3.4. Sieci komputerowe

Wstęp

Sieci komputerowe, podobnie jak systemy operacyjne, rozwijają się bardzo dynamicznie. Co chwilę słyszymy o nowych technologiach, nowych sposobach przekazywania danych, o nowych protokołach i narzędziach. Każdy z nas na co dzień spotyka się z sieciami komputerowymi. Internet jest dziś tak powszechny jak kiedyś radio czy telewizja. Nie będzie też wielkim odkryciem stwierdzenie, że internet nie istniałby, gdyby nie sieć komputerowa. Coraz popularniejsze stają się też nowe technologie, jak sieci bezprzewodowe, bluetooth czy też sieci komórkowe. Znajomość zagadnień leżących u podstaw projektowania i wykorzystywania sieci komputerowych przyda się każdemu, kto chce być na bieżąco z nowoczesnymi technologiami. W tym podrozdziale znajdziesz podstawowe informacje o sieciach komputerowych.

3.4.1. Podział sieci komputerowych

Sieć komputerowa jest zbiorem sprzętu i oprogramowania współpracujących ze sobą w celu wymiany danych lub współużytkowania zasobów.

Wymianę danych lub współużytkowanie zasobów przeprowadzają protokoły komunikacyjne, będące zbiorem reguł pozwalających na komunikowanie się. Zbiór tych reguł jest akceptowany przez obie strony wymiany danych.

Podział ze względu na zasięg

Sieci komputerowe można podzielić ze względu na rozległość. Są to sieci:

- LAN (ang. *Local Area Networks*) — lokalna, wewnętrzna sieć obejmująca najczęściej obszar pracowni, szkoły, jednego lub kilku budynków. Jest to najmniej rozległa postać sieci komputerowej.
- MAN (ang. *Metropolitan Area Networks*), zwana siecią miejską, to duża sieć komputerowa, której zasięg obejmuje aglomerację lub miasto. Tego typu sieci używają najczęściej połączeń światłowodowych do komunikacji pomiędzy wchodzącymi w jej skład rozrzuconymi sieciami LAN. Przykładem sieci miejskich są sieci budowane przez ośrodki akademickie, które łączą nie tylko budynki uniwersyteckie, lecz także ośrodki poza głównymi zabudowaniami. Takie sieci mają też połączenia WAN z innymi uniwersytetami oraz często z internetem.

- WAN (ang. *Wide Area Networks*) — sieć rozległa, łącząca ze sobą oddzielne sieci LAN i MAN. W ten sposób sieci WAN łączą geograficznie oddalonych użytkowników. Są to największe sieci komputerowe, których przykładem jest internet.

Podział ze względu na topologię

Kolejny ważny podział sieci komputerowych związany jest z ich topologią, czyli rozmieszczeniem komputerów w sieci i ich wzajemnym połączeniem.

Topologie sieci LAN mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. Topologia fizyczna określa, jak rozmieszczone są poszczególne elementy wchodzące w skład takiej sieci. Topologia logiczna opisuje wszelkie możliwe połączenia między parami mogących się komunikować punktów sieci.

Elementy fizyczne sieci to:

- komputery (hosty),
- podłączone do sieci urządzenia sieciowe (np. router, hub, switch, modem, drukarka sieciowa),
- media umożliwiające połączenie elementów sieciowych (np. okablowanie).

Oto najczęściej spotykane topologie sieciowe:

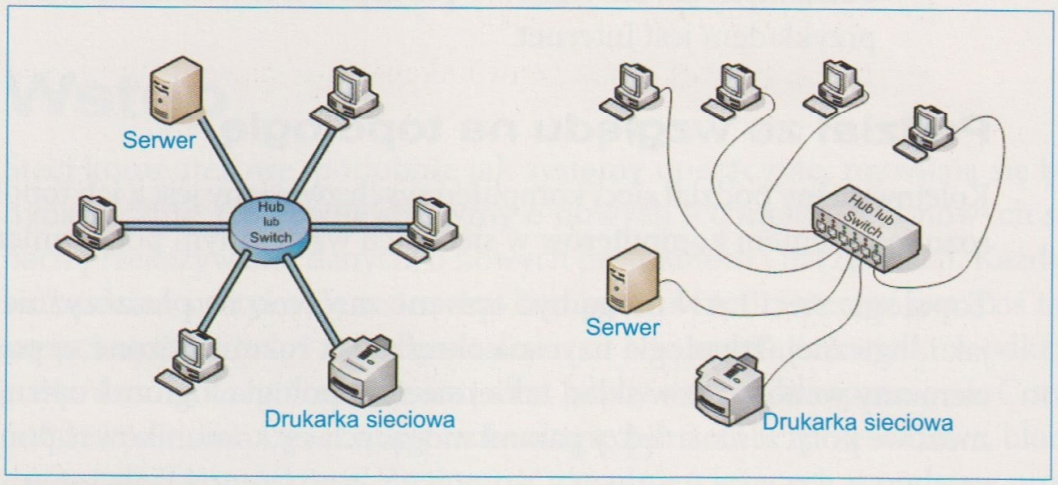
- z magistralą liniową,
- gwiazdy,
- pierścienia, podwójnego pierścienia,
- mieszane:
  - pierścień-gwiazda,
  - gwiazda-pierścień,
- drzewa,
- komórkowa.

Topologia logiczna opisuje reguły komunikacji, z których powinna korzystać każda stacja robocza (host) podczas komunikowania się w sieci. Poza połączeniem fizycznym hostów i ustaleniem standardu komunikacji, topologia fizyczna zapewnia bezbłędną transmisję danych.

Topologia gwiazdy (ang. *star*)

Z połączeniem takim mamy do czynienia wtedy, gdy wszystkie elementy sieci podłączone są do jednego węzła centralnego, jak na rysunku 3.22. Funkcję węzła centralnego mogą pełnić urządzenia sieciowe takie jak koncentrator (hub) lub przełącznik (switch). Uszkodzenie węzła centralnego skutkuje paraliżem

całej sieci. Z kolei uszkodzenie jednego z połączeń powoduje jedynie zerwanie połączenia z danym komputerem, a pozostała część sieci działa poprawnie.

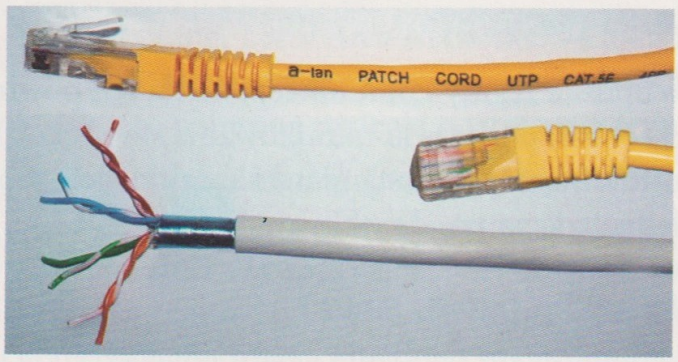


Rysunek 3.22. Topologia gwiazdy

Połączenia między komputerami a węzłem centralnym realizowane są za pomocą popularnej skrętki (rysunek 3.23). Skrętka wyróżnia się dużą niezawodnością. Jej użycie obniża koszty budowy sieci. Rozróżniamy dwa rodzaje tego typu kabla:

- kabel ekranowany **STP** (ang. *Shielded Twisted Pair*) lub ekranowany foliowany **FTP** (ang. *Foiled Twisted Pair*),
- kabel nieekranowany **UTP** (ang. *Unshielded Twisted Pair*).

Kable ekranowane zmniejszają straty transmisji oraz zwiększają odporność na zakłócenia. Mimo to powszechnie stosuje się skrętkę nieekranowaną (zapewne z powodów ekonomicznych). Jednak wszędzie tam, gdzie występują pola magnetyczne i gdzie konieczna jest niezawodność działania sieci (w szpitalach, wojsku, bankach), stosuje się skrętkę ekranowaną.



Rysunek 3.23. Skrętka STP (ekranowana) z czterema parami przewodów i kabel zakończony wtyczką RJ-45

Odległości pomiędzy komputerami a hubem lub switchem nie powinny przekraczać 100 metrów. Jest to dominujące rozwiązanie we współczesnych sieciach LAN.

Zalety:

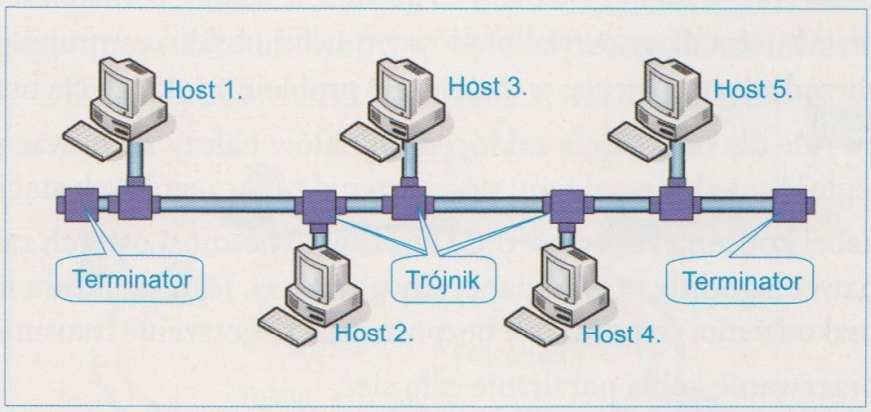
- łatwa konserwacja i lokalizacja uszkodzeń,
- prosta rekonfiguracja sieci,
- proste (łatwe) podłączenie kolejnego urządzenia sieciowego,
- stosunkowo szybka komunikacja w sieci,
- niezawodność (uszkodzenie jednego z połączeń nie paraliżuje całej sieci).

Wady:

- duża liczba kabli (tyle połączeń, ile urządzeń),
- ograniczona możliwość rozbudowy sieci,
- ograniczenie odległości komputera od koncentratora (huba) — w zależności od kategorii wynosi ona maksymalnie od 90 do około 110 m,
- w przypadku awarii huba przestaje działać cała sieć.

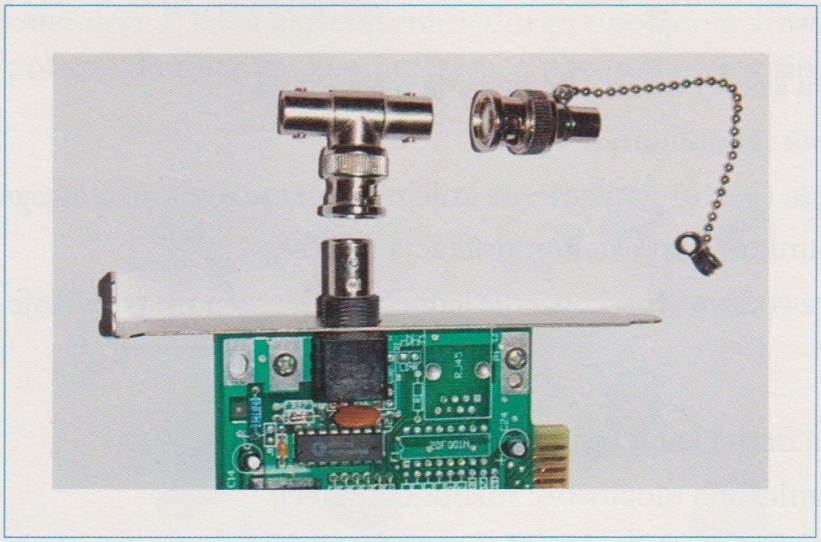
Topologia magistrali (ang. *bus*)

Topologia magistrali, zwanej czasami szyną, pokazana została na rysunku 3.24. W topologii tej nie przewidziano żadnych urządzeń pośredniczących, zatem wszystkie hosty przyłączone do sieci słuchają transmisji przesyłanych magistralą i odbierają pakiety do nich zaadresowane. Dane są przesyłane kablem do wszystkich elementów sieci. Brak dodatkowych urządzeń sprawia, że sieci lokalne oparte na topologii magistrali są proste w konstrukcji i niedrogie. Są one przeznaczone przede wszystkim do użytku w domach i małych biurach.



Rysunek 3.24.
Topologia magistrali

Typowa magistrala składa się z pojedynczego kabla łączącego wszystkie komputery (hosty) w sposób charakterystyczny dla sieci równorzędnej. Długość sieci w tej topologii nie powinna przekroczyć 185 m (licząc od jednego terminatora do drugiego). Kabel koncentryczny biegnie od komputera do komputera i jest podłączany do kart sieciowych. Każda z kart sieciowych zaopatrzona jest w złącze cylindryczne **BNC** (ang. *Bayonet Neill-Concelman*), do którego podłączany jest trójnik, jak na rysunku 3.25. W przypadku uszkodzenia kabla przestaje działać cała sieć.



Rysunek 3.25. Karta sieciowa ze złączem BNC, trójnik i terminator

Zalety magistrali:

- małe zużycie kabla, niski koszt samej sieci,
- prosta instalacja,
- bardzo prosta rozbudowa sieci,
- łatwe łączenie segmentów sieci w jeden system (bez zmian oprogramowania komunikacyjnego),
- każdy komputer jest podłączony tylko do jednego kabla.

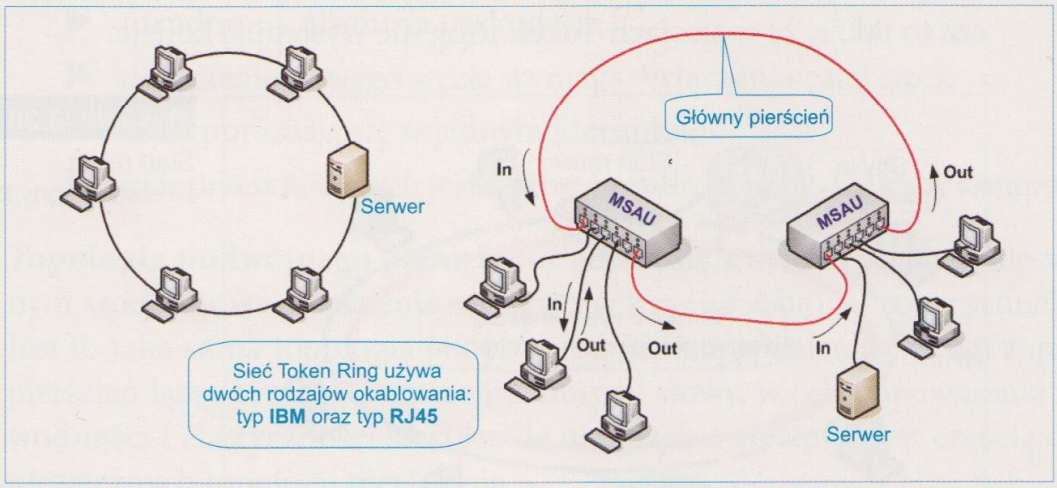
Wady magistrali:

- problem z dostępem do sieci — wszystkie komputery współużytkują jeden kabel,
- utrudniona diagnostyka błędów z powodu braku centralnego systemu zarządzającego siecią; w dużej sieci problem z lokalizacją uszkodzenia,
- zwykle dla uniknięcia zakłóceń sygnałów należy zachować pewną odległość między punktami przyłączenia poszczególnych stacji,
- kabel koncentryczny jest dość wrażliwy. Nie znosi ostrych zakrętów ani nawet łagodnie przykładanej siły gniotącej. Jego struktura łatwo ulega uszkodzeniu, co powoduje bezpośrednie pogorszenie transmisji sygnału,
- przerwanie kabla paraliżuje całą sieć,
- sieć wolna, niski transfer danych — 10 Mb/s (kabel 10 Base-2).

Topologia pierścienia (ang. *ring*)

W topologii pierścienia połączenie kablowe elementów sieciowych tworzy zamknięty pierścień, tak jak to pokazano na rysunku 3.26. W sieci Token Ring stacje sieciowe podłącza się bezpośrednio do urządzeń MSAU (ang. *Multi-Station Access Unit*), które z kolei łączy się ze sobą tak, by tworzyły jeden duży pierścień. Urządzenia MSAU mają wbudowane elementy obejściowe umożliwiające pracę

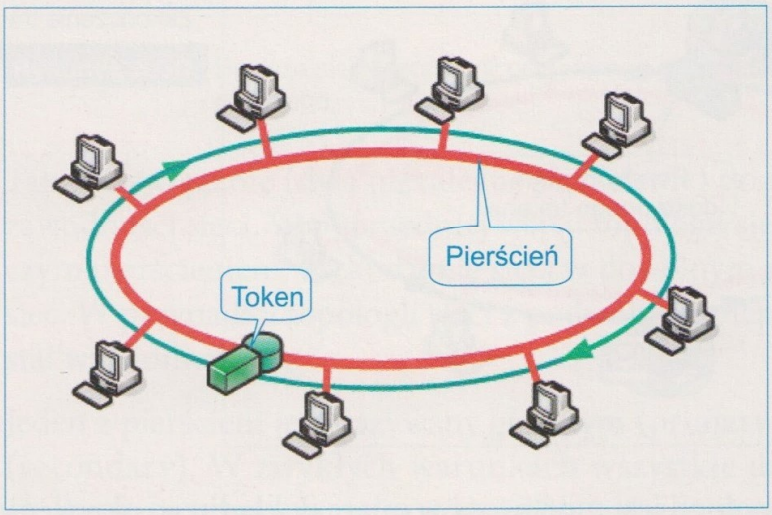
pierścienia nawet po odłączeniu dowolnej stacji z MSAU. To oznacza, że odłączenie lub awaria któregoś z komputerów nie paraliżuje sieci.



Rysunek 3.26. Topologia pierścienia (schemat ogólny, przykładowe rozwiązanie połączenia)

Dane przesyłane są wokół pierścienia, w jednym kierunku. Każda stacja robocza pobiera i odpowiada na pakiety do niej zaadresowane, a pozostałe pakiety przesyła dalej, do następnej stacji roboczej, wchodzącej w skład sieci. Jak to się dzieje?

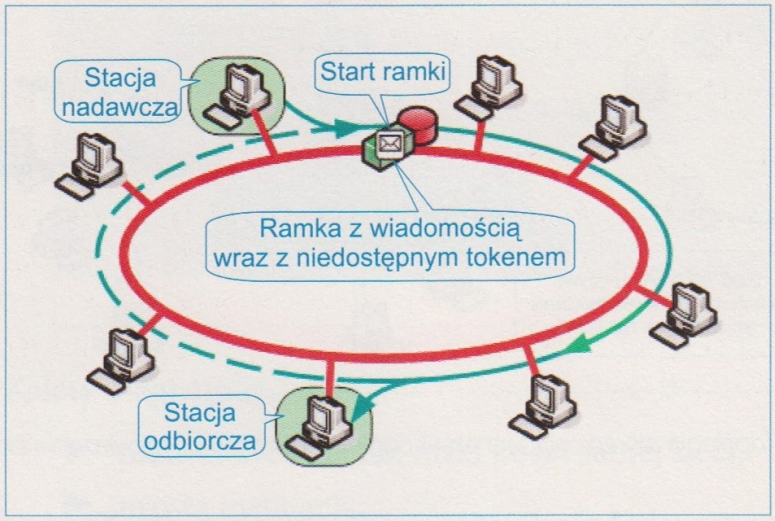
W pierścieniu sieci Token Ring krąży mała ramka, zwana tokenem (żetonem). Stacja sieciowa uzyskuje prawo do transmisji informacji tylko wtedy, gdy posiada token. Jeśli więc dowolna stacja sieciowa przejmuje token, ale w tym momencie nie zamierza transmitować danych, przesyła żeton do następnej w kolejności stacji sieciowej, co ilustruje rysunek 3.27. Każda stacja może przetrzymywać token tylko przez określony czas (np. 10 ms).



Rysunek 3.27.
Cisza w sieci — krąży token

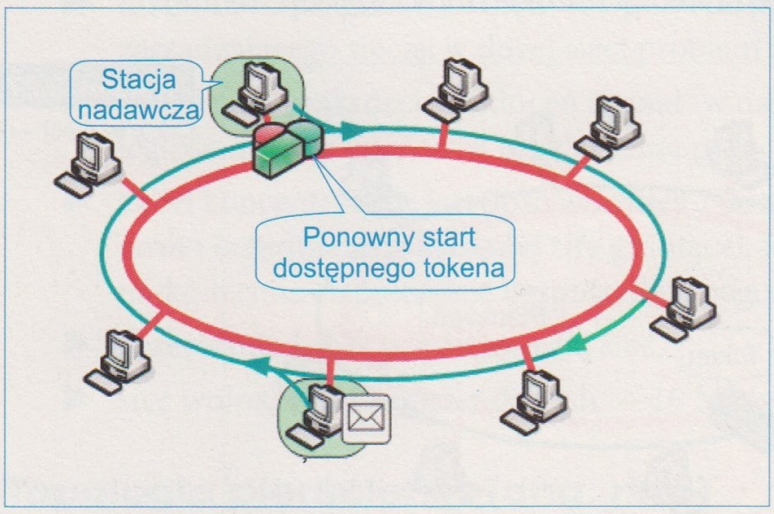
Stacja nadawcza, przy której znajdzie się token, mająca informację do przesłania, zmienia jeden bit w tokenie, co powoduje start ramki z niedostępnym tokenem, następnie dodaje informację, którą chce transmitować, po czym ca-

łość wysyła do następnej stacji w pierścieniu. W czasie, gdy ramka przesuwa się w pierścieniu, nie ma w nim dostępnego tokenu, co oznacza, że inne stacje, chcące w tym czasie rozpocząć transmisję, muszą czekać (rysunek 3.28). Oznacza to także, że w sieciach Token Ring nie występują kolizje.



