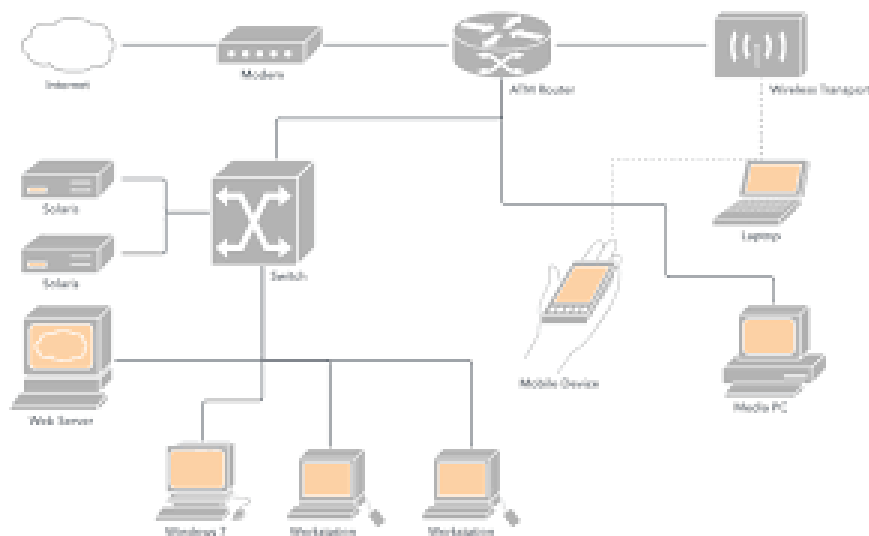


Rapport de Projet : Conception d'un Réseau Universitaire Étendu avec Cisco Packet Tracer



- Rédigé par : *LOUTFI IKRAM*
- Professeur : *Pr. AMAMOU AHMED*
- Etablissement : *Ecole d'Ingénierie digitale et d'intelligence artificielle*
- Filière : *Cyber sécurité*
- Niveau/semestre : *Première année cycle d'ingénieur/S5*
- Module : *Advanced Networking*

Table de matières

1 Introduction	3
1.1 Contexte du Projet	3
1.2 Problématiques Identifiées.....	7
1.3 Objectifs du Projet.....	7
2 Concepts Théoriques.....	8
2.1 VLAN (Virtual Local Area Network)	8
2.2 Planification d'un Adressage IP avec VLSM.....	9
2.3 Routage Inter-VLAN.....	10
2.4 Configuration du acls pour bloquer la communication entre bâtiment A et Admin 12	
2.5 Protocoles de Routage Dynamique	12
3 Sécurité Réseau : Théorie et Configuration	13
4 Conclusion.....	16

1 Introduction

1.1 Contexte du Projet

Dans un environnement universitaire moderne, la connectivité réseau est un élément clé pour assurer un fonctionnement fluide des activités académiques et administratives. Avec l'essor des technologies numériques et des plateformes collaboratives, les universités doivent disposer d'une infrastructure réseau robuste, évolutive et sécurisée pour répondre aux besoins croissants en matière de communication et de partage de ressources.

L'université a identifié des lacunes dans son infrastructure réseau actuelle, notamment en termes de segmentation, de sécurité et de gestion centralisée. Cela limite l'efficacité de la collaboration entre les utilisateurs, tout en augmentant les risques de failles de sécurité. En réponse à ces défis, ce projet vise à concevoir une topologie réseau qui optimise la connectivité tout en assurant une isolation stricte entre les différents groupes d'utilisateurs et en facilitant une gestion efficace du réseau.

L'université est composée de cinq bâtiments :

- **Quatre bâtiments académiques (A, B, C, D)**

- **Groupes utilisateurs**

- **Professeurs** : Responsables de l'enseignement et de la recherche. Ils ont besoin d'un accès prioritaire et sécurisé aux ressources pédagogiques et aux bases de données.
- **Étudiants** : Principaux utilisateurs des infrastructures réseau, nécessitant un accès aux outils d'apprentissage en ligne, aux laboratoires virtuels, et aux plateformes collaboratives.
- **Visiteurs** : Intervenants externes ou invités, dont l'accès doit être limité aux services de base tels qu'Internet.

