

Configuration de la sécurité des ports de commutateur

Topologie

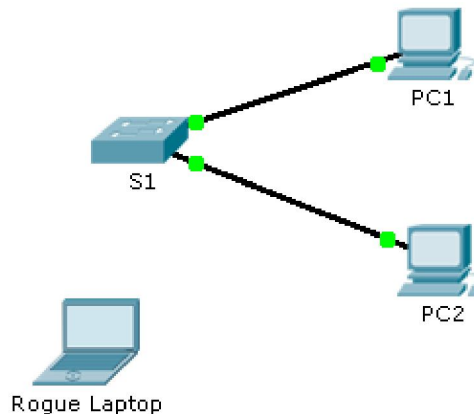


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Objectifs

Partie 1 : configuration de la sécurité des ports

Partie 2 : vérification de la sécurité des ports

Contexte

Dans cet exercice, 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.

Partie 1 : Configuration de la sécurité des ports

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

```
S1(config)# interface range fa0/1 - 2
```

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

- 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
```

Packet Tracer : configuration de la sécurité des ports de commutateur

- 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.

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

- d. Définissez la violation de sorte que les ports Fast Ethernet 0/1 et 0/2 ne soient pas désactivés en cas de violation, mais que les paquets soient abandonnés s'ils proviennent d'une source inconnue.

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

- e. Désactivez tous les ports inutilisés restants. Indice : utilisez le mot-clé **range** pour appliquer cette configuration à tous les ports simultanément.

```
S1(config-if-range) # interface range fa0/3 - 24 , gi1/1 - 2
```

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

Partie 2 : Vérification de la sécurité des ports

- a. À partir de **PC1**, envoyez une requête ping à **PC2**.
- 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.
- c. Connectez **Rogue Laptop** à un port de commutateur inutilisé. Vous voyez que les témoins de liaison sont rouges.
- d. 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**.
- e. Déconnectez **PC2** et connectez **Rogue Laptop** au port de **PC2**. Vérifiez que **Rogue Laptop** ne peut pas envoyer de requête ping à **PC1**.
- f. Affichez les violations de sécurité du port auquel le périphérique **Rogue Laptop** est connecté.

```
S1# show port-security interface fa0/2
```

- g. Déconnectez **Rogue Laptop** et reconnectez **PC2**. Vérifiez que **PC2** peut envoyer une requête ping à **PC1**.
- h. Pourquoi **PC2** peut envoyer une requête ping à **PC1** alors que **Rogue Laptop** ne peut pas ? La sécurité des ports qui a été activée sur le port a autorisé l'accès uniquement au périphérique dont l'adresse MAC a été apprise au début et l'a interdit aux autres.