzenie ładunków. One z kolei dostarczają napięcia lub ciśnienia elektrycznego, które umożliwia przepływ elektronów przez różne urządzenia. Linie oznaczają przewodnik, który jest zazwyczaj przewodem miedzianym. Włącznik można sobie wyobrazić jako pojedynczy przewód, który może być otwarty (przerwany) w celu uniemożliwienia przepływu elektronów. Gdy dwa jego końce zostaną zwarte (zamkną obwód), elektryny będą mogły płynąć. Na koniec, żarówka stanowi rezystancję dla przepływu elektronów, co powoduje, że elektryny uwalniają energię w postaci światła. Obwody spotykane w sieciach komputerowych wykorzystują znacznie bardziej skomplikowane warianty tego bardzo prostego obwodu. W przypadku systemów elektrycznych AC i DC przepływ elektronów następuje zawsze od źródła naładowanego ujemnie w kierunku źródła naładowanego dodatnio. Jednak aby mógł nastąpić kontrolowany przepływ elektronów, wymagany jest obwód zamknięty. **Rysunek (obok)** przedstawia część obwodu elektrycznego, za pomocą którego zasilanie dostarczane jest do domu lub biura.



### 3.1.6 Specyfikacja kabla

Z kablami związane są różne specyfikacje oraz oczekiwania dotyczące wydajności.

Jakie szybkości transmisji można uzyskać dla różnych typów kabli? Szybkość transmisji bitowej w kablu jest bardzo istotna. Ma na nią wpływ rodzaj użytego przewodnika.

Jakiego typu transmisja brana jest pod uwagę? Czy transmisja będzie cyfrowa, czy analogowa? Użytkownik może wybrać transmisję cyfrową, czyli transmisję w paśmie podstawowym, albo transmisję analogową, czyli szerokopasmową.

Jaką odległość może pokonać sygnał przez określony typ kabla, zanim słumieniu sygnału stanie się znaczące? Innymi słowy, czy sygnał ulegnie takiemu osłabieniu, że gdy dotrze do urządzenia odbiorczego, nie będzie ono w stanie poprawnie go odebrać i zinterpretować? Odległość, którą sygnał pokonuje poprzez kabel, ma bezpośredni wpływ na słumieniu sygnału. Osłabienie sygnału jest więc bezpośrednio związane z odlegością, która jest przezeń pokonywana oraz z typem użytego kabla.

Niektóre przykłady specyfikacji sieci Ethernet, które odnoszą się do typu kabla, są następujące:

#### 10BASE-T

Specyfikacja 10BASE-T dotyczy transmisji o szybkości równej 10 Mb/s. Transmisja jest dokonywana w paśmie podstawowym (baseband), stąd skrót „Base”. Oznaczenie „T” dotyczy skrętki.

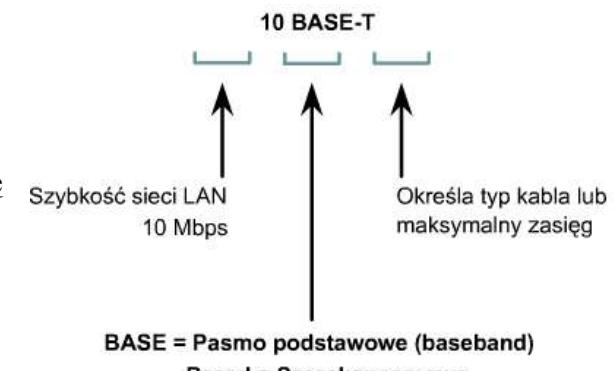
Specyfikacja 10BASE5 dotyczy transmisji o szybkości równej 10 Mb/s. Transmisja jest dokonywana w paśmie podstawowym, czyli jest interpretowana cyfrowo. Oznaczenie „5” dotyczy możliwości przesyłania przez kabel sygnału na odległość około 500 metrów, zanim tłumienność wpłynie na możliwość odebrania i odpowiedniego zinterpretowania odbieranego sygnału. Specyfikacja 10BASE5 jest często określana jako Thicknet. Jednak w rzeczywistości Thicknet to typ sieci, podczas gdy 10BASE5 oznacza specyfikację Ethernet używaną w tej sieci.

Specyfikacja 10BASE2 dotyczy transmisji o szybkości równej 10 Mb/s.

Transmisja jest dokonywana w paśmie podstawowym, czyli jest interpretowana cyfrowo. Oznaczenie „2” w nazwie 10BASE2 odnosi się do maksymalnej długości segmentu – około 200 metrów, zanim tłumienność wpłynie na możliwość odebrania i odpowiedniego zinterpretowania odbieranego sygnału. Faktycznie maksymalna długość segmentu wynosi 185 metrów. Specyfikacja 10BASE2 jest często określana jako Thinnet. Jednak w rzeczywistości Thinnet to typ sieci, podczas gdy 10BASE2 oznacza specyfikację Ethernet używaną w tej sieci.

### 3.1.7 Kabel koncentryczny

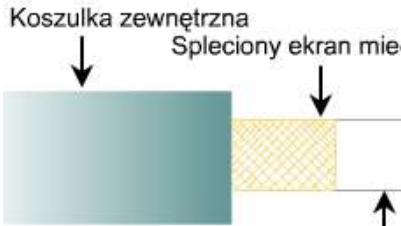
Kabel koncentryczny składa się z miedzianego przewodnika otoczonego warstwą elastycznej izolacji. Z kolei izolacja ta, jest otoczona splecioną miedzianą taśmą lub folią metalową działającą jak drugi przewód w obwodzie oraz ekran dla znajdującego się wewnątrz przewodnika. Ta druga warstwa lub ekran zmniejsza także ilość zewnętrznych zakłóceń elektromagnetycznych. Ekran pokryty jest koszulką izolacyjną. Przewód centralny może być także wykonany, dla zmniejszenia kosztów, z cyny pokrytej aluminium. Kabel koncentryczny używany w sieci LAN zapewnia kilka korzyści. Może być kładziony na większych odległościach niż skrętka ekranowana (STP), nieekranowana (UTP) oraz kabel ScTP, bez stosowania wtórników. Wtórni regenerują sygnał w sieci, aby mogła ona objąć większy obszar. Kabel koncentryczny jest tańszy niż kabel światłowodowy, a technologia została dobrze poznana. Była ona używana przez wiele lat do transmisji



BASE = Pasmo podstawowe (baseband)

Broad = Szerokopasmowe

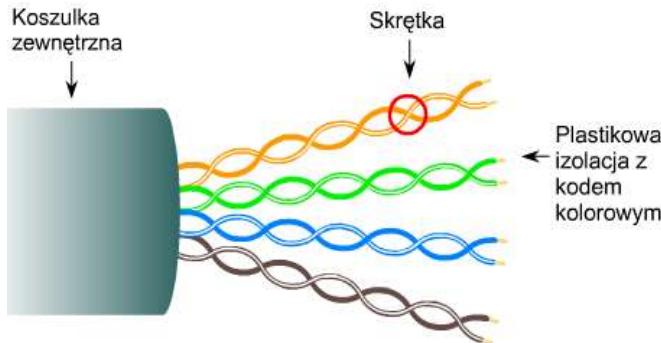
danych różnych typów, w tym sygnałów telewizji kablowej. Pracując z kablem, należy koniecznie wziąć pod uwagę jego rozmiar. W miarę zwiększenia grubości kabla trudniej jest z nim pracować. Należy pamiętać, że kabel musi być przeprowadzony przez istniejące przewody i korytko, które mają ograniczony rozmiar. Kabel koncentryczny jest dostępny w wielu rozmiarach. Kabel o największej średnicy znalazł zastosowanie jako kabel sieci szkieletowych Ethernet, ponieważ umożliwia transmisję sygnału na większe odległości i ma lepsze charakterystyki tłumienia szumów. Ten typ kabla koncentrycznego jest często zwany Thicknet. Jak sugeruje nazwa potoczna („gruba sieć”), ten typ kabla może okazać się w pewnych sytuacjach trudny w montażu. Ogólnie, im bardziej w montażu jest medium sieciowe, tym droższa jest jego instalacja. Kabel koncentryczny jest droższy w instalacji niż skrętka. Dlatego kabel Thicknet praktycznie nie jest już używany poza instalacjami do specjalnych zastosowań. W przeszłości kabel koncentryczny Thinnet o średnicy zewnętrznej wynoszącej zaledwie 0,35 cm był używany w sieciach Ethernet. Był on szczególnie przydatny w tych instalacjach kablowych, które wymagały wielu zawinięć i skręceń kabla. Ponieważ sieć Thinnet była łatwa w montażu, była również tańsza. Z tego też powodu określano ją niekiedy mianem Cheapernet. Zewnętrzna warstwa miedziana lub metalowa siatka w kablu koncentrycznym stanowi połowę obwodu elektrycznego. Dlatego też należy szczególnie zatrudnić się o zapewnienie dobrego połączenia elektrycznego na obu jego końcach, aby możliwe było jego prawidłowe uziemienie. Nieprawidłowe połączenie przewodu ekranującego jest jednym z najczęstszych źródeł problemów z połączaniami, które pojawiają się w instalacjach z użyciem kabla koncentrycznego. Nieprawidłowe połączenie przewodów skutkuje wystąpieniem szumów elektrycznych zakłócających transmisję sygnału w medium sieciowym. Właśnie z tego względu sieć Thinnet nie jest już tak często używana, nie jest również uwzględniana w najnowszych standardach sieci Ethernet (szybkość 100 Mb/s i wyższa).



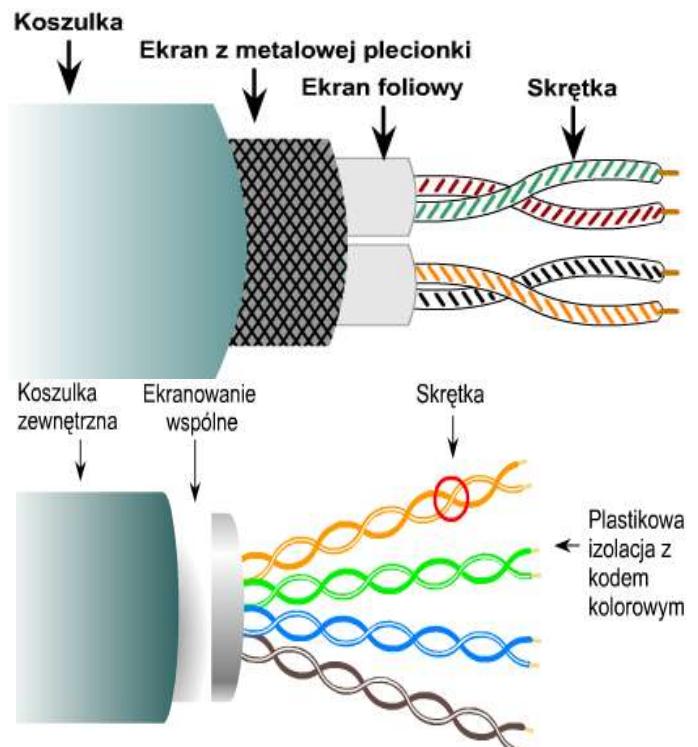
- Szybkość i przepustowość: 10 - 100 Mb/s
- Średni koszt węzła: tani
- Rozmiar medium i złącza: średni
- Maksymalna długość kabla: 500 m



### 3.1.8 Kabel STP



Skrętka ekranowana (STP) łączy w sobie techniki ekranowania, znoszenia i skręcania przewodów. Każda para przewodów jest owinięta metalową folią. Dwie pary przewodów są owinięte metalową siatką lub folią. Jest to zazwyczaj kabel 150-omowy. Kabel STP przeznaczony do zastosowań w instalacjach sieci Token Ring redukuje szумy elektryczne w kablu, takie jak sprząganie i przesłuch pomiędzy parami żył. Kabel STP redukuje również szum elektroniczny pochodzący z zewnętrz, na przykład interferencję elektromagnetyczną (EMI) i zakłócenia radiowe (RFI). Skrętka ekranowana ma podobne wady i zalety co skrętka nieekranowana (UTP). Kabel STP zapewnia lepszą ochronę przed wszelkiego rodzaju zewnętrznymi zakłóceniami, ale jest droższy i trudniejszy w montażu niż kabel UTP. Rozwiązaniem hybrydowym, powstały z połączenia kabla UTP i STP, jest ekranowany kabel UTP (ScTP), znany również jako skrętka foliowana (FTP). ScTP to kabel UTP owinięty ekranem z metalowej folii lub siatki. ScTP, tak jak UTP, jest kablem 100-omowym. Wielu instalatorów i producentów kabli może używać terminu STP do opisania kabla ScTP. Należy pamiętać, że dzisiejsze określenie STP odnosi się do czteroparowego ekranowanego kabla. Mało prawdopodobne by prawdziwy kabel STP był używany w jakiejkolwiek instalacji sieciowej. Metalowy materiał ekranujący w kablu STP i ScTP musi być uziemiony po obu końcach. Jeśli uziemienie nie będzie właściwe lub jeśli wystąpią jakiekolwiek nieciągłości ekranu, kabel STP i ScTP może stać się bardzo



podatny na zakłócenia związane z szumem. Dzieje się tak dlatego, że ekran zachowuje się wówczas jak antena odbierająca niepożądane sygnały. Działa to jednak w obie strony. Nie tylko uniemożliwia zewnętrznym falom elektromagnetycznym tworzenie szumów w przewodach transmisji danych, ale także minimalizuje emisję fal elektromagnetycznych. Fale te mogą powodować szum w innych urządzeniach. Kabla STP i ScTP nie można kłaść bez użycia wtórników sygnału na tak długich odcinkach jak innych mediach sieciowych, takich jak kabel koncentryczny czy kabel światłowodowy. Większa izolacja i ekranowanie powoduje znaczne zwiększenie rozmiaru, wagi i kosztów kabla. Materiały ekranujące sprawiają, że wykonanie zakończeń kabla jest trudniejsze i łatwiej o słabe jakościowo wykonanie. Mimo to kable STP i ScTP wciąż odgrywają ważną rolę, zwłaszcza w Europie, a także w instalacjach gdzie w pobliżu kabli występują silne zakłócenia radiowe lub interferencje elektromagnetyczne.

### 3.1.9 Kabel UTP

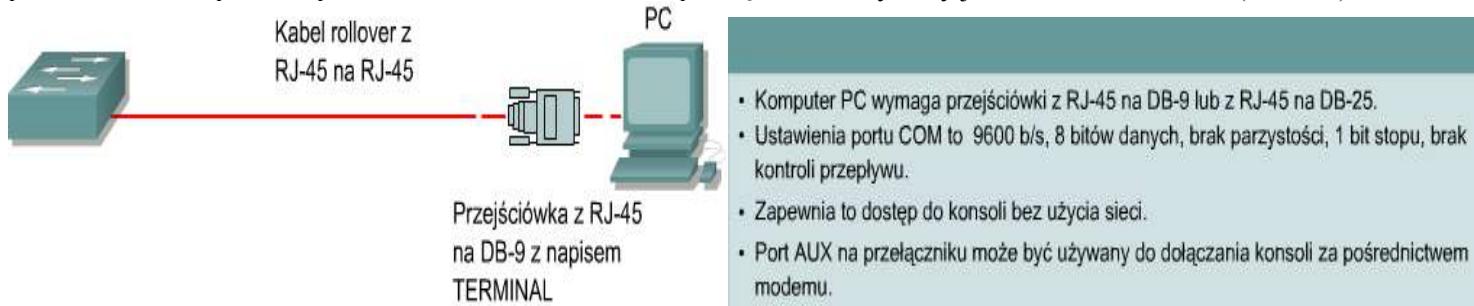
Skrętka nieekranowana (UTP) (**OBOK**) to stosowany w wielu sieciach medium składające się z czterech par przewodów. Każdy z ośmiu miedzianych przewodów w kablu UTP jest pokryty materiałem izolacyjnym. Ponadto każda para przewodów jest ze sobą skręcona. Ten typ kabla bazuje wyłącznie na efekcie znoszenia w skręconej parze przewodów, co ogranicza pogorszenie sygnału spowodowane zakłóceniami EMI i RFI. Aby jeszcze bardziej zmniejszyć przesłuch pomiędzy parami żył w kablu UTP, liczba skręceń poszczególnych par przewodów jest różna. Podobnie jak w wypadku kabla STP, kabel UTP musi spełniać ścisłe wymagania opisujące liczbę skręceń lub spleceń dozwolonych na jednostkowym odcinku kabla. Standard TIA/EIA-568-B.2 zawiera wymagania dotyczące jakości kabla. Mówią one o doprowadzeniu do każdego gniazdka dwóch kabli, jednego przeznaczonego do transmisji głosu, a drugiego do transmisji danych. Jeden z tych dwóch kabli, służący do transmisji głosu, musi być czterożyłową skrętką UTP. Kable kategorii 5e są obecnie najczęściej zalecane i stosowane w instalacjach. Jednakże przewidywanie analityków i niezależne badania wskazują, że kable kategorii 6 zajmą miejsce kabli kategorii 5e w instalacjach sieciowych. Fakt, że połączenie w kategorii 6 oraz wymagania kanałowe są wstecz kompatybilne do kategorii 5e sprawia, że klientom bardzo łatwo jest wybrać kategorię 6 i zastąpić kategorię 5e w swych sieciach. Zastosowania, które działają na kategorii 5e, będą działać na kategorii 6.

Skrętka nieekranowana ma wiele zalet. Łatwo jest ją instalować i jest tańsza niż inne typy mediów sieciowych. W rzeczywistości cena metra kabla UTP jest niższa niż innych typów kabli używanych w sieciach LAN. Prawdziwą zaletą jest jednak jej rozmiar. Ponieważ średnica zewnętrzna jest niewielka, kabel UTP nie wypełnia korytek tak szybko, jak inne typy kabli. Jest to bardzo istotny czynnik, który powinien zostać wzięty pod uwagę, szczególnie w przypadku instalowania sieci w starszych budynkach. Ponadto, jeśli kabel UTP jest instalowany ze złączami RJ-45, potencjalne źródła szumów sieciowych zostają znacznie zredukowane, a dobre i trwałe połączenie jest praktycznie gwarantowane. Użycie skrętki nie jest jednak pozbawione wad. Kabel UTP jest bardziej podatny na szum elektryczny i zakłócenia niż inne typy mediów sieciowych, a odległość pomiędzy wzmacniaczami sygnału jest znacznie mniejsza w przypadku kabla UTP niż w przypadku kabla koncentrycznego i kabli światłowodowych. Kabel ze skręconymi parami był kiedyś uważany za wolniejszy, jeśli chodzi o transmisję danych niż inne typy kabli. Dziś już się tak nie uważa. Kabel ze skręconymi parami jest obecnie uważany za najszybsze medium miedziane. Aby komunikacja mogła mieć miejsce, sygnał wysyłany przez źródło musi być interpretowany przez odbiornik. Jest to prawdziwe zarówno z perspektywy oprogramowania, jak i perspektywy fizycznej. Transmitowany sygnał musi być prawidłowo odebrany przez obwód przeznaczony do odbioru sygnałów. Styk nadawczy w punkcie źródłowym musi mieć dobre połączenie ze stykiem odbiorczym w punkcie docelowym. Poniżej opisano typy połączeń kablowych używanych pomiędzy urządzeniami intersieci.

**Na rysunku** przełącznik sieci LAN jest podłączony do komputera. Kabel łączący port przełącznika z portem interfejsu sieciowego komputera jest nazywany **kablem prostym**.

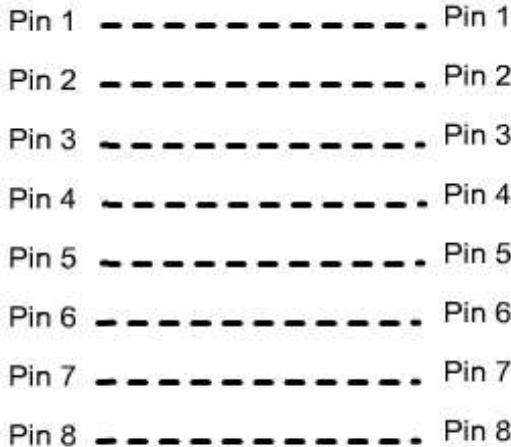
**Na rysunku** dwa przełączniki są ze sobą połączone. Kabel łączący port jednego przełącznika z portem drugiego przełącznika jest **nazywany kablem z przepłotem**.

**Przedstawiony na rysunku (dolnym)** kabel łączący przejściówkę RJ-45 w porcie COM komputera z portem konsoli w routerze lub przełączniku nazywany jest kablem do konsoli (rollover).

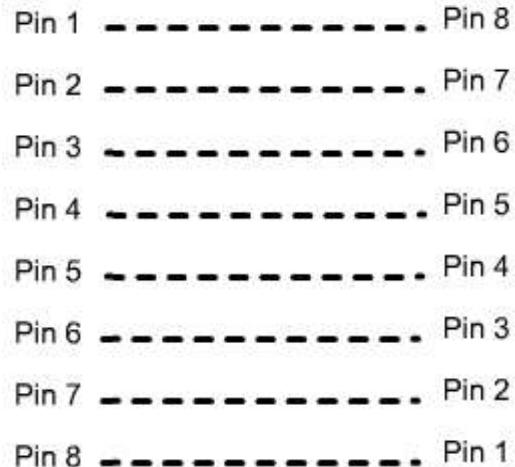


Kable określa się na podstawie typu połączeń (wyrowadzeń) prowadzących z jednego jego końca na drugi. Jeśli kabel nie został jeszcze poprowadzony w ścianie, technik może porównać dwa końce tego samego kabla, umieszczając je obok siebie. Technik porównuje kolory połączeń RJ-45 po umieszczeniu obu końcówek zaczepem skierowanym w kierunku dłoni, a końcówkami kabli skierowanymi od siebie. Kabel prosty powinien mieć takie samo wzór kolorów na obu końcach. W przypadku kabla z przepłotem kolory styków 1 i 2 na drugim końcu pojawią się w stykach 3 i 6 i na odwrót. Dzieje się tak dlatego, że styki transmitujące i odbierające są ze sobą zamienione. W przypadku kabla do konsoli (rollover) kombinacja kolorów od strony lewej do prawej na jednym końcu powinna być odwrotna niż kombinacja kolorów na drugim końcu.

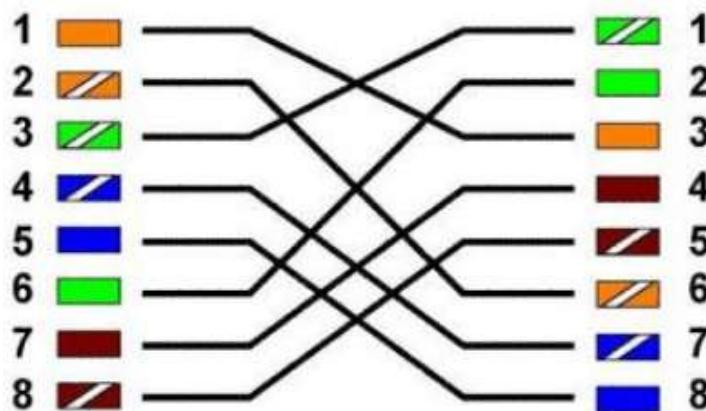
### 1. Schemat kabla prostego



### 2. Schemat kabla rolloer



### 3. Schemat kabla krosowego EIA/TIA T568B Crossover Diagram



## 3.2 Media optyczne

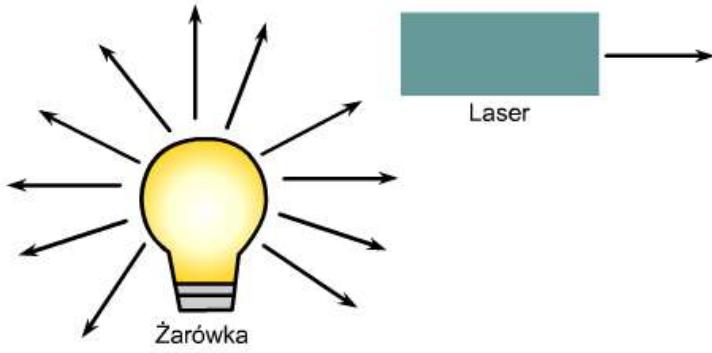
### 3.2.1 Widmo elektromagnetyczne

Światło używane w sieciach światłowodowych stanowi jeden z rodzajów energii elektromagnetycznej. Gdy ładunek elektryczny porusza się, zmieniając cyklicznie swój kierunek, tworzony jest rodzaj energii zwany energią elektromagnetyczną. Energia ta może w postaci fal przemieszczać się przez próżnię, powietrze i inne materiały, takie jak szkło. Istotną właściwością fali energii jest jej długość. Fale radiowe, mikrofale, fale radarowe, światło widzialne, promieniowanie X i promieniowanie gamma pozornie znacznie różnią się od siebie. Jednak wszystkie są rodzajami energii elektromagnetycznej. Jeśli wszystkie typy fal elektromagnetycznych ułożą się w kolejności od największej do najmniejszej długości fali, powstanie ciąg zwany widmem elektromagnetycznym. Długość fali elektromagnetycznej jest określona przez częstotliwość, z jaką ładunek wytwarzający falę porusza się w jedną i drugą stronę. Jeśli ładunek porusza się w jedną i drugą stronę powoli, długość generowanej fali jest duża. Ruch ładunku elektrycznego można sobie przedstawić jako ruch patyka zanurzonego jednym końcem w basenie. Jeśli patyk porusza się w jedną i drugą stronę powoli, generuje fale na wodzie o dużej odległości pomiędzy szczytami fal. Jeśli patyk porusza się w obie strony szybciej, odległość pomiędzy szczytami fal będzie mniejsza. Ponieważ fale elektromagnetyczne generowane są w ten sam sposób, mają wiele wspólnych właściwości. Wszystkie fale poruszają się w próżni z tą samą prędkością. Wynosi ona około 300 000 kilometrów na sekundę lub inaczej 186283 mil na sekundę. Jest to także prędkość światła. Ludzkie oko może odbierać energię elektromagnetyczną o długości fali pomiędzy 700 a 400 nanometrów (nm). Nanometr to jedna miliardowa metra (0,000 000 001 metra). Energia elektromagnetyczna o długości fali pomiędzy 700 a 400 nm jest nazywana światłem widzialnym. Światło o długości fali około 700 nm jest widziane jako kolor czerwony. Najkrótsze fale, widziane jako kolor fioletowy, mają długość około 400 nm. Ta część widma elektromagnetycznego jest widoczna jako kolory tęczy. Fale o długościach niewidocznych dla ludzkiego oka są używane do transmisji danych przez światłowód. Są to fale nieznacznie dłuższe niż światło czerwone i dlatego są nazywane światłem podczerwonym. Światło podczerwone jest używane w pilotach do telewizorów. Długość fali światła w światłowodzie wynosi 850 nm, 1310 nm lub 1550 nm. Wybrano fale o tych właśnie długościach, ponieważ lepiej od innych przemieszczają się one przez światłowód.

### 3.2.2 Promieniowy model światła

Fale elektromagnetyczne wychodzące ze źródła poruszają się po liniach prostych. Te linie proste wychodzące ze źródła są nazywane promieniami. O promieniach światła można myśleć jako o wąskich wiązkach światła podobnych do wytwarzanych przez lasery. W próżni światło porusza się ruchem jednostajnym prostoliniowym z prędkością 300 000 kilometrów na sekundę. Światło porusza się jednak wolniej w innych ośrodkach, takich jak powietrze, woda i szkło. Gdy promień światła, nazywany promieniem padającym, przekracza granicę dwóch ośrodków, pewna część energii światła przenoszonej przez promień zostaje odbita. Dlatego możemy przeglądać się w lustrze. Światło, które zostało odbite, jest

nazywane promieniem odbitym. Energia światła w promieniu padającym, która nie została odbita, wniknie w szkło. Promień wchodzący zostanie odchylony o pewien kąt od pierwotnej ścieżki. Ten promień jest nazywany promieniem załamany. To, w jakim stopniu promień padający zostanie załamany, zależy od kąta, pod jakim promień pada na powierzchnię szkła, i od stosunku prędkości, z jakimi światło porusza się w tych dwóch ośrodkach. Załamanie promienia świetlnego na granicy dwóch substancji stanowi powód, dla którego promień światła jest w stanie podróżować poprzez światłowód, nawet jeśli światłowód zostanie wygięty w pętlę. Gęstość optyczna szkła wpływa na stopień załamania promienia światła w szkle. Gęstość optyczna określa, jak bardzo promień światła zmniejsza szybkość przy przechodzeniu przez daną substancję. Im większa jest gęstość optyczna materiału, tym bardziej światło zwalnia w porównaniu z prędkością w próżni. Stosunek szybkości światła w próżni do szybkości światła w ośrodku jest nazywany współczynnikiem załamania (IR). Stąd też miara gęstości optycznej ośrodka jest współczynnik załamania tego ośrodka. Ośrodek o dużym współczynniku załamania jest gęstszy optycznie i bardziej spowalnia światło niż ośrodek o mniejszym współczynniku załamania. W przypadku substancji takiej jak szkło, współczynnik załamania (gęstość optyczna) może zostać zwiększyony poprzez dodanie do szkła związków chemicznych. Poprzez oczyszczenie szkła można zmniejszyć współczynnik załamania. Kolejne lekcje dostarczą dalszych informacji na temat odbicia i załamania oraz ich związku z konstrukcją i działaniem światłowodu.



Substancja	Współczynnik załamania
Powietrze	1.000
Szkło	1.523
Diament	2.419
Woda	1.333

$$\text{Współczynnik załamania} = n = \frac{\text{Szybkość światła w próżni}}{\text{Szybkość światła w materiale}}$$

### 3.2.3 Do przemyślenia

Gdy promień światła (promień padający) uderza w lśniącą powierzchnię płaskiego kawałka szkła, część energii światła w promieniu jest odbijana. Kąt pomiędzy promieniem padającym a prostą prostopadłą do powierzchni szkła przechodzącą przez punkt padania promienia padającego jest nazywany kątem padania. Prosta prostopadła jest nazywana normalną. Nie jest to promień światła, ale narzędzie umożliwiające pomiar kątów. Kąt pomiędzy promieniem odbitym a normalną jest nazywany kątem odbicia. Prawo odbicia mówi, że kąt odbicia promienia światła jest równy kątowi padania. Innymi słowy, kąt, pod jakim promień światła uderza w powierzchnię odbijającą, określa kąt, pod jakim promień zostanie odbity od tej powierzchni.

### 3.2.4 Załamanie

Gdy światło trafia na granicę pomiędzy dwoma ośrodkami przeźroczystymi, dzieli się na dwie części. Część promienia światła jest odbijana z powrotem do pierwszego ośrodka, pod kątem odbicia równym kątowi padania. Energia pozostała w promieniu światła przekracza granicę i dostaje się do drugiego ośrodka. Jeśli promień padający uderzy w powierzchnię szklaną dokładnie pod kątem 90 stopni, to wejdzie prosto w szkło. Promień nie zostanie załamany. Jeśli jednak promień padający nie pada dokładnie pod kątem 90 stopni w stosunku do powierzchni, promień wchodzący w szkło zostanie załamany. Zakrzywienie wchodzącego promienia jest nazywane załamaniem. Stopień załamania promienia uzależniony jest od współczynnika załamania obu przeźroczystych ośrodków. Jeśli światło przechodzi z ośrodka o mniejszym współczynniku załamania do ośrodka o większym współczynniku załamania, promień jest załamywany w kierunku normalnej. Jeśli światło przechodzi z substancji o większym współczynniku załamania do substancji o mniejszym współczynniku załamania, promień jest załamywany w kierunku przeciwnym do normalnej. Wyobraźmy sobie promień światła poruszający się pod kątem różnym od 90 stopni przez granicę pomiędzy szkłem a diamentem. Współczynnik załamania światła dla szkła wynosi około 1,523. Współczynnik załamania dla diamentu wynosi około 2,419. Dlatego promień po wejściu w diament zostanie zakrzywiony w kierunku normalnej. Gdy światło przekroczy granicę pomiędzy diamentem a powietrzem pod kątem innym niż 90 stopni, promień zostanie zakrzywiony w kierunku przeciwnym do normalnej. Powodem tego jest fakt, że powietrze ma współczynnik załamania światła bliski 1, czyli niższy niż współczynnik załamania diamentu.

### 3.2.5 Całkowite odbicie wewnętrzne

Promień światła, który jest włączany i wyłączany w celu przesyłania danych (jedynek i zer) w światłowodzie, musi w nim pozostać aż do momentu dotarcia do odległego końca. Promień nie może zostać załamany i przedostać się do materiału otaczającego światłowód. Załamanie spowodowałoby utratę części energii światła zawartej w promieniu. Światłowód musi być zaprojektowany w taki sposób, aby jego powierzchnia zewnętrzna działała jak lustro dla poruszającego się w nim promienia światła. **Jeśli promień światła próbujący wydostać się przez ścianę światłowodu zostanie odbity do wnętrza światłowodu pod kątem kierującym go w stronę odległego końca światłowodu, będzie to dobry „tunel” lub**

**„rurociąg” dla fal świetlnych.** Dzięki znajomości praw odbicia i załamania można zaprojektować taki światłowód, który będzie przenosił fale świetlne z minimalną utratą energii. Aby promień świetlny w światłowodzie był odbijany z powrotem do światłowodu bez straty energii spowodowanej załamaniem, muszą zostać spełnione następujące dwa warunki:

Rdzeń światłowodu musi mieć większy współczynnik załamania ( $n$ ), niż otaczający go materiał. Materiał otaczający rdzeń światłowodu jest nazywany płaszczem.

Kąt padania promienia świetlnego musi być większy niż kąt krytyczny dla rdzenia i płaszcza.

Gdy spełnione są oba te warunki, całe światło wpadające do światłowodu jest odbijane z powrotem do jego wnętrza. Zjawisko to jest nazywane całkowitym odbiciem wewnętrzny i stanowi fundamentalną zasadę projektowania światłowodów. Całkowite odbicie wewnętrzne powoduje, że promienie świetlne w światłowodzie odbijają się od granicy rdzenia z płaszczem i kontynuują podróż w kierunku odległego końca światłowodu. Światło będzie poruszać się poprzez rdzeń światłowodu wielokrotnie załączaną ścieżką.

Światłowód spełniający pierwszy warunek można utworzyć z łatwością. Ponadto można kontrolować kąt padania promieni świetlnych wchodzących do rdzenia. Wprowadzenie ograniczeń dwóch wymienionych poniżej czynników umożliwia kontrolowanie kąta padania:

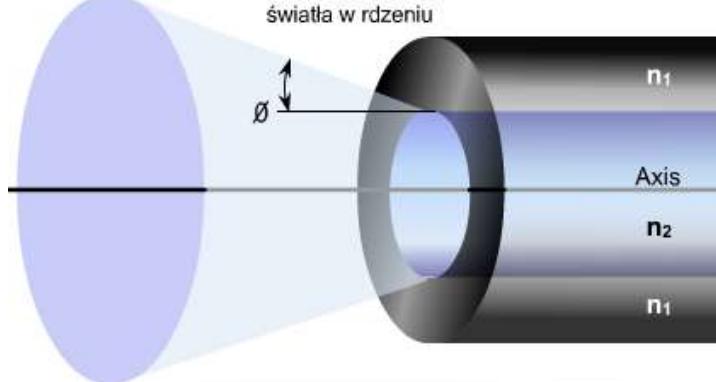
**Apertura numeryczna światłowodu** – apertura numeryczna rdzenia to zakres kątów padania, pod którymi promienie światła mogą wejść w światłowód, aby zostać całkowicie odbite.

**Mody** – ścieżki, którymi promień światła może się poruszać podczas przechodzenia przez światłowód.

Kontrolując oba te warunki, można uzyskać całkowite odbicie wewnętrzne w światłowodzie. Dzięki temu można utworzyć przewodnik fal świetlnych znajdujący zastosowanie w transmisji danych.

$n_1$  = współczynnik załamania światła w płaszczu

$n_2$  = współczynnik załamania światła w rdzeniu

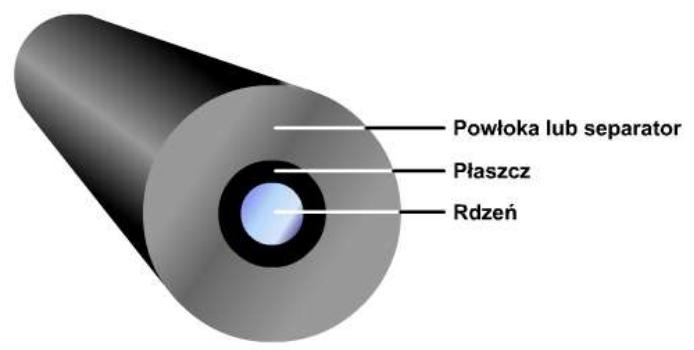
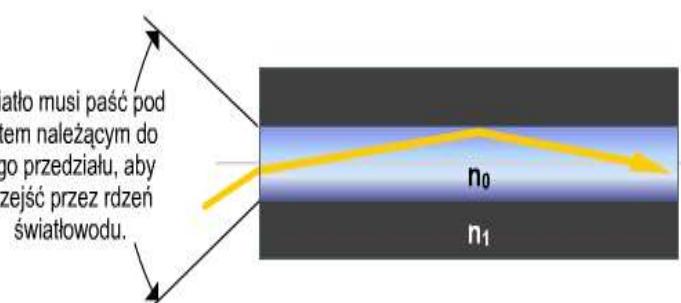
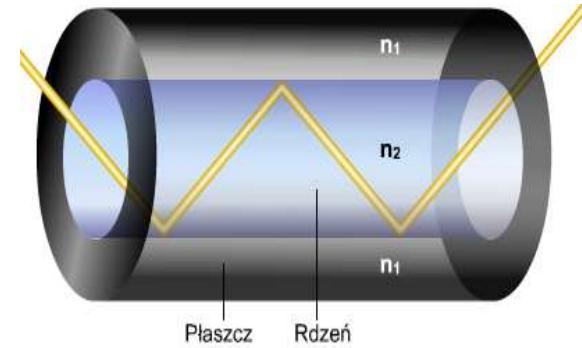


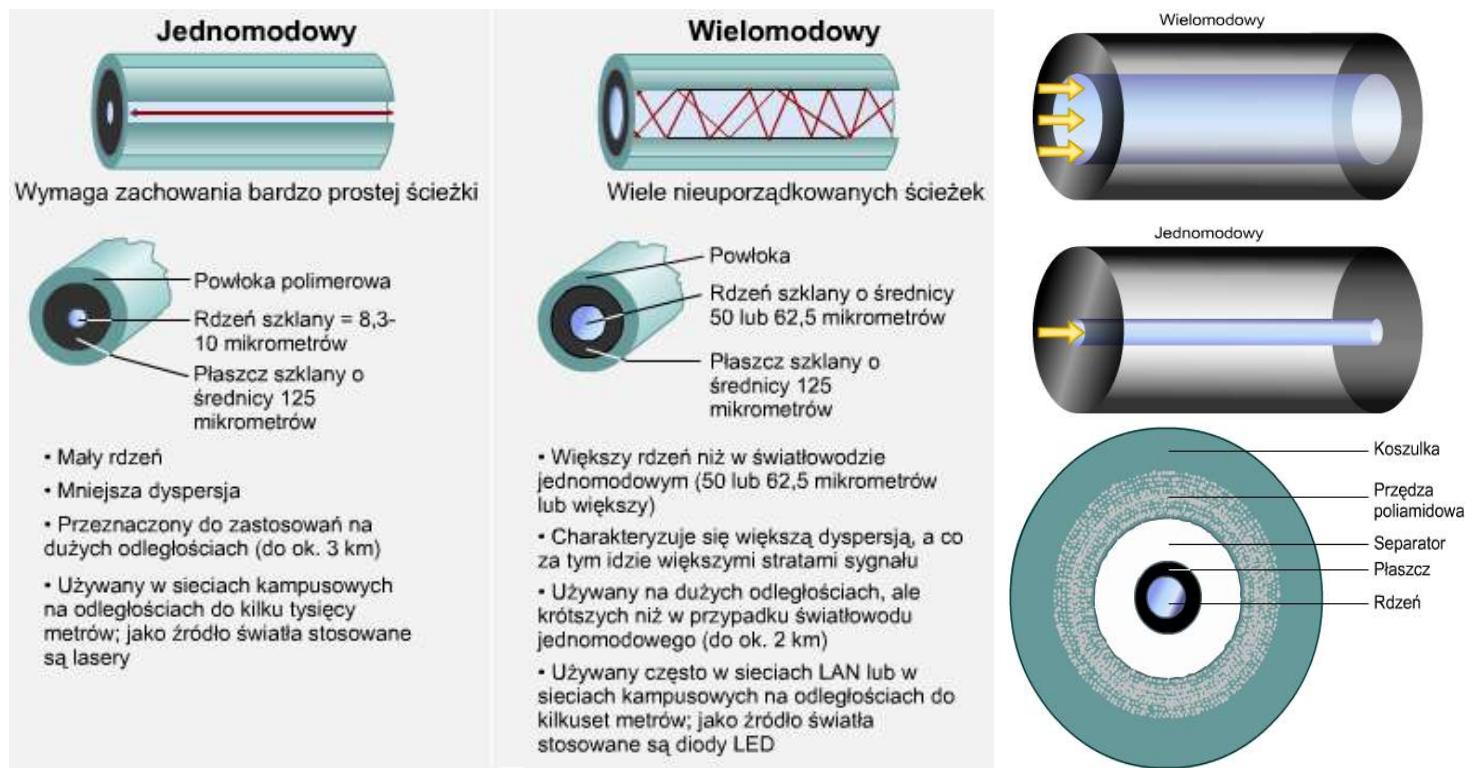
Apertura numeryczna (NA) określa przedział kątów, w którym następuje całkowite odbicie wewnętrzne.

### 3.2.6 Światłowód wielodomowy

Część światłowodu, przez którą przepływa promień światła, jest nazywana rdzeniem światłowodu. Promienie światła mogą wejść w światłowód tylko wtedy, gdy ich kąt padania znajduje się w przedziale apertury numerycznej światłowodu. Podobnie po wejściu promieni w rdzeń światłowodu istnieje ograniczona liczba ścieżek optycznych, którymi światło może przemieszczać się w światłowodzie. Te ścieżki optyczne są nazywane modami. Jeśli średnica rdzenia jest wystarczająco duża, aby światło mogło przepływać wieloma ścieżkami, światłowód jest nazywany światłowodem „wielodomowym”. Światłowód jednomodowy ma rdzeń o znacznie mniejszej średnicy. Umożliwia on promieniom światła poruszanie się tylko wzdłuż jednego modu w światłowodzie (Z dołu światłowód).

**Każdy kabel światłowodowy** używany w sieciach komputerowych składa się z dwóch szklanych światłowodów umieszczonych w oddzielnych osłonach. Jeden światłowód transmituje dane z urządzenia A do urządzenia B. Drugi światłowód transmituje dane z urządzenia B do urządzenia A. Światłowody te są podobne do dwóch jezdni drogi dwupasmowej lub autostrady, po których jeździ się w przeciwnych kierunkach. Dzięki temu możliwe jest połączenie pełnoduplexowe. Skrętką miedzianą zawiera osobną parę





przewodów do wysyłania i osobną do odbierania. Obwody światłowodowe używają jednego włókna światłowodu do wysyłania, a drugiego do odbierania.

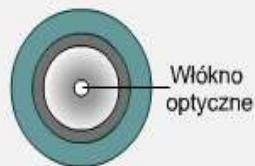
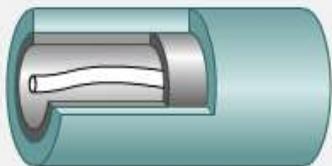
Zazwyczaj te dwa kable światłowodowe znajdują się w jednej koszulce zewnętrznej aż do miejsca, w którym zostają podłączone złącza. Do momentu podłączenia złączy nie ma konieczności ekranowania światłowodu, ponieważ znajdujące się wewnątrz światło nie może się z niego wydostać. Oznacza to, że w wypadku światłowodów nie zachodzi zjawisko przesłuchu. Bardzo często spotyka się wiele par światłowodów umieszczonych w tym samym kablu. Umożliwia to poprowadzenie pojedynczego kabla pomiędzy węzłami dystrybucji, piętrami lub budynkami. Jeden kabel może zawierać od 2 do 48 oddzielnego światłowodów. W wypadku kabla miedzianego dla każdego obwodu musiałby być poprowadzony oddzielny kabel UTP. Światłówód może przesyłać większą ilość bitów w ciągu sekundy na większe odległości, niż jest to możliwe w przypadku kabla miedzianego. Każdy kabel światłowodowy składa się zazwyczaj z pięciu części. Te części to rdzeń, płaszcz, bufor (separator), element wzmacniający i koszulka zewnętrzna. **Rdzeń** jest elementem transmitującym światło, znajdującym się w samym środku światłowodu. Wszystkie sygnały świetlne przesyłane są przez rdzeń. Rdzeń jest zazwyczaj wykonany ze szkła powstałego z połączenia dwutlenku krzemu (krzemionki) z innymi składnikami. W światłowodach wielomodowych jako rdzeń wykorzystywany jest typ szkła zwany szkłem o gradientowym współczynniku załamania. W szkle tego rodzaju współczynnik załamania maleje w kierunku zewnętrznej krawędzi rdzenia. Z tego względu obszar zewnętrzny rdzenia ma mniejszą gęstość optyczną niż środek i światło porusza się szybciej w zewnętrznej części rdzenia. Przy takiej konstrukcji promień światła poruszający się modem biegnącym przez środek rdzenia, nie musi przebywać tak długiej drogi jak promień poruszający się modem, który odbija się wewnątrz światłowodu. Wszystkie promienie powinny dotrzeć do końca światłowodu w tej samej chwili. Dzięki temu odbiornik na końcu światłowodu odbiera silny blysk światła, a nie długi, przyłumiony impuls. **Rdzeń** jest otoczony przez płaszcz. Płaszcz jest wykonany z tlenków krzemu o mniejszym współczynniku załamania niż rdzeń. Poruszające się w rdzeniu światłowodu promienie światła są odbijane od granicy między rdzeniem a płaszczem, ulegając całkowitemu odbiciu wewnętrzemu. Standardowy wielomodowy kabel światłowodowy jest powszechnie stosowany w sieciach LAN kablem światłowodowym. W standardowym wielomodowym kablu światłowodowym stosowany jest światłówód z rdzeniem o średnicy 62,5 lub 50 mikrometrów i płaszczu o rozmiarze 125 mikrometrów. Zazwyczaj używane jest oznaczenie 62,5/125 lub 50/125.

Mikrometr to jedna milionowa metra ( $1 \mu\text{m}$ ). **Płaszcz** jest otoczony przez materiał separujący (bufor), którym zazwyczaj jest plastik. Bufor chroni rdzeń i płaszcz przed uszkodzeniem. Istnieją dwa podstawowe typy kabli: konstrukcje z luźną tubą i konstrukcje z pokryciem ścisłym. Większość światłowodów używanych w sieciach LAN to kable wielomodowe z pokryciem ścisłym. W przypadku kabli z pokryciem ścisłym bufor otaczający płaszcz ma z nim bezpośredni kontakt.

Najważniejsza praktyczna różnica pomiędzy tymi dwoma typami wiąże się z ich zastosowaniem. Kable z luźną tubą są głównie używane w instalacjach na zewnątrz budynków, a instalacje z pokryciem ścisłym są używane wewnątrz budynków.

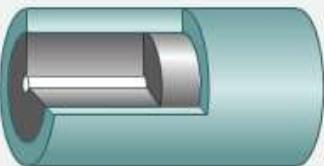
**Element wzmacniający** otaczający bufor zapobiega rozcięgnięciu światłowodu przez instalatorów podczas przeciagania. Często stosowanym do tego celu materiałem jest Kevlar, który używany jest również do produkcji kamizelek kuloodpornych. Ostatnim elementem jest **koszulka zewnętrzna**. Koszulka zewnętrzna otaczająca kabel chroni światłowód przed wytarciem, rozpuszczalnikami i innymi zanieczyszczeniami. Koszulka zewnętrzna światłowodu wielomodowego jest zazwyczaj pomarańczowa, ale używane są również inne kolory. Podczerwone diody LED lub lasery VCSEL (Vertical Cavity Surface Emitting Lasers) to dwa typy źródeł światła używanych zazwyczaj razem ze światłowodem wielomodowym. Obu tych źródeł nie można używać jednocześnie. Diody LED są nieznacznie tańsze w produkcji i nie wymagają zachowania tak dużej ostrożności jak lasery. Jednak nie mogą one transmitować światła przez światłowód tak daleko jak

### Konstrukcja z luźną tubą



- Włókno może przesuwać się w kat
- Eliminuje lokalne naprężenia
- Zapobiega mikrozgięciom
- Niższa tlumienność

### Konstrukcja z ciasnym separatorem



- Włókno jest usytuowane trwale w kablu
- Wysoka odporność na uszkodzenia
- Odporność na ścieranie
- Mały rozmiar

lasery. Światłowód wielomodowy (62,5/125) może przesyłać dane na odległość do 2000 metrów.

### 3.2.7 Światłowód jednodomowy

Światłowód jednodomowy składa się z tych samych części co wielomodowy. Koszulka zewnętrzna światłowodu jednodomowego jest zazwyczaj żółta. Główna różnica pomiędzy światłowodem wielomodowym a jednodomowym polega na tym, że światłowód jednodomowy umożliwia przesłanie tylko jednego modu światła przez kabel światłowodowy o mniejszej średnicy. Rdzeń światłowodu jednodomowego ma średnicę od osmiu do dziesięciu mikrometrów. Najczęściej spotykane są rdzenie o średnicy dziewięciu mikrometrów. Oznaczenie 9/125 na koszulce izolacyjnej światłowodu jednodomowego wskazuje, że rdzeń ma średnicę 9 mikrometrów, a otaczający go płaszcz — 125 mikrometrów.

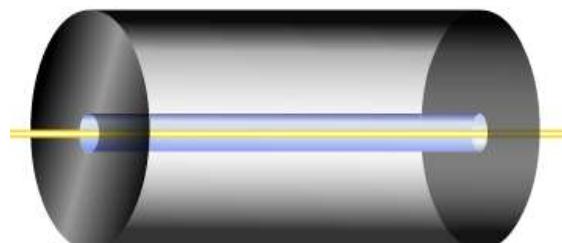
Jako źródło światła w światłowodzie jednodomowym używany jest laser pracujący w podczerwieni. Generowany przez niego promień światła dostaje się do rdzenia pod kątem 90 stopni. W wyniku tego dane przenoszone przez impulsy promienia światelnego w światłowodzie jednodomowym są transmitowane w linii prostej przez środek rdzenia. Zwiększa to zarówno szybkość przesyłania danych, jak i odległość, na jaką mogą zostać przesłane.

Dzięki swojej konstrukcji światłowód jednodomowy może osiągnąć wyższe szybkości transmisji danych (szerokość pasma) i większe odległości w porównaniu ze światłowodem wielomodowym. W światłowodzie jednodomowym można przesyłać dane w sieci LAN na odległość do 3000 metrów. Aczkolwiek dystans ten jest uznawany jako standard, nowsze technologie zwiększyły tę odległość i będą omawiane w następnych modułach. W światłowodzie wielomodowym można przesyłać dane na odległość do 2000 metrów. Lasery i światłowody jednodomowe są droższe niż diody LED i światłowody wielomodowe. W związku z powyższymi cechami światłowód jednodomowy jest często używany w połączeniach między budynkami.

### OSTRZEŻENIE::

**W światłowodzie jednodomowym stosuje się światło lasera o długości fali większej niż długość fal światła widzialnego. Laser jest tak silny, że może spowodować poważne uszkodzenie oczu. Nie należy zatem nigdy patrzeć na końcówkę światłowodu, którego odległy koniec jest podłączony do urządzenia. Nigdy też nie należy patrzeć w port transmisyjny w karcie sieciowej, przełączniku lub routerze. Należy pamiętać o zakładaniu zaślepek ochronnych na końcówki światłowodu i na porty światłowodowe w przełącznikach lub routerach. Konieczne jest zachowanie szczególnej ostrożności.**

Rysunek przedstawia porównanie rozmiarów rdzenia i płaszcza dla obu typów światłowodów o różnych średnicach rdzenia. Mniejsza średnica i bardziej złożona struktura rdzenia w światłowodzie jednodomowym sprawia, że światłowód jednodomowy ma większą szerokość pasma i może być prowadzony na większe odległości niż światłowód wielomodowy. Koszty jego wytwarzania są jednak większe.

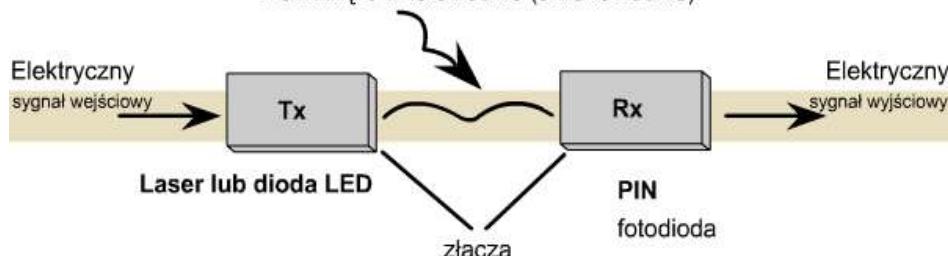


Wielomodowy	Wielomodowy	Wielomodowy	Jednodomowy
100-140 mikrometrów	62,5-125 mikrometrów	50-125 mikrometrów	9-125 mikrometrów

### 3.2.8 Inne komponenty optyczne

#### ŚWIATŁO

Zamknięte w falowodzie (światłowodzie)



jest nadajnik i odbiornik.

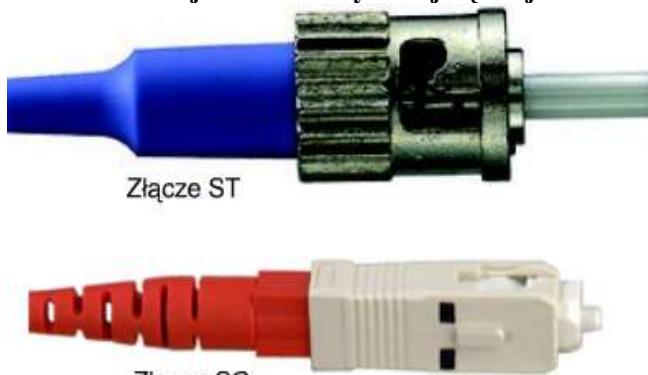
Większość danych przesyłanych w sieciach LAN ma postać sygnałów elektrycznych. Jednak do przesyłania danych w światłowodach wykorzystywane jest światło. Potrzebny jest więc element, który na jednym końcu światłowodu przetworzy prąd elektryczny w światło, na drugim zaś przetworzy światło ponownie w prąd elektryczny. Oznacza to, że potrzebny

Nadajnik odbiera od przełączników i routerów dane, które muszą zostać przesłane. Dane mają postać sygnałów elektrycznych. Nadajnik konwertuje sygnały elektroniczne w odpowiadające im impulsy światła. Istnieją dwa typy źródeł światła używanych do kodowania i wysyłania danych za pośrednictwem kabla:

**Diody świecące** (LED) wytwarzające światło podczerwone o długości fali równej 850 nm lub 1310 nm. Są one używane w światłowodach wielomodowych w sieciach LAN. Do skupienia wiązki światła podczerwonego na końcu światłowodu wykorzystywane są soczewki.

**Lasery** to źródła tworzące cienką wiązkę intensywnego podczerwonego światła o długości fali wynoszącej zazwyczaj 1310 nm lub 1550 nm. Lasery są używane w światłowodach jednomodowych na dużych dystansach, z którymi mamy do czynienia w sieciach WAN lub szkieletach sieci kampusowych. Konieczne jest zachowanie szczególnej ostrożności, aby zapobiec uszkodzeniu oka.

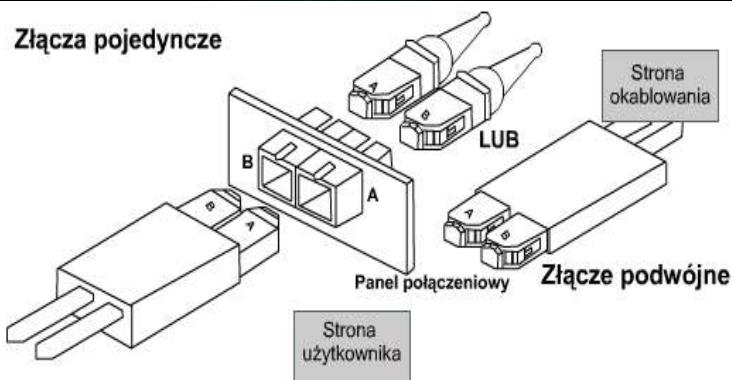
Każde źródło światła można bardzo szybko zapalić i zgasić w celu wysłania danych (jedynek i zer) z szybkością wielu bitów na sekundę. Na drugim końcu światłowodu znajduje się odbiornik. Odbiornik działa w podobny sposób jak ogniwo fotoelektryczne w kalkulatorze zasilanym energią słoneczną. Gdy światło padnie na odbiornik, wytwarzana jest elektryczność. Pierwszym zadaniem odbiornika jest wykrycie impulsu światła przychodzącego ze światłowodu. Następnie odbiornik konwertuje impuls światła z powrotem na taki sam sygnał elektryczny, jaki dotarł do nadajnika na odległym końcu światłowodu. Teraz sygnał ma ponownie postać zmian napięcia. Sygnał jest gotowy do wysłania przez przewód miedziany i odebrania przez urządzenie elektroniczne, takie jak komputer, przełącznik lub router. Urządzenia półprzewodnikowe, które są zazwyczaj używane jako odbiorniki w łączach światłowodowych, są nazywane fotodiodami PIN (ang. p-intrinsic-n diodes). **Fotodiody PIN** są tak skonstruowane, aby były wrażliwe na światło o długości fali 850, 1310 lub 1550 nm, które jest generowane przez nadajnik na odległym końcu światłowodu. Gdy na fotodiode PIN padnie impuls światła o odpowiedniej długości fali, wytworzy ona szybko prąd elektryczny o napięciu odpowiednim dla sieci. Gdy tylko światło przestaje padać na fotodiode PIN, ustaje wytwarzanie napięcia. Powoduje to zmiany napięcia w kablu miedzianym; zmiany te odpowiadają jedynkom i zerom, za pomocą których zapisano dane. **Do końców światłowodu podłączane są złącza, dzięki czemu światłowód może być podłączony jedynie do portów w nadajniku lub odbiorniku. Najczęściej stosowanym typem złącza w światłowodach wielomodowych jest złącze SC (Subscriber Connector). W światłowodzie jednomodowym najczęściej stosowane jest złącze ST (Straight Tip).**



W sieciach optycznych oprócz niezbędnych urządzeń, takich jak nadajniki, odbiorniki, złącza i światłowody, często spotkać można wtórniiki i panele połączeniowe światłowodów. **Wtórniiki** są optycznymi wzmacniaczami, które odbierają osłabione impulsy światła poruszającego się na dużych odcinkach i przywracają im pierwotny kształt, natężenie i czas trwania. Te zregenerowane sygnały mogą być następnie przesłane w dalszą drogę do odbiornika znajdującego się na odległym końcu światłowodu. **Panele połączeniowe** światłowodów są podobne do paneli połączeniowych używanych w przypadku kabli miedzianych. Panele te zwiększały elastyczność sieci optycznych, umożliwiając szybkie zmiany połączeń między urządzeniami, takimi jak przełączniki i routery, a różnymi dostępnymi wiązkami światłowodów lub połączeniami kablowymi.

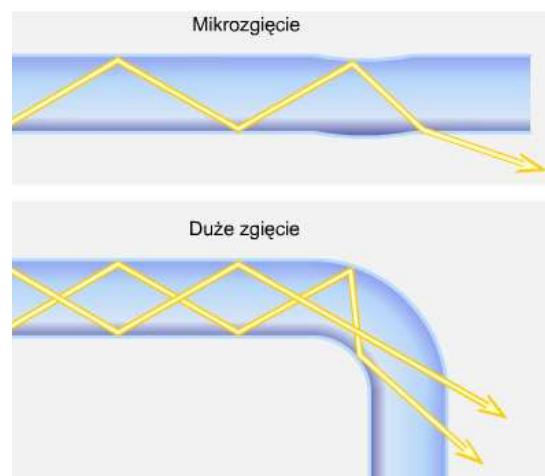
### 3.2.9 Sygnały i szумy w światłowodach

Na kabel światłowodowy nie wywierają wpływu zewnętrzne źródła szumu, stanowiące problem w przypadku mediów miedzianych, ponieważ światło zewnętrzne nie może dostać się do światłowodu, z wyjątkiem punktu po stronie nadajnika. Płaszczyzny okrywają bufor i koszulkę zewnętrzną, uniemożliwiając światłu przedostanie się do środka lub wydostanie się z kabla. Co więcej, transmisja światła w jednym ze znajdujących się w kablu światłowodów nie powoduje zakłóceń transmisji w żadnym innym światłowodzie. Oznacza to, że w światłowodzie nie występują problemy z przesłuchem, spotykane w mediach miedzianych. W rzeczywistości jakość łącz światłowodowych jest tak dobra, że najnowsze standardy dotyczące sieci Ethernet o prędkości jednego gigabita i dziesięciu gigabitów na sekundę określają zasięg transmisji, który dalece przekracza tradycyjny dwukilometrowy zasięg pierwszych sieci Ethernet. Transmisja światłowodowa umożliwia używanie protokołu sieci Ethernet w sieciach miejskich (MAN) i rozległych (WAN). Mimo iż

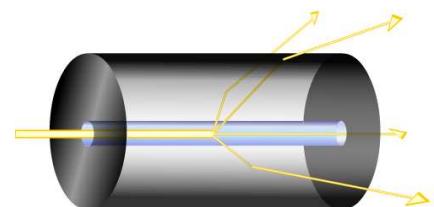


światłowód jest najlepszym z mediów transmisyjnych, przenoszącym duże ilości danych na znaczne odległości, nie jest on pozbawiony wad. Gdy światło przesyłane jest światłowodem, część jego energii jest tracona. Wraz ze wzrostem odległości, na którą jest przesyłany sygnał świetlny w sieci, maleje jego moc. Tłumienie sygnału spowodowane jest wieloma czynnikami, w tym naturą samego światłowodu. Najbardziej istotnym czynnikiem jest rozpraszanie. Rozpraszanie światła w światłowodzie jest spowodowane przez mikroskopijne niejednorodności (zniekształcenia) w jego strukturze, które odbijają i rozpraszają część energii świetlnej. Kolejną przyczyną utraty energii świetlnej jest pochłanianie. Kiedy promień światła pada na pewne typy zanieczyszczeń chemicznych, traci część swojej energii. Energia świetlna jest wtedy przekształcana w małe ilości energii cieplnej. Pochłanianie sprawia, że sygnał świetlny staje się przytłumiony. Innymi czynnikami powodującymi tłumienność sygnału świetlnego są nieregularności powstałe podczas produkcji rdzenia lub chropowatości występujące na granicy między rdzeniem a płaszczem. Sygnał świetlny traci moc z powodu nieidealnego całkowitego odbicia wewnętrznego w nierównym obszarze światłowodu. Każda mikroskopijna niedoskonałość w grubości lub symetrii światłowodu będzie miała wpływ na całkowite odbicie wewnętrzne, zaś płaszcz pochłonie część energii świetlnej. Dyspersja impulsu światła również ogranicza odległość transmisji w światłowodzie. Dyspersja to termin techniczny dotyczący rozprzestrzeniania się impulsów świetlnych podczas ich drogi w światłowodzie. Światłowód wielomodowy o gradientowym współczynniku załamania został zaprojektowany w celu kompensacji różnicy długości różnych modów, przez które przechodzi światło w rdzeniu o dużej średnicy. W światłowodzie jednomodowym nie występuje problem wielu ścieżek, którymi światło może się przemieszczać. Jednakże dyspersja chromatyczna występuje zarówno w światłowodzie wielomodowym jak i jednomodowym. Powodem występowania dyspersji chromatycznej jest różna prędkość przechodzących przez szkło fal świetlnych o różnych długościach. Na tej samej zasadzie światło jest rozszczepiane przez pryzmat. W idealnym przypadku dioda LED lub laser powinny emitować światło o tylko jednej częstotliwości. Wtedy dyspersja chromatyczna nie stanowiłaby problemu. Niestety, lasery, a w jeszcze większym stopniu diody LED, generują szereg fal o różnych długościach, więc dyspersja chromatyczna ogranicza odległość, na którą sygnał może być transmitowany w światłowodzie. Jeśli sygnał zostanie przesłany na zbyt dużą odległość to to, co było na początku jasnym impulsem energii świetlnej, dotrze do odbiornika rozmyte, rozszczepione i przyciemnione. Odbiornik nie będzie w stanie odróżnić jedynki od zera.

### 3.2.10 Instalowanie, konserwacja i testowanie światłowodu



Główna przyczyna zbyt dużej tłumienności światłowodu jest niewłaściwa instalacja. Jeśli światłowód zostanie rozciągnięty lub zbyt mocno wygięty, w jego rdzeniu mogą powstać mikroskopijne



pęknięcia, które będą rozpraszać promienie światła. Zbyt mocne zagięcie światłowodu może zmienić kąt padania promienia padającego na granicę między rdzeniem a płaszczem. W takim wypadku kąt padania może stać się mniejszy niż kąt krytyczny dla całkowitego odbicia wewnętrznego. Zamiast odbić się od zgięcia, niektóre promienie światła przedostaną się do płaszcza i zostaną utracone. Aby zapobiec zbyt mocnemu zgięciu światłowodu, jest on zazwyczaj prowadzony przez pewien typ zainstalowanej rury zwanej rurą przelotową. Rura przelotowa jest znacznie sztywniejsza od światłowodu i nie może zostać wygięta tak mocno, aby światłowód

znajdujący się w niej został zbyt mocno zakrzywiony. Rura przelotowa zabezpiecza światłowód, ułatwia jego przeciaganie i gwarantuje, że kąt zgięcia (granica krzywizny) światłowodu nie zostanie przekroczony. Kiedy światłowód zostanie przeciągnięty, jego końcówki muszą zostać odpowiednio przycięte i wypolerowane, aby uzyskać gładkie zakończenie. Do badania gładkości i kształtu końcówek światłowodu używany jest mikroskop lub przyrząd testowy z wbudowaną lupą. Następnie na końcówkę światłowodu starannie nakładane jest złącze. Nieprawidłowo zainstalowane złącza, nieprawidłowe połączenie lub połączenie dwóch kabli o różnej średnicy rdzenia powodują znaczne osłabienie sygnału świetlnego. Kiedy światłowód i złącza zostaną zainstalowane, złącza i końcówki światłowodów muszą być utrzymywane w nieskazitelnej czystości. Na końcówkach światłowodu powinny być założone zaślepki ochronne, które zapobiegają ich uszkodzeniu. Przed podłączeniem światłowodu do portu w przełączniku lub routerze należy zdjąć zaślepki, a końcówki światłowodu muszą zostać oczyszczone. Końcówki światłowodu należy czyścić pozbawioną włókien szmatką do soczewek i czystym alkoholem izopropylowym. Porty światłowodu w przełączniku lub routerze również powinny być zakryte, gdy nie są używane, i czyszczone ściereczką do soczewek oraz alkoholem izopropylowym przed wykonaniem połączenia.

Zabrudzone końcówki światłowodu powodują znaczny spadek ilości światła docierającego do odbiornika.

Rozpraszanie, pochłanianie, dyspersja, nieprawidłowa instalacja i zabrudzone końcówki światłowodu zmniejszają siłę sygnału świetlnego i określano są jako szum światłowodowy. Przed użyciem kabla światłowodowego należy go przetestować, aby upewnić się, że do odbiornika dociera wystarczająca ilość światła umożliwiająca wykrycie zer i jedynek w sygnale. Podczas planowania łączą światłowodowego należy obliczyć możliwą do tolerowania wielkość utraty mocy. Określa się to jako budżet tłumienności optycznej. Tak jak budżet domowy. Gdy wszystkie stałe wydatki zostaną odjęte od przychodu, pozostać musi wystarczająca ilość pieniędzy na przetrwanie miesiąca.

Decybel (dB) jest jednostką używaną do pomiaru wielkości utraty sygnału. Mówi ona, jaka część mocy wysyłanej przez nadajnik w rzeczywistości dociera do odbiornika.

## Wykończenia powierzchni zakończenia włókna

Płaskie: Zakończenie powoduje odbicie światła z powrotem do włókna w wyniku skokowej zmiany współczynnika załamania spowodowanej połączeniem szkło-powietrze-szkło.

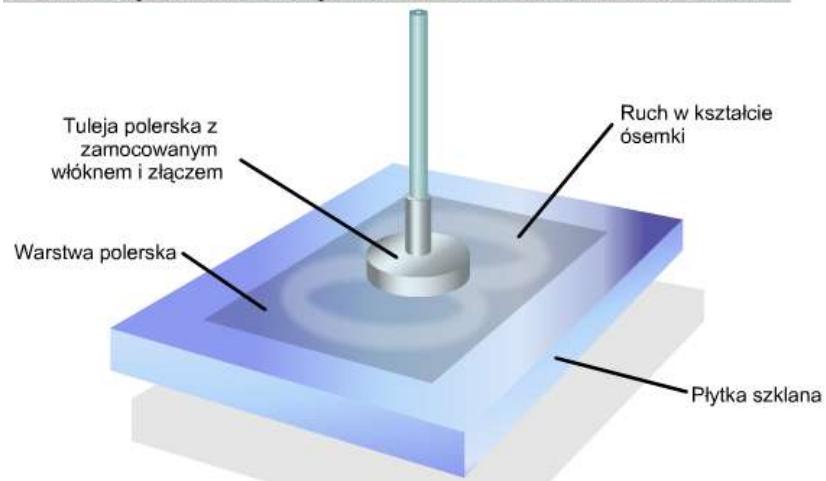
Pod kątem: Wypolerowane złącza powodują wydostanie się odbitego światła poza rdzeń i rozproszenie w płaszczu.

Kontakt fizyczny: Zakończenie zmniejsza odbicie z powrotem do włókna dzięki temu, że nieciągłość współczynnika załamania jest bardzo mała.

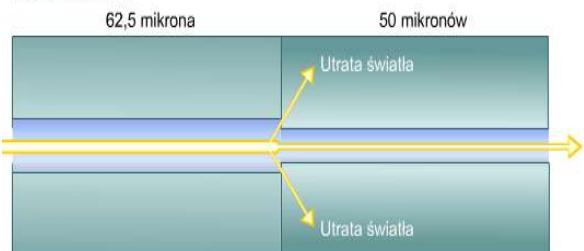
Ultragładkie: Do polerowania zakończeń złącza używane są różne rodzaje warstw polerskich, co zapewnia wyjątkowo gładką powierzchnię.



## Techniki polerowania powierzchni zakończenia włókna



### Spawanie



utworzenie standardu, który odpowiadałby rozwiązaniom producentów. **Standard 802.11b** jest nazywany również standardem Wi-Fi™ lub standardem dla sieci bezprzewodowych o dużej szybkości i dotyczy systemów DSSS, które pracują z szybkością 1, 2, 5,5 i 11 Mb/s. Wszystkie systemy 802.11b są zgodne wstępnie, gdyż obsługują również system 802.11 dla szybkości 1 i 2 Mb/s, lecz tylko w przypadku technologii DSSS. Zgodność z poprzednimi wersjami jest szczególnie ważna, ponieważ umożliwia modernizację sieci bezprzewodowej bez potrzeby wymiany kart sieciowych lub punktów dostępu. **Urządzenia 802.11b** uzyskują wyższe szybkości przesyłania danych dzięki zastosowaniu innej techniki kodowania niż w przypadku 802.11, umożliwiając przesłanie większej ilości danych w tej samej ramce czasowej.

Większość urządzeń 802.11b wciąż nie osiąga pasma 11 Mb/s i pracuje głównie z szybkością od 2 do 4 Mb/s. **Standard 802.11a** dotyczy urządzeń sieci WLAN pracujących w paśmie transmisyjnym 5 GHz. Użycie pasma 5 GHz uniemożliwia współdziałanie z urządzeniami standardu 802.11b, ponieważ pracują one w paśmie 2,4 GHz. Urządzenia 802.11a są w stanie dostarczyć dane z szybkością 54 Mb/s, a przy zastosowaniu technologii zwanej „podwajanie szybkości”, uzyskano szybkość 108 Mb/s. W środowisku produkcyjnym bardziej typową szybkością jest 20–26 Mb/s. **Standard 802.11g** zapewnia takie samo pasmo jak 802.11a, ale jest zgodny wstępnie z urządzeniami 802.11b, używając technologii modulacji OFDM (Orthogonal Frequency Division Multiplexing) oraz korzystając z pasma 2,4 GHz. Firma Cisco opracowała punkt dostępu pozwalający na jednoczesne zastosowanie urządzeń zgodnych ze standardami 802.11b i 802.11a w tej samej sieci WLAN. Punkt dostępu oferuje usługi „bramy”, umożliwiając komunikację pomiędzy urządzeniami, które inaczej nie mogłyby się komunikować.

Testowanie łączy światłowodowych jest bardzo istotne i należy przechowywać wyniki tych testów. Używanych jest kilka rodzajów sprzętu do testowania światłowodów. Dwa najważniejsze przyrządy to miernik utraty mocy optycznej i optyczny reflektometr (OTDR).

Oba te mierniki służą do testowania kabla optycznego i sprawdzania, czy kabel spełnia standardy TIA dotyczące światłowodu. Za ich pomocą można także sprawdzić, czy utrata mocy łącza nie spada poniżej budżetu tłumienności optycznej. Mierniki OTDR mogą dostarczyć dodatkowych szczegółowych informacji diagnostycznych na temat łącza światłowodowego. Mogą w ten sposób zostać użyte do rozwiązywania ewentualnych problemów z łączem.

### 3.3 Media bezprzewodowe

#### 3.3.1. Organizacje i standardy dotyczące bezprzewodowej sieci LAN

Zrozumienie przepisów i standardów dotyczących technologii bezprzewodowych sprawi, że wdrażane sieci będą współpracowały ze sobą i będą zgodne z tymi standardami. Podobnie jak w wypadku sieci kablowych, głównym twórcą standardów obowiązujących w sieciach bezprzewodowych jest organizacja IEEE. Standardy te zostały utworzone na kanwie przepisów podstawowych wydanych przez komisję FCC (Federal Communications Commission).

Podstawową technologią opisaną w standardzie 802.11 jest DSSS (Direct Sequence Spread Spectrum). Technologia DSSS dotyczy urządzeń bezprzewodowych pracujących w zakresie

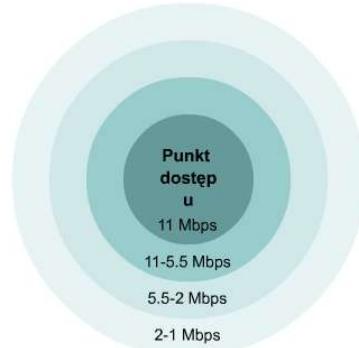
szbkości od 1 do 2 Mb/s. System używający technologii DSSS może pracować z szybkością do 11 Mb/s, nie będzie jednak uważany za zgodny ze standardem, jeśli szybkość przekracza 2 Mb/s. Kolejnym zatwierdzonym standardem był standard 802.11b, w którym prędkość transmisji zwiększo do 11 Mb/s. Chociaż sieci WLAN DSSS były w stanie współpracować z sieciami WLAN FHSS (Frequency Hopping Spread Spectrum), występowały problemy, które zmusiły producentów do zmian w projekcie. W tym wypadku zadaniem IEEE stało się

### 3.3.2 Urządzenia bezprzewodowe i topologie sieci bezprzewodowych

Sieć bezprzewodową mogą stanowić już dwa urządzenia. – Węzłami mogą być komputery osobiste lub komputery przenośne. Dzięki bezprzewodowym kartom sieciowym można łatwo utworzyć sieć „ad hoc” porównywalną z przewodową siecią równorzędną. Oba urządzenia pracują w tym środowisku jako serwery i klienci. Mimo iż łączność jest zapewniona, zabezpieczenia są minimalne, podobnie jak przepustowość. Innym problemem w tego typu sieci jest zgodność. Często zdarza się, że bezprzewodowe karty sieciowe pochodzące od różnych producentów nie chcą ze sobą współpracować. Aby rozwiązać problem zgodności, często instalowany jest punkt dostępu (access point – AP), który działa jak centralny hub pracujący w trybie infrastruktury sieci WLAN. Punkt dostępu jest wpinany do kablowej sieci LAN w celu umożliwienia dostępu do Internetu i łączności z siecią przewodową. Punkt dostępu jest wyposażony w antenę i zapewnia łączność bezprzewodową na określonym obszarze zwanym komórką. W zależności od infrastruktury lokalizacji, w której zainstalowany jest punkt dostępu, oraz rozmiaru i wzmocnienia anteny, rozmiary komórek mogą się znacznie różnić. Najczęściej przedział wielkości będzie wynosił od 90 do 150 metrów. Aby obsługiwać większe obszary, można zainstalować wiele punktów dostępu, których zasięgi będą się częściowo pokrywać. Pokrywanie umożliwia „roaming” pomiędzy komórkami. Przypomina to usługi oferowane przez dostawców usług telefonii komórkowej. Pokrywanie się zasięgów w sieciach złożonych z wielu punktów dostępu ma zasadnicze znaczenie, jeśli chodzi o zapewnienie mobilności urządzeń wewnętrz sieci WLAN. Mimo iż nie jest to określone w standardach IEEE, pożąданie jest pokrywanie się rzędu 20–30%. Taki stopień pokrywania ułatwia przechodzenie pomiędzy komórkami, umożliwiając płynne podłączanie i rozłączanie, bez przerywania dostępu do usług. Po aktywizacji klienta sieci WLAN zaczyna on „nasłuchiwać” zgodnego urządzenia, z którym zostanie „skojarzony”. Operacja ta jest nazywana „skanowaniem” i może być aktywna lub pasywna. **Skanowanie aktywne** polega na wysyłaniu ramki próbującej z węzła, który chce się dołączyć do sieci. Ramka ta będzie zawierać identyfikator SSID (Service Set Identifier) sieci, z którą urządzenie chce się połączyć. Gdy zostanie odnaleziony punkt dostępu o takim samym identyfikatorze SSID, punkt ten wysła ramkę z odpowiedzią. W ten sposób kończy się etap uwierzytelniania i przypisania. **Węzły skanowania pasywnego** nasłuchują ramek zarządzających (sygnałów nawigacyjnych) wysyłanych przez punkty dostępu (tryb infrastruktury) i przez równorzędne węzły klienckie (tryb ad hoc). Po odebraniu przez węzeł sygnału nawigacyjnego zawierającego identyfikator SSID sieci, z którą ma nastąpić połączenie, następuje próba połączenia z tą siecią. Skanowanie pasywne jest procesem ciągłym, a węzły mogą tworzyć lub usuwać przypisanie z punktami dostępu w zależności od siły sygnału.

### 3.3.3 W jaki sposób następuje komunikacja w bezprzewodowej sieci LAN

Po ustaleniu połączenia z siecią WLAN, węzeł przesyła ramki w taki sam sposób, jak w każdej innej sieci 802.x. Jednakże sieci WLAN nie używa się ramek standardu 802.3. Z tego względu określenie bezprzewodowa sieć Ethernet jest mylące. Istnieją trzy typy ramek: sterujące, zarządzające i danych. Tylko ramki danych są podobne do ramek 802.3. Rozmiar danych użytkowych w ramkach bezprzewodowych i ramkach 802.3 wynosi 1500 bajtów, jednakże ramka sieci Ethernet nie może przekroczyć rozmiaru 1518 bajtów, podczas gdy ramki sieci bezprzewodowej mogą mieć rozmiar do 2346 bajtów. Zazwyczaj rozmiar ramki WLAN będzie ograniczony do 1518 bajtów, ponieważ sieć bezprzewodowa jest najczęściej podłączona do kablowej sieci Ethernet. Ponieważ częstotliwości radiowe (RF) to medium dzielone, może wystąpić kolizja, podobnie jak to się zdarza w dzielonych mediach przewodowych. Główna różnica jest taka, że nie istnieje metoda, dzięki której węzeł źródłowy mógłby wykryć wystąpienie kolizji. Z tego względu w sieciach WLAN używana jest metoda CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Jest ona podobna do metody CSMA/CD stosowanej w sieciach Ethernet. Po wysłaniu ramki przez węzeł źródłowy, węzeł odbiorczy zwraca potwierdzenie (ACK). Może to spowodować zużycie 50% dostępnego pasma. Ten narzuca w porównaniu z narzutem protokołu unikania kolizji zmniejszą rzeczywistą przepustowość maksymalnie do 5,0–5,5 Mb/s w bezprzewodowej sieci LAN 802.11b o przepustowości 11 Mb/s. Na wydajność sieci ma również wpływ siła sygnału i pogorszenie jakości sygnału spowodowane odległością lub zakłóceniami. W miarę pogarszania sygnału może zostać zastosowana metoda adaptacyjnego wyboru szybkości ARS (Adaptive Rate Selection). Powoduje to spadek szybkości transmisji z 11 Mb/s do 5,5 Mb/s, z 5,5 Mb/s do 2 Mb/s lub z 2 Mb/s do 1 Mb/s.



#### Ramki zarządzania

- Ramka żądania przypisania
- Ramka odpowiedzi przypisania
- Ramka żądania próbkowania
- Ramka odpowiedzi próbkowania
- Ramka sygnału nawigacyjnego
- Ramka uwierzytelniania

#### Ramki sterujące

- Żądanie wysłania (RTS)
- Gotowość do nadawania (CTS)
- Potwierdzenie

#### Ramki danych

oną podobna do metody CSMA/CD stosowanej w sieciach Ethernet. Po wysłaniu ramki przez węzeł źródłowy, węzeł odbiorczy zwraca potwierdzenie (ACK). Może to spowodować zużycie 50% dostępnego pasma. Ten narzuca w porównaniu z narzutem protokołu unikania kolizji zmniejszą rzeczywistą przepustowość maksymalnie do 5,0–5,5 Mb/s w bezprzewodowej sieci LAN 802.11b o przepustowości 11 Mb/s. Na wydajność sieci ma również wpływ siła sygnału i pogorszenie jakości sygnału spowodowane odległością lub zakłóceniami. W miarę pogarszania sygnału może zostać zastosowana metoda adaptacyjnego wyboru szybkości ARS (Adaptive Rate Selection). Powoduje to spadek szybkości transmisji z 11 Mb/s do 5,5 Mb/s, z 5,5 Mb/s do 2 Mb/s lub z 2 Mb/s do 1 Mb/s.

