Konfiguracja Port Security na przełącznikach Cisco

Port Security to funkcja przełącznika Cisco, która pozwala na kontrolowanie dostępu do portów przełącznika poprzez ograniczenie liczby urządzeń, które mogą się do nich podłączyć. Dzięki tej funkcji można także ograniczyć dostęp do portów tylko dla wybranych urządzeń na podstawie adresów MAC. Port Security jest często stosowany w celu zwiększenia bezpieczeństwa sieci lokalnych.

1. Zasady działania Port Security

Port Security umożliwia przełącznikowi wykrycie nieautoryzowanego urządzenia podłączającego się do portu i odpowiednią reakcję na to zdarzenie. Konfigurując tę funkcję, można ustawić:

• Maksymalną liczbę adresów MAC dozwoloną na porcie.

• Statyczne lub dynamiczne przypisanie adresów MAC.

• Działania podejmowane po naruszeniu zasad bezpieczeństwa.

2. Typy naruszeń (Violation Modes)

Cisco oferuje trzy tryby reakcji na naruszenia zasad bezpieczeństwa na porcie:

1. Protect – odrzuca ruch z adresów MAC, które przekraczają maksymalną dozwoloną liczbę, bez wyłączania portu i bez logowania zdarzenia.

2. Restrict – odrzuca ruch z adresów przekraczających limit, ale loguje zdarzenia naruszenia i zwiększa licznik naruszeń.

3. Shutdown – domyślny tryb naruszenia; port zostaje wyłączony (w stan „error-disabled”) i wymaga ręcznego lub automatycznego resetu.

3. Konfiguracja Port Security

Poniżej przedstawiono kroki do konfiguracji Port Security:

Krok 1: Przejdź do trybu konfiguracji portu

```
Switch# configure terminal
Switch(config)# interface FastEthernet0/1
```

Krok 2: Włącz Port Security

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

Krok 3: Ustaw maksymalną liczbę adresów MAC

```
Switch(config-if)# switchport port-security maximum 2
```

Krok 4: Skonfiguruj adresy MAC

```
Switch(config-if)# switchport port-security mac-address 00AA.BBCC.DDEE

Wybierz, czy adresy MAC mają być ustawione dynamicznie, czy statycznie.
```

Krok 5: Ustawienie trybu naruszenia (Violation Mode)

```
Switch(config-if)# switchport port-security violation shutdown

Alternatywnie:
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security violation protect
```

Krok 6: Wyświetlanie informacji o konfiguracji Port Security

```
Switch# show port-security interface FastEthernet0/1
Switch# show port-security
```

4. Przykład konfiguracji

```
Switch# configure terminal
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address 00AA.BBCC.DDEE
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# end
```

5. Najlepsze praktyki

Dostosuj maksymalną liczbę adresów MAC odpowiednio do potrzeb – ogranicz do jednego, jeśli oczekujesz tylko jednego urządzenia. Używaj trybu restrict lub protect w środowiskach produkcyjnych, aby unikać przypadkowego wyłączenia portów. Regularnie monitoruj stan portów i zdarzenia naruszeń, aby upewnić się, że sieć działa bezpiecznie.