Techniques de Réseaux Informatiques (TRI)

Elaboré par : A. EL GHATTAS

Janvier 2010

INTRODUCTION

« PREPAnet pour réussir à l'examen… » vient pour aider les stagiaires de la filière Techniques de Réseaux Informatiques (TRI), deuxième année, à se préparer pour l'examen de fin de formation théorique. Vous trouverez des exercices, des études de cas,…avec corrigés, vous trouvez aussi les énoncés des examens de fin de formation des dernières années.

A. EL GHATTAS
Errachidia, le 12 Avril 2009

RAPPEL

Le calcul de la moyenne générale est comme suit :
Moyenne générale de fin de formation : (moyenne de passage + moyenne des modules×2 + moyenne de la théorie×2 + moyenne de la pratique×3 + moyenne de la communication)/9
Avec : moyenne de la communication = (arabe + français + anglais)/3
Exemple : un stagiaire ayant obtenu les notes suivantes :
Moyenne de passage : **09**/20
Moyenne des modules : **12**/20
Moyenne de la théorie : **08**/20
Moyenne de la pratique : **11**/20
Arabe : **13**/20
Français : **10**/20
Anglais : **07**/20
A pour moyenne générale : **10.22**/20 ➔admis
On rappelle aussi que :

- Les stagiaires ayant obtenu aux examens de fin de formation, une moyenne générale supérieure ou égale à 09/20 et inférieure à 10/20 seront soumis aux délibérations du CGCP en vue de décider:

- soit de les autoriser à redoubler;
- soit de les exclure.

- Le droit au redoublement n'est accordé qu'une seule fois durant le cycle de formation.
- Tout stagiaire ayant obtenu une moyenne inférieure à 09/20 aux examens de fin de formation est automatiquement exclu.

SOMMAIRE

Exonet 1 : URL, Web, FTP, messagerie électronique……. 6
Corrigé : …… 9
Exonet 2 : Web, FTP, courrier électronique…… 11
Corrigé : …… 13
Exonet 3 : Linux, FTP, intranet……... 15
Corrigé : …… 18
Exonet 4 : messagerie électronique, trame Ethernet…… 20
Corrigé : …… 24
Exonet 5 : sous réseaux, proxy…… 25
Corrigé : …… 26
Exonet 6: ISA Server (firewall, VPN,…)…….. 27
Corrigé : …… 28
Exonet 7 : firewall, virus, chiffrement……. 29
Corrigé : …… 33
Exonet 8 : VLAN, routage, firewall, proxy……. 35
Corrigé : …… 41
Exonet 9 : configuration d'un routeur, ACL…… 43
Corrigé : …… 49
Exonet 10 : routage, NAT/PAT, Proxy……... 51
Corrigé : …… 53
Exonet 11 : routage et adressage……. 55
Corrigé : …… 59
Exonet 12 : adressage de sur-réseau, routage…….. 61
Corrigé : …… 62
Exonet 13 : DNS et la délégation de zone……... 63
Corrigé : …… 69
Exonet 14 : sous adressage, DHCP……. 72
Corrigé : …… 74
Exonet 15 : adressage, routage, DNS…….. 78
Corrigé : …… 82
Exonet 16 : adressage, routage, firewall…….. 84
Corrigé : …… 87
Exonet 17 : adressage, DHCP, sécurité…… 89
Corrigé : …… 92
Exonet 18 : routage, firewall, ARP…….. 95
Corrigé : …… 100
Exonet 19 : adressage, DHCP, HTTP…….. 103
Corrigé : …… 106
Exonet 20 : routage, DHCP……. 108
Corrigé : …… 116
Exonet 21 : VLAN, DHCP, filtrage……. 119
Corrigé : …… 124
Exonet 22 : routage, DNS, proxy, chiffrement…… 126
Corrigé : …… 132
Exonet 23 : VLAN, DNS, filtrage…… 136
Corrigé : …… 142

Exonet 24 : routage, sécurité…… 145
Corrigé : …… 150
Exonet 25 : commutation, sécurité……... 153
Corrigé : …… 159
Exonet 26 : commutation, routage, filtrage…….. 162
Corrigé : …… 170
Exonet 27 : VPN, table de routage, VLAN, Wi-Fi…… 173
Corrigé : …… 178
Exonet 28 : DHCP, DNS, VLAN……..…….. 182
Corrigé : …… 189

EXONET N° 1

Pour se préparer pour les examens de fin de formation, vous sollicitez l'aide de votre formateur pour vous donner les sujets et corrigés des épreuves d'examen de la filière TRI des années précédentes.
Il vous fournit pour cela un point de départ, l'adresse d'un site Internet dont il apprécie régulièrement la pertinence, le site : **http://www.tri-errachidia.org.ma**

Navigation dans le site
Sur votre poste de travail connecté à Internet, vous utilisez votre navigateur et saisissez l'adresse fournie.

1. Analysez la structure de l'adresse fournie : « http://www.tri-errachidia.org.ma».
2. Expliquez les opérations qui se sont déroulées entre le moment où vous avez saisi votre adresse et celui où elle s'est affichée comme présenté ci-dessus.
Quel est le protocole qui a alors été mis en jeu, entre quelles machines s'est il entremis et quelle en est la finalité ?

Recherche d'un examen

Dans l'écran précédent, vous choisissez dans le menu le lien « Téléchargement FTP » ce qui vous conduit à l'écran :

Vous choisissez « examens »…

…et vous voyez le dossier « examen de fin de formation » dans lequel vous trouvez les différents documents qui vous intéressent.

3. Quelles différences constatez-vous ici dans la mise en œuvre des protocoles HTTP et FTP ?

4. Analysez la structure de l'adresse « ftp://ftp.tri-errachidia.org.ma/ » qui apparaît dans la barre d'adresse de votre navigateur.

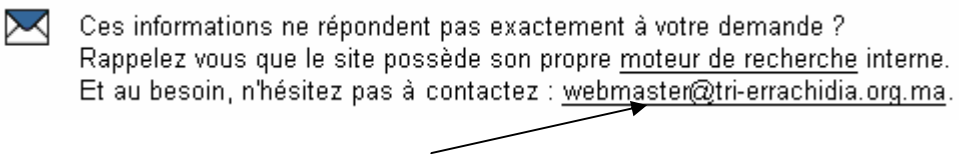
5. Votre navigateur prend-il en charge aussi bien le protocole HTTP que le protocole FTP ?

6. Quelles sont les informations qui apparaissent lorsqu'on visite un « site FTP » ? Comment sont-elles structurées ?

Recherche complémentaire

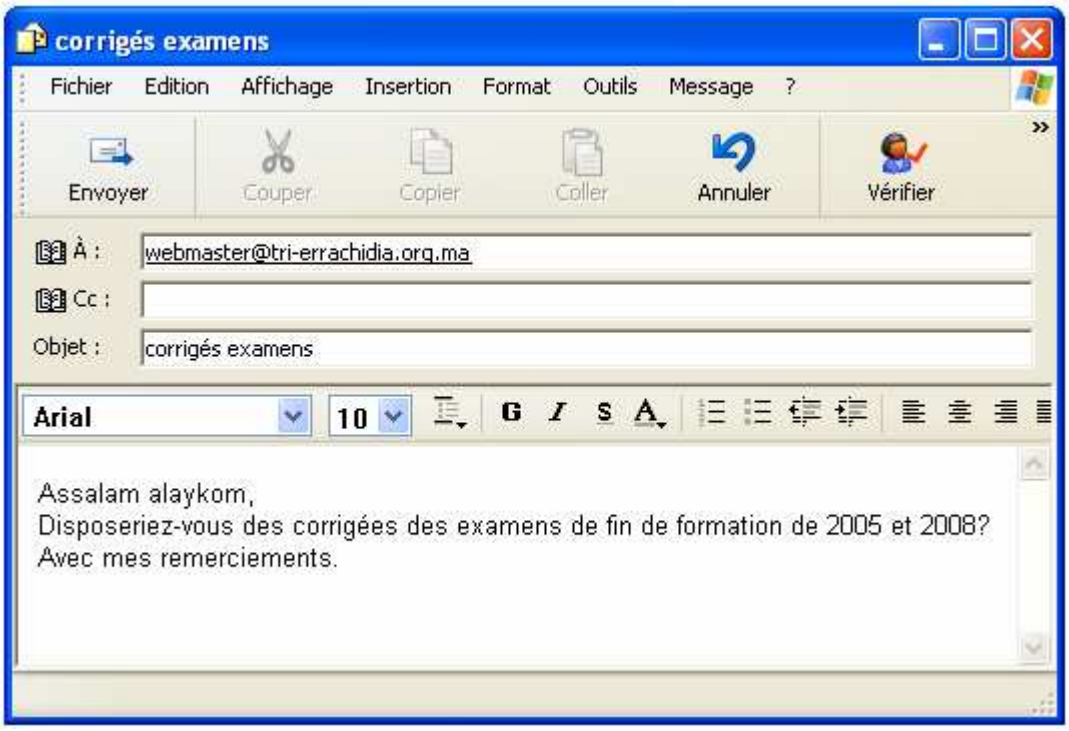
Le document que vous avez téléchargé répond partiellement à vos besoins, il vous manque les corrigés de quelques examens. Vous pensez que ces informations ne sont peut-être fournies que sur demande express.

Dans le bas de la page « Téléchargement FTP », vous avez repéré une information qui peut vous être utile :



Vous cliquez sur le lien « webmaster@tri-errachidia.org.ma ».

Ce clic ouvre votre gestionnaire de courrier, dans lequel vous saisissez votre demande avant de l'envoyer :



7. Analysez la structure de l'adresse « webmaster@tri-errachidia.org.ma »

8. Pourquoi votre gestionnaire de courrier a-t-il été automatiquement ouvert ?

9. Quel est le protocole mis en œuvre lorsque vous expédiez ce courrier ?

10. De quels outils logiciels disposerez-vous pour prendre connaissance de la réponse et quels sont les protocoles utilisés pour la relève du courrier ?

Corrigé Exonet N° 1

Question 1. Analysez la structure de l'adresse réticulaire (URL) fournie : « **http://www.tri-errachidia.org.ma** ».

Comme son nom l'indique, une URL (Uniform Resource Locator) permet d'identifier une ressource dans l'espace Internet ; une ressource est une page fournie par un serveur à un client selon un certain protocole ; chez le client la page codifiée à l'aide du langage HTML est affichée après avoir été interprétée par son explorateur.
Le client, c'est la machine de l'utilisateur disposant de l'explorateur Internet Explorer dans notre exemple.

http : nom du protocole utilisé pour le dialogue entre le serveur et le client.

www : nom du serveur fournissant les ressources. Ce nom est choisi arbitrairement par son administrateur ; traditionnellement, c'est www mais ce n'est pas une obligation. Ce n'est pas un nom de machine physique, mais celui d'un service Web implémenté dans une machine.

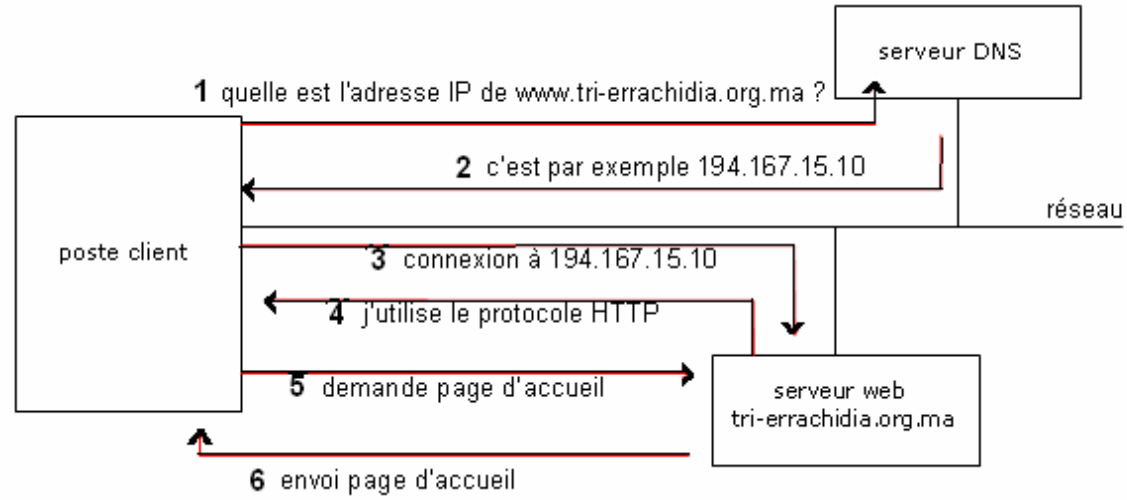
tri-errachidia.org.ma :nom du domaine (ma) dans lequel se trouve un sous-domaine (org) , réservé pour quelques organisations, qui contient le sous sous domaine (tri-errachidia).
Les caractères : ou / sont des séparateurs.

