

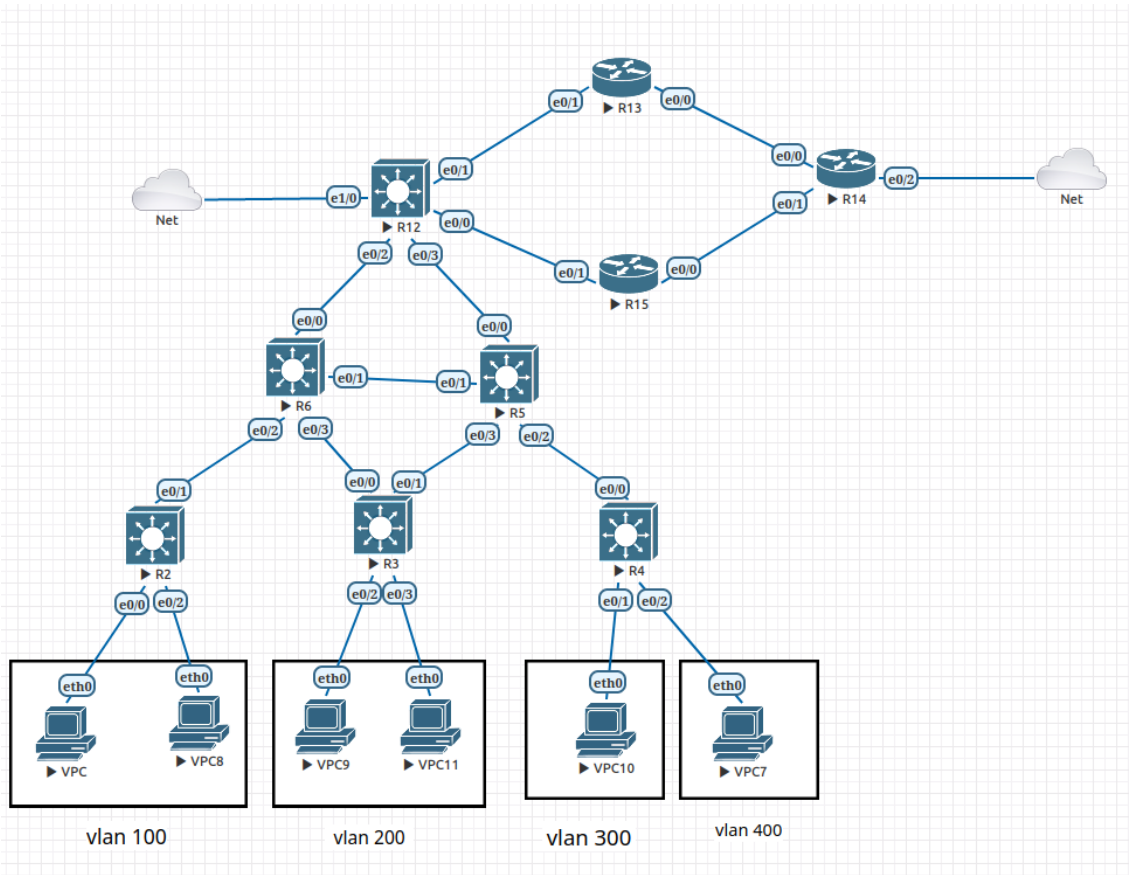
# **Rapport SAE 3.03 Partie LAN**

**Desvernois Louis, Brutschy Jules, Bilger Thomas**

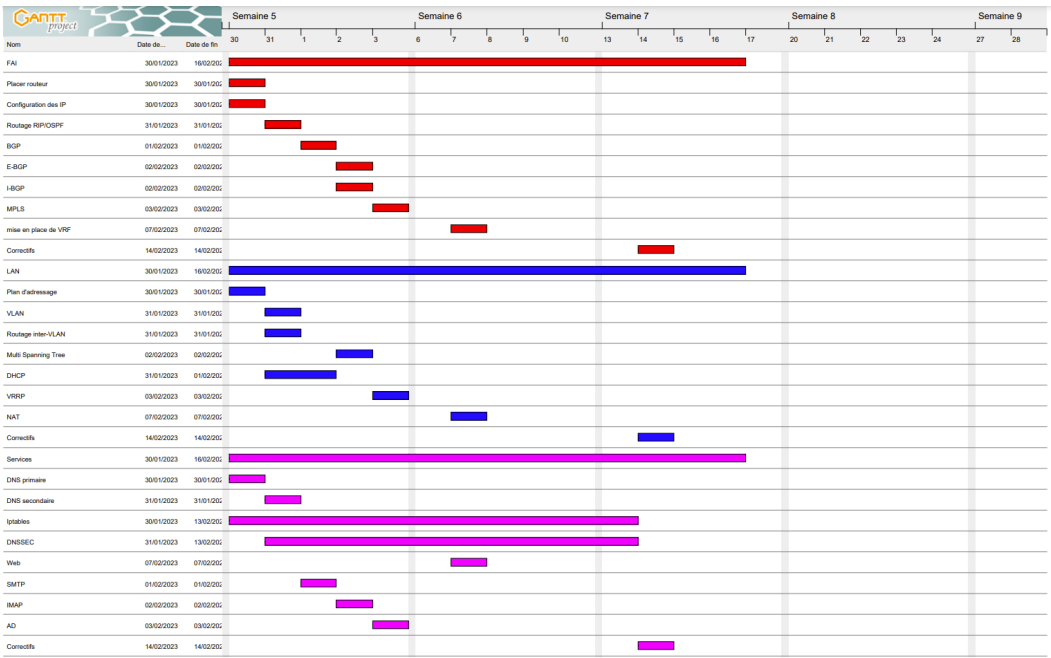
## Sommaire

Rapport SAE 3.03 Partie LAN.....	1
Plan d'adressage.....	3
Mise en place des vlans.....	3
Routage inter-vlan.....	4
Multi spanning-tree.....	4
DHCP.....	5
VRRP.....	5
NAT overloaded.....	7
Conclusion.....	8

Dans ce rapport vous trouverez toutes l'étapes pour configurer le LAN ci-dessous.



Lors de la mise en place de la maquette nous avons suivi le déroulé suivant (partie bleu).



