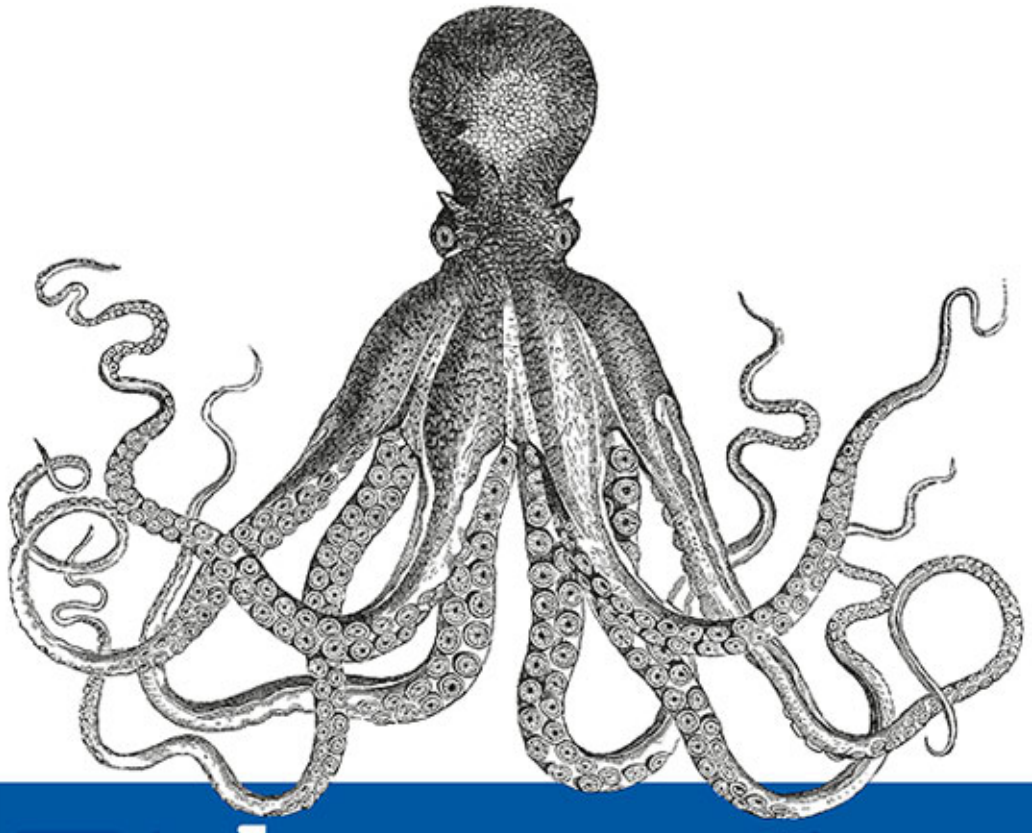
O'REILLY®



Ethernet
Biblia administratora

KOMPENDIUM WIEDZY O SIECIACH ETHERNET!

Charles E. Spurgeon
Joann Zimmerman

HELION

Tytuł oryginału: Ethernet: The Definitive Guide

Tłumaczenie: Radosław Meryk

ISBN: 978-83-246-9618-5

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/ethern
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Część IV Przełączniki Ethernet i projektowanie sieci

Część VI Dodatki

ROZDZIAŁ 18.

Przełączniki Ethernet

Przełączniki Ethernet (ang. *switches*), znane również jako mosty (ang. *bridges*), są podstawowym blokiem budulcowym sieci i są tak powszechnie stosowane, że często się o nich zapomina. Można zbudować sieć, nie wiedząc zbyt wiele o tym, jak działają przełączniki. Jednak podczas budowy większych systemów sieciowych zrozumienie działania przełączników oraz zapisów standardów pozwalających na wspólne działanie przełączników jest bardzo przydatne.

Technologię Ethernet stosuje się do budowy sieci różnych rozmiarów — od najmniejszych do największych oraz od najprostszych do najbardziej skomplikowanych. Ethernet łączy komputery domowe i inne urządzenia gospodarstwa domowego. Przełączniki dla sieci domowych są zazwyczaj małe, tanie i proste. Sieci Ethernet łączą się także z internetem, a przełączniki dla dostawców usług internetowych są duże, drogie i skomplikowane.

W sieciach kampusowych i korporacyjnych często wykorzystuje się różne przełączniki — zarówno prostsze i tańsze, stosowane wewnątrz szaf z okablowaniem do podłączenia urządzeń na danym piętrze budynku, jak i większe i droższe, które są używane w szkielecie sieci do łączenia przełączników wszystkich budynków w większy system sieciowy. Sieci centrów danych mają swoje szczególne wymagania. Zazwyczaj obejmują przełączniki o wysokiej wydajności, które mogą być połączone w taki sposób, aby zapewnić dużą elastyczność sieci.

Według szacunków branżowych światowy rynek przełączników korporacyjnych w 2013 roku osiągnął przychody w wysokości ponad 5 miliardów dolarów na kwartał. Daje to ponad 20 miliardów dolarów przychodu rocznie. W trzecim kwartale 2013 roku sprzedano dziesiątki milionów portów Ethernet, w tym 4,7 miliona portów 10-gigabitowych. Aby zaspokoić duży i stale rosnący rynek dla przełączników Ethernet, sprzedawanych jest wiele odmian przełączników oferowanych w wielu różnych cenach.

Wiele rodzajów przełączników oraz różnorodność ich funkcji to bardzo obszerny temat. Opisanie całego zakresu technologii i różnych sposobów, na jakie można wykorzystywać przełączniki w projektach sieci, wymagałoby całej książki, a nawet kilku. Zamiast tego w tym rozdziale zamieszczono wprowadzenie w tę tematykę oraz krótki przewodnik wyjaśniający, jak działają przełączniki. W rozdziale 19. omówiono, jak korzystać z przełączników w projektach sieciowych, oraz zamieszczono przegląd najbardziej przydatnych funkcji do projektowania sieci z przełącznikami. Opisano między innymi podstawowe funkcje zawarte w większości przełączników, a także bardziej zaawansowane funkcje, które można znaleźć w droższych i specjalistycznych przełącznikach.

Podstawowe funkcje przełączników

Przełączniki Ethernet łączą ze sobą urządzenia poprzez przekazywanie ramek Ethernet pomiędzy urządzeniami, które są do nich podłączone. Przenosząc ramkę Ethernet między portami, przełącznik łączy ruch transmitowany przez poszczególne połączenia sieciowe w większą sieć.

Przełączniki Ethernet wykonują swoją funkcję poprzez *mostkowanie* ramki Ethernet pomiędzy segmentami sieci Ethernet. Aby tego dokonać, kopiują ramkę Ethernet z jednego portu do drugiego na podstawie adresu dostępu do medium (MAC) w ramce Ethernet. Mostkowanie Ethernet zostało początkowo zdefiniowane w standardzie IEEE 802.1D, „IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges".

Najnowsza wersja standardu 802.1D dotyczącego mostów pochodzi z 2004 roku. Standard 802.1D rozszerzono i poprawiono w kolejnym standardzie — 802.1Q -2011, „Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks".

Dzięki standaryzacji operacji mostkowania przełączników można kupować przełączniki od różnych dostawców i mieć pewność, że będą one ze sobą współpracować, gdy zostaną połączone w pojedynczy projekt sieci. Zdefiniowanie zestawu standardów, jakie producenci mogą ze sobą uzgodnić i wdrożyć w swoich projektach przełączników, było ciężką pracą, którą wykonali inżynierowie pracujący nad normalizacją.

Mosty i przełączniki

Pierwsze mosty Ethernet były urządzeniami dwuportowymi, które mogły połączyć dwa segmenty Ethernet pracujące na kablu koncentrycznym. W tamtych czasach Ethernet obsługiwał wyłącznie połączenia za pomocą kabli koncentrycznych. Później, gdy opracowano skrętkę Ethernet, a przełączniki z wieloma portami stały się powszechnie dostępne, były one często wykorzystywane jako centralny punkt połączenia — koncentrator systemów okablowania sieci Ethernet. Przyczyniło się to do powstania nazwy „koncentrator przełączający" (ang. *switching hub*). Obecnie te urządzenia są nazywane po prostu przełącznikami.

Sporo się zmieniło, odkąd we wczesnych latach osiemdziesiątych po raz pierwszy opracowano mosty Ethernet. Z biegiem lat komputery stały się powszechne. Wiele osób korzysta w swojej pracy z wielu urządzeń, w tym z laptopów, smartfonów i tabletów. Każdy telefon VoIP i każda drukarka jest komputerem, a nawet systemy zarządzania budynkami oraz systemy kontroli dostępu (zamki drzwi) są połączone w sieć. Nowoczesne budynki mają wiele punktów dostępu bezprzewodowego (AP), co pozwala na dostarczanie usług Wi-Fi 802.11 dla takich urządzeń jak smartfony i tablety. Każdy punkt dostępowy również jest podłączony do przewodowego systemu Ethernet. W efekcie współczesne sieci Ethernet mogą zawierać setki połączeń przełączników w budynku i tysiące połączeń przełączników w sieci kampusowej.

Czym jest przełącznik?

Czytelnik z pewnością wie o istnieniu innych urządzeń sieciowych stosowanych do łączenia sieci, nazywanych *routerami*. Istnieją ważne różnice w sposobie działania pomiędzy mostami a routerami. Oba urządzenia mają swoje wady i zalety, o czym za chwilę się przekonamy.

Ujmując to w największym skrócie: mosty przenoszą ramkę między segmentami sieci w oparciu o adresy Ethernet. Most wymaga niewielu czynności konfiguracyjnych bądź wcale nie wymaga konfiguracji. Z kolei routery przesyłają pakiety pomiędzy sieciami, korzystając z adresów protokołów wysokiego poziomu. Każda sieć, która jest połączona, musi być skonfigurowana w routerze. Jednak i mosty, i routery są używane do budowy większych sieci, a oba urządzenia są nazywane na rynku „przełącznikami".

Na określanie mostów Ethernet będziemy zamiennie używać słów „most" i „przełącznik". Należy jednak pamiętać, że *przełącznik* to ogólna nazwa urządzeń sieciowych, które mogą działać jak mosty, routery lub oba te urządzenia, w zależności od zestawu funkcji i konfiguracji. Należy zapamiętać, że z punktu widzenia ekspertów mostkowanie i routing to dwa różne sposoby przełączania pakietów. Oba te mechanizmy dają różne możliwości. Dla naszych celów będziemy stosować praktykę producentów urządzeń Ethernet, którzy używają słowa „przełącznik" lub bardziej szczegółowo „przełącznik Ethernet", aby opisać urządzenia tworzące most dla ramek Ethernet.

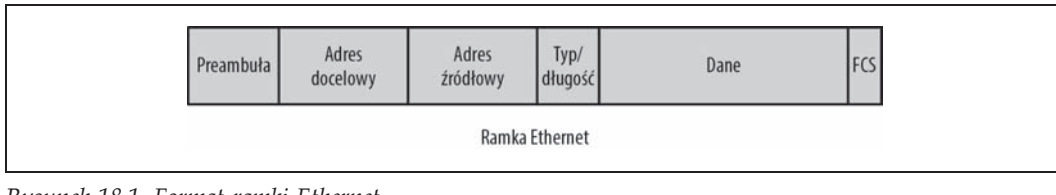
O ile standard 802.1D zawiera specyfikacje dla mostkowania ramek sieci lokalnej (LAN) między portami przełącznika oraz opisuje kilka innych aspektów podstawowego działania mostu, o tyle unika się w nim opisywania takich kwestii jak wydajność przełączników lub mostów czy sposób budowania przełączników. Zamiast tego producenci konkurują ze sobą, starając się zapewnić przełączniki w wielu przedziałach cenowych oraz o różnej wydajności i możliwościach.

W rezultacie powstał duży i konkurencyjny rynek przełączników Ethernet, dzięki czemu klienci mają większe możliwości wyboru. Mnogość modeli i możliwości przełączników może być myląca. Różne rodzaje przełączników opisano w rozdziale 19.

Działanie przełączników ethernetowych

Sieci służą do przenoszenia danych między komputerami. Aby było to możliwe, przesyłane dane są zorganizowane we fragmenty danych zwane *ramkami* Ethernet. Ramki „podróżują" po sieci Ethernet, a pole danych ramki służy do przenoszenia danych pomiędzy komputerami. Ramki są po prostu dowolnymi sekwencjami informacji, których format zdefiniowano w standardzie.