Caractéristiques des bâtiments académiques

- Chaque bâtiment est constitué de quatre étages, où les réseaux locaux (LAN) doivent être indépendants mais interconnectés, permettant la communication sélective et sécurisée entre les étages et les autres bâtiments académiques.

- **Un bâtiment administratif**

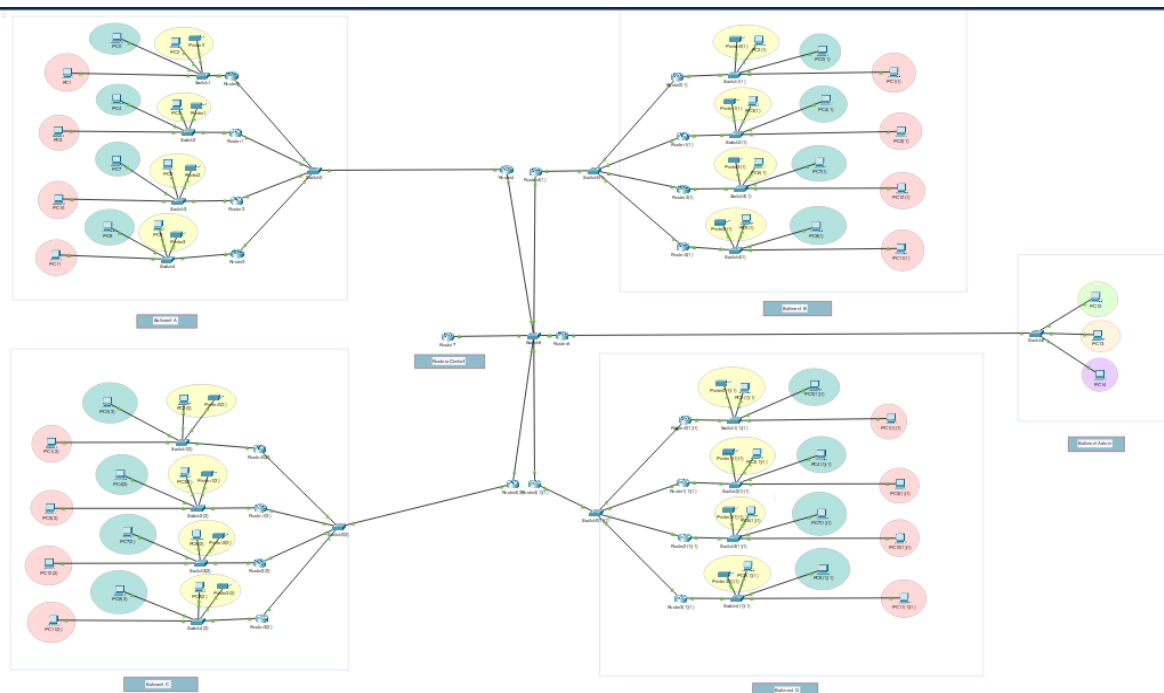
- **Groupes utilisateurs**

- **Administrateurs** : Chargés de la gestion générale de l'université, nécessitant un accès sécurisé aux systèmes de gestion.
- **Services financiers** : Responsables des transactions budgétaires et financières, leur réseau doit être hautement sécurisé.
- **Direction** : Accès exclusif aux données stratégiques et confidentielles, avec des restrictions sévères sur les communications externes.

Caractéristiques du bâtiment administratif

- Ce bâtiment central joue un rôle crucial dans la gestion des opérations de l'université et nécessite une infrastructure réseau robuste pour interagir efficacement avec les bâtiments académiques, tout en maintenant une isolation stricte pour protéger les données sensibles.

Topologie



Couleur	Vlan
Yellow	Vlan 10
Blue	Vlan 20
Pink	Vlan 30
Green	Vlan 100
Orange	Vlan 200
Purple	Vlan 300

1.2 Problématiques Identifiées

- **Manque de segmentation réseau**

L'absence de VLANs dans l'infrastructure actuelle expose tous les utilisateurs à des risques de sécurité accrus et crée des conflits de trafic réseau.