Rysunek 3.28.
Start ramki — niedostępny token

Ramka informacyjna, krążąc w pierścieniu, osiąga wreszcie stację odbiorczą, która kopiuje ją do dalszego przetwarzania. Ramka kontynuuje wędrówkę w pierścieniu aż do momentu osiągnięcia stacji nadawczej. Tutaj zostaje usunięta z pierścienia. Stacja nadawcza może sprawdzić, czy ramka dotarła do stacji odbiorczej i tam została skopiowana. Stacja nie ma prawa wysłania nowej wiadomości. Po zakończeniu transmisji generuje zatem nowy token (zmienia bit) i wysyła go do następnej stacji (rysunek 3.29). Dopiero gdy ponownie otrzyma token, może wysłać nową wiadomość.



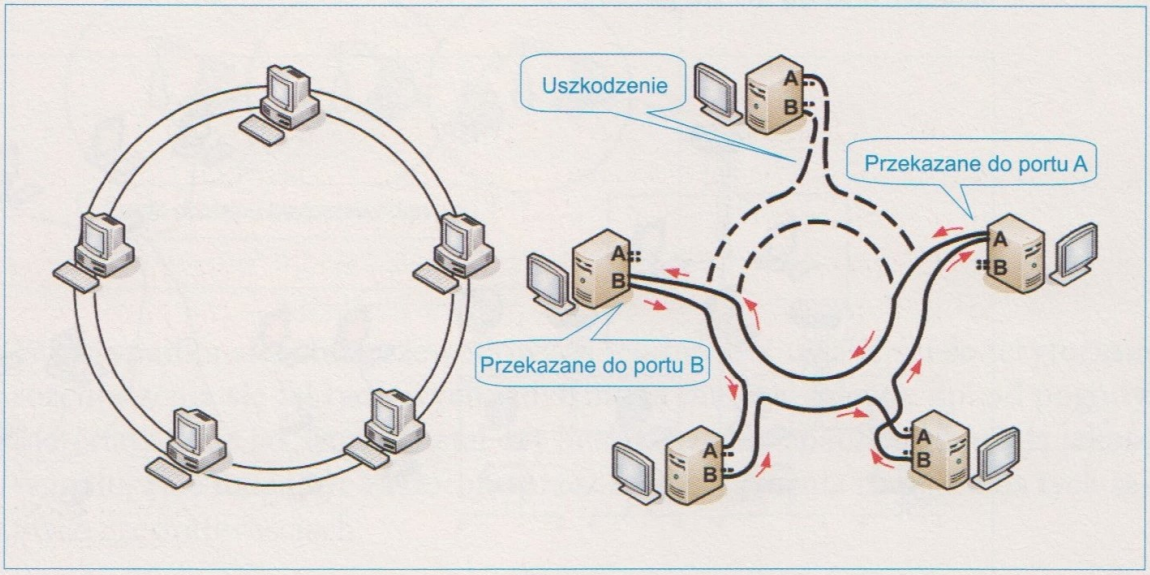
Rysunek 3.29.
Zakończenie transmisji — ponowny start tokena

Zaletą takiej topologii jest możliwość w miarę dokładnego określenia czasu odpowiedzi sieci. Czas ten się wydłuża, gdy sieć jest rozbudowana. Z kolei wadą takiej topologii jest jej unieruchomienie po przerwaniu połączenia kablowego.

Wady pierścienia:

- awaria jednego węzła lub łącza może być powodem awarii całej sieci,
- utrudniona diagnoza uszkodzeń,
- dołączenie nowego węzła wymaga wyłączenia całej sieci,
- dane poruszają się w jednym kierunku,
- czas przesyłu danych jest wprost proporcjonalny do liczby komputerów.

Topologia podwójnego pierścienia składa się z dwóch pierścieni o wspólnym środku (dwa pierścienie nie są połączone ze sobą) — zob. rysunek 3.30. Jest to taka sama topologia jak poprzednia, z tą różnicą, że drugi zapasowy pierścień łączy te same urządzenia. Innymi słowy, w celu zapewnienia niezawodności i elastyczności sieci każde urządzenie sieciowe jest częścią dwóch niezależnych topologii pierścienia.



Rysunek 3.30. Reakcja sieci w topologii podwójnego pierścienia na uszkodzenie pierścienia głównego

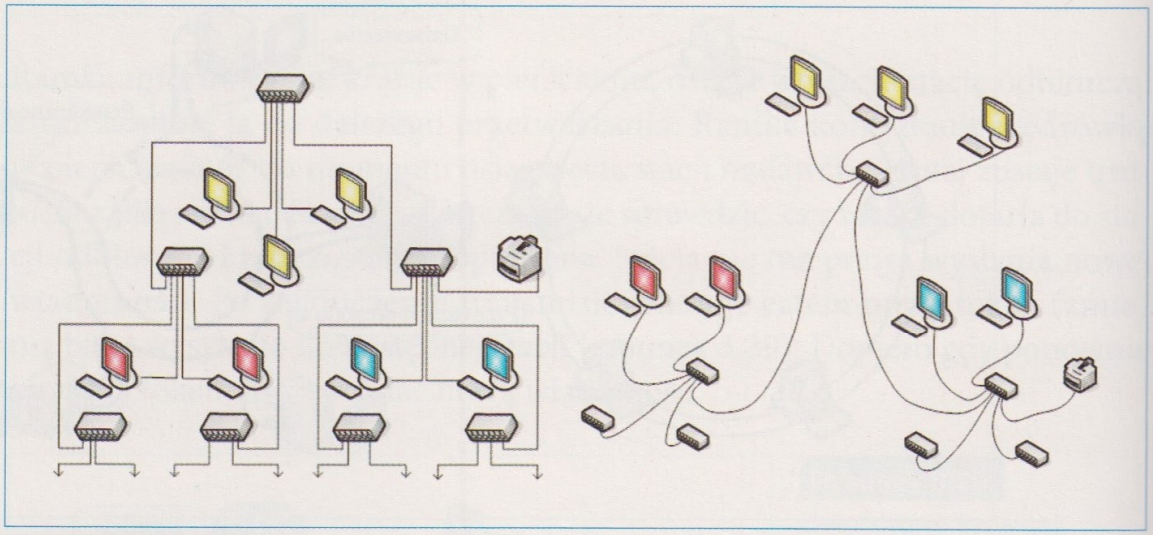
Takie rozwiązanie (dwa niezależne pierścienie) pozwala na zwiększenie niezawodności sieci. W poprzedniej wersji topologii sieci Token Ring z pojedynczym pierścieniem, uszkodzenie sieci w dowolnym miejscu paraliżowało całą sieć. W przypadku topologii sieci z podwójnym pierścieniem problem ten został wyeliminowany.

Jeden z pierścieni jest nazywany głównym (primary), drugi — pomocniczym (secondary). W zwykłych warunkach wszystkie dane krążą po pierścieniu głównym, a pomocniczy pozostaje niewykorzystany. Pierścień pomocniczy zostaje użyty wyłącznie wtedy, gdy pierścień główny ulega przerwaniu. Następuje wówczas automatyczna rekonfiguracja polegająca na przełączeniu portów i przekierowaniu sygnału do pierścienia pomocniczego w taki sposób, aby sygnał mógł nadal podążać w zamkniętym pierścieniu.

Dlatego też często spotykamy się z określeniem, że w obu pierścieniach podobne strumienie danych krążą w przeciwnych kierunkach. Ma to oczywiście miejsce wtedy, gdy pierścień pomocniczy musi być wykorzystywany podczas awarii pierścienia głównego.

Topologia drzewa (ang. *tree*)

Topologia drzewa nazywana jest także hierarchiczną. Przypomina topologię gwiazdy, z tą różnicą, że na jej zakończeniach zamiast stacji roboczych mogą być przyłączane kolejne koncentratory, do których przyłączamy kolejne stacje lub kolejne koncentratory. Dzięki temu możemy budować naprawdę duże i wydajne sieci. Istnieją dwa rodzaje tej topologii: drzewo binarne, gdzie każdy węzeł ma dwa połączenia, jak na rysunku 3.31, oraz drzewo szkieletowe, w którym węzły rozchodzą się od pnia szkieletu. Pień to przewód składający się z kilku warstw rozgałęzień. Przepływ informacji jest hierarchiczny, pierwszeństwo mają „ci na górze".



Rysunek 3.31. Drzewo binarne — topologia drzewa

Topologia ta jest bardzo elastyczna i w niektórych systemach transportu sieciowego umożliwia praktycznie dowolne konfiguracje. Wadą tego typu rozwiązania jest utrudnienie wyszukiwania błędów sieci w wypadku awarii.

Zalety:

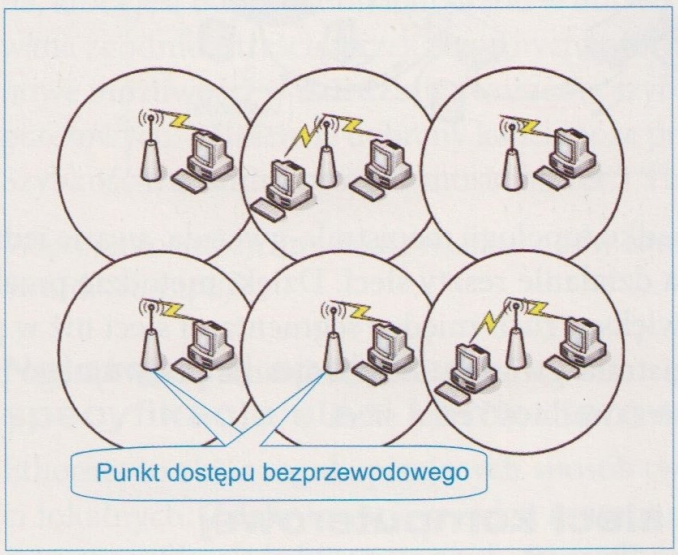
- pozwala na stosowanie krótszych przewodów,
- ogranicza liczbę urządzeń, które muszą być podłączone do centralnego węzła.

Wady:

- awaria na łączu pomiędzy koncentratorami odcina cały segment sieci.

Topologia komórkowa (ang. *cellular topology*)

Topologia komórkowa składa się z kulistych lub sześciennych obszarów, z których każdy ma jeden węzeł będący centrum. W topologii komórkowej nie ma fizycznego połączenia, dane transmitowane są za pomocą fal elektromagnetycznych, co symbolicznie ilustruje rysunek 3.32. Czasami węzły odbiorcze przemieszczają się, a czasami przemieszczają się węzły nadawcze (na przykład komunikacyjne łącze satelitarne). Oczywistą zaletą topologii komórkowej (bezprzewodowej) jest to, że nie ma tu fizycznego medium — jest atmosfera lub próżnia kosmiczna.



Rysunek 3.32.
Topologia komórkowa

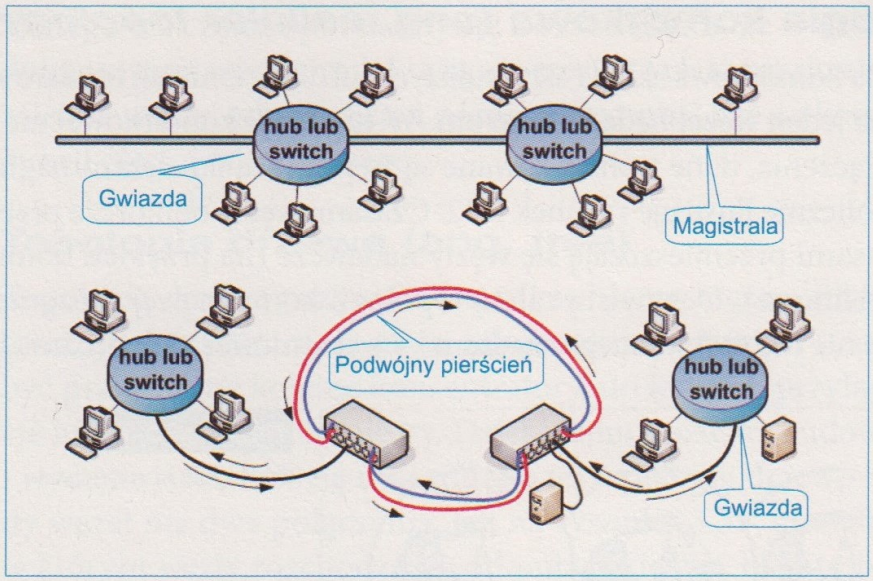
W przypadku sieci bezprzewodowych trudno jest ustalić ścisłe terytorium rozchodzenia się fal radiowych, gdyż mogą one być zależne np. od pogody. Materiały takie jak woda, metal czy beton również znacznie obniżają jakość sygnału. Fale mogą być zakłócane przez inne urządzenia nadające na tych samych częstotliwościach.

Topologia mieszana

Sieci rzadko są projektowane w postaci pojedynczej topologii. W topologii mieszanej dwie (lub więcej) topologie połączone są w jedną sieć. Na przykład można zaprojektować sieć topologii gwiazdy i magistrali w celu wykorzystania zalet każdej z nich. Dwa rodzaje topologii mieszanych są często stosowane: **magistrala-gwiazda** oraz **podwójny pierścień-gwiazda** (rysunek 3.33).

W topologii magistrala-gwiazda kilka sieci o topologii gwiazdy jest połączonych w układzie magistrali. Awaria jednego komputera nie wpływa na działanie reszty sieci. Jednakże jeśli awarii ulegnie koncentrator łączący wszystkie komputery gwiazdy, to komputery podłączone do tego urządzenia nie będą mogły komunikować się w sieci.

W topologii podwójny pierścień-gwiazda komputery są podłączone do centralnego urządzenia jak w topologii gwiazdy. Jednakże urządzenia te są połączone ze sobą w topologii podwójnego pierścienia.



Rysunek 3.33. Topologie mieszane: topologia gwiazda-magistrala oraz topologia gwiazda-podwójny pierścień

Podobnie jak w przypadku topologii magistrala-gwiazda, awaria jednego komputera nie wpływa na działanie reszty sieci. Dzięki metodzie przekazywania tokena możliwy jest większy ruch między segmentami sieci niż w przypadku sieci o topologii magistrala-gwiazda. Zastosowanie podwójnego pierścienia gwarantuje większą niezawodność całej sieci.

Specyfikacje sieci komputerowej i podstawowe media sieciowe

Przepustowość (pojemność kanału) to maksymalna ilość informacji, jaka może być przesłana przez kanał telekomunikacyjny lub łącze w jednostce czasu, mierzona w b/s (bps, ang. *bits per second*).

Przepływność to szybkość transmisji danych (ang. *bit rate*), mierzona w takich samych jednostkach jak przepustowość.

Ze względu na tę samą jednostkę, przepustowość jest mylnie utożsamiana z przepływnością. Przepływność jest miarą natężenia strumienia informacji (danych), podczas gdy przepustowość jest cechą toru lub kanału telekomunikacyjnego.

Okablowanie strukturalne

W przypadku sieci komputerowych rozróżniamy kilka podstawowych typów okablowania. Są one ściśle powiązane z zastosowaną topologią sieciową. Na przykład specyfikacja Ethernet umożliwia wykorzystanie topologii fizycznej gwiaździstej lub magistrali, ale nie umożliwia zbudowania sieci o topologii pierścienia.

W zależności od specyfikacji sieci komputerowej stosujemy różne okablowanie. Ze względu na ciągły rozwój sieci i technologii obserwujemy tworzenie nowych standardów, które umożliwiają wydajniejszą i bezpieczniejszą komunikację w sieci. Mówiąc o mediach transmisyjnych, powinniśmy pamiętać, że nie mamy tu do czynienia jedynie z sieciami opartymi na połączeniach kablowych opisanych powyżej (BNC i skrętka). Obecnie stosujemy jeszcze sieci oparte na światłowodach oraz na technologii radiowej.

W światłowodach do transmisji informacji wykorzystywana jest wiązka światła, która jest odpowiednikiem prądu w innych kablach. Wiązka ta jest modulowana zgodnie z treścią przekazywanych informacji. To rozwiązanie otworzyło nowe możliwości w dziedzinie tworzenia szybkich i niezawodnych sieci komputerowych. Właściwie dobrany kabel może przebiegać w każdym środowisku. Szybkość transmisji może wynosić nawet 3 Tb/s.

Więcej informacji na temat światłowodów zamieszczono na płycie CD w pliku *Swiatlowody.pdf*.

Najczęściej spotykane specyfikacje sieci komputerowej

Ethernet to zbiór reguł opisujących sposób tworzenia i działania głównie sieci lokalnych. Zdefiniowano między innymi sposoby przesyłania informacji oraz specyfikację kabli sieciowych. Specyfikacja ta została podana w standardzie 802.3 IEEE (ang. *Institute of Electrical and Electronic Engineers* — Instytut Inżynierów Elektryków i Elektroników). Szczegółowy podział i opis specyfikacji znajduje się na płycie CD w dokumencie *Specyfikacje sieci komputerowej.pdf*.

HSPA — mobilny szerokopasmowy dostęp do internetu. Muzyka i wideo na żądanie oraz mobilna telewizja to tylko kilka przykładowych usług, które zyskują na swojej atrakcyjności dzięki wprowadzeniu HSPA (ang. *High Speed Packet Access*), czyli szybkiej transmisji pakietowej. Sieci HSPA są aktualnie komercyjnie dostępne w wielu krajach na świecie, w tym również w Polsce. Pozwalają na osiągnięcie szybkości do 14,4 Mb/s w kierunku do abonenta oraz do 1,92 Mb/s w kierunku od abonenta do sieci. Uruchomienie komercyjnej usługi HSPA w większości sieci zaowocowało bardzo dużym, ciągłym wzrostem ruchu pakietowego abonentów. Niezaprzeczalny sukces tej technologii pozwala operatorom już dziś na silną rywalizację z sieciami kablowymi w oferowaniu dostępu do internetu.

Dziś mamy do czynienia z powszechną dostępnością przenośnych urządzeń HSPA, takich jak karty PC, telefony oraz komputery przenośne z wbudowanymi modemami. Atrakcyjne taryfy, w połączeniu z imponującymi osiągami oferowanymi przez HSPA, są czynnikiem, który powoduje zwiększone zainteresowanie rynku usługami bezprzewodowej transmisji danych.

LTE (ang. *Long Term Evolution*, czyli ewolucja długofalowa) jest nazwą sieci mobilnej. Standard umożliwia zwiększenie możliwości transferu danych w systemach telefonii komórkowej. Zaproponowany przez Sony Ericsson i T-Mobile, został przyjęty w styczniu 2008 roku. Oferuje transfery na poziomie ponad 100 Mb/s (teoretycznie nawet do 300 Mb/s). LTE zostanie uruchomione w różnej gamie częstotliwości, w przedziale od 1,25 do 20 MHz. Zastosowanie będzie zależało od dostępności spektrum w danym kraju. Technologia LTE ma szansę na szybkie upowszechnienie, gdyż wprowadzenie jej nie wiąże się z koniecznością budowy zupełnie nowej infrastruktury. Niezbędne jest tylko przebudowanie istniejących stacji bazowych, by można było oferować klientom mobilny dostęp do internetu czwartej generacji (4G), w którym przeglądanie stron internetowych i wymiana plików będzie możliwa natychmiast po kliknięciu.

Urządzenia sieciowe — rozbudowa sieci

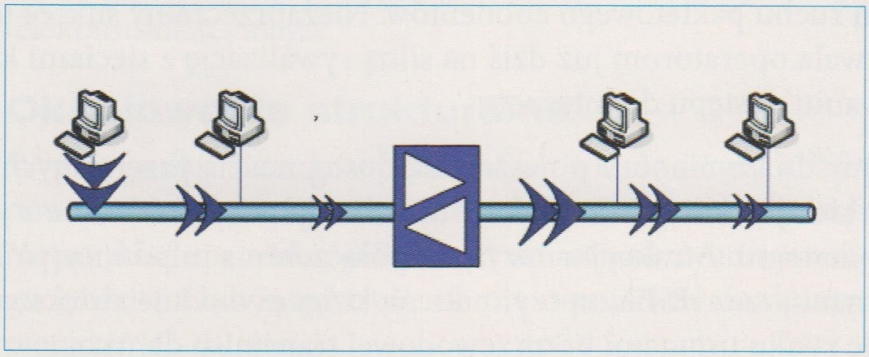
Rozwijające się firmy lub przedsiębiorstwa często stają przed problemem rozbudowy sieci komputerowej. Inne potrzebują wydajniejszej, czyli szybszej sieci. Nie można powiększać sieci jedynie przez dodanie nowych komputerów i okablowania. Każda topologia sieciowa lub architektura sieciowa ma swoje ograniczenia. Można jednak w istniejącej sieci zainstalować dodatkowe urządzenia w celu jej rozbudowy.

Urządzenia sieciowe zapewniają prawidłowe działanie sieci. Pełnią określone funkcje, takie jak: regeneracja sygnału, filtrowanie pakietów, trasowanie (routing), konwersja i translacja sygnału.

