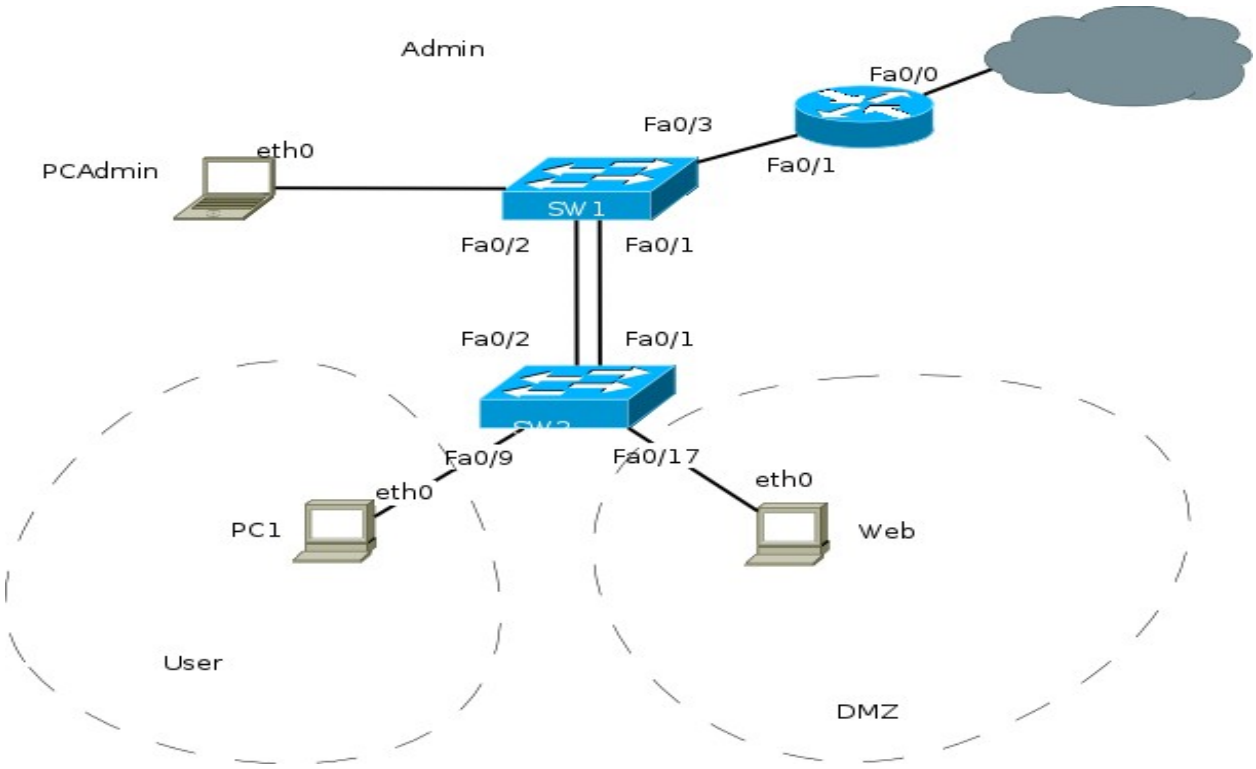
TP3 : Reseau

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gi0/0	172.16.XY.13	255.255.255.240	172.16.XY.14
	Gi1/1	N/A	N/A	N/A
	Gi0/1.100			N/A
	Gi0/1.101			N/A
	Gi0/1.102			N/A
Sw1	VLAN100			
Sw2	VLAN100			
PC1	eth0			
Web	eth0			
PCAdmin	eth0			

Scenario

Vous devez mettre en œuvres les vlans, le routage inter vlan, puis mettre en place la traduction d'adresse. 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. Vous devez aussi y ajouter la réponse à toutes les questions posées.

Affectation des ports

Switch 1

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

Switch 2

Ports	Assignment
Fa0/1 – 0/2	802.1q Trunks (Native VLAN 100)
Fa0/9-0/16	Vlan 101 - User
Fa0/17-0/24	Vlan 102 - DMZ
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: Plan d'adressage

Vous allez configurer un réseau avec des adresses privées 192.168.0.0/24 et des adresses publiques 172.16.XY.0/18. X est le numero du plot et Y votre numéro de groupe. Vous allez devoir le découper le reseau privé en 3

Step 1 : Calculer les adresses de réseau de manière à suivre la demande suivant :

- DMZ 12 machines (plus le routeur). Il doit utiliser les adresses les plus petites proposées. Par exemple le serveur WEB doit utiliser l'adresse 192.168.0.1
- User 100 machines (plus le routeur)
- Admin 29 machines (plus le routeur)

Step 2 : Remplissez le tableau en page 1 de manière à

- Donner au routeur la dernière adresse du réseau
- Donner au SW1 et SW2 les adresses 1 et 2 du reseau d'administration
- Donner aux ordinateurs la première adresse libre

Task 3: Configuration de base

Step 1 : Configurer les 2 switchs

- Configurer le nom
- Désactiver la recherche DNS .
- Configurer un utilisateur root dont le mot de passe est cisco (avec tout les droits).
- Configurer un mot d'accueil.
- Configurer un mot de passe d'exécution privilégiée.
- Configurer les log synchrones.
- Configurer un accès telnet via les utilisateur locaux.

Task 4: Configurer les vlan

Step 1: Configurer les vlans

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

Task 5: Configurer les adresses de gestion

Step 1 : L'interface de gestion sur les switchs, leur route par défaut.

