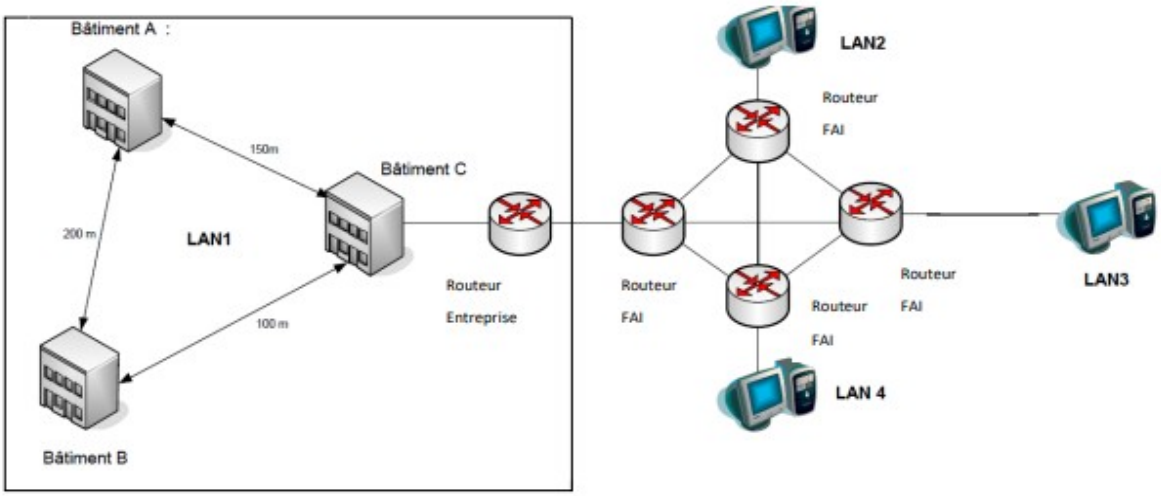
SAE2.01 Construire un réseau informatique pour une petite structure



SOMMAIRE

- Introduction page 3

PARTIE THÉORIQUE ET PRATIQUE

- Préambule page 4
- 1. Etude du plan d’adressage page 6
- 2. Le matériel pour créer cette topologie complète. page 8
- 3. liste du matériel nécessaire au minimum page 9
- 4. Mettre en place le routage inter-VLAN. page 10
- 5. Tableaux de configurations par LAN et par routeurs FAI page 10
- 6. Mise en place du routage inter-sites. page 14
- 7. Mise en place du NAT. page 15
- 8. Mise en place ACL page 17
- DS TP page 21
- Mon plan packet tracer page

INTRODUCTION

Dans le cadre de la SAE 2.01, je serai amené à concevoir, simuler et configurer l'architecture réseau d'un établissement scolaire réparti sur quatre sites géographiques distincts, chacun étant structuré autour de plusieurs VLANs. Ce projet a pour objectif de mettre en œuvre une infrastructure réseau complète et fonctionnelle, en répondant à un cahier des charges technique précis.

Concrètement, je devrai commencer par établir un plan d'adressage IP optimisé, basé sur la plage d'adresses 172.16.0.0/16, en appliquant la méthode VLSM afin de minimiser le gaspillage d'adresses et éviter les chevauchements. Ensuite, il me faudra choisir de manière justifiée les équipements réseau pour chaque site (routeurs, switchs, câblage), en tenant compte des performances nécessaires, du type de connectique (Gigabit Ethernet), et de la topologie prévue, notamment la présence d'une boucle entre les bâtiments.

Je devrai ensuite configurer tous les VLANs nécessaires : un VLAN pour l'administration du matériel (VLAN 10), un pour les services administratifs (VLAN 20), deux pour les formations A et B (VLANs 30 et 40), ainsi qu'un VLAN pour les enseignants (VLAN 100). À cela s'ajoute la configuration des routeurs pour assurer le routage inter-VLAN au sein de chaque site, ainsi que le routage inter-sites, en utilisant le protocole dynamique RIP et en répartissant les liaisons point à point à partir du réseau 192.168.1.0/24.

Par la suite, je mettrai en place un NAT (Network Address Translation) pour permettre à l'ensemble des sites d'accéder à Internet via une adresse publique fournie par le FAI. J'ajouterai également des ACL (Access Control Lists) pour restreindre les flux réseau en fonction des règles de sécurité spécifiées : par exemple, seuls certains VLANs pourront accéder aux serveurs TFTP ou FTP, et le VLAN administration devra être isolé mais autorisé à accéder au web.

Enfin, je devrai tester la connectivité et la conformité du réseau à l'aide d'une simulation sous Packet Tracer, incluant un sous-ensemble représentatif du réseau complet. Ce fichier de simulation me permettra de valider le bon fonctionnement des différentes fonctionnalités (routage, NAT, ACL, etc.) avant de réaliser une maquette en salle de TP avec les autres binômes.

Préambule

• Quelle catégorie de câble ETERNET faut-il ?

Vue qu'il a des connexions entre les bâtiments jusqu'à 200 m dans chaque LAN, j'ai opté pour un câble fibre optique multimode (OM3). Elle est utilisée dans les réseaux locaux rapides, comme dans les centres de données ou pour relier des bâtiments entre eux.
Elle est aussi compatible avec des connecteurs standards comme **LC**, **SC** ou **ST**.

- **LC** : Petit connecteur fibre optique, souvent utilisé dans les réseaux modernes, avec un système de clips (comme une prise RJ45).
- **SC** : Connecteur un peu plus gros que le LC, facile à brancher, souvent utilisé dans les réseaux d'entreprise.
- **ST** : Connecteur rond avec verrouillage par rotation, ancien modèle souvent utilisé dans les installations plus anciennes.

• Quel matériel sera utilisé dans chaque bâtiment pour cette connexion ?

Pour connecter deux bâtiments avec de la fibre OM3, chaque bâtiment a besoin du même matériel, car la communication se fait dans les deux sens. Donc, dans chaque bâtiment, on installera :

- Un switch manageable avec port SFP pour pouvoir gérer le réseau et brancher la fibre.
- Un module SFP multimode (ex : 1000Base-SX) pour convertir les signaux électriques en signaux lumineux.
- Des connecteurs LC pour relier la fibre au module.

Attention : On aura besoin du même équipement des deux côtés de la fibre, sinon la liaison ne fonctionne pas.

• Peut-on les connecter directement à l'aide d'un câble ? Dans le cas négatif, proposer une solution.

On ne peut pas connecter directement les bâtiments avec un simple câble réseau (RJ45), car la distance maximale pour ce type de câble est de 100 mètres. Or, certaines liaisons entre les bâtiments dépassent cette limite (200 m entre A et B, 150 m entre A et C). De plus, les câbles cuivre subissent des pertes de signal et des interférences sur de longues distances.

La solution consiste donc à utiliser de la fibre optique multimode OM3, qui permet de couvrir ces distances tout en assurant un débit élevé et une transmission stable. Pour cela, chaque bâtiment doit être équipé d'un switch avec port SFP, d'un module SFP multimode (comme un 1000Base-SX) et de connecteurs LC pour raccorder la fibre.

• On va créer une boucle entre les trois bâtiments. Quel en est l'intérêt ? Quel protocole va permettre le fonctionnement de ce type de topologie ? Que se passe-t-il si les SWITCH ne gèrent pas ce protocole ? Routeur Entreprise Routeur FAI Routeur FAI Routeur Routeur FAI FAI.

Créer une boucle entre les trois bâtiments permet d'assurer une redondance : si un lien tombe, le trafic peut passer par un autre chemin, ce qui rend le réseau plus fiable et disponible. Pour que cette topologie fonctionne correctement, il faut utiliser le protocole **STP (Spanning Tree Protocol)**, qui évite les boucles réseau en bloquant temporairement certains liens. Si les switchs ne gèrent pas le STP, des tempêtes de broadcast peuvent se produire, ce qui peut saturer le réseau et le rendre inutilisable.