Question 2. Expliquez les opérations qui se sont déroulées entre le moment où vous avez saisi votre adresse réticulaire et celui où elle s'est affichée comme présenté ci-dessus.
Quel est le protocole qui a alors été mis en jeu, entre quelles machines s'est il entremis et quelle en est la finalité ?

Entre la saisie de l'adresse « www.tri-errachidia.org.ma » et l'obtention de la page affichée avec une adresse complétée dans la barre d'adresse, on peut constater que notre client a réussi à obtenir la réponse à deux questions :

- où se trouve la machine que je désire joindre ?
- quel est le protocole de communication qu'elle utilise ?

1. Où est la machine www.tri-errachidia.org.ma ? : un serveur DNS (Domain Name Server) dont l'adresse IP est connue de mon poste de travail me fournit la réponse sous la forme de son adresse IP.
2. Quel est le protocole de communication qu'elle utilise ? : une requête envoyée par mon poste client à destination de la machine dont on connaît maintenant l'adresse IP reçoit une réponse de la part de ce serveur qui inclut le protocole qu'il utilise (HTTP). La demande de la page d'accueil du serveur selon ce protocole permet alors l'affichage observé.



Question 3. Quelles différences constatez vous ici dans la mise en œuvre des protocoles HTTP et FTP ?

Pages affichées selon le protocole HTTP :
- affichage sous forme de texte riche ;
- contenu varié : essentiellement du texte mais aussi des objets divers (images, animations…) ;
- présence de liens hypertextes (navigation entre les pages).

Pages affichées selon le protocole FTP :
- affichage sous la forme d'un explorateur ;
- accès une arborescence de dossiers.

Question 4. Analysez la structure de l'adresse « **ftp://ftp.tri-errachidia.org.ma/** » qui apparaît dans la barre d'adresse de votre navigateur.

ftp : le nom du protocole utilisé ici ;
ftp.tri-errachidia.org.ma :le serveur nommé ftp dans le sous domaine tri-errachidia du sous domaine org du domaine ma
On visualise les différents dossiers présents sur ce serveur.

Question 5. Votre navigateur prend il en charge aussi bien le protocole HTTP que le protocole FTP ?

On constate que le navigateur utilisé ici, mais ce sera aussi le cas pour d'autres navigateurs, dialogue avec un serveur aussi bien selon le protocole HTTP que FTP.
Ce protocole est imposé par le serveur. Le client doit donc pouvoir s'y adapter.

Question 6. Quelles sont les informations qui apparaissent lorsqu'on visite un « site FTP » ? Comment sont elles structurées ?

Le navigateur présente une arborescence de dossiers.

Question 7. Analysez la structure de l'adresse « **webmaster@tri-errachidia.org.ma** »

webmaster :nom d'une boîte aux lettres électronique.
tri-errachidia.org.ma :dans le sous domaine tri-errachidia du sous domaine org du domaine ma.
@ : séparateur.

Question 8. Pourquoi votre gestionnaire de courrier a t il été automatiquement ouvert ?

Parce que sur votre poste il existe une association préinstallée entre le protocole d'envoi de courrier (SMTP) et l'application que vous utilisez par défaut pour expédier votre courrier.

Question 9. Quel est le protocole mis en œuvre lorsque vous expédiez ce courrier ?

C'est le protocole SMTP (Simple Mail Transfer Protocol).

Question 10. De quels outils logiciels disposerez vous pour prendre connaissance de la réponse et quels seront les protocoles utilisés pour la relève du courrier ?

On peut prendre connaissance de la réponse directement sur le serveur en utilisant son navigateur ; c'est le cas de la consultation par exemple des boîtes Gmail, HotMail. L'utilisateur envoie des requêtes au serveur de courrier et en reçoit les réponses sous protocole HTTP (présentation des données). Le traitement du courrier sur le serveur est alors réalisé par le protocole IMAP (Internet Message Access Protocol) : consultation du courrier, suppression...
On peut également utiliser un logiciel de gestion de courrier (on parle de « client de messagerie »), par exemple Microsoft Outlook (Express), Qualcomm Eudora qui va transférer le message sur la machine du client ; dans ce cas, ce logiciel recourt au protocole POP3 (Post Office Protocol version 3) ou IMAP.

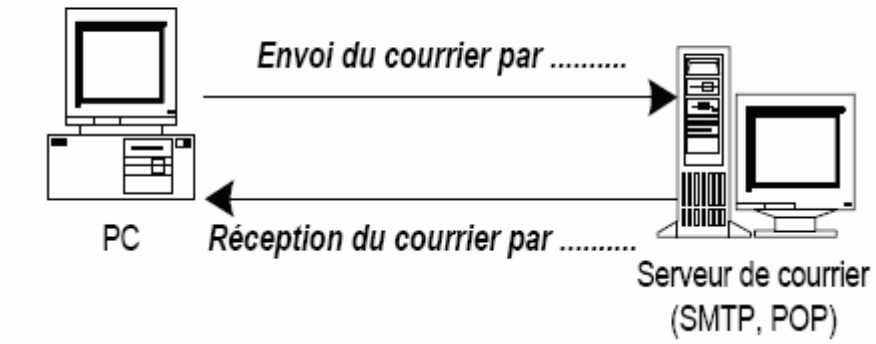
EXONET N° 2

Dans le cadre du développement de Internet et Intranet, l'entreprise **REZOnet** a installé un serveur Linux et l'a connecté au niveau du commutateur des ses serveurs centraux. Pour réaliser l'accès vers le monde extérieur, un accès RNIS a été retenu. Ce serveur Internet aura pour rôle de:
- gérer le courrier électronique du REZOnet
- diffuser les informations du site Web local
- filtrer les données

1. Donner la définition et le rôle de WWW, HTML et HTTP ?
2. On vous donne l'URL suivant: http://www.microsoft.com/products/pc.htm
- Donner la définition et le rôle d'une URL
- Décomposer cette URL en différentes parties en donnant le rôle de chacune d'entre elles
3. Par quel moyen fait-on la correspondance entre l'adresse IP d'un serveur et son nom sur Internet ?
4. Donner la définition et le rôle de SMTP
5. Donner la définition et le rôle de POP
6. Donner la syntaxe générale d'une adresse e-mail
7. Compléter (Annexe 1) l'interaction entre un client et un serveur SMTP et POP
Tout personnel autorisé pourra se connecter au serveur Linux depuis son domicile soit pour consulter des données spécifiques, soit pour naviguer sur le Web.
8. Citer 4 possibilités d'accès à un fournisseur d'accès Internet.
Il vous faut configurer un poste sous Windows 98 afin de permettre une connexion au fournisseur d'accès Internet.
9. Compléter l'annexe 2 (Point d'accès: 05 35 57 57 57, Serveur DNS: 212.217.0.1, Adresse IP obtenue par mon fournisseur, Domaine: rezonet.ma, Hôte : localhost, Nom utilisateur de connexion : admin@rezonet.ma, mot de passe : a5b6cde_rezo).
10. Pour un accès par RTC, donner le type de protocole utilisé.

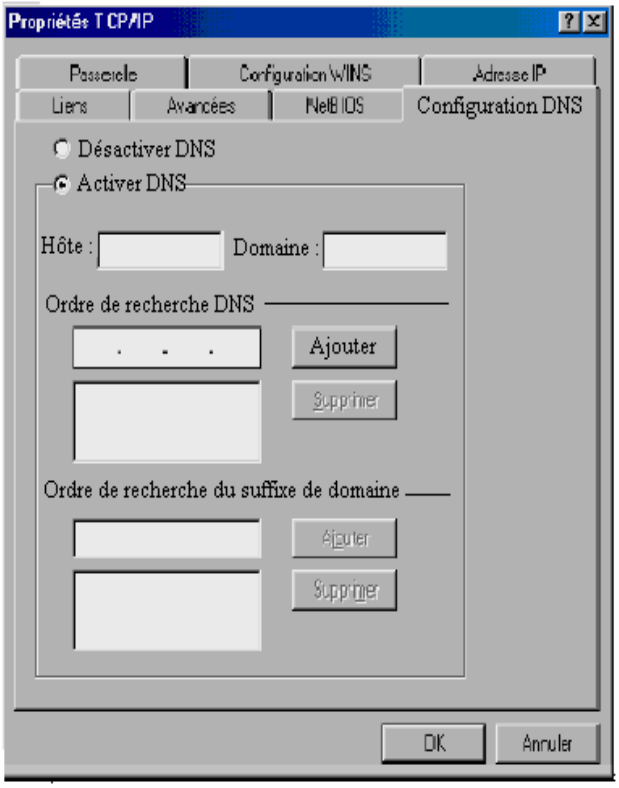
Annexe 1

Interaction entre un client et un serveur SMTP et POP



Annexe 2

Configuration de Windows98 pour un accès à Internet



Corrigé Exonet N° 2

Question 1. Donner la définition et le rôle de WWW, HTML et HTTP ?

Le World Wide Web (WWW ou Web ou W3) est une banque d'informations (textuelles, imagées, sonores vidéo) basé sur un système de noeuds et de liens qu'on nomme hypertexte.
Hyper Text Markup Language (HTML) : Langage utilisé dans le WWW pour écrire des documents hypertextes.
HyperText Transfer Protocol (HTTP). Protocole de transfert de fichiers et documents HTML sur Internet.

Question 2. On vous donne l'URL suivant: http://www.microsoft.com/products/pc.htm
- Donner la définition et le rôle d'une URL
- Décomposer cette URL en différentes parties en donnant le rôle de chacune d'entre elles

Une URL (Uniform Resource Locator) donne l'emplacement d'un fichier sur le Web.
http : Protocole
www.microsoft.com : emplacement réseau / domaines
products : chemin / répertoire
pc.html : nom du fichier

Question 3. Par quel moyen fait on la correspondance entre l'adresse IP d'un serveur et son nom sur Internet ?

Serveur DNS

Question 4. Donner la définition et le rôle de SMTP

Le courrier électronique sur TCP/IP et sur Internet utilise le protocole SMTP (Simple Mail Transfer Protocol).

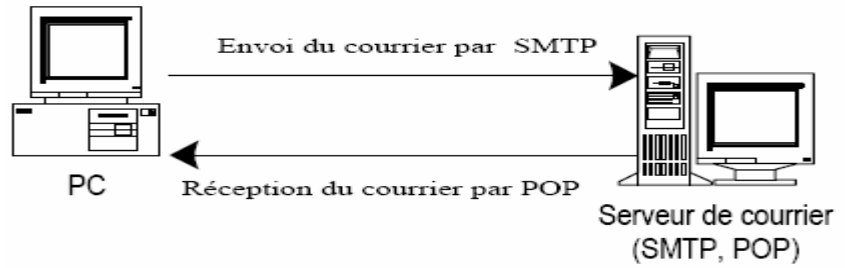
Question 5. Donner la définition et le rôle de POP

Le protocole POP (Post Office Protocole) permet d'aller chercher son courrier personnel sur le serveur responsable de le recevoir.

Question 6. Donner la syntaxe générale d'une adresse e-mail

Une adresse de courrier électronique est formé de trois parties : le nom de l'utilisateur, le caractère @ et le nom du domaine.

