Rapport de Projet
Conception et Déploiement d'une Infrastructure Réseau Multisites Segmentée

Auteur : Imad Smahi

Module : Réseaux Informatiques

Professeur : M. Azeddine KHIAT

Année Académique : 2025/2026

Date de soumission : 07 Janvier 2026

II. Introduction & Objectifs

Dans le contexte actuel de la transformation numérique, les infrastructures réseau d'entreprise doivent être à la fois robustes, évolutives et sécurisées. Ce projet, réalisé dans le cadre du module "Réseaux Informatiques", porte sur la conception et la simulation d'une architecture réseau multisites à l'aide de l'outil Cisco Packet Tracer.
L'objectif principal est d'interconnecter un site central (siège social) avec deux agences distantes, en mettant en œuvre des technologies et des protocoles standards pour garantir la performance, la sécurité et la résilience du réseau [main.md].

Le rapport détaille la démarche suivie, depuis la définition des besoins jusqu'à la validation fonctionnelle de la solution. Les choix de conception ont été guidés par trois objectifs fondamentaux :

- **Segmentation et Organisation Logique :** Isoler les différents départements ou groupes d'utilisateurs au sein du réseau local du siège. L'utilisation de VLANs (Virtual Local Area Networks) permet de créer des domaines de diffusion distincts, améliorant ainsi la sécurité et l'efficacité du réseau en limitant la propagation des trames de broadcast.
- **Sécurité d'Accès et des Données :** Protéger le réseau contre les accès non autorisés et les vulnérabilités courantes. Cet objectif est atteint par la mise en place d'un VLAN natif dédié, la configuration d'un accès administratif sécurisé via SSH, et la séparation des flux de données et de gestion.
- **Haute Disponibilité et Redondance :** Assurer la continuité de service en cas de défaillance d'un lien. L'agrégation de liens via le protocole LACP (Link Aggregation Control Protocol) entre les commutateurs du siège augmente la bande passante et fournit une redondance de chemin. De plus, la topologie WAN triangulaire offre une redondance potentielle pour la communication entre les sites.

III. Topologie & Plan d'Adressage

3.1. Topologie du Réseau

L'architecture réseau est structurée autour d'un modèle "hub-and-spoke", où le siège (R1) agit comme le hub central connectant les deux agences distantes (R2 et R3). La topologie, visualisée ci-dessous, a été conçue sur Cisco Packet Tracer pour simuler un environnement d'entreprise réaliste [topologie.md].

