Koszty urządzeń w poszczególnych technologiach

WDM

Ceny urządzeń WDM są bardzo zróżnicowane i uzależnione ściśle od konfiguracji, ze względu na duży stopień swobody możemy podać przybliżoną cenę systemu WDM złożonego z terminala WDM obsługującego 32 kanały optyczne, 2 λ, kształtującą się na poziomie 200000 Euro. Zwiększając liczbę lambd zwiększa się cena w przybliżeniu o 40 000 Euro za lambdę. Koszt wzmacniacza ILA wynosi około 100 000 Euro. Koszt modemu WDM (1310/1550nm/45km) waha się na poziomie 2000 Euro, natomiast modem WDM (1550/1310nm/45km) kosztuje 2500 Euro. Jak widać system WDM jest kosztownym systemem transmisyjnym jednak przy dużych odległościach i dużych przepustowościach system jest niezbędny i jak pokazują zaprezentowane wyniki bardzo efektywny, a przy tym niezbyt skomplikowany daje to temu systemowi szerokie perspektywy zastowania w najbliżzej przyszłości. Koszt przesłania 1 Mbit danych możemy szacować na około 0,005 zł.

SDH

Sieci synchroniczne SDH są standardem w telekomunikacji zapewniając nowoczesny, efektywny system transportowy o wielu zastosowaniach.

Jak więc widac ceny urządzeń SDH są dużo niższe od urządzeń WDM i dlatego też stanowią alternatywę dla urządzeń WDM. Koszt przesłania 1Mbit waha się na poziomie 0,003 zł.

Wbrew przewidywaniom ATM nie zdobył dużego udziału w rynku komponentów sieci lokalnych. Potencjalnie pozostaje nadal technologią przyszłości. Na razie przyjął się jedynie w bardzo

dużych przedsiębiorstwach, gdzie wspiera tylko szkielet o wysokiej przepływności. Panuje na ogół zgodny pogląd, że trudności aplikacyjne ATM są przejściowe i upowszechnienie nie opóźni się zbyt dużo.

Daje się zauważyć stopniowy zmierzch współdzielonego dostępu do medium i coraz częstsze zastępowanie koncentratorów przełącznikami. Oprócz Ethernetu wielkim zwycięzcą technologicznym jest też przełączanie IP. Technologia ta łączy bardzo silnie inteligencję trasowania i szybkość przełączania komórek. Sukces przełączania IP jest poważny i jednocześnie w ostatnich latach ma największy wpływ na przeobrażanie urządzeń sieciowych – *route once, switch many.* Technika IP interesuje teraz w najwyższym stopniu te przedsiębiorstwa, które chcą rozwijać intranety i tworzyć sieci w pełni IP. Przełączanie IP zastąpi z czasem routery w sieciach przedsiębiorstw, a po sukcesach w sieciach lokalnych rozszerzy się zapewne także na łącza telekomunikacyjne. Na razie większość producentów przełączników nie wspiera standardów trasowania dla sieci telekomunikacyjnych, lecz ogranicza funkcjonowanie swoich przełączników do lokalnych sieci przedsiębiorstw.

Na wykresie 26 uwzględnione zostały następujące elemenety:

– Koszt ruterów zawierających karty liniowe

– Koszt urządzeń WDM wraz z elementami OLT, OADM oraz transponderami

– Całkowity koszt urzadzeń

Ceny urządzeń stosowanych w transmisji przy użyciu DPT oraz Gigabit Ethernet były prawie jednakowe podczas gdy POS okazał się 11% droższy od pozostałych systemów. Wynika to z tego iż, DPT wymaga znacznie mniej kart liniowych STM – 16 niż POS oraz karty liniowe systemu DPT są tańsze niż POS. Oczywiście jak widać największą efektywność uzyskuje technika DPT, ze względu na niskie koszty urządzeń zarówno WDM jak i routerów.

Koszty urządzeń w technologiach WDM (Wavelength Division Multiplexing) i SDH (Synchronous Digital Hierarchy) różnią się znacząco ze względu na specyfikę tych rozwiązań. W przypadku technologii WDM, urządzenia są zazwyczaj droższe z uwagi na skomplikowaną infrastrukturę, która pozwala na multipleksowanie wielu długości fal świetlnych na jednym włóknie optycznym. Wymaga to zaawansowanych komponentów optycznych, takich jak lasery o precyzyjnych długościach fal, filtry optyczne i wzmacniacze, co podnosi koszty inwestycyjne. Dodatkowo, urządzenia do zarządzania i monitorowania transmisji optycznej w WDM są bardziej złożone technologicznie.

Z kolei w technologii SDH urządzenia są zazwyczaj tańsze, ponieważ opierają się na bardziej ustandaryzowanych i dojrzałych technologiach transmisji cyfrowej. Koszty związane z SDH obejmują przede wszystkim urządzenia do multipleksacji czasowej, które są prostsze w porównaniu do rozwiązań WDM. SDH pozwala na łatwą integrację z istniejącymi systemami, co obniża koszty wdrożenia w porównaniu z WDM, które może wymagać znacznych inwestycji w infrastrukturę światłowodową oraz specjalistyczne urządzenia optyczne.

Routing w sieci ATM

Do zapewnienia właściwego trasowania komórek przez sieci ATM stosuje się jeden z trzech sposobów wyznaczania połączeń: routing centralny, routing rozproszony oraz najnowszą wersję routingu mieszanego – znanego pod nazwą przełączników z

protokołem MPOA.

Historycznie pierwszym i nadal jeszcze stosowanym jest routing cenrtalny. Polega on na instalacji w sieci ATM jednego dużego, szybkiego i inteligentnego routera, włączonego jednocześnie do wielu (wszystkich) sieci wirtualnych. Ze względu na ograniczoną wydajność, skalowalność i odporność pojedynczego routera centralnego i jego łącza, rozwiązanie to nie daje się do trasowania w większych sieciach ATM.

Powiązanie protokołem typu OSPF kilku równolegle działających routerów centralnych, rozmieszczonych w różnych punktach sieci ATM, pozwala na zwiększenie niezawodności (odporności na awarię każdego z nich) i wzrost ich wydajności. Brak wiedzy o topologii sieci powoduje, że dane między sieciami wirtualnymi mogą być przesyłane okrężnymi trasami.

Odmiennym i bardziej efektywnym rozwiązaniem jest routing rozproszony, w którym każde urządzenie dostępowe Ethernet / ATM jest jednocześnie przełącznikiem brzegowym (warstwa 2) i routerem (warstwa 3). Każde urządzenie dostępowe z możliwością trasowania jest włączone do wszystkich sieci wirtualnych, w których uczestniczy, a wybór najlepszego routera jest dokonywany protokołem typu OSPF *(Open Shortest Path First)*, stosowanym w sieciach TCP / IP. Wadami routerów rozproszonych są: wysoki koszt urządzeń, trudności w administrowaniu całością sieci oraz konieczność implementacji zabezpieczeń, gdyż routing dokonuje się w wielu niezależnie konfigurowanych węzłach.

Współczesną odmianę routingu rozproszonego jest protokół MPOA *(Multi-Protocol Over ATM)*, mające zalety routingu centralnego, a pozbawiony jego wad. W tym sposobie routingu jedynymi urządzeniami trasującymi (w warstwie 3) są wybrane routery – stosunkowo nieliczne, lecz technicznie zaawansowane – znajdujące się w sieci ATM. Przy niewielkim obciążeniu całość ruchu w sieci jest trasowana przez te ustalone routery. Wzrost przepływności w sieci powyżej wyznaczonego progu powoduje

utworzenie połączenia krótszą trasą i bezpośredni przekaz pakietów przez przełączniki ATM, znajdujące się na trasie między użytkownikami, z pominięciem routera trasującego. Po ustalonym czasie nieaktywności urządzenia brzegowe „zapominają ” o bezpośrednim połączeniu, a ponowienie komunikacji dokonuje się router trasujący.

ATM a usługi telekomunikacyjne

ATM określa standard komunikacji w sieciach rozległych. Dzięki niemu zniknie bariera pomiędzy sieciami lokalnymi a rozległymi. Barierą tą jest obecnie spadek przepustowości związany z przesyłaniem danych w sieciach publicznych. Inną barierą są urządzenia realizujące połączenia w sieciach WAN, na zasadzie „przechowaj i prześlij” (np. routery).

Routing w sieci ATM

Asynchronous Transfer Mode (ATM) to technologia sieciowa opracowana z myślą o przekazywaniu różnych typów danych, takich jak głos, wideo i dane cyfrowe, z dużą szybkością i małymi opóźnieniami. ATM znajduje szerokie zastosowanie w sieciach szerokopasmowych i telekomunikacyjnych, gdzie kluczowa jest sprawność routingu – procesu decydującego o tym, jak pakiety danych będą przekazywane z punktu nadawczego do odbiorcy w najbardziej optymalny sposób.

ATM jest siecią działającą w trybie łącza komutowanego, co oznacza, że dane przesyłane są przez ustanowione wcześniej trasy lub połączenia, a poszczególne jednostki danych, nazywane komórkami, poruszają się po tej samej trasie. Komórki mają stałą długość 53 bajtów, co sprawia, że transmisja jest przewidywalna, a opóźnienia są minimalne. Dzięki temu ATM doskonale sprawdza się w zastosowaniach wymagających dużej przepustowości i niskich opóźnień, jak wideokonferencje czy transmisje wideo.

Zasady routingu w sieci ATM

W sieci ATM routing opiera się na technologii przełączania ścieżek wirtualnych (VP – Virtual Path) i kanałów wirtualnych (VC – Virtual Channel). Są to logiczne ścieżki i kanały, po których przesyłane są dane. Routing odbywa się zatem na dwóch poziomach:

1. **Ścieżki wirtualne (VP)** – reprezentują one logiczne połączenia między dwoma punktami sieci. W jednej ścieżce może znajdować się wiele kanałów wirtualnych. VP pełnią rolę „autostrad" dla danych w sieci ATM, co ułatwia zarządzanie ruchem i przyspiesza routing.
2. **Kanały wirtualne (VC)** – są to jednostkowe połączenia w ramach ścieżek wirtualnych. Przełączniki ATM korzystają z tych kanałów, aby kierować każdą komórkę w sieci ATM do miejsca docelowego. W sieci ATM każde urządzenie jest przypisane do konkretnego kanału wirtualnego, co zapewnia sprawny i efektywny przesył danych.

W ramach sieci ATM stosuje się dwa główne typy połączeń:

- **Połączenia stałe (PVC – Permanent Virtual Circuits)** – są one ustanawiane na stałe i wykorzystywane w połączeniach, gdzie przewidywany ruch jest wysoki i regularny. PVC nie wymaga renegocjacji przy każdej transmisji, co skraca czas przesyłania danych, ale jednocześnie obniża elastyczność.
- **Połączenia zestawiane na żądanie (SVC – Switched Virtual Circuits)** – te połączenia są tworzone dynamicznie w momencie zapotrzebowania na transmisję. Są bardziej elastyczne i efektywne w zarządzaniu siecią, jednak ich zestawienie trwa nieco dłużej w porównaniu do PVC, ponieważ wymaga procesu negocjacji.

Proces routingu w sieci ATM

Proces routingu w sieci ATM różni się od klasycznego routingu

IP w sieciach pakietowych, ponieważ w sieci ATM wymagane jest uprzednie zestawienie połączenia przed przesyłem danych. Routing ten odbywa się poprzez następujące kroki:

1. **Zestawienie połączenia** – zanim dane zostaną przesłane, nawiązane zostaje połączenie, ustalane jest mapowanie kanałów i ścieżek wirtualnych między nadawcą a odbiorcą.
2. **Przełączanie ścieżek i kanałów wirtualnych** – połączenia są realizowane poprzez przełączniki ATM, które przypisują identyfikatory VP i VC. Dzięki temu każda komórka jest przesyłana zgodnie z wytyczonymi trasami.
3. **Przesył komórek** – kiedy trasa zostanie ustalona, komórki ATM podróżują przez sieć w sposób niezmienny. Została określona stała trasa, co umożliwia komórkom dotarcie do celu w stałym czasie.