• Quels sont les VLAN qui devront pouvoir circuler sur ces liens pour un bon fonctionnement ? Comment devront-être configurés les ports utilisés pour ces liens ?

Tous les VLAN utilisés sur le site doivent pouvoir circuler entre les bâtiments, car les équipements (postes, serveurs) peuvent être installés dans n'importe lequel. Il faudra donc permettre le passage des VLAN 10 (admin), 20 (services), 30 (formation_A), 40 (formation_B) et 100 (enseignants) sur les liens reliant les switchs.

Pour cela, les ports utilisés entre les switchs doivent être configurés en mode trunk, afin de transporter plusieurs VLAN simultanément. Ces ports devront accepter tous les VLAN nécessaires, avec les trames VLAN marquées (taguées) selon la norme 802.1q.

1. Etude du plan d’adressage :

Vous disposez de la plage d’adresses 172.16.0.0/16. Prévoyez un plan d’adressage qui répondra aux contraintes ci-dessous :

Nom du réseau local	Nombre maximal de machines à héberger
LAN 1	300
LAN 2	8000
LAN 3	8500
LAN 4	2000

Chaque LAN i devra disposer d'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.

Numéro du réseau local	Nombre de machines VLAN admin (VLAN 10)	Nombre de machines VLAN services (VLAN 20)	Nombre de machines VLAN formation_A (VLAN 30)	Nombre de machines VLAN formation_B (VLAN 40)	Nombre de machines VLAN enseignants (VLAN 100)	
LAN 1	2	31	90	80	20	
LAN 2	8	20	300	300	40	
LAN 3	8	64	512	514	127	
LAN 4	20	32	255	512	40	

Proposer un plan d’adressage en tenant compte du cahier des charges présenté et qui optimise l’espace d’adressage (continuité dans les adresses en partant de 172.16.0.0 et utilisation du VLSM). Le plan sera présenté dans un tableau comme ci-dessous afin de faciliter la vérification du non chevauchement des espaces d’adresses.

	Nombre de machines VLAN ADMIN	Nombre de machines VLAN SERVICE	Nombre de machines VLAN FORMATION A	Nombre de machines VLAN FORMATION B	Nombre de machines VLAN ENSEIGNANTS
LAN1	2 (+1 pour la passerelle)	31	90	80	20
Ad/MSR	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
Plage	172.16.105.97 à 172.16.105.102	172.16.105.1 à 172.16.105.62	172.16.104.1 à 172.16.104.126	172.16.104.129 à 172.16.104.254	172.16.105.65 à 172.16.105.94
LAN2	8	20	300	300	40
Ad/MSR	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
Plage	172.16.68.97 à 172.16.68.110	172.16.68.65 à 172.16.68.94	172.16.64.1 à 172.16.65.254	172.16.66.1 à 172.16.67.254	172.16.68.1 à 172.16.68.62
LAN3	8	64	512	514	127
Ad/MSR	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
Plage	172.16.9.129 à 172.16.9.142	172.16.9.1 à 172.16.9.126	172.16.4.1 à 172.16.7.254	172.16.0.1 à 172.16.3.254	172.16.8.1 à 172.16.8.254
LAN4	20	32	255	512	40
Ad/MSR	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
Plage	172.16.102.129 à 172.16.102.158	172.16.102.65 à 172.16.102.126	172.16.100.1 à 172.16.101.254	172.16.96.1 à 172.16.99.254	172.16.102.1 à 172.16.102.62

Python propose un module « ipaddress », utilisez celui-ci dans un programme pour vérifier qu'il n'y a pas de chevauchement entre les réseaux que vous avez choisi.

```
import ipaddress

# Dictionnaire des sous-réseaux extraits du tableau
# La clé est une description (LAN, VLAN) et la valeur est l'adresse CIDR
subnets_data = {
  # LAN 1
  "LAN1 - ADMIN": "172.16.105.96/29",
  "LAN1 - SERVICE": "172.16.105.0/26",
  "LAN1 - FORMATION A": "172.16.104.0/25",
  "LAN1 - FORMATION B": "172.16.104.128/25",
  "LAN1 - ENSEIGNANTS": "172.16.105.64/27",
  # LAN 2
  "LAN2 - ADMIN": "172.16.68.96/28",
  "LAN2 - SERVICE": "172.16.68.64/27",
  "LAN2 - FORMATION A": "172.16.64.0/23",
  "LAN2 - FORMATION B": "172.16.66.0/23", # Note: Ce réseau est inclus dans
172.16.64.0/23
  "LAN2 - ENSEIGNANTS": "172.16.68.0/26",
  # LAN 3
  "LAN3 - ADMIN": "172.16.9.128/28",
  "LAN3 - SERVICE": "172.16.9.0/25",
  "LAN3 - FORMATION A": "172.16.4.0/22",
  "LAN3 - FORMATION B": "172.16.0.0/22",
  "LAN3 - ENSEIGNANTS": "172.16.8.0/24",
  # LAN 4
  "LAN4 - ADMIN": "172.16.102.128/27",
  "LAN4 - SERVICE": "172.16.102.64/26",
  "LAN4 - FORMATION A": "172.16.100.0/23",
  "LAN4 - FORMATION B": "172.16.96.0/22",
  "LAN4 - ENSEIGNANTS": "172.16.102.0/26"
}

# Crée une liste d'objets (description, objet IPv4Network)
networks = []
for name, cidr in subnets_data.items():
  try:
    network_obj = ipaddress.ip_network(cidr, strict=False)
    networks.append((name, network_obj))
  except ValueError as e:
    print(f"Erreur de format pour {name} ({cidr}): {e}")
```

```
print("Vérification des chevauchements pour tous les réseaux du tableau...\n")

# Vérification des chevauchements
overlap_found = False
# Crée une liste des clés pour pouvoir itérer par index
network_keys = list(networks)

for i in range(len(network_keys)):
  for j in range(i + 1, len(network_keys)):
    name1, net1 = network_keys[i]
    name2, net2 = network_keys[j]

    if net1.overlaps(net2):
      print(f"❌ Chevauchement détecté !")
      print(f"  - Réseau 1 ({name1}): {net1}")
      print(f"  - Réseau 2 ({name2}): {net2}\n")
      overlap_found = True

if not overlap_found:
  print("✅ Aucun chevauchement n'a été détecté entre les sous-réseaux.")
```

2. Choisir, en justifiant, le matériel pour créer cette topologie complète. (Donner la liste.)

Matériel par bâtiment (x3 bâtiments par LAN, donc x12 au total)

- **1 Switch manageable avec port SFP**
  ➤ Pour gérer les VLANs et la connexion fibre entre bâtiments (liaisons >100m).
  Exemple : Cisco Catalyst 2960 ou 3560.
- **1 Module SFP multimode (1000Base-SX)**
  ➤ Permet d'utiliser la fibre OM3 (distance >100m).
- **1 Câble fibre optique multimode OM3 avec connecteurs LC**
  ➤ Débit élevé, faible atténuation sur de longues distances.
- **Postes clients selon les VLANs**
  ➤ PC simulés dans Packet Tracer (3-5 par VLAN pour test).
- **Serveurs (par LAN)**
  ➤ 1 serveur TFTP sur VLAN 10 (admin)
  ➤ 1 serveur WEB sur VLAN 20 (services)
  ➤ Matériel : Cisco generic server (dans Packet Tracer)

Interconnexion des LAN (backbone)

- **4 Routeurs (1 par LAN)**
  ➢ Pour le routage inter-VLAN local et RIP pour l'interconnexion inter-sites.
  Exemple : Cisco 2901.
- **1 Routeur FAI / NAT (point de sortie vers WAN)**
  ➢ Connecté au réseau 161.3.36.32/28 (NAT).
  ➢ Doit avoir une interface connectée au WAN et une autre vers le cœur du réseau.
- **Switch central (optionnel)**
  ➢ Pour connecter les routeurs entre eux si le cœur de réseau est centralisé.

