TP : Configuration d'un Réseau d'Entreprise avec OSPF Multi-Zone et VLANs sous Cisco Packet Tracer

Hasna Daoui

Khadija Bouargalne

November 2024

1 Introduction

Dans le cadre de ce TP, nous avons pour objectif de concevoir et configurer un réseau d'entreprise simulé en utilisant Cisco Packet Tracer, en intégrant les concepts de VLAN (Virtual LAN) et du protocole de routage OSPF (Open Shortest Path First) multi-zones. Ce réseau doit répondre aux besoins de sécurité, d'optimisation de la gestion des flux et de segmentation des départements, pour garantir une organisation efficace et sécurisée.

L'architecture cible se base sur une structure OSPF subdivisée en plusieurs zones, permettant ainsi de limiter la diffusion des routes à chaque département tout en assurant une connectivité centralisée via une zone backbone (Zone 0). L'utilisation des VLANs assure l'isolement des flux des différents départements (Administration, Comptabilité, Informatique, Ressources Humaines et Invités), et facilite la gestion de la sécurité au niveau des switches.

Ce rapport décrit en détail les étapes de configuration de chaque composant, les défis rencontrés, ainsi que les solutions adoptées pour assurer une interconnexion fluide entre les départements, tout en maintenant l'intégrité et la sécurité des données.

2 Routage

les définitions et les objectifs du routage, ainsi que les types, avantages et inconvénients des protocoles OSPF et RIP :

1. Routage

Le routageest le processus de sélection du chemin optimal pour transmettre des paquets de données à travers un réseau, d'un appareil source à une destination finale. Les routeurs, en utilisant des tables de routage et des protocoles

de routage, déterminent le meilleur chemin pour atteindre les réseaux ou sous-réseaux distants.

Objectifs du Routage

- Optimisation des chemins: Trouver le chemin le plus rapide ou le plus efficace pour la transmission de données.

- Réduction de la congestion : Éviter les chemins surchargés en redistribuant les flux de trafic.

- Fiabilité : Assurer une communication continue même en cas de panne de certains chemins grâce à des routes de secours.

- Gestion de la sécurité : Restreindre ou autoriser l'accès à certains réseaux.

Types de Routage

Il existe trois principaux types de routage : 1. Routage statique : Configuré manuellement par l'administrateur, sans mises à jour automatiques. 2. Routage dynamique : Utilise des protocoles de routage pour découvrir et adapter les chemins en fonction de l'état du réseau.

Protocoles de Routage Dynamique Les protocoles de routage dynamique sont divisés en plusieurs catégories, notamment OSPF (Open Shortest Path First) et RIP (Routing Information Protocol).

OSPF (Open Shortest Path First) OSPF est un protocole de routage de type **link-state** utilisé dans les réseaux de grande taille.

- Fonctionnement: - Les routeurs échangent des informations d'état des liens pour connaître la topologie complète du réseau.

- Utilise l'algorithme Dijkstra pour calculer les routes les plus courtes.

- Organise le réseau en zones pour réduire le volume de trafic et améliorer la performance.

- Avantages : - Convergence rapide : OSPF met à jour rapidement les routes en cas de changement dans le réseau.

- Scalabilité : Convient aux grands réseaux grâce à la structure multi-zones.

- Moins de trafic de mise à jour: Échange d'informations uniquement lorsque des changements sont détectés.

- Inconvénients : - Complexité de configuration: Plus complexe à configurer que RIP, notamment avec la gestion des zones.

- Consommation de ressources : Utilise davantage de CPU et de mémoire sur les routeurs.

RIP (Routing Information Protocol) RIP est un protocole de routage de type **distance-vector** adapté aux petits réseaux.

- Fonctionnement :

- Les routeurs échangent des informations sur la distance (nombre de sauts) pour chaque destination.

- Les mises à jour de routage sont envoyées toutes les 30 secondes.

- Avantages:

- Simplicité de configuration: Facile à mettre en œuvre pour les petits réseaux.

- Compatibilité: Bien adapté aux réseaux de petite taille sans besoin de configurations complexes.

- Inconvénients :

- Convergence lente : Prend plus de temps pour s'adapter aux changements du réseau.

- Limite de sauts : Limité à 15 sauts, ce qui le rend inefficace pour les grands réseaux.

- **Consommation de bande passante :** Envoie des mises à jour fréquentes, même si le réseau reste inchangé.

En résumé, OSPF est recommandé pour les réseaux de grande taille en raison de sa rapidité de convergence et de sa capacité de segmentation en zones. RIP, bien que plus simple, est limité aux réseaux de petite envergure en raison de sa lenteur de convergence et de sa limite de distance.