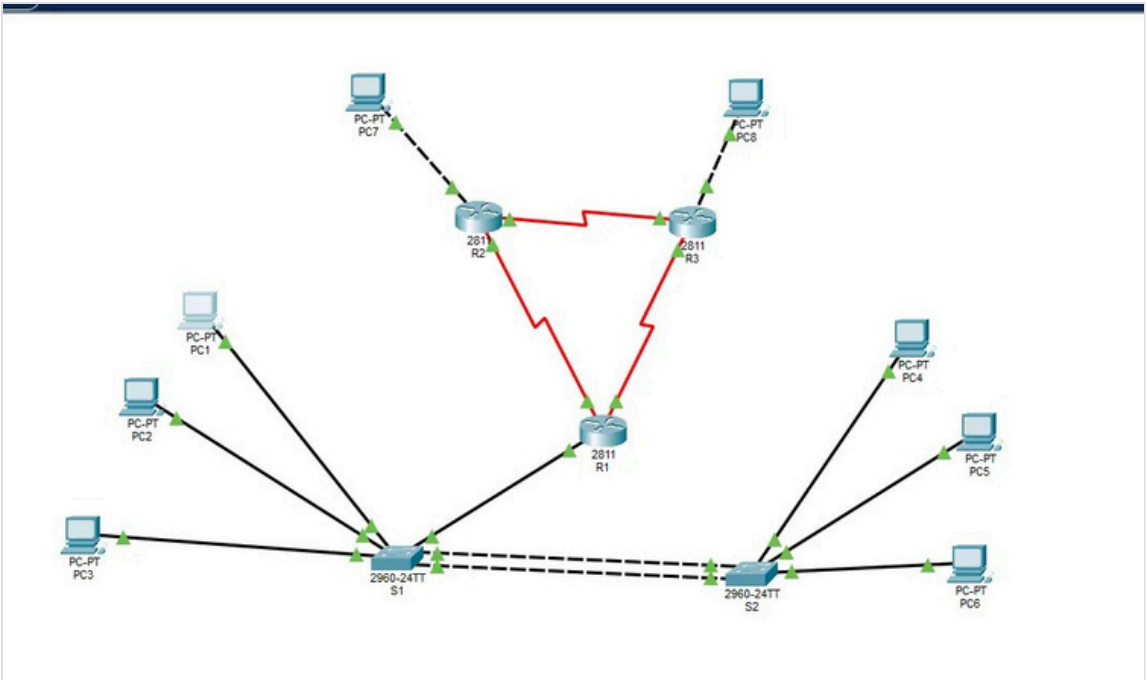

Figure 1 : Topologie réseau globale du projet

Les principaux composants de cette topologie sont :

- **Site Central (Siège) :** Composé d'un routeur **R1** (modèle 2811) et de deux commutateurs de couche 2, **S1** et **S2** (modèle 2960). R1 assure le routage inter-VLAN ("Router-on-a-Stick") et la connectivité WAN. S1 et S2 sont interconnectés via un EtherChannel pour la redondance et l'agrégation de bande passante.
- **Sites Distants (Agences) :** Représentés par les routeurs **R2** et **R3**, connectés au siège via des liaisons séries simulées.
- **Interconnexion WAN :** Les trois routeurs sont interconnectés dans une topologie triangulaire via des liaisons séries, formant l'infrastructure WAN.

3.2. Plan d'Adressage

Un plan d'adressage structuré est essentiel pour la gestion et l'évolutivité du réseau. Nous avons utilisé l'adressage IPv4 avec la technique VLSM (Variable Length Subnet Masking) pour optimiser l'utilisation des adresses [main.md].

3.2.1. Adressage du LAN (Siège)

Le réseau local du siège est segmenté en plusieurs VLANs pour des raisons de sécurité et d'organisation. Chaque VLAN dispose de son propre sous-réseau, avec le routeur R1 servant de passerelle par défaut. Les adresses des passerelles sont confirmées par la configuration des sous-interfaces sur R1 [r1.png].

Tableau 1 : Plan d'adressage des VLANs du site central

VLAN ID	Nom / Rôle	Réseau	Masque de sous-réseau	Adresse de la passerelle (R1)

10	Utilisateurs 1	172.18.10.0	255.255.255.0 (/24)	172.18.10.14
20	Utilisateurs 2	172.18.20.0	255.255.255.0 (/24)	172.18.20.14
30	Utilisateurs 3	172.18.30.0	255.255.255.0 (/24)	172.18.30.14
50	Natif (Sécurité)	172.18.50.0	255.255.255.0 (/24)	172.18.50.14
60	Admin / Gestion	172.18.60.0	255.255.255.0 (/24)	172.18.60.14

3.2.2. Adressage du WAN

Les liaisons point à point entre les routeurs utilisent des masques /30 pour économiser l'espace d'adressage, n'allouant que deux adresses IP utilisables par lien. Les adresses sont issues du bloc 10.0.0.0/8, couramment utilisé pour les réseaux internes étendus.

Tableau 2 : Plan d'adressage des liaisons WAN

Liaison	Réseau	Masque de sous-réseau	Adresse IP (Équipement 1)	Adresse IP (Équipement 2)
R1 - R2	10.0.30.176	255.255.255.252 (/30)	10.0.30.177 (R1 - S0/3/0)	10.0.30.178 (R2 - S0/3/0)
R1 - R3	10.0.30.180	255.255.255.252 (/30)	10.0.30.181 (R1 - S0/3/1)	10.0.30.182 (R3)
R2 - R3	10.0.30.184	255.255.255.252 (/30)	10.0.30.185 (R2 - S0/3/1)	10.0.30.186 (R3)

IV. Configuration Switching - Niveau 2

La configuration de la couche 2 au sein du siège est cruciale pour la segmentation et la résilience. Elle repose sur la création de VLANs, la configuration de liens Trunk et l'agrégation de liens avec EtherChannel.

