Timothée SICCHIA

MEWO  23/10/2024

Initiation spanning-tree

**Optimisez votre réseau**

Dans une entreprise, il est fréquent d'ajouter des commutateurs en fonction de sa croissance pour répondre aux besoins. Par exemple, pour préparer l'arrivée d'un nouvel employé, installer une imprimante supplémentaire ou mettre en place des caméras de surveillance...

Ces commutateurs peuvent être ajoutés à chaque étage ou pour chaque service, chaque fois que cela est nécessaire. Souvent, ces commutateurs sont interconnectés, ce qui est une pratique recommandée. En effet, cela évite la congestion des données et offre une redondance des chemins réseau. C'est précisément cette redondance qui peut poser problème en créant trois types d'incidents :

* Des tempêtes de diffusion (broadcast storm),
* Des duplications de trames,
* Une instabilité des tables MAC.

Ces trois problèmes sont en fait causés par un seul et même phénomène : les boucles réseau. Explorons ce sujet plus en profondeur !

**Le problème des boucles réseau**

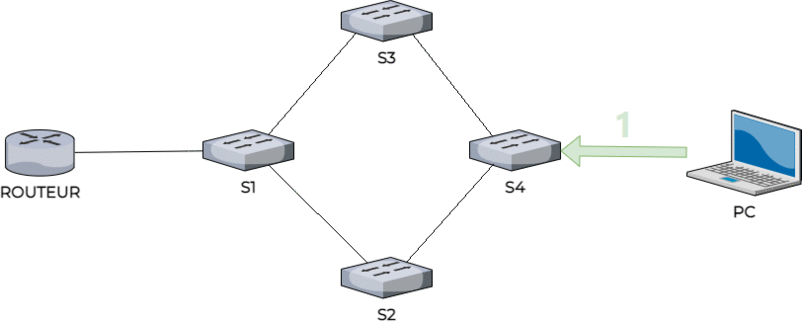
Imaginons une topologie dans laquelle les commutateurs 2 et 3 sont configurés pour assurer une protection en cas de panne :

Une image contenant ordinateur, capture d’écran, conception

Description générée automatiquement

**1. Les tempêtes de diffusion**

Lorsque notre architecture est en place, voyons ce qu’il se passe si le PC-1 envoie une requête DHCP (DHCP DISCOVER), un message de type broadcast, au routeur qui agit en tant que serveur DHCP.



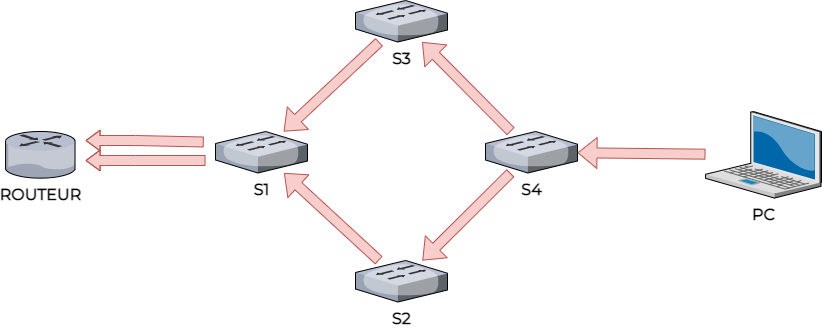
Le commutateur 4 reçoit la trame du PC-1 et la diffuse sur tous ses ports, ce qui est normal pour une adresse de diffusion, elle est destinée à tous les appareils.

Les commutateurs 2 et 3 reçoivent également cette trame et la diffusent à leur tour sur tous leurs ports, l'envoyant ainsi au commutateur 1 mais aussi au commutateur 4, qui l'avait initialement envoyée.

Résultat : les quatre commutateurs continuent de s'envoyer en boucle la trame DHCP du PC-1, consommant inutilement les ressources CPU des commutateurs.

**2. Les duplications de trame**

Ce problème est similaire au premier, mais au lieu de se répéter indéfiniment, la trame est dupliquée deux fois, du PC-1 au routeur. Imaginons cette fois que le PC-1 connaisse l'adresse IP du serveur et veuille lui envoyer une trame.



