Dans ce nouveau chapitre, je vous propose d’optimiser votre réseau, en créant de la redondance pour pallier les pannes. Cette optimisation risque de vous poser quelques problèmes que l’on va évidemment résoudre ensemble. Nous en profiterons pour faire un peu de théorie. Évidemment, vous la mettrez tout de suite en pratique, en étudiant le protocole Spanning Tree. C’est parti !

**Optimisez votre réseau**

Il est commun dans une entreprise d’ajouter des switchs en fonction de la taille de l’entreprise pour répondre aux besoins. Par exemple, si vous voulez préparer l’arrivée d’un nouveau venu, installer une nouvelle imprimante ou des caméras de vidéosurveillance...

Ces switchs peuvent être ajoutés à chaque étage ou chaque division. En fait, à chaque fois que cela est nécessaire. Les switchs se retrouvent bien souvent branchés les uns aux autres, ce qui est une bonne pratique. En effet, cela permet de ne pas avoir de goulot d’étranglement et cela permet la redondance des chemins. C’est justement cette redondance qui pose problème ; 3 problèmes exactement :

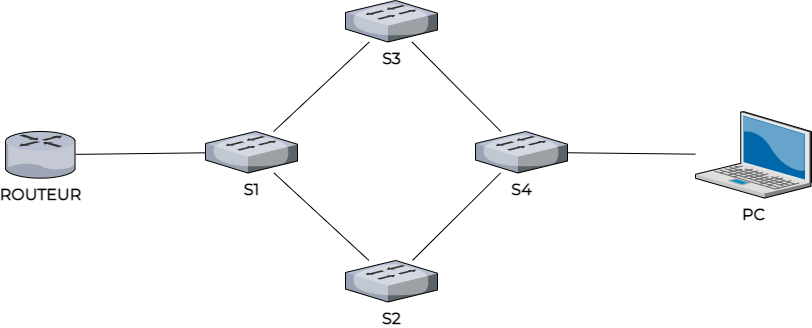
1. Un problème dit de tempêtes de broadcast.
2. Un problème de duplication de trame.
3. Un problème d’instabilité des tables MAC.

Ces trois problèmes peuvent se résumer en un seul : **un problème de boucle**. Voyons ça de plus près !

Le moment tant redouté est déjà arrivé, nous allons faire un peu de théorie !  Voyons rapidement ce que signifie ce problème de boucle avant de le résoudre.

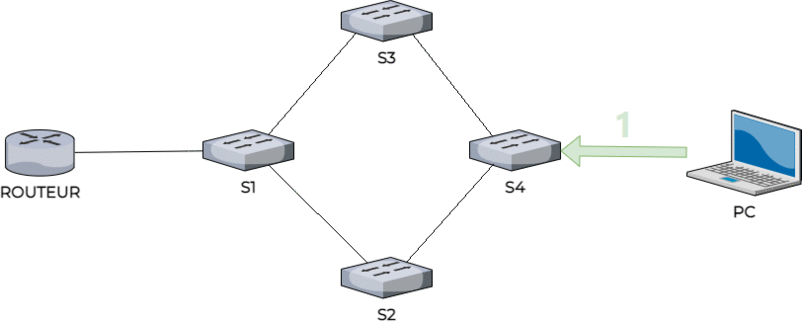
**Vous avez un problème de boucle**

Partons de cette topologie où les switchs 2 et 3 se protègent en cas de panne :



**1. Les tempêtes de broadcast**

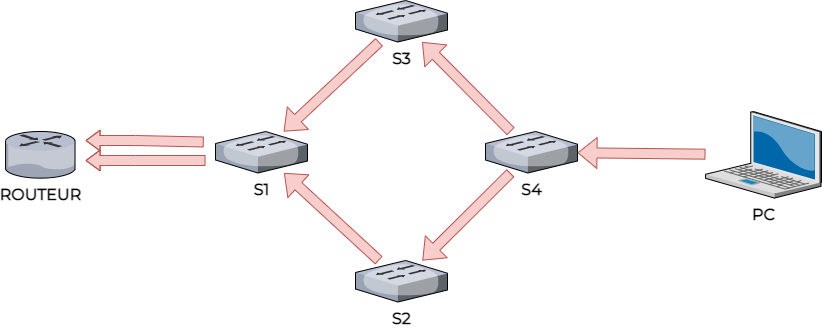
Maintenant que notre architecture est refondée, regardons ce qu’il se passe si le PC-1 envoie une demande de DHCP (DHCP DISCOVER), un message broadcast donc, au routeur qui se trouve être le serveur DHCP.



