LOCAL AREA NETWORK. TOPOLOGIE, PROTOKOŁY I PROJEKTY

Istnieje wiele sposobów opisywania sieci LAN, a każda z nich daje wgląd w implementację i różnice w produktach, a także w punktach narażenia na bezpieczeństwo. Ta sekcja wprowadza różne terminy i perspektywy jako podstawę do dyskusji w poniższych sekcjach.

CHARAKTERYSTYKA SIECI LAN

Jednym ze sposobów opisu sieci LAN jest opisanie cech, które odróżniają sieć lokalną od innych typów sieci. Najczęstsze cechy to:

* Mały zasięg geograficzny (dwie najbardziej odległe stacje mogą znajdować się w odległości do 5 kilometrów [km] lub mniej)

* Duża szybkość (szybkość transmisji danych znacznie przekracza 1 milion [megabitów bitów na sekundę] [Mb / s] i do 1 miliarda [gigabit] bitów na sekundę [Gbps])

* Media specjalne (powszechne zastosowanie kabla koncentrycznego i światłowodu, a także skrętka)

* Własność prywatna

Ten rodzaj sieci ma zatem zupełnie inny wygląd niż Internet lub inne publiczne lub prywatne sieci rozległe (WAN). Więcej osób ma dostęp do infrastruktury sieci LAN niż do infrastruktury niemal dowolnej sieci WAN. Użytkownicy sieci LAN mogą z łatwością "szpiegować" się nawzajem poprzez wąchanie pakietów, co zwykle jest bardzo trudne w Internecie. Pojedynczy użytkownik może doprowadzić do zatrzymania sieci LAN. Firmowa sieć LAN to zazwyczaj podstawowy dostęp użytkowników do Internetu. Użytkownicy w sieci LAN znajdują się za firmową zaporą i routerem; niektóre badania sugerują, że są odpowiedzialne za 80 procent zdarzeń związanych z bezpieczeństwem. Inne sieci LAN obejmują sieci hotelowe, które są często wykorzystywane przez przestępców jako przydatne źródła informacji poufnych dostępnych w niezabezpieczonych systemach tymczasowo podłączonych do tych usług dostępu do Internetu. Często sukces tych ataków wynika z braku wykształcenia i świadomości użytkowników, takich jak wybieranie złych haseł, brak aktualnych plików sygnatur wirusów lub komputerów podłączonych do sieci LAN bez zapór ogniowych. Czasami ataki są bardziej wyrafinowane, takie jak używanie sniffera pakietów do nauki hasła innego użytkownika lub podejmowanie kroków mających na celu obniżenie wydajności sieci.

KOMPONENT SIECI LAN

Zasadniczo do zbudowania sieci LAN potrzebne są cztery podstawowe komponenty, zapewniające własne luki w zabezpieczeniach i ekspozycje perspektywicznye:

1. Komputery. Są to podstawowe urządzenia podłączone do sieci. Czytaj "komputer" bardzo szeroko; termin ten może obejmować komputery osobiste (PC), minikomputery, komputery typu mainframe, serwery plików, drukarki, plotery, urządzenia mobilne (np. smartfony i tablety), serwery komunikacyjne i urządzenia do łączenia sieci. Może również zawierać analizatory protokołów.

2. Media. Są to fizyczne środki, za pomocą których komputery są ze sobą połączone. Nośniki LAN to nieekranowana skrętka (UTP), kabel koncentryczny (kabel koncentryczny), światłowód i urządzenia bezprzewodowe (radiowe). Nośniki bezprzewodowe mają punkty połączeń w całym obszarze, w którym urządzenia mogą łączyć się z siecią, a każde miejsce jest potencjalnym punktem połączenia w środowisku bezprzewodowym.

3. Karta interfejsu sieciowego (NIC). Jest to fizyczne połączenie z komputera do medium LAN. Starsze karty sieciowe są kartami wewnętrznymi; jedynym widocznym elementem jest fizyczne podłączenie

do sieci LAN, często gniazdo RJ-45. Coraz więcej adapterów korzysta z gniazd uniwersalnej magistrali szeregowej (USB) na nowoczesnych komputerach. Chociaż karty sieciowe mają szeroki zakres cen w zależności od ich możliwości, przeznaczenia i dostawcy, można zakupić wewnętrzną kartę sieciową 1 Gb / s na komputer osobisty (PC) za mniej niż 7 USD, adapter USB Ethernet na około 14 USD i bezprzewodowy Adapter USB za mniej niż 13 USD w momencie pisania w styczniu 2013 r.

4. Oprogramowanie. Trzy powyższe elementy zapewniają fizyczną łączność. Oprogramowanie - często nazywane systemem operacyjnym sieci (NOS) - jest niezbędne, aby urządzenia mogły faktycznie korzystać z udostępniania zasobów, które może zapewnić sieć LAN. NOS obsługuje wiele typów usług, takich jak udostępnianie plików, udostępnianie drukarek, działanie klient / serwer, usługi komunikacyjne i inne.

Chociaż sieć LAN musi być badana w sposób holistyczny, każdy z tych komponentów w każdym dołączonym węźle może również wymagać sprawdzenia.

PARAMETRY TECHNOLOGII LAN

Ostatnim sposobem omówienia specyfiki działania sieci LAN jest opisanie technologii:

* Topologia fizyczna. Fizyczny układ nośnika.

* Topologia logiczna. Logiczna relacja węzłów sieci LAN między sobą.

* Standard Media Access Control (MAC). Specyfikacja opisująca reguły, które każdy węzeł wykonuje, aby określić, kiedy nadejdzie jego kolej, aby transmitować na nośniku.

* Korzystanie z protokołu Logic Link Control (LLC). Określa format ramki stosowany powyżej warstwy MAC i dodatkowe usługi.

* Używanie protokołów wyższych warstw. Definiuje komunikacyjne protokoły węzeł-węzeł i dodatkowe aplikacje wyższej warstwy.

Nie ma znaczenia, w jaki sposób sieć LAN jest sklasyfikowana lub opisana. Istotne jest jednak, aby sieć LAN była rozumiana z różnych perspektyw, aby móc zastosować badanie bezpieczeństwa sieci.

TOPOLOGIA LAN

WAN zazwyczaj używają jakiejś technologii przełączanej, takiej jak tradycyjne przełączanie obwodów, przełączanie pakietów (np. X.25) lub szybkie przełączanie pakietów (np. Przekaźnik ramki lub tryb przesyłania asynchronicznego [ATM]). Rzeczywiście, linie punkt-punkt zazwyczaj łączą przełączniki sieciowe, tak, że istnieje jednorazowa transmisja danych na linii w tym samym czasie. Historycznie, sieci LAN były rozgłaszane, co oznacza, że każda stacja LAN słyszy każdą transmisję na nośniku. Topologie LAN muszą zatem wspierać charakter rozgłaszania sieci i zapewniać pełną łączność między wszystkimi stacjami. Topologia sieci jest używana do opisania dwóch problemów. Fizyczna topologia opisuje, w jaki sposób stacje LAN są fizycznie połączone, aby mogły komunikować się ze sobą. Topologia logiczna opisuje, w jaki sposób wpływa na nadawany charakter sieci LAN, a zatem, w jaki sposób stacje uczestniczą w procesie uzyskiwania pozwolenia na transmisję na nośniku. Znaleziono trzy popularne topologie LAN: gwiazda, pierścień i magistrali.

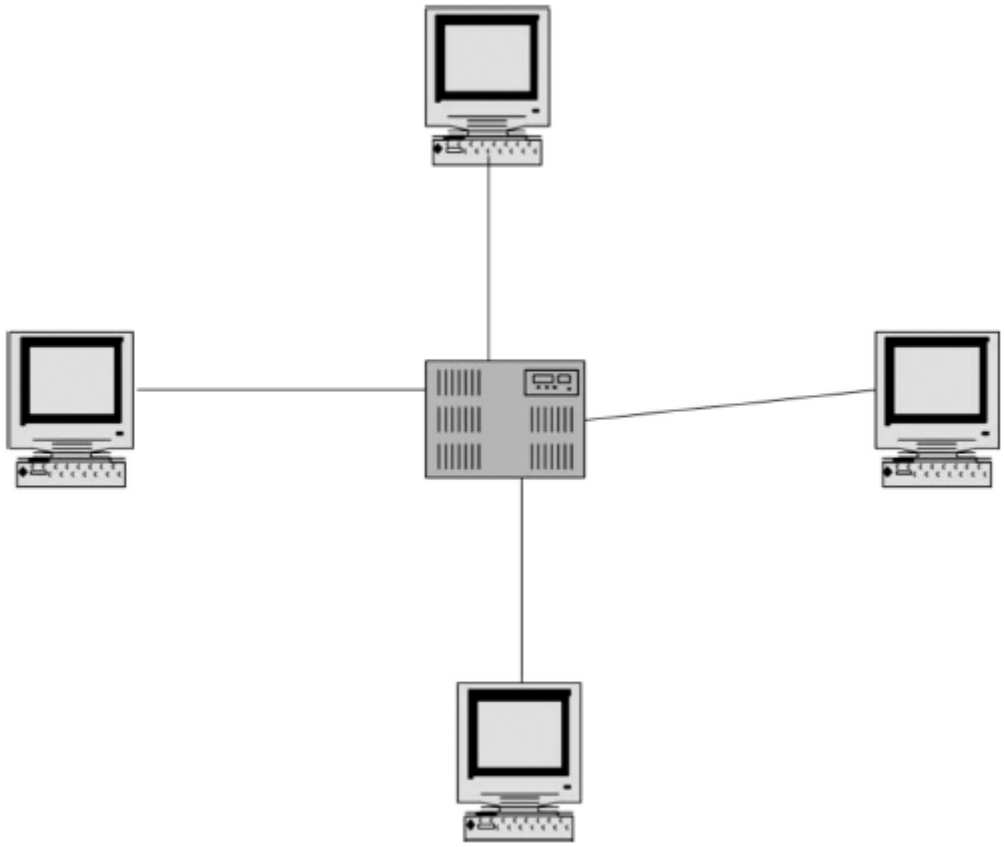
KONTROLA SIECI

Ponieważ sieci lokalne są sieciami rozgłoszeniowymi, konieczne jest, aby tylko jeden węzeł mógł transmitować w tym samym czasie. Wszystkie sieci LAN korzystają z rozproszonego schematu kontroli dostępu, co oznacza, że wszystkie węzły stosują te same reguły, aby uzyskać dostęp do nośnika

sieciowego i żaden węzeł LAN nie kontroluje dostępu innych węzłów. W ten sposób węzły sieci LAN mogą działać w trybie online i offline, nie powodując spadku sieci. Ten opis nie sugeruje, że w sieci LAN nie ma żadnych krytycznych elementów. W rzeczywistości, jeśli centralny koncentrator, przełącznik lub przekaźnik ulegnie awarii, nastąpi awaria sieci LAN. Kontrola rozproszona sugeruje jednak, że wszystkie węzły (stacje użytkownika) stosują te same reguły dostępu, a awaria pojedynczego węzła nie spowoduje obniżenia LAN. Schemat kontroli dostępu jest zdefiniowany przez protokół MAC.

TOPOLOGIA GWIZDY

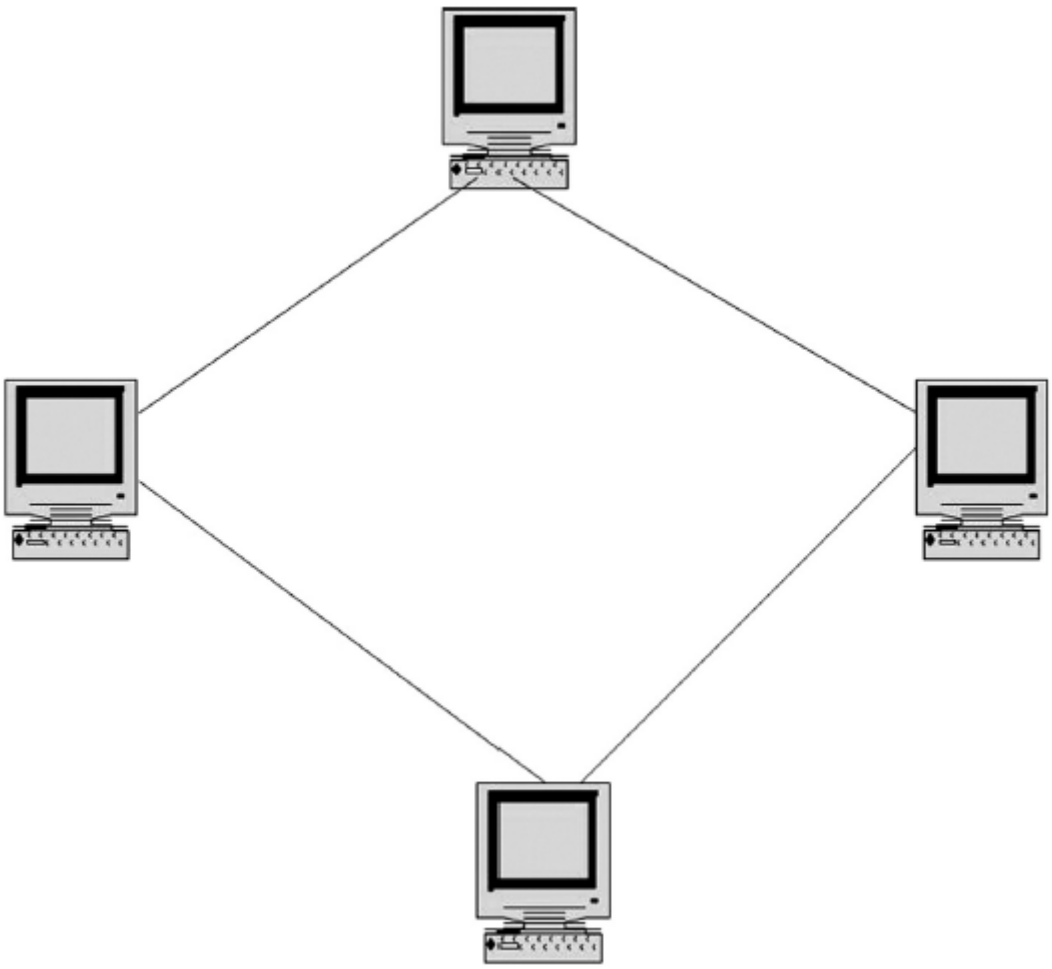
W topologii gwiazdy



wszystkie urządzenia w sieci LAN są połączone za pomocą jakiegoś urządzenia centralnego. Ponieważ sieci lokalne korzystają ze schematów rozproszonego dostępu, cała komunikacja odbywa się z jednego węzła do drugiego, a urządzenie centralne zapewnia jedynie ścieżkę między parami urządzeń. Fizyczne topologie gwiazd mają ogromną przewagę nad innymi topologiami, ponieważ znacznie ułatwiają administrowanie siecią, konserwację, rekonfigurację i odzyskiwanie błędów. Wady obejmują pojedynczy punkt awarii.

