Rozdział 26

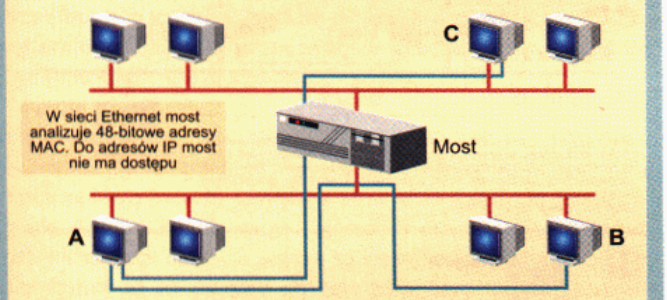
Sprzęt sieciowy

Mosty

Mosty to proste urządzenia śledzące adresy MAC umieszczane w przesyłanych do nich pakietach. Mosty nie mają dostępu do adresów warstwy sieciowej, dlatego nie można ich użyć do dzielenia sieci opartej na protokole TCP/IP na dwie podsieci IP. To zadanie mogą wykonywać wyłącznie routery.

Prosty most pełni funkcję inteligentnego regeneratora. Odbiera i retransmituje pakiety, analizując przy tym, skąd pakiet przyszedł i dokąd należy go przesłać. Jeśli pakiet nie powinien być retransmitowany, most nie obsługuje go. W przeciwnym wypadku pakiet jest kierowany na drugą stronę mostu.

Most sprzęgający dwa segmenty LAN



Mosty są urządzeniami sprzęgającymi w jeden organizm dwa segmenty tej samej sieci LAN lub dzielącymi tę sieć na dwa oddzielne segmenty (kolizji, ale nie rozgłoszeniowe). Wykorzystują do tego adresy generowane przez warstwę łącza (*Layer 2*) modelu OSI.

Most może być urządzeniem wolno stojącym, ale może też przybrać postać modułu instalowanego w *chassis* lub w hubie. Most buduje specjalną bazę danych (tabelę mostowania), która zawiera informacje o topologii sieci.

Analizując adresy MAC, urządzenie wie, czy dany pakiet należy wyekspediować na drugą stronę mostu czy też pozostawić bez odpowiedzi. Sprzęgane segmenty mogą być budowane przy użyciu tej samej technologii (Ethernet–Ethernet) lub reprezentować odmienne standardy (Ethernet–Token Ring). Mosty łączące dwie sieci LAN, z których każda jest budowany przy użyciu innej technologii, nazywamy mostami translacyjnymi.

Rodzaje mostów

W zakresie technologii mostowania pakietów możemy wyróżnić trzy rodzaje mostów:

- transparentne,
- oparte na technologii *Source Routing*,
- oparte na technologii *Spanning Tree*.

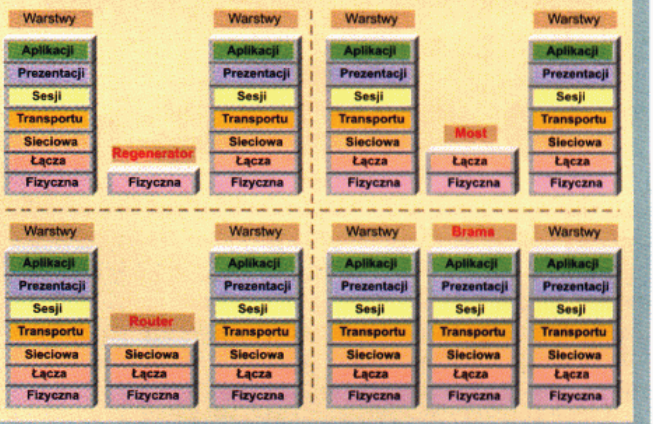
Kiedy most transparentny jest zainstalowany pierwszy raz, ekspediuje na drugą stronę wszystkie adresy zawierające nie znane mu adresy. Most taki „uczy" się topologii sieci i dopiero po pewnym czasie tworzy tabelę mostowania; korzystając z jej usług jedne pakiety akceptuje, a inne odrzuca. Mosty odczytują adresy generowane w podwarstwie MAC drugiej warstwy modelu OSI (warstwa łącza). Są to w przypadku sieci Ethernet 48-bitowe adresy kart sieciowych, przypisywane im na stałe przez producentów w momencie wytwarzania karty. Mosty *Spanning Tree* (metoda używana w sieciach Ethernet) mają jedną podstawową zaletę – zapobiegają powstawaniu w sieci pętli pakietów, które mogą nieraz kompletnie zablokować medium. Metoda *Source Routing* jest stosowana w sieciach Token Ring – pakiet danych zawiera wtedy informację o tym, którą drogą ma dotrzeć do celu. Mosty korzystają w tej metodzie ze specjalnych algorytmów (wysyłając wcześniej w sieć pakiety pełniące rolę „badaczy", przechodzących przez wszystkie mosty, i wracających do nadawcy). Dzięki temu pakiet trafia do stacji przeznaczenia przechodząc przez minimalną liczbę węzłów sieci.

Mosty operują w warstwie MAC i mogą sprzęgać sieci homogeniczne, czyli tego samego standardu (np. IEEE 802.3). Niektóre mosty – zwane translacyjnymi *(translational bridges)* – wykonują dodatkowe funkcje, dzięki którym mogą sprzęgać sieci heterogeniczne (różnych standardów, np. IEEE 802.3 i IEEE 802.5).

Mosty można też podzielić na dwie grupy, zależnie od tego, w jakim środowisku są stosowane. Stosując to rozróżnienie mamy do czynienia z mostami pracującymi lokalnie lub mostami sprzęgającymi odległe sieci LAN.

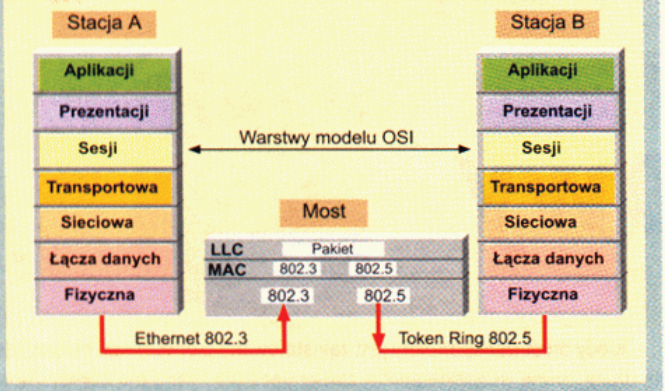
Należy jeszcze wspomnieć o specyficznym węźle sieci, który nie jest ani mostem, ani routerem. Jest czymś pośrednim. Mowa o **brouterze** (zlepek

W których warstwach OSI operuje most?



Mosty operują w drugiej warstwie modelu OSI (warstwa łącza). Najczęściej łączą dwa segmenty sieci LAN wykorzystujące tę samą technologię, ale są też dostępne mosty sprzęgające sieć Ethernet z Token Ring. Ponieważ mosty nie mają dostępu do informacji zawartych w warstwie sieciowej, nie mogą zawiadywać ruchem pakietów przesyłanych przez sieci rozległe, tak jak to robią routery.

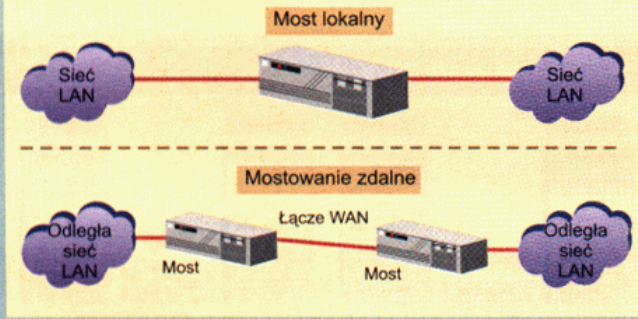
Tak pracuje most translacyjny



Stacja A pracująca w sieci 802.3 wygenerowała pakiet, opakowała go: „kopertą" używaną przez protokół stosowany w tej sieci i następnie wyekspediowała w łącze. Pakiet po dotarciu do mostu jest rozpakowywany z „koperty" (podwarstwa MAC warstwy łącza) i przekazywany do górnej podwarstwy warstwy łącza (czyli LLC) do dalszego przetwarzania. Tutaj most zapakowuje pakiet w kolejną kopertę (tym razem używaną przez protokół stosowany w sieci 802.5) i przekazuje do dolnej warstwy celem wyekspediowania w łącze. Pakiet jest wreszcie odbierany przez stację B. Z mostowaniem translacyjnym należy postępować bardzo ostrożnie. Nie zawsze jest bowiem tak, że wszystkie rodzaje pól w ramce lub inne parametry są wspierane przez sprzęgane sieci. Wtedy most translacyjny nie będzie przekazywać pakietów poprawnie.

dwóch słów - *bridge* i *router*). Jest to podrasowany most, ubogi krewny routera. Brouter wykonuje wszystkie operacje przypisywane mostowi, a dodatkowo ma możliwość analizowania adresów generowanych w warstwie sieciowej. Dlatego brouter może np. trasować specyficzny rodzaj pakietów (np. generowanych przez protokół IP), a wszystkie inne pakiety mostować w ten sam sposób, jak to robią klasyczne mosty. Broutery są obecnie stosowane niezmiernie rzadko i zostały całkowicie wyparte przez routery wielo-protokołowe.

Dwa rodzaje mostów: lokalny i zdalny

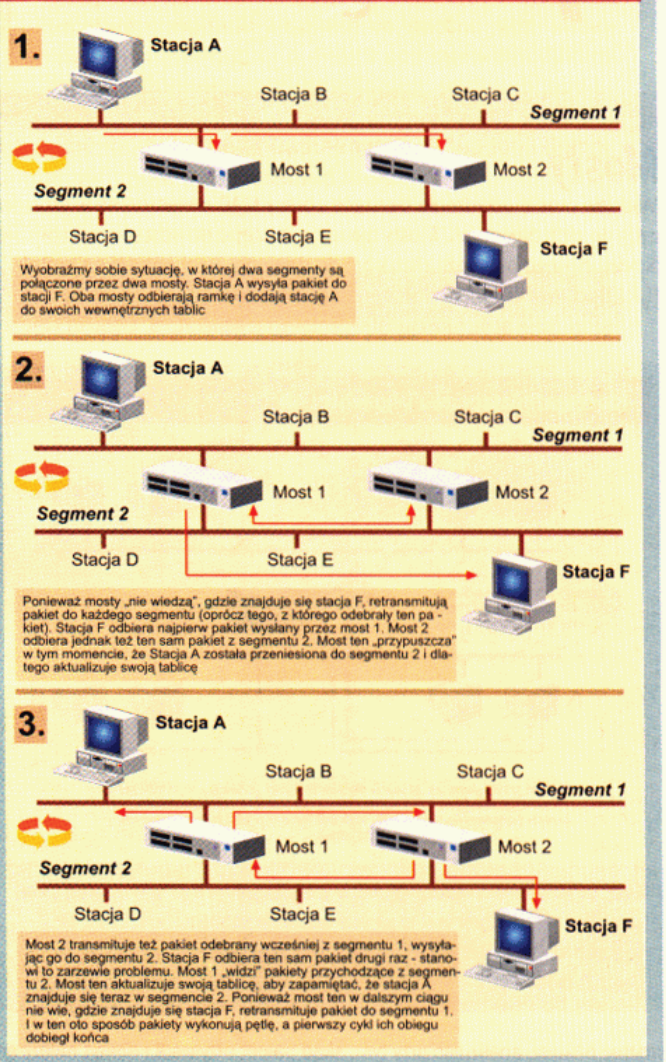


Jak sama nazwa wskazuje, most lokalny sprzęga w jeden organizm dwa lokalne segmenty tej samej sieci LAN. Most zdalny łączy ze sobą dwie sieci oddalone od siebie fizycznie o wiele kilometrów, używając najczęściej do tego celu łącza telekomunikacyjnego. Technika zdalnego mostowania ma tę zaletę, że łącze pracuje bardzo szybko. Chociaż eksploatowane obecnie łącza WAN pracują już bardzo wydajnie, to sieci LAN (a więc naturalne środowisku stosowania mostów) dysponują jednak nadal dużo większą przepustowością niż sieci WAN. I chociaż most zdalny nie zwiększy w żaden sposób przepustowości łącza WAN, to dzięki zastosowaniu specjalnych technik (buforów gromadzących transmitowane i odbierane pakiety) może z powodzeniem obsłużyć nawet bardzo wymagającą aplikację, która nie pracowałaby nigdy równie wydajnie w momencie zainstalowania w miejsce mostu standardowego routera.

Spanning Tree

Jeśli w sieci opartej na **mostowaniu** jedne segmenty komunikują się z innymi segmentami używając **zapasowych ścieżek połączeń** (nadmiarowość), to do środowiska takiego powinno się wprowadzić protokół **Spanning Tree**. Protokół ten gwarantuje, że oba połączenia (podstawowe i zapasowe) będą funkcjonować poprawnie i nie przysporzą administratorowi sieci kłopotów. Problem ten dotyczy też sieci VLAN, ponieważ sieć wirtualna ma archi-

Mechanizm powstawania pętli



Jeśli segmenty komunikują się między sobą przy użyciu kilku mostów (nadmiarowość), to jedno łącze pełni rolę podstawowej ścieżki połączenia, obsługującej cały ruch pakietów wymienianych między tymi segmentami. Drugie łącze jest zapasową ścieżką połączenia, pozostającą w stanie oczekiwania. Jeśli pierwsze połączenie ulega uszkodzeniu, to do akcji wkracza algorytm Spanning Tree i („znając" topologię całej sieci) uruchamia drugie połączenie. Bez technologii Spanning Tree sieci o opisanej topologii grozi poważne niebezpieczeństwo, polegające na tym, że pakiety zaczną być od pewnego momentu obsługiwane przez oba, a nie jedno połączenie. Może wtedy dojść do krachu, ponieważ pakiety będą bez przerwy krążyć od jednego segmentu do drugiego, tworząc niekończącą się pętlę. Jest to możliwe, ponieważ w sieci LAN opartej na mostach powinna zawsze być tylko jedna ścieżka połączenia między stacjami A i F. Jeśli jest kilka takich ścieżek, to istnieje prawdopodobieństwo - a właściwie pewność - że te same pakiety będą przesyłane z jednego miejsca do drugiego i z powrotem, tworząc niebezpieczne pętle. Dzieje się tak, ponieważ tablice obsługujące mosty i przełączniki warstwy 2 są aktualizowane w sposób wymuszający powstawanie pętli.

tekturę, którą można porównać do sieci opartej na mostach. W każdej sieci VLAN należy wtedy implementować oddzielne mechanizmy transportu pakietów, wykorzystujące do tego celu Spanning Tree. (jch)

Wybrani producenci mostów

Allied Telesyn International	Hewlett-Packard
Asante Technologies	IBM
CNet Technology	Madge
Cabletron Systems	Olicom
D-Link Systems	RAD Data Communications
Gandalf Technologies	RND Networks

Huby i przełączniki

W sieciach komputerowych i telekomunikacyjnych spotykamy się często z takimi terminami jak **hub**, **koncentrator**, **repeater** (regenerator) czy **przełącznik** i **router**. O ile jest stosunkowo łatwo odróżnić router od innych urządzeń (routery działają w warstwie 3 modelu OSI, a koncentratory, regeneratory i przełączniki nie sięgają tak wysoko), o tyle trudniej jest już odróżnić np. hub od koncentratora. Z regeneratorami sprawa jest prostsza – są to urządzenia pracujące w najniższej warstwie modelu OSI, realizującej zgoła odmienne zadania niż koncentrator lub hub, nie mówiąc już o routerze. W dodatku bywa, że wszystkich tych terminów używa się zamiennie, ponieważ granice między określanymi przez nie urządzeniami są płynne i np. pracujący w sieci hub jest też koncentratorem, tyle że wykonującym ściśle określone zadanie.

Koncentrator

Koncentrator jest specyficznym multiplekserem, obsługującym wiele dołączonych do niego kanałów, używanych przez różne urządzenia do transmitowania danych. Kanały mogą najczęściej pracować jednocześnie, a odbierane z nich dane lub sygnały są kierowane do jednego medium. Koncentratory są na przykład używane przez firmy telekomunikacyjne podłączające zdalnych użytkowników do Internetu (protokół PPP), korzystających z usług łącz komutowanych. Koncentrator odbiera z wielu dołączonych do niego modemów sygnały i przesyła je przez jedno szybko pracujące łącze do węzła sieci Internet.

Wybrani producenci regeneratorów

Allied Telesyn International	Hewlett-Packard
Cabletron Systems	NBase Communications
Cisco Systems	RAD Data Communications
Compex	Xyplex Networks

Koncentratory są używane w lokalnych sieciach komputerowych do odbierania danych z wielu stanowisk pracy i kierowania ich do kolejnego segmentu sieci. Tego rodzaju koncentrator pracujący w środowisku sieci LAN jest określany mianem huba (Ethernet) lub urządzenia MAU (*Media Access Unit*) – sieci Token Ring.

Repeater (regenerator)

Jest to urządzenie sieciowe używane do regenerowania lub replikowania sygnałów. Regenerator może odtwarzać (czyli przywracać im pierwotną postać) sygnały analogowe lub cyfrowe, które są zbyt słabe, aby je dalej transmitować. Regeneratory analogowe pełnią najczęściej rolę prostych wzmacniaczy, podczas gdy regeneratory cyfrowe odbierają dane i po odpowiedniej obróbce kierują je do kolejnego segmentu sieci LAN.

