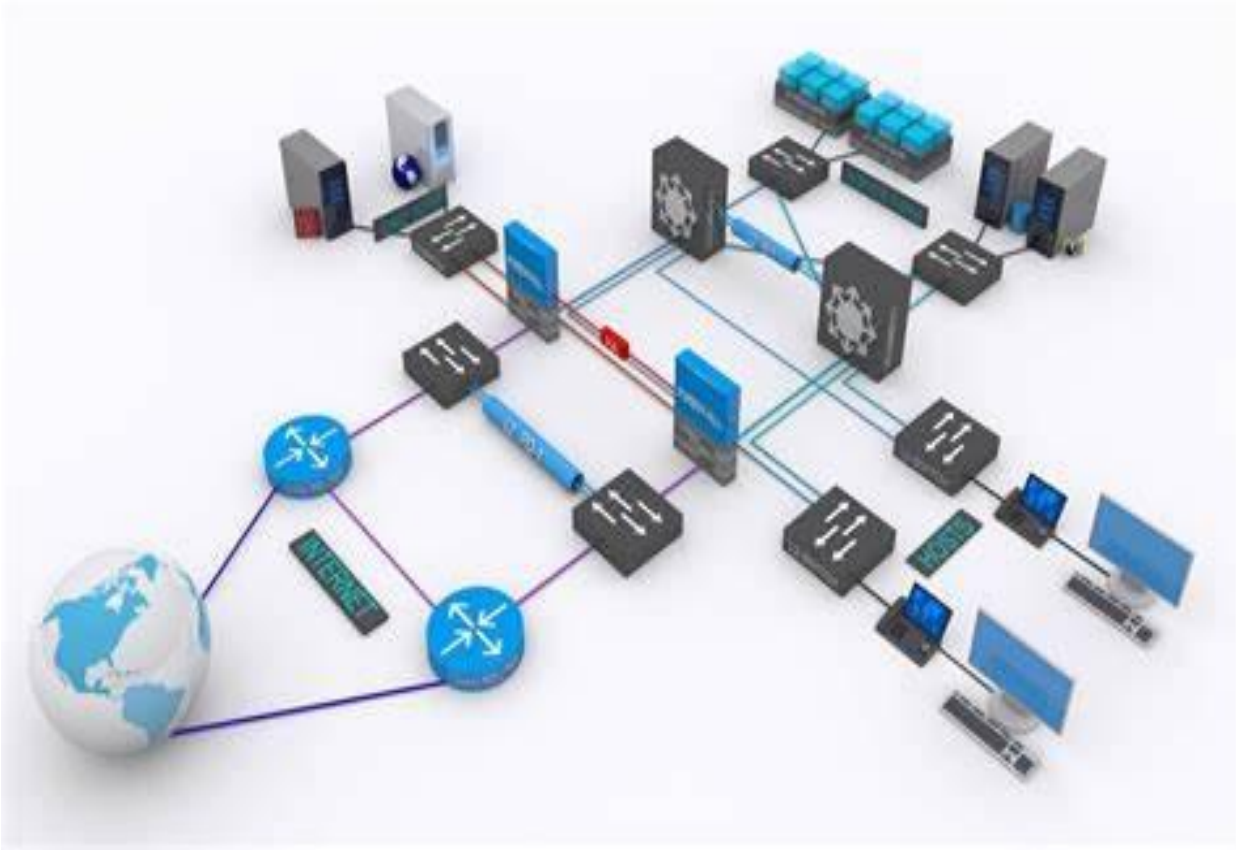
Rapport Technique de la SAE21 :

VLAN, Routage, NAT, ACL



SOMMAIRE

Introduction

Le projet consiste à étudier et mettre en place le réseau d'une école de type UJM, composé de plusieurs sites géographiques interconnectés. Chaque site héberge deux formations, des serveurs WEB et TFTP, ainsi que du personnel enseignant et administratif. L'objectif est de mettre en place une solution de routage externe utilisant le protocole RIP, permettant la communication entre les différents sites et l'accès à Internet. De plus, des mesures de sécurité sont mises en place pour contrôler les flux de trafic et assurer un accès approprié aux différentes ressources du réseau. Les serveurs WEB sont accessibles depuis le WAN, tandis que les serveurs TFTP sont réservés à un accès depuis le VLAN administration pour les sauvegardes de configurations.

