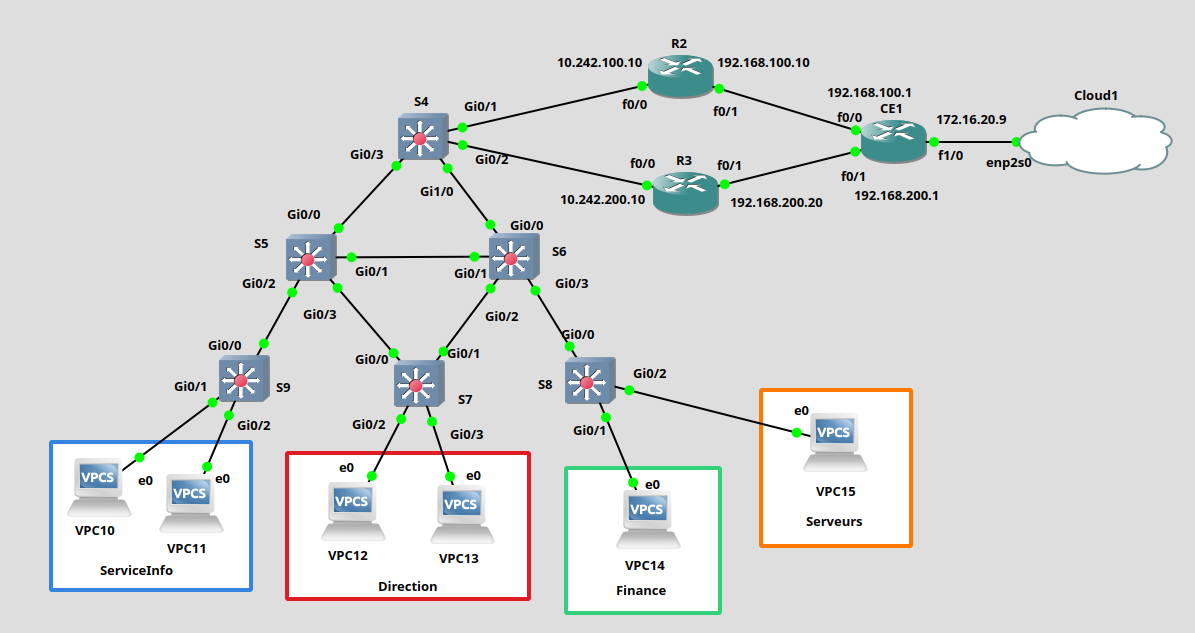
**Rapport partie LAN**

**1-Architecture de mon Réseau**

**2-Protocoles utilisés**

**3-Explications de ma topologie**



**1-Architecture de mon Réseau**

**1.1 Les VPCs**

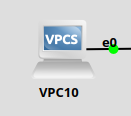
Mon réseau est composé de 6 PCs qui composent 4 VLANs:

**VLAN Service Informatique** (en bleu)

**VLAN Direction** (en rouge)

**VLAN Finance** (en vert)

**VLAN Serveurs** (en orange)



**Les PCs** (VPC10, VPC11, VPC12, VPC13, VPC14, VPC15)

**-VPC10 et VPC11** (ServiceInfo) : Deux postes de la section « ServiceInfo ». Ce sont des hôtes finaux qui envoient et reçoivent du trafic sur le réseau.

**-VPC12 et VPC13** (Direction) : Deux postes de la « Direction ». C’est le même principe : hôtes finaux pour cette équipe.

**-VPC14** (Finance) : Poste de la « Finance ».

**-VPC15** (Serveurs) : Poste/serveur pour les services (base de données, application, etc.) accessible par les autres machines.

**1.2 Les Switchs**

Les Switchs forment la couche de distribution de mon réseau.

Ils permettent l’interconnexion des PC entre eux et l’interconnexion vers les routeurs.

Le Switch 4 est un nœud qui relie les Switchs du bas (S5 et S6) avec les Routeurs (R2 et R3).

Les Switchs S5, S6, S7, S8 et S9 servent à segmenter les différentes zones et à se répartir le trafic. Ils gèrent aussi les VLANs.

**1.3 Les Routeurs**

R2 et R3 assurent le routage entre les différents réseaux IP. Ils permettent aussi d’acheminer le trafic vers CE1 ou de servir de redondance.

CE1 est le Customer Edge Routeur. Il est le routeur de sortie vers le WAN ou vers l'extérieur.. Il connecte le réseau interne au Cloud1 (le WAN). En gros, c’est la passerelle qui va fournir l’accès vers internet.

**1.4 Le Cloud**

Il représente l’accès à internet.

**Cette partie concerne la partie de Marius Keltz qui s’occupe du FAI**

**2-Protocoles utilisés**

**2.1Routage Dynamique : OSPF**

OSPF (Open Shortest Path First) est un protocole de routage dynamique de type link-state. Il permet aux routeurs de partager leurs informations de topologie de réseau de manière hiérarchique (avec des aires). Chaque routeur calcule alors le meilleur chemin (Shortest Path First) vers toutes les destinations qu’il connaît.

