

**Materiały Pomocnicze do Kolokwium I
z przedmiotu Lokalne Sieci Komputerowe**

Spis treści

ORGANIZACJE USTANAWIAJĄCE STANDARDY	3
MODEL REFERENCYJNY ISO/OSI.....	4
NOŚNIKI TRANSMISJI FIZYCZNEJ	6
Nośniki przewodowe	6
Nośniki bezprzewodowe	9
ELEMENTY AKTYWNE SIECI	10
TYPY I TOPOLOGIE SIECI LAN.....	11
Typy serwerów.....	12
Typy sieci.....	13
Topologie sieci lokalnych	14
Topologie złożone	18
STANDARDY SIECI LAN.....	19
Ethernet	19
Fast Ethernet	20
Token Ring.....	21
PROTOKOŁY SIECIOWE.....	21
TCP/IP.....	22
IPX/SPX.....	24
Apple Talk	25
NetBEUI	25
SIECI BEZPRZEWODOWE.....	25
Technologie sieci bezprzewodowych.....	26
Struktury sieci WLAN.....	27
Rodzaje sieci bezprzewodowych.....	28
LITERATURA	31

Organizacje ustanawiające standardy

ANSI

Amerykański Narodowy Instytut Normalizacji (ang. ANSI - The American National Standards Institute) jest prywatną organizacją niekomercyjną. Jej misją jest ułatwianie rozwoju, koordynacji oraz publikowanie nieobligatoryjnych standardów. Organizacja ta nie wdraża aktywnie ani nie narzuca nikomu swoich standardów. Uczestniczy natomiast w pracach organizacji ustanawiających standardy globalne, takich jak IOS, IEC itp., w związku z tym niezgodność z jej standardami powoduje niezgodność ze standardami globalnymi.

IEEE

Instytut Elektryków i Elektroników (ang. IEEE - The Institute of Electrical and Electronic Engineers) jest odpowiedzialny za definiowanie i publikowanie standardów telekomunikacyjnych oraz przesyłania danych. Jego największym osiągnięciem jest zdefiniowanie standardów LAN oraz MAN. Standardy te tworzą wielki i skomplikowany zbiór norm technicznych, ogólnie określany jako "Project 802" lub jako seria standardów 802. Celem IEEE jest tworzenie norm, które byłyby akceptowane przez instytut ANSI. Akceptacja taka zwiększyłaby ich forum dzięki uczestnictwu ANSI w globalnych organizacjach określających standardy.

ISO

Międzynarodowa Agencja Normalizacyjna (ang. ISO - International Organization for Standardization) została utworzona w 1946 roku w Szwajcarii, w Genewie. ISO jest niezależnym podmiotem wynajętym przez Organizację Narodów Zjednoczonych do określania standardów międzynarodowych. Zakres jej działania obejmuje praktycznie wszystkie dziedziny wiedzy ludzkiej, poza elektryką i elektroniką. Aktualnie ISO składa się z ponad 90 różnych organizacji standardo-dawczych z siedzibami na całym świecie. Najważniejszym standardem opracowanym przez ISO jest Model Referencyjny Połączonych Systemów Otwartych, czyli model OSI.

IEC

Międzynarodowa Komisja Elektrotechniczna (ang. IEC - International Electrotechnical Commission), z siedzibą również w Genewie, została założona w 1909 roku. Komisja IEC ustanawia międzynarodowe standardy dotyczące wszelkich zagadnień elektrycznych i elektronicznych. Aktualnie w jej skład wchodzi 40 państw. W Stanach Zjednoczonych Instytut ANSI reprezentuje zarówno IEC, jak i ISO. IEC oraz ISO dostrzegły, że technologie informatyczne stanowią potencjalny obszar zazębiania się ich kompetencji; w celu określenia standardów dla technologii informatycznych utworzyły, więc Połączony Komitet Techniczny (ang. JTC - Joint Technical Committee).

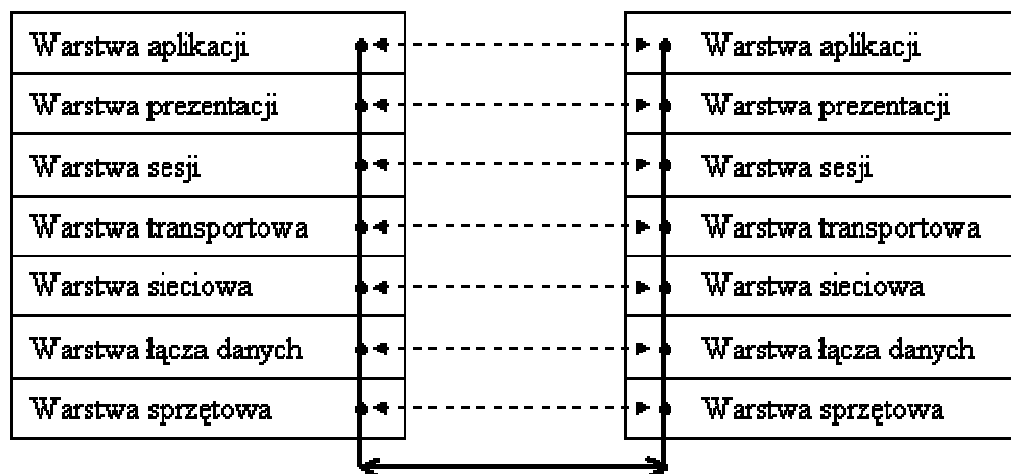
IAB

Komisja Architektury Internetu (ang. IAB - Internet Architecture Board) zarządza techniczną stroną rozwoju sieci Internet. Składa się z dwóch komisji roboczych: Grupy Roboczej ds. Technicznych Internetu oraz z Grupy Roboczej ds. Naukowych Internetu. Grupy te są odpowiedzialne za ustanawianie standardów technicznych dla Internetu, jak również nowych standardów, takich jak protokół Internetu IP.

Model referencyjny ISO/OSI

W 1977 roku „Międzynarodowa Organizacja Normalizacyjna” opracowała wzorcowy „Model łączenia systemów otwartych”. Ideą przyświecającą tym działaniom, było umożliwienie współdziałania ze sobą produktów pochodzących od różnych producentów. Proces komunikacji został podzielony na 7 etapów, zwanych warstwami, ze względu na sposób przechodzenia pomiędzy nimi informacji. Często struktura tworzona przez warstwy OSI nazywana jest stosem protokołów wymiany danych. W złożonym zagadnieniu komunikacji wyodrębnia się pewne niezależne zadania, które mogą być rozwiązywane przez wydzielone układy sprzętowe lub pakiety oprogramowania zwane obiektami. Klasę obiektów rozwiązujących dane zagadnienie nazywa się warstwą. Pojęcie warstwy nie jest jednoznaczne z pojęciem protokołu – funkcje danej warstwy mogą być wykonywane przez kilka różnych protokołów. Każdy protokół komunikuje się ze swoim odpowiednikiem, będącym implementacją tego samego protokołu w równorzędnej warstwie komunikacyjnej systemu odległego. Warstwy (a dokładnie konkretne protokoły zawarte w tej warstwie) komunikują się bezpośrednio z odpowiadającymi im warstwami w odległym hoście. Należy więc też zapewnić reguły przekazywania informacji w dół do kolejnych warstw pracujących na danym komputerze. Dane przekazywane są od wierzchołka stosu, poprzez kolejne warstwy, aż do warstwy fizycznej, która przesyła je przez sieć do odległego hosta. Na szczycie stosu znajdują się usługi świadczone bezpośrednio użytkownikowi przez aplikacje sieciowe, na spodzie – sprzęt realizujący transmisję sygnałów niosących informacje.

Każda kolejna warstwa musi jedynie znać format danych wymagany do komunikacji poprzez warstwę niższą zwany protokołem wymiany danych. Przy przechodzeniu do warstwy niższej dana warstwa dokleja do otrzymanych przez siebie danych nagłówek z informacjami dla swojego odpowiednika na odległym hoście. W ten sposób kolejne warstwy nie ingerują w dane otrzymane z warstwy poprzedniej. Przy odbieraniu danych z warstwy niższej, dana warstwa interpretuje ten nagłówek „doklejony” poprzez swojego odpowiednika i jeśli zachodzi potrzeba przekazania danych do warstwy wyższej, usuwa swój nagłówek i przekazuje dane dalej.



Rys.1. Transmisja danych pomiędzy kolejnymi warstwami ISO/OSI.

Warstwa fizyczna (*physical layer*)

Zapewnia transmisję danych pomiędzy węzłami sieci. Definiuje interfejsy sieciowe i medium transmisji. Określa m.in. sposób połączenia mechanicznego (wtyczki, złącza), elektrycznego (poziomy napięcie, prądów), standard fizycznej transmisji danych. W skład jej obiektów wchodzi min.: przewody, karty sieciowe, modemy, wzmacniaki, koncentratory.

Warstwa łącza danych (*data link layer*)

Zapewnia niezawodność łącza danych. Definiuje mechanizmy kontroli błędów w przesyłanych ramach lub pakietach. Jest ona ściśle powiązana z warstwą fizyczną, która narzuca topologię. Warstwa ta często zajmuje się również kompresją danych. W skład jej obiektów wchodzi sterowniki urządzeń sieciowych, np.: sterowniki (*drivery*) kart sieciowych oraz mosty (*bridge*) i przełączniki (*switche*).

Warstwa sieciowa (*network layer*)

Zapewnia metody ustanawiania, utrzymywania i rozłączania połączenia sieciowego. Obsługuje błędy komunikacji. Ponadto jest odpowiedzialna za trasowanie (*routing*) pakietów w sieci, czyli wyznaczenie optymalnej trasy dla połączenia. W niektórych warunkach dopuszczalne jest gubienie pakietów przez tę warstwę. W skład jej obiektów wchodzi min.: routery (*routery*).

Warstwa transportowa (*transport layer*)

Zapewnia przezroczysty transfer danych typu *point-to-point*. Dba o kolejność pakietów otrzymywanych przez odbiorcę. Sprawdza poprawność (CRC) przesyłanych pakietów i w przypadku ich uszkodzenia lub zaginięcia, zapewnia ich retransmisję. Powyżej tej warstwy dane mogą być traktowane jako strumień.

Warstwa sesji (*session layer*)

Zapewnia aplikacjom na odległych komputerach realizację wymiany danych pomiędzy nimi. Kontroluje nawiązywanie i zrywanie połączenia przez aplikację. Jest odpowiedzialna za poprawną realizację zapytania o daną usługę. Do warstwy tej można zaliczyć funkcje API udostępniane programiście przez bibliotekę realizującą dostęp do sieci na poziomie powyżej warstwy transportowej takie jak np. biblioteka strumieni i gniazdek BSD.