Do urządzeń umożliwiających rozbudowę sieci należą: wzmacniak, koncentrator, most, przełącznik, router.

Wzmacniak (ang. *repeater*)

Wzmacniaki odbierają sygnały i retransmitują je z oryginalną mocą i charakterystyką, co ilustruje rysunek 3.34. Jeśli kabel jest bardzo długi, sygnał słabnie i może stać się nieczytelny. Zainstalowanie wzmacniaka między segmentami kabla umożliwia przesyłanie sygnału na większe odległości.



Rysunek 3.34. Wzmacniak (*repeater*) wzmacnia sygnał, umożliwia przedłużenie sieci

Wzmacniaki nie tłumaczą i nie filtrują sygnałów. Aby wzmacniak działał prawidłowo, oba segmenty podłączone do wzmacniaka muszą używać tej samej metody dostępu. Na przykład wzmacniak nie może tłumaczyć pakietów sieci Ethernet na pakiety sieci Token Ring.

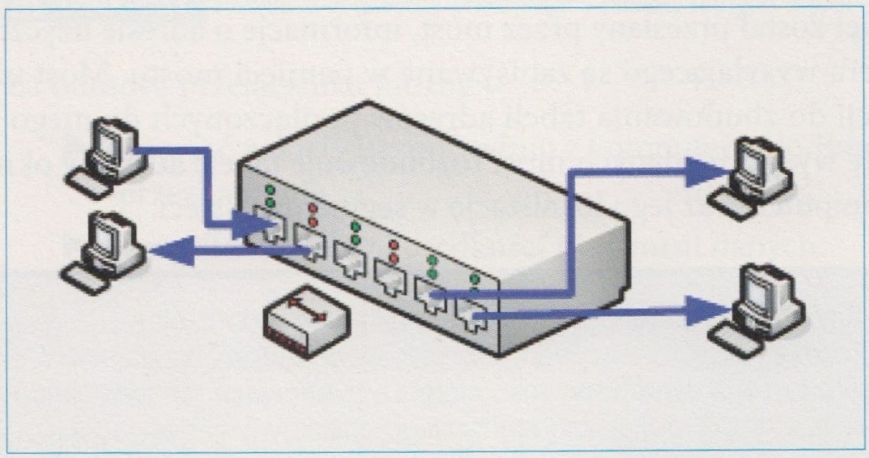
Wzmacniaki nie mogą pełnić funkcji filtrów zapobiegających problemom w ruchu sieciowym. Wzmacniaki przesyłają każdy bit danych z jednego segmentu do drugiego, nawet jeśli dane zawierają pakiety nieprawidłowe lub takie, które nie są przeznaczone dla żadnego komputera w segmencie.

Za pomocą wzmacniaka można:

- połączyć dwa segmenty podobnego lub różnego okablowania,
- regenerować sygnał w celu zwiększenia jego zasięgu,
- przekazywać cały ruch w sieci w obu kierunkach,
- połączyć dwa segmenty najtańszym kosztem.

Koncentrator (ang. *hub*)

Koncentrator to urządzenie do łączenia komputerów pracujących w topologii gwiazdy. Jeśli jest używany koncentrator, przerwanie kabla sieciowego nie wpływa na całą sieć, a jedynie na odcięty segment oraz komputery do niego podłączone. Koncentrator ma wiele portów do podłączania urządzeń sieciowych. Pojedynczy pakiet danych jest wysyłany przez koncentrator do wszystkich podłączonych komputerów. Tę zasadę działania ilustruje rysunek 3.35.



Rysunek 3.35. Koncentrator (*hub*) transmituje dane do wszystkich komputerów w topologii gwiazdy

Istnieją dwa rodzaje koncentratorów:

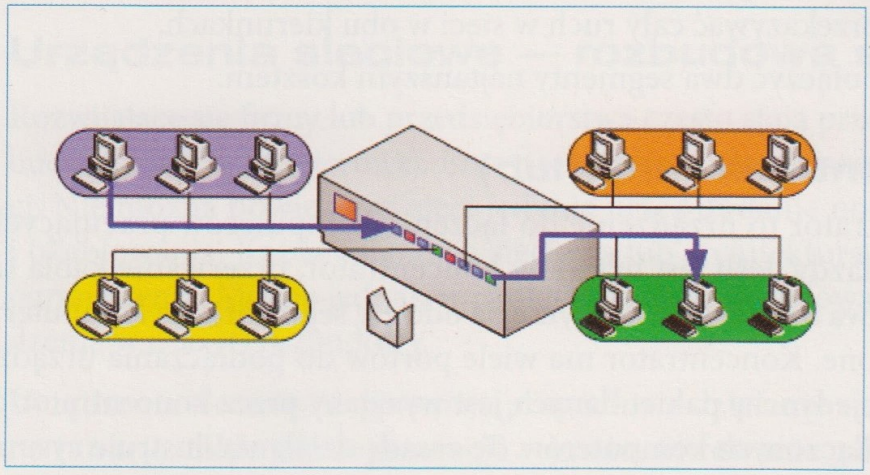
- pasywne, które wysyłają przychodzący sygnał, bez jego przetwarzania, bezpośrednio do portów,
- aktywne, czasami nazywane wzmacniakami wieloportowymi, które odbierają sygnał, przetwarzają go i retransmitują w jego oryginalnej postaci do wszystkich podłączonych komputerów i urządzeń.

Za pomocą koncentratora można:

- w łatwy sposób zmienić i rozbudować system okablowania,
- połączyć różne rodzaje okablowania poprzez różne porty koncentratora.

Most (ang. *bridge*)

Most jest urządzeniem przesyłającym pakiety danych między segmentami sieci LAN, używającymi tego samego protokołu komunikacyjnego. Most przesyła jednorazowo jeden sygnał. Jeśli pakiet jest adresowany do komputera w tym samym segmencie co komputer wysyłający, most zatrzymuje pakiet wewnątrz tego segmentu. Jeśli pakiet jest adresowany do innego segmentu, most przesyła go do tego segmentu, co pokazano na rysunku 3.36.



Rysunek 3.36. Transmisja sygnału poprzez most między dwoma segmentami sieci

Jeśli pakiet został przesłany przez most, informacje o adresie fizycznym MAC komputera wysyłającego są zapisywane w pamięci mostu. Most używa tych informacji do zbudowania tabeli adresów podłączonych do niego urządzeń. W trakcie wysyłania danych most rozbudowuje tabelę adresów określających każdy komputer oraz jego lokalizację w segmentach sieci.

Adres fizyczny MAC (ang. *Media Access Control*) to 48-bitowy niepowtarzalny adres urządzenia sieciowego jednoznacznie identyfikujący urządzenia w sieci. Sam adres składa się z dwóch głównych części — pierwsza identyfikuje producenta urządzenia, a druga rodzaj urządzenia i jego unikatowy numer.

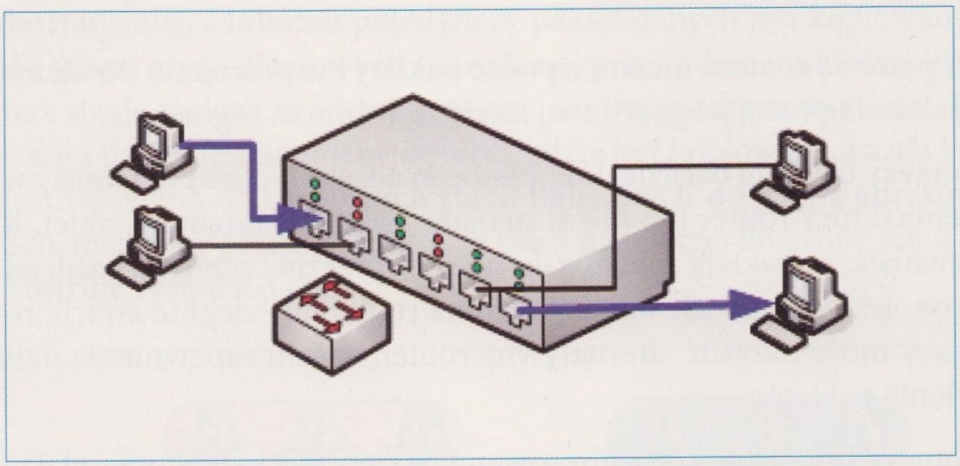
Za pomocą mostu można:

- zwiększyć liczbę segmentów,
- uwzględnić zwiększenie liczby komputerów w sieci,
- zmniejszyć wpływ zbyt dużej liczby komputerów na przepustowość sieci,
- podzielić przeciążoną sieć na dwie odseparowane sieci, aby zmniejszyć ruch w każdym segmencie i zwiększyć wydajność każdej sieci,

- połączyć różne elementy okablowania, np. skrętkę z kablem koncentrycznym.

Przełącznik (ang. *switch*)

Przełączniki działają podobnie jak mosty, lecz oferują bardziej bezpośrednie połączenie między komputerami źródłowym i docelowym. Kiedy przełącznik odbierze pakiet danych, tworzy oddzielne wewnętrzne połączenie między dwoma portami i, bazując na informacji zawartej w nagłówku każdego pakietu, przesyła pakiet dalej jedynie do portu komputera przeznaczenia, co ilustruje rysunek 3.37. Dzięki temu połączenie jest odizolowane od innych portów, a komputery źródłowy i przeznaczenia mogą w pełni wykorzystać przepustowość sieci.



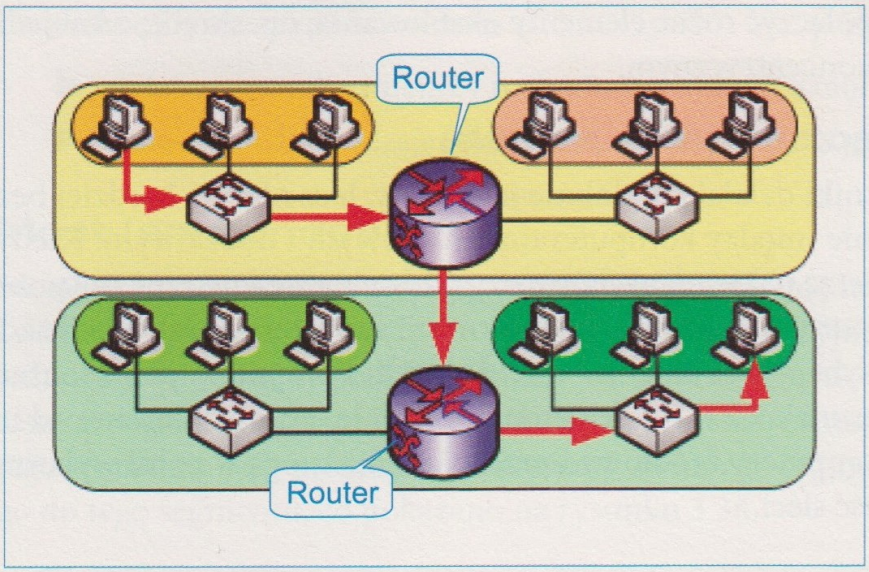
Rysunek 3.37. Przełącznik (*switch*) przesyłający pakiety danych w jednej podsieci

Za pomocą przełącznika można:

- wysyłać pakiety bezpośrednio z komputera źródłowego do komputera przeznaczenia,
- umożliwić większe prędkości transmisji danych.

Router

Router jest urządzeniem działającym podobnie jak most lub przełącznik, lecz ma dodatkowe możliwości. Przesyłając dane między różnymi segmentami sieci, routery sprawdzają nagłówek pakietu, aby określić najlepszą drogę jego przesłania. Drogę pakietu przesyłanego z jednej sieci do drugiej poprzez router ilustruje rysunek 3.38. Dzięki informacjom przechowywanym w tablicy routingu router zna ścieżki do wszystkich segmentów sieci. Zapisuje w tablicy adresy kolejnych segmentów, do których może posyłać pakiety danych. Routery umożliwiają współużytkowanie przez wszystkich użytkowników pojedynczego łącza do sieci internet.



Rysunek 3.38. Przesłanie pakietu poprzez router pomiędzy różnymi podsieciami

Za pomocą routera można wysyłać pakiety bezpośrednio do komputera przeznaczenia pracującego w innej sieci lub w innym segmencie.

Routery używają bardziej kompletnego adresu pakietu niż mosty w celu określenia, który router lub klient ma jako następny odebrać pakiet. Routery zapewniają, że pakiety wędrują do miejsca przeznaczenia najbardziej efektywną trasą. Jeśli połączenie między dwoma routerami ulegnie awarii, router wysyłający może określić alternatywny router, w celu zapewnienia dalszego przesyłania pakietów.

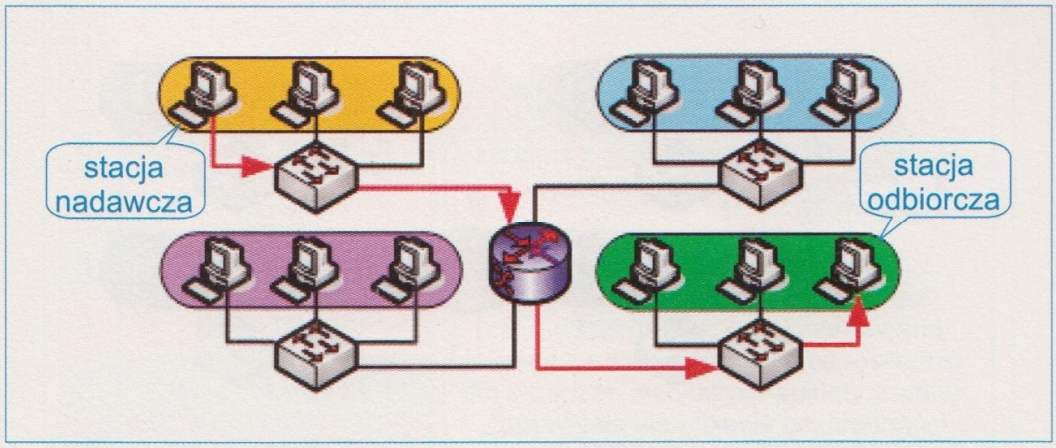
Routery czytają tylko zaadresowane pakiety sieciowe i przesyłają informacje tylko wtedy, gdy adres sieci jest znany. Dlatego routery nie przesyłają uszkodzonych danych. Możliwość kontroli przesyłanych danych przez router zmniejsza ruch między sieciami i pozwala routerom na bardziej efektywne wykorzystanie połączeń, niż jest to możliwe przy zastosowaniu mostów. Obciążenie sieci jest więc mniejsze.

Sposoby transmisji i adresowania w LAN

Wyróżnia się trzy sposoby transmisji i adresowania w sieciach lokalnych LAN:

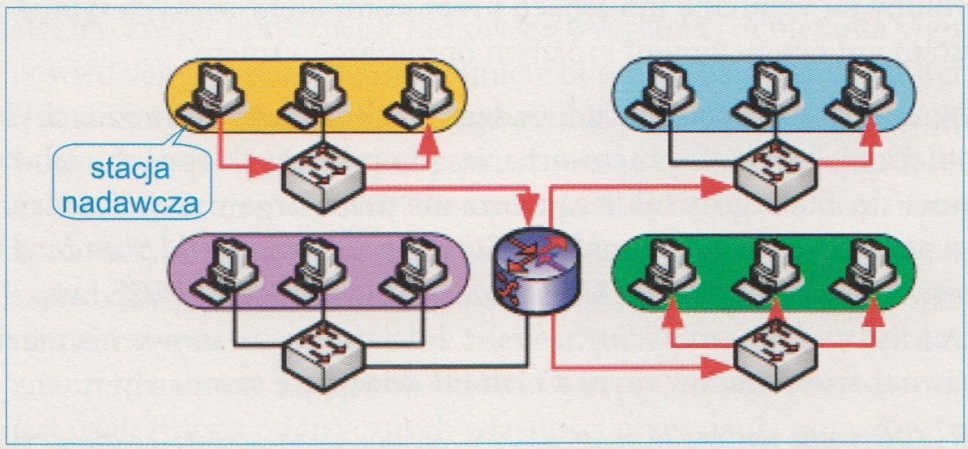
- transmisja pojedyncza Unicast,
- transmisja grupowa Multicast,
- transmisja rozgłoszeniowa Broadcast.

W transmisji Unicast pojedynczy pakiet jest wysyłany przez stację nadawczą **do jednej stacji odbiorczej**. Przedtem jednak stacja nadawcza adresuje pakiet, używając adresu stacji odbiorczej. Po zaadresowaniu pakiet jest wysyłany do sieci. Taką transmisję do pojedynczej stacji odbiorczej ilustruje rysunek 3.39.



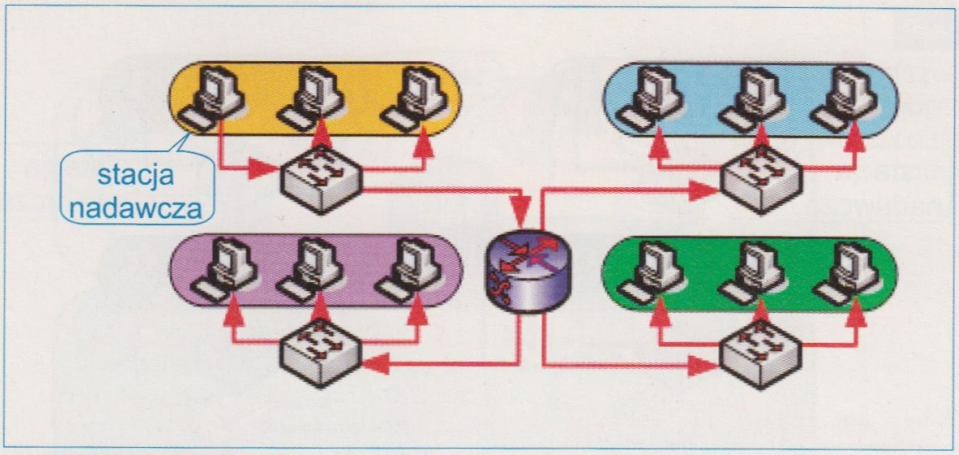
Rysunek 3.39. Transmisja do pojedynczej stacji odbiorczej — Unicast

W transmisji Multicast pojedynczy pakiet danych jest kopiowany i **wysyłany do grupy stacji sieciowych** (określonej przez adres multicast). Przedtem jednak stacja nadawcza adresuje pakiet, używając adresu multicast. Po zaadresowaniu pakiet jest wysyłany do sieci, gdzie jest kopiowany; każda kopia pakietu jest wysyłana do wszystkich stacji należących do grupy adresów multicast. Schematyczny przekaz pakietu ze stacji nadawczej do grupy stacji odbiorczych ilustruje rysunek 3.40.



Rysunek 3.40. Transmisja grupowa Multicast

W transmisji Broadcast pojedynczy pakiet jest kopiowany i wysyłany **do wszystkich stacji sieciowych**. W tym typie transmisji stacja nadawcza adresuje pakiet, używając adresu broadcast. Następnie pakiet jest wysyłany do sieci, gdzie jest kopiowany; kopie są wysyłane do wszystkich stacji sieciowych. Schematyczny przekaz pakietu ze stacji nadawczej do wszystkich stacji sieciowych ilustruje rysunek 3.41.



Rysunek 3.41 Transmisja rozgłoszeniowa Broadcast

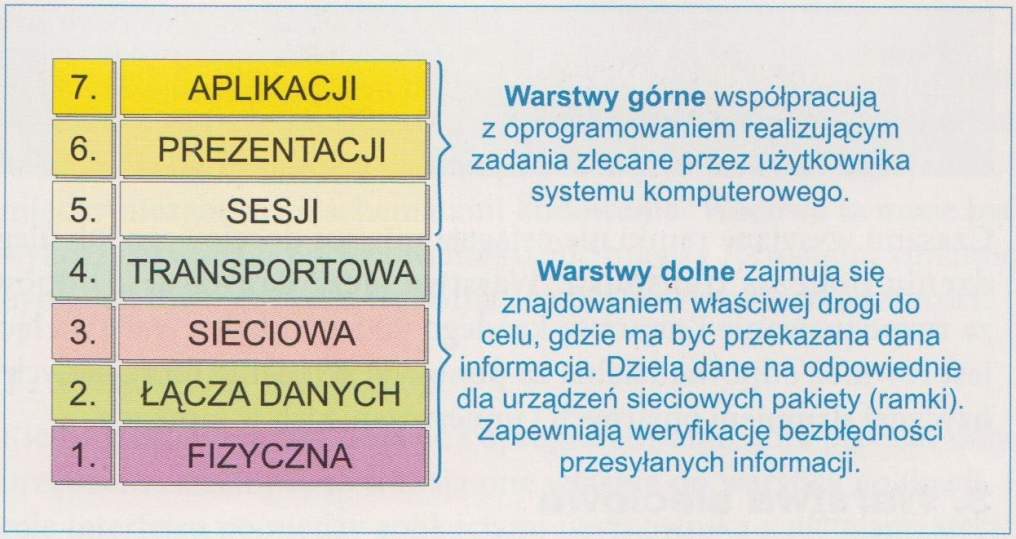
3.4.2. Model OSI

We wczesnych latach istnienia sieci transmitowanie danych poprzez sieć sprawiało wiele problemów, ponieważ duże firmy opracowywały własne, różne standardy łączenia komputerów w sieć. Aplikacje działające na różnych rodzajach komputerów, napisane przez różnych producentów, nie były w stanie komunikować się ze sobą. Niezbędne było stworzenie standardu, który pozwoliłby na wymianę informacji przez komputery różnych typów, z różnymi systemami operacyjnymi i różnym oprogramowaniem.

