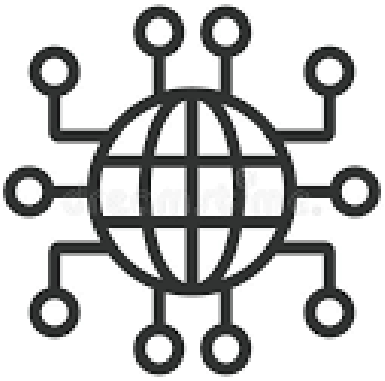
BASOL Teo
Session 2025

BTS Services Informatiques aux Organisations
Option Solutions d'Infrastructure, Systèmes et Réseaux

Épreuve E6 - Administration des systèmes et Réseaux

Documentation Technique



Réalisation n°2 : Segmentation et routage dynamique sur le réseau

Table des matières

I. Contexte

La Maison des Ligues de Lorraine (M2L) héberge diverses ligues sportives régionales, chacune ayant des besoins de communication spécifiques. Actuellement, le réseau de la M2L nécessite une mise à niveau pour améliorer la sécurité, la performance, et la gestion du trafic, tout en assurant une évolutivité pour les besoins futurs.

Pour répondre à ces exigences, ce projet vise à restructurer le réseau de la M2L en mettant en place une architecture robuste et segmentée.

Architecture Réseau Proposée :

- Routage Dynamique OSPF avec Multi-Area :
    - Le routage OSPF (Open Shortest Path First) permet l'échange des routes entre les routeurs qui l'utilisent. La gestion s'en trouve facilitée et plus flexible. Le protocole fonctionne grâce à la définition de plusieurs zones (area) avec une area 0 aussi appelée backbone qui sert de point d'ancrage.
    - OSPF sera implémenté comme protocole de routage dynamique pour assurer une communication efficace et adaptable entre les différents segments du réseau.
    - Le réseau sera divisé en trois zones (areas) OSPF pour optimiser le routage et réduire la charge sur les routeurs.
    - Une zone backbone (Area 0) interconnectera les trois routeurs principaux, assurant une connectivité centrale.
    - Routeur 1 sera configuré dans Area 1, gérant les VLAN 10 et 20.
    - Routeur 2 sera configuré dans Area 2, gérant les VLAN 30 et 40.
- Routage Inter-VLAN :
    - Des VLANs seront créés pour segmenter le réseau, isolant le trafic des différentes ligues sportives et des services administratifs.
    - VLAN 10 et VLAN 20 seront attribués au Routeur 1.
    - VLAN 30 et VLAN 40 seront attribués au Routeur 2.
    - Le routage inter-VLAN sera configuré sur les routeurs pour permettre la communication contrôlée entre ces VLANs.
- Routeur Mikrotik comme Passerelle Internet :
    - Un routeur Mikrotik sera utilisé comme passerelle principale pour fournir une connectivité Internet à l'ensemble de l'infrastructure réseau de la M2L.
    - Le Mikrotik assurera les fonctions de NAT (Network Address Translation), de pare-feu et de gestion de la bande passante.

Objectifs :

