

» Idź do

- Spis treści
- Przykładowy rozdział

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl
© Helion 1991-2008

Budowa sieci komputerowych na przełącznikach i routerach Cisco

Autor: Adam Józefiok

ISBN: 83-246-0680-7

Format: 158x235, stron: 304



Dowiedz się jak zaprojektować sprawnie działającą sieć komputerową

- Jak dobrać odpowiedni rodzaj sieci komputerowej?
- Jak połączyć urządzenia pracujące w sieci?
- Jak uruchomić i podłączyć router?

Sieci komputerowe zapewniają to, co we współczesnym społeczeństwie najważniejsze – szybki dostęp do informacji i komunikację między ludźmi. Wykorzystywane są niemal wszędzie: w telekomunikacji, medycynie, motoryzacji, szkolnictwie, nauce i rozrywce. Zdomowały się na dobre w małych przedsiębiorstwach i globalnych organizacjach, umożliwiając wymianę dokumentów między pracownikami i kontrahentami, a także dostęp do zasobów wewnętrznych firmy dla współpracowników mobilnych. Współczesne firmy nie mogą więc funkcjonować bez sieci, dlatego też należy zapewnić sprawne jej funkcjonowanie, odpowiednio ją przygotować i zabezpieczyć – nawet jeśli jest to tylko sieć domowa.

Książka „Budowa sieci komputerowych na przełącznikach i routerach Cisco” to niezbędny podręcznik dla wszystkich, którzy dopiero rozpoczynają swoją przygodę z sieciami komputerowymi oraz urządzeniami Cisco. Dzięki temu przewodnikowi poznasz mechanizmy działania sieci, funkcjonowanie poszczególnych urządzeń sieciowych, sposoby działania przełączników oraz routerów, a także metody konfiguracji. Nauczysz się także jak zabezpieczyć komputery przed zewnętrznymi atakami oraz przygotować system operacyjny do pracy w sieci.

- Podstawy sieci komputerowych
- Przeglądarki internetowe
- Media sieciowe
- Projektowanie sieci i okablowania
- Model sieci komputerowych
- Sieć Ethernet
- Przełączniki Cisco
- Sieci VLAN
- Protokół VTP i STP
- Routery Cisco
- Protokoły routingu
- Listy ACL i bezpieczeństwo w sieci

Twórz sieci komputerowe na własny użytek i na potrzeby biznesu

Spis treści

Wstęp	9
Część I Sieci komputerowe	11
Rozdział 1. Podstawy sieci komputerowych	13
Wstęp	13
Nieco historii	13
Dokumenty RFC	14
Co to jest sieć komputerowa i do czego służy	15
Symbole używane w książce	16
Rodzaje sieci komputerowych	16
Sieci LAN	17
Sieci WAN	17
Sieci MAN	17
Sieci PAN	19
Sieci VPN oraz SAN	19
Sieci SAN	20
Pojęcie sieci heterogenicznych i homogenicznych	20
Topologie sieciowe	21
Internet	24
Przeglądarki internetowe	25
Rozdział 2. Media sieciowe	29
Wstęp	29
Media miedziane	29
Kabel koncentryczny	30
Skrętka nieekranowana	30
Skrętka ekranowana	31
Media optyczne	36
Komunikacja bezprzewodowa	37
Rozdział 3. Działanie sieci komputerowej	41
Wstęp	41
Urządzenia pracujące w sieci	41
Urządzenia aktywne	42
Urządzenia pasywne	50