Sécurité

- **ACLs configurées sur les routeurs**
  ➢ Pour restreindre les flux selon le cahier des charges (accès HTTP, FTP, ping, etc.).
- **Topologie en boucle avec STP activé sur les switchs**
  ➢ Redondance / évite les tempêtes de broadcast.

3. Avant de configurer le matériel vous allez réaliser une simulation sur Packet-Tracer (penser aux notions de cybersécurité). Faire une liste du matériel nécessaire au minimum pour faire les tests de connectivité entre les VLAN. Proposer un fichier de simulation.

Dans chaque lan :

Équipement	Quantité	Rôle
Routeur	1	Routage inter-VLAN
Switch manageable (avec mode trunk)	1	Transport des VLANs
PC VLAN 10 (admin)	1	Test d'accès admin
PC VLAN 20 (services)	1	Test accès service
PC VLAN 30 (formation A)	1	Test accès formation A
PC VLAN 40 (formation B)	1	Test accès formation B
PC VLAN 100 (enseignants)	1	Test accès prof
Serveur TFTP (VLAN 10)	1	Test sauvegarde admin
Serveur Web (VLAN 20)	1	Test HTTP public
Câbles Ethernet	x	Connexions réseau

+ 4 routeur FAI au milieu pour l'interconnexion entre les différents LAN
Voici la répartition des équipements de chaque LAN :

Dans le bâtiment A :

- 1 PC vlan 30
- 1 PC vlan 10
- 1 serveur TFTP vlan 10

Dans le bâtiment B :

- 1 PC vlan 40
- 1 PC vlan 100

Dans le bâtiment C :
- 1 PC vlan 20
- 1 serveur WEB vlan 20

4. Mettre en place le routage inter-VLAN.

Dans chaque routeur de chaque lan, on configure des port en encapsulation dot1Q numéro_vlan associé et leurs adresses de passerelles.

Exemple :

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.105.97 255.255.255.248
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.105.1 255.255.255.192
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.104.1 255.255.255.128
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.104.129 255.255.255.128
!
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.16.105.65 255.255.255.224
!
interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.252
 duplex auto
 speed auto
```

5. Compléter le document suivant en relevant les informations importantes et en les consignant dans des tableaux pour archivage.

Voici les configurations de chaque LAN :

LAN1 :

Configuration des ports de switch

ports	Mode (access ou trunk)	VLAN untagged (802.3)	VLAN(s) tagged (802.1q)
Fa0/1	access	30	
Fa0/2	access	40	
Fa0/3	access	100	
Fa0/4	trunk	-	10,20,30,40,100

IP des équipements du LAN 1

machines	Adresse IP	masque	passerelle
PC1 (admin)	172.16.105.98	255.255.255.248	172.16.105.97
SERVEUR TFTP (admin)	172.16.105.99	255.255.255.248	172.16.105.97
PC2 (services)	172.16.105.2	255.255.255.192	172.16.105.1

machines	Adresse IP	masque	passerelle
SERVEUR WEB (services)	172.16.105.3	255.255.255.192	172.16.105.1
PC3 (formation_A)	172.16.104.2	255.255.255.128	172.16.104.1
PC4 (formation_B)	172.16.104.130	255.255.255.128	172.16.104.129
PC5 (enseignants)	172.16.105.66	255.255.255.224	172.16.105.65
Interface g0/0.10 Routeur	172.16.105.97	255.255.255.248	-
Interface g0/0.20 Routeur	172.16.105.1	255.255.255.192	-
Interface g0/0.30 Routeur	172.16.104.1	255.255.255.128	-
Interface g0/0.40 Routeur	172.16.104.129	255.255.255.128	-
Interface g0/0.100 Routeur	172.16.105.65	255.255.255.224	-
Interface g0/1 Routeur	192.168.2.2	255.255.255.252	-

LAN2 :

Configuration des ports de switch

ports	Mode (access ou trunk)	VLAN untagged (802.3)	VLAN(s) tagged (802.1q)
Fa0/1	access	30	
Fa0/2	access	40	
Fa0/3	access	100	
Fa0/4	trunk	-	10,20,30,40,100

IP des équipements du LAN

machines	Adresse IP	masque	passerelle
PC1 (admin)	172.16.68.98	255.255.255.240	172.16.68.97
SERVEUR TFTP (admin)	172.16.68.99	255.255.255.240	172.16.68.97
PC2 (services)	172.16.68.66	255.255.255.224	172.16.68.65
SERVEUR WEB (services)	172.16.68.67	255.255.255.224	172.16.68.65
PC3 (formation_A)	172.16.64.2	255.255.254.0	172.16.64.1
PC4 (formation_B)	172.16.66.2	255.255.254.0	172.16.66.1
PC5 (enseignants)	172.16.68.2	255.255.255.192	172.16.68.1
Interface g0/0.10 Routeur	172.16.68.97	255.255.255.240	-
Interface g0/0.20 Routeur	172.16.68.65	255.255.255.224	-
Interface g0/0.30 Routeur	172.16.64.1	255.255.254.0	-
Interface g0/0.40 Routeur	172.16.66.1	255.255.254.0	-
Interface g0/0.100 Routeur	172.16.68.1	255.255.255.192	-
Interface g0/1 Routeur	192.168.2.6	255.255.255.252	-

LAN3 :

Configuration des ports de switch

ports	Mode (access ou trunk)	VLAN untagged (802.3)	VLAN(s) tagged (802.1q)
Fa0/1	access	30	
Fa0/2	access	40	
Fa0/3	access	100	
Fa0/4	trunk	-	10,20,30,40,100
...	...	...	...

IP des équipements du LAN 3

machines	Adresse IP	masque	passerelle
PC1 (admin)	172.16.9.130	255.255.255.240	172.16.9.129
SERVEUR TFTP (admin)	172.16.9.131	255.255.255.240	172.16.9.129
PC2 (services)	172.16.9.2	255.255.255.128	172.16.9.1
PC3 (formation_A)	172.16.4.10	255.255.252.0	172.16.4.1
PC4 (formation_B)	172.16.0.10	255.255.252.0	172.16.0.1
PC5 (enseignants)	172.16.8.10	255.255.255.0	172.16.8.1
Interface g0/0.10 Routeur	172.16.9.129	255.255.255.240	-
Interface g0/0.20 Routeur	172.16.9.1	255.255.255.128	-
Interface g0/0.30 Routeur	172.16.4.1	255.255.252.0	-
Interface g0/0.40 Routeur	172.16.0.1	255.255.252.0	-
Interface g0/0.100 Routeur	172.16.8.1	255.255.255.0	-
Interface g0/1 Routeur	192.168.2.10	255.255.255.252	

LAN4 :

Configuration des ports de switch

ports	Mode (access ou trunk)	VLAN untagged (802.3)	VLAN(s) tagged (802.1q)
Fa0/1	access	30	
Fa0/2	access	40	
Fa0/3	access	100	
Fa0/4	trunk	-	10,20,30,40,100

IP des équipements du LAN

machines	Adresse IP	masque	passerelle
PC1 (admin)	172.16.102.130	255.255.255.224	172.16.102.129
Serveur TFTP	172.16.102.131	255.255.255.224	172.16.102.129
PC2 (services)	172.16.102.66	255.255.255.192	172.16.102.65
Serveur Web	172.16.102.67	255.255.255.192	172.16.102.65
PC3 (formation_A)	172.16.100.2	255.255.254.0	172.16.100.1
PC4 (formation_B)	172.16.96.2	255.255.252.0	172.16.96.1
PC5 (enseignants)	172.16.102.2	255.255.255.192	172.16.102.1
Interface g0/0.10 Routeur	172.16.102.129	255.255.255.224	-

machines	Adresse IP	masque	passerelle
Interface g0/0.20 Routeur	172.16.102.65	255.255.255.192	-
Interface g0/0.30 Routeur	172.16.100.1	255.255.254.0	-
Interface g0/0.40 Routeur	172.16.96.1	255.255.252.0	-
Interface g0/0.100 Routeur	172.16.102.1	255.255.255.252	-

Mot de passe des routeurs FAI:

Routeur FAI	enable	VTY	console
FAI 1	FAI	FAI_1	rt1
FAI 2	FAI	FAI_2	rt2
FAI 3	FAI	FAI_3	rt3
FAI 4	FAI	FAI_4	rt4

Mot de passe des routeurs LANs :

Routeur LAN	enable	VTY	console
LAN1	LAN	LAN_1	lan1
LAN2	LAN	LAN_2	lan2
LAN3	LAN	LAN_3	lan3
LAN4	LAN	LAN_4	lan4

exemple :

