

SAE303 Concevoir un réseau multisites

Rapport LAN

Table des matières

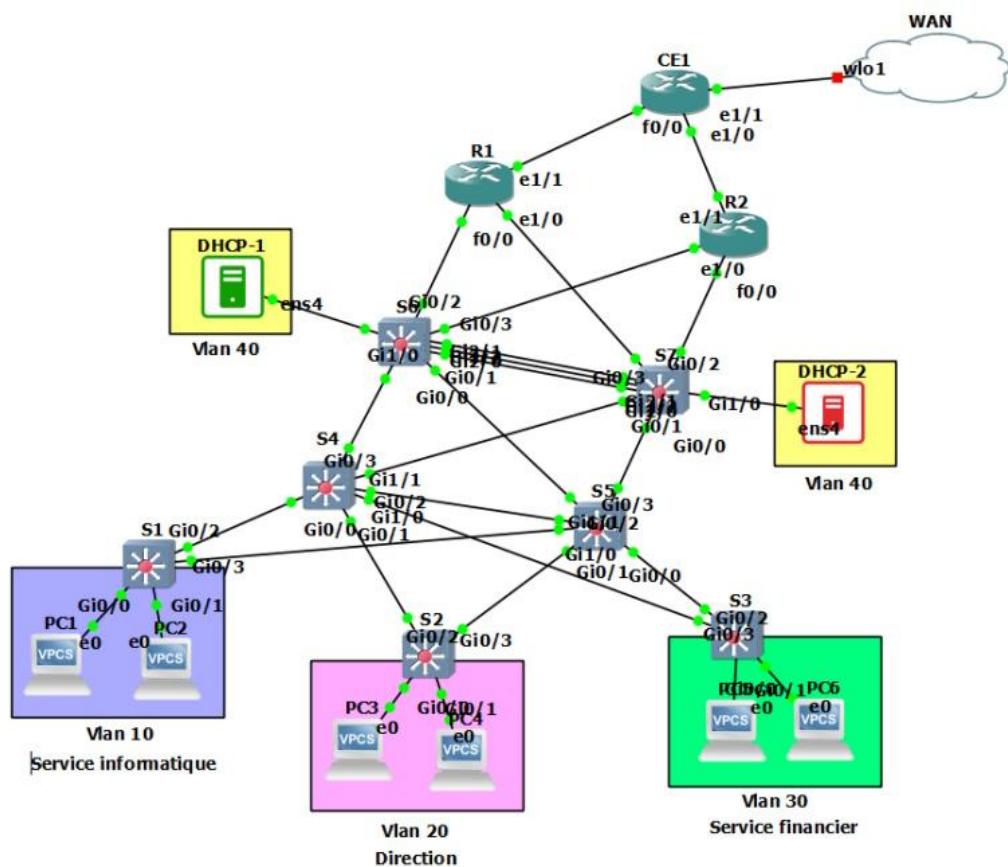
Introduction	2
VLANs - Segmentation du réseau	3
Architecture	3
Création	3
Affectation	4
Spanning tree - Gestion des boucles réseau	5
Serveurs DHCP - Adressage ip des postes	6
OSPF - Distribution des routes	8
VRRP - Redondance de la passerelle	9
NAT	10
Conclusion	10

Introduction

Ce projet a été réalisé par groupe de trois étudiants : FRITSCHY Mathéo, SADECK Rayane et STOCK Alexis. Il comportait trois grandes parties, un réseau LAN d'entreprise qui est décrit dans ce rapport, la partie services réseau ainsi que la partie WAN qui était en fait la liaison de plusieurs LAN d'entreprises et de leurs services grâce à un FAI.

La partie LAN a été réalisée sous GNS3 par moi-même et est un réseau de type «Three-tier layer» qui a pour but d'être hiérarchisé, redondant et robuste pour accepter des pannes matérielles et évolutif.

Voici la maquette :



VLANs - Segmentation du réseau

Architecture

Nous avons donc 4 vlans différents qui segmentent le réseau principal pour séparer les services de l'entreprise. Chaque réseau est défini par 10.242.xy.0 avec le numéro de vlan en y et le numéro du site de l'entreprise en x.

- Vlan 10 - Service informatique : **10.242.110.0/24**
 - ✧ Passerelle : 10.242.110.254
- Vlan 20 - La direction : **10.242.120.0/24**
 - ✧ Passerelle : 10.242.120.254
- Vlan 30 - Service financier : **10.242.130.0/24**
 - ✧ Passerelle : 10.242.130.254
- Vlan 40 - Serveurs : **10.242.140.0/24**
 - ✧ Passerelle : 10.242.140.254

Création

Sur un premier switch on crée les vlans et on configure le mode VTP en serveur pour les partager :