## Plan d'adressage

Pour le découpage d'adresses de cette maquette, un réseau nous a été attribué.

- 10.242.xy.0/17

x étant le numéro de la succursale et y étant le numéro du vlan.

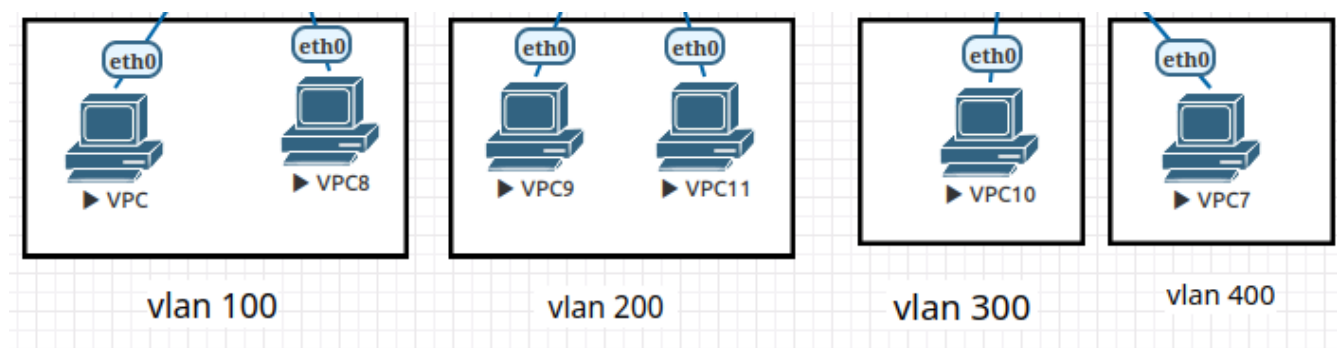
nous avons donc pour notre succursale le plan suivant:

- 10.242.11.0/24 pour le valn 100
- 10.242.12.0/24 pour le vlan 200
- 10.242.13.0/24 pour le vlan 300
- 10.242.14.0/24 pour le vlan 400

Pour des raisons de simplicités chaque sous-réseaux et en /24

## Mise en place des vlans

Dans un premier temps il est essentiel de mettre en place les différents vlans qui composent le réseau.



