SAE 21 - Construire un réseau

RT12

Semestre 2

I. Introduction

Le projet mené durant cette SAE a pour objectif de consolider votre savoir-faire sur le matériel réseau de niveau deux (commutateur) et trois (routeur). Vous êtes maintenant capable de construire un réseau local constitué de commutateurs et de routeurs et de mettre en place des règles de sécurité simples. Dans cette SAE, vous travaillerez de manière individuelle et utiliserez le logiciel GNS3. La section II décrit le réseau à mettre en place. La section III décrit les services à déployer. La section IV décrit les règles de sécurité à mettre en place.

II. Mise en place du réseau

la figure 1 illustre la topologie du réseau à déployer. Vous partagez le réseau *192.168.64.0/20* avec l'ensemble de vos camarades.

II.1. Réseau local et VLAN

On désire créer trois VLAN où chacun est associé à un groupe d'utilisateurs. Le premier regroupe les personnes de l'administration, le second celui des développeurs, et le dernier celui des administrateurs. Le numéro de VLAN attribué à chaque groupe doit être le suivant :

— administration : VLAN 100,
— développeur : VLAN 200,
— administrateur : VLAN 300.

La gestion des VLANs sera centralisée sur le commutateur *commutateur-fed*. Le VLAN natif sera déplacé sur le VLAN 999 et sera également tagué pour plus de sécurité. Afin d'assurer l'interconnexion des VLAN, il est impératif de réaliser le routage inter-vlan sur le commutateur nommé *commutateur-fed*. Un équilibrage de charge sera mis en place entre les deux commutateurs pour les VLAN 100, 200 et 300 avec le protocole Spanning-tree en utilisant trois liens. Il consistera à dédier un VLAN à chaque lien, mais si un lien tombe, un autre devra supporter deux VLAN et ainsi de suite pour chaque lien qui tombera.

II.2. adressage IP

Votre groupe RT12, se voit attribuer le réseau *192.168.64.0/20* que vous devez partager entre vous. Vous devez réaliser une première segmentation de ce réseau, afin que chaque personne du groupe possède son propre sous réseau et ait suffisamment d'adresses. On considère que

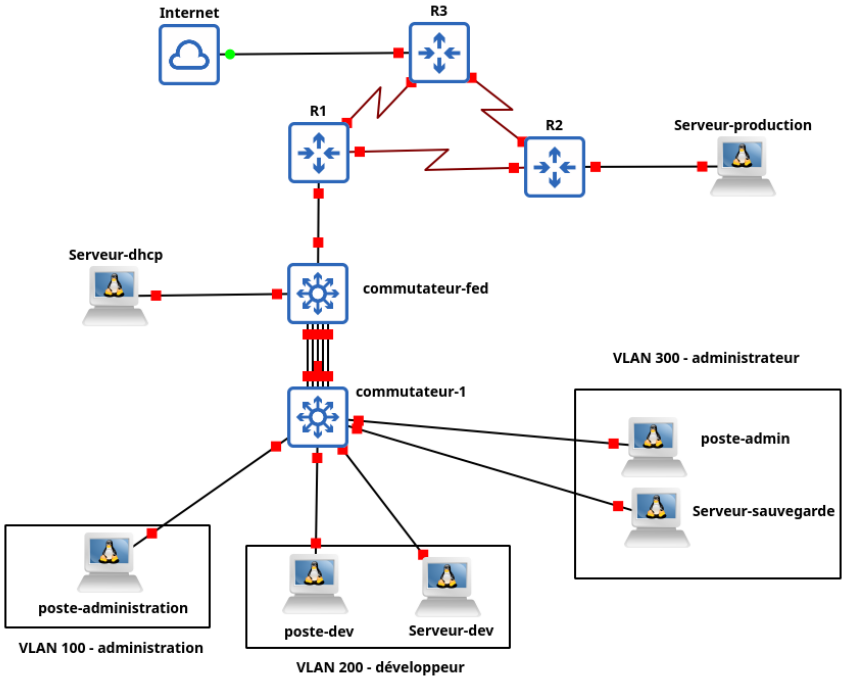

FIGURE 1 – Topologie du réseau

votre groupe est composé de 32 personnes. Le réseau de chaque personne du groupe devra être segmenté une nouvelle fois, afin de réserver un certain nombre d'adresses :

- quatre pour le VLAN administration,
- quatre pour le VLAN utilisateur,
- quatre pour le VLAN administrateur,
- quatre pour la partie production,
- réserver des adresses pour l'interconnexion entre les routeurs et avec le commutateur.

La segmentation du réseau de chaque personne devra se faire avec un masque variable. Les adresses des serveurs seront fixes. La connexion avec le réseau extérieur est ignorée dans cette partie. Le service DHCP sera assuré par le serveur nommé *Serveur-dhcp*. .

II.3. Interconnexion des équipements de niveau 3

Les adresses dédiées à la liaison entre les équipements de niveau 3 doivent avoir un masque de type */30*. Le protocole RIP v2 sera utilisé comme protocole de routage.

III. Mise en place de services

Nous allons maintenant déployer des services sur les trois serveurs, sauvegarde, dev et production.

III.1. Serveur FTP

Déployer un service FTP sur le serveur nommé, *Serveur-sauvegarde*. L'accès anonyme sera autorisé et deux utilisateurs à savoir *Antoine* et *Élise* auront un accès en lecture/écriture.

III.2. Serveur Web

Installer le service Apache sur le serveur dev et le serveur de production. Modifier la page par défaut sur le serveur dev et utiliser le programme *rsync* pour écraser par copie la page web par défaut sur le serveur de production.

IV. Sécurité du réseau

On souhaite maintenant appliquer quelques mesures de sécurité.

IV.1. Sécurité des ports des commutateurs

On souhaite sécuriser les ports des commutateurs en autorisant uniquement la première machine connectée sur le port. En vous aidant du mot clef *port-security*, appliquer cette mesure de sécurité sur tous les ports des deux commutateurs.

IV.2. ACL du routeur R2

Implémenter des ACL, afin de n'autoriser que le trafic HTTP et le traffic sur les ports 22 et 873, ports utilisés par rsync.

IV.3. ACL du routeur de bordure

Implémenter des ACL afin de n'autoriser que le trafic ICMP et HTTP venant de l'extérieur.

V. Interconnexion au réseau de l'IUT

En utilisant l'élément Cloud qui représente le réseau extérieur, configurer le routeur *R3* pour accéder au réseau extérieur depuis n'importe quelle machine.