1- Choix des matériels

Choix du matériel et câblage

1- Catégorie de câble Ethernet
Pour une connexion Gigabit Ethernet, on utilise des câbles de catégorie 5e (Cat 5e) ou catégorie 6 (Cat 6) pour des distances allant jusqu'à 100 mètres.
On ne pourra pas les connecter à l'aide d'un câble.
Pour des distances plus longues des câbles à fibre optique seront nécessaires.

2- Matériel dans chaque bâtiment
Switch Gigabit Ethernet : Chaque bâtiment nécessitera un switch capable de gérer les VLANs et les connexions Gigabit, Cisco Catalyst 2960.
Routeur : Pour l'interconnexion des sites, chaque site aura besoin d'un routeur capable de gérer le routage dynamique RIP, Routeur 1941 pour les LAN et Router-PT-Empty pour connecter les sites.

3- Boucle entre les bâtiments
Intérêt : La création d'une boucle permet d'assurer la redondance. Si un lien échoue, le trafic peut toujours passer par un autre chemin, augmentant ainsi la fiabilité du réseau.
Protocole : Le protocole STP (Spanning Tree Protocol) permettra d'éviter les boucles de réseau en désactivant dynamiquement les chemins redondants.
Conséquences si les SWITCH ne gèrent pas STP : Sans STP, une boucle réseau pourrait causer une tempête de broadcast, ce qui pourrait paralyser le réseau.
Configuration des ports : Les ports utilisés pour les liens inter-bâtiments doivent être configurés en mode trunk pour permettre la circulation de plusieurs VLANs sur le même lien.

2- Etude du plan d'adressage

Nous disposons la plage d'adresses 172.16.0.0/16. Avec comme outil Online IP Subnet Calculator and CIDR Calculator (subnet-calculator.com), j'ai prévu un plan d'adressage qui répond aux contraintes. Cette division en sous résous pour chaque LAN a été effectuée du LAN avec le plus grand nombre de machines à héberger vers le plus petit. Aussi, chaque réseau LAN a été divisé en sous réseau pour chaque VLAN.

Chaque LAN dispose au moins 5 vlans :

• un pour l'administration des SWITCH, routeurs et des serveurs : VLAN 10 , nom : admin
• un pour les services administratifs du site (scolarité, direction, secrétariat, ...) dans lequel est aussi installé un serveur WEB pour fournir des informations générales : VLAN 20, nom : services.

Les bâtiments étant mutualisés entre deux formations, il faudra aussi :

• un VLAN pour les étudiants de la formation A : VLAN 30, nom : formation_A

• un VLAN pour les étudiants de la formation B : VLAN 40, nom : formation_B

• un VLAN pour les enseignants.