1. Le switch 4 reçoit la trame du PC-1 et la diffuse sur tous ses ports, c’est le fonctionnement normal pour une adresse broadcast, elle est destinée à tout le monde.
2. Les switchs 2 et 3 reçoivent aussi la trame du PC-1.
3. Ils la diffuse de la même manière sur tous leurs ports, envoyant les messages au switch 1 mais aussi au switch 4 qui vient de leur envoyer.
4. Résultat : les quatre switchs vont s’envoyer en permanence la trame DHCP du PC-1, faisant utiliser le CPU de ces switchs pour rien.

**2. Les duplications de trame**

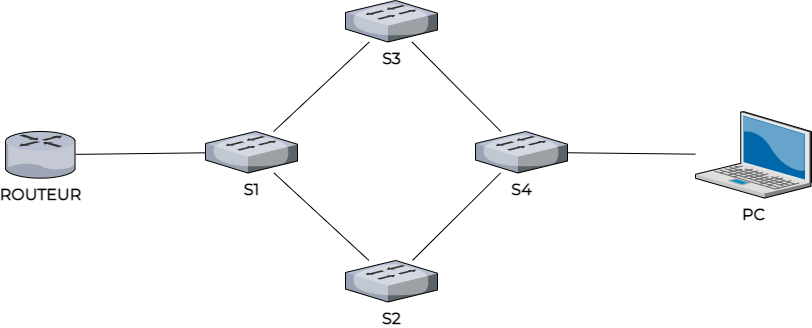
Ce problème est plus ou moins identique au premier mais au lieu de se répéter à l’infini il se répétera que deux fois, du PC-1 au routeur. Imaginons cette fois-ci que le PC-1 connaisse l’adresse IP du serveur et qu’il souhaite lui envoyer une trame.

Duplication de trame

* Le switch 4 va recevoir la trame, voir qu’il possède l’adresse MAC du serveur dans sa table et donc lui envoyer le message.
* Les switchs 2 et 3 vont effectuer la même opération.
* Le switch 1 va donc envoyer deux fois le même message et le routeur le recevoir aussi deux fois.

**3. L’instabilité des tables MAC**

Reprenons l’exemple de la duplication des trames. Cependant, intéressons-nous plus particulièrement aux tables MAC plutôt qu’à la trame elle-même.



Partons du cas où les tables MAC des 4 switchs sont vides.

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

* Lorsque la trame du routeur arrive sur le switch 3, il met à jour sa table avec l’adresse MAC du routeur, le switch 2 en fait de même.
* Chaque switch veut maintenant envoyer la trame vers le PC-1 mais aucun des deux ne sait encore où il se situe ; ils ne l’ont pas dans leurs tables MAC. Chaque switch va donc envoyer la trame sur tous ses ports, ici le port 1, sauf celui qui est déjà renseigné (le port2).
* Le switch 3 envoie la trame par le port 1, qui va transiter par le switch 4, le switch 2 va donc mettre à jour sa table MAC avec l’adresse MAC du routeur associé au port 1 ! Le switch 2 en fait de même et donc le switch 3 met aussi sa table à jour.

Ce qui donne :

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

Voilà le problème, les tables des switchs vont se mettre en permanence à jour, ce qui va aussi leur prendre des ressources en CPU.

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

Afin de vérifier tout cela, désactivons le spanning-tree qui empêche que ses problèmes ne surviennent (qui est automatiquement lancé sur les appareils CISCO) avec la commande :

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

Vous voyez que le spanning-tree se lance sur des VLAN et non sur des interfaces.

Lançons maintenant un ping du routeur vers le poste-1 et vérifions l’état du CPU des switchs avec la commande :

show processes cpu

Vous allez vite vous apercevoir que l’utilisation du CPU monte en flèche, que les switchs vont devenir de plus en plus lents jusqu’à atteindre les 100 % de CPU et planter. Seule solution : les redémarrer.