```
Router(config)#enable sec
Router(config)#enable secret FAI
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password rt1
Router(config-line)#login
Router(config)#line vty 0 4
Router(config-line)#pass
Router(config-line)#password FAI_2
Router(config-line)#login
Router(config-line)#exi
```

6. Mise en place du routage inter-sites. On vous demande de mettre en place une solution de routage externe à l'aide de RIP. Pour les liaisons intersites, vous découperez le réseau 192.168.1.0 en sous-réseaux pour créer des liaisons points à points

Liaison	Sous-réseau	IP Routeur A	IP Routeur B
FAI1 ↔ FAI2	192.168.1.0/30	192.168.1.1	192.168.1.2
FAI1 ↔ FAI3	192.168.1.4/30	192.168.1.5	192.168.1.6
FAI1 ↔ FAI4	192.168.1.8/30	192.168.1.9	192.168.1.10
FAI2 ↔ FAI3	192.168.1.12/30	192.168.1.13	192.168.1.14
FAI2 ↔ FAI4	192.168.1.16/30	192.168.1.17	192.168.1.18

Liaison	Sous-réseau	IP Routeur A	IP Routeur B
FAI3 ↔ FAI4	192.168.1.20/30	192.168.1.21	192.168.1.22

Liaison	réseau	Masque
R1 ↔ FAI1	192.168.1.24	255.255.255.252
R2 ↔ FAI2	192.168.1.28	255.255.255.252
R3 ↔ FAI3	192.168.1.32	255.255.255.252
R4 ↔ FAI4	192.168.1.36	255.255.255.252

Dans chaque routeur, on doit attribuer une configurations afin que les routeurs de chaque LAN puissent communiquer entre eux pour avoir la connectivité entre chaque LAN.
Voici un exemple de configuration :
Pour le FAI 1 :

```
interface GigabitEthernet0/0
 ip address 192.168.1.25 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.1.0
 default-information originate
 no auto-summary
```

Pour le LAN 1 :

```
interface GigabitEthernet0/1
 ip address 192.168.1.26 255.255.255.252
 duplex auto
 speed auto
router rip
 version 2
 network 172.16.0.0
 network 192.168.1.0
 no auto-summary
!
```

7. Mise en place du NAT.

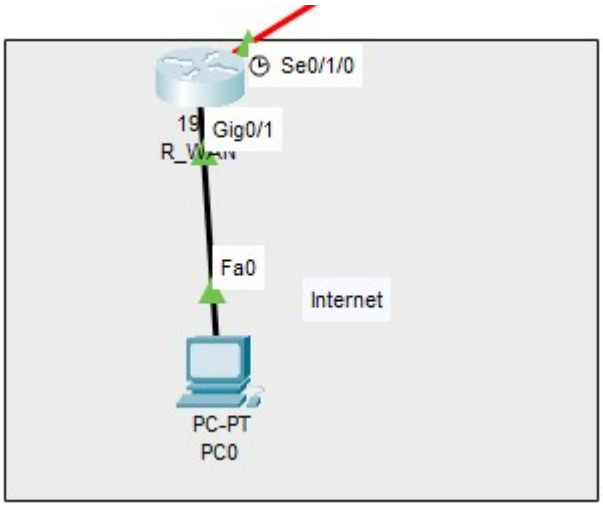
Pour mettre en place le NAT, nous allons choisir le routeur FAI 1 pour l'héberger. Ce routeur aura une interface connectée vers notre réseau interne, c'est à dire vers les autres routeurs FAI et une autre connectée au WAN.

On prendra donc l'interface G0/0 pour l'interface interne qui sera connecté aux autres FAI et LANs ainsi que l'interface Serial0/1/1 connecté à l'interface externe, le WAN.

Sur l'interface S0/1/1 du routeur FAI_1, on attribuera l'adresse 161.3.36.33/28 qui sera connecté au port S0/1/0 du routeur R_WAN en 161.3.36.34/28.

```
interface Serial0/1/1
 ip address 161.3.36.33 255.255.255.240
 ip nat outside
interface Serial0/1/0
 ip address 161.3.36.34 255.255.255.240
 clock rate 2000000
```

De plus, on aura un port en g0/1 sur ce même routeur pour le connecter à un PC qui simulera internet en 192.168.100.1.



On rajoutera sur ce routeur, un interface en loopback 0 avec l'ip adresse 8.8.8.8 (adresse de google), ainsi qu'une route par défaut pour aller à l'adresse 161.3.36.34 qui est l'interface S0/1/1 du routeur FAI.

```
interface Loopback0
 ip address 8.8.8.8 255.255.255.255
```

routeur FAI :

```
ip route 0.0.0.0 0.0.0.0 161.3.36.34
```

Ensuite, on configure le nat sur le routeur FAI_1 afin que chaque serveur web ai sa propre adresse en 161.3.36.32/28 sur les ports 80 (http) et 443 (https).

```
ip nat inside source list 1 interface Serial0/1/1 overload
ip nat inside source static tcp 172.16.105.3 80 161.3.36.35 80
ip nat inside source static tcp 172.16.105.3 443 161.3.36.35 443
ip nat inside source static tcp 172.16.68.67 80 161.3.36.36 80
ip nat inside source static tcp 172.16.68.67 443 161.3.36.36 443
ip nat inside source static tcp 172.16.9.3 80 161.3.36.37 80
ip nat inside source static tcp 172.16.9.3 443 161.3.36.37 443
ip nat inside source static tcp 172.16.102.67 80 161.3.36.38 80
ip nat inside source static tcp 172.16.102.67 443 161.3.36.38 443
ip nat inside source static 172.16.105.3 161.3.36.35
```

on met dans les interfaces, les ip nat inside et outside:

```
interface Serial0/0/0
 ip address 192.168.1.1 255.255.255.252
 ip nat inside
!
interface Serial0/0/1
 ip address 192.168.1.5 255.255.255.252
 ip nat inside
!
interface Serial0/1/0
 ip address 192.168.1.9 255.255.255.252
 ip nat inside
!
interface Serial0/1/1
 ip address 161.3.36.33 255.255.255.240
 ip nat outside
!
```

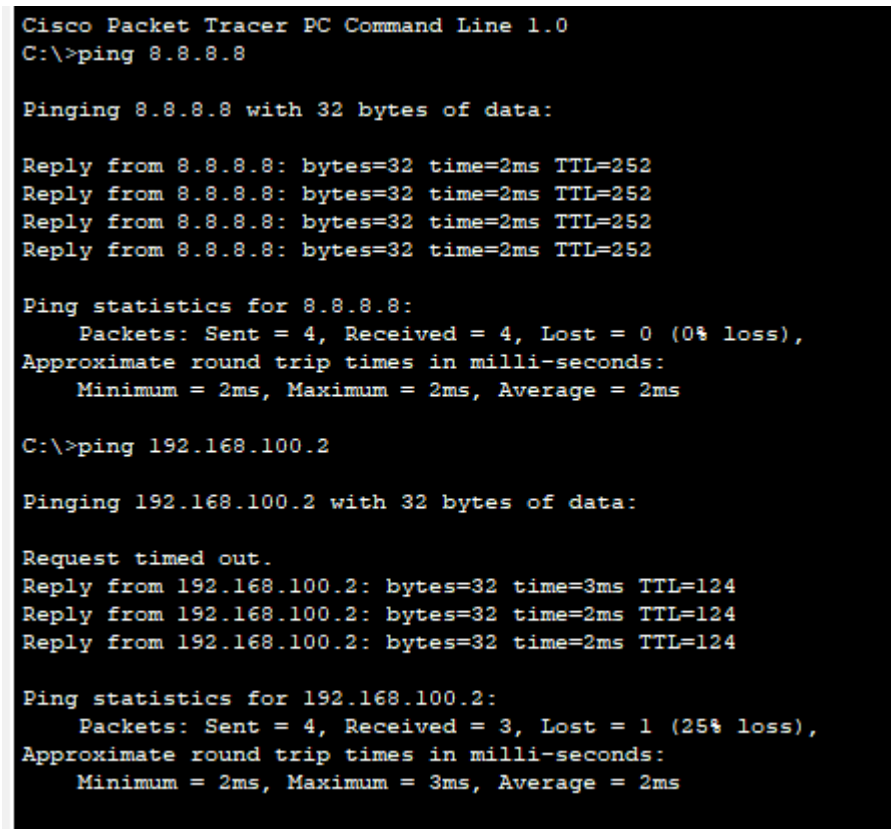
Sur le routeur FAI_1, on met aussi des ACL afin de permettre le réseau 172.16.0.0 de passer (adresse de différentes machines de chaque LAN) ainsi que le réseau 192.168.1.0 qui permet la connectivité entre les LANs et les routeurs FAI.

```
access-list 1 permit 192.168.1.0 0.0.0.3
access-list 1 permit 172.16.0.0 0.0.255.255
!
```

Pour finir, on rajoutera une ip sur le routeur R_WAN afin de faire une liaison entre le 161.3.36.32 et 161.3.36.33

```
ip classless
ip route 161.3.36.32 255.255.255.240 161.3.36.33
!
```

Il fait une liaison entre le réseau (161.3.36.32) et le routeur FAI1 (161.3.36.33°
Une fois terminé, on fait des test avec les machines de différents réseaux pour voir si ça fonctionne.



8. Mise en place ACL

Dans cette partie du projet, j'ai configuré les Listes de Contrôle d'Accès (ACLs) pour sécuriser le réseau et gérer les flux de données, comme demandé dans le cahier des charges. Mon objectif était de filtrer le trafic entre les différents VLANs de chaque site (LAN) et de contrôler les accès depuis et vers Internet (le WAN).

Ma Démarche :

Pour cela, j'ai utilisé des ACLs étendues nommées. J'ai choisi ce type d'ACL car elles permettent un filtrage plus précis (basé sur les adresses IP source et destination, les protocoles et les ports) et sont plus faciles à identifier grâce à leur nom. La convention de nommage que j'ai adoptée est ACL_VLAN_{num_du_vlan} (par exemple, ACL_VLAN_10 pour le VLAN 10).

Ces ACLs ont été appliquées en entrée (in) sur les sous-interfaces VLAN des routeurs de chaque LAN (R_LAN1, R_LAN2, R_LAN3, R_LAN4). Cela permet de vérifier le trafic dès qu'il provient d'un VLAN et essaie d'entrer dans le routeur pour aller ailleurs. Pour le routeur FAI_1, qui gère la connexion à Internet, j'ai appliqué une ACL spécifique en entrée sur son interface WAN pour filtrer le trafic venant de l'extérieur.

Principaux Ports et Protocoles Gérés :

J'ai configuré les ACLs pour gérer les protocoles et ports suivants, essentiels au fonctionnement et à la sécurité du réseau :

- **WEB :** TCP port 80 (HTTP, mot-clé www) et TCP port 443 (HTTPS).
- **DNS :** UDP port 53 (mot-clé domain) pour la résolution des noms.
- **TFTP :** UDP port 69 (mot-clé tftp) pour la sauvegarde des configurations des routeurs.
- **FTP :** TCP port 21 (mot-clé ftp pour la commande) et TCP port 20 (pour les données).
- **ICMP :** Pour les tests de connectivité (ping) et certains messages d'erreur réseau.

Exemple :

Sur le FAI_1 :

```
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit 192.168.2.0 0.0.0.3
ip access-list extended ACL_WAN
 deny ip any 172.16.105.96 0.0.0.7
 deny ip any 172.16.68.96 0.0.0.15
 deny ip any 172.16.9.128 0.0.0.15
 deny ip any 172.16.102.128 0.0.0.31
 permit tcp any host 161.3.36.35 eq www
 permit tcp any host 161.3.36.35 eq 443
 permit tcp any host 161.3.36.36 eq www
 permit tcp any host 161.3.36.36 eq 443
 permit tcp any host 161.3.36.37 eq www
 permit tcp any host 161.3.36.37 eq 443
 permit tcp any host 161.3.36.38 eq www
 permit tcp any host 161.3.36.38 eq 443
 permit tcp any any established
 permit icmp any any echo-reply
 permit icmp any any unreachable
```

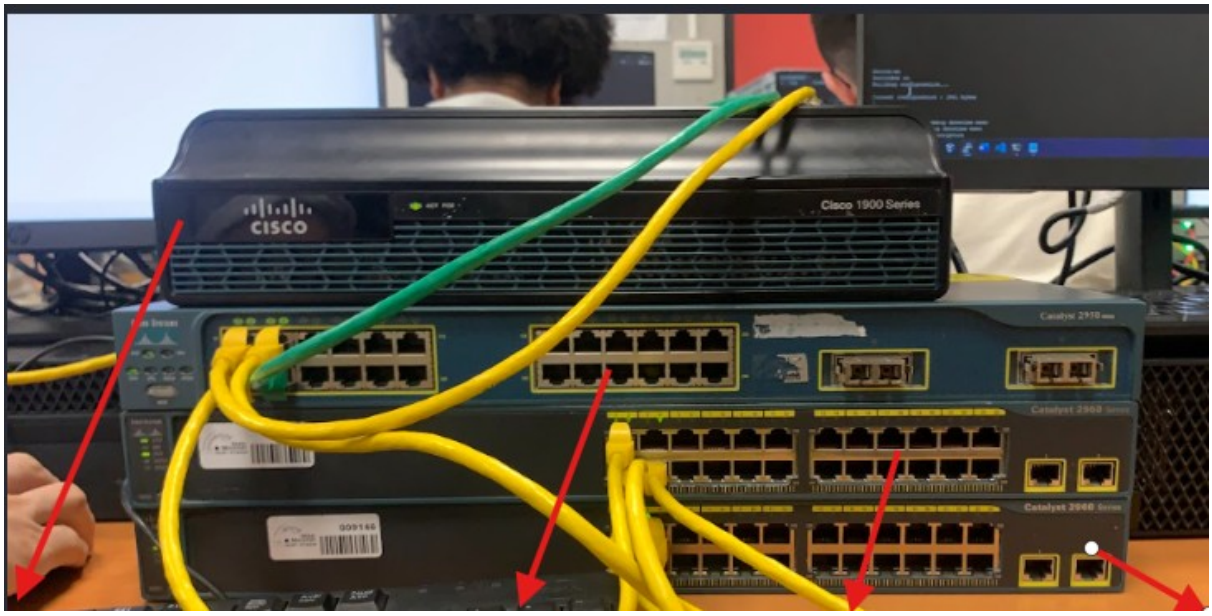
Sur router du LAN1 :

