**Implementați securitatea portului**

**Securizare porturi neutilizate**

Dispozitivele de nivel 2 sunt considerate a fi cea mai slabă verigă din infrastructura de securitate a unei companii. Atacurile de nivel 2 sunt unele dintre cele mai ușor de implementat de către hackeri, dar aceste amenințări pot fi, de asemenea, atenuate cu unele soluții comune de nivel 2.

Toate porturile (interfețele) switch-ului trebuie securizate înainte ca comutatorul să fie implementat pentru utilizare în producție. Modul în care este securizat un port depinde de funcția acestuia.

O metodă simplă pe care o folosesc mulți administratori pentru a ajuta la securizarea rețelei împotriva accesului neautorizat este de a dezactiva toate porturile neutilizate de pe un comutator. De exemplu, dacă un switch Catalyst 2960 are 24 de porturi și există trei conexiuni Fast Ethernet în uz, este o practică bună să dezactivați cele 21 de porturi neutilizate. **Navigați la fiecare port neutilizat și lansați comanda de închidere** Cisco IOS . Dacă un port trebuie reactivat mai târziu, acesta poate fi activat cu comanda **no shutdown** .

Pentru a configura o serie de porturi, utilizați comanda **interfață interval** .

**Switch(config)# tip de gamă de interfețe modul/primul număr – ultimul număr**

De exemplu, pentru a închide porturile pentru Fa0/8 prin Fa0/24 pe S1, ar trebui să introduceți următoarea comandă.

**S1(config)# interface range fa0/8 - 24**

**S1(config-if-range)# shutdown**

**%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down**

**(output omitted)**

**%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down**

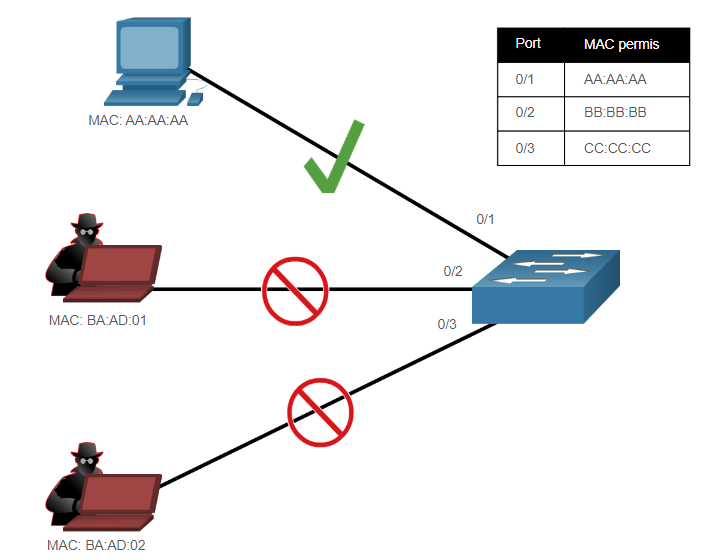
**S1(config-if-range)#**

**Reduceți atacurile din tabelul de adrese MAC**

Cea mai simplă și eficientă metodă de a preveni atacurile de depășire a tabelului de adrese MAC este activarea securității porturilor.

Securitatea porturilor limitează numărul de adrese MAC valide permise pe un port. Permite unui administrator să configureze manual adresele MAC pentru un port sau să permită comutatorului să învețe în mod dinamic un număr limitat de adrese MAC. Când un port configurat cu securitatea portului primește un cadru, adresa MAC sursă a cadrului este comparată cu lista de adrese MAC sursă securizate care au fost configurate manual sau învățate dinamic pe port.

Limitând numărul de adrese MAC permise pe un port la una, securitatea porturilor poate fi utilizată pentru a controla accesul neautorizat la rețea, așa cum se arată în figură.



Graficul arată un comutator conectat la trei dispozitive. Deasupra comutatorului este un tabel de adrese MAC cu portul 0/1 cu MAC permis AA:AA:AA, portul 0/2 permis MAC BB:BB:BB și portul 0/2 permis MAC CC:CC:CC. Comutatorul arată portul 0/1 care este conectat la un PC cu o adresă MAC AA:AA:AA. Acest link are o bifă verde. Apoi portul 0/2 de pe comutator este conectat la un laptop necinstite cu adresa MAC BA:AD:01. Legătura are un cerc roșu cu o linie prin el. Portul 0/3 oprit al comutatorului este, de asemenea, conectat la un laptop necinstiți cu adresa MAC BA:AD:02. Această legătură are și un cerc roșu cu o linie prin el.

