

SIECI CISCO W MIESIĄC

PODRĘCZNIK ADMINISTRATORA



BEN PIPER

Tytuł oryginału: Learn Cisco Network Administration

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-3971-2

Original edition copyright © 2017 by Manning Publications Co.
All rights reserved.

Polish edition copyright © 2018 by HELION SA
All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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/sicimi>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

<i>Przedmowa</i>	11
<i>Podziękowania</i>	13
<i>O tej książce</i>	15
<i>O autorze</i>	17
Rozdział 1. Zanim zaczniemy	19
1.1. Czy ta książka jest dla Ciebie?	19
1.2. Jak korzystać z tej książki?	21
1.2.1. Główne rozdziały	21
1.2.2. Laboratorium	21
1.2.3. Dalsze badania	21
1.2.4. Jeden krok dalej	21
1.3. Uwagi dotyczące laboratorium	22
1.3.1. Wybór środowiska laboratoryjnego	22
1.3.2. Laboratorium wirtualne	23
1.3.3. Ćwiczenie na żywej sieci produkcyjnej	24
1.3.4. Moje zalecenia dotyczące środowiska laboratoryjnego	24
1.3.5. Wersje IOS-u Cisco	24
1.4. Zasoby internetowe	25
1.5. Słowo na temat moich zaleceń	25
1.6. Jak natychmiast zostać efektywnym administratorem sieci?	26
Rozdział 2. Co to jest sieć Cisco?	27
2.1. Prawda o routerach i przełącznikach	28
2.2. Adresy MAC	29
2.3. Ramka ethernetowa: duża koperta	31
2.3.1. Kiedy wszyscy mówią, nikt nie słucha	31
2.4. Domeny rozgłoszeniowe	32
2.4.1. Zamykanie bram floodowania: tablica adresów MAC	34
2.4.2. Podzielenie domeny rozgłoszeniowej	34
2.4.3. Łączenie domen rozgłoszeniowych	35
2.4.4. Adresowanie urządzeń w różnych domenach rozgłoszeniowych	36
2.5. Adresy protokołu internetowego (IP)	37
2.5.1. Gdzie jesteś?	37
2.5.2. Dylemat: adres IP czy MAC	38
2.5.3. Protokół ARP	39
2.6. Łączenie domen rozgłoszeniowych za pomocą routera	40
2.6.1. Gdzie jesteś? Gdzie ja jestem?	41
2.6.2. Podsieci	42
2.7. Przechodzenie przez domeny rozgłoszeniowe za pomocą bramy domyślnej	43
2.8. Zarządzanie routerami i przełącznikami	46
2.9. Laboratorium	47

Rozdział 3. Przyspieszony kurs systemu IOS firmy Cisco	49
3.1. Co to jest IOS?	49
3.2. Logowanie się do urządzeń Cisco	50
3.3. Polecenie show	52
3.3.1. <i>Filtrowanie danych wyjściowych</i>	55
3.4. Identyfikacja wersji IOS-u oraz pakietu	57
3.4.1. <i>Numerы wersji</i>	58
3.4.2. <i>Pakiety</i>	58
3.5. Przeglądanie bieżącej konfiguracji	59
3.6. Zmiana bieżącej konfiguracji	60
3.7. Zapisywanie konfiguracji startowej	62
3.8. Polecenie no	63
3.9. Polecenia omówione w tym rozdziale	64
3.10. Laboratorium	64
Rozdział 4. Zarządzanie portami przełączników	65
4.1. Sprawdzanie statusu portu	66
4.2. Włączanie portów	68
4.2.1. <i>Polecenie interface range</i>	70
4.3. Wyłączanie portów	71
4.3.1. <i>Wyszukiwanie nieużywanych interfejsów</i>	71
4.4. Zmiana prędkości portu oraz duplexu	73
4.4.1. <i>Prędkość</i>	73
4.4.2. <i>Dupleks</i>	74
4.4.3. <i>Autonegocjacja</i>	74
4.4.4. <i>Zmiana prędkości portu</i>	75
4.4.5. <i>Zmiana duplexu</i>	76
4.5. Polecenia omówione w tym rozdziale	76
4.6. Laboratorium	77
Rozdział 5. Zabezpieczanie portów przy użyciu funkcji Port Security	79
5.1. Minimalna konfiguracja Port Security	80
5.1.1. <i>Zapobieganie atakom MAC flooding</i>	80
5.1.2. <i>Tryby naruszenia</i>	84
5.2. Testowanie funkcji Port Security	85
5.3. Jak sobie radzić z przenoszeniem urządzeń	86
5.3.1. <i>Port Security nigdy nie zapomina!</i>	86
5.3.2. <i>Czas starzenia się</i>	88
5.4. Uniemożliwianie dostępu nieautoryzowanym urządzeniom	90
5.4.1. <i>Zapewnienie maksymalnego bezpieczeństwa portów</i>	90
5.4.2. <i>Lepkie adresy MAC</i>	91
5.4.3. <i>Zastrzeżenia dotyczące lepkich adresów MAC</i>	93
5.5. Polecenia omówione w tym rozdziale	93
5.6. Laboratorium	93

Rozdział 6. Zarządzanie wirtualnymi sieciami LAN (VLAN-ami)	95
6.1. Czym jest VLAN?	96
6.2. Inwentaryzacja VLAN-ów	96
6.2.1. Baza danych VLAN-ów	96
6.2.2. Domyślny VLAN	98
6.2.3. Ile VLAN-ów należy utworzyć?	98
6.2.4. Planowanie nowego VLAN-u	98
6.3. Tworzenie VLAN-ów	99
6.4. Przypisywanie VLAN-ów do portów	101
6.4.1. Sprawdzanie konfiguracji portów	101
6.4.2. Ustawianie dostępu do VLAN-u	101
6.4.3. Ustawianie trybu dostępu	103
6.5. VLAN-y głosowe	104
6.6. Korzystanie z nowych sieci VLAN	105
6.7. Polecenia omówione w tym rozdziale	106
6.8. Laboratorium	106
Rozdział 7. Przekraczanie bariery VLAN-ów przy użyciu komutowanych interfejsów wirtualnych	107
7.1. Związek między VLAN-em i podsiecią	108
7.2. Przełączniki czy routery?	112
7.2.1. Włączanie routingu IP	113
7.3. Czym są komutowane interfejsy wirtualne?	113
7.3.1. Tworzenie i konfigurowanie interfejsów SVI	114
7.4. Bramy domyślne	116
7.4.1. Sprawdzanie połączeń między sieciami VLAN	118
7.5. Polecenia omówione w tym rozdziale	118
7.6. Laboratorium	118
Rozdział 8. Przypisywanie adresów IP za pomocą protokołu DHCP	121
8.1. Przełączać czy nie przełączać?	122
8.2. Konfigurowanie serwera DHCP firmy Cisco	122
8.2.1. Zakresy	122
8.2.2. Opcje	124
8.2.3. Czas dzierżawy	124
8.2.4. Podsieci i VLAN-y	124
8.3. Konfigurowanie puli DHCP	125
8.4. Wyłączanie adresów z przypisywania	126
8.5. Konfigurowanie urządzeń do żądania adresów DHCP	128
8.6. Powiązanie pul DHCP z VLAN-ami	129
8.7. Tworzenie drugiej puli DHCP	131
8.8. Wyświetlanie dzierżaw DHCP	133
8.9. Korzystanie z serwerów DHCP innych niż Cisco	133
8.9.1. Korzystanie z pomocy przełącznika — polecenie <code>ip helper-address</code>	134

8.10. Polecenia omówione w tym rozdziale	135
8.11. Laboratorium	135
Rozdział 9. Zabezpieczenie sieci za pomocą list kontroli dostępu IP	137
9.1. Blokowanie ruchu IP – IP	138
9.1.1. Tworzenie listy dostępu	139
9.2. Zastosowanie listy ACL do interfejsu	142
9.3. Blokowanie ruchu IP – podsieć	144
9.3.1. Maski wieloznaczne	145
9.3.2. Podmienianie list ACL	146
9.3.3. Zastosowanie listy kontroli dostępu do komutowanego interfejsu wirtualnego	147
9.4. Blokowanie ruchu podsieć – podsieć	148
9.5. Polecenia omówione w tym rozdziale	152
9.6. Laboratorium	152
Rozdział 10. Łączenie przełączników za pomocą kanałów trunkowych	153
10.1. Podłączanie nowego przełącznika	154
10.2. Czym są łącza trunkowe VLAN-ów?	155
10.2.1. Konfigurowanie łącza trunkowego	156
10.2.2. Konfigurowanie DTP do automatycznego negocjowania trunku	157
10.3. Konfigurowanie przełącznika Switch2	159
10.3.1. Konfigurowanie VLAN-ów na nowym przełączniku	160
10.4. Przenoszenie urządzeń do nowego przełącznika	162
10.5. Zmiana kapsułkowania trunku	163
10.6. Polecenia omówione w tym rozdziale	165
10.7. Laboratorium	165
Rozdział 11. Automatyczne konfigurowanie VLAN-ów przy użyciu protokołu VTP	167
11.1. Kilka słów ostrzeżenia	168
11.2. Konfigurowanie przełącznika Switch1 jako serwera VTP	169
11.3. Konfigurowanie przełącznika Switch2 jako klienta VTP	170
11.4. Tworzenie nowych VLAN-ów na przełączniku Switch1	171
11.5. Włączanie funkcji VTP pruning	173
11.6. Polecenia omówione w tym rozdziale	177
11.7. Laboratorium	177
Rozdział 12. Zastosowanie protokołu Spanning Tree do ochrony przed powstawaniem pętli między mostkami	179
12.1. Jak działa Spanning Tree?	180
12.1.1. Jak Spanning Tree radzi sobie z awariami łączy?	183
12.2. Rapid Spanning Tree	186
12.3. PortFast	188