Duplication de trame

Le commutateur 4 reçoit la trame et détecte qu'il a l'adresse MAC du serveur dans sa table, il lui envoie donc le message. Cependant, les commutateurs 2 et 3 effectuent la même opération, ce qui conduit le commutateur 1 à envoyer deux fois le même message, et le routeur à recevoir deux fois la trame.

**3. L’instabilité des tables MAC**

Prenons à nouveau l'exemple de la duplication des trames, mais concentrons-nous cette fois sur les tables MAC plutôt que sur la trame elle-même.

Une image contenant ordinateur, capture d’écran, conception

Description générée automatiquement

Imaginons que les tables MAC des quatre commutateurs soient vides.

|  |  |  |
| --- | --- | --- |
| **SWITCH 2** | **PORTS** | **ADRESSE MAC** |
|  | **1** | **?** |
|  | **2** | **?** |
| **SWITCH 3** | **PORTS** | **ADRESSE MAC** |
|  | **1** | **?** |
|  | **2** | **?** |

Lorsqu'une trame en provenance du routeur arrive sur le commutateur 3, celui-ci met à jour sa table avec l'adresse MAC du routeur, et le commutateur 2 fait de même.

Chaque commutateur veut envoyer la trame vers le PC-1, mais aucun ne sait encore où se trouve le PC-1, car il n’est pas dans leurs tables MAC. Ils diffusent donc la trame sur tous leurs ports, sauf celui par lequel ils ont reçu la trame.

|  |  |  |
| --- | --- | --- |
| **SWITCH 2** | **PORTS** | **ADRESSE MAC** |
|  | **1** | **?** |
|  | **2** | **Adresse MAC du routeur** |
| **SWITCH 3** | **PORTS** | **ADRESSE MAC** |
|  | **1** | **?** |
|  | **2** | **Adresse MAC du routeur** |

Finalement, les tables MAC se mettent à jour en boucle, ce qui entraîne une surcharge inutile des ressources CPU des commutateurs.

**Simulons le problème en désactivant le spanning-tree**

Pour vérifier cela, nous allons désactiver le protocole spanning-tree qui est censé empêcher ces problèmes de survenir (il est activé par défaut sur les appareils Cisco) en utilisant la commande :

(config)# no spanning-tree vlan 1-4094

Ensuite, exécutez un ping du routeur vers le PC-1 et vérifiez l'état du CPU des commutateurs avec la commande suivante :

show processes cpu

Vous constaterez rapidement une montée en flèche de l'utilisation du CPU, les commutateurs deviendront de plus en plus lents, jusqu'à atteindre 100 % d'utilisation et planter. La seule solution sera alors de les redémarrer.

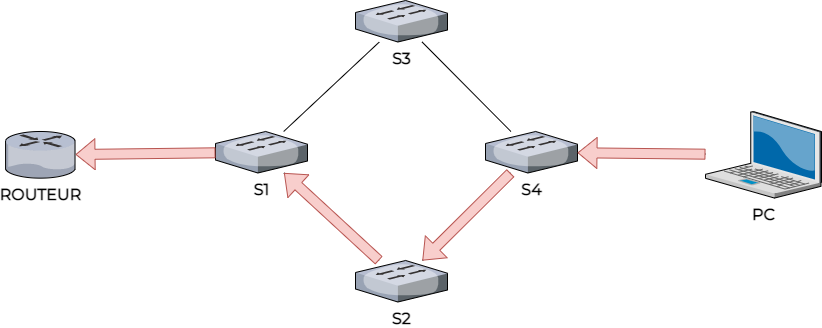
**Appliquez la solution**

La solution à ces problèmes consiste à configurer le protocole spanning-tree. Mais avant cela, voyons comment il fonctionne.

**Créez un seul chemin**

Le principe du spanning-tree est simple. Il consiste à élire un seul chemin pour les communications entre le PC-1 et le routeur, en bloquant certains ports au niveau logique. Si un commutateur tombe en panne, le chemin change automatiquement. Dans cet exemple, nous allons sélectionner le commutateur 2 comme étant celui par lequel passe le chemin principal entre le PC et le routeur.