Regenerator sprzęga w sieci komputerowej poszczególne segmenty (a nie podsieci) sieci LAN, zwiększając w ten sposób jej zasięg. Jeden segment sieci Ethernet 10Base-5 (tzw. gruby Ethernet) może mieć np. długość 500 m, a cała nitka takiej sieci (topologia linii) może się składać z trzech segmentów sprzęganych w całość przez dwa regeneratory (razem 1500 m).

Prosty hub jest niczym innym jak wieloportowym regeneratorem, ponieważ odbiera dane od podłączonych do niego komputerów (np. za pomocą skrętki nieekranowanej, 10Base-T), retransmitując je do łącza opartego np. na technologii 10Base-5 (tzw. gruby Ethernet). Hub przełączający porty jest natomiast wieloportowym koncentratorem wyposażonym w kilka (najczęściej cztery lub osiem) pracujących niezależnie od siebie regeneratorów. Regenerator nie jest obdarzony żadną inteligencją i nie może wykonywać zadań realizowanych przez mosty czy tym bardziej routery.

Hub

Dwadzieścia lat temu (gdy sieci LAN zaczynały dopiero robić karierę) mało kto słyszał o hubach. Pierwsze sieci Ethernet były oparte na tzw. żółtym kablu (standard 10Base-5), gdzie wszystkie stacje współdzieliły medium, którym był kabel koncentryczny zakończony z każdej strony terminatorami o oporności 50 omów. Sieć taka miała topologię linii, a jeden segment kabla 10Base-5 może mieć długość 500 m.

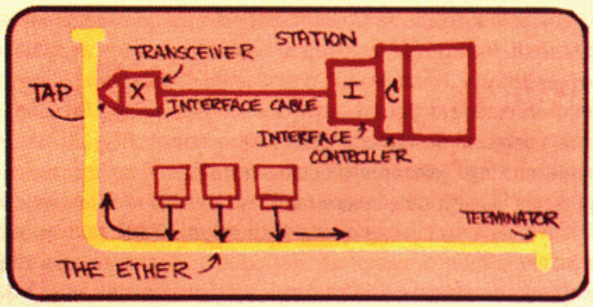
Trzy rodzaje hubów

Huby możemy podzielić na pasywne, inteligentne i przełączające.

- **Hub pasywny** przekazuje po prostu sygnały odbierane z każdego dołączonego do niego portu na wszystkie pozostałe porty.
- **Hub inteligentny** (*managable*, czyli z możliwością zarządzania) przetwarza odbierane sygnały i przekazuje do innych portów (do wszystkich, do niektórych – tak jak ma to miejsce w przypadku huba przełączającego porty, a nieraz tylko do jednego; zależy to już od rodzaju huba). Hub taki może już filtrować pakiety i poddawać je kontroli. Huby inteligentne są wyposażane w rozwiązania, dzięki którym ruch pakietów przepływających przez taki węzeł sieci może być monitorowany przez administratora sieci. Administrator ma najczęściej możliwość logicznego włączania i wyłączania wskazanych portów z eksploatacji.
- **Huby przełączające** można podzielić na dwie grupy: przełączające porty i takie, które przełączają ramki. Hub przełączający porty to wieloportowy koncentrator wyposażony w kilka regeneratorów i specjalny układ zarządzają-

Jeden z pierwszych rysunków sieci Ethernet

Widoczny tu odręczny szkic wykonał w 1976 roku sam twórca tej technologii, Robert Metcalfe



Pierwsze sieci Ethernet były oparte na standardzie 10Base-5. Twórcą sieci Ethernet jest Robert Metcalfe, a technologię tę opracowano z myślą o przesyłaniu danych drogą radiową (stąd nazwa – Ethernet), a nie kablem, jakby to z pozoru mogło się wydawać. Standard 10Base-5 przewiduje, że sieć ma topologię liniową (topologia gwiazdy powstała w momencie opracowania koncepcji koncentratorów) i może się składać z pięciu odcinków kabla koncentrycznego, każdy o długości 500 m (stąd liczba 5 w nazwie standardu). Poszczególne odcinki kabla są połączone regeneratorami, a wszystkie stacje współdzielą dostęp do jednego medium. Ponieważ stacje można instalować co 2,5 m (stosując tzw. transceivery, przy użyciu oryginalnej techniki – ostry bolec wciskany mechanicznie za pomocą specjalnego narzędzia w przewód kabla koncentrycznego), to z usług takiej sieci może teoretycznie korzystać około tysiąca stacji.

cy przyłączaniem portów do poszczególnych regeneratorów, które logicznie reprezentują w takim układzie różne domeny kolizji. Hub przełączający ramki odczytuje adres stacji docelowej i kieruje pakiet tylko do tego portu, do którego ta stacja jest dołączona. Hub przełączający ramki to przełącznik.

Konstrukcja hubów

Biorąc pod uwagę konstrukcję hubów, można je podzielić na: wolno stojące, wieżowe i modularne (chociaż zdarzają się też huby reprezentujące mieszankę tych rozwiązań).

- **Huby wolno stojące** mają stałą konfigurację i są z reguły wyposażone w rozwiązania pozwalające łączyć je z innymi hubami (łącze 10Base-5 lub kaskada budowana za pomocą skrętki łączącej dwa huby). Huby wolno stojące są tanie, ponieważ najczęściej nie można nimi zarządzać (chociaż dynamiczny rozwój technologii powoduje, że inteligentne huby wolno stojące wypierają z rynku proste huby pasywne). Huby wolno stojące nadają się do obsługi niewielkich grup roboczych, składających się z czterech do maks. dwudziestu czterech stanowisk pracy.
- **Huby wieżowe** dysponują tymi samymi opcjami co huby wolno stojące, z tą jednak różnicą, że można – używając krótkich odcinków kabli – budować z nich rozbudowane węzły sieci (wieże), składające się z wielu hubów. Po połączeniu w jeden zestaw kilku hubów wieżowych mamy do czynienia ze specyficznym hubem modularnym, którym można zarządzać jak pojedynczym węzłem sieci. Jeden hub w takiej wieży pełni wtedy najczęściej rolę modułu służącego do zarządzania pozostałymi urządzeniami (wchodzącymi w skład tej wieży).

Huby wieżowe mają jedną podstawową zaletę – za ich pomocą można w dowolny i bardzo elastyczny sposób rozbudowywać stopniowo strukturę sieci. Nie trzeba od razu kupować dużego huba, a w razie potrzeby można dokupić tylko kolejny „klocek lego" (czytaj hub wieżowy), poszerzając możliwości wybranego węzła sieci. Jest to tanie i proste rozwiązanie. Wszystkie huby wieżowe są hubami inteligentnymi – można nimi zarządzać.

- **Huby modularne** mają budowę modułową (jedno *chassis* z wieloma gniazdami rozszerzeń) i można nimi zarządzać. W gniazdach rozszerzeń można instalować różnego rodzaju moduły (karty), dysponujące kilkoma portami; moduły te reprezentują właściwie oddzielne huby wolno stojące. Wszystkie gniazda (a więc i moduły) korzystają z usług szybko pracującej magistrali i towarzyszących jej układów scalonych, realizujących zadanie przełączania pakietów. Każdy z portów wbudowanych w dowolny moduł może przesyłać pakiety do innych portów wbudowanych w pozostałe moduły.

Huby wolno stojące są tanie, natomiast huby modularne należą do najdroższych. Nie ma się czemu dziwić – są to uniwersalne węzły sieci, będące prawdziwymi „kombajnami", potrafiącymi obsłużyć dowolnego rodzaju protokół komunikacyjny, medium i technologię sieciową. Do huba takiego można dołączać sieci Ethernet, Fast Ethernet, Token Ring lub ATM. Wszystko zależy od tego, jaki rodzaj modułu zainstalujemy i z jaką przepustowością pracują układy przełączające ramki lub komórki zainstalowane w hubie. Hub modularny ma najczęściej 4–12 gniazd. Biorąc pod uwagę fakt, że jeden moduł może dysponować dziesięcioma portami, do huba 12-gniazdowego można dołączyć aż 120 stacji. Huby modularne nadają się więc doskonale do instalowania w rozbudowanych sieciach LAN.

Wybrani producenci hubów (Ethernet/Fast Ethernet)

3Com	Hewlett-Packard
Allied Telesyn International	IBM
Bay Networks	Intel
Cabletron Systems	Madge
Cisco Systems	NBase
Compaq	Olicom
Compex	SMC
D-Link	Transition Networks

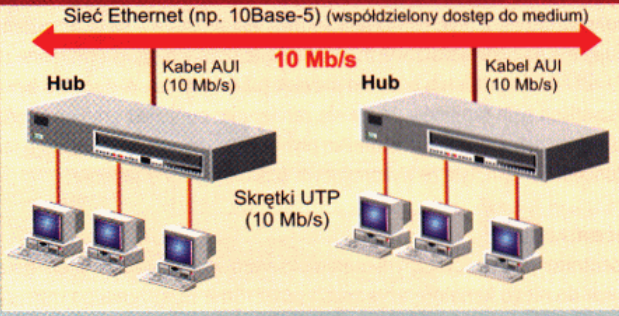
Jak pracują proste huby?

Jak wcześniej wspomniano, proste huby pełnią funkcję wieloportowych regeneratorów. A regenerator to takie urządzenie, które wzmacniając sygnały, pozwala zwiększać długość jednego segmentu sieci komputerowej (agregując jednocześnie ruch pakietów, ale w ramach technologii współdzielonego dostępu do medium). Hub taki dysponuje najczęściej jednym portem podłączonym do sieci szkieletowej (w przypadku Ethernetu będzie to np. technologia 10Base-5 lub 10Base-2) i wieloma portami standardu 10Base-T. Hub nie dzieli sieci na mniejsze segmenty, ale tylko zwiększa jej zasięg.

Huby przełączające porty

Wzrastające oczekiwania użytkowników eksploatujących sieci LAN przyczyniły się do powstania kolejnego rodzaju huba – tym razem przełączającego porty. Nie należy przy tym mylić urządzenia przełączającego porty (*port switching hub*) z klasycznym przełącznikiem, czyli z hubem przełączającym ramki (*frame switching hub*). Ten drugi rodzaj huba omówiono w części poświęconej przełącznikom. Jak sama nazwa wskazuje, hub przełączający porty operuje na poziomie portów (a nie ramek, tak jak to robi przełącznik).

Tak pracują huby pasywne zainstalowane w sieci Ethernet 10 Mb/s

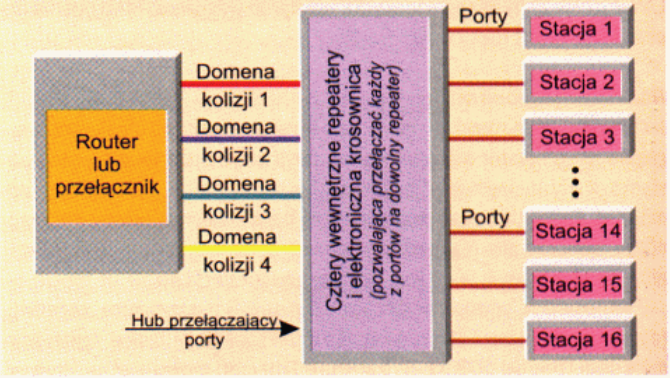


Przykład sieci Ethernet opartej na dwóch standardach: 10Base-5 i 10Base-T. Stacje robocze są podłączone przez porty RJ-45 (skrętka nieekranowana) do huba, który przez port AUI (*Adapter Unit Interface*), kabel TDC (*Transceiver Drop Cable*) i transceiver komunikuje się z tzw. żółtym kablem. Każda stacja, chcąc wyekspediować dane, musi tu rywalizować o dostęp do medium zarówno ze stacjami dołączonymi do huba, jak i z pozostałymi stacjami (albo innymi hubami) dołączonymi do kabla 10Base-5 (tzw. gruby Ethernet).

Kiedy stosować huby przełączające porty?

Huby przełączające porty można rozbudować tak, by obsługiwały nawet do 200 stanowisk pracy. Jednak sprzęt tego rodzaju sprawdza się najlepiej w środowiskach pracy składających się z nie więcej niż 50 stanowisk. W każdym razie, jeśli sieć składa się z ponad 100 stanowisk, lepiej jest zdać się na rozwiązanie oparte na przełączaniu ramek.

Tak pracują huby przełączające porty



Konwencjonalne huby odbierają pakiety z portu i przekazują je do wszystkich innych portów. Huby przełączające porty segmentują sieć LAN, zwiększając znacznie jej przepustowość. Dzięki takiemu zabiegowi (który sprowadza się do budowania kilku oddzielnych domen kolizji) osiągamy podobny efekt, jak w przypadku zastosowania wysokiej klasy urządzenia, opartego na technologii przełączania ramek. Z tą różnicą, że znacznie mniejszym kosztem.

Jeszcze nie przełącznik, ale już nie repeater

Huba przełączającego porty można umieścić (jeśli weźmiemy pod uwagę zadania realizowane przez tego rodzaju sprzęt) między prostymi koncentratorami (repeaterami) i pełnokrwistymi przełącznikami. Zamiast definiowania, że każdy port jest oddzielną podsiecią, huby przełączające porty tworzą cztery (czasami osiem) wewnętrznych segmentów (regeneratorów), z których każdy zachowuje się względem podłączonego do niego portu tak, jakby był oddzielną podsiecią. Huby przełączające porty mają najczęściej konstrukcję wieżową i dysponują dopracowanymi mechanizmami zarządzania, w tym opcją *load balancing*.

Jak pracuje hub przełączający porty?

Na czym polega przełączanie portów i czym ta technologia różni się od metody polegającej na przełączaniu ramek, która jest stosowana w dużych, korporacyjnych systemach sieciowych?

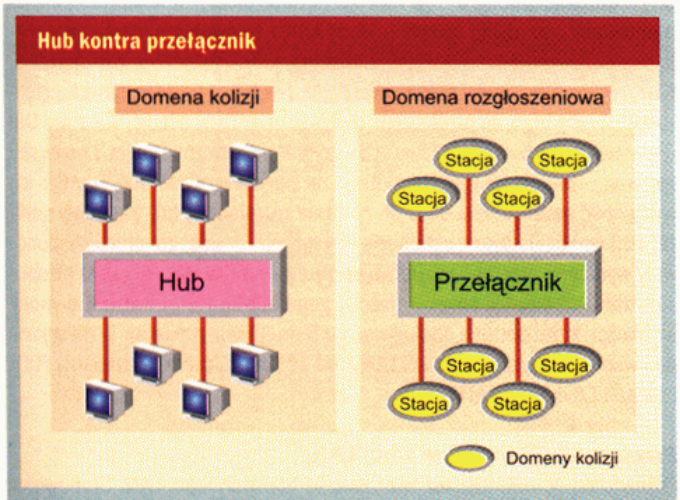
Sieć komputerowa składa się z segmentów, po których krążą pakiety generowane przez stanowiska pracy zainstalowane w danym segmencie. Każdy z segmentów można porównać do dwupasmowej (dwukierunkowej) autostrady. Każda taka autostrada stanowi w sieci Ethernet oddzielną domenę kolizji. Jeśli do danego segmentu podłączymy zbyt wiele urządzeń, na autostradzie powstanie korek – w sieci pojawi się tak wiele pakietów, że przepustowość segmentu znacznie zmaleje.

Urządzenia przełączające radzą sobie z tym problemem, tworząc oddzielne segmenty (separując je w ten sposób od siebie). Każdy taki segment (port) obsługuje tylko jedno stanowisko lub co najwyżej kilka stanowisk pracy. Przełącznik portów decyduje wtedy, gdzie należy kierować ruch pakietów generowanych w obrębie każdego z segmentów, i kieruje pakiety z fizycznego portu huba do jednego z wewnętrznych repeaterów. W hubie przełączającym porty każde wydzielone pasmo przenoszenia danych (czyli zdefiniowaną przez użytkownika – lub automatycznie przez sam hub – grupę portów) jest obsługiwane przez jeden z wewnętrznych, pracujących niezależnie od siebie repeaterów. Nad całością pieczę sprawuje elektroniczna krosownica (matryca przełączania portów), która pozwala przyłączyć każdy z portów do dowolnego repeatera.

Ponieważ przełączanie jest realizowane lokalnie (jak już wspomniano, zadanie to wykonują specjalne układy), to proces ten przebiega bardzo sprawnie – można powiedzieć, że z możliwie maksymalną szybkością, z jaką można wykonać tego rodzaju operację. Dlatego technologia ta jest łatwiejsza do zaimplementowania (i można to zrobić tańszym kosztem) niż technologia oparta na przełączaniu ramek. Ważne jest przy tym to, że technologia przełączania portów oferuje równie wiele zalet, co przełączanie ramek.

Przełącznik ramek pracuje w ten sposób, że przegląda każdą ramkę sieci Ethernet i definiuje na tej podstawie, z którego segmentu pochodzi dany pakiet, i do jakiego segmentu należy go przesłać. Układy wykonujące to zadanie muszą być więc obdarzone pewną inteligencją i urządzenia takie są przez to nieco droższe.

Niezależnie jednak od tego, jakie rozwiązanie wybierzemy (przełączanie portów lub ramek), efekt jest zawsze taki sam – liczba kolizji występujących w sieci LAN znacznie spada, a jej przepustowość wzrasta. Powód jest prosty – w każdym przypadku w architekturze sieci pojawiają się nowe „pasma" do transmitowania ruchu pakietów. Podsumowując można powiedzieć, że z im większej liczby segmentów składa się sieć LAN, tym wydajniej pracuje.



