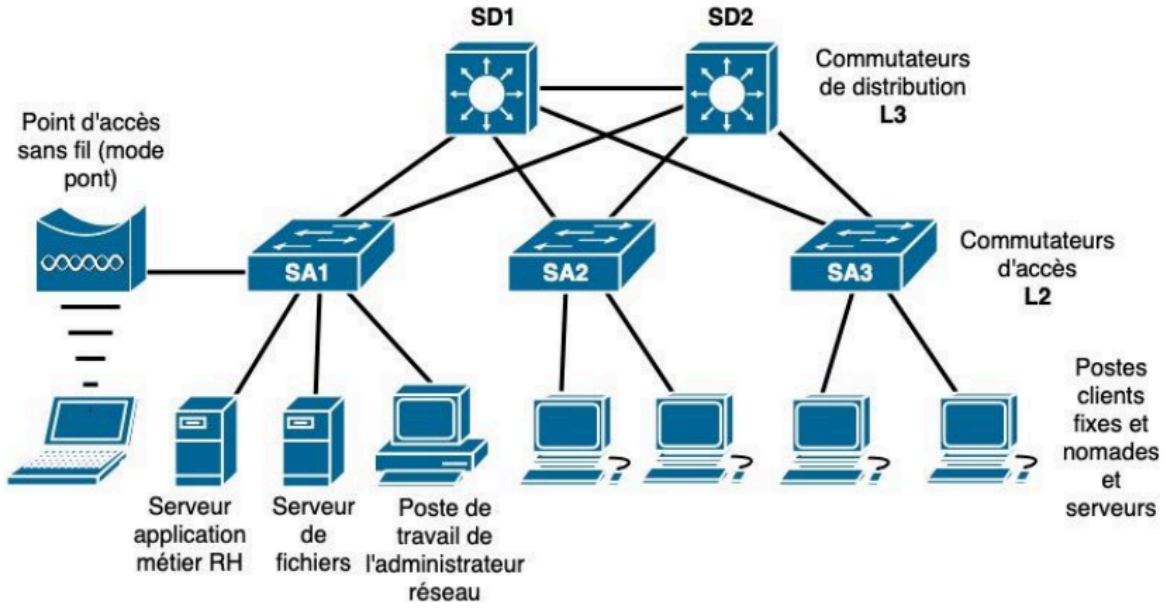
# SAE CYBER

## Compte Rendu

## Mise en place et gestion d'un réseau sécurisé multi-sites

v.1.0



# SOMMAIRE



# 1. Introduction

Dans le cadre de la SAE 3.Cyber03, nous avons été chargés de concevoir et de sécuriser une infrastructure réseau multi-sites. Le projet inclut la mise en place de **VLANs**, du **routage inter-VLANs**, la configuration de la **redondance** via **PVST+** et **HSRP**, et l'interconnexion des différents sites via un **VPN MPLS**. L'objectif principal est de garantir à la fois la performance et la sécurité du réseau tout en respectant les besoins de l'entreprise décrits dans le cahier des charges.

## 2. Problématique

L'entreprise dispose de trois sites distants qui doivent être interconnectés de manière sécurisée tout en garantissant une haute disponibilité et une séparation des différents services via des **VLANs**. Chaque site a besoin d'une redondance au niveau de la passerelle par défaut pour maintenir l'accès à Internet en cas de défaillance d'un équipement réseau. Le projet repose également sur l'utilisation d'**ACLs** pour filtrer les accès et protéger les données sensibles. Enfin, les trois sites doivent être reliés via un **VPN MPLS**, garantissant la communication sécurisée entre eux.

## 3. Développement

### Partie 1 : Configuration du réseau local (VLANs et routage inter-VLAN)

Nous avons commencé par la **création des VLANs** sur les commutateurs de niveau 3 (**SD1** et **SD2**) pour séparer les différents services (Ressources Humaines, Ventes, Serveurs, Gestion, Wi-Fi). Chaque VLAN a été associé à une **Switch Virtual Interface (SVI)** pour permettre le routage inter-VLANs.

**Table d'adresse ip :**

| Site | VLAN | Fonction | Adresse Réseau | Passerelle | Plage DHCP |
|---|---|---|---|---|---|
| Site 1 | VLAN 10 | Ressources Humaines | 192.168.10.0/24 | 192.168.10.1 | 192.168.10.11 - 192.168.10.254 |
| | VLAN 20 | Ventes | 192.168.20.0/24 | 192.168.20.1 | 192.168.20.11 - 192.168.20.254 |
| | VLAN 30 | Serveurs | 192.168.30.0/24 | 192.168.30.1 | 192.168.30.11 - 192.168.30.254 |

| | | | | | |
|---|---|---|---|---|---|
| | VLAN 40 | Gestion | 192.168.40.0/24 | 192.168.40.1 | 192.168.40.11 - 192.168.40.254 |
| Site 2 | VLAN 10 | Ressources Humaines | 192.168.11.0/24 | 192.168.11.1 | 192.168.11.11 - 192.168.11.254 |
| | VLAN 20 | Ventes | 192.168.21.0/24 | 192.168.21.1 | 192.168.21.11 - 192.168.21.254 |
| | VLAN 30 | Serveurs | 192.168.31.0/24 | 192.168.31.1 | 192.168.31.11 - 192.168.31.254 |
| | VLAN 40 | Gestion | 192.168.41.0/24 | 192.168.41.1 | 192.168.41.11 - 192.168.41.254 |
| Site 3 | VLAN 10 | Ressources Humaines | 192.168.12.0/24 | 192.168.12.1 | 192.168.12.11 - 192.168.12.254 |
| | VLAN 20 | Ventes | 192.168.22.0/24 | 192.168.22.1 | 192.168.22.11 - 192.168.22.254 |
| | VLAN 30 | Serveurs | 192.168.32.0/24 | 192.168.32.1 | 192.168.32.11 - 192.168.32.254 |
| | VLAN 40 | Gestion | 192.168.42.0/24 | 192.168.42.1 | 192.168.42.11 - 192.168.42.254 |

**2. Routeurs PE (Provider Edge) pour l'Interconnexion MPLS**

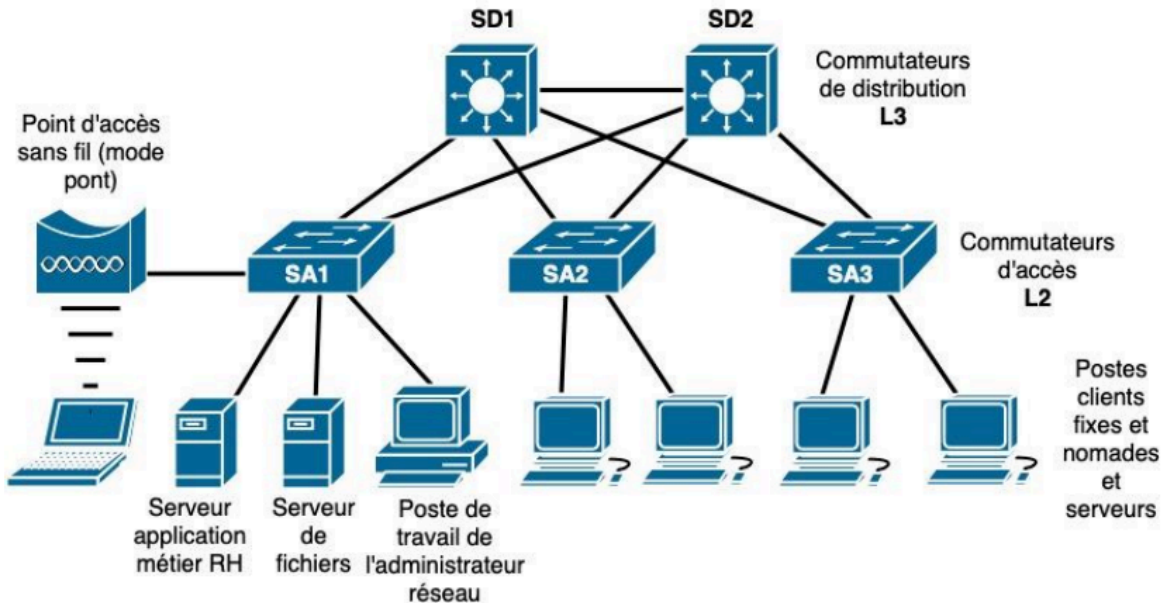
| **Routeur** | **Interface** | **Adresse IP** | **Remarque** |
|---|---|---|---|
| PE1 | Gig0/0 | 10.0.0.1/30 | Connexion PE1 ↔ PE2 |

| | | | |
|---|---|---|---|
| PE2 | Gig0/0 | 10.0.0.2/30 | Connexion PE2 ↔ PE1 |
| PE1 | s1/1 | 20.20.1.1/24 | Connexion vers backbone MPLS |
| PE2 | s1/2 | 20.20.2.2/24 | Connexion vers backbone MPLS |
| PE3 | s1/3 | 20.20.3.3/24 | Connexion vers backbone MPLS |
| P | s1/1 | 20.20.1.2/24 | Backbone MPLS |
| P | s1/2 | 20.20.2.3/24 | Backbone MPLS |
| P | s1/3 | 20.20.3.2/24 | Backbone MPLS |