Ce qui nous donne :



Spanning-tree

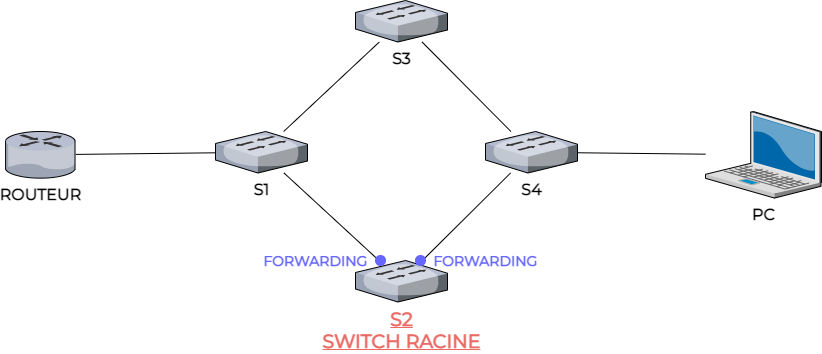
Voyons donc comment cela se passe.

**L'algorithme spanning-tree**

L'algorithme de spanning-tree est conçu pour trouver le chemin le plus court possible entre deux points du réseau.

Pour cela, il commence par l’élection d’un commutateur racine, appelé **switch racine** ou **root**. Ce dernier est sélectionné en fonction de son identifiant **BID (Bridge ID)**, composé de l'adresse MAC du commutateur et d'une priorité. Le commutateur avec le BID le plus bas sera choisi comme root.

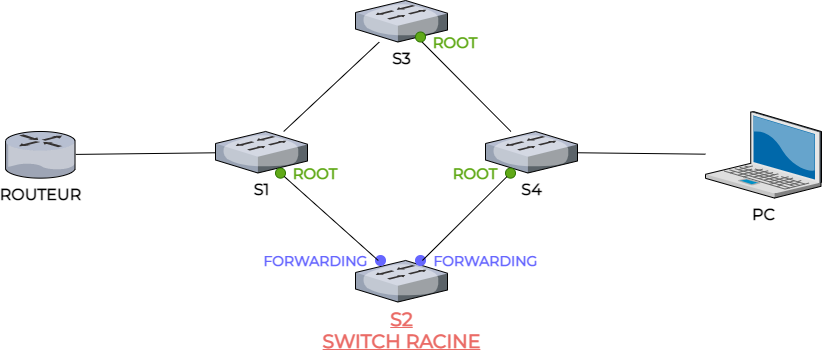
(config)#spanning-tree vlan vlan-id priority priority



Spanning-tree et ports forwarding

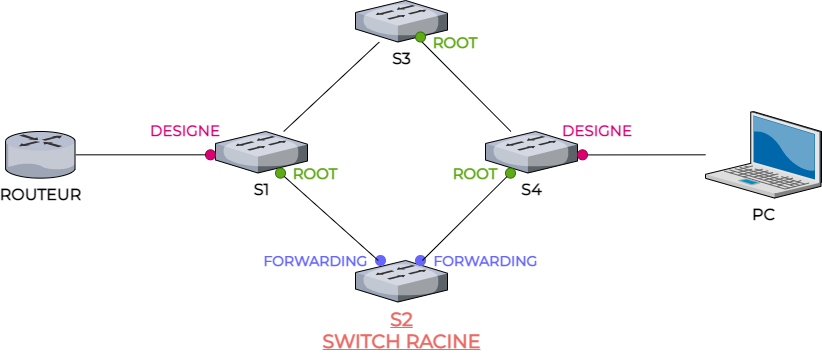
Tous les autres commutateurs du réseau vont choisir un port qui les relie au commutateur racine de la manière la plus rapide possible. Ce port est appelé **port root**. Le chemin est évalué en fonction de la rapidité de la connexion entre les commutateurs. Plus la connexion est rapide, plus le coût est faible. Ce coût peut être ajusté si vous voulez forcer le passage par un chemin spécifique plutôt qu'un autre.

(config-if)#spanning-tree cost <cost>



Spanning-tree et ports root

Le protocole spanning-tree désignera ensuite les ports qui permettent aux terminaux (comme les PC) de se connecter au switch racine le plus rapidement possible. Ces ports sont appelés **ports désignés**.