3 Objectifs du TP

L'objectif de ce TP est de concevoir et de configurer un réseau complexe pour une entreprise en utilisant Cisco Packet Tracer. Vous allez configurer le protocole de routage OSPF en le subdivisant en plusieurs zones et organiser le réseau en VLANs pour optimiser la gestion et la sécurité des données. Ce TP permettra de se familiariser avec les concepts avancés de routage et de segmentation de réseau.

4 Contexte

Une entreprise souhaite structurer son réseau en plusieurs départements, chacun ayant des exigences de sécurité et de routage spécifiques. Le réseau doit être configuré pour supporter la communication inter-département tout en garantissant l'isolement des données grâce à des VLANs.L'architecture doit permettre aux différents départements de communiquer efficacement grâce au routage OSPF, tout en ayant des zones OSPF distinctes pour segmenter le réseau. En outre, la configuration de VLANs permettra de diviser les départements et d'améliorer la sécurité interne.Topologie Réseau Divisé en Trois Zones OSPF :

• Zone 0 (Backbone) : Servira de zone principale pour la communication entre les autres zones.

• Zone 1 : Inclura les réseaux du département "Administration".

• Zone 2 : Inclura les réseaux du département "Comptabilité" et "Informatique".

• Zone 3 : Inclura le réseau du département "Ressources Humaines".

Dispositifs et Segmentation VLAN :

• Switchs d'Accès et de Distribution : Pour chaque département, prévoir un switch d'accès pour la connexion des terminaux et un switch de distribution pour l'interconnexion entre les switches d'accès.

• VLANs :

• VLAN 10 : Administration

• VLAN 20 : Comptabilité

• VLAN 30 : Informatique
• VLAN 40 : Ressources Humaines
• VLAN 50 : Invités (Guest)

Connexion Internet (simulée) :

• Un routeur supplémentaire, connectant le réseau d'entreprise à un "simulateur d'Internet". Ce routeur sera directement connecté à la zone 0.Exigences de Configuration

Configuration des VLANs :

• Créez et attribuez chaque VLAN correspondant aux départements définis ci-dessus.

• Sur chaque switch d'accès, configurez les ports pour qu'ils appartiennent aux VLANs appropriés.

• Configurez le Trunking VLAN entre les switchs d'accès et les switchs de distribution pour permettre la communication inter-VLAN au sein du réseau.

Configuration d'OSPF avec Multi-Zones :

• Activez le protocole OSPF sur tous les routeurs et configurez trois zones OSPF distinctes comme mentionné ci-dessus.

• Zone 0 doit être configurée comme le backbone et être reliée à toutes les autres zones (Zone 1, Zone 2 et Zone 3).

• Assurez-vous que chaque routeur dans une zone partage les informations de routage uniquement avec les routeurs de la même zone et le backbone.

• Configurez une authentification de routage OSPF pour sécuriser les échanges entre les routeurs dans chaque zone.

Configuration de la Communication Inter-VLAN :

• Configurez un routeur comme "Router-on-a-Stick" pour assurer le routage entre les VLANs, en définissant des sous-interfaces pour chaque VLAN.

• Assurez-vous que seuls les VLANs nécessaires peuvent communiquer entre eux selon les exigences de sécurité (ex. VLAN Invités ne peut pas accéder aux VLANs des départements).

Simulation de la Connexion Internet :

• Configurez le routeur de connexion Internet pour simuler une passerelle externe.

• Les terminaux des VLANs internes (VLAN 10 à VLAN 40) doivent pouvoir envoyer du trafic vers l'Internet simulé, mais pas les utilisateurs du VLAN 50 (Invités).Étapes de Réalisation

Étude et Conception de la Topologie :

• Analysez la topologie et déterminez les sous-réseaux IP nécessaires pour chaque VLAN.

• Créez le schéma de la topologie dans Cisco Packet Tracer en positionnant les routeurs, switchs et terminaux comme indiqué.

Configuration des Routeurs et Switches :

• Configurez les adresses IP pour chaque routeur et chaque sous-interface selon les besoins des VLANs.

• Mettez en place le routage OSPF et attribuez les routeurs aux zones OSPF correspondantes.

Vérification et Tests :

• Testez la connectivité entre les terminaux dans chaque VLAN pour vérifier l'isolement et la communication inter-départements.

• Testez la connectivité entre les différentes zones OSPF et assurez-vous que les routes sont correctement propagées.

• Vérifiez que les terminaux des VLANs internes peuvent accéder à la connexion Internet simulée et que le VLAN Invités n'y a pas accès.