4.1. Création des VLANs et Trunking (802.1Q)

Les VLANs 10, 20, 30, 50 et 60 ont été créés sur les deux commutateurs S1 et S2. Les ports connectés aux PCs ont été assignés en mode "access" au VLAN approprié. Pour permettre la communication de ces VLANs entre les équipements (S1-S2 et S1/S2-R1),

les liaisons inter-commutateurs et la liaison vers le routeur ont été configurées en mode "trunk" avec l'encapsulation **802.1Q**.

Une mesure de sécurité importante a été la configuration du **VLAN natif 50**. Par défaut, le VLAN natif est le VLAN 1. En le changeant pour un VLAN dédié et inutilisé par les utilisateurs (VLAN 50), on se prémunit contre les attaques de type "VLAN hopping" qui exploitent le trafic non tagué sur les trunks. La capture ci-dessous, prise sur S2, confirme que le Port-Channel 1 est en mode trunking et utilise bien le VLAN 50 comme natif.

```
S2>show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      50

Port        Vlans allowed on trunk
Po1         1,10,20,30,50,60

Port        Vlans allowed and active in management domain
Po1         1,10,20,30,50,60

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,20,30,50,60
S2>
```

État du trunk sur le commutateur S2.

4.2. EtherChannel (LACP)

Pour renforcer la liaison entre les commutateurs S1 et S2, un **EtherChannel** a été configuré en utilisant le protocole **LACP** (Link Aggregation Control Protocol). Les interfaces physiques FastEthernet 0/21 et 0/22 des deux commutateurs ont été groupées dans un canal de port logique (Port-channel 1). Cette configuration offre deux avantages majeurs :

- **Augmentation de la bande passante :** La bande passante totale de la liaison est la somme des bandes passantes des liens membres.
- **Redondance :** Si l'un des liens physiques tombe en panne, le trafic est automatiquement basculé sur les liens restants du canal, assurant une continuité de service sans interruption.

La commande `show etherchannel summary` sur S1 confirme que le groupe de canaux 1 (Po1) est opérationnel (SU - Layer2 in-use) et que les ports Fa0/21 et Fa0/22 y sont bien

agrégés (P - in port-channel).

```
S1>show 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: 1
Number of aggregators:                       1

Group Port-channel Protocol Ports
------+-------------+----------+-----------------------------------
-------------
1         Po1(SU)             LACP         Fa0/21(P) Fa0/22(P)
S1>
```

Résumé de la configuration EtherChannel sur le commutateur S1.

V. Configuration Routage Inter-VLAN - Niveau 3

Pour que les appareils situés dans des VLANs différents puissent communiquer entre eux, un routage de couche 3 est nécessaire. Dans notre topologie, cette fonction est assurée par le routeur R1 selon le modèle **"Router-on-a-Stick"**.

Cette méthode consiste à utiliser une seule interface physique du routeur (FastEthernet0/0) connectée à un port trunk du commutateur. L'interface physique est ensuite divisée en plusieurs **sous-interfaces logiques**, une pour chaque VLAN à router. Chaque sous-interface est configurée avec :

- L'encapsulation **dot1q**, qui spécifie l'ID du VLAN auquel elle est associée.
- Une adresse IP unique dans le sous-réseau du VLAN correspondant, qui servira de **passerelle par défaut** pour tous les hôtes de ce VLAN.

La commande `show ip interface brief` exécutée sur R1 montre clairement les sous-interfaces (Fa0/0.10, Fa0/0.20, etc.) configurées avec les adresses IP des passerelles pour

chaque VLAN. Toutes les sous-interfaces sont actives ("up/up"), ce qui indique que la configuration est fonctionnelle.

```
R1#show ip interface brief
Interface Protocol                IP-Address      OK? Method Status
FastEthernet0/0
up                                unassigned      YES unset      up
FastEthernet0/0.10
up      FastEthernet0/0.20        172.18.10.14    YES manual up
up      FastEthernet0/0.30
up      FastEthernet0/0.50        172.18.20.14    YES manual up
up
FastEthernet0/0.60                172.18.30.14    YES manual up
up
Serial0/3/0                       172.18.50.14    YES manual up
up Serial0/3/1 up ... R1#
                                  172.18.60.14    YES manual up

                                  10.0.30.177     YES manual up

                                  10.0.30.181     YES manual up
```

État des interfaces et sous-interfaces sur le routeur R1.

