TP3 Réseaux d'entreprise

Antoine Laguette & Guillaume Tisserand & Juliette Bluem

7 décembre 2022

Table des matières

1 Introduction

Durant trois TP, nous allons mettre en place une topologie type d'entreprise :

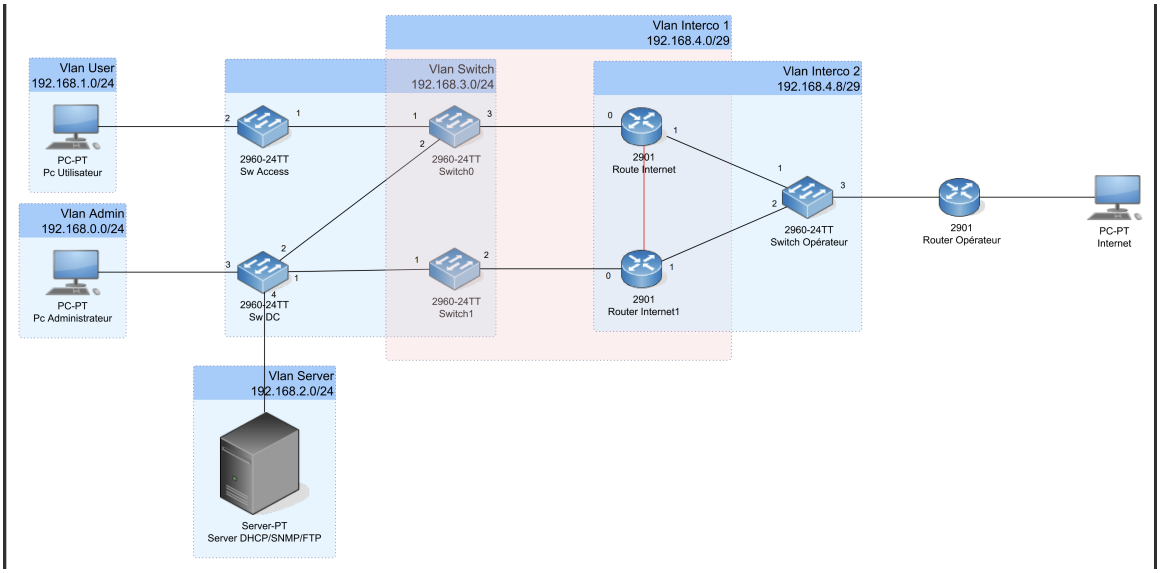

FIGURE 1 – Topologie

Elle nous a servis dans la première séance à utiliser différent protocoles comme le VTP, le DHCP et le LACP, mais aussi des technologies comme la stackwise qui nous a permis de coupler deux switch pour n'en faire qu'un.
Lors de la deuxième séance, nous avons pu mettre en place des pratiques connues et acquises, comme les ACL ou le SSH, mais aussi nous permettre de découvrir le DHCP snooping, le chiffrement de mots de passe et la sécurité de ports.

Pour cette troisième et dernière séaance nous allons voir comment utiliser différentes solutions/technologies comme le routage dynamique OSPF, SNMPv3, NAT et l'utilisation d'archive path avec FTP

2 OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage pour les réseaux locaux d'entreprise. Il permet de déterminer le plus court chemin à travers un réseau en utilisant un algorithme de calcul d'itinéraire appelé l'algorithme de Dijkstra.
Le protocole OSPF utilise des informations sur les liens et les coûts associés à chacun d'eux pour calculer le meilleur itinéraire pour les données qui transitent à travers le réseau. Il utilise également des annonces de protocole pour échanger des informations sur les liens et les coûts avec les autres routeurs OSPF sur le réseau, ce qui lui permet de mettre à jour en permanence sa table de routage.
Ainsi, lorsqu'un paquet de données est envoyé à travers un réseau OSPF, le routeur OSPF utilise sa table de routage pour déterminer le chemin le plus court pour atteindre sa destination finale. Cela permet d'optimiser la performance du réseau en évitant les itinéraires inutiles ou peu efficaces.

