Document technique

AP – SISR

Segmentation d’un réseau

Dates du projet :
Début le 03/04/2026
Fin le 10/04/2026

Ouahli Ilian
Bardet Arthur
Olympe Soussou

Sommaire

Table des matières

Présentation du contexte

La Maison des Ligues fait appel à l'entreprise *NetworkSI*, une SSII dans laquelle nous intervenons en tant que techniciens réseau. Après avoir déjà déployé une infrastructure comprenant un contrôleur de domaine et des services centralisés, l'organisation souhaite désormais renforcer la sécurité et l'architecture de son réseau.

Dans cette optique, la Maison des Ligues a décidé de cloisonner son réseau afin de mieux segmenter les différents services internes et contrôler les flux de communication. Cette évolution repose sur la mise en place de VLAN (Virtual Local Area Network) ainsi que sur l'utilisation du routage Inter-VLAN, permettant une communication maîtrisée entre les différentes zones du réseau.

L'infrastructure physique existante s'appuie sur :

- Des switches Cisco Catalyst 2960 présents à chaque étage
- Un routeur Cisco 2901/2911 assurant le routage
- Une interconnexion des baies via fibre optique vers une baie centrale

Chaque service de l'entreprise est désormais isolé dans un VLAN dédié avec un plan d'adressage IP spécifique. Certains environnements sensibles comme les serveurs (Active Directory, NextCloud) ou les zones visiteurs et démonstration font l'objet de restrictions d'accès strictes.

Par ailleurs, l'entreprise impose :

- **Une gestion fine des droits d'accès entre les VLAN**
- **Une administration sécurisée en SSH**
- **Une sauvegarde des configurations réseau via un serveur TFTP**
- **Une continuité de service avec des règles d'accès clairement définies**

L'ensemble de la solution devra être maquetté et validé dans un environnement de simulation (Packet Tracer) avant déploiement réel.

Les objectifs attendus

Les objectifs attendus

Cet atelier professionnel a pour objectif de développer des compétences avancées en administration réseau et sécurité des infrastructures.

Les principaux objectifs sont :

- **Mettre en place une segmentation réseau via VLAN**
- **Configurer le routage Inter-VLAN pour permettre les communications autorisées**
- **Déployer des ACL (Access Control Lists) afin de contrôler les flux entre les différentes zones**
- **Sécuriser l'administration des équipements via SSH**
- **Assurer la sauvegarde des configurations sur un serveur TFTP**
- **Vérifier les droits d'accès aux services critiques (Active Directory, NextCloud, Internet)**
- **Réaliser des tests de validation de l'infrastructure**

Voici ci-dessous la liste de nos différentes tâches :

