

9. Protokoły sieciowe TCP/IP

Urządzenia w sieci komputerowej komunikują się ze sobą i wymieniają informacje. Wymiana informacji musi przebiegać w ściśle określony sposób umożliwiający przesyłanie danych. Każde z komunikujących się urządzeń musi przestrzegać pewnych ustalonych zasad i reguł postępowania. Zbiór zasad i norm, których muszą przestrzegać komunikujące się ze sobą urządzenia, nazywamy **protokołem komunikacyjnym**. Komunikacja pomiędzy urządzeniami może przebiegać w trybie **połączeniowym** (connection oriented) lub **bezpoleczeniowym** (connectionless oriented).

Tryb **połączeniowy** polega na ustanowieniu logicznego połączenia pomiędzy dwoma komunikującymi się ze sobą urządzeniami. Aby rozpocząć komunikację, należy najpierw nawiązać połączenie. Z trybu połączeniowego korzysta się wtedy, gdy powstaje potrzeba przesyłania wielu komunikatów w obu kierunkach, np. podczas korzystania z usługi telnet. W trybie **bezpoleczeniowym** komunikaty przekazywane są niezależnie, np. przekazywanie wiadomości za pomocą poczty elektronicznej.

W komunikacji biorą udział przynajmniej dwa urządzenia. Jeżeli jedno urządzenie wysyła dane do dokładnie jednego urządzenia, to taki tryb transmisji nazywamy **jednostkowym** (unicast). W sieciach rozwiązane to jest w ten sposób, że każde urządzenie posiada swój unikatowy adres. Dane wysłane przez nadawcę docierają do wielu urządzeń, ale odbierane są tylko przez to urządzenie, którego adres jest adresem docelowym (pozostałe urządzenia ignorują dane, które nie są przeznaczone dla nich). Urządzenie nadawcze może wysłać informację do wszystkich dostępnych urządzeń. W takim przypadku adresem docelowym jest specjalny adres nazywany **rozgłoszeniowym** (broadcast). Urządzenia traktują transmisje na adres rozgłoszeniowy, tak jakby były adresowane na ich adres jednostkowy. W **rozgłaszaniu grupowym** (multicast) dane przeznaczone są tylko do wybranej grupy urządzeń. Adres docelowy jest specjalnym adresem, określającym wybrane urządzenia z danej sieci. W transmisji grupowej unika się wielokrotnego wysyłania tego samego komunikatu do wielu nadawców, po każdym łączy sieciowym informacja jest przekazywana jednokrotnie.

Transmisja **jednokierunkowa** (simplex) to transmisja, w której odbiornik nie może przesłać odpowiedzi ani innych danych. Przykładem tego typu transmisji jest emisja audycji radiowych, gdzie słuchacz przy odbiorniku radiowym może tylko odbierać informacje pochodzące z nadajnika. Tego typu transmisje nie są stosowane w sieciach komputerowych.

Półdupleks (half duplex) to transmisja dwukierunkowa, naprzemienna. W danym momencie jest ustalony tylko jeden kierunek transmisji, a urządzenie może albo nadawać, albo odbierać informacje. Dla odwrócenia kierunku transmisji potrzebny jest system sygnalizacji wskazujący, że urządzenie ukończyło nadawanie i może odbierać informacje. Przykładem jest amatorska stacja krótkofalowa lub radio CB. **Dupleks** (full duplex) to transmisja jednoczesna i dwukierunkowa. Wymaga zazwyczaj dwóch par przewodów dla sieci cyfrowych. Dla połączeń analogowych dla jednej pary przewodów szerokość pasma dzielona jest na dwie części. Przykładem jest rozmowa telefoniczna.

Aby usługi i aplikacje sieciowe mogły prawidłowo działać, muszą mieć zapewnione odpowiednie warunki. Najważniejszymi warunkami są:

- niezawodność przesyłania danych,
- przepustowość łączy,
- czas odpowiedzi.

Niektóre usługi sieciowe, takie jak poczta elektroniczna, transfer plików, pobieranie stron internetowych itp. wymagają niezawodnego przesyłania danych. Nadawca i odbiorca mogą komunikować się między sobą aby upewnić się, że wszystkie dane dotarły bez błędów i w odpowiedniej kolejności. W wypadku błędów protokoły te żądają retransmisji uszkodzonych lub zagubionych danych. Dla tych usług stosowane są protokoły zapewniające niezawodny transport danych. Inne usługi, takie jak przesyłanie dźwięku lub obrazu na żywo, tolerują utratę pewnej ilości danych. W ich przypadku niewielkie zakłócenia spowodowane brakiem części danych są mniej uciążliwe dla odbiorcy niż przerwy w odtwarzaniu spowodowane retransmisją. W tym przypadku stosowane są protokoły zawodnego transportu danych. Nie oznacza to, że dane nie dotrą do miejsca przeznaczenia lecz tylko to, że protokoły nie gwarantują bezbłędnego dostarczenia danych.

Aby działać bez zakłóceń, niektóre aplikacje muszą być w stanie transmitować lub odbierać dane z określoną prędkością. Na przykład aplikacja odtwarzająca pliki multimedialne musi odbierać taką ilość danych, która jest niezbędna do wyświetlania filmu lub odtwarzania muzyki. Aplikacja taka wymaga określonej przepustowości. Jeżeli warunek ten nie będzie spełniony, to aplikacja nie będzie działała prawidłowo (lub w ogóle się nie uruchomi) albo będzie zmuszona pracować przy innych parametrach, np. rozdzielczości obrazu lub jakości dźwięku.

Istnieje pewna grupa aplikacji pracujących w tzw. czasie rzeczywistym, które dopuszczają niewielkie czasy opóźnienia przesyłanych danych. Przykładem może być telekonferencja, w której opóźnienia w transmisji danych powodują przerwy w rozmowie. W grach sieciowych czas pomiędzy wykonaniem czynności, np. kliknięciem myszą, a reakcją na to zdarzenie musi być krótki, aby zapewnić płynność gry.

9.1. Model sieci OSI

Ponieważ protokoły mogą być skomplikowane, nadaje się im strukturę warstwową. Według modelu OSI (Open Systems Interconnection) wyróżniamy siedem takich warstw. Każda warstwa komunikuje się tylko z warstwą bezpośrednio wyższą i bezpośrednio niższą. Warstwy wyższe korzystają z usług warstw niższych, a warstwy niższe świadczą usługi na rzecz warstw wyższych.

Trzy warstwy górne (aplikacji, prezentacji i sesji) zapewniają współpracę z oprogramowaniem realizującym zadania użytkownika systemu komputerowego. Tworzą one interfejs pozwalający na komunikację z warstwami niższymi.

Warstwa **aplikacji** zajmuje się specyfikacją interfejsu, który wykorzystują aplikacje do przesyłania danych do sieci. Warstwa ta świadczy usługi końcowe dla aplikacji. Na tym poziomie działają aplikacje sieciowe, dostępne bezpośrednio dla użytkownika, takie jak poczta elektroniczna, przeglądarka stron WWW itp. Jeżeli użytkownik posługuje się oprogramowaniem działającym w architekturze klient-serwer, to po jego stronie znajduje się klient, a serwer działa na komputerze podłączonym do sieci. Serwer i klient działają w warstwie aplikacji.