TOPOLOGIA PERŚCIENIA

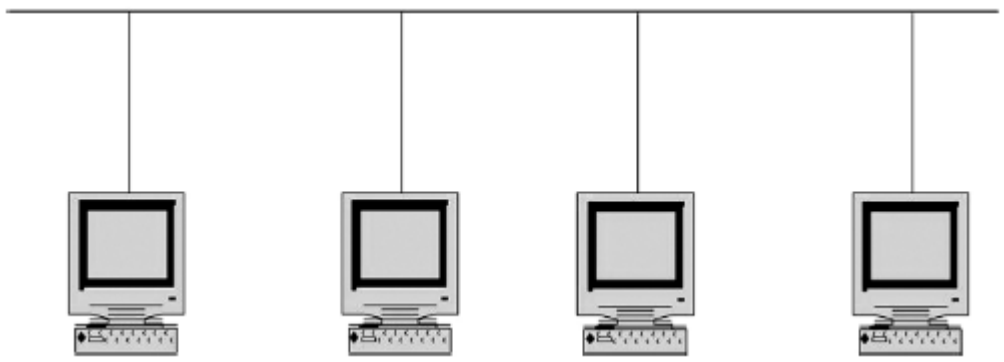
W topologii pierścienia węzły są połączone zestawami połączeń punkt-punkt, które są zorganizowane w okrąg



Stacje łączą się z medium za pomocą aktywnych kranów, które są w rzeczywistości bitowymi wzmacniaczami; bit jest odczytywany z linii wejściowej, utrzymywany przez pojedynczy czas bitowy, a następnie przesyłany do linii wyjściowej. Stacja przesyła komunikat w sieci wysyłając strumień bitów na jego wychodzący link; w ten sposób pierścienie mają charakter jednokierunkowy. Ponieważ wszystkie inne stacje widzą bity jeden po drugim, odbiorca nie ma uprzedniego ostrzeżenia o nadejściu wiadomość. Z tego powodu nadajnik jest odpowiedzialny za usunięcie wiadomości z ringu, gdy bity powracają. Schemat MAC zapewnia, że wiele stacji nie transmituje w tym samym czasie. Ponadto pierścień jest siecią transmisji szeregowej. Ponieważ stacja wysyła wiadomość po trochu na raz, każda inna stacja zobaczy komunikat w momencie przejścia, ale każda z nich odbierze inną część wiadomości w dowolnym momencie. Pierścienie są powszechną fizyczną topologią LAN. Jednak w przeciwieństwie do gwiazd, mają wiele punktów awarii: jeśli jedno łącze lub jedno aktywne dotknięcie zawodzi, integralność pierścienia zostaje zniszczona. Jeśli prawdopodobieństwo uszkodzenia pojedynczego elementu wynosi p i jest n elementów, wówczas prawdopodobieństwo niepowodzenia P {F} sieci LAN

$$P\{F\} = 1 - (1 - p)^n$$

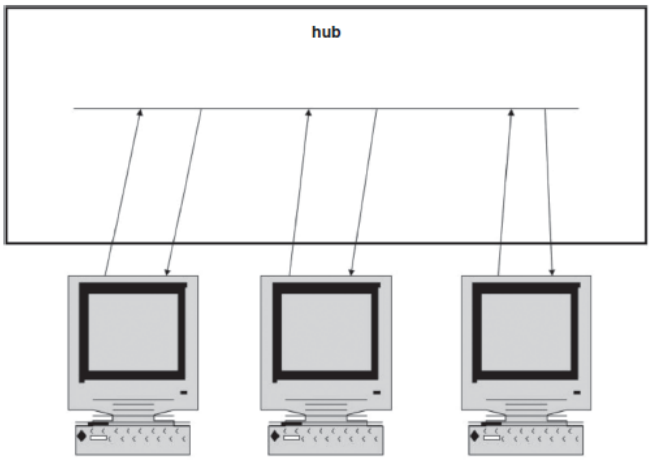
Wraz ze wzrostem liczby elementów prawdopodobieństwo awarii sieci rośnie wykładniczo. Ten problem ma tak krytyczny charakter, że prawie wszystkie produkty pierścieniowe używają schematu gwiezdnego lub mają wbudowaną redundancję dla tej właśnie sytuacji.



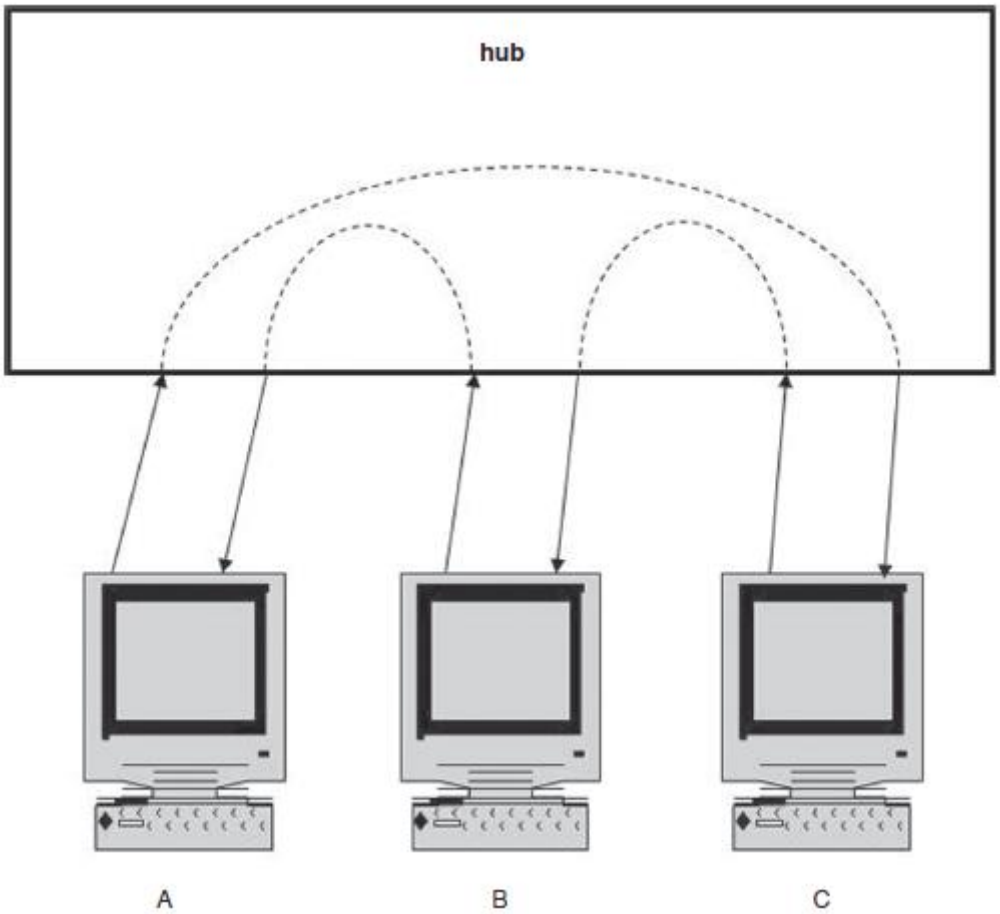
wszystkie urządzenia są połączone z jednym elektrycznie ciągłym medium; z tego powodu ta topologia nazywana jest również zwykłą siecią kablową lub siecią współdzieloną. Węzły łączą się z medium za pomocą biernego kranu, który monitoruje przepływ bitów bez zmiany jego położenia. Jest to podobne do działania woltomierza; mierzy napięcie na linii energetycznej bez zmiany dostępnego napięcia. Sieci magistrali są analogiczne do sposobu, w jaki urządzenia są podłączone do linii prądu zmiennego (AC). Wszystkie urządzenia pobierają energię z tego samego źródła, nawet jeśli znajdują się na różnych fizycznych segmentach sieci dystrybucji energii w budynku. Ponadto działanie urządzeń jest niezależne od siebie; jeśli przerwie automat z kawą, toster nadal będzie działał. Magistrala jest jednoczesną siecią rozgłoszeniową, co oznacza, że wszystkie stacje odbierają przesłaną wiadomość zasadniczo w tym samym czasie (ignorując opóźnienie propagacji przez medium). Większość domowych i biznesowych sieci LAN wykorzystuje magistralę pasma podstawowego, w której sygnały prądu stałego (DC) są podawane bezpośrednio do magistrali przez nadajnik bez żadnych modyfikacji. Ponadto, transmisje na magistrali pasma podstawowego są rozgłaszane dwukierunkowo i nie mogą być zmieniane przez odbiorniki. Technologie magistrali LAN są wykorzystywane w systemach telewizji kablowej. Przykładowo, wykorzystują magistralę szerokopasmową, w której sygnały są modulowane (to jest przesunięte częstotliwościowo) do pewnych częstotliwości dla transmisji w jednym lub drugim kierunku. Autobusy są najstarszą topologią sieci LAN i generalnie są ograniczone pod względem rodzaju medium, z którego mogą korzystać. Zazwyczaj nie cierpią one na problemy z pojedynczym punktem awarii.

TOPOLOGIA FIZYCZNA A LOGICZNA

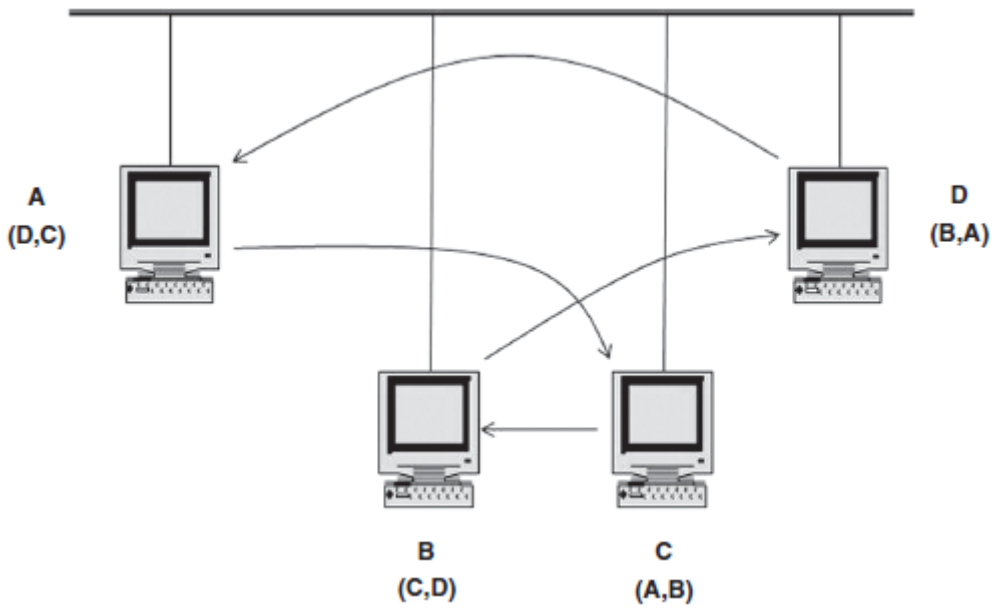
Rozróżnienie zostało dokonane powyżej pomiędzy fizyczną i logiczną topologią sieci LAN. Topologia fizyczna opisuje, w jaki sposób stacje są fizycznie ustawione i połączone ze sobą, podczas gdy logiczne topologia opisuje sposób propagacji sygnałów i logiczne działanie sieci. We wszystkich dzisiejszych powszechnie używanych sieciach LAN topologia logiczna różni się od fizycznej topologii. Najpopularniejszą obecnie konfiguracją sieci LAN jest szyna przewodowa



Ten rodzaj sieci ma topologię gwiazdy, w której wszystkie stacje są fizycznie połączone za pomocą połączeń punkt-punkt z urządzeniem centralnym. To urządzenie centralne zawiera magistralę, która łączy wszystkie porty I / O w taki sposób, że gdy jedna stacja nadaje komunikat, wszystkie stacje otrzymają ją. Ponieważ działa to dokładnie tak samo jak transmisja symultaniczna, lub magistrala, sieć, kategoryzujemy tę konfigurację jako fizyczną gwiazdę, logiczną magistralę. Inną popularną konfiguracją jest pierścień z gwiazdą



W tej konfiguracji bity będą przemieszczać się w porządku logicznym od stacji A do B, C, A i tak dalej, co odpowiada operacji szeregowego rozgłaszania pierścienia. Nazywamy to gwiazdą fizyczną, pierścień logiczny. Chociaż dziś jest to rzadkość, kolejną technologią hybrydową jest pierścień przewodowy



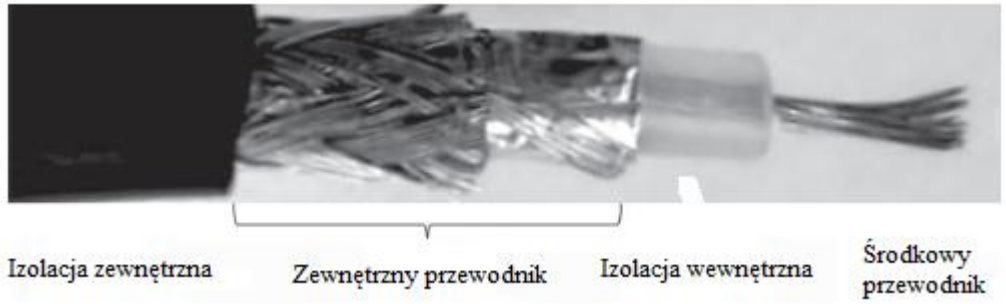
W tej konfiguracji węzły są pasywnie dołączane do pojedynczego kabla, tworząc fizyczną magistralę. Każda stacja przechowuje tabelę określającą adres poprzedniej i następnej stacji, tworząc w ten sposób pierścień logiczny.

MEDIA

Następne akapity omawiają trzy podstawowe typy obecnie używanych mediów LAN. Ze względu na ich stosunkowo dużą prędkość, mały rozmiar geograficzny i chronione środowisko, wiele rodzajów mediów może być wykorzystywanych w sieciach LAN.

