Sommaire

Mise en place d'un système de garde-barrière ou pare-feu (*firewall*), logiciel ou matériel.

Cela permet de bloquer certains ports et donc de diminuer les risques d'intrusion.

On peut admettre de mettre en place un point d'accès aux serveurs *web* qui ne soit pas directement relié au réseau local (zone démilitarisée) mais isolé par un pare-feu et un routeur.

Une solution utilisant un *proxy* (serveur mandataire) qui intègre des systèmes de filtrage entrants et sortant peut également être retenu.

3 cas EPOKA (développeur 2004)

3.1 Désigner le type du matériel d'interconnexion MATINTER *et définir son rôle.*

Le matériel d'interconnexion *MATINTER* est un **routeur**. Un routeur est connecté à plusieurs réseaux IP, à ce titre il dispose d'une adresse IP sur chaque réseau. Ceci lui permet de faire circuler les paquets entre les différents réseaux IP. Il peut également être
On acceptera le terme de **passerelle** : par contre, on attend en explication le rôle d'un routeur.

3.2 Expliquer la cause de ce problème et proposer le paramétrage IP opérationnel du poste de travail « P01 ».

Le message d'erreur *« Impossible de joindre l'hôte de destination »* est dû à une configuration incomplète de l'adressage IP du poste de travail « P01 ».
En effet, en appliquant le masque réseau 255.255.255.0 sur l'adresse IP de l'expéditeur et sur l'adresse IP du destinataire, le poste « P01 » détermine que les 2 correspondants appartiennent à des réseaux IP distincts. Il ne peut donc émettre le paquet sur le réseau, à moins de connaître l'adresse IP d'un routeur qui, lui, sait acheminer les paquets sur différents réseaux IP.
L'erreur vient donc du fait que la passerelle n'est pas renseignée dans la configuration IP du poste de travail « P01 ».

Cela ne peut venir du routeur puisque le routeur répond à la même commande lancée par « P02 » (ce qui sous-entend que l'adresse IP et le masque de « P02 » ne l'empêche pas de communiquer au delà du routeur).

Cela ne peut venir de la carte réseau ou du câble de « P01 » puisque la commande lancée par « P01 » sur « P03 » et ne passant pas par le routeur fonctionne aussi (ce qui démontre au passage que l'adresse IP et le masque de « P01 » sont corrects).

Modifier le masque réseau et le passer à 255.255.0.0 éviterait l'utilisation du routeur mais cela ne fonctionne que si les postes sont sur le même segment physique, ce qui est douteux compte tenu du schéma et ne correspond pas au cahier des charges.
Modifier l'adresse IP pour intégrer le poste sur le même réseau éviterait aussi l'utilisation du routeur mais cela ne fonctionne toujours que si les postes sont sur le même segment physique et cela empêche la communication avec « P02 » et « P03 » et reste contraire au cahier des charges.

Le paramétrage IP opérationnel du poste de travail « P01 » est donc le suivant :
Adresse IP : 192.168.10.21
Masque réseau : 255.255.255.0
Adresse IP passerelle : 192.168.10.1 (adresse IP du routeur sur le réseau IP 192.168.10.0)

3.3 Recenser les protocoles d'application mis en œuvre entre les postes clients et le serveur de messagerie d'une part, entre les postes clients et le serveur web *d'autre part. Préciser le rôle de chaque protocole.*

Le dialogue entre les postes clients et le serveur de messagerie repose sur le protocole **SMTP** (*Simple Mail Transfer Protocol*) pour l'envoi du courrier sortant. C'est le protocole **SMTP** qui est également en charge d'acheminer le courrier de serveur en serveur jusqu'au serveur destinataire.
Pour la réception du courrier entrant, le dialogue repose sur l'un des protocoles **POP** (*Post Office Protocol*) ou **IMAP** (*Internet Mail Access Protocol*).
Le protocole POP procède simplement à un transfert des messages reçus du serveur vers le client, avec suppression définitive de ces messages côté serveur. Le protocole **IMAP** est plus riche en fonctionnalités (possibilité de télécharger uniquement les en-têtes de messages).
A noter que les protocoles POP et IMAP imposent au client de s'authentifier (login + mot de passe) pour pouvoir accéder au courrier entrant.