- **Risque de sécurité élevé**

Les données sensibles circulant dans le bâtiment administratif, comme les informations financières ou les dossiers académiques, sont potentiellement vulnérables en raison d'une communication non restreinte avec les autres bâtiments.

- **Gestion inefficace**

L'absence de routage dynamique entraîne une surcharge administrative pour gérer les routes manuellement, particulièrement dans un environnement à multiples sous-réseaux.

1.3 Objectifs du Projet

- L'objectif principal est de concevoir une infrastructure réseau répondant aux exigences suivantes :

1. Segmentation et isolation des utilisateurs

- Créer des VLANs pour séparer les groupes utilisateurs au sein des bâtiments et entre eux.
- Garantir une communication inter-VLAN uniquement là où elle est nécessaire.

2. Sécurité renforcée

- Mettre en place des ACLs (Access Control Lists) pour limiter l'accès entre les VLANs académiques et administratifs.
- Configurer Port Security sur les switches pour protéger le réseau contre les menaces internes.

3. Interconnectivité optimale

- Faciliter la communication entre les bâtiments académiques et le bâtiment administratif via un routeur central ou un switch backbone.
- Mettre en œuvre un routage dynamique (OSPF) pour simplifier la gestion des routes et optimiser les performances réseau.

4. Évolutivité et flexibilité

- Utiliser une conception modulaire pour permettre une extension facile de l'infrastructure réseau.

5. Prévoir une optimisation de l'utilisation des adresses IP grâce au VLSM.

2 Concepts Théoriques

2.1 VLAN (Virtual Local Area Network)

Un VLAN est un réseau logique créé à l'intérieur d'un réseau physique.

- **Isolation** : Les VLANs permettent de séparer logiquement les groupes d'utilisateurs (par exemple, étudiants, professeurs, visiteurs) tout en partageant la même infrastructure physique.
- **Sécurité** : L'isolation limite la propagation des attaques et protège les données sensibles.
- **Performance** : Réduit le trafic de diffusion et optimise l'utilisation des ressources réseau.

Cas d'utilisation dans le projet :

- Création de VLANs pour les professeurs, étudiants et visiteurs dans les bâtiments académiques.
- Séparation des VLANs pour les administrateurs, les services financiers et la direction dans le bâtiment administratif.

Configuration des vlan et activation du mode access :

```
Switch(config)#
Switch(config)#ENABLE
% Incomplete command.
Switch(config)#VLAN 10
Switch(config-vlan)#name prof
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#NAME STUDENT
Switch(config-vlan)#EXIT
Switch(config)#VLAN 30
Switch(config-vlan)#NAME VISITER
Switch(config-vlan)#EXIT
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 1
Switch(config-if)#switchport trunk allowed vlan 10
Switch(config-if)#switchport trunk allowed vlan add 20
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#EXIT
Switch(config)#
```

Copy

Paste

2.2 Planification d'un Adressage IP avec VLSM

Le VLSM permet de subdiviser un réseau en sous-réseaux de tailles variables en fonction des besoins réels. Cela optimise l'utilisation des adresses IP.

Méthode de calcul :

- 1. Identifier le nombre d'hôtes nécessaires pour chaque VLAN.
- 2. Choisir un masque de sous-réseau correspondant.
- 3. Réserver les plages d'adresses pour éviter les chevauchements.

Exemple d'étage 1 dans le projet :