5 Le schema

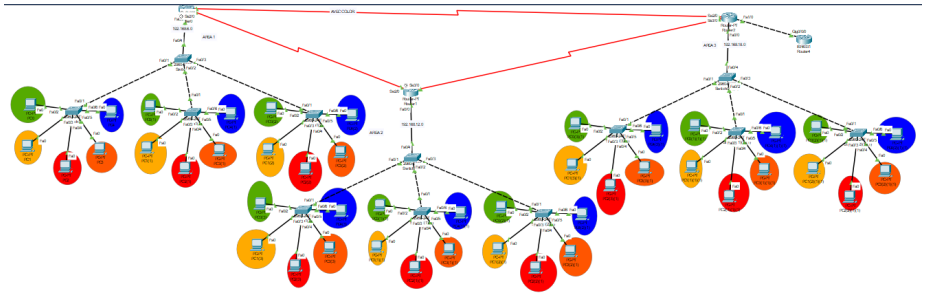

Figure 1: Caption for the figure.

6 Creation de Vlan Database

ID VLAN	Nom VLAN	Type	Statut	Couleur
2	Administration	Standard	Actif	Bleu
3	Comptabilité	Standard	Actif	Rouge
4	Informatique	Standard	Actif	Orange
5	Ressources Humaines	Standard	Actif	Jaune
6	Invités (Guest)	Standard	Actif	Vert

Table 1: Base de données VLAN

VLAN	Nom VLAN	Adresses IP
6	Client	192.168.1.1, 192.168.1.2, 192.168.1.3
5	Ressources Humaines	192.168.2.1, 192.168.2.2, 192.168.2.3
3	Comptabilité	192.168.3.1, 192.168.3.2, 192.168.3.3
4	Informatique	192.168.4.1, 192.168.4.2, 192.168.4.3
2	Administration	192.168.5.1, 192.168.5.2, 192.168.5.3

Table 2: Adresses IP par VLAN dans la Zone 1

VLAN	Nom VLAN	Adresses IP
6	Client	192.168.7.1, 192.168.7.2, 192.168.7.3
5	Ressources Humaines	192.168.8.1, 192.168.8.2, 192.168.8.3
3	Comptabilité	192.168.9.1, 192.168.9.2, 192.168.9.3
4	Informatique	192.168.10.1, 192.168.10.2, 192.168.10.3
2	Administration	192.168.11.1, 192.168.11.2, 192.168.11.3

Table 3: Adresses IP par VLAN dans la Zone 2

VLAN	Nom VLAN	Adresses IP
6	Client	192.168.13.1, 192.168.13.2, 192.168.13.3
5	Ressources Humaines	192.168.14.1, 192.168.14.2, 192.168.14.3
3	Comptabilité	192.168.15.1, 192.168.9.2, 192.168.15.3
4	Informatique	192.168.16.1, 192.168.16.2, 192.168.16.3
2	Administration	192.168.17.1, 192.168.17.2, 192.168.17.3

Table 4: Adresses IP par VLAN dans la Zone 3

7 Tables de routage de routeurs:

Table de Routage - Routeur (Zone 1)

Interface	Adresse IP	Réseau	Zone OSPF
F0/0	192.168.6.1	192.168.6.0/24	1
F0/0.2	192.168.2.1	192.168.2.0/24	1
F0/0.3	192.168.3.1	192.168.3.0/24	1
F0/0.4	192.168.4.1	192.168.4.0/24	1
F0/0.5	192.168.5.1	192.168.5.0/24	1
F0/0.6	192.168.1.1	192.168.1.0/24	1
Serial2/0	192.168.20.1	192.168.20.0/24	0
Serial3/0	192.168.19.1	192.168.19.0/24	0

Table 5: Table de routage pour le routeur en Zone 1 avec OSPF

Interface	Adresse IP	Réseau	Zone OSPF
F0/0	192.168.12.1	192.168.12.0/24	2
F0/0.2	192.168.8.1	192.168.8.0/24	2
F0/0.3	192.168.9.1	192.168.9.0/24	2
F0/0.4	192.168.10.1	192.168.10.0/24	2
F0/0.5	192.168.11.1	192.168.11.0/24	2
F0/0.6	192.168.7.1	192.168.7.0/24	2
Serial2/0	192.168.20.2	192.168.20.0/24	0
Serial3/0	192.168.21.2	192.168.21.0/24	0

Table 6: Table de routage pour le routeur en Zone 2 avec OSPF

Interface	Adresse IP	Réseau	Zone OSPF
F0/0	192.168.18.1	192.168.18.0/24	3
F0/0.2	192.168.14.1	192.168.14.0/24	3
F0/0.3	192.168.15.1	192.168.15.0/24	3
F0/0.4	192.168.16.1	192.168.16.0/24	3
F0/0.5	192.168.17.1	192.168.17.0/24	3
F0/0.6	192.168.13.1	192.168.13.0/24	3
Serial2/0	192.168.21.1	192.168.21.0/24	0
Serial3/0	192.168.19.2	192.168.19.0/24	0
F1/0	192.168.30.1	192.168.30.0/24	0

Table 7: Table de routage pour le routeur en Zone 3 avec OSPF

Interface	Adresse IP	Réseau	Zone OSPF
G0/0/0	192.168.30.2	192.168.30.0/24	0

Table 8: Table de routage pour le routeur provider en Area 0 avec OSPF

8 Exemple de configuration :

Zone 1:

1.Configuration de pc.