Zadaniem warstwy **prezentacji** jest przetworzenie danych pochodzących z warstwy aplikacji do postaci standardowej, której wymagają warstwy niższe, a gdy informacje płyną w kierunku warstwy aplikacji, warstwa prezentacji tłumaczy dane otrzymane z warstw niższych na format zgodny z aplikacją dla której są przeznaczone. Odpowiada także za kompresję i szyfrowanie.

Zadaniem warstwy **sesji** jest zarządzanie przebiegiem komunikacji podczas połączenia między dwoma komputerami. Przepływ tej komunikacji nazywany jest sesją. Warstwa ta nadzoruje połączenie i kontroluje, która aplikacja łączy się z którą dzięki czemu może zapewnić właściwy kierunek przepływu danych. W razie przerwania połączenia, nawiązuje je ponownie. Ponadto określa, czy komunikacja może zachodzić w jednym kierunku, czy w obu kierunkach i gwarantuje zakończenie wykonywania bieżącego żądania przed przyjęciem kolejnego.

Zadaniem czterech najniższych warstw jest transmisja danych. Zajmują się odnajdywaniem odpowiedniej drogi do miejsca przekazania konkretnej informacji. Dzieli dane na odpowiednie dla danej warstwy **jednostki danych** PDU (Protocol Data Unit). Dodatkowo zapewniają weryfikację bezbłędności przesyłanych danych. Warstwy dolne to warstwa transportowa, sieciowa, łącza danych oraz fizyczna. Warstwa **transportowa** przesyła wiadomość kanałem stworzonym przez warstwę sieciową. W tym celu dzieli dane otrzymane z warstwy sesji na **segmenty**, które są kolejno numerowane i wysyłane do stacji docelowej. Zapewnia właściwą kolejność otrzymanych segmentów, a w razie zaginięcia lub uszkodzenia segmentu może zażądać jego retransmisji. Stacja docelowa może również wysłać potwierdzenie odebrania segmentu.

Warstwa **sieciowa**, jako jedyna, dysponuje wiedzą dotyczącą fizycznej topologii sieci. Rozpoznaje, jakie trasy łączą poszczególne komputery i sieci i na tej podstawie decyduje, którą z nich wybrać. Jednostką danych w tej warstwie jest **pakiet**. Warstwa ta odpowiada za adresowanie logiczne węzłów sieci (adresy IP).

Warstwa **łącza danych** nadzoruje warstwę fizyczną i steruje fizyczną wymianą bitów. Ma możliwość zmiany parametrów pracy warstwy fizycznej, tak aby obniżyć liczbę pojawiających się podczas przekazu błędów. Definiuje mechanizmy **kontroli błędów** CRC (Cycle Redundancy Check) i zapewnia dostarczanie ramek informacji do odpowiednich węzłów sieci na podstawie fizycznego adresu MAC karty sieciowej. Jednostką danych w tej warstwie jest ramka. Warstwa łącza danych dzieli się na dwie podwarstwy:

- LLC (Logical Link Control!) - sterowania łączem danych - kontroluje poprawność transmisji i obsługuje tworzenie ramek. Współpracuje przede wszystkim z warstwą sieciową.
- MAC (Media Access Control!) - sterowania dostępem do nośnika - zapewnia dostęp do nośnika sieci lokalnej i współpracuje przede wszystkim z warstwą fizyczną.

Warstwa **fizyczna** odpowiedzialna jest za przesyłanie strumieni bitów bez kontroli ruchu i bez uwzględnienia rodzaju informacji. Określa ona wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego oraz radiowego wysyłania i odbierania sygnałów. Ustala sposób przesyłania bitów i odległości przerw między nimi.

- umożliwia łatwiejsze zastępowanie jednego rozwiązania innym, bez konieczności wprowadzania zmian w innych warstwach,
- wprowadza niezależność poszczególnych rodzajów nośników danych wykorzystywanych w sieciach - jedne zastępują (bądź uzupełniają) drugie.

Mimo iż aplikacje wydawać by się mogło, że komunikuje się bezpośrednio z odpowiadającą jej aplikacją uruchomioną na innym komputerze, to komunikacja ta nie jest bezpośrednia. Aplikacja bowiem w celu przekształcenia danych i dostarczenia ich do miejsca docelowego wywołuje funkcje oferowane przez warstwę prezentacji. Podobnie, warstwa prezentacji jednego systemu wirtualnie porozumiewa się z warstwą prezentacji innego systemu zdalnego, w rzeczywistości wywołując funkcje warstwy sesji, pozwalające na sterowanie sesją i dostarczenie danych do warstwy prezentacji systemu zdalnego. Tego rodzaju „wirtualna” komunikacja zachodzi na poziomie każdej warstwy poza fizyczną na poziomie której dwa urządzenia połączone są przy użyciu określonego nośnika i kontaktują się rzeczywiście (fizycznie). Model OSI to podstawowy model komunikacji sieciowej. Model ten jest najlepszym narzędziem służącym do nauki wysyłania i odbierania danych w sieci. Pozwala on obserwować funkcje poszczególnych warstw sieci. Model OSI jest traktowany jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Model ten jest otwarty, co oznacza, że każdy może z niego korzystać bez wnoszenia opłat licencyjnych.

9.3. Model sieci TCP/IP

Oprócz modelu OSI istnieją także inne modele sieci, z których najbardziej popularny model **TCP/IP** powstał na zamówienie Departamentu Obrony USA. Model TCP/IP jest powszechnie stosowany, między innymi w sieci Internet. Model ten jest ściśle związany ze stosem protokołów TCP/IP. Podobnie jak w modelu OSI możemy w nim wyróżnić warstwy, jednak funkcje są różne, pomimo iż niektóre z nich posiadają jednakowe nazwy. Model TCP/IP składa się z czterech warstw.

Warstwa aplikacji obejmuje funkcje trzech najwyższych warstw modelu OSI (aplikacji, prezentacji i sesji). Użytkownicy uruchamiają programy, które uzyskują dostęp do usług za pośrednictwem protokołu na poziomie warstwy transportu i wysyłają lub odbierają dane w postaci pojedynczych komunikatów lub strumienia bajtów. Programy użytkowe przekazują do warstwy transportowej dane w wymaganym formacie, aby mogły one zostać dostarczone w odpowiednie miejsce. W warstwie tej działa wiele protokołów aplikacji, między innymi http, ftp, telnet, ssh, smtp, pop3 itp. Podstawowym zadaniem **warstwy transportowej** jest zapewnienie komunikacji między programami użytkownika. Warstwa ta może zarządzać przepływem informacji oraz zapewniać niezawodność przesyłania przez porządkowanie segmentów danych i retransmisję uszkodzonych lub zagubionych segmentów. W komputerze może działać wiele aplikacji wymieniających dane w sieci przy wykorzystaniu portów określonych dla każdego połączenia i nie nastąpi wymieszanie się przesyłanych przez nie danych. Warstwa transportowa dzieli strumień danych na segmenty, a w nagłówku umieszcza numer portu identyfikujący aplikację wysyłającą lub odbierającą dane. W warstwie tej działa **protokół połączeniowy TCP** oraz **bezpołączeniowy UDP**.