Aby umożliwić współpracę urządzeń pochodzących od różnych dostawców, konieczne stało się opracowanie zasad opisujących sposoby ich komunikowania się. Standardy takie są tworzone przez organizacje międzynarodowe. Do najbardziej znanych należą ISO (ang. *International Standard Organization* — Międzynarodowa Organizacja Standardów) i IEEE (ang. *Institute of Electrical and Electronic Engineers*). Chociaż ich postanowienia nie mają mocy prawnej, wiele rządów czyni z nich obowiązujące standardy.

W roku 1978 Międzynarodowa Organizacja Normalizacyjna (ISO) zaproponowała model architektury sieci, zwany modelem OSI (ang. *Open System Interconnection*) integrujący wszystkie lokalne podsieci. Był to pierwszy krok w kierunku stworzenia jednolitego standardu komunikacyjnego.

Podstawowym założeniem modelu jest podział systemów sieciowych na siedem warstw pokazanych na rysunku 3.42, współpracujących ze sobą w ściśle określony sposób. Model ten nie określa fizycznej budowy poszczególnych warstw, a koncentruje się na sposobach ich współpracy.



Rysunek 3.42. Warstwy w modelu OSI

Funkcje poszczególnych warstw

1. Warstwa fizyczna

Fundamentem, na którym zbudowany jest model referencyjny OSI, jest jego warstwa fizyczna. Określa ona wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego, radiowego wysyłania i odbierania sygnałów. Jest odpowiedzialna za przesyłanie strumieni bitów. Odbiera ramki danych z warstwy 2. (łącza danych) i przesyła szeregowo, bit po bicie, całą ich strukturę oraz zawartość. Jest ona również odpowiedzialna za odbiór kolejnych bitów przychodzących strumieni danych. Strumienie te są następnie przesyłane do warstwy łącza danych w celu ich ponownego ukształtowania. Warstwa ta ustala również szybkość wysyłania informacji, zależną od jakości połączenia. Warstwa pierwsza nie jest wyposażona w żadne mechanizmy pozwalające jej na rozróżnianie znaczenia i wagi kolejnych bitów. Operuje jedynie wartościami 1 i 0, czyli jest uzależniona od fizycznych własności przesyłania sygnałów (elektrycznych lub optycznych). Parametry przesyłu zależą od rodzaju użytego nośnika, np. od jego długości, kształtu czy impedancji. Warstwa fizyczna obejmuje procesy i mechanizmy dotyczące przenoszenia sygnałów. Nie obejmuje natomiast medium transmisyjnego, czyli nośnika (kabli koncentrycznych, skrętki, światłowodów). Media transmisyjne czasami określane są mianem warstwy zerowej.

2. Warstwa łącza danych

Jest odpowiedzialna za końcową zgodność przesyłania danych. Zajmuje się pakowaniem instrukcji danych w tzw. ramki i wysyłaniem ich do warstwy fizycznej.

Ramka jest strukturą warstwy łącza danych, która zawiera ilość informacji wystarczającą do pomyślnego przesyłania danych przez sieć lokalną do ich miejsca docelowego.

Czasami wysyłane ramki nie osiągają miejsca docelowego lub ulegają uszkodzeniu podczas transmisji. Warstwa łącza danych jest odpowiedzialna za rozpoznawanie i naprawę każdego takiego błędu. Warstwa łącza danych jest również odpowiedzialna za ponowne składanie otrzymanych z warstwy fizycznej strumieni binarnych i umieszczanie ich w ramkach.

3. Warstwa sieciowa

Warstwa sieciowa jest odpowiedzialna za określenie trasy transmisji między komputerem nadawcą a komputerem odbiorcą. Warstwa ta nie ma żadnych wbudowanych mechanizmów korekcji błędów i w związku z tym musi polegać na wiarygodnej transmisji końcowej warstwy łącza danych. Warstwa sieciowa używana jest do komunikowania się z komputerami znajdującymi się poza lokalnym segmentem sieci LAN. Umożliwia im to własna architektura trasowania, niezależna od adresowania fizycznego warstwy 2. Korzystanie z warstwy sieciowej nie jest obowiązkowe. Wymagane jest jedynie wtedy, gdy komputery komunikujące się znajdują się w różnych segmentach sieci przedzielonych routerem.

4. Warstwa transportowa

Warstwa transportowa dba o poprawność przesyłania danych. Aby informacje mogły zostać przesłane w dół, często muszą zostać podzielone na mniejsze fragmenty. Warstwa transportowa jest odpowiedzialna za przesyłanie danych i integralność transmisji. Ustala odpowiednią kolejność pakietów przed wysłaniem ich zawartości do warstwy sesji. Odpowiada za nawiązywanie połączenia, wymianę danych oraz zamykanie połączenia. Potrafi wykrywać pakiety, które zostały odrzucone przez routery i automatycznie generować żądanie ich ponownej transmisji.

5. Warstwa sesji

Warstwa sesji otrzymuje od różnych aplikacji dane, które muszą zostać odpowiednio zsynchronizowane. Warstwa ta potrafi rozpoznać połączenia między aplikacjami, dzięki czemu może zapewnić właściwy kierunek przepływu informacji. W nowoczesnych systemach sieciowych może jednocześnie pracować wiele aplikacji. Warstwa sesji odpowiada za nawiązanie sesji, zapewnienie uporządkowanej wymiany danych między aplikacjami i zamknięcie sesji, korzysta przy tym z usług warstwy transportowej (w niektórych sieciach obie warstwy są ze sobą połączone).

6. Warstwa prezentacji

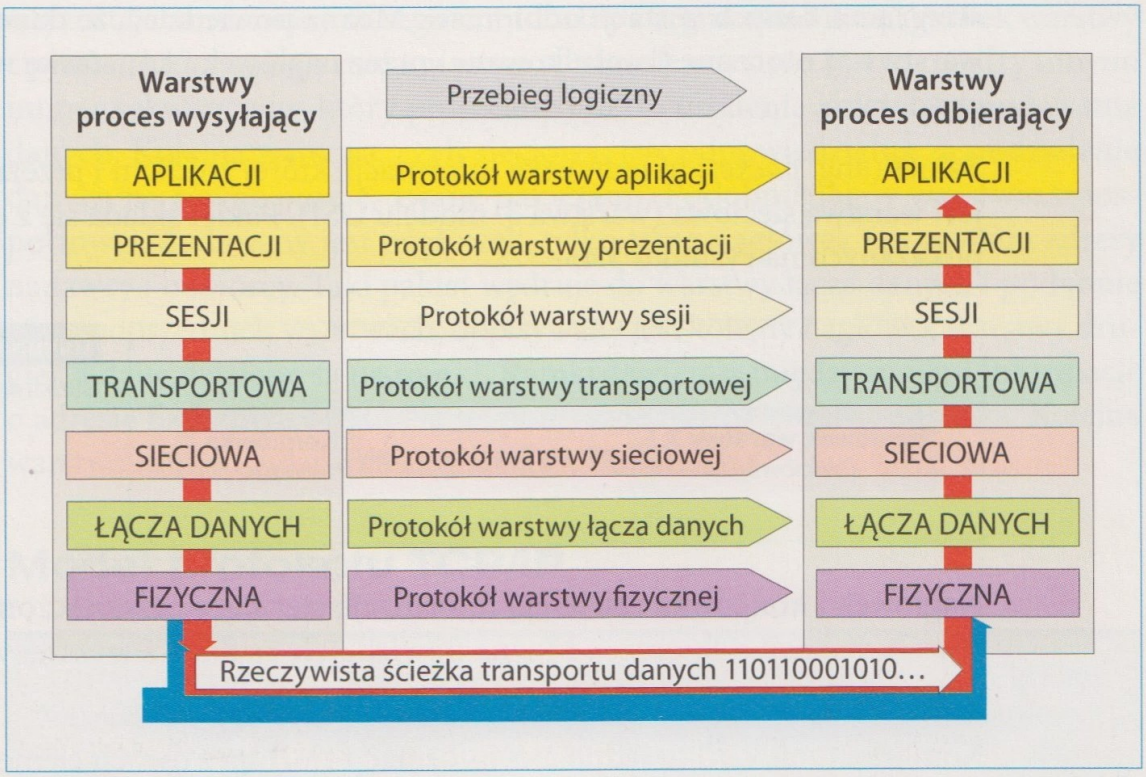
Warstwa prezentacji jest odpowiedzialna za zarządzanie sposobem kodowania wszelkich danych. Nie każdy komputer korzysta z tych samych schematów kodowania danych, więc warstwa prezentacji odpowiedzialna jest za translację między niezgodnymi schematami kodowania. Warstwa ta może być również wykorzystywana do niwelowania różnic między formatami zmiennopozycyjnymi, jak również do szyfrowania i rozszyfrowywania wiadomości.

7. Warstwa aplikacji

Kiedy użytkownik, korzystając z oprogramowania, chce przesłać dane poprzez urządzenia sieciowe, to trafiają one właśnie do warstwy aplikacji. Pełni ona rolę interfejsu pomiędzy aplikacjami użytkownika a usługami sieci. Warstwę tę można uważać za inicjującą sesje komunikacyjne.

Przepływ informacji pomiędzy warstwami

Aby dane mogły pokonać stos złożony z poszczególnych warstw, warstwy te muszą się między sobą komunikować. Co więcej — muszą być określone konkretne protokoły sieciowe, wykorzystywane do porozumiewania się. Mamy wtedy do czynienia z przebiegiem logicznym informacji pomiędzy warstwami, pokazanym na rysunku 3.43. W rzeczywistości jednak sprawa ma się nieco inaczej. Prawdziwa komunikacja odbywa się poprzez warstwę fizyczną.



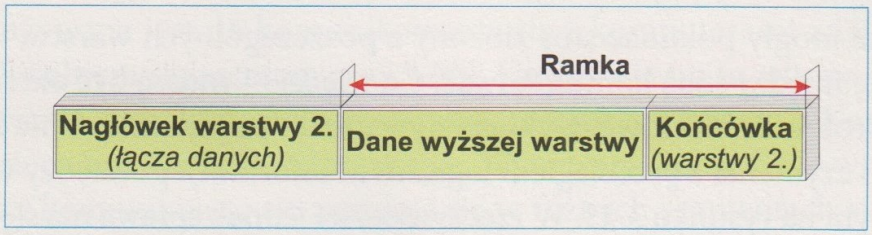
Rysunek 3.43. Komunikacja między warstwami modelu OSI

Protokoły sieciowe to zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych.

Formaty informacji przesyłanych w sieci

W sieci przesyłane są dane oraz informacje sterujące. Jedne i drugie mogą przyjmować różne formaty. Jednak aby dokładnie zrozumieć, jakie formaty informacji są przesyłane w sieci, należy poznać nazwy tych formatów. Problem z nazwami jest bardzo poważny, gdyż nie zawsze są one używane konsekwentnie, co może powodować spore nieporozumienia.

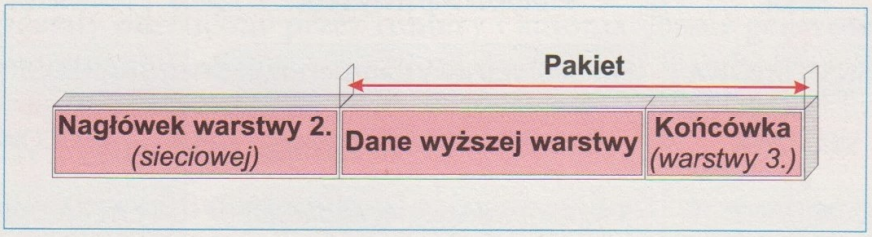
Ramka (ang. *frame*) to jednostka informacji, której źródłem i przeznaczeniem jest warstwa łącza danych (warstwa 2. modelu OSI). Ramka składa się z elementów pokazanych na rysunku 3.44.



Rysunek 3.44.
Struktura ramki

Nagłówek i końcówka zawierają informację sterującą przeznaczoną dla warstwy łącza danych w stacji odbiorczej. Można powiedzieć, że dane z wyższej warstwy są otoczone (kapsułkowane) przez nagłówek i końcówkę warstwy łącza danych.

Pakiet (ang. *packet*) to jednostka informacji, której źródłem i przeznaczeniem jest warstwa sieciowa (warstwa 3. modelu OSI). Pakiet składa się z elementów pokazanych na rysunku 3.45.



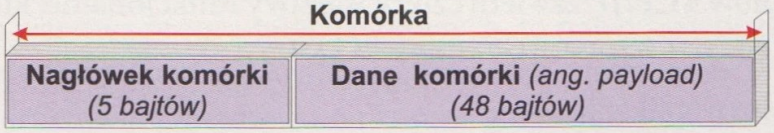
Rysunek 3.45.
Struktura pakietu

Nagłówek i końcówka zawierają informację sterującą przeznaczoną dla warstwy 3. w stacji odbiorczej. Można powiedzieć, że dane z wyższej warstwy są otoczone przez nagłówek i końcówkę warstwy 3.

Komórka (ang. *cell*) to jednostka informacji złożona z dwóch elementów:

- nagłówka komórki o długości 5 bajtów,
- danych komórki o długości 48 bajtów.

Komórka ma zawsze stałą długość 53 bajtów i odnosi się do warstwy łącza danych (warstwa 2. modelu OSI), którą schematycznie pokazano na rysunku 3.46. Komórki są używane w sieciach technologii ATM (ang. *Asynchronous Transfer Mode*) — jest to technologia związana z przenoszeniem ruchu multimedialnego i SMDS (ang. *Switched Multimegabit Data Service*).



Rysunek 3.46.
Struktura komórki

Datagram jest jednostką informacji, której źródłem i przeznaczeniem jest warstwa sieciowa (warstwa 3. modelu OSI), używająca bezpołączeniowej obsługi sieci.

Segment jest jednostką informacji, której źródłem i przeznaczeniem jest warstwa transportowa modelu OSI.

Komunikat jest jednostką informacji, której źródłem i przeznaczeniem jest zwykle warstwa aplikacji.

Jak w praktyce przebiega przekazywanie strumienia danych?

Strumień danych wypływa z warstw 7., 6. i 5. Dopiero w warstwie transportowej zostaje zamieniony na segmenty. Każdy z segmentów ma nagłówek warstwy czwartej, który zostaje nadany przez tę właśnie warstwę. Jest to między innymi numer sekwencyjny, który potrzebny jest do ustalenia kolejności podawania danych. Kolejna warstwa, czyli sieciowa, jest odpowiedzialna za podzielenie danych na równe porcje, zwane pakietami. Podobnie jak w warstwie transportowej, dodawany jest nagłówek, tylko teraz nagłówek ten zawiera adresy nadawcy i odbiorcy. Taki pakiet wędruje do warstwy łącza danych i podobnie jak w poprzednich warstwach, dopisywany jest kolejny nagłówek warstwy drugiej, a dane dzielone są na ramki. Ramki zawierają między innymi informacje o adresie fizycznym MAC. Na tej podstawie można określić adresata. Kolejna warstwa zamienia dane na ciąg znaków binarnych.

Model protokołu TCP/IP

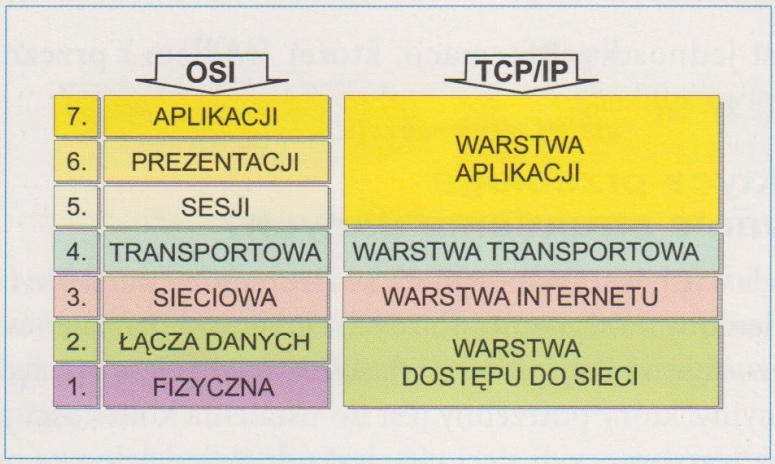
TCP/IP (ang. *Transmission Control Protocol/Internet Protocol* — protokół kontroli transmisji) jest pakietem najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. Jest następcą protokołu NCP i najczęściej obecnie wykorzystywanym standardem sieciowym, stanowiącym podstawę współczesnego internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: TCP oraz IP.

Protokół internetu (IP) został opracowany dla Departamentu Obrony USA, który szukał sposobu połączenia różnych rodzajów posiadanych komputerów i sieci je obsługujących w jedną, wspólną sieć. Osiągnięto to za pomocą warstwowego protokołu, który odizolował aplikacje od sprzętu sieciowego. Protokół ten, znany jako model TCP/IP, używa modelu nieco różniącego się od modelu OSI.

Stos protokołów TCP/IP zawiera cztery warstwy funkcjonalne, które nawiązują do siedmiu warstw wzorcowego modelu OSI:

- warstwę aplikacji,
- warstwę transportową,
- warstwę sieciową,
- warstwę dostępu do sieci.

Rysunek 3.47 przedstawia porównanie modeli OSI TCP/IP.

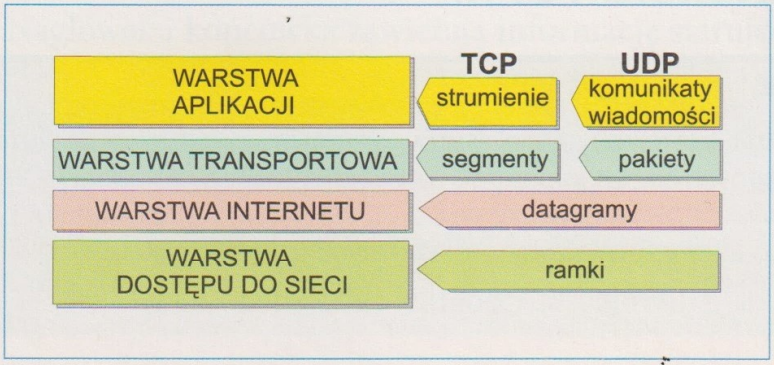


Rysunek 3.47. Porównanie modeli OSI TCP/IP

Podobnie jak w modelu OSI, kolejne warstwy dołączają lub usuwają (w zależności od tego, w którą stronę przesuwają się dane) własne nagłówki.

Dane przekazywane z TCP do IP nazywane są segmentem TCP. Dane, które IP przesyła do interfejsu sieciowego, nazywane są datagramem IP. Ciąg bitów przepływający w sieci Ethernet nazywany jest ramką.

Rysunek 3.48 przedstawia nazwy jednostek danych w kolejnych warstwach modelu TCP/IP.



Rysunek 3.48. Nazwy jednostek danych w kolejnych warstwach modelu TCP/IP

Funkcje spełniane przez poszczególne warstwy modelu OSI nie pokrywają się z funkcjami warstw modelu TCP/IP. Stąd też poziomy warstw TCP/IP nie odpowiadają poziomom warstw modelu OSI. Na powyższym rysunku została przedstawiona jedynie zbieżność nazewnictwa warstw w obu modelach.

Zadania warstw w TCP/IP

Warstwa aplikacji (ang. *process layer*), nazywana również warstwą procesową lub warstwą programów użytkowych, to najwyższy poziom, w którym pracują niezbędne dla użytkownika aplikacje takie jak serwer WWW czy przeglądarka internetowa. Obejmuje ona zestaw gotowych protokołów, które aplikacje wykorzystują do przesyłania różnego typu informacji w sieci, czyli do wysyłania lub odbierania danych w postaci pojedynczych komunikatów lub strumienia bajtów.

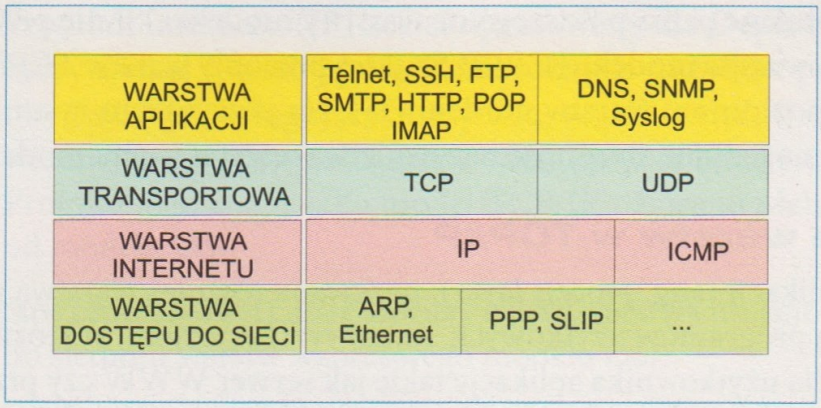
Warstwa transportowa (ang. *host-to-host layer*) — jej podstawowym zadaniem jest zapewnienie przesyłania danych oraz kierowanie właściwych informacji do odpowiednich aplikacji. Opiera się to na wykorzystaniu portów określonych dla każdego połączenia. W jednym komputerze może istnieć wiele aplikacji wymieniających dane z tym samym odbiorcą w sieci i nie nastąpi wymieszanie się przesyłanych przez nie danych. To właśnie ta warstwa nawiązuje i kończy połączenia między komputerami oraz gwarantuje pewność transmisji. W tym celu organizuje wysyłanie przez odbiorcę potwierdzenia otrzymania danych oraz ponowne wysyłanie przez nadawcę utraconych pakietów.

