Configuration des VLANs

Allez, on attaque la configuration. On vas d'abord créer mes VLANs sur le premier switch.

- *Switch> enable*
- *Switch# configure terminal*

Mode privilégié, puis mode configuration globale. Classique!

- *Switch(config)# hostname SW1-Etage1*

On change le hostname pour être cohérent.

- *SW1-Etage1(config)# vlan 10*
- *SW1-Etage1(config-vlan)# name COMPTABILITE*
- *SW1-Etage1(config-vlan)# exit*

on crée le VLAN 10 et on lui donne le nom "COMPTABILITE". Le nom, c'est facultatif, mais c'est une BONNE PRATIQUE. Ça aide énormément pour la documentation et le troubleshooting !

- *SW1-Etage1(config)# vlan 20*
- *SW1-Etage1(config-vlan)# name RH*
- *SW1-Etage1(config-vlan)# exit*
- *SW1-Etage1(config)# vlan 30*
- *SW1-Etage1(config-vlan)# name IT*
- *SW1-Etage1(config-vlan)# exit*

Pareil pour les VLANs 20 et 30. Voilà, nos VLANs sont créés !

Maintenant, il faut assigner les ports aux bons VLANs. Et attention, ces ports seront des ports ACCESS !

- *SW1-Etage1(config)# interface fastEthernet 0/1*
- *SW1-Etage1(config-if)# switchport mode access*
- *SW1-Etage1(config-if)# switchport access vlan 10*
- *SW1-Etage1(config-if)# exit*

- interface fa0/1 : je sélectionne le port où est connecté PC0
- switchport mode access : je force le port en mode ACCESS
- switchport access vlan 10 : j'assigne ce port au VLAN 10

PC0 sera donc dans la comptabilité !

- *SW1-Etage1(config)# interface fastEthernet 0/2*
- *SW1-Etage1(config-if)# switchport mode access*
- *SW1-Etage1(config-if)# switchport access vlan 20*
- *SW1-Etage1(config-if)# exit*

Et PC1 va dans le VLAN 20, les RH.

Maintenant, il faut faire EXACTEMENT la même chose sur le Switch 2. On crée les VLANs 10, 20, 30 avec les mêmes noms... On assigne Fa0/1 au VLAN 10, Fa0/2 au VLAN 20... Et voilà !

Parfait ! Nos VLANs sont créés et nos PCs sont assignés. Mais ils ne peuvent toujours pas communiquer entre les étages... Normal, les switches ne sont pas connectés !

Configuration du TRUNK

Et maintenant... Le moment que vous attendez tous... On va créer notre lien TRUNK !

On prends un câble droit, et on connecte le port FastEthernet 0/24 du Switch 1... au port FastEthernet 0/24 du Switch 2.

Physiquement, nos switches sont maintenant reliés. Mais ce n'est pas suffisant ! Il faut CONFIGURER ce lien en mode Trunk.

Sur le Switch 1 :

- *SW1-Etage1(config)# interface fastEthernet 0/24*
- *SW1-Etage1(config-if)# switchport mode trunk*

Cette commande est CRUCIALE ! `switchport mode trunk` dit au port : "Hé ! Tu n'es plus un port normal, tu es un TRUNK. Tu dois transporter TOUS les VLANs !"

- *SW1-Etage1(config-if)# switchport trunk allowed vlan 10,20,30*

Et là, on ajoute une commande de SÉCURITÉ : `switchport trunk allowed vlan 10,20,30`.

Pourquoi ? Par défaut, un trunk laisse passer TOUS les VLANs (1 à 4094). Ce n’est pas toujours ce qu'on veut ! Ici, on autorise explicitement seulement mes VLANs 10, 20 et 30. C'est une EXCELLENTE pratique de sécurité !

- *SW1-Etage1(config-if)# exit*

Maintenant, SUPER IMPORTANT : il faut faire la MÊME configuration sur le Switch 2 !

