Moduł 10. Podstawy routingu i działanie sieci

Protokół IP jest najważniejszym protokołem routowanym używanym w Internecie. Zastosowanie adresowania IP pozwala na przesyłanie pakietów ze źródła do celu przy użyciu najlepszej dostępnej ścieżki. Propagacja pakietów, zmiany enkapsulacji, protokoły zorientowane połączeniowo i bezpołączeniowe są równie ważne dla zagwarantowania właściwego przesyłania danych do celu. W tym module dokonano przeglądu wszystkich wymienionych funkcji.

Dla osób poznających zagadnienia sieciowe różnica pomiędzy protokołami routującymi (protokołami routingu) a protokołami routowanymi stanowi źródło częstych pomyłek. Wyrazy te brzmią podobnie, ale mają całkowicie różne znaczenia. W module tym przedstawione zostały także protokoły routingu, które umożliwiają routerom tworzenie tablic pozwalających określić najlepszą ścieżkę do dowolnego hosta w Internecie.

Nie ma dwóch takich samych organizacji na świecie. Co więcej, system adresów podzielonych na trzy klasy (A, B i C) nie jest odpowiedni dla wszystkich organizacji. Jednakże system adresowania z podziałem na klasy pozwala na pewną elastyczność polegającą na możliwości tworzenia podsieci. Zastosowanie podsieci umożliwia administratorom sieci określenie rozmiarów fragmentów sieci, na których będą operować. Po ustaleniu podziału sieci maska podsieci może być użyta do określenia położenia każdego urządzenia w sieci.

10.1 Protokół routowany

10.1.1 Protokoły routowane

Protokół jest zbiorem reguł określających sposoby wzajemnej komunikacji komputerów w sieci. Komputery porozumiewają się ze sobą poprzez wymienianie wiadomości zawierających dane. Aby komputery mogły przyjąć i przetworzyć te wiadomości, musi być zdefiniowany sposób ich interpretacji. Przykłady wiadomości obejmują te, które ustanawiają połączenia ze zdalnym komputerem, wiadomości e-mail oraz pliki przesyłane przez sieć.

Protokół opisuje:

- wymagany format wiadomości;
- sposób, w jaki komputery muszą wymieniać wiadomość w kontekście danej operacji.

Zastosowanie protokołu routowanego pozwala na przesyłanie przez router danych między węzłami znajdującymi się w różnych sieciach. Żeby protokół mógł być routowany, musi umożliwiać przydział numeru sieci i numeru hosta każdemu indywidualnemu urządzeniu. Niektóre protokoły, takie jak IPX, wymagają tylko numeru sieci, ponieważ używają one adresu MAC jako numeru hosta. Inne protokoły, np. protokół IP, wymagają kompletnego adresu składającego się z części odpowiadającej sieci oraz hostowi. Aby rozróżnienie tych dwóch części było możliwe, protokoły te wymagają również maski sieci. Adres sieci jest uzyskiwany przez obliczenie iloczynu logicznego adresu i maski sieci.

Maska sieci jest stosowana po to, by umożliwić traktowanie grup następujących po sobie adresów IP jako pojedynczej części. Gdyby nie możliwość grupowania, każdy host musiałby być odwzorowany oddzielnie do operacji routingu. Nie byłoby to możliwe przy uwzględnieniu liczby hostów znajdujących się w Internecie, która zgodnie z danymi Internet Software Consortium wynosi około 233 101 500.

10.1.2 Protokół IP jako protokół routowany

Protokół IP (ang. *Internet Protocol*) jest najszerzej używaną implementacją metody hierarchicznego adresowania w sieci. Protokół IP jest protokołem bezpołączeniowym, zawodnym i realizuje dostarczanie danych przy użyciu dostępnych możliwości. Pojęcie „bezpołączeniowy” oznacza, że nie nawiązuje się wydzielonego połączenia przed rozpoczęciem transmisji, jak dzieje się to w wypadku rozmowy telefonicznej. Protokół IP określa najefektywniejszą trasę na podstawie protokołu routingu. Określenia zawodny i realizujący dostarczanie danych przy użyciu dostępnych możliwości nie implikują, że system jest zawodny i nie pracuje dobrze, ale oznaczają, że protokół IP nie dokonuje sprawdzenia, czy dane dotarły do celu. Funkcję tę, jeśli jest wymagana, pełnią protokoły wyższych warstw.

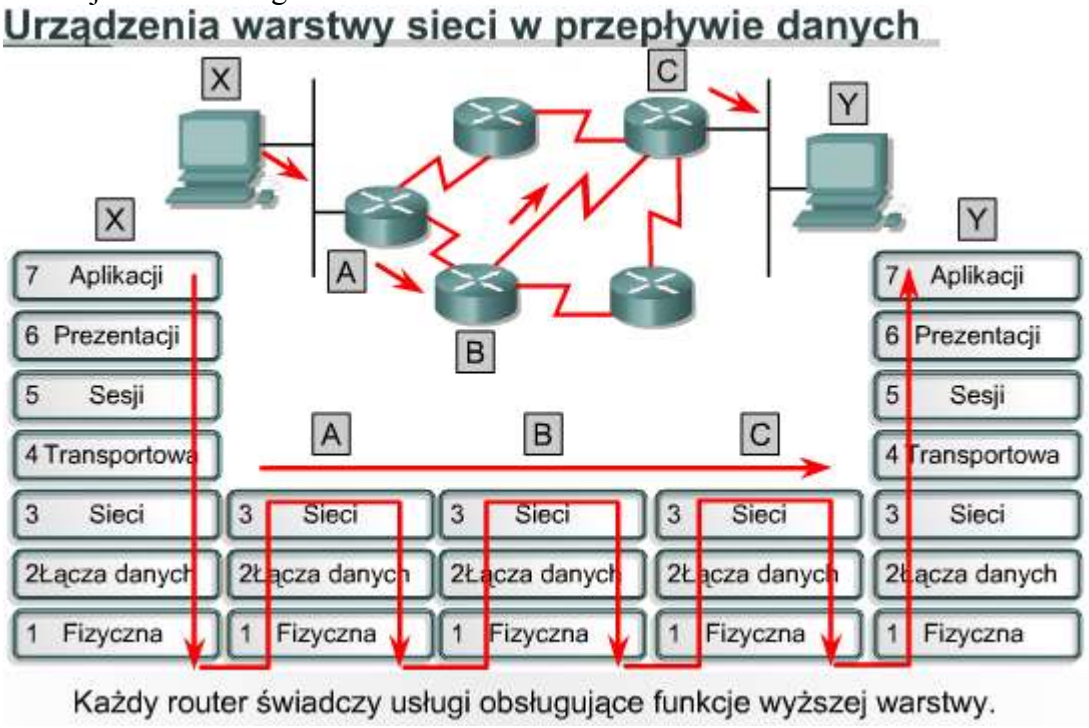
W trakcie przepływu danych przez kolejne warstwy OSI są one przetwarzane na każdym z etapów. W warstwie sieciowej dane podlegają enkapsulacji i przyjmują formę pakietów, zwanych także datagramami. Protokół IP określa zawartość nagłówka pakietu IP, który zawiera dane adresowe oraz inne informacje sterujące, ale nie obejmuje danych właściwych. Protokół IP przyjmuje wszystkie dane przekazywane z wyższych warstw.

10.1.3 Propagacja pakietów oraz przełączanie wewnątrz routera

W trakcie przesyłania pakietów w intersieci do miejsca docelowego nagłówki i stopki warstwy 2 są usuwane i zastępowane w każdym urządzeniu warstwy 3. Dzieje się tak dlatego, że jednostki danych warstwy 2 — ramki — przeznaczone są do adresowania lokalnego. Jednostki danych warstwy 3 — pakiety — przeznaczone są do adresowania typu end-to-end.

Ramki Ethernet warstwy 2 są przystosowane do działania w domenie rozgłoszeniowej z wykorzystaniem adresu MAC wbudowanego w urządzenie. Inne typy ramek warstwy 2 stosowane są w szeregowych łączach protokołu PPP (Point-to-Point Protocol) oraz w połączeniach protokołu Frame Relay, gdzie wykorzystywane są inne metody adresowania warstwy 2. Bez względu na użyty typ adresowania warstwy 2 format ramki jest zaprojektowany do

funkcjonowania w ramach domeny rozgłoszeniowej tej warstwy, gdyż po przejściu danych przez urządzenie warstwy 3 informacje warstwy 2 ulegają zmianie.
Po odebraniu ramki w interfejsie routera wyodrębniany jest docelowy adres MAC. Następnie odbywa się sprawdzenie, czy ramka jest adresowana bezpośrednio do interfejsu routera lub jest ramką rozgłoszeniową. W obu wypadkach ramka jest akceptowana. W przeciwnym razie ramka jest odrzucana, ponieważ jest kierowana do innego urządzenia w domenie kolizyjnej. Stopka zaakceptowanej ramki zawiera pole cyklicznej kontroli nadmiarowej (CRC), którego wartość jest wyodrębniana i porównywana z wartością obliczoną w celu potwierdzenia, że dane ramki są wolne od błędów. Jeśli weryfikacja nie powiedzie się, ramka jest odrzucana. Jeśli rezultat sprawdzenia jest pozytywny, nagłówek i stopka ramki są usuwane, a pakiet jest przekazywany do warstwy 3. Tam następuje sprawdzenie, czy jest on kierowany do routera, czy też ma być przesłany do innego urządzenia w intersieci. Jeśli docelowy adres IP odpowiada jednemu z portów routera, nagłówek warstwy 3 jest usuwany i dane są przekazywane do warstwy 4. Jeśli pakiet ma zostać przesłany, docelowy adres IP jest porównywany z adresami znajdującymi się w tablicy routingu. Jeśli odpowiadający adres zostanie odnaleziony albo istnieje trasa domyślna, pakiet będzie wysłany do interfejsu określonego w tablicy routingu. Gdy pakiet jest przełączany do interfejsu wyjściowego, zostaje uzupełniony o odpowiedni nagłówek oraz stopkę zawierający nową wartość cyklicznej kontroli nadmiarowej (CRC). Ramka jest następnie przesyłana do kolejnej domeny rozgłoszeniowej prowadzącej do miejsca docelowego.