Fichier du plan d'adressage des LAN et VLAN : Plan d'adressage - Google Sheets

Afin de vérifier qu'il n'y a pas de chevauchement entre les réseaux que nous avons choisi, nous allons utiliser un code python :

```python
import ipaddress

def check_ip_overlap(ip_networks):
    """
    Vérifie s'il y a un chevauchement d'adresses IP.
    :param ip_networks: Liste des adresses IP et masques de sous-réseau (en format string).
    :return: True si les adresses IP se chevauchent, False sinon.
    """
    networks = []
    for ip_net in ip_networks:
        try:
            network = ipaddress.IPv4Network(ip_net)
            for existing_network in networks:
                if network.overlaps(existing_network):
                    return True
            networks.append(network)
```

```
        except ValueError:
            # En cas d'adresse IP ou de masque de sous-réseau invalide
            return False
    return False
ip_networks = [
    "172.16.105.96/29",
    "172.16.105.0/26",
    "172.16.104.0/25",
    "172.16.104.128/25",
    "172.16.105.64/27",
    "172.16.68.96/28",
    "172.16.68.64/27",
    "172.16.64.0/23",
    "172.16.66.0/23",
    "172.16.68.0/26",
    "172.16.9.128/28",
    "172.16.9.0/25",
    "172.16.4.0/22",
    "172.16.0.0/22",
    "172.16.8.0/24",
    "172.16.102.128/27",
    "172.16.102.64/26",
    "172.16.100.0/23",
    "172.16.96.0/22",
    "172.16.102.0/26"
]

if check_ip_overlap(ip_networks):
    print("Il y a un chevauchement d'adresses IP.")
else:
    print("Il n'y a pas de chevauchement d'adresses IP.")
```

```
In [1]: runfile('C:/Users/micho/untitled1.py', wdir='C:/
Users/micho')
Il n'y a pas de chevauchement d'adresses IP.

In [2]:
```

3- Configuration des matériels

Pour la simulation j'ai eu besoin de 5 switches, 4 pour l'inter-connexion des VLAN et 1 pour le WAN.

Sur chaque switch j'ai configuré les interfaces pour les différentes VLAN et chaque fois je mettais le VLAN qui a le plus de postes en mode native sur l'interface de sortie.

L'interface reliant le switch au routeur est configuré en mode trunk et les autres inerfaces en mode access.

Par exemple sur le LAN 1, j'ai mis le VLAN 30 en native sur l'interface fa0/1 qui est l'interface de sortie, c'est-à-dire l'interface qui relie le switch au routeur.

La configuration est quasiment le même sur les autres switches qui se trouvent sur les différentes LAN seul le VLAN native change.

Exemple de configuration du switch1 du LAN1 :

```
!
interface FastEthernet0/1
 switchport trunk native vlan 30
 switchport trunk allowed vlan 10,20,30,40,100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
```

Au niveau de ce switch, nous avons le port 1 configuré en mode trunk avec l'ensemble des Vlans de ce LAN1, avec le vlan 30 comme vlan native.

L'interface fa0/7 qui relie le serveur tftp au switch est niveau du vlan 10, qui est le vlan admin et le fa0/8, reliant le serveur web au switch est lui au niveau du vlan 20 qui est le vlan services.

Configuration de S2 du LAN2 :

```
interface FastEthernet0/1
 switchport trunk native vlan 30
 switchport trunk allowed vlan 10,20,30,40,100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
```

Ici, c'est le fa0/8 qui est relié au serveur tftp sur le vlan 10 et le fa0/7 relie le serveur web au switch sur le vlan 20.

Configuration de S4 du LAN4 :

```
interface FastEthernet0/1
 switchport trunk native vlan 40
 switchport trunk allowed vlan 10,20,30,40,100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
```

Ici, nous constatons que seul le vlan native change, comme annoncé au début, nous avons choisi le vlan avec le plus grand nombre de machines comme vlan native, ici le vlan 40. L'interface fa0/7 pour le serveur tftp et celui fa0/8 pour le serveur web.

Configuration S3 du LAN3 :

```
interface FastEthernet0/1
 switchport trunk native vlan 40
 switchport trunk allowed vlan 10,20,30,40,100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
```

Pour les routeurs 1941 de chaque LAN aussi on a quasiment les mêmes configurations. Sur les interfaces g0/0, j'ai créé des sous-interfaces pour chaque VLAN avec l'encapsulation et leur passerelle. Aussi, il ne faut pas oublier de préciser le VLAN natif sur le routeur sinon la connexion pourrait ne pas marcher entre les VLANs.

