



efrei

PARIS PANTHÉON-ASSAS UNIVERSITÉ

MISE EN PLACE ROUTAGE INTER VLAN

À Propos de SITKA

- Nom de l'Entreprise : SITKA
- Type de Société : Société Anonyme (SA)
- Nombre d'Employés : 1560
- Le chiffre d'affaires annuel de SITKA s'élève à 19 600 000€

Introduction : Dans les réseaux informatiques modernes, la segmentation en VLANs (Virtual Local Area Networks) est une pratique courante pour organiser et sécuriser le trafic. Cependant, pour permettre la communication entre ces VLANs, le routage inter-VLAN devient indispensable. Cette présentation mettra en lumière l'importance du routage inter-VLAN et ses avantages pour les réseaux d'entreprise.

Points forts :

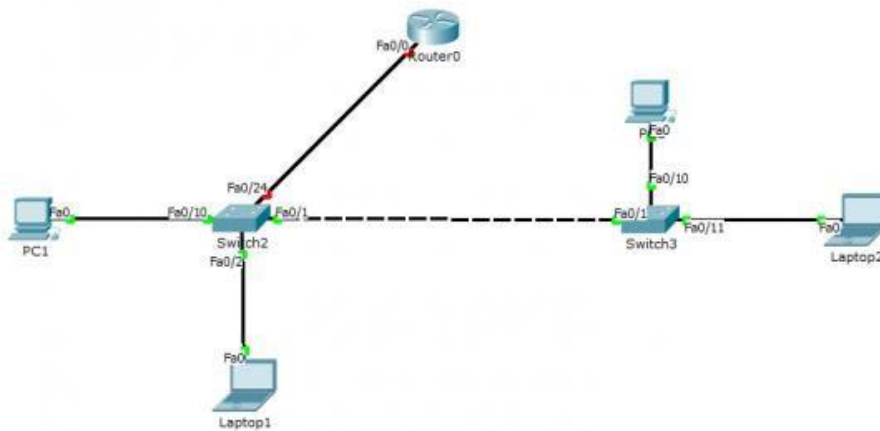
1. **Sécurité Renforcée :** Le routage inter-VLAN permet de segmenter le trafic en fonction des besoins et des niveaux de sécurité requis. Les données sensibles peuvent ainsi être isolées dans des VLANs dédiés, renforçant la sécurité globale du réseau en cas de compromission.
2. **Optimisation des Performances :** En séparant le trafic en VLANs distincts, le routage inter-VLAN réduit la congestion du réseau et optimise les performances en évitant les collisions et les goulets d'étranglement.
3. **Flexibilité et Scalabilité :** Le routage inter-VLAN offre une flexibilité totale dans la conception du réseau, permettant de créer et de modifier facilement des VLANs en fonction des besoins évolutifs de l'entreprise. Cela garantit une infrastructure réseau agile et scalable.
4. **Contrôle Fin de la Communication :** En utilisant des règles de routage et des listes de contrôle d'accès (ACL), le routage inter-VLAN permet un contrôle précis sur les flux de données entre les VLANs, assurant une gestion efficace des autorisations et des restrictions de communication.

Présentation du projet

Mise en place d'un réseau simple composé de 4 postes de travail, deux switches et un routeur. Les deux switches partageront des VLANs et le routeur se chargera des tâches de routage inter-VLANs sous les équipements réseaux de CISCO. Ainsi, nous régulerons plus facilement le flux (Les vlans bloquent les adresses de diffusions), nous pourrons créer des espaces de travail indépendants et la sécurité sera améliorée car les flux réseaux seront isolés.

Schéma du réseau

Pour schématiser le réseau, j'utiliserais le logiciel Packet Tracer version 8.0.0 :



Configuration des Vlans

La première étape à suivre une fois que le câblage est en place est de créer les deux VLANS (10 et 20) sur nos deux switches. avec une liaison par port trunk entre le switch 2 et le switch 3.

Remarque : Les lignes de configuration suivantes sont à exécuter sur les deux Switchs

```
Switch>enable
Switch#conf t
```

Nous allons ensuite créer les VLANS et les nommer :

```
Switch(config)#vlan 10
Switch(config-vlan)#name vlan_10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name vlan_20
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Native
Switch(config-vlan)#exit
```

Nous créons également un VLAN natif dont l'explication sera faite un peu plus bas dans le tutoriel.