10.1.4 Protokół IP (ang. Internet Protocol)

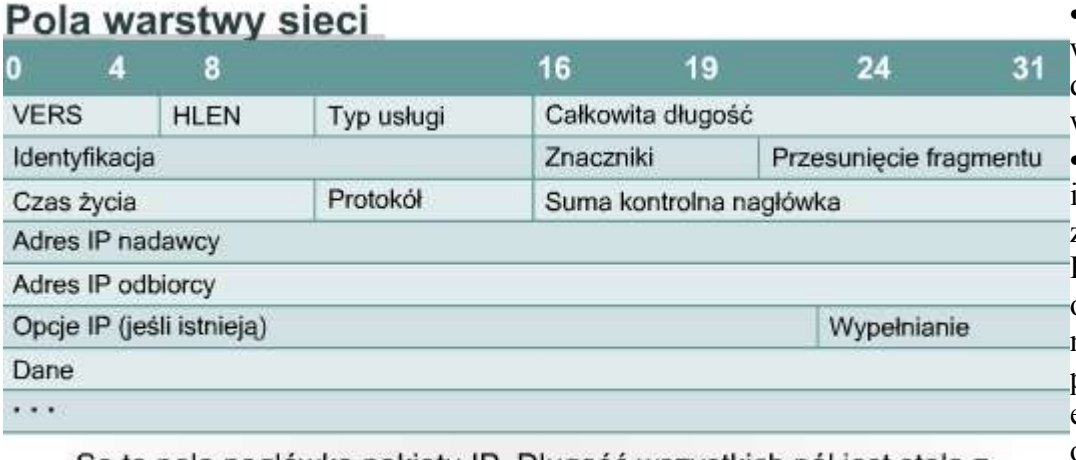
Istnieją dwa rodzaje usług dostarczania danych: zorientowane połączeniowo i bezpołączeniowe. Te dwa typy usług zapewniają właściwe dostarczanie typu end-to-end (czyli pomiędzy punktami końcowymi) danych w intersieci.
W większości sieci używany jest bezpołączeniowy system dostarczania. Różne pakiety mogą podążać różnymi ścieżkami w sieci, ale po osiągnięciu celu są one ponownie składane. W systemie bezpołączeniowym przed wysłaniem pakietu nie nawiązuje się kontaktu z punktem docelowym. Dobrym porównaniem dla systemu bezpołączeniowego jest system pocztowy. Przed nadaniem przesyłki nikt nie kontaktuje się z odbiorcą, żeby sprawdzić, czy ją przyjmie. Także nadający nie wie, czy list dotarł do celu.
W systemach zorientowanych połączeniowo przed rozpoczęciem przesyłania danych pomiędzy nadawcą i odbiorcą nawiązywane jest połączenie. Przykładem sieci zorientowanej połączeniowo jest systemem telefoniczny. Dzwoniący wybiera numer, nawiązywane jest połączenie i dochodzi do komunikacji.

Bezpołączeniowe procesy sieciowe są często zwane procesami z przełączaniem pakietów. W trakcie przesyłania pakietów ze źródła do celu mogą być one przełączane do różnych ścieżek i mogą osiągnąć miejsce docelowe w innej kolejności. Każdy pakiet zawiera informacje, takie jak adres docelowy i numer kolejny (sekwencyjny), które pozwalają skoordynować go z innymi dochodzącymi pakietami. Pakiety te są zatem składane w odpowiedniej kolejności już po dotarciu do celu. Urządzenia mogą ustalać ścieżkę dla każdego pakietu z osobna przy uwzględnieniu różnych kryteriów. Niektóre kryteria, takie jak dostępne pasmo, mogą więc być różne dla każdego pakietu.
Zorientowane połączeniowo procesy sieciowe często są zwane procesami z komutacją łączy. Przed rozpoczęciem przesyłania danych nawiązywane jest połączenie z odbiorcą, dopiero potem rozpoczyna się transfer danych. Wszystkie pakiety poruszają się jeden po drugim w ramach tego samego obwodu fizycznego lub wirtualnego. Internet jest olbrzymią siecią bezpołączeniową, w której większość pakietów jest dostarczana przy użyciu protokołu IP. Protokół TCP uzupełnia protokół IP o zorientowane połączeniowo usługi warstwy 4 z gwarancją niezawodności.

10.1.5 Budowa pakietu IP

Pakiety IP składają się z danych z wyższych warstw oraz nagłówka IP. Nagłówek IP zawiera następujące pola:

- **Wersja** — określa format nagłówka pakietu IP. 4-bitowe pole wersji zawiera liczbę 4, jeśli jest to pakiet IPv4, a liczbę 6, jeśli jest to pakiet IPv6. Pole to nie jest jednak stosowane do rozróżniania pomiędzy pakietami IPv4 a IPv6 - taką rolę pełni pole typu protokołu obecne w ramce warstwy drugiej.
- **Długość nagłówka IP (HLEN)** — określa długość nagłówka datagramu jako wielokrotność słów 32-bitowych. Jest to całkowita długość wszystkich informacji znajdujących się w nagłówku, obejmująca dwa pola nagłówka o zmiennych długościach.
- **Typ usługi*(TOS, ang. Type-of-service)*** — określa poziom ważności, który został przypisany przez protokół wyższej warstwy; osiem bitów.
- **Całkowita długość** — określa długość całego pakietu w bajtach z uwzględnieniem danych i nagłówka; 16 bitów. Aby uzyskać długość pola danych, od długości całkowitej należy odjąć wartość HLEN.
- **Identyfikacja** — zawiera liczbę całkowitą identyfikującą bieżący datagram; 16 bitów. Jest to numer sekwencyjny.
- **Flagi** — pole o długości trzech bitów, w którym dwa mniej znaczące bity sterują fragmentacją. Jeden bit określa, czy pakiet może zostać podzielony na fragmenty, a drugi służy do oznaczenia ostatniego pakietu w serii podzielonych pakietów.
- **Przesunięcie fragmentu** — pole pomocne przy składaniu fragmentów datagramu; 13 bitów. Pole to pozwala na zakończenie poprzedniego pola na granicy 16 bitów.
- **Czas życia (TTL, Time To Live)** — pole określające liczbę przeskoków, które może wykonać pakiet. Liczba ta jest zmniejszana o jeden za każdym razem, gdy pakiet przechodzi przez router. Gdy licznik osiągnie wartość zero, pakiet jest odrzucany. Zapobiega to przesyłaniu pakietu w nieskończonej pętli.
- **Protokół** — pole wskazujące, który protokół wyższej warstwy, taki jak TCP lub UDP, odbiera pakiety przychodzące po zakończeniu przetwarzania IP; osiem bitów.
- **Suma kontrolna nagłówka** — pole pomagające zapewnić integralność nagłówka; 16 bitów.
- **Adres nadawcy** — pole określające adres IP węzła nadawczego; 32 bity.
- **Adres odbiorcy** — pole określające adres IP węzła odbiorczego; 32 bity.
- **Opcje** — pole umożliwiające protokołowi IP obsługę różnych opcji, takich jak funkcje zabezpieczeń; zmienna długość.



Są to pola nagłówka pakietu IP. Długość wszystkich pól jest stała z wyjątkiem pól opcji IP oraz uzupełniania

- **Wypełnianie** — zera dodane w celu zagwarantowania, że długość nagłówka jest wielokrotnością 32 bitów.
- **Dane** — pole zawierające informacje wyższych warstw; zmienna długość do 64 kB.

Podczas gdy adresy nadawcy i odbiorcy są istotne, inne pola nagłówka sprawiają, że protokół IP jest bardzo elastyczny. Pola nagłówka określają adresy nadawcy oraz odbiorcy pakietu, a także

długość przenoszonego komunikatu. Ponadto w nagłówku IP może być zawarta informacja dotycząca routingu, która może być długa i mieć złożoną strukturę.

10.2 Protokoły routingu IP

10.2.1 Przegląd routingu

Routing jest funkcją realizowaną w warstwie 3 modelu (SIECI) OSI. Routing jest hierarchicznym schematem organizacyjnym pozwalającym na łączenie pojedynczych adresów w grupy. Pojedyncze adresy traktowane są jak jedna całość do momentu, gdy wymagany jest adres odbiorcy w celu końcowego dostarczenia danych. Routing jest procesem znajdowania najwydajniejszej ścieżki łączącej dwa urządzenia. Podstawowym urządzeniem wykonującym proces routingu jest router.

Poniżej wymieniono dwie podstawowe funkcje pełnione przez router:

- Routery muszą utrzymywać tablice routingu oraz zapewnić informowanie pozostałych routerów o zmianach topologii sieci. Funkcja ta, mająca na celu wymianę informacji dotyczących sieci z innymi routerami, wykonywana jest przy użyciu protokołów routingu.
- Po odebraniu pakietu router musi za pomocą tablicy routingu określić miejsce, do którego pakiet powinien zostać wysłany. Router przełącza pakiety, kierując je do odpowiedniego interfejsu, dodaje niezbędne informacje dotyczące podziału na ramki z uwzględnieniem tego interfejsu, a następnie wysyła pakiety.

Router jest urządzeniem warstwy sieci, które określa optymalną ścieżkę przesyłania ruchu sieciowego przy wykorzystaniu jednej lub kilku metryk routingu. Metryki routingu są wartościami służącymi do określania przewagi jednej ścieżki nad inną. Protokoły routingu korzystają ze zróżnicowanych kombinacji metryk w celu dokonania wyboru najlepszej ścieżki.