Par exemple, sur mon **Switch 4**, je rentre la commande suivante:

*router ospf 1*

*redistribute connected subnets*

*redistribute static subnets*

*network 10.242.0.0 0.0.255.255 area 0*

Cela signifie que le routeur S4 participe au processus OSPF, il annonce les réseaux connectés et les réseaux statiques.

10.242.x.x est couvert par l’aire 0.

Pour le **Routeur 2**, voici mes commandes:

*router ospf 1*

*redistribute connected subnets*

*redistribute static subnets*

*network 10.242.20.0 0.0.0.255 area 0*

*network 10.242.0.0 0.0.255.255 area 0*

*network 192.168.200.0 0.0.0.255 area 0*

R2 annonce donc les sous-réseaux 10.242.20.x, 10.242.100.x, 172.16.20.x et 192.168.100.x via OSPF.

Le **Routeur 3** va annoncer d’autres réseaux:

*router ospf 1*

*redistribute connected subnets*

*redistribute static subnets*

*network 10.242.20.0 0.0.0.255 area 0*

*network 10.242.0.0 0.0.255.255 area 0*

*network 192.168.200.0 0.0.0.255 area 0*

Pour finir, le **Routeur CE1** partage le réseau du WAN → 172.16.20.8 ainsi que les réseaux des routeurs **R2** et **R3** → 192.168.100.0 /// 192.168.200.0

Ce protocole sert à ce que les routeurs s’échangent leurs routes de façon dynamique.

Chaque routeur connaît alors la topologie sans même qu’il ait la configuration manuelle.

**2.2Protocole de Redondance → VRRP**

Le protocole VRRP (Virtual Router Redundancy Protocol) permet de configurer plusieurs routeurs en passerelles virtuelles redondantes pour un réseau local. Un routeur est élu Master et les autres sont en Backup. L’adresse IP virtuelle est utilisée par les hôtes comme passerelle par défaut.

Routeur2 →

*interface FastEthernet0/0*

*ip address 10.242.100.10 255.255.255.0*

*vrrp 1 ip 10.242.100.1*

*vrrp 1 priority 120*

Le routeur 2 fait donc partie du groupe VRRP numéro 1.

Routeur3 →

*interface FastEthernet0/0*

*ip address 10.242.200.10 255.255.255.0*

*vrrp 1 ip 10.242.100.1*

*vrrp 1 priority 240*

Le routeur 3 fait aussi partie du groupe VRRP 1. La seule différence est que leur priorité n’est pas la même.

**R2** et **R3** se partagent une adresse IP virtuelle.

**2.3 NAT (Network Address Translation)**

Le NAT permet de faire correspondre des adresses privées à une adresse publique lors de la sortie vers Internet ou vers le WAN. Il existe plusieurs modes de NAT comme le PAT (Port Address Translation).

Routeur2 →

*ip nat inside source list 1 interface FastEthernet0/0 overload*

Routeur3 →

*ip nat inside source list 1 interface FastEthernet0/0 overload*

Routeur CE1 →

*interface FastEthernet0/0*

*ip nat outside*

*interface FastEthernet0/1*

*ip nat outside*

*interface FastEthernet1/0*

*ip nat inside*

*ip nat inside source list 1 interface FastEthernet1/0 overload*

*...*

*access-list 1 permit 10.242.10.0 0.0.0.255*

*access-list 1 permit 10.242.20.0 0.0.0.255*

*access-list 1 permit 10.242.30.0 0.0.0.255*

*access-list 1 permit 10.242.40.0 0.0.0.255*

Ici, Fa0/0 et Fa0/1 sont déclarées “outside”, tandis que Fa1/0 est “inside”.

L’ACL 1 autorise les sous-réseaux 10.242.x.x (les VLANs 10, 20, 30 et 40).

CE1 réalise la traduction vers le WAN quand ces flux sortent via l’interface Fa1/0.

**2.4 DHCP (Dynamic Host Configuration Protocol)**

Le DHCP automatise l’attribution d’adresses IP et de passerelles par défaut.

Ici, c’est le **Switch4** (un switch L3) qui sert de serveur DHCP pour les VLAN10, VLAN20, VLAN30 et VLAN40.

Voici la configuration de mon DHCP sur le Switch4.

*ip dhcp pool vlan20*

*network 10.242.20.0 255.255.255.0*

*default-router 10.242.20.1*

*dns-server 8.8.8.8*

*ip dhcp pool vlan10*

*network 10.242.10.0 255.255.255.0*

*default-router 10.242.10.1*

*dns-server 8.8.8.8*

*ip dhcp pool vlan30*

*network 10.242.30.0 255.255.255.0*

*default-router 10.242.30.1*

*dns-server 8.8.8.8*

*ip dhcp pool vlan40*

*network 10.242.40.0 255.255.255.0*

*default-router 10.242.40.1*

*dns-server 8.8.8.8*

Les hôtes dans chaque VLAN recevront une adresse IP en 10.242.X.0/24, la passerelle associée (10.242.X.1) et un serveur DNS (8.8.8.8).