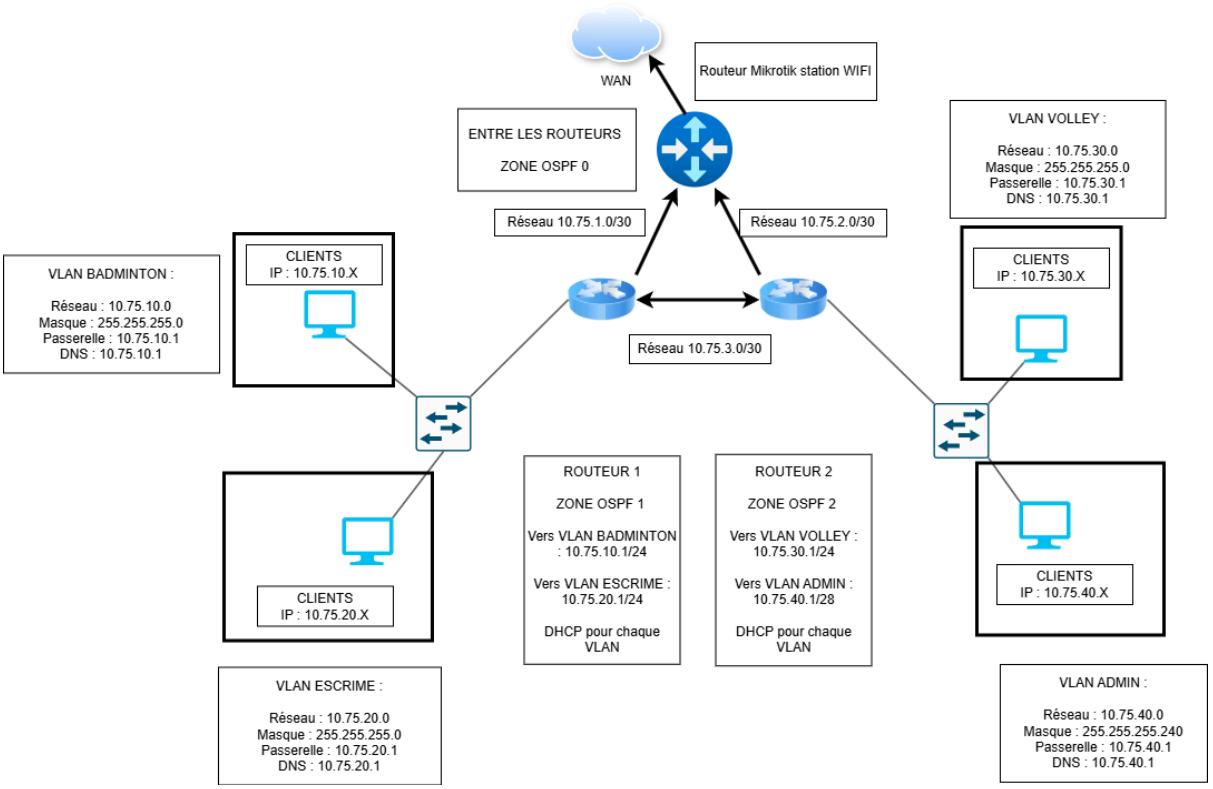
- Amélioration de la Sécurité : La segmentation en VLANs permettra d'isoler le trafic et de mettre en œuvre des politiques de sécurité spécifiques à chaque segment.
- Optimisation des Performances : Le routage OSPF assurera des chemins optimaux pour le trafic réseau, réduisant la latence et améliorant la bande passante disponible.
- Scalabilité : L'architecture multi-Area OSPF permettra d'étendre facilement le réseau à l'avenir.
- Gestion Centralisée d'Internet : Le routeur Mikrotik facilitera la gestion de la connexion Internet, la sécurité périmétrique et le contrôle de l'accès.

II. Prérequis

- Matériel :
    - Un routeur Mikrotik permettant une connexion au wifi extérieur
    - Deux routeurs et deux commutateurs Cisco
    - A minima, deux machines clientes
    - 9 câbles RJ45
- Logiciels/Services
    - Le logiciel Winbox pour configurer le routeur Mikrotik
    - Picocom (Linux) ou Putty (Windows) pour configurer les équipements Cisco
    - Un accès Wifi

III. Présentation Générale de l'Architecture Réseau

A. Schéma et logique



Le réseau est structuré selon une architecture hiérarchique en 3 zones OSPF :

- Area 0 – Backbone : Zone centrale d'échange de routes entre les équipements.
    - Interconnecte les Routeurs 1, 2, et Mikrotik.
    - Interfaces utilisées : liaisons point-à-point série (Serial0/0/0) entre R1 et R2 ; FastEthernet0/0 vers Mikrotik.
- Area 1 – Ligues Badminton et Escrime :
    - Rattachée au Routeur 1
    - Contient les VLAN 10 et VLAN 20
- Area 2 – Ligue Volley et Administration :
    - Rattachée au Routeur 2
    - Contient les VLAN 30 et VLAN 40

Chaque VLAN est associé à un sous-réseau IP distinct. Le routage inter-VLAN est géré localement sur chaque routeur via des sous-interfaces encapsulées en 802.1Q.