Exemple de configuration du routeur 2 du LAN2 :

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.68.110 255.255.255.240
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.68.94 255.255.255.224
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30 native
 ip address 172.16.64.2 255.255.254.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.66.2 255.255.254.0
!
interface GigabitEthernet0/0.50
 no ip address
!
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.16.68.62 255.255.255.192
!
```

L’ensemble des configurations de chaque matériel se trouve au niveau du fichier de simulation.

4- Routage Inter-vlan

Avec le fichier : Configuration matériels.xlsx - Google Sheets, nous avons l'ensemble des adresses Ip choisies pour chaque matériel, pour chaque interface des routeurs.

Pour le routage inter-vlan, après une configuration des switches de chaque LAN, j'ai encapsulé la passerelle de chaque vlan en fonction de leur routeur sans oublier de mettre le vlan native choisie sur chaque LAN au niveau du routeur.

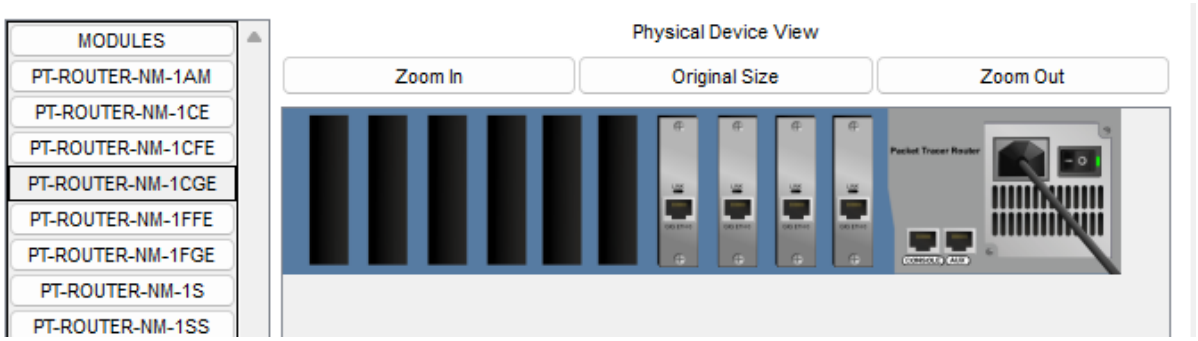
Sans une activation des interfaces, je n'avais toujours pas une connexion entre les vlan. Du coup, j'activais l'interface du routeur qui lui relie au switch avec la commande **no sh.**

Avec une bonne configuration, l'ensemble des VLAN communiquent entre eux.

Exemple de connectivité dans le LAN1, par une capture vidéo : Routage-Intervlan.mp4.

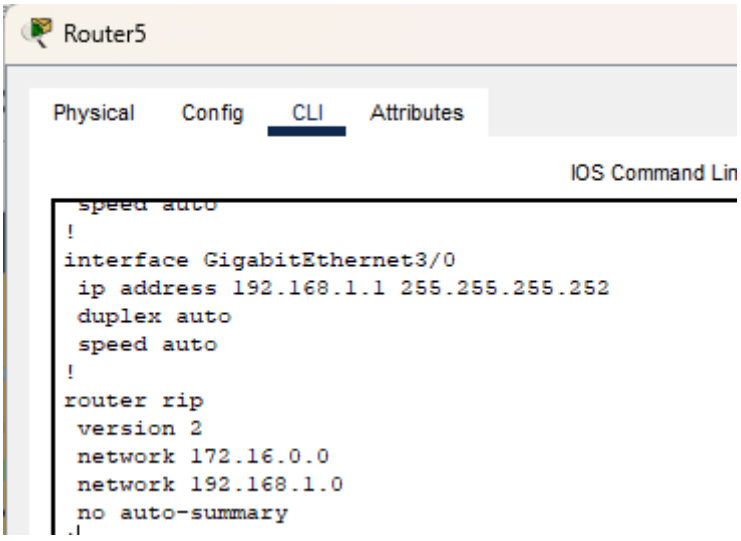
5- Routage Inter-Sites

Après une configuration pour le routage Inter-vlan, j'ai utilisé les routeurs Router PT Empty comme routeurs FAI en ajoutant les interfaces gigabits à ces routeurs :



Pour la configuration, j'ai utilisé le routeur Rip en annonçant les réseaux 172.16.0.0 (réseau des vlan) et 192.168.1.0 (réseau des interfaces des routeurs) sur les routeurs FAI.

Protocole Rip sur le routeur5 :



Ce protocole permet aux routeurs de partager des informations sur la topologie du réseau, afin de déterminer les meilleures routes pour le transfert des paquets de données. L'option no auto-summary est utilisée pour améliorer la précision des annonces de routage en évitant la récapitulation automatique au niveau des limites des réseaux de classe.

Pour un premier test de connectivité, je n'arrivais pas à connecter un site vers un autre.

J'ai dû mettre une route par défaut sur les routeurs qui sont reliés aux différents vlan : avec la commande **ip route 0.0.0.0 0.0.0.0 g0/1** avec **g0/1** l'interface de sortie.

Test de connectivité entre le LAN 1 et le LAN 2 : Routage-InterSites.mp4

6- Configuration des NAT :

D'abord, faut créer le pool d'adresse avec lequel les pc sorte sur le Wan, ensuite une access-list et enfin l'appliquer sur les interfaces d'entrées (inside) et sortie (outside)

Attention pour les serveurs, c'est un peu particulier, parce qu'ils doivent garder les mêmes adresses publiques. Pour cela faut renseigner l'adresse privée du serveur et l'adresse publique avec laquelle il sort sur le WAN.

Mettre les interfaces g0/0-3/0en inside et le g4/0 en outside car relié au WAN.