**3. Routeurs CE (Customer Edge) pour la Connexion MPLS**

| **Routeur** | **Interface** | **Adresse IP** | **Connecté à** |
|---|---|---|---|
| CE1 | Gig0/0 | 192.168.1.1/24 | PE1 |
| CE2 | Gig0/0 | 192.168.2.1/24 | PE2 |
| CE3 | Gig0/0 | 192.168.3.1/24 | PE3 |

## Tâche 1 : réseau d'un site




Pour réaliser la Tâche 1 de la SAE 3.Cyber03, nous allons configurer un réseau local pour un site, avec segmentation en VLANs, routage inter-VLANs, configuration d'ACLs, et mise en place de la redondance. Nous utiliserons des commandes Cisco (IOS) simulées sur GNS3 pour configurer les équipements réseau.

## Topologie sur GNS3:

### 1. Topologie du réseau local

Le réseau d'un site est constitué de deux commutateurs de niveau 3 (**SD1** et **SD2**) et de plusieurs **VLANs**, avec les spécifications suivantes :

- **VLAN 10** : Ressources Humaines (RH)
- **VLAN 20** : Ventes
- **VLAN 30** : Serveurs
- **VLAN 40** : Gestion (administration réseau)

Nous configurons le routage inter-VLANs sur les commutateurs, créons des **ACLs** pour filtrer le trafic, et mettons en place la redondance avec **PVST+** et **HSRP**.

# 3. Développement

### Partie 1 : Configuration du réseau local (VLANs et routage inter-VLAN)

#### Création des VLANs

Les VLANs sont configurés sur les commutateurs de niveau 3 (**SD1** et **SD2**) pour isoler les différents services : RH, Ventes, Serveurs, Gestion, et Wi-Fi.

**Commandes pour créer les VLANs sur les SDx et SAx :**

```
enable
configure terminal
vlan 10
 name RH
vlan 20
 name Ventes
vlan 30
 name Serveurs
vlan 40
 name Gestion
exit
```

- **vlan 10** : Crée un VLAN avec l'ID 10
- **name RH** : Donne un nom au VLAN pour mieux l'identifier

On répète ces commandes pour les autres VLANs

**Configuration des interfaces:**

Chaque VLAN est associé à des interfaces spécifiques sur les commutateurs SAx.

**Commandes pour associer les interfaces aux VLANs :**

```
interface range gi0/2-3
 switchport mode access
 switchport access vlan 10

interface range gi1/0-3
 switchport mode access
 switchport access vlan 20

interface range gi2/0-3
 switchport mode access
 switchport access vlan 30

interface range gi3/0-3
 switchport mode access
 switchport access vlan 40
```

- interface FastEthernet 0/1 : On sélectionne l'interface
- switchport mode access : Définit le port en mode accès (non trunk)

- switchport access vlan 10 : Associe ce port au VLAN 10

On répète ces étapes pour chaque port et VLAN.

**Routage inter-VLAN:**

Pour permettre la communication entre les VLANs, nous configurons des **Switch Virtual Interfaces (SVI)** sur les commutateurs de niveau 3.

**Commandes pour SD1 :**

```
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
 description VLAN_RH
no shut

interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 description VLAN_Ventes
no shut

interface vlan 30
 ip address 192.168.30.1 255.255.255.0
 description VLAN_Serveurs
no shut

interface vlan 40
 ip address 192.168.40.1 255.255.255.0
 description VLAN_Gestion
no shut
```

- **interface Vlan10** : Création d'une interface virtuelle pour le VLAN 10
- **ip address 192.168.20.1 255.255.255.0** : Attribue une adresse IP
- **no shutdown** : Active l'interface

```
# Configurer les ports trunk pour les liaisons entre SA1 et SD1/SD2 :

pour les SAx :

interface range gi0/1-2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
```

```
 no shutdown

pour les SDx :

interface range fa0/1-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
 no shutdown
```

**Activation du routage IP:**

Le routage inter-VLAN doit être activé pour permettre la communication entre les VLANs.

**Commandes :**

```
ip routing
```

Cette commande permet au switch de router le trafic entre les VLANs.

**Sur site 1 : Configuration DHCP sur SD1**

Attribuons des plages d'adresses pour chaque VLAN et définissons les options nécessaires (par exemple, passerelle par défaut, DNS).

```
# Activer le service DHCP sur SD1
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp excluded-address 192.168.50.1 192.168.50.10

# Pool pour le VLAN RH (VLAN 10)
ip dhcp pool VLAN_RH
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8

# Pool pour le VLAN Ventes (VLAN 20)
ip dhcp pool VLAN_Ventes
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
```

```
# Pool pour le VLAN Serveurs (VLAN 30)
ip dhcp pool VLAN_Serveurs
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8

# Pool pour le VLAN Gestion (VLAN 40)
ip dhcp pool VLAN_Gestion
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 8.8.8.8
```

```
Exemple pour SA1 :
interface vlan 10
no ip helper-address 192.168.10.1
# Adresse de SD1 pour le DHCP

interface vlan 20
no ip helper-address 192.168.20.1

interface vlan 30
no ip helper-address 192.168.30.1

interface vlan 40
no ip helper-address 192.168.40.1

write memory
copy running-config startup-config
```

**Sur site 2 : Configuration DHCP sur SD1**

Attribuons des plages d'adresses pour chaque VLAN et définissons les options nécessaires (par exemple, passerelle par défaut, DNS).

```
interface vlan 10
 ip address 192.168.11.1 255.255.255.0
 description VLAN_RH
no shut

interface vlan 20
```

```
 ip address 192.168.21.1 255.255.255.0
 description VLAN_Ventes
no shut

interface vlan 30
 ip address 192.168.31.1 255.255.255.0
 description VLAN_Serveurs
no shut

interface vlan 40
 ip address 192.168.41.1 255.255.255.0
 description VLAN_Gestion
no shut
```

```
# Activer le service DHCP sur SD1
ip dhcp excluded-address 192.168.11.1 192.168.11.10
ip dhcp excluded-address 192.168.21.1 192.168.21.10
ip dhcp excluded-address 192.168.31.1 192.168.31.10
ip dhcp excluded-address 192.168.41.1 192.168.41.10

# Pool pour le VLAN RH (VLAN 10)
ip dhcp pool VLAN_RH
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 8.8.8.8

# Pool pour le VLAN Ventes (VLAN 20)
ip dhcp pool VLAN_Ventes
 network 192.168.21.0 255.255.255.0
 default-router 192.168.21.1
 dns-server 8.8.8.8

# Pool pour le VLAN Serveurs (VLAN 30)
ip dhcp pool VLAN_Serveurs
 network 192.168.31.0 255.255.255.0
 default-router 192.168.31.1
 dns-server 8.8.8.8

# Pool pour le VLAN Gestion (VLAN 40)
ip dhcp pool VLAN_Gestion
 network 192.168.41.0 255.255.255.0
 default-router 192.168.41.1
 dns-server 8.8.8.8
```

```
Exemple pour SA1 :
interface vlan 10
no ip helper-address 192.168.11.1
# Adresse de SD1 pour le DHCP

interface vlan 20
no ip helper-address 192.168.21.1

interface vlan 30
no ip helper-address 192.168.31.1

interface vlan 40
no ip helper-address 192.168.41.1

write memory
copy running-config startup-config
```