Warstwa prezentacji (*presentation layer*)

Zapewnia tłumaczenie danych, definiowanie ich formatu oraz odpowiednią składnię. Umożliwia przekształcenie danych na postać standardową, niezależną od aplikacji. Rozwiązuje takie problemy jak niezgodność reprezentacji liczb, znaków końca wiersza, liter narodowych itp. Odpowiada także za kompresję i szyfrowanie.

Warstwa aplikacji (*application layer*)

Zapewnia aplikacjom metody dostępu do środowiska OSI. Warstwa ta świadczy usługi końcowe dla aplikacji, min.: udostępnianie zasobów (plików, drukarek). Na tym poziomie rezydują procesy sieciowe dostępne bezpośrednio dla użytkownika.

Nośniki transmisji fizycznej

Na nośniki transmisji składają się wszelkie sposoby przesyłania sygnałów generowanych przez mechanizmy warstwy pierwszej modelu OSI. Ze względu na definicję nośniki możemy podzielić na materialne i niematerialne. Ich wybór opiera się o kilka cech, które należy rozważyć projektując sieć:

- wymagania szerokości pasma aplikacji i użytkownika,
- perspektywy rozwoju sieci,
- odległości między systemami komputerów,
- środowisko geograficzne (kabel, transmisja radiowa lub satelitarna),
- wymagana tolerancja błędów
- środowisko – rodzaj i moc zakłóceń generowanych przez otoczenie,
- cena.

Nośniki przewodowe

Kabel koncentryczny

Kabel koncentryczny składa się z dwóch współosiowych przewodów. Najczęściej spotykany rodzaj kabla koncentrycznego składa się z pojedynczego przewodu miedzianego biegnącego w materiale izolacyjnym. Izolator jest otoczony innym cylindrycznie biegnącym przewodnikiem, którym może być przewód lity lub pleciony, otoczony z kolei następną warstwą izolacyjną. Całość osłonięta jest koszulką ochronną z polichlorku winylu. Wyróżniamy dwa rodzaje tego kabla 10Base-5 i 10Base-2.

Przepustowość kabla koncentrycznego:

- 10Base-5 (gruby)-10 Mb/s (500m)
- 10Base-2 (cienki)-10 Mb/s (185m)

Zalety:

- ze względu na posiadaną ekranizację, jest mało wrażliwy na zakłócenia i szumy,
- jest tańszy niż ekranowany kabel skręcany,
- posiada twardą osłonę, dzięki czemu jest bardziej odporny na uszkodzenia fizyczne.

Wady:

- ograniczenie szybkości do 10Mbit,
- niewygodny sposób instalacji (duże łącza, łączki T, duża grubość),
- słaba skalowalność (problemy z dołączeniem nowego komputera),
- trudności przy lokalizowaniu usterki.

Dziś zastosowanie koncentryków ogranicza się do przesyłania sygnałów szerokopasmowych telewizji kablowych.

Skrętka dwużyłowa

Skrętka dwużyłowa składa się z dwóch dość cienkich przewodów o średnicy od 0,4 do 0,9mm każdy. Przewody pokryte są cienką warstwą polichloru winylu i splecione razem. Skręcenie to równoważy promieniowanie na jakie wystawiony jest każdy z dwóch przewodów znosząc w ten sposób zakłócenia elektromagnetyczne.

Dwoma najczęściej stosowanymi rodzajami skrętek ośmiożyłowych są ekranowana i nie ekranowana. Skrętka ekranowana STP ma dodatkową warstwę folii lub metalowego przewodu oplatającego przewody. Powodem wprowadzenia ekranowania było ograniczenie do minimum wpływu na jakość transmisji zakłóceń częstotliwościami radiowymi i elektromagnetycznymi. W praktyce ekranowanie chroni przed promieniowaniem zewnętrznym, niestety zatrzymuje również promieniowanie indukowane, które odbite od ekranu powraca do przewodu miedzianego, co może, z dużym prawdopodobieństwem, powodować uszkodzenie sygnału. Skrętka ośmiożyłowa nieekranowana UTP ma przewody podzielone na cztery grupy po dwa przewody. Każda para składa się z przewodu dodatniego i ujemnego i obsługuje tylko jedno zadanie przykładowo wysyłanie gdzie inna w tym czasie odbiera sygnał. Pozostałe pary w większości sieci lokalnych nie są używane (wyjątkiem jest przesyłanie sygnału z prędkością 100Mbps i większą gdzie wykorzystane są wszystkie pary). Przepustowość skrętki zależna jest od jej kategorii.

Skrętka:

- kategorii 1 to kabel telefoniczny
- kategorii 2 do 4 Mb/s,
- kategorii 3 do 10 Mb/s,
- kategorii 4 do 16 Mb/s,
- kategorii 5 do 100 Mb/s,
- kategorii 6 do 622 Mb/s.

Zalety:

- jest najtańszym medium transmisji,
- wysoka prędkość transmisji (do 1000Gb/s),
- łatwe diagnozowanie uszkodzeń,
- łatwa instalacja,
- odporność na poważne awarie,
- jest akceptowana przez wiele rodzajów sieci.

Wady:

- niższa długość odcinka kabla niż w innych mediach stosowanych w Internecie,
- mała odporność na zakłócenia (skrętki nie ekranowanej),
- niska odporność na uszkodzenia mechaniczne.

Kabel światłowodowy

Obecnie najnowocześniejszym medium transmisyjnym jest światłowód. Zasada jego działania opiera się na transmisji impulsów świetlnych między nadajnikiem przekształcającym sygnały elektryczne na świetlne, a odbiornikiem przekształcającym sygnały świetlne odebrane ze światłowodu w sygnały elektryczne. Dostępne są w wielu kształtach, rozmiarach i kategoriach długości fal. Nośnikiem w kablu światłowodowym jest szkło, ale równie dobrze może nim być optycznej jakości plastik, jego średnica waha się od 5 mikronów do rozmiarów, które cokolwiek łatwiej dostrzec gołym okiem. Wyróżniamy dwa rodzaje światłowodów wielomodowe i jednomodowe. Światłowód wielomodowy charakteryzuje się tym, że promień światła może być wprowadzony do niego pod różnymi kątami – modami. Oznaczeniem najczęściej w sieciach LAN stosowanego włókna szklanego jest 62,5/125 gdzie pierwsza podaje średnicę rdzenia a druga średnicę płaszczka ochronnego w mikronach.

W światłowodzie jednomodowym rdzeń złożony jest z wielu warstw o różnych współczynnikach załamania. Dodatkową różnicą jest zmniejszenie średnicy rdzenia do 9nm. Dzięki temu w światłowodzie propagowany jest tylko jeden mod. Nie istnieje zjawisko całkowitego odbicia wewnętrznego na granicy rdzenia i płaszczka. Zwiększona została również częstotliwość pracy takiego włókna, co poszerza pasmo pracy sieci. Niestety koszt takiego światłowodu jest znacznie wyższy niż światłowodu wielomodowego, a dodatkowo instalacja

wymaga o wiele większej precyzji przy wprowadzaniu promienia świetlnego (diody laserowe) do rdzenia. Kable światłowodowe wykorzystywane są parami jeden służy do wysyłania sygnałów a drugi do ich odbioru. Ich zastosowanie w sieciach LAN zwykle ogranicza się do łączenia serwerów i koncentratorów. Przepustowość kabli światłowodowych może sięgać 3Tb/s.

Zalety:

- bardzo duża prędkość transmisji,
- daleki zasięg sygnału bez konieczności wzmacniania,
- dużo większa pojemność łącza w porównaniu z przewodem miedzianym.

Wady:

- w przypadku uszkodzenia włókna miejsce to jest trudne do wykrycia,
- wymaga użycia specjalistycznego sprzętu w przypadku instalacji i naprawy usterki.

Nośniki bezprzewodowe

Radio

Fale elektromagnetyczne mogą być wykorzystywane nie tylko do nadawania programów telewizyjnych i radiowych, ale i do transmisji danych komputerowych. Nieformalnie o sieci, która korzysta z elektromagnetycznych fali radiowych, mówi się że działa na falach radiowych, a transmisję określa się transmisją radiową. Sieci takie nie wymagają bezpośredniego fizycznego połączenia między komputerami. W zamian za to każdy uczestniczący w łączności komputer jest podłączony do anteny, która zarówno nadaje, jak i odbiera fale. Anteny używane w sieciach mogą być duże lub małe w zależności od żądanego zasięgu. Antena zaprojektowana na przykład do metalowego słupka o długości 2 m zainstalowanego na dachu. Antena umożliwia komunikację wewnątrz budynku może być tak mała, że zmieści się wewnątrz przenośnego komputera (tzn. mniejsza niż 20 cm).

Mikrofale

Do przekazywania informacji może być również używane promieniowanie elektromagnetyczne o częstotliwościach spoza zakresu wykorzystywanego w radio i telewizji. W szczególności w telefonii komórkowej używa się mikrofal do przenoszenia rozmów telefonicznych. Kilka dużych koncernów zainstalowało systemy komunikacji mikrofalowej jako części swoich sieci. Mikrofałe, chociaż są to fale o wyższej częstotliwości niż fale radiowe, zachowują się inaczej. Zamiast nadawania we wszystkich kierunkach mamy w tym przypadku możliwość ukierunkowania transmisji, co zabezpiecza przed odebraniem sygnału przez innych. Dodatkowo za pomocą transmisji mikrofalowej można przenieść więcej informacji niż za pomocą transmisji radiowej o mniejszej częstotliwości. Jednak, ponieważ mikrofałe nie przechodzą

przez struktury metalowe, transmisja taka działa najlepiej, gdy mamy „czystą” drogę między nadajnikiem a odbiornikiem. W związku z tym większość instalacji mikrofalowych składa się z dwóch wież wyższych od otaczających budynków i roślinności, na każdej z nich jest zainstalowany nadajnik skierowany bezpośrednio w kierunku odbiornika na drugiej.