MAC: AA:AA:AAMAC: BA:AD:01MAC: BA:AD:020/10/20/3PortMAC permis0/10/20/3AA:AA:AABB:BB:BBCC:CC:CC

**Notă** : adresele MAC sunt afișate ca 24 de biți pentru simplitate.

**Activați Port Security**

Observați în exemplu, comanda **switchport port-security** a fost respinsă. Acest lucru se datorează faptului că securitatea porturilor poate fi configurată numai pe porturi de acces configurate manual sau porturi trunchi configurate manual. În mod implicit, porturile de comutare Layer 2 sunt setate la automat dinamic (trunking activat). Prin urmare, în exemplu, portul este configurat cu comanda de configurare a interfeței de **acces în modul switchport .**

**Notă** : Securitatea porturilor trunchi depășește scopul acestui curs.

**S1(config)# interface f0/1**

**S1(config-if)# switchport port-security**

**Command rejected: FastEthernet0/1 is a dynamic port.**

**S1(config-if)# switchport mode access**

**S1(config-if)# switchport port-security**

**S1(config-if)# end**

**S1#**

Utilizați comanda **show port-security interface** pentru a afișa setările curente de securitate a portului pentru FastEthernet 0/1, așa cum se arată în exemplu. Observați cum este activată securitatea portului, starea portului este Securizat, ceea ce înseamnă că nu există dispozitive atașate și nu a avut loc nicio încălcare, modul de încălcare este Închidere și cum numărul maxim de adrese MAC este 1. Dacă un dispozitiv este conectat la port, starea portului comutatorului va afișa Secure-up și comutatorul va adăuga automat adresa MAC a dispozitivului ca MAC securizat. În acest exemplu, niciun dispozitiv nu este conectat la port.

**S1# show port-security interface f0/1**

**Port Security : Enabled**

**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:Vlan : 0000.0000.0000:0**

**Security Violation Count : 0**

**S1#**

**Notă** : Dacă un port activ este configurat cu comanda **switchport port-security** și mai multe dispozitive sunt conectate la acel port, portul va trece la starea dezactivată de eroare. Această condiție este discutată mai târziu în acest subiect.

După ce securitatea portului este activată, pot fi configurate alte specificații de securitate a portului, așa cum se arată în exemplu.

**S1(config-if)# switchport port-security ?**

**aging Port-security aging commands**

**mac-address Secure mac address**

**maximum Max secure addresses**

**violation Security violation mode**

**S1(config-if)# switchport port-security**

**Limitați și aflați adresele MAC**

Pentru a seta numărul maxim de adrese MAC permise pe un port, utilizați următoarea comandă:

**Switch(config-if)# switchport port-security valoarea maximă**

Valoarea implicită de securitate a portului este 1. Numărul maxim de adrese MAC sigure care pot fi configurate depinde de comutator și de IOS. În acest exemplu, maximul este 8192.

**S1(config)# interface f0/1**

**S1(config-if)# switchport port-security maximum ?**

**<1-8192> Maximum addresses**

**S1(config-if)# switchport port-security maximum**

Comutatorul poate fi configurat pentru a afla despre adresele MAC pe un port securizat într-unul din trei moduri:

**1 . Configurat manual**

Administratorul configurează manual o adresă(e) MAC statică(e) utilizând următoarea comandă pentru fiecare adresă MAC sigură de pe port:

**Switch(config-if)# switchport port-security mac-address sticky**

**2 . Învățat dinamic**

Când este introdusă comanda **switchport port-security** , sursa MAC curentă pentru dispozitivul conectat la port este securizată automat, dar nu este adăugată la configurația de pornire. Dacă comutatorul este repornit, portul va trebui să învețe din nou adresa MAC a dispozitivului.