Étage	VLAN	Sous-réseau	Adresses utilisables	Broadcast
1	10	192.168.1.0/28	192.168.1.1 - 192.168.1.14	192.168.1.15
	20	192.168.1.16/28	192.168.1.17 - 192.168.1.30	192.168.1.31
	30	192.168.1.32/28	192.168.1.33 - 192.168.1.46	192.168.1.47
2	10	192.168.1.48/28	192.168.1.49 - 192.168.1.62	192.168.1.63
	20	192.168.1.64/28	192.168.1.65 - 192.168.1.78	192.168.1.79
	30	192.168.1.80/28	192.168.1.81 - 192.168.1.94	192.168.1.95
3	10	192.168.1.96/28	192.168.1.97 - 192.168.1.110	192.168.1.111
	20	192.168.1.112/28	192.168.1.113 - 192.168.1.126	192.168.1.127
	30	192.168.1.128/28	192.168.1.129 - 192.168.1.142	192.168.1.143
4	10	192.168.1.144/28	192.168.1.145 - 192.168.1.158	192.168.1.159
	20	192.168.1.160/28	192.168.1.161 - 192.168.1.174	192.168.1.175
	30	192.168.1.176/28	192.168.1.177 - 192.168.1.190	192.168.1.191
Étage	VLAN	Sous-réseau	Adresses utilisables	Broadcast
1	10	192.168.2.0/28	192.168.2.1 - 192.168.2.14	192.168.2.15
	20	192.168.2.16/28	192.168.2.17 - 192.168.2.30	192.168.2.31
	30	192.168.2.32/28	192.168.2.33 - 192.168.2.46	192.168.2.47
2	10	192.168.2.48/28	192.168.2.49 - 192.168.2.62	192.168.2.63
	20	192.168.2.64/28	192.168.2.65 - 192.168.2.78	192.168.2.79
	30	192.168.2.80/28	192.168.2.81 - 192.168.2.94	192.168.2.95
3	10	192.168.2.96/28	192.168.2.97 - 192.168.2.110	192.168.2.111
	20	192.168.2.112/28	192.168.2.113 - 192.168.2.126	192.168.2.127
	30	192.168.2.128/28	192.168.2.129 - 192.168.2.142	192.168.2.143
4	10	192.168.2.144/28	192.168.2.145 - 192.168.2.158	192.168.2.159
	20	192.168.2.160/28	192.168.2.161 - 192.168.2.174	192.168.2.175
	30	192.168.2.176/28	192.168.2.177 - 192.168.2.190	192.168.2.191

Étage	VLAN	Sous-réseau	Adresses utilisables	Broadcast
1	10	192.168.3.0/28	192.168.3.1 - 192.168.3.14	192.168.3.15
	20	192.168.3.16/28	192.168.3.17 - 192.168.3.30	192.168.3.31
	30	192.168.3.32/28	192.168.3.33 - 192.168.3.46	192.168.3.47
2	10	192.168.3.48/28	192.168.3.49 - 192.168.3.62	192.168.3.63
	20	192.168.3.64/28	192.168.3.65 - 192.168.3.78	192.168.3.79
	30	192.168.3.80/28	192.168.3.81 - 192.168.3.94	192.168.3.95
3	10	192.168.3.96/28	192.168.3.97 - 192.168.3.110	192.168.3.111
	20	192.168.3.112/28	192.168.3.113 - 192.168.3.126	192.168.3.127
	30	192.168.3.128/28	192.168.3.129 - 192.168.3.142	192.168.3.143
4	10	192.168.3.144/28	192.168.3.145 - 192.168.3.158	192.168.3.159
	20	192.168.3.160/28	192.168.3.161 - 192.168.3.174	192.168.3.175
	30	192.168.3.176/28	192.168.3.177 - 192.168.3.190	192.168.3.191

Étage	VLAN	Sous-réseau	Adresses utilisables	Broadcast
1	10	192.168.4.0/28	192.168.4.1 - 192.168.4.14	192.168.4.15
	20	192.168.4.16/28	192.168.4.17 - 192.168.4.30	192.168.4.31
	30	192.168.4.32/28	192.168.4.33 - 192.168.4.46	192.168.4.47
2	10	192.168.4.48/28	192.168.4.49 - 192.168.4.62	192.168.4.63
	20	192.168.4.64/28	192.168.4.65 - 192.168.4.78	192.168.4.79
	30	192.168.4.80/28	192.168.4.81 - 192.168.4.94	192.168.4.95
3	10	192.168.4.96/28	192.168.4.97 - 192.168.4.110	192.168.4.111
	20	192.168.4.112/28	192.168.4.113 - 192.168.4.126	192.168.4.127
	30	192.168.4.128/28	192.168.4.129 - 192.168.4.142	192.168.4.143
4	10	192.168.4.144/28	192.168.4.145 - 192.168.4.158	192.168.4.159
	20	192.168.4.160/28	192.168.4.161 - 192.168.4.174	192.168.4.175
	30	192.168.4.176/28	192.168.4.177 - 192.168.4.190	192.168.4.191