Le dialogue entre les postes clients et le serveur *web* repose sur le protocole **HTTP** (*HyperText Transfer Protocol*). C'est un protocole texte qui s'appuie sur des requêtes émises par le client portant sur l'obtention de pages HTML. Le serveur *web* renvoie des réponses contenant les pages demandées.

On peut également citer le format **MIME** (*Multipurpose Internet Mail Extensions*) pour encoder le contenu des messages. Il permet d'encoder tout type de données et d'adjoindre des fichiers de toute taille. Ce format est utilisé conjointement aux protocoles HTTP, SMTP, POP et IMAP.

Remarques :
Certaines réponses peuvent citer le protocole DNS, mais celui-ci n'est pas exigé car il se situe en amont du dialogue entre le client et les serveurs *web* et de messagerie, pour récupérer l'adresse IP correspondant au nom de machine.

La citation d'autres protocoles (FTP, HTTPS, …) ne sera pas pénalisée.

4 Cas Polymousse (réseau 2005)

4.1 Expliquer à quelle classe correspond l'adresse 10.0.0.0 et donner le masque de sous-réseau par défaut correspondant à cette classe.

L'adresse 10.0.0.0 est comprise entre 1.0.0.0 et 127.0.0.0, elle correspond donc à une classe A.
- Le masque de sous-réseau associé à une classe A est 255.0.0.0.

4.2 Calculer le nombre maximum de divisions que le plan d'adressage permet de définir.

Le plan d'adressage prévoit 16 bits pour le masque de sous réseau des divisions, soit 8 bits (16 – 8) pour la partie sous réseau. Ce qui permet d'adresser 256 (2^8) sous-réseaux.

4.3 Donner le masque de sous-réseau qui permet d'adresser les 11 sous-réseaux des succursales de la division Espagne. **Justifier la réponse**

Pour adresser un minimum de 11 sous-réseaux, il faut au minimum prélever 4 bits sur la partie hôte. On dispose alors de 16 (2^4) sous-réseaux.

- Pour les divisions, le masque est déjà sur 16 bits, pour les succursales de l'Espagne, le masque sera donc sur 20 bits (16 + 4). Soit 255.255.240.0

4.4 Indiquer les adresses IP des sous-réseaux accessibles, en utilisant la première ligne de la table de routage du routeur nommé R.Belgique, présentée sur l'annexe 1. Expliquer la réponse

- La première ligne de la table de routage fait référence à un masque de 20 bits donc toutes les adresses disposant des mêmes 20 premiers bits seront routées :

Soit les succursales

S2 **: 00001010.00001010.0001**0001.0 soit 10.10.17.0
S3 **: 00001010.00001010.0001**0010.0 soit 10.10.18.0
S4 **: 00001010.00001010.0001**0100.0 soit 10.10.20.0

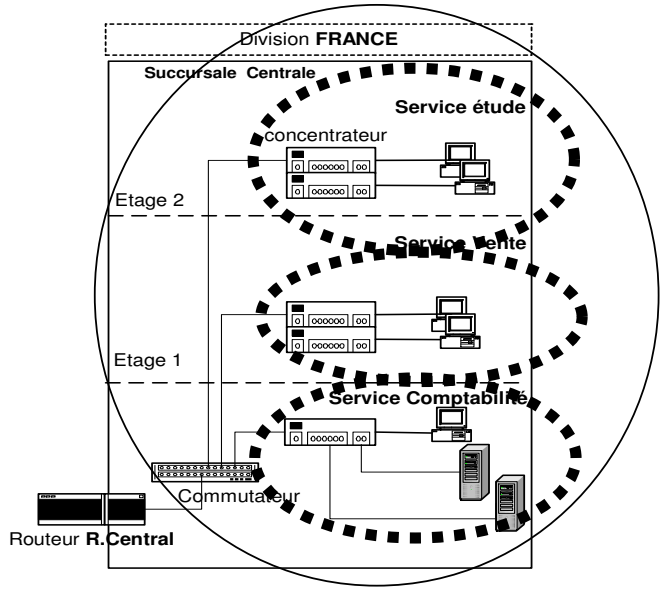
4.5 Donner le nombre de domaines de collision et le nombre de domaines de diffusion présents dans le réseau de la division France

Un domaine de diffusion (*broadcast domain*) est une aire logique d'un réseau informatique où n'importe quel ordinateur connecté au réseau peut directement transmettre à tous les autres.