**3 . Învățat dinamic – Lipicios**

Administratorul poate activa comutatorul să învețe în mod dinamic adresa MAC și să le „lipească” de configurația care rulează utilizând următoarea comandă:

**Switch(config-if)# switchport port-security adresa mac sticky**

Salvarea configurației de rulare va trimite adresa MAC învățată dinamic la NVRAM.

Următorul exemplu demonstrează o configurație completă de securitate a porturilor pentru FastEthernet 0/1 cu o gazdă conectată la portul Fa0/1. Administratorul specifică maximum 2 adrese MAC, configurează manual o adresă MAC securizată și apoi configurează portul pentru a afla în mod dinamic adrese MAC sigure suplimentare până la maximum 2 adrese MAC securizate. Utilizați **interfața show port-security** și comanda **show port-security address** pentru a verifica configurația.

**\*Mar 1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1#conf t**

**Enter configuration commands, one per line. End with CNTL/Z.**

**S1(config)#**

**S1(config)# interface fa0/1**

**S1(config-if)# switchport mode access**

**S1(config-if)# switchport port-security**

**S1(config-if)# switchport port-security maximum 2**

**S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234**

**S1(config-if)# switchport port-security mac-address sticky**

**S1(config-if)# end**

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 0 mins**

**Aging Type : Absolute**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1# show port-security address**

**Secure Mac Address Table**

**-----------------------------------------------------------------------------**

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

**---- ----------- ---- ----- -------------**

**1 a41f.7272.676a SecureSticky Fa0/1 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -**

**-----------------------------------------------------------------------------**

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

**Max Addresses limit in System (excluding one mac per port) : 8192**

**S1#**

Ieșirea comenzii **show port-security interface** verifică dacă securitatea portului este activată, există o gazdă conectată la port (adică Secure-up), vor fi permise un total de 2 adrese MAC și S1 a învățat o adresă MAC static și o adresă MAC dinamic (adică, sticky).

Ieșirea comenzii **show port-security address** listează cele două adrese MAC învățate.

**Îmbătrânirea securității portuare**

Îmbătrânirea securității porturilor poate fi utilizată pentru a seta timpul de îmbătrânire pentru adresele securizate statice și dinamice pe un port. Două tipuri de îmbătrânire sunt acceptate pentru fiecare port:

* **Absolut** - Adresele securizate de pe port sunt șterse după perioada de vechime specificată.
* **Inactivitate** - Adresele securizate de pe port sunt șterse numai dacă sunt inactive pentru perioada de vechime specificată.

Utilizați vechimea pentru a elimina adresele MAC securizate de pe un port securizat fără a șterge manual adresele MAC securizate existente. Limitele de timp învechite pot fi, de asemenea, mărite pentru a se asigura că adresele MAC securizate din trecut rămân, chiar dacă sunt adăugate noi adrese MAC. Îmbătrânirea adreselor securizate configurate static poate fi activată sau dezactivată în funcție de port.

Utilizați comanda **switchport port-security aging** pentru a activa sau dezactiva îmbătrânirea statică pentru portul securizat sau pentru a seta timpul sau tipul de îmbătrânire.

**Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}**

Parametrii pentru comandă sunt descriși în tabel.

|  |  |
| --- | --- |
| **Parametru** | **Descriere** |
| **static** | Activați vechimea pentru adresele securizate configurate static pe acest port. |
| **time time** | Specificați timpul de îmbătrânire pentru acest port. Intervalul este de la 0 la 1440 de minute. Dacă timpul este 0, vechimea este dezactivată pentru acest port. |
| **type absolute** | Setați timpul absolut de îmbătrânire. Toate adresele securizate de pe acest port expiră exact după timpul (în minute) specificat și sunt eliminate din lista de adrese securizate. |
| **type inactivity** | Setați tipul de îmbătrânire inactivitate. Adresele securizate de pe acest port expiră numai dacă nu există trafic de date de la adresa sursă securizată pentru perioada de timp specificată. |

**Notă** : adresele MAC sunt afișate ca 24 de biți pentru simplitate.

Exemplul arată un administrator care configurează tipul de vechime la 10 minute de inactivitate și utilizând comanda **show port-security interface** pentru a verifica configurația.