Warstwa internetowa przyjmuje segmenty z warstwy transportowej razem z informacjami identyfikującymi odbiorcę. Zadaniem jej jest wysyłanie pakietów i dostarczenie ich do miejsca przeznaczenia, niezależnie od trasy, po której będą przesyłane. Protokołem zarządzającym tą warstwą jest **protokół IP**. Warstwa dzieli dane na pakiety, dodaje nagłówek zawierający między innymi adres IP nadawcy i odbiorcy. Na podstawie adresu IP miejsca docelowego podejmowana jest decyzja, czy wysłać pakiet wprost do odbiorcy w sieci lokalnej, czy też do routera, który przekaże go do odpowiedniego interfejsu sieciowego. Routery pracujące w niej wyznaczają najlepsze trasy do miejsca przeznaczenia pakietów, proces ten określany jest jako **trasowanie** lub **routing**. Warstwa ta zajmuje się także pakietami przychodzącymi, sprawdzając ich poprawność i stwierdzając za pomocą algorytmu trasowania, czy należy je przesłać dalej, czy też przetwarzać na miejscu. W przypadku pakietów adresowanych do maszyny lokalnej oprogramowanie tej warstwy usuwa nagłówek pakietu i wybiera protokół transportowy, który go będzie dalej obsługiwał. Warstwa ta wysyła też komunikaty kontrolne i komunikaty o błędach oraz obsługuje komunikaty przychodzące.

Warstwa dostępu do sieci odbiera pakiety IP i przesyła je przez daną sieć. Zapewnia interfejs z siecią fizyczną i zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi. Najczęściej są to karty sieciowe lub modemy. Formatuje dane do transmisji przez nośnik oraz adresuje dane do podsieci, opierając się na adresach fizycznych. Zapewnia sprawdzanie błędów przesyłu danych za pomocą sumy kontrolnej ramki.

W tabeli poniżej porównano model OSI i TCP/IP oraz przedstawiono protokoły najczęściej używane w poszczególnych warstwach.

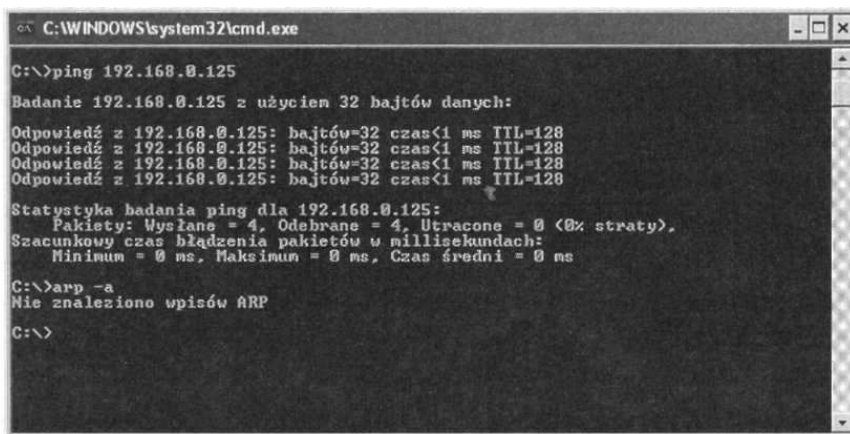
Model OSI	Model TCP/IP	Protokoły		
Warstwa aplikacji	Warstwa aplikacji	telnet, ssh, http, smtp, pop3, ftp	tftp, dns	
Warstwa prezentacji				
Warstwa sesji				
Warstwa transportowa	Warstwa transportowa	TCP	UDP	
Warstwa sieciowa	Warstwa internetowa	IP, ICMP IGMP, RIP, OSPF, BGP		ARP
Warstwa łączy danych	Warstwa dostępu do sieci	Ethernet		
Warstwa fizyczna				

W modelu TCP/IP sieci lokalne w warstwie dostępu do sieci budowane są w oparciu o standard Ethernet. W sieciach rozległych WAN w tej warstwie stosowane są różne technologie, np. połączenia modemowe, DSL, Frame Relay, ATM.

Na styku pomiędzy warstwą internetową i warstwą dostępu do sieci działa protokół **ARP** (Address Resolution Protocol), który pozwala na ustalenie adresu sprzętowego MAC hosta, gdy dany jest adres warstwy sieciowej IP. Z protokołu tego korzystamy podczas wysyłania danych. Podczas

komunikacji urządzeń w sieci dane muszą przejść wszystkie etapy enkapsulacji. W nagłówku pakietu urządzenie nadawcze umieszcza adres IP nadawcy oraz odbiorcy. Adres nadawcy jest przydzielony każdemu urządzeniu, adres odbiorcy jest wprowadzany przez użytkownika w postaci adresu IP lub nazwy domenowej komputera. Adresy te są więc znane i urządzenie może utworzyć pakiet. W nagłówku ramki potrzebny jest adres MAC nadawcy i odbiorcy. Każda karta sieciowa posiada unikatowy adres MAC, więc urządzenie „zna” swój adres, brakuje jeszcze adresu MAC urządzenia odbiorcy. Do ustalenia tego właśnie adresu wykorzystywany jest protokół ARP.

Gdy komputer chce skorzystać z protokołu ARP, przygotowuje specjalny pakiet zapytania ARP, który jest wysyłany na adres rozgłoszeniowy, dzięki czemu dociera do wszystkich urządzeń w sieci lokalnej. Urządzenie o szukanym adresie sieciowym odpowiada, przesyłając pakiet z odpowiedzią zawierającą adres sprzętowy MAC. Komputer dysponuje już wszystkimi adresami i może przygotować ramkę. Aby uniknąć konieczności wysyłania kolejnego zapytania ARP, komputer zapisuje sobie w specjalnej tablicy informacje o adresach urządzeń, z którymi się komunikował. Przed następnym wysłaniem zapytania ARP sprawdzi w tablicy, czy nie ma zapisanego poszukiwanego adresu. Komputery mogą się ze sobą komunikować za pośrednictwem adresu fizycznego tylko w obrębie danej sieci (w warstwie drugiej modelu OSI). Jeśli jakieś informacje mają być przesłane do innej sieci, to protokół ARP jest wykorzystywany do uzyskania informacji o adresie bramy sieciowej. Na rysunku 9.4 pokazano zawartość tablicy ARP komputera, który komunikował się z innymi urządzeniami. Protokół odwrotny **RARP** (Reverse Address Resolution Protocol) pozwala na ustalenie adresu IP na podstawie adresu fizycznego MAC.