**Sur site 3 : Configuration DHCP sur SD1**

Attribuons des plages d'adresses pour chaque VLAN et définissons les options nécessaires (par exemple, passerelle par défaut, DNS).

```
interface vlan 10
 ip address 192.168.12.1 255.255.255.0
 description VLAN_RH
no shut

interface vlan 20
 ip address 192.168.22.1 255.255.255.0
 description VLAN_Ventes
no shut

interface vlan 30
 ip address 192.168.32.1 255.255.255.0
 description VLAN_Serveurs
no shut

interface vlan 40
 ip address 192.168.42.1 255.255.255.0
 description VLAN_Gestion
no shut
```

-

```
interface vlan 10
 ip address 192.168.12.1 255.255.255.0
 description VLAN_RH
no shut

interface vlan 20
 ip address 192.168.22.1 255.255.255.0
 description VLAN_Ventes
no shut

interface vlan 30
 ip address 192.168.32.1 255.255.255.0
 description VLAN_Serveurs
no shut

interface vlan 40
 ip address 192.168.42.1 255.255.255.0
 description VLAN_Gestion
no shut
```

```
# Activer le service DHCP sur SD1
ip dhcp excluded-address 192.168.12.1 192.168.12.10
ip dhcp excluded-address 192.168.22.1 192.168.22.10
ip dhcp excluded-address 192.168.32.1 192.168.32.10
ip dhcp excluded-address 192.168.42.1 192.168.42.10

# Pool pour le VLAN RH (VLAN 10)
ip dhcp pool VLAN_RH
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 8.8.8.8

# Pool pour le VLAN Ventes (VLAN 20)
ip dhcp pool VLAN_Ventes
 network 192.168.22.0 255.255.255.0
 default-router 192.168.22.1
 dns-server 8.8.8.8

# Pool pour le VLAN Serveurs (VLAN 30)
ip dhcp pool VLAN_Serveurs
 network 192.168.32.0 255.255.255.0
 default-router 192.168.32.1
 dns-server 8.8.8.8
```

```
# Pool pour le VLAN Gestion (VLAN 40)
ip dhcp pool VLAN_Gestion
 network 192.168.42.0 255.255.255.0
 default-router 192.168.42.1
 dns-server 8.8.8.8
```

```
Exemple pour SA1 :
interface vlan 10
no ip helper-address 192.168.12.1
# Adresse de SD1 pour le DHCP

interface vlan 20
no ip helper-address 192.168.22.1

interface vlan 30
no ip helper-address 192.168.32.1

interface vlan 40
no ip helper-address 192.168.42.1

write memory
copy running-config startup-config
```

## Partie 3 : Interconnexion des sites avec VPN MPLS

### Analyse du Statut de Connexion LDP entre P et les Routeurs PE:

**Résumé :** Le protocole LDP (Label Distribution Protocol) est utilisé pour établir et maintenir des connexions entre les routeurs dans un réseau MPLS. Le statut des voisins LDP entre le routeur P et trois routeurs PE est le suivant :

1. **Routeur voisin : 3.3.3.3**
   - Connexion TCP : 3.3.3.3.646 - 4.4.4.4.62418
   - État : Actif
   - Nombre de messages envoyés/reçus : 13/13
   - Source de découverte LDP : Serial1/3, IP source : 20.20.3.2
   - Adresse associée : 192.168.3.1
2. **Routeur voisin : 2.2.2.2**
   - Connexion TCP : 2.2.2.2.646 - 4.4.4.4.42274
   - État : Actif
   - Nombre de messages envoyés/reçus : 13/13
   - Source de découverte LDP : Serial1/2, IP source : 20.20.2.2
   - Adresse associée : 192.168.2.1

3. **Routeur voisin : 1.1.1.1**
    - Connexion TCP : 1.1.1.1.646 - 4.4.4.4.47311
    - État : Actif
    - Nombre de messages envoyés/reçus : 11/12
    - Source de découverte LDP : Serial1/1, IP source : 20.20.1.2
    - Adresse associée : 192.168.1.1

Le protocole LDP est opérationnel pour les trois voisins LDP, avec des connexions TCP stables et un échange de messages conforme. Chaque interface série (Serial1/1, Serial1/2, Serial1/3) sert de point de découverte pour les voisins respectifs.

```
P#sh mpls ldp neighbor
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 3.3.3.3.646 - 4.4.4.4.62418
        State: Oper; Msgs sent/rcvd: 13/13; Downstream
        Up time: 00:01:56
        LDP discovery sources:
          Serial1/3, Src IP addr: 20.20.3.2
        Addresses bound to peer LDP Ident:
          192.168.3.1     3.3.3.3         20.20.3.2
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 2.2.2.2.646 - 4.4.4.4.42274
        State: Oper; Msgs sent/rcvd: 13/13; Downstream
        Up time: 00:01:47
        LDP discovery sources:
          Serial1/2, Src IP addr: 20.20.2.2
        Addresses bound to peer LDP Ident:
          192.168.2.1     2.2.2.2         20.20.2.2
    Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 1.1.1.1.646 - 4.4.4.4.47311
        State: Oper; Msgs sent/rcvd: 11/12; Downstream
        Up time: 00:01:36
        LDP discovery sources:
          Serial1/1, Src IP addr: 20.20.1.2
        Addresses bound to peer LDP Ident:
          192.168.1.1     1.1.1.1         20.20.1.2
P#
P#
```

**Statut du Voisin LDP entre PE1 et P**

**Résumé :** Le protocole LDP (Label Distribution Protocol) entre le routeur PE1 et le routeur P (identifié par 4.4.4.4) montre une connexion fonctionnelle avec les détails suivants :

- **Routeur voisin : 4.4.4.4**
    - Connexion TCP : 4.4.4.4.47311 - 1.1.1.1.646
    - État : Actif (Oper)
    - Nombre de messages envoyés/reçus : 13/13
    - Direction : Downstream
    - Durée de la connexion : 00:02:54
    - Source de découverte LDP : Serial1/1, IP source : 20.20.1.1
    - Adresses associées au voisin LDP :

- 20.20.2.1
- 20.20.3.1
- 20.20.1.1

La connexion entre PE1 et P est stable, avec une synchronisation parfaite des messages LDP, indiquant un bon état opérationnel de la liaison et une bonne distribution des étiquettes pour le trafic MPLS.

```
PE1#sh mpls ldp neighbor
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 4.4.4.4.47311 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 13/13; Downstream
        Up time: 00:02:54
        LDP discovery sources:
          Serial1/1, Src IP addr: 20.20.1.1
        Addresses bound to peer LDP Ident:
          4.4.4.4         20.20.2.1       20.20.3.1       20.20.1.1
PE1#
```

**Statut du Voisin LDP entre PE2 et P:**

Résumé : La connexion LDP entre le routeur PE2 et le routeur P (identifié par 4.4.4.4) est opérationnelle, avec les détails suivants :

- Routeur voisin : 4.4.4.4
  - Connexion TCP : 4.4.4.4.42274 - 2.2.2.2.646
  - État : Actif (Oper)
  - Nombre de messages envoyés/reçus : 14/14
  - Direction : Downstream
  - Durée de la connexion : 00:02:57
  - Source de découverte LDP : Serial1/2, IP source : 20.20.2.1
  - Adresses associées au voisin LDP :
    - 4.4.4.4
    - 20.20.2.1
    - 20.20.3.1
    - 20.20.1.1

La liaison LDP entre PE2 et P fonctionne correctement, avec un échange complet de messages et une bonne synchronisation pour la distribution des étiquettes MPLS. La durée de l'uptime montre une stabilité dans l'échange des informations de voisinage.

```
PE2#sh mpls ldp neighbor
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 2.2.2.2:0
        TCP connection: 4.4.4.4.42274 - 2.2.2.2.646
        State: Oper; Msgs sent/rcvd: 14/14; Downstream
        Up time: 00:02:57
        LDP discovery sources:
          Serial1/2, Src IP addr: 20.20.2.1
        Addresses bound to peer LDP Ident:
          4.4.4.4         20.20.2.1       20.20.3.1       20.20.1.1
PE2#
```

**Statut du Voisin LDP entre PE3 et P**

Résumé : La connexion LDP entre le routeur PE3 et le routeur P (identifié par 4.4.4.4) est opérationnelle, avec les détails suivants :

- Routeur voisin : 4.4.4.4
  - Connexion TCP : 4.4.4.4.62418 - 3.3.3.3.646
  - État : Actif (Oper)
  - Nombre de messages envoyés/reçus : 12/12
  - Direction : Downstream
  - Durée de la connexion : 00:01:21
  - Source de découverte LDP : Serial1/3, IP source : 20.20.3.1
  - Adresses associées au voisin LDP :
    - 4.4.4.4
    - 20.20.2.1
    - 20.20.3.1
    - 20.20.1.1

La connexion LDP entre PE3 et P est stable, avec un bon échange de messages LDP pour la distribution des étiquettes MPLS. Bien que l'uptime soit plus court par rapport aux autres voisins, la communication reste fonctionnelle et opérationnelle.

```
PE3#sh mpls ldp neighbor
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 3.3.3.3:0
        TCP connection: 4.4.4.4.62418 - 3.3.3.3.646
        State: Oper; Msgs sent/rcvd: 12/12; Downstream
        Up time: 00:01:21
        LDP discovery sources:
          Serial1/3, Src IP addr: 20.20.3.1
        Addresses bound to peer LDP Ident:
          4.4.4.4         20.20.2.1       20.20.3.1       20.20.1.1
PE3#
```

**Configuration des routeurs PE**

Nous avons interconnecté les trois sites via un **VPN MPLS**, en utilisant des routeurs **Provider Edge (PE)** pour simuler le réseau opérateur et Customer Edge(CE).