**S1(config)# interface fa0/1**

**S1(config-if)# switchport port-security aging time 10**

**S1(config-if)# switchport port-security aging type inactivity**

**S1(config-if)# end**

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1#**

**Moduri de încălcare a securității porturilor**

Dacă adresa MAC a unui dispozitiv atașat la port diferă de lista de adrese securizate, atunci are loc o încălcare a portului. În mod implicit, portul intră în starea dezactivată de eroare.

Pentru a seta modul de încălcare a securității porturilor, utilizați următoarea comandă:

**Switch(config-if)# switchport port-security violation { protect | restrânge | oprire }**

Următoarele tabele arată cum reacţionează un comutator pe baza modului de încălcare configurat.

Descrieri ale modului de încălcare a securității

|  |  |
| --- | --- |
| **Modul** | **Descriere** |
| **shutdown**  **(default)** | Portul trece imediat la starea dezactivată de eroare, stinge LED-ul portului și trimite un mesaj syslog. Crește contorul de încălcări. Când un port securizat se află în starea dezactivată de eroare, un administrator trebuie să-l reactiveze introducând comenzile de **închidere** și **fără închidere .** |
| **restrict** | Portul elimină pachetele cu adrese sursă necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Acest mod face ca contorul de încălcări de securitate să crească și generează un mesaj syslog. |
| **protect** | Acesta este cel mai puțin sigur dintre modurile de încălcare a securității. Portul elimină pachete cu adrese MAC necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Nu este trimis niciun mesaj syslog. |

**Comparația modului de încălcare a securității**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modul de încălcare** | **Renunță la traficul ofensator** | **Trimite un mesaj Syslog** | **Măriți contorul de încălcări** | **Închide portul** |
| Protect | da | Nu | Nu | Nu |
| R**estrict** | da | da | da | Nu |
| **SHutdown** | da | da | da | da |

Următorul exemplu arată un administrator care modifică încălcarea securității în „restricționare”. Ieșirea comenzii **show port-security interface** confirmă că modificarea a fost făcută.

**S1(config)# interface f0/1**

**S1(config-if)# switchport port-security violation restrict**

**S1(config-if)# end**

**S1#**

**S1# show port-security interface f0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Restrict**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1#**

**Porturi în stare dezactivată de eroare**

Ce se întâmplă când încălcarea securității portului este oprită și are loc o încălcare a portului? Portul este oprit fizic și plasat în starea dezactivată de eroare și nu este trimis sau primit niciun trafic pe acel port.

În figură, încălcarea securității portului este schimbată înapoi la setarea implicită de oprire. Apoi gazda cu adresa MAC a41f.7272.676a este deconectată și o nouă gazdă este conectată la Fa0/1.

Observați cum sunt generate pe consolă o serie de mesaje legate de securitatea porturilor.

**S1(config)# int fa0/1**

**S1(config-if)# switchport port-security violation shutdown**

**S1(config-if)# end**

**S1#**

**\*Mar 1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1#**

**\*Mar 1 00:24:32.829: %PM-4-ERR\_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state**

**\*Mar 1 00:24:32.838: %PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.**

**\*Mar 1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down**

**S1#**

**Notă** : Protocolul portului și starea conexiunii sunt schimbate în jos și LED-ul portului este stins.

În exemplu, comanda **show interface** identifică starea portului ca fiind **err-disabled** . Ieșirea comenzii **show port-security** interface arată acum starea portului ca Secure-shutdown în loc de Secure-up. Contorul de încălcări de securitate crește cu 1.

**S1# show interface fa0/1 | include down**

**FastEthernet0/18 is down, line protocol is down (err-disabled)**

**(output omitted)**

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-shutdown**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7273.018c:1**

**Security Violation Count : 1**

**S1#**

Administratorul ar trebui să determine ce a cauzat încălcarea securității Dacă un dispozitiv neautorizat este conectat la un port securizat, amenințarea de securitate este eliminată înainte de a reactiva portul.

În exemplul următor, prima gazdă este reconectată la Fa0/1. Pentru a reactiva portul, utilizați mai întâi comanda **shutdown** , apoi folosiți comanda **no shutdown** pentru a face portul operațional, așa cum se arată în exemplu.

