Années : 2024-2025

BTS SIO

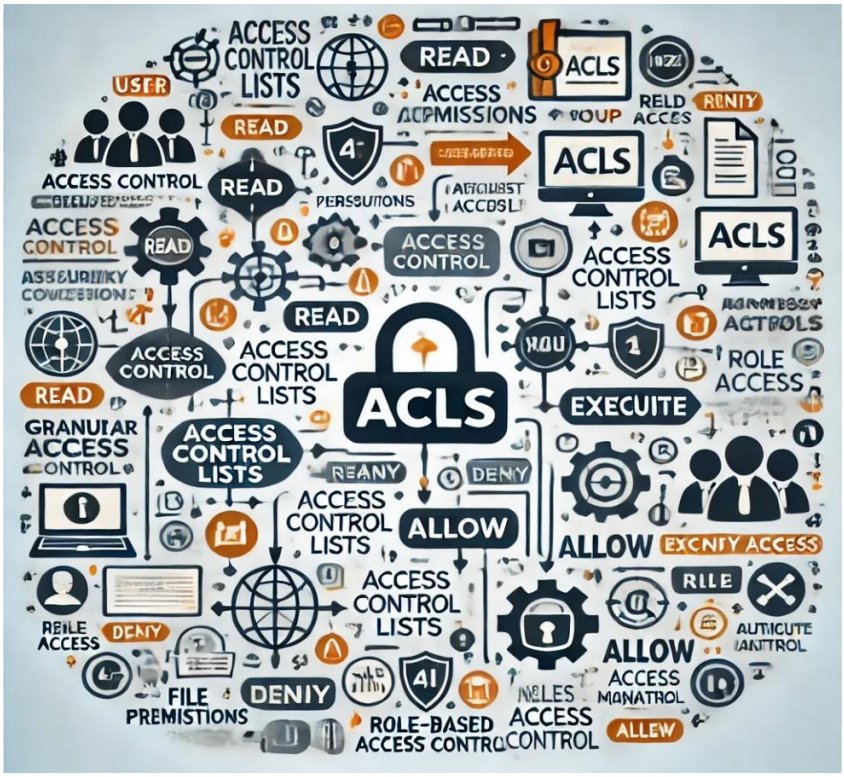
Situation professionnelle numéro 5

Implémentation des ACLs pour la gestion sécurisée des accès dans un environnement multi-utilisateurs

Description :

Les ACLs (Listes de Contrôle d'Accès) sont des mécanismes utilisés pour gérer les droits d'accès à des ressources informatiques (fichiers, répertoires, systèmes, etc.). Elles permettent de spécifier qui peut accéder à quoi et de quelle manière (lecture, écriture, exécution, etc.). Les ACLs sont un outil essentiel pour sécuriser un réseau ou un système en définissant de manière granulaire les permissions des utilisateurs ou groupes d'utilisateurs.

Mots-clés :



Nom	Date	Tampon
Manuela Yamthe Bieleu	26/05/2014	

Plan de la situation

Le cahier des charges

1. L’expression des besoins

Votre entreprise souhaite renforcer la sécurité des données et des ressources informatiques en implémentant un système de **Listes de Contrôle d'Accès (ACLs)**. L'objectif est de garantir que seules les personnes autorisées aient accès aux informations sensibles et aux ressources critiques, tout en permettant une gestion fine des droits d'accès pour chaque utilisateur ou groupe d'utilisateurs.

2. La description de l’existant

L'entreprise utilise actuellement un système de gestion des accès basé principalement sur des permissions simples attribuées au niveau des fichiers et répertoires, sans recours aux Listes de Contrôle d'Accès (ACLs). L'accès aux ressources informatiques (fichiers, répertoires, applications) est principalement géré via des mécanismes d'authentification basés sur des utilisateurs et des groupes, mais sans granularité spécifique concernant les droits d'accès à des fichiers ou répertoires particuliers.

3. L’analyse des choix

L’objectif de cette analyse est d’évaluer les différentes solutions disponibles pour implémenter un système de gestion des droits d’accès basé sur les ACLs, tout en répondant aux besoins spécifiques identifiés dans la description de l'existant. Cela inclut la sécurité, la granularité des permissions, la facilité de gestion et l’intégration avec l’infrastructure existante.

