# SIECI CISCO W MIESIĄC

## PODRĘCZNIK ADMINISTRATORA


BEN PIPER

MANNING

Helion

Tytuł oryginału: Learn Cisco Network Administration

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-3971-2



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.

# Spis treści

# 5 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 odległych 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 określę konkretne zagrożenia, przed którymi może chronić funkcja Port Security,

żebyś mógł samodzielnie zadecydować, 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 pomaga chronić każdy poziom zabezpieczeń Port Security. Zacznijmy 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

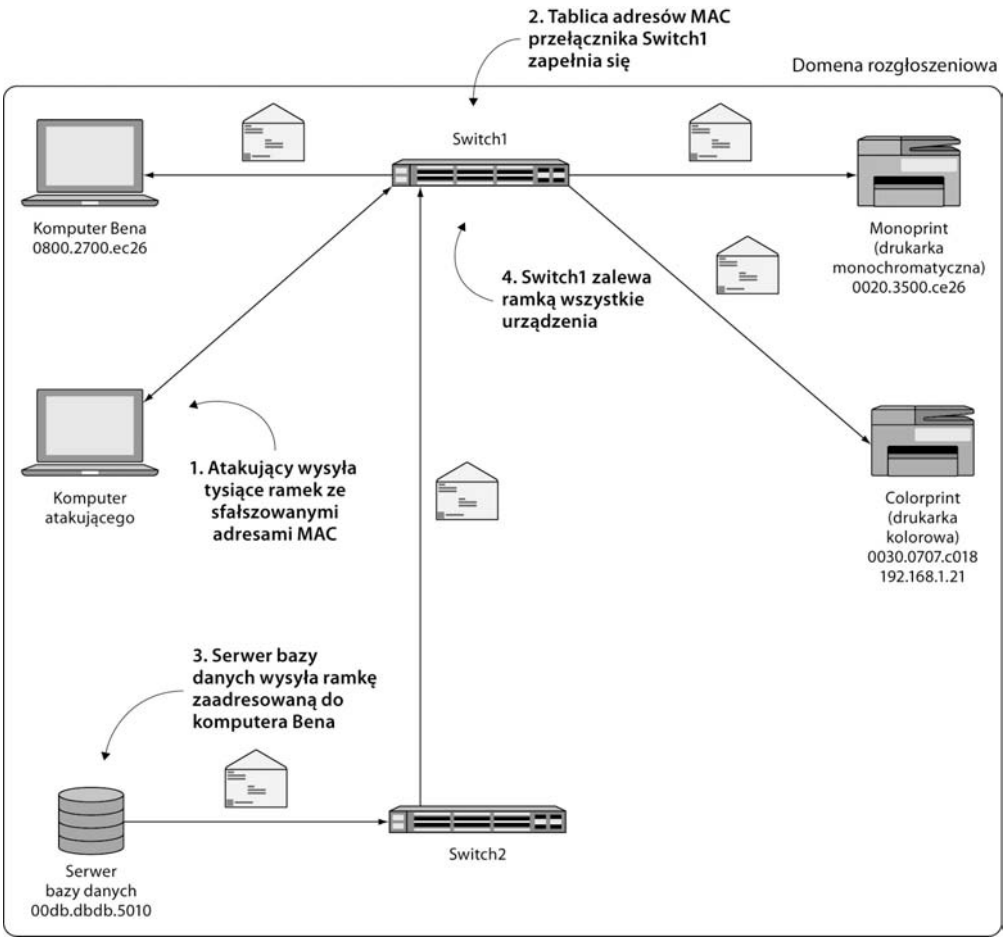
Przypomnijmy z rozdziału 2., że przełącznik utrzymuje tablicę adresów MAC zawierającą adres MAC każdego urządzenia oraz port, do którego dane urządzenie jest podłączone. Tabela 5.2 jest przykładem typu informacji, jakie można znaleźć w tablicy adresów MAC. Dzięki śledzeniu lokalizacji każdego urządzenia 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 pozornie 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 (podsłuchiwaczem) 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 wysyła do przełącznika Switch1 tysiące ramek ze sfałszowanymi źródłowymi adresami MAC. W kroku 2. zapełnia się tablica adresów MAC przełącznika Switch1. W kroku 3. serwer bazy danych wysyła 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 `MaxSecure Addr` (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 ona 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 podpina 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 jakiejkolwiek 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 zestarzały 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
Aging Type                 : Absolute
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
```

**Czas starzenia się ustawiony na 10 minut.**

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

**To urządzenie nie zostało zamienione i starzeje się niezależnie od pozostałych adresów.**

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.

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

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

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. Zacznij 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 `switch ↪port 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*

## E



## F



## G



## I



## K

## L



## Ł



## M



## N



## O



## P

## R



## S



## Ś

## T



## U



## V



## W

## Z



## Ż

## 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.



ISBN 978-83-283-3971-2
9 788328 339712