KABEL KONCENTRYCZNY

Kabel koncentryczny (kabel koncentryczny) to oryginalny nośnik LAN. Jego nazwa pochodzi od fizycznej budowy samego kabla



W środku kabla znajduje się przewodnik, zwykle wykonany z miedzi, który otoczony jest izolatorem, który z kolei jest otoczony innym przewodnikiem, który działa jako ekran elektryczny. Ponieważ ekran całkowicie otacza środkowy przewodnik, a obie mają wspólną oś, ekran zapobiega zewnętrznym zakłóceniom elektrycznym wpływającym na sygnały na przewodniku i zapobiega generowaniu przez zakłócenia sygnału na przewodach innych kabli. Kable koncentryczne różnią się rozmiarem od 1/4-1 cala (6,35-25.4 mm), w zależności od grubości żyły, ekranu i izolacji. Zastosowania dla zakresu koncentrycznego od telewizji kablowej do sieci LAN. Można osiągnąć prędkości przekraczające kilkaset Mb / s na odległościach od kilkuset do kilku tysięcy metrów. Kabel koncentryczny ma również wysoką odporność na zakłócenia elektromagnetyczne i radiowe. Łatwo jest jednak dotknąć. Kabel

koncentryczny jest widoczny tylko w fizycznych sieciach LAN, takich jak Ethernet. Oryginalna specyfikacja Ethernetu wymagała w rzeczywistości cienkiego kabla koncentrycznego; późniejsza wersja, w której zastosowano cienki (CATV) kodek, została nazwana CheaperNet. Coax zwykle nie znajduje się w sieciach gwiazdowych lub pierścieniowych. Kabel koncentryczny jest łatwy do podsłuchu

SKRĘTKA NIEEKRANOWANA

Medium cieszące się obecnie największą popularnością wśród aplikacji LAN to skrętka. Skrętka składa się z dwóch izolowanych przewodów miedzianych, które są skręcone wokół siebie

Jest to zwykle drut o przekroju od 22 do 26 (to jest 0,025 "/ 0,644 mm do 0,016" / 0,405 mm), taki sam, jak w przypadku okablowania telefonicznego. Skręcenie przewodów wokół siebie minimalizuje wpływ zewnętrznego promieniowania elektrycznego na sygnał przenoszony na przewodzie; jeśli napięcie zewnętrzne jest zastosowany do jednego drutu pary, zostanie zastosowany jednakowo do drugiego drutu. Skręcenie skutecznie eliminuje efekt zewnętrznego szumu. Wraz ze wzrostem liczby skrętów na cal poprawia się charakterystyka redukcji szumów; niestety, podobnie jak ogólna ilość kabla i koszt. Większość skrętki dla aplikacji telefonicznych ma 10 do 15 obrotów na stopę. Rodzaj skrętki pokazany na rysunku 6.8 nosi nazwę nieekranowanej skrętki (UTP), ponieważ sama para przewodów nie jest ekranowana. Zdolność przesyłu danych UTP jest ogólnie wskazywana przez jego kategorię:

Kabel poziomu 1 (czasami zwany kodem kategorii 1 lub kat. 1) to starszy kabel o częstotliwości 0,4 MHz, wykorzystywany w niektórych aplikacjach telefonicznych i modemowych, ale generalnie nie nadaje się do aplikacji z danymi.

Kabel poziomu 2 (czasami nazywany kodem kategorii 2 lub kat. 2) to kabel 4 MHz używany w starszych systemach terminalowych, takich jak IBM 3270 BISYNC.

Kable kategorii 3 (kat. 3) mają maksymalną szerokość pasma 16 MHz i są oceniane na 10 Mb / s na odcinku przewodu wynoszącym 100 m (chociaż często można uzyskać prędkości 100 Mb / s). Kabel Cat 3 ma przepustowość do 16 Mb / s i jest używany przede wszystkim do telefonów.

Kabel kategorii 4 (kat. 4) o maksymalnej przepustowości 20 MHz został wykorzystany w 16-bitowych sieciach Token Ring IBM. Dziś nie jest powszechnie postrzegany.

Kabel kategorii 5 (kat. 5) ma maksymalną szerokość pasma 100 MHz i jest oceniany dla głosu lub danych z prędkością do 100 Mb / s na odcinku przewodu wynoszącym 100 metrów. Cat 5e jest przystosowany do sieci Ethernet w trybie pełnego dupleksu i 1 gigabajta (Gb / s). To są najbardziej powszechne kable LAN w użyciu.

Kabel kategorii 6 (kat. 6) ma moc do 250 MHz na odcinku przewodu o długości od 15 do 100 metrów. Cat 6 jest przeznaczony do stosowania w bardzo szybkich aplikacjach szerokopasmowych z szybkością transmisji danych do 10 Gb / s. Przewód Cat 6a jest wariantem Cat 6, oceniane na 500 MHz i 10 Gb / s.

Kabel kategorii 7 (kat. 7) ma znamionową częstotliwość 600 MHz i wykorzystuje cztery pary. Każda para przewodów w osłonie kabla i sama osłona są ekranowane w celu zapobiegania zakłóceniom

elektromagnetycznym przy prędkości transmisji danych do 10 Gb / s. Cat 7a ma przepustowość do 1000 MHz i szybkość transmisji danych 10 Gbps

PARA SKRĘCONA

Medium cieszące się obecnie największą popularnością wśród aplikacji LAN to skrętka. Skrętka składa się z dwóch izolowanych przewodów miedzianych, które są skręcone wokół siebie (patrz Rysunek 6.8). Jest to zwykle drut o przekroju od 22 do 26 (to jest 0,025 "/ 0,644 mm do 0,016" / 0,405 mm), taki sam, jak w przypadku przewodów telefonicznych. Skręcenie przewodów wokół siebie minimalizuje wpływ zewnętrznego promieniowania elektrycznego na sygnał przenoszony na przewodzie; jeśli napięcie zewnętrzne jest zastosowany do jednego drutu pary, zostanie zastosowany jednakowo do drugiego drutu. Skręcenie skutecznie eliminuje efekt zewnętrznego szumu. Wraz ze wzrostem liczby skrętów na cal poprawia się charakterystyka redukcji szumów; niestety, podobnie jak ogólna ilość kabla i koszt. Większość skrętki dla aplikacji telefonicznych ma 10 do 15 obrotów na stopę. Rodzaj skrętki pokazany na rysunku powyżej nosi nazwę nieekranowanej skrętki (UTP), ponieważ sama para przewodów nie jest ekranowana. Zdolność przesyłu danych UTP jest ogólnie wskazywana przez jego kategorię:

Kabel poziomu 1 (czasami zwany kodem kategorii 1 lub kat. 1) to starszy kabel o częstotliwości 0,4 MHz, wykorzystywany w niektórych aplikacjach telefonicznych i modemowych, ale generalnie nie nadaje się do aplikacji z danymi.

Kabel poziomu 2 (czasami nazywany kodem kategorii 2 lub kat. 2) to kabel 4 MHz używany w starszych systemach terminalowych, takich jak IBM 3270 BISYNC.

Kable kategorii 3 (kat. 3) mają maksymalną szerokość pasma 16 MHz i są oceniane na 10 Mb / s na odcinku przewodu wynoszącym 100 m (chociaż często można uzyskać prędkości 100 Mb / s). Kabel Cat 3 ma przepustowość do 16 Mb / s i jest używany przede wszystkim do telefonów.

Kabel kategorii 4 (kat. 4) o maksymalnej przepustowości 20 MHz został wykorzystany w 16-bitowych sieciach Token Ring IBM. Dziś nie jest powszechnie postrzegany.

Kabel kategorii 5 (kat. 5) ma maksymalną szerokość pasma 100 MHz i jest oceniany dla głosu lub danych z prędkością do 100 Mb / s na odcinku przewodu wynoszącym 100 metrów. Cat 5e jest przystosowany do sieci Ethernet w trybie pełnego dupleksu i 1 gigabajta (Gb / s). To są najbardziej powszechne kable LAN w użyciu.

Kabel kategorii 6 (kat. 6) ma moc do 250 MHz na odcinku przewodu o długości od 15 do 100 metrów. Cat 6 jest przeznaczony do stosowania w bardzo szybkich aplikacjach szerokopasmowych z szybkością transmisji danych do 10 Gb / s. Przewód Cat 6a jest wariantem Cat 6, oceniane na 500 MHz i 10 Gb / s.

Kabel kategorii 7 (kat. 7) ma znamionową częstotliwość 600 MHz i wykorzystuje cztery pary. Każda para przewodów w osłonie kabla i sama osłona są ekranowane w celu zapobiegania zakłóceniom elektromagnetycznym przy prędkości transmisji danych do 10 Gb / s. Cat 7a ma przepustowość do 1000 MHz i szybkość transmisji danych 10 Gbps.

UTP jest powszechnie spotykany w fizycznej sieci przewodowej i pierścieniowej LAN; nigdy nie jest używany w fizycznym autobusie i rzadko w fizycznym dzwonku. Podobnie jak w przypadku kabla koncentrycznego, łatwo jest go podsłuchać. Ponadto, wiele sieci LAN wykorzystujących protokół UTP wykonuje również połączenia za pośrednictwem paneli krosujących, które często nie są chronione, ponieważ technicy instalujący połączenia nie są świadomi problemów związanych z bezpieczeństwem, zapewniając scentralizowany dostęp do dziesiątek lub setki połączeń. Innym wariantem skrętki jest ekranowana skrętka (STP), w której każda para przewodów jest otoczona metalową osłoną, która

zapewnia taką samą funkcję jak zewnętrzny przewód w kablu koncentrycznym. Protokół STP był używany tylko w pierścieniu gwiazdowym IBM Token Ring.

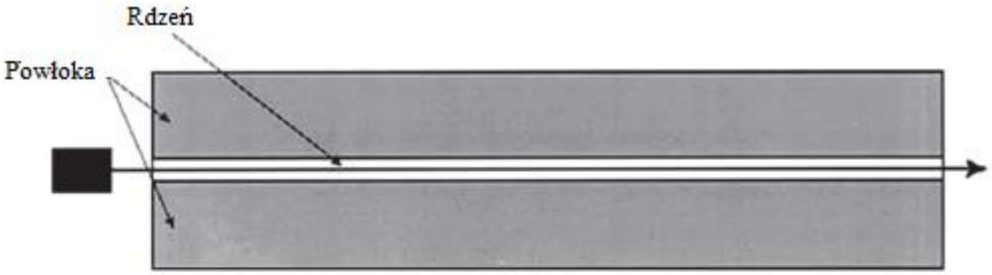
ŚWIATŁOWÓD

Światłowód jest cienkim elastycznym medium, które działa jak falowód dla sygnałów w zakresie 10^{14} - 10^{15} Hz, który obejmuje widmo światła widzialnego i część widma w podczerwieni. Światłowód jest doskonałym medium dla komunikacji cyfrowej; jest zasadniczo odporny na wszelkiego rodzaju zakłócenia radiowe lub magnetyczne i bardzo trudny (przy użyciu wysoko wyspecjalizowanego sprzętu) do ukradkowego ukradkowania. Teoretycznie w stanie w celu osiągnięcia szybkości transmisji danych rzędu bilionów bitów na sekundę, światłowód osiągnął prędkość transmisji danych 100 Gbps na włóknach o długości 4 450 mil (7 000 km); Praktyczny limit jest zwykle spowodowany przez elektronikę wykonującą konwersję optyczno-elektryczną. W aplikacjach WAN ten limit prędkości jest przekraczany na jeden z dwóch sposobów.

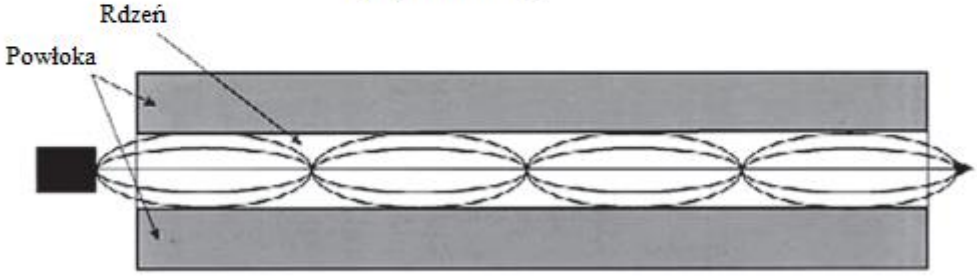
1. Przełącznik optyczny może zakończyć światłowód bez żadnej konwersji elektryczno-optycznej.

2. Gęsto-zwielokrotnione dzielenie falowe (DWDM) pozwala na jednoczesne przenoszenie 100 lub więcej strumieni bitów 10 Gb / s na pojedynczym paśmie włókien. Te technologie mogą w końcu znaleźć drogę do sieci LAN.

Elektronika jest kluczowym elementem każdego systemu światłowodowego. Przychodzący sygnał elektryczny przesyłany na światłowodzie jest przetwarzany na sygnał optyczny przez nadajnik. Typowymi źródłami optycznymi są dioda emitująca światło (LED) lub dioda laserowa wtrysku (ILD). Diody LED są tańsze niż ILD, ale są ograniczone do niższych prędkości. Sygnał optyczny jest odbierany przez urządzenie zwane fotodiodą, które zasadniczo zlicza fotony i konwertuje zliczenie na sygnał elektryczny. Typowe fotodiody to fotodioda pozytywna-negatywna (PIN) i fotodioda lawinowa (APD). Kod PIN jest mniejszy drogie niż APD, ale jest ograniczone do niższych prędkości. Fizyczna i transmisyjna charakterystyka światłowodu są tutaj pokazane



Tryb jednomodowy



Zwielokrotniony indeks wielomodowy

W centrum kabla światłowodowego znajduje się rdzeń, cienki, elastyczny nośnik zdolny do przenoszenia sygnału świetlnego. Rdzeń ma zwykle wielkość od 2 do 125 mikrometrów lub mikronów

o średnicy i mogą być wykonane z różnych szklanych lub plastikowych związków. Otaczający rdzeń jest warstwą zwaną okładziną. Optyczne właściwości okładziny zawsze różnią się od charakterystyki rdzenia, tak że sygnały świetlne przemieszczające się przez rdzeń pod kątem odbijają się i pozostają w rdzeniu. Powłoka może mieć różną grubość od kilku do kilkuset mikronów. Najbardziej zewnętrzną warstwą jest kurtka. Składający się z plastiku lub gumy, jego zadaniem jest zapewnienie kabla z fizyczną ochroną przed wilgocią, przenoszeniem i innymi czynnikami środowiskowymi. Do komunikacji głosowej i transmisji danych wykorzystuje się dwa rodzaje kabli światłowodowych, zróżnicowanych pod względem charakterystyki transmisji. Światłowód wielomodowy (MMF) ma średnicę rdzenia od 50 do 125 µm. Ponieważ ta średnica jest stosunkowo duża, promienie światła pod różnymi kątami będą przemieszczać się przez rdzeń. Zjawisko to, znane jako rozproszenie modalne, ma wpływ na ograniczenie szybkości transmisji i / lub odległości kabla. MMFcable jest zwykle ograniczone do maksymalnej długości kabla wynoszącej 2 km. Światłowód jednomodowy (SMF) eliminuje problem wielu ścieżek MMF, wykorzystując cienki rdzeń o średnicy od 2 do 8 µm. Ten cienkodrutowy kabel zapewnia pojedynczą ścieżkę propagacji, dzięki czemu można osiągnąć bardzo wysokie szerokości pasma na dużych odległościach (do 10 km). SMF jest najdroższym rodzajem światłowodu i jest zwykle wykorzystywany do transmisji danych długodystansowych i sieci telekomunikacyjnych. MMF jest powszechnie używany w sieciach LAN; to jest mniej kosztowne ale nadal może obsługiwać wymagane szybkości transmisji danych i odległości. Kabel optyczny jest niezwykle trudny do podsłuchu, ale łatwo go przyciąć. Takie kable powinny być chronione przez ekranowane przewody, nie umieszczane w dostępnych miejscach, takich jak obok listwy przypodłogowej na podłodze publicznego korytarza - w szpitalu!

