Table des matières

Mise en œuvre de la sécurité des ports

1. Sécurisation des ports inutilisés

Tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur soit déployé pour une utilisation en production. La façon dont un port est sécurisé dépend de sa fonction.

Pour sécuriser le réseau contre les accès non autorisé on peut :

Désactiver tous les ports qui ne sont pas exploités sur un commutateur.
Par exemple, si un commutateur Catalyst 2960 à 24 ports et si trois connexions Fast Ethernet sont utilisées, il est conseillé de désactiver les 21 ports inutilisés. Naviguez vers chaque port inutilisé et exécutez la commande **shutdown** de Cisco IOS. Si un port doit être réactivé plus tard, il peut être activé en exécutant la commande **no shutdown** .

Pour configurer un ensemble de ports, exécuter la commande **interface range** .

```
Switch(config)# interface range type module/first-number - last-number
```

Par exemple, pour désactiver les ports Fa0 / 8 à Fa0 / 24 sur S1, exécuter la commande suivante:

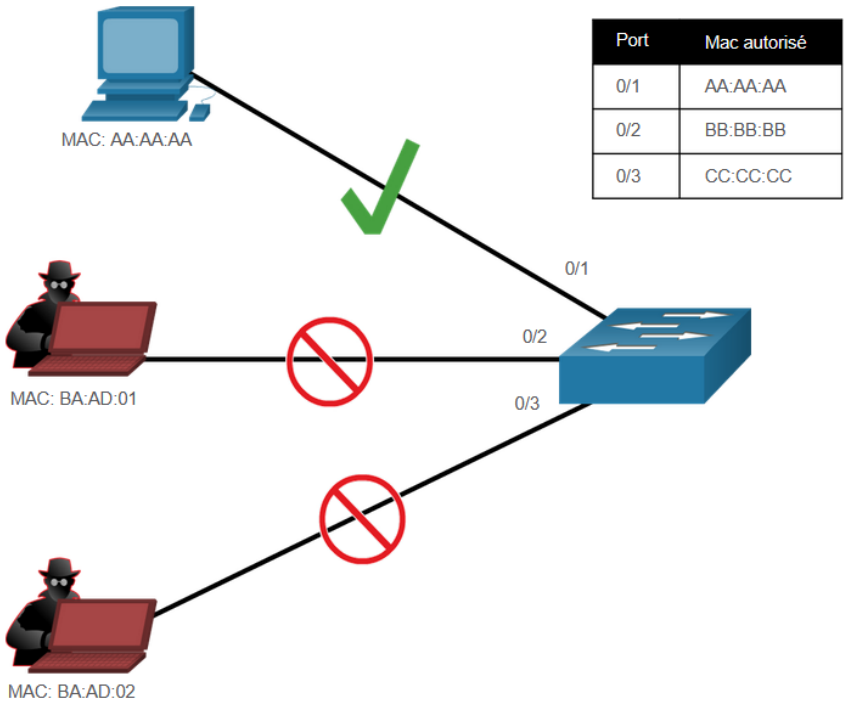
```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
```

2. Atténuation des attaques de table d'adresses MAC

La méthode la plus simple et la plus efficace qui permet d'éviter la saturation des attaques de la table adresse MAC est **d'activer la sécurité des port**s.

La sécurité des ports limite le nombre d'adresses MAC autorisées sur un port. Il permet à un administrateur de configurer manuellement les adresses MAC d'un port ou de permettre au commutateur d'apprendre dynamiquement un nombre limité d'adresses MAC. Lorsqu'un port configuré avec la sécurité des ports reçoit une trame, le système recherche l'adresse MAC source de la trame dans la liste des adresses source sécurisées qui ont été configurées manuellement ou automatiquement (par apprentissage) sur le port.

En limitant le nombre d'adresses MAC autorisées sur un port à un, la sécurité du port peut être utilisée pour contrôler l'accès non autorisé au réseau, comme illustré dans la figure.



Port	Mac autorisé
0/1	AA:AA:AA
0/2	BB:BB:BB
0/3	CC:CC:CC

Remarque: Les adresses MAC sont représentées comme 24 bits pour la simplicité.

