Packet Tracer - Configuration de la Sécurité de Commutateur

Tableau de VLAN

| Commutateur | Numéro de VLAN | Nom du VLAN | Appartenances des ports | Réseau |
| --- | --- | --- | --- | --- |
| SW-1 | 10 | Admin | F0/1, F0/2 | 192.168.10.0/24 |
| SW-1 | 20 | Commercial | F0/10 | 192.168.20.0/24 |
| SW-1 | 99 | Gestion | F0/24 | 192.168.99.0/24 |
| SW-1 | 100 | Natif | G0/1, G0/2 | Aucun |
| SW-1 | 999 | BlackHole | Tous inutilisés | Aucun |
| SW-2 | 10 | Admin | F0/1, F0/22 | 192.168.10.0/24 |
| SW-2 | 20 | Ventes | F0/10 | 192.168.20.0/24 |
| SW-2 | 99 | Gestion | F0/24 | 192.168.99.0/24 |
| SW-2 | 100 | Natif | Aucun | Aucun |
| SW-2 | 999 | BlackHole | Tous inutilisés | Aucun |

# Objectifs

Partie 1 : Créer un trunc sécurisé.

Partie 2 : Sécuriser les ports du commutateur inutilisés.

Partie 3 :Mettre en œuvre La sécurité des Ports.

Partie 4 : Activer L'espionnage (snooping) DHCP.

Partie 5 : Configurer Rapid PVST+, PortFast et la protection BPDU.

# Contexte

Vous améliorez la sécurité sur deux commutateurs d'accès dans un réseau partiellement configuré. Vous mettez en œuvre la gamme de mesure de sécurité qui a été présenté dans ce module selon les exigences ci-dessous. Notez que le routage a été configuré sur ce réseau, donc la connectivité entre les hôtes sur différents VLAN devrait fonctionner quand terminée.

# Instructions

## Créer un trunc sécurisé.

* + - 1. Connectez les ports G0/2 des deux commutateurs de couche d'accès.
      2. Configurez les ports G0/1 et G0/2 comme truncs statiques sur les deux commutateurs.
      3. Désactivez la négociation DTP sur les deux côtés de la liaison.
      4. Créez le VLAN 100 et lui attribuez le nom Native sur les deux commutateurs.
      5. Configurez tous les ports de trunc sur les deux commutateurs pour utiliser VLAN 100 comme VLAN natif.

## Sécuriser Les Portes du Commutateur Inutilisés.

* + - 1. Désactivez tous les ports de commutateur inutilisés sur SW-1.
      2. Sur SW1, créez le VLAN 999 et nommez-le BlackHole. Le nom configuré doit correspondre exactement à l'exigence.
      3. Déplacez tous les ports de commutateur inutilisés vers le VLAN BlackHole.

## Mettre en œuvre la sécurité des ports.

* + - 1. Activez la sécurité des ports sur tous les ports d'accès actifs du commutateur SW-1.
      2. Configurez les ports actifs pour permettre l'apprentissage d'un maximum de 4 adresses MAC sur les ports.
      3. Pour les ports F0 / 1 sur SW-1, configurez statiquement l'adresse MAC du PC à l'aide de la sécurité des ports.
      4. Configurez chaque port d'accès actif afin qu'il ajoute automatiquement les adresses MAC apprises sur le port à la configuration courante.
      5. Configurez le mode de violation de sécurité des ports pour abandonner les paquets des adresses MAC qui dépassent le maximum, générer une entrée Syslog, mais pas désactiver les ports.

## Configurer L'espionnage (snooping) DHCP

* + - 1. Configurez les portes trunc sur SW-1 comme des ports approuvés.
      2. Limitez les ports non approuvés sur SW-1 à cinq paquets DHCP par seconde.
      3. Sur SW-2, activez l'espionnage DHCP globalement pour les VLAN 10, 20 et 99.

**Remarque :** La configuration d'espionnage (snooping) DHCP ne peut pas noter correctement dans Packet Tracer.

## Configurer PortFast et la protection BPDU.

* + - 1. Activez PortFast sur tous les ports d'accès utilisés sur SW-1.
      2. Activez la protection BPDU (BPDU Guard) sur tous les ports d'accès utilisés sur SW-1.
      3. Configurez SW-2 pour que tous les ports d'accès utilisent PortFast par défaut.

Fin du document