Kontrola transmisji portów sieciowych

Port Security

- funkcjonalność bezpieczeństwa portu (Port Security) pozwala na ograniczenie dostępu do portu przełącznika, poprzez ograniczenie liczby adresów oraz/lub zweryfikowanie adresów fizycznych MAC, mogących podłączyć się do danego portu
- wskazanie bezpiecznych adresów MAC portu, uniemożliwi prawidłową transmisję urządzeniom prezentującym się, innymi od zdefiniowanych, źródłowymi adresami fizycznymi
- w zależności od źródła pozyskania wartości bezpiecznej adresacji fizycznej, rozróżnia się trzy typy bezpiecznych adresów MAC:
  - statyczne (Static)
  - dynamiczne (Dynamic)
  - przyczepne (Sticky)

⇘ porty przełącznika, dla których będzie uruchamiana funkcjonalność, muszą znajdować się w trybie dostępowym (mode access)

Port Security

- **statyczne wpisy MAC** (Secure Static MAC address)
  - statyczny adres skonfigurowany manualnie, przechowywany w pliku konfiguracji bieżącej, startowej oraz w tablicy przełączania
  - wpis permanentny
- **dynamiczne wpisy MAC** (Secure Dynamic MAC address)
  - adres dodawany dynamicznie według kolejności ogłaszania swojej obecności w ramach portu
  - w wyniku poznania adresu MAC dodawany jest wpis statyczny w tablicy przełączania, który zerowany jest po ponownym uruchomieniu urządzenia oraz w sytuacjach dezaktywacji portu,
  - brak możliwości zachowania bezpiecznego adresu MAC

Port Security

- **przyczepne wpisy MAC** (Secure Sticky MAC address)
  - adres dodawany dynamicznie według kolejności ogłaszania swojej obecności w ramach portu
  - w wyniku poznania adresu MAC, dodawany jest wpis statyczny w tablicy przełączania oraz wpis w konfiguracji bieżącej (po zapisaniu także startowej)
  - wpis zerowany jest po ponownym uruchomieniu urządzenia
  - zapisanie konfiguracji przed ponownym uruchomieniem zapewnia zachowanie wpisów z adresami MAC -> wpis permanentny

- naruszenie określonych zasad bezpieczeństwa ma miejsce w sytuacjach:
  - próby dodania do tablicy przełączania większej (od zadeklarowanej) liczby dopuszczalnych adresów fizycznych MAC
  - wykrycia tego samego adresu, który został nauczony dynamicznie lub był wpisany statycznie, w ramach innego portu tej samej sieci wirtualnej VLAN

Port Security

- w stosunku do portu, który naruszył zasady bezpieczeństwa, mogą zostać podjęte następujące akcje:
  - **protekcja portu (protect)** –> w sytuacji, gdy liczba bezpiecznych adresów osiągnęła wartość maksymalną, ramki z nieznaną adresacją źródłową będą odrzucane do momentu powiększenia maksymalnej liczby adresów dopuszczalnych w ramach portu lub usunięcia bieżących wpisów statycznych -> brak powiadomienia administracyjnego o złamaniu zasad bezpieczeństwa

Port Security

- w stosunku do portu który naruszył zasady bezpieczeństwa, mogą zostać podjęte następujące kroki:
  - **ograniczenie portu (restrict)** –> w sytuacji, gdy liczba bezpiecznych adresów osiągnęła wartość maksymalną zadeklarowaną dla portu, ramki z nieznaną adresacją źródłową będą odrzucane do momentu powiększenia maksymalnej liczby adresów dopuszczalnych w ramach portu lub usunięcia bieżących wpisów statycznych -> naruszenie zasad bezpieczeństwa generuje pułapkę SNMP, wiadomość dla dziennika zdarzeń (Syslog) oraz inkrementuje licznik statystyk
  - **wyłączenie portu (shutdown)** -> naruszenie zasad bezpieczeństwa portu wymusza wyłączenie portu poprzez przejście w stan error-disabled -> inkrementowany jest licznik statystyk, generowana jest pułapka SNMP oraz wiadomość dla dziennika zdarzeń (Syslog); opcja domyślna

Port Security

- zestawienie składowych akcji, które mogą zostać podjęte, w stosunku do portu który naruszył zasady bezpieczeństwa warstwy 2 modelu ISO/OSI

Typ	Protect	Restrict	Shutdown
Transmisja	-	-	-
Pułapka SNMP	-	tak	tak
Dziennik zdarzeń	-	tak	tak
Licznik statystyk	-	tak	tak
Wyłączenie portu	-	-	tak

⇘ prawidłowe funkcjonowanie protokołu SNMP oraz dziennika zdarzeń (Syslog), wymaga prawidłowej konfiguracji serwisów w/w mechanizmów

Port Security

- uruchomienie funkcjonalności portu bezpiecznego w ramach interfejsu sieciowego

```
(config-if)# switchport  port-security
```

- określenie polityki, w stosunku do portu, który naruszył zasady bezpieczeństwa

```
(config-if)# switchport  port-security  violation  {  protect  |  restrict  |  shutdown  }
```

✓ protect	konfiguracja akcji protekcji portu
✓ restrict	konfiguracja akcji ograniczenia portu
✓ shutdown	konfiguracja akcji wyłączenia portu, wartość domyślna

Port Security

- określenie maksymalnej dopuszczalnej liczby adresów MAC, mogących pracować w ramach portu

```
(config-if)# switchport  port-security  maximum  max_mac
```