Ici nous mettons en place 4 vlans sur le switch de layer 3 (R12) 100/200/300/400 avec leur adresse IP associée, grâce aux commandes suivantes.

```
switch>en
switch#conf t
switch(config)#int vlan 100
switch(config-if)#ip address 10.242.11.1
```

Ces commandes sont a répéter pour chaque vlan.

Sur les switches du bas de l'arborescence (R2/R3/R4), configurez les différentes interfaces en fonction de leur vlan.

```
switch>en
switch#conf t
switch(config)#int eth 0/0
switch(config-if)switchport access vlan 100
```

Commandes à répéter pour chaque interface concernée.

## Routage inter-vlan

Maintenant que nous avons configuré les différents vlans, nous souhaitons qu'ils puissent communiquer entre eux. Pour cela nous allons faire du routage inter-vlan. Sur chaque switch qui compose l'arborescence. Pour cela nous appliquons les commandes suivantes.

```
switch>en
switch#conf t
switch(config)#int range eth 0/x-x <--le x désigne les interfaces de
l'encapsulation
switch(config-if)switchport trunk encapsulation dot1q
switch(config-if)switchport mode trunk
```

exemple avec R2

```
interface Ethernet0/0
  switchport access vlan 100
!
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/2
  switchport access vlan 100
!
interface Ethernet0/3
!
```

exemple avec R6

```
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Pour vérifier que tout est en ordre attribuez une adresse fixe sur les pc qui composent les vlans et tentez un ping d'un vlan à l'autre.

## Multi spanning-tree

Le protocole MST est un protocole de niveau 2 (couche liaison de données) qui permet de créer plusieurs instances de Spanning Tree Protocol (STP) sur un même réseau. Cela permet d'éviter les boucles de commutation et de maximiser l'utilisation de la bande passante.

Pour mettre en place ce protocole nous allons utiliser les commandes suivantes

```
switch>en
switch#conf t
switch(config)#spanning-tree mode mst
switch(config)#spanning-tree mst configuration
switch(config-mst)#name NETWORKLESSONS
switch(config-mst)#revision 1
switch(config-mst)#instance 1 vlan 1,100,200,300,400
```

Pensez à ajouter une prioriter sur le switch de layer 3 avec la commande

```
switch(config)#spanning-tree mst 1 priority 4096
```

## DHCP

Nous souhaitons dès à présent avoir des adresses dynamiques sur les machines qui composent le LAN. Pour cela nous mettons en place plusieurs pools-DHCP sur le switch de layer 3, grâce aux commandes suivantes.

```
switch>en
switch#conf t
switch(config)#ip dhcp pool 100
switch(dhcp-config)# network 10.242.11.0 255.255.255.0
switch(dhcp-config)#default-router 10.242.11.1
switch(dhcp-config)#lease 4
```

Ces commandes sont à répéter pour chaque VLAN.

De plus nous devons exclure l'adresse des VLANs pour cela nous utilisons la commande

```
switch(config)#ip dhcp excluded-address 10.242.11.1
```

Faites de même avec les autres adresses des VLANs.

## VRRP

Maintenant que toute la partie switch est configurée nous allons nous attaquer aux routeurs. Commençons par R13 et R15, avec l'attribution des IP aux interfaces.

- Les interfaces e0/1 les adresses sont en 10.242.10.1/24(R13) et 10.242.10.2/24(R15)
- Les interfaces e0/0 les adresses sont en 192.168.10.1/30(R13) et 192.168.10.5/30(R15)

Si vous tentez de faire un ping d'un PC vers une interface des routeurs vous verrez que le ping ne passe pas.

Pour remédier à ça nous allons mettre en place un routage RIP sur les routeurs R13, R15 et sur le switch R12 avec les commandes qui suivent.