**2.5 Spanning Tree MST (Multiple Spanning Tree)**

Le protocole Spanning Tree sert à éviter les boucles dans les réseaux.

MST permet de regrouper plusieurs VLAN dans une instance MST. Ça va donc réduire la charge de calcul.

Switch 4 →

*spanning-tree mode mst*

*spanning-tree mst configuration*

*name Region\_MST*

*revision 1*

*instance 1 vlan 10-20*

*instance 2 vlan 30-40*

Le Switch4 active le protocole MST.

Il active ensuite les instances 1 et 2. L’instance 1 gère les VLANs 1 et 2. L’instance 2 gère les VLANs 3 et 4.

**2.6 Gestion des VLANs**

Chaque VLAN a sa propre interface sur le **Switch4**, servant de default gateway.

Les liaisons entre routeurs sont configurées en mode trunk (encapsulation dot1q).

Switch4 →

*interface GigabitEthernet0/3*

*switchport trunk allowed vlan 10,20,30,40*

*switchport trunk encapsulation dot1q*

*switchport mode trunk*

Tous les VLANs que j’ai créés sont autorisés sur ce trunk.

Interfaces de mes VLANs

*interface Vlan10*

*ip address 10.242.10.1 255.255.255.0*

*interface Vlan20*

*ip address 10.242.20.1 255.255.255.0*

*interface Vlan30*

*ip address 10.242.30.1 255.255.255.0*

*interface Vlan40*

*ip address 10.242.40.1 255.255.255.0*

Chacune de ces interfaces est configurée pour servir de passerelle au sein de chaque VLAN.

**2.7 Routes Statiques**

Même si j’utilise OSPF, il y a quand même des routes statiques.

Switch4 →

*ip route 0.0.0.0 0.0.0.0 10.242.100.10*

*ip route 172.16.0.0 255.255.0.0 10.242.100.10*

**Switch4** envoi le trafic par défaut vers **Routeur2.**

Routeur2 →

*ip route 0.0.0.0 0.0.0.0 192.168.100.1*

Le **Routeur2** envoi les routes par défaut vers le **CE1**.

Routeur3 →

*ip route 0.0.0.0 0.0.0.0 192.168.0.1*

CE1 →

*ip route 0.0.0.0 0.0.0.0 10.129.6.160*

CE1 a une route par défaut qui pointe vers 10.129.6.160.

C’est la passerelle pour atteindre le WAN.

**2.8 ACL (Access-list Protocol)**

Les ACLs permettent de contrôler le trafic en acceptant ou refusant certaines plages d’adresses IP.

CE1 →

*access-list 1 permit 10.242.10.0 0.0.0.255*

*access-list 1 permit 10.242.20.0 0.0.0.255*

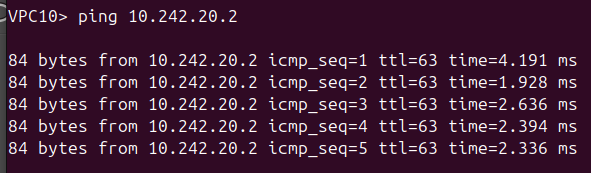
*access-list 1 permit 10.242.30.0 0.0.0.255*

*access-list 1 permit 10.242.40.0 0.0.0.255*

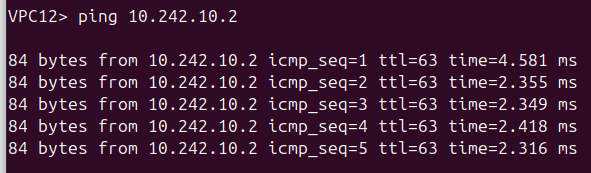
ACL 1 autorise les réseaux 10.242.x.x, qu’il associe ensuite à → ip nat inside source list 1 interface FastEthernet1/0 overload.

**Pings Inter-VLANs**

Dans ma topologie, chaque VLAN peut communiquer avec un autre. Par exemple, un VPC du VLAN 10 peut communiquer avec un VPC du VLAN 20.



Dans cet exemple, je ping le VPC 12 avec le VPC 10.



Cette fois-ci, je ping le VPC 10 à partir du VPV 12.

Je peux donc ping entre chaque VLANs.

**Conclusion Générale**

Mon architecture combine plusieurs protocoles qui assurent:

-La circulation des informations entre les différents VLAN (grâce au routage **OSPF**)

-La haute disponibilité de mon réseau (grâce à **VRRP**, où R2 et R3 ont un rôle de passerelle virtuelle)

-La simplicité de gestion des IP (grâce au **DHCP**)

-L’accès vers l’extérieur (grâce au **NAT** sur R2, R3 et CE1)

-La sécurité de base (grâce aux **ACLs** pour le NAT).

-La robustesse (grâce à **MSTP** qui empêche les boucles)