12.4. Polecenia omówione w tym rozdziale	190
12.5. Laboratorium	190
Rozdział 13. Optymalizacja wydajności sieci przy użyciu kanałów port channel	191
13.1. Statyczny czy dynamiczny?	192
13.1.1. Statyczny	192
13.1.2. Dynamiczny	193
13.2. Konfigurowanie dynamicznego kanału port channel za pomocą protokołu LACP	193
13.3. Tworzenie statycznego kanału port channel	197
13.4. Metody równoważenia obciążenia	199
13.5. Polecenia omówione w tym rozdziale	202
13.6. Laboratorium	202
Rozdział 14. Zwiększanie poziomu skalowalności sieci poprzez łączenie routerów i przełączników	203
14.1. Konfiguracja router na patyku	204
14.2. Podłączanie routera Router1	205
14.3. Konfigurowanie podinterfejsów	207
14.4. Tablica routingu IP	211
14.5. Zastosowanie listy ACL do podinterfejsu	213
14.6. Polecenia omówione w tym rozdziale	214
14.7. Laboratorium	214
Rozdział 15. Ręczne kierowanie ruchem za pomocą tablicy routingu IP	215
15.1. Podłączanie routera Router1 do przełącznika Switch2	216
15.2. Konfigurowanie podsieci tranzytowych	218
15.2.1. Przypisywanie tranzytowych adresów IP bezpośrednio do interfejsów fizycznych	218
15.2.2. Przypisywanie tranzytowych adresów IP do podinterfejsów i interfejsów SVI	220
15.3. Usuwanie łącza trunkowego między przełącznikami	221
15.4. Konfigurowanie bram domyślnych	221
15.5. Tworzenie puli DHCP dla podsieci Executives	222
15.6. Polecenia omówione w tym rozdziale	229
15.7. Laboratorium	229
Rozdział 16. Przyspieszony kurs protokołów routingu dynamicznego	231
16.1. Identyfikatory routerów	233
16.1.1. Konfigurowanie interfejsów pętli zwrotnej	233
16.2. Konfigurowanie EIGRP	234
16.2.1. Wybieranie najlepszej ścieżki	239
16.2.2. Omijanie awarii łączy	241
16.2.3. Podsumowanie konfiguracji EIGRP	242
16.3. Protokół OSPF	243

16.4. Polecenia omówione w tym rozdziale	247
16.5. Laboratorium	247
Rozdział 17. Śledzenie urządzeń	249
17.1. Scenariusze śledzenia urządzeń	249
17.2. Etapy śledzenia urządzenia	250
17.2.1. Uzyskiwanie adresu IP	250
17.2.2. Śledzenie urządzenia do ostatniego skoku	250
17.2.3. Uzyskiwanie adresu MAC	250
17.3. Przykład 1. — śledzenie drukarki sieciowej	251
17.3.1. Śledzenie do ostatniego skoku za pomocą traceroute	251
17.3.2. Protokół CDP	252
17.3.3. Uzyskiwanie adresu MAC urządzenia	253
17.3.4. Wyświetlanie tablicy adresów MAC	253
17.4. Przykład 2. — śledzenie serwera	254
17.4.1. Śledzenie do ostatniego skoku za pomocą traceroute	255
17.4.2. Uzyskiwanie adresu MAC urządzenia	256
17.4.3. Wyświetlanie tablicy adresów MAC	256
17.5. Polecenia omówione w tym rozdziale	258
17.6. Laboratorium	259
Rozdział 18. Zabezpieczanie urządzeń Cisco	261
18.1. Tworzenie uprzywilejowanego konta użytkownika	262
18.1.1. Testowanie konta	262
18.2. Rekonfiguracja linii VTY	264
18.2.1. Włączenie SSH i wyłączenie dostępu poprzez Telnet	264
18.2.2. Ograniczanie dostępu SSH przy użyciu list dostępu	266
18.3. Zabezpieczanie portu konsoli	267
18.4. Polecenia omówione w tym rozdziale	268
18.5. Laboratorium	268
Rozdział 19. Łatwiejsze rozwiązywanie problemów dzięki użyciu rejestrowania i debugowania	271
19.1. Konfigurowanie bufora rejestrowania	272
19.2. Polecenia debugowania	273
19.2.1. Debugowanie funkcji Port Security	274
19.2.2. Debugowanie DHCP	275
19.2.3. Debugowanie VTP	276
19.2.4. Debugowanie routingu IP	277
19.3. Poziomy ważności rejestrowania	278
19.4. Konfigurowanie syslogu	280
19.5. Polecenia omówione w tym rozdziale	281
19.6. Laboratorium	282

Rozdział 20. Odzyskiwanie sprawności po katastrofie	283
20.1. Zawęż zakres do podzbioru urządzeń	284
20.2. Ponowne uruchamianie urządzeń	284
20.2.1. Planowanie ponownego uruchamiania	285
20.3. Usuwanie konfiguracji startowej	286
20.4. Resetowanie hasła	288
20.4.1. Resetowanie hasła na routerze	288
20.4.2. Resetowanie hasła na przełączniku	290
20.5. Polecenia omówione w tym rozdziale	291
Rozdział 21. Lista kontrolna wydajności i poprawności funkcjonowania elementów sieci	293
21.1. Czy CPU jest przeciążony?	294
21.2. Jaki jest czas pracy systemu?	295
21.3. Czy uszkodzone są kabel sieciowy lub gniazdo?	296
21.4. Czy czasy pingów są wyjątkowo wysokie lub niespójne?	296
21.5. Czy trasy trzepoczą?	297
21.6. Polecenia omówione w tym rozdziale	298
21.7. Laboratorium	298
Rozdział 22. Następne kroki	301
22.1. Źródła związane z certyfikacją	301
22.2. Virtual Internet Routing Lab firmy Cisco	302
22.3. Rozwiązywanie problemów z łącznością użytkowników końcowych	302
22.4. Nigdy nie ma końca	303
Skorowidz	305

Zabezpieczanie portów przy użyciu funkcji Port Security

W poprzednim rozdziale dowiedziałeś się, jak zabezpieczyć nieużywane porty, wyłączając je. Wyłączenie nieużywanych portów może powstrzymać złoczyńcę przed podłączeniem złośliwego urządzenia do takiego portu i uzyskaniem nieautoryzowanego dostępu do sieci. Może również pomóc wyszkolić użytkowników (zwłaszcza tych w oddalonych biurach), aby dzwonili do działu IT, *zanim* zaczną coś przestawiać. Po kilku rundach chodzenia między przełącznikiem i biurkiem oraz bezowocnego przepinania komputera z jednego pustego portu do drugiego większość użytkowników wpadnie wreszcie na pomysł, że należałoby najpierw zadzwonić do informatyka.

Chociaż wyłączenie portów jest najbardziej bezpieczną opcją radzenia sobie z nieużywanymi portami, to żaden sposób nie zabezpiecza używanych portów. W żywym środowisku większość portów przełączników *będzie* w użyciu.

Funkcja *Port Security*, czyli zabezpieczanie portów, jest wszechstronną funkcją, która może zmniejszyć liczbę ataków na sieć i zapobiec nieautoryzowanym działaniom, takim jak przenoszenie, dodawanie i zmienianie urządzeń. Osiąga się to dzięki ograniczeniu liczby unikatowych adresów MAC, które mogą korzystać z danego portu. Jak pewnie pamiętasz, każde urządzenie w sieci ma unikatowy adres MAC, który służy do komunikacji z innymi urządzeniami w tej samej domenie rozgłoszeniowej. Wszechstronność ma kluczowe znaczenie, ponieważ zabezpieczenia nie są opcją, która zadowala wszystkich w równym stopniu. Niektóre organizacje wolą minimalny poziom zabezpieczeń, podczas gdy inne wymagają poziomu bezpieczeństwa graniczącego z paranoją. Zamiast wskazywać Ci, jaki poziom bezpieczeństwa powinna mieć Twoja sieć, w tym rozdziale okreśłem konkretne zagrożenia, przed którymi może chronić funkcja Port Security,

żebyś mógł samodzielnie zdecydować, jak bardzo restrykcyjny chcesz być. Potem pokażę Ci, jak skonfigurować Port Security, aby ta funkcja spełniała Twoje wymagania.

Nie zaprezentuję Ci wszystkich możliwości konfigurowania Port Security. Zamiast tego nauczę Cię, jak skonfigurować tę funkcję dla minimalnego i maksymalnego poziomu zabezpieczeń, tak jak pokazano w tabeli 5.1.

Tabela 5.1. Poziomy zabezpieczeń funkcji Port Security

Poziom zabezpieczeń	Ochrona przed atakami
Minimalny	MAC flooding, Denial of Service, podsłuchiwanie ruchu sieciowego
Maksymalny	Wszystkie powyższe oraz dodatkowo nieautoryzowany dostęp do urządzeń i rozprzestrzenianie złośliwego oprogramowania

Tabela 5.1 zawiera listę ataków, przed którymi pomagają chronić każdy poziom zabezpieczeń Port Security. Zaczynijmy od minimalnego poziomu.

5.1. Minimalna konfiguracja Port Security

Chociaż nie mogę Ci wskazać, jaki poziom bezpieczeństwa powinna mieć Twoja sieć, mogę Ci powiedzieć, że zdecydowanie powinieneś włączyć minimalną konfigurację Port Security na wszystkich portach użytkownika końcowego.

Bezpieczeństwo jest zawsze kompromisem. Musisz rozważyć, czy warto poświęcić czas, pieniądze i wysiłek w celu obrony przed konkretnym zagrożeniem. Funkcja Port Security jest częścią systemu IOS, więc korzystanie z niej nie pociąga za sobą dodatkowych kosztów. Natomiast czas i wysiłek potrzebne do skonfigurowania Port Security na minimalnym poziomie są nieistotne. W zamian otrzymujesz spokój i ochronę przed potencjalnie wyniszczającym i kosztownym atakiem, nazywanym atakiem MAC flooding.