Jak pokazano na rysunku 18.1, pierwszym odbieranym polem ramki Ethernet jest adres docelowy zawierający adres urządzenia, do którego jest przesyłana ramka (pole preambuły na początku ramki jest automatycznie odcinane w chwili odebrania ramki przez interfejs Ethernet, zatem adres docelowy pozostaje pierwszym odbieranym polem).



Rysunek 18.1. Format ramki Ethernet

Następnym polem jest adres źródłowy, który wskazuje urządzenie wysyłające ramkę. Za adresami występuje kilka innych pól, w tym pole danych, które zawiera dane przesyłane pomiędzy komputerami (pełny opis struktury ramki Ethernet można znaleźć w rozdziale 4.).

Ramki są zdefiniowane w warstwie 2. — łącza danych — siedmiowarstwowego modelu sieci OSI. Zgodnie z tym, co napisano w rozdziale 2., siedmiowarstwowy model opracowano w celu zorganizowania rodzajów informacji przesyłanych pomiędzy komputerami. Model ten pomaga określić sposób wysyłania informacji oraz określić strukturę opracowywania standardów realizacji tego zadania. Ponieważ przełączniki Ethernet działają na lokalnych ramkach sieci w obszarze warstwy łącza danych, to czasami można spotkać nazwy „urządzenie warstwy łącza", „urządzenie warstwy 2." czy „przełączniki warstwy 2.".

Ethernet działa jak system transportu ciężarowego, który pozwala na transportowanie pomiędzy komputerami pakietów TCP/IP przesyłanych jako dane w ramce Ethernet. Chociaż ramki Ethernet są także określane jako „pakiety", to w standardach do opisania kontenera do przenoszenia danych między komputerami wykorzystywane jest pojęcie „ramka".

Protokół TCP/IP bazuje na *pakietach* warstwy sieci. Pakiety TCP/IP są przesyłane pomiędzy komputerami w polach danych *ramek* Ethernet.

Przełączniki Ethernet są zaprojektowane w taki sposób, że ich działanie jest niewidoczne dla urządzeń w sieci. To uzasadnia nazwę *mostkowanie przezroczyste* (ang. *transparent bridging*) stosowaną do opisania tego podejścia do łączenia sieci. „Przezroczystość" oznacza, że przełącznik Ethernet po podłączeniu do systemu nie wprowadza żadnych zmian w przesyłanych ramkach Ethernet. Przełącznik automatycznie rozpoczyna pracę. Nie jest wymagana żadna konfiguracja przełącznika i nie trzeba wprowadzać żadnych zmian w komputerach podłączonych do sieci Ethernet. Dzięki temu działanie przełącznika jest dla nich przezroczyste.

W dalszej części przyjrzymy się podstawowym funkcjom mostu umożliwiającym przekazywanie ramek Ethernet pomiędzy portami.

Nauka adresów

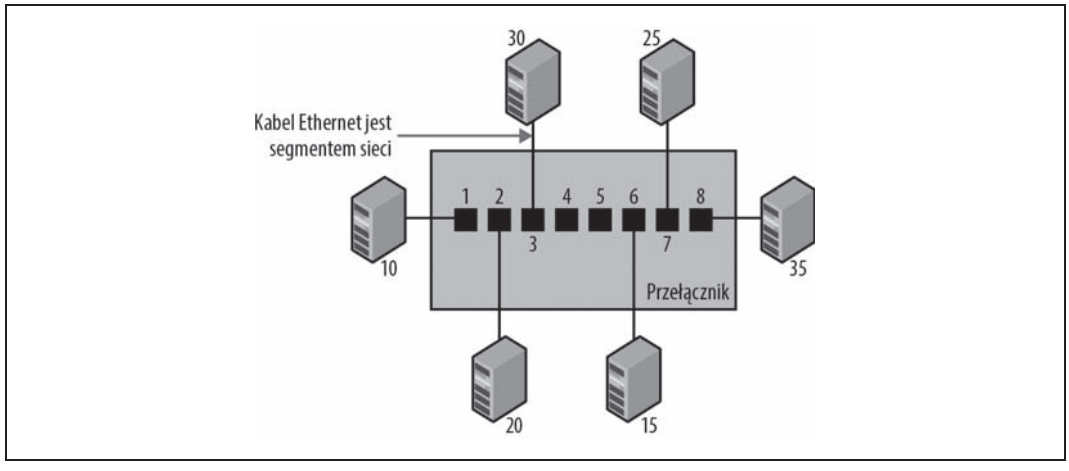
Przełącznik ethernetowy zarządza transmisją ramek pomiędzy portami przełącznika podłączonymi do kabli sieci Ethernet przy użyciu reguł przekazywania ruchu opisanych w standardzie mostkowania IEEE 802.1D. Przekazywanie ruchu bazuje na nauce adresów. Przełączniki przekazują ruch na podstawie 48-bitowych adresów MAC używanych w standardach sieci LAN, w tym w standardzie Ethernet.

Aby to zrobić, przełącznik uczy się, które urządzenia (zwane w standardzie „stacjami") znajdują się w określonych segmentach sieci. W tym celu monitoruje adresy źródłowe we wszystkich odbieranych ramkach. Gdy urządzenie Ethernet wysyła ramkę, umieszcza w niej dwa adresy. Są to adres *docelowy* urządzenia, do którego ramka jest wysyłana, oraz adres *źródłowy* urządzenia, które ramkę wysyła.

Sposób „uczenia się" przełącznika jest dosyć prosty. Podobnie jak wszystkie interfejsy Ethernet, każdy port przełącznika ma unikatowy adres MAC, który został przypisany fabrycznie. Jednak w przeciwieństwie do zwykłego urządzenia sieci Ethernet, które akceptuje ramki adresowane bezpośrednio do niego, interfejs Ethernet umieszczony w każdym porcie przełącznika działa w trybie *promiscuous*. W tym trybie interfejs jest zaprogramowany do otrzymywania *wszystkich* ramek, które są widoczne w porcie, a nie tylko tych, które zostały wysłane do adresu MAC interfejsu Ethernet w tym porcie przełącznika.

Ponieważ każda ramka jest odbierana na każdym porcie, oprogramowanie przełącznika odczytuje adres źródłowy ramki i dodaje go do tabeli adresów utrzymywanej w przełączniku. W ten sposób przełącznik automatycznie wykrywa, które stacje są dostępne na danych portach.

Na rysunku 18.2 pokazano przełącznik Ethernet łączący sześć urządzeń. Dla wygody w roli adresów stacji użyto liczb zamiast rzeczywistych 6-bajtowych adresów MAC. W miarę jak stacje wysyłają ramki, przełącznik odbiera każdą wysłaną ramkę i tworzy tabelę, formalnie nazywaną *bazą danych przekazywania* (ang. *forwarding database*). Tabela ta zawiera informacje o tym, które stacje są dostępne na określonych portach.



Rysunek 18.2. Nauka adresów w przełączniku

Kiedy każda stacja prześle co najmniej jedną ramkę, przełącznik będzie dysponował bazą danych przekazywania w postaci zaprezentowanej w tabeli 18.1.

Tabela 18.1. Baza danych przekazywania utrzymywana przez przełącznik

Port	Stacja
1.	10.
2.	20.
3.	30.
4.	Brak stacji
5.	Brak stacji
6.	15.
7.	25.
8.	35.

Następnie przełącznik korzysta z tej bazy danych przy podejmowaniu decyzji dotyczących przekazywania pakietów. Proces ten nazywa się *filtrowaniem adaptacyjnym*. Bez bazy adresowej przełącznik musiałby wysyłać ruch otrzymywany w określonym porcie do wszystkich innych portów. Tylko w takim przypadku miałby pewność, że ramka dotrze do celu. Dzięki bazie danych adresów ruch jest filtrowany w zależności od adresów docelowych. Przełącznik jest „adaptacyjny" w tym sensie, że automatycznie uczy się nowych adresów.

Dzięki zdolności do uczenia się można dodawać nowe stacji do sieci bez konieczności ręcznej konfiguracji przełącznika. Aby przełącznik dowiedział się o nowej stacji lub aby stacje dowiedziały się o przełączniku, konfiguracja nie jest potrzebna.

W każdym systemie Ethernet, który nadal używa segmentów kabli koncentrycznych i (lub) koncentratorów repeaterów, może występować wiele stacji w jednym segmencie sieci. Podłączenie takiego segmentu do przełącznika spowoduje, że pojedynczy port będzie gwarantował dostęp do wielu stacji.

Gdy przełącznik odbiera ramkę przeznaczoną dla stacji o adresie, który jeszcze nie był widziany, przełącznik wysyła ramkę do wszystkich portów innych niż port, z którego ramka przybyła. Proces ten nazywa się *zalewaniem* (ang. *flooding*). Bardziej szczegółowo omówiono go poniżej. Wyłączenie z transmisji portu przełącznika, który odebrał ramkę, zapobiega obserwowaniu tego samego ruchu więcej niż jeden raz przez stacje należące do współdzielonego segmentu. Dzięki temu pojedyncza stacja podłączona do portu nie otrzyma kopii ramki, którą przed chwilą wysłała.

Filtrowanie ruchu

Gdy przełącznik zbuduje bazę danych adresów, posiada wszystkie informacje niezbędne do selektywnego filtrowania i przekazywania ruchu. Gdy przełącznik uczy się adresów, sprawdza również każdą ramkę w celu podjęcia decyzji dotyczącej przekazywania pakietów na podstawie adresu docelowego w ramce. Przyjrzyjmy się, w jaki sposób są podejmowane takie decyzje w przełączniku wyposażonym w osiem portów — takim jak pokazano na rysunku 18.2.

Załóżmy, że ramka jest przesyłana od 15. do 20. stacji. Ponieważ ramka jest przesyłana przez stację 15., przełącznik odczytuje ramkę na porcie 6. i wykorzystuje bazę danych adresów do określenia, który z jego portów jest związany z adresem docelowym tej ramki. W tym przypadku adres docelowy odpowiada stacji 20., a w bazie danych adresów (tabela 18.1) widać, że aby dotrzeć do stacji 20., ramka musi być wysłana do portu 2.

Każdy port przełącznika ma możliwość zapisania małej ilości danych w pamięci. Pamięć ta wystarcza do zapisania ramki przed transmisją przez kabel Ethernet podłączony do portu. Jeśli port jest już zajęty transmisją, w czasie gdy dociera do niego ramka w celu przesłania, ramka może być przechowana przez krótki czas, jaki jest potrzebny do tego, by port mógł zakończyć przekazywanie poprzedniej ramki. W celu transmisji ramki przełącznik umieszcza ją w *kolejce przełączania pakietów* do transmisji w porcie 2.

W trakcie tego procesu przełącznik przesyłający ramkę Ethernet z jednego portu do drugiego nie wprowadza żadnych zmian w danych, adresie lub innych polach podstawowej ramki Ethernet. Posługując się naszym przykładem, ramka jest przekazywana do portu 2. w stanie nienaruszonym — dokładnie w takiej postaci, w jakiej została odebrana w porcie 6. W związku z tym działanie przełącznika jest przezroczyste dla wszystkich stacji w sieci.

Należy zwrócić uwagę, że przełącznik nie prześle ramki przeznaczonej do stacji zapisanej w bazie danych przekazywania do żadnego portu, który nie jest podłączony do miejsca docelowego. Mówiąc inaczej, ruch przeznaczony do urządzenia w określonym porcie będzie wysłany tylko do tego portu. Żadne inne porty nie będą widziały ruchu przeznaczonego do tego urządzenia. Ta logika przełączania utrzymuje ruch w postaci wyizolowanej wyłącznie do tych

kabli (segmentów) Ethernet, które są niezbędne do odebrania ramki od nadawcy i przekazania jej do urządzenia docelowego.

Uniemożliwia to przepływ niepotrzebnego ruchu do innych segmentów systemu sieciowego, co jest główną zaletą przełączników. Pod tym względem sieci z przełącznikami działają inaczej niż pierwsze systemy Ethernet, w przypadku których ruch z dowolnej stacji był widziany przez inne stacje niezależnie od tego, czy tego chcieliśmy, czy nie. Filtrowanie ruchu przez przełącznik zmniejsza obciążenie ruchu przesyłanego przez zbiór kabli podłączonych do przełącznika, a tym samym podnosi wydajność wykorzystania pasma sieci.