A.1 Réalisation du schéma réseau

A.2 Mise en place de l'accès distant SSH

A.3 Création des Vlan

A.4 Routage InterVlan

A.5 Tests

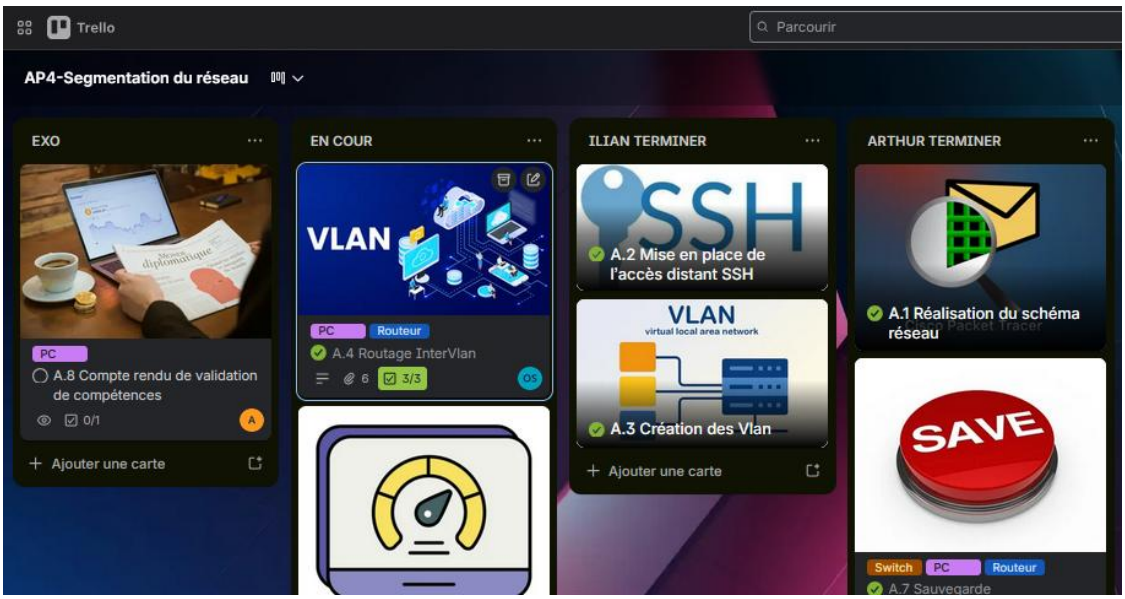
A.6 Réalisation des ACL

A.7 Sauvegarde

Comment travailler en binôme ?

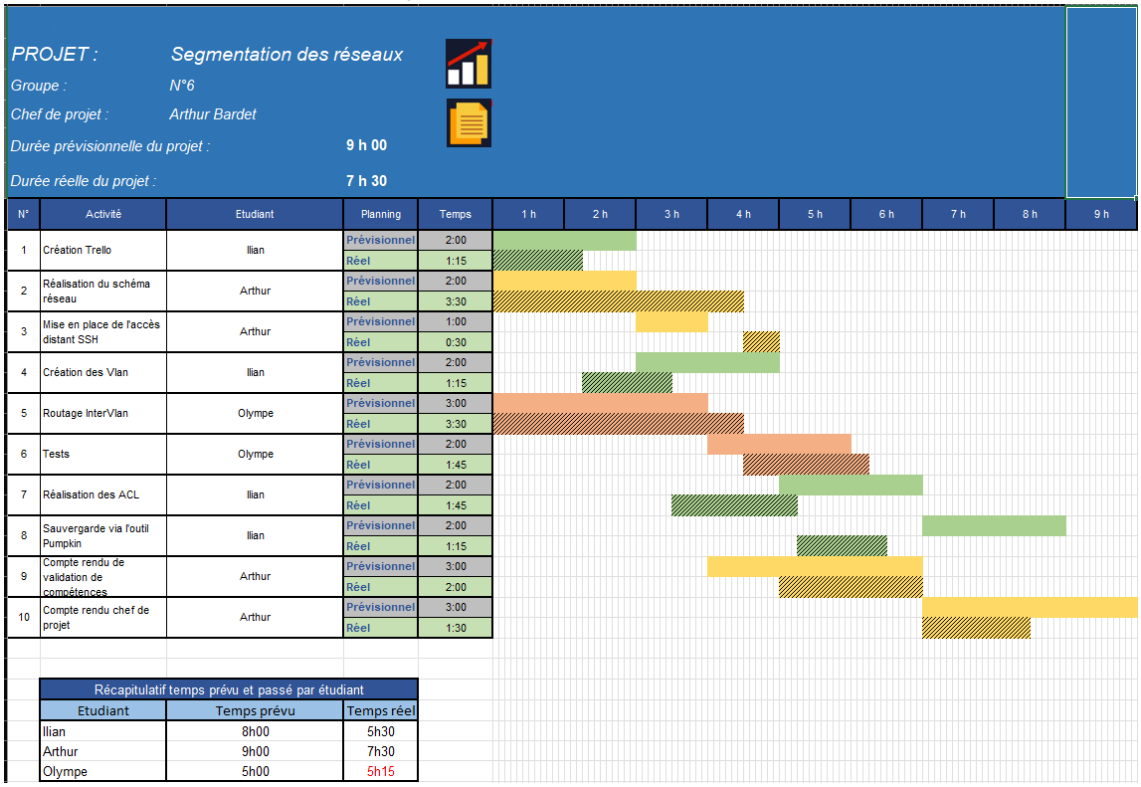
Pour réaliser ce travail, il faut répartir les tâches entre les membres du groupe de travail. Comme vu ci-dessus, on va utiliser le logiciel « Trello » qui va nous permettre de faire cela. La répartition des tâches se fait également à l'aide des compétences déjà acquises.

« Capture d'écran de l'appli Trello et de nos activités »



Notre deuxième outil a été Gantt qui nous a servi à nous repérer dans le temps. C'est-à-dire qu'il nous a permit de nous fixer un planning de travail. Puis au fur et à mesure, on renseigne le temps que l'on a réellement utilisé pour savoir où l'on en a perdu ou non.