Warstwa sieciowa lub warstwa protokołu internetowego (ang. *internet protocol layer*), odpowiada za obsługę komunikacji jednej maszyny z drugą. Przyjmuje ona pakiety z warstwy transportowej razem z informacjami identyfikującymi odbiorcę, kapsułkuje pakiet w datagramie IP, wypełnia jego nagłówek i przekazuje datagram do interfejsu sieciowego. Niektóre urządzenia sieciowe posiadają tę warstwę jako najwyższą. Są to routery, które zajmują się kierowaniem ruchu w sieci. Proces szukania przez routery właściwej drogi określa się jako routing.

Warstwa dostępu do sieci lub warstwa fizyczna (ang. *network access layer*) jest najniższą warstwą i to ona zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi. Najczęściej są to karty sieciowe lub modemy. Realizuje ona następujące funkcje:

- sterowanie przepływem,
- ustalanie priorytetów,
- zabezpieczenie przed błędami,
- utajnienie przesyłanych danych.

Na rysunku 3.49 znajduje się zbiór usług i grupa przykładowych protokołów, które są powiązane z odpowiednimi warstwami protokołem TCP/IP.



Rysunek 3.49. Zbiór protokołów i usług poszczególnych warstw TCP/IP

W warstwie transportu działa protokół TCP, zaś protokół IP znajduje się w warstwie internetu. Warstwa transportu odpowiedzialna jest za znalezienie drogi łączącej dwa hosty oraz określenie logicznej adresacji. Host to każdy komputer podłączony do internetu lub innej sieci używającej protokołu TCP/IP i mający unikatowy adres IP.

Adres IP (ang. *Internet Protocol Address*)

Adres IP to unikatowy numer przyporządkowany urządzeniom sieci komputerowych.

IPv4

Adres IPv4 składa się z 32 bitów, a więc z 4 oktetów (oktet = 8 bitów). Przedstawiając adres w postaci czytelnej dla wszystkich użytkowników i łatwiejszy do zapamiętania, zazwyczaj wartość każdego oktetu zapisuje się osobną liczbą dziesiętną, poszczególne oktety oddzielając kropkami, np. 83.3.250.66 (każda liczba dziesiętna odpowiada 8 bitom adresu IP).

Ten ogólnie przyjęty sposób zapisu adresu IP, w sposób czytelny dla użytkownika, jest znany jako format bajtowo-dziesiętny, a taki zapis nosi nazwę notacji dziesiętnej z kropkami (ang. *dotted quad notation*).

Na przykład 32-bitowy adres 10000010 00001010 00001100 00011111 jest zapisany jako 130.10.12.31.

Fenomen tego systemu adresowania polega na tym, że umożliwia on wyznaczanie tras pakietów. Jest to możliwe dzięki temu, że adres IP zawiera informację o tym, do jakiej sieci jest włączony dany komputer, oraz jednoznaczny adres komputera w tej sieci. Adres IP jest używany przy wszystkich operacjach związanych z wymianą informacji z danym komputerem.

W obrębie adresu wyróżnia się dwa składniki: identyfikator sieciowy (ang. *network id*) oraz identyfikator komputera (ang. *host id*). Istnieją różne klasy adresowe, o różnej długości tych dwóch składników:

- Klasa A to adresy o 8-bitowym identyfikatorze sieciowym i 24-bitowym identyfikatorze hosta, czyli 8/24 (network id/host id).
- Klasa B to adresy o 16-bitowym identyfikatorze sieciowym i 16-bitowym identyfikatorze hosta, czyli 16/16 (network id/host id).
- Klasa C to adresy o 24-bitowym identyfikatorze sieciowym i 8-bitowym identyfikatorze hosta, czyli 24/8 (network id/host id).

Bity w adresie IP są zatem interpretowane jako: [adres sieci, adres hosta].

Wszystkie hosty w danej sieci mają ten sam adres sieci i unikatowy adres hosta. Dwa komputery w różnych sieciach muszą mieć inne adresy sieciowe, ale mogą mieć ten sam adres hosta.

O przynależności adresu IP do danej klasy adresowej świadczą pierwsze bity adresu IP (pierwszy oktet). Na rysunku 3.50 pokazano poszczególne klasy adresowe wraz z pierwszymi bitami adresu oraz z zakresami adresów należących do każdej z klas (adres najniższy i adres najwyższy sieci).

klasa	Struktura bitowa adresu IP	Zakres adresów	Zakres adresów IP dostępnych dla użytkowników
A	0 | Sieć (7 bitów) | Host (24 bity)	0.0.0.0 127.255.255.255	1.0.0.0 126.0.0.0
B	1 0 | Sieć (14 bitów) | Host (16 bitów)	128.0.0.0 191.255.255.255	128.0.0.0 191.254.0.0
C	1 1 0 | Sieć (21 bitów) | Host (8 bitów)	192.0.0.0 223.255.255.255	192.0.0.0 223.255.254.0
D	1 1 1 0 | adres grupowy (28 bitów)	224.0.0.0 239.255.255.255	żaden
E	1 1 1 1 | zarezerwowane na przyszłość	240.0.0.0 255.255.255.255	żaden

Rysunek 3.50. Klasy adresów IPv4

Obserwując pierwszy oktet adresu, możemy stwierdzić, do jakiej klasy należy dany adres, w efekcie możemy stwierdzić, ile bitów będzie adresowało sieć, a ile sam komputer. Zwróćmy uwagę, że aby określić przynależność do jednej z trzech zasadniczych klas (A, B, C), wystarczą dwa pierwsze bity.

Adresów klasy A wykorzystywanych przez duże sieci jest niewiele. W tej klasie może istnieć zaledwie 126 sieci, z których każda ma ponad 16 milionów hostów (mimo że jest to adres 7-bitowy, wartości 0 i 127 mają specjalne znaczenie, stąd 128–2 = 126 adresów sieci).

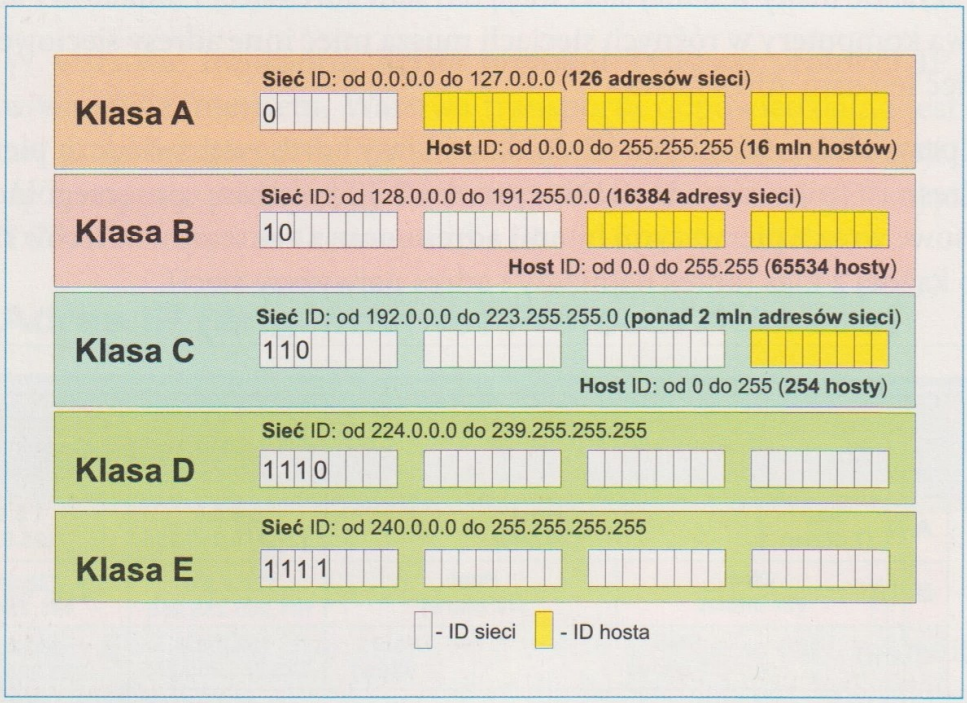
Klasa B przeznaczona jest dla sieci średniej wielkości, mających od 2^8 do 2^{16} maszyn. 14 bitów określa sieć, a 16 bitów komputer. W efekcie otrzymujemy 16 384 sieci, które mogą mieć do 65 535 komputerów każda.

W klasie C sieć adresowana jest za pomocą 21 bitów — daje to 2^{21} sieci (ponad 2 miliony), ale w każdej z nich może być co najwyżej 2^8, czyli 256 adresów IP.

Adres klasy D (ang. *multicast address*) ma specjalne znaczenie — jest używany w sytuacji, gdy zachodzi jednoczesna transmisja do większej liczby urządzeń.

Adresy klasy E mają specjalne znaczenie — są używane w celach eksperymentalnych i zostały zarezerwowane na przyszłość.

Szczegółowy rozkład ID sieci i ID hosta ilustruje rysunek 3.51.



Rysunek 3.51. Tablica adresów klasowych IPv4

Jeszcze nie tak dawno sądzono, że pula około 4 miliardów adresów IPv4 na długo zapewni niezawodne działanie internetu. Szacuje się, że każdego dnia przybywa kilkanaście tysięcy nowych hostów podłączonych do sieci. Problem z możliwością wyczerpania puli adresów IP jest bardzo poważny.

Jednak internet ciągle działa, a nowe komputery podłączane są do sieci. Jak to jest możliwe? I dlaczego mimo ograniczonej liczby adresów IPv4 nadal można podłączać komputery do internetu?

Problem ten rozwiązano na kilka sposobów:

- Pierwszy sposób polegał na opracowaniu nowego protokołu internetowego, zwanego dziś IPv6. Jest to rozwiązanie, które radykalnie zwiększy przestrzeń adresową z 32 bitów w IPv4 aż do 128 bitów w IPv6. Jednakże wprowadzenie IPv6 zajmie kilka lat, a migracja z IPv4 do IPv6 nie zostanie przeprowadzona w krótkim czasie.

IP v4 to 4*8 bitów = 32 bity,

IP v6 to 8*16 bitów = 128 bitów.

- Krótkoterminowym rozwiązaniem jest koncepcja CIDR (ang. *Classless Inter-Domain Routing*), która umożliwia bardziej wydajny sposób przydzielania przestrzeni adresowej IPv4, przez eliminację tradycyjnej koncepcji klas A, B i C.
- Zastosowanie puli adresów IP prywatnych w sieci lokalnej i podłączenie jej do internetu poprzez jeden adres publiczny. Proces tłumaczenia adresu z puli prywatnej na publiczną i odwrotnie to translacja adresów, czyli NAT (ang. *Network Address Translation*). W praktyce oznacza to, że korzystając z jednego adresu publicznego IP, możemy podłączyć do internetu wiele komputerów, tak jak to ma miejsce np. w szkole.

Adresy specjalne

Adres 127.0.0.0, mimo że ma wartość z zakresu odpowiadającego klasie A, jest zarezerwowany dla tzw. pętli zwrotnej, służącej do testowania TCP/IP dla danego komputera. Gdy program używa adresu pętli zwrotnej jako adresu odbiorcy, oprogramowanie protokołu komunikacyjnego przekazuje dane komputerowi bez wysyłania ich do sieci. Pakiety wysyłane do sieci 127.0.0.0 nie powinny nigdy zostać przekazane do żadnej sieci.

Wszystkie bity części adresu przeznaczonego dla hostów nie mogą mieć wartości 1. Taki adres to adres rozgłoszeniowy (ang. *broadcast*). Wysłanie wiadomości pod adresem, w którym w części hosta znajdują się same jedynki, jest wysłaniem wiadomości do wszystkich, czyli komunikatem sieciowym (rozgłoszeniowym). Na przykład adres 152.23.255.255 oznacza „wszystkie hosty" w sieci 152.23.0.0 (klasy B).

Adres 255.255.255.255 oznacza, że wszystkie węzły danej sieci otrzymają ten pakiet.

Wszystkie bity w części adresu przeznaczonego dla hostów nie mogą mieć wartości 0. Taki adres oznacza adres sieci.

Adres sieci i adres rozgłoszeniowy nie mogą być użyte do adresowania hostów. Dlatego zawsze liczba hostów jest mniejsza o 2 od całej puli dostępnych adresów. W każdej sieci klasy C można utworzyć 256 adresów IP, jednak dwa z nich są adresami specjalnymi (sieci i rozgłoszeniowym), więc dla hostów pozostają 254. Ostatni oktet przeznaczony dla hostów, czyli 8 bitów, pozwala na podłączenie $2^8-2 = 256-2 = 254$ hostów. Dla klasy B, odpowiednio: $2^{16}-2$ hosty, a dla klasy A — $2^{24}-2$ hostów.

Adres z samymi zerami wskazuje na lokalną sieć. Adres 0.0.0.88 wskazuje na host z numerem 88 w tej sieci klasy C.

Adresy niepubliczne (prywatne)

Adresów niepublicznych, inaczej zwanych nierutowalnymi, nie można używać w internecie. Są one przeznaczone do budowy sieci lokalnych. Jeśli sieć publiczna korzysta z adresów niepublicznych (prywatnych), a hosty mają mieć dostęp do internetu, musi zostać zastosowane maskowanie adresów niepublicznych, inaczej zwane NAT-owaniem.

Dokument RFC 1918 określa, jakie adresy IP mogą być użyte wewnątrz prywatnej sieci. Zarezerwowane są dla nich trzy grupy adresów IP klas A, B, C. Wydzielone odpowiednie pule adresowe przeznaczone na adresy niepubliczne zestawiono na rysunku 3.52.

Klasa	Zakresy adresów prywatnych w danych klasach	
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Rysunek 3.52. Zakresy adresów niepublicznych (prywatnych)

Maski sieciowe (IPv4)

Maska sieci składa się, podobnie jak adres IP, z 4 oktetów. Używana jest do wydzielenia z adresu IP części odpowiadającej za identyfikację sieci i części odpowiadającej za identyfikację komputera.

Klasa adresów sieciowych wyznacza maskę sieciową, co pokazano na rysunku 3.53.

Klasa	Bity – maska podsieci	Notacja dziesiętna
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Rysunek 3.53. Domyślne maski dla klas adresowych A, B, C

Należy pamiętać, że maska (jak również adres IPv4) zapisana jest w postaci binarnej, a zapis kropkowo-dziesiętny stosowany jest dla wygody użytkowników.

Adresowanie bezklasowe

Podział adresów na klasy adresowe spowodował, że dużo adresów IP marnowało się. Rozważmy dla przykładu średnich rozmiarów przedsiębiorstwo, które potrzebuje 300 adresów IP. Adres klasy C, dający 254 adresy hostów, jest niewystarczający. Wykorzystanie dwóch adresów klasy C dostarczy więcej

adresów, niż potrzeba, ale w wyniku tego w ramach przedsiębiorstwa powstaną dwie odrębne sieci. Z kolei zastosowanie adresu klasy B zapewni potrzebne adresy w ramach jednej sieci, ale zmarnuje się w ten sposób 65234 (65534–300) adresów.

Od 1997 roku podział na klasy sieci jest już nieaktualny. Obecnie adresy IPv4 są przydzielane bez specjalnego zwracania uwagi na klasy sieci — wg założeń CIDR (ang. *Classless Inter-Domain Routing*).

Zaczęto więc nadawać maski, które nie są maskami według klas adresów IP (czyli takich, w których liczba jedynek jest wielokrotnością oktetów, zob. rysunek 3.53). Zwiększenie liczby jedynek przy takiej samej liczbie bitów (32) umożliwiło np. uzyskanie maski 11111111 11111111 11111111 11110000 (255.255.255.240), która pozwala na objęcie podsiecią 14 hostów (14 numerów IP). Rysunek 3.54 przedstawia wszystkie możliwe podsieci dla zakresu od 2 do 254 hostów. Wprowadzenie pozaklasowej maski podsieci pozwoliło na ekonomiczne wykorzystanie numerów IPv4.

Maska *(dziesiętnie)*	Maska *(binarnie)*	Liczba podsieci	Liczba hostów w podsieci
255.255.255.0	11111111 11111111 11111111 00000000	1	254
255.255.255.128	11111111 11111111 11111111 10000000	2	126
255.255.255.192	11111111 11111111 11111111 11000000	4	62
255.255.255.224	11111111 11111111 11111111 11100000	8	30
255.255.255.240	11111111 11111111 11111111 11110000	16	14
255.255.255.248	11111111 11111111 11111111 11111000	32	6
255.255.255.252	11111111 11111111 11111111 11111100	64	2
255.255.255.254	11111111 11111111 11111111 11111110	128	0

Rysunek 3.54. Wszystkie możliwe podsieci dla zakresu od 2 do 254 hostów

Host jest zatem określany przez adres IP i maskę podsieci.

Adres sieciowy (IPv4)

Aby określić adres sieci, należy wykonać funkcję AND pomiędzy adresem IP a jego maską sieci. Zasadę koniunkcji (iloczynu logicznego) przypomina rysunek 3.55. Adres sieciowy jest **bitowym iloczynem** maski sieciowej i adresu IP hosta.

Kombinacja bitów	Wartość
1 AND **1**	**1**
1 AND **0**	**0**
0 AND **1**	**0**
0 AND **0**	**0**

Rysunek 3.55. Koniunkcja bitów

Czasami można spotkać skrótowo zapisany adres IP w postaci: 197.3.182.0/24, gdzie część stojąca przed znakiem / jest adresem IP, zaś liczba 24 jest skrótowo zapisaną maską sieciową. Jest to liczba bitów ustawionych w masce sieciowej na 1, czyli przy standardowej 32-bitowej masce jest to 11111111 11111111 11111111 00000000 (255.255.255.0).

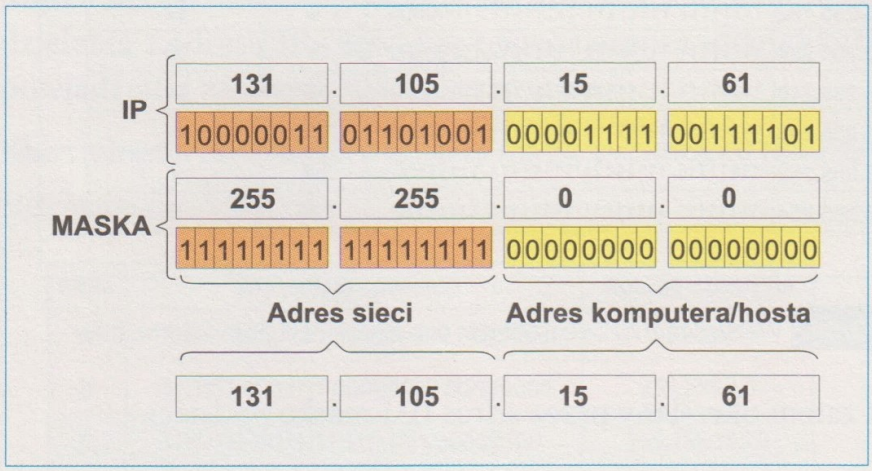
Przykład 3.1.

Dla adresu IP: 131.105.15.61/16 określ jego klasę, adres sieci oraz adres hosta.

Określenie klasy polega na sprawdzeniu pierwszych bitów pierwszego oktetu badanego adresu IP. W tym przypadku należy sprawdzić wartość 131, zamieniając ją na zapis binarny: 10000101. Dwa pierwsze bity wystarczą dla określenia klasy. Pozycja zera na drugim miejscu świadczy o tym, że adres IP 131.105.15.61 należy do klasy adresowej B.

Analizując maskę sieci, można określić adres sieci oraz adres komputera (hosta). Maska definiuje bowiem podział adresu IP na część złożoną z adresu sieci i adresu komputera (hosta) w danej sieci komputerowej. Zapis IP w postaci 131.105.15.61/16 oznacza, że jest to maska domyślna 255.255.0.0.

Wykonując binarne AND adresu IP i maski, otrzymasz adres sieci. Obliczenia zawarto na rysunku 3.56.



Rysunek 3.56. Rozróżnianie adresu sieci i hosta na podstawie maski

Odpowiedź: Ten adres należy do sieci klasy B. Adres sieci to 131.105.0.0, a adres hosta w tej sieci to 0.0.15.61.

Ćwiczenie 3.11.

Znając adresy IP oraz maski dwóch komputerów, sprawdź, czy oba komputery należą do tej samej sieci. Pierwszy komputer ma adres IP 172.21.10.10/16, drugi —172.21.11.102/16.

Adres rozgłoszeniowy — BROADCAST

Adres rozgłoszeniowy jest specjalnym adresem IP. Wszystkie komputery w sieci nasłuchują pakietów kierowanych na ten adres. Jeżeli chcemy wysłać pakiet adresowany do wszystkich komputerów w danej sieci, korzystamy właśnie z adresu rozgłoszeniowego. Przykładowo są to informacje dotyczące tablicy routingu. W niektórych przypadkach jako adresu rozgłoszeniowego używa się adresu sieci.