## Configuration du routeur PE1

### Connecté au site CLIENT1.

```
conf t
hostname PE1

! Configuration des interfaces
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.252
 no shutdown

interface Serial1/1
 ip address 20.20.1.2 255.255.255.252
 no shutdown
 mpls ip

! Loopback pour BGP
interface Loopback0
 ip address 1.1.1.1 255.255.255.255

! Activation MPLS LDP
mpls ldp router-id Loopback0 force

! OSPF pour le transport des routes
router ospf 1
 router-id 1.1.1.1
 network 20.20.1.0 0.0.0.3 area 0
 network 1.1.1.1 0.0.0.0 area 0

! BGP pour VPN MPLS avec P
router bgp 100
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit
end
```

Cette configuration met en place un routeur PE (Provider Edge) dans un réseau MPLS VPN pour connecter un client (CLIENT1).

- Interface Backbone (**FastEthernet0/0)** : Connectée au réseau MPLS avec MPLS activé.
- Interface Client (**FastEthernet0/1**) : Associée à la VRF **CLIENT1** et connectée au réseau du client 192.168.1.0/24.
- VRF CLIENT1 : Définit un Route Distinguisher (RD) et des Route Targets pour l'export/import des routes.
- BGP (AS 65000) :
    - Établit une session avec un routeur P (**10.0.0.2**, AS **65000**).
    - Active l'address-family vpnv4 pour l'échange des routes VPN.
    - Redistribue le réseau du client (192.168.1.0/24) dans BGP

## Configuration du routeur PE2

**Connecté au site CLIENT2.**

```
conf t
hostname PE2

! Configuration des interfaces
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.252
 no shutdown

interface Serial1/2
 ip address 20.20.2.2 255.255.255.252
 no shutdown
 mpls ip

! Loopback pour BGP
interface Loopback0
 ip address 2.2.2.2 255.255.255.255

! Activation MPLS LDP
mpls ldp router-id Loopback0 force

! OSPF pour le transport des routes
```

```
router ospf 1
 router-id 2.2.2.2
 network 20.20.2.0 0.0.0.3 area 0
 network 2.2.2.2 0.0.0.0 area 0

! BGP pour VPN MPLS avec P
router bgp 100
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit
end
```

## Résumé

Cette configuration met en place un routeur PE (Provider Edge) pour le client CLIENT2 dans un environnement MPLS VPN.

- Interface Backbone (**FastEthernet0/0**) : Connectée au réseau MPLS avec MPLS activé pour transporter les routes.
- Interface Client (**FastEthernet0/1**) : Connectée au réseau local du client CLIENT2 avec l'adresse **192.168.2.0/24** et associée à la VRF CLIENT2.
- VRF CLIENT2 :
    - Route Distinguisher (RD) et Route Targets sont définis pour l'export et l'import des routes de la VRF.
- BGP (**AS 65000**) :
    - Une session BGP est établie avec le routeur P (**10.0.0.6, AS 65000**).
    - L'address-family vpnv4 est activée pour l'échange des routes VPN.
    - Le réseau 192.168.2.0/24 de CLIENT2 est redistribué via BGP.

## Configuration du routeur PE3

**Connecté au site CLIENT3.**

```
conf t
```

```
hostname PE3

! Configuration des interfaces
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.252
 no shutdown

interface Serial1/3
 ip address 20.20.3.2 255.255.255.252
 no shutdown
 mpls ip

! Loopback pour BGP
interface Loopback0
 ip address 3.3.3.3 255.255.255.255

! Activation MPLS LDP
mpls ldp router-id Loopback0 force

! OSPF pour le transport des routes
router ospf 1
 router-id 3.3.3.3
 network 20.20.3.0 0.0.0.3 area 0
 network 3.3.3.3 0.0.0.0 area 0

! BGP pour VPN MPLS avec P
router bgp 100
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit
end
```

## Résumé

Cette configuration met en place un routeur PE (Provider Edge) pour le client CLIENT3 dans un réseau MPLS VPN.

- Interface Backbone (**FastEthernet0/0**) : Connectée au réseau MPLS avec MPLS activé pour assurer la connectivité dans le backbone MPLS.
- Interface Client **(FastEthernet0/1**) : Cette interface est associée à la VRF CLIENT3 et connectée au réseau local du client, 192.168.3.0/24.
- VRF CLIENT3 :
    - Définition du Route Distinguisher (RD) et des Route Targets pour l'exportation et l'importation des routes dans le VPN.
- BGP (AS 65000) :
    - Une session BGP est configurée avec le routeur P (**10.0.0.10**, AS **65000**).
    - L'address-family vpnv4 est activée pour l'échange des routes VPN.
    - Le réseau 192.168.3.0/24 de CLIENT3 est redistribué via BGP pour que les informations de routage soient propagées dans le réseau MPLS**.**

## Vérification

**Une fois la configuration terminée, utilisez ces commandes pour tester :**

```
show mpls ldp neighbor      ! Vérifier les voisins MPLS
show mpls forwarding-table  ! Vérifier la table MPLS
show ip bgp vpnv4 all       ! Vérifier les routes VPN dans BGP
ping vrf CLIENT1 192.168.2.1 ! Tester la communication entre les clients
ping vrf CLIENT1 192.168.3.1
ping vrf CLIENT2 192.168.3.1
```

**Vérification des Voisins MPLS LDP:**

```
P#show mpls ldp neighbor
    Peer LDP Ident: 10.0.0.1:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 10.0.0.1.42088 - 4.4.4.4.646
        State: Oper; Msgs sent/rcvd: 18/6; Downstream
        Up time: 00:02:44
        LDP discovery sources:
          Serial1/1, Src IP addr: 10.0.0.1
        Addresses bound to peer LDP Ident:
          10.0.0.1
    Peer LDP Ident: 10.0.0.5:0; Local LDP Ident 4.4.4.4:0
        TCP connection: 10.0.0.5.49171 - 4.4.4.4.646
        State: Oper; Msgs sent/rcvd: 17/7; Downstream
        Up time: 00:02:44
        LDP discovery sources:
          Serial1/2, Src IP addr: 10.0.0.5
        Addresses bound to peer LDP Ident:
          10.0.0.5
```

La commande **show mpls ldp neighbor** affiche les informations des voisins LDP (Label Distribution Protocol) sur un routeur utilisant MPLS (Multiprotocol Label Switching). Voici les détails de la sortie :

### 1. Identification des voisins LDP

Chaque voisin est identifié par un LDP Ident (LDP Identifier) sous la forme IP:0. Dans cet exemple, le routeur local (4.4.4.4) a établi des sessions LDP avec deux voisins :

- Voisin 1 : **10.0.0.1:0**
- Voisin 2 : **10.0.0.5:0**

## 2. Connexions TCP établies

LDP utilise TCP (port 646) pour établir des sessions :

- Avec **10.0.0.1** via le port 42088
- Avec **10.0.0.5** via le port 49171

## 3. État des sessions LDP

L'état des sessions LDP est **Oper** (opérationnel), indiquant que les voisins sont bien établis.

## 4. Statistiques des messages échangés

- Avec **10.0.0.1**: 18 messages envoyés, 6 reçus
- Avec **10.0.0.5**: 17 messages envoyés, 7 reçus

## 5. Découverte LDP et interfaces associées

- La découverte LDP pour **10.0.0.1** se fait via Serial1/1 (Source IP: **10.0.0.1**).
- La découverte LDP pour **10.0.0.5** se fait via Serial1/2 (Source IP: **10.0.0.5**).

