Sieci komputerowe. Budowa i działanie

Autor: Marcin Mucha
ISBN: 83-7197-863-4
Format: B5, stron: 304

„Dopiero sieć to komputer" – to hasło firmy Sun doskonale oddaje znaczenie sieci komputerowych we współczesnym świecie, a jego praktyczną ilustracją jest kariera Internetu. Sieci komputerowe czy też teleinformatyczne, to nie tylko Internet: to także sieci lokalne, sieci, którymi przesyłane są rozmowy w telefonii komórkowej, sieci bezprzewodowe – cała sieciowa infrastruktura, będąca podstawą funkcjonowania większości gałęzi przemysłu, usług i mediów.

Książka, przeznaczona dla zainteresowanych technologiami teleinformatycznymi, opisuje podstawowe rodzaje sieci komputerowych. Przestawiony jest zarówno ich model logiczny, jak i konkretne rodzaje urządzeń, używanych do ich budowy. Czytelnik znajdzie tu wiele przydatnych schematów, norm i standardów. Szczegółowo opisane zostały sposoby rozwiązywania typowych problemów, występujących przy projektowaniu i budowie sieci.

Omówiono:

- Historię sieci komputerowych
- Model referencyjny OSI
- Topologie sieci
- Rodzaje dostępu do sieci
- Adresy IP, porty aplikacji, komunikacja w sieciach i pomiędzy nimi
- Urządzenia sieciowe, karty sieciowe
- Normy budowy sieci
- Sieci VLSM
- Techniki instalacji urządzeń i okablowania
- Sieci w systemach Windows

Dzięki tej książce zapoznasz się z teorią i praktyką współczesnych sieci komputerowych i teleinformatycznych.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 12.

Techniki instalacji różnych standardów sieci komputerowych

Instalacja sieci komputerowej to złożony proces, na który składa się określenie wymagań co do maksymalnego kosztu elementów w postaci kart sieciowych, przełączników, routerów, urządzeń zabezpieczających, okablowania, gniazd przyłączeniowych, puszek, listew przenoszących okablowanie, szaf, szafeczek, aż po taśmy nanoszące odpowiednie numery identyfikacyjne na każde z zakończeń sieciowych.

Pierwszym etapem wdrażania danego rodzaju sieci jest określenie wymagań. Z reguły spotykamy się z dwoma typami wymagań. Jedno z nich zorientowane będzie na jakość i wydajność całego projektu, inne kierować się będzie wyłącznie niskim kosztem instalacji.

Ta oczywista sytuacja inicjuje instalację sieci komputerowej. Na tym etapie musimy dobrze zorientować się w sytuacji, co powinno przebiegać w dwóch strefach.

Pierwsza z nich dotyczy dokładnego rozeznania co do rodzaju środowiska, jakie otacza dany budynek czy budynki. Druga powinna nam wskazywać możliwość zastosowania odpowiedniego rozwiązania technicznego, które będzie zgodne z założeniami finansowymi.

Te pierwsze dwa kroki w większości instalacji sieciowych mają decydujący wpływ na ich rodzaj i typ. Pierwszy z wspomnianych etapów nakazuje nam sporządzenie planu zabudowy budynku czy też budynków i otaczającego środowiska. Wykonując taki plan, powinniśmy szczególną uwagę zwrócić na odległości pomiędzy ważnymi punktami, węzłami sieci. Oznacza to przystosowanie planowanego rozwiązania sieciowego tak, by zgadzało się z założeniami i normami okablowania poziomego i pionowego.

Powstaje teraz pytanie, jak rozwiązać napotykane problemy. Jednym z nich jest określenie zewnętrznego przebiegu okablowania sieciowego. Jest to z reguły okablowanie szkieletowe. Jak pamiętamy z poprzednich rozdziałów, w obrębie okablowania szkieletowego możemy wykorzystywać rozwiązania w postaci nośników miedzianych, czyli dzisiejszych struktur okablowania UTP, STP i ich wzbogaceń. Możemy także wykorzystywać nośniki fizyczne w postaci okablowania światłowodowego, zarówno jedno-, jak i wielomodowego. Okablowanie światłowodowe, podobnie jak i miedziane, występuje pod różnymi postaciami. I tak spotkać możemy okablowanie stacyjne, okablowanie wykonane w specjalnych osłonach czy okablowanie przeznaczone do instalacji na zewnętrznych ścianach budynków.

Użycie określonego typu okablowania oczywiście zależy od nas. Jednak gdy dokonamy złego wyboru, możemy mieć później problemy z prawidłowymi transmisjami w sieci lub też pojawią się nagłe awarie sprzętu, występujące podczas wyładowań atmosferycznych.

Na świecie przyjęła się pewna zasada, określająca instalacje zarówno wewnątrz budynków, jak i na zewnątrz. Wykonując instalację wewnątrz budynków, możemy używać każdego typu okablowania. Jednak sytuacja komplikuje się przy instalacjach poza danym budynkiem. Jeśli jakiś fragment sieci ma przebiegać na zewnątrz, rozsądnie jest użyć okablowania światłowodowego, które zabezpieczy nas przed niepożądanymi skutkami wyładowań atmosferycznych.

Oczywiście instalacja okablowania światłowodowego powinna przebiegać w specjalnych tunelach, zabezpieczających światłowód przed mechanicznym uszkodzeniem.

Możemy spotkać się także z sytuacją, w której musimy poprowadzić fragment sieci na obszarze między budynkami, oddzielonymi drogą publiczną. Jest to sytuacja zdecydowanie niepożądana przez instalatorów, gdyż wymaga wielu upoważnień i zgody ze strony miasta, bez czego nie możemy wykonać instalacji przechodzącej przez strukturę drogi.

W takim przypadku warto zastanowić się nad dwoma typami rozwiązań bezprzewodowych.

Pierwszym i najwydajniejszym rozwiązaniem jest instalacja oparta na systemach transmitujących falę elektromagnetyczną w bardzo wysokich częstotliwościach (długościach światła), inaczej mówiąc, bezprzewodowe połączenie optyczne.

Rozwiązanie opierające się na odbiorniku i nadajniku optycznym umożliwia uzyskanie bardzo wysokiej jakości transmisji, zarówno pod względem prędkości, jak i poprawności. Zastosowanie takiego rozwiązania wymaga podstawowego założenia, jakim jest brak przeszkód i pełna widoczność pomiędzy nadajnikiem a odbiornikiem. Uzyskanie takiego punktu jest konieczne dla użycia tego rozwiązania.

Transmisje przebiegające w oparciu o tego typu systemy odbywają się w bardzo wysokich częstotliwościach. Ta wysoka częstotliwość obrazuje się nam w postaci długości fali świetlnej, tak jak przy transmisjach światłowodowych.

System wspomnianej transmisji, bazujący na przesyłaniu danych w postacji fal świetlnych o odpowiedniej długości, jest w pewnym stopniu podobny do technik przesyłania danych przy użyciu światłowodów. Zauważalna gołym okiem różnica pomiędzy tymi systemami polega na braku ośrodka transmisji (jakim jest włókno światłowodowe) w przypadku transmisji bezprzewodowych oraz innej budowie i charakterystyce nadajników i odbiorników.

Użycie wspomnianego rozwiązania wymaga widoczności optycznej obu zakończeń połączenia, pomiędzy którymi ma przebiegać transmisja. Jest to jeden z wielu wymogów, niezbędnych, by możliwe było zainstalowanie i użycie tego typu rozwiązania. Założenie to wynika z samego charakteru transmisji, na jakiej opiera się to rozwiązanie. Jak wspomniałem, polega ona na przesyłaniu wiązki światła o odpowiedniej długości. Jeśli przy danym urządzeniu bądź też podczas zapoznawania się z informacjami dotyczącymi jakiegoś urządzenia napotkamy jakiekolwiek parametry wyrażane w postacji długości fali świetlnej, możemy być wtedy pewni, że urządzenie to działa w oparciu o transmisję w bardzo wysokich częstotliwościach.

Transmisja opierająca się na bardzo wysokich częstotliwościach zapewnia odpowiednią wydajność, jednak jest bardzo wrażliwa na przeszkody, które mogłaby napotkać na swojej drodze. Problem polega na pochłanianiu wszelkich transmisji bezprzewodowych, które przebiegają w oparciu o wysoką częstotliwość. W przypadku bezprzewodowego połączenia optycznego nie może dojść do sytuacji, w której pomiędzy nadajnikiem a odbiornikiem znajduje się jakaś przeszkoda, obojętne, czy ma ona postać ściany, drzewa czy też szkła. Próba transmisji przez takie ośrodki zakończy się całkowitym pochłonięciem wysłanego strumienia przez pierwszą przeszkodę. W systemach transmisji opartej na przesyłaniu światła wymagana jest poprawna widoczność.

Warunek ten stanowi pierwszy wymóg ze strony samego urządzenia transmisji bezprzewodowej. *Optolinki*, bo z takim określeniem możemy spotkać się przy urządzeniach przesyłających dane w oparciu o wspomnianą metodę, mają jeszcze kilka innych ważnych wymogów; na zachowanie się takiego połączenia mają wpływ także warunki pogodowe.

Optolinki jako urządzenia transmisji bezprzewodowej oprócz *widoczności transmisyjnej* wymagają także specyficznych warunków pracy. Konieczna jest odpowiednia instalacja urządzeń, tak by były odporne na niepożądane drgania podłoża. Wpływ wibracji podłoża na nadajnik i odbiornik może spowodować nagłą stratę połączenia, jeśli odległość pomiędzy nimi jest spora. Z pozoru mała wibracja lub nagłe drgnięcie nadajnika przy dużej odległości może wyrazić się w postaci kilkucentymetrowego przesunięcia, odchylenia skupionej wiązki fali od punktu odbiorczego.

Właśnie z tego powodu instalacja takich punktów świetlnej transmisji powinna mieć miejsce z dala od dostępu ludzi czy też urządzeń powodujących wibrację podłoża. Jeśli uporamy się z tym problemem i mamy już wybrane przez siebie miejsca na montaż tych urządzeń, sprawdźmy i oceńmy, czy nie będą one narażone na mocne naświetlenie

przez promienie słoneczne. Wbrew pozorom instalacja urządzeń w miejscach, w których mogą być one poddane działaniu promieni słonecznych, może mocno zakłócić przebieg transmisji. Spowodowane jest to przez odbicia promieniowania słonecznego zarówno na soczewkach nadajników półprzewodnikowych, jak i odbiorników. Pojawienie się na soczewce każdego z tych urządzeń promieniowania innego niż pochodzące z nadajnika może zakłócić przebieg nadawanej transmisji w przypadku nadajnika, może także wprowadzić błędy w odczycie, korekcji, jaka dokonywana jest w odbiorniku. Dobrym rozwiązaniem będzie instalacja takiego zestawu urządzeń w specjalnych osłonach czy obudowie.

Wspomniana zabudowa zapobiegnie także zabrudzeniu nadajnika czy odbiornika, jakie może pojawić się w czasie eksploatacji w różnych warunkach pogodowych, np. podczas deszczu.

Rozwiązanie wspomnianych „niewidocznych" problemów (niektórzy nie zauważają drzew lub rogów budynków, znajdujących się pomiędzy nadajnikiem i odbiornikiem) jest podstawą do zastosowania tego typu koncepcji.

Właściwe działanie, umożliwiające efektywne wykorzystanie tego nowoczesnego rozwiązania, zależy od czynników atmosferycznych.