Projektowanie sieci oraz okablowania	51
Projekt sieci	51
Okablowanie	52
Szafy	53
Serwerownia	53
System zasilania	54
Przesyłanie informacji w postaci zer i jedynek	55
System binarny (dwójkowy)	55
System szesnastkowy	58
Ćwiczenia praktyczne	60
Szybkości przesyłania danych	61
Pasma	61
Transfer danych	63
Przepustowość	63
Modele sieci komputerowych	64
Formaty przesyłanych danych	64
Model ISO-OSI	65
MODEL TCP/IP	67
Enkapsulacja i deenkapsulacja	76
Adresacja w sieci	77
Klasy adresów IP	78
Konfiguracja adresów IP	81
Dzielenie na podsieci	88
Problemy podczas konfiguracji sieci	92
Rozdział 4. Sieć Ethernet	95
Wprowadzenie	95
Ethernet	95
Ramka ethernetowa	96
Mechanizm CSMA/CD	97
Rodzaje Ethernetu	99
Jak połączyć ze sobą dwa komputery?	100
Problemy po wykonaniu połączenia	101
Przeglądanie zawartości dysków	102
Część II Przełączniki Cisco	103
Rozdział 5. Informacje wstępne	105
Wprowadzenie	105
Przełącznik	106
Przełączanie w sieciach	107
Uruchamianie przełącznika	110
Sposoby podłączenia do przełącznika	111
Połączenie konsolowe	111
Metody konfiguracji	115
Linia poleceń	116
Przeglądarka internetowa	116
System menu	117
System operacyjny przełącznika	119
Tryby pracy	120
Wpisywanie poleceń	120
System pomocy	122
Pierwsza konfiguracja	124

Konfiguracja z linii komend	126
Polecenie show	127
Polecenia trybu uprzywilejowanego	133
Poznawanie sąsiadów w sieci	154
Tworzenie dziennika zdarzeń	156
Rozdział 6. Sieci VLAN	165
Wprowadzenie	165
Sieć VLAN	165
Konfiguracja sieci VLAN	166
Rozdział 7. Protokół VTP i połączenia bezpośrednie	171
Połączenia bezpośrednie	171
ISL	172
IEEE 802.1q	172
Protokół VTP	173
Rozdział 8. Protokół STP	177
Informacje wstępne	177
Problemy z nadmiarowością	178
Działanie protokołu Spanning Tree	179
Stany portów	180
Protokół RSTP	181
Część III Routery Cisco	183
Rozdział 9. Informacje wstępne na temat routerów	185
Wprowadzenie	185
Do czego służy router?	185
Budowa routera Cisco	186
Procesor	186
Pamięć	187
System operacyjny IOS	187
Interfejsy routera	188
Uruchamianie routera i pierwsze podłączenie	190
Sekwencja uruchomieniowa	190
Podłączanie do routera	190
Tryb konfiguracyjny	192
System operacyjny routera	195
Tryby pracy	195
Pomoc systemu IOS	196
Konfiguracja — podstawowe polecenia	197
Polecenia show	197
Polecenia trybu uprzywilejowanego	201
Uruchamianie serwera DHCP na routerze	208
Uruchamianie NAT	209
Poznawanie sąsiadów w sieci	214
Rozdział 10. Routing i protokoły routingu	217
Wprowadzenie	217
Routing	217
Tablice routingu	218
Protokoły routingu — informacje wstępne	219
Zewnętrzne i wewnętrzne protokoły routingu	223

Algorytmy występujące w protokołach routingu	223
Algorytm wektora odległości	223
Algorytm łączy-stan	224
Rodzaje routingu	225
Routing klasowy	225
Routing bezklasowy	225
Protokoły routingu	226
Protokół RIPv1 (klasowy)	226
Protokół RIPv2 (bezklasowy)	231
Protokół EIGRP (bezklasowy)	232
Protokół OSPF (bezklasowy)	236
Najważniejsze technologie WAN	241
Co to jest linia dzierżawiona	241
Technologie WAN	242
Rozdział 11. Listy ACL i bezpieczeństwo w sieci	247
Wprowadzenie	247
Listy ACL	247
Konfiguracja prostej listy ACL	248
Maski wzorca	249
Bezpieczeństwo pracy w sieci	251
Polityka bezpieczeństwa firmy	252
Niebezpieczeństwa w sieci	253
Obrona przed atakami	259
Zabezpieczenia systemu informatycznego	261
Przygotowanie systemu operacyjnego do pracy w sieci	264
Rozdział 12. Słownik pojęć wraz z wyjaśnieniami	267
Literatura	285
Skorowidz	287

Rozdział 8.