Le protocole OSPF permet la découverte automatique des routes dans chaque zone et garantit un basculement rapide en cas de modification topologique. Les interfaces reliées aux VLANs sont déclarées en mode passif pour empêcher l'envoi inutile de paquets OSPF sur les segments utilisateur.

B. Rôles des équipements

1. Routeur Mikrotik (passerelle internet)
    - Fait office de sortie unique vers Internet
    - Fonctionnalités :
        - NAT pour translation d'adresses
        - DHCP client sur interface WAN
        - Intégré à l'Area 0 pour la diffusion des routes
2. Routeur 1 – VLAN 10 et 20 / Area 0 et 1
    - Gère le trafic des ligues connectées aux VLAN 10 (10.75.10.0/24) et VLAN 20 (10.75.20.0/24), situés dans l'Area 1 d'OSPF
    - Fournit le routage inter-VLAN local
    - Relié à la backbone via :
        - Interface série vers R2 (10.75.3.1/30)
        - Interface FastEthernet0/0 (10.75.1.2/30)
    - Serveur DHCP configuré pour chaque VLAN
    - Route statique par défaut vers le routeur Mikrotik (via 10.75.1.1)
3. Routeur 2 – VLAN 30 & 40 / Area 0 et 2
    - Gère le trafic des ligues connectées aux VLAN 30 (10.75.30.0/24) et VLAN 40 (10.75.40.0/28), situés dans l'Area 2 d'OSPF
    - Fournit le routage inter-VLAN localement
    - Relié à la backbone via :
        - Interface série vers R1 (10.75.3.2/30)
        - Interface FastEthernet0/0 (10.75.2.2/30)
    - Serveur DHCP configuré pour chaque VLAN
    - Route statique par défaut vers le routeur Mikrotik (via 10.75.2.1)
4. Switch 1
    - Connecté au routeur 1 (R1)
    - Port FastEthernet0/1 en mode trunk qui autorise tous les VLANs définit à transiter
    - Port FastEthernet0/2 en mode access pour le VLAN 10
    - Port FastEthernet0/3 en mode access pour le VLAN 20
5. Switch 2
    - Connecté au routeur 2 (R2)

- Port FastEthernet0/1 en mode trunk
- Port FastEthernet0/2 en mode access pour le VLAN 30
- Port FastEthernet0/3 en mode access pour le VLAN 40

IV. Configuration du Routeur Mikrotik

A. Connexion au Wifi externe

1. Création du security Profiles
    - Commandes :
        - /interface wireless security-profiles set [find default=yes] supplicant-identity=MikroTik add authentication-types=wpa-psk,wpa2-psk mode=dynamic-keys name=profile1 supplicant-identity="" wpa-pre-shared-key=iticparis wpa2-pre-shared-key=******

Le Security Profile sert de clé d'accès pour se connecter au wifi externe.

2. Connexion au Wifi
    - Commandes :
        - /interface wireless set [find default-name=wlan1] band=2ghz-b/g/n disabled=no frequency=2417 security-profile=profile1 ssid="ITIC Paris"

Ici, l'interface wlan1 est connectée au réseau externe et le routeur Mikrotik est en mode station.