5.1.1. Zapobieganie atakom MAC flooding

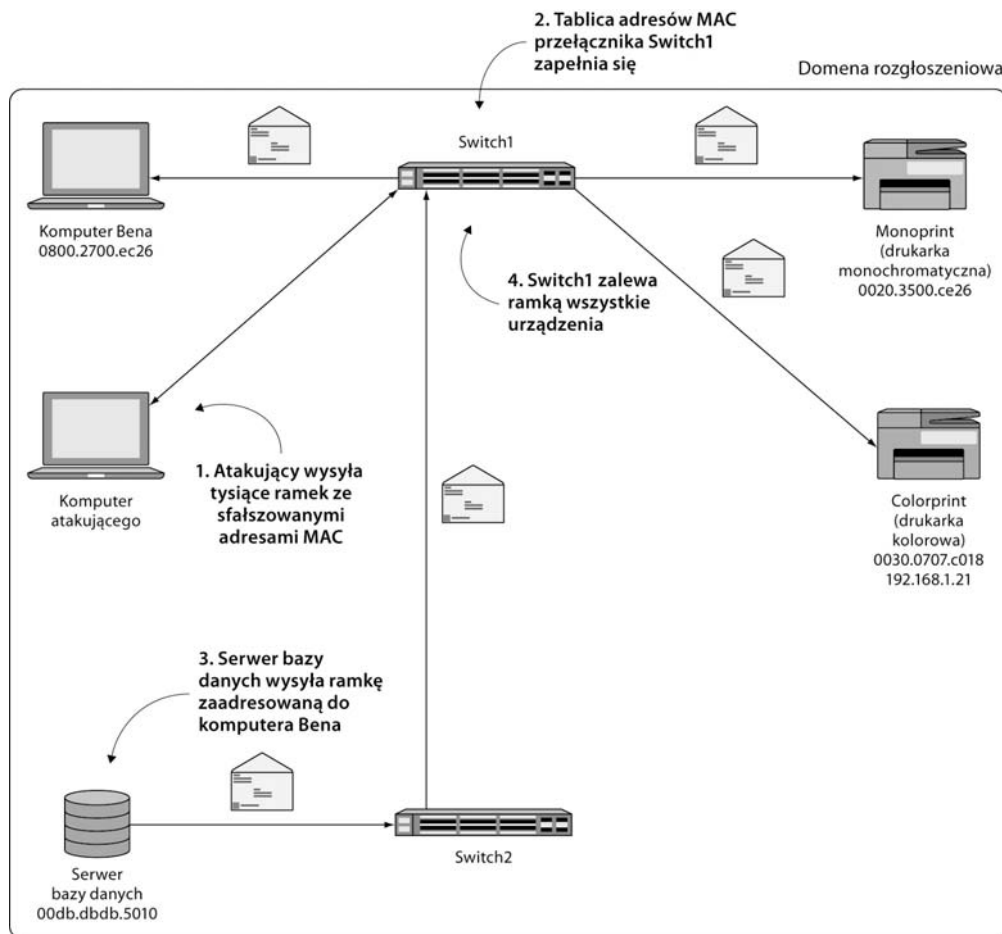
Przypomnijmy z rozdziału 2., że przełącznik utrzymuje tablicę adresów MAC zawierającą adres MAC każdego urządzenia oraz port, do którego dane urządzenie jest podłączone. Tabela 5.2 jest przykładem typu informacji, jakie można znaleźć w tablicy adresów MAC. Dzięki śledzeniu lokalizacji każdego urządzenia przełącznik unika zalewania każdą ramką każdego urządzenia.

Tabela 5.2. Przykładowa tablica adresów MAC

Urządzenie	Adres MAC	Port przełącznika
Komputer Bena	0800.2700.ec26	FastEthernet0/1

W ataku MAC flooding złośliwy program stale wysyła ramki z adresami źródłowymi, które są sfałszowanymi lub podmienionymi adresami MAC. Ponieważ każda ramka pochodzi z innego adresu MAC, tablica adresów MAC przełącznika wypełnia się tymi fałszywymi adresami, a przełącznik nie ma wyboru i musi wysyłać każdą ramkę do każdego portu. W efekcie komputer, na którym działa złośliwy program, staje się snifferem (podsłuchiwcem) sieciowym, będącym w stanie przechwycić każdą ramkę w sieci.

Rysunek 5.1 ilustruje, w jaki sposób atakujący może używać ataku MAC flooding w celu przechwytywania ruchu.



Rysunek 5.1. Atak MAC flooding

W kroku 1. atakujący wysła do przełącznika Switch1 tysiące ramek ze sfalszowanymi źródłowymi adresami MAC. W kroku 2. zapelnia się tablica adresów MAC przełącznika Switch1. W kroku 3. serwer bazy danych wysła ramkę zaadresowaną do mojego komputera. Switch2 przekazuje tę ramkę do przełącznika Switch1. Wreszcie w kroku 4. przełącznik Switch1 zalewa tą ramką wszystkie porty, łącznie z tym podłączonym do komputera atakującego.

Tak naprawdę dzieje się jednak coś znacznie gorszego. MAC flooding może skutkować odmową usługi (ang. *denial of service*) dla wszystkich użytkowników. Przypomnij sobie powiedzenie z rozdziału 2.: „Kiedy wszyscy mówią, nikt nie słucha”. MAC flooding poważnie zmniejsza wydajność sieci aż do punktu, w którym staje się ona praktycznie

bezużyteczna. Wyobraź sobie, że dziesiątki dzwoniących klientów zostaje naraz rozłączonych, ponieważ ruch Voice over IP nie może przechodzić przez sieć. Dzięki funkcji Port Security Ty jako administrator sieci możesz mieć pewność, że nigdy nie wpakujesz się w taką nieznośną sytuację, w której będziesz musiał poradzić sobie z tego typu wydarzeniem. Wystarczy tylko jeden niechroniony port, żeby atak MAC flooding zablokował Twoją sieć, dlatego tak ważne jest skonfigurowanie funkcji Port Security na każdym porcie.

UWAGA Przed atakami MAC flooding możesz chronić się za pomocą oprogramowania antywirusowego zainstalowanego na komputerach osobistych i serwerach oraz upewniając się, że użytkownicy końcowi nie mają dostępu administracyjnego do swoich komputerów. Jednak te metody nie są w 100% niezawodne. Port Security jest najbardziej niezawodnym sposobem zapobiegania atakowi MAC flooding, nawet jeśli zawiodą inne środki bezpieczeństwa.

Zwykle przełącznika nie obchodzi, ile różnych adresów MAC jest na tym samym porcie. Dopuszcza ruch niezależnie od źródłowego adresu MAC. Pamiętaj, że adresy MAC zostały wymyślone, aby umożliwić natychmiastowe działanie urządzeń po podłączeniu ich do sieci. Jednak właśnie to zachowanie *plug-and-play* umożliwia przeprowadzanie ataków MAC flooding.

Oczywistym rozwiązaniem jest ograniczenie liczby adresów MAC, które mogą być jednocześnie powiązane z danym portem. To właśnie robi Port Security. Konfigurujesz tę funkcję, aby dopuszczała określoną liczbę równoczesnych adresów MAC, a następnie dostęp jest przyznawany w kolejności zgłoszeń. Spójrzmy na przykład.

Załóżmy, że masz użytkownika z dwoma urządzeniami — komputerem PC i telefonem IP Cisco — podłączonymi do tego samego portu. Telefon jest fizycznie podłączony do przełącznika, a komputer jest fizycznie podłączony do telefonu i przez niego się komunikuje. Tabela 5.3 przedstawia, jak mniej więcej wyglądałyby te urządzenia w tablicy adresów MAC.

Tabela 5.3. Tablica adresów MAC

Urządzenie	Adres MAC	Port
PC	0123.4567.8901	FastEthernet0/23
Telefon IP	0123.4598.7654	FastEthernet0/23

Te dwa urządzenia reprezentują dwa unikatowe adresy MAC, więc musisz ograniczyć maksymalną liczbę adresów MAC do dwóch za pomocą polecenia interfejsu switchport port-security maximum 2.

SPRÓBUJ TERAZ Zlokalizuj port z dwoma podłączonymi do niego urządzeniami. Jeśli masz komputer podłączony poprzez telefon IP, to doskonale. Jeśli nie, możesz nadal wykonać to ćwiczenie. Po prostu zmień polecenie, aby dopuszczało tylko jeden adres MAC.

Wykonaj poniższe polecenia, aby skonfigurować maksymalną dozwoloną liczbę dwóch adresów MAC na porcie:

```
interface fa0/1
switchport mode access
switchport port-security maximum 2
```

Na tym etapie nic nie powinno się stać. To dlatego, że wspomniane polecenie nie włącza w rzeczywistości funkcji Port Security. Może Ci się to wydawać sprzeczne z intuicją, ale tak naprawdę jest to błogosławieństwo. Źle skonfigurowana funkcja Port Security może w efekcie uczynić port bezużytecznym. Ważne jest, żebyś dowiedział się, ile adresów MAC powinno być dopuszczonych na każdym z portów, *zanim* włączysz Port Security.

Jeśli nie masz pewności co do liczby adresów MAC, możesz ustawić jakąś wysoką wartość, na przykład 10, a następnie wrócić do tego później i poprawić. W ten sposób, jeśli Twój szef ma ukryty pod biurkiem sekretny przełącznik grupy roboczej z podłączonymi ośmioma różnymi adresami MAC, dowiesz się o tym z IOS-u zamiast od niego.

SPRÓBUJ TERAZ Po poprawnym ustawieniu maksymalnej liczby adresów MAC włącz funkcję Port Security za pomocą polecenia interfejsu `switchport port-security`.

Teraz sprawdź konfigurację za pomocą polecenia `show port-security`.

Powinieneś zobaczyć coś podobnego do tego:

```
Switch1#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1          2              2              0                  Shutdown
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

Dane wyjściowe nie dostarczają wielu szczegółów, ale jest to wystarczające, żeby dowiedzieć się, co się tutaj dzieje. Po włączeniu Port Security na porcie funkcja zwraca uwagę na adresy MAC, które komunikują się na tym porcie w danym momencie, i zapamiętuje je — maksymalnie tyle adresów, ile określiłeś. To właśnie pokazuje kolumna `MaxSecureAddr` (maksymalna liczba bezpiecznych adresów). W tym listingu maksymalna liczba adresów MAC dozwolonych na porcie Fa0/1 wynosi 2.

Kolumna `CurrentAddr` (bieżące adresy) wskazuje liczbę adresów MAC, którą przełącznik widział na porcie od momentu włączenia Port Security. W tym listingu ta liczba również wynosi 2, ponieważ podłączone są tylko dwa urządzenia.

W kolumnie `SecurityViolation` (naruszenie bezpieczeństwa) znajduje się informacja, ile razy przełącznik wykrył na tym porcie dodatkowy adres MAC powyżej dozwolonego maksimum. Tak jak można oczekiwać, liczba ta wynosi 0.

Ostatnia kolumna, oznaczona jako `Security Action` (podejmowane działania bezpieczeństwa), jest prawdopodobnie najważniejsza. Zawiera listę działań, jakie funkcja Port

Security podejmie, gdy wykryje *naruszenie* — dodatkowy adres MAC przekraczający skonfigurowane maksimum. To działanie Cisco nazywa **trybem naruszenia** (ang. *violation mode*).

5.1.2. Tryby naruszenia

Skonfigurujemy dwa tryby naruszenia: zamknięcie (shutdown) i ograniczenie (restrict).

ZAMKNIĘCIE

W poprzednim listingu trybem naruszenia jest zamknięcie. Oznacza to dokładnie to, o czym myślisz. Jeśli Port Security wykryje naruszenie bezpieczeństwa, czyli dodatkowy adres MAC poza maksymalnymi dwoma dopuszczonymi, całkowicie wyłączy port. Bez ostrzeżenia. Bez zadawania pytań.

Zachowanie powodujące zamknięcie portu jest domyślne. Podejrzewam, że w ten sposób Cisco chce zapobiec sytuacjom, w których ktoś przypadkowo skonfigurował Port Security, a następnie zastanawia się, dlaczego nic nie działa. Gdy używany port przestanie nagle działać po włączeniu funkcji Port Security, może to być dość dramatyczne i trudne do przegapienia.

OGRANICZENIE

Alternatywny tryb naruszenia, ograniczenie, jest nieco subtelniejszy. Gdy w tym trybie pojawia się naruszenie, Port Security utrzymuje włączony port, ale uniemożliwia komunikowanie się nowym adresom MAC. W pewnym sensie przypomina to dynamiczną listę dostępu, która nie dopuszcza adresów MAC przekraczających określone maksimum.

Prawdopodobnie nie będziesz chciał, aby funkcja Port Security całkowicie zamykała port przy wykryciu naruszenia. W takim przypadku musisz ręcznie ustawić tryb naruszenia na ograniczenie za pomocą polecenia interfejsu `switchport port-security violation restrict`.

SPRÓBUJ TERAZ Zmień tryb naruszenia na ograniczenie za pomocą następującego polecenia:

```
switchport port-security violation restrict
```

Jak zawsze, sprawdź konfigurację, używając polecenia `show port-security`.

Powinieneś zobaczyć, że tryb naruszenia w ostatniej kolumnie zmienił się z Shutdown na Restrict. Wszystko inne pozostanie takie samo:

```
Switch1#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1          2              2              0                  Restrict
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```


Gdy Port Security wykryje naruszenie, nie zamknie portu ani w żaden inny sposób nie wpłynie na dwa pierwsze adresy MAC. Będą one nadal komunikować się normalnie i tylko kolejne adresy zostaną zablokowane.

JEDEN KROK DALEJ Trybu naruszenia shutdown możesz użyć, aby uniemożliwić komukolwiek podłączenie nieautoryzowanego punktu dostępu bezprzewodowego wykorzystującego technologię zasilania PoE (ang. *Power over Ethernet*). Kiedy IOS zamyka port na przełączniku PoE, odcina zasilanie wszelkim podłączonym do tego portu urządzeniom. Jest to również powód, dla którego nie używamy z reguły trybu naruszenia shutdown na portach z podłączonymi telefonami IP.

5.2. Testowanie funkcji Port Security

Jednym z najciekawszych aspektów funkcji Port Security jest jej testowanie. Nie musisz w tym celu przeprowadzać własnego ataku MAC flooding. Wystarczy, że na tym samym porcie pojawi się jeden dodatkowy adres MAC. Jest na to kilka sposobów.

Jeśli masz do czynienia z komputerem PC i telefonem IP, odłącz ten komputer od telefonu i podepnij w to miejsce laptop. Gdy przełącznik zobaczy adres MAC laptopa, funkcja Port Security zarejestruje naruszenie bezpieczeństwa i uniemożliwi temu adresowi komunikację.

Jeśli masz tylko jeden komputer PC, podłącz niewielki przełącznik grupy roboczej pomiędzy przełącznikiem Cisco i komputerem. Weź dwa laptopy lub telefony IP i podłącz je do przełącznika grupy roboczej. Daje to trzy adresy MAC na tym samym porcie — wystarczy, żeby spowodować naruszenie Port Security.

SPRÓBUJ TERAZ Ważne jest, żebyś podczas testowania funkcji Port Security dokładnie obserwował różne rzeczy. IOS może pokazać w czasie rzeczywistym informacje o tym, co robi Port Security. Wystarczy w trybie uprzywilejowanym wpisać polecenie terminal monitor.

Następnie użyj jednej z wymienionych powyżej metod w celu przetestowania funkcji Port Security.

Po podłączeniu trzeciego urządzenia powinien się pojawić komunikat podobny do tego:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by
MAC address 0800.27ba.dbad on port FastEthernet0/1.
```

Ten komunikat konsoli nie pozostawia wiele miejsca na interpretację. Podaje port, na którym doszło do naruszenia, oraz adres MAC będący tego przyczyną — dobre informacje, przydatne podczas testowania.

Jeśli wykonasz teraz ponownie polecenie `show port-security`, powinieneś zobaczyć wzrost liczby naruszeń bezpieczeństwa w kolumnie `SecurityViolation`:

```
Switch1#sh port-security
Secure Port    MaxSecureAddr    CurrentAddr    SecurityViolation    Security Action
              (Count)          (Count)        (Count)
-----
```

```
-----
Fa0/1      2      2      18      Restrict
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

Liczba 18 może wydawać się nieco niespodziewana, biorąc pod uwagę, że funkcja Port Security powinna zablokować tylko jeden adres MAC. Licznik SecurityViolation jest zwiększany za każdym razem, gdy nieautoryzowany adres MAC próbuje wysłać ramkę. Jeśli poprawnie skonfigurowałeś maksymalną liczbę adresów MAC, wartość licznika nie powinna być bardzo wysoka. Jeżeli jednak jest wysoka, to wskazówka, że musisz zbadać urządzenia w tym porcie.

JEDEN KROK DALEJ Możesz wyzerować licznik SecurityViolation poprzez wyłączenie portu i ponowne jego włączenie. W chwili, gdy powstaje ten rozdział, nie ma żadnego polecenia do bezpośredniego zerowania liczników.

5.3. Jak sobie radzić z przenoszeniem urządzeń

Wspomniałem już wcześniej, że Port Security działa na zasadzie kolejności zgłoszeń. Kiedy fizycznie odłączysz urządzenie od zabezpieczonego portu, funkcja Port Security zapomni wszystkie adresy MAC, które widziała na tym porcie. Dlatego, jeśli podłączysz inne urządzenie do tego samego portu, Port Security nadal będzie na to pozwalać. Działa to dobrze w przypadkach, gdy przenoszenie urządzeń zawsze pociąga za sobą fizyczne odłączenie czegoś od przełącznika. Przykładowo, gdy użytkownik zmienia biurko i ktoś fizycznie odłączy jego komputer i telefon IP od przełącznika.

Istnieje jednak jeszcze jedna możliwość. Załóżmy, że administrator systemów informatycznych musi jednocześnie podłączyć do sieci pięć nowych komputerów w celu zainstalowania oprogramowania, pobrania aktualizacji i tak dalej, aby przygotować te komputery dla nowych użytkowników. Jest jednak pewien problem: w biurze, w którym pracują, jest tylko jedno gniazdo sieciowe. Aby zachować wydajność i przygotować komputery na czas, administrator podcina do tego gniazda mały 8-portowy przełącznik grupy roboczej, a do niego podłącza wszystkie nowe komputery.

5.3.1. Port Security nigdy nie zapomina!

W szafie sieciowej gniazdo jest podłączone do portu FastEthernet0/12 na przełączniku. Odrobiłeś pracę domową i wiesz, że nigdy nie powinno być więcej niż pięć jednoczesnych adresów MAC na porcie, do którego podłączony jest przełącznik grupy roboczej. Konfigurujesz więc funkcję Port Security, aby dopuszczała maksymalnie pięć adresów MAC.

SPRÓBUJ TERAZ Nie ma problemu, jeśli tak naprawdę nie masz podłączonego małego przełącznika. To tylko ćwiczenie. Użyj poniższych poleceń, aby skonfigurować Port Security w celu dopuszczania maksymalnie pięciu jednoczesnych adresów MAC na porcie FastEthernet0/12:

```

interface fa0/12
switchport port-security maximum 5
switchport port-security violation restrict
switchport port-security

```

Po uruchomieniu przez administratora systemu pięciu komputerów każdy zaczyna wysyłać ruch ze swoim unikatowym adresem MAC. Wszystko działa zgodnie z oczekiwaniami, a komputery mogą normalnie komunikować się z siecią. Polecenie `show port-security` potwierdza, że funkcja Port Security jest włączona i niczego nie blokuje:

```

Switch1#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1          2               0              0                  Restrict
Fa0/12         5               5              0                  Restrict
-----
Total Addresses in System (excluding one mac per port) : 4
Max Addresses limit in System (excluding one mac per port) : 6144

```

Po zakończeniu pracy administrator zamyka maszyny i podłącza do przełącznika grupy roboczej pięć nowych, aby je skonfigurować. Ale teraz jest kolejny problem. Żadna z maszyn nie może w ogóle połączyć się z siecią. Ponownie sprawdzasz Port Security i widzisz następujące informacje:

```

Switch1#show port-security
Secure Port    MaxSecureAddr  CurrentAddr    SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1          2               0              0                  Restrict
Fa0/12         5               5              30                  Restrict
-----
Total Addresses in System (excluding one mac per port) : 4
Max Addresses limit in System (excluding one mac per port) : 6144

```

Adres MAC został zablokowany. ←

Funkcja Port Security nie odpuściła pierwotnych pięciu adresów MAC. Nadal je pamięta, a tym samym nie zezwala na komunikowanie się nowym komputerom.

Ważne, żebyś zrozumiał, dlaczego tak się dzieje. Port Security nie ma pojęcia, że oryginalne pięć komputerów zostało odłączonych od sieci. Ten fakt ukrywa 8-portowy przełącznik grupy roboczej. Funkcja Port Security wie tylko, że widziała pięć unikatowych adresów MAC, a potem zobaczyła pięć nowych. Zgodnie z konfiguracją Port Security dopuszcza tylko pięć pierwszych adresów MAC i blokuje kolejne.

Mógłbyś powiedzieć administratorowi systemów, aby po prostu odłączył lub zrestartował przełącznik grupy roboczej za każdym razem, gdy podpina nową grupę komputerów, ale to niepraktyczne, denerwujące i powoduje przedwczesne zużywanie się przełącznika. Potrzebujesz innego sposobu na zmuszenie funkcji Port Security, aby zapominała o tych adresach MAC bez jakiegokolwiek ręcznej interwencji.

5.3.2. Czas starzenia się

Czas starzenia się (ang. *aging time*) jest parametrem, który może spowodować okresowe zapominanie przez funkcję Port Security adresów MAC, których się nauczyła.

