Mettre en œuvre la sécurité des ports

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous réseau
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	Carte réseau (NIC)	10.10.10.10	255.255.255.0
PC2	Carte réseau (NIC)	10.10.10.11	255.255.255.0
Ordinateur portable escroc	Carte réseau (NIC)	10.10.10.12	255.255.255.0

Objectif

Partie 1: Configuration de la sécurité des ports

Partie 2: Vérification de la sécurité des ports

Contexte

Dans cette activité, vous allez 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.

Étape 1: Configuration de la sécurité des ports

a. Accédez à la ligne de commande pour **S1** et activez la sécurité des ports sur les ports Fast Ethernet 0/1 et 0/2.

Commandes saisies et capture d'écran de votre configuration (show run) :

```
S1(config)#interface range f0/1 - 2
S1(config-if-range)#switchport port-security
```

```
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
!
```

b. Optez pour le niveau maximum, de sorte qu'un seul périphérique puisse accéder aux ports Fast Ethernet 0/1 et 0/2.

Commandes saisies et capture d'écran de votre configuration (show run) :

```
S1(config)#interface range f0/1-2
S1(config-if-range)#switchport port-security maximum 1
```

c. Sécurisez les ports de sorte que l'adresse MAC d'un périphérique soit apprise de manière dynamique et ajoutée à la configuration en cours.

Commandes saisies et capture d'écran de votre configuration (show run) :

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

```
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
```

d. Réglez le mode de violation de sorte que les ports Fast Ethernet 0/1 et 0/2 ne soient pas désactivés lorsqu'une violation se produit, mais qu'une notification de la violation de sécurité soit générée et que les paquets de source inconnue soient rejetés.

Commandes saisies et capture d'écran de votre configuration (show run) :

```
S1(config)#interface range f0/1-2
S1(config-if-range)#switchport port-security violation restrict
```

```
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

e. Désactivez tous les ports inutilisés restants. Utilisez le mot clé **range** pour appliquer cette configuration à tous les ports simultanément.

Commandes saisies et capture d'écran de votre configuration (show run) :

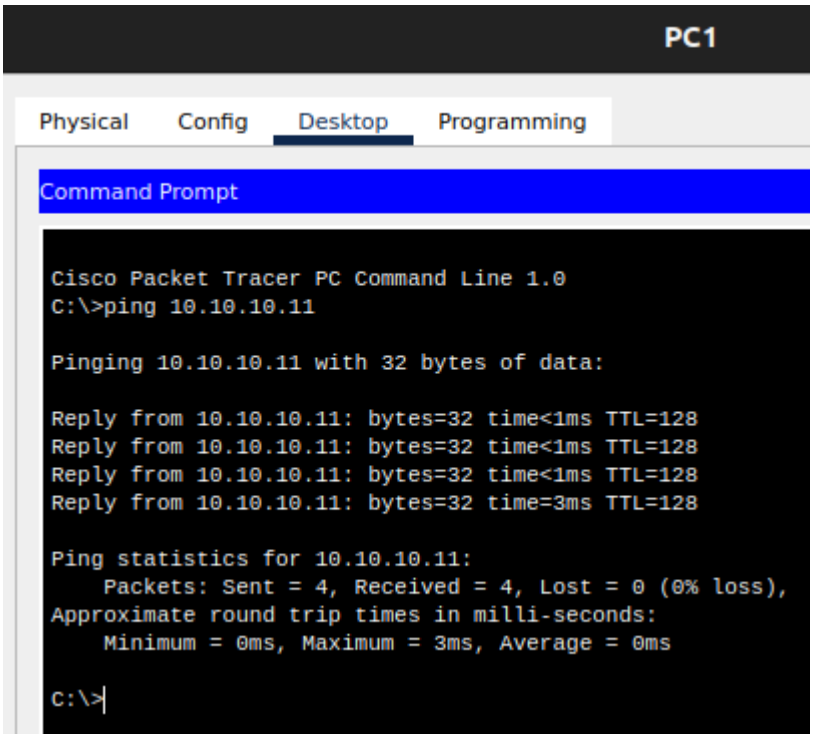
```
S1(config)#interface range f0/1-2
S1(config-if-range)#interface range f0/3 - 24, g0/1 - 2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

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

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down


interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
```

VALIDATION :

Étape 2: Vérification de la sécurité des ports

a. À partir de **PC1**, envoyez une requête ping à **PC2**.

Commandes saisies et capture d'écran :



b. Vérifiez que la sécurité des ports est activée et que les adresses MAC de **PC1** et **PC2** ont été ajoutées à la configuration en cours.

Commandes saisies et capture d'écran de la configuration (show run) :

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.B027.2245
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.647C.697E
!
```

c. Utilisez les commandes show port-security pour afficher les informations de configuration.