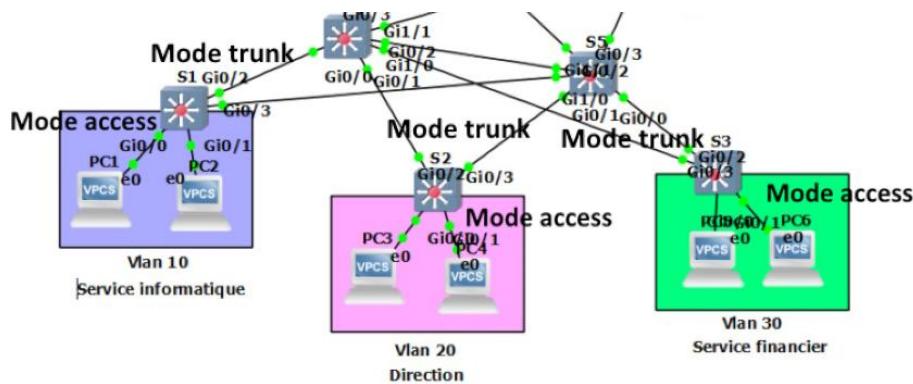
```
vtp domain UCExchange
vtp mode server
vlan 10
name Informatique
vlan 20
name Direction
vlan 30
name Finance
vlan 40
name Serveur
```

Sur les autres il suffit alors de faire :

```
vtp domain UCExchange
vtp mode client
```

Affectation

Pour les switchs d'accès que sont S1, S2 et S3, les ports reliés aux PCs des services sont en **mode access** et les autres ports qui les relient aux switchs supérieurs en **mode trunk**.



Pour cela :

```
interface range GigabitEthernet 0/0-1
switchport access vlan X
switchport mode access
```

Où X représente le numéro du Vlan du service où se trouve l'équipement.

Pour les autres liens (entre les switchs), on utilise à chaque fois le mode trunk pour transporter tous les vlans :

```
interface range GigabitEthernet X/X-X
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10, 20, 30, 40
switchport mode trunk
```

Le ping inter-VLAN est donc possible après configuration des passerelles de chaque vlan sur l'interface virtuelle du vlan :

```
PC3> ping 10.242.110.52
10.242.110.52 icmp_seq=1 timeout
10.242.110.52 icmp_seq=2 timeout
84 bytes from 10.242.110.52 icmp_seq=3 ttl=63 time=364.778 ms
84 bytes from 10.242.110.52 icmp_seq=4 ttl=63 time=396.943 ms
84 bytes from 10.242.110.52 icmp_seq=5 ttl=63 time=261.480 ms

PC3> ping 10.242.110.52
84 bytes from 10.242.110.52 icmp_seq=1 ttl=63 time=257.384 ms
84 bytes from 10.242.110.52 icmp_seq=2 ttl=63 time=300.005 ms
84 bytes from 10.242.110.52 icmp_seq=3 ttl=63 time=263.833 ms
84 bytes from 10.242.110.52 icmp_seq=4 ttl=63 time=308.908 ms
84 bytes from 10.242.110.52 icmp_seq=5 ttl=63 time=394.732 ms
```

Spanning tree - Gestion des boucles réseau

Le Spanning Tree, ici le **MST** (Multiple Spanning Tree) nous permet d'éviter les boucles réseau dans les configurations comme la notre où plusieurs switchs sont reliés entre eux et peuvent créer des communications infinies. MST utilise des instances pour regrouper des VLANs afin de gérer la charge réseau et la redondance. Ici nous regroupons les vlans 10 et 20 ensemble et 30 et 40 ensemble.

Voici la configuration commune aux deux switchs S6 et S7 :

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

Puis sur chacun des deux il faut inverser les valeurs de priorité des instances afin de définir les «root bridges» :

Sur le premier :

```
spanning-tree mst1 priority 4096      (devient le root bridge des vlans 10 et 20)
spanning-tree mst2 priority 8192
```

Et sur l'autre :

```
spanning-tree mst1 priority 8192      (devient le root bridge des vlans 30 et 40)
spanning-tree mst2 priority 4096
```

Serveurs DHCP - Adressage ip des postes

Les serveurs **DHCP** (Dynamix Host Configuration Protocol) permettent de donner aux machines une adresse ip en fonction du VLAN dans lequel elles se situent. Ces serveurs sont ici configurés sur des machines Linux grâce au service dhcpcd. Lors des validations, j'avais configuré les deux serveurs dhcp de la même manière, ce qui a de grandes chances de causer des conflits d'IP. Pour assurer une tolérance aux pannes, on peut effectivement créer deux serveurs DHCP mais avec différentes plages d'adresse. Ainsi, si un des serveurs DHCP tombe en panne, il sera toujours possible d'obtenir des adresses via le second.

Il est aussi possible d'utiliser un serveur pour la moitié des vlans et l'autre pour la seconde moitié afin de moins congestionner chaque serveur et pour éviter que toute la société soit bloqué en cas de panne.