Gdy administrator systemów skończy konfigurować jeden zestaw pięciu komputerów, około 10 minut zajmie mu odłączenie ich, przeniesienie, a następnie podłączenie nowego zestawu. Chcesz, żeby w tym czasie adresy MAC z pierwszego zestawu zastarzały się, aby zanim administrator systemów podłączy drugi zestaw, funkcja Port Security zapomniała o pierwszych pięciu komputerach.

SPRÓBUJ TERAZ Czas starzenia się, podobnie jak wszystkie inne opcje Port Security, jest ustawiany dla każdego portu osobno. Użyj poniższych poleceń, aby ustawić czas starzenia się na 10 minut:

```
interface fa0/12
switchport port-security aging time 10
```

Aby zweryfikować konfigurację, użyj następującego polecenia:

```
show port-security interface fa0/12
```

Oto przykład tego, co powinieneś zobaczyć:

```
Switch1#show port-security interface fa0/12
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 10 mins ← Czas starzenia się
Aging Type              : Absolute   ustawiony na 10 minut.
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 5
Total MAC Addresses     : 5
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0800.271c.0b57:1
Security Violation Count : 30
```

W czwartej linii listingu możesz zobaczyć czas starzenia się (Aging Time) w minutach. Port Security odlicza czas starzenia się dla każdego adresu MAC *niezależnie* na podstawie tego, kiedy zobaczył dany adres. Możesz to podejrzeć za pomocą polecenia `show port-security address`:

```
Switch1#show port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0800.2742.aab8	SecureDynamic	Fa0/12	6
1	0800.2782.4c93	SecureDynamic	Fa0/12	6
1	0800.27b8.b488	SecureDynamic	Fa0/12	6
1	0800.27e4.bb01	SecureDynamic	Fa0/12	6
1	0800.7200.3131	SecureDynamic	Fa0/12	6

```
-----
Total Addresses in System (excluding one mac per port) : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

Zwróć uwagę, że każdy adres MAC ma taki sam Remaining Age (pozostały czas). To nie jest zaskakujące, ponieważ administrator systemów uruchomił wszystkie pięć komputerów jednocześnie.

Przypuśćmy teraz, że administrator systemów skończył z czterema z pięciu komputerów i wyłączył je. Pozostał mu jeden komputer do zrobienia, więc zostawił go włączonego. Przyniósł cztery nowe komputery, podłączył je i wyłączył. Zgłosił, że wszystko nadal wydaje się działać poprawnie.

Ponownie uruchamiasz polecenie `show port-security address`:

```
Switch1#show port-security address
      Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)	
1	0800.2708.e69b	SecureDynamic	Fa0/12	9	
1	0800.27b6.b091	SecureDynamic	Fa0/12	9	
1	0800.27c1.5607	SecureDynamic	Fa0/12	9	
1	0800.27f4.803e	SecureDynamic	Fa0/12	9	
1	0800.7200.3131	SecureDynamic	Fa0/12	8	← To urządzenie nie zostało zamienione i starzeje się niezależnie od pozostałych adresów.

```
-----
Total Addresses in System (excluding one mac per port) : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

Zwróć uwagę, że cztery pierwsze adresy MAC są inne, a ich pozostały czas starzenia się wynosi 9 minut. Ostatni adres, który należy do komputera *nieodłączonego* przez administratora systemów, nie uległ zmianie i ma pozostały czas starzenia się 8 minut. Ponieważ adres MAC tego komputera znajdował się już na liście dozwolonych adresów MAC, nadal może uzyskać dostęp do sieci, nawet po wyzerowaniu licznika. Gdy licznik osiągnie zero, zresetuje się do 10 minut.

Skoro skonfigurowałeś już czas starzenia się, prawdopodobnie nigdy nie będziesz już musiał grzebać w ustawieniach Port Security na tym konkretnym porcie. Jeśli administrator systemów będzie miał kiedyś problemy z połączeniem, będzie musiał jedynie poczekać kilka minut i spróbować ponownie.

Prawdopodobnie ustalenie właściwego czasu starzenia się adresów MAC będzie wymagało od Ciebie wykonania kilku prób i popełnienia paru błędów. Jeśli okaże się, że nowo podłączane urządzenia nie mogą uzyskać dostępu do sieci, być może będziesz musiał zmniejszyć czas starzenia się. Pamiętaj o potrzebach użytkownika i nie czuj się przymuszony do ustawiania długiego czasu starzenia się. Nawet jeśli ustawisz bardzo krótki czas starzenia się, powiedzmy 1 minutę, port nadal będzie chroniony przed atakiem MAC flooding. Ustawienie dłuższego czasu nie zapewni Ci zwiększonego bezpieczeństwa. Jeżeli jednak wymagasz bardziej rygorystycznych zabezpieczeń, funkcja Port Security również może Ci to zagwarantować.

5.4. Uniemożliwianie dostępu nieautoryzowanym urządzeniom

Dotychczas nauczyłeś się, jak skonfigurować funkcję Port Security, aby zapobiec atakom MAC flooding bez zakłócania legalnego ruchu użytkowników. Jeśli jeszcze samodzielnie trochę poszperasz w IOS-ie i zastosujesz metodę prób i błędów, będziesz mógł skonfigurować Port Security na wszystkich portach użytkownika końcowego w taki sposób, że nikt nawet tego nie zauważy.

Chociaż minimalna konfiguracja Port Security może być świetna dla wydajności użytkowników końcowych, nie wszystkie organizacje są tak zadowolone. Niektóre z nich mają surowe wymagania dotyczące bezpieczeństwa, które zabraniają podłączania do sieci niefirmowych urządzeń. Nie wystarcza im ograniczanie liczby adresów MAC na porcie. Musisz określić, które *konkretne* adresy MAC mogą korzystać z danego portu. Wydaje się to kłopotliwym zadaniem, ale jak się przekonasz, w przypadku funkcji Port Security jest to zaskakująco łatwe.

Nawet jeśli Twoja organizacja nie wymaga takiego uciążliwego poziomu zabezpieczeń, nadal zdecydowanie sugeruję Ci kontynuowanie lektury tego podrozdziału. Już mówię dlaczego. W rozdziale 4. dowiedziałeś się, że jednym z powodów wyłączania nieużywanych portów jest uniemożliwienie osobie, która wejdzie do biura prosto z ulicy z zainfekowanym laptopem, podłączenie tego sprzętu przy jakimś pustym biurku. Ale nawet jeśli skrupulatnie sprawdzasz i wyłączasz nieużywane porty raz dziennie i dwa razy w niedzielę, nie powstrzyma to nikogo od odłączenia pracującego komputera i podłączenia zainfekowanego laptopa.

Można prawdopodobnie wymyślić inne powody ograniczania portu do pojedynczego urządzenia. Na początku rozdziału powiedziałem, że pokażę Ci, jak skonfigurować Port Security w celu zapewnienia maksymalnego bezpieczeństwa. Skoro masz już pewne wyobrażenie o tym, kiedy może być to potrzebne, nauczę Cię, jak to zrobić.

JEDEN KROK DALEJ Bezpieczeństwo polega na tworzeniu warstw ochrony. Chociaż każda organizacja z odrobiną zdrowego rozsądku podejmuje określone działania, aby fizycznie uniemożliwić ludziom wchodzenie prosto z ulicy ze złośliwymi urządzeniami, nie neguje to potrzeby podejmowania technicznych środków mających na celu ochronę sieci. Wszystkie zabezpieczenia można złamać. Możesz mieć jedynie nadzieję, że spowolni to atakującego na tyle, że sam zrezygnuje i poszuka łatwiejszego celu. Port Security jest jedną z technologii, która może utrudnić atakującemu życie.

5.4.1. Zapewnienie maksymalnego bezpieczeństwa portów

Przypomnijmy, że funkcja Port Security po włączeniu zapamiętuje i dopuszcza adresy MAC w takiej kolejności, w jakiej je wykrywa, aż wyczerpie się skonfigurowana maksymalna liczba adresów. Gdy fizycznie podłączone do portu urządzenie zostaje odłączone,

Port Security zapomina te adresy MAC. Jeśli skonfigurowałeś parametr starzenia się na przykład na 5 minut, Port Security zapomni każdy adres MAC po 5 minutach od jego zarejestrowania.

W środowisku o wysokim poziomie zabezpieczeń funkcja Port Security ma działać nieco inaczej. Po pierwsze, powinna dopuszczać i zapamiętywać konkretne adresy MAC urządzeń, które mają być podłączone. Po drugie, nigdy nie powinna zapominać tych adresów MAC — *nigdy!* Nawet jeśli ktoś wyłączy port, odłączy urządzenie lub zrestartuje przełącznik, te adresy MAC mają być przyklejone do portu jako jedyne autoryzowane adresy MAC, które mogą z niego korzystać. Można to osiągnąć, używając czegoś, co Cisco nazywa **lepkimi adresami MAC** (ang. *sticky MAC addresses*).

5.4.2. Lepkie adresy MAC

Lepki adres MAC jest przechowywany na stałe w konfiguracji startowej w sekcji konfiguracji interfejsu. Te adresy MAC są nazywane *lepkimi* dlatego, że nie musisz ich ręcznie konfigurować. Zamiast tego pozwalasz funkcji Port Security wykrywać je w zwykły sposób, a IOS automatycznie zapisuje je w bieżącej konfiguracji. To sprytny sposób na osiągnięcie wysokiego poziomu bezpieczeństwa przy niewielkim wysiłku.

Żałujmy, że Twoja organizacja ma komputer stojący w półpublicznym obszarze, na przykład w holu lub recepcji. Chcesz uniemożliwić, aby ktokolwiek mógł przyjść po godzinach pracy i podłączyć do tego samego portu złośliwe urządzenie. Ponieważ na tym porcie zawsze powinien być widywany tylko jeden adres MAC, konfigurujesz maksymalną liczbę adresów MAC na jeden. Następnie za pomocą polecenia `switchport port-security mac-address sticky` instruujesz funkcję Port Security, aby na stałe zapamiętała ten adres MAC.