Nous allons maintenant créer nos ports trunk sur les interfaces Fa0/1 de nos deux switches. Le port trunk va permettre, au travers des trames 802.1q de faire transiter des trames tagguées (ou étiquetées) selon un Vlan ou un autre afin que tous les Vlan autorisés puissent passer au travers d'un même lien. Plus clairement, c'est un port qui peut faire passer plusieurs VLAN vers un autre élément actif. Cela permet, dans notre cas, de faire communiquer les VLANS 10 et 20 entres des éléments connectés à deux switches différents. Sans port trunk, il faudrait une liaison entre les switches par VLANs.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 20,30,99
```

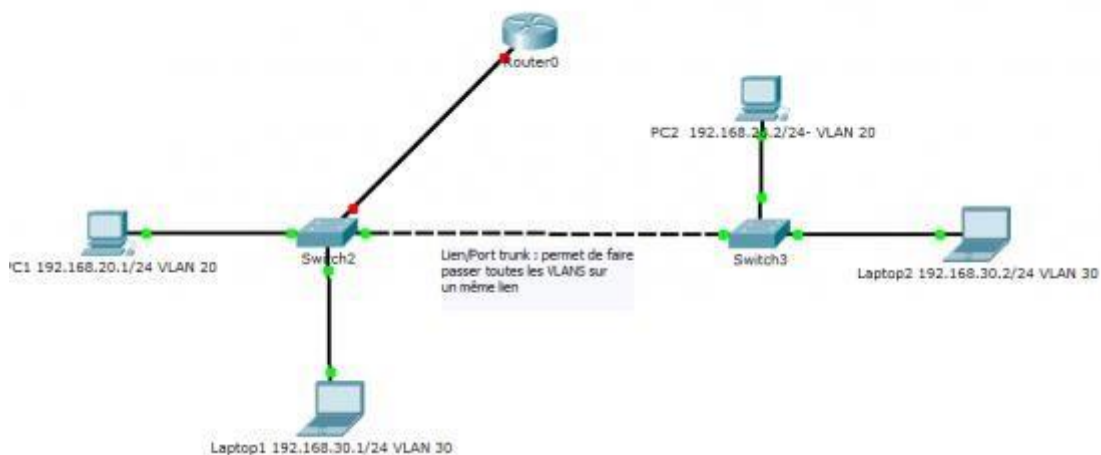
```
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Faisons un petit point sur le terme "native vlan" sur ce lien : [vlan natif](#)