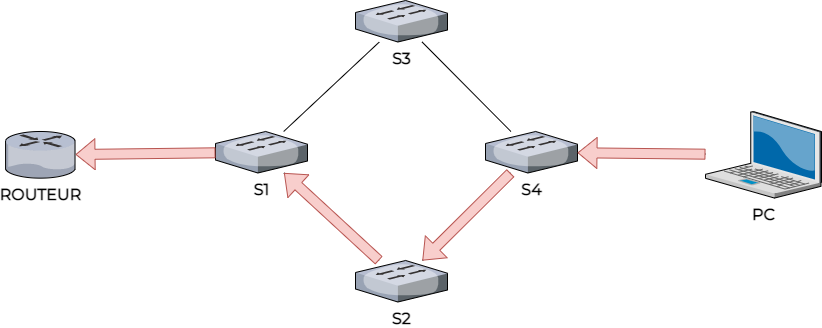
**Appliquez la solution**

Vous vous en doutez, pour résoudre ces problèmes vous allez configurer le protocole spanning-tree. Mais avant cela, il vous faut comprendre comment il fonctionne.

**Créez un seul chemin**

L’idée du spanning-tree est simple. Vous allez élire un seul chemin du PC-1 au routeur en bloquant, au niveau logique, certains ports. Évidemment, en cas de panne d’un switch, ce chemin changera automatiquement. Dans notre exemple, nous allons choisir le switch 2 pour le chemin du PC vers le routeur.

Ce qui nous donne :

Spanning-tree

Voyons donc comment cela se passe.

**L'algorithme spanning-tree**

N’ayez pas peur, l’algorithme est gentil et ne vous fera aucun mal. Encore une fois, il n’y a rien de compliqué, il s’agit juste de trouver le chemin le plus court possible.

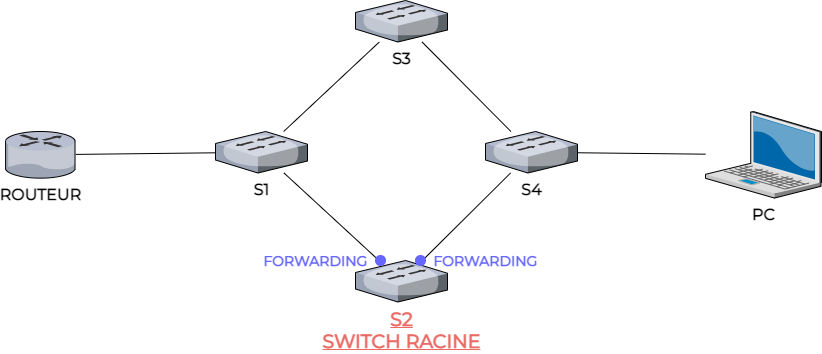
Euh, mais c’est quoi un algorithme ?

Un algorithme est une suite d’instructions nous permettant de résoudre un problème. Il s’agit dans notre cas de trouver le chemin le plus court d’un point à un autre.

De quel point vers quel autre ?

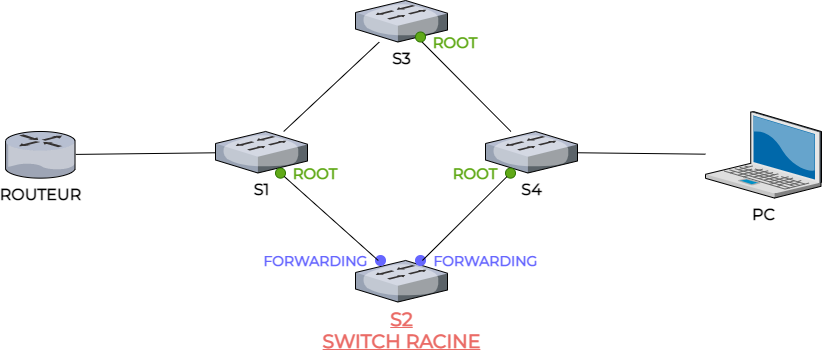
Bonne question ! C’est pour cela que le protocole commence par l’élection d’un point de départ, que l’on va appeler switch racine ou root. Ce switch est choisi en fonction de son BID (pour Bridge ID). Il s’agit d’un identifiant regroupant l’adresse MAC du switch et une priorité. Il vous est possible et même conseillé de régler cette priorité. Le switch avec le BID le plus faible sera choisi comme switch racine par le protocole spanning-tree. Tous les ports de ce switch seront en état forwarding c’est-à-dire qu'aucun de ses ports ne sera bloqué.