3. Obtenir une IP dynamiquement sur l'interface wlan1
    - Déclarer un DHCP Client sur l'interface wlan1
    - Ajouter le réseau externe et sa passerelle sur le DHCP Server
    - Créer un pool dans DHCP Server pour obtenir une IP sur l'interface wlan1 et ainsi créer la connexion au réseau externe
    - Commandes :
        - DHCP Client :
            - /ip dhcp-client add disabled=no interface=wlan1
        - DHCP Server :
            - /ip dhcp-server add address-pool=dhcp_pool1 disabled=no interface=wlan1 name=dhcp1
            - /ip dhcp-server network add address=10.190.4.0/22 gateway=10.190.4.1

        - /ip pool add name=dhcp_pool1 ranges=10.190.4.2-10.190.7.254
4. Règle de Firewall
    - Commandes :
        - /ip firewall nat add action=masquerade chain=srcnat out-interface=wlan1

Le NAT de type masquerade permet de convertir les adresses privées du réseau interne en une adresse publique à la sortie vers Internet.

B. Configuration des interfaces

1. Interface bridge
    - Ce bridge ne contient aucun port physique, avec l'adresse IP la plus basse, il servira de router-id au protocole OSPF
    - Commandes :
        - /interface bridge add comment="bridge pour router-id ospf" name=bridge1 protocol-mode=none
        - /ip address add address=0.0.0.1 interface=bridge1 network=0.0.0.1
2. Interface ether2 (vers R1)
    - Sert de connexion avec le routeur 1
    - Commande :
        - /ip address add address=10.75.1.1/30 interface=ether2 network=10.75.1.0
3. Interface ether3 (vers R2)
    - Sert de connexion avec le routeur 2
    - Commande :
        - /ip address add address=10.75.2.1/30 interface=ether3 network=10.75.2.0

C. Protocole OSPF

Le Mikrotik participe au routage OSPF avec les routeurs Cisco, dans l'Area 0 (backbone), ce qui permet de propager les routes internes à travers le réseau entier.

1. Ajoute des interfaces au protocole
    - Indique quels ports font partis du processus OSPF. Le port wlan1 est en mode passive pour ne pas envoyer des requêtes OSPF sur ce port.

- Commandes :
    - /routing ospf interface add interface=ether2 add interface=ether3 add interface=wlan1 passive=yes

2. Déclaration des réseaux directement connectés au routeur
    - Permet l'échange des routes à travers tout le réseau interne
    - Commandes :
        - /routing ospf network add area=backbone network=10.75.1.0/30 add area=backbone network=10.75.2.0/30

V. Configuration du Routeur 1 Cisco

PS : Sauf précisions contraires, toutes les commandes se réalisent en mode enable (administrateur) et configuration terminale. Lorsque l'on se connecte au routeur, entrer les commandes **enable** puis **configure terminal**

A. Configuration des interfaces

1. Interface FastEthernet0/0
    - Interface connectée au routeur Mikrotik
    - Avec un masque en /30 pour n'autorise que deux machines sur le réseau (le routeur Mikrotik et le router R1)
    - Commandes :
        - interface FastEthernet0/0, pour entrer sur l'interface
        - no shutdown, sert à allumer l'interface
        - ip address 10.75.1.2 255.255.255.252, ici, on attribue l'adresse IP de l'interface
2. Interface Serial0/0/0
    - Interface connectée au routeur 2 cisco (R2)
    - Avec un masque en /30 pour n'autorise que deux machines sur le réseau (le router R1 et le routeur R2)
    - Commandes :
        - interface Serial0/0/0, pour entrer sur l'interface
        - no shutdown, sert à allumer l'interface
        - ip address 10.75.3.1 255.255.255.252, adresse IP de l'interface
3. Interface FastEthernet0/1
    - Cette interface servira de connexion physique vers le LAN, mais n'aura pas d'IP, car le réseau et composé de plusieurs VLAN. Il faudra donc créer des sous-interfaces virtuelles pour chaque VLAN.
    - Commande :
        - interface FastEthernet0/1, pour entrer sur l'interface