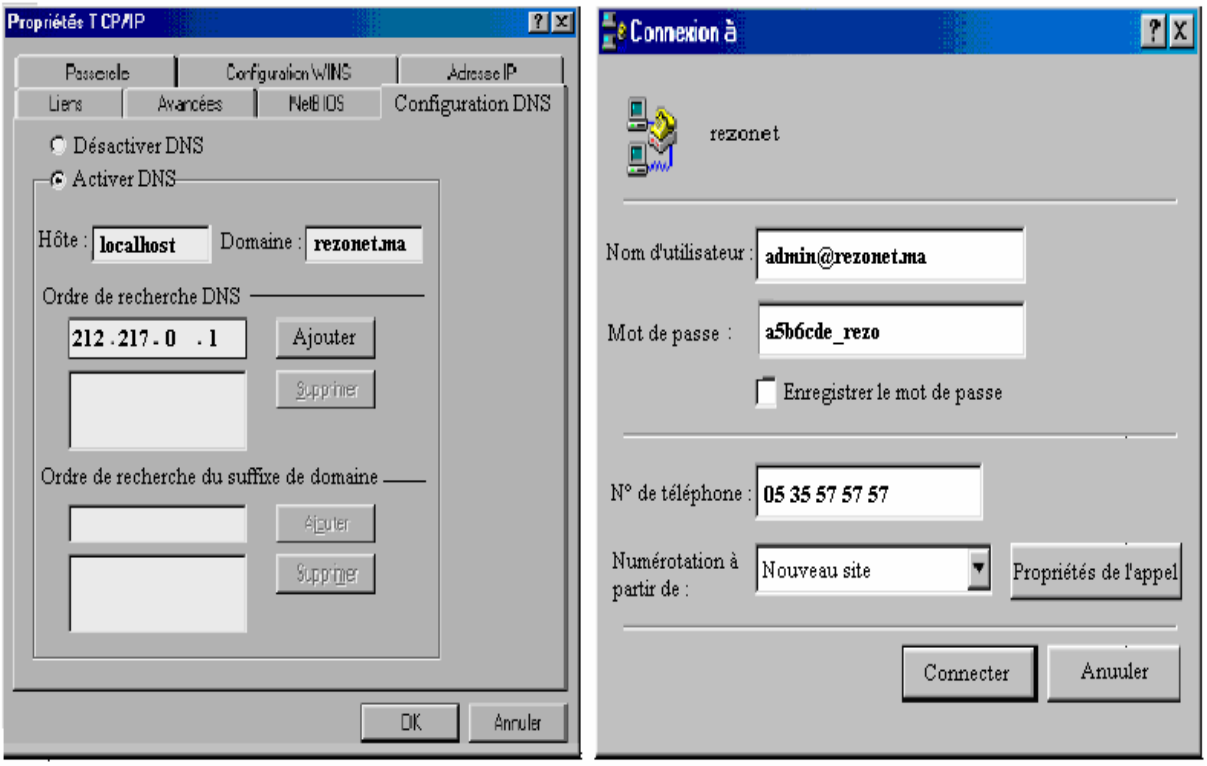
Question 7. Compléter (Annexe 1) l'interaction entre un client et un serveur SMTP et POP



Question 8. Citer 4 possibilités d'accès à un fournisseur d'accès Internet.

Les différents modes de connexion disponibles pour accéder à un fournisseur d'accès sont :
- RTC
- Numéris
- L'ADSL
- Le câble
- Le satellite…

Question 9. Compléter l'annexe 2 (Point d'accès :05 35 57 57 57, Serveur DNS :212.217.0.1, Adresse IP obtenue par mon fournisseur, Domaine :rezonet.ma, Hôte :localhost, Nom utilisateur de connexion admin@rezonet.ma, mot de passe : a5b6cde_rezo).



Question 10. Pour un accès par RTC, donner le type de protocole utilisé.

PPP (Point to Point Protocol). Protocole permettant la connexion entre ordinateurs et routeurs par lignes synchrones et asynchrones. Successeur du SLIP,il possède une correction d'erreur et des possibilités d'affectation d'adresse en réseau.

EXONET N° 5

La société REZOnet possède un serveur Linux possédant un serveur ftp, qui est installé dans toutes les distributions, ainsi qu'un client ftp en ligne de commande.

Partie I :

1. Quelle est la signification du sigle ftp ?

2. Quelle est l'utilité de ce service réseau ?

Le serveur ftp est déclaré dans le fichier /etc/inetd.conf mais pas toujours activé.

3. Quelle modification faut-il réaliser dans le fichier inetd.conf se trouvant en annexe pour activer le serveur ftp ?

Les fichiers de configuration :

/etc/ftpaccess : ce fichier définit la plupart des contrôles d'accès pour votre serveur ftp. Vous pouvez créer des groupes logiques pour contrôler l'accès depuis d'autres sites, limiter le nombre de connexions simultanées…….

/etc/ftphosts : ce fichier est utilisé pour autoriser ou non l'accès du serveur à un certain nombre de machines……

/etc/ftpusers : ce fichier contient la liste des utilisateurs qui ne peuvent accéder à votre machine via ftp.

4. Vous n'êtes pas déclaré sur le serveur (fichiers en annexes), quel nom de login utiliser? Pourquoi ?

5. Quel fichier est à modifier pour autoriser root à se connecter ? Quelle est la modification à réaliser dans le fichier ?

Les fichiers .rpm sous Linux sont des fichiers binaires qui permettent d'installer des programmes.

6. Donner dans l'ordre la syntaxe des différentes commandes à utiliser pour rapatrier le fichier « netscape-communicator-4.7.i386.rpm » depuis un serveur sur une station linux?

7. Donner la syntaxe de l'URL nécessaire pour se connecter au serveur ftp dont le nom DNS est « ftp.microsoft.com » avec un navigateur web ?

Partie II :

La direction de REZOnet pense mettre en place un serveur sur la toile (Web) permettant, dans un premier temps, la mise en ligne d'un système d'information interne (intranet) puis, dans un deuxième temps, de l'ouvrir à la clientèle via l'internet (extranet).

8. Expliquer ce qu'est un intranet.

9. Citer les spécificités du développement d'un intranet par rapport à d'autres types d'architectures client-serveur.

10. Citer les problèmes que peut poser l'accès de la clientèle via l'internet. Proposer des solutions pour les éviter.

Annexe 1

Extrait du fichier /etc/inetd.conf

```
# inetd.conf This file describes the services that will be available
# through the INETD TCP/IP super server
#discard stream tcp nowait root internal
#discard dgram udp wait root internal
#chargen dgram udp wait root internal
#time stream tcp nowait root internal
#time dgram udp wait root internal
# These are standard services.
#ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
# Shell, login, exec, comsat and talk are BSD protocols.
shell stream tcp nowait root /usr/sbin/tcpd in.rshd
login stream tcp nowait root /usr/sbin/tcpd in.rlogind
#exec stream tcp nowait root /usr/sbin/tcpd in.rexecd
#comsat dgram udp wait root /usr/sbin/tcpd in.comsat
talk dgram udp wait root /usr/sbin/tcpd in.talkd
ntalk dgram udp wait root /usr/sbin/tcpd in.ntalkd
# End of inetd.conf
linuxconf stream tcp wait root /bin/linuxconf linuxconf --http
```

Extrait du fichier /etc/ftpusers

```
bin, daemon, adm, lp, sync, root, shutdown, halt, mail, news, ucp, operator, games, nobody
```

Extrait du fichier /etc/ftpacces

```
class all real,guest,anonymous *
email root@localhost
loginfails 5
readme README* login
readme README* cwd=*
message /welcome.msg login
message .message cwd=*
compress yes guest,real,anonymous
tar yes guest,real,anonymous
log transfers guest,real,anonymous inbound,outbound
shutdown /etc/shutmsg
passwd-check rfc822 warn
guestgroup profs Damotte
chmod yes guest,real,anonymous
delete yes guest,real,anonymous
overwrite yes guest,real,anonymous
```

Annexe 2

Les principales commandes ftp

help : Affiche l'ensemble des commandes supportées par le serveur FTP

status : Permet de connaître certains paramètres de la machine cliente

binary : Cette commande vous fait basculer du mode ASCII (envoi de documents textes) au mode binary (envoi de fichiers en mode binaire, c'est-à-dire pour les fichiers non texte, commandes images ou des programmes)

ascii : Bascule du mode binary au mode ascii. Ce mode est le mode par défaut

type : Permet d'afficher le mode courant de transfert (binary ou ascii)

user : Vous permet de réouvrir une session sur le site FTP en cours avec un nom d'utilisateur différent. Un nouveau mot de passe vous sera alors demandé

ls : Permet de lister les fichiers présents dans le répertoire courant. La commande "ls -l" donne des informations supplémentaires sur les fichiers

pwd : Affiche le nom complet du répertoire courant

Cd : Cette commande signifie change directory, elle permet de changer le répertoire courant. La commande "cd .." permet d'accéder au répertoire de niveau supérieur

mkdir : La commande mkdir (sous UNIX, ou md sous système Microsoft) permet de créer un répertoire dans le répertoire courant. L'utilisation de cette commande est réservée aux utilisateurs ayant un accès le permettant

rmdir : La commande rmdir (sous UNIX, ou rd sous système Microsoft) permet de supprimer un répertoire dans le répertoire courant. L'utilisation de cette commande est réservée : aux utilisateurs ayant un accès le permettant

get : Cette commande permet de récupérer un fichier présent sur le serveur Si la commande est suivie d'un nom de fichier, le fichier distant est transféré sur la machine locale dans le répertoire local en cours

Si la commande est suivie de deux noms de fichiers, le fichier distant (le premier nom) est transféré sur la machine locale : dans le répertoire local en cours, avec le nom de fichier précisé (le deuxième nom)

Si jamais le nom de fichier contient des espaces, il faut veiller à le saisir entre guillemets

put : Cette commande permet d'envoyer un fichier local sur le serveur Si la commande est suivie d'un nom de fichier, le fichier local est transféré sur le serveur dans le répertoire distant en cours

Si la commande est suivie de deux noms de fichiers, le fichier local (le premier nom) est transféré sur le serveur dans le répertoire distant en cours, avec le nom de fichier précisé (le deuxième nom)

Si jamais le nom de fichier contient des espaces, il faut veiller à le saisir entre guillemets

open : Ferme la session en cours et ouvre une nouvelle session sur un autre serveur FTP

close : Ferme la session en cours, en laissant le logiciel FTP client actif

bye ou quit : Déconnecte le logiciel client du serveur FTP et le met en état inactif

Corrigé Exonet N° 3

Question 1. Quelle est la signification du sigle ftp ?

File Transfert Protocol

Question 2. Quelle est l'utilité de ce service réseau ?

Transfert de fichiers client serveur entre systèmes d'exploitation différents.

Question 3. Quelle modification faut-il réaliser dans le fichier inetd.conf se trouvant en annexe pour activer le serveur ftp ?

Supprimer le symbole # devant la ligne ftp ……..

Question 4. Vous n'êtes pas déclaré sur le serveur (fichiers en annexes), quel nom de login utiliser? Pourquoi ?

anonymous (fichier /etc/access)

Question 5. Vous n'êtes pas déclaré sur le serveur (fichiers en annexes), quel nom de login utiliser? Pourquoi ?
Modifier le fichier /etc/ftpusers en supprimant le nom root

Question 6. Donner dans l'ordre la syntaxe des différentes commandes à utiliser pour rapatrier le fichier « netscapecommunicator4.7.i386.rpm » depuis un serveur sur une station linux?

ftp nom serveur
nom de login et mot de passe
binary
get nom_de_fichier.rpm
quit

Question 7. Donner la syntaxe de l'URL nécessaire pour se connecter au serveur ftp dont le nom DNS est « ftp.microsoft.com » avec un navigateur web ?

ftp://ftp.microsot.com

Question 8. Expliquer ce qu'est un intranet.

Intranet : utilisation des standards de l'Internet (HTML, http, SMTP, …) pour développer des applications internes à l'entreprise, que le réseau soit local ou étendu.

Question 9. Citer les spécificités du développement d'un intranet par rapport à d'autres types d'architectures client-serveur.

Les spécifités du développement d'un intranet sont :

- davantage de middleware standard, accès universel, pas de déploiement spécifique sur chaque type de plate-forme
- l'application est développée sur le serveur, une mise à jour de l'application est immédiate pour tous les clients quelle que soit leur plate-forme

Question 10. Citer les problèmes que peut poser l'accès de la clientèle via l'internet. Proposer des solutions pour les éviter.

Le problème majeure concerne la sécurité du réseau local vis-à-vis des accès externes : risque de visibilité de resources sensibles, risque de prise de contrôle à distance et d'actions malveillantes.
Les solutions possibles :

- utilisation d'adresses non routables sur le réseau local.
- mise en place d'un firewall destiné à filtrer les paquets entrants sur des critères prédéfinis (adresses accessibles, types de services autorisés,etc.).
- authentification des utilisateurs distants par un compte anonyme dont les droits et permissions sont très limités.
- Contrôle par mot de passe dans l'application en prévoyant un code d'accès sur le bon de réception

EXONET N° 4

1. Citer 3 protocoles permettant d'envoyer des e-mails et/ou d'en recevoir ?
2. Dans la messagerie électronique, on utilise des adresses du type **r.errachidi@menara.ma**.
Que représente la deuxième partie de cette adresse ?
Un analyseur de protocole situé dans "**le réseau S**" a permis de faire un relevé entre une station A du réseau de "**T**" et un serveur de l'entreprise **REZOnet** situé dans le "**réseau S**" au cours d'un échange initié par l'utilisateur.
Voici une des trames ETHERNET II récupérées :

00	04	75	CE	24	CF	00	0D	29	D4	69	7F	08	00	45	00
00	31	EE	6D	40	00	80	06	6C	02	0A	53	04	21	C3	34
D1	0E	0D	68	00	8F	DE	08	55	7A	79	36	D4	8F	50	18
F8	4D	A0	7A	00	00	34	37	20	6E	6F	6F	70	0D	0A	

A l'aide des annexes 1, 2 et 3 :
3.1. Préciser les valeurs des adresses MAC source et destinataire.
3.2. Faire un schéma représentant la station A et le serveur en indiquant les sockets utilisés par le client et le serveur.
Remarque : un socket est la combinaison de trois éléments : l'adresse IP de la machine, le protocole au niveau transport et le numéro du port.
3.3. Indiquer la signification des numéros de port source et destination.
3.4. Quelles sont les principales caractéristiques du protocole de niveau TRANSPORT utilisés ?
4. Conclusion : Quel est l'objectif de la demande initiée par l'utilisateur ?

