Paweł **Zaręba**

Projekty i rozwiązania sieciowe w praktyce

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Grafika na okładce została wykorzystana za zgodą Shutterstock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

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

ISBN: 978-83-283-7401-0

Printed in Poland.

Spis treści

Wstęp

„Podążaj za pasją! Kto pracuje z pasji, jest bogatszy od tego, kto pracuje dla pieniędzy".

Kesuke Miyagi

Definicja informatyki, którą zapamiętałem ze studiów, mówiła, że informatyka to dziedzina nauki zajmująca się przetwarzaniem, przesyłaniem i przechowywaniem danych oraz środkami technicznymi służącymi tym celom. Po ponad 10 latach wymaga ona jednak aktualizacji. Informatyka to także nauka o tym, jak zabezpieczać czy chronić dane, ale i jak je udostępniać.

Konieczność aktualizacji tej definicji obrazuje, jak szybko rozwija się informatyka. Obecnie składają się na nią dziesiątki specjalizacji. Ja spośród nich wybrałem sieci komputerowe. Dlaczego — to proste. Sieci to moja pasja. Jedna z kilku, jakie mam w życiu.

Inżynier sieciowy to prestiżowe stanowisko w świecie IT. Jako specjaliści wiemy dokładnie, co się dzieje w sieciach komputerowych. Możemy sprawdzić, jakie dane są przesyłane, od kogo do kogo, kiedy i gdzie. Jest to pewien przywilej. Przywilej, którego nie mają inni specjaliści IT. Sieci komputerowe to fundament działania wszelkich usług IT. Jeśli nie działa sieć, to wszystko, co jest powyżej sieci (czyli aplikacje, internet, chmura, wszystkie systemy wewnętrzne, zabezpieczenia itp.) jest niedostępne. Zawsze zadziwia mnie to, że większość pracowników IT pozasieciowych specjalności uważa, że sieć musi działać, ponieważ raz została zrobiona i skonfigurowana. Jest to oczywistym błędem. Każdy sieciowiec wie to doskonale. Praca specjalisty ds. sieci nie jest łatwa. Wybierając tę drogę, musisz mieć świadomość, że często Twoja praca nie będzie przez innych przedstawicieli IT odpowiednio doceniana. Regułą jest brak uznania dla prawidłowo funkcjonującej sieci i obciążanie winą właśnie sieci w momencie, kiedy nie działa cokolwiek, co nawet bardzo luźno jest z nią związane. Dlatego decydując się na tę specjalizację, musisz kochać to, co robisz. Nie ma innego wyjścia. Na pocieszenie powiem, że to wszystko wynagradza.

W pracy zawodowej niemal od samego początku jestem związany z sieciami komputerowymi. To, co proponuję Ci w swoich książkach, oparte jest na moim własnym doświadczeniu. Poza wykonywaniem obowiązków inżyniera sieci działam także czynnie jako dydaktyk. Prowadzę laboratoria z przedmiotów sieciowych dla Akademii WSB w Dąbrowie Górniczej. To doświadczenie pozwoliło mi poznać potrzeby przyszłych inżynierów sieci oraz lepiej zrozumieć, na jakie obszary wiedzy należy położyć szczególny nacisk. Mimo że dodatkowa praca w weekendy w roli dydaktyka wymagała poświęcenia mojego prywatnego czasu, doświadczenie to jest dla mnie bezcenne. Pośród moich studentów byli tacy, którzy posiadali

bardzo dużą wiedzę sieciową, ale też tacy, którym brakowało podstawowych informacji. Za swój sukces uważam to, że nawet osoby, które początkowo nie interesowały się tematem sieci, po zajęciach zadawały pytania i prosiły o wyjaśnienia dotyczące bardziej zaawansowanych kwestii. Uświadomiło mi to, jak bardzo młodzi informatycy potrzebują praktyki i kontaktu z kimś doświadczonym w tym zawodzie. Nie sposób bowiem nauczyć się wszystkiego z suchej wiedzy zawartej w podręcznikach akademickich.

Zwykle jest tak, że pierwsza napisana książka to niewiadoma. Każdy autor przechodzi wtedy po raz pierwszy całą tę skomplikowana procedurę. Pisanie jest tylko niewielką jej częścią. Autor też się uczy i popełnia błędy. Błędy, które stara się skorygować, pisząc drugą książkę. Dlatego też z reguły ta druga książka jest dużo lepsza. Mam nadzieję, że będzie tak też w moim przypadku.

Jeśli sięgnąłeś po *Projekty i rozwiązania sieciowe w praktyce* po przeczytaniu mojej pierwszej książki, mam nadzieję, że książka ta spełni Twoje oczekiwania, a nawet pozytywnie Cię zaskoczy. Jeśli nie wiedziałeś nic o tym, że jako pierwsze na rynku pojawiły się *Praktyczne projekty sieciowe*, szczerze zachęcam do ich przeczytania. Zagadnienia zawarte w pierwszej książce są treściami bazowymi i bardzo ułatwiają przygodę z konfigurowaniem i analizą projektów sieciowych.

Po napisaniu pierwszej książki czekałem na opinie czytelników. Dla każdego autora pozytywny odbiór przez osoby, dla których się pisze, jest najważniejszy. Moja druga książka jest wynikiem rozmów z czytelnikami i powstała niejako w odpowiedzi na prośby o rozbudowanie pewnych zagadnień. Wśród osób czytających moją książkę byli studenci, wykładowcy, eksperci, specjaliści, a także pracownicy innych działów IT, nie tylko tych związanych z sieciami komputerowymi. Moje książki mają jeden cel — w sposób maksymalnie prosty przedstawiać skomplikowane zagadnienia sieciowe z jednoczesnym przemycaniem informacji, które dla każdego sieciowca powinny być wiedzą podstawową.

A oto telegraficzny skrót tego, co przygotowałem dla Ciebie tym razem.

Rozdział 1

W rozdziale pierwszym zaczniemy od podstaw. Wyjaśnię różnicę między podstawowymi urządzeniami sieciowymi takimi jak router i przełącznik. Będę tłumaczył, czym się różnią komponenty sieciowe takie jak GBIC, SFP. Wyjaśnię i rozwinę skrót 1U. Przyjrzymy się temu, w jaki sposób przełącznik przechowuje adresy MAC. Zinterpretujemy parametry sieciowe hosta. Przeanalizujemy architekturę ISO/OSI oraz architekturę modelu TCP/IP. Dodatkowo, co bardzo istotne, będziemy mówić o modelach projektowania sieci oraz warstwach projektu sieciowego. Zobaczysz, jak dostać się do urządzeń sieciowych za pomocą bezpośredniego połączenia oraz zdalnie. Opiszę, co oferują i jak działają obecnie urządzenia sieciowe. Jakie technologie posiadają i jaka jest różnica między nimi. Zajmiemy się też wyjaśnieniem terminologii fachowej. Pojawią się takie pojęcia jak uplink, MDI-X, RJ45, WIC-2T oraz inne. Ponadto dla tych bardziej zainteresowanych czytelników dodałem wyjaśnienie, czym jest PVLAN, czyli prywatny VLAN.

W rozdziale tym znajdziesz także informacje o modułach routera, o HSRP, czyli wirtualizacji bramy domyślnej. Jednym słowem, duży przegląd tematów sieciowych, bez poznania których nie będziemy w stanie rozpocząć swojej przygody z *Projektami i rozwiązaniami sieciowymi w praktyce*.

Rozdział 2

To zagadnienia związane z adresacją IP. W pracy zawodowej ten temat na pewno będzie Cię dotyczył, niezależnie od tego, czy będziesz pracował w sieciach, czy w szeroko pojętym IT. Po przeczytaniu tego rozdziału będziesz umiał wyliczyć adresacje IP, zaprojektować sieć dla oddziału firmy lub dla swoich usług. Zobaczysz praktyczny podział adresacji o globalnym zasięgu, jakie stosuje się obecnie w sieciach. Ponadto wyjaśnię Ci tematy związane z adresami IP, czyli broadcast, unicast, multicast czy anycast, żebyś miał pełne informacje o danym zagadnieniu. Wszystko jedno, czy będziesz pracował z serwerami, przełącznikami w chmurze, czy adresacją sieciową; czy będziesz zgłaszał do działu sieciowego chęć stworzenia nowej podsieci, czy sam będziesz to robił — powinieneś wiedzieć, o co w tym wszystkim chodzi i jak się to robi. W tym rozdziale pojawią się więc obliczenia oraz schematy sieci od tych małych, aż po bardzo rozbudowane. Mam nadzieję, że informacje zawarte w tej części książki sprawią, że wyjaśnienie, dlaczego adresacja 192.168.0.0/24 jest lepsza dla domu niż adresacja 10.0.0.0/8, nie będzie już dla Ciebie problemem.

Rozdział 3

To krótki rozdział opisujący, jakie niespodzianki mogą Cię spotkać w sieci LAN. Zobaczysz, jakim problemem jest burza rozgłoszeniowa i jak bronić się przed tym zjawiskiem. Opiszę STP oraz EtherChannel. Po przeczytaniu tego rozdziału zrozumiesz, czym jest pętla w sieci LAN. Dowiesz się, jak nie łączyć przełączników i jak optymalnie agregować porty.

Rozdział 4

To bardzo ważny, z mojego punktu widzenia, rozdział. Omówię tutaj, co sieciowiec powinien umieć, jakich narzędzi używać, jak diagnozować sieci. Będzie o TTL, Ping, ARP, Tracert, Nslookup i wielu innych. W pracy inżyniera sieciowego nieraz będziesz musiał rozwiązywać problemy w sieciach i szukać ich przyczyny. Od czego zacząć? Jak się za to zabrać? Tutaj opiszę, z jakich narzędzi podstawowych i zaawansowanych korzystamy obecnie w diagnostyce sieci oraz jakie narzędzia potrzebne nam są do tworzenia projektów sieciowych, automatyzacji, schematów i symulacji. To bardzo ważne zagadnienia pod kątem Twojej praktyki zawodowej.