    - no shutdown, sert à allumer l'interface et par conséquent toutes les sous-interfaces qui seront créées sur cette interface physique.
4. Interface FastEthernet0/1.10 (interface virtuelle dédiée au VLAN 10)
    - Cette sous-interface virtuelle servira de passerelle et de connexion au VLAN 10.
    - Commandes :
        - interface FastEthernet0/1.10, pour créer et entrer sur l'interface
        - encapsulation dot1Q 10, pour autoriser le VLAN 10
        - ip address 10.75.10.1 255.255.255.0, adresse IP de la sous-interface
5. Interface FastEthernet0/1.20 (interface virtuelle dédiée au VLAN 20)
    - Cette sous-interface virtuelle servira de passerelle et de connexion au VLAN 20.
    - Commandes :
        - interface FastEthernet0/1.20, pour créer et entrer sur l'interface
        - encapsulation dot1Q 20, pour autoriser le VLAN 20
        - ip address 10.75.20.1 255.255.255.0, adresse IP de la sous-interface

B. Création des DHCP pour chaque VLAN

Le routeur 1 fournira également le service DHCP pour les VLANs 10 et 20, afin que chaque appareil obtienne leur IP, masque, passerelle et DNS dynamiquement.

1. DHCP pour le VLAN 10
    - Commandes :
        - ip dhcp pool VLAN10, création du pool DHCP avec le nom VLAN10 et permet de rentrer en configuration DHCP
        - network 10.75.10.0 255.255.255.0, déclaration du réseau du VLAN 10
        - default-router 10.75.10.1, indication de la passerelle
        - dns-server 8.8.8.8, indication du serveur DNS
2. DHCP pour le VLAN 20
    - Commandes :
        - ip dhcp pool VLAN20, création du pool DHCP avec le nom VLAN20 et permet de rentrer en configuration DHCP
        - network 10.75.20.0 255.255.255.0, déclaration du réseau du VLAN 20
        - default-router 10.75.20.1, indication de la passerelle
        - dns-server 8.8.8.8, indication du serveur DNS

C. Routage dynamique et statique

Le routage s'effectuera grâce au protocole OSPF et à une route statique par défaut qui permettra de rediriger le trafic sortant vers le routeur Mikrotik.

1. Routage statique
    - Le routage statique, comme évoqué précédemment, permettra de rediriger le trafic sortant vers le routeur Mikrotik et ainsi fournir l'accès internet au réseau interne, ici au VLAN 10 et 20.
    - Commande :
        - ip route 0.0.0.0 0.0.0.0 10.75.1.1
2. Routage dynamique (OSPF)
    - Commandes :
        - router ospf 10, déclaration du processus OSPF et entré en mode configuration du protocole.
        - passive-interface FastEthernet0/1, ici cette interface et toutes les sous-interfaces ne recevront aucuns paquets de découverte de routeur voisin
        - network 10.75.1.0 0.0.0.3 area 0, déclaration du réseau entre ce routeur et le Mikrotik dans la backbone
        - network 10.75.3.0 0.0.0.3 area 0, déclaration du réseau entre ce routeur et le routeur 2 Cisco dans la backbone
        - network 10.75.10.0 0.0.0.255 area 1, déclaration du réseau du VLAN 10 dans l'area 1
        - network 10.75.20.0 0.0.0.255 area 1, déclaration du réseau du VLAN 20 dans l'area 1

VI. Configuration du Routeur 2 Cisco

PS : Sauf précisions contraires, toutes les commandes se réalisent en mode enable (administrateur) et configuration terminale. Lorsque l'on se connecte au routeur, entrer les commandes **enable** puis **configure terminal**

A. Configuration des interfaces

1. Interface FastEthernet0/0
    - Interface connectée au routeur Mikrotik
    - Avec un masque en /30 pour n'autorise que deux machines sur le réseau (le routeur Mikrotik et le router R2)
    - Commandes :
        - interface FastEthernet0/0, pour entrer sur l'interface
        - no shutdown, sert à allumer l'interface