Annexe 1

Assignation de certains ports associés aux processus serveurs en fonction des protocoles de transport TCP et UDP.

Processus	Port	Protocole Description
ftp-data	20	File Transfer [Default Data]
ftp	21	File Transfer [Control]
ssh	22	SSH Remote Login Protocol
telnet	23	Telnet
smtp	25	Simple Mail Transfer
domain	53	Domain Name Server
bootpc	68	Bootstrap Protocol Client
tftp	69	Trivial File Transfer
http	80	World Wide Web HTTP
pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
sftp	115	Simple File Transfer Protocol
nntp	119	Network News Transfer Protocol
statsrv	133	Statistics Service
netbios-ns	137	NETBIOS Name Service
netbios-dgm	138	NETBIOS Datagram Service
netbios-ssn	139	NETBIOS Session Service
Imap2	143	Interim Mail Access Proto v2
snmp	161	Simple Net Mgmt Proto
https	443	MComhttps
Microsoft-DS	445	NETBIOS Datagram Service(Win2000)
P2P	6881 to 6889	client P2P

Annexe 2

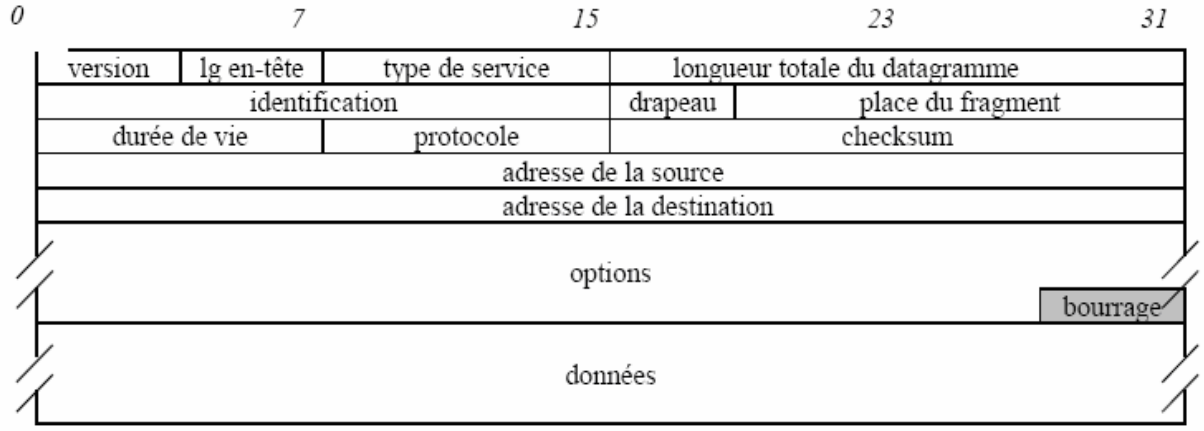
FORMAT D'UNE TRAME ETHERNET_II

Adresse MAC Destination 6 octets	Adresse MAC Source 6 octets	Protocole Niveau 3 2 octets	Données niveau 3 + bourrage éventuellement 46 octets minimum, 1 500 octets maximum	CRC 4 octets

Exemples de valeurs du champ protocole d'une trame ETHERNET_II

Champ protocole (hexadécimal)	Protocole
0x0800	DOD IP (Internet)
0x0806	ARP
0x80D5	IBM SNA Service on Ether
0x8035	RARP
0x86DD	IPv6

FORMAT D'UN DATAGRAMME IP



Les champs spécifiques d'un paquet IP sont:
- **version** est codé sur 4 bits. Actuellement ce champ a une valeur égale à 4 (IPv4).
- **longueur de l'en-tête** ou IHL (Internet Header Length) sur 4 bits spécifie le nombre de mots de 32 bits qui composent l'en-tête. Si le champ option est vide, l'IHL vaut 5.
- **type de service** ou ToS (Type of Service) est codé sur 8 bits. Spécifie à la passerelle intermédiaire le type d'acheminement attendu.
- **identification** codé sur 16 bits permet de sécuriser le réassemblage des paquets après fragmentation.
- **drapeau** codé sur 3 bits a le 1er bit toujours nul, le 2ème bit à 0 indique que le paquet peut être fragmenté et à 1 s'il ne peut pas l'être, le 3ème bit à 0 indique s'il s'agit du dernier fragment et à 1 que d'autres fragments suivent.
- **place du fragment** codé sur 13 bits indique la position du 1er octet dans le datagramme total non fragmenté. Il s'agit d'un nombre multiple de 8 octets.
- **durée de vie** détermine en seconde, la durée de vie d'un datagramme. Cette valeur est décrémentée toutes les secondes ou à chaque passage à travers une passerelle.
- **protocole** codé sur 8 bits indique le protocole de la couche supérieure (liste donnée par le rfc 1700, ex: "1"=ICMP, "2"=IGMP, "6"=TCP, "17"=UDP).
- **checksum** est la somme de contrôle portant sur l'en-tête.
- **adresses** de la source et de la destination sont codées sur 32 bits.
- **option** est de longueur variable et peut être nul.

Annexe 3

FORMAT DES MESSAGES TCP

Bit 0 – 7	8 – 15	16 – 23	24 – 31
Port source		Port destination	
Numéro de séquence			
Acquittement			
Lg entête	6 bits réservés	6 drapeaux	Fenêtre
Checksum		Pointeur message urgent	
Options (bourrage)			
Data			

Port source et Port destination : Ils identifient les programmes d'application.
N° de séquence : Il indique le n° du 1er octet transmis dans le segment.
Acquittement : indique le n° du prochain octet attendu par l'émetteur de ce message
Lg entête : sur 4 bits, elle indique la taille en mots de 32 bits de l'entête
Drapeaux : bit URG : Validation de la valeur du champ "pointeur message urgent"
bit ACK : la valeur du champ "acquittement" peut être prise en compte
bit PSH : le données doivent être immédiatement transmises à la couche supérieure
bit RST : fermeture de la connexion à cause d'une erreur irrécupérable
bit SYN : ouverture de la connexion
bit FIN : fin de connexion (plus de data à émettre)
Fenêtre : Nombre d'octets que le récepteur peut accepter sans ACR.
Pointeur de message urgent : Si le drapeau URG est positionné, les données passent avant le flot de données normales. Ce champ indique alors la position de l'octet de la fin des données urgentes.
Le champ option peut-être utilisé si deux machines doivent se mettre d'accord sur une taille maximale de segment appelé MSS (Maximum Segment Size).

Corrigé Exonet N° 4

Question 1. Citer 3 protocoles permettant d'envoyer des e-mails et/ou d'en recevoir ?

SMTP, POP2, POP3 et IMAP.

Question 2. Dans la messagerie électronique, on utilise des adresses du type r.errachidi@menara.ma.
Que représente la deuxième partie de cette adresse ?

La deuxième partie de r.errachidi@menara.ma représente le nom du domaine où se trouve le serveur de messagerie c-à-d le nom du bureau de poste contenant la boîte aux lettres r.errachidi.

Question 3.1. Préciser les valeurs des adresses MAC source et destinataire.

L'équipement source correspond à l'adresse MAC 00:0d:29:d4:69:7f
L'équipement cible qui correspond à l'adresse MAC 00:04:75:ce:24:cf

Question 3.2. Faire un schéma représentant la station A et le serveur en indiquant les sockets utilisés par le client et le serveur.

Question 3.3. Indiquer la signification des numéros de port source et destination.

Le port source 3432 indique le port d'émission (client dynamique) ouvert par la station
Le port Destination 143 indique que le port de réception correspond au service de messagerie IMAP.

Question 3.4. Quelles sont les principales caractéristiques du protocole de niveau TRANSPORT utilisés ?

Les qualités du protocole TCP:
- Fiabilité : retransmission des trames non acquittées
- Gestion des flux: négociation de la taille de la fenêtre de transmission.
- Offre une transmission en mode connecté.
- Remise en ordre des segments reçus.

Question 4. Conclusion : Quel est l'objectif de la demande initiée par l'utilisateur ?

L'objectif est de récupérer le courrier présent sur le serveur de messagerie.

EXONET N° 5

Un établissement scolaire utilise un serveur mandataire (Proxy) dans le DNS, pour contrôler les accès à Internet.
Ce Proxy permet entre autre d'autoriser ou pas l'accès à Internet en fonction de l'adresse IP du réseau auquel appartient la machine.
L'administrateur du réseau a organisé son plan d'adressage en fonction des salles.
Chaque salle dispose d'une plage d'adresses spécifique qui va permettre au niveau du Proxy d'interdire ou d'autoriser l'accès à Internet à tous les postes de la salle.
L'annexe 1 donne le plan d'adressage utilisé.
L'annexe 2 donne les règles d'accès à Internet pour la journée du 15 Octobre 2008.

1. Déterminer quelles sont les salles qui n'ont pas accès à Internet le 15 Octobre.
2. Expliquer pourquoi le Proxy peut appliquer des masques différents alors que les postes sont tous configurés avec le même masque et la même adresse réseau.
3. Donner la ou les règles à appliquer pour interdire l'accès à la salle 204 et 208.
4. Donner la règle à appliquer pour interdire l'accès à la salle 201 et 202.
5. Expliquer les autres fonctions d'un Proxy.

Annexes

Annexe 1 : Plan d'adressage

Adresse IP du réseau de l'établissement :
10.100.40.0
Masque du réseau :
255.255.255.0
Plage d'adresses par salle :

Salle 201 : 10.100.40.1 à 10.100.40.15	**Salle 206 :** 10.100.40.129 à 10.100.40.142
Salle 202 : 10.100.40.17 à 10.100.40.31	**Salle 207 :** 10.100.40.145 à 10.100.40.158
Salle 203 : 10.100.40.33 à 10.100.40.62	**Salle 208 :** 10.100.40.161 à 10.100.40.174
Salle 204 : 10.100.40.65 à 10.100.40.70	**Salle 209 :** 10.100.40.177 à 10.100.40.190
Salle 205 : 10.100.40.96 à 10.100.126	**Salle 210** : 10.100.40.73 à 10.100.40.78

Annexe 2 : Règles du 15 octobre 2008

Accès autorisé à tous sauf aux réseaux ci-dessous :
10.100.40.32 masque 255.255.255.224
10.100.40.128 masque 255.255.255.192

Corrigé Exonet N° 5

Question 1. Déterminer quelles sont les salles qui n'ont pas accès à Internet le 15 Octobre.

Le masque 255.255.255.224 détermine une plage de 32 adresses (256 - 224 ou 2^5). L'adresse de réseau 10.100.40.32 donne la première adresse de la plage. Donc la première règle interdit l'accès à la salle 203.
Le masque 255.255.255.192 détermine une plage de 64 adresses (256 - 192 ou 2^6). L'adresse de réseau 10.100.40.128 donne la première adresse de la plage
La deuxième règle interdit donc l'accès aux salles 206, 207, 208, 209. On aurait d'ailleurs pu utiliser le masque 255.255.255.128 qui aurait donné le même résultat.

Question 2. Expliquer pourquoi le Proxy peut appliquer des masques différents alors que les postes sont tous configurés avec le même masque et la même adresse réseau.

La configuration des postes n'a pas d'importance à ce niveau. Le Proxy reçoit un paquet en provenance d'un poste, il récupère dans l'entête IP l'adresse source du paquet et lui applique le masque de chaque règle en comparant le résultat obtenu à l'adresse réseau de la règle. En cas d'égalité le paquet est rejeté. Il ne faut pas oublier que le masque de sous réseau n'est pas dans l'entête IP.
L'administrateur réseau a bien sur choisi un plan d'adressage qui lui permettait en fonction du nombre de postes par salle d'appliquer ce type de restriction.

Question 3. Donner la ou les règles à appliquer pour interdire l'accès à la salle 204 et 208.