Domeny rozgłoszeniowe i domeny kolizji

Tak jak routery pozwalają segmentować sieć LAN, dzieląc ją na kilka domen rozgłoszeniowych, tak samo robią to przełączniki, ale dzielą sieć na mniejsze domeny kolizji. Zwykły hub pracuje w trybie współdzielonego dostępu do medium. Jeśli do takiego huba jest dołączonych np. osiem stacji, to jednocześnie mogą się ze sobą komunikować dwie stacje. Pozostałe muszą czekać na moment, kiedy dwie stacje zakończą sesję łączności i medium zostanie zwolnione. Huby przełączające mogą obsługiwać jednocześnie wszystkie osiem stacji (zakładając, że pierwsza będzie się komunikować z drugą, trzecia z czwartą, piąta z szóstą, a siódma z ósmą), gwarantując każdej takie samo pasmo przenoszenia danych. Tak więc w przypadku sieci Ethernet 10 Mb/s pakiety będą przepływać przez hub przełączający z szybkością 40 Mb/s (transmisja w trybie półdupleksu; cztery razy po 10 Mb/s).

Przełączniki

Przełączniki (*switches*) są inteligentnie pracującymi węzłami sieci, nazywanymi hubami przełączającymi ramki. Takiej nazwy (hub przełączający) używano z chwilą wprowadzenia tego rodzaju sprzętu na rynek. Przełączniki odbierają pakiety z jednego portu, poddają je filtrowaniu i wysyłają do drugiego portu. Klasyczne przełączniki odczytują adresy zawarte w warstwie MAC, dlatego mogą obsługiwać pakiety generowane przez dowolny protokół operujący w warstwie sieciowej modelu OSI. Słowo klasyczne jest tu użyte celowo, ponieważ przełączniki pracujące w trybie *Layer 3 Switching* (zwane też przełącznikami trasującymi) mają już dostęp do adresów sieciowych stacji docelowych (czyli w sieciach Internet do adresów IP). Lokalne sieci komputerowe oparte na przełącznikach nazywamy przełączanymi sieciami LAN. W przypadku sieci Ethernet używa się określenia przełączany Ethernet.

Przełączniki muszą dysponować wydajnie pracującym układem przełączania ramek, który poradzi sobie z natłokiem pakietów. Możemy podzielić sieć za pomocą przełączników na wiele domen kolizji, ale nadal wszystkie będą pracować w ramach tej samej domeny rozgłoszeniowej. Każdy pakiet *broadcast* musi dotrzeć do wszystkich bez wyjątku stacji. Jedynym rozwiązaniem jest wtedy zastosowanie routera lub przełącznika pracującego w trybie *Layer 3 Switching*, który poradzi sobie z pakietami *broadcast*, stosując odpowiednie mechanizmy filtrowania.

Różne technologie przełączania ramek

Przełączniki instalowane w sieciach LAN obsługują pakiety używając najczęściej jednej z dwóch technologii:

- *cut through* (przełączanie bezzwłoczne),
- *store and forward* (zapamiętaj i wyślij).

Pierwsza technologia jest wydajniejsza, ponieważ węzeł sieci czyta adres MAC i kieruje pakiet natychmiast do portu przeznaczenia (nie czekając nawet na koniec ramki). Ale za szybkość trzeba płacić. Pakiety ekspediowane w sieć w tym trybie nie są sprawdzane i wszelkiego rodzaju błędy czy przekłamania nie mogą zostać wykryte przez przełącznik. Jeśli liczba pakietów kierowanych do przełącznika wzrasta powyżej określonego progu, to

niektóre przełączniki nie odrzucają ich, lecz magazynują na okres przejściowy w specjalnych buforach.

Przełącznik działający w trybie „zapamiętaj i wyślij" pracuje inaczej. Węzeł sieci odczytuje całą ramkę, zapisuje ją w pamięci i dopiero wtedy odczytuje adres MAC. Przełącznik sprawdza, czy pakiet został odebrany prawidłowo (brak błędów) i dopiero wtedy kieruje do portu przeznaczenia. Przełącznik taki pracuje wolniej, ale za to prawie niezawodnie. Tak więc przełączniki *cut through* należy stosować tam, gdzie zależy nam głównie na szybkości, a ewentualne przekłamania nie „położą" nam aplikacji. Te aplikacje, które nie tolerują błędów pojawiających się w danych, powinny być obsługiwane przez przełączniki pracujące w trybie „zapamiętaj i wyślij".

Inne metody przełączania ramek

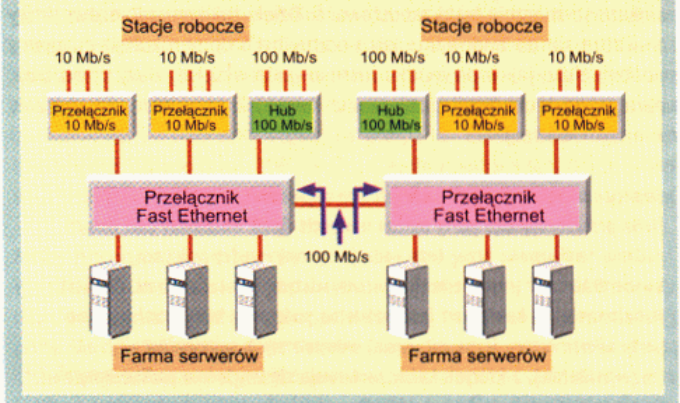
Niektóre przełączniki pracują w trybie pośrednim pomiędzy trybem *cut through* a *store-and-forward*. Są one nazywane przełącznikami *fragment free* lub *adaptive switching*.

Pierwsza metoda jest podobna do *cut through*, jednak przełącznik zaczyna transmitować ramkę do stacji przeznaczenia dopiero wtedy, gdy odbierze pierwsze 64 bajty. Powoduje to nieco większe opóźnienia, jednak gwarantuje, że ewentualne kolizje nie będą przenoszone z jednej domeny kolizji do drugiej (co może nieraz występować przy stosowaniu metody *cut through*).

Metoda inteligentnego przełączania (*intelligent switching*) łączy *cut through* i *store-and-forward*. Na początku przełącznik pracuje w szybkim trybie *cut through*, ale z chwilą przekroczenia określonego poziomu błędów (np. dwudziestu na sekundę) układ przełączania zaczyna pracować w trybie *store-and-forward*. Gdy sytuacja wraca do normy (brak błędów), do akcji wchodzi znowu tryb *cut through*.

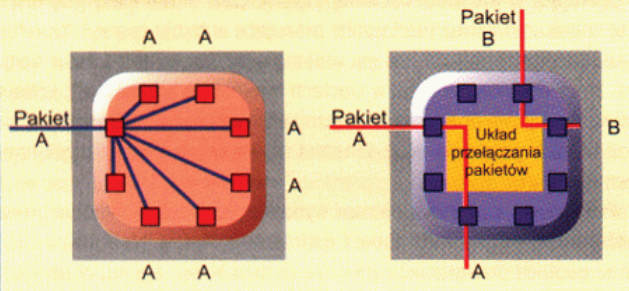
Niekiedy przełącznik dysponuje jednym, centralnym układem przełączania ramek, a w innych rozwiązaniach mamy do czynienia z architekturą rozproszoną (np. układy przełączające ramki mogą się znajdować w każdym nowym module instalowanym w przełączniku). Przełącznik pracuje dużo szybciej niż router, ponieważ zadanie przełączania ramek jest realizowane w dużym stopniu przez warstwę sprzętową takiego węzła sieci (np. specjalizowane układy ASIC). W routerze znakomita większość zadań związanych z trasowaniem pakietów jest realizowana przez oprogramowanie.

Typowe zastosowanie przełączników



Szybko pracujące serwery są podłączone do przełączników Fast Ethernet, które nie komunikują się ze stacjami roboczymi bezpośrednio, ale za pośrednictwem przełączników 10 Mb/s lub prostych hubów pracujących z szybkością 100 Mb/s. Widoczna tu topologia sieci zapewnia każdej stacji roboczej szybki dostęp do serwerów, a dodatkowa korzyść polega na tym, że przełączniki Fast Ethernet nie stanowią oddzielnych węzłów sieci, ale mogą wymieniać między sobą pakiety dzięki obecności łącza 100 Mb/s.

Hub standardowy i hub przełączający



Każdy hub przełączający dysponuje wydajnie pracującym układem do przełączania ramek, dzięki któremu pakiet trafia tylko do jednego portu, a nie do wszystkich, tak jak ma to miejsce w przypadku zwykłego huba. Układy przełączania ramek muszą pracować bardzo wydajnie, tak aby mogły obsłużyć wszystkie pakiety kierowane do jego portów. Producenci przełączników stosują różne technologie przełączania ramek, korzystając najczęściej z technik *cut through* lub *store-and-forward*. Każda z nich ma swoje wady i zalety. Mówiąc najogólniej, przełączniki oparte na technologii *cut through* pracują szybko, ale mniej pewnie (brak mechanizmów kontrolujących przetwarzane pakiety), podczas gdy przełączniki typu *store-and-forward* kontrolują dokładnie proces przełączania ramek, ale pracują wolniej.

Przełączniki trasujące (routing switches)

Przełącznik trasujący (*routing switch*) to taki, który potrafi wyznaczać pakietom marszrutę, czyli operować nie tylko w drugiej, ale też w trzeciej warstwie modelu OSI. Urządzenia takie zachowują się więc podobnie jak routery. Ponieważ routing w tego rodzaju węzłach sieci jest najczęściej implementowany przy użyciu sprzętu (układy ASIC), to przełączniki trasujące mają większą wydajność niż klasyczne routery oparte na oprogramowaniu. Klasyczne routery mają za to tę przewagę, że można je elastycznie konfigurować. Z racji tego, że przełączniki tej klasy operują w trzeciej warstwie OSI (Sieciowa), nazywane są „Layer-3 Switches". Przełączniki Layer 3 pierwszej generacji opierały się (tak jak routery) na silnych procesorach. Dlatego ich wydajność pozostawiała dużo do życzenia (przełączały lub trasowały poniżej 100 tys. pakietów na sekundę). Przełączniki drugiej generacji dysponowały wydajniej pracującą warstwą sprzętową i miały dużo większą przepustowość. Przełączniki Layer 3 trzeciej generacji to już prawdziwe demony szybkości, które potrafią obsługiwać od 5 do 30 mln pakietów IP na sekundę i wspierają całą gamę sieci LAN – od 10Base-T, przez 100Base-T, FDDI i Gigabit Ethernet do ATM.

Przełączniki i wirtualne sieci LAN

Przełączniki umożliwiają też tworzenie wirtualnych sieci LAN. Stanowiska takiej sieci są fizycznie zlokalizowane w różnych punktach (sieciach, podsieciach i segmentach), a łączy je w sieć wirtualną jedynie pewien klucz logiczny. Sieć wirtualna pozwala administratorom pokonywać ograniczenia, które niesie ze sobą sposób adresowania stacji przez protokół komunikacyjny TCP/IP. Protokół ten przewiduje, że jeden port routera może obsługiwać stanowiska zlokalizowane tylko w konkretnej podsieci. Przełączniki pozwalają natomiast grupować w ramach wirtualnej sieci te stacje, które są podłączone do różnych portów. Sieci wirtualne pozwalają optymalizować natężenie ruchu pakietów w poszczególnych częściach sieci. Dzięki nim można też w łatwy sposób rekonfigurować i zmieniać strukturę sieci. Sieć wirtualną można porównać do zmieniającej się dynamicznie struktury połączeń w komutowanej sieci telefonicznej. Administrator sieci pełni tu rolę centrali telefonicznej, łącząc ze sobą logicznie w jedną strukturę porozrzucane po sieci LAN stacje.

Tradycyjne sieci LAN i sieci ATM

Największą siłą i zaletą technologii ATM jest to, że operuje ona w najniższej warstwie sieciowej, tam gdzie mamy do czynienia z pojedynczymi komórkami. Wszystkie funkcje generowane przez wyższe warstwy – od routingu realizowanego w warstwie 3 do połączeń międzysieciowych – można w przypadku technologii ATM przełożyć na strumień komórek transmitowanych z taką szybkością, jaką może oferować tylko pracująca bardzo wydajnie warstwa sprzętowa łącza ATM.

Usługi sieci ATM

Technologia ATM została tak zaprojektowana, aby sieci tego standardu mogły obsługiwać każdy rodzaj aplikacji, używając do tego celu czterech podstawowych klas usług:

CBR (*Constant Bit Rate*) – stała, dająca się przewidzieć potrzebna przepustowość łącza; zastosowanie – np. przesyłanie w czasie rzeczywistym nieskompresowanych pakietów audio, czyli głosu.

VBR (*Variable Bit Rate*) – zmienna, nie dająca się przewidzieć potrzebna przepustowość łącza; zastosowanie – np. przesyłanie skompresowanych pakietów wideo.

ABR (*Available Bit Rate*) – negocjowana przepustowość łącza; zastosowanie – np. praca w trybie „non real time" czy transmitowanie dużych porcji komórek.

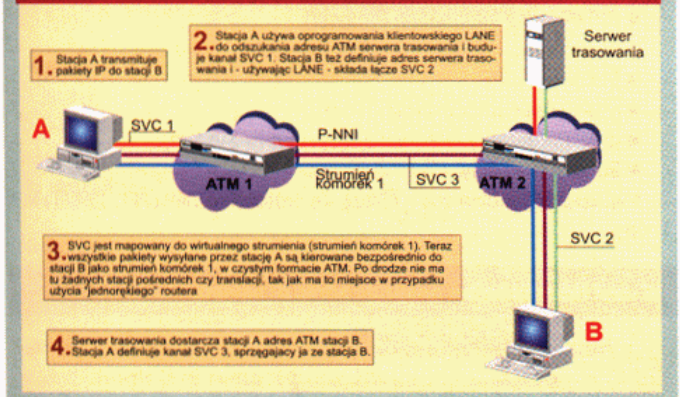
UBR (*Unspecified Bit Rate*) – nie zdefiniowana przepustowość łącza; zastosowanie – pozostałe rodzaje ruchu komórek.

U podstaw działania przełącznika ATM leży cała sfera zarządzania sygnałami – jest to dość skomplikowany proces konfigurowania i składania połączeń. Przykładem najprostszego interfejsu realizującego to zadanie jest UNI (*User-to-Network Interface*), który pozwala sprzęgać stacje ATM z przełącznikiem ATM. Jeśli w sieci pracuje kilka przełączników, to muszą one porozumiewać się między sobą. Kwestię tę reguluje specyfikacja NNI (*Network-to-Network Interface*), opisująca zasady pracy interfejsu łączącego dwa przełączniki ATM. Dynamiczny routing jest w środowisku ATM realizowany przez Private NNI (P-NNI) wersja 1.0. P-NNI opiera się na hierarchicznej strukturze podmiotów dołączonych do sieci i pracuje podobnie jak klasyczne protokoły routingu IP, np. OSPF (*Open First Path First*). P-NNI pozwala przełącznikom wyznaczać marszruty wirtualnych połączeń SVC, wybierać najlepszą z możliwych ścieżek i w przypadku uszkodzenia jednego z połączeń kierować inną drogą strumień komórek do stacji przeznaczenia. Każdy przełącznik powinien bezwzględnie wspierać dwie specyfikacje: UNI (w wersji 3.0, 3.1 lub najnowszej – 4.0) i P-NNI.

Można wymienić trzy podstawowe usługi pozwalające sprzęgać sieci LAN z przełącznikami ATM: Classical IP (RFC-1577), LANE 1.0 i Multiprotocol over ATM (MPOA).

(jch)

Technologia MPOA



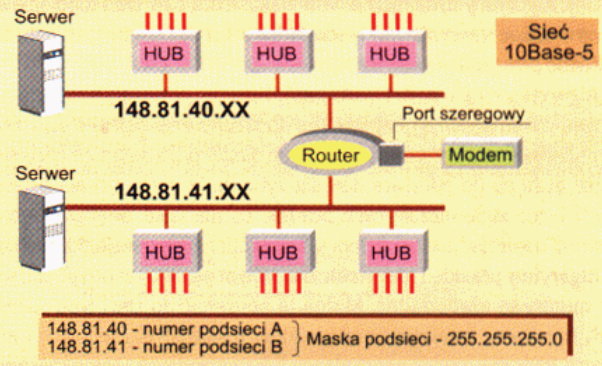
Classical IP i LANE opierają na koncepcji zakładającej, że klienci inicjują połączenia, korzystając z usług specjalnych serwerów (oprogramowanie). Serwery takie dysponują bazami danych zawierającymi informacje (adresy ATM i LAN oraz mechanizm mapowania tych adresów) o wszystkich stacjach dołączonych do sieci ATM. Jeśli klient chce nawiązać łączność z konkretną stacją LAN, to wysyła do serwera jej adres. Następnie serwer dostarcza klientowi stosowny adres ATM tej stacji, który jest wykorzystywany do złożenia łącza sprzęgającego dwie stacje. Różnica między Classical IP i LANE polega na tym, że ten pierwszy protokół (jak wskazuje zresztą sama nazwa) obsługuje wyłącznie sieci IP, podczas gdy LANE może być użyte do sprzęgania z łączem ATM stacji opartych na innych niż IP technologiach. O protokołach LANE czy Classical IP można zapomnieć wtedy, gdy zamierzamy eksploatować sieć opartą wyłącznie na technologii ATM (np. szybko pracująca sieć szkieletowa WAN). Ale jest to bardzo rzadki przypadek.

Routery

Węzły sieci operujące w trzeciej (sieciowej) warstwie modelu OSI noszą nazwę routerów. Są to urządzenia wyposażone najczęściej w kilka interfejsów sieciowych LAN, porty obsługujące sieci WAN, pracujący wydajnie procesor i specjalne oprogramowanie zawiadujące ruchem pakietów przepływających przez router. Chociaż routerem może też być zwykły komputer dysponujący kilkoma kartami sieciowymi i specjalnym oprogramowaniem, to jest to najczęściej dedykowany komputer, dysponujący rozwiązaniami znacznie zwiększającymi wydajność tego rodzaju węzłów sieci.

