**Karta sieciowa**

Karta sieciowa to podzespół elektroniczny służący do przetwarzania pakietów danych w sygnały (oraz sygnałów w pakiety danych), które następnie są przesyłane w sieci. Kar­ta sieciowa jest nazywana adapterem sieciowym (ang. network adapter) lub interfejsem sieciowym (NIC, ang. NetWork Interface Card). Pozwala na połączenie komputera z siecią i internetem. Karty sieciowe obsługują standardy stosowane w sieciach. Zadania karty sie­ciowej to transmisja i rozszyfrowywanie informacji między łączami komunikacyjnymi.

W zależności od stosowanego w sieci medium transmisyjnego istnieją odmienne spo­soby podłączenia kabla sieciowego do urządzeń. Na karcie sieciowej znajduje się złącze do podłączenia medium transmisyjnego. W tym celu urządzenie zostało wyposażane w specjalną kartę rozszerzeń z odpowiednimi gniazdami. Niektóre karty sieciowe umoż­liwiają połączenie w trybie bezprzewodowym. Dodatkowo są wyposażone w antenę.

Karty sieciowe z odpowiadającymi im wtyczkami do połączenia z siecią

Każda ta sieciowa może pracować tylko w jednym standarcie, np. Ethernet, Token Ring, FDDI, Arcnet. Na potrzeby tego podręcznika zostanie omówiona tylko praca w stan­dardzie Ethernet.

Do połączenia karty sieciowej z komputerem służą łącza typu: ISA, PCI, PCI-Express, PCMCIA, USB.

Karcie sieciowej przez producenta jest nadawany unikatowy adres fizyczny MAC (ang. Media Access Control). Składa się on z 48 bitów, z których pierwsze 24 rozróżniają producenta karty sieciowej (ang. vendor codę), a pozostałe to unikatowy identyfikator dane­go egzemplarza karty. Przykładowo adres 00:0A:E6:3E:FD:E1 oznacza:

00:0A:E6 - producent Elitegroup Computer Systems Co.;

3E:FD:E1 - kolejny numer karty wyprodukowanej przez ECS.

Wcześniej adres MAC był na stałe zapisywany w pamięci ROM. Obecnie w nowych kartach ethernetowych jest możliwa zmiana nadanego wcześniej adresu.

**Hub (koncentrator)**

Koncentrator sieciowy jest urządzeniem łączącym segmenty sieci przez przesyłanie sygna­łów elektrycznych z jednego portu do wszystkich urządzeń sieciowych podłączonych do huba. To urządzenie o wielu portach służące do przyłączenia np. stacji roboczych. Umoż­liwia zwiększenie liczby węzłów. Rozprowadzając sygnał, nie filtruje go. Zadaniem huba jest wzmocnienie i powielanie sygnałów w sieci lokalnej.

Koncentrator

Pracuje w warstwie fizycznej modelu OSI. W związku z tym nie analizuje ramek pod kątem adresów MAC.

Wyróżnia się dwa typy koncentratorów: pasywne i aktywne. Huby pasywne to skrzyn­ki, do których są podłączone wszystkie węzły sieci. Koncentratory aktywne dodatkowo wzmacniają sygnał, co umożliwia prawie dwukrotne wydłużenie najbardziej odległych węzłów sieci. Te drugie wymagają zasilania układów wzmacniaczy sygnałów.

Zaletą koncentratorów jest brak opóźnień. Niestety dość poważną wadę stanowi to, że gdy wiele urządzeń zaczyna jednocześnie wysyłać pakiety danych, dochodzi do kolizji. Z tego względu najlepiej sprawują się na końcach sieci, gdzie liczba urządzeń nie przekracza pięć.

**Switch (przełącznik)**

Przełącznik sieciowy (ang. switch) jest urządzeniem przekazującym ramki między segmen­tami sieci z doborem portu przełącznika, na który ramka jest przekazywana. Umożliwia komunikację między węzłami. Jest wiełoportowym mostem, który przekazuje pakiety na podstawie zawartego w pakiecie adresu MAC. Przekazuje pakiety tylko do docelowego por­tu, a nie do wszystkich, tak jak hub. Dlatego jest nazywany „inteligentnym hubem”.