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.0.125
Badanie 192.168.0.125 z użyciem 32 bajtów danych:
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Statystyka badania ping dla 192.168.0.125:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 <0% straty>.
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms
C:\>arp -a
Nie znaleziono wpisów ARP
C:\>
```

Rys. 9.4. Tablica ARP

9.4. Protokoły warstwy sieciowej

Protokół IP (Internet Protocol) jest odpowiedzialny za przesyłanie pakietów pomiędzy użytkownikami sieci. Jest protokołem bezpołączeniowym, co oznacza, że w trakcie transmisji nie sprawdza się poprawności pakietów przesyłanych przez sieć. Nie ma zatem gwarancji ich dostarczenia, ponieważ mogą one zostać po drodze zagubione lub uszkodzone.

Podstawowymi funkcjami protokołu IP jest:

- określanie i tworzenie struktury pakietu.
- określanie schematu adresowania logicznego IP,

- kierowanie ruchem pakietów w sieci.

IP jest protokołem zawodnym. Jedynym kryterium pozwalającym sprawdzić poprawność przesyłania jest suma kontrolna nagłówka zawarta w polu Header Checksum. Jeżeli w trakcie transmisji został odkryty błąd, to pakiet jest niszczone przez stację, która wykryła niezgodność. W takim przypadku nie ma żadnych powtórek transmisji i kontroli przepływu danych. Nagłówek protokołu IP jest wykorzystywany do transportu danych między urządzeniem źródłowym i docelowym. Budowa nagłówka pokazana jest na rys. 9.5.

Rys. 9.5 Budowa nagłówka protokołu IP

1 bajt		2 bajt	3 bajt	4 bajt
Wersja	Długość nagrania	Typ usług	Całkowita długość pakietu	
Identyfikacja		Flags	Przesunięcie fragmentu	
Czas życia	Protokół	Suma kontrolna		
Adres źródłowy				
Adres docelowy				
Opcje				
Dane				

Znaczenie wybranych pól nagłówka:

- Czas życia TTL (Time To Live) określa maksymalny czas przebywania pakietu w sieci. Każdy router, przez który przechodzi pakiet, zmniejsza wartość o 1. Gdy wartość w polu osiągnie zero, pakiet jest kasowany. Zabezpiecza to sieć przed przesyłaniem pakietów krążących w pętli. Maksymalna wartość tego pola wynosi 255, co oznacza że na trasie pakietu nie może być więcej niż 255 routerów.
- Adres źródłowy - adres IP nadawcy pakietu.
- Adres docelowy - adres IP odbiorcy pakietu.

Warstwa sieciowa odpowiada za wybranie optymalnej trasy, po jakiej przesyłany będzie każdy pakiet. Jeżeli odbiorca znajduje się w tej samej sieci, pakiet będzie wysłany bezpośrednio do niego. W przeciwnym razie musi być przekazany do bramy łączącej sieci. Decyzję o wyborze trasy podejmuje router na podstawie adresu IP urządzenia docelowego, umieszczonego w nagłówku pakietu oraz w oparciu o informacje posiadane w tablicy routingu. W tablicy tej router przechowuje informacje o wszystkich sieciach, do których jest w stanie wysłać pakiety. Jeżeli w tablicy routingu nie ma adresu docelowego, umieszczonego w pakiecie, router może wysłać pakiet, korzystając z trasy domyślnej (jeżeli została zdefiniowana), lub pakiet jest kasowany. Przykładowa tablica routingu pokazana jest na rys. 9.6.