MEDIA BEZPRZEWODOWE

Bezprzewodowe sieci LAN wykorzystują sygnały radiowe do łączenia ze sobą węzłów sieci LAN. Bezprzewodowe sieci LAN są coraz powszechniejsze w środowiskach, w których:

* Trudno jest zainstalować nowe okablowanie (np. W budynku z azbestem w ścianach).

* Są użytkownicy mobilni (np. W szpitalu lub wypożyczalni samochodów).

* Trudno jest uzyskać prawo do okablowania (np. Środowiska kampusowe obejmujące jezdnie).

* Potrzebna jest tymczasowa sieć (np. Podczas konferencji lub spotkania).

* Obszary mieszkalne nie mają innych obiektów sieciowych.

* Centra konferencyjne, hotele, szkoły wyższe i uniwersytety potrzebują szerokiego i łatwego dostępu do sieci.

Bezprzewodowe sieci LAN zazwyczaj wykorzystują technologię podczerwieni, rozproszone widmo lub technologię komunikacji mikrofalowej. Podczerwień (IR) jest używana do różnych aplikacji komunikacyjnych, monitorujących i kontrolnych. Jest również używany do takich aplikacji poza siecią LAN, jak zdalne sterowanie domową rozrywką, budowanie zabezpieczeń i detektorów ruchu, medycznych urządzeń diagnostycznych i systemów naprowadzania rakiet. W przypadku bezprzewodowych sieci LAN, najbardziej rozpowszechnione pasmo podczerwieni wykorzystuje sygnały o długości fali w zakresie od 800 do 1000 nanometrów (nm lub 10^{-9}</sup> m). Rozproszone IR działa z szybkością transmisji danych od 1 do 4 Mb / s na odległościach do 200 stóp i może być wykorzystywane do stacjonarnych lub mobilnych węzłów sieci LAN. Directed Beam IR, który wymaga linii wzroku, działa z szybkością transmisji danych od 1 do 10 Mb / s na odległościach do 80 stóp. Systemy IR są ograniczone do jednego pokoju, ponieważ sygnały nie mogą przechodzić przez ściany. Spread spectrum jest technologią komunikacji bezprzewodowej w regionie 2.4 lub 5 gigaherców (GHz lub miliardy cykli na

sekundę), w których rzeczywista częstotliwość nadawanego sygnału jest rozmyślnie zmieniana podczas transmisji. Początkowo przesunięcie częstotliwości było ze względów bezpieczeństwa, aby zapobiec monitorowaniu komunikacji kanały. W sieci LAN stosowane są dwa typy technologii widma rozproszonego:

1. W widmie rozpraszania częstotliwości (FHSS), 3 nadajnik wysyła sygnał na zestaw częstotliwości radiowych przeskakując z częstotliwości na częstotliwość w interwałach podzielonych na sekundy, co wydaje się być sekwencją losową. Sekwencja nie jest losowa, a odbiornik zmienia częstotliwości w synchronizacji z nadajnikiem. FHSS może obsługiwać szybkości transmisji danych od 1 do 3 Mb / s do odległości 330 stóp (100 m).

2. W bezpośrednim widmie rozproszonym (DSSS) każdy bit w pierwotnym strumieniu danych jest reprezentowany przez wiele bitów w transmitowanym sygnale, rozprowadzając sygnał w szerokim zakresie częstotliwości. Jednym z rezultatów DSSS jest to, że system może osiągnąć większą przepustowość niż oryginalny sygnał. DSSS może obsługiwać szybkości transmisji danych przekraczające 20 Mb / s aż do odległości 1000 stóp (300 m).

Innym schematem modulacji wykorzystywanym w bezprzewodowych sieciach LAN jest ortogonalne zwielokrotnianie z podziałem częstotliwości (OFDM). OFDM jest odmianą multipleksowania z podziałem częstotliwości i wykorzystuje przedni układ korekcji błędów i ortogonalne podnośne w celu zminimalizowania przesłuchów częstotliwości i błędów bitowych. Bezprzewodowe punkty dostępowe można kupić za mniej niż 100 USD, co czyni je atrakcyjną alternatywą dla nawet sieci LAN opartych na UTP w wielu scenariuszach. Mikrofalowe sieci LAN odnoszą się do komunikacji w zakresie 1, 5 i 19 GHz. Energia elektromagnetyczna o częstotliwości wyższej niż 1 GHz i prędkości przesyłania danych do 20 Mb / s może być utrzymany na odległość do 130 stóp. Jedną z głównych wad mikrofali jest to, że licencje Federal Communications Commission (FCC) są wymagane dla wielu z tych częstotliwości.

PODSUMOWANIE

We wczesnych latach 80. XX wieku kabel koncentryczny był najczęściej używanym medium LAN. Skrętka, używana do aplikacji telefonicznych, nie była używana w sieciach LAN, ponieważ nie można było osiągnąć wysokich prędkości. Technologia światłowodowa wciąż jest w powijakach i było bardzo drogie. Wszystko to zmieniło się we wczesnych latach dziewięćdziesiątych, kiedy elektronika napędzająca skrętkę znacznie się poprawiła, a technologia światłowodów znacznie się rozwinęła. Rzadko zdarza się, aby kabel współosiowy był używany dzisiaj w sieci LAN; zamiast tego częściej stosuje się UTP (mniej kosztowne niż koncentryczne) lub światłowód (wyższe prędkości niż koncentryczne). Bezalternatywne sieci LAN są realną alternatywą dla sieci przewodowych, ale trudniej ją zabezpieczyć.4 Jednakże wzrost dostępu do sieci Internet pod koniec 2000 r. wyprzedził stacjonarne subskrypcje szerokopasmowe; w 2011 r. tempo wzrostu liczby abonamentów bezprzewodowych było 200 do 300 procent stawek wzrostu dla stałych subskrypcji

Media Access Control

Jak wspomniano, sieci lokalne to sieci rozgłoszeniowe łączące urządzenia równorzędne, wszystkie mające równy dostęp do medium. Te cechy stawiają dwa wymagania dotyczące protokołu kontrolującego dostęp do sieci:

1. Może istnieć tylko jedna stacja nadająca w danym czasie, ponieważ wiele nadajników może powodować zniekształcone wiadomości.

2. Wszystkie stacje muszą przestrzegać tych samych reguł dostępu do sieci, ponieważ nie ma stacji głównej.

Schematy kontrolujące dostęp do nośnika sieciowego nazywane są protokołami kontroli dostępu do nośnika (MAC). Mimo że wiele różnych systemów LAN MAC zostało wprowadzonych do działających produktów, najczęściej są to warianty dwóch podejść: rywalizacji i rozproszonego sondowania. Systemy te zostaną omówione poniżej, wraz z odniesieniem do odpowiedniego standardu LAN IEEE.

RYWALIZACJA

Sieć rywalizacji można porównać do grupy osób siedzących wokół stołu konferencyjnego bez przewodniczącego. Kiedy ktoś chce mówić, najpierw trzeba ustalić, czy ktoś już mówi; jeśli ktoś mówi, nikt nie może zacząć, dopóki ta osoba się nie zatrzyma. Kiedy dana osoba wykryje ciszę przy stole, zaczyna mówić. Jeśli dwoje ludzi zacznie rozmawiać w tym samym czasie, doszło do kolizji i trzeba ją rozwiązać. W ludzkiej analogii zderzenia są rozwiązywane na jeden z dwóch sposobów: albo obydwa głośniki zatrzymują się i odkładają do siebie ("grzeczne wycofanie"), albo obydwa kontynuują mówienie głośniej i głośniej, aż się poddaje ("algorytm grubiaństwa"). Schemat rywalizacji używany w sieciach lokalnych jest podobny do sytuacji zwrotnej i jest nazywany dostępem wielu osób z wykrywaniem kolizji (CSMA / CD). CSMA / CD jest jednym z najstarszych używanych obecnie systemów MAC MAC, używanych początkowo w sieci Ethernet i stając się podstawą standardu IEEE 802.3 (do opisania). Chociaż w sieciach LAN stosowane były inne systemy rywalizacji, CSMA / CD to taki, który przetrwał i dobrze prosperuje na rynku. CSMA / CDworks w logicznych sieciach magistrali. Kiedy stacja jest gotowa do nadawania, najpierw słucha medium sieciowego ("sens przewoźnika"). Jeśli stacja wykryje transmisję na linii, będzie nadal monitorować kanał, dopóki nie będzie bezczynny. Po wykryciu ciszy stacja z wiadomością do wysłania zacznie nadawać. Stacje kontynuują monitorowanie kanału podczas transmisji, tak że po wykryciu kolizji wszystkie nadajniki przestają nadawać. Sieci CSMA / CD wykorzystują schemat przesunięcia, aby pierwsza kolizja nie spowodowała zmniejszenia sieci. Bez schematu cofania wszystkie nadajniki wykryłyby kolizję i przestałyby transmitować; po ponownym usłyszeniu ciszy na linii wszystkie stacje znowu zaczną nadawać i znów będą się ze sobą zderzać. Schemat wycofania powoduje, że stacje podejmują losową decyzję, czy wysłać, czy nie, po wykryciu ciszy na kanale po wystąpieniu kolizji. CSMA / CD używa schematu wycofania zwanego obcym odgórnym wykładniczym ekspresem. Chociaż nazwa ta jest pełna, to bardzo dokładnie opisuje ten proces. Kiedy stacja jest gotowa do nadawania i wykrywa ciszę na linii, spróbuje wysłać wiadomość z prawdopodobieństwem 1 (tj. 100% prawdopodobieństwa, że będzie transmitować); prawdopodobieństwo to nazywa się trwałością schematu MAC. Jeśli dojdzie do kolizji, stacja przestanie nadawać i ponownie zaczeka na milczenie na linii. Gdy ponownie wykryta zostanie cisza, stacja będzie transmitować z prawdopodobieństwem 1/2 (tj. Istnieje 50 procent szans, że przekaże i 50 procent szans, że nie). Jeśli dwie koleje były zaangażowane w kolizję i oboje cofają się do stanu trwającego 1/2, to istnieje 50 procent szans, że jeden przekaże, a jeden odroczy od następnej okazji transmisji, 25 procent szans, że oba odstąpić od następnej szansy i 25 procent szansy, że oba zderzają się ponownie Jeśli stacja zderzy się ponownie, jej wytrzymałość ponownie zostanie przecięta na pół, teraz do 1/4. Wszystkie stacje biorące udział w zderzeniu upuszczają swoją trwałość, a każda stacja niezależnie określa, czy przekaże przy następnym wystąpieniu ciszy, czy nie. Tak długo, jak zdarzają się kolizje, trwałość jest przecinana na pół do momentu, gdy stacja pomyślnie transmituje lub ma 16 nieudanych prób przesłania wiadomości. Po 16 nieudanych próbach stacja się poddaje. Po tym, jak stacja pomyślnie przesyła lub ma 16 nieudanych prób, trwałość stacji powraca do 1, a operacja trwa tak jak poprzednio. Bezprzewodowe sieci LAN również używają formy rywalizacji, ale ogólnie nie jest to CSMA / CD, ponieważ wykrywanie kolizji nie jest praktyczne w środowisku bezprzewodowym. Zamiast tego stacje nadal używają CSMA - nasłuchują kanału bezczynnego - ale niekoniecznie transmitują, gdy kanał jest bezczynny. Zamiast tego, czekają, aby sprawdzić, czy kanał pozostaje bezczynny przez jakiś czas, próbując powstrzymać kolizję. Jest to forma CSMA z unikaniem kolizji (CSMA / CA).

