Compte rendu

-

SAE3.CYBER.03

Date	05/02/2025
Membre	LEBON Johan MONTEGU Jérémie LEPERLIER Aymeric

Table des matières

Introduction **4**
Plan d'adressage des sites **5**
Configuration du site 1 ..... **7**
Topologie du Site : **7**
Liste des équipements utilisés : **8**
Configuration des Commutateurs de distribution L3 ..... **8**
- Configuration de SD1 8
- Configuration de SD2 12
Configuration des Commutateurs d'accès L2 ..... **15**
- Configuration de SA1 15
- Configuration de SA2 17
- Configuration de SA3 19
Configuration des ACL **21**
Réalisation des tests sur le site **23**
Configuration de l'interconnexion des sites **31**
Topologie pour l'interconnexion des sites : **31**
Liste des équipements utilisés : **31**
Plan d'adressage : **32**
Configuration des Commutateurs de distribution L3 ..... **33**
- Configuration de ESW7 33
- Configuration de ESW8 34
- Configuration de ESW9 35
Configuration des routeurs (Cisco 7200) **37**
- Configuration de PE1 37
- Configuration de PE2 41
- Configuration de PE3 44
- Configuration de P (routeur coeur du réseau opérateur) 47
Réalisations des tests : **49**
Réajustement des ACL sur les routeurs PE : **53**
Conclusion **57**
Tableau des acronymes **58**
Annexe **59**
Configuration du Site 2 : **59**
Configuration de SD3 : 59
Configuration de SD4 : 61
Configuration de SA4 : 64

Configuration de SA5 : 65
Configuration de SA6 : 66
Configuration du Site 3 : 68
Configuration de SD5 : 68
Configuration de SD6 : 70
Configuration de SA7 : 73
Configuration de SA8 : 74
Configuration de SA9 : 75

Introduction

Dans le cadre du projet **SAÉ 3.Cyber.03** intitulé *Concevoir un réseau informatique sécurisé multi-sites*, l'objectif était de concevoir et de mettre en œuvre une infrastructure réseau sécurisée interconnectant trois sites distants via un **VPN MPLS**.

En tant que futurs professionnels en **réseaux et télécommunications**, spécialisés en **cybersécurité**, ce projet nous a permis d'aborder des problématiques concrètes liées à la conception, à l'administration et à la sécurisation des **réseaux multi-sites**.

Ce compte rendu présente les étapes de réalisation, les défis rencontrés, les solutions mises en œuvre ainsi que les résultats obtenus. Il met également en avant les connaissances pratiques acquises dans des domaines clés tels que le **routage dynamique, la sécurité réseau** et l'administration d'infrastructures complexes.

Plan d'adressage des sites

	Site 1	Site 2	Site 3
VLAN 10/ 11 / 12	192.168.10.0/24	192.168.11.0/24	192.168.12.0/24
VLAN 20/ 21 / 22	192.168.20.0/24	192.168.21.0/24	192.168.22.0/24
VLAN 30/ 31 / 32	192.168.30.0/24	192.168.31.0/24	192.168.32.0/24
VLAN 40/ 41 / 42	192.168.40.0/24	192.168.41.0/24	192.168.42.0/24
VLAN 50/ 51 / 52	192.168.50.0/24	192.168.51.0/24	192.168.52.0/24
Switchs SDs de chaque site sur les interfaces vlans	192.168.10.1 /24 192.168.20.1 /24 192.168.30.1 /24 192.168.40.1 /24 192.168.50.1 /24 192.168.10.2 /24 192.168.20.2 /24 192.168.30.2 /24 192.168.40.2 /24 192.168.50.2 /24	192.168.11.1 /24 192.168.21.1 /24 192.168.31.1 /24 192.168.41.1 /24 192.168.51.1 /24 192.168.11.2 /24 192.168.21.2 /24 192.168.31.2 /24 192.168.41.2 /24 192.168.51.2 /24	192.168.12.1 /24 192.168.22.1 /24 192.168.32.1 /24 192.168.42.1 /24 192.168.52.1 /24 192.168.12.2 /24 192.168.22.2 /24 192.168.32.2 /24 192.168.42.2 /24 192.168.52.2 /24
Redondance HSRP (pour chaque vlan)	192.168.10.254 192.168.20.254 192.168.30.254 192.168.40.254 192.168.50.254	192.168.11.254 192.168.21.254 192.168.31.254 192.168.41.254 192.168.51.254	192.168.12.254 192.168.22.254 192.168.32.254 192.168.42.254 192.168.52.254
PC - RH	192.168.10.10 /24 gtw : 192.168.10.254	192.168.11.10 /24 gtw : 192.168.11.254	192.168.12.10 /24 gtw : 192.168.12.254
PC - VENTES	192.168.20.10 /24 gtw : 192.168.20.254	192.168.21.10 /24 gtw : 192.168.21.254	192.168.22.10 /24 gtw : 192.168.22.254
PC - ADMIN	192.168.40.10 /24 gtw : 192.168.40.254	192.168.41.10 /24 gtw : 192.168.41.254	192.168.42.10 /24 gtw : 192.168.42.254
PC - SERVEUR-RH	192.168.30.10 /24 gtw :	192.168.31.10 /24 gtw :	192.168.32.10 /24 gtw :

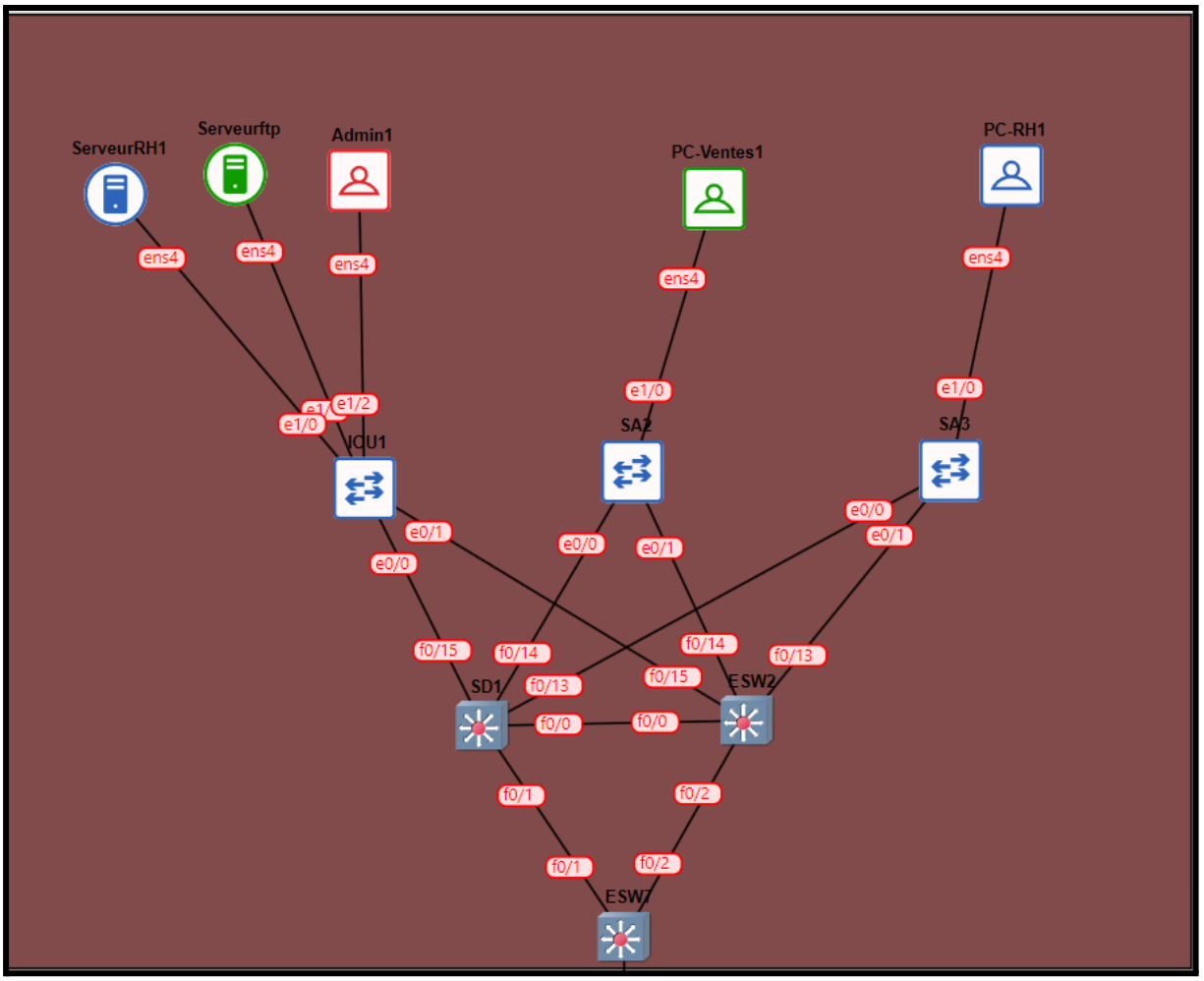
	192.168.30.254	192.168.31.254	192.168.32.254
PC - SERVEUR-FTP	192.168.30.20 /24 gtw : 192.168.30.254	192.168.31.20 /24 gtw : 192.168.31.254	192.168.32.20 /24 gtw : 192.168.32.254

Configuration du site 1

Topologie du Site :

Le **site 1** est constitué de plusieurs **commutateurs interconnectés** qui assurent la distribution du trafic vers les différents équipements du réseau. Les machines connectées incluent **ServeurRH1, ServeurFTP, Admin1, PC-Ventes1 et PC-RH1**.

