Packet Tracer - 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.

## Configuration de la sécurité des ports

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

Ouvrez la fenêtre de configuration.

S1(config)# **interface range f0/1 – 2**

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

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

S1(config-if-range)# **switchport port-security maximum 1**

* + 1. Sécurisez les ports de sorte que l'adresse MAC d'un périphérique soit apprise de manière dynamique et ajoutée à la configuration en cours.

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

* + 1. 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.

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

* + 1. Désactivez tous les ports inutilisés restants. Utilisez le mot clé **range** pour appliquer cette configuration à tous les ports simultanément.

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

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

## Vérification de la sécurité des ports

* + 1. À partir de **PC1**, envoyez une requête ping à **PC2**.
    2. 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.

S1# **show run | begin interface**

* + 1. Utilisez les commandes show port-security pour afficher les informations de configuration.

S1# **show port-security**

S1# **show port-security address**

* + 1. Connectez **Rogue Laptop** à un port de commutateur inutilisé. Vous voyez que les témoins de liaison sont rouges.
    2. 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.**
    3. 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**.
    4. Affichez les violations de sécurité du port pour le port auquel **Rogue Laptop** est connecté.

S1# **show port-security interface f0/2**

Fermez la fenêtre de configuration.

### Question:

Combien de violations se sont produites?

Sai

sissez vos réponses ici

* + 1. Déconnectez **Rogue Laptop** et reconnectez **PC2**. Vérifiez que **PC2** peut envoyer une requête ping à **PC1**.

### Question:

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

Saisissez vos réponses ici