### 3.3.4 Uwierzytelnianie i przypisanie

Uwierzytelnianie w sieci WLAN następuje w warstwie 2. Jest to proces uwierzytelniania urządzenia, a nie użytkownika. To bardzo ważne zagadnienie, o którym należy pamiętać podczas rozpatrywania bezpieczeństwa sieci WLAN, rozwiązywania problemów oraz ogólnego zarządzania. Uwierzytelnianie może być wyłączone, tak jak w przypadku nowego punktu dostępu i karty sieciowej używających domyślnych konfiguracji. Klient wysyła ramkę żądania uwierzytelnienia do punktu dostępu, gdzie ramka zostaje zaakceptowana lub odrzucona. Klient jest powiadamiany o wyniku za pomocą ramki odpowiedzi uwierzytelniania. Punkt dostępu może być również skonfigurowany do przekazywania zadania uwierzytelniania do specjalnego serwera, który w tym celu może przeprowadzać bardziej złożone procesy. Przypisanie wykonywane po uwierzytelnieniu jest stanem, który umożliwia klientowi korzystanie z usług punktu dostępu przy transmisji danych.

## Typy uwierzytelniania i przypisania

Nieuwierzytelnione i nieprzypisane

Węzeł jest odłączony od sieci i nie jest przypisany do punktu dostępu.

Uwierzytelnione i nieprzypisane

Węzeł został uwierzytelniony w sieci, ale nie jest jeszcze przypisany do punktu dostępu. Uwierzytelnione i przypisane

Węzeł jest podłączony do sieci i może nadawać i odbierać dane poprzez punkt dostępu.

**Metody uwierzytelniania** W zaleceniu IEEE 802.11 wymieniono dwa typy procesu uwierzytelniania. Pierwszym procesem uwierzytelniania jest system otwarty. Jest to standard otwartej łączności, w której jedynie identyfikator SSID musi być zgodny. Może on być używany w środowisku zabezpieczonym lub niezabezpieczonym, ale ryzyko podsłuchu na niskim poziomie w celu odkrycia identyfikatora SSID sieci WLAN jest wysokie.

Drugim procesem jest współdzielony klucz. Proces ten wymaga użycia szyfrowania WEP (Wired Equivalent Privacy). WEP to prosty algorytm używający kluczy 64- i 128-bitowych. Punkt dostępu jest skonfigurowany z kluczem szyfrującym, a węzły próbujące uzyskać dostęp do sieci poprzez ten punkt dostępu muszą mieć odpowiadający mu klucz. Statycznie przypisane klucze WEP zapewniają wyższy poziom bezpieczeństwa niż system otwarty, ale na pewno nie są odporne na włamania. **Problem** nieuprawnionego dostępu do sieci WLAN znalazł rozwiązanie w wielu nowych technologiach zabezpieczeń.

### 3.3.5 Widmo fal radiowych i mikrofal

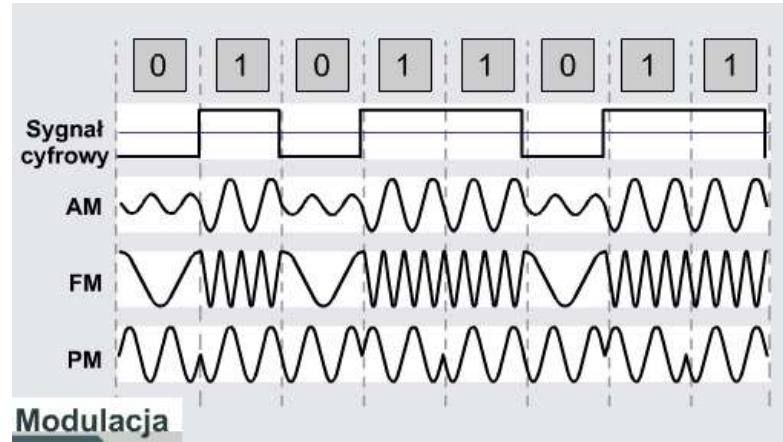
Komputery wysyłają i odbierają sygnały danych w postaci elektronicznej. Nadajniki radiowe konwertują te sygnały elektryczne na fale radiowe. Zmiana prądu elektrycznego w antenie nadajnika powoduje wygenerowanie fali radiowej. Te fale radiowe rozchodzą się z anteny po liniach prostych. Fale radiowe są jednak tłumione w miarę oddalania się od anteny nadawczej. W sieci WLAN sygnał radiowy mierzony w odległości 10 metrów od anteny nadawczej będzie miał tylko 1/100 oryginalnej mocy. Podobnie jak światło, fale radiowe mogą być pochłaniane przez niektóre ośrodki i odbijane przez inne. Przy przechodzeniu z jednego ośrodka, jak na przykład

powietrze, do innego ośrodka, jak na przykład gipsowa ściana, fale radiowe ulegają załamaniu. Fale radiowe są również rozpraszane i pochłaniane przez krople wody w powietrzu. Te właściwości fal radiowych należy brać pod uwagę podczas planowania sieci WLAN w budynku lub kampusie. Proces oceny lokalizacji przeznaczonej na instalację sieci WLAN jest określany jako „wywiad techniczny”. Ponieważ sygnały radiowe słabną w miarę oddalania się od nadajnika, odbiornik musi być również wyposażony w antenę. Gdy fale radiowe dotrą do anteny, w antenie zostaną wygenerowane słabe prądy elektryczne. Prądy elektryczne wywołane odebranymi falami radiowymi odpowiadają prądom, które pierwotnie wygenerowały fale radiowe w antenie nadajnika. Odbiornik wzmacnia te słabe sygnały elektryczne. W nadajniku sygnały elektryczne (dane) pochodzące z komputera lub sieci LAN nie są bezpośrednio wysyłane do anteny nadajnika. Sygnały te są używane do zmiany drugiego, silniejszego sygnału zwanego nośną. Proces zmiany sygnału nośnej, która jest przesyłana do anteny, jest nazywany modulacją. Istnieją trzy podstawowe sposoby modulacji sygnału nośnej. Na przykład, stacje radiowe stosujące modulację amplitudową (AM) modulują wysokość (amplitude) sygnału nośnej. Stacje radiowe stosujące modulację częstotliwościową (FM) modulują częstotliwość sygnału nośnej za pomocą sygnału elektrycznego z mikrofonu. W sieciach WLAN stosowany jest trzeci typ modulacji nazywany modulacją fazową (PM), który jest używany do nałożenia sygnału danych na sygnał nośnej emitowany przez nadajnik. W tym typie modulacji bity danych w sygnale elektrycznym zmieniają fazę sygnału nośnej. Odbiornik demoduluje sygnał nośnej, który dociera do jego anteny. Następnie interpretuje sygnały zmiany fazy sygnału nośnej i odtwarza z nich oryginalny elektryczny sygnał danych.

### 3.3.6 Sygnały i szумy w sieci WLAN

W kablowej sieci Ethernet proces diagnozowania przyczyny zakłóceń jest bardzo prosty. W przypadku użycia technologii RF należy wziąć pod uwagę wiele rodzajów zakłóceń. **Technologia wąskopasmowa** jest przeciwieństwem technologii szerokopasmowej. Jak sugeruje nazwa, wąskie pasmo nie wywiera wpływu na całe pasmo częstotliwości w sygnale bezprzewodowym. Jednym z rozwiązań problemów z zakłóceniami wąskopasmowymi może być po prostu zmiana kanału, którego używa punkt dostępu. W rzeczywistości diagnozowanie przyczyny zakłóceń wąskopasmowych może być kosztowne i czasochłonne. Identyfikacja źródła zakłóceń wymaga użycia analizatora widma, a nawet proste modele takich urządzeń są bardzo kosztowne. Wszystkie zakłócenia interferencyjne pasma mają wpływ na cały zakres pasma.

Technologia Bluetooth™, której działanie polega na przeskakiwaniu wiele razy na sekundę przez całe pasmo 2,4 GHz, może spowodować znaczne zakłócenia w sieci 802.11b. Nie jest niczym niezwykłym napotkanie w niektórych instytucjach korzystających z sieci bezprzewodowej znaku nakazującego wyłączenie przed wejściem do budynku wszystkich urządzeń korzystających z technologii Bluetooth™. Urządzeniem, które często umyka uwadze jako źródło zakłóceń, jest powszechnie używana w domach i biurach kuchenka mikrofalowa. Wyciek z kuchenki mikrofalowej energii, nawet tak niewielkiej jak jeden wat, do pasma RF może spowodować poważne zakłócenia w sieci. Telefony bezprzewodowe pracujące w paśmie 2,4 GHz mogą również powodować zakłócenia w sieci. Ogólnie rzecz biorąc, nawet najbardziej



ekstremalna pogoda nie spowoduje zakłócenia sygnału RF. Jednak mgła lub bardzo duża wilgotność może mieć wpływ na sieci bezprzewodowe. Wyładowania atmosferyczne mogą również wprowadzić do atmosfery ładunek elektryczny i zmienić drogę transmitowanego sygnału. Pierwszym i najbardziej oczywistym źródłem problemów z sygnałami jest stacja nadawcza i typ anteny. Stacja o większej mocy będzie wysyłać sygnał dalej, a antena paraboliczna, która skupia sygnał, zwiększy zasięg transmisji. W środowisku małego biura czy domu większość punktów dostępu korzysta z dwóch anten dookólnych, które transmitują sygnał we wszystkich kierunkach, kosztem zmniejszonego zasięgu.

### 3.3.7 Bezpieczeństwo w sieciach bezprzewodowych

W poprzednim rozdziale przedstawiono trudności związane z zapewnieniem bezpieczeństwa w sieci bezprzewodowej. Wszędzie tam, gdzie istnieją sieci bezprzewodowe, bezpieczeństwo jest zagrożone. Stanowiło to problem w początkowym okresie istnienia sieci WLAN. Wielu administratorów nadal nie potrafi zaimplementować efektywnej strategii zabezpieczeń. Powstało wiele nowych rozwiązań zabezpieczeń, takich jak wirtualne sieci prywatne VPN (Virtual Private Networking) i protokół EAP (Extensible Authentication Protocol). W protokole EAP punkt dostępu nie dokonuje uwierzytelniania klienta, ale przekazuje te obowiązki bardziej wyspecjalizowanemu urządzeniu, najczęściej wydzielonemu serwerowi zaprojektowanemu do tego celu. Użycie technologii zintegrowanego serwera VPN powoduje utworzenie tunelu na istniejącym protokole, takim jak IP. Jest to połączenie warstwy 3, w przeciwieństwie do połączenia warstwy 2, które istnieje pomiędzy punktem dostępu a węzłem nadawczym.

- **EAP-MD5 Challenge** – protokół EAP to najwcześniejszy typ uwierzytelniania, który jest bardzo podobny do protokołu ochrony hasła CHAP stosowanego w sieciach przewodowych.
- **LEAP (Cisco)** – protokół LEAP (Lightweight Extensible Authentication Protocol) jest głównie używany przez bezprzewodowe punkty dostępu firmy Cisco w sieciach WLAN. Protokół LEAP zapewnia bezpieczeństwo podczas wymiany poświadczeń, dokonuje szyfracji przy użyciu dynamicznych kluczy WEP i obsługuje uwierzytelnianie wzajemne.
- **Uwierzytelnianie użytkownika** – umożliwia nawiązywanie połączeń oraz wysyłanie i odbieranie danych w sieci bezprzewodowej wyłącznie uwierzytelnionym użytkownikom.
- **Szyfrowanie** – zapewnia usługi szyfrowania chroniące dane przed intruzami.
- **Uwierzytelnianie danych** – zapewnia integralność danych dzięki uwierzytelnianiu urządzenia źródłowego i docelowego.

Technologia VPN chroni skutecznie sieć bezprzewodową przed nieautoryzowanym dostępem, podczas gdy sieć WLAN, na którą nie narzucono żadnych ograniczeń, przekierowuje ruch pomiędzy wszystkimi węzłami, bez względu na to czy powinny one należeć do tej sieci czy nie. Fale radiowe często wykraczają poza obszar domu lub biura, w którym sieci są zainstalowane, zatem bez zastosowania zabezpieczeń intruzy mogą infiltrować sieć przy odrobinie wysiłku. Z drugiej strony wprowadzenie zabezpieczenia niskiego poziomu w sieci WLAN stanowi minimalny wysiłek dla administratora sieci.

#### Media transmisyjne używane w sieciach

- Kabel koncentryczny
- Skrętka ekranowana
- Skrętka nieekranowana
- Łączność bezprzewodowa

## Moduł 4: Testowanie kabli

## Wprowadzenie

Medium sieciowe w sensie dosłownym stanowi fizyczny szkielet sieci. Zła jakość okablowania sieciowego powoduje awarie sieci i spadek wydajności. Wszystkie media, takie jak przewody miedziane, światłowody oraz media bezprzewodowe, wymagają testowania w celu określenia ich zgodności ze ścisłe określonymi normami. Z testowaniem okablowania wiążą się pewne pojęcia matematyczne i elektroniczne, takie jak sygnał, fala, częstotliwość i szum. Znajomość tych pojęć pomaga w opanowaniu wiedzy o sieciach, instalacji i testowaniu okablowania. Aby sieć lokalna funkcjonowała prawidłowo, media warstwy fizycznej powinny być zgodne ze specyfikacjami określonymi w standardach branżowych. Tłumienie czyli słabnięcie sygnału oraz szum czyli interferencja sygnałów mogą powodować problemy w sieciach, ponieważ przesypane dane mogą zostać zniekształcone do tego stopnia, że po odebraniu zostaną źle zinterpretowane lub staną się zupełnie nieczytelne. Prawidłowe wykonanie złączy i właściwa instalacja okablowania są w związku z tym bardzo istotne. Jeśli instalacja, naprawa czy dokonywane zmiany będą zgodne ze standardami, to tłumienie i poziomy szumu powinny zostać znacznie zminimalizowane. Po zainstalowaniu kabla można użyć urządzenia certyfikującego, które sprawdzi czy zostały spełnione wymagania standardów TIA/EIA.

### 4.1 Wprowadzenie do testowania kabli opartego na częstotliwości

#### 4.1.1 Fale

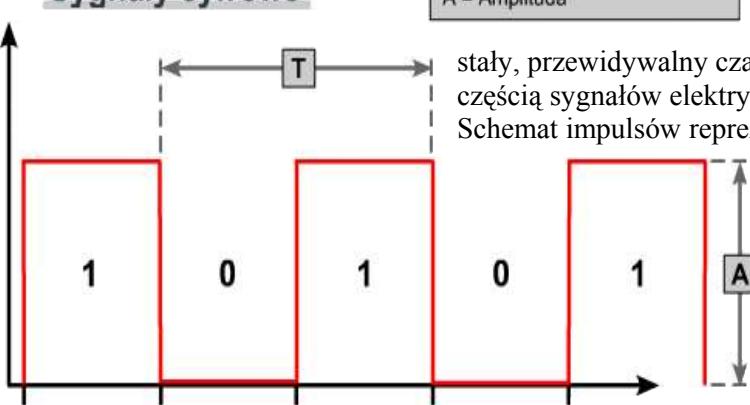
Fala stanowi sposób przenoszenia energii z miejsca na miejsce. Istnieje wiele rodzajów fal, ale wszystkie można opisać za pomocą podobnej terminologii. Fale można wyobrazić sobie jako zaburzenia. W całkowicie nieruchomym wiadrze z wodą nie ma fal, ponieważ nie ma zaburzeń. Natomiast w morzu zawsze istnieją wykrywalne fale wynikające z takich zaburzeń, jak wiatr i pływy. Możliwe jest podanie w metrach wysokości, czyli amplitudy fal morskich. Fala może zostać opisana również ze względu na to, jak często uderza w brzeg. Tę cechę określa się za pomocą okresu i częstotliwości. Okres fali to mierzona w sekundach ilość czasu, jaka upływa między uderzeniem dwóch kolejnych fal o brzeg. Częstotliwość to liczba fal, które uderzają w brzeg w ciągu jednej sekundy; mierzy się ją w hercach (Hz). Jeden herc odpowiada jednej fali na sekundę, czyli jednemu cyklowi na sekundę. Aby lepiej zapoznać się z tymi pojęciami, należy poeksperymentować, zmieniając amplitudę i częstotliwość fali na ilustracji. Specjalistów w dziedzinie sieci zazwyczaj interesują fale napięcia w medium miedzianym, fale świetlne w światłowodzie i rozchodzące się w przestrzeni zaburzenia pól elektrycznych i magnetycznych, zwane falami elektromagnetycznymi. Amplituda sygnału elektrycznego nadal odpowiada wysokości fali, ale mierzona jest w woltach (V), a nie w metrach (m). Okres fali to mierzona w sekundach ilość czasu potrzebna na

przejście pełnego cyklu zmian napięcia. Częstotliwość jest to mierzona w hercach (Hz) liczba pełnych cykli na sekundę. Jeśli zaburzenie zostało wywołane celowo i ma przejście pełnego cyklu zmian napięcia. Częstotliwość jest to mierzona w hercach (Hz) liczba pełnych cykli na sekundę. Jeśli zaburzenie zostało wywołane celowo i ma

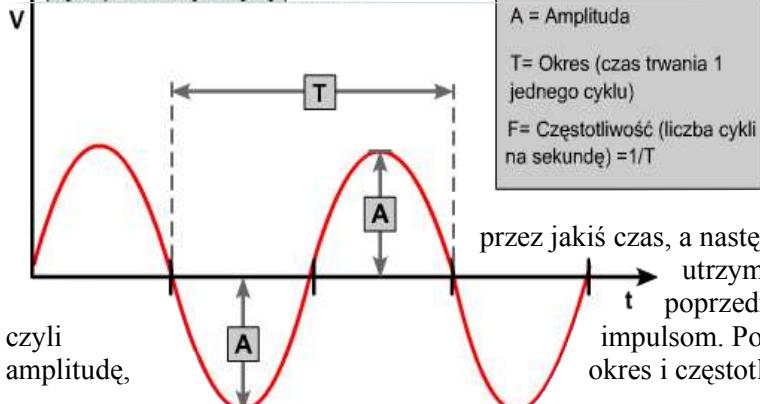
A = Amplituda

stały, przewidywalny czas trwania, nazywane jest impulsem. Impulsy są ważną częścią sygnałów elektrycznych, ponieważ stanowią podstawę transmisji cyfrowej. Schemat impulsów reprezentuje tu wartości transmitowanych danych.

#### Sygnały cyfrowe



- Impulsy dyskretnie (nieciągłe)
- Możliwe są tylko dwa stany (1/0, włączony/wyłączony)
- Napięcie przeskakuje między poziomami



czyli amplitudę,

- Ciągły przebieg napięcia
- Napięcie zmienia się w czasie
- Możliwe różne rodzaje kodowania

A = Amplituda

T = Okres (czas trwania 1 jednego cyklu)

F = Częstotliwość (liczba cykli na sekundę) =  $1/T$

Najważniejsze trzy systemy liczbowe stosowane w sieciach to:

Dwójkowy: o podstawie 2

Dziesiętny: o podstawie 10

Szesnastkowy: o podstawie 16

#### 4.1.2 Fale sinusoidalne i prostokątne

Reprezentację graficzną fal sinusoidalnych stanowią krzywe zwane sinusoidami, będące wykresami pewnych funkcji matematycznych. Mają one określone cechy charakterystyczne. Funkcje te są okresowe, co oznacza, że w regularnych odstępach czasu powtarza się ten sam wzorzec. Fale sinusoidalne cechują się ciągłą zmiennością, co oznacza, że nie istnieją dwa sąsiadujące ze sobą punkty na wykresie, dla których funkcja miałaby

te samą wartość. Sinusoidy są graficznym odwzorowaniem wielu naturalnych zdarzeń, które zmieniają się równomiernie w czasie. Przykładami takich zdarzeń mogą być: zmiana odległości między Ziemią i Słońcem, zmiana wysokości podczas jazdy na diabelskim młynie czy zmiana pory wschodu słońca. Fale sinusoidalne zmieniają się w sposób ciągły, czyli stanowią przykład fal analogowych. Fale prostokątne, podobnie jak sinusoidalne, są okresowe. Ich wykresy jednak nie zmieniają się w sposób ciągły. Fala ma określoną wartość przez jakiś czas, a następnie wartość ta ulega nagłej zmianie na inną. Druga wartość utrzymuje się przez jakiś czas i również nagle powraca do poprzedniej. Fale prostokątne odpowiadają sygnałom cyfrowym, impulsom. Podobnie jak inne fale, fale prostokątne mają określoną okres i częstotliwość.

#### 4.1.3 Wykładniki i logarytmy

Przypomnijmy, że podstawa systemu liczbowego informuje, za pomocą ilu symboli zapisuje się liczby, czyli ile symboli może znaleźć się na danej pozycji. Na przykład liczby w systemie dwójkowym są zapisywane za pomocą tylko dwóch cyfr: 0 i 1. W układzie dziesiętnym istnieje dziesięć możliwych cyfr: od 0 do 9. W układzie szesnastkowym istnieje szesnaście możliwych symboli: cyfry od 0 do 9 i litery od A do F. Jak wiadomo, wartość  $10 \times 10$  można zapisać w następujący sposób:  $10^2$ . Zapis  $10^2$  oznacza dziesięć do kwadratu, czyli do potęgi drugiej. W takim zapisie 10 stanowi podstawę, a 2 — wykładnik potęgi. Wartość  $10 \times 10 \times 10$  można zapisać w następujący sposób:  $10^3$ . Zapis  $10^3$  oznacza dziesięć do sześciu, czyli do potęgi trzeciej. Podstawą nadal jest 10, ale wykładnikiem — 3. Zamieszczone poniżej ćwiczenie multimedialne umożliwia nabranie wprawy w obliczaniu potęg. Po wpisaniu wartości x obliczana jest wartość y, a po wpisaniu wartości y — wartość x. Podstawa systemu liczbowego określa także wartość cyfr na poszczególnych pozycjach. Najmniej znacząca cyfra ma wartość równą podstawa<sup>0</sup>, czyli jeden. Następna cyfra ma wartość równą podstawa<sup>1</sup>. W przypadku liczb dwójkowych wartość ta wynosi 2, dziesiętnych — 10, a szesnastkowych — 16. Zapis wykładniczy ułatwia zapisywanie bardzo dużych lub bardzo małych liczb. Znacznie łatwiej jest zapisać miliard w postaci  $10^9$  niż jako 1000000000. Zapis taki zmniejsza również ryzyko błędu. Wiele obliczeń związanych z testowaniem kabli wykonywanych jest na bardzo dużych liczbach, dlatego najczęściej używany jest zapis wykładniczy. Z zapisem wykładniczym można się zapoznać, wykonując odpowiednie ćwiczenie interaktywne. Jednym ze sposobów operowania bardzo dużymi lub bardzo małymi liczbami, które występują w sieciach, jest ich przekształcenie zgodnie z odpowiednią regułą, czyli funkcją matematyczną, zwaną logarymem. Symbolem logarytmu jest „log”, a dowolna liczba może zostać użyta jako podstawa systemu logarytmów. Jednakże, podstawa 10 ma wiele atutów, nieosiągalnych dla typowych obliczeń, przez inne liczby będące podstawami. Można powiedzieć, że podstawa 10 jest wręcz przeznaczona do typowych obliczeń. Jednakże, podstawa 10 ma wiele atutów, nieosiągalnych dla typowych obliczeń w przypadku innych liczb będących podstawami. Aby obliczyć logarytm dziesiętny liczby, należy użyć kalkulatora lub skorzystać z ćwiczenia interaktywnego. Można także obliczać logarytmy liczb niebędących potegami 10, ale nie można obliczyć logarytmu liczby ujemnej. Nauka obliczania logarytmów wykracza poza zakres tematyczny tego kursu, jednak terminologia związana z logarytmami jest powszechnie używana przy wyrażaniu wartości w decybelach oraz pomiaru intensywności sygnałów w mediach miedzianych, światłowodach i w sieciach bezprzewodowych.

#### 4.1.4 Decybele

Decybele (dB) są jednostką miary używaną do opisywania sygnałów w sieci. Pojęcie decybelu wiąże się z omówionymi już pojęciami wykładnika i logarytmu opisanymi w poprzednich częściach. Istnieją dwa wzory służące do obliczania wartości wyrażonych w decybelach:

$$dB = 10 \log_{10} (P_{\text{końcowa}} / P_{\text{odniesienia}})$$

$$dB = 20 \log_{10} (V_{\text{końcowe}} / V_{\text{odniesienia}})$$

We wzorach zastosowano następujące oznaczenia:

$P_{\text{końcowa}}$  oznacza spadek lub wzmacnienie mocy fali. Wartości wyrażane w dB (decybelach) mogą być liczbami ujemnymi co wskazuje na spadek mocy w miarę przemieszczania się fali, ale mogą także być dodatnie, wskazując na przyrost mocy po wzmacnieniu sygnału.

$\log_{10}$  oznacza, że dla liczby w nawiasie ma zostać obliczony jej logarytm dziesiętny.

$P_{\text{odniesienia}}$  jest to moc dostarczona na wyjściu wyrażona w watach (W).

$P_{\text{odniesienia}}$  jest to moc początkowa wyrażona w watach (W).

$V_{\text{końcowe}}$  jest to napięcie dostarczone na wyjściu wyrażone w woltach (V)

$V_{\text{odniesienia}}$  jest to napięcie początkowe wyrażone w woltach (V).

Pierwsze równanie służy do porównywania mocy (P), a drugie — napięcia (V). Równanie mocy stosuje się zazwyczaj do fal świetlnych płynących przez światłowód oraz do fal radiowych w powietrzu. Do fal elektromagnetycznych w kablach miedzianych stosuje się równanie napięcia. Powyższe równania mają kilka wspólnych cech. Aby obliczyć moc końcową, do wzoru  $dB = 10 \log_{10} (P_{\text{końcowa}} / P_{\text{odniesienia}})$  należy podstawić odpowiednie wartości dB i  $P_{\text{odniesienia}}$ . To równanie można zastosować, aby dowiedzieć się, ile mocy pozostaje w fali radiowej po przebyciu określonej drogi przez różne materiały. Aby bliżej zapoznać się z pojęciem decybeli, w ćwiczeniu interaktywnym wykonaj opisane poniżej przykładowe obliczenia:

Jeśli moc źródła lasera czyli  $P_{\text{odniesienia}}$  wynosi siedem mikrowatów ( $7 \times 10^{-6}$  W), a całkowita utrata mocy w łączu światłowodowym wynosi 13 dB, to jaka jest wartość mocy, która dotarła do celu?

Jeśli łączny spadek mocy w światłowodzie wynosi 84 dB, a moc źródłowego lasera ( $P_{\text{odniesienia}}$ ) wynosi jeden miliwat ( $1 \times 10^{-3}$  W), jaka jest moc dostarczanego sygnału?

Jeśli napięcie zmierzone na końcu kabla wynosi dwa mikrowolty ( $2 \times 10^{-6}$  V), a napięcie źródłowe wynosi jeden wolt, jaki jest przyrost lub utrata napięcia wyrażona w decybelach? Czy ta wartość jest dodatnia, czy ujemna? Czy oznacza ona przyrost, czy spadek napięcia?

**4.1.5 Przedstawianie sygnałów w dziedzinie czasu i częstotliwości** Jednym z najważniejszych faktów ery informacji jest możliwość przedstawienia danych oznaczających słowa, obrazy, filmy czy muzykę za pomocą zmian napięcia w przewodach i urządzeniach elektronicznych. Dane przedstawione za pomocą zmian napięcia można przekształcić w fale świetlne lub radiowe, a następnie ponownie w fale napięcia. Jako przykład rozważmy telefon analogowy. Fale dźwiękowe wytworzane przez głos osoby dzwoniącej docierają do mikrofonu w słuchawce. Mikrofon przekształca energię dźwięku w odpowiadające głosowi zmiany napięcia elektrycznego.

Gdyby wykreślić zmiany napięcia w czasie, mielibyśmy charakterystykę danego głosu. Oscyloskop stanowi ważne urządzenie elektroniczne służące do śledzenia przebiegu sygnałów elektrycznych, takich jak fale i impulsy napięcia. Oś x na

ekranie oscyloskopu oznacza czas, a oś y — napięcie lub natężenie prądu. Zazwyczaj oś y umożliwia wyświetlanie dwóch kanałów wejściowych, można więc obserwować przebiegi dwóch fal jednocześnie.

Analizowanie sygnałów za pomocą oscyloskopu nosi nazwę analizy w dziedzinie czasu, ponieważ na osi x, która odpowiada dziedzinie funkcji matematycznej, odkładany jest czas. Sygnały bada się także, analizując ich częstotliwość. W tej analizie na osi x odkładane są częstotliwości. Przebiegi na potrzeby analizy częstotliwości wykresla urządzenie nazywane analizatorem widma. Do przesyłania sygnałów elektromagnetycznych używane są różne częstotliwości, dzięki czemu sygnały nie interferują ze sobą. Przy przesyłaniu sygnałów radiowych z modulacją częstotliwości (FM, Frequency Modulation) używane są inne częstotliwości niż przy sygnałach telewizyjnych lub satelitarnych. Nastrojenie radioodbiornika na inną stację radiową polega na zmianie częstotliwości odbieranej przez radio.

#### 4.1.6 Sygnały analogowe i cyfrowe w dziedzinie czasu i częstotliwości

Aby zrozumieć złożoność problemów związanych z sygnałami w sieciach i testowaniem instalacji kablowych, zobaczymy, jak sygnały analogowe zmieniają się w zależności od czasu i częstotliwości. Rozważmy najpierw elektryczną falę sinusoidalną o pojedynczej częstotliwości w zakresie słyszalnym. Jeśli taki sygnał zostanie wysłany do głośnika, będzie można usłyszeć dźwięk.

Następnie wyobraźmy sobie kombinację kilku fal sinusoidalnych. W jej wyniku powstaje fala znacznie bardziej złożona niż fala sinusoidalna. Słyszać byłoby kilka dźwięków. Wykres kilku dźwięków składa się z pojedynczych linii odpowiadających częstotliwości każdego z nich. Wreszcie wyobraźmy sobie złożony sygnał, taki jak ludzki głos lub dźwięk instrumentu muzycznego. Sygnałowi składającemu się z wielu różnych dźwięków odpowiada widmo ciągłe.

#### 4.1.7 Szum w dziedzinie czasu i częstotliwości

Szum jest ważnym pojęciem używanym w systemach komunikacyjnych, w tym również w sieciach lokalnych. Potocznie szum oznacza niepożądane dźwięki, natomiast w terminologii telekomunikacyjnej są to niepożądane sygnały. Szum pochodzący ze źródeł naturalnych lub technologicznych dołącza się do sygnałów przenoszących dane. W każdym systemie komunikacyjnym istnieje pewna ilość szumu. Nie można go wyeliminować, niemniej jednak dobra znajomość źródeł szumu umożliwia pewne zniwelowanie jego skutków. Istnieje wiele źródeł szumu:

- pobliskie kable przenoszące sygnały z danymi;
- interferencja radiowa (RFI, radio frequency interference), czyli szum pochodzący z innych sygnałów, które są przesyłane w niedalekiej odległości;
- interferencja elektromagnetyczna (EMI, electromagnetic interference), czyli szum pochodzący z pobliskich źródeł promieniowania elektromagnetycznego, takich jak silniki i światła;
- szum laserowy w nadajniku lub odbiorniku sygnału optycznego.

Szum, który jednakowo zakłóca wszystkie częstotliwości transmisji, nazywany jest szumem białym. Szum, który wpływa tylko na wąski zakres częstotliwości, nosi nazwę szumu wąskopasmowego. Gdy biały szum zostaje wykryty przez radioodbiornik, szum ten może zakłócać wszystkie stacje radiowe. Szum wąskopasmowy zakłóca natomiast tylko transmisje kilku stacji, które nadają na podobnych częstotliwościach.

#### 4.1.8 Szerokość pasma

**Szerokość pasma** jest ważnym pojęciem używanym w systemach telekomunikacyjnych. Pojęcie to rozpatrywane inaczej w przypadku transmisji analogowej oraz cyfrowej. **Szerokość pasma**

w transmisji analogowej zazwyczaj odnosi się do zakresu częstotliwości analogowego systemu elektronicznego. Określa ona zakres częstotliwości wysyłanych przez stację radiową lub wzmacniacz elektroniczny. Jednostką przepustowości w paśmie analogowym (podobnie jak częstotliwości) jest herc. **Szerokość pasma w transmisji cyfrowej** jest rozumiana najczęściej jako przepustowość i określa, jaką ilość informacji można przesyłać z jednego miejsca do drugiego w danym przedziale czasu. Podstawową jednostką przepustowości w paśmie cyfrowym są bity na sekundę (b/s). Ponieważ w sieciach lokalnych można przesyłać dane z szybkością tysięcy milionów bitów na sekundę, przepustowość podaje się w kilobitach na sekundę (kb/s) lub megabitach na sekundę (Mb/s). Szerokość pasma jest ograniczona przez rodzaj medium fizycznego, zaawansowanie poszczególnych technologii oraz prawa fizyki. Podczas testowania kabli w celu określenia szerokości pasma kabla miedzianego w paśmie cyfrowym używa się pomiaru szerokości pasma w paśmie analogowym. **Sygnały cyfrowe są złożone z wielu sinusoidalnych fal analogowych.** Częstotliwości analogowe są emitowane z jednego końca kabla i odbierane na drugim. Podczas pomiaru porównuje się sygnał na obu jego końcach i na tej podstawie oblicza tłumienie sygnału. Ogólnie rzecz biorąc, media obsługujące szersze pasmo analogowe przy niewielkim stopniu tłumienia mają większą przepustowość w paśmie cyfrowym.

### 4.2 Sygnały i szумy

#### 4.2.1 Przesyłanie sygnałów przez kable miedziane i światłowody

W przewodzie miedzianym sygnałami przenoszącymi dane są poziomy napięcia odpowiadające zerom i jedynkom w systemie dwójkowym. Poziomy napięcia mierzy się względem napięcia zerowego zarówno w nadajniku, jak i odbiorniku. Ten poziom odniesienia nosi nazwę ziemi sygnałowej. Ważne jest, aby zarówno urządzenie nadawcze, jak i odbiorcze odwoływało się do tego samego punktu odniesienia o napięciu zero woltów. Jeśli tak jest, mówi się, że oba urządzenia są prawidłowo uziemione. Aby sieć lokalna działała prawidłowo, urządzenie odbiorcze musi właściwie interpretować zera i jedynki transmitowane jako poziomy napięcia. Ponieważ współczesne technologie sieci Ethernet zapewniają szybkości

przesyłania danych rzędu miliardów bitów na sekundę, każdy bit musi zostać zinterpretowany prawidłowo, mimo że czas jego trwania jest bardzo krótki. Oznacza to, że sygnał po przejściu przez kabel i złącza musi zachować jak najwięcej ze swojej początkowej mocy. Ponieważ pojawiać się będą coraz szybsze protokoły Ethernet, nowe instalacje należy wykonywać przy użyciu jak najlepszych kabli, złączy i urządzeń sprzągających, takich jak bloki zaciskowe i panele połączeniowe.

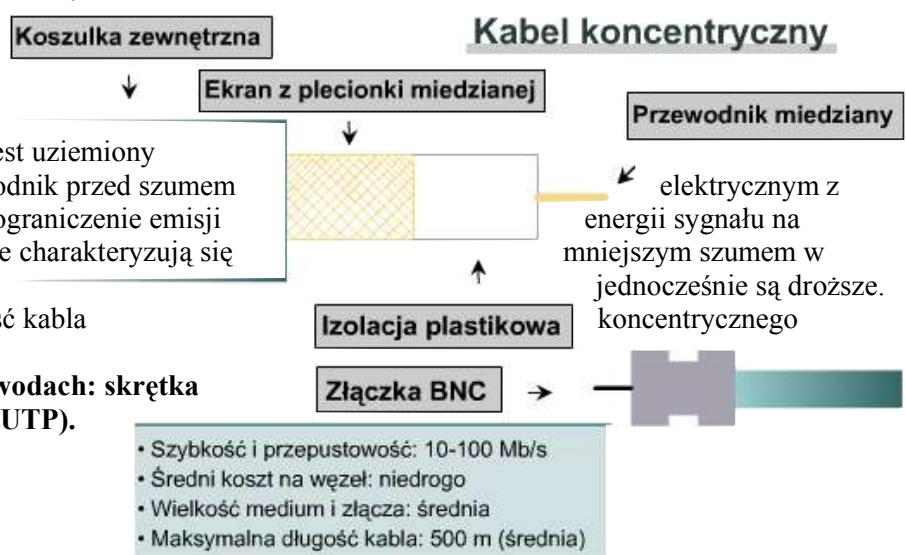
**Istnieją dwa podstawowe rodzaje kabli miedzianych: ekranowane i nieekranowane.** W kablu ekranowanym materiał ekranujący ma za zadanie zabezpieczenie sygnału przenoszącego dane przed szumem pochodząącym ze źródeł zewnętrznych oraz przed szumem generowanym przez sygnały elektryczne w kablu.

#### Przykładem takiego kabla jest kabel koncentryczny

Składa się on ze litego

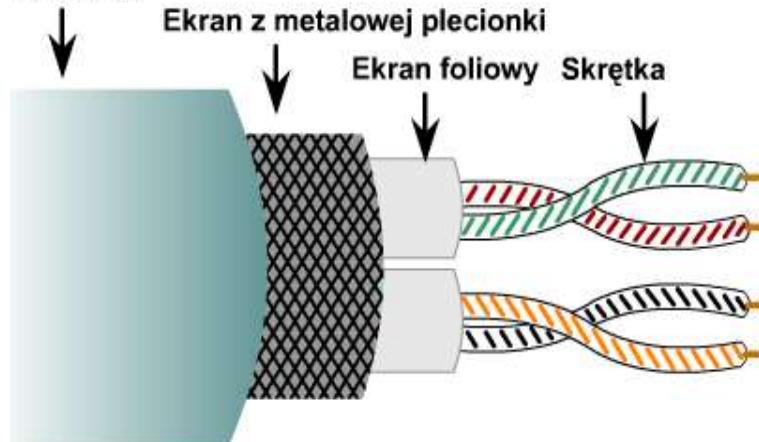
przewodu miedzianego otoczonego materiałem izolacyjnym, a następnie ekranem plecionym z drugiego przewodnika. W sieciach LAN ekran jest uziemiony elektrycznie, co zabezpiecza wewnętrzny przewodnik przed szumem zewnętrzny. Ekran zmniejsza także straty poprzez ograniczenie emisji zewnętrz kabla. Dzięki temu kable koncentryczne charakteryzują się porównaniu z innymi kablami miedzianymi, ale Ponadto konieczność uziemienia ekranu i grubość kabla utrudnia jego instalację.

**Istnieją dwa rodzaje kabli o skręconych przewodach: skrętka ekranowana (STP) i skrętka nieekranowana (UTP).**

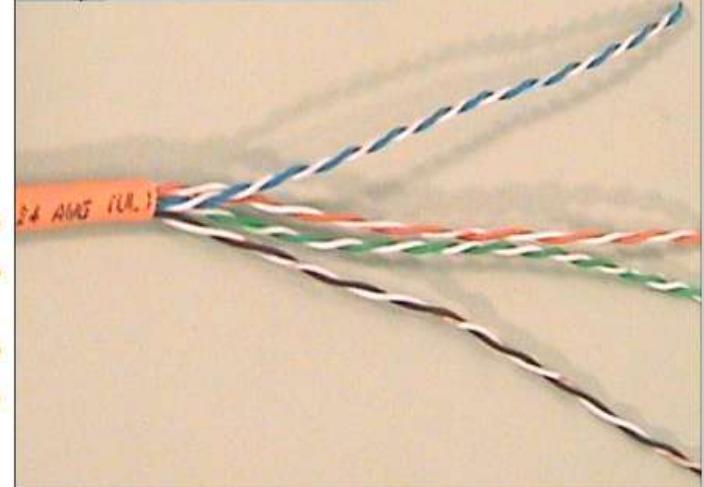


#### Skrętka ekranowana

Koszulka



#### Skrętka nieekranowana

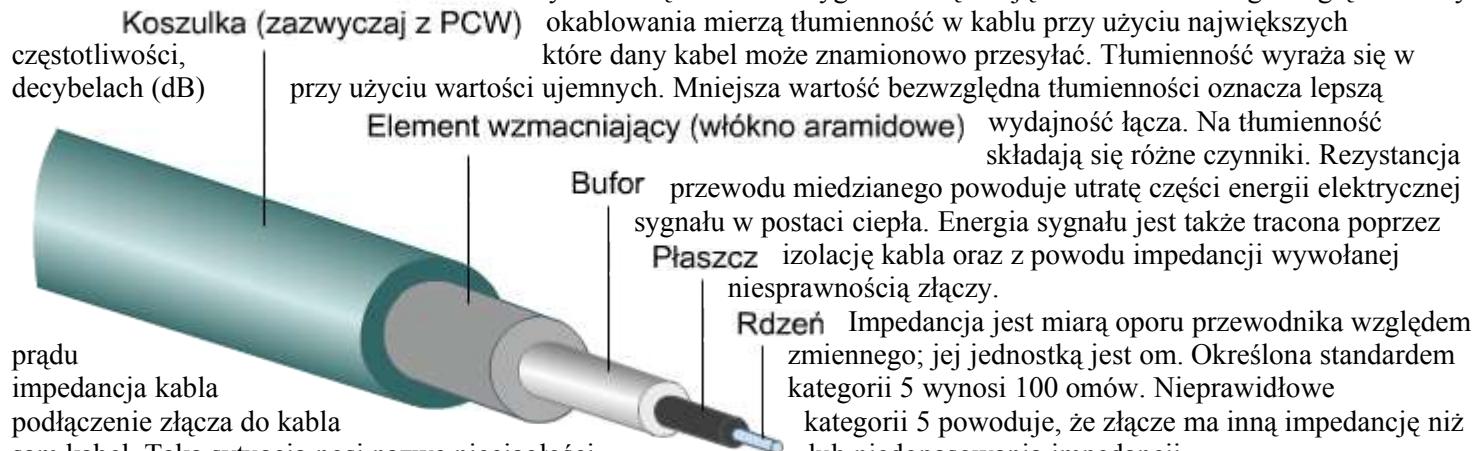


**Skrętka ekranowana** jest wyposażona w uziemiony zewnętrzny ekran przewodzący prąd, który izoluje sygnały od zewnętrznego szumu elektrycznego. W skrętce ekranowanej stosuje się także wewnętrzne ekrany foliowe zabezpieczające każdą z par przewodów przed szumem generowanym przez pozostałe pary. Kabel STP jest czasami błędnie nazwany ScTP (Screeened Twisted Pair). ScTP odnosi się jednak do skręcanych i ekranowanych kabli kategorii 5 lub 5e, natomiast terminem STP określa się specyficzny kabel IBM, który posiada jedynie dwie pary przewodów. **Skrętka ekranowana ScTP** jest droższa, trudniejsza w instalacji i rzadziej używana niż skrętka nieekranowana. **Skrętka nieekranowana** jest bardziej narażona na szum zewnętrzny z powodu braku ekranu, ale jest ona używana częściej ze względu na niższą cenę i łatwość instalacji. W kablach światłowodowych dane są przenoszone w postaci sygnałów polegających na zmianach intensywności światła odpowiadających zerom i jedynkom systemu dwójkowego. W kablu o tej samej długości natężenie sygnału światlnego nie spada w takim stopniu jak moc sygnału elektrycznego. Sygnałów optycznych nie zakłóca szum elektryczny, a światłowodów nie trzeba uziemiać, chyba że koszulka zawiera metal lub linkę wzmacniającą. Dlatego używane są one do połączeń między piętrami i budynkami. Coraz niższe koszty i coraz większe wymagania co do szybkości sprawiają, że światłowody mogą stać się powszechniejszym medium w sieciach lokalnych.

#### 4.2.2 Tłumienność i tłumienność przejścia w kablu miedzianym

## Kabel światłowodowy

Tłumienność jest to spadek amplitudy sygnału na całej długości łącza. Długie kable i wysokie częstotliwości sygnału zwiększą tłumienność. Z tego względu testery



prądu  
impedancia kabla  
podłączenie złącza do kabla  
sam kabel. Taka sytuacja nosi nazwę nieciągłości

Nieciągłość impedancji zwiększa tłumienność, ponieważ część wysyłanego sygnału — zamiast zostać przesłana do odbiornika — zostanie odbita z powrotem do urządzenia wysyłającego, podobnie jak ma to miejsce w przypadku echa. Efekt ten potęguje się, gdy istnieje wiele nieciągłości powodujących odbicie kolejnych części pozostałoego sygnału z powrotem do nadajnika. Gdy z kolei odbicie napotka kierunku pierwotnego sygnału, tworząc efekt echa. Echo dociera do odbiornika w różnych odstępach czasu, określając wartość właściwego sygnału. Proces ten nosi nazwę rozsynchonizowania i jest przyczyną błędów w transmisji danych.

Połączone skutki tłumienia sygnału i nieciągłości impedancji na linii komunikacyjnej noszą nazwę tłumienności przejścia. Prawidłowe funkcjonowanie sieci wymaga, aby wszystkie kable i złącza miały jednakową impedancję, bez jakichkolwiek nieciągłości w

### 4.2.3 Źródła szumu w kablach miedzianych

Na szum składa się wszelka energia elektryczna w transmisyjnym, która utrudnia zinterpretowanie przez odbiornik danych wysyłanych z nadajnika. Procedura certyfikacji TIA/EIA-568-B wymaga obecnie testowania kablów pod kątem różnego rodzaju szumów. **Przesłuch** polega na przeniesieniu sygnału z jednego przewodu do drugiego znajdującego się w pobliżu. Zmiana napięcia w przewodzie generuje energię elektromagnetyczną. Energia ta promieniuje z przewodu, podobnie jak sygnał radiowy z nadajnika. Sąsiednie przewody w kablem działają jak anteny, odbierając wygenerowaną energię, która zakłóca przesyłanie danych w tych przewodach.

Przesłuch może także pochodzić od sygnałów z innych kabli leżących w pobliżu. Nazywa się on wtedy przesłuchem obcym (ang. alien crosstalk). Przesłuch stanowi większy problem przy wyższych częstotliwościach transmisji. **Urządzenie testujące** kable mierzy przesłuch, wysyłając sygnał testowy do jednej pary przewodów. Następnie tester mierzy amplitudę niepożądanej sygnału (przesłuchu) indukowanego w innych parach przewodów w tym kablu. **Efekt przesłuchu** wykorzystuje się w skrętkach w celu zmniejszenia szumu. W skrętce para przewodów służy do transmisji jednego sygnału. Para ta jest skręcona w taki sposób, aby każdy przewód doświadczał podobnego przesłuchu. Ponieważ szum będzie identyczny w obu przewodach, łatwiejsze będzie jego wykrycie i odfiltrowanie w urządzeniu odbiorczym. Skręcenie par przewodów pomaga także zredukować przesłuch danych i szum pochodzący z sąsiedniej pary. Skrętka nieekranowana wyższych kategorii wymaga gęstszej skręcenia każdej pary przewodów w kablu, aby umożliwić zmniejszenie przesłuchu na wyższych częstotliwościach transmisji. Aby zapewnić niezawodną komunikację w sieci lokalnej, przy zakładaniu złączy na końcach skrętki nieekranowanej przewody należy rozkręcać na jak najkrótszym odcinku.

### 4.2.4 Rodzaje przesłuchu

wysokie częstotliwości sygnału zwiększą tłumienność. Z tego względu testery okablowania mierzą tłumienność w kablu przy użyciu największych częstotliwości, decybelach (dB) przy użyciu wartości ujemnych. Mniejsza wartość bezwzględna tłumienności oznacza lepszą wydajność łącza. Na tłumienność składają się różne czynniki. Rezystancja przewodu miedzianego powoduje utratę części energii elektrycznej sygnału w postaci ciepła. Energia sygnału jest także tracona poprzez izolację kabla oraz z powodu impedancji wywołanej niesprawnością złączy.

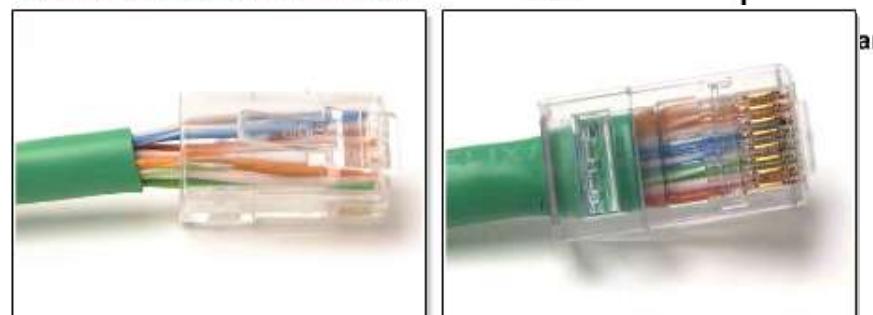
**Rdzeń** Impedancja jest miarą oporu przewodnika względem zmiennego; jej jednostką jest om. Określona standardem kategorii 5 wynosi 100 omów. Nieprawidłowe kategorie 5 powodują, że złącze ma inną impedancję niż lub niedopasowania impedancji.

**Tłumienie** pierwszą nieciągłość, część sygnału odbija się w wielokrotnego

Kabel sieciowy między komputerami utrudniając



### Łączenie przewodów



Złącze niesprawne przewody nie są skręcone na zbyt długim odcinku.

Złącze sprawne przewody są nieskręcone tylko na tyle, na ile jest to niezbędne w celu założenia złącza.

Wyróżniamy trzy rodzaje przesłuchu:

- przesłuch zbliżny (NEXT, Near-end Crosstalk),
- przesłuch zdalny (FEXT, Far-end Crosstalk),
- przesłuch zbliżny skumulowany w jednej parze (PSNEXT, Power Sum Near-end Crosstalk).

**Przesłuch zbliżny (NEXT)** jest to stosunek amplitud

napięcia sygnału testowego i sygnału przesłuchu mierzonych na tym samym końcu połączenia. Przesłuch zbliżny jest wyrażany w decybelach (dB) wartości ujemnych. Im większa liczba (mniejsza wartość bezwzględna), tym większy szum: tak samo temperatury ujemne bliskie zero oznaczają, że jest cieplej. Zazwyczaj testery okablowania nie wyświetlają znaku minus oznaczającego ujemne wartości przesłuchu zbliżonego. Odczyt NEXT o wartości 30 dB (co faktycznie ma znaczyć -30 dB) oznacza mniejszy przesłuch zbliżny i bardziej czysty sygnał niż NEXT o wartości 10 dB.

Wartość NEXT należy zmierzyć na obu końcach linii dla każdej pary względem każdej innej pary w skrótce nieekranowanej. Aby skrócić czas testowania, niektóre urządzenia umożliwiają przesłuchów NEXT przy większych odstępach między zostało to określone w standardzie TIA/EIA. W wyniku tego pomiary mogą nie być zgodne ze standardem TIA/EIA-568-B i stwarzają ryzyko przeoczenia wydajność połączenia kablowego, przesłuch zbliżny należy okablowania na obu końcach linii. Taki sposób pomiaru jest celu zapewnienia pełnej zgodności ze specyfikacją kabla o wysokiej przepustowości.

Ze względu na tłumienność przesłuch pojawiający się dalej od nadajnika powoduje mniejszy szum w kablu niż przesłuch zbliżny. Ten przesłuch nosi nazwę **przesłuchu zdalnego, czyli FEXT**. Szum powodowany przez przesłuch zdalny nadal powraca do źródła, ale jest tłumiony podczas powrotu. Dlatego nie stanowi on takiego problemu jak przesłuch zbliżny.

#### Przesłuch zbliżny skumulowany w jednej parze

przesłuchów zbliżnych pochodzących ze wszystkich par przewodów w kablu. Przesłuch PSNEXT jest obliczany dla każdej pary przewodów na podstawie przesłuchu zbliżnego pochodzącego od pozostałych trzech par. Połączony przesłuch z wielu równoległych źródeł transmisji może w znacznym stopniu pogorszyć jakość sygnału. Certyfikaty TIA/EIA-568-B wymagają obecnie testów sprawdzających wielkość przesłuchu PSNEXT.

W niektórych sieciach opartych na specyfikacji Ethernet, na przykład 10BASE-T i 100BASE-TX, dane są odbierane w danym kierunku tylko z jednej pary przewodów. Jednakże w wypadku nowszych technologii, takich jak 1000BASE-T, w których dane są odbierane w tym samym kierunku z wielu par, pomiary przesłuchu PSNEXT są bardzo istotne.

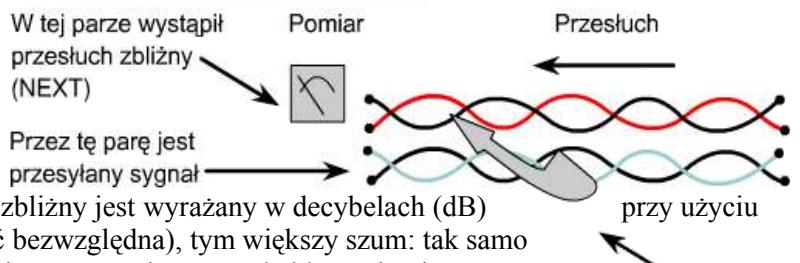
### 4.2.5 Standardy testowania kabli

Standard TIA/EIA-568-B określa dziesięć testów, które musi przejść kabel miedziany, aby mógł zostać użyty w nowoczesnych, szybkich sieciach Ethernet. Wszystkie połączenia kablowe należy testować z zastosowaniem maksymalnych wartości znamionowych wskazanych dla testowanej kategorii kabli.

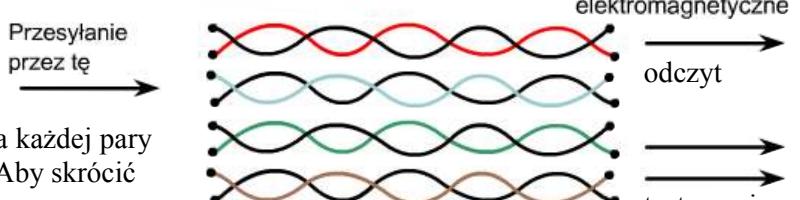
Dziesięć podstawowych parametrów, które muszą być przetestowane dla połączenia kablowego, aby spełniało standardy TIA/EIA:

- mapa połączeń,
- tłumienność przejścia,
- przesłuch zbliżny (NEXT),

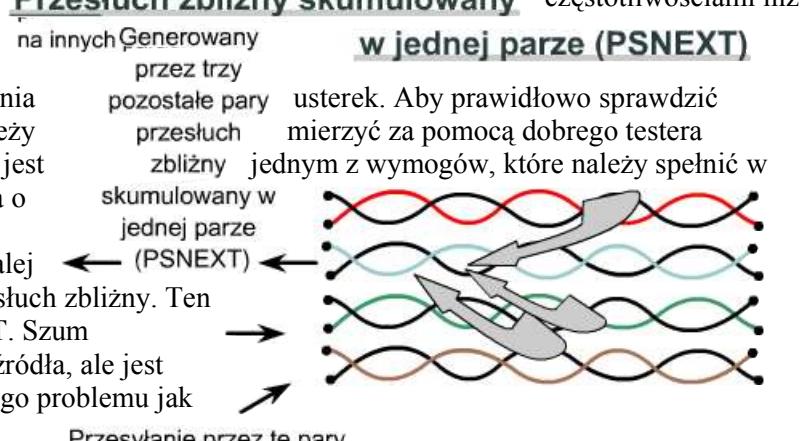
### Przesłuch zbliżny (NEXT)



### Przesłuch zdalny (FEXT)



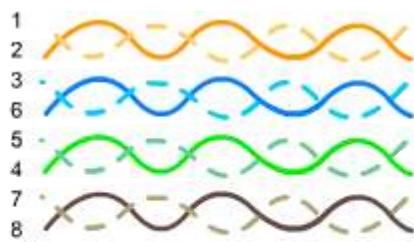
### Przesłuch zbliżny skumulowany w jednej parze (PSNEXT)



(PSNEXT) jest wynikiem kumulacji

przesłuch zbliżny skumulowany w jednej parze (PSNEXT), wyrównany współczynnik przesłuchu zdalnego (ELFEXT), skumulowany współczynnik przesłuchu zdalnego (PS ELFEXT), straty odbiciowe, opóźnienie propagacji, długość kabla, różnica opóźnień (delay skew).

**Standard Ethernet** określa, że każdy ze styków złącza RJ-45 ma specyficzne zadanie. Karta sieciowa wysyła sygnały przez styki 1 i 2, a odbiera na stykach 3 i 6. Przewody w skrętkę nieekranowanej muszą być podłączone do odpowiednich styków na obu końcach kabla. Test mapy połączeń polega na sprawdzeniu, czy w kablu nie ma przewodów rozwartych ani zwartych. Przewód rozwarty to taki, który nie jest prawidłowo podłączony do złączki. Przewód zwarty to przewód połączony z drugim przewodem.



Poprawne podłączenie  
(standard T568B)

Mapa połączeń umożliwia również sprawdzenie, czy wszystkie osiem przewodów podłączono do odpowiednich styków na obu końcach kabla. Mapa przewodów umożliwia wykrywanie różnych błędów podłączenia. Błąd podłączenia polegający na odwróceniu pary

wtedy, gdy para przewodów jest prawidłowo podłączona do jednej złączki, a odwrotnie do

Ma to miejsce na przykład wtedy, gdy na jednym końcu przewód biało/pomarańczowy jest podłączony do styku 1, a przewód pomarańczowy — do styku 2, natomiast na drugim końcu odwrotnie. Przykład takiego podłączenia przedstawiono na ilustracji.

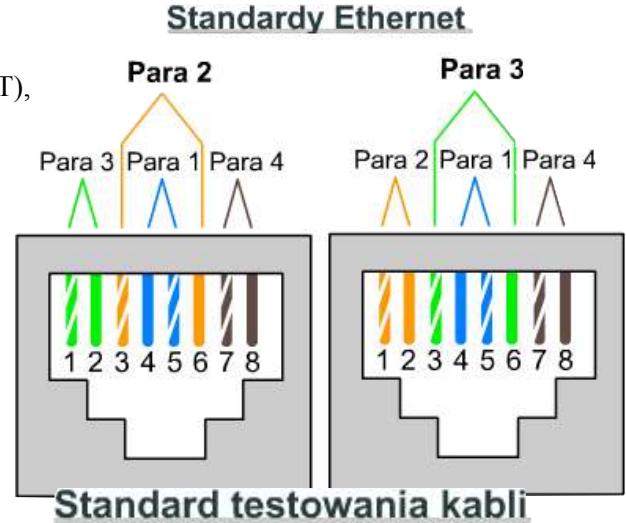
Błąd polegający na rozdzieleniu par ma miejsce wtedy, gdy pojedynczy przewód z jednej pary został zamieniony z pojedynczym przewodem z innej pary. Takie połączenie powoduje zmniejszenie efektu znoszenia i sprawia, że kabel jest bardziej podatny na przesłuchy i interfeference. Aby zobaczyć, na czym polega błąd tego typu, należy przyjrzeć się dokładnie numerom styków na ilustracji. Rozdzielenie par powoduje, że dwie pary przewodów nadawczych lub odbiorczych nie są ze sobą skręcone.

Błąd polegający na zamianie par miejscami występuje wtedy, gdy jakaś para przewodów jest podłączona do różnych styków na obu końcach. Błąd ten różni się od odwrócenia pary, ponieważ w wypadku odwrócenia pary przewody na obu końcach podłączone są do tej samej pary styków, tylko odwrotnie.

#### 4.2.6 Inne parametry testowe

Połączone skutki tłumienia sygnału i nieciągłości impedancji na linii komunikacyjnej noszą nazwę tłumienności przejścia. Tłumienność przejścia mierzy się na zdalnym końcu kabla i wyraża w decybelach. Standard TIA/EIA wymaga, żeby kabel i jego złącza obowiązkowo zostały przetestowane pod względem tłumienności przejścia przed zastosowaniem w sieci LAN. **Pomiar przesłuchu** odbywa się w trakcie czterech odrębnych testów Tester okablowania mierzy przesłuch zbliżny, wysyłając sygnał testowy do jednej z par i mierząc amplitudę przesłuchu odebranego przez inne pary przewodów. Przesłuch zbliżny jest to wyrażony w decybelach stosunek amplitud napięcia sygnału testowego i sygnału przesłuchu mierzonych na tym samym końcu kabla. Należy pamiętać, że tester wyświetla wartość bezwzględną przesłuchu. Liczba określająca przesłuch jest ujemna, czyli większa liczba na wyświetlaczu oznacza mniejszy przesłuch. Jak wspomniano wyżej, test PSNEXT jest w istocie rezultatem obliczeń opartych na połączeniu efektów przesłuchu zbliżonego. **Test ELFEXT** (wyrównanego współczynnika przesłuchu zdalnego między dwoma parami mierzonymi w odniesieniu do sygnału źródłowego) opiera się na pomiarze przesłuchu zdalnego. Przesłuch ELFEXT para–para jest wyrażonym w dB stosunkiem zmierzonego przesłuchu zdalnego do tłumienności przejścia pary przewodów, której sygnał jest zakłócanym przez przesłuch zdalny. Wartość ELFEXT jest ważnym parametrem w sieciach Ethernet działających w technologii 1000BASE-T. Parametr PS ELFEXT stanowi skumulowany efekt przesłuchów ELFEXT pochodzących ze wszystkich par przewodów. **Straty odbiciowe** to wyrażona w decybelach miara liczby odbić spowodowanych wszystkimi nieciągłościami impedancji na całej długości linii. Warto przypomnieć, że głównego problemu związanego ze stratami odbiciowymi nie stanowi utrata pierwotnej mocy sygnału. Istotne jest natomiast to, że echa sygnału spowodowane nieciągłościami docierają do odbiornika w różnych odstępach czasu, powodując rozsynchonizowanie sygnału.

#### 4.2.7 Parametry czasowe



Standard testowania kabli

WIREMAP	
177ft	1 2
180ft	3 4
177ft	5 6
180ft	7 8
\$	\$

kabla.  
występuje  
drugiej.

Prawidłowe podłączenie przewodów

WIREMAP		WIREMAP	
178ft	1 2	122ft	1 2
181ft	3 4	180ft	3 4
121ft	5 6	178ft	5 6
180ft	7 8	180ft	7 8
\$	\$	\$	\$

Przewody rozwarte

Przewody zwarte

Opóźnienie propagacji to parametr badany poprzez prosty pomiar czasu przesyłania sygnału testowanym kablem. Opóźnienie sygnału w parze przewodów zależy od ich długości, stopnia skręcenia i właściwości elektrycznych. Opóźnienia są mierzone w setnych częściach nanosekundy. Jedna nanosekunda to jedna miliardowa, czyli 0,000000001 sekundy. Standard TIA/EIA-568-B określa limit opóźnienia propagacji dla różnych kategorii skrętki nieekranowanej. **Obliczenia długości kabli** opierają się na pomiarach opóźnienia propagacji. Standard TIA/EIA-568-B.1 stanowi, że fizyczną długość linii oblicza się według pary przewodów o najkrótszym opóźnieniu sygnału elektrycznego. Testery mierzą długość przewodu na podstawie opóźnienia sygnału elektrycznego w teście TDR, nie zaś opierając się na fizycznej długości koszulki kabla. Ponieważ przewody w kablu są skręcone, sygnały przebywają większy dystans, niż wynikłoby to z fizycznej długości kabla. Pomiar TDR polega na wysłaniu impulsu przez parę przewodów i zmierzeniu czasu, jaki upłynie do momentu powrotu tego impulsu przez tę samą parę. **Test TDR** nie tylko pozwala określić długość kabla, ale także odległość do takich uszkodzeń, jak przewody zwarte i rozwarte. Kiedy impuls napotka przewody zwarte lub rozwarte albo podłączenie niskiej jakości, całość lub część jego energii powróci do testera okablowania. Może to zostać użyte do obliczenia przybliżonej odległości od uszkodzenia. Jest to przydatne przy szukaniu na linii niesprawnego punktu połączenia, którym może być np. gniazdko ścienne. W różnych parach przewodów w jednym kablu opóźnienia propagacji mogą się nieco różnić od siebie ze względu na liczbę skrętów i właściwości elektryczne poszczególnych par. Różnica między parami w opóźnieniu nosi nazwę różnicę opóźnień. Różnica opóźnień jest newralgicznym parametrem w sieciach o dużej prędkości, w których dane są jednocześnie przesyłane przez kilka par przewodów, na przykład Ethernet 1000BASE-T. Jeśli różnica opóźnień między parami jest za duża, bity nie docierają jednocześnie i nie jest możliwe ponowne złożenie danych. Nawet jeśli łącze nie jest przeznaczone do tego typu transmisji danych, testowanie błędu opóźnienia umożliwia jego modernizację w kierunku sieci o większej przepustowości. Wszystkie połączenia kablowe w sieci lokalnej muszą przejść każdy z opisanych wyżej testów, w sposób określony w standardzie TIA/EIA-568-B, aby można było mówić o zgodności ze standardem. Zgodność ze standardem musi być potwierdzona przez urządzenie certyfikacyjne, które zapewnia, że wszystkie konieczne testy zakończyły się powodzeniem. Testy te dają pewność, że połączenia kablowe będą działały niezawodnie przy wysokich częstotliwościach i szybkościach. Testy kabli należy wykonywać podczas ich instalowania, a następnie regularnie ponawiać, aby mieć pewność, że instalacje sieci LAN spełniają standardy branżowe. Aby zyskać pewność, że testy są dokładne, należy prawidłowo korzystać z wysokiej jakości urządzeń testujących. Wyniki testów trzeba również dokładnie udokumentować.

#### 4.2.8 Testowanie światłowodów

Łącze światłowodowe składa się z dwóch oddzielnych włókien szklanych działających jako niezależne ścieżki danych. Jedno włókno przesyła sygnały w jedną stronę, a drugie w przeciwną. Każde włókno jest otoczone nieprzepuszczalną dla światła powłoką, dlatego w światłowodach nie występuje przesłuch. W światłowodach nie występują również problemy z interferencją elektromagnetyczną ani z szumem. Pojawia się tłumienie, ale w znacznie mniejszym stopniu niż w kablach miedzianych. **W łączach światłowodowych** występuje optyczny odpowiednik nieciągłości impedancji znanej ze skrętki nieekranowanej. Kiedy światło napotka nieciągłość optyczną, taką jak zanieczyszczenie szkła bądź mikrorysy, jego część jest odbijana w przeciwną stronę. Oznacza to, że tylko ułamek pierwotnego sygnału przechodzi dalej w kierunku odbiornika. W rezultacie do odbiornika dociera mniej światła, co utrudnia rozpoznanie sygnału. Podobnie jak w wypadku skrętki nieekranowanej, nieprawidłowo zainstalowane złącza są główną przyczyną odbić światła i strat mocy sygnału. Ponieważ w wypadku światłowodów nie ma problemów z szumem, podstawową kwestią jest moc sygnału światelnego docierającego do odbiornika. Jeśli tłumienie spowoduje osłabienie odbieranego sygnału światelnego, mogą wystąpić błędy w interpretacji danych. Testowanie światłowodów polega przede wszystkim na wysłaniu światła i sprawdzaniu, czy odpowiednia jego ilość dociera do odbiornika. **Konieczne jest obliczenie akceptowalnego stopnia utraty mocy sygnału**, tak aby nie była ona niższa od wymaganej przez odbiornik. Rachunek taki nazywa się budżetem optycznym połączenia światłowodowego. Urządzenie do testowania światłowodów, składające się ze źródła światła i miernika mocy sprawdza, czy budżet ten nie został przekroczyony. Jeśli włókno nie przejdzie tego testu, inne urządzenie testowe może zostać użyte do wskazania, w którym miejscu połączenia wystąpiła nieciągłość. Optyczne urządzenie TDR znane jako OTDR może posłużyć do lokalizacji takich nieciągłości. Zazwyczaj problem powstaje w wyniku nieprawidłowego podłączenia jednego lub wielu złącz. Urządzenie OTDR odnajdzie miejsce, w którym znajduje się wadliwe połączenie wymagające wymiany. Po usunięciu usterek konieczne jest ponowne przetestowanie kabla.

#### 4.2.9 Nowy standard

W czerwcu 2002 roku opublikowano uzupełnienie standardu TIA-568 dotyczące okablowania kategorii 6 (czyli Cat 6). Oficjalną nazwą standardu jest ANSI/TIA/EIA-568-B.2-1. Nowy standard opisuje zestaw parametrów wydajnościowych, które należy testować w instalacjach sieci Ethernet, a także określa liczby punktów wymagane do pomyślnego zaliczenia każdego z testów. Kable kategorii 6 muszą pomyślnie przejść wszystkie testy. Mimo iż testy kategorii 6 są w zasadzie takie same, jak w standardzie Cat 5, nowy certyfikat wymaga większej liczby punktów. Kabel kategorii 6 musi przenosić częstotliwości do 250 MHz oraz wykazywać niższe poziomy przesłuchu i strat odbiciowych. Wszystkie pomiary wymagane przez certyfikaty Cat 5, Cat 5e i Cat 6 dla połączeń stałych i połączeń kanałowych można wykonać za pomocą testera okablowania z serii Fluke DSP-4000 lub Fluke OMNIScanner2 lub podobnych urządzeń. Na rysunku przedstawiono analizator okablowania Fluke DSP-4100 z adapterem DSP-LIA013 do testowania okablowania kategorii 5e.

## Podsumowanie

- Z testowaniem okablowania wiążą się następujące pojęcia matematyczne i elektroniczne: sygnał, fala, częstotliwość i szum. Znajomość tych pojęć pomaga w opanowaniu wiadomości o sieciach, instalacji i testowaniu okablowania.
- Tłumienie (słabnięcie sygnału) i szum (interferencja sygnałów) powodują problemy z sieciami, ponieważ dane mogą zostać zniekształcone do tego stopnia, że po odebraniu będą nieczytelne. Prawidłowe podłączenie złączy i właściwa instalacja okablowania są w związku z tym bardzo istotne.

## Moduł 5. Okablowanie sieci LAN I WAN

Mimo iż każda lokalna sieć komputerowa jest inna, istnieje wiele zagadnień projektowych, które są wspólne dla wszystkich sieci LAN. Na przykład w większości sieci LAN wykorzystywane są te same standardy i komponenty. W tym module przedstawiono informacje dotyczące elementów lokalnych sieci Ethernet oraz powszechnie stosowanych urządzeń LAN.

Obecnie dostępne są różne rodzaje połączeń WAN. Mogą to być rozmaite połączenia: od komutowanych po szerokopasmowe. Różnią się one szerokością pasma, ceną i wymaganymi urządzeniami. W tym module przedstawiono informacje dotyczące różnych typów połączeń WAN.

### 5.1 Okablowanie sieci LAN

#### 5.1.1 Warstwa fizyczna sieci LAN

Typy medium są oznaczane przy użyciu różnych symboli. Sieć Token Ring jest oznaczana kółkiem. Sieć FDDI jest oznaczana dwoma współśrodkowymi kółkami, a sieć Ethernet — prostą kreską.

Połączenia szeregowe są oznaczane zygzakiem.

**Sieć komputerową można zbudować przy użyciu różnych mediów.** Zadaniem medium jest przenoszenie informacji przesyłanych siecią LAN. W lokalnych sieciach bezprzewodowych medium jest fala elektromagnetyczna rozchodząca się w powietrzu lub w przestrzeni kosmicznej. W przypadku innych mediów do przenoszenia sygnałów sieciowych stosowane są przewody, kable lub światłowody. Media sieciowe stanowią warstwę pierwszą — fizyczną — sieci LAN. Każde medium ma wady i zalety.

Przy porównywaniu zalet i wad na ogół warto uwzględnić:

- dopuszczalną długość kabla,
- koszt,
- łatwość instalacji,
- podatność na zakłócenia.

Sygnały sieciowe mogą być przenoszone za pośrednictwem kabli koncentrycznych, światłowodów, a nawet bezprzewodowo. Jednak podstawowym medium, który będzie omawiany, jest nieekranowana skrętka kategorii 5 (Cat 5 UTP), do której należy również rodzina kabli kategorii 5e. Sieci LAN można budować na bazie wielu topologii oraz wielu różnych mediów fizycznych. Na rysunku zaprezentowano niektóre technologie warstwy fizycznej, które mogą być wykorzystane do budowy sieci Ethernet.

#### 5.1.2 Sieć Ethernet w kampusie

Standard Ethernet jest najbardziej powszechną techniką, w jakiej realizowane są sieci LAN. Po raz pierwszy został on zaimplementowany przez grupę firm Digital (DEC), Intel i Xerox, którą określa się wspólnym skrótem DIX. Grupa DIX utworzyła i zaimplementowała pierwszą specyfikację lokalnej sieci Ethernet, która stała się podstawą specyfikacji 802.3 instytutu IEEE wydanej w roku 1980. Specyfikacja 802.3 została później rozszerzona przez IEEE o trzy nowe standardy: 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet over Fiber) i 802.3ab (Gigabit Ethernet over UTP). Wymagania dotyczące sieci mogą wymuszać aktualizację do szybszych topologii sieci Ethernet. Większość sieci Ethernet obsługuje szybkości 10 Mb/s i 100 Mb/s. Nowa generacja produktów multimedialnych, związanych z przetwarzaniem obrazu i bazami danych może spowodować szybkie przeciążenie sieci Ethernet działających z tradycyjnymi szybkościami 10 i 100 Mb/s.

Administratorzy sieci powinni rozważyć użycie sieci Gigabit Ethernet w różnych zastosowaniach: poczynając od sieci szkieletowej, a kończąc na odcinkach prowadzących bezpośrednio do użytkowników. Koszty instalacji nowego okablowania i kart sieciowych mogą jednak uniemożliwić taką modernizację. Instalacja sieci Gigabit Ethernet aż do komputera użytkownika nie jest jeszcze standardem. Ogólnie rzecz biorąc, techniki Ethernet można wykorzystywać w sieci kampusowej na kilka różnych sposobów:

- Aby zapewnić odpowiednią wydajność na poziomie użytkowników, można użyć sieci Ethernet o szybkości 10 Mb/s. W wypadku klientów lub serwerów wymagających szerszego pasma można użyć sieci Ethernet o szybkości 100 Mb/s.
- Sieć Fast Ethernet jest używana do budowy łącz między użytkownikiem i urządzeniami sieciowymi. Może ona obsługiwać ruch pochodzący z poszczególnych segmentów sieci Ethernet.
- Aby zwiększyć wydajność sieci klient-serwer w kampusie i uniknąć występowania tzw. wąskich gardeł, do łączenia serwerów firmowych można stosować sieci Fast Ethernet.
- Miedzy urządzeniami sieci szkieletowej powinny być instalowane sieci Fast Ethernet lub Gigabit Ethernet, jeśli pozwalają na to względy ekonomiczne.

### Media



Token Ring

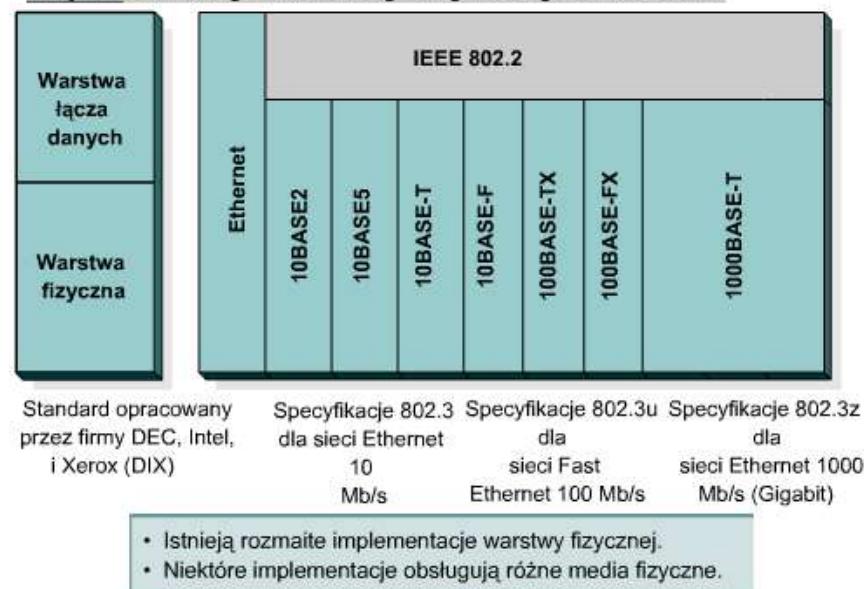


Łącze Ethernet

Łącze szeregowe



### Implementacja warstwy fizycznej sieci LAN



### 5.1.3 Wymagania dotyczące mediów i złączy w sieciach

#### Ethernet

Przed dokonaniem wyboru sposobu implementacji sieci Ethernet należy rozważyć wymagania dotyczące mediów i złączy związane z poszczególnymi sposobami implementacji. Pod uwagę należy także wziąć wymaganą wydajność sieci.

Specyfikacje kabli i złączy używanych do obsługi implementacji sieci

Ethernet są oparte na standardach organizacji EIA/TIA. Kategorie kabli określone dla sieci Ethernet pochodzą ze standardu EIA/TIA-568 (SP-2840)

dotyczącego telekomunikacyjnego okablowania budynków komercyjnych.

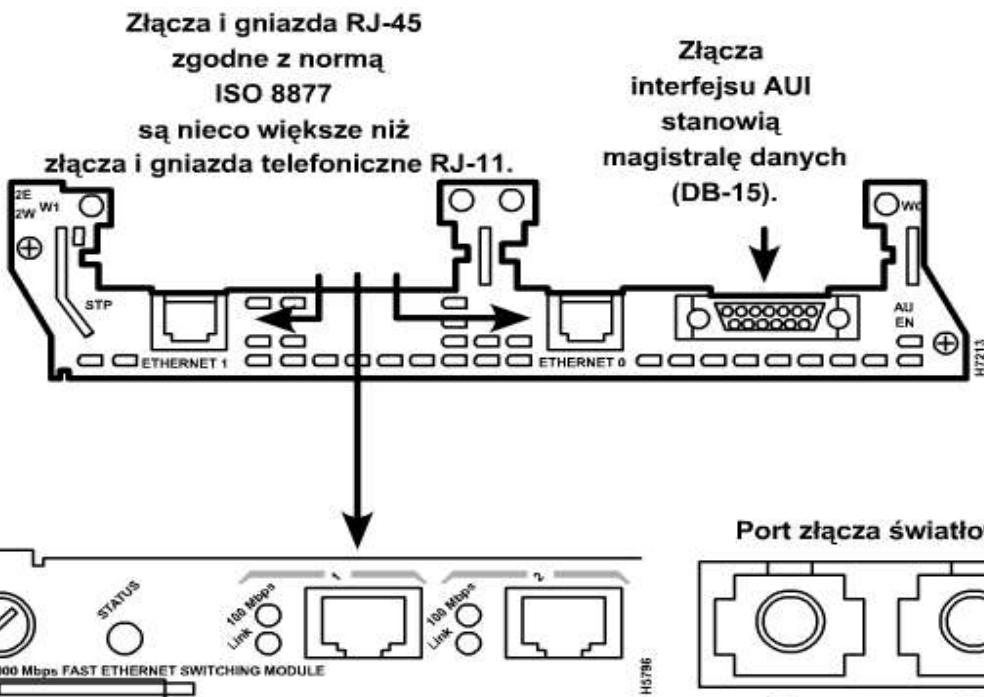
Na rysunku przedstawiono porównanie specyfikacji kabli i złączy dla najbardziej powszechnych implementacji sieci Ethernet. Istotną kwestią jest różnica między medium, które mogą zostać użyte w sieci Ethernet o szybkości 10 Mb/s a medium, które mogą być użyte w sieci Ethernet o szybkości 100 Mb/s. Do budowy sieci, w której będą używane obie prędkości 10 Mb/s i 100 Mb/s, trzeba zastosować skrętkę nieekranowaną kategorii conajmniej 5.

#### Wymagania dotyczące mediów i złączy w sieciach Ethernet

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Medium	50-omowy kabel koncentryczny (cienki Ethernet)	50-omowy kabel koncentryczny (gruby Ethernet)	Skrętka nieekranowana EIA/TIA kategorii 3, 4, 5 (dwie pary)	Skrętka nieekranowana EIA/TIA kategorii 5 (dwie pary)	Światłowód wielomodowy 62,5/125	STP	Skrętka nieekranowana EIA/TIA kategorii 5 (cztery pary)	Światłowód wielomodowy 62,5/50	Światłowód wielomodowy 62,5-lub 50-mikrometrowy; 9-mikrometrowy światłowód jednomodowy
Maksymalna długość segmentu	185 m	500 m	100 m	100 m	400 m	25 m	100 m	275 m w przypadku światłowodu grubości 62,5 mikrometra; 550 m w przypadku światłowodu grubości 50 mikrometrów; od 3 do 10 km w przypadku światłowodu jednomodowego	440 m w przypadku światłowodu grubości 62,5 mikrometra; 550 m w przypadku światłowodu grubości 50 mikrometrów; od 3 do 10 km w przypadku światłowodu jednomodowego
Topologia	Magistrala	Magistrala	Gwiazda	Gwiazda	Gwiazda	Gwiazda	Gwiazda	Gwiazda	Gwiazda
Złącze	BNC	Interfejs AUI	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Złącze SC	

### 5.1.4 Połączenia

Na rysunku przedstawiono różne typy połączeń wykorzystywane w przypadku poszczególnych implementacji warstwy fizycznej. Najbardziej powszechnie są złącza i gniazdo RJ-45. Złącza RJ-45 zostaną bardziej szczegółowo omówione w następnej sekcji. W niektórych przypadkach typ złącza karty sieciowej nie pasuje do medium, do którego ma nastąpić podłączenie. Na rysunku przedstawiono interfejs do podłączenia 15-stykowego złącza interfejsu AUI. Złącze AUI umożliwia podłączanie różnych mediów przy wykorzystaniu odpowiedniego transceivera. Transceiver stanowi przejściówkę, która przekształca jeden typ połączenia w inny. Zazwyczaj nadajnik-odbiornik (transceiver) umożliwia podłączenie kabla zakończonego złączem RJ-45 czy też kabla koncentrycznego lub światłowodowego do interfejsu AUI. W sieciach 10BASE5 Ethernet (Thicknet, czyli „gruby” Ethernet) do połączenia interfejsu AUI z transceiverem przy głównym kablu jest używany krótki kabel.