Voici comment est configuré le serveur DHCP-1 :

Commencer par configurer l'adresse IPv4 du serveur dans le fichier de configuration /etc/network/interfaces, ajouter les lignes :

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

Pour configurer le DHCP en lui même, on précise d'abord quelle interface livrera le service DHCP dans le fichier : /etc/default/isc-dhcp-server où il faut que «**INTERFACESv4=ens4**» apparaisse sans commentaire.

```
GNU nano 7.2          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDV4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpcd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens4"
#INTERFACESv6=""
```

On configure ensuite le service DHCP dans /etc/dhcp/dhcpd.conf pour le premier serveur :

```
# Pour le Vlan 10 :  
subnet 10.242.110.0 netmask 255.255.255.0 {  
    range 10.242.110.1 10.242.110.25;  
    option routers 10.242.110.254;  
}  
# Pour le Vlan 20 :  
Subnet 10.242.120.0 netmask 255.255.255.0 {  
    range 10.242.120.1 10.242.120.25;  
    option routers 10.242.120.254;  
}
```

Et de la même façons pour les autres VLANs. La ligne subnet précise le réseau auquel il faut attribuer les adresses, la range définit l'adresse de début et de fin du DHCP et l'option routers définit la passerelle.

Pour le deuxième serveur, on fait la même chose mais avec le reste de la plage à définir, comme ceci pour les deux premiers VLANs :

```
# Pour le Vlan 10 :  
subnet 10.242.110.0 netmask 255.255.255.0 {  
    range 10.242.110.26 10.242.110.50;  
    option routers 10.242.110.254;  
}  
# Pour le Vlan 20 :  
Subnet 10.242.120.0 netmask 255.255.255.0 {  
    range 10.242.120.26 10.242.120.50;  
    option routers 10.242.120.254;  
}
```

OSPF - Distribution des routes

Il ne faut pas oublier de configurer la partie routage du réseau. Pour cela, il existe le protocole **OSPF** (Open Shortest Path First) qui facilite la circulation des routes entre les routeurs de façon dynamique. Il faut également le configurer sur les switchs de niveau 3 (S6 et S7).

Configuration Switch L3 :

```
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
```

Il s'agit en fait de déclarer tous les réseaux connectés, dont les liens entre chaque routeurs et chaque VLAN.

Il y en a donc moins pour les routeurs :

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
```

CE1 :

```
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
```

VRRP - Redondance de la passerelle

Le **VRRP** (Virtual Router Redundancy Protocol) crée des passerelles virtuelles qui peuvent être attribuées à plusieurs switchs L3 ou routeurs. Cela permet encore une fois une tolérance aux pannes car on définit une seule passerelle aux PCs mais si le switch L3 ou routeur qui avait cette adresse tombe en panne, l'autre reste accessible et permet donc la de maintenir la communication.

Voici la configuration à faire pour chaque interface de passerelle :

Premier Switch L3 (S6):

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

Second Switch L3 (S7):

```
interface Vlan10
ip address 10.242.110.102 255.255.255.0
vrrp 10 ip 10.242.110.254
vrrp 10 priority 90
```

Ainsi, les postes s'adressent à la passerelle 10.242.110.254 mais ne savent pas s'il s'agit du S6 ou S7. En temps normal, le S6 est prioritaire car il a la VRRP priority la plus élevée mais en cas de panne, il n'y aura aucune différence pour les PCs.

Cela dit, comme vu lors des validations, il aurait été préférable de configurer le VRRP au niveau des routeurs et non des switchs. Le principe de redondance reste le même mais à un autre niveau du réseau.

NAT

Pour accéder au WAN et aux autres sites, il faut configurer le NAT (Network Address Translation) sur le routeur de bordure CE1 afin de faire communiquer les adresses privées locales avec des adresses publiques grâce à CE1.

Création d'une ACL qui autorise le trafique du réseau local avec un masque inversé :

```
access-list 1 permit 10.242.0.0 0.0.255.255
```

Configuration de l'interface de sortie :

```
interface ethernet 1/1
ip nat outside
```

Interface fastethernet et ethernet 1/0 :

```
ip nat inside
Ip nat inside source list 1 interface ethernet 1/1 overload
```

Cette configuration a pour effet de faire passer le traffique sortant des interfaces «inside» par l'interface ethernet 1/1 qui est en overload car c'est elle qui est reliée à l'extérieur.

Conclusion

Cette architecture à trois niveaux utilise divers protocoles qui assurent la circulation de l'information de manière stable et évolutive. Grâce à cela, on obtient un réseau qui est à la fois :

- Segmenté : Grâce aux différents **VLANs** de chaque service interconnectés avec des liens **trunk**.
- Hiérarchisé : Chaque niveau du réseau a une tâche bien précise. On retrouve la partie accès directement reliée aux postes, la partie distribution juste au dessus puis la partie cœur de réseau.
- Disponible : Avec le **VRRP** qui donne le rôle de la passerelle à deux machines, aux deux serveurs **DHCP** qui assure une configuration IP continue et à la structure du **Spanning Tree** qui inclue plusieurs switch et gère les boucles réseau tout en gérant plusieurs routes de secours. Les règles **NAT** assurent une connexion au réseau externe.
- Evolutif : Il n'est pas compliqué d'ajouter un service ou un appareil sur le réseau, il suffit d'ajouter un VLAN qui sera partagé via le **VTP**, il faut juste configurer les liens trunks et access. Un poste reçoit automatiquement un adressage sans configuration particulière.