## 6. Adresses liées aux voisins

Chaque voisin possède une seule adresse IP associée (**10.0.0.1** et **10.0.0.5**).

```
P#show bgp summary
BGP router identifier 4.4.4.4, local AS number 65000
BGP table version is 22, main routing table version 22
4 network entries using 468 bytes of memory
4 path entries using 208 bytes of memory
2/1 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 924 total bytes of memory
BGP activity 7/3 prefixes, 11/7 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1        4 65000      43      48        0    0    0 00:03:55 Active
10.0.0.5        4 65000      43      48        0    0    0 00:03:54 Active
10.0.0.9        4 65000      43      48        0    0    0 00:03:51 Active
192.168.1.1     4   100       0       0        0    0    0 never    Active
192.168.2.1     4   200       0       0        0    0    0 never    Active
192.168.3.1     4   300       0       0        0    0    0 never    Active
P#
```

Cette commande affiche l'état des sessions BGP du routeur, y compris les voisins, l'AS local, les échanges de messages et l'état des connexions. Ici, toutes les sessions BGP sont en "Active", indiquant un problème de connexion avec les voisins, nécessitant une vérification des configurations et de la connectivité réseau.

---

### Résumé

✅ **MPLS activé sur le backbone pour transporter les labels.**
✅ **BGP utilisé pour l'échange des routes entre les PE sans OSPF.**
✅ **VRF isolées pour chaque client afin d'assurer la séparation du trafic.**
✅ **Test de connectivité entre les clients via le réseau MPLS.**

Cette configuration assure une interconnexion MPLS sécurisée et optimisée.

Voici la configuration pour un seul routeur PE qui gère trois clients (PE1, PE2, PE3) et trois routeurs CE connectés à chaque client.
Nous utilisons MPLS VPN et BGP, sans OSPF, pour l'interconnexion des sites clients.

---

### Topologie

- PE (Provider Edge) : Routeur central qui gère plusieurs clients.
- CE1, CE2, CE3 (Customer Edge) : Routeurs clients connectés à PE.
- VRF (Virtual Routing and Forwarding) : Segmentation du trafic pour chaque client.

---

## Configuration du routeur PE

```
conf t
! Activation MPLS sur l'interface backbone (vers le P)
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.252
 mpls ip
 no shutdown

! Interface vers CE1 (CLIENT1)
interface GigabitEthernet0/1
 ip vrf forwarding CLIENT1
 ip address 192.168.1.1 255.255.255.252
 no shutdown

! Interface vers CE2 (CLIENT2)
interface GigabitEthernet0/2
```

```
 ip vrf forwarding CLIENT2
 ip address 192.168.2.1 255.255.255.252
 no shutdown

! Interface vers CE3 (CLIENT3)
interface GigabitEthernet0/3
 ip vrf forwarding CLIENT3
 ip address 192.168.3.1 255.255.255.252
 no shutdown

! Configuration VRF pour chaque client
ip vrf CLIENT1
 rd 1:1
 route-target export 1:1
 route-target import 1:1

ip vrf CLIENT2
 rd 2:2
 route-target export 2:2
 route-target import 2:2

ip vrf CLIENT3
 rd 3:3
 route-target export 3:3
 route-target import 3:3

! Configuration BGP
router bgp 65000
 bgp log-neighbor-changes

 ! Configuration avec P
 neighbor 10.0.0.2 remote-as 65000

 address-family vpnv4
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community extended
 exit

 ! Configuration des CE (Customer Edge)
 address-family ipv4 vrf CLIENT1
  neighbor 192.168.1.2 remote-as 100
  network 192.168.10.0 mask 255.255.255.0
 exit

 address-family ipv4 vrf CLIENT2
```

```
 neighbor 192.168.2.2 remote-as 200
 network 192.168.20.0 mask 255.255.255.0
exit

address-family ipv4 vrf CLIENT3
 neighbor 192.168.3.2 remote-as 300
 network 192.168.30.0 mask 255.255.255.0
exit
end
```

### Résumé

Cette configuration met en place un routeur Provider Edge (PE) dans un réseau MPLS avec BGP et VRF pour isoler plusieurs clients.

- MPLS activé sur l'interface backbone (**GigabitEthernet0/0**) pour établir des connexions avec le routeur P.
- Séparation des clients avec des VRF (Virtual Routing and Forwarding) pour CLIENT1, CLIENT2 et CLIENT3.
- BGP configuré pour échanger les routes entre le PE (**AS 65000**) et :
    - Le routeur P **(AS 65000**) pour le transport MPLS VPN.
    - Les routeurs CE (**AS 100, 200, 300)** via des sessions BGP dans leurs VRF respectifs.
- Annonce des réseaux clients via BGP dans chaque VRF.

## Configuration du routeur CE1 (Customer Edge 1)

```
conf t
interface GigabitEthernet3/3
 no switchport
 ip address 192.168.1.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 no switchport
 ip address 192.168.10.1 255.255.255.0
 no shutdown

router bgp 100
```

```
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 65000
 address-family ipv4
  network 192.168.10.0 mask 255.255.255.0
 exit
 address-family vpnv4
  neighbor 192.168.1.1 activate
  send-community extended
 exit
end
```

### Résumé

Cette configuration met en place un routeur CE (Customer Edge) connecté à un routeur PE (Provider Edge) dans un réseau MPLS VPN.

- Interface WAN (**GigabitEthernet3/3**) : Connectée au routeur PE (**192.168.1.1**), attribuée à l'AS **65000**.
- Interface LAN (**GigabitEthernet0/1**) : Utilisée pour le réseau local du client (**192.168.10.0/24**).
- BGP activé (AS 100) :
    - Établit une session avec le PE (**192.168.1.1**, AS 6**5000)**.
    - Annonce le réseau local (**192.168.10.0/24**).
    - Active **vpnv4** et envoie les communautés étendues pour le transport MPLS VPN.

## Configuration du routeur CE2 (Customer Edge 2)

```
conf t
interface GigabitEthernet3/3
 no switchport
 ip address 192.168.2.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 no switchport
 ip address 192.168.20.1 255.255.255.0
 no shutdown
```

```
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.2.1 remote-as 65000
 address-family ipv4
  network 192.168.20.0 mask 255.255.255.0
 exit
 address-family vpnv4
  neighbor 192.168.2.1 activate
  send-community extended
 exit
end
```

Cette configuration met en place un routeur CE2 connecté au routeur PE dans un réseau MPLS VPN pour le client AS 200.

- Interface WAN (**GigabitEthernet3/3**) : Connectée au PE (**192.168.2.1**), appartenant à l'AS **65000.**
- Interface LAN (**GigabitEthernet0/1**) : Fournit la connectivité au réseau local du client (192.168.20.0/24).
- BGP activé (AS 200) :
    - Établit une session avec le PE **(192.168.2.1**, AS **65000**).
    - Annonce le réseau 192.168.20.0/24 via BGP.
    - Active vpnv4 et envoie les communautés étendues pour l'intégration dans le VPN MPLS.

## Configuration du routeur CE3 (Customer Edge 3)

```
conf t
interface GigabitEthernet3/3
 no switchport
 ip address 192.168.3.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 no switchport
 ip address 192.168.30.1 255.255.255.0
```

```
 no shutdown

router bgp 300
 bgp log-neighbor-changes
 neighbor 192.168.3.1 remote-as 65000
 address-family ipv4
  network 192.168.30.0 mask 255.255.255.0
 exit
 address-family vpnv4
  neighbor 192.168.3.1 activate
  send-community extended
 exit
end
```

### Résumé

Cette configuration met en place un routeur CE3 connecté au PE dans un réseau MPLS VPN pour le client AS 300.

- Interface WAN (**GigabitEthernet3/3**) : Connectée au PE (**192.168.3.1**), appartenant à l'AS **65000**.
- Interface LAN (**GigabitEthernet0/1**) : Fournit la connectivité au réseau local du client (192.168.30.0/24).
- BGP activé (AS 300) :
    - Établit une session BGP avec le PE (**192.168.3.1**, AS **65000**).
    - Annonce le réseau 192.168.30.0/24 via BGP.
    - Active vpnv4 et envoie les communautés étendues pour l'intégration dans le VPN MPLS.