3.1 Offres du marché

Solution	Fonctionnalités clés	Avantages	Limites	Coût
Windows ACLs (NTFS)	Gestion des droits détaillés (lecture, écriture, exécution), intégration avec Active Directory.	Solution intégrée, interface graphique conviviale, support natif dans Windows.	Limité aux environnements Windows, nécessite des connaissances sur les permissions NTFS.	Inclus (Windows).
ACLs POSIX (Linux)	Gestion des droits (rwx) pour utilisateurs et groupes via setfacl et getfacl.	Gratuit, intégré dans Linux, flexible.	Interface en ligne de commande, complexité accrue dans des	Inclus (Linux).

			environnements hétérogènes.	
FreeIPA (Open Source)	Centralisation des utilisateurs et ACLs, intégration Kerberos, interface web.	Gratuit, adapté aux environnements Linux, gestion centralisée avancée.	Complexité d'installation et de configuration, moins adapté à Windows.	Gratuit.
OpenLDAP	Gestion des ACLs avec centralisation des permissions, extensible avec d'autres outils open-source.	Flexible, mature, support communautaire actif.	Configuration complexe, principalement en ligne de commande.	Gratuit.
AWS IAM	Gestion des rôles et des politiques d'accès, contrôle d'accès aux services AWS via JSON.	Granularité élevée, intégration native avec AWS, évolutif.	Limité à AWS, nécessite des compétences spécifiques pour écrire les politiques JSON.	Payant (usage).
Azure Active Directory (AAD)	Gestion des accès cloud et sur site, contrôle basé sur les rôles (RBAC), intégration avec les services Microsoft.	Intégré avec les services Microsoft, gestion unifiée, support avancé.	Dépendance à Azure, coût variable.	Payant (usage).
Google Cloud IAM	Gestion des permissions sur Google Cloud, contrôle basé sur les rôles et les ACLs.	Simplicité d'utilisation, intégration avec Google Cloud, bonne granularité.	Limité aux environnements Google Cloud.	Payant (usage).

Mise en œuvre

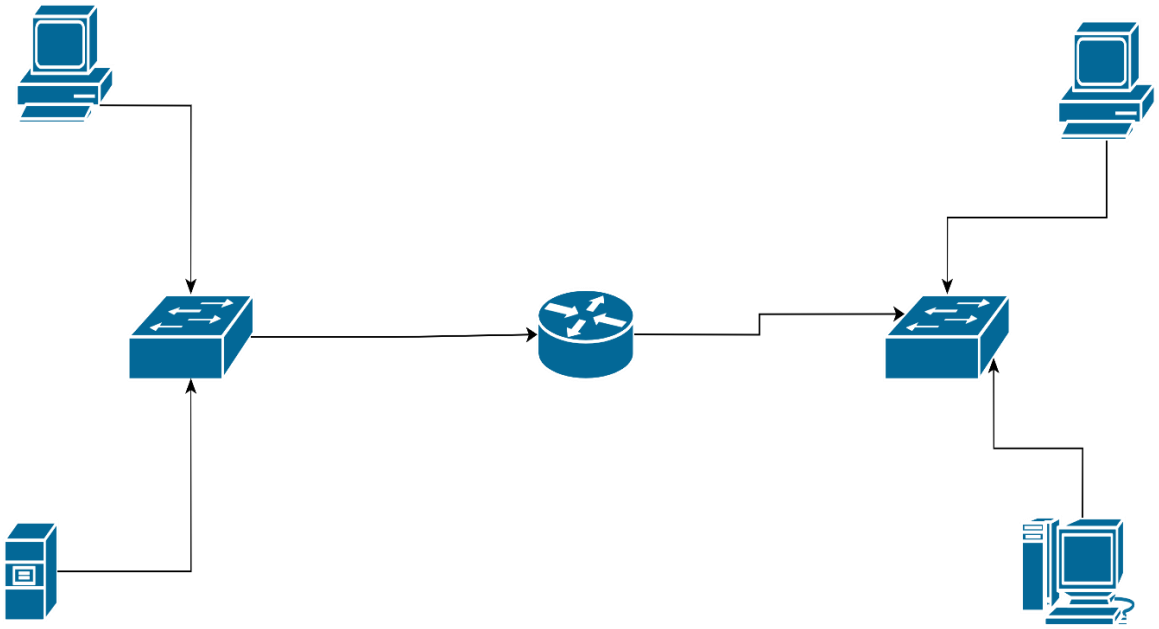
La mise en œuvre des **ACLs (Access Control Lists)** dans **Cisco Packet Tracer** permet de simuler le filtrage et le contrôle du trafic réseau en configurant des routeurs et des commutateurs. Voici un guide étape par étape pour mettre en place des ACLs sur Cisco Packet Tracer.

