

SAE 21 - Construire un réseau

RT 12

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. Segmentation du réseau local

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.

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 votre groupe est composé de 32 personnes. Le réseau de chaque personne du groupe devra être segmenté une nouvelle fois, afin de réservier 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,
- réservier des adresses pour l'interconnexion entre les routeurs et avec le commutateur.

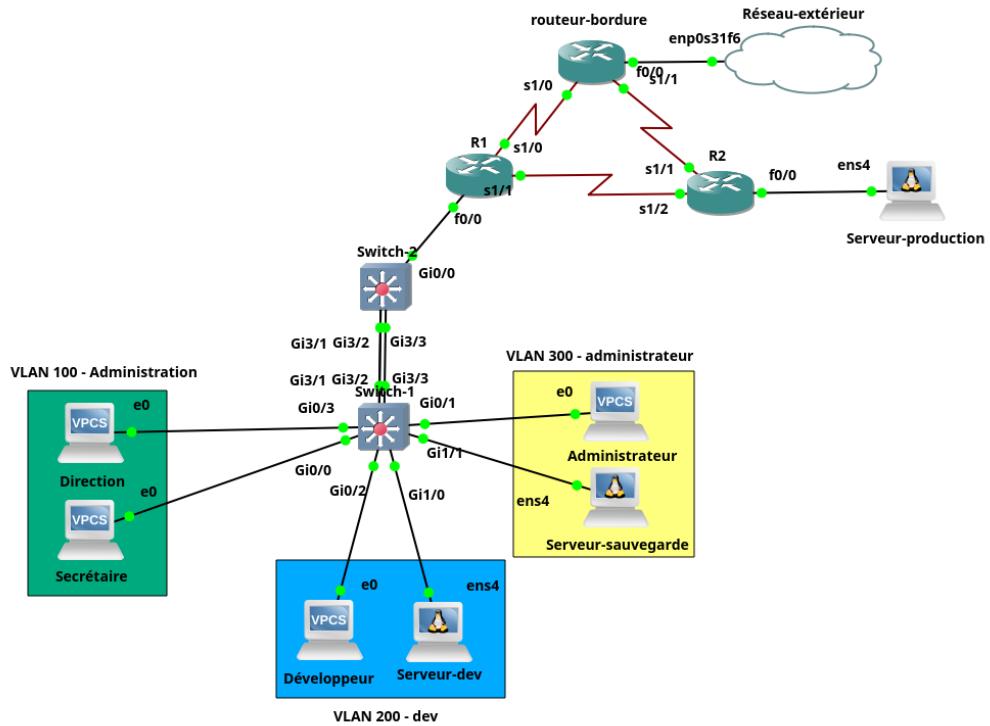


FIGURE 1 – Topologie du réseau

La segmentation du réseau de chaque personne devra se faire avec un masque variable. Les adresses des serveurs seront fixes et correspondront à la valeur de la première adresse IP du sous-réseau. La connexion avec le réseau extérieur est ignorée dans cette partie.

II.3. Gestion des VLAN

Afin d'assurer l'interconnexion des VLAN, il est impératif de réaliser le routage inter-vlan sur le commutateur nommé *Switch-2*. Le *Switch-1* et le *Switch-2* sont reliés par trois liens. Il est demandé d'effectuer un équilibrage de charge des VLAN entre ces deux commutateurs, avec le protocole Spanning-tree. 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.4. DHCP

Activer le protocole DHCP sur le commutateur nommé *Switch-2*, afin d'attribuer une configuration réseau aux PC dans les VLANs.

II.5. 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, *serveur-sauvegarde*, *serveur-dev* et *serveur-dev*.

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. Implémenter une ACL qui effectue une surcharge NAT sur le trafic provenant du VLAN administration vers le réseau extérieur.

V. Interconnexion des maquettes

En utilisant l'élément Cloud qui représente le réseau extérieur, interconnecter cet élément avec le routeur de bordure et configurer le routeur afin de pouvoir interconnecter votre maquette GNS3 avec celle d'un camarade.