SPRÓBUJ TERAZ Wybierz port z podłączonym tylko jednym urządzeniem i skonfiguruj funkcję Port Security, aby dopuszczała jeden lepki adres MAC:

```
interface fa0/1
switchport port-security maximum 1
switchport port-security mac-address sticky
```

Teraz dzieje się magia. Gdy tylko Port Security zobaczy adres MAC, zapisuje go w bieżącej konfiguracji. Można to sprawdzić za pomocą polecenia `show run interface fa0/1`:

```
Switch1#show run interface fa0/1
Building configuration...
```

```
Current configuration : 233 bytes
```

```
!
```

```
interface FastEthernet0/1
switchport mode access
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.7200.3131
End
```

Wykonałeś
to polecenie.

Funkcja Port Security
dodała ten lepki
adres MAC.

Zwróć uwagę, że dwie ostatnie linie konfiguracji interfejsu są prawie identyczne z wyjątkiem adresu MAC. Pierwsza linia to polecenie, które wykonałeś, a druga została dodana przez Port Security.

JEDEN KROK DALEJ Prawdopodobnie zauważyłeś, że polecenie `switchport port-security maximum 1` nie pojawia się w konfiguracji. Nie jest to błąd i nie znaczy, że zrobiłeś coś złego. Czasami IOS zmienia lub usuwa określone polecenia konfiguracji, jeśli są zbędne lub niepotrzebne. Port Security domyślnie dopuszcza tylko jeden adres MAC na port, więc bezpośrednie ustawienie maksimum na 1 jest niepotrzebne.

Teraz dla porównania wpisz polecenie `show port-security address`:

```
Switch1#sh port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0800.7200.3131	SecureSticky	Fa0/1	-

Zwróć uwagę, że typem jest **SecureSticky** i nie ma czasu starzenia się.

```
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Ten sam adres pojawia się tutaj, a kolumna *Remaining Age* jest pusta, ponieważ ów wpis nigdy nie wygaśnie. Dopóki ręcznie nie usuniesz konfiguracji dodanej przez Port Security, ten adres MAC będzie pamiętany.

SPRÓBUJ TERAZ Odłącz fizycznie komputer od portu, na którym skonfigurowałeś lepki adres MAC, i podłącz do niego inne urządzenie. Co się dzieje?

Powinieneś zobaczyć wzorzec podobny do tego:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
2c27.d737.9ad1 on port FastEthernet0/1.
```

Rozłączenie uprawnionego komputera

Podłączenie nieautoryzowanego urządzenia

Port Security blokuje adres MAC nieautoryzowanego urządzenia.

W przypadku prawdziwego ataku hakerskiego intruz może spędzić kilka minut, próbując dowiedzieć się, dlaczego nie może uzyskać dostępu do sieci. Może próbować dostosować ustawienia sieciowe, ponownie uruchomić komputer lub podłączyć się do innego portu. Ważne jest to, że funkcja Port Security udaremnia próbę uzyskania nieautoryzowanego dostępu na zasadzie *plug-and-play*.

Chociaż jest to dobra konfiguracja, ma jedną wadę.

JEDEN KROK DALEJ Adresy MAC można dość łatwo fałszować. Zaawansowany haker może poznać adres MAC autoryzowanego komputera i sklonować go. Nadal

jednak wymaga to czasu. Pamiętaj, że nie chodzi o to, żeby polegać na funkcji Port Security jak na jedynym i ostatecznym zabezpieczeniu. Jej jedynym zadaniem jest utrudnienie atakującemu wykonania jego zadania, czyli wyrządzenia szkód.

5.4.3. Zastrzeżenia dotyczące lepkich adresów MAC

Dodatkowe zabezpieczenie w postaci lepkich adresów MAC wiąże się z pewnym kompromisem. Jeśli kiedykolwiek zajdzie potrzeba zastąpienia urządzenia, będziesz musiał ręcznie wyedytować konfigurację portu, aby usunąć stary adres MAC, a nowy mógł zająć jego miejsce. We wcześniejszym przykładzie funkcja Port Security dodała do bieżącej konfiguracji następującą linię:

```
switchport port-security mac-address sticky 0800.7200.3131
```

Aby to usunąć, trzeba przede wszystkim upewnić się, że ten konkretny adres MAC nie korzysta już z tego portu. Następnie musisz wejść do trybu konfiguracji interfejsu i poprzedzić polecenie słowem kluczowym `no`.

SPRÓBUJ TERAZ Odłącz komputer od portu FastEthernet0/1 lub po prostu zamknij port. Następnie wykonaj poniższe polecenia, aby usunąć lepki adres MAC. Pamiętaj o zmianie adresu MAC w poleceniu, aby odpowiadał Twojej konfiguracji:

```
int fa0/1  
no switchport port-security mac-address sticky 0800.7200.3131
```

Gdy ponownie wpiszesz `show run int fa0/1`, lepki adres MAC powinien zniknąć.

To wszystko! Port Security automatycznie doda do bieżącej konfiguracji następny adres MAC, który zobaczy. Trzeba jeszcze pamiętać o tym, że po zapisaniu lepkich adresów MAC w bieżącej konfiguracji przez funkcję Port Security trzeba ręcznie zapisać konfigurację startową, aby adresy utrzymywały się podczas ponownych uruchomień przełącznika.

5.5. Polecenia omówione w tym rozdziale

Podczas przeglądania listy poleceń w tabeli 5.4 należy pamiętać, że różne porty mogą być skonfigurowane z całkowicie odmiennymi ustawieniami Port Security. To czyni tę funkcję wszechstronną, ale oznacza również, że trzeba indywidualnie sprawdzać konfigurację portu podczas rozwiązywania potencjalnego problemu.

5.6. Laboratorium

Skoro poćwiczyłeś już konfigurowanie funkcji Port Security na kilku portach, jesteś gotowy, aby włączyć Port Security na wszystkich portach użytkowników końcowych. Wystarczy jeden niechroniony port, żeby atak MAC flooding zablokował Twoją sieć.

Wykonując poniższe czynności w celu dokończenia ćwiczeń z laboratorium, pamiętaj, aby użyć polecenia `interface range` do jednoczesnego zastosowania konfiguracji do wielu portów:

Tabela 5.4. Polecenia użyte w tym rozdziale

Polecenie	Tryb konfiguracji	Opis
switchport port-security maximum 5	Interfejsu	Dopuszcza maksymalnie 5 adresów MAC
switchport port-security violation restrict	Interfejsu	Kolejne adresy MAC ponad dopuszczalną liczbę są blokowane
switchport port-security violation shutdown	Interfejsu	Każdy kolejny adres MAC ponad dopuszczalną liczbę uruchamia zamknięcie portu
switchport port-security	Interfejsu	Włącza funkcję Port Security
switchport port-security mac-address sticky	Interfejsu	Zapisuje dopuszczony adres MAC (lub adresy) w bieżącej konfiguracji
show port-security	Nie dotyczy	Wyświetla, na których portach włączona jest funkcja Port Security
show port-security interface fa0/1	Nie dotyczy	Wyświetla szczegółowe informacje o konfiguracji Port Security dla danego portu
show port-security address	Nie dotyczy	Wyświetla dopuszczone adresy MAC według portów
show run interface fa0/1	Nie dotyczy	Wyświetla całą konfigurację poziomu interfejsu dla portu FastEthernet0/1

1. Zaczynaj od skonfigurowania maksymalnej liczby adresów MAC dla każdego portu. Jeśli masz już rozeznanie, ile adresów MAC powinno być na każdym porcie, ustaw to za pomocą polecenia `switchport port-security maximum`. W przeciwnym razie, jeśli nie jesteś pewien, ustaw zachowawczo jakąś wysoką wartość, na przykład 50. Maksymalna liczba adresów MAC dozwolonych dla każdego portu wynosi 3072.
2. Następnie ustaw tryb naruszenia na wszystkich portach na ograniczenie za pomocą polecenia `switchport port-security violation restrict`. Możesz wrócić do tego później i w razie potrzeby zmienić tryb zamknięcie, ale nie zaczynaj od tego.
3. Na koniec włącz funkcję Port Security za pomocą polecenia interfejsu `switchport port-security`. Jeśli zrobiłeś wszystko prawidłowo, nie powinno wydarzyć się nic dramatycznego (chyba że właśnie ktoś przeprowadza na Twoją sieć atak MAC flooding). Aby zweryfikować konfigurację, użyj poleceń `show`, których nauczyłeś się w tym rozdziale.

Skorowidz

A

- access point, 27
- ACE, access control entry, 139
- ACL, access control lists, 137
- adres IP, 37, 38
 - automatyczne żądanie, 128
 - statyczny, 128
 - tranzytowy, 218
- adres MAC, 29, 38
 - docelowy, 31
 - rozgłoszeniowy, 39
 - źródłowy, 31
- adres podsieci, 108
- adresowanie urządzeń, 36
- Aging Time, 88
- ARP
 - odpowiedź, 40
 - żądanie, 40
- ARP, Address Resolution Protocol, 39, 205
- AS, autonomous system, 235
- atak MAC flooding, 80, 81
- automatyczne
 - konfigurowanie VLAN-ów, 167
 - negocjowanie trunku, 157
 - żądanie adresu IP, 128
- autonegocjacja, 74
- awaria
 - sieci, 283
 - łączy, 183, 241

B

- baner logowania, 62
- bezpieczeństwo portów, 90
- bieżąca konfiguracja, 59
- blokowanie ruchu
 - IP – IP, 138
 - IP – podsieć, 144
 - podsieć – podsieć, 148
- brama domyślna, 43, 110, 116
 - konfigurowanie, 221
- bufor rejestrowania, 272
 - konfigurowanie, 272

C

- CCENT, 19, 301
- CCNA, 19, 301
- CDP, Cisco Discovery Protocol, 252
- certyfikacja, 301
- CLI, command-line interface, 49
- CPU, 294
- czas
 - dzierżawy DHCP, 124, 209
 - pingowania, 296
 - pracy systemu, 295
 - starzenia się, aging time, 88

D

- debugowanie, 271, 273
 - DHCP, 275
 - funkcji Port Security, 274
 - routingu IP, 277
 - VTP, 276
- DHCP
 - czas dzierżawy, 124
 - debugowanie, 275
 - konfigurowanie puli, 125
 - konfigurowanie serwera, 122
 - opcje, 124
 - przypisywanie adresów IP, 121
 - tworzenie puli, 131
 - wyłączanie adresów z przypisywania, 126
 - wyświetlanie dzierżaw, 133
- DHCP, Dynamic Host Configuration Protocol, 121
- DNS, Domain Name System, 121
- domeny rozgłoszeniowe, 32, 34
 - adresowanie urządzeń, 36
 - brama domyślna, 43
 - łączenie, 35, 40
 - ograniczenie rozmiaru, 34
 - określanie, 42
- domyślna reguła blokowania, 141
- domyślny VLAN, 98
- dostęp
 - do VLAN-u, 101
 - nieautoryzowany urządzeń, 90
- SSH, 266

DTP, Dynamic Trunking Protocol, 156, 192
 dupleks, 74
 dynamiczny port channel, 193
 dzierżawa DHCP, 133, 209

E

EIGRP, 231
 konfigurowanie, 234
 enkapsulacja, 43
 EPT, Extended Page Tables, 24
 EtherChannel, 191
 EtherChannel Misconfiguration Guard, 197

F

filtrowanie danych wyjściowych, 55, 57
 firewall, 27
 floodowanie, 31
 funkcja
 EtherChannel Misconfiguration Guard, 197
 port channel, 191
 Port Security, 79
 PortFast, 189
 VTP pruning, 173

G

gniazdo, 296
 graficzny interfejs użytkownika, GUI, 49
 grupa portów, 191
 GUI, graphical user interface, 49

I

identyfikacja
 pakietu, 57
 wersji IOS-u, 57
 identyfikator
 OUI, 30
 routerów, 233
 IGP, Interior Gateway Protocol, 231
 interfejs, 66
 routingu, 219
 wiersza poleceń, CLI, 49
 wirtualny, 107, 113
 interfejsy SVI, 113
 konfigurowanie, 114
 tworzenie, 114

inwentaryzacja VLAN-ów, 96
 IOS, Internetwork Operating System, 23,
 49, 140

K

kabel sieciowy, 296
 kanał
 EtherChannel, 191
 trunkowy VLAN, 154
 kapsułkowanie, 43
 pakietu IP, 45
 trunku, 163
 karta sieciowa, 22, 29
 klient
 terminala, 50
 VTP, 170
 kolumna
 NAME, 97
 PORTS, 97
 STATUS, 97
 VLAN, 97
 komunikat
 DHCP Discover, 129
 DHCP Offer, 129
 komutowane interfejsy wirtualne, 107, 113
 konfiguracja
 bieżąca, 59
 globalna, 60
 minimalna Port Security, 80
 router na patyku, 204
 startowa, 62
 konfigurowanie
 bram domyślnych, 221
 bufora rejestrowania, 272
 DTP, 157
 dynamicznego kanału port channel, 193
 EIGRP, 234
 interfejsów pętli zwrotnej, 233
 interfejsów SVI, 114
 łącza trunkowego, 156
 podinterfejsów, 207
 podsieci tranzytowych, 218
 port channel, 192
 przełącznika Switch1, 169
 przełącznika Switch2, 159, 170
 puli DHCP, 125
 serwera DHCP, 122, 133
 syslogu, 280
 urządzeń do żądania adresów, 128
 VLAN-ów, 160

konto użytkownika
 lokalne, 261
 uprzywilejowane, 262
 kontrola
 CPU, 294
 czasów pingowania, 296
 czasu pracy systemu, 295
 elementów sieci, 293
 połączenia fizycznego, 296
 tras IP, 297
 korzystanie z sieci VLAN, 105

L

laboratorium wirtualne, 23
 LACP, Link Aggregation Control Protocol, 193
 lekkie adresy MAC, 91, 93
 linia VTY, 264
 linie danych wyjściowych, 56
 listy kontroli dostępu, ACL, 137, 266
 dla podinterfejsu, 213
 komutowany interfejs wirtualny, 147
 podmienianie, 146
 ruch IP – IP, 138
 ruch IP – podsieć, 144
 ruch podsieć – podsieć, 148
 logowanie się do urządzeń, 50
 lokalne konto użytkownika, 261

Ł

łącza trunkowe
 konfigurowanie, 156
 usuwanie, 221
 łączenie
 domen rozgłoszeniowych, 35
 przełączników, 153
 routerów i przełączników, 203

M

MAC flooding, 80
 MAC, Media Access Control, 29
 maski podsieci, 42, 109
 interfejsów SVI, 114
 wieloznaczne, 145
 metody równoważenia obciążenia, 199

N

NACL, 139
 następny skok, next hop, 224
 nazwa domeny, 124
 NIC, network interface card, 22, 29
 nieautoryzowany dostęp, 90
 nieulotna pamięć RAM, 62, 287
 numery wersji, 58
 NVRAM, 62, 287

O

obszar, area, 243
 odzyskiwanie sprawności, 283
 ponowne uruchamianie urządzeń, 284
 resetowanie hasła, 288
 na przełączniku, 290
 na routerze, 288
 usuwanie konfiguracji startowej, 286
 zawężanie zakresu urządzeń, 284
 ograniczanie dostępu SSH, 266
 ograniczenie, restrict, 84
 floodowania, 35
 okno konfiguracji PuTTY, 51
 omijanie awarii łączy, 241
 opcje DHCP, 124
 optymalizacja wydajności sieci, 191
 OSPF, Open Shortest Path First, 231, 243
 OUI, organizationally unique identifier, 30

P

PAGP, Port Aggregation Protocol, 193
 pakiet, 58
 IP, 45, 47
 pamięć RAM, 62
 parametr starzenia się, 88
 pełny duplex, 74
 pętla
 między mostkami, 180
 zwrotna, 233
 planowanie
 nowego VLAN-u, 98
 ponownego uruchamiania, 285
 platforma VIRL, 23
 podinterfejs, 207
 listy ACL, 213

- podłączanie
 - nowego przełącznika, 154
 - routera do przełącznika, 216
 - routera Router1, 205
 - telefonów IP, 203
- podmienianie list ACL, 146
- podsieci, 42, 108, 124
 - pula DHCP, 222
 - tranzytowe, 218
- podskakiwanie, bouncing, 75, 158
- PoE, Power over Ethernet, 85
- pole
 - Alternatywny serwer DNS, 124
 - Brama domyślna, 110, 124
 - Preferowany serwer DNS, 124
- polecenia debugowania, 273
- polecenie
 - (no) shutdown, 77
 - access-class Management in, 269
 - area 0, 248
 - channel-group 1 mode active, 202
 - channel-group 1 mode on, 202
 - clear logging, 281
 - config, 64
 - config-register 0x2102, 291
 - configure terminal, 64
 - confreg 0x2142, 291
 - copy, 64
 - debug ip routing, 281
 - debug port-security, 281
 - debug sw-vlan vtp, 281
 - default-router, 136
 - delete nvram:startup-config, 291
 - deny ip host, 152
 - dns-server, 136
 - domain-name, 136
 - duplex full/half/auto, 77
 - encapsulation dot1Q 600, 214
 - exit, 106
 - interface loopback0, 248
 - interface range, 70, 77, 202
 - interface vlan 600, 119
 - ip access-group 150 in, 152
 - ip access-list extended 150, 152
 - ip address, 119
 - ip dhcp excluded-address, 136
 - ip dhcp pool MoL, 136
 - ip helper-address, 134, 136
 - ip route profile, 299
 - ip routing, 119, 229
 - ipconfig /all, 132
 - lease, 136
 - line vty 0 4, 269
 - logging buffered 8192, 281
 - logging buffered debugging, 281
 - logging buffered warnings, 281
 - logging host, 281
 - logging trap debugging, 281
 - name Executives, 106
 - network, 136
 - no, 63
 - no interface port-channel 1, 202