Les **liens entre commutateurs** sont configurés en **trunk**, permettant ainsi le transport de plusieurs VLANs sur une seule liaison physique.



Liste des équipements utilisés :

Pour la mise en place de cette infrastructure réseau, nous avons utilisé :

- **3 commutateurs de distribution L3 (Etherswitch)** : ils assurent le routage inter-VLAN et l'agrégation du trafic vers l'extérieur du site.
- **2 commutateurs d'accès L2 (Cisco IOU L2)** : ils permettent la connexion des hôtes aux VLANs correspondants.
- **5 machines Debian** : parmi elles, deux serveurs (un serveur RH et un serveur FTP) et trois postes clients, représentant les différents services du site.

Configuration des Commutateurs de distribution L3

- Configuration de SD1

Dans un premier temps, nous avons défini les VLANs nécessaires sur le commutateur SD1 en respectant l'organisation du réseau :

```
vlan database
vlan 10 name RH_SITE1
vlan 20 name Ventes_SITE1
vlan 30 name Serveurs_SITE1
vlan 40 name Gestion_SITE1
vlan 50 name Wifi_SITE1
exit
```

Ensuite, nous avons attribué une adresse IP aux interfaces VLAN correspondantes, tout en intégrant le protocole **HSRP** pour assurer la redondance des passerelles :

```
enable
conf t
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 standby 10 ip 192.168.10.254
 standby 10 priority 110
 standby 10 preempt
no sh
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 standby 20 ip 192.168.20.254
no sh
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 standby 30 ip 192.168.30.254
 standby 30 priority 110
 standby 30 preempt
no sh
interface vlan 40
 ip address 192.168.40.1 255.255.255.0
 standby 40 ip 192.168.40.254
no sh
interface vlan 50
 ip address 192.168.50.1 255.255.255.0
 standby 50 ip 192.168.50.254
 standby 50 priority 110
 standby 50 preempt
no sh
end
```

Par ailleurs, nous avons configuré les liaisons trunk entre les commutateurs SD et SA afin de permettre le passage des différentes VLANs :

```
enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/1
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/15
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

end
```

Cette approche assure que tous les VLANs nécessaires sont bien propagés entre les équipements du site.

Enfin, nous avons activé le protocole **PVST+** pour garantir la stabilité du réseau en définissant **SD1 comme root bridge pour le VLAN RH (VLAN 10)** :

```
conf t
spanning-tree vlan 10 priority 24576 // Root bridge pour vlan 10
end
```

Cette configuration assure une gestion efficace des chemins actifs et évite les boucles réseau.

Puis, on va configurer le protocole OSPF qui servira pour l'interconnexion des sites qui permet d'annoncer les réseaux du site 1 :

```
conf t
ip routing
router ospf 4
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
end
```

Une fois terminée la configuration on sauvegarde avec la commande :

```
wr
```

- **Configuration de SD2**

Comme sur SD1, on a créé les VLANs sur SD2.

```
vlan database
vlan 10 name RH_SITE1
vlan 20 name Ventes_SITE1
vlan 30 name Serveurs_SITE1
vlan 40 name Gestion_SITE1
vlan 50 name Wifi_SITE1
exit
```

De manière similaire à SD1, nous avons configuré SD2 pour prendre en charge le routage inter-VLAN et assurer la redondance avec **HSRP**.

```
enable
conf t
interface vlan 10
 ip address 192.168.10.2 255.255.255.0
 standby 10 ip 192.168.10.254
no sh
exit
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
 standby 20 ip 192.168.20.254
 standby 20 priority 110
 standby 20 preempt
no sh
exit
interface vlan 30
 ip address 192.168.30.2 255.255.255.0
 standby 30 ip 192.168.30.254
no sh
exit
interface vlan 40
 ip address 192.168.40.2 255.255.255.0
 standby 40 ip 192.168.40.254
 standby 40 priority 110
 standby 40 preempt
```

```
no sh
exit
interface vlan 50
 ip address 192.168.50.2 255.255.255.0
 standby 50 ip 192.168.50.254
no sh
end
```

Comme sur SD1, après avoir configuré les adresses IP, on a mis en place le routage inter-VLAN sur SD2. Les liens entre SD1, SD2 et les SAs ont été configurés en trunk pour permettre le passage des VLANs.

```
enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/2
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/15
no sh
```

```
switchport mode trunk
switchport trunk allowed vlan 1-1005
end
```

La principale différence est que SD2 est défini comme root bridge pour le VLAN Ventes (VLAN 20).

On configure le protocole PVST+ pour respecter le cahier des charges et on définit le VLAN Ventes (VLAN 20) comme root primaire sur SD2.

```
conf t
spanning-tree vlan 20 priority 24576
end
```

Puis, on va configurer le protocole OSPF qui servira pour l'interconnexion des sites qui permet d'annoncer les réseaux du site 1.

```
conf t
ip routing
router ospf 4
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
end
```

Et une fois la configuration de SD2 terminée on sauvegarde la config avec la commande :

```
wr
```

Configuration des Commutateurs d'accès L2

- Configuration de SA1

Comme pour les commutateurs d'accès L3, on a d'abord créé les VLANs.

```
enable
configure terminal
vlan 10
name VLAN_RH
no sh
exit
vlan 20
name VLAN_Ventes
no sh
exit
vlan 30
name VLAN_Serveurs
no sh
exit
vlan 40
name VLAN_Gestion
no sh
exit
vlan 50
name VLAN_Wifi
no sh
exit
```

Une fois les vlans créés, nous avons attribués les vlans à des interfaces du commutateur en suivant la topologie :

```
interface e1/0
switchport mode access
switchport access vlan 30
no sh
exit
interface e1/1
switchport mode access
switchport access vlan 30
no sh
exit
interface e1/2
switchport mode access
switchport access vlan 40
no sh
exit
```

Et ensuite pour finir nous avons configuré les interfaces trunk pour permettre le passage des différentes vlans :

```
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
end
```

Une fois la configuration fini, on sauvegarde avec la commande :

```
wr
```

- **Configuration de SA2**

Ensuite pour le reste des commutateurs, la configuration est similaire sauf pour l'attribution des vlans aux interfaces :

```
enable
configure terminal
vlan 10
name VLAN_RH
exit
vlan 20
name VLAN_Ventes
exit
vlan 30
name VLAN_Serveurs
exit
vlan 40
name VLAN_Gestion
exit
vlan 50
name VLAN_Wifi
exit
```

Ensuite, nous attribuons le VLAN 20 à une interface du commutateur.

```
interface e1/0
switchport mode access
switchport access vlan 20
no sh
exit
```

Puis, nous configurons les interfaces trunk pour permettre le passage des différents VLANs.

```
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
exit
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
end
```

Une fois la configuration terminée, nous la sauvegardons avec la commande :

```
wr
```

- **Configuration de SA3**

On réalise la même configuration pour SA3 en créant d'abord les VLANs :

```
enable
configure terminal
vlan 10
name VLAN_RH
exit
vlan 20
name VLAN_Ventes
exit
vlan 30
name VLAN_Serveurs
exit
vlan 40
name VLAN_Gestion
exit
vlan 50
name VLAN_Wifi
exit
```

On attribue ensuite le VLAN 10 à une interface du commutateur :

```
interface e1/0
switchport mode access
switchport access vlan 10
no sh
exit
```

Puis, nous configurons les interfaces trunk pour permettre le passage des différents VLANs :

```
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
exit
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50
no sh
end
```

Une fois la configuration terminée, nous la sauvegardons avec la commande :

```
wr
```

Configuration des ACL

Nous avons défini plusieurs listes de contrôle d'accès (ACL) pour restreindre l'accès aux ressources critiques en fonction des services :

- ACL pour le serveur RH : seuls les postes du service RH et l'administrateur réseau peuvent accéder au port 443 du serveur RH.
- ACL pour le serveur FTP : seuls les postes du service Ventes et l'administrateur réseau peuvent accéder au port 21 du serveur FTP.
- ACL de gestion : empêche tous les VLANs (sauf celui de gestion) d'accéder au VLAN de gestion, tout en permettant aux administrateurs réseau de joindre tous les autres VLANs.

```
configure terminal
ip access-list extended ACL_RH_FTP

permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.20 eq 21
permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.20 eq 21
permit udp any host 224.0.0.2 eq 1985
permit icmp any 192.168.30.0 0.0.0.255
deny tcp 192.168.10.0 0.0.0.255 host 192.168.30.20 eq 21
deny tcp 192.168.20.0 0.0.0.255 host 192.168.30.10 eq 443
exit

// On l'applique sur l'interface du vlan 30 en sortie //

interface vlan 30
ip access-group ACL_RH_FTP out
exit
```

L'ACL **ACL_RH_FTP** assure les restrictions suivantes :

- Seuls les **postes RH** et l'**administrateur réseau** peuvent accéder au serveur RH sur **HTTPS**.
- Seuls les **postes Ventes** et l'administrateur peuvent accéder au serveur FTP.
- Bloque tout accès non autorisé aux services critiques.

```
conf t
ip access-list extended ACL_Gestion
deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
permit ip 192.168.40.0 0.0.0.255 any
exit

// On l'applique sur l'interface du vlan 40 en sortie //
```

Nous avons rencontré un problème avec cette ACL que nous n'avons pas encore réussi à résoudre. Elle bloque correctement l'accès des autres VLANs au VLAN de gestion, comme prévu. Cependant, un dysfonctionnement persiste : le VLAN de gestion ne peut atteindre aucun hôte du réseau. Il parvient à communiquer avec les passerelles du site, mais l'accès aux machines des autres VLANs reste impossible.