Rozdział 5

Rozdział ten jest swoistą perełką. Odpowiem w nim na pytanie, na które nie każdy zna odpowiedź, czyli „Jak działa internet?". Pytanie, na które kiedyś i ja nie znałem odpowiedzi. Rozdział ten związany jest z routingiem BGP. Mam nadzieję, że po przeczytaniu go zrozumiesz, jak działa internet, i spojrzysz poza sieć LAN.

Poruszę oczywiście metody dostępu do internetu. Nie zabraknie terminów operatorskich związanych z zapewnieniem dostępu do internetu takich jak DSLAM, BRAS/BNG, OLT, ONT, RNC, BTS, 4G. Ciekawe, prawda? A to jeszcze nie koniec. Internet to nie tylko organizacja techniczna związana ze sprzętem i sieciami, to także podział administracyjny na adresację IP dla poszczególnych rejonów na świecie — o tym też będzie powiedziane. Oczywiście na praktycznych przykładach. Będzie o tranzycie i peeringu z punktu widzenia operatora ISP (dostawcy usług internetowych), a także o numerach AS. Obiecuję więc, że będzie ciekawie.

Rozdział 6

To kolejny rozdział pisany z myślą o bardziej zaawansowanych czytelnikach. Pokażę w nim, jak od strony operatora ISP jesteśmy w stanie za pomocą tylko jednego routera zapewnić osobne, niezależne instancje routingu dla poszczególnych klientów. W poprzedniej książce ograniczenia wynikające z Packet Tracer nie pozwoliły nam obserwować działania sieci MPLS oraz przeanalizować VRF czy skonfigurować MP-BGP. Tutaj to nadrobimy. Na podstawie prawdziwego projektu stworzonego z GNS3 zobaczysz, jak dostawca usług od początku do końca konfiguruje MPLS-a. Rozwiniemy skróty takie jak VRF, router CE, PE czy P. Będziemy analizować tablice routingu oraz tworzyć konfigurację krok po kroku, po to żeby ostatecznie zweryfikować status naszej konfiguracji.

Rozdział 7

Rozdział ten jest ukłonem w stronę tych osób, które chciały zobaczyć konfigurację sieci za pomocą urządzeń innych niż Cisco. W tym rozdziale stworzyłem projekt, który de facto będziesz mógł sam wykonać. Skonfigurujemy proste połączenie z internetem z wykorzystaniem routera MikroTik. Wykonamy prawdziwe testy połączenia włącznie z NAT, a wcześniej skonfigurujemy dostęp do naszego urządzenia, uruchomimy GUI, skonfigurujemy interfejsy i opiszemy najważniejsze obszary konfiguracji MikroTika. Po przeczytaniu tego rozdziału na pewno będziesz mógł samodzielnie zacząć przygodę z MikroTikiem.

Rozdział 8

W tym rozdziale postaram się wytłumaczyć usługę kluczową dla internetu, czyli DNS. Usługę często bagatelizowaną. Usługę, którą zwykle ustawiamy raz i na tym kończą się nasze problemy z konfiguracją i utrzymaniem tej usługi. Zrozumienie DNS jest bardzo istotne z punktu widzenia internetu. Jest to ogromny hierarchiczny system, bez którego nic w internecie nie działa! Mam nadzieję, że rozdział ten poprowadzi Cię w sposób zrozumiały przez to, co niezrozumiałe i często niedopowiedziane. Dodatkowo przeanalizujemy słownik terminów związanych z DNS oraz przejrzymy rekordy DNS. Mam nadzieję, że po przeczytaniu tego rozdziału zrozumiesz kluczową rolę DNS w sieciach.

Rozdział 9

To omówienie tego, czym jest i jak działa chmura. W rozdziale tym będziemy używać chmury Azure firmy Microsoft, aby stworzyć wirtualną sieć. Na pewno poszerzymy horyzonty o nowe, nieznane obszary sieci. Opiszę Ci krok po kroku, jak budować sieci VNET i łączyć je między sobą. Jak tworzyć wirtualne maszyny w chmurze oraz jak się do nich łączyć. Stworzymy własny serwer z działającą stroną i upublicznimy go w internecie. Przygotujemy kontener. Będziemy ustawiać dostęp za pomocą bastionu i zobaczymy, jak działa NAT. Wszystko po to, żebyś stał się kompletnym sieciowcem, dla którego chmura to tylko kolejna przestrzeń, gdzie możesz latać.

Rozdział 10

To bardzo przyjemny rozdział, w którym oprócz projektu PAT, czyli (NAT overloaded), nauczysz się korzystania z Cisco Modeling Labs. Opiszę w nim, jak skonfigurować środowisko oraz jak wykonać każdy element konfiguracji. Naniesiemy komponenty sieciowe na symulatorze, wykonamy połączenia fizyczne w GUI oraz konfigurację w CLI. Prześledzimy, jak działa PAT, gdy będziemy łączyć się z zasobem w chmurze Azure ze swojego komputera w sieci LAN.

Rozdział 11

Nie zawsze oddział firmy jest łączony za pomocą tunelu VPN. Często używamy rozwiązań dostawców usług WAN i przesyłamy tablice routingu między oddziałami właśnie przez sieć WAN. Treści zawarte w tym rozdziale są niezwykle interesujące, ale i zaawansowane. W projekcie skonfigurowałem oddziały firmy, które używają właśnie protokołu routingu OSPF. Następnie dodałem routery komunikujące się z ISP, na których działa BGP, a także BGP i OSPF. Kolejne etapy to część, w której pokażę, jak wygląda komunikacja i relacja między prywatnym AS a publicznym AS oraz jak działa redystrybucja. Istotą tego rozdziału będzie ukazanie, jak za pomocą BGP będziemy w stanie przenieść tablice routingu OSPF między oddziałami firm, aby każdy oddział widział wszystkie sieci LAN w całej globalnej firmie.

Rozdział 12

Miałem to szczęście, że zacząłem karierę sieciową od poznania dokładnie warstwy pierwszej sieci. Dzięki temu mogłem instalować gniazda sieciowe oraz patch panele, skręcać kable, robić testy okablowania, instalować serwery, szafy oraz wiele innych rzeczy. W tym rozdziale przyjrzymy się temu, jak sieci wyglądają od strony serwerowni. Obecnie coraz częściej praca z warstwą pierwszą sieci jest w dużych korporacjach outsourcowana. Sprawia to, że sieciowcy często nie mają wiedzy i doświadczenia w tym zakresie. Bywa to dużym problemem, dlatego warto wiedzieć, jak działa warstwa pierwsza, jak diagnozować problemy wynikające z usterek w tym zakresie oraz trafnie oceniać sytuację. W tym rozdziale podzielę się z Tobą doświadczeniem zdobytym w latach, kiedy często zajmowałem się warstwą pierwszą sieci.

Rozdział 13

W tej części opiszę, jak używać narzędzia Postman do komunikacji z REST API systemu Cisco DNA Center. Pokażę, jak uruchomić publiczną usługę demo ze strony Cisco. Pokażę również, gdzie znajduje się dokumentacja REST API oraz jak działa REST API. Wykonamy kilka requestów oraz opiszemy ich wyniki. Wyniki przeanalizujemy w formacie JSON. Zobaczymy komendy narzędzia CURL oraz wiele innych. Jestem pewien, że rozdział ten zainicjuje Twój rozwój sieciowy, jeśli jeszcze nie znałeś tych obszarów sieci.

Rozdział 14

Krótki, ale bardzo ważny rozdział książki. Zachęcający do poszerzenia sieciowych horyzontów. Pokażę Ci w nim, jak napisać kod programu w języku Python, który wykona request REST API do systemu DNAC. Kod będzie zawierał uwierzytelnianie za pomocą tokena. Zobaczysz edytor, którego używam, a także biblioteki Python niezbędne do wykonania requestów oraz serializacji czy deserializacji danych. Rozdział ten to nie tylko chęć popularyzacji Pythona w komunikacji REST API, ale także zachęcenie Cię do własnych eksperymentów. Dzięki językowi skryptowemu jesteś w stanie pobrać, zaktualizować czy stworzyć dane na zdalnym systemie według własnych upodobań i przetworzyć je w sposób, w jaki tylko chcesz.

Rozdział 15

To ostatni rozdział książki. Nasze spotkanie zakończymy bardzo ciekawym projektem sieci związanym z automatyzacją. Dowiesz się, jak stworzyć maszynę wirtualną i zmapować ją poprawnie do GNS-a. Przygotujemy środowisko, w którym zainstalujemy i skonfigurujemy Ansible oraz dodatkowe pakiety oprogramowania. Zrobimy projekt, w którym ze stacji deweloperskiej będziemy konfigurować ustawienia sieciowe na trzech routerach Cisco. Będziemy wykonywać różne zadania. W rozdziale tym przejdziemy kolejno przez pobieranie konfiguracji, dodawanie ustawień, konfigurację NTP i inne. Będziesz zaskoczony, jak automatyzacja może ułatwić nam pracę.

* * *

Pisanie książki nie jest łatwe. Szczególnie w dzisiejszych czasach. Codzienny pęd, kariera zawodowa, udział w projektach, przygotowanie do certyfikacji, a przede wszystkim czas dla rodziny i dla siebie, chwile na hobby i sport. Wszystko to nie ułatwia sprawy, a człowiek często żałuje, że doba nie jest z gumy i nie da się rozciągnąć. W tym natłoku codziennych spraw ciężko o systematyczność i niesłabnące zaangażowanie w pisanie.