Les plages d'adresses des salles 204 et 208 ne sont pas contiguës, il faut donc une règle pour chaque salle. La salle 204 dispose des adresses 10.100.40.65 à 70, et la première adresse à ne pas interdire correspond à la première adresse de la salle 210. Il faut donc bloquer au plus 8 adresses (de 64 à 72), soit un masque de 255.255.255.248 (256-8) pour une première adresse de 10.100.40.64
Pour la salle 208, la plage à interdire est de 16 adresses (entre 10.100.40.160 et 175), pour un masque de 255.255.255.240 (256-16) et une adresse de 10.100.40.160
Il faut donc appliquer les règles suivantes :
10.100.40.64 masque 255.255.255.248
10.100.40.160 masque 255.255.255.240

Question 4. Donner la règle à appliquer pour interdire l'accès à la salle 201 et 202.

En appliquant les principes précédents, on détermine la règle suivante :
Interdire l'accès au réseau
10.100.40.0 masque 255.255.255.224

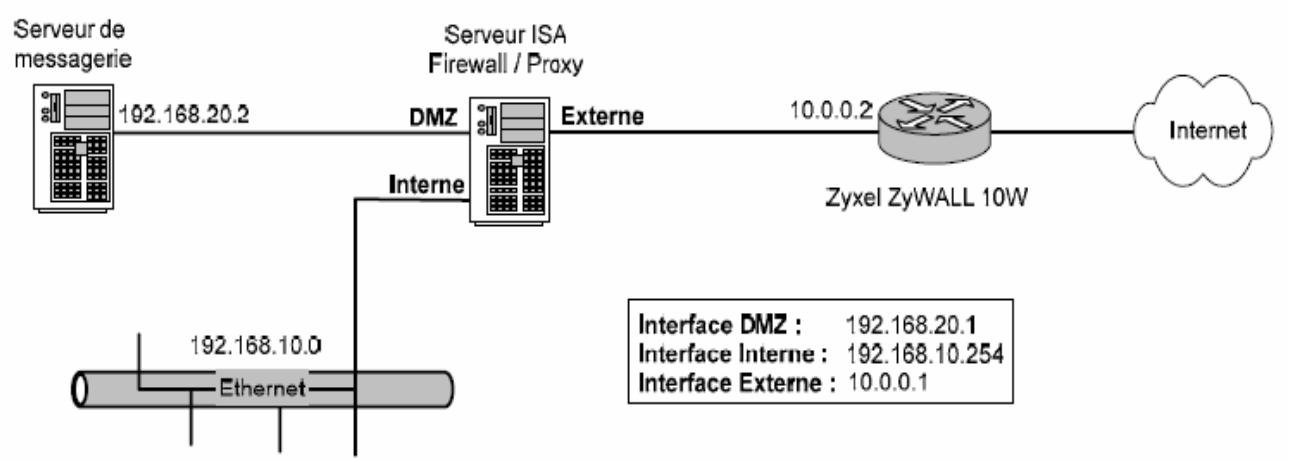
Question 5. Expliquer les autres fonctions d'un Proxy.

Un Proxy est utilisé également pour mettre en cache les pages Web consultées.
Un Proxy a aussi une fonction de translation d'adresses. C'est l'adresse générée par le Proxy qui part sur Internet (selon la configuration bien sûr) et non l'adresse des postes qui font appel à lui. On parle alors de réseau privé et de réseau public et du protocole NAT (Network Address Translator).
Un Proxy peut filtrer les sites Web consultés en utilisant pour cela un fichier des sites interdits. Il peut aussi interdire certains protocoles (FTP par exemple) ou le téléchargement de certains fichiers en fonction de leur extension (MP3 par exemple). Il joue alors le rôle de pare-feu.
Enfin un Proxy peut disposer d'un Anti-virus général qui s'applique à tous les fichiers en provenance de l'Internet avant de les introduire dans le réseau local.

EXONET N° 6

Le serveur ISA (Internet Security and Acceleration Server 2000) remplit les fonctions de firewall (pare-feu) et de serveur proxy.

Configuration des interfaces du serveur ISA :



Lors de la configuration du serveur ISA, les règles de sécurité suivantes ont été mises en oeuvre pour l'accès au serveur de messagerie :

	Action	Protocols	From	To	Condition
1	Allow	FTP HTTP HTTPS	Internal VPN Clients	External DMZ	All Users
2	Allow	All Protocols	VPN Clients	Internal	All Users
3	Allow	DNS	Internal VPN Clients	DMZ	All Users
4	Deny	All Protocols	All Networks	All Networks	All Users

1. Indiquez ce qu'est le protocole HTTPS et précisez son utilité (donnez un exemple d'utilisation).

2. Indiquez ce qu'est un "Client VPN". Vous donnerez la signification de l'abréviation VPN.

Les règles de sécurité sont traitées de manière séquentielle (ordre croissant). Pour chaque trame reçue, le firewall parcourt la liste des règles jusqu'à ce qu'il trouve une règle qui s'applique. L'ordre dans lequel sont spécifiées les règles est très important.

3. Expliquez l'action de la règle N°1 sur les trames en provenance du réseau 192.168.10.0

4. Expliquez l'action de la règle N°3, Précisez la fonction du protocole DNS et donnez la signification de l'abréviation DNS.

Quel est le serveur qui remplit la fonction de serveur DNS ?

5. La règle N°4 est indispensable au bon fonctionnement du firewall, pourquoi ?

6. Les règles de sécurité mises en oeuvre permettent-elles aux utilisateurs d'accéder au serveur de messagerie ? Pourquoi ?

Quelle règle faut-il ajouter, et à quelle place, pour permettre à tous les utilisateurs internes et externes d'accéder à la messagerie ?

Corrigé Exonet N° 6

Question1. Indiquez ce qu'est le protocole HTTPS et précisez son utilité (donnez un exemple d'utilisation).

Hyper **T**ext **T**ransfer **P**rotocol **S**écurisé, accès sécurisé à Internet : paiement en ligne, consultation de compte bancaire …

Question2. Indiquez ce qu'est un "Client VPN". Vous donnerez la signification de l'abréviation VPN.

Client distant qui se connecte au réseau via une liaison sécurisée VPN (Virtual Private Network ou réseau privé virtuel) en utilisant Internet comme support.

Question3. Expliquez l'action de la règle N°1 sur les trames en provenance du réseau 192.168.10.0

La règle N°1 **autorise** (Allow) le passage des messages **FTP, HTTP et HTTPS** de l'interface interne (réseau 192.168.10.0) et des clients VPN vers l'interface externe (accès à Internet) et vers la DMZ (accès au serveur de messagerie) pour tous les utilisateurs (All Users).

Question4. Expliquez l'action de la règle N°3, Précisez la fonction du protocole DNS et donnez la signification de l'abréviation DNS.
Quel est le serveur qui remplit la fonction de serveur DNS ?

La règle N°3 **autorise** (Allow) le passage des messages **DNS** de l'interface interne (réseau 192.168.10.0) et des clients VPN vers la DMZ (accès au serveur de messagerie) pour tous les utilisateurs (All Users).
DNS : Domain Name System (ou Service), indispensable pour accéder à Internet car il effectue la liaison entre un nom de machine et son adresse IP. Le serveur de messagerie fait également office de serveur DNS.

Question5. La règle N°4 est indispensable au bon fonctionnement du firewall, pourquoi ?

Pour une sécurité maximum il faut interdire tout ce qui n'a pas été autorisé dans les règles précédentes, c'est le rôle de **la règle N°4 qui interdit** (Deny) **tous les protocoles** en provenance de tous les réseaux et vers tous les réseaux pour tout le monde.

Question6. Les règles de sécurité mises en oeuvre permettent elles aux utilisateurs d'accéder au serveur de messagerie ? Pourquoi ?
Quelle règle faut il ajouter, et à quelle place, pour permettre à tous les utilisateurs internes et externes d'accéder à la messagerie ?

Non, car les protocoles de messagerie (**SMTP** et **POP**) ne sont pas autorisés.
Il faut donc **ajouter une règle autorisant les protocoles SMTP et POP entre tous les réseaux et la DMZ** pour tous le monde et la placer avant la règle N°4 :

	Action	Protocols	From	To	Condition
3	…	…	…	…	…
4	**Allow**	**SMTP POP**	**All Networks***	**DMZ**	**All Users**
5	Deny	All Protocols	All Networks	All Networks	All Users

*« **All Networks »** peut être remplacé par « **External** + **Internal** »

EXONET N° 7

L'entreprise CENTAURE, dirigée par M.ARABI, emploie 27 salariés. Elle est constituée de deux services indépendants : le service multimédia assure l'installation et le développement des solutions clientes couvrant à la fois les aspects réseau et multimédia ; le service administratif, quant à lui, assure la gestion interne de l'entreprise.
Le schéma du réseau de la société est décrit en **annexe 1**.

Les postes du service multimédia sont amenés à faire beaucoup d'accès Internet très consommateurs en bande passante.
Pour améliorer les temps de réponse, la société a mis en service un serveur proxy.
1. Expliquer dans quelles conditions d'usage ce type de serveur répond à l'objectif visé.

La société, soucieuse d'améliorer sa notoriété, décide de mettre en ligne un serveur HTTP et FTP accessible au public. Ce serveur, installé dans les locaux de CENTAURE, sera placé dans une zone démilitarisée (DMZ) comme l'indique l'**annexe 1**.
L'équipement pare-feu (firewall) contrôle les accès qui arrivent sur ses différentes interfaces. Il est programmé de telle façon que seul le trafic réseau respectant les règles indiquées dans l'**annexe 2** est accepté. Ces règles peuvent faire référence à des adresses IP d'ordinateurs, des adresses de réseau et des protocoles réseau.
Un serveur mandataire (proxy) est également installé entre le routeur R1 et le pare-feu : il est le point de passage obligatoire de tous les accès du réseau local vers l'Internet.
2. Expliquer en quoi la mise en œuvre d'une zone démilitarisée permet d'améliorer la sécurité du réseau local.

Un anti-virus a révélé la présence d'un programme « cheval de Troie » sur le serveur situé dans la DMZ. L'étude révèle que le "troyen" n'a pas été placé par les protocoles HTTP ou FTP.
3.a. Expliquer ce qu'est « cheval de Troie » et comment les antivirus détectent sa présence.
3.b. Donner deux exemples de faille intrinsèque relative au protocole FTP.
3.c. En analysant les règles de l'annexe 2, indiquer quelle règle a pu permettre l'installation de ce programme.
3.d. Proposer, pour réduire les risques liés à ce type de problème, une ou plusieurs règles en remplacement de la règle concernée.

Ce « cheval de Troie » est destiné à perturber le fonctionnement du réseau local, en s'exécutant automatiquement périodiquement.
4. En analysant les règles de l'annexe 2, indiquer si les postes du réseau local sont susceptibles d'être atteints par le « cheval de Troie ».

L'administrateur réseau du service Multimédia prend en charge l'administration du serveur HTTP et FTP (192.168.10.10). Il doit donc avoir la possibilité de lancer une commande TELNET vers ce serveur, depuis sa machine dont l'adresse IP est 192.168.1.75.
Le serveur PROXY a été paramétré afin de pouvoir traiter le protocole TELNET.
5. a. Citer les interfaces du pare-feu concernées par une commande TELNET.
5. b. Pour chacune de ces interfaces, rédiger les règles nécessaires pour permettre l'emploi de cette commande, en donnant leur numéro d'ordre.

Pour permettre une tolérance aux pannes le **serveur 1** comporte un dispositif matériel permettant de mettre en œuvre un système RAID (redundant arrays of inexpensive disk) au niveau 1.

6. Expliquer ce qu'est un tel système.

Les utilisateurs du service Multimédia se plaignent de recevoir de nombreux pourriels (spams).

7. a. Définir la notion de pourriel (spam) et préciser en quoi ils constituent une gêne pour l'entreprise.

7. b. Proposer une solution qui permet de se protéger contre les spams.

CENATURE envisage élargir ses activités pour cela elle sous-traite une partie de son activité en confiant à des entreprises extérieures l'installation des réseaux chez les clients.

La mise en œuvre d'une nouvelle application est envisagée pour permettre aux sous-traitants de consulter leur planning et d'enregistrer leurs indisponibilités. Cette application sera hébergée sur le serveur web.