```
interface GigabitEthernet0/0
 ip address 192.168.1.22 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 ip address 192.168.1.14 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet2/0
 ip address 192.168.1.34 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet3/0
 ip address 192.168.1.17 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet4/0
 ip address 192.168.1.41 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
```

• NAT **Dynamique** : Le pool d'adresses `NETWORK` fournit une plage d'adresses IP publiques pour les translations dynamiques, permettant aux appareils internes d'utiliser une adresse IP publique du pool pour accéder à Internet.

• NAT **Statique** : Les entrées statiques mappent spécifiquement certaines adresses IP internes à des adresses IP publiques fixes, garantissant que ces appareils internes sont toujours accessibles via les mêmes adresses IP publiques.

```
!
ip nat pool NETWORK 161.3.36.37 161.3.36.46 netmask 255.255.255.240
ip nat inside source list 1 pool NETWORK
ip nat inside source static 172.16.105.2 161.3.36.33
ip nat inside source static 172.16.68.66 161.3.36.34
ip nat inside source static 172.16.9.2 161.3.36.35
ip nat inside source static 172.16.102.66 161.3.36.36
ip classless
!
```

L'access-list permet aux différents LAN de se connecter au WAN.

```
!
access-list 1 permit 172.16.0.0 0.0.255.255
!
!
```

• Inside **Local** : Les adresses IP des appareils internes au réseau privé.

• Inside **Global** : Les adresses IP publiques utilisées par le routeur pour représenter les adresses internes lorsqu'elles communiquent avec le monde extérieur.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  161.3.36.33       172.16.105.2       ---                ---
---  161.3.36.34       172.16.68.66       ---                ---
---  161.3.36.35       172.16.9.2         ---                ---
---  161.3.36.36       172.16.102.66      ---                ---
```

Ping d'un serveur web vers le WAN :

```
C:\>ping 161.3.131.2

Pinging 161.3.131.2 with 32 bytes of data:

Reply from 161.3.131.2: bytes=32 time=10ms TTL=124
Reply from 161.3.131.2: bytes=32 time=11ms TTL=124
Reply from 161.3.131.2: bytes=32 time=11ms TTL=124
Reply from 161.3.131.2: bytes=32 time=23ms TTL=124

Ping statistics for 161.3.131.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 23ms, Average = 13ms
```

