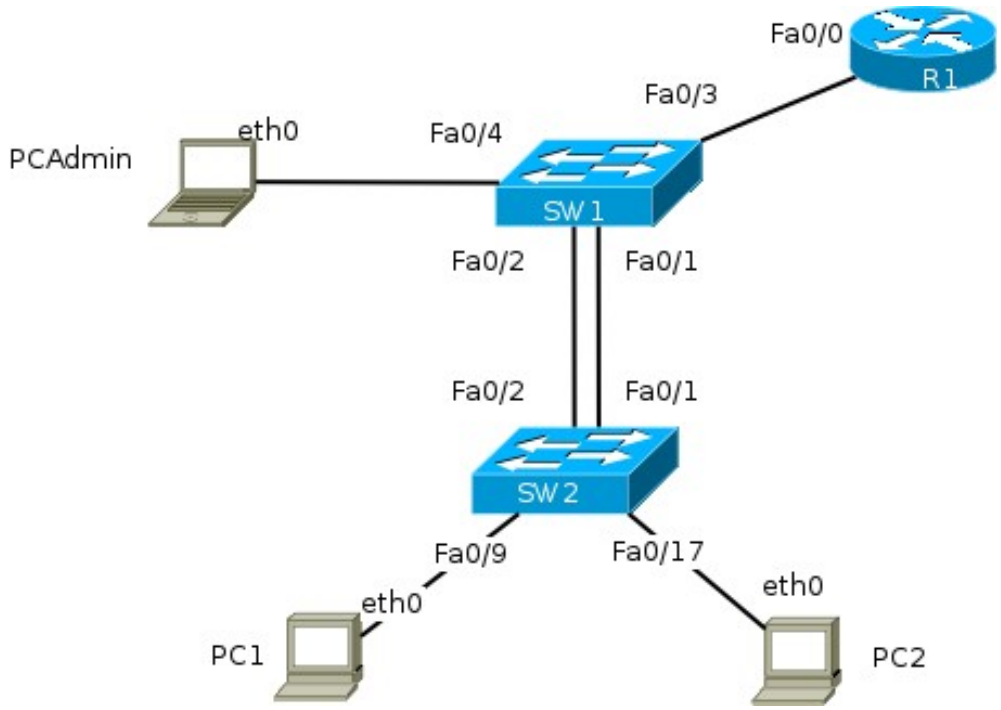
TP2 : Vlan

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	N/A	N/A	N/A
	F0/0.100	192.168.100.254	255.255.255.0	N/A
	F0/0.101	192.168.101.254	255.255.255.0	N/A
	F0/0.102	192.168.102.254	255.255.255.0	N/A
Sw1	VLAN100	192.168.100.1	255.255.255.0	192.168.100.254
Sw2	VLAN100	192.168.100.2	255.255.255.0	192.168.100.254
PC1	eth0	192.168.101.1	255.255.255.0	192.168.101.254
PC2	eth0	192.168.102.2	255.255.255.0	192.168.102.254
PCAdmin	eth0	192.168.100.10	255.255.255.0	192.168.100.254

Scenario

Vous devez en œuvres les vlans et le routage inter vlan. Utilisez **cisco** pour tous les mots de passe d'accès et **class** pour le mode privilégié. Vous devez rendre un rapport électronique à votre encadrant de TP, ce dernier comportant pour chaque question les commandes utilisées et si besoin leurs résultats.