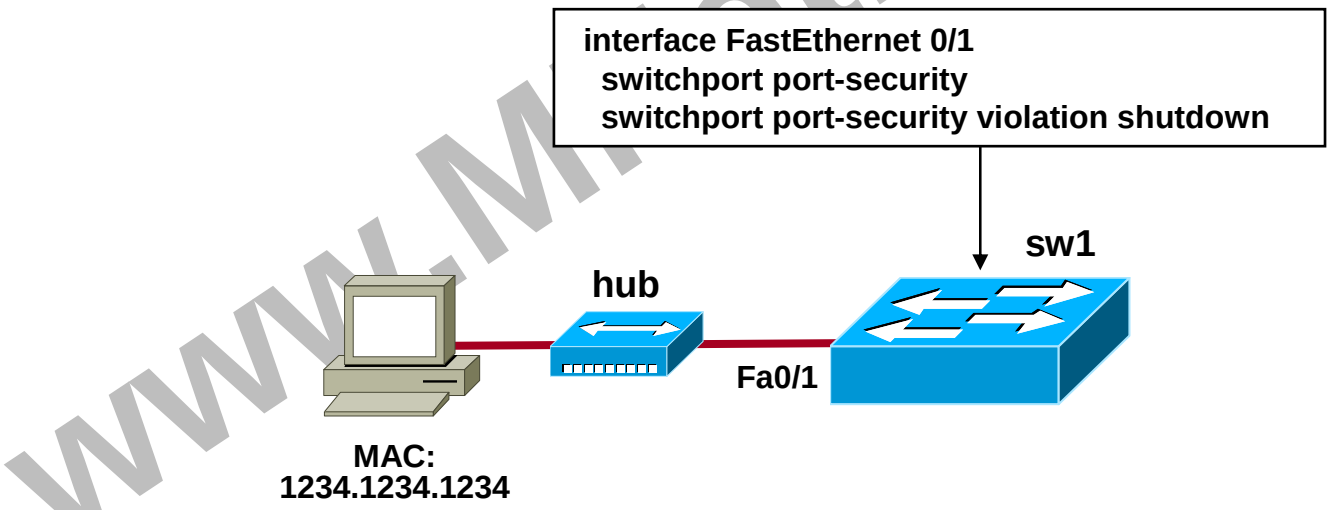
- wyświetlenie podstawowej konfiguracji portów bezpiecznych

```
# show  port-security  [ address ]  [  interface  intf_type number  ]
```

✓ *max_mac*	maksymalna liczba adresów fizycznych, których przekroczenie spowoduje naruszenie zasad bezpieczeństwa portu, zakres: 1 – 132 adresów fizycznych, domyślnie 1
✓ *intf_type number*	odwołanie do interfejsu fizycznego
✓ address	wyświetlenie bezpiecznych adresów MAC

Port Security

• dla podanego poniżej przykładu interfejsu Fa0/1, włączona zostaje funkcjonalność portów bezpiecznych oraz określona zostaje polityka w przypadku naruszenia zasad bezpieczeństwa -> wyłączenie interfejsu (tryb err-disabled)



⇘ violation shutdown – to opcja domyślna, z tego powodu może nie być widoczna w konfiguracji przełącznika

Port Security

```
sw1#show port-security interface FastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 1234.1234.1234
Security Violation Count   : 0
```

- przykład weryfikacji funkcjonalności bezpiecznych portów
- funkcjonalność włączona na interfejsie Fa0/1 oraz wyłączona na Fa0/2

```
sw1#sho port-security interface FastEthernet 0/2
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 1212.1212.1212
Security Violation Count   : 0
```

Port Security

- w tablicy przełączania, automatycznie dodany zostanie wpis statyczny, reprezentujący bezpieczny adres
- wpis adresu MAC będzie obowiązywał do czasu:
  - wyłączenia administracyjnego portu
  - ponownego uruchomienia przełącznika
  - wyłączenia bezpośredniego połączenia do portu, przykładowo poprzez wyłączenie podłączonego komputera lub urządzenia aktywnego
  - manualnego wyczyszczenia portów bezpiecznych

```
sw1#show mac-address-table interface FastEthernet 0/1
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1       1234.1234.1234    STATIC      Fa0/1
Total Mac Addresses for this criterion: 1
```

```
sw1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)        (Count)
---------------------------------------------------------------------------
  Fa0/1          1              1              0              Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024

sw1#show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------
Vlan    Mac Address    Type            Ports    Remaining Age
                                                    (mins)
----    -----------    ---             -----    -------------
1    1234.1234.1234    SecureDynamic   Fa0/1        -
-----------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
sw1#
```

Port Security

- przykład weryfikacji funkcjonalności bezpiecznych portów w trybie wyłączenia portu

Port Security

- wyczyszczenie bezpiecznego adresu nauczonego dynamicznie

```
# clear  port-security  dynamic  [ address  hhhh.hhhh.hhhh.hhhh  ]
```

- wyczyszczenie bezpiecznych adresów nauczonych dynamicznie w ramach określonego portu

```
# clear  port-security  dynamic  [  interface  intf_type number  ]
```


✓ *intf_type number*	odwołanie do interfejsu fizycznego
✓ *hhhh.hhhh.hhhh*	wartość bezpiecznego adresu fizycznego

