فعال کردن Port Security در سوئیچهای سیسکو

Port Security یکی از خصوصیتهای کنترل ترافیک لایه ۲ در سوئیچهای Catalyst سیسکو می باشد . دلیل استفاده از Port Security این است که به شما این امکان را میدهد که به تعداد خاصی از آدرسهای مک مبداء اجازه ورود به پورت رابدهید . و یکی از مواردی که زیاد کاربرد دارد زمانی است که کاربران با استفاده از سوئیچهای dumb بصورت غیر قانونی وصل به شبکه میشوند (به عنوان مثال دو یا سه کاربر می توانند از طریق یک پورت access از شبکه استفاده کنند) . بعلاوه دستگاههای unmanaged عیب یابی را برای مدیر شبکه پیچیده میکند که این راه بهترین روش که جلو این کار را بگیریم.

فعال کردن port security :

port securityبا پارامترهای پیش فرض با استفاده از یک دستور روی اینترفیس فعال میشود.

```
Switch(config)# interface f0/13
2 Switch(config-if)# switchport port-security
```

با دستور show port-security شما میتوانید تنظیمات پیش فرض port security را مشاهده نماییم:

```
1  Switch# show port-security interface f0/13
2  Port Security : Enabled
3  Port Status : Secure-down
4  Violation Mode : Shutdown
5  Aging Time : 0 mins
6  Aging Type : Absolute
7  SecureStatic Address Aging : Disabled
8  Maximum MAC Addresses : 1
9  Total MAC Addresses : 0
10 Configured MAC Addresses : 0
```

11 Sticky MAC Addresses : 0

12 Last Source Address:Vlan : 0000.0000.0000:0

13 Security Violation Count : 0

همانطوری که مشاهده مینمایید تعدادی خصوصیت در تصویر بالا دیده می شود که همه را میتوانیم تنظیم کنیم که در ادامه در مورد آنها توضیحات لازم را ارائه میکنم.

وقتی که یک host به پورتی که این قابلیت را روی آن تنظیم کرده ایم متصل شودآدرس مک host به عنوان اولین فریم دریافت شده و پورت آن را ضبط میکند:

1 Switch# show port-security interface f0/13

2 Port Security : Enabled

3 Port Status : Secure-up

4 Violation Mode : Shutdown

5 Aging Time : 0 mins

6 Aging Type : Absolute

7 SecureStatic Address Aging : Disabled

8 Maximum MAC Addresses : 1

9 Total MAC Addresses : 1

10 Configured MAC Addresses : 0

11 Sticky MAC Addresses : 0

12 Last Source Address:Vlan : 001b.d41b.a4d8:10

13 Security Violation Count : 0

اکنون اتصال host را از پورت سوئیچ قطع میکنیم، یک سوئیچ کوچک یا هاب را به آن متصل میکنیم و مجددا host اصلی را به هاب یا سوئیچ متصل شده وصل میکنیم و بعد از یک ثانیه host غیر مجاز را به سوئیچ unmanaged یا هاب متصل کنیم هردو host تلاش میکنند که از پورت access به صورت share استفاده کنند . با هم میبینیم چه اتفاقی زمانی که host دوم شروع به فرستادن ترافیک میکند می افتد.

```
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/13, putting Fa0/13 in err-disable state

%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address

0021.55c8.f13c on port FastEthernet0/13.
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to down

%LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to down
```

اگر مجداد به وضعیت port security پورت را بررسی کنیم میتوانیم ببینیم که یک تخلف مک آدرس جدیدی اتفاق افتاده است.

```
Switch# show port-security interface f0/13
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:Vlan : 0021.55c8.f13c:10
Security Violation Count : 1
```

```
14 Switch# show interfaces f0/13
15 FastEthernet0/13 is down, line protocol is down (err-disabled)
16 Hardware is Fast Ethernet, address is 0013.c412.0f0d (bia 0013.c412.0f0d)
17 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
18 reliability 255/255, txload 1/255, rxload 1/255
19 Encapsulation ARPA, loopback not set
```

به صورت پیش فرض یک تخلف امنیتی پورت (port security violation) اینترفیش را مجبور به حالت error-disabled میکند که میبایستی مدیر شبکه دوباره آنرا با دستور shutdown و در ادامه ان no shutdown روی اینترفیس فعال کند.