On spécifie également les VLANS que nous souhaitons laisser passer sur notre trunk à savoir les trames étiquetées sur les VLAN 20,30 et 99. Par défaut, toutes les VLANS peuvent passer sur un port trunk. Si nous spécifions l'autorisation de certaines VLANs, les autres ne seront pas acceptés à transiter. Nous allons maintenant affecter les ports voulus à nos différentes VLANS. On présume que nous souhaitons affecter les ports Fa0/10 des deux switches sur la VLAN 20 et les ports Fa0/11 sur le VLAN 30, on exécute donc ces commandes sur nos deux switches :

```
Switch(config)#interface fa0/10
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/11
Switch(config-if)#switchport access vlan 30
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

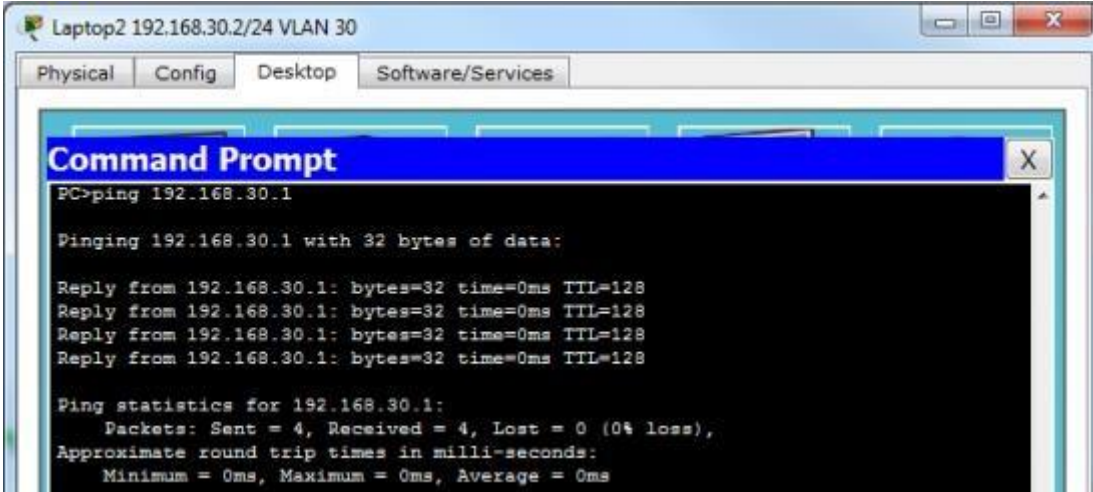
Voici à présent le schéma de notre réseau, j'ai juste ajouté des détails sur les postes pour savoir sur quel VLAN ils sont :



J'ai également ajouté des IPs à mes postes. Ceux sur la VLAN 20 appartiennent au réseau "192.168.20.0/24" et ceux sur le VLAN 30 appartiennent au réseau "192.168.30.0/24" (pour faire simple).

IV. Test Vlans

Nous allons maintenant tester la connectivité des postes situées sur la même VLAN. On prend pas exemple le poste "Laptop2" sur le VLAN 30 et avec l'IP 192.168.30.2 pour pinger le poste "Laptop1" située sur la VLAN 30 de l'autre switch et avec l'IP 192.168.30.1 :



```
Laptop2 192.168.30.2/24 VLAN 30
Physical Config Desktop Software/Services
Command Prompt
PC>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=0ms TTL=128
Reply from 192.168.30.1: bytes=32 time=0ms TTL=128
Reply from 192.168.30.1: bytes=32 time=0ms TTL=128
Reply from 192.168.30.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

On peut faire la même chose en pingant du poste "PC1" au poste "PC2" qui sont également tout deux sur le même VLAN (20 cette fois ci). Les plus curieux auront remarqué que le "PC1" ou "PC2" ne peuvent pinger "Laptop1" et "Laptop2" qui sont sur des VLANS différentes (20 et 30). C'est justement la problématique que nous venons de nous créer est que les VLANS isolent correctement les groupes de postes/d'utilisateur mais bloquent complètement la communication entre elles.

Pourquoi ?

Les VLANs sont des LAN virtuelle (d'où leur nom) et comme chaque LAN, nous ne pouvons les interconnectés que par l'intermédiaire de routeur (d'élément gérant la couche 3 - réseau plus spécifiquement). Nous avons maintenant besoin de router nos différentes VLANS entre elles pour qu'elles puissent communiquer. Nous abordons donc la deuxième partie du tutoriel qui est donc le routage inter-vlan.

V. Routage inter-vlan

Il se peut qu'un besoin de communication se fasse entre les deux groupes de travail. Il est alors possible de faire communiquer deux Vlans sans pour autant compromettre leur sécurité.

Pour cela nous utilisons un routeur relié à un des deux switches. Nous appelons ce type de routage inter-vlan un Router-on-stick. Cela signifie que le routeur va, par intermédiaire d'un seul lien physique routeur et faire transiter un ensemble de VLAN. On aurait également pu mettre en place un switch de niveau trois qui aurait été capable d'effectuer les tâches de routage inter-vlan.

Plusieurs Vlans peuvent avoir pour passerelle un même port physique du routeur qui sera "découpé" en plusieurs interfaces virtuelles. Nous pouvons en effet diviser un port du routeur selon les Vlans à router et ainsi créer une multitude de passerelles virtuelles avec des adresses IP différentes.