Wykonujemy działanie logiczne negujące `IP XOR MASKA`, czyli `NOT(IP XOR MASKA)`. Zasadę działania alternatywy wykluczającej ilustruje rysunek 3.57.

Kombinacja bitów	Wartość
1 XOR 1	0
1 XOR 0	1
0 XOR 1	1
0 XOR 0	0

Rysunek 3.57.

Alternatywa wykluczająca xor jest prawdziwa wtedy i tylko wtedy, gdy dokładnie jedno ze zdań p lub q jest prawdziwe

Przykład 3.2.

Oblicz adres rozgłoszeniowy dla IP 195.116.241.160/27.

IP	11000011	01110100	11110001	10100000	
maska	11111111	11111111	11111111	11100000	
xor	00111100	10001011	00001110	01000000	— wynik działania logicznego `xor`
not	11000011	01110100	11110001	10111111	— negacja wyniku, będąca adresem rozgłoszeniowym
broadcast		195.116.241.191			— adres rozgłoszeniowy w zapisie kropkowo-dziesiętnym

Ćwiczenie 3.12.

Dla przykładowego numeru IP i maski 218.131.18.56/22 oblicz adres sieci i adres rozgłoszeniowy broadcast.

Dzielenie sieci — podsieci

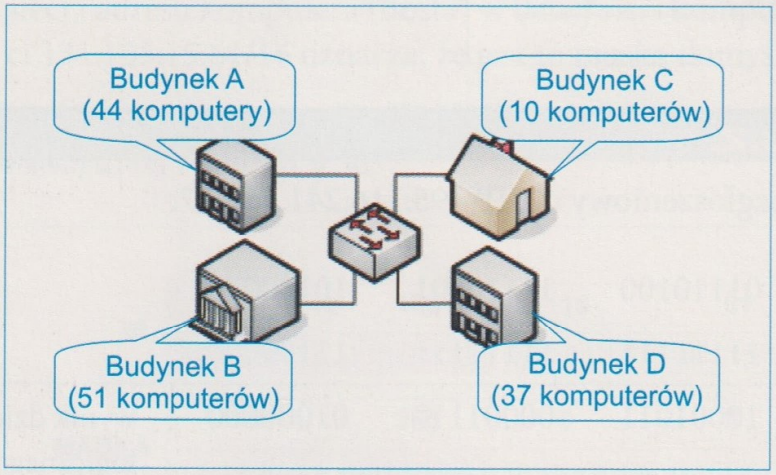
Pierwotnie adresowanie IP wymagało, by każda sieć miała unikatową część adresującą sieć, w której można przyłączyć określoną liczbę hostów. Dla przykładu adres hosta: 198.200.55.X jest adresem klasy C, gdzie X jest liczbą z zakresu

1 – 254. Nawet jeśli w sieci pracuje tylko 40 komputerów, to bez stosowania podsieci wszystkie adresy od 198.200.55.1 do 198.200.55.254 byłyby zarezerwowane. W ten sposób 214 adresów (254–40) pozostaje niewykorzystanych. Dzięki zastosowaniu podsieci sieć ta może wykorzystać tylko 62 adresy (zgodnie z podziałem na 4 podsieci, co wyliczono na rysunku 3.54). Będą to adresy z zakresu od 198.200.55.1 do 198.200.55.63. Zmarnowane zostaną zaledwie 24 adresy, a pozostałe 186 adresów tej sieci może być wykorzystanych przez innych użytkowników. Jako wyjaśnienie niech posłuży przykład 3.3.

Przykład 3.3.

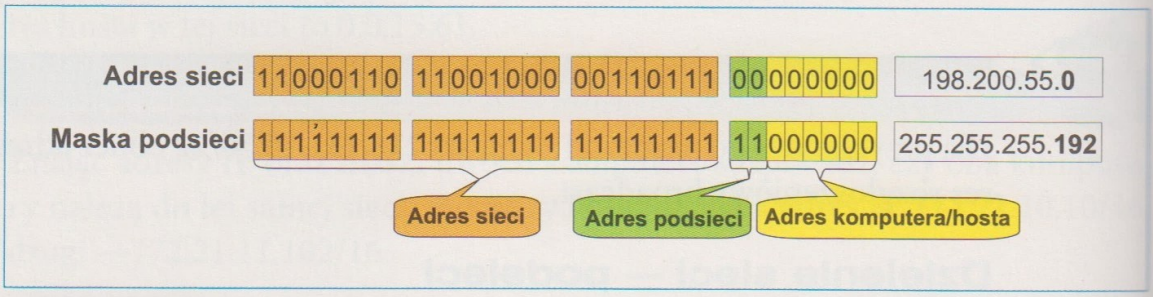
Należy podzielić sieć klasy C o adresie 198.200.55.0/24 na podsieci obsługujące poszczególne budynki pokazane na rysunku 3.58.

Możemy utworzyć podsieci, w których liczba hostów przyjmie następujące wartości: 2, 4, 8, 16, 32, 64, 128, 256. Analizując rysunek 3.58, należy utworzyć cztery podsieci o 62 dostępnych adresach hostów.



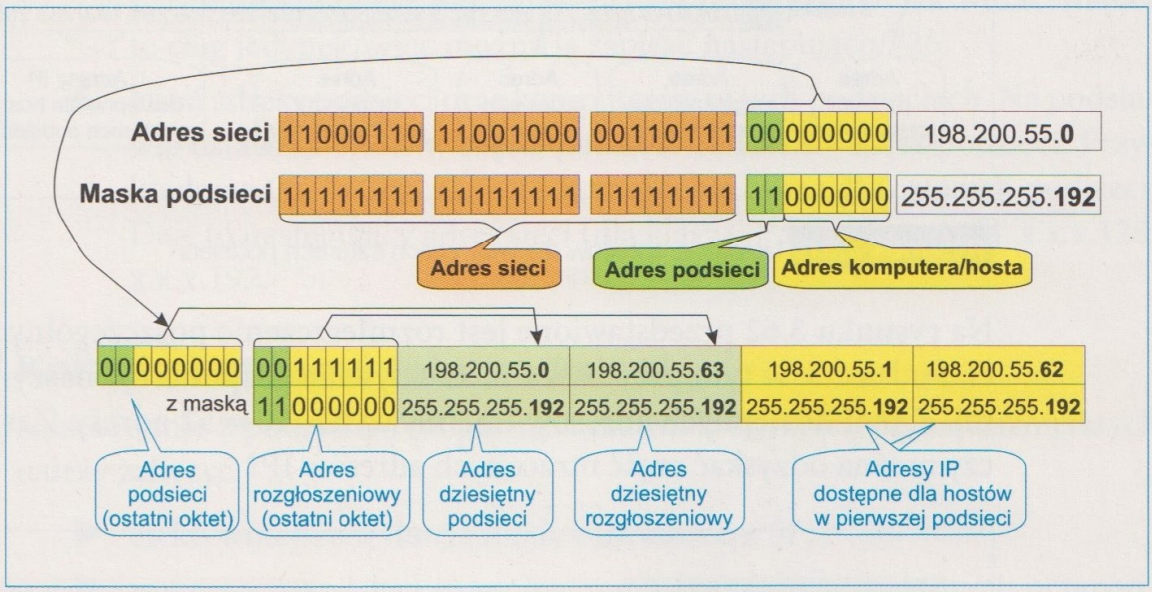
Rysunek 3.58. Rozmieszczenie komputerów w czterech budynkach wydziałów uczelni

Ostatni oktet adresu komputera w sieci klasy C jest przeznaczony do adresowania hostów. Ze względu na fakt, że chcemy utworzyć cztery podsieci, dla adresu podsieci należy wykorzystać pierwsze dwa bity z czwartego oktetu adresu C. Podział ten spowoduje wprowadzenie maski, w której pierwsze dwa bity przyjmą wartość 1, jak na rysunku 3.59.



Rysunek 3.59. Ustalenie maski w celu utworzenia czterech podsieci

Znając ostatni oktet maski dla podziału sieci na cztery podsieci, możemy ustalić adres maski na 255.255.255.192 (11000000 = 192). Mając ustaloną maskę, można ustalić adresy czterech podsieci. Adresy czterech podsieci są związane z dwoma pierwszymi bitami czwartego oktetu adresu IP, który może przyjąć cztery różne wartości (00, 01, 10, 11). Szczegółowe obliczenia związane z pierwszą podsiecią przedstawione są na rysunku 3.60. Ponieważ wszystkie obliczenia są przeprowadzane w tym przypadku na ostatnim oktecie przeznaczonym dla hostów (klasa C), pokazano jedynie bity tego czwartego oktetu.

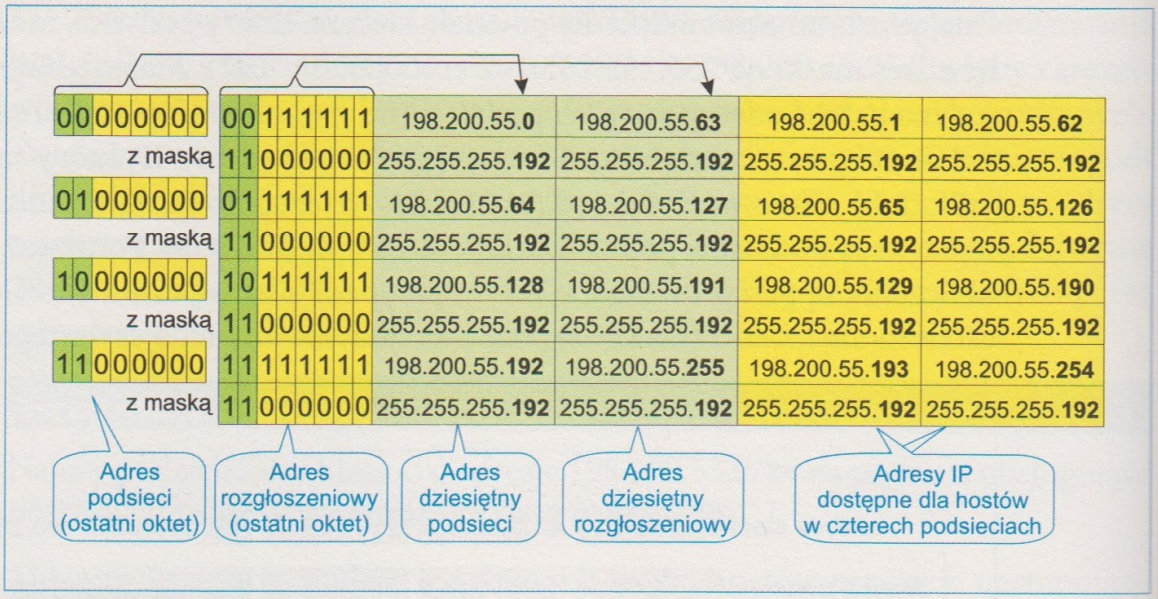


Rysunek 3.60. Ustalenie adresów w pierwszej podsieci

Mimo że w pierwszej podsieci przeznaczyliśmy na adresację hostów 6 bitów, do sieci możemy podłączyć maksymalnie 62 komputery (adresy skrajne są zarezerwowane: 198.200.55.0 — to adres sieci, natomiast 198.200.55.63 to adres rozgłoszeniowy). Dla potrzeb zadania jest to wystarczająca liczba hostów.

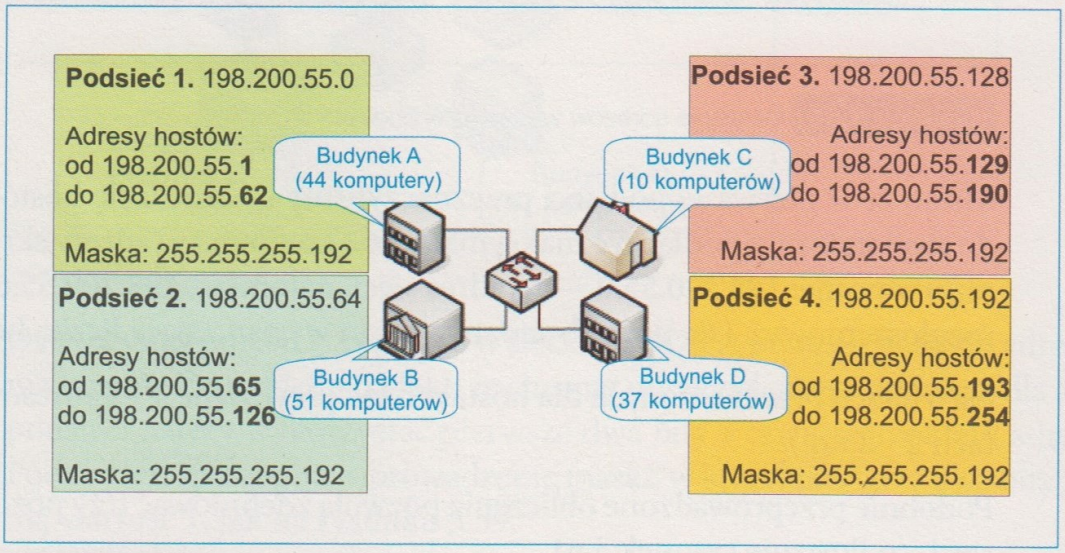
Na 6 bitach przeznaczonych dla hosta można przydzielić 2^6-2 adresów (na 5 bitach 2^5-2 itd.).

Podobnie przeprowadzone obliczenia pozwolą zdefiniować trzy pozostałe podsieci, co ilustruje rysunek 3.61.



Rysunek 3.61. Ustalenie adresów dla wszystkich czterech podsieci

Na rysunku 3.62 przedstawione jest rozmieszczenie poszczególnych podsieci. Podsieć 3. w tym przypadku nieefektywnie gospodaruje naszymi adresami. Z puli dostępnych adresów tracimy aż 62–10 = 52 adresy. Zastanów się, czy można odzyskać część utraconych adresów IP?



Rysunek 3.62. Przydzielenie czterech podsieci

Etapy tworzenia podsieci

1. Ustal, jakiej klasy adres trzeba podzielić (w przykładzie był adres klasy C).
2. Ustal, ile podsieci trzeba utworzyć (w przykładzie cztery).
3. Ile bitów potrzeba na ustalenie adresu podsieci?

$$liczba\_podsieci = 2^{liczba\_bitów\_przeznaczona\_na\_podsieć}$$

Jeśli chcemy mieć cztery podsieci, potrzebujemy dwóch bitów; gdy potrzebujemy 5 podsieci, dzielimy sieć na 8 podsieci i potrzebujemy dla nich 3 bitów. Pamiętaj, że bity podsieci można „odbierać" wyłącznie z części hosta, nie z części sieci. Liczba możliwych podsieci w klasie C to: 2,4,8,16,32,64,128. W klasie B: 2,4,8,16,32,64,128,256,512,1024...

4. Pamiętając o klasie adresowej (w tym przypadku C), ustalamy, ile bitów ma być przydzielonych dla tworzenia podsieci. Na tej podstawie ustalamy maskę podsieci: 255.255.255.192, co odpowiada zapisowi binarnemu 11111111 11111111 11111111 11000000. Jak widać, maska to ciąg jedynek, więc można ją zapisać następująco: /26.
5. Ustal adresy podsieci oraz komputerów w tych podsieciach. Na podstawie ustawień bitów w części podsieci obliczamy adres podsieci. Przykładowo 00, 01, 10, 11 — to kombinacje bitów dla czterech podsieci. Daje to następujący adres sieci (dla klasy C): x.x.x.0, x.x.x.64, x.x.x.128, x.x.x.192.

Korzyści stosowania podsieci

Adresowanie z podziałem na podsieci ma wiele korzyści, do najważniejszych należy zaliczyć:

- efektywniejsze wykorzystanie puli adresów IP;
- utworzone podsieci mogą być separowane, co w niektórych przypadkach jest wymagane;
- mimo istnienia podsieci, można utworzyć reguły umożliwiające współpracę podsieci;
- przez wyodrębnienie podsieci zmniejsza się ruch w sieci.

Ćwiczenie 3.13.

Podziel adres sieciowy IP: 208.182.34.0 na 16 podsieci.

Ćwiczenie 3.14.

Na podstawie adresu IP hosta i maski podsieci ustal jego klasę oraz oblicz adres rozgłoszeniowy, adres sieci, adres podsieci.

IP: 83.3.249.66

Maska podsieci: 255.255.255.248.

Przykład 3.4.

Czy adres IP hosta 207.13.47.48 z maską 255.255.255.248 jest prawidłowy? Odpowiedź uzasadnij.

Sprawdzimy adres sieci dla tego IP oraz dla tej maski.

IP	207.13.47.48	11001111.00001101.00101111.00110000
maska	255.255.255.248	11111111.11111111.11111111.11111000
adres sieci	207.13.47.48	11001111.00001101.00101111.00110000

Przy masce 255.255.255.248 (29 jedynek) podany w ćwiczeniu adres IP można zapisać następująco: 207.13.47.48/29. W tym przypadku na adresy hostów przeznaczone są 3 bity (8 kolejnych adresów). Dwa z tych ośmiu są zarezerwowane, pierwszy na adres sieci (jak w tym przypadku), ostatni na broadcast (adres rozgłoszeniowy). Adresy tej sieci są zatem następujące:

207.13.47.48 — adres sieci,

207.13.47.49 — adres hosta,

207.13.47.50 — adres hosta,

207.13.47.51 — adres hosta,

207.13.47.52 — adres hosta,

207.13.47.53 — adres hosta,

207.13.47.54 — adresy hosta,

207.13.47.55 — adres rozgłoszeniowy.

W tym przypadku nieprawidłowe jako adresy hostów będą adresy skrajne (sieci 207.13.47.48 i rozgłoszeniowy 207.13.47.55).

Adres IPv4: 200.10.6.2 nie jest adresem sieci przy masce 24-bitowej (255.255.255.0) — poprawnym adresem sieci jest w tym wypadku 200.10.6.0 (zera w części hosta).

Jeśli wystąpił konflikt adresów IP, system Windows ustawi adres IP na 0.0.0.0.

Adresowanie IPv6

Protokół IPv6 (ang. *Internet Protocol version 6*) jest nowszą wersją protokołu IP, która ma zastąpić IPv4. Pierwsze dokumenty opisujące IPv6 pochodzą z 1995 roku. Protokół IPv6 wprowadzono ze względu na pewne ograniczenia protokołu IPv4 oraz na wyczerpującą się pulę wolnych adresów IP.

Poniżej podajemy główne cechy nowego protokołu:

- Nowy format nagłówka. Nagłówek IPv6 ma nowy format, który zaprojektowano w taki sposób, aby zminimalizować obciążenie związane z przetwarzaniem nagłówka (na routerach pośrednich). Nagłówki IPv4 i IPv6 nie współdziałają ze sobą i protokół IPv6 nie jest zgodny z protokołem IPv4. Aby host lub router rozpoznawał i przetwarzał oba

formaty nagłówków, musi korzystać z implementacji zarówno protokołu IPv4, jak i IPv6.

- Olbrzymia przestrzeń adresowa. Źródłowe i docelowe adresy IPv6 mają 128 bitów (dla porównania: adresy IPv4 składają się tylko z 32 bitów).
- Ułatwiona konfiguracja adresów. Dla uproszczenia konfiguracji hostów protokół IPv6 obsługuje konfigurację adresów zarówno przy obecności serwera DHCP, jak i bez serwera DHCP. W tym drugim przypadku hosty podłączone do łącza automatycznie konfigurują swoje adresy IPv6 dla tego łącza.

Budowa IPv6

Dla IPv6 128-bitowy adres dzieli się na 16-bitowe człony. Każdy 16-bitowy blok konwertowany jest do postaci szesnastkowej.

Oto 128-bitowy adres IPv6 (podzielony na 16-bitowe fragmenty):

1101100101011100 0000110011001100 1000000100001010 1111110001000010
1111010110100001 0111001000100001 0001000010011010 0000000000010011

Każdy 16-bitowy człon adresu jest, dla skrócenia zapisu, zapisywany w postaci szesnastkowej i oddzielony dwukropkiem. Oto rezultat:

D95C:0CCC:810A:FC42:F5A1:7221:109A:0013

Reprezentacja IPv6 może zostać uproszczona przez usunięcie poprzedzających zer z każdego bloku 16-bitowego, przy czym każdy blok musi posiadać przynajmniej jeden znak. Po wyrzuceniu poprzedzających zer reprezentacja adresu wygląda następująco:

D95C:CCC:810A:FC42:F5A1:7221:109A:13

Niektóre typy adresów zawierają dłuższe sekwencje zer. Aby jeszcze bardziej uprościć adres IPv6, sąsiadujące sekwencje 16-bitowych bloków złożonych z zer w formacie szesnastkowym mogą zostać zapisane jako ::. Przykładowo, adres typu link-local FE80:0:0:0:2AC:FF:FE9A:4CA2 może zostać skrócony do postaci FE80::2AC:FF:FE9A:4CA2. Kompresji zer można użyć tylko raz w danym adresie! Prefiks w IPv6 pełni podobną funkcję jak maska w IPv4. Prefiks to liczba w systemie dziesiętnym, która informuje o liczbie bitów przeznaczonych na „adres sieci", np. 26DA:D4:0:1F3B::/64.