```

R4# ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS,
L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o - ODR
Gateway of last resort is not set
[1] C    10.77.0.0/16 is directly connected, Ethernet0
[2] C    10.80.0.0/16 is directly connected, Ethernet0
[3] C    10.5.0.0/16 is directly connected, Ethernet0
[4] C    10.125.0.0/16 is directly connected, Ethernet0
[5] C    10.1.0.0/16 is directly connected, Ethernet0
[6] R    192.168.5.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[7] R    192.168.1.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[8] R    192.168.2.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[9] R    192.168.3.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[10] R   192.168.4.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
R4#

```

Rys. 9.6. Tablica routingu

Z tablicy tej wynika, że pakiet adresowany do sieci 10.77.0.0/16 wysłany zostanie za pomocą interfejsu Ethernet0, a pakiety adresowane do sieci 192.168.1.0/24 wysyłane będą interfejsem Serial0.

9.4.1 Protokoły routingu

Informacje o trasach w tablicach routingu mogą być wprowadzane **statycznie** przez administratora, lecz wymaga to dużo czasu i rekonfiguracji wszystkich routerów w przypadku zmian w sieci. Routery mogą również uczyć się tras w sposób **dynamiczny**. W tym celu korzystają z protokołów routingu do wymiany między sobą informacji o trasach lub topologii sieci. Na podstawie tych informacji ustalane są optymalne trasy prowadzące do poszczególnych sieci i umieszczane w tablicy routingu. Przekładami protokołów routingu są RIP, OSPF, IGRP, EIGRP.

Protokół RIP jest protokołem routingu typu dystans-wektor (distance-vector). Ze względu na niskie wymagania sprzętowe może być używany przez wszystkie routery. Router, na którym uruchomiony jest protokół RIP, wysyła do swoich bezpośrednich sąsiadów zawartość swojej tablicy routingu w określonych, stałych przedziałach czasu, standardowo co 30 s. Router po przyjęciu aktualizacji od sąsiada porównuje ją z własną tablicą routingu i w razie konieczności uaktualnia ją. W tablicy routingu znajdują się najlepsze trasy do wszystkich sieci. Jako miarę jakości trasy (metrykę) w protokole RIP przyjęto liczbę przeskoków (hopów) pomiędzy routerami, jakie pakiet musi wykonać, aby dotrzeć do celu. Gdy router przyjmie uaktualnienie tablicy routingu, które zawiera nowe lub zmienione informacje o trasach, to dodaje jedynkę do wartości metryki wskazanej w uaktualnieniu i wpisuje zmianę do tablicy routingu. Adresem następnego przeskoku jest adres IP nadawcy. Liczba przeskoków jest ograniczona do 15. Dlatego RIP nie może być stosowany w bardzo dużych sieciach. RIP dobrze spełnia swoje zadanie w sieciach jednorodnych, to znaczy takich, w których wszystkie łącza mają jednakową przepustowość.

Protokół OSPF (Open Shortest Path First) jest, podobnie jak RIP, protokołem otwartym, co oznacza, że jego specyfikacja jest ogólnie dostępna. Protokół OSPF jest protokołem routingu typu **stanu łącza** (link-state), wykorzystującym **algorytm SPF** (Dijkstry) do obliczania najkrótszych ścieżek. Metryką w protokole OSPF jest koszt, który jest powiązany z przepustowością łącza (im większa przepustowość,

tym niższy koszt). Protokół OSPF przeznaczony jest do dużych sieci. Sieć taka może być podzielona na obszary. Routery w danym obszarze, na których uruchomiono protokół OSPF wymieniają się wzajemnie krótkimi komunikatami LSA (Link-State Advertisement). Na podstawie tych komunikatów każdy router zbiera informacje o całej topologii obszaru, a następnie za pomocą algorytmu SPF oblicza najlepsze trasy do wszystkich sieci. Każdy obszar musi być dołączony do obszaru 0 (szkieletowego), co pozwala na połączenie sieci w jedną całość. Zmiany dokonane w jednym z obszarów nie powodują konieczności uruchomienia algorytmu SPF w pozostałych obszarach. Obliczanie ścieżek w poszczególnych obszarach jest łatwiejsze i wymaga mniejszego nakładu obliczeniowego. Ze względu na konieczność dokonywania skomplikowanych obliczeń, protokół OSPF ma większe wymagania sprzętowe niż RIP.

Protokół IGRP (Interior-Gateway Routing Protocol) i jego następca **EIGRP** (Extended IGRP) zostały opracowane przez firmę CISCO. IGRP podobnie jak RIP jest protokołem typu dystans-wektor, ale wykorzystuje jako metrykę różne kombinacje czterech miar: opóźnienia, szerokości pasma (przepustowości), obciążenia i niezawodności. Protokół ten zastępowany jest przez EIGRP. EIGRP jest protokołem hybrydowym, to znaczy posiada najlepsze cechy algorytmów routingu z wykorzystaniem wektora odległości i według stanu łącza. Protokół EIGRP do wyznaczania tras stosuje **algorytm DUAL** (Diffusing - Update ALgorithm). Jest on zalecany do stosowania przez CISCO. Współcześnie liczba routerów w sieci Internet jest tak duża, że żaden z nich nie byłby w stanie przechowywać tras do wszystkich sieci. Aby temu zapobiec i ułatwić zarządzanie w Internecie, wprowadzono hierarchię routingu. Największą jednostką w hierarchii jest **system autonomiczny AS** (Autonomous System), który jest zbiorem sieci pod wspólną administracją z ustaloną wspólną strategią routingu. System AS można podzielić na pewną liczbę **obszarów** (areas), które są grupami sąsiednich sieci i przyłączonych hostów. Poszczególne obszary sprzęgają routery graniczne obszaru (area border routers). Router graniczny utrzymuje oddzielną dla każdego obszaru bazę danych o topologii. Protokoły RIP, OSPF, IGRP i EIGRP są protokołami **routingu wewnętrznego** IGP (Interior Gateway Protocols) i mogą działać wewnątrz systemu autonomicznego. Do ustalania tras pomiędzy systemami autonomicznymi wykorzystywane są **zewnętrzne protokoły routingu** EGP (Exterior Gateway Protocol), np. protokół BGP

9.4.2 Rozsyłanie grupowe informacji

Normalna komunikacja z wykorzystaniem protokołu IP odbywa się między jednym nadawcą i jednym odbiorcą (nie licząc pakietów rozgłoszeniowych). Dla niektórych aplikacji użyteczne jest wysyłanie informacji jednocześnie do wielu odbiorców, np. giełdowe informacje dla brokerów, połączenia konferencyjne, odbierania audycji radiowych i telewizyjnych za pośrednictwem Internetu.

Rozgłaszanie grupowe (multicasting) jest technologią opierającą się na następujących zasadach:

- routery obsługujące transmisję przekazują pakiety multicastowe do danej sieci tylko wtedy, gdy w tej sieci znajduje się przynajmniej jeden członek konkretnej grupy multicastowej. Pojedynczy host może być członkiem jednej lub więcej grup.
- komputery do powiadomienia routera o członkostwie w danej grupie lub o jego rezygnacji

wykorzystują protokół **IGMP** (Internet Group Management Protocol). Hosty zgłaszają za pomocą IGMP swoje członkostwo w grupie multicastowej do dowolnego sąsiadującego routera multicastowego.

- komputery mogą być odbiorcami, nadawcami lub pełnić obie te role jednocześnie w danej grupie multicastingowej.

Dane przesyłane są na specjalne adresy multicastowe określające grupę, która jest zainteresowana konkretnym typem danych. Wszystkie multicastowe adresy IP mieszczą się w zakresie od 224.0.0.0 do 239.255.255.255. Zakres ten określa tylko grupę odbiorców, nadawcy posiadają zawsze adres unicastowy. Adresy w zakresie 224.0.0.0 -- 224.0.0.255 są zarezerwowane dla protokołów w sieciach lokalnych i nie mogą być przekazywane przez routery, np. adresy 224.0.0.5 i 224.0.0.6 wykorzystywane są przez protokół routingu OSPF do przesyłania informacji pomiędzy wszystkimi routerami. Zakres adresów od 224.0.1.0 do 238.255.255.255 jest zakresem adresów globalnych, które mogą być wykorzystywane do multicastingu między organizacjami oraz przez Internet. Część z nich jest zarezerwowana dla niektórych aplikacji, np. 224.0.1.1 dla protokołu NTP (Network Time Protocol). Zakres adresów od 239.0.0.0 do 239.255.255.255 jest zakresem o ograniczonym zasięgu, przeznaczonym dla grup lokalnych lub jednej organizacji. Więcej informacji o adresach IP znajduje się w rozdziale „Adresowanie IP” w drugiej części podręcznika.

W routerze protokół IGMP śledzi, do których sieci należy wysłać transmisje grupowe, na podstawie przynależności hostów do grup. Każdy router okresowo odpytuje swoje sieci, aby sprawdzić, czy dostarczanie danych grupowych nadal jest wymagane. Kontrola ta odbywa się za pomocą zapytań o członkostwo hosta, które kierowane są pod zarezerwowany adres IP 224.0.0.1. Hosty przynależące do grup odpowiadają na ten komunikat raportem, którego adres docelowy odpowiada wymaganemu adresowi grupowemu. Przyłączenie do grupy odbywa się przez transmisje pakietu IGMP - Host Membership Report. Pakiet ten zawiera adres IP pożądanej grupy. Przyłączenie hosta do grupy obejmuje dwa procesy u klienta:

- host powiadamia router, że chce przyłączyć się do odpowiedniej grupy.
- host wiąże dynamicznie IP z adresem grupowym zarezerwowanym dla danej aplikacji oraz z zarezerwowanym adresem Ethernet.

Host, który podłączy się do nowej grupy multicastowej, ma obowiązek wysłać natychmiastowy Raport do tej grupy, bez czekania na zapytanie od routera. Aby korzystać z transmisji multicastowych, należy dysponować odpowiednią aplikacją obsługującą ten rodzaj transmisji.

9.4.3 Protokół ICMP

Ścisłe związane z protokołem IP jest protokół **ICMP** (Internet Control Message Protocol). Protokół IP, jako bezpołączeniowy, nie posiada mechanizmów informowania o błędach w funkcjonowaniu sieci IP oraz diagnostyki sieci. Do tego celu przeznaczony jest protokół ICMP. Umożliwia on przesyłanie między komputerami lub routerami informacji o błędach występujących w funkcjonowaniu sieci IP. Najczęściej używanymi poleceniami korzystającymi w protokołu ICMP są ping i tracert.

Ping jest to program używany w sieciach komputerowych działających w oparciu o protokół TCP/IP, służący do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostem testującym i testowanym oraz określenie jakości połączenia przez pomiar liczby zgubionych pakietów oraz czasu potrzebnego na ich transmisję. Ping wysyła pakiety **żądania echa** ICMP (Echo Request) i odbiera **odpowiedzi na żądanie echa** ICMP (Echo Reply). Jako argument dla polecenia ping można podać adres IP lub nazwę domenową komputera testowanego (rys. 9.7).

Komputery powinny odpowiadać na żądanie echa, lecz większość współczesnych programów typu firewall blokuje ten proces, w konsekwencji czego możemy nie otrzymać odpowiedzi, mimo że istnieje połączenie pomiędzy hostami.



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.0.125
Badanie 192.168.0.125 z użyciem 32 bajtów danych:
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.0.125: bajtów=32 czas<1 ms TTL=128
Statystyka badania ping dla 192.168.0.125:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w milisekundach:
Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms
C:\>ping www.wp.pl
Badanie www.wp.pl [212.77.100.101] z użyciem 32 bajtów danych:
Odpowiedź z 212.77.100.101: bajtów=32 czas=26ms TTL=248
Odpowiedź z 212.77.100.101: bajtów=32 czas=26ms TTL=248
Odpowiedź z 212.77.100.101: bajtów=32 czas=27ms TTL=248
Odpowiedź z 212.77.100.101: bajtów=32 czas=28ms TTL=248
Statystyka badania ping dla 212.77.100.101:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w milisekundach:
Minimum = 26 ms, Maksimum = 28 ms, Czas średni = 26 ms
C:\>
```

Rys. 9.7. Działanie programu ping

Program **tracert** (w systemach Linux program nazywa się traceroute) jest przeznaczony do śledzenia trasy, po jakiej przesyłane są pakiety w sieci.