## Vérification

### Sur PE

```
show mpls ldp neighbor       ! Vérifier les voisins MPLS
show mpls forwarding-table   ! Vérifier la table MPLS
show ip bgp vpnv4 all        ! Vérifier les routes VPN dans BGP
```

```
P#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     2.2.2.2/32       0          Se1/2       point2point
17     Pop tag     3.3.3.3/32       0          Se1/3       point2point
18     Pop tag     1.1.1.1/32       0          Se1/1       point2point
P#
```

### Sur CE1, CE2 et CE3

```
show ip bgp summary        ! Vérifier les routes BGP
ping 192.168.20.1          ! Tester la connexion CLIENT1 vers CLIENT2
ping 192.168.30.1          ! Tester la connexion CLIENT1 vers CLIENT3
```

```
Switch#show ip bgp summary
BGP router identifier 192.168.40.1, local AS number 100
BGP table version is 3, main routing table version 3
1 network entries using 144 bytes of memory
1 path entries using 84 bytes of memory
1/1 BGP path/bestpath attribute entries using 164 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 392 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4        65000       0       0        1    0    0 never    Idle
Switch#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

- BGP est activé sur le switch (AS 100) avec un voisin 192.168.1.1 (PE, AS 65000).
- La session BGP est en "Idle", ce qui signifie qu'elle n'est pas encore établie. Cela peut être dû à :
    - Une mauvaise configuration BGP (ex : mauvais numéro d'AS ou problème d'authentification).
    - Un problème de connectivité entre le switch et le routeur PE.
    - Le PE qui n'a pas de configuration BGP correspondante pour AS 100.
- Tests ICMP réussis vers 192.168.20.1 (CE2) et 192.168.30.1 (CE3), ce qui prouve que la connectivité de base fonctionne.

### Actions Recommandées

1. Vérifier la configuration BGP du PE (192.168.1.1, AS 65000) et s'assurer qu'il accepte une session avec AS 100.

2. Vérifier que le port TCP 179 (utilisé par BGP) est ouvert entre le switch et le PE.
3. Exécuter la commande **show ip bgp neighbors** pour plus de détails sur l'état de la session BGP.
4. Vérifier si un ACL ou un pare-feu bloque la session BGP.

## Résumé

✅ Un seul PE (Provider Edge) gère plusieurs clients avec des VRF séparées.
✅ Chaque CE (Customer Edge) utilise BGP pour annoncer son réseau au PE.
✅ Le backbone MPLS transporte les routes clients de manière isolée.
✅ Aucune configuration OSPF, tout est basé sur BGP VPNv4 et MPLS.

## Sur SD1 (pour les interfaces des VLANs et serveurs)

**ACL 1 : Autoriser uniquement le VLAN RH et l'administrateur réseau à accéder au serveur RH sur le port 443**

```
access-list 101 permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.100 eq 443
access-list 101 permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.100 eq 443
access-list 101 permit ip any any

interface Vlan30
 ip access-group 101 in
```

## Analyse ligne par ligne :

1. access-list 101 permit tcp 192.168.10.0 0.0.0.255 host 192.168.30.100 eq 443
   - Cette ligne autorise le trafic TCP provenant du réseau 192.168.10.0/24 (VLAN RH) vers l'hôte 192.168.30.100 (Serveur RH) uniquement sur le port 443 (HTTPS).
   - Traduction : Les machines du VLAN RH peuvent accéder au serveur RH via HTTPS.
2. access-list 101 permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.100 eq 443
   - Cette ligne autorise le trafic TCP provenant du réseau 192.168.40.0/24 (VLAN Gestion) vers 192.168.30.100 sur le port 443.
   - Traduction : L'administrateur réseau (présent dans le VLAN Gestion) peut également accéder au serveur RH via HTTPS.
3. access-list 101 permit ip any any
   - Cette règle permet tout autre trafic non explicitement filtré par les règles précédentes.
   - Traduction : Une fois que les règles spécifiques ont été évaluées, tout autre trafic est autorisé sans restriction.

## Application sur l'interface VLAN30 :

- interface Vlan30
    - Définit l'interface VLAN 30 (où est connecté le serveur RH).
- ip access-group 101 in
    - Applique l'ACL 101 en entrée sur l'interface VLAN30.
    - Impact : Seuls les paquets entrant sur cette interface respectant les règles définies dans l'ACL sont acceptés.

## Résumé du fonctionnement :

- Seuls les utilisateurs des VLAN RH (192.168.10.0/24) et Gestion (192.168.40.0/24) peuvent accéder au serveur RH (192.168.30.100) via HTTPS (port 443).
- Tout autre trafic est autorisé (grâce à la dernière ligne permit ip any any).
- Cette configuration garantit que seules les entités autorisées peuvent interagir avec le serveur via HTTPS, tout en permettant d'autres types de communications.

**ACL 2 : Autoriser uniquement le VLAN Ventes et l'administrateur réseau à accéder au serveur FTP**

```
access-list 102 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.200 eq 21
access-list 102 permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.200 eq 21
access-list 102 permit ip any any
interface Vlan30
ip access-group 102 in
```

## Explication ligne par ligne :

```
access-list 102 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.200 eq 21
```

Cette ligne **autorise** le trafic TCP provenant du réseau **192.168.20.0/24** (VLAN Ventes) vers l'hôte **192.168.30.200** (Serveur FTP) uniquement sur le **port 21** (**FTP**).

```
access-list 102 permit tcp 192.168.40.0 0.0.0.255 host 192.168.30.200 eq 21
```

Cette ligne **autorise** le trafic TCP provenant du réseau **192.168.40.0/24** (VLAN Gestion) vers **192.168.30.200** sur le **port 21**.

```
access-list 102 permit ip any any
```

Cette règle **permet tout autre trafic** non filtré par les règles précédentes.

**Impact :** Après avoir appliqué les premières restrictions, tout autre trafic est accepté sans restriction.

## Application sur l'interface VLAN30 :

```
interface Vlan30
```

Définit l'interface VLAN 30 (où est connecté le serveur FTP).

```
ip access-group 102 in
```

Applique l'ACL **102 en entrée** sur l'interface VLAN30.

**Impact :** Seuls les paquets respectant les règles définies sont autorisés à entrer dans VLAN30.

## Résumé du fonctionnement :

- **Seuls les VLANs Ventes (192.168.20.0/24) et Gestion (192.168.40.0/24) peuvent accéder au serveur FTP (192.168.30.200) via le port 21.**
- Tout autre trafic est **autorisé** par la dernière règle (permit ip any any).
- Cela garantit que les utilisateurs non autorisés **(ex. VLAN RH, autres VLANs)** ne peuvent pas accéder au serveur FTP.

**ACL 3 : Empêcher tous les VLANs sauf celui de gestion d'accéder au VLAN de gestion**

```
access-list 103 deny ip any 192.168.40.0 0.0.0.255
access-list 103 permit ip 192.168.40.0 0.0.0.255 any
access-list 103 permit ip any any

interface Vlan40
 ip access-group 103 in
```

## Explication ligne par ligne :

```
access-list 103 deny ip any 192.168.40.0 0.0.0.255
```

- Bloque tout trafic provenant de n'importe quelle source (any) vers le réseau 192.168.40.0/24 (VLAN Gestion).
- Impact : Les autres VLANs ne peuvent pas accéder au VLAN Gestion.

```
access-list 103 permit ip 192.168.40.0 0.0.0.255 any
```

- Autorise le trafic provenant du VLAN Gestion (192.168.40.0/24) vers n'importe quelle destination (any).
- Impact : Les machines du VLAN Gestion peuvent communiquer avec tous les autres VLANs et réseaux externes.

```
access-list 103 permit ip any any
```

- Autorise tout autre trafic non bloqué par les règles précédentes.
- Impact : Évite de bloquer involontairement du trafic non lié au VLAN Gestion.

---

Application sur l'interface VLAN40 :

```
interface Vlan40
```

- Définit l'interface VLAN 40 (VLAN Gestion).

```
ip access-group 103 in
```

- Applique l'ACL 103 en entrée sur l'interface VLAN40.
- Impact : Seuls les paquets respectant ces règles sont acceptés en entrée sur VLAN40.

### Résumé du fonctionnement :

- Bloque l'accès de tous les autres VLANs vers VLAN40 (Gestion).
- Autorise les machines du VLAN40 à initier des connexions vers d'autres VLANs et réseaux externes.
- Tout autre trafic est autorisé après ces règles.

➡ **Ces configurations sont toutes réalisées sur le commutateur SD1**, car les VLANs et serveurs sont généralement gérés par le L3 switch principal.

---

## 2. Configuration de la Redondance avec PVST+

### Sur SD1 (Root primaire pour VLAN RH)

```
spanning-tree mode pvst
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root secondary
```

### Explication des commandes :

```
spanning-tree mode pvst
```

- Active le mode **PVST+**, qui maintient une **instance STP par VLAN**.
- Cela permet un meilleur contrôle et une meilleure répartition du trafic par VLAN.