 - no switchport, 229
 - permit ip, 152
 - permit ip any any, 152
 - port-channel load-balance src-mac, 202
 - reload, 64, 281
 - reload cancel, 291
 - reload in 15, 291
 - router eigrp 7, 248
 - router ospf 1, 248
 - show arp, 259
 - show cdp neighbors, 259
 - show etherchannel load-balance, 202
 - show etherchannel summary, 202
 - show interfaces counters errors, 299
 - show interfaces pruning, 178
 - show interfaces status, 77
 - show interfaces trunk, 165, 178
 - show ip dhcp binding, 136
 - show ip eigrp neighbor, 248
 - show ip interface, 229
 - show ip ospf neighbor, 248
 - show ip protocols, 248
 - show ip route, 119, 214, 299
 - show ip route profile, 299
 - show logging, 281
 - show mac address-table, 259
 - show port-security, 94
 - show port-security address, 94
 - show processes cpu history, 299
 - show run interface, 94
 - show run interface fa0/2, 77
 - show running-config, 64
 - show spanning-tree vlan 700, 190
 - show startup-config, 64
 - show users, 269
 - show version, 64, 299
 - show vlan brief, 106
 - show vlans 600, 214

- show vtp status, 178
- spanning-tree etherchannel guard
 - misconfig, 202
- spanning-tree mode rapid-pvst, 190
- spanning-tree portfast, 190
- speed, 77
- ssh, 269
- switchport access vlan 700, 106
- switchport mode access, 106
- switchport mode trunk, 165
- switchport port-security, 94
- switchport port-security mac-address sticky, 94
- switchport port-security maximum 5, 94
- switchport port-security violation restrict, 94
- switchport port-security violation shutdown, 94
- switchport trunk encapsulation dot1q, 165
- switchport voice vlan, 106
- telnet, 165
- traceroute, 251, 255, 259
- transport input ssh, 269
- undebg all, 281
- username ben privilege 15 secret cisco, 269
- vlan 700, 106
- vtp mode client, 178
- vtp mode server, 178
- vtp password MoL, 178
- vtp pruning, 178
- ponowne uruchamianie urządzeń, 284, 291
- port
 - channel, 191
 - dynamiczny, 193
 - konfigurowanie dynamicznego kanału, 193
 - statyczny, 192
 - tworzenie statycznego kanału, 197
- Port Security, 79
 - Aging Time, 88
 - blokowanie urządzeń, 90
 - debugowanie funkcji, 274
 - maksymalne bezpieczeństwo portów, 90
 - minimalna konfiguracja, 80
 - poziomy zabezpieczeń, 80
 - przenoszenie urządzeń, 86
 - testowanie funkcji, 85
 - zapobieganie atakom MAC flooding, 80
- PortFast, 188
- porty
 - autonegociacja, 74
 - dostępu do wielu VLAN-ów, 105
 - dupleks, 74
 - ethernetowe, 65
 - konsoli, 267
 - maksymalne bezpieczeństwo, 90
 - przełączników, 65
 - sprawdzanie konfiguracji, 101
 - sprawdzanie statusu, 66
 - stan
 - administracyjnie zamknięty, administratively down, 68
 - wyłączony, disabled, 68
 - zamknięty, shutdown, 68
 - status
 - connected, podłączony, 67
 - disabled, wyłączony, 67
 - notconnect, niepodłączony, 67
 - statycznego dostępu, 101
 - włączanie, 68
 - wyłączanie, 71
 - zabezpieczanie, 79
 - zmiana duplexu, 76
 - zmiana prędkości, 73, 75
- powiadomienia, notifications, 279
- poziomy ważności rejestrowania, 278
- półdupleks, 74
- prędkość portu, 73, 75
- problemy z łącznością, 302
- procesor, 294
- profilowanie tablicy tras, 298
- protokoły routingu dynamicznego, 231
- protokół
 - ARP, 39, 205
 - CDP, 252
 - DHCP, 121
 - DTP, 156, 192
 - EIGRP, 231
 - IGP, 231
 - IP, 37
 - LACP, 193
 - OSPF, 231, 243
 - PAGP, 193
 - Rapid Spanning Tree, 186
 - Spanning Tree, 180, 191
 - VTP, 167, 276
- przeglądanie bieżącej konfiguracji, 59
- przekazanie pakietu IP, 47

przełącznik, switch, 27
 połączenia fizyczne, 153, 154
 przenoszenie urządzeń, 162
 Switch1, 169
 Switch2, 159, 170
 zarządzanie portami, 65
 przenoszenie urządzeń, 86, 162
 przerywanie, break, 31, 288
 przyleganie, adjacency, 238
 przypisywanie tranzytowych adresów IP, 121
 do interfejsów fizycznych, 218
 do podinterfejsów i interfejsów SVI, 220
 PSTN, 203
 pula DHCP
 dla podsieci, 222
 punkty dostępu bezprzewodowego, 27
 PuTTY, 51

R

ramka ethernetowa, 31
 Rapid Spanning Tree, 186
 regex, 57
 reguły
 ACL, 137
 IOS, 140
 rejestrowanie, 271
 poziomy ważności, 278
 rekonfiguracja linii VTY, 264
 relacja przylegania, 238
 resetowanie hasła, 288, 291
 na przełączniku, 290
 na routerze, 288
 router, 27, 28
 kapsułkowanie pakietu IP, 45
 łączenie domen rozgłoszeniowych, 40
 router na patyku, 204
 topologia fizyczna, 216
 routing
 dynamiczny, 231
 IP, 44, 113, 211
 debugowanie, 277
 między podsieciami, 222, 228
 w sieci rozległej, 204
 rozgłoszeniowy adres MAC, 39
 rozmiar domeny rozgłoszeniowej, 34
 rozszerzona lista dostępu IP, 139
 równoważenie obciążenia, 199

ruch
 IP – IP, 138
 IP – podsieć, 144
 podsieć – podsieć, 148

S

scenariusze śledzenia urządzeń, 249
 serwer
 DNS, 121
 syslogu, 280
 VTP, 169
 sieci
 zwiększanie poziomu skalowalności, 203
 sieć Cisco, 27
 skalowalność, 243
 sieci, 203
 słowo kluczowe exclude, 57
 Spanning Tree, 180
 awarie łączy, 183
 sprawdzanie
 konfiguracji portów, 101
 połączeń VLAN, 118
 SSH, 264
 status portu, 66
 connected, 67
 disabled, 67
 notconnect, 67
 statyczne adresy IP, 128
 statyczny port channel, 192
 sticky MAC addresses, 91
 STP, Spanning Tree, 191
 SVI, switched virtual interfaces, 113
 switch, *Patrz* przełącznik, 27
 switchport mode dynamic desirable, 165
 system
 autonomiczny, AS, 235
 IOS, 49
 operacyjny IOS, 49
 operacyjny NX-OS, 26

Ś

śledzenie
 drukarki sieciowej, 251
 serwera, 254
 urządzeń, 249
 do ostatniego skoku, 249–251, 255
 etapy, 250
 środowisko laboratoryjne, 22, 24

T

tablica
 adresów MAC, 34, 80, 82, 253, 256
 routing, 211, 215, 298
 technologia zasilania PoE, 85
 telefonia VoIP, 104
 testowanie
 funkcji Port Security, 85
 konta, 262
 traceroute, 251, 255
 trasowanie IP, 44, 297
 tryb
 konfiguracji globalnej, 60
 konfiguracyjny, 51
 ROMMON, 288
 uprzywilejowany, 51
 tryby naruszenia
 ograniczenie, 84
 zamknięcie, 84
 trzepotanie, flapping, 75
 tworzenie
 interfejsów SVI, 114
 listy dostępu, 139
 nowych VLAN-ów, 171
 puli DHCP, 131, 222
 statycznego kanału port channel, 197
 uprzywilejowanego konta użytkownika,
 262
 VLAN-ów, 99

U

uprzywilejowane konto użytkownika, 262
 urządzenia Cisco
 zabezpieczenia, 261
 ustawianie trybu dostępu, 103
 ustawienia sieciowe komputera, 123
 usuwanie
 konfiguracji startowej, 286, 291
 łącza trunkowego, 221
 uzyskiwanie adresu
 IP, 250
 MAC, 250, 253, 256

V

VIRL, Virtual Internet Routing Lab, 23, 302
 VLAN, virtual LAN, 95
 automatyczne konfigurowanie, 167

domyślny, 98
 głosowy, 104
 inwentaryzacja, 96
 konfigurowanie, 160
 lokalna bazie danych, 96
 łącza trunkowe, 155
 planowanie, 98
 podsieci, 108
 przekraczanie bariery, 107
 przypisywanie do portów, 101
 pula DHCP, 129
 sprawdzanie połączeń, 118
 tworzenie, 99, 171
 ustawianie trybu dostępu, 101, 103
 VoIP, Voice over IP, 104
 VPN, virtual private network, 215
 VTP, VLAN Trunking Protocol, 167, 276
 debugowanie, 276
 pruning, 173, 174

W

WAN, wide area network, 204
 wersje IOS-u Cisco, 24
 wiązania, bindings, 133
 wiązka, bundle, 191
 wirtualizacja, 24
 virtualne
 interfejsy komutowane, 107, 113
 laboratorium, 24
 podsieci, 108
 sieci LAN, *Patrz* VLAN
 sieci prywatne, VPN, 215
 włączanie
 funkcji VTP pruning, 173
 portów, 68
 routingu IP, 113
 SSH, 264
 wpis kontroli dostępu, ACE, 139
 wybieranie
 najlepszej ścieżki, 239
 środowiska laboratoryjnego, 22
 wyczerpanie DHCP, 124
 wydajność sieci, 191
 wykluczanie linii, 57
 wyłączanie
 adresów z przypisywania, 126
 portów, 71
 wyrażenia regularne, 57
 wyszukiwanie nieużywanych interfejsów, 71

wyświetlanie
dzierżaw DHCP, 133
tablicy adresów MAC, 253, 256

Z

zabezpieczanie
portów, 79
portu konsoli, 267
urządzeń Cisco, 261
zalewanie, 31
urządzeń ramką ethernetową, 32
załączanie linii, 55
zamknięcie, shutdown, 84
zamykanie bram floodowania, 34
zapisywanie konfiguracji startowej, 62
zapominanie adresów MAC, 88

zarządzanie
portami przełączników, 65
przełącznikami, 46
routerami, 46
wirtualnymi sieciami LAN, 95
zastosowanie listy ACL, 142
zmiana
bieżącej konfiguracji, 60
dupleksu, 76
kapsułkowania trunku, 163
prędkości portu, 73, 75
znak
kratki, 62
potoku, 55
zapytania, 61

Ż

żądanie
adresu IP, 128
ARP, 39

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA



Helion SA

SIECI CISCO — NIEZAWODNE ROZWIĄZANIA!

Routery i przełączniki Cisco stały się synonimem niezawodnych technologii sieciowych. Miliony sieci na całym świecie działają dzięki tym urządzeniom. Niestety, jeśli sieć oparta na technologii Cisco ma być bezpieczna i bezawaryjna, wymaga od administratora wiedzy i zaangażowania. Tymczasem sieci komputerowe są jedną z najtrudniejszych koncepcji w informatyce. Poziom złożoności tego zagadnienia bywa przytłaczający, a dotychczas wydawane książki o sieciach są zbyt akademickie i teoretyczne. W żaden sposób nie ułatwiają przyswojenia praktycznych umiejętności.

Jeśli chcesz nauczyć się administrowania siecią Cisco, ale zniechęcają Cię nieprzystępne podręczniki, to trzymasz w ręku właściwą książkę. Bez zbędnej teorii zaczniesz wykonywać konkretne zadania. Podczas ćwiczeń poznasz różne pojęcia i zobaczysz, jak nabierają sensu. Dowiesz się, jak zaimplementować struktury i układy interfejsu użytkownika. Poznasz architekturę MVVM i nauczysz się implementować ją w swoich aplikacjach. Zrozumiesz trudniejsze zagadnienia, na przykład włączanie do aplikacji funkcji specyficznych dla danej platformy mobilnej, współpraca z usługami Microsoft Azure App oraz obsługa zewnętrznych bibliotek, takich jak Razor. Ile czasu będziesz potrzebować? Wystarczą przerwy obiadowe na przestrzeni jednego miesiąca!

W książce między innymi:

- podstawowe pojęcia: ramki, domeny rozgłoszeniowe, MAC, protokoły
- system IOS i zarządzanie przełącznikami
- LAN-y, VLAN-y i wirtualne interfejsy
- zarządzanie serwerem DHCP
- zapewnianie bezpieczeństwa sieci
- rozwiązywanie problemów i przywracanie pracy po awarii

BEN PIPER jest inżynierem systemów informatycznych, praktykującym konsultantem IT i autorem książek o sieciach komputerowych. Posiada liczne certyfikaty firm Cisco, Citrix i Microsoft, w tym CCNA i CCNP Cisco. Jest autorem ponad 17 kursów w serwisie Pluralsight. Koncentruje się na zarządzaniu sieciami, certyfikacji CCNP Cisco oraz administrowaniu serwerami Windows.

		Sprawdź nasze szkolenia!		KOD KORZYŚCI Sięgnij po więcej! ▶					
	hellon.pl	 AKADEMIA IT & BUSINESS WWW.SZKOLENIA.HELION.PL		ISBN 978-83-283-3971-2					
	0 801 339900								
	0 601 339900								
INFORMATYKA W NAJLEPSZYM WYDANIU				Cena: 69,00 zł					