        - ip address 10.75.2.2 255.255.255.252, ici, on attribue l'adresse IP de l'interface
2. Interface Serial0/0/0
    - Interface connectée au routeur 1 Cisco (R1)
    - Avec un masque en /30 pour n'autorise que deux machines sur le réseau (le router R1 et le routeur R2)
    - Commandes :
        - interface Serial0/0/0, pour entrer sur l'interface
        - no shutdown, sert à allumer l'interface
        - ip address 10.75.3.2 255.255.255.252, adresse IP de l'interface
3. Interface FastEthernet0/1
    - Cette interface servira de connexion physique vers le LAN, mais n'aura pas d'IP, car le réseau et composé de plusieurs VLAN. Il faudra donc créer des sous-interfaces virtuelles pour chaque VLAN.
    - Commande :
        - interface FastEthernet0/1, pour entrer sur l'interface
        - no shutdown, sert à allumer l'interface et par conséquent toutes les sous-interfaces qui seront créées sur cette interface physique.
4. Interface FastEthernet0/1.30 (interface virtuelle dédiée au VLAN 30)
    - Cette sous-interface virtuelle servira de passerelle et de connexion au VLAN 30.
    - Commandes :
        - interface FastEthernet0/1.30, pour créer et entrer sur l'interface
        - encapsulation dot1Q 30, pour autoriser le VLAN 30
        - ip address 10.75.30.1 255.255.255.0, adresse IP de la sous-interface
5. Interface FastEthernet0/1.40 (interface virtuelle dédiée au VLAN 40)
    - Cette sous-interface virtuelle servira de passerelle et de connexion au VLAN 40.
    - Commandes :
        - interface FastEthernet0/1.40, pour créer et entrer sur l'interface
        - encapsulation dot1Q 40, pour autoriser le VLAN 40
        - ip address 10.75.40.1 255.255.255.240, adresse IP de la sous-interface

B. Création des DHCP pour chaque VLAN

Le routeur 1 fournira également le service DHCP pour les VLANs 30 et 40, afin que chaque appareil obtienne leur IP, masque, passerelle et DNS dynamiquement.

1. DHCP pour le VLAN 30
    - Commandes :
        - ip dhcp pool VLAN30, création du pool DHCP avec le nom VLAN10 et permet de rentrer en configuration DHCP
        - network 10.75.30.0 255.255.255.0, déclaration du réseau du VLAN 30
        - default-router 10.75.30.1, indication de la passerelle
        - dns-server 8.8.8.8, indication du serveur DNS
2. DHCP pour le VLAN 40
    - Commandes :
        - ip dhcp pool VLAN40, création du pool DHCP avec le nom VLAN40 et permet de rentrer en configuration DHCP
        - network 10.75.40.0 255.255.255.240, déclaration du réseau du VLAN 40
        - default-router 10.75.40.1, indication de la passerelle
        - dns-server 8.8.8.8, indication du serveur DNS

C. Routage dynamique et statique

Le routage s'effectuera grâce au protocole OSPF et à une route statique par défaut qui permettra de rediriger le trafic sortant vers le routeur Mikrotik.

1. Routage statique
    - Le routage statique, comme évoqué précédemment, permettra de rediriger le trafic sortant vers le routeur Mikrotik et ainsi fournir l'accès internet au réseau interne, ici au VLAN 30 et 40.
    - Commande :
        - ip route 0.0.0.0 0.0.0.0 10.75.2.1
2. Routage dynamique (OSPF)
    - Commandes :
        - router ospf 10, déclaration du processus OSPF et entré en mode configuration du protocole.
        - passive-interface FastEthernet0/1, ici cette interface et toutes les sous-interfaces ne recevront aucuns paquets de découverte de routeur voisin
        - network 10.75.2.0 0.0.0.3 area 0, déclaration du réseau entre ce routeur et le Mikrotik dans la backbone
        - network 10.75.3.0 0.0.0.3 area 0, déclaration du réseau entre ce routeur et le routeur 1 Cisco dans la backbone
        - network 10.75.30.0 0.0.0.255 area 1, déclaration du réseau du VLAN 30 dans l'area 1

- network 10.75.40.0 0.0.0.15 area 1, déclaration du réseau du VLAN 40 dans l'area 1

VII. Configuration des Switch

PS : Sauf précisions contraires, toutes les commandes se réalisent en mode enable (administrateur) et configuration terminale. Lorsque l'on se connecte au commutateur, entrer les commandes **enable** puis **configure terminal**

A. Configuration du Commutateur 1

Le commutateur SW1 est responsable de la gestion des VLANs BADMINTON (VLAN 10) et ESCRIME (VLAN 20). Il agit comme point de connexion pour les périphériques appartenant à ces deux VLANs et gère également la communication inter-commutateur via une liaison trunk.

