Rapport SAE 3.03 - Partie LAN :

Table des matières

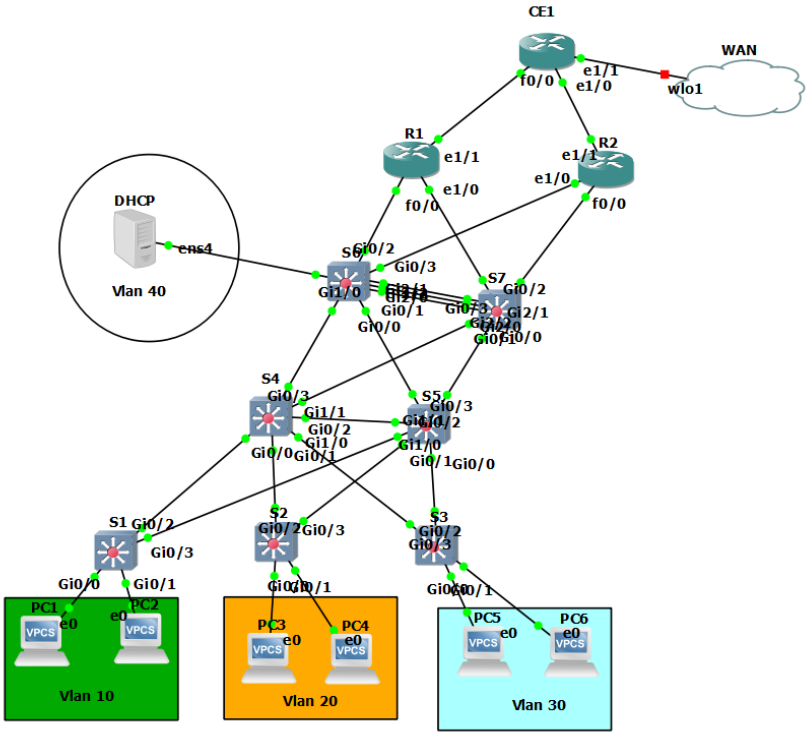
Introduction :

Dans le cadre de ce projet, nous avons conçu et implémenté une architecture réseau LAN sur GNS3. L'architecture, composée de trois niveaux distincts : accès, distribution et cœur permet d'assurer une gestion optimale et une grande flexibilité du réseau.
Dans notre topologie, nous avons structuré les équipements de la manière suivante :

- Niveau d'accès : les switches S1, S2, S3 directement connectés aux PC des différents VLANs.
- Niveau de distribution : les switches S4, S5, S6, S7 assurant l'interconnexion des VLANs et le routage inter-VLAN.
- Niveau de cœur : les routeurs R1, R2 et le routeur CE1, assurant la liaison vers l'extérieur et la fonction NAT.

Cette architecture permet une gestion plus claire des VLANs, du routage, ainsi que l'intégration de protocoles de redondance et de haute disponibilité (MST, VRRP), assurant ainsi un réseau robuste et évolutif.

Voici le schéma de la topologie réseau :



Adressage :

VLAN :

La création de VLANs (Virtual Local Area Networks) est essentielle dans un réseau pour segmenter le trafic de manière logique. Cela améliore la sécurité, réduit les interférences, et rend le réseau plus rapide et plus facile à gérer.
Nous avons ici créé 4 VLANs :

VLAN	Service	Plage IP	Passerelle
10	Informatique	10.242.110.0/24	10.242.110.254 ou 10.242.110.252
20	Direction	10.242.120.0/24	10.242.120.254 ou 10.242.120.252
30	Financier	10.242.130.0/24	10.242.130.254 ou 10.242.130.252
40	Admin	10.242.140.0/24	10.242.140.254 ou 10.242.140.252

Voici les commandes faites pour créer ces Vlans :

```
vlan 10
 name informatique
vlan 20
 name Direction
vlan 30
 name Financier
vlan 40
 name Admin
```

Sur les switches S1, S2, S3 chaque port qui connecte un PC est configuré en mode access.
Par exemple :

```
interface Gi0/0
 switchport mode access
 switchport access vlan 10
```

Ces commandes doivent être faites pour chaque switch d'accès :

- S1 : VLAN 10 pour PC1 et PC2
- S2 : VLAN 20 pour PC3 et PC4
- S3 : VLAN 30 pour PC5 et PC6

Trunks :

Pour transporter les VLAN nous avons configuré les liens entre les switches en modes trunk. Par exemple :

```
interface GigabitEthernet0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,40
```

Ces commandes doivent être faites sur les 2 ports des liens ci-dessous :