Urządzenia w postaci optolinków są szczególnie czułe na wszelkiego rodzaju opady deszczu, mgłę czy też takie czynniki, które nie wchodzą w skład pogody, ale natury. Mowa tutaj o nagle i niespodziewanie przelatujących ptakach. Każdorazowe znalezienie się takiego obiektu w polu widzenia urządzeń końcowych zakłóci lub przerwie naszą transmisję, wywołując końcowy spadek w ogólnej transmisji. Niestety, nie da się temu zapobiec. Jednak szybkość i sprawność dzisiejszych urządzeń pozwala na zminimalizowanie czasu widoczności takiej przerwy, dziury transmisyjnej.

Urządzenia te, jak wspomniałem, są bardzo podatne na warunki pogodowe. Wymagają od instalatorów odpowiedniego odniesienia odległości pomiędzy urządzeniami końcowymi w stosunku do możliwych opadów, mgły, jaka z reguły ma miejsce w zadanym terenie, do mocy urządzeń. Takie podejście pozwoli na zminimalizowanie efektów zakłócania połączenia przez krople deszczu czy też mgłę, ograniczającą widoczność optyczną.

Transmisja w czasie opadów deszczu narażona jest na zmiany, rozszczepianie transmitowanych fal na kroplach deszczu. W takiej sytuacji kropelki deszczu zadziałają jak miniaturowe zwierciadła, powodując niekiedy zmianę toru danego fragmentu transmitowanej wiązki.

Podobna sytuacja występuje przy transmisji w obszarach zamglonych czy zapylonych. Pył lub mgła także składają się z miniaturowych cząsteczek, które w przypadku mgły dadzą efekt transmisji przez różnie ustawione soczewki, a w przypadku pyłu zadziałają jak miniaturowe pochłaniacze promieni.

W czasie instalacji jakiegokolwiek typu optolinku musimy uzyskać wzajemną widoczność urządzeń końcowych. Owa widoczność odnosi się do odpowiedniego wzajemnego wycentrowania urządzeń, tak by wysłana wiązka padała na soczewkę odbiorczą odbiornika. W przeciwnym razie urządzenia nie będą w stanie nawiązać i ustanowić połączenia.

Wszystkie wymienione cechy to niezbędne elementy, jakie powinniśmy wziąć pod uwagę zarówno podczas planowania użycia tego typu rozwiązania, jak i samego jego zakupu. Sprawdźmy, jakimi parametrami dysponuje sprzęt, jaki mamy zamiar zakupić, w jakim stopniu dopuszcza on pracę w przedstawionych sytuacjach.

Drugim typem rozwiązania, jaki możemy zastosować, jest rozwiązanie klasy IEEE 802.11. Podobnie jak optolinki, transmisja bezprzewodowa radiowa pozwala na rozwiązanie problemu przeprowadzenia sygnału przez trudno dostępne obszary.

Użycie nadajników i odbiorników pracujących przy częstotliwościach x GHz (rozwiązania w klasie 802.11) w porównaniu z bardzo wysoką częstotliwością pracy optolinków okazuje się łatwiejsze i tańsze w eksploatacji.

Zastosowanie bezprzewodowych kart sieciowych i stacji bazowych pozwala na przesyłanie strumieni danych w nieskoncentrowanych wiązkach. Użyłem specjalnie takiego określenia, by już na samym początku zaznaczyć podstawową różnicę pomiędzy tymi dwoma rozwiązaniami. Urządzenia pracujące w oparciu o przesyłanie danych w nieskoncentrowanych wiązkach generują falę na wzór fal radiowych, rozchodzących się w charakterze okręgów.

Dzięki takiemu rozwiązaniu transmitowana fala o odpowiedniej częstotliwości trafia do wielu urządzeń. Rozwiązanie to pozwala na uniknięcie wielokrotnego użycia połączeń optolinkowych tylko po to, by transmisja trafiła „jednocześnie" do wielu oddalonych i trudno dostępnych punktów sieci. Jest to zaleta tego typu rozwiązania.

Ponieważ raz wysłana fala rozchodzi się po znacznym obszarze, istnieje niebezpieczeństwo odebrania ważnych dla nas informacji przez obce hosty lub podszycie się hosta (gdy sieć jest zabezpieczona co do zakresu adresów IP, jakie hosty mogą uzyskać) pod inny, przechwycenie jego transmisji. Jest to oczywista wada tego rozwiązania, które jednak da się zabezpieczyć. W takiej sytuacji widać przewagę połączenia bazującego na kierunkowym przesyłaniu danych.

Rozproszone, że tak to określę, rozchodzenie się fal w urządzeniach zgodnych z IEEE 802.11, jest mniej podatne na przeszkody w postaci ścian, budynków czy też szkła. Ponieważ transmisja odbywa się w znacznie niższym paśmie, jak np. 2,4 GHz, jest ona mniej podatna na pochłanianie.

Efekt pochłaniania dotyczy fal rozchodzących się przy wysokich częstotliwościach. Im są one wyższe, tym bardziej dane urządzenie będzie podatne na wszelkiego rodzaju zakłócenia.

W przypadku fal radiowych spotkać się możemy z wszelkiego rodzaju odbiciami. Odbicie dotyczy wyłącznie fal rozchodzących się w takim zakresie, o którym mówi się częstotliwość. *Odbicie* to efekt, powstający po wysłaniu przez nadajnik fali, która natrafia na jakąś przeszkodę. W takiej sytuacji fala może zostać zniekształcona, odbita w innym kierunku, zakłócając w ten sposób przebieg pozostałych fal; część tej fali może także zostać pochłonięta. Odbicie jest elementem nierozłącznie związanym z transmisją radiową.

Transmisja radiowa jest także narażona na efekty *łamliwości fal*. Zjawisko to jest częściowo związane z odbiciami. Współczynnik łamliwości wzrasta wraz ze wzrostem częstotliwości transmisji. Wzrost częstotliwości niesie ze sobą możliwość precyzyjnego kierowania strumieniem, ale także naraża go na częściowe lub całkowite pochłanianie, jak w przypadku transmisji przy użyciu optolinków.

Na możliwość zastosowania jednego ze wspomnianych rozwiązań wpływa jeszcze jeden ważny czynnik, który dotyczy obszaru Polski i odnosi się do zastosowania połączeń IEEE 802.11, pracujących w oparciu o transmisje radiowe. W przypadku wyboru tego rozwiązania musimy zwrócić się z odpowiednim wnioskiem do URTiP w Warszawie o wydanie odpowiedniego pozwolenia na korzystanie z transmisji zachodzącej w paśmie powyżej 800 MHz.

W przypadku zastosowania połączeń typu optolink nie jest wymagane uzyskanie odpowiedniego pozwolenia, co sprawia, iż „jedynymi" warunkami, jakie musimy spełnić w przypadku takiego rozwiązania, są wszystkie reguły nakreślone przez producenta i standard danego optolinku.

Przy dokonywaniu wyboru pomiędzy tymi rozwiązaniami musimy rozważyć wspomniane cechy. Jednak szczególną uwagę należy poświęcić głównemu elementowi, z powodu którego decydujemy się skorzystać z danego rozwiązania.

W podanym przypadku transmisji pomiędzy budynkami, pomiędzy którymi przebiega droga, dobrym rozwiązaniem będzie użycie optolinków. Rozwiązanie to zapewni wysoką wydajność, pewność, że dane dotarły w wiadome miejsce.

Użycie rozwiązania radiowego także przyniesie pożądany efekt, jednak na pewno nie uzyskamy wysokiej jakości połączenia, będziemy borykać się z problemami dotyczącymi nieautoryzowanej możliwości odbierania sygnału przez niewidoczne hosty.

Będąc już przy omawianiu technologii radiowej, dobrze jest zaznaczyć możliwość jej wykorzystania w miejscach trudno dostępnych. Dobrym przykładem zastosowania technologii radiowej jest użycie jej w miejscach dużego skupienia hostów, które jako takie nie są oddzielone znaczącymi barierami, jak ma to miejsce w biurach. Większość pomieszczeń biurowych bazuje na pomieszczeniach typu boks. Pomieszczenia tego typu, a raczej ścianki oddzielające, wykonane są najczęściej z tektury. Tego typu rozwiązanie nie stanowi specjalnej przeszkody dla fali radiowej, zapewniającej dostęp danego hosta, wyposażonego w odpowiednią bezprzewodową kartę sieciową, do zasobów sieci. Jest to rozwiązanie powszechnie stosowane także w dzisiejszych nowoczesnych kawiarniach, lotniskach czy też innych miejscach, w których dostęp do sieci nie może być utrudniony.

Przedstawione rozwiązanie instalacji sieciowej na obszarze otwartym oraz trudno dostępnym na pewno będzie nam pomocne przy projektowaniu typowych instalacji sieciowych.

Wybór metody oczywiście pozostawia się danemu instalatorowi, który w kolejnym kroku powinien przygotować dokładny plan adaptacji sieci do środowiska, w jakim ma ona istnieć.

Projekt sieciowy

Projekt instalacji sieci komputerowej to dla każdego instalatora czy wykonawcy zbiór wytycznych, których powinien się trzymać podczas wdrażania instalacji sieciowej. Z samego założenia dokładność planu powinna odwzorowywać rozwiązania techniczne, jakimi ma posłużyć się wykonawca podczas prac montażowych.

Na poprawnie wykonany plan składa się między innymi właściwa topologia budynków, zawierająca ich prawdziwe wymiary; na plan powinna zostać naniesiona mapa połączeń.

Do poprawnego wykonania projektu potrzebnych będzie jeszcze kilka informacji, zawartych w planie instalacji elektrycznej danego obiektu. Przy projektowaniu instalacji komputerowej powinniśmy mieć dostęp do aktualnego planu przebiegu obwodów elektrycznych w budynku. Uzyskanie takich informacji w wielu przypadkach sprowadza się do obniżenia kosztów projektowania sieci komputerowej. Jeśli mamy taki plan, jesteśmy w stanie dokładnie określić, na jakiej wysokości, w jakich punktach przebiegają ścieżki okablowania elektrycznego, wiemy, gdzie następuje ich koncentracja, znamy ich dokładny rozkład.

Instalacja komputerowa jest bardzo czuła na wszelkie zakłócenia w postaci fali elektromagnetycznej, pochodzące najczęściej z pola otaczającego przebiegające w ścianach okablowanie elektryczne.

Znajomość tych informacji pozwoli tak zaadaptować sieć komputerową, by w jak najmniejszym stopniu uzyskiwała ona styczność z przebiegami instalacji elektrycznej. Dzięki temu już w fazie projektowania możemy uwzględnić odpowiednie rozwiązania, jak np. ekranowane korytka, które możemy umieścić w miejscach, gdzie sieć komputerowa mogłaby zostać zagrożona przez wymierny wpływ pola elektromagnetycznego pochodzącego z instalacji elektrycznej.

Jeśli uwzględnimy w czasie projektowania takie właśnie punkty, uchroni to nas przed stratą czasu spowodowaną przesuwaniem lub reorganizowaniem przebiegu danego fragmentu sieci. Oszczędzimy przy tym również nadmiar okablowania, eliminujące ewentualne dodatkowe punkty połączeniowe, które w sieciach komputerowych są najczęstszymi punktami wprowadzającym spadek ogólnej wydajności sieci.

Sam projekt sieciowy w zależności od wymogów może składać się z dwóch części. Pierwszą z nich jest *projekt logiczny*. Projekt logiczny przedstawia ogólny zarys topologii, na którym odnajdziemy najważniejsze punkty sieci, pokazujące jednoznacznie, jaki charakter będzie miała topologia sieciowa. Na drugą część projektu sieciowego składa się *projekt fizyczny*. Projekt fizyczny, jak wskazuje sama nazwa, to przedstawienie praktycznych rozwiązań, które na planie logicznym nie znalazły odzwierciedlenia.