Port Security

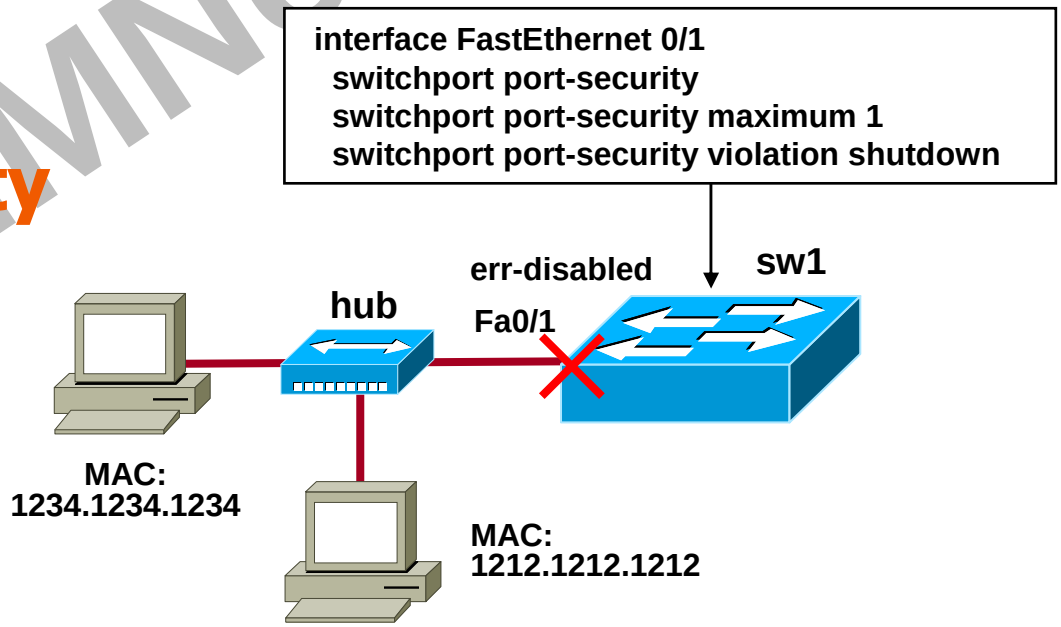
```
sw1#sho port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports     Remaining Age
                                                        (mins)
----    -----------       ----              -----     -------------
   1    000f.8f12.7a86    SecureDynamic     Fa0/24        -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024

sw1#clear port-security dynamic address 000f.8f12.7a86
sw1#clear port-security dynamic interface FastEthernet 0/24
sw1#
sw1#sho port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type              Ports     Remaining Age
                                                        (mins)
----    -----------       ----              -----     -------------
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- przykład manualnego czyszczenia wartości bezpiecznych adresów MAC

Port Security

- domyślnie maksymalna liczba dopuszczalnych bezpiecznych adresów MAC dla każdego interfejsu wynosi 1
- podłączenie drugiego użytkownika do połączenia interfejsu Fa0/1, spowoduje złamanie założeń bezpieczeństwa portu i wyłączenie interfejsu z powodu wykrytego błędu (err-disabled)
- powyższa sytuacja uniemożliwi transmisję wszystkim podłączonym do tego portu urządzeniom



- ponowna aktywacja interfejsu wymaga jego wyłączenia (shutdown) oraz ponownego uruchomienia (no shutdown)
- warunkiem prawidłowej aktywacji, jest pozytywne spełnienie nałożonych warunków bezpieczeństwa -> w naszym przypadku będzie to usunięcie kolejno przyłączonego węzła lub zwiększenie dopuszczalnej liczby bezpiecznych MAC adresów

```
sw1#
12:20:11: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting
Fa0/1 in err-disable state
sw1#
12:20:11: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 1212.1212.1212 on port FastEthernet0/1.
sw1#
12:20:12: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
sw1#
12:20:13: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
sw1#sho int fa0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 000d.bd12.9b41 (bia 000d.bd12.9b41)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
                    ....
```

Port Security

```
sw1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)       (Count)
---------------------------------------------------------------------------
  Fa0/1            1             0             1              Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024

sw1#
```

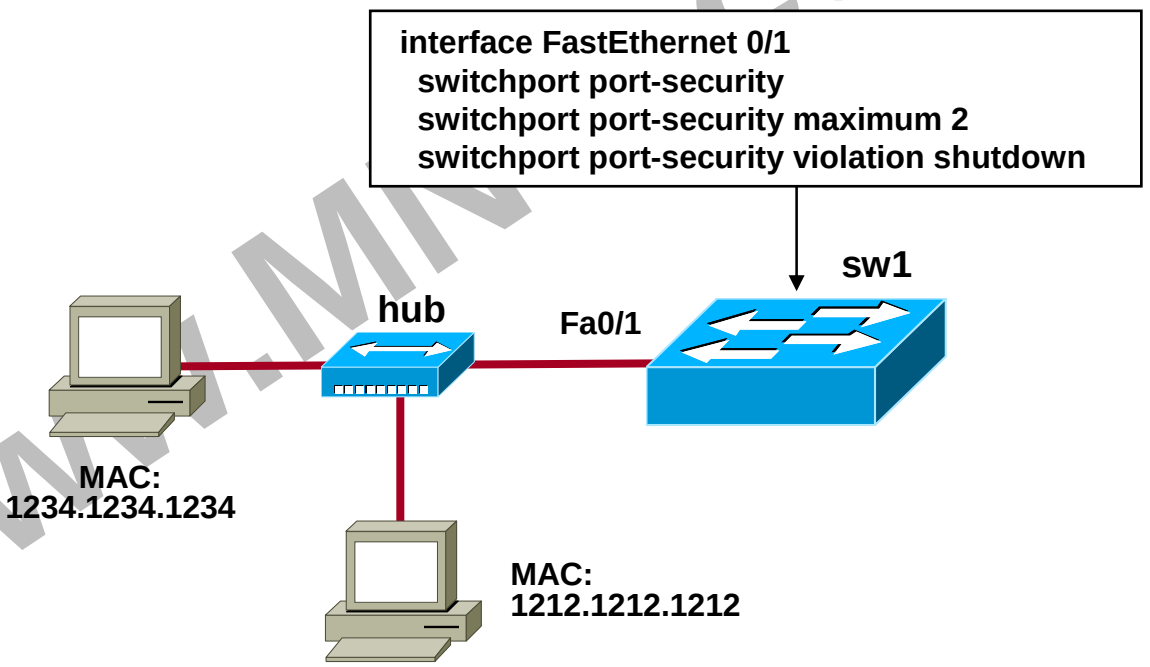
Port Security

- ponieważ złamanie założeń bezpieczeństwa portu, wprowadza interfejs w stan wyłączenia (err-disbled), z tablicy przełączania oraz tablicy bezpiecznych portów usuwane są odpowiednie wpisy MAC
- inkrementowany jest jednocześnie licznik założeń bezpieczeństwa (Security Violation)