Ping d'un PC vers le WAN :

```
C:\>ping 161.3.131.2

Pinging 161.3.131.2 with 32 bytes of data:

Reply from 161.3.131.2: bytes=32 time=61ms TTL=124
Reply from 161.3.131.2: bytes=32 time=12ms TTL=124
Reply from 161.3.131.2: bytes=32 time=11ms TTL=124
Reply from 161.3.131.2: bytes=32 time=12ms TTL=124

Ping statistics for 161.3.131.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 61ms, Average = 24ms
```

Configuration des ACLs :

VLAN 30

Configuration ACL : formationA

```
plaintext
Copier le code
ip access-list extended formationA
 permit ip 172.16.64.0 0.0.1.255 172.16.66.0 0.0.1.255
 permit ip 172.16.64.0 0.0.1.255 172.16.68.0 0.0.0.63
 permit ip 172.16.64.0 0.0.1.255 161.3.131.0 0.0.0.7
 permit ip 172.16.64.0 0.0.1.255 172.16.68.64 0.0.0.31

interface gigabitEthernet 0/0.30
 ip access-group formationA in
```

- **ACL "formationA" :** Cette ACL permet au réseau 172.16.64.0/23 d'accéder aux réseaux 172.16.66.0/23, 172.16.68.0/26, 161.3.131.0/29 et 172.16.68.64/27.
- **Application sur l'interface VLAN 30 :** Les règles sont appliquées à l'interface gigabitEthernet 0/0.30 en entrée (`in`), ce qui signifie que tout le trafic entrant sur cette interface sera filtré selon ces règles.

VLAN 40

Configuration ACL : formationB

```
plaintext
Copier le code
ip access-list extended formationB
 permit ip 172.16.66.0 0.0.1.255 172.16.64.0 0.0.1.255
 permit ip 172.16.66.0 0.0.1.255 172.16.68.0 0.0.0.63
 permit ip 172.16.66.0 0.0.1.255 161.3.131.0 0.0.0.7
 permit ip 172.16.66.0 0.0.1.255 172.16.68.64 0.0.0.31

interface gigabitEthernet 0/0.40
 ip access-group formationB in
```

- **ACL "formationB" :** Cette ACL permet au réseau 172.16.66.0/23 d'accéder aux réseaux 172.16.64.0/23, 172.16.68.0/26, 161.3.131.0/29 et 172.16.68.64/27.
- **Application sur l'interface VLAN 40 :** Les règles sont appliquées à l'interface gigabitEthernet 0/0.40 en entrée.

VLAN 100

Configuration ACL : enseignant

```
plaintext
Copier le code
ip access-list extended enseignant
 permit ip 172.16.68.0 0.0.0.63 172.16.66.0 0.0.1.255
 permit ip 172.16.68.0 0.0.0.63 172.16.64.0 0.0.1.255
```

```
 permit ip 172.16.68.0 0.0.0.63 161.3.131.0 0.0.0.7
 permit ip 172.16.68.0 0.0.0.63 172.16.68.64 0.0.0.31
 permit tcp 172.16.68.0 0.0.0.63 172.16.102.128 0.0.0.31 eq ftp

interface gigabitEthernet 0/0.100
 ip access-group enseignant in
```

- **ACL "enseignant" :** Cette ACL permet au réseau 172.16.68.0/26 d'accéder aux réseaux 172.16.66.0/23, 172.16.64.0/23, 161.3.131.0/29 et 172.16.68.64/27. Elle permet également l'accès FTP (port 21) à l'adresse 172.16.102.128/27.
- **Application sur l'interface VLAN 100 :** Les règles sont appliquées à l'interface gigabitEthernet 0/0.100 en entrée.

VLAN 20

Configuration ACL : service

```
plaintext
Copier le code
ip access-list extended service
 permit tcp 172.16.68.64 0.0.0.31 172.16.102.128 0.0.0.31 eq ftp

interface gigabitEthernet 0/0.20
 ip access-group service in
```

- **ACL "service" :** Cette ACL permet au réseau 172.16.68.64/27 d'accéder au service FTP (port 21) sur l'adresse 172.16.102.128/27.
- **Application sur l'interface VLAN 20 :** Les règles sont appliquées à l'interface gigabitEthernet 0/0.20 en entrée.