Program ten wysyła pakiet żądania echa z polem TTL (Time To Live) ustawionym na kolejne wartości, od 1 do 30. Wartość TTL jest zmniejszana przy przechodzeniu przez kolejne routery na trasie. Jeżeli pole TTL osiągnie wartość 0, pakiet jest kasowany przez router. Router dodatkowo wysyła za pomocą protokołu ICMP informację zwrotną o błędzie. Komputer źródłowy uzyskuje, bezpośrednio po wysłaniu żądania o wartości 1, adres IP pierwszego routera na trasie. W następnym pakiecie pole TTL ma wartość 2, co powoduje, że pierwszy router zmniejszy tę wartość do 1, a drugi router zmniejszy TTL do 0 i skasuje pakiet wysyłając komunikat o błędzie. W ten sposób program tracert może prześledzić trasę w sieci zawierającej nie więcej niż 30 routerów. Brak odpowiedzi na zadany pakiet sygnalizowany jest znakiem gwiazdki „*” i może wynikać z konfiguracji firewalla lub przeciążenia sieci. Przykład działania polecenia tracert pokazano na rys. 9.8.

```

C:\WINDOWS\system32\cmd.exe
C:\>tracert www.onet.pl

Trasa śledzenia do www.onet.pl [213.180.138.148]
przewyższa maksymalną liczbę przeskoków 30

 1  <1 ms    <1 ms    <1 ms    192.168.0.1
 2   6 ms     7 ms     9 ms     10.36.0.1
 3  10 ms    *        9 ms     172.17.147.1
 4  18 ms    17 ms    17 ms    172.17.11.134
 5  19 ms    17 ms    17 ms    z-atnan.vectra.pl [194.153.134.29]
 6   *       *        *        Upłynął limit czasu żądania.
 7  34 ms    34 ms    35 ms    com-BR4.z.dab-BR1.net.onet.pl [213.180.142.1]
 8  35 ms    34 ms    33 ms    com-CR1.z.com-BR4.net.onet.pl [213.180.142.5]
 9  36 ms    38 ms    35 ms    sg.m1.onet.pl [213.180.138.148]

Śledzenie zakończone.
C:\>

```

Rys. 9.8. Działanie polecenia tracert

9.5. Protokoły warstwy transportowej

W warstwie transportowej w stosie protokołów TCP/IP może działać protokół połączeniowy TCP lub protokół bezpołączeniowy UDP.

9.5.1 Protokół TCP

Protokół **TCP** (Transmission Control Protocol) działa w warstwie transportowej w trybie połączeniowym. Korzystanie z trybu połączeniowego umożliwia zagwarantowanie dostarczenia danych do odbiorcy. Połączenia TCP są połączeniami wirtualnymi, rozpoznawanymi po adresach i portach urządzeń docelowych i źródłowych. Połączenia takie charakteryzują się możliwościami sterowania przepływem, potwierdzaniem odbioru, zachowywaniem kolejności danych, kontrolą błędów i przeprowadzaniem retransmisji. Segmenty TCP składają się z nagłówka i danych. Budowa nagłówka TCP pokazana jest na rys. 9.9.

1 bajt		2 bajt		3 bajt		4 bajt	
Port źródłowy				Port docelowy			
Numer sekwencyjny							
Numer potwierdzenia							
Długość nagrania	Rezerwa	Znaczniki		Okno			
Suma kontrolna				Wskaźnik pilności			
Opcje							
Dane							

Rys. 9.9. Budowa nagłówka TCP

Najważniejszymi polami nagłówka TCP są:

- port źródłowy,
- port docelowy,
- numer sekwencyjny,
- numer potwierdzenia,
- okno.

Ponieważ na komputerze posiadającym jeden adres IP może jednocześnie działać wiele aplikacji, to do ich identyfikacji wykorzystuje się **porty**. Porty reprezentowane są przez liczby naturalne z zakresu od 0 do 65535. Numery portów od 0 do 1023 są ogólnie znane (well-known port numbers) i zarezerwowane dla usług, np. WWW korzysta z portu 80, a telnet z portu 23. Dzięki portom możemy określić, dla jakiej aplikacji przeznaczony jest segment danych (port docelowy), lub z którego portu wysłano dane (port źródłowy).

Komunikacja między aplikacjami może się odbywać za pomocą **gniazd** (socket). Gniazdo to kombinacja adresu IP i numeru portu. Gniazdo jednoznacznie określa proces w sieci lub zakończenie logicznego łącza komunikacyjnego między dwiema aplikacjami. Jeśli aplikacje uruchomione są na dwóch różnych komputerach, to para odpowiadających im gniazd definiuje połączenie. Gniazdo możemy traktować jako kanał komunikacyjny - jeden program wpisuje do niego dane, a drugi je odbiera. Serwer otwiera gniazdo i oczekuje na połączenie. Klient łączący się z otwartym gniazdem musi znać sieciowy adres komputera oraz numer portu. Każdy przesyłany segment danych oznaczany jest kolejnym **numerem sekwencyjnym**. Przed rozpoczęciem transmisji nadawca i odbiorca wymieniają między sobą numery sekwencyjne. Odbiorca wiadomości na podstawie numeru sekwencyjnego ustala kolejność segmentów oraz sprawdza, czy wszystkie segmenty dotarły do miejsca przeznaczenia. Potwierdzenie odebrania segmentu polega na wysłaniu przez odbiorcę numeru kolejnego segmentu, który powinien być przesłany. Na przykład jeżeli ostatni poprawnie odebrany segment miał numer 123, to odbiorca wyśle numer potwierdzenia 124 (numer następnego segmentu, który ma być przesłany). Potwierdzenie wysyłane jest po odebraniu pewnej liczby danych określonych w polu **okno**. Jeżeli w sieci występuje dużo błędów, to wielkość okna jest zmniejszana, aby częściej otrzymywać potwierdzenia i przez to zmniejszyć liczbę segmentów danych wymagających retransmisji. Jeżeli liczba błędów się zmniejsza, to rozmiar okna jest powiększany, aby zapewnić większą przepustowość sieci.

9.5.2 Protokół UDP

Protokół UDP (User Datagram Protocol) działa w warstwie transportowej w trybie bezpołączeniowym. Protokół ten nie gwarantuje dostarczenia danych do odbiorcy. Jeżeli pakiet nie dotrze do odbiorcy, lub dotrze uszkodzony, UDP nie podejmie żadnych działań zmierzających do retransmisji danych, a zapewnienie niezawodności pozostawi warstwie wyższej. Nagłówek protokołu UDP (rys. 9.10) jest prostszy niż TCP. Protokół wykorzystywany jest do szybkiego przesyłania danych w niezawodnych sieciach.

Dzięki temu, że istnieją dwa alternatywne względem siebie protokoły w warstwie transportowej, TCP i UDP, możliwy jest dobór przez aplikacje odpowiedniego dla siebie rozwiązania.