1. Nommage du commutateur
   - hostname SW1

2. Configuration des VLANs
   - VLAN 10 : BADMINTON
   - VLAN 20 : ESCRIME
   - VLAN 30 : VOLLEY (défini, mais non utilisé sur ce switch pour l'accès)
   - VLAN 40 : ADMIN (défini, mais non utilisé sur ce switch pour l'accès)

3. Configuration des interfaces
   - FastEthernet0/10: Port d'accès pour le VLAN 10 (BADMINTON).
     - interface FastEthernet0/10
     - switchport access vlan 10
     - switchport mode access
   - FastEthernet0/20: Port d'accès pour le VLAN 20 (ESCRIME).
     - interface FastEthernet0/20
     - switchport access vlan 20
     - switchport mode access
   - FastEthernet0/24: Port trunk permettant le trafic des VLANs 10 et 20
     - interface FastEthernet0/24
     - switchport trunk allowed vlan 10-20
     - switchport mode trunk

B. Configuration du Commutateur 2

Le commutateur SW2 gère les VLANs VOLLEY (VLAN 30) et ADMIN (VLAN 40). Il est configuré pour connecter les périphériques de ces VLANs et pour communiquer avec d'autres commutateurs via une liaison trunk.

1. Nommage du commutateur
    - hostname SW2

2. Configuration des VLANs
    - VLAN 10 : BADMINTON (défini, mais non utilisé sur ce switch pour l'accès)
    - VLAN 20 : ESCRIME (défini, mais non utilisé sur ce switch pour l'accès)
    - VLAN 30 : VOLLEY
    - VLAN 40 : ADMIN

3. Configuration des Interfaces
    - FastEthernet0/3: Port d'accès pour le VLAN 30 (VOLLEY).
        - interface FastEthernet0/3
        - switchport access vlan 30
        - switchport mode access
    - FastEthernet0/4: Port d'accès pour le VLAN 40 (ADMIN).
        - interface FastEthernet0/4
        - switchport access vlan 40
        - switchport mode access
    - FastEthernet0/24: Port trunk permettant le trafic des VLANs 30 et 40 vers d'autres commutateurs
        - interface FastEthernet0/24
        - switchport trunk allowed vlan 30-40
        - switchport mode trunk

VIII. Analyse et Vérification

La mise en œuvre de cette architecture réseau segmentée avec routage dynamique OSPF a été analysée et vérifiée pour garantir sa performance et sa conformité aux objectifs initiaux.

A. Vérification de la connectivité et du routage

- **Tests de ping inter-VLAN et inter-zone :** Des tests de ping ont été effectués depuis des clients de différents VLANs (VLAN 10, 20, 30, 40) vers des ressources situées dans d'autres VLANs, et ce, à travers les Routeurs 1 et 2. Tous les pings ont été concluants, confirmant le bon fonctionnement du routage inter-VLAN sur chaque routeur et la capacité des routeurs Cisco à échanger des routes via OSPF entre les Area 1, Area 2 et Area 0.
- **Vérification des tables de routage OSPF :** Les commandes show ip route ospf et show ip ospf neighbor ont été utilisées sur les routeurs Cisco et une vérification de la table de routage du routeur Mikrotik a confirmé la présence de toutes les routes attendues.
- **Vérification de l'accès Internet :** Des clients des VLANs 10, 20, 30 et 40 ont été testés pour accéder à Internet. L'accès a été validé pour tous, confirmant le bon fonctionnement du NAT sur le routeur Mikrotik et de la route statique par défaut configurée sur R1 et R2.
- **Tests de DHCP :** Les clients ont correctement obtenu des adresses IP, masques de sous-réseau, passerelles par défaut et serveurs DNS via les pools DHCP configurés sur les Routeurs 1 et 2 pour leurs VLANs respectifs.

