

# ***Rapport Du Projet Thématique***

## **THEME**

**Implémentation du Protocole BGP dans un Réseau WAN.**

Dirigé Par :  
**Pr. Nguyen Thi-Mai-Trang**

Présenté Par :  
**BELKHODJA Ibrahim**  
**HANOU Rimy**

**JUIN 2024**

## Table des Matières

<b>I. Introduction .....</b>	<b>1</b>
<b>II. Définition du projet .....</b>	<b>1</b>
1) Contexte .....	1
2) Cahier de charges .....	1
3) Stratégie de travail.....	2
<b>III. Organisation du travail.....</b>	<b>3</b>
1) Répartition des tâches.....	3
2) Méthodologie de travail .....	3
<b>IV. Travail réalisée.....</b>	<b>3</b>
1) Description de l'architecture du réseau.....	3
2) Câblages .....	5
3) Plan d'adressage : .....	5
4) Détails du Plan d'Adressage .....	22
5) Configuration des Sites .....	6
6) Configuration routage interne OSPF .....	9
7) Configuration routage externe BGP .....	11
<b>V. Analyse des résultats obtenus.....</b>	<b>13</b>
A. Scénario 1 : Communication interne entre les différents sites de l'entreprise A .....	13
B. Scénario 2 : Communication inter-entreprises (entreprise A et entreprise B) .....	18
<b>VI. Problèmes rencontrés.....</b>	<b>20</b>
<b>VII. Conclusion.....</b>	<b>21</b>
<b>VIII. Annexes .....</b>	<b>22</b>

## I. Introduction

Dans le cadre de notre programme académique, nous avons entrepris un projet réseau ayant pour but de consolider et de mettre en pratique les connaissances théoriques acquises au cours de l'année. L'objectif principal de ce projet est d'appliquer concrètement nos compétences dans un environnement réaliste.

## II. Définition du projet

### 1) Contexte

Notre projet consiste à déployer les protocoles de routage BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First) dans un réseau WAN, connectant deux entreprises distinctes présente dans différent pays : l'Entreprise **A** et l'Entreprise **B**.

Le réseau sera conçu pour offrir une connectivité robuste et sécurisée, tout en optimisant les performances et en assurant une redondance adéquate.

### 2) Cahier de charges

Pour la réalisation de ce projet, on a d'abord commencé par définir les objectifs et la faisabilité de ce projet, et on a suivi le cahier des charges suivant :

Notre projet comporte plusieurs exigences spécifiques telles que la conception de la topologie du réseau, la configuration du routage BGP et OSPF ainsi que l'implémentation des différent protocoles qui vont assurer la redondance (HSRP, STP, PortFast, EtherChannel) et la sécurité (VPN, SSH) de notre réseau.

Les configurations de HSRP, EtherChannel, et PortFast seront intégrées à l'intérieur des AS pour optimiser les performances et assurer la redondance.

Les objectifs spécifiques comprennent :

- Concevoir une topologie réseau adaptée aux besoins de l'organisation.
- Configurer les protocoles de routage BGP et OSPF pour assurer une connectivité optimale.
- Mettre en place des mécanismes de redondance tels que HSRP, STP, EtherChannel pour garantir la disponibilité du réseau.
- Sécuriser l'infrastructure en configurant des mesures de sécurité telles que SSH, VPN.
- Effectuer des tests de connectivité et d'analyse de performance pour valider le bon fonctionnement du réseau.

L'infrastructure réseau devra répondre aux spécifications techniques suivantes :

- **Topologie réseau :** Une topologie en étoile sera adoptée, avec des commutateurs d'accès connectés à des commutateurs de distribution, eux-mêmes reliés à des routeurs de cœur.

- **Protocoles de routage** : le protocole BGP sera utilisé pour la connectivité externe entre les deux entreprises, tandis qu'OSPF sera utilisé pour le routage interne.
- **Redondance** : le protocole HSRP sera configuré pour assurer la redondance au niveau des passerelles par défaut, STP pour éviter les boucles de commutation, EtherChannel pour agréger les liens et PortFast pour accélérer la convergence des ports.
- **Sécurité** : SSH sera configuré pour sécuriser l'accès aux équipements réseau, un VPN sera mis en place pour sécuriser les communications.
- **Tests** : Des tests de connectivité à l'aide de Ping et de traceroute seront réalisés, ainsi que l'utilisation de Sniffers pour analyser le trafic réseau et évaluer les performances.

### 3) Stratégie de travail

Après l'étude de notre cahier de charge, on a décidé de partager le travail en deux parties, une partie recherche et configuration interne des AS et une partie recherche et configuration externe entre les AS.

- Pour la partie **recherche et configuration interne des AS** on a suivi la stratégie suivante :

Dans la phase initiale de configuration interne des AS, nous avons d'abord concentré nos efforts sur la segmentation du réseau et la mise en place de mesures de sécurité de base, notamment la configuration des VLANs, des interfaces trunk/Access ainsi que les paramètres de sécurité. En parallèle, nous avons mis en œuvre des fonctionnalités de redondance telles que HSRP, STP et EtherChannel pour garantir la haute disponibilité du réseau.

Après avoir terminé ça, Nous avons mené une recherche approfondie sur les concepts d'OSPF et les meilleures pratiques de configuration des zones OSPF, puis avons conçu la topologie OSPF en définissant les zones appropriées. Dans la phase de configuration proprement dite, nous avons activé OSPF sur les routeurs et les switches layer 3 afin de garantir la connectivité interne. De plus, nous avons configuré les protocoles de redondance et pris des mesures de sécurité telles que l'utilisation de SSH.

Enfin, nous avons validé notre configuration en effectuant des tests de connectivité OSPF et en vérifiant les tables de routage OSPF pour assurer un routage efficace.

- Pour la partie **recherche et configuration Externe entre AS** on a suivi la stratégie suivante :

Notre objectif dans cette partie était d'assurer une communication robuste et sécurisée entre nos deux entreprises (2AS). Pour cela, nous avons suivi une approche méthodique, débutant par une phase de recherche approfondie sur les concepts fondamentaux de BGP et les meilleures pratiques de configuration. En parallèle, nous avons planifié les connexions BGP en définissant les relations de peering entre les AS et en planifiant l'adressage IP des interfaces externes.

Enfin, pour valider notre configuration, nous avons effectué des tests de connectivité BGP en utilisant des commandes Ping, traceroute et en effectuant des requêtes HTTP pour vérifier la connectivité entre les AS et avec les différents serveurs présents sur les deux AS.

En suivant cette stratégie de travail, nous assurons une approche méthodique et organisée pour l'implémentation des protocoles de routage internes et externes dans notre réseau WAN.

### III. Organisation du travail

#### 1) Répartition des tâches

Notre groupe a réalisé un projet en réseau, ce qui a nécessité une collaboration étroite et continue. À la différence des projets habituels en informatique ou en robotique, cette collaboration était essentielle du fait que nous avons travaillé sur un fichier commun. pkt. Cette méthode nous a obligés à travailler de manière synchronisée, car chaque modification apportée par l'un des membres de l'équipe devait être immédiatement comprise par l'autre pour éviter toute confusion lors des prochaines sessions de travail. Ainsi, ce projet a réellement été un travail collectif où chaque membre a contribué de manière significative à l'ensemble des tâches, permettant une avancée harmonieuse et efficace du projet.

#### 2) Méthodologie de travail

Pour garantir une collaboration efficace et une progression régulière de notre projet d'implémentation du Protocole BGP dans un réseau WAN nous avons adopté une stratégie de travail collaborative et flexible.

Chaque jour de la semaine, on se réunit via la plateforme Discord pour partager l'avancement de notre travail, les recherches effectuées, les solutions trouvées, et les propositions de nouvelles idées. Ces réunions quotidiennes nous permettent de discuter des étapes complétées, d'identifier les obstacles rencontrés, et de planifier les tâches à accomplir pour le jour suivant. Nous échangeons ouvertement des idées et des solutions potentielles pour résoudre les problèmes et améliorer les configurations existantes.

Cette approche flexible nous permet d'ajuster notre stratégie chaque fois que nous rencontrons un blocage ou une situation compliquée. En fonction des défis rencontrés, nous modifions notre approche et recherchons de nouvelles méthodes ou outils pour surmonter les obstacles.

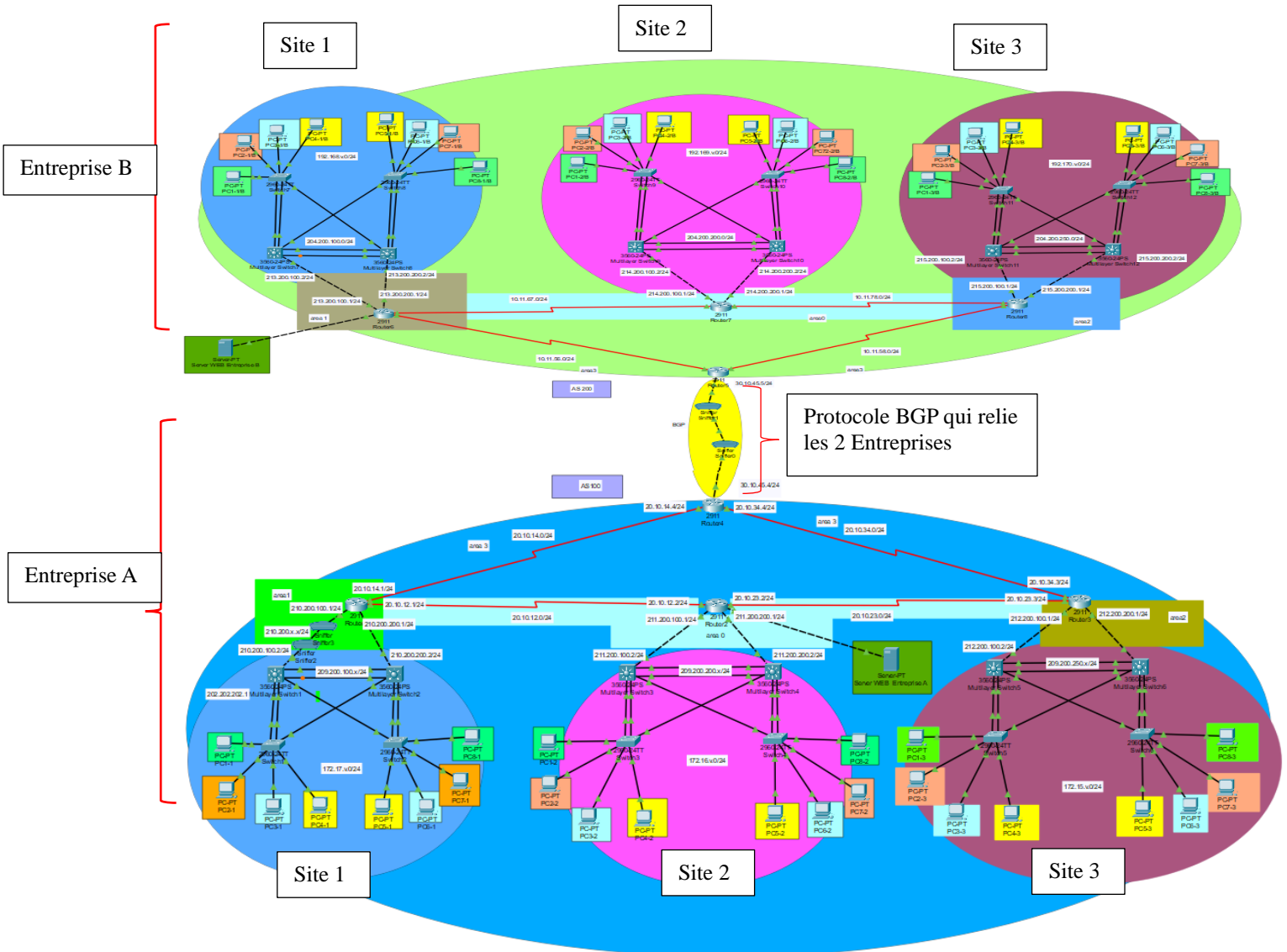
Cette documentation continue est essentielle pour maintenir un suivi précis des configurations et des modifications apportées, faciliter la révision et l'amélioration continue du réseau, et préparer un rapport final détaillé.