Projekt fizyczny stanowi największy zbiór informacji, które instalator musiał wcześniej przemyśleć i nanieść w postaci konkretnego rozwiązania.

Te dwa przedstawione elementy informują nas tylko o końcowym wyglądzie sieci, jaki uzyskujemy po wykonaniu prac projektowych.

Do uzyskania takiego końcowego planu potrzebne jest przemyślenie wielu elementów, po wykonaniu których możemy dopiero przystąpić do projektowania.

Pierwszym elementem jest określenie punktów ważnych z punktu widzenia odbiorcy projektu. Musimy zatem ustalić, czego oczekiwać będzie od sieci użytkownik. Dla każdej instalacji sieciowej kluczowy element stanowi wymóg określenia jej ważnych punktów. Z reguły informacje takie powinniśmy uzyskać od użytkownika. Nasza instalacja powinna mieć taki charakter, by już w samym projekcie można było zauważyć jej zalety, które odzwierciedlą się w praktyce spełnieniem tych najważniejszych wymogów.

Jeśli mamy już informacje na temat „strategicznych punktów sieci", musimy zestawić je ze sobą, by móc dokonać logicznego podziału funkcji i operacji, jakie wykonywane będą w danej strefie. I tak określamy, jakie czynności wykonywane będą w danym obszarze sieci. Sprawdzamy, jakie funkcje będą wymagane od strony funkcjonalnej sieci (przepustowość, bezpieczeństwo, dostępność, skalowalność). W ten sposób uzyskujemy przyszły obraz prac, jakie realizowane będą w danym obszarze, zestawiając je z wymogami, jakim powinna sprostać instalacja sieci komputerowej.

Po zakończeniu takiego rozeznania powinniśmy mieć informacje także co do ilości punktów gniazd przyłączeniowych, jakie potrzebne będą w danym pomieszczeniu, oraz miejsc ich instalacji, tak by ogólna odległość pomiędzy przyłączanym sprzętem komputerowym nie przekroczyła 5 metrów. We wszystkich kwestiach dotyczących dopuszczalnej odległości i możliwości rozwiązania danej koncentracji połączeń odsyłam do rozdziałów wcześniejszych, w których przedstawiłem wszystkie niezbędne wymogi dla okablowania miedzianego i światłowodowego oraz ich przebiegów.

Jeśli rozważenie podstawowych wymogów mamy już za sobą, powinniśmy te informacje nanieść na nasz początkowy plan — projekt.

Ten prosty krok odkryje przed nami ogólny zarys przebiegu okablowania, jaki powinniśmy zastosować, by uzyskać pożądany efekt w postaci dostarczenia odpowiedniej usługi we właściwe miejsce.

Kolejnym etapem przygotowania projektu sieciowego jest określenie punktów koncentracji okablowania. W sieciach komputerowych wyróżnić można wiele rodzajów punktów tak zwanej *koncentracji*. W zasadzie można powiedzieć, że w sieci komputerowej spotkać możemy:

- główny punkt koncentracji,
- pośredni punkt koncentracji,
- końcowy punkt koncentracji.

Te trzy z pozoru nieciekawie brzmiące nazwy odnoszą się do najważniejszych fragmentów sieci. Dlaczego najważniejszych? Na to pytanie postaram się udzielić odpowiedzi poprzez przedstawienie funkcji takich węzłów oraz urządzeń, jakie możemy tam spotkać.

Główny punkt koncentracji

Główny punkt koncentracji z reguły powinien znajdować się w osobnym pomieszczeniu. Pomieszczenie, w którym możemy umieścić urządzenia oraz punkty koncentracji okablowania szkieletowego, powinno spełniać przynajmniej wymienione warunki.

Wielkość pomieszczenia. Powinien to być obszar całkowicie wolny od wszelkich ścian działowych, okien oraz mebli. Wszystko po to, by zapewnić urządzeniom pracującym w tym pomieszczeniu zarówno dobry obieg powietrza, jak i łatwy i pewny dostęp.

Punkty dostępu do sieci elektrycznej. Powinniśmy unikać instalowania urządzeń wchodzących w skład punktów głównej koncentracji w pomieszczeniach o dużej ilości gniazdek elektrycznych. Dlaczego? Gdy instalujemy ważny element sieci, jakim jest punkt głównej koncentracji (w angielskich materiałach można spotkać się z oznaczeniem POP) w miejscu o wielu możliwościach przyłączenia się do sieci elektrycznej, wzrasta szansa na wystąpienie w danym pomieszczeniu pożaru, spowodowanego przez awarię któregoś z gniazdek. W takiej sytuacji narażamy najważniejszy fragment sieci na nieprzewidywalne i niepotrzebne ryzyko.

Dobór pomieszczenia powinien także odbywać się pod względem rodzaju i ilości zainstalowanych w nim *punktów oświetlenia*. Jest to również bardzo ważny i często pomijany element przy doborze pomieszczenia. Jak wiemy, wszelkie źródła energii wykorzystujące zasilanie elektryczne generują własne źródła pola elektromagnetycznego o określonej częstotliwości. Duże nagromadzenie takich punktów w postaci oświetlenia może negatywnie wpłynąć na długość i jakość pracy urządzeń w sieci i ogólną jej wydajność. Unikajmy zatem bliskiej styczności takich punktów oświetleniowych, szczególnie w postaci oświetlenia jarzeniowego, z urządzeniami wchodzącymi w skład centralnego punktu koncentracji.

Oczywiście w każdym pomieszczeniu powinno znajdować się jakieś źródło światła, jednak starajmy się uzyskać jak największą odległość pomiędzy źródłem światła a urządzeniami sieci komputerowej.

Dostęp do pomieszczenia.Tu chyba nie ma żadnych wątpliwości. Punkt głównej koncentracji to wręcz strategiczny fragment sieci, którego awaria najczęściej odzwierciedla się w ogólnej niedostępności poszczególnych stref sieciowych czy też usług, jak choćby dostęp do baz danych czy zasobów sieci Internet.

Właśnie z tego powodu dostęp do pomieszczenia powinien być jak najlepiej zabezpieczony. Zabezpieczenie to specjalne drzwi w połączeniu z odpowiednim systemem kontroli i uwierzytelniania tożsamości osoby uzyskującej dostęp. Mile widziane są tu wszelkie rozwiązania w postaci elektronicznych urządzeń rejestrujących ruch czy dane osoby uzyskującej dostęp w połączeniu z dokładną datą. Oczywiście nie istnieje nic, co da nam stuprocentową pewność, że sieć nie zostanie celowo uszkodzona przez któregoś z pracowników. Jednak podniesie to nasz ogólny komfort i bezpieczeństwo zasobów znajdujących się w sieci.

Wymogiem dla pomieszczenia, które ma zostać zaadaptowane do roli centralnego punktu koncentracji, jest posiadanie przez nie *drzwi otwieranych na zewnątrz*. Ten nieco dziwaczny wymóg jest naprawdę bardzo istotny. Dlaczego? Wyobraźmy sobie, co mogłoby się stać, gdyby ktoś gwałtownie otworzył drzwi otwierające się do wewnątrz pomieszczenia. Oczywiście mógłby uszkodzić, zniszczyć urządzenia znajdujące się w tym pomieszczeniu, a jak się domyślamy, nie należą one do tanich.

Z drugiej strony uzyskujemy większą przestrzeń, którą możemy lepiej zaadaptować, uzyskując np. łatwiejszy dostęp do szaf krosowych czy też lepszą cyrkulację powietrza.

Oczywiście nie ma sensu wspominać tutaj o doborze odpowiednio suchego pomieszczenia, nikt przecież nie zaryzykuje instalacji tak ważnych systemów w pomieszczeniu, które może zostać zalane przy pierwszych lepszych opadach deszczu. Warto jednak jeszcze raz wspomnieć o doborze takiego pomieszczenia, które nie będzie kusić osób niepowołanych na przykład nie osłoniętymi, nie zabezpieczonymi oknami znajdującymi się tuż na parterze. Wystrzegajmy się takich sytuacji, a jeśli to możliwe, wybierzmy takie pomieszczenie, w którym nie ma okien lub w którym da się je łatwo zamurować.

Pośredni punkt koncentracji

Pośredni punkt koncentracji to element często występujący w sieciach składających się z wielu rozmaitych pomieszczeń i budynków. Z reguły urządzenia znajdujące się w jego obrębie są łączone z głównym punktem koncentracji za pośrednictwem okablowania szkieletowego.

Po co stosuje się punkt pośredniej koncentracji? Jest wiele powodów, jednak jeśli będziemy wykonywać projekt sieciowy, zauważymy, że zastosowanie punktu pośredniej koncentracji nie tylko zmniejsza ogólną ilość przewodów, jakie potrzebne są do budowy całej sieci, ale także ich łączną długość. Posiadając taki punkt, nie musimy instalować każdej wiązki okablowania do odległego często punktu głównej koncentracji, lecz do punktów ich pośredniej koncentracji. Z drugiej strony uzyskujemy dodatkowy punkt w sieci, w obrębie którego możemy wpłynąć na charakter i rodzaj uzyskiwanych połączeń.

W małych sieciach punkty te często przybierają formę szaf, szafek, w których nie znajduje się duża ilość urządzeń. Jeśli tak jest w naszym przypadku, to możemy posunąć się do próby montażu takiego punktu w obszarze np. sufitu podwieszanego czy też na zapleczu jakiegoś pomieszczenia.

Jeśli jednak mamy do czynienia z dużą siecią, punkty te mogą zawierać równie imponującą ilość sprzętu, a przede wszystkim połączeń, jak punkty głównej koncentracji. Dlatego w takiej sytuacji warto również na lokalizację takiego punktu pośredniej koncentracji poświęcić dodatkowe pomieszczenia. Co do wymogów wobec takiego pomieszczenia, to tak jak w przypadku punktów głównej koncentracji musi ono mieć określone cechy.

Wielkość pomieszczenia. Powinien to być obszar całkowicie wolny od wszelkich ścian działowych, okien oraz mebli. Wszystko po to, by zapewnić urządzeniom pracującym w tym pomieszczeniu zarówno dobry obieg powietrza, jak i łatwy i pewny dostęp. Pamiętajmy, że pomieszczenia pośredniej koncentracji mogą być zdominowane przez ogromne ilości pasywnych koncentratorów — tak można określić np. *patch panele* (o tym dalej), w związku z czym mogą być one zapełnione dużą ilością okablowania, które jak wszystko wymaga odpowiedniego miejsca i zarządzania.

Punkty dostępu do sieci elektrycznej. Powinniśmy unikać instalacji urządzeń wchodzących w skład punktów pośredniej koncentracji w pomieszczeniach o dużej ilości gniazdek elektrycznych. Dlaczego? Gdy instalujemy taki bardzo ważny punkt sieci, jakim jest punkt pośredniej koncentracji, w miejscu o wielu możliwościach przyłączenia się do sieci elektrycznej, wzrasta szansa na wystąpienie w danym pomieszczeniu pożaru, spowodowanego przez awarię któregoś z gniazdek. W takiej sytuacji narażamy ważny fragment sieci na nieprzewidywalne i niepotrzebne ryzyko. Dobór pomieszczenia powinien także odbywać się pod względem rodzaju i ilości zainstalowanych w nim *punktów oświetlenia*. Jest to również bardzo ważny i często pomijany przy doborze pomieszczenia element. Jak wiemy, wszelkie źródła energii opierające się na zasilaniu elektrycznym generują własne pola elektromagnetyczne o określonej częstotliwości. Duże nagromadzenie takich punktów w postaci oświetlenia może negatywnie wpłynąć na długość i jakość pracy urządzeń w sieci i ogólną jej wydajność. Unikajmy zatem bliskiej styczności takich punktów oświetleniowych, szczególnie w postaci oświetlenia jarzeniowego.