ROZPOROSZONE POBIERANIE

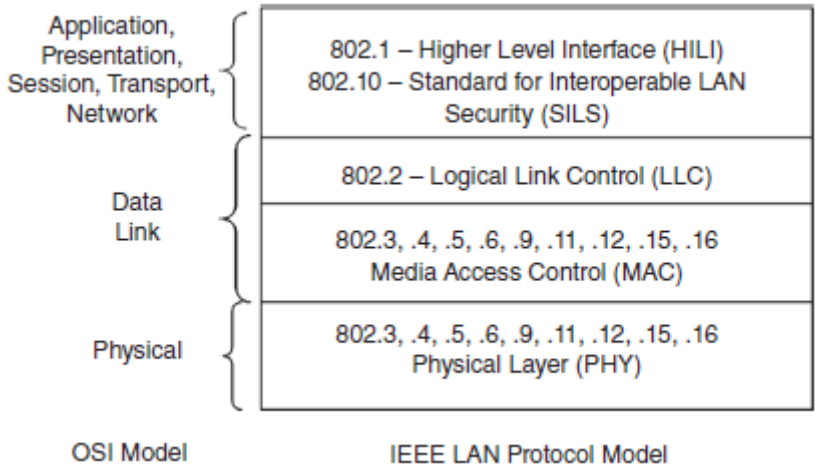
Wyobraź sobie, że ta sama grupa ludzi siedzi przy tym samym stole konferencyjnym, wciąż bez przewodniczącego. Jedna osoba przy stole ma mikrofon i może powiedzieć cokolwiek komukolwiek w pokoju. Wszyscy w pokoju, oczywiście usłyszą wiadomość. Zasada jest taka, że jedyną osobą, która może mówić, jest ta, która ma mikrofon; co więcej, osoba będzie trzymała się mikrofonu tylko wtedy, gdy ma coś do powiedzenia i może go przytrzymać tylko przez pewien maksymalny czas. Gdy pierwsza osoba skończy rozmowę lub upłynie termin, mikrofon zostanie przekazany kolejnej osobie przy stole. Osoba 2 może teraz mówić lub natychmiast przekazać mikrofon osobie 3. Ostatecznie pierwsza osoba przy stole otrzyma mikrofon z powrotem i dostanie kolejną okazję do rozmowy. Opisany schemat jest implementowany w sieciach LAN ze schematem zwanym tokenem przechodzącym. Jest to podstawą dla IBM Token Ring i stanowi drugi najczęściej stosowany algorytm LAN MAC. Przekazywanie tokena, w jednym lub drugim wariancie, jest podstawą standardów IEEE 802.4 i 802.5, a także dla FDDI (Fiber Distributed Data Interface). Przekazywanie tokenów wymaga logicznej topologii pierścienia. Kiedy stacja ma dane do wysłania inna stacja, musi czekać, aż otrzyma wzór bitowy reprezentujący token. Tokeny są wysyłane w taki sposób, że tylko jedna stacja będzie je widzieć w danym momencie; w ten sposób, jeśli stacja widzi token, ma tymczasową, wyłączną własność sieci. Jeśli stacja otrzymuje token i nie ma danych do wysłania, przekazuje token. Jeśli ma dane do wysłania, generuje ramkę zawierającą dane. Po wysłaniu ramki stacja wygeneruje i wyśle kolejny token. Sieć token ring jest logicznym pierścieniem zaimplementowanym w fizycznej topologii, która obsługuje operację emisji szeregowej (to jest gwiazdę lub pierścień). Każda stacja odbiera transmisje bitów na raz i regeneruje bity dla następnej stacji. Stacja transmitująca ramkę przesyła bity na swoim łączu wyjściowym i odbiera je z powrotem na swoim łączu wejściowym. Nadajnik jest odpowiedzialny za usunięcie swojej wiadomości z sieci. Po zakończeniu nadawania stacja przekazuje sterowanie do innej stacji wysyłając bity zawierające token na wyjściowym łączu. Następna stacja na pierścieniu, która chce nadawać i widzi token, może następnie wysłać swoją ramkę danych. Pierścienie Token (standaryzowane w 802.5 i FDDI) są najczęstszą implementacją przekazywania tokena. Sieć Token Bus (jak określono w 802.4) jest koncepcyjnie podobna do tokena, z tym wyjątkiem, że jest zaimplementowana przy użyciu równoczesnej topologii rozgłoszeniowej (to jest magistrali). W tej fizycznej topologii wszystkie stacje słyszą wszystkie transmisje. Stacja, która chce przesłać dane do drugiej, będzie adresować ramkę do docelowego odbiornika w sieci, jak w szynie CSMA / CD. Po zakończeniu transmisji stacja przekaże tokenowi do następnej stacji logicznie w pierścieniu; podczas gdy wszystkie stacje będą słyszeć transmisję tokenu, tylko jedna stacja, do której jest adresowana, odbierze ją. Po otrzymaniu tokena stacja może lub nie może przesyłać danych, ale w każdym przypadku jest odpowiedzialna za przekazanie tokena do następnej stacji w pierścieniu logicznym. W końcu token powróci na pierwszą stację.

PROTOKOŁY I STANDARDY LAN

Model referencyjny Open Systems Interconnection (OSI) nadal stanowi standardową platformę, za pomocą której można opisywać architektury komunikacji danych, w tym architektury sieci LAN. Podstawowa architektura protokołu LAN łatwo odwzorowuje model OSI

MODELE OSI A ARCHITEKTURA SIECI LAN

Chociaż architektura protokołu LAN może być powiązana z modelem OSI, nie ma doskonałego odwzorowania typu "jeden do jednego" warstw protokołów



Warstwa fizyczna OSI jest analogiczna do warstwy fizycznej LAN (PHY). Oba określają takie rzeczy jak:

* Charakterystyka elektryczna interfejsu

* Charakterystyka mechaniczna złącza i medium

* Obwody interfejsów i ich funkcje

* Właściwości medium

* Szybkość sygnalizacji

* Metoda sygnalizacji

Większość specyfikacji warstwy fizycznej LAN zawiera dwie podwarstwy. Niższa podwarstwa opisuje aspekty warstwy fizycznej, które są specyficzne dla danego medium; wyższa podwarstwa opisuje te aspekty, które są niezależne od nośnika. Warstwa łącza danych OSI, odpowiedzialna za komunikację bezbłędną między dowolnymi dwoma urządzeniami komunikacyjnymi, jest reprezentowana przez dwie podwarstwy w sieci LAN. Niższą podwarstwą jest MAC, który zajmuje się problemami, w jaki sposób stacja powinna uzyskać dostęp do medium sieciowego. MAC jest odpowiedzialny za komunikację bezbłędną nad PHY i określa takie rzeczy jak:

* Ramy

* Adresowanie

* Wykrywanie błędów bitowych

* Kontrola i utrzymanie protokołu MAC

* Zasady dotyczące dostępu do medium

Górna podwarstwa nazywa się Logic Link Control (LLC). Protokół LLC jest odpowiedzialny za utrzymywanie logicznego połączenia między dwiema komunikującymi się stacjami LAN. LLC określa takie zasady, jak:

* Sekwencjonowanie ramek

* Kontrola błędów

* Ustanowienie i zakończenie połączenia logicznego

* Adresowanie usług wyższej warstwy

Przypominając, że główne funkcje warstwy sieci to routing i kontrola przeciążenia, istnieją dwa powody, dla których żadna warstwa protokołu LAN nie działa tak jak warstwa sieciowa OSI:

1. Nie ma potrzeby stosowania algorytmu routingu w sieci rozgłoszeniowej, ponieważ wszystkie stacje odbierają wszystkie transmisje; adres odbiorcy jest zawarty w samej przekładni.

2. Kontrola nad zatorami również nie stanowi problemu w sieci rozgłoszeniowej; sieć rozgłoszeniowa musi być ograniczona do jednego nadajnika na raz, a jest to realizowane przez warstwę MAC.

Nie ma standardów dla sieci LAN odpowiadających wyższym czterem warstwom modelu OSI. Nawet w mniej zorganizowanych latach 80. protokoły end-to-end jako takie nie były wymagane w środowisku sieci LAN, ponieważ komunikacja typu "end-to-end" była ograniczona do węzłów w sieci LAN, a do tego MAC gwarantował komunikację bezbłędną. Dopiero gdy popularność sieci LAN, poprzez dostęp WAN i LAN do Internetu, zyskała popularność, konieczne stały się inne protokoły end-to-end. IP (i inne protokoły warstwy sieciowej) również zyskały na popycie. Te protokoły są powiązane z oprogramowaniem komunikacyjnym w ramach sieciowego systemu operacyjnego (NOS) i zostaną omówione później.

STANDARDY IEEF 802

Chociaż nie są one bezpośrednio związane z bezpieczeństwem, warto zapoznać się ze standardami opisującymi sieci lokalne, z których najczęstszymi są standardy IEEE 802. IEEE Computer Society utworzyło Komitet ds. Projektu 802 w lutym 1980 r. W celu stworzenia norm dla sieci LAN w ramach bardziej ogólnych prac nad standardami dla mikroprocesorów; żadna inna organizacja nie podejmowała podobnych działań normalizacyjnych. Pierwotnie miał istnieć jeden standard sieci LAN, działający z prędkością od 1 do 20 Mb / s. Standard został podzielony na trzy części: PHY, MAC i interfejs wysokiego poziomu (HILI), aby umożliwić innym pakietom protokołów posiadanie wspólnej granicy protokołu z siecią LAN. Pierwotny MAC był oparty na standardzie Ethernet, ale inne programy MAC zostały szybko dodane i, z biegiem lat, komitet 802 odniósł się do wielu schematów LAN. Wszystkie mają wspólną cechę interfejsu do pojedynczego protokołu LLC, który zapewnia wspólny interfejs między HILI i dowolnym MAC. Opis grup roboczych Projektu 802 (WG) i ich stan na październik 2012

802.1-WARSTWOWA SIEĆ LAN Protocols Working Group. Zapewnia ramy dla zagadnień wyższych warstw, w tym architektury protokołów, zabezpieczeń, protokołów typu end-to-end, mostowania, pracy w Internecie, zarządzania siecią i pomiaru wydajności.

802.2-GRUPA ROBOCZA KONTROLI LOGICZNEJ ŁĄCZA. Zapewnia spójny interfejs pomiędzy dowolnymi protokołami LANMAC i warstwami wyższymi. W zależności od zastosowanych opcji, LLC może zapewnić wykrywanie i korekcję błędów, dostarczanie sekwencyjne i kapsułkowanie wieloprotokołowe. Ta WG została rozwiązana

802.3- GRUPA ROBOCZA ETHERNET. Definiuje specyfikacje MAC i PHY dla sieci magistrali CSMA / CD.

802.4-TOKEN BUS WORKING GROUP. Definiuje specyfikacje MAC i PHY dla linii przesyłającej tokeny w oparciu o prace pierwotnie wykonane w General Motors w ramach protokołu Manufacturing Automation Protocol (MAP). Odpowiedni do posadzek fabrycznych i linii montażowych, MAP nigdy nie osiągnął szerokiego zastosowania. Ta WG została rozwiązana.

802.5- GRUPA ROBOCZA TOKEN RING. Definiuje specyfikacje MAC i PHY dla pierścienia przechodzącego tokena.

802.6- GRUPA ROBOCZA , METROPOLITAN AREA NETWORK (MAN). Definiuje specyfikacje MAC i PHY dla MAN. W szczególności, standard 802.6 definiuje MAC i PHY o nazwie Distributed Queue Dual Bus

(DQDB), który był jednym z MAC wykorzystywanych w Switched Multimegabit Data Service (SMDS) i Wirelessless Data Broadcast Service (CBDS). Wprowadzone na początku lat 90. XX wieku, żadna z tych usług nie jest w użyciu. Ta WG została rozwiązana.

802.7-GRUPA DORADCZAS DS. TECHNOLOGII SZEROKOPASMOWYH(BBTAG). Doradza innym podkomisjom 802 dotyczącym zmian w technologii szerokopasmowej i ich wpływowi na standardy 802. Ta WG została rozwiązana.

802.8 – GRUPA DORADCZA DS. TECHNOLOGII ŚWIATŁOWODOWEJ(FOTAG). Doradza innym podkomisjom 802 dotyczącym zmian w technologii światłowodów i ich wpływowi na standardy 802. Ta WG została rozwiązana.

802.9- GRUPA ROBOCZA INTEGRATED SERVICES LAN (ISLAN). Definiuje specyfikacje MAC i PHY dla zintegrowanego dostępu terminala głosowego / danych do zintegrowanych sieci usług, w tym ISLAN i MAN oraz usług zintegrowanych . sieci cyfrowe (ISDN). Jedyną praktyczną implementację wdrożono w produktach IsoEthernet, opisanych w standardzie IEEE 802.9a. Ta WG została rozwiązana.

802.10. – GRUPA ROBOCZA DS. BEZPIECZEŃSTWA. Definiuje procedury zapewniania mechanizmów bezpieczeństwa w połączonych sieciach lokalnych, w tym kryptografii i certyfikatów. Ta WG została rozwiązana.

802.11- GRUPA ROBOCZA WIRELESS LAN (WLAN). Definiuje specyfikacje MAC i PHY dla nośnika "przez powietrze". Oryginalna standardowa operacja standardu 802.11 zdefiniowała operację z szybkością 1 lub 2 Mb / s przy użyciu pasma 2,4 GHz i technologii rozproszonego widma DSSS lub FHSS; nominalne maksymalne odległości wynosiły 330 stóp (100 m). Najczęstsze obecnie dostępne warianty to:

* 802.11b - prędkość przesyłu danych do 11 Mb / s przy nominalnej maksymalnej odległości do 460 stóp (140 m) na częstotliwości 2,4 GHz za pomocą DSSS.

* Szybkość 802.11g do 54 Mb / s przy nominalnej maksymalnej odległości do 460 stóp (140 m) na częstotliwości 2,4 GHz z wykorzystaniem DSSS lub OFDM.

* Szybkość 802.11n-danych do 150 Mb / s przy nominalnej maksymalnej odległości do 820 stóp (250 m) na częstotliwości 2,4 lub 5 GHz z wykorzystaniem OFDM. Oczekuje się, że przyszłe standardy 802.11 zapewnią szybkość przesyłania danych do 82,7 Mb / s przy częstotliwości 5 GHz z wykorzystaniem OFDM.

802.12 - Grupa robocza ds. Priorytetu zapotrzebowania: Opisuje jedną ze specyfikacji MAC i PHY pierwotnie proponowanych dla prędkości 100 Mb / s LAN i dubbingowanych 100BASE-VG / AnyLAN. W dużej mierze niewykorzystany, a grupa robocza została rozwiązana.

802.13. (Ten numer nigdy nie został przypisany do WG, ponieważ uważano, że 13 przeszkodziłoby produktom na rynku.)

802.14. - GRUPA ROBOCZA MODEMU KABLOWEGO. Pierwotnie przeznaczone do opisywania sieci LAN dla systemów telewizji kablowej. Ta WG została rozwiązana.

802.15- GRUPA ROBOCZA WIRELESS PERSONAL AREA NETWORK (WPAN). Definiuje MAC i PHY dla krótkiej sieci bezprzewodowej pomiędzy urządzeniami przenośnymi i mobilnymi, takimi jak komputery osobiste, urządzenia PDA, telefony komórkowe, pagery i inny sprzęt komunikacyjny.

802.16- GRUPA ROBOCZA BROADBAND WIRELESS ACCESS (BBWA). Określa MAC i PHY dla szybkiego dostępu do sieci bezprzewodowej na stosunkowo krótkich odległościach. Standardy BBWA odnoszą się do połączenia "pierwsza mila / ostatnia mila" w bezprzewodowych sieciach metropolitalnych,

rozszerzając zasięg mieszkaniowych usług szerokopasmowych, takich jak modem kablowy lub cyfrowa linia abonencka (DSL).

802.17 — GRUPA ROBOCZA Resilient Packet Ring (RPR). Definiuje standardy wspierające rozwój i wdrażanie lokalnych, metropolitalnych i rozległych sieci RPR w celu elastycznego i wydajnego transferu pakietów danych z szybkością skalowalną do wielu gigabitów na sekundę. Ta grupa robocza znajduje się obecnie w stanie hibernacji

802.18-TECHNICZNA GRUPA DORADCZA DS. REGULACJI RADIOWYCH (RR-TAG). W imieniu innych 802 WG, wykorzystujących komunikację radiową, ta TAG monitoruje i aktywnie uczestniczy w bieżących krajowych i międzynarodowych działaniach regulacyjnych związanych z radiem.