Scenario

Réseau 1 : Le réseau des employés, où chaque poste de travail a une adresse IP unique (par exemple, 192.168.1.10, 192.168.1.20, etc.).

Réseau 2 : Le réseau réservé aux serveurs, où se trouve un serveur d'applications critiques utilisé pour la gestion des projets (adresse IP : 192.168.2.10).

L'objectif est de **limiter les accès au serveur** de manière stricte, car il contient des informations sensibles et stratégiques pour l'entreprise. Seul le poste de travail du responsable des projets, situé dans le Réseau 1, doit pouvoir accéder à ce serveur.



Chaque pc représente ici un département spécifique de l'entreprise :

PC	Département	**Rôle**	Accès réseau autorisé	Restrictions
PC1	Ressources Humaines	Gestion des employés	Serveur RH uniquement	Bloqué pour les données financières.
PC2	Comptabilité	Gestion des finances	Serveur financier uniquement	Bloqué pour les données RH.
PC3	Informatique (IT)	Maintenance du réseau	Accès complet au serveur et gestion du réseau	Pas de restrictions.
PC4	Marketing ou Commercial	Relation client et projets	Serveur marketing ou CRM	CRM Bloqué pour les données

				RH et financières.

Cette structure simplifie l'administration des ACLs tout en assurant la séparation des responsabilités et la sécurité des données.

3.2 Tableau d'adressage IP

Le tableau ci-dessous présente le **plan d'adressage IP** utilisé dans le cadre de l'implémentation des ACLs. Chaque département est isolé dans un **VLAN dédié**, avec une **plage d'adresses spécifique**. Le masque de sous-réseau permet de définir les bornes de chaque sous-réseau pour une segmentation logique efficace.

Équipement / Poste	Département	Adresse IP	VLAN	Masque de sous-réseau	Rôle
PC1	Ressources Humaines	192.168.10.10	10	255.255.255.0	Accès uniquement au serveur RH
PC2	Comptabilité	192.168.10.10	20	255.255.255.0	Accès uniquement au serveur financier
PC3	Informatique (IT)	192.168.30.10	30	255.255.255.0	Accès complet (admin réseau + maintenance)
PC4	Marketing / Commercial	192.168.30.10	40	255.255.255.0	Accès au **serveur CRM** uniquement
Serveur DHCP	Projets / Applications	192.168.2.10	10	255.255.255.0	Attribue les IP aux VLANs via DHCP Relay

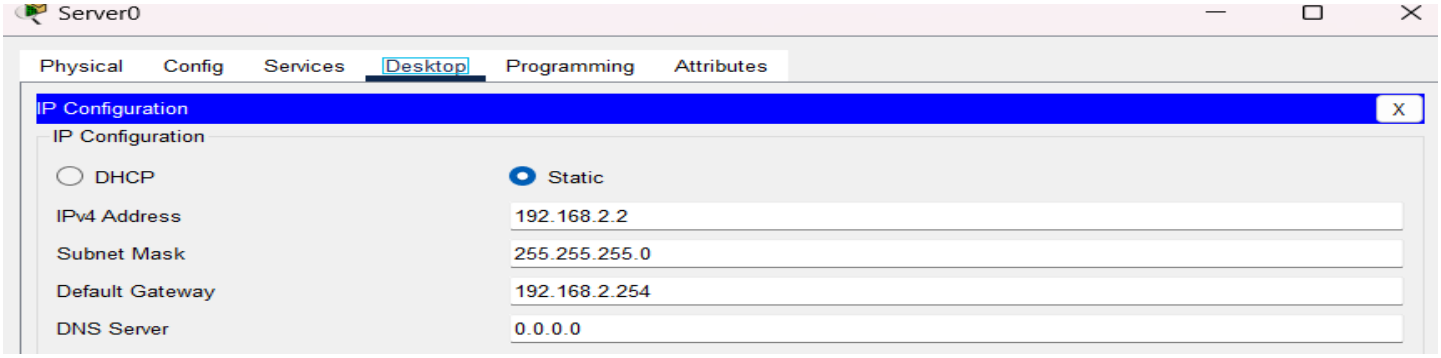
Passerelle VLAN 10	_	192.168.10.1	10	255.255.255.0	Interface routeur pour VLAN 10
Passerelle VLAN 20	_	192.168.20.1	20	255.255.255.0	Interface routeur pour VLAN 20
Passerelle VLAN 30	_	192.168.30.1	30	255.255.255.0	Interface routeur pour VLAN 30
Passerelle VLAN 40	_	192.168.40.1	40	255.255.255.0	Interface routeur pour VLAN 40