Flooding ramek

W przełącznikach działa automatyczny mechanizm, który powoduje, że po pewnym czasie (zazwyczaj po pięciu minutach) braku ramki z określonej stacji wpisy w bazach danych przekazywania są uznawane za przestarzałe. Jeśli stacja nie wysyła ruchu przez pewien okres, przełącznik usuwa wpis odpowiadający tej stacji z bazy danych przekazywania. Dzięki temu baza danych przekazywania nie rozrasta się z powodu przeterminowanych wpisów, które nie odzwierciedlają rzeczywistości.

Kiedy jednak wpis adresu określonej stacji stanie się przestarzały, to następnym razem, gdy przełącznik odbierze ramkę przeznaczoną dla tej stacji, nie będzie miał żadnej informacji o tej stacji w bazie danych. Taka sytuacja ma również miejsce w przypadku podłączenia nowej stacji do przełącznika lub po wyłączeniu, a następnie ponownym włączeniu stacji po czasie dłuższym niż pięć minut. W jaki sposób przełącznik postępuje z pakietami przeznaczonymi do nieznanej stacji?

Rozwiązanie jest proste: przełącznik przekazuje ramki przeznaczone do nieznanej stacji do wszystkich portów przełącznika innych niż ten, z którego ramka dotarła. Jest to tzw. *zalewanie* (ang. *flooding*), polegające na przekazaniu ramki do wszystkich innych stacji niż stacja nadawcy. Flooding ramek daje gwarancję, że ramka z nieznanego adresu docelowego dotrze do wszystkich łączy i zostanie odebrana przez właściwe urządzenie docelowe, pod warunkiem że jest ono podłączone do sieci i jest aktywne. Kiedy nieznane urządzenie odpowie na tę ramkę, przełącznik automatycznie nauczy się, do którego portu jest podłączone urządzenie, i w przypadku ruchu przeznaczonego do tego urządzenia nie będzie stosował floodingu.

Ruch rozgłoszeniowy i multiemisja

Oprócz ramek skierowanych do jednego adresu lokalne sieci komputerowe mogą wysyłać ramki skierowane do adresów grupowych, zwanych adresami *multicast* lub adresami *multiemisji*. Takie ramki są odbierane przez zbiór stacji. W sieciach LAN są również ramki skierowane do wszystkich stacji. Są one wysyłane na adres *rozgłoszeniowy* (ang. *broadcast*). Adresy grupowe zawsze zaczynają się od określonego wzorca bitowego zdefiniowanego w standardzie Ethernet. Dzięki temu przełącznik może zidentyfikować ramki przeznaczone do konkretnego urządzenia i odróżnić je od tych, które powinny być skierowane do grupy urządzeń.

Ramki przesyłane na adres multiemisji mogą być odebrane przez wszystkie stacje skonfigurowane do słuchania tego adresu *multicast*. Oprogramowanie Ethernet, nazywane również „sterownikiem interfejsu", programuje interfejs w taki sposób, aby akceptował ramki wysyłane na adres grupowy. W ten sposób interfejs jest postrzegany jako członek grupy. Fabrycznie

przypisany adres interfejsu Ethernet to tzw. adres *unicast*. Każdy interfejs Ethernet może odbierać ramki *unicast* i ramki *multicast*. Inaczej mówiąc, interfejs może być zaprogramowany do odbierania ramek wysyłanych na jeden lub większą liczbę grupowych adresów docelowych, a także ramki wysyłane na adres MAC *unicast* należący do tego interfejsu.

Przekazywanie ruchu rozgłoszeniowego i multiemisji

Adres rozgłoszeniowy jest adresem grupy wszystkich stacji. Jest on szczególnym przypadkiem adresu *multicast*. Pakiet wysłany na adres rozgłoszeniowy (adres ten składa się z samych jedynek) jest odbierany przez wszystkie stacje w sieci LAN. Ponieważ pakiety rozgłoszeniowe muszą być odebrane przez wszystkie stacje w sieci, przełącznik osiągnie ten cel przez *flooding* pakietów rozgłoszeniowych do wszystkich portów z wyjątkiem tego, z którego pakiet został przyjęty — nie ma potrzeby, aby wysyłać pakiet z powrotem do urządzenia nadawczego. W ten sposób pakiet rozgłoszeniowy wysłany przez dowolną stację dotrze do wszystkich innych stacji w sieci LAN.

Ruch *multicast* może być trudniejszy w obsłudze od ramek rozgłoszeniowych. Bardziej zaawansowane (i zwykle droższe) przełączniki zawierają obsługę protokołów wykrywania grup multiemisji. Umożliwiają one stacjom poinformowanie przełącznika o adresach grup multiemisji, z których stacja chce odbierać ramki. Dzięki temu przełącznik wysyła pakiety *multicast* tylko do portów podłączonych do stacji, które wykazały swoje zainteresowanie odbiorem ruchu multiemisji. Jednak tańsze przełączniki bez możliwości wykrywania, które porty są podłączone do stacji nasłuchujących określonego adresu multiemisji, muszą stosować technikę *floodingu* pakietów *multicast* do wszystkich portów innych niż port, z którego odebrano ruch multiemisji — tak jak w przypadku ruchu rozgłoszeniowego.

Zastosowanie ruchu rozgłoszeniowego i multiemisji

Stacje wysyłają pakiety rozgłoszeniowe i pakiety multiemisji z wielu powodów. Wysokopoziomowe protokoły sieciowe, takie jak TCP/IP, używają ramek rozgłoszeniowych lub ramek multiemisji w ramach procesu wykrywania adresów. Ruch rozgłoszeniowy i multiemisja są również wykorzystywane do dynamicznego przydzielania adresów do stacji, gdy zostanie ona po raz pierwszy włączona i musi znaleźć wysokopoziomowy adres sieciowy. Multiemisja jest również wykorzystywana przez niektóre aplikacje multimedialne, które wysyłają dane audio i wideo w ramkach multiemisji do odbioru przez grupę stacji. Jest także stosowana w grach dla wielu użytkowników jako sposób przesyłania danych do grupy graczy.

Z tego powodu w typowej sieci zwykle pewna część ruchu to ruch rozgłoszeniowy i multiemisja. Jeśli liczba takich ramek jest na odpowiednio niskim poziomie, to ruch tego rodzaju nie sprawia żadnych problemów. Kiedy jednak wiele stacji zostanie połączonych za pomocą przełączników w pojedynczą dużą sieć, flooding ramek rozgłoszeniowych i ramek multiemisji może stanowić znaczną część ruchu. Duże natężenie ruchu rozgłoszeniowego lub multiemisji może powodować przeciążenia sieci, ponieważ każde urządzenie w sieci musi odbierać i przetwarzać ruch rozgłoszeniowy oraz określone typy multiemisji. Przy odpowiednio dużej liczbie pakietów mogą wystąpić problemy z wydajnością stacji.

Aplikacje strumieniowe (wideo) wysyłające ramki multiemisji z dużą szybkością mogą generować intensywny ruch. Systemy tworzenia kopii zapasowych dysków i kopiowania dysków bazujące na multiemisji również mogą generować dużo ruchu. Jeśli ten ruch jest wysyłany do wszystkich portów, może dojść do przeciążenia sieci. Jednym ze sposobów uniknięcia tego

rodzaju zatorów jest ograniczenie liczby stacji podłączonych do pojedynczej sieci. Dzięki temu procent ruchu rozgłoszeniowego i multiemisji nie osiągnie na tyle wysokiego poziomu, aby stanowiło to problem.

Innym sposobem ograniczenia natężenia ruchu pakietów multiemisji i rozgłoszeniowych jest podzielenie sieci na wiele wirtualnych sieci LAN (VLAN). Każda z takich sieci działa jako osobna i odrębna od pozostałych sieć LAN. Jeszcze innym sposobem jest użycie routera, nazywanego również przełącznikiem warstwy 3. Ponieważ router nie przesyła automatycznie ruchu rozgłoszeniowego i multiemisji pomiędzy sieciami, to dzięki zastosowaniu routera tworzą się oddzielne domeny rozgłoszeniowe. Obie metody kontroli rozprzestrzeniania się ruchu multiemisji i rozgłoszeniowego zostały omówione bardziej szczegółowo w dalszej części tej książki (sieci VLAN w tym rozdziale, natomiast routery w następnym).

Łączenie przełączników

Do tej pory dowiedzieliśmy się, że pojedynczy przełącznik może przekazywać ruch na podstawie utworzonej dynamicznie bazy danych przekazywania. Główna trudność w tym prostym modelu działania przełącznika polega na tym, że wiele połączeń pomiędzy przełącznikami może tworzyć pętle, które są przyczyną zatłoczenia sieci lub jej przeciążenia.

Pętle przekazywania

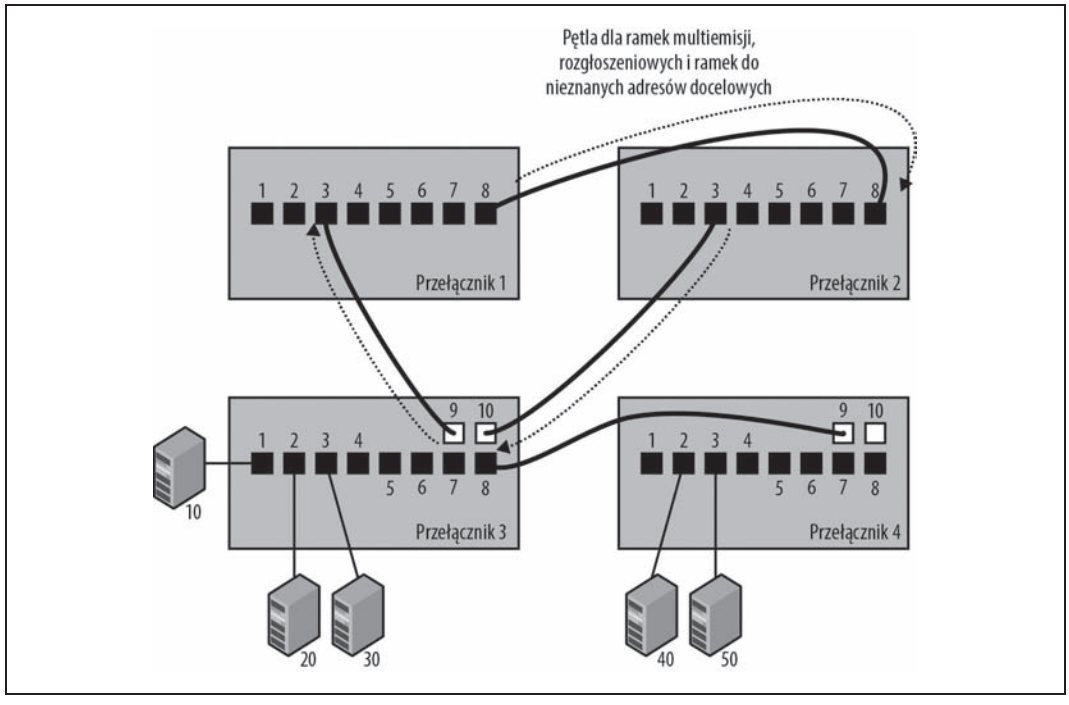
Budowa i działanie sieci Ethernet wymagają, aby pomiędzy dowolnymi dwoma stacjami istniała tylko jedna droga transmisji pakietów. Ethernet rozrasta się poprzez rozszerzanie gałęzi w topologii sieci o *strukturze drzewa*, która składa się z kilku przełączników podłączonych jako gałęzie centralnego przełącznika. Istnieje niebezpieczeństwo, że w złożonej sieci przełączniki z wieloma połączeniami z innymi przełącznikami będą tworzyły pętle w sieci.

W sieci z przełącznikami połączonymi ze sobą w pętlę pakiety będą krążyć w pętli bez końca, co może doprowadzić do bardzo dużego natężenia ruchu i przeciążeń.

