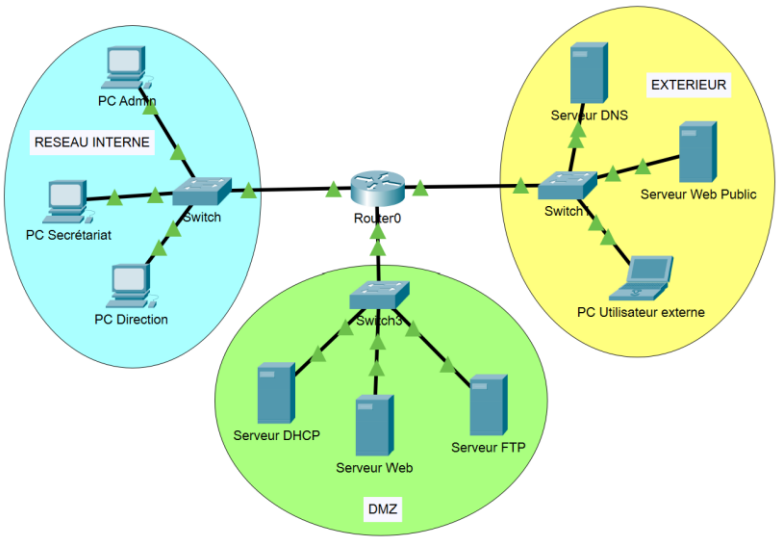
Travaux Pratiques R&T 1ère année
Durée : 3 heures
SAE21
Cisco - Etude de cas



Nom :
Groupe de TP :
Date :

OBJECTIFS - TOPOLOGIE

⇨ Configuration d'un réseau d'entreprise avec VLAN et limitation des accès par ACL

Vous utiliserez pour ce TP le logiciel Cisco Packet Tracer.

Pour l'ensemble des questions suivantes vous décrirez votre façon de procéder dans le **compte rendu de TP** et vous joindrez également votre **fichier Packet Tracer** dans l'espace Cours en ligne.

MANIPULATIONS

Partie 1 – Création du réseau de l'entreprise

Le réseau privé de l'entreprise (à gauche du schéma) comprend 2 VLAN : 1 pour l'administrateur du réseau (PC Admin), 1 pour le Personnel (PC Secrétariat et PC Direction).

1. Faites une proposition de découpage en sous-réseaux pour le réseau privé de l'entreprise (10.0.0.0/8), précisez les adresses attribuées aux 2 VLAN.

2. Implémentez les VLAN sur le switch et configurez port par port l'affectation des VLAN (Mettre une adresse IP du sous réseau Admin sur l'interface VLAN Admin).

3. Quel sera le type de liaison entre le switch et le routeur ? Expliquez.

4. Implémentez la configuration sur le routeur (routage inter-vlan).

5. Testez avec la commande ping la communication inter-vlan via le routeur.

6. Configurez le switch afin que le PC-Admin puisse l'administrer via le protocole SSH.

7. Mettez en place une ACL afin d'autoriser uniquement le PC-Admin à accéder à la configuration du switch par SSH (les requêtes SSH vers le switch doivent être bloquées pour les machines du personnel) .

Partie 2 – Ajout de la DMZ et du réseau extérieur

La DMZ de l'entreprise (en bas du schéma) comprend 3 serveurs (Web, DHCP, FTP). Le réseau extérieur (à droite du schéma) est représenté par deux serveurs publics (Web et DNS) ainsi que par un PC d'un utilisateur extérieur.

1. Configurez le serveur DHCP pour distribuer les IP sur l'ensemble du réseau de l'entreprise (sous-réseaux Admin et Personnel).

2. Mettez en place une ACL afin d'autoriser les PC du sous-réseau Personnel à accéder aux serveurs de la DMZ.

3. Mettez en place une ACL afin d'autoriser les PC du sous-réseau Personnel à accéder aux serveurs extérieurs.

4. Depuis le PC Secretariat, vérifiez les accès vers les serveurs Web interne (HTTP) et externe (HTTPS).

5. Mettez en place une ACL afin d'autoriser le PC extérieur à accéder au serveur web de la DMZ en HTTPS.