Un **CRM** (Customer Relationship Management) est un outil qui permet à une entreprise de centraliser et de gérer toutes les informations liées à ses clients, comme leurs noms, numéros de téléphone ou adresses e-mail et par conséquent ne peut être acceccible par tous. Il facilite également le suivi des ventes en indiquant qui a acheté quoi, et aide à organiser les actions commerciales, comme les appels ou les e-mails. En regroupant toutes ces données, le CRM permet à l'entreprise de mieux connaître ses clients et d'entretenir une relation de qualité avec eux, ce qui améliore la fidélisation et la satisfaction.

4. Mise en place du serveur DHCP

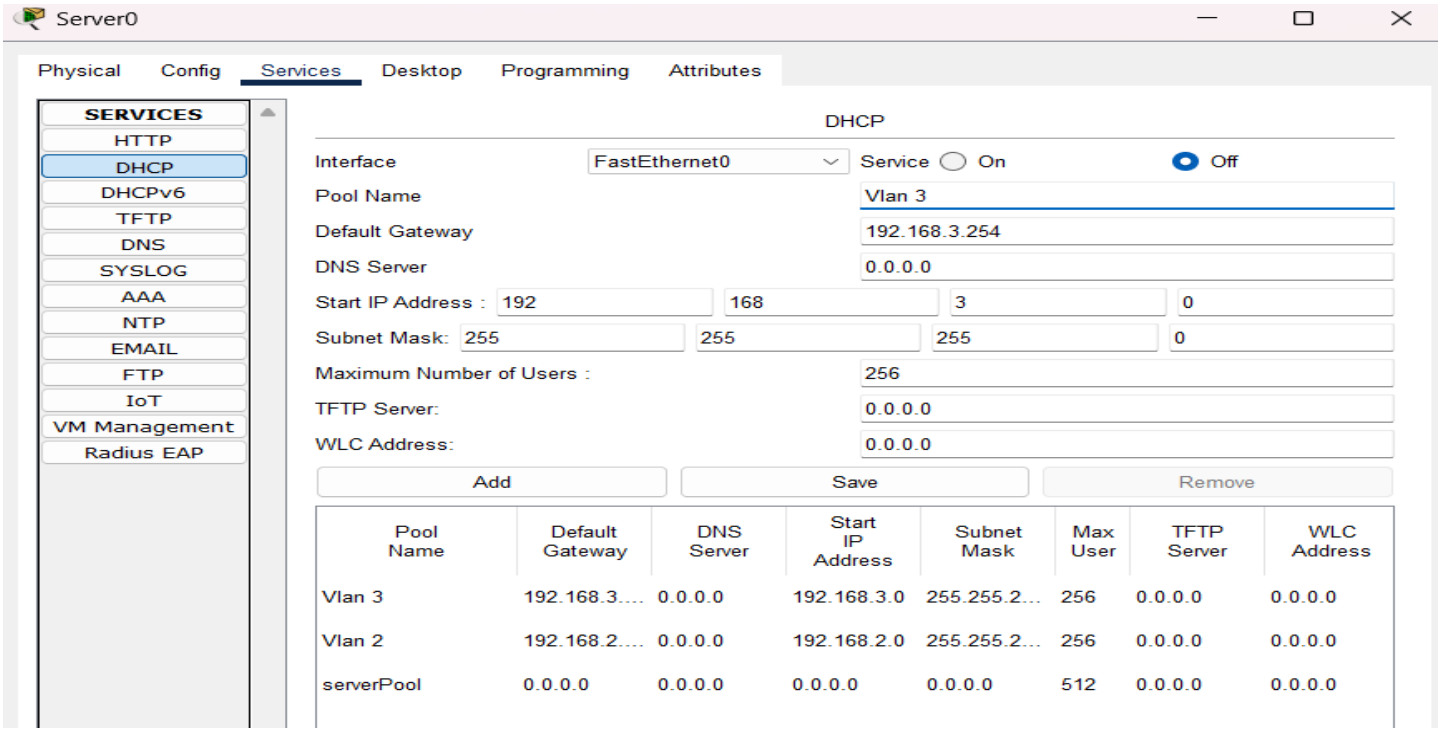
Le serveur DHCP attribue automatiquement des adresses IP aux appareils dans chaque département.