```
sw1#show port-security interface FastEthernet 0/1
Port Security                : Enabled
Port Status                  : Secure-shutdown
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address          : 1212.1212.1212
Security Violation Count     : 1
```

Port Security

- przykład konfiguracji bezpiecznych portów dla dwóch urządzeń dołączonych do jednego interfejsu przełącznika



Port Security

- sposobem automatycznego wyprowadzenia interfejsu ze stanu błędu (err-disbled) jest zastosowanie mechanizmu odzyskiwania portów
- warunkiem prawidłowej aktywacji, jest pozytywne spełnienie nałożonych warunków bezpieczeństwa
- uruchomienie mechanizmu odzyskiwania portów ze stanu błędu, którego źródłem jest polityka bezpieczeństwa

```
(config)# errdisable  recovery  cause  psecure-violation
```

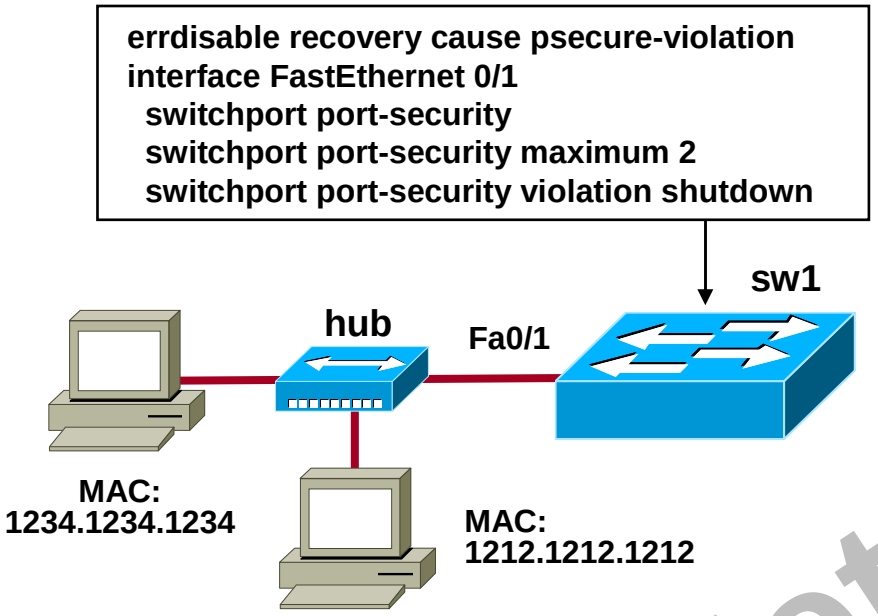
- mechanizm w odstępach 5 minutowych (domyślnie) będzie próbował aktywować interfejs
- modyfikacja czasu kolejnych prób odzyskania portu