```
router(config)#router rip
router(config-router)#version 2
router(config-router)#network 10.242.0.0
```

```
router rip
version 2
network 10.0.0.0
```

Des à présents nous pouvons effectuer des ping des pc vers les interffaces des routeurs R13 et R15.

Passons à la mise en place de VRRP, le protocole VRRP permet de créer un groupe virtuel de routeurs qui partagent une adresse IP virtuelle pour fournir une redondance et améliorer la disponibilité et la fiabilité des réseaux. Le routeur virtuel est élu parmi les routeurs du groupe et les autres routeurs du groupe sont des routeurs de sauvegarde qui prennent le relais si le routeur virtuel devient indisponible. Ici nous mettons ce protocole sur les routeurs R13 et R15 (routeur de sauvegarde).

#### Commandes pour R13

```
router(config)#int ethernet0/1
router(config-if)#vrrp 1 ip 10.242.10.3
router(config-if)#vrrp 1 timers advertise msec 100
router(config-if)#vrrp 1 priority 110
router(config-if)#vrrp 1 authentication Finger
```

#### Commandes pour R15

```
router(config)#int ethernet0/1
router(config-if)#vrrp 1 ip 10.242.10.3
router(config-if)#vrrp 1 timers learn
router(config-if)#no vrrp 1 preempt
router(config-if)#vrrp 1 authentication Finger
```

#### configuration vrrp de R13

```
Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.242.10.3
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 0.100 sec
Preemption enabled
Priority is 110
Authentication text, string "Finger"
Master Router is 10.242.10.1 (local), priority is 110
Master Advertisement interval is 0.100 sec
Master Down interval is 0.870 sec
```



## configuration vrrp de R15

```
Ethernet0/1 - Group 1
  State is Backup
  Virtual IP address is 10.242.10.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption disabled
  Priority is 100
  Authentication text, string "Finger"
  Master Router is 10.242.10.1, priority is 110
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.608 sec) Learning
```

## NAT overloaded

Dernière étape mais pas des moindres de notre configuration du LAN. Le NAT overloaded permet de limiter le nombre d'adresses IP publiques nécessaires pour un réseau en permettant à plusieurs périphériques d'accéder à Internet en utilisant une seule adresse IP publique.

Pour cela il faut tout d'abord configurer notre routeur R14

- Donner des adresses ip aux interfaces
  - 192.168.10.2/30 pour eth 0/0
  - 192.168.10.6/30 pour eth 0/1
  - 192.168.20.10/24 pour eth 0/2
- Ajouter un routage RIP pour le réseau 192.168.10.0

Ensuite nous pouvons installer le NAT avec les commandes

```
router(config)#int eth 0/0
router(config-if)#ip nat inside
router(config-if)#ip virtual-reassembly in
```

Même chose pour l'interface eth 0/1

Sur l'interface eth 0/2

```
router(config)#int eth 0/0
router(config-if)#ip nat outside
router(config-if)#ip virtual-reassembly in
```

Creation d'une acl pour permettre la translation des adresses du réseau avec

```
router(config)#ip acces-list standard PAT
router(config-std-nacl)permit 10.242.8.0 0.0.7.255
router(config-std-nacl)exit
router(config)ip nat inside source list PAT interface Ethernet0/2 overload
```

L'adresse renseigné couvre toutes les adresses ip de la succursale.

Pour verfié que vorte NAT fonctionne tentez de faire un ping entre un pc de votre LAN vers un pc extérieur au LAN. Si le ping passe correctement, vous pouvez tpaer la commande suivante sur R14

```
router#sh ip nat translation
```

```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 192.168.20.1:17    10.242.10.254:17  192.168.20.2:17    192.168.20.2:17
```

Nous pouvons voir que la translation d'ip est bel et bien faite.

## Conclusion

Nous avons les différents protocoles qui permettent de mettre en place notre LAN. Avec la création des vlan qui ajoute une gestion des sous réseaux et une première couche de sécurité. L'interconnection des vlan permettant la communication au sein du réseau. Le multi spanning tree qui permet d'éviter les boucles de commutation. Le DHCP donnant des adresses ip aux équipements du LAN. Le VRRP assurant une redondance au niveau des routeurs. Enfin le NAT overloaded permettant de communiquer vers l'extérieur du LAN avec une adresse publique. Nous pouvons donc voir que ces différents protocoles sont indispensable au bon fonctionnement d'un LAN simple.