**S1(config)# interface fa0/1**

**S1(config-if)# shutdown**

**S1(config-if)#**

**\*Mar 1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down**

**S1(config-if)# no shutdown**

**S1(config-if)#**

**\*Mar 1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1(config-if)#**

**Verificați securitatea portului**

După configurarea securității portului pe un comutator, verificați fiecare interfață pentru a verifica dacă securitatea portului este setată corect și verificați pentru a vă asigura că adresele MAC statice au fost configurate corect.

**Securitatea porturilor pentru toate interfețele**

Pentru a afișa setările de securitate a porturilor pentru comutator, utilizați comanda **show port-security** . Exemplul indică faptul că un singur port este configurat cu comanda switchport port-security.

**S1# 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) : 8192**

**S1#**

**Securitate port pentru o interfață specifică**

Utilizați comanda **show port-security interface** pentru a vizualiza detaliile pentru o anumită interfață, așa cum se arată anterior și în acest exemplu.

**S1# show port-security interface fastethernet 0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7273.018c:1**

**Security Violation Count : 0**

**S1#**

**Verificați adresele MAC învățate**

Pentru a verifica dacă adresele MAC „se lipesc” de configurație, utilizați comanda **show run** așa cum se arată în exemplul pentru FastEthernet 0/19.

**S1# show run interface fa0/1**

**Building configuration...**

**Current configuration : 365 bytes**

**!**

**interface FastEthernet0/1**

**switchport mode access**

**switchport port-security maximum 2**

**switchport port-security mac-address sticky**

**switchport port-security mac-address sticky a41f.7272.676a**

**switchport port-security mac-address aaaa.bbbb.1234**

**switchport port-security aging time 10**

**switchport port-security aging type inactivity**

**switchport port-security**

**end**

**S1#**

**Verificați adresele MAC securizate**

Pentru a afișa toate adresele MAC securizate care sunt configurate manual sau învățate dinamic pe toate interfețele switch-ului, utilizați comanda **show port-security address** , așa cum se arată în exemplu.

**S1# show port-security address**

**Secure Mac Address Table**

**-----------------------------------------------------------------------------**

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

**---- ----------- ---- ----- -------------**

**1 a41f.7272.676a SecureSticky Fa0/1 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -**

**-----------------------------------------------------------------------------**

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

**Max Addresses limit in System (excluding one mac per port) : 8192**

S1#

**Syntax Checker - Implement Port Security**

Implement port security for a switch interface based on the specified requirements

You are currently logged into S1. Configure FastEthernet 0/5 for port security by using the following requirements:

**Use the interface name fa0/5 to enter interface configuration mode.**

**Enable the port for access mode.**

**Enable port security.**

**Set the maximum number of MAC address to 3.**

**Statically configure the MAC address aaaa.bbbb.1234.**

**Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.**

**Return to privileged EXEC mode.**

**S1(config)#interface fa0/5**

**S1(config-if)#switchport mode access**

**S1(config-if)#switchport port-security**

**S1(config-if)#switchport port-security maximum 3**

**S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234**

**S1(config-if)#switchport port-security mac-address sticky**

**S1(config-if)#end**

**Enter the command to verify port security for all interfaces.**

**S1#show port-security**

**Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action**

**(Count) (Count) (Count)**

**---------------------------------------------------------------------------**

**Fa0/5 3 2 0 Shutdown**

**---------------------------------------------------------------------------**

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

**Max Addresses limit in System (excluding one mac per port) : 8192**

**Enter the command to verify port security on FastEthernet 0/5. Use fa0/5 for the interface name.**

**S1#show port-security interface fa0/5**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 0 mins**

**Aging Type : Absolute**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 3**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : 0090.2135.6B8C:1**

**Security Violation Count : 0**

**Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.**

**S1#show port-security address**

**Secure Mac Address Table**

**-----------------------------------------------------------------------------**

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

**---- ----------- ---- ----- -------------**

**1 0090.2135.6b8c SecureSticky Fa0/5 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/5 -**

**-----------------------------------------------------------------------------**

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

**Max Addresses limit in System (excluding one mac per port) : 8192**

**You have successfully configured and verified port security for the interface.**