- *SW2-Etage2(config)# interface fastEthernet 0/24*
- *SW2-Etage2(config-if)# switchport mode trunk*
- *SW2-Etage2(config-if)# switchport trunk allowed vlan 10,20,30*
- *SW2-Etage2(config-if)# exit*

Les deux côtés du trunk DOIVENT être en mode trunk ! Si un côté est en trunk et l'autre en access, ça ne fonctionnera PAS. C'est une erreur classique de débutant !

Et voilà ! Notre trunk est configuré. Nos VLANs peuvent maintenant voyager entre les deux switches !

Vérification de la configuration

Bon réflexe en réseau : TOUJOURS vérifier votre config ! On va utiliser quelques commandes show.

- *SW1-Etage1# show interfaces trunk*

Port Mode Encapsulation Status Native vlan

Fa0/24 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/24 10,20,30

Regardez bien :

- Mode : "on" - bon signe !
- Encapsulation : "802.1q" - notre tagging est actif
- Status : "trunking" - le trunk est UP et fonctionnel !
- Vlans allowed : 10, 20, 30 - exactement ce qu'on a configuré

C'est PARFAIT !

Autre commande

- *SW1-Etage1# show vlan brief*

VLAN Name Status Ports

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

1 default active Fa0/3, Fa0/4, ...

10 COMPTABILITE active Fa0/1

20 RH active Fa0/2

30 IT active

Vous voyez ? Le port Fa0/24 n'apparaît PAS ici. C'est NORMAL ! Les ports trunk ne sont pas listés dans le show vlan, parce qu'ils ne sont pas assignés à UN seul VLAN.

Si vous voyez votre port trunk dans cette liste, c'est qu'il n'est PAS en mode trunk !

Tests de connectivité

Dernière étape : tester que tout fonctionne ! Je vais donner des adresses IP à mes PCs.

PC0 (VLAN 10) : 192.168.10.1 / 255.255.255.0

PC2 (VLAN 10 - étage 2) : 192.168.10.2 / 255.255.255.0

PC1 (VLAN 20) : 192.168.20.1 / 255.255.255.0

PC3 (VLAN 20 - étage 2) : 192.168.20.2 / 255.255.255.0

PC0 et PC2 sont dans le VLAN 10, même sous-réseau. PC1 et PC3 sont dans le VLAN 20, autre sous-réseau.

Allez, moment de vérité ! Est-ce que PC0 peut pinguer PC2 à travers le trunk ?

PC> ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

BOOM ! Ça fonctionne ! PC0 et PC2 sont sur deux switches différents, mais grâce au trunk, ils communiquent parfaitement !

Maintenant, est-ce que PC0 (VLAN 10) peut pinguer PC1 (VLAN 20) ?

PC> ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Et NON ! Timeout ! Et c'est EXACTEMENT ce qu'on veut ! Les VLANs sont bien isolés. PC0 et PC1 ne peuvent pas se parler, même s'ils sont sur le même switch.

Notre configuration est PARFAITE !

Bonne pratiques & Tips

Avant de conclure, laissez-moi vous partager quelques bonnes pratiques ESSENTIELLES pour les Trunk en production.

Par défaut, le native VLAN est le VLAN 1. En production, changez-le TOUJOURS pour un VLAN inutilisé, par exemple le VLAN 99. Pourquoi ? Sécurité ! Le VLAN 1 est une cible d'attaques classiques.

- *switchport trunk native vlan 99*

On l'a fait dans notre lab : n'autorisez que les VLANs nécessaires sur le trunk. Ne laissez pas TOUS les VLANs passer par défaut !

DTP, le Dynamic Trunking Protocol, peut être exploité pour des attaques. Forcez le mode trunk et désactivez la négociation :

- *switchport mode trunk*
- *switchport nonegotiate*

Ça paraît bête, mais DOCUMENTEZ vos Trunk ! Quel port va où, quels VLANs passent... Croyez-moi, dans 6 mois, vous serez content de l'avoir fait !

Ces quatre pratiques vont vous éviter 90% des problèmes de trunk en production !