### 5.1.5 Implementacja skrętki nieekranowanej (UTP)

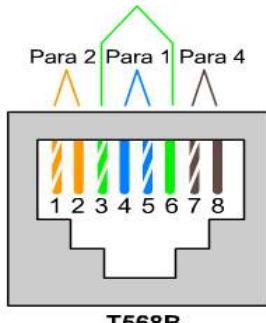
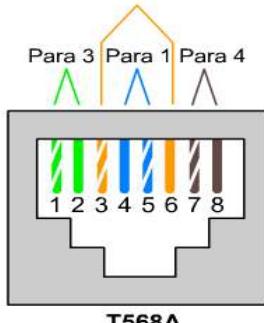
Specyfikacja EIA/TIA opisuje złącze RJ-45 przeznaczone dla skrętki nieekranowanej (UTP). Litery RJ oznaczają typ złącza (skrót od ang. „registered jack”), a liczba 45 — określony sposób instalowania przewodów. Przez przezroczystą końcówkę złącza RJ-45 widać osiem kolorowych przewodów. Cztery przewody (od T1 do T4) służą do przenoszenia napięcia. W języku angielskim noszą one nazwę „tip”. Cztery pozostałe przewody (od R1 do R4) są uziemione i po angielsku są nazywane „ring”. „Tip” i „ring” to pojęcia wywodzące się z wczesnych lat rozwoju telefonii; po polsku funkcjonują określenia „żyła a” i „żyła b”. Współcześnie angielskie terminy „tip” i „ring” odnoszą się do przewodu plus i minus w parze. Przewody pierwszej pary w kablu lub złączu są oznaczone jako T1 i R1. Druga para to T2 i R2 itd.

**Złącze RJ-45 stanowi komponent męski**, zaciśnięty na końcu kabla. Gdy patrzymy na złącze męskie z przodu, styki są ponumerowane od 8 po lewej stronie do 1 po stronie prawej, co przedstawiono na rysunku .

**Gniazdo stanowi komponent żeński**, który znajduje się w urządzeniu sieciowym, gniazdku ściennym lub panelu połączeniowym, co przedstawiono na rysunku . Na rysunku przedstawiono tył gniazda: to tu wykonuje się połączenia zaciskowe z kablem UTP sieci Ethernet.



## Standardy EIA/TIA T568A i EIA/TIA T568B



Aby między złączem i gniazdem mógł przepływać prąd, przewody muszą być ułożone w kolejności zgodnej ze schematem T568A lub T568B standardu EIA/TIA-568-B.1, co pokazano na rysunku.

W celu określenia kategorii EIA/TIA kabla, który powinien zostać użyty do podłączenia urządzenia, należy odnieść się do dokumentacji tego urządzenia lub znaleźć na nim etykietkę w pobliżu gniazda. Jeżeli nie ma żadnych etykiet ani dokumentacji, należy użyć kategorii 5E lub wyższej, ponieważ wyższe kategorie mogą być użyte w miejscu niższych. Ponadto należy określić, czy do podłączenia ma zostać zastosowany kabel prosty, czy też z przeplotem.

Jeśli spojrzymy na oba złącza kabla ułożone obok siebie, zobaczymy w każdym z nich kolorowe przewody. Jeżeli kolejność przewodów w obu końcówkach kabla jest taka sama, oznacza to, że jest to kabel prosty — taką sytuację przedstawiono na rysunku (Zastosowanie1...).

Natomiast gdy przyjrzymy się złączom RJ-45 na obu końcach kabla z przeplotem, zobaczymy, że niektóre przewody po jednej stronie kabla są podłączone do innego styku niż po drugiej stronie. Na rysunku (Łączenie...) widać, że styki 1 i 2 jednego złącza są podłączone odpowiednio do styków 3 i 6 drugiego.

Na rysunku (obok) zamieszczono wskazówki dotyczące typów kabli stosowanych do tworzenia połączeń między urządzeniami Cisco.

**Kabli prostych należy używać przy wykonywaniu następujących połączeń:**

- połączenie przełącznika z routerem,
- połączenie przełącznika z komputerem lub serwerem,
- połączenie koncentratora z komputerem lub serwerem.

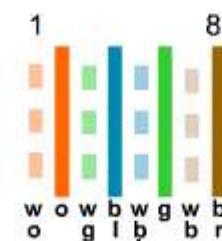
**Kabli z przeplotem należy używać do wykonywania następujących połączeń:**

- połączenie przełącznika z przełącznikiem,
- połączenie przełącznika z koncentratorem,
- połączenie koncentratora z koncentratorem,

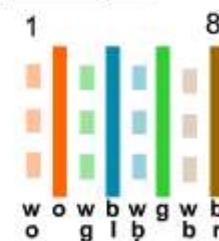
## Zastosowanie skrętki nieekranowanej

### Styk Etykieta

1	TD+
2	TD-
3	RD+
4	NC
5	NC
6	RD-
7	NC
8	NC



### kabel prosty



Przewody na obu końcach kabla są ułożone w tej samej kolejności.

## Łączenie urządzeń przy użyciu kabla z przeplotem

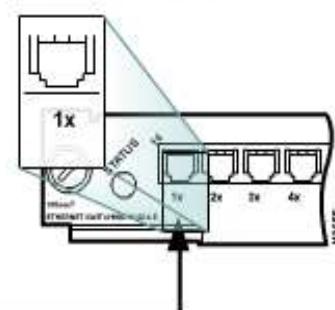
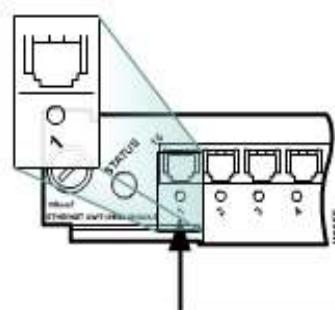
### Styk Etykieta Styk Etykieta

1	RD+	1	TD+
2	RD-	2	TD-
3	TD+	3	RD-
4	NC	4	NC
5	NC	5	NC
6	TD-	6	RD-
7	NC	7	NC
8	NC	8	NC

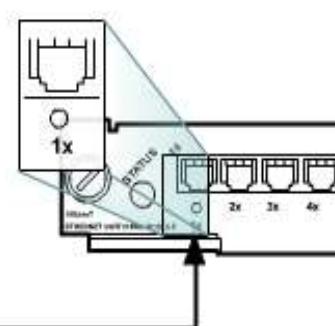
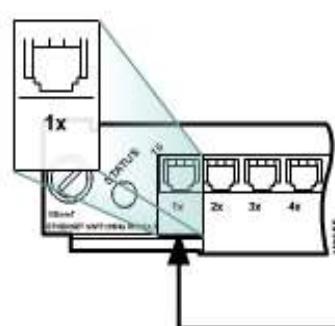


Para przewodów pomarańczowych i para przewodów zielonych są zamienione miejscami na jednym końcu

## Zastosowanie skrętki nieekranowanej kabla z przeplotem



Jeśli jeden port jest oznaczony znakiem x, należy użyć kabla prostego.



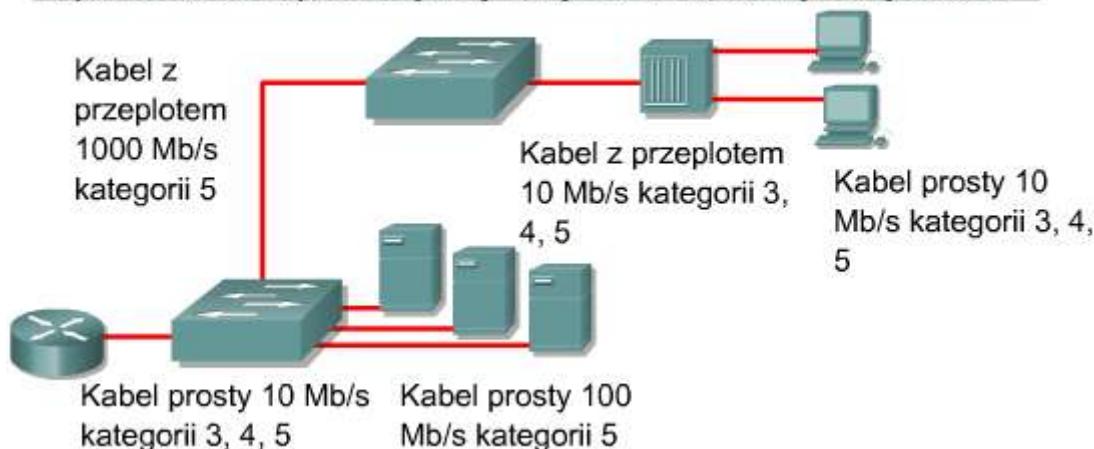
Jeśli OBYDWA porty są oznaczone znakami x lub żaden z nich nie jest tak oznaczony, należy użyć kabla z przeplotem.

- połączenie routera z routeraem,
- połączenie komputera z komputerem,
- połączenie routera z komputerem.

Na rysunku ostatnim pokazano, jak szeroka może być gama kabli potrzebnych w jednej sieci komputerowej.

Wymagana kategoria kabla UTP zależy od wybranego typu sieci Ethernet.

### Łączenie urządzeń przy użyciu kabla z przeplotem



### 5.1.6 Wtórnikи

Angielski odpowiednik terminu „wtórnik”, czyli „repeater” (dosłownie „powtarzacz”), pochodzi z wczesnego okresu prób przekazywania informacji na duże odległości. Odnosi się on do sytuacji, w której osoba znajdująca się na pewnym wzgórzu powtarza sygnał odebrany od osoby znajdującej się na poprzednim wzgórzu. Proces ten trwał tak długo, aż wiadomość dotarła do celu. W przypadku telegrafu, telefonu, urządzeń mikrofalowych i światłowodowych wtórnikи są używane do wzmacniania sygnałów przesyłanych na duże odległości.

Wtórnik odbiera sygnał, regeneruje go i przesyła dalej. Wtórnik prowadzi regenerację i resynchronizację sygnałów sieciowych na poziomie bitów, co umożliwia przesyłanie ich na większe odległości. Standardy Ethernet oraz IEEE 802.3 wprowadzają jednakże zasadę 5-4-3 określającą liczbę wtórników i segmentów przy dostępie współdzielonym w szkielecie topologii drzewiastej. Zasada 5-4-3 wyróżnia w sieci dwa typy fizycznych segmentów: segment z użytkownikami oraz segment bez użytkowników (połączeniowy). Do segmentu z użytkownikami dołączone są komputery użytkowników. Natomiast segmenty połączeniowe służą tylko do bezpośredniego połączenia dwóch wtórników. Zasada mówi, że pomiędzy dowolnymi węzłami w sieci może być maksymalnie pięć segmentów, połączonych przez cztery wtórnikи lub koncentratory i tylko trzy z tych pięciu segmentów mogą mieć dołączonych użytkowników.

Protokół Ethernet wymaga, by sygnał wysłany poprzez LAN dotarł do każdej części sieci w określonym przedziale czasu. To właśnie zapewnia zasadę 5-4-3. Każdy wtórnik, który retransmituje sygnał dodaje pewne niewielkie opóźnienie do sygnału, więc zasadę tę zaprojektowano, aby zminimalizować czas transmisji. Zbyt duże opóźnienie w sieci LAN zwiększa liczbę spóźnionych kolizji i zmniejsza wydajność sieci LAN.

### 5.1.7 Koncentratory

Koncentratory są w rzeczywistości wieloportowymi wtórnikami. W wielu wypadkach jedyna różnica między tymi dwoma urządzeniami wynika z liczby dostępnych portów. Zwykły wtórnik jest wyposażony w dwa porty, a koncentrator może mieć od czterech do dwudziestu czterech portów. Koncentratory są najczęściej używane w sieciach Ethernet 10BASE-T lub 100BASE-T, chociaż występują także w innych architekturach sieciowych.

Zastosowanie koncentratora powoduje zmianę topologii sieci z liniowej topologii magistrali, w której poszczególne urządzenia są podłączone bezpośrednio do przewodu, na topologię gwiazdy. W przypadku zastosowania koncentratorów dane dochodzące do portu koncentratora są elektrycznie powielane we wszystkich pozostałych portach podłączonych do tego samego segmentu sieci — oprócz portu, z którego zostały odebrane.

Istnieją trzy podstawowe typy koncentratorów:

- **Pasywne:** Koncentrator pasywny jest po prostu fizycznym punktem połączenia. Nie modyfikuje on ani nie analizuje ruchu, który przez niego przechodzi. Nie wzmacnia też ani nie usuwa zakłóceń sygnału. Koncentrator pasywny służy jedynie podłączeniu urządzeń do współdzielonego medium. Nie wymaga zasilania.
- **Aktywne:** Koncentrator aktywny musi być podłączony do gniazdka elektrycznego, ponieważ potrzebuje zasilania, aby wzmacnić przychodzący sygnał przed przekazaniem go do innych portów.
- **Inteligentne:** Po angielsku koncentratory inteligentne są czasem nazywane „smart hubs” („sprytne koncentratory”). Urządzenia te działają jak koncentratory aktywne, a oprócz tego są wyposażone w mikroprocesor i udostępniają funkcje diagnostyczne. Koncentratory inteligentne są droższe niż koncentratory aktywne, ale za to bardziej użyteczne przy rozwiązywaniu problemów.



Urządzenia podłączone do koncentratora odbierają cały ruch, który przez niego przechodzi. Im więcej urządzeń jest podłączonych do koncentratora, tym bardziej prawdopodobne jest występowanie kolizji. Kolizja zachodzi wtedy, gdy w tym samym czasie więcej niż jedna stacja robocza wysła dane przez sieć. W takiej sytuacji wszystkie dane ulegają uszkodzeniu. O urządzeniach dołączonych do tego samego segmentu sieci mówi się, że należą do jednej domeny kolizyjnej. Nazwa koncentrator wynika z faktu, że takie urządzenie jest centralnym punktem lokalnej sieci Ethernet.

### 5.1.8 Łączność bezprzewodowa

Sieć bezprzewodową można zbudować przy użyciu znacznie mniejszej ilości okablowania niż w wypadku innych sieci. Sygnały bezprzewodowe to fale elektromagnetyczne rozchodzące się w powietrzu. W sieciach bezprzewodowych do przenoszenia sygnałów z jednego komputera do innego bez stałego połączenia kablowego wykorzystywane jest promieniowanie elektromagnetyczne o częstotliwościach radiowych (RF), generowane przez lasery, o częstotliwościach w zakresie podczerwieni (IR) oraz mikrofale (łączność satelitarna). Okablowanie występuje tylko w punktach dostępu do sieci. Stacje robocze znajdujące się w zasięgu sieci bezprzewodowej można łatwo przenosić bez potrzeby rozłączania i podłączania okablowania sieciowego.

Komunikacja bezprzewodowa jest powszechnie stosowana, jeśli chodzi o komputery znajdujące się w ruchu. Dzieje się tak w wypadku telepracowników, samolotów, satelitów, sond kosmicznych, promów kosmicznych i stacji kosmicznych.

Podstawowymi elementami sieci bezprzewodowej są urządzenia nazywane nadajnikami i odbiornikami. Nadajnik przekształca dane źródłowe w fale elektromagnetyczne (EM), które są przesyłane do odbiornika. Odbiornik przekształca te fale elektromagnetyczne ponownie w dane, które są dostarczane do urządzenia docelowego. Aby możliwa była dwukierunkowa komunikacja, każde z urządzeń musi być wyposażone zarówno w nadajnik, jak i w odbiornik. Wielu producentów urządzeń sieciowych łączy nadajnik i odbiornik w jedną jednostkę. Takie urządzenie nosi nazwę „nadajnik-odbiornik” (ang. transceiver) lub „bezprzewodowa karta sieciowa”. Wszystkie urządzenia w bezprzewodowej sieci LAN (WLAN) muszą być wyposażone w odpowiednie bezprzewodowe karty sieciowe.

W przypadku sieci komputerowych najczęściej wykorzystywanymi technikami bezprzewodowymi są IR (podczerwień) i RF (częstotliwości radiowe). Technika IR ma swoje wady. Aby działanie takiej sieci było możliwe, stacje robocze i urządzenia cyfrowe muszą znajdować się „na linii wzroku” nadajnika. Sieci wykorzystujące promieniowanie podczerwone stanowią dobre rozwiązanie, jeśli wszystkie urządzenia cyfrowe wymagające połączenia z siecią znajdują się w jednym pomieszczeniu. Sieć taką można szybko zbudować, ale sygnały danych mogą być tłumione lub zakłócone przez osoby chodzące po pokoju lub wilgoć w powietrzu. Opracowywane są jednak nowe techniki IR, które będą mogły działać również poza linią wzroku.

Techniki radiowe (RF) mogą być stosowane, gdy urządzenia znajdują się w różnych pomieszczeniach, a nawet w różnych budynkach. Zastosowanie tego rodzaju sieci jest ograniczone zasięgiem sygnałów radiowych. W przypadku techniki RF można wykorzystywać jedną lub wiele częstotliwości.

Pojedyncza częstotliwość może ulegać zewnętrznym zakłóceniom i zniekształceniom wynikającym z ukształtowania terenu. Może też zostać łatwo podsłuchana, co sprawia, że transmisja danych nie jest bezpieczna. Problem zabezpieczenia transmisji danych można rozwiązać, rozpraszając widmo sygnału przez użycie wielu częstotliwości, dzięki czemu będzie on bardziej odporny na zakłócenia i trudniejszy do podsłuchania.

Obecnie rozproszenie widma transmisji w sieciach WLAN uzyskuje się przy użyciu dwóch metod: FHSS (skokowa zmiana częstotliwości w widmie rozproszonym) i DSSS (sekwencja bezpośrednia w widmie rozproszonym). Szczegóły techniczne dotyczące działania tych metod wykraczają poza zakres materiału tego kursu.

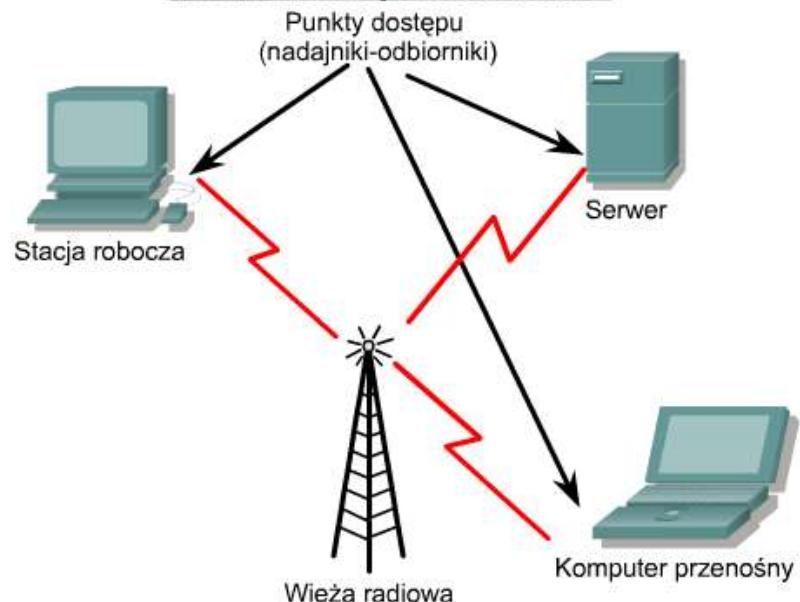
### 5.1.9 Mosty

Czasami istnieje konieczność podzielenia dużej sieci LAN na mniejsze, łatwiejsze do zarządzania segmenty. Pozwala to zmniejszyć ruch w pojedynczej sieci LAN i zwiększyć geograficzny zasięg sieci ponad obszar, który może obsługiwać pojedynczą sieć lokalną. Do łączenia segmentów sieci służą takie urządzenia, jak mosty, przełączniki, routery i bramy. Przełączniki i mosty działają w warstwie łącza danych modelu OSI. Zadaniem mostu jest podejmowanie decyzji, czy sygnały należy przesyłać do sąsiedniego segmentu sieci, czy też nie.

W chwili odebrania ramki z sieci w tablicy mostu sprawdzany jest docelowy adres MAC i na tej podstawie następuje filtracja, rozgłoszanie lub skopiowanie ramki do drugiego segmentu. Proces decyzyjny przebiega następująco:

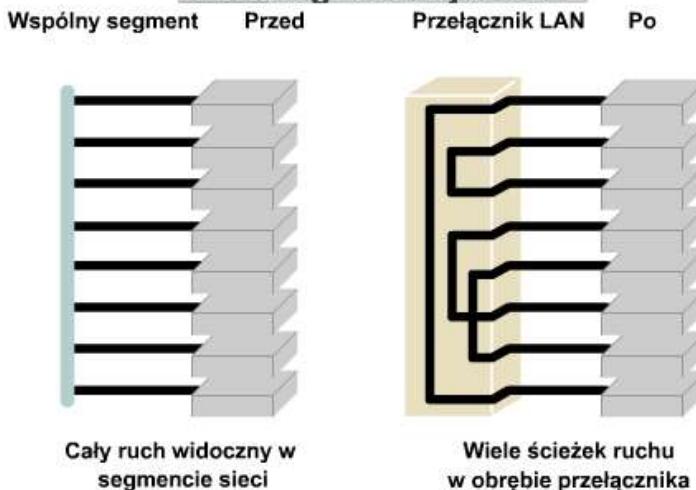
- Jeśli urządzenie docelowe znajduje się w tym samym segmencie co ramka, most blokuje przejście ramki do innych segmentów. Takie działanie nosi nazwę filtracji.

### Medium bezprzewodowe



- Jeśli urządzenie docelowe znajduje się w innym segmencie, most przekazuje ramkę do odpowiedniego segmentu.
- Jeśli adres docelowy nie jest znany mostowi, ramka jest przekazywana do wszystkich segmentów oprócz tego, z którego została odebrana. Takie działanie nosi nazwę rozgłaszenia.
- Właściwe umiejscowienie mostu może znacznie zwiększyć wydajność sieci.

### Mikrosegmentacja sieci



Wydzielone ścieżki między hostem nadawcy i hostem odbiorcy

### **5.1.10 Przełączniki**

Przełącznik można opisać jako wieloportowy most. Typowy most może być wyposażony jedynie w dwa porty łączące dwa segmenty sieci, natomiast przełącznik może mieć wiele portów. Liczba portów zależy od tego, ile segmentów sieci trzeba połączyć. Podobnie jak dzieje się to w przypadku mostów, przełączniki wykorzystują informacje o pakietach odbieranych z różnych komputerów w sieci. Informacje te są używane do tworzenia tablic przesyłania, które pozwalają określić miejsce docelowe dla danych przesyłanych między komputerami w sieci.

Chociaż oba urządzenia są podobne, przełącznik jest bardziej zaawansowaną konstrukcją niż most. W przypadku mostu konieczność przekazania ramki do drugiego segmentu sieci jest określana na podstawie adresu MAC. Przełącznik natomiast jest wyposażony w wiele portów, do których jest podłączonych wiele segmentów sieci. Przełącznik wybiera port, do którego jest podłączone docelowe urządzenie lub stacja robocza.

Przełączniki sieci Ethernet stają się bardzo popularnym rozwiązaniem, ponieważ — podobnie jak mosty — pozwalają na zwiększenie wydajności sieci poprzez zwiększenie szybkości i szerokości pasma.

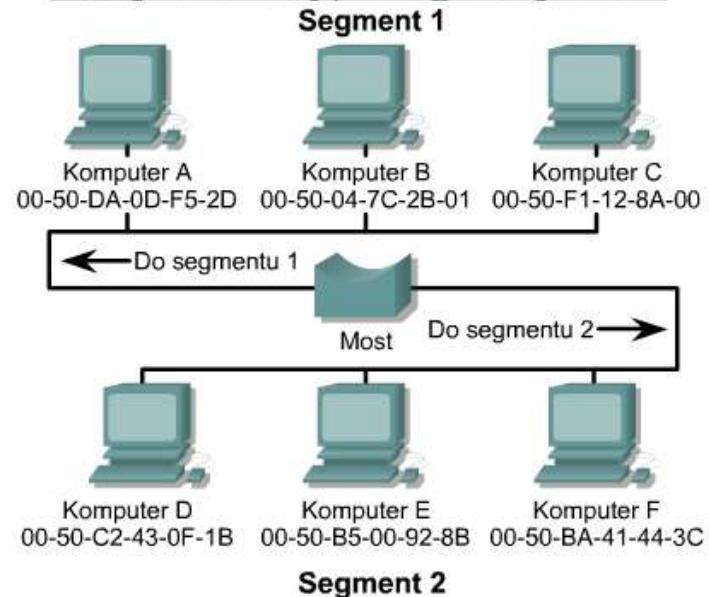
Przełączanie jest techniką zmniejszającą przeciążenie sieci Ethernet LAN przez obniżenie ruchu i zwiększenie szerokości pasma. Koncentratory można łatwo zastąpić przełącznikami, ponieważ nie wymaga to wymiany istniejącego okablowania. Umożliwia to zwiększenie wydajności bez zbytniej ingerencji w istniejącą sieć.

We współczesnej komunikacji wszystkie urządzenia

przełączające wykonują dwie podstawowe operacje. Pierwsza operacja nosi nazwę przełączania (komutacji) ramek danych. Przełączanie ramek jest procesem, w którym rama jest odbierana z medium wejściowego, a następnie jest przesyłana do medium wyjściowego. Drugi aspekt działania jest związany z obsługą przełączzeń, co obejmuje tworzenie i utrzymywanie tablic przełączzeń oraz wyszukiwanie pętli.

Przełączniki działają znacznie szybciej niż mosty i mogą obsługiwać nowe funkcje, takie jak wirtualne sieci LAN.

### Mosty rozdzielające segmenty sieci

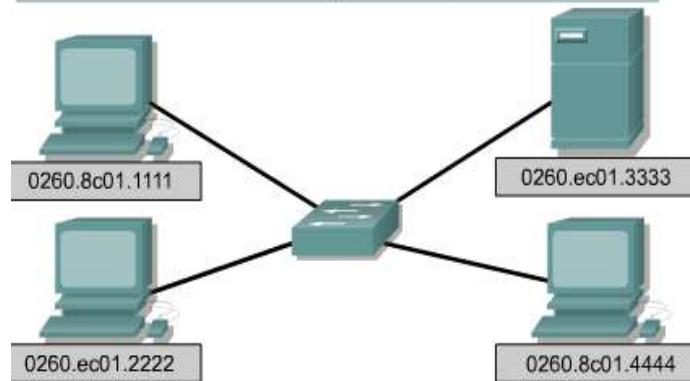


**Przełącznik Cisco serii 2900**



**Tablica przełączania**

Interfejs	Adres MAC
E0	0260.8c01.1111
E0	0260.ec01.2222
E1	0260.ec01.3333
E1	0260.8c01.4444



Przełącznik Ethernet ma wiele zalet. Jedną z jego zalet jest to, że umożliwia wielu użytkownikom komunikację równoległą przez wykorzystanie obwodów wirtualnych i wydzielonych segmentów sieci w środowisku bezkolizyjnym. Dzięki temu następuje maksymalne zwiększenie szerokości pasma dostępnej we współdzielonym medium. Kolejną zaletą stanowi niski koszt wprowadzenia przełączników do sieci LAN ze względu na możliwość wykorzystania istniejących urządzeń i okablowania.

### 5.1.11 Podłączanie hosta

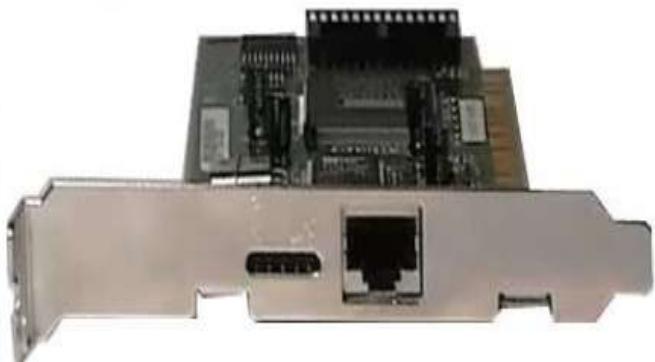
Zadaniem karty sieciowej jest podłączenie hosta do medium sieciowego. Karta sieciowa jest obwodem drukowanym, który można umieścić w złączu rozszerzeń płyty głównej lub urządzenia peryferyjnego komputera. Karty sieciowe są także niekiedy nazywane adapterami sieciowymi. W wypadku komputerów przenośnych karta sieciowa ma rozmiar karty kredytowej. **Karty sieciowe** są zaliczane do urządzeń warstwy 2, ponieważ do każdej karty jest przypisany unikatowy kod nazywany adresem MAC. Jest on używany do sterowania przesyłaniem danych hosta w sieci. Więcej informacji o adresie MAC zostanie podanych później. Karta sieciowa steruje dostępem hosta do medium.

W niektórych przypadkach typ złącza karty sieciowej nie odpowiada typowi medium, które ma być do niej podłączone. Dobrym przykładem takiej sytuacji jest router Cisco 2500. Router jest wyposażony w złącze AUI. Do złącza AUI należy podłączyć kabel UTP kategorii 5 dla sieci Ethernet. W tym celu należy użyć urządzenia o nazwie nadajnik-odbiornik (transceiver). Urządzenie to przekształca jeden rodzaj sygnału lub złącza w inny. Na przykład do złącza RJ-45 można podłączyć 15-stykowy interfejs AUI dzięki zastosowaniu transceivera. Uważa się, że takie urządzenia działają w warstwie 1, ponieważ przetwarzają bity, nie operując informacjami adresowymi ani związanymi z protokołami wyższych warstw. Nie istnieje standardowy symbol, który oznaczałby kartę sieciową. Z góry zakłada się, że gdy urządzenie sieciowe jest przyłączone do sieci, to w tym miejscu znajduje się karta sieciowa lub podobne urządzenie. Każda kropka na mapie topologii oznacza albo kartę sieciową, albo port, który działa jak karta sieciowa.

### Karta sieciowa (płyta z układami scalonymi)



**Karta sieciowa (złącze medium)**

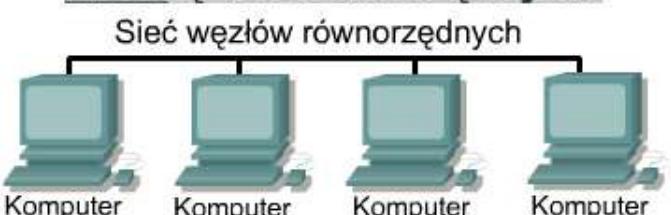


### 5.1.12 Sieć węzłów równorzędnych

Korzystając z technik LAN i WAN, można połączyć wiele komputerów. W celu zapewnienia rozmaitych usług połączone siecią komputery realizują różne funkcje we wzajemnych relacjach. W przypadku niektórych zastosowań komputery muszą działać jak równorzędni partnerzy. Inne aplikacje udostępniają swoje funkcje w sieci, co powoduje powstawanie nierównorzędnych relacji, w których jeden komputer obsługuje wiele innych. W obu wypadkach dwa komputery zwykle komunikują się ze sobą przy użyciu protokołów typu żądanie-odpowiedź. Jeden komputer wysyła żądanie udostępnienia usługi, a drugi odbiera je i reaguje na nie. Komputer żądający staje się klientem, a komputer odpowiadający — serwerem.

W sieci węzłów równorzędnych komputery działają jak równorzędni partnerzy. W takim układzie każdy komputer może realizować zarówno funkcje klienta, jak i serwera. W danej chwili komputer A może zażądać pliku z komputera B, który zareaguje, udostępniając ten plik komputerowi A. Komputer A działa jako klient, a komputer B działa jako serwer. Później oba komputery mogą się zamienić rolami. **W sieci węzłów równorzędnych poszczególni użytkownicy kontrolują swoje własne zasoby.** To oni decydują, czy udostępnić określone pliki innym użytkownikom. Mogą także zażądać hasła przed umożliwieniem innym dostępu do swoich zasobów. Ponieważ to użytkownicy podejmują decyzje, nie ma centralnego punktu sterowania lub administrowania siecią. Ponadto poszczególni użytkownicy muszą tworzyć swoje własne kopie zapasowe systemów, aby mieć możliwość odzyskania danych w przypadku awarii. Gdy dany komputer działa jako serwer, jego użytkownik może zauważać obniżenie wydajności wynikające z obsługi żądań pochodzących z innych komputerów. Instalacja i obsługa sieci węzłów równorzędnych jest względnie łatwa. Oprócz odpowiedniego systemu operacyjnego zainstalowanego w komputerach nie są potrzebne żadne dodatkowe urządzenia. Ponieważ to użytkownicy zarządzają swoimi zasobami, administratorzy nie są potrzebni.

### Sieć węzłów równorzędnych



W miarę rozrastania się sieci coraz trudniej jest koordynować relacje między równorzędnymi węzłami. Sieć węzłów równorzędnych działa dobrze, gdy jest w niej 10 lub mniej komputerów. Ze względu na to, że sieci węzłów równorzędnych nie są zbyt dobrze skalowalne, ich wydajność gwałtownie maleje, gdy liczba komputerów w sieci rośnie. Poza tym, z racji tego, że użytkownicy sterują dostępem do zasobów na swoich komputerach, zapewnienie odpowiedniego poziomu bezpieczeństwa może być utrudnione. Ograniczenia dotyczące sieci węzłów równorzędnych można zlikwidować, stosując model pracy klient-serwer.

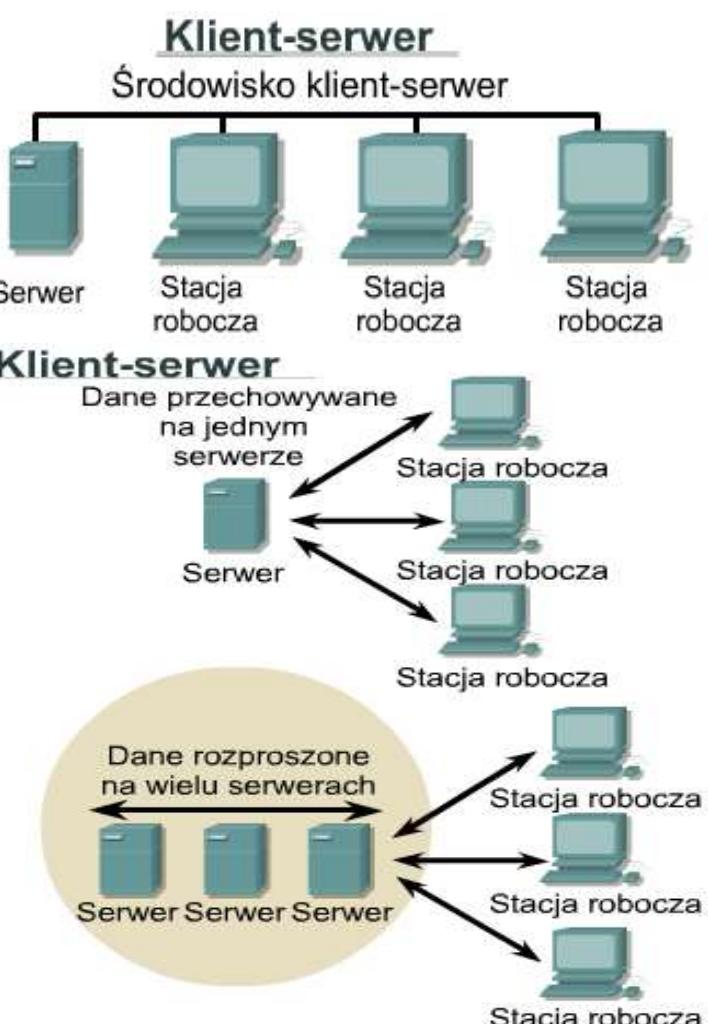
### 5.1.13 Sieć klient-serwer

W modelu klient-serwer usługi sieciowe są udostępniane przez wyznaczony komputer nazywany serwerem. Serwer odpowiada na żądania klientów. Serwer jest komputerem centralnym, który jest cały czas dostępny, aby mógł reagować na żądania klientów dotyczące plików, drukowania, aplikacji i innych usług. Większość sieciowych systemów operacyjnych oparta jest na modelu klient-serwer. Zwykle komputery stojące na biurkach działają jako klienci, a jeden lub kilka komputerów dysponujących większą mocą obliczeniową, pamięcią i specjalnym oprogramowaniem działają jako serwery. Serwery są tak zaprojektowane, aby mogły jednocześnie obsługiwać żądania wielu klientów. Przed uzyskaniem dostępu do zasobów serwera, klient musi zostać rozpoznany i uwierzyteliony. Jest to realizowane poprzez przypisanie każdemu klientowi nazwy konta i hasła, które jest sprawdzane przez usługę uwierzytelniającą. Usługa uwierzytelniająca działa jak strażnik strzegący dostępu do sieci. Dzięki centralnemu zarządzaniu kontami użytkowników, zabezpieczeniami i dostępem model sieci oparty na serwerach upraszcza administrowanie dużymi sieciami.

Skoncentrowanie na serwerach zasobów sieciowych, takich jak pliki, drukarki i aplikacje, ułatwia także tworzenie i obsługę kopii zapasowych generowanych danych. Zamiast przechowywać zasoby rozproszone po poszczególnych komputerach, można przechowywać je na specjalnych wydzielonych serwerach, co sprawia, że są łatwiej dostępne. Większość systemów typu klient-serwer umożliwia rozszerzanie możliwości sieci poprzez dodawanie nowych usług, które zwiększą jej użyteczność.

Rozdzielenie funkcji w sieciach klient-serwer ma wiele zalet, ale wiążą się z tym także pewne koszty. Chociaż nagromadzenie zasobów na systemach serwerów zapewnia większe bezpieczeństwo, łatwiejszy dostęp i skoordynowaną kontrolę, serwer staje się newralgicznym punktem awarii sieci. Jeśli nie działa serwer, sieć w ogóle nie może funkcjonować. Do administrowania serwerami i ich obsługi niezbędny jest przeszkolony i doświadczony personel. Zwiększa to koszt działania takiej sieci. Systemy serwerów wymagają także dodatkowych urządzeń i specjalnego oprogramowania, co dodatkowo zwiększa koszt.

Na rysunkach i przedstawiono podsumowanie zalet i wad sieci węzłów równorzędnych oraz sieci klient-serwer.



### Sieć węzłów równorzędnych a sieć klient-serwer

Zalety sieci węzłów równorzędnych	Zalety sieci klient-serwer
Tańsza implementacja.	Lepsze zabezpieczenia.
Nie wymaga dodatkowego specjalnego oprogramowania do administrowania siecią.	Łatwiejsze administrowanie, gdy sieć jest duża, ponieważ administracja jest skoncentrowana.
Nie jest wymagany administrator sieci.	Kopie zapasowe wszystkich danych można umieścić w jednym miejscu.

## Sieć węzłów równorzędnych a sieć klient-serwer

Wady sieci węzłów równorzędnych	Wady sieci klient-serwer
W przypadku dużych sieci nie funkcjonuje zbyt dobrze i trudno nią administrować.	Wymaga kosztownego specjalnego oprogramowania do administrowania siecią i jej obsługi.
Każdy użytkownik musi umieć wykonywać zadania administracyjne.	Komputer pełniący rolę serwera jest bardziej kosztowny i wydajniejszy.
Jest mniej bezpieczna.	Wymaga doświadczonego administratora.
Wszystkie komputery korzystające z udostępnionych zasobów obniżają wydajność.	Awaria w jednym punkcie może spowodować awarię całej sieci. Dane użytkowników są niedostępne, gdy serwer nie działa.

## 5.2 Okablowanie sieci WAN

### 5.2.1 Warstwa fizyczna sieci WAN

Implementacje warstwy fizycznej różnią się w zależności od odległości urządzeń od usług, szybkości i typu samej usługi. Połączenia szeregowe są używane do obsługi takich usług WAN, jak wydzielone linie dzierżawione wykorzystujące protokół PPP (Point-to-Point

Protocol) lub Frame Relay. Szybkość tych połączeń mieści się w zakresie od 2400 b/s do 1,544 Mb/s w przypadku usługi T1 i 2,048 Mb/s w przypadku usługi E1.

Sieć ISDN udostępnia połączenia na żądanie oraz usługi zwrotnego wybierania numeru. Interfejs ISDN BRI (Basic Rate Interface) składa się z dwóch kanałów do przenoszenia

informacji (kanały B) o szybkości 64 kb/s oraz jednego kanału D o szybkości 16 kb/s używanego do celów sygnalizacyjnych i innych zadań związanych z zarządzaniem łączem. W celu przenoszenia danych kanałem B jest zwykle używany protokół PPP.

Wraz ze wzrostem zapotrzebowania na usługi szerokopasmowe o dużej szybkości w budynkach mieszkalnych coraz bardziej popularne stają się połączenia DSL i modemy kablowe. Na przykład typowe stałe łącze DSL może zapewnić szybkość standardu T1/E1 za pośrednictwem istniejącej linii telefonicznej. W wypadku usług kablowych wykorzystywany jest istniejący kabel koncentryczny linii telewizji kablowej. Kabel koncentryczny umożliwia łączność dorównującą szybkością łączom DSL lub nawet szybszą. Usługi DSL i modemy kablowe zostaną omówione bardziej szczegółowo w innym module.

### 5.2.2 Połączenia szeregowe w sieciach WAN

Do komunikacji na duże odległości w sieciach WAN wykorzystywana jest transmisja szeregową. Polega ona przesyłaniu bitów danych pojedynczym kanałem. Proces ten zapewnia niezawodną komunikację na duże odległości oraz umożliwia wykorzystanie konkretnych zakresów częstotliwości sygnałów elektromagnetycznych i optycznych.

Częstotliwości są mierzane liczbą cykli na sekundę, a wyrażane są w hercach (Hz). W wypadku sygnałów przesyłanych głosową linią telefoniczną używany jest zakres częstotliwości o szerokości 4 kHz. Szerokość zakresu częstotliwości jest nazywana szerokością pasma. W sieciach komputerowych szerokość pasma jest mierzona liczbą bitów przesyłanych w ciągu sekundy.

W wypadku routera firmy Cisco połączenie fizyczne w siedzibie klienta jest realizowane przy wykorzystaniu jednego spośród dwóch typów połączeń szeregowych. Pierwszy typ połączenia szeregowego to łącze o 60 stykach. Drugie łącze

Typy usług w sieciach WAN					
Cisco HDLC	PPP	Frame Relay	ISDN BRI	Modem DSL	Modem kablowy
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 High Speed Serial Interface (HSSI)	RJ-45 Uwaga: Styki wyjściowe interfejsu ISDN BRI różnią się od styków sieci Ethernet.	RJ-11 Działa na linii telefonicznej.	F Działa na linii telewizji kablowej.		

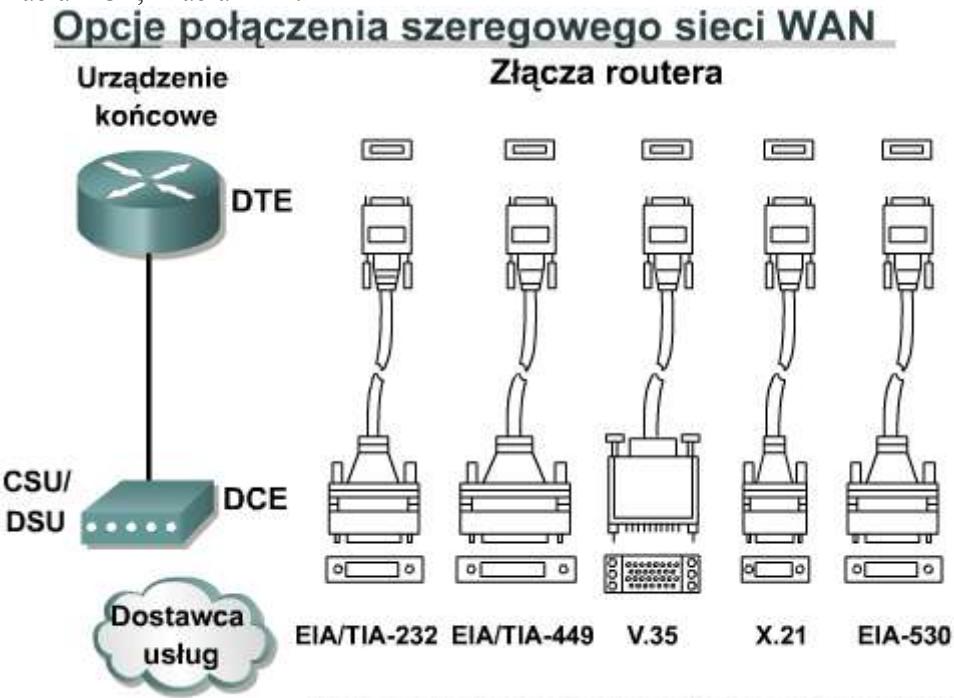
- Istnieją rozmaite implementacje warstwy fizycznej.
- Specyfikacje kabli określają szybkość łączą.

### Porównanie standardów fizycznych

Dane (b/s)	Odległość (metry)	
	EIA/TIA-232	EIA/TIA-449
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1 (1.544 Mbps)	—	15

jest nieco mniejsze. Jest ono nazywane szeregowym złączem „inteligentnym”. Rodzaj złącza zależy od typu używanych urządzeń.

Jeśli występuje bezpośrednie połączenie z dostawcą usługi lub z urządzeniem generującym sygnał taktujący, takim jak jednostka CSU/DSU, router stanowi urządzenie DTE i należy użyć szeregowego kabla DTE. Zwykle tak właśnie jest. Czasami jednak to lokalny router musi zapewnić sygnał taktujący i wtedy należy użyć kabla DCE. W ćwiczeniu dotyczącym routerów jeden z łączonych routerów będzie musiał realizować funkcje taktowania. Połączenie będzie więc wymagało użycia i kabla DCE, i kabla DTE.



### Połączenia sieciowe w jednostce CSU/DSU

#### 5.2.3 Routery i połączenia szeregowe

Zadaniem routerów jest wybór trasy dla pakietów od źródła do celu w sieci LAN oraz zapewnienie łączności z siecią WAN. W środowisku sieci LAN router ogranicza rozgłoszanie, udostępnia usługi określania lokalnych adresów, takie jak ARP i RARP, oraz umożliwia segmentację sieci przy wykorzystaniu struktury podsieci. Aby realizacja tych usług była możliwa, router musi być podłączony do sieci LAN i WAN.

Oprócz wybrania typu kabla, trzeba także określić, czy należy użyć złącza DTE, czy też DCE. Złącze DTE jest końówką łącza WAN podłączoną do urządzenia użytkownika. Złącze DCE zwykle stanowi punkt, w którym odpowiedzialność za dostarczenie danych przechodzi w ręce dostawcy usług.

W przypadku bezpośredniego połączenia z dostawcą usług lub takim urządzeniem, jak jednostka CSU/DSU, które będzie generowało sygnał taktujący, router jest urządzeniem DTE i wymaga użycia kabla szeregowego DTE. Jest to typowa sytuacja w przypadku podłączania routera. Jednak w niektórych przypadkach to router musi pełnić funkcję urządzenia DCE. W środowisku testowym realizacja bezpośredniego połączenia dwóch routerów wymaga, aby jeden z nich pełnił rolę urządzenia DTE, a drugi — urządzenia DCE.

Wykonując okablowanie routerów do połączenia szeregowego, można skorzystać z portów wbudowanych lub modułowych. Typ użytego portu będzie miał wpływ na składnię, której trzeba będzie użyć do skonfigurowania każdego interfejsu.

**Interfejsy routerów o stałych portach szeregowych mają oznaczenie typu portu i numeru portu.**

**Interfejsy routerów o modułowych portach szeregowych mają oznaczenie typu portu, gniazda i numeru portu.**  
Gniazdo jest miejscem, w którym umieszcza się moduł. Aby skonfigurować port na karcie modułowej, należy zdefiniować interfejs, używając składni „<typ portu> <numer gniazda>/<numer portu>”. Na przykład, gdy interfejs jest szeregowy, moduł jest zainstalowany w gnieździe 1, a numer portu jest równy 0, należy użyć składni „serial 1/0”.

#### Urządzenia DTE i DCE pracujące na łączach szeregowych

##### Urządzenie końcowe DTE

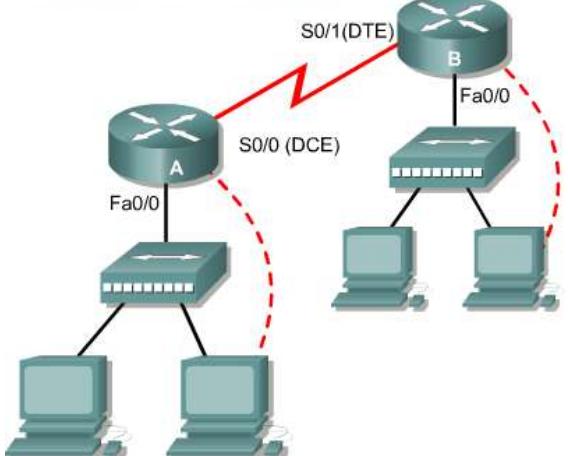
- końówka urządzenia użytkownika na łączu WAN

##### Urządzenie komunikacyjne DCE

- końówka ciągu komunikacyjnego ze strony dostawcy usług sieci WAN
- odpowiada za synchronizację w czasie

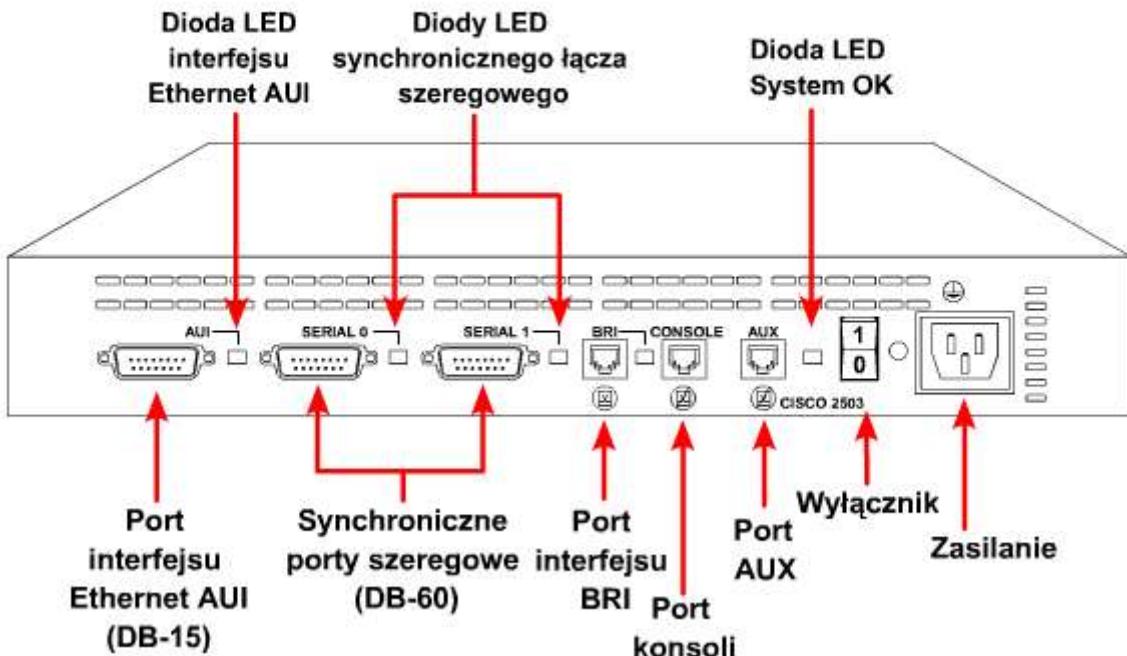


#### Bezpośrednie połączenie szeregowe



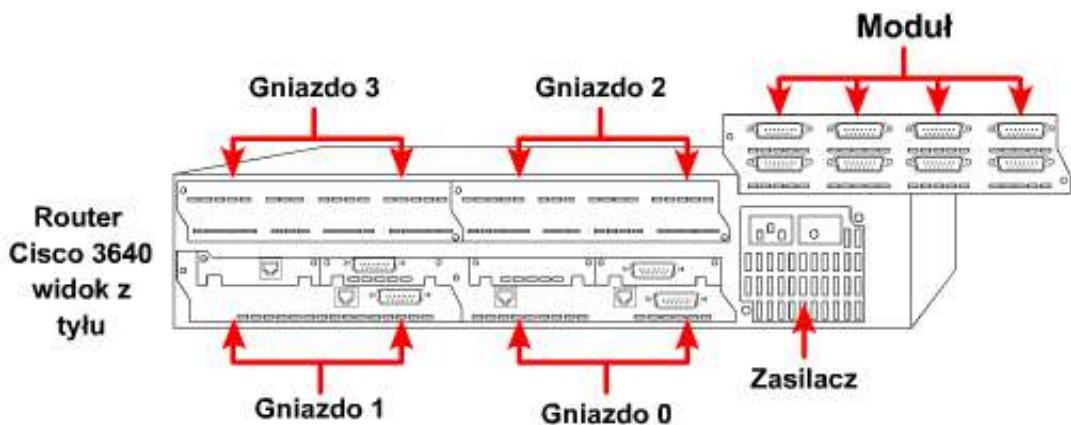
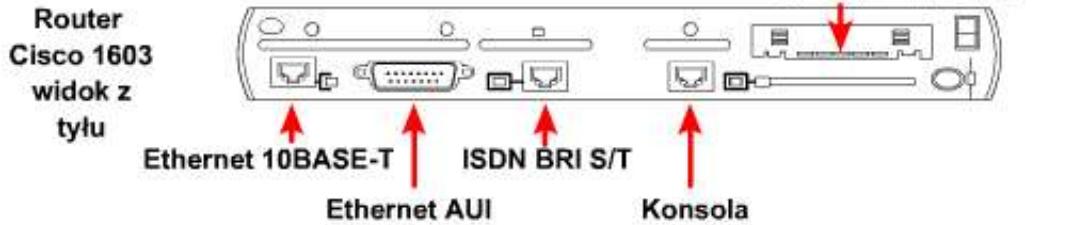
## Wbudowane interfejsy

**Router Cisco 2503 widok z tyłu**



## Modułowe interfejsy szeregowe

**Szergowe porty sieci WAN mogą mieć konstrukcję modularną**



### 5.2.4 Routery i połączenia ISDN BRI

W przypadku interfejsów ISDN BRI dostępne są dwa ich typy: BRI S/T i BRI U. Aby określić, który typ jest wymagany, należy sprawdzić, kto dostarczył urządzenie NT1.

Urządzenie NT1 znajduje się między routerem i przełącznikiem ISDN dostawcy usług. Jest ono używane do połączenia czteroprzewodowego okablowania abonenta z konwencjonalną dwuprzewodową pętlą lokalną. W Ameryce Północnej urządzenie NT1 zwykle instalowane jest przez klienta, podczas gdy w innych częściach świata to dostawca usług zapewnia urządzenie NT1.

Jeśli urządzenie NT1 nie jest zintegrowane z routerem, może zaistnieć konieczność użycia zewnętrznego urządzenia NT1.

Czy w routerze znajduje się zintegrowane urządzenie NT1, można łatwo sprawdzić na etykietce interfejsów routera.

Interfejs BRI ze zintegrowanym urządzeniem NT1 jest oznaczony jako BRI U. Interfejs BRI bez urządzenia NT1 jest oznaczony jako BRI S/T. Ze względu na to, że router może być wyposażony w kilka różnych interfejsów ISDN, podczas

zakupu należy określić, jaki interfejs jest potrzebny. Typ interfejsu BRI można określić, patrząc na etykietę portu. Do połączenia portu ISDN BRI z urządzeniem dostawcy usług należy użyć prostego kabla UTP kategorii 5. **UWAGA:** Bardzo ważne jest, aby kabel biegący od portu ISDN BRI został włożony wyłącznie do gniazda ISDN lub przełącznika ISDN. Napięcia używane w interfejsie ISDN BRI mogą poważnie uszkodzić urządzenia inne niż urządzenia ISDN.

### 5.2.5 Routery i połączenia DSL

Router Cisco 827 ADSL jest wyposażony w jeden interfejs ADSL. Aby podłączyć linię ADSL do portu ADSL routera, należy wykonać następujące czynności:

- podłączyć kabel telefoniczny do portu ADSL routera;
- podłączyć drugi koniec kabla do gniazdka telefonicznego.

Aby podłączyć router do usługi DSL, należy użyć kabla telefonicznego ze złączami RJ-11. Łącze DSL działa na standardowej linii telefonicznej, wykorzystując styki 3 i 4 standardowego złącza RJ-11.

### 5.2.6 Routery i połączenia kablowe

Router Cisco uBR905 umożliwia abonentom w małych biurach lub biurach domowych (SOHO) szybki dostęp do sieci poprzez system telewizji kablowej. Router uBR905 jest wyposażony w interfejs do kabla koncentrycznego lub złącza typu F, który umożliwia bezpośrednie podłączenie routera do systemu telewizji kablowej. W celu podłączenia routera do systemu telewizji kablowej używany jest kabel koncentryczny i złącze typu F.

Aby podłączyć router Cisco uBR905 do systemu telewizji kablowej, należy wykonać następujące czynności:

- Upewnij się, że router nie jest podłączony do źródła zasilania.
- Znajdź kabel koncentryczny RF wychodzący ześciennego koncentrycznego gniazdka telewizji kablowej.
- W razie potrzeby zainstaluj rozgałęźnik kabla, aby rozdzielić sygnały dla telewizora i komputera. Jeśli jest to konieczne, zainstaluj filtr górnoprzepustowy, aby zlikwidować wzajemne zakłócanie się sygnałów przeznaczonych dla telewizora i komputera.
- Podłącz kabel koncentryczny do złącza typu F w routerze. Dokrć końcówkę kabla palcami, upewnij się, że jest dokręcona na tyle, na ile jest to możliwe bez użycia klucza, a następnie dokrć ją jeszcze o 1/6 obrotu przy użyciu klucza.
- Upewnij się, że wszystkie pozostałe złącza kabli koncentrycznych, rozgałęźniki, przejściówka i uziemienia są trwale zamocowane na całej drodze od punktu dystrybucyjnego do routera Cisco uBR905.

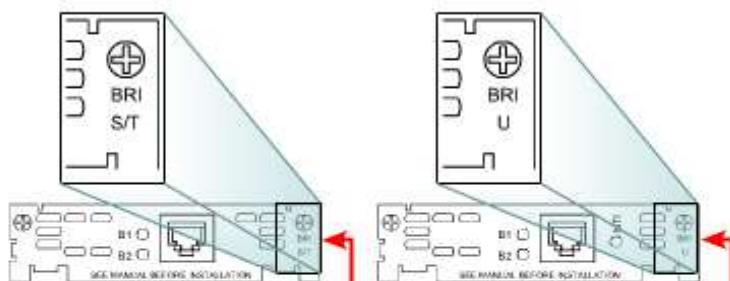
#### **UWAGA:**

Złącza nie należy dokręcać zbyt mocno. Może to spowodować jego pęknięcie. Nie należy używać klucza dynamometrycznego, ponieważ grozi to dokręceniem złącza o więcej niż zalecone 1/6 obrotu po dokręceniu go palcami.

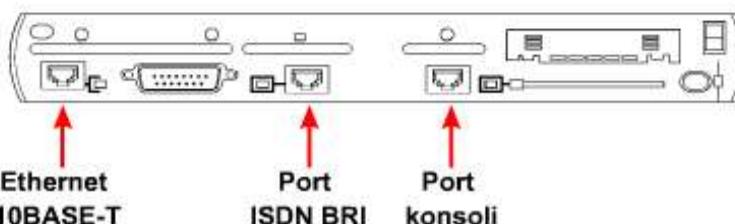
## Interfejsy routera do łączy ISDN

Określ, czy potrzebny jest interfejs BRI S/T, czy BRI U.

Routery są wyposażone w porty jednego lub obydwu typów.



Sprawdź etykietę portu

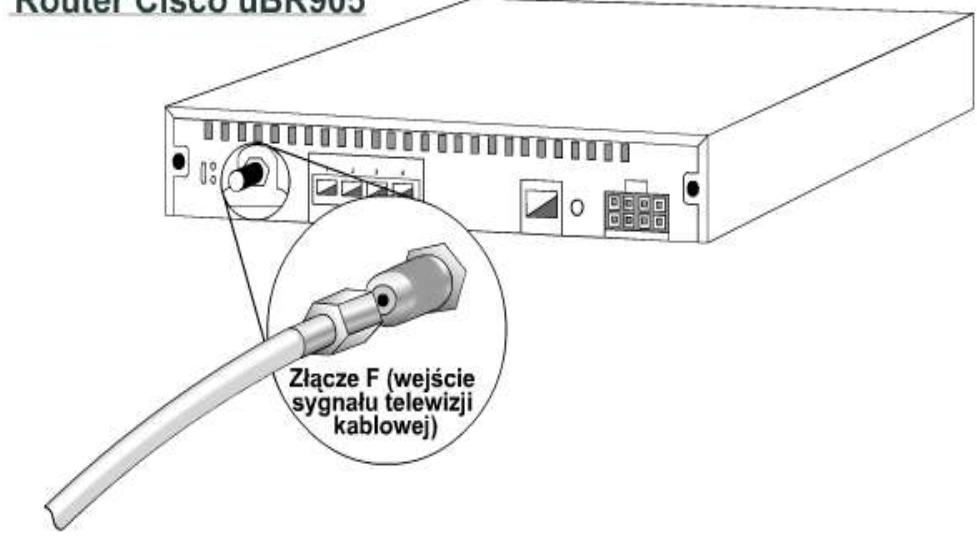


Router Cisco 827-4V



Gniazdko ścienne

### Router Cisco uBR905



Do źródła sygnału telewizji kablowej

Złącze F (wejście sygnału telewizji kablowej)

## 5.2.7 Połączenia z konsolą

W celu przeprowadzenia wstępnej konfiguracji urządzenia Cisco należy je podłączyć bezpośrednio do konsoli zarządzającej. Port zarządzający w wypadku urządzeń Cisco jest nazywany portem konsoli. Port konsoli umożliwia monitorowanie i konfigurację koncentratora, przełącznika lub routera firmy Cisco.

Między terminaliem i portem konsoli należy użyć kabla do konsoli (rollover) ze złączami RJ-45. W kablu rollover, nazywanym także kablem konsolowym, przewody ułożone są w innej kolejności niż w kablach prostych lub kablach z przeplotem ze złączami RJ-45, które są używane w interfejsach Ethernet lub ISDN BRI. Styki kabla do konsoli są połączone w następujący sposób:

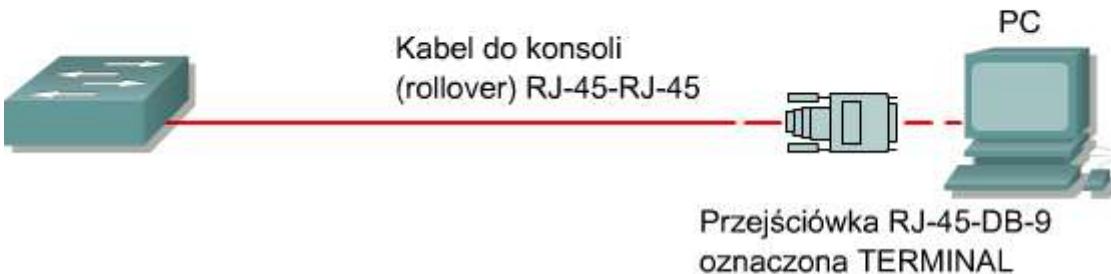
**1 z 8            2 z 7            3 z 6            4 z 5            5 z 4            6 z 3            7 z 2            8 z 1**

Aby połączyć terminal z portem konsoli Cisco, należy wykonać dwie czynności. Najpierw kablem do konsoli połącz port konsoli w routerze z portem szeregowym stacji roboczej. Do podłączenia kabla do komputera lub terminala może być potrzebna przejściówka RJ-45-DB-9 lub RJ-45-DB-25. Następnie skonfiguruj aplikację emulacji terminala, określając następujące ustawienia dla portu COM: 9600 b/s, 8 bitów danych, brak kontroli parzystości, 1 bit stopu i brak kontroli przepływu.

Port AUX umożliwia zarządzanie poza pasmem przy użyciu modemu. Aby można było korzystać z portu AUX, trzeba go skonfigurować tak, jak port konsoli. Dla portu AUX również wprowadź ustawienia: 9600 b/s, 8 bitów danych, brak kontroli parzystości, 1 bit stopu i brak kontroli przepływu.

### Połączenie z konsolą

Urządzenie z konsolą



- W celu podłączenia komputera PC potrzebna jest przejściówka ze złącza RJ-45 na DB-9 lub z RJ-45 na DB-25.
- Ustawienia portu COM są następujące: 9600 b/s, 8 bitów danych, brak kontroli parzystości, 1 bit stopu, brak kontroli przepływu.
- Taki sposób podłączenia umożliwia dostęp do konsoli poza pasmem.
- Do portu AUX przełącznika można dołączyć konsolę podłączoną poprzez modem.

### Okablowanie sieci LAN i WAN

- Wtórniiki, koncentratory, mosty i przełączniki to urządzenia powszechnie stosowane w sieciach LAN.
- Istnieją dwa główne typy sieci LAN: sieć węzłów równorzędnych i klient-serwer.
- W sieciach WAN wykorzystywana jest szeregowa transmisja danych. Do typów połączeń stosowanych w sieciach WAN należą łącza ISDN, DSL i modemy kablowe.

## **Moduł 6. Podstawy działania sieci Ethernet**

Ethernet jest obecnie najpopularniejszą technologią LAN. Ethernet nie stanowi jednej technologii, lecz stanowi zbiór technologii LAN, i może być najlepiej objaśniony z wykorzystaniem modelu odniesienia OSI. Wszystkie sieci LAN muszą rozwiązać podstawowy problem dotyczący nazewnictwa pojedynczych stacji (węzłów), sieć Ethernet nie jest tu wyjątkiem. Specyfikacje sieci Ethernet obejmują różne media, szerokości pasma oraz inne elementy warstw 1 i 2. Niemniej jednak, podstawowy format ramki oraz schemat adresowania są takie same dla wszystkich odmian standardu Ethernet.

W celu zapewnienia równoczesnego dostępu wielu stacji do fizycznego medium i innych urządzeń sieciowych opracowano różne strategie dostępu do medium. Zapoznanie się ze sposobem, w jaki urządzenia sieciowe uzyskują dostęp do medium sieciowego, jest niezbędne do zrozumienia mechanizmów działania całej sieci i rozwiązywania problemów z nią związanych.

### **6.1 Podstawy działania sieci Ethernet**

#### **6.1.1 Wprowadzenie do technologii Ethernet**

Większość ruchu w Internecie jest zarówno generowana, jak i trafia do hostów pracujących w sieci Ethernet. Poczynając od lat siedemdziesiątych, technologia Ethernet rozwijała się, starając się sprostać rosnącym wymaganiom dotyczącym dużej szybkości działania sieci LAN. Po pojawieniu się nowego medium, którym był światłowód, technologia Ethernet została przystosowana do wykorzystania oferowanej przez niego większej szerokości pasma i niskiego współczynnika błędów. Ten sam protokół, który w roku 1973 transmitował dane z szybkością 3 Mb/s, obecnie przesyła informacje z szybkością 10 Gb/s. Sukces technologii Ethernet jest związany z następującymi czynnikami: - prostota i łatwość obsługi, - możliwość dostosowywania się do nowych technologii, - niezawodność, - niski koszt instalacji i rozbudowy.

Wraz z wprowadzeniem gigabitowego Ethernetu standard, który początkowo był technologią przeznaczoną dla sieci LAN, teraz rozciąga się na odległości czyniące Ethernet standardem dla sieci miejskich (MAN) oraz sieci rozległych (WAN).

Pierwotny zamysł technologii Ethernet wyrósł z potrzeby rozwiązania następującego problemu: jak pozwolić dwóm lub więcej hostom na wykorzystywanie tego samego medium i zapobiec zderzeniom sygnałów? Problem dostępu wielu użytkowników do wspólnego medium był na początku lat siedemdziesiątych przedmiotem studiów na Uniwersytecie Hawajskim. System nazwany Alohanet został zaprojektowany po to, aby pozwolić różnym stacjom na Wyspach Hawajskich na ustrukturalizowany dostęp do dzielonego pasma częstotliwości radiowych w eterze. Badania te stały się później podstawą metody dostępu w technologii Ethernet znanej jako CSMA/CD.

Pierwsza na świecie sieć LAN była oparta na pierwotnej wersji technologii Ethernet. Zaprojektował ją ponad trzydzieści lat temu Robert Metcalfe wraz ze swoimi współpracownikami z firmy Xerox. Pierwszy standard Ethernet został opublikowany w 1980 r. przez konsorcjum, w skład którego wchodziły firmy Digital Equipment Company, Intel oraz Xerox (DIX). Pragnieniem Roberta Metcalfe'a było, aby technologia Ethernet stała się rozwiązaniem, z którego każdy mógłby korzystać, tak więc został on zaprezentowany jako ogólnodostępny standard otwarty. Pierwsze produkty zaprojektowane na podstawie standardu Ethernet zaczęły być sprzedawane we wczesnych latach osiemdziesiątych. Transmisja w technologii Ethernet osiągała szybkość do 10 Mb/s i była realizowana przez gruby kabel koncentryczny na odległościach do 2 kilometrów (km). Ten typ kabla koncentrycznego był określany jako Thicknet (ang. *thick* — gruby) i miał mniej więcej grubość małego palca. W roku 1985 standardy dotyczące sieci LAN zostały opublikowane przez komitet ds. standardów dla sieci lokalnych i miejskich instytutu Institute of Electrical and Electronics Engineers (IEEE). Numery tych standardów rozpoczynają się od liczby 802. Technologii Ethernet przyznano numer 802.3. Specjalisci z instytutu IEEE chcieli zachowania zgodności z modelem ISO (ang. *International Standards Organization*)/OSI. Aby to osiągnąć, standard IEEE 802.3 musiał sprostać wymogom określonym w definicji warstwy 1 oraz dolnej części warstwy 2 modelu OSI. W rezultacie w standardzie 802.3 wprowadzono niewielkie modyfikacje w stosunku do początkowej wersji standardu Ethernet.

Różnica pomiędzy tymi dwoma standardami jest tak niewielka, że każda karta sieciowa Ethernet może nadawać i odbierać zarówno ramki Ethernet, jak i 802.3. Zasadniczo Ethernet oraz IEEE 802.3 są tymi samymi standardami. Szerokość pasma w sieci Ethernet rzędu 10 Mb/s znacznie przewyższała wymagania powolnych komputerów osobistych (PC) lat osiemdziesiątych. Do początku lat dziewięćdziesiątych komputery klasy PC stały się znacznie szybsze, wzrosły rozmiary plików i zaczął się pojawiać problem wąskiego gardła w przepływie danych. W większości wypadków problem ten był spowodowany niską dostępnością pasma. W roku 1995 instytut IEEE zaprezentował standard dla technologii Ethernet 100 Mb/s. Następnie, w latach 1998 i 1999 zostały opublikowane standardy dla technologii Ethernet o przepustowości jednego gigabita na sekundę (1 Gb/s, miliard bitów na sekundę). Wszystkie te standardy są zasadniczo zgodne z pierwotnym standardem Ethernet. Ramka Ethernet może zostać przez komputer PC wyposażony w starszą, opartą na kablu koncentrycznym 10 Mb/s kartą sieciową, zostać

przesłana przez łącze światłowodowe Ethernet o przepustowości 10 Gb/s, a na końcu trafić do karty sieciowej 100 Mb/s. Dopóki pakiet pozostaje w sieci Ethernet, nie ulega on modyfikacjom. Z tego powodu technologia Ethernet jest uważana za wysoce skalowalną. Szerokość pasma w sieci może być wielokrotnie zwiększała bez zmiany stosowanej technologii Ethernet. Pierwotny standard technologii Ethernet był wielokrotnie poprawiany w celu dostosowania go do potrzeb nowych mediów transmisyjnych i wyższych prędkości transmisji. Poprawki te stanowią źródło standardów dla nowych technologii i utrzymują zgodność pomiędzy wariantami sieci Ethernet.

### **6.1.2 Zasady nazewnictwa w standardzie IEEE Ethernet**

Technologia Ethernet nie stanowi jednej technologii, lecz całą rodzinę technologii sieciowych obejmującą tradycyjny Ethernet, Fast Ethernet oraz Gigabit Ethernet. Szybkości technologii Ethernet mogą wynosić 10, 100, 1000 lub 10 000 Mb/s. Podstawowy format ramki oraz mechanizm działania podwarstw IEEE w ramach warstw 1 i 2 modelu OSI pozostają spójne we wszystkich formach technologii Ethernet.

Kiedy zachodzi potrzeba rozszerzenia technologii Ethernet przez dodanie nowego medium lub nowej funkcjonalności, instytut IEEE wydaje nowe uzupełnienie standardu 802.3. Takie nowe uzupełnienia otrzymują jedno- lub dwuliterowe oznaczenie, np. 802.3u. Do uzupełnienia jest także przypisany skrócony opis (zwany identyfikatorem). Skrócony opis składa się z:

- \* liczby określającej szybkość transmisji w Mb/s;
- \* słowa „base”, wskazującego, że jest używana sygnalizacja pasma podstawowego;
- \* jednej lub więcej liter alfabetu, określających rodzaj wykorzystywanego medium (F = kabel światłowodowy, T = miedziana skrętka nieekranowana).

Ethernet jest oparty na sygnalizacji pasma podstawowego, która wykorzystuje całą szerokość pasma medium transmisyjnego. Sygnał danych jest przesyłany bezpośrednio przez medium transmisyjne.

W sygnalizacji szerokopasmowej, sygnał danych nigdy nie jest bezpośrednio umieszczany w medium transmisyjnym. Ethernet używały sygnalizacji szerokopasmowej w standardzie 10BROAD36. Był to standard IEEE dla sieci Ethernet 802.3, używającej sygnalizacji szerokopasmowej po grubym kablu koncentrycznym, działającym z prędkością 10 Mbps. Dziś standard ten uważa się za nieaktualny. Sygnał danych moduluje sygnał analogowy (sygnał nośnej) i tak zmodulowany sygnał nośnej podlega transmisji. Sygnalizacja szerokopasmowa jest wykorzystywana w emisji radiowej i w telewizji kablowej.

Instytut IEEE nie może zmusić producentów sprzętu sieciowego do bezwzględnego stosowania się do wszystkich szczegółowych rozwiązań w ramach każdego ze standardów. IEEE ma nadzieję osiągnąć następujące cele:

- \* dostarczanie fachowych informacji niezbędnych do budowy urządzeń zgodnych ze standardami Ethernet,
- \* promowanie innowacji wprowadzanych przez producentów.

### **6.3.1 Technologia Ethernet i model OSI**

**Technologia Ethernet funkcjonuje w dwóch obszarach modelu OSI: w dolnej połowie warstwy łączą danych, znanej jako podwarstwa MAC, oraz w warstwie fizycznej.**

Przy przesyłaniu danych pomiędzy dwiema stacjami sieci Ethernet informacje często przechodzą przez wórtnik. Ruch przechodzący przez wórtnik jest widoczny dla wszystkich innych stacji z tej samej domeny kolizyjnej. Domena kolizyjna jest więc zasobem wspólnym. Problemy powstające w jednej części domeny kolizyjnej zwykle mają wpływ na całą domenę kolizyjną.

Wórtnik jest odpowiedzialny za przesyłanie całego ruchu do wszystkich pozostałych portów. Ruch odbierany przez wórtnik nigdy nie jest wysyłany na port, z którego pochodzi. Każdy wykryty przez wórtnik sygnał zostanie przesłany. Jeśli sygnał jest osłabiony przez tłumienie lub szum, wórtnik spróbuje go odtworzyć i zregenerować. Standardy gwarantują minimalną szerokość pasma i możliwość działania poprzez określenie maksymalnej liczby stacji w segmencie, maksymalnej długości segmentu, maksymalnej liczby wórtników pomiędzy stacjami itd.

Stacje oddzielone wórtnikami pozostają w tej samej domenie kolizyjnej. Stacje oddzielone mostami lub routerami znajdują się w różnych domenach kolizyjnych. **Rysunek** pokazuje odwzorowanie różnych technologii Ethernet na niższą połowę warstwy 2 modelu OSI i całą warstwę 1. Ethernet w warstwie 1 dotyczy połączenia z medium oraz sygnałów, strumieni bitów transmitowanych przez media, elementów, które umieszczały sygnały w mediach i różnych topologii sieciowych. Warstwa 1 technologii Ethernet odgrywa zasadniczą rolę w komunikacji, która zachodzi pomiędzy urządzeniami, lecz każda z jej funkcji ma ograniczenia, którymi zajmuje się warstwa 2.

Podwarstwy warstwy łączą danych realizują zadania dotyczące zgodności technologicznej i komunikacji między komputerami. Zadaniem podwarstwy MAC jest współpraca z elementami fizycznymi, które będą służyć do przekazywania informacji. Podwarstwa LLC (ang. *Logical Link Control*) pozostaje stosunkowo niezależna od

### **Nazwy technologii Ethernet składają się z trzech części**

Szybkość	Metoda sygnalizacji	Medium
10	BASE	2
100	BROAD	5
1000		-T
10G		-TX
		-SX
		-LX

# Standardy IEEE 802.x

Sterowanie logiczne 802.2

Mostowanie 802.1							
Przegląd i architektura standardu 802 (802.1a)	802.3	Magistrala z przekazywaniem tokenu 802.4	Metoda dostępu DQDB 802.6	Uslugi zintegrowane 802.9	Bezprzewodowa sieć LAN 802.11	Priorytet zadania (VG) 802.12	Telewizja kablowa 802.14
Ethernet		Token Ring					Bezprzewodowa sieć PAN 802.15

fizycznego sprzętu, który zostanie użyty w procesie komunikacji.

**Rysunek** pokazuje odwzorowanie różnych technologii Ethernet na niższą połowę warstwy 2 oraz całą warstwę 1 modelu OSI. Istnieje także wiele innych rodzajów sieci Ethernet, na rysunku przedstawiono te najpopularniejsze.

## Warstwa 1 w porównaniu z warstwą 2

- Warstwa 1 nie może komunikować się z warstwami wyższego poziomu.
- Warstwa 2 dokonuje tego za pomocą mechanizmu LLC (Logical Link Control).
- Warstwa 1 nie może identyfikować komputerów.
- Warstwa 2 korzysta z procesu adresowania.
- Warstwa 1 jest w stanie jedynie opisywać strumienie bitów.
- Warstwa 2 organizuje grupy bitów w ramki.
- Na poziomie warstwy 1 nie można określić, który komputer z grupy, w której wszystkie komputery próbują wysyłać dane w tym samym momencie, przesyła dane dwójkowe.
- Warstwa 2 korzysta z systemu o nazwie kontrola dostępu do medium (MAC).

## Technologie Ethernet odwzorowane w modelu OSI

Podwarstwa LLC (Logical Link Control)

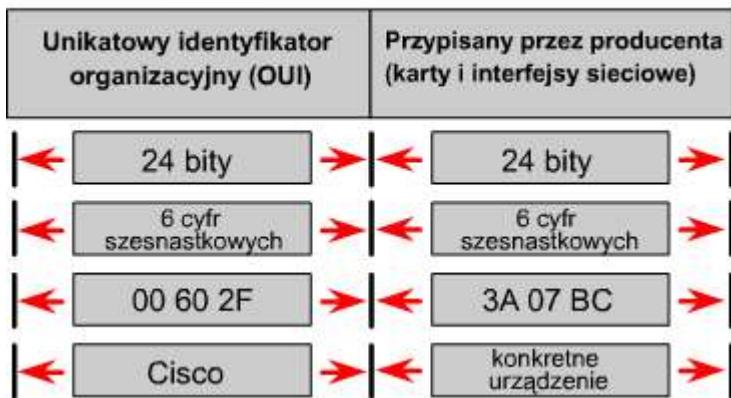
### Kontrola dostępu do medium 802.3

Podwarstwa sygnalizacji	10BASE5 (500m) 50 Ohm Coax N-Style	10BASE2 (185m) 50 Ohm Coax BNC	10BASE-T (100m) 100 Ohm UTP RJ-45	100BASE-TX (100m) 100 Ohm UTP RJ-45	1000BASE-CX (25m) 150 Ohm STP mini-DB-9	1000BASE-T (100m) 100 Ohm UTP RJ-45	1000BASE-SX (220-550m) MM Fiber SC	1000BASE-LX (550-5000m) m) MM or SM Fiber SC
Medium fizyczne								

### 6.1.4 Nazewnictwo

Aby umożliwić lokalne dostarczanie ramek w technologii Ethernet, musi istnieć system adresowania, tj. sposób unikalnej identyfikacji komputerów i interfejsów. Technologia Ethernet wykorzystuje adresy fizyczne MAC, które mają długość 48 bitów i w systemie szesnastkowym są zapisywane w postaci dwunastu cyfr. Wartość pierwszych sześciu cyfr jest zarządzana przez instytut IEEE i identyfikuje producenta lub dostawcę. Ta część adresu MAC jest znana jako unikalny identyfikator OUI (ang. *Organizational Unique Identifier*). Pozostałe sześć cyfr w zapisie szesnastkowym reprezentuje numer seryjny interfejsu lub inną wartość określana przez producenta danego sprzętu. Adresy MAC są czasami oznaczane jako adresy wbudowane (BIA), ponieważ są one wbudowane w

## Format adresu MAC



pamięć ROM i kopiowane do pamięci RAM w momencie inicjowania karty sieciowej. W warstwie łączą danych nagłówki i stopki MAC są dodawane do danych wyższej warstwy. Nagłówek i stopka zawierają informację kontrolną przeznaczoną dla warstwy łącza danych w systemie odbiorcy. Dane z wyższych warstw są enkapsulowane w ramkę warstwy łączą danych, pomiędzy nagłówkiem a stopką, a następnie wysłane do sieci. Karta sieciowa wykorzystuje adresy MAC do oceny, czy komunikat powinien być przekazany do wyższych warstw modelu OSI. Karta sieciowa przeprowadza tę ocenę, nie zajmując czasu procesora, co umożliwia szybszą komunikację w sieci Ethernet.

Urządzenie w sieci Ethernet, rozpoczynając transmisję danych, może kierować dane do drugiego urządzenia za pomocą jego adresu MAC jako adresu docelowego. Urządzenie źródłowe dołącza nagłówek z adresem MAC żądanego adresata i wysyła dane do sieci. Podczas przesyłania danych w mediach sieciowych karta sieciowa każdego urządzenia w sieci sprawdza, czy jej adres MAC odpowiada adresowi fizycznemu odbiorcy zawartemu w ramce danych. Jeśli adresy nie są zgodne, ramka zostaje odrzucona przez kartę sieciową. Gdy dane osiągną węzeł docelowy, karta sieciowa wykona ich kopię i prześle ramkę do wyższych warstw modelu OSI. **W sieci Ethernet nagłówek MAC musi być analizowany przez wszystkie węzły, nawet jeśli komunikujące się węzły sąsiadują ze sobą.** Wszystkie urządzenia, które są podłączone do sieci LAN bazującej na technologii Ethernet, m.in. stacje robocze, drukarki, routery i przełączniki, mają interfejsy rozpoznawane za pomocą adresu MAC.

### 6.1.5 Proces podziału na ramki w warstwie 2

Zakodowane strumienie bitów (danych) w mediach fizycznych stanowią olbrzymie osiągnięcie technologiczne, lecz one same nie są w stanie sprawić, by została nawiązana komunikacja. Podział na ramki pomaga uzyskać niezbędne informacje, które nie mogłyby być pobrane z samych tylko zakodowanych strumieni bitów. Oto przykłady takich informacji:

- \* Które komputery komunikują się ze sobą.
- \* Kiedy zaczyna się i kończy komunikacja pomiędzy poszczególnymi komputerami.
- \* Informacje pomocne w wykrywaniu błędów, które wystąpiły podczas komunikacji.
- \* Czyja kolej na „mówienie” podczas „rozmowy” komputerów.