### IV. Travail réalisée

#### 1) Description de l'architecture du réseau

- **Entreprise A** et **Entreprise B** sont les deux principales entités du réseau.
- Les deux entreprises sont interconnectées via BGP pour permettre la communication entre elles.
- Chaque entreprise est composée de **trois sites**, connectés via OSPF et contient un server WEB.
- Chaque site comprend **4 départements** représentés par 4 différents VLANs.

L'objectif est de créer une topologie réseau robuste, sécurisé et optimisé, offrant une redondance adéquate.



Chaque Entreprise répond aux exigences de connectivité et de robustesse avec trois sites distincts (Area 1, Area 2, Area 3), interconnectés par le protocole OSPF. Chaque site est lié à l'Area 0, assurant une communication efficace.

Par exemple pour l'entreprise A :

- Le site 1 dispose du routeur R1, servant d'AS border router et connecté à l'Area 0 et Area 1 et Area 3 il dispose aussi de 2 MLS (switch layer 3) connecter à l'area 1.
- Le site 2 comprend le routeur R2 et les MLS 3 et 4, et sont tous relié au backbone Area 0.
- Le site 3, quant à lui, comporte le routeur R3 relié aux différents Area 0, 2, 3 ainsi que les MLS 6 et 7, relié à l'Area 2.

Le même principe pour l'**entreprise B** :

- **Le site 1** dispose du routeur R6, servant d'AS border router et connecté à l'Area 0 et Area 1 et Area 3 il dispose aussi de 2 MLS connecter à l'area 1.
- **Le site 2** comprend le routeur R7 et les MLS 9 et 10, et sont tous relié au backbone Area 0.
- **Le site 3**, quant à lui, comporte le routeur R8 relié aux différents Area 0, 2, 3 ainsi que les MLS 11 et 12, relié à l'Area 2.

Pour étendre le réseau de l'**entreprise A** celui de l'**entreprise B** nous avons intégré les routeurs R4 et R5 respectivement ou l'implémentation du routage BGP va être configuré.

## 2) Câblages

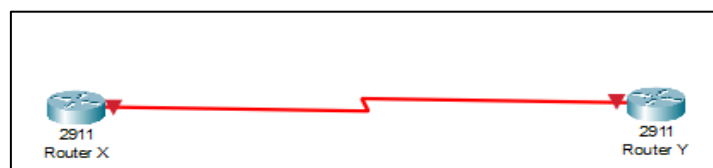
L'utilisation de câbles séries et de câbles croisés dans votre architecture réseau est justifiée par les besoins spécifiques de connectivité et de performance.

- **Câbles Séries** : Utilisés pour des connexions point-à-point fiables entre les routeurs, idéaux pour les liaisons WAN et les communications longue distance.
- **Câbles Croisés** : Utilisés pour des connexions directes entre les routeurs et les switches multicouches, optimisant la communication et réduisant les risques de collision.

Ces choix de câblage contribuent à la robustesse, la flexibilité et la performance globale de votre réseau, assurant ainsi une infrastructure efficace et fiable.

## 3) Plan d'adressage :

Pour effectuer notre plan d'adressage IP, nous avons d'abord calculé les plages d'adresses nécessaires en fonction de la topologie réseau. Voici les adresses IP choisies pour les deux entreprises et la connexion entre les routeurs R4 et R5 :



### ▪ **Entreprise A :**

Pour l'entreprise A, nous avons choisi l'adresse 20.10.XY.0/24, où X et Y sont déterminés en fonction des noms des routeurs. La règle est de choisir X comme le plus petit chiffre et Y comme le plus grand chiffre selon les noms des routeurs.

**Exemple :** Si les routeurs sont nommés Router 2 et Router 3, l'adresse serait 20.10.23.0/24.

### ▪ **Entreprise B :**

Pour l'entreprise B, nous avons choisi l'adresse 10.11.XY.0/24, où X et Y sont également déterminés en fonction des noms des routeurs de la même manière.

**Exemple :** Si les routeurs sont nommés Router 1 et Router 4, l'adresse serait 10.11.14.0/24.

### ▪ **Connexion entre les Routeurs R4 et R5 :**

Pour la connexion entre les routeurs R4 et R5, nous avons choisi l'adresse 30.10.45.0/24.





➤ **Figure montrant le protocole EtherChannel dans le MLS 1 :**

```

S1-1#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----
1      Po1 (SU)      LACP        Fa0/1 (P) Fa0/2 (P)
2      Po2 (RU)      -           Fa0/4 (P) Fa0/5 (P)

```

### 5.3) Mise en Place des Protocoles de Sécurité et de Redondance

En parallèle avec la configuration d'EtherChannel, nous avons choisi de configurer les switches Layer 3 en tant que **serveurs DHCP**. Cela nous a permis d'attribuer dynamiquement des adresses IP aux différents terminaux présents sur chaque VLAN, simplifiant ainsi la gestion des adresses IP. Grâce à cette configuration, nous avons pu rendre notre réseau interne plus performant, redondant et sécurisé.

Et enfin pour assurer un minimum de sécurité ainsi qu'une redondance accrue afin de ne pas surcharger le trafic, nous avons configuré le protocole HSRP (**Hot Standby Router Protocol**). Cela permet de répartir le trafic sur plusieurs routes, améliorant ainsi les performances de notre réseau interne.

➤ **Figure montrant un Exemple de configuration HRP sur MLS 1 :**

```

interface Vlan10
  mac-address 00e0.b030.9a01
  ip address 172.17.10.1 255.255.255.0
  standby 10 ip 172.17.10.254
  standby 10 preempt
!
interface Vlan20
  mac-address 00e0.b030.9a02
  ip address 172.17.20.1 255.255.255.0
  standby 20 ip 172.17.20.254
  standby 20 preempt
!
interface Vlan30
  mac-address 00e0.b030.9a03
  ip address 172.17.30.1 255.255.255.0
  standby 30 ip 172.17.30.254
  standby 30 priority 110
  standby 30 preempt
!
interface Vlan40
  mac-address 00e0.b030.9a04
  ip address 172.17.40.1 255.255.255.0
  standby 40 ip 172.17.40.254
  standby 40 priority 110
  standby 40 preempt
!

```

Grâce à cette configuration, nous avons implémenté HSRP de manière que les paquets des VLANs 10 et 20 sortent via le MLS (Multi-Layer Switch) 2, tandis que ceux des VLANs 30 et 40 sortent via le MLS 1. L'objectif est de répartir la charge sur les données sortantes pour garantir une bonne redondance de notre réseau interne, tout en assurant une alternative de sortie pour nos données en cas de panne de l'un des MLS. Cette mise en place du protocole assure ainsi une efficacité accrue contre les pannes et maintient la continuité des services réseau.

De plus, nous avons configuré le protocole STP pour éviter les boucles réseau en désactivant les liens redondants jusqu'à ce qu'ils soient nécessaires.

➤ **Figure montrant la configuration du protocole stp sur le MLS 1 :**

```
!
spanning-tree mode pvst
spanning-tree vlan 30,40 priority 24576
spanning-tree vlan 10,20 priority 28672
!
```

#### **5.4) Configuration de PortFast**

La configuration de PortFast a été un ajout de notre part pour accélérer la convergence des interfaces Access de nos terminaux. Cette configuration a été réalisée grâce aux commandes suivantes :

```
spanning-tree portfast
spanning-tree bpduguard enable
```

Après avoir terminé toutes ces implémentations, nous avons configuré le protocole SSH (Secure Shell). Ce protocole permet de sécuriser l'accès aux différents routeurs et switches de couches 2 et 3 en créant des sessions protégées par des utilisateurs et des mots de passe chiffrés. La configuration a été faite à travers les commandes suivantes :

```
Hostname S1-1
Ip domain-name xx.com
Username xx secret xx
Crypto key generate rsa 1025
Line vty 0 15
Login local
Transport input ssh
```

#### **5.5) Configuration VPN entre les différents sites de chaque entreprise**

On a aussi implémenté le VPN entre les différents routeurs présents dans nos zones OSPF ce qui nous a permis de rendre nos données transmises plus sécurisées en créant des routes tunnel, l'implémentation a été faite grâce aux commandes suivantes :

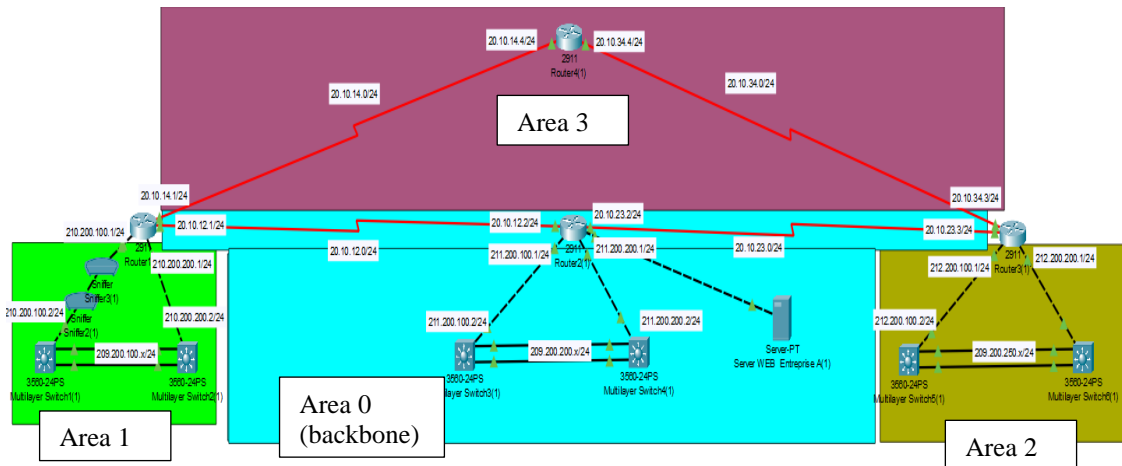
```
Interface tunnel 1
Ip address x.x.x.x masque x.x.x.x
No shutdown
Tunnel source x
Tunnel destination x.x.x.x
```

Grâce à ces configurations, notre réseau interne est maintenant optimisé capable de gérer les besoins complexes des environnements modernes tout en assurant une robustesse et une redondance accrues.

## 5) Configuration routage interne OSPF

Dans le cadre de la conception et de la mise en œuvre de notre réseau, nous avons opté pour le protocole de routage OSPF (Open Shortest Path First) en raison de ses nombreux avantages en termes de performance, de flexibilité et de gestion.

- Figure qui représente les différentes Area ou OSPF a été configurer :



En effet OSPF est un protocole de routage à état de lien qui excelle dans les environnements réseau de grande envergure et complexes.