Routery są stosowane zarówno w sieciach LAN, jak i WAN. W sieciach LAN (**routery lokalne**) są używane wtedy, gdy system chcemy podzielić na dwie lub więcej podsieci, czyli poddać operacji segmentowania. Segmentacja sieci powoduje, że poszczególne podsieci są od siebie odseparowane i pakiety (zarówno *Point-to-Point*, jak i *multicast* czy *broadcast*) nie przenikają z jednej podsieci do drugiej. Korzyść jest oczywista: w ten sposób zwiększamy przepustowość każdej z podsieci.

Router sprzęga podsieci A i B oraz łączy sieć LAN ze światem zewnętrznym (port szeregowy i modem)



Jak sama nazwa wskazuje (ang. *route* to trasa), routery wyznaczają pakietom marszruty, kierując je do odpowiedniego portu lub karty sieciowej. Routery nie interesują się adresami MAC (w przypadku sieci Ethernet jest to 48-bitowa liczba przypisywana każdej karcie sieciowej), a po odebraniu pakietu odczytują i poddają analizie adres budowany w obszarze warstwy sieciowej. W sieciach Internet będzie do adres IP przypisywany przez administratora każdemu ze stanowisk pracy. Adres taki składa się zawsze z dwóch części: jedna definiuje adres sieci, a druga adres komputera pracującego w tej sieci. I tak np. numer 148.81.40.10 oznacza (zakładając, że administrator zdefiniował dodatkowo maskę podsieci 255.255.255.0), że stacja docelowa jest zainstalowana w sieci 148.81.40, a jej numer to 10. Ponieważ routery służą do sprzęgania różnych sieci komputerowych (czyli takich, którym przypisano inne adresy definiujące numer sieci), to do routera zostaną wysłane tylko te pakiety, które są kierowane do innych sieci. Żaden pakiet oznaczony numerem 148.81.10.X nie trafi do routera, ponieważ stacja docelowa pracuje w tej samej sieci, a nie na zewnątrz.

Wybrani producenci routerów

3Com	**Intel**
Bay Networks	**Lucent Technologies**
Cabletron Systems	**Olicom**
Cisco Systems	**Newbridge Networks**
Compex	**RND Networks**
Gandalf Technologies	**Xyplex Networks**
Hewlett-Packard	**ZyXEL Communications Corp**
IBM	

Inną rolę pełnią **routery dostępowe,** czyli sprzęgające sieć LAN ze światem zewnętrznym. W tym przypadku nie chodzi już o segmentację sieci LAN na mniejsze domeny rozgłoszeniowe, ale o zainstalowanie węzła sieci ekspediującego przez łącze WAN pakiety generowane przez pracujące w sieci LAN stacje do innego routera pracującego po drugiej stronie tego łącza. Oczywiście, może się zdarzyć i tak, że jeden router obsługuje zarówno pakiety lokalne, jak i te kierowane na zewnątrz.

Routery zakładają tabele routingu i mają zdolność „uczenia się" topologii sieci, wymieniając informacje z innymi routerami zainstalowanymi w sieci. Ponieważ prawie wszystkie operacje związane z odbieraniem i ekspediowaniem pakietów do odpowiedniego portu są realizowane w routerze przez oprogramowanie, to tego rodzaju węzły sieci pracują dużo wolniej niż np. przełączniki.

Protokoły trasowania wyznaczają pakietom marszruty opierając się na różnych algorytmach. Mogą to być algorytmy statyczne lub dynamiczne, *single path* lub *multi path*, płaskie lub hierarchiczne, *host intelligent* lub *router intelligent*, *intradomain* lub *interdomain* i opierające się na technologii *link state* lub *distance vector*.

Algorytmy trasowania

Algorytmy statyczne i dynamiczne. Algorytm statyczny nie jest właściwie algorytmem. Wszystkie drogi routingu wyznacza tu bowiem na stałe sam administrator systemu. Jeśli topologia sieci zmieni się, router jest po prostu bezsilny. Algorytmy dynamiczne natomiast śledzą cały czas topologię sieci (praca w czasie rzeczywistym) i modyfikują w razie potrzeby tabele routingu zakładane przez router.

Algorytmy *single path* i *multi path*. Niektóre protokoły trasowania wyznaczają pakietom kilka dróg dostępu do stacji przeznaczenia, czyli wspierają multipleksowanie. I tak jak algorytm *single path* definiuje tylko jedną ścieżkę dostępu do adresata, tak algorytm *multi path* pozwala przesyłać pakiety przez wiele niezależnych ścieżek, co nie tylko zwiększa szybkość transmisji pakietów, ale też chroni system routingu przed skutkami awarii.

Algorytmy płaskie i hierarchiczne. W tym pierwszym przypadku wszystkie routery są równorzędne. Można to porównać do sieci typu „peer-to-peer". Nie ma tu (ze względu na strukturę logiczną) ważniejszych i mniej ważnych routerów czy też nadrzędnych lub podrzędnych. Algorytmy hierarchiczne postrzegają sieć jako strukturę zhierarchizowaną, dzieląc ją na domeny. Pakietami krążącymi w obrębie każdej domeny zawiaduje wtedy właściwy router, przekazując je routerowi nadrzędnemu lub podrzędnemu.

Algorytmy *host intelligent* i *router intelligent*. Niektóre algorytmy zakładają, że całą drogę pakietu do stacji przeznaczenia wyznaczy od razu stacja nadająca. Mamy wtedy do czynienia z trasowaniem źródłowym (*source routing*, czyli *host intelligent*). W tym układzie router pełni tylko rolę „przekaźnika" odbierającego pakiet i ekspediującego go do następnego miejsca. W algorytmach *router intelligent* stacja wysyłająca nie ma pojęcia, jaką drogę przemierzy pakiet, zanim dotrze do adresata. Obowiązek wyznaczenia pakietowi marszruty spoczywa na routerach.

Algorytmy *intradomain* i *interdomain*. Algorytmy trasowania *intradomain* operują wyłącznie w obszarze konkretnej domeny, podczas gdy algorytmy *interdomain* zawiadują pakietami biorąc pod uwagę nie tylko zależności zachodzące w ramach konkretnej domeny, ale też powiązania między tą domeną i innymi, otaczającymi ją domenami. Optymalne marszruty wyznaczane przez algorytm *intradomain* nie muszą być (i najczęściej nie są) najlepsze, jeśli porównamy je z optymalnymi marszrutami wypracowanymi przez algorytm *interdomain* („widzący" całą strukturę sieci).

Algorytm *link state* i *distance vector*. Algorytm *link state* (znany jako *shortest path first*) rozsyła informacje routingu do wszystkich węzłów obsługujących połączenia międzysieciowe. Każdy router wysyła jednak tylko tę część tabeli routingu, która opisuje stan jego własnych łączy. Algorytm *distance vector* (znany też pod nazwą *Bellman-Ford*) wysyła w sieć całą tabelę routingu, ale tylko do sąsiadujących z nim routerów. Mówiąc inaczej, algorytm *link state* rozsyła wszędzie, ale za to niewielkie, wybrane porcje informacji, podczas gdy *distance vector* rozsyła komplet informacji, ale tylko do najbliższych węzłów sieci. Każdy z algorytmów ma swoje wady i zalety. *Link state* jest skomplikowany i trudny do konfigurowania oraz wymaga obecności silniejszego procesora CPU. Odnotowuje za to szybciej wszelkie zmiany zachodzące w topologii sieci. *Distance vector* nie pracuje może tak stabilnie, ale jest za to łatwiejszy do implementowania i sprawuje się dobrze w dużych sieciach składających się z kilkudziesięciu czy nawet kilkuset routerów.

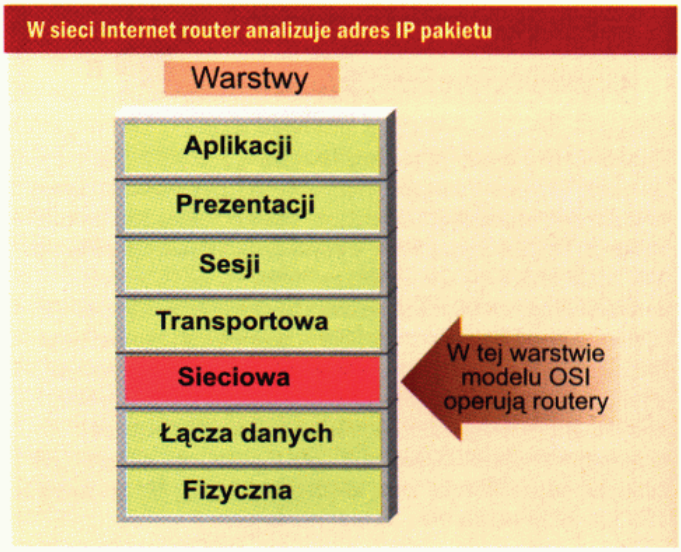
Po odebraniu pakietu i odczytaniu adresu IP stacji docelowej (sieć TCP/IP) router musi zawsze wyekspediować go na zewnątrz. Jeśli stacja docelowa jest zlokalizowana w innej sieci czy podsieci LAN dołączonej do routera, to sprawa jest prosta – router dołącza do takiego pakietu adres MAC tej stacji (pobierając go z tabeli ARP) i wysyła do określonej karty sieciowej. Jeśli jednak stacja docelowa znajduje się w zupełnie innej sieci LAN, to router musi go opakować w specjalną „kopertę" (czyli posłużyć się odpowiednim protokołem routingu) i przesłać do innego routera. Nie należy przy tym mylić dwóch pojęć: protokołu używanego do trasowania pakietów (*routing protocol*) i protokołów obsługiwanych przez router (*routed protocol*). Router może np. obsługiwać tylko sieć Internet i wtedy potrafi wyznaczać marszruty pakietom generowanym przez protokół IP. Istnieją też routery wieloprotokołowe, które potrafią obsługiwać pakiety generowane przez kilka różnych protokołów, np. przez dwa protokoły: IP i IPX.

Protokoły trasowania

Jeśli chodzi o protokoły używane do trasowania pakietów i komunikowania się z innymi routerami (oraz do modyfikowania i zarządzania tabelami routingu), to można wymienić sześć podstawowych protokołów:

- RIP (*Routing Information Protocol*),
- IGRP (*Interior Gateway Routing Protocol*),
- Enhanced IGRP,
- OSFP (*Open Shortest Path First*),
- IS-IS (*Integrated Intermediate System-to-System*)
- Routing statyczny.

Największą popularnością cieszą się protokoły OSFP (RFC 1247) i RIP (1058).



Należący do protokołów grupy Distance Vector Protokół RIP pracuje w ten sposób, że router rozsyła do innych routerów pracujących w sieci całą tabelę routingu lub tę jej część, która została zmieniona. Informacja RIP jest transmitowana przy użyciu dwóch protokołów IP i UDP. Parametr Metric definiuje liczbę skoków (*hop count*), jaką pokonuje, zanim dotrze do celu. Jeśli w polu Metric pojawi się liczba 16, to znaczy, że stacja docelowa jest niedostępna. Routery odbierają informację RIP i na jej podstawie wyznaczają pakietom najkrótszą drogę do stacji przeznaczenia. Informacje RIP są rozsyłane po sieci w regularnych odstępach czasu, najczęściej co 30 sekund. Ich odbieraniem i przetwarzaniem zajmują się w unixowych węzłach sieci *demony* (specjalne programy), które śledzą cały czas dane nadsyłane do portu (mowa o oprogramowaniu) oznaczonego numerem 520.

Protokół RIP

Pole	Bajtów	Typowa wartość
Polecenie	1	1. Żądanie 2. Odpowiedź 3. Obsolete 4. Obsolete 5. Poll 6. Poll entry
Wersja	1	1 lub 2
Zarezerwowane	2	Zera
Adres rodziny	2	2 dla adresów IP
Zarezerwowane	2	Zera
Adres IP	4	Adres stacji
Zarezerwowane	8	Zera
Metric	4	Od 1 do 16

Protokół OSPF

Pole	Bajtów	Typowe wartości
Wersja	1	2
Typ pakietu	1	1. Hello 2. Database 3. Link state (żądanie) 4. Link State (update) 5. Link State (potwierdzenie)
Długość pakietu	2	Długość pakietu w bajtach
ID (router)	4	Adres IP nadawcy
ID (obszar)	4	Adres obszaru
Suma kontrolna	2	Wyliczona suma kontrolna
Typ identyfikacji	2	1. Brak
		2. Proste hasło
Identyfikacja (dane)	8	Dane identyfikacyjne

OSFP należy do protokołów LSP (*Link State Protocol*). Pracuje w ten sposób, że każdy router zbiera informacje o aktualnym stanie połączeń w sieci i rozsyła je do innych routerów, które wykorzystują je do aktualizowania swoich tabel routingu. Protokoły trasowania LSP wyznaczają pakietom marszruty posiłkując się algorytmem Dijsktry i wymagają obecności silniejszych procesorów niż protokoły oparte na technologii DV (*Distance Vector*). Inaczej niż RIP, OSFP posługuje się bezpośrednio protokołem IP, a pakiety OSFP są rozpoznawane dzięki temu, że protokół wstawia do jednego z pól (*protocol field*) datagramu IP określoną wartość.

Różne wydajności

W sieciach szkieletowych instaluje się routery o **najwyższej wydajności** (klasy *high end*), które powinny wspierać wszystkie rodzaje interfejsów używanych w sieciach LAN i WAN oraz obsługiwać maksymalnie dużo protokołów transportu i trasowania (nawet tych rzadko używanych). Niektóre routery z tej grupy są w stanie obsłużyć nawet do 50 portów.

Routery **średniej mocy** są najczęściej używane w sieciach korporacyjnych do łączenia się z serwerami zainstalowanymi w sieciach bazowych. Mogą one też służyć do budowy sieci bazowych w mniejszych przedsiębiorstwach. Typowy router tej klasy składa się z dwóch do trzech portów sieci LAN oraz z czterech do ośmiu portów sieci WAN.

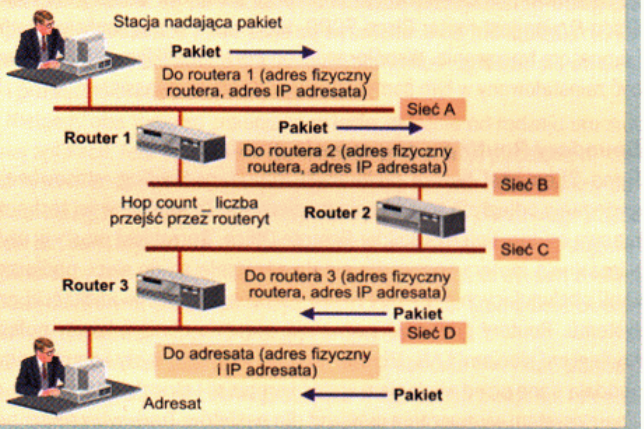
No i wreszcie **routery oddziałowe**, które łączą mało obciążone sieci LAN z resztą firmy. Są one z reguły wyposażone w jeden port LAN (obsługujący sieć Ethernet lub Token Ring) i dwa porty WAN małej szybkości, obsługujące łącza dedykowane lub komutowane. Są to chyba najczęściej kupowane routery, gdyż pozwalają stosunkowo niewielkim kosztem rozbudować sieć komputerową czy łączyć odległe biura i oddziały firmy z centralą.

Architektury routerów instalowanych w sieciach szkieletowych i routerów oddziałowych różnią się zasadniczo, ponieważ urządzenia te pełnią inne funkcje. Pierwsze dają się łatwo rozbudowywać i po ponownym skonfigurowaniu dostosowywać do nowych warunków pracy. Muszą one dysponować dużą przepustowością i są wyposażane w szybko pracujące procesory i interfejsy oraz w oprogramowanie, które potrafi automatycznie optymalizować ruch pakietów krążących po sieci. Obsługują wiele protokołów transportu w sieciach LAN i WAN, od protokołu sieci Arcnet do protokołu X.25. Zupełnie inaczej jest z routerami oddziałowymi. Są to najczęściej urządzenia wyposażone na stałe w kilka portów i jeden procesor zarządzający pracą trzech do czterech interfejsów. I chociaż mogą one obsługiwać te same protokoły co router bazowy, to ich oprogramowanie jest stosunkowo proste. Wykonuje ono bowiem nieskomplikowane, rutynowe operacje przesyłania pakietów między określonymi portami.

Routery i ATM

Wielu czołowych producentów routerów wprowadza do produkowanych przez siebie urządzeń technologię ATM. I tak np. firma Newbridge buduje routery architektury VIVID (*Video, Voice, Image and Data*), która pozwala wyposażać je w interfejsy sieci ATM. Technologia VIVID jest oparta na pracy trzech produktów: VIVID Route Server, VIVID Ridge i VIVID Workgroup Switch. VIVID Route Server jest programem ładowanym na komputery pracujące pod systemem Unix. Najważniejszym elementem tej architektury jest VIVID Ridge, który poddaje pakiety sieci Ethernet lub Token Ring (sieci przesyłające pakiety w trybie bezpołączeniowym) konwersji na komórki sieci ATM (tryb łącza bezpośredniego). Następnie jest uruchamiany pakiet VI-

Router sprzęga podsieci A i B oraz łączy sieć LAN ze światem zewnętrznym (port szeregowy i modem)



Zanim pakiet dotrze od adresata, może być obsługiwany przez wiele routerów. Liczbę routerów mierzy się parametrem *hop count*. Jest to nic innego jak miara efektywności drogi w sieciach opartych na routerach. Jedno przejście przez router to jeden *hop* (skok). Aby określić długość drogi, routery wymieniają między sobą okresowo informacje o przebiegu pakietów, mierząc jednocześnie efektywność poszczególnych tras. Pakiet (na rysunku) przechodzi przez trzy routery, dlatego parametr *hop count* dla tej trasy równa się 3.