Switch (przełącznik)

W odróżnieniu od koncentratora przełącznik pracuje głównie w warstwie łącza danych modelu OSI, dzięki czemu przekazuje ramki do docelowego segmentu sieci. Umożliwia zmniejszenie obciążenia przez podział sieci na mikrosegmenty. Jest to możliwe tylko wte­dy, gdy do jednego segmentu jest przyłączana jedna stacja robocza. Wynika z tego, że każdy port jest wejściem do jednego segmentu sieci. Nie występują wtedy kolizje, a raczej są ograniczone do jednego hosta i użytkownik ma możliwość korzystania z całej dostępnej szerokości pasma.

Switch analizuje adresy MAC nadawcy i odbiorcy otrzymanej ramki. Przy okazji adres nadawcy jest wykorzystywany do tworzenia tablicy skojarzeń przechowującej adresy MAC oraz odpowiadające im porty. Jej pojemność mieści się od 4096 do 16 384 wpisów. Skoja­rzenie adresu MAC z portem nie jest bezterminowe. Jeżeli przez określony czas nie ma aktywności dla danego skojarzenia, automatycznie jest ono usuwane z tablicy.

Kiedy przełącznik otrzyma ramkę, to najpierw sprawdza, czy w tablicy jest przypisany port do adresu MAC nadawcy. Jeżeli nie ma takich danych, wysyła ramkę na wszystkie porty, oprócz źródłowego. W zależności od tego, z którego portu otrzyma odpowiedź, taką korelację zapisuje w tablicy między portem a adresem nadawcy ramki źródłowej. Jeżeli w tablicy znajduje się skojarzenie, to dana ramka jest przesyłana wyłącznie na port skoja­rzony z adresem MAC nadawcy.

Przekazywanie ramek może odbywać się w różnych trybach:

* *Fastforward (cut-through)* - najmniejsze opóźnienie, ramka jest bezzwłocznie przesyłana po otrzymaniu adresu docelowego;
* *Storę and forward* - największe opóźnienie, jest sprawdzana suma kontrolna ramek: błędne ramki i takie, które biorą udział w kolizjach, nie są transmitowane dalej;
* *Fragment free* - jest sprawdzana poprawność nagłówka ramki.

Standardowym trybem pracy przełącznika jest fastforward. Kiedy liczba błędów wynos: kilkanaście na sekundę, switch automatycznie przechodzi w tryb storę and forward. Jest to tzw. inteligentne przełączanie. Pozwala ono na optymalizację przepustowości sieci w za­leżności od jakości przesyłanych danych.

Ponadto przełączniki zarządzalne umożliwiają wydzielanie sieci wirtualnych VLAN (ang. Virtual Local Area NetWork). Polega to na tym, że ruch z portów przypisanych do dane: sieci VLAN jest przekazywany do portów należących do tej sieci oraz portów wspólnych (ang. trunk). Przypisanie portów może być statyczne, co wymusza zapamiętanie, które porty należą do danej sieci, lub odbywa się na podstawie adresu MAC podłączonego urządzenia.

Między dwoma podłączonymi do siebie przełącznikami sieci wirtualne są obsługiwane za pomocą połączenia trunk. Każda ramka przesyłana w ten sposób posiada dodatkowe 4 bajty danych wstawionych za adresem nadawcy, w których jest zapisany identyfikator sie­ci VLAN, gdzie odbywa się transmisja. Takie ramki nazywa się oznaczonymi (ang. tagged), a ich maksymalna długość wynosi 1522 bajty.

Pierwsze dwa bajty są znacznikiem TPID (ang. Tag Protocol Identifier) i zawsze mają wartość 0 x 8100. Umożliwiają identyfikację ramki jako oznaczonej w standardzie 802.1Q. Kolejne dwa bajty TCI (ang. Tag Control Information) składają się z następujących danych: (ang. Priority Codę Point) - trzy bity do oznaczenia priorytetu ramki. Standard IEEE 802.1p definiujący sposób użycia pola przedstawiono poniżej.