Un domaine de collision est une zone logique d'un réseau informatique où les trames de données peuvent entrer en collision entre elles. Dans le cas du réseau Ethernet, le domaine de collision comprend l'ensemble des segments connectés par des concentrateurs ou répéteurs.

Il y a **3 (ou 4) domaines de collision et 1 domaine de diffusion,** le segment entre le routeur et le commutateur peut-être considéré comme un domaine de collision.

- Soit le schéma suivant.



Domaine de diffusion
Domaine de collision

5 Cas Viste (réseau 2004)

5.1 Expliquer la cause de ce dysfonctionnement et proposer une solution qui, sans acquisition de matériel supplémentaire, permettrait de connecter l'ordinateur portable à partir de chacun des trois sites.

L'analyse de l'**annexe** et le texte nous indiquent la présence d'un serveur DHCP desservant le réseau local des bureaux (« *dont les postes sont configurés en adresse IP dynamique* »). Lors de la connexion du portable sur le réseau local des bureaux, au moyen du point d'accès WiFi, le serveur DHCP doit normalement attribuer une adresse IP au portable. La connectivité du portable au réseau est donc assurée de façon transparente.

Sur le plan, on constate que pour le chai et la cave, les postes clients ont une adresse IP fixe. Le serveur DHCP se trouve de plus « de l'autre coté » d'un routeur, donc inaccessible aux demandes DHCP non relayées.

Les solutions à déployer sont donc :

- soit la mise en place d'un relais DHCP en précisant la nécessité d'ajouter de nouvelles étendues sur le serveur DHCP existant (*cette solution est d'ailleurs celle « présentée » dans l'**annexe 2***),
- soit l'activation d'un serveur DHCP qui pourrait être inclus dans les points d'accès (AP - *Access Point*) WiFi, ou mis en place sur l'une des stations si le système d'exploitation le permet.

5.2 Indiquer la classe, l'adresse réseau et le nombre d'hôtes que peut accueillir chacun des sous-réseaux représentés dans le nouveau plan d'adressage. Vous justifierez vos réponses.

Réseau 1 : 192.168.0.0/29 (locaux techniques, DMZ)

- 192 en binaire 1100 0000 => début par 110 => Classe C
- Adresse réseau : 192.168.0.0
- Nombre d'hôtes : masque sur 29 bits => reste 3 bits pour les hôtes. On dispose donc de 2^3 soit 8 adresses, on enlève [000] et [111] il reste donc 6 hôtes possibles (2^3 - 2).

Réseau 2, 3, 4 : 172.16.0.0/24, 172.16.1.0/24 (Chai), 172.16.2.0/24 (Cave),

- 172 en binaire 1010 1100 => début par 10 => Classe B
- Adresse réseau : 172.16.0.0, 172.16.1.0, 172.16.2.0
- Nombre d'hôtes : masque sur 24 bits => reste 8 bits pour les hôtes. On dispose donc de 2^8 soit 256 adresses, on enlève [0000 0000] (adresse de « réseau ») et [1111 1111] (adresse de *broadcast*) il reste donc 254 hôtes possibles (2^8 - 2).

*Remarque : 2^8 n'est pas considéré comme une réponse valable, les deux adresses 0000 0000 et 1111 1111 doivent **impérativement** être exclues !*

5.3 Indiquer en quoi une telle configuration est utile.

En cas de défaillance du serveur DHCP basé sur la base WiFi, le relais DHCP est présent ici, pour assurer la « continuité de service ». Dans ce cas, il faut prévoir sur les différents serveurs DHCP des étendues de secours pour les sous-réseaux pour lesquels on veut assurer la tolérance de panne.

5.4 Expliquer les principales différences techniques qui existent entre l'ADSL actuel et le SDSL proposé par la société de service.

L'ADSL (*Asymetric Digital Subscriber Line*) autorise un débit montant plus faible que le débit descendant (ce qui est observable sur le schéma de l'annexe 1.1). Le SDSL (*Symetric Digital Subscriber Line*) permet un débit montant **identique et garanti** au débit descendant (ce qui est observable sur le schéma de l'annexe 1.2).