« Capture d'écran de notre Gantt »



PROJET : Segmentation des réseaux
Groupe : N°6
Chef de projet : Arthur Bardet
Durée prévisionnelle du projet : 9 h 00
Durée réelle du projet : 7 h 30

N°	Activité	Etudiant	Planning	Temps
1	Création Trello	Ilian	Prévisionnel	2:00
			Réel	1:15
2	Réalisation du schéma réseau	Arthur	Prévisionnel	2:00
			Réel	3:30
3	Mise en place de l'accès distant SSH	Arthur	Prévisionnel	1:00
			Réel	0:30
4	Création des Vlan	Ilian	Prévisionnel	2:00
			Réel	1:15
5	Routage InterVlan	Olympe	Prévisionnel	3:00
			Réel	3:30
6	Tests	Olympe	Prévisionnel	2:00
			Réel	1:45
7	Réalisation des ACL	Ilian	Prévisionnel	2:00
			Réel	1:45
8	Sauvergarde via l'outil Pumpkin	Ilian	Prévisionnel	2:00
			Réel	1:15
9	Compte rendu de validation de compétences	Arthur	Prévisionnel	3:00
			Réel	2:00
10	Compte rendu chef de projet	Arthur	Prévisionnel	3:00
			Réel	1:30

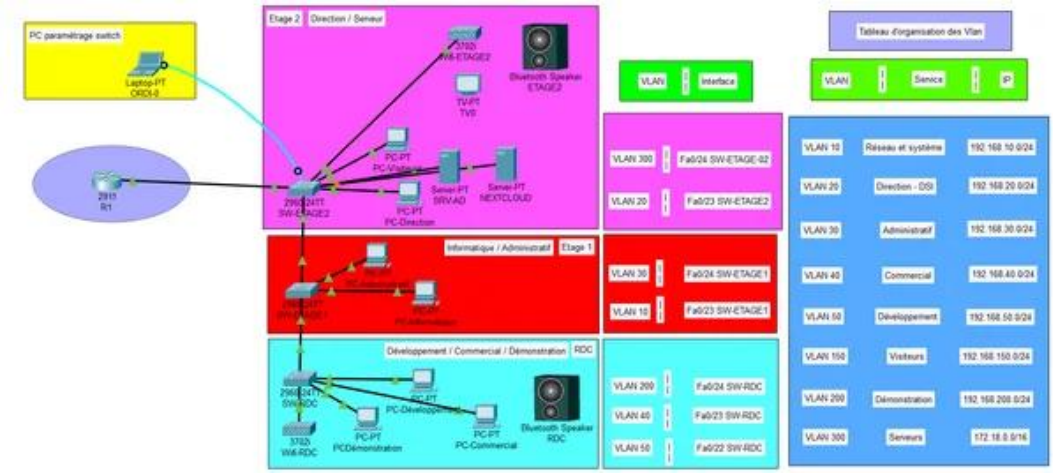
Récapitulatif temps prévu et passé par étudiant		
Etudiant	Temps prévu	Temps réel
Ilian	8h00	5h30
Arthur	9h00	7h30
Olympe	5h00	5h15

A.1 Réalisation du schéma réseau

Pour cette activité, il faut réaliser un schéma réseau. Pour se faire je me suis rendu sur le logiciel CISCO PACKET TRACER utilisé en cours. A l'aide des différente possibilités du logiciel il faut réaliser cette maquette le plus réaliste possible.

Pour faire correctement se schéma, on c'est inspiré et aidé des différents schéma réalisé en cours. Pour être le plus réaliste possible, il a fallut prendre connaissance du document évaluer le nombre minimum de PC et équipement réseau à utiliser. Il a également fallut penser à diviser les zones ainsi que penser à bien nommé les postes étages, switch etc...

« Capture schéma réseau »



A.2 Mise en place de l’accès distant SSH

Dans le cadre de cette activité, nous avons configuré un accès distant sécurisé via le protocole SSH sur un switch afin de permettre son administration à distance en toute sécurité.

La première étape a consisté à définir les éléments d’identification de l’équipement :

- **Attribution d’un nom d’hôte unique**
- **Configuration d’un nom de domaine nécessaire à la génération des clés de chiffrement**

Ensuite, une paire de clés RSA a été générée avec un modulus de 2048 bits afin d’assurer un niveau de sécurité suffisant pour les échanges chiffrés.

