Exercices (suite) : thème 3 - Question 6

Question 6 : Comment les technologies répondent-elles aux besoins de collaboration ?

Exercice 1 : serveur DHCP *(durée indicative : 5 min)*

A droite, une capture d'écran d'informations concernant la configuration d'un serveur DHCP.

Questions :

1. Combien d'équipements pourront être adressés simultanément par ce serveur ?

Le serveur DHCP peut octroyer les adresses IP allant de 172.20.0.20 à 172.20.0.100, soit un total de 81 adresses IP : 100 - 20 + 1 = 81.

2. Pendant combien de temps un équipement pourra-t-il conserver son adresse IP ?

Le serveur DHCP fournit une configuration IP aux hôtes du réseau qui en font la demande. Cette configuration est soumise à un « bail », c'est-à-dire que cette configuration n'est plus valable au-delà d'une certaine durée, lorsque le « bail » a expiré.

La durée du bail est par défaut de 60000 secondes.
Ceci équivaut à 60000/60 = 1000 minutes ou encore 1000/60 ≈ 16,67 heures (16h40 min).

3. Quels sont les paramètres délivrés par le serveur DHCP ?

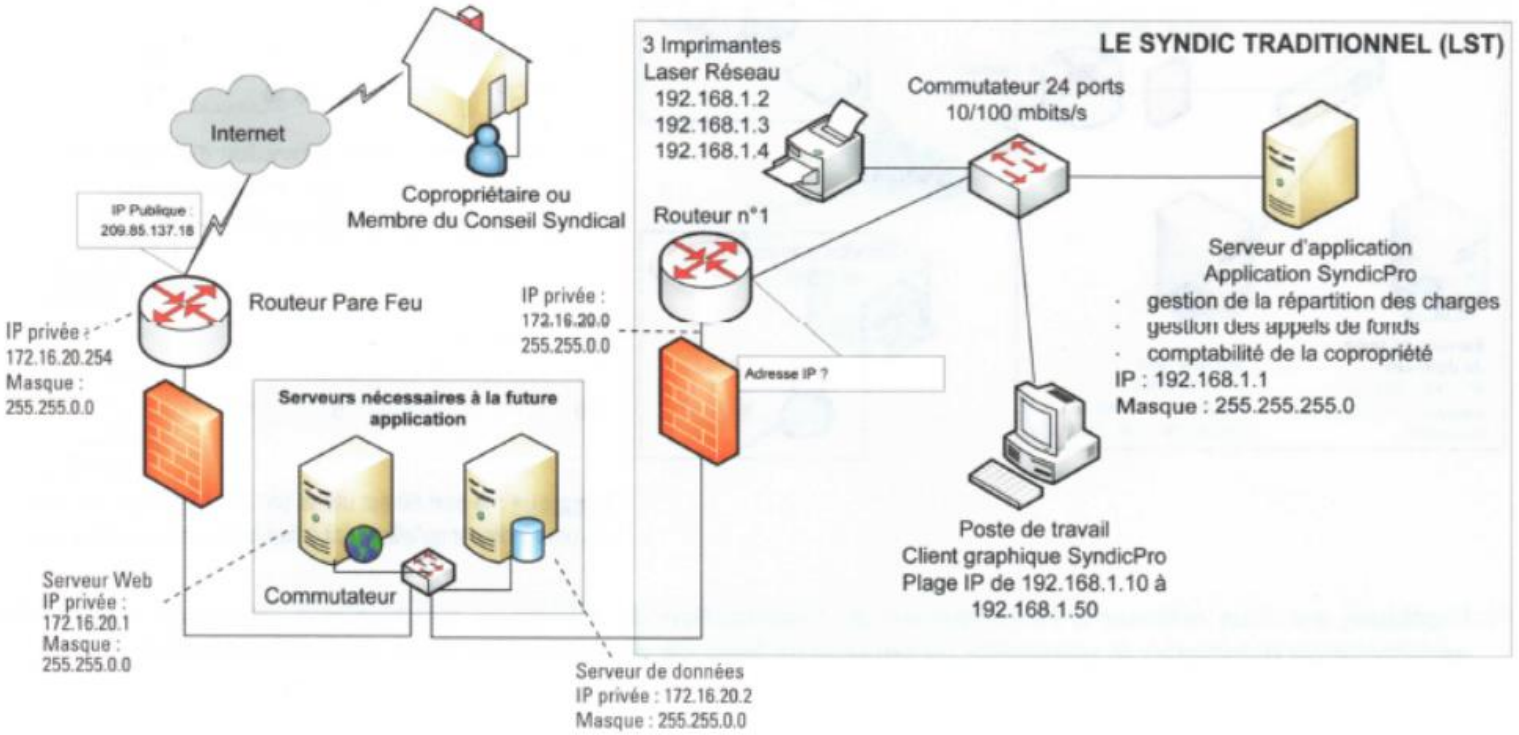
Le serveur DHCP délivre aux hôtes du réseau leur configuration IP, c'est-à-dire toutes les informations nécessaires à ces derniers pour communiquer sur le réseau local mais encore pour pouvoir tenter de communiquer avec l'extérieur du réseau local. Le serveur DHCP délivre en particulier :