Dozwolone jest zastąpienie jednego bloku zer podwójnym dwukropkiem, początkowe zera w grupach również mogą być opuszczane, w związku z czym poniższe sposoby zapisu są prawidłowe i równoznaczne sobie:

2001:0CA7:0000:0000:0000::2528:57F8

2001:0CA7:0:0:0:0:2528:57F8

2001:0CA7:0:0::2528:57F8

2001:0CA7::2528:57F8

2001:CA7::2528:57F8

Sekwencja ostatnich 4 bajtów adresu może być również zapisana w postaci adresu IPv4, z wykorzystaniem kropek jako separatorów — adres ::ffff:80.55.69.250 jest równoznaczny adresowi ::ffff:5037:45FA.

Gdy jest to wymagane, do adresu może być dołączona maska sieci w notacji CIDR, np. 2004:0da6:1212::/48. Jeżeli natomiast zachodzi potrzeba podania portu docelowego (np. w adresie URL), adres IPv6 otaczany jest nawiasami kwadratowymi, np.:

```
http://[2004:0da6:1212:08d5:1321:8c12:0381:6322]:443/
```

3.4.3. Podstawowe rodziny protokołów

Wyróżniamy trzy podstawowe grupy protokołów sieciowych.

- NetBEUI — opracowany w 1985 r. przez firmę IBM. Używany w małych, odizolowanych sieciach LAN typu peer-to-peer, nierutowalny.
- IPX/SPX — opracowany w latach 70. przez firmę Novell. Jest protokołem rutowalnym, dlatego może być wykorzystywany do budowy złożonych sieci. Bardzo popularny w latach dziewięćdziesiątych, zastąpiony przez stos protokołów TCP/IP z powodu braku mechanizmów zapewniających poprawną transmisję.
- TCP/IP — najczęściej stosowany zestaw protokołów sieciowych, który łączy komputery pracujące na różnych platformach sprzętowo-systemowych. Jest protokołem rutowalnym.

Protokół nierutowalny (np. NetBEUI) — protokół wykorzystujący jedynie adresowanie zapewniane przez warstwy 1. i 2. (np. adresy MAC dla sieci Ethernet), przez co nie może służyć komunikacji pomiędzy sieciami o różnej architekturze fizycznej (inny sposób adresowania, inna budowa ramek itd.). Protokoły tego typu sprawdzają się jedynie w niewielkich sieciach LAN. Protokoły nierutowalne nie są „przepuszczane" przez routery.

Protokoły rutowalne (np. TCP/IP lub IPX/SPX) pozwalają na przesyłanie danych pomiędzy sieciami. Router — urządzenie łączące sieci – odczytuje informacje i podejmuje decyzje, dokąd i jaką drogą przesłać pakiet informacji.

Protokoły internetu

Warstwa aplikacji

ADSP (AppleTalk), APPC, AFP (AppleTalk), DAP, DLC, DNS(53), ed2k, FTAM, FTP(20,21), Gopher, HTTP(80), HTTPS(443), IMAP(143), IRC(194,529), Named Pipes, NCP(524), NetBIOS(137,138,139), NWLink, NBT, NNTP(119), NTP(123), PAP, POP(3110), RPC, RTSP, SNMP(161,162), SMTP(25), SMB, SSL/TLS, SSH(22), TDI, Telnet(23), X.400, X.500, XDR, ZIP (AppleTalk).

Kolejność alfabetyczna. Cyfry w nawiasie oznaczają numery portów.

Warstwa transportowa

ATP (AppleTalk), NBP (AppleTalk), NetBEUI, RTP, RTMP (AppleTalk), SCTP SPX, TCP, UDP.

Warstwa sieciowa

DDP (AppleTalk), ICMP, IP, IPsec, IPX, NAT, NWLink, NetBEUI.

Warstwa dostępu do sieci

ARP, 10BASE-T, 802.11 WiFi, ADSL, Ethernet, EtherTalk, FDDI, Fibre Channel, ISDN, LocalTalk (AppleTalk), NDIS, ODI, PPP, RS-232, SLIP, Token-Ring, TokenTalk (AppleTalk), V.90.

Protokół HTTP

HTTP (ang. *Hypertext Transfer Protocol* — protokół przesyłania dokumentów hipertekstowych) to protokół sieci WWW (ang. *World Wide Web*). Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW. Zadaniem stron WWW jest publikowanie informacji — natomiast protokół HTTP umożliwia ich udostępnianie.

Protokół HTTP jest bardzo użyteczny, ponieważ udostępnia znormalizowany sposób komunikowania się komputerów ze sobą. Określa on formę żądań klienta dotyczących danych oraz formę odpowiedzi serwera na te żądania. Jest zaliczany do protokołów bezstanowych (ang. *stateless*), ponieważ nie zachowuje żadnych informacji o poprzednich transakcjach z klientem (po zakończeniu transakcji wszystko „przepada"). Pozwala to znacznie zmniejszyć obciążenie serwera, jednak jest kłopotliwe w sytuacji, gdy trzeba zapamiętać konkretny stan dla użytkownika, który wcześniej łączył się już z serwerem. Najczęstszym rozwiązaniem tego problemu jest wprowadzenie mechanizmu **cookies**.

HTTP standardowo korzysta z portu nr 80.

Protokół FTP

FTP (ang. *File Transfer Protocol* — protokół transferu plików) — protokół typu klient-serwer, który umożliwia przesyłanie plików z serwera i na serwer poprzez sieć TCP/IP.

Do komunikacji wykorzystywane są dwa połączenia TCP. Jedno z nich jest połączeniem kontrolnym, za pomocą którego przesyłane są polecenia do serwera, drugie służy do transmisji danych.

FTP wykorzystuje do transmisji danych port 20, natomiast do kontroli transmisji — port 21. Podstawową zaletą FTP jest możliwość kontynuowania przerwanego transferu danych aż do uzupełnienia brakujących części pliku. Główną wadą protokołu jest jednak brak możliwości szyfrowania transmisji, pomimo tego nadal jest on popularnym protokołem przesyłania danych.

Protokół SMTP

SMTP (ang. *Simple Mail Transfer Protocol*) to protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w internecie. SMTP działa najczęściej na porcie 25. Łatwo przetestować serwer SMTP przy użyciu programu telnet.

SMTP nie pozwala na pobieranie wiadomości ze zdalnego serwera. Do tego celu służą POP3 lub IMAP.

POP3

POP3 (ang. *Post Office Protocol version 3*) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP. Większość internautów korzysta z POP3 do odbioru poczty.

Protokół POP3 powstał dla użytkowników, którzy nie są cały czas dostępni w internecie, przez co poczta nie może dotrzeć do nich protokołem SMTP. W takiej sytuacji w sieci istnieje specjalny serwer, który przez SMTP odbiera przychodzącą pocztę i ustawia ją w kolejce. Kiedy użytkownik połączy się z siecią, wówczas — korzystając z POP3 — może pobrać czekające na niego listy do lokalnego komputera. Protokół ten ma jednak wiele ograniczeń.

Telnet

Telnet jest usługą (programem) pozwalającą na zdalne połączenie się komputera (terminala) z oddalonym od niego komputerem (serwerem) przy użyciu sieci. Do tego celu wykorzystywany jest protokół TCP-IP oraz standardowo przypisany port 23. Telnet umożliwia zatem ustanowienie zdalnej sesji na serwerze tak, jak gdyby użytkownik siedział tuż przed nim.

Wszystkie polecenia muszą być wprowadzane w trybie znakowym w wierszu poleceń. Polecenia wydawane za pomocą naszego komputera przesyłane są poprzez sieć do serwera, na którym zainstalowane jest oprogramowanie serwera telnetu.

Do korzystania z tej usługi niezbędne jest posiadanie na serwerze konta typu shell.

Usługa ta uruchamiana jest po wpisaniu polecenia: `telnet adres`, gdzie `adres` jest adresem IP komputera, z którym chcemy się połączyć, lub jego nazwą domenową, gdyż telnet dopuszcza obie te formy podawania adresu. Po nawiązaniu połączenia w celu zalogowania się do serwera należy podać nazwę użytkownika oraz hasło (login i password).

Protokół IP

Najważniejszym protokołem komunikacyjnym warstwy sieciowej jest protokół IP. Jego cechy to:

- protokół bezpołączeniowy (nie wysyła i nie przyjmuje żadnych informacji kontrolnych, które przed wysłaniem danych ustanawiałyby połączenie między odbiorcą a nadawcą),
- brak korekcji błędów,
- nie sprawdza, czy dane zostały prawidłowo odebrane,
- zajmuje się adresowaniem datagramu.

3.4.4. Obsługa i konfiguracja sieci w Windows

Jak skonfigurować komputer pracujący pod kontrolą systemu operacyjnego Windows tak, aby uzyskać dostęp do internetu?

Dokładne instrukcje zamieszczone zostały na płycie CD w pliku *Obsługa i konfiguracja sieci w Windows.pdf*.

3.4.5. Bezpieczeństwo sieci

Żyjemy w świecie, który nieustannie się rozwija. Rozwój ten nie omija sieci komputerowych. Przesyłanie różnorodnych danych poprzez sieć jest bardzo wygodne, ale i bardzo niebezpieczne. Dane narażone są na kradzież. Sieciowi włamywacze oraz różnego rodzaju wandale prześcigają się w łamaniu coraz to nowszych zabezpieczeń. Nawet najbardziej doświadczeni administratorzy sieci oraz osoby odpowiedzialne za bezpieczeństwo danych cyfrowych muszą nieustannie podnosić swoje umiejętności. W dzisiejszych czasach podanie

loginu oraz hasła nie jest wystarczającym zabezpieczeniem naszych danych. Istnieje bardzo wiele niebezpieczeństw czyhających na dane znajdujące się w sieci komputerowej.

W jaki sposób nasze dane mogą zostać ukradzione?

Najprostszy sposób to uzyskanie bezpośredniego dostępu do komputera, w którym znajdują się dane. Dostęp ten można uzyskać po dokonaniu lokalnego lub zdalnego włamania się do tego komputera. **Hakerzy**, jak nazywa się potocznie ludzi przeprowadzających elektroniczne włamania, używają wielu metod. Najczęściej wykorzystywane są luki, które znajdują się w protokole sieciowym TCP/IP oraz protokołach mu pokrewnych. Sam protokół TCP/IP nie ma żadnych mechanizmów szyfrowania, co oznacza, że dane wysyłane są w sposób jawny.

Często wykorzystywane są błędy w zabezpieczeniach, które popełnił administrator sieci.

Innym sposobem włamania jest zdobycie przez hakera danych umożliwiających zalogowanie się na zdalnej maszynie. Najbardziej niebezpieczne jest włamanie na konto administratora komputera lub sieci. Usuwanie skutków takiego włamania jest bardzo trudne i nigdy nie daje stuprocentowej pewności, czy haker nie będzie miał możliwości kolejnego przejęcia kontroli nad naszym komputerem.

Mając na uwadze bezpieczeństwo danych, należy przestrzegać pewnych standardów bezpieczeństwa. Ich zbiór został opublikowany w **Orange Book** przez Departament Obrony USA, gdzie zdefiniowano siedem poziomów bezpieczeństwa komputerowego systemu operacyjnego. Są to poziomy: D, C1, C2, B1, B2, B3 oraz A1, które opisane zostały w umieszczonym na płycie CD pliku *Orange Book.pdf*.

Hasła

Metoda oparta na hasłach jest chyba najbardziej rozpowszechnioną metodą uwierzytelniania użytkownika. Oczywiście metoda ta nie daje stuprocentowej pewności, że osoba logująca się jako użytkownik jest tą osobą, która ma prawo się logować. W zasadzie, gdy mamy do czynienia z tego typu logowaniem poprzez środowisko sieciowe, złamanie hasła jest stosunkowo proste.

Metoda nasłuchiwania sieci może potencjalnemu hakerowi dostarczyć wszystkich informacji, by mógł odczytać kombinację użytych znaków, które stanowią hasło. Programy takie jak IPtrace, Snop czy też LanWatch, są często stosowanymi narzędziami do nasłuchu i identyfikacji hasła. Szczególnie niebezpieczne

jest połączenie ze zdalną maszyną za pomocą protokołu **telnet**. Dane, takie jak hasło i login, przesyłane są otwartym tekstem (bez szyfrowania), co powoduje możliwość przejęcia danych i uprawnień.

Bardzo niebezpieczne są wszelkiego typu programy zainstalowane nieświadomie przez użytkownika na jego maszynie, takie jak **konie trojańskie**, które często mają na celu pozyskanie danych logowania.

Typowym sposobem łamania haseł jest tzw. atak poprzez słownik (ang. *dictionary attack*). Polega on na próbkowaniu programu autoryzującego całym słownikiem danych. Jeżeli weźmiemy pod uwagę, że w przypadku klasycznego systemu Unix maksymalna długość hasła wynosi 8 znaków, a funkcja szyfrująca używa tylko siedmiu bitów znaczących, otrzymujemy klucz o długości 56 bitów. Ponieważ większość użytkowników stosuje proste hasła, pole poszukiwań może być zawężone tylko do np. małych liter — odpowiada to sytuacji używania klucza o długości 19 bitów. Przykładem programu dokonującego ataku poprzez słownik jest COPS, który używa tej metody do diagnozowania skuteczności zabezpieczeń hasłem. Dlatego należy używać hasła jak najdłuższego i dopilnować, aby zawierało ono zarówno litery małe, jak i wielkie oraz z liczby. Hasło nie jest na całe życie, należy je często zmieniać.

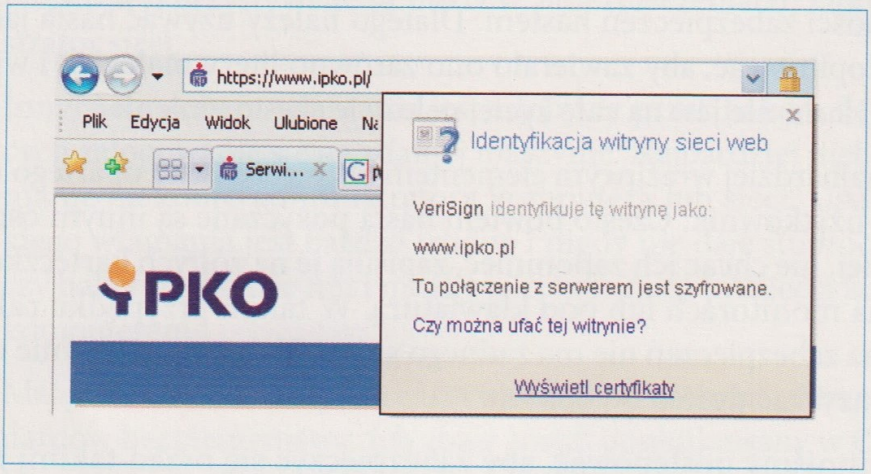
Jednak najbardziej wrażliwym elementem bezpieczeństwa opartego na hasłach jest sam użytkownik. Często bowiem hasła pożyczane są innym osobom, a te najczęściej, nie chcąc ich zapomnieć, zapisują je na żółtych karteczkach i przyklejają na monitorach lub pod klawiaturą. W takim przypadku cała polityka haseł oraz zabezpieczeń nie ma żadnego sensu. Haker musi jedynie umieć czytać, aby uzyskać dostęp do danych.

Jak powinniśmy postępować, aby zabezpieczyć się przed takimi niebezpieczeństwami?

Jeśli chodzi o hasła, w pierwszej kolejności należy wprowadzić jasną politykę bezpieczeństwa obowiązującą wszystkich użytkowników, którzy mają prawo logować się do komputerów i sieci. Należy tak skonfigurować konta użytkowników, aby system sam przypominał o wygaśnięciu ważności hasła. Co więcej, system powinien w przybliżeniu określić siłę hasła zaproponowanego przez użytkownika. Hasła powinny składać się z małych i wielkich liter oraz cyfr. W przypadku udostępnienia zdalnego logowania do sieci należy tak skonfigurować tę usługę, aby każda nowa sesja logowania wymagała podania nowego hasła. Można również zwiększyć poziom uwierzytelnienia użytkownika przez wprowadzenie dodatkowych zabezpieczeń w postaci kart logowania czy też technologii sprawdzania linii papilarnych. Oczywiście te technologie nie wyczerpują gamy możliwości zwiększenia poziomu bezpieczeństwa podczas logowania. Innym sposobem zwiększania bezpieczeństwa danych w sieci jest tworzenie zaszyfrowanego połączenia, dzięki któremu cała komunikacja między komputerami jest szyfrowana w obie strony.

Szyfrowanie a prywatność

Szyfrowanie jest skomplikowaną technologią, jednak w praktyce często z tej technologii korzystamy, nawet nie wiedząc o tym. Przykładowo, przy próbie zalogowania się na konto internetowe banku użytkownik po wprowadzeniu przykładowego adresu **www.ipko.pl** zostanie przekierowany na stronę **https://www.ipko.pl/**. Użycie protokołu http wraz z protokołem szyfrowania SSL (o czym świadczy początek adresu **https://**) gwarantuje szyfrowanie informacji między komputerami połączonymi w sieci. Jednak, mimo iż wszystko na razie wygląda prawidłowo, należy się jeszcze upewnić, że znajdujemy się tam, gdzie trzeba. Aby mieć pewność, że nie otwarliśmy strony, która tylko udaje bank internetowy, należy bezwzględnie sprawdzić informacje o certyfikacie, a właściwie ważność certyfikatu, oraz to, na kogo certyfikat jest wystawiony. W tym celu na pasku adresowym kliknij symbol kłódki, tak jak to pokazano na rysunku 3.63, która powinna być zamknięta, a następnie wybierz **Wyświetl certyfikat**, co spowoduje wyświetlenie okna z danymi dotyczącymi certyfikatu.



Rysunek 3.63. Informacja o szyfrowaniu połączenia oraz o szczegółach certyfikatu

Z informacji, które znajdują się na zakładce **Szczegóły**, można wywnioskować, że faktycznie strona, na której się znajdujemy, jest miejscem, gdzie możemy rozpocząć proces logowania.

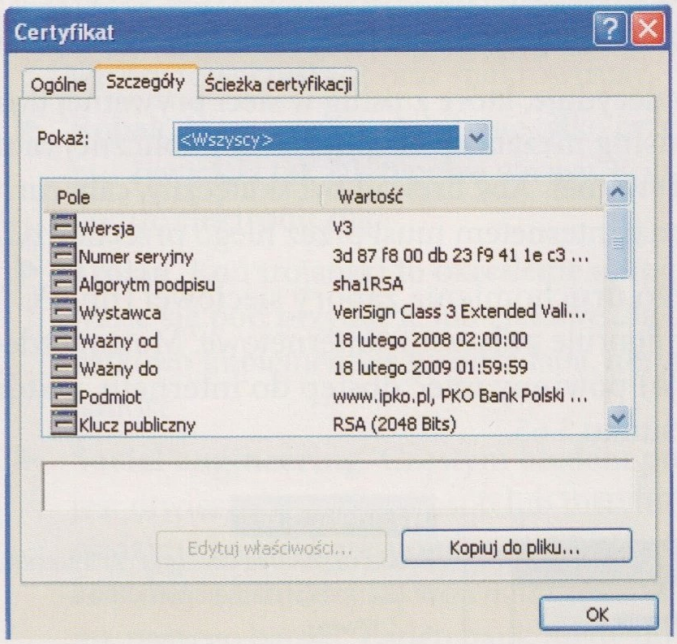
Jak działa protokół SSL?

SSL (ang. *Secure Sockets Layer*) to protokół zabezpieczający komunikację w internecie, przede wszystkim połączenia http oraz ftp. Obsługuje również certyfikaty stron. W skrócie jego działanie można przedstawić następująco:

- Komputer chcący się połączyć z serwerem wysyła wiadomość zawierającą informacje o metodzie szyfrowania, metodzie kompresji danych i wersji protokołu. Wysyłany jest również klucz publiczny z komputera na serwer.
- Serwer wysyła klientowi swój klucz publiczny oraz informacje potwierdzające, że parametry połączenia są już uzgodnione na warunkach klienta.

- Serwer wysyła do klienta swój certyfikat, który należy zweryfikować. Od tego momentu wszystkie dane przesyłane pomiędzy tymi hostami uważane są za autentyczne, co więcej, dodatkowe klucze służą do zaszyfrowania wymienianych informacji między klientem a serwerem.

Sesja SSL zostanie zakończona w wypadku wylogowania lub gdy klient odłączy się od serwera — np. zamknie okno przeglądarki lub wpisze inny adres URL. Obecnie większość banków działających w Polsce, które oferują usługi bankowości internetowej, używa protokołu **SSL 3.0 (V3)**. Klucz do szyfrowania informacji jest **2048-bitowy**, co ilustruje rysunek 3.64.



Rysunek 3.64.
Szczegółowe informacje na temat certyfikatu protokołu SSL

Kolejnym przykładem zastosowania szyfrowania jest komunikacja z punktem dostępowym sieci internetowej bezprzewodowej (hotspot). Aby połączenie było bezpieczne, należy je tak skonfigurować, by zapewniało autoryzowany dostęp do sieci bezprzewodowej oraz bezpieczeństwo przesyłania danych. W tym przypadku największą rolę odgrywa prawidłowe skonfigurowanie punktu dostępowego Wi-Fi. W pierwszej kolejności należy się zalogować do routera przy użyciu połączenia kablowego i zmienić hasło administratora na inne niż fabryczne. Przed uaktywnieniem opcji Wi-Fi należy ustanowić sposób szyfrowania (najlepiej na **WPA(2)**). Ten standard musi być obsługiwany przez wszystkie urządzenia działające w sieci bezprzewodowej (Wi-Fi). Jeśli jest taka możliwość, włącz opcję odpowiedzialną za **firewall** (**zaporę sieciową**). Można również zablokować obwieszczanie identyfikatora **SSID**, co spowoduje, że nasza sieć nie będzie widziana przez innych. Zmniejszy to liczbę prób włamań, co oczywiście zwiększy bezpieczeństwo.