```
ip access-list extended ACL_VLAN_10
 permit tcp 172.16.105.96 0.0.0.7 host 8.8.8.8 eq www
 permit tcp 172.16.105.96 0.0.0.7 host 8.8.8.8 eq 443
 permit udp 172.16.105.96 0.0.0.7 host 8.8.8.8 eq domain
 permit udp 172.16.105.96 0.0.0.7 host 172.16.105.99 eq tftp
 permit udp 172.16.105.96 0.0.0.7 host 172.16.68.99 eq tftp
 permit udp 172.16.105.96 0.0.0.7 host 172.16.9.131 eq tftp
 permit udp 172.16.105.96 0.0.0.7 host 172.16.102.131 eq tftp
 permit icmp 172.16.105.96 0.0.0.7 any
ip access-list extended ACL_VLAN_20
 permit tcp 172.16.105.0 0.0.0.63 host 172.16.102.70 eq ftp
 permit tcp 172.16.105.0 0.0.0.63 host 8.8.8.8 eq www
 permit tcp 172.16.105.0 0.0.0.63 host 8.8.8.8 eq 443
 permit udp 172.16.105.0 0.0.0.63 host 8.8.8.8 eq domain
 permit tcp 172.16.105.0 0.0.0.63 any eq www
 permit tcp 172.16.105.0 0.0.0.63 any eq 443
 deny ip 172.16.105.0 0.0.0.63 172.16.105.64 0.0.0.31
 permit icmp 172.16.105.0 0.0.0.63 host 172.16.105.99
 permit icmp 172.16.105.0 0.0.0.63 host 172.16.68.99
 permit icmp 172.16.105.0 0.0.0.63 host 172.16.9.131
 permit icmp 172.16.105.0 0.0.0.63 host 172.16.102.131
 deny ip 172.16.105.0 0.0.0.63 172.16.105.96 0.0.0.7
 permit ip 172.16.105.0 0.0.0.63 any
 permit tcp 172.16.105.0 0.0.0.63 host 172.16.102.70 eq 20
ip access-list extended ACL_VLAN_30
 permit tcp 172.16.104.0 0.0.0.127 host 8.8.8.8 eq www
 permit tcp 172.16.104.0 0.0.0.127 host 8.8.8.8 eq 443
 permit udp 172.16.104.0 0.0.0.127 host 8.8.8.8 eq domain
 permit tcp 172.16.104.0 0.0.0.127 any eq www
 permit ip 172.16.104.0 0.0.0.127 172.16.104.128 0.0.0.127
 permit ip 172.16.104.0 0.0.0.127 172.16.105.64 0.0.0.31
 permit icmp 172.16.104.0 0.0.0.127 host 172.16.105.99
 permit icmp 172.16.104.0 0.0.0.127 host 172.16.68.99
 permit icmp 172.16.104.0 0.0.0.127 host 172.16.9.131
 permit icmp 172.16.104.0 0.0.0.127 host 172.16.102.131
 deny ip 172.16.104.0 0.0.0.127 172.16.105.96 0.0.0.7
 permit icmp 172.16.104.0 0.0.0.127 any
 permit ip 172.16.104.0 0.0.0.127 any
 permit tcp 172.16.104.0 0.0.0.127 any eq 443
ip access-list extended ACL_VLAN_40
 permit tcp 172.16.104.128 0.0.0.127 host 8.8.8.8 eq www
 permit tcp 172.16.104.128 0.0.0.127 host 8.8.8.8 eq 443
 permit udp 172.16.104.128 0.0.0.127 host 8.8.8.8 eq domain
 permit tcp 172.16.104.128 0.0.0.127 any eq www
 permit tcp 172.16.104.128 0.0.0.127 any eq 443
 permit ip 172.16.104.128 0.0.0.127 172.16.104.0 0.0.0.127
 permit icmp 172.16.104.128 0.0.0.127 host 172.16.105.99
 permit icmp 172.16.104.128 0.0.0.127 host 172.16.68.99
 permit icmp 172.16.104.128 0.0.0.127 host 172.16.9.131
 permit icmp 172.16.104.128 0.0.0.127 host 172.16.102.131
 deny ip 172.16.104.128 0.0.0.127 172.16.105.96 0.0.0.7
 permit icmp 172.16.104.128 0.0.0.127 any
 permit ip 172.16.104.128 0.0.0.127 any
 permit ip 172.16.104.128 0.0.0.127 172.16.105.64 0.0.0.31
```