Protokół STP

Informacje wstępne

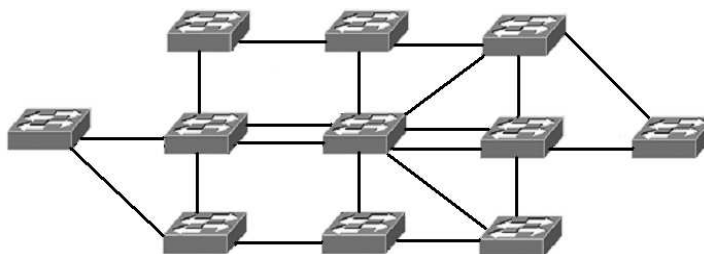
Nowoczesne sieci komputerowe muszą charakteryzować się przede wszystkim: szybkością działania, skalowalnością, a co najważniejsze — dostępnością. Wyobraź sobie sieć komputerową, której dostępność w ciągu miesiąca równa jest 10%. Oznaczałoby to, że w ciągu miesiąca tylko przez 3 dni sieć działałaby poprawnie. Nie trzeba nawet tłumaczyć, co by się stało, gdyby taka sieć została uruchomiona w banku. Oczywiście przykład jest bardzo skrajny, niemniej dzięki niemu zrozumiesz, jak ważne jest to, by sieć dostępna była o każdym czasie w ciągu całego roku.

Obecnie wszystkie duże firmy, dla których ciągłe działanie sieci w przedsiębiorstwie jest kluczowe, dążą do tego, aby osiągnąć dostępność sieci równą 100%. Stosują więc różnego rodzaju środki, aby cel ten mógł stać się realny. Szybkie serwery, markowe urządzenia sieciowe, dodatkowe linie energetyczne i wykwalifikowani specjaliści to tylko niektóre z metod, jakie umożliwiają osiągnięcie tego celu. Jedną z metod zapewnienia wysokiej dostępności w sieci jest również wprowadzenie nadmiarowości.

Nadmiarowość to nic innego jak zapewnienie kilku równoczesnych dróg do tego samego punktu docelowego (rysunek 8.1). Nadmiarowość może być związana nie tylko z łączami, ale również z urządzeniami pracującymi w sieci. Można np. duplikować główne przełączniki lub routery, żeby podczas awarii jednego z nich sieć mogła dalej realizować swoje priorytetowe zadania.

Rysunek 8.1.

Przykład nadmiarowości występującej w sieci



Na powyższym rysunku znajduje się typowy przykład zastosowania w sieci nadmiarowości. Do niektórych przełączników można dostać się nawet czterema różnymi drogami.

Pomimo ogromu zalet, jakie niesie ze sobą zastosowanie nadmiarowości w sieciach opartych na przełącznikach warstwy drugiej, istnieje również wiele problemów, z którymi administrator musi sobie poradzić, aby zastosowana nadmiarowość nie wyrządziła więcej szkody niż pożytku.

Problemy z nadmiarowością

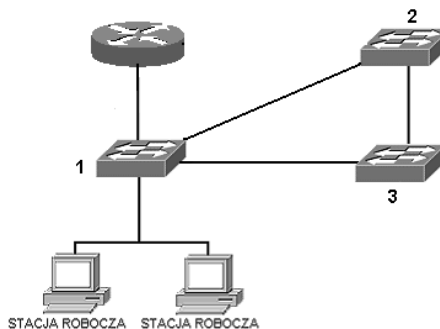
Podczas stosowania nadmiarowości w sieciach opartych na przełącznikach warstwy drugiej pojawiają się pewne problemy dotyczące transmisji ramek. Problemy są na tyle poważne, że w pewnych sytuacjach mogą unieruchomić sieć i uniemożliwić komunikację stacjom roboczym. W skrajnych przypadkach konieczne jest wyłączenie urządzeń sieciowych i ponowna ich konfiguracja (poprawna). Jak już wiesz, takie działanie znacznie obniża dostępność sieci. Dlatego opracowany został protokół STP (ang. *Spanning Tree Protocol*), który częściowo rozwiązuje niektóre problemy podczas transmisji ramek.