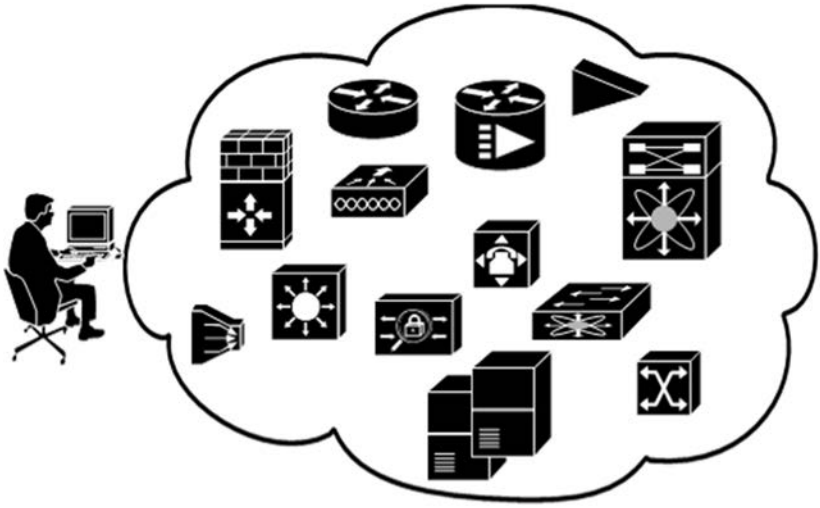
Książka, którą trzymasz w dłoniach, została przeze mnie przemyślana i stworzona krok po kroku. Zawarte w niej treści wybrałem na podstawie mojego wieloletniego doświadczenia w pracy z sieciami komputerowymi. Jest to jednak wybór subiektywny. Jeśli po przeczytaniu książki będziesz mieć jakieś pytania lub sugestie, zapraszam Cię do kontaktu pod adresem mailowym *pawel.zareba@op.pl*.

Informacja zwrotna od czytelników jest dla mnie zawsze inspirująca i niezmiernie ważna.

Cóż, nie pozostaje mi nic innego, jak podziękować Ci za to, że spośród ogromu pozycji wybrałeś właśnie moją książkę. Zakładam, że jeśli poszukujesz źródeł nastawionych na praktyczną stronę sieci, nie stoisz w miejscu i chcesz się ciągle rozwijać. Często mówi się, że kto się nie rozwija, ten się cofa. Jest to prawda. Prawda szczególnie odnosząca się do pracy w IT.

Zapraszam zatem do lektury i wspólnego odkrywania sieci komputerowych. Zaczynajmy!

ROZDZIAŁ 1. Sieciowa przystawka — smacznego!



W środowisku sieciowym zawsze znajdziemy routery i przełączniki. Inżynier czy administrator sieci musi znać różnicę między tymi urządzeniami oraz zasadę ich działania.

W rozdziale tym będzie sporo fundamentów. Zaczniemy od przełącznika i jego najważniejszych funkcji, zobaczymy jego miejsce w różnych topologiach sieciowych, a następnie w ten sam sposób przyjrzymy się routerom i ich zastosowaniu, a także możliwościom.

Przełącznik, jak sama nazwa wskazuje, jest to urządzenie przełączające. Co przełączają przełączniki? Odpowiedź brzmi — ramki ethernetowe. Ramka ethernetowa, potocznie mówiąc, krąży w warstwie drugiej modelu ISO/OSI, to znaczy w warstwie łącza danych. Dla przypomnienia przedstawiam na rysunku 1.1 ramkę ethernetową, złożoną z odpowiednich składowych, podzieloną na odpowiednie ilości bajtów.

RAMKA ETHERNET					
8	6	6	2	46 - 1500	4
PREAMBUŁA	ADRES MAC ODBIORCY	ADRES MAC NADAWCY	TYP	DANE	CRC

RYSUNEK 1.1. Budowa ramki Ethernet

Nie chciałbym się tutaj za bardzo skupiać na analizie ramki sieciowej — dużo o tym można znaleźć w internecie, czytając Wikipedię lub podręczniki o teorii sieci. Jednak nie zostawię Cię zupełnie, bez choćby krótkiego przypomnienia poszczególnych elementów. Wybiórczo opiszę kilka z nich, tak jak np. preambuła służąca do synchronizacji strumienia bitów. Jest to ciąg bitów informujący urządzenie, że po tym strumieniu nastąpi seria bitów adresu odbiorcy, nadawcy itd.

Wartości liczbowe przedstawiają ilość bajtów w danym polu (jeden bajt to 8 bitów — tak wiem, tę informację mogłem pominąć, bo przecież każdy to wie).

Adres odbiorcy to np. 6 bajtów, czyli 6×8 (bitów) = 48 bitów, i to właśnie nasz adres MAC. Na rysunku 1.2 pokazana jest wartość szesnastkowa adresu MAC, którą znajdziesz w konfiguracji swojej karty sieciowej.

```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : A8-7E-EA-6F-A5-05
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

RYSUNEK 1.2. Adres fizyczny widoczny z konsoli Windows

Zapamiętaj: adres MAC nazywany jest często adresem fizycznym, w odróżnieniu od adresu IP, zwanego logicznym — fizycznym, ponieważ jego adres jest unikatowy, można powiedzieć, trwale przypisany do urządzenia fizycznego. Nie ma dwóch takich urządzeń fizycznych, by miały ten sam adres MAC w sieci. Oczywiście nie rozmawiamy tutaj o sytuacji celowej próby podszycia się i modyfikacji adresu MAC przez hakera.

Adres A8-7E-EA-6F-A5-05 to inaczej w zapisie binarnym:

1010 1000 – 0111 1110 – 1110 1010 – 0110 1111 – 1010 0101 – 0000 0101

Karta sieciowa złożona z milionów tranzystorów rozlokowanych w przedziwnych układach scalonych przesyła ten ciąg zer i jedynek za pomocą impulsów elektrycznych, fal bezprzewodowych czy impulsów świetlnych przez sieć komputerową.

Przełącznik taki jak L2, czyli warstwy drugiej, przede wszystkim przetwarza te ramki i na podstawie adresu MAC nadawcy i odbiorcy przypisuje je do odpowiednich portów w tablicy MAC, budując tablicę przekazywania. W tej tablicy znajdują się adresy MAC skojarzone z portami. *CAM* (*Content Addressable Memory*)

tworzy właśnie takie tablice MAC. Poniżej przedstawiona jest zawartość CAM, czyli tablica MAC adresów przechowywana w tej pamięci:

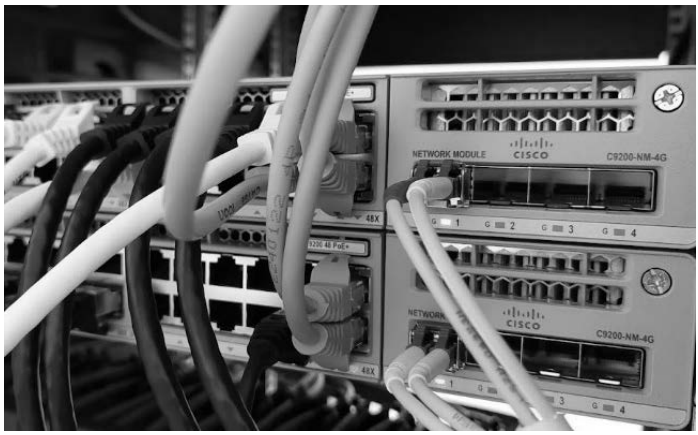
```
Switch#sh mac address-table
Mac Address Table
-------------------------------------------

