SAE 2.01 – Construire un réseau

Objectifs de la SAE

Cette SAE a été l'occasion de mettre en œuvre de manière concrète les compétences acquises en réseau, notamment sur les équipements de niveau 2 (commutateurs) et de niveau 3 (routeurs).
Elle visait à consolider notre capacité à concevoir, configurer et sécuriser un réseau local complet, à l'aide de GNS3, un logiciel de simulation permettant d'intégrer des routeurs, commutateurs, serveurs et hôtes dans un environnement virtuel.

---

1. Mise en place du réseau

a) Création de VLANs

Trois VLANs ont été mis en place :

- **VLAN 100** : Administration
- **VLAN 200** : Développeurs
- **VLAN 300** : Administrateurs

Un VLAN natif (VLAN 999) a été configuré, et **le tagging a été activé pour renforcer la sécurité**.
La gestion centralisée des VLANs a été assurée par le commutateur principal nommé **commutateur-fed**.

b) Routage Inter-VLAN

Le **routage inter-VLAN** a été implémenté sur le commutateur-fed, permettant aux différents VLANs de communiquer entre eux.

c) Spanning Tree et Redondance

Un **équilibrage de charge** a été mis en œuvre entre les commutateurs pour les VLANs 100, 200 et 300 grâce au protocole **Spanning Tree**, avec trois liens redondants. Chaque VLAN était assigné à un lien principal, avec bascule automatique en cas de défaillance d'un lien.

---

2. Plan d’adressage IP

Nous disposions du réseau **192.168.64.0/20**, partagé entre les 32 étudiants du groupe RT12. Chaque étudiant devait sous-segmenter son sous-réseau pour allouer :

- 4 adresses pour chaque VLAN (100, 200, 300),
- 4 adresses pour une zone de production,
- des adresses pour les interconnexions routeur ↔ commutateur.

Les liaisons entre routeurs utilisaient des **masques /30**.
Le service DHCP a été installé sur un serveur dédié nommé **serveur-dhcp**, et utilisé pour distribuer les adresses dynamiquement.

---

3. Mise en place des services

Trois serveurs distincts ont été configurés, chacun avec un rôle précis :

a) Serveur FTP

Installé sur le **Serveur-sauvegarde**, avec accès anonyme activé.
Deux comptes utilisateurs (Antoine et Élise) ont été créés avec des droits en lecture/écriture.

b) Serveur Web

Les serveurs **dev** et **production** ont été configurés avec Apache.
Sur le serveur dev, une page web personnalisée a été créée, puis **copiée automatiquement via `rsync`** sur le serveur production, afin d’assurer la synchronisation du contenu.

---

4. Sécurisation du réseau

a) Port-security sur les commutateurs

Une politique de **port-security** a été appliquée sur tous les ports des deux commutateurs, restreignant chaque port à la **première machine connectée**, pour éviter tout branchement non autorisé.

b) ACL sur le routeur R2

Des **Listes de Contrôle d’Accès (ACL)** ont été configurées pour :

- n’autoriser que le trafic HTTP (port 80),
- ainsi que les ports 22 (SSH) et 873 (rsync).

c) ACL sur le routeur de bordure

Sur le routeur connecté au réseau extérieur, seules les connexions **ICMP (ping)** et **HTTP (port 80)** en provenance de l’extérieur ont été autorisées.

---

5. Connexion au réseau de l’IUT

À l’aide de l’élément **Cloud** dans GNS3, une **passerelle vers le réseau extérieur** a été mise en place via le routeur R3, permettant à toutes les machines internes d’avoir accès à Internet.

Conclusion

Cette SAE a été particulièrement enrichissante.
Elle m’a permis :

- de maîtriser la conception complète d’un réseau structuré,
- de configurer avec rigueur les VLANs, le routage, les serveurs et les règles de sécurité,
- d’apprendre à planifier un adressage IP avec masques variables,
- et d’automatiser des tâches de synchronisation et de filtrage réseau.

Photo du projet :