VI. Configuration du routeur

Nous allons donc créer nos interface virtuelles sur le port Fa0/0 de notre routeur. Il faut tout d'abord absolument activer l'interface physique pour que les interfaces virtuelles soient opérationnelles :

```
Router>enable
Router#configuration terminal
Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Nous allons ensuite créer l'interface **fa0/0.1** (interface virtuelle 1 de l'interface physique fa0/0), nous dirons que ce port virtuel sur la passerelle des postes du VLAN 20 :

```
Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.254 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Nous faisons pareil pour l'interface fa0/0.2 et les postes du réseau du vlan 30

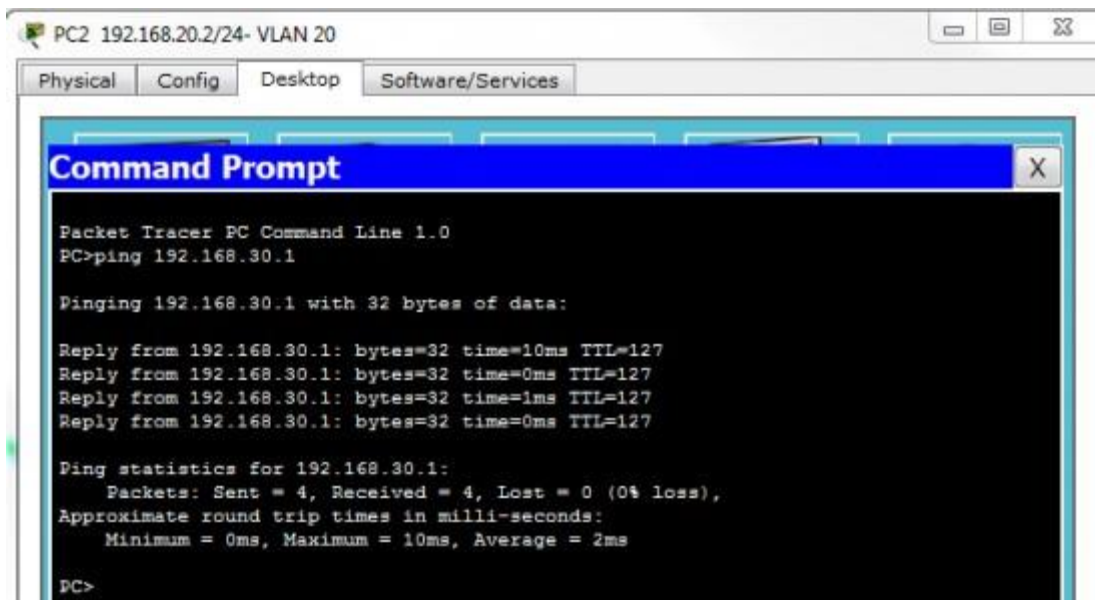
```
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.254 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Un petit mot de la commande "**encapsulation dot1q**". La norme de trame **802.1q** indique que les trames sont étiquetées pour contenir le numéro de vlan à laquelle elles sont destinées/attribuées. La commande "**encapsulation dot1q 30**" permet donc d'encapsuler une trame pour transiter sur le vlan 30 si elle est destinée à celui ci. Le routeur a besoin de cette information par exemple quand il voit une trame venant du vlan 20 (étiquetée vlan 20) qui souhaite se diriger sur le vlan 30. Il change donc à ce moment la son étiquetage 802.1q pour que les switches puissent correctement acheminé la trame vers le ou les postes du vlan 30. N'oublions pas notre switch ! Il faut également mettre le port **fa0/24** de notre "**Switch2**" (qui fait la liaison avec le routeur) en mode trunk pour que lui aussi puisse acheminer toutes les VLANs vers et depuis le routeur :

```
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 20,30,99
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

VII. Test Routage Vlan

Une fois que nous avons mis les bonnes passerelles à nos postes (par exemple 192.168.20.254 pour les postes du VLAN 20 dans le cas de notre schéma de test), nous pouvons tester la communication inter-VLAN par l'intermédiaire d'un simple ping par exemple du poste 192.168.20.2 vers 192.168.30.1



```
PC2 192.168.20.2/24- VLAN 20
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=10ms TTL=127
Reply from 192.168.30.1: bytes=32 time=0ms TTL=127
Reply from 192.168.30.1: bytes=32 time=1ms TTL=127
Reply from 192.168.30.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

PC>
```