Oczywiście w każdym pomieszczeniu powinno znajdować się jakieś źródło światła, jednak starajmy się uzyskać jak największą odległość pomiędzy źródłem światła a urządzeniami sieci komputerowej.

Dostęp do pomieszczenia. Tu chyba nie ma żadnych wątpliwości. Punkt pośredniej koncentracji, tak jak i punkt głównej koncentracji to wręcz strategiczny fragment sieci, którego awaria najczęściej odzwierciedla się w ogólnej niedostępności poszczególnych stref sieciowych czy też usług, jak choćby dostęp do baz danych czy zasobów sieci Internet.

Właśnie z tego powodu dostęp do pomieszczenia powinien być jak najbardziej zabezpieczony. Tak jak w przypadku punktu głównej koncentracji, tak i tu wtargnięcie niepożądanej osoby do takiego pomieszczenia pozwoli jej na przekonfigurowanie sieci nawet w taki sposób, że uzyska ona dostęp do z zamierzenia izolowanych fragmentów sieci i usług. Dbajmy zatem o bezpieczeństwo tych pomieszczeń.

Wymogiem dla pomieszczenia, które ma zostać zaadaptowane do roli pośredniego punktu koncentracji, jest posiadanie przez nie *drzwi otwieranych na zewnątrz*. Ten nieco dziwaczny wymóg jest naprawdę bardzo istotny. Dlaczego? Wyobraźmy sobie, co mogłoby się stać, gdyby ktoś gwałtownie otworzył drzwi otwierające się do wewnątrz pomieszczenia. Oczywiście mógłby uszkodzić, zniszczyć urządzenia znajdujące się w tym pomieszczeniu, a jak się domyślamy, nie należą one do tanich.

Z drugiej strony uzyskujemy większą przestrzeń, którą możemy lepiej zaadaptować, uzyskując np. łatwiejszy dostęp do szaf krosowych czy też lepszą cyrkulację powietrza.

Punkt końcowej koncentracji

Punkt końcowej koncentracji to obszar, który właściwie kojarzy nam się z przyłączaniem, terminacją gniazd przyłączeniowych oraz okablowania z niego wychodzącego. Wszystkie połączenia pochodzące z obszarów pracy powinny trafiać właśnie do punktów terminacji końcowej.

Punkty terminacji końcowej lub też wewnętrznej słusznie kojarzą się nam z wszelkiego rodzaju koncentratorami, przełącznikami, które montowane są w specjalnych szafkach określanych w materiałach angielskich jako *Consolidation point*. Instalacja takiej szafki ma zagwarantować odpowiednie zainstalowania urządzeń i zagospodarowanie okablowania, jak również ochronę znajdujących się wewnątrz urządzeń przed dostępem osób niepowołanych.

Wszystkie połączenia wychodzące z punktów koncentracji końcowej mogą trafić wyłącznie do gniazd przyłączeniowych znajdujących się w obszarach pracy. Wiele rozwiązań wymaga prowadzenia podwójnej ilości okablowania do każdego z gniazd. Jest to wymóg, którego zaletę można zauważyć np. w czasie awarii połączenia pomiędzy punktem koncentracji końcowej a jednym z dwóch gniazd przyłączeniowych obszaru pracy.

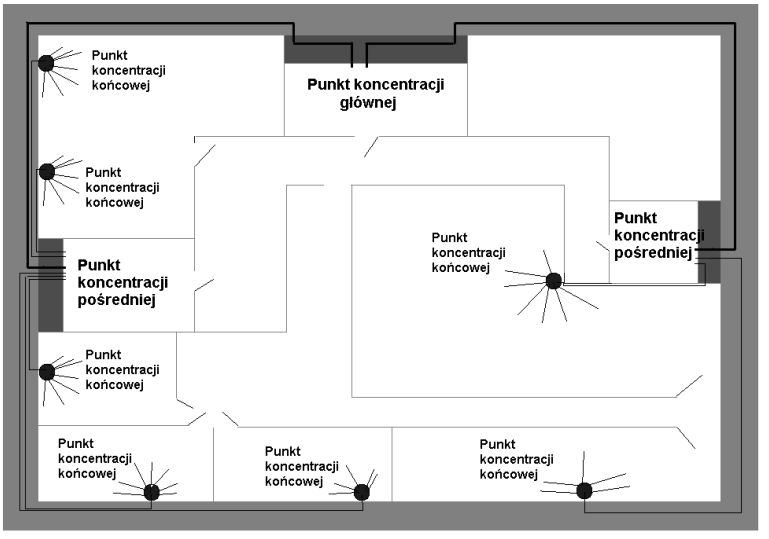
Co prawda rozwiązanie takie podnosi koszty całej sieci, jednak warto je zastosować w celu uzyskania zarówno większej ilości punktów przyłączeniowych przypadających na dane stanowisko, jak i większej dostępność pasma. Jeśli do gniazda przyłączeniowego poprowadzimy dwie równoległe ścieżki okablowania, które z drugiej strony trafią na odpowiednio skonfigurowany przełącznik, możemy uzyskać dokładnie takie samo pasmo dla gniazda pierwszego i drugiego. Przyłączając do niego urządzenia, uzyskujemy izolowane pasmo oraz pewność, że transmisja pierwszego urządzenia nie wpłynie specjalnie na szybkość pracy drugiego. Opisana sytuacja nie dotyczy opcji, w której zamiast przełącznika umieścimy koncentrator.

Z drugiej strony z takiego punktu koncentracji końcowej okablowanie wychodzące może trafić wyłącznie do obszarów koncentracji pośredniej. Całość struktury przedstawia rysunek 12.1.

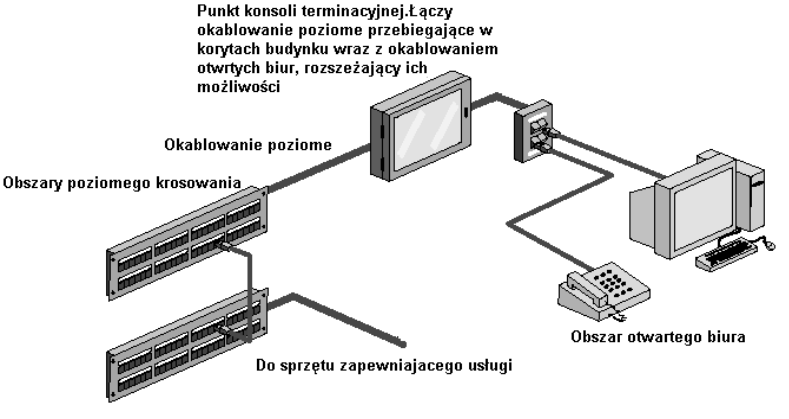
Rysunek 12.1 przedstawia tylko prosty przykład rozmieszczenia omawianych punktów koncentracji i posługiwania się nimi. W praktyce obszary zaznaczone kolorem czerwonym zawierają duże ilości okablowania, które dopiero po odpowiednim ich ułożeniu i oznaczeniu trafiają do właściwych urządzeń i serwerów. Punkty oznaczone kolorem niebieskim to szafki zawierające przełączniki, koncentratory, z których wyprowadzone okablowanie trafia do gniazd przyłączeniowych, zdefiniowanych przy każdym ze stanowisk, które wymaga dostępu do sieci.

Rysunek 12.2 przedstawia rozwinięcie punktów końcowej terminacji, pokazując właściwe przyłączenia urządzeń końcowych obszaru pracy.

Po przedstawieniu przebiegu okablowania w budynku i zapoznaniu się z jego charakterem, punktami koncentracji oraz obszarami głównego sterowania, jakim jest punkt głównej koncentracji, możemy rozważyć, jakie urządzenia mają wejść w skład danej sieci.



Rysunek 12.1. *Koncentracja połączeń*



Rysunek 12.2. *Końcowe przyłączenie urządzeń obszaru pracy*

Określenie tego punktu zależeć będzie od dwóch czynników:

1. Jakości oferowanych przez sieć usług podczas sprawnego i wydajnego funkcjonowania oraz ochrony.
2. Środków, jakie możemy przeznaczyć na wykonanie i wdrożenie projektu.

Oczywiście dobór urządzeń zawsze zależy od wykonawcy, jednak musi on mieć orientację co do możliwości użycia, uruchomienia oraz korzyści, jakie przyniesie instalacja danego sprzętu.

Podstawową zasadą, którą musimy się kierować, dokonując wyboru sprzętu i jego późniejszej instalacji, jest umieszczanie go w miejscach, do których zwykli użytkownicy nie mają dostępu. Nie możemy sobie pozwolić na sytuację, w której takie urządzenia, jak np. przełączniki znajdują się w „pierwszym lepszym" rogu pomieszczenia, tylko i wyłącznie dlatego, że tak było wygodnie. Takie podejście do spraw instalacji jest niedopuszczalne. A jeśli już ktoś wdrożył taki pomysł, to powinien się cieszyć, na pewno

będzie miał duże pole do popisu podczas pierwszej awarii sieci, w czasie której lokalizacja uszkodzenia przebiegać będzie zarówno w terenie (taka osoba musi przecież sprawdzić, czy ktoś np. nie dopiął się do wolnego portu), a następnie na warstwach wyższych modelu OSI (w przypadku nagłych niestabilności sieci, wywoływanych przez transmisję zbędnych pakietów przez tajemniczy host). Opisana sytuacja wydaje się może nieco dziwna, ale przecież czego innego można się spodziewać przy takim podejściu do spraw bezpieczeństwa przez instalatora czy też administratora danej sieci komputerowej.

Wspomniana sytuacja nie jest wymyślona. Jest to częsty problem w sieciach, zarządzanych przez kilka osób, z których każda ma swój własny, odrębny pomysł na rozwiązanie danej sytuacji.

Wracając do naszego planu przygotowania i wdrożenia sieci, widzimy już, jak ważne jest odpowiednie rozmieszczenie urządzeń, tak by nie kusiły, nie zachęcały swym interesującym i tajemniczym widokiem typowych użytkowników sieci.

Urządzenia głównego punktu koncentracji sieci

Obszar POP, bo taką nazwę możemy spotkać w różnej dokumentacji, stanowi najważniejszy punkt sieci. To właśnie w tych pomieszczeniach dokonuje się całej administracji siecią. Pomieszczenia te to z reguły wypełnione po brzegi sprzętem pokoje. Właśnie z tego powodu punkty POP zawierają zarówno urządzenia aktywne, jak i pasywne.

Pojęcie *urządzeń aktywnych* odnosi się z reguły do urządzeń, których funkcjonowanie uwarunkowane jest zasilaniem elektrycznym.

Urządzenia pasywne, jak zapewne się domyślamy, stanowią podstawę dla instalacji urządzeń aktywnych.

W pomieszczeniach POP możemy spotkać się z:

- routerami i bramami,
- przełącznikami,
- zaporami obronnym,
- modemami, zapewniającymi dostęp do sieci publicznych,
- systemami serwerów dla sieci VoIP,
- serwerami baz danych,
- serwerami zapewniającymi kontrolę ruchu danych w sieci,
- serwerami zapewniającymi usługi zarówno dla sieci wewnętrznej, jak i zewnętrznej, obsługującymi zadania SSH, POP3, SMTP, FTP, DNS, HTTP, NNTP, NTP i wiele innych.