802.19-Wireless Coexistence Working Group. Opracowuje i utrzymuje polityki określające obowiązki 802 deweloperów standardów w zakresie rozwiązywania problemów współistnienia z istniejącymi standardami i innymi normami będącymi w trakcie opracowywania.

802.20 - GRUPA ROBOCZA MOBILNEGO DOSTĘPU SZEROKOPASMOWEGO(MBWA). Określa specyfikację interfejsu bezprzewodowego opartego na pakietach, zoptymalizowanego dla usług opartych na protokole IP. Celem jest umożliwienie ogólnoświatowego wdrażania niedrogich, wszechobecnych bezprzewodowych sieci szerokopasmowych , sieci dostępowe, które spełniają potrzeby biznesowe i mieszkaniowe rynki użytkowników końcowych. Ta grupa robocza znajduje się obecnie w stanie hibernacji.

802.21-GRUPA ROBOCZA DS. NIEZALEŻNEGO PRZEKAZYWANIA MEDIÓW. Opracowanie norm umożliwiających przekazywanie i współdziałanie między heterogenicznymi typami sieci, w tym sieciami 802 i nie-802.

802.22- GRUPA ROBOCZA WIRELESS REGIONAL AREA NETWORKS. Opracowanie standardu dla radiowego interfejsu PHY, MAC i interfejsu lotniczego do użytku przez urządzenia nieobjęte licencją na zasadzie nieinterferowania w widmie przydzielonym do telewizji.

802.23-GRUPA ROBOCZA DS. SYTUACJI NADZWYCZAJNYH. Ta grupa robocza została stworzona w celu zdefiniowania struktury IEEE 802 dla sieci LAN, która byłaby zgodna z odpowiednimi wymaganiami władz cywilnych dla systemów komunikacyjnych. Ta grupa robocza została rozwiązana.

802.24-Smart Grid Technology Advisory Group. Ta TAG została stworzona w celu zapewnienia łączności między komitetem 802 a przemysłem inteligentnym i organami regulacyjnymi oraz w celu zapewnienia koordynacji i współpracy między 802 grupami roboczymi zajmującymi się inteligentnymi sieciami.

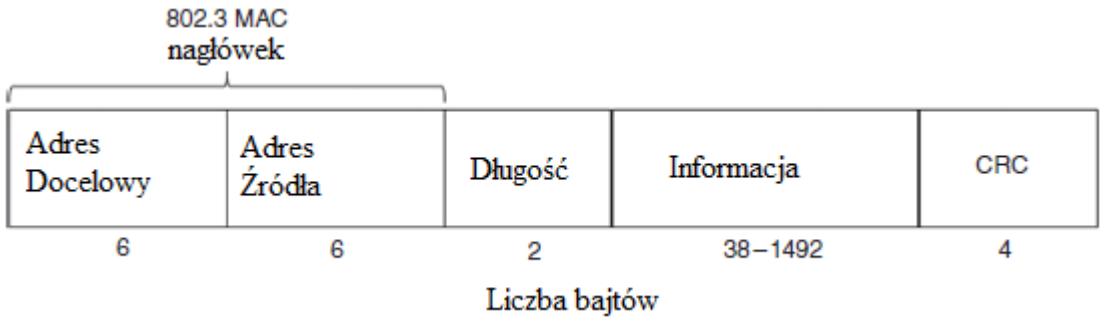
STANDARD IEEE 802.3 CSMA / CD

Oryginalny standard IEEE 802.3, opublikowany po raz pierwszy w 1985 roku, opisuje PHY i MAC dla sieci magistrali CSMA / CD działającej na grubym kablu koncentrycznym. Obecnie implementacja sieci 802.3 może wykorzystywać dowolne typy mediów, w tym UTP i światłowód. Bez wątpienia najpopularniejsze są starsze wersje UTP. Komitet 802.3 przewidział różne rodzaje mediów, które mogą być używane, i opracował nazewnictwo w celu identyfikacji rzeczywistej fizycznej realizacji, przy użyciu formatu:

[szybkość (Mbps)] [typ sygnalizacji] [długość segmentu (m) lub typ nośnika]

Oryginalna specyfikacja 802.3, na przykład, działała z szybkością 10 Mb / s, wykorzystywała sygnalizację pasma podstawowego (cyfrową) i ograniczała pojedynczy odcinek kabla koncentrycznego do długości

500 m (1640 stóp); kabel został oznaczony jako 10BASE5. W rzeczywistości, największa odległość między dwiema stacjami 802,3 mogłaby wynosić 2,8 km (9200 stóp), więc wzmacniacze mogą być używane do połączenia kilku kabli koncentrycznych o długości 500 m. Niedawno wprowadzono tańszą wersję, zwaną CheaperNet, działającą na cienkich koncentrycznych kablach ograniczonych do 185 m (610 stóp); ta PHY jest oznaczona 10BASE2. W połowie lat osiemdziesiątych firma AT & T wprowadziła produkt o nazwie StarLAN, który działał z szybkością 1 Mb / s na UTP. Mimo że produkt ten od dawna pozostawał nieczytelny, był pierwszym, który przełamał barierę 1 Mb / s na UTP. Kolejne wersje 802.3, które wykorzystują UTP, wykorzystują topologię gwiazdy, w której każdy węzeł sieci łączy się bezpośrednio z centralnym koncentratorem. Pierwsza 10-Mbps wersja 802.3 została oznaczona jako 10BASE-T, oznaczające użycie nośnika UTP (które według standardu okablowania jest ograniczone do odległości 100 m lub 330 stóp). Wersja światłowodu 10 Mb / s 802.3 to 10BASE-F. Obecnie dostępne są oczywiście wersje 100 Mb / s i 1 Gb / s (np. 100BASE-T i 1000BASE-T). Technologia Full-duplex Ethernet wykorzystuje połączenia punkt-punkt w konfiguracji gwiazdy i skutecznie podwaja prędkość linii, umożliwiając jednocześnie obu stacjom transmisję. Ilustracja pokazuje format ramki IEEE 802.3MAC, głównie w celach informacyjnych.



Pola i ich funkcje to:

* Preambuła. Używany do synchronizacji zegara; zatrudnia 7 powtórzeń 8-bitowego wzorca 10101010. (8 bitowych bitów = 1 bajt = 1 oktet)

* Rozpocznij ogranicznik ramki (SFD). Wzór bitowy 10101011 oznacza faktyczny początek ramki. 1 oktet.

* Adres docelowy (DA). 48-bitowy adres MAC stacji, która powinna otrzymać tę ramkę. Adres all-1s w 48 bitach binarnych (ff-ff-ff-ff-ff-ff w systemie szesnastkowym) to adres rozgłoszeniowy, wskazujący, że wszystkie stacje powinny otrzymać ten komunikat.

* Adres źródłowy (SA). 48-bitowy adres MAC stacji wysyłającej tę ramkę.

* Długość. Liczba oktetów w polu danych LLC, wartość od 0 do 1500. 2 oktety.

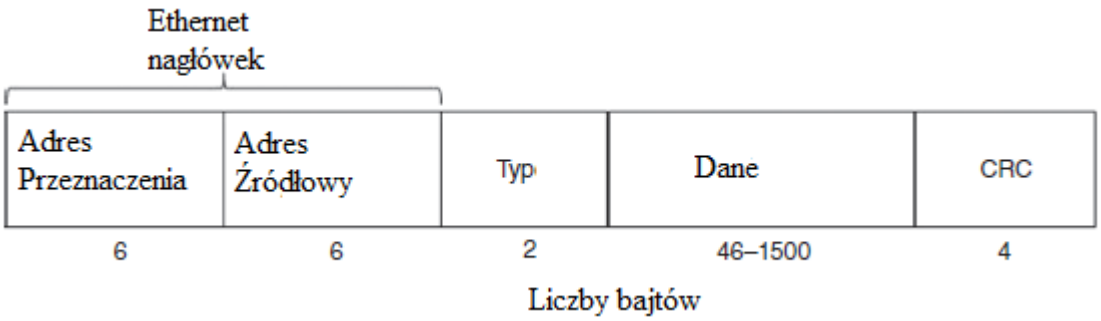
*Dane LLC. Dane z LLC (i wyższych warstw). To pole zawiera 3-oktetowy nagłówek LLC, nagłówek 5-oktetowy 802.2 podsieciowego dostępu do protokołu (SNAP) i od 38 do 1492 oktetów danych wyższej warstwy.

* Pad. Dodatkowe oktety, aby ramka miała co najmniej długość 64 oktetów; to minimum jest wymagane przez sieci CSMA / CD jako część mechanizmu wykrywania kolizji.

* Kolejność sprawdzania ramki (FCS). Pozostały czas obliczeń CRC-32 wykorzystywanych do wykrywania błędów bitowych. 4 oktety.

Ethernet II Standard CSMA / CD IEEE oparty jest na specyfikacji Ethernet opracowanej w Xerox's Palo Alto Research Center (PARC) w połowie lat siedemdziesiątych. Kiedy Xerox po raz pierwszy zdecydował

się wprowadzić na rynek Ethernet, nie było modelu OSI ani żadnych standardów lub produktów sieci LAN. Biorąc pod uwagę to środowisko, Xerox poszukiwał wsparcia dla tej nowej specyfikacji. Specyfikacja Ethernetu została wspólnie rozprowadzona (i sprzedana) przez Digital Equipment Corporation (DEC, teraz Compaq), Intel i Xerox (stąd czasami znany jako Ethernet DIX). Podczas gdy standard 802.3 opiera się na Ethernecie II, dwa nie są dokładnie takie same. Ilustracja 6.12 pokazuje format ramki Ethernet MAC, głównie w celu porównania z ramką IEEE.



Pola i ich funkcje to:

* Preambuła. Używany do synchronizacji zegara; stosuje wzór bitowy 10101010 ... 10101011. 8 oktetów.

* Adres docelowy (DA). 48-bitowy adres MAC stacji, która powinna otrzymać tę ramkę. Adres all-1s (ff-ff-ff-ff-ff-ff) to adres rozgłoszeniowy, wskazujący, że wszystkie stacje powinny otrzymać ten komunikat.

* Adres źródłowy (SA). 48-bitowy adres MAC stacji wysyłającej tę ramkę.

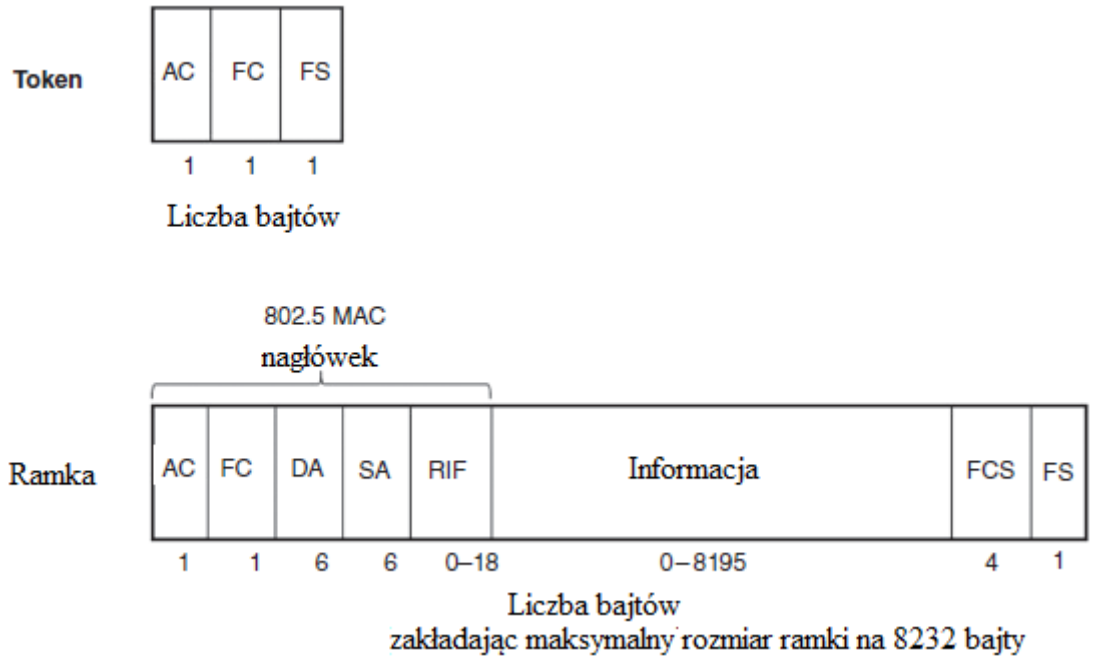
* Identyfikator protokołu (PID). Wskaźnik informacji o protokole transportowany w polu Informacje. Przykładowe wartości obejmują wartości 2048 i 2054, aby wskazać odpowiednio protokół internetowy (IP) i protokół ARP (Address Resolution Protocol). 2 oktety.

* Informacja. Jednostka danych protokołu z protokołu określonego w polu PID. 46 do 1500 oktetów. (Obowiązkiem wyższej warstwy jest zapewnienie, że w ramce znajdują się co najmniej 46 oktetów danych.)

* Kolejność sprawdzania ramki (FCS). Pozostały czas obliczeń CRC-32 wykorzystywanych do wykrywania błędów bitowych. 4 oktety.

Punkt porównywania formatów ramek Ethernetu i 802.3 ma przede wszystkim charakter historyczny, ponieważ dzisiejsze implementacje to 802.3, a nie Ethernet. To powiedziawszy, warto zauważyć, że te dwie specyfikacje są w rzeczywistości różne. Być może jest to drobnostka i było powszechnie mylące w branży odniesienie do Ethernetu IEEE 802.3 (nawet komitet IEEE 802.3 jest teraz znany jako Grupa EthernetWorking), ale była to ważna różnica zarówno dla administratora sieci, jak i dla specjalista ds. bezpieczeństwa. W szczególności, w przeszłości, jeśli jedno urządzenie LAN zrozumiało enkapsulację Ethernet, nie byłoby w stanie skutecznie komunikować się z innym urządzeniem LAN, które rozumiało tylko enkapsulację IEEE 802.3. Oba urządzenia mogą jednak współdzielić ten sam szkielet medium, ponieważ elektronika jest taka sama. Na przykład serwer NetWare z protokołem warstwy sieciowej IPX (Internetwork Packet Exchange) na podstawie ramek IEEE 802.3 może z łatwością dzielić się siecią z hostem systemu UNIX z protokołem IP przez Ethernet, ale utrzymuje pewną odporność na ataki hosta IP dla systemu NetWare serwer, ponieważ obie sieci nie mogły się komunikować.