Podział na ramki jest procesem enkapsulacji warstwy 2. Ramka jest jednostką danych protokołu warstwy 2. Do wizualizacji bitów może służyć wykres napięcia w funkcji czasu. Jednakże, kiedy mamy do czynienia z większymi jednostkami danych, adresowaniem i informacjami kontrolnymi, wykres napięcia w funkcji czasu może stać się zawiły i mylący. Innym typem diagramu, który może być wykorzystany, jest *diagram formatu ramki* oparty na wykresie napięcia w funkcji czasu. Diagramy formatu ramki są czytane od strony lewej do prawej, tak jak wykres na oscyloskopie. Diagramy formatu ramki pokazują różne grupy bitów (pola) pełniące inne funkcje. Jest wiele różnych typów ramek opisywanych przez różne standardy. Pojedyncza, ogólna rama zawiera sekcje, zwane polami, a każde pole składa się z bajtów. Nazwy tych pól są następujące:

\* pole początku ramki, \* pole adresu, \* pole typu/długości, \* pole danych, \* pole kodu kontrolnego ramki. Gdy komputery są podłączone do medium fizycznego, musi istnieć sposób, w jaki mogą zwrócić na siebie uwagę innych komputerów, by nadać wiadomość: „Nadchodzi ramka”. W różnych technologiach istnieją różne sposoby realizacji tego procesu, lecz wszystkie ramki, niezależnie od technologii, zawierają na początku sygnalizacyjną sekwencję bajtów. **Wszystkie ramki zawierają informacje dotyczące nazw, takie jak nazwa węzła źródłowego (adres MAC) i nazwa węzła docelowego (adres MAC).**

W większości ramek występują pewne wyspecjalizowane pola. W niektórych technologiach pole długości określa dokładną długość ramki w bajtach. W niektórych ramkach występuje pole typu, które określa protokół warstwy 3 odpowiedzialny za wysłanie żądania. Urządzenie w sieci Ethernet, rozpoczynając transmisję danych, może kierować dane do drugiego urządzenia przy użyciu jego adresu MAC jako adresu docelowego. Paczka danych zawiera w sobie wiadomość, którą trzeba przesłać lub dane aplikacji użytkownika. Może zajść potrzeba dodania bajtów wypełniających, aby rama osiągnęła minimalną wymaganą długość. W skład pola danych ramek zgodnych ze standardami IEEE wchodzą również bajty LLC (ang. *logical link control*). Podwarstwa LLC pobiera dane protokołu sieciowego, pakiet IP, a następnie dodaje informacje kontrolne pomocne w dostarczeniu danego pakietu IP do węzła docelowego.

Warstwa 2 komunikuje się z wyższymi warstwami poprzez podwarstwę LLC. Wszystkie ramki oraz zawarte w nich bity, bajty i pola są podatne na błędy pochodzące z różnych źródeł. Pole kodu kontrolnego ramki (FCS) zawiera liczbę, która jest obliczana przez węzeł źródłowy na podstawie danych w ramce. Pole FCS jest następnie dodawane na końcu wysyłanej ramki. Kiedy ramka jest odbierana przez węzeł docelowy, liczba FCS jest ponownie przeliczana i porównywana z liczbą FCS zawartą w ramce. Jeśli są one różne, zakłada się, że wystąpił

błąd i ramka jest odrzucana. Ponieważ źródło nie może wykryć czy ramka została faktycznie odrzucona, protokoły zorientowane połączeniowo wyższych warstw muszą zainicjować ewentualną retransmisję. Ponieważ te protokoły, jak np. TCP, żądają potwierdzenia otrzymania danych (ACK) przez stronę odbiorczą, w odpowiednim czasie, zwykle dochodzi do takiej właśnie retransmisji.

### Są trzy podstawowe sposoby obliczania kodu kontrolnego ramki FCS:

**Cykliczna kontrola nadmiarowa (CRC):** wykonuje obliczenia na danych.

**Parzystość dwuwymiarowa:** każdy kolejny bajt jest wstawiany do dwuwymiarowej tablicy, następnie wykonywana jest kontrola nadmiarowości w każdej kolumnie i wierszu, tworząc tym samym dziewiąty bajt wskazujący nieparzystą lub parzystą liczbę jedynek binarnych.

**Internetowa suma kontrolna:** dodawane są wartości wszystkich bitów danych, wynik jest sumą kontrolną. Węzeł transmitujący dane musi pozyskać uwagę innych urządzeń, aby zacząć i zakończyć przesyłanie ramki. Pole długości wyznacza koniec, a ramka jest uważana za zakończoną po wystąpieniu kodu FCS. Czasami występuje formalna sekwencja bajtów nazywana znacznikiem końca ramki.

### Format ramki ogólnej

Nazwy pól				
A	B	C	D	E
Pole początku ramki	Pole adresu	Pole typu/długości	Pole danych	Pole FCS

#### 6.1.6 Struktura ramki w technologii Ethernet

#### Ethernet IEEE 802.3

Obliczenie kodu FCS							
Preambuła 7	Znacznik SFD 1	Cel 6	Źródło 6	Długość / Typ 2	Dane	Wypełnienie od 46 do 1500	Kod FCS 4

#### Pola ramek Ethernet IEEE 802.3

Oktety	Opis
• 7	Preambuła
• 1	Znacznik początku ramki (SFD)
• 6	Adres MAC odbiorcy
• 6	Adres MAC nadawcy
• 2	Pole długości/typu (długość, jeśli wartość jest mniejsza od 0600 szesnastkowo; w przeciwnym razie typ protokołu)
• od 46 do 1500 dane*	(jeśli mniej niż 46 oktetów, to na końcu konieczne jest dodanie wypełnienia)
• 4	Kod kontrolny ramki FCS (suma kontrolna CRC)

Na poziomie warstwy łączna danych struktura ramki jest prawie identyczna dla wszystkich szybkości technologii Ethernet, od 10 Mb/s do 10 000 Mb/s. Na poziomie warstwy fizycznej prawie wszystkie wersje technologii Ethernet różnią się znacznie, gdyż dla każdej szybkości transmisji przyjęte zostały inne założenia architektoniczne. W wersji technologii Ethernet, rozwijanej przez firmę DIX przed przyjęciem wersji Ethernet IEEE 802.3, preambuła i znacznik początku ramki (SFD) były połączone w jedno pole, mimo iż sekwencja bitów była identyczna. Pole

długość/typ oznaczało jedynie długość ramki we wczesnych wersjach IEEE, zaś w wersji DIX wyłącznie typ ramki. Te dwa sposoby wykorzystania pola zostały oficjalnie połączone w późniejszej wersji standardu IEEE, ponieważ oba były powszechnie używane. Pole typu w technologii Ethernet II zostało włączone do obecnej definicji ramki 802.3. Węzeł odbierający musi ustalić protokół warstwy wyższej, którego dane są obecne w przychodzącej ramce, poprzez analizę pola typ/długość. Jeżeli wartość dwóch oktetów jest równa lub większa niż 0x0600 szesnastkowo, czyli 1536 dziesiętnie, to zawartość pola danych jest dekodowana stosownie do wskazanego typu protokołu. Ethernet II jest formatem ramki używanym zwykle w sieciach TCP/IP.

### Ethernet II

- Standard wprowadzony przez DIX.
- Używany w sieciach TCP/IP
- W celu określenia protokołu wyższej warstwy stosowane jest pole typu.
- Przykłady typów:
  - 0x0806 = ARP
  - 0x0800 = IPv4

## 6.1.7 Pola ramek w technologii Ethernet

Oto niektóre z dozwolonych lub wymaganych pól ramki Ethernet 802.3:  
preambuła, znacznik początku ramki, adres odbiorcy, adres nadawcy, długość/typ, dane i wypełnienie, FCS, rozszerzenie.

Preambuła jest naprzemiennym wzorcem jedynek i zer używanym do synchronizacji taktowania w asynchronicznych implementacjach technologii Ethernet o szybkości 10 Mb/s i wolniejszych. Szybsze wersje technologii Ethernet są synchroniczne i takie informacje taktujące są nadmiarowe, zostały jednak zachowane dla utrzymania zgodności.

Znacznik początku ramki (SFD) składa się z pola o długości jednego oktetu oznaczającego koniec informacji taktujących i zawierającego sekwencję bitów 10101011.

Pole adresu odbiorcy zawiera adres MAC odbiorcy. Adres odbiorcy może być adresem pojedynczego hosta, adresem grupowym lub rozgłoszeniowym.

Pole adresu nadawcy zawiera adres MAC nadawcy. Adres nadawcy jest, ogólnie biorąc, adresem pojedynczego hosta nadającego węzła sieci Ethernet. Rośnie jednak liczba stosowanych protokołów wirtualnych, które wykorzystują i czasem współdzielą dany adres MAC nadawcy w celu zidentyfikowania wirtualnej jednostki.

Pole długości/typu ma dwa różne przeznaczenia. Jeśli jego wartość jest mniejsza niż 1536 dziesiętnie (0x600 szesnastkowo), to wartość ta określa długość. Interpretacja tego pola jako „długość” jest stosowana wówczas, gdy warstwa LLC zapewnia identyfikację protokołu. Wartość typu określa protokół wyższej warstwy, który ma być użyty do odebrania danych po zakończeniu przetwarzania w sieci Ethernet. Długość wskazuje liczbę bajtów danych, które następują po tym polu.

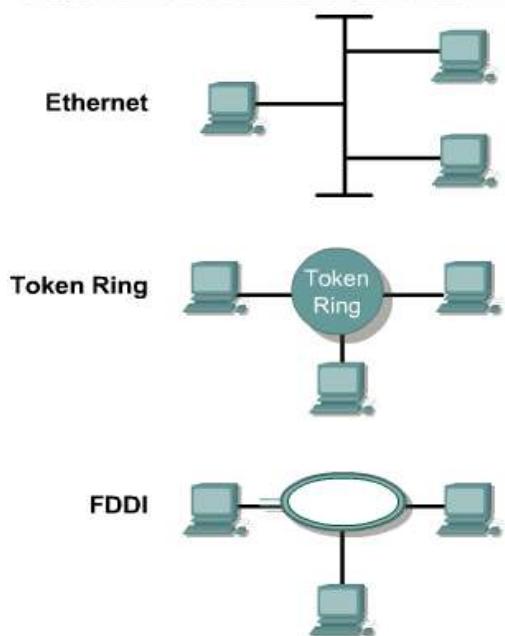
Pole danych i ewentualne wypełnienie mogą mieć każdą długość, która nie spowoduje, że zostanie przekroczony maksymalny rozmiar ramki.

Maksymalna jednostka transmisyjna (MTU) dla sieci Ethernet wynosi 1500 oktetów, tak więc dane nie powinny przekroczyć tego rozmiaru. Zawartość tego pola nie jest określona. Gdy dane użytkownika nie są wystarczająco długie, aby ramka osiągnęła minimalną długość, bezpośrednio po nich zostaje umieszczone wypełnienie o nieokreślonej treści. Zgodnie z wymaganiami standardu Ethernet ramka nie powinna być krótsza niż 64 oktety i dłuższa niż 1518 oktetów.

Pole FCS zawiera czterobajtową wartość CRC tworzoną przez urządzenie wysyłające i ponownie przeliczaną przez urządzenie odbierające w celu sprawdzenia, czy ramka nie została uszkodzona. Nie ma potrzeby obejmowania wartością sumy kontrolnej jej samej, gdyż jeśli zdarzy się przekłamanie sumy, nie będzie ona odpowiadać zawartości ramki. Nie jest możliwe rozróżnienie pomiędzy uszkodzeniem pola FCS i uszkodzeniem dowolnego poprzedniego pola użytego do obliczeń.

## 6.2 Funkcjonowanie sieci Ethernet

### Popularne technologie sieci LAN



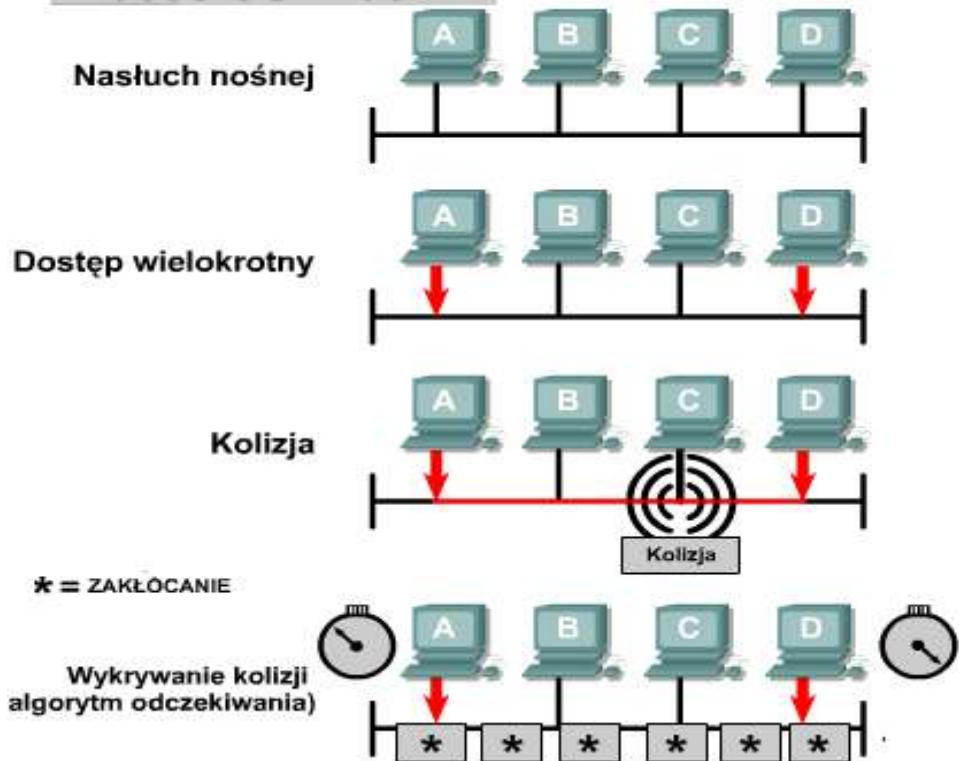
### 6.2.1 Kontrola dostępu do medium (MAC)

Kontrola dostępu do medium (MAC) odnosi się do protokołów określających, który komputer lub która domena kolizyjna może wysyłać dane. Podwarstwy MAC i LLC wspólnie stanowią wersję IEEE warstwy 2 modelu OSI. MAC i LLC są podwarstwami warstwy 2. Mechanizmy dostępu do medium (MAC) mogą być podzielone na dwie ogólne kategorie: deterministyczną (zgodnie z kolejnością) i niedeterministyczną (pierwszy przychodzi, pierwszy obsłużony).

Przykładami protokołów deterministycznych są protokoły Token Ring i FDDI. W sieci opartej na protokole Token Ring pojedyncze hosty są zorganizowane w pierścień, a specjalny token danych jest przekazywany dookoła tego pierścienia do każdego hosta po kolei. Gdy host chce nadawać, przechwytuje token, wysyła dane przez ograniczony czas, a następnie przekazuje token do następnego hosta w pierścieniu. Protokół Token Ring jest środowiskiem bezkolizyjnym, ponieważ w określonym czasie może nadawać tylko jeden host. Niedeterministyczne protokoły MAC opierają się na podejściu typu „pierwszy przychodzi, pierwszy obsłużony” (ang. *first come, first served*). Takim prostym systemem jest CSMA/CD (Carrier Sense Multiple Access / Collision Detection - Wielodostęp do medium z wykrywaniem nośnej). Karta sieciowa nasłuchuje, czekając na brak sygnału w medium, i zaczyna nadawanie. Jeśli dwa węzły nadają jednocześnie, występuje kolizja i żaden z węzłów nie może transmitować danych.

*first come, first served*). Takim prostym systemem jest CSMA/CD (Carrier Sense Multiple Access / Collision Detection - Wielodostęp do medium z wykrywaniem nośnej). Karta sieciowa nasłuchuje, czekając na brak sygnału w medium, i zaczyna nadawanie. Jeśli dwa węzły nadają jednocześnie, występuje kolizja i żaden z węzłów nie może transmitować danych.

## Proces CSMA/CD



kontrolowany w pierścieniu) oraz topologia podwójnego pierścienia fizycznego (okablowanie w formie podwójnego pierścienia).

### 6.2.2 Reguły MAC i wykrywanie kolizji/oczekiwanie

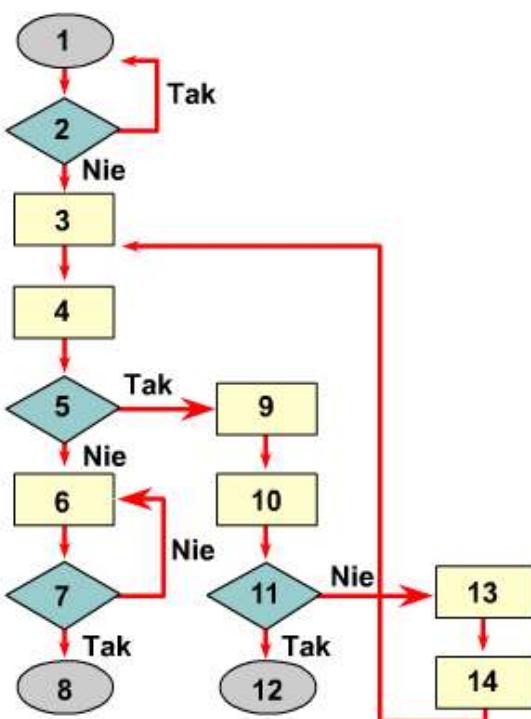
Ethernet jest technologią polegającą na rozgłaszananiu informacji w dzielonym (wspólnym) medium.

Wykorzystywana w technologii Ethernet metoda dostępu CSMA/CD spełnia trzy funkcje:

- \* wysyłanie i odbieranie ramek z danymi,
- \* dekodowanie ramek i sprawdzanie poprawności zawartych w nich adresów przed przekazaniem ich do wyższych warstw modelu OSI,
- \* wykrywanie błędów wewnętrz ramek lub w sieci.

## Proces CSMA/CD

1. Host zamierza nadawać
2. Czy wykryto nośną?
3. Złożenie ramki
4. Początek transmisji
5. Czy wykryto kolizję?
6. Kontynuacja transmisji
7. Czy transmisja dobiegła końca?
8. Transmisja zakończona
9. Rozgłoszanie sygnału zakłócającego
10. Próby = Próby + 1
11. Próby > Zbyt wiele?
12. Zbyt wiele kolizji, przerwanie transmisji
13. Algorytm oblicza czas oczekiwania
14. Oczekiwanie przez t mikrosekund



Token Ring, FDDI oraz Ethernet stanowią trzy popularne technologie warstwy 2. Wszystkie trzy podejmują kwestie adresowania w warstwie 2, podziału na ramki, podwarstw LLC i MAC jak również kwestie sygnalizacji i mediów transmisyjnych. Oto konkretne technologie dla każdej z nich:

**Ethernet:** topologia magistrali logicznej (przepływ informacji jest realizowany w liniowej magistrali) oraz fizyczna gwiazda lub rozszerzona gwiazda (okablowanie w formie gwiazdy).

**Token Ring:** topologia pierścienia logicznego (innymi słowy, przepływ informacji jest kontrolowany w pierścieniu) oraz topologia fizycznej gwiazdy (innymi słowy, okablowanie przyjmuje formę gwiazdy).

**FDDI:** topologia pierścienia logicznego (przepływ informacji jest

W metodzie dostępu CSMA/CD urządzenia sieciowe z danymi do transmisji pracują w trybie nasłuchu przed nadawaniem. Oznacza to, że jeśli węzeł ma wysłać dane, musi najpierw sprawdzić, czy medium sieciowe nie jest zajęte. Jeśli węzeł wykryje, że sieć jest zajęta, będzie oczekiwany przez losowo wybrany czas przed ponowieniem próby. Jeśli węzeł wykryje, że medium nie jest zajęte, rozpoczęcie nadawania i nasłuchiwanie. Celem nasłuchiwanie przez węzeł jest upewnienie się, że żadna inna stacja nie nadaje w tym samym czasie. Po zakończeniu transmisji danych

urządzenie powróci do trybu nasłuchiwanie.

Wystąpienie kolizji jest wykrywane przez urządzenia sieciowe na podstawie wzrostu amplitudy sygnału w medium sieciowym. Jeśli wystąpi kolizja, transmisja będzie kontynuowana przez krótki czas przez każdy z nadających węzłów, aby upewnić się, że wszystkie pozostałe węzły wykryły kolizję. Gdy kolizja zostanie wykryta przez wszystkie węzły, rozpoczyna się wykonywanie algorytmu oczekiwania i transmisja zostaje zatrzymana.

Węzły zatrzymują nadawanie na losowo wybrany czas, określony przez algorytm oczekiwania. Po wygaśnięciu okresu opóźnienia każdy węzeł w sieci może podjąć próbę uzyskania dostępu do medium sieciowego. Urządzeniom zaangażowanym w kolizję nie przysługuje pierwszeństwo wysyłania danych.

### 6.2.3 Taktowanie w sieci Ethernet

Podstawowe zasady i specyfikacje prawidłowego funkcjonowania sieci Ethernet nie są szczególnie złożone, choć niektóre z szybszych implementacji warstwy fizycznej takimi się stają. Mimo podstawowej prostoty działania sieci Ethernet, jeśli pojawi się w niej problem, wyizolowanie jego źródła często nastręcza trudności. Z powodu powszechnie stosowanej w technologii Ethernet architektury magistrali, opisywanej również jako rozproszony pojedynczy punkt awarii, problem zasięgiem swym obejmuje zwykle wszystkie urządzenia wewnętrz domeny kolizyjnej. W sytuacjach, gdy wykorzystywane są wtórni, zasięg ten może rozszerzać się na urządzenia umieszczone w odległości do czterech segmentów. Każda mająca nadać wiadomość stacja w sieci Ethernet najpierw „nasłuchuje”, aby upewnić się, że żadna inna stacja nie nadaje w tym momencie. Jeśli w kablu jest cisza, stacja taka natychmiast zaczyna nadawać. Przesyłanie sygnału elektrycznego po kablu zabiera pewien czas (zwany opóźnieniem), a każdy kolejny wtórnik wprowadza dodatkowe, niewielkie opóźnienie przy przekazywaniu ramki z jednego portu do kolejnego. W wyniku tych opóźnień może się zdarzyć, że więcej niż jedna stacja zacznie nadawanie niemal w tym samym czasie. Rezultatem tego jest kolizja.

Jeśli podłączona stacja pracuje w trybie pełnego dupleksu, to może ona równocześnie wysyłać i odbierać, a kolizje nie powinny się pojawiać. Praca w trybie pełnego dupleksu zmienia również uwarunkowania dotyczące taktowania i eliminuje pojęcie szczeliny czasowej. Praca w trybie pełnego dupleksu pozwala na budowę większych sieci, ponieważ usunięto ograniczenia czasowe nałożone w celu wykrycia kolizji.

W trybie półdupleksu, przy założeniu, że nie występuje kolizja, stacja nadawcza transmituje 64 bity informacji synchronizacyjnej znane jako preambuła. Stacja nadawcza wysyła wtedy następujące informacje:

- \* informacje o adresowaniu MAC nadawcy i odbiorcy;
- \* pewne inne informacje nagłówka;
- \* właściwą, zasadniczą treść danych;
- \* sumę kontrolną (FCS) używaną do upewnienia się, czy wiadomość nie została po drodze uszkodzona.

Stacje odbierające ramkę przeliczają sumę FCS, aby ustalić, czy przychodząca wiadomość jest poprawna, a następnie przekazują poprawną wiadomość do następnej, wyższej warstwy w stosie protokołów.

Wersje technologii Ethernet pracujące z szybkością 10 Mb/s i wolniejsze są asynchroniczne. Asynchroniczność oznacza, że każda stacja odbierająca wykorzystuje osiem oktetów informacji taktowania do zsynchronizowania obwodu odbiorczego dla nadchodzących danych, po czym odrzuca je. Implementacje technologii Ethernet pracujące z szybkością 100 Mb/s i szybsze są synchroniczne. Synchroniczność oznacza, że informacja taktowania nie jest wymagana, lecz dla utrzymania zgodności pole preambuły i znacznik początku ramki (SFD) są obecne.

We wszystkich odmianach technologii Ethernet o szybkości transmisji nieprzekraczającej 1000 Mb/s standard wyznacza minimalny czas pojedynczej transmisji nie krótszy niż szczelina czasowa. Szczelina czasowa dla technologii Ethernet 10 i 100 Mb/s jest równa czasowi transmisji 512 bitów (czyli 64 oktetów). Szczelina czasowa dla technologii Ethernet 1000 Mb/s jest równa czasowi transmisji 4096 bitów (czyli 512 oktetów). Szczelina czasowa jest obliczana przy założeniu maksymalnych długości kabli w największej dopuszczalnej architekturze sieciowej. Wszystkie czasy opóźnień propagacji sprzętowej są na poziomie dopuszczalnego maksimum, a gdy zostanie wykryta kolizja, używana jest 32-bitowa sekwencja zakłócająca.

Rzeczywista obliczona szczelina czasowa jest nieco dłuższa niż teoretyczna ilość czasu wymagana do przebycia drogi pomiędzy najdalszymi punktami domeny kolizyjnej, zderzenia się z inną transmisją w ostatnim możliwym momencie, powrotu fragmentów kolizyjnych do stacji wysyłającej i ich wykrycia. Aby system działał, pierwsza stacja musi dowiedzieć się o kolizji zanim zakończy wysyłanie ramki o najmniejszym dopuszczalnym rozmiarze. Aby umożliwić działanie sieci Ethernet 1000 Mb/s w trybie półdupleksu, przy wysyłaniu krótkich ramek dodano pole rozszerzenia służące jedynie do utrzymania urządzenia transmitującego w stanie zajętości na tyle długo, by mogły wrócić fragmenty kolizyjne. Pole to jest obecne tylko przy szybkości 1000 Mb/s w przypadku łączących pracujących w trybie półdupleksu, po to, aby ramki o minimalnym rozmiarze były wystarczająco długie, by móc sprostać wymaganiom szczeliny czasowej. Bity rozszerzenia są odrzucane przez stację odbierającą.

W technologii Ethernet 10 Mb/s transmisja jednego bitu w warstwie MAC trwa 100 nanosekund (ns). Przy szybkości 100 Mb/s transmisja tego samego bitu trwa 10 ns, a przy szybkości 1000 Mb/s trwa ona tylko 1 ns. W przybliżonych szacunkach często wykorzystywana jest wartość 20,3 cm (8 cali) na nanosekundę do obliczania opóźnienia propagacji w kablu UTP. Oznacza to, że w 100 metrach kabla UTP przesłanie sygnału 10BASE-T na całej długości przewodu trwa krócej niż czas transmisji pięciu bitów.

Dla funkcjonowania metody CSMA/CD stosowanej w sieciach Ethernet konieczne jest, aby stacja wysyłająca wiedziała o wystąpieniu kolizji zanim zostanie zakończona transmisja ramki o minimalnym rozmiarze. Przy szybkości 100 Mb/s taktowanie systemu jest ledwie w stanie obsłużyć sieci o długości kabla równej 100 metrów. Przy szybkości 1000 Mb/s wymagane są specjalne korekty, gdyż prawie cała ramka o minimalnym rozmiarze

zostałaby wysłana, zanim pierwszy bit pokonałby pierwsze 100 metrów kabla UTP. Z tego powodu tryb półdupleksu nie jest dozwolony w technologii 10 Gigabit Ethernet.

#### 6.2.4 Przerwy międzyramkowe i oczekiwanie

Minimalny odstęp pomiędzy dwiema niekolidującymi ramkami jest zwany przerwą międzyramkową. Jest on mierzony od ostatniego bitu pola FCS pierwszej ramki do pierwszego bitu preambuły ramki drugiej.

Po wysłaniu ramki wszystkie stacje w sieci Ethernet 10 Mb/s muszą oczekwać co najmniej przez czas transmisji 96 bitów (9,6 mikrosekundy), zanim następna ramka może zostać poprawnie wysłana przez którykolwiek stację. W szybszych wersjach sieci Ethernet odstęp pozostaje taki sam (czas transmisji 96 bitów), lecz czas, który musi upłynąć, jest odpowiednio krótszy. Czas ten po angielsku określa się mianem „interframe spacing” albo „interframe gap” — najczęstsze polskie określenie to „przerwa międzyramkowa”. Przerwa ta ma na celu zapewnienie wolniejszym stacjom czasu na przetworzenie poprzedniej ramki i przygotowanie się do odbioru następnej ramki.

Zadaniem węzła jest regeneracja pełnych 64 bitów informacji taktujących, tj. preambuły i pola SFD, na początku każdej ramki. Dzieje się tak mimo możliwości utraty części bitów początku preambuły z powodu powolnej synchronizacji. Ze względu na konieczność dokonania taktowania bitów ramki na nowo mała redukcja przerwy międzyramkowej jest nie tylko możliwa, lecz również oczekiwana. Niektóre chipsety w sieciach Ethernet są wrażliwe na skrócenie przerwy międzyramkowej, przez co po jej zmniejszeniu mogą wystąpić problemy z wykrywaniem ramek. Wraz ze wzrostem mocy przetwarzania komputerów stacjonarnych mogą one łatwo nasycić ruchem segment sieci Ethernet i rozpoczęć ponowne nadawanie przed upływem czasu opóźnienia związanego z przerwą międzyramkową.

Po wystąpieniu kolizji i gdy w kablu nie ma sygnału z żadnej ze stacji (każda oczekuje przez czas pełnej przerwy międzyramkowej), stacje biorące udział w kolizji muszą odczekać dodatkowy czas (który może rosnąć wykładniczo) przed przystąpieniem do próby ponownego nadania ramki, przy nadawaniu której wystąpiła kolizja. Okres oczekiwania jest celowo zaprojektowany jako losowy, po to, by dwie stacje nie generowały takiego samego opóźnienia przed ponowieniem transmisji, gdyż powodowałoby to wystąpienie kolejnych kolizji. Częściowo zostało to osiągnięte przez zwiększenie najkrótszego interwału, na podstawie którego jest określany losowy czas ponowienia transmisji przy każdej następnej próbie. Okres oczekiwania jest mierzony w przyrostach jednostki „szczelina czasowa”.

Jeśli warstwie MAC nie uda się wysłanie ramki w ciągu 16 prób, rezygnuje i zwraca błąd do warstwy sieci. Taki zdarzenie jest dosyć rzadkie i zachodzi jedynie przy niezmiernie dużych obciążeniach sieci lub gdy w sieci istnieje jakiś problem natury fizycznej.

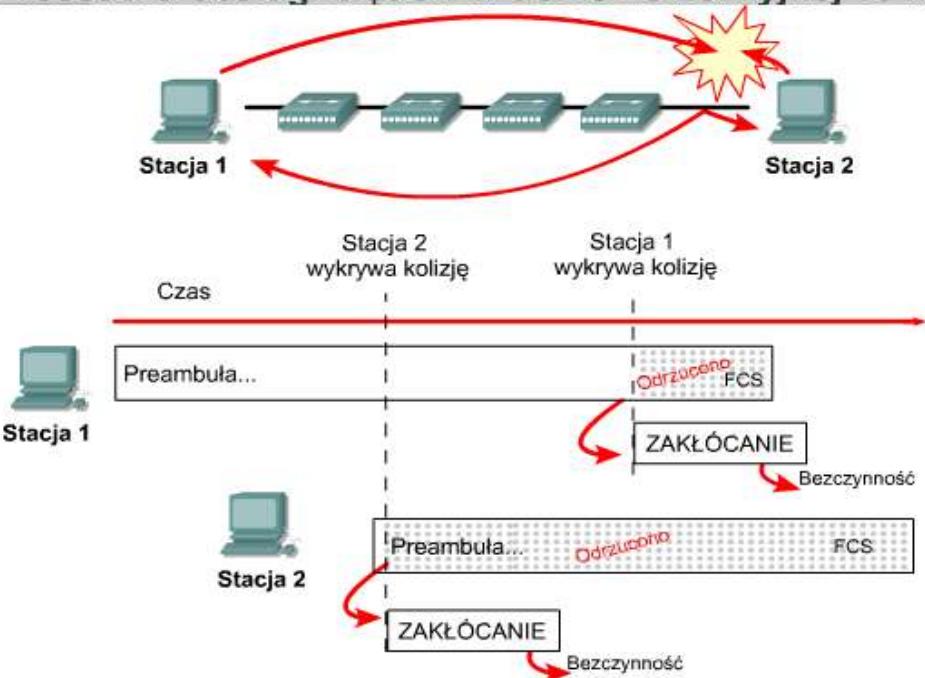
#### 6.2.5 Obsługa błędów

Najczęstszymi błędami w sieciach Ethernet są kolizje. Kolizje są mechanizmem służącym do rozwiązywania problemu rywalizacji o dostęp do sieci. Niewielka liczba kolizji umożliwia płynne, nieskomplikowane i związane z niewielkim narzutem rozstrzyganie rywalizacji węzłów o dostęp do zasobów sieciowych. Gdy rywalizacja o dostęp do sieci staje się zbyt duża, kolizje mogą stać się znaczącą przeszkodą w sprawnym funkcjonowaniu sieci. Rezultatem kolizji jest utrata pasma sieci równe czasowi początkowej transmisji i sygnału sekwencji zakłócającej. Jest to opóźnienie konsumpcyjne, które obejmuje wszystkie węzły sieciowe i z dużym prawdopodobieństwem powoduje znaczące obniżenie przepustowości sieci.

Znaczna większość kolizji występuje w czasie transmisji samego początku ramki, zwykle przed polem SFD. Kolizje występujące przed polem SFD zazwyczaj nie są zgłoszane do wyższych warstw, tak jakby wcale nie wystąpiły. Gdy tylko kolizja zostaje wykryta, stacje wysyłające nadają 32-bitowy sygnał zakłócający, który wymusza wykrycie kolizji. Jest to realizowane tak, aby wszystkie przesyłane dane zostały całkowicie uszkodzone, co umożliwi wszystkim stacjom wykrycie kolizji.

Na rysunku dwie stacje nasłuchują w celu upewnienia się, że w kablu nie ma sygnału, po czym nadają. Stacja 1 mogła nadać znaczącą część ramki, zanim sygnał osiągnął ostatni segment kabla. Stacja 2 nie odebrała pierwszego bitu transmisji przed rozpoczęciem swej własnej transmisji i zdołała wysłać jedynie kilka bitów, zanim karta sieciowa wykryła kolizję. Stacja 2 natychmiast przerwała bieżącą transmisję, zastępując ją 32-bitowym sygnałem zakłócającym, i wstrzymała wszystkie dalsze transmisje. Podczas trwania kolizji i zakłóceń wykrytych przez stację 2 fragmenty kolizyjne wracały do stacji 1 przez domenę kolizyjną połączoną węzłem. Stacja 2 zakończyła transmisję 32-bitowego sygnału zakłócającego i ucichła, zanim kolizja dotarła z powrotem do stacji 1, dla której kolizja pozostała nadal niewidoczna i która kontynuowała nadawanie. Kiedy w końcu fragmenty kolizyjne dotarły do stacji 1, ona również przerwała bieżącą transmisję, wstawiając 32-bitowy sygnał zakłócający zamiast pozostały części ramki. Po wysłaniu 32-bitowego sygnału zakłócającego stacja 1 wstrzymała wszystkie transmisje. Sygnał zakłócający może być złożony z jakichkolwiek danych binarnych, o ile nie tworzą one sumy kontrolnej właściwej dla już nadanej części ramki. Najczęściej występującym wzorcem dla sygnału zakłócającego jest po prostu powtarzający się ciąg zer i jedynek, taki sam jak dla preambuły. Wzorzec ten przeglądany przez

## Procedura obsługi błędów w domenie kolizyjnej 10 Mb/s



trakcie próby wysłania ramki, a podczas następnej próby ramka została pomyślnie wysłana. Kolizja wielokrotna wskazuje, że ta sama ramka wielokrotnie brała udział w kolizji, zanim nastąpiło jej pomyślne wysłanie.

Powstające w wyniku kolizji fragmenty kolizyjne to częściowe lub uszkodzone ramki, które są krótsze niż 64 oktety i mają błędnią sumę FCS. Istnieją trzy rodzaje kolizji: **lokalne, zdalne, spóźnione**.

**Kolizja lokalna** w kablu koncentrycznym (10BASE2 i 10BASE5) występuje, gdy sygnał podróżujący wzduż kabla napotka sygnał z innej stacji. Przebiegi falowe ulegają wówczas nałożeniu, powodując wzajemne znoszenie niektórych części sygnału oraz wzmacnienie lub podwojenie innych jego części. Podwojenie sygnału powoduje podniesienie poziomu napięcia sygnału powyżej dozwolonego maksimum. Właśnie to przekroczenie napięcia jest wykrywane przez wszystkie stacje podłączone do lokalnego segmentu kabla jako kolizja. Na początku przebiegu pokazanego na rysunku znajdują się zwykłe dane zakodowane w standardzie Manchester. Kilka cykli dalej amplituda fali w próbce podwaja się. Jest to początek kolizji, w której dwie fale ulegają nałożeniu. Krótko przed końcem próbki amplituda wraca do stanu normalnego. Dzieje się tak, gdy pierwsza stacja przestaje nadawać po wykryciu kolizji, a sygnał zakłócający pochodzący z drugiej kolidującej stacji jest ciągle widoczny. W kablu UTP, takim jak 10BASE-T, 100BASE-TX lub 1000BASE-T, kolizja jest wykrywana w segmencie lokalnym tylko wtedy, gdy stacja wykryje sygnał w parze RX, prowadząc w tym samym momencie nadawanie w parze TX. Ponieważ oba sygnały są przesyłane w różnych parach przewodów, nie ma żadnych charakterystycznych zmian w sygnale. Kolizje w kablu UTP są rozpoznawane tylko wtedy, gdy stacja pracuje w trybie półduplekusu. Jedyną funkcjonalną różnicę pomiędzy pracą w trybie półduplekusu i pełnego duplekstu w tym kontekście stanowi to, czy pary transmitująca i wysyłająca mogą być używane równocześnie. Jeśli stacja nie jest zajęta nadawaniem, nie może wykryć kolizji lokalnej. Z drugiej strony, wada kabla, taka jak nadmierny przesłuch, może spowodować, że stacja będzie odbierać własną transmisję jako kolizję lokalną.

**Zdalna kolizja** jest rozpoznawana po wielkości ramki, która jest mniejsza od minimalnego rozmiaru i ma błędnią sumę kontrolną FCS, nie zaś po symptomach lokalnej kolizji, takich jak nadmiarowe napięcie czy równoczesna aktywność na liniach RX/TX. Ten rodzaj kolizji jest zwykle wynikiem wystąpienia kolizji po drugiej stronie połączenia z użyciem wtórnika. Wtórnik nie przekaże dalej stanu nadmiernego napięcia i nie może spowodować

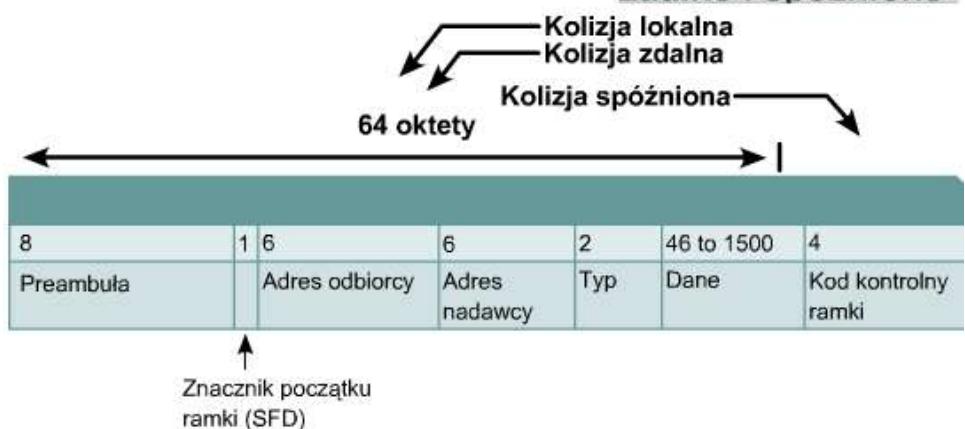
jednoczesnej aktywności obu par (TX i RX) w tym samym czasie. Aby spowodować wystąpienie aktywności w obu parach przewodów, stacja musiałaby nadawać, a to z kolei wywołoby kolizję lokalną. W sieciach opartych na kablu UTP jest to najczęściej obserwowany rodzaj kolizji.

analizator protokołowy przyjmuje postać sekwencji powtarzających się cyfr szesnastkowych: 5 lub A. Uszkodzona, częściowo nadana wiadomość jest zwykle nazywana fragmentami kolizyjnymi lub runtami. Zwykłe kolizje mają mniej niż 64 oktety długości i dlatego są wykrywane zarówno przez test minimalnej długości, jak i przez test sumy kontrolnej FCS.

### 6.2.6 Rodzaje kolizji

Kolizja ma zazwyczaj miejsce, gdy dwie lub więcej stacji sieci Ethernet nadają równocześnie wewnętrz jednej domeny kolizyjnej. Kolizja pojedyncza to taka, która została wykryta w

### Podsumowanie rodzajów kolizji: lokalne, zdalne i spóźnione



**Nie ma możliwości wystąpienia normalnej** (dozwolonej) kolizji po wysłaniu przez stacje nadające pierwszych 64 oktetów danych. Kolizje pojawiające się po pierwszych 64 oktetach są nazywane „kolizjami spóźnionymi”. Najbardziej znaczącą różnicą pomiędzy kolizjami spóźnionymi a kolizjami występującymi przed wysłaniem pierwszych 64 oktetów jest fakt, że karta sieciowa Ethernet automatycznie ponowi transmisję ramki, która uległa normalnej kolizji, lecz ponownie takie nie nastąpi w wypadku kolizji spóźnionej. Z punktu widzenia kart sieciowych transmisja przebiegała pomyślnie, a fakt utraty ramki muszą wykryć wyższe warstwy stosu protokołów. Inaczej niż w wypadku retransmisji, stacja wykrywająca kolizję spóźnioną obsługuje ją w dokładnie ten sam sposób jak kolizję normalną.

### 6.2.7 Błędy w sieci Ethernet

Wiedza dotycząca typowych błędów jest nie do przecenienia zarówno, jeśli chodzi o zrozumienie funkcjonowania sieci Ethernet, jak i rozwiązywanie dotyczących jej problemów.

Poniżej wymienione zostały źródła błędów w sieci Ethernet:

**Kolizja lub runt:** równoczesna transmisja występująca przed upływem szczeliny czasowej.

**Kolizja spóźniona:** równoczesna transmisja występująca po upływie szczeliny czasowej.

**Jabber, dłuża ramka i błędy zakresu:** nadmiernie lub niedopuszczalnie dłuża transmisja.

**Krótką ramka, fragment kolizyjny lub runt:** niedopuszczalnie krótka transmisja.

**Błąd FCS:** uszkodzona transmisja.

**Błąd wyrównania:** niewystarczająca lub nadmierna liczba wysyłanych bitów (nie przekraczająca 8 bitów).

**Błąd zakresu:** niezgodność rzeczywistej i zgłoszonej liczby oktetów w ramce.

**Ghost lub jabber:** nadzwyczaj dłuża preambuła lub zdarzenie zakłócania.

Podczas gdy kolizje lokalne i zdalne są uważane za część normalnej pracy sieci Ethernet, kolizje spóźnione są uważane za błędy. Obecność błędów w sieci zawsze wskazuje na konieczność dalszej analizy. Waga problemu decyduje o tym, jak szybko należy podjąć działania zmierzające do jego rozwiązania w zależności od wykrytych błędów. Niewielka ilość błędów wykrywanych przez wiele minut lub godzin będzie miała niski priorytet. Tysiące błędów wykrytych w czasie kilku minut wskazują, że konieczna jest pilna analiza problemu.

Angielski termin „jabber” definiuje się w pewnych fragmentach standardu 802.3 jako transmisję o czasie trwania odpowiadającym przesłaniu od 20 000 do 50 000 bitów. Jednakże większość narzędzi diagnostycznych zgłasza błąd jabber za każdym razem, gdy wykryta transmisja przekracza maksymalny dozwolony rozmiar ramki, który jest znacznie mniejszy niż czas transmisji 20 000 do 50 000 bitów. Większość odwołań do terminu „jabber” odnosi się więc do bardziej poprawnego pojęcia długich ramek.

Długa ramka to ramka, której rozmiar przekracza dozwolone maksimum, biorąc pod uwagę fakt znakowania ramki. Nie ma znaczenia, czy ramka zawiera poprawną sumę kontrolną FCS. Błąd ten zwykle oznacza, że w sieci wykryto jabber.

Krótką ramka to ramka o długości mniejszej niż minimalna dopuszczalna długość (64 oktetów) z prawidłowym kodem kontrolnym ramki (FCS). Niektóre analizatory protokołowe i monitory sieciowe nazywają takie ramki „runtami”. Ogólnie, obecność krótkich ramek nie musi oznaczać złego funkcjonowania sieci.

Angielski termin „runt” jest, ogólnie rzecz biorąc, nieprecyzyjnym, potocznym pojęciem oznaczającym elementy o wielkości mniejszej niż dozwolony rozmiar ramki. Może się on odnosić do krótkich ramek z poprawną sumą kontrolną FCS, mimo że z reguły odnosi się do fragmentów kolizyjnych.

### 6.2.8 Suma kontrolna FCS i nie tylko

Odebrana ramka, która ma nieprawidłową sekwencję kontrolną ramki, nazywaną również błędem sumy kontrolnej lub błędem CRC, różni się od pierwotnie wysłanej co najmniej jednym bitem. Jeśli chodzi o ramkę z błędem sumy FCS, informacje nagłówka są prawdopodobnie poprawne, lecz suma kontrolna obliczona przez stację odbierającą nie zgadza się z sumą kontrolną dołączoną na końcu ramki przez stację wysyłającą. W takim wypadku ramka zostaje odrzucona.

Wysoka liczba błędów FCS pochodzących z jednej stacji zwykle wskazuje na wadliwą kartę sieciową i/lub wadliwy albo uszkodzony sterownik programowy bądź wadliwy kabel łączący tę stację z siecią. Jeśli błędy FCS pochodzą z wielu stacji, zwykle świadczy to o złym okablowaniu, wadliwej wersji sterownika karty sieciowej, wadliwym porcie koncentratora lub szumie indukowanym w systemie okablowania.

Wiadomość, która nie kończy się na granicy oktetu, jest znana pod nazwą błędu wyrównania. Zamiast prawidłowej liczby bitów tworzących grupę pełnych oktetów, występują bity dodatkowe (mniej niż osiem). Taka ramka jest przycinana do granicy najbliższego oktetu i, jeśli suma kontrolna FCS jest błędna, zgłaszany jest błąd wyrównania. Błąd ten często jest spowodowany złym sterownikiem lub kolizją oraz zazwyczaj towarzyszy mu błędna suma kontrolna FCS.

Odebrana ramka zawierająca popawną wartość pola długości, lecz niezgodną rzeczywistą liczbę oktetów liczonych w jej polu danych, jest znana pod nazwą błędu zakresu. Błąd ten występuje również, gdy wartość pola długości jest mniejsza niż minimalny dozwolony rozmiar pola danych nieuwzględniający wypełnienia. Podobny

błąd określany terminem „poza zakresem” (ang. *Out of Range*) jest zgłaszany, gdy wartość pola długości wskazuje rozmiar danych większy od dozwolonego.

Firma Fluke Networks wprowadziła termin „zjawa” (ang. *ghost*) na oznaczenie energii (szumu) wykrywanej w kablu, która wydaje się ramką, ale brak jej poprawnego pola SFD. Aby ramka została zaklasyfikowana jako zjawa, jej długość, łącznie z preambułą, musi wynosić co najmniej 72 oktety. W przeciwnym razie przypadek taki jest klasyfikowany jako zdalna kolizja. Ze względu na szczególną naturę zjaw ważne jest zaznaczenie, że wyniki testów są w dużym stopniu zależne od tego, w którym miejscu segmentu dokonano pomiaru.

Przyczyną tych błędów są zazwyczaj pętle zerujące i inne problemy z okablowaniem. Większość narzędzi monitorujących sieć nie rozpoznaje istnienia zjaw z tego samego powodu, z którego nie rozpoznają kolizji preambuł. Narzędzia te polegają całkowicie na danych, które przekazuje im chipset. Błędy takie nie są zgłoszane przez programowe analizatory protokołowe, wiele bazujących na sprzęcie analizatorów protokołowych, podręczne narzędzia diagnostyczne, jak również przez większość próbników zdalnego monitorowania (RMON, ang. *remote monitoring*).

### **6.2.9 Autonegocjacja w sieci Ethernet**

W miarę jak Ethernet rozwijał się od szybkości 10 Mb/s do 100 Mb/s i 1000 Mb/s jednym z wymagań było zapewnienie współdziałania między każdą z tych technologii, nawet w tak dużym stopniu, że interfejsy technologii 10, 100 i 1000 Mb/s mogłyby być bezpośrednio połączone. Został zaprojektowany proces zwany procesem autonegocjacji szybkości w trybie półduplekstu lub pełnego dupleksu. W konkretnym przypadku, w czasie wprowadzania technologii Fast Ethernet standard uwzględniał metodę automatycznej konfiguracji danego interfejsu w celu dopasowania go do szybkości i możliwości partnera połączeniowego. Proces ten definiuje sposób, w jaki dwie stacje na wspólnym łączu mogą autonegocjować konfigurację oferującą najlepszy wspólny poziom wydajności. Zapewnia on tę dodatkową korzyść, że angażuje tylko najwyższe części warstwy fizycznej. Technologia 10BASE-T wymagała, żeby każda stacja wysyłała sygnał Link Pulse co około 16 milisekund, jeśli nie była zajęta nadawaniem wiadomości. Metoda autonegocjacji zaadoptowała ten sygnał i przemianowała go na sygnał Normal Link Pulse (NLP). Gdy seria sygnałów NLP jest przesyłana w grupie w celu autonegocjacji, grupa ta jest nazywana serią Fast Link Pulse (FLP). Każda seria FLP jest przesyłana w tym samym interwale czasowym co sygnał NLP, jej przeznaczeniem jest umożliwienie normalnej pracy urządzeniom opartym na starszej technologii 10BASE-T w wypadku, gdy powinny otrzymać serię FLP.

Autonegocjacja jest realizowane przez wysyłanie serii sygnałów Link Pulse standardu 10BASE-T przez każdego z partnerów połączeniowych. Seria przekazuje możliwości stacji nadającej do jej partnera połączeniowego. Kiedy obie stacje zinterpretują ofertę partnera, przełączają się na konfigurację o najwyższej wspólnej wydajności i ustanawiają połączenie z odpowiadającą jej szybkością transmisji. Jeśli komunikacja zostanie przerwana z dowolnego powodu i nastąpi utrata połączenia, obaj partnerzy połączeniowi w pierwszej kolejności próbują połączyć się ponownie z ostatnio wynegocjonowaną szybkością. Jeśli to się nie powiedzie lub jeśli upłynieło zbyt dużo czasu od utraty połączenia, proces autonegocjacji zaczyna się od początku. Połączenie może zostać utracone na skutek czynników zewnętrznych, takich jak awaria kabla, lub na skutek zresetowania jednego z partnerów.

### **6.2.10 Ustalanie połączenia oraz tryby pełnego dupleksu i półduplekstu**

Partnerzy połączeniowi mogą pominąć prezentację konfiguracji odpowiadającej ich możliwościom. Pozwala to administratorom sieciowym wymusić wybraną szybkość i tryb dupleksu portów bez wyłączania funkcji autonegocjacji.

Autonegocjacja jest funkcją opcjonalną w większości implementacji technologii Ethernet. Jego implementacji wymaga technologia Gigabit Ethernet, mimo że użytkownik może tę funkcję wyłączyć. Autonegocjacja była pierwotnie zdefiniowana dla implementacji technologii Ethernet opartych na okablowaniu UTP, a następnie została rozszerzona, tak by funkcjonowała z implementacjami światłowodowymi.

Gdy stacja biorąca udział w autonegocjacji próbuje po raz pierwszy nawiązać połączenie, powinna włączyć sygnalizację 100BASE-TX w celu podjęcia próby natychmiastowego ustanowienia połączenia. Jeśli sygnalizacja 100BASE-TX jest obecna, a stacja obsługuje standard 100BASE-TX, podjęta zostanie próba ustalenia połączenia bez negocjacji. Jeśli sygnalizacja spowoduje nawiązanie połączenia lub zostanie odebrana seria FLP, stacja będzie kontynuowała komunikację z wykorzystaniem tej technologii. Jeśli partner połączeniowy zamiast serii FLP nadaje sygnał NLP, automatycznie zakłada się, że urządzenie to jest stacją opartą na technologii 10BASE-T. Podczas tego początkowego interwału testowania obecności innych technologii ścieżka transmisyjna wysyła serie FLP. Standard nie zezwala na równoległe wykrycie jakiekolwiek innej technologii.

Jeśli połączenie zostało ustanowione za pośrednictwem wykrywania równoległego, to połączenie musi być realizowane w trybie półduplekstu. Istnieją tylko dwie metody, za pomocą których można nawiązać połączenie w trybie pełnego dupleksu. Jedna z nich obejmuje pełen cykl autonegocjacji, zaś druga to administracyjne wymuszenie pracy obu partnerów połączeniowych w trybie pełnego dupleksu. Jeśli jeden z partnerów połączeniowych działa w wymuszonym trybie pełnego dupleksu, a drugi partner próbuje autonegocjacji, to pewne

jest wystąpienie niedopasowania dupleksu. Spowoduje to kolizje i błędy na tym łączu. Co więcej, jeśli tryb pełnego dupleksu został wymuszony po jednej stronie, musi być on wymuszony również po drugiej stronie. Wyjątkiem od tej reguły jest technologia 10 Gigabit Ethernet, która nie obsługuje trybu półdupleksowego. Implementacje sprzętowe wielu producentów realizują funkcję cyklicznego przechodzenia przez różne możliwe stany. Przez chwilę są wysyłane serie FLP w celu autonegocjacji, później sprzęt zostaje skonfigurowany w trybie Fast Ethernet, następnie przez pewien czas podejmowana jest próba połączenia, po czym urządzenie jedynie nasłuchuje. Niektórzy producenci nie uwzględniają żadnych aktywnych prób połączenia do czasu odebrania przez interfejs serii FLP lub innego schematu sygnalizacji.

Istnieją dwa tryby dupleksu: półdupleks i pełny dupleks. Dla mediów współdzielonych tryb półdupleksu jest obowiązkowy. Wszystkie implementacje oparte na kablu koncentrycznym są półdupleksowe z natury i nie mogą pracować w trybie pełnego dupleksu. Implementacje oparte na skrętce UTP i światłowodzie mogą pracować w trybie półdupleksu. Implementacje technologii 10 Gb/s zostały określone z uwzględnieniem jedynie trybu pełnego dupleksu.

W trybie półdupleksu w danym momencie może nadawać tylko jedna stacja. W implementacjach na kablach koncentrycznych druga nadająca stacja spowoduje nałożenie się sygnałów i ich zniekształcenie. Ponieważ w wypadku kabla UTP i światłowodu nadawanie odbywa się przede wszystkim za pomocą osobnych par przewodów, sygnały nie mają możliwości nakładania się i zniekształcania. Technologia Ethernet zawiera reguły arbitrażu służące do rozwiązywania konfliktów powstających w sytuacjach, gdy więcej niż jedna stacja próbuje nadawać w tym samym czasie. Jeśli chodzi o połączenia punkt-punkt w trybie pełnego dupleksu, każda ze stacji może nadawać w dowolnym czasie bez względu na to, czy druga stacja prowadzi w danym momencie transmisję. Autonegocjacja pozwala na uniknięcie większości sytuacji, w których jedna stacja w połączeniu punkt-punkt nadaje zgodnie z regułami półdupleksu, a druga nadaje w trybie pełnego dupleksu.

## Moduł 7. Technologie używane w sieciach ETHERNET

Ethernet stał się najpopularniejszą technologią stosowaną w sieciach LAN głównie dlatego, że w porównaniu z innymi technologiami jest łatwiejszy w implementacji. Sieci Ethernet zawdzięczają swoje powodzenie także elastyczności tej technologii, która zmieniała się wraz z pojawianiem się nowych potrzeb użytkowników i możliwości mediów. W tym module przedstawiono szczegółowe informacje dotyczące najważniejszych odmian sieci Ethernet. Celem nie jest przekazanie wszystkich informacji o każdym rodzaju sieci Ethernet, a raczej pokazanie elementów wspólnych wszystkim jej rodzajom.

Zmiany w technologii Ethernet zaowocowały znacznymi ulepszeniami w stosunku do sieci Ethernet 10 Mb/s z początku lat osiemdziesiątych. Standard sieci Ethernet 10 Mb/s pozostawał praktycznie niezmieniony do roku 1995, kiedy organizacja IEEE ogłosiła standard Fast Ethernet 100 Mb/s. Ostatnie lata przyniosły jeszcze gwałtowniejszy wzrost szybkości mediów, co spowodowało przechodzenie z sieci Fast Ethernet na sieć Gigabit Ethernet. Standardy dla sieci Gigabit Ethernet pojawiły się w ciągu zaledwie trzech lat. Teraz ogólnie dostępna jest jeszcze szybsza wersja sieci Ethernet, czyli 10 Gigabit Ethernet, a opracowywane są sieci o większej prędkości.

W porównaniu z wcześniejszymi sieciami Ethernet w tych szybszych wersjach nie zmieniły się metody adresowania MAC, algorytm CSMA/CD i format ramki. Zmianie uległy jednak inne elementy podwarstwy MAC, warstwy fizycznej oraz samego medium. Często spotyka się teraz karty sieciowe (NIC) dla mediów miedzianych, które mogą pracować z prędkościami 10/100/1000 Mb/s. W węzłach dystrybucji okablowania standardem stają się gigabitowe porty w routeraх i przełącznikach. Standardem w większości nowych okablowań szkieletowych jest stosowanie sieci Gigabit Ethernet opartych na światłowodach.

### 7.1 Sieci Ethernet 10 Mb/s i 100 Mb/s

#### 7.1.1. Sieć Ethernet 10 Mb/s

Sieci Ethernet 10BASE5, 10BASE2 i 10BASE-T są uznawane za klasyczne sieci Ethernet; Klasyczne sieci Ethernet mają cztery cechy wspólne. Są to: parametry czasowe, format ramki, proces transmisji oraz podstawowe reguły obowiązujące przy ich projektowaniu.

**Rysunek pokazuje parametry Ethernetu 10 Mb/s.** Ten typ Ethernetu oraz wersje wolniejsze są asynchroniczne. Każda stacja odbiorcza używa specjalnych ośmiu oktetów do zsynchronizowania swych układów odbiorczych z nadchodzącyymi danymi. Sieci 10BASE5, 10BASE2 i 10BASE-T mają takie same parametry czasowe. Dla przykładu czas przesłania 1 bitu przy prędkości 10 Mb/s = 100 nanosekund (ns) = 0,1 mikrosekundy = 1 dziesięciomilionowa część sekundy.

To oznacza, że w Etherencie 10 Mb/s przesłanie 1 bitu w podwarstwie MAC trwa 100 ns.

Dla wszystkich prędkości w Etherencie, 1000 Mb/s lub wolniejszych, transmisja nie może być krótsza niż szczelina czasowa. Szczelina czasowa jest minimalnie dłuższa niż czas, który jest teoretycznie potrzebny na przejście od jednego końca maksymalnie dużej, prawidłowej domeny kolizyjnej do drugiego końca, kolizję z inną transmisją możliwe póżno, a następnie powrót uszkodzonego fragmentu, by został wykryty przez stację nadawczą.

#### Sieci 10BASE5, 10BASE2 i 10BASE-T mają także wspólny format ramki.

Proces transmisji w klasycznych sieciach Ethernet przebiega w ten sam sposób aż do niższej części warstwy fizycznej modelu OSI. Gdy ramka przechodzi z podwarstwy MAC do warstwy fizycznej, przed umieszczeniem bitów z warstwy fizycznej w medium przeprowadzane są dodatkowe operacje. Jedną z ważnych operacji jest wstawienie sygnału SQE (Signal Quality Error). SQE to transmisja wysyłana przez transceiver z powrotem do

### Typy sieci Ethernet

Podwarstwa LLC (Logical Link Control)	
802.3 Media Access Control (kontrola dostępu do medium)	
Fizyczna warstwa sygnałowa	Medium fizyczne
10BASE5 (500 m) 50-omowy kabel koncentryczny	10BASE2 (185 m) 50-omowy kabel koncentryczny ze złączem BNC
10BASE-T (100 m) 100-omowy kabel UTP ze złączeniem RJ-45	100BASE-TX (100 m) 100-omowy kabel UTP ze złączeniem RJ-45
100BASE-FX (228-412 m) światłowód MM ze złączeniem SC	100BASE-FX (228-412 m) światłowód MM ze złączeniem SC
1000BASE-T (100 m) 100-omowy kabel UTP ze złączeniem RJ-45	1000BASE-SX (220-550 m) światłowód MM ze złączeniem SC
	1000BASE-LX (550-5000 m) światłowód MM lub SM ze złączeniem SC
	10GBASE-(róźne) światłowód MM lub SM ze złączeniem SC

### Parametry pracy sieci Ethernet 10 Mb/s

Parametr	Wartość
Czas transmisji bitu	100 nanosekund (ns)
Czas trwania szczeliny	Czas transmisji 512 bitów (64 oktetów)
Przerwa międzyramkowa	96 bitów *
Limit prób po kolizji	16
Limit zwiększania okresu odczekiwania po kolizji	10
Rozmiar sekwencji zakłócającej	32 bity
Maksymalny rozmiar ramki bez znacznika VLAN	1518 oktetów
Minimalny rozmiar ramki	512 bitów (64 oktesy)

kontrolera by sprawdzić, czy jego układy wykrywania kolizji działają prawidłowo. SQE jest też zwany sygnałem bicia serca (heartbeat). Sygnał SQE został zaprojektowany do wcześniejszych wersji Ethernetu gdzie host nie zawsze wiedział czy transceiver jest w danym momencie faktycznie przyłączony. Sygnał ten jest zawsze używany w trybie półdupleksu. Sygnał SQE może być także używany w trybie pełnego dupleksu, ale nie jest to konieczne.

#### Sygnal SQE jest aktywny w następujących przypadkach:

W czasie od 4 do 8 mikrosekund po normalnej transmisji, sygnalizując, że wychodząca ramka została pomyślnie przesłana.

W wypadku wystąpienia kolizji w medium.

Gdy w medium pojawi się nieprawidłowy sygnał, taki jak odbicia wynikające ze zwarcia kabla lub zbyt długie ramki (jabber).

W wypadku przerwania transmisji.

Wszystkie rodzaje sieci Ethernet 10 Mb/s przeprowadzają na oktetach otrzymanych z podwarstwy MAC proces zwany kodowaniem liniowym. Kodowanie liniowe opisuje sposób przesyłania bitów przez przewody. Najprostsze metody kodowania mają niekorzystne charakterystyki czasowe i elektryczne. Ze względu na to zaprojektowano takie kody, które mają pożądane własności transmisyjne. W sieci 10 Mb/s używany jest schemat kodowania Manchester.

Do określenia wartości binarnej dla danego okresu bitu w kodowaniu Manchester wykorzystywany jest kierunek zbocza pośrodku okna czasowego. Górnny przebieg ma opadające zbocze, więc jest interpretowany jako 0 binarne. Następny przebieg ma zbocze narastające, które jest interpretowane jako 1 binarna. Trzeci przebieg zawiera zmieniającą się sekwencję liczb binarnych. W wypadku zmieniających się danych binarnych nie istnieje potrzeba powrotu do poprzedniego poziomu napięcia. Jak widać na trzecim i czwartym przebiegu, wartości binarne są wyznaczone przez kierunek zmian w czasie trwania danego bitu. Poziomy napięcia na początku i końcu każdego okresu bitu nie wyznaczają wartości binarnych. Architektura sieci klasycznego Ethernetu ma wiele cech wspólnych. Sieci składają się zwykle z różnych rodzajów mediów. Dzięki zgodności ze standardem mogą one ze sobą współpracować. Ogólny projekt architektury nabiera zasadniczego znaczenia przy tworzeniu sieci złożonej z różnych mediów. Gdy sieć się rozrasta, łatwiej przekroczyć maksymalne limity opóźnień. **Limity czasowe zależą od takich parametrów, jak:**

- długość kabla i jego opóźnienie propagacji,
- opóźnienia wórników,
- opóźnienia transceiverów,
- zmniejszanie przerwy międzyramkowej,
- opóźnienia wewnętrz stacji.

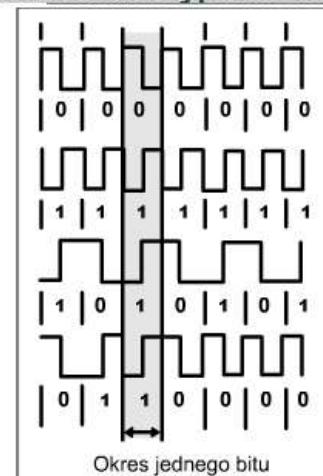
Sieć Ethernet 10 Mb/s może działać bez przekraczania limitów czasowych, jeśli składa się z nie więcej niż pięciu segmentów oddzielonych nie więcej niż czterema wórnikami. Jest to tak zwana reguła 5-4-3. Na drodze między dwiema odległymi stacjami nie mogą znajdować się więcej niż cztery kolejne wórniki. Pomiędzy tymi stacjami nie mogą znajdować się także więcej niż trzy wykorzystywane segmenty.

#### 7.1.2 10BASE5

W oryginalnej sieci Ethernet 10BASE5 z roku 1980 dane były transmitowane z prędkością 10 Mb/s przez magistralę, którą stanowił pojedynczy gruby kabel koncentryczny. Technologia 10BASE5 jest ważna, ponieważ było to pierwsze medium używane przez sieci Ethernet. Technologia 10BASE5 stanowiła część oryginalnego standardu 802.3. Podstawową zaletą technologii 10BASE5 był zasięg. Dziś można ją spotkać w starszych typach instalacji, nie jest jednak zalecana w nowych instalacjach. Systemy zbudowane w technologii 10BASE5 są niedrogie i nie wymagają konfiguracji, ale bardzo trudno dziś znaleźć na rynku takie podstawowe komponenty, jak karty sieciowe, zaś sama technologia nie jest odporna na odbicia sygnału w kablu. Systemy 10BASE5 cechują się także pojedynczym punktem awarii.

W systemach tych stosowane jest kodowanie typu Manchester. W kablu znajduje się jednolity centralny przewodnik. Każdy z maksymalnie pięciu segmentów grubego kabla koncentrycznego może mieć do 500 metrów długości. Okablowanie jest duże, ciężkie i trudne w instalacji. Jednak stosunkowo duża dopuszczalna długość segmentu stanowiła zaletę, co przedłużyło korzystanie z tej technologii w pewnych zastosowaniach.

#### Przykłady kodowania typu Manchester.



Przykład kodowania typu Manchester. Oś Y przedstawia napięcie, a os X przedstawia czas.

Ponieważ medium jest pojedynczy kabel koncentryczny, tylko jedna stacja może transmitować pakiety w danej chwili, gdyż w przeciwnym wypadku nastąpi kolizja. Z tego powodu sieć 10BASE5 działa tylko w trybie półdupleksu, przez co maksymalna prędkość przesyłania danych wynosi 10 Mb/s.

### 7.1.3 10BASE2

Technologia 10BASE2 została wprowadzona w roku 1985. Proces instalacji stał się prostszy dzięki mniejszemu rozmiarowi i wadze oraz większej elastyczności kabla. Ta technologia jest nadal

używana w starszych sieciach natomiast stosowanie jej w nowych instalacjach nie jest zalecane, podobnie jak sieci 10BASE5. Jest ona tania i nie wymaga stosowania hubów. Także w jej wypadku trudno jest znaleźć na rynku odpowiednie karty sieciowe.

Również w technologii 10BASE2 wykorzystywane jest kodowanie typu Manchester. Komputery w sieci LAN są łączone ze sobą za pomocą nieprzerwanego łańcucha odcinków kabli koncentrycznych. Kable przyłącza się do złącz typu T na kartach sieciowych za pomocą złączy BNC.

W technologii 10BASE2 jako wewnętrzną żyłę używa się linki. Każdy z maksymalnie pięciu segmentów kabla koncentrycznego może mieć długość do 185 metrów, a każda stacja jest podłączona bezpośrednio do złącza BNC typu T na kablu.

Tylko jedna stacja może transmitować dane naraz, gdyż w przeciwnym razie nastąpi kolizja. Również w technologii 10BASE2 używany jest tryb półdupleksu. Maksymalna szybkość transmisji w technologii 10BASE2 wynosi 10 Mb/s.

Do pojedynczego segmentu 10BASE2 można przyłączyć do 30 stacji. Spośród pięciu kolejnych segmentów między dwiema stacjami tylko do trzech z nich mogą być podłączone komputery.

### 7.1.4 10BASE-T

Technologia 10BASE-T została wprowadzona w roku 1990.

Zamiast kabla koncentrycznego jest w niej używana tańsza i łatwiejsza w instalacji skrętka nieekranowana (UTP) kategorii 3.

Kabel jest podłączany do centralnego urządzenia zawierającego wspólną szynę.

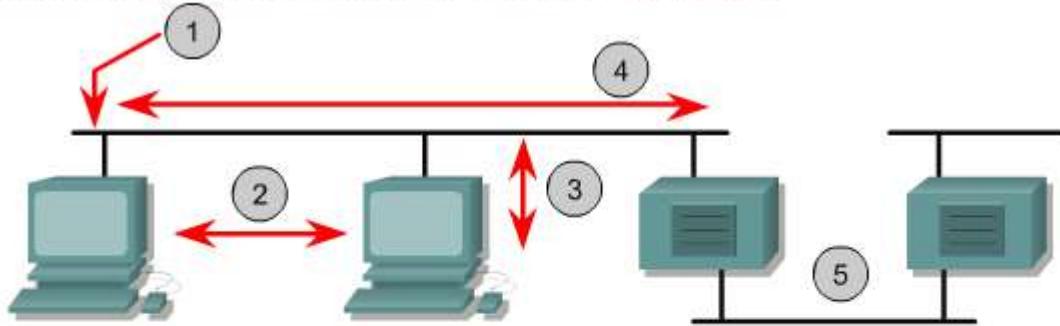
Tym urządzeniem jest hub.

Znajduje się on w środku zestawu kabli, które rozchodzą się do

komputerów w podobny sposób jak szpary w kole. Taki układ określa się mianem topologii gwiazdy. Długość kabli wychodzących z huba oraz sposób instalacji skrętki nieekranowanej przyczynił się do tworzenia układów gwiazd złożonych z gwiazd, nazywanych topologią gwiazdy rozszerzonej. Technologia 10BASE-T była początkowo półdupleksowa. Później dodano możliwość pracy w pełnym dupleksie. Gwałtowny wzrost popularności Ethernetu nastąpił w drugiej połowie lat dziewięćdziesiątych, kiedy Ethernet stał się dominującą technologią sieci LAN.

Również w technologii 10BASE-T wykorzystywane jest kodowanie typu Manchester. Skrętka nieekranowana 10BASE-T ma jednolity przewodnik w każdym przewodzie kabla poziomego o maksymalnej długości 90 metrów.

## Ograniczenia projektowe sieci 10BASE2



1. Oba końce kabla koncentrycznego powinny być zakończone terminatorami o impedancji falowej 50 omów.
2. Minimalna odległość pomiędzy punktami wpięcia urządzeń do kabla wynosi 0,5 metra.
3. Każda stacja musi być bezpośrednio połączona z trójnikiem BNC wpięтыm do kabla koncentrycznego.
4. Maksymalna długość segmentu wynosi 185 metrów.
5. Do segmentów sieci pomiędzy węzłami mogą być dołączone tylko dwa urządzenia, którymi są te węzły.

używana w starszych sieciach natomiast stosowanie jej w nowych instalacjach nie jest zalecane, podobnie jak sieci 10BASE5. Jest ona tania i nie wymaga stosowania hubów. Także w jej wypadku trudno jest znaleźć na rynku odpowiednie karty sieciowe.

Również w technologii 10BASE2 wykorzystywane jest kodowanie typu Manchester. Komputery w sieci LAN są łączone ze sobą za pomocą nieprzerwanego łańcucha odcinków kabli koncentrycznych. Kable przyłącza się do złącz typu T na kartach sieciowych za pomocą złączy BNC.

W technologii 10BASE2 jako wewnętrzną żyłę używa się linki. Każdy z maksymalnie pięciu kolejnych segmentów kabla koncentrycznego może mieć długość do 185 metrów, a każda stacja jest podłączona bezpośrednio do złącza BNC typu T na kablu.

Tylko jedna stacja może transmitować dane naraz, gdyż w przeciwnym razie nastąpi kolizja. Również w technologii 10BASE2 używany jest tryb półdupleksu. Maksymalna szybkość transmisji w technologii 10BASE2 wynosi 10 Mb/s.

Do pojedynczego segmentu 10BASE2 można przyłączyć do 30 stacji. Spośród pięciu kolejnych segmentów między dwiema stacjami tylko do trzech z nich mogą być podłączone komputery.

## Układ styków gniazdka modułowego w sieci 10BASE-T

Numer styku	Sygnał
1	TD+ (dane wysypane, dodatni sygnał różnicowy)
2	TD- (wysypane, ujemny sygnał różnicowy)
3	RD+ (dane odbierane, dodatni sygnał różnicowy)
4	Nie używane
5	Nie używane
6	RD- (dane odbierane, ujemny sygnał różnicowy)
7	Nie używane
8	Nie używane

komputerów w podobny sposób jak szpary w kole. Taki układ określa się mianem topologii gwiazdy. Długość kabli wychodzących z huba oraz sposób instalacji skrętki nieekranowanej przyczynił się do tworzenia układów gwiazd złożonych z gwiazd, nazywanych topologią gwiazdy rozszerzonej. Technologia 10BASE-T była początkowo półdupleksowa. Później dodano możliwość pracy w pełnym dupleksie. Gwałtowny wzrost popularności Ethernetu nastąpił w drugiej połowie lat dziewięćdziesiątych, kiedy Ethernet stał się dominującą technologią sieci LAN.

Również w technologii 10BASE-T wykorzystywane jest kodowanie typu Manchester. Skrętka nieekranowana 10BASE-T ma jednolity przewodnik w każdym przewodzie kabla poziomego o maksymalnej długości 90 metrów.

Do skrętki nieekranowanej używane są ośmioistykowe złącza RJ-45. Chociaż kabel kategorii 3 jest wystarczający dla sieci 10BASE-T, do wszelkich nowych instalacji zaleca się używanie kabla kategorii 5e lub lepszego. We wszystkich czterech parach przewodów należy zastosować wyprowadzenia styków T568-A lub T568-B. Instalacja tego typu kabli umożliwia korzystanie z różnych protokołów bez potrzeby zmiany okablowania. Na rysunku pokazano wyprowadzenia styków dla połączenia w technologii 10BASE-T. Para transmitująca po stronie odbiorczej jest połączona z parą odbiorczą w dołączonym urządzeniu.

W zależności od konfiguracji używany jest tryb półduplexu bądź pełnego dupleksu. Sieć 10BASE-T przenosi dane z prędkością 10 Mb/s w trybie półduplexu i z prędkością 20 Mb/s w trybie pełnego dupleksu.

### 7.1.5 Okablowanie i architektura w technologii 10BASE-T

Łącza w sieci 10BASE-T składają się zwykle z połączeń stacji z hubem lub z przełącznikiem. Huby są wieloportowymi wtyrkami i należy je uwzględniać przy obliczaniu limitu liczby wtyrków między odległymi stacjami. Huby nie dzielą segmentów sieci na oddzielne domeny kolizyjne. Ze względu na to, że huby i wtyrki zwiększą długość segmentu wewnętrz pojedynczej domeny kolizyjnej, istnieje ograniczenie co do liczby hubów w danym segmencie. Mosty i przełączniki dzielą segment na osobne domeny kolizyjne; w takiej sytuacji jedynym ograniczeniem dotyczącym odległości między przełącznikami są ograniczenia narzucone przez medium. W sieciach 10BASE-T odległość między przełącznikami jest ograniczona do 100 m.

Chociaż huby można łączyć, lepiej unikać takiego układu. Zapobiega to przekroczeniu maksymalnego opóźnienia między odległymi stacjami. Jeśli potrzebnych jest wiele hubów, najlepiej jest ułożyć je hierarchicznie, tworząc strukturę podobną do drzewa. Wydajność zwiększy się, jeżeli między stacjami będzie mniej wtyrków.

Na rysunku przedstawiono przykładową architekturę. Wszystkie odległości między stacjami są dopuszczalne. Jednak całkowita odległość między skrajnymi punktami sieci jest taka, że architektura zbliża się do swego górnego limitu. Najważniejszym zagadnieniem, które należy rozpatrzyć, jest utrzymanie minimalnych opóźnień między odległymi stacjami, niezależnie od architektury i użytych mediów. Krótsze maksymalne opóźnienie zaowocuje lepszą ogólną wydajnością.

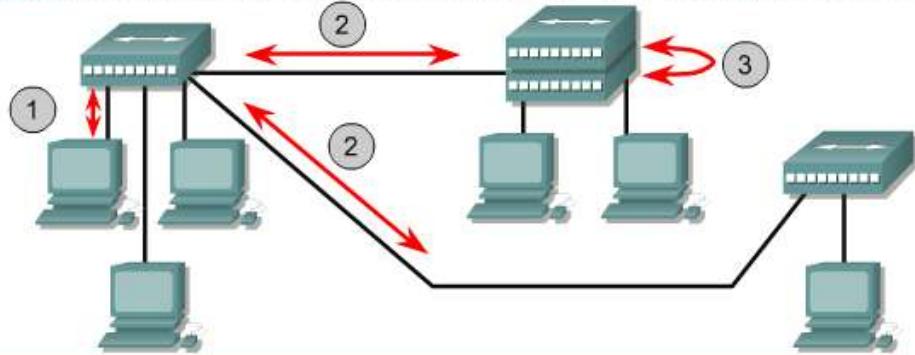
Łącza 10BASE-T bez wtyrków mogą mieć długość do 100 m. Wydaje się, że to duża odległość, jednak w praktyce przy okablowywaniu budynku długość ta jest zwykle w całości wykorzystywana. Huby mogą rozwijać problemy z odległością, ale pozwalają na propagację kolizji. Powszechnie użycie przełączników przyczyniło się do zmniejszenia znaczenia problemu odległości. Jeżeli stacje robocze znajdują się w odległości mniejszej niż 100 m od przełącznika, to za przełącznikiem odległość tę można zacząć mierzyć od początku.

### 7.1.6 Sieć Ethernet 100 Mb/s

Technologia Ethernet 100 Mb/s jest znana również pod nazwą Fast Ethernet. Dwie technologie, które zyskały na znaczeniu, to 100BASE-TX, używająca miedzianej skrętki nieekranowanej UTP, oraz 100BASE-FX, używająca światłowodu wielomodowego.

Trzy charakterystyczne elementy, wspólne dla technologii 100BASE-TX i 100BASE-FX, to parametry czasowe, format ramki i elementy procesu transmisji. Obie technologie, 100BASE-TX i 100BASE-FX, mają jednakowe parametry czasowe. Zauważmy, że czas przesłania jednego bitu z prędkością 100 Mb/s wynosi  $10 \text{ ns} = 0,01 \text{ mikrosekundy}$ .

### Ograniczenia projektowe sieci 10BASE-T z regeneratorami



1. Długość kabla UTP łączącego stację z hubem, lub przebiegającego pomiędzy hubami wynosi zwykle od 1 do 100 m
2. Każdy koncentrator jest wieloportowym regeneratorem, więc łącza pomiędzy koncentratorami są uwzględniane przy obliczaniu maksymalnej liczby wtyrków.
3. Te dwa zestawialne koncentratory z połączonymi ze sobą panelami tylnymi uważa się za jeden koncentrator [regenerator].

### Parametry pracy sieci Ethernet 100 Mb/s

Parametr	Wartość
Czas transmisji bitu	10 nanosekund (ns)
Czas trwania szczeliny	Czas transmisji 512 bitów (64 oktetów)
Przerwa międzyramkowa	96 bitów
Limit prób po kolizji	16
Limit zwiększania okresu odczekiwania po kolizji	10
Rozmiar sekwencji zakłócającej	32 bity
Maksymalny rozmiar ramki bez znacznika VLAN	1518 oktetów
Minimalny rozmiar ramki	512 bitów (64 oktesy)

1 stumilionową część sekundy.

### Format ramki sieci 100 Mb/s jest taki sam, jak w sieci

**10 Mb/s.** Sieć Fast Ethernet jest dziesięć razy szybsza niż sieć 10BASE-T. Z powodu większej

prędkości należy zachować ostrożność, gdyż wysyłane bity są krótsze i występują częściej. Sygnały o większej częstotliwości są bardziej narażone na szумy. W celu zaradzenia tym problemom w sieciach Ethernet 100 Mb/s używane są dwa oddzielne etapy kodowania. W pierwszym etapie kodowania używana jest metoda o nazwie 4B/5B, a w drugiej właściwe kodowanie liniowe, zależne od typu medium, którym jest kabel miedziany lub włókno światłowodowe.

### 7.1.7 100BASE-TX

W roku 1995 technologia 100BASE-TX (używająca skrętki nieekranowanej kategorii 5) stała się standardem, który odniósł sukces komercyjny.

Oryginalna technologia Ethernet, używająca kabli koncentrycznych, działała w trybie transmisji półduplexowej, tak więc tylko jedno urządzenie w danym czasie mogło przesyłać dane. Jednak w roku 1997 możliwości Ethernetu zostały poszerzone o transmisję w trybie pełnego dupleksu, co umożliwiło przesyłanie danych przez więcej niż jeden komputer w tym samym czasie. Przełączniki zaczęły wypierać huby. Umożliwiały one bowiem transmisję w trybie pełnego dupleksu, a czas obsługi ramek sieci Ethernet był bardzo krótki.

W technologii 100BASE-TX dane są kodowane przy użyciu kodu 4B/5B, a następnie konwertowane przy użyciu kodu MLT-3 (Multi-Level Transmit-3). **Na rysunku przedstawiono wyprowadzenia styków połączenia w standardzie 100BASE-TX. Należy zauważyć, że istnieją dwie oddzielne ścieżki nadawczo-odbiorcze. Tak samo jest w sieci 10BASE-T.**

W sieci 100BASE-TX dane mogą być przesyłane z prędkością 100 Mb/s w trybie półduplexu. W trybie pełnego dupleksu możliwe jest przesyłanie danych z prędkością 200 Mb/s. Tryb pełnego dupleksu będzie zyskiwał na znaczeniu wraz ze zwiększeniem prędkości sieci Ethernet.