La première étape consiste à attribuer une adresse IP statique au serveur, afin qu'il puisse distribuer correctement les adresses IP aux autres appareils du réseau. Pour ce faire, effectuez un clic droit sur le serveur, accédez à l'onglet **Desktop**, puis configurez les paramètres réseau en saisissant l'adresse IP, le masque de sous-réseau et la passerelle par défaut (gateway).



5. Configuration des switches

Une fois cela fait, accédez à l'onglet **Services**, où vous devrez configurer tous les sous-réseaux présents dans le réseau (VLAN).



On configure les siwtches en saisissant les lignes de commandes suivantes dans l'interface CLI :

!S0

en

conf t

vlan 2

name vlan2

exit

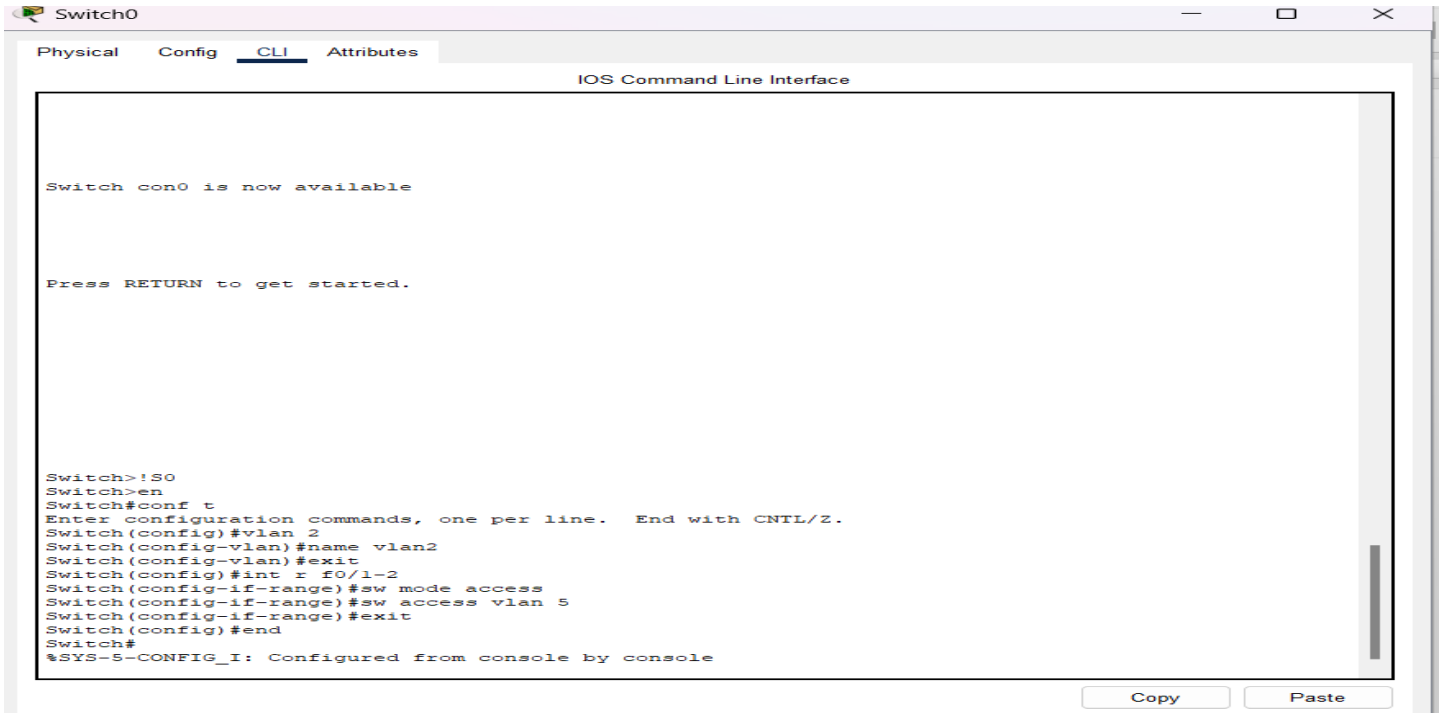
int r f0/1-2

sw mode access

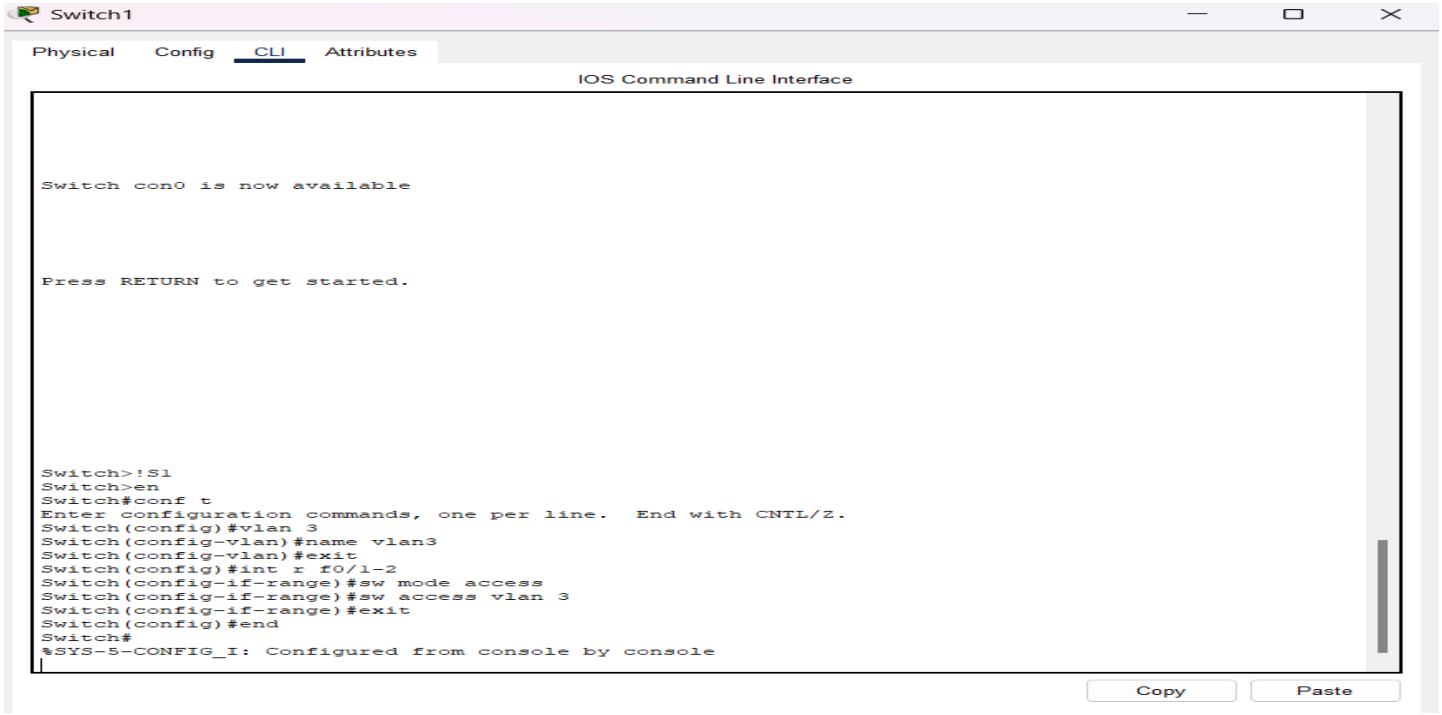
sw access vlan 5

exit

end



On refait la même opération pour l'autre switch



6. Configuration du routeur

On active le routage et on configure une sous-interface pour **chaque VLAN**. Chaque sous-réseau a sa propre IP . afin de pouvoir exécuter directement mon script , on le copie tout d'abord dans le bloc note .

```
interface g0/0.10
 encapsulation dot1Q 10           ! VLAN 10 (RH)
 ip address 192.168.10.1 255.255.255.0
exit

interface g0/0.20
 encapsulation dot1Q 20           ! VLAN 20 (Comptabilité)
 ip address 192.168.20.1 255.255.255.0
exit

interface g0/0.30
 encapsulation dot1Q 30           ! VLAN 30 (IT)
 ip address 192.168.30.1 255.255.255.0
exit

interface g0/0.40
 encapsulation dot1Q 40           ! VLAN 40 (Marketing)
 ip address 192.168.40.1 255.255.255.0
exit

interface g0/0.100