```
(config)# errdisable  recovery  interval  recovery_sec
```

✓ *recovery_sec* — czasookres prób odzyskania transmisji dla portu w stanie błędu, zakres: 30 – 86400 sekund, domyślnie: 300 sekund

⇘ polecenie dotyczy wszystkich interfejsów sieciowych

Port Security

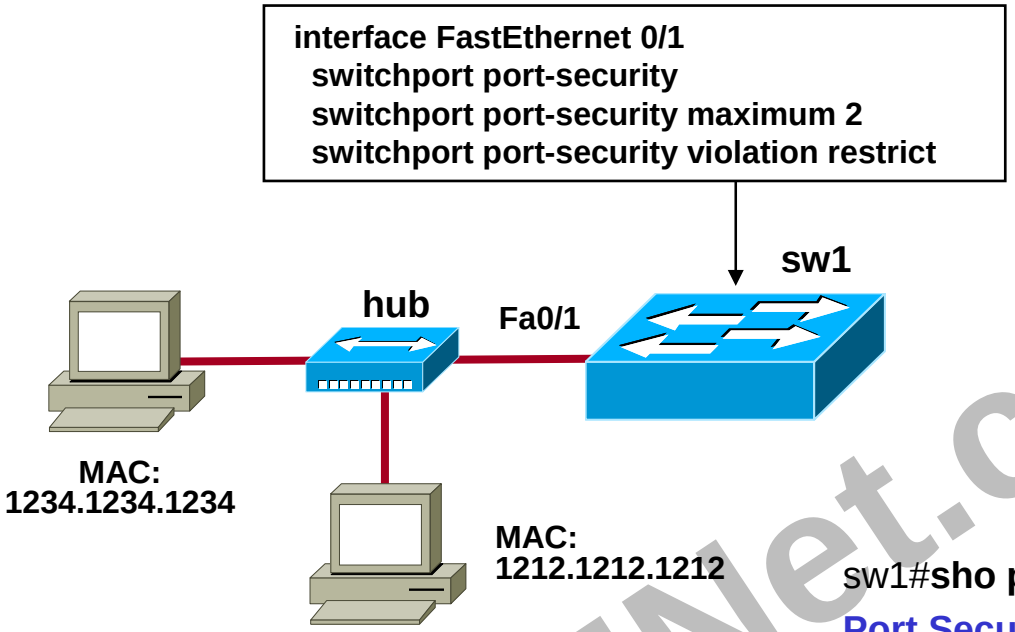


- przykład automatycznego wyprowadzenia interfejsu ze stanu błędu (err-disbled) za pomocą mechanizmu odzyskiwania portów

sw1#
Oct 30 11:48:18: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
Oct 30 11:48:18: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 1234.1234.1234 on port FastEthernet0/1.
Oct 30 11:48:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Oct 30 11:48:20: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
sw1#
Oct 30 11:52:59: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/1
Oct 30 11:53:03: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Oct 30 11:53:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
sw1#

Port Security

- tryb restrykcji portu, analogicznie jak tryb błędu, dodaje wpis statyczny do tablicy przełączania oraz tablicy bezpieczeństwa
- główna różnica w stosunku do trybu wyłączenia polega na zachowaniu portu w sytuacji złamania zasad bezpieczeństwa
- interfejs w takiej sytuacji pozostaje aktywny, nowy adres który spowodował złamanie polityki bezpieczeństwa nie zostanie wpisany w tablicę przełączania, ani też dodany do tablicy adresów bezpiecznych
- zachowanie takie umożliwia dalszą prawidłową transmisję urządzeniom zarejestrowanym w tablicy MAC oraz tablicy bezpieczeństwa, natomiast urządzenia przekraczające dopuszczalne limity będą blokowane
- przełącznik jednocześnie będzie generował pułapki SNMP oraz wiadomości dziennika zdarzeń dla adresu łamiącego zasady bezpieczeństwa oraz inkrementował licznik statystyk



Port Security

- przykład konfiguracji oraz weryfikacji funkcjonalności restrykcji portów bezpiecznych

sw1#**sho port-security interface fastEthernet 0/1**

Port Security	**: Enabled**
Port Status	**: Secure-up**
Violation Mode	**: Restrict**
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	**: 2**
Total MAC Addresses	**: 2**
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address	**: 1234.1234.1235**
Security Violation Count	**: 243**

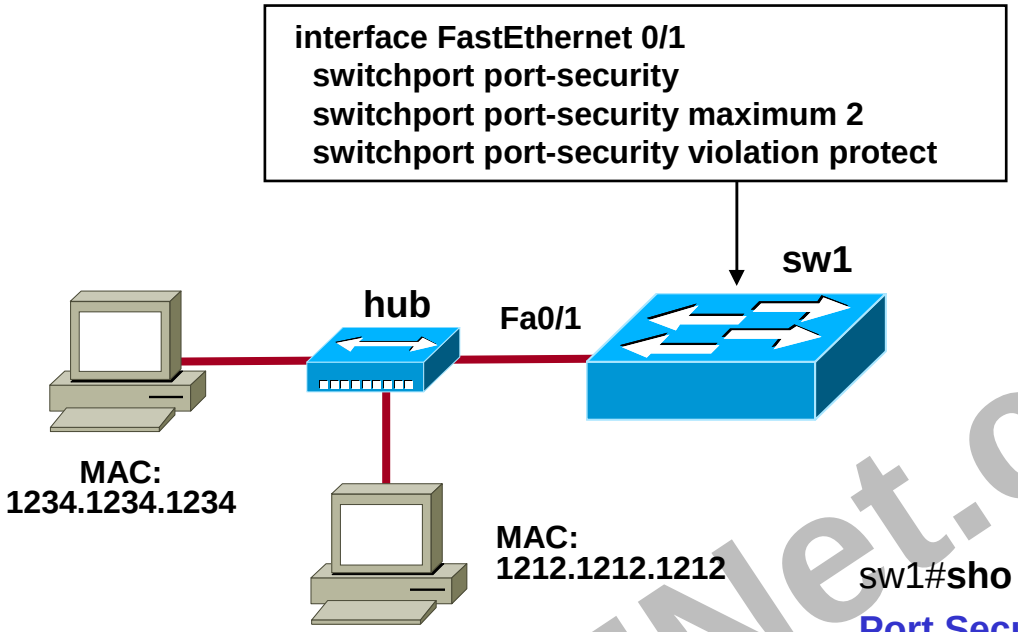
Port Security

- przykład weryfikacji trybu restrykcji portu -> powiadomienia będą generowane co 5 sekund (o ile ma miejsce naruszająca zasady bezpieczeństwa transmisja)