3. Activer la sécurité des ports

Notez que dans l'exemple, la commande **switchport port-security** a été refusée. En effet, la sécurité des ports ne peut être configurée que sur des ports d'accès configurés manuellement ou des ports de trunc de réseau configurés manuellement. Par défaut, les ports de commutateur de couche 2 sont réglés sur l'auto dynamique (trunking activée). Par conséquent, dans l'exemple, le port est configuré avec la commande de configuration de l'interface **switchport mode access** .

Remarque : la sécurité des ports trunc dépasse le cadre de ce cours.

```
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#
```

Exécutez la commande **show port-security interface**pour afficher les paramètres de sécurité de port actuels pour FastEthernet 0/1, comme illustré dans l'exemple. Notez comment la sécurité des ports est activée, le mode de violation est arrêté et comment le nombre maximal d'adresses MAC est 1. Si un périphérique est connecté au port, le commutateur ajoute automatiquement l'adresse MAC du périphérique en tant que MAC sécurisé. Dans cet exemple, aucun périphérique n'est connecté au 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#
```

Remarque: si un port actif est configuré avec la commande **switchport port-security** et que plusieurs périphériques sont connectés à ce port, le port passera à l'état désactivé par erreur. Cette condition est abordée plus tard dans cette rubrique.

Une fois la sécurité des ports est activée, d'autres spécificités de sécurité des ports peuvent être configurées, comme illustré dans l'exemple.

```
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode <cr>
S1(config-if)# switchport port-security
```

4. Limiter et apprendre les adresses MAC

Pour définir le nombre maximal d'adresses MAC autorisées sur un port, utilisez la commande suivante :

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

La valeur de sécurité du port par défaut est 1. Le nombre maximal d'adresses MAC sécurisées qui puissent être configurées dépend du commutateur et de l'IOS. Dans cet exemple, le maximum est 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Le commutateur est configuré pour en savoir plus sur les adresses MAC sur un port sécurisé de trois manières :

1. Configuration manuelle

L'administrateur configure manuellement une ou des adresses MAC statiques à l'aide de la commande suivante pour chaque adresse MAC sécurisée sur le port :

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

2. Apprentissage dynamique

Lorsque la commande **switchport port-security** est exécutée, le MAC source actuel pour le périphérique connecté au port est automatiquement sécurisé mais n'est pas ajouté à la configuration en cours. Si le commutateur est redémarré, le port devra réapprendre l'adresse MAC du périphérique.

3. Apprentissage dynamique - Sticky

L'administrateur peut activer le commutateur pour apprendre dynamiquement l'adresse MAC et le «coller» à la configuration en cours en utilisant la commande suivante:

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

En conservant la configuration en cours, l'apprentissage dynamique d'adresse MAC sera enregistrée dans la NVRAM.

L'exemple illustre une configuration complète de sécurité de port pour FastEthernet 0/1. L'administrateur spécifie un maximum de 4 adresses MAC, configure manuellement une adresse MAC sécurisée, puis configure le port pour apprendre dynamiquement des adresses MAC sécurisées supplémentaires jusqu'à 4 adresses MAC sécurisées au maximum. Utilisez les commandes **show port-security interface** et **show port-security address** pour vérifier la configuration.