### Wyprowadzenia styków złącza modułowego w sieci 100BASE-TX

Numer styku	Sygnal
1	TD+ (dane wysyłane, dodatni sygnał różnicowy)
2	TD- (dane wysyłane, ujemny sygnał różnicowy)
3	RD+ (dane odbierane, dodatni sygnał różnicowy)
4	Nie używane
5	Nie używane
6	RD- (dane odbierane, ujemny sygnał różnicowy)
7	Nie używane
8	Nie używane

### 7.1.8 100BASE-FX

Wraz z wprowadzeniem sieci Fast Ethernet opartej na kablach miedzianych powstała potrzeba utworzenia jej wersji światłowodowej. Wersja oparta na

światłowodach mogłaby być używana w sieciach szkieletowych, połączeniach między piętrami i budynkami, gdzie kable miedziane są mniej przydatne, oraz w środowiskach o dużych zakłóceniach. Aby zaspokoić te potrzeby, wprowadzono technologię 100BASE-FX. Jednak technologia 100BASE-FX nigdy nie odniosła sukcesu. Powodem tego było szybkie wprowadzenie standardów Gigabit Ethernet dla kabli miedzianych i światłowodów. Standardy Gigabit Ethernet są obecnie dominującą technologią w instalacjach szkieletowych, szybkich przełącznicach oraz w innych zastosowaniach związanych z infrastrukturą.

Taktowanie, format ramki i transmisja są takie same dla obydwu wersji technologii Fast Ethernet 100 Mb/s.

**Na rysunku przedstawiono podsumowanie informacji dotyczących łączą i wyprowadzeń styków w technologii 100BASE-FX. Najczęściej używana jest para światłowodów ze złączami ST lub SC. Możliwa jest transmisja z prędkością 200 Mb/s, ponieważ w sieci 100BASE-FX wykorzystywane są oddzielne włókna optyczne dla ścieżki nadawczej (Tx) i odbiorczej (Rx).**

### Ramka sieci Ethernet

#### Ramka sieci Ethernet

Preambuła	SFD	Adres docelowy	Adres źródłowy	Długość pola danych	Dane	Pole wypełnienia	FCS
7	1	6	6	2	46 to 1500		4

### Wyprowadzenia złącza w sieci 100BASE-FX

Włókno światłowodowe	Sygnal
1	Tx (diody LED i nadajniki laserowe)
2	Rx (szybkie fotodiody detekcyjne)

## 7.1.9 Architektura sieci

### Fast Ethernet

Łącza Fast Ethernet zwykle składają się z połączeń między stacją a hubem lub przełącznikiem. Huby uważane są za wieloportowe węzły, a przełączniki — za wieloportowe mosty. W obu przypadkach obowiązuje ograniczenie długości skrętki nieekranowanej do 100 m. Węzeł klasy I może wprowadzać opóźnienia o maksymalnej długości nie przekraczającej 140 czasów transmisji bitu. Każdy węzeł zamieniający jedną z wersji sieci Ethernet na inną jest

węzłem klasy I. Węzeł klasy II ogranicza wprowadzane opóźnienie do 92 czasów transmisji bitu, ponieważ natychmiast powtarza transmisję przychodzącego sygnału na wszystkie porty bez żadnych translacji. Aby jednak osiągnąć tak małe opóźnienia, węzeł ten może łączyć tylko segmenty używające tej samej techniki sygnalizacji. Podobnie jak w przypadku wersji 10 Mb/s, w wersji 100 Mb/s także można modyfikować niektóre reguły architektury. Jednak praktycznie nie można wprowadzać dodatkowych opóźnień. Jeśli chodzi o sieć 100BASE-TX, zdecydowanie odradza się modyfikację reguł architektury. Kabel między dwoma węzłami klasy II w sieci 100BASE-TX nie może być dłuższy niż 5 metrów. Dość często można spotkać łączę w sieci Fast Ethernet działające w półduplekcie. Jednak tryb ten jest niepożądany, gdyż schemat sygnalizacji został zaprojektowany pod kątem pracy w pełnym dupleksie.

**Na rysunku przedstawiono długości kabli dla różnych konfiguracji architektury.** Łącza 100BASE-TX mogą nie korzystać z węzłów, jeśli odległości są krótsze niż 100 m. Wprowadzenie przełączników zmniejszyło znaczenie tego ograniczenia długości. Ponieważ większość sieci Fast Ethernet korzysta z przełączników, są to praktyczne ograniczenia odległości między urządzeniami.

## 7.2 Sieć Ethernet Gigabit i 10 Gigabit

### 7.2.1 Sieć Ethernet 1000 Mb/s

Standardy sieci Ethernet 1000 Mb/s, czyli Gigabit Ethernet, umożliwiają transmisję zarówno w medium miedzianym, jak i światłowodowym. Standard 1000BASE-X, znany również pod nazwą IEEE 802.3z, opisuje pełnodupleksozą technologię światłowodową, która umożliwia transmisję z prędkością 1 Gb/s. Natomiast standard 1000BASE-T, lub inaczej IEEE 802.3ab używa kabli miedzianych o kategorii 5 lub wyższej.

Jak pokazano na rysunku, w technologiach 1000BASE-TX, 1000BASE-SX i 1000BASE-LX używane są te same parametry czasowe. Czas transmisji bitu wynosi 1 nanosekundę (0,000 000 001 sekundy) czyli 1 miliardową część sekundy. Format ramki sieci Gigabit Ethernet jest taki sam jak w sieciach Ethernet 10 Mb/s i 100 Mb/s. Sieci Gigabit Ethernet w zależności od implementacji mogą stosować różne metody zamiany ramek na bity przesypane w kablu.

Różnice między klasyczną technologią Ethernet, technologią Fast Ethernet i Gigabit Ethernet występują w warstwie fizycznej. Skrócony z powodu większej prędkości stosowanej w nowszych standardach czas transmisji bitu wymaga specjalnego traktowania. Ponieważ bity są przekazywane do medium w krótszym czasie i częściej, traktowanie staje się bardzo istotne. Transmisja o dużej prędkości wymaga częstotliwości bliskich wartościom krytycznym dla medium miedzianego. Powoduje to większą podatność bitów na szum w medium miedzianym.

## Przykłady architektur i maksymalnych długości kabli

Architektura	100BASE-TX	100BASE-FX	100BASE-TX i FX
Komputer-komputer, komputer-przełącznik, przełącznik-przełącznik (półduplek lub pełny duplex)	100 m	412 m	N/A
Jeden węzeł klasy I (półduplek)	200 m	272 m	100 m (TX) 160.8 m (FX)
Jeden węzeł klasy II (półduplek)	200 m	320 m	100 m (TX) 208 m (FX)
Dwa węzły klasy II (półduplek)	205 m	228 m	105 m (TX) 211.2 m (FX)

## Parametry pracy sieci Gigabit Ethernet

Parametr	Wartość
Typy sieci Ethernet	1 ns
Czas trwania szczeliny	Czas transmisji 4096 bitów
Przerwa międzyramkowa	96 bitów *
Limit prób po kolizji	16
Limit zwiększania okresu odczekiwania po kolizji	10
Rozmiar sekwencji zakłócającej	32 bity
Maksymalny rozmiar ramki bez znacznika VLAN	1518 oktetów
Minimalny rozmiar ramki	512 bitów (64 oktety)
Limit przesyłania w trybie wiązkowym	65 536 bitów

Ten problem wymagał wprowadzenia w sieciach Gigabit Ethernet dwóch oddzielnych etapów kodowania. Transmisja danych stała się bardziej efektywna dzięki wprowadzeniu kodów reprezentujących strumień bitów. Zakodowane dane umożliwiają synchronizację, efektywne wykorzystanie pasma oraz mają zwiększyony odstęp sygnału od szumu.

W warstwie fizycznej wzorce bitów z warstwy MAC są zamieniane na symbole. Symbolami mogą być także takie informacje sterujące, jak początek i koniec ramki lub znacznik wolnego medium. Podczas kodowania ramka jest zamieniana na symbole sterujące i symbole danych w celu zwiększenia przepustowości sieci.

W światłowodowych sieciach Gigabit Ethernet (standard 1000BASE-X) używane jest kodowanie 8B/10B, które jest podobne do kodowania 4B/5B. Następnie stosowany jest prosty kod liniowy NRZ (*Non-Return to Zero*), kodujący światło wprowadzane do włókna optycznego. Zastosowanie prostszego procesu kodowania jest możliwe dzięki temu, że światłowy może przenosić sygnały o szerszym paśmie.

## 7.2.2. 1000BASE-T

Instalacja sieci Fast Ethernet, mająca na celu zwiększenie szerokości pasma dostępnej dla stacji roboczych, spowodowała tworzenie wąskich gardeł po stronie dochodzącej sieci (upstream). Standard 1000BASE-T (IEEE 802.3ab) został utworzony w celu uzyskania dodatkowego pasma, które ułatwiłoby rozwiązywanie tego problemu. Standard ten umożliwiał osiągnięcie większej przepustowości w takich zastosowaniach, jak sieci szkieletowe wewnętrz budynków, łączące między przełącznikami, farmy serwerów oraz w przypadku innych funkcji wykonywanych przez węzły dystrybucji okablowania, jak również służył do połączeń wysokowydajnych stacji roboczych. Standard Fast Ethernet został zaprojektowany tak, aby mógł korzystać z istniejących kabli miedzianych kategorii 5, które spełniają wymagania dla kabli kategorii 5e. Większość zainstalowanych i poprawnie zakończonych kabli kategorii 5 może przejść certyfikację dla kabli kategorii 5e. Jedną z najważniejszych cech standardu 1000BASE-T jest możliwość współpracy ze standardami 10BASE-T i 100BASE-TX.

Ponieważ kabel kategorii 5e może niezawodnie przenosić dane z prędkością do 125 Mb/s, uzyskanie prędkości 1000 Mb/s (Gigabit) stanowiło wyzwanie dla tego projektu. Pierwszym krokiem na tej drodze było wykorzystanie wszystkich czterech par kabli zamiast tradycyjnych dwóch par, używanych w sieciach 10BASE-T i 100BASE-TX. Zostało to osiągnięte przy użyciu skomplikowanych układów, które umożliwiły transmisję pełnoduplexową na tej samej parze przewodów. Daje to prędkość 250 Mb/s na parę. Mając do dyspozycji cztery pary przewodów, możemy osiągnąć żądaną prędkość 1000 Mb/s. Ponieważ informacje są transmitowane jednocześnie czterema ścieżkami, układ sterujący nadajnika musi dzielić ramki, a odbiornika — składać je ponownie.

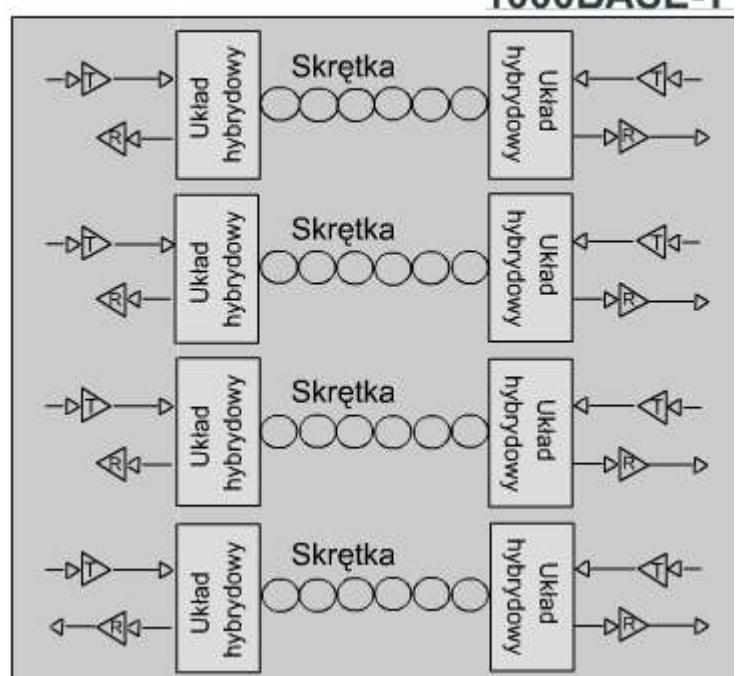
W przypadku skrętki nieekranowanej kategorii 5e lub lepszej stosowane jest kodowanie 1000BASE-T oraz kodowanie liniowe 4D-PAM5. Transmisja i odbiór danych występuje jednocześnie na tym samym przewodzie w obydwu kierunkach. Jak można oczekiwąć, prowadzi to do ciągłych kolizji na parach przewodów. W wyniku tych kolizji powstają skomplikowane sekwencje napięć.

Osiągnięcie przepustowości 1 Gb/s wymaga stosowania skomplikowanych zintegrowanych układów, używających takich technik, jak tłumienie echa, korekcja błędów FEC (*Forward Error Correction*) w warstwie pierwszej oraz odpowiedni dobór poziomów napięć.

W okresie nieaktywności w kablu występuje dziewięć poziomów napięć, a podczas transmisji danych — 17. Sygnał w przewodzie bardziej przypomina sygnał analogowy niż cyfrowy z powodu dużej liczby stanów i działania szumu. System ten, podobnie jak analogowy, jest bardziej podatny na szумy spowodowane przez kabel i problemy z zakończeniami kabla.

Dane ze stacji wysyłającej są starannie dzielone na cztery równoległe strumienie, następnie są kodowane, transmitowane i odbierane równolegle, po czym zostają złożone z powrotem w jeden strumień bitów. Na rysunku przedstawiono równoczesną pracę w pełnym dupleksie na czterech parach przewodów. Standard 1000BASE-T umożliwia działanie zarówno w półduplexie, jak i pełnym dupleksie. Powszechnie wykorzystywany jest tryb pełnego dupleksu standardu 1000BASE-T.

## Przebieg transmisji sygnału w sieci 1000BASE-T



### 7.2.3 Technologie 1000BASE-SX i LX

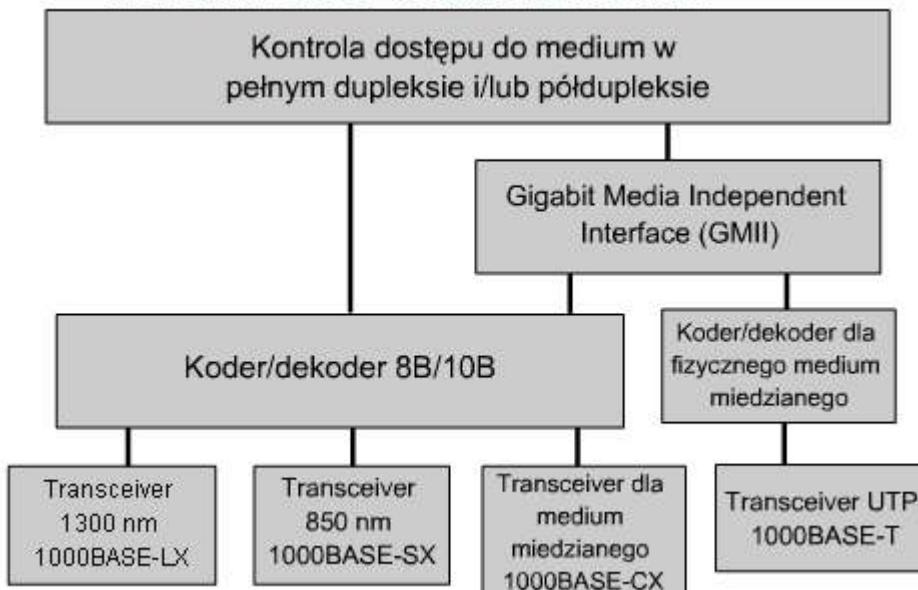
Standard IEEE 802.3 rekomenduje jako preferowaną technologię dla sieci szkieletowych światłowodową sieć Gigabit Ethernet.

Taktowanie, format ramki i transmisja są takie same we wszystkich wersjach sieci 1000 Mb/s. W warstwie fizycznej zdefiniowano dwa schematy kodowania sygnału.

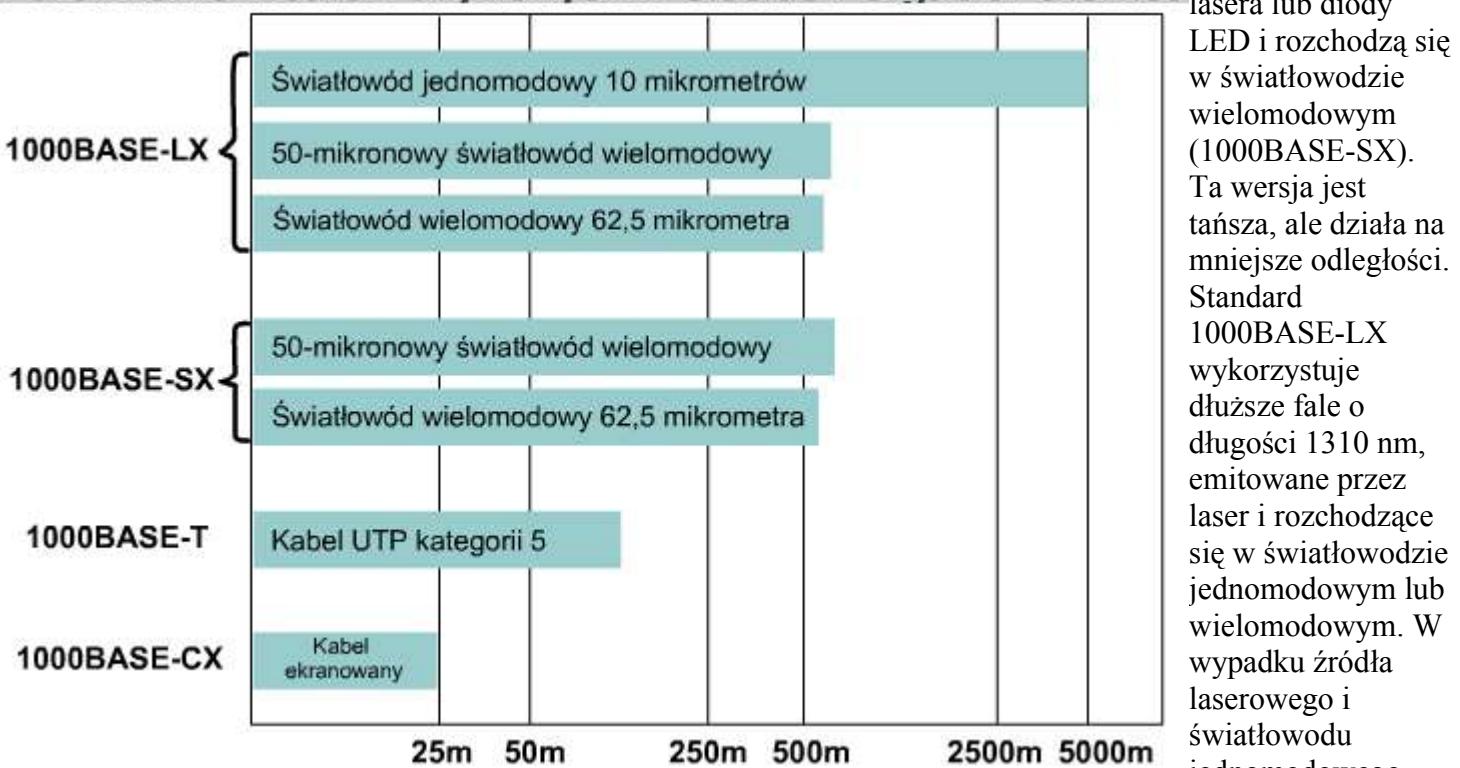
Kodowanie 8B/10B jest używane w światłowodach i ekranowanych mediach miedzianych, a modulacja amplitudy impulsów PAM5 (*Pulse Amplitude Modulation*) w skrótce nieekranowanej.

- Korzyści ze stosowania światłowodowej sieci Gigabit Ethernet**
- Odporność na szумy
  - Nie występują problemy z potencjałem uziemienia
  - Bardzo duży zasięg transmisji
  - Wiele dostępnych urządzeń 1000BASE-X
  - Może być użyty do łączenia rozproszonych segmentów sieci Fast Ethernet

#### Warstwy sieci Gigabit Ethernet



#### Porównanie mediów używanych w sieciach Gigabit Ethernet



można osiągnąć odległości do 5000 metrów. Ponieważ każdorazowe włączenie i wyłączenie diody LED lub lasera wymagałoby długiego czasu, światło jest emitowane z małą lub dużą mocą. Logiczne zero jest reprezentowane przez małą moc, a jedynka — przez dużą.

Metoda MAC traktuje takie łącze jako połączenie punkt-punkt. Ponieważ do transmisji (Tx) i odbioru (Rx) wykorzystywane są oddzielne włókna, transmisja jest z założenia pełnoduplexowa. Sieci Gigabit Ethernet

W standardzie 1000BASE-X stosowane jest kodowanie 8B/10B, po którym następuje kodowanie liniowe NRZ. Kodowanie NRZ do określenia wartości binarnej dla danego okresu bitu używa poziomu sygnału w oknie czasowym. W przeciwieństwie do innych opisanych schematów kodowania, ten system wykorzystuje poziomy sygnału, a nie zbocza. Oznacza to, że określenie, czy dany bit jest zerem, czy jedynką, następuje na podstawie poziomu sygnału, a nie wtedy, gdy sygnał zmienia poziomy.

Sygnały NRZ są następnie emitowane do włókna światłowodowego przy użyciu źródeł światła o dużej lub małej długości fali. Krótsze fale mają długość 850 nm, pochodzą z lasera lub diody LED i rozchodzą się w światłowodzie wielomodowym (1000BASE-SX).

Ta wersja jest tańsza, ale działa na mniejsze odległości. Standard 1000BASE-LX wykorzystuje dłuższe fale o długości 1310 nm, emitowane przez laser i rozchodzące się w światłowodzie jednomodowym lub wielomodowym. W wypadku źródła laserowego i światłowodu jednomodowego

pozwalały na zastosowanie tylko jednego węzła między dwiema stacjami. Na rysunku przedstawiono porównanie mediów dla sieci Ethernet 1000BASE.

#### 7.2.4 Architektura sieci Gigabit Ethernet

W łączach pełnodupleksowych odległość jest ograniczona wyłącznie właściwościami medium, a nie opóźnieniem w obie strony. Ponieważ większość sieci Gigabit Ethernet jest przełączana, wartości przedstawione na rysunkach i stanowią praktyczne ograniczenia łączy między urządzeniami. Dozwolone są topologie gwiazdy, rozszerzonej gwiazdy oraz połączenia łańcuchowe. Zagadnieniem ważniejszym niż ograniczenia dotyczące odległości i czasu staje się zatem wybór topologii logicznej i schematu przepływu danych.

W sieciach 1000BASE-T używana jest taka sama skrętka nieekranowana jak w sieciach 10BASE-T lub 100BASE-TX, ale łącze musi być wyższej jakości i spełniać wymogi kategorii 5e lub klasy D ISO (2000).

W sieci 1000BASE-T niepożądane są wszelkie modyfikacje reguł architektury. Przy odległości 100 metrów sieć 1000BASE-T pracuje na granicy możliwości odtworzenia przez sprzęt transmitowanego sygnału. Wszelkie problemy z okablowaniem lub szum w otoczeniu mogą spowodować, że nawet spełniający normy kabel nie umożliwi prawidłowej pracy na dystansie zgodnym ze specyfikacją.

Zaleca się, aby wszystkie łącza pomiędzy stacją a hubem lub przełącznikiem pracowały w trybie autonegocjacji, który pozwala osiągnąć najwyższą ogólną wydajność. Zapobiega to przypadkowym błędom konfiguracji innych parametrów, wymaganych do prawidłowego działania sieci Gigabit Ethernet.

#### Maksymalne długości kabli w sieci 1000BASE-SX

Medium	Przepustowość modalna	Odległość maksymalna
Światłowód wielomodowy 62,5 µm	160	220 m
Światłowód wielomodowy 62,5 µm	200	275 m
Światłowód wielomodowy 50 µm	400	500 m
Światłowód wielomodowy 50 µm	500	500 m

#### Maksymalne długości kabli w sieci 1000BASE-LX

Medium	Przepustowość modalna	Odległość maksymalna
Światłowód wielomodowy 62,5 µm	500	550 m
Światłowód wielomodowy 50 µm	400	550 m
Światłowód wielomodowy 50 µm	500	550 m
Światłowód jednomodowy 10 µm	N/A	5000 m

#### 7.2.5 Sieć 10 Gigabit Ethernet

Standard IEEE 802.3ae został zaadaptowany na potrzeby pełnodupleksowej transmisji przez światłowód z prędkością 10 Gb/s. Występują jednak duże podobieństwa między standardem 802.3ae a standardem oryginalnej sieci Ethernet 802.3. Standard 10 Gigabit Ethernet (10GbE) jest wykorzystywany nie tylko w sieciach LAN, ale i w sieciach MAN oraz WAN.

Dzięki temu samemu formatowi ramki oraz zgodności z poprzednimi standardami innych elementów specyfikacji warstwy 2 sieci Ethernet, standard 10GbE umożliwia korzystanie z szerszego pasma, zachowując przy tym możliwość współpracy z istniejącą infrastrukturą sieci.

Wraz z powstaniem technologii 10GbE nastąpiła poważna zmiana w koncepcji stosowania sieci Ethernet.

Technologia Ethernet tradycyjnie jest uważana za technologię sieci LAN, ale standardy warstwy fizycznej sieci 10GbE umożliwiają zarówno zwiększenie dystansu do 40 km przy użyciu światłowodu jednomodowego, jak również zapewniają zgodność z sieciami SONET (*Synchronous Optical Network*) oraz sieciami SDH (*Synchronous Digital Hierarchy*).

Możliwość pracy na odległość do 40 km powoduje, że technologia 10GbE jest technologią odpowiednią dla sieci MAN. Zgodność z sieciami SONET/SDH aż do poziomu OC-192 (prędkość do 9,534640 Gb/s) powoduje, że technologia 10GbE jest technologią odpowiednią dla sieci WAN. Technologia 10GbE może także w pewnych zastosowaniach rywalizować z technologią ATM.

Podsumowując zastanówmy się, jakie są podobieństwa i różnice między sieciami 10GbE a innymi wersjami sieci Ethernet.

Format ramki jest taki sam, co pozwala na współpracę bez ponownego podziału na ramki lub konwersji protokołu pomiędzy wszystkimi odmianami tych sieci: klasyczną, Fast, Gigabit Ethernet i 10 Gigabit Ethernet. Czas transmisji bitu wynosi 0,1 nanosekundy. Pozostałe parametry czasowe są odpowiednio przeskalowane. Ponieważ używane są jedynie światłowodowe połączenia pełnodupleksowe, nie ma potrzeby korzystania z technologii CSMA/CD.

Podwarstwy standardu 802.3 należące do warstw 1 i 2 modelu OSI są w większości zachowane, z kilkoma dodatkami umożliwiającymi pracę z łączami światłowodowymi o długości 40 km oraz współpracę z technologiami SONET/SDH.

Możliwe jest tworzenie elastycznych, efektywnych, niezawodnych i względnie tanich sieci Ethernet typu end-to-end.

Można używać protokołu TCP/IP w sieciach LAN, MAN i WAN, korzystając tylko z jednej metody transportu w warstwie 2.

Podstawowym standardem technologii CSMA/CD jest standard IEEE 802.3. Suplement do tego standardu (zatytułowany 802.3ae) opisuje rodzinę technologii 10GbE. Jak zwykle w wypadku nowych technologii, rozważane są różne implementacje, między innymi następujące:

**10GBASE-SR:** przeznaczona do pracy na krótkich odległościach (od 26 m do 82 m) w istniejących już światłowodach wielomodowych;

**10GBASE-LX4:** używa technologii WDM (*Wavelength Division Multiplexing*), umożliwia pracę na odległościach od 240 m do 300 m na zainstalowanych już wielomodowych łączach światłowodowych oraz na odległościach do 10 km w światłowodach jednomodowych;

**10GBASE-LR i 10GBASE-ER:** umożliwia pracę na odległości 10 km i 40 km przy użyciu światłowodu jednomodowego;

**10GBASE-SW, 10GBASE-LW i 10GBASE-EW:** znane pod wspólną nazwą 10GBASE-W i przeznaczone do pracy w sieciach SONET/SDH WAN opartych na standardzie STM (*Synchronous Transport Module*) OC-192.

Grupa zadaniowa IEEE 802.3ae i organizacja 10-Gigabit Ethernet Alliance (10 GEA) opracowują standardy dla tych powstających technologii.

Technologia Ethernet 10 Gb/s (IEEE 802.3ae) stała się standardem w czerwcu 2002 roku. Jest to pełnodupleksowy protokół, dla którego jedynym medium jest światłowód. Maksymalna odległość transmisji zależy od rodzaju używanego światłowodu. Przy użyciu jako medium światłowodu jednomodowego maksymalna odległość wynosi 40 kilometrów (25 mil). Członkowie organizacji IEEE rozpoczęli dyskusje, w trakcie których zasugerowano możliwość utworzenia standardów sieci Ethernet o prędkościach 40, 80 lub nawet 100 Gb/s.

## Parametry pracy sieci 10 Gigabit Ethernet

Parametr	Wartość
Czas transmisji bitu	0,1 nsec
Czas trwania szczeliny	nie ma zastosowania *
Przerwa międzyramkowa	96 bitów **
Limit prób po kolizji	nie ma zastosowania *
Limit zwiększania okresu odczekiwania po kolizji	nie ma zastosowania *
Rozmiar sekwencji zakłócającej	nie ma zastosowania *
Maksymalny rozmiar ramki bez znacznika VLAN	1518 oktetów
Minimalny rozmiar ramki	512 bitów (64 oktety)
Limit przesyłania w trybie wiązkowym	nie ma zastosowania *
Stopień rozszerzenia przerw międzyramkowych	104 bity***

\* W sieci 10 Gigabit Ethernet nie jest możliwa praca w półdupleksie, zatem nie mają zastosowania parametry związane z czasem trwania szczeliny i obsługą kolizji. \*\* Podana wartość jest standardową przerwą międzyramkową. \*\*\* Stopień rozszerzania przerw międzyramkowych dotyczy wyłącznie definicji sieci 10GBASE-W.

### 7.2.6 Architektury sieci 10 Gigabit Ethernet

Podobnie jak w wypadku sieci Gigabit Ethernet, zwiększenie szybkości wprowadza dodatkowe wymagania. Skrócony z powodu większej prędkości czas transmisji bitu wymaga specjalnego traktowania. Podczas transmisji w sieci 10GbE czas trwania każdego bitu wynosi 0,1 nanosekundy. Oznacza to, że w czasie potrzebnym do przesyłania jednego bitu danych w sieci Ethernet 10 Mb/s zostanie przesłanych 1000 bitów danych w sieci 10GbE. Z powodu krótkiego okresu bitu w sieci 10GbE trudno zazwyczaj wyróżnić bit danych spośród szumu.

Transmisja w sieci 10GbE jest uzależniona od dokładnego taktowania, które umożliwia oddzielenie danych od efektów szumu w warstwie fizycznej. Taki jest cel synchronizacji.

W celu rozwiązywania problemów związanych z synchronizacją, pasmem i odstępem sygnału od szumu, sieci 10 Gigabit Ethernet używają dwóch oddzielnych etapów kodowania. Transmisja jest bardziej efektywna dzięki użyciu kodów reprezentujących dane użytkownika. Zakodowane dane umożliwiają synchronizację, efektywne wykorzystanie pasma oraz mają zwiększyony odstęp sygnału od szumu.

We wszystkich wersjach sieci 10GbE (oprócz 10GBASE-LX4) używane są złożone szeregowe strumienie bitów. W sieciach 10GBASE-LX4 wykorzystywana jest technika WWDM (*Wide Wavelength Division Multiplex*), która pozwala na jednoczesne multipleksowanie czterech strumieni bitów, gdyż do światłowodu wprowadzane jest światło o czterech długościach fal.

Na rysunku przedstawiono szczególny przypadek użycia czterech laserów o nieco różniących się długościach fal. Podeczas odbierania sygnału z medium strumień światła jest demultipleksowany na cztery oddzielne strumienie sygnału optycznego. Te cztery strumienie sygnału optycznego są następnie zamieniane na cztery strumienie elektryczne i poddawane odwrotnemu procesowi, w miarę przechodzenia do coraz wyższych podwarstw warstwy MAC.

Aktualnie większość produktów w technologii 10GbE jest dostępna w formie modułów lub kart linii dla wysokowydajnych przełączników i routerów.

Można oczekwać, że wraz z rozwojem technologii 10GbE pojawi się większa liczba różnych urządzeń. W miarę jak technologie optyczne będą ewoluowały do produktów tych zostaną dołączone ulepszone nadajniki i odbiorniki, które pozwolą jeszcze lepiej wykorzystać ich modułowość.

Wszystkie odmiany sieci 10GbE korzystają ze światłowodów jako mediów.

Wykorzystywane są światłowody jednomodowe

10 μm oraz wielomodowe 50 μm i 62,5 μm. Dopuszczalne jest używanie światłowodów o różnych charakterystykach dyspersji i tłumienia, ale ogranicza to możliwą długość sieci.

Chociaż w tej technologii wykorzystywane są wyłącznie światłowody, niektóre maksymalne długości kabli są zaskakująco niewielkie. Dla sieci 10 Gigabit Ethernet nie zdefiniowano wtórnika, ponieważ nie jest obsługiwany tryb półduplexu.

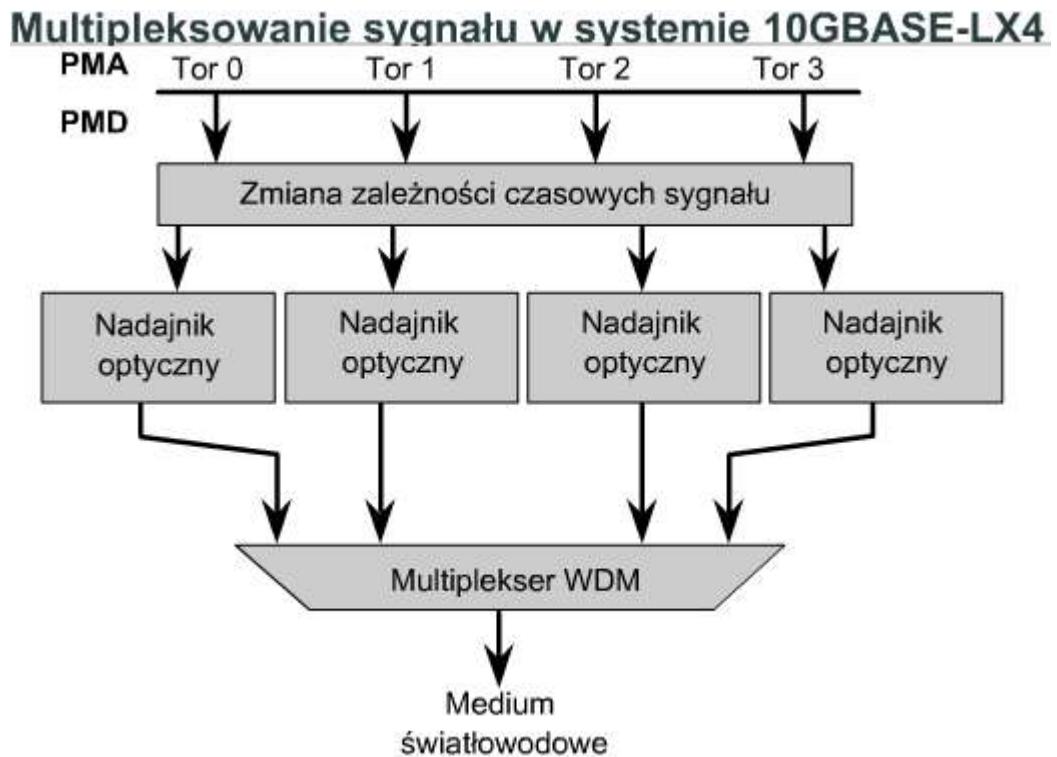
Podobnie jak w wersji 10 Mb/s, 100 Mb/s i 1000 Mb/s, tutaj także można w niewielkim stopniu modyfikować niektóre reguły architektury. Możliwe zmiany dotyczą strat sygnału i zniekształceń w medium. Z powodu dyspersji sygnału i innych zjawisk sygnał świetlny jest niemożliwy do odczytania po przebyciu pewnej odległości.

## 7.2.7 Przyszłość technologii Ethernet

Ewolucja sieci Ethernet wyglądała następująco: sieci klasyczne → Fast → Gigabit → technologie wielogigabitowe. Chociaż inne technologie sieci LAN nadal są używane w starszych instalacjach, w nowych instalacjach sieci LAN dominuje technologia Ethernet. Dominacja tej technologii osiągnęła takie rozmiary, że Ethernet jest uważany przez niektórych za podstawowy protokół sieci LAN. Technologia Ethernet jest aktualnie standardem dla połączeń poziomych, pionowych oraz połączeń między budynkami. Nowo powstające wersje technologii Ethernet powodują zatarcie różnic pomiędzy sieciami LAN, MAN i WAN.

Obecnie, gdy sieci 1 Gigabit Ethernet są powszechnie dostępne, a produkty 10 Gigabit Ethernet zaczynają powoli wchodzić na rynek, organizacje IEEE oraz 10-Gigabit Ethernet Alliance pracują nad standardami 40 Gb/s, 100 Gb/s i nawet 160 Gb/s. To, które technologie zostaną przyjęte, zależy od wielu czynników, między innymi dojrzałości tych technologii i standardów, ich przyjęcia przez rynek oraz kosztów.

Dla sieci Ethernet zaproponowano inne niż CSMA/CD schematy arbitrażu. Zniknął problem kolizji występujący w fizycznych topologiach magistrali 10BASE5 i 10BASE2 oraz hubów 10BASE-T i 100BASE-TX. Używanie



skrętki nieekranowanej lub światłowodów z oddzielnymi ścieżkami Tx i Rx oraz malejący koszt przełączników spowodował, że połączenia półdupleksowe na współdzielonym medium bardzo straciły na znaczeniu.

### **Przyszłość mediów sieciowych zależy od ich rodzajów:**

Miedziane (do 1000 Mb/s, możliwe, że więcej).

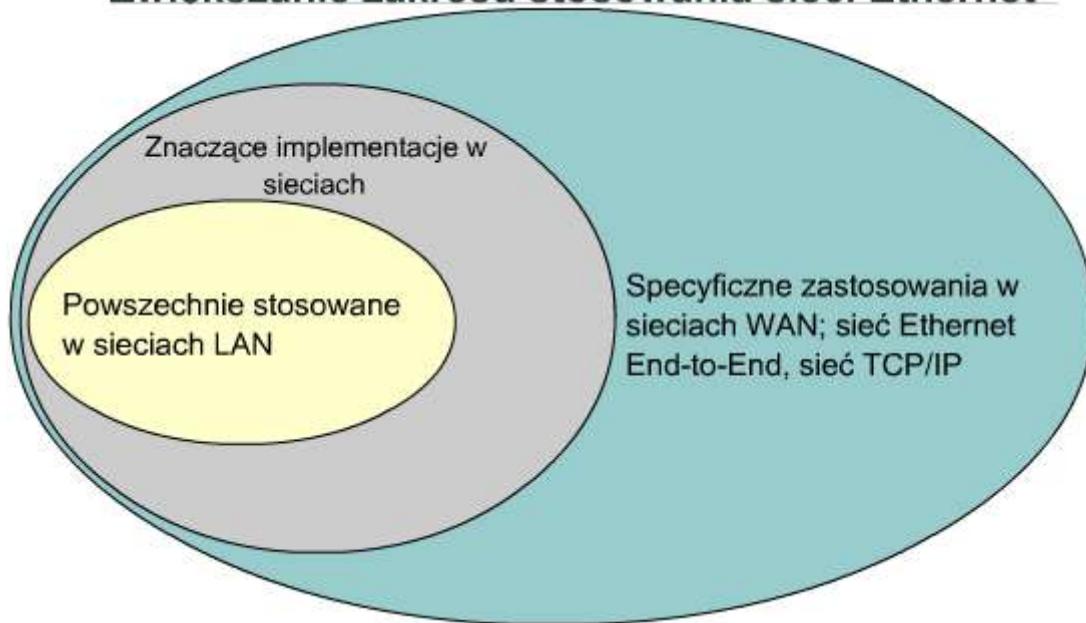
Bezprzewodowe (zbliżają się do 100 Mb/s, możliwe, że więcej).

Światłowody (aktualnie 10 000 Mb/s, a wkrótce więcej).

W mediach miedzianych i bezprzewodowych występują pewne ograniczenia fizyczne i praktyczne wpływające na najwyższą możliwą do przeniesienia częstotliwość sygnału. W przewidywanej przyszłości nie będzie to stanowiło ograniczenia dla światłowodów. Limit szerokości pasma dla światłowodu jest bardzo duży i na razie nie stanowi problemu. W systemach światłowodowych czynnikiem ograniczającym szybkość jest technologia elektroniczna (nadajniki i odbiorniki) oraz proces wytwarzania włókien optycznych. Prawdopodobnie nadchodzące udoskonalenia sieci Ethernet będą ukierunkowane na wykorzystanie źródeł laserowych i światłowodów jednomodowych. W czasach, gdy sieć Ethernet była powolna, działała w trybie półdupleksu, występowali w niej kolizje, a ustalanie priorytetów było procesem „demokratycznym”, nie rozważano potrzeby wprowadzenia usługi QoS (*Quality of Service*) dla obsługi wybranych rodzajów danych. Takimi danymi są rozmowy telefoniczne IP oraz rozgłaszone transmisje wideo.

Dominujące obecnie na rynku szybkie i pełnodupleksowe technologie Ethernet umożliwiają pracę nawet przy zastosowaniach korzystających z mechanizmu jakości usług QoS. Zwiększa to obszar możliwych zastosowań sieci Ethernet. Zakrawa na paradoks, że choć możliwość użycia mechanizmów QoS w połączeniach typu end-to-end spowodowała wprowadzenie technologii ATM w sieciach WAN i stacjach roboczych w połowie lat dziewięćdziesiątych, to właśnie sieci Ethernet, a nie ATM, zaczynają spełniać te wymagania.

### **Zwiększenie zakresu stosowania sieci Ethernet**



## Moduł 8. Przełączanie w sieciach Ethernet

Współdzielona sieć Ethernet w idealnych warunkach sprawuje się doskonale. Kiedy liczba urządzeń próbujących uzyskać dostęp do sieci jest niewielka, liczba kolizji utrzymuje się w akceptowalnych granicach. Jednakże gdy w sieci przybywa użytkowników, zwiększa się liczba kolizji, co doprowadzić do nadmiernego spadku wydajności. Aby pomóc ograniczyć skalę problemów wydajnościowych wynikających ze zwiększonej liczby kolizji, opracowano mechanizmy mostowania. Rozwój mechanizmów mostowania doprowadził do powstania techniki przełączania, która stała się kluczową technologią w nowoczesnych lokalnych sieciach Ethernet.

Zjawiska kolizji i rozgłaszenia są naturalnymi elementami współczesnych sieci komputerowych. W rzeczywistości są one częścią sieci Ethernet oraz technologii wyższych warstw. Jednak gdy ilość tych zjawisk przekracza wartość optymalną, wydajność sieci spada. Idea domen kolizyjnych i rozgłoszeniowych dotyczy określenia takich sposobów projektowania sieci, które pozwalają na ograniczenie negatywnych efektów kolizji i rozgłaszenia. W tym module zajmujemy się wpływem kolizji i rozgłaszenia na ruch w sieci, a także opiszymy sposoby wykorzystania mostów i routerów do segmentowania sieci w celu uzyskania lepszej wydajności.

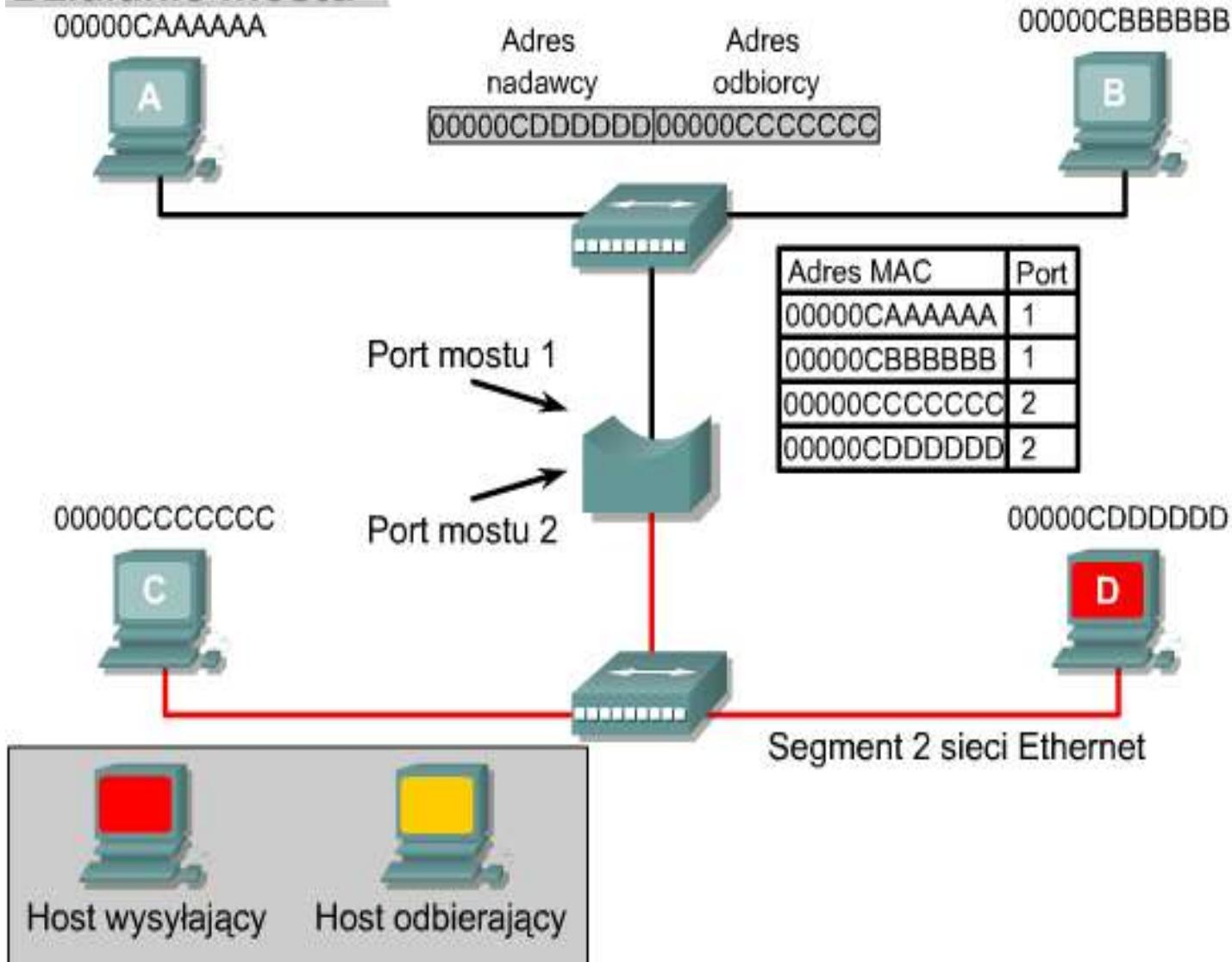
### 8.1 Przełączanie w sieciach Ethernet

#### 8.1.1 Mostowanie w warstwie 2

Gdy do fizycznego segmentu sieci Ethernet zostaje dodana większa liczba węzłów, wzrasta rywalizacja o dostęp do medium. Sieć Ethernet jest medium wspólnym, co oznacza, że w danym momencie może nadawać tylko jeden węzeł. Dodawanie kolejnych węzłów zwiększa wymagania dotyczące dostępnego pasma oraz dodatkowo obciąża medium. Wzrost liczby węzłów w pojedynczym segmencie zwiększa prawdopodobieństwo wystąpienia kolizji, co prowadzi do częstszych retransmisji. Problem ten można rozwiązać przez podzielenie jednego dużego segmentu na części stanowiące odrębne domeny kolizyjne.

Aby było to możliwe, most przechowuje tablicę adresów MAC oraz przypisanych im portów. Most przekazuje lub odrzuca ramki w oparciu o wpisy w tabeli.

### Działanie mostu



### Poniższa procedura ilustruje działanie mostu:

- Po uruchomieniu mostu jego tablica jest pusta. Most oczekuje na pojawienie się ruchu w segmencie. Wykryty ruch jest obsługiwany przez most.
- Host A wysyła pakiety ping do hosta B. Ponieważ dane transmitowane są w całym segmencie domeny kolizyjnej, zarówno host B, jak i most przetwarzają pakiety.
- Adres nadawcy ramki zostaje dodany do tablicy mostu. Ponieważ adres znajduje się w polu adresu nadawcy, a ramka została odebrana na porcie nr 1, musi być ona skojarzona w tablicy z portem nr 1.
- W tablicy mostu poszukiwany jest adres odbiorcy. Ponieważ adresu nie ma w tablicy, mimo że znajduje się on w tej samej domenie kolizyjnej, ramka jest przekazywana do innego segmentu. Adres hosta B nie został jeszcze zapisany, ponieważ zapamiętywany jest jedynie adres nadawcy.
- Host B przetwarza żądanu ping i wysyła odpowiedź ping do hosta A. Dane są przesyłane przez całą domenę kolizyjną. Zarówno host A, jak i most odbierają i przetwarzają ramkę.
- Adres nadawcy ramki zostaje dodany do tablicy mostu. Ponieważ tablica mostu nie zawiera adresu nadawcy, a został on odebrany na porcie 1, adres nadawcy ramki musi być skojarzony z portem 1 w tablicy. W celu odnalezienia pozycji zawierającej adres odbiorcy ramki przeszukiwana jest tablica mostu. Ponieważ adres znajduje się w tablicy, odszukany zostaje odpowiadający mu port. Adres hosta A zostaje skojarzony z portem, na który została wysłana ramka, więc nie jest ona dalej przekazywana.
- Host A wysyła teraz pakiety ping do hosta C. Ponieważ dane są transmitowane w całej domenie kolizyjnej, zarówno most, jak i host B przetwarzają ramkę. Ramka zostaje odrzucona przez hosta B, ponieważ nie była do niego kierowana.
- Adres nadawcy ramki zostaje dodany do tablicy mostu. Ponieważ adres jest już zapisany w tablicy mostu, pozycja jest jedynie odświeżana.
- Tablica mostu jest przeszukiwana w celu odnalezienia pozycji zawierającej adres odbiorcy ramki. Ponieważ adresu nie ma w tablicy, ramka jest przekazywana do innego segmentu. Adres hosta C nie został jeszcze zapisany, gdyż zapamiętywany jest jedynie adres nadawcy.
- Host C przetwarza żądanu ping i wysyła odpowiedź ping do hosta A. Dane są przesyłane przez całą domenę kolizyjną. Zarówno host D, jak i most otrzymują i przetwarzają ramkę. Ramka zostaje odrzucona przez hosta D, ponieważ nie była do niego kierowana.
- Adres nadawcy ramki zostaje dodany do tablicy mostu. Ponieważ adres znajduje się w polu adresu nadawcy, a ramka zostaje odebrana na porcie nr 2, musi być ona skojarzona w tablicy z portem nr 2.
- Tablica mostu jest przeszukiwana w celu odnalezienia pozycji zawierającej adres odbiorcy ramki. Adres znajduje się w tablicy, lecz jest on skojarzony z portem 1, więc ramka jest przekazywana do innego segmentu.
- Gdy host D transmisuje dane, jego adres MAC zostaje również zapisany w tablicy mostu. W ten sposób most kontroluje ruch pomiędzy domenami kolizyjnymi.

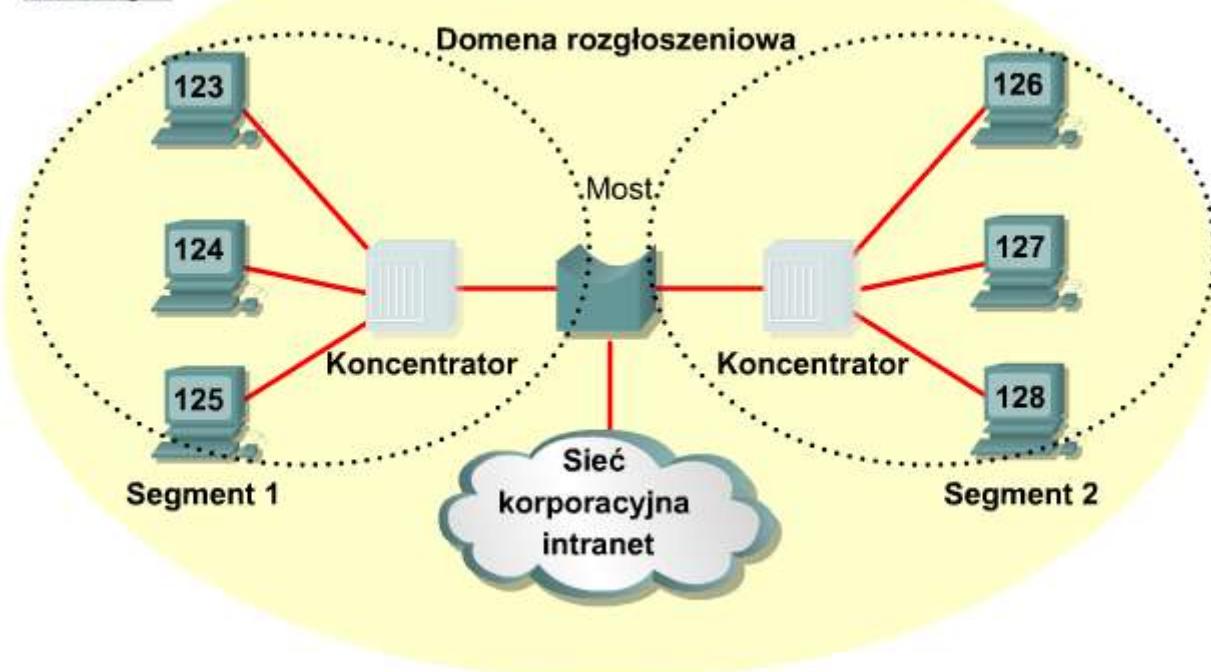
Są to operacje, jakie podejmuje most w celu przekazywania i odrzucania ramek, które są odbierane na dowolnym z jego portów.

#### 8.1.2 Przełączanie w warstwie 2

Zasadniczo most zawiera tylko dwa porty i rozdziela domenę kolizyjną na dwie części. Wszystkie wybory dokonywane przez most opierają się na adresach MAC lub inaczej adresowaniu w warstwie 2 i nie wpływają na adresowanie logiczne zwane także adresowaniem w warstwie 3. Tak więc most dzieli domenę kolizyjną, nie wpływając przy tym na domenę logiczną lub rozgłoszeniową. Niezależnie od liczby mostów w sieci cała sieć będzie współdzieliła tę samą logiczną przestrzeń adresową (o ile nie ma w niej urządzenia korzystającego z procesu adresowania w warstwie 3, takiego jak router). Most utworzy dodatkowe domeny kolizyjne, nie zwiększając jednak liczby domen rozgłoszeniowych.

W istocie przełącznik jest szybkim, wieloportowym mostem mogącym zawierać dziesiątki portów. W przeciwnieństwie do mostu, który powoduje powstanie dwóch domen kolizyjnych, w tym przypadku osobna domena kolizyjna jest tworzona w obrębie każdego z portów. W sieci składającej się z dwudziestu węzłów istnieje dwadzieścia domen kolizyjnych, jeśli każdy węzeł jest podłączony do innego portu przełącznika. Przy uwzględnieniu portu połączenia nadzawanego (uplink) pojedynczy przełącznik tworzy dwadzieścia jeden domen kolizyjnych, z których każda zawiera jeden węzeł. Przełącznik dynamicznie tworzy i utrzymuje tablicę pamięci asocjacyjnej (CAM, ang. *Content-Addressable Memory*), przechowując dla każdego portu wszystkie niezbędne informacje dotyczące adresów MAC.

## Mosty

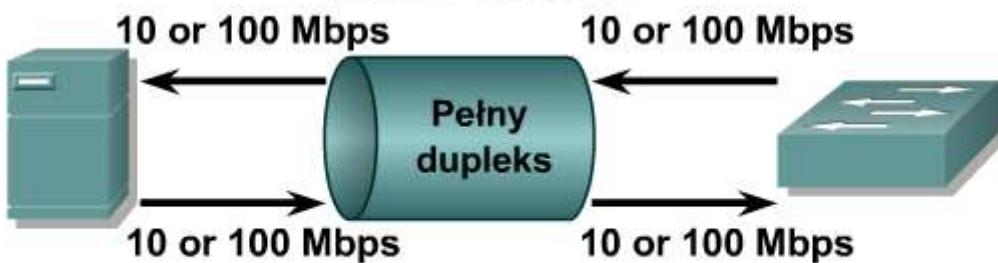


### **8.1.3 Działanie przełącznika**

Przełącznik jest po prostu mostem z wieloma portami. Gdy do portu przełącznika jest podłączony tylko jeden host, domena kolizyjna na medium współdzielonym składa się jedynie z dwóch elementów: portu przełącznika i dołączonego do niego hosta. Każdy z dwóch węzłów w tym małym segmencie (domenie kolizyjnej) składa się z portu przełącznika oraz hosta podłączonego do niego. Takie małe segmenty fizyczne zwane są mikrosegmentami. W sytuacji, gdy podłączone są tylko dwa węzły, pojawia się dodatkowa możliwość. W sieci wykorzystującej skrótkę jedna para przewodów używana jest do przenoszenia transmitowanego sygnału z jednego węzła do drugiego. Oddzienna para jest wykorzystywana do odbioru lub przekazywania sygnału zwrotnego. Możliwe jest przesyłanie sygnałów w obydwu kierunkach równocześnie. Zdolność komunikowania się w obydwu kierunkach równocześnie określana jest jako pełny dupleks. Większość przełączników i kart sieciowych obsługuje komunikację w trybie pełnego dupleksu. W trybie tym nie występuje rywalizacja o dostęp do medium. W związku z tym pojęcie domeny kolizyjnej przestaje istnieć. Teoretycznie w trybie pełnego dupleksu szerokość pasma zostaje podwojona.

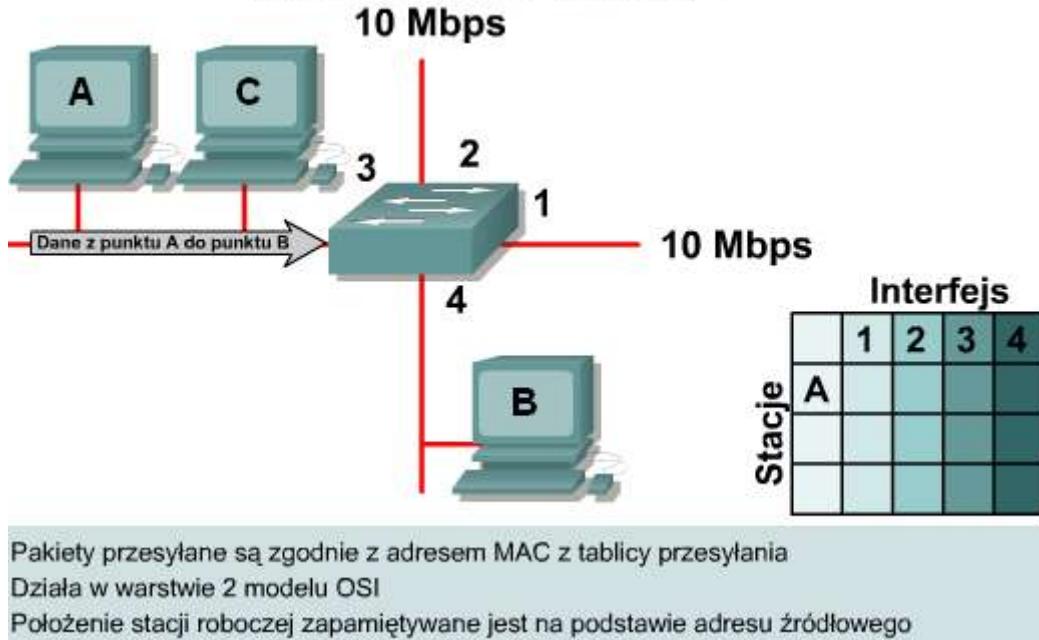
Oprócz szybszych mikroprocesorów i pamięci, opracowanie przełączników umożliwiły dwie inne innowacje technologiczne. Pamięć asocjacyjna (CAM) działa odwrotnie niż pamięć tradycyjna. Wprowadzenie danych do pamięci spowoduje zwrot skojarzonego z nimi adresu. Wykorzystanie pamięci asocjacyjnych (CAM) pozwala przełącznikowi na bezpośrednie odnalezienie portu skojarzonego z adresem MAC bez konieczności wykorzystywania algorytmów wyszukiwania. Układ ASIC (ang. *Application-Specific Integrated Circuit*) jest urządzeniem składającym się z bramek logicznych o nieprzypisanych funkcjach, które mogą zostać zaprogramowane tak, aby realizować operacje z prędkością układów logicznych. Działania, które wcześniej mogły być realizowane programowo, teraz mogą być wykonywane sprzętowo z wykorzystaniem układów ASIC. Wykorzystanie tych technologii w znaczący sposób zredukowało opóźnienia wprowadzane przez oprogramowanie oraz pozwoliło dotrzymać kroku zapotrzebowaniu wielu mikrosegmentów na dane oraz sprostać dużym szybkościom bitowym.

#### Pełny dupleks



- Szerokość pasma pomiędzy węzłami jest dwukrotnie większa
- Transmisja wolna od kolizji
- Dwie ścieżki danych o przepustowości 10 lub 100 Mb/s

## Działanie przełącznika



### 8.1.4 Opóźnienie

Opóźnienie to różnica pomiędzy czasem, kiedy urządzenie nadawcze rozpoczęta wysyłanie ramki, a czasem, gdy jej początkowa część osiągnie swój cel. Opóźnienie ramki przesyłanej pomiędzy źródłem i miejscem docelowym może być spowodowane przez wiele różnych czynników:

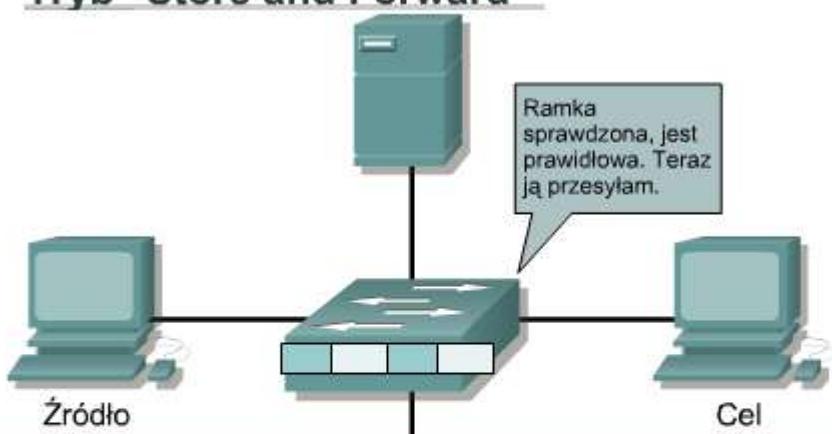
- Opóźnienia medium spowodowane skończoną prędkością, z jaką może poruszać się sygnał w medium fizycznym.
- Opóźnienia obwodów wnoszone przez układy elektroniczne przetwarzające sygnał na jego drodze.
- Opóźnienia programowe powodowane przez procesy decyzyjne realizowane przez oprogramowanie w celu implementacji funkcji przełączania i obsługi protokołów.
- Opóźnienia powodowane przez zawartość ramki oraz miejsce w obrębie ramki objęte procesami decyzyjnymi dotyczącymi przełączania. Na przykład urządzenie nie może skierować ramki do portu docelowego, dopóki nie zostanie odczytany adres MAC odbiorcy.

### 8.1.5 Tryby przełączania

Sposób przełączania ramki do portu docelowego stanowi rozwiązań kompromisowe między wartością opóźnienia i niezawodnością. Przełącznik może zacząć przesyłać ramkę zaraz po otrzymaniu adresu MAC odbiorcy. Taki sposób przełączania nazywany jest przełączaniem „cut-through”.

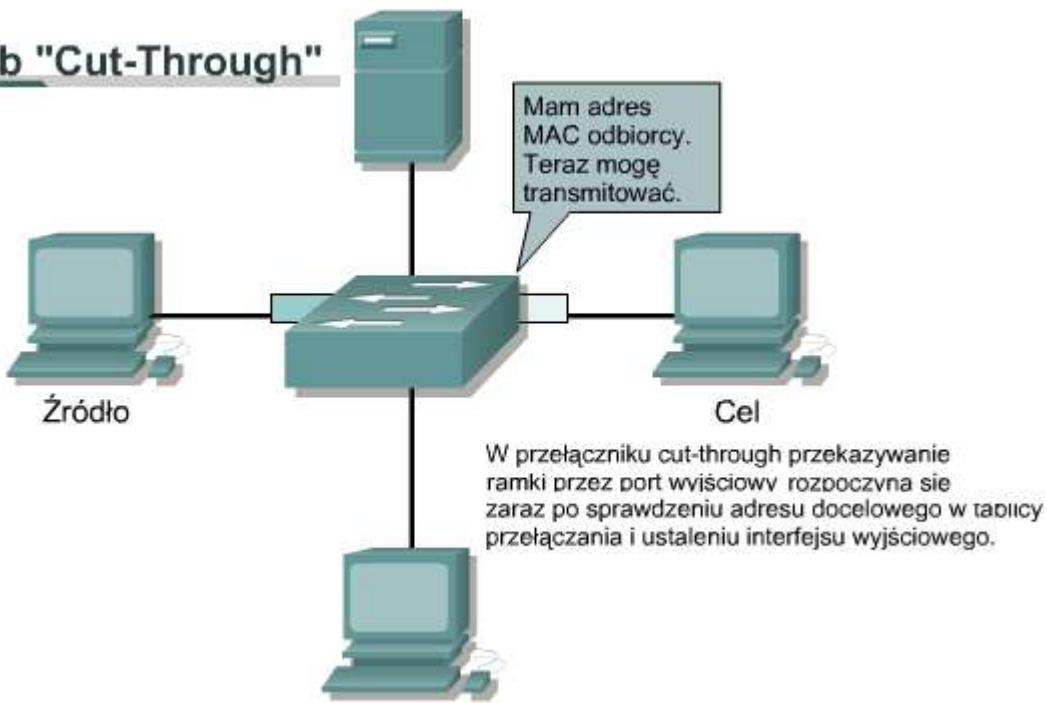
Charakteryzuje się on najmniejszym opóźnieniem. Jednak w tym przypadku wykrywanie błędów nie jest możliwe. Z drugiej strony, przełącznik może odebrać całą ramkę przed przesłaniem jej dalej przez port docelowy. W tej sytuacji przed wysłaniem ramki do punktu docelowego istnieje możliwość sprawdzenia kodu kontrolnego ramki (FCS) przez oprogramowanie przełącznika. Można w ten sposób upewnić się, że ramka została poprawnie odebrana. W przypadku wykrycia błędu odrzucenie ramki jest realizowane przez przełącznik, a nie przez komputer docelowy. Ponieważ przed przekazaniem cała zawartość ramki jest przechowywana w pamięci, ten tryb określa się mianem „store-and-forward” (zachowaj i przekaż). Tryb „fragment-free” stanowi kompromis pomiędzy metodami „cut-through” i „store-and-forward”. W przypadku metody „fragment-free” odbierane są pierwsze 64 bajty zawierające nagłówek ramki, przełączanie rozpoczyna się zanim zostanie odebrane pole danych i suma kontrolna. W trybie tym weryfikowana jest poprawność adresowania oraz informacji

### Tryb "Store and Forward"



W przypadku przełącznika store and forward kopiwana jest cała ramka, obliczana jest wartość cyklicznej kontroli nadmiarowej (CRC, Cyclic Redundancy Check) i sprawdzana jest długość ramki. Jeśli wartość CRC oraz długość ramki są poprawne, w tabeli przełącznika wyszukiwany jest adres odbiorcy, ustalany jest interfejs wyjściowy, a następnie ramka jest przekazywana w miejsce docelowe.

## Tryb "Cut-Through"



protokołu LLC (Logical Link Control) w celu zapewnienia, że przetwarzanie danych oraz informacje określające punkt docelowy będą prawidłowe. Gdy do przełączania używana jest metoda „cut-through”, zarówno port źródłowy, jak i port docelowy muszą pracować z tą samą szybkością bitową, aby nie uszkodzić ramki. Przełączanie takie określa się mianem symetrycznego. Jeżeli szybkości bitowe są

różne, ramka musi być zapisana z jedną szybkością, a następnie wysłana z inną. Ten typ przełączania określa się mianem asymetrycznego. Do przełączania asymetrycznego musi być wykorzystywany tryb „store-and-forward”. Przełączanie asymetryczne zapewnia połączenia komutowane pomiędzy portami o różnych szerokościach pasma, na przykład 100 Mb/s i 1000 Mb/s. Przełączanie asymetryczne jest zoptymalizowane pod kątem ruchu generowanego przez połączenia typu klient-serwer, gdzie wiele klientów jednocześnie komunikuje się z serwerem, co wymaga zapewnienia szerszego pasa po stronie portu serwera w celu ograniczenia możliwości powstania wąskiego gardła w tym punkcie.

### 8.1.6 Protokół drzewa opinającego

Gdy wiele przełączników połączonych jest w ramach jednej struktury drzewiastej, wystąpienie pętli przełączania jest mało prawdopodobne. Jednak sieci komutowane są zwykle zaprojektowane tak, aby zapewnić ścieżki nadmiarowe, co ma gwarantować niezawodność i odporność na błędy. Występowanie ścieżek nadmiarowych jest pomocne, jednak zastosowanie ich może nieść za sobą niepożądane efekty uboczne. Pętla przełączania jest jednym z takich efektów. Pętla przełączania może wystąpić przez przypadek lub być konsekwencją świadomego działania. Może ona doprowadzić do burzy rozgłoszeń, która gwałtownie obejmie całą sieć. Aby zapobiec możliwości powstania pętli, przełączniki wyposażone są w oparty na standardach protokół drzewa opinającego (STP). Każdy przełącznik w sieci LAN, który wykorzystuje protokół drzewa opinającego (STP), wysyła przez każdy swój port specjalne komunikaty zwane jednostkami BPDU (ang. Bridge Protocol Data Unit), aby zakomunikować innym przełącznikom swoją obecność i umożliwić wybór mostu głównego sieci. Następnie przełączniki wykorzystują algorytm drzewa opinającego w celu identyfikacji i zamknięcia ścieżek nadmiarowych.

**Każdy port przełącznika używającego algorytmu drzewa opinającego znajduje się w jednym z pięciu stanów:**

**Blokowanie Nasłuch Zapamiętywanie Przesyłanie Wyłączony**

Stany STP	Cel
Blokowanie	Otrzymywanie jednostek BPDU
Nasłuch	Tworzenie aktywnej topologii
Zapamiętywanie	Tworzenie tablicy mostowania
Przekazywanie	Wysyłanie i odbiór danych użytkowych
Wyłączony	Wyłączony administracyjnie

**Port może przechodzić z jednego stanu do innego w następujących cyklach:**

\* od inicjacji do blokowania

\* od blokowania do nasłuchu lub zablokowania

\* od nasłuchu do zapamiętywania lub zablokowania

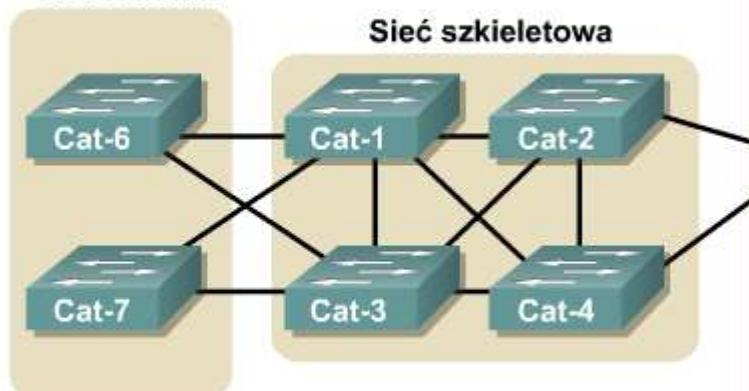
\* od zapamiętywania do przesyłania lub zablokowania

\* od przesyłania do zablokowania

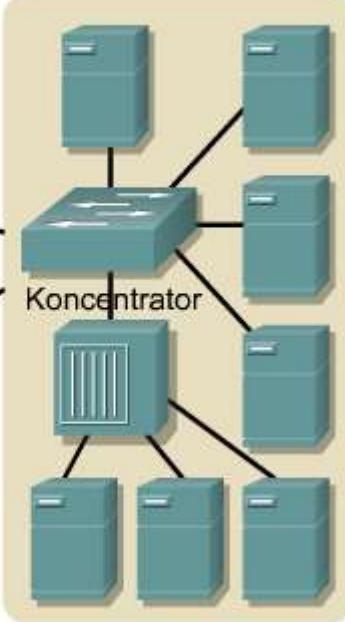
Wynikiem zidentyfikowania i wyeliminowania pętli z wykorzystaniem protokołu STP jest powstanie hierarchicznej struktury drzewiastej wolnej od zapętleń. Alternatywne ścieżki są jednak w dalszym ciągu dostępne i mogą być wykorzystane w razie potrzeby.

## Działanie drzewa opinającego

Węzeł dystrybucji okablowania



Farma serwerów



## 8.2 Domena kolizyjna i domena rozgłoszeniowa

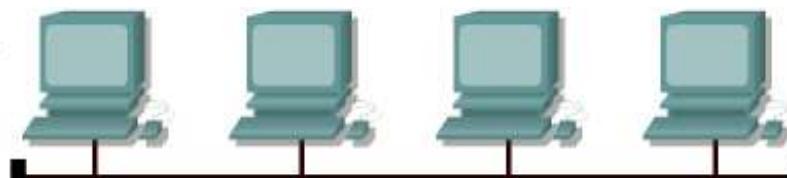
### 8.2.1 Środowiska ze współdzielonym medium

Przyswojenie sobie pojęcia domeny kolizyjnej wymaga zrozumienia, czym są kolizje i co je powoduje. W celu wyjaśnienia pojęcia kolizji, dokonano przeglądu mediów oraz topologii warstwy pierwszej.

Niektóre sieci są ze sobą bezpośrednio połączone i wszystkie hosty współdzielą warstwę 1. Poniżej przedstawiono przykłady:

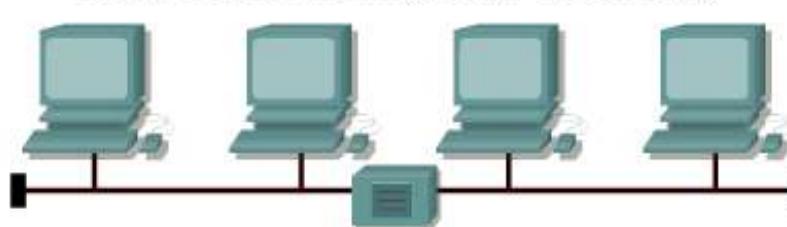
- **Środowisko ze współdzielonym medium:** Występuje, gdy wiele hostów ma dostęp do tego samego medium. Jeśli na przykład kilka komputerów jest dołączonych do tego samego przewodu lub światłowodu to współdzielą one to samo środowisko medium.
- **Rozszerzone środowisko ze współdzielonym medium:** Jest to specjalny rodzaj środowiska ze współdzielonym medium, w którym urządzenia sieciowe mogą rozszerzyć środowisko w taki sposób, że możliwy jest wielodostęp lub większa długość połączeń kablowych.
- **Środowisko sieciowe typu punkt-punkt:** Często stosuje się je w sieciowych połączeniach telefonicznych. Jest ono najbardziej znane użytkownikom domowym. Stanowi taki typ współdzielonego środowiska sieciowego, w którym pojedyncze urządzenie jest połączone z innym pojedynczym urządzeniem (tak jak w przypadku połączenia komputera z dostawcą usług internetowych za pomocą modemu i linii telefonicznej).

### Typy sieci

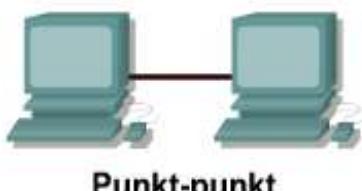


Media współdzielone (dostęp wielokrotny)

Połączone bezpośrednio



Media rozszerzone (dostęp wielokrotny przy wykorzystaniu urządzenia sieciowego warstwy 1)



Umiejętność zidentyfikowania środowiska ze współdzielonym medium jest ważna, ponieważ tylko tam występują kolizje. Sieć drogowa jest przykładem współdzielonego środowiska, w którym mogą występować kolizje, ponieważ duża liczba pojazdów korzysta z tych samych dróg. Wraz ze zwiększaniem się w systemie liczby pojazdów, zwiększa się prawdopodobieństwo wystąpienia kolizji.

Współdzielona sieć danych jest bardzo podobna do systemu dróg. Zostały zdefiniowane reguły określające zasady dostępu do medium sieciowego, jednak czasem, ze względu na natężenie ruchu, stosowanie reguł nie wystarcza

i występują kolizje

## 8.2.2 Domeny kolizyjne

Domeny kolizyjne są połączonymi fizycznymi segmentami sieci, w których mogą wystąpić kolizje. Kolizje mogą sprawić, że sieć będzie działać mało wydajnie. Przy każdym wystąpieniu kolizji transmisja zatrzymywana jest na pewien czas.

Długość tej przerwy jest różna i zależy od algorytmu oczekiwania w przypadku każdego urządzenia sieciowego.

Typy urządzeń, które łączą segmenty medium, wyznaczają granice domen kolizyjnych. Urządzenia te zostały zaklasyfikowane jako urządzenia warstw 1, 2 i 3 modelu OSI. Urządzenia warstwy 1 nie rozdzielają domen kolizyjnych, urządzenia warstw 2 i 3 rozdzielają domeny kolizyjne. Rozdzielanie domen kolizyjnych (zwiększenie ich liczb) przy użyciu urządzeń warstw 2 i 3 jest także znane jako segmentacja.

Podstawową funkcją urządzeń warstwy 1, takich jak węzły i koncentratory jest rozszerzanie segmentów kablowych sieci Ethernet. Dzięki powiększeniu sieci można dodać większą liczbę hostów. Każdy dodany host zwiększa jednak potencjalnie natężenie ruchu w sieci. Ponieważ urządzenia warstwy 1 przekazują dalej wszystkie informacje przesypane przez medium, im intensywniejszy ruch jest generowany wewnątrz domeny kolizyjnej, tym większe jest prawdopodobieństwo kolizji. Efektem końcowym jest zmniejszona wydajność sieci. Efekt ten zostanie jeszcze spotęgowany, jeśli wszystkie komputery w tej sieci zgłoszą duże zapotrzebowanie na pasmo. Innymi słowy: urządzenia warstwy 1 rozszerzają domenę kolizyjną, lecz rozmiar sieci LAN może równocześnie zostać zbyt mocno powiększony, co zwiększy liczbę problemów dotyczących kolizji.

Według reguły czterech węzłów w sieci Ethernet, pomiędzy dwoma dowolnymi komputerami w sieci nie powinny znajdować się więcej niż cztery węzły lub koncentratory. Aby zapewnić prawidłowe funkcjonowanie sieci 10BASE-T z węzłami, czas opóźnienia w obie strony musi zawierać się w określonych granicach. W innym przypadku niektóre stacje robocze nie będą w stanie wykryć wszystkich kolizji w sieci. Reguła czterech węzłów uwzględnia opóźnienia wprowadzane przez węzły, opóźnienia propagacji i opóźnienia wprowadzane przez karty sieciowe. Złamanie reguły czterech węzłów może prowadzić do naruszenia granicy maksymalnego opóźnienia. Po przekroczeniu tej granicy liczba kolizji spóźnionych zwiększa się radykalnie. Kolizja spóźniona występuje po wyemitowaniu pierwszych 64 bajtów ramki. Nie jest wymagane, aby chipsety kart sieciowych podejmowały automatyczną retransmisję w przypadku wystąpienia kolizji spóźnionej. Ramki spóźnionych kolizji wprowadzają opóźnienie zwane opóźnieniem konsumpcyjnym. Kiedy zwłoka i opóźnienie konsumpcyjne wzrastają, wydajność sieci spada.

**Według reguły 5-4-3-2-1 nie należy przekraczać poniższych wartości:**

- Pięć segmentów medium sieciowego
- Cztery węzły lub koncentratory
- Trzy segmenty sieci zawierające hosty
- Dwie sekcje łączy (bez hostów)
- Jedna duża domena kolizyjna

Reguła 5-4-3-2-1 zawiera również wskazówki pozwalające utrzymać w odpowiednich granicach obustronne opóźnienia występujące w sieci współdzielonej.

## 8.2.3 Segmentacja

Historia rozwoju sposobów, w jaki radzono sobie z kolizjami i domenami kolizyjnymi w sieci Ethernet, sięga badań prowadzonych na Uniwersytecie Hawajskim w roku 1970. Próby stworzenia bezprzewodowego systemu komunikacyjnego dla wysp Hawajskich doprowadziły do opracowania protokołu znanego pod nazwą Aloha. Protokół Ethernet został stworzony na bazie protokołu Aloha.

Zdolność identyfikowania domen kolizyjnych jest ważną umiejętnością specjalistów sieciowych. Podłączenie kilku komputerów do pojedynczego współdzielonego medium, do którego nie są podłączone inne urządzenia sieciowe, tworzy domenę kolizyjną. Sytuacja ta powoduje ograniczenie liczby komputerów, które mogą korzystać z medium. Taki ograniczony zbiór zwany jest także segmentem. Urządzenia warstwy 1 rozszerzają domeny kolizyjne, lecz nie kontrolują ich.

## Obliczanie opóźnienia transmisji w obie strony

(opóźnienie węzła + opóźnienie kablowe + opóźnienie karty sieciowej) x 2 < maksymalnego opóźnienia transmisji w obie strony

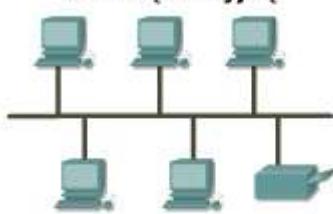
Opóźnienie węzła dla sieci 10BASE-T < 2 mikrosekundy na węzeł Opóźnienie kablowe ~ 0,55 mikrosekundy na 100 metrów Opóźnienie karty sieciowej ~ 1 mikrosekunda na kartę sieciową.

Maksymalne opóźnienie powrotne (czas transmisji bitu w sieciach 10BASE-T równy 0,1 mikrosekundy pomnożony przez minimalną długość ramki równą 512 bitów) wynosi 51,2 mikrosekundy.