Le protocole SSH version 2 a ensuite été activé, garantissant un chiffrement sécurisé des connexions distantes.

La configuration s’est poursuivie par le paramétrage des lignes virtuelles (VTY) :

- **Restriction des accès pour n’autoriser que le protocole SSH**
- **Activation de l’authentification locale pour sécuriser l’accès aux équipements**

Cette configuration permet ainsi de remplacer les accès non sécurisés (comme Telnet) par une solution fiable et conforme aux bonnes pratiques de sécurité.

Bien que la mise en place de SSH soit techniquement simple, elle a entraîné une perte de temps imprévue, notamment en raison de certaines étapes de configuration nécessitant de la rigueur et des vérifications.

Au final, cette activité m'a permis de comprendre l'importance de la sécurisation des accès distants ainsi que les étapes nécessaires à la mise en œuvre d'un accès administrateur fiable sur un équipement réseau.

A.3 Création des Vlan

Mise en place des VLAN et du protocole VTP

Dans le cadre de cette activité, nous avons mis en place une segmentation du réseau à l'aide de VLAN, ainsi que la configuration du protocole VTP (VLAN Trunking Protocol) afin de centraliser la gestion des VLAN sur plusieurs commutateurs.

Configuration du switch principal (étage 2)

Le switch du deuxième étage a été défini comme nœud central du domaine VTP. Les actions suivantes ont été réalisées :

- **Définition d'un nom de domaine VTP afin d'identifier le réseau**
- **Configuration du switch en mode serveur, lui permettant de créer, modifier et supprimer les VLAN**
- **Mise en place d'une sécurisation du domaine VTP via un mot de passe**

Les VLAN demandés ont ensuite été créés sur ce switch à l'aide des commandes appropriées (numéro et nom des VLAN).

Intégration des switches secondaires

Les switches des autres étages ont été intégrés au domaine VTP :

- **Configuration en mode client, leur permettant de recevoir automatiquement les VLAN depuis le serveur**
- **Mise en place de liaisons trunk (802.1Q) entre les switches afin d'assurer la propagation des informations VTP**

Une fois la configuration terminée, les VLAN créés sur le switch principal ont été automatiquement répliqués sur les autres équipements.

Affectation des VLAN aux ports

Les ports des switches ont ensuite été configurés en fonction des besoins de chaque étage :

- **Étage 2 : VLAN 20, 150 et 300**
- **Étage 1 : VLAN 10 et 30**
- **Rez-de-chaussée : VLAN 40, 50 et 200**

Retour sur l'activité

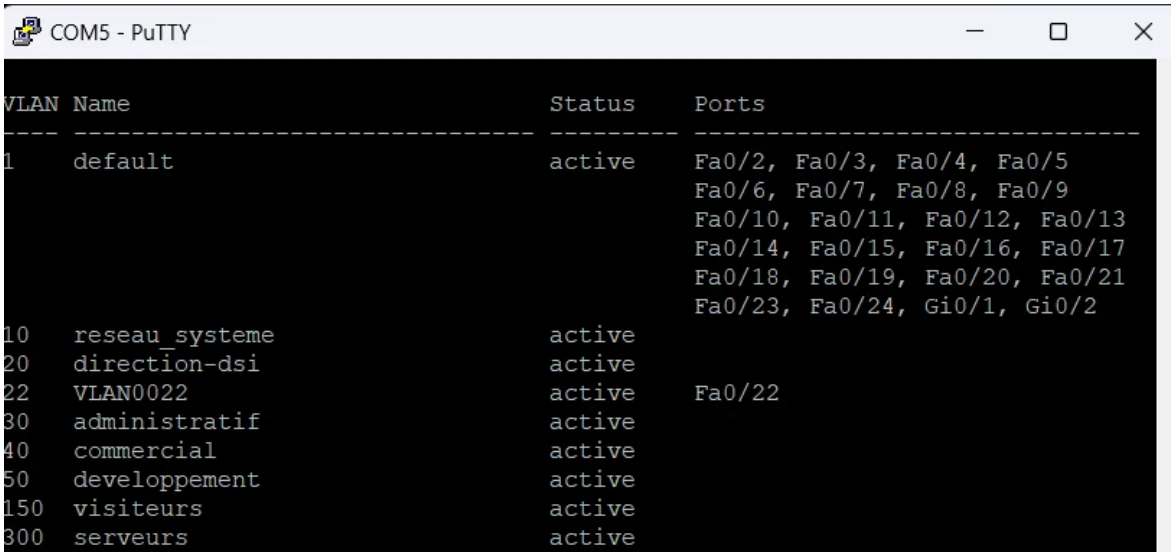
L'activité s'est révélée globalement simple à mettre en œuvre, notamment pour la création et la propagation des VLAN via VTP.