Réalisation des tests sur le site

Après la mise en place des configurations, nous avons procédé à une série de tests pour vérifier la connectivité et la bonne application des ACL :

Tests de communication interne (avant l'application des ACL)

- Tous les postes peuvent communiquer entre eux au sein du site.

Depuis le PC-RH vers les différents hôtes :

- PC-RH vers le PC-Ventes :

```
debian@debian:~$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=14.6 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=18.6 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=63 time=20.0 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=63 time=12.3 ms
64 bytes from 192.168.20.10: icmp_seq=7 ttl=63 time=19.8 ms
^C
--- 192.168.20.10 ping statistics ---
7 packets transmitted, 5 received, 28.5714% packet loss, time 6039ms
rtt min/avg/max/mdev = 12.303/17.067/19.974/3.074 ms
debian@debian:~$
```

- PC-RH vers l'Admin :

```
debian@debian:~$ ping 192.168.40.10
PING 192.168.40.10 (192.168.40.10) 56(84) bytes of data.
64 bytes from 192.168.40.10: icmp_seq=2 ttl=63 time=127 ms
64 bytes from 192.168.40.10: icmp_seq=3 ttl=63 time=20.0 ms
64 bytes from 192.168.40.10: icmp_seq=4 ttl=63 time=98.0 ms
64 bytes from 192.168.40.10: icmp_seq=5 ttl=63 time=21.0 ms
64 bytes from 192.168.40.10: icmp_seq=6 ttl=63 time=72.8 ms
^C
--- 192.168.40.10 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5039ms
rtt min/avg/max/mdev = 19.977/67.738/126.944/42.227 ms
debian@debian:~$
```

- PC-RH vers le Serveur FTP :

```
debian@debian:~$ ping 192.168.30.20
PING 192.168.30.20 (192.168.30.20) 56(84) bytes of data.
64 bytes from 192.168.30.20: icmp_seq=2 ttl=63 time=26.5 ms
64 bytes from 192.168.30.20: icmp_seq=3 ttl=63 time=18.6 ms
64 bytes from 192.168.30.20: icmp_seq=4 ttl=63 time=30.7 ms
64 bytes from 192.168.30.20: icmp_seq=5 ttl=63 time=20.6 ms
64 bytes from 192.168.30.20: icmp_seq=6 ttl=63 time=23.3 ms
^C
--- 192.168.30.20 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5011ms
rtt min/avg/max/mdev = 18.647/23.962/30.685/4.281 ms
debian@debian:~$
```

- PC-RH vers le Serveur RH :

```
debian@debian:~$ ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=63 time=37.5 ms
64 bytes from 192.168.30.10: icmp_seq=2 ttl=63 time=19.1 ms
64 bytes from 192.168.30.10: icmp_seq=3 ttl=63 time=23.5 ms
64 bytes from 192.168.30.10: icmp_seq=4 ttl=63 time=24.2 ms
64 bytes from 192.168.30.10: icmp_seq=5 ttl=63 time=18.8 ms
64 bytes from 192.168.30.10: icmp_seq=6 ttl=63 time=23.1 ms
^C
--- 192.168.30.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 18.841/24.377/37.535/6.247 ms
debian@debian:~$
```

La communication dans le site fonctionne correctement.

Tests après l'application des ACL

- **Le PC du service RH** peut accéder au serveur RH via HTTPS mais ne peut pas se connecter au serveur FTP.
- **Le PC du service Ventes** peut accéder au serveur FTP mais ne peut pas accéder au serveur RH via HTTPS.
- **Le poste d'administration** peut accéder aux deux serveurs sans restriction.
- **Le VLAN Gestion** est bien isolé, empêchant toute connexion entrante non autorisée.

- PC-RH vers le Serveur RH sur le port 443 :

```
debian@debian:~$ telnet 192.168.30.10 443
Trying 192.168.30.10...
Connected to 192.168.30.10.
Escape character is '^]'.
```

- PC-RH vers le Serveur FTP sur le port 21 :

```
debian@debian:~$ ftp 192.168.30.20
ftp: Can't connect to `192.168.30.20:21': No route to host
ftp: Can't connect to `192.168.30.20:ftp'
ftp>
```

```
debian@debian:~$ ping 192.168.30.20
PING 192.168.30.20 (192.168.30.20) 56(84) bytes of data.
64 bytes from 192.168.30.20: icmp_seq=1 ttl=63 time=148 ms
^C
--- 192.168.30.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 147.792/147.792/147.792/0.000 ms
```

Il ne peut donc pas accéder au FTP, mais il peut bien ping le serveur, ce qui confirme que l'ACL fonctionne correctement pour le PC-RH.

On vérifie maintenant pour le PC-Ventes qui lui doit pouvoir accéder au serveur FTP et ne doit pas pouvoir accéder à HTTPS sur le serveur RH :

- PC-Ventes vers le Serveur RH sur le port 443 :

```
debian@debian:~$ ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=2 ttl=63 time=13.2 ms
^C
--- 192.168.30.10 ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1027ms
rtt min/avg/max/mdev = 13.204/13.204/13.204/0.000 ms
debian@debian:~$ telnet 192.168.30.10 443
Trying 192.168.30.10...
telnet: Unable to connect to remote host: No route to host
debian@debian:~$
```

Il peut ping le serveur mais le port 443 est bien bloqué.

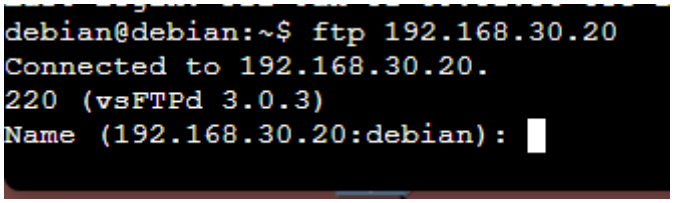
- PC-Ventes vers le Serveur FTP sur le port 21 :

```
debian@debian:~$ ftp 192.168.30.20
Connected to 192.168.30.20.
220 (vsFTPd 3.0.3)
Name (192.168.30.20:debian):
```

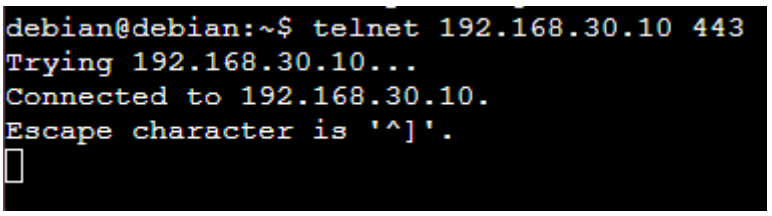
Le PC-Ventes accède bien au serveur FTP donc le test fonctionne pour ce PC également.

Maintenant on vérifie que le PC admin peut lui accéder aux deux serveurs :

- PC-Admin vers le Serveur FTP sur le port 21 :



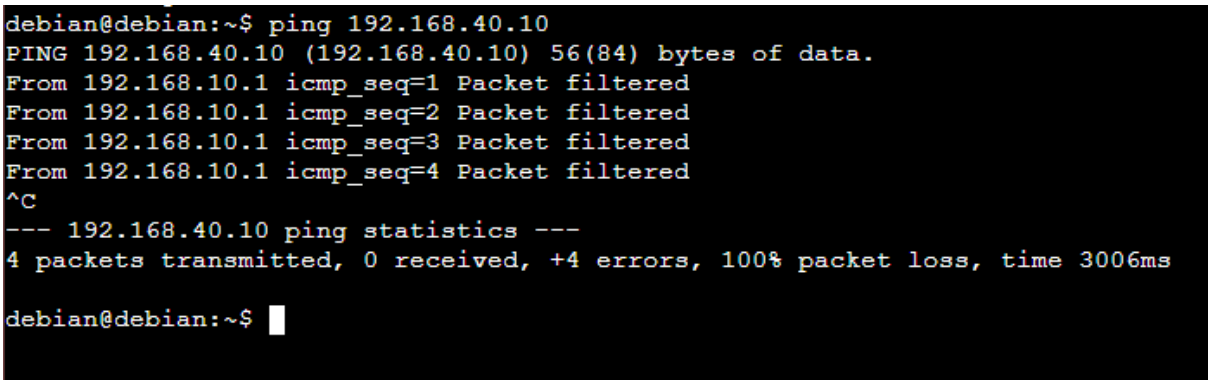
- PC-Admin vers le Serveur RH sur le port 443 :



Les deux tests ont correctement fonctionné. Cette ACL est donc configurée correctement.