Routery służą do łączenia segmentów sieci lub całych sieci. Routery przesyłają ramki danych pomiędzy sieciami na podstawie informacji warstwy 3. Routery podejmują decyzje logiczne dotyczące wyboru najlepszej ścieżki transmisji danych. Następnie pakiety kierowane są na odpowiedni port wyjściowy, gdzie przeprowadzany jest proces enkapsulacji. Procesy enkapsulacji i dekapsulacji zachodzą za każdym razem, gdy pakiet jest przesyłany przez router. Router musi zdekapsułkować ramkę warstwy drugiej, aby uzyskać dostęp do nagłówka warstwy trzeciej i odczytać odpowiadający tej warstwie adres. Jak pokazano na rysunku , proces przesyłania danych pomiędzy urządzeniami końcowymi obejmuje enkapsulację i dekapsulację na poziomie wszystkich siedmiu warstw modelu OSI. Podczas enkapsulacji strumień danych jest dzielony na segmenty, dodawane są odpowiednie nagłówki i stopki, po czym dane zostają przesłane. Dekapsulacja jest procesem odwrotnym. Nagłówki i stopki są usuwane, a następnie tworzony jest jednolity strumień.

W kursie tym skupiono uwagę na najpowszechniej stosowanym protokole routowanym — protokole IP. Innymi protokołami routowanymi są między innymi protokoły IPX/SPX i AppleTalk. Protokoły te zapewniają obsługę warstwy 3. Protokoły nieroutowane nie obsługują warstwy 3. Najbardziej popularnym protokołem nieroutowanym jest protokół NetBEUI. Protokół NetBEUI jest nieskomplikowanym, szybkim i wydajnym protokołem, którego funkcjonalność ograniczona jest do dostarczania ramek wewnątrz pojedynczego segmentu.

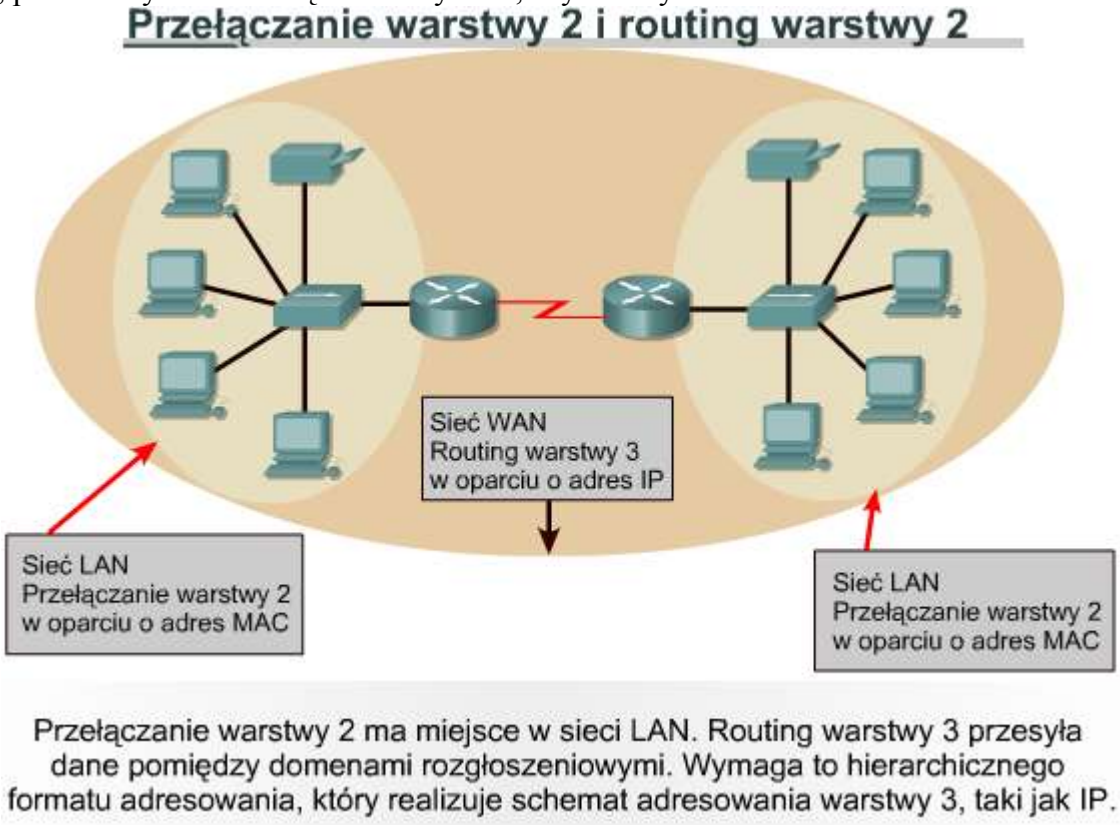
10.2.2 Routing a przełączanie

Routing jest często porównywany z przełączaniem. Niedoświadczonemu obserwatorowi może wydawać się, że routing i przełączanie pełnią tę samą funkcję. Główna różnica polega na tym, że przełączanie odbywa się w 2

warstwie modelu OSI — w warstwie łącza danych, natomiast routing jest prowadzony w warstwie 3. Oznacza to, że routing i przełączanie wykorzystują różne informacje w procesie przesyłania danych ze źródła do celu.

Relacja pomiędzy przełączaniem i routingiem jest taka sama jak między lokalnymi i międzymiastowymi rozmowami telefonicznymi. Rozmowa lokalna prowadzona w obrębie tego samego numeru kierunkowego obsługiwana jest przez centralę lokalną. Jednakże centrala lokalna może przechowywać informacje dotyczące jedynie numerów lokalnych w swoim zasięgu. Nie może ona obsługiwać połączeń ze wszystkimi numerami telefonicznymi na świecie. Gdy centrala otrzymuje żądanie połączenia z telefonem spoza obsługiwanego numeru kierunkowego, przełącza je do centrali wyższego poziomu, która rozpoznaje numery kierunkowe. Centrala wyższego poziomu przełącza rozmowę, tak aby została przekazana do centrali lokalnej odpowiadającej strefie wybranego numeru kierunkowego.

Router pełni funkcję zbliżoną do centrali wyższego poziomu opisanej w przytoczonym przykładzie. Na rysunku pokazane zostały tablice ARP wykorzystywane do adresowania w warstwie 2 (adresy MAC) oraz tablice routingu wykorzystywane do adresowania w warstwie 3 (adresy IP). Każdy interfejs komputera oraz routera utrzymuje własną tablicę ARP dla celów komunikacji w warstwie 2. Tablica ARP danego urządzenia ma zastosowanie tylko w domenie rozgłoszeniowej, do której jest ono podłączone. Routery przechowują dodatkowo tablicę routingu pozwalającą na przesyłanie danych poza domenę rozgłoszeniową. Każda pozycja tablicy ARP zawiera parę adresów IP-MAC. Adresy MAC na Rysunku są zastąpione akronimem MAC, gdyż rzeczywiste adresy MAC są zbyt długie i nie zmieściłyby się na rysunku. Tablice routingu przechowują dodatkowo informację na temat sposobu zapamiętania danej trasy (w tym przypadku — połączonej bezpośrednio [C] albo odnalezionej z wykorzystaniem protokołu RIP [R]), adresy IP osiągalnych sieci, liczbę przeskoków lub odległości do tych sieci oraz interfejs, przez który dane muszą zostać wysłane, aby dotarły do celu.



Przełączanie warstwy 2 ma miejsce w sieci LAN. Routing warstwy 3 przesyła dane pomiędzy domenami rozgłoszeniowymi. Wymaga to hierarchicznego formatu adresowania, który realizuje schemat adresowania warstwy 3, taki jak IP.