Podczerwień

Bezprzewodowe zdalne sterowniki używane w urządzeniach takich jak telewizory czy wieże stereo komunikują się za pomocą transmisji w podczerwieni. Taka transmisja jest ograniczona do małej przestrzeni i zwykle wymaga, aby nadajnik był nakierowany na odbiornik. Sprzęt wykorzystujący podczerwień jest w porównaniu z innymi urządzeniami nie drogi i nie wymaga anteny. Transmisja w podczerwieni może być użyta w sieciach komputerowych do przenoszenia danych. Możliwe jest na przykład wyposażenie dużego pokoju w pojedyncze połączenia na podczerwień, które zapewnia dostęp sieciowy do wszystkich komputerów w pomieszczeniu. Komputery będą połączone siecią podczas przemieszczania ich w ramach tego pomieszczenia. Sieci oparte na podczerwieni są szczególnie wygodne w przypadku małych, przenośnych komputerów.

Światło laserowe

Wspomniano już, że światło może zostać użyte do komunikacji poprzez światłowody. Promień światła może być również użyty do przenoszenia danych powietrzem. W połączeniu wykorzystującym światło są dwa punkty – w każdym znajduje się nadajnik i odbiornik. Sprzęt ten jest zamontowany w stałej pozycji, zwykle na wieży, i ustawiony tak, że nadajnik w jednym miejscu wysyła promień światła dokładnie do odbiornika w drugim. Nadajnik wykorzystuje laser do generowania promienia świetlnego gdyż jego światło pozostaje skupione na długich dystansach. Światło lasera podobnie jak mikrofałe porusza się po linii prostej i nie może być przesłaniane. Niestety promień lasera nie przenika przez roślinność. Tłumią go również śnieg i mgła. To powoduje, że transmisje laserowe mają ograniczone zastosowanie.

Elementy aktywne sieci

Każda sieć musi posiadać elementy aktywne (tzw. urządzenia sieciowe). Jak już napisałem powyżej służą one do wysyłania, przesyłania, wzmacniania, modyfikowania danych „wędrujących” po sieci.

Karta sieciowa (NIC - Network Interface Card)

Jest to urządzenie łączące komputer z siecią komputerową zawierające dwa interfejsy - jeden, do połączenia z siecią i drugi interfejs, do połączenia z komputerem. Obecnie produkowane karty sieciowe mają wbudowany własny

procesor, co umożliwia przetwarzanie niektórych danych bez angażowania głównego procesora oraz własną pamięć RAM, która pełni rolę bufora w przypadku, gdy karta nie jest w stanie przetworzyć napływających z dużą szybkością danych. Karta posiada dwa interfejsy wyjściowe: UTP i BNC (nigdy nie mogą one działać równocześnie). Rozróżnia się również karty 10 i 100Mb; te drugie są to z oczywistych względów karty UTP.

Koncentrator (HUB)

Koncentrator jest jednym z urządzeń najczęściej spotykanych w sieciach. Do niego właśnie podłączane są wszystkie kable biegnące od komputerów. Działa jak urządzenie wzmacniające i rozsyłające sygnały ze stacji sieciowych. Nie bada otrzymanej informacji tylko przekazuje ją dalej. Sygnał wysłany przez komputer dociera do koncentratora, który przesyła go dalej przez wszystkie swoje porty (gniazda). Jest to wada, ponieważ informacja wejściowa, aby dotrzeć do celu, zostaje rozproszona po całej sieci, powodując dużo niepotrzebnego ruchu.

Przełącznik (switch)

Przełączniki są zbliżone wyglądem do koncentratorów. W przeciwieństwie do nich analizują otrzymane ramki, aby kontrolować ruch w sieci. „Uczą się”, do którego z portów podłączeni są adresaci informacji, a następnie kierują przesyłanie danych wyłącznie do wskazanych odbiorców. Stosowanie ich w sieci poważnie ogranicza niepotrzebny ruch, gdyż dane nie są rozsyłane do wszystkich portów urządzenia.

Router (brama, gateway)

Router stosowany jest zarówno w sieciach LAN jak i WAN. Routery lokalne używane są wtedy gdy chcemy umożliwić przesyłanie pakietów pomiędzy dwoma lub więcej segmentami sieci (podsieciami). Normalnie przesyłanie danych jest niemożliwe, ponieważ obie podsieci mają różne adresy. Jedną dużą sieć dzieli się na kilka podsieci głównie po to by zmniejszyć domenę kolizji. Jak widać zastosowanie routera spowoduje zwiększenie przepustowości sieci. Zadaniem routera dostępowego jest umożliwienie komunikacji pomiędzy siecią LAN, a WAN.

Typy i topologie sieci LAN

Niezbędnym warunkiem wstępnym podziału sieci lokalnych na warstwy jest poznanie dwóch jej atrybutów; metodologii dostępu do sieci oraz topologii sieci. Metodologia dostępu do zasobów sieci LAN opisuje sposób udostępniania zasobów przyłączonych do sieci. Ten aspekt sieci często decyduje o jej typie. Natomiast topologia sieci LAN odnosi się do sposobu organizacji koncentratorów i okablowania.

Typy serwerów

Najbardziej powszechnymi urządzeniami podstawowymi przyłączonymi do sieci LAN są: klienci, serwer oraz drukarki. Urządzeniem podstawowym jest takie urządzenie, które może uzyskać bezpośredni dostęp do innych urządzeń lub umożliwić innym urządzeniom dostęp do siebie. Serwer to dowolny komputer przyłączony do sieci LAN, zawiera zasoby udostępniane innym urządzeniom przyłączonym do tej sieci. Klient to natomiast dowolny komputer który za pomocą sieci uzyskuje dostęp do zasobów umieszczonych na serwerze. Drukarki są oczywiście urządzeniami wyjścia tworzącymi wydruki zawartości plików.

Serwery plików

Serwer plików jest scentralizowanym mechanizmem składowania plików z których mogą korzystać grupy użytkowników. Nie wszystkie pliki jednak nadają się do przechowywania w serwerze plików. Pliki prywatne, zastrzeżone i nie nadające się do użycia przez osoby korzystające z sieci najlepiej pozostawić na lokalnym dysku twardym.

Zalety:

- centralna lokalizacja magazynu współdzielonych plików,
- możliwość wprowadzenia wielu technik pozwalających na ochronę danych przed zakłóceniami w dostawach prądu elektrycznego,
- zorganizowany archiwizowanie danych,
- znacznie większa wydajność odczytywania plików niż w zwykłym komputerze.

Serwery wydruków

Serwery mogą być również używane do współdzielenia drukarek przez użytkowników sieci lokalnej. Jediną funkcją serwerów wydruków jest przyjmowanie żądań wydruków ze wszystkich urządzeń sieci, ustawienie ich w kolejki i wysłanie ich do odpowiedniej drukarki. Każda drukarka przyłączona do serwera wydruków ma swoją własną listę kolejności. Żądania zwykle przetwarzane są w kolejności w jakiej zostały otrzymane.

Serwery aplikacji

Równie często serwery służą jako centralne składy oprogramowania użytkowego. Serwer aplikacji jest miejscem w którym znajdują się wykonywalne programy użytkowe. Aby móc uruchomić określony program, klient musi

nawiązać połączenie z takim serwerem. Aplikacja jest następnie uruchamiana, ale nie na komputerze-kliencie, lecz na serwerze, następnie pobieranie kopii programów do uruchomienia na komputerach lokalnych umożliwia serwery plików. Serwery aplikacji umożliwiają organizacji zmniejszenie kosztów zakupu oprogramowania użytkowego.

Typy sieci

Typ sieci opisuje sposób, w jaki przyłączone do sieci zasoby są udostępniane. Zasobami mogą być klienci, serwery lub inne urządzenia, pliki itd., które do klienta lub serwera są przyłączone. Zasoby te udostępniane są na jeden z dwóch sposobów: równorzędny i serwerowy.

Sieci równorzędne (każdy-z-każdym)

Sieci typu każdy-z-każdym obejmuje nie ustrukturalizowany dostęp do zasobów sieci. Każde urządzenie z tego typu sieci może być jednocześnie klientem, jak i serwerem. Wszystkie urządzenia takiej sieci są zdolne do bezpośredniego pobierania danych, programów i innych zasobów. Innymi słowy, każdy komputer pracujący w takiej sieci jest równorzędny w stosunku do każdego innego – w sieciach tego typu nie ma hierarchii. Sieci tego typu najczęściej znajdują zastosowanie w małych instytucjach o ograniczonej technologii informatycznej i małymi potrzebami współdzielenia informacji.

Zalety:

- łatwe do wdrożenia jak również w obsłudze,
- tanie w eksploatacji,
- mogą być ustanowione przy wykorzystaniu prostych systemów operacyjnych,
- odporne na błędy i przekłamania.

Wady:

- użytkownicy muszą pamiętać wiele haseł,
- brak centralnego składu zasobów,
- brak centralnej jednostki odpowiedzialnej za utrzymanie konwencji korzystania z zasobów.

Sieci oparte na serwerach (klient- serwer)

W sieciach tych zasoby często udostępnione gromadzone są w komputerach odrębnej warstwy zwanych serwerami. Serwery zwykle nie mają użytkowników bezpośrednich. Są one raczej komputerami wielodostępnymi, które regulują udostępnianie swoich zasobów szerokiej rzeszy klientów. W sieciach tego typu z klientów zdjęty jest ciężar funkcjonowania jako serwery wobec innych klientów. Wiele jest korzyści płynących z opartego na serwerach

podejścia do współdzielenia zasobów sieci. Korzyści te bezpośrednio odpowiadają ograniczeniom sieci każdy-z-każdym. Obszarami, w których zastosowanie serwer-klient przynosi korzyści, są więc bezpieczeństwo, wydajność oraz administracja. Sieci oparte na serwerach są bardzo przydatne, zwłaszcza w organizacjach dużych oraz wymagających zwiększonego bezpieczeństwa i bardziej konsekwentnego zarządzania zasobami przyłączonymi do sieci. Koszty dodane sieci opartych na serwerach mogą jednak przesunąć je poza zasięg możliwości finansowych małych organizacji.

Zalety:

- sieci te są dużo bezpieczniejsze niż sieci równorzędne,
- duża wydajność sieci,
- w prosty sposób można zmienić rozmiary sieci.

Wady:

- instalacja i obsługa wymaga znacznych nakładów finansowych.

Sieci mieszane

Obecnie standardowo zakładane są sieci będące mieszanką sieci równorzędnych (każdy z każdym) i serwerowych (opartych na serwerze). Przykładem tego rodzaju sieci jest sieć o architekturze serwerowej grupującej centralnie zasoby, które powinny być ogólnodostępne. W ramach takiej organizacji sieci, udostępnianie zasobów wewnątrz lokalnych grup roboczych może nadal odbywać się na zasadzie dostępu równorzędnego.