W sieci ATM komórki przesyłane są bez sprawdzania ich poprawności na poziomie przełączników, co oznacza, że sieć sama w sobie nie oferuje mechanizmów retransmisji błędnych danych. Z tego powodu ATM jest bardziej zależne od jakości fizycznej infrastruktury, ponieważ błędne komórki muszą zostać odtworzone lub ponownie wysłane na poziomie aplikacji.

Metody routingu w sieciach ATM

Do routingu w sieciach ATM stosowane są różne algorytmy i metody, w zależności od skali sieci oraz wymagań jakościowych. Główne podejścia to:

- **Routing statyczny** – trasy są ustalane ręcznie przez administratorów. Sprawdza się w małych sieciach o stałej strukturze ruchu, gdzie nie ma potrzeby częstych zmian tras.
- **Routing dynamiczny** – trasy są wybierane dynamicznie na podstawie aktualnych warunków w sieci. W tym podejściu wykorzystywane są protokoły, które analizują parametry sieciowe, jak przepustowość czy opóźnienia, aby wybrać optymalną trasę.

W praktyce routing dynamiczny w sieci ATM jest rzadziej stosowany ze względu na konieczność utrzymania jakości transmisji i niskiego opóźnienia, które łatwiej osiągnąć przy trasach stałych.

Zalety i wyzwania routingu w sieci ATM

Routing w sieci ATM zapewnia wysoką efektywność, zwłaszcza w środowiskach, gdzie przesyłane są dane o stałym strumieniu, takie jak transmisje audio i wideo. Użycie komórek o stałej długości umożliwia przewidywalność ruchu oraz kontrolę nad opóźnieniami, co czyni tę technologię idealną do zastosowań, gdzie jakość transmisji jest kluczowa.

Jednak routing w sieci ATM wiąże się również z wyzwaniami, szczególnie ze względu na konieczność dokładnego planowania tras, by zapewnić wymaganą przepustowość dla różnych rodzajów danych. ATM nie jest zoptymalizowane pod kątem transmisji pakietowych o zmiennym rozmiarze, co sprawia, że współczesne zastosowania mogą być ograniczone przez specyfikę routingu stałego.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.

Analiza wyników i wnioski

We wczesnych latach dziewięćdziesiątych panowało przekonanie, że ATM odniesie sukces jako powszechnie stosowana technologia sieciowa. Zakła□dano nowe firmy, zajmujące się projektowaniem i sprzedażą przełączników ATM oraz adapterów do publicznego i wewnętrznego użytku. Jednak ATM upowszechnia się powoli. Wiele z rozwiązań wciąż jeszcze nie przybrało ostatecznego kształtu.

W szczególności klienci i producenci nadal poszukują sposobów integracji ATM z istniejącymi technologiami sieci lokalnych. W międzyczasie pojawiły się sieci Gigabit Ethernet o przepustowości jednego Gigabita, które prawdopodobnie będą stanowiły konkurencję dla technologii ATM. Oferują bowiem dużą przepustowość przy jednoczesnej zgodności z istniejącymi sieciami Ethernet.

Należy pamiętać, że obecnie coraz wygodniej jest instalować w budynkach okablowanie, które będzie mogło obsługiwać zarówno transmisję głosu, jak i danych. Wybór technologii ATM jest w takim przypadku oczywisty z uwagi na wbudowane mechanizmy QoS. Jest to ponadto technologia skalowalna, zapewniająca transmisję z prędkością od 25Mbit/s do 2.46Gbit/s, łatwo dająca się integrować z sieciami telekomunikacyjnymi.

Skalowalność ATM ma szczególne znaczenie dla rozwijających się firm. ATM nie hamuje rozwoju przedsiębiorstwa. Rosnące wymagania w odniesieniu do łączy przesyłających dane i głos mogą być spełniane przez zwiększanie szerokości pasma. Obecnie coraz szerzej upowszechniają się rozwiązania multimedialne, takie jak wideofony i wideokonferencje, odbywające się za pośrednictwem sieci. Instytucje, które nie będą korzystać z tego rodzaju usług nie sprostają konkurencji. Nie wolno zapominać, że jeszcze kilkanaście lat temu w wielu instytucjach powszechnie używano maszyn do pisania. Komunikacja jest kluczem do konkurencyjności, a usługi takie jak poczta elektroniczna, wspólne korzystanie z dokumentów, oprogramowanie do pracy grupowej, oprogramowanie sterujące obiegiem dokumentów i in. z pewnością wspomagają komunikację międzyludzką. W miarę upowszechniania się tego rodzaju usług, zwiększać się będzie zapotrzebowanie na pasmo transmisyjne. Z tego powodu technologie takie jak ATM. Gigabit czy 10Gigabit Ethernet, które są technologiami skalowalnymi, umożliwiającymi stopniowy rozwój sieci, tak by sprostać rosnącym wymaganiom.

Natomiast po dokładnej analizie standardów teleinformatycznych sieci lokalnych można wysunąć wnioski, że dominującym

standardem budowy tych sieci będzie Fast oraz XGigabitEthernet. Poza bardzo istotnym aspektem cenowym należy wziąć pod uwagę popularność tego standardu i fakt, że gro aplikacji sieciowych i internetowych oparta jest na protokole IP. A bądź co bądź żaden z analityków nie wybierze standardu droższego dającego porównywalną wydajność. Analizując ceny rozwiązań sieci lokalnych wzięto pod uwagę tylko koszty urządzeń sieciowych i okablowania. W tym przypadku nie ma sensu nawet próba wliczania kosztów montażu. Żadna z firm zajmujących się montażem okablowania strukturalnego nie podaje oficjalnych cen. Uzależnia je od ilości punktów przyłączeniowych i praktycznej możliwości ralizacji. Dlatego przy porównaniu aspektów cenowych rozwiązań dostępnych na polskim rynku

wzięto pod uwagę pewien określony na potrzeby niniejszej pracy współczynnik. Jest to mianowicie koszt 1Mb danych przy podłączaniu stacji końcowej oddalonej o 100m od koncentratora/przełącznika.

Powyższy wykres może nasunąć pytanie: czy technologia Ethernet10 jest droższa niż Ethernet100. Otóż odpowiedź jest stosunkowo prosta. Przy obecnej sytuacji rynkowej i relatywnie dużej podaży urządzeń Fast Ethernet ich ceny są wyższe od urządzeń Ethernet10. Różnica cen jest jednak niewspółmierna do różnicy uzyskiwanej przepustowości – dla FastEthernetu jest ona dziesięciokrotnie wyższa. Podobnie sytuacja ma się z Gigabit Ethernetem – tam przpustowość jest stukrotnie wyższa niż w Ethernet10. Natomiast jest to standard stosunkowo nowy i ceny urządzeń na skutek relatywnie mniejszego popytu są wyższe. Generalnie jednak panuje tendencja rynkowa sztucznego zawyżania cen produktów wykorzystujących jako media światłowody. Natomiast budowanie sieci lokalnych w oparciu o Gigabit Ethernet ma jeszcze jedną dosyć istotną wadę. Obecnie konstruowane stacje końcowe klasy PC wyposażane w dyski ULTRA-ATA i przy prędkościach magistrali rzędu 100MHz, nie nadążają za postępem w teletransmisji i nie są w stanie obsłużyć takich

przepustowości. Przeprowadzone badania wykazały, że wykorzystanie przepustowości w transmisji punkt-punkt przy zastosowaniu Gigabit Ethernetu i stacjach końcowych klasy PIII 500MHz jest na poziomie kilkunastu (15-17) procent. Na zastosowanie Gigabit Ethernetu do łączenia stacji roboczych będziemy musieli jeszcze poczekać. Natomiast standard ten sprawdza się perfekcyjnie w przypadku realizacji sieci szkieletowych rozwiązań kampusowych czy wewnątrz oroporacyjnych.

Może nasuwać się również pytanie o przyszłość ATM 25/125. Podstawowy problem w tej technologii tkwi w stosunkowo silnej pozycji Ethernetu oraz małym popycie na te urządzenia a co za tym idzie wyższą ceną. Poza tym sam proces konfiguracji i utrzymania tej sieci jest stosunkowo trudniejszy niż w przypadku Ethernetu. ATM jako standard budowy sieci będzie miał zastosowanie w przypadku systemów transmisji danych wymagających określonych przepustowości *(real time services*), takich jak głos czy wideo ale w przypadku realizacji sieci lokalnych nastąpi zanik tego standardu.

W przypadku sieci rozległych (tu: nie mylić z sieciami operatorskimi) analiza dotyczy głównie analizy kosztów dostępu do sieci operatorskich i rozległych połączeń korporacyjnych (np. ISP, połączenia między oddziałami firmy). W zasadzie rozważane są połączenia punkt-punkt, które podzielono w celu lepszej analizy na dwie grupy:

– połączenia stałe (Frmae Relay, XDSL)

– połączenia dodzwaniane (PPP, L2TP, ISDN)

W ramach grupy połączeń dodzwanianych analizie poddano tutaj standardy PPP, L2TP raz ISDN. Tabela 42 obrazuje koszty montażu (instalacji) łącz opartych na tych standardach i korzystania z nich przy transmisji na poziomie 64Kb/sek.

Jak widać są to koszty transmisji są podobne w obydwu przypadkach. Można dokonać pewnej hierarchii technologii pod

kątem ich funkcjonalności oraz przydatności do konkretnych zapotrzebowań. Technologię PPP stosuje się masowo jako metodę dostępu do ISP *(Internet Service Provider)*. Można ją również stosować do połączeń pomiędzy oddziałami firmy ale tylko w przypadku bardzo małego ruchu centrala <-> oddziały. Jeżeli pomiędzy oddziałami dane wymieniane są na zasadzie *Not Real Time Services* (np. transfer plików, poczta elektroniczna, wysyłanie sprawozdań dziennych, itp.) to zastosowanie standardu PPP jest celowe. W przypadku L2TP sytuacja jest podobna aczkolwiek daje prawie 18 krotne (!) obniżenie kosztów w przypadku gdy oddziały firmy znajdują się poza granicami Polski. Zastosowanie obu tych metod jest sensowne ale tylko w przypadku gdy cały sumaryczny transfer danych jest na poziomie maksymalnie kilku Mb. Inaczej przestaje się to opłacać ze względu na to, że połączenie musi być wówczas zestawiane a tym samym i taryfikowane przez stosunkowo długi kres czasu.

Natomiast usługi ISDN mają tę przewagę nad klasyczną telefonią, że rzeczywiście mamy do dyspozycji w przypadku dostępu podstawowego 128Kb/sek. Jednoczesne wykorzystanie obu daje nam możliwość posiadania na jednej linii łącza telefonicznego oraz łącza danych o przepustowości 64kb/sek. Poza tym że nie blokujemy sobie linii telefonicznej na czas transmisji jak to ma miejsce w przypadku PPP/L2TP. Dodatkowo są to kanały cyfrowe a co za tym idzie mamy rzeczywiście 64kb/sek a nie jak w PPP/L2TP <64kb/sek. W przypadku PPP/L2TP należy liczyć się z faktem, że linie analogowe realizowane na skrętce w zależności choćby od jakości montażu i warunków pogodowych zmieniają swoje parametry i w rzeczywistości uzyskujemy czasem dużo mniejsze (nawet o połowę) faktyczne przepustowości takich linii. Dodatkowo ISDN ułatwia dosyć proste skalowanie – możemy agregować obydwa kanały B i stawiając po obu stronach routery uzyskać połączenie na poziomie 128kb/sek.