1 bajt	2 bajt	3 bajt	4 bajt
Port źródłowy		Port docelowy	
Długość		Suma kontrolna	
Dane			

Rys. 9.10. Budowa nagłówka protokołu UDP

9.6. Protokoły warstwy aplikacji

W warstwie aplikacji modelu TCP/IP funkcjonuje wiele protokołów, umożliwiających świadczenie usług dla użytkowników. Podczas przesyłania danych przez sieci, dane mogą być przesyłane za pomocą różnych technologii. Dla autora listu poczty elektronicznej pracującego w warstwie aplikacji nie ma znaczenia, czy jego list przesyłany będzie do Internetu za pomocą modemu, neostrady, czy innej technologii. Dane mogą być przesyłane przy wykorzystaniu różnych mediów, np. najpierw z laptopa za pomocą fal radiowych, później kablem miedzianym, a w końcu łączem światłowodowym. Dzięki standaryzacji warstwa aplikacji jest niezależna od protokołów warstw niższych oraz używanych mediów transmisyjnych. Aplikacje mogą być wykorzystywane niezależnie od tego, czy pracujemy w sieci lokalnej, czy globalnej. Najczęściej używanymi protokołami warstwy aplikacji są:

- **FTP** (File Transfer Protocol) - do przesyłania plików w sieci,
- **HTTP** (Hypertext Transfer Protocol) - do pobierania stron WWW,
- **SMTP** (Simple Mail Transfer Protocol) - do wysyłania poczty elektronicznej,
- **POP3** (Post Office Protocol v 3) - do pobierania poczty elektronicznej,
- **IMAP** (Internet Message Access Protocol) - do pobierania poczty elektronicznej,
- **DNS** (Domain Name System) - do zamiany nazw domenowych na adresy IP,
- **TFTP** (Trivial File Transfer Protocol) - uproszczona wersja protokołu FTP wykorzystywana np. do instalacji systemów operacyjnych w urządzeniach sieciowych, takich jak routery lub przełączniki.

Większość z wymienionych wyżej protokołów obsługuje usługi umożliwiające wykonanie określonych zadań w sieci, np. wysłanie lub odebranie poczty elektronicznej, pobranie pliku lub strony WWW. Wyjątkiem jest usługa DNS.

System **DNS** to hierarchiczna usługa nazw przeznaczona dla hostów w sieci TCP/IP. Pozwala nadawać komputerom świadczącym pewne usługi w sieci nazwy domenowe i tłumaczy je na używane przez komputery adresy IP. Nazwy domenowe są wygodne dla użytkowników posługujących się nimi zamiast trudnych do zapamiętania adresów IP. Komputery potrafią operować wyłącznie na adresach IP, co wymaga mechanizmu tłumaczenia nazw na adresy. System DNS jest rozproszoną bazą danych obsługiwaną przez wiele serwerów, z których każdy posiada tylko informacje o domenie, którą zarządza, oraz o adresie serwera nadrzędnego. Na najwyższym poziomie znajdują się tzw. **główne serwery nazw** (root level servers), które znajdują się w Stanach Zjednoczonych i podłączone są do szybkich sieci szkieletowych Internetu. Przechowują one adresy serwerów nazw dla domen najwyższego poziomu, np. .com, .edu, .org, oraz domen krajowych, np. .pl, .de, .uk. Adresy serwerów głównych muszą być znane każdemu innemu serwerowi nazw. Wewnątrz każdej domeny można tworzyć tzw. subdomeny, np. wewnątrz domeny .pl utworzono wiele domen regionalnych jak [.waw.pl](#), [.lodz.pl](#) itp, oraz funkcjonalnych jak [.com.pl](#), [.gov.pl](#) lub [.org.pl](#), należących do firm, organizacji lub osób prywatnych.

Ogólne zasady przyznawania nazw domen i adresów IP nadzorują dwie instytucje - **IANA** (Internet Assigned Number Authority) i **ICANN** (The Internet Corporation for Assigned Names and Numbers). Instytucje te przekazują swoje uprawnienia na lokalne instytucje i firmy, np. w Polsce nadzór nad domeną .pl jako całością, oraz obsługą rejestrowania domen takich jak [.com.pl](#), [.biz.pl](#), [.org.pl](#),

[.net.pl](http://net.pl) oraz innych domen funkcjonalnych pełni **NASK** (Naukowa i Akademicka Sieć Komputerowa). Aby móc pracować w Internecie, komputer musi znać adresy IP serwerów DNS dla swojej domeny. Zazwyczaj dla każdej domeny utrzymywane są dwa niezależne serwery nazw, dzięki czemu w razie awarii lub zbyt dużego obciążenia **podstawowego serwera DNS** (primary name server) można korzystać z **serwera rezerwowego** (secondary name server).

9.7. Inne zestawy protokołów

Zestaw protokołów **IPX/SPX** (Internet Packet EXchange/Sequential Packet Exchange) firmy Novell bierze nazwę od swoich dwóch głównych protokołów - międzysieciowej wymiany pakietów **IPX** i sekwencyjnej wymiany pakietów **SPX**. Protokół IPX/SPX zyskał popularność jako protokół wykorzystywany w sieci Novell Netware. Netware był faktycznym standardem sieciowego systemu operacyjnego dla sieci lokalnych w latach 80. Protokół IPX przypomina IP; jest protokołem bezpołączeniowym, który nie wymaga ani nie zapewnia potwierdzenia każdego transmitowanego pakietu. Protokół IPX korzysta z SPX w zakresie porządkowania kolejności i innych usług połączeniowych warstwy 4. Protokół SPX jest protokołem połączeniowym i może być wykorzystywany do przesyłania danych między klientem a serwerem, dwoma serwerami lub dwoma klientami. SPX zapewnia niezawodność transmisjom IPX, zarządzając połączeniem i udostępniając sterowanie strumieniem danych, kontrolę błędów i porządkowanie kolejnych pakietów. Stos protokołów IPX/SPX obejmuje cztery warstwy funkcjonalne: dostępu do nośnika, łącza danych, Internetu i aplikacji. Głównym protokołem warstwy aplikacji jest **protokół rdzenia NetWare** (NCP). Protokół NCP można wykorzystać do drukowania, współdzielenia plików, poczty elektronicznej i dostępu do folderów.

Protokół NetBEUI (NetBIOS Extended User Interface) został opracowany przez IBM. Jest małym, ale wydajnym protokołem komunikacyjnym. Nie wymaga wprowadzania żadnych informacji podczas konfiguracji, a stacje wyszukują obecne w sieci komputery za pomocą komunikatów rozgłoszeniowych. Jego zastosowanie ogranicza się do sieci lokalnych, w których pracują komputery wykorzystujące systemy operacyjne firmy Microsoft. Protokół ten do identyfikowania komputerów w sieci używa ich nazw i nie umożliwia wyznaczania tras, domyślnie był stosowany w sieci Windows 3.11 i Windows 95.