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

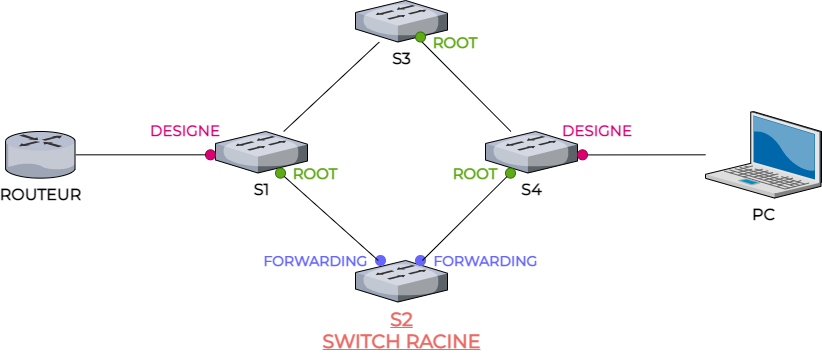
Spanning-tree et ports forwarding

Tous les autres switchs du réseau vont sélectionner le port les menant le plus rapidement au switch racine, ce port s’appelle le port root. Ce chemin sera évalué comme étant le plus court en prenant en compte la vitesse du lien qui les relie. Plus le lien est rapide, plus le coût est faible. Ce coût peut être modifié si vous souhaitez passer par un chemin plutôt que par un autre.

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

Spanning-tree et ports root

Le protocole spanning-tree va ensuite désigner les ports permettant aux terminaux (PC) de joindre le switch racine le plus rapidement, on les appelle les ports désignés.

Spanning-tree et ports désignés

Les ports qui ne sont ni root, ni désignés, sont bloqués.

En cas de panne d’un switch, il faut que ces 4 étapes soient rapidement répétées. C’est pourquoi le protocole spanning-tree envoie régulièrement des messages broadcast grâce au Bridge Protocol Data Units (BPDU). Ces BPDU envoient des messages de switchs en switchs sur :

* + La configuration (pour créer le spanning tree) ;
  + Les changements de topologies (si un lien est coupé, ou un switch HS).

**Mettez-le en pratique**

La mise en pratique va consister à :

* Activer le spanning-tree avec la commande :  spanning-tree vlan 1

Switch# configure terminal

Switch(config)# spanning-tree vlan 1

Switch(config)# end

Switch#

* Choisir un routeur root. Ici, vous allez choisir le switch 2 qui se trouve être au centre du réseau. Pour cela, tapez la commande :  spanning-tree vlan 1 root primary

Switch# configure terminal

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

Switch(config)# end

Switch#

* Choisir un routeur root secondaire en cas de panne du premier. Ici vous allez choisir le switch 3 en tapant la commande :  spanning-tree vlan 1 root secondary

Switch# configure terminal

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

Switch(config)# end

Switch

Pour vérifier tout cela et comprendre un peu mieux ce qu’il se passe, entrez la commande :

show spanning-tree.

Vous devriez obtenir quelque chose qui ressemble à ça :

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

Dans la prochaine partie, vous découvrirez tout ce qu’il faut savoir pour créer des liens entre les routeurs, appelé protocoles de routage.

**En résumé**

* Pour que votre réseau soit performant et sûr, il vous faut créer des chemins redondants en ajouter des switchs menant aux mêmes parties du réseau.
* Sans le protocole spanning-tree, cette redondance posera de gros problèmes comme les tempêtes de broadcast, les messages reçus deux fois ou l’inconstance des tables MAC.
* Le spanning-tree résout ces problèmes en empêchant toute boucle de se former.
* Le protocole spanning tree crée un seul chemin sur le réseau. Pour cela, il faut :
  + Choisir un switch racine ou root ;
  + Choisir un switch secondaire ;
  + Sélectionner les chemins les plus courts vers ce switch racine ;
  + Désactiver les ports qui ne servent à rien.
* Il est possible d'influencer les choix du protocole spanning tree en modifiant les priorités des switchs et le coût d’un lien :
  + **spanning-tree vlan 1 root priority**;
  + **spanning-tree vlan 1 root secondary**.
  + La commande**show spanning-tree**vous affiche les informations sur le protocole spanning-tree.