Natomiast w przypadku grupy połączeń stałych dokonano porównania dwóch najszerzej stosowanych w Polsce rozwiązań

konstrukcyjnych. Są to standardy Frame Relay oraz xDSL. Należy zauważyć, że w warunkach polskich istnieje pewna nieścisłość w przypadku tych dwóch rozwiązań. Wynika ona z faktu, że operatorzy sieci Frame Relay de facto stosują standardy xDSL jako metodę realizacji łącza dostępowego do operatorskiej sieci Frame Realy (TP S.A., Telbank). Poniższa tabela i wykres obrazują porównanie kosztów obydwu rozwiązań.

Porównanie funkcjonalno cenowe jest tutaj utrudnione. Wynika ono przede wszystkim z baraku liniowości wzrostu opłat za usługi Frame Relay w zależności od parametrów łączy (CIR, odległość punktów końcowych). Dlatego na potrzeby niniejszej analizy przyjęto pewne założenia. Teoretyczna linia ma zasięg 5km a ceny odnosimy do 64 kilobitowego łącza transmisyjnego. Dodatkowo w przypadku łączy stałych za kilometr łącza płacimy opłatę abonamentową zawsze a w przypadku Frame Relay tylko wtedy gdy mamy do czynienia z łączem długim (np. Warszawa-Poznań a nie wewnątrz metropolii).

xDSL jest jak można zauważyć optymalną techniką w przypadku realizacji łącz transmisji danych na odległościach rzędu kilku kilometrów. Wykorzystuje ona sytuacje rynkowo techniczną polskiego ogólnopolskiego operatora telekomunikacyjnego (TP S.A.). Przeważająca ilość połączeń miedzianych umożliwia im jeszcze zestawianie bezpośrednich linii dedykowanych na krótkich kilkukilometrowych odległościach. Wraz z postępem i wymianą infrastruktury telekomunikacyjnej podstawowym medium stanie się światłowód i wykorzystywanie tego typu łącz stanie się niemożliwe. Dlatego obecnie pomimo rozwoju technologii xDSL coraz szerzej mówi się o modemach światłowodowych. Jest kwestią bezdyskusyjną, że operacje kodowania i kompresji dają znaczne zyski klientom dzierżawiącym linie (można zamówić tańsze łącze o mniejszej przepustowości). Jednak przez najbliższe kilkanaście lat technologie xDSL będą wiodły prym w swojej klasie zastosowań. Kolejnym krokiem będzie wymiana istniejących torów na łącza cyfrowe operatora lokalnego/krajowego. Jednak ceny tych łącz są o wiele wyższe

niż rozwiązań opartych na technice xDSL. Natomiast wymiana skrętki na światłowód w strefie dostępu do klienta przez bardzo długi okres będzie nieopłacalna dla operatora i dostęp szerokopasmowy do sieci operatorskiej będzie realizowany w technologii xDSL. Natomiast w kwestii sieci Frame Relay to istniejąca infrastruktura jest i będzie wykorzystywana przez najbliższe lata. Jednak znacząca pozycja ATM w dziedzinie sieci transmisji danych może mieć wpływ na proces utraty rynku przez standard FrameRelay. Jednak w porównaniu z techniką xDSL i rozwiązaniach rozległych (np. krajowych) jest relatywnie tańszą techniką niż dzierżawa kanałów cyfrowych. Poza tym daje elastyczność nie zapewnianą przez dzierżawione łącza cyfrowe. Jednak w opinii autorów zostanie wyparta przez standard ATM dający lepszą funkcjonalność i skalowalność. ATM daje też bardziej optymalniejsze i efektywniejsze wykorzystanie zasobów sieci operatora telekomunikacyjnego oraz znacznie lepsze możliwości utrzymywania jakości usług dzięki zaimplementowanym mechanizmom QoS. Rozwiązania oparte o ATM dodatkowo nie wymagają zmiany infrastruktury dostępowej. Nowe łącza dostępowe o większej przepustowości budowane są w oparciu o technikę światłowodową lub xDSL *(ATM over xDSL)*.

Sieci rozległe

FDDI

Standard FDDI *(Fiber Distibuted Data Interface)* opracowany został przez komitet X3T9.5 Amerykańskiego Instytutu Normalizacyjnego ANSI. Pierwotnie był przeznaczony do

zastosowań z wykorzystaniem kabla świa□tłowodowego (stąd nazwa), lecz obecnie istnieje również wersja wykorzystująca kable miedziane (na znacznie krótszych dystansach). Bywa stosowany w sieciach kampusowych. Pracuje w topologii podwójnego pierścienia, zawierającego do 500 węzłów. Maksy□malna długość pierścienia wynosi 100 km, a szybkość transmisji 100 Mb/s. Te parametry kwalifikują standard FDDI do zastosowań w sieciach metro□politalnych MAN *(Metropolitan Area Network)* i WAN *(Wide Area Network).*

Istotną zaletą FDDI jest wyższa w stosunku do innych standardów protekcja sieci. Podwójna pętla pierścienia daje zabezpieczenie (redundancję) na wypadek awarii. W takiej sytuacji pierścień rekonfiguruje się, a cała sieć nie przerywa pracy. Każda stacja posiada przekaźniki, które zamykają pierścień w razie jego uszkodzenia lub omijają stację w przypadku jej awarii.

Standard FDDI jest często wykorzystywany w charakterze sieci szkieletowej. Segmenty sieci lokalnych (LAN), wraz z systemami minikomputerowymi, mainframe i innymi, dołączane są do takiego szkieletu. W przypadku bardzo małych sieci, zawierających pojedyncze segmenty LAN, bardziej celowe może być zastosowanie, jako szkieletu, kabla koncentrycznego Ethernet. Standard FDDI jest jednak zdecydowanie lepszy w przypadku sieci z wieloma segmentami LAN, o znacznym natężeniu ruchu, pochodzącego od szybkich lub graficznych stacji roboczych. Warto zauważyć, że szybkie wersje standardu Ethernet (Fast Ethernet i 100VG-AnyLAN) są tak samo funkcjonalne, jak FDDI, lecz ich ogranicze□nia odległościowe nie pozwalają na zastosowania w sieciach szkieletowych o dużym zasięgu. Konkurencją tu niewątpliwie będzie GigabitEthernet budowany w oparciu o światłowody jednomodowe (zwłaszcza na odległościach do kilku kilometrów).

Typowe rozwiązanie sieci teleinformaytcznej w oparciu o standard FDDI przedstawiono na rysunku 46. Urządzenie podłączone do obydwu pierścieni może zamknąć je w przypadku

przerwy w dowolnym punkcie, czego nie potrafi stacja podłączona tylko do jednego z nich (za to jest tańsza). Jeśli uszkodzeniu ulegnie komputer podłączony do koncentratora FDDI, ten ostatni zapewnia ciągłość pierścienia (nie zależy ona od karty w komputerze).

Standard FDDI wykorzystuje kable optyczne (jednomodowe i wielomodowe), jak również kable miedziane – skrętkę nieekranowaną UTP oraz ekranowaną STP. Wersje pracujące na kablu miedzianym należą do standardu CDDI *(Copper Disributed Data Interface),* którego zasięg jest ograniczony do l00m. W standardzie FDDI uzyskuje się dostęp do medium metodą *token passing* (przekazywanie znacznika).

Standard FDDI-II został opracowany dla sieci, w których konieczne jest przesyłane dużych ilości danych w czasie rzeczywistym. Jest to taka modyfikacja systemu FDDI, aby możliwe było przenoszenie synchronicznych danych. Konieczne jest, aby wszystkie węzły sieci posiadały interfejs FDDI-II, w przeciwnym wypadku będzie ona pracować jak podstawowy FDDI. Funkcjonujące stacje FDDI powinny zostać podłączone do oddzielnej sieci. Standard FDDI-II nie został jednak powszechnie przyjęty ze względu na brak kompatybilności z używanym do tej pory FDDI. Poza tym, systemy Fast i GigabitEthernet oraz ATM oferują w większości wypadków podobne bądź lepsze rozwiązania.

Alternatywną techniką okablowania w standardzie FDDI może być zastosowanie miedzianej skrętki nieekranowanej (UTP). Taka wersja systemu nosi nazwę CDDI. Sieć taką, realizowaną za pomocą kabla do transmisji danych kategorii 5 oraz ekranowanej skrętki IBM typ l (STP), określa standard ANSI TP-PMD (*Twisted–Pair–Physical-Medium-Dependent).* Poza długością kabla, zachowane są w tym przypadku wszystkie parametry FDDI. Skrętka nieekranowana (UTP) umożliwia lokalizację węzłów sieci w odległości do 100 m, podczas gdy światłowód – do 2km.

Jest to standard, który powoli traci na popularności na rzecz

FastEthernetu i GigabitEthernetu. Kart sieciowych opartych na standardzie FDDI praktycznie się nie spotyka a jeżeli już to firmy mają pojedyncze egzemplarze w celach serwisowych i nie prowadzą ich sprzedaży. Natomiast spotyka się jeszcze ten standard w sieciach kampusowych i metropolitalnych. Aczkolwiek w tym środowisku jest to również standard zanikający. Wypierany jest z rynku głównie przez ATM oraz GigabitEthernet – standardy dające większa skalowalność i kompatybilność z istniejącymi standardami.

PPP *(Point to Point Protocol)*

Społeczność internetowa przyjęła dwie metody hermetyzacji i przesyłania datagramów protokołu IP *(Internet Protocol)* poprzez szeregowe połączenia typu "punkt z punktem". Jednym z nich jest protokół SLIP *(Serial Line Internet Protocol)*, drugą – protokół PPP *(Point-to-Point Protocol)*. O ile pierwotnie używano SLIP, jednak obecnie dominuje protokół PPP, gdyż umożliwia współpracę z innymi protokołami, np. IPX *(Internetwork Packet Exchange)*. PPP zdefiniowano w raportach IETF *(Internet Engineering Task Force)* RFC o numerach od 1661 do 1663.

Protokół PPP zapewnia połączenia routera z routerem, komputera z routerem i komputera z komputerem. Jest on powszechnie wykorzysty□wany do nawiązywania łączności z Internetem poprzez linie telefoniczne.

Na przykład użytkownicy pracujący w domu mogą zadzwonić do swojego lokalnego dostawcy usług internetowych (ISP). Gdy modemy nawiążą połą□czenie, pomiędzy komputerem użytkownika i ISP tworzona jest sesja PPP. Proces ten może obejmować weryfikację tożsamości użytkownika oraz przypisanie mu numeru IP. Zasadniczo od tej chwili komputer użytkowni□ka staje się rozszerzeniem sieci IP obsługiwanej przez dostawce usług inter□netowych. Port szeregowy i modem użytkownika posiadają ten sam zakres funkcjonalności jak karty sieciowe przyłączone do sieci ISP. Protokół PPP hermetyzuje pakiety protokołów

wysokiego poziomu i przesyła je poprzez łącze.

Warstwa fizyczna protokołu PPP umożliwia transmisję poprzez łącza asynchroniczne i synchroniczne przy pomocy różnych protokołów, np. EIA-232-E, EIA-422, EIA-423 oraz CCITT V.24 i V.35. Warstwa łącza danych oparta jest na strukturze ramki typu HDLC *(High-level Data Link Control)*. Do tworzenia i kontroli kanału łączącego dwie maszyny wykorzystuje się protokół LCP *(Link Control Protocol)*.

Koszty takiego rozwiązania są relatywnie niskie i porównywalne z techniką USB. Technikę tę masowo stosuje się do korzystania z usług ISP. Zasadniczo koszt modemu jest uzależniony kilku czynników:

– maksymalnej przepływności która można przy jego pomocy uzyskać,

– interfejsu wymiany danych z komputerem (PCI/ISA/zewnętrzny RS),

– funkcji dodatkowych (własny procesor sygnałowy, fax, sekretarka),

– firmy go produkującej.

Obecnie praktycznie nie stosuje się modemów o przepływnościach mniejszych niż 56kb/s a ich ceny mają tendencję spadkową.

Podane ceny odzwirciedlają oczywiście polską specyfikę rynku telekomunikacyjnego oraz podane są przy założeniu, że połączenie z serwerem ISP jest w ramach taryfikacji połączeń lokalnych. Oczywiście istnieją metody dostępu do ISP zwane *CallBack* jednak nie odbiegają one praktycznie kosztowo od standardowego rozwiązania opartego na PPP.