STANDARD TOKEN-RING IEEE 802.5 Standard Token-Ring IEEE 802.5 został oparty na produkcie IBM o tej samej nazwie. Zarówno standard, jak i produkt pochodzą z około 1985 roku. Zostało to opisane tutaj dla celów historycznych. Pierścień tokenów ma logiczną topologię pierścieni, chociaż został zbudowany jako gwiazda fizyczna. Zaprojektowany do pracy z kablem STP lub UTP, większość implementacji działa z prędkością 16 Mb / s lub wyższą. Adres MAC 802.5 był w zasadzie taki sam jak schemat przekazania tokena. Pola ramki MAC



są to:

* Rozpocznij ogranicznik (SD). Zaznacza faktyczny początek transmisji. Wzór bitowy JK0JK000, gdzie J i K reprezentują specjalne symbole na linii.11 1 oktet.

* Kontrola dostępu (AC). Wskazuje, czy ta transmisja jest tokenem (to jest brak danych), czy ramką (to znaczy zawiera dane). To pole zawiera również informacje o priorytecie tej transmisji. 1 oktet.

* Kontrola ramki (FC). Wskazuje, czy ta ramka zawiera dane dotyczące LLC (i wyższej warstwy) lub informacje zarządzania MAC; jeśli jest to informacja specyficzna dla MAC, to pole wskazuje również typ ramki MAC. 1 oktet.

* Adres docelowy (DA). 48-bitowy adres MAC stacji, do której przeznaczona jest ta ramka.

* Adres źródłowy (SA). 48-bitowy adres MAC stacji wysyłającej tę ramkę.

* Pole informacji o routingu (RIF). Pole opcjonalne, używane tylko w sieciach wielopierścieniowych wykorzystujących routing źródłowy i w którym zamierzony odbiornik znajduje się na innym pierścieniu niż nadajnik. W routingu źródłowym, nadajnik może określić zamierzoną ścieżkę tej ramki, wyznaczając do ośmiu pośrednich sieci.12 do 18 oktetów.

* Informacje (INFO). Zawiera ramkę LLC lub informacje zarządzania MAC. Maksymalna długość nie jest określona przez standard, ale długość tego pola będzie ograniczona przez czas wymagany do przesłania całej ramki, kontrolowany przez parametr czasu oczekiwania na token.

* Kolejność sprawdzania ramki (FCS). Pozostałości z obliczeń CRC-32 w celu wykrycia błędów bitowych w ramce. 4 oktety.

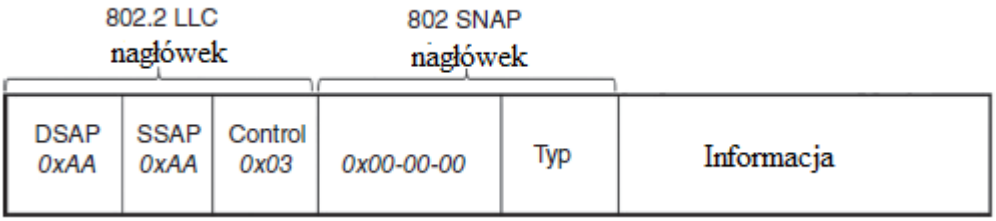
* End delimiter (ED). Sygnalizuje koniec transmisji, ze wzorem bitowym JK1JK1IE, gdzie J i K są takie, jak opisano w polu SD. I-bit wskazuje, czy ta ramka jest ostatnią klatką z sekwencji wielu klatek, a E-bit wskazuje, czy błąd został wykryty przez odbiornik (E); bity te są usuwane przez oryginalnego nadawcę, gdy ramka powraca do tej stacji. 1 oktet.

* Status ramki (FS). Wzór bitowy AC00AC00; bity te wskazują, czy adres docelowy ramki został rozpoznany przez dowolną stację w sieci (A) i czy ta klatka została pomyślnie skopiowana przez zamierzonego odbiorcę (C). 1 oktet.

Jak pokazano, token zawiera tylko trzy oktety, pola SD, AC i ED. Stacja wysyła ramkę zawsze, gdy istnieją dane użytkownika lub informacje o adresie MAC do wysłania. Stacja musi czekać, aż otrzyma token, zanim wygeneruje ramkę. Stacja nadawcza jest odpowiedzialna za wygenerowanie nowego tokena po przesłaniu pojedynczej ramki. Przypomnij sobie, że przesłane bity powracają do nadawcy i to ta stacja usuwa bity z sieci. Zgodnie z pierwotnym standardem, nadajnik wyśle token po wysłaniu wszystkich bitów ramki i musi poczekać, aż zobaczy co najmniej powracające pole SA, aby sprawdzić, czy faktycznie usuwa własną ramkę z sieci. Opcjonalnie wczesne wydanie tokena umożliwia nadajnikowi generowanie nowego tokenu natychmiast po zakończeniu wysyłania bitów z jego ramki, nawet jeśli pole SA jeszcze nie zostało zwrócone. Ta ostatnia opcja została opracowana w celu poprawy wydajności w bardzo dużych środowiskach typu Token Ring, takich jak standard FDDI American National Standards Institute (ANSI). Obecnie, 802.5 token ringów jest głównie ograniczone do środowisk IBM i istnieje wiele rzeczy, które można tam znaleźć. FDDI jest częściej spotykane w środowiskach kampusów wielourządzeniowych, wykorzystywanych jako szkielet do łączenia sieci Ethernet / 802.3. FDDI to być stopniowo wycofywane; ostatni sprzedawca produktów FDDI odpadł z rynku w 1999 r.

STANDAD IEEE 802.2 LLCM

Protokół IEEE 802.2 LLC miał zapewnić wspólny interfejs pomiędzy 802 LANMAC a aplikacjami wyższej warstwy. W przypadku LLC, podstawowy schemat MAC jest przezroczysty dla aplikacji, podobnie jak aplikacja jest przezroczysta dla MAC. TheLLC został zaprojektowany do obsługi dowolnej liczby usług, z których najczęstszą jest niepotwierdzona usługa bezpołączeniowa (używana głównie w sieciach rywalizacyjnych) oraz potwierdzona usługa zorientowana na połączenie (używana przede wszystkim w środowiskach z tokenami). LLC jest luźno oparty na bitorientowanym protokole wyższego poziomu Data Link Control (HDLC) zarówno w formacie operacyjnym, jak i ramowym



Ramka LLC pojawia się w polu Informacji ramki MAC. Pierwsze dwa pola nagłówka LLC są polami Destination Service Access Point (DSAP) i Source Service Access Point (SSAP), pierwotnie przeznaczonymi do identyfikacji usług wyższej warstwy w węźle źródłowym i docelowym. Jest to koncepcja podobna do portów w protokole TCP (Transmission Control Protocol) i UDP (User Datagram Protocol), ale nigdy nie została dobrze zaimplementowana, a wartości DSAP i SSAP są zwykle takie same. Trzecie pole to pole kontrolne, identyfikujące rodzaj ramki. Protokół SNAP (ang. Subnetwork Access Protocol) to protokół IEEE 802, który może być używany do identyfikowania dowolnego protokołu utworzonego przez dowolną agencję i jest powszechnie stosowany powyżej warstwy LLC. W takim przypadku nagłówek SNAP następuje bezpośrednio po nagłówku LLC. Używanie SNAP jest

wskazywane przez pola LLC, gdy zarówno pola DSAP, jak i SSAP są ustawione na wartość 170 (0xAA), a pole Control jest ustawione na wartość 3 (03), aby wskazać, że jestrama nienumerowana. Nagłówek SNAP ma dwa pola. 3-bajtowe pole OUI (Organizationally Unique Identifier) odnosi się do organizacji, która opracowała protokół wyższej warstwy lub sposób odwoływania się do protokołu. Dwubajtowe pole Type identyfikuje protokół przy użyciu numeru zdefiniowanego przez organizację. Protokół IP (Internet Protocol) i protokół ARP (Address Resolution Protocol) przedstawiają przykładowe zastosowania protokołu SNAP. Powszechnym formatem nagłówka SNAP obejmującego te protokoły byłoby ustawienie wartości OUI na 0 (0x00-00-00) w celu identyfikacji IEEE / ISO jako organizacji. Pole Type będzie następnie używać wartości EtherType z 2048 (0x08-00) i 2054 (0x08-06), aby wskazać odpowiednio użycie IP i ARP.

URZĄDZENIA POŁĄCZENIOWE

Urządzenia do łączenia sieci LAN są używane do łączenia pojedynczych sieci LAN w celu zbudowania dużej sieci korporacyjnej. Mogą również łączyć ze sobą komponenty LAN w sieci WAN i zapewniać dostęp do sieci LAN. Kilka rodzajów takich urządzeń jest używanych do połączeń między sieciami LAN, w tym koncentratorów, przełączników, mostów i routerów. Głównym rozróżnieniem tych urządzeń jest warstwa OSI, na której działają, a wszystkie omówione są w następnych sekcjach.

HUBY

Koncentratory są używane do budowania fizycznie przewodowych sieci LAN, wykorzystując media, które są w zasadzie punkt-punkt z natury (takie jak UTP i światłowód). Zauważ, że to wewnętrzne okablowanie piasty określa jego logiczny charakter, dzięki czemu logiczna magistrala lub Pierścień LAN może być fizycznie połączony z gwiazdą. Tak zwane koncentratory Ethernet obsługują sieci 10, 100 i / lub 1000 Mb / s Ethernet lub 802.3. Różne koncentratory będą miały różną liczbę portów, na ogół w zakresie od 4 do 32. Huby zapewniają tylko fizyczną łączność; gdy ramka dociera do jednego portu, hub przesyła ramkę z powrotem do wszystkich innych portów, co symuluje środowisko magistrali broadcast. Wiele koncentratorów można łączyć ze sobą, tworząc dość duże sieci. Piasty Token-Ring, ogólnie nazywane wielostanowiskowymi jednostkami dostępowymi (MAU), wyglądają podobnie do koncentratorów Ethernetowych, ale mają różne okablowanie wewnętrzne. Gdy anMAU otrzymuje transmisję na jednym porcie, przesyła tę transmisję, nieco na raz, do następnego portu sekwencyjnie na MAU. W ten sposób symuluje środowisko pierścienia.

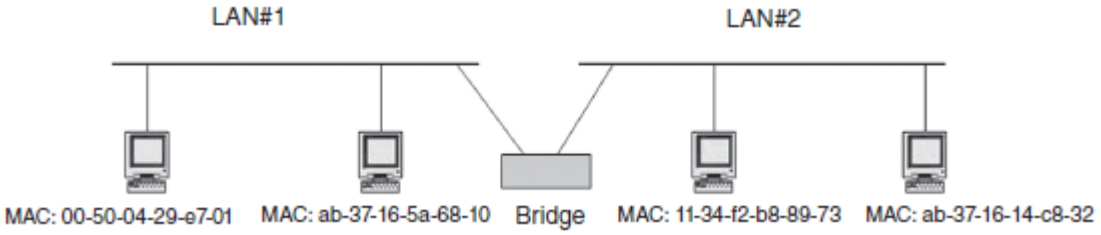
PRZEŁĄCZNIKI

Przełączniki są zwykle stosowane w środowisku CSMA / CD i rozszerzają możliwości koncentratora. Przełącznik działa na połączeniu warstw PHY i MAC. Oprócz zapewnienia fizycznej łączności, takiej jak koncentrator, przełącznik poznaje adres MAC wszystkich podłączonych do niego stacji. Kiedy ramka dociera do portu przełącznika, przełącznik sprawdza docelowy adres MAC i umieszcza ramkę na porcie związany z tym adresem (który może być portem prowadzącym do innego przełącznika). Przełączniki są używane głównie w celu poprawy wydajności. Biorąc pod uwagę opisany wcześniej scenariusz, wiele stacji może przesyłać jednocześnie bez kolizji. Co więcej, przełączniki mogą działać w trybie pełnego dupleksu, co oznacza, że pojedyncza stacja może zarówno nadawać, jak i odbierać w tym samym czasie. Na przykład sieć Ethernet z przełączaniem 10 Mb / s, może osiągnąć wydajność podobną do wydajności sieci Ethernet LAN z koncentratorem 100 Mb / s. (Było to prawdziwym dobrodziejstwem w tych środowiskach, w których nie jest możliwe uaktualnienie kart sieciowych o przepustowości 10 Mb / s i okablowania.) Istnieje subtelne zagrożenie dla wykorzystania przełączników w porównaniu do koncentratorów. W szczególności, jeśli użytkownik umieści sniffer pakietów w koncentrowanej sieci LAN, sniffer zobaczy każdą klatkę, ponieważ koncentrator symuluje środowisko transmisji. Sniffer pakietów w przełączanej sieci nie będzie tak skuteczny; pobierze tylko te ramki, które są specjalnie

adresowane do adresu rozgłaszania sieci LAN. Powiedział, że wiele przełączników pochodzi z port administracyjny, który można ustawić do monitorowania wszystkich portów w celu rozwiązywania problemów.

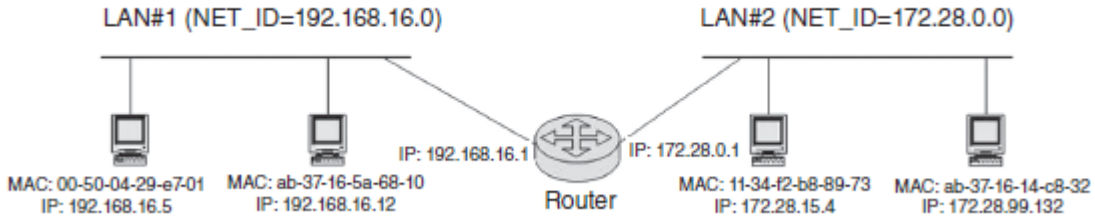
MOSTY

Most zapewnia połączenie punkt-punkt między dwiema sieciami LAN, zazwyczaj tymi, które wykorzystują podobne schematy MAC. Mosty działają w warstwie MAC, a ich działanie jest kontrolowane przez adres MAC. W środowiskach Ethernet zwykle stosuje się mosty edukacyjne. W bardzo prostym przypadku rozważ most łączący dwie sieci LAN, # 1 i # 2



Kiedy dowolna stacja LAN wysyła ramkę, zarówno adres docelowy, jak i źródłowy są zawarte w transmisji. Ponieważ ramki pojawiają się w sieciach, most widzi wszystkie adresy źródłowe i buduje tabelę, która łączy adresy MAC z jedną lub drugą siecią LAN, w końcu poznając lokalizację wszystkich stacji sieciowych. Proces ten jest czasami nazywany nauczaniem wstecznym, ponieważ most uczy się lokalizacji stacji, które transmitują. Most to proste urządzenie przechowujące i przesyłające ramkę. Podobnie jak wszystkie stacje w sieci LAN, a bridge analizuje adres docelowy wszystkich przesyłanych ramek. Jeśli transmisja w sieci nr 1 zawiera adres docelowy stacji w sieci LAN nr 2, most przesunie ramkę. Jeśli transmisja zawiera nieznany adres docelowy, most również przesunie ramkę. Chociaż most opiera decyzje na adresie MAC, nie jest to urządzenie inteligentne; oznacza to, że wie, że stacja o określonym adresie MAC jest w jednym lub drugim kierunku, ale nie wie dokładnie, gdzie znajduje się ta stacja. Ponieważ mosty muszą budować tabele zawierające wszystkie adresy stacji, których się uczą, mosty nie są szczególnie skalowalne dla dużych sieci. Mostki również rozszerzają domenę rozgłoszeniową (to znaczy, jeżeli ramka transmitowana w LAN # 1 jest wysyłana na adres rozgłoszeniowy, zostanie przekazana do sieci LAN nr 2).