```
ip access-list extended ACL_VLAN_100
 permit tcp 172.16.105.64 0.0.0.31 host 8.8.8.8 eq www
 permit tcp 172.16.105.64 0.0.0.31 host 8.8.8.8 eq 443
 permit udp 172.16.105.64 0.0.0.31 host 8.8.8.8 eq domain
 permit tcp 172.16.105.64 0.0.0.31 any eq www
 permit tcp 172.16.105.64 0.0.0.31 any eq 443
 permit tcp 172.16.105.64 0.0.0.31 host 172.16.102.70 eq 20
 permit tcp 172.16.105.64 0.0.0.31 host 172.16.102.70 eq ftp
 permit ip 172.16.105.64 0.0.0.31 172.16.104.0 0.0.0.127
 permit ip 172.16.105.64 0.0.0.31 172.16.104.128 0.0.0.127
 deny ip 172.16.105.64 0.0.0.31 172.16.105.0 0.0.0.63
 permit icmp 172.16.105.64 0.0.0.31 host 172.16.105.99
 permit icmp 172.16.105.64 0.0.0.31 host 172.16.68.99
 permit icmp 172.16.105.64 0.0.0.31 host 172.16.9.131
 permit icmp 172.16.105.64 0.0.0.31 host 172.16.102.131
 deny ip 172.16.105.64 0.0.0.31 172.16.105.96 0.0.0.7
 permit icmp 172.16.105.64 0.0.0.31 any
 permit ip 172.16.105.64 0.0.0.31 any
!
```

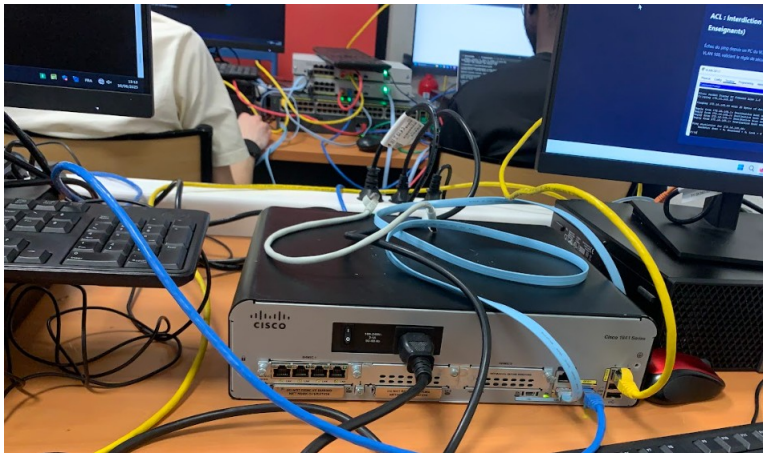
On a dû configurer un LAN en particulier pour construire en réel le réseau qu'on a configuré sur packet tracer.
On a donc choisi le LAN 2, on a mis sur le PC de gauche, le vlan 10 (c'est celui qui héberge le serveur TFTP), celui du milieu est en vlan 20 (le serveur WEB), et enfin le PC de droite en vlan 40.
On a donc configuré sur ces PC, leurs adresses IP respectives pour chaque VLAN.

Pour cette configuration, on a besoin de 3 switchs pour simuler les 3 bâtiments dans le LAN. Un routeur LAN_2 pour faire passer les sous interfaces et le connecté au routeur FAI qui fera la connexion entre les autres LANs.



router LAN 2 SWC SWB SWA

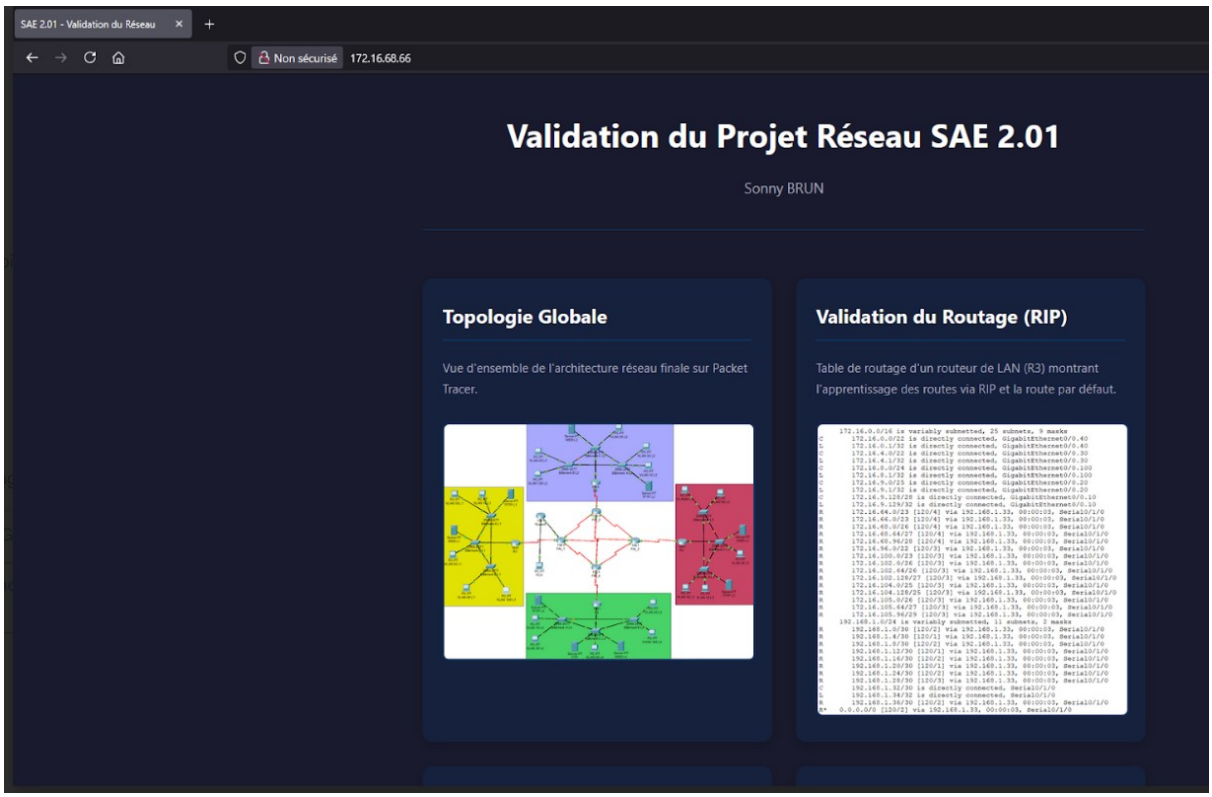
Le routeur LAN 2 sera connecté au routeur FAI:



On fait des tests à l'aide de la commande ping pour voir si la connectivité fonctionne.

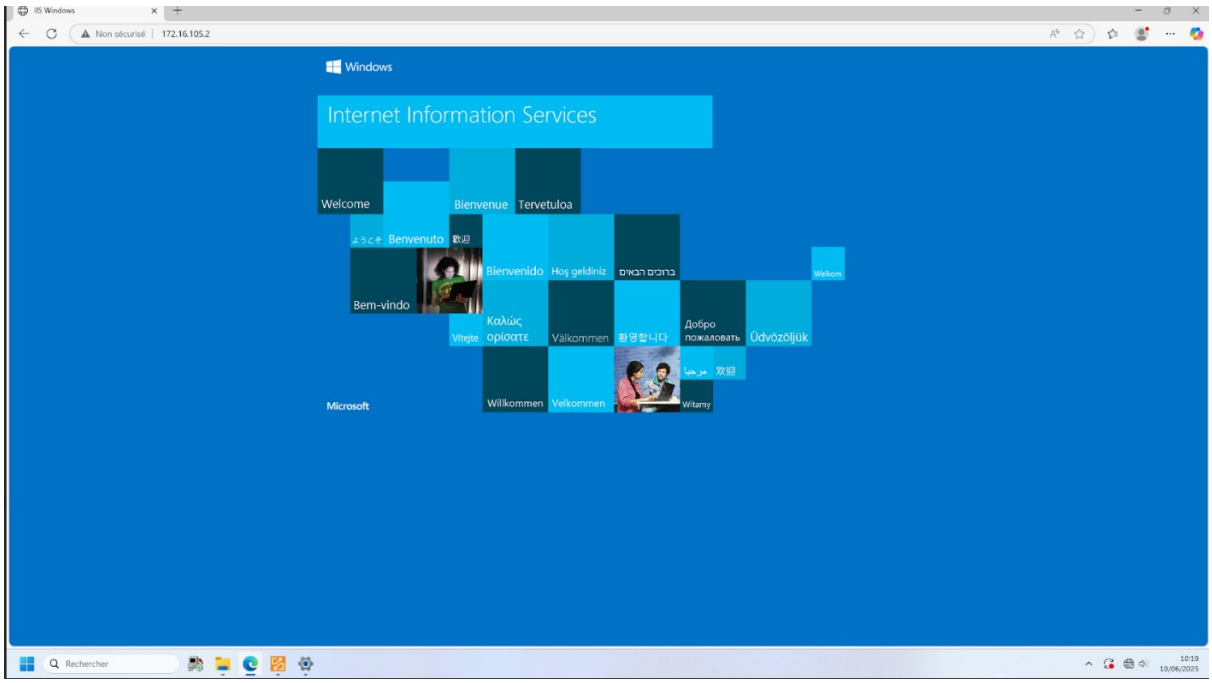
```
Router#ping 192.168.1.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#ping 192.168.1.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#ping 192.168.1.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router#ping 192.168.1.26
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.26, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Ensuite le VLAN 10 et VLAN 20 représenteront respectivement le serveur TFTP et le serveur WEB.
On installe alors pour le VLAN 10, tftp_d et pour le WLAN 20, XAMPP
Une fois ces installations faites, on teste depuis un VLAN différent par exemple, le VLAN 40 si on arrive à accéder à la page WEB.



On voit ici que ça fonctionne bien.

On passe maintenant à l'interconnectivité entre les LAN (2 Routeur FAI connecté entre eux) et on test pour savoir si on peut accéder à leurs page web depuis notre LAN.



Enfin, nous avons ajoutés des ACL afin de faire passer ou d'interdire les requête entre chaque PC du LAN ou entre le réseau WAN.