Zapętlone pakiety będą krążyć z maksymalną prędkością łącza sieciowego do momentu, aż natężenie ruchu osiągnie tak wysoki poziom, że sieć stanie się nasycona. Ramki rozgłoszeniowe i multiemisji w prostych przełącznikach są kierowane do wszystkich portów. Podobnie — do wszystkich portów — są kierowane ramki *unicast* wysyłane do nieznanych stacji. Cały ten ruch będzie krążył w ewentualnej pętli. Gdy utworzy się pętla, ten tryb błędnej pracy może wystąpić bardzo szybko: sieć będzie całkowicie zajęta wysyłaniem ruchu rozgłoszeniowego, multiemisji i nieznanych ramek. W tej sytuacji stacjom trudno będzie wysyłać ruch *unicast* przeznaczony do znanych stacji.

Niestety, pomimo starań bardzo łatwo może dojść do powstania pętli podobnych do tych, które na rysunku 18.3 oznaczono przerywaną linią ze strzałkami. W miarę rozrastania się sieci oraz zwiększania liczby przełączników i węzłów dystrybucji okablowania kontrolowanie wszystkich połączeń i zapobieganie tworzeniu pętli staje się wyjątkowo trudne.

Podczas gdy pętla pokazana na rysunku jest oczywista, w złożonym systemie sieciowym stwierdzenie, czy przełączniki nie zostały połączone w pętlę, może być trudne. W standardzie IEEE 802.1D dotyczącym mostów zdefiniowano *protokół drzewa rozpinającego* (ang. *Spanning Tree Protocol*, STP), który pozwala uniknąć zapętlania poprzez automatyczne wyłączanie pętli przekazywania. Protokół ten opiszemy w następnym punkcie.



Rysunek 18.3. Pętla przekazywania pomiędzy przełącznikami

Protokół drzewa rozpinającego

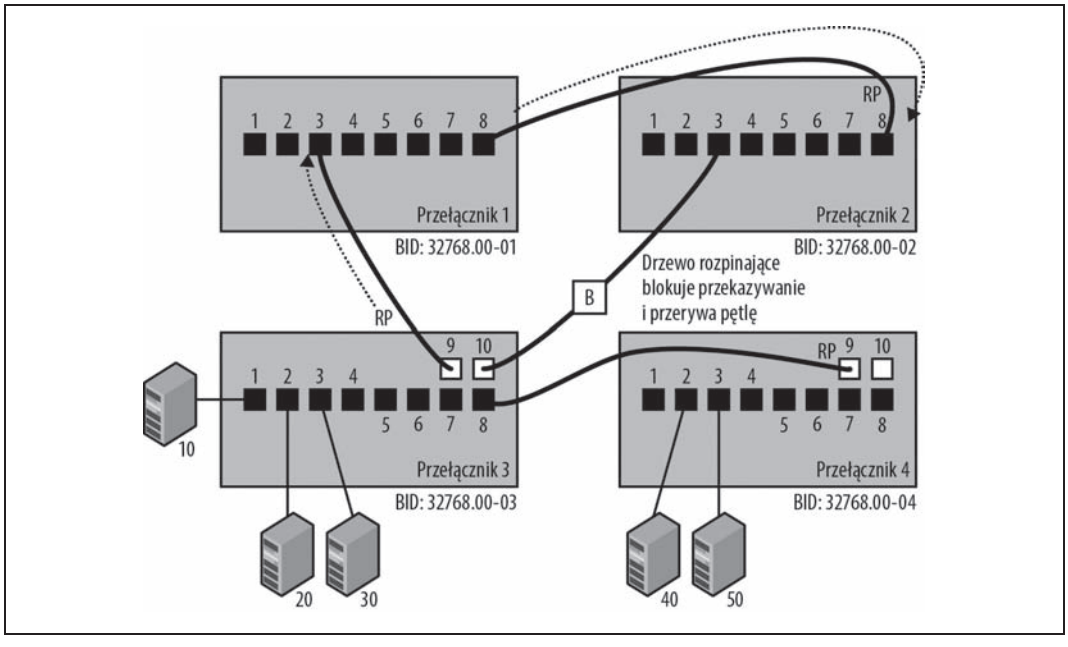
Celem protokołu drzewa rozpinającego jest umożliwienie przełącznikom automatycznego tworzenia zbiorów ścieżek wolnych od pętli. Protokół pozwala na eliminację pętli nawet w skomplikowanej sieci z wieloma ścieżkami prowadzącymi przez wiele przełączników. Możliwość dynamicznego tworzenia topologii drzewa w sieci poprzez zablokowanie przekazywania pakietów na niektórych portach jest mechanizmem pozwalającym grupie przełączników ethernetowych na automatyczne konfigurowanie ścieżek wolnych od pętli. Działanie protokołu drzewa rozpinającego opisano w standardzie IEEE 802.1D. Każdy przełącznik, który jest zgodny ze standardem 802.1D, musi obsługiwać protokół drzewa rozpinającego.

Należy pamiętać, że tanie przełączniki mogą nie obsługiwać protokołu drzewa rozpinającego. W związku z tym nie są w stanie zablokować pętli przekazywania pakietów. Warto także wiedzieć, że niektórzy producenci, którzy zapewniają obsługę tego protokołu, domyślnie go wyłączają. W takim przypadku należy ręcznie włączyć obsługę protokołu STP, aby zapewnić ochronę sieci przed pętlami.

Pakiety drzewa rozpinającego

Działanie algorytmu drzewa rozpinającego bazuje na komunikatach konfiguracyjnych wysyłanych przez każdy przełącznik w pakietach zwanych BPDU (ang. *bridge protocol data units*). Każdy pakiet BPDU jest wysyłany na docelowy adres multiemisji przypisany na potrzeby działania drzewa rozpinającego. Wszystkie przełączniki IEEE 802.1D dołączają do grupy multi-

emisji BPDU i słuchają ramek wysyłanych na ten adres. Dzięki temu każdy przełącznik może wysyłać i odbierać komunikaty konfiguracyjne drzewa rozpinającego. Sposób działania tego mechanizmu pokazano na rysunku 18.4.



Rysunek 18.4. Działanie drzewa rozpinającego

Adres MAC multiemisji dla grupy mostów ma wartość 01-80-C2-00-00-00. Odmiany protokołu drzewa rozpinającego zawierające usprawnienia wprowadzane przez producentów mogą również korzystać z innych adresów. Na przykład opracowany przez Cisco protokół PVST (ang. *Per-VLAN Spanning Tree*) wysyła pakiety BPDU na adres 01-00-0C-CC-CC-CD.

Wybór głównego mostu

Proces tworzenia drzewa rozpinającego zaczyna się od skorzystania z informacji zawartych w wiadomościach konfiguracyjnych BPDU w celu automatycznego wyboru *głównego mostu* (ang. *root bridge*). Elekcja bazuje na identyfikatorze mostu (ang. *bridge ID*, BID). Ten tworzony jest na podstawie kombinacji konfigurowalnej wartości priorytetu mostu (domyślnie 32 768) oraz unikatowego adresu MAC Ethernet zwanego adresem *systemowym MAC*, który jest przypisany do każdego mostu na potrzeby realizacji algorytmu drzewa rozpinającego. Mosty wysyłają do siebie pakiety BPDU, a most z najmniejszą wartością identyfikatora BID jest automatycznie wybierany jako główny.

Przy założeniu, że pozostawiono domyślną wartość 32 768 priorytetu mostu, głównym mostem zostanie most o najniższym adresie Ethernet.

W przykładzie pokazanym na rysunku 18.4 przełącznik 1. ma najniższą wartość identyfikatora BID. W rezultacie procesu wyboru drzewa rozpinającego przełącznik 1. został uznany za

most główny. Wybranie mostu głównego jest podstawowym elementem dla pozostałych operacji realizowanych przez protokół drzewa rozpinającego.

Może się zdarzyć, że most o niskiej wydajności w sieci ma najniższą wartość adresu MAC, co spowoduje wybranie go jako mostu głównego. Możemy skonfigurować niższy priorytet centralnego mostu w sieci, aby uzyskać pewność, że to on zostanie głównym. Główny most w miarę możliwości powinien być zlokalizowany w centrum sieci i działać na przełączniku o jak najwyższej wydajności.

Wybieranie ścieżki o najmniejszym koszcie

Po wybraniu głównego mostu każdy most inny niż główny używa informacji użytych w procesie wyboru głównego mostu w celu ustalenia, który z jego portów ma ścieżkę o najmniejszym koszcie do mostu głównego. Temu portowi jest przypisywana rola portu głównego (ang. *root port*, RP). Wszystkie mosty również obliczają ścieżkę o najmniejszym koszcie do mostu głównego dla swoich pozostałych połączeń i oznaczają każdy jako port wyznaczony (ang. *designated port*, DP). Most posiadający port DP jest mostem wyznaczonym (ang. *designated bridge*, DB).

Koszt ścieżki jest obliczany na podstawie szybkości, z jaką działają porty. Im większa szybkość, tym niższy koszt. Gdy pakiety BPDU są przesyłane w systemie, gromadzą informację o liczbie portów, przez które przechodzą, i o szybkości każdego portu. Ścieżki z wolniejszymi portami mają wyższe koszty. Całkowity koszt określonej ścieżki pomnożony przez liczbę przełączników jest sumą kosztów wszystkich segmentów sieci dla tej ścieżki. Jeśli istnieje wiele ścieżek do mostu głównego o tym samym koszcie, to zostanie użyta ścieżka połączona mostem z najniższym identyfikatorem BID.

Po zrealizowaniu tego procesu mosty dysponują informacjami o zbiorze portów głównych i portów wyznaczonych. Pozwala to mostom usunąć wszystkie pętle i utrzymywać drzewo przekazywania pakietów, które obejmuje cały zbiór urządzeń podłączonych do sieci — stąd nazwa „protokół drzewa rozpinającego”.

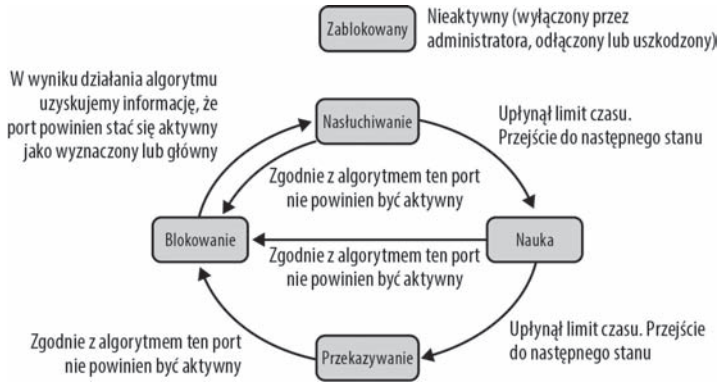
Blokowanie pętli

Kiedy proces drzewa rozpinającego ustali status portu, zbiór portów głównych i wyznaczonych dostarcza algorytmowi drzewa rozpinającego informacji potrzebnych do zidentyfikowania najlepszych ścieżek. Przekazywanie pakietów na dowolnym porcie, który nie jest portem głównym lub wyznaczonym, jest wyłączone poprzez *blokowanie* przesyłania pakietów do tego portu.

Chociaż zablokowane porty nie przekazują pakietów, w dalszym ciągu otrzymują pakiety BPDU. Zablokowany port oznaczono na rysunku 18.4 literą B. Oznacza to, że port 10. na przełączniku 3. jest zablokowany i że łącze to nie przekazuje pakietów. Szybki protokół drzewa rozpinającego (ang. *Rapid Spanning Tree Protocol*, RSTP) wysyła pakiety BPDU co dwie sekundy. W ten sposób monitoruje stan sieci, a zablokowany port może zostać odblokowany w przypadku wykrycia zmiany ścieżki.

Stany portów w protokole drzewa rozpinającego

Gdy aktywne urządzenie zostanie podłączone do portu przełącznika, port przechodzi przez szereg stanów w miarę przetwarzania odebranych pakietów BPDU, a proces drzewa rozpinającego określa, w jakim stanie powinien być port. Na rysunku 18.5 pokazano różne stany



Rysunek 18.5. Stany portów w algorytmie drzewa rozpinającego

portów. Podczas stanów *nasłuchiwania* i *nauki* proces drzewa rozpinającego w tym porcie nasłuchuje pakietów BPDU i uczy się adresów źródłowych na podstawie wszystkich odebranych ramek.

Diagram stanów pokazuje stany portów algorytmu drzewa rozpinającego. Można wyróżnić następujące stany:

Zablokowany
: Port w tym stanie został celowo wyłączony przez administratora lub automatycznie, ponieważ łącze zostało odłączone bądź port jest uszkodzony i nie działa. Port może wejść w stan *Zablokowany* z dowolnego innego stanu i może przejść ze stanu *Zablokowany* do dowolnego innego stanu.