Taki zakres urządzeń nie jest może regułą co do jego umieszczania na terenie POP, jednak wielu instalatorów i administratorów wręcz domaga się takiego umiejscowienia elementów. Z jednej strony takie rozmieszczenie urządzeń zapewnia łatwą i szybką

kontrolę nad działaniem sieci, pozwala lepiej i taniej zabezpieczyć jej ważny punkt. Ogranicza także możliwość wewnętrznego ataku na sieć, wykonanego z wielu różnych miejsc sieci.

Z drugiej strony, gromadząc urządzenia kontrolujące i zarządzające ruchem w całej sieci w jednym centralnym punkcie, musimy być pewni co do jego odpowiedniego zabezpieczenia.

Urządzenia koncentracji pośredniej

Punkty przyłączane do POP w obszarze sieci szkieletowej zapewniają odpowiednie logiczne, a następnie fizyczne rozmieszczenie zarówno okablowania, jak i struktury adresowej sieci. Punkty pośredniej koncentracji są często równie ważne jak punkt POP.

Główna różnica co do lokowanego w nich sprzętu wynika z braku instalacji systemów serwerowych. Jak zostało to wielokrotnie zaznaczone, obszary koncentracji pośredniej powinny zapewniać optymalizacją połączeń, w obrębie której mogą one dokonywać elektrycznego przełączania ścieżek, realizując tę funkcję przez np. przełączniki.

Punkty te powinny zapewniać dostęp dla każdego z punktów terminacji pośredniej. W związku z tym wymogiem muszą być wyposażone we wszelkie rozwiązania wzmacniające sygnał, takie jak repetery, koncentratory czy też przełącznik nadrzędny, przez który punkt koncentracji pośredniej nawiązuje połączenie z POP.

Punkty pośredniej koncentracji są też często wykorzystywane jako dodatkowe routery bądź też przełączniki umożliwiające tworzenie tak zwanych obszarów VLAN. Dzięki takim rozwiązaniom administrator sieci uzyskuje dodatkową możliwość zarówno kontroli ruchu, jak i dopasowania odpowiednich obszarów końcowych, tak by były one bezpieczne oraz wydajniejsze.

Oczywiście instalacja routerów o słabej wydajności nie przyniesie tu pożądanego efektu. Pamiętajmy zatem, by w miarę możliwości dobrać jak najlepsze urządzenie.

Instalacja routerów w punktach pośredniej koncentracji oprócz wspomnianych zalet da także możliwość wprowadzenia odrębnej lub też dokładniejszej adresacji IP wewnątrz sieci.

Ponieważ punkt POP i obszary pośredniej koncentracji skupiają w swoim obrębie często ogromne ilości okablowania, co może stanowić później problem podczas uruchamiania czy też diagnostyki sieci, dla zaradzenia takiej sytuacji w miejscach koncentracji okablowania stosuje się często specjalne kratowe tunele, które zarówno doprowadzają, jak i utrzymują w odpowiednim ładzie całe okablowanie.

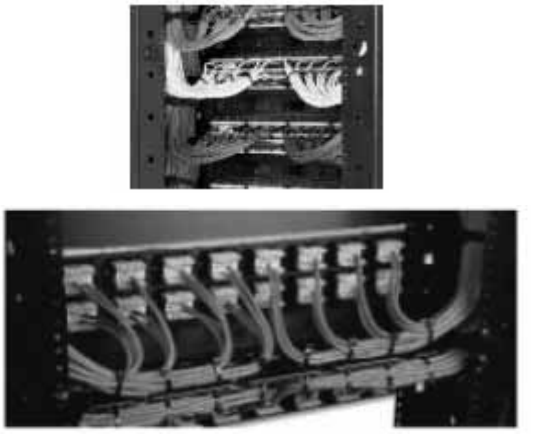
Czemu jest to takie ważne? Otóż w wielu sieciach ilość punktów, do których ma zostać doprowadzona sieć, jest tak duża, że ilość okablowania przeprowadzonego pomiędzy tymi końcowymi punktami a punktami koncentracji pośredniej nie dałaby się objąć półtorametrowym pasem. Właśnie dlatego w takiej sytuacji wymaga się budowania specjalnych stelaży, które będą w stanie odpowiednio poprowadzić okablowanie i utrzymać je w porządku oraz zagwarantować łatwiejszy późniejszy dostęp do sieci.

Każde zakończenie takiego tunelu doprowadza okablowanie do punktów koncentracji pośredniej, niekiedy też do punktu koncentracji głównej.

Okablowanie opuszczające taki specjalny tunel czy też koryto prowadzące trafia do specjalnej szafy wypełnionej strukturą *patch paneli*.

Pojęcie *patch panelu* odnosi się do pasywnej struktury, zapewniającej z jednej strony stałą terminację okablowania przebiegającego np. między punktem POP a punktami pośredniej terminacji, a z drugiej strony posiadającej specjalnie rozmieszczone gniazda, pozwalające zarówno na łatwe wpięcie danego obszaru, jak i jego późniejsze przepięcie w inny obszar sieci. Rozwiązania oparte na strukturach *patch paneli* umożliwiają także łatwe i pewne zdefiniowanie punktu, do którego ma zostać podpięty dany fragment sieci czy host oraz wprowadzają ład w samo rozłożenie okablowania. Opisaną sytuację dobrze zobrazuje rysunek 12.3.

Rysunek 12.3. *Tylna terminacja okablowania sieciowego*



Zamieszczony rysunek przedstawia sposób zarządzania okablowaniem przebiegającym pomiędzy punktami zarówno pośredniej, jak i końcowej terminacji. Zauważmy, z jaką ilością okablowania możemy spotkać się przy wdrażaniu sieci o wielu punktach przyłączeniowych. Pokazane rozwiązanie pozwoli łatwo i pewnie zarządzić przebiegającym okablowaniem i rozmieścić je.

Struktury *patch paneli* w zależności od wielkości sieci umieszcza się w specjalnych *rackach*. Ponieważ wszystkie rozwiązania sieciowe przystosowane do instalacji wykonane są w określonych wymiarach, dlatego też zakup i instalacja obramowania typu *rack* pozwala nam nie tylko na instalację odpowiedniej ilości *patch paneli*, ale także na dobre rozmieszczenie w obszarze *racka* urządzeń takich jak router, przełączniki, koncentratory, a nawet serwery.

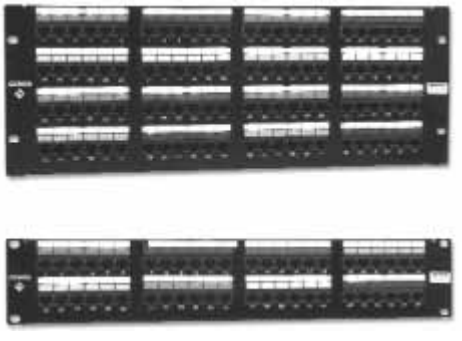
Każdy dobrze wykonany i rozwiązany *patch panel* zapewni nam obszar, w obrębie którego będziemy mogli sprawnie i logicznie przymocować i rozprowadzić okablowanie.

Takie zarządzanie okablowaniem jest naprawdę ważne. W przeciwnym razie możemy doprowadzić do sytuacji, w której w pewnym punkcie zgromadzimy ogromną ilość kabli, przez co nie będziemy w stanie dokonać ich właściwego i czytelnego połączenia.

Nie uzyskamy także odpowiedniej żywotności okablowania, które nieodpowiednio rozmieszczone i przytwierdzone będzie narażone na przerwania wewnętrznych włókien czy to światłowodowych, czy to miedzianych.

Przednia część *patch panelu* (rysunek 12.4) w zależności od rozwiązania producenta może prezentować przed instalatorem odpowiednio rozmieszczone pola. Każde z takich pól ma odpowiednią etykietę, którą możemy i powinniśmy przyporządkować na planie do odpowiedniego urządzenia, punktu końcowego. Zapewni nam to sprawne poruszanie się po sporej ilości okablowania, uchroni nas także przed zbędnym poszukiwaniem odpowiedniego zakończenia sieciowego.

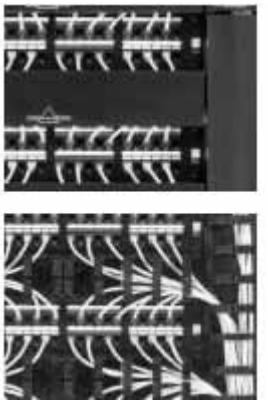
Rysunek 12.4.
Przednia część patch panelu



Oczywiście wielkość, czyli ilość portów, jakie możemy wykorzystać do naszego zaterminowania, zależy wyłącznie od naszych potrzeb.

Końcowa instalacja oraz odpowiednio rozłożone okablowanie odkrywają przed nami imponującą niekiedy ilość połączeń, którymi możemy później łatwo zarządzać. Sytuację taką przedstawia rysunek 12.5.

Rysunek 12.5.
Odpowiednio rozłożone i zaterminowanie okablowanie



W końcowej części rozplanowywania połączeń z uwzględnieniem *patch paneli* jako szaf połączeń będziemy musieli zastosować odpowiedni schemat adresowania tych połączeń, który jednoznacznie określać będzie punkt w szafie, gdzie dany host czy sprzęt teleinformatyczny zostanie przyłączony. Jednak nim do tego dojdziemy, musimy zorientować się, jak może wyglądać rozmieszczenie i wyprowadzenie połączeń w punktach agregacji końcowej czy też w punktach konsolidacyjnych.

Z reguły obszary końcowego przyłączenia znajdują się bezpośrednio w pomieszczeniach, w których mamy dokonać przyłączenia urządzeń komputerowych czy też teleinformatycznych. Właśnie z tego powodu powinniśmy zastosować rozwiązanie zapewniające zarówno łatwy dostęp instalatora do przyłączy, jak i uniemożliwiające bezpośrednią ingerencję osób niepożądanych w fizyczny schemat połączeń.

Rozwiązaniem są tu wszelkie szafy, wyposażone w miniaturowe wewnętrzne *racki*, do których możemy zamocować wymagane urządzenia zarówno w postaci koncentratorów, jak i przełączników. Wymagane jest także użycie takiego rozwiązania, które umożliwi nam poprawny opis przyłączy oraz zapewni ich odpowiednią ilość potrzebną teraz do przyłączenia oraz pozwalającą na dalszy przewidywany, skalowany rozwój. Elementy, które z pewnością będą nam przydatne, możemy zobaczyć na rysunku 12.6. Rysunek przedstawia pojedynczy obszar konsolidacyjny, w obrębie którego dokonujemy właściwego krosowania połączeń. Ich końce mogą biec do odpowiednio rozmieszczonych i zamocowanych gniazd przyłączeń końcowych.

Rysunek 12.6.
Punkt konsolidacyjny

Przedstawione rozwiązanie umożliwia dołączanie odpowiednich obwodów sieci za pomocą specjalnych noży. Noże pozwalają na ich bezpośrednie umieszczenie w szczelinie wykonanej z połączenia plastiku i odpowiedniego ostrego styku włókna okablowania. Odpowiednio wykonane połączenie chroni okablowanie zarówno przed wpływem czynników środowiska zewnętrznego, jak i dostępem osób niepożądanych.

Punkty końcowej terminacji często wyposażane są w podobne otwierane szafki, w których możemy umieszczać odpowiednie przełączniki czy też koncentratory. Różnią się one jednak budową. Szafka pozwalająca na umieszczenie opisanych urządzeń posiada wewnątrz odpowiedni stelaż (*rack*), w obrębie którego możemy umieszczać urządzenia.

Wielkość szafki powinna być tak dobrana, by zapewniała odpowiednią cyrkulację powietrza, łatwy dostęp i pewne mocowanie dla wszystkich urządzeń.