Porównanie technologii

Cecha	Routery	Mosty	Przełączniki
Łatwość instalacji i konfigurowania	Trudne w konfigurowaniu	Łatwe w konfigurowaniu	Łatwe w konfigurowaniu
Bezpieczeństwo pracy	Filtrowanie pakietów wyższych warstw (np. SMTP czy FTP)	Filtrowanie adresów warstwy MAC	Brak filtrowania
Sposób trasowania pakietów	Skomplikowane algorytmy trasowania	Użycie algorytmu STA zapobiega powstawaniu pętli ramek	Brak mechanizmów trasowania
Interfejsy sieci LAN	Ethernet, Fast Ethernet, FDDI, ATM, TR, GE	Nie obsługują sieci wysokich szybkości	Ethernet, Fast Ethernet, FDDI, ATM, TR, GE
Wsparcie dla ATM	Dostępne	Niedostępne	Dostępne

Routery pracują dużo wolniej niż przełączniki, ale mają w porównaniu z tymi ostatnimi wiele zalet. Wiele routerów najnowszej generacji potrafi nie tylko trasować, ale też przełączać pakiety. Wbrew wcześniejszym przewidywaniom, mówiącym, że przełączniki przyczynią się do definitywnego wyrugowania routerów z architektury sieci komputerowych, nic takiego nie nastąpiło. W wielu wypadkach routery są nadal niezastąpione, szczególnie w sieciach rozległych, które leżą poza zasięgiem przełączników. Gwałtowny rozwój technologii (sprzętu i oprogramowania) spowodował, że producenci budują węzły sieci (konstrukcja modularna; w urządzeniu takim można w każdej chwili zainstalować dodatkową kartę czy moduł), które są prawdziwymi "kombajnami", integrującymi różne sposoby zawiadywania pakietami krążącymi po sieciach LAN/WAN: routing, mostowanie, przełączanie i najnowszą technologię IP Switching (korzystającą nieraz z usług łączy ATM).

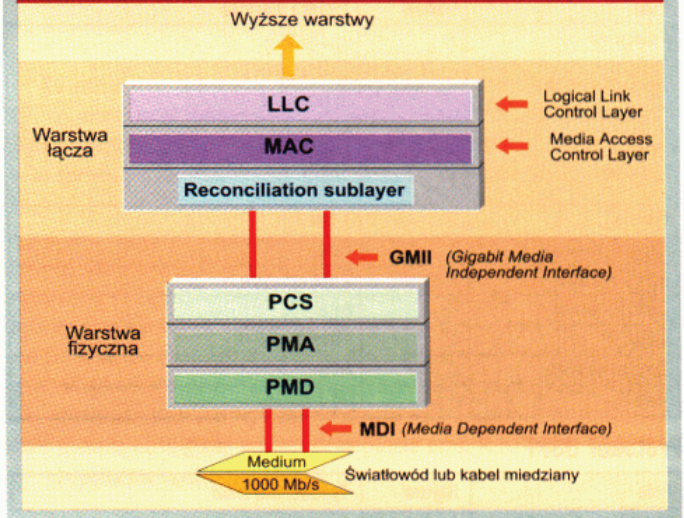
VID Route Server, który wyznacza optymalną marszrutę dla pakietów przesyłanych na linii LAN – LAN i LAN – ATM. VIVID Workgroup Switch jest natomiast wieloportowym przełącznikiem matrycowym obsługującym ruch komórek sieci ATM. Tak więc systemy architektury VIVID wykonują zadania trasowania i przełączania pakietów.

Cisco używa architektury podobnej do VIVID. Nosi ona nazwę *Cisco Fusion* i też składa się z trzech części: procesora interfejsu (który łączy sieci LAN lub WAN), procesora marszrut, posiłkującego się protokołami trasowania RIP, OSPF, RTMP (*Routing Table Maintenance Protocol* – protokół stosowany przez sieci AppleTalk) i innymi, oraz z procesora przełączania, którego zadaniem jest przełączanie i transmisja pakietów. Częścią architektury *Cisco Fusion* jest router Cisco 7000, który pełni w niej funkcję interfejsu i procesora trasowania. Współpracuje on z przełącznikiem ATM, który może być zainstalowany w tym samym lub w oddzielnym chassis.

Boundary Routing – trasowanie graniczne

Firma 3Com jest twórcą technologii *Boundary Routing*, stosowanej do sprzęgania odległych biur z siecią macierzystą. To właśnie w tej technologii pracują routery linii NETBuilder Remote Office. Sprzęt jest prosty w użyciu, a instalacja routera sprowadza się do włączenia go do sieci, podłączenia kabli obsługujących sieci LAN i WAN i włożeniu dyskietki inicjującej pracę systemu. Routery graniczne pozwalają znacznie obniżyć koszty połączeń z odległymi sieciami LAN. Używają one do tego celu łączy komutowanych, poddają dane przed wysłaniem w sieć kompresji i stosują swój własny, oryginalny system wyznaczania marszrut dla pakietów. Tradycyjny router przejmuje na siebie wszystkie zadania związane z wyznaczaniem marszrut dla odbieranych pakietów. Przy trasowaniu granicznym łączy się on z zainstalowanym w odległej sieci bazowej routerem przez port WAN, który przesyła pakiety zgodnie z protokołem podobnym do *Point-to-Point Protocol* (jest to protokół rodziny IP używany przy przesyłaniu pakietów przez łącza komutowane). I to właśnie router bazowy podejmuje decyzje związane z wyznaczaniem marszrut dla pakietów. Zarówno sieć bazowa, jak i odległa sieć LAN są traktowane jako jeden spójny organizm. Mówiąc inaczej, router sieci bazowej traktuje odległe biuro jako jeden ze swoich portów WAN. W układzie tym obu portom routerów (bazowemu i pracującemu w odległej sieci LAN) jest przypisywany ten sam adres protokołu IP. Widać więc, że router graniczny (pracujący w odległej sieci) jest urządzeniem stosunkowo prostym i dlatego niedrogim. Po odebraniu pakietu musi on podjąć tylko jedną decyzję: odesłać go z powrotem do sieci LAN (jeśli tam znajduje się stacja przeznaczenia) czy przesłać do routera bazowego, który podejmuje decyzję, co z nim dalej robić. Routery graniczne obsługują też sieci Frame Relay, filtrują pakiety, poddają je kompresji i przyznają im różne poziomy priorytetu. Inne możliwe rozwiązania to: automatyczne nawiązywanie łączności przez zapasowe łącze komutowane (w przypadku awarii podstawowego) czy rezerwowanie określonej przepustowości łącza na zgłoszone żądanie.

Architektura protokołów Gigabit Ethernet



Minimalna długość ramki Ethernet wynosi 64 bajty. Ograniczenie to jest konieczne – stacja ekspediująca w sieć ramkę nie może bowiem zakończyć swej aktywności, zanim pierwszy bit ramki nie dotrze do stacji docelowej. Wynika to z prostego założenia – minimalny czas potrzebny na wykrycie kolizji jest czasem, w jakim sygnał przemierza cały odcinek łącza. Ten minimalny czas jest nazywany *Slot Time* (szczelina, którą można zdefiniować w mikrosekundach; można też podać liczbę bajtów – *Slot Size* – przesłanych w danym przedziale czasu przez sieć Ethernet). W sieciach Ethernet parametr *Slot Size* wynosi 64 bajty i długość ramki nie może zejść poniżej tej wartości. Maksymalna długość całego łącza w sieci Ethernet wynosi 2,5 km (pięć odcinków połączonych ze sobą czterema wzmacniakami). Wraz ze wzrostem szybkości transmisji danych (mierzonej w bitach na sekundę) jest rzeczą oczywistą, że czas potrzebny na przesłanie ramki ulega skróceniu. Jeśli długość ramki (przy zachowaniu tej samej długości łącza) nie ulega zmianie, to stacja nadająca dane robi to tak szybko, że nie jest w stanie wykrywać kolizji. Aby nie dopuścić to tego, należy wykonać jedną z dwóch operacji – zwiększyć parametr *Slot Time* (czyli zwiększyć minimalną długość ramki) lub obniżyć długość łącza. W sieci Fast Ethernet maksymalną długość łącza obniżono do 100 m, dzięki czemu parametr *Slot Size* (minimalna długość ramki) pozostał taki sam jak w sieci Ethernet. W przypadku sieci Gigabit Ethernet należałoby zmniejszyć długość łącza do 10 m, jeśli chcielibyśmy pozostawić taką samą, minimalną długość ramki (64 bajty). Nie wchodziło to oczywiście w grę, gdyż łącze o maksymalnej długości 10 m nie zadowala nikogo. Pozostało więc rozwiązanie polegające na zwiększeniu minimalnej długości ramki – parametr *Slot Size* wynosi w sieci Gigabit Ethernet 512 bajtów. Projektanci tej sieci chcieli jednak, aby technologia była kompatybilna z Ethernetem i Fast Ethernetem. Dlatego zdecydowano się nie zmieniać (w danym przypadku nie zwiększać) parametru definiującego minimalną długość ramki (czy też, mówiąc konkretnie, obszaru zajmowanego przez pola: SFD, DA, SA, typ/długość i DANE), a posłużyć się rozszerzeniem „Carrier Event". Dzięki takiej operacji minimalna długość obszaru zajmowanego przez dane i bity kontrolne pozostała w sieciach Ethernet, Fast Ethernet i Gigabit Ethernet taka sama – 64 bajty.

Ethernet 10, 100 i 1000 Mb/s

Routery najnowszej generacji pracują bardzo szybko, nie tylko dlatego, że tak efektywnie trasują pakiety, ale również dlatego, że za partnera mają media pracujące 10 lub nawet 100 razy szybciej niż tradycyjne rozwiązania. Chodzi tu o technologię Ethernet, dlatego uwaga ta dotyczy tych routerów, które są instalowane wewnątrz sieci LAN (sprzęgają ze sobą różne podsieci), a nie routerów kierujących pakiety do sieci rozległych. Żadna z technologii stosowanych do budowania sieci LAN nie zrobiła takiej kariery jak Ethernet. Szacuje się, że w 1996 roku 83 proc. sprzętu sieciowego pracowało w tej właśnie technologii. W 1995 roku komitet IEEE zaakceptował kolejną odmianę Ethernetu – standard Fast Ethernet. Sieci oparte na tej technologii transmitują pakiety dziesięć razy szybciej (100 Mb/s) i oferują szereg nowych opcji, takich jak praca w trybie pełnego dupleksu czy usługa autodetekcji (czyli automatycznego rozpoznawania rodzaju technologii zastosowanej przez konkretne łącze – może to być Ethernet lub Fast Ethernet). Obecnie mamy do czynienia z technologią, dzięki której sieć LAN może pracować sto razy szybciej niż poczciwy Ethernet. Gigabit Ethernet – 1000 Mb/s.

Warstwa MAC sieci Gigabit Ethernet używa tego samego protokołu dostępu do medium (CSMA/CD) co klasyczny Ethernet. Maksymalna długość jednego segmentu sieci sprzęgającego dwie stacje jest tu ograniczona do wartości narzuconej przez CSMA/CD.

(jch)

Serwery

Pojęcie **serwer** należy zawsze rozpatrywać w kontekście architektury **klient/serwer**. Tam gdzie jest serwer, tam bezwzględnie musi też być klient. Serwer jest więc takim elementem instalowanym w sieci komputerowej, który świadczy klientom określone usługi. Celowo użyto tu słowa element, gdyż pod nazwą serwer może się kryć zarówno komputer dysponujący określonymi urządzeniami (a więc sprzęt), jak i oprogramowanie. Mamy więc pierwszy podział – konkretne rozwiązanie sprzętowe lub program świadczący specyficzny rodzaj usług.

Rodzaje serwerów

Rozróżniamy całą gamę serwerów: serwery aplikacji, terminali, plików, zarządzające bazami danych, webowe, drukowania, zdalnego dostępu i wiele innych. Jak już wspomniano, pod pojęciem serwer może się kryć zarówno sprzęt, jak i oprogramowanie. Serwerem zdalnego dostępu może być specjalistyczny program zainstalowany na komputerze ogólnego przeznaczenia lub komputer (czyli sprzęt, któremu towarzyszy odpowiednie oprogramowanie) realizujący wyłącznie to zadanie. W tym momencie mamy do czynienia z dedykowanym serwerem, a więc takim, który wykonuje wyłącznie przypisane mu z góry zadanie. Z drugiej strony może się też zdarzyć tak, że w pamięci jednego komputera uruchomiono kilka programów pełniących rolę serwerów (np. serwer webowy i serwer DNS).

Serwer zainstalowany w sieci (mowa o sprzęcie) pełni najczęściej rolę serwera plików, aplikacji, bazy danych lub świadczy swe usługi przeglądarkom, czyli jest serwerem webowym. Odpowiednie połączenie rozwiązań sprzętowych z konkretnym systemem operacyjnym powoduje, że jeden komputer nadaje się lepiej do pełnienia roli serwera plików, a inny serwera aplikacji. Wiadomo np., że najwydajniejszymi serwerami plików są komputery pracujące pod systemem operacyjnym NetWare, Windows NT natomiast nadaje się do zarządzania serwerami aplikacji.

Serwer plików

Serwer plików to komputer świadczący usługi wymagające częstego dostępu do plików. W porównaniu ze zwykłą stacją roboczą serwer plików powinien dysponować wieloma pojemnymi dyskami twardymi, dużą pamięcią RAM i szybko pracującą magistralą danych. Serwery plików najwyższej klasy dysponują dodatkowymi rozwiązaniami, które zwiększają ich szybkość, niezawodność i bezpieczeństwo pracy. Mogą to być np. elementy redundancyjne (dyski twarde, zasilacze, wentylatory, a nawet procesory), które wkraczają do akcji w momencie awarii elementu podstawowego. Niekiedy serwer taki dysponuje nawet zapasową kartą sieciową, nie mówiąc już o powszechnie dzisiaj stosowanej technologii *hot-swapping* (możliwość wymiany elementu bez konieczności wyłączania serwera z eksploatacji).

Serwer plików jest więc pojemnym repozytorium danych, które mogą być współdzielone przez wielu użytkowników. Zależnie od zastosowanego systemu operacyjnego rozróżniamy dedykowane i nie dedykowane serwery plików. I tak np. po zainstalowaniu systemu NetWare mamy do czynienia z serwerem dedykowanym (CPU nie może wykonywać innych zadań niż te związane z realizacją zadań zleconych mu przez serwer plików). Ograniczenie to można w jakiś sposób obejść, uruchamiając na komputerze moduły NLM realizujące inne zadania. Ponieważ systemy Windows NT i OS/2 LAN Server pracują w trybie *multiprocessing*, to pracujące pod nimi serwery plików są serwerami nie dedykowanymi.

Serwer aplikacji

Serwery aplikacji są komputerami, w pamięci których zainstalowano określony rodzaj aplikacji, np. program zarządzający bazą danych. Serwery aplikacji pracują najczęściej pod systemami działającymi w trybie *multiuser* (np. Unix czy OS/2), czyli mogącymi świadczyć swe usługi jednocześnie wielu użytkownikom. Wiele serwerów aplikacji zleca wykonywanie niektórych zadań klientom. I tak np. serwer bazy danych wyszuka i przetworzy określone informacje, ale interfejs wyświetlający je jest zainstalowany w pamięci klienta. Ogranicza to w znacznym stopniu ruch pakietów krążących po sieci.

Serwer komunikacyjny

Jest to specyficznego rodzaju serwer sprzęgający zdalnych użytkowników z siecią LAN. Serwer taki dysponuje wieloma portami komunikacyjnymi współpracującymi z modemami analogowymi lub cyfrowymi. Całością zarządza, oczywiście, specjalne oprogramowanie, które odbiera dane z łączy komutowanych (lub dedykowanych) i przekazuje je po odpowiednim przetworzeniu do sieci LAN. Podobny proces ma miejsce przy przesyłaniu danych w drugą stronę.

Konfiguracja serwera komunikacyjnego zależy od tego, w jakim trybie jest realizowany zdalny dostęp. Może to być tryb zdalnego sterowania (*remote control mode*) lub tryb zdalnego dostępu (*remote node mode*). Przykładem użytkownika pracującego w trybie zdalnego sterowania jest korzystający z peceta wyposażonego w modem i oprogramowanie pcanywhere lub Reachout. Dane są po naciśnięciu klawisza przesyłane do odległego komputera, a odbierane informacje są wyświetlane na monitorze. Tryb *remote node access* pozwala odległemu użytkownikowi zgłaszać się do sieci LAN i prowadzić pracę jak lokalny użytkownik.

Niekiedy oba tryby są zmieniane w locie, zależnie od rodzaju uruchomionej aplikacji. Jeśli użytkownik uruchamia np. aplikację pocztową (*e-mail*), to system zdalnego dostępu pracuje w trybie *remote node* (zdalny dostęp do odległego węzła, w tym przypadku do serwera pocztowego). Jeśli jednak ten sam użytkownik zechce skorzystać z usług aplikacji obsługiwanej przez silny komputer zainstalowany w odległej sieci, to system zdalnego dostępu zaczyna pracować w trybie *remote control* (zdalne sterowanie zadaniem realizowanym przez odległy komputer).