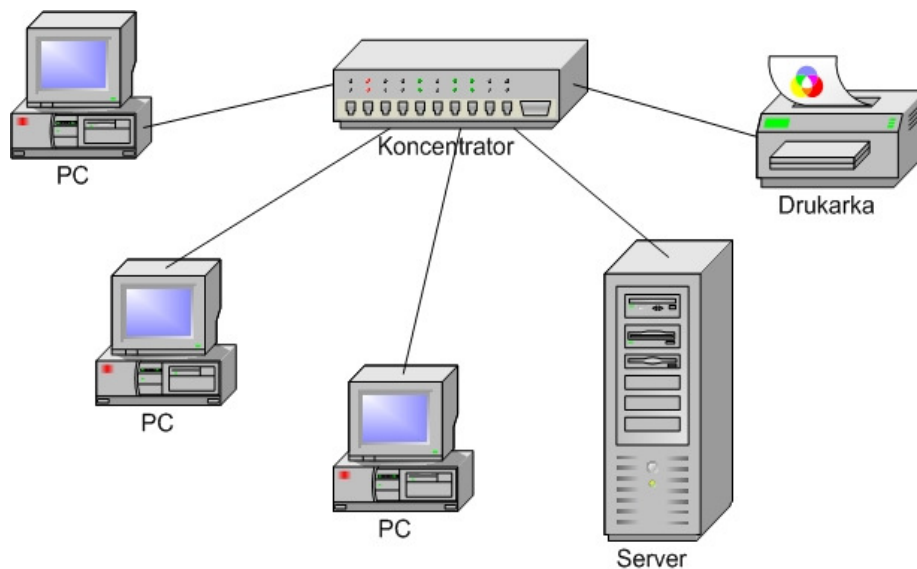
Topologie sieci lokalnych

Topologie sieci LAN mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. Topologia fizyczna określa geometryczną organizację sieci lokalnych. Topologia logiczna opisuje wszelkie możliwe połączenia między parami mogącymi się komunikować punktów końcowych sieci. Za jej pomocą opisywać można, które punkty końcowe mogą się komunikować z innymi, a także ilustrować, które z takich par mają wzajemne, bezpośrednie połączenie fizyczne.

Topologia gwiazdy

Połączenia sieci LAN o topologii gwiazdy z przyłączonymi do niej urządzeniami rozchodzą się z jednego, wspólnego punktu, którym jest koncentrator (HUB) okablowanie całej sieci w tym przypadku opiera się na skrzętce cztero parowej i kart sieciowych z wyjściem na UTP co przedstawia poniższy rysunek. Odległości pomiędzy komputerami a koncentratorom nie powinny przekraczać odległości 100 metrów. W bardzo łatwy sposób można połączyć dwie takie sieci o topologii gwiazdy, wystarczy połączyć koncentratory

odpowiednim przewodem (UTP, BNC), w zależności od modelu koncentratora łączymy je za pomocą przewodu koncentrycznego lub „skrętki” (gniazdo to nazywa się UPLINK). Odmienne niż w topologiach pierścienia - tak fizycznej, jak i wirtualnej - każde urządzenie przyłączone do sieci w topologii gwiazdy może uzyskiwać bezpośredni i niezależny od innych urządzeń dostęp do nośnika. W tym celu urządzenia te muszą współdzielić dostępne szerokości pasma koncentratora. Przykładem sieci LAN o topologii gwiazdy jest 10BaseT Ethernet. Połączenia w sieci LAN o małych rozmiarach i topologii gwiazdy rozchodzą się z jednego wspólnego punktu. Każde urządzenie przyłączone do takiej sieci może inicjować dostęp do nośnika niezależnie od innych przyłączonych urządzeń. Topologie gwiazdy stały się dominującym we współczesnych sieciach LAN rodzajem topologii. Są one elastyczne i stosunkowo tanie w porównaniu z bardziej skomplikowanymi sieciami LAN o ściśle regulowanych metodach dostępu.



Rys. 2. Topologia gwiazdy

Zalety:

- łatwy do modyfikacji układ kabli,
- możliwość dodawania nowych stacji roboczych,
- łatwa kontrola i likwidację problemów.

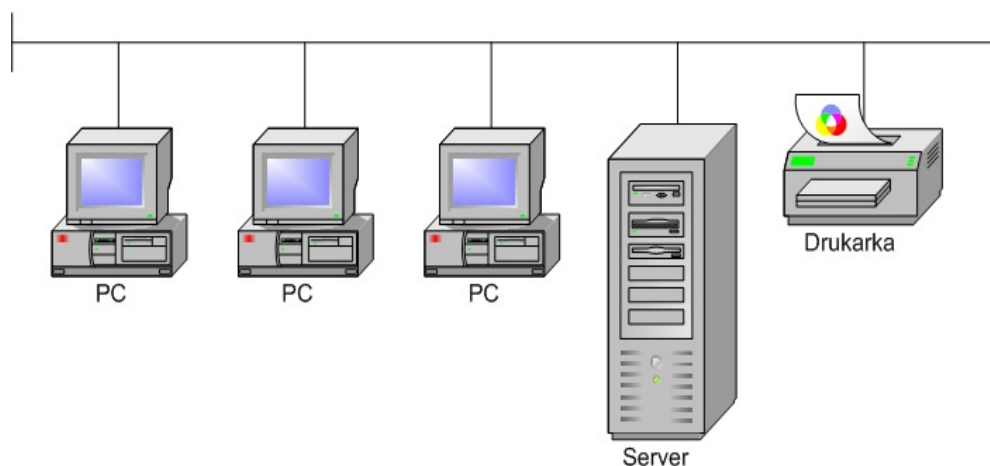
Wady:

- duża ilość kabli,
- wzrost ceny ze względu na konieczność zastosowania dłuższego kabla.

Topologia magistrali

Topologię magistrali (szyna, bus) wyróżnia to, że wszystkie węzły sieci połączone są ze sobą za pomocą pojedynczego, otwartego (czyli umożliwiającego przyłączanie kolejnych urządzeń) kabla. Kabel taki obsługuje

tylko jeden kanał i nosi nazwę magistrali. Niektóre technologie oparte na magistrali korzystają z więcej niż jednego kabla, dzięki czemu obsługiwać mogą więcej niż jeden kanał, mimo że każdy z kabli obsługuje niezmiennie tylko jeden kanał transmisyjny. Oba końce magistrali muszą być zakończone opornikami ograniczającymi, zwanymi również często terminatorami. Oporniki te chronią przed odbiciami sygnału. Zawsze gdy komputer wysyła sygnał, rozchodzi się on w przewodzie automatycznie w obu kierunkach. Jeśli sygnał nie napotka na swojej drodze terminatora, to dochodzi do końca magistrali, gdzie zmienia kierunek biegu. W takiej sytuacji pojedyncza transmisja może całkowicie zapisać wszystkie dostępne szerokości pasma i umożliwić wysyłanie sygnałów pozostałym komputerom przyłączonym do sieci. Przykładową topologię magistrali przedstawia ten rysunek. Typowa magistrala składa się z pojedynczego kabla łączącego wszystkie węzły w sposób charakterystyczny dla sieci równorzędnej, długość sieci w tej topologii nie powinna przekroczyć odległości 185 m (licząc od jednego terminatora do drugiego). Brak jakichkolwiek urządzeń zewnętrznych, w tym wzmacniaków, sprawia, że magistrale sieci lokalnych są proste i niedrogie. Jest to również przyczyną ograniczeń dotyczących odległości, funkcjonalności i skalowalności sieci. Topologia ta jest więc stosowana praktyczna jedynie dla najmniejszych sieci LAN. Wobec tego obecnie dostępne sieci lokalne o topologii magistrali są tanimi sieciami równorzędnymi udostępniającymi podstawowe funkcje współdziałania sieciowego. Topologie te są przeznaczone przede wszystkim do użytku w domach i małych biurach.



Rys. 3. Topologia magistrali

Zalety:

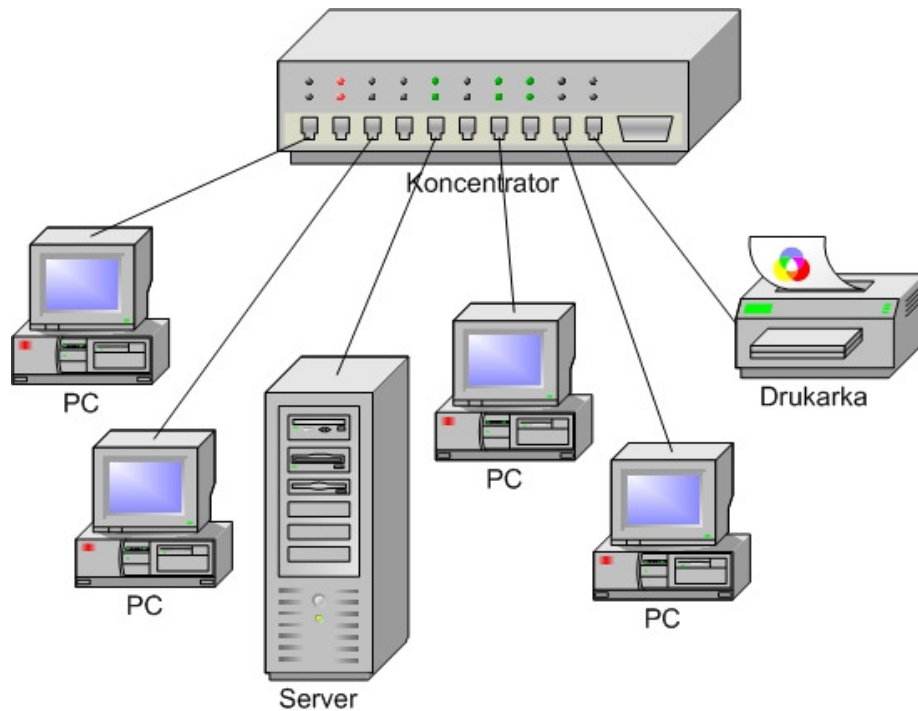
- wymaga najmniejszej ilości kabli,
- prosty układ okablowania,
- niezawodna.

Wady:

- trudna diagnostyka i lokalizacja błędów,
- przy dużym ruchu w sieci możliwe opóźnienia.