Zastosowanie przełączników warstwy drugiej w sieciach opartych na nadmiarowości sprzyja pojawieniu się zjawiska zwanego **burzą rozgłoszeniową** (ang. *broadcast storm*).

Burza rozgłoszeniowa związana jest z transmisją ramek rozgłoszeniowych, które wysyłane są zawsze na wszystkie interfejsy przełącznika. Kierując się poniższym rysunkiem (rysunek 8.2), wyobraź sobie, że ze stacji roboczej na router (który w tym przypadku jest domyślną bramą) zostało wysłane rozgłoszenie. Rozgłoszenie zostaje przechwycone przez przełącznik 1, który rozpoczyna transmisję na wszystkie swoje interfejsy. Przełączniki 2 i 3 również otrzymują ramkę. Przełącznik 2 po odebraniu ramki skieruje ją do przełącznika 3, a ten znowu skieruje ją do przełącznika 1. Proces będzie się powtarzał w nieskończoność, mimo iż już na samym początku komunikacji wszystkie przełączniki otrzymały wymagane kopie ramek.

Rysunek 8.2.

Burza rozgłoszeniowa



Kolejny problem powstaje wtedy, kiedy pracujące w sieci przełączniki otrzymują wiele tych samych kopii ramek. Takie zjawisko może być konsekwencją opisaną wcześniej burzy rozgłoszeniowej. Jeśli chodzi o otrzymywanie kopii tych samych ramek, problem nie tkwi w samym procesie otrzymywania, lecz w interpretacji nadchodzących kopii. Dzieje się tak, ponieważ niektóre działające w sieciach protokoły błędnie inter-

pretują nadchodzące kopie i traktują je jako błędy transmisji. Wędrujące kopie tych samych ramek wprowadzają również zamieszanie na interfejsach przełącznika, gdyż ta sama ramka na wielu interfejsach przełącznika może spowodować błędne wpisy w tablicy MAC lub konieczność szybkiego aktualizowania tablic. W takiej sytuacji wiele zasobów przełącznika zajmuje się obsługą tablic MAC, co znacznie spowalnia jego normalne działanie.

Działanie protokołu Spanning Tree

Protokół STP został stworzony po to, aby zapobiegać między innymi problemom opisanym wyżej. Generalnie protokół STP umożliwia taką konfigurację przełączników, aby w sieci nie powstawały pętle. Protokół STP tworzy wirtualne drzewo bez pętli, zawierające wszystkie przełączniki oraz wszystkie nadmiarowe ścieżki. Na szczycie drzewa znajduje się przełącznik główny, którego zadanie opiera się na zarządzaniu całą siecią oraz protokołem STP.

Protokół został ostatecznie poprawiony i sporządzony przez IEEE (początkowo utworzony został przez firmę DEC). Ostatecznie algorytm STP został zawarty w specyfikacji IEEE802.1d.

W swoim działaniu protokół STP wykorzystuje koszt ścieżki oparty na szybkości łącza. Tak więc dla szybkości 10Mb/s koszt wynosi 100, dla 100 Mb/s wynosi 19, dla 1 Gb/s wynosi 4 i dla 10 Gb/s wynosi 2. Im mniejszy koszt, tym lepsza ścieżka.

W pierwszej fazie działania i dokonywania zbieżności STP wybiera swój przełącznik główny. W przełączniku głównym wszystkie jego porty są portami desygnowanymi znajdującymi się w stanie przekazywania.