Dla skrętki nieekranowanej o długości 500 m połączonej przez cztery węzły lub koncentratory oraz dwie karty sieciowe całkowite opóźnienie byłoby dużo niższe od maksymalnego opóźnienia transmisji w obie strony.

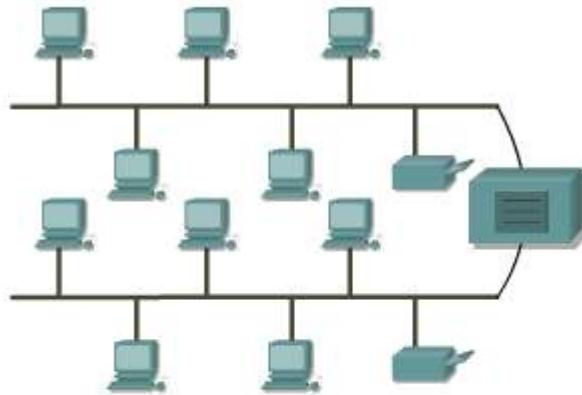
## Urządzenia warstwy 1 powiększają domenę kolizyjną

Dostęp współużytkowany jest domeną kolizyjną

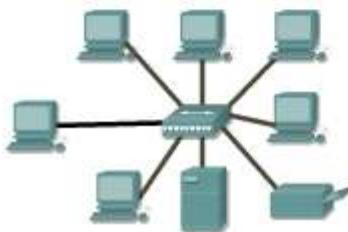


Domena kolizyjna

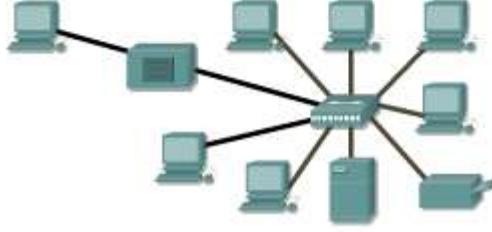
roszzerzona przez węźłownika



Domena kolizyjna utworzona przez koncentrator



Domena kolizyjna rozszerzona przez węźłownika



Urządzenia warstwy 2 segmentują czyli dzielą domeny kolizyjne. Segmentacja ta jest prowadzona dzięki kontroli propagacji ramek dokonywanej w oparciu o adres MAC przypisany do każdego urządzenia używanego w sieci Ethernet. Urządzenia warstwy 2 — mosty i przełączniki — rejestrują adresy MAC i ich występowanie w poszczególnych segmentach. Wykonywanie tej czynności pozwala urządzeniom kontrolować ruch na poziomie warstwy 2. Dzięki tej funkcji sieci działają sprawniej, ponieważ dane mogą być przesyłane w różnych segmentach sieci LAN w tym samym czasie, nie powodując przy tym kolizji. Poprzez zastosowanie mostów i przełączników domena kolizyjna jest dzielona na mniejsze części, które stają się osobnymi domenami kolizyjnymi.

Mniejsze domeny kolizyjne zawierają mniej hostów, co powoduje mniejszy ruch niż w pierwotnej domenie kolizyjnej. Mniejsza liczba hostów znajdujących się w pojedynczej domenie kolizyjnej sprawia, że dostępność medium jest bardziej prawdopodobna. Mostowana sieć działa dobrze do momentu, gdy ruch pomiędzy segmentami połączonymi za pomocą mostów staje się zbyt duży. W tym przypadku urządzenie warstwy 2 może samo stać się wąskim gardłem spowalniającym komunikację.

**Urządzenia warstwy 3, podobnie jak urządzenia warstwy 2, nie przesyłają kolizji. Z tego powodu wykorzystanie urządzeń warstwy 3 w sieci powoduje podział domen kolizyjnych na mniejsze domeny.**

**Urządzenia warstwy 3 poza podziałem domen kolizyjnych pełnią również inne funkcje. Urządzenia warstwy 3 oraz ich funkcje będą szczegółowo opisane w części dotyczącej domen rozgłoszeniowych.**

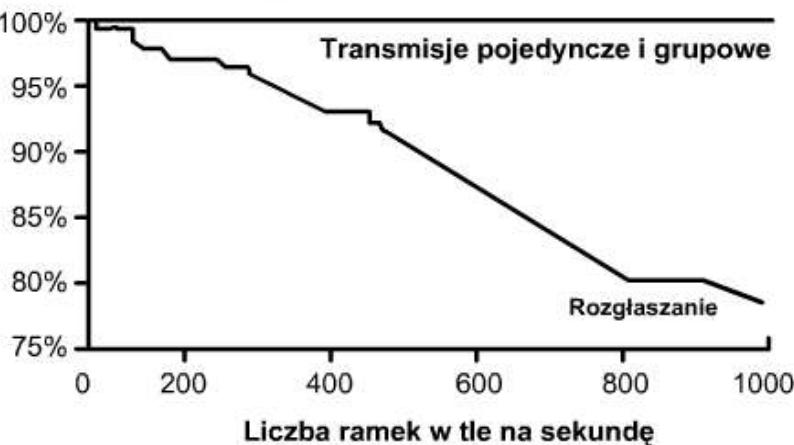
### **8.2.4 Rozgłaszenie w warstwie 2**

Protokoły wykorzystują ramki rozgłoszeniowe i wieloemisyjne na poziomie warstwy 2 modelu OSI do komunikacji pomiędzy domenami kolizyjnymi. Kiedy węzeł ma nawiązać komunikację ze wszystkimi hostami w sieci, wysyła ramkę rozgłoszeniową z adresem odbiorcy równym 0xFFFFFFFFFFFF. Ramkę z takim adresem muszą rozpoznać karty sieciowe wszystkich hostów.

Urządzenia warstwy 2 muszą rozpropagowywać ruch rozgłoszeniowy i grupowy na wszystkie porty. Sumaryczny ruch rozgłoszeniowy i grupowy generowany przez wszystkie urządzenia w sieci nazywany jest promieniowaniem rozgłoszeniowym. Zdarza się, że obieg promieniowania rozgłoszeniowego może tak nasycić sieć, że zabraknie pasma dla danych aplikacji. W tym przypadku nowe połączenia sieciowe nie mogą być ustanowione, a nawiązane już połączenia mogą zostać zerwane. Sytuacja taka jest nazywana burzą rozgłoszeniową. Prawdopodobieństwo wystąpienia burzy rozgłoszeniowej wzrasta wraz z rozrostem sieci przełączanej.

Promieniowanie rozgłoszeniowe wpływa na wydajność hostów w sieci, ponieważ karty sieciowe przerywają normalną pracę procesora, aby przetworzyć każde rozgłoszenie lub emisję grupową, którą są objęte. **Na rysunku przedstawione są wyniki testów prowadzonych przez firmę Cisco ukazujące wpływ promieniowania rozgłoszeniowego na wydajność procesora komputera SPARCstation 2 firmy SUN wyposażonego w standardową wbudowaną kartę sieci Ethernet. Jak wyniki pokazują, stacja robocza może zostać skutecznie zablokowana przez rozgłoszanie zalewające sieć. W skrajnych sytuacjach obserwowano szczytowe poziomy ruchu rozgłoszeniowego rzędu tysięcy rozgłoszeń na sekundę podczas burzy rozgłoszeń. Testy prowadzone w kontrolowanym środowisku sieciowym z wieloma emisjami rozgłoszeniowymi i grupowymi ukazują mierzalne obniżenie wydajności systemu**

## Wpływ emisji rozgłoszeń na hosty w sieci IP



zlokalizować adres MAC, który nie znajduje się w jej tablicy ARP. Pomimo że liczby pokazane na rysunku mogą wydawać się niskie, reprezentują średnią, dobrze zaprojektowaną sieć IP. Gdy ruch rozgłoszeniowy i związany z emisjami grupowymi osiąga szczyt z powodu burzy, szczytowa strata mocy procesora może być o cały rząd wielkości większa od wielkości średniej. Burze rozgłoszeniowe mogą być powodowane przez urządzenie żądające informacji od zbyt mocno rozrośniętej sieci. Urządzenie nie jest w stanie przetworzyć tak dużej liczby odpowiedzi, bądź też pierwsze żądanie wyzwala podobne żądania od innych urządzeń, co skutecznie blokuje normalny ruch w sieci.

Na przykład adres w poleceniu **telnet mumble.com** jest tłumaczony na adres IP w procesie wyszukiwania w ramach protokołu DNS. W celu zlokalizowania odpowiadającego adresu MAC rozgłoszane jest żądanie ARP. Zwykle stacje robocze IP przechowują w pamięci podręcznej wewnętrznych tablicach ARP od 10 do 100 adresów na czas około dwóch godzin. Dla typowej stacji roboczej może to być 50 adresów w przeciągu 2 godzin, co daje 0,007 żądań ARP na sekundę. Tak więc 2000 stacji końcowych generuje około 14 żądań ARP na sekundę.

Znaczący wzrost ruchu rozgłoszeniowego może być spowodowany działaniem protokołów routingu skonfigurowanych w danej sieci. Zdarza się, że administratorzy sieci w ramach strategii nadmiarowości i dostępności konfigurują wszystkie stacje robocze, tak aby był na nich uruchomiony protokół RIP. Co 30 sekund protokół RIPv1 wykorzystuje rozgłoszanie w celu retransmisji tablic routingu do innych routerów. Jeśli działanie protokołu RIP zostało skonfigurowane na 2000 stacji roboczych, a przesłanie tablicy routingu wymagałoby średnio 50 pakietów, stacje robocze generowałyby 3333 rozgłoszenia na sekundę. Większość administratorów sieci konfiguruje niewielką liczbę routerów (zwykle od 5 do 10), na których ma być uruchomiony protokół RIP. 10 routerów z protokołem RIP wygenerowałoby 16 rozgłoszeń na sekundę w przypadku tablicy routingu o rozmiarze 50 pakietów.

Aplikacje z emisją grupową IP mogą niekorzystnie wpływać na wydajność dużej, dobrze skalowanej sieci przełączanej. Oprócz tego, że emisja grupowa jest wydajną metodą przesyłania strumienia danych multimedialnych do wielu użytkowników, to niestety oddziałuje ona na każdego użytkownika w sieci przełączanej. Dana aplikacja wideo operująca pakietami może wygenerować siedmiomegabajtowy strumień danych rozgłoszeniowych, który w sieci przełączanej zostałby rozszyfrowany do każdego segmentu, powodując wystąpienie poważnego zatoru.

### 8.2.5 Domeny rozgłoszeniowe

Domena rozgłoszeniowa jest zbiorem domen kolizyjnych połączonych ze sobą urządzeniami warstwy 2. Podział sieci LAN na większą liczbę domen kolizyjnych zwiększa prawdopodobieństwo uzyskania przez każdy host dostępu do medium. Prawdopodobieństwo kolizji zostaje zredukowane, a każdy host zyskuje możliwość dostępu do szerszego pasma. Jednak pakiety rozgłoszeniowe są przesyłane przez urządzenia warstwy 2 i, jeśli występują zbyt często, mogą zmniejszyć wydajność całej sieci LAN. Ponieważ urządzenia warstw 1 i 2 nie mają wpływu na emisje rozgłoszeniowe, muszą być one kontrolowane przez urządzenia warstwy 3. Całkowity rozmiar domeny rozgłoszeniowej można zidentyfikować, wyszukując wszystkie domeny kolizyjne, w których jest przetwarzana ramka rozgłoszeniowa. Innymi słowy, obejmuje ona obszar sieci ograniczony urządzeniami warstwy trzeciej. Domeny rozgłoszeniowe są kontrolowane na poziomie warstwy 3, ponieważ routery nie przesyłają rozgłoszeń. W rzeczywistości routery działają w warstwach 1, 2 oraz 3 i, tak samo jak urządzenia warstwy 1, są fizycznie połączone do medium oraz transmitują dane za jego pośrednictwem. Dane podlegają enkapsulacji na wszystkich interfejsach i są traktowane tak samo jak w każdym innym urządzeniu warstwy 2. Routery mogą segmentować domeny rozgłoszeniowe w warstwie 3.

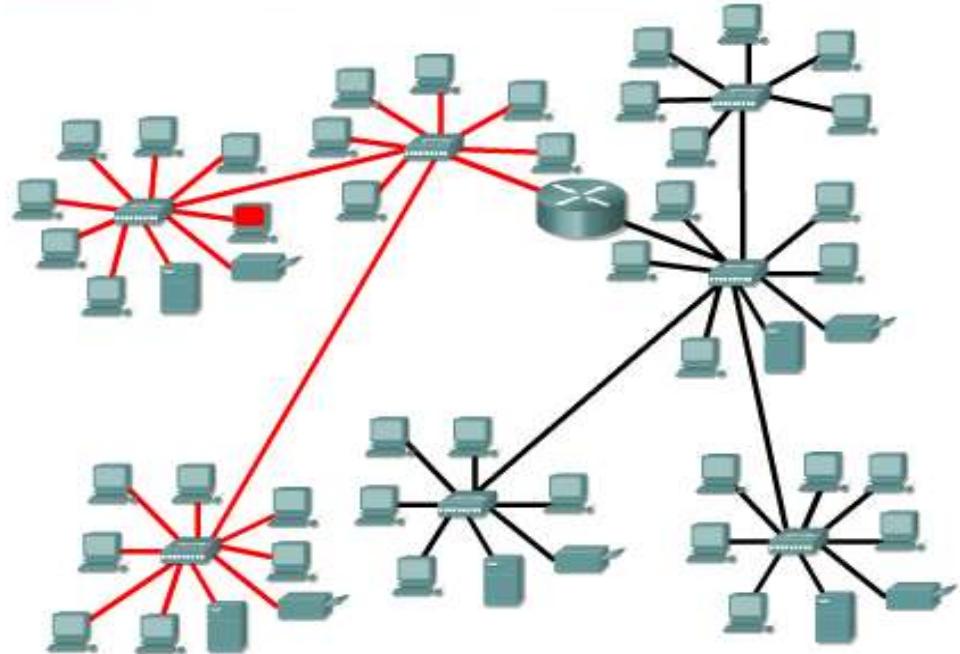
Żeby pakiet został przesłany przez router, musi być wcześniej przetworzony przez urządzenie warstwy 2, a informacje ramki muszą być usunięte. Przesyłanie w warstwie 3 oparte jest na adresie IP odbiorcy, a nie na adresie

przy zaledwie 100 rozgłoszeniach lub emisjach grupowych na sekundę. Najczęściej host niebędący adresatem w żaden sposób nie korzysta z przetworzenia rozgłoszenia. Host nie jest zainteresowany ogłaszaną usługą lub wie już o jej istnieniu. Wysoki poziom promieniowania rozgłoszeniowego może w zauważalny sposób obniżyć wydajność hosta. Stacje robocze, routery i aplikacje rozgłoszeniowe stanowią trzy źródła rozgłoszania i emisji grupowej w sieciach IP.

Stacja robocza rozgłasza żądanie protokołu ARP za każdym razem, gdy trzeba

MAC. Aby doszło do przesłania pakietu, musi on zawierać docelowy adres IP spoza zakresu adresów przypisanych danej sieci LAN. Adres ten musi być zawarty w wewnętrznej tablicy routingu routera.

## Segmentacja domeny rozgłoszeniowej



Użycie routera w miejsce urządzenia mostującego blokuje zgłaszczenie w warstwie drugiej. Urządzenia warstwy trzeciej są jedynymi urządzeniami powstrzymującymi rozmawianie.

### 8.2.6 Wprowadzenie do przepływu danych

Pojęcie przepływu danych w kontekście domen kolizyjnych i rozgłoszeniowych obejmuje sposób, w jaki ramka rozprzestrzenia się w sieci. Dotyczy to przepływu informacji przez urządzenia warstw 1, 2 i 3 oraz sposobów efektywnej enkapsulacji danych w celu ich przesłania między warstwami.

Należy pamiętać, że proces enkapsulacji na poziomie warstwy sieciowej obejmuje adresy IP nadawcy i odbiorcy, a na poziomie warstwy łączącej danych — adresy MAC nadawcy i odbiorcy.

**Dobrze jest zapamiętać, że urządzenia warstwy 1 zawsze przekazują, natomiast urządzenia warstwy 2 „chcą” przekazać ramkę. Innymi słowy, urządzenie warstwy 2 przekaże ramkę, chyba że zaistnieją określone okoliczności. Urządzenie warstwy 3 nie przekaże ramki, jeśli nie zaistnieje taka potrzeba.**

Zastosowanie tej reguły pomoże zrozumieć, w jaki sposób dane są przesyłane przez sieć.

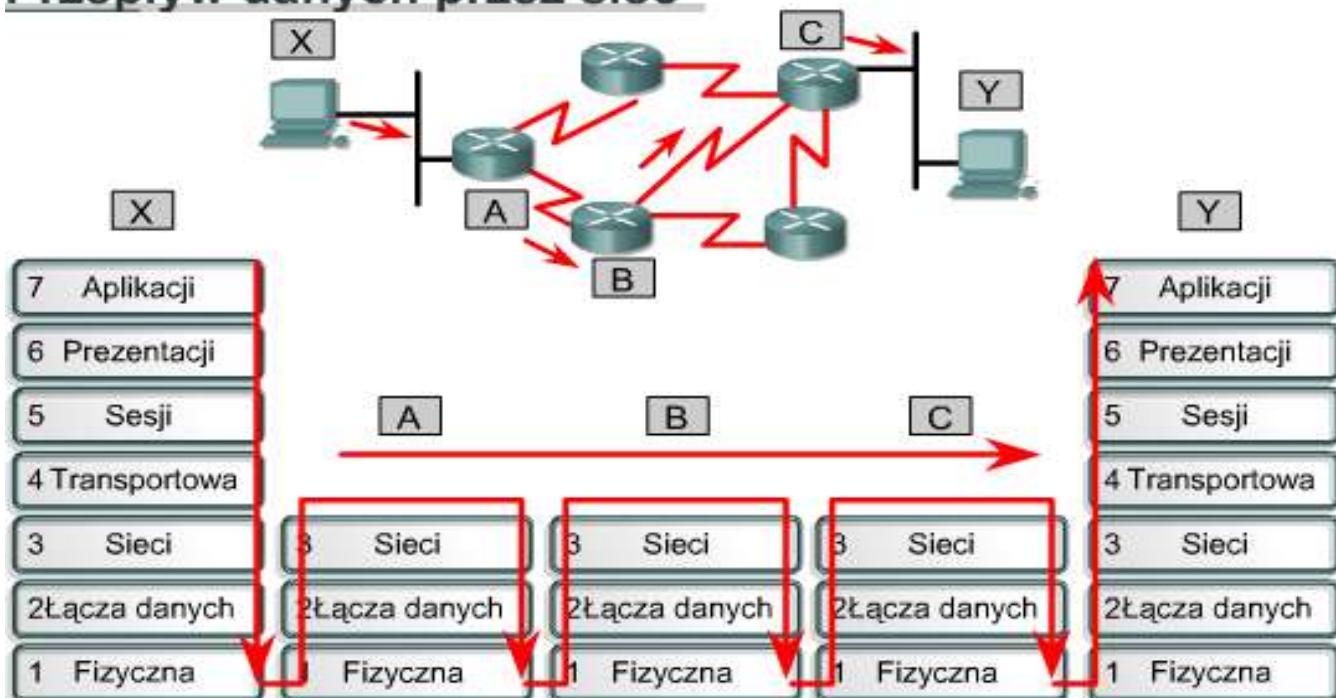
Urządzenia warstwy 1 nie filtryują danych, więc wszystkie odebrane dane są przekazywane do następnego segmentu. Zwracana ramka poddawana jest procesom regeneracji i synchronizacji, które przywracają jej początkową jakość. Wszystkie segmenty połączone za pośrednictwem urządzeń warstwy 1 stanowią tę samą domenę kolizyjną i rozgłoszeniową.

Urządzenia warstwy 2 filtryują ramki w oparciu o adres MAC odbiorcy. Ramka jest przekazywana, jeśli jest kierowana do nieznanego odbiorcy poza domeną kolizyjną. Ramka zostanie przekazana także w przypadku, gdy jest częścią transmisji grupowej, pojedynczej lub rozgłoszeniowej kierowanej poza lokalną domeną kolizyjną. Urządzenie warstwy 2 nie przekaże ramki tylko w przypadku, gdy zostanie stwierdzono, że host nadawcy i odbiorcy znajdują się w tej samej domenie kolizyjnej. Urządzenie warstwy 2, takie jak most, tworzy wiele domen kolizyjnych, lecz utrzymuje pojedynczą domenę rozgłoszeniową.

Urządzenia warstwy 3 filtryują pakiety danych w oparciu o adres IP odbiorcy. Pakiet zostanie przesłany tylko w przypadku, gdy adres IP odbiorcy znajduje się poza domeną rozgłoszeniową, a router zidentyfikował miejsce, do którego pakiet ma zostać skierowany. Urządzenia warstwy 3 tworzą wiele domen kolizyjnych i rozgłoszeniowych.

Przepływ danych przez routowaną sieć IP wymaga przesyłania informacji pomiędzy urządzeniami zarządzającymi ruchem w warstwach 1, 2 i 3 modelu OSI. Warstwę 1 wykorzystuje się do transmitowania danych w medium fizycznym, warstwa 2 służy do zarządzania domenami kolizyjnymi, natomiast warstwa 3 do zarządzania domenami rozgłoszeniowymi.

# Przepływ danych przez sieć



Przepływ danych w sieci skupia się na pierwszej, drugiej i trzeciej warstwie modelu OSI. Dzieje się to po nadaniu przez hosta wysyłającego i przed odebraniem przez hosta odbierającego.

## 8.2.7 Czym jest segment sieci?

Tak jak wiele innych pojęć i skrótów, słowo segment ma wiele znaczeń. Słownikowa definicja tego pojęcia brzmi:

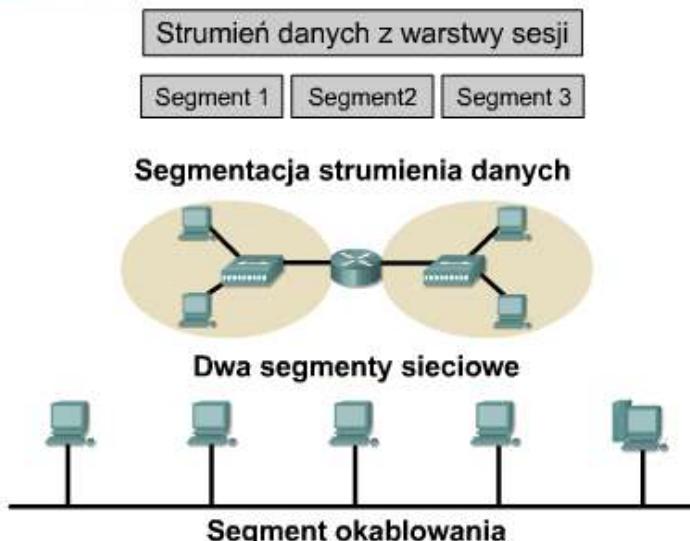
- oddzielna część czegoś
- jedna z części, na które jest lub mogłyby być podzielona jednostka lub zbiór

W przypadku transmisji danych używa się następujących definicji:

- Sekcja sieci, której granice wyznaczają mosty, routery lub przełączniki.
- W sieci LAN o topologii magistrali segment jest ciągłym odcinkiem obwodu elektrycznego często połączonym z innymi podobnymi segmentami przy użyciu wtyczników.
- Pojęcie używane w specyfikacji protokołu TCP do opisu pojedynczej jednostki informacji w warstwie transportowej. Do opisu logicznych grup informacji na różnych poziomach modelu odniesienia OSI służą również pojęcia: *datagram, ramka, komunikat i pakiet*. Są one używane w różnych środowiskach technicznych.

Aby poprawnie zdefiniować pojęcie segmentu, należy podać kontekst, w jakim używane jest to słowo. Jeśli słowo segment jest używane w kontekście protokołu TCP, określa ono oddzielną porcję danych. Jeśli natomiast jest użyte w kontekście fizycznego medium sieciowego w sieci routowanej, oznacza jedną z części lub sekcji składających się na całą sieć.

## Segmenty



Wyróżnia się różne typy segmentów sieci komputerowych. Znaczenie pojęcia segment zależy od kontekstu danego zdania.

## Podsumowanie

- Trzy najczęściej stosowane przełączania to: store-and-forward, cut-through oraz fragment-free.
- Protokół drzewa opinającego stosowany jest w celu unikania i eliminowania pętli w sieci.
- Urządzenia warstwy 1 nie dzielą domen kolizyjnych.
- Urządzenia warstwy 2 i 3 dzielą domeny kolizyjne.
- Urządzenia warstwy 1 i 2 nie blokują rozgłoszania.

## Moduł 9. Zestaw protokołów TCP/IP

Internet został zaprojektowany jako sieć łączności, która mogłyby działać także w okresie wojny. Chociaż Internet ewoluował w zupełnie innych kierunkach, niż wyobrażali to sobie jego twórcy, nadal jego podstawę stanowi zestaw protokołów TCP/IP. Architektura protokołów TCP/IP doskonale nadaje się do wykorzystania w zdecentralizowanej i odpornej na błędy sieci. Taką siecią jest Internet. Wiele z używanych aktualnie protokołów zostało opartych na czterowarstwowym modelu TCP/IP. Warto poznać zarówno model sieciowy TCP/IP, jak i model OSI. Każdy z nich ma własną strukturę, wyjaśniającą działanie sieci, ale modele te mają wiele wspólnych cech. Bez zrozumienia obydwu tych modeli administrator może dysponować zbyt małą wiedzą, aby rozumieć, dlaczego sieć działa w taki, a nie inny sposób. Każde urządzenie w Internecie, które komunikuje się z innymi urządzeniami internetowymi, musi mieć unikatowy identyfikator. Identyfikator ten jest nazywany adresem IP, ponieważ routery w celu znalezienia najlepszej trasy do danego urządzenia używają protokołu IP, należącego do trzeciej warstwy. Aktualnie używana wersja protokołu IP, czyli IPv4, została zaprojektowana w okresie, gdy zapotrzebowanie na adresy nie było duże. Gwałtowny rozwój Internetu zaczął grozić wyczerpaniem puli dostępnych adresów IP. Do zwiększenia możliwości wykorzystania adresów IP bez wyczerpania dostępnej puli adresów wykorzystywany jest podział na podsieci, translacja adresów sieciowych NAT (*Network Address Translation*) oraz adresy prywatne. Inna wersja protokołu IP (protokół IPv6) ma dużo większą przestrzeń adresową, co pozwala na uwzględnienie lub rezygnację z metod wykorzystywanych do wyeliminowania niedostatków protokołu IPv4. Aby stać się częścią Internetu, każdy komputer potrzebuje nie tylko fizycznego adresu MAC, ale i unikatowego adresu IP, nazywanego również adresem logicznym. Istnieje kilka metod przypisywania urządzeniu adresu IP. Niektóre urządzenia zawsze mają adres statyczny, podczas gdy innym przydzielany jest tymczasowy adres za każdym razem, gdy łączą się z siecią. Gdy potrzebny jest adres IP przypisywany dynamicznie, urządzenie może go otrzymać przy użyciu kilku metod. Aby efektywnie routować pakiety pomiędzy urządzeniami, trzeba także rozwiązać inne problemy. Na przykład powtarzane adresy IP mogą uniemożliwić efektywne przekazywanie danych.

### 9.1 Wprowadzenie do protokołów TCP/IP

#### 9.1.1 Historia i przyszłość modelu TCP/IP

##### Adresy IPv4 i IPv6

0 0 1 0 0 0 0 1 . 1 0 0 0 0 1 1 0 . 1 1 0 0 0 0 0 1 . 0 0 0 0 0 0 1 1	33 . 134 . 193 . 3
0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 : 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0	3ffe : 1900
0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1	6545 : 3
0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 : 1 1 1 1 1 0 0 0 0 0 0 0 0 1 0 0	230 : f804
0 1 1 1 1 1 0 1 0 1 1 1 1 1 : 0 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0	7ebf : 12c2

Model odniesienia TCP/IP został utworzony przez Departament Obrony USA w ramach prac nad projektem sieci, która przetrwała w każdych warunkach. Aby to lepiej wyjaśnić, wyobraźmy sobie świat połączony różnymi łączami kablowymi, światłowodowymi, mikrofalowymi i satelitarnymi. Następnie wyobraźmy sobie, że chcemy mieć możliwość przesyłania danych do dowolnego węzła takiej sieci bez względu na warunki.

Departament Obrony USA potrzebował niezawodnej metody transmisji danych do dowolnego miejsca przeznaczenia, niezależnie od warunków. Utworzenie modelu TCP/IP pomogło rozwiązać ten trudny problem. Model TCP/IP stał się od tego czasu standardem, na którym oparty jest Internet.

Czytając o warstwach modelu TCP/IP, należy pamiętać, w jakim celu utworzono Internet. Pomoże to uniknąć nieporozumień. Model TCP/IP składa się z następujących czterech warstw: warstwy aplikacji, warstwy transportowej, warstwy internetowej oraz warstwy dostępu do sieci. Niektóre z warstw modelu TCP/IP mają takie same nazwy jak warstwy modelu OSI. Ważne jest, aby nie pomylić funkcji poszczególnych warstw w tych modelach, ponieważ są one różne w każdym z nich.

Aktualnie używana wersja TCP/IP stała się standardem we wrześniu 1981 roku.

## 9.1.2 Warstwa aplikacji

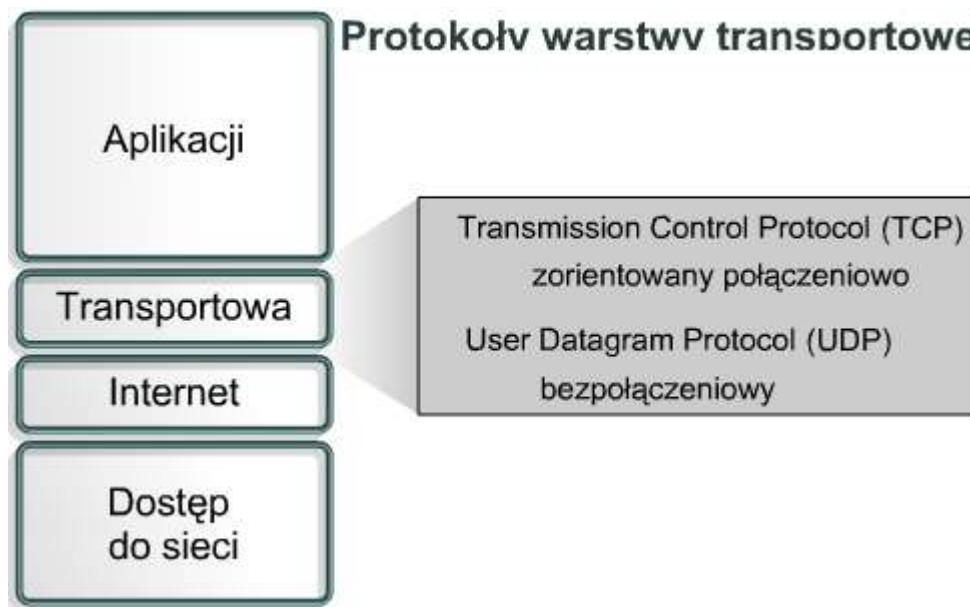
Warstwa aplikacji modelu TCP/IP obsługuje protokoły wysokopoziomowe oraz zajmuje się zagadnieniami związanymi z reprezentacją danych, kodowaniem i sterowaniem konwersacją. Zestaw protokołów TCP/IP łączy w jednej warstwie wszystkie zagadnienia związane z aplikacjami i zapewnia odpowiednie opakowanie danych przed przekazaniem ich do następnej warstwy. Zestaw protokołów TCP/IP zawiera nie tylko specyfikacje protokołów warstwy internetowej i warstwy transportowej, takich jak IP i TCP, ale również specyfikacje powszechnie używanych aplikacji. TCP/IP zawiera protokoły przesyłania plików, poczty elektronicznej i zdalnego logowania, a także:

- **Protokół FTP (*File Transfer Protocol*)** — protokół FTP jest niezawodną usługą zorientowaną połączeniowo, używającą protokołu TCP do przesyłania danych pomiędzy systemami korzystającymi z FTP. Umożliwia on dwukierunkowe przesyłanie plików binarnych i tekstowych.
- **Protokół TFTP (*Trivial File Transfer Protocol*)** — protokół TFTP jest bezpołączeniową usługą, która używa protokołu UDP. Protokół TFTP jest używany przez router do przesyłania plików konfiguracyjnych oraz obrazów systemu Cisco IOS, a także do przesyłania plików pomiędzy systemami korzystającymi z TFTP. Protokół ten jest użyteczny w niektórych sieciach LAN, ponieważ w stabilnym środowisku działa szybciej niż protokół FTP.
- **Protokół NFS (*Network File System*)** — protokół NFS jest utworzonym przez firmę Sun Microsystems zestawem protokołów rozproszonego systemu plików, który umożliwia korzystanie z plików znajdujących się na zdalnych urządzeniach pamięciowych, takich jak dyski sieciowe.
- **Protokół SMTP (*Simple Mail Transfer Protocol*)** — protokół SMTP odpowiada za przesyłanie poczty elektronicznej pomiędzy komputerami w sieci. Nie umożliwia on przesyłania danych innych niż tekstowe.
- **Protokół Telnet (*Terminal emulation*)** — protokół Telnet umożliwia zdalny dostęp do innego komputera. Pozwala on użytkownikowi na zalogowanie się na hoście internetowym i wykonywanie poleceń. Klient usługi Telnet jest nazywany hostem lokalnym. Serwer usługi Telnet jest nazywany hostem zdalnym.
- **Protokół SNMP (*Simple Network Management Protocol*)** — protokół SNMP umożliwia monitorowanie i sterowanie urządzeniami sieciowymi, zarządzanie konfiguracją, zbieranie danych statystycznych oraz zarządzanie wydajnością i zabezpieczeniami.
- **Protokół DNS (*Domain Name System*)** — protokół DNS jest używanym w Internecie systemem tłumaczenia nazw domen i należących do nich publicznie dostępnych węzłów sieciowych na adresy IP.

## Aplikacje TCP/IP



## Protokoły warstwy transportowej

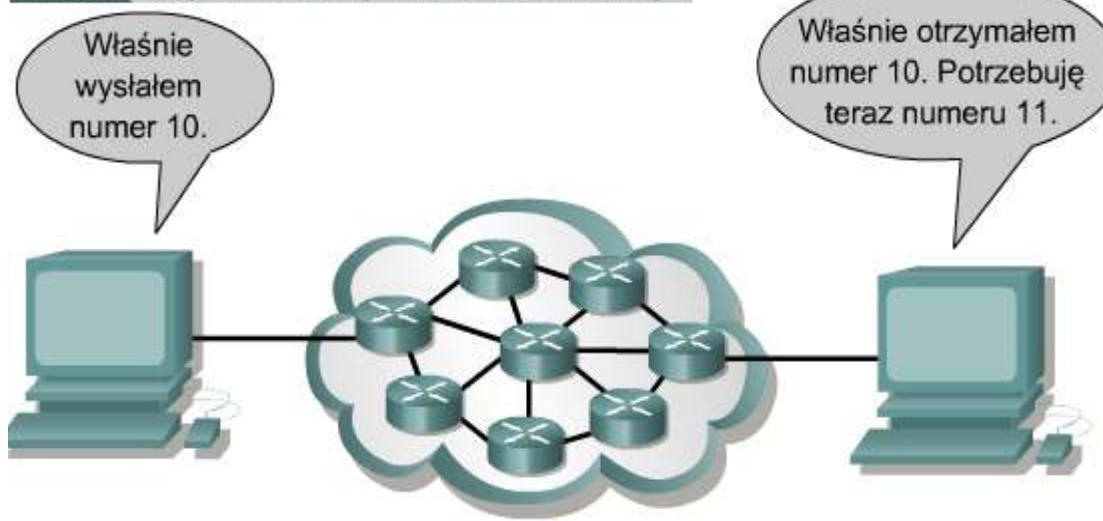


Internet jest zwykle przedstawiany w postaci chmury. Warstwa transportowa wysyła pakiety danych ze źródła do miejsca przeznaczenia poprzez taką chmurę. Przy korzystaniu z protokołu TCP podstawowym zadaniem warstwy

## 9.1.3 Warstwa transportowa

Warstwa transportowa zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Ustanawia ona logiczne połączenie pomiędzy punktami końcowymi w sieci, czyli hostem wysyłającym i odbierającym. Protokoły transportowe dzielą i scalają dane wysyłane przez aplikacje wyższej warstwy w jeden strumień danych przepływający między punktami końcowymi, tworzący połączenie logiczne. Strumień danych warstwy transportowej obsługuje transport typu end-to-end, czyli transport między punktami końcowymi.

## Protokoły warstwy transportowej



transportowej jest kontrola typu end-to-end, zapewniana przez okna przesuwne, potwierdzenia i niezawodność w stosowaniu kolejnych numerów pakietów. Warstwa transportowa tworzy także połączenia typu end-to-end pomiędzy aplikacjami na hostach. W skład usług transportowych wchodzą wszystkie poniższe usługi:

### W przypadku zarówno TCP, jak i UDP

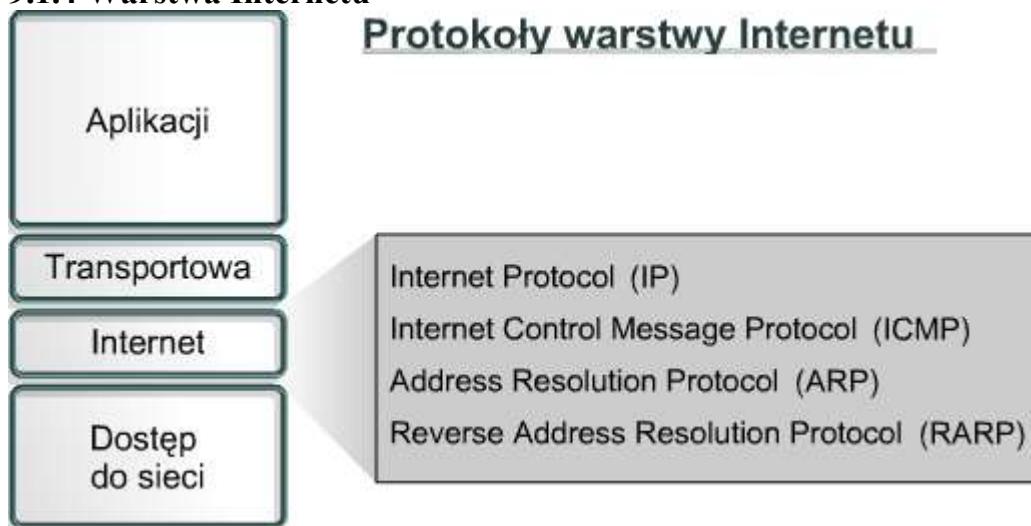
- dzielenie danych aplikacji wyższej warstwy,
- wysyłanie segmentów z jednego urządzenia końcowego do innego,

### Tylko w przypadku TCP

- ustanawianie połączenia typu end-to-end,
- kontrola przepływu zapewniana przez okna przesuwne,
- niezawodność zapewniana przez numery sekwencyjne i potwierdzenia.

Internet jest zwykle przedstawiany w postaci chmury. Warstwa transportowa wysyła pakiety danych ze źródła do miejsca przeznaczenia poprzez taką chmurę. Chmura ta musi radzić sobie z takimi zagadnieniami, jak wybór najlepszej trasy spośród kilku dostępnych.

### 9.1.4 Warstwa Internetu



Zadaniem warstwy Internetu jest wybranie najlepszej ścieżki dla pakietów przesyłanych w sieci. Podstawowym protokołem działającym w tej warstwie jest protokół IP (*Internet Protocol*). W tej warstwie następuje określenie najlepszej ścieżki i przełączanie pakietów.

**W warstwie internetowej modelu TCP/IP działają następujące protokoły:**

- Protokół IP, który zapewnia usługę bezpołączeniowego dostarczania pakietów przy użyciu dostępnych możliwości. Protokół IP nie bierze pod uwagę zawartości pakietu, ale wyszukuje ścieżkę do miejsca docelowego.
- Protokół ICMP (*Internet Control Message Protocol*), który zapewnia funkcje kontrolne i informacyjne.
- Protokół ARP (*Address Resolution Protocol*), który znajduje adres warstwy łącza danych MAC dla znanego adresu IP.
- Protokół RARP (*Reverse Address Resolution Protocol*), który znajduje adres IP dla znanego adresu MAC.

#### Protokół IP spełnia następujące zadania:

- definiuje format pakietu i schemat adresowania,
- przesyła dane pomiędzy warstwą internetową i warstwą dostępu do sieci,
- kieruje pakiety do zdalnych hostów.

Protokół IP jest czasem nazywany protokołem zawodnym. Nie oznacza to jednak, że protokół IP nie dostarcza poprawnie danych poprzez sieć. Jego „zawodność” polega po prostu na tym, że protokół IP nie wykrywa i nie koryguje błędów. Te funkcje są wykonywane przez protokoły z wyższych warstw, transportowej lub aplikacji.

### 9.1.5 Warstwa dostępu do sieci

Warstwa dostępu do sieci jest także nazywana warstwą interfejsu sieciowego. Warstwa dostępu do sieci jest odpowiedzialna za wszystkie zagadnienia związane z tworzeniem łącza fizycznego służącego do przekazywania pakietu IP do medium sieciowego. Obejmuje ona szczegółowe rozwiązania dotyczące technologii sieciowych LAN i WAN, łącznie ze szczegółami dotyczącymi warstwy fizycznej i warstwy łącza danych modelu OSI. Sterowniki aplikacji, modemów i innych urządzeń działają na poziomie warstwy dostępu do sieci. Warstwa dostępu do sieci definiuje funkcje umożliwiające korzystanie ze sprzętu sieciowego i dostęp do medium transmisyjnego. Standardowe protokoły modemowe, takie jak SLIP (*Serial Line Internet Protocol*) i PPP (*Point-to-Point Protocol*), umożliwiają dostęp do sieci za pośrednictwem połączenia modemowego. Ponieważ zależności pomiędzy specyfikacjami sprzętu, oprogramowania i medium transmisyjnego są skomplikowane, w warstwie tej działa wiele protokołów. Może to powodować zamieszanie wśród użytkowników. Większość znanych protokołów działa w warstwie internetowej i transportowej modelu TCP/IP.

Warstwa dostępu do sieci odpowiada między innymi za odwzorowywanie adresów IP na adresy sprzętowe i enkapsulację pakietów IP w ramki. Warstwa dostępu do sieci definiuje połączenie z fizycznym medium sieci w zależności od rodzaju sprzętu i interfejsu sieciowego.

Dobrym przykładem konfigurowania warstwy dostępu do sieci jest konfigurowanie systemu Windows po włożeniu do komputera karty sieciowej. W zależności od wersji systemu Windows karta sieciowa może zostać automatycznie wykryta przez system operacyjny, po czym zostaną zainstalowane odpowiednie sterowniki. W starszej wersji systemu

Windows użytkownik sam musiałby określić sterownik karty sieciowej. Producent karty dostarcza takich sterowników na dyskietkach lub dyskach CD-ROM.

### 9.1.6 Porównanie modelu OSI z modelem TCP/IP

#### Porównanie modelu TCP/IP z modelem OSI

TCP/IP Model



OSI Model



Powyżej przedstawiono porównanie modelu OSI z modelem TCP/IP z uwzględnieniem podobieństw i różnic:

#### Podobieństwa modeli OSI i TCP/IP:

- Oba modele składają się z warstw.
- Oba modele mają warstwy aplikacji, chociaż świadczą one bardzo różne usługi.
- Oba mają porównywalne warstwy sieciowe i transportowe.
- W oby wypadkach zakładane jest wykorzystanie techniki przełączania pakietów, a nie komutacji łączy.
- Specjalisci w dziedzinie sieci powinni znać oba te modele.

## Różnice pomiędzy modelem OSI i TCP/IP:

- W modelu TCP/IP zadania warstwy prezentacji i sesji są realizowane przez warstwę aplikacji.
- W modelu TCP/IP jedna warstwa pełni rolę warstw łączących danych i fizycznej modelu OSI.
- Model TCP/IP wydaje się prostszy ze względu na mniejszą liczbę warstw.
- Jeżeli w warstwie transportowej modelu TCP/IP używany jest protokół UDP, nie ma gwarancji pewnego dostarczenia pakietów, co gwarantuje warstwa transportowa modelu OSI.

Internet powstał opierając się na standardach protokołów TCP/IP. Model TCP/IP zyskuje na znaczeniu właśnie dzięki swoim protokołom. Z drugiej strony, zwykle nie buduje się sieci na podstawie modelu OSI. Model OSI jest natomiast używany do wyjaśniania procesu komunikacji.

### 9.1.7 Architektura Internetu

Chociaż struktura Internetu jest złożona, jego działanie opiera się na kilku prostych zasadach. W tej sekcji przyjrzymy się podstawowej architekturze Internetu. Internet jest oparty na pozornie prostym pomyśle, który powtórzony na dużą skalę umożliwia prawie natychmiastowe przesyłanie w dowolnym momencie danych między dowolnymi klientami sieci.

Sieci LAN są mniejszymi sieciami, obejmującymi ograniczony obszar geograficzny. Połączenie wielu sieci LAN pozwala na funkcjonowanie Internetu. Sieci LAN mają jednak ograniczoną wielkość. Odległość nadal stanowi przeszkodę, chociaż opracowano nowe techniki zwiększające szybkość transmisji, takie jak Gigabit, 10 Gigabit Ethernet lub Metro Optical.

Jednym ze sposobów zapoznania się z architekturą Internetu jest skupienie się na komunikacji w warstwie aplikacji pomiędzy komputerem źródłowym, docelowym i komputerami pośredniczącymi w tej wymianie informacji. Umieszczenie identycznych egzemplarzy aplikacji na wszystkich komputerach w sieci mogłoby uprościć dostarczanie wiadomości w dużej sieci. Jednak takie rozwiązań nie skaluje się dobrze. Aby nowe oprogramowanie poprawnie działało, trzeba by zainstalować nowe aplikacje na każdym komputerze w sieci. Aby poprawnie działały nowy sprzęt, trzeba by zmodyfikować oprogramowanie. Każda awaria komputera pośredniczącego lub działającej na nim aplikacji spowodowałaby przerwanie łańcucha wymienianych komunikatów.

Internet został oparty na zasadzie połączeń pomiędzy warstwami sieci. Używając jako przykładu modelu OSI można powiedzieć, że celem jest utworzenie niezależnych modułów realizujących poszczególne funkcje sieci. Pozwala to na zróżnicowanie technik wykorzystywanych w sieciach LAN w warstwach 1 i 2 oraz aplikacji działających w warstwach 5, 6 i 7. Model OSI umożliwia odseparowanie szczegółów dotyczących wyższych i niższych warstw. To z kolei umożliwia pośredniczącym urządzeniom sieciowym przekazywanie ruchu bez zajmowania się szczegółami dotyczącymi sieci LAN.

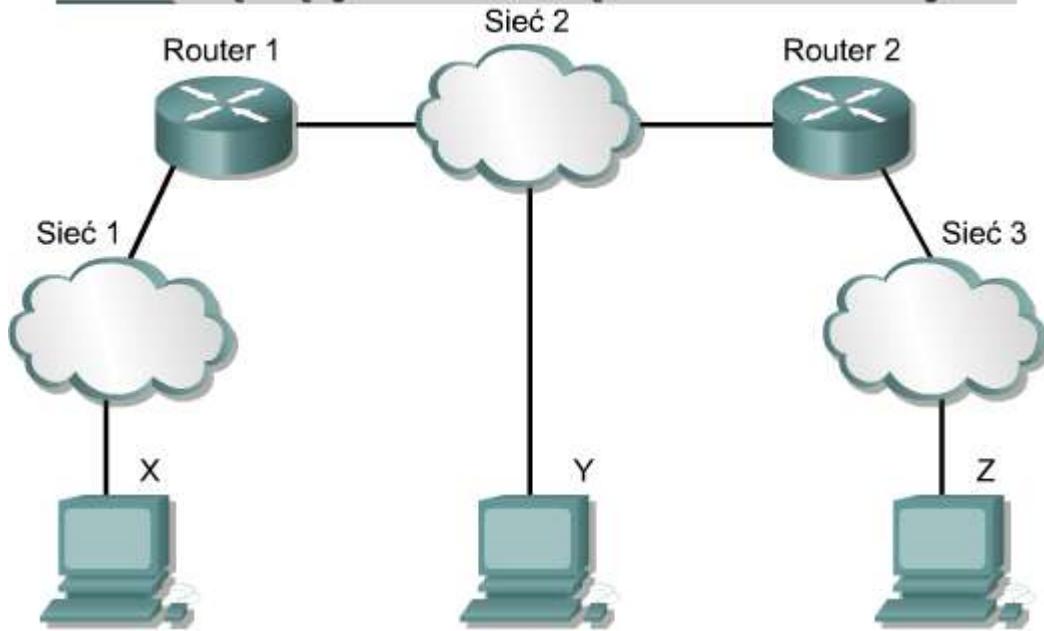
Prowadzi to do koncepcji intersieci, czyli budowania sieci z innych sieci. Sieć złożona z innych sieci jest nazywana internetem (intersiecią), przy czym wyraz ten jest pisany małą literą. Gdy mówimy o sieciach, które powstały z sieci Departamentu Obrony USA, na bazie których działa światowa sieć WWW, używamy pojęcia Internet, pisanego dużą literą. Intersieci muszą się skalować odpowiednio do liczby sieci i przyłączonych komputerów. Muszą one także umożliwiać przenoszenie danych na ogromne odległości. Muszą być na tyle elastyczne, aby uwzględnić ciągłe udoskonalenia techniczne. Jak również muszą być w stanie dostosować się do dynamicznych warunków panujących w sieci. Intersieci powinny być również tanie w utrzymaniu. Poza tym muszą być tak zaprojektowane, aby umożliwiać transmisję danych do dowolnego miejsca o dowolnym czasie.



określa się jako bezpośrednio podłączone do routera. Router jest potrzebny do podejmowania wszystkich wymaganych do komunikacji między tymi sieciami decyzji o wyborze tras. Do obsługi dużego ruchu sieciowego potrzebna jest duża liczba routerów.

Na rysunku obok rozszerzono poprzedni schemat do trzech sieci fizycznych połączonych dwoma routerami. Routery podejmują złożone decyzje, które pozwalają wszystkim użytkownikom we wszystkich sieciach na komunikowanie się pomiędzy sobą. Nie wszystkie sieci są ze sobą bezpośrednio połączone. Router musi umieć radzić sobie z taką sytuacją.

## Router łączący sieć lokalną z sieciami zdalnymi



sytuacji routery przekazują innym routерom komunikaty. Każdy router dzieli się informacjami o tym, do jakich sieci jest przyłączony. Dzięki tym informacjom tworzona jest tablica routingu.

Wymagane przez użytkowników jest ukrycie szczegółów. Jednak fizyczna i logiczna struktura chmury Internetu może być bardzo złożona. Internet gwałtownie rozrósł się, aby mogło z niego korzystać coraz więcej użytkowników. Fakt, że Internet powiększył się na tyle, że zawiera ponad 90 000 routerów szkieletowych oraz 300 000 000 użytkowników końcowych, świadczy o tym, że jego architektura jest oparta na solidnych podstawach.

Dwa komputery znajdujące się w dowolnych miejscach na świecie mogą komunikować się bez problemów, jeżeli tylko spełniają pewne specyfikacje dotyczące sprzętu, oprogramowania i protokołów. Standardyzacja sposobów i procedur przesyłania danych pomiędzy sieciami umożliwiła utworzenie Internetu.

### 9.2. Adresy

#### internetowe

##### 9.2.1 Adresowanie IP

Aby dwa systemy mogły się komunikować, muszą mieć możliwość zidentyfikowania i odnalezienia siebie nawzajem. Chociaż adresy przedstawione na rysunku nie są prawdziwymi adresami sieciowymi, ilustrują jednak pojęcie grupowania adresów.

Komputer może być przyłączony do więcej niż jednej sieci. W takiej sytuacji komputerowi

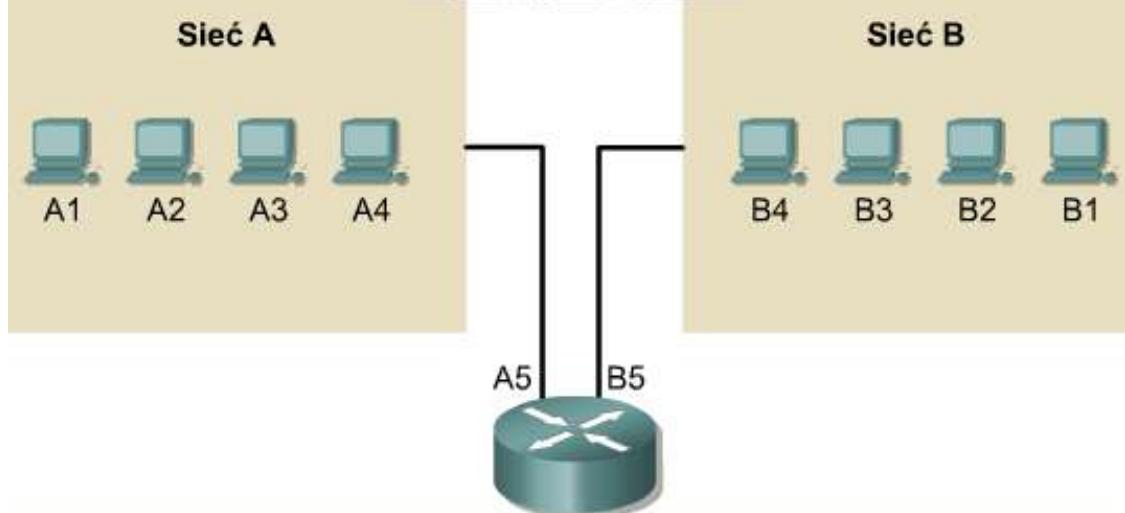
musi zostać przypisany więcej niż jeden adres. Każdy z tych adresów identyfikuje wtedy połączenie komputera z inną siecią. Nie mówi się, że urządzenie ma adres, ale że każdy punkt przyłączenia, czyli interfejs urządzenia, ma adres w danej sieci. Pozwala to innym komputerom zlokalizować takie urządzenie w odpowiedniej sieci.

Połączenie litery (adresu sieci) i liczby (adresu hosta) tworzy unikatowy adres każdego urządzenia w sieci.

Każdemu komputerowi w sieci TCP/IP trzeba przypisać unikatowy identyfikator, czyli adres IP. Adres ten należy

Jedną z możliwości jest przechowywanie przez router listy wszystkich komputerów i wszystkich ścieżek do nich. Na tej podstawie router mógłby decydować, w jaki sposób przekazywać pakiety danych. Przekazywanie opiera się na adresie IP komputera docelowego. Takie rozwiązanie stało się niewygodne, gdyby wzrosła liczba użytkowników. Lepiej skaluje się rozwiązanie, w którym router przechowuje listę wszystkich sieci, ale pozostawia lokalne dostarczenie pakietów lokalnej sieci fizycznej. W tej

### Adresy hostów



Chociaż podane adresy nie są prawdziwe, jednak obrazują ideę grupowania adresów. Litery A i B oznaczają tutaj sieć, a kolejne liczby identyfikują poszczególne hosty. Połączenie litery (adresu sieci) i liczby (adresu hosta) tworzy unikatowy adres każdego urządzenia w sieci.

### Format adresu IP

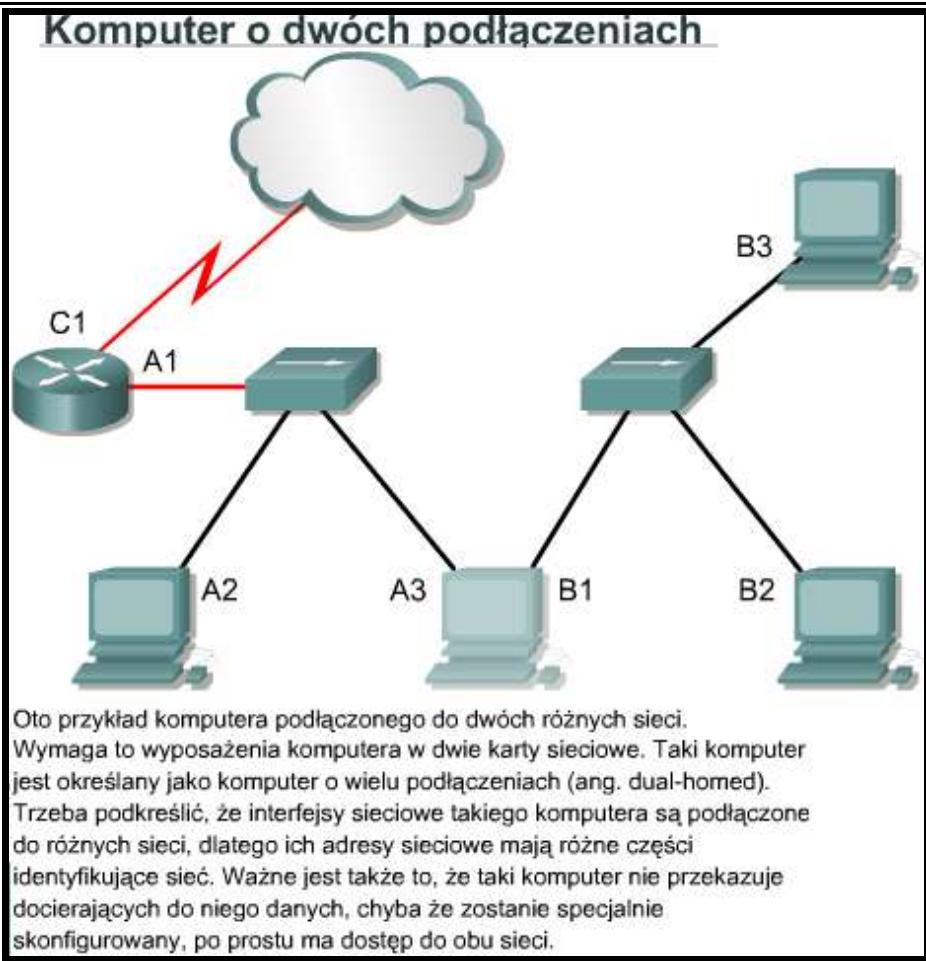


32 bity

do warstwy 3 i pozwala jednemu komputerowi w sieci zlokalizować inny. Wszystkie komputery mają także

unikatowy adres fizyczny zwany adresem MAC. Adresy te są nadawane przez producentów kart sieciowych i należą do warstwy 2 modelu OSI.

**Adres IP jest 32-bitową sekwencją zer i jedynek.** Na rysunku pokazano przykładową liczbę 32-bitową. W celu ułatwienia korzystania z adresów IP zwykle zapisuje się je w postaci czterech liczb dziesiętnych oddzielonych kropkami. Na przykład adres IP pewnego komputera może być równy 192.168.1.2. Inny komputer może mieć adres 128.10.2.1. Ten sposób zapisywania adresów jest nazywany notacją dziesiętną kropkową. W tej notacji każdy adres IP jest zapisywany w czterech częściach oddzielonych kropkami. Każda część adresu jest nazywana oktetem, ponieważ składa się z ośmiu cyfr w systemie dwójkowym. Na przykład adres IP 192.168.1.8 zapisany w systemie dwójkowym ma postać



11000000.10101000.00000001.00001000. Notacja dziesiętna kropkowa jest łatwiejsza do zrozumienia w porównaniu do zapisu dwójkowego. Pomaga ona uniknąć wielu pomyłek, które powstałyby w wypadku użycia jedynie liczb dwójkowych.

Używając notacji kropkowej, łatwiej dostrzec wzory, w jakie układają się liczby. Przedstawione na rysunku liczby w zapisie dwójkowym i dziesiętnym kropkowym reprezentują te same wartości, ale łatwiej porównywać wartości zapisane w notacji dziesiętnej. Jest to jeden z głównych problemów przy bezpośredniej pracy z liczbami dwójkowymi. Długie ciągi powtarzanych jedynek i zer powodują, że łatwiej o pominięcie lub zamianę cyfr. Pomiędzy adresami 192.168.1.8 i 192.168.1.9 łatwo można zauważycią związek, ale jest on już mniej widoczny w wypadku adresów 11000000.10101000.00000001.00001000 i 11000000.10101000.00000001.00001001. Patrząc na zapis w systemie dwójkowym, trudno jest zauważycią, że są to kolejne liczby.

### Wartości dwójkowe i dziesiętne

Dwójkowo: 11000000.10101000.00000001.00001000 oraz 11000000.10101000.00000001.00001001

Dziesiętnie: 192.168.1.8 oraz 192.168.1.9

Zarówno liczby dwójkowe, jak i dziesiętne odpowiadają tym samym wartościami. Znacznie łatwiej jest nam jednak posługiwać się liczbami dziesiętnymi rozdzielonymi kropkami. Jest to jeden z często spotykanych problemów przy bezpośredniej pracy z liczbami dwójkowymi. W długichłańcuchach powtarzających się zer i jedynek bardziej prawdopodobne jest przestawienie lub pominięcie cyfr.

#### 9.2.2 Zamiana liczb dziesiętnych i dwójkowych

Każdy problem można rozwiązać na wiele sposobów. Również w wypadku zamiany liczb dziesiętnych na dwójkowe istnieje szereg różnych metod. Poniżej przedstawiono jedną z nich, nie jest to jednak metoda jedyna. Uczestnik kursu może uznać inne metody za prostsze. Jest to kwestia osobistych upodobań.

Przy zamianie liczby dziesiętnej na dwójkową trzeba znaleźć taką największą potęgę dwójką, która mieści się w liczbie dziesiętnej. Jeżeli proces zamiany dotyczy komputerów, najlepiej rozpocząć od największych wartości, które mieszczą się w jednym lub dwóch bajtach. Jak już wcześniej wspomniano, najczęściej bity grupują się po osiem i taka grupa tworzy jeden bajt. Jednak czasami największa liczba możliwa do zapisania przy użyciu jednego bajtu jest zbyt mała w stosunku do potrzebnej wartości. W tym celu łączy się bajty. Zamiast dwóch liczb ośmioróżowych tworzy się jedną liczbę 16-bitową. Zamiast trzech liczb ośmioróżowych — jedną 24-bitową. Obowiązują wtedy takie same reguły, jak dla liczb 8-bitowych. Aby uzyskać wartość w danej kolumnie, należy pomnożyć przez dwa wartość z kolumny poprzedniej.

Ponieważ przy pracy z komputerami najczęściej korzysta się z bajtów, najlepiej rozpocząć obliczenia od granic bajtów. Zaczniemy od kilku przykładów. Najpierw zamieńmy liczbę 6783. Ponieważ liczba ta jest większa od 255, największej wartości mieszczącej się w jednym bajcie, będziemy używać dwóch bajtów. Zaczynamy więc liczenie od  $2^{15}$ . Liczba 6783 zapisana w systemie dwójkowym jest równa 00011010 01111111.

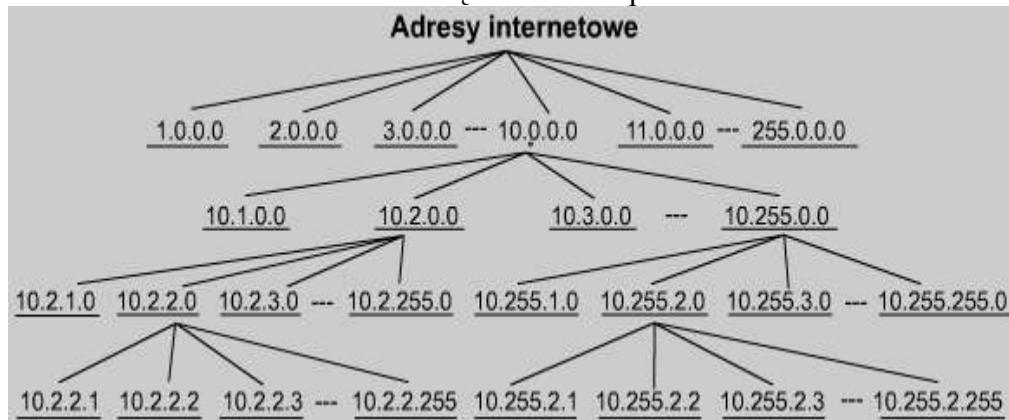
Drugim przykładem jest liczba 104. Ponieważ jest ona mniejsza niż 255, będziemy ją przedstawiać za pomocą jednego bajta. Dwójkowym odpowiednikiem liczby 104 jest liczba 01101000.

Metoda ta jest skuteczna w wypadku dowolnej liczby dziesiętnej. Rozważmy liczbę dziesiątną równą milion. Ponieważ milion jest większy niż największa wartość mieszcząca się w dwóch bajtach (liczba 65 535), trzeba użyć przynajmniej trzech bajtów. Mnożąc kolejne wartości przez dwa, otrzymujemy dla 24 bitów, czyli trzech bajtów, wartość 16 777 215. Oznacza to, że największa wartość mieszcząca się w trzech bajtach to 16 777 215. Tak więc rozpoczynamy liczenie od 24-go bitu i kontynuujemy aż do osiągnięcia zera. Wykonując opisaną wcześniej procedurę, możemy stwierdzić, że liczbie dziesiętnej jeden milion odpowiada liczba dwójkowa 00001111 01000010 01000000.

Zamiana liczb dwójkowych na dziesiętne jest procesem odwrotnym. Wystarczy po prostu umieścić liczbę dwójkową w tabeli; jeżeli w danej kolumnie występuje cyfra jeden, należy dodać odpowiadającą jej wartość do wyniku. Zamieńmy liczbę 00000100 00011101 na wartość dziesiętną. Wynikiem jest liczba 1053.

### 9.2.3 Adresowanie IPv4

Do przekazywania pakietów z sieci źródłowej do sieci docelowej router używa protokołu IP. Pakiety muszą zawierać zarówno identyfikator sieci źródłowej, jak i docelowej. Używając adresu IP sieci docelowej, router może dostarczyć pakiet do odpowiedniej sieci. Gdy pakiet przybywa do routera połączonego z siecią docelową, router ten używa adresu IP do zlokalizowania konkretnego komputera w tej sieci. System ten działa podobnie do poczty. Przy przesyłaniu listu należy najpierw na podstawie kodu dostarczyć go do urzędu pocztowego w mieście docelowym. Ten urząd pocztowy musi odnaleźć punkt docelowy w danym mieście na podstawie nazwy ulicy i numeru domu. Proces ten składa się z dwóch etapów.



Podobnie każdy adres IP składa się z dwóch części. Jedna część identyfikuje sieć, do której komputer jest przyłączony, a druga identyfikuje ten komputer w sieci docelowej. **Jak pokazano na rysunku**, każdy oktet może przedstawać liczbę od 0 do 255. Każdy z oktetów wyznacza 256 grup, a każda z nich dzieli się na 256 podgrup, z których każda zawiera 256

adresów. Korzystając z adresu grupy znajdującej się bezpośrednio na wyższym poziomie hierarchii nad rozpatrywaną grupą, można opisywać wszystkie grupy, na które dzieli się ten adres, za pomocą pojedynczej jednostki.

Adres taki jest nazywany adresem hierarchicznym, ponieważ składa się z różnych poziomów. W adresie IP dwa identyfikatory połączone są w jedną liczbę. Liczba ta musi być unikatowa, bowiem w przeciwnym wypadku niemożliwy byłby routing pakietów. Pierwsza część identyfikuje adres sieci, w której znajduje się dany system. Druga część, zwana częścią hosta, identyfikuje pojedyncze urządzenie w tej sieci.

Adresy IP są podzielone na klasy, które definiują wielkie, średnie i małe sieci. Adresy klasy A są przypisywane sieciom великим. Adresy klasy B są przeznaczone dla sieci średnich, a klasy C — dla sieci małych. Przy określaniu, która część adresu identyfikuje sieć, a która hosta, pierwszym krokiem jest określenie klasy adresu IP.

### Klasy adresów IP

Klasa adresu	Liczba sieci	Liczba hostów w sieci
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (rozsyłanie grupowe)	nd.	nd.

\* Zakres adresów 127.x.x.x jest zarezerwowany na adres pętli zwrotnej, który jest używany do testowania i celów diagnostycznych.

## Rozpoznawanie klas adresów

Klasa adresu IP	Bitły najbardziej znaczące	Zakres adresów pierwszego oktetu	Liczba bitów w adresie sieci
Klasa A	0	0 - 127 *	8
Klasa B	10	128 - 191	16
Klasa C	110	192 - 223	24
Klasa D	1110	224 - 239	28

\* Zakres adresów 127.x.x.x jest zarezerwowany na adres pętli zwrotnej, który jest używany do testowania i celów diagnostycznych.

### 9.2.4 Adresy IP klas A, B, C, D i E

Aby dostosować się do potrzeb sieci o różnych rozmiarach oraz ułatwić ich klasyfikowanie, adresy IP zostały podzielone na grupy zwane klasami. Podział ten jest nazywany adresowaniem klasowym. Każdy pełny 32-bitowy adres IP można podzielić na część identyfikującą sieć i część identyfikującą hosta. Bit lub zestaw bitów na początku każdego adresu określa jego klasę. Istnieje pięć klas adresów IP, co pokazano na rysunku.

Adresy klasy A zostały przeznaczone dla wyjątkowo dużych sieci i mogą zawierać ponad 16 milionów adresów hostów. Adresy klasy A do identyfikacji sieci używają tylko pierwszego oktetu. Pozostałe trzy oktety stanowią adres hosta.

Pierwszy bit adresu klasy A jest zawsze równy 0. W takim przypadku najmniejsza możliwa do przedstawienia liczba to 00000000, czyli 0 dziesiętnie, a największa to 01111111, czyli 127 dziesiętnie. Liczby 0 i 127 są zarezerwowane i nie można ich używać jako adresów sieci.

Każdy adres, którego pierwszy oktet ma wartość z przedziału od 1 do 126, jest adresem klasy A. Adres sieciowy 127.0.0.0 jest zarezerwowany na potrzeby testowania pętli zwrotnej.

Routery lub inne urządzenia mogą używać tego adresu do wysyłania pakietów do samych siebie. Tak więc liczby tej nie można przypisać żadnej sieci.

Adresy klasy B zostały przeznaczone na potrzeby sieci średnich i dużych. Adres IP klasy B do identyfikacji sieci używa pierwszych dwóch z czterech oktetów. Pozostałe dwa oktety określają adres hosta.

Pierwsze dwa bity pierwszego oktetu

adresu klasy B są zawsze równe 10. Pozostałe sześć bitów może zawierać jedynki lub zera. Tak więc najmniejszą liczbą, która może reprezentować adres klasy B, jest 10000000, czyli 128 dziesiętnie, a największą — 10111111, czyli 191 dziesiętnie. Każdy adres, którego pierwszy oktet ma wartość z przedziału od 128 do 191, jest adresem klasy B.

Spośród wszystkich klas adresów najczęściej wykorzystywana jest klasa C. Ta przestrzeń adresowa została przeznaczona dla małych sieci, zawierających maksymalnie 254 hosty.

Adres klasy C zaczyna się od dwójkowej wartości 110. Tak więc najmniejszą możliwą do przedstawienia liczbą jest 11000000, czyli 192 dziesiętnie, a największą — 11011111, czyli 223 dziesiętnie. Adres zawierający w pierwszym oktacie wartość z przedziału od 192 do 223 jest adresem klasy C.

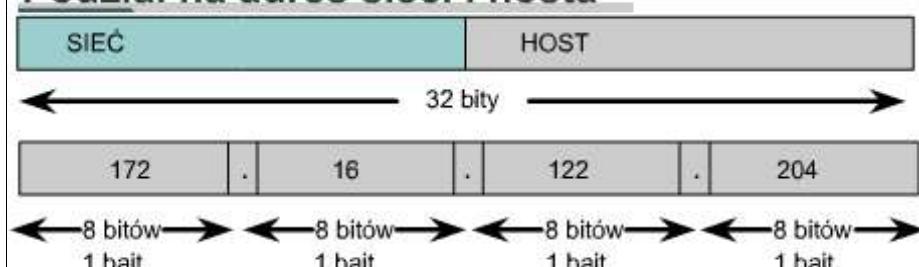
Klasa D została utworzona w celu umożliwienia rozsyłania grupowego przy użyciu adresów IP. Adres rozsyłania grupowego jest unikatowym adresem sieciowym, który kieruje pakiety o tym adresie docelowym do

### Przedrostki klas adresów

Klasa A	Sieć	Host		
Octet	1	2	3	4
Klasa B	Sieć	Host		
Octet	1	2	3	4
Klasa C	Sieć	Host		
Octet	1	2	3	4
Klasa D	Host			
Octet	1	2	3	4

Adresy klasy D są używane przez grupy przy rozsyłaniu grupowym. Nie trzeba przydzielać oktetów lub bitów w celu rozdzielenia adresu sieci i hosta. Adresy klasy E są zarezerwowane do badań.

### Podział na adres sieci i hosta



Adres IP można zawsze podzielić na część sieciową i część hosta. W schemacie adresowania klasowego podział ten przebiega zawsze na granicy pełnych oktetów.

zdefiniowanej wcześniej grupy adresów IP. Dzięki temu pojedynczy komputer może przesyłać jeden strumień danych równocześnie do wielu odbiorców.

Przestrzeń adresowa klasy D, podobnie jak pozostałe przestrzenie adresowe, jest matematycznie ograniczona. Pierwsze cztery bity adresu klasy D muszą być równe 1110. Tak więc w przypadku adresów klasy D wartość pierwszego oktetu należy do zakresu od 11100000 do 11101111, czyli od 224 do 239 dziesiątkiem. Adres IP zawierający w pierwszym oktacie wartości z przedziału od 224 do 239 jest adresem klasy D.

Zdefiniowano także klasę E adresów IP. Adresy te zostały jednak zarezerwowane przez Internet Engineering Task Force (IETF) na potrzeby badawcze. Tak więc nie oddano do publicznego użytku żadnych adresów klasy E. Pierwsze cztery bity każdego adresu klasy E mają zawsze wartość 1. Tak więc pierwszy oktet dla adresów klasy E może przyjmować wartości od 11110000 do 11111111, czyli od 240 do 255 dziesiątkiem.

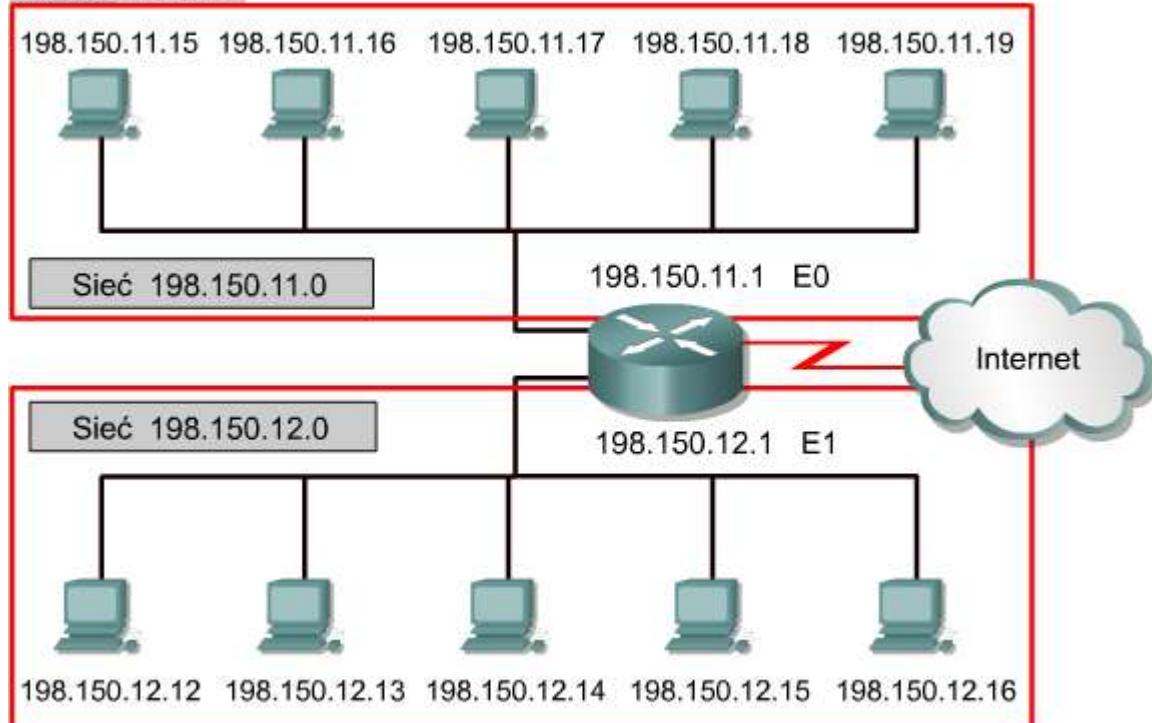
### 9.2.5 Zarezerwowane adresy IP

Niektóre adresy hostów są zarezerwowane i nie można ich przypisać urządzeniom w sieci. Te zarezerwowane adresy hostów to:

**Adres sieci:** używany do identyfikowania samej sieci.

Na rysunku górnego obszar zaznaczony prostokątem reprezentuje sieć 198.150.11.0. Dane wysłane spoza tej sieci do dowolnego należącego do niej hosta (198.150.11.1–198.150.11.254) będą w istocie wysyłane na adres sieci (198.150.11.0). Numery hostów mają znaczenie tylko wtedy, gdy dane przesyłane są w sieci lokalnej. Sieć LAN z dolnego prostokąta działa tak samo jak przedstawiona wyżej. Jedyną różnicą jest adres sieci równy 198.150.12.0.

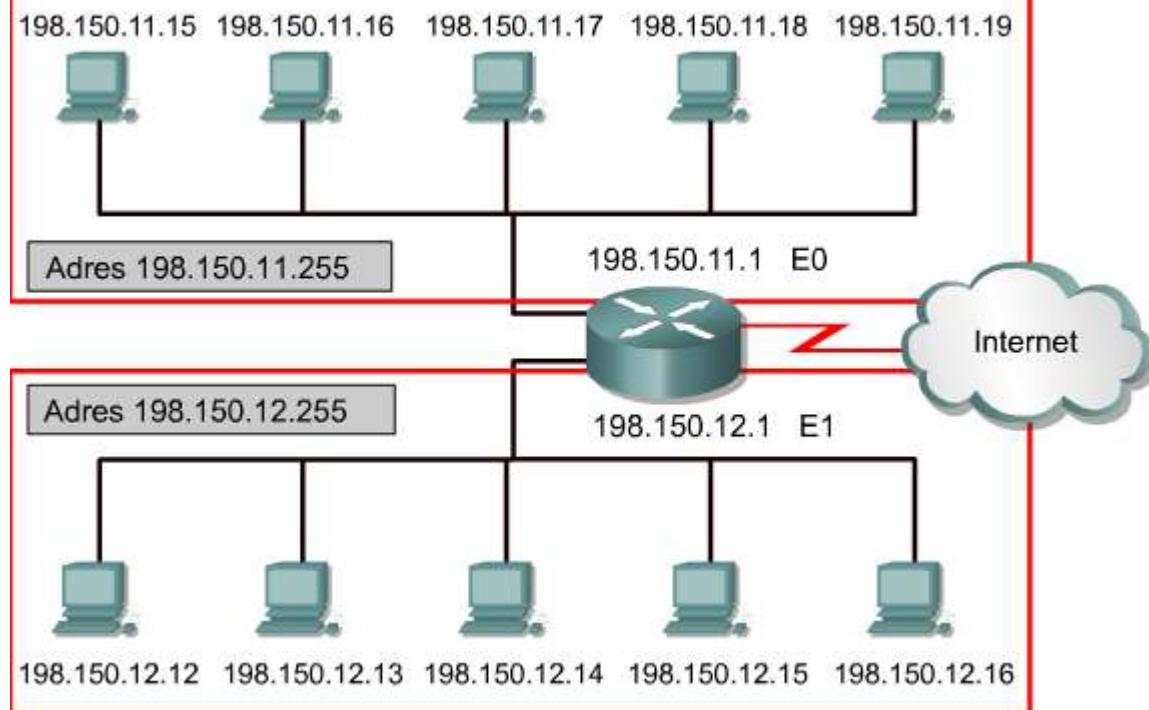
#### Adres sieci



**Adres rozgłoszeniowy:** używany do rozsyłania pakietów do wszystkich urządzeń w sieci.

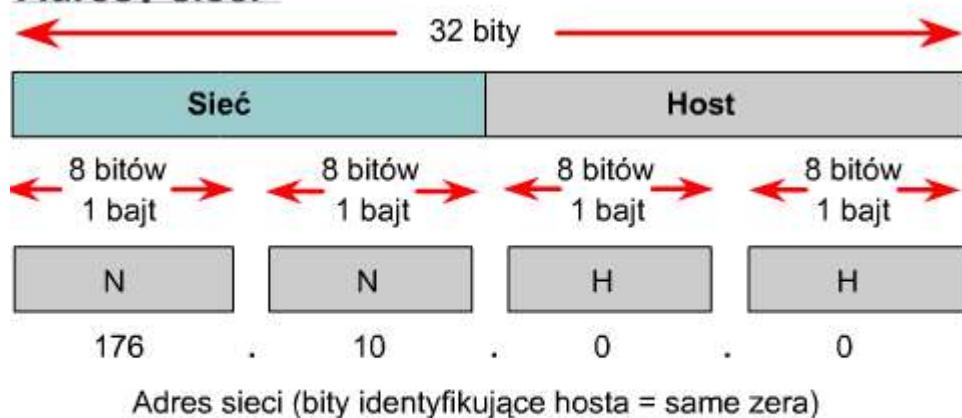
Na rysunku górnego obszar zaznaczony prostokątem reprezentuje adres rozgłoszeniowy 198.150.11.255. Dane wysyłane na ten adres dotrą do wszystkich komputerów w danej sieci (198.150.11.1–198.150.11.254). Sieć LAN z dolnego prostokąta działa tak samo jak przedstawiona wyżej. Jedyną różnicą jest adres rozgłoszeniowy równy 198.150.12.255.

## Adres rozgłoszeniowy



Adres IP, którego część identyfikująca hosta zawiera same zera, jest zarezerwowany jako adres sieci. W przykładowej sieci klasy A adres 113.0.0.0 jest adresem IP sieci (identyfikatorem sieci), która zawiera host 113.1.2.3. Router używa adresu IP sieci do przesyłania danych w Internecie. W przykładowej sieci klasy B adres 176.10.0.0 jest adresem sieci, **co widać na rysunku**.

## Adresy sieci



Ten adres klasy B ma wszystkie bity identyfikujące hosta równe zeru. Powoduje to, że jest on traktowany jako adres sieci.

W adresie sieciowym klasy B pierwsze dwa oktety są przeznaczone na część identyfikującą sieć. Pozostałe dwa oktety (czyli 16 bitów) zawierają zera, ponieważ są przeznaczone na część identyfikującą hosta i są używane do identyfikacji urządzeń przyłączonych do sieci. Na przykład adres IP 176.10.0.0 jest adresem sieci. Adres taki nigdy nie zostanie przypisany jako adres hosta.