Topologia przełączana

Budowa i funkcjonowanie tego typu topologii opiera się na koncentratorze przełączającym (switch). Każdy port oraz urządzenie, które jest doń przyłączone, ma własną dedykowaną szerokość pasma. Choć pierwotnie przełączniki przesyłały dalej ramki na podstawie ich adresów fizycznych, to postęp technologiczny szybko zmienia ten stan rzeczy. Obecnie dostępne są przełączniki, które potrafią przetwarzać komórki, ramki, a nawet pakiety używające adresów warstwy 3, takie jak protokół IP. Przełączniki poprawiają sprawność sieci LAN na dwa sposoby. Pierwszy polega na zwiększaniu szerokości pasma dostępnego w sieci. Na przykład, przełączany koncentrator Ethernetu o 8 portach zawiera 8 odrębnych domen kolizji, z których każda przesyła dane z prędkością 10 Mbps, co daje łączną szerokość pasma rzędu 80 Mbps. Drugi sposób zwiększania sprawności przełączanych sieci LAN polega na zmniejszaniu liczby urządzeń, wymuszających udostępnianie wszystkich segmentów pasma szerokości. Każda przełączana domena kolizji składa się jedynie z dwóch urządzeń : urządzenia sieciowego oraz portu koncentratora przełączanego, z którym urządzenie to jest połączone. Wyłącznie te dwa urządzenia mogą rywalizować o szerokość pasma 10 Mbps w segmencie, w którym się znajdują. W sieciach, które nie korzystają z metody dostępu do nośnika na zasadzie rywalizacji o szerokość pasma – takich jak Token Ring lub FDDI – tokeny krążą między dużo mniejszą liczbą urządzeń sieciowych niż ma to zwykle miejsce w sieciach o dostępie opartym na zasadzie rywalizacji. Jedynym problemem dużych sieci przełączanych (komutowanych) polega na tym, że przełączniki nie rozróżniają rozgłoszeniowych transmisji danych. Zwiększenie sprawności sieci jest wynikiem segmentacji wyłącznie domeny kolizji, a nie domeny rozgłaszania. Nadmierne natężenie rozgłaszania może więc znacznie i niekorzystnie wpłynąć na wydajność sieci LAN.



Rys. 4. Topologia przełączana

Topologie złożone

Topologie złożone są rozszerzeniami lub połączeniami podstawowych topologii fizycznych. Topologie podstawowe są odpowiednie jedynie do bardzo małych sieci LAN. Wyróżniamy dwa podstawowe rodzaje topologii złożonych, łańcuchy i hierarchie. Pierwsza z nich jest bardzo prostą do zrealizowania topologią powstającą w wyniku połączenia szeregowego koncentratorów. Nowoczesne, wysokowydajne sieci lokalne, takie jak Fast Ethernet, nakładają jednak ściśle ograniczenia dotyczące średnicy sieci i liczby połączonych w jej ramach koncentratorów i wzmacniaków. Łańcuchy stosowane są głównie ze względu na prostotę wykonania i uniknięcie kosztów związanych z tworzeniem odpowiedniego szkieletu sieci w danej instytucji. Kolejnym rodzajem topologii złożonej są hierarchie, składają się z kilku warstw koncentratorów. Każda z tych warstw realizuje inną funkcję sieci. Warstwa podstawowa jest w tego rodzaju sieciach zarezerwowana dla komunikacji między stacją roboczą a serwerem. Poziomy wyższe umożliwiają grupowanie wielu poziomów użytkowników. Wszystkie koncentratory bez względu na to w której warstwie się znajdują najczęściej są urządzeniami identycznymi. Wyróżniamy trzy rodzaje hierarchie: hierarchiczne pierścienie, gwiazdy i melanże. Organizacja hierarchiczna jest najodpowiedniejszą dla sieci LAN o rozmiarach średnich do dużych, w których rozwiązuje ona problemy skalowalności i nasilenia ruchu w sieci.

Standardy sieci LAN

Ethernet

Ethernet jest dobrze znaną i szeroko używaną techniką sieciową o topologii szynowej. Został on opracowany przez Xerox Corporation's Palo Alto Research Center we wczesnych latach siedemdziesiątych. Obecnie ten typ sieci znany jest jako PARC Ethernet lub Ethernet I. Sieci Ethernet mogą pracować w paśmie podstawowym lub mogą być szerokopasmowe, pełnodupleksowe lub półdupleksowe. Mogą wykorzystywać jeden z pięciu różnych nośników i pracować z prędkościami z zakresu od 10 Mbps do 1Gbps.

Na sprzęt, który może być używany do obsługi sieci Ethernet, składają się:

- karty sieciowe,
- koncentratory wzmacniające,
- koncentratory nie wzmacniające,
- mosty,
- routery.

10Base2

Budowa sieci 10Base2 jest oparta na kablu koncentrycznym 50 Ω dla którego maksymalna długość wynosi 185 metrów. Można ta odległość zwiększać za pomocą wzmacniaków, koncentratorów, mostów lub routerów. Wykorzystując routery dzielimy sieć na segmenty, które mogą być rozgałęziane do 30 razy, przy czym w każdym rozgałęzieniu może pracować do 64 urządzeń. Zaletą sieci opartej na kablu koncentrycznym jest możliwość jego szpuntowania, tzn. rozgałęziania bez przerywania kabla.

10Base5

Interfejs 10Base5 wykorzystuje dużo grubszy koncentryk niż 10Base2. Skuteczność transmisji w przewodzie miedzianym jest bowiem funkcją grubości przewodnika. Im większa jest jego średnica, tym większą osiąga się szerokość pasma, pozwala to na wydłużenie jednego odcinka do 500 metrów. W rezultacie, kabel 10Base5 może być rozgałęziany do 100 razy, przy zachowaniu maksymalnej liczby 64 urządzeń dla każdego rozgałęzienia.

10BaseT

Specyfikacja 10BaseT, wbrew powszechnemu przekonaniu, nie określa rodzaju użytego kabla. Dotyczy ona natomiast specjalnej techniki sygnalizowania dla nieekranowanej skrętki dwużyłowej wykorzystującej cztery przewody spełniające wymogi trzeciej kategorii wydajności. Nazwy przewodów wskazują na ich funkcje oraz biegunowość. Jedna para przewodów obsługuje

dotatnie i ujemne bieguny obwodu nadawania. Druga para obsługuje dodatnie i ujemne bieguny obwodu odbioru. Wzmacniaki/koncentratory 10BaseT używają przyporządkowań wyprowadzeń, które umożliwiają tworzenie łączy z portami kart sieciowych. W normalnych warunkach urządzenie końcowe zawsze jest połączone z urządzeniem komunikacyjnym. Komplementarność interfejsów tych urządzeń pozwala łączyć je bezpośrednio za pomocą kabla, bez obaw o konflikty między nadawaniem i odbiorem.

10BaseFL

Specyfikacja ta opisuje transmisję sygnału kablem światłowodowym o średnicy 62.5/125 mikrona z prędkością 10 Mbps. Maksymalna długość kabla wynosi 2 km. Połączenie to jest podobne jak dla skrętki połączeniem typu punkt - punkt i jest wykorzystywane do łączenia ze sobą koncentratorów, lub serwerów z koncentratorami.

10BaseFOIRL

Najnowsza specyfikacja opisująca interfejs międzynosnikowy oparty na światłowodzie jest 10BaseFOIRL. Określa ona przesyłanie danych światłowodem pomiędzy dwoma koncentratorami. Do transmisji danych wykorzystywany jest światłowod o średnicy 8.3 mikrona, do którego sterowania wykorzystuje się diodę laserową ILD. Maksymalna długość połączenia wynosi 5 km.

Fast Ethernet

Zwiększenie prędkości sieci Ethernet z 10 Mbps do 100 Mbps wymagało opracowania całkowicie nowej warstwy fizycznej i wprowadzenia niewielkich zmian w warstwie łącza danych, która musiała zostać dopasowana do nowej warstwy fizycznej. Opracowano w związku z tym nowy standard Fast Ethernet. Fast Ethernet jest rozszerzeniem specyfikacji IEEE 802.3 do 100 Mbps. Właściwie jest on bardzo podobny do Ethernet 10BaseT, ale działa o wiele szybciej. Wielu producentów wspomogło ten proces, oferując karty sieciowe obsługujące dwie szybkości transmisji 10 i 100 Mbps. Takie karty są w stanie albo automatycznie wybierać optymalną prędkość, uwzględniając typ okablowania i odległość od koncentratora, lub też prędkość może być wybierana ręcznie. Rozszerzenie standardu 802.3 (do 100 Mbps) obejmuje trzy różne interfejsy międzynosnikowe (MDI):

100BaseTX

Obejmuje ona kable ekranowanej skrętki dwużyłowej (STP) Kategorii 1 i nieekranowanej skrętki dwużyłowej (UTP) Kategorii 5. Ponieważ standard ten jest rozszerzeniem specyfikacji Ethernetu IEEE 802.3, włożono wiele wysiłku, aby produkt ten w bardzo dużym stopniu przypominał 10BaseT.

100BaseFX

100BaseFX - jest odpowiednikiem 100BaseTX dla światłowodu. Może obsługiwać transmisje danych z szybkością 100 Mbps na odległość 400 metrów, wykorzystując dwie żyły światłowodu 62,5/125 dlatego są idealnym rozwiązaniem do łączenia koncentratorów.

100BaseT4

100BaseT4 umożliwia transmisję danych z szybkością 100 Mbps przez cztery pary przewodów telefonicznych na odległość do 100 metrów. Możliwe jest także przeprowadzenie transmisji z wykorzystaniem UTP Kategorii 4 i 5.

Token Ring

Token Ring jest kolejną architekturą sieci LAN znormalizowaną przez IEEE. Ma ona wiele cech wspólnych z Ethernetem i innymi architekturami sieci LAN należącymi do standardów sieciowych IEEE 802. Początkowo Token Ring był technologią dostosowaną do pasma 4 Mbps, później przepustowość podniesiono do 16 Mbps. Dziś istnieją rozwiązania zwiększające prędkość sygnału w sieci Token Ring do 100 lub nawet 128 Mbps.

W odróżnieniu od Ethernetu, z jego chaotyczną i nieregulowaną metodą wielodostępu, Token Ring pozwala w danym czasie nadawać tylko jednemu urządzeniu. Nie występują więc dzięki temu rozwiązaniu żadne kolizje. Dostęp do nośnika jest przyznawany poprzez przekazywanie tokenu w ustalony sposób. Token może być tylko jeden i jest on modyfikowany przez urządzenie transmitujące w celu utworzenia nagłówka ramki danych. Gdyby nie było tokenu, nie dałoby się utworzyć nagłówka ramki danych i transmisja byłaby niemożliwa. Urządzenie odbierające kopiuje dane przesyłane w ramce, zmieniając przy tym (negując) niektóre bity nagłówka ramki i w ten sposób potwierdzając odbiór. Sama ramka dalej krąży w pierścieniu, aż powróci do swojego nadawcy. Urządzenie, które wysłało ramkę, pobiera ją teraz z sieci i usuwa z niej dane oraz adresy. Współdzielona sieć Token Ring posiada wiele zalet w porównaniu z innymi architekturami LAN. Sieć ta wyróżnia się również monitorowaniem działania sieci. Istnieją również mechanizmy automatycznego wykrywania awarii sprzętu i informowania o nich innych stacji w pierścieniu.