Vlan Mac Address Type Ports
---- ----------- -------- -----
1 0001.c945.0c6b DYNAMIC Fa0/1
1 000d.bdc1.ed85 DYNAMIC Fa0/2
1 0030.f257.2a24 DYNAMIC Fa0/3
```

Gdy ramka jest wysyłana do przełącznika, urządzenie sprawdza, czy adres docelowy jest skojarzony z danym portem. Jeśli jest taki wpis, to ramka jest po prostu przekazywana na dany port. Jeśli nie, to przełącznik wysyła zapytanie do wszystkich portów z wyjątkiem tego, z którego otrzymał ramkę. Jeśli któryś z portów odpowie, wtedy tablica jest uzupełniana. Zadaniem przełączników jest szybkie przełączanie ramek, segmentacja, agregacja i łączenie dużej liczby urządzeń. Dzięki właśnie takiemu procesowi przełącznik warstwy drugiej to urządzenie bardzo szybkie, gdyż przełączanie — w porównaniu z routowaniem, gdzie wymagane jest dodatkowo przetwarzanie — jest zadaniem szybszym.

Przełączanie działa w różnych trybach, których nie będę opisywał szczegółowo w tej książce. Jest to temat na poziomie CCNP. Wspomnę tylko, jak mam to w zwyczaju, że jedne tryby przełączania sprawdzają np. CRC, zanim prześlą ramkę dalej, co wpływa na szybkość, inne z kolei przesyłają ramki tak szybko jak to możliwe, zanim otrzymają wszystkie informacje. Słowo kluczowe dla osób zainteresowanych to *CEF* lub *fast forwarding*.

Rysunek 1.3 pokazuje, jak wyglądają wieloportowe przełączniki warstwy drugiej firmy Cisco.



RYSUNEK 1.3. Przełączniki sieciowe Cisco Catalyst serii 9200 o rozmiarze 1U

Skupmy się najpierw na wyglądzie zewnętrznym przełącznika. Jeśli spojrzymy na niego od frontu, zwykle posiada on port mini-USB z napisem *console* oraz dużą ilość portów ethernetowych. W starszych przełącznikach zamiast portu mini-USB był port RJ45, a jeszcze wcześniej szeregowy port COM. Port ten służy do podłączenia się bezpośrednio do urządzenia. Zwykle standardowy przełącznik płaski, który montujemy do szafy rackowej, ma rozmiar 1U. Numeracja „U" wynika ze znormalizowanych wymiarów dla szaf rackowych w centrach danych czy serwerowniach. W branży teleinformatycznej przyjęło się, że wysokość sprzętu podaje się w tzw. „U". W praktyce 1U = 44,5 mm. Powyższe przełączniki posiadają dodatkowe porty SFP.

Czym jest SFP, a czym GBIC? Te skróty są często mylone. Spotkałem się z osobami, które nawet patrząc na port SFP, myliły go z GBIC, i odwrotnie. Tak więc jaka jest różnica między SFP oraz GBIC? Poniższa ilustracja powinna rozwiać wszelkie wątpliwości, jeśli chodzi o wygląd zewnętrzny, czyli kształt. Oba są transmiterami laserowymi stosowanymi dla połączeń światłowodowych. Jak widać na rysunku 1.4, SFP jest węższy w porównaniu z szeroką wkładką GBIC.

RYSUNEK 1.4.
Moduł GBIC oraz SFP

Źródło:
shutterstock.com

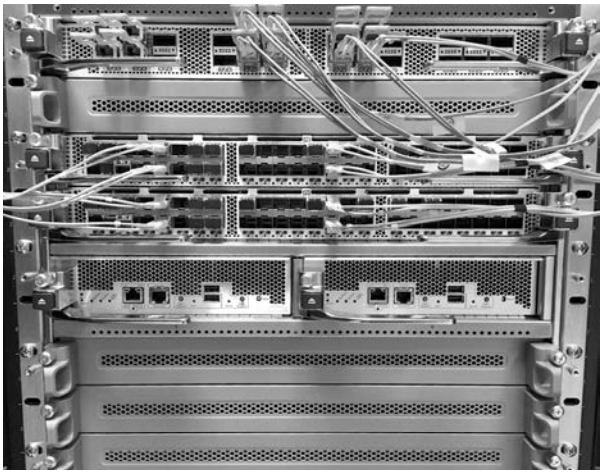
Moduły te wkłada się po prostu w wolny slot przełącznika, nawet przy uruchomionym przełączniku. Zwykle nie wymagają one żadnej specjalnej konfiguracji.

Można powiedzieć, że działają podobnie i obsługują podobne zakończenia światłowodów — LC czy SC. Istotną różnicą jest na pewno rozmiar modułów. GBIC zwykle zajmuje większą powierzchnię przełącznika niż mała wkładka SFP. To oczywiście nie oznacza, że używać powinno się tylko SFP, bo są mniejsze. To wszystko zależy od wielu czynników.

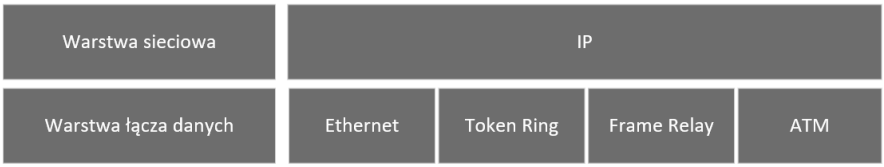
Na przykład w modułowych przełącznikach typu chassis, jak Cisco C6500, stosowane są karty liniowe z wejściem na wkładki GBIC. Przełączniki chassis są bardzo wygodną opcją, jeśli chodzi o konfigurację, i rozmiar nie ma już takiego znaczenia. Są one wybierane ze względu na skalowalność i zarządzanie. Zwykle są to urządzenia dedykowane do *DC* (*Data Center*) — centrów danych, bardzo rzadko używane są w przedsiębiorstwach, choć bywają i tam. Na pewno warto stosować je w miejscach, gdzie modułowość znacznie ułatwia funkcjonowanie i przerwy w działaniu przełącznika nie są akceptowalne. Jeśli potrzeba kolejnych 48 portów, nie ma problemu — zamawiamy moduł, wkładamy do przełącznika i po problemie. Nie zastanawiamy się nad zmianą topologii STP, nad agregacją czy innymi tematami związanymi z konfiguracją. Na rysunku 1.5 pokazuję, jak wygląda taki przełącznik modułowy dla centrum danych.

RYSUNEK 1.5.
Nowoczesny przełącznik dla centrum danych

Źródło: *shutterstock.com*



Jak zostało wyjaśnione we wstępie, przełączniki L2 działają na warstwie łącza danych, czyli drugiej warstwie modelu ISO/OSI. Na rysunku 1.6 przypominam warstwy drugą oraz trzecią modelu ISO/OSI oraz zaznaczam, na jakiej warstwie pracują przełączniki L2 (nie mylić z przełącznikami L3 warstwy trzeciej, gdzie występuje routing, czyli praca na warstwie sieciowej).



RYSUNEK 1.6. Warstwa sieciowa oraz łącza danych

Jak widać, warstwa łącza danych jest miejscem pracy przełączników L2. Przełączniki w przedsiębiorstwach (*enterprise*) w warstwie drugiej pracują w Ethernecie, czyli przesyłają ramki ethernetowe. Istnieją jednak także przełączniki, które przesyłają nie tylko ruch ethernetowy. Są też takie, które przesyłają ruch w komórkach ATM czy w ramkach Frame Relay. Jaka jest różnica między ATM a Ethernetem? Na jakie dystanse mogą przesyłać dane? To kolejny ciekawy temat wykraczający poza ramy tej książki. Zachęcam serdecznie do zapoznania się z tymi kwestiami, ponieważ mogą one się pojawić gdzieś w Waszych sieciach.

Wiedza o tym, jak działa ISDN, jest wg mojej opinii bardzo interesująca dla kogoś, kto pasjonuje się sieciami komputerowymi. Obecnie każdy używa telefonów komórkowych 4G, 5G czy rozmawia w technologii VoIP, ale wciąż jednak gdzieś są jeszcze neostrady, faksy czy linie ISDN. Oczywiście czas tych technologii się kończy, niemniej jednak warto pamiętać o tym, co było, gdyż w mojej ocenie masz wówczas pełną wizję sieci. To samo dotyczy początku internetu czy usług DNS, gdzie nazwy FQDI oraz IP były utrzymywane w plikach tekstowych i udostępniane przez FTP, zanim wprowadzono system root serwerów w DNS-ie. Historia sieci jest interesująca, choć oczywiście nie dla każdego. To była taka mała dygresja.

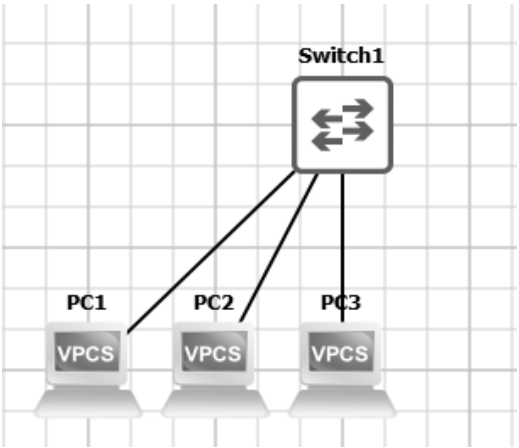
Jak już wspomniałem wcześniej, w książce będę czasem omawiał tematy poboczne, które pozwolą oderwać się na moment od aspektów technicznych.