Nous commençons donc pas installer les deux routeur, et leur donnons des adresses IP : 192.168.4.2/29 pour le routeurInternet1 et 192.168.4.1/29 pour le routeurInternet0.
Nous mettons ensuite en place le protocole de routage sur ces deux routeurs et sur le switch de niveau 3. Voici un exemple des commandes entrées sur le routeurInternet0 :
R0(CONFIG)#ROUTER OSPF 100
R0(CONFIG-ROUTER)NETWORK 192.168.3.0 0.0.0.255 AREA 0
R0(CONFIG-ROUTER)NETWORK 192.168.4.0 0.0.0.7 AREA 0
R0(CONFIG-ROUTER)#NETWORK 192.168.4.8 0.0.0.7 AREA 0
Nous devons ensuite redistribuer les routes :
Tout d'abord, les connectées :
R0(CONFIG)#ROUTER OSPF 100
R0(CONFIG-ROUTER)#REDISTRIBUTE CONNECTED
Puis les autres, par un routage statique :
R1(CONFIG)#IP ROUTE 0.0.0.0 0.0.0.0 192.168.3.2 R0(CONFIG)#ROUTER OSPF 100 R0(CONFIG-ROUTER)#REDISTRIBUT
STATIC R0(CONFIG-ROUTER)#DEFAULT-INFORMATION ORIGINATE

Nous vérifions notre routage grâce à la commande SHOW IP ROUTE.

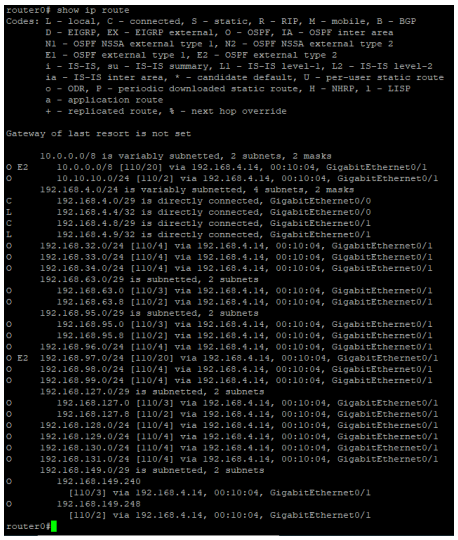

FIGURE 2 – Configuration OSPF sur R0

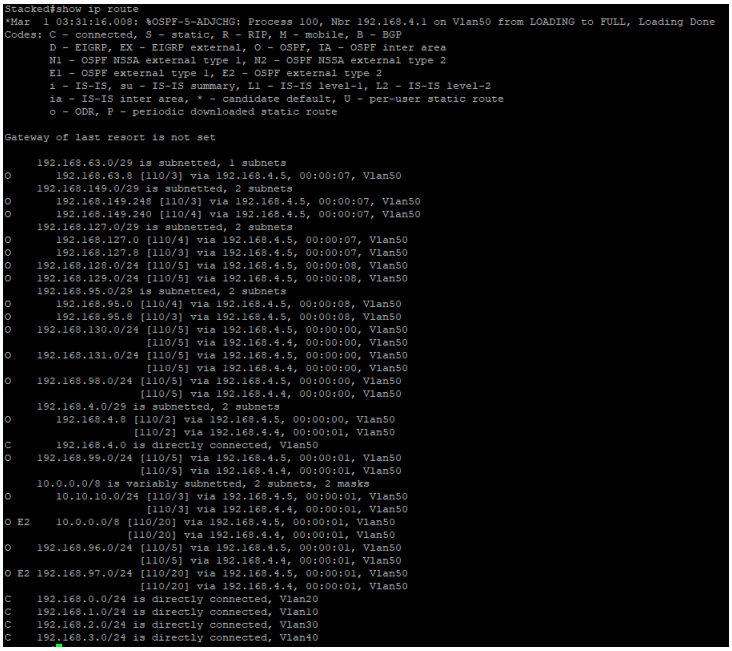

FIGURE 3 – Configuration OSPF sur switchs Staked

On voit bien sur les captures que la table de routage contient des routes issues de l'OSPF.

Attention, il faut bien penser à affecter les vlans aux interfaces physiques - et les bons. En l'occurrence, il nous fallait attribuer le vlan 50 aux interfaces fa1/0/1 et fa2/0/1 des switchs stakés de niveau 3.