- S1 – S4, S5
- S2 – S4, S5
- S3 – S4, S5
- S4 – S5, S6, S7
- S5 – S6, S7

A présent nous pouvons ping entre les VLANs par exemple ici le PC3 (VLAN 20) peut communiquer avec le VLAN 10.

```
PC3> ip dhcp
DDORA IP 10.242.120.2/24 GW 10.242.120.254

PC3> ping 10.242.110.2
84 bytes from 10.242.110.2 icmp_seq=1 ttl=63 time=203.221 ms
84 bytes from 10.242.110.2 icmp_seq=2 ttl=63 time=459.757 ms
84 bytes from 10.242.110.2 icmp_seq=3 ttl=63 time=204.679 ms
84 bytes from 10.242.110.2 icmp_seq=4 ttl=63 time=395.413 ms
84 bytes from 10.242.110.2 icmp_seq=5 ttl=63 time=222.388 ms
```

MST :

Pour garantir la redondance réseau et éliminer les risques de boucles de commutation, nous avons choisi le protocole MST (Multiple Spanning Tree). Contrairement à PVST+ ou RSTP, MST optimise les performances en regroupant les VLAN en instances partagées, ce qui simplifie la gestion du réseau. En cas de panne, sa capacité à converger rapidement réduit les interruptions de service. MST améliore aussi l'équilibrage du trafic en exploitant plusieurs chemins simultanément grâce à la configuration de root bridges pour chaque instance.

Nous avons regroupé les VLAN en deux instances :

- Instance 1 : VLAN 10 et VLAN 20
- Instance 2 : VLAN 30 et VLAN 40
-

Les commandes à faire sont :

```
spanning-tree mode mst
spanning-tree extend system-id
spanning-tree mst configuration
 name MST
 revision 1
 instance 1 vlan 10-20
 instance 2 vlan 30-40
```

Ensuite, on définit les priorités pour chaque instance pour que S6 devienne le root bridge pour l'instance 1 et S7 devienne le root bridge pour l'instance 2 :

Sur S6 :

```
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
```

Sur S7 :

```
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
```

OSPF :

Le protocole de routage dynamique OSPF (Open Shortest Path First) a été mis en place pour assurer une diffusion efficace et rapide des routes entre les différents équipements du réseau, notamment les routeurs (R1, R2) et les switches de niveau 3 (S6, S7), ainsi que le routeur CE1.

Configuration sur les switches L3 (S6 et S7) :

Les switches S6 et S7 sont configurés pour inclure les réseaux locaux (VLAN 10, 20, 30, 40) et les liaisons montantes vers les routeurs R1 et R2.
Voici un exemple de configuration pour le switch S6 :

```
router ospf 1
  network 10.242.100.0 0.0.0.3 area 0
  network 10.242.100.4 0.0.0.3 area 0
  network 10.242.110.0 0.0.0.255 area 0
  network 10.242.120.0 0.0.0.255 area 0
  network 10.242.130.0 0.0.0.255 area 0
  network 10.242.140.0 0.0.0.255 area 0
```

Configuration sur les routeurs (R1 et R2) :

Les routeurs R1 et R2 déclarent leurs interfaces réseau respectives pour garantir une connectivité optimale au sein de l'area 0.

R1 :

```
router ospf 1
 network 10.242.100.0 0.0.0.3 area 0
 network 10.242.100.8 0.0.0.3 area 0
 network 10.242.100.20 0.0.0.3 area 0
```

R2 :

```
router ospf 1
 network 10.242.100.4 0.0.0.3 area 0
 network 10.242.100.12 0.0.0.3 area 0
 network 10.242.100.16 0.0.0.3 area 0
```

Configuration sur le routeur CE1 :

Sur le routeur CE1, les réseaux internes sont également déclarés, y compris une interface Loopback qui peut être utilisée pour le routage ou comme identifiant stable dans le réseau.

```
router ospf 1
 network 10.242.100.16 0.0.0.3 area 0
 network 10.242.100.20 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
```

Ping du PC du VLAN 1 vers le routeur CE1 :

```
PC2> ip dhcp
DDORA IP 10.242.110.2/24 GW 10.242.110.254

PC2> ping 192.168.20.1
84 bytes from 192.168.20.1 icmp_seq=1 ttl=253 time=227.088 ms
84 bytes from 192.168.20.1 icmp_seq=2 ttl=253 time=217.773 ms
84 bytes from 192.168.20.1 icmp_seq=3 ttl=253 time=294.921 ms
84 bytes from 192.168.20.1 icmp_seq=4 ttl=253 time=291.121 ms
84 bytes from 192.168.20.1 icmp_seq=5 ttl=253 time=211.013 ms

PC2>
```

DHCP :

Le serveur DHCP se trouve dans le vlan 40 et est essentiel dans ce réseau, il permet de distribuer les adresses IP dans les VLANs 10, 20, 30 et 40, avec des plages d'adresses distinctes pour éviter les conflits. Une fois sur un PC nous avons juste à faire la commande « *ip dhcp* » pour obtenir une adresse IP.

```
PC2> ip dhcp
DDORA IP 10.242.110.2/24 GW 10.242.110.254
```

Configuration du serveur DHCP :