Przełącznikiem głównym zostaje ten przełącznik, który posiada tzw. najniższy identyfikator **BID** (ang. *bridge ID*). Identyfikator ten zawiera priorytet oraz adres MAC przełącznika. Identyfikator zostaje przypisany przez administratora. W specyfikacji IEEE 802.1d priorytet może zostać przypisany domyślnie i osiągnąć wartość 32 768. Jeśli dwa przełączniki posiadają te same wartości liczbowe w priorytecie, to przełącznikiem głównym zostaje ten, który posiada najniższą wartość w adresie MAC; np. jeśli przełącznik A posiada adres *0a00.2321.1321*, a przełącznik B posiada adres *0a00.1111.1111*, to przełącznik B zostanie przełącznikiem głównym (oczywiście tylko wtedy, kiedy oba będą posiadały te same priorytety).

W drugiej fazie STP wybiera port główny na przełączniku, który nie jest głównym przełącznikiem (wszystkie przełączniki oprócz głównego przełącznika są przełącznikami niegłównymi). Port główny zostaje wybrany na podstawie najniższego kosztu dla ścieżki prowadzącej od przełącznika głównego do portu głównego przełącznika niegłównego.

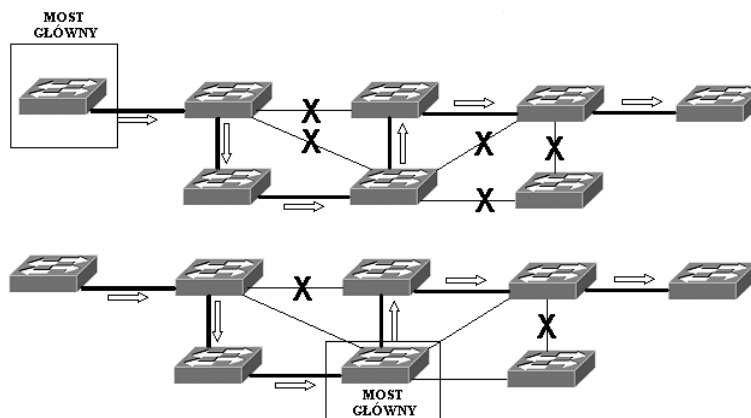
W ostatniej fazie zostają wybrane porty desygnowane. Wybór następuje tylko na tych przełącznikach, które są połączone z przełącznikiem głównym ścieżką o najniższym koszcie. Porty desygnowane również znajdują się w trybie przekazywania.

Pozostałe porty przełączników, które nie zostały wybrane, są uznawane za porty nie-desygnowane i przechodzą w stan blokowania, aby zapewnić w sieci brak pętli. Port w stanie blokowania nie przekazuje ruchu.

W ten sposób w sieci rozpoczyna się proces „porządkowania” mający na celu wyłączenie tych ścieżek, które aktualnie nie są potrzebne, a których działanie spowodowałoby pętle w sieci (rysunek 8.3). Na poniższym rysunku widać, że została tylko jedna ścieżka, która łączy przełączniki znajdujące się na brzegach.

Rysunek 8.3.

Działanie
protokołu STP



Należy jeszcze wspomnieć, że aby przełączniki mogły ustawiać pomiędzy sobą wszystkie opisane wcześniej parametry, muszą jakoś wymieniać ze sobą informacje. Robią to domyślnie co 2 sekundy za pomocą specjalnych ramek grupowych zwanych **BPDU** (ang. *bridge protocol data unit*).

Stany portów

Podczas ustalania właściwych ścieżek port przełącznika może przyjąć cztery stany, do których zaliczamy:

Blokowanie (ang. *locking*) — w tym stanie port przełącznika może odbierać ramki BPDU, natomiast nie wysyła żadnych BPDU, jak również nie wysyła żadnych danych użytkownika.