L2TP

L2TP *(Layer 2 Tunneling Protocol)* jest jednym z protokołów stworzonych pod kątem ninimalzacji i redukcji kosztów połączeń

z sieciami odległymi poprzez linie telefoniczne. Najtańszym rozwiązaniem jest oczywiście Internet i usługi oferowane przez jej operatorów ISP *(Internet Sevice Provider).* Kluczowe znaczenie ma tutaj właśnie protokół L2TP, stworzony na podstawie protokołu L2F *(Layer 2 Forwarding)* firmy Cisco.

Firmy Microsoft i Cisco Systems opracowały podobne protokoły wirtualnych połączeń komutowanych, stawiając sobie jednak odmienne cele. Obydwa rozwiązania pozwalają na przekazywanie usług zdalnego dostępu operatorom ISP. Z uwagi na fakt, iż firma Cisco jest przede wszystkim producentem sprzętu, stosowanie jej protokołu L2F wymaga rozbudowy bazy sprzętowej – zarówno po stronie operatora, jak i usługobiorcy – o urządzenia z nim kompatybilne. Protokół L2F obsługuje szereg protokołów warstwy 3, natomiast protokół L2TP jest rozszerzeniem L2F – nie wymaga dodatkowego sprzętu, umożliwiając ponadto kontrolę przepływu danych.

Typowe połączenia internetowe, nawiązywane przez użytkownika linii komutowanych, dokonywane są przy użyciu protokołu komunikacji między dwiema stacjami – PPP *(Point-to-Point Frotocol).*L2TP zwiększa możliwości protokołu PPP – oferując zdalnemu użytkownikowi możliwość przedłużenia łącza PPP, poprzez Internet, do serwera instytucji/firmy. Z reguły w takiej sytuacji tworzony jest tunel łączący (poprzez Internet), sprzedawcę usług internetowych z instytucją. Gdy tunel zostaje utworzony użytkownik może komunikować się z siecią korporacyjną poprzez łącze, które symuluje zwykłe, bezpośrednie połączenie komutowane.

Takie rozwiązanie znajduje uzasadnienie z kilku powodów:

– Zamiast nawiązywać połączenie międzymiastowe (do bezpośredniego skomunikowania się z korporacyjnym serwerem zdalnego dostępu NAS), użytkownik odległy łączy się jedynie z lokalnym operatorem internetowym.

– Protokół realizuje wirtualne łącze komutowane *(virtual dial-*

up), ponieważ użytkownik nie nawiązuje połączenia z siecią korporacyjną przez łącze komutowane. Połączenie realizowane w rzeczywistości tylko symuluje (udaje) łącze komutowane.

– Dzięki hermetyzacji w ramkach protokołu PPP, użytkownik odległy może uzyskiwać dostęp do komputerów swej firmy/instytucji używając różnych protokołów – np. IP, IPX, SNA.

– Protokół L2TP zapewnia przezroczystość systemów końcowych. Oznacza to, że zarówno odległy użytkownik jak i serwer korporacyjny, nie wymagają – by bezpiecznie usługę tę realizować – specjalnego oprogramowania.

– Instytucja może korzystać z własnych metod autoryzacji użytkowników, niezależnych od operatora internetowego

Połączenie pomiędzy klientem odległym a siecią korporacyjną działa jak zwykłe połączenie PPP. Protokół L2TP realizuje zadanie identyfikacji tożsamości użytkownika, jednak dane przesyłane przez Internet nie są kodowane. Istnieje więc tu pewna luka jeżeli chodzi o bezpieczeństwo danych. W tym celu stosuje się rozwinięcia protokołu IP, np. IPSec realizujący procedurę kodowania danych dla różnych protokołów tunelowych.

Niewątpliwie jest to rozwiązanie znacznie obniżające koszty połączeń o zasięgu globalnym i światowym. Korzystając ze standardowego połączenia PPP, w warunkach polskich uzyskuje się 18-krotne (!!!) obniżenie kosztów połączenia. Aczkolwiek zakres stosowania tego rozwiązania ma sens jedynie wówczas (warunki polskie) gdy w tradycyjnym połączeniu PPP musielibyśmy skorzystać połączeń międzynarodowych. Kolejnym mankamentem tego rozwiązania są ograniczenia pasma takiego kanału wynikające z samej specyfiki połączeń komutowanych. Maksymalnie jesteśmy w stanie przesłać do 56K używając wąskopasmowych modemów analogowych. Wynika to z ograniczenia pasma przez operatora telekomunikacyjnego na wejściach urządzeń komutujących w centralach. Stosowanie modemów

szerokopasmowych nie spowodowałoby poprawy sytuacji. Dodatkowo należy wziąć pod uwagę zmniejszenie przepustowości rzeczywistej wynikającej z informacji dodanych samego protokołu oraz z faktu czasowych przeciążeń w sieciach internetowych. Kosztowo rozwiązanie kształtuje się praktycznie identycznie jak standardowe rozwiązania PPP. Należałoby jedynie dodatkowo doliczyć koszty licencji oprogramowania.

xDSL

Technika cyfrowej linii abonenckiej DSL *(Digital Subscriber Line)* może zdecydowanie poprawić efektywność wykorzystania rzeczywistego pasma transmisyjnego istniejącej sieci abonenckiej. DSL umożliwia osiągnięcie szybkości dochodzących do 52 Mb/s.

Stosowanie technik DSL poprawia efektywność wykorzystania istniejących połączeń wykonanych w oparciu o skrętkę miedzianą, poprowadzonych między lokalną centralą a większością abonentów. Szerokość pasma częstotliwości w takim prze□wodzie jest ograniczona i możliwe jest tylko transmisja danych z szybkością 64kb/s. Wprawdzie sama skrętka umożliwia transmisję z większą szybkością, jednak urządzenia zainstalowane w centralach telefonicz□nych zawężają pasmo uniemożliwiając uzyskanie szybkości większej niż 64kb/s. Dzieje się tak w przypadku łączy komutowanych. Jednak miedzy innymi w Polsce operatorzy telekomunikacyjni umożliwiają zestawianie linii dzierżawionych omijających cyfrowe urządzenia komutujące. Daje to szerokie pole dla wykorzystywania technik XDSL, które są w stanie wykorzystać praktycznie szersze pasmo linii dzierżawionych niż ma to miejsce w przypadku połączeń komutowanych realizowanych w warstwie dostępowej na bazie tego samego medium fizycznego (skrętka nieekranowana).

Linie DSL mogą być symetryczne (dane przepływają z tą samą szybkością w obu kierunkach) lub asymetryczne (szybkość przesyłania danych do abonenta jest większa niż od abonenta do

sieci). Łącza asymetryczne dobrze nadają się do komunikacji z Internetem, gdyż z reguły użytkownicy więcej danych pobierają niż wysyłają.

Należy pamiętać, że wraz ze wzrostem szybkości transmisji, zmniejsza się jej maksymalny zasięg. Linia dedykowana na stałe łączy abonenta z siecią FrameRelay, ATM lub punktem dostępu do Internetu (ISP). Abonent musi dysponować odpowiednim modemem DSL, a operator – odpowiednio wyposażoną centralą.

Bliższego omówienia wymagają główne typy techniki DSL najszerzej stosowane w sieciach teleinformatycznych:

– HDSL *(High-bit-rate Digital Subscriber Line).* HDSL to najczęściej spotykany i najbardziej dojrzały wariant usług DSL. Zapewnia szybkości transmisji odpowiadające przepustowości linii Tl (1.544Mbit/s) w liniach o maksymalnej długości 3.6km. Praktycznie technika HDSL umożliwia transmisję danych z większymi szybkościami (np. 2048Mb/s) aczkolwiek jest to w dużej mierze uzależnione od parametrów linii (długości, parametrów fizyczne samej skrętki: izolacji, średnicy żył miedzianych, itp.). W literaturze spotyka się opisy, że linie dedykowane powinny być oddzielone fizycznie od łącz telefonicznych. Jednak w warunkach praktycznych i nowych modemach HDSL warunek ten nie jest konieczny do spełnienia.

– SDSL *(Symmetrical Digital Subscriber Line).* SDSL to symetryczna, dwukierunkowa linia DSL, podobna do HDSL lecz zrealizowana w postaci pojedynczej pary przewodów (skrętki). Wykorzystuje częstotliwości wykraczające poza pasmo głosu, dzięki czemu w tym samym przewodzie można przesyłać głos i dane.

– ADSL (*Asymmetrical Digital Subscriber Line).* ADSL ma największe szansę zdobycia popularności jako szybka technologia telekomunikacyjna, przeznaczona do użytku w pętli lokalnej, tj. między abonentem a centralą. Jest to technika asymetryczna, co oznacza że transmisja do użytkownika odbywa

się znacznie szybciej niż transmisja do sieci. Odpowiada to potrzebom typowego użytkownika Internetu, który więcej informacji pobiera z serwerów WWW niż do nich wysyła. ADSL wykorzystuje częstotliwości wykraczające poza pasmo głosu, a zatem ten sam kabel może być używany przez oba systemy telekomunikacyjne. Szybkość transmisji od użytkownika do sieci mieści się w przedziale od 16kb/s do 640kb/s, natomiast w drugim kierunku od 1,544Mb/s (5,5km linii) do 8,448 (2,7km linii).

– VDSL *(Very high bit rate Digital Subscriber Line).* VDSL to technologia podobna do ADSL, lecz zapewniająca znacznie większe szybkości transmisji danych. Ma charakter asymetryczny, a zatem transmisja do użytkownika odbywa się szybciej niż transmisja do sieci. Usługi VDSL mogą być realizowane przy wykorzystaniu przewodów sieci telefonicznej i ISDN. Szybkości transmisji od użytkownika do sieci mieszczą się w przedziale od 1,6 Mb/s do 2,3Mb/s., natomiast w drugim kierunku od 12,96Mb/s (1,4 km linii) do 51,84 (0,3km linii)

– RADSL *(Rate-Adaptive Digital Subscriber Line).* Usługi zbliżone do ADSL, lecz zapewniające dodatkowo możliwość dopasowania szybkości transmisji do jakości i długości linii. Przy nawiązaniu połączenia szybkość transmisji ustala się, korzystając z techniki odpytywania linii *(line polling).*

W przypadku abonentów instytucjonalnych, linia ADSL może bezpośrednio przesyłać komórki ATM do przełączników ATM operatora. W komórkach ATM, przesyłanych linią ADSL, umieszcza się pakiety IP. Firma Arial Corporation opracowała kartę ATM, umożliwiającą bezpośrednie – bez użycia modemu – podłączenie stacji roboczej do linii ADSL.

W systemach ADSL stosuje się obecnie dwie konkurencyjne metody kodowania (modulacji) sygnału. Pierwsza metoda nosi nazwę DMT *(Discrete MultiTone)* i ma status standardu ANSI. Za alternatywną techniką – CAP *(Carrierless Amplitude and Phase)* – opowiada się wielu producentów. W modemach ADSL,

wykorzystujących technikę modulacji DMT, stosowane jest multipleksowanie z podziałem częstotliwości, co pozwala na utworzenie trzech oddzielnych kanałów. Są to kanały odpowiednio dla: transmisji głosu (telefonicznych), wolnych transmisji od użytkownika do sieci i szybkich transmisji z sieci do użytkownika. Łącze do transmisji głosu jest dzięki odpowiednim filtrom odizolowane od kanałów ADSL i zapewnia gwarantowaną, ciągłą obsługę rozmów telefonicznych. Separacja kanałów głosu i danych zachowana jest także w centrali telefonicznej, co pozwala na ograniczenie zatorów w sieci telefonicznej.