Violation Mode :

Shutdown(که بصورت پیش فرض میباشد):

اینترفیس در حالت error-disabled قرار می گیرد و تمام ترافیک ورودی را بلاک میکند.

Protect:

فریمهای که از مک آدرسهایی که اجازه ندارد برسد را حذف میکند و ترافیکهایی که اجازه عبور دارند به صورت عادی مجوز عبور داده میشود.

Restrict:

همانند protect ولی در این حالت یک syslog message ایجاد میشود و به تعداد تخلف (violation) می افزاید.

با تغییر دادن حالت violation به restrict اگر زمانی یک تخلف رخ دهد باخبر میشویم ولی ترافیکها سالم سالم باقی میمانند.

```
1 Switch(config-if)# switchport port-security violation restrict
2 Switch(config-if)# ^Z
3 Switch#
4 %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  0021.55c8.f13c on port FastEthernet0/13.
5
6 Switch# show port-security interface f0/13
```

```
7  Port Security : Enabled
8  Port Status : Secure-up
9  Violation Mode : Restrict
10 Aging Time : 0 mins
11 Aging Type : Absolute
12 SecureStatic Address Aging : Disabled
13 Maximum MAC Addresses : 1
14 Total MAC Addresses : 1
15 Configured MAC Addresses : 0
16 Sticky MAC Addresses : 0
17 Last Source Address:Vlan : 0021.55c8.f13c:10
18 Security Violation Count : 3
19 Switch(config-if)# switchport port-security violation restrict
20 Switch(config-if)# ^Z
21 Switch#
22 %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
23 0021.55c8.f13c on port FastEthernet0/13.
24
25 Switch# show port-security interface f0/13
26 Port Security : Enabled
27 Port Status : Secure-up
28 Violation Mode : Restrict
29 Aging Time : 0 mins
30 Aging Type : Absolute
31 SecureStatic Address Aging : Disabled
```

```
32 Maximum MAC Addresses : 1
33 Total MAC Addresses : 1
34 Configured MAC Addresses : 0
35 Sticky MAC Addresses : 0
36 Last Source Address:Vlan : 0021.55c8.f13c:10
   Security Violation Count : 3
```

متاسفانه ترافیک متخلف به صورت نمایش log ادامه دارد و همچنین به مقدار violation اضافه میگردد تا اینکه host متخلف ازبین برود یا به عبارتی ارتباطش قطع شود.

Maximum MAC Addresses :

به صورت پیش فرض port security تعداد یک آدرس مک را برای ورودی محدود کرده است که میتوانیم آنرا تغییر دهیم برای مثال برای عبور دادن مک آدرس یک host و یک IP phone که بصورت سری به پورت سوئیچ متصل شده اند می توانیم از این خصوصیت استفاده کنیم .

و یک مثال دیگر اینکه فکر کنید که یک هاب با ۱۲ پورت دارید که به سوئیچ متصل باشد و شما بخواهید به ۱۲ مک آدرس اجازه عبور بدهید باید با استفاده از این دستور تغییرات را اعمال کنید.

– تعداد ماکزیمم مک آدرسی که میتوانیم برای یک پورت تعیین کنیم ۱۳۲ مک آدرس می باشد .

برای تغییر این خصوصیت از دستور زیر استفاده میکنیم.

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

و همچنین گزینه وجود دارد که میتوانیم تعداد ماکزیمم مک برای vlan های access و voice را تعیین کنیم(فرض میکنیم که یک voice vlan روی اینترفیس تنظیم شده است)

```
1 Switch(config-if)# switchport port-security maximum 1 vlan access
2 Switch(config-if)# switchport port-security maximum 1 vlan voice
```

یاد گیری MAC Address

یک مدیر شبکه میتواند تعیین کند که ترافیک چه مک آدرسی اجازه عبور از اینترفیس را دارد.مک آدسها میتوانند به صورت انتخابی برای هر vlan تنظیم شوند (access یا voice)

```
1 Switch(config-if)# switchport port-security mac-address 001b.d41b.a4d8 ?
2 vlan set VLAN ID of the VLAN on which this address can be learned
3
4 Switch(config-if)# switchport port-security mac-address 001b.d41b.a4d8 vlan access
```

بدیهی است که روش استفاده static برای مک آدرس روش راحتی نیست شما میتوانید از روش راحت تری با استفاده گرینه sticky روی دستور port security به صورت اتومات مک آدرس host ی را که به پورت سوئیچ متصل است را اختصاص دهید.