```
spanning-tree vlan 10 root primary
```

- Définit le **commutateur comme Root Bridge principal** pour le **VLAN 10**.
- Le **Root Bridge** est le switch qui a l'ID de pont (Bridge ID) le plus bas.
- Cette commande ajuste automatiquement la priorité STP pour assurer qu'il soit élu **Root Bridge** pour VLAN 10.

```
spanning-tree vlan 20 root secondary
```

- Définit ce switch comme **Root Bridge secondaire** pour **VLAN 20**.
- Si le Root Bridge principal pour VLAN 20 tombe en panne, ce switch deviendra **Root Bridge**.

## Résumé

- PVST+ permet une instance STP par VLAN pour un meilleur contrôle du trafic.
- SD1 est Root Bridge pour VLAN 10 et secondaire pour VLAN 20.
- SD2 peut être configuré comme Root Bridge pour VLAN 20 et secondaire pour VLAN 10, équilibrant ainsi la charge.

## Sur SD2 (Root primaire pour VLAN Ventes)

```
spanning-tree mode pvst
spanning-tree vlan 20 root primary
spanning-tree vlan 10 root secondary
```

## Explication des commandes :

```
spanning-tree mode pvst
```

- Active **PVST+**, qui maintient une **instance STP distincte par VLAN**.
- Cela permet un **meilleur contrôle du trafic** et une **répartition optimisée de la charge** sur plusieurs liens redondants.

```
spanning-tree vlan 20 root primary
```

- Définit ce commutateur comme **Root Bridge principal** pour le **VLAN 20**.
- Cela ajuste automatiquement sa **priorité STP** pour qu'il ait l'ID de pont (Bridge ID) le plus bas et soit élu **Root Bridge** pour ce VLAN.

```
spanning-tree vlan 10 root secondary
```

- Définit ce commutateur comme **Root Bridge secondaire** pour **VLAN 10**.
- Si le Root Bridge principal du VLAN 10 tombe en panne, ce commutateur prendra le relais.

### Résumé

- PVST+ permet un STP indépendant par VLAN, améliorant la résilience et l'efficacité du réseau.
- Ce switch est Root Bridge pour VLAN 20 et secondaire pour VLAN 10.
- Un second switch (SD1) peut être configuré en Root Bridge pour VLAN 10 et secondaire pour VLAN 20 pour équilibrer la charge.

**➡ Ces configurations doivent être réalisées sur les deux commutateurs SD1 et SD2.**

---

## 3. Configuration de la Redondance avec HSRP

### Sur SD1 (Passerelle active pour VLAN RH, passive pour VLAN Ventes)

```
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 1 ip 192.168.10.1
 standby 1 priority 110
 standby 1 preempt

interface Vlan20
 ip address 192.168.20.3 255.255.255.0
 standby 2 ip 192.168.20.1
 standby 2 priority 90
 standby 2 preempt
```

## Explication des commandes :

### 1. Configuration du VLAN 10 :

- ip address 192.168.10.2 255.255.255.0
  → Définit l'adresse IP physique de l'interface VLAN 10 sur ce switch.
- standby 1 ip 192.168.10.1
  → Définit l'adresse IP **virtuelle HSRP** (**192.168.10.1**) qui servira de passerelle par défaut pour les hôtes du VLAN 10.
- standby 1 priority 110
  → Définit une **priorité HSRP de 110** (valeur par défaut = **100**).
  → Le routeur avec la **plus haute priorité** devient **actif**.
- standby 1 preempt
  → Permet au routeur de **reprendre son rôle de passerelle active** lorsqu'il redevient opérationnel après une panne.

### 2. Configuration du VLAN 20 :

- ip address 192.168.20.3 255.255.255.0
  → Définit l'adresse physique de l'interface VLAN 20.
- standby 2 ip 192.168.20.1
  → Définit l'adresse IP virtuelle HSRP pour ce VLAN (192.168.20.1).
- standby 2 priority 90
  → Définit une priorité plus basse (90), donc ce switch sera en standby pour VLAN 20.
- standby 2 preempt
  → Permet au routeur de récupérer son rôle en cas de rétablissement.

## Résumé :

HSRP assure une redondance de passerelle pour éviter les interruptions réseau.
Le switch avec la priorité la plus haute devient actif et l'autre est en mode standby.
En cas de panne, le switch standby prend automatiquement le relais.
L'équilibrage de charge peut être optimisé en définissant un Root Bridge différent pour chaque VLAN avec PVST+.

### Sur SD2 (Passerelle active pour VLAN Ventes, passive pour VLAN RH)

```
interface Vlan10
 ip address 192.168.10.3 255.255.255.0
 standby 1 ip 192.168.10.1
 standby 1 priority 90
 standby 1 preempt

interface Vlan20
 ip address 192.168.20.2 255.255.255.0
```

```
standby 2 ip 192.168.20.1
standby 2 priority 110
standby 2 preempt
```

## Explication des commandes :

### 1. Interface VLAN 10 :

```
interface Vlan10
 ip address 192.168.10.3 255.255.255.0
 standby 1 ip 192.168.10.1
 standby 1 priority 90
 standby 1 preempt
```

- ip address 192.168.10.3 255.255.255.0
  → Adresse physique de l'interface VLAN 10 sur ce switch.
- standby 1 ip 192.168.10.1
  → Définit l'adresse IP virtuelle HSRP utilisée comme passerelle par défaut des hôtes du VLAN 10.
- **standby 1 priority 90**
  → Définit une priorité de 90 (moins élevée que sur l'autre switch qui a 110).
  → Ce switch sera en standby (backup) pour VLAN 10.

```
standby 1 preempt
```

- → Active la récupération automatique du rôle de passerelle après une panne.

### 2. Interface VLAN 20 :

```
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby 2 ip 192.168.20.1
 standby 2 priority 110
 standby 2 preempt
```

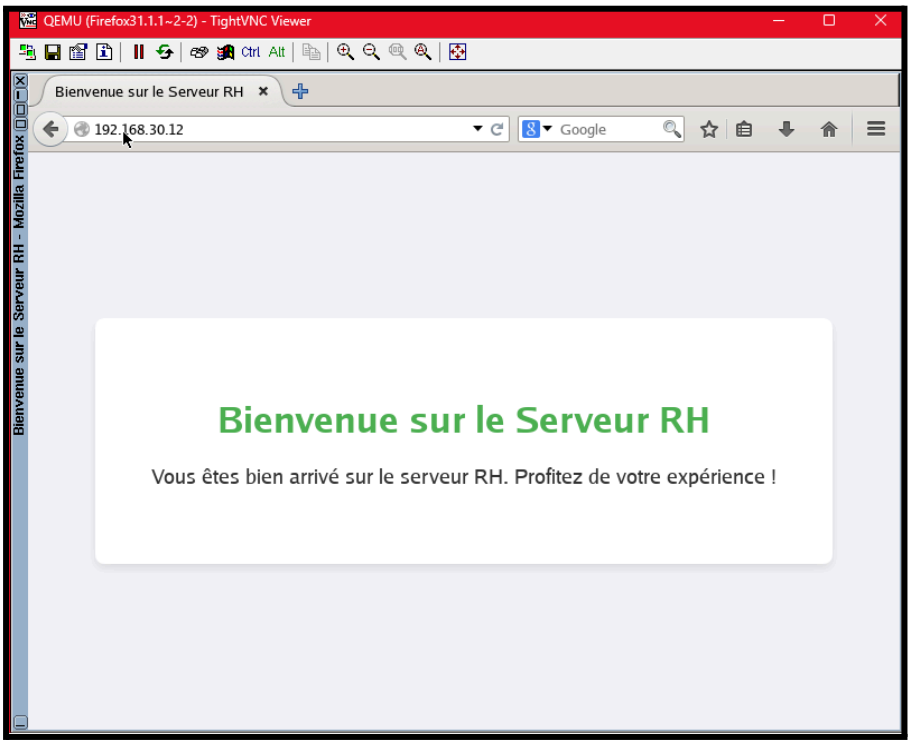
- ip address 192.168.20.2 255.255.255.0
  → Adresse physique de l'interface VLAN 20 sur ce switch.
- standby 2 ip 192.168.20.1
  → Définit l'adresse IP virtuelle HSRP pour VLAN 20.
- standby 2 priority 110
  → Définit une priorité de 110, ce qui signifie que ce switch sera actif pour VLAN 20.
- standby 2 preempt
  → Permet de récupérer son rôle de passerelle en cas de rétablissement après une panne.

## Résumé

-HSRP permet une continuité du service avec un basculement automatique de la passerelle en cas de panne.
-L'équilibrage de charge est optimisé en répartissant le rôle de passerelle entre les deux switches.
- STP (PVST+) peut être utilisé en complément pour éviter les boucles et améliorer la répartition du trafic.

---

## Configuration des serveur




**Configuration d'un serveur FTP sécurisé (vsftpd)** Installation de vsftpd

Sur un serveur Debian/Ubuntu :