Blokowanie
: Port, który jest włączony, ale nie jest portem głównym lub wyznaczonym, mógłby powodować pętlę przełączania, gdyby był aktywny (tzn. w stanie *Przekazywanie*). Aby tego uniknąć, port wchodzi w stan *Blokowanie*. Do portu w stanie *Blokowanie* nie są wysyłane ani nie są z niego odbierane żadne dane ze stacji. Po zainicjowaniu portu (łącze zaczyna działać po podłączeniu zasilania) port zazwyczaj przechodzi do stanu *Blokowanie*. Kiedy na podstawie pakietu BPDU lub upływu limitu czasu przełącznik wykryje, że może zaistnieć potrzeba, aby port stał się aktywny, port przejdzie do stanu nasłuchiwania na drodze do stanu przekazywania. Jeśli inne łącza przestaną działać, port może przejść ze stanu *Blokowanie* do stanu *Przekazywanie*. W czasie kiedy port znajduje się w stanie *Blokowanie*, port nie przestaje odbierać pakietów BPDU.

Nasłuchiwanie
: W tym stanie port odrzuca ruch, ale nadal przetwarza wszelkie pakiety BPDU, które odebrał, i reaguje na wszelkie nowe informacje, które mogłyby doprowadzić port do powrotu do stanu *Zablokowany*. Na podstawie informacji otrzymanych w pakietach BPDU port może przejść do stanu *Nauka*. Stan nasłuchiwania pozwala algorytmowi drzewa rozpinającego zdecydować, czy atrybuty tego portu, takie jak koszt portu, powinny spowodować, że port stanie się częścią drzewa rozpinającego, czy też ma powrócić do stanu *Blokowanie*.

Nauka
: W tym stanie port jeszcze nie przekazuje ramek, ale uczy się adresów źródłowych na podstawie odebranych ramek i dodaje je do bazy danych filtrowania. Przełącznik wypełnia

tabelę adresów MAC pakietami, które usłyszał w danym porcie, aż upłynie limit czasu. Następnie przechodzi do stanu *Przekazywanie*.

Przekazywanie
: Jest to stan pracy, w którym port wysyła i odbiera dane stacji. Przychodzące pakiety BPDU są monitorowane. Dzięki temu proces drzewa rozpinającego w przełączniku może wykryć, czy powinien przełączyć port do stanu *Blokowanie*, aby zapobiec powstaniu pętli.

Wersje protokołu drzewa rozpinającego

Oryginalny protokół drzewa rozpinającego znormalizowany w standardzie IEEE 802.1D określał pojedynczy proces drzewa rozpinającego działający na przełączniku. Pozwalał on na zarządzanie wszystkimi portami i sieciami VLAN w przełączniku za pomocą jednej maszyny stanów drzewa rozpinającego. Żaden zapis w standardzie nie zakazuje producentom opracowywania własnych udoskonaleń protokołu drzewa rozpinającego. Niektórzy producenci opracowali własne implementacje, a w jednym przypadku zdefiniowano osobne procesy drzewa rozpinającego na poziomie każdej sieci VLAN. Podejście to zostało zastosowane przez firmę Cisco Systems w wersji protokołu o nazwie PVST (ang. *Per-VLAN Spanning Tree*). Protokół drzewa rozpinającego z obsługą sieci VLAN — taki jak PVST — może uwzględniać sieci VLAN podczas zarządzania nadmiarowymi ścieżkami.

Standard protokołu drzewa rozpinającego IEEE ewoluował na przestrzeni lat. Zaktualizowaną wersję, o nazwie *Rapid Spanning Tree Protocol*, zdefiniowano w 2004 roku. Jak wskazuje nazwa, protokół RSTP zwiększył szybkość działania protokołu. Standard 802.1Q obejmuje zarówno protokół RSTP, jak i nową wersję protokołu drzewa rozpinającego o nazwie MST (ang. *multiple spanning tree* — dosł. wielokrotne drzewo rozpinające). Oba były zaprojektowane tak, aby zapewnić wsteczną zgodność z poprzednimi wersjami protokołu[1]. Wersję MST omówiono dokładniej w standardzie „802.1Q Multiple Spanning Tree Protocol".

Podczas budowania sieci z wieloma przełącznikami należy zwrócić szczególną uwagę na to, w jaki sposób producent przełącznika obsłużył algorytm drzewa rozpinającego, oraz na wersję protokołu w przełącznikach. Najczęściej stosowane wersje — klasyczny protokół STP i nowszy RSTP — współdziałają ze sobą. Obie nie wymagają konfiguracji, co sprawia, że działają w trybie „plug and play".

Przed zainstalowaniem nowego przełącznika w sieci należy się dokładnie zapoznać z dokumentacją dostarczoną przez producenta i dobrze zrozumieć sposób jego działania. Niektórzy producenci nie włączają domyślnie protokołu drzewa rozpinającego na wszystkich portach. Inni implementują funkcje specjalne lub wersje protokołu drzewa rozpinającego specyficzne dla dostawców.

Zazwyczaj producenci dokładają starań, aby ich implementacja protokołu drzewa rozpinającego bezproblemowo działała ze wszystkimi innymi przełącznikami. Istnieje jednak tyle odmian własności i konfiguracji, że czasami mogą się pojawić pewne problemy. Problemów można uniknąć dzięki czytaniu dokumentacji oraz testowaniu nowych przełączników przed wdrożeniem ich w sieci.

[1] W standardzie IEEE 802.1Q (uwaga 1., s. 319) można znaleźć stwierdzenie, że „Protokoły drzewa rozpinającego określone przez ten standard zastępują wersje protokołu STP — *Spanning Tree Protocol* (STP) — zdefiniowanego w standardzie IEEE 802.1D przed 2004 rokiem, ale ułatwiają migrację, ponieważ współpracują z tymi starszymi wersjami".

W oryginalnej wersji protokołu drzewa rozpinającego stany nasłuchiwania i nauki trwały 30 sekund. W tym czasie pakiety nie były przekazywane. W nowszej wersji szybkiego protokołu drzewa rozpinającego RSTP możliwe jest przypisanie do portu typu „brzegowy", co oznacza, że wiemy, iż port jest podłączony do stacji końcowej (użytkownika komputera, telefonu VoIP, drukarki itp.), a nie do innego przełącznika. Pozwala to maszynie stanów RSTP ominąć proces uczenia się i nasłuchiwania na tym porcie i natychmiastowo przejść do stanu przekazywania.

Dzięki temu, że stacja może od razu rozpocząć wysyłanie i odbieranie pakietów, można uniknąć takich problemów jak limity czasu aplikacji na komputerach użytkowników po ich ponownym uruchomieniu.

Przed powstaniem protokołu RSTP niektórzy producenci opracowali własne wersje tej własności. Na przykład firma Cisco Systems udostępniła polecenie `portfast`, które umożliwiało portowi brzegowemu natychmiastowe rozpoczęcie przekazywania pakietów.

Chociaż nie jest to wymagane do działania protokołu RSTP, warto ręcznie skonfigurować porty brzegowe RSTP, aby uniknąć problemów w przypadku komputerów użytkowników. Ustawienie typu portu na brzegowy oznacza również, że maszyna stanów RSTP nie musi wysyłać pakietu BPDU po zmianie stanu łącza (włączenia łącza lub jego wyłączenia) na tym porcie. Własność ta umożliwia zmniejszenie natężenia ruchu związanego z protokołem drzewa rozpinającego w sieci.

Wynalazczyni protokołu drzewa rozpinającego, Radia Perlman, napisała wiersz opisujący, jak działa protokół[2]. Czytając wiersz, warto wiedzieć, że w kategoriach matematycznych sieć może być reprezentowana jako typ grafu znany jako siatka (ang. *mesh*) oraz że celem protokołu drzewa rozpinającego było przekształcenie dowolnej struktury sieci w strukturę drzewa bez pętli.

Co do grafów — zacniejszego
nie uświadczysz niźli drzewo.
Drzewo bowiem z założenia
to bez pętli połączenia,
z konarami rozpiętymi
sieci wszechsięgającymi.
Najpierw musisz wybrać korzeń
— tutaj numer ci pomoże.
Do korzenia ścieżek patrzaj,
od najkrótszych je zaznaczaj.
Spec dla kabli miejsce znajdzie,
a most drzewo wnet odnajdzie.

— Radia Perlman
Algorym

Ten krótki opis ma na celu jedynie dostarczenie podstawowego opisu działania systemu. Jak można się spodziewać, jest więcej szczegółów i zawiłości, które tutaj nie zostały omówione. Kompletny opis działania maszyny stanów drzewa rozpinającego zawarto w standardach IEEE 802.1. Warto do nich zajrzeć w celu pełniejszego zrozumienia sposobu działania protokołu.

[2] R. Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, wydanie 2., Addison-Wesley, New York 1999, s. 46.

Szczegółowe informacje na temat specyficznych dla producentów ulepszeń protokołu drzewa rozpinającego można znaleźć w dokumentacji wskazanego dostawcy. Więcej informacji można również znaleźć za pośrednictwem łączy wymienionych w dodatku A.

Problemy wydajności przełączników

Pojedyncze pełnodupleksowe połączenie Ethernet jest przeznaczone do przesyłania ramek Ethernet pomiędzy interfejsami Ethernet po obu stronach. Połączenie działa ze znaną przepływnością i znaną maksymalną liczbą ramek na sekundę[3]. Wszystkie połączenia Ethernet dla danej prędkości charakteryzują się taką samą szybkością transmisji i szybkością przesyłania ramek. Jednak dodanie przełączników do systemu sieciowego tworzy bardziej złożony system. Teraz limity wydajności sieci są określone przez wydajność połączeń Ethernet oraz przełączników. Zależą także od wszelkich zatorów, które mogą wystąpić w systemie, w zależności od topologii. To do użytkownika należy obowiązek zadbania o to, aby zakupione przełączniki miały możliwość wykonania pracy.

Wewnętrzna elektronika przełączników może nie być w stanie utrzymać pełnej szybkości przesyłania ramek dla ruchu ze wszystkich portów. Inaczej mówiąc, jeśli na wszystkich portach przełącznika jednocześnie pojawi się wysokie obciążenie ruchu i będzie to obciążenie ciągłe, a nie tylko krótkie impulsy, przełącznik może nie być w stanie obsłużyć zakumulowanej szybkości połączenia i może zacząć gubić ramki. Jest to tzw. *blokowanie* — stan, który występuje w układzie przełącznika, kiedy nie ma wystarczających dostępnych zasobów do zapewnienia przepływu danych przez przełącznik. *Przełącznik nieblokujący* to taki, który zapewnia wystarczającą wewnętrzną zdolność przełączania, aby możliwe było obsłużenie pełnego obciążenia, nawet jeśli wszystkie porty są równocześnie aktywne przez długi czas. Jednak nawet nieblokujący przełącznik — w zależności od wzorców ruchu — może gubić ramki w warunkach przeciążenia.

Wydajność przekazywania pakietów

Typowy przełącznik ma dedykowane obwody wsparcia, które są przeznaczone do poprawienia szybkości, z jaką przełącznik może przesłać ramkę i wykonać takie podstawowe funkcje jak wyszukiwanie adresów ramek w bazie danych filtrowania. Ponieważ obwody wspierające i szybka pamięć buforowa są droższymi komponentami, całkowita wydajność przełącznika zależy od przyjętego kompromisu pomiędzy kosztami tych wysokowydajnych komponentów a ceną, jaką jest skłonna zapłacić większość klientów. W związku z tym można zauważyć, że nie wszystkie przełączniki działają równie wydajnie.

Niektóre tańsze urządzenia mogą mieć niższą wydajność przekazywania pakietów, mniejsze tabele filtrowania adresów i mniejsze pamięci buforowe. Większe przełączniki z większą liczbą portów mają zazwyczaj komponenty wyższej wydajności, w związku z czym są droższe. Przełączniki zdolne do obsługi maksymalnej szybkości przekazywania ramek we wszystkich swoich portach, określane także jako przełączniki nieblokujące, mogą pracować w *prędkości łącza*. W pełni nieblokujące przełączniki, które mogą jednocześnie obsługiwać maksymalną

[3] Na przykład sieć LAN Ethernet działająca z szybkością 100 Mb/s LAN w przypadku ramki o minimalnym rozmiarze 64 bajtów może wysłać maksymalnie 148 809 ramek na sekundę.

szybkość transmisji na wszystkich portach, są dziś powszechnie dostępne, ale zawsze warto sprawdzić specyfikację przełącznika, który bierzemy pod uwagę.