Maintenant on va appliquer la deuxième ACL pour le vlan de gestion, nous allons tester d'abord depuis chaque vlan de ping vers la vlan de Gestion puis l'inverse :

- PC-RH vers le PC-Admin :



- PC-Ventes vers le PC-Admin :

```
debian@debian:~$ ping 192.168.40.10
PING 192.168.40.10 (192.168.40.10) 56(84) bytes of data.
From 192.168.20.2 icmp_seq=1 Packet filtered
From 192.168.20.2 icmp_seq=2 Packet filtered
From 192.168.20.2 icmp_seq=3 Packet filtered
From 192.168.20.2 icmp_seq=4 Packet filtered
^C
--- 192.168.40.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3006ms

debian@debian:~$
```

- Serveur FTP vers le PC-Admin :

```
debian@debian:~$ ping 192.168.40.10
PING 192.168.40.10 (192.168.40.10) 56(84) bytes of data.
From 192.168.30.1 icmp_seq=1 Packet filtered
From 192.168.30.1 icmp_seq=2 Packet filtered
From 192.168.30.1 icmp_seq=3 Packet filtered
From 192.168.30.1 icmp_seq=4 Packet filtered
^C
--- 192.168.40.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3006ms

debian@debian:~$
```

- Serveur RH vers le PC-Admin :

```
debian@debian:~$ ping 192.168.40.10
PING 192.168.40.10 (192.168.40.10) 56(84) bytes of data.
From 192.168.30.1 icmp_seq=1 Packet filtered
From 192.168.30.1 icmp_seq=2 Packet filtered
From 192.168.30.1 icmp_seq=3 Packet filtered
From 192.168.30.1 icmp_seq=4 Packet filtered
^C
--- 192.168.40.10 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3007ms

debian@debian:~$
```

Tous les autres vlans ne peuvent pas accéder au vlan de Gestion, cependant nous allons voir que le PC admin de gestion ne peut atteindre aucun hôte du site :

- PC-Admin vers le PC-RH :

```
debian@debian:~$ ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
```

*

Le PC-Admin ne peut pas atteindre et cela est de même pour les autres vlans :

```
debian@debian:~$ ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
^C
--- 192.168.30.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4087ms

debian@debian:~$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
^C
--- 192.168.20.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4097ms

debian@debian:~$ ping 192.168.30.20
PING 192.168.30.20 (192.168.30.20) 56(84) bytes of data.
^C
--- 192.168.30.20 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3055ms

debian@debian:~$
```

Cette ACL fonctionne à moitié ici car elle bloque bien effectivement l'accès au vlan Gestion sur les autres vlans, mais le vlan de Gestion n'arrive plus a atteindre les autres et donc est bloqué.

La mise en place du réseau du site 1 a nécessité la configuration de plusieurs équipements et services essentiels pour assurer **la segmentation du réseau, la haute disponibilité et la sécurité des communications**. L'implémentation des VLANs, du routage inter-VLAN avec HSRP et du protocole PVST+ a permis d'optimiser la fiabilité et la performance du réseau. De plus, l'application des ACL a permis d'améliorer la sécurité en limitant l'accès aux ressources sensibles en fonction des besoins des utilisateurs. Cette architecture constitue une base solide pour l'interconnexion avec les autres sites et l'extension du réseau global.

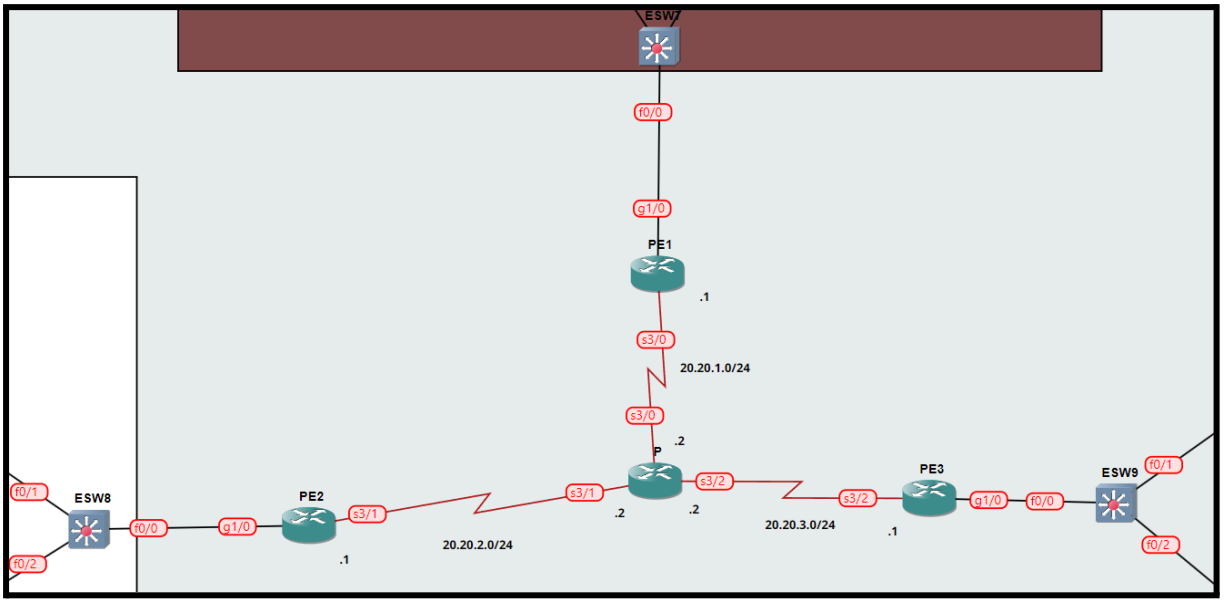
Configuration du Site 2 et 3 en **Annexe**

- **Configuration du Site 2**
- **Configuration du Site 3**

Configuration de l'interconnexion des sites

Après la configuration des 3 sites, l'objectif de cette deuxième tâche est de mettre en place et valider l'interconnexion des trois sites à l'aide d'un VPN MPLS.

Topologie pour l'interconnexion des sites :



Liste des équipements utilisés :

- 4 routeurs (Cisco 7200)
- 3 Commutateurs de distribution L3 (Etherswitch)

Plan d'adressage :

	Interface	Adresse + masque
PE1	S3/0 Lo0	20.20.1.1 /24 1.1.1.1 /32
PE2	S3/1 Lo0	20.20.2.1 /24 2.2.2.2 /32
PE3	S3/2 Lo0	20.20.3.1 /24 3.3.3.3 /32
P	S3/0 S3/1 S3/2	20.20.1.2 /24 20.20.2.2 /24 20.20.3.2 /24

Configuration des Commutateurs de distribution L3

Tout d'abord, nous allons configurer les commutateurs de distribution L3 liés aux SD de chaque site pour permettre de faire passer les vlans en un seul lien trunk vers le PE.
Pour cela on va configurer les vlans et les liens trunks sur les 3 commutateurs.

- Configuration de ESW7

Nous avons d'abord configurer les vlans :

```
vlan database
vlan 10 name RH_SITE1
vlan 20 name Ventes_SITE1
vlan 30 name Serveurs_SITE1
vlan 40 name Gestion_SITE1
vlan 50 name Wifi_SITE1
exit
```

Puis nous avons configurés les liens trunks vers les SD et vers le routeur PE pour permettre le passage des vlans :

```
enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/1
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/2
no sh
switchport mode trunk
```

```
switchport trunk allowed vlan 1-1005
exit
```

Une fois la configuration terminée on la sauvegarde avec la commande :

```
wr
```

- **Configuration de ESW8**

Pour ESW8 c'est la même config que ESW7 sauf que ce sont les vlans du site 2 donc on configure les vlans du site 11 :

```
vlan database
vlan 11 name RH_SITE2
vlan 21 name Ventes_SITE2
vlan 31 name Serveurs_SITE2
vlan 41 name Gestion_SITE2
vlan 51 name Wifi_SITE2
exit
```

Puis nous avons configurés les liens trunks vers les SDs du site 2 et vers le routeur PE2 pour permettre le passage des vlans :

```
enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/1
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit
```

```
interface f0/2
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit
```

Une fois la configuration terminée on la sauvegarde avec la commande :

```
wr
```

- **Configuration de ESW9**

On fait la même config sauf que ce sont les vlans du site 3 cette fois ci :

```
vlan database
vlan 12 name RH_SITE3
vlan 22 name Ventes_SITE3
vlan 32 name Serveurs_SITE3
vlan 42 name Gestion_SITE3
vlan 52 name Wifi_SITE3
exit
```

Puis nous avons configurés les liens trunks vers les SDs du site 3 et vers le routeur PE3 pour permettre le passage des vlans :

```
enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/1
no sh
switchport mode trunk
```

```
switchport trunk allowed vlan 1-1005
exit

interface f0/2
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit
```

Une fois la configuration terminée on la sauvegarde avec la commande :

```
wr
```

Configuration des routeurs (Cisco 7200)

Nous allons configurer d'abord les 3 routeurs PE puis le routeur P pour les connecter entre eux et ensuite activer mpls

- ## Configuration de PE1

Sur PE1 on va configurer l'interface S3/0 et activer mpls sur celle-ci et configurer l'interface Lo0 :

```
enable
conf t
interface s3/0
no sh
mpls ip
ip address 20.20.1.1 255.255.255.0
interface lo0
ip address 1.1.1.1 255.255.255.255
no sh
end
```

Ensuite nous avons configurés OSPF pour annoncer les réseaux aux autres routeurs :

```
conf t
router ospf 1
network 20.20.1.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
end
```

Puis on va configurer sur ce routeur une vrf qu'on va nommer Site1 qui exportera les routes du site 1 vers les autres sites et importera les routes des autres sites :

```
conf t
ip vrf Site1
rd 100:1
route-target export 100:1
route-target import 100:2
route-target import 100:3
end
```

