

SA21

Construire un réseau informatique pour une petite structure

Contexte pédagogique :

CM 3 séances

TD encadrés 8 séances 1h15 :

TD non encadrés 5 séances 1h15 : (travail en autonomie)

TP 1 séance :

Le travail sera réalisé en **binôme**. Un rendu sera exigé en fin de SAE ainsi qu'une preuve de fonctionnement du montage. Des dépôts sont prévus à chaque fin de séance de SAE non encadrée et serviront d'évaluations intermédiaires. Toute absence de rendu entrainera la note de 0 sur la note intermédiaire (comptant pour 1/5 de la note finale).

Contexte professionnel :

Le professionnel R&T peut être sollicité pour construire et mettre en place le réseau informatique d'une « petite » entreprise multisites. L'objectif est alors de répondre aux besoins de commutation, de routage, de services réseaux de base et de sécurité formulés pour la structure. Ce réseau s'appuie sur des équipements et des services informatiques incontournables mais fondamentaux pour fournir à la structure un réseau fonctionnel et structuré.

Spécificité de la SAE :

Cette SAE se place dans le cadre de la réalisation d'une maquette de réseau (démonstrateur). C'est une pratique courante qui permet de tester des fonctionnalités avant de les mettre en œuvre chez un client par exemple. Dans notre cas nous utiliserons PacketTracer pour réaliser la maquette.

Matériels à votre disposition :

- Ordinateurs des salles de TP réseaux

Logiciels à disposition :

- Logiciel de simulation de réseau PacketTracer

Cahier des charges :

La petite entreprise pour laquelle vous travaillez souhaite mettre en place son réseau d'entreprise. Elle est située sur 3 sites comme présenté sur la *Figure 1*. Veillez à bien utiliser les routeurs 2811 pour l'interconnexion avec le réseau opérateur et le 1841 pour le routeur central (sur lequel vous rajouterez des cartes pour avoir le nombre nécessaire de connexions).

Réseau opérateur :

Vous utiliserez des adresses en /30 pour les liens sur le réseau de l'opérateur. En effet il n'y a dans notre maquette que 2 machines sur ces réseaux.

Site principal :

Il contient les principaux serveurs (DNS / WEB) de l'entreprise. Il possède une structure avec une DMZ (zone démilitarisée) dans laquelle se trouvent justement ces serveurs.

- La DMZ possède un adressage IP publique en 200.0.0.0/24.
- Le réseau interne sera composé d'adresses privées. Une traduction d'adresse sera mise en place pour que ces machines puissent aller sur internet.
- Vous choisirez un nom pour cette entreprise (cela sera utile plus tard pour la partie DNS).
- Vous devrez prévoir le plan d'adressage de toutes les machines.