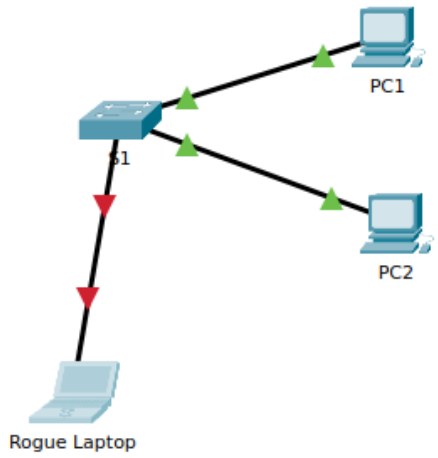
Commandes saisies et capture d'écran de votre configuration (show run) :

```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1          1                0         Restrict
        Fa0/2        1          1                0         Restrict
---------------------------------------------------------------------
```

```
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    00E0.B027.2245    SecureSticky                  Fa0/1         -
   1    0001.647C.697E    SecureSticky                  Fa0/2         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

d. Connectez **Rogue Laptop** à un port de commutateur non utilisé. Vous voyez que les témoins de liaison sont rouges.

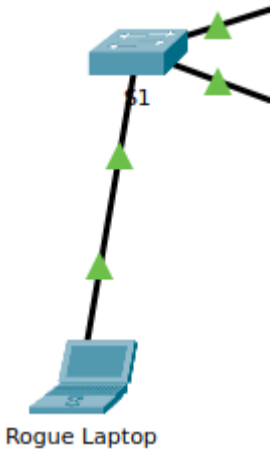
Capture d'écran :



e. Activez le port et vérifiez que **Rogue Laptop** peut envoyer une requête ping à **PC1** et **PC2**. Après cette vérification, arrêtez le port connecté à **Rogue Laptop.**

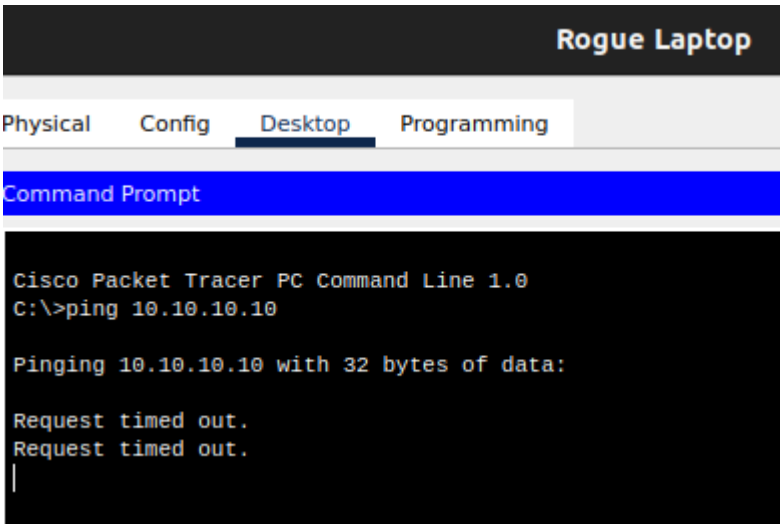
Capture d'écran :

```
S1(config)#interface f0/3
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

S1(config-if)#
```



f. Déconnectez **PC2** et connectez **Rogue Laptop** à F0 / 2, qui est le port auquel PC2 était initialement connecté. Vérifiez que **Rogue Laptop** ne peut pas envoyer de requête ping à **PC1**.

Tests et capture d'écran :



g. Affichez les violations de sécurité du port pour le port auquel **Rogue Laptop** est connecté.

Commandes saisies et capture d'écran :

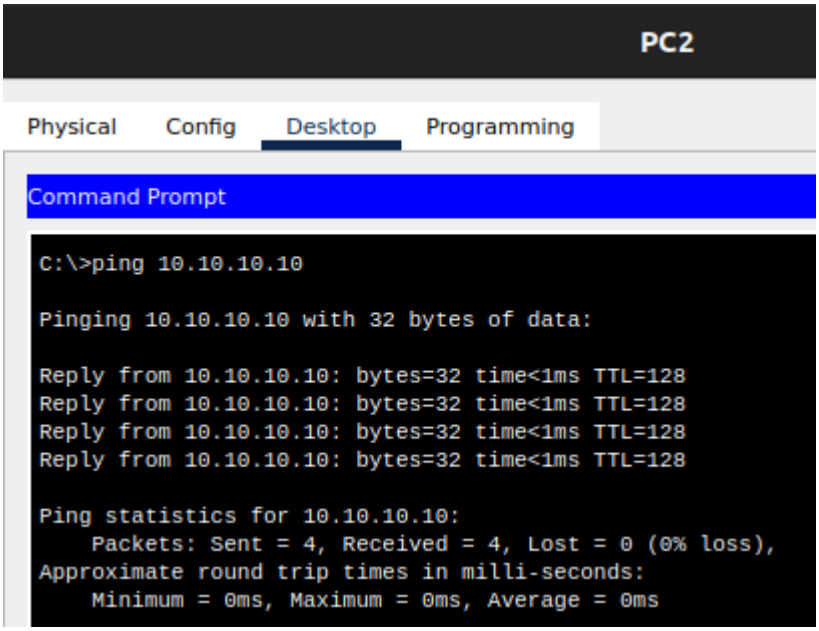
```
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show port-security interface f0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
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       : 1
Last Source Address:Vlan   : 0002.4A42.C51C:1
Security Violation Count   : 5
```

Combien de violations se sont produites?

Il y a 5 violations de sécurité.

h. Déconnectez **Rogue Laptop** et reconnectez **PC2**. Vérifiez que **PC2** peut envoyer une requête ping à **PC1**.

Pourquoi **PC2** peut envoyer une requête ping à **PC1** alors que **Rouge Laptop** ne peut pas?



La sécurité du port permettait uniquement au premier appareil détecté (via son adresse MAC) d'y accéder et bloque tous les autres.

VALIDATION :