Adresem hosta w sieci 176.10.0.0 mógłby być adres 176.10.16.1. W tym przykładzie „176.10” to część identyfikująca sieć, a „16.1” —

hosta.



Aby wysłać dane do wszystkich urządzeń w sieci, potrzebny jest adres rozgłoszeniowy. Rozgłaszenie to rozsyłanie danych do wszystkich urządzeń w sieci. Aby zagwarantować przetworzenie rozgłoszonych danych przez wszystkie urządzenia w sieci, komputer wysyłający musi użyć takiego adresu docelowego, który zostanie rozpoznany i przetworzony. Adresy rozgłoszeniowe mają część identyfikującą hosta wypełnioną jedynek (przy zapisie adresu w systemie dwójkowym). W przykładowej sieci 176.10.0.0 ostatnie 16 bitów stanowi pole hosta, czyli część identyfikującą go.

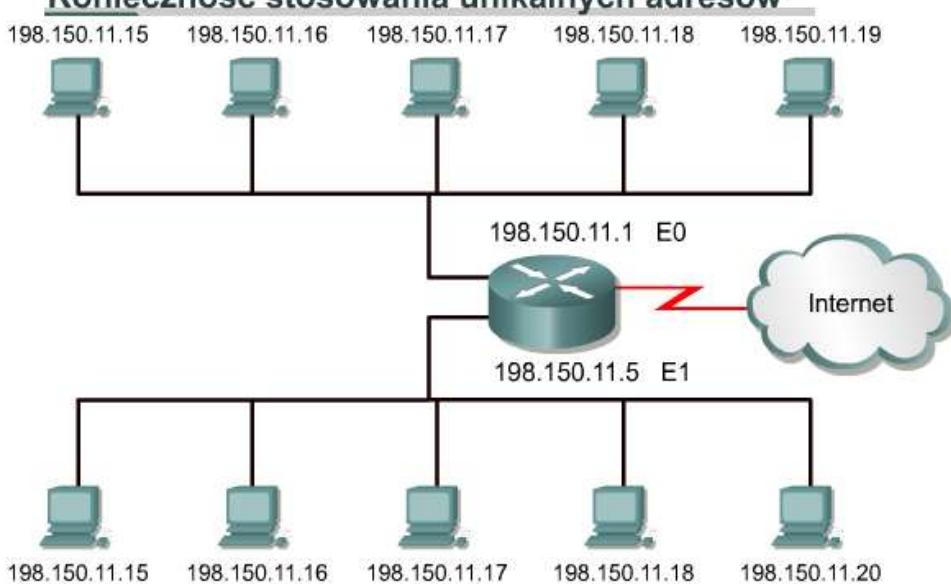
Pakiet rozgłoszeniowy wysyłany do wszystkich urządzeń w tej sieci zawierałby adres docelowy 176.10.255.255. Liczba 255 pojawia się dlatego, że jest to wartość oktetu zawierającego liczbę dwójkową 11111111.

## 9.2.6 Publiczne i prywatne adresy IP

Stabilność działania Internetu zależy bezpośrednio od niepowtarzalności używanych publicznie adresów sieciowych. Na rysunku przedstawiono problem związany ze schematem adresowania sieci.

Widac, że obydwie sieci mają adres 198.150.11.0. W tej sytuacji router nie byłby w stanie prawidłowo przekazywać pakietów danych. Podwojone adresy sieciowe IP uniemożliwiają routerowi wykonywanie zadania, którym jest wybieranie najlepszej ścieżki. Każde urządzenie w sieci wymaga unikatowego adresu.

Konieczne było opracowanie



procedury zapewniającej rzeczywistą unikalność adresów. Początkowo zajmowała się tym organizacja Internet Network Information Center (InterNIC). Organizacja InterNIC już nie istnieje, a jej miejsce zajęła organizacja Internet Assigned Numbers Authority (IANA). IANA ostrożnie rozporządza pozostałą pulą adresów IP, aby nie wystąpiło powielenie publicznie używanych adresów. Sytuacja taka spowodowałaby niestabilność Internetu oraz utrudniłaby dostarczanie datagramów do sieci.

Publiczne adresy IP są unikatowe. Żadne dwa komputery połączone z publiczną siecią nie mogą mieć takich samych adresów IP, ponieważ publiczne adresy IP są globalne i zestandardyzowane. Wszystkie urządzenia podłączone do Internetu stosują się do tego systemu. Publiczny adres IP można otrzymać za pewną opłatą od dostawcy usług internetowych (ISP) lub z rejestru odpowiedniego dla danego regionu.

W związku z gwałtownym rozwojem Internetu publiczne adresy IP zaczęły się wyczerpywać. Aby rozwiązać ten problem, opracowano nowe systemy adresowania, takie jak bezklasowy routing międzydomenowy CIDR (classless interdomain routing) i IPv6. Systemy CIDR i IPv6 zostaną omówione w dalszej części kursu.

Innym rozwiązaniem problemu zbliżającego się wyczerpania publicznych adresów IP jest korzystanie z adresów prywatnych. Jak już wspomniano, w sieciach publicznych hosty muszą mieć unikatowe adresy IP. Jednak prywatne, nie podłączone do Internetu sieci mogą używać dowolnych adresów hostów, jeśli tylko adresy te są unikatowe wewnętrz sieci prywatnej. Obok sieci publicznych istnieje wiele sieci prywatnych. Nie zaleca się jednak używania w prywatnej sieci dowolnych adresów, ponieważ kiedyś sieć taka może zostać podłączona do Internetu. W dokumencie RFC 1918 zarezerwowano trzy bloki adresów IP do prywatnego, wewnętrznego użytku.

Te trzy bloki to jedna klasa A, zakres adresów klasy B oraz zakres adresów klasy C. Adresy należące do tych zakresów nie są routowane w sieci szkieletowej Internetu. Routery internetowe natychmiast odrzucają adresy prywatne. Przypisując adresy w niepublicznym intranecie, sieci testowej lub domowej, można używać tych adresów zamiast adresów globalnie unikatowych. Podłączenie do Internetu sieci używającej adresów prywatnych wymaga translacji adresów prywatnych na adresy publiczne. Proces translacji jest określany jako translacja adresów sieciowych NAT (*Network Address Translation*). Zwykle proces translacji NAT jest wykonywany przez router. Technika NAT, razem z technikami CIDR i IPv6, zostanie szczegółowo opisana w dalszej części materiałów szkoleniowych.

### 9.2.7 Wprowadzenie do podziału na podsieci

Podział na podsieci jest kolejną metodą zarządzania adresami IP. Sieć 131.108.0.0 została podzielona na podsieci: 131.108.1.0, 131.108.2.0 i 131.108.3.0. Dodatkowo metoda ta zapobiega całkowitemu wyczerpaniu adresów IP. Opis sieci TCP/IP byłby niekompletny bez przedstawienia podziału na podsieci. Dla administratora systemu podział na podsieci jest sposobem na wydzielenie i zaadresowanie oddzielnych części sieci LAN. Małą sieć nie zawsze trzeba dzielić na podsieci. Jest to jednak konieczne w przypadku dużych lub bardzo dużych sieci. Podział na podsieci oznacza wykorzystanie maski podsieci do podzielenia sieci na mniejsze, bardziej efektywne i łatwiejsze w zarządzaniu segmenty, czyli podsieci. Można to porównać do systemu numeracji telefonicznej, który składa się z numerów regionów, central i numerów lokalnych.

Administrator musi rozwiązać te problemy przy tworzeniu i rozszerzaniu sieci. Ważne jest, aby wiedzieć, ile jest potrzebnych podsieci lub sieci, oraz ile hostów będzie potrzebnych w każdej z nich. Jeśli korzystamy z podziału na podsieci, nie musimy ograniczać się do domyślnych masek sieci klasy A, B lub C, dzięki czemu możliwe jest bardziej elastyczne projektowanie sieci.

Adresy podsieci zawierają część identyfikującą sieć oraz pole podsieci i pole hosta. Pole podsieci i pole hosta są tworzone z części przeznaczonej pierwotnie na adres hosta w całej sieci. Możliwość zdecydowania, w jaki sposób podzielić oryginalną część identyfikującą hosta na nowe pola podsieci i hosta, umożliwia administratorowi sieci elastyczny sposób adresowania. Aby utworzyć adres podsieci, administrator pożyczca bity z pola hosta i przeznacza je na pole podsieci. Minimalna liczba pożyczanych bitów wynosi dwa. Gdyby tworząc podsieć, pożyczyc tylko jeden bit, numerem sieci byłaby sieć .0.

Adresem rozgłoszeniowym byłaby wtedy sieć .255. Maksymalnie można pożyczyc dowolną liczbę bitów, jeżeli tylko pozostawi się przynajmniej dwa bity na numer hosta.

### Podręczna tablica korzystania z podsieci

Pierwszy oktet numeru hosta w notacji dziesiętnej	Liczba podsieci	Liczba hostów klasy A w podsieci	Liczba hostów klasy B w podsieci	Liczba hostów klasy C w podsieci
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

### 9.2.8 IPv4 kontra IPv6

Gdy w latach 80. zaczęto wprowadzać system TCP/IP, korzystał on z dwupoziomowego schematu adresowania. W tamtych czasach było to wystarczająco skalowalne rozwiązanie. Niestety, twórcy protokołów TCP/IP nie mogli przewidzieć, że ich dzieło stanowić będzie podstawę globalnej sieci wymiany informacji, handlu i rozrywki. W ciągu ostatnich dwudziestu lat protokół IP wersja 4 (IPv4) oferował strategię adresowania, która, choć skalowalna w owym czasie, powodowała nieefektywne przydzielanie adresów.

Adresy klas A i B stanowią 75 procent przestrzeni adresowej IPv4, jednak możliwe jest przydzielić tylko mniej niż 17 000 organizacji. Adresów sieci klasy C jest znacznie więcej niż adresów klas A lub B, jednak stanowią one jedynie 12,5 procent wszystkich możliwych czterech miliardów adresów IP.

Niestety, adresy klasy C są ograniczone do 254 hostów. Jest to zbyt mało, aby zaspokoić potrzeby większych organizacji, które nie mogą otrzymać adresu klasy A lub B. Nawet gdyby było więcej adresów klas A, B lub C, zbyt wiele adresów sieciowych spowodowałoby zatrzymanie pracy routerów w Internecie na skutek olbrzymich tablic routingu, wymaganych do przechowywania ścieżek do każdej z sieci.

Już w roku 1992 organizacja Internet Engineering Task Force (IETF) określiła dwa następujące problemy:

- Wyczerpywanie pozostały, nieprzypisanych jeszcze adresów sieciowych IPv4. W tym czasie przestrzeń adresowa klasy B była bliska wyczerpania.
- Gwałtowny wzrost rozmiarów tablic routingu w związku z coraz większą liczbą wchodzących do użycia sieci klasy C. Będący tego rezultatem zalew informacji o nowych sieciach groził uniemożliwieniem efektywnej pracy routerów internetowych;

W ciągu ostatnich dwóch dziesięcioleci utworzono wiele rozszerzeń schematu IPv4. Rozszerzenia te były zaprojektowane w celu zwiększenia efektywności wykorzystania 32-bitowej przestrzeni adresowej. Dwa z ważniejszych rozszerzeń to maski podsieci i bezklasowy routing międzydomenowy CIDR, które zostaną omówione bardziej szczegółowo w toku dalszych lekcji.

W międzyczasie zdefiniowano i utworzono jeszcze bardziej skalową wersję protokołu IP, czyli IP wersję 6 (IPv6). Protokół IPv6 używa 128 bitów zamiast 32, stosowanych aktualnie w protokole IPv4. Do reprezentowania tych 128 bitów schemat IPv6 używa liczb szesnastkowych. Schemat IPv6 zawiera 340 sekstylionów adresów. Ta wersja protokołu IP powinna zapewnić wystarczającą liczbę adresów, aby zaspokoić przyszłe potrzeby komunikacyjne.

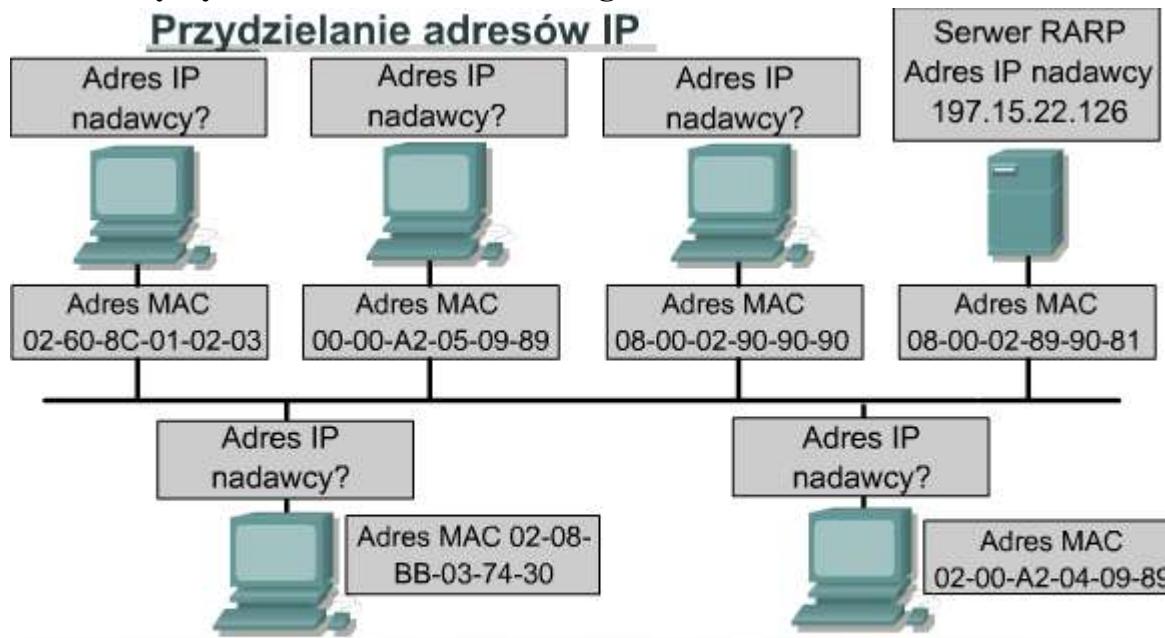
## IPv4 i IPv6

Protokół IP wersja 4 (IPv4)	4 oktety
11010001.11011100.11001001.01110001	
209.156.201.113	
4 294 467 295 adresów IP	
Protokół IP wersja 6 (IPv6)	16 oktetów
10100101.00100100.01110010.11010011	
00101100.10000000.11011101.00000010	
00000000.00101001.11101100.01111010	
00000000.00101011.11101010.01110011	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
$3.4 \times 10^{38}$ adresy IP	

jako separatorów. Poszczególne pola adresu IPv6 mają rozmiar 16 bitów. Aby adresy łatwiej było odczytywać, w każdym polu można pominąć początkowe zera. Pole :0003: zostało zapisane jako :3:. Skrócona reprezentacja 128-bitowego adresu IPv6 używa ośmiu liczb 16-bitowych, przedstawionych w postaci czterech cyfr szesnastkowych. Po latach badań i rozwoju protokół IPv6 jest powoli wprowadzany w wybranych sieciach. Być może w przyszłości protokół IPv6 zastąpi protokół IPv4 jako podstawowy protokół Internetu.

## 9.3 Uzyskiwanie adresu IP

### 9.3.1 Otrzymywanie adresu internetowego



Hosty mają przydzielone adresy fizyczne dzięki karcie sieciowej, która łączy komputer z medium fizycznym. Należy wybrać sposób przydzielania hostowi adresu IP. Istnieją dwie metody przydzielania adresu IP: statyczna i dynamiczna.

Host, aby móc działać w Internecie, musi otrzymać globalnie unikatowy adres.

Fizyczny adres MAC hosta ma znaczenie tylko lokalne, ponieważ identyfikuje hosta w sieci lokalnej. Ponieważ jest to adres warstwy 2, router nie używa go do przekazywania pakietów na zewnątrz sieci LAN.

W komunikacji internetowej najczęściej używane są adresy IP. Protokół ten jest hierarchicznym schematem

adresowania, który pozwala na łączenie pojedynczych adresów i traktowanie ich jako oddzielnych grup. Te grupy adresów pozwalają na efektywny transfer danych w Internecie.

Administratorzy mają dwie możliwości przypisania adresu IP. Mogą to zrobić statycznie lub dynamicznie. W dalszej części tej lekcji przedstawimy adresowanie statyczne oraz trzy warianty adresowania dynamicznego. Niezależnie od wybranego schematu adresowania żadne dwa interfejsy nie mogą mieć takich samych adresów IP. Dwa hosty o tym samym adresie IP mogłyby spowodować konflikt nie pozwalający im poprawnie funkcjonować.

Jak pokazano na rysunku , hosty uzyskują adres fizyczny dzięki temu, że mają kartę sieciową, która umożliwia ich połączenie do medium fizycznego.

### 9.3.2 Statyczne przypisywanie adresu IP

Statyczne przypisywanie działa najlepiej w wypadku małych sieci, w których rzadko zachodzą zmiany. Administrator ręcznie przypisuje i zarządza adresami IP każdego komputera, drukarki lub serwera w intranecie. Prawidłowe zarządzanie zapobiega problemom związanym z powielonymi adresami IP. Jest to możliwe tylko wtedy, gdy trzeba zajmować się jedynie niewielką liczbą urządzeń.

Serwerom należy przypisywać statyczne adresy IP, aby stacje robocze i inne urządzenia zawsze wiedziały, w jaki sposób uzyskać dostęp do wymaganych usług. Wyobraźmy sobie, jak trudno byłoby dodzwonić się do firmy, w której każdego dnia zmieniano by numer telefonu.

Inne urządzenia, którym należy przypisać statyczne adresy IP, to drukarki sieciowe, serwery aplikacji oraz routery.

### 9.3.3 Przypisywanie adresów IP za pomocą protokołu RARP

#### Struktura wiadomości ARP/RARP

bit 015		bit 1631	
Typ sprzętu		Typ protokołu	
HLen (1 bajt)	PLen (1 bajt)	Operacja	
Adres sprzętowy nadawcy (bajty 14)		Adres protokołowy nadawcy (bajty 12)	
Adres sprzętowy nadawcy (bajty 56)		Adres sprzętowy odbiorcy (bajty 12)	
Adres protokołowy nadawcy (bajty 34)		Adres protokołowy odbiorcy (bajty 36)	
Adres sprzętowy odbiorcy (bajty 36)		Adres protokołowy odbiorcy (bajty 14)	
Struktura nagłówka RARP			

urządzeniu poznać własny adres IP. Urządzenia używające protokołu RARP wymagają obecności w sieci serwera RARP, który odpowiada na ich żądania.

#### Opis pól wiadomości ARP/RARP

Pole	Opis
Typ sprzętu	Określa typ interfejsu sprzętowego,dla którego nadawca żąda odpowiedzi.
Typ protokołu	Określa typ adresu protokołu wysokiego poziomu dostarczonego przez nadawcę.
HLen	Długość adresu sprzętowego.
PLen	Długość adresu protokołowego.
Operacja	Używane są następujące wartości: 1. Żądanie ARP. 2. Odpowiedź ARP. 3. Żądanie RARP. 4. Odpowiedź RARP. 5. Dynamiczne żądanie RARP. 6. Dynamiczna odpowiedź RARP. 7. Dynamiczny błąd RARP. 8. Żądanie InARP. 9. Odpowiedź InARP.
Adres sprzętowy (HA) nadawcy	Długość adresu sprzętowego w bajtach (HLen).
Adres protokołowy (PA) nadawcy	Długość adresu protokołowego w bajtach (PLen).
Adres sprzętowy (HA) odbiorcy	Długość adresu sprzętowego w bajtach (HLen).
Adres protokołowy (PA) odbiorcy	Długość adresu protokołowego w bajtach (PLen).

Protokół RARP (*Reverse Address Resolution Protocol*) przypisuje znanemu adresowi MAC adres IP. To przypisanie pozwala urządzeniom sieciowym enkapsulować dane przed wysłaniem ich do sieci. Urządzenie sieciowe, takie jak na przykład bezdyskowa stacja robocza, może znać swój adres MAC, ale nie znać adresu IP. Protokół RARP pozwala

Rozważmy sytuację, gdy urządzenie źródłowe chce wysłać dane do innego urządzenia. W naszym przykładzie urządzenie źródłowe zna swój adres MAC, ale nie może znaleźć własnego adresu IP w tablicy ARP. Aby urządzenie docelowe mogło odebrać dane, przekazać je do wyższych warstw modelu OSI oraz odpowiedzieć urządzeniu źródłowemu, urządzenie źródłowe musi znać zarówno własny adres MAC, jak i adres IP. Tak więc urządzenie źródłowe rozpoczęta proces zwany żądaniem RARP. Żądanie to pomaga urządzeniu źródłowemu wykryć swój adres IP. Żądania RARP są rozglaszane w sieci LAN i odpowiadają na nie serwery RARP, którymi zwykle są routery.

**Protokół RARP używa takiego samego formatu pakietów jak protokół ARP.** Jednak w żądaniu RARP występują inne niż w żądaniu ARP nagłówki MAC i pole kodu operacji. Format pakietu RARP zawiera miejsca dla adresów MAC urządzenia źródłowego i docelowego. Pole źródłowego adresu IP jest puste. Pakiet ten jest rozglaszany wśród wszystkich urządzeń w sieci, dlatego adresem docelowym MAC jest FF:FF:FF:FF:FF:FF.

Stacje robocze używające protokołu RARP mają zapisany w pamięciach ROM kod powodujący rozpoczęcie procesu żądania RARP.

### 9.3.4. Przypisywanie adresów IP za pomocą protokołu BOOTP

#### Struktura wiadomości protokołu BOOTP

bit 07	bit 815	bit 1623	bit 2431
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 bajty)			
Sekundy (2 bajty)			Nieużywane
Ciaddr (4 bajty)			
Yiaddr (4 bajty)			
Siaddr (4 bajty)			
Giaddr (4 bajty)			
Chaddr (16 bajtów)			
Nazwa serwera (64 bajty)			
Nazwa pliku ładowującego (128 bajtów)			
Dane specyficzne dla producenta (64 bajty)			
Struktura wiadomości protokołu BOOTP			

Protokół BOOTP (*Bootstrap Protocol*) działa w środowisku typu klient — serwer i wymaga tylko pojedynczej wymiany pakietów do pobrania informacji o adresie IP. W przeciwnieństwie do protokołu RARP pakiety BOOTP mogą zawierać nie tylko adres IP, ale i adres routera, adres serwera oraz informacje zależne od producenta sprzętu.

Z protokołem BOOTP związany jest problem polegający na tym, że nie został on zaprojektowany do dynamicznego przypisywania adresów. Aby użyć tego protokołu, administrator sieci tworzy plik konfiguracyjny zawierający

parametry dla każdego urządzenia. Administrator musi dodawać do niego hosty i zarządzać bazą danych BOOTP. Choć adresy są przypisywane dynamicznie, nadal istnieje relacja jeden do jednego pomiędzy liczbą adresów IP a liczbą hostów. Oznacza to, że dla każdego hosta IP w sieci musi istnieć profil BOOTP zawierający przypisany mu adres IP. Żadne dwa profile nie mogą zawierać takich samych adresów IP. Profile te mogłyby być użyte w tym samym czasie, co oznaczałoby przypisanie dwóm hostom tego samego adresu IP.

Urządzenie przy starcie używa protokołu BOOTP do pobrania adresu IP. Protokół BOOTP do przesyłania komunikatów używa protokołu UDP. Komunikat UDP jest enkapsulowany w pakiecie IP. Komputer używa protokołu BOOTP do wysłania pakietu rozgłoszeniowego na adres IP składający się z samych jedynek, czyli 255.255.255.255 w notacji dziesiętnej. Serwer BOOTP otrzymuje ten pakiet i w odpowiedzi wysyła również pakiet rozgłoszeniowy. Klient otrzymuje ramkę i sprawdza jej adres MAC. Jeżeli w polu adresu docelowego klient znajdzie swój adres MAC, a w polu adresu docelowego IP adres rozgłoszeniowy, pobierze adres IP i inne informacje zawarte w komunikacie odpowiedzi BOOTP.

#### Opis pól wiadomości protokołu BOOTP

Pole	Opis
Op	Kod operacji dla wiadomości. Wiadomości mogą być typu BOOTREQUEST albo BOOTREPLY
Htype	Typ adresu sprzętowego
HLen	Długość adresu sprzętowego
Hops	Klient wpisuje zero; to pole jest używane przez serwer BOOTP podczas wysyłania żądania do innej sieci
Xid	Identyfikator transakcji
Secs	Liczba sekund, które upłynęły od chwili rozpoczęcia procesu uzyskiwania lub odnawiania adresu
Ciaddr	Adres IP klienta
Yiaddr	"Twój" (klienta) adres IP
Siaddr	Adres IP następnego serwera, który ma być użyty w procesie uruchamiania.
Giaddr	Adres IP agenta przekazującego używany podczas uruchamiania za pośrednictwem takiego agenta.
Chaddr	Adres sprzętowy klienta
Server Host Name	Definiuje określony serwer, z którego mają być pobrane informacje protokołu BOOTP.
Boot File Name	Umożliwia używanie wielu plików uruchomieniowych, dzięki czemu na hostach mogą działać różne systemy operacyjne.
Vendor Specific Area	Zawiera opcjonalne informacje pochodzące od producenta, które mogą zostać przekazane do hosta.

### 9.3.5 Zarządzanie adresami IP przy użyciu protokołu DHCP

#### Struktura wiadomości protokołu DHCP

bit 07	bit 815	bit 1623	bit 2431
Op (1)	Htype (1)	HLen (1)	Hops (1)
	Xid (4 bajty)		
Sekundy (2 bajty)		Flagi (2 bajty)	
	Ciaddr (4 bajty)		
	Yiaddr (4 bajty)		
	Siaddr (4 bajty)		
	Giaddr (4 bajty)		
	Chaddr (16 bajtów)		
	Nazwa serwera (64 bajty)		
	Nazwa pliku ładowającego (128 bajtów)		
	Obszar używany przez producenta (może zostać zmieniony)		
	Struktura wiadomości protokołu DHCP		

Protokół dynamicznej konfiguracji hostów DHCP (*Dynamic Host Configuration Protocol*) jest następcą protokołu BOOTP. W przeciwieństwie do protokołu BOOTP protokół DHCP pozwala hostowi pobierać adres IP dynamicznie, dzięki czemu administrator sieci nie musi tworzyć oddzielnego profili dla każdego urządzenia. Do używania protokołu DHCP konieczne jest jedynie zdefiniowane zakresu adresów IP na serwerze DHCP. Host, przyłączając się do sieci,

kontakuje się z serwerem DHCP i żąda przypisania adresu. Serwer DHCP wybiera adres i wydzierżawia go temu hostowi. Protokół DHCP pozwala na pobranie całej konfiguracji sieciowej komputera w jednym komunikacie.

Oznacza to pobranie wszystkich danych przesyłanych w komunikacie BOOTP oraz wydzierżawionego adresu IP i maski podsieci.

Główną zaletą protokołu DHCP w porównaniu z protokołem BOOTP jest możliwość obsługi użytkowników mobilnych. Mobilność umożliwia użytkownikom swobodną zmianę połączeń sieciowych w zależności od miejsca pracy. Nie ma tutaj występującej w systemie BOOTP potrzeby przechowywania stałego profilu dla każdego urządzenia przyłączonego do sieci. Ważną zaletą protokołu DHCP jest możliwość wydzierżawienia adresu IP oraz odzyskania go w celu przypisania innemu użytkownikowi, gdy pierwszy użytkownik zwolni ten adres. Oznacza to, że protokół DHCP umożliwia utworzenie relacji jeden do wielu między adresami IP i komputerami, a także że adres jest dostępny dla każdego, kto przyłącza się do sieci.

#### Opis pól wiadomości protokołu DHCP

Op	Kod operacji dla wiadomości. Wiadomości mogą być typu BOOTREQUEST albo BOOTREPLY.
Htype	Typ adresu sprzętowego
Hlen	Długość adresu sprzętowego
Hops	Klient wpisuje zero; pole to jest używane przez serwer BOOTP podczas wysyłania żądania do innej sieci.
Xid	Identyfikator transakcji
Secs	Liczba sekund, które upłynęły od chwili rozpoczęcia procesu uzyskiwania lub odnawiania adresu.
Flagi	Flagi
Ciaddr	Adres IP klienta
Yiaddr	"Twój" (klienta) adres IP
Siaddr	Adres IP następnego serwera, który ma być użyty w procesie uruchamiania.
Giaddr	Adres IP agenta przekazującego używany podczas uruchamiania za pośrednictwem takiego agenta.
Chaddr	Adres sprzętowy klienta
Server Host Name	Definiuje określony serwer, z którego mają być pobrane informacje protokołu BOOTP.
Boot File Name	Umożliwia używanie wielu plików uruchomieniowych, dzięki czemu na hostach mogą działać różne systemy operacyjne.
Vendor Specific Area	Zawiera opcjonalne informacje pochodzące od producenta, które mogą zostać przekazane do hosta.

### 9.3.6 Problemy z określaniem adresów

Jednym z głównych problemów w sieciach jest sposób komunikowania się z innymi urządzeniami sieciowymi. W komunikacji TCP/IP datagram w lokalnej sieci musi zawierać zarówno adres MAC, jak i adres IP urządzenia docelowego. Adresy te muszą być prawidłowe i muszą odpowiadać adresom MAC i IP urządzenia docelowego. Jeżeli nie będą pasowały, datagram zostanie odrzucony przez host docelowy. Komunikacja w segmencie sieci LAN wymaga dwóch adresów. Musi istnieć możliwość automatycznego odwzorowywania adresów IP na adresy MAC. Zbyt dużo czasu zajmowałoby użytkownikom tworzenie takich odwzorowań ręcznie. Zestaw protokołów TCP/IP zawiera protokół o nazwie ARP (*Address Resolution Protocol*), który automatycznie pobiera adres MAC dla transmisji lokalnych. Inaczej jest przy wysyłaniu danych poza sieć lokalną.

Komunikacja pomiędzy dwoma segmentami sieci LAN wymaga dodatkowej pracy. Potrzebne są adresy IP i MAC zarówno urządzenia docelowego, jak i pośredniczącego urządzenia routującego. Zestaw protokołów TCP/IP zawiera odmianę protokołu ARP o nazwie proxy ARP, która dostarcza adres MAC urządzenia pośredniczącego w transmisji z sieci LAN do innego segmentu sieciowego

### 9.3.7 Protokół odwzorowania adresów ARP (*Address Resolution Protocol*)

#### Pozycja tablicy ARP

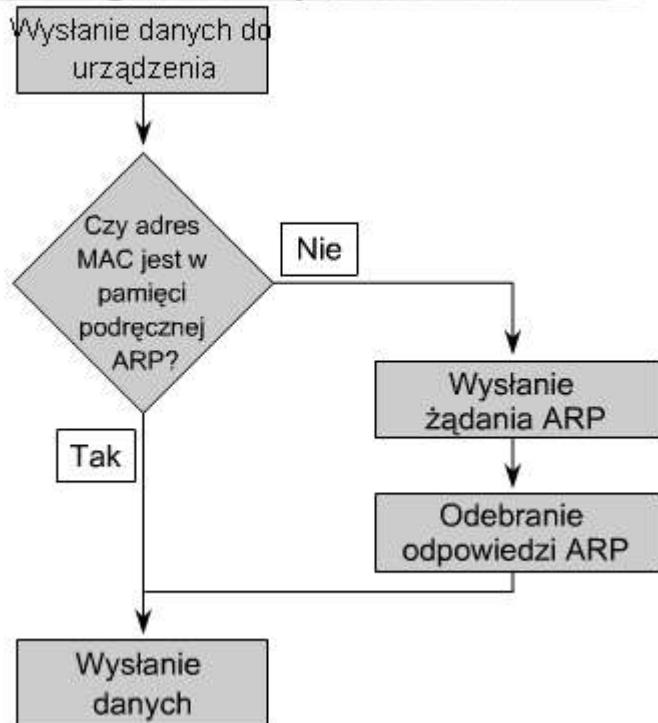
Pozycja tablicy ARP		
Adres internetowy	Adres fizyczny	Typ
68.2.168.1	00-50-57-00-76-84	dynamiczny

Tablica ARP komputera o adresie 198.150.11.36

MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35

IP innych urządzeń podłączonych do tej samej sieci LAN. Tablice te nazywane są tablicami ARP. Przechowywane są one w pamięci RAM urządzenia, które automatycznie zarządza zapamiętanymi informacjami. Bardzo rzadko stosowane jest ręczne dodawanie przez użytkownika wpisów do tablicy ARP. Każde urządzenie w sieci utrzymuje własną tablicę ARP. Gdy urządzenie chce wysłać dane przez sieć, używa informacji zawartych w tej tablicy.

#### Proces korzystania z protokołu ARP



W przypadku sieci TCP/IP pakiet danych musi zawierać zarówno adres MAC, jak i adres IP urządzenia docelowego. Pakiet nie zawierający jednego z nich nie zostanie przekazany z warstwy 3 do warstw wyższych. Dzięki temu adresy MAC i IP służą do wzajemnej kontroli. Gdy urządzenie określi adresy IP urządzeń docelowych, może dodać do pakietów danych docelowe adresy MAC.

Niektóre urządzenia przechowują tablice zawierające adresy MAC i

Gdy urządzenie źródłowe określi docelowy adres IP, przeszukuje tablicę ARP w celu znalezienia adresu MAC urządzenia docelowego. Jeżeli urządzenie źródłowe znajdzie pozycję w tablicy dla docelowego adresu IP i docelowego adresu MAC, skojarzy adres IP z adresem MAC i będzie ich używać do enkapsulacji danych. Pakiet danych może wówczas zostać przesłany poprzez medium sieciowe, po czym zostanie odebrany przez urządzenie docelowe. Istnieją dwie metody zbierania przez urządzenia adresów MAC potrzebnych do enkapsulacji danych. Pierwszą metodą jest monitorowanie ruchu w lokalnym segmencie sieci. Wszystkie stacje w sieci Ethernet analizują ruch, aby sprawdzić, czy dane są przeznaczone dla nich. Częścią tego procesu jest zapisywanie adresu IP i MAC źródła datagramu w tablicy ARP. Zatem podczas przesyłania danych przez sieć pary adresów są umieszczane w tablicy ARP. Innym sposobem pobrania tej pary adresów do transmisji danych jest rozgłoszenie żądania ARP. Komputer potrzebujący pary adresów IP i MAC rozgłasza żądanie ARP. Wszystkie urządzenia w sieci analizują to żądanie. Jeżeli jedno z urządzeń lokalnych będzie miało pasujący do żądania adres IP, wyśle odpowiedź ARP zawierającą parę adresów IP-MAC. W wypadku gdy adres IP należy do sieci lokalnej, a

komputer nie istnieje lub jest wyłączony, nie pojawi się odpowiedź na żądanie ARP. W tej sytuacji urządzenie źródłowe zgłasza błąd. Jeżeli żądanie dotyczy innej sieci IP, można użyć innej metody. Routery nie przekazują pakietów rozgłoszania. Jeżeli włączony jest mechanizm proxy ARP, router korzysta z niej. Protokół proxy ARP jest odmianą protokołu ARP. W tej odmianie router wysyła do hosta odpowiedź ARP z adresem MAC interfejsu, na którym otrzymał żądanie. Router odpowiada takim adresem MAC na żądania, których adres IP nie należy do zakresu adresów podsieci lokalnej.

Inną metodą wysyłania danych na adres urządzenia w innym segmencie sieci jest skonfigurowanie bramy domyślnej. Brama domyślna to opcja hosta umożliwiająca przechowywanie adresu IP interfejsu routera w konfiguracji hosta. Host źródłowy porównuje docelowy adres IP z własnym adresem, aby sprawdzić, czy oba adresy IP znajdują się w tym samym segmencie. Jeżeli host docelowy znajduje się w innym segmencie, host źródłowy wysyła dane, używając prawdziwego adresu IP urządzenia docelowego i adresu MAC routera. Adres MAC routera jest pobierany z tablicy ARP przy użyciu adresu IP routera.

Jeżeli w routerze nie skonfigurowano mechanizmu proxy ARP albo na hoście nie ustawiono bramy domyślnej, ruch sieciowy nie może opuścić sieci lokalnej. Jeden z tych dwóch warunków musi być spełniony, aby uzyskać połączenie z urządzeniami spoza sieci lokalnej.

## **Moduł 10. Podstawy routingu i działanie sieci**

Protokół IP jest najważniejszym protokołem routowanym używanym w Internecie. Zastosowanie adresowania IP pozwala na przesyłanie pakietów ze źródła do celu przy użyciu najlepszej dostępnej ścieżki. Propagacja pakietów, zmiany enkapsulacji, protokoły zorientowane połączeniowo i bezpołączeniowe są równie ważne dla zagwarantowania właściwego przesyłania danych do celu. W tym module dokonano przeglądu wszystkich wymienionych funkcji.

Dla osób poznających zagadnienia sieciowe różnica pomiędzy protokołami routującymi (protokołami routingu) a protokołami routowanymi stanowi źródło częstych pomyłek. Wyrazy te brzmią podobnie, ale mają całkowicie różne znaczenia. W module tym przedstawione zostały także protokoły routingu, które umożliwiają routerom tworzenie tablic pozwalających określić najlepszą ścieżkę do dowolnego hosta w Internecie.

Nie ma dwóch takich samych organizacji na świecie. Co więcej, system adresów podzielonych na trzy klasy (A, B i C) nie jest odpowiedni dla wszystkich organizacji. Jednakże system adresowania z podziałem na klasy pozwala na pewną elastyczność polegającą na możliwości tworzenia podsieci. Zastosowanie podsieci umożliwia administratorom sieci określenie rozmiarów fragmentów sieci, na których będą operować. Po ustaleniu podziału sieci maska podsieci może być użyta do określenia położenia każdego urządzenia w sieci.

### **10.1 Protokół routowany**

#### **10.1.1 Protokoły routowane**

Protokół jest zbiorem reguł określających sposoby wzajemnej komunikacji komputerów w sieci. Komputery porozumiewają się ze sobą poprzez wymienianie wiadomości zawierających dane. Aby komputery mogły przyjąć i przetworzyć te wiadomości, musi być zdefiniowany sposób ich interpretacji. Przykłady wiadomości obejmują te, które ustanawiają połączenia ze zdalnym komputerem, wiadomości e-mail oraz pliki przesyłane przez sieć.

##### **Protokół opisuje:**

- wymagany format wiadomości;
- sposób, w jaki komputery muszą wymieniać wiadomość w kontekście danej operacji.

Zastosowanie protokołu routowanego pozwala na przesyłanie przez router danych między węzłami znajdującymi się w różnych sieciach. Żeby protokół mógł być routowany, musi umożliwiać przydział numeru sieci i numeru hosta każdemu indywidualnemu urządzeniu. Niektóre protokoły, takie jak IPX, wymagają tylko numeru sieci, ponieważ używają one adresu MAC jako numeru hosta. Inne protokoły, np. protokół IP, wymagają kompletnego adresu składającego się z części odpowiadającej sieci oraz hostowi. Aby rozróżnienie tych dwóch części było możliwe, protokoły te wymagają również maski sieci. Adres sieci jest uzyskiwany przez obliczenie iloczynu logicznego adresu i maski sieci.

Maska sieci jest stosowana po to, by umożliwić traktowanie grup następujących po sobie adresów IP jako pojedynczej części. Gdyby nie możliwość grupowania, każdy host musiałby być odwzorowany oddziennie do operacji routingu. Nie byłoby to możliwe przy uwzględnieniu liczby hostów znajdujących się w Internecie, która zgodnie z danymi Internet Software Consortium wynosi około 233 101 500.

#### **10.1.2 Protokół IP jako protokół routowany**

Protokół IP (ang. *Internet Protocol*) jest najszerzej używaną implementacją metody hierarchicznego adresowania w sieci. Protokół IP jest protokołem bezpołączeniowym, zawodnym i realizuje dostarczanie danych przy użyciu dostępnych możliwości. Pojęcie „beopołączeniowy” oznacza, że nie nawiązuje się wydzielonego połączenia przed rozpoczęciem transmisji, jak dzieje się to w wypadku rozmowy telefonicznej. Protokół IP określa najefektywniejszą trasę na podstawie protokołu routingu. Określenia zawodny i realizujący dostarczanie danych przy użyciu dostępnych możliwości nie implikują, że system jest zawodny i nie pracuje dobrze, ale oznaczają, że protokół IP nie dokonuje sprawdzenia, czy dane dotarły do celu. Funkcję tę, jeśli jest wymagana, pełnią protokoły wyższych warstw.

W trakcie przepływu danych przez kolejne warstwy OSI są one przetwarzane na każdym z etapów. W warstwie sieciowej dane podlegają enkapsulacji i przyjmują formę pakietów, zwanych także datagramami. Protokół IP określa zawartość nagłówka pakietu IP, który zawiera dane adresowe oraz inne informacje sterujące, ale nie obejmuje danych właściwych. Protokół IP przyjmuje wszystkie dane przekazywane z wyższych warstw.

#### **10.1.3 Propagacja pakietów oraz przełączanie wewnętrz routera**

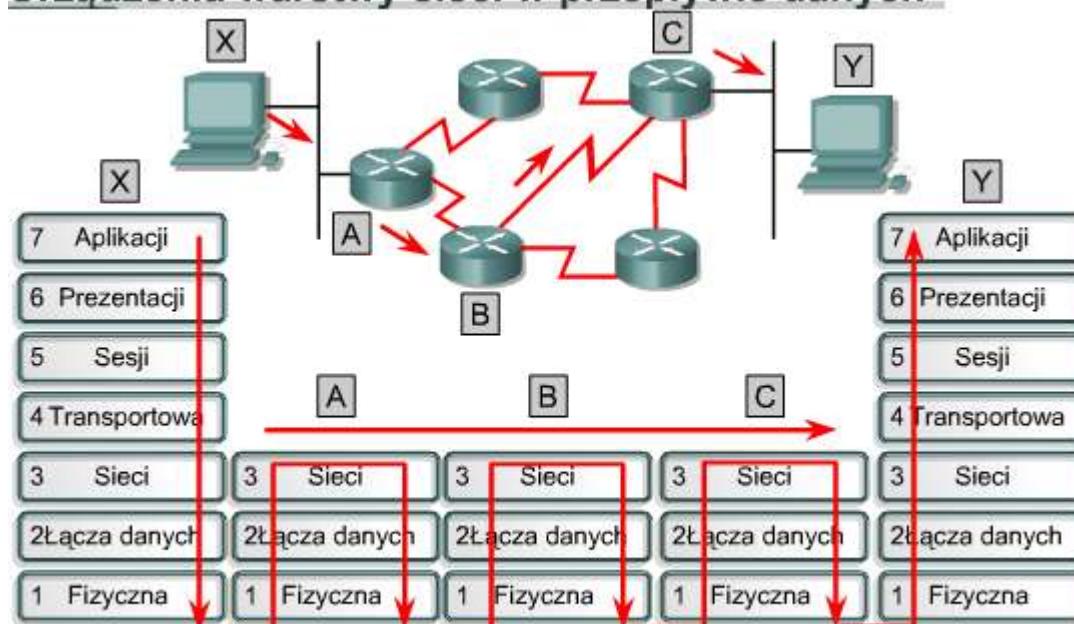
W trakcie przesyłania pakietów w intersieci do miejsca docelowego nagłówki i stopki warstwy 2 są usuwane i zastępowane w każdym urządzeniu warstwy 3. Dzieje się tak dlatego, że jednostki danych warstwy 2 — ramki — przeznaczone są do adresowania lokalnego. Jednostki danych warstwy 3 — pakiety — przeznaczone są do adresowania typu end-to-end.

Ramki Ethernet warstwy 2 są przystosowane do działania w domenie rozgłoszeniowej z wykorzystaniem adresu MAC wbudowanego w urządzenie. Inne typy ramek warstwy 2 stosowane są w szeregowych łączach protokołu PPP (Point-to-Point Protocol) oraz w połączeniach protokołu Frame Relay, gdzie wykorzystywane są inne metody adresowania warstwy 2. Bez względu na użyty typ adresowania warstwy 2 format ramki jest zaprojektowany do

funkcjonowania w ramach domeny rozgłoszeniowej tej warstwy, gdyż po przejściu danych przez urządzenie warstwy 3 informacje warstwy 2 ulegają zmianie.

Po odebraniu ramki w interfejsie routera wyodrębniany jest docelowy adres MAC. Następnie odbywa się sprawdzenie, czy ramka jest adresowana bezpośrednio do interfejsu routera lub jest ramką rozgłoszeniową. W obu wypadkach ramka jest akceptowana. W przeciwnym razie ramka jest odrzucana, ponieważ jest kierowana do innego urządzenia w domenie kolizyjnej. Stopka zaakceptowanej ramki zawiera pole cyklicznej kontroli nadmiarowej (CRC), którego wartość jest wyodrębniana i porównywana z wartością obliczoną w celu potwierdzenia, że dane ramki są wolne od błędów. Jeśli weryfikacja nie powiedzie się, ramka jest odrzucana. Jeśli rezultat sprawdzenia jest pozytywny, nagłówek i stopka ramki są usuwane, a pakiet jest przekazywany do warstwy 3. Tam następuje sprawdzenie, czy jest on kierowany do routera, czy też ma być przesłany do innego urządzenia w intersieci. Jeśli docelowy adres IP odpowiada jednemu z portów routera, nagłówek warstwy 3 jest usuwany i dane są przekazywane do warstwy 4. Jeśli pakiet ma zostać przesłany, docelowy adres IP jest porównywany z adresami znajdującymi się w tablicy routingu. Jeśli odpowiadający adres zostanie odnaleziony albo istnieje trasa domyślna, pakiet będzie wysłany do interfejsu określonego w tablicy routingu. Gdy pakiet jest przełączany do interfejsu wyjściowego, zostaje uzupełniony o odpowiedni nagłówek oraz stopkę zawierający nową wartość cyklicznej kontroli nadmiarowej (CRC). Ramka jest następnie przesyłana do kolejnej domeny rozgłoszeniowej prowadzącej do miejsca docelowego.

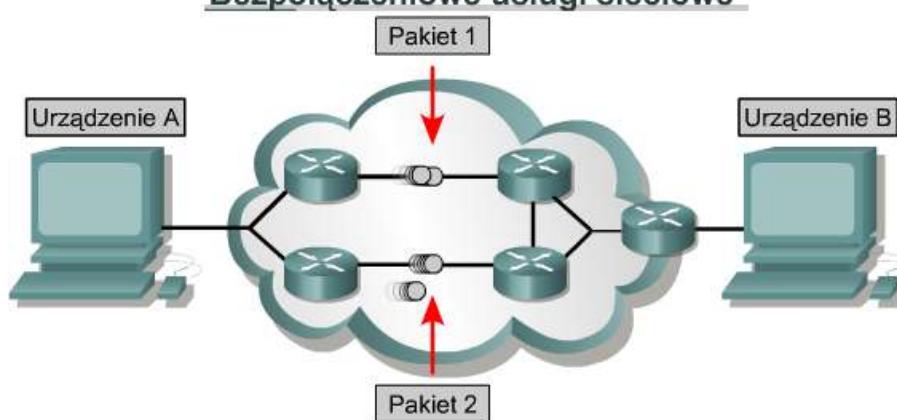
## Urządzenia warstwy sieci w przepływie danych



Każdy router świadczy usługi obsługujące funkcje wyższej warstwy.

### **10.1.4 Protokół IP (ang. Internet Protocol)**

#### Bezpołączeniowe usługi sieciowe



Istnieją dwa rodzaje usług dostarczania danych: zorientowane połączeniowo i bezpołączeniowe. Te dwa typy usług zapewniają właściwe dostarczanie typu end-to-end (czyli pomiędzy punktami końcowymi) danych w intersieci.

W większości sieci używany jest bezpołączeniowy system dostarczania. Różne pakiety mogą podążać różnymi ścieżkami w sieci, ale po osiągnięciu celu są one ponownie składane. W systemie bezpołączeniowym przed wysłaniem pakietu nie nawiązuje się

kontaktu z punktem docelowym. Dobrym porównaniem dla systemu bezpołączeniowego jest system pocztowy. Przed nadaniem przesyłki nikt nie kontaktuje się z odbiorcą, żeby sprawdzić, czy ją przyjmie. Także nadający nie wie, czy list dotarł do celu.

W systemach zorientowanych połączeniowo przed rozpoczęciem przesyłania danych pomiędzy nadawcą i odbiorcą nawiązywane jest połączenie. Przykładem sieci zorientowanej połączeniowo jest systemem telefonicznym. Dzwoniący wybiera numer, nawiązywane jest połączenie i dochodzi do komunikacji.

Bezpołączeniowe procesy sieciowe są często zwane procesami z przełączaniem pakietów. W trakcie przesyłania pakietów ze źródła do celu mogą być one przełączane do różnych ścieżek i mogą osiągnąć miejsce docelowe w innej kolejności. Każdy pakiet zawiera informacje, takie jak adres docelowy i numer kolejny (sekwencyjny), które pozwalają skoordynować go z innymi dochodzącymi pakietami. Pakiety te są zatem składane w odpowiedniej kolejności już po dotarciu do celu. Urządzenia mogą ustalać ścieżkę dla każdego pakietu z osobna przy uwzględnieniu różnych kryteriów. Niektóre kryteria, takie jak dostępne pasmo, mogą więc być różne dla każdego pakietu.

Zorientowane połączeniowo procesy sieciowe często są zwane procesami z komutacją łączy. Przed rozpoczęciem przesyłania danych nawiązywane jest połączenie z odbiorcą, dopiero potem rozpoczyna się transfer danych. Wszystkie pakiety poruszają się jeden po drugim w ramach tego samego obwodu fizycznego lub wirtualnego. Internet jest olbrzymią siecią bezpołączeniową, w której większość pakietów jest dostarczana przy użyciu protokołu IP. Protokół TCP uzupełnia protokół IP o zorientowane połączeniowo usługi warstwy 4 z gwarancją niezawodności.

### 10.1.5 Budowa pakietu IP

Pakiety IP składają się z danych z wyższych warstw oraz nagłówka IP. Nagłówek IP zawiera następujące pola:

- **Wersja** — określa format nagłówka pakietu IP. 4-bitowe pole wersji zawiera liczbę 4, jeśli jest to pakiet IPv4, a liczbę 6, jeśli jest to pakiet IPv6. Pole to nie jest jednak stosowane do rozróżniania pomiędzy pakietami IPv4 a IPv6 - taką rolę pełni pole typu protokołu obecne w ramce warstwy drugiej.
- **Długość nagłówka IP (HLEN)** — określa długość nagłówka datagramu jako wielokrotność słów 32-bitowych. Jest to całkowita długość wszystkich informacji znajdujących się w nagłówku, obejmująca dwa pola nagłówka o zmiennych długościach.
- **Typ usługi(TOS, ang. Type-of-service)** — określa poziom ważności, który został przypisany przez protokół wyższej warstwy; osiem bitów.
- **Calkowita długość** — określa długość całego pakietu w bajtach z uwzględnieniem danych i nagłówka; 16 bitów. Aby uzyskać długość pola danych, od długości całkowitej należy odjąć wartość HLEN.
- **Identyfikacja** — zawiera liczbę całkowitą identyfikującą bieżący datagram; 16 bitów. Jest to numer sekwencyjny.
- **Flagi** — pole o długości trzech bitów, w którym dwa mniej znaczące bity sterują fragmentacją. Jeden bit określa, czy pakiet może zostać podzielony na fragmenty, a drugi służy do oznaczenia ostatniego pakietu w serii podzielonych pakietów.
- **Przesunięcie fragmentu** — pole pomocne przy składaniu fragmentów datagramu; 13 bitów. Pole to pozwala na zakończenie poprzedniego pola na granicy 16 bitów.
- **Czas życia (TTL, Time To Live)** — pole określające liczbę przeskoków, które może wykonać pakiet. Liczba ta jest zmniejszana o jeden za każdym razem, gdy pakiet przechodzi przez router. Gdy licznik osiągnie wartość zero, pakiet jest odrzucany. Zapobiega to przesyłaniu pakietu w nieskończonej pętli.
- **Protokół** — pole wskazujące, który protokół wyższej warstwy, taki jak TCP lub UDP, odbiera pakiety przychodzące po zakończeniu przetwarzania IP; osiem bitów.
- **Suma kontrolna nagłówka** — pole pomagające zapewnić integralność nagłówka; 16 bitów.
- **Adres nadawcy** — pole określające adres IP węzła nadawczego; 32 bity.
- **Adres odbiorcy** — pole określające adres IP węzła odbiorczego; 32 bity.
- **Opcje** — pole umożliwiające protokołowi IP obsługę różnych opcji, takich jak funkcje zabezpieczeń; zmienna długość.

### Pola warstwy sieci

0	4	8	16	19	24	31
VERS	HLEN	Typ usługi	Całkowita długość			
Identyfikacja			Znaczniki	Przesunięcie fragmentu		
Czas życia	Protokół		Suma kontrolna nagłówka			
Adres IP nadawcy						
Adres IP odbiorcy						
Opcje IP (jeśli istnieją)				Wypełnianie		
Dane						
...						

Są to pola nagłówka pakietu IP. Długość wszystkich pól jest stała z wyjątkiem pól opcji IP oraz uzupełniania

• **Wypełnianie** — zera dodane w celu zagwarantowania, że długość nagłówka jest wielokrotnością 32 bitów.  
 • **Dane** — pole zawierające informacje wyższych warstw; zmienna długość do 64 kB. Podczas gdy adresy nadawcy i odbiorcy są istotne, inne pola nagłówka sprawiają, że protokół IP jest bardzo elastyczny. Pola nagłówka określają adresy nadawcy oraz odbiorcy pakietu, a także

długość przenoszonego komunikatu. Ponadto w nagłówku IP może być zawarta informacja dotycząca routingu, która może być dłuża i mieć złożoną strukturę.

## 10.2 Protokoły routingu IP

### 10.2.1 Przegląd routingu

Routing jest funkcją realizowaną w warstwie 3 modelu (SIECI) OSI. Routing jest hierarchicznym schematem organizacyjnym pozwalającym na łączenie pojedynczych adresów w grupy. Pojedyncze adresy traktowane są jak jedna całość do momentu, gdy wymagany jest adres odbiorcy w celu końcowego dostarczenia danych. Routing jest procesem znajdowania najwydajniejszej ścieżki łączącej dwa urządzenia. Podstawowym urządzeniem wykonującym proces routingu jest router.

**Poniżej wymieniono dwie podstawowe funkcje pełnione przez router:**

- Routery muszą utrzymywać tablice routingu oraz zapewniać informowanie pozostałych routerów o zmianach topologii sieci. Funkcja ta, mająca na celu wymianę informacji dotyczących sieci z innymi routerami, wykonywana jest przy użyciu protokołów routingu.
- Po odebraniu pakietu router musi za pomocą tablicy routingu określić miejsce, do którego pakiet powinien zostać wysłany. Router przełącza pakiety, kierując je do odpowiedniego interfejsu, dodaje niezbędne informacje dotyczące podziału na ramki z uwzględnieniem tego interfejsu, a następnie wysyła pakiety.

**Router jest urządzeniem warstwy sieci**, które określa optymalną ścieżkę przesyłania ruchu sieciowego przy wykorzystaniu jednej lub kilku metryk routingu. Metryki routingu są wartościami służącymi do określania przewagi jednej ścieżki nad inną. Protokoły routingu korzystają ze zróżnicowanych kombinacji metryk w celu dokonania wyboru najlepszej ścieżki.

Routery służą do łączenia segmentów sieci lub całych sieci. Routery przesyłają ramki danych pomiędzy sieciami na podstawie informacji warstwy 3. Routery podejmują decyzje logiczne dotyczące wyboru najlepszej ścieżki transmisji danych. Następnie pakiety kierowane są na odpowiedni port wyjściowy, gdzie przeprowadzany jest proces enkapsulacji. Procesy enkapsulacji i dekapsulacji zachodzą za każdym razem, gdy pakiet jest przesyłany przez router. Router musi zdekapsułkować ramkę warstwy drugiej, aby uzyskać dostęp do nagłówka warstwy trzeciej i odczytać odpowiadający tej warstwie adres. Jak pokazano na rysunku , proces przesyłania danych pomiędzy urządzeniami końcowymi obejmuje enkapsulację i dekapsulację na poziomie wszystkich siedmiu warstw modelu OSI. Podczas enkapsulacji strumień danych jest dzielony na segmenty, dodawane są odpowiednie nagłówki i stopki, po czym dane zostają przesłane. Dekapsulacja jest procesem odwrotnym. Nagłówki i stopki są usuwane, a następnie tworzony jest jednolity strumień.

W kursie tym skupiono uwagę na najpowszechniej stosowanym protokole routowanym — protokole IP. Innymi protokołami routowanymi są między innymi protokoły IPX/SPX i AppleTalk. Protokoły te zapewniają obsługę warstwy 3. Protokoły nieroutowane nie obsługują warstwy 3. Najbardziej popularnym protokołem nieroutowanym jest protokół NetBEUI. Protokół NetBEUI jest nieskomplikowanym, szybkim i wydajnym protokołem, którego funkcjonalność ograniczona jest do dostarczania ramek wewnętrz pojedynczego segmentu.

### 10.2.2 Routing a przełączanie

Routing jest często porównywany z przełączaniem. Niedoświadczonemu obserwatorowi może wydawać się, że routing i przełączanie pełnią tę samą funkcję. Główna różnica polega na tym, że przełączanie odbywa się w 2

warstwie modelu OSI — w warstwie łącza danych, natomiast routing jest prowadzony w warstwie 3. Oznacza to, że routing i przełączanie wykorzystują różne informacje w procesie przesyłania danych ze źródła do celu.

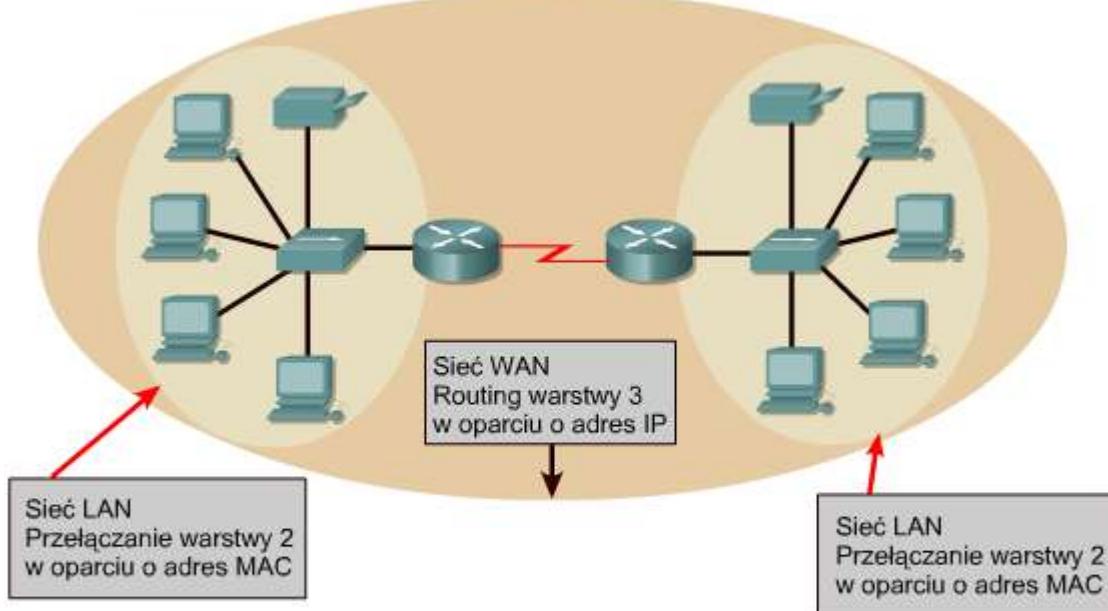
Relacja pomiędzy przełączaniem i routingu jest taka sama jak między lokalnymi i międzymiastowymi rozmowami telefonicznymi. Rozmowa lokalna prowadzona w obrębie tego samego numeru kierunkowego obsługiwana jest przez centralę lokalną. Jednakże centrala lokalna może przechowywać informacje dotyczące jedynie numerów lokalnych w swoim zasięgu. Nie może ona obsługiwać połączeń ze wszystkimi numerami telefonicznymi na świecie. Gdy centrala otrzymuje żądanie połączenia z telefonem spoza obsługiwanej numeru kierunkowego, przełącza je do centrali wyższego poziomu, która rozpoznaje numery kierunkowe. Centrala wyższego poziomu przełącza rozmowę, tak aby została przekazana do centrali lokalnej odpowiadającej strefie wybranego numeru kierunkowego.

#### Warstwa sieci



Router pełni funkcję zbliżoną do centrali wyższego poziomu opisanej w przytoczonym przykładzie. Na rysunku pokazane zostały tablice ARP wykorzystywane do adresowania w warstwie 2 (adresy MAC) oraz tablice routingu wykorzystywane do adresowania w warstwie 3 (adresy IP). Każdy interfejs komputera oraz routera utrzymuje własną tablicę ARP dla celów komunikacji w warstwie 2. Tablica ARP danego urządzenia ma zastosowanie tylko w domenie rozgłoszeniowej, do której jest ono podłączone. Routery przechowują dodatkowo tablicę routingu pozwalającą na przesyłanie danych poza domenę rozgłoszeniową. Każda pozycja tablicy ARP zawiera parę adresów IP-MAC. Adresy MAC na Rysunku są zastąpione akronimem MAC, gdyż rzeczywiste adresy MAC są zbyt długie i nie zmieściłyby się na rysunku. Tablice routingu przechowują dodatkowo informację na temat sposobu zapamiętania danej trasy (w tym przypadku — połączonej bezpośrednio [C] albo odnalezionej z wykorzystaniem protokołu RIP [R]), adresy IP osiągalnych sieci, liczbę przeskoków lub odległość do tych sieci oraz interfejs, przez który dane muszą zostać wysłane, aby dotarły do celu.

## Przełączanie warstwy 2 i routing warstwy 2



**Przełączanie warstwy 2 ma miejsce w sieci LAN. Routing warstwy 3 przesyła dane pomiędzy domenami rozgłoszeniowymi. Wymaga to hierarchicznego formatu adresowania, który realizuje schemat adresowania warstwy 3, taki jak IP.**

Przełącznik warstwy 2 tworzy swoją tablicę przekazywania (*forwarding table*), zawierającą adresy MAC. Kiedy host ma dane do wysłania na adres IP inny niż lokalny, wysyła ramkę do najbliższego routera, zwanego także jego bramą domyślną. Adres MAC routera jest używany przez hosta jako adres MAC odbiorcy.

Przełącznik łączy segmenty należące do tej samej sieci lub podsieci logicznej. Jeśli przełącznik ma przesłać ramkę do hosta nie należącego do sieci lokalnej, przekazuje ją na podstawie adresu MAC odbiorcy do routera. Router dokonuje analizy adresu odbiorcy warstwy 3 w celu podjęcia decyzji dotyczącej przesłania pakietu. Host X zna adres IP routera, ponieważ w jego konfiguracji IP jest zawarty adres IP bramy domyślnej.

Podobne jak przełącznik przechowuje tablicę znanych adresów MAC, router przechowuje tablicę adresów IP zwaną tablicą routingu. Adresy MAC nie są logicznie zorganizowane, natomiast adresy IP tworzą strukturę hierarchiczną. Przełącznik jest w stanie obsługiwać umiarkowaną liczbę niezorganizowanych adresów MAC, gdyż musi on przeszukiwać tablicę tylko w celu odnalezienia adresów należących do tego samego segmentu. Routery muszą obsługiwać większą liczbę adresów. Dlatego routery wymagają zastosowania zorganizowanego systemu adresowania z możliwością grupowania podobnych adresów i traktowania ich jak pojedynczej jednostki sieciowej do momentu, aż dane nie dotrą do segmentu docelowego. Jeśli adresy IP nie miałyby zorganizowanej struktury, Internet po prostu nie mógłby funkcjonować. Taką sytuację można porównać do biblioteki zawierającej miliony pojedynczych zadrukowanych stron ułożonych na ogromnym stosie. Cały ten materiał jest bezużyteczny, gdyż nie jest możliwe odnalezienie pojedynczego dokumentu. Gdy strony są zorganizowane w formie książek, możliwa jest identyfikacja każdej strony, a kiedy książki są także uporządkowane w formie indeksu, odnalezienie i wykorzystanie informacji staje się dużo łatwiejsze.

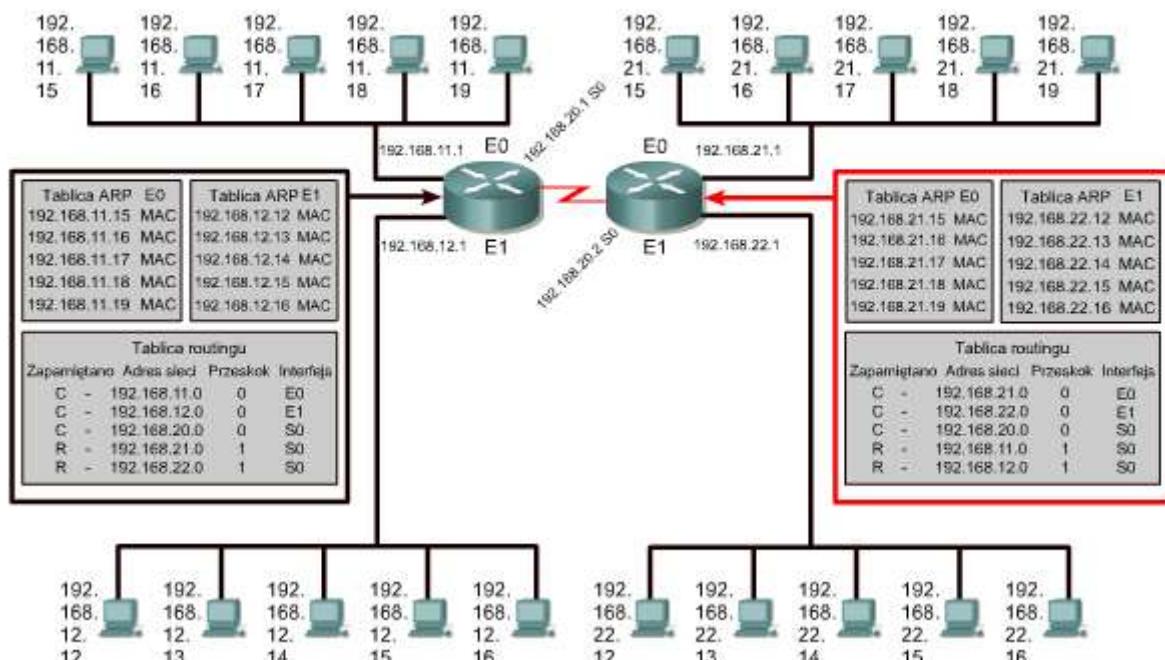
Kolejną różnicą pomiędzy sieciami przełączanymi a sieciami routowanymi jest to, że sieci przełączane nie blokują rozgłoszeń. W rezultacie przełączniki mogą zostać przeciążone przez burze rozgłoszeń. Routery blokują rozgłoszenia sieci LAN, więc burze rozgłoszeń obejmują tylko macierzyste domeny rozgłoszeniowe. Dzięki blokowaniu rozgłoszeń routery zapewniają wyższy poziom bezpieczeństwa i kontroli szerokości pasma niż przełączniki.

## Porównanie cech routera i przełącznika

Kryteria	Router	Przełącznik
Szybkość	Wolniejszy	Szybszy
Warstwa OSI	Warstwa 3	Warstwa 2
Użyte adresowanie	IP	MAC
Pakiety rozgłoszeniowe	Blokowane	Przekazywanie
Bezpieczeństwo	Wyższe	Niższe

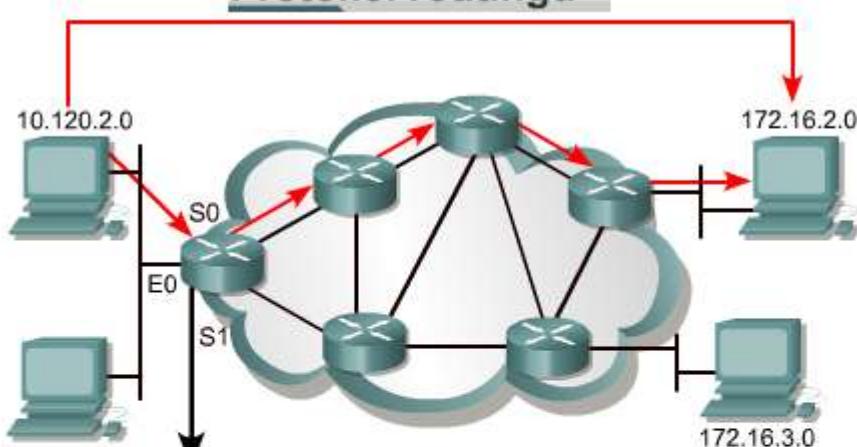
Szybkość i bezpieczeństwo stanowią względne porównanie i zależą od konfiguracji urządzenia.

### Tablice ARP i tablice routingu



### 10.2.3 Protokły routowane a protokoły routingu

#### Protokół routingu



Protokół sieciowy	Sieć docelowa	Interfejs wyjściowy
Podłączony	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Protokoły routingu są używane pomiędzy routerami do określania ścieżek i utrzymywania tablic routingu

Po określeniu ścieżki router może routować pakiety

Protokół routingu = RIP, IGRP

Protokoły wykorzystywane w warstwie sieci w celu transmisji danych pomiędzy hostami za pośrednictwem routera nazywane są protokołami routowanymi. Protokoły routowane zapewniają transport danych przez sieć. Protokoły routingu umożliwiają routerowi dokonanie wyboru najlepszej ścieżki prowadzącej ze źródła do celu.

**Do funkcji protokołów routowanych należą między innymi:**

- Zastosowanie dowolnego zestawu protokołów dostarczającego wystarczającej ilości informacji w adresie warstwy sieci, aby umożliwić routerowi przesłanie danych do następnego urządzenia, a w konsekwencji do celu.
- Zdefiniowanie formatu i sposobu wykorzystania pól wewnętrznych pakietu.

**Przykładami protokołów routowanych są:** protokół IPX (ang. *Internet Network*

*Packet Exchange*) stosowany w rozwiązaniach firmy Novell oraz protokół IP (ang. *Internet Protocol*). Do grupy tej należą również protokoły DECnet, AppleTalk, Banyan VINES oraz XNS (ang. *Xerox Network Systems*). Routery wykorzystują protokoły routingu w celu wymiany informacji i tablic routingu. Innymi słowy, protokoły routingu umożliwiają routerom prowadzenie routingu w ramach protokołów routowanych.

## **Do funkcji protokołów routingu należą między innymi:**

- Dostarczanie procesów pozwalających na współdzielenie informacji o trasach.
- Umożliwienie komunikacji między routerami w celu aktualizacji i utrzymywania tablic routingu.

Przykładami protokołów routingu obsługujących protokół IP są protokoły RIP (ang. *Routing Information Protocol*), IGRP (ang. *Interior Gateway Routing Protocol*), OSPF (ang. *Open Shortest Path First*), BGP (ang. *Border Gateway Protocol*) oraz EIGRP (ang. *Enhanced IGRP*).

### **10.2.4 Określanie ścieżki**

Określanie ścieżki odbywa się na poziomie warstwy sieci. Funkcja określania ścieżki pozwala routerowi na porównanie adresu odbiorcy z dostępными trasami zawartymi w tablicy routingu i na wybór najlepszej ścieżki. Routery mogą zdobyć informacje na temat dostępnych tras za pomocą routingu statycznego lub dynamicznego. Trasy skonfigurowane ręcznie przez administratorów sieci określone są mianem tras statycznych. Trasy, o których informacje zostały otrzymane od innych routerów za pomocą protokołu routingu, określone są mianem tras dynamicznych.

**Routery wykorzystują** proces określania ścieżki w celu podjęcia decyzji dotyczącej portu, przez który należy wysłać nadchodzący pakiet, aby dotarł do swego adresata. Proces ten nazywany jest także routingu pakietów. Każdy router na drodze przesyłanego pakietu nazywany jest przeskokiem. Liczba przeskoków jest długością drogi. Proces określania ścieżki może być porównany do prowadzenia samochodu z jednego miejsca w mieście do innego. Kierowca posiada mapę pokazującą możliwe drogi do punktu docelowego, tak jak router zawiera tablicę routingu. Kierowca pokonuje kolejne skrzyżowania, tak jak pakiet jest przekazywany między routerami w trakcie pojedynczego przeskoku. Na każdym skrzyżowaniu kierowca może wybrać trasę, skręcając w lewo lub w prawo bądź jadąc prosto. Podobnie router określa, przez który port wyjściowy należy wysłać pakiet.

Na decyzje podejmowane przez kierowcę mają wpływ takie czynniki, jak ruch na drodze, ograniczenia prędkości, liczba pasów ruchu, opłaty za przejazd oraz dostępność trasy. Czasami szybciej jedzie się dłuższą trasą, wybierając węższą, mniej uczęszczaną boczną uliczką zamiast zatłoczonej autostrady. Podobnie decyzje podejmowane przez routery bazują na obciążeniu, szerokości pasma, opóźnieniu, koszcie i niezawodności łącza sieci.

**Proces opisany poniżej wykonywany jest podczas określania trasy dla każdego pakietu:**

- Router porównuje adres IP z otrzymanego pakietu ze swoimi tablicami IP.
- Z pakietu pobierany jest adres docelowy.
- W odniesieniu do adresu docelowego stosowana jest maska pierwszego wpisu z tablicy routingu.
- Zamaskowany adres docelowy i wpis w tablicy routingu są ze sobą porównywane.
- Jeżeli wartości te są równe, pakiet jest przesyłany do portu odpowiadającego wpisowi w tablicy.
- W przypadku braku zgody sprawdzany jest kolejny wpis w tablicy.
- Jeżeli pakietowi nie odpowiada żaden wpis z tablicy routingu, router sprawdza, czy została ustawiona trasa domyślna.
- Jeżeli tak, pakiet zostaje przesłany przez przypisany jej port. Trasa domyślna to trasa skonfigurowana przez administratora sieci, którą wysyłane są pakiety, gdy nie zostanie znaleziony odpowiadający im wpis w tablicy routingu.
- Jeżeli nie istnieje domyślna trasa, pakiet jest odrzucany. Zazwyczaj do nadawcy wysyłana jest wiadomość zwrotna informująca, że odnalezienie punktu docelowego było niemożliwe.

### **10.2.5 Tablice routingu**

Routery wykorzystują protokoły routingu w celu tworzenia i utrzymywania tablic routingu zawierających informacje dotyczące tras. Wspomaga to proces określania ścieżki. Protokoły routingu powodują wypełnienie tablic routingu różnymi informacjami dotyczącymi tras. Informacje te różnią się w zależności od użytego protokołu. Tablice routingu zawierają informacje niezbędne do przesyłania pakietów danych przez połączone ze sobą sieci. Urządzenia warstwy 3 łączą domeny rozgłoszeniowe lub sieci LAN. Aby przesyłanie danych mogło się odbywać, wymagany jest hierarchiczny schemat adresowania.

**Routery rejestrują potrzebne informacje w swoich tablicach routingu, w tym następujące dane:**

- **Typ protokołu** — typ protokołu routingu, na podstawie którego został utworzony wpis w tablicy.
- **Odniesienia do punktu docelowego/następnego przeskoku** — odniesienia informujące router o tym, że punkt docelowy jest połączony z routerem bezpośrednio lub że może on zostać osiągnięty poprzez kolejny router, zwany następnym przeskokiem na drodze do punktu docelowego. Kiedy router otrzymuje pakiet, sprawdza adres docelowy, a następnie próbuje odszukać odpowiadający mu wpis w tablicy routingu.
- **Metryki routingu** — różne protokoły routingu używają różnych metryk routingu. Metryki routingu służą do określania zasadności wyboru danej trasy. Na przykład protokół RIP (ang. *Routing Information Protocol*) wykorzystuje liczbę przeskoków jako jedyną metrykę routingu. W protokole IGRP (ang. *Interior Gateway*

*(Routing Protocol)* w celu obliczenia złożonej metryki używana jest kombinacja metryk szerokości pasma, obciążenia, opóźnienia i niezawodności.

- **Interfejsy wyjściowe** — interfejsy, przez które należy wysłać dane w celu dostarczenia ich do punktu docelowego.

Aby utrzymać tablice routingu, routery komunikują się między sobą, przekazując wiadomości dotyczące aktualizacji tras. Niektóre protokoły routingu cyklicznie wysyłają wiadomości aktualizacyjne, inne natomiast wysyłają te wiadomości tylko w wypadku zmiany topologii sieci. Niektóre protokoły przesyłają pełne tablice routingu w każdej wiadomości, natomiast inne przesyłają tylko informacje na temat zmienionych tras. Router tworzy i utrzymuje swoją tablicę routingu na podstawie aktualizacji tras uzyskiwanych od sąsiednich routerów.

### 10.2.6 Algorytmu i metryki routingu

Algorytm jest szczegółowym rozwiązaniem danego problemu. W przypadku routingu pakietów różne protokoły routingu wykorzystują różne algorytmy routingu przy podejmowaniu decyzji dotyczących portu, przez który należy przesłać nadchodzący pakiet. Decyzje podejmowane przez algorytmy routingu opierają się na metrykach.

**Protokoły routingu projektowane są z myślą o realizacji jednego lub kilku z poniższych założeń:**

- **Optymalizacja** — optymalizacja określa skuteczność protokołu routingu w wyborze najlepszej ścieżki. Ścieżka zależeć będzie od metryk i ich wag wykorzystywanych w obliczeniach. Na przykład jeden algorytm może wykorzystywać metryki liczby przeskaków i opóźnienia, przypisując metrykom opóźnienia większą wagę.
- **Prostota i niski narzut** — im prostszy jest algorytm, tym wydajniej będzie przetwarzany przez procesor i pamięć routera. Ten parametr jest istotny, gdyż umożliwia rozrost sieci do dużych rozmiarów, takich jak w przypadku Internetu.
- **Odporność na błędy i stabilność** — algorytm routingu powinien funkcjonować poprawnie w obliczu niecodziennych albo nieprzewidzianych okoliczności, takich jak awarie sprzętu komputerowego, duże obciążenie i błędy implementacji.
- **Elastyczność** — algorytm routingu powinien szybko dostosowywać się do różnorakich zmian zachodzących w sieci. Zmiany te obejmują dostępność routerów, wielkość pamięci poszczególnych routerów, zmiany pasma i opóźnień występujących w sieci.
- **Szybka zbieżność** — zbieżnością określa się proces uzgadniania dostępnych tras pomiędzy wszystkimi routerami. Kiedy jakieś zdarzenie w sieci zmieni dostępność routera, niezbędne są aktualizacje w celu przywrócenia łączności w sieci. Algorytmy routingu, które charakteryzuje niska zbieżność, mogą spowodować, że dane nie zostaną dostarczone.

Algorytmy routingu wykorzystują różne metryki w celu określenia najlepszej ścieżki. Każdy algorytm routingu na swój sposób dokonuje interpretacji najlepszego wyboru. Algorytm routingu generuje liczbę, zwaną wartością metryki, dla każdej ścieżki w sieci. Zaawansowane algorytmy routingu opierają wybór trasy na wielu metrykach, tworząc z nich pojedynczą metrykę złożoną. Zwykle mniejsze wartości metryk wskazują preferowane ścieżki. Metryki mogą być obliczane na podstawie pojedynczego parametru charakteryzującego ścieżkę lub kilku różnych parametrów. **Poniżej przedstawiono parametry najczęściej wykorzystywane przez protokoły routingu:**

- **Szerokość pasma** — przepustowość łącza w kontekście transmitowanych danych. Zwykle połączenie Ethernet o paśmie 10 Mb/s jest bardziej pożąданie od łącza dzierżawionego o paśmie 64 kb/s.
- **Opóźnienie** — czas potrzebny do przesłania pakietu w każdym łączu na drodze ze źródła do celu. Opóźnienie zależy od szerokości pasma łączy pośrednich, ilości danych, które mogą być tymczasowo przechowywane w każdym routerze, przeciążenia sieci oraz fizycznej odległości.
- **Obciążenie** — aktywność występująca w ramach zasobu sieciowego, takiego jak router czy łączce.
- **Niezawodność** — zazwyczaj tym mianem określana jest stopa błędów występujących w danym łączu sieciowym.
- **Liczba przeskaków** — liczba routerów, przez które musi być przesłany pakiet, zanim dotrze do punktu docelowego. Każdy router, przez który muszą zostać przesłane dane, odpowiada pojedynczemu przeskokowi. Ścieżka, której liczba przeskaków wynosi cztery, wskazuje, że dane przesyłane tą ścieżką muszą pokonać cztery routery nim dotrą do punktu docelowego. Jeśli istnieje kilka różnych ścieżek, preferowana jest ścieżka o najmniejszej liczbie przeskaków.
- **Impulsy zegarowe** — opóźnienie na łączu danych mierzane impulsami zegarowymi komputera IBM PC. Jeden impuls to około 1/18 sekundy.
- **Koszt** — dowolna wartość przypisana przez administratora sieci, zwykle oparta na szerokości pasma, wydatku pieniężnym lub innej mierze

## Algorytmy i metryki routingu

Protokół	Metryka	Maksymalna liczba routerów	Pochodzeni
RIP	Liczba przeskóków	15	Xerox
IGRP	<ul style="list-style-type: none"><li>Szerokość pasma</li><li>Obciążenie</li><li>Opóźnienie</li><li>Niezawodność</li></ul>	255	Cisco

Metryki routingu to wartości używane do określenia najlepszej ścieżki do następnego przeskoku.

### 10.2.7 Algorytmy IGP i EGP

System autonomiczny jest siecią lub zbiorem sieci pod wspólną kontrolą administracyjną, przykładem może być domena cisco.com. System autonomiczny składa się z routerów stanowiących spójny obraz routingu dla świata zewnętrznego.