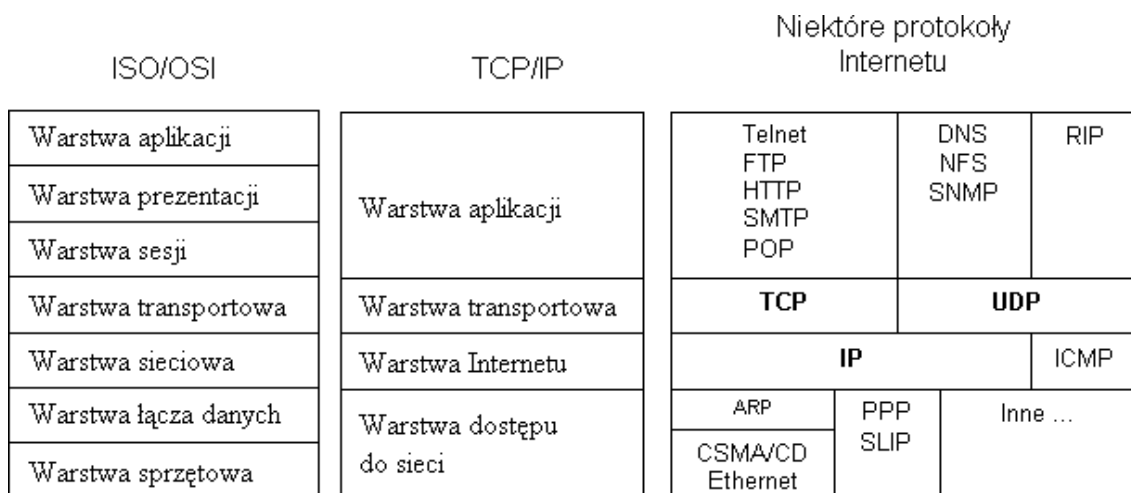
Protokoły sieciowe

Protokołem w sieci komputerowej nazywamy zbiór powiązań i połączeń jej elementów funkcjonalnych. Tylko dzięki nim urządzenia tworzące sieć mogą się porozumiewać. Podstawowym zadaniem protokołu jest identyfikacja procesu, z którym chce się komunikować proces bazowy. Z uwagi na to, że zwykle w sieci pracuje wiele komputerów, konieczne jest podanie sposobu określania

właściwego adresata, sposobu rozpoczynania i kończenia transmisji, a także sposobu przesyłania danych. Przesyłana informacja może być porcjowana - protokół musi umieć odtworzyć informację w postaci pierwotnej. Ponadto informacja może z różnych powodów być przesłana niepoprawnie - protokół musi wykrywać i usuwać powstałe w ten sposób błędy. Różnorodność urządzeń pracujących w sieci może być przyczyną niedopasowania szybkości pracy nadawcy i odbiorcy informacji - protokół powinien zapewniać synchronizację przesyłania danych poprzez zrealizowanie sprzężenia zwrotnego pomiędzy urządzeniami biorącymi udział w transmisji. Ponadto z uwagi na możliwość realizacji połączenia między komputerami na różne sposoby, protokół powinien zapewniać wybór optymalnej drogi.

TCP/IP

Zestaw protokołów został opracowany w celu umożliwienia komunikacji między różnymi typami systemów komputerowych, jak również między różnymi sieciami. Agencja DARPA oraz Stanford University rozpoczęły pracę nad protokołem TCP w 1973 r. Efektem 5-letniego okresu badań było opracowanie dwóch wzajemnie uzupełniających się protokołów: protokołu połączeniowego TCP i protokołu bezpołączeniowego IP (stąd nazwa TCP/IP). Protokoły TCP/IP są wykorzystywane w systemach UNIX-owych, sieciach lokalnych i sieciach rozległych. Protokoły służą do łączenia oddzielnych fizycznie sieci w jedną sieć logiczną. Architektura protokołów TCP/IP jest trochę odmienna od modelu ISO/OSI. Mamy tutaj do czynienia z czterowarstwowym hierarchicznym modelem protokołów TCP/IP. Dane generowane przez programy aplikacyjne są przekazywane w dół stosu jeśli mają być przesyłane poprzez sieć i w górę stosu przy odbiorze. Każda warstwa stosu dodaje do danych przekazywanych z warstwy wyższej informacje sterujące w postaci nagłówków. Nagłówek dodany w warstwie wyższej jest traktowany jako dane w warstwie niższej.



Rys. 5. Schemat protokołu TCP/IP

Warstwa dostępu do sieci

Warstwa ta jest najniższą warstwą w hierarchii architektury protokołów TCP/IP. W warstwie tej do datagramów IP dodaje się nagłówki oraz zakończenie i w ten sposób otrzymuje się ramki przesyłane w sieci. Funkcje tej warstwy odpowiadają w przybliżeniu funkcjom trzech najniższych warstw modelu ISO/OSI. Do komunikacji w sieciach rozległych lub przez łącza szeregowe mogą być stosowane takie protokoły jak PPP (Point-to-Point Protocol) lub SLIP (Serial Line IP). Te dwa ostatnie protokoły zostały specjalnie opracowane do przesyłania datagramów IP poprzez szeregowe łącza dwupunktowe. Protokół SLIP zazwyczaj jest stosowany do łączenia pojedynczych komputerów poprzez łącza szeregowe. Natomiast w sieciach rozległych zalecane jest stosowanie protokołu PPP.

Warstwa Internet

Znajduje się powyżej warstwy dostępu do sieci. Podstawowym protokołem tej warstwy jest IP. Protokół ten jest odpowiedzialny za przesyłanie pakietów zwanych datagramami między użytkownikami sieci. Jest to protokół bezpołączeniowy, co oznacza, że datagramy są przesyłane przez sieć bez kontroli poprawności ich dostarczenia. W efekcie datagram może zostać zgubiony w sieci, przekłamaný lub zniekształcony. Protokół IP jest przeznaczony do sieci o bardzo dobrej jakości i niezawodności łączy transmisyjnych. Drugim protokołem tej warstwy jest ICMP ściśle związany z IP. Służy on do przesyłania komunikatów o nieprawidłowościach w pracy sieci. Protokół pozwala na przesyłanie wiadomości sterujących między węzłami sieci. Wiadomości te dotyczą sterowania przepływem, testowania połączeń, wskazania alternatywnych połączeń i wykrywania niedostępnych użytkowników.

Warstwa transportowa

Jest to warstwa zapewniająca bezpośrednie połączenie między końcowymi użytkownikami (systemami) wymieniającymi informacje. Do najważniejszych protokołów tej warstwy zaliczamy TCP oraz UDP. Protokół TCP jest protokołem połączeniowym umożliwiającym wykrywanie błędów na obu końcach połączenia. Ma on możliwość ustanowienia i utrzymania połączenia wirtualnego między dwoma użytkownikami w celu przesyłania danych, sterowania przepływem, przesyłania potwierdzeń oraz kontroli i korekcji błędów. Protokół UDP jest protokołem bezpołączeniowym, nie posiadającym mechanizmów sprawdzania poprawności dostarczenia danych do miejsca przeznaczenia. Segmenty TCP jak i pakiety UDP w celu ich dalszego przesłania są umieszczane wewnątrz datagramu IP.

Warstwa aplikacji

Zawiera procesy wykorzystujące protokoły TCP lub UDP. Protokoły tej warstwy dostarczają użytkownikom różnych usług. Do najbardziej znanych protokołów warstwy aplikacji korzystających z TCP należą:

- TELNET dla usług terminalowych. Pozwala na rozpoczęcie sesji poprzez sieć.
- TFTP (Trivial File Transfer Protocol) dla prostych usług transferu plików. Jest to uproszczona wersja protokołu FTP.
- FTP (File Transfer Protocol) dla transferu plików. Umożliwia interakcyjne przesyłanie plików.
- SMTP (Simple Mail Transfer Protocol) dla wymiany poczty elektronicznej.

Natomiast do bardziej znanych protokołów warstwy aplikacji korzystających z protokołu UDP należą:

- DNS (Domain Name Service) do zamiany adresów IP na nazwy urządzeń sieciowych.
- RIP (Routing Information Protocol) do wymiany informacji związanych z aktualizacją reguły doboru tras w węzłach sieci.
- NFS (Network File System) do współdzielenia plików przez wiele komputerów dołączonych do sieci.

Do najistotniejszych zalet protokołów TCP/IP można zaliczyć:

- otwartość i niezależność od specyfikacji sprzętowo-programowej systemów komputerowych,
- możliwość integracji wielu różnych rodzajów sieci komputerowych,
- wspólny schemat adresacji pozwalający na jednoznaczne zaadresowanie każdego użytkownika,
- istnienie standardowych protokołów warstw wyższych.

IPX/SPX

IPX/SPX - jest to zestaw protokołów firmy Novell, bierze on nazwę od swoich dwóch głównych protokołów: międzysieciowej wymiany pakietów IPX i sekwencyjnej wymiany pakietów SPX. Ten firmowy stos protokołów został oparty na protokole systemów sieciowych firmy Xerox, wykorzystywanym w pierwszej generacji Ethernet. Protokół IPX w dużym stopniu przypomina IP. Jest bezpołączeniowym protokołem datagramowym, który nie wymaga ani nie zapewnia potwierdzenia każdego transmitowanego pakietu. Protokół IPX polega na SPX w taki sam sposób, w jaki protokół IP polega na TCP w zakresie porządkowania kolejności i innych usług połączeniowych warstwy 4. Stos protokołów IPX/SPX obejmuje cztery warstwy funkcjonalne: dostępu do nośnika, łącza danych, Internetu i aplikacji. Głównym protokołem warstwy aplikacji jest protokół rdzenia NetWare (NCP). Protokół NCP można bezpośrednio sprzęgnąć zarówno z protokołem SPX, jak i IPX. Jest

wykorzystywany do drukowania, współdzielenia plików, poczty elektronicznej i dostępu do katalogów. Innymi protokołami warstwy aplikacji są: protokół informacyjny trasowania, firmowy protokół ogłoszeniowy usługi i protokół obsługi łącza systemu NetWare. Protokół warstwy Internetu SPX jest protokołem połączeniowym i może być wykorzystywany do przesyłania danych między klientem serwerem, dwoma serwerami czy dwoma klientami. Tak jak w przypadku TCP, protokół SPX zapewnia niezawodność transmisjom IPX, zarządzając połączeniem i udostępniając sterowanie strumieniem danych, kontrolę błędów i porządkowanie kolejnych pakietów.