Il est particulièrement adapté à notre topologie en raison de sa scalabilité, permettant de gérer efficacement un grand nombre de routes et d'appareils. En utilisant une architecture hiérarchique basée sur des zones, OSPF réduit la taille des tables de routage et minimise le trafic de mise à jour, optimisant ainsi les ressources réseau.

Afin de commencer la configuration de ce protocole de routage dynamique on a d'abord activé le protocole OSPF sur chaque routeur et switch layer 3. Cela est indispensable pour permettre le routage dynamique entre les différents segments du réseau.

- Sur chaque routeur et multi switch, nous avons utilisé la commande suivante pour entrer en mode configuration du routeur OSPF :

**Router ospf 1**

C'est la première étape pour commencer à utiliser OSPF, permettant aux routeurs de commencer à échanger des informations de routage. Le numéro '1' représente le processus OSPF, et il doit être répété sur tous les routeurs du réseau.

- Ensuite, pour le processus de spécification, chaque interface a été associée à une zone OSPF appropriée en utilisant la commande suivante :

**Network [network-address] [wildcard-mask] area [area-id]**

- Ou bien la commande suivante :

**Interface [interface-id] ip ospf [process-id] area [area-id]**

À travers l'une de ces commandes on a pu identifier les réseaux qui seront inclus dans le processus OSPF et les associe à une zone spécifique. Ce qui permet aux routeurs OSPF de connaître les sous-réseaux locaux et de les annoncer aux autres routeurs OSPF, ce qui est crucial pour la construction de la table de routage OSPF.

- A travers les différentes commandes suivantes :

**Show ip ospf neighbor**  
**Show ip ospf**  
**Show ip route ospf**

Nous avons vérifié l'état des voisins OSPF, les informations sur le processus OSPF et les routes OSPF dans la table de routage de nos routeurs et layer 3 switches ce qui nous a permis de nous assurer que la configuration est correcte et que les routes sont bien définies. Ces commandes nous permettent aussi de diagnostiquer et résoudre les problèmes potentiels.

- Voici un exemple de la fenêtre de commande que nous avons utilisée pour configurer OSPF dans le site 1 (area 1) de l'entreprise A. La configuration OSPF pour le R1 a été réalisée avec les commandes suivantes :

**Router ospf 1**  
**router-id 8.8.8.8**  
**log-adjacency-changes**  
**Network 20.10.12.0 0.0.0.255 area 0**  
**Network 20.10.14.0 0.0.0.255 area 3**

- On peut confirmer la bonne configuration de nos commandes pour chaque routeur à travers la commande « **sh ip ospf neighbor** » :

```
S1-l#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
8.8.8.8	1	FULL/DR	00:00:38	210.200.100.1	GigabitEthernet0/1
1.1.1.1	1	FULL/BDR	00:00:37	172.17.10.2	Vlan10
1.1.1.1	1	FULL/BDR	00:00:37	172.17.20.2	Vlan20
1.1.1.1	1	FULL/BDR	00:00:37	172.17.30.2	Vlan30
1.1.1.1	1	FULL/BDR	00:00:37	172.17.40.2	Vlan40
1.1.1.1	1	FULL/BDR	00:00:33	209.200.100.2	Port-channel2

```
S1-l#
```

Comme le montre le résultat de la commande « **sh ip ospf neighbor** » on a fait on sorte de configurer dans chaque segment du réseau ou le protocole OSPF est configurer le router DR et le router BDR ici par exemple dans le routeur 1 on a configurer l'interface g0/1 en tant que DR en lui donnant le plus grand RID à travers la commande « **Router-id 8.8.8.8** » et on a aussi configurer le BDR en lui donnant le second plus grand RID , la même configuration a été faite sur les autres segments du réseau pour les autre routeur ou on a configurer OSPF dans notre topologie.

## 6.1) Analyses DR et BDR

Les rôles de DR (Designated Router) et BDR (Backup Designated Router) attribués à l'Int g0/1 avec une adresse de 210.200.100.1 et aux autres interfaces respectivement, sont essentiels pour la redondance et la résilience du réseau. Ces rôles garantissent une centralisation efficace des mises à jour de routage OSPF et une reprise rapide en cas de défaillance du DR, grâce à la présence du BDR. La configuration actuelle montre que les adjacences OSPF sont correctement établies, affirmant une stabilité et une efficacité optimales du protocole OSPF sur R1.

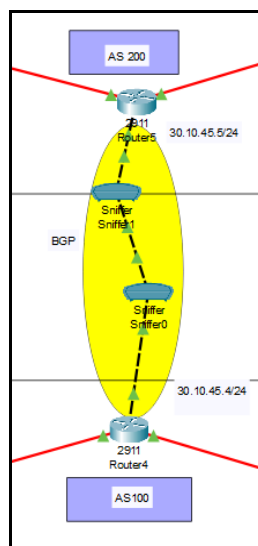
En outre à travers ces résultats on peut dire que la configuration OSPF sur nos différents routeurs et multi switches est bien conçue, avec des adjacences correctement établies et des rôles de DR et BDR bien définis. Cette configuration assure une diffusion efficace des mises à jour de routage et une résilience accrue du réseau, grâce à une reprise rapide en cas de défaillance du routeur désigné.

## 6) Configuration routage externe BGP

Le Border Gateway Protocol (BGP) est un protocole de routage extérieur utilisé pour l'échange d'informations de routage entre des systèmes autonomes (AS). Contrairement aux protocoles de routage internes comme OSPF, BGP gère le routage entre différents AS, garantissant ainsi une connectivité fiable sur Internet.

Chaque étape de la configuration BGP joue un rôle important dans l'établissement de sessions BGP, la publicité des routes, et la sécurité et la performance du réseau.

- Dans notre topologie la configuration de protocole BGP se fera entre les routeurs 4 et 5 :



- Afin de commencer notre configuration la première chose qu'on a faite est la déclaration du processus BGP à travers la commande :

<b>Router bgp [AS_Number]</b>
-------------------------------

À travers cette commande qu'on a implémenté sur les 2 routeurs en donnant un numéro AS différent pour chacun on a pu initialiser le processus BGP sur les routeurs.

Nous avons attribué le numéro **AS 100** au routeur 4 et le numéro **AS 200** au routeur 5, l'importance de donner de différent numéro AS est parce que ce numéro identifie de manière unique un groupe de réseaux sous une administration unique.

- Après avoir activé le protocole BGP sur nos deux routeurs la deuxième étape à faire est de configurer les voisins (peers) BGP afin d'établir des sessions BGP entre voisins ce qui est essentiel pour échanger des informations de routage. Ceci peut être fait à travers la commande :

<b>Neighbor [IP_Address] remote-as [AS_Number]</b>
--

En fournissant l'adresse IP de l'interface voisin ainsi que le numéro de l'AS voisin la session BGP sera établie entre nos deux routeurs 4 et 5.

La connexion entre voisins peut être à l'intérieur du même AS (**iBGP**) ou entre différents AS (**eBGP**). Ici dans notre cas on utilisera **eBGP** vu que la communication des voisins sera entre 2 différents AS

- Et enfin l'étape finale sera d'annoncer les réseaux qu'on veut publier à notre voisin BGP qui se fera à travers la commande :

<b>Network [IP_Address] mask [Subnet_Mask]</b>
--

- Cette commande permet d'annoncer les réseaux qu'on souhaite publier à notre voisin BGP.
- Permet au routeur de partager des informations sur les réseaux internes avec d'autres routeurs BGP pour garantir la connectivité.
- Il est crucial de spécifier correctement les sous-réseaux pour éviter la publicité incorrecte de routes.

Avec ça se termine les commandes pour configurer BGP de manière simple néanmoins pour assurer qu'il n'y'aura pas de problème de routage entre le protocole BGP et OSPF on doit s'assurer que la redistribution des routes entre BGP et OSPF est implémenter.

- **La redistribution des routes :**

La redistribution des routes va permettre à un routeur d'importer des routes apprises par un protocole de routage dans un autre. Par exemple, redistribuer les routes BGP dans OSPF et vice versa.

A travers cette redistribution on peut garantir une communication fluide entre les réseaux internes et externes, tout en maintenant une flexibilité et une résilience optimales du réseau.

- Cette redistribution se fait à travers la commande suivante :

<b>Router ospf [OSPF_Process_ID] Redistribute bgp [BGP_AS_Number] subnets</b>
---

- **Bgp [BGP\_AS\_Number]** spécifie le numéro de l'AS (Autonomous System) de BGP dont les routes seront redistribuées.
- **Subnets** indique que les sous-réseaux (routes spécifiques, pas seulement les routes résumées) seront redistribués. Sans ce mot-clé, seules les routes de réseau majeures (classfull) seraient redistribuées.

## V. Analyse des résultats obtenus

On a proposé 2 scenarios pour bien étudier nos résultats :

- ❖ Le premier scenario étant d'établir une communication entre les différents sites de l'entreprise A et voir comment nos paquets sortent du réseau privé pour aller vers les autres sites, à travers ce scenario on pourra voir et analyser comment le protocole HSRP STP et EtherChannel agissent pour rendre notre réseau plus performant et comment les données des différents départements (VLANs) utilisent le protocole de routage dynamique OSPF pour pouvoir parcourir le réseau pour arriver au serveur web de l'entreprise.
- ❖ Le deuxième scenario va être d'établir une communication entre un département de l'entreprise A avec un autre département de l'entreprise B grâce à ce scenario on pourra voir comment nos paquets parcourent le réseau en utilisant le protocole BGP pour aller d'un AS vers un autre.

### A. Scénario 1 : Communication interne entre les différents sites de l'entreprise A

#### Objectif

Établir une communication entre les différents sites de l'entreprise A et analyser comment les paquets sortent du réseau privé pour atteindre les autres sites.

Pour arriver à faire ça on va tout d'abord commencer par pinger du PC 1-1 (PC1-sites x) présent dans le vlan 40 area 1 avec une adresse 172.17.40.3 vers le PC 2-2 (172.16.30.3) et le PC 3-3 (172.15.20.3) présent dans le site 2 et 3 à l'intérieur du vlan 30 et 20 respectivement.

#### ➤ Figure qui montre les Ping :

```
C:\>ping 172.16.30.3

Pinging 172.16.30.3 with 32 bytes of data:

Reply from 172.16.30.3: bytes=32 time=2ms TTL=124
Reply from 172.16.30.3: bytes=32 time=3ms TTL=124
Reply from 172.16.30.3: bytes=32 time=1ms TTL=124
Reply from 172.16.30.3: bytes=32 time=2ms TTL=124

Ping statistics for 172.16.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

Ping PC 1-1 vers  
PC 2-2

```
C:\>ping 172.15.20.3

Pinging 172.15.20.3 with 32 bytes of data:

Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=24ms TTL=123
Reply from 172.15.20.3: bytes=32 time=10ms TTL=123

Ping statistics for 172.15.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 24ms, Average = 10ms

C:\>
```

Ping PC 1-1 vers  
PC 3-3

Comme le montre le résultat la communication a été établie sans problème ce qui prouve que notre routage OSPF marche à merveille et donc ya connectivité entre les différents sites de l'entreprise A, maintenant pour pouvoir voir comment les paquets arrivent à destination on va utiliser la commande trace route et on verra par quelle passerelle les données passent pour arriver à destination.

```
C:\>tracert 172.16.30.3

Tracing route to 172.16.30.3 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  172.17.40.1
  1  1 ms  0 ms  0 ms  210.200.200.1
  2  2 ms  11 ms  7 ms  20.10.12.2
  3  1 ms  1 ms  0 ms  211.200.100.2
  4  *      *      6 ms  172.16.30.3

Trace complete.
```

Sans VPN

Tracert du PC 1-1  
vers PC 2-2

Gateway du MLS 1

Comme le résultat du traceroute le montre lors de sa sortie nos données sortent par la passerelle 172.17.40.1 du MLS 1 pour aller vers l'interface 210.200.100.1 et 20.10.12.2 ensuite elle prend le Gateway 211.200.200.2 pour arriver finalement à destination le PC 2-2.