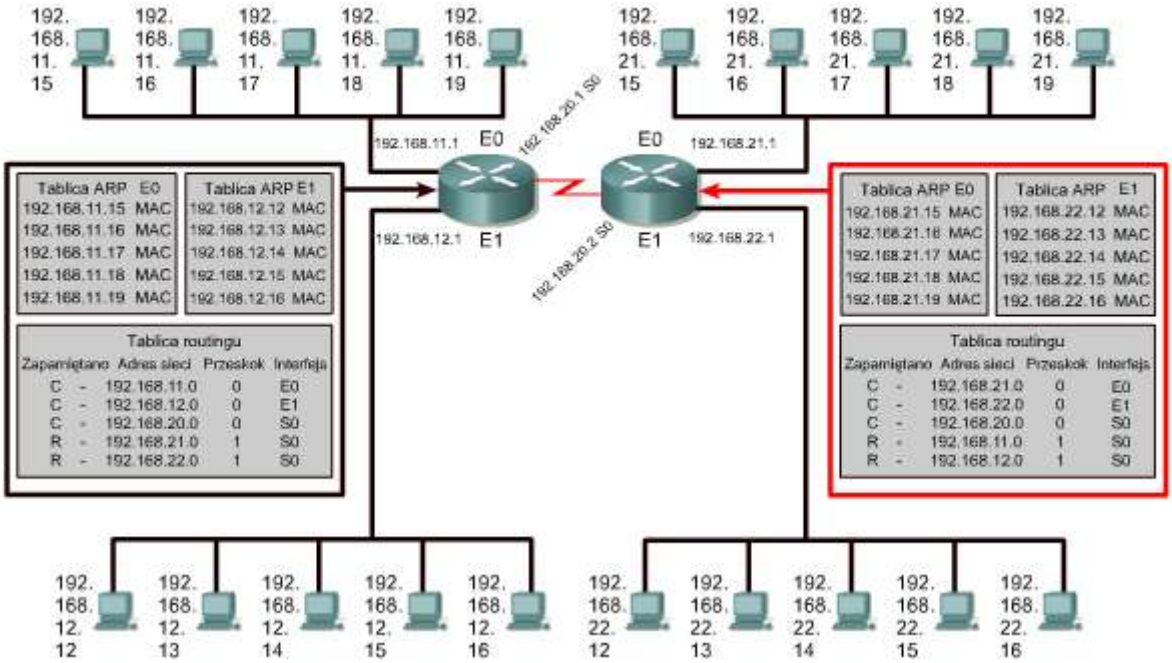
Przełącznik warstwy 2 tworzy swoją tablicę przekazywania (*forwarding table*), zawierającą adresy MAC. Kiedy host ma dane do wysłania na adres IP inny niż lokalny, wysyła ramkę do najbliższego routera, zwanego także jego bramą domyślną. Adres MAC routera jest używany przez hosta jako adres MAC odbiorcy.
Przełącznik łączy segmenty należące do tej samej sieci lub podsieci logicznej. Jeśli przełącznik ma przesłać ramkę do hosta nie należącego do sieci lokalnej, przekazuje ją na podstawie adresu MAC odbiorcy do routera. Router dokonuje analizy adresu odbiorcy warstwy 3 w celu podjęcia decyzji dotyczącej przesłania pakietu. Host X zna adres IP routera, ponieważ w jego konfiguracji IP jest zawarty adres IP bramy domyślnej.
Podobne jak przełącznik przechowuje tablicę znanych adresów MAC, router przechowuje tablicę adresów IP zwaną tablicą routingu. Adresy MAC nie są logicznie zorganizowane, natomiast adresy IP tworzą strukturę hierarchiczną. Przełącznik jest w stanie obsługiwać umiarkowaną liczbę niezorganizowanych adresów MAC, gdyż musi on przeszukiwać tablicę tylko w celu odnalezienia adresów należących do tego samego segmentu. Routery muszą obsłużyć większą liczbę adresów. Dlatego routery wymagają zastosowania zorganizowanego systemu adresowania z możliwością grupowania podobnych adresów i traktowania ich jak pojedynczej jednostki sieciowej do momentu, aż dane nie dotrą do segmentu docelowego. Jeśli adresy IP nie miałyby zorganizowanej struktury, Internet po prostu nie mógłby funkcjonować. Taką sytuację można porównać do biblioteki zawierającej miliony pojedynczych zadrukowanych stron ułożonych na ogromnym stosie. Cały ten materiał jest bezużyteczny, gdyż nie jest możliwe odnalezienie pojedynczego dokumentu. Gdy strony są zorganizowane w formie książek, możliwa jest identyfikacja każdej strony, a kiedy książki są także uporządkowane w formie indeksu, odnalezienie i wykorzystanie informacji staje się dużo łatwiejsze.
Kolejną różnicą pomiędzy sieciami przełączanymi a sieciami routowanymi jest to, że sieci przełączane nie blokują rozgłoszeń. W rezultacie przełączniki mogą zostać przeciążone przez burze rozgłoszeń. Routery blokują rozgłoszenia sieci LAN, więc burze rozgłoszeń obejmują tylko macierzyste domeny rozgłoszeniowe. Dzięki blokowaniu rozgłoszeń routery zapewniają wyższy poziom bezpieczeństwa i kontroli szerokości pasma niż przełączniki.

Porównanie cech routera i przełącznika

Kryteria	Router	Przełącznik
Szybkość	Wolniejszy	Szybszy
Warstwa OSI	Warstwa 3	Warstwa 2
Użyte adresowanie	IP	MAC
Pakiety rozgłoszeniowe	Blokowane	Przekazywanie
Bezpieczeństwo	Wyższe	Niższe

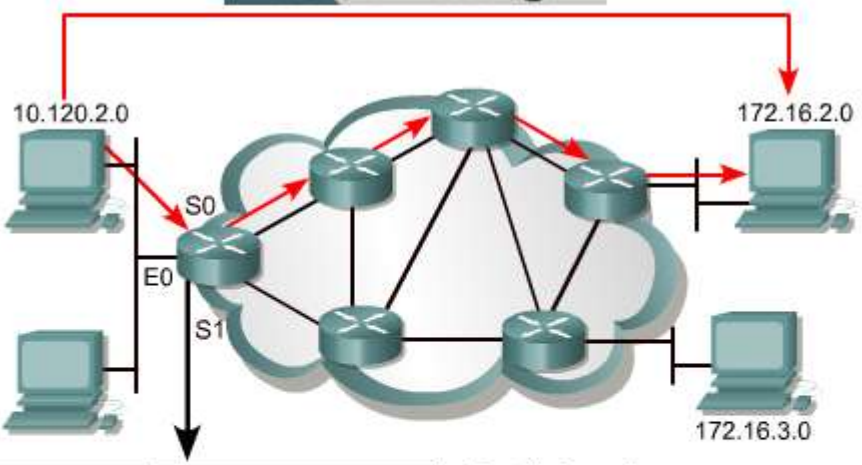
Szybkość i bezpieczeństwo stanowią względne porównanie i zależą od konfiguracji urządzenia.

Tablice ARP i tablice routingu



10.2.3 Protokoły routowane a protokoły routingu

Protokół routingu



Protokół sieciowy	Sieć docelowa	Interfejs wyjściowy
Podłączony	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Protokoły routingu są używane pomiędzy routerami do określania ścieżek i utrzymywania tablic routingu

Po określeniu ścieżki router może routować pakiety

Protokół routingu = RIP, IGRP

Protokoły wykorzystywane w warstwie sieci w celu transmisji danych pomiędzy hostami za pośrednictwem routera nazywane są protokołami routowanymi. Protokoły routowane zapewniają transport danych przez sieć. Protokoły routingu umożliwiają routerowi dokonanie wyboru najlepszej ścieżki prowadzącej ze źródła do celu.

Do funkcji protokołów routowanych należą między innymi:

- Zastosowanie dowolnego zestawu protokołów dostarczającego wystarczającej ilości informacji w adresie warstwy sieci, aby umożliwić routerowi przesłanie danych do następnego urządzenia, a w konsekwencji do celu.
- Zdefiniowanie formatu i sposobu wykorzystania pól wewnątrz pakietu.

Przykładami protokołów routowanych są: protokół IPX (ang. *Internetwork Packet Exchange*) stosowany w rozwiązaniach firmy Novell oraz protokół IP (ang. *Internet Protocol*). Do grupy tej należą również protokoły DECnet, AppleTalk, Banyan VINES oraz XNS (ang. *Xerox Network Systems*). Routery wykorzystują protokoły routingu w celu wymiany informacji i tablic routingu. Innymi słowy, protokoły routingu umożliwiają routerom prowadzenie routingu w ramach protokołów routowanych.

Do funkcji protokołów routingu należą między innymi:

- Dostarczanie procesów pozwalających na współdzielenie informacji o trasach.
- Umożliwienie komunikacji między routerami w celu aktualizacji i utrzymywania tablic routingu.

Przykładami protokołów routingu obsługujących protokół IP są protokoły RIP (ang. *Routing Information Protocol*), IGRP (ang. *Interior Gateway Routing Protocol*), OSPF (ang. *Open Shortest Path First*), BGP (ang. *Border Gateway Protocol*) oraz EIGRP (ang. *Enhanced IGRP*).

10.2.4 Określanie ścieżki

Określanie ścieżki odbywa się na poziomie warstwy sieci. Funkcja określania ścieżki pozwala routerowi na porównanie adresu odbiorcy z dostępnymi trasami zawartymi w tablicy routingu i na wybór najlepszej ścieżki. Routery mogą zdobyć informacje na temat dostępnych tras za pomocą routingu statycznego lub dynamicznego. Trasy skonfigurowane ręcznie przez administratorów sieci określane są mianem tras statycznych. Trasy, o których informacje zostały otrzymane od innych routerów za pomocą protokołu routingu, określane są mianem tras dynamicznych.

Routery wykorzystują proces określania ścieżki w celu podjęcia decyzji dotyczącej portu, przez który należy wysłać nadchodzący pakiet, aby dotarł do swego adresata. Proces ten nazywany jest także routingiem pakietów. Każdy router na drodze przesyłanego pakietu nazywany jest przeskokiem. Liczba przeskoków jest długością drogi. Proces określania ścieżki może być porównany do prowadzenia samochodu z jednego miejsca w mieście do innego. Kierowca posiada mapę pokazującą możliwe drogi do punktu docelowego, tak jak router zawiera tablicę routingu. Kierowca pokonuje kolejne skrzyżowania, tak jak pakiet jest przekazywany między routerami w trakcie pojedynczego przeskoku. Na każdym skrzyżowaniu kierowca może wybrać trasę, skręcając w lewo lub w prawo bądź jadąc prosto. Podobnie router określa, przez który port wyjściowy należy wysłać pakiet.

Na decyzje podejmowane przez kierowcę mają wpływ takie czynniki, jak ruch na drodze, ograniczenia prędkości, liczba pasów ruchu, opłaty za przejazd oraz dostępność trasy. Czasami szybciej jedzie się dłuższą trasą, wybierając węższą, mniej uczęszczaną boczną uliczkę zamiast zatłoczonej autostrady. Podobnie decyzje podejmowane przez routery bazują na obciążeniu, szerokości pasma, opóźnieniu, koszcie i niezawodności łącza sieci.

Proces opisany poniżej wykonywany jest podczas określania trasy dla każdego pakietu:

- Router porównuje adres IP z otrzymanego pakietu ze swoimi tablicami IP.
- Z pakietu pobierany jest adres docelowy.
- W odniesieniu do adresu docelowego stosowana jest maska pierwszego wpisu z tablicy routingu.
- Zamaskowany adres docelowy i wpis w tablicy routingu są ze sobą porównywane.
- Jeżeli wartości te są równe, pakiet jest przesyłany do portu odpowiadającego wpisowi w tablicy.
- W przypadku braku zgodności sprawdzany jest kolejny wpis w tablicy.
- Jeżeli pakietowi nie odpowiada żaden wpis z tablicy routingu, router sprawdza, czy została ustawiona trasa domyślna.
- Jeśli tak, pakiet zostaje przesłany przez przypisany jej port. Trasa domyślna to trasa skonfigurowana przez administratora sieci, którą wysyłane są pakiety, gdy nie zostanie znaleziony odpowiadający im wpis w tablicy routingu.
- Jeśli nie istnieje domyślna trasa, pakiet jest odrzucany. Zazwyczaj do nadawcy wysyłana jest wiadomość zwrotna informująca, że odnalezienie punktu docelowego było niemożliwe

10.2.5 Tablice routingu

Routery wykorzystują protokoły routingu w celu tworzenia i utrzymywania tablic routingu zawierających informacje dotyczące tras. Wspomaga to proces określania ścieżki. Protokoły routingu powodują wypełnienie tablic routingu różnymi informacjami dotyczącymi tras. Informacje te różnią się w zależności od użytego protokołu. Tablice routingu zawierają informacje niezbędne do przesyłania pakietów danych przez połączone ze sobą sieci. Urządzenia warstwy 3 łączą domeny rozgłoszeniowe lub sieci LAN. Aby przesyłanie danych mogło się odbywać, wymagany jest hierarchiczny schemat adresowania.