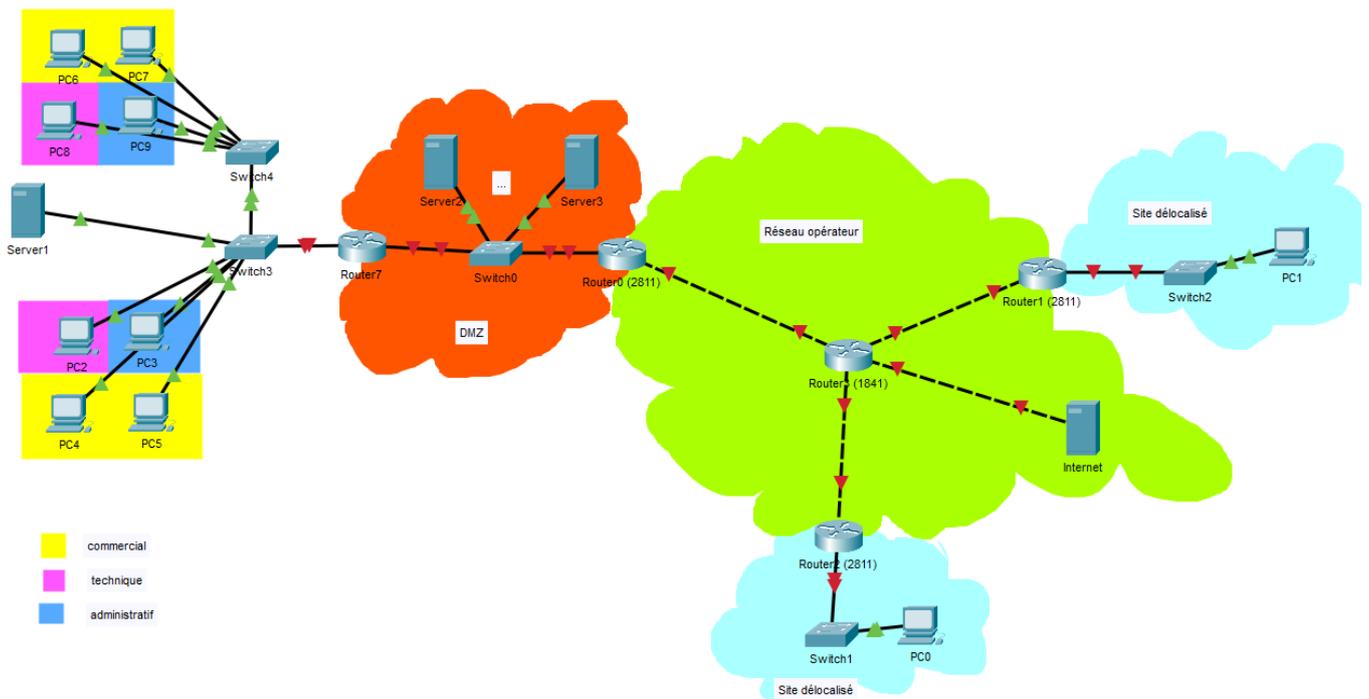


Figure 1: Schéma de principe du réseau.

- Au niveau de la structure de l'entreprise, on retrouve **3 services**, les **administratifs** qui travaillent dans les locaux de l'entreprise, les **commerciaux** qui peuvent être amenés à voyager en dehors des murs de l'entreprise et le **SI** (service informatique) qui doit gérer le réseau et les serveurs. Il y a également des **services internes** (représenté dans la maquette uniquement par site WEB interne pour simplifier).
- L'entreprise souhaite avoir un **serveur web externe** qui contiendra une simple page html avec le nom de l'entreprise. Ce serveur sera placé dans la DMZ et sera accessible à tout le monde.
- L'entreprise souhaite gérer son nom de domaine. Elle a donc un serveur DNS dans la partie DMZ qui référence le serveur WEB externe.

- L'entreprise souhaite également avoir **serveur Web interne** (qui contient des données internes à l'entreprise. On le représentera par une simple page web pour plus de simplicité). Ce dernier ne sera accessible que pour les utilisateurs du réseau interne et via un VPN pour les utilisateurs sur les sites délocalisés.
- On mettra en place un serveur **DHCP** pour le réseau interne pour chaque service.
- On souhaite mettre un peu de sécurité au niveau des échanges entre les différents services pour les isoler les uns des autres, il vous faudra proposer une solution.
- Au niveau des accès, il faudra prévoir des règles de sécurité pour que :
 - Les administratifs aient accès au serveur interne, à la DMZ et à Internet. Ils ne doivent cependant pas avoir accès aux autres réseaux internes.
 - Les commerciaux doivent avoir accès au serveur interne, à la DMZ et à Internet. Ils ne doivent pas non plus avoir accès aux autres services.
 - Le service technique doit avoir accès à tous les services internes, mais ne doit pas pouvoir sortir du réseau interne.
 - La machine administrateur reliée au niveau de la DMZ pour la partie administration des serveurs aura accès aux serveurs mais ne pourra ni aller dans les réseaux internes, ni aller sur internet. Elle ne devra pas être joignable par des machines de l'Internet

Sites délocalisés :

Les sites délocalisés sont censés représenter les commerciaux en déplacement. Ils ne sont donc constitués que d'une machine reliée derrière un routeur (on parle de postes nomades) Au niveau des accès ils doivent pouvoir joindre les machines de la DMZ, le serveur représentant l'Internet et ne doivent pouvoir joindre le serveur WEB interne que grâce au VPN configuré sur leur routeur.

Remarque : Pour simplifier le montage on pourra se limiter à un site distant

Internet :

Internet est représenté par un simple réseau avec un serveur web. Au niveau des accès le serveur doit pouvoir être joint par tout le monde. Le serveur doit pouvoir joindre les machines de la DMZ. En revanche, il ne doit pas pouvoir initier une connexion vers les machines du réseau interne ni les postes sur les sites distants.

Délivrables :

- Le fichier PacketTracer contenant la maquette de votre réseau.
- Trois documents contenant
 - Pour le premier : l'explication de vos choix en termes de sécurité, d'architecture physique du réseau et de plan d'adressage.
 - Pour le deuxième, la liste complète des commandes utilisées pour configurer les équipements actifs de votre réseau.
 - E troisième, la procédure de test (recette) de votre maquette. Attention toutes les fonctionnalités doivent être testées.

Méthodologie d'évaluation :

L'évaluation finale de la SAE portera sur les critères suivants (critères issus du portefeuille) :

L'étudiant agit avec qualité. Il est mieux à même d'Administrer car :

- Il choisit les solutions et technologies réseaux adaptées
- Il respecte les principes fondamentaux de la sécurité informatique
- Il utilise une approche rigoureuse pour la résolution des dysfonctionnements
- Il respecte les règles métiers
- Il assure une veille technologique
- Il lie entre elles les composantes essentielles

L'étudiant a appris et est mieux à même d'Administrer car :

- Il comprend l'architecture des systèmes numériques et les principes du codage de l'information.
- Il sait configurer les fonctions de base du réseau local
- Il maîtrise les rôles et les principes fondamentaux des systèmes d'exploitation afin d'interagir avec ceux-ci pour la configuration et administration des réseaux et services fournis
- Il sait identifier les dysfonctionnements du réseau local
- Il sait installer un poste client
- Il lie entre eux les apprentissages critiques