Table des matières

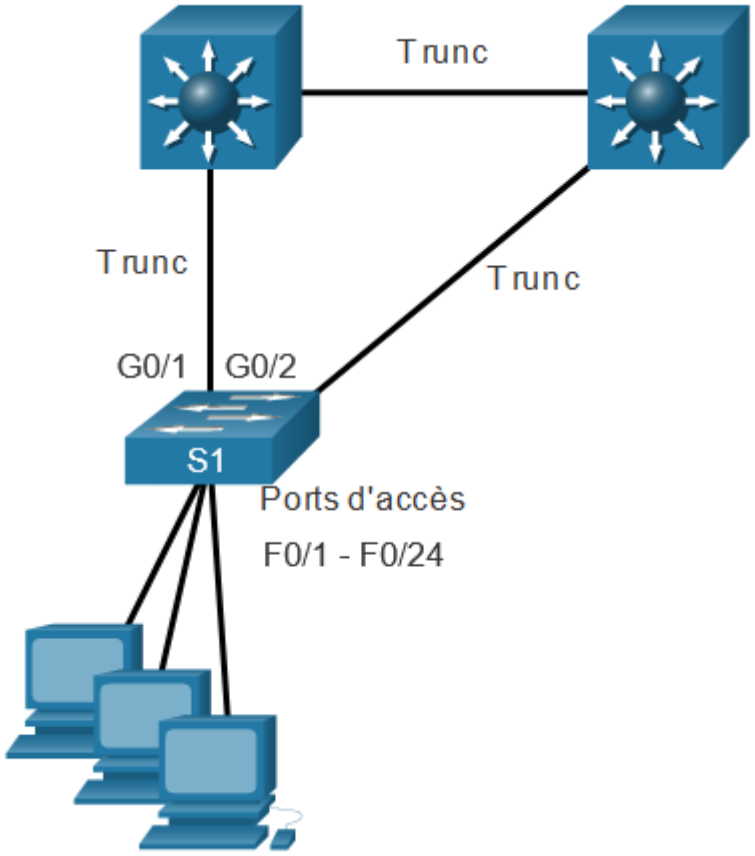
Atténuer les attaques du STP

1. PortFast et protection BPDU

Rappelez-vous que les attaquants du réseau peuvent manipuler le protocole STP (Spanning Tree Protocol) pour mener une attaque en usurpant le pont racine et en modifiant la topologie d'un réseau. Pour atténuer les attaques de manipulation du protocole Spanning Tree (STP), utilisez PortFast et Bridge Protocol Data Unit (BPDU) Garde :

- **PortFast** - Avec PortFast, une interface configurée comme un port d'accès ou trunc passe immédiatement de l'état de blocage à celui de transfert, et contourne ainsi les situations d'écoutes et d'apprentissages. Appliquer à tous les ports d'utilisateur final. PortFast ne doit pas être configuré que sur les ports connectés aux périphériques finaux.
- **BPDU Guard** - Une erreur de BPDU guard désactive immédiatement un port qui reçoit un BPDU. Comme PortFast, BPDU guard ne doit pas être configuré que sur les ports connectés aux périphériques finaux.

Dans la figure, les ports d'accès pour S1 doivent être configurés avec PortFast et BPDU Guard.



2. Configurer PortFast

PortFast contourne les situations d'écoute et d'apprentissage STP pour limiter le temps que les ports d'accès doivent attendre que STP se converge. Si PortFast est activé sur un port connecté à un autre commutateur, alors il y en a un risque de créer une boucle Spanning Tree.

PortFast peut être activée alternativement sur une interface avec la commande de configuration **spanning-tree portfast** . Alternativement, PortFast peut être configurée sur tous les ports non trunc avec la commande de configuration globale **spanning-tree portfast default** .

Pour vérifier si PortFast est activé globalement, vous pouvez utiliser la commande **show running-config | commande begin span** ou la commande **show spanning-tree summary** . Pour vérifier si PortFast est activé sur l'interface, utilisez la commande **show running-config interface** *type / number*, comme indiqué dans l'exemple suivant. La commande **show spanning-tree interface** *type/number* **detail** peut également être utilisée pour la vérification.