Oczywiście na wyposażeniu takiej szafy powinny znajdować się odpowiednie punkty, czy to w postaci naklejek, czy też pasków-obrączek, za pomocą których możemy poprawnie zdefiniować przyłączane okablowanie.

Takie przedstawienie punktów koncentracji okablowania oraz powodów, dla jakich warto je zastosować, pozwala zaplanować dalsze działania.

W kolejnym etapie projektowania musimy rozplanować położenie wszystkich omawianych wcześniej punktów. Nasz plan musi być zgodny co do norm odległości i rozmieszczenia, jakie przedstawiane były w części poprzedniej.

Poprawne rozplanowanie w oparciu jedynie o zgodność adresową niewiele daje z punktu widzenia wydajności, efektywności i kontroli ruchu transmitowanych danych. Dlatego poprawnego rozważenia rozmieszczenia punktów sieci i gniazd przyłączeń końcowych musimy dokonać pod wpływem następujących czynników:

- Określenia operacji, jakie prawdopodobnie i zarazem najczęściej wykonywane będą w danym obszarze czy obszarach pracy.
- Schematu adresowania IP, który zagwarantuje zarówno odpowiedni dostęp do danych, jak i dalszą skalowalność sieci.

Rozpatrzenie tych podstawowych czynników, które wpłyną na łatwość wykorzystania i kontrolę zasobów sieci, należy wykonać przed logicznym rozmieszczeniem punktów sieci. Po dokonaniu projektu adresacji, o którym możemy przeczytać w dalszej części, musimy podjąć środki, mające na celu odpowiednie oznaczenie wszystkich połączeń. Zadanie to musi zostać wykonane tak, by przy każdym przyłączu końcowym (TO), do którego przypinamy sprzęt komputerowy czy też teleinformatyczny, znajdowała się etykieta. Informacje, które etykieta powinna zawierać, muszą jednoznacznie wskazywać na końcowy numer szafy, do którego prowadzi dane połączenie, a także określać, w jakim gnieździe danej szafy należy szukać zakończenia tego połączenia.

Dokonanie takiego opisu na etykietach, określających numery gniazd-połączeń, zapewni czytelność układu okablowania i umożliwi łatwe odnalezienie drugiego końca kabla nawet w przypadku przebiegu okablowania wewnątrz ścian czy innych trudno dostępnych obszarów.

Jak przygotować odpowiedni plan rozmieszczenia?

Odpowiednie rozmieszczenie punktów koncentrujących w obszarze budynku powinno pozwalać na łatwe zarządzanie zakresem możliwości dostępowych do danych usług w stosunku do danego obszaru. Jako instalatorzy, po przeprowadzonym na samym początku planowania sieci wywiadzie co do potrzeb danych działów czy grup platform systemowych i hostów wiemy, jaka usługa powinna być dostępna w danym obszarze.

Wykreślając taką mapę na obszarze budynków, uzyskujemy łatwy i czytelny obraz zależności odpowiadających danej grupie. W dalszym kroku powinniśmy zająć się elementem bezpieczeństwa czy też ochrony danych obszarów przed niepożądanym dostępem określonych hostów. Taki sposób podejścia do projektu zapewni już na samym początku

wydajne, funkcjonalne rozwiązanie. Wiele aspektów bezpieczeństwa da się przecież uzyskać poprzez budowę odpowiednio ograniczonej czy też wydzielonej architektury sieci.

Jeśli dokładnie określiliśmy zakres wymogów i potrzeb danych obszarów sieci, musimy odnieść ten fakt do struktury logicznej, a później fizycznej sieci.

Podziału dokonać możemy na kilka sposobów. Jednym z lepszych rozwiązań jest sprzętowe ograniczenie styków różnych grup ze sobą. Co należy rozumieć pod pojęciem *sprzętowego podziału*? Jako instalatorzy mamy prawo, a nawet jesteśmy zobligowani do takiego zorganizowania obszaru ruchu pakietów czy też ramek w sieci, by ograniczyć wpływ niepotrzebnego ich poruszania się po szkielecie sieci. Naszym celem jest przede wszystkim zapewnienie wysokiej jakości usług w danym obszarze, tak by każdy mógł swobodnie wykonywać własne prace oraz tak, by ruch, jaki generowany jest w jednym z obszarów, nie wpływał na transmisję w innym. Powinniśmy się także skupić na możliwości sterowania i kontrolowania przepływu danych pomiędzy poszczególnymi punktami sieci. Ważnym elementem będzie także kontrola ruchu brodcastowego i sterowania oraz określenie, które pakiety mogą podróżować przez dany obszar.

Wszystkie wspomniane sytuacje znajdują swoje rozwiązanie już przez zastosowanie rozwiązań sprzętowych, które możemy określić mianem *rozwiązania na warstwie sprzętowej*.

W takiej fazie projektu niezbędna jest znajomość modelu referencyjnego OSI oraz urządzeń występujących i funkcjonujących na danej warstwie tego modelu. Musimy także dobrze znać zarówno sposób działania danego urządzenia, jak i zachowania się danego obszaru, segmentu po wprowadzeniu takiego urządzenia w jego strukturę.

Budowa obszarów i grup wyspecjalizowanych

Jeśli wykonaliśmy wszystkie wcześniejsze czynności i rozumiemy potrzebę podziału sieci już na samej warstwie sprzętowej, możemy przystąpić do wdrożenia danego rozwiązania w projekcie sieci.

Podziału sieci na wyspecjalizowane grupy możemy dokonać przez zastosowanie kilku urządzeń. Jasne jest, że w celu wykonania powyższego schematu możemy poruszać się jedynie w obrębie drugiej i trzeciej warstwy modelu OSI, gdyż tylko urządzenia tam się znajdujące mają możliwość kierowania obszarami ruchu pakietów i ramek.

Pierwszym urządzeniem, o jakim powinniśmy pomyśleć, jest przełącznik. Na rynku dostępnych jest wiele przełączników działających w różnych systemach przełączania. Wyboru przełącznika powinniśmy dokonać, analizując cztery właściwości:

- szybkość,
- liczbę dostępnych portów,
- możliwość zarządzania,
- rodzaj obsługiwanych interfejsów sieciowych.

Szybkość danego przełącznika powinna odnosić się do wymaganej przepustowości, jaką musimy udostępnić w danym obszarze. Proszę zatem dobrać taki przełącznik, którego łączna przepustowość będzie w stanie zagwarantować żądaną przepływność w kierunku danego hosta. Polecane dziś rozwiązania wynoszą od 100 Mb/s dla bardzo małych obszarów do 1 Gb/s dla obszarów np. 10 hostów, z których każdy niezależnie może wykorzystać 100 Mb/s. Oczywiście wybór urządzenia ze względu na jego wydajność zależy tylko od nas.

Przy wyborze urządzenia pamiętajmy o wymogu *skalowalności*, czyli funkcjonalności sieci przez okres minimum 5 – 10 lat. Zatem nie dobierajmy danego urządzenia tylko i wyłącznie w taki sposób, by zapewniało ono odpowiednio wydajne działanie jedynie dla sieci o obecnym kształcie. Starajmy się w miarę możliwości wybrać jak najszybsze rozwiązanie z myślą o możliwości późniejszej rekonfiguracji danego fragmentu grupy czy też całego obszaru grupy o np. dodatkowe hosty.

Liczba dostępnych portów to czynnik w zasadzie nie wymagajacy wyjaśnień. Dla każdego instalatora sieci oczywisty jest wybór urządzenia, zapewniającego możliwość dołączenia takiej liczby hostów, jaka przypada na obszar obsługi danego hosta plus jeden wolny port na połączenie przełącznika z innym urządzeniem, które też może znajdować się w obszarze przyłączania końcowego czy pośredniego.

Musimy także pozostawić przynajmniej jeden wolny port na obsługę nieoczekiwanej awarii jednego z interfejsów przełącznika oraz jeden na ewentualne rozszerzenie możliwości przyłączania dodatkowych hostów w grupie przez dodatkowy przełącznik.

Możliwość zarządzania to kolejny bardzo ważny element zarówno z punktu widzenia samej osoby projektującej i uruchamiającej sieć, jak i jej późniejszego administratora. Możliwości zarządzania danego przełącznika zależą oczywiście od modelu i producenta. W ważnych fragmentach sieci (a które takie nie są?) powinniśmy stosować markowe rozwiązania, co do których mamy zaufanie i z którymi najczęściej się spotykamy. Tylko w taki sposób jesteśmy w stanie poznać możliwości danego urządzenia i jego odpowiednią konfigurację. Możliwość zarządzania powinna przejawiać się już w samej budowie urządzenia. Na tylnej ściance danego przełącznika powinien znajdować się odpowiedni port konsolowy, przez który możemy uzyskać dostęp do urządzenia. Rozwiązanie takie realizowane jest rozmaicie przez różnych producentów. Sprawdźmy, czym dysponuje model, który zamierzamy zastosować. Tak jak pokazano to we wcześniejszych rozdziałach, wskazujących na cechy i sposoby zarządzania, funkcja zarządzania powinna stwarzać odpowiedni zakres możliwości, które będą nam potrzebne.

Do takich cech śmiało możemy zaliczyć np. rozwiązania kontrolne oparte na SNMP, kontrolę przepływności, wybór metody przełączania czy też bardziej zaawansowane funkcje pozwalające na tworzenie izolowanych segmentów sieci w celu ograniczenia domen brodcastowych, a co za tym idzie, także możliwość ograniczenia domen kolizji przy odpowiedniej konfiguracji. Rozwiązanie takie możliwe jest dzięki posiadaniu przełącznika realizującego funkcje tak zwanych *Virtual LAN*, czyli w skrócie VLAN.

Użycie takiego typu przełącznika pozwoli na jeszcze dokładniejsze zarządzanie w obszarze danej grupy, co zaowocuje wydajniejszym jej działaniem, odciążeniem sieci ze zbędnych ramek *brodcast* oraz ochroną wirtualnie wydzielonych i separowanych obszarów.

W wielu przypadkach jest oczywiste, że wybór przełącznika zależy od obsługiwanego typu interfejsu sieciowego. Na rynku dostępnych jest wiele rozwiązań obsługujących zarówno interfejsy miedziane, czyli np. dla sieci 10BaseT, jak i interfejsy dla sieci, również *Fast Ethernetu* czy też *Gigabit Ethernetu* lub zwykłego IEEE 802.3. Przy zakupie przełącznika możemy rozważyć jeszcze jeden element, który może nam pomóc przy wyborze danego interfejsu. Na rynku dostępne są rozwiązania określane mianem *tranciverów*. *Tranciver*, o czym można dowiedzieć się więcej we wcześniejszych rozdziałach, może nam posłużyć jako „przejściówka" pomiędzy różnymi fizycznymi mediami nośnika. I tak dla przykładu możemy dokonać zakupu np. przełącznika 2 Gb/s, wyposażonego jedynie w porty RJ 45, i przyłączyć do niego ważny host okablowaniem typu światłowód. Właśnie w tym miejscu, czyli pomiędzy interfejsem RJ-45 przełącznika a zakończeniem światłowodu, np. ST, możemy użyć *trancivera*, który sam w sobie dokona odpowiedniego przekształcenia sygnału optycznego w elektryczny i na odwrót. Istotnym elementem w takiej sytuacji jest sensowność takiego rozwiązania; jeśli nasz przełącznik nie jest specjalnie wydajny, to przyłączenie do niego takiego hosta nie poprawi jakości funkcjonowania danego połączenia.