Pour améliorer la sécurité du réseau, bloquer le trafic OSPF peut empêcher les routeurs non autorisés d'obtenir des informations sur la topologie du réseau, ce qui peut renforcer la sécurité du réseau en empêchant les attaquants de recueillir des informations sur sa configuration.
Pour se faire, nous utilisons la commande suivante :
STAKED#PASSIVE-INTERFACE FA0/2 Sans cela, nous voyions grâce à Wireshark des trames OSPF passer, ce n'est plus le cas.

3 HSRP

Le routage OSPF et le routage HSRP (Hot Standby Router Protocol) sont tous deux des protocoles de routage utilisés dans les réseaux locaux pour gérer le trafic de données. Cependant, ils sont conçus pour des fonctions différentes.

Nous l'avons vu précédemment, le routage OSPF est un protocole de routage dynamique qui permet aux routeurs d'échanger des informations de routage pour déterminer le meilleur chemin pour acheminer les données à travers le réseau. Il est utilisé pour fournir des itinéraires efficaces pour le trafic de données sur les réseaux locaux étendus.

Le routage HSRP, en revanche, est un protocole de routage statique utilisé pour offrir une haute disponibilité du réseau. Il permet à plusieurs routeurs de travailler ensemble en tant que groupe de secours pour s'assurer qu'il y a toujours un routeur actif pour envoyer et recevoir des paquets réseau. Si le routeur actif tombe en panne, un autre routeur prend immédiatement sa place pour assurer la continuité du service.En effet, l'adresse IP de la passerelle est configurée sur deux routeurs différents. Une seule de ces deux interfaces est active. Si l'interface active n'est plus accessible, l'interface passive devient active. Le routage HSRP est principalement utilisé pour garantir que les réseaux

critiques restent en ligne en tout temps.

En résumé, le routage OSPF est un protocole de routage dynamique utilisé pour calculer les itinéraires les plus efficaces pour le trafic de données sur les réseaux locaux étendus, tandis que le routage HSRP est un protocole de routage statique utilisé pour fournir une haute disponibilité du réseau en permettant à plusieurs routeurs de travailler ensemble en tant que groupe de secours.

Pour le mettre en place, nous allons modifier légèrement la topologie initialement prévue. En effet, il n'y aura finalement pas de lien de vie entre les routeurs, on passera par les switchs stakés de niveau 3.
Et nous configurons les équipements :
R0(config)#int ge0/0/0 R0(config-if)#standby 100 ip 192.168.4.3 R0(config-if)#standby 100 priority 110 R0(config-if)#standby 100 preempt R0(config-if)#end R1(config)#int ge0/0/0 R1(config-if)#standby 100 ip 192.168.4.3 R1(config-if)#standby 100 preempt R1(config-if)#end
Il n'y a rien à faire sur le switch.

On vérifie notre travail via un ping continu :

Figure 4 – Vérification HSRP

On voit sur l'image qu'en débranchant un des liens entre les switchs stakés et le routeur actif, le ping se poursuit. Nous avons un message sur le router nous indiquant le changement.
En d'autres termes, si on désactive le lien principal, le second (initialement en standby) prend le relais.

Attention toute fois à bien configurer HSRP du bon coté des routeurs. En effet, au début, nous l'avions mis en place coté interco2. Il faut bien se placer coté LAN.

4 SNMPv3

SNMPv3 (Simple Network Management Protocol version 3) est une version améliorée du protocole SNMP (Simple Network Management Protocol) utilisé pour gérer et surveiller les équipements réseau. SNMPv3 apporte plusieurs améliorations par rapport aux versions précédentes du protocole, notamment en matière de sécurité.
Le SNMPv3 utilise des mécanismes de cryptage pour protéger les échanges de données entre les équipements réseau et les outils de gestion de réseau. Il prend en charge l'authentification des utilisateurs et des agents, ainsi que l'encryptage des données pour empêcher les attaquants de les lire. Le SNMPv3 permet également de gérer plusieurs niveaux de privilèges pour les utilisateurs et les agents, ce qui permet de contrôler les informations qui peuvent être consultées et modifiées.

En résumé, le SNMPv3 est une version améliorée du protocole SNMP qui offre des fonctionnalités de sécurité avancées pour protéger les échanges de données entre les équipements réseau et les outils de gestion de réseau.