- Une adresse IP (privée) => celle-ci permet d'identifier l'hôte sur le réseau local ;
- Un masque de sous-réseau => celui-ci permet d'identifier le réseau local auquel l'hôte appartient, c'est-à-dire de calculer l'adresse IP de son réseau de rattachement (cela permet aussi accessoirement de calculer l'adresse IP de broadcast du réseau) ;
- L'adresse IP de la passerelle => celle-ci permet à l'hôte de savoir par qui il doit passer pour communiquer avec l'extérieur du réseau local.

Exercice 2 : évolution d'un réseau informatique *(durée indicative : 15 min)*

Le Syndic Traditionnel (LST) est une entreprise dont l'activité est la gestion de copropriétés. Une copropriété est une propriété immobilière divisée en lots. Chaque copropriétaire possède un ou plusieurs lots. Chaque lot comporte une partie privative (par exemple un appartement et une cave…) et une quote-part des parties communes.

Pour assurer la gestion des immeubles, le syndic LST utilise actuellement une application informatique « SyndicPro » qui ne permet cependant pas de répondre à tous les besoins, notamment d'information des copropriétaires. LST envisage donc de développer une nouvelle application, nommée EasyCop, offrant un portail d'accès à des services. La mise en place d'EasyCop conduit à modifier l'architecture du réseau (entre pointillés, l'architecture de départ) :



Questions :

1. Expliquer ce que représente l'information 255.255.255.0 qui concerne la configuration IP de chaque hôte du réseau. Expliquer son utilité.

L'adresse IP 255.255.255.0 est le masque de sous-réseau des hôtes du réseau. Cette configuration IP permet de connaître l'adresse IP du réseau et l'adresse de broadcast du réseau auquel chaque hôte appartient.

2. Proposer une adresse IP cohérente pour le route n°1 (sur le schéma ci-dessus).

On peut par exemple lui attribuer l'adresse IP 192.168.1.5 ou tout autre adresse, pourvu que l'adresse IP soit de la forme 192.168.1.X (192.168.1 est la partie réseau des adresses IP du réseau 192.168.1.0), avec X un nombre compris entre 1 et 254 qui n'est pas déjà utilisé par un autre hôte.

3. Indiquer à quelle adresse IP les copropriétaires doivent se connecter pour entre sur le portail LST.

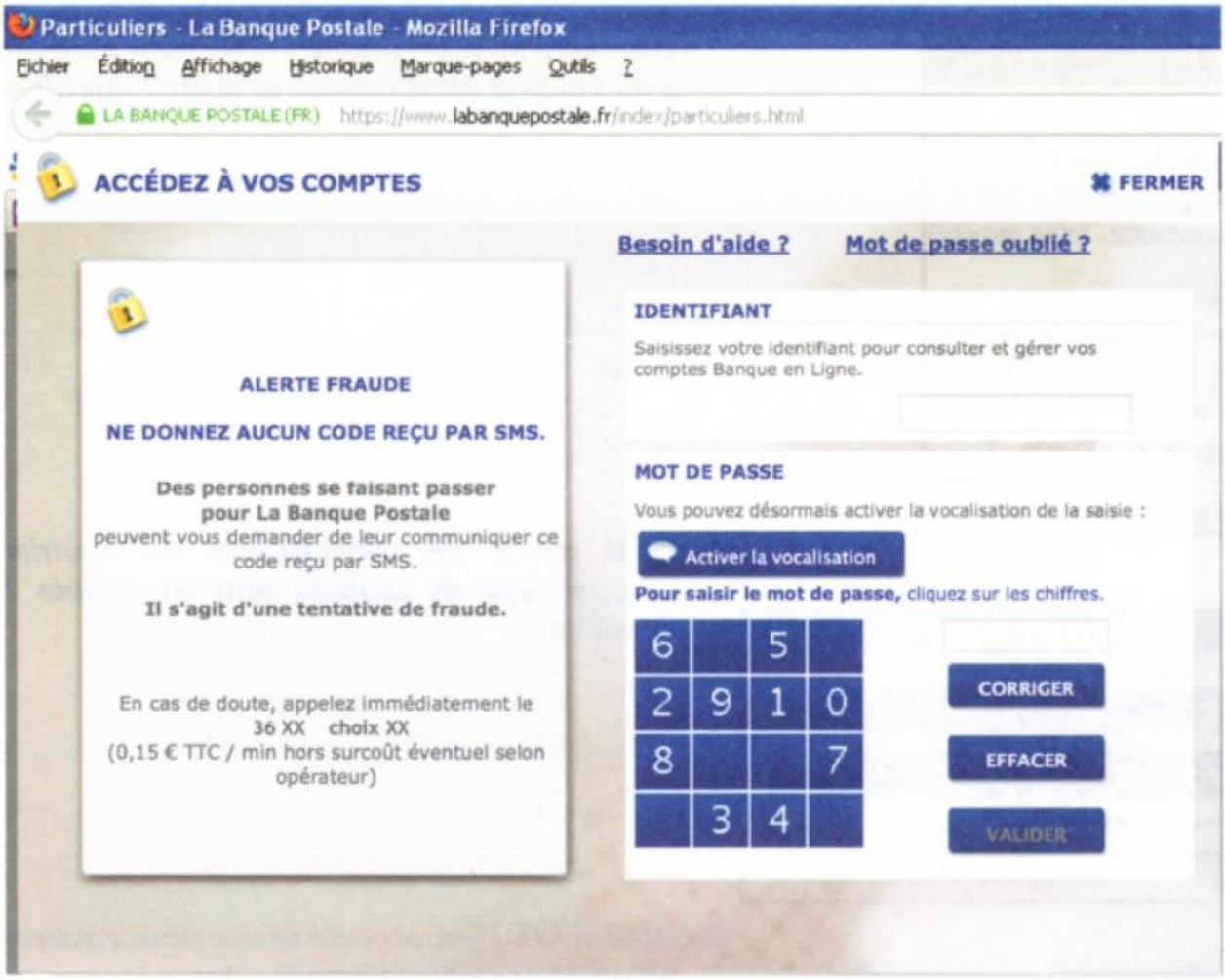
Les adresses IP privée utilisée à l'intérieur du réseau du SYNDIC sont inaccessibles en-dehors du réseau local. Elles sont non routables. Par conséquent, les copropriétaires devront utiliser l'adresse IP publique du routeur (209.85.137.18) s'il veulent se connecter au portail LST.