Routery rejestrują potrzebne informacje w swoich tablicach routingu, w tym następujące dane:

- **Typ protokołu** — typ protokołu routingu, na podstawie którego został utworzony wpis w tablicy.
- **Odniesienia do punktu docelowego/następnego przeskoku** — odniesienia informujące router o tym, że punkt docelowy jest połączony z routerem bezpośrednio lub że może on zostać osiągnięty poprzez kolejny router, zwany następnym przeskokiem na drodze do punktu docelowego. Kiedy router otrzymuje pakiet, sprawdza adres docelowy, a następnie próbuje odszukać odpowiadający mu wpis w tablicy routingu.
- **Metryki routingu** — różne protokoły routingu używają różnych metryk routingu. Metryki routingu służą do określania zasadności wyboru danej trasy. Na przykład protokół RIP (ang. *Routing Information Protocol*) wykorzystuje liczbę przeskoków jako jedyną metrykę routingu. W protokole IGRP (ang. *Interior Gateway*

Routing Protocol) w celu obliczenia złożonej metryki używana jest kombinacja metryk szerokości pasma, obciążenia, opóźnienia i niezawodności.
- **Interfejsy wyjściowe** — interfejsy, przez które należy wysłać dane w celu dostarczenia ich do punktu docelowego.

Aby utrzymać tablice routingu, routery komunikują się między sobą, przekazując wiadomości dotyczące aktualizacji tras. Niektóre protokoły routingu cyklicznie wysyłają wiadomości aktualizacyjne, inne natomiast wysyłają te wiadomości tylko w wypadku zmiany topologii sieci. Niektóre protokoły przesyłają pełne tablice routingu w każdej wiadomości, natomiast inne przesyłają tylko informacje na temat zmienionych tras. Router tworzy i utrzymuję swoją tablicę routingu na podstawie aktualizacji tras uzyskiwanych od sąsiednich routerów.

10.2.6 Algorytmu i metryki routingu

Algorytm jest szczegółowym rozwiązaniem danego problemu. W przypadku routingu pakietów różne protokoły routingu wykorzystują różne algorytmy routingu przy podejmowaniu decyzji dotyczących portu, przez który należy przesłać nadchodzący pakiet. Decyzje podejmowane przez algorytmy routingu opierają się na metrykach.

Protokoły routingu projektowane są z myślą o realizacji jednego lub kilku z poniższych założeń:

- **Optymalizacja** — optymalizacja określa skuteczność protokołu routingu w wyborze najlepszej ścieżki. Ścieżka zależeć będzie od metryk i ich wag wykorzystanych w obliczeniach. Na przykład jeden algorytm może wykorzystywać metryki liczby przeskoków i opóźnienia, przypisując metrykom opóźnienia większą wagę.
- **Prostota i niski narzut** — im prostszy jest algorytm, tym wydajniej będzie przetwarzany przez procesor i pamięć routera. Ten parametr jest istotny, gdyż umożliwia rozrost sieci do dużych rozmiarów, takich jak w przypadku Internetu.
- **Odporność na błędy i stabilność** — algorytm routingu powinien funkcjonować poprawnie w obliczu niecodziennych albo nieprzewidzianych okoliczności, takich jak awarie sprzętu komputerowego, duże obciążenie i błędy implementacji.
- **Elastyczność** — algorytm routingu powinien szybko dostosowywać się do różnorakich zmian zachodzących w sieci. Zmiany te obejmują dostępność routerów, wielkość pamięci poszczególnych routerów, zmiany pasma i opóźnień występujących w sieci.
- **Szybka zbieżność** — zbieżnością określa się proces uzgadniania dostępnych tras pomiędzy wszystkimi routerami. Kiedy jakieś zdarzenie w sieci zmieni dostępność routera, niezbędne są aktualizacje w celu przywrócenia łączności w sieci. Algorytmy routingu, które charakteryzuje niska zbieżność, mogą spowodować, że dane nie zostaną dostarczone.

Algorytmy routingu wykorzystują różne metryki w celu określenia najlepszej ścieżki. Każdy algorytm routingu na swój sposób dokonuje interpretacji najlepszego wyboru. Algorytm routingu generuje liczbę, zwaną wartością metryki, dla każdej ścieżki w sieci. Zaawansowane algorytmy routingu opierają wybór trasy na wielu metrykach, tworząc z nich pojedynczą metrykę złożoną. Zwykle mniejsze wartości metryk wskazują preferowane ścieżki. Metryki mogą być obliczane na podstawie pojedynczego parametru charakteryzującego ścieżkę lub kilku różnych parametrów. **Poniżej przedstawiono parametry najczęściej wykorzystywane przez protokoły routingu:**

- **Szerokość pasma** — przepustowość łącza w kontekście transmitowanych danych. Zwykle połączenie Ethernet o paśmie 10 Mb/s jest bardziej pożądane od łącza dzierżawionego o paśmie 64 kb/s.
- **Opóźnienie** — czas potrzebny do przesłania pakietu w każdym łączu na drodze ze źródła do celu. Opóźnienie zależy od szerokości pasma łączy pośrednich, ilości danych, które mogą być tymczasowo przechowywane w każdym routerze, przeciążenia sieci oraz fizycznej odległości.
- **Obciążenie** — aktywność występująca w ramach zasobu sieciowego, takiego jak router czy łącze.
- **Niezawodność** — zazwyczaj tym mianem określana jest stopa błędów występujących w danym łączu sieciowym.
- **Liczba przeskoków** — liczba routerów, przez które musi być przesłany pakiet, zanim dotrze do punktu docelowego. Każdy router, przez który muszą zostać przesłane dane, odpowiada pojedynczemu przeskokowi. Ścieżka, której liczba przeskoków wynosi cztery, wskazuje, że dane przesyłane tą ścieżką muszą pokonać cztery routery nim dotrą do punktu docelowego. Jeśli istnieje kilka różnych ścieżek, preferowana jest ścieżka o najmniejszej liczbie przeskoków.
- **Impulsy zegarowe** — opóźnienie na łączu danych mierzone impulsami zegarowymi komputera IBM PC. Jeden impuls to około 1/18 sekundy.
- **Koszt** — dowolna wartość przypisana przez administratora sieci, zwykle oparta na szerokości pasma, wydatku pieniężnym lub innej mierze

Algorytmy i metryki routingu

Protokół	Metryka	Maksymalna liczba routerów	Pochodzeni
RIP	Liczba przeskoków	15	Xerox
IGRP	• Szerokość pasma • Obciążenie • Opóźnienie • Niezawodność	255	Cisco

Metryki routingu to wartości używane do określenia najlepszej ścieżki do następnego przeskoku.

10.2.7 Algorytmy IGP i EGP

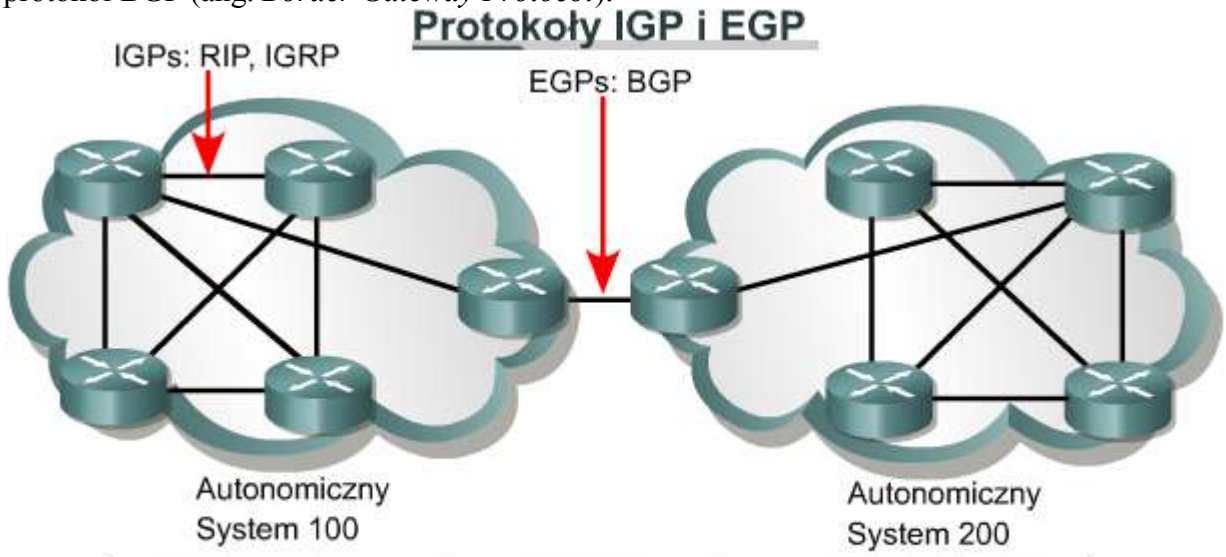
System autonomiczny jest siecią lub zbiorem sieci pod wspólną kontrolą administracyjną, przykładem może być domena cisco.com. System autonomiczny składa się z routerów stanowiących spójny obraz routingu dla świata zewnętrznego.

Protokoły IGP (ang. *Interior Gateway Protocols*) i EGP (ang. *Exterior Gateway Protocols*) stanowią dwie rodziny protokołów routingu.