On a configuré notre protocole HSRP de façon à ce que les données du vlan 10 et 20 puissent sortir à travers le MLS 2 avec l'adresse Gateway 172.17.40.2 tandis que pour les vlan 30 et 40 on a configuré le HSRP de façon à ce que les données puissent sortir du MLS 1 avec le Gateway 172.17.40.1 et c'est exactement ce qu'on remarque à travers la commande tracert vu qu'on a pingé à partir du PC1-1 qui est présent dans le vlan 40 on peut aussi confirmer sa en visualisant le résultat du protocole HSRP à travers la commande « **sh standby brief** » :

#### ➤ Exemple du résultat du protocole HSRP dans MLS 1 :

```
Multilayer Switch1
S1-1#sh standby brief
          P indicates configured to preempt.
+-----+-----+-----+-----+-----+-----+-----+
Interface Grp  Pri  P State   Active            Standby            Virtual IP
-----
Vl10      10   100  P Standby 172.17.10.2       local              172.17.10.254
Vl20      20   100  P Standby 172.17.20.2       local              172.17.20.254
Vl30      30   110  P Active  local             172.17.30.2        172.17.30.254
Vl40      40   110  P Active  local             172.17.40.2        172.17.40.254
S1-1#
```

Active localement  
pour les vlan 30, 40

Standby localement  
pour les vlan 10, 20  
Et active pour ces  
deux Vlan dans le  
MLS 2

Comme le montre le résultat l'implémentation a été un succès et donc on bien pu avoir un partage de données ce qui peut améliorer le trafic lors de la sortie des données du réseau privé du site 1 vers l'extérieur.



Et enfin on arrive bien à remarquer que l'implémentation du VPN marche aussi à travers le tracer :

Tracert du PC 1-1  
vers PC 2-2

```
C:\>tracert 172.16.30.3

Tracing route to 172.16.30.3 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    172.17.40.1
  1  0 ms    0 ms    0 ms    210.200.200.1
  2  1 ms    1 ms    1 ms    10.0.0.2
  3  1 ms    2 ms    1 ms    211.200.100.2
  4  2 ms    1 ms    1 ms    172.16.30.3

Trace complete.

C:\>
```

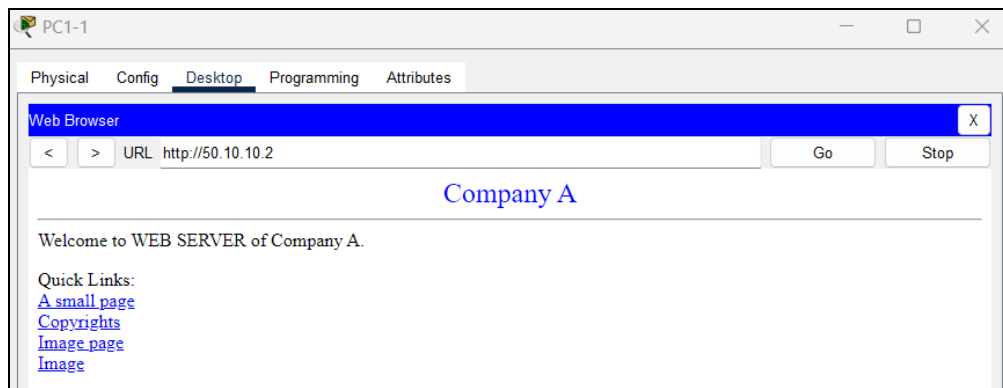
Notre réseau interne marche à merveille sans aucun problème et à travers le protocole OSPF le routage a été un succès on peut le vérifier à travers la commande **sh ip route ospf**.

```
R1#show ip route os
R1#show ip route ospf
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O   10.10.0.0 [110/2000] via 10.0.0.2, 00:00:30, Tunnel1
    20.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O   20.10.34.0 [110/128] via 20.10.14.4, 00:14:30, Serial0/0/1
O   50.0.0.0 [110/1001] via 10.0.0.2, 00:03:05, Tunnel1
    172.15.0.0/24 is subnetted, 4 subnets
O IA 172.15.10.0 [110/2002] via 10.0.0.2, 00:00:30, Tunnel1
O IA 172.15.20.0 [110/2002] via 10.0.0.2, 00:00:30, Tunnel1
O IA 172.15.30.0 [110/2002] via 10.0.0.2, 00:00:30, Tunnel1
O IA 172.15.40.0 [110/2002] via 10.0.0.2, 00:00:30, Tunnel1
    172.16.0.0/24 is subnetted, 4 subnets
O   172.16.10.0 [110/1002] via 10.0.0.2, 00:03:05, Tunnel1
O   172.16.20.0 [110/1002] via 10.0.0.2, 00:03:05, Tunnel1
O   172.16.30.0 [110/1002] via 10.0.0.2, 00:03:05, Tunnel1
O   172.16.40.0 [110/1002] via 10.0.0.2, 00:03:05, Tunnel1
    172.17.0.0/24 is subnetted, 4 subnets
O   172.17.10.0 [110/2] via 210.200.200.2, 00:10:45, GigabitEthernet0/1
[110/2] via 210.200.100.2, 00:10:45, GigabitEthernet0/0
O   172.17.20.0 [110/2] via 210.200.200.2, 00:12:55, GigabitEthernet0/1
[110/2] via 210.200.100.2, 00:12:55, GigabitEthernet0/0
O   172.17.30.0 [110/2] via 210.200.200.2, 00:12:55, GigabitEthernet0/1
[110/2] via 210.200.100.2, 00:12:55, GigabitEthernet0/0
O   172.17.40.0 [110/2] via 210.200.200.2, 00:12:55, GigabitEthernet0/1
[110/2] via 210.200.100.2, 00:12:55, GigabitEthernet0/0
E E2 192.168.10.0 [110/20] via 20.10.14.4, 00:13:49, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.168.20.0 [110/20] via 20.10.14.4, 00:13:49, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.168.30.0 [110/20] via 20.10.14.4, 00:13:49, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.168.40.0 [110/20] via 20.10.14.4, 00:13:49, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.169.10.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.169.20.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.169.30.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.169.40.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.170.10.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.170.20.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
O E2 192.170.30.0 [110/20] via 20.10.14.4, 00:13:39, Serial0/0/1
[110/20] via 10.0.0.2, 00:00:30, Tunnel1
```

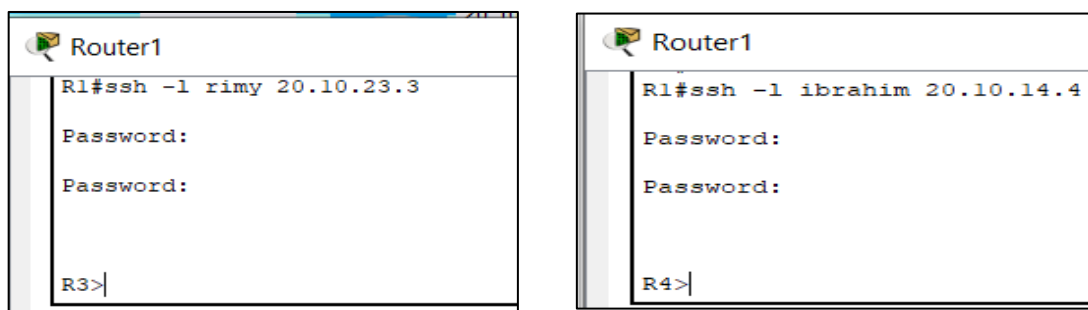
- **Les routes intra-aires (O)** montrent que le routeur 1 appartient directement à l'aire backbone (aire 0) et utilise principalement les interfaces Serial0/0/0 et Serial0/0/1 pour ses connexions internes.
- **Les routes inter-aires (IA)** démontrent une communication avec d'autres aires (1, 2, 3) OSPF connectées au backbone, ce qui est essentiel pour maintenir une connectivité fluide à travers tout le domaine OSPF.

Enfin, les routes externes de type 2 (E2) indiquent des réseaux externes introduits dans le domaine OSPF, avec des chemins spécifiques via l'interface Serial0/0/1 pour atteindre ces réseaux externes. Cette table de routage illustre la robustesse du réseau, assurant une haute disponibilité et une tolérance aux pannes grâce à une redondance efficace et une accessibilité étendue à divers sous-réseaux internes et externes.

On peut aussi communiquer avec le serveur web de l'entreprise A à partir du PC1-1 en lançant une requête HTTP :



Comme l'indique le résultat on a bien pu accéder au server web présent sur l'entreprise A. Comme ya communication entre nos différents sites de **l'entreprise A** on peut aussi vérifier si le protocole de sécurité d'accès SSH marche en essayant de se connecter à un routeur présent dans un autre site à travers le routeur 1 présent sur le site 1.

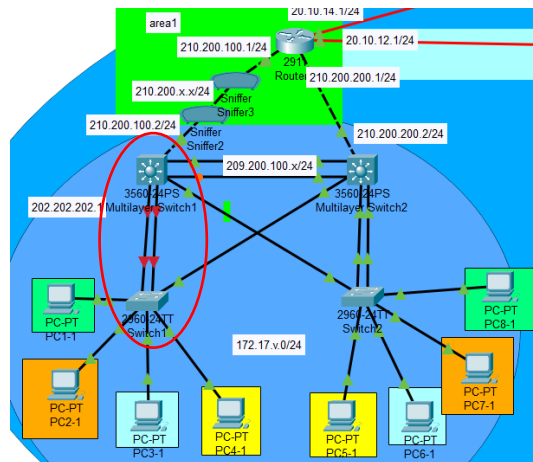


La connexion SSH réussie indique que le protocole de sécurité fonctionne correctement pour l'accès à distance.

Afin de tester l'efficacité du protocole HSRP implémenté dans notre topologie interne on a fait en sorte que le câble qui relie le MLS 1 avec le switch layer 2 du site 1 tombe en panne puis on a émulé le scénario 1 qui est l'établissement d'une communication entre le PC1-1 du site 1 et le PC 3-3 du site 3.

- **Déconnexion du Câble** : Nous avons physiquement déconnecté le câble reliant le MLS 1 au switch Layer 2 du site 1.

Déconnectement  
du câble qui relie  
le MLS1 au  
switch layer 2



- **Vérification du Trafic** : Nous avons effectué un traceroute et un Ping entre les PC concernés pour vérifier le chemin emprunté par les données.

```

C:\>tracert 172.15.20.3

Tracing route to 172.15.20.3 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    172.17.40.2
  1  0 ms    *      0 ms    210.200.200.1
  2  3 ms    1 ms    6 ms    20.10.12.2
  3  3 ms    0 ms    0 ms    20.10.23.3
  4  6 ms    1 ms    17 ms   212.200.100.2
  5  1 ms    *      2 ms    172.15.20.3

Trace complete.

C:\>ping 172.15.20.3

Pinging 172.15.20.3 with 32 bytes of data:

Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=44ms TTL=123
Reply from 172.15.20.3: bytes=32 time=3ms TTL=123
Reply from 172.15.20.3: bytes=32 time=6ms TTL=123

Ping statistics for 172.15.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 44ms, Average = 14ms
  
```

Gateway  
du MLS 2

Ping et traceroute entre  
PC1-1 et PC 3-3

Comme le résultat l'indique lorsque notre câble est panne nos données des différents VLANs (département) vont sortir à travers l'autre MLS (MLS 2) automatiquement ce qui prouve que le HSRP marche bien et donc que notre réseau interne est capable de détecter une panne de liaison et de rerouter le trafic via un chemin alternatif sans être interrompu.