VI. Configuration Routage Statique WAN

La connectivité entre le siège et les agences distantes est réalisée via le réseau WAN. Pour cette topologie simple et maîtrisée, le **routage statique** a été privilégié par rapport aux protocoles de routage dynamique (comme OSPF ou EIGRP). Ce choix se justifie par plusieurs avantages dans ce contexte :

- **Sécurité :** Aucune annonce de routage n'est échangée entre les routeurs, ce qui réduit la surface d'attaque.
- **Performance :** Le routage statique ne consomme ni bande passante pour les mises à jour, ni ressources CPU/RAM pour les calculs d'algorithmes.
- **Prévisibilité :** Les chemins de données sont fixes et entièrement contrôlés par l'administrateur.

6.1. Routage sur les Agences (R2, R3)

Les routeurs R2 et R3 sont considérés comme des routeurs de "stub networks" (réseaux d'extrémité), car ils n'ont qu'un seul point de sortie logique vers le reste du réseau : le routeur du siège R1. Dans ce cas, la configuration la plus efficace consiste à définir une **route par défaut** (`0.0.0.0/0`). Cette route unique indique au routeur d'envoyer tout trafic destiné à des réseaux qu'il ne connaît pas directement vers le routeur suivant, ici R1.

La table de routage de R2, présentée ci-dessous, confirme la présence de cette route par défaut statique (marquée `S*`) pointant vers l'adresse IP de R1 sur la liaison série (`10.0.30.177`).

```
R2>show ip route
...
Gateway of last resort is 10.0.30.177 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
S C      10.0.30.128/27 [1/0] via 10.0.30.186 10.0.30.160/28 is directly
L C      connected, FastEthernet0/0 10.0.30.174/32 is directly connected,
L        FastEthernet0/0 10.0.30.176/30 is directly connected, Serial0/3/0
C        10.0.30.178/32 is directly connected, Serial0/3/0
L        10.0.30.184/30 is directly connected, Serial0/3/1
S*       10.0.30.185/32 is directly connected, Serial0/3/1
R2
>     0.0.0.0/0 [1/0] via 10.0.30.177
```

Table de routage du routeur d'agence R2.

6.2. Routage sur le Siège (R1)

Contrairement aux agences, le routeur central R1 doit connaître explicitement le chemin vers chaque sous-réseau distant. Des routes statiques doivent donc être configurées sur R1 pour chaque réseau local des agences R2 et R3, ainsi que pour la liaison WAN qui les interconnecte (10.0.30.184/30). Par exemple, pour atteindre le réseau local de R2 (`10.0.30.160/28`), R1 doit avoir une route statique pointant vers l'adresse IP de R2 (`10.0.30.178`).

VII. Tests & Validation

Une série de tests a été menée pour valider le bon fonctionnement de l'infrastructure et la connectivité de bout en bout. Les résultats confirment la réussite de la plupart des objectifs de configuration.

7.1. Test 1 : Connectivité Inter-VLAN

Objectif : Vérifier que le routage "Router-on-a-Stick" sur R1 fonctionne correctement et permet aux hôtes de différents VLANs de communiquer.

Méthode : Un test de ping a été effectué depuis un PC du réseau vers l'adresse IP d'un autre appareil dans un VLAN différent. La capture ci-dessous montre un ping vers `172.18.20.1` (probablement un PC dans le VLAN 20).

Résultat : Le test est majoritairement réussi, avec 3 paquets reçus sur 4. La perte du premier paquet est un comportement normal et attendu, souvent dû au temps nécessaire à la résolution ARP (Address Resolution Protocol) pour trouver l'adresse MAC de la destination. Le succès des pings suivants confirme que le trafic est correctement routé entre les VLANs par R1.

```
C:\>ping 172.18.20.1 Pinging 172.18.20.1 with 32 bytes of data:
Request timed out.
Reply from 172.18.20.1: bytes=32 time<1ms TTL=127
Reply from 172.18.20.1: bytes=32 time<1ms TTL=127
Reply from 172.18.20.1: bytes=32 time<1ms TTL=127


Ping statistics for 172.18.20.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
...
```

Test de ping inter-VLAN.

7.2. Test 2 : Accès en Gestion Sécurisée (SSH)

Objectif : Valider la configuration du VLAN de gestion (VLAN 60) et la possibilité d'administrer les équipements réseau de manière sécurisée.