La principale difficulté rencontrée a concerné l'identification précise des ports physiques sur les switches, étape essentielle pour garantir une affectation correcte des interfaces aux différents VLAN.

Cette activité m'a permis de mieux comprendre :

- **La segmentation réseau via VLAN**
- **Le fonctionnement du VTP pour la gestion centralisée**
- **L'importance de la rigueur dans la configuration des ports**

« Capture création Vlans »



La commande « show vlan », permet de monter les Vlans créées ainsi que le nom qui leur a été donné. Comme par exemple le Vlan 10 qui porte le nom « reseau_systeme ».

A.4 Routage InterVlan

Mise en place du routage Inter-VLAN

Dans le cadre de cette activité intitulée *Routage Inter-VLAN*, l'objectif était de permettre la communication entre les différents VLAN tout en respectant la segmentation du réseau mise en place précédemment.

Pour cela, nous nous sommes appuyés sur la maquette réseau réalisée sous Cisco Packet Tracer, ainsi que sur les fiches de connaissances fournies.

Configuration des interfaces de routage

La mise en œuvre du routage Inter-VLAN a nécessité la création de sous-interfaces sur le routeur, chacune associée à un VLAN spécifique. Au total, 8 interfaces logiques ont été configurées pour correspondre aux différents services de l'entreprise.

Pour chaque VLAN :

- **Une sous-interface a été créée (ex : GigabitEthernet0/0.10 pour le VLAN 10)**
- **Un encapsulation 802.1Q a été configurée avec l'identifiant du VLAN**
- **Une adresse IP de passerelle a été attribuée pour permettre la communication des postes du VLAN**

Répartition des sous-interfaces configurées

- **VLAN 10 – Réseau & Système → G0/0.10**
- **VLAN 20 – Direction / DSI → G0/0.20**
- **VLAN 30 – Administratif → G0/0.30**
- **VLAN 40 – Commercial → G0/0.40**
- **VLAN 50 – Développement → G0/0.50**
- **VLAN 150 – Visiteurs → G0/0.150**
- **VLAN 200 – Démonstration → G0/0.200**
- **VLAN 300 – Serveurs → G0/0.300**

Chaque sous-interface joue le rôle de passerelle par défaut pour les machines de son VLAN, permettant ainsi la communication inter-réseaux via le routeur.

Résultat obtenu

Une fois la configuration terminée, les différents VLAN ont pu communiquer entre eux selon les règles définies, validant ainsi le bon fonctionnement du routage Inter-VLAN.

Retour sur l'activité

Cette activité a été globalement logique et structurée, notamment grâce à la maquette déjà réalisée en amont. Elle permet de bien comprendre le lien entre segmentation réseau (VLAN) et routage.

Cependant, elle demande de la rigueur, notamment dans :

- **La cohérence entre les numéros de VLAN et les sous-interfaces**
- **La configuration des adresses IP de passerelle**

- **L’encapsulation correcte en 802.1Q**

Au final, cette activité m’a permis de mieux comprendre le fonctionnement du routage Inter-VLAN, élément essentiel pour faire communiquer des réseaux segmentés tout en conservant un bon niveau de contrôle et de sécurité.

« Capture, résultat de la création de sous-interfaces »

```
% Invalid input detected at '^' marker.

Router(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.18.0.0/16 is directly connected, GigabitEthernet0/0.300
L        172.18.0.254/32 is directly connected, GigabitEthernet0/0.300
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L        192.168.10.254/32 is directly connected, GigabitEthernet0/0.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L        192.168.20.254/32 is directly connected, GigabitEthernet0/0.20
      192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.22.0/24 is directly connected, GigabitEthernet0/0.22
L        192.168.22.254/32 is directly connected, GigabitEthernet0/0.22
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L        192.168.30.254/32 is directly connected, GigabitEthernet0/0.30
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
L        192.168.40.254/32 is directly connected, GigabitEthernet0/0.40
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.50.0/24 is directly connected, GigabitEthernet0/0.50
L        192.168.50.254/32 is directly connected, GigabitEthernet0/0.50
      192.168.150.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.150.0/24 is directly connected, GigabitEthernet0/0.150
L        192.168.150.254/32 is directly connected, GigabitEthernet0/0.150
      192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.200.0/24 is directly connected, GigabitEthernet0/0.200
L        192.168.200.254/32 is directly connected, GigabitEthernet0/0.200
Router(config)#
```

A.5 Tests

Phase de tests et validation de la solution

Une fois l'ensemble des configurations réalisées, nous avons procédé à une phase de validation afin de vérifier la conformité de l'infrastructure avec le cahier des charges.