Étage	VLAN	Sous-réseau	Adresses utilisables	Broadcast
1	100	192.168.5.0/28	192.168.5.1 - 192.168.5.14	192.168.5.15
2	200	192.168.5.16/28	192.168.5.17 - 192.168.5.30	192.168.5.31
3	300	192.168.5.32/28	192.168.5.33 - 192.168.5.46	192.168.5.47

2.3 Routage Inter-VLAN

Le routage inter-VLAN permet la communication entre différents VLANs à l'aide d'un routeur ou d'un switch de niveau 3 (Layer 3). Cela repose sur des sous-interfaces associées à chaque VLAN.

Protocole utilisé : Encapsulation dot1Q

- **Encapsulation VLAN ID** : Ajout d'un identifiant VLAN dans l'en-tête Ethernet pour transporter plusieurs VLANs sur un lien physique unique.

Cas d'utilisation dans le projet :

- Assurer la communication entre les VLANs Professeurs et Étudiants pour partager des ressources pédagogiques.
- Bloquer la communication entre le VLAN Étudiants et le VLAN Administrateurs via des ACLs.

Configuration des interfaces virtuelles pour chaque vlan :

```
Router#
Router#ENABLE
Router#CONFIG TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#INTERFACE GIG0/0
Router(config-if)#NO SHUTDOWN
^
% Invalid input detected at '^' marker.

Router(config-if)#NO SHUTDOWN
Router(config-if)#EXIT
Router(config)#INTERFACE GIG0/0.10
^
% Invalid input detected at '^' marker.

Router(config)#INTERFACE GIG0/0.10
Router(config-subif)#ENCAPSULATION DOT1Q 10
Router(config-subif)#IP ADDRESS 192.168.1.1 255.255.255.240
Router(config-subif)#NO SHUTDOWN
Router(config-subif)#EXIT
Router(config)#INTERFACE GIG0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#INTERFACE GIG0/0.20
Router(config-subif)#ENCAPSULATION DOT1Q 20
Router(config-subif)#IP ADDRESS 192.168.1.17 255.255.255.240
Router(config-subif)#NO SHUTDOWN
Router(config-subif)#EXIT
Router(config)#INTERFACE GIG0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-subif)#INTERFACE GIG0/0.30
Router(config-subif)#ENCAPSULATION DOT1Q 30
Router(config-subif)#IP ADDRESS 192.168.1.33 255.255.255.240
Router(config-subif)#NO SHUTDOWN
Router(config-subif)#EXIT
Router(config)#
```

Copy

Paste

2.4 Configuration du ACLs pour bloquer la communication entre bâtiment A et Admin

```
Router>
Router>
Router>
Router>ENABLE
Router#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#IP
Router(config)#IP ACCESS-LIST EXTENDED BLOCK_VLAN10_TO_VLAN100_200_300
Router(config-ext-nacl)#deny ip 192.168.1.48 0.0.0.15 192.168.5.0 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.48 0.0.0.15 192.168.5.16 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.48 0.0.0.15 192.168.5.32 0.0.0.15
Router(config-ext-nacl)#PERMIT IP ANY ANY
Router(config-ext-nacl)#EXIT
Router(config)#INTERFACE GIG0/0.10
Router(config-subif)#IP ACCESS-GROUP BLOCK_VLAN10_TO_VLAN100_200_300 IN
Router(config-subif)#EXIT
Router(config)#IP ACCESS-LIST EXTENDED BLOCK_VLAN20_TO_VLAN100_200_300
Router(config-ext-nacl)#deny ip 192.168.1.64 0.0.0.15 192.168.5.0 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.64 0.0.0.15 192.168.5.16 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.64 0.0.0.15 192.168.5.32 0.0.0.15
Router(config-ext-nacl)#PERMIT IP ANY ANY
Router(config-ext-nacl)#EXIT
Router(config)#INTERFACE GIG0/0.20
Router(config-subif)#IP ACCESS-GROUP BLOCK_VLAN20_TO_VLAN100_200_300 IN
Router(config-subif)#EXIT
Router(config)#IP ACCESS-LIST EXTENDED BLOCK_VLAN30_TO_VLAN100_200_300
Router(config-ext-nacl)#deny ip 192.168.1.80 0.0.0.15 192.168.5.0 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.80 0.0.0.15 192.168.5.16 0.0.0.15
Router(config-ext-nacl)#deny ip 192.168.1.80 0.0.0.15 192.168.5.32 0.0.0.15
Router(config-ext-nacl)#PERMIT IP ANY ANY
Router(config-ext-nacl)#EXIT
Router(config)#INTERFACE GIG0/0.30
Router(config-subif)#IP ACCESS-GROUP BLOCK_VLAN30_TO_VLAN100_200_300 IN
Router(config-subif)#EXIT
Router(config)#
```