Grâce à ces étapes de vérifications, on a pu établir que notre réseau interne fonctionne efficacement avec OSPF pour le routage dynamique, HSRP pour la redondance des passerelles, EtherChannel pour l'augmentation de la bande passante et la résilience, et les autres vérifications confirment l'accès sécurisé et la bonne communication entre les différents sites de l'entreprise.

## B. Scénario 2 : Communication inter-entreprises (entreprise A et entreprise B)

### Objectif

Établir une communication entre un département de l'entreprise A et un département de l'entreprise B en utilisant BGP pour gérer la communication entre différents AS.

Afin de commencer l'analyse de notre scénario on va faire un Ping entre le PC 1-1 du site 1 de l'entreprise A avec (le PC 1-3 du site 3 et le PC1-1 du site 1 et le PC2-2 du site 2) de l'entreprise B.

PC1-1

Physical Config Desktop Programming Attributes

Command Prompt

C:\>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:

Reply from 192.168.40.3: bytes=32 time=15ms TTL=122  
Reply from 192.168.40.3: bytes=32 time=6ms TTL=122  
Reply from 192.168.40.3: bytes=32 time=6ms TTL=122  
Reply from 192.168.40.3: bytes=32 time=18ms TTL=122

Ping statistics for 192.168.40.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 6ms, Maximum = 18ms, Average = 11ms

C:\>ping 192.170.20.3

Pinging 192.170.20.3 with 32 bytes of data:

Reply from 192.170.20.3: bytes=32 time=36ms TTL=120  
Reply from 192.170.20.3: bytes=32 time=10ms TTL=120  
Reply from 192.170.20.3: bytes=32 time=14ms TTL=120  
Reply from 192.170.20.3: bytes=32 time=9ms TTL=120

Ping statistics for 192.170.20.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 9ms, Maximum = 36ms, Average = 17ms

C:\>ping 192.169.30.3

Pinging 192.169.30.3 with 32 bytes of data:

Reply from 192.169.30.3: bytes=32 time=25ms TTL=121  
Reply from 192.169.30.3: bytes=32 time=5ms TTL=121  
Reply from 192.169.30.3: bytes=32 time=14ms TTL=121  
Reply from 192.169.30.3: bytes=32 time=6ms TTL=121

Ping statistics for 192.169.30.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 5ms, Maximum = 25ms, Average = 12ms

C:\>|

Ping entre PC1-1 et PC1-1/B

Ping entre PC1-1 et PC1-3/B

Ping entre PC1-1 et PC2-2/B

Comme le montre le résultat de notre Ping la connectivité entre les deux entreprises A et B est un succès ce qui prouve que nos routes bgp implémenter précédemment fonctionne et que la redistribution des routes OSPF fonctionne.

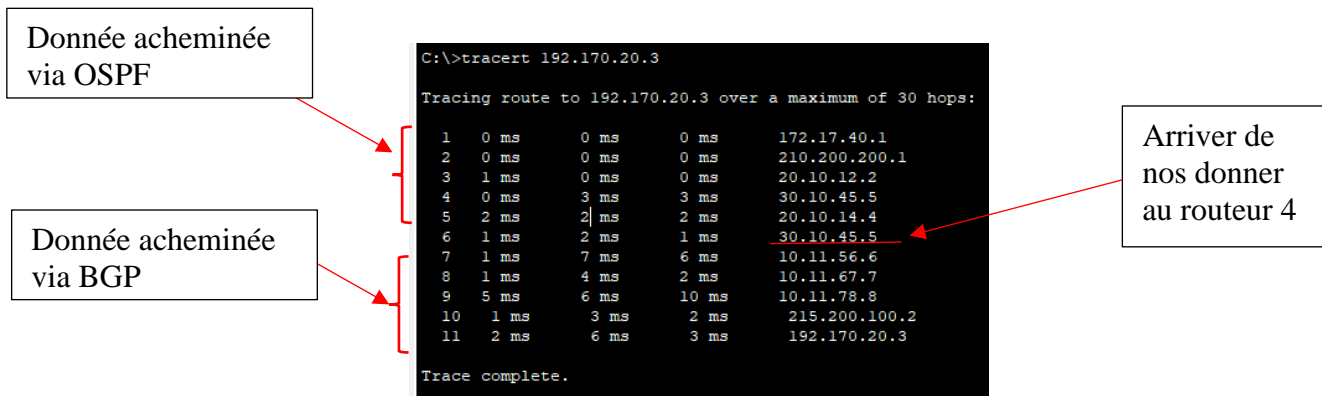
On peut aussi vérifier les implémentations des routes à travers la commande « **sh ip bgp** » :

```
R4#sh ip bgp
BGP table version is 27, local router ID is 30.10.45.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop        Metric LocPrf Weight Path
*> 50.0.0.0/8      0.0.0.0                0 0 0 100 i
*> 172.15.10.0/24  0.0.0.0                0 0 0 100 i
*> 172.15.20.0/24  0.0.0.0                0 0 0 100 i
*> 172.15.30.0/24  0.0.0.0                0 0 0 100 i
*> 172.15.40.0/24  0.0.0.0                0 0 0 100 i
*> 172.16.10.0/24  0.0.0.0                0 0 0 100 i
*> 172.16.20.0/24  0.0.0.0                0 0 0 100 i
*> 172.16.30.0/24  0.0.0.0                0 0 0 100 i
*> 172.16.40.0/24  0.0.0.0                0 0 0 100 i
*> 172.17.10.0/24  0.0.0.0                0 0 0 100 i
*> 172.17.20.0/24  0.0.0.0                0 0 0 100 i
*> 172.17.30.0/24  0.0.0.0                0 0 0 100 i
*> 172.17.40.0/24  0.0.0.0                0 0 0 100 i
*> 192.168.10.0/24 30.10.45.5             0 0 0 200 i
*> 192.168.20.0/24 30.10.45.5             0 0 0 200 i
*> 192.168.30.0/24 30.10.45.5             0 0 0 200 i
*> 192.168.40.0/24 30.10.45.5             0 0 0 200 i
*> 192.169.10.0/24 30.10.45.5             0 0 0 200 i
*> 192.169.20.0/24 30.10.45.5             0 0 0 200 i
*> 192.169.30.0/24 30.10.45.5             0 0 0 200 i
*> 192.169.40.0/24 30.10.45.5             0 0 0 200 i
*> 192.170.10.0/24 30.10.45.5             0 0 0 200 i
*> 192.170.20.0/24 30.10.45.5             0 0 0 200 i
*> 192.170.30.0/24 30.10.45.5             0 0 0 200 i
*> 192.170.40.0/24 30.10.45.5             0 0 0 200 i
*> 213.200.50.0/24 30.10.45.5             0 0 0 200 i
```

Comme le résultat de la commande l'indique le router 4 présents dans l'entreprise A connaît belle et bien les réseaux de l'entreprise B ce qui confirme également que les routes BGP mises en place entre les deux entreprises sont opérationnelles. BGP est essentiel pour la communication entre différents systèmes autonomes (AS), et son bon fonctionnement est crucial pour assurer une connectivité inter-entreprises stable et efficace.

Pour approfondir nos tests on peut utiliser traceroute pour pouvoir voir comment nos paquets évoluent pour arriver à destination :



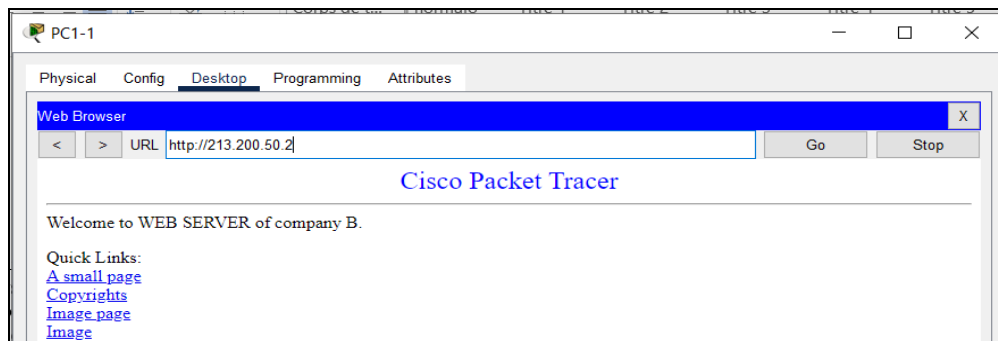
Comme le résultat de la commande l'indique lorsque les données sont envoyées du PC 1-1 sortent du réseau interne et après avoir été routé à travers le protocole dynamique OSPF pour arriver au routeur 4 nos données sont routées à travers le protocole BGP pour aller à destination.

Cette analyse révèle que les données sont d'abord acheminées via OSPF à l'intérieur de chaque entreprise, puis via BGP pour atteindre l'autre entreprise. Cette observation souligne l'importance de la coopération entre OSPF et BGP pour une connectivité inter-entreprise efficace et démontre que la redistribution des paquets entre OSPF et BGP est réussie.

BGP Open															
0                     8                     24                     Bits															
Version:4				AS:100								HT:180			
				ID:503983364											
				Length				Optional Parameter(VARIABLE LENGTH):0							

Des Sniffers ont été déployés entre les routeurs 4 et 5 pour capturer les paquets échangés. L'analyse visuelle des paquets a confirmé que la communication s'effectue correctement via les protocoles BGP et OSPF, renforçant ainsi les résultats précédents. De plus, cette capture a permis de vérifier la stabilité du trafic et l'absence de perturbation ou de perte de données.

Comme la communication entre les deux entreprises est réussie on peut aussi voir qu'on peut accéder au serveur web de l'entreprise B à travers l'entreprise A en faisant une requête HTTP depuis notre PC1-1 présent sur l'entreprise A vers le serveur web de l'entreprise B comme le montre le résultat suivant :



Comme le résultat l'indique la connexion au serveur web est réussie, démontrant ainsi une communication opérationnelle entre les serveurs des deux entreprises.

Cette analyse approfondie confirme le succès de la mise en place de la communication inter-entreprises entre les départements des entreprises A et B, avec une configuration BGP efficace assurant une connectivité stable et fiable.

## VI. Problèmes rencontrés

### ➤ Problèmes rencontrés et solutions apportées :

Lors de la conception de notre réseau complexe, nous avons rencontré plusieurs limitations inhérentes à l'utilisation de Cisco Packet Tracer. Ces limitations incluent des contraintes sur le nombre de périphériques pris en charge, des fonctionnalités de protocole incomplètes, et des capacités de simulation restreintes par rapport à un environnement de production réel. Par exemple, certaines fonctionnalités avancées de BGP et des mécanismes de sécurité réseau ne sont pas entièrement implémentés dans Packet Tracer, ce qui complique l'évaluation de la performance et de la sécurité du réseau. Pour pallier ces limitations nous avons simplifié notre conception initiale pour correspondre aux capacités de Packet Tracer.