Pour garantir une vérification complète, une check-list de tests a été mise en place :

- **Test des accès via SSH**
- **Test du fonctionnement des VLAN**
- **Test du routage Inter-VLAN**

I. Test de l'accès SSH sur les switches

Dans le cadre des exigences de sécurité, un accès distant sécurisé via SSH a été configuré sur les switches.

Nous avons vérifié :

- **La possibilité de se connecter à distance aux équipements**
- **Le bon fonctionnement de l'authentification**
- **La stabilité de la connexion entre les différents équipements**

Les tests ont confirmé que l'accès SSH est fonctionnel et conforme aux attentes, permettant une administration sécurisée des équipements réseau.

II. Test des VLAN

Afin de valider la segmentation du réseau, nous avons effectué des tests sur les VLAN précédemment configurés.

Les vérifications ont porté sur :

- **L’affectation correcte des ports aux VLAN**
- **L’isolement des réseaux (absence de communication directe entre VLAN non autorisés)**
- **La propagation des VLAN via VTP**

Les résultats obtenus confirment que les VLAN sont correctement configurés et opérationnels, assurant une bonne séparation des différents services.

III. Test du routage Inter-VLAN

Après la mise en place du routage Inter-VLAN, des tests de connectivité ont été réalisés afin de valider la communication entre les différents réseaux.

Nous avons vérifié :

- **La communication entre VLAN autorisés via des tests de type *ping***
- **Le bon fonctionnement des passerelles configurées sur le routeur**
- **La cohérence globale du routage**

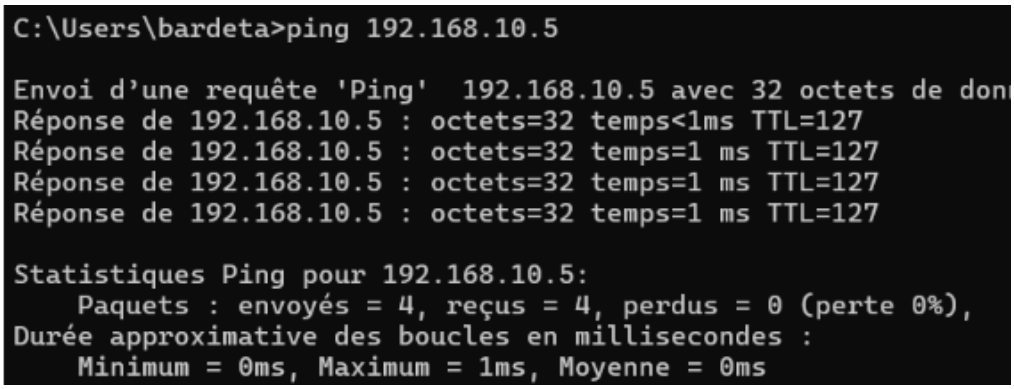
Les tests ont démontré que le routage Inter-VLAN est fonctionnel, permettant aux différents services de communiquer conformément aux règles définies.

Conclusion des tests

L’ensemble des tests réalisés est concluant. L’infrastructure mise en place répond aux exigences du cahier des charges, tant sur le plan fonctionnel que sécuritaire.

Cette phase de validation confirme que la solution est opérationnelle, cohérente et prête à être déployée dans un environnement réel.

« Capture de ping d'un Vlan vers un autre »



A.6 Réalisation des ACL

Dans le cadre de cette activité, nous avons mis en place des listes de contrôle d'accès (ACL) sur un routeur afin de filtrer et contrôler le trafic réseau entre différents segments de l'infrastructure.

La configuration a été réalisée directement sur l'équipement réseau à l'aide de commandes spécifiques. Les règles ont été définies en précisant les adresses IP source et destination, ainsi que les types de flux autorisés ou refusés. Une attention particulière a été portée à l'ordre des règles, élément essentiel pour garantir le bon fonctionnement du filtrage.