Step 2 : Les interfaces du PC admin.

Step 3 : Tester les ping entre les switchs et le PC admin

Task 6 : 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 et la route par défaut

Step 3: Configurer le routage inter vlan et vérifier le (Utiliser des ping entre tous les appareils).

Task 7: Serveur DHCP

Step 1: Configurer le routeur de manière à ce qu'il soit serveur DHCP pour le réseau User

Step 2: Pour attribuer les adresses, créez un pool nomé “**poolUSER**” :

- proposant toutes les adresse du reseau user sauf les 10 dernières;
- donnant le nom de domain **univ.fr;**
- donnant l'adresse du serveur dns 8.8.8.8;
- donnant le routeur par defaut;
- attribuant les adresses pour 6h.;

Step 3: Configurer la machine PC1 pour être client DHCP. Peut-elle contacter le serveur web à l'adresse 192.168.0.1 ? L'interface externe du routeur R1 172.16.XY.13 ? Le routeur par défaut de R1 172.16.XY.14 ? Pourquoi ?

Step 4: Quel est l'importance de la lease ? Quelle valeur proposeriez-vous pour un réseau wifi dans une gare ? Justifiez.

Task 8 : ACLs Standarts

Les ACLs standards ne permettent de filtrer qu'en fonction de la source. Assez souvent il faut les placer au plus proche de la partie protégée.

Step 1: Vous devez protéger les switchs et le routeur pour que seuls les utilisateurs du réseau admin puissent se connecter en telnet. Pour cela créer une *ACL standart* nommée **telnet** :

- Qui autorise les connexions telnet ou ssh depuis le réseau admin.
- Sauf depuis le routeur R1 lui même.

- Et interdit tous les autres.

Vous appliquerez l'ACL au bon endroit.

Task 9: Traduction d'adresse NAT

Pour le moment, les serveurs extérieurs ne peuvent pas répondre aux machines de votre réseau car ce dernier utilise des adresses privées 192.168.0.0/24. Le routeur R1 va donc :

- Appliquer une traduction d'adresse statique de 172.16.XY.1 vers le serveur 192.168.0.1
- Appliquer une traduction d'adresse dynamique utilisant les adresses publiques 172.16.XY.10 à 172.16.XY.13 (nommé le pool d'adresse **natPOOL**).

La traduction dynamique devra permettre à plus de 4 machines de se connecter à internet en même temps. Elle doit traduire les adresses en provenance de tout les réseaux USER et admin. Vous aurez besoin d'une ACL pour cela, utilisez une ACL standart numérotée **1.**

Step 1: Faites fonctionner les traductions et testez-les.

Step 2: Qu'implique la phrase “La traduction dynamique devra permettre à plus de 4 machines de se connecter à internet en même temps” ? Pourquoi ?

Task 10 : ACL étendues

Les ACL étendues permettent d'utiliser le protocol, la source, la destination ou les ports du paquet. En général, on les place dès que possible pour éviter de charger le réseaux ou les apareils avec des paquets inutils.

Step1: Le reseau DMZ est succeptible d'être compromis. Vous devez donc faire en sorte que ce dernier ne contacte pas les machines du reseau *USER,* sauf si c'est la réponse d'une connexion TCP vers un serveur http (l'origine de la réponse sera donc le port 80 d'un serveur de la DMZ). Pour cela utilisez une ACL étendue numérotée dont le numéro sera le plus petit possible. Vous devez l'appliquer à la sortie du réseau DMZ (entrée de l'interface du routeur). Attention à ne pas perturber les autres paquets.

Step2: Pour le moment le reseau DMZ ne contient qu'un serveur web. Les connexions depuis l'extérieur vers se réseau doivent donc se limiter à l'accès via TCP au port 80 du serveur 172.16.0.1 ou à la réponse sur un port dynamique TCP ou UDP. Vous savez que sur ce serveur, les ports dynamiques sont les ports supérieurs à 1024. De plus il faut laisser passer les requetes DNS.

- Dans votre rapport citez 2 endroits différents où vous pouvez appliquer l'ACL et décrire les ACLs correspondantes dans les 2 cas. Attention, il ne faut pas perturber les autres connexions (par exemple extérieur vers réseau USER).
- Vous devez choisir d'appliquer l'ACL le plus tôt possible pour éviter de charger le réseau avec des paquets qui seront détruit.
- Faites le via une ACL étendue nommée **toDMZ**

Task 11: Protection du reste du réseau.

Question 1 : Est-ce qu'un attanquant extérieur peut facilement toucher les machines des réseaux USER et ADMIN ? Pourquoi ? Par exemple que se passe-t-il si on branche une machine sur le même switch que l'interface Gigabyte 0/0 routeur R1 et qu'il tente un ping 192.168.0.33 ?

Question 2 : Est-ce que la protection est totale ? Peut-elle être contournée ?

Question 3 : Peut-on créer une ACL qui permet à toute machine interne de sortir vers l'extérieur, mais pas à une machine externe d'entrer ? Attention,

- Vous n'administrez pas les machines du reseau USER, vous ne pouvez pas savoir si certains ports sont uniquement utilisés pour les applications clientes.
- Les connexions TCP (et la pluspart des connexion UDP) suppose que le serveur répond

Question 4 : Si oui donnez l'ACL, sinon, que manque-t'il pour faire cela ?

Task 12: Nettoyer

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