Au cours de notre configuration initiale nous avons rencontré plusieurs problèmes parmi elles les routeurs configurés avec HSRP qui ne prenaient pas le rôle attendu (actif/standby), causant des interruptions de service lors des basculements. Pour résoudre ce problème, nous avons ajusté les priorités HSRP et activé la préemption afin de garantir que le routeur avec la plus haute priorité prenait toujours le rôle actif ainsi nous avons pu corriger ce problème notamment à travers les tests sur les basculements en simulant des pannes pour vérifier que HSRP fonctionnait correctement.

Un autre défi était la redistribution des routes entre OSPF et BGP, les routes apprises via OSPF n'étaient pas redistribuées dans BGP, ce qui empêchait la communication entre les départements des entreprises A et B.

Pour résoudre ce problème, nous avons configuré la redistribution des routes OSPF dans BGP dans le processus OSPF. Nous avons également configuré la redistribution inverse pour s'assurer que les routes BGP étaient connues par OSPF, assurant ainsi une communication fluide entre les AS.

Grâce à la résolution méthodique de ces problèmes, nous avons pu assurer une configuration réseau robuste et performante, permettant une communication fluide et sécurisée entre les différents sites et départements de l'entreprise. Chaque problème rencontré a permis d'améliorer la résilience et la performance de notre infrastructure, garantissant un réseau fiable pour les opérations quotidiennes.

## VII. Conclusion

Ce projet nous a permis de mettre en pratique nos connaissances en réseaux, en particulier pour la conception, la configuration et la gestion d'un réseau complexe utilisant les protocoles BGP et OSPF.

Nous avons conçu une topologie réseau intégrant deux entreprises situées dans des pays différents, reliées par un réseau WAN. La connectivité robuste et sécurisée a été assurée grâce à l'utilisation des protocoles BGP pour la connectivité externe et OSPF pour le routage interne. Des mécanismes de redondance comme HSRP, STP, EtherChannel, VPN et PortFast ont été mis en place pour garantir la disponibilité et l'optimisation des performances du réseau.

Les tests de connectivité, incluant des pings et des tracert entre différents sites et départements, ont confirmé le bon fonctionnement de notre configuration. La résilience du réseau a été démontrée par la gestion des pannes et des basculements automatiques des routes. La redistribution des routes entre OSPF et BGP a également été configurée pour assurer une communication fluide entre les entreprises A et B.

Ce projet nous a permis d'acquérir une expérience pratique significative en configuration et gestion de réseaux complexes. Nous avons renforcé notre capacité à travailler en équipe, à documenter nos configurations, et à résoudre des problèmes techniques complexes. De plus, ce projet a approfondi notre compréhension des concepts théoriques des réseaux et nous a fourni les compétences nécessaires pour gérer des réseaux d'entreprise de taille moyenne à grande. Chaque défi rencontré, qu'il s'agisse de limitations de Packet Tracer ou de problèmes de configuration spécifiques, nous a permis d'améliorer notre méthodologie de travail et de garantir une infrastructure réseau fiable et performante.

## VIII. Annexes

### 1) Détails du Plan d'Adressage

On trouvera les détails de notre plan d'adressage dans les tableaux suivant :

Nom du routeur	Interface G0/0	Interface G0/1	Interface S0/0	Interface S0/1	Area
Routeur R1	210.200.100.1/24	210.200.200.1/24	20.10.12.1/24	20.10.14.1/24	1
Routeur R2	211.200.100.1/24	211.200.200.1/24	20.10.12.2/24	20.10.23.2/24	0
Routeur R3	212.200.100.1/24	212.200.200.1/24	20.10.34.3/24	20.10.23.3/24	2

Nom du routeur	Interface G0/0	Interface G0/1	Interface S0/0	Interface S0/1	Area
Routeur R6	213.200.100.1/24	213.200.200.1/24	20.10.67.6/24	20.10.56.6/24	1
Routeur R7	214.200.100.1/24	214.200.200.1/24	10.11.67.7/24	10.11.78.7/24	0
Routeur R8	215.200.100.1/24	215.200.200.1/24	20.10.78.8/24	20.10.58.8/24	2

Nom du routeur	Interface G0/1	Interface S0/0	Interface S0/1	Area
Routeur R4	30.10.45.4/24	20.10.14.4/24	20.10.34.4/24	3
Routeur R5	30.10.45.5/24	10.11.56.5/24	10.11.58.5/24	3

#### Entreprise A :

Chaque site de l'entreprise A possède deux MLS, avec les adresses suivantes :

- MLS1.1 – MLS 1.2 : 209.200.100.x/24
- MLS 2.1 – MLS 2.2 : 209.200.200.x/24
- MLS 3.1 - MLS 3.2 : 209.200.250.x/24

Pour les réseaux privés et les PCS (Personal Communication Services), les adresses sont divisées par zones (areas) et VLANs :

- Area 0: 172.17.v.0/24 (VLANs: 10, 20, 30, 40)
- Area 1: 172.16.v.0/24 (VLANs: 10, 20, 30, 40)
- Area 2: 172.15.v.0/24 (VLANs: 10, 20, 30, 40)

#### Entreprise B :

L'entreprise B suit une structure similaire avec des plages d'adresses différentes :

- MLS1.1 – MLS 1.2 : 204.200.100.x/24
- MLS 2.1 – MLS 2.2 : 204.200.200.x/24
- MLS 3.1 - MLS 3.2 : 204.200.250.x/24

Les réseaux privés et les PCS pour l'entreprise B sont également organisés par zones et VLANs :



- Area 0: 192.169.v.0/24 (VLANs: 10, 20, 30, 40)
- Area 1: 192.168.v.0/24 (VLANs: 10, 20, 30, 40)
- Area 32: 192.170.v.0/24 (VLANs: 10, 20, 30, 40)

## 2) Configurations de la topologie

Voici les étapes à suivre et les commandes à exécuter pour configurer la topologie proposée dans notre projet.

### Configuration des VLANs

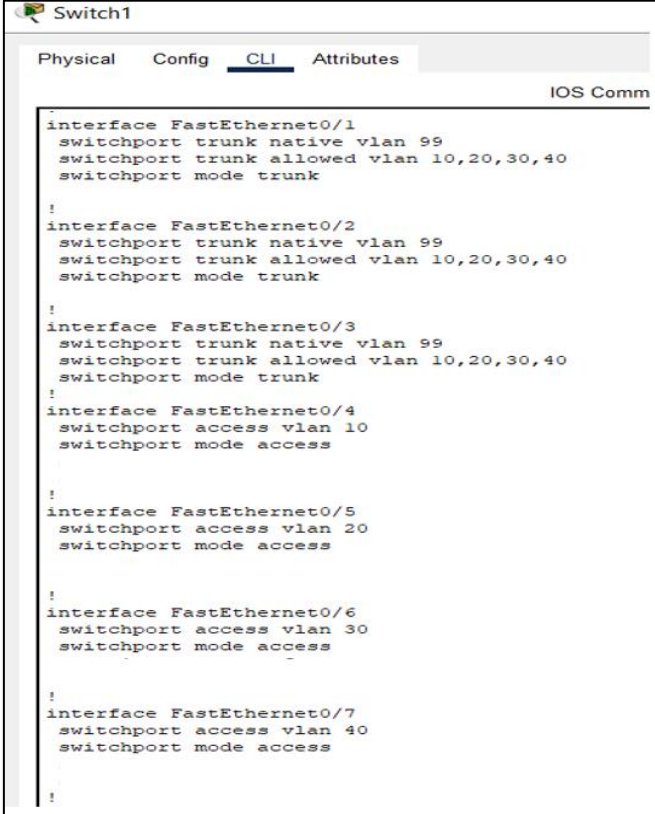
Dans chaque site, nous allons d'abord commencer notre configuration en créant les VLANs sur les switches de niveau 2 et 3. Pour ce faire, On a exécuté les commandes suivantes.

#### ➤ Exemple de l'Implémentation VLANs.

```
S1-1(config)#vlan 10  
S1-1(config)#vlan 20  
S1-1(config)#vlan 30  
S1-1(config)#vlan 40
```

Après avoir créé les VLANs correspondant aux quatre départements de notre topologie sur chaque switch de niveau 2 et 3, on a configuré les liens d'accès entre les switches et les terminaux, ainsi que les liens trunk entre les switches de niveau 2 et 3, afin de permettre la communication inter-VLAN.

#### ➤ Exemple de la configuration des liens trunk et Access sur le switch 1 du site 1.



```
Switch1  
Physical Config CLI Attributes  
IOS Comm  
interface FastEthernet0/1  
switchport trunk native vlan 99  
switchport trunk allowed vlan 10,20,30,40  
switchport mode trunk  
!  
interface FastEthernet0/2  
switchport trunk native vlan 99  
switchport trunk allowed vlan 10,20,30,40  
switchport mode trunk  
!  
interface FastEthernet0/3  
switchport trunk native vlan 99  
switchport trunk allowed vlan 10,20,30,40  
switchport mode trunk  
!  
interface FastEthernet0/4  
switchport access vlan 10  
switchport mode access  
!  
interface FastEthernet0/5  
switchport access vlan 20  
switchport mode access  
!  
interface FastEthernet0/6  
switchport access vlan 30  
switchport mode access  
!  
interface FastEthernet0/7  
switchport access vlan 40  
switchport mode access  
!
```

## Configuration de l'EtherChannel

Après avoir terminé la configuration des VLANs, on a ensuite configuré les liens EtherChannel pour agréger plusieurs liens physiques en un seul lien logique, ce qui a augmenté la bande passante et a fourni une redondance.

### ➤ Exemple de la configuration du EtherChannel sur le Switch 1 Site 1.

```
Int range f0/1-2
Shutdown
Channel-group 1 mode on
Int po1
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

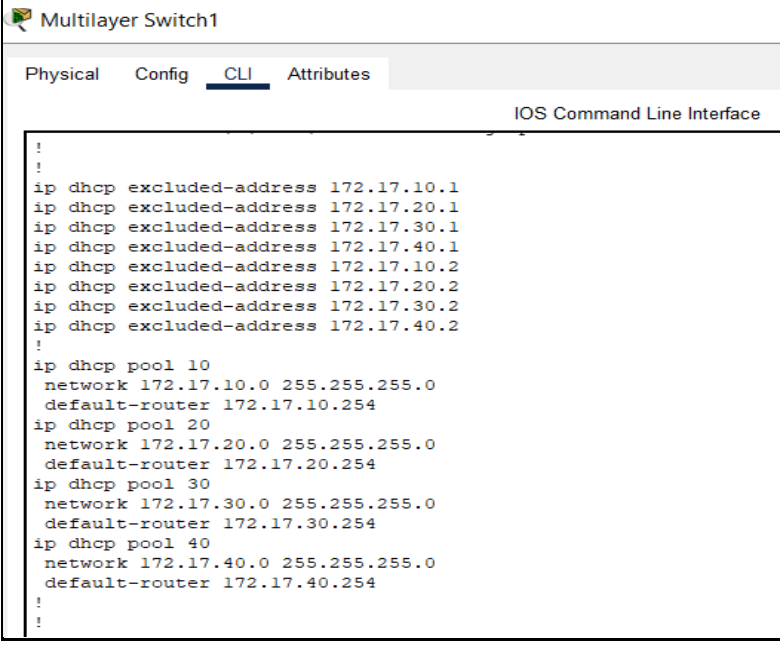
Démonstration du résultat avec la commande « **show running-config** » :

```
interface Port-channel1
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
channel-group 1 mode active|
```

## Configuration de DHCP

Maintenant que tous les liens de nos sites sont actifs, nous pouvons configurer le protocole DHCP sur nos deux switches multicouches afin d'attribuer dynamiquement les paramètres TCP/IP aux terminaux.

### ➤ Exemple de la configuration du DHCP sur Multi Switch 1.