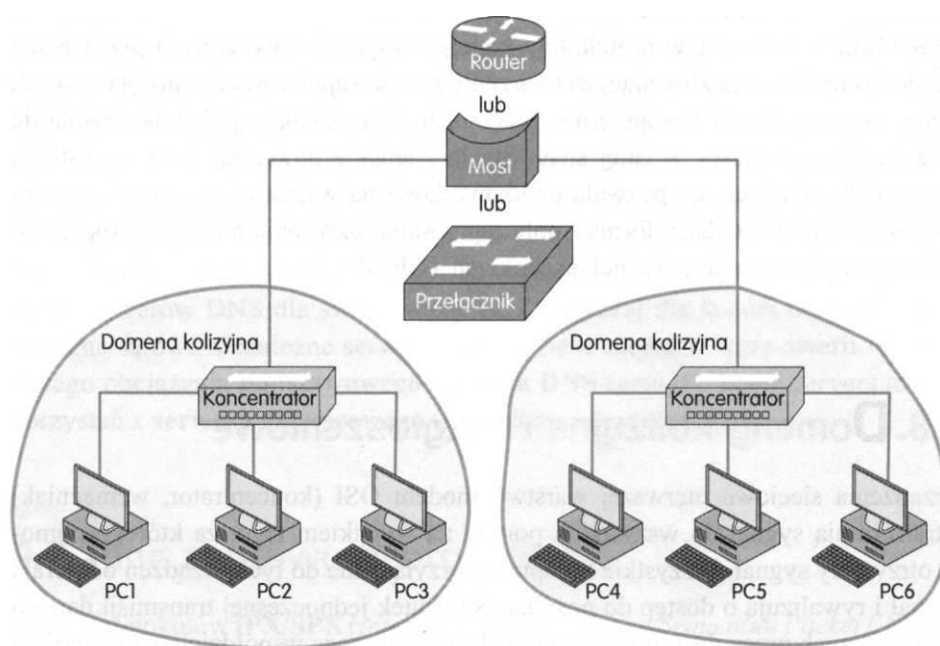
AppleTalk jest to zestaw protokołów komunikacyjnych stworzonych przez firmę Apple Computer, umożliwiających tworzenie sieci komputerowych i podstawowych usług sieciowych dla komputerów Macintosh. Urządzenia AppleTalk regularnie ogłaszają swoje nazwy w całej sieci. Stacje klienckie otrzymują listę wszystkich dostępnych urządzeń, co pozwala użytkownikowi na wybór urządzenia, z którym zamierza wymieniać dane. Firma Apple zaprzestała rozwijania protokołu AppleTalk i obecnie wykorzystuje w swoich produktach TCP/IP.

9.8. Domeny kolizyjne i rozgłoszeniowe

Urządzenia sieciowe pierwszej warstwy modelu OSI (koncentrator, wzmacniak) retransmitują sygnał do wszystkich portów za wyjątkiem tego, za którego pomocą otrzymały sygnał. Wszystkie komputery przyłączone do tych urządzeń odbierają sygnał i rywalizują o dostęp do nośnika. Na skutek

jednoczesnej transmisji danych realizowanych przez dwa lub więcej urządzeń za pomocą współdzielonego medium transmisyjnego może dojść do **kolizji**. Kolizje występujące w sieciach z dostępem do nośnika na zasadzie rywalizacji są zjawiskiem niekorzystnym, lecz nie możemy ich uniknąć. Obszar sieci, w którym może dojść do kolizji danych nadawanych przez różne stacje nazywamy **domeną kolizyjną** (Collision domain). W domenie kolizyjnej maksymalna liczba urządzeń wynosi 1024, lecz im jest ich więcej, tym prawdopodobieństwo wystąpienia kolizji jest większe. Ryzyko wystąpienia kolizji możemy ograniczyć przez odpowiednie zaprojektowanie sieci oraz stosowanie urządzeń ograniczających wielkość domen kolizyjnych, takich jak mosty, przełączniki lub routery.

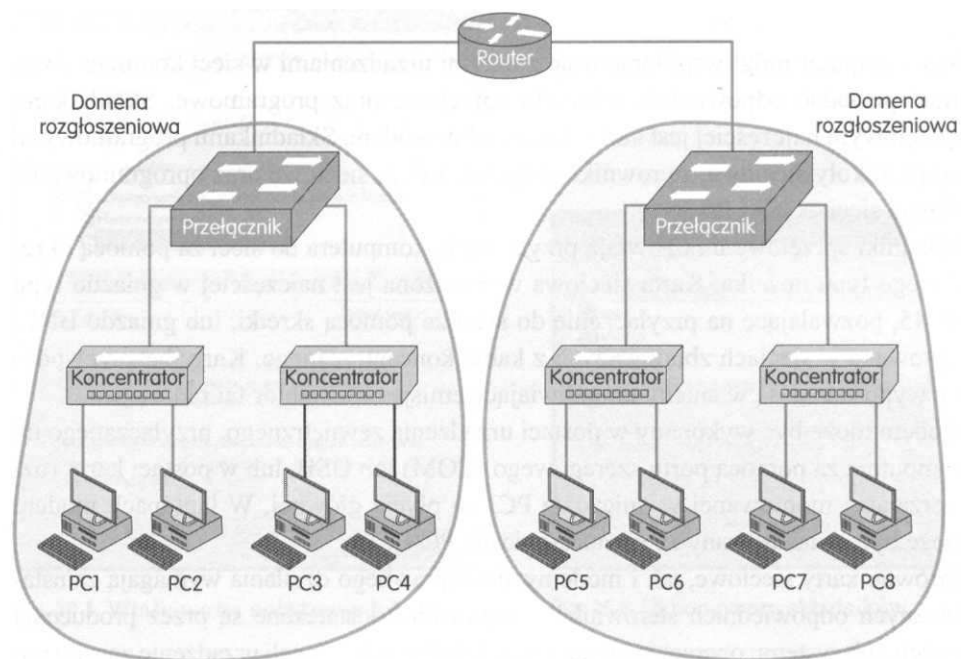
Efektywne projektowanie sieci prowadzi do organizacji struktury sieci w taki sposób, aby domeny kolizyjne były jak najmniejsze. Urządzenia, takie jak: przełącznik, most lub router, pozwalają na zmniejszenie obszaru domeny kolizyjnej. Transmisje realizowane pomiędzy urządzeniami w obrębie domeny kolizyjnej nie są przesyłane przez mosty, przełączniki i routery do innych domen. Jeżeli komputer PC1 (rys. 9.11) będzie przysyłał dane do komputera PC2, to most, przełącznik lub router stwierdzi, że oba komputery są przyłączone do tego samego portu (domeny kolizyjnej) i nie prześle ramki do drugiego portu. W tym samym czasie po drugiej stronie urządzenia może odbywać się inna transmisja, np. z komputera PC4 do PC5, co zwiększa wydajność sieci. Jeżeli transmisja odbywać się będzie pomiędzy komputerami znajdującymi się w różnych domenach kolizyjnych, np. PC1 i PC4, to ramka dotrze do wszystkich komputerów w obu domenach. Jakakolwiek inna transmisja w tym samym czasie w tych domenach spowoduje kolizję.



Rys. 9.11. Podział sieci na domeny kolizyjne

W sieci przesyłane mogą być również komunikaty rozgłoszeniowe. Obszar sieci, w którym następuje emisja komunikatu rozgłoszeniowego wysyłanego przez jedną stację do wszystkich innych, nazywamy **domeną rozgłoszeniową** (Broadcast domain). Urządzenia warstwy pierwszej (koncentrator i wzmacniak) oraz drugiej (most i przełącznik) przekazują ruch rozgłoszeniowy. Urządzenia te rozszerzają domenę rozgłoszeniową natomiast urządzenia warstwy trzeciej (router) ograniczają jej rozmiar. Rozmiar

domeny rozgłoszeniowej można ograniczyć również przez zdefiniowanie sieci wirtualnych VLAN (Virtual Local Area Network). Komunikacja między sieciami wirtualnymi musi się odbywać za pośrednictwem routera. Komunikaty rozgłoszeniowe wysyłane przez komputer, np. PC1, będą docierać tylko do komputerów PC2, PC3 i PC4, przesyłanie ich do pozostałych komputerów w sieci zostanie zablokowane przez router (rys. 9.12).



Rys. 9.12. Podział sieci na domeny rozgłoszeniowe