

Spis treści

Przedmowa	11
Podziękowania	13
O tej książce	15
O autorze	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. Filtrowanie danych wyjściowych	55
3.4. Identyfikacja wersji IOS-u oraz pakietu	57
3.4.1. Numery wersji	58
3.4.2. Pakiety	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. Polecenie interface range	70
4.3. Wyłączanie portów	71
4.3.1. Wyszukiwanie nieużywanych interfejsów	71
4.4. Zmiana prędkości portu oraz duplexu	73
4.4.1. Prędkość	73
4.4.2. Dupleks	74
4.4.3. Autonegocjacja	74
4.4.4. Zmiana prędkości portu	75
4.4.5. Zmiana duplexu	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. Zapobieganie atakom MAC flooding	80
5.1.2. Tryby naruszenia	84
5.2. Testowanie funkcji Port Security	85
5.3. Jak sobie radzić z przenoszeniem urządzeń	86
5.3.1. Port Security nigdy nie zapomina!	86
5.3.2. Czas starzenia się	88
5.4. Uniemożliwianie dostępu nieautoryzowanym urządzeniom	90
5.4.1. Zapewnienie maksymalnego bezpieczeństwa portów	90
5.4.2. Lepkie adresy MAC	91
5.4.3. Zastrzeżenia dotyczące lepkich adresów MAC	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 ip helper-address	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 SVT	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. Siedzenie 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. Siedzenie 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
20.3. 20.2.1. Planowanie ponownego uruchamiania	285

20.4. Usuwanie konfiguracji startowej	286
20.5. 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

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