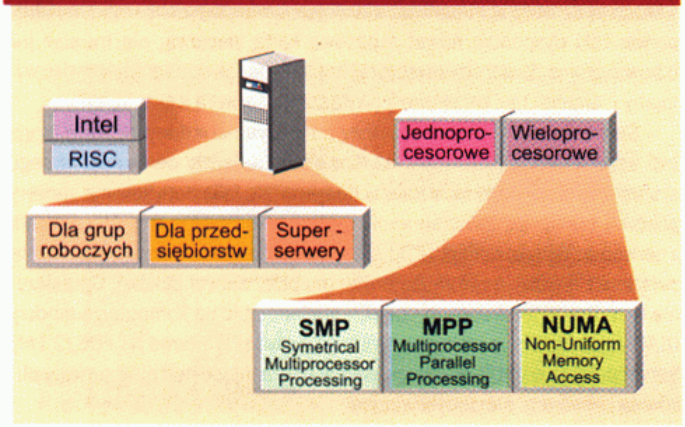
Z usług serwerów zdalnego dostępu mogą obecnie korzystać wszyscy: odległe biura, lokalne sieci LAN pracujące w sąsiednim budynku, telepracownicy (praca w domu) czy użytkownik notebooka podłączonego do gniazdka telefonicznego w pokoju hotelowym.

Serwery w sieci

Serwer sieciowy jest dedykowanym systemem komputerowym wydzielonym w sieci celem świadczenia określonych usług. To, jakie to będą usługi, zależy już od oprogramowania zainstalowanego w pamięci serwera.

Rolę serwera w sieci może od biedy pełnić podrasowany pecet. Jednak mało kto tak postępuje, ponieważ to się po prostu nie opłaca. Serwer de-

Rodzaje serwerów



dykowany dysponuje szeregiem rozwiązań, których nigdy nie znajdziemy w komputerze osobistym.

Ze względu na wydajność serwery można podzielić z grubsza na trzy grupy (z grubsza, bo czasami bardzo trudno jest powiedzieć, do której grupy dany serwer należy zaliczyć):

- serwery do obsługi grup roboczych,
- serwery dla przedsiębiorstw,
- superserwery.

Serwery zaliczane do pierwszej grupy realizują mniej wymagające zadania i nie muszą dysponować tak dużą mocą obliczeniową jak serwery świadczące usługi całemu przedsiębiorstwu, czyli bardzo dużej (liczonej nieraz w setki) liczbie stanowisk pracy. Na serwerach dla przedsiębiorstw są z reguły uruchamiane kluczowe aplikacje (nazywane też krytycznymi), od których zależy prawidłowe funkcjonowanie całej firmy. Dlatego serwer dla przedsiębiorstw musi nie tylko pracować bardzo wydajnie, ale też niezawodnie. Stąd w tej grupie serwerów znajdziemy cały szereg rozwiązań nazywanych nadmiarowymi. Mówiąc prościej, chodzi o to, że wiele elementów serwera jest dublowanych – jeśli jeden z elementów ulega awarii, to jego zadanie przejmuje element zapasowy. Superserwery są używane do specjalnych zadań, przetwarzając dane wielokrotnie szybciej niż serwery zaliczane do dwóch poprzednich kategorii.

Jaka magistrala?

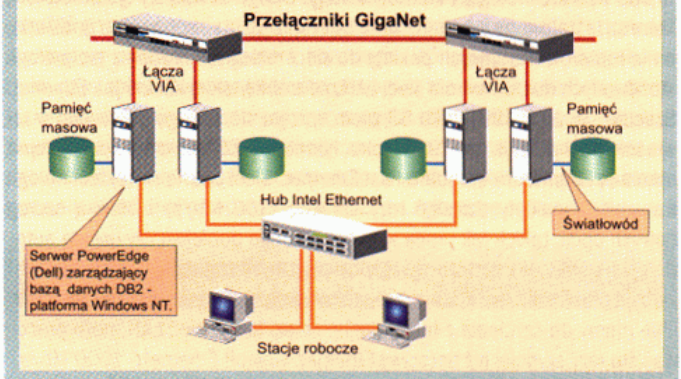
Jak wiadomo, serwer komunikuje się ze światem zewnętrznym przez kartę sieciową. Im szybsza sieć, tym szybciej pracuje karta. Serwer musi więc dysponować taką szyną danych, która zapewnia odpowiednio wysoką przepustowość. Serwer wyposażony w popularną szynę danych ISA może wysyłać i odbierać dane z sieci z maksymalną szybkością rzędu 10–25 Mb/s. Konfiguracja taka może zdać egzamin w przypadku współdzielonego Ethernetu, ale serwer z szyną ISA nie nadąży już za kartą Fast Ethernet. Dlatego serwery są wyposażane w szynę PCI i EISA. Przepustowości różnego rodzaju szyn danych instalowanych w serwerach podano w tabeli.

Serwery do obsługi grup roboczych dysponują szynami EISA lub PCI, są wyposażone w wysokiej klasy procesory (np. Pentium Pro, a wprowadzane ostatnio na rynek serwery tej klasy najczęściej dysponują już dwoma procesorami), szybko pracujące kontrolery dysków i co najmniej kilka dysków twardych. Serwery mogą wymieniać dane z kartą sieciową z szybkością 50 Mb/s (maks. 80 Mb/s). Serwery dla przedsiębiorstw są z reguły systemami wieloprocesorowymi (najczęściej dwa lub cztery procesory), a dyski twarde pracują w ramach macierzy dyskowej RAID (niezawodność). Serwery tej klasy muszą pracować pewnie, dlatego szereg elementów jest dublowanych. Serwer dla przedsiębiorstw pracuje bardzo wydajnie i jest w stanie wymieniać dane z siecią z szybkością dochodzącą do 100 Mb/s. Można w nich więc śmiało instalować karty sieciowe Fast Ethernet bez obawy o to, że serwer nie podoła tego rodzaju obciążeniom.

Wydajność serwera zależy nie tylko od przepustowości magistrali danych i zastosowanego procesora, ale też od liczby procesorów i architektury układów wspierających wieloprocesorowość. Serwery jednoprocesorowe odchodzą powoli do przeszłości. Coraz więcej serwerów jest wyposażanych w dwa lub cztery procesory.

Duży klaster opracowany przez firmę Dell

Klaster składający się z 16-tu serwerów zarządzających bazą danych DB2 (IBM). Serwery komunikują się między sobą przez łącze pracujące w oparciu o technologię Virtual Interconnect Architecture (VIA)



Dell Computer jest twórcą klastra składającego się z 16 serwerów platformy Windows NT, zarządzających wysokowydajną bazą danych DB2 (IBM). Klaster może się składać z 16 serwerów PowerEdge 6300 – każdy wyposażony w cztery procesory Pentium II Xeon taktowane z częstotliwością 400 MHz. Komputery komunikują się między sobą przez łącze Ethernet, wykorzystując do tego celu gigabitowe karty sieciowe i przełączniki wyprodukowane przez firmę GigaNet. Klaster udostępnia klientom informacje przechowywane w bazie danych DB2 Universal Database (IBM), której konfiguracja została dostosowana do specyficznego środowiska pracy. Serwery wymieniają między sobą dane, posługując się sterownikami opracowanymi przez firmę GigaNet, pracującymi zgodnie ze specyfikacją VIA (*Virtual Interconnect Architecture*). Specyfikacja (opracowana przez firmy Microsoft, Compaq i Intel) opisuje pracę łącza transmitującego dane z bardzo dużą szybkością i charakteryzuje się tym, iż liczba instrukcji używanych do wymiany danych między serwerami jest ograniczona do minimum.

Przetwarzanie wieloprocesorowe

Jeśli chodzi o architekturę wieloprocesorową, to obecnie najczęściej stosowanymi są serwery **SMP** (*Symmetrical Multiprocessor Processing* – symetryczne przetwarzanie wieloprocesorowe). Każdy z procesorów wchodzących w skład serwera SMP współdzieli te same zasoby systemu – magistralę danych, układy I/O i jedną centralną pamięć – mając do każdego z tych elementów takie same prawa dostępu.

Konkurencyjna architektura nosi nazwę **MPP** (*Multiprocessor Parallel Processing* – masowe przetwarzanie równoległe) i opiera się na następującym założeniu: serwer MPP może się składać z wielu procesorów (których może być kilkadziesiąt, a nawet kilkaset), dysponujących oddzielnymi pamięciami RAM, szynami danych i układami sterującymi pracą każdego z tych podmiotów. Architektura MPP nie spełniła jednak pokładanych w niej nadziei. Barierą nie do pokonania okazało się oprogramowanie zarządzające pracą tak skomplikowanej maszyny do przetwarzania danych. Bardzo trudno jest bowiem opracować efektywnego zarządcę, który dzieliłby aplikację na mniejsze części i przydzielał je każdemu procesorowi MPP do wy-

Przepustowości szyn danych instalowanych w serwerach

Szyna danych	Maks. teoretyczna przepustowość (w Mb/s)	Rzeczywista przepustowość (w Mb/s)
ISA	66	10-25
PC Card	66	10-20
EISA	264	64
MCA	320	80
PCI	1056	264

Architektura serwerów NUMA-Q (Sequent)

Od strony rozwiązań sprzętowych serwer platformy **NUMA** można porównać do klastra komputerowego. Komputer taki składa się z szeregu węzłów obliczeniowych, komunikujących się między sobą przez szybko pracujące łącza. Każdy węzeł obliczeniowy dysponuje oddzielną pamięcią i szyną danych. Jednak NUMA to coś innego niż zwykły klaster. NUMA wprowadza pojęcie „lokalnej pamięci" (fizyczna pamięć zainstalowana w konkretnym węźle obliczeniowym) i „zdalnej pamięci" (pamięć zainstalowana w innym węźle obliczeniowym). Warto w tym momencie zauważyć, że koncepcja lokalnej i zdalnej pamięci odnosi się wyłącznie do warstwy sprzętowej rozwiązania i tak jest realizowana. Z punktu widzenia programisty obie te pamięci tworzą jedną lokalną pamięć postawioną do dyspozycji całego systemu NUMA. Tak więc jeśli system NUMA składa się z trzech węzłów obliczeniowych i w każdym zainstalowano pamięć o pojemności 1 GB, to programista dysponuje jedną logiczną pamięcią (i to adresowaną w sposób ciągły), której przestrzeń adresowa wynosi 3 GB.

Inną charakterystyczną cechą serwerów platformy NUMA jest koncepcja „zdalnej pamięci podręcznej". W większości systemów NUMA każdy węzeł obliczeniowy dysponuje nie tylko własną pamięcią lokalną, ale też lokalną pamięcią podręczną, w której przechowywane są części danych rezydujących w zdalnych pamięciach. To właśnie w tych pamięciach podręcznych znajdują się kopie zasobów przechowywanych w pamięciach lokalnych towarzyszących innym węzłom obliczeniowym. Na rysunku przedstawiono architekturę opracowaną przez firmę Sequent, wykorzystywaną przez serwery linii NUMA-Q. Litera Q oznacza, że w skład każdego z węzłów obliczeniowych wchodzą cztery procesory.

To co najbardziej odróżnia systemy NUMA od innych systemów wieloprocesorowych, to fakt, że serwery tej platformy są wyposażone w dodatkowy sprzęt, dzięki któremu cała pamięć jest postrzegana jako jedna logiczna całość. Jeśli program operujący w węźle obliczeniowym numer 1 chce odczytać z pamięci dane, to serwer sprawdza, czy podany adres znajduje się w lokalnej pamięci zainstalowanej w danym węźle. Jeśli tak, to dane są natychmiast odczytywane. Jeśli nie, serwer sprawdza zawartość lokalnej pamięci podręcznej. Proszę pamiętać, że pamięć ta jest zainstalowana w danym węźle obliczeniowym, dlatego czas dostępu do danych jest bardzo krótki. Jeśli i w tej pamięci nie ma danych, wtedy warstwa sprzętowa serwera wysyła automatycznie stosowne żądanie do tego węzła obliczeniowego, w którym rezydują dane. Po pewnym czasie węzeł ten odeśle do węzła numer 1 potrzebne dane. Dane są zapisywane do lokalnej pamięci podręcznej towarzyszącej węzłowi numer 1. Jeśli program zechce po jakimś czasie odczytać ponownie te dane, to nie będą już one pobierane z innego węzła, ale z lokalnej pamięci podręcznej przechowującej zdalne dane. Istotne jest to, że wszystkie te operacje (chodzi o spójne zarządzanie wszystkimi pamięciami – lokalnymi, zdalnymi i lokalnymi pamięciami podręcznymi) są realizowane wyłącznie przez sprzęt, a nie przez oprogramowanie.

konania. Technologia MPP jest obecnie stosowana do budowania superserwerów. Wieloprocesorowe serwery obsługujące grupy robocze i przedsiębiorstwa opierają się na architekturze SMP.

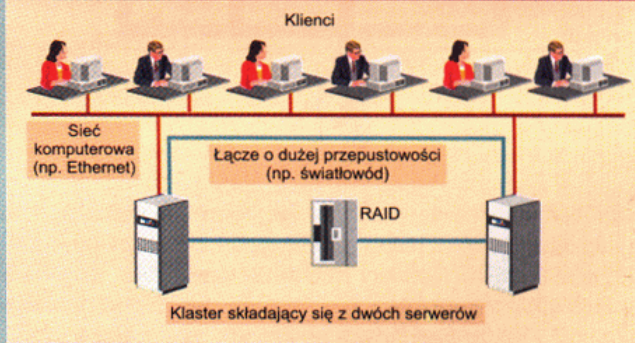
Ostatnio coraz większym powodzeniem cieszy się architektura serwerów wieloprocesorowych nosząca nazwę **NUMA.** NUMA to pierwsze litery wyrazów *Non-Uniform Memory Access* (niejednolity dostęp do pamięci). Co kryje się za tym terminem? Mówiąc najprościej, jest to połączenie architektury SMP (nieco zmienionej i dostosowanej do nowego otoczenia) z technologią gron (klastry komputerowe). Z tym że gronem nie jest tu oddzielny komputer, ale jednostki obliczeniowe wchodzące w skład serwera NUMA. Podobnie jak maszyny SMP, serwery NUMA składają się z wielu procesorów połączonych w jeden logiczny organizm, co pozwala uzyskiwać bardzo dużą wydajność. Podstawowym elementem serwera architektury NUMA (przynajmniej takie rozwiązanie jest stosowane obecnie) jest jednostka obliczeniowa składająca się z czterech procesorów – *quad*. Kwartet procesorów jet umieszczony na jednej płycie, a jednostki *quad* komunikują się między sobą korzystając z usług szybko pracujących łączy, które mają przepustowość rzędu 1 GB/s. Główna różnica między architekturą NUMA i SMP polega na tym, że w przypadku tej pierwszej każdy procesor ma do dyspozycji swoją własną pamięć, a w serwerach SMP wszystkie procesory współdzielą tę samą pamięć, z którą komunikują się przez jedną szynę danych. Jest to bardzo ważna cecha nowej architektury (elastyczność), ponieważ serwer NUMA można w prosty sposób rozbudować, osiągając wydajność potrzebną do efektywnej obsługi konkretnej aplikacji. Problem z serwerami SMP polega na tym, że można w nich co prawda dokładać kolejne procesory, ale wtedy przepustowość magistrali danych sprzęgających te układy ze współdzieloną pamięcią znacznie spada (chodzi nie o przepustowość zagregowaną, nie ulegającą zmianie, ale o przepustowość udostępnianą każdemu z procesorów). Jeśli w serwerze SMP zainstalujemy zbyt dużo procesorów, to szyna danych jest przeciążona i procesory mają ciągłe kłopoty z uzyskaniem do niej dostępu. Stąd w serwerze SMP można zainstalować co najwyżej 16 procesorów, a serwer NUMA można rozbudowywać i rozbudowywać. Co prawda zawsze można połączyć ze sobą dwa 16-procesorowe serwery SMP w jeden klaster, ale nie ma to wiele wspólnego ze skalowalnością, lecz raczej z niezawodnością pracy takiego układu (jeśli jeden serwer ulega awarii, jego zadania przejmuje druga część klastra).

Rodzaje procesorów

Na rynku dominują obecnie dwie architektury procesorów stosowanych do budowania serwerów: RISC (*Reduced Instruction Set Computer*) i CISC (*Complex Instruction Set Computer*). Większą popularnością cieszą się serwery platformy CISC, kojarzonej najczęściej z procesorami firmy Intel (ale do tej platformy należą też np. układy CPU produkowane przez Motorolę).

Jak sama nazwa wskazuje, układy RISC pracują opierając się na ograniczonej liczbie rozkazów. W latach osiemdziesiątych obowiązywała zasada, że układ CPU powinien dysponować jak największą liczbą instrukcji. Właśnie wtedy zaczęto też myśleć o procesorach z niewielką (w stosunku do architektury CISC) liczbą instrukcji. I tak powstały układy RISC, które pracują bardzo szybko i są tanie (układ architektury RISC zawiera mało tranzystorów, dzięki czemu łatwo jest go zaprojektować i produkować). Wśród specjalistów nie ma do tej pory zgody co to tego, która architektura zwycięży w przy-

Przetwarzanie wielokomputerowe – klaster



Klaster to jednostka obliczeniowa składająca się z kilku powiązanych ze sobą fizycznie i logicznie komputerów. Każdy komputer pełni rolę oddzielnego węzła obliczeniowego (*node*), który dysponuje niezależną kopią systemu operacyjnego i zbiorem aplikacji. Całość tworzy jednak jeden wirtualny komputer, realizujący powierzone mu zadanie.

szłości. Zwolennicy RISC argumentują, że są to układy szybkie i tanie, dlatego wygrają rywalizację z CISC. Przeciwnicy podkreślają natomiast, że tak proste w budowie układy jak RISC wymagają obecności skomplikowanego oprogramowania. Ponieważ układy CISC upodobniają się w coraz większym stopniu do układów RISC (i odwrotnie), to jest bardzo możliwe, że podział na procesory CISC i RISC przestanie za kilka lat obowiązywać.