```
sw1#
14:11:35: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:11:40: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:11:45: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:11:50: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:11:55: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:12:00: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:12:05: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:12:10: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
sw1#
14:12:15: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address 1234.1234.1235 on port FastEthernet0/1.
```

Port Security

- tryb protekcji portu, analogicznie jak tryby błędu oraz restrykcji, dodaje wpis statyczny do tablicy przełączania oraz tablicy bezpieczeństwa
- w sytuacji złamania zasad bezpieczeństwa interfejs pozostaje aktywny -> nowy adres który spowodował złamanie polityki bezpieczeństwa, nie zostanie wpisany w tablicę przełączania, ani też dodany do tablicy adresów bezpiecznych
- zachowanie takie umożliwia dalszą prawidłową transmisję urządzeniom zarejestrowanym w tablicy MAC oraz tablicy bezpieczeństwa, natomiast urządzenia przekraczające dopuszczalne limity będą blokowane
- przełącznik nie będzie generował pułapek SNMP czy wiadomości dziennika zdarzeń dla adresu łamiącego zasady bezpieczeństwa, nie będzie także inkrementowany licznik statystyk



Port Security

- przykład konfiguracji oraz weryfikacji funkcjonalności protekcji portów bezpiecznych

sw1#**sho port-security interface FastEthernet 0/1**

Port Security	**: Enabled**
Port Status	**: Secure-up**
Violation Mode	**: Protect**
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	**: 2**
Total MAC Addresses	**: 2**
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address	**: 1234.1234.1235**
Security Violation Count	**: 243**

Port Security

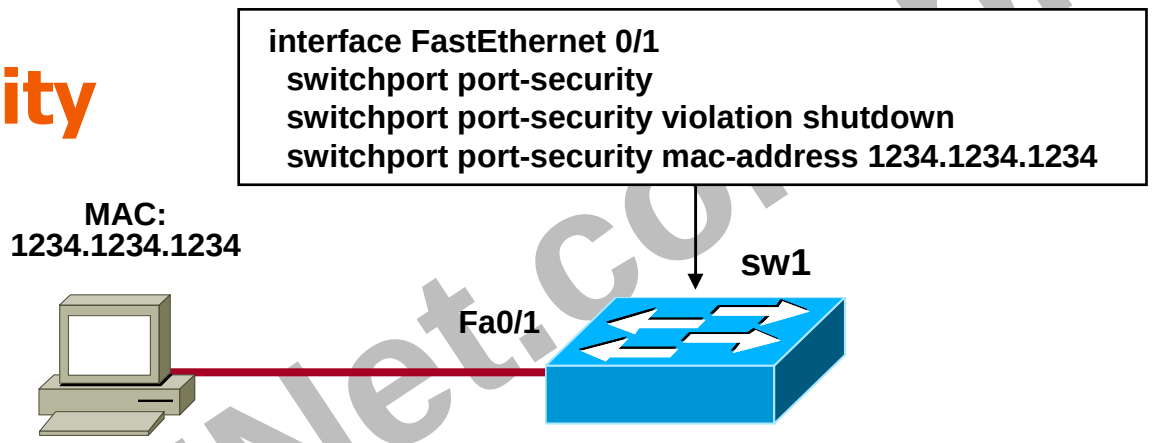
- wszystkie rozwiązania poznane do tej pory bazowały na dynamicznym poznawaniu bezpiecznej adresacji źródłowej MAC
- alternatywą dla rozwiązań bezpiecznych adresów poznawanych dynamicznie są bezpieczne adresy statyczne
- bezpieczny adres statyczny wymaga konfiguracji manualnej, przechowywany jest w pliku konfiguracji bieżącej, a po zapisaniu także w startowej oraz w tablicy przełączania -> wpis permanentny

(config-if)# switchport port-security mac-address *hhhh.hhhh.hhhh*

✓ *hhhh.hhhh.hhhh* wartość bezpiecznego adresu fizycznego

Port Security

- uruchomienie funkcjonalności portu bezpiecznego ze statyczną konfiguracją bezpiecznego adresu MAC



sw1#**show port-security address**

Secure Mac Address Table

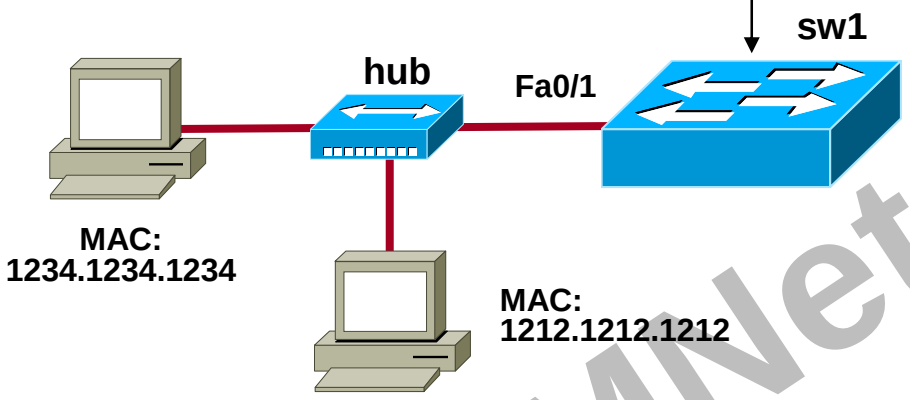
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	**1234.1234.1234**	**SecureConfigured**	**Fa0/1**	**-**

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 1024

Port Security

```
interface FastEthernet 0/1
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation protect
  switchport port-security mac-address 1234.1234.1234
  switchport port-security mac-address 1212.1212.1212
```



- podłączenie większej liczby urządzeń ze statyczną konfiguracją bezpiecznych adresów MAC, wymaga jawnej deklaracji ich maksymalnej dopuszczalnej liczby (domyślnie 1)

sw1#**show port-security address**

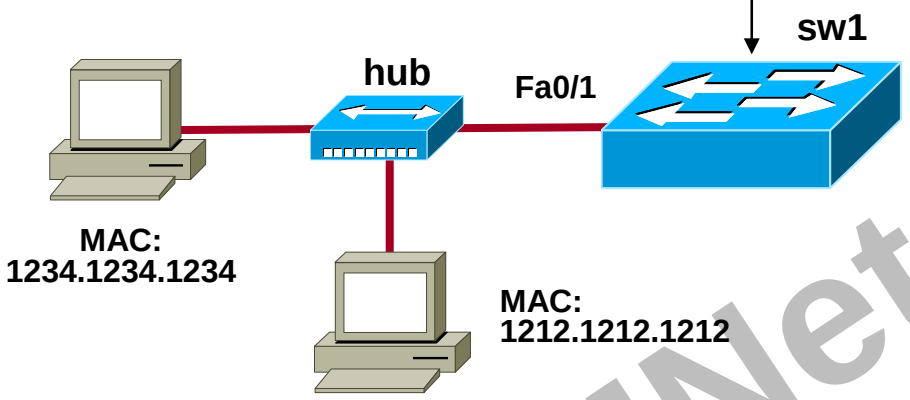
Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	1234.1234.1234	SecureConfigured	Fa0/1	-
1	1212.1212.1212	SecureConfigured	Fa0/1	-

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 1024

```
interface FastEthernet 0/1
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation protect
  switchport port-security mac-address 1234.1234.1234
```



- w sytuacji, gdy liczba adresów statycznie skonfigurowanych jest mniejsza od zdefiniowanej maksymalnej liczby adresów bezpiecznych, pozostałe adresy poznawane są jako dynamiczne

sw1#**show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	1234.1234.1234	SecureConfigured	Fa0/1	-
1	1212.1212.1212	SecureDynamic	Fa0/1	-

Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 1024

Port Security

Port Security

- wyczyszczenie z konfiguracji statycznego bezpiecznego adresu MAC