Protokoły IGP prowadzą routing danych wewnątrz systemu autonomicznego.

- Protokoły RIP i RIPv2 (ang. *Routing Information Protocol*),
- Protokół IGRP (ang. *Interior Gateway Routing Protocol*),
- Protokół EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*),
- Protokół OSPF (ang. *Open Shortest Path First*),
- Protokół IS-IS (ang. *Intermediate System-to-Intermediate System*).

Protokoły EGP prowadzą routing danych między systemami autonomicznymi. Przykładem protokołu z rodziny EGP jest protokół BGP (ang. *Border Gateway Protocol*).



System autonomiczny to zbiór sieci znajdujących się w jednej wspólnej domenie administracyjnej. Protokoły IGP działają w obrębie systemu autonomicznego. Protokoły EGP łączą różne systemy autonomiczne.

10.2.8 Stan łącza i wektor odległości

Protokoły routingu mogą być przypisane do rodziny protokołów IGP lub EGP, w zależności od tego, czy grupa routerów jest objęta wspólną administracją, czy też nie. Protokoły z rodziny IGP mogą zostać dalej podzielone na protokoły wektora odległości i protokoły stanu łącza.

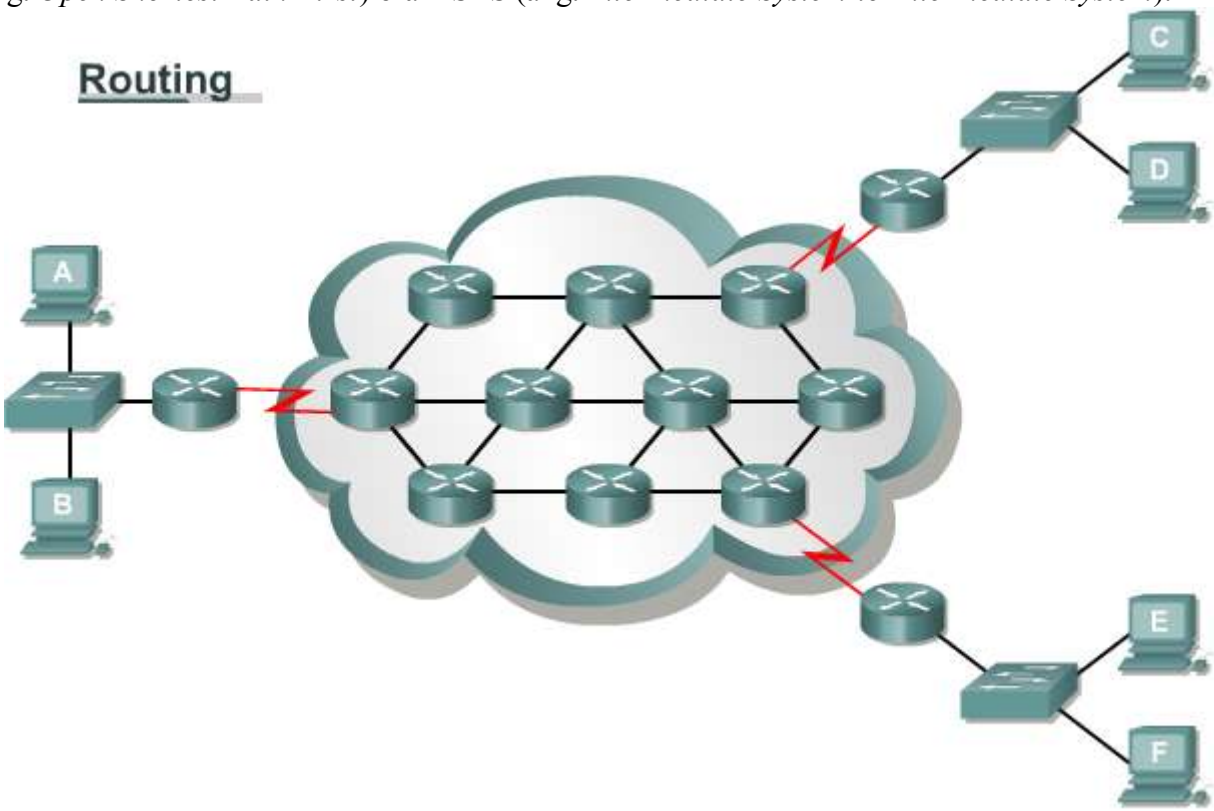
W rozwiązaniach opartych na wektorze odległości określana jest odległość oraz kierunek, wektor, do dowolnego łącza w intersieci. Odległością może być liczba przeskoków do łącza. Routery korzystające z algorytmów routingu działających na podstawie wektora odległości cyklicznie przesyłają do routerów sąsiadujących wszystkie pozycje swoich tablic routingu lub ich część. Proces ten odbywa się nawet wtedy, gdy w sieci nie wystąpiły żadne zmiany. Po otrzymaniu aktualizacji trasy router może sprawdzić wszystkie znane trasy i wprowadzić zmiany w swojej tablicy routingu. Proces ten jest w języku angielskim określany także mianem „routing by rumor". Informacje o sieci, którymi dysponuje router, opierają się na danych uzyskanych od sąsiadujących routerów.

Poniżej wymieniono przykładowe protokoły wektora odległości:

- **Protokół RIP *(ang. Routing Information Protocol)*** — najczęściej stosowany w Internecie protokół z rodziny IGP. Protokół RIP wykorzystuje liczbę przeskoków jako jedyną metrykę.

- **Protokół IGRP** ***(ang. Interior Gateway Routing Protocol)*** — protokół z rodziny IGP opracowany przez firmę Cisco w celu rozwiązania problemów związanych z procesem routingu w dużych sieciach heterogenicznych.
- **Protokół EIGRP** ***(ang. Enhanced IGRP)*** — protokół z rodziny IGP będący własnością firmy Cisco. Wykorzystuje on wiele funkcji protokołu stanu łącza. Z tego powodu określany jest mianem zrównoważonego protokołu hybrydowego, jednak w rzeczywistości jest to zaawansowany protokół routingu oparty na wektorze odległości.

Protokoły routingu z wykorzystaniem stanu łącza zostały zaprojektowane w celu eliminacji ograniczeń protokołów routingu opartych na wektorze odległości. Protokoły routingu z wykorzystaniem stanu łącza szybko reagują na zmiany w sieci poprzez wysyłanie wyzwalanych aktualizacji jedynie po wystąpieniu takich zmian. Protokoły routingu z wykorzystaniem stanu łącza wysyłają okresowe aktualizacje, zwane także odświeżaniem stanu łącza, co pewien dłuższy czas, na przykład co 30 minut.
Gdy trasa lub łącze ulegnie zmianie, urządzenie, które wykryło zmianę, tworzy ogłoszenie o stanie łącza LSA (ang. *link-state advertisement*) dotyczące tego łącza. Ogłoszenie LSA jest następnie wysyłane do wszystkich sąsiednich urządzeń. Każde urządzenie prowadzące routing odbiera kopię ogłoszenia LSA, dokonuje aktualizacji swojej bazy danych stanów łączy i przesyła ogłoszenie LSA do wszystkich sąsiednich urządzeń. Rozgłaszanie LSA jest niezbędne, aby zagwarantować, że wszystkie urządzenia prowadzące routing przed aktualizacją tablic routingu utworzą bazy danych ściśle odzwierciedlające topologię sieci.
Algorytmy routingu według stanu łącza wykorzystują swoje bazy danych do utworzenia pozycji tablicy routingu zawierających najkrótsze ścieżki. Przykładami protokołów z wykorzystaniem stanu łącza mogą być protokoły OSPF (ang. *Open Shortest Path First*) oraz IS-IS (ang. *Intermediate System-to-Intermediate System*).



10.2.9 Protokoły routingu

Protokół RIP jest protokołem routingu z wykorzystaniem wektora odległości, w którym stosuje się liczbę przeskoków jako metrykę służącą do określenia kierunku i odległości do dowolnego łącza w intersieci. Jeżeli do punktu docelowego prowadzi więcej niż jedna ścieżka, protokół RIP wybierze tę, która zawiera najmniejszą liczbę przeskoków. Jednak z powodu wykorzystania w protokole RIP liczby przeskoków jako jedynej metryki nie zawsze wybrana zostanie najszybsza ścieżka. Co więcej, protokół RIP nie może dokonywać routingu pakietów na odległości większe niż 15 przeskoków. Protokół RIPv1 (RIP wersja 1) wymaga, żeby wszystkie urządzenia w sieci używały tej samej maski podsieci. Dzieje się tak dlatego, że w aktualizacji tras nie uwzględnia on informacji na temat maski podsieci. Określane jest to mianem routingu klasowego.
Protokół RIPv2 (RIP wersja 2) dokonuje routingu z uwzględnieniem prefiksu i wysyła w ramach aktualizacji tras informacje dotyczące masek podsieci. Określane jest to mianem routingu bezklasowego. W routingu bezklasowym różne podsieci w tej samej sieci mogą mieć różne maski podsieci. Wykorzystanie różnych masek podsieci w ramach tej samej sieci określane jest mianem maskowania VLSM (ang. *variable-length subnet masking*).