نکته:برای غیر فعال کردن هر کدام از دستورات با گذاشتن عبارت no به ابتدای آن میتوانیم آن دستور را غیر فعال کنیم:

```
1  Switch(config-if)# no switchport port-security mac-address 001b.d41b.a4d8
2  Switch(config-if)# switchport port-security mac-address sticky
3  Switch(config-if)# ^Z
4  Switch# show port-security interface f0/13
5  Port Security : Enabled
6  Port Status : Secure-up
7  Violation Mode : Restrict
8  Aging Time : 0 mins
9  Aging Type : Absolute
10 SecureStatic Address Aging : Disabled
11 Maximum MAC Addresses : 1
```

12 Total MAC Addresses : 1

13 Configured MAC Addresses : 0

14 Sticky MAC Addresses : 1

15 Last Source Address:Vlan : 001b.d41b.a4d8:10

16 Security Violation Count : 0

کاهش زمان ضبط مک آدرس(MAC Address Aging) در port security :

به صورت پیش فرض مک آدرس بصورت همیشگی در پورتی که قابلیت port security را فعال کرده ایم ضبط میشود .با aging میتوانیم تنظیم کنیم که آدرس ضبط شده توسط port security بعد ازطی یک زمان معین expire شود. این خصوصیت به یک host جدید اجازه میدهد که به پورتی که اتصال host از آن قطع شده متصل شود. Aging میتواند برای تاثیر در یک مدت زمان معینی تنظیم شود یا مدت زمان که هیچ فعالیتی انجام نشود.

در مثال زیر تنظیمات به این صورت است که مک آدرس بعد ار ۵ دقیقه عدم فعالیت expire میشود.

1 Switch(config-if)# switchport port-security aging time 5

2 Switch(config-if)# switchport port-security aging type inactivity

3 Switch(config-if)# ^Z

4 Switch# show port-security interface f0/13

5 Port Security : Enabled

6 Port Status : Secure-up

7 Violation Mode : Restrict

8 Aging Time : 5 mins

9 Aging Type : Inactivity

10 SecureStatic Address Aging : Disabled

11 Maximum MAC Addresses : 1

```
12 Total MAC Addresses : 1
13 Configured MAC Addresses : 0
14 Sticky MAC Addresses : 0
15 Last Source Address:Vlan : 001b.d41b.a4d8:10
16 Security Violation Count : 0
```

بعد از ۵ دقیقه خواهیم دید که آدرس پاک شده است:

```
1  Switch# show port-security interface f0/13
2  Port Security : Enabled
3  Port Status : Secure-up
4  Violation Mode : Restrict
5  Aging Time : 5 mins
6  Aging Type : Inactivity
7  SecureStatic Address Aging : Disabled
8  Maximum MAC Addresses : 1
9  Total MAC Addresses : 0
10 Configured MAC Addresses : 0
11 Sticky MAC Addresses : 0
12 Last Source Address:Vlan : 001b.d41b.a4d8:10
13 Security Violation Count : 0
```

Auto-recovery:

برای اجتناب از مداخله دستی برای برگرداندن وضعیت پورت به حالت عادی زمانی که پورت توسط port security مجبور به رفتن به حالت error-disabled میشود میتوانیم قابلیت auto-recovery را برای Port security violation فعال کنیم.فاصله زمانی که پورت به حالت عادی بر میگردد بر حسب ثانیه است.

```
1 Switch(config)# errdisable recovery cause psecure-violation
2 Switch(config)# errdisable recovery interval 600
```

در مثال بالا خواهیم دید که بعد از ده دقیقه که پورت به حال error-disabled رفته است . به صورت اتومات عملکرد پورت به حالت عادی برمیگردد.

```
1 %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/13
2
3 %LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to up
4
5 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state t
```

نکته: port security یک خصوصیت امنیتی قابل اطمینان نیست. چون mac-address ها قابل spoof شدن میباشند و چندین host هنوز میتوانند به راحتی پشت یک روتر کوچک مخفی شوند.