2.Configuration de switchs.

Switch1:

```
configure terminal
no ip domain-lookup
vlan 6
exit
vlan 2
exit
vlan 3
exit
vlan 4
exit
vlan 5
exit
interface fastEthernet 0/2
switchport mode access
switchport access vlan 6
exit
interface fastEthernet 0/3
switchport mode access
switchport access vlan 2
exit
```

interface fastEthernet 0/4
switchport mode access
switchport access vlan 3
exit
interface fastEthernet 0/5
switchport mode access
switchport access vlan 4
exit
interface fastEthernet 0/6
switchport mode access
switchport access vlan 5
exit
interface fastEthernet 0/1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit

Switch2:

configure terminal
no ip domain-lookup
vlan 6
exit
vlan 2
exit
vlan 3
exit
vlan 4
exit
vlan 5
exit
interface fastEthernet 0/2
switchport mode access
switchport access vlan 6
exit
interface fastEthernet 0/3
switchport mode access
switchport access vlan 2
exit
interface fastEthernet 0/4
switchport mode access
switchport access vlan 3
exit
interface fastEthernet 0/5

switchport mode access
switchport access vlan 4
exit
interface fastEthernet 0/6
switchport mode access
switchport access vlan 5
exit
interface fastEthernet 0/1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit

Switch3:

configure terminal
no ip domain-lookup
vlan 6
exit
vlan 2
exit
vlan 3
exit
vlan 4
exit
vlan 5
exit
interface fastEthernet 0/2
switchport mode access
switchport access vlan 6
exit
interface fastEthernet 0/3
switchport mode access
switchport access vlan 2
exit
interface fastEthernet 0/4
switchport mode access
switchport access vlan 3
exit
interface fastEthernet 0/5
switchport mode access
switchport access vlan 4
exit
interface fastEthernet 0/6
switchport mode access

switchport access vlan 5
exit
interface fastEthernet 0/1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
Switch0(switch de destribution):
interface fastEthernet 0/1
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
interface fastEthernet 0/2
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
interface fastEthernet 0/3
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
interface fastEthernet 0/4
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan 5
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
switchport trunk allowed vlan add 4
exit
Configuration de routeur:
Creation de interface physique:
interface FastEthernet0/0

ip address 192.168.6.1 255.255.255.0
no shutdown
exi
interface serial/2
ip address 192.168.20.1 255.255.255.0
no shutdown
ex
interface serial/3
ip address 192.168.19.1 255.255.255.0
no shutdown
ex

Creation de interface vertuel pour vlan

interface Fa0/0.6
encapsulation dot1Q 6
ip address 192.168.13.254 255.255.255.0
no shutdown
exit
interface Fa0/0.2
encapsulation dot1Q 2
ip address 192.168.14.254 255.255.255.0
no shutdown
exit
interface Fa0/0.3
encapsulation dot1Q 3
ip address 192.168.15.254 255.255.255.0
no shutdown
exit
interface Fa0/0.4
encapsulation dot1Q 4
ip address 192.168.16.254 255.255.255.0
no shutdown
exit
interface Fa0/0.5
encapsulation dot1Q 5
ip address 192.168.17.254 255.255.255.0
no shutdown
exit

Configuration OSPF

router ospf 100
network 192.168.1.0 0.0.0.255 area 1
network 192.168.2.0 0.0.0.255 area 1
network 192.168.3.0 0.0.0.255 area 1
network 192.168.4.0 0.0.0.255 area 1
network 192.168.5.0 0.0.0.255 area 1
network 192.168.19.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0

network 192.168.6.0 0.0.0.255 area 1

9 Conclusion :

Ce rapport a présenté la configuration et la mise en œuvre de la solution réseau, en se concentrant sur le routage OSPF et la segmentation VLAN pour assurer une communication optimisée et sécurisée entre les sous-réseaux. Les choix effectués, tant au niveau de l'adressage IP que de la structuration des zones OSPF, ont permis de répondre aux besoins de segmentation du trafic et de hiérarchisation du réseau. La mise en place d'interfaces encapsulées en 802.1Q a renforcé la flexibilité et l'évolutivité du réseau.

L'ensemble des tests réalisés confirme la stabilité et l'efficacité de la configuration, en accord avec les objectifs initiaux. En conclusion, cette configuration permet une gestion centralisée tout en assurant une haute disponibilité et une répartition efficace du trafic. Il est recommandé de surveiller régulièrement le réseau et d'ajuster les paramètres OSPF et VLAN selon l'évolution des besoins et de la charge du réseau.