Affectation des ports

Switch 1

Ports	Assignment
Fa0/1 – 0/3	802.1q Trunks (Native VLAN 100)
Fa0/4 – 0/8	VLAN 100 – Gestion
Fa0/9 – 0/16	VLAN 101 – Enseignants
Fa0/17 – 0/24	VLAN 102 – Étudiants
Autres ports	Désactiver

Switch 2

Ports	Assignment
Fa0/1 – 0/2	802.1q Trunks (Native VLAN 100)
Fa0/9-0/16	Vlan 101 - Enseignants
Fa0/17-0/24	Vlan 102 - Etudiants
Autres ports	Désactiver

Task 1: Préparer le réseaux

Step 1: Câbler le réseau comme montré dans le diagramme

Step 2: Effacer les configuration existante (startup-config et vlan.dat)

Step 3: Redémarrer les switches

Task 2: Configuration de base

Configurer les 2 switchs

- Configurer le nom
- Désactiver la recherche DNS .
- Configurer un mot de passe d'exécution privilégié.
- Configurer un mot d'accueil.
- Configurer un mot de passe console.
- Configurer les log synchrones.
- Configurer un accès telnet..

Task 3: Configurer les Vlan

Step 1 : Configurer les VLANs sur les commutateurs.

Pour cela utiliser les noms :

VLAN	VLAN Name
VLAN 100	**management**
VLAN 101	**faculty-staff**
VLAN 102	**Students**

Step 2: Configurer les ports trunk en limitant les vlan autorisés à 100, 101 et 102.

Step 3: Configurer les ports d'accès en fonction du tableau de description.

Task 4: Configurer les adresses de gestion

Step 1: L'interface de gestion sur les switch.

Step 2: Les interfaces des 3 PC.

Step 3 : Tester les ping entre les switch et les PC, lesquels peuvent/ne peuvent pas communiquer ensemble ? Pourquoi ?

Task 5: Configurer le routage inter vlan (router on a stick)

Step 1: Faire la configuration basique du routeur (nom, telnet ...).

Step 2: Configurer l'interface Fa0/0.

Step 3: Vérifier le routage inter vlan (Utiliser des ping entre tous les appareils)**.**

Task 6 : Configurer l'agrégation de lien

Step 1: Agréger la liaison double entre SW1 et SW2**.**

Step 2: Vérifiez que le routage inter vlan fonctionne toujours.

Task 7 : Mac Flooding

Sur pcadmin, installez un serveur web (paquet apache2) et contactez le depuis PC1.

Step 1: Pouvez-vous espioner la communication depuis PC2 ? Pourquoi ?

Step 2: Sur PC2 installez le paquet dsniff et utilisez la commande macof pour remplir la table d'adresse MAC de SW2. Combien d'adresse contient la table mac de SW2 ? Pouvez-vous espionez la communication de PC1 à PCAdmin depuis PC2 ? Pourquoi ?

Step 3: Comment empêcher cette attaque ? Faite le sur tout les ports d'accès des 2 switch.

Task 8 : Plus de sécurités

Step 1 : Désactiver les ports non attribués à un vlan (pour cela utiliser la commande `interface range`...).

Step 2 : fair en sorte d'éviter qu'un communtateur branché sur le port ne change la racine de l'arbre ;

Step 3 : Sur tout les port ésactiver CDP et la négociation de trunk.

Step 4 : Ajouter une sécurité pour banir les attaquant qui essayent de se connecter en testant tous les mots de passe.

Task 9 : Si vous avez le temps

Vous allez tenter de faire un man in the middle avec le protocole ssh.

Step 1 : Sur R1 configurer les acces ssh avec un mot de passe quelconque. Authorisez la version 1 du protocol.

Step 2 : Utilisez sshmitm depuis PC admin pour ouvir un serveur sur le port 2222 qui est transferé sur le serveur ssh du routeur. Depuis PC1 connectez vous sur le port 2222 de PCAdmin (avec la version 1 du protocol). Observez ce qui passe.

Step 3 : Dans la question précedante, la victime est au courant de ce qui se passe car elle doit contacter le serveur de PCAdmin et pas celui du routeur. Pouvez-vous détourner le flus xxh du serveur en utilisant arpspoof ?

Task 8 : En plus du rapport

Sur chaque switch et routeur, fournissez à votre encadrant le résultat de la commande **`show run`**

Task 9 : Nettoyer

Effacer les configurations (et les fichiers vlan.dat) de tous les appareils, éteignez et ranger les commutateurs, les cables ...