Méthode : Une connexion SSH a été initiée depuis un poste de travail vers l'adresse IP de gestion du commutateur S2 (`172.18.60.2`), qui se trouve dans le VLAN 60.

Résultat : La connexion a été établie avec succès après la saisie du mot de passe, comme le montre l'invite de commande `S2>`. Ce test confirme que le VLAN 60 est fonctionnel, que le routage vers ce VLAN est correct, et que le service SSH est bien configuré sur le commutateur, permettant une gestion à distance chiffrée.

```
C:\>ssh -l admin 172.18.60.2
Password:
S2>
```

Connexion SSH réussie vers le commutateur S2.

Un test de ping complémentaire depuis R1 vers la même adresse (`172.18.60.2`) montre un taux de succès de 60% [test3.png], indiquant une connectivité de base mais potentiellement une légère instabilité initiale, typique dans un environnement simulé.

7.3. Test 3 : Vérification du Chemin WAN (Traceroute)

Objectif : Analyser le chemin emprunté par les paquets depuis le réseau local du siège vers une destination sur un site distant.

Méthode : Une commande `traceroute` a été lancée depuis un PC du VLAN 10 vers l'adresse IP `10.0.30.129`, qui appartient au réseau `10.0.30.128/27` (un réseau distant atteignable via R2 puis R3, d'après la table de routage de R2 [test4.png]).

Résultat : Le test a échoué. La trace montre que le paquet atteint bien sa passerelle par défaut sur R1 (`172.18.10.14`), mais ne parvient pas à progresser au-delà. Les réponses suivantes alternent entre des timeouts et des réponses de la même passerelle.

```
Tracing route to 10.0.30.129 over a maximum of 30 hops:

1         0    ms       0 ms        0    ms  172.18.10.14
2         0 ms            *        0 ms     172.18.10.14    Request
3            *          0 ms           *     timed out.
...
30        0ms         0ms         0ms      172.18.10.14

Trace complete.
```

Échec du traceroute vers un site distant.

Analyse : Cet échec indique une anomalie dans la configuration du routage sur R1. Le routeur R1 semble ne pas avoir de route statique pour le réseau de destination `10.0.30.128/27`. En l'absence d'une route correspondante, le routeur ne sait pas où envoyer le paquet et le rejette ou, dans ce cas, crée une boucle de routage locale. Ce test,
bien qu'ayant échoué, est crucial car il met en évidence un point de configuration à corriger pour achever la connectivité WAN.

VIII. Conclusion

Ce projet a permis de mettre en pratique les concepts fondamentaux de l'administration réseau en concevant et en déployant une infrastructure multisites simulée. Les objectifs initiaux ont été largement atteints : le réseau du siège a été segmenté avec succès à l'aide de VLANs, la résilience a été améliorée grâce à un EtherChannel LACP, et le routage inter-VLAN est pleinement fonctionnel. La mise en place d'un VLAN natif spécifique et d'un accès SSH sécurisé a également permis de répondre aux exigences de sécurité de base.

La phase de validation a confirmé le bon fonctionnement de la plupart des composants de l'architecture. Cependant, elle a également révélé une lacune critique dans la configuration du routage statique WAN sur le routeur central R1, empêchant la connectivité de bout en bout vers certains réseaux distants. Ce résultat souligne l'importance capitale d'une phase de tests exhaustive pour identifier et corriger les erreurs de configuration.

En conclusion, l'infrastructure déployée constitue une base solide et bien structurée. Les prochaines étapes consisteraient à corriger la configuration de routage statique sur R1 pour établir une connectivité WAN complète. Pour une évolution future, on pourrait envisager le remplacement du routage statique par un protocole de routage dynamique comme OSPF pour une gestion plus automatisée et évolutive des routes, ainsi que la mise en place de listes de contrôle d'accès (ACLs) pour affiner la politique de sécurité entre les VLANs.

IX. Lien GitHub

L'ensemble des fichiers de configuration et le fichier de simulation Cisco Packet Tracer (.pkt) sont disponibles sur le dépôt GitHub du projet.

- **Lien :** GitHub - Imadsm2002/Projet-Reseau-Imad-Smahi
- **Description :** Conception et déploiement d'un réseau multisite.