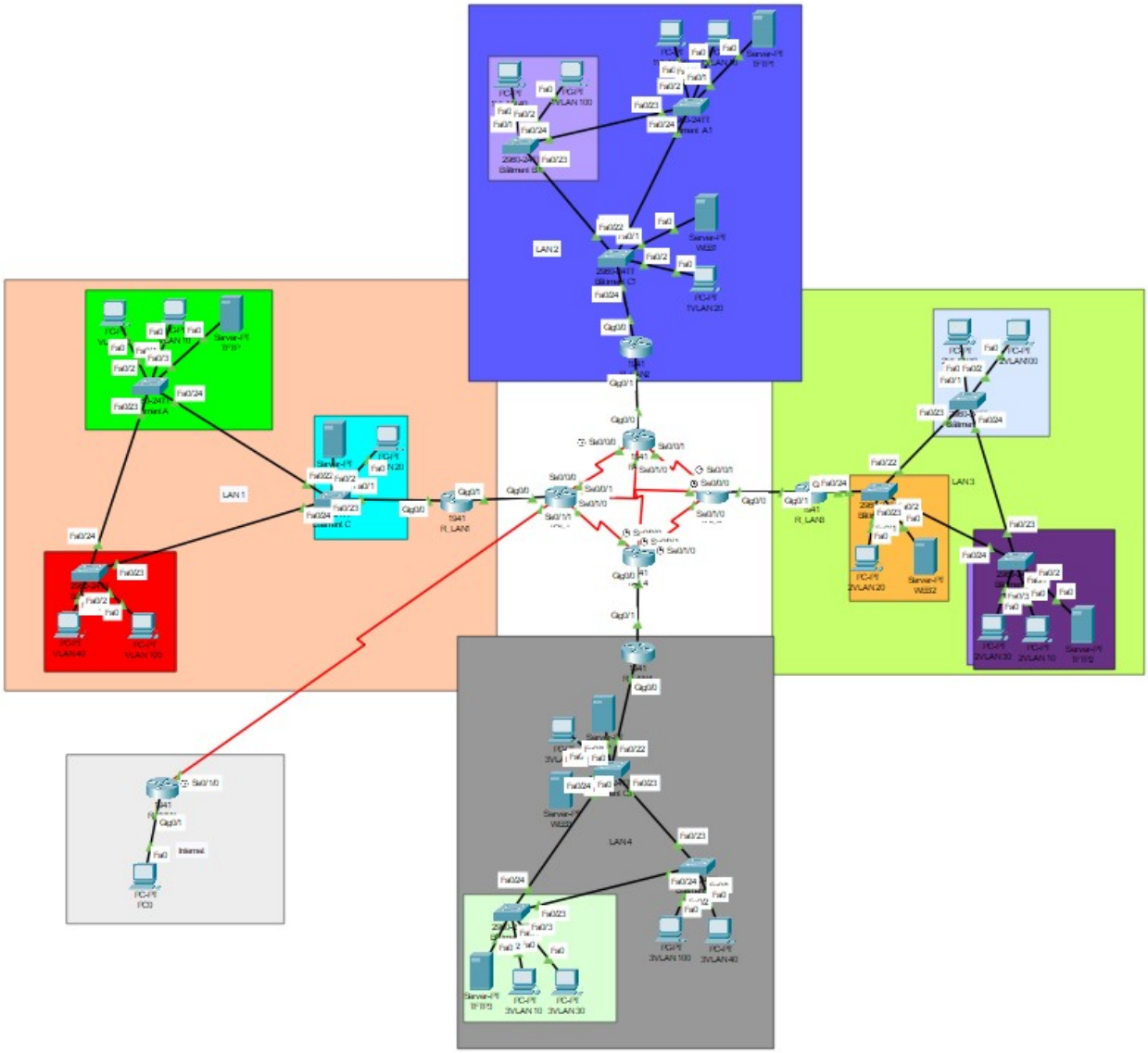
Voici un exemple d'un bout de configuration:

```
 permit icmp any host 172.16.68.98 echo
 permit icmp any host 172.16.9.130 echo
 permit icmp any host 172.16.102.130 echo
 permit tcp 172.16.68.0 0.0.0.63 host 172.16.102.68 eq ftp
 deny   ip 172.16.68.0 0.0.0.63 172.16.105.0 0.0.0.63
 deny   ip 172.16.68.0 0.0.0.63 172.16.68.64 0.0.0.31
 deny   ip 172.16.68.0 0.0.0.63 172.16.9.0 0.0.0.127
 deny   ip 172.16.68.0 0.0.0.63 172.16.102.64 0.0.0.63
 deny   ip any 172.16.105.96 0.0.0.7
 deny   ip any 172.16.68.96 0.0.0.15
 deny   ip any 172.16.9.128 0.0.0.15
 deny   ip any 172.16.102.128 0.0.0.31
ip access-list extended ACL_SERVICES_IN_L2
 permit tcp any any established
 permit icmp any any echo-reply
 permit tcp 172.16.68.64 0.0.0.31 host 172.16.102.68 eq ftp
 permit tcp 172.16.68.64 0.0.0.31 host 172.16.105.2 eq www
 permit tcp 172.16.68.64 0.0.0.31 host 172.16.68.66 eq www
 permit tcp 172.16.68.64 0.0.0.31 host 172.16.9.2 eq www
 permit tcp 172.16.68.64 0.0.0.31 host 172.16.102.66 eq www
 permit icmp 172.16.68.64 0.0.0.31 host 172.16.105.98 echo
 permit icmp 172.16.68.64 0.0.0.31 host 172.16.68.98 echo
 permit icmp 172.16.68.64 0.0.0.31 host 172.16.9.130 echo
 permit icmp 172.16.68.64 0.0.0.31 host 172.16.102.130 echo
 deny   ip 172.16.68.64 0.0.0.31 172.16.105.64 0.0.0.31
 deny   ip 172.16.68.64 0.0.0.31 172.16.68.0 0.0.0.63
 deny   ip 172.16.68.64 0.0.0.31 172.16.8.0 0.0.0.255
 deny   ip 172.16.68.64 0.0.0.31 172.16.102.0 0.0.0.63
 deny   ip 172.16.68.64 0.0.0.31 172.16.105.96 0.0.0.7
 deny   ip 172.16.68.64 0.0.0.31 172.16.68.96 0.0.0.15
 deny   ip 172.16.68.64 0.0.0.31 172.16.9.128 0.0.0.15
 deny   ip 172.16.68.64 0.0.0.31 172.16.102.128 0.0.0.31
```

```
ip access-list extended ACL_ADMIN_IN_L2
 permit tcp any any established
 permit icmp any any echo-reply
 permit tcp 172.16.68.96 0.0.0.15 any eq www
 permit tcp 172.16.68.96 0.0.0.15 any eq 443
 permit icmp 172.16.68.96 0.0.0.15 host 8.8.8.8 echo
 permit udp 172.16.68.96 0.0.0.15 host 172.16.105.98 eq tftp
 permit udp 172.16.68.96 0.0.0.15 host 172.16.68.98 eq tftp
 permit udp 172.16.68.96 0.0.0.15 host 172.16.9.130 eq tftp
 permit udp 172.16.68.96 0.0.0.15 host 172.16.102.130 eq tftp
 permit tcp 172.16.68.96 0.0.0.15 host 172.16.105.2 eq www
 permit tcp 172.16.68.96 0.0.0.15 host 172.16.68.66 eq www
 permit tcp 172.16.68.96 0.0.0.15 host 172.16.9.2 eq www
 permit tcp 172.16.68.96 0.0.0.15 host 172.16.102.66 eq www
ip access-list extended ACL_ETUD_ENS_IN_L2
 permit tcp any any established
 permit icmp any any echo-reply
 permit ip any 172.16.104.0 0.0.0.127
 permit ip any 172.16.104.128 0.0.0.127
 permit ip any 172.16.105.64 0.0.0.31
 permit ip any 172.16.64.0 0.0.1.255
 permit ip any 172.16.66.0 0.0.1.255
 permit ip any 172.16.68.0 0.0.0.63
 permit ip any 172.16.4.0 0.0.3.255
 permit ip any 172.16.0.0 0.0.3.255
 permit ip any 172.16.8.0 0.0.0.255
 permit ip any 172.16.100.0 0.0.1.255
 permit ip any 172.16.96.0 0.0.3.255
 permit ip any 172.16.102.0 0.0.0.63
 permit tcp any any eq www
 permit tcp any any eq 443
 permit icmp any host 8.8.8.8 echo
 permit tcp any host 172.16.105.2 eq www
 permit tcp any host 172.16.68.66 eq www
 permit tcp any host 172.16.9.2 eq www
 permit tcp any host 172.16.102.66 eq www
 permit icmp any host 172.16.105.98 echo
```

Remarque: pour le TFTP, on a essayé de copier la conf de chaque équipement à l’aide de la commande copy running-config tftp et le petit souci est que les fichiers .txt des configurations des équipements apparaissaient sans contenues à l'intérieur.

On peut en conclure qu’il fallait avoir les droits afin de pouvoir récupérer les configurations.


LAN1
LAN2
LAN3
LAN4
R_LAN8
Internet