Wymagana wydajność i cena kupowanych przełączników mogą się różnić w zależności od ich lokalizacji w sieci. Przełączniki używane w rdzeniu sieci muszą mieć wystarczającą ilość zasobów do obsługi dużych obciążeń ruchu sieciowego. Jest tak, ponieważ w rdzeniu sieci zbiega się ruch z wszystkich stacji roboczych. Przełączniki rdzeniowe muszą mieć wystarczające zasoby do obsługi wielu transmisji i dużego obciążenia ruchu trwającego przez długi czas. Z drugiej strony przełączniki stosowane na brzegach sieci mogą mieć mniejszą wydajność, ponieważ są one potrzebne jedynie do obsługi obciążenia ruchem tylko z bezpośrednio podłączonych stacji.

Pamięć portu przełącznika

Wszystkie przełączniki zawierają pewną ilość szybkiej pamięci buforowej, w której ramki są przechowywane przez krótki czas, zanim zostaną przekazane do innego portu lub portów przełącznika. Mechanizm ten jest znany jako *przełączanie typu store-and-forward* (dosł. zapamiętaj i przekaż). Wszystkie przełączniki zgodne ze standardem IEEE 802.1D działają w trybie *store-and-forward*. W tym trybie przed przekazaniem pakiet jest w pełni odbierany w porcie i umieszczany (zapamiętywany) w szybkiej pamięci bufora portu. Większa ilość pamięci bufora umożliwia mostowi obsługiwanie dłuższych strumieni ramek, co skutkuje lepszą wydajnością przełącznika w warunkach wzmożonego ruchu w sieci LAN. W powszechnie stosowanych projektach przełączników wykorzystuje się pulę szybkiej pamięci buforowej, która w miarę potrzeby może być przydzielana dynamicznie do indywidualnych portów przełącznika.

Procesor przełącznika i pamięć RAM

Biorąc pod uwagę, że przełącznik jest w zasadzie specjalizowanym komputerem, centralny procesor i RAM w przełączniku mają istotne znaczenie dla takich funkcji jak działanie procesu drzewa rozpinającego, dostarczanie informacji potrzebnych do zarządzania, obsługa strumieni pakietów multiemisji oraz zarządzanie portami przełącznika i konfiguracją funkcji.

Jak zwykle w branży komputerowej, im większa wydajność procesora i ilość pamięci RAM, tym lepiej, ale za te cechy trzeba również więcej zapłacić. Producenci często nie udostępniają klientom specyfikacji procesora i pamięci RAM przełącznika. Zazwyczaj w przypadku droższych przełączników informacje te są dostępne, ale dla określonego przełącznika nie można zamówić szybszego procesora lub większej ilości pamięci RAM. Informacje te mogą się okazać przydatne do porównania modeli różnych dostawców. W ten sposób możemy znaleźć te przełączniki, które mają najlepsze parametry.

Specyfikacje przełącznika

Wydajność przełącznika zawiera szereg metryk, w tym maksymalną przepustowość lub zdolność przełączania wewnętrznej elektroniki przełącznika. Należy również zwrócić uwagę na maksymalną liczbę adresów MAC, które może pomieścić baza danych adresów, a także na maksymalną szybkość, wyrażoną w liczbie pakietów na sekundę, jaką przełącznik może przekazać we wszystkich portach.

Poniżej zamieszczono zbiór specyfikacji przełącznika skopiowany z typowego arkusza produktu. Specyfikacje producenta zostały zapisane kursywą. Dla uproszczenia w tym przykładzie pokażemy specyfikację dla małego, taniego przełącznika z pięcioma portami. Zaprezentowanie specyfikacji ma na celu pokazanie kilku typowych wartości przełączników. Ma także pomóc w zrozumieniu, co oznaczają te wartości oraz co się dzieje, gdy hasła marketingowe i dane techniczne spotkają się na jednej stronie.

Przekazywanie

Store-and-forward

Dotyczy standardowego działania przełącznika 802.1D. Przed przekazaniem pakiet jest w całości odbierany i zapisywany do bufora portu (zapamiętywany)[4].

Buforowanie pakietów on-chip 128 KB

Całkowita ilość pamięci buforowania pakietów dostępna dla wszystkich portów. Buforowanie jest współdzielone pomiędzy portami na żądanie. Jest to typowy poziom buforowania dla małych, pięcioportowych przełączników przeznaczonych do obsługi połączeń klienckich w warunkach domowych.

Wydajność

Przepustowość: 10 Gb/s (bez blokowania)

Ponieważ ten przełącznik może obsługiwać pełne obciążenie ruchu na wszystkich portach działających przy maksymalnej szybkości ruchu na każdym porcie, jest to przełącznik nieblokujący. Każdy z pięciu portów może pracować z szybkością do 1 Gb/s. W trybie pełnego dupleksu maksymalna szybkość przesyłania pakietów za pośrednictwem przełącznika z wszystkimi portami aktywnymi może wynosić 5 Gb/s w kierunku wychodzącym (zwanym także kierunkiem *egress*) i 5 Gb/s w kierunku przychodzącym (zwanym także kierunkiem *ingress*). Producenci w specyfikacji lubią podawać łączną, zagregowaną przepustowość 10 Gb/s, chociaż 5 Gb/s danych *ingress* na pięciu portach jest wysyłanych jako 5 Gb/s danych *egress*. Gdybyśmy przyjęli, że maksymalna wartość transferu danych przez przełącznik wynosi 5 Gb/s, technicznie mielibyśmy rację, ale w ten sposób nie odnieślibyśmy sukcesu w marketingu[5].

Prędkość przekazywania

Port 10 Mb/s: 14 800 pakietów/sek.

Port 100 Mb/s: 148 800 pakietów/sek.

Port 1000 Mb/s: 1 480 000 pakietów/sek.

Dane te pokazują, że porty mogą obsługiwać pełną szybkość przełączania pakietów składających się z ramek Ethernet o minimalnej wielkości (64 bajty). Jest to największa szybkość pakietów przy najmniejszym rozmiarze ramki. Większe ramki mogą być przesyłane w mniejszej liczbie ramek na sekundę, zatem jest to specyfikacja szczytowej

[4] Niektóre przełączniki przeznaczone do stosowania w centrach danych i innych wyspecjalizowanych sieciach obsługują tryb pracy zwany *przełączaniem cut-through*, w którym proces przekazywania pakietu rozpoczyna się, zanim cały pakiet zostanie wczytany do pamięci bufora. Celem tej metody jest skrócenie czasu wymaganego do przekazania pakietu za pomocą przełącznika. Ponadto w tej metodzie pakiety są przekazywane z błędami, ponieważ przekazywanie pakietu rozpoczyna się przed otrzymaniem pola kontroli błędów.

[5] Gdyby producenci przełączników sprzedawali samochody, wtedy prawdopodobnie samochód z wartością 200 km/h na prędkościomierzu sprzedawaliby jako pojazd, który ma zagregowaną łączną prędkość 800 km/h, ponieważ każde z czterech kół może osiągnąć szybkość 200 km/h w tym samym czasie. Jest to tzw. arytmetyka marketingowa wykorzystywana na rynku urządzeń sieciowych.

wydajności przełącznika Ethernet. Pokazuje to, że przełącznik może obsłużyć maksymalną szybkość przesyłania pakietów we wszystkich portach i dla wszystkich obsługiwanych szybkości.

Opóźnienie (w przypadku pakietów 1500-bajtowych)
10 Mb/s: 30 mikrosekund (maks.)
100 Mb/s: 6 mikrosekund (maks.)
1000 Mb/s: 4 mikrosekundy (maks.)

Jest to czas potrzebny na przekazanie ramki Ethernet z portu odbiorczego do portu nadawczego przy założeniu, że port nadawczy jest dostępny i nie jest zajęty nadawaniem innej ramki. Jest to miara wewnętrznego opóźnienia przełączania nałożonego przez elektronikę przełącznika. Wartość ta jest również prezentowana jako 30 µs, z wykorzystaniem greckiego znaku µ (mi) oznaczającego „mikro". Mikrosekunda to jedna milionowa sekundy, a opóźnienie 30 milionowych sekundy dla portu działającego z szybkością 10 Mb/s jest rozsądną wartością dla taniego przełącznika. Podczas porównywania przełączników warto pamiętać, że im niższa wartość, tym lepiej. Droższe przełączniki zazwyczaj charakteryzują się niższymi opóźnieniami.

Baza danych adresów MAC: 4000

Ten przełącznik może obsługiwać do 4000 unikatowych adresów stacji w bazie danych adresów. Wartość tego rzędu jest całkowicie wystarczająca dla pięcioportowego przełącznika przeznaczonego do wykorzystania w domu i małej firmie.

Średni czas między awariami (ang. *Mean time between failures, MTBF*)*: >1 milion godzin (~114 lat)*

Współczynnik MTBF jest wysoki, ponieważ ten przełącznik jest mały, nie ma wentylatora, który mógłby się zużyć, i ma małą liczbę komponentów. Nie ma w nim zbyt wielu elementów, które mogłyby się zepsuć. To nie znaczy, że przełącznik nie może ulec awarii, ale w zastosowanych układach elektronicznych występuje niewiele awarii, dlatego średni czas między awariami dla tego przełącznika jest bardzo wysoki[6].

Zgodność ze standardami
IEEE 802.3i 10BASE-T Ethernet
IEEE 802.3u 100BASE-TX Fast Ethernet
IEEE 802.3ab 1000BASE-T Gigabit Ethernet
Uwzględnia znaczniki priorytetów IEEE 802.1p oraz DSCP
Ramki jumbo: do 9720 bajtów

Pod hasłem „zgodność ze standardami" sprzedawca rozumie listę standardów, z którymi ten przełącznik jest zgodny. Pierwsze trzy pozycje oznaczają, że porty przełącznika obsługują standardy Ethernetu na skrętce dla szybkości 10, 100 i 1000 Mb/s. Szybkości te są automatycznie wybierane w interakcji z połączeniem klienta przy użyciu ethernetowego protokołu automatycznej negocjacji. Sprzedawca twierdzi także, że ten przełącznik honoruje znaczniki priorytetów klas usług na poziomie ramek Ethernet. W warunkach zatorów w pierwszej kolejności są odrzucane te ramki, które mają znaczniki niższego priorytetu. Ostatnia pozycja na tej liście informuje, że przełącznik może obsługiwać niestandardowe rozmiary ramki Ethernet, często zwane *ramkami*

[6] Życzę szczęścia przy próbie zwrotu pieniędzy za przełącznik, który popsuje się na przykład po 70 latach. Jeśli nawet będziemy żyli tak długo, to producent przełącznika prawdopodobnie nie.

jumbo. Czasami są one konfigurowane w interfejsach Ethernet dla określonej grupy klientów i ich serwerów w dążeniu do poprawy wydajności[7].

Ten zbiór specyfikacji producenta pokazuje, jakie szybkości portów obsługuje przełącznik, i daje wyobrażenie o tym, jak sprawnie przełącznik będzie działał w systemie. Kupując większe przełączniki o wyższej wydajności, przeznaczone do zastosowania na poziomie rdzenia sieci, należy zwrócić uwagę na inne specyfikacje przełączników. Są to między innymi wsparcie dla dodatkowych funkcji, takich jak protokoły zarządzania multiemisji, dostęp do wiersza poleceń umożliwiający skonfigurowanie przełącznika oraz protokół SNMP (ang. *Simple Network Management Protocol*) pozwalający na monitorowanie działania i wydajności przełącznika.

Jeśli korzystamy z przełączników, powinniśmy pamiętać o wymaganiach dotyczących ruchu sieciowego. Jeśli na przykład sieć zawiera wysokowydajne klienty żądające usług od pojedynczego serwera lub zbioru serwerów, to każdy przełącznik, którego użyjemy, musi mieć wystarczająco wysoką wewnętrzną wydajność przełączania, odpowiednio wysokie szybkości działania portów i szybkości łączy *uplink* oraz wystarczający rozmiar buforów portów do obsługi zadania. Ogólnie rzecz biorąc, droższe przełączniki zbudowane na bazie wysokowydajnych komponentów mają również duże możliwości buforowania. Trzeba jednak dokładnie przeczytać specyfikacje i porównać oferty różnych dostawców, aby mieć pewność dobrania najlepszego przełącznika do wybranego zastosowania.