VLAN 10

Configuration ACL : admin

```
plaintext
Copier le code
ip access-list extended admin
 deny ip any 172.16.105.96 0.0.0.15
 permit ip 172.16.105.96 0.0.0.15 161.3.131.0 0.0.0.7
 permit ip 172.16.105.96 0.0.0.15 172.16.68.0 0.0.0.63

interface gigabitEthernet 0/0.10
 ip access-group admin in
```

- **ACL "admin" :** Cette ACL refuse tout le trafic vers le réseau 172.16.105.96/28 (deny ip any 172.16.105.96 0.0.0.15). Ensuite, elle permet l'accès de ce réseau aux réseaux 161.3.131.0/29 et 172.16.68.0/26.
- **Application sur l'interface VLAN 10 :** Les règles sont appliquées à l'interface gigabitEthernet 0/0.10 en entrée.

Résumé de l'Utilité

- **VLAN 30 et 40 :** Ces VLANs sont configurés pour permettre la communication entre les réseaux de formation et d'autres réseaux spécifiques tout en filtrant le trafic entrant selon les besoins.
- **VLAN 100 :** Ce VLAN est dédié aux enseignants, avec des permissions d'accès étendues y compris l'accès FTP, suggérant un besoin de transférer des fichiers.
- **VLAN 20 :** Ce VLAN est destiné à des services spécifiques avec une permission ciblée pour le service FTP.
- **VLAN 10 :** Ce VLAN a des restrictions plus strictes, interdisant l'accès à un sous-réseau spécifique tout en permettant des accès restreints à d'autres réseaux.

Simulation Réelle :

Nous allons tester notre simulation en réelle. Pour cela nous allons utiliser deux routeurs 1941, un switch et 3 PC.

Affectation des adresses IP suivantes sur les PC :

@Vlan 10 : 172.16.102.129

@Vlan 20 : 172.16.102.65

@Vlan 30 : 172.16.100.1

Configuration du switch du LAN4 :

Mettre les vlans sous les interfaces. Mettre l'interface g0/24 en mode trunk, se reliant au routeur FAI avec l'ensemble des vlans créés.

```
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 40
 switchport mode access

interface GigabitEthernet1/0/10
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 10,20,30,40,100
 switchport mode trunk
!
```

Configuration du routeur FAI :

Nous avons encapsulé la passerelle de chaque VLAN sous l'interface du routeur FAI g0/0/0.

```
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 172.16.102.158 255.255.255.224
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 172.16.102.126 255.255.255.192
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 172.16.101.254 255.255.254.0
!
interface GigabitEthernet0/0/0.40
 encapsulation dot1Q 40
 ip address 172.16.96.2 255.255.252.0
!
interface GigabitEthernet0/0/0.100
 encapsulation dot1Q 100
 ip address 172.16.102.62 255.255.255.192
!
```

Test de connectivité entre les différents vlans :

Après configuration, nous arrivons à envoyer des paquets depuis chaque vlan.

```
C:\Users\admin>ping 172.16.100.1

Envoi d'une requête 'Ping'  172.16.100.1 avec 32 octets de données :
Réponse de 172.16.100.1 : octets=32 temps<1ms TTL=127
Réponse de 172.16.100.1 : octets=32 temps=3 ms TTL=127
Réponse de 172.16.100.1 : octets=32 temps<1ms TTL=127
Réponse de 172.16.100.1 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.16.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms

C:\Users\admin>ping 172.16.102.65

Envoi d'une requête 'Ping'  172.16.102.65 avec 32 octets de données :
Réponse de 172.16.102.65 : octets=32 temps<1ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps<1ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps=1 ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.16.102.65:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

```
Microsoft Windows [version 10.0.19045.3208]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\admin>ping 172.16.102.129