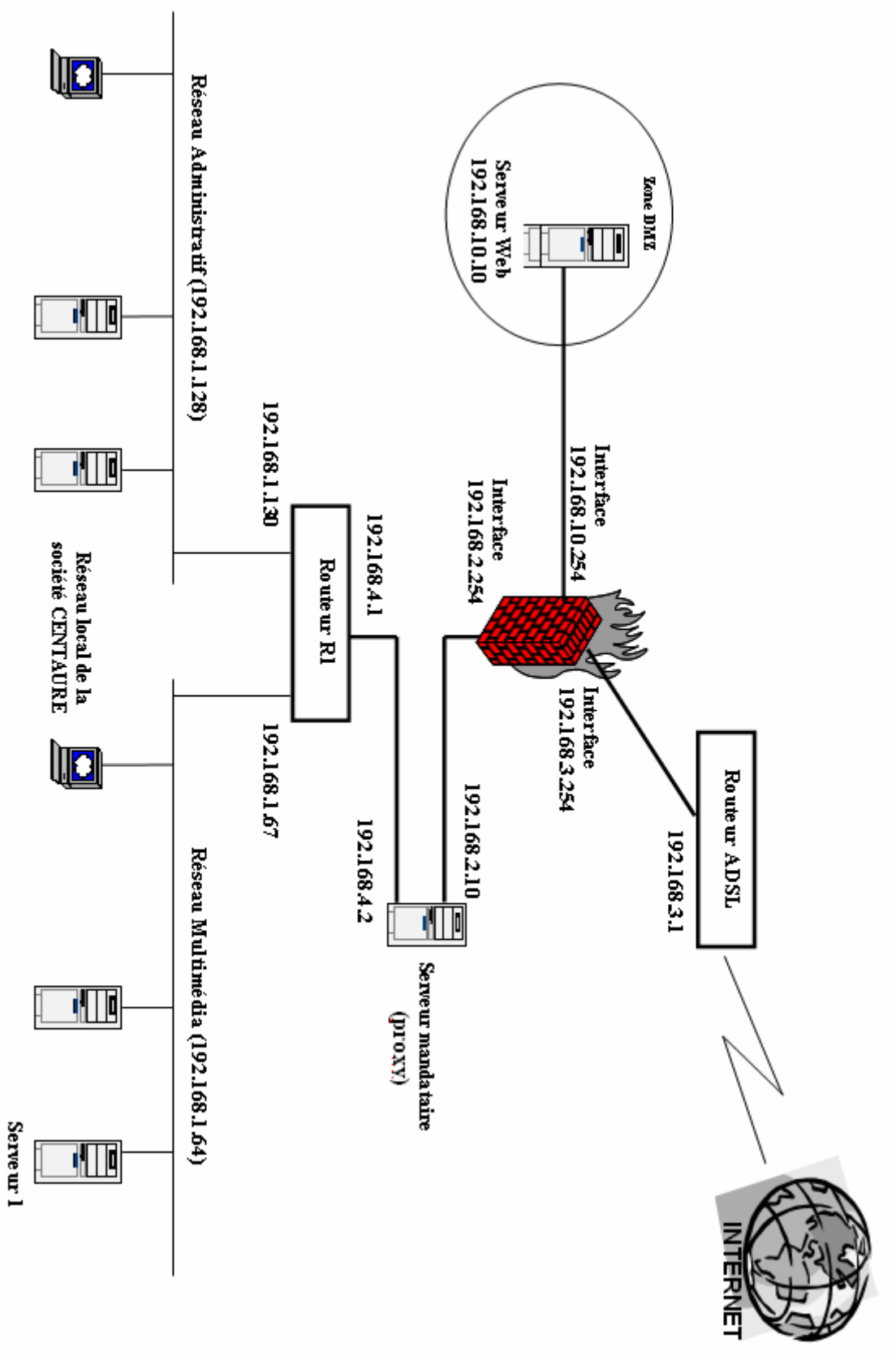
Le souci de l'entreprise est d'assurer la sécurité des échanges avec les sous-traitants et notamment la confidentialité et l'authentification. Le dispositif conseillé à CENATURE base sa sécurité sur une méthode de chiffrement asymétrique des informations échangées. Monsieur ARABI souhaite en maîtriser le principe.

8. Expliquer, éventuellement à l'aide d'un schéma, le mode de fonctionnement de cette méthode en précisant le type de clé utilisé par chacun des intervenants (émetteur et récepteur du message) pour assurer confidentialité et authentification dans l'échange.

La mise en œuvre des techniques de chiffrement implique souvent un tiers de confiance, prestataire de service.

9. Expliquer comment ce tiers de confiance intervient dans la procédure d'échange d'informations.

Annexe 1 : schéma du réseau de la société CENTAURE



Annexe 2 : Règles d'accès programmées sur le pare-feu

Interface 192.168.3.254

Ordre	Source	Destination	Service	Accès
1	Any	192.168.2.10	HTTP	Accepté
2	Any	192.168.2.10	FTP	Accepté
3	Any	192.168.2.10	DNS	Accepté
4	Any	192.168.2.10	SMTP	Accepté
5	Any	192.168.2.10	POP3	Accepté
6	Any	192.168.10.10	Any	Accepté
7	Any	Any	Any	Refusé

Interface 192.168.2.254

Ordre	Source	Destination	Service	Accès
1	192.168.2.10	Any	Any	Accepté
2	Any	Any	Any	Refusé

Interface 192.168.10.254

Ordre	Source	Destination	Service	Accès
1	192.168.10.10	Any	HTTP	Accepté
2	192.168.10.10	Any	FTP	Accepté
3	Any	192.168.1.128	Any	Refusé
4	Any	192.168.1.64	Any	Refusé
5	Any	Any	Any	Refusé

Remarques :

Any : quelle que soit la valeur.

Une règle traduit un droit ou un refus d'accès ; les règles sont évaluées dans l'ordre.
Si une action est appliquée, on ne passe pas à la règle suivante.

Par exemple, la règle 1 de l'interface 192.168.10.254 indique que tout paquet entrant sur cette interface, provenant de 192.168.10.10, destiné à n'importe quelle machine du réseau et encapsulant une requête du protocole HTTP, sera accepté.

Corrigé Exonet N° 7

Question 1. Expliquer dans quelles conditions d'usage ce type de serveur répond à l'objectif recherché.

Le serveur Proxy est ici utilisé pour mettre en cache les pages accédées sur Internet. Les temps de réponse seront améliorés si les personnes du service multimédia consultent souvent les mêmes sites. Si chacun d'eux consulte des sites différents et jamais les mêmes, la fonction cache du serveur Proxy n'améliorera pas les temps de réponse.

Question 2. Expliquer en quoi la mise en œuvre d'une zone démilitarisée permet d'améliorer la sécurité du réseau local.

Lorsqu'une entreprise désire rendre l'un de ses serveurs accessible depuis Internet, le risque est grand d'ouvrir une brèche de sécurité vers l'ensemble du réseau local.
Une zone démilitarisée permet de ne rendre accessible de l'extérieur qu'une partie des serveurs en isolant totalement le reste du réseau. Généralement, on trouve sur les DMZ les serveurs Web, voire les serveurs de messagerie et les serveurs DNS.

Question 3.a. Expliquer ce qu'est « cheval de Troie » et comment les antivirus détectent sa présence.
Question 3.b. Donner un exemple de faille intrinsèque relative au protocole FTP.
Question 3.c. En analysant les règles de l'annexe 2, indiquer quelle règle a pu permettre l'installation de ce programme.
Question 3.d. Proposer, pour réduire les risques liés à ce type de problème, une ou plusieurs règles en remplacement de la règle concernée.

a. Un cheval de Troie est un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté.
Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus. Certains antivirus utilisent un contrôleur d'intégrité pour vérifier si les fichiers ont été modifiés.
b. Le premier défaut du protocole FTP est de ne pas encrypter les mots de passe lors de leur transit sur le réseau. Le deuxième défaut est Le serveur FTP anonyme qui pose de plus gros problèmes
c. Il s'agit de la règle 6 de l'interface 192.168.3.254. Elle permet depuis Internet d'arriver sur le serveur Web en utilisant des services quelconques (Telnet…)
d. Il faut limiter aux seuls protocoles web (HTTP et FTP) l'accès au serveur 192.168.10.10, en rajoutant deux règles après avoir supprimé la règle 6.
Cependant l'accès FTP ne préserve pas de l'installation d'un programme et de son activation si le serveur web n'est pas correctement configuré.

Question 4. En analysant les règles de l'annexe 2, indiquer si les postes du réseau local sont susceptibles d'être atteints par le « cheval de Troie ».

Les règles 3 et 4 sur l'interface 192.168.10.254 empêchent l'accès au réseau local, sauf si le cheval de Troie utilise des services basés sur HTTP ou FTP.

Question 5.a. Citer les interfaces du pare-feu concernées par une commande TELNET.
Question 5.b. Pour chacune de ces interfaces, rédiger les règles nécessaires pour permettre l'emploi de cette commande, en donnant leur numéro d'ordre.

a.. Les interfaces concernées sont 192.168.2.254 et 192.168.10.254
b. La ligne numéro 1 de l'interface 192.168.2.254 autorise le passage vers le serveur internet.
Il faut autoriser le retour sur l'interface 192.168.10.254 avec la règle suivante :
Source 192.168.10.10 Destination : 192.168.2.10 Service : Telnet Accès : Accepté
qui doit être intercalée avant la ligne 3.

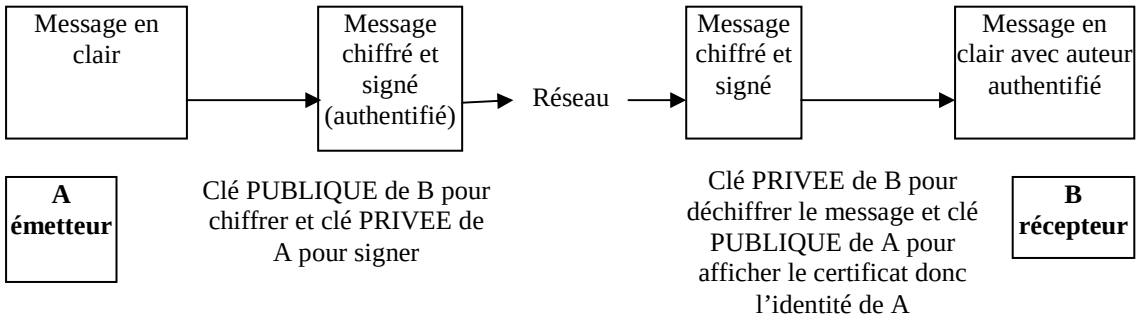
Question 6. Expliquer le système RAID1

Il existe plusieurs niveaux de systèmes RAID. Ils utilisent plusieurs disques durs pour garantir la sécurité des données ou augmenter les performances d'entrées-sorties du système de stockage.
Dans un système RAID 1, pour garantir l'intégrité des données, le contrôleur de disques effectue les mêmes opérations sur les deux disques. La panne de l'un des disques n'entraîne donc aucune perte de données. Coûteux en termes d'espace disque (50 % du volume dédié à la sécurité), un système Raid 1 n'améliore pas les taux de transfert.

Question 7.a. Définir la notion de pourriel (spam) et préciser en quoi ils constituent une gêne pour l'entreprise.
Question 7.b. Proposer une solution qui permet de se protéger contre les spams.

7.a. Pourriel (spam) : désigne les communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes.
Les pourriels polluent les boites aux lettres des usagers des messageries et nécessitent de leur part un temps de traitement parfois non négligeable (tri, suppression…). Par ailleurs ils sont parfois porteurs de virus, chevaux de Troie, espiogiciels… ce qui peut nuire à l'efficacité des systèmes (destruction de données, ralentissement des systèmes…).
7.b. Pour se protéger contre les spams on pourra par exemple installer un filtre anti spams au niveau du serveur de messagerie.

Question 8. Expliquer, éventuellement à l'aide d'un schéma, le mode de fonctionnement de cette méthode en précisant le type de clé utilisé par chacun des intervenants (émetteur et récepteur du message) pour assurer confidentialité et authentification dans l'échange.



Question 9. Expliquer comment ce tiers de confiance intervient dans la procédure d'échange d'informations.

Le tiers de confiance, ou autorité de certification et d'enregistrement, a pour rôle la délivrance d'un certificat permettant d'associer une clé publique à une entité. Ce tiers assure la validité du lien et garantit l'authentification du détenteur. Le certificat délivré possède une date de validité lui conférant ainsi une durée de vie.