Dans le fichier /etc/default/isc-dhcp-server :

```
INTERFACESv4="ens4"
```

Dans le fichier /etc/dhcp/dhcpd.conf :

```
#Vlan 10
subnet 10.242.110.0 netmask 255.255.255.0 {
   range 10.242.110.1 10.242.110.100;
   option routers 10.242.110.254;}

#Vlan 20
subnet 10.242.120.0 netmask 255.255.255.0 {
   range 10.242.120.1 10.242.120.100;
   option routers 10.242.120.254;}

#Vlan 30
subnet 10.242.130.0 netmask 255.255.255.0 {
   range 10.242.130.1 10.242.130.100;
   option routers 10.242.130.254;}

#Vlan 40
subnet 10.242.140.0 netmask 255.255.255.0 {
   option routers 10.242.140.254;}
```

Dans le fichier /etc/network/interfaces pour configurer l'ip du serveur en statique :

```
auto ens4
iface ens4 inet static
      address 10.242.140.253
      netmask 255.255.255.0
      gateway 10.242.140.254
```

VRRP :

Le protocole VRRP (Virtual Router Redundancy Protocol) permet de configurer une passerelle par défaut virtuelle et redondante pour chaque VLAN, assurant ainsi une haute disponibilité. En cas de panne d'un switch L3 (S6 ou S7), le second prend automatiquement le relais sans nécessiter d'intervention ni de reconfiguration des clients.

Configuration VRRP pour le VLAN 10 :

Sur S6 :

```
interface Vlan10
 ip address 10.242.110.254 255.255.255.0
 vrrp 10 ip 10.242.110.101
 vrrp 10 priority 110
```

Sur S7 :

```
interface Vlan10
 ip address 10.242.110.252 255.255.255.0
 vrrp 10 ip 10.242.110.101
 vrrp 10 priority 90
```

L'adresse 10.242.110.101 est partagée entre les deux switches via VRRP.
Priorités :

- S6 a une priorité de 110 et agit comme le Master VRRP pour le VLAN 10.
- S7 a une priorité de 90 et reste en mode Backup VRRP pour le VLAN 10.

En cas de défaillance de S6, S7 prend automatiquement le rôle de master pour maintenir la connectivité réseau.
La même approche est appliquée aux VLANs 20, 30 et 40, avec une répartition des rôles entre S6 et S7 pour équilibrer la charge :

- S6 est configuré comme Master VRRP pour les VLANs 10 et 20.
- S7 est configuré comme Master VRRP pour les VLANs 30 et 40.

Cela permet de répartir la charge globale entre les deux switches tout en garantissant une redondance complète.

NAT :

Le NAT permet aux hôtes du réseau local (répartis dans différents VLANs) d'accéder à l'extérieur en partageant une adresse IP publique. Cette fonctionnalité est essentielle pour économiser les adresses IPv4 et masquer les adresses internes. Dans notre maquette, le routeur CE1 prend en charge cette fonction.

Configuration des interfaces :

- Interface Ethernet1/0 : Connectée à l'extérieur, elle est configurée comme ip nat outside.
- Interfaces Ethernet0/0 et Ethernet0/1 : Connectées au réseau local, elles sont configurées comme ip nat inside.

Liste d'accès (ACL) :

Des ACL sont utilisées pour spécifier les plages d'adresses du LAN autorisées à utiliser le NAT :

access-list 1 permit 10.242.110.0 0.0.255.255
access-list 1 permit 10.242.120.0 0.0.255.255
access-list 1 permit 10.242.130.0 0.0.255.255
access-list 1 permit 10.242.140.0 0.0.255.255

NAT overload :

Le NAT overload est activé pour permettre à plusieurs hôtes internes de partager une seule adresse IP publique.
La commande suivante lie l'ACL a l'interface externe pour effectuer le NAT :
ip nat inside source list 1 interface Ethernet1/0 overload

Exemple : si un poste du VLAN 10 initie une connexion à un site web, son adresse source sera traduite en l'adresse publique de Ethernet1/0**.**

Conclusion :

Ce projet de création d'un réseau LAN sur GNS3 nous a permis de mettre en pratique des notions importante en réseau et de beaucoup nous améliorer.
Grâce à l'organisation (accès, distribution, cœur) nous avons pu structurer efficacement le réseau pour assurer modularité, robustesse, et gestion simplifiée.
Nous avons beaucoup pu apprendre sur :

- La segmentation du réseau via des VLANs pour renforcer la sécurité et l'efficacité.
- La redondance avec MST, VRRP et OSPF, garantissant une disponibilité et une stabilité élevées.
- L'intégration d'un serveur DHCP pour la gestion dynamique des adresses IP.
- L'utilisation du NAT pour l'accès internet des hôtes tout en préservant les adresses IPv4.

Nous avons pu rencontrer beaucoup de difficultés notamment avec la mise en place de VRRP mais finalement nous avons réussi à finir le projet et le faire fonctionner.