Envoi d'une requête 'Ping'  172.16.102.129 avec 32 octets de données :
Réponse de 172.16.102.129 : octets=32 temps<1ms TTL=127
Réponse de 172.16.102.129 : octets=32 temps=2 ms TTL=127
Réponse de 172.16.102.129 : octets=32 temps=1 ms TTL=127
Réponse de 172.16.102.129 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 172.16.102.129:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

Ping du vlan 10 vers le vlan 30 :

```
C:\Users\admin>ping 172.16.102.65

Envoi d'une requête 'Ping'  172.16.102.65 avec 32 octets de données :
Réponse de 172.16.102.65 : octets=32 temps=1 ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps=2 ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps=1 ms TTL=127
Réponse de 172.16.102.65 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 172.16.102.65:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

Inter-Sites :

Adresse de la passerelle : 192.168.1.13

Adresse du Routeur FAI : 192.168.1.14

Interface FAI : g0/0/0 : 192.168.1.29 et g0/0/1 : 192.168.1.30

```
C:\Users\admin>ping 172.16.68.98

Envoi d'une requête 'Ping'  172.16.68.98 avec 32 octets de données :
Réponse de 172.16.68.98 : octets=32 temps=1 ms TTL=123
Réponse de 172.16.68.98 : octets=32 temps=3 ms TTL=123
Réponse de 172.16.68.98 : octets=32 temps=2 ms TTL=123
Réponse de 172.16.68.98 : octets=32 temps=2 ms TTL=123

Statistiques Ping pour 172.16.68.98:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 3ms, Moyenne = 2ms
```

```
C:\Users\admin>ping 172.16.8.1

Envoi d'une requête 'Ping'  172.16.8.1 avec 32 octets de données :
Réponse de 172.16.8.1 : octets=32 temps=1 ms TTL=124
Réponse de 172.16.8.1 : octets=32 temps=3 ms TTL=124
Réponse de 172.16.8.1 : octets=32 temps=1 ms TTL=124
Réponse de 172.16.8.1 : octets=32 temps=2 ms TTL=124

Statistiques Ping pour 172.16.8.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 3ms, Moyenne = 1ms
```

Mis en place de ssh :

Nous avons juste changé l'heure et la date manuellement puis créer une clée ssh ensuite créer un utilisateur et un mot de passe pour la connexion et enfin faire le transport ssh pour ensuite vérifier la connectivité ssh sur un des pc du vlan 10 qui est définit sur le switch.

```
Switch#clock set 15:30:00 june 18 2024
Jun 18 15:30:01.744: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:30:04 UTC Tue
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#crypto key generate rsa
The name for the keys will be: Switch.example.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 10 seconds)

Switch(config)#
Switch(config)#
Jun 18 15:30:43.910: %SSH-5-ENABLED: SSH 1.99 has been enabled
Switch(config)#username dase password dase
Switch(config)#line vty 0 15
Switch(config-line)#trans
Switch(config-line)#transport in
Switch(config-line)#transport input ss
Switch(config-line)#transport input ssh
Switch(config-line)#log
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#ip ssh version 2
Switch(config)#ip ssh authentication-retries 2
Switch(config)#write memory
```

Test de l'accès à ssh :

```
C:\Users\admin>ssh dase@172.16.102.135
The authenticity of host '172.16.102.135 (172.16.102.135)' can't be established.
RSA key fingerprint is SHA256:MUqvqP/Pzgoi4rhloVoqRwW2aA62Ox/HeN/wO6W2UBs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.102.135' (RSA) to the list of known hosts.
Password:
```

Conclusion

En conclusion, le projet de mise en place du réseau pour une école de type UJM a permis de développer et de tester des compétences clés en matière de VLAN, routage inter-VLAN, routage inter-sites, NAT et ACL. Les choix matériels et les configurations effectuées ont été validés par des tests de connectivité réussis, démontrant l'efficacité et la robustesse de la solution mise en œuvre. Cette expérience pratique renforce la compréhension des concepts théoriques et prépare efficacement à la gestion de réseaux complexes dans un environnement professionnel.