Sécurité de la couche liaison de données

Introduction

La couche liaison de données du modèle OSI [1)] (couche 2) se charge de transférer les données au sein d'un réseau local.

Comme nous allons le voir tout au long de ce projet, il est nécessaire de protéger physiquement et logiquement l'ensemble des éléments (configuration du câblage, des commutateurs, points d'accès, interfaces, adresses, ...) de la couche 2[2)] pour que les données soient transmises de manière sécurisée.

Situation initiale et objetctif

Contexte

NB: Rien de ce qui va suivre n'existe vraiment, heureusement...

L'entreprise **CORPORATE**, située à Melgven (29) est spécialisée dans l'édition de cartes de visite pour les professionnels Bretons.

Logo de bon goût de l'entreprise.

Elle comprend :

- Une équipe de direction composée d'une dizaine de cadres;
- Un service accueil/secrétariat qui reçoit les nombreuses demandes de renseignement et devis, composé de 10 personnes;
- Un service comptabilité/gestion composé de 5 personnes;
- Une équipe de commerciaux composée de 12 ~~crapul..~~ personnes.

L'entreprise possède un réseau adressé en 10.0.0.0/8 qui comprend l'ensemble des ordinateurs de l'entreprise et un réseau adressé 172.20.0.0/16 comportant plusieurs serveurs : Web, Mail, Stockage, Impression et serveurs d'application métier (création des cartes de visites, gestion, paie, ...). Ces deux réseaux sont connectés au moyen d'un routeur commun situé dans l'entreprise.

Chaque personne est équipée d'un PC fixe à l'exception des commerciaux équipés d'ordinateurs portables.

Schéma logique du réseau de l'entreprise :

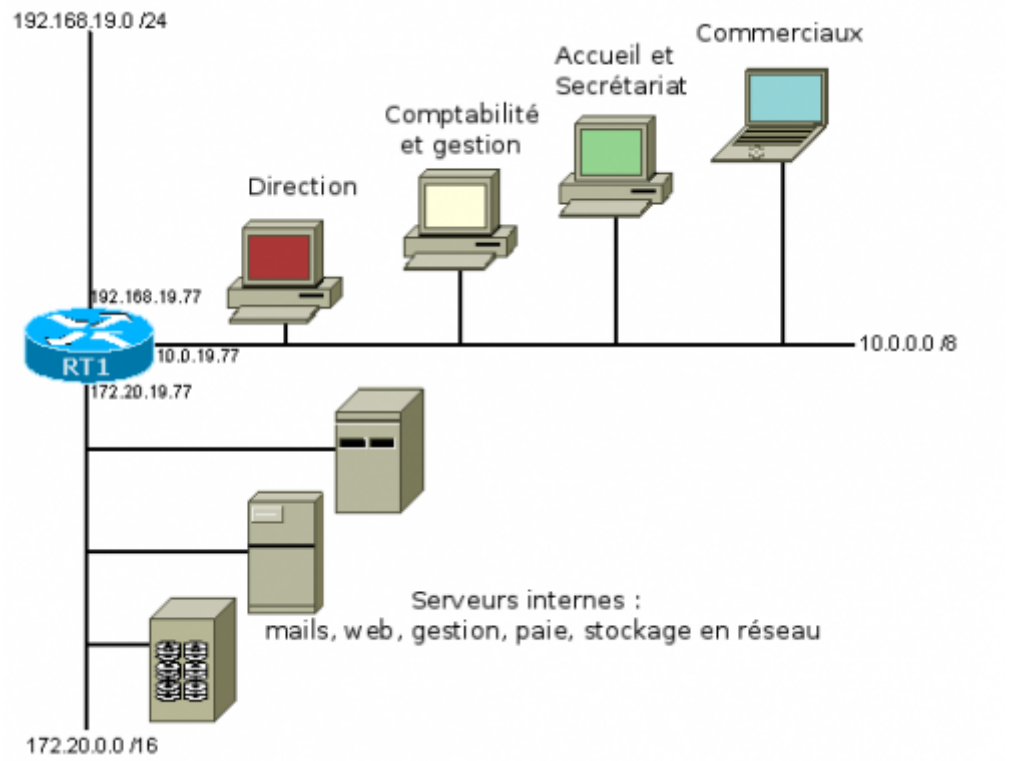
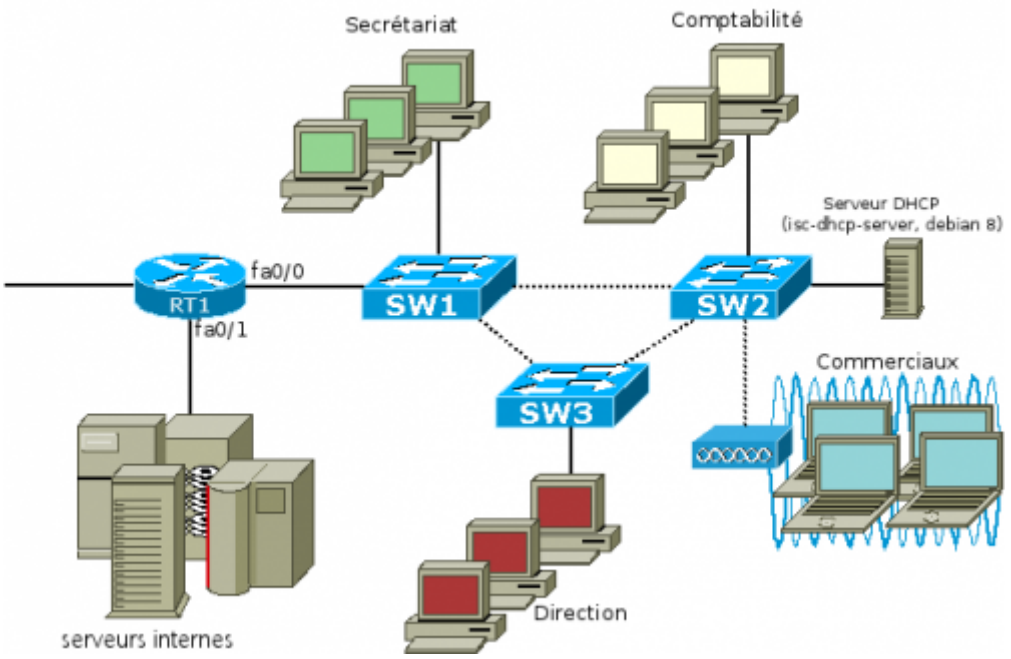