(ang. Canonical Format Indicator) - jednobitowy identyfikator informujący o tym, w jakim standardzie pracuje sieć LAN. 0 - Ethernet, 1 - Token Ring.

VI i (ang. VLAN Identifier) - 12-bitowe pole określające, do której sieci należy ramka. VID - 0x000 ramka nie należy do żadnej sieci wirtualnej, VID - 0x001 wykorzystywane dla mostów, 0xFFF - brak możliwości konfiguracji. Pozostały zakres 0x002-0xFFE to możliwe identyfikatory VLAN.

**Router (trasownik)**

Trasownik (ang. router) to urządzenie, którego zadaniem jest łączenie różnych sieci komputerowych. Pełni funkcję węzła komunikacyjnego. Przesyła pakiety między połą­czonymi sieciami. Analizuje adres sieciowy i wyznacza najlepszą trasę do przesłania pakietu danych. Rozbudo­wany o funkcję Wi-Fi odgrywa rolę punktu dostępowego (ang. access point). Umożliwia sterowanie przepustowo­ścią sieci oraz zapewnia bezpieczeństwo. Pracuje w war­stwie sieciowej modelu OSI.

Router

Przekazuje pakiety z sieci źródłowej do docelowej na podstawie informacji zawartych w pakietach TCP/IP. Taki proces nosi nazwę routingu, routowania łub trasowania.

Obsługa ruchu w sieci odbywa się za pomocą procesorów sieciowych NP (ang. NetWork Processor) lub dedykowanych wysoko wyspecjalizowanych układów cyfrowych ASIC / FPGA (ang. Application Specific Integrated Circuit / Field-Pro- grammable Gate Array) zaprojektowanych do realizacji ściśle określonych zadań.

Układ ASIC / FPGA znajdujący się na płycie routera

Pierwszymi routerami były komputery ogólnego przeznaczenia. Obecnie są to niewielkie, wysoko wyspecjalizowane urządzenia, których interfejsy sieciowe łączy bardzo szybka magi­strala wewnętrzna. Są to interfejsy różnych typów, takich jak kable miedziane, światłowody lub transmisja bezprzewodowa. Każdy interfejs korzysta ze specjalnego oprogramowania, w które dla różnych standardów protokołów komunikacji sieciowej jest wyposażony router. Umożliwia to przesyłanie pakietów danych z jednego protokołu transmisji do drugiego.

Gdy do sieci jest podłączonych wiele routerów, wymieniają one między sobą informacje na temat adresów odbiorców, wykorzystując dynamiczny protokół routingu.

Najpopularniejszymi protokołami klasy IGP (ang. Interior Gate Protocol), wewnętrzny­mi względem systemu autonomicznego, w którym pracują, są OSPF (ang. Open Shortest Path First) oraz ISIS (ang. Intermediate System to Intermediate System). Pierwszy charakte­ryzuje się m.in. dobrą slcalowalnością oraz wyborem optymalnych ścieżek. Obecnie jest dominującym protokołem trasowania wewnętrznego. Drugi, choć tak jak OSPF posługuje się algorytmem Dijkstry, jest protokołem używanym głównie przez dużych operatorów internetowych ze względu na możliwość trasowania datagramów protokołu IP i inne.

Schemat połączeń przewodowych i bezprzewodowych routera z węzłami sieci

Każdy router tworzy tabelę z wykazem preferowanych tras między dwoma dowolnymi systemami w połączonych sieciach. Tabela ta nosi nazwę lynamicznej tablicy trasowania i przechowuje ścieżki do konkretnych obszarów sieci oraz związane z nimi metryki, np. liczba routerów na drodze do miejsca docelowego. Taka tablica może być również dostar­czona przez administratora sieci i wtedy określa się ją mianem

Router, który służy do łączenia podsieci hosta z innymi sieciami, nazywamy bramką domyślną.