Apple Talk

Gdy komputery Apple zyskały większą popularność, a ich użytkownicy zaczęli z nich korzystać w sposób bardziej wyszukany, nieunikniona została konieczność połączenia ich w sieć. Sieć opracowana przez Apple jest tak przyjazna użytkownikowi jak komputery Apple. Z każdym komputerem sprzedawany jest AppleTalk, czyli stos protokołów pracy sieciowej, a także niezbędny sprzęt. AppleTalk jest siecią równoprawną dostarczającą proste funkcję jak korzystanie z plików i drukarek. Inaczej niż w sieciach klient-serwer, funkcjonalności sieci równoprawnej nie ograniczają żadne sztywne definicje. Każdy komputer może działać jako serwer i klient. Stos protokołów AppleTalk obejmuje pięć warstw funkcjonalnych: dostępu do sieci, datagramową, sieci, informacji o strefach i aplikacji. Warstwa fizyczna i łącza danych służą do zapewnienia zgodności z technologiami sieciowymi opartymi na ustanowionych standardach.

NetBEUI

Protokół NetBEUI został opracowany przez IBM i wprowadzony na rynek w 1985 roku. Jest stosunkowo małym ale wydajnym protokołem komunikacyjnym LAN. NetBEUI jest wyłącznie protokołem transportu sieci LAN dla systemów operacyjnych Microsoft. Zalety korzystania z protokołu NetBEUI są następujące: Komputery korzystające z systemów operacyjnych lub oprogramowania sieciowego firmy Microsoft mogą się komunikować. NetBEUI jest w pełni samodostrajającym się protokołem i najlepiej działa w małych segmentach LAN. Ma minimalne wymagania odnośnie pamięci. Zapewnia doskonałą ochronę przed błędami transmisji, a także powrót do normalnego stanu w razie ich wystąpienia. Wadą protokołu NetBEUI jest fakt, że nie może być trasowany i niezbyt dobrze działa w sieciach WAN.

Sieci bezprzewodowe

WLAN jest elastycznym systemem komunikacji zaimplementowanym jako uzupełnienie, lub jako rozwiązanie alternatywne dla tradycyjnej sieci kablowej. Wykorzystując częstotliwości radiowe (RF), sieć bezprzewodowa wysyła i odbiera dane przez medium jakim jest ziemski atmosfera, minimalizując konieczność użycia połączeń kablowych. Tak więc sieć

bezprzewodowa łączy w sobie transmisję danych z mobilnością użytkownika. Sieci bezprzewodowe zyskały dużą popularność w wielu zastosowaniach, w tym medycyna, handel, produkcja, magazynowanie i nauce. Użytkownicy w tych segmentach rynku zyskują na wydajności, używając przenośnych terminali i komputerów do stałej, bieżącej transmisji danych do centralnych systemów przetwarzania. Dzisiejsze sieci bezprzewodowe postrzegane są jako doskonała alternatywna technologia dla szerokiego spektrum zastosowań.

Doświadczenia rynków europejskich pokazują, że istnieją dwie zasadnicze możliwości budowy sieci WLAN. Pierwsza, sieci prywatne, instalowane w biurach, sklepach, szkołach, szpitalach, fabrykach w celu rozszerzenia lub zamiany sieci przewodowej LAN. Druga, publiczne, określane często mianem HOT SPOT, na lotniskach, dworcach kolejowych, centrach konferencyjnych czy kawiarenkach internetowych.

Technologie sieci bezprzewodowych

Wąskiego pasma (ang. Narrow Band)

Wąskopasmowy system radiowy nadaje i odbiera informacje na określonej częstotliwości radiowej. Utrzymuje częstotliwość sygnału radiowego w jak najwęższym paśmie wystarczającym do przekazu informacji. Niepożądane przesłuchy pomiędzy kanałami komunikacyjnymi są eliminowane poprzez przydzielanie użytkownikom określonych pasm częstotliwości.

Prywatna linia telefoniczna jest podobna do częstotliwości radiowej. Każdy dom w okolicy ma swą własną linię telefoniczną. Ludzie w jednym domu nie mogą słyszeć rozmowy z innej linii. W systemie radiowym, prywatność i brak nakładania się sygnałów osiąga się przy użyciu oddzielnych częstotliwości radiowych. Odbiornik radiowy odfiltrowuje wszystkie sygnały radiowe oprócz sygnału o określonej dla niego częstotliwości.

Szerokiego widma (ang. Spread Spectrum)

Większość sieci bezprzewodowych używa technologii szerokiego widma. Technologia ta została opracowana na potrzeby wojska do użycia w stabilnych i bezpiecznych systemach komunikacyjnych o krytycznym znaczeniu. Technologia Spread-spectrum jest zaprojektowana tak by poświęcić prędkość transmisji (wydajność) na rzecz niezawodności, integralności i bezpieczeństwa. Innymi słowy, większa część całkowitej przepustowości jest zużywana w porównaniu z transmisją wąskopasmową, lecz dzięki temu sygnał jest w efekcie "głośniejszy" i łatwiejszy do odbioru, jeśli odbiornik zna parametry nadawanego sygnału. Jeśli odbiornik nie jest dostrojony do właściwej częstotliwości, sygnał szerokiego widma wygląda dla niego jak szum. Są dwa rodzaje technologii szerokiego widma:

FHSS (Frequency-Hopping Spread Spectrum)

W technologii FHSS przydzielone pasmo dzielone jest na wiele kanałów, podobnie jak w GSM. Liczba i szerokość kanałów są stałe. Nadajnik zmienia częstotliwość zgodnie z sekwencją pseudolosową zdefiniowaną przez algorytm skoku, negocjowana na początku transmisji. Interferencja na jednej częstotliwości powoduje powtórzenie transmisji pakietu. Niezaprzeczną zaletą FHSS jest redundancyjne pokrycie wielu punktów dostępu, co eliminuje problem przeciążania zawsze tego samego punktu dostępu i dodatkowo zwiększa odporność na zakłócenia radioelektryczne. Dla niepożądanego odbiornika, THSS wygląda jak krótkotrwałe impulsy szumów.

DSSS (Direct-Sequence Spread Spectrum Technology)

Technologia DSSS bazuje na kluczkowaniu sygnału danych szybkozmienną sekwencją pseudolosową, generowaną przez specjalny układ nadajnika. Elementy takiej sekwencji nazywa się chipami a ich długość jest ułamkiem długości bitu danych i ma wpływ na jakość transmisji: im dłuższy chip, tym większe prawdopodobieństwo odtworzenia rzeczywistej wartości bitu danych. Sygnał danych trafia po kluczkowaniu do modulatora, a stamtąd w postaci szumu w eter. Odbiornik z kolei taki sygnał demoduluje i poddaje kluczkowaniu taką samą sekwencją jak nadajnik, ale wytworzoną przez swój autonomiczny generator sekwencji pseudolosowej. Bardzo wiele zależy zatem od synchronizacji obydwu generatorów. Dla niepożądanego odbiornika, DSSS wygląda jak szerokopasmowy szum o niskiej mocy i jest ignorowany przez większość wąskopasmowych odbiorników. Przy użyciu technik modulacji sygnału DSSS możemy uzyskać dużo większe prędkości przesyłu. Modulacje DBPS i DQPSK zapewniają nam szybkość do 2Mbps z kolei modulacja CCK oparta na skomplikowanych matematycznych wzorach kodujących pozwala osiągnąć prędkość nawet do 11Mbps.

Podczerwień

Trzecia technologia, rzadko używana w komercyjnych sieciach bezprzewodowych to transmisja w podczerwieni. Systemy na podczerwień (IR) używają do przenoszenia danych bardzo wysokich częstotliwości, tuż poniżej pasma widzialnego w spektrum elektromagnetycznym. Podobnie jak światło, IR nie może przenikać obiektów nieprzezroczystych, jest to technologia zarówno kierunkowa (linia widzialności) jak i rozproszona. Niedrogie systemy kierunkowe oferują bardzo krótkie zasięgi, rzędu 1 metra i są zwykle stosowane w indywidualnych sieciach lokalnych, lecz czasami używają specyficznych aplikacji bezprzewodowych. Wysokowydajne kierunkowe systemy IR są niepraktyczne dla użytkowników przenośnych, i przez to stosowane jedynie w połączeniach podsieci. Rozproszona (lub odblaskowa) technologia bezprzewodowa nie wymaga (linii widzialności), lecz komórki takiej sieci ograniczają się do jednego pomieszczenia.

Struktury sieci WLAN

Sieć WLAN najprościej mówiąc jest to zespół urządzeń komunikujących się ze sobą drogą radiową za pomocą specjalnych adapterów nadawczo odbiorczych. Zasadniczo wyróżniamy trzy struktury sieci radiowych ze względu na ich organizację, oto one:

IBSS (Independent Basic Service Set)

Jest typowym przykładem sieci niezależnej. W tym elementarnym przypadku do stworzenia sieci potrzebne są dwie rzeczy: komputer i radiowa karta sieciowa. Każda stacja nadawczo odbiorcza posiada ten sam priorytet i komunikuje się z innymi komputerami bezpośrednio, bez żadnych dodatkowych urządzeń aktywnych kierujących ruchem w LAN-ie. Po prostu wystarczy "wsadzić" do komputera kartę radiową, zainstalować sterowniki, i już możemy rozkoszować się niczym nie ograniczoną komunikacją z innymi komputerami (z danej podsieci) wyposażonymi w karty radiowe. Nie wolno zapominać o ustawieniu we wszystkich urządzeniach tego samego identyfikatora domeny, umożliwiającego komunikację tylko z wybranymi maszynami, i zabezpieczającego przed nieautoryzowanym użytkowaniem naszej sieci WLAN.