Notez que lors PortFast est active, les messages d'avertissement s'affichent.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

3. Configuration BPDU Guard

Même si PortFast est activé, l'interface écoutera toujours les BPDU. Les BPDU inattendus peuvent être accidentels ou faire partie d'une tentative non autorisée d'ajouter un commutateur au réseau.

Si une BPDU est reçue sur un port d'accès activé par BPDU Guard, le port est mis en état désactivé par erreur. Cela signifie que le port est arrêté et doit être réactivé manuellement ou récupéré automatiquement par la commande globale **errdisable recovery cause psecure_violation**.

BPDU Guard peut être activé sur un port à l'aide de la commande de configuration d'interface **spanning-tree bpduguard enable**. Autrement, utiliser la commande de configuration globale **spanning-tree portfast bpduguard default** pour activer globalement la protection BPDU sur tous les ports où PortFast est activée.

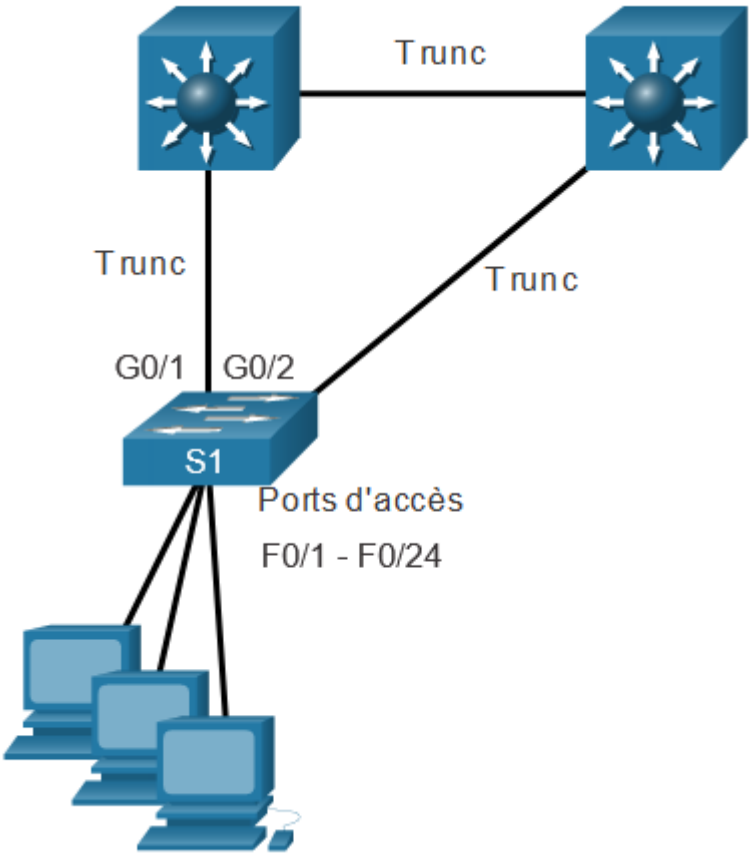
Pour afficher des informations sur l'état du spanning tree, utilisez la commande **show spanning-tree summary**. Dans l'exemple, PortFast par défaut et BPDU Guard sont activés comme situation par défaut pour les ports configurés en mode d'accès.

Remarque: Activez toujours BPDU Guard sur tous les ports activés par PortFast.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

4. Exercice Atténuer les attaques STP

Mettez en œuvre Portfast et BPDU Guard pour un commutateur en fonction de la topologie suivante et des exigences spécifiées.



Vous êtes actuellement connecté à S1. Complétez les étapes suivantes pour implémenter PortFast et BPDU Guard sur tous les ports d'accès:

- Passez en mode de configuration d'interface pour **fa0/1 – 24**.
- Configurez le port en mode d'accès.
- Repassez en mode de configuration globale.
- Activez Portfast par défaut sur tous les ports d'accès.
- Activez BPDU Guard par défaut sur tous les ports d'accès.