W przypadku rozwiązań opartych na technice xDSL należy wziąć pod uwagę warunki polskie (tylko takie w istocie nas interesują). Dzierżawa łącz dedykowanych poza obszarem lokalnym mija się praktycznie z celem. Wynika to ze specyfiki rozwiązań sieci transmisyjnych polskich operatorów telekomunikacyjnych. Połączenia lokalne w ramach aglomeracji najczęściej prowadzone są z użyciem par miedzianych. Natomiast w przypadku połączeń strefowych i międzystrefowych połączenie klient – operator jest realizowane przy wykorzystaniu skrętki miedzianej jednak potem w przypadku przesyłania między- i strefowego połączenie wchodzi na trakty SDH o określonej przepustowości (dla telefonicznych usług standardowych 64Kbs/). Dlatego też techniki xDSL maja zastosowanie w dwóch przypadkach:

1. System końcowy musi leżeć w ramach tej samej aglomeracji gdzie istnieje możliwość poprowadzenia skrętki miedzianej bez wprowadzania sygnału na przełącznice cyfrowe ,

2. Systemem końcowym jest operator telekomunikacyjny będący jednocześnie dostawcą usług (np. ISP).

Koszty takiego rozwiązania podzielić można na dwie grupy: sprzęt wraz z montażem i opłaty miesięczne za dzierżawę takiej linii.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.

Przełączniki

Przełącznik *(switch)* to urządzenie, pozwalające zrealizować podobną koncepcję jak most, tyle że na większą skalę. Tradycyjny most ma dwa porty i pozwala na połączenie dwóch segmentów sieci. Natomiast przełącznik wyposażony jest w całą macierz portów, pozwalającą na łączenie większej liczby segmentów. Jeśli stacja chce wysłać dane do komputera podłączonego do innego portu, przełącznik szybko utworzy tymczasowe połączenie między dwoma portami, tak że wszystkie stacje robocze podłączone do tych portów znajdą się na chwilę w jednym segmencie sieci. Komutacja służy zwiększeniu wydajności sieci LAN poprzez ograniczenie liczby stacji w każdym segmencie. Sam przełącznik przesyła ramki między portami z bardzo dużą szybkością i nie wprowadza w sieci opóźnień. Najlepszą wydajność uzyskuje się w sytuacji, gdy do każdego portu podłączona jest tylko jedna stacja. Wówczas w ogóle nie występują konflikty dostępu do medium. Przełącznik na czas transmisji tworzy połączenie między portem nadawcy a portem odbiorcy.

Przełączniki funkcjonują w warstwie łącza danych modelu protokołów OSI. W związku z tym w literaturze technicznej spotyka się określenie *Layer 2 switching,* czyli „komutacja w warstwie 2''. Technikę dzielenia sieci LAN nazywa się *mikrosegmentacją,* gdyż sieć można dzielić na coraz mniejsze segmenty – aż do chwili, gdy pojedynczy port można przeznaczyć do obsługi.

Stosowane przełączniki posiadają wiele portów, przy czym każdy z nich w zasadzie odpowiada segmentowi sieci. Przełączniki mogą błyskawicznie połączyć ze sobą dowolne dwa porty, dzięki czemu przyłączone do nich urządzenia stają się częścią tej samej domeny rozgłaszania *(broadcast domain).*

Przełączniki umożliwiają łatwe konstruowanie sieci hierarchicznych, której przykład ilustruje rysunek 31. U wierzchołka struktury umieszczony jest przełącznik o dużej wydajności, który obsługuje ruch generowany przez urządzenia niższego poziomu, integrujące lokalne sieci wydziałowe lub grupy robocze. W tak zorganizowanej sieci można łatwo zestawić połączenie między dwoma dowolnymi urządzeniami.

Przełączniki są wrażliwe na przeciążenia, ale tradycyjne metody sterowania przepływem danych nie mają tu zastosowania. Problemem bowiem nie jest szybkość przełącznika, ale porty, które nie są w stanie odebrać wszystkich, przesyłanych do nich ramek i komórek.

Przełączniki ATM różnią się zasadniczo pod względem odporności na przeciążenia od przełączników sieci lokalnych. Zanim w przełączniku ATM zostanie wysłana jakakolwiek ramka, urządzenie tworzy tak zwane połączenie wirtualne. Dzięki kalkulacji przepływności ustanowionego łącza, przełącznik ATM może zapobiegać przeciążeniom.

Dla kontrastu, w sieciach lokalnych pakiety (ramki) są przesyłane bezpośrednio do przełączników, bez wcześniejszej konfiguracji połączenia. Jeśli liczba ramek przekroczy możliwości przełącznika, to niektóre pakiety mogą być utracone. Dlatego urządzenia przełączające w sieciach lokalnych są zazwyczaj wyposażone w bufory, które przetrzymują pakiety kierowane do zajętych portów. Metoda jest co prawda skuteczna, ale obniża wydajność urządzenia, gdyż buforowanie danych powoduje przerwy i opóźnienia w transmisji. Najlepszym rozwiązaniem jest po prostu zakup bardzo szybkiego przełącznika.

Routery

Routery są urządzeniami sieciowymi, przeznaczonymi do łączenia zarówno podobnych, jak i niejednorodnych segmentów sieci. Routery pozwalają każdej podłączonej sieci zachować jej wewnętrzne adresy, charakterystyki rozgłaszania itp., ale każde połączenie z inną siecią musi się odbywać za ich pośrednictwem.

Dostępne na rynku urządzenia umożliwiają wybór z całej gamy routerów wyposażonych w interfejsy, dostosowane do wymagań każdej sieci lokalnej i rozległej. Standardowy router jest wyposażony w procesor, pewną ilość pamięci i dwa lub więcej interfejsy wejścia/wyjścia. Po otrzymaniu przesyłki, urządzenie przetrzymuje ją chwilowo w pamięci. W tym czasie sprawdza nagłówek pakietu, aby określić docelowe miejsce informacji, analizuje, czy przesyłka nie jest uszkodzona oraz sprawdza jej licznik skoków. W przypadku, gdy pakiet nie jest uszkodzony, a jego licznik dopuszczalnych przeskoków jest większy od zera, router przebudowuje nagłówek przesyłki i transmituje ją do kolejnego portu sieci.

Za wytyczanie marszruty pakietu odpowiedzialne są protokoły oraz algorytmy routingu. Routery wykorzystują te protokoły do porozumiewania się między sobą, celem zdobycia wiadomości o topologii sieci. Na podstawie zgromadzonych informacji budują następnie tablice połączeń *(routing tables)*, które pełnią rolę mapy przy przesyłaniu pakietu. Bazując na informacjach zawartych w tablicach połączeń, routery wybierają trasę kolejnego etapu na drodze pakietu.

Podsumowując routery realizują następujące funkcje:

– Ograniczają przepływ danych nadawanych w trybie rozgłoszeniowym *(broadcast)* pomiędzy sieciami. Kierując się wbudowaną „inteligencją" decydują o przekazaniu (lub nie) pakietów do innych sieci.

– Pełnią rolę bariery ochronnej (tzn. filtrują dane

przepływające między sieciami, analizując ich adresy IP, dane aplikacji, itp.)

– Zapewniają połączenia z sieciami rozległymi.

– Umożliwiają budowę sieci z nadmiarowymi, alternatywnymi torami przepływu danych.

Modemy

Modem jest to urządzenie umożliwiające połączenie dwóch komputerów poprzez komutowaną, publiczną sieć telefoniczną bądź łącze dzierżawione zestawione na stałe. Modem przyłączony do urządzenia transmitującego dane (DTE) zamienia jego sygnał cyfrowy na sygnał analogowy, który następnie przekazuje przez sieć telefoniczną. Modem przyłączony do urządzenia odbiorczego z powrotem zamienia sygnał analogowy na cyfrowy.

Wyróżniamy dwa rodzaje modemów:

– Modemy telefoniczne *(consumer voicegrade modems).* Większość modemów dostępnych w sklepach przeznaczona jest do współpracy ze standardowymi liniami telefonicznymi zaprojektowanymi do przekazu głosu.

– Modemy szerokopasmowe *(broadband modems).* Modemy te służą do realizacji połączeń realizowanych poza publiczną siecią telefoniczną. Przedsiębiorstwa mogą instalować linie prywatne przeznaczone wyłącznie do transmisji danych lub posłużyć się techniką mikrofalową, przekazując dane pomiędzy umieszczonymi na masztach antenami. W obu przypadkach mogą osiągnąć bardzo dużą prędkość transmisji posługując się modemami szerokopasmowymi.

Połączenie modemu z urządzeniem DTE *(Data Terminal Equipment)* realizuje się zazwyczaj poprzez kabel szeregowy lub USB *(Uniwersal Serial Bus)*. Modem telefoniczny połączony jest z centralą telefoniczną poprzez linię lokalną. W centrali dokonywana jest odpowiednia komutacja łączy, analogicznie jak

w przypadku rozmów telefonicznych, w wyniku czego powstaje bezpośrednie łącze pomiędzy modemami.

Przekaz danych poprzez połączenie lokalne podlega pewnym ograniczeniom. Ustanowiono standard, zgodnie z którym przekaz głosu odbywa się w paśmie 300-3300Hz. Układy komutacyjne odfiltrowują wyższe częstotliwości. Dlatego opracowano wiele technik – np. kodowanie i kompresję – mających na celu przekazanie w paśmie 300-3300Hz możliwie największej ilości informacji. Zauważmy, że usługi xDSL *(Digital Subscriber Line)* pozwalają wykorzystać wyższe częstotliwości, dzięki czemu można uzyskać większą prędkość transmisji w połączeniu lokalnym. Spowodowane jest to omijaniem wspomnianych powyżej układów filtrujących.

Modemy mogą działać w trybie synchronicznym, asynchronicznym lub obu. Ogólnie rzecz biorąc modemy synchroniczne są sprawniejsze od asynchronicznych i wykorzystywane są zazwyczaj do obsługi linii prywatnych.

Modemy telefoniczne dostępne są w wersjach zewnętrznych i wewnętrznych (w formie kart do komputerów). Modem zewnętrzny łączony jest ze złączem szeregowym komputera. Gdy jeden modem łączy się z drugim, ten odpowiada, po czym następuje wymiana sygnałów służąca określeniu parametrów transmisji. Podczas tej fazy wstępnej negocjowana jest maksymalna prędkość przesyłania sygnałów oraz możliwość użycia kompresji.

Modem pełnodupleksowy (*full-duplex)* przetwarza sygnały w obu kierunkach z tą samą szybkością. Nowsze, szybkie (56kb/s) modemy telefoniczne (np. X2 firmy U.S. Robotics) są asymetryczne, tj. kanał przyjmujący dane jest szybszy od kanału nadawczego.

W przypadku modemów 56kb/s istnieją dwa rywalizujące ze sobą standardy. Firma U.S. Robotics (wchodząca obecnie w skład 3Com) nazywa swą technologię X2, natomiast Lucent/Rockwell Semiconductor Systems określa swoją ofertę jako K56flex.

Modemy typu 56K stały się podstawowym wyposażeniem użytkowników Internetu. Przyczyna jest prosta: wzrost szybkości pobierania danych do 56kb/s (o ile jedna ze stron połączenia pracuje w trybie cyfrowym). Obecnie większość dostawców usług internetowych posiada banki modemów typu 56K umożliwiające ich klientom szybki dostęp do Internetu. Jednakże z wykorzystaniem tych modemów wiążą się pewne ograniczenia mające wpływ na rzeczywistą szybkość transmisji.

– Na drugim końcu linii musi znajdować się urządzenie pracujące w trybie cyfrowym. W przeciwnym wypadku modem 56K automatycznie przełącza się na tryb analogowy i szybkość transmisji spada do 28,8 lub 33,6kb/s.

– Tylko pobieranie danych przebiega z szybkością 56kb/s. Wysyłanie danych odbywa się z szybkością 28,8kb/s lub 33kb/s.

– Na drugim końcu połączenia (czyli np. u dostawcy usług internetowych lub w przedsiębiorstwie) musi być zainstalowany kompatybilny modem umożliwiający transmisję z prędkością 56kb/s.