Nous allons maintenant configurer les sous interfaces liés au ESW et les attribués à la vrf Site1 qui transporte les différentes vlans en activant également mpls ip :

```
enable
conf t
interface gi1/0
no sh
mpls ip
interface gi1/0.10
encapsulation dot1q 10
ip vrf forwarding Site1
ip address 192.168.10.253 255.255.255.0
no sh
mpls ip
interface gi1/0.20
encapsulation dot1q 20
ip vrf forwarding Site1
ip address 192.168.20.253 255.255.255.0
no sh
mpls ip
interface gi1/0.30
encapsulation dot1q 30
ip vrf forwarding Site1
ip address 192.168.30.253 255.255.255.0
no sh
mpls ip
interface gi1/0.40
```

```
encapsulation dot1q 40
ip vrf forwarding Site1
ip address 192.168.40.253 255.255.255.0
no sh
mpls ip
interface gi1/0.50
encapsulation dot1q 50
ip vrf forwarding Site1
ip address 192.168.50.253 255.255.255.0
no sh
mpls ip
end
```

Ensuite nous avons configuré les voisins BGP :

```
conf t
router bgp 100
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 100
neighbor 3.3.3.3 remote-as 100
neighbor 2.2.2.2 update-source Loopback0
neighbor 3.3.3.3 update-source Loopback0
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 3.3.3.3 activate
neighbor 2.2.2.2 send-community extended
neighbor 3.3.3.3 send-community extended
exit-address-family
end
```

Puis nous avons redistribué les routes OSPF dans BGP :

```
conf t
router bgp 100
address-family ipv4 vrf Site1
redistribute ospf 4
end
```

Et :

```
conf t
router ospf 4 vrf Site1
 redistribute bgp 100 subnets
 redistribute connected subnets
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
end
```

Une fois la configuration terminée je sauvegarde avec la commande :

```
wr
```

- **Configuration de PE2**

Le principe de configuration est la même pour PE2 et PE3 sauf que la configuration des adresses et les vrf ne sont pas les mêmes :

```
enable
conf t
interface s3/1
no sh
mpls ip
ip address 20.20.1.2 255.255.255.0


interface lo0
ip address 2.2.2.2 255.255.255.255
no sh
end


conf t
router ospf 1
network 20.20.2.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
end


conf t
ip vrf Site2
rd 100:2
route-target export 100:2
route-target import 100:1
route-target import 100:3
end



enable
conf t
interface gi1/0
```

```
no sh
mpls ip

interface gi1/0.11
encapsulation dot1q 11
ip vrf forwarding Site2
ip address 192.168.11.253 255.255.255.0
no sh
mpls ip


interface gi1/0.21
encapsulation dot1q 21
ip vrf forwarding Site2
ip address 192.168.21.253 255.255.255.0
no sh
mpls ip


interface gi1/0.31
encapsulation dot1q 31
ip vrf forwarding Site2
ip address 192.168.31.253 255.255.255.0
no sh
mpls ip

interface gi1/0.41
encapsulation dot1q 41
ip vrf forwarding Site2
ip address 192.168.41.253 255.255.255.0
no sh
mpls ip




interface gi1/0.51
encapsulation dot1q 51
```

```
ip vrf forwarding Site2
ip address 192.168.51.253 255.255.255.0
no sh
mpls ip
end
wr

conf t
router bgp 100
bgp log-neighbor-changes
neighbor 1.1.1.1 remote-as 100
neighbor 3.3.3.3 remote-as 100
neighbor 1.1.1.1 update-source Loopback0
neighbor 3.3.3.3 update-source Loopback0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 3.3.3.3 activate
neighbor 1.1.1.1 send-community extended
neighbor 3.3.3.3 send-community extended
exit-address-family
end

conf t
router bgp 100
address-family ipv4 vrf Site2
redistribute ospf 5
end

conf t
router ospf 5 vrf Site2
 redistribute bgp 100 subnets
 redistribute connected subnets
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.31.0 0.0.0.255 area 0
 network 192.168.41.0 0.0.0.255 area 0
 network 192.168.51.0 0.0.0.255 area 0
end

wr
```

- **Configuration de PE3**

Nous avons configuré PE3 :

```
enable
conf t
interface s3/2
no sh
mpls ip
ip address 20.20.2.2 255.255.255.0

interface lo0
ip address 3.3.3.3 255.255.255.255
no sh
end


conf t
router ospf 1
network 20.20.3.0 0.0.0.255 area 0
network 3.3.3.3 0.0.0.0 area 0
end


conf t
ip vrf Site3
rd 100:3
route-target export 100:3
route-target import 100:1
route-target import 100:2
end

enable
conf t
interface gi1/0
no sh
mpls ip
interface gi1/0.12
encapsulation dot1q 12
ip vrf forwarding Site3
```

```
ip address 192.168.12.253 255.255.255.0
no sh
mpls ip
interface gi1/0.22
encapsulation dot1q 22
ip vrf forwarding Site3
ip address 192.168.22.253 255.255.255.0
no sh
mpls ip
interface gi1/0.32
encapsulation dot1q 32
ip vrf forwarding Site3
ip address 192.168.32.253 255.255.255.0
no sh
mpls ip
interface gi1/0.42
encapsulation dot1q 42
ip vrf forwarding Site3
ip address 192.168.42.253 255.255.255.0
no sh
mpls ip
interface gi1/0.52
encapsulation dot1q 52
ip vrf forwarding Site3
ip address 192.168.52.253 255.255.255.0
no sh
mpls ip
end
wr

conf t
router bgp 100
bgp log-neighbor-changes
neighbor 1.1.1.1 remote-as 100
neighbor 2.2.2.2 remote-as 100
neighbor 1.1.1.1 update-source Loopback0
neighbor 2.2.2.2 update-source Loopback0
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 2.2.2.2 activate
```

```
neighbor 1.1.1.1 send-community extended
neighbor 2.2.2.2 send-community extended
exit-address-family
end

conf t
router bgp 100
address-family ipv4 vrf Site3
redistribute ospf 6
end

conf t
router ospf 6 vrf Site3
 redistribute bgp 100 subnets
 redistribute connected subnets
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.22.0 0.0.0.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.42.0 0.0.0.255 area 0
 network 192.168.52.0 0.0.0.255 area 0
end

wr
```

- **Configuration de P (routeur coeur du réseau opérateur)**

Et pour finir nous avons configuré le routeur P, qui est le routeur coeur du réseau MPLS qui va permettre la distribution des routes au sein du réseau :

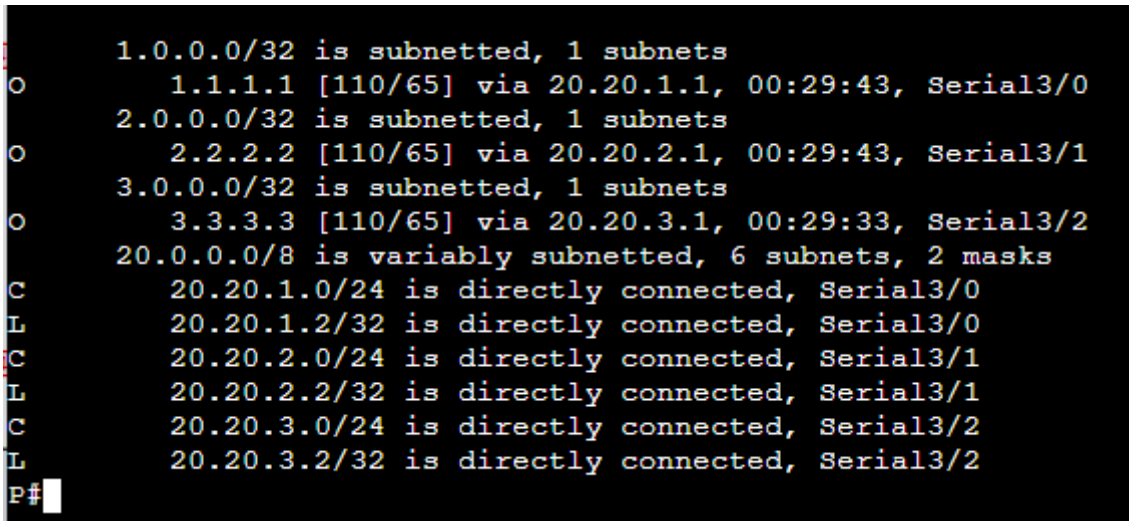
Nous avons configuré les interfaces de P :

```
enable
conf t
interface s3/0
ip address 20.20.1.2 255.255.255.0
no sh
mpls ip
interface s3/1
ip address 20.20.2.2 255.255.255.0
no sh
mpls ip
interface s3/2
ip address 20.20.3.2 255.255.255.0
no sh
mpls ip
end
```

Ensuite nous avons configuré OSPF et vérifier que les routes de chaque routeur apparaissent bien :

```
conf t
router ospf 1
network 20.20.1.0 0.0.0.255 area 0
network 20.20.2.0 0.0.0.255 area 0
network 20.20.3.0 0.0.0.255 area 0
end
```

Nous avons vérifié les routes OSPF :



OSPF a donc bien été configuré.