Poniżej przedstawię pewne koncepcje oraz różne przykłady użycia przełączników zależnie od wymagań projektowych. Jak wiadomo, w różnych sytuacjach będziemy musieli zastosować różne rozwiązania. Czasem nie warto kupować przełącznika oferującego dużo funkcji, jeśli nie będziemy z nich korzystali.

Scenariusz pierwszy to, gdy używamy przełącznika, który zakupiliśmy. Od opuszczenia fabryki ma on skonfigurowany VLAN natywny, gdzie wszystkie porty do niego należą i niezależnie, gdzie podłączymy urządzenia końcowe (drukarki, komputery, inne), będą one miały ze sobą łączność. Piszę o tym, gdyż spotkałem się kiedyś w pracy z pytaniami kolegów chcących zrobić sieć w domu, czy jak kupią przełącznik np. Cisco czy inny, to czy muszą coś konfigurować na starcie. Odpowiedź brzmi — nie trzeba, ponieważ domyślnie wszystkie porty są w natywnym VLAN-ie. Oczywiście nie znam wszystkich produktów na całym świecie — wyjątki być może się zdarzają.

Prosty przykład, który wcześniej opisałem, widzimy na rysunku 1.7. Widać przełącznik L2 jako urządzenie w warstwie dostępu, do którego podłączone są trzy hosty (komputery PC1, PC2, PC3).

RYSUNEK 1.7.
Proste podłączenie trzech hostów do jednego przełącznika



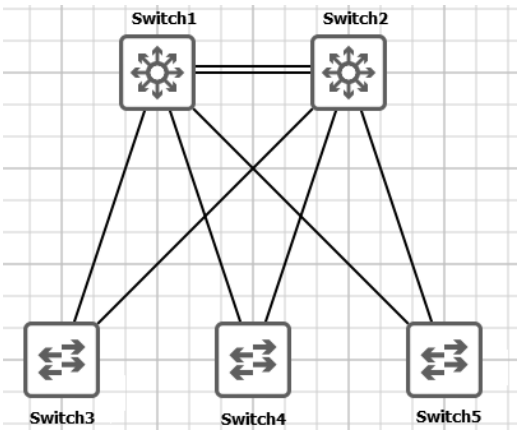
Jeśli zaadresujemy hosty ręcznie, odpowiednio: PC1 = 192.168.0.5/24, PC2 = 192.168.0.6/24 oraz trzeci host PC3 = 192.168.0.7/24, to znaczy wszystkie z maską /24, wówczas komputery wpięte do sieci poprzez kabel sieciowy, potocznie nazywany RJ45, będą mogły się komunikować wzajemnie w tym samym segmencie LAN, bez żadnej dodatkowej konfiguracji. Ideą tego przykładu było pokazanie warstwy dostępu w jak najprostszej postaci. Słowo-klucz to warstwa dostępu. Oznacza ona miejsce, gdzie podłączone są urządzenia końcowe (*endpointy*).

W drugim scenariuszu nasz projekt będzie się troszkę komplikował. Dodane zostały dwa przełączniki. Są to przełączniki 1 oraz 2, które są już, jak widzisz, powyżej przełączników 3, 4 i 5.

Przełączniki 3, 4, 5 — są przełącznikami w warstwie dostępu. Już wiesz, co to oznacza.

Przełączniki 1, 2 są w warstwie zwanej dystrybucyjną lub agregacyjną. Pełnią one ważną rolę. Mają za zadanie zapewnić przełącznikom dostępowym optymalny i niezawodny, czyli odporny na awarię, dostęp do innych segmentów sieci, np. warstwy rdzenia, WAN-u lub dostęp do internetu. Oto przykład (rysunek 1.8).

RYSUNEK 1.8. Warstwa dystrybucji oraz dostępu

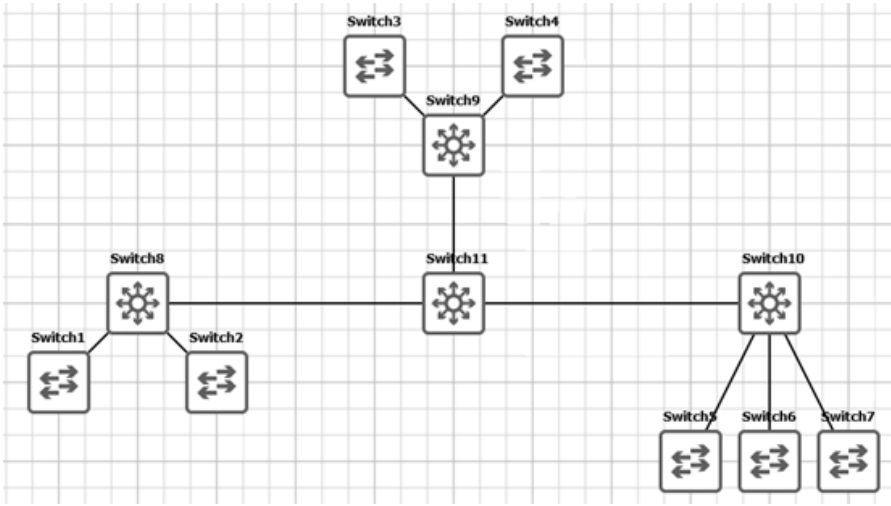


Zwykle uplinki, czyli połączenia między przełącznikami, łączymy tak, aby w razie awarii jednego łącza ruch sieciowy był nadal możliwy. Przykładem są przełączniki 1 i 2 na powyższym rysunku, pomiędzy którymi mamy dwa kable sieciowe zapewniające redundancję.

W razie awarii okablowania między każdym przełącznikiem mamy albo inną trasę, albo zapasowe łącze. Szczegóły tego podłączenia zostaną omówione w kolejnych rozdziałach. Warte zapamiętania jest, że tego typu topologia sieciowa jest projektowana zwykle w mniejszych oddziałach firm, gdzie nie wymaga się dodatkowej warstwy rdzenia. A warstwa dystrybucji służy jednocześnie jako warstwa dystrybucji i rdzenia.

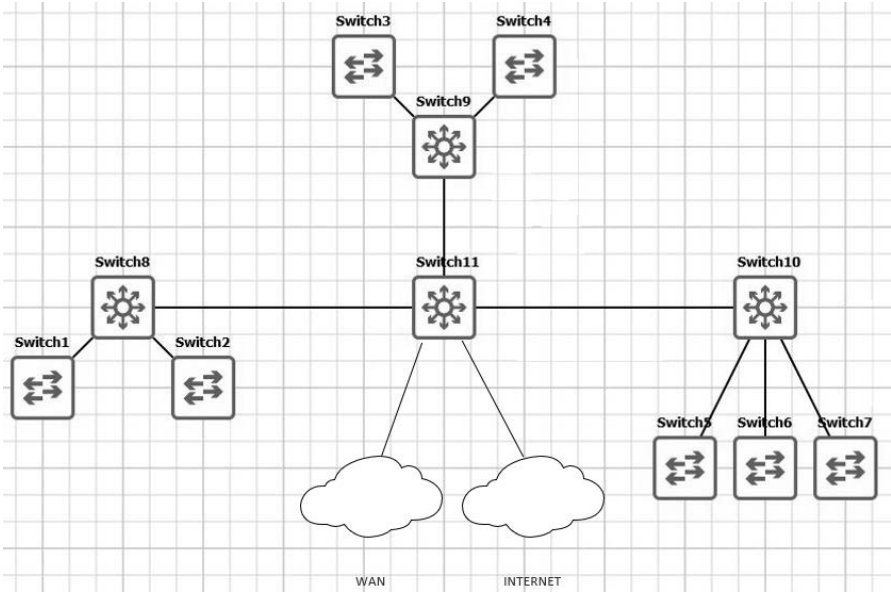
Ostatnim przykładem będą przełączniki w projekcie sieci kampusowej. I tutaj właśnie pokażę Ci, gdzie jest miejsce rdzenia (*core*) w projekcie LAN. W poniższym projekcie każdy oddział łączy się z centralnym punktem (tutaj przełącznik numer 11), który jest urządzeniem w warstwie rdzenia. Tego typu struktura sieci może być stosowana np. na kampusach uniwersyteckich, gdzie wszystkie wydziały mają swoje sieci, czy w centrali firmy z budynkami powiązanymi, magazynami, logistyką, produkcją.

Jak widać na poniższym schemacie (rysunek 1.9), każdy przełącznik numer 8, 9, 10 (warstwa dystrybucji) posiada uplink (łącze) do przełącznika numer 11 w rdzeniu. Przełącznik w rdzeniu przesyła ruch między oddziałami w kampusie, a także jest wyjściem do WAN-u lub internetu. To przełącznik 11 jest głównym punktem wymiany danych, który powinien działać jak najszybciej, i na tego typu urządzeniach w rdzeniu powinno się stosować jak najmniej złożoną konfigurację. W rdzeniu najważniejsza jest szybkość i optymalna konfiguracja.



RYSUNEK 1.9. Warstwa rdzenia, dystrybucji oraz dostępu

Schemat na rysunku 1.10 pokazuje natomiast, gdzie znajdują się zwykle połączenie z internetem lub WAN-em w tego typu topologiach. Jak widać poniżej, każdy oddział kampusu lub segment, który łączy się z rdzeniem, ma dostęp do takich usług jak WAN czy internet właśnie przez centralny punkt zwany rdzeniem sieci. Teraz już zapewne rozumiesz, czemu w przedsiębiorstwach zwykle stosuje się topologię zwaną *collapsed core*, czyli tak zwany zwinięty rdzeń.



RYSUNEK 1.10. Warstwa rdzenia z dostępem do internetu oraz WAN-u

Kontynuujmy temat przełączników: istotnym jest zrozumienie różnicy pomiędzy przełącznikiem L2 a L3. Przełączniki sieciowe mogą działać także w warstwie trzeciej, tak jak routery. Czyli mogą routować pakiety, budować tablice routingu oraz obsługiwać wszelkie funkcje na warstwie IP. Możesz na przykład uruchomić routing OSPF czy BGP, a on będzie wykonywał to samo, co router, czyli będzie utrzymywał tablicę routingu i podejmował decyzje o najlepszej trasie. To takie inteligentne przełączniki. Przykładem może tu być Cisco Catalyst 3750, przełącznik klasy enterprise (rysunek 1.11).

RYSUNEK 1.11. Przełączniki sieciowe Cisco Catalyst serii 3560, 3560-X oraz 3750-X

Zwykle aby dostać się do przełącznika, mamy dwie drogi. Robimy to zdalnie albo lokalnie. Na początku zanim podłączymy się zdalnie, musimy się podłączyć bezpośrednio. Używamy wówczas bezpośredniego połączenia za pomocą kabla konsolowego. Jak widać na rysunku 1.12, z jednej strony mamy końcówkę RJ45, która będzie podłączona do portu *console* (teraz już rzadziej stosowana, obecnie to mini-USB), a z drugiej strony do komputera. Jak wiadomo, obecnie laptopy nie dysponują portem szeregowym starego typu COM, tylko USB. Dlatego większość administratorów ma odpowiednie przejściówki.

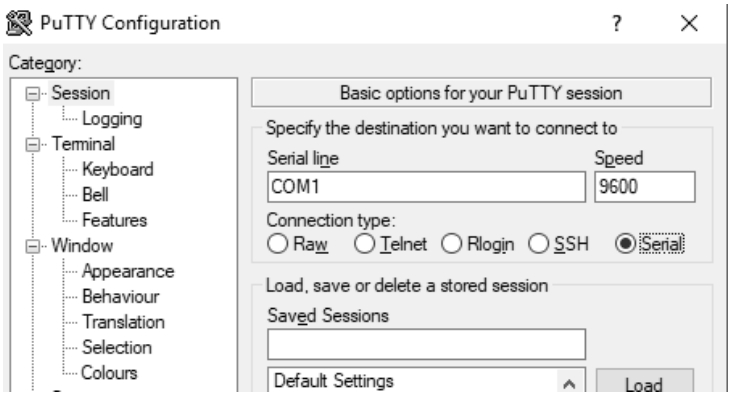
RYSUNEK 1.12. Kabel konsolowy do zarządzania urządzeniem sieciowym

Źródło *shutterstock.com*

Tak jak pisałem powyżej, nowsze urządzenia mają port mini- lub mikro-USB i USB, więc tutaj problemów nie ma z przejściówkami.