```
*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#
```

The output of the **show port-security interface** command verifies that port security is enabled, there is a host connected to the port (i.e., Secure-up), a total of 2 MAC addresses will be allowed, and S1 has learned one MAC address statically and one MAC address dynamically (i.e., sticky).

The output of the **show port-security address** command lists the two learned MAC addresses.

5. Obsolescence de la sécurité des ports

L'obsolescence de la sécurité des ports peut être utilisée pour définir le temps d'obsolescence des adresses sécurisées statiques et dynamiques sur un port. Deux types d'obsolescence sont pris en charge par port:

- **Absolue** - Les adresses sécurisées sur le port sont supprimées après le temps d'obsolescence spécifié.
- **Inactivité** - Les adresses sécurisées sur le port sont supprimées uniquement si elles sont inactives pendant la durée d'obsolescence spécifiée.

Utilisez l'obsolescence pour supprimer les adresses MAC sécurisées sur un port sécurisé sans supprimer manuellement les adresses MAC sécurisées existantes. Les limites de temps d'obsolescence peuvent également être augmentés pour garantir que les anciennes adresses MAC sécurisées persistent, même lorsque de nouvelles adresses MAC sont ajoutées. l'obsolescence des adresses sécurisées configurées statiquement peut être activé ou désactivé par port.

Exécutez la commande **switchport port-security aging** pour activer ou désactiver l'obsolescence statique pour le port sécurisé, ou pour définir le temps ou le type d'obsolescence.

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

Les paramètres de la commande sont décrits dans le tableau.

Paramètre Description staticEnable aging pour les statiques sécurisés configurés adresses sur ce port.time time Spécifiez le temps d'obsolescence pour ce port. La gamme est de 0 à 1440 minutes. Si le temps est 0, aging est désactivé pour ce port. Saisissez absoluteSet the absolute aging time. Toutes les adresses sécurisées sur ce port expire exactement après le temps (en minutes) spécifié et est supprimé de la liste d'adresses sécurisées.Saisissez inactivitySet the inactivity aging Saisissez : Les adresses sécurisées sur ce port ne vieillissent que s'il n'y a pas de données le trafic provenant de l'adresse source sécurisée pour la période spécifiée.

Paramètre	Description
statique	Activez la commande aging pour les adresses sécurisées configurées statiquement sur ce port.
time *time*	Spécifiez aging time pour ce port. La gamme est de 0 à 1440 minutes. Si le temps est 0, aging est désactivé pour ce port.
Aging Type : Absolute	Réglez Absolute Aging Type Toutes les adresses sécurisées sur l'âge de ce port expire exactement après le temps (en minutes) spécifié et sont supprimés de la liste d'adresse sécurisé.
Aging Type : Inactivity	Réglez Inactivity Aging Type Les adresses sécurisées sur ce port expirent uniquement s'il n'y a pas de trafic de données provenant de l'adresse source sécurisée pour une période de temps spécifiée.

Remarque: Les adresses MAC sont représentées comme 24 bits pour la simplicité.

L'exemple montre un administrateur configurant le type d'obsolescence (aging type) à 10 minutes d'inactivité et en exécutant la commande **show port-security interface** pour vérifier la configuration.

```
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#
```

6. Modes de Violation de la Sécurité des Ports

Si l'adresse MAC d'un périphérique connecté au port est différent de la liste des adresses sécurisées, alors une violation de port se produit. Par défaut, le port entre l'état error-disabled.

Pour définir le mode de violation de sécurité du port, exécutez la commande suivante:

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

Le tableau suivant indique la réaction d'un commutateur selon le mode de violation configuré.

6.1. Descriptions du Mode de Violation de la Sécurité

Mode	Description
Démarrer (par défaut)	Le port passe immédiatement à l'état désactivé par erreur, éteint le voyant du port et envoie un message Syslog. Il incrémente le compteur de violations. Compteur Lorsqu'un port sécurisé est dans l'état désactivé par erreur, un administrateur doit le réactiver en entrant le **shutdown** et **no shutdown** commands.
restreindre	Le port supprime les paquets avec des adresses source MAC inconnues jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour descendre en dessous du maximum valeur ou augmentez la valeur maximale. Ce mode provoque la

	sécurité de violation compteur pour augmenter et générer un message syslog.
protéger	Il s'agit du mode de violation de sécurité le moins sécurisé. Le port supprime les paquets avec des adresses source MAC inconnues jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour descendre en dessous du maximum ou augmentez la valeur maximale. No syslog message est envoyé.

6.2. Comparaison du mode de violation de la sécurité

Mode de Violation	Rejeter un trafic illégal	Envoi d'un message Syslog	Incrémentation du Compteur de Violation	Arrêt du port
Protéger	Oui	Non	Non	Non
Restreindre	Oui	Oui	Oui	Non
Arrêt	Oui	Oui	Oui	Oui

L'exemple indique qu'un administrateur modifie la violation de sécurité pour «Restreindre». Le résultat de commande **show port-security interface** confirme que la modification a été effectuée.

```
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#
```

7. Ports en état error-disabled

Quand un port est arrêté et placé dans l'état error-disabled, aucun trafic n'est envoyé ou reçu sur ce port. Une série de messages liés à la sécurité des ports s'affiche sur la console, comme illustré dans l'exemple suivant.

```
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#
```

Remarque: le protocole du port et l'état de la liaison passent à l'état bas et le voyant du port est éteint.

Dans l'exemple, la commande **show interface** identifie l'état du port comme étant **error-disabled**. Le résultat de la commande **show port-security interface** affiche désormais l'état du port comme étant **secure-shutdown**. Le compteur de violation de sécurité incrémente par 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#
```

L'administrateur doit déterminer la cause de la violation de sécurité. Si un périphérique non autorisé est connecté à un port sécurisé, la menace de sécurité est éliminée avant de réactiver le port.