 encapsulation dot1Q 100          ! VLAN 100 (Serveur DHCP)
 ip address 192.168.100.1 255.255.255.0
exit
```

6.1 Activation du routage IP

Cette commande active le routage IP sur le routeur, permettant ainsi la communication entre les VLANs :

```
ip routing
```

6.2 DHCP Relay – Redirection des requêtes DHCP vers le serveur

Étant donné que le serveur DHCP est situé dans le VLAN 100, il est nécessaire de rediriger les requêtes DHCP des autres VLANs vers ce serveur :

```
!R0
en
interface g0/0.10
ip helper-address 192.168.100.1
exit

interface g0/0.20
ip helper-address 192.168.100.1
exit

interface g0/0.30
ip helper-address 192.168.100.1
exit

interface g0/0.40
ip helper-address 192.168.100.1
exit
```

7. Mise en place des ACLs (Listes de Contrôle d'Accès)

Pour protéger le serveur critique (192.168.2.10), des ACLs sont configurées pour restreindre l'accès . Ces règles permettent uniquement au poste du service informatique (192.168.30.10) d'accéder au serveur critique. Les autres accès sont refusés.

```
************************
access-list 100 permit ip host 192.168.30.10 host 192.168.2.10
access-list 100 deny ip any host 192.168.2.10
access-list 100 permit ip any any
```

Ln 23, Col 1 | 402 caractères | 100% | Windows (CRLF) | UTF-8

Puis on applique la règle sur l'interface d'entrée :

```
****************************************
interface g0/0
 ip access-group 100 in
```

Ln 27, Col 1 | 487 caractères | 100% | Windows (CRLF) | UTF-8

8. Résultat escompté