Kolejnym urządzeniem, którym możemy się posłużyć, jest router. Router jako urządzenie „tak inteligentne jak jego administrator", potrafi pokierować ruchem tak, jak sobie tego życzymy.

Użycie routera w danym punkcie sieci — np. w punkcie koncentracji pośredniej — zapewni nam dodatkową funkcjonalność, która zaowocuje generowaniem izolowanych czy też kontrolowanych sieci wewnętrznych. Router jako urządzenie potrafiące sterować ruchem pakietów pozwoli nam na stworzenie także wewnętrznych podsieci, do czego powinniśmy zmierzać. Dlaczego? Odpowiedź na to pytanie została poparta praktycznym rozwiązaniem przedstawionym we wcześniejszej partii materiału. Użycie VLSM wewnątrz danej wyspecjalizowanej grupy pozwoli uchronić się choćby od nieautoryzowanego podłączenia. Możliwe jest to dzięki określaniu odpowiedniej grupy adresów, jakie możemy wykorzystać w danym obszarze. W ten sposób realizujemy także dodatkową funkcję, jak minimalizacja domen kolizji. Wynika to z samej istoty VLSM, której użycie przyczynia się do powstania sieci wewnątrz sieci. A jak wiemy, informacje reprezentowane w postaci różnych protokołów mogą krążyć w obszarze sieci lub międzysieci jedynie pod warunkiem, że pomiędzy obszarami znajduje się urządzenie — router — które zna drogę dla dalszego przebiegu danego pakietu.

W przeciwnym razie żadna informacja z danej podsieci nie opuści swojego obszaru.

Prezentowane rozwiązanie jest często stosowane w wysoce zaawansowanych sieciach. Dzieje się tak dlatego, że zastosowanie wewnątrz danego obszaru geograficznego sieci wielu podsieci czy też sieci wiąże się z użyciem routera, na którym powinniśmy uruchomić protokół trasowania. Uruchomienie protokołu trasowania obsługującego VLSM, np. RIPv2 czy OSPF, wiąże się z nałożeniem na router dodatkowych obowiązków. Przecież każdy przychodzący pakiet musi zostać odpowiednio sprawdzony, a następnie przekierowany, przełączony na właściwy interfejs. Właśnie z tego powodu powstają dwa problemy:

- tablica trasowania — częste rozsyłanie odpowiednich informacji o stanie sieci,
- szybkość routera.

Wymienione czynniki stanowią zarazem i pozytywny element w sieci, i utrapienie. Zapewne wiele osób może mieć odmienne zdanie, dlatego w nawiązaniu do tego tematu postaram się przybliżyć wspomniany problem.

Użycie routera wewnątrz prywatnej czy też lokalnej sieci wiąże się z wymogiem wykonywania na każdym pakiecie przemieszczającym się przez sieć odpowiednich czynności. Jest to niezbędne dla określenia dalszej drogi przebiegu danego pakietu. Jak zapewne się domyślamy, wykonywanie przez router wspomnianej czynności wiąże się z zajęciem pewnego czasu pracy, w okresie którego każdy pakiet jest chwilowo zatrzymywany w celu określenia jego dalszego przebiegu. Sytuacja nie wymyka się spod kontroli, gdy nasza sieć jest mało wykorzystywana.

Kiedy jednak sieci, pomiędzy którymi znajduje się router, są w ciągłym niemal stanie wymiany danych, możemy wtedy zaobserwować wyraźne i naprawdę bardzo duże spowolnienie w transmisji danych. Sytuacja oczywiście jest do rozwiązania, jednak wiąże się to z zastosowaniem naprawdę wysoko wydajnych routerów. Większość routerów pracujących w sieciach obsługuje interfejsy ethernetowe, czyli jak wiemy te, które wymieniają dane z prędkością 10 Mb/s. Użycie wydajniejszego routera to często kilkakrotnie wyższy koszt zakupu.

Proszę nie mylić routera z coraz częściej pojawiającymi się na rynku urządzeniami typu router-switch. *Urządzenia tego typu stanowią niedrogie hybrydowe rozwiązania, które* łączą w sobie niektóre funkcje przełącznika, takie jak duża ilość portów, z niektórymi funkcjami routera.

Różnicę można zauważyć już na pierwszy rzut oka. *Router-switch* to bardzo ubogie, a zarazem tanie rozwiązanie. Często potrafi nadzorować tylko niektóre funkcje trasowania, rozszerzając je o możliwość przyłączenia wielu interfejsów pracujących z wysoką prędkością, np. 100 Mb/s.

Kupno takiego urządzenia pozwoli na bardzo ubogie konfigurowanie sieci i nie ma co ukrywać, że w większości przypadków nie spełni ono swych zadań. Pamiętajmy, że jako prosta hybryda, łączy w sobie tylko pewne cechy, z których jedna, np. przełącznik, jest dominującą funkcją, a trasowanie to tylko mały okrojony dodatek.

Gdybyśmy chcieli użyć prawdziwego routera posiadającego choćby dwa porty *Ethernetu*, musimy liczyć się z wydatkiem rzędu kilkunastu tysięcy złotych (np. Cisco 2514).

To proste porównanie różnych rozwiązań zwraca naszą uwagę na jakość i szybkość zastosowanego rozwiązania.

Instalacja wewnątrz sieci kilku routerów obsługujących różne sieci tego samego typu wiąże się z jeszcze jednym wspomnianym zagadnieniem. Oprócz dokonywania przez router ciągłych operacji związanych z samym trasowaniem, musi on także rozsyłać (częstotliwość i charakter wymiany informacji o strukturze sieci są oczywiście zależne od metody protokołów trasujących) w określonych odstępach czasu odpowiednie pakiety, informujące inne routery o zmianach czy też aktualnym stanie dostępności sieci. Takie ciągłe rozsyłanie informacji w szybkich sieciach nie stanowi problemu. Jeśli jednak nasza sieć z założenia projektowana jest jako stosunkowo wolna, jednak wystarczająca, musimy liczyć się z dużym spadkiem wydajności i przepustowości.

Będąc już przy wyjaśnianiu sensowności użycia routera wewnątrz mało wydajnej sieci, należy rozpatrzyć sensowność użycia pewnych możliwości zaimplementowanych w systemie operacyjnym routera (IOS — *Inetrnetworking Operating System*). Jak wiemy, router oprócz głównej funkcji przełączania i zarazem kierowania przebiegiem pakietów w obrębie obszarów między sieciami, pozwala na ustawienie odpowiednich funkcji, jak *access-listy*, pełniące rolę *firewalla*. W większość routerów funkcje te są zaimplementowane. Co ciekawe, czasem możemy spotkać router bardzo wysokiej klasy, który nie będzie miał możliwości wykonania takiego filtrowania, jakie dostępne jest na przykład w modelach tańszych. Wyjaśnienie tej sytuacji wiąże się z sensownością używania takiego rozwiązania. Router jako urządzenie jest przeznaczony do kierowania przepływających pakietów na dany interfejs. Uruchomienie na jakimkolwiek routerze dodatkowych funkcji, które sprawdzałyby, czy dany pakiet może zostać zaakceptowany, powoduje bardzo duże utrudnienia w działaniu sieci. Niekiedy uruchomienie *access-listy* na routerze może obniżyć wydajność danego węzła nawet o 40%. Właśnie z tego powodu droższe modele pozbawione są takich funkcji.

Jeśli planujemy uruchomienie w naszej sieci usługi kontroli dostępu hostów do danych fragmentów sieci i usług, powinniśmy unikać wzbogacania zakresu wykonywanych przez router operacji o filtrowanie pakietów.

Jeśli jednak dla bezpieczeństwa sieci wymagana jest kontrola w postaci filtrowania przemieszczających się pakietów, pomyślmy nad użyciem systemów i urządzeń przeznaczonych specjalnie do tego celu. Mowa tutaj oczywiście o systemach *firewall*, które dziś są już naprawdę bardzo rozwinięte. Użycie w sieci takiego rozwiązania jest korzystne mimo niewielkiego spadku jej wydajności; zwiększa możliwości konfiguracji danych węzłów oraz ewentualnego automatycznego podjęcia przez systemy *firewalli* właściwych czynności w razie wykrycia ataku.

W wielu rozwiązaniach urządzeń określanych mianem *firewalli* możemy spotkać się z informacjami, mówiącymi o rodzaju zaprogramowanych typów ataków, jakie dany *firewall* jest w stanie wykryć. Działanie takiego urządzenia wzbogacone o np. sondy sieciowe może zaowocować w postaci automatycznego generowania chociażby listu do administratora o zachodzącym, zablokowanym ataku.

Jak zawsze ocenę sensowności użycia danego rozwiązania pozostawia się projektantowi, to w jego gestii jest stwierdzenie, czy dane rozwiązanie jest faktycznie potrzebne.

Wśród przedstawianych możliwości rozwiązana danego problemu i efektów, jakie to rozwiązanie przynosi, nie zostało wymienione urządzenie określane jako koncentrator.

Taki stan jest zupełnie zamierzony. Koncentrator jako urządzenie warstwy pierwszej jest zupełnie niezdolny do kontrolowania, kierowania, zarządzania czy też ograniczania obszarów, w obrębie których dane pakiety mogą funkcjonować. Właśnie z tego powodu instalacja wewnątrz sieci rozwiązań opartych na koncentratorach przyniesie jedynie ogromny spadek wydajności, wpływając tym samym na skalowalność całej struktury.

Zastosowanie nawet wysokiej jakości koncentratora 100 Mb/s w sieci nie zagwarantuje uzyskania pożądanego pasma dla żadnego z hostów, może także przyczynić się do utraty kontroli nad sygnałami typu *brodcast*, które mogą niepotrzebnie zdominować sieć.

Z drugiej strony przy malejących kosztach przełączników należy poważnie zastanowić się nad stosunkiem niższej ceny koncentratora do wymiernego wysokiego wpływu na wydajność całego projektu.

Na tym etapie mamy już konkretną wiedzę na temat możliwości adaptacji określonego rozwiązania w stosunku do danego obszaru. Dlatego też w kolejnej fazie projektu powinniśmy zająć się omówieniem sposobu wykonania połączeń tworzących szkielet sieci.

Jak wiemy, szkielet to najważniejszy fragment obwodu każdej sieci; od jego właściwego funkcjonowania zależy końcowa wydajność całego projektu. Właśnie z tego powodu powinniśmy określić stopień transmisji, jaka może odbywać się w obrębie szkieletu. W tym celu znów musimy odwołać się do podziału, jakiego dokonaliśmy w sieci, i określić czynności, jakie będą najczęściej wykonywane w danym obszarze. Uzyskane informacje musimy oczywiście odnieść do lokalizacji zasobów, z których dane grupy hostów będą korzystały. Takie rozważenie sytuacji na pewno pozytywnie wpłynie na określenie technologii, w jakiej ma zostać wykonany szkielet. Podejście to uchroni nas również przed niemiłym zaskoczeniem, z jakim możemy się spotkać po wdrożeniu sieci, w której czynnik ten nie został uwzględniony.

Pamiętajmy także o wymogu skalowalności sieci, ponieważ wykonanie szkieletu z reguły sprowadza się do instalacji ogromnej ilości połączeń, które powinny być instalowane tylko raz. Właśnie dlatego użyjmy takiego rozwiązania, które w razie potrzeby podwyższenia ogólnej przepustowości szkieletu będzie się wiązało jedynie z wymianą urządzeń znajdujących się w centralnych punktach sieci, tworzących szkielet, bądź też po obu stronach danego połączenia sieciowego.