Należy jednak zauważyć, że standardy określają maksymalne szybkości przesyłu danych, jednak zakłócenia na linii, odległość i topologia systemu komutującego mogą spowodować redukcję faktycznych osiągów modemów.

Odrębną grupę modemów stanowią modemy wykorzystywane w cyfrowych pętlach abonenckich DSL *(Digital Subscriber Line)*. Zasada działania takich modemów jest zasadniczo podobna aczkolwiek należy zwrócić uwagę na pewne charakterystyczne cechy modemów opartych na technice xDSL:

– Umożliwiają one transfer danych z przepustowością do 52Mb/s (np. w przypadku modemów VDSL)

– Najczęściej wykorzystuje się nie połaczenia komutowane w centralach operatora telefonicznego ale zestawione łącza dedykowane

– W celu zwiększenia przepływnosci wykorzystuje się wiecej niż jedną parę przewodów

– Wykorzystuje się zaawansowane metody modulacji wielowartościowych

Dzięki braku filtracji częstotliwości wyższych niż 3300Hz (jak to ma miejsce w przypadku cyfrowych central telefonicznych) przepływności są aż tak duże w porównaniu ze standardowymi połączeniami komutowanymi. Aczkolwiek dzierżawa linii dedykowanej jest znacznie droższa niż standardowe połączenia komutowane jednak generalnie jest rozwiązaniem relatywnie tańszym od bezpośrednich łączy cyfrowych (zwłaszcza światłowodowych). Analiza cenowa poszczególnych rozwiązań została przedstawiona w kolejnych rozdziałach.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.

Elementy sieci

Karty sieciowe

Karty sieciowe NIC *(Network Interface Card)* są to urządzenia umożliwiające komputerowi połączenie z siecią. Stosując nomenklaturę modelu OSI karty sieciowe działają w warstwie fizycznej i tworzą punkt przyłączenia do określonego rodzaju okablowania sieciowego (kabla koncentrycznego, skrętki lub światłowodu). Karty sieciowe definiowane są poprzez protokoły warstwy fizycznej i warstwy łącza danych. Protokoły fizyczne definiują mechaniczne i elektryczne specyfikacje interfejsu, np. fizyczny sposób przyłączania kabli. Specyfikacja

elektryczna określa sposoby transmisji strumieni bitów poprzez kabel oraz sygnały sterujące, które zapewniają odpowiednią synchronizację przesyłanych przez sieć danych. Każda karta implementuje określony sposób dostępu do nośnika, zgodny z określoną normą.

Transmisja danych z pamięci operacyjnej urządzenia końcowego może być dokonywana zgodnie z kilkoma standardami. Poniżej zostały omówione najważniejsze z nich:

– W metodzie DMA *(Direct Memory Access)* sterownik bezpośredniego dostępu do pamięci przejmuje kontrolę nad magistralą systemową i przesyła dane z karty sieciowej do odpowiedniego miejsca w pamięci komputera, co umożliwia odciążenie procesora.

– W przypadku korzystania z pamięci współdzielonej wspomniana pamięć może być zainstalowana na karcie i bezpośrednio dostępna dla procesora, lub stanowić wydzieloną część pamięci operacyjnej, do której dostęp ma zarówno procesor komputera jak i karta sieciowa.

– Z kolei w technice *bus mastering* karta sieciowa może przesyłać dane bezpośrednio do pamięci operacyjnej bez przerywania pracy procesora systemowego.

Większość kart sieciowych wyposażona jest w gniazdo umożliwiające przyłączenie układu PROM, który umożliwia zdalną inicjalizację systemu. Układ ten wykorzystuje się w komputerach bezdyskowych. Komputery bezdyskowe są tańsze od standardowych urządzeń dyskowych. Gwarantują także większy poziom bezpieczeństwa.

Koncentratory

Koncentrator *(hub)* jest jednym z istotnych elementów sieci IP. Zasadniczo jego rola sprowadza się do rozgłaszania pakietów wysyłanych z jednej stacji (aktualnie nadającej) do pozostałych stacji podłączonych do portów tego koncentratora.

Obecnie raczej odchodzi się od stosowani koncentratorów na koszt wydajniejszych przełączników. Stacje robocze, podłączone do tego samego koncentratora, mogą się wzajemnie i bezpośrednio komunikować, ponieważ należą do tej samej domeny rozgłoszeniowej *(broadcast domain).* Koncentratory „inteligentne" posiadają wbudowane funkcje zarządzające, które mogą wykorzystywać administratorzy, np. do blokady niektórych portów, monitorowania ruchu w sieciach i rozwiązywania problemów.

Koncentratory są również klasyfikowane jako „autonomiczne", „wieżowe" *(stackable)* i „modularne":

– Koncentrator autonomiczny przeznaczony jest do pracy z wydzieloną, odległą od innych grupą. Zawiera zwykle port, umożliwiający połączenie z innymi hubami.

– Koncentratory „wieżowe" podobne są do autonomicznych, z tym, że możliwe jest zestawianie ich w stosy w tej samej szafie rozdzielczej. Wtedy pracują razem jako jeden koncentrator, tworząc jedną sieć lokalną. Administrator może również utworzyć na tej bazie wiele sieci LAN i połączyć je poprzez przełączniki/routery.

– Koncentratory „modularne" zbudowane są jako otwarte platformy, wyposażone w złącza, umożliwiające instalację kart rozszerzających. Karty te mogą pełnić funkcje koncentratorów powtarzających, przełączników, koncentratorów Token Ring , wejść sieci WAN *(Wide Area Network)* i wiele innych.

Wśród koncentratorów modularnych wyróżnia się kilka głównych typów tych urządzeń. Podstawowym kryterium ich podziału jest rozwiązanie magistrali danych:

– Magistrala standardowa *(standard bus)*. Jest to stosowana w tanich urządzeniach szyna PCI *(Peripheral Component Interconnect),* taka jak w komputerach osobistych. Wszystkie podłączone do niej moduły stanowią jedną sieć lokalną.

– Magistrala zwielokrotniona *(multiple bus),* W tym rozwiązaniu płyta główna zawiera kilka szyn systemowych, każdą dla sieci LAN określonego typu. Karta rozszerzająca wkładana jest do złącza na szynie, skonfigurowanej do danego typu sieci. Połączenie wszystkich sieci odbywa się za pomocą karty routera.

– Magistrala dzielona *(segmented bus)*. W tym wypadku szyna zwielokrotniona podzielona zostaje na segmenty, spajane poprzez standardowe złącza. Administrator może wydzielić logiczne segmenty sieci lokalnych, konfigurując każdy segment jako należący do określonej sieci. Może to wykonać ręcznie lub z użyciem interfejsu zarządzającego.

– Magistrala multipleksowana *(muliplexed bus).* Pojedyncza magistrala za pomocą techniki multipleksowania zostaje podzielona na kilka szyn logicznych. Każda z nich jest kanałem w zwielokrotnionym strumieniu danych. Tak jak i przy magistrali dzielonej, logiczne segmenty mogą być dowolnie tworzone w ramach sieci fizycznej.

Dzięki funkcjom zarządzania rejestrowane są informacje na temat ruchu pakietów i powstających błędów, które pozwalają na dostrajanie i rozwiązywanie problemów sieciowych. Informacje te są przechowywane w specjalnej bazie MIB *(Management Information Base)*.Odpowiednio ustawione alarmy informują go o przekroczeniu wartości progowych pewnych parametrów, co może spowodować problemy w pracy sieci. Najpopularniejszym protokołem zarządzającym jest SNMP *(Simple Network Management Protocol).*

Mosty

Most *(bridge)* to urządzenie łączące dwa segmenty sieci. Most może służyć do zwiększenia fizycznego zasięgu sieci LAN albo dzielić dużą sieć na dwie części, tak aby mniejsza liczba stacji konkurowała o dostęp do medium w każdym z segmentów.

Mosty funkcjonują na poziomie LLC (kontroli łącza logicznego). Na rysunku 30 pokazano most, który łączy dwie sieci Ethernet. Ramka sieci Ethernet dociera do jednego portu mostu i wypływa z drugiego portu do przyległego segmentu sieci. Most przesyła dalej tylko te ramki, które adresowane są do drugiego segmentu sieci, co pozwala uniknąć niepotrzebnego dostarczania pakietów do obu sieci.

Omówione funkcje mostów nie odbiegają znacząco od funkcji wzmacniaków *(repeater),* zasadnicza różnica polega na tym, że mosty prze syłają ramki, biorąc pod uwagę zapisane w nich adresy MAC *(Medium Access Control),* czyli adresy fizyczne, przypisane do kart sieciowych. Fil trowanie ramek eliminuje m.in. wpływ kolizji w jednym segmencie sieci na funkcjonowanie pozostałych segmentów. A zatem mosty mogą wyelimino wać wpływ problemów, występujących w jednym z segmentów, na pozo stałe segmenty sieci. Ponadto mosty łączą sieci za pośrednictwem różnych typów łączy, takich jak linie komutowane, łącza światłowodowe, a nawet łącza satelitarne. Typowe zastosowanie mostu przedstawiono na rysunku 30.

Należy podkreślić, że obecnie w wielu sytuacjach zaleca się stosowanie w miejsce mostów routery i przełączniki. Urządzenia te zapewniają większą elastyczność konfiguracji sieciowej, a ich ceny znacznie spadły, czyniąc z nich bardzo praktyczny nabytek. Co najważniejsze, routery mogą bez trudu łączyć odmienne sieci.

Połączenia między zdalnymi mostami realizowane są za pośrednictwem linii analogowych, przy użyciu modemu, lub za pośred nictwem cyfrowych linii dzierżawionych. W przypadku połączeń zdalnych wybór między liniami dzierżawionymi a komutowanymi powinien być uzależniony od charakteru transmisji da nych. W niektórych przypadkach między ośrodkami przesyłana jest jedynie poczta elektroniczna, aktualizacje plików, kopie zapasowe i temu podobne dane. Dla tego rodzaju transmisji odpowiednia jest często linia z połącze niem na żądanie – połączenia nawiązywane są wyłącznie w razie potrzeby, co

ogranicza opłaty za czas trwania połączenia. Linia dedykowana może okazać się najlepszym rozwiązaniem w przypadku połączeń, w których użytkownicy w dwóch ośrodkach stale komunikują się ze sobą, a ruch jest intensywny i ciągły. W środowiskach sieci kampusowych do łączenia sieci LAN w różnych budynkach stosuje się często prywatne mosty, wykorzystujące komunikację radiową lub łącza światłowodowe.

Niektórzy producenci oferują mosty dzielące obciążenie *(load-sharing bridges),* które potrafią wykorzystać łącza rezerwowe do obsługi części obciążenia, nie powodując przy tym powstawania pętli. Most dzielący obciążenie jest najwydajniejszym typem mostu. Wykorzystuje algorytm drzewa częściowego, a jednocześnie używa do przesyłania pakietów podwójnego łącza, co zwiększa wydajność komunikacji międzysieciowej.

W sytuacji, gdy sieć Ethernet jest połączona za pośrednictwem mostu z siecią szkieletową FDDI, ramki Ethernet muszą zostać odpowiednio dopasowane do warunków transportu w sieci. Realizuje się to na dwa sposoby:

– Hermetyzacja *(encapsulation).* Metoda ta polega na umieszczeniu kompletnej ramki Ethernet w pakiecie FDDI wysyłanym w sieci. Gdy pakiet dotrze do mostu prowadzącego do sieci docelowej, zostaje rozpakowany i wysłany do węzła docelowego. Hermetyzacja jest typową metodą zaimplementowaną w większości mostów łączących sieci Ethernet z FDDI. W rozwiązaniu tym zakłada się, że węzły sieci Ethernet nigdy nie będą musiały komunikować się z żadnymi, prócz mostów, węzłami przyłączonymi bezpośrednio do sieci lokalnej FDDI. Ramki poddane hermetyzacji stają się bezużyteczne aż do chwili, w której zostają rozpakowane przez odbierający je most.