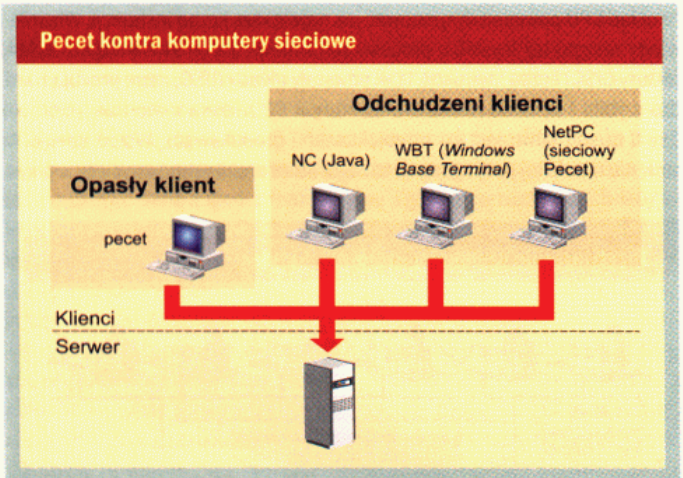
Komputery sieciowe

Komputer sieciowy to inaczej „odchudzony" klient, dysponujący ograniczonymi zasobami sprzętowymi (wyposażony w niewielki dysk twardy lub nie posiadający w ogóle tego rodzaju urządzenia), zaprojektowany z myślą o ścisłej współpracy z siecią komputerową (przede wszystkim z Internetem). Ponieważ użytkownicy komputerów PC rzadko wykorzystują wszystkie możliwości tego rodzaju stacji, to zrodził się pomysł komputera sieciowego, który korzysta z zasobów rezydujących w pamięci serwera. Komputer sieciowy jest więc specyficznego rodzaju klientem, do którego przylgnął przydomek „odchudzony"

Odchudzony klient

W aplikacjach architektury klient/serwer jest to klient polegający w dużo większym – w porównaniu do peceta – stopniu na serwerze. Producenci sprzętu i oprogramowania sieciowego podzielili się na dwa obozy. Po jednej stronie (reprezentowanej przez Netscape i Sun Microsystems) znajdują się zwolennicy klienta opartego na języku Java (komputer **NC**), a po – firmy (pod wodzą Microsoftu i Intela) popierające koncepcję komputera sieciowego klasy **NetPC** albo terminala Windows.

NetPC to prosty, łatwy w użyciu, oparty na systemie Windows komputer. Sprzęt Net PC udostępnia także możliwości standardu „Zero Administration„ – zdalne ładowanie aplikacji, automatyczne uaktualnienie systemu. Pozwala to na budowanie sieci, w których zarządzanie będzie całkowicie scentralizowane, a przez to znacznie wygodniejsze i tańsze. Jedną z podstawowych cech odróżniających ten produkt od zwykłego komputera PC jest fakt, iż jest zaprojektowany właśnie z myślą o centralnym zarządzaniu



Toczy się obecnie ostra walka o opanowanie rynku komputerów sieciowych. Na placu boju pozostały trzy technologie: komputer sieciowy NC (wykorzystujący aplety Java), opracowany i wspierany przez tandem Microsoft/Intel sieciowy pecet (standard NetPC) i terminal systemu Windows – twórcą tej technologii (określanej mianem WBT – *Windows Base Terminal*) jest Microsoft. Jest jeszcze za wcześnie, aby przesądzić, która z tych technologii weźmie górę. Wydaje się jednak, że najwięcej szans na sukces ma komputer NC. Zyska on jednak większe poparcie dopiero wtedy, gdy wzrośnie podaż aplikacji tej platformy. Dopóki to nie nastąpi, tradycyjny pecet wyposażony w procesor Intela (platforma Wintel, czyli system operacyjny Windows plus procesor Intel) nie będzie miał poważnego rywala.

w sieci. Ponadto użytkownicy mogą nadal korzystać ze wszystkich „dobrodziejstw" standardowego peceta.

Jeden z koronnych argumentów wysuwanych przez zwolenników koncepcji komputera sieciowego brzmi: komputer sieciowy jest tani. Chodzi tu zarówno o cenę produktu, jak i koszty związane z eksploatacją i utrzymaniem w ruchu tego rodzaju stanowiska pracy. Dwie firmy – Oracle i Sun – zaproponowały nawet konkretną konfigurację komputera sieciowego: od 4 do 64 MB pamięci RAM, 8 MB pamięci ROM, gniazdo SmartCard, interfejs sieciowy, interfejs na podczerwień, port równoległy i dwa porty standardu PS/2.

Network Computer i Java

Komputery sieciowe oparte na języku Java – promowane głównie przez Sun Microsystems – nazywane są komputerami klasy **NC** (*Network Computer*). **Java** jest językiem programowania opracowanym przez Sun Microsystems. Na początku produkt nosił nazwę OAK i projektowano go z myślą o zarządzaniu pracą różnego rodzaju elektronicznych urządzeń przenośnych. Powstanie sieci WWW spowodowało, że OAK wzbogacono o nowe możliwości i przemianowano w 1995 r. na Javę. Java to język obiektowy podobnym do C++. Pliki źródłowe mają rozszerzenie *.java* i są kompilowane na format bajtowy, a pliki tego formatu można rozpoznać po tym, że mają rozszerzenie *.class*.

Aplety i serwlety

Kod bajtowy jest interpretowany przez oprogramowanie (rezydujące po stronie klienta) na kod binarny i po wykonaniu tej operacji aplikacja jest gotowa do pracy. Kod języka Java jest dość skomplikowany, ale ma jedną podstawową zaletę – można go uruchamiać na komputerze dowolnej platformy, dysponującym wirtualną maszyną Java – JVM (*Java Virtual Machine*). Jest to oprogramowanie kompilujące aplety Javy na kod maszynowy komputera konkretnej platformy sprzętowej. Dlatego aplikacje pisane w tym języku są w pełni przenośne, to znaczy można je uruchamiać w różnych środowiskach: Windows, Unix, Macintosh OS itp. Kod bajtowy Javy można łatwo przekonwertować na język maszynowy komputera, posługując się opracowaną ostatnio, pracującą bardzo szybko, technologią JIT. Jest to specyficznego rodzaju konwerter pracujący w trybie *Just-in-Time*, czyli „na bieżąco". Małe aplikacje napisane w języku Java są nazywane apletami, a do podobnego rodzaju aplikacji rezydujących po stronie serwera przylgnęła nazwa serwlety. Aplety są przechowywane w pamięci serwera i każdy klient może ściągnąć taki aplet do siebie (korzystając z usług przeglądarki webowej), a następnie uruchomić konkretną aplikację opartą na takim aplecie. Niektórzy sądzą, że kolejne wersje systemu operacyjnego Windows będą też dysponować podobnego rodzaju narzędziami (interpretator kodu bajtowego Java), dzięki którym komputer będzie mógł ściągać z odległych serwerów aplety i następnie uruchamiać je.

Sun Microsystems ma w swojej ofercie komputer sieciowy NC oparty na technologii Java. Urządzenie nosi nazwę JavaStation i pracuje pod systemem operacyjnym JavaOS, który pozwala szybko uruchamiać aplikacje platformy Java. Sun instaluje w pamięci komputera przeglądarkę HotJava Browser, a użytkownik może doinstalować wiele aplikacji użytkowych, takich jak np. e-mail, kalendarz itp. Java Station wymaga obecności w sieci serwera linii NetraJ Family i jest wyposażona w procesor Sparc-II (100 MHz; pamięć cache Level 1 o pojemności 16 kB na instrukcje i 8 kB na dane), 14- lub 17-calowy monitor, interfejs sieciowy 10/100Base-T, 16 MB pamięci RAM (z możliwością rozszerzenia do 64 MB) i pamięć błyskową 8 MB.

NetPC

Ponieważ komputery NC (oparte na języku Java) były wyzwaniem rzuconym Microsoftowi, nie trzeba było długo czekać na ripostę. Microsoft – chcąc nie chcąc – musiał się pogodzić z faktem, że „komputer to sieć", i przystąpić do kontrofensywy, proponując komputer sieciowy klasy NetPC, czyli sieciowego peceta.

Komputery NetPC można wyposażać w systemy Microsoft Windows. Z zastosowaniem takiej samej jak w przypadku pecetów platformy systemowej wiążą się korzyści z wykorzystania istniejącego już oprogramowania. Można więc uruchamiać na NetPC oprogramowanie przeznaczone dla systemu Windows, jak również oprogramowanie napisane w Javie.

Komputer NetPC jest dzieckiem firm Microsoft i Intel. Mówiąc najprościej NetPC jest niczym innym jak „ubogim krewnym" komputera PC, przystosowanym do pracy w środowisku sieciowym. NetPC może zarówno korzystać z usług sieci, jak i wykonywać lokalnie aplikacje Windows. Od zwykłego peceta różni się tym, że warstwa sprzętowa komputera jest lepiej przystosowana do otoczenia sieciowego i dysponuje wieloma rozwiązaniami pozwalającymi zarządzać stacją NetPC zdalnie. Komputery NetPC to urządzenia platformy Wintel (Windows plus Intel). Nie spotkamy w nich stacji dyskietek ani stacji CD-ROM, chociaż są wyposażane w dysk twardy. Pełni on tu jednak rolę pamięci cache świadczącej swe usługi aplikacjom sieciowym, a nie jest używany do magazynowania dużych porcji danych i całych programów, jak ma to miejsce w przypadku peceta. Do zarządzania i administrowania komputerem NetPC użytkownik stosuje aplikacje klasy ZAW (*Zero Administration Windows*), które pracując zdalnie znacznie obniżają koszty eksploatacji komputera sieciowego.

Windows Base Terminal

Terminal Windows reprezentuje prostą stację typu *dumb terminal*, pozwalającą uruchamiać aplikacje Windows. Terminal korzysta z usług serwerów platformy Windows NT. Całe przetwarzanie i obróbka danych są wykonywane przez serwer, a terminal przesyła tylko do serwera polecenia (klawiatura i mysz) i odbiera dane, wyświetlając je na ekranie. Ponieważ Windows NT nie jest systemem operacyjnym pracującym w trybie *multi-user* (jak np. Unix), to na serwerach tej platformy trzeba uruchamiać dodatkowe oprogramowanie, które podoła temu zadaniu. Istnieje kilka odmian oprogramowania pozwalającego zamienić system Windows NT w taki produkt, który może obsłużyć jednocześnie wielu klientów. Jednak największą popularnością cieszy się pakiet WinFrame.

WinFrame

WinFrame jest technologią opracowaną przez firmę Citrix Systems, dzięki której serwer Windows NT zaczyna pracować w trybie *multi-user*. WinFrame w połączeniu z inną technologią Citrixa, noszącą nazwę ICA (ICA to protokół komunikacyjny sterujący wymianą danych między klientem i serwerem WinFrame) powoduje, że serwer Windows NT zaczyna funkcjonować jak klasyczny minikomputer. Dlatego klienci pracujący pod innymi niż Windows systemami operacyjnymi (np. Macintosh, Unix i DOS) mogą uruchamiać aplikacje Windows.

Czas pokaże, która z koncepcji komputera sieciowego weźmie górę: NC, NetPC czy terminal systemu Windows. Początkowy entuzjazm zwolenników NC osłabł ostatnio i pecety trzymają się nadal mocno. NetPC i terminale Windows też nie cieszą wielkim powodzeniem. Przyszłość pokaże, czy pecet wytrzyma próbę czasu, czy też przegra lub przekształci się w zupełnie nowy sprzęt.

(jch)

Modemy

Modem to skrót od słów **MO**dulacja **DEM**odulacja. Jest to urządzenie pozwalające komputerowi transmitowaćdane przez zwykłą linię telefoniczną. Informacje przetwarzane przez komputer mają postać cyfrową (bity), podczas gdy przez linię telefoniczną są przesyłane sygnały analogowe. Modem jest specyficznego rodzaju konwerterem, który zamienia sygnały cyfrowe na analogowe (modulacja) i analogowe na cyfrowe (demodulacja). Sygnał analogowy jest przesyłany przez linię telefoniczną dysponującą pasmem przenoszenia o szerokości 3 kHz. Dane mogą być transmitowane w obie strony jednocześnie (pełny dupleks) lub naprzemiennie (półdupleks). Całe pasmo przenoszenia danych jest najczęściej dzielone na dwie umowne części: przez jedną część pasma modemy transmitują właściwe dane, a druga służy do wymiany sygnałów sterujących. Sposób podziału pasma i definiowania poszczególnych kanałów komunikacyjnych zależy od konkretnych rozwiązań i nie jest obligatoryjny, ale jest opisany przez standardy telekomunikacyjne oznaczone symbolem **V. numer standardu**. Poszczególni producenci modemów stosują różne technologie.

Modemy można klasyfikować biorąc za punkt wyjścia jedną z kilku cech. A mogą to być takie cechy (parametry), jak: długość łącza, rodzaj łącza, tryb pracy, synchronizacja, rodzaj modulacji czy wreszcie szybkość.

Długość łącza

Modemy na **małe odległości** (*short haul*) to tanie urządzenia przesyłające dane na odległość do 15 kilometrów. Modemy tego rodzaju są instalowane w sieciach prywatnych, a nie w publicznych sieciach telefonicznych.

Modemy **wąskopasmowe** klasy VG (*voice grade*) to najczęściej stosowane modemy, przesyłające dane przez publiczne sieci telefoniczne. Modemy tego rodzaju przesyłają dane przez łącze dedykowane lub przez łącze komutowane (to jest złożone na czas trwania sesji, tak jak w przypadku rozmowy telefonicznej).

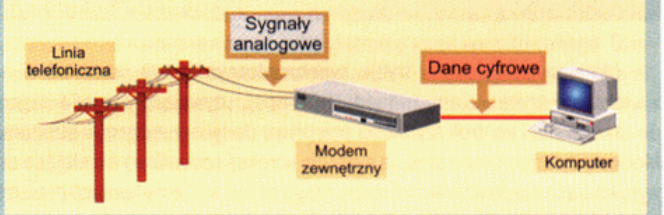
Modemy **szerokopasmowe** (*wideband*) to szybko pracujące urządzenia, używające stabilnie pracujących, dedykowanych łączy (oferujących szerokie pasmo przenoszenia danych), które sprzęgają ze sobą na stałe np. dwa komputery. Dużą karierę robi ostatnio modem szerokopasmowy DSL (*Digital Subscriber Line*), przesyłający dane przez dwa niesymetryczne pasma: 8 Mb/s (do abonenta) i 2 Mb/s (od abonenta). Modem radiowy RF (*Radio Frequency*) jest kolejnym przykładem modemu szerokopasmowego. Modem ten (obsługujący telewizję kablową CATV) oferuje pasmo przenoszenia danych rzędu 10 MHz.

Rodzaj łącza

Do pierwszej grupy należy zaliczyć modemy dołączane do *dedykowanych*, *prywatnych* lub *dzierżawionych* łączy, które w warstwie fizycznej są najczęściej kablem czteroprzewodowym.

Druga grupa to modemy przesyłające dane przez łącza typu *dial up* (komutowane), czyli przez publiczną sieć telefoniczną – PSTN (*Public Switched Telephone Network*). Modemy tego rodzaju mają dużo trudniejsze zadanie, ponieważ parametry łącza mogą być za każdym razem inne.

Modem może być kartą instalowaną w komputerze lub zewnętrznym urządzeniem dołączanym do portu RS-232

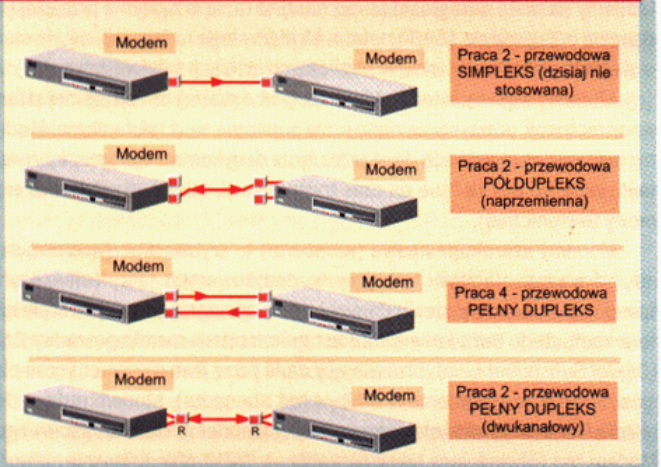


Modemy mogą przybierać postać kart instalowanych wewnątrz komputera (wyposażonych w łącze odpowiadające gniazdu wbudowanemu w płytę główną komputera – np. ISA lub IESA) lub wolno stojących, zewnętrznych urządzeń. W tym drugim przypadku modem musi być najczęściej zasilany z niezależnego źródła. Ceny popularnych modemów, przeznaczonych dla indywidualnego użytkownika, kształtują się w granicach od 100 do 300 zł. Modemy profesjonalne, budowane z myślą o przedsiębiorstwach, są już droższe (oferując przy tym szereg dodatkowych rozwiązań i usług) i kosztują powyżej 1000 zł. Jeśli przedsiębiorstwo decyduje się na zainstalowanie serwera zdalnego dostępu – RAS (*Remote Access Server*), to nie musi kupować modemów, ponieważ stanowią one integralną część tego rodzaju serwerów.

Synchronizacja

Większość modemów pracujących w trybie **asynchronicznym** (dane nie są tu transmitowane zgodnie z sygnałami przekazywanymi przez zegar, a oba modemy znają tylko nominalną szybkość transmisji) przesyła dane z niewielkimi szybkościami – do 1800 bps. Modemy tego rodzaju pracują często w oparciu o modulację FSK (*Frequency Shift Keying*) i używają czterech częstotliwości: dwóch do transmitowania i dwóch do odbierania danych. Modemy mogą przesyłać dane przez kable dwu- i czteroprzewodowe. W przypadku kabla dwuprzewodowego modem może pracować w trybie pełnego dupleksu, dzieląc podstawowy kanał na dwa mniejsze.