```
sudo apt update
sudo apt install vsftpd -y
```

Sur un serveur CentOS/RHEL :

```
sudo yum install vsftpd -y
```

### Configuration de vsftpd

Éditez le fichier de configuration :

```
sudo nano /etc/vsftpd.conf
```

Modifiez ou ajoutez ces paramètres pour répondre au cahier des charges :

```
# Interdit l'accès anonyme
anonymous_enable=NO

# Active l'accès des utilisateurs locaux
local_enable=YES

# Permet l'écriture pour les utilisateurs locaux
write_enable=YES

# Empêche les utilisateurs d'accéder à d'autres répertoires
chroot_local_user=YES

# Active le mode passif pour éviter des problèmes de pare-feu
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000

# Sécurisation du transfert avec TLS
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
force_local_logins_ssl=YES
force_local_data_ssl=YES
```

Enregistrez (**Ctrl+X**, puis **Y**, puis **Enter**).

---

## Création des utilisateurs FTP

Créez un utilisateur dédié pour le FTP :

```
sudo adduser ftpuser
sudo passwd ftpuser
```

Créez un dossier FTP et ajustez les permissions :

```
sudo mkdir -p /home/ftpuser/ftp
```

```
sudo chown ftpuser:ftpuser /home/ftpuser/ftp
sudo chmod 750 /home/ftpuser/ftp
```

---

### Génération d'un certificat SSL (TLS) pour sécuriser les connexions

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

---

### Redémarrage et activation du serveur FTP

```
sudo systemctl restart vsftpd
sudo systemctl enable vsftpd
```

---

### Tester la connexion FTP

**En ligne de commande** :

```
ftp localhost
```

**Avec un client FTP comme FileZilla** :

- Hôte : **sftp://IP_DU_SERVEUR**
- Utilisateur : **ftpuser**
- Mot de passe : celui défini précédemment
- Port : **21** (FTP) ou **990** (FTPS)

### Configuration d'un utilisateur FTP sécurisé sous Debian

### Explication:

Cette configuration permet de créer un utilisateur FTP sécurisé avec un répertoire dédié et un certificat SSL pour renforcer la sécurité des connexions. Pour compléter l'installation, il faut configurer vsftpd (Very Secure FTP Daemon) pour utiliser ce certificat et restreindre l'accès des utilisateurs FTP à leur répertoire personnel.

```
root@debian:/home/debian# sudo adduser ftpuser
sudo passwd ftpuser
Adding user `ftpuser' ...
Adding new group `ftpuser' (1002) ...
Adding new user `ftpuser' (1002) with group `ftpuser' ...
Creating home directory `/home/ftpuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftpuser
Enter the new value, or press ENTER for the default
        Full Name []: [ 1485.595905] device-mapper: uevent: version 1.0.3
[ 1485.603379] device-mapper: ioctl: 4.43.0-ioctl (2020-10-01) initialised: dm-devel@redhat.com

        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] [ 1526.739501] systemd[1]: systemd 247.3-7+deb11u6 running in system mode. (+PAM +AUDIT +SELINUX +
IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL +XZ +LZ4 +ZSTD +SECCOMP +BLKID +ELFUTILS +KMOD +IDN2 -IDN +
PCRE2 default-hierarchy=unified)
[ 1526.752293] systemd[1]: Detected virtualization kvm.
[ 1526.755151] systemd[1]: Detected architecture x86-64.
[ 1526.987514] systemd-journald[191]: Received SIGTERM from PID 1 (systemd).
[ 1526.991495] systemd[1]: Stopping Journal Service...
[ 1527.005163] systemd[1]: systemd-journald.service: Succeeded.
[ 1527.007029] systemd[1]: Stopped Journal Service.
[ 1527.010627] systemd[1]: Starting Journal Service...
[ 1527.043387] systemd[1]: Started Journal Service.
[ 1527.059069] systemd-journald[12105]: Received client request to flush runtime journal.
s
New password:
Retype new password:
passwd: password updated successfully
root@debian:/home/debian# sudo mkdir -p /home/ftpuser/ftp
sudo chown ftpuser:ftpuser /home/ftpuser/ftp
sudo chmod 750 /home/ftpuser/ftp
root@debian:/home/debian# sudo mkdir -p /home/ftpuser/ftp
root@debian:/home/debian# sudo chown ftpuser:ftpuser /home/ftpuser/ftp
root@debian:/home/debian# sudo chmod 750 /home/ftpuser/ftp
root@debian:/home/debian# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/
certs/vsftpd.pem
Generating a RSA private key
.............+++++
.........................................+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:^C
```

```
.........................................+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:^C
root@debian:/home/debian# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/
certs/vsftpd.pem
Generating a RSA private key
.........+++++
.........................+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:974
Locality Name (eg, city) []:974
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IUT
Organizational Unit Name (eg, section) []:IUT
Common Name (e.g. server FQDN or YOUR name) []:IUT
Email Address []:
root@debian:/home/debian#
```

## Outils Utilisés:

Pour la conception et la sécurisation du réseau, plusieurs outils ont été mobilisés :

- **GNS3** : Utilisé pour la simulation et la configuration des équipements réseau dans un environnement virtuel.
- **Cisco IOS** : Interface de ligne de commande permettant la configuration des routeurs et commutateurs.
- **Linux (Debian/Ubuntu)** : Système d'exploitation utilisé pour configurer et sécuriser les services réseau, notamment le serveur FTP.
- **vsftpd** : Serveur FTP sécurisé mis en place avec chiffrement TLS pour la gestion des fichiers.
- **ACLs (Access Control Lists)** : Implémentées sur les équipements réseau pour filtrer les accès et renforcer la sécurité.

## Problèmes Rencontrés:

Lors de la mise en place du réseau sécurisé multi-sites, plusieurs défis ont été rencontrés :

1. **Problèmes de routage inter-VLAN** : L'activation du routage IP et la configuration correcte des interfaces ont nécessité des ajustements pour permettre la communication entre les VLANs.
2. **Configuration complexe du VPN MPLS** : La mise en place des VRF et des sessions BGP a nécessité une compréhension approfondie du routage dynamique et des tables de routage spécifiques à chaque client.
3. **Gestion des ACLs** : La définition de règles de filtrage adaptées a demandé des tests rigoureux pour éviter des blocages involontaires du trafic légitime.
4. **Sécurisation des accès** : La configuration des accès aux serveurs, notamment via FTP sécurisé avec TLS, a demandé une gestion fine des utilisateurs et des permissions.

Malgré ces difficultés, des solutions ont été trouvées pour garantir une infrastructure performante et sécurisée.

## Conclusion:

La mise en place d'un réseau sécurisé multi-sites dans le cadre de la SAE 3.Cyber03 a permis d'intégrer différentes solutions pour garantir la performance, la fiabilité et la protection des communications. La segmentation du réseau via VLANs, l'optimisation du routage inter-VLAN et la configuration de la redondance avec HSRP et PVST+ ont assuré une haute disponibilité du système. L'interconnexion sécurisée des sites via MPLS a permis d'établir une communication fiable tout en préservant l'isolation des données sensibles.

Ce projet a mis en évidence les défis liés à la gestion et à la sécurisation d'une infrastructure réseau d'entreprise, notamment en termes de configuration des équipements, de gestion des accès et de prévention des pannes. Malgré certaines difficultés rencontrées, les objectifs ont été atteints, permettant de concevoir un réseau performant et sécurisé. Cette expérience nous a apporté une meilleure maîtrise des technologies réseau et une approche méthodique pour résoudre des problématiques complexes liées à la cybersécurité et à l'administration des infrastructures IT.