Jakie są następne kroki? Mamy kabelek, mamy sterowniki automatycznie wykrywające urządzenie na porcie USB. Teraz przychodzi czas na wyświetlenie okna konsoli przełącznika.

Obecnie najbardziej popularnym programem jest wciąż PuTTY (rysunek 1.13). Narzędzie to umożliwia połączenie się za pomocą portu COM, jak i zdalnie przez SSH. Poniżej widać okienko programu PuTTY. Nie znam administratora sieci, który by nie kojarzył tego programu.



RYSUNEK 1.13. Narzędzie PuTTY

Dla większości podłączeń bezpośrednich konfiguracja jest zwykle standardowa. Polega na ustawieniu szybkości przesyłania bitów na sekundę oraz wybraniu numeru portu COM. Jeśli teraz skonfigurujemy sobie adres IP interfejsu zarządzającego, to będziemy mogli łączyć się z naszym urządzeniem zdalnie.

Większość z nas wie, że Telnet działający na porcie 23 jest metodą dostępu, lecz przesyła on dane w postaci niezaszyfrowanej przez sieć, co zwykle nie jest akceptowalne w biznesie. Dlatego preferowany dostęp do urządzeń to dostęp z użyciem protokołu SSH na porcie 22. Aby połączyć się zdalnie, oprócz adresu IP musimy skonfigurować SSH, gdzie będziemy ustawiać algorytmy szyfrowania, klucze itp. Ostatnią rzeczą jest dodanie konta użytkownika i hasła.

Mając adres IP, otwarty i skonfigurowany port 22 oraz założonego użytkownika, możemy bez problemu podłączyć się do takiego urządzenia.

Jak wiesz, często zdarza mi się, że zaczynając opisywać dane zagadnienie, przypominam sobie, że dobrze byłoby wspomnieć o czymś, co jest z tym powiązane, ponieważ jest wiele technologii i tematów, którymi warto uzupełnić materiał opisujący dane zagadnienie. Tak więc skoro jesteśmy przy przełącznikach, warto wspomnieć o MDI-X. Jest to funkcja przełącznika umożliwiająca wykrycie, czy kabel RJ45 jest krosowy, czy prosty. Można powiedzieć, że zwalnia nas od myślenia, czy podłączyliśmy przełącznik do przełącznika lub komputer do przełącznika dobrym kablem.

W trakcie prowadzenia zajęć praktycznych na uczelni studenci mówili mi, że po co się martwić, czy kabel jest krosowy, czy prosty, skoro jest MDI-X na przełączniku i działa. Jest w tym racja. Natomiast ja myślę, że bez względu na to, czy ta funkcja jest, czy jej nie ma, czy jest włączona, czy wyłączona, powinniśmy wiedzieć, że jest coś takiego.

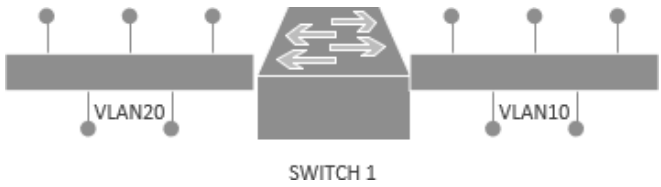
Przypomnę, że kabel sieciowy ze złączem 8P8C zwany jest również RJ45. Ogólnie kabel ten stosujemy do łączenia różnych urządzeń w sieci. Kabla krosowego używamy tyko, gdy łączymy router – router lub komputer – komputer, komputer – router, natomiast kabla prostego do łączenia różnych urządzeń, czyli router – switch, komputer – switch. Tak więc MDI-X mimo błędnie dobranego kabla jest w stanie uzyskać połączenie między węzłami.

O MDI-X czy o kierunkach transmisji i odbioru sygnału na poszczególnych przewodach można napisać naprawdę dużo i jest sporo książek czy schematów sieci. Niemniej nie byłbym sobą, gdybym nie opisał prosto pewnych prawidłowości.

W skrócie powiem, że gniazda RJ45 na swoich pinach przesyłają i odbierają sygnały RX, TX (odbiór, transmisja), a także czasem niskie napięcie elektryczne (np. dla zasilania punktów dostępowych lub telefonów VoIP). Jeśli użyjemy kabla prostego między komputerem a przełącznikiem, to na przewodach, na których następuje transmisja danych (TX) z komputera, drugie urządzenie odbiera dane (RX). Tak są skonfigurowane piny na gnieździe sieciowym. W przypadku np. TX (transmisji z komputera do komputera) gdy użyjemy tego samego kabla prostego, to sygnał TX (transmisja na przewodach w kablu) trafia do komputera na piny, gdzie także jest ustawiona transmisja danych na porcie karty sieciowej — a powinien być odbiór RX. W tym przypadku komputery nie skomunikują się ze sobą. Dlatego krosujemy kable, czyli zamieniamy pary przewodów TX z RX w kablu, wówczas urządzenia mające takie same ustawienia pinów w gnieździe fizycznym będą w stanie poprawnie się skomunikować.

Teraz przejdziemy do krótkiego omówienia wirtualnej sieci LAN zwanej VLAN oraz prywatnej wersji VLAN, czyli PVLAN. Na rysunku 1.14 widzimy prosty przykład dwóch segmentów w sieci LAN na przełączniku numer 1 — są to VLAN 20 oraz VLAN 10.

RYSUNEK 1.14.
Dwa segmenty sieci LAN



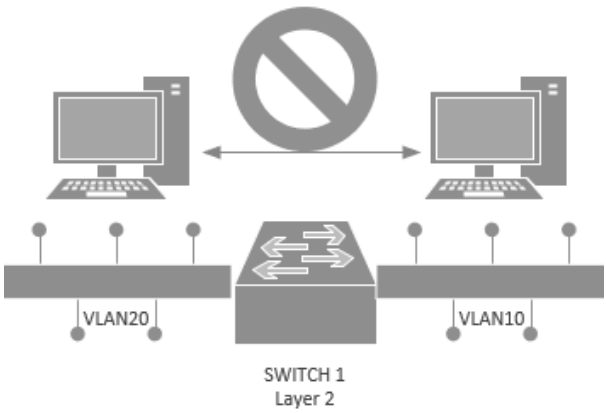
Najbardziej powszechną i podstawową operacją przy konfiguracji przełącznika jest utworzenie VLAN-u, czyli wirtualnej podsieci w ramach tego samego urządzenia. Do czego służy VLAN?

VLAN tworzymy, gdy chcemy:

- ograniczyć domenę rozgłoszeniową — broadcast (o tym opowiem w kolejnych rozdziałach);
- izolować/grupować hosty w podsieci;
- usprawnić administrację i zarządzanie sieciami (segmentacja sieci i logiczne podziały);
- zwiększyć bezpieczeństwo (ACL nałożone na VLAN = VACL).

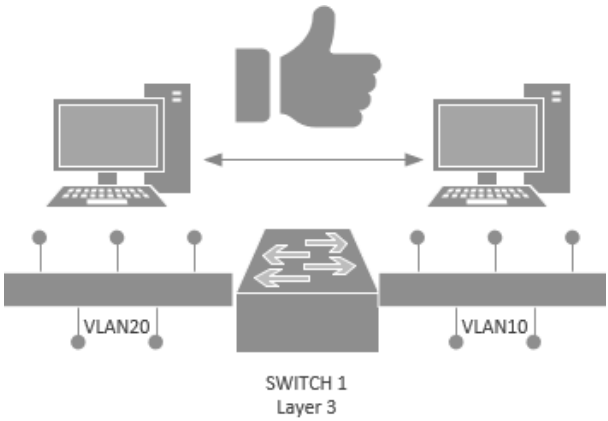
Pamiętajmy, że domyślnie hosty między VLAN-ami nie mogą się ze sobą skontaktować, ponieważ nie istnieje routing między VLAN-ami, dopóki go nie uruchomimy. Obrazuje to rysunek 1.15.

RYSUNEK 1.15.
Brak routingu między komputerami PC



Gdy chcemy zapewnić komunikację między VLAN-ami, wówczas musimy uruchomić routing. A do tego celu musimy użyć przełącznika warstwy trzeciej L3 (rysunek 1.16).

RYSUNEK 1.16.
Routing między komputerami PC



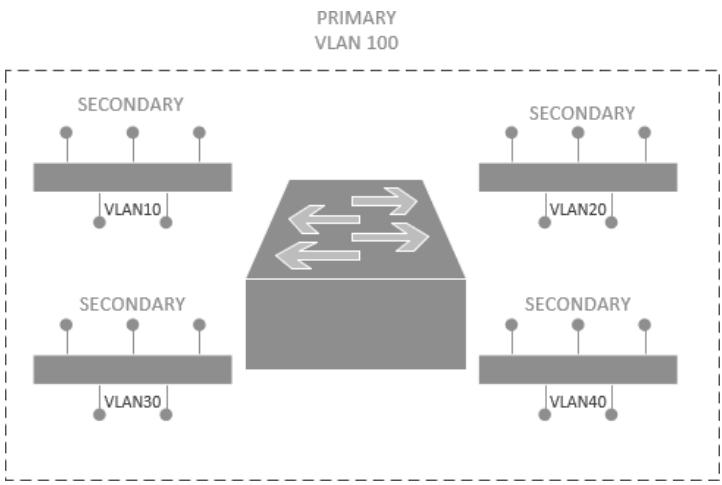
Jeśli jesteśmy już przy przełącznikach i VLAN-ach, warto wspomnieć o PVLAN-ie (*Private VLAN*). Jest to zagadnienie omawiane na poziomie CCNP.

PVLAN stosuje się szczególnie często u ISP do odseparowania klientów w danym VLAN-ie lub w Data Center do ograniczenia komunikacji serwerów różnych podmiotów należących do wspólnego VLAN-u. Robi się to głównie w celu zwiększenia pewnego poziomu bezpieczeństwa poprzez odizolowanie hostów będących w tym samym VLAN-ie lub po prostu uzyskania bezpiecznej, bardziej wymagającej segmentacji sieci czy oszczędzenia numerów VLAN. Można powiedzieć, że używając PVLAN-u, tworzymy VLAN we VLAN-ie.