Nasłuchiwanie (ang. *listening*) — umożliwia wysyłanie i odbieranie ramek BPDU w celu próby ustalenia aktywnej topologii. W tym czasie zostaje wybrany przełącznik główny, porty desygnowane oraz porty główne.

Uczenie się (ang. *learning*) — w tym stanie port jest w stanie wysyłać i odbierać BPDU.

Przekazywanie (ang. *forwarding*) — port przełącznika w tym stanie przekazuje otrzymane ramki.

Zmiana stanu portów z nasłuchiwania na stan uczenia się oraz ze stanu uczenia się na stan przekazywania jest nazywana opóźnieniem przekazywania i wynosi domyślnie 15 sekund. Jeśli podsumować wszystkie czasy potrzebne do osiągnięcia stanu zbieżności, to przełącznik potrzebuje około 50 sekund.

Wszystkie obliczenia protokołu STP są ponawiane zawsze wtedy, kiedy w jakikolwiek sposób zmieni się topologia sieci.

Protokół RSTP

Mimo iż protokół STP dość znacznie chroni sieć przed powstawaniem pętli, posiada również kilka ograniczeń. Przede wszystkim jeśli wykorzystuje się protokół STP, to trzeba się liczyć z ograniczeniem rozpiętości sieci do 7 przełączników (warstwy drugiej). Drugim ograniczeniem jest bardzo wolna zbieżność osiągana nawet w 50 sekund, trzecim ograniczeniem jest brak zaimplementowanych mechanizmów bezpieczeństwa.

Te ograniczenia spowodowały, że organizacja IEEE opracowała ulepszony protokół RSTP (ang. *Rapid Spanning Tree Protocol*) eliminujący wady poprzednika. Protokół ten został zawarty w specyfikacji **802.1w**.

W RSTP każdy port może przyjąć trzy stany:

- ♦ odrzucania (ang. *discarding*) — w tym stanie port może nasłuchiwać, ale nie może odbierać ani wysyłać żadnych ramek;
- ♦ uczenia się (ang. *learning*) — w tym stanie port może uczyć się adresów MAC, lecz nie może wysyłać żadnych ramek;
- ♦ przekazywania (ang. *forwarding*) — ten tryb uprawnia zarówno do odbierania ramek, jak i ich przesyłania.

Podczas działania protokołu RSTP przydziela portom odpowiednie role, w których dany port może pracować. Port może być:

- ♦ główny (ang. *root port*) — port znajduje się w stanie przekazywania, może więc odbierać i wysyłać ramki;
- ♦ desygnowany (ang. *designet port*) — port w stanie przekazywania wysyłający najlepsze BPDU do segmentu sieci;
- ♦ alternatywny (ang. *alternate port*) — port tworzący alternatywną ścieżkę do przełącznika głównego;
- ♦ zapasowy (ang. *backup port*) — port tworzy ścieżkę zapasową (mniej pożądaną), znajduje się w stanie odrzucania;
- ♦ zablokowany (ang. *blocked port*) — port nie ma żadnego zastosowania i nie odgrywa żadnej roli w działaniu drzewa rozpinającego.

W protokole RSTP wprowadzono również wysyłanie BPDU co ustalony interwał czasu, zwany *hello time*. Ramki hello są wysyłane zawsze, nawet wtedy, kiedy nie otrzymują żadnych danych z sąsiednich przełączników. W przypadku nieotrzymania 3 ramek *hello* od innych przełączników połączenie uznawane jest za utracone.

W działaniu obydwu protokołów brakowało jeszcze jednej funkcjonalności. Była nią możliwość uruchamiania wielu instancji STP w sieciach VLAN. Dlatego organizacja IEEE wraz z firmą Cisco opracowała standard zwany IEEE 802.1s, czyli Multiple Spanning Tree Protocol (MST).

Rozszerzenie to umożliwia uruchamianie niezależnej topologii drzewa rozpinającego w każdej sieci VLAN.