Le réseau de l'entreprise est désormais structuré, sécurisé et conforme aux bonnes pratiques de gestion des accès. Chaque utilisateur ou service est isolé dans un VLAN spécifique, et les droits d'accès aux ressources critiques sont finement contrôlés à l'aide d'ACLs.Le serveur DHCP automatise efficacement l'attribution des adresses IP, tandis que le routage inter-VLAN assure la communication entre les départements autorisés. Grâce à l'implémentation des ACLs, seuls les postes autorisés peuvent accéder aux données sensibles, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des ressources réseau.

Conclusion

Ce projet a permis de mettre en œuvre une solution complète de sécurisation des accès réseau grâce à l'utilisation des ACLs (Listes de Contrôle d'Accès) dans un environnement multi-utilisateurs simulé. En analysant les besoins de l'entreprise et en tenant compte de son infrastructure existante, une architecture réseau segmentée par VLANs a été définie afin d'assurer une meilleure séparation des services.La configuration des équipements réseau, notamment le routeur, les switches et le serveur DHCP, a permis d'automatiser la gestion des adresses IP et d'implémenter des politiques de sécurité précises. L'ajout d'ACLs a joué un rôle central en restreignant les accès aux ressources critiques, comme le serveur de projets sensibles, en fonction des rôles de chaque poste utilisateur.Ce travail m'a permis de renforcer mes compétences en administration réseau, en sécurité informatique, et en configuration d'équipements Cisco. Il démontre l'importance de la planification, de la segmentation réseau et de la gestion des accès pour garantir un environnement informatique à la fois fonctionnel, structuré et sécurisé.