Rozwiązanie PVLAN stosujemy na przykład, gdy chcemy, aby klienci podłączeni do tego samego VLAN-u komunikowali się tylko między sobą albo grupa hostów komunikowała się tylko z określoną grupą hostów. PVLAN pozwala nam w pewnym sensie tak dostroić ten ruch, aby był zgodny z naszymi wymaganiami. Gdybyśmy dla przykładu mieli farmę serwerów, w której każdy należałby do innej firmy, i chcielibyśmy, aby każdy komunikował się z bramą domyślną, ale nie komunikował się z pozostałymi serwerami — innymi słowy, nie widział ich ruchu sieciowego — w tym przypadku pomoże nam właśnie konfiguracja PVLAN-u bez zbędnych ACL czy innych funkcji blokujących ruch sieciowy.

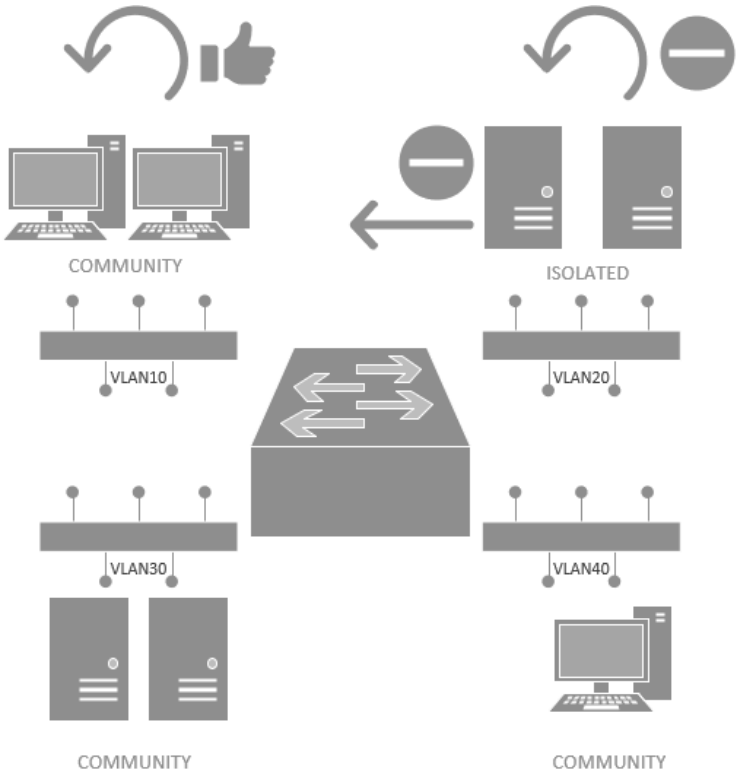
Przyjrzyjmy się temu bliżej na konkretnym przykładzie. Od strony technicznej wygląda to tak, że tworzymy główny VLAN nazywany *PRIMARY*, a następne „pod-VLAN-y" wewnątrz głównego *PRIMARY*. Te „pod-VLAN-y" określane są jako *SECONDARY*. Dla jasności podział ten przedstawiony jest na rysunku 1.17.

RYSUNEK 1.17. VLAN — PRIMARY oraz SECONDARY



Kolejną rzeczą, którą wykonujemy, jest podział VLAN-ów *SECONDARY* na sieci typu albo *ISOLATED*, albo *COMMUNITY*. W zależności od naszych potrzeb wybieramy odpowiedni typ. Zacznijmy od różnic między *ISOLATED* a *COMMUNITY* VLAN.

Typ *ISOLATED* to sieć, w której porty są izolowane. Występuje tu brak komunikacji z innymi hostami w ramach VLAN-u *SECONDARY*. Natomiast jeśli chodzi o *COMMUNITY*, to komunikacja między hostami we VLAN-ie jest możliwa w ramach tego samego VLAN-u, natomiast niemożliwa w ramach innej drugorzędnej (*SECONDARY*) sieci VLAN. Najlepiej zobrazuje to schemat na rysunku 1.18.

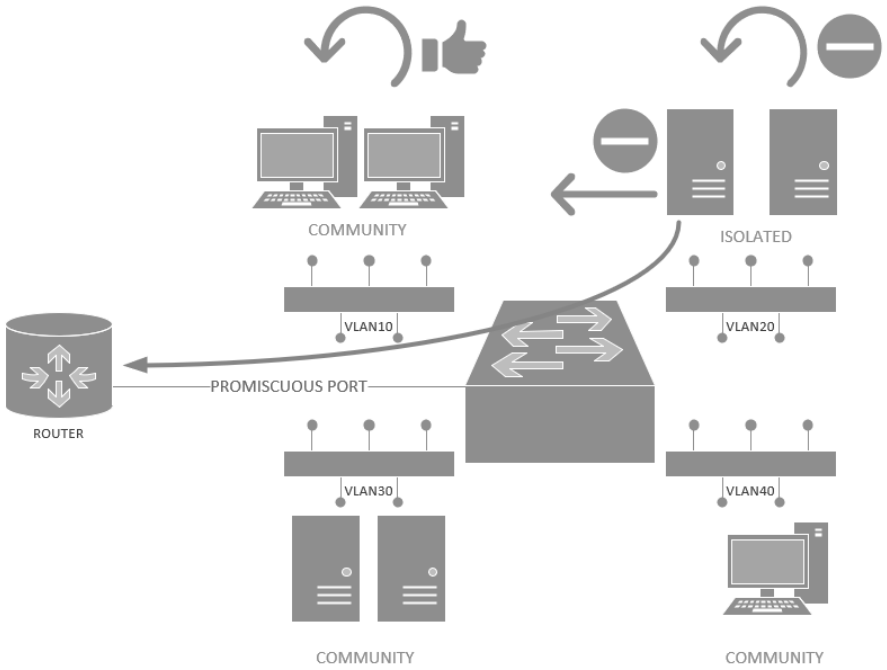


RYSUNEK 1.18. Komunikacja w obrębie VLAN-ów i między nimi w obrębie PVLAN-u

Oczywiście przy okazji konfiguracji PVLAN-u trzeba wspomnieć o specjalnym porcie *promiscuous port*. Port ten służy do niezależnej komunikacji między VLAN-ami. Innymi słowy musimy skonfigurować ten port na interfejsie, który będzie przenosił ruch między VLAN-ami. Zwykle jest to port podłączony do bramy domyślnej. Jak wiadomo, sieci *ISOLATED* i *COMMUNITY* mają wspólną cechę. Mogą komunikować się z siecią *PRIMARY* (główną) i właśnie w tej sieci ustawia się port typu mieszanego, który umożliwia komunikację np. z routerem. Najlepiej widać to na przykładzie z rysunku 1.19.

Myślę, że jak na wprowadzenie w temat przełączników będzie to dla Ciebie wystarczająca dawka wiedzy. Jeśli chodzi o praktyczną konfigurację sieci VLAN, zachęcam do przeczytania mojej poprzedniej książki, w której to w programie Packet Tracer od początku do końca sami tworzymy i testujemy połączenia sieciowe bezpośrednio na emulatorze, przygotowujemy różne VLAN-y, inter-VLAN routing i inne typy połączeń.

To nie koniec funkcji, jakie oferują nam nowoczesne przełączniki. Czy słyszałeś o STP, VSS, oraz Port Channel? To wszystko będzie opisane w kolejnych rozdziałach. A teraz może krótka przerwa na herbatkę lub kawkę, zanim przejdziemy do opisu routerów?



RYSUNEK 1.19. Komunikacja z sieci VLAN do routera dla PVLAN-u

Router to inteligentne urządzenie, które obsługuje wiele typów połączeń fizycznych. Głównym zadaniem routera jest poprawne kierowanie czy sterowanie ruchem sieciowym. W przeciwieństwie do przełącznika warstwy drugiej router analizuje tablice routingu w celu dobrania najlepszej ścieżki do sieci docelowej. Routery posiadają dużo większe możliwości obliczeniowe niż przełączniki. Router pracuje w warstwie trzeciej modelu ISO/OSI, czyli przetwarza pakiety IP. Wykonuje także dodatkowe funkcje jak np. QoS, PBR, ACL, inspekcje pakietów oraz wiele, wiele innych, nawet bardzo zaawansowanych.

W instalacjach domowych stosujemy routery proste zakupione w markecie lub te, które dostajemy od ISP. Są one zwykle zintegrowane z wi-fi. Mowa o routerach takich producentów jak np. Netgear, D-Link, Asus czy inne. Są też routery takie pośrodku, które oferują dużo funkcji, a nadal są budżetową opcją, czyli np. MikroTik (czasem używany w poważnych instalacjach ISP czy automatyce domowej). Następnie mamy urządzenia zaawansowane oferujące profesjonalne funkcje, dodatkową redundancję zasilania i wysoką wydajność — są to urządzenia klasy enterprise do wymagających zastosowań komercyjnych, gdzie oferowane jest także wsparcie techniczne.

Router MikroTik routerboard RB2011UAS-2HND-IN (rysunek 1.20) często stosowany jest przez mniejszych ISP lub w mniejszych sieciach. Oferuje on wiele funkcji oraz posiada stabilny system operacyjny.

RYSUNEK 1.20.
Router MikroTik dla domu i biura z wi-fi

Źródło:
shutterstock.com

Na rysunku 1.21 widać typowy router klasy enterprise — Cisco serii 3900 Integrated Service Router, stosowany bardzo często przez ISP oraz duże przedsiębiorstwa (korporacje).

RYSUNEK 1.21.
Router Cisco ISR 3900

Jak widać, router posiada wolne sloty na moduły WIC. Moduły WIC Cisco WAN Interface Card mają możliwość podłączenia routera do łącza WAN za pomocą odpowiedniego interfejsu. Może to być np. WIC 2T posiadający dwa porty szeregowe (synchroniczne i asynchroniczne).

Kart tego typu jest bardzo wiele, zależnie od technologii WAN. Dla przykładu możemy podłączyć do routera kartę WIC, która obsługuje ISDN BRI jako łącze backupowe w naszym urządzeniu. Wówczas mamy dwa łącza: jedno podstawowe, drugie zapasowe.

Routery, które pracują w ISP, są bardziej obciążone niż te w oddziale przedsiębiorstwa, gdyż te w ISP obsługują zazwyczaj setki tablic routingu, VRF, mają więcej aktywnych protokołów routingu niż tylko BGP oraz przetwarzają ogromną ilość ruchu.

Zrobię w tym momencie małą dygresję. Książkę, którą właśnie czytasz, starałem się pisać w sposób bardzo uniwersalny, zrozumiały dla różnych specjalistów sieci, jak i ludzi niezwiązanych z sieciami. Tematy, które mogą nie być interesujące dla Ciebie, dla innych mogą być bardzo ciekawe. Sztuka polega na tym, aby każdy wyciągnął z tej książki to, co go interesuje; uzupełnił swój obraz sieci o te brakujące puzzle, które gdzieś pominął w trakcie analizy czy rozważań dotyczących sieci.

Książka, którą trzymasz w rękach, na pewno nie będzie odbierana tak samo przez każdego. Doświadczenie, które zdobyłem podczas rozmów po napisaniu poprzedniej książki, pokazało mi, że inaczej odbierze ją ktoś na poziomie CCIE, inaczej specjalista od bezpieczeństwa sieci, inaczej ją zrozumie specjalista od centrów danych, a jeszcze inaczej specjalista czy inżynier zajmujący się monitoringiem sieci lub administrator poczty. Obecnie administratorzy sieci to także specjaliści od serwerów i wirtualizacji, a technologie tworzenia wirtualnych sieci jak VMware NSX-T już od lat oferują rozwiązania wirtualizacji. Dla nich też jest ta książka. Ma ona uzupełniać brakujące puzzle Waszej wiedzy na podstawie praktycznych projektów, które dla Was przygotowałem.