Cztery podstawowe tryby pracy modemu



Półdupleks. Modem może przesyłać dane w obu kierunkach, ale niejednocześnie. Wymagana tu jest obecność specjalnego systemu sygnalizacji, który pozwala zarządzać transmisją danych – raz w jednym kierunku, a w innej chwili w drugim.
Pełny dupleks. Modem może przesyłać dane jednocześnie w obu kierunkach. W przypadku kabla dwuprzewodowego modemy stosują różne metody separowania jednego toru transmisji (nadawanie) od drugiego (odbieranie), tak aby nie dochodziło do przesłuchów. Najczęściej jest tu stosowana technologia FDM (*Frequency Division Multiplexing* – każdy tor pracuje na oddzielnej częstotliwości nośnej) lub EC (*Echo Cancelling* – niwelowanie odbić). Praca w trybie pełnego dupleksu przewiduje, że modem może przesyłać dane jednocześnie w obu kierunkach z pełną szybkością. Te modemy, które w jednym kierunku przesyłają dane z mniejszą (niż to wynika ze specyfikacji) szybkością, są czasami nazywane modemami typu *split-speed* lub *asymmetric modem*.
Simplex. Modem może przesyłać dane tylko w jednym kierunku, pełniąc więc wyłącznie rolę nadajnika albo odbiornika.

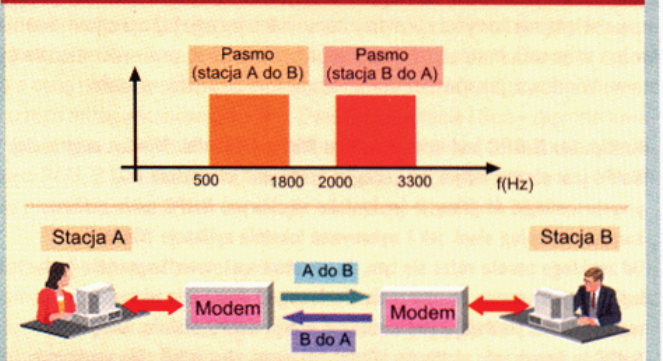
Modemy pracujące w trybie **synchronicznym** mogą przesyłać dane z większymi szybkościami (ponad 1800 bps), używając impulsów zegara do taktowania i kontroli szybkości przepływu danych między obu stronami. Modemy synchroniczne stosują systemy korekcji (*equalizer*) niwelujące czy wyrównujące niedoskonałości łącza. Mogą to być systemy korekcji pracujące automatycznie (badające za każdym razem stan łącza i dostosowujące pracę modemu do aktualnie panujących warunków) lub wymagające asysty personelu technicznego.

Rodzaj modulacji

Modemy stosują różne metody modulacji sygnałów. Najważniejsze z nich to:

- AM – modulacja amplitudy. Szybkość 4800 bps i więcej.
- FM – modulacja częstotliwości. Razem z kluczowaniem częstotliwości (technologia FSK) ten rodzaj modulacji umożliwia transmitowanie danych z szybkością od 300 (pełny dupleks) do 1200 bps (półdupleks).
- CPM – ciągła modulacja częstotliwości. Technologia pracująca podobnie jak FM, pozwalająca przesyłać dane z szybkością ponad 1200 bps.

Praca w trybie .....



Danym transmitowanym w trybie asynchronicznym nie towarzyszą impulsy zegarowe. Aby zapobiec powstawaniu błędów (brak zegara sprzyja przekłamaniom), dane są przesyłane w postaci niewielkich bloków, a modemy generują specjalne bity startu i stopu. Najczęściej stosowanym systemem kodowania przy tego rodzaju transmisji jest siedmiobitowy kod ASCII plus bit parzystości (*even parity*).

- PM – modulacja fazy. Średnia szybkość transmisji danych od 1200 do 4800 bps.

Wymienione poniżej trzy popularne techniki modulacji pracują bardzo wydajnie, budując większą liczbę punktów konstelacji, dzięki czemu modemy akustyczne osiągnęły już chyba kres swoich możliwości.

- QAM – modulacja kwadraturowa. Szybkość do 9600 bps.
- TCM –modulacja *Trellis Coded Modulation*. Szybkość do 28 000 bps.
- MD – modulacja Delta. Jeśli chodzi o zamianę sygnałów analogowych na postać cyfrową, to jest to obecnie najwydajniej pracująca technologia.

Port RS-232

Istnieje jeden stosowany powszechnie interfejs (w każdym bez wyjątku komputerze), z usług którego może korzystać modem: port RS-232. Dlatego każdy modem wystarczy podłączyć do portu RS-232 (a z drugiej strony do gniazdka telefonicznego), aby nawiązać łączność z odległym komputerem. Pod warunkiem oczywiście, że wcześniej zainstalujemy w pamięci komputera odpowiednie oprogramowanie. Istnieją też modemy wewnętrzne, które są instalowane na kartach umieszczanych w jednym z gniazd rozszerzeń wbudowanych w płytę główną komputera.

Należy jeszcze wspomnieć o modemach będących wyłącznie oprogramowaniem. Rozwiązania takie są jednak stosowane bardzo rzadko i wymagają obecności silnego procesora, co najmniej klasy Pentium.

Bity kontra body

Data rate to liczba zmian sygnału, jaką modem może wygenerować w ciągu określonego czasu (np. jednej sekundy). Szybkość pracy modemów jest podawana w bodach (*baud*). Jeśli stan linii może się zmienić w ciągu jednej sekundy (z logicznego „0" na „1" i odwrotnie) sto razy, to urządzenie może pracować z szybkością 100 bodów. Szybkość pracy modemu i szybkość transmisji danych (która jest definiowana w bitach na sekundę) to dwie różne sprawy. Chodzi o to, że modem może wyekspediować w sieć w momencie zmiany sygnału z jednego stanu logicznego na drugi więcej niż jeden bit. I tak modem pracujący z szybkością 1200 bodów może np. (zależnie od zastosowanej technologii) transmitować dane z szybkością 4800 bps (bitów na sekundę).

Maksymalna szybkość transmitowania danych przez modem (czyli przepustowość łącza) jest jednak ograniczona prawem Shannona, które wyraża się wzorem: P=W*log2 (1+S/N). W przypadku linii telefonicznych parametr W (szerokość pasma) wynosi 3000 Hz. Parametr S to moc transmitowanego sygnału, a N poziom szumów – współczynnik S/N przyjmuje najczęściej wartość 1500. Łatwo więc wyliczyć, że teoretyczna przepusto-

Terminologia

- **Adaptive Packet Assembly**: możliwość dynamicznego zmieniania długości pakietu, zależnie od jakości łącza.
- **ASVD:** jednoczesne przesyłanie dźwięku i danych (analogowy system transmisji danych.)
- **Język AT** to język zleceń stosowany przez modemy (opracowany przez Hayes Microcomputers Products), stosowany obecnie przez wszystkich producentów modemów. Każde polecenie zaczyna się od liter „AT", po których są wstawiane kolejne litery i cyfry. I tak np. polecenie ATDT345678 inicjuje łączność komutowaną ze stacją o numerze 345678, nakazując jednocześnie lokalnemu modemowi, aby numery były transmitowane w trybie tonowym (a nie impulsowym). Inne polecenia aktywują modem, zarządzają systemem korekcji błędów, kontrolują głośnik czy definiują, po jakiej liczbie wywołań modem ma odpowiedzieć drugiej stronie. Poszczególne rodzaje modemów stosują różne odmiany tego języka, ponieważ producenci dodają nieraz swoje firmowe polecenia. Dlatego przed przystąpieniem do programowania modemu należy zawsze zapoznać się z dokumentacją i sprawdzić, jaki rodzaj poleceń AT wspiera dany model modemu.
- **bps** (bity na sekundę) to parametr definiujący, jak szybko modem może transmitować dane. Szybkość pracy modemów mierzy się też w bodach. Trzeba jednak pamiętać, że body to nie to samo co bps. Modem pracujący z szybkością 1200 bodów może np. transmitować dane z szybkością 2400 lub 4800 bps. Najszybsze modemy mogą ekspediować dane w sieć z szybkością 56 600 bps, a nawet szybciej, jeśli dodatkowo zastosujemy kompresję danych. Nie zawsze opłaca się kupować drogi, szybki modem, ponieważ będzie on i tak przesyłać dane z taką szybkością, z jaką pracuje urządzenie zainstalowane po drugiej stronie łącza.
- **Flash memory** (pamięć błyskowa): niektóre modemy są wyposażane w pamięć błyskową zamiast konwencjonalnej pamięci ROM. Korzyść jest oczywista – użytkownik może szybko i w każdej chwili zmienić oprogramowanie zarządzające pracą modemu (a więc protokoły komunikacyjne) na inne.
- **Handshaking:** uzgadnianie warunków transmisji danych. Operacja polega na wymianie między komunikującymi się modemami szeregu sygnałów definiujących warunki całego procesu transmisji danych (a więc wstępne nawiązanie łączności, właściwy transfer pliku i zakończenie sesji łączności).
- **K56Flex:** protokół pozwalający transmitować pakiety przez łącza modemowe z szybkością 56 000 bps.
- **Kompresja danych:** większość produkowanych obecnie modemów potrafi kompresować dane przed wysłaniem ich w sieć, co oczywiście zwiększa przepustowość łącza. Ale uwaga – rozwiązanie takie ma sens wyłącznie wtedy, gdy drugi modem wspiera ten sam tryb kompresji.
- **V17:** protokół obsługujący faksy, transmitujący pakiety z szybkością 14 000 bps.
- **V61:** protokół przesyłający jednocześnie dane i dźwięk (z szybkością do 4800 bps.)
- **V8:** protokół skracający czas potrzebny do nawiązania łączności, używany podczas sesji negocjacyjnej V.34.

wość łącza telefonicznego nie może być większa niż 45 kb/s. Jest to kres możliwości modemów transmitujących dane przez publiczne sieci telefoniczne.

Kompresja danych

Szybkość transmisji danych przesyłanych przez łącze komutowane (oraz każde inne łącze) przy użyciu modemu można zwiększyć stosując jedną z technologii kompresji danych. Protokoły komunikacyjne (uznawane powszechnie za nieformalny standard), definiujące rodzaj kompresji danych oraz zastosowane metody wykrywania i poprawiania błędów, noszą nazwę **MNP** (*Microcom Networking Protocol*; technologia opracowana przez firmę Microcom).

Rodzina protokołów MNP składa się z dziesięciu pozycji, od MNP1 do MNP10. I tak np. MNP4 sprawdza poprawność przesyłania danych (wykrywanie błędów) i dopasowuje automatycznie szybkość transmisji danych do

Protokoły komunikacyjne używane przez modemy

Protokół	Maks. szybkość (bps)	Tryb pracy
Bell 103	300	Pełny dupleks
CCIT V.21	300	Pełny dupleks
ITU V.22	1200	Półdupleks
ITU V.22bis	2400	Pełny dupleks
ITU V.29	9600	Półdupleks
ITU V.32	9600	Pełny dupleks
ITU V.32bis	14 400	Pełny dupleks
ITU V.34	28 800	Pełny dupleks
ITU V.34+	33 600	Pełny dupleks
ITU V.90	56 600	Pełny dupleks
V.42	standard korekcji błędów (opracowany przez ITU) używany przez modemy	
V.42bis	standard opisujący sposób kompresji danych (w stosunku 4:1) przesyłanych przez modemy stosujące tryb korekcji błędów V.42	

jakości technicznej danego łącza. MNP5 reguluje natomiast kwestie związane z kompresowaniem danych, a MNP6 bada, z jaką maksymalną szybkością może pracować modem usytuowany na drugim końcu łącza, i dostosowuje się do tej szybkości. Najczęściej wspieranymi przez modemy klasami MNP są klasy 4 i 5 (MNP4 i MNP5). Szczególnie przydatny jest standard MNP5, pozwalający zwiększyć szybkość transmisji danych nawet dwukrotnie. Systemy kompresji danych pracujące zgodnie z klasą MNP10 pozwalają zwiększyć przepustowość łącza nawet trzykrotnie.

Ponieważ funkcje MNP są realizowane przez warstwę sprzętową modemów, to mają wpływ na wszystkie bez wyjątku informacje przesyłane przez linię telefoniczną. W przypadku innych protokołów (takich jak np. Xmodem i Kermit), które opierają się na pracy oprogramowania, kompresji są poddawane wyłącznie same dane. Inne standardy regulujące kwestie korekcji błędów i kompresowania danych to: **V.42** (korekcja błędów) i **V.42.bis** (kompresowanie danych przy użyciu metody Lempel-Ziv, dzięki czemu modem o nominalnej szybkości 33,6 kb/s może transmitować dane z szybkością ok. 100 kb/s - współczynnik kompresji 3:1).

Standardy

Każdy modem dysponuje interfejsami pracującymi zgodnie z akceptowanymi przez przemysł informatyczny standardami. Dane są przesyłane przez te interfejsy przy użyciu specjalnych protokołów telekomunikacyjnych, formatujących je w określony sposób. Niektóre protokoły (jak np. CCITT V.34) mają status oficjalnych standardów, podczas gdy inne są rozwiązaniami firmowymi. Na szczęście każdy modem wspiera zawsze co najmniej jeden popularny protokół, dzięki czemu bez przeszkód może się porozumiewać z innym modem zainstalowanym po drugiej stronie łącza komutowanego. Dzieje się tak w przypadku transmitowania danych z mniejszymi szybkościami. Protokoły obsługujące większe szybkości nie mają często statusu oficjalnie zatwierdzonych standardów.

Faksy/modemy

Na rynku są dostępne faksy/modemy, a więc sprzęt integrujący dwie technologie. Jeśli chodzi o sposób przesyłania faksów, to faks/modem pracuje najczęściej zgodnie z jedną z dwóch specyfikacji: Class 1 i Class 2.

Standard **Class 1** zleca wykonanie większości zadań związanych z przesyłaniem faksów samemu komputerowi i oprogramowaniu obsługującemu faks. Sam modem ma tu niewiele do roboty. Zaletą tej specyfikacji jest to, że bardzo łatwo jest poddać cały system modyfikacji – wystarczy zainstalować nowszą wersję oprogramowania obsługującego faks.

Standard **Class 2** zleca wstępne nawiązywanie łączności i uzgadnianie warunków transmisji danych samemu modemowi. Zarówno komputer, jak i oprogramowanie obsługujące faks zachowują się biernie i nie uczestniczą w tej operacji. Systemy oparte na tym standardzie pracują efektywniej, po-

nieważ komputer nie jest obciążany dodatkowymi zadaniami związanymi z obsługą faksu.

Modemy DSVD

Na rynku spotkać można modemy typu *voice/data* (głos/dane). Modemy te - znane też jako sprzęt DSVD (*Digital Simultaneous Voice and Data*) - potrafią równolegle transmitować dane i głos, dysponując układami, które automatycznie przełączają tryb pracy. Urządzenie takie zachowuje się więc w jednej chwili jak modem, a za moment jak zwykły telefon. Modemy tego rodzaju dysponują zawsze głośnikiem i mikrofonem. Urządzenia pracujące zgodnie ze specyfikacją DSVD są produkowane od 1995 r. przez firmy Intel, Hayes i U.S. Robotics (obecnie 3Com), które zwróciły się już do ITU z prośbą o zatwierdzenie tej technologii jako standardu.

Modemy 56 kb/s

Sporą karierę zrobiła technologia **X2** opracowana przez U.S. Robotics (obecnie 3Com), dzięki której modem może przysyłać dane przez linię telefoniczną z szybkością 56 kb/s. Przez dłuższy czas uważano, że przez miedziany kabel telefoniczny dane można przesyłać co najwyżej z szybkością 33,6 kb/s. X2 pokonuje tę granicę wykorzystując fakt, że wiele central telefonicznych wymienia między sobą dane, korzystając z usług szybko pracujących łącz cyfrowych. X2 pomija więc procedury związane z zamianą danych z postaci cyfrowej na sygnał analogowy i przesyła dane cyfrowe bezpośrednio do modemu użytkownika. I chociaż X2 pozwala wymieniać dane z siecią Internet dużo szybciej niż zwykły modem, to trzeba pamiętać o pewnych ograniczeniach:

1. Dane są przesyłane szybko tylko w jedną stronę, to jest do komputera (*downloading*). Transmisja danych w drugą stronę (*uploading*) odbywa się przy użyciu tradycyjnych technologii modemowych.

2. Połączenie jest możliwe tylko wtedy, gdy po drugiej stronie pracuje modem wspierający tę technologię.

3. Łącze telefoniczne musi mieć dobrą jakość. W przeciwnym razie szybkość transmisji danych spada poniżej założonego poziomu 56 kb/s.

Najnowszy standard (zatwierdzony przez ITU w 1998 roku) nosi nazwę **V.90** i opisuje pracę modemów przesyłających dane z szybkością 56 kb/s. Wydaje się, że specyfikacja ta pogodzi wreszcie dwie rywalizujące ze sobą technologie 56 kb/s (X2 firmy 3Com i K56flex firmy Rockwell Semiconductor). Obaj producenci modemów zapowiedzieli już, że kolejne wersje produkowanego przez nich sprzętu będą już pracować zgodnie z zaleceniami proponowanymi przez V.90. Co ważne, ci użytkownicy, którzy eksploatują już modemy 56 kb/s, będą mogli łatwo przejść na technologię V.90, modyfikując tylko oprogramowanie zarządzające pracą tych modemów.

(jch)