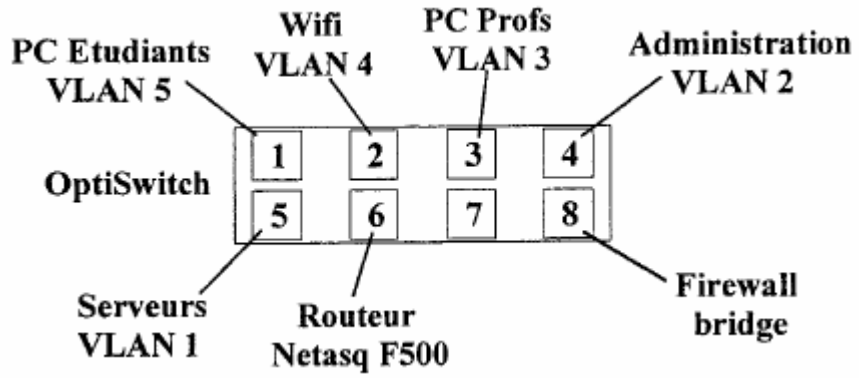
EXONET N° 8

Le réseau de l'université **UNIV** est organisé comme suit :

- L'organisation logique s'articule sur 5 VLAN répartis de la façon suivante :

Nom du réseau	VLAN Id	Adresse IP du réseau
Serveurs	1	193.49.176.0/24
Administration	2	192.168.4.0/24
PC Profs	3	192.168.9.0/24
Wifi	4	192.168.8.0/24
PC Etudiants	5	192.168.7.0/24

- Le schéma ci-dessous indique quels numéros de port physiques du backbone sont connectés :



Le Netasq F500 est désigné par le constructeur comme un firewall. En fait, cette machine est configurée de façon à intégrer les fonctions suivantes : firewall, routeur et serveur DHCP

La communication directe entre les différents réseaux de UNIV n'est possible qu'à travers le Netasq. Ce dernier assure le routage « InterVlan(s) ». Sur son lien physique avec l'OptiSwitch, il possède donc une adresse IP par VLAN ; ses adresses IP sont indiquées par la tableau ci-dessous :

VLAN Id	Adresse IP du Netasq
1	193.49.176.250/24
2	192.168.4.254/24
3	192.168.9.254/24
4	192.168.8.254/24
5	192.168.7.254/24

Le serveur proxy (réseau « Serveurs ») assure uniquement les accès Web et FTP des stations de UNIV, sauf pour toutes les stations du réseau « PC Profs » pour lesquelles le Netasq réalise alors une translation d'adresse IP. Les accès autres que Web et FTP se font sans passer par le proxy.

Le firewall bridge assure le filtrage du trafic entre le réseau externe, la DMZ et le réseau local UNIV.

Toutes les requêtes provenant du réseau externe sont dirigées vers les services de la DMZ.

Seul le routeur Netasq et le serveur proxy peuvent faire des requêtes vers l'extérieur.

Dans le VLAN 4, la première adresse du réseau IP (soit 192.168.8.1/24) est attribuée à un poste de supervision. Ce poste permet d'assurer la télémaintenance sur tous les postes et serveurs du site UNIV.

Les informations utiles concernant l'adressage IP du réseau de UNIV se trouvent sur le schéma donné en Annexe 1.

1. Il apparaît que les VLAN sont gérés comme des réseaux IP. **Pourquoi a-t-on opté pour cette solution ?**
2. Le routeur Netasq F500 assure un routage « InterVlan(s) ». De ce fait, sur son lien avec l'OptiSwitch, il possède une adresse IP par VLAN.
Sur le document réponse 1, compléter la table de routage du routeur.
3. Les réseaux existants permettent d'adresser chacun 254 machines. Le nombre d'étudiants augmentant, une extension des possibilités d'adressage est envisagée pour le réseau PC-étudiants.
3.1. Donner le masque de sous-réseau qui permettrait de multiplier au moins par deux le nombre de machines (sans changer les adresses existantes et en se limitant à un maximum de 1500 machines adressables). Justifier votre réponse.
3.2. Donner, dans ce cas, l'adresse de diffusion.
3.3. Indiquer sur le document réponse 1 quelle serait la modification dans la table de routage du routeur Netasq F500.
4. Les configurations IP des stations du VLAN 3 sont attribuées dynamiquement par le Netasq F500. Sachant que les 10 premières et 10 dernières adresses de la plage totale sont réservées à d'autres usages, **compléter le tableau du document réponse 1 en indiquant les paramètres de configuration DHCP, les valeurs correspondantes et en précisant leur caractère optionnel.**
5. Tous les accès Web et FTP des machines de UNIV se font par l'intermédiaire du serveur proxy. **Compléter la table de routage de ce serveur sur le document réponse 1.**

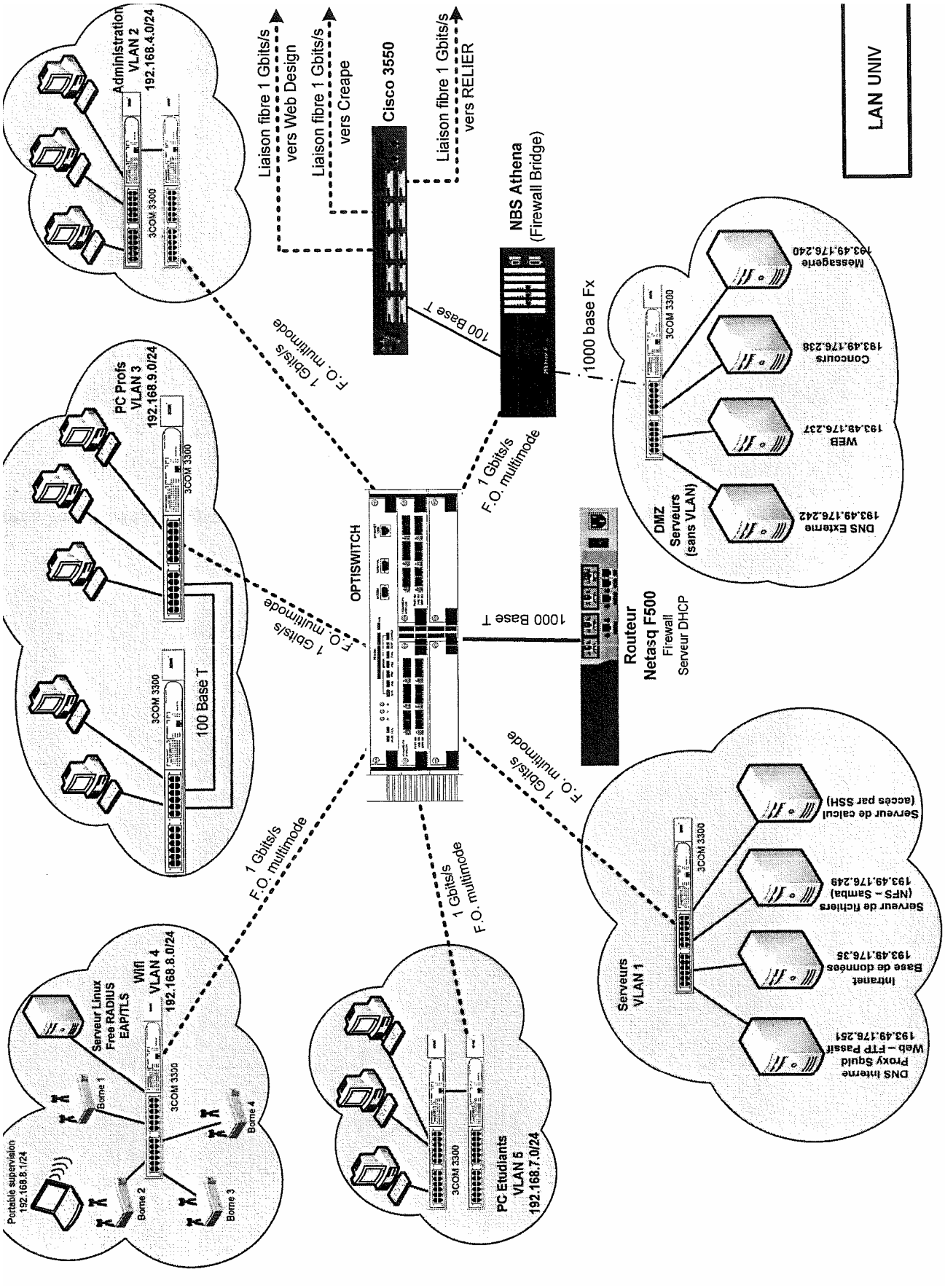
Le firewall Netasq F500 en plus de la translation d'adresses IP a pour tâche de filtrer le trafic entrant et sortant en fonction du cahier des charges donné ci-dessous.
Ce cahier des charges du firewall Netasq est constitué des règles suivantes :
Contraintes : les accès Web et FTP :
Tous les accès directes Web et FTP vers Internet sont interdits sauf :

i. requêtes et réponses pour les adresses IP du réseau PC Profs ;
ii. requêtes et réponses pour la station du Supervision ;
iii. les réponses du proxy (port : 1080) sont autorisées vers le LAN.

Contraintes : les accès DNS :
Seules la résolution DNS à destination du serveur « DNS externe » situé dans la DMZ est autorisée.

6. En vous basant sur ces contraintes et sur le document annexe 2, écrire les règles de filtrage correspondantes en complétant le tableau du document réponse 2.
NB. -Tenir compte de la priorité : une règle énoncée est toujours prioritaire vis-à-vis de celles qui la suivent.
-Un accès à un service induit un échange dans les deux sens (requête, réponse). Il est donc nécessaire d'en tenir compte dans les règles de filtrage.
7. Admettant que le firewall bridge laisse passer les requêtes provenant de l'Internet, est-il nécessaire de prévoir des règles qui protégent le LAN des ces accès ? Justifier votre réponse.

Annexe 1


LAN UNIV
Liaison fibre 1 Gbits/s vers Web Design
Liaison fibre 1 Gbits/s vers Creape
Liaison fibre 1 Gbits/s vers RELIER
Cisco 3550
NBS Athena
(Firewall Bridge)
1000 base Fx
100 Base T
1 Gbits/s F.O. multimode
OPTISWITCH
1000 Base T
Routeur
Netasq F500
Firewall
Serveur DHCP
Administration
VLAN 2
192.168.4.0/24
PC Profs
VLAN 3
192.168.9.0/24
100 Base T
Wifi
VLAN 4
192.168.8.0/24
Serveur Linux
Free RADIUS
EAP/TLS
Portable supervision
192.168.8.1/24
Borne 1
Borne 2
Borne 3
Borne 4
PC Etudiants
VLAN 5
192.168.7.0/24
Serveurs
VLAN 1
DNS interne
Proxy Squid
Web – FTP Passif
193.49.176.251
Intranet
Base de donnees
193.49.176.35
Serveur de fichiers
(NFS – Samba)
193.49.176.249
Serveur de calcul
(acces par SSH)
DMZ
Serveurs
(sans VLAN)
DNS Externe
193.49.176.242
WEB
193.48.176.237
Concours
193.49.176.238
Messagerie
193.49.176.240
3COM 3300

Annexe 2

Port (décimal)	Type	Affectation
20	TCP	FTP données
21	TCP	FTP
22	TCP	SSH : connexion sécurisée
23	TCP	Telnet
25	TCP	SMTP
53	UDP	DNS
67	UDP	BootP
69	UDP	TFTP
80	TCP	HTTP
88	TCP	Kerberos
110	TCP	POP3
113	TCP	Service d'authentification
137	UDP	NetBios
139	TCP	NetBios
161	UDP	SNMP
520	UDP	Routing
546	UDP	DHCP
750	TCP/UDP	KERBEROS

Document réponse 1

Question 2 Table de routage du routeur Netasq F500

Destinations réseau	*Masque réseau*	*Adresse passerelle*	*Adresse interface*
0.0.0.0	0.0.0.0	.....	.....
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
192.168.4.0	255.255.255.0	.....	.....
192.168.7.0	.....	.....	.....
192.168.8.0	.....	.....	.....
192.168.9.0	.....	.....	.....
193.49.176.0	.....	.....	.....
255.255.255.255	255.255.255.255	193.49.176.250	193.49.176.250

Question 3.3 Suite à l'extension du réseau « PC-étudiants », indiquez ci-dessous quelle serait la ligne qui viendrait en remplacement de la ligne grisée ci-dessus.

.....	.....	.....	.....

Question 4 Configuration du DHCP

Noms des paramètres	Valeur(s) associée(s)	Optionnel (oui/non)

Question 5 Table de routage du serveur Proxy

Destinations réseau	*Masque réseau*	*Adresse passerelle*	*Adresse interface*
0.0.0.0	0.0.0.0	.....	.....
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
192.168.1.0	255.255.255.0	.....	.....
192.168.2.0	.....	.....	.....
192.168.3.0	.....	.....	.....
192.168.4.0	.....	.....	.....
192.168.5.0	.....	.....	.....
193.49.176.0	.....	.....	.....
255.255.255.255	255.255.255.255	.....	.....