```
# clear port-security static [ address hhhh.hhhh.hhhh.hhhh ]
```

- wyczyszczenie z konfiguracji wszystkich bezpiecznych statycznych adresów MAC przypisanych w ramach określonego portu

```
# clear port-security static [ interface intf_type number ]
```


✓ *intf_type number*	odwołanie do interfejsu fizycznego
✓ *hhhh.hhhh.hhhh*	wartość bezpiecznego adresu fizycznego

Port Security

- alternatywą dla rozwiązań statycznych bezpiecznych adresów są statycznie przylepne (Sticky) adresy bezpieczne
- przylepny bezpieczny adres statyczny nie wymaga konfiguracji manualnej, przechowywany jest w pliku konfiguracji bieżącej, a po zapisaniu także w startowej oraz w tablicy przełączania
- zapisanie konfiguracji przed ponownym uruchomieniem zapewnia zachowanie wpisów z adresami MAC -> wpis permanentny

(config-if)# switchport port-security mac-address sticky [*hhhh.hhhh.hhhh* **]**

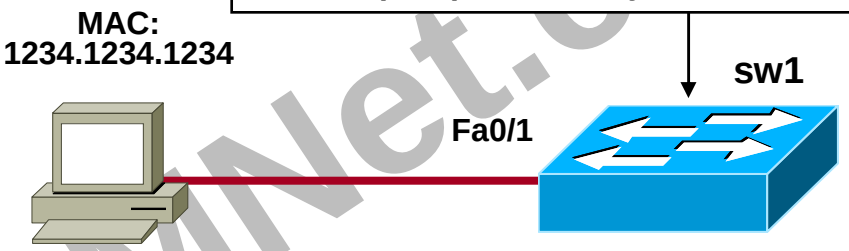
✓ *hhhh.hhhh.hhhh* wartość bezpiecznego adresu fizycznego

⇘ statyczne przyczepne adresy MAC nie wymagają jawnej konfiguracji

- uruchomienie funkcjonalności portu bezpiecznego z konfiguracją przylepnych adresów MAC-> wartość statycznego adresu przyczepnego zostanie dodana automatycznie do konfiguracji

Port Security

```
interface FastEthernet 0/1
  switchport port-security
  switchport port-security violation shutdown
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 1234.1234.1234
```



sw1#**show port-security address**

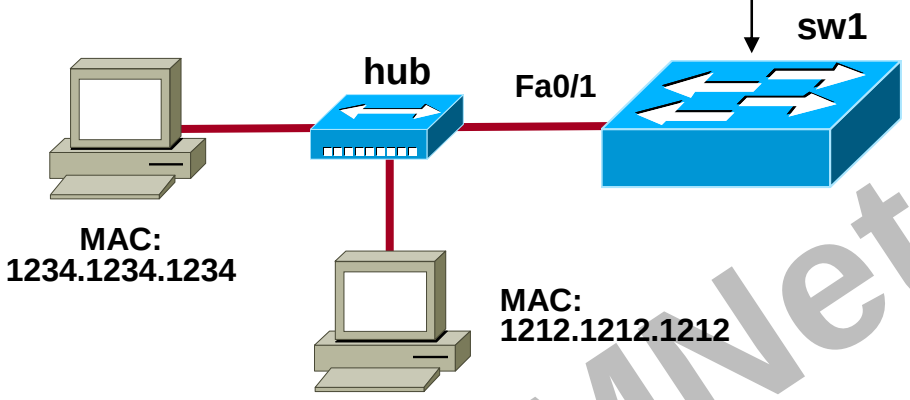
Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	1234.1234.1234	SecureSticky	Fa0/1	-

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024

Port Security

```
interface FastEthernet 0/1
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation protect
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 1234.1234.1234
  switchport port-security mac-address sticky 1212.1212.1212
```



- podłączenie większej liczby urządzeń z przylepną konfiguracją bezpiecznych adresów MAC, wymaga jawnej deklaracji ich maksymalnej dopuszczalnej liczby (domyślnie 1)

sw1#**show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	1234.1234.1234	SecureSticky	Fa0/1	-
1	1212.1212.1212	SecureSticky	Fa0/1	-

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 1024

Port Security

- wyczyszczenie z konfiguracji statycznego przylepnego adresu MAC

```
# clear port-security static [ address hhhh.hhhh.hhhh.hhhh ]
```

- wyczyszczenie z konfiguracji wszystkich bezpiecznych przylepnych adresów w ramach określonego portu

```
# clear port-security static [ interface intf_type number ]
```


✓ *hhhh.hhhh.hhhh*	wartość bezpiecznego adresu fizycznego
✓ *intf_type number*	odwołanie do interfejsu fizycznego

Port Security

- bezpieczne wpisy adresów MAC w ramach portów przełącznika mogą wygasać -> są one usuwane z konfiguracji oraz tablicy adresów bezpiecznych
- wygasanie domyślnie dotyczy adresów nauczonych dynamicznie
- określenie czasu po którym wygasną adresy bezpieczne

```
(config-if)# switchport port-security aging time age_time
```


✓ *age_time* — czas wygaśnięcia adresów w minutach, dla wartości 0 wygasanie adresów jest wyłączone, zakres: 0 – 1440 minut, domyślnie czas wygasania ustawiony jest 0 minut

Port Security

- czas wygasania może być określony jako:
  - absolute (bezwzględny) -> wygaśnięcie adresu następuje po określonym czasie, opcja domyślna
  - inactivity (brak aktywności) -> wygaśnięcie adresu następuje w sytuacji braku transmisji przez określony czas