Spanning-tree et ports désignés

Les ports qui ne sont ni des **ports root**, ni des **ports désignés** seront automatiquement bloqués par le protocole spanning-tree pour éviter les boucles.

Si un commutateur tombe en panne, ces quatre étapes sont répétées rapidement afin de rétablir un chemin fonctionnel. Le protocole spanning-tree envoie régulièrement des messages broadcast appelés **Bridge Protocol Data Units (BPDU)** pour surveiller l’état du réseau et maintenir la topologie à jour. Ces messages signalent deux choses :

* La configuration de la topologie réseau (pour maintenir l’arbre spanning-tree),
* Les changements dans la topologie (comme la déconnexion d'un lien ou la panne d'un commutateur).

**Mettez-le en pratique**

La mise en pratique va consister à :

* **Activation du spanning-tree :** Activez le protocole spanning-tree sur votre réseau avec la commande suivante :

Switch# configure terminal

Switch(config)# spanning-tree vlan 1

Switch(config)# end

Switch#

* **Définir un commutateur racine (root) :** Pour choisir le commutateur principal (root) du réseau, ici le commutateur 2, utilisez la commande suivante :

Switch# configure terminal

Switch(config)# spanning-tree vlan 1 root primary

Switch(config)# end

Switch#

* **Choisir un commutateur racine secondaire :** Pour avoir un commutateur de secours (root secondaire) en cas de défaillance du premier, sélectionnez le commutateur 3 avec cette commande :

Switch# configure terminal

Switch(config)# spanning-tree vlan 1 root secondary

Switch(config)# end

Switch#

**Vérifier la configuration :** Pour vérifier l’état du spanning-tree sur votre réseau, utilisez la commande suivante :

show spanning-tree

Vous devriez voir une sortie similaire à celle-ci :

VLAN0001

Spanning tree enabled protocol rstp

Root ID    Priority    24577                 (C’est la priorité du switch root, celle que vous avez définie avec la commande spanning-tree vlan 1 root priority)

Address     00bb.f94d.d900      (C’est l’adresse du switch root, le switch 2)

Cost        8

Port        2 (GigabitEthernet0/1)        (le port root du switch 3)

Hello Time   2 sec Max Age 20 sec  Forward Delay 15 sec (les BPDU sont envoyé toutes les 2 secondes si il n’y a pas de réponse au bout de 20 secondes on change le spanning-tree)

Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)

Address     00bb.f97f.3400

Hello Time   2 sec Max Age 20 sec  Forward Delay 15 sec

Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type

------------------- ---- --- --------- -------- --------------------------------

Gi0/0               Altn BLK 4         128.1    Shr            (il s’agit du port bloqué)

Gi0/1               Root FWD 4         128.2    Shr

Gi0/2               Desg FWD 4         128.3    Shr

Ici j’ai tapé la commande **show spanning-tree** sur le switch 3.

Vous avez enfin les deux composants vous permettant d’administrer votre réseau et savez les paramétrer pour votre LAN :

* Le switch, pour relier vos appareils du même réseau
  + VLAN
  + spanning-tree
  + VLAN interface
* et le routeur pour interconnecter deux réseaux différents
  + routage fixe
  + sub-interface
  + DHCP
  + NTP
  + NAT

**En résumé**

Pour garantir la performance et la sécurité de votre réseau, il est crucial de créer des chemins redondants en ajoutant des commutateurs pour relier différentes parties du réseau. Cependant, sans le protocole spanning-tree, cette redondance peut causer des problèmes tels que :

* Des tempêtes de diffusion,
* La duplication des messages,
* L’instabilité des tables MAC.

Le protocole spanning-tree résout ces problèmes en bloquant les boucles réseau. Il crée un chemin unique à travers le réseau, en procédant aux étapes suivantes :

1. Sélection d’un commutateur racine (root),
2. Sélection d’un commutateur de secours,
3. Choix des chemins les plus courts vers le commutateur racine,
4. Blocage des ports inutiles.

Il est également possible d’influencer les décisions du protocole en ajustant les priorités des commutateurs et le coût des liens avec les commandes suivantes :

spanning-tree vlan 1 root priority;

spanning-tree vlan 1 root secondary.

La commande show spanning-tree vous permet de visualiser l'état et la configuration du spanning-tree sur votre réseau.