Ensuite nous avons activé BGP sur le routeur P pour qu'il puisse permettre de distribuer les routes aux autres routeurs PE via BGP :

```
conf t
router bgp 100
bgp log-neighbor-changes
neighbor 1.1.1.1 remote-as 100
neighbor 2.2.2.2 remote-as 100
neighbor 3.3.3.3 remote-as 100
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 2.2.2.2 activate
neighbor 3.3.3.3 activate
neighbor 1.1.1.1 send-community extended
neighbor 2.2.2.2 send-community extended
neighbor 3.3.3.3 send-community extended
end
```

Et une fois la config terminée on sauvegarde avec la commande :

```
wr
```

Réalisations des tests :

Après avoir configuré les routeurs, je vérifie sur la vrf du Site1 que les routes ont étés distribués donc sur le routeur PE1 je tape la commande :

```
show ip route vrf Site1
```

```
Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0.10
L        192.168.10.253/32 is directly connected, GigabitEthernet1/0.10
B     192.168.11.0/24 [200/0] via 2.2.2.2, 00:40:30
B     192.168.12.0/24 [200/0] via 3.3.3.3, 00:40:30
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet1/0.20
L        192.168.20.253/32 is directly connected, GigabitEthernet1/0.20
B     192.168.21.0/24 [200/0] via 2.2.2.2, 00:40:30
B     192.168.22.0/24 [200/0] via 3.3.3.3, 00:40:30
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, GigabitEthernet1/0.30
L        192.168.30.253/32 is directly connected, GigabitEthernet1/0.30
B     192.168.31.0/24 [200/0] via 2.2.2.2, 00:40:30
B     192.168.32.0/24 [200/0] via 3.3.3.3, 00:40:30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, GigabitEthernet1/0.40
L        192.168.40.253/32 is directly connected, GigabitEthernet1/0.40
B     192.168.41.0/24 [200/0] via 2.2.2.2, 00:40:30
B     192.168.42.0/24 [200/0] via 3.3.3.3, 00:40:30
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, GigabitEthernet1/0.50
L        192.168.50.253/32 is directly connected, GigabitEthernet1/0.50
B     192.168.51.0/24 [200/0] via 2.2.2.2, 00:40:30
B     192.168.52.0/24 [200/0] via 3.3.3.3, 00:40:30
PE1#
```

Nous constatons que les routes de chaque site ont bien étés distribués, et on vérifie maintenant sur les routeurs SD que les routes des autres sites apparaissent bien avec la commande :

```
show ip route
```

```
Gateway of last resort is not set

O E2 192.168.12.0/24 [110/1] via 192.168.50.253, 00:00:38, Vlan50
                     [110/1] via 192.168.40.253, 00:00:38, Vlan40
                     [110/1] via 192.168.20.253, 00:00:38, Vlan20
                     [110/1] via 192.168.10.253, 00:00:38, Vlan10
O E2 192.168.31.0/24 [110/1] via 192.168.50.253, 00:00:38, Vlan50
                     [110/1] via 192.168.40.253, 00:00:38, Vlan40
                     [110/1] via 192.168.20.253, 00:00:38, Vlan20
                     [110/1] via 192.168.10.253, 00:00:38, Vlan10
C    192.168.30.0/24 is directly connected, Vlan30
O E2 192.168.42.0/24 [110/1] via 192.168.50.253, 00:00:39, Vlan50
                     [110/1] via 192.168.40.253, 00:00:39, Vlan40
                     [110/1] via 192.168.20.253, 00:00:39, Vlan20
                     [110/1] via 192.168.10.253, 00:00:39, Vlan10
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
O E2 192.168.11.0/24 [110/1] via 192.168.50.253, 00:00:40, Vlan50
                     [110/1] via 192.168.40.253, 00:00:40, Vlan40
                     [110/1] via 192.168.20.253, 00:00:40, Vlan20
                     [110/1] via 192.168.10.253, 00:00:40, Vlan10
O E2 192.168.41.0/24 [110/1] via 192.168.50.253, 00:00:40, Vlan50
                     [110/1] via 192.168.40.253, 00:00:40, Vlan40
                     [110/1] via 192.168.20.253, 00:00:40, Vlan20
                     [110/1] via 192.168.10.253, 00:00:40, Vlan10
O E2 192.168.21.0/24 [110/1] via 192.168.50.253, 00:00:40, Vlan50
                     [110/1] via 192.168.40.253, 00:00:40, Vlan40
                     [110/1] via 192.168.20.253, 00:00:40, Vlan20
                     [110/1] via 192.168.10.253, 00:00:40, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
O E2 192.168.22.0/24 [110/1] via 192.168.50.253, 00:00:41, Vlan50
                     [110/1] via 192.168.40.253, 00:00:41, Vlan40
                     [110/1] via 192.168.20.253, 00:00:41, Vlan20
                     [110/1] via 192.168.10.253, 00:00:41, Vlan10
O E2 192.168.52.0/24 [110/1] via 192.168.50.253, 00:00:41, Vlan50
                     [110/1] via 192.168.40.253, 00:00:41, Vlan40
                     [110/1] via 192.168.20.253, 00:00:41, Vlan20
                     [110/1] via 192.168.10.253, 00:00:41, Vlan10
O E2 192.168.51.0/24 [110/1] via 192.168.50.253, 00:00:44, Vlan50
                     [110/1] via 192.168.40.253, 00:00:44, Vlan40
                     [110/1] via 192.168.20.253, 00:00:44, Vlan20
                     [110/1] via 192.168.10.253, 00:00:44, Vlan10
C    192.168.50.0/24 is directly connected, Vlan50
O E2 192.168.32.0/24 [110/1] via 192.168.50.253, 00:00:44, Vlan50
                     [110/1] via 192.168.40.253, 00:00:44, Vlan40
                     [110/1] via 192.168.20.253, 00:00:44, Vlan20
                     [110/1] via 192.168.10.253, 00:00:44, Vlan10
SD1#
```

et sur SD2 :

```
O E2 192.168.12.0/24 [110/1] via 192.168.50.253, 00:02:23, Vlan50
                     [110/1] via 192.168.40.253, 00:02:23, Vlan40
                     [110/1] via 192.168.20.253, 00:02:23, Vlan20
                     [110/1] via 192.168.10.253, 00:02:23, Vlan10
O E2 192.168.31.0/24 [110/1] via 192.168.50.253, 00:02:23, Vlan50
                     [110/1] via 192.168.40.253, 00:02:23, Vlan40
                     [110/1] via 192.168.20.253, 00:02:23, Vlan20

*Mar  1 00:03:47.819: %SYS-5-CONFIG_I: Configured from console by cons
     [110/1] via 192.168.10.253, 00:02:23, Vlan10
C    192.168.30.0/24 is directly connected, Vlan30
O E2 192.168.42.0/24 [110/1] via 192.168.50.253, 00:02:24, Vlan50
                     [110/1] via 192.168.40.253, 00:02:24, Vlan40
                     [110/1] via 192.168.20.253, 00:02:24, Vlan20
                     [110/1] via 192.168.10.253, 00:02:24, Vlan10
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.40.0/24 is directly connected, Vlan40
O E2 192.168.11.0/24 [110/1] via 192.168.50.253, 00:02:27, Vlan50
                     [110/1] via 192.168.40.253, 00:02:27, Vlan40
                     [110/1] via 192.168.20.253, 00:02:27, Vlan20
                     [110/1] via 192.168.10.253, 00:02:27, Vlan10
O E2 192.168.41.0/24 [110/1] via 192.168.50.253, 00:02:27, Vlan50
                     [110/1] via 192.168.40.253, 00:02:27, Vlan40
                     [110/1] via 192.168.20.253, 00:02:27, Vlan20
                     [110/1] via 192.168.10.253, 00:02:27, Vlan10
O E2 192.168.21.0/24 [110/1] via 192.168.50.253, 00:02:27, Vlan50
                     [110/1] via 192.168.40.253, 00:02:27, Vlan40
                     [110/1] via 192.168.20.253, 00:02:27, Vlan20
                     [110/1] via 192.168.10.253, 00:02:27, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
O E2 192.168.22.0/24 [110/1] via 192.168.50.253, 00:02:29, Vlan50
                     [110/1] via 192.168.40.253, 00:02:29, Vlan40
                     [110/1] via 192.168.20.253, 00:02:29, Vlan20
                     [110/1] via 192.168.10.253, 00:02:29, Vlan10
O E2 192.168.52.0/24 [110/1] via 192.168.50.253, 00:02:29, Vlan50
                     [110/1] via 192.168.40.253, 00:02:29, Vlan40
                     [110/1] via 192.168.20.253, 00:02:29, Vlan20
                     [110/1] via 192.168.10.253, 00:02:29, Vlan10
O E2 192.168.51.0/24 [110/1] via 192.168.50.253, 00:02:29, Vlan50
                     [110/1] via 192.168.40.253, 00:02:29, Vlan40
                     [110/1] via 192.168.20.253, 00:02:29, Vlan20
                     [110/1] via 192.168.10.253, 00:02:29, Vlan10
C    192.168.50.0/24 is directly connected, Vlan50
O E2 192.168.32.0/24 [110/1] via 192.168.50.253, 00:02:29, Vlan50
                     [110/1] via 192.168.40.253, 00:02:29, Vlan40
                     [110/1] via 192.168.20.253, 00:02:30, Vlan20
                     [110/1] via 192.168.10.253, 00:02:30, Vlan10
SD2#
```

Donc les routes sont bien distribuées sur les Deux commutateurs SD de chaque site et si un commutateur tombe l'autre commutateur prendra le relais jusqu'à qu'il soit à nouveau allumé.