Podstawowe funkcje przełączników

Po omówieniu podstawowego działania przełączników przejdziemy do opisania niektórych funkcji, które przełączniki obsługują. Wielkość sieci i jej przewidywany rozwój wpływają na sposób korzystania z przełączników Ethernet oraz na rodzaje funkcji przełączników, które są potrzebne. W sieci działającej w domu lub pojedynczej przestrzeni biurowej wystarczy jeden lub kilka małych i tanich przełączników, które zapewniają podstawowe usługi Ethernet z szybkościami wystarczającymi do spełnienia naszych potrzeb. Ewentualnie przełączniki te mogą być wzbogacone kilkoma dodatkowymi funkcjami. Takie sieci nie są na tyle złożone, aby spodziewać się, że wystąpią problemy ze stabilnością. Nie można również oczekiwać zbyt dużego rozwoju tych sieci.

Z drugiej strony sieci średniej wielkości, które obsługują wiele biur, mogą potrzebować bardziej zaawansowanych przełączników z pewnymi funkcjami ułatwiającymi ich zarządzanie i konfigurację. Jeśli stacje robocze wymagają wysokowydajnych sieci w celu uzyskania dostępu do serwerów plików, to w sieci mogą być potrzebne przełączniki wyposażone w szybkie porty *uplink*. Większe sieci kampusowe złożone z setek lub nawet tysięcy połączeń sieciowych zazwyczaj mają strukturę hierarchiczną bazującą na przełącznikach z szybkimi portami *uplink*. W takich przełącznikach są potrzebne bardziej zaawansowane funkcje umożliwiające zarządzanie siecią i wspomagające utrzymanie stabilności sieci.

[7] Ramki *jumbo* mogą działać lokalnie dla określonego zbioru komputerów, którymi zarządzamy i które skonfigurujemy. Jednak w internecie działają miliardy portów Ethernet, które pracują ze standardowym maksymalnym rozmiarem ramki 1500 bajtów. Aby zapewnić sprawne działanie systemu w internecie, należy utrzymywać standardowe rozmiary ramek.

Zarządzanie przełącznikami

W zależności od ceny przełączniki mogą być wyposażone w interfejs zarządzania i oprogramowanie zarządzające, które pozwala na zbieranie i wyświetlanie statystyk dotyczących pracy przełącznika, aktywności sieci, ruchu w portach i błędów. Wiele droższych przełączników oferuje pewien zakres funkcji zarządzających. Producenci zazwyczaj dostarczają oprogramowanie zarządzające działające w przeglądarce internetowej. Czasami również pozwala ono na zalogowanie się do przełącznika za pośrednictwem portu konsoli na przełączniku lub przez sieć.

Oprogramowanie zarządzające umożliwia skonfigurowanie szybkości portów i funkcji na przełączniku. Dostarcza również informacji monitorowania na temat działania przełącznika i jego wydajności. Przełączniki, które obsługują protokół drzewa rozpinającego, zazwyczaj dostarczają także interfejs zarządzania, który pozwala skonfigurować działanie algorytmu drzewa rozpinającego na poziomie każdego portu przełącznika. Do innych konfigurowalnych opcji mogą należeć szybkość portu, funkcje automatycznej negocjacji oraz inne obsługiwane zaawansowane funkcje przełączników.

Protokół SNMP

Wiele systemów zarządzania przełączników używa protokołu SNMP (ang. *Simple Network Management Protocol*), który zapewnia niezależny od producenta sposób wyodrębniania informacji o działaniu przełącznika. Informacje te obejmują zazwyczaj wartości natężenia ruchu na portach przełącznika, liczniki błędów pozwalające na identyfikację urządzeń, w których występują problemy, i wiele innych. Pakiety oprogramowania do zarządzania siecią bazujące na protokole SNMP mogą pobierać informacje z wielu urządzeń sieciowych, a nie tylko z przełączników.

Na rynku dostępnych jest wiele pakietów oprogramowania, które pozwalają pobierać z przełącznika informacje zarządzania bazujące na protokole SNMP i wyświetlać je administratorowi sieci. Dostępnych jest również kilka pakietów open source, które zapewniają dostęp do informacji SNMP i pozwalają wyświetlać te informacje w postaci wykresów oraz zestawień tekstowych. Łącza do bardziej szczegółowych informacji można znaleźć w rozdziale 21.

Porty-lustra

Kolejną przydatną funkcją przełączników umożliwiającą monitorowanie i rozwiązywanie problemów są *porty-lustra pakietów*. Własność ta umożliwia skopiowanie ruchu z jednego lub większej liczby portów przełącznika do portu-lustra. Do portu-lustra można podłączyć laptop, na którym działa aplikacja analizatora sieci, aby w ten sposób przeprowadzić badania ruchu sieciowego.

Port-lustro może być bardzo przydatny do śledzenia problemów w sieci na urządzeniach podłączonych do wybranego przełącznika. Producenci zastosowali różne podejścia do portów-luster. Mają one różne możliwości i ograniczenia w zależności od konkretnej implementacji. Niektórzy producenci pozwalają również na to, aby ruch z portu-lustra był skierowany przez sieć do zdalnego odbiornika. Dzięki temu można zdalnie rozwiązywać problemy sieciowe. Porty-lustra nie są ustandaryzowaną funkcją przełączników, dlatego producenci mogą zapewniać obsługę tej własności, lecz nie muszą tego robić.

Filtry ruchu przełączników

Filtry ruchu przełączników umożliwiają menedżerom sieci określenie reguł filtrowania ramek Ethernet na podstawie zbioru parametrów. Zakres filtrów obsługiwanych przez przełączniki różni się w zależności od producenta. Tańsze urządzenia bez interfejsów zarządzania nie mają funkcji filtrowania, natomiast urządzenia droższe i o wyższej wydajności mogą oferować kompletny zestaw filtrów dostępnych do ustawiania przez administratora sieci.

Za pomocą tych filtrów menedżer sieci może skonfigurować przełączniki tak, aby sterowały ruchem w sieci na podstawie takich informacji jak adresy ramek Ethernet oraz typ protokołu wysokiego poziomu przesyłany za pośrednictwem ramek. Filtry mogą wpływać na pogorszenie wydajności, należy zatem sprawdzić w dokumentacji przełącznika, jaki efekt wywrze zastosowanie określonego filtra.

Filtry działają na zasadzie porównywania wzorców wyrażonych w postaci wartości liczbowych lub nazw portów protokołu (np. HTTP, SSH) z wzorcami bitowymi występującymi w ramkach Ethernet. Kiedy wzorzec jest zgodny, filtr inicjuje pewne działania — zazwyczaj polegają one na odrzuceniu ramki, a tym samym na zablokowaniu ruchu. Należy pamiętać, że stosując filtry, możemy spowodować tyle samo problemów, ile próbujemy rozwiązać.

Filtry, które mają dopasowywać wzorce w polu danych ramki, mogą stwarzać problemy, w przypadku gdy te wzorce występują również w ramkach, których nie chcemy filtrować. Filtr ustawiony tak, aby pasował do jednego zbioru liczb szesnastkowych w określonym miejscu w polu danych ramki, może działać dobrze dla protokołu sieciowego, którym próbujemy sterować, ale może również zablokować protokół sieciowy, o którym nawet nie wiedzieliśmy, że istnieje.

Tego rodzaju filtry są zwykle stosowane do sterowania przepływem określonego protokołu sieciowego. Działają na zasadzie identyfikacji części protokołu w polu danych ramki Ethernet. Niestety, menedżerowi sieci trudno przewidzieć zakres danych, które mogą być przesyłane w sieci. W zależności od konstrukcji filtra może on pasować do ramek, które nie miały być filtrowane. Debugowanie awarii spowodowanych przez nieodpowiednio zdefiniowany filtr może być trudne. Zwykle nie jest jasne, dlaczego zazwyczaj dobrze funkcjonujący Ethernet przestaje działać dla określonej aplikacji lub na pewnym zbiorze stacji.

Filtry w przełącznikach są często stosowane jako próba uzyskania większej kontroli poprzez zapobieganie interakcji w warstwie działania wysokopoziomowego protokołu sieciowego. Jeśli właśnie dlatego implementujemy filtry przełączników, to powinniśmy rozważyć użycie routerów warstwy 3., które działają w warstwie sieci i automatycznie zapewniają ten poziom izolacji, bez potrzeby ręcznego konfigurowania filtrów.

Routery warstwy 3. dostarczają również funkcji filtrowania, które mogą być łatwiejsze do wdrożenia, ponieważ są przeznaczone do pracy w obszarach pól i adresów protokołów wysokiego poziomu. W ten sposób można w prosty sposób napisać filtr, który chroni sprzęt sieciowy przed atakiem, na przykład poprzez ograniczanie dostępu do adresów TCP/IP zarządzania urządzeniami. Więcej informacji na temat zastosowań routerów zamieścimy w następnym rozdziale.

Zarządzanie filtrami przełączników

Właściwe skonfigurowanie filtrów oraz utrzymywanie ich, kiedy już zostaną skonfigurowane, może być złożonym przedsięwzięciem. W miarę jak sieć się rozwija, trzeba śledzić, które

przełączniki mają filtry, i upewnić się, w jaki sposób skonfigurowane filtry wpływają na działanie systemu w sieci. Często bowiem trudno przewidzieć, jakie mogą być skutki działania filtra.

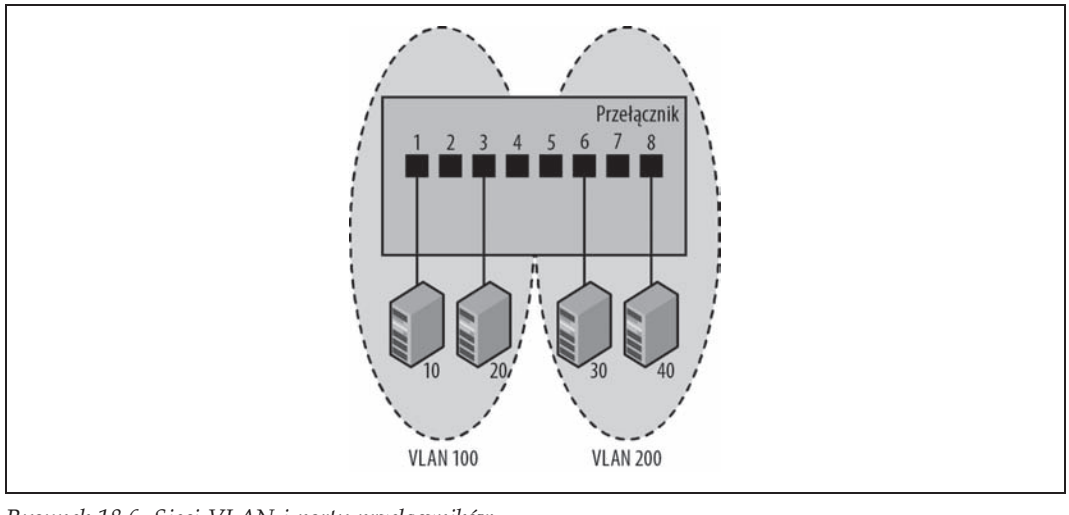
Dokumentowanie zastosowanych filtrów oraz sposobu, w jaki są one wykorzystywane, może skrócić czas rozwiązywania problemów. Jednak bez względu na to, jak dobrze udokumentowane są filtry, filtry dopasowujące mogą powodować przestoje. W związku z tym filtry należy stosować tylko wtedy, gdy jest to konieczne, i z zachowaniem jak największej ostrożności.

Wirtualne sieci LAN

Szeroko stosowaną własnością, która zazwyczaj jest dostępna w droższych przełącznikach, jest możliwość grupowania portów przełącznika w wirtualne sieci lokalne, zwane również sieciami VLAN. Mówiąc prościej, sieć VLAN to grupa portów przełącznika, które działają tak, jakby były niezależnymi przełącznikami. Tworzy się je poprzez manipulowanie oprogramowaniem przekazywania ramek w przełączniku.