Nous avons notamment travaillé sur :

- **La création d'ACL standards et étendues**
- **L'ajout de commentaires pour faciliter la lisibilité des configurations**
- **L'autorisation de flux spécifiques, comme le trafic HTTP et HTTPS**
- **Le blocage de certains services, notamment le FTP (ports 20 et 21)**
- **L'affectation des ACL aux interfaces du routeur (en entrée ou en sortie)**
- **La vérification des ACL configurées et de leur application sur les interfaces**

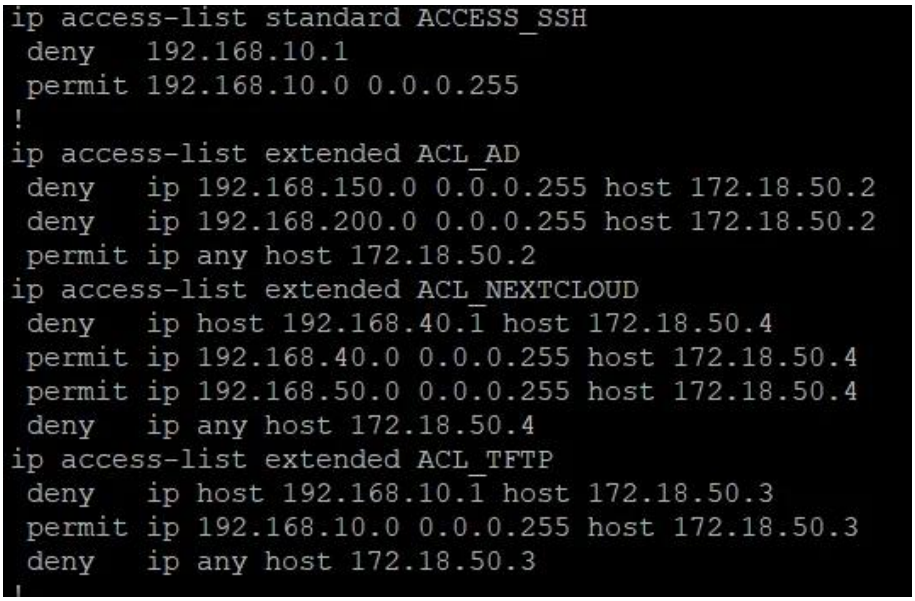
Une fois les ACL mises en place, des tests de connectivité ont été réalisés entre les différents équipements du réseau. Ces tests ont permis de valider le comportement attendu : certaines communications étaient autorisées tandis que d'autres étaient correctement bloquées en fonction des règles définies.

L'activité s'est déroulée de manière fluide et a été globalement bien comprise. Elle a nécessité de la rigueur, notamment dans la définition et l'organisation des règles de filtrage.

Au final, cette activité m'a permis de mieux comprendre le rôle des ACL dans la sécurisation d'un réseau, ainsi que leur mise en œuvre concrète

sur un équipement Cisco. Elle constitue une compétence essentielle dans l'administration et la protection des infrastructures réseau.

« Capture de la réalisation des ACL »



```
ip access-list standard ACCESS_SSH
 deny   192.168.10.1
 permit 192.168.10.0 0.0.0.255
!
ip access-list extended ACL_AD
 deny   ip 192.168.150.0 0.0.0.255 host 172.18.50.2
 deny   ip 192.168.200.0 0.0.0.255 host 172.18.50.2
 permit ip any host 172.18.50.2
ip access-list extended ACL_NEXTCLOUD
 deny   ip host 192.168.40.1 host 172.18.50.4
 permit ip 192.168.40.0 0.0.0.255 host 172.18.50.4
 permit ip 192.168.50.0 0.0.0.255 host 172.18.50.4
 deny   ip any host 172.18.50.4
ip access-list extended ACL_TFTP
 deny   ip host 192.168.10.1 host 172.18.50.3
 permit ip 192.168.10.0 0.0.0.255 host 172.18.50.3
 deny   ip any host 172.18.50.3
!
```

A.7 Sauvegarde

Sauvegarde des configurations via serveur TFTP

Dans le cadre de cette activité, nous avons réalisé la sauvegarde des configurations d'un routeur et de plusieurs switches en utilisant le protocole TFTP (Trivial File Transfer Protocol) à l'aide du logiciel PumpKIN.