Nous allons maintenant tester la connectivité vers un autre site avec le PC-RH du site 1 on va ping le PC-RH du site 2 et 3 :

- PC-RH du site 1 vers le PC-RH du site 2 :

```
pdebian@debian:~$ ping 192.168.11.10
PING 192.168.11.10 (192.168.11.10) 56(84) bytes of data.
From 192.168.10.254: icmp_seq=1 Redirect Network(New nexthop: 192.168.10.253)
64 bytes from 192.168.11.10: icmp_seq=1 ttl=60 time=216 ms
64 bytes from 192.168.11.10: icmp_seq=2 ttl=60 time=91.9 ms
From 192.168.10.254: icmp_seq=3 Redirect Network(New nexthop: 192.168.10.253)
64 bytes from 192.168.11.10: icmp_seq=3 ttl=60 time=94.6 ms
64 bytes from 192.168.11.10: icmp_seq=4 ttl=60 time=60.7 ms
64 bytes from 192.168.11.10: icmp_seq=5 ttl=60 time=52.5 ms
64 bytes from 192.168.11.10: icmp_seq=6 ttl=60 time=46.1 ms
^C
--- 192.168.11.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 46.093/93.658/216.117/57.795 ms
debian@debian:~$
```

- PC-RH du site 1 vers le PC-RH du site 3 :

```
debian@debian:~$ ping 192.168.12.10
PING 192.168.12.10 (192.168.12.10) 56(84) bytes of data.
64 bytes from 192.168.12.10: icmp_seq=1 ttl=60 time=152 ms
64 bytes from 192.168.12.10: icmp_seq=2 ttl=60 time=68.2 ms
64 bytes from 192.168.12.10: icmp_seq=3 ttl=60 time=59.4 ms
64 bytes from 192.168.12.10: icmp_seq=4 ttl=60 time=58.8 ms
64 bytes from 192.168.12.10: icmp_seq=5 ttl=60 time=53.7 ms
64 bytes from 192.168.12.10: icmp_seq=6 ttl=60 time=99.2 ms
^C
--- 192.168.12.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 53.748/81.967/152.413/34.851 ms
debian@debian:~$
```

Maintenant il faut réajuster les ACL car les ACL sont configurés sur les sites en local mais par exemple avec le PC-RH je ne suis pas censé pouvoir accéder au serveur ftp, mais vu que les ACL ont étés configurés que pour les sites dans leur réseau local il faut ajuster des ACL sur les routeurs PE.

Pour le test des ACLs, nous avons installé sur les machines debian telnet et FTP pour pouvoir tester le bon fonctionnement, et sur les serveurs nous avons installé apache2 avec openssl pour le port 443 et vsftpd sur le serveur ftp pour tester le port 21.

- PC-RH du site 1 vers le Serveur ftp du site 2 :

```
debian@debian:~$ ftp 192.168.31.20
Connected to 192.168.31.20.
220 (vsFTPd 3.0.3)
Name (192.168.31.20:debian):
```

Réajustement des ACL sur les routeurs PE :

On va donc réajuster les ACL en fonction des sous réseaux des différents Sites :

Pour l'ACL :

```
configure terminal
ip access-list extended ACL_RH_FTP

permit tcp 192.168.11.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.12.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.41.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.42.0 0.0.0.255 host 192.168.30.10 eq 443
permit tcp 192.168.21.0 0.0.0.255 host 192.168.30.20 eq 21
permit tcp 192.168.22.0 0.0.0.255 host 192.168.30.20 eq 21
permit tcp 192.168.41.0 0.0.0.255 host 192.168.30.20 eq 21
permit tcp 192.168.42.0 0.0.0.255 host 192.168.30.20 eq 21

permit udp any host 224.0.0.2 eq 1985

permit icmp any 192.168.30.0 0.0.0.255

deny tcp 192.168.11.0 0.0.0.255 host 192.168.30.20 eq 21
deny tcp 192.168.12.0 0.0.0.255 host 192.168.30.20 eq 21
```

```
deny tcp 192.168.21.0 0.0.0.255 host 192.168.30.10 eq 443
deny tcp 192.168.22.0 0.0.0.255 host 192.168.30.10 eq 443
exit

// On l'applique sur l'interface gi1/0.30 du routeur PE1 en sortie //

interface gi1/0.30
ip access-group ACL_RH_FTP out
exit
```

On vérifie maintenant les tests :

Par exemple le PC-RH du site 2 vers le serveur FTP du site 1 :

- PC-RH du site 2 vers le Serveur ftp du site 1 :

```
debian@debian:~$ ftp 192.168.30.20
ftp: Can't connect to `192.168.30.20:21': No route to host
ftp: Can't connect to `192.168.30.20:ftp'
ftp>
```

- PC-RH du site 3 vers le Serveur ftp du site 1 :

```
ft      debian@debian:~$ ftp 192.168.30.20
ftp: Can't connect to `192.168.30.20:21': No route to host
ftp: Can't connect to `192.168.30.20:ftp'
ftp>
```

Le PC-RH du site 2 et 3 ne peuvent pas accéder au Serveur FTP du site 1 donc l'ACL fonctionne correctement et maintenant on va tester depuis le PC-Ventes vers le serveur RH du site un sur le port 443 :

- PC-Ventes du site 2 vers le Serveur RH du site 1 :

```
debian@debian:~$ telnet 192.168.30.10 443
Trying 192.168.30.10...
telnet: Unable to connect to remote host: No route to host
debian@debian:~$
```

- PC-Ventes du site 3 vers le Serveur RH du site 1 :

```
debian@debian:~$ telnet 192.168.30.10 443
Trying 192.168.30.10...
telnet: Unable to connect to remote host: No route to host
debian@debian:~$
```

L'ACL_RH_FTP fonctionne maintenant aussi pour bloquer l'accès depuis le Site 2 et 3, il faut donc maintenant ajuster l'ACL pour PE2 et PE3 :

Pour PE2 :

```
configure terminal
ip access-list extended ACL_RH_FTP

permit tcp 192.168.10.0 0.0.0.255 host 192.168.31.10 eq 443
permit tcp 192.168.12.0 0.0.0.255 host 192.168.31.10 eq 443
permit tcp 192.168.40.0 0.0.0.255 host 192.168.31.10 eq 443
permit tcp 192.168.42.0 0.0.0.255 host 192.168.31.10 eq 443
permit tcp 192.168.20.0 0.0.0.255 host 192.168.31.20 eq 21
permit tcp 192.168.22.0 0.0.0.255 host 192.168.31.20 eq 21
permit tcp 192.168.40.0 0.0.0.255 host 192.168.31.20 eq 21
permit tcp 192.168.42.0 0.0.0.255 host 192.168.31.20 eq 21

permit udp any host 224.0.0.2 eq 1985

permit icmp any 192.168.31.0 0.0.0.255

deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.20 eq 21
deny tcp 192.168.12.0 0.0.0.255 host 192.168.31.20 eq 21
deny tcp 192.168.20.0 0.0.0.255 host 192.168.31.10 eq 443
deny tcp 192.168.22.0 0.0.0.255 host 192.168.31.10 eq 443
exit


// On l'applique sur l'interface gi1/0.30 du routeur PE1 en sortie //

interface gi1/0.31
ip access-group ACL_RH_FTP out
exit
```

Pour PE3 :

```
configure terminal
ip access-list extended ACL_RH_FTP

permit tcp 192.168.10.0 0.0.0.255 host 192.168.32.10 eq 443
permit tcp 192.168.11.0 0.0.0.255 host 192.168.32.10 eq 443
permit tcp 192.168.40.0 0.0.0.255 host 192.168.32.10 eq 443
permit tcp 192.168.41.0 0.0.0.255 host 192.168.32.10 eq 443
permit tcp 192.168.20.0 0.0.0.255 host 192.168.32.20 eq 21
permit tcp 192.168.21.0 0.0.0.255 host 192.168.32.20 eq 21
permit tcp 192.168.40.0 0.0.0.255 host 192.168.32.20 eq 21
permit tcp 192.168.41.0 0.0.0.255 host 192.168.32.20 eq 21

permit udp any host 224.0.0.2 eq 1985

permit icmp any 192.168.32.0 0.0.0.255

deny tcp 192.168.10.0 0.0.0.255 host 192.168.32.20 eq 21
deny tcp 192.168.11.0 0.0.0.255 host 192.168.32.20 eq 21
deny tcp 192.168.20.0 0.0.0.255 host 192.168.32.10 eq 443
deny tcp 192.168.21.0 0.0.0.255 host 192.168.32.10 eq 443
exit


// On l'applique sur l'interface gi1/0.30 du routeur PE1 en sortie //

interface gi1/0.32
ip access-group ACL_RH_FTP out
exit
```

Nous n’avons pas ajusté l'ACL Gestion du fait que celle ci ai déjà des problèmes.

Conclusion

Ce projet nous a permis d'implémenter une **infrastructure réseau multi-site** en intégrant des technologies avancées comme **MP-BGP, MPLS** et **PVST+**.

Nous avons rencontré certaines difficultés, notamment dans la redistribution dynamique des routes et la mise en place de l'ACL **de gestion**, malgré le fait que celle-ci ne fonctionne pas, nous avons obtenu un **réseau fonctionnel et sécurisé**.

Grâce à ce projet, nous avons renforcé nos compétences en **routage, switching, gestion de la sécurité et politiques d'accès**, et développé une approche méthodique dans la **résolution des problèmes réseau**.