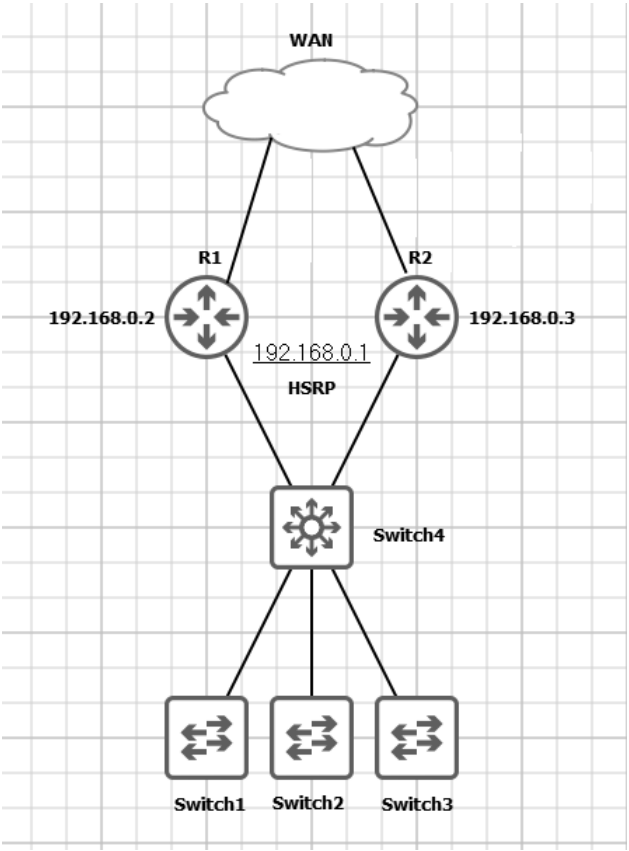
Książka będzie pełna dygresji i często właśnie tematów pobocznych, będę wyjaśniał terminy związane z daną technologią i podkreślał, co jest najbardziej istotne i warte zapamiętania. Mam nadzieje, że to właśnie podejście uczyni moją książkę bardziej wartościową dla Ciebie.

Router stanowi w przedsiębiorstwie bramę domyślą do internetu czy WAN-u. Aby osiągnąć pewien zadowalający stopień bezpieczeństwa w razie awarii, stosujemy w sieciach FHRP, czyli protokół redundancji pierwszego skoku. Na rysunku 1.22 umieściłem taki przykład, w którym mamy dwa routery dostarczone przez ISP. Oba skonfigurowane są jako HSRP (jest to typ FHRP).

Przełącznik numer 4 działający w warstwie dystrybucji/rdzenia jest skonfigurowany tak, aby używał wirtualnego adresu 192.168.0.1 jako adresu naszej bramy domyślnej. Routery R1 oraz R2 posiadają własne adresy IP i są odpowiednio skonfigurowane, aby jeden z routerów był głównym i aby przez niego przechodził ruch sieciowy, natomiast drugi był routerem w trybie *standby* i zadziałał w razie awarii. W konfiguracji sieciowej przełącznika 4, a dokładnie w tablicy routingu, wygląda to tak, iż wszystkie adresy IP oznaczone w konfiguracji jako 0.0.0.0 0.0.0.0 są przekierowane na bramę domyślną o adresie 192.168.0.1. Szczegółową konfigurację HSRP z projektem wykonałem w mojej poprzedniej książce.

Jeśli host podłączony do sieci LAN chce uzyskać dostęp do innej sieci poza swoją, to wówczas pakiet IP jest otwierany w celu sprawdzenia docelowego IP oraz analizowany w tablicy routingu na przełączniku L3. Jeśli nie będzie w tablicy routingu adresu pasującego do adresu wskazanego w pakiecie IP przez hosta, to wówczas ruch sieciowy jest skierowany do adresu ostatniej szansy, czyli adresu 0.0.0.0. Jak już pisałem, adres ten jest przekierowany na wirtualny adres 192.168.0.1 obsługiwany przez jeden z aktywnych routerów: albo R1, albo R2. I dalej routowany jest do WAN-u.

RYSUNEK 1.22.
Lokalizacja HSRP
w topologii sieciowej



Jak widać, nasz ISP zapewnił to, że brama domyślna 192.168.0.1 będzie dostępna, nawet gdy jeden z routerów będzie wyłączony lub uszkodzony. Taką ochronę bramy domyślnej daje nam jeden z protokołów, jakim jest HSRP (mamy jeszcze VRRP czy GLBP). W poprzedniej książce za pomocą dostępnego za darmo symulatora Packet Tracer skonfigurowałem routery w trybie HSRP oraz zasymulowałem awarię sieci.

Konfiguracja HSRP to także ułatwienie dla ISP w momencie okna serwisowego. W sytuacji, gdy trzeba uruchomić ponownie router, drugi bardzo szybko przejmuje jego rolę. Jeden router działa w trybie *active*, drugi *standby*. Jak widać, nie ma tutaj wyrównywania obciążenia, a jest tylko zapewnienie redundancji bramy domyślnej. W takim momencie specjalista CCNP przełączania i routowania mógłby powiedzieć: „Miałem to na egzaminie, znam ten temat". Natomiast specjalista IT On Site lub inny pokrewny właśnie zrozumiał, dlaczego dostawca usług zainstalował w szafie rackowej dwa urządzenia zamiast jednego. Zadbałem także o kolegów bardziej zaawansowanych. W niniejszej książce nie zabraknie również zaawansowanych tematów sieciowych związanych z BGP, VRF czy MPLS, w których będziemy analizować większe sieci. Omówię tu tematy związane z DNS, chmurą, automatyzacją i programowaniem oraz wiele innych.

Zatytułowałem ten rozdział „Sieciowa przystawka — smacznego!". Myślę, że to odpowiedni tytuł. Porównaliśmy konkretnie przełączniki z routerami oraz poruszyliśmy wiele pobocznych kwestii związanych z tymi urządzeniami. Uważam, że na początek to była wystarczająca dawka wiedzy, ale i punkt startowy, od którego możemy zacząć iść dalej. Było to lekkie przypomnienie, a zarazem utrwalenie istotnych informacji, przeplatane tematami mogącymi Cię zainspirować oraz różnymi technicznymi terminami czy definicjami.

Gratulacje, że przeczytałeś ten rozdział. Czytaj dalej. Zapraszam do lektury.

Praktycznie rzecz ujmując... o sieciach

Paweł Zaręba, autor *Praktycznych projektów sieciowych*, od wielu lat związany z branżą IT i ICT, za namową swoich wiernych czytelników napisał drugą książkę. Tę wcześniejszą można traktować jako kompendium wiedzy na temat sieci komputerowych — *Projekty i rozwiązania sieciowe w praktyce* są niejako kontynuacją tamtej publikacji.

Podczas lektury tej książki, wymagającej znajomości zagadnień sieciowych, utrwalisz podstawowe pojęcia z zakresu sieci (takie jak router, przełącznik), odkryjesz niespodzianki w sieci LAN i zasady funkcjonowania internetu, zrozumiesz, czym jest i do czego służy DNS, zapoznasz się z chmurą i jej działaniem, spojrzysz na sieci od kuchni, czyli od serwerowni. Dzięki przemyślanym przykładom dowiesz się między innymi, jak używać narzędzia Postman, samodzielnie wykonasz projekt sieci związany z automatyzacją i przeprowadzisz własne eksperymenty w języku skryptowym Python.

Ten przewodnik, skierowany do poszukujących praktycznych aspektów sieci i do zaawansowanych sieciowców, ma jeden cel: jak najprzystępniej przedstawić skomplikowane zagadnienia sieciowe, a jednocześnie ugruntować podstawowe informacje.

- **Komponenty sieciowe i architektura modelu TCP/IP**
- **Projektowanie adresacji IP**
- **Narzędzia do diagnostyki sieci**
- **Metody dostępu do internetu**
- **Niezależne wirtualne instancje routingu VRF**
- **Konfiguracja sieci za pomocą routera Mikrotik**
- **Tajniki Cisco Modeling Lab**
- **Przenoszenie tablic routingu OSPF za pomocą BGP**
- **Utworzenie sieci wirtualnej w GNS3**
- **Mapowanie maszyn wirtualnych**
- **NAT i CGNAT**
- **Działanie sieci od strony ISP (MPLS L3VPN i MPBGP)**
- **Korzystanie z REST API**
- **Wirtualizacja sieci w chmurze Azure**
- **Cisco DNA Center**

Spójrz na sieci od strony praktycznej!

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej! ▶

ISBN 978-83-283-7401-0

9 788328 374010

Cena: 69,00 zł