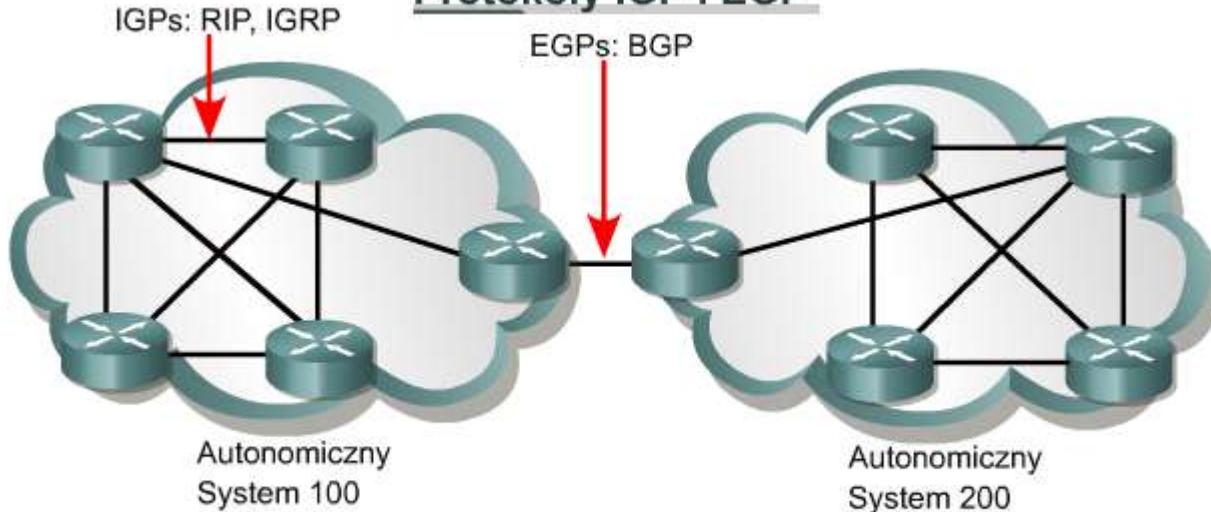
Protokoły IGP (ang. *Interior Gateway Protocols*) i EGP (ang. *Exterior Gateway Protocols*) stanowią dwie rodziny protokołów routingu.

**Protokoły IGP prowadzą routing danych wewnętrz systemu autonomicznego.**

- Protokoły RIP i RIPv2 (ang. *Routing Information Protocol*),
- Protokół IGRP (ang. *Interior Gateway Routing Protocol*),
- Protokół EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*),
- Protokół OSPF (ang. *Open Shortest Path First*),
- Protokół IS-IS (ang. *Intermediate System-to-Intermediate System*).

Protokoły EGP prowadzą routing danych między systemami autonomicznymi. Przykładem protokołu z rodziny EGP jest protokół BGP (ang. *Border Gateway Protocol*).

### Protokoły IGP i EGP



System autonomiczny to zbiór sieci znajdujących się w jednej wspólnej domenie administracyjnej. Protokoły IGP działają w obrębie systemu autonomicznego. Protokoły EGP łączą różne systemy autonomiczne.

### 10.2.8 Stan łącza i wektor odległości

Protokoły routingu mogą być przypisane do rodziny protokołów IGP lub EGP, w zależności od tego, czy grupa routerów jest objęta wspólną administracją, czy też nie. Protokoły z rodziny IGP mogą zostać dalej podzielone na protokoły wektora odległości i protokoły stanu łączna.

W rozwiązańach opartych na wektorze odległości określana jest odległość oraz kierunek, wektor, do dowolnego łącza w intersieci. Odległością może być liczba przeskóków do łączna. Routery korzystające z algorytmów routingu działających na podstawie wektora odległości cyklicznie przesyłają do routerów sąsiadujących wszystkie pozycje swoich tablic routingu lub ich część. Proces ten odbywa się nawet wtedy, gdy w sieci nie wystąpiły żadne zmiany.

Po otrzymaniu aktualizacji trasy router może sprawdzić wszystkie znane trasy i wprowadzić zmiany w swojej tablicy routingu. Proces ten jest w języku angielskim określany także mianem „routing by rumor”. Informacje o sieci, którymi dysponuje router, opierają się na danych uzyskanych od sąsiadujących routerów.

Poniżej wymieniono przykładowe protokoły wektora odległości:

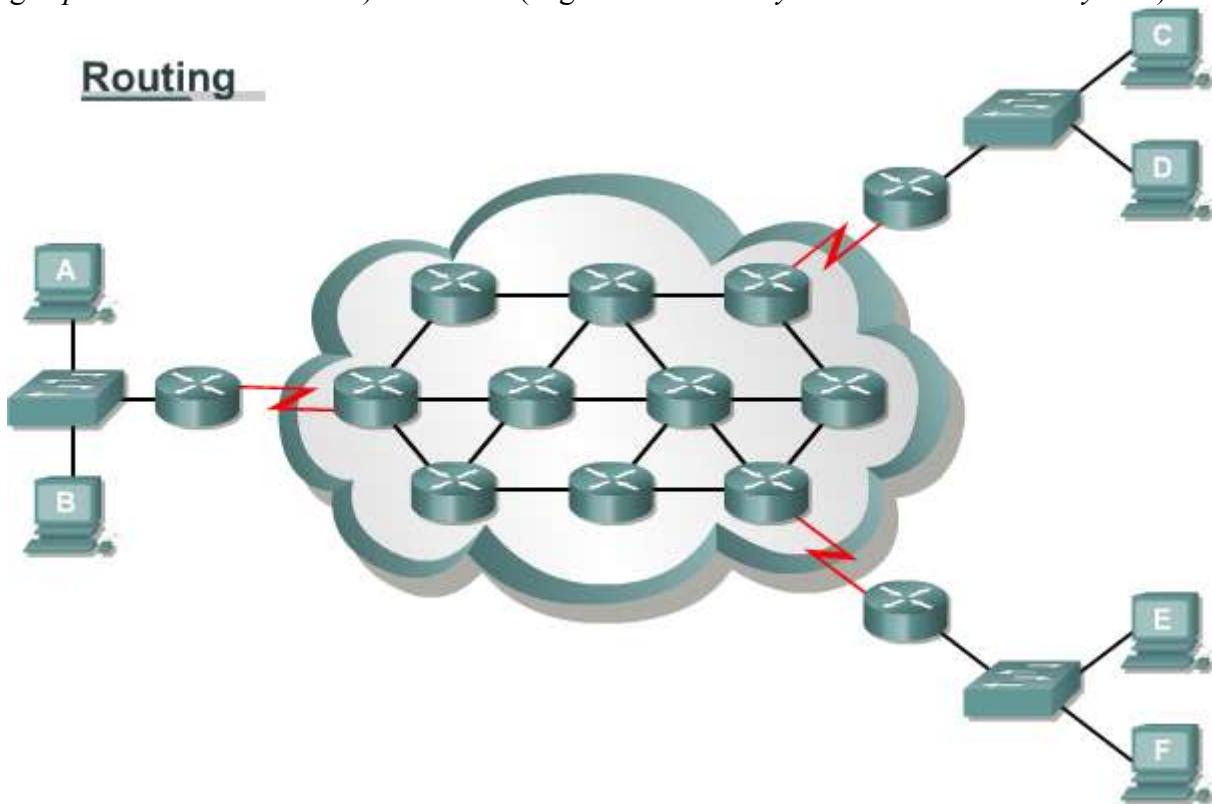
- **Protokół RIP (ang. *Routing Information Protocol*)** — najczęściej stosowany w Internecie protokół z rodziny IGP. Protokół RIP wykorzystuje liczbę przeskóków jako jedyną metrykę.

- **Protokół IGRP (ang. Interior Gateway Routing Protocol)** — protokół z rodziny IGP opracowany przez firmę Cisco w celu rozwiązywania problemów związanych z procesem routingu w dużych sieciach heterogenicznych.
- **Protokół EIGRP (ang. Enhanced IGRP)** — protokół z rodziny IGP będący własnością firmy Cisco. Wykorzystuje on wiele funkcji protokołu stanu łączka. Z tego powodu określany jest mianem zrównoważonego protokołu hybrydowego, jednak w rzeczywistości jest to zaawansowany protokół routingu oparty na wektorze odległości.

Protokoły routingu z wykorzystaniem stanu łączka zostały zaprojektowane w celu eliminacji ograniczeń protokołów routingu opartych na wektorze odległości. Protokoły routingu z wykorzystaniem stanu łączka szybko reagują na zmiany w sieci poprzez wysyłanie wyzwalań aktualizacji jedynie po wystąpieniu takich zmian. Protokoły routingu z wykorzystaniem stanu łączka wysyłają okresowe aktualizacje, zwane także odświeżaniem stanu łączka, co pewien dłuższy czas, na przykład co 30 minut.

Gdy trasa lub łączka ulegnie zmianie, urządzenie, które wykryło zmianę, tworzy ogłoszenie o stanie łączka LSA (ang. *link-state advertisement*) dotyczące tego łączka. Ogłoszenie LSA jest następnie wysyłane do wszystkich sąsiednich urządzeń. Każde urządzenie prowadzące routing odbiera kopię ogłoszenia LSA, dokonuje aktualizacji swojej bazy danych stanów łączek i przesyła ogłoszenie LSA do wszystkich sąsiednich urządzeń. Rozgłaszenie LSA jest niezbędne, aby zagwarantować, że wszystkie urządzenia prowadzące routing przed aktualizacją tablic routingu utworzą bazy danych ściśle odzwierciedlające topografię sieci.

Algorytmy routingu według stanu łączka wykorzystują swoje bazy danych do utworzenia pozycji tablicy routingu zawierających najkrótsze ścieżki. Przykładami protokołów z wykorzystaniem stanu łączka mogą być protokoły OSPF (ang. *Open Shortest Path First*) oraz IS-IS (ang. *Intermediate System-to-Intermediate System*).



### 10.2.9 Protokoły routingu

Protokół RIP jest protokołem routingu z wykorzystaniem wektora odległości, w którym stosuje się liczbę przeskoków jako metrykę służącą do określenia kierunku i odległości do dowolnego łączka w intersieci. Jeżeli do punktu docelowego prowadzi więcej niż jedna ścieżka, protokół RIP wybierze tę, która zawiera najmniejszą liczbę przeskoków. Jednak z powodu wykorzystania w protokole RIP liczby przeskoków jako jedynej metryki nie zawsze wybrana zostanie najszybsza ścieżka. Co więcej, protokół RIP nie może dokonywać routingu pakietów na odległość większe niż 15 przeskoków. Protokół RIPv1 (RIP wersja 1) wymaga, żeby wszystkie urządzenia w sieci używały tej samej maski podsieci. Dzieje się tak dlatego, że w aktualizacji tras nie uwzględnia on informacji na temat maski podsieci. Określone jest to mianem routingu klasowego.

Protokół RIPv2 (RIP wersja 2) dokonuje routingu z uwzględnieniem prefiksu i wysyła w ramach aktualizacji tras informacje dotyczące masek podsieci. Określone jest to mianem routingu bezklasowego. W routingu bezklasowym różne podsieci w tej samej sieci mogą mieć różne maseki podsieci. Wykorzystanie różnych masek podsieci w ramach tej samej sieci określone jest mianem maskowania VLSM (ang. *variable-length subnet masking*).

Protokół IGRP jest zaprojektowanym przez firmę Cisco protokołem routingu opartym na wektorze odległości. Protokół IGRP został utworzony specjalnie w celu rozwiązywania problemów związanych z routingu w dużych sieciach, gdzie zasięg takich protokołów jak RIP okazał się już niewystarczający. Protokół IGRP wybiera najszybszą dostępną ścieżkę, opierając się na szerokości pasma, obciążeniu, opóźnieniu i niezawodności. Cechuje go także znacznie większa maksymalna liczba przeskoków w porównaniu z protokołem RIP. Protokół IGRP korzysta jedynie z routingu klasowego.

Protokół OSPF jest protokołem routingu z wykorzystaniem stanu łączego zaprojektowanym przez organizację IETF (Internet Engineering Task Force) w 1988 roku. Został on opracowany na potrzeby dużych skalowanych interseci, dla których protokół RIP nie był już wystarczający.

Protokół IS-IS (ang. *Intermediate System-to-Intermediate System*) jest protokołem routingu z wykorzystaniem stanu łączego stosowanym przez protokoły routowane inne niż protokół IP. Protokół Integrated IS-IS jest rozszerzoną implementacją protokołu IS-IS obsługującą różne protokoły routowane, w tym także protokół IP. Podobnie jak IGRP, protokół EIGRP jest własnością firmy Cisco. Protokół EIGRP jest zaawansowaną wersją protokołu IGRP. W szczególności, protokół EIGRP cechuje doskonała wydajność działania, w tym szybka zbieżność i niski narzut na szerokość pasma. Protokół EIGRP jest zaawansowanym protokołem wektora odległości wykorzystującym także pewne funkcje protokołu stanu łączego. Z tego powodu protokół EIGRP jest czasami określany mianem hybrydowego protokołu routingu.

Protokół BGP (ang. *Border Gateway Protocol*) jest przykładem protokołu EGP (ang. *External Gateway Protocol*). Protokół BGP wymienia informacje o routingu pomiędzy systemami autonomicznymi, gwarantując przy tym wybór ścieżki pozbawionej zapętleń. BGP jest głównym protokołem ogłoszania informacji o trasach wykorzystywanym przez największe firmy i dostawców usług sieciowych działających w Internecie. BGP4 jest pierwszą wersją protokołu BGP obsługującą bezklasowy routing międzydomenowy (CIDR) oraz agregację tras. W przeciwieństwie do protokołów IGP (ang. *Internal Gateway Protocol*), takich jak RIP, OSPF i EIGRP, protokół BGP nie korzysta z metryk, takich jak liczba przeskoków, szerokość pasma czy opóźnienie. Zamiast tego, protokół BGP podejmuje decyzje dotyczące routingu, bazując na regułach sieci lub regułach wykorzystujących różnorodne atrybuty ścieżki BGP.

### 10.3 Zasady funkcjonowania podsieci

#### 10.3.1 Klasy sieciowych adresów IP

##### Wzory bitowe adresów IP

Klasa A	Sieć	Host		
Oktet	1	2	3	4

Klasa B	Sieć	Host		
Oktet	1	2	3	4

Klasa C	Sieć	Host		
Oktet	1	2	3	4

Klasa D	Host			
Oktet	1	2	3	4

Tak jak zostało to opisane we wcześniejszej części tego modułu, klasy adresów IP umożliwiają obsługę od 256 do 16,8 miliona hostów. Klasy mogą być podzielone na mniejsze podsieci w celu efektywnego zarządzania ograniczoną liczbą adresów IP. Rysunek zawiera przegląd możliwości podziału między sieci i hosty.

Adresy klasy D są używane w grupach wieloemisyjnych. W tym przypadku nie ma potrzeby wydzielania części sieciowej i części hosta.

Adresy klasy E są zarejestrowane tylko do badań.

#### 10.3.2 Wprowadzenie do podsieci i przyczyny ich tworzenia

W celu utworzenia struktury podsieci bity hosta muszą być przypisane jako bity podsieci. Często określane jest to mianem „pożyczania” bitów. Jednak bardziej odpowiednim pojęciem jest „użyczanie” bitów. Proces rozpoczyna się zawsze od wysuniętego najbardziej na lewo bitu hosta, który położony jest najbliżej ostatniego oktetu sieci. Adres podsieci zawiera części sieci odpowiadające klasom A, B i C, a także pole podsieci i pole hosta. Pola podsieci i hosta tworzone są na podstawie pierwotnej części hosta głównego adresu IP. Jest to realizowane poprzez przypisanie niektórych bitów z pierwotnej części hosta do części sieciowej adresu. Możliwość podziału pierwotnej części hosta na nowe pola podsieci i hosta zapewnia administratorom sieci elastyczność adresowania. Poza ułatwieniem zarządzania, tworzenie podsieci pozwala administratorowi na ograniczenie zjawiska rozgłaszenia i wprowadzenie niskopoziomowej ochrony w sieci LAN. Tworzenie podsieci zapewnia nieco wyższy

poziom bezpieczeństwa, ponieważ dostęp do innych podsieci jest możliwy jedynie za pośrednictwem usług routera. Co więcej, zastosowanie list dostępu umożliwia wprowadzenie zabezpieczeń dostępu. Na podstawie różnych kryteriów zawartych na tego typu listach można umożliwić dostęp do podsieci lub odmówić go. Listy dostępu zostaną omówione szerzej w dalszej części kursu. Właściciele sieci klas A i B zauważali, że możliwość tworzenia podsieci stanowi źródło dochodu poprzez dzierżawę albo sprzedaż poprzednio nieużywanych adresów IP. Podział na podsieci jest dla danej sieci operacją wewnętrzną. Z zewnątrz sieć LAN jest widziana jako pojedyncza sieć z pominięciem jakichkolwiek szczegółów dotyczących jej struktury wewnętrznej. Dzięki takiej strukturze sieci tablice routingu są niewielkie i wydajne. Weźmy np. lokalny węzeł o adresie 147.10.43.14 w podsieci 147.10.43.0. Z zewnątrz widziany jest tylko ogłaszanym adresie sieci głównej 147.10.0.0, gdyż lokalny adres podsieci 147.10.43.0 jest poprawny tylko w sieci LAN, w której zastosowano podział na podsieci.

### 10.3.3 Ustalanie adresu maski podsieci

Wybór liczby bitów wykorzystywanych podczas procesu tworzenia podsieci zależy będzie od wymaganej maksymalnej liczby hostów przypadających na podsieć. Podczas obliczania liczby podsieci i hostów tworzonych w procesie pożyczania bitów konieczna jest znajomość podstaw matematyki liczb binarnych i wartości pozycji bitów w każdym oktacie.

Ostatnie dwa bity ostatniego oktetu, niezależnie od klasy adresu IP, nie mogą być w żadnym przypadku przypisane do podsieci. Bit te nazywane są dwoma najmniej znaczącymi bitami. Wykorzystanie do tworzenia podsieci wszystkich dostępnych bitów z wyjątkiem ostatnich dwóch sprawi, że w każdej z podsieci będą mogły znajdować się tylko dwa hosty. Jest to praktyczna metoda oszczędzania adresów w adresowaniu szeregowych łączów routerów. Jednak w przypadku działającej sieci LAN spowodowałoby to niedopuszczalne podniesienie kosztów wyposażenia. Maska podsieci udziela routerowi informacji potrzebnych do określenia, w której sieci i podsieci znajduje się konkretny host. Jedynki binarne w masce podsieci wskazują pozycje bitów części sieciowej. Bit podsieci to te, które zostały pożyczone z pierwotnej części hosta. Jeśli zostały pożyczone trzy bity, maska adresu klasy C będzie miała postać 255.255.255.224. W formacie z ukośnikiem maska ta będzie reprezentowana jako /27. Liczba stojąca za ukośnikiem jest całkowitą liczbą bitów użyta w częściach adresu odpowiadających sieci i podsieci. **W celu określenia potrzebnej liczby bitów projektujący sieć muszą określić liczbę hostów w największej podsieci oraz liczbę podsieci.** Jako przykład przedstawiono sytuację, w której sieć musi składać się z sześciu podsieci zawierających po 25 hostów każda. Liczba bitów, których przypisanie musi zostać zmienione, może zostać szybko określona przy wykorzystaniu tabeli podsieci. W wierszu zatytułowanym „Liczba podsieci możliwych do wykorzystania” odnaleźć można informację, że w przypadku sześciu podsieci trzeba pożyczyc dodatkowe trzy bity do stworzenia maski podsieci. Z tabeli wynika także, że w każdej ze stworzonych podsieci maksymalna ilość hostów wynosi 30, co jest zgodne z wymaganiami tego przykładu. Różnica pomiędzy liczbą hostów możliwych do wykorzystania a całkowitą liczbą hostów wynika z użycia pierwszego wolnego adresu jako identyfikatora, a ostatniego jako adresu rozgłoszeniowego dla każdej podsieci. Podział na odpowiednią liczbę podsieci zawierających wymaganą liczbę hostów prowadzi do tego, że część potencjalnych adresów hostów jest tracona. Routing klasowy nie pozwala na wykorzystanie tych adresów. Jednakże routing bezklasowy, o którym będzie mowa w dalszej części kursu, pozwala na odzyskanie wielu z nich.

Metoda wykorzystana przy tworzeniu tablicy podsieci może być użyta do rozwiązywania wszystkich problemów związanych z tworzeniem podsieci. **W metodzie wykorzystywany jest następujący wzór:**

Liczba podsieci możliwych do wykorzystania = dwa do potęgi równej liczbie przypisanych bitów podsieci lub bitów pożyczonych, minus dwa. Odjęcie dwóch wynika z uwzględnienia adresów zarezerwowanych na identyfikator i adres rozgłoszeniowy sieci.

Liczba hostów możliwych do wykorzystania = dwa do potęgi równej liczbie pozostałych bitów, minus dwa (adresy zarezerwowane na identyfikator i rozgłaszenie podsieci)

Tabela podsieci (pozycja bitu i wartość)								
Bit pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1

Tabela podsieci (identyfikator maski podsieci)								
Format z ukośnikiem	/25	/26	/27	/28	/29	/30	N/A	N/A
Maska	128	192	224	240	248	252	254	255
Bit pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

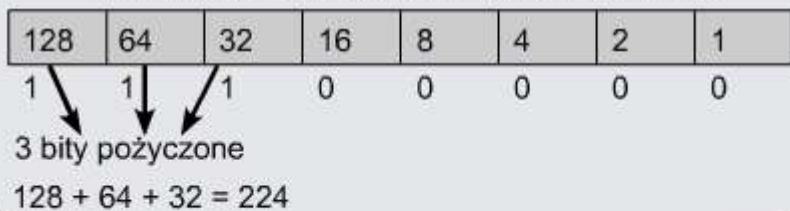
## Tabela podsieci

Format z ukośnikiem	/25	/26	/27	/28	/29	/30	Nd.	Nd.
Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Calkowita liczba podsieci		4	8	16	32	64		
Liczba podsieci możliwych do wykorzystania		2	6	14	30	62		
Calkowita liczba hostów		64	32	16	8	4		
Liczba hostów możliwych do wykorzystania		62	30	14	6	2		

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

## Tworzenie podsieci

Liczba 224 w czwartym oktacie oznacza całkowitą wartość odpowiadającą pozycjom pożyczonych bitów.



### 10.3.4 Zastosowanie maski podsieci

Po ustaleniu maski podsieci można ją wykorzystać do utworzenia schematu podsieci. **Tabela przedstawiona na rysunku prezentuje przykładowe podsieci i adresy powstałe przez przypisanie trzech bitów do pola podsieci.** Powstanie osiem podsieci, z których każda składać się będzie z 32 hostów. Numerowanie podsieci rozpoczyna się od zera (0). Pierwsza podsieć jest zawsze określana mianem podsieci zerowej.

Podczas tworzenia tabeli podsieci trzy pola wypełniane są automatycznie, wypełnienie pozostałych wymaga pewnych obliczeń. Identyfikator podsieci zerowej równy jest numerowi sieci głównej, w tym przypadku: 192.168.10.0. Identyfikator rozgłoszania dla całej sieci równy jest największym dopuszczalnemu numerowi, w tym przypadku: 192.168.10.255. Trzecim podanym numerem jest identyfikator podsieci numer siedem. Składa się on z trzech oktetów sieci oraz

numeru maski podsieci wstawionego na pozycji czwartego oktetu. Do pola podsieci zostały przypisane trzy bity; ich łączna wartość wynosi 224. Identyfikator podsieci numer siedem to 192.168.10.224. Te wstawione liczby stają się punktami kontrolnymi służącymi do sprawdzenia poprawności po wypełnieniu tabeli.

## Schemat podsieci

Nr podsieci	Ident. podsieci	Zakres hostów	Identyfikator rozgłoszania
0	192.168.10.0	.1-.30	192.168.10.31
1	192.168.10.32	.33-.62	192.168.10.63
2	192.168.10.64	.65-.94	192.168.10.95
3	192.168.10.96	.97-.126	192.168.10.127
4	192.168.10.128	.129-.158	192.168.10.159
5	192.168.10.160	.161-.190	192.168.10.191
6	192.168.10.192	.193-.222	192.168.10.223
7	192.168.10.224	.225-.254	192.168.10.255

Kiedy korzystamy z tabeli podsieci lub wzoru przypisanie trzech bitów do pola podsieci spowoduje przypisanie 32 hostów do każdej podsieci. Pozwala to na określenie wartości kroku przy obliczaniu identyfikatora kolejnej podsieci. Począwszy od zerowej podsieci, dodanie liczby 32 do poprzedzającego numeru spowoduje ustalenie identyfikatora każdej podsieci. Należy zwrócić uwagę, że identyfikator podsieci zawiera same zera w części hosta.

W każdej podsieci pole rozgłaszenia ma ostatni numer składający się w części hosta z samych

jedynek binarnych. Zastosowanie tego adresu umożliwia rozgłoszanie tylko do członków pojedynczej podsieci. Ponieważ identyfikator podsieci zerowej wynosi 192.168.10.0, a podsieć składa się łącznie z 32 hostów, identyfikator rozgłoszenia będzie równy 192.168.10.31. Począwszy od zera, 32. kolejna liczba ma wartość 31. Należy pamiętać, że zero (0) jest rzeczywistą liczbą wykorzystywaną w świecie zagadnień sieciowych. Kolumna identyfikatora rozgłoszenia może zostać wypełniona w taki sam sposób jak kolumna identyfikatora podsieci. Należy po prostu dodać liczbę 32 do poprzedzającego identyfikatora rozgłoszenia w podsieci. Można także zacząć od ostatniego, najniższego pola kolumny i posuwać się do góry, wstawiając liczby powstałe przez odjęcie jedynki od identyfikatora poprzedzającej podsieci.

### 10.3.5 Tworzenie podsieci w sieciach klasy A i B

Procedura tworzenia podsieci w sieciach klasy A i B jest taka sama jak w przypadku klasy C, z tą różnicą, że można użyć znaczco większej liczby bitów. Liczba bitów możliwych do przypisania do pola podsieci w adresie klasy A wynosi 22, natomiast w klasie B — 14 bitów.

Poprzez przypisanie 12 bitów adresu klasy B do pola podsieci uzyskujemy maskę podsieci równą 255.255.255.240 lub /28. Przypisane zostało wszystkie osiem bitów trzeciego oktetu, dając liczbę 255, będącą największą liczbą, jaką można zapisać na ośmiu bitach. W czwartym oktacie zostały przypisane cztery bity, dając liczbę 240. Przypomnijmy, że maska podsieci w formacie z ukośnikiem stanowi sumę wszystkich bitów przypisanych do pola podsieci powiększoną o ustalone bity sieci.

Poprzez przypisanie 20 bitów adresu klasy A do pola podsieci uzyskujemy maskę podsieci równą 255.255.255.240 lub /28. Do pola podsieci przypisano wszystkie osiem bitów drugiego i trzeciego oktetu oraz cztery bity czwartego oktetu.

W tej sytuacji widać, że maska podsieci dla adresów klasy A i B wydaje się być identyczna. O ile maska nie odnosi się do adresu sieci, nie jest możliwe określenie liczby bitów przypisanych do pola podsieci.

Niezależnie od klasy sieci, która ma zostać podzielona na podsieci, obowiązują te same reguły:

**Całkowita liczba podsieci =  $2^{\text{do potegi równej liczbie pożyczonych bitów}}$**  **Całkowita liczba hostów =  $2^{\text{do potegi równej liczbie pozostałych bitów}}$**

**Liczba podsieci możliwych do wykorzystania =  $2^{\text{do potegi równej liczbie pożyczonych bitów}}$**  **minus 2 Liczba hostów**

**możliwych do wykorzystania =  $2^{\text{do potegi równej liczbie pozostałych bitów}}$**  **minus 2**

**Tabela podsieci**

Format z ukośnikiem	/25	/26	/27	/28	/29	/30	Nd.	Nd.
Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Całkowita liczba podsieci		4	8	16	32	64		
Liczba podsieci możliwych do wykorzystania		2	6	14	30	62		
Całkowita liczba hostów		64	32	16	8	4		
Liczba hostów możliwych do wykorzystania		62	30	14	6	2		

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

### Tworzenie podsieci

Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Podsieci	2	4	8	16	32	64	128	256

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu девятиu bitów.

### 10.3.6 Obliczanie adresu podsieci z wykorzystaniem operacji iloczynu logicznego

Routery wykorzystują maski podsieci w celu określenia sieci, do której należą poszczególne hosty. Proces ten określany jest mianem iloczynu logicznego. Routery określają identyfikator podsieci odebranego pakietu przy użyciu binarnego procesu iloczynu logicznego. Iloczyn logiczny przypomina mnożenie.

Proces ten odbywa się na poziomie liczb dwójkowych. Dlatego maska i adres IP muszą być prezentowane w

#### Operacja iloczynu logicznego (AND)

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

Zasada jest następująca wynik wszystkich operacji z wyjątkiem 1 AND 1 wynosi 0 (zero).

#### Obliczanie identyfikatora podsieci

Adres pakietu	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Maska	255.255.255.224	11111111.11111111.11111111.11100000
Ident. podsieci	201.10.11.64	11001001.00001010.00001011.01000000

dostępnych jest wiele kalkulatorów wspomagających tworzenie podsieci. Jednakże administratorzy sieci muszą znać sposoby ręcznego przeprowadzania obliczeń przy tworzeniu podsieci, aby móc skutecznie zaprojektować schemat sieci i kontrolować poprawność wyników uzyskanych za pomocą kalkulatora podsieci. Kalkulator podsieci nie umożliwia przygotowania wstępnego schematu, może jedynie obliczyć końcowe dane adresowe. Co więcej, w trakcie trwania egzaminu certyfikacyjnego korzystanie z jakichkolwiek kalkulatorów jest zabronione

#### Podsumowanie

- Protokół jest zestawem reguł określających sposób komunikacji komputerów w sieciach.
- Protokół routowany przesyła dane poprzez sieć.
- Protokoły routingu umożliwiają routерom wybór najlepszej ścieżki dla danych od miejsca źródłowego do docelowego.
- Zastosowanie podsieci umożliwia administratorom sieci określenie rozmiarów fragmentów sieci, na których będą operować.

formacie dwójkowym. Adres IP oraz adres podsieci poddawane są operacji iloczynu logicznego, w wyniku którego otrzymywany jest identyfikator podsieci. Rezultat jest wykorzystywany przez router w celu przesłania pakietu przez właściwy interfejs.

Tworzenie podsieci jest umiejętnością, którą trzeba opanować. Minie wiele godzin spędzonych na wykonywaniu ćwiczeń praktycznych, zanim uzyska się umiejętność tworzenia elastycznych i przydatnych schematów. W sieci WWW

## Moduł 11. Warstwa transportowa i aplikacji

Zadaniem warstwy transportowej TCP/IP jest, jak sugeruje jej nazwa, transport danych pomiędzy aplikacjami urządzenia źródłowego i docelowego. Dokładne poznanie działania warstwy transportowej jest niezbędne do zrozumienia zagadnień związanych z nowoczesnymi sieciami przesyłania danych. W module tym zostaną opisane funkcje i usługi tej krytycznej warstwy modelu sieciowego TCP/IP.

Wiele aplikacji sieciowych znajdujących się w warstwie aplikacji modelu TCP/IP jest dobrze znanych nawet sporadycznym użytkownikom sieci. Na przykład terminy HTTP, FTP i SMTP są akronimami często spotykanymi przez użytkowników przeglądarki WWW i klientów poczty elektronicznej. W module tym zostały również opisane funkcje tych oraz innych aplikacji modelu sieciowego TCP/IP.

### 11.1 Warstwa transportowa TCP/IP

#### 11.1.1 Wprowadzenie do warstwy transportowej

Do podstawowych zadań warstwy transportowej, warstwy 4 modelu OSI, należą transportowanie informacji i sterowanie ich przepływem ze źródła do celu w sposób niezawodny i dokładny. Kontrola typu end-to-end oraz niezawodność są zapewniane przez okna przesuwne, numery kolejne i potwierdzenia.

Aby zrozumieć niezawodność i kontrolę przepływu, można wyobrazić sobie kogoś, kto po rocznej nauce języka obcego odwiedza kraj, w którym ten język jest używany. Podczas rozmowy słowa muszą być wypowiadane powoli i dla pewności powtarzane, by nie zgubić sensu rozmowy. Tym właśnie jest kontrola przepływu.

Warstwa transportowa zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Umożliwia ona nawiązanie połączenia logicznego

między punktami końcowymi sieci. Protokoły warstwy transportowej dzielą na segmenty i ponownie składają dane wysypane przez aplikacje wyższej warstwy, przesyłając je w tym samym strumieniu danych warstwy transportowej. Strumień danych warstwy transportowej obsługuje transport typu end-to-end, czyli transport między punktami końcowymi.

Strumień ten jest logicznym połączeniem pomiędzy punktami końcowymi sieci. Do jego podstawowych zadań należy transportowanie informacji i sterowanie ich przepływem ze źródła do celu w sposób niezawodny i dokładny. Podstawowym zadaniem warstwy 4 jest zapewnienie kontroli typu end-to-end z wykorzystaniem metody okien przesuwnych oraz zapewnienie niezawodności za pomocą mechanizmów numerów kolejnych i potwierdzeń. Warstwa transportowa określa połączenia typu end-to-end pomiędzy aplikacjami na hostach.

**Usługi transportowe obejmują następujące usługi podstawowe:**

- segmentacja danych aplikacji wyższej warstwy,
- ustanawianie operacji typu end-to-end,
- transport segmentów między dwoma hostami końcowymi,
- kontrola przepływu zapewniana przez okna przesuwne,
- niezawodność zapewniana przez numery sekwencyjne i potwierdzenia.

TCP/IP jest kombinacją dwóch oddzielnych protokołów. Protokół IP działa w warstwie 3 i jest protokołem bezpołączeniowym odpowiadającym za dostarczanie danych poprzez sieć z dołożeniem wszelkich starań. Protokół TCP działa w warstwie 4 i jest usługą zorientowaną połączeniowo odpowiedzialną za kontrolę przepływu i niezawodność. Połączenie tych protokołów w parę zapewnia szerszy zakres usług. Razem stanowią one podstawę dla całego zestawu protokołów, zwanego zestawem protokołów TCP/IP. Na jego podstawie powstał Internet.

#### 11.1.2 Kontrola przepływu

Podczas przesyłania segmentów danych przez warstwę transportową podejmowane są starania, aby nie dopuścić do utraty danych. Przyczyną utraty danych może być sytuacja, w której host odbierający nie jest w stanie

#### Warstwa transportowa

Niezawodne przesyłanie danych można osiągnąć poprzez:

- Zapewnienie, że wysyłający otrzyma potwierdzenie dostarczenia segmentów
- Umożliwienie retransmisji wszystkich niepotwierdzonych segmentów
- Umieszczenie segmentów w poprawnej kolejności w miejscu przeznaczenia
- Funkcje sterowania oraz unikania przeciążeń

#### Analogie do warstwy transportowej

Hiszpański (język podstawowy)

Angielski (jeden rok nauki)

Wolniejsze

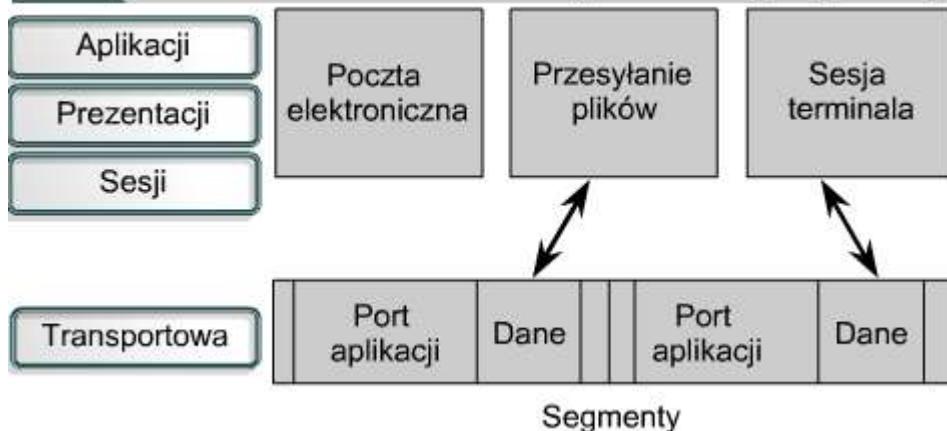
porozumiewanie się

Angielski (jedyny język)

przetwarzać danych z taką szybkością, z jaką one do niego docierają. Host odbierający jest wtedy zmuszony do ich odrzucenia. Kontrola przepływu zapobiega problemowi przepełnienia buforów hosta odbierającego. Protokół TCP zawiera mechanizm kontroli przepływu polegający na umożliwieniu komunikacji pomiędzy hostem wysyłającym i odbierającym. W ten sposób oba hosty ustalają prędkość transferu danych na wartość odpowiadającą każdemu z nich.

### 11.1.3 Przegląd operacji ustanawiania, obsługi i zakończenia sesji

#### Multipleksowanie konwersacji warstwy wyższej



(multipleksowaniem) konwersacji warstwy wyższej. Wiele równoczesnych konwersacji jednostek warstwy wyższej może być multipleksowanych na pojedynczym połączeniu.

Jedną z funkcji warstwy transportowej jest ustanowienie sesji zorientowanej połączeniowo pomiędzy podobnymi urządzeniami pracującymi w warstwie aplikacji. Aby rozpocząć transfer danych, obie aplikacje, zarówno wysyłająca jak i odbierająca, przekazują informację do swoich systemów operacyjnych, że zostanie zainicjowane połączenie. Połączenie zainicjowane przez jeden węzeł musi zostać zaakceptowane przez drugi węzeł. Moduły oprogramowania protokołu w dwóch systemach operacyjnych komunikują się ze sobą za pośrednictwem wysyłanych przez sieć wiadomości w celu zweryfikowania, czy transfer jest autoryzowany i czy obie strony są gotowe.

Zostaje ustanowione połączenie, a po zakończeniu wszystkich czynności synchronizacyjnych rozpoczyna się transfer danych. W czasie przesyłania oba urządzenia nadal się komunikują za pomocą oprogramowania protokołu w celu weryfikacji poprawności odbieranych danych.

Na rysunku zaprezentowane zostało typowe połączenie pomiędzy systemem wysyłającym i odbierającym. Pierwsze uzgodnienie jest żądaniem synchronizacji. Drugie i trzecie uzgodnienie potwierdzają początkowe żądanie synchronizacji, równocześnie synchronizując parametry połączenia w przeciwnym kierunku. Końcowy segment uzgodnienia jest potwierdzeniem służącym do poinformowania adresata, że obie strony są zgodne, iż zostało ustanowione połączenie. Po ustanowieniu połączenia rozpoczyna się transfer danych.

#### **Przeciążenie podczas transferu danych może wystąpić z dwóch powodów:**

- Po pierwsze, szybki komputer może być w stanie generować ruch szybciej, niż sieć może go przekazywać.
- Po drugie, jeśli wiele komputerów równocześnie wysyła datagramy do tego samego adresata, może on zostać przeciążony, mimo że problemu nie spowodował żaden pojedynczy komputer.

Gdy datagramy są odbierane przez bramę lub hosta szybciej niż mogą zostać przetworzone, są one tymczasowo przechowywane w pamięci. Jeśli ruch trwa dalej, w końcu zostaje wyczerpana pamięć hosta lub bramy, co powoduje odrzucanie kolejnych datagramów.

Zamiast dopuszczenia do utraty danych, proces TCP na odbierającym hoście może wysłać do nadawcy powiadomienie „nie gotowy”. Wskaźnik ten, działający jak znak stopu, sygnalizuje wysyłającemu, żeby przerwał wysyłanie danych. Gdy odbierający może obsłużyć dalsze dane, wysyła wskaźnik transportowy „gotowy”. Po odebraniu tego wskaźnika wysyłający może wznowić transmisję segmentów.

Na końcu transferu danych host nadający wysyła sygnał wskazujący koniec transmisji. Na końcu sekwencji danych host odbierający potwierdza koniec transmisji i połączenie jest zamknięte.

### 11.1.4 Uzgadnianie trójetatowe

Protokół TCP jest protokołem zorientowanym połączeniowo. Wymaga on ustanowienia połączenia przed rozpoczęciem przesyłania danych. Aby ustanowić lub zainicjować połączenie, muszą zostać zsynchronizowane początkowe numery sekwencyjne (ISN) obu hostów. Synchronizacja polega na wymianie ustanawiających połączenie segmentów zawierających bit kontrolny zwany SYN (synchronizacja) oraz numery ISN. Segmente zawierające bit SYN są również nazywane segmentami „SYN”. Rozwiążanie to wymaga odpowiedniego

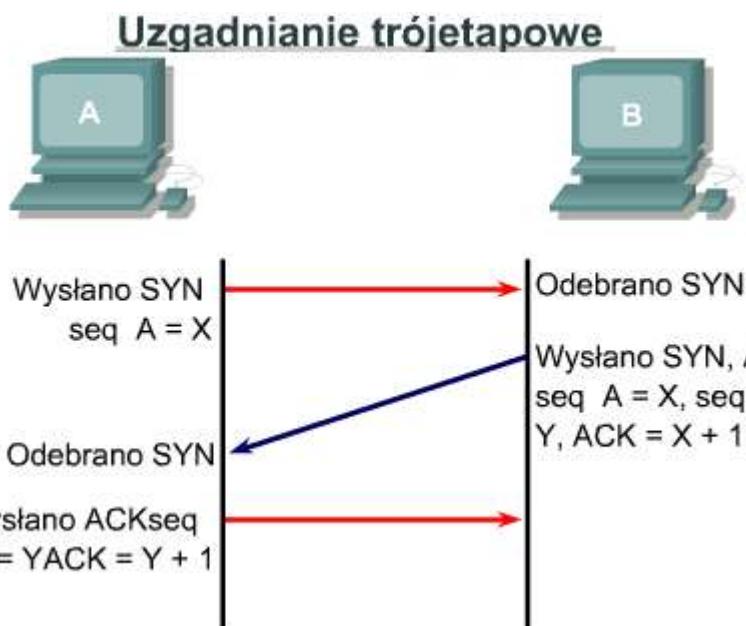
W modelu odniesienia OSI wiele aplikacji może współdzielić to samo połączenie transportowe. Funkcje transportu danych są realizowane na zasadzie wysyłania segmentu za segmentem. Innymi słowy, różne aplikacje mogą wysyłać segmenty danych w oparciu o zasadę „pierwszy przychodzi, pierwszy obsłużony”. Pierwszy odebrany segment będzie obsłużony jako pierwszy. Segmenty te mogą podlegać routingowi do tego samego lub różnych adresatów. Jest to nazywane zwielokrotnianiem

mechanizmu wybierania początkowego numeru sekwencyjnego oraz procesu uzgadniania służącego do wymiany numerów ISN.

Synchronizacja wymusza wysłanie przez każdą ze stron własnego początkowego numeru sekwencyjnego i odbiór potwierdzenia wymiany (ACK) od strony przeciwej. **Każda strona musi również odebrać od drugiej strony numer ISN i wysłać potwierdzenie ACK. Kolejność jest następująca:**

1. Wysyłający host (A) inicjuje połączenie przez wysłanie pakietu SYN do odbiorcy (hosta B) ze swoim numerem początkowym ISN = X:  $A \rightarrow B \text{ SYN, seq A} = X$
2. B otrzymuje pakiet, zapamiętuje, że numer sekwencyjny seq hosta A = X, odpowiada pakietem z ustawionym bitem ACK i numerem potwierdzenia X + 1, a także określa swój numer początkowy ISN = Y. Potwierdzenie ACK z numerem X + 1 oznacza, że host B otrzymał wszystkie oktety do oktetu X włącznie i będzie oczekiwany na oktet o numerze X + 1:  $B \rightarrow A \text{ ACK, seq A} = X, \text{SYN seq B} = Y, \text{ACK} = X + 1$
3. A otrzymuje pakiet od B, wie, że numer sekwencyjny seq hosta B = Y, i odpowiada pakietem z ustawionym bitem ACK i numerem potwierdzenia Y + 1, co kończy proces ustanawiania połączenia:  $A \rightarrow B \text{ ACK, seq B} = Y, \text{ACK} = Y + 1$

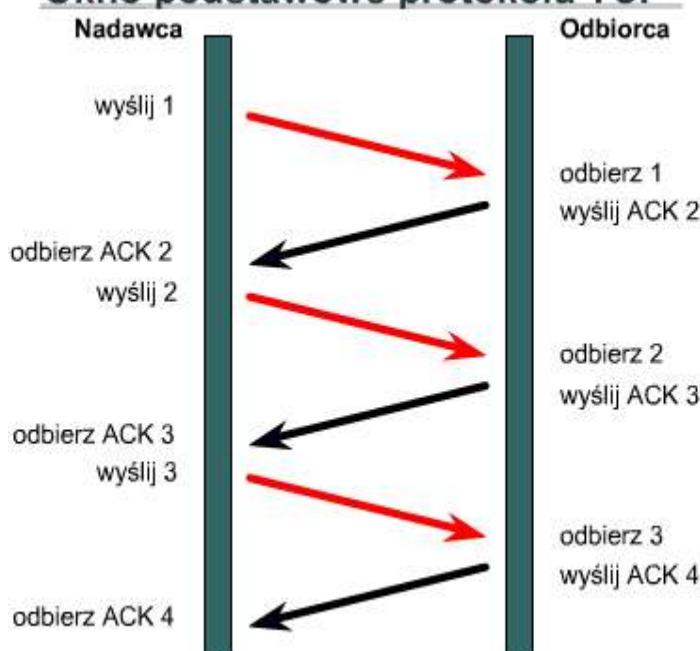
Wymiana ta jest zwana uzgadnianiem trójetapowym.



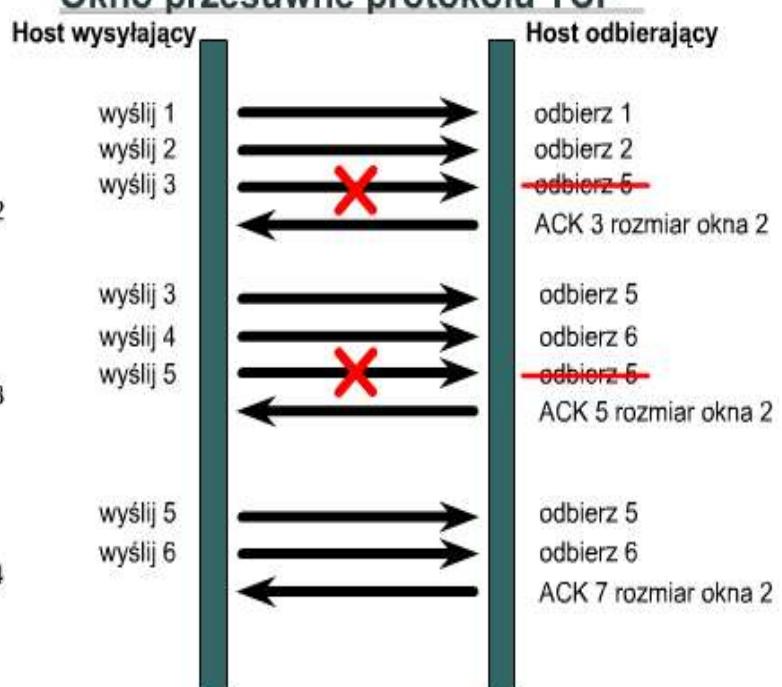
Uzgadnianie trójetapowe jest konieczne ze względu na to, że numery sekwencyjne nie są związane z globalnym zegarem w sieci i protokoły TCP mogą mieć różne mechanizmy wybierania numeru ISN. Odbiorca pierwszego segmentu SYN nie ma innego sposobu na rozpoznanie starego lub spóźnionego segmentu niż pamiętanie ostatniego numeru podczas kolejnego połączenia. Pamiętanie tego numeru nie zawsze jest możliwe. Dlatego odbiorca musi zwrócić się do wysyłającego o weryfikację segmentu SYN.

### 11.1.5 Okienkowanie

#### Okno podstawowe protokołu TCP



#### Okno przesuwne protokołu TCP



Aby zapewnić niezawodność zorientowanego połączeniowo transferu danych, pakiety danych muszą być dostarczane do odbiorcy w tej samej kolejności, w której zostały wysłane. Przesyłanie danych za pomocą danego protokołu nie powiedzie się, jeśli jakieś pakiety danych zostaną utracone, uszkodzone, powielone lub odebrane w

innej kolejności. Łatwym rozwiązaniem jest potwierdzanie przez odbiorcę odbioru każdego pakietu przed wysłaniem kolejnego.

Gdyby nadawca musiał czekać na potwierdzenie po wysłaniu każdego pakietu, przepustowość byłaby niska. Z tego powodu w przypadku większości niezawodnych protokołów zorientowanych połączeniowo dozwolone jest pozostawanie więcej niż jednego pakietu bez potwierdzenia w danym czasie. Czas pozostały po zakończeniu transmisji pakietu danych przez nadawcę i przed zakończeniem przetwarzania otrzymanego przez niego potwierdzenia jest wykorzystywany do przesłania większej ilości danych. Liczba pakietów danych, które nadawca może wysłać przed otrzymaniem potwierdzenia, jest określana jako rozmiar okna lub okno.

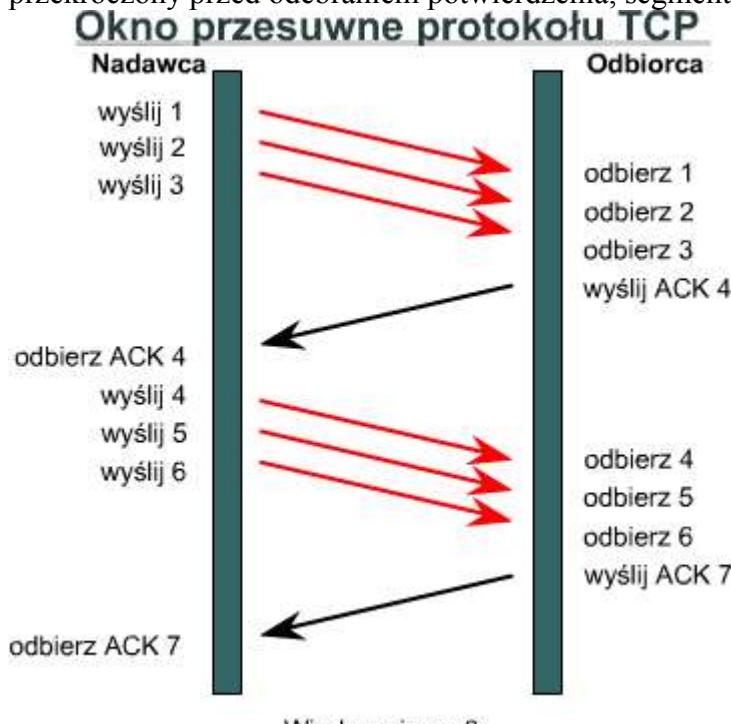
Protokół TCP wykorzystuje potwierdzenia typu expectational. Potwierdzenia typu expectational oznaczają, że numer potwierdzenia odnosi się do pakietu, który jest oczekiwany jako następny. Obrazowym pojęciem opisującym dynamiczną negocjację rozmiaru okna podczas sesji TCP jest okienkowanie. Okienkowanie to mechanizm kontroli przepływu. Wymaga ono, żeby urządzenie źródłowe otrzymywało od adresata potwierdzenie po wysłaniu określonej ilości danych. Odbierający proces TCP zgłasza „okno” do wysyłającego procesu TCP. Okno to określa liczbę pakietów, poczynając od numeru potwierdzenia, do których odebrania jest obecnie gotów odbierający proces TCP.

Przy rozmiarze okna równym 3 urządzenie źródłowe może wysłać do adresata trzy bajty. Urządzenie źródłowe musi następnie czekać na potwierdzenie. Gdy adresat otrzyma trzy bajty, wysyła potwierdzenie do urządzenia źródłowego, które teraz może wysłać kolejne trzy bajty. Jeśli adresat z powodu przepelnienia buforów nie otrzyma tych trzech bajtów, to nie wyśle potwierdzenia. Ponieważ źródło nie otrzyma potwierdzenia, będzie to oznaczało, że bajty powinny być wysłane ponownie, a szybkość transmisji powinna zostać zmniejszona.

Jak pokazano na rysunku, nadawca wysyła trzy pakiety przed rozpoczęciem oczekiwania na potwierdzenie ACK. Jeśli odbiorca może obsłużyć okno o rozmiarze tylko dwóch pakietów, z okna odrzucony zostaje pakiet trzeci, określa się go jako następny, a nowa wartość rozmiaru okna jest określana jako dwa. Nadawca wysyła kolejne dwa pakiety, lecz ma ciągle ustawiony rozmiar okna równy trzy. Oznacza to, że nadawca będzie nadal oczekiwał potwierdzenia od odbiorcy po wysłaniu trzech pakietów. Odbiorca odpowiada, żądając piątego pakietu i nadal określając rozmiar okna równy dwa.

### 11.1.6 Potwierdzenia

Niezawodne dostarczanie gwarantuje, że strumień danych wysłany z jednego urządzenia jest dostarczony przez łącze danych do innego urządzenia bez powielenia lub utraty danych. Potwierdzenie pozytywne wraz z retransmisją jest techniką, która gwarantuje niezawodne dostarczanie danych. Potwierdzenie pozytywne wymaga, by odbiorca po odebraniu danych skontaktował się ze źródłem i wysłał wiadomość potwierdzającą. Nadawca zachowuje zapis dotyczący każdego wysłanego pakietu danych (segmentu TCP) i oczekuje na potwierdzenie. W momencie wysłania segmentu zostaje również przez nadawcę uruchomiony zegar. Jeśli założony czas zostanie przekroczony przed odebraniem potwierdzenia, segment będzie ponownie wysłany.



**Na rysunku został zaprezentowany nadawca wysyłający pakiety danych 1, 2 i 3. Odbiorca potwierdza odbiór pakietów przez żądanie pakietu 4. Po odbiorze potwierdzenia nadawca wysyła pakiety 4, 5 i 6. Jeśli pakiet 5 nie dotrze do celu, odbiorca wysyła potwierdzenie z żądaniem ponownego wysłania pakietu 5. Nadawca wysyła ponownie pakiet 5, po czym odbiera potwierdzenie z żądaniem kontynuacji transmisji poczawszy od pakietu 7.**

Protokół TCP zapewnia kolejność segmentów poprzez potwierdzenia odnoszące się do następnego w kolejności segmentu. Przed wysłaniem każdy segment jest numerowany. Po stronie stacji odbierającej protokół TCP ponownie składają segmenty w całą wiadomość. Jeśli numer sekwencyjny w szeregu został opuszczony, segment ten jest transmitowany ponownie. Segmente, które nie zostały potwierdzone w zadany czasie, zostaną wysłane ponownie.

### Control Protocol

### 11.1.7 Protokół TCP (ang. Transmission

Protokół TCP jest należącym do warstwy 4 protokołem zorientowanym połączeniowo, który zapewnia niezawodną transmisję danych w trybie pełnego dupleksu. TCP jest częścią stosu protokołów TCP/IP. W środowisku zorientowanym połączeniowo przed rozpoczęciem transferu informacji musi zostać ustanowione połączenie między dwoma stacjami końcowymi. Protokół TCP jest odpowiedzialny za podział wiadomości na segmenty, ponowne złożenie ich na stacji docelowej, ponowne wysłanie wszystkich nieodebranych informacji i scalenie wiadomości z segmentów. Zapewnia on obwód wirtualny pomiędzy aplikacjami użytkowników końcowych.

#### **Protokoly, które wykorzystują protokół TCP:**

- protokół FTP (ang. *File Transfer Protocol*),
- protokół HTTP (ang. *Hypertext Transfer Protocol*),
- protokół SMTP (ang. *Simple Mail Transfer Protocol*),
- protokół Telnet.

#### **Poniżej podano definicje pól segmentu TCP:**

- **port źródłowy:** numer portu nadającego,
- **port odbiorcy:** numer wywoływanego portu,
- **numery sekwencyjne:** numery używane do zapewnienia prawidłowej kolejności nadchodzących danych,
- **numer potwierdzenia:** następny oczekiwany oktet TCP,
- **HLEN:** liczba 32-bitowych słów w nagłówku,
- **zarezerowane:** pole ustawione na wartość zero,
- **bity kodowe:** funkcje sterujące (na przykład nawiązywanie i kończenie sesji),
- **okno:** liczba oktetów, którą zaakceptuje nadawca,
- **suma kontrolna:** suma kontrolna obliczona na podstawie pól nagłówka i danych,
- **wskaźnik pilności:** (ang. *Urgent Pointer*) określa koniec pilnych danych,
- **opcja:** jedna obecnie definiowana opcja — maksymalny rozmiar segmentu TCP,
- **dane:** dane protokołu wyższej warstwy.

#### **Format segmentu protokołu TCP**

Bit 0	Bit 15	Bit 16	Bit 31
Port źródłowy (16)		Port docelowy (16)	
Numer sekwencyjny (32)			
Numer potwierdzenia (32)			
Długość nagłówka (4)	Zarezerowane (6)	Bity kontrolne (6)	Okno (16)
Suma kontrolna (16)			Wskaźnik pilności (16)
Opcje (0 lub 32, jeśli istnieją)			
Dane (zmienna długość)			



#### **11.1.8 Protokół UDP (ang. User Datagram Protocol)**

#### **Format datagramu protokołu UD**

Bit 0	Bit 15	Bit 16	Bit 31
Port źródłowy (16)		Port docelowy (16)	
Długość (16)		Suma kontrolna (16)	
Dane (jeśli istnieją)			



**Nie ma pól numeru kolejnego i potwierdzenia**

Protokół UDP jest bezpołączeniowym protokołem transportowym należącym do stosu protokołów TCP/IP.

Protokół UDP to prosty protokół wymiany datagramów bez potwierdzania czy gwarancji ich dostarczenia.

Przetwarzanie błędów i retransmisja muszą być obsłużone przez protokoły wyższych warstw.

Protokół UDP nie wykorzystuje mechanizmów okienkowania ani potwierdzeń, więc niezawodność, jeśli jest wymagana, musi być zapewniana przez protokoły warstwy aplikacji. Protokół UDP jest zaprojektowany dla aplikacji, które nie mają potrzeby składania sekwencji segmentów.

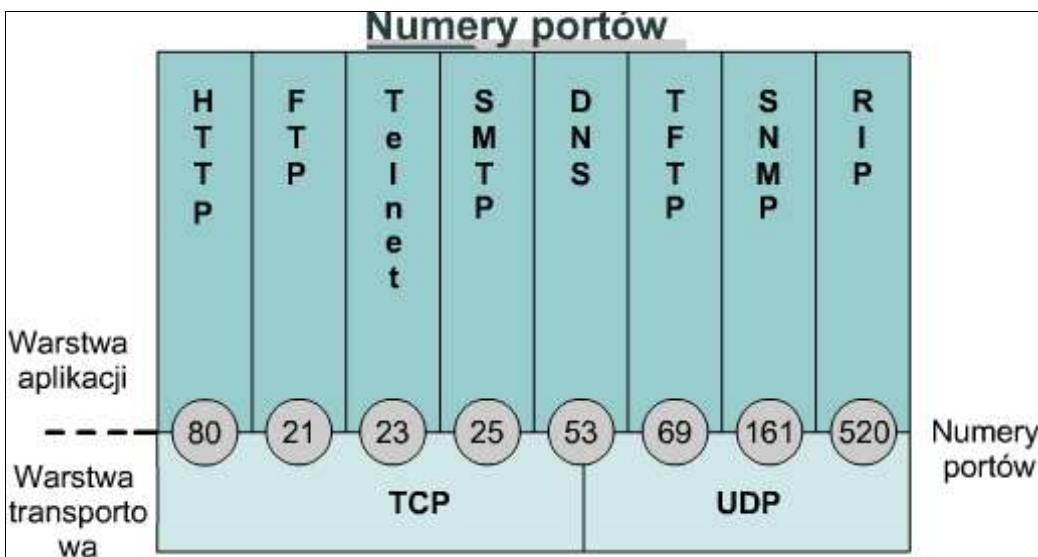
#### **Protokoły, które wykorzystują protokół UDP:**

- protokół TFTP (ang. *Trivial File Transfer Protocol*),
- protokół SNMP (ang. *Simple Network Management Protocol*),
- protokół DHCP (ang. *Dynamic Host Control Protocol*),
- protokół DNS (ang. *Domain Name System*).

#### **Poniżej podano definicje pól segmentu UDP:**

- **port źródłowy:** numer portu nadającego,
- **port odbiorcy:** numer wywoływanego portu,
- **długość:** liczba bajtów nagłówka i danych,
- **suma kontrolna:** suma kontrolna obliczona na podstawie pól nagłówka i danych,
- **dane:** dane protokołu wyższej warstwy.

### 11.1.9 Numery portów wykorzystywanych w protokołach TCP i UDP



wykorzystywane standardowe numery portów 20 i 21. Port 20 jest przeznaczony dla transmisji danych, zaś port 21 jest używany do sterowania. Do konwersacji, które nie dotyczą aplikacji z przypisany dobrym znakom numerem portu, numery portów są przydzielane losowo z określonego zakresu powyżej numeru 1023. Niektóre porty są zarezerwowane zarówno w protokole TCP, jak i UDP, lecz aplikacje mogą ich nie obsługiwać. **Numery portów mają przydzielone następujące zakresy:**

- Numery poniżej 1024 są uważane za dobrze znane numery portów.
- Numery portów powyżej 1023 są przydzielane dynamicznie.
- Zarejestrowane numery portów to takie, które zostały zarejestrowane dla określonych aplikacji producenta. Większość z nich znajduje się powyżej numeru 1024.

Numery portów są wykorzystywane przez systemy końcowe do wyboru właściwej aplikacji. Host źródłowy dynamicznie przydziela numery portów źródła rozpoczęcej transmisję. Numery te są zawsze większe od 1023.

## 11.2 Warstwa aplikacji

### 11.2.1 Wprowadzenie do warstwy aplikacji modelu TCP/IP

W procesie projektowania modelu TCP/IP w jego warstwie aplikacji zostały zawarte warstwy sesji i prezentacji modelu OSI. Oznacza to, że reprezentacja danych, kodowanie i sterowanie konwersacją są obsługiwane w warstwie aplikacji zamiast w osobnych, niższych warstwach, jak to ma miejsce w modelu OSI. Taki projekt zapewnia projektantom oprogramowania maksymalną elastyczność na poziomie warstwy aplikacji modelu TCP/IP.

**Protokoły TCP/IP, obsługujące przesyłanie plików, pocztę elektroniczną i zdalne logowanie, są prawdopodobnie najlepiej znane użytkownikom Internetu. Protokoły te obejmują następujące aplikacje:**

- protokół DNS (ang. *Domain Name System*),
- protokół FTP (ang. *File Transfer Protocol*),
- protokół HTTP (ang. *Hypertext Transfer Protocol*),
- protokół SMTP (ang. *Simple Mail Transfer Protocol*),
- protokół SNMP (ang. *Simple Network Management Protocol*),
- protokół Telnet

W protokołach TCP i UDP numery portów (gniazd) są wykorzystywane do przekazywania informacji do wyższych warstw. Numery portów służą do rozróżniania różnorodnych konwersacji odbywających się w tym samym czasie w sieci. Projektanci aplikacji uzgodnili korzystanie z dobrze znanych numerów portów wydanych przez komitet Internet Assigned Numbers Authority (IANA). W każdym dialogu między aplikacjami FTP są



**11.2.2 System DNS** Internet bazuje na hierarchicznym schemacie adresowania. Umożliwia on oparcie routingu na klasach adresów zamiast na pojedynczych adresach.

## Warstwa aplikacji

### Światowe domeny ogólne

- COM** - Domena ta jest przeznaczona dla jednostek komercyjnych, tzn. dla przedsiębiorstw. Ze względu na wielki rozrost tej domeny istnieje obawa o obciążenie administracyjne i wydajność systemu, jeśli przyrost utrzyma się na obecnym poziomie. Rozważa się podział domeny COM i pozwolenie na przyszłą rejestrację jednostek komercyjnych w domenach podrzędnych.
- EDU** - Domena ta była pierwotnie przeznaczona dla wszystkich instytucji edukacyjnych. Zostało tu zarejestrowanych wiele uniwersytetów, szkół, college'ów, organizacji oferujących usługi edukacyjne oraz konsorcjów edukacyjnych. Ostatnio została podjęta decyzja o ograniczeniu dalszej rejestracji do czteroletnich college'ów i uniwersytetów. Szkoly i college'e dwuletnie mają być rejestrowane w domenach krajowych (zob. poniżej fragment dot. domeny US, szczególnie K-12 oraz CC).
- NET** - Domena ta przeznaczona jest tylko dla komputerów dostawców usług sieciowych, to jest komputerów NIC i NOC, komputerów administracyjnych oraz komputerów węzłów sieciowych. Klienci dostawców usług sieciowych będą mieli własne nazwy domen (nie w domenie nadzędnej NET ang. Top Level Domain, TLD).
- ORG** - Domena ta jest przeznaczona jako ogólna domena TLD dla organizacji, których profil nie odpowiada innym jednostkom. Mogą tu znaleźć swoje miejsce niektóre organizacje pozarządowe.
- INT** - Domena ta jest przeznaczona dla organizacji ustanowionych na mocy umów międzynarodowych lub dla międzynarodowych baz danych.

### Ogólne domeny dotyczące tylko Stanów Zjednoczonych

- GOV** - Domena ta była pierwotnie przeznaczona dla wszelkiego rodzaju biur i agencji rządowych. Ostatnio została podjęta decyzja o tym, żeby rejestrować w tej domenie tylko agencje federalne rządu USA. Agencje stanowe i lokalne są rejestrowane w domenie krajowej.
- MIL** - Domena ta jest używana przez wojsko USA.

### Przykład kodu domeny krajowej

- US** - Domena US, jako przykład domeny krajowej, umożliwia rejestrację wszelkiego rodzaju jednostek w Stanach Zjednoczonych na podstawie podziału polityczno-administracyjnego, tzn. ma następującą hierarchię:  
<nazwa\_jednostki>.<region>. <kod stanu>. US. Na przykład:  
IBM.Armonk.NY.US. Co więcej, gałęzie domeny US w ramach każdego stanu zawierają kody dla szkół (K12), college'ów społecznych (CC), szkół technicznych (TEC), stanowych agencji rządowych (STATE), rad samorządowych (COG), bibliotek (LIB), muzeów (MUS) oraz kilku innych ogólnych typów jednostek.

### Istnieją również nazwy ogólne, których przykładami są:

- **.edu**: witryny edukacyjne,
- **.com**: witryny komercyjne,
- **.gov**: witryny rządowe,
- **.org**: witryny organizacji non-profit,
- **.net**: usługi sieciowe.

Umożliwia on oparcie routingu na klasach adresów zamiast na pojedynczych adresach. Problemem, jaki wywołuje to po stronie użytkownika, jest skojarzenie poprawnego adresu z daną witryną internetową. Bardzo łatwo zapomnieć adres IP danej witryny, gdyż nie zawiera on nic, co mogłoby się kojarzyć z jej treścią. Można sobie wyobrazić trudność zapamiętania adresów IP dziesiątek, setek czy nawet tysięcy witryn internetowych. System nazw domen został zaprojektowany po to, by skojarzyć treść witryny z jej adresem. System nazw domen (DNS) to system używany w Internecie do tłumaczenia nazw domen i ich publicznie ogłoszonych węzłów sieciowych na adresy IP. Domena jest grupą komputerów, które są ze sobą powiązane poprzez ich geograficzną lokalizację lub typ prowadzonej działalności. Nazwa domeny jest łańcuchem znaków, cyfr lub kombinacją obu. Zwykle nazwa domeny będzie nazwą lub skrótem reprezentującym adres numeryczny witryny internetowej. W Internecie istnieje ponad 200 domen górnego poziomu, których przykładami są:

- **.us**: Stany Zjednoczone (United States),
- **.uk**: Wielka Brytania (United Kingdom).

### 11.2.3 FTP i TFTP

Protokół FTP jest niezawodną usługą zorientowaną połączeniowo, która wykorzystuje protokół TCP do przesyłania plików pomiędzy systemami obsługującymi protokół FTP. Głównym zadaniem protokołu FTP jest przesyłanie plików poprzez kopiowanie i przenoszenie ich pomiędzy serwerami i klientami. W przypadku kopowania plików z serwera protokół FTP najpierw ustanawia połączenie sterujące między klientem i serwerem. Następnie między komputerami zostaje ustanowione drugie połączenie, za pośrednictwem którego są przesyłane dane. Transfer danych może się odbywać w trybie ASCII lub w trybie binarnym. Tryby te określają sposób kodowania dla plików danych, co w modelu OSI jest zadaniem warstwy prezentacji. Po zakończeniu przesyłania plików połączenie danych zostaje automatycznie zakończone. Gdy cała sesja kopowania i przenoszenia plików jest zakończona, po wylogowaniu się i zakończeniu sesji przez użytkownika zostaje zamknięte połączenie sterujące służące do przesyłania poleceń.

Protokół TFTP jest usługą bezpołączeniową wykorzystującą protokół UDP (ang. *User Datagram Protocol*). Protokół TFTP jest używany przez router do przesyłania plików konfiguracyjnych oraz obrazów systemu Cisco IOS, a także do przesyłania plików pomiędzy systemami korzystającymi z TFTP. Protokół TFTP został zaprojektowany jako niewielki i prosty w implementacji. Dlatego też brak mu większości funkcji protokołu FTP. Protokół TFTP pozwala na odczyt i zapis plików do lub ze zdalnego serwera, lecz nie umożliwia wyświetlanego zawartości katalogów i nie ma obecnie żadnych funkcji związanych z uwierzytelnianiem użytkownika. Protokół ten jest przydatny w niektórych sieciach LAN, gdyż działa on szybciej niż protokół FTP i w stabilnym środowisku pracuje niezawodnie.

### 11.2.4 Protokół http

#### Adres URL

http://	www.	cisco.com	/edu/
Określa protokół, jaki ma być użyty przez przeglądarkę.	Identyfikuje nazwę hosta lub nazwę określonego komputera.	Reprezentuje jednostkę domeny witryny WWW.	Identyfikuje folder, w którym strona WWW jest zlokalizowana na serwerze. Ponieważ nazwa strony nie jest podana, przeglądarka załadowuje domyślną stronę określoną przez serwer.

Elementy standardowego adresu URL (ang. Uniform Resource Locator).

klient-serwer, co oznacza, że do funkcjonowania wymaga zarówno komponentów klienta, jak i serwera. Dane są prezentowane przez przeglądarkę WWW w formie multimedialnej na stronach WWW, które wykorzystują tekst, grafikę, dźwięk i pliki wideo. Strony WWW są tworzone za pomocą języka służącego do formatowania zwanego HTML (ang. *Hypertext Markup Language*). Polecenia języka HTML tak kierują pracą przeglądarki WWW na danej stronie WWW, by przedstawiła ona wygląd tej strony w określony sposób. Co więcej, język HTML określa miejsca umieszczenia tekstu, plików i obiektów, które mają być przesłane z serwera WWW do przeglądarki. Hiperłącza sprawiają, iż poruszanie się po sieci WWW jest proste. Hiperłącze jest obiektem, wyrazem, frazą lub obrazkiem na stronie WWW. Po jego kliknięciu przeglądarka zostaje przekierowana na inną stronę WWW. Strona WWW zawiera (przeważnie ukryty w opisie HTML) adres lokalizacji znany jako adres URL (ang. *Uniform Resource Locator*).

W adresie URL <http://www.cisco.com/edu/>, część „http://” informuje przeglądarkę o tym, jakiego protokołu należy użyć. Druga część, „www” jest nazwą hosta lub nazwą określonej maszyny o danym adresie IP. Ostatnia część, „/edu/”, identyfikuje położenie na serwerze określonego folderu zawierającego domyślną stronę WWW. Zwykle przeglądarka WWW otwiera się na stronie początkowej lub „domowej” (ang. *home*). Adres URL strony domowej został wcześniej zapisany w obszarze konfiguracji przeglądarki WWW i może być zmieniony w dowolnym momencie. Na stronie startowej można kliknąć jedno z hiperłączy do stron WWW lub wpisać adres URL na pasku adresu przeglądarki. Przeglądarka WWW sprawdza protokół pod kątem potrzeby otwarcia innego programu, a następnie za pomocą systemu DNS określa adres IP serwera WWW. Następnie warstwy transportowa, sieci, łącza danych i fizyczna współpracują w celu zainicjowania sesji z serwerem WWW. Dane przesyłane do serwera HTTP zawierają nazwę katalogu z lokalizacją strony WWW. Dane mogą również zawierać nazwę konkretnego pliku ze stroną HTML. Jeśli żadna nazwa nie została podana, zostaje użyta nazwa domyślna określona w konfiguracji serwera.

Serwer w odpowiedzi na żądanie wysyła do klienta WWW cały tekst, pliki audio i wideo oraz grafikę, zgodnie z instrukcjami HTML. Wszystkie te pliki zostają ponownie złożone przez przeglądarkę po stronie klienta w celu

Protokół HTTP (ang. *Hypertext Transfer Protocol*) działa w sieci WWW, która jest najszybciej rozwijającą się i najczęściej używaną częścią Internetu. Jednym z głównych powodów niezwykłego rozwoju sieci WWW jest związana z nią łatwość dostępu do informacji. Przeglądarka WWW jest aplikacją typu

utworzenia widoku strony WWW, a następnie sesja zostaje zakończona. Po kliknięciu innej strony znajdującej się na tym samym lub innym serwerze cały proces zaczyna się od nowa.

### 11.2.5 Protokół SMTP

Serwery poczty elektronicznej w celu wysyłania i odbioru poczty komunikują się ze sobą za pomocą protokołu SMTP (ang. *Simple Mail Transfer Protocol*). Protokół SMTP przesyła wiadomości e-mail w formacie ASCII, wykorzystując do tego protokół TCP.

Gdy serwer poczty elektronicznej otrzymuje wiadomość przeznaczoną dla klienta lokalnego, przechowuje ją i oczekuje, aż klient pobierze pocztę. Klienci poczty elektronicznej mogą pobierać przeznaczone dla nich wiadomości na kilka sposobów. Mogą użyć programów, które uzyskują bezpośredni dostęp do plików serwera pocztowego, lub ściągnąć pocztę za pomocą jednego z wielu protokołów sieciowych. Najbardziej popularnymi protokołami klientów poczty elektronicznej są POP3 oraz IMAP4, oba wykorzystują do transportu danych protokół TCP. Pomimo że klienci poczty elektronicznej wykorzystują do pobierania poczty takie specjalne protokoły, to prawie zawsze do jej wysyłania używają protokołu SMTP. Ponieważ do wysyłania i odbierania poczty są używane dwa różne protokoły i prawdopodobnie dwa różne serwery, zdarza się, że klienci pocztowi mogą wykonywać tylko jedno z tych zadań. Dlatego zwykle dobrze jest osobno rozwiązywać problemy dotyczące wysyłania i odbierania poczty elektronicznej.

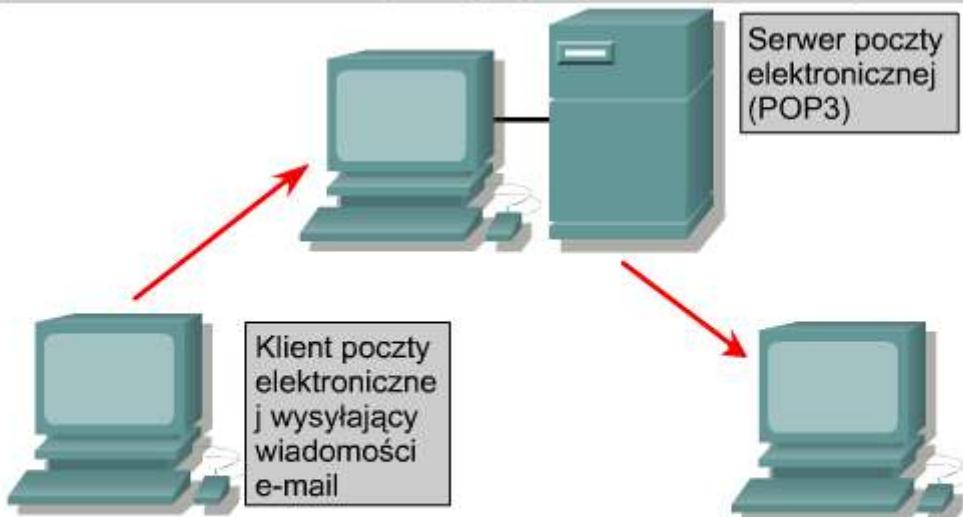
Podczas sprawdzania konfiguracji klienta pocztowego należy upewnić się, że ustawienia protokołów SMTP i POP lub IMAP są poprawnie skonfigurowane. Dobrym sposobem sprawdzenia osiągalności serwera pocztowego jest próba nawiązania połączenia Telnet z portem SMTP (25) lub POP3 (110). Aby przetestować możliwość skontaktowania się z usługą SMTP na serwerze pocztowym o adresie IP 192.168.10.5, można w wierszu poleceń systemu Windows użyć następującego polecenia:

```
C:\>telnet 192.168.10.5 25
```

Protokół SMTP nie oferuje wielu możliwości zabezpieczeń i nie wymaga żadnego uwierzytelniania.

Administratorzy często nie zezwalają hostom spoza sieci wewnętrznej na wykorzystywanie ich serwera SMTP do wysyłania lub przekazywania poczty. Robią tak, aby uniemożliwić nieautoryzowanym użytkownikom wykorzystanie ich serwerów jako przekaźników poczty (ang. *mail relay*)

### Przesyłanie wiadomości e-mail pomiędzy serwerem pocztowym a klientem



Podczas wysyłania wiadomości e-mail zaprezentowany proces ma za zadanie wysłać tę wiadomość do serwera pocztowego obsługującego danego użytkownika. Użytkownik ten następnie pobiera wiadomość z serwera pocztowego.

### 11.2.6 Protokół SNMP

Protokół SNMP (ang. *Simple Network Management Protocol*) jest protokołem warstwy aplikacji ułatwiającym wymianę pomiędzy urządzeniami sieciowymi informacji związanych z zarządzaniem.

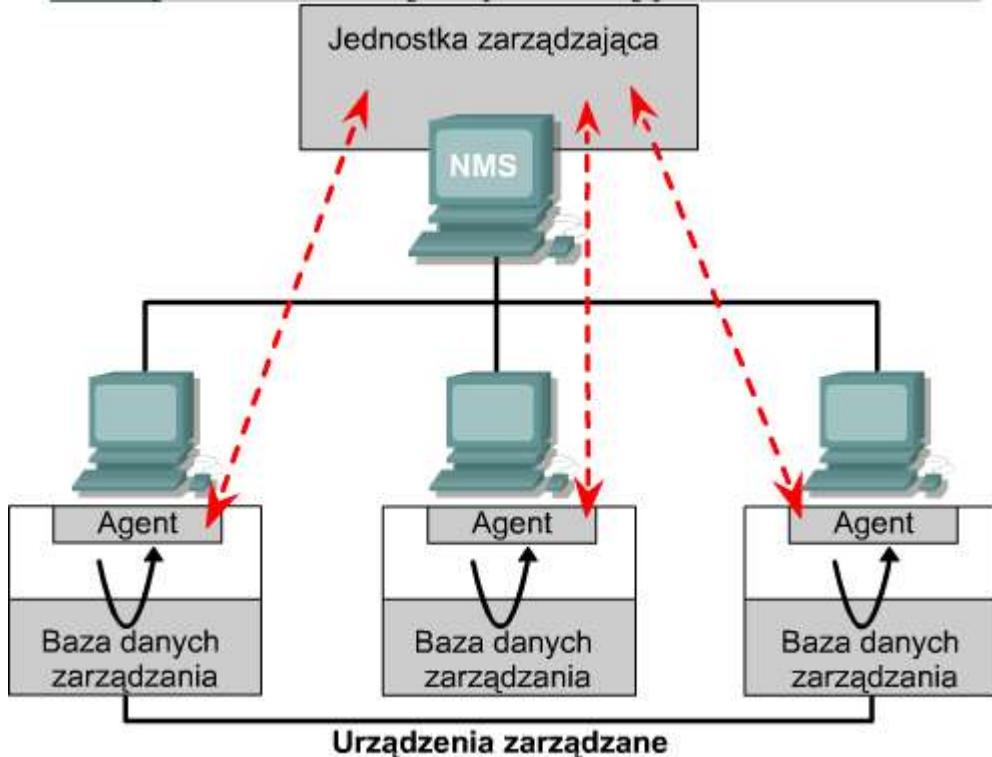
Protokół SNMP umożliwia administratorom sieci zarządzanie wydajnością sieci, odnajdywanie i rozwiązywanie problemów sieciowych oraz planowanie rozwoju sieci. Protokołem warstwy transportowej w ramach SNMP jest protokół UDP.

**Sieć zarządzana za pomocą protokołu SNMP składa się z trzech następujących elementów kluczowych:**

- **System zarządzania siecią (NMS):** system NMS uruchamia aplikacje, które monitorują i sterują urządzeniami zarządzanymi. Większość funkcji przetwarzania i zasobów pamięci wymaganych do zarządzania siecią jest zapewniana przez system NMS. W każdej zarządzanej sieci musi istnieć przynajmniej jeden system NMS.

- **Urządzenia zarządzane:** urządzenia zarządzane to węzły sieci, które zawierają agenta SNMP i są elementami zarządzanej sieci. Urządzenia zarządzane zbierają i przechowują informacje dotyczące zarządzania oraz udostępniają je systemom NMS za pomocą protokołu SNMP. Urządzeniami zarządzanymi, zwany czasem elementami sieci, mogą być routery, serwery dostępowe, przełączniki, mosty, koncentratory, komputery lub drukarki.
- **Agenci:** agenci to moduły oprogramowania do zarządzania siecią znajdujące się w zarządzanych urządzeniach. Agent ma lokalną wiedzę na temat informacji dotyczących zarządzania i tłumaczy te informacje na postać zgodną z protokołem SNMP

## Zarządzanie siecią za pomocą protokołu SNMP



### 11.2.7 Protokół Telnet

Oprogramowanie klienckie Telnet zapewnia możliwość zalogowania się do zdalnych hostów internetowych z uruchomionym serwerem Telnet, a następnie wykonywanie poleceń przy użyciu wiersza poleceń. Klient usługi Telnet jest nazywany hostem lokalnym. Serwer Telnet, wykorzystujący specjalne oprogramowanie zwane demonem, jest nazywany hostem zdalnym.

Aby nawiązać połączenie z klientem Telnet, musi zostać wybrana opcja połączenia. Zwykle pojawia się okienko dialogowe z zapytaniem o nazwę hosta i typ terminala. Nazwa hosta to adres IP lub nazwa DNS zdalnego komputera. Typ terminala opisuje rodzaj emulacji, jaką powinien realizować klient Telnet. Operacje realizowane za pomocą protokołu Telnet nie wykorzystują mocy obliczeniowej komputera transmitującego. Zamiast tego, do zdalnego hosta transmitowane są naciśnięcia klawiszy, a ekran wynikowy jest przesyłany z powrotem na lokalny monitor. Całe przetwarzanie i zapis wyników są realizowane po stronie komputera zdalnego.

Telnet pracuje na poziomie warstwy aplikacji modelu TCP/IP. Zatem protokół Telnet funkcjonuje w trzech górnego warstwach modelu OSI. Warstwa aplikacji realizuje polecenia. Warstwa prezentacji obsługuje formatowanie, zwykle w kodzie ASCII. Zadaniem warstwy sesji jest transmisja. W modelu TCP/IP wszystkie te funkcje należą do warstwy aplikacji.