Protokół IGRP jest zaprojektowanym przez firmę Cisco protokołem routingu opartym na wektorze odległości. Protokół IGRP został utworzony specjalnie w celu rozwiązania problemów związanych z routingiem w dużych sieciach, gdzie zasięg takich protokółów jak RIP okazał się już niewystarczający. Protokół IGRP wybiera najszybszą dostępną ścieżkę, opierając się na szerokości pasma, obciążeniu, opóźnieniu i niezawodności. Cechuje go także znacznie większa maksymalna liczba przeskoków w porównaniu z protokołem RIP. Protokół IGRP korzysta jedyne z routingu klasowego.
Protokół OSPF jest protokołem routingu z wykorzystaniem stanu łącza zaprojektowanym przez organizację IETF (Internet Engineering Task Force) w 1988 roku. Został on opracowany na potrzeby dużych skalowanych intersieci, dla których protokół RIP nie był już wystarczający.
Protokół IS-IS (ang. *Intermediate System-to-Intermediate System*) jest protokołem routingu z wykorzystaniem stanu łącza stosowanym przez protokoły routowane inne niż protokół IP. Protokół Integrated IS-IS jest rozszerzoną implementacją protokołu IS-IS obsługującą różne protokoły routowane, w tym także protokół IP.
Podobnie jak IGRP, protokół EIGRP jest własnością firmy Cisco. Protokół EIGRP jest zaawansowaną wersją protokołu IGRP. W szczególności, protokół EIGRP cechuje doskonała wydajność działania, w tym szybka zbieżność i niski narzut na szerokość pasma. Protokół EIGRP jest zaawansowanym protokołem wektora odległości wykorzystującym także pewne funkcje protokołu stanu łącza. Z tego powodu protokół EIGRP jest czasami określany mianem hybrydowego protokołu routingu.
Protokół BGP (ang. *Border Gateway Protocol*) jest przykładem protokołu EGP (ang. *External Gateway Protocol*). Protokół BGP wymienia informacje o routingu pomiędzy systemami autonomicznymi, gwarantując przy tym wybór ścieżki pozbawionej zapętleń. BGP jest głównym protokołem ogłaszania informacji o trasach wykorzystywanym przez największe firmy i dostawców usług sieciowych działających w Internecie. BGP4 jest pierwszą wersją protokołu BGP obsługującą bezklasowy routing międzydomenowy (CIDR) oraz agregację tras. W przeciwieństwie do protokołów IGP (ang. *Internal Gateway Protocol*), takich jak RIP, OSPF i EIGRP, protokół BGP nie korzysta z metryk, takich jak liczba przeskoków, szerokość pasma czy opóźnienie. Zamiast tego, protokół BGP podejmuje decyzje dotyczące routingu, bazując na regułach sieci lub regułach wykorzystujących różnorodne atrybuty ścieżki BGP.

10.3 Zasady funkcjonowania podsieci

10.3.1 Klasy sieciowych adresów IP

Wzory bitowe adresów IP

Klasa A	Sieć	Host		
Oktet	1	2	3	4

Klasa B	Sieć		Host	
Oktet	1	2	3	4

Klasa C	Sieć			Host
Oktet	1	2	3	4

Klasa D	Host			
Oktet	1	2	3	4

Adresy klasy D są używane w grupach wieloemisyjnych. W tym przypadku nie ma potrzeby wydzielania części sieciowej i części hosta. Adresy klasy E są zarejestrowane tylko do badań.

Tak jak zostało to opisane we wcześniejszej części tego modułu, klasy adresów IP umożliwiają obsługę od 256 do 16,8 miliona hostów. Klasy mogą być podzielone na mniejsze podsieci w celu efektywnego zarządzania ograniczoną liczbą adresów IP. Rysunek zawiera przegląd możliwości podziału między sieci i hosty.

10.3.2 Wprowadzenie do podsieci i przyczyny ich tworzenia

W celu utworzenia struktury podsieci bity hosta muszą być przypisane jako bity podsieci. Często określane jest to mianem „pożyczania" bitów. Jednak bardziej odpowiednim pojęciem jest „użyczanie" bitów. Proces rozpoczyna się zawsze od wysuniętego najbardziej na lewo bitu hosta, który położony jest najbliżej ostatniego oktetu sieci. Adres podsieci zawiera części sieci odpowiadające klasom A, B i C, a także pole podsieci i pole hosta. Pola podsieci i hosta tworzone są na podstawie pierwotnej części hosta głównego adresu IP. Jest to realizowane poprzez przypisanie niektórych bitów z pierwotnej części hosta do części sieciowej adresu. Możliwość podziału pierwotnej części hosta na nowe pola podsieci i hosta zapewnia administratorom sieci elastyczność adresowania. Poza ułatwieniem zarządzania, tworzenie podsieci pozwala administratorowi na ograniczenie zjawiska rozgłaszania i wprowadzenie niskopoziomowej ochrony w sieci LAN. Tworzenie podsieci zapewnia nieco wyższy

poziom bezpieczeństwa, ponieważ dostęp do innych podsieci jest możliwy jedynie za pośrednictwem usług routera. Co więcej, zastosowanie list dostępu umożliwia wprowadzenie zabezpieczeń dostępu. Na podstawie różnych kryteriów zawartych na tego typu listach można umożliwić dostęp do podsieci lub odmówić go. Listy dostępu zostaną omówione szerzej w dalszej części kursu. Właściciele sieci klas A i B zauważyli, że możliwość tworzenia podsieci stanowi źródło dochodu poprzez dzierżawę albo sprzedaż poprzednio nieużywanych adresów IP. Podział na podsieci jest dla danej sieci operacją wewnętrzną. Z zewnątrz sieć LAN jest widziana jako pojedyncza sieć z pominięciem jakichkolwiek szczegółów dotyczących jej struktury wewnętrznej. Dzięki takiej strukturze sieci tablice routingu są niewielkie i wydajne. Weźmy np. lokalny węzeł o adresie 147.10.43.14 w podsieci 147.10.43.0. Z zewnątrz widziany jest tylko ogłaszany adres sieci głównej 147.10.0.0, gdyż lokalny adres podsieci 147.10.43.0 jest poprawny tylko w sieci LAN, w której zastosowano podział na podsieci.

10.3.3 Ustalanie adresu maski podsieci

Wybór liczby bitów wykorzystywanych podczas procesu tworzenia podsieci zależeć będzie od wymaganej maksymalnej liczby hostów przypadających na podsieć. Podczas obliczania liczby podsieci i hostów tworzonych w procesie pożyczania bitów konieczna jest znajomość podstaw matematyki liczb binarnych i wartości pozycji bitów w każdym oktecie.

Ostatnie dwa bity ostatniego oktetu, niezależnie od klasy adresu IP, nie mogą być w żadnym przypadku przypisane do podsieci. Bity te nazywane są dwoma najmniej znaczącymi bitami. Wykorzystanie do tworzenia podsieci wszystkich dostępnych bitów z wyjątkiem ostatnich dwóch sprawi, że w każdej z podsieci będą mogły znajdować się tylko dwa hosty. Jest to praktyczna metoda oszczędzania adresów w adresowaniu szeregowych łączy routerów. Jednak w przypadku działającej sieci LAN spowodowałoby to niedopuszczalne podniesienie kosztów wyposażenia. Maska podsieci udziela routerowi informacji potrzebnych do określenia, w której sieci i podsieci znajduje się konkretny host. Jedynki binarne w masce podsieci wskazują pozycje bitów części sieciowej. Bity podsieci to te, które zostały pożyczone z pierwotnej części hosta. Jeśli zostały pożyczone trzy bity, maska adresu klasy C będzie miała postać 255.255.255.224. W formacie z ukośnikiem maska ta będzie reprezentowana jako /27. Liczba stojąca za ukośnikiem jest całkowitą liczbą bitów użytą w częściach adresu odpowiadających sieci i podsieci. **W celu określenia** potrzebnej liczby bitów projektujący sieć muszą określić liczbę hostów w największej podsieci oraz liczbę podsieci. Jako przykład przedstawiono sytuację, w której sieć musi składać się z sześciu podsieci zawierających po 25 hostów każda. Liczba bitów, których przypisanie musi zostać zmienione, może zostać szybko określona przy wykorzystaniu tabeli podsieci. W wierszu zatytułowanym „Liczba podsieci możliwych do wykorzystania" odnaleźć można informację, że w przypadku sześciu podsieci trzeba pożyczyć dodatkowe trzy bity do stworzenia maski podsieci. Z tabeli wynika także, że w każdej ze stworzonych podsieci maksymalna ilość hostów wynosi 30, co jest zgodne z wymaganiami tego przykładu. Różnica pomiędzy liczbą hostów możliwych do wykorzystania a całkowitą liczbą hostów wynika z użycia pierwszego wolnego adresu jako identyfikatora, a ostatniego jako adresu rozgłoszeniowego dla każdej podsieci. Podział na odpowiednią liczbę podsieci zawierających wymaganą liczbę hostów prowadzi do tego, że część potencjalnych adresów hostów jest tracona. Routing klasowy nie pozwala na wykorzystanie tych adresów. Jednakże routing bezklasowy, o którym będzie mowa w dalszej części kursu, pozwala na odzyskanie wielu z nich.

Metoda wykorzystana przy tworzeniu tablicy podsieci może być użyta do rozwiązania wszystkich problemów związanych z tworzeniem podsieci. **W metodzie wykorzystywany jest następujący wzór:**

Liczba podsieci możliwych do wykorzystania = dwa do potęgi równej liczbie przypisanych bitów podsieci lub bitów pożyczonych, minus dwa. Odjęcie dwóch wynika z uwzględnienia adresów zarezerwowanych na identyfikator i adres rozgłoszeniowy sieci.