Tableau des acronymes

Acronyme	Signification
VLAN	Virtual Local Area Network
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multi-Protocol Label Switching
ACL	Access Control List
SD	Switch de Distribution (Layer 3)
PE	Provider Edge (Routeur en périphérie MPLS)
VRF	Virtual Routing and Forwarding
OSPF	Open Shortest Path First (Protocole de routage)
LDP	Label Distribution Protocol
HSRP	Hot Standby Router Protocol
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
STP	Spanning Tree Protocol

Annexe

Configuration du Site 2 :

Configuration de SD3 :

```
vlan database
vlan 11 name RH_SITE2
vlan 21 name Ventes_SITE2
vlan 31 name Serveurs_SITE2
vlan 41 name Gestion_SITE2
vlan 51 name Wifi_SITE2
exit

enable
conf t
interface vlan 11
 ip address 192.168.11.1 255.255.255.0
 standby 11 ip 192.168.11.254
 standby 11 priority 110
 standby 11 preempt
no sh
interface vlan 21
 ip address 192.168.21.1 255.255.255.0
 standby 21 ip 192.168.21.254
no sh
interface vlan 31
 ip address 192.168.31.1 255.255.255.0
 standby 31 ip 192.168.31.254
 standby 31 priority 110
 standby 31 preempt
no sh
interface vlan 41
 ip address 192.168.41.1 255.255.255.0
 standby 41 ip 192.168.41.254
no sh
interface vlan 51
 ip address 192.168.51.1 255.255.255.0
 standby 51 ip 192.168.51.254
```

```
 standby 51 priority 110
 standby 51 preempt
no sh
end


enable
conf t
interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/15
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
end


conf t
spanning-tree vlan 11 priority 24576
end


conf t
router ospf 5
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.31.0 0.0.0.255 area 0
 network 192.168.41.0 0.0.0.255 area 0
 network 192.168.51.0 0.0.0.255 area 0
end
```

```
wr
```

Configuration de SD4 :

```
vlan database
vlan 11 name RH_SITE2
vlan 21 name Ventes_SITE2
vlan 31 name Serveurs_SITE2
vlan 41 name Gestion_SITE2
vlan 51 name Wifi_SITE2
exit

enable
conf t
interface vlan 11
 ip address 192.168.11.2 255.255.255.0
 standby 11 ip 192.168.11.254
no sh
exit
interface vlan 21
 ip address 192.168.21.2 255.255.255.0
 standby 21 ip 192.168.21.254
 standby 21 priority 110
 standby 21 preempt
no sh
exit
interface vlan 31
 ip address 192.168.31.2 255.255.255.0
 standby 31 ip 192.168.31.254
no sh
exit
interface vlan 41
 ip address 192.168.41.2 255.255.255.0
 standby 41 ip 192.168.41.254
 standby 41 priority 110
 standby 41 preempt
no sh
```

```
exit
interface vlan 51
 ip address 192.168.51.2 255.255.255.0
 standby 51 ip 192.168.51.254
no sh
end

enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/2
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
exit

interface f0/15
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

conf t
spanning-tree vlan 21 priority 24576
```

```
end

conf t
ip routing
router ospf 5
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
 network 192.168.31.0 0.0.0.255 area 0
 network 192.168.41.0 0.0.0.255 area 0
 network 192.168.51.0 0.0.0.255 area 0
end

wr
```

Configuration de SA4 :

```
enable
configure terminal
vlan 11
name VLAN_RH
no sh
exit
vlan 21
name VLAN_Ventes
no sh
exit
vlan 31
name VLAN_Serveurs
no sh
exit
vlan 41
name VLAN_Gestion
no sh
exit
vlan 51
name VLAN_Wifi
no sh
exit
interface e1/0
switchport mode access
switchport access vlan 31
exit
interface e1/1
switchport mode access
switchport access vlan 31
no sh
exit
interface e1/2
switchport mode access
switchport access vlan 41
no sh
exit

interface e0/0
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 11,21,31,41,51
no sh
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 11,21,31,41,51
no sh
wr
```

Configuration de SA5 :

```
enable
configure terminal
vlan 11
name VLAN_RH
exit
vlan 21
name VLAN_Ventes
exit
vlan 31
name VLAN_Serveurs
exit
vlan 41
name VLAN_Gestion
exit
vlan 51
name VLAN_Wifi
exit
interface e1/0
switchport mode access
switchport access vlan 21
exit
configure terminal
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
switchport trunk allowed vlan 11,21,31,41,51
exit
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 11,21,31,41,51
end
wr
```

Configuration de SA6 :

```
enable
configure terminal
vlan 11
name VLAN_RH
exit
vlan 21
name VLAN_Ventes
exit
vlan 31
name VLAN_Serveurs
exit
vlan 41
name VLAN_Gestion
exit
vlan 51
name VLAN_Wifi
exit
interface e1/0
switchport mode access
switchport access vlan 11
exit
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 11,21,31,41,51
exit
interface e0/1
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 11,21,31,41,51
end
wr
```

Configuration du Site 3 :

Configuration de SD5 :

```
vlan database
vlan 12 name RH_SITE3
vlan 22 name Ventes_SITE3
vlan 32 name Serveurs_SITE3
vlan 42 name Gestion_SITE3
vlan 52 name Wifi_SITE3
exit

enable
conf t
interface vlan 12
 ip address 192.168.12.1 255.255.255.0
 standby 12 ip 192.168.12.254
 standby 12 priority 110
 standby 12 preempt
no sh
interface vlan 22
 ip address 192.168.22.1 255.255.255.0
 standby 22 ip 192.168.22.254
no sh
interface vlan 32
 ip address 192.168.32.1 255.255.255.0
 standby 32 ip 192.168.32.254
 standby 32 priority 110
 standby 32 preempt
no sh
interface vlan 42
 ip address 192.168.42.1 255.255.255.0
 standby 42 ip 192.168.42.254
no sh
interface vlan 52
 ip address 192.168.52.1 255.255.255.0
 standby 52 ip 192.168.52.254
 standby 52 priority 110
 standby 52 preempt
no sh
```

```
end

enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
interface f0/1
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/15
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

conf t
spanning-tree vlan 12 priority 24576
end


conf t
ip routing
router ospf 6
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.22.0 0.0.0.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.42.0 0.0.0.255 area 0
```

```
 network 192.168.52.0 0.0.0.255 area 0
end
wr
```

Configuration de SD6 :

```
vlan database
vlan 12 name RH_SITE3
vlan 22 name Ventes_SITE3
vlan 32 name Serveurs_SITE3
vlan 42 name Gestion_SITE3
vlan 52 name Wifi_SITE3
exit

enable
conf t
interface vlan 12
 ip address 192.168.12.2 255.255.255.0
 standby 12 ip 192.168.12.254
no sh
exit
interface vlan 22
 ip address 192.168.22.2 255.255.255.0
 standby 22 ip 192.168.22.254
 standby 22 priority 110
 standby 22 preempt
no sh
exit
interface vlan 32
 ip address 192.168.32.2 255.255.255.0
 standby 32 ip 192.168.32.254
no sh
exit
interface vlan 42
 ip address 192.168.42.2 255.255.255.0
 standby 42 ip 192.168.42.254
 standby 42 priority 110
 standby 42 preempt
no sh
```

```
exit
interface vlan 52
 ip address 192.168.52.2 255.255.255.0
 standby 52 ip 192.168.52.254
no sh
end

enable
conf t
interface f0/0
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/2
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/13
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/14
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005

interface f0/15
no sh
switchport mode trunk
switchport trunk allowed vlan 1-1005
end

conf t
spanning-tree vlan 22 priority 24576
end

conf t
```

```
ip routing
router ospf 6
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.22.0 0.0.0.255 area 0
 network 192.168.32.0 0.0.0.255 area 0
 network 192.168.42.0 0.0.0.255 area 0
 network 192.168.52.0 0.0.0.255 area 0
end

wr
```

Configuration de SA7 :

```
enable
configure terminal
vlan 12
name VLAN_RH
no sh
exit
vlan 22
name VLAN_Ventes
no sh
exit
vlan 32
name VLAN_Serveurs
no sh
exit
vlan 42
name VLAN_Gestion
no sh
exit
vlan 52
name VLAN_Wifi
no sh
exit
interface e1/0
```

```
switchport mode access
switchport access vlan 32
exit
interface e1/1
switchport mode access
switchport access vlan 32
no sh
exit
interface e1/2
switchport mode access
switchport access vlan 42
no sh
exit

interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
no sh
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
no sh
wr
```

Configuration de SA8 :

```
enable
configure terminal
vlan 12
name VLAN_RH
exit
vlan 22
name VLAN_Ventes
exit
vlan 32
name VLAN_Serveurs
```

```
exit
vlan 42
name VLAN_Gestion
exit
vlan 52
name VLAN_Wifi
exit
interface e1/0
switchport mode access
switchport access vlan 22
exit
configure terminal
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
exit
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
end
wr
```

Configuration de SA9 :

```
enable
configure terminal
vlan 12
name VLAN_RH
exit
vlan 22
name VLAN_Ventes
exit
vlan 32
name VLAN_Serveurs
exit
vlan 42
name VLAN_Gestion
```

```
exit
vlan 52
name VLAN_Wifi
exit
interface e1/0
switchport mode access
switchport access vlan 12
exit
configure terminal
interface e0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
exit
interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 12,22,32,42,52
end
wr
```