– Translacja (tłumaczenie). Most realizujący translację dokonuje konwersji pakietów Ethernet do postaci pakietów FDDI. W rozwiązaniu tym aktualna pozostaje większość omówionych wcześniej problemów dotyczących konwersji. Translacja jest

mniej efektywna niż hermetyzacja, umożliwia jednak komunikację węzłów sieci Ethernet z węzłami sieci FDDI. Jeśli sieć FDDI wykorzystywana jest po prostu jako sieć szkieletowa, to preferowanym rozwiązaniem pozostaje hermetyzacja.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.

Ethernet jako podstawowy system budowy sieci IP

Ethernet jako system budowy sieci powstał w 1970 r. w Palo Alto Research Center firmy Xerox. Jego twórcą był dr Robert Metcalf. Rozwijany w latach osiemdziesiątych we współpracy z firmami DEC i Intel stał się znany jako standard DIX Ethernet – od pierwszych liter nazw wdrażających go firm. Standard IEEE 802.3 określa podobny typ sieci ale różniący się formatem ramki. To wlaśnie standard IEEE 802.3, został on przyjęty przez międzynarodową organizację standaryzacyjną ISO *(Interrnational Organization for Standartization)* jako standard światowy.

Należy zauważyć, że nazwa Ethernet jest nadawana wszystkim systemom, posługującym się techniką dostępu do medium transmisyjnego z wykrywaniem kolizji CSMA/CD. Obecnie, prawidłową nazwą tego standardu jest IEEE 802.3, lecz ogromna popularność określenia Ethernet powoduje, że większość producentów i publikacji wciąż używa tego terminu. Dla wyjaśnienia często stosuje się nazwę Ethemet 802.3.

Istnieje wiele odmian systemów opartych na specyfikacji IEE 802.3 Ethernet. Są to, m. in., systemy o szybkości 10 Mb/s,

100 Mb/s, 1Gb/s wykorzystujące jako medium kabel koncentryczny, skrętkę wieloparową, lub światłowody. Najpopularniejsze obecnie są rozwiązania oparte na skrętce nieekranowanej.

Należy zaznaczyć, że pojęcie Ethernet odnosi się nie do jednej, lecz do wielu standardów budowy sieci lokalnych, z których wyróżnić należy trzy podstawowe kategorie:

1. Ethernet i IEEE 802.3 – jest to kilka specyfikacji określających sieci lokalne, z których każda pracuje z przepływnością 10 Mb/s.

2. Ethernet 100 Mb/s – jest to pojedyncza specyfikacja, znana również jako Fast Ethernet, określająca sieć pracującą z przepływnością 100 Mb/s.

3. Ethernet 1000 Mb/s – jest to pojedyncza specyfikacja, znana również jako Gigabit Ethernet, określająca sieć pracującą z przepływnością 1000Mb/s.

Obecnie prowadzone sa prace nad nową kategorią Ethernetu – 10Gb Ethernet aczkolwiek rzeczywiste i sprawnie działające implementacje tego systemu nie sa jeszcze praktycznie stosowane.

W sieci Ethernet wszystkie stacje korzystają ze wspólnego medium transmisyjnego. Dostęp do niego odbywa się za pomocą metody CSMA/CD – wykrywanie nośnej i detekcja kolizji). Metoda CSMA/CD jest efektywna przy małym ruchu w sieci. Przy większym jego natężeniu wzrasta liczba kolizji. Przerywanie transmisji i ponawianie ich później, kiedy sieć jest stale obciążona, jedynie pogarsza sytuację i doprowadza do obniżenia wydajności i zauważalnego dla użytkowników zwolnienia pracy. Jednym z rozwiązań jest ograniczenie liczby stacji roboczych w segmencie sieci LAN a coraz częściej stosuje się „inteligentne” przełączniki pracujące w topologii gwiazdy i eliminujące podstawowe wady protokołu CSMA/CD.

Kolizje są zasadniczym powodem limitowania długości magistrali Ethernet. Przy większych długościach pojawia się tak duże opóźnienie propagacji sygnału, że przestaje prawidłowo działać mechanizm ich wykrywania. Stacja rozpoczynająca transmisję na jednym z końców zbyt długiego kabla może „nie zauważyć", że w tym samym momencie, na drugim końcu, zaczęła się transmisja z innej.

Na rysunku 28 przedstawiono przykładową strukturę: dwie „podsieci", połączone ze sobą przy pomocy routera/przełacznika.

Wprawdzie sieci Ethernet i IEEE 802.3 są bardzo podobne, to jednak istnieją między nimi różnice wymagające omówienia. Ethernet zapewnia usługi w warstwie fizycznej i w warstwie łącza danych, tymczasem IEEE 802.3 działa w warstwie l oraz częściowo w warstwie 2. Ponadto IEEE 802.3 nie definiuje podwarstwy LLC *(Logical Link Control),* ale specyfikuje wiele różnych warstw fizycznych, gdy tymczasem Ethernet ogranicza się tylko do jednej. Poniższa tabela przedstawia porównanie podstawowych parametrów najpopularniejszych obecnie wersji Ethernet i IEEE 802.3.

Protokoły warstwy łącza danych

Bardzo ważna i dosyć charakterystyczna warstwą w sieciach lokalnych opartych na protokole IP jest warstwa łącza danych. W modelu odniesienia OSI warstwa łącza danych znajduje się bezpośrednio nad warstwą fizyczną. A zatem w jej ramach zdefiniowane są protokoły, które współpracują z fizycznymi komponentami łącza, takimi jak karty sieciowe i okablowanie. Protokoły warstwy łącza danych dzielą dane na ramki i nadzorują przepływ danych przez łącze. Protokoły takie zaprojektowano pierwotnie z myślą o połączeniach dwupunktowych i nadal głównie w ten sposób obsługują one transmisję danych. W sieciach ze wspólnym medium, takich jak Ethernet, konieczne jest zastosowanie dodatkowych protokołów dostępu do medium. W sieciach IP opartych na standardzie Ethernet takim protokołem

dostępu do medium jest CSMA/CD. W przypadku intersieci często istnieje konieczność stosowania innych protokołów warstwy łącza danych.

Wybór między połączeniową lub bezpołączeniową metodą komunikacji uzależniony jest od właściwości stosowanej sieci. Jeśli jest to sieć bezprzewodowa, w której często zdarza się utrata ramek, to preferowanym rozwiązaniem będzie przesyłanie potwierdzeń już w warstwie łącza danych. Jednak w takim przypadku duża część pasma transmisyjnego zajęta będzie przez transmisję potwierdzeń. W niezawodnych sieciach stosowanie połączeniowych protokołów łącza danych jest z reguły zbędne.

Poniżej opisane zostały najbardziej popularne i najczęściej stosowane protokoły warstwy łącza danych:

– **HDLC** *(High-levelData Link Protocot).* Protokół ten jest oparty na protokole SDLC *(Synchronous Data Link Protocol),* opracowanym przez firmę IBM i będącym częścią architektury IBM SNA *(Systems Network Architecure).* Wiele innych protokołów używa tych samych procedur i tego samego formatu ramki, co HDLC.

– **LLC** *(Logical Link Control).* Protokół ten zdefiniowało stowarzyszenie IEEE *(Institute of Electrical and Electronic Engineers)* w ramach swojej rodziny standardów sieciowych 802.x.

– **LAP** *(Link Access Procedurę).* Wyróżnia się trzy główne protokoły z rodziny LAP:

– **LAPB** *(LAPBalanced)* to protokół obsługujący połączenia dwupunktowe w sieciach pakietowych X.25.

– **LAPD** *(LAP for D Channel)* realizuje kontrolę łącza danych w kanale D linii ISDN *(Integrated Servi-ces Digital Network).*

– **LAPF** *(LAP for Frame-Mode Bearer Services)* to protokół kontroli łącza danych w sieciach typu *Frame Relay*

(działających w oparciu o przekazywanie ramek).

– **SLIP** *(Serial Line Interface Protocol).* SLIP to mechanizm kontroli łącza danych, służący do przesyłania pakietów IP – zwykle pomiędzy dostawcą usług internetowych a domowym użytkownikiem, korzystającym z linii telefonicznej. Protokół SLIP ma pewne ograniczenia, w szczególności nie oferuje żadnych mechanizmów wykrywania i poprawiania błędów. Kontrolę muszą nad poprawnością transmisji muszą sprawować protokoły wyższych warstw.

– **PPP** *(Point-to-Point Protocol).* Protokół PPP realizuje te same funkcje co SLIP (tzn. jest powszechnie stosowany do obsługi połączeń z Internetem za pośrednictwem linii telefonicznych), z tym że charakteryzuje się większą sprawnością i może transportować różne rodzaje pakietów, a nie tylko IP.

Instytut IEEE opracował standard podziału warstwy łącza danych w sieciach LAN na dwa poziomy. Pierwszy z nich to poziom kontroli dostępu do medium MAC *(Medium Access Control),* a drugi to poziom kontroli łącza logicznego LLC *(Logical Link Control).* Oba poziomy przedstawiono na rysunku 29.

W niższym poziomie MAC zdefiniowana jest metoda dostępu do medium. Może to być metoda CSMA/CD, *Token Ring* lub inny interfejs fizyczny, zgodny ze standardami IEEE. Poziom LLC pośredniczy w komunikacji między warstwą sieciową a jednym z protokołów warstwy MAC.

Lokalne i rozległe sieci komputerowe

Przez ostatnie kilkadziesiąt lat postęp w dziedzinie telekomunikacji i informatyki, pod względem swojej dynamiki był zjawiskiem precedensowym. Budowane sieci transportowe wykorzystujące techniki światłowodowe oparte na standardach PDH/SDH/ATM/WDM przeznaczone były głównie dla potrzeb telekomunikacyjnych. Natomiast sieci komputerowe rozumiano początkowo jako odizolowane praktycznie od sieci telekomunikacyjnych byty. Jednak na przestrzeni ostatnich trzydziestu lat widac jak mylne było to podejście. Wraz z rozwojem rynku informatycznego wytworzyła się potrzeba komunikacji międzysieciowej; struktury informatyczne dużych firm nie tylko z branży IT rozrastały się do tego stopnia, że sieci komputerowe zaczęły „wychodzić" z budynków korporacji. Powstało pytanie: jak najtaniej i najefektywniej połączyć sieci lokalne. Odpowiedź przyszła właśnie ze strony rynku telekomunikacyjnego. Przy wykorzystaniu zdobyczy informatyki, telekomunikacja daje możliwości zaspokojenia zapotrzebowań rynku transmisji danych. W obszarze sieci informatycznych dominującą pozycję posiadają obecnie sieci oparte na protokole IP. W poniższym rozdziale poddano analizie sieci lokalne i rozległe wykorzystujące ten protokół jako protokół warstwy sieciowej modelu OSI *(Open System Interconnection).* Szczególny nacisk położono na analizę technik budowy sieci IP i kierunki rozwoju tego obszaru rynku teleinformatycznego.

Ogólna charakterystyka sieci IP

Geneza powstania sieci IP

Na początku lat 70-tych w Stanach Zjednoczonych powstała pakietowa sieć ARPANET. Fundatorem ARPANET była agencja ARPA, przekształcona później w DARPA *(Defense Advanced Research Projects Agency).* Sieć ARPANET łączyła ośrodki militarne,

rządowe laboratoria naukowe i wyższe uczelnie. Z czasem ewoluowała, stając się siecią szkieletową Internetu, a z nazwy ARPANET zrezygnowano oficjalnie w roku 1990. W 1983 roku z sieci ARPANET wydzielono wojskową sieć MILNET. Poza tym, to właśnie z ARPANET-u wywodzi się jeden z najważniejszych obecnie protokołów: Transmission Control Protocol/Internet Protocol (TCP/IP).

Pierwsze moduły TCP/IP zainstalowano w 1980 roku. Bardzo istotną rolę w rozwoju TCP/IP odegrał rządowy program testowania i wydawania certyfikatów potwierdzających zgodność tworzonych produktów z opublikowanymi standardami.