Liczba hostów możliwych do wykorzystania = dwa do potęgi równej liczbie pozostałych bitów, minus dwa (adresy zarezerwowane na identyfikator i rozgłaszanie podsieci)

Tabela podsieci (pozycja bitu i wartość)

Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1

Tabela podsieci (identyfikator maski podsieci)

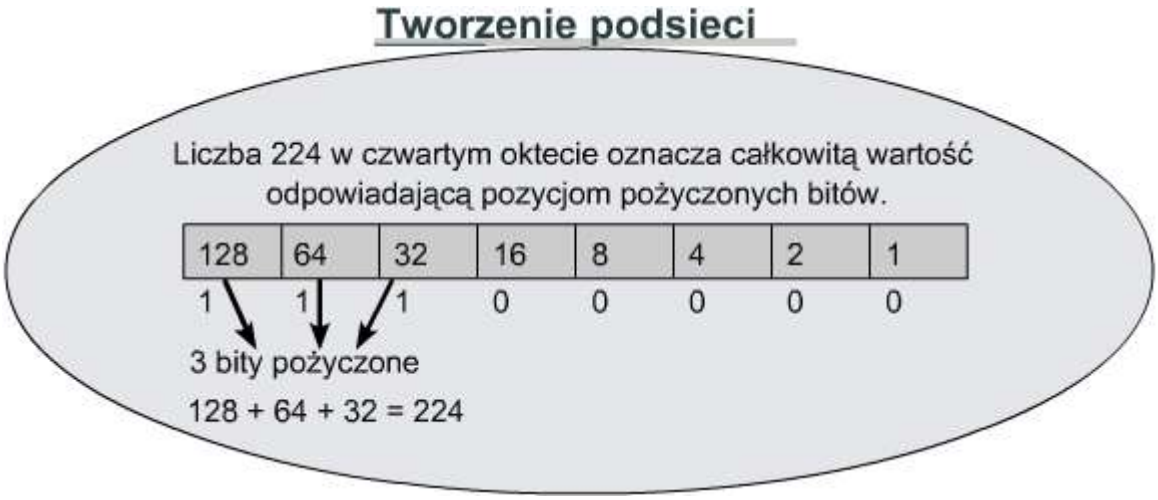
Format z ukośnikiem	/25	/26	/27	/28	/29	/30	N/A	N/A
Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

Tabela podsieci

Format z ukośnikiem	/25	/26	/27	/28	/29	/30	Nd.	Nd.
Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Całkowita liczba podsieci		4	8	16	32	64		
Liczba podsieci możliwych do wykorzystania		2	6	14	30	62		
Całkowita liczba hostów		64	32	16	8	4		
Liczba hostów możliwych do wykorzystania		62	30	14	6	2		

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.



10.3.4 Zastosowanie maski podsieci

Po ustaleniu maski podsieci można ją wykorzystać do utworzenia schematu podsieci. **Tabela przedstawiona na rysunku prezentuje przykładowe podsieci i adresy powstałe przez przypisanie trzech bitów do pola podsieci.** Powstanie osiem podsieci, z których każda składać się będzie z 32 hostów. Numerowanie podsieci rozpoczyna się od zera (0). Pierwsza podsieć jest zawsze określana mianem podsieci zerowej.

Podczas tworzenia tabeli podsieci trzy pola wypełniane są automatycznie, wypełnienie pozostałych wymaga pewnych obliczeń. Identyfikator podsieci zerowej równy jest numerowi sieci głównej, w tym przypadku: 192.168.10.0. Identyfikator rozgłaszania dla całej sieci równy jest największemu dopuszczalnemu numerowi, w tym przypadku: 192.168.10.255. Trzecim podanym numerem jest identyfikator podsieci numer siedem. Składa się on z trzech oktetów sieci oraz numeru maski podsieci wstawionego na pozycji czwartego oktetu. Do pola podsieci zostały przypisane trzy bity; ich łączna wartość wynosi 224. Identyfikator podsieci numer siedem to 192.168.10.224. Te wstawione liczby stają się punktami kontrolnymi służącymi do sprawdzenia poprawności po wypełnieniu tabeli.

Schemat podsieci

Nr podsieci	Ident. podsieci	Zakres hostów	Identyfikator rozgłaszania
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Kiedy korzystamy z tabeli podsieci lub wzoru przypisanie trzech bitów do pola podsieci spowoduje przypisanie 32 hostów do każdej podsieci. Pozwala to na określenie wartości kroku przy obliczaniu identyfikatora kolejnej podsieci. Począwszy od zerowej podsieci, dodanie liczby 32 do poprzedzającego numeru spowoduje ustalenie identyfikatora każdej podsieci. Należy zwrócić uwagę, że identyfikator podsieci zawiera same zera w części hosta.

Tabela podsieci

Format z ukośnikiem	/25	/26	/27	/28	/29	/30	Nd.	Nd.
Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Całkowita liczba podsieci		4	8	16	32	64		
Liczba podsieci możliwych do wykorzystania		2	6	14	30	62		
Całkowita liczba hostów		64	32	16	8	4		
Liczba hostów możliwych do wykorzystania		62	30	14	6	2		

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

W każdej podsieci pole rozgłaszania ma ostatni numer składający się w części hosta z samych jedynek binarnych. Zastosowanie tego adresu umożliwia rozgłaszanie tylko do członków pojedynczej podsieci. Ponieważ identyfikator podsieci zerowej wynosi 192.168.10.0, a podsieć składa się łącznie z 32 hostów, identyfikator rozgłaszania będzie równy 192.168.10.31. Począwszy od zera, 32. kolejna liczba ma wartość 31. Należy pamiętać, że zero (0) jest rzeczywistą liczbą wykorzystywaną w świecie zagadnień sieciowych. Kolumna identyfikatora rozgłaszania może zostać wypełniona w taki sam sposób jak kolumna identyfikatora podsieci. Należy po prostu dodać liczbę 32 do poprzedzającego identyfikatora rozgłaszania w podsieci. Można także zacząć od ostatniego, najniższego pola kolumny i posuwać się do góry, wstawiając liczby powstałe przez odjęcie jedynki od identyfikatora poprzedzającej podsieci.

10.3.5 Tworzenie podsieci w sieciach klasy A i B

Procedura tworzenia podsieci w sieciach klasy A i B jest taka sama jak w przypadku klasy C, z tą różnicą, że można użyć znacząco większej liczby bitów. Liczba bitów możliwych do przypisania do pola podsieci w adresie klasy A wynosi 22, natomiast w klasie B — 14 bitów.

Poprzez przypisanie 12 bitów adresu klasy B do pola podsieci uzyskujemy maskę podsieci równą 255.255.255.240 lub /28. Przypisane zostało wszystkie osiem bitów trzeciego oktetu, dając liczbę 255, będącą największą liczbą, jaką można zapisać na ośmiu bitach. W czwartym oktecie zostały przypisane cztery bity, dając liczbę 240. Przypomnijmy, że maska podsieci w formacie z ukośnikiem stanowi sumę wszystkich bitów przypisanych do pola podsieci powiększoną o ustalone bity sieci.

Poprzez przypisanie 20 bitów adresu klasy A do pola podsieci uzyskujemy maskę podsieci równą 255.255.255.240 lub /28. Do pola podsieci przypisano wszystkie osiem bitów drugiego i trzeciego oktetu oraz cztery bity czwartego oktetu.

W tej sytuacji widać, że maska podsieci dla adresów klasy A i B wydaje się być identyczna. O ile maska nie odnosi się do adresu sieci, nie jest możliwe określenie liczby bitów przypisanych do pola podsieci.

Niezależnie od klasy sieci, która ma zostać podzielona na podsieci, obowiązują te same reguły:

Całkowita liczba podsieci = $2^{\text{do potęgi równej liczbie pożyczonych bitów}}$ Całkowita liczba hostów= $2^{\text{do potęgi równej liczbie pozostałych bitów}}$ Liczba podsieci możliwych do wykorzystania = $2^{\text{do potęgi równej liczbie pożyczonych bitów}}$ minus 2 Liczba hostów możliwych do wykorzystania= $2^{\text{do potęgi równej liczbie pozostałych bitów}}$ minus 2

Tworzenie podsieci

Maska	128	192	224	240	248	252	254	255
Bity pożyczone	1	2	3	4	5	6	7	8
Wartość	128	64	32	16	8	4	2	1
Podsieci	2	4	8	16	32	64	128	256

W przypadku adresu klasy C i maski /25 wypożyczony jest tylko jeden bit, jak pokazano w tabeli powyżej. Natomiast w przypadku adresu klasy B ta sama maska odpowiada wypożyczeniu dziewięciu bitów.

10.3.6 Obliczanie adresu podsieci z wykorzystaniem operacji iloczynu logicznego

Routery wykorzystują maski podsieci w celu określenia sieci, do której należą poszczególne hosty. Proces ten określany jest mianem iloczynu logicznego. Routery określają identyfikator podsieci odebranego pakietu przy użyciu binarnego procesu iloczynu logicznego. Iloczyn logiczny przypomina mnożenie.

Proces ten odbywa się na poziomie liczb dwójkowych. Dlatego maska i adres IP muszą być prezentowane w formacie dwójkowym. Adres IP oraz adres podsieci poddawane są operacji iloczynu logicznego, w wyniku którego otrzymywany jest identyfikator podsieci. Rezultat jest wykorzystywany przez router w celu przesłania pakietu przez właściwy interfejs.

Operacja iloczynu logicznego (AND)

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

Zasada jest następująca wynik wszystkich operacji z wyjątkiem 1 AND 1 wynosi 0 (zero).

Obliczanie identyfikatora podsieci

Adres pakietu	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Maska	255.255.255.224	11111111.11111111.11111111.11100000
Ident. podsieci	201.10.11.64	11001001.00001010.00001011.01000000

Tworzenie podsieci jest umiejętnością, którą trzeba opanować. Minie wiele godzin spędzonych na wykonywaniu ćwiczeń praktycznych, zanim uzyska się umiejętność tworzenia elastycznych i przydatnych schematów. W sieci WWW dostępnych jest wiele kalkulatorów wspomagających tworzenie podsieci. Jednakże administratorzy sieci muszą znać sposoby ręcznego przeprowadzania obliczeń przy tworzeniu podsieci, aby móc skutecznie zaprojektować schemat sieci i kontrolować poprawność wyników uzyskanych za pomocą kalkulatora podsieci. Kalkulator podsieci nie umożliwia przygotowania wstępnego schematu, może jedynie obliczyć końcowe dane adresowe. Co więcej, w trakcie trwania egzaminu certyfikacyjnego korzystanie z jakichkolwiek kalkulatorów jest zabronione

Podsumowanie

- Protokół jest zestawem reguł określających sposób komunikacji komputerów w sieciach.
- Protokół routowany przesyła dane poprzez sieć.
- Protokoły routingu umożliwiają routerom wybór najlepszej ścieżki dla danych od miejsca źródłowego do docelowego.
- Zastosowanie podsieci umożliwia administratorom sieci określenie rozmiarów fragmentów sieci, na których będą operować.