En pratique, on configurera le routeur pour que les requêtes HTTP et/ou HTTPS (typiquement sur le port 80) transmises à destination de l'IP publique du routeur soient redirigées vers le serveur web (172.16.20.1). Ainsi, pour les copropriétaires, tout se passera comme s'ils s'adressaient directement au serveur web.

4. Expliquer ce qui permet de voir que les nouveaux serveurs ne sont pas sur le même réseau que les autres serveurs de LST. Quelles sont les raisons de ce choix ?

Les nouveaux serveurs ont pour masque de sous-réseau 255.255.0.0 et non 255.255.255.0. Ils sont donc rattachés au réseau local 172.16.0.0 et non 192.168.1.0. Ils ne sont donc pas rattachés au même réseau que le reste du réseau de LST. Ce choix est très probablement motivé par des problématiques de sécurité. Ceci permet d'isoler la partie du réseau de LST qui est accessible de l'extérieur de celle qui n'a aucune raison d'être accessible de l'extérieur. Ainsi, si les serveurs permettant d'accéder au portail LST sont piratés (sur le réseau 172.16.0.0), cela sera potentiellement sans incidence sur les hôtes se trouvant sur le réseau 192.168.1.0.

Exercice 3 : sécurité et piratage



Questions :

1. Repérer des éléments de sécurisation de ce site.

Cette pages web comporte les éléments de sécurisations suivants :

- Le site est sécurisé grâce au protocole HTTPS. Ce protocole permet de chiffrer (=crypter) les messages échangés mais encore de s'assurer de l'authenticité du site internet grâce à un certificat SSL (=certificat d'authenticité), c'est-à-dire que cela assure également à l'utilisateur qu'il se trouve bel et bien sur le site de La Banque Postal ;
- Le site affiche un message d'alerte. Il s'agit d'un message de prévention.
- Le site comporte un système d'authentification (de connexion).
- Le système d'authentification comporte un pave numérique généré aléatoirement, ce qui complique très certainement les tentatives de piratage.

2. Qu'est-ce que le *phishing* (hameçonnage) ?

Extrait Wikipedia : « L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs

pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. »

3. Qu'est-ce que le *pharming* ?

Extrait Wikipedia : « Le pharming (ou dévoiement1 en français) est une technique de piratage informatique exploitant des vulnérabilités DNS. Cette technique œuvre de manière que, pour une requête DNS d'un nom de domaine, ce ne soit pas l'adresse IP réelle du nom de domaine qui soit donnée, mais celle d'un site frauduleux. »

4. Contre laquelle de ces deux techniques les certificats SSL luttent-t-il ?

Le certificat SSL ou certificat d'authenticité permet à l'utilisateur de savoir qu'il s'adresse bien au serveur (en l'occurrence le serveur web de La Banque Postale) auquel il tente d'accéder. Dans le cas présent, il permet d'être certain qu'on est bien sur le site de La Banque Postale. De manière général, cela permet à l'utilisateur de s'assurer de l'authenticité de l'identité du serveur auquel il s'adresse (nom de domaine et adresse IP publique).

Ainsi, le certificat SSL permet de lutter contre le pharming, lequel consisterait ici à usurper l'identité du serveur web de La Banque Postale.