```
(config-if)# switchport port-security aging type { inactivity | absolute }
```

Port Security

- uruchomienie funkcjonalności wygasania adresów statycznych powoduje wygaśnięcie statycznego adresu po określonym czasie i uniemożliwia przypisanie nowych adresów statycznych w ramach danego portu

- wygaśnięcie adresu statycznego skutkuje usunięciem bezpiecznego wpisu z konfiguracji bieżącej oraz tablic: przełączania i portów bezpiecznych -> jeżeli urządzenie jest aktywne adres zostanie poznany jako dynamiczny

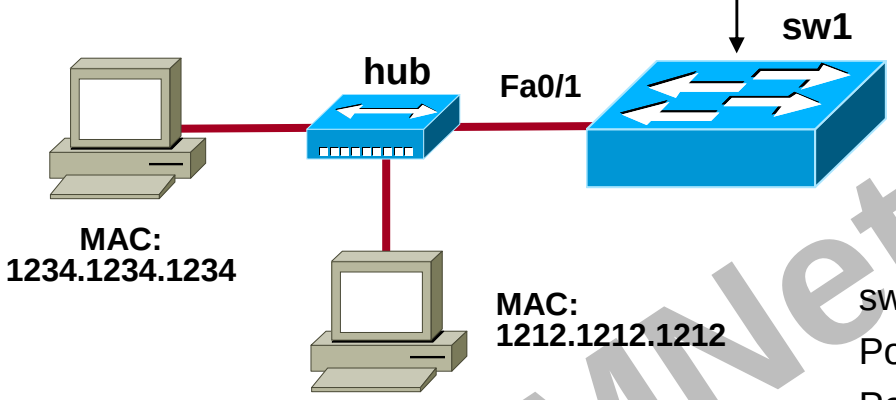
- przyczepne adresy statyczne nie podlegają mechanizmom wygasania

- uruchomienie funkcjonalności wygasania adresów statycznych

```
(config-if)# switchport  port-security  aging  static
```

Port Security

```
interface FastEthernet 0/1
  switchport port-security
  switchport port-security maximum 2
  switchport port-security violation shutdown
  switchport port-security aging time 60
  switchport port-security aging type inactivity
  switchport port-security aging static
```



- przykład konfiguracji oraz weryfikacji funkcjonalności wygasania statycznych oraz dynamicznych adresów portów bezpiecznych po 60 minutach
- wygaśniecie nastąpi w przypadku braku aktywności ze strony urządzenia

sw1#**sho port-security interface FastEthernet 0/1**

Port Security	: Enabled
Port Status	: Secure-up
Violation Mode	: Shutdown
Aging Time	**: 60 mins**
Aging Type	**: Inactivity**
SecureStatic Address Aging	**: Enabled**
Maximum MAC Addresses	: 2
Total MAC Addresses	: 2
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address	: 1234.1234.1235
Security Violation Count	: 243

Port Security

- weryfikacja dodawania oraz usuwania portów bezpiecznych

sw1#**debug port-security**
000403: 03:33:19: %SYS-5-CONFIG_I: Configured from console by console
sw1#
000404: 03:33:34: PSECURE:
PSECURE: Address 000f.8f12.7a86 aged out
000405: 03:33:34: PSECURE: Deleting secure MAC address 000f.8f12.7a86 on port: Fa0/2
000406: 03:33:34: PSECURE: Delete dynamic secure address: 000f.8f12.7a86
000407: 03:33:34: PSECURE: Delete dynamic secure address:000f.8f12.7a86
000408: 03:33:34: PSECURE: psecure_platform_del_mac_addrs: Do nothing, called to delete <1,000f.8f12.7a86> to FastEthernet0/2
000409: 03:33:34: PSECURE: psecure_delete_address_not_ok address <1,000f.8f12.7a86> allowed
000410: 03:33:37: PSECURE: Adding 000f.8f12.7a86 as dynamic on port Fa0/2 for vlan 1
000411: 03:33:37: PSECURE: Adding address vlan 1 000f.8f12.7a86 to port-security
000412: 03:33:37: PSECURE: psecure_platform_add_mac_addrs: Do nothing, called to add <1,000f.8f12.7a86> to FastEthernet0/2
sw1#

Port Security

- ograniczenia funkcjonalności bezpieczeństwa portów:
  - interfejs musi się znajdować w trybie dostępowym (access), trybie magistralowym (trunk; negocjacje magistrali nie są dopuszczalne) lub trybie tunelu 802.1Q (802.1Q Tunnel)
  - nie może być portem dostępu dynamicznego
  - nie może być portem docelowym analizy transmisji (SPAN)
  - nie może należeć do grup agregujących porty (EtherChannel)
  - uruchomienie opcji bezpieczeństwa dla portu dostępowego (access) skutkuje uruchomieniem bezpieczeństwa dla portu sieci głosowej
  - nie można konfigurować statycznych lub przyczepnych adresów dla sieci głosowych (Voice VLAN)

Port Security

- ograniczenia funkcjonalności bezpieczeństwa portów:
  - opcje protekcji (Protect) i ograniczenia (Shutdown) portu nie mogą być jednocześnie aktywowane
  - przełącznik nie wspiera czasów bezczynności dla przyczepnych adresów MAC
  - w sytuacji konfiguracji głosowej sieci VLAN w ramach portu z adresami przyczepnymi, przełącznik poznaje adresy głosowej sieci VLAN jako adresy dynamiczne, pozostałe adresy sieci danych są odnotowywane jako przyczepne
  - konfiguracja sieci głosowych Voice VLAN wymaga ustawienia liczby dopuszczalnych adresów na wartość minimalnie dwóch
  - wpisy statyczne w tablicy przełączania (mac-address-table static) mają priorytet nad mechanizmami portów bezpiecznych