Jeśli producent obsługuje sieci VLAN w przełączniku, dostarcza interfejs zarządzania, który pozwala menedżerowi sieci skonfigurować to, które porty należą do danych sieci VLAN.

Jak pokazano na rysunku 18.6, można skonfigurować ośmioportowy przełącznik w taki sposób, że porty od 1. do 4. będą w jednej sieci VLAN (nazwanej tu VLAN 100), natomiast porty od 5. do 8. w innej (nazwanej tutaj VLAN 200). Pakiety mogą być przesyłane z 10. do 20. stacji, ale nie z 10. do 30. i 40. stacji. Ponieważ te sieci VLAN działają jako odrębne sieci, pakiety rozgłoszeniowe lub multiemisji wysłane w sieci VLAN 100 nie będą przesyłane do portów należących do sieci VLAN 200 — sieci VLAN zachowują się tak, jakbyśmy rozdzielili ośmioportowy przełącznik na dwa niezależne czteroportowe przełączniki.



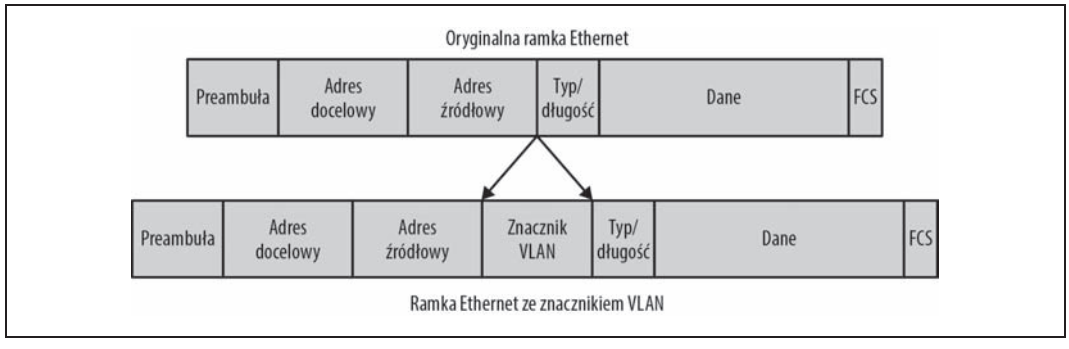
Rysunek 18.6. Sieci VLAN i porty przełączników

Producenci dostarczają także innych własności sieci VLAN. Na przykład członkostwo w sieci VLAN może bazować na zawartości ramek zamiast wyłącznie na określeniu tego, które porty przełącznika są członkami wskazanej sieci VLAN. W tym trybie pracy ramki po odebraniu w porcie przełącznika są przesyłane przez zestaw filtrów. Filtry są skonfigurowane w taki sposób, aby ramki spełniały pewne kryterium, np. adres źródłowy w ramce lub zawartość pola

typu, która określa wysokopoziomowy protokół przesyłany w polu danych ramki. Sieci VLAN definiuje się zgodnie z tymi filtrami. W zależności od tego, jaki zestaw kryteriów spełniają ramki, są one automatycznie umieszczane w odpowiednich sieciach VLAN.

Standard VLAN 802.1Q

Standard znakowania sieci VLAN IEEE 802.1Q został opublikowany po raz pierwszy w 1998 roku. Określa on niezależny od producenta sposób implementacji sieci VLAN. Jak pokazano na rysunku 18.7, system znakowania VLAN wykorzystany w standardzie 802.1Q dodaje cztery bajty danych do ramki Ethernet — za adresem docelowym, a przed polem typu lub rozmiaru. Zwiększa to maksymalny rozmiar ramki w sieci Ethernet do 1522 bajtów.



Rysunek 18.7. Ramka Ethernet ze znacznikiem VLAN

Standard 802.1Q zapewnia również obsługę priorytetów ramek Ethernet przy użyciu bitów klasy usług CoS (ang. *Class of Service*) zdefiniowanych w standardzie 802.1p. Standard 802.1Q zapewnia miejsce w znaczniku VLAN, które pozwala korzystać z bitów CoS 802.1p do określenia priorytetów ruchu. Istnieją trzy bity zarezerwowane dla wartości CoS. Dzięki temu możliwe jest zastosowanie ośmiu wartości (0 – 7) do zidentyfikowania ramek o różnych poziomach usług.

Łączenie sieci VLAN

Sieci VLAN są szeroko stosowane w projektach sieciowych do zapewnienia niezależnych od siebie sieci. Pomaga to kontrolować przepływ ruchu poprzez wyizolowanie ruchu wysyłanego pomiędzy określonymi grupami stacji. Każda sieć VLAN działa jak oddzielny przełącznik. Nie ma innego sposobu na połączenie oddzielnych sieci VLAN niż zastosowanie pomiędzy nimi routera warstwy 3.

Budowanie większych sieci poprzez łączenie sieci VLAN za pomocą routerów warstwy 3. zapobiega również propagacji pakietów rozgłoszeniowych i multiemisji widocznych w dużych sieciach warstwy 2. Uzyskuje się to poprzez przeniesienie operacji przekazywania pakietów pomiędzy sieciami VLAN do protokołu warstwy 3.

Z powodu występujących pętli, nieprawidłowo działającego oprogramowania i ataków skanowania adresów może dojść do „zalewania" sieci pakietami rozgłoszeniowymi i multiemisji. Wszystkie urządzenia podłączone do określonej sieci VLAN są narażone na takie „zalewanie". Można to również opisać w ten sposób, że wszystkie urządzenia należą do tej samej „domeny awarii". Stworzenie odrębnych sieci VLAN i połączenie ich za pomocą routerów warstwy 3.

również tworzy odrębne domeny awarii. Dzięki podłączeniu populacji urządzeń w osobnych sieciach VLAN można ograniczyć liczbę urządzeń w określonej domenie awarii, a tym samym poprawić niezawodność, dostępność i stabilność sieci.

Protokół MSTP 802.1Q

Protokół MSTP (ang. *Multiple Spanning Tree Protocol*) został opracowany w suplemencie 802.1s w 2003 roku i został włączony do wydania standardu 802.1Q z 2005 roku. Bazuje na protokole RSTP i jest zdefiniowany jako opcjonalne rozszerzenie protokołu RSTP, które pozwala przełącznikom obsługującym sieci VLAN na korzystanie z wielu drzew rozpinających.

Dzięki temu ruch należący do różnych sieci VLAN może przepływać przez różne ścieżki w obrębie tej samej sieci przełączników. Zatem standard MSTP jest „świadomy istnienia sieci VLAN" i dobrze nadaje się do pracy w sieciach zawierających wiele sieci VLAN oraz wiele ścieżek *uplink*. Protokół MSTP zaprojektowano również z myślą o zminimalizowaniu liczby pakietów BPDU potrzebnych do zbudowania drzew rozpinających dla wielu sieci VLAN. W związku z tym taki system jest bardziej wydajny.

Należy zauważyć, że klasyczny protokół STP i nowszy protokół RSTP dla wielu sieci są wystarczające. Nawet wtedy, gdy nie ma sieci VLAN w sieci, protokoły te nadal są w stanie zablokować ścieżki pętli. Protokół MSTP opracowano w celu zapewnienia „świadomości istnienia sieci VLAN" w przypadku bardziej złożonych projektów sieciowych oraz w celu stworzenia bardziej efektywnego modelu działania bazującego na wielu „regionach" drzewa rozpinającego. W tych regionach może działać wiele egzemplarzy drzewa rozpinającego (ang. *Multiple Spanning Tree*, MST) — do 64. Zastosowanie wielu regionów wymaga, aby administrator sieci skonfigurował mosty MST jako członków określonych regionów, co potencjalnie powoduje, że MST są bardziej skomplikowane w konfiguracji i obsłudze.

Podczas gdy standard MST zapewnia korzyści polegające na strukturyzacji dużego systemu na regiony i zmniejszeniu ilości przetwarzania potrzebnego do utrzymania drzewa rozpinającego, może także wymagać więcej wysiłku na początku — trzeba bowiem zrozumieć zasady dotyczące konfiguracji i zaimplementować je w przełącznikach. Producenci przyjęli MSTP jako domyślny system drzewa rozpinającego na niektórych przełącznikach — zazwyczaj wysokowydajnych systemach przeznaczonych do użytku w centrach danych i zdolnych do obsługi dużej liczby sieci VLAN. Jednak protokół RSTP i klasyczny protokół STP są nadal powszechnie stosowanymi wersjami protokołu drzewa rozpinającego. Dzięki własności „plug and play" oraz zdolności do tworzenia drzewa rozpinającego bez wkładania wysiłku w konfigurację systemy te okazują się skuteczne w wielu projektach sieciowych.

Jakość usług (QoS)

Zarządzanie priorytetami ruchu w celu faworyzowania niektórych rodzajów ruchu w stosunku do innych kategorii w warunkach zatłoczenia to kolejna możliwość przełączników. 32-bitowe pole dodane przez standard IEEE 802.1Q zapewnia wsparcie dla pól priorytetyzacji ruchu. Pola te umożliwiają rozróżnienie ośmiu różnych wartości klas usług, jak również znaczników VLAN.

Standard 802.1p określa poziomy priorytetyzacji ruchu, które są przesyłane w tagu 802.1Q CoS i używane do oznaczenia ramki z wartością priorytetu. Dzięki temu w przypadku wystąpienia przeciążenia sieci na porcie przełącznika niektóre rodzaje ruchu mogą być faworyzowane.

Jeśli skonfigurowano CoS na porcie przełącznika, to w sytuacji gdy port stanie się zatłoczony, ramki Ethernet, które nie są oznaczone wysokim priorytetem, zostają odrzucone jako pierwsze.

Jeśli przełącznik obsługuje te funkcje, trzeba się zapoznać z dokumentacją dostawcy w celu uzyskania instrukcji ich konfiguracji. Chociaż standardy IEEE opisują mechanizmy, które umożliwiają stosowanie priorytetów, to standardy nie określają, jak te własności powinny być zaimplementowane lub skonfigurowane. Decyzje w tej sprawie należą do każdego producenta. Oznacza to, że szczegółowych informacji na temat stosowania priorytetów w określonym przełączniku należy szukać w dokumentacji dostawcy sprzętu.

Skorowidz

4

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

Q

R

S

Ś

T

U

W

X

Z

Ż

O'REILLY®

Ethernet
Biblia administratora

Standard Ethernet powstał w 1976 roku w ośrodku badawczym firmy Xerox. Wykorzystywany do budowy sieci lokalnych, znajduje zastosowanie praktycznie w każdym miejscu. Sieci Ethernet spotkasz zarówno w mieszkaniach czy domach, jak i w biurach czy centrach danych. W zależności od budżetu, jakim dysponujesz, możesz zbudować sieć dostosowaną do własnych potrzeb. Nowoczesne sieci Ethernet pozwalają na niezawodne przesyłanie danych z ogromnymi prędkościami. W Twoje ręce oddajemy biblię wiedzy o sieciach Ethernet, która odpowie na wszystkie nurtujące Cię pytania oraz zaprezentuje nowoczesne techniki wykorzystania tych sieci. Przekonasz się, jak wygląda proces automatycznej negocjacji oraz jak zasilać urządzenia za pomocą Ethernetu. W kolejnych rozdziałach znajdziesz charakterystyczne elementy popularnych sieci 10, 100 i 1000 Mb/s oraz niezwykle wydajnych sieci o prędkości dochodzącej do 400 Gb/s. Trzecia część tej książki została poświęcona budowie systemu Ethernet. Poznasz tu systemy okablowania strukturalnego, dostępne kable, złącza oraz przełączniki. Książka ta jest obowiązkową pozycją na półce każdego administratora, który chce dogłębnie poznać swoją sieć.

Dzięki tej książce:

- poznasz historię standardu Ethernet
- zrozumiesz zasadę jego działania
- zobaczysz, jaki potencjał kryją sieci Ethernet
- nauczysz się projektować wydajne rozwiązania
- poznasz tajniki działania Twojej sieci

Biblia administratora sieci Ethernet!

helion.pl
księgarnia internetowa

Nr katalogowy: 25454

Księgarnia internetowa:
http://helion.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

Helion

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ
KOD KORZYŚCI

ISBN 978-83-246-9618-5

Cena 79,00 zł