Nous n'en avons pas eu le temps suite à de nombreuses erreurs, mais nous aurions dû rentrer les commandes suivantes :

Switch stacked :
```
Stacked(config)# snmp-server group 1 v3 priv
Stacked(config)# snmp-server user polytech v3 auth sha polytech priv aes 128 polytech
Stacked(config)# snmp-server contact Polytech<guillaume.tisserand7@etu.univ-lorraine.fr>
Stacked(config)# snmp-server location ServerPolytech
Stacked(config)# exit
```

Switch Acces :
```
SWA(config)# snmp-server group 1 v3 priv
SWA(config)# snmp-server user polytech v3 auth sha polytech priv aes 128 polytech
SWA(config)# snmp-server contact Polytech<guillaume.tisserand7@etu.univ-lorraine.fr>
SWA(config)# snmp-server location ServerPolytech
SWA(config)# exit
```

Switch DC :
```
SWDC(config)# snmp-server group 1 v3 priv
SWDC(config)# snmp-server user polytech v3 auth sha polytech priv aes 128 polytech
SWDC(config)# snmp-server contact Polytech<guillaume.tisserand7@etu.univ-lorraine.fr>
SWDC(config)# snmp-server location ServerPolytech
SWDC(config)# exit
```

5 Archive path & FTP

FTP (File Transfer Protocol) est un protocole utilisé pour transférer des fichiers sur un réseau informatique. L'archive path peut être utilisé pour spécifier l'emplacement d'un fichier sur le réseau lorsqu'on utilise FTP pour le transférer. Par exemple, si vous souhaitez transférer un fichier appelé mon_fichier.txt situé dans le dossier mes_documents sur un serveur FTP nommé mon_serveur, vous pouvez utiliser l'archive path \\mon_serveur\mes_documents\mon_fichier.txt pour indiquer l'emplacement du fichier sur le réseau. En général, l'archive path est utilisé conjointement avec FTP pour permettre aux utilisateurs de transférer des fichiers sur un réseau de manière simple et efficace.

Pour le mettre en place, nous devions utiliser les commandes suivantes :

Sauvegarde de configuration :
```
SW1# copy running-config startup-config
```

Configuration ftp sur router :
```
R0(config)#ip ftp polytech
R0(config)#ip ftp password polytech
R0(config)#end
```

On fait ensuite un copy running-config ftp et on répond au questions :
```
Address or name of remote host []? 10.66.64.10
Destination filename [R1-confg]? backup_cfg_for_router
```

La configuration est finalisé au message : Writing backup_cfg_for_router ! 1030 bytes copied in 3.341 secs (308 bytes/sec)

On fait pareil sur l'autre routeur : Router#copy ftp : running-config
Address or name of remote host [10.66.64.10] ?
Source filename [backup_cfg_for_router] ?
Destination filename [running-config] ?

La réponse de l'équipement est la suivante : Accessing ftp :\\10.66.64.10\backup_cfg_for_router...
Loading backup_cfg_for_router ! [OK - 1030/4096 bytes] 1030 bytes copied in 13.213 secs (78 bytes/sec)

6 NAT

Le NAT (Network Address Translation) est une technique utilisée par les routeurs pour permettre à plusieurs ordinateurs de partager une connexion à Internet en utilisant une seule adresse IP publique. Le routeur utilise le NAT pour suivre les communications entrantes et sortantes, et pour traduire les adresses IP privées des ordinateurs connectés en une seule adresse IP publique, ce qui permet aux paquets de données de voyager sur Internet. En général, cela permet d'optimiser l'utilisation des adresses IP publiques disponibles et de protéger les ordinateurs connectés en masquant leurs adresses IP privées

Pour le configurer, voici les commandes que nous aurions dû rentrer :
Sur R1 :
R1(config)#int (Switchop)
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#int (switch1)
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)# ip nat inside source static (@IP sur laquelle arrive les paquets sur le routeur) (@IP Naté public)
Sur R0 :
R0(config)#int (Switchop)
R0(config-if)#ip nat outside
R0(config-if)#exit
R0(config)#int (switch0)
R0(config-if)#ip nat inside
R0(config-if)#exit

Nous aurions vérifier notre configuration à l'aide des commandes suivantes.
R1#show ip nat translations
R1#show run