B. Analyse de la performance et de la sécurité

- **Fiabilité et évolutivité :** Le protocole OSPF, par sa nature dynamique, assure une bonne résilience en cas de défaillance d'un chemin, permettant une reconvergence rapide du réseau. Cette architecture est également hautement évolutive, facilitant l'ajout de nouvelles ligues ou de services sans perturber l'ensemble du réseau.
- **Gestion centralisée de l'accès Internet :** Le routeur Mikrotik joue son rôle de passerelle Internet unique de manière efficace, simplifiant la gestion du NAT et offrant une plateforme pour d'éventuelles règles de pare-feu plus avancées à l'avenir.

IX. Conclusion et Préconisations

A. Conclusion

Ce projet de restructuration du réseau de la Maison des Ligues de Lorraine (M2L) a été un succès, répondant pleinement aux objectifs d'amélioration de la sécurité, de la performance, de la gestion du trafic et de la scalabilité. L'implémentation d'une architecture réseau segmentée à l'aide de VLANs, combinée à un routage dynamique OSPF multi-Area et à un routeur Mikrotik pour la passerelle Internet, a permis de créer une infrastructure robuste, flexible et sécurisée.

Les principaux bénéfices observés sont :

- **Sécurité accrue :** La segmentation en VLANs isole efficacement les différentes entités, limitant la propagation d'incidents de sécurité.
- **Gestion simplifiée :** L'automatisation du routage par OSPF réduit la charge administrative, et la centralisation de l'accès Internet facilite son contrôle.
- **Évolutivité future :** L'architecture est conçue pour s'adapter facilement aux besoins croissants de la M2L, permettant l'ajout de nouvelles ligues ou services sans refonte majeure.

L'expérience acquise à travers ce projet a été précieuse, tant dans la compréhension des mécanismes de routage et de segmentation que dans la manipulation de matériels et logiciels hétérogènes (Cisco IOS et RouterOS Mikrotik).

B. Préconisations

Pour aller plus loin et renforcer davantage l'infrastructure de la M2L, les préconisations suivantes sont formulées :

1. **Mise en place d'un serveur DNS interne :** Actuellement, le DNS 8.8.8.8 de Google est utilisé. L'installation d'un serveur DNS interne (par exemple, sur un serveur dédié ou sur le routeur Mikrotik si ses capacités le permettent) offrirait une meilleure résolution de noms locale, une latence réduite et un contrôle accru sur les requêtes DNS.
2. **Implémentation de règles de pare-feu avancées :** Bien que le NAT masquerade assure une sécurité de base, il est fortement recommandé de configurer des règles de pare-feu plus spécifiques sur le routeur Mikrotik. Cela permettrait de filtrer le trafic entrant et sortant de manière plus granulaire, de bloquer des ports ou protocoles non nécessaires, et de mettre en place des listes de contrôle d'accès (ACL) pour des restrictions de communication plus fines entre les VLANs
3. **Documentation et plan de reprise d'activité :** Il est crucial de maintenir à jour une documentation technique complète de l'architecture et des configurations. Parallèlement, l'élaboration d'un plan de reprise d'activité permettrait d'anticiper les défaillances majeures et d'assurer une continuité de service en cas d'incident.
4. **Gestion des mises à jour :** Établir une procédure régulière de mise à jour du firmware des équipements réseau (routeurs, switchs) pour bénéficier des dernières fonctionnalités, correctifs de sécurité et améliorations de performance.

Ces préconisations, si elles sont mises en œuvre, permettront à la M2L de disposer d'une infrastructure réseau encore plus résiliente, sécurisée et performante, prête à accompagner son développement futur.