BSS (Basic Service Set)

Wyżej przedstawiona konfiguracja (IBSS) jest wystarczająca w przypadku małych, tymczasowych i niezorganizowanych sieci. Co jednak się stanie jeśli zapagniemy połączyć ją z kablową instalacją np. 10Base-T lub też zwiększyć zasięg poruszania się stacji roboczych? Tutaj konstruktorzy proponują urządzenie zwane HUB-em AP (Access Point, punkt dostępu, koncentrator radiowy). Ów element spełnia funkcję bardzo podobną do huba stosowanego w sieciach UTP, mianowicie wzmacnia i regeneruje odebrany sygnał oraz kieruje ruchem w LAN-ie. Teraz wszystkie stacje robocze należące do danej podsieci (domeny radiowej) nie komunikują się już bezpośrednio ze sobą lecz za pośrednictwem owego koncentratora. Maksymalna ilość komputerów obsługiwanych jednocześnie przez AP jest ściśle określona przez producenta i oscyluje w granicach kilkudziesięciu urządzeń. Takie rozwiązanie znacznie zwiększa zasięg sieci.

ESS (Extended Service Set)

Jest siecią złożoną; powstaje podczas połączenia ze sobą co najmniej dwóch podsieci BSS. Wystarczy zespolić ze sobą HUB-y AP tradycyjnym okablowaniem umożliwiając w ten sposób komunikację stacjom bezprzewodowym z tradycyjną siecią LAN oraz z jednostkami znajdującymi się w innych podsieciach radiowych. Jeśli przy okazji zapewnimy nakładanie się na siebie sygnałów z poszczególnych podsieci możliwe będzie poruszanie się komputerów po całej sieci ESS.

Rodzaje sieci bezprzewodowych

Wi-Fi (Wireless Fidelity)

Sieci Wi-Fi do przesyłania danych wykorzystują niewielki zakres pasma wokół bazowej częstotliwości 2,4 GHz. Choć bezprzewodowe kart sieciowe mogą się komunikować bezpośrednio między sobą niemal zawsze centrum sieci jest punkt dostępowy, który dodatkowo może pełnić funkcję np. routera. Działa on podobnie jak koncentrator w tradycyjnej sieci, czyli stanowi dla wielu komputerów punkt styku, organizując ruch w sieci. Prawie zawsze wyposażony jest w gniazdo sieciowe, pozwalające wpiąć do sieci tradycyjnej, dzięki czemu sieć bezprzewodowa i przewodowa mogą funkcjonować razem. Rosnąca popularność bezprzewodowych sieci lokalnych wśród użytkowników Internetu wywołała u organizacji standaryzujących zainteresowanie pracami nad projektami standardów sieciowych. Powstają i rozwijają ich liczne wersje prześcigające się między sobą walorami użytkowymi. Poniżej przedstawię podstawowe z nich:

IEEE 802.11

Standard ten powstał jako pierwszy w sieciach WLAN i został oparty na bazie protokołu CSMA/CA, wykorzystując technikę frequency hopping w paśmie częstotliwości 2,4 GHz, pozwalając na transmisję danych z szybkością do 2 Mb/s. Technika ta polegająca na rozkładaniu energii transmisji w szerszym widmie częstotliwości-pasmo użytkowe zostaje podzielone na kilkadziesiąt kanałów, a transmisja odbywa się w kolejnych kanałach, przełączanych według określonego algorytmu. Standard 802.11 nie stał się zbyt popularny, zastąpiły go ulepszone wersje.

IEEE 802.11b

Jest to standard pracujący również w 2,4-gigahercowym paśmie częstotliwości jednak oparty jest na technice transmisji DSSS. Polega ona na ciągłym przesyłaniu danych sygnałem małej mocy. Dane opatrzone są informacjami kontrolno – korekcyjnymi o znacznej objętości pozwalającymi na odtworzenie poprawnej zawartości nawet z mocno uszkodzonego przekazu. Technika DSSS umożliwia znacznie efektywniejsze wykorzystanie dostępnego pasma, pozwalając na uzyskanie szybkości transmisji do 11 Mb/s.

IEEE 802.11a

W odróżnieniu od poprzednio przedstawionych, standard ten nie wykorzystuje bardzo często używanego przez inne urządzenia pasma 2,4 GHz, a znacznie wyższe 5 GHz. Wysoka częstotliwość w połączeniu z tak zwaną modulacją ortogonalną pozwoliły na uzyskanie przepustowości wynoszącej 55 Mb/s. Modulacja ortogonalna polega na podziale pasma na wiele kanałów i transmisji danych równolegle we wszystkich dostępnych kanałach. Jednak urządzenia sieciowe oparte na tym standardzie ze względu na zastosowanie różnej organizacji warstwy transmisyjnej nie mogą współpracować

z urządzeniami standardu 802.11b. Zmusiło to producentów do wprowadzenia na rynek konstrukcji dwusystemowych, zdolnych do pracy w obu standardach.

IEEE 802.11g

Ten standard przenosi stosowaną w 802.11a technikę modulacji ortogonalnej do stosowanego w 802.11b pasma 2,4 GHz. Efektem tego jest uzyskanie zbliżonej do 50 Mb/s przepływności, jednak przy nieco mniejszej liczbie kanałów, warunkującej sumaryczną przepustowość sieci. Co jednak bardzo istotne urządzenia tego standardu mogą być konstruowane jako zgodne co do współpracy z najbardziej dotąd rozpowszechnionym standardem 802.11b.

Sieci Wi-Fi dla większego bezpieczeństwa transmisji danych wykorzystują techniki szyfrujące połączenie zwane potocznie WEP. Obejmują one kodowanie 64-bitowe jak również 128-bitowe stanowiące dużo lepszą zaporę. Niektórzy producenci oferują nawet 256 bitów, jednak takie rozwiązania działają tylko wówczas, gdy cały sprzęt sieciowy pochodzi od jednego producenta. Jeśli chce się zabezpieczyć sieć w sposób jeszcze bardziej wyrafinowany, wówczas należy zastosować jako punkt dostępowy router obsługujący funkcję filtrowania adresów MAC. Adres taki jest unikatowym w skali światowej numerem, przypisywanym konkretnemu urządzeniu sieciowemu np. karcie sieciowej. Tworząc na routerze listę wszystkich adresów MAC, które mają prawo korzystać z sieci ograniczamy dostęp do sieci nie pożądanym osobom.

Sieci Bluetooth

Łączność bezprzewodowa Bluetooth wykorzystuje pasmo częstotliwości ISM zawierające się w przedziale od 2400 do 2483,5 MHz, zakres ten podzielony jest 79 kanałów rozmieszczonych co 1 MHz (od 2402 do 2480 MHz). W czasie połączenia kanały zmieniane są z częstotliwością 1600 razy na sekundę. Takie rozwiązanie zwane rozpraszaniem widma z przeskokiem częstotliwości zastosowano po to, aby zapewnić większą odporność przesyłania danych na zakłócenia. Zasięg większości urządzeń Bluetooth nie przekracza 10 metrów, a moc nadajników 1 mW. Maksymalna szybkość transmisji nie przekracza 1 Mb/s, jednak podobnie jak w wielu innych standardach bezprzewodowych zależy od lokalizacji sieci. Dla zwiększenia bezpieczeństwa w czasie nawiązywania połączenia stosowana jest weryfikacja kluczy jak również szyfrowanie danych. Bezpieczeństwo zwiększa fakt, iż częstotliwość, na jakiej pracuje nadajnik i odbiornik jest zmienna.

W niedalekiej przyszłości sieci te mogą stać się poważnym konkurentem dla sieci Wi-Fi, jednak popularna obecnie wersja tego standardy oznaczona numerem 1.1 nadaje się głównie do komunikacji z urządzeniami peryferyjnymi i nie oferuje wystarczającej szybkości przesyłania danych niezbędnej dla niektórych zastosowań. Na szczęście Bluetooth ciągle się rozwija. W kolejnej wersji standardu 1.2 szybkość zostanie zwiększona do 2-3 Mb/s, a w wersji 2.0 prawdopodobnie do 12 Mb/s.

Zalety sieci WLAN

- Jest prosta w montażu i konfiguracji.
- Łatwa diagnoza usterki.
- Daje duże możliwości rozbudowy (modularność).
- Nieograniczona swoboda poruszania się.
- Nie wymaga okablowania.
- Można ją połączyć z kablową siecią LAN.
- Anteny kierunkowe pozwalają osiągnąć znaczny zasięg sieci.

Literatura

Pozycje książkowe:

1. M. Sportack, „Sieci komputerowe-Księga eksperta”, Helion, Gliwice 1999
2. M.A. Miller, „Internetworking” ,Read Me, Warszawa 1999
3. W. Buchman, „ Sieci komputerowe” ,Komunikacji i Łączności, Warszawa 1993
4. T. Zydornia, „PC i Sieci komputerowe” ,PLJ, Warszawa 1993
5. Cz. Kościelny, „ Sieci komputerowe-skrypt” ,Zielona Góra 1999
6. F.J. Derfler, „Jak działają sieci” ,PWN, Warszawa 1995
7. A. Wolisz, „Podstawy lokalnych sieci komputerowych” ,Naukowo-Techniczne, Warszawa 1992
8. W. Moczurad, „W sieci”, Fortis, Kraków 1993
9. J. Habraken, „ABC Sieci komputerowych”, Helion, Warszawa 2002
10. T.Ogletree, „Rozbudowa i naprawa sieci” , Helion, Warszawa 2001
11. B.A. Miller, Ch. Bisdikian, „Bluetooht“, Helion, Warszawa 2003
12. B. Zieliński, „Bezprzewodowe sieci komputerowe”, Helion, Warszawa 2000
13. Z. Gierada, „Sieci komputerowe w rzeczywistości szkolnej”, Politechnika Lubelska, Lublin 2003

Czasopisma:

14. PC WORLD KOMPUTER, „Technologia bezprzewodowa”, Nr 3/2003
15. ENTER, „Świat wolny od drutów”, Nr 3/2003
16. ENTER, „Budujemy sieci”, Nr 4/2003
17. ENTER, „Sąsiedzi, połączcie się”, Nr 5/2003
18. EKSPERT, „Czas na Bluetooth”, Nr 2/2003
19. NET WORLD, „Dostęp do sieci LAN przez BLUETOOTH”, Nr 2/2003

20. CHIP, „Szybciej do sieci!”, Nr 2/2003
21. CHIP, „Podziel się pajęczyną!”, Nr 3/2003

Strony Internetowe:

22. www.net.w.pl
23. www.lan.pl
24. www.kki.net.pl
25. www.orfi.uwm.edu.pl
26. www.bestpartner.pl
27. www.wlan.p-net.pl
28. www.trilan.pl