Pour réactiver le port, utilisez d'abord la commande **shutdown** puis utilisez la commande **no shutdown** pour que le port soit fonctionnel, comme indiqué dans l'exemple.

```
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)#
```

8. Vérification de la sécurité des ports

Après avoir configuré la sécurité des ports sur un commutateur, examinez chaque interface pour vérifier que la sécurité des ports est correctement définie et assurez-vous que les adresses MAC statiques ont été correctement configurées.

Sécurité du port pour toutes les interfaces

Pour afficher les paramètres de sécurité des ports pour un commutateur, utilisez la commande **show port-security**. L'exemple indique que les 24 interfaces sont configurées avec la commande **switchport port-security** car le maximum autorisé est 1 et le mode de violation est arrêté. Aucun appareil n'est connecté. Par conséquent, le CurrentAddr (Count) est 0 pour chaque interface.

```
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#
```

Sécurité du port pour une interface spécifique

Utilisez la commande **show port-security interface** pour afficher les détails d'une interface spécifique, comme indiqué précédemment et dans cet exemple.

```
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#
```

Vérifiez les adresses MAC apprises

Pour vérifier que les adresses MAC «collent» à la configuration, utilisez la commande **show run** comme indiqué dans l'exemple pour 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#
```

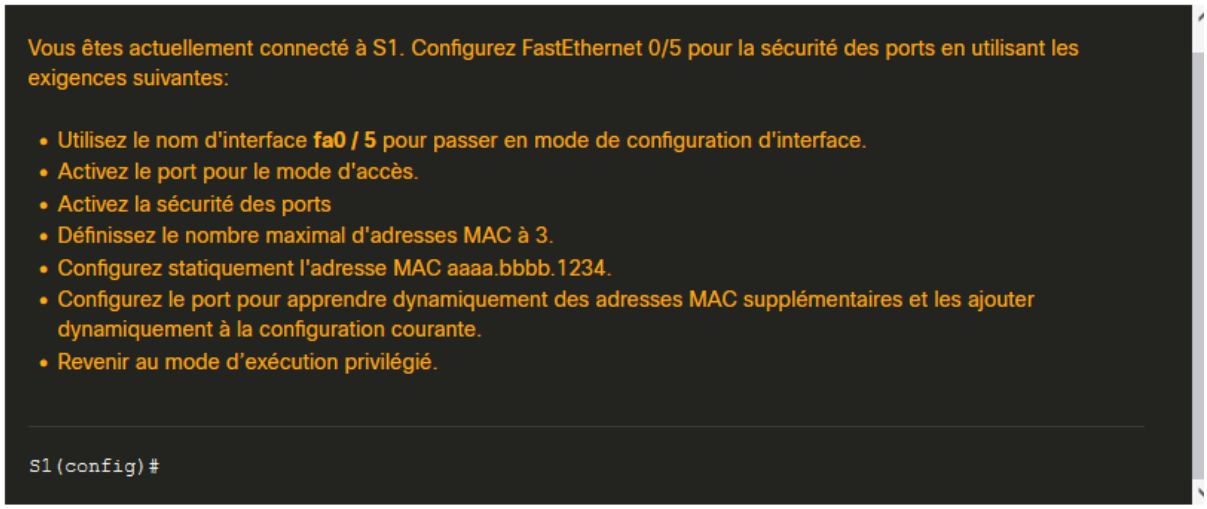
Vérification des adresses MAC sécurisées

Pour afficher toutes les adresses MAC sécurisées configurées manuellement ou apprises dynamiquement sur toutes les interfaces de commutateur, utilisez la commande **show port-security address** comme indiqué dans l'exemple.

```
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#
```

9. Vérificateur de syntaxe - Mettez en œuvre la sécurité des ports

Mettre en œuvre la sécurité des ports pour une interface de commutateur en fonction des exigences spécifiées



10. Mettre en œuvre la sécurité des ports

Avec Packet Tracer, vous pouvez configurer et vérifier la sécurité des ports sur un commutateur. La sécurité des ports vous permet de limiter le trafic d'entrée d'un port en limitant les adresses MAC autorisées à envoyer du trafic sur ce port.