Schéma physique de départ :



L'objectif est naturellement de **sécuriser la transmission des données** sur la couche 2 du modèle OSI.

Sommaire

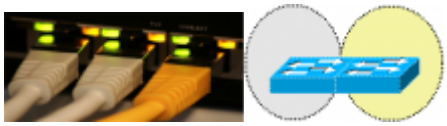
I. Sécurité physique

Protection physique des éléments de la couche 2
Dans ce premier chapitre, nous commencerons par étudier les mesures de protection physique des commutateurs (accès au matériel) et comment se prémunir contre les connexions hasardeuses et les tempêtes de diffusion.

II. Transfert de données et ARP

Vulnérabilités de la couche 2
Nous allons nous intéresser au faiblesses de la couche 2 du modèle OSI, et particulièrement au protocole ARP en démontrant l'efficacité des attaques MIDM[3)].
Nous créerons ensuite un faux serveur DHCP afin de se faire passer pour la passerelle par défaut de nos victimes.
Dans les deux cas nous allons capturer le contenu des échanges sur le réseau.

III. Surveillance, port security, snooping et VLAN



Surveillance, port security, snooping et VLAN
Nous allons voir dans ce chapitre les moyens à notre disposition pour nous protéger des attaques vues dans le chapitre précédent.

IV. Le protocole IEEE 802.1x

Utilisation du protocole IEEE 802.1x
L'ensemble des éléments vus plus hauts restent susceptibles de subir des attaques de type

usurpation d'adresse MAC et si les locaux sont mal protégés, il est possible de se brancher sur une prise réseau prévue pour d'autres.
Comment faire pour identifier et authentifier avec certitude chaque connexion sur la couche 2? C'est ce que nous allons voir dans ce chapitre.

1)

Open Systems Interconnection

2)

NB : nous n'irons pas au delà d'Ethernet (http://www.ieee802.org/3/) dans toute la suite du wiki

3)

Man in the middle