Wszystkie przedstawione kroki prowadzą do uzyskania czytelnego schematu sieci, który musimy wdrożyć. Jeśli wszystkie przedstawione w powyższym tekście elementy zostały poprawnie wykorzystane, możemy przystąpić do ostatniego punktu, jaki stanowi *adresowanie IP*. Niektórzy zapewne zapytają, dlaczego dopiero teraz.

Taka sytuacja wynika z wymogu uzyskania przez instalatora-projektanta dokładnego obrazu sieci, który uwzględniać będzie wszystkie istotne cechy, takie jak bezpieczeństwo, rodzaj użytych urządzeń, ochrona obszarów przed nadmiernym rozpropagowywaniem ramek. Wszystkie te i inne wcześniej wymienione właściwości muszą stwarzać czytelny, fizycznie unormowany podział sieci. Dopiero w fazie uzyskania takiej jasności sytuacji możemy przystąpić do wdrożenia odpowiedniego schematu IP. Właściwe dostosowanie adresowania IP do posiadanego i czytelnego wizerunku połączeń w sieci i ich wewnętrznych zależności nie jest już zadaniem trudnym.

Większość prac wykonanych w etapach wcześniejszych będzie nam narzucała pewne konkretne rozwiązania. Dla przykładu, instalując w sieci routery, musieliśmy kierować się potrzebą minimalizacji sieci, jej mikrosegmentacji. Jeśli właśnie takie było nasze założenie, to staje się jasne, że we wspomnianym obszarze powinniśmy użyć odpowiedniego adresowania, jakim na pewno powinno być adresowanie sieci w systemie VLSM.

Użycie takiego rozwiązania uzupełni tylko tak zwany *sprzętowy podział sieci*. Wdrożenie takiego schematu zaowocuje uzyskaniem dokładniejszej i pewniejszej możliwości kontrolowania liczby hostów przyłączonych w danym segmencie. VLSM jako technika

minimalizacji i zarządzania przestrzeniami adresowymi zapewni nam odpowiednią możliwość zaadresowana istniejącego obszaru taką ilością adresów IP, która odzwierciedli wewnętrzne potrzeby danej podsieci, a także wpłynie korzystnie na działanie i funkcjonowanie całej struktury.

Oczywiście funkcjonalna strona zaadresowanej sieci IP powinna wyrażać się w ogólnie czytelnej hierarchii dostępu. Dlatego dokonując adresowania w obszarze geograficznym sieci, musimy mieć na uwadze, które sieci mają być dostępne dla danych hostów. Pamiętajmy, że utworzenie wewnątrz obszaru sieci wielu jej segmentów czy też podsieci będzie się wiązało z przymusem użycia bram albo routerów. Z kolei duża ilość urządzeń kierujących przepływem pakietów między sieciami spowoduje zbyt duże spowolnienie sieci, na które nie możemy sobie pozwolić.

Z drugiej strony nie możemy pozwolić sobie na taką adresację IP, która sama przez się wygeneruje nam sieci o bardzo dużej liczbie hostów. Taki efekt spowoduje nadmierne obciążenie sieci, które na pewno wyrażałoby się przez próby komunikacji między hostami, ciągłe ich zanikanie czy też ogromne ilości powtórzeń, retransmisji następujących przy każdej próbie adresowania.

Integracja różnych mechanizmów sieciowych

Podczas projektowania sieci wielokrotnie będziemy mogli się spotkać z wymogiem połączenia sieci o odmiennych mechanikach. Pojęcie odmiennych mechanik sieci w tym przypadku powinno nam się kojarzyć z takimi projektami jak IEEE 802.3, czyli *Ethernet*, w stosunku do IEEE 802.5, czyli *Token Ring*.

Jeśli nasz projekt sieciowy powinien zawierać integrację tych dwóch różnych sieci i mechanik sieciowych, musimy liczyć się z przymusem zastosowania urządzeń, które pozwolą na ich połączenie oraz późniejszą wymianę danych.

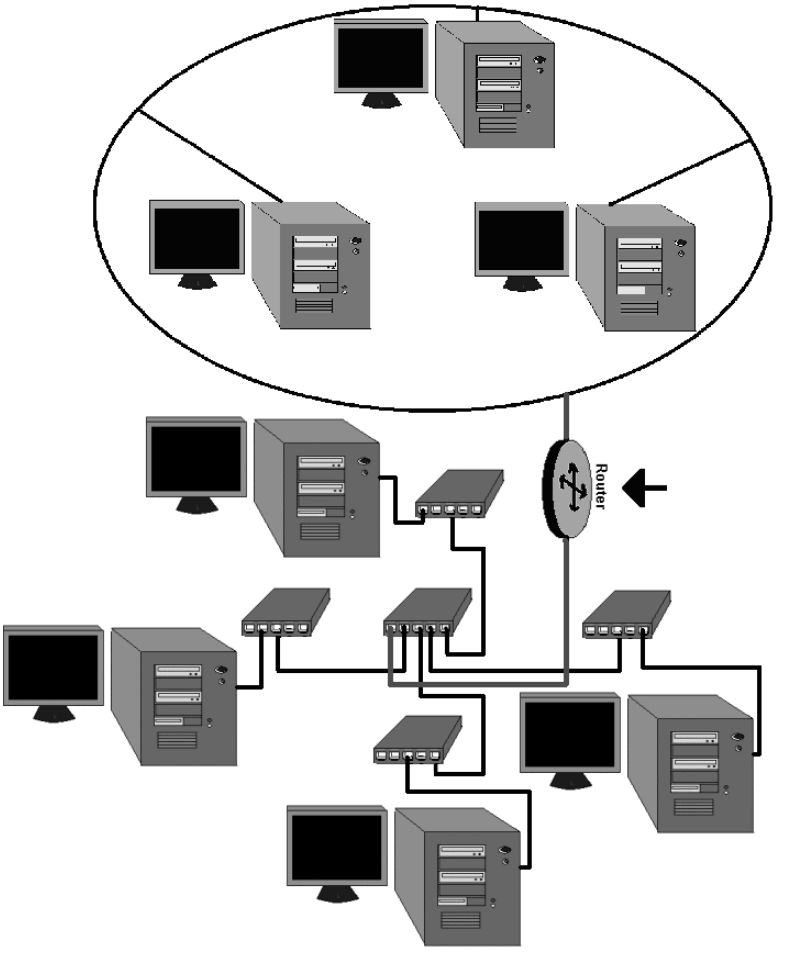
Jak wiemy z poprzednich rozdziałów, *Ethernet* i *Token Ring* obsługiwane są przez inne schematy pozwalające na wymianę danych. Mowa oczywiście o CSMA/CD w przypadku sieci *Ethernet* oraz mechanice *Token* w przypadku sieci pierścieniowej. Jak wiemy, nie ma możliwości bezpośredniego połączenia tych dwóch topologii sieci. Różnią się przecież sposobem, w jaki host może uzyskać dostęp do nadawania.

Rozwiązaniem takiej sytuacji, która z punktu widzenia funkcjonalności sieci jest mało pożądana, jest użycie routera czy też innego mostu translacyjnego. Router jako urządzenie warstwy trzeciej będzie w stanie odpowiednio pokierować trasą pakietu, tak by mógł się on poruszać pomiędzy tymi dwiema różnymi strukturami. Sytuację taką przedstawia rysunek 12.7.

Na rysunku ukazano punkt połączeniowy pomiędzy różnymi sieciami. W podanym przykładzie translacja odbywa się przy użyciu specjalnego routera.

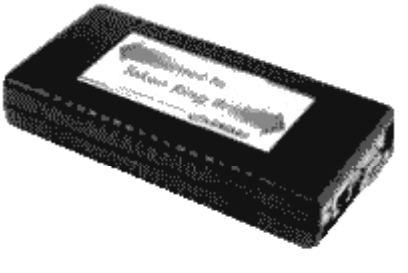
Od strony technicznej router musi zapewniać możliwość dołączenia interfejsów zarówno *Token Ring*, jak i *Ethernetu*. Tylko w ten sposób możemy uzyskać jakąkolwiek możliwość połączenia tych sieci.

Rysunek 12.7.
Integracja dwóch sieci różnych pod względem mechaniki



Oczywiście sam pomysł połączenia takich dwóch mediów można zrealizować przez specjalne mosty, takie jak ten prezentowany na rysunku 12.8.

Rysunek 12.8.
Most dla sieci Token Ring i Ethernet



Oczywiście przedstawiony sposób zrealizowania połączeń pomiędzy tymi dwiema różnymi technologiami sieciowymi nie może zostać ograniczony jedynie do zgodności na poziomie warstwy sprzętowej.

Dla poprawnej komunikacji pomiędzy tymi sieciami wymagane jest także używanie jednolitego schematu protokołów. W takiej sytuacji musimy doprowadzić do tego, by w obu sieciach używany był ten sam protokół wymiany danych.

Jeśli w większej części sieci zdecydowaliśmy się użyć protokołu klasy IPv4, to do poprawnej współpracy tych dwóch różnych obszarów również musimy użyć tego protokołu.

Takie rozwiązanie pozwoli na bezproblemowe połączenie w funkcjonalną całość zarówno *Token Ringu*, jak i *Ethernetu*.

Przedstawiając pewien schemat postępowania przy projektowaniu i późniejszej realizacji sieci, starałem się ukazać mechanizm zazębiania się różnych elementów zarówno logicznych, jak i fizycznych sieci.

Jak wielokrotnie zaznaczałem, uzyskanie odpowiedniego kształtu sieci nie jest łatwe. Jedyną pomocą w stworzeniu właściwego projektu sieci będzie rozplanowanie wszystkich wymienianych punktów z osobna i dopiero późniejsze ich konfrontowanie ze sobą. Tylko w taki sposób możemy już w fazie projektowania dostrzec pewnie „niewielkie" błędy, które mogą w tym momencie zakończyć się jedynie drobną kreślarską zmianą, redukującą ogólny koszt wdrożenia i uruchomienia sieci.

Skończony projekt sieci powinien ukazać się nam jako funkcjonalna i przemyślana forma, która swoimi rozwiązaniami technicznymi poprze swą funkcjonalność i skalowalność.

Wdrożenie sporządzonego projektu

Zakończenie czynności projektowania danej struktury sieciowej powinno zaowocować jego wdrożeniem. Przedstawiony schemat postępowania nie obejmuje swoim zakresem całego postępowania, jakie należy przeprowadzić, by projekt w całości został ukończony.

Omawiany proces przygotowania projektowania przedstawiono tak , by czytelnik mógł praktycznie wykorzystać omówione wcześniej elementy.

Aby poprawnie wykonać projekt, należy uwzględnić w nim jeszcze takie elementy, jak:

- dokładny model i funkcje, jakie może pełnić instalowany sprzęt,
- typ i rodzaj użytego okablowania,
- ilość użytego okablowania plus pozostawiony zapas,
- rodzaj użytych wtyków,
- rodzaj i typ użytych gniazd przyłączeniowych,
- typ użytych *racków*, punktów konsolidacyjnych,
- dokładne rozmieszczenie i rodzaj wykonanych połączeń,
- dokładne rozmieszczenie gniazd przyłączeniowych.

Wszystkie te dodatkowe cechy powinny znaleźć się na naszym planie, by podczas instalacji każda osoba zaangażowana w przedsięwzięcie wiedziała dokładnie, jak wykonać dany fragment instalacji, którędy poprowadzić okablowanie, jak dokonać terminacji itp.

Podczas wykonywania prac połączeniowych w obrębie okablowania typu skrętka będą nam potrzebne dokładne informacje co do sposobu, w jaki możemy wykonać połączenie w danym punkcie sieci.

Wszystkie te informacje znajdziemy w rozdziale dotyczącym okablowania sieci i rodzaju połączeń.