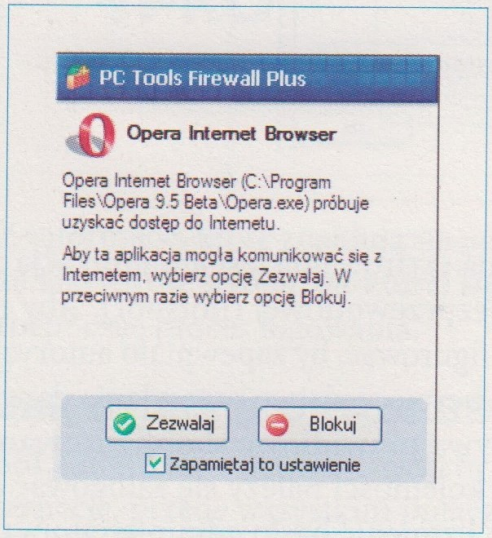
Bardzo ważną sprawą jest regularna aktualizacja oprogramowania routera. Nawet najdroższy router nie zapewni bezpieczeństwa, jeśli w jego oprogramowaniu znajduje się luka. Aktualizacja oprogramowania usuwa wykryte błędy oprogramowania, dlatego powinniśmy regularnie odwiedzać stronę internetową producenta.

Każdy z komputerów podłączonych do sieci powinien również być zabezpieczony przez swoje oprogramowanie zapory sieciowej oraz program antywirusowy, który powinien być jak najczęściej aktualizowany i cały czas aktywny.

Zapora sieciowa (ang. *firewall*) składa się z pewnej liczby komponentów sieciowych (sprzętowych i programowych) montowanych w punkcie styku dwóch sieci. Głównym jej zadaniem jest zachowanie reguł bezpieczeństwa między siecią prywatną a niezabezpieczoną siecią publiczną, na przykład internetem.

Właśnie ta zapora decyduje, które z usług w sieci prywatnej dostępne są z zewnątrz i z jakich usług niezabezpieczonej sieci publicznej można korzystać z poziomu sieci prywatnej. Aby firewall był skuteczny, cały ruch danych między siecią prywatną a internetem musi przez niego przechodzić.

Podczas pierwszego uruchomienia zapory sieciowej (np. *PC Tools Firewall Plus*) program konfiguruje połączenie internetowe. Musimy zdecydować, które usługi (aplikacje) powinny mieć dostęp do internetu, a które nie, tak jak to pokazano na rysunku 3.65.



Rysunek 3.65.
Próba uzyskania dostępu do Internetu przez przeglądarkę internetową — Zezwalaj

Aplikacje, które nie powinny mieć dostępu do internetu, zostaną zablokowane. Jeśli polecenie **Blokuj** ma być zapamiętane na stałe, należy zaznaczyć opcję **Zapamiętaj to ustawienie**. Również dostęp z zewnątrz do naszego komputera jest znacznie utrudniony przez działanie zapory sieciowej.

Złośliwe oprogramowanie malware (ang. *malicious software*)

Kolejnymi zagrożeniami, które możemy napotkać podczas podłączenia sieci do internetu, są zagrożenia związane z różnymi atakami na sieć. Do złośliwego oprogramowania zaliczyć należy wszelkie aplikacje, skrypty i ingerencje mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Rozróżniamy następujące typy ataków i zagrożeń:

- **Wirus**. Program lub fragment wrogiego, wykonalnego kodu, który dołącza się do innego programu, nadpisuje go lub zamienia w celu reprodukcji samego siebie bez zgody użytkownika. Ze względu na różne rodzaje infekcji wirusy dzielą się na: wirusy gnieżdżące się w boot sektorze dysku twardego, wirusy pasożytnicze, wirusy wieloczęściowe, wirusy towarzyszące oraz makrowirusy.
- **Robak**. Wirus rozmnażający się tylko przez sieć. Nie potrzebuje programu żywiciela tak jak typowe wirusy. Robaki często powielają się przez pocztę elektroniczną.
- **Trojan**. Koń trojański to określenie oprogramowania, które — podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje — dodatkowo implementuje niepożądaną, ukrytą przed użytkownikiem działalność.
- **Social engineering**. Częstym błędem popełnianym przez wiele osób jest otwieranie maili od osób lub instytucji, z którymi zwykle nie prowadzimy żadnej korespondencji. Nigdy nie powinniśmy korzystać z linków, które znajdują się wewnątrz listu, w celu połączenia się ze stroną np. naszego banku. Żaden bank nigdy do nas takiego maila nie skieruje i nigdy nie poprosi nas o uzupełnienie w ten sposób jakichkolwiek danych. Nieostrożne kliknięcie linku przekieruje nas na stronę hakera. Próby wyłudzenia ważnych informacji są realizowane nie tylko poprzez pocztę elektroniczną. W praktyce inżynieria społeczna, o której jest tutaj mowa, sprowadza się do świadomego wprowadzenia w błąd pracownika konkretnej organizacji lub firmy celem zdobycia poufnych danych, najczęściej haseł dostępu.
- **Skanery i exploity**. Kolejnym problemem mogą być skanery i exploity. **Exploit** to program, który jest nastawiony na przejęcie kontroli nad atakowanym systemem. W programach takich definiowane są rodzaje rozpoznawanych luk. Exploity mogą być wykorzystywane przez osoby niemające elementarnej wiedzy z zakresu technik hakerskich, co powoduje, że tego typu ataki są niezwykle popularne. **Skanery** to programy służące do testowania i wykrywania luk w serwerze. Są to narzędzia przeznaczone dla administratora sieci, który powinien dbać o bezpieczeństwo serwera, jednak często skanery używane są przez osoby chcące włamać się

do serwera poprzez niezabezpieczone luki. Skanery są jednymi z najpopularniejszych narzędzi do naruszania bezpieczeństwa systemów przez użytkowników mających dostęp do internetu. Każdy bardziej złożony atak jest poprzedzony dokładnym zebraniem informacji o celu ataku.

- **Sniffing**. To kolejne zagrożenie dla naszej sieci. Polega na dokładnym sprawdzeniu, jakiego typu dane są przesyłane w sieci ofiary. Podsłuchiwanie ruchu (ang. *sniffing*) jest narzędziem niezwykle skutecznym. Liczba informacji, które tą drogą można zdobyć, wystarcza do uzyskania pełnej kontroli nad komputerem ofiary. Lekarstwem na to, by wszelkie przechwytywane pakiety były nieużyteczne z punktu widzenia podsłuchującego, jest korzystanie z szyfrowanych protokołów. Mowa tu o takich protokołach jak **https** lub szyfrowanych protokołach pocztowych — **pop** oraz **smtp**. Należy również wspomnieć, że szanse skutecznego podsłuchu mogą zostać ograniczone przez stosowanie odpowiednich urządzeń sieciowych, takich jak switch. Zapewniają one, że każdy pakiet jest wysyłany tylko i wyłącznie z punktu A do punktu B, z pominięciem innych hostów. Co za tym idzie, wszelkie próby podsłuchu nie mają racji bytu.
- **Spoofing**. To szereg technik zmierzających do podszycia się pod kogoś innego w sieci. Idea jest prosta. Gdy następuje uwierzytelnienie klienta, intruz łączy się z sesją, udając uwierzytelnioną maszynę. Później aplikacje uznają, że komunikują się ciągle z tym samym klientem. Jeżeli potencjalny intruz zdoła wysłać pakiety w imieniu autoryzowanego wcześniej klienta, to może np. zerwać połączenie, zmodyfikować sesję (np. zmieniając kwotę 100 zł na 100 000 zł) lub też doprowadzić do przejęcia całości połączenia. Każde z tych działań niesie za sobą potencjalne niebezpieczeństwo. Jak się chronić przed takim atakiem? Ochrona polega głównie na skorzystaniu z połączenia szyfrowanego. Można również zastosować zaawansowany firewall, który potrafi skojarzyć adres IP hosta z wysyłanymi do niego pakietami.
- **Rootkity**. Są to programy, które po zainstalowaniu w systemie tak go modyfikują, aby możliwe było wykonanie zaprogramowanych czynności bez ich wykrycia. **Rootkity** pomagają ukryć się innym procesom, które wykonują niepożądane czynności w systemie. Na przykład, jeżeli w systemie znajdują się **backdoors** (tylne drzwi), które śledzą wykonywane czynności, to **rootkit** ukrywa otwarte porty, mogące być ostrzeżeniem przed niepożądaną komunikacją. A gdy program rozsyłający spam rozpoczyna wysyłanie wiadomości poczty elektronicznej, wówczas rootkit ukrywa wszelkie czynności związane z ich wysyłaniem.
- **Dialer**. Zadaniem tego programu jest zestawienie połączenia internetowego typu dial-up (połączenie wykorzystujące modem komputerowy oraz linię telefoniczną abonenta). Złośliwe dialery zestawiają takie połą-

czenia z numerami w odległych krajach lub z tzw. numerami o podwyższonej płatności (w Polsce numery 0700 i 0400). Koszt takiego połączenia nierzadko dochodzi do kilkunastu zł za minutę. **Dialery** instalują się podstępnie np. podczas wizyt na stronach z crackami, kluczami (serialami), na stronach z treściami pornograficznymi lub nielegalnym oprogramowaniem i muzyką, a następnie zestawiają połączenie z wysoko płatnymi numerami i narażają ofiarę na ogromne rachunki telefoniczne.

- **Adware**. Rodzaj oprogramowania rozpowszechnianego bezpłatnie. W zamian za możliwość darmowego użytkowania, oprogramowanie wyświetla reklamy, zazwyczaj w postaci graficznych banerów. Programy adware to również element tzw. złośliwego oprogramowania, instalującego w systemie operacyjnym dodatkowe, trudne do usunięcia moduły, których zadaniem jest wyświetlanie niechcianych przez odbiorcę reklam (niezależnie od reklam w darmowo użytkowanym programie). Złośliwe adware bardzo często występują wspólnie z programami szpiegowskimi **spyware**.
- **Spyware**. Programy komputerowe, których celem jest szpiegowanie działań użytkownika. Programy te gromadzą informacje o użytkowniku i wysyłają je, często bez jego wiedzy i zgody, autorowi programu. Do takich informacji należeć mogą: adresy WWW stron internetowych odwiedzanych przez użytkownika, dane osobowe, numery kart płatniczych, hasła, zainteresowania użytkownika (np. na podstawie słów wpisywanych w oknie wyszukiwarki), adresy e-mail, archiwum. Programy te czasami mogą wyświetlać reklamy lub rozsyłać spam.

Złośliwe oprogramowanie, aby przedostać się do komputera, korzysta z różnych kanałów. Może być pobrane z internetu i zainstalowane przez **trojany**. Podczas próby uzyskania dostępu do witryny WWW może wyświetlić się prośba o zgodę na zainstalowanie niezbędnego lub aktualnego oprogramowania pochodzącego z niepewnego źródła. Gdy wyrazimy zgodę, zostanie zainstalowane niebezpieczne oprogramowanie.

Formanty *ActiveX* uatrakcyjniają przeglądane strony, dostarczając materiały wideo, animowaną zawartość itd. Programy te mogą jednak działać nieprawidłowo lub pobierać niepożądaną zawartość. W niektórych przypadkach mogą służyć do dyskretnego zbierania informacji o systemie, niszczenia znajdujących się w nim danych, instalowania oprogramowania bez wiedzy użytkownika lub zezwalania innej osobie na zdalne przejęcie kontroli nad komputerem. Uwzględniając te zagrożenia, należy instalować wyłącznie programy, których wydawcom można całkowicie zaufać. Jak zainstalować formant *ActiveX*? Przy pierwszym uruchomieniu strony z formantem *ActiveX* w górnej części okna przeglądarki pojawi się pasek z komunikatem *Ta witryna sieci Web chce zainstalować następujący dodatek*:. Należy kliknąć ten pasek, a następnie wybrać *Zainstaluj formant ActiveX*:.

Efektów działania szkodliwego oprogramowania jest wiele. Może to być uruchomienie niegroźnego programu lub utrata wszelkich plików z dysków. Niektóre programy mogą wykraść ważne osobiste dane (takie jak numer i hasło do konta bankowego) i przekazać je niepowołanym osobom, jak również umożliwić włamanie do komputera i przejęcie nad nim kontroli (tzw. **zombie**). Zombie to komputer zainfekowany i działający w sieci, który może służyć między innymi do masowej wysyłki e-maili, a także jako jedno z ogniw do przeprowadzania rozległych ataków DDoS.

Atak DDoS (ang. *Distributed Denial of Service*) polega na jednoczesnym atakowaniu ofiary z wielu miejsc. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (zainfekowane sieci mogą liczyć nawet 100 000 komputerów **zombie**). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pamięć, czas procesora, pasmo sieciowe, co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu. Użytkownicy maszyn zainfekowanych najczęściej nie zdają sobie sprawy, że ich komputery zostały wykorzystane do nielegalnych celów. Niektóre ze skryptów przeprowadzających atak po zakończeniu ataku mogą samoczynnie odinstalować się, nie pozostawiając żadnych śladów swojej obecności w systemie.

Groźba ataku DDoS bywa czasami używana do szantażowania firm, dla których przerwa w działaniu systemu przekłada się na bezpośrednie straty finansowe. W takich przypadkach osoby stojące za atakiem żądają okupu za odstąpienie od ataku lub jego przerwanie. **Szantaż taki jest przestępstwem**.

Atak typu DoS (ang. *Denial of Service* — odmowa usługi) polega na wysłaniu do serwera-ofiary bardzo dużej liczby zapytań (np. kilku tysięcy odwołań do tej samej strony internetowej). Powoduje to przeciążenie i znaczne spowolnienie pracy atakowanego serwera lub zawieszenie pojedynczej usługi sieciowej. W wielu przypadkach atak taki prowadzi do zawieszenia serwera. Atak DoS jest dokonywany z pojedynczego komputera, więc zlokalizowanie sprawcy sprowadza się do określenia jego numeru IP. Reszta należy do organów ścigania.

Zatruwanie DNS (ang. *cache poisoning*) polega na wysłaniu do serwera DNS fałszywego rekordu kojarzącego nazwę domeny z adresem IP. Serwer DNS zapamiętuje go na pewien czas (do kilku godzin) i zwraca klientom zapamiętany adres IP, czego skutkiem jest przekierowanie na fałszywą stronę.

3.4.6. Zadania

Zadanie 3.1.

Co nazywamy siecią komputerową? Wymień i opisz rodzaje sieci komputerowych. Podaj przykłady różnych sieci.

Zadanie 3.2.

Odpowiedz na postawione poniżej pytania.

1. Co to jest protokół sieciowy?
2. Na czym polega komunikacja między hostami w ramach modelu OSI?
3. Co to jest pakiet i ramka — do jakich warstw modelu OSI należą?
4. Jakie zadania pełnią poszczególne warstwy modelu OSI?
5. Scharakteryzuj transmisję unicast, multicast i broadcast.
6. Co oznacza, że protokół jest nierutowalny? Podaj przykład protokołu nierutowalnego.
7. Na czym polega usługa DHCP?
8. Jaką funkcję pełnią serwery DNS?
9. Co to jest adres URL? Podaj przykłady.
10. Co to są adresy specjalne? Podaj przykłady.
11. Jak można obliczyć adres sieciowy i rozgłoszeniowy?
12. W jaki sposób działa protokół SSL?
13. Na jakie zagrożenia narażony jest komputer połączony z internetem?

Zadanie 3.3.

Przedstaw kilka urządzeń sieciowych — omów je i podaj przykładowe zastosowania.

Wymień klasy adresowe IPv4. Ile hostów można zaadresować w poszczególnych klasach?

Zadanie 3.4.

Podaj przykłady zastosowań adresów publicznych i prywatnych.

Zadanie 3.5.

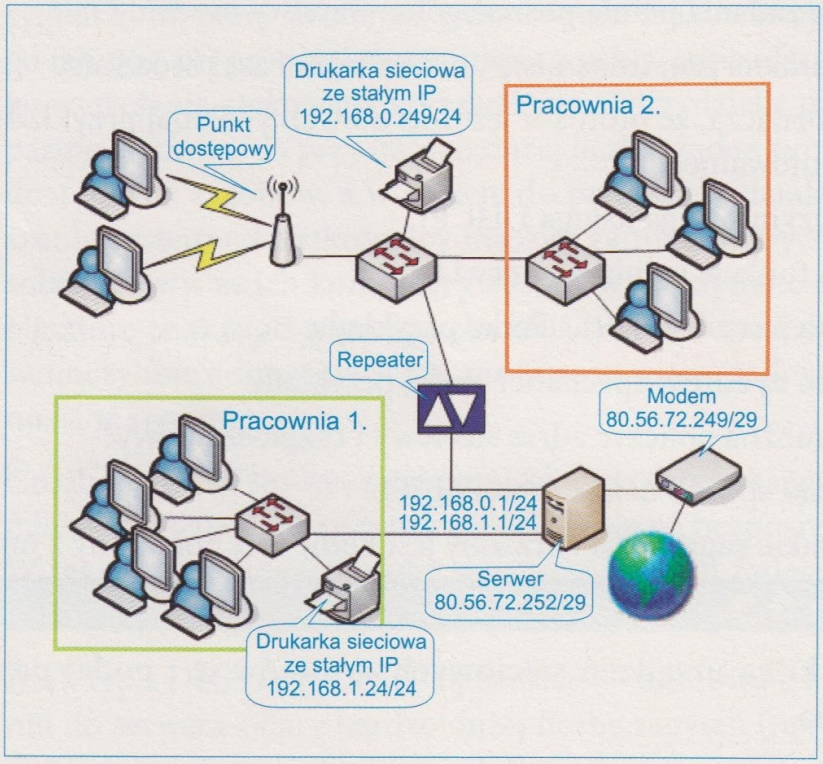
Wymień trzy topologie sieci LAN. Narysuj sieć LAN w topologii magistrali, pierścienia i gwiazdy. W jakiej topologii są połączone komputery w szkolnej pracowni komputerowej?

Zadanie 3.6.

Posiadasz adres IP 31.11.0.0/24. Zaproponuj projekt sieci LAN w topologii drzewiastej, obsługującej: dwie pracownie komputerowe (po 15 stanowisk) Twojej szkoły, dwie pracownie gimnazjum (po 10 komputerów), część administracyjną szkoły (5 komputerów), dwa centra multimedialne (po 4 komputery), kawiarenkę (6 stanowisk), pokój nauczycielski (3 stanowiska).

Zadanie 3.7.

Przyjrzyj się uważnie zaprojektowanej sieci, której schemat zamieszczono na rysunku 3.66. Określ, jakie adresy IP przypiszesz komputerom w obu pracowniach.



Rysunek 3.66.
Projekt sieci do zadań od 3.8 do 3.12

Zadanie 3.8.

Jakie adresy mógłby przydzielać serwer DHCP komputerom podłączonym do punktu dostępowego sieci bezprzewodowej pokazanej na rysunku 3.66?

Zadanie 3.9.

Na rysunku 3.66 zamieszczono **repeater**. Jak sądzisz, co spowodowało jego umiejscowienie? Dlaczego nie ma drugiego takiego urządzenia w segmencie sieci obsługującym pracownię 1.?

Zadanie 3.10.

Ile kart sieciowych znajduje się w serwerze pokazanym na rysunku 3.66? Podaj ich adresy sieciowe.

Zadanie 3.11.

Napisz adresy rozgłoszeniowe obu utworzonych podsieci w projekcie zamieszczonym na rysunku 3.66.

Zadanie 3.12.

Co przyczyniło się do powstania protokołu nowej generacji IPv6? Scharakteryzuj go.

Zadanie 3.13.

Uproszczony zapis adresu IPv6 podano następująco: 2004:ac5::428:35a2. Podaj w zapisie heksadecymalnym, decymalnym oraz binarnym pełny zapis 8 członów tego adresu.

Zadanie 3.14.

Wymień podstawowe zagrożenia, które powstają po podłączeniu komputera do sieci. W jaki sposób zabezpieczysz swój podłączony do internetu komputer?

3.5. Podstawy tworzenia stron WWW

Hipertekst to sposób gromadzenia i prezentacji informacji, umożliwiający tworzenie struktury i wyszukanie potrzebnej informacji, bez konieczności czytania całych tekstów.

Hipertekst cechuje organizacja danych w postaci niezależnych dokumentów hipertekstowych (**węzłów**) zawierających porcję informacji, połączonych **odsyłaczami** (odnośnikami, hiperlinkami).

WWW to hipertekstowy, multimedialny, sieciowy system informacyjny, którego podstawowym zadaniem jest publikowanie informacji.

W systemie WWW węzłem jest strona WWW.

3.5.1. Podstawowe elementy usługi WWW

Język HTML (ang. *HyperText Markup Language* — hipertekstowy język znaczników) — system formatowania dokumentów.