Copy

Paste

2.5 Protocoles de Routage Dynamique

Les protocoles de routage permettent aux routeurs de partager dynamiquement des informations sur les réseaux connectés. Cela facilite la gestion des routes et optimise les performances.

Protocole utilisé dans le projet : OSPF (Open Shortest Path First)

▪ Fonctionnement

OSPF utilise l'algorithme SPF (Shortest Path First) pour calculer le chemin le plus court vers chaque destination.

▪ Avantages

- Convergence rapide.
- Optimisation des chemins basés sur des coûts (liés à la bande passante).
- Support des réseaux hiérarchiques via des zones (Area).

Cas d'utilisation dans le projet :

- Connecter les routeurs de chaque étage et chaque bâtiment au routeur central pour partager les routes dynamiquement.

Table de routage du routeur central

```
Router#
Router#
Router#sh ip route ospf
  192.168.1.0/28 is subnetted, 12 subnets
O       192.168.1.0 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.16 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.32 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.48 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.64 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.80 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.96 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.112 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.128 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.144 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.160 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.1.176 [110/3] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
  192.168.2.0/28 is subnetted, 12 subnets
O       192.168.2.0 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.16 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.32 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.48 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.64 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.80 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.96 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.112 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.128 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.144 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.160 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.176 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.2.192 [110/3] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
  192.168.3.0/28 is subnetted, 11 subnets
O       192.168.3.0 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.16 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.32 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.48 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.64 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.80 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.96 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.112 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.128 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.144 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.160 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.3.176 [110/3] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
  192.168.4.0/28 is subnetted, 12 subnets
O       192.168.4.0 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.16 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.32 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.48 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.64 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.80 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.96 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.112 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.128 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.144 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.160 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
O       192.168.4.176 [110/3] via 192.168.10.5, 00:00:32, GigabitEthernet0/0
  192.168.5.0/28 is subnetted, 3 subnets
O       192.168.5.0 [110/2] via 192.168.10.6, 00:00:32, GigabitEthernet0/0
O       192.168.5.16 [110/2] via 192.168.10.6, 00:00:32, GigabitEthernet0/0
O       192.168.5.32 [110/2] via 192.168.10.6, 00:00:32, GigabitEthernet0/0
O       192.168.6.0 [110/2] via 192.168.10.2, 00:00:32, GigabitEthernet0/0
O       192.168.7.0 [110/2] via 192.168.10.3, 00:00:32, GigabitEthernet0/0
O       192.168.8.0 [110/2] via 192.168.10.4, 00:00:32, GigabitEthernet0/0
O       192.168.9.0 [110/2] via 192.168.10.5, 00:00:32, GigabitEthernet0/0

Router#
Router#
Router#
```

Copy

Paste

3 Sécurité Réseau : Théorie et Configuration

Concept :

Port Security est une fonctionnalité des switches qui permet de restreindre le nombre d'appareils (définis par leur adresse MAC) autorisés à se connecter à un port. Cela permet de sécuriser le réseau contre des attaques comme le **MAC flooding**, où un attaquant envoie de nombreuses adresses MAC pour saturer la table de commutation d'un switch, ce qui pourrait mener à une vulnérabilité exploitée par un attaquant pour intercepter le trafic réseau.