Transmisja danych w sieciach IP

Protokół IP (obecnie w wersji 4, czyli IPv4) jest podstawowym protokołem dla routingu pakietów w Internecie i sieciach opartych o protokoły TCP/IP. Pozwala na stworzenie systemu komunikacji pomiędzy połączonymi sieciami. Protokół ARP (*Address Resolution Protocol)* wykorzystywany jest w sieciach TCP/IP do odwzorowania adresów IP *(Internet Protocol)* w fizyczne adresy MAC *(Medium Access Control).* Adres IP identyfikuje konkretny komputer w podsieci, należącej do sieci złożonej. Jest zatem międzysieciowym adresem wysokiego poziomu. Fizyczny adres MAC jest sprzętowo zakodowany i przypisany do karty sieciowej. Adresy MAC używane są wyłącznie przy przesyłaniu ramek między komputerami podłączonymi do tej samej sieci. Nie mogą być stosowane przy przesyłaniu ramek do komputerów podłączonych do innych sieci, oddzielonych routerami od sieci nadawcy. Jeśli ramka ma przekroczyć barierę, jaką stanowi router, konieczne jest użycie adresu IP (przy założeniu, że sieć funkcjonuje w oparciu o protokół TCP/IP). Przykładowy transport datagramu IP pomiędzy dwoma hostami (A1 i C1) przedstawia rysunek 27.

Dla uproszczenia numeryczne adresy hostów, sieci i routerów zastąpiono literami. Np. źródło pakietu w sieci A ma adres Al, a router A/B łączy sieci A i B. Warto zauważyć, że

protokół IP świadczy usługi nie wymagające bezpośredniego połączenia pomiędzy nadawcą a odbiorcą. Protokół wyższego poziomu – TCP, w przeciwieństwie do IP jest zorientowany połączeniowo. IP wykonuje wszystkie działania, niezbędne dla dostarczenia pakietów, ale nie może zagwarantować, że nie zostaną one odrzucone lub utracone. Sprawą zapewnienia kompletności pakietów i ich ewentualnego odtworzenia zajmuje się system końcowy. Jego zadaniem jest również sterowaniem właściwym przepływem pakietów i ich porządkowanie. Funkcje te realizowane są za pomocą protokołu TCP. Jednostką transmisji danych na poziomie protokołu sieci jest pakiet IP. Należy pamiętać, że długość datagramu (łącznie dane i nagłówek) nie może przekroczyć 65.535 bajtów.

Adresowanie w sieciach IP

Każdy element w ramach sieci IP ma swoją jednoznaczną identyfikację. W środowisku TCP/IP istnieją trzy metody identyfikacji systemu hosta w sieci:

1. Adres fizyczny – najczęściej unikalny w skali światowej,

2. Adres IP – unikalny w skali podsieci

3. Nazwa domenowa – unikalna w skali domeny

Adres fizyczny jest adresem MAC (*Medium Access Control),* zaszytym w karcie sieciowej komputera. Stosowany jest wyłącznie do adresowania wewnątrz sieci lokalnych (LAN).

Adres IP identyfikuje system hosta w środowisku międzysieciowym. IP jest adresem numerycznym, jednoznacznie identyfikującym system hosta w sieci złożonej. Ma on postać liczby 32-bitowej (4 bajty), która nazywana jest „przestrzenią adresową". Składa się dwóch części:

1. Identyfikator sieci – określa konkretną sieć (grupę komputerów)

2. Identyfikator hosta – określa konkretny komputer w danej

sieci

Dla zapisu adresu IP stosuje się notację dziesiętną, w której każdy bajt od□dzielony jest separatorem (kropką). Są trzy sposoby podziału adresu: po pierwszym, drugim lub trzecim bajcie. Uzyskuje się w ten sposób cztery klasy adresów (A, B, C, D). Protokół IPv4 dobrze sobie radzi z obsługą społeczności internetowej, ale jego ograniczona przestrzeń adresowa stała się źródłem narastających pro□blemów w miarę wzrostu liczby połączonych komputerów. Od 1990 roku organizacja IETF (*Internet Engineering Task Force)* pracuje nad unowocześnieniem protokołu IP. Rezultatem tych działań jest całkiem nowy protokół IPv6, obsługujący wszystkie inne protokoły internetowe, ale niekompatybilny „w dół" z protokołem IPv4. Protokół IPv6 został opisany w biuletynach RFC 1883 i RFC 1887. Najważniejszą cechą protokołu IPv6 jest znacznie powiększona przestrzeń adresowa. Na adres przeznaczono bowiem aż 16 bajtów (w porównaniu do 16 bitów IPv4). Daje to praktycznie nieograniczone możliwości adresowania urządzeń w sieci.

IP poprzez Gigabit Ethernet poprzez WDM

Szacuje się że Ethernet stanowi 85 % sieci LAN na świecie. Nowa technika Gigabit Ethernet może zostać zastosowana do rozszerzenia przepustowości obecnie eksploatowanych sieci LAN, MAN, WAN, poprzez zastosowanie Gigabitowych kart liniowych w ruterach IP, które kosztują w przybliżeniu 5 razy mniej niż

karty SDH o zbliżonych przepustowościach. Z tego też powodu Gigabit Ethernet może być również atrakcyjny w przypadku transmisji IP poprzez pierścienie WDM, lub na dłuższych odcinkach transmisyjnych wykorzystujących WDM. Również w najbliższej przyszłości zestandaryzowaniu ulegnie 10 Gigabit Ethernet (GbE). Przykład sieci IP opartej na interfejsach Gigabit Ethernet możemy zobaczyć poniżej. Gigabitowe karty liniowe mogą być stosowane w ruterach IP lub w szybkich przełącznikach Ethernetowych warstwy 2. W przypadku sieci opartych o technologię Ethernet o niższych przepustowościach (np. 10 Base – T lub 100 Base – T) może zostać zastosowany tryb half – duplex, gdzie pasmo dostępne do transmisji jest współdzielone przez wszystkich użytkowników i w obu kierunkach transmisji. Została tu zastosowana technika CSMA – CD.

Nakłada to jednak ograniczenia na fizyczne rozmiary sieci, w której czas transmisji nie może przekroczyć wartości szczeliny czasowej która określa minimalną długość ramki (512 bitów dla 10 Base – T oraz 100 Base – T). Dla przepustowości 1Gb/s użycie minimalnej długości ramki oznaczałoby, iż sieć Ethernet mogłaby osiągnąć długość jedynie 10 m, z tego to powodu minimalna długość ramki została zdefiniowana jako 4096 bitów dla Gigabit Ethernet. Jednak nadal daje to ograniczeni na długość sieci 100m, dlatego też tryb full-duplex jest tu bardziej atrakcyjny. W przypadku zastosowania techniki Gigabit Ethernet (1000Base -X) w trybie full – duplex, uzyskujemy prostą enkapsulację i ramkowanie pakietów IP i tryb CSMA – CD nie jest wykorzystywany. Przełączniki Ethernetowe mogą również być używane w celu rozbudowy topologii sieci nie tylko w połączeniach typu punkt – punkt.

Gigabit Ethernet zapewnia również gwarancję jakość usługi QoS zdefiniowaną w zaleceniu IEEE 802.1Q oraz 802.1p. Uzyskanie gwarancji jakości usługi poprzez Ethernet jest możliwe dzięki zastosowaniu pakietów znacznika definiujących priorytet lub klasę usługi danego pakietu. Znaczniki te umożliwiają aplikacjom komunikację dotyczącą priorytetów pakietów z

urządzeniami pośredniczącymi w transporcie pakietów.

Protekcja i odtwarzanie

Istnieją trzy typy protekcji i odtwarzania w architekturze IP / WDM. W zależności od rodzaju awarii możemy się zabezpieczyć przed:

– przerwaniem połączenia kablowego: dotyczy zarówno systemów WDM z optyczną protekcją OMSP *(Optical Multiplex Section Protection)*

– awarią sprzętu transmisyjnego oraz przerwaniu połączenia kablowego: dotyczy przede wszystkim systemów SDH (kiedy protekcja SDH jest stosowana) i szczególnie zabezpieczonych systemów WDM wyposażonych w OCHP *(Optical Channel Protection)*

– przed awarią ruterów: dotyczy sieci zawierających rutery IP oraz systemów duplikowanych.

Dopuszczalne jest łącznie zabezpieczeń. Na przykład OMSP może być wykorzystywane do szybkiego przełączania w przypadku uszkodzenia połączenia kablowego, podobnie w przypadku sieci IP posiadających wolne zasoby transmisyjne, ruch może zostać przerutowany w obrębie uszkodzonego węzła-rutera.

Zabezpieczenie przed przerwaniem połączenia kablowego z wykorzystaniem OMSP.

OMSP wykorzystuje przełączniki optyczne w celu przywrócenia grupy n długości fal równocześnie. OMSP może być liniowy (1+1) lub dzielony (OMSPRing).

Zabezpieczenie przed uszkodzeniom urządzeń WDM z wykorzystaniem OCHP.

OCHP – przełączanie jest realizowane poprzez warstwę optyczną co oznacza że każda długość fali wymaga oddzielnego przełącznika. Oznacza to zwiększoną ilość przełączników optycznych ale jednocześnie daje większą selektywność i

jednocześnie z łatwością można zrealizować protekcję transponderów dzięki takiej architekturze. Poniższy rysunek przedstawia węzeł wykorzystujący OCHP.

Protekcja i odtwarzanie w obrębie sieci IP

Alternatywą dla protekcji przez przełączanie w systemach SDH i WDM w celu zabezpieczania przeciwko awariom urządzeń transmisyjnych lub uszkodzeń przewodów transmisyjnych jest jedynie odtwarzanie. Rysunek 24 prezentuje przykład niezabezpieczonego systemu WDM z dołączonymi ruterami IP.

W przypadku uszkodzenia połączenia kablowego pomiędzy ruterami A i B ruch IP poprzednio rutowany z A do C poprzez B zostanie przerutowany poprzez D. Odtwarzanie połączenia w sieci IP zawiera aktualizację tablic routingu. W przypadku standardowych protokołów takich jak OSPF lub RIP zachowywany jest zapis o stanie dotychczasowym i uaktualnianie następuje sukcesywnie. Szybkość z jaką może zostać to wykonane uzależniona jest od wielkości sieci i typu algorytmu rutującego. Uaktualnianie 64 MB tablic rutingu w ruterach wewnątrz dużej sieci może zająć kilka godzin zanim sieć osiągnie właściwy poziom wydajności. Rysunek pokazuje dodatkowo strukturę, w której rutery IP są zduplikowane. Każdy z ruterów podstawowych i zapasowych działa na swoim własnym kanale WDM. Rutery podstawowe i zapasowe są połączone bezpośrednio więc w przypadku awarii jednego z nich usługa automatycznie odtwarza połączenie na poziomie IP.

Podsumowanie protekcja i odtwarzanie

W przypadku IP poprzez ATM poprzez SDH funkcjonalność pod względem protekcji i odtwarzania na poszczególnych warstwach wygląda następująco:

* Ruch o niskim priorytecie, 1:1 protekcja kanałów gdy pojemność transmisyjna nie jest wykorzystywana dla celów protekcyjnych ruchu podstawowego. Jeśli wymagana jest protekcja kanałów ruchu podstawowego, ruch dodatkowy jest

opróżniany.

* Automatyczne odtwarzanie istnieje gdy Półstałe połączenia wirtualne (Soft PVC’s) są stosowane. Jeżeli takie połączenie wirtualne zostanie rozłączone z powodu awarii systemu przełączania lub awarii połączenia kablowego punkt docelowy jest odpowiedzialny za przywrócenie połączenia. Częstotliwość prób przywrócenia połączenia jest uzależniona od implementacji.

Zauważalny jest trend do upraszczania warstwy SDH, w połączeniu z sekcją odtwarzania w warstwie IP i protekcją w warstwie optycznej WDM.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.