L'objectif était de sécuriser les configurations des équipements réseau en les transférant vers un ordinateur, afin de pouvoir les restaurer en cas de panne, d'erreur de manipulation ou de réinitialisation.

Mise en place du serveur TFTP

L'ordinateur a été configuré en tant que serveur TFTP via le logiciel PumpKIN :

- **Installation et lancement du logiciel**
- **Définition d'un répertoire de stockage pour les sauvegardes**
- **Vérification de l'adresse IP du PC et de la connectivité réseau avec les équipements**

Procédure de sauvegarde

Une fois la communication établie, la sauvegarde a été effectuée depuis les équipements réseau :

- **Utilisation de la commande : copy running-config tftp**
- **Saisie de l'adresse IP du serveur TFTP (PC)**
- **Définition du nom du fichier de sauvegarde**

Cette procédure a été réalisée pour le routeur ainsi que pour les switches, permettant de centraliser l'ensemble des configurations sur le poste de travail.

Résultat obtenu

Les fichiers de configuration ont été correctement transférés et enregistrés dans le dossier défini sur le PC. Cela garantit une sauvegarde fiable et exploitable en cas de besoin.

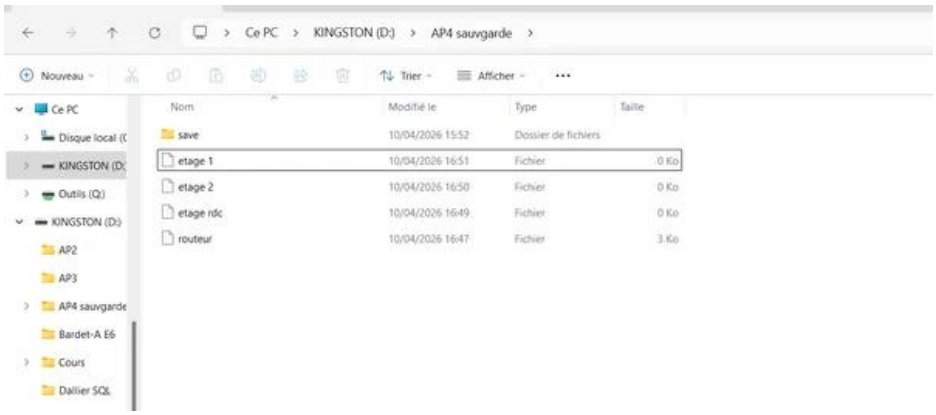
Retour sur l’activité

L’activité s’est déroulée de manière fluide et efficace. La mise en place du serveur TFTP avec PumpKIN a été rapide, et la communication réseau entre les équipements et le PC n’a posé aucune difficulté particulière.

La seule vigilance nécessaire concernait la bonne configuration des adresses IP afin d’assurer la connectivité entre les équipements et le serveur TFTP.

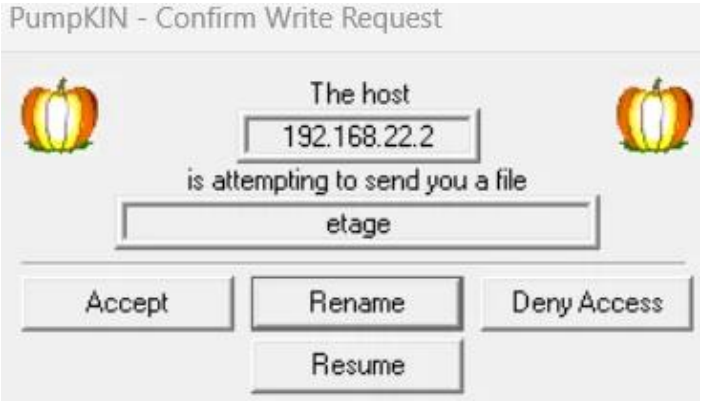
Au final, cette manipulation a permis de comprendre l’importance de la sauvegarde des configurations dans une infrastructure réseau. Le résultat est pleinement satisfaisant, avec des sauvegardes réalisées correctement et exploitables en cas de besoin.

« Capture des fichier sauvegardés »



Ici on peut voir les fichiers qui ont étaient sauvegardé sur le serveur TFTP (ici notre PC client).

« Capture de l'interface PumpKIN »



Cette capture représente l'interface PumpKIN. A chaque fois il fallait mettre l4ip destinataire (celle de l'équipement à sauvegarder). Puis mettre un commande sur ce même équipement.

« Capture de la commande à réaliser »