```

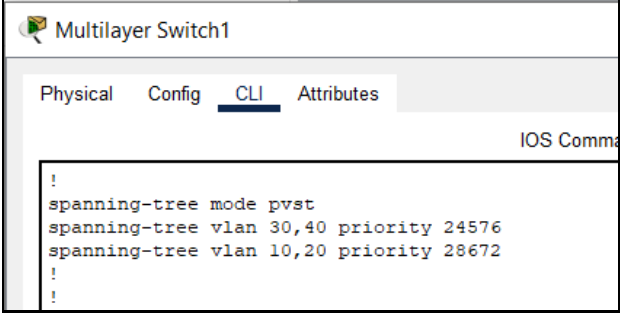
!
!
ip dhcp excluded-address 172.17.10.1
ip dhcp excluded-address 172.17.20.1
ip dhcp excluded-address 172.17.30.1
ip dhcp excluded-address 172.17.40.1
ip dhcp excluded-address 172.17.10.2
ip dhcp excluded-address 172.17.20.2
ip dhcp excluded-address 172.17.30.2
ip dhcp excluded-address 172.17.40.2
!
ip dhcp pool 10
 network 172.17.10.0 255.255.255.0
 default-router 172.17.10.254
ip dhcp pool 20
 network 172.17.20.0 255.255.255.0
 default-router 172.17.20.254
ip dhcp pool 30
 network 172.17.30.0 255.255.255.0
 default-router 172.17.30.254
ip dhcp pool 40
 network 172.17.40.0 255.255.255.0
 default-router 172.17.40.254
!
!

```

## Configuration de STP

Après avoir réussi à attribuer dynamiquement les paramètres TCP/IP aux terminaux, nous allons configurer le protocole STP afin de réduire la charge sur nos switches de couche 3 en choisissant par quelles voies les données des différents VLANs configurés précédemment vont transiter.

### ➤ Exemple de la configuration du STP sur Multi Switch 1.

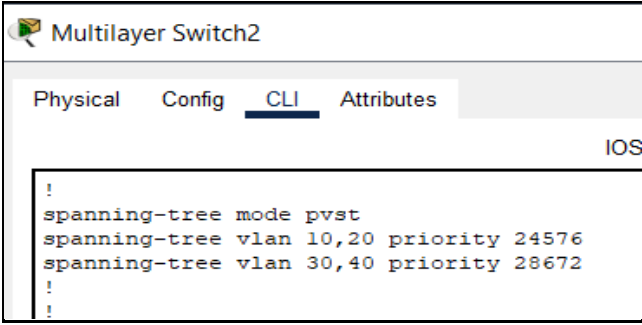


```

!
spanning-tree mode pvst
spanning-tree vlan 30,40 priority 24576
spanning-tree vlan 10,20 priority 28672
!
!

```

### ➤ Exemple de la configuration du STP sur Multi switch 2 .



```

!
spanning-tree mode pvst
spanning-tree vlan 10,20 priority 24576
spanning-tree vlan 30,40 priority 28672
!
!

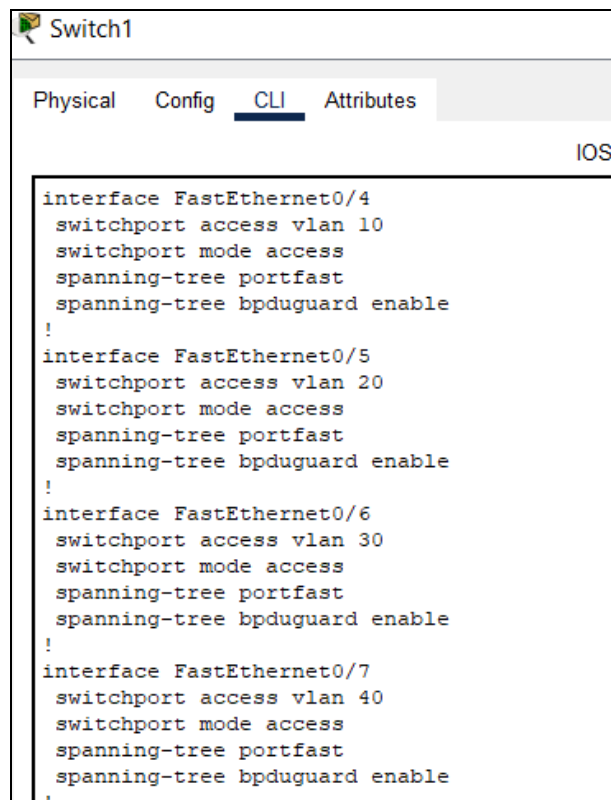
```

Après avoir terminé la configuration du protocole STP, nous configurons le PortFast sur chaque interface d'accès (interface entre PC et switch L2) afin de permettre la convergence rapide des ports d'accès.

- On peut accomplir cela grâce aux commandes suivantes :

```
S1 (config-if)#spanning-tree portfast
S1 (config-if)#spanning-tree bpduguard enable
```

- Exemple de la configuration du PortFast sur Switch 1.

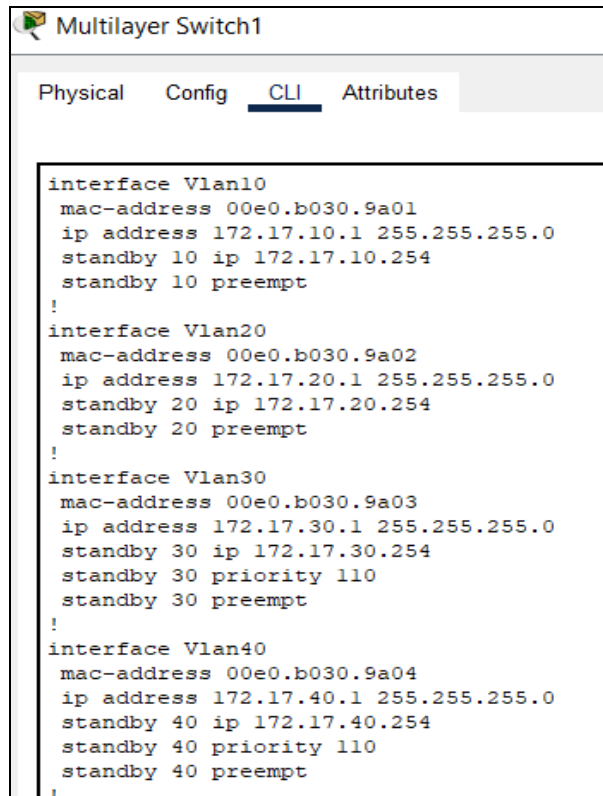


```
Switch1
Physical Config CLI Attributes
IOS
interface FastEthernet0/4
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/5
  switchport access vlan 20
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/6
  switchport access vlan 30
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface FastEthernet0/7
  switchport access vlan 40
  switchport mode access
  spanning-tree portfast
  spanning-tree bpduguard enable
!
```

## Configuration de HSRP

Maintenant que nous avons terminé les configurations précédentes, nous allons configurer HSRP pour rendre la topologie du site plus redondante et efficace contre les pannes. La configuration sera réalisée de manière que les données des VLAN 30 et 40 sortent par un switch multicouche, et les données des VLAN 10 et 20 par un autre switch multicouche.

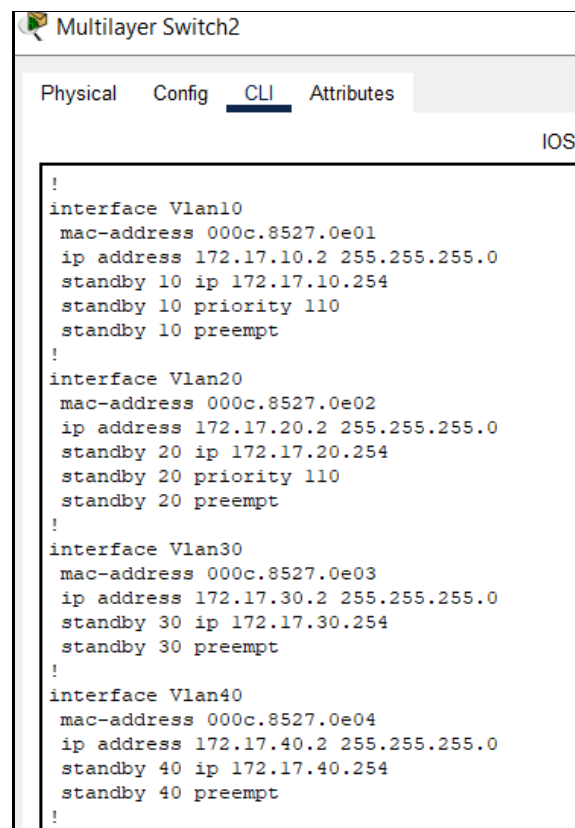
- Exemple de la configuration du HSRP sur Multi Switch 1.



The screenshot shows the configuration interface for Multilayer Switch1. The 'CLI' tab is selected, displaying the following configuration:

```
interface Vlan10
  mac-address 00e0.b030.9a01
  ip address 172.17.10.1 255.255.255.0
  standby 10 ip 172.17.10.254
  standby 10 preempt
!
interface Vlan20
  mac-address 00e0.b030.9a02
  ip address 172.17.20.1 255.255.255.0
  standby 20 ip 172.17.20.254
  standby 20 preempt
!
interface Vlan30
  mac-address 00e0.b030.9a03
  ip address 172.17.30.1 255.255.255.0
  standby 30 ip 172.17.30.254
  standby 30 priority 110
  standby 30 preempt
!
interface Vlan40
  mac-address 00e0.b030.9a04
  ip address 172.17.40.1 255.255.255.0
  standby 40 ip 172.17.40.254
  standby 40 priority 110
  standby 40 preempt
!
```

➤ Exemple de la configuration du HSRP sur Multi Switch 2.



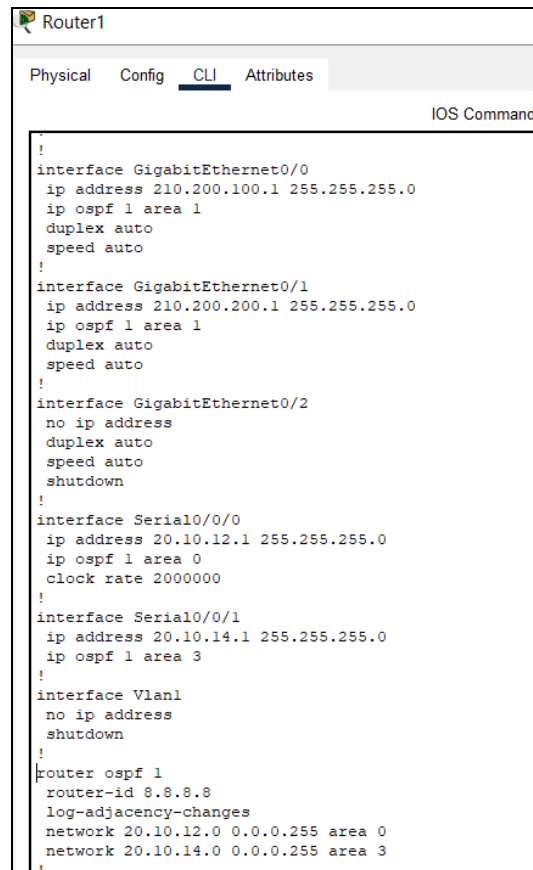
The screenshot shows the configuration interface for Multilayer Switch2. The 'CLI' tab is selected, displaying the following configuration:

```
!
interface Vlan10
  mac-address 000c.8527.0e01
  ip address 172.17.10.2 255.255.255.0
  standby 10 ip 172.17.10.254
  standby 10 priority 110
  standby 10 preempt
!
interface Vlan20
  mac-address 000c.8527.0e02
  ip address 172.17.20.2 255.255.255.0
  standby 20 ip 172.17.20.254
  standby 20 priority 110
  standby 20 preempt
!
interface Vlan30
  mac-address 000c.8527.0e03
  ip address 172.17.30.2 255.255.255.0
  standby 30 ip 172.17.30.254
  standby 30 preempt
!
interface Vlan40
  mac-address 000c.8527.0e04
  ip address 172.17.40.2 255.255.255.0
  standby 40 ip 172.17.40.254
  standby 40 preempt
!
```

## Configuration de OSPF

Maintenant que nous avons terminé la configuration des différents sites, nous pouvons commencer la configuration du routage dynamique OSPF afin de permettre la communication entre les différents sites de l'entreprise.

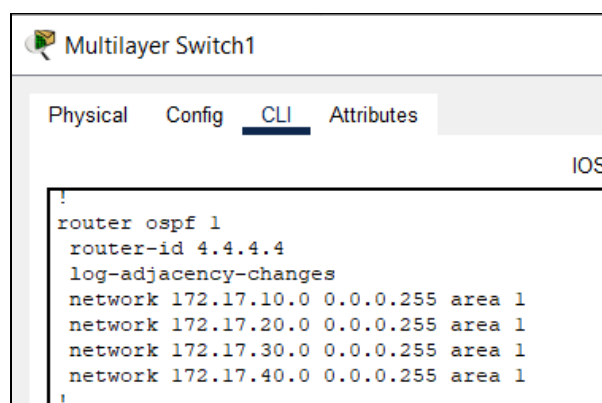
### ➤ Exemple de la configuration du OSPF sur Routeur 1.



```
Router1
Physical Config CLI Attributes
IOS Command

!
interface GigabitEthernet0/0
ip address 210.200.100.1 255.255.255.0
ip ospf 1 area 1
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 210.200.200.1 255.255.255.0
ip ospf 1 area 1
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial10/0/0
ip address 20.10.12.1 255.255.255.0
ip ospf 1 area 0
clock rate 2000000
!
interface Serial10/0/1
ip address 20.10.14.1 255.255.255.0
ip ospf 1 area 3
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 8.8.8.8
log-adjacency-changes
network 20.10.12.0 0.0.0.255 area 0
network 20.10.14.0 0.0.0.255 area 3
!
```

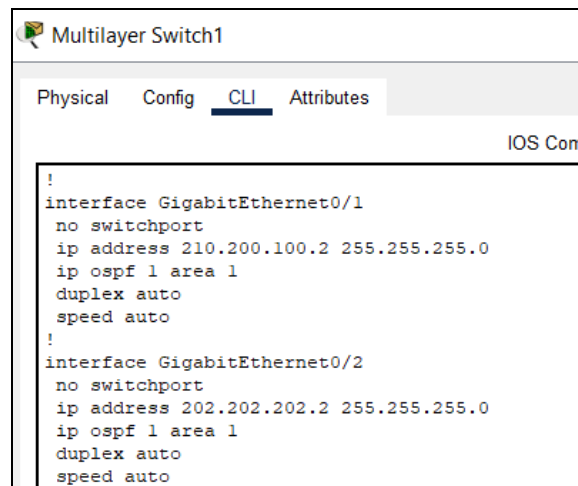
### ➤ Exemple de la configuration du OSPF sur Multi Switch 1.



```
Multilayer Switch1
Physical Config CLI Attributes
IOS

!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
network 172.17.10.0 0.0.0.255 area 1
network 172.17.20.0 0.0.0.255 area 1
network 172.17.30.0 0.0.0.255 area 1
network 172.17.40.0 0.0.0.255 area 1
!
```

➤ **Exemple de la configuration des interfaces OSPF du Multi switch 1 .**

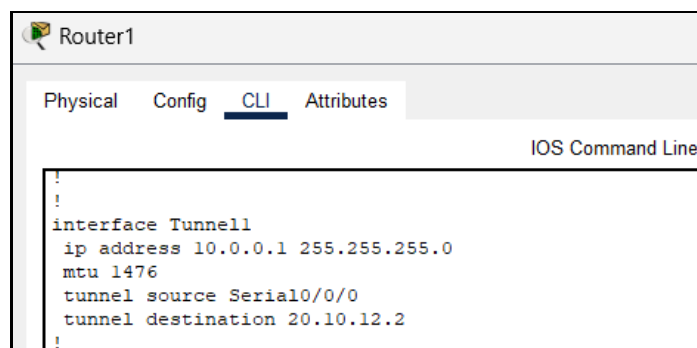
A screenshot of a network configuration window titled "Multilayer Switch1". It has tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The "CLI" tab shows the "IOS Com" (IOS Command Line) interface. The configuration text is as follows:

```
!
interface GigabitEthernet0/1
no switchport
ip address 210.200.100.2 255.255.255.0
ip ospf 1 area 1
duplex auto
speed auto
!
interface GigabitEthernet0/2
no switchport
ip address 202.202.202.2 255.255.255.0
ip ospf 1 area 1
duplex auto
speed auto
```

### **Configuration de VPN**

Après avoir implémenté le routage OSPF et afin de sécuriser davantage le routage de nos données, nous configurons des tunnels virtuels (VPN).

➤ **Exemple de la configuration du VPN su le Routeur 1 :**

A screenshot of a network configuration window titled "Router1". It has tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The "CLI" tab shows the "IOS Command Line" interface. The configuration text is as follows:

```
!
!
interface Tunnell
ip address 10.0.0.1 255.255.255.0
mtu 1476
tunnel source Serial0/0/0
tunnel destination 20.10.12.2
!
```

### **Configuration de SSH et mécanismes de sécurité**

Pour terminer la configuration interne de l'entreprise, nous configurons le protocole SSH ainsi que des mécanismes de sécurité pour renforcer l'accès à nos différents routeurs, switches Layer 2 et Layer 3.

➤ **Exemple de la configuration des mécanismes de sécurité sur le Multi switch 1.**

Ces commandes permettent d'établir un mot de passe pour accéder au mode enable.

Line console 0 Password ekko Login
--

Ces commandes permettent d'établir un mot de passe crypter pour accéder au mode privilégié.

Enable secret ekko

Ou bien les commandes suivantes :

Enable password ekko  
Service password-encryption

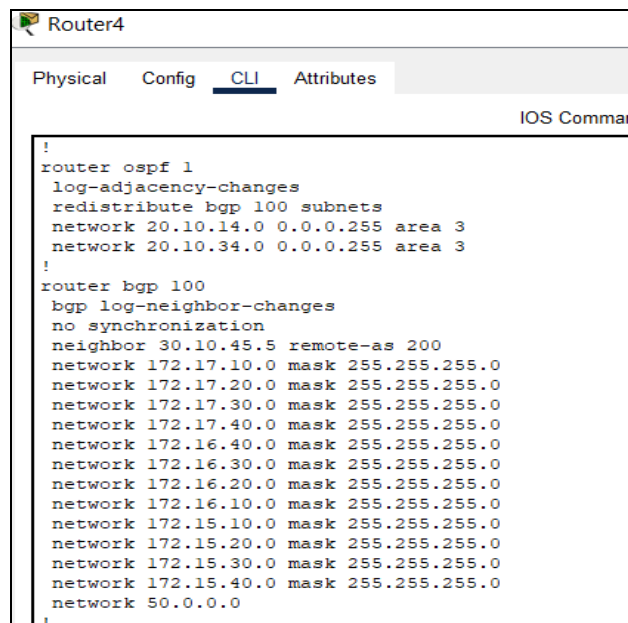
➤ **La configuration du SSH .**

**Hostname S1-1**  
**Ip domain-name xx.com**  
**Username xx secret xx**  
**Crypto key generate rsa 1025**  
**Line vty 0 15**  
**Login local**  
**Transport input ssh**

## Configuration de BGP

Avec cela, nous terminons la configuration interne de l'entreprise. Nous pouvons maintenant commencer la configuration du routage dynamique BGP, ce qui permettra de faciliter la communication entre les deux entreprises.

➤ **Exemple de la configuration du BGP sur Routeur 4 :**

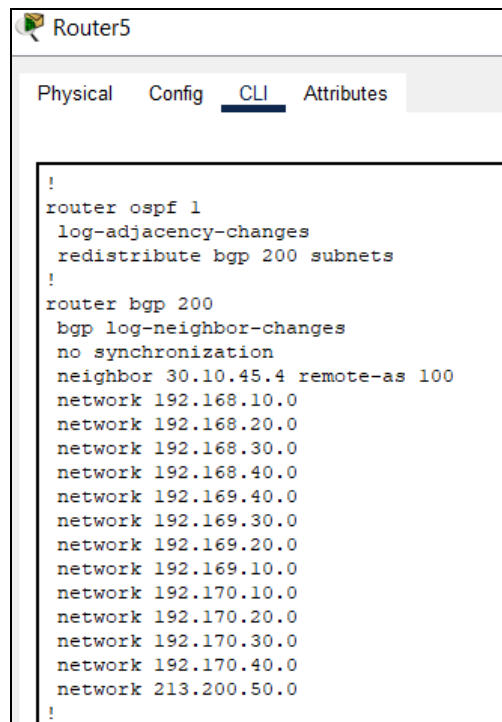


```
Router4
Physical Config CLI Attributes
IOS Command Line Editor

!
router ospf 1
 log-adjacency-changes
 redistribute bgp 100 subnets
 network 20.10.14.0 0.0.0.255 area 3
 network 20.10.34.0 0.0.0.255 area 3
!
router bgp 100
 bgp log-neighbor-changes
 no synchronization
 neighbor 30.10.45.5 remote-as 200
 network 172.17.10.0 mask 255.255.255.0
 network 172.17.20.0 mask 255.255.255.0
 network 172.17.30.0 mask 255.255.255.0
 network 172.17.40.0 mask 255.255.255.0
 network 172.16.40.0 mask 255.255.255.0
 network 172.16.30.0 mask 255.255.255.0
 network 172.16.20.0 mask 255.255.255.0
 network 172.16.10.0 mask 255.255.255.0
 network 172.15.10.0 mask 255.255.255.0
 network 172.15.20.0 mask 255.255.255.0
 network 172.15.30.0 mask 255.255.255.0
 network 172.15.40.0 mask 255.255.255.0
 network 50.0.0.0
!
```



➤ La Configuration du BGP sur le routeur 5.



```
!
router ospf 1
 log-adjacency-changes
 redistribute bgp 200 subnets
!
router bgp 200
 bgp log-neighbor-changes
 no synchronization
 neighbor 30.10.45.4 remote-as 100
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.30.0
 network 192.168.40.0
 network 192.169.40.0
 network 192.169.30.0
 network 192.169.20.0
 network 192.169.10.0
 network 192.170.10.0
 network 192.170.20.0
 network 192.170.30.0
 network 192.170.40.0
 network 213.200.50.0
!
```

Avec cela, nous concluons les commandes utilisées pour configurer notre topologie.