Principe de Fonctionnement :

- **Port Security** vérifie l'adresse MAC source des paquets entrant dans un port.
- Un maximum d'adresses MAC autorisées peut être défini sur chaque port.
- Si un appareil non autorisé tente de se connecter au port, différentes actions peuvent être définies pour gérer la violation :
 - **Shutdown** : Le port est désactivé et aucun appareil ne peut y accéder
 - **Protect** : Le switch ignore les paquets venant de l'adresse MAC inconnue.
 - **Restrict** : Le switch ignore les paquets et génère une alerte sans désactiver le port.

Avantages de Port Security :

- **Protection contre le MAC flooding** : En limitant le nombre d'adresses MAC sur un port, le switch empêche une saturation de sa table de commutation.
- **Contrôle d'accès strict** : Permet de garantir que seuls les appareils autorisés (identifiés par leur adresse MAC) peuvent se connecter.
- **Réaction automatique aux violations** : Le switch peut prendre automatiquement des mesures pour bloquer les connexions non autorisées.






Cas d'Utilisation :

Si un utilisateur tente de connecter un second appareil sur un port déjà occupé, le port sera désactivé (en cas de violation `shutdown`). L'administrateur devra ensuite réactiver manuellement le port une fois l'incident traité.

```
Switch>
Switch>
Switch>
Switch>ENABLE
Switch#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#INT RANGE FA0/1-4
Switch(config-if-range)#SWITCHPORT MODE ACCESS
Switch(config-if-range)#SWITCHPORT PORT-SECURITY
Switch(config-if-range)#SWITCHPORT PORT-SECURITY MAXIMUM 1
Switch(config-if-range)#SWITCHPORT PORT-SECURITY MAC-ADDRESS STICKY
Switch(config-if-range)#SWITCHPORT PORT-SECURITY VIOLATION RESTRICT
Switch(config-if-range)#EXIT
Switch(config)#
```

Copy

Paste

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time/ser	Periodic	Num	Edit	Delete
	Successful	PC4	PC7(1)	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1(2)	Printer2(1)	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC6(...	PC13	ICMP		0.000	N	2	(edit)	(delete)

- **Les communications réussies (Statut : Réussi)**

- **PC4 → PC7(1) (ICMP)** : Cela indique que la communication entre deux appareils dans des bâtiments académiques différents fonctionne correctement. Le réseau semble bien configuré pour permettre la communication entre ces deux équipements. Cela peut signifier que les trunks et le routage inter-VLAN entre les bâtiments académiques sont correctement configurés.
- **PC1(2) → Imprimante(1) (ICMP)** : Une autre communication réussie entre un PC et une imprimante dans un même bâtiment académique, ce qui montre que les appareils au sein du même bâtiment peuvent communiquer correctement sans problème.

- **La communication échouée (Statut : Échoué)**

- **PC6 → PC13 (ICMP)** : Ce résultat indique un problème de connectivité entre un PC dans le bâtiment académique et un autre dans le bâtiment administratif. Comme l'ICMP échoue, cela explique que ACLs a bloqué le trafic entre les VLANs académiques et administratifs.

4 Conclusion

La conception et la configuration d'un réseau universitaire étendu avec Cisco Packet Tracer ont permis de répondre efficacement aux exigences de connectivité, d'isolation, et de sécurité. La mise en place d'une topologie bien structurée, combinée à une gestion rigoureuse des VLANs, a assuré une communication fluide entre les différents bâtiments et utilisateurs tout en respectant les politiques d'accès. L'utilisation du protocole OSPF et des ACLs a renforcé la fiabilité et la sécurité du réseau.

Ce projet a également été l'occasion d'approfondir mes compétences techniques, notamment en matière de routage inter-VLAN, d'adressage IP avec VLSM, et de gestion des switches et routeurs. Les défis rencontrés, tels que l'optimisation des configurations et la garantie de l'isolation des VLANs, ont été une opportunité d'apprentissage et de perfectionnement.

Je tiens à exprimer ma gratitude envers les efforts et l'engagement que j'ai investis dans la réalisation de ce projet. Chaque étape a été une expérience enrichissante, renforçant ma passion pour les réseaux et mon envie de continuer à exceller dans ce domaine.