ROUTERY Router jest koncepcyjnie podobny do mostu, ponieważ jest także urządzeniem do przechowywania i przekazywania. Router działa jednak w warstwie sieci i dlatego jest o wiele potężniejszym urządzeniem niż most. Jak pokazuje ekspozycja



każde urządzenie LAN ma zarówno adres aMAC (sprzęt), jak i warstwę sieciową (oprogramowanie) (w tym przypadku adres IP jest przykładowym adresem warstwy sieciowej). Ponieważ adresy warstwy sieci są hierarchiczne, same sieci mają numer identyfikacyjny sieci (identyfikator NET w załączniku 6.16). Adresy warstwy sieciowej są dobrze dostosowane do środowisk, w których pośrednie urządzenia muszą znaleźć najlepszą trasę między sieciami. Podobnie jak most, router jest uważany za kolejną stację w sieci LAN, do której jest podłączony. Jeśli router zobaczy transmisję w sieci LAN nr 1 (z

identyfikatorem NET 192.168.16.0) zawierającym adres docelowy stacji w innej sieci, przekieruje pakiet do właściwej sieci docelowej, nawet jeśli oznacza to przejście przez inny router by tam dotrzeć. Ten przykład pokazuje również inną istotną różnicę między mostami i routerami. W środowisku zmostkowanym stacja w sieci LAN # 1 wysyła ramkę do pewnego adresu MAC i nie ma wiedzy o tym, czy docelowe miejsce docelowe znajduje się w tej samej sieci LAN, czy nie; most przesunie ramę w razie potrzeby, ale wszystko to jest przezroczyste dla nadawcy i odbiorcy. Jednak w środowisku routowanym nadawca może stwierdzić, czy odbiornik znajduje się w tej samej lub innej sieci, po prostu przez sprawdzenie docelowego adresu sieciowego. W rzeczywistości router włącza się tylko wtedy, gdy pakiet musi opuścić sieć lokalną; dlatego w środowisku IP należy podać adres domyślnej bramy (routera). Routery ograniczają również domenę rozgłoszeniową. Jeśli stacja w sieci LAN # 1 transmituje ramkę z wykorzystaniem adresu MAC transmisji, ramka nie przechodzi dalej niż router. Routery budują swoje tabele routingu zupełnie inaczej niż mosty. Podczas gdy mosty uczą się względnej lokalizacji stacji, obserwując adres źródłowy ramki, pakiety poznają adres warstwy sieciowej za pomocą protokołów routingu, które pozwalają grupom routery do wymiany informacji o routingu.

PODSUMOWANIE

Huby, przełączniki, mosty i routery są powszechnie używanymi urządzeniami do łączenia sieci. Są to narzędzia w zestawie dla każdego, kto pracuje z sieciami lokalnymi, jako budulec wszystkiego - od małych i średniej wielkości sieci lokalnych po duże sieci korporacyjne i globalny Internet.

SYSTEMY OPERACYJNE SIECI

Podobnie jak system operacyjny zarządza zasobami komputera, sieciowy system operacyjny (NOS) zapewnia oprogramowanie kontrolujące zasoby LAN. NOS zwykle zawierają oprogramowanie zapewniające przynajmniej te funkcje:

* Sterowniki sprzętowe to oprogramowanie umożliwiające komunikację NOS z kartą NIC.

* Oprogramowanie komunikacyjne pozwala komunikować się z aplikacjami działającymi na różnych węzłach sieci LAN.

* Usługi są funkcjonalnymi aspektami NOS i powodują, że ludzie korzystają z sieci LAN w pierwszej kolejności. Przykłady usług obejmują usługi plików (udostępnianie plików), usługi drukowania (w większości udostępnione drukarki), usługi przesyłania wiadomości (e-mail), usługi komunikacyjne (dostęp do Internetu LAN) i usługi faksowe (często udostępniane faksy).

NOS są zwykle klasyfikowane jako peer to peer lub client / server. Sieć LAN typu "każdy z każdym" pozwala dowolnemu węzłowi LAN na komunikację z dowolnym innym węzłem sieci LAN, a każdy węzeł sieci LAN może świadczyć usługi innym węzłom. W środowisku klient / serwer (lub serwer) każdy węzeł jest klientem lub serwerem. W tym scenariuszu serwery są specjalnymi węzłami, które oferują usługi innym serwerom lub klientom, gdy są nimi klienci zwykłe stacje robocze użytkowników końcowych. Klienci mogą komunikować się tylko z serwerem. Podczas oceny lub testowania bezpieczeństwa sieci LAN oprogramowanie jest najczęstszym punktem narażenia, podatności na zagrożenia i użytkowania, szczególnie w przypadku ataków zdalnych. Niektóre próbki NOS, które były historycznie znaczące, obejmują:

AppleTalk. Apple Mac mają wbudowane funkcje LAN od momentu ich powstania w 1985 roku. Pierwotnie, używając schematu o nazwie LocalTalk, AppleTalk był siecią typu peer-to-peer działającą w sieci 10 Mb / s CSMA / CD LAN. Protokół warstwy sieciowej historycznie powiązany z protokołem AppleTalk nazwano protokołem dostarczania datagramów (DDP). Apple wycofało wsparcie AppleTalk w 2009 roku i obsługuje sieci oparte na TCP / IP.

Microsoft Networking. Systemy operacyjne Microsoft mają funkcje LAN od czasu Windows for Workgroups (WfW lub Windows 3.11). Korzystając z nieekranowanego protokołu o nazwie Sieciowy podstawowy system wejścia / wyjścia (Net-BIOS) Extended User Interface (NetBEUI), systemy klienckie Windows (Windows 3.11 i nowsze) można łatwo wykorzystać do zbudowania przystępnej cenowo, prostej sieci peer-to-peer dla pliku udostępnianie i drukarki. Protokołu NetBEUI nie można naprawić, ponieważ nie zapewnia mechanizmu adresowania, który umożliwia wzajemne połączenie, ale jest oddzielny

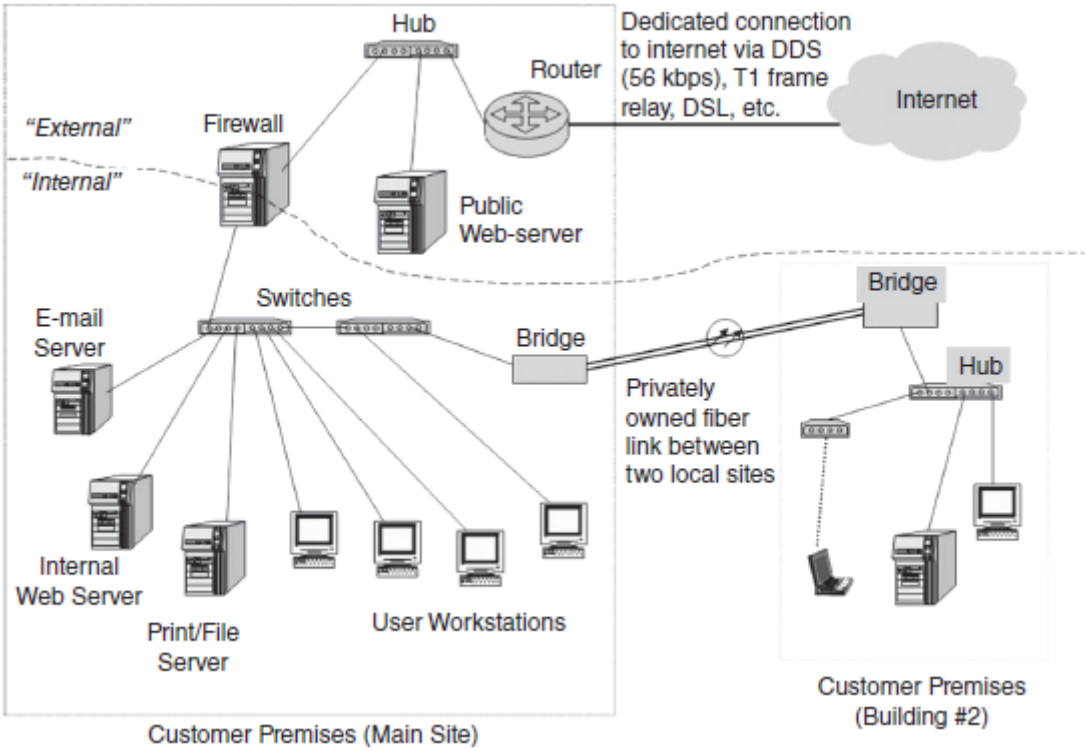
Podsieci NetBEUI. Jeżeli dwie sieci NetBEUI są zawarte w dowolny sposób, będą wyglądać jak jedna duża sieć. (Dlatego właśnie dysk twardy z niepoprawnie skonfigurowanymi systemami Windows można przeglądać z Internetu.) Microsoft zdefiniował NetBIOS przez TCP / IP (NBT) w latach 80. XX w., Aby wspierać enkapsulację komunikatów NetBIOS w komunikatach TCP i UDP. Większość sieci Microsoft opiera się bardziej na TCP / IP niż na NetBEUI.

Microsoft Windows Server (w tym Windows NT Server, Windows Server 2003, Windows Server 2008 i Windows Server 2012). Wybór NOS dla środowisk sieciowych Windows, Windows Server to system operacyjny klient / serwer Microsoftu. Systemy klienckie mogą uruchamiać prawie każdy system operacyjny Windows, od Windows XP lub NT Workstation do Windows VISTA, Windows 7 lub Windows 8. Klienci w sieci Windows Server mogą tworzyć sieci typu peer-to-peer. Sieć Microsoft opiera się na Active Directory i TCP / IP.

Novell NetWare. Novell zaoferował jedną z pierwszych sieci klasy PC we wczesnych latach osiemdziesiątych, wykorzystując autorską sieć LAN opartą na gwiazdach. W latach 90. NetWare był najbardziej znanym klientem / serwerem NOS i stanowił ponad 70% rynku NOS. Protokół warstwy sieciowej skojarzony z klasycznym systemem NetWare jest protokołem IPX (Internetwork Packet Exchange). Na przełomie wieków firma Microsoft szybko zjadła popularność NetWare, a ten protokół zdominował protokół TCP / IP. W tym czasie Novell przejął Linux i TCP / IP, a NetWare został zastąpiony przez Open Enterprise Server.

UNIX i Linux Protokół TCP / IP jest protokołem komunikacji sieciowej dla systemów UNIX od 1984 roku, umożliwiając hostom opartym na systemie UNIX zbudowanie sieci klient / serwer (i wreszcie sieci typu peer-to-peer). Protokół TCP / IP był również integralną częścią systemu Linux od jego powstania w 1991 roku. Dzięki TCP / IP każdy system może uruchomić oprogramowanie serwera (demon), aby świadczyć usługi innym systemom, dzięki czemu każdy system może działać jako klient lub serwer, w zależności od aplikacji.

PODSUMOWANIE



Ilustracja przedstawia możliwy projekt sieci obejmujący wiele elementów opisanych tu (a także kilka innych, które nie zostały opisane). Router tej sieci zapewnia interfejs do Internetu i jest podłączony za pośrednictwem pewnego rodzaju dedykowanego połączenia, na przykład łącza dzierżawionego 56 Kb / s lub T1 (1,544 Mb / s), przekaźnika ramek lub cyfrowej linii abonenckiej. W tym scenariuszu router jest fizycznie zlokalizowany w głównej witrynie. Z punktu widzenia bezpieczeństwa organizacja może podzielić swoją sieć na zewnętrzną i wewnętrzną, wewnętrzną chronioną przez zaporę ogniową. Sieć zewnętrzna obejmuje router, serwer publicWeb i zaporę ogniową. Te trzy systemy są połączone za pomocą piasty, do której są przymocowane za pomocą kabla UTP Cat5. W tym scenariuszu hub może w rzeczywistości zaimplementować 10BASE-T lub 100BASE-T Ethernet, a nawet token ring. Zewnętrzne i wewnętrzne sieci są połączone przez firewall, który w tym przypadku będzie miał dwie karty sieciowe. Dwie sieci są odrębne i odrębne; zapora sieciowa nie rozszerza domeny rozgłaszania żadnej z sieci i w rzeczywistości te dwie sieci miałyby różne identyfikatory sieci IP. Sieć wewnętrzna w witrynie głównej to zbiór serwerów i stacji roboczych użytkowników, które są połączone za pomocą zestawu przełączników. W tym przykładzie są to 8-portowe przełączniki Ethernet o szybkości 100 Mb / s. Ponieważ jest więcej niż 8 urządzeń, same przełączniki muszą być ze sobą połączone. Istnieje kilka opcji:

*Przełączniki kaskadowe łączą się fizycznie ze sobą, przedłużając płytę montażową przełącznika, tworząc większy przełącznik (w tym przypadku przełącznik 16-portowy).

* Łącze światłowodowe może być użyte do połączenia przełącznika, zwykle z prędkością backplane w zakresie 1 + Gb / s.

* Łącze UTP może być używane do łączenia przełączników przez dwa z portów 100-Mbps.

Aby połączyć LAN w budynku nr 2 z siecią LAN w miejscu głównym, wystarczy połączenie punkt-punkt między parą mostów. W tym przypadku budynki są oddalone o kilka kilometrów, co wymaga użycia światłowodu. W budynku nr 2 istnieje inna sieć LAN oparta na koncentratorze, z laptopem wykorzystującym technologię bezprzewodową, komunikującą się z węzłem dostępu, który jest również

podłączony do koncentratora. Ta część zawiera jedynie powierzchnie koncepcji, standardów i technologii sieci LAN. Ich badania są ważne dla specjalistów od bezpieczeństwa, ponieważ sieci LAN są podstawą wszystkich sieci. Jako sieć sieci obejmuje Internet