Document réponse 2

Question 7

N° règle	Source		Destination		Action (passer/bloquer)
	machine ou réseau	N° de port TCP	machine ou réseau	N° de port TCP	

Remarque :

- dans le cas ou la source et/ou la destination et/ou le port peuvent être indifférents, la (ou les) valeur(s) sera (seront) « Any ».
- la source ou la destination doit être spécifiée sous le format CIDR (@IP/mask).
- Si la source ou la destination est un réseau, le mask sera celui du sous-réseau.
- Si la source ou la destination est un hôte, le mask sera /32

Corrigé Exonet N° 8

Question 1. Il apparaît que les VLAN sont gérés comme des réseaux IP. Pourquoi a-t-on opté pour cette solution ?

Les VLAN sont gérés comme des sous-réseaux afin de permettre le routage entre eux.

Question 2. Le routeur Netasq F500 assure un routage « InterVlan(s) ». De ce fait, sur son lien avec l'OptiSwitch, il possède une adresse IP par VLAN.
Sur le document réponse 1, compléter la table de routage du routeur.

Destinations réseau	*Masque réseau*	*Adresse passerelle*	*Adresse interface*
0.0.0.0	0.0.0.0	**193.49.176.254**	**193.49.176.250**
127.0.0.0	255.0.0.0	**127.0.0.1**	127.0.0.1
192.168.4.0	255.255.255.0	**192.168.4.254**	**192.168.4.254**
192.168.7.0	**255.255.255.0**	**192.168.7.254**	**192.168.7.254**
192.168.8.0	**255.255.255.0**	**192.168.8.254**	**192.168.8.254**
192.168.9.0	**255.255.255.0**	**192.168.9.254**	**192.168.9.254**
193.49.176.0	**255.255.255.0**	**193.49.176.250**	**193.49.176.250**
255.255.255.255	255.255.255.255	193.49.176.250	193.49.176.250

Les réseaux existants permettent d'adresser chacun 254 machines. Le nombre d'étudiants augmentant, une extension des possibilités d'adressage est envisagée pour le réseau PC étudiants.

Question 3.1. Donner le masque de sous-réseau qui permettrait de multiplier au moins par deux le nombre de machines (sans changer les adresses existantes et en se limitant à un maximum de 1500 machines adressables). Justifier votre réponse.

Question 3.2. Donner, dans ce cas, l'adresse de diffusion.

Question 3.3. Indiquer sur le document réponse 1 quelle serait la modification dans la table de routage du routeur Netasq F500.

3.1. La solution qui permettra de doubler les possibilités d'adressage du sous réseau « PC-Etudiants » consiste à diminuer d'une unité le nombre de bits du masque.
Il passera donc à « /23 » soit à 255.255.254.0
Diminuer de 2 bits provoquerait un chevauchement avec le réseau 192.168.4.0 ; diminuer de 3bits dépasserait la limite du nombre de machines imposé.

3.2. Dans ce cas, l'adresse de broadcast est 192.168.7.255

3.3.

192.168.6.0	**255.255.254.0**	**192.168.7.254**	**192.168.7.254**

Question 4. Les configurations IP des stations du VLAN 3 sont attribuées dynamiquement par le Netasq F500. Sachant que les 10 premières et 10 dernières adresses de la plage totale sont réservées à d'autres usages, compléter le tableau du document réponse 1 en indiquant les paramètres de configuration DHCP, les valeurs correspondantes et en précisant leur caractère optionnel.

Noms des paramètres	Valeur(s) associée(s)	Optionnel (oui/non)
Adresse IP	**de 192.168.8.11 à 192.168.8.244**	**non**
Adresse de passerelle	**192.168.8.254**	**oui**
Durée du bail	-----	**non**
Masque de sous-réseau	**255.255.255.0**	**non**
Adresse DNS	**Pas d'adresse**	**oui**
Adresse Wins	-----	**oui**
Nom de domaine	-----	**oui**

Question 5. Tous les accès Web et FTP des machines de UNIV se font par l'intermédiaire du serveur proxy. Compléter la table de routage de ce serveur sur le document réponse 1.

Destinations réseau	*Masque réseau*	*Adresse passerelle*	*Adresse interface*
0.0.0.0	0.0.0.0	**193.49.176.254**	**193.49.176.251**
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
192.168.4.0	255.255.255.0	**193.49.176.250**	**193.49.176.251**
192.168.7.0	**255.255.255.0**	**193.49.176.250**	**193.49.176.251**
192.168.8.0	**255.255.255.0**	**193.49.176.250**	**193.49.176.251**
192.168.9.0	**255.255.255.0**	**193.49.176.250**	**193.49.176.251**
193.49.176.0	**255.255.255.0**	**193.49.176.251**	**193.49.176.251**
255.255.255.255	255.255.255.255	**193.49.176.251**	**193.49.176.251**

Question 6. En vous basant sur ces contraintes et sur le document annexe 2, écrire les règles de filtrage correspondantes en complétant le tableau du document réponse 2.

N° règle	Source		Destination		Action (passer/bloquer)
	machine ou réseau	N° de port TCP	machine ou réseau	N° de port TCP	
1	192.168.9.0/24	ANY	ANY	80	PASSER
2	192.168.8.1/24	ANY	ANY	80	PASSER
3	ANY	80	192.168.9.0/24	ANY	PASSER
4	ANY	80	192.168.8.1/32	ANY	PASSER
5	193.149.176.251/32	1080	ANY	ANY	PASSER
6	192.168.9.0/24	ANY	ANY	20	PASSER
7	192.168.9.0/24	ANY	ANY	21	PASSER
8	192.168.8.1/32	ANY	ANY	20	PASSER
9	192.168.8.1/32	ANY	ANY	21	PASSER
10	ANY	20	192.168.9.0/24	ANY	PASSER
11	ANY	21	192.168.9.0/24	ANY	PASSER
12	ANY	20	192.168.8.1/32	ANY	PASSER
13	ANY	21	192.168.8.1/32	ANY	PASSER
14*	192.168.0.0/16	ANY	193.49.176.0/24	ANY	PASSER
15	193.49.176.252/32	53	ANY	ANY	PASSER
16	ANY	ANY	ANY	ANY	BLOQUER

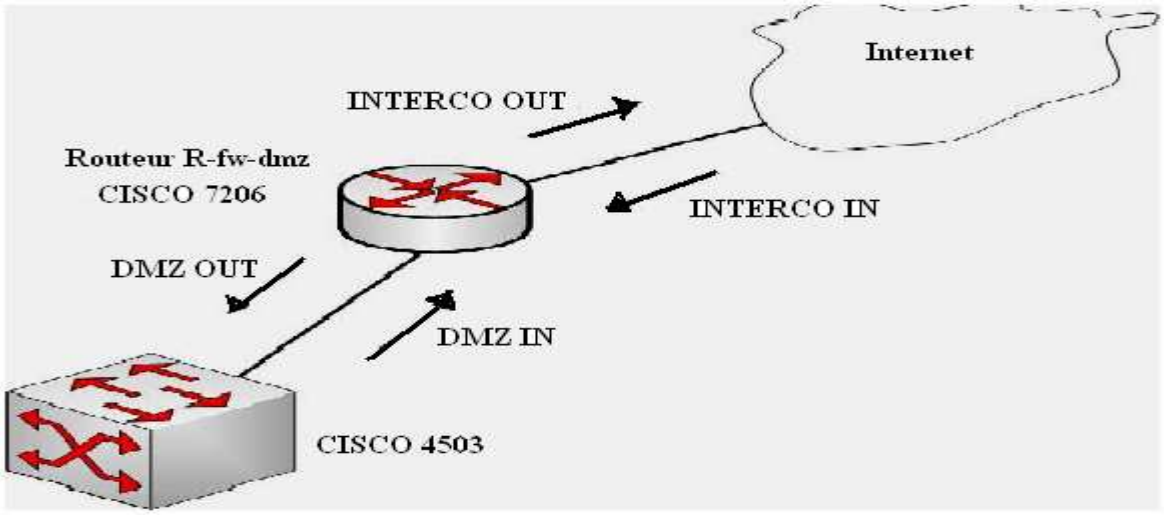
Question 7. Admettant que le firewall bridge laisse passer les requêtes provenant de l'Internet, est il nécessaire de prévoir des règles qui protégent le LAN des ces accès ? Justifier votre réponse.

Non, il n'est pas nécessaire de créer une régle pour bloquer les accès externes, ceux-ci seront inopérants du fait de la translation d'adresse et de port (PAT) utilisé sur le Netasq.

EXONET N° 9

Le réseau de l'entreprise REZOnet est composé de différents sites répartis sur toute la région d'Errachidia. Le routeur qui nous intéresse (R-fw-dmz) se situe sur le site Errachidia centre et joue le rôle de passerelle filtrante vers Internet pour tous les sites en utilisant la translation d'adresses et les listes d'accès (access-list).

Zoom sur le routeur et ses interfaces :



L'intitulé du routeur R-fw-dmz fait penser à Firewall et DMZ.

1.1. Expliquer le rôle d'un firewall.

1.2. Expliquer ce qu'est une DMZ.

1.3. Citer 2 protocoles routables et 2 protocoles de routage.

1.4. Hormis celles filtrées, **citer 2 types de trames qui ne sont pas routées par le routeur R-fw-dmz.**

2.1. En vous aidant des annexes 1 et 2 **compléter le document réponse 1 qui concerne une partie de la configuration du routeur R-fw-dmz .**

2.2. Pour les règles des lignes **4** et **6** du document réponse 1 **calculer les plages d'adresses des réseaux concernés.**

2.3. Pourquoi toutes les access-lists présentes dans la configuration du routeur se terminent par "permit ip any any" ?

2.4. Si l'on souhaite interdire le service TFTP, **quelle ligne faut-il ajouter à la configuration du routeur dans l'access-list "dmz_in".**

Document réponse 1

Ligne	*Extrait de la configuration du routeur*	*Explications*
1	deny udp any any range 6881 6889	
2	deny tcp any any range 135 139	
3	deny udp any any eq 445	
4	deny tcp 10.0.0.0 0.255.255.255 any eq smtp log	
5	deny ip any 172.16.0.0 0.15.255.255	
6	deny ip 195.52.208.0 0.0.7.255 any	
7	permit ip any any	

Annexe 1

Les routeurs sont des équipements de niveau 3 (réseau) et sont chargés de l'acheminement des datagrammes IP entre les réseaux.
En terme de sécurité, ils sont chargés plus précisément :
· de la recherche de chemins de secours
· du filtrage des broadcasts
· du filtrage des datagrammes IP (ACL)
· du contrôle des correspondances entre ports et adresses IP, et entre adresses MAC et adresses IP. (contrôle d'usurpation)

Les ACL (Access Control Lists)

Les ACL sont des filtres appliqués à chaque datagramme IP transitant à travers le routeur et qui ont pour paramètres :
· l'adresse IP de la source
· l'adresse IP de la destination
· le type du paquet (tcp, udp, icmp, ip)
· le port de destination du paquet
Pour un datagramme donné, l'ACL prend deux valeurs :
· **deny** : le paquet est rejeté.
· **permit** : le paquet peut transiter par le routeur.

Syntaxe

Les routeurs Cisco acceptent deux types d'ACL :
· l'access-list simple :
access-list access-list-number {deny|permit} protocole ip-source source-masque
· l'access-list étendue (extended) :
access-list access-list-number {deny|permit} protocole ip-source source-masque ip destination destination-masque port-destination

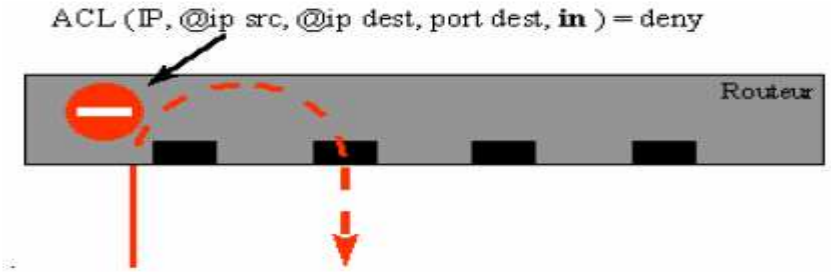
access-list-number • entre 1 et 99 (simples) • entre 100 et 199 (étendus)	numéro d'access-list :
deny	interdit l'accès lorsque les conditions sont vérifiées
permit	autorise l'accès lorsque les conditions sont vérifiées
protocole	nom ou numéro d'un protocole IP, comme **icmp**, **tcp**, **udp** ou **ip** pour préciser tous les protocoles ip
ip-source • l'adresse précisée sur 32 bits, • **any** pour toutes les stations (équivaut à 0.0.0.0 255.255.255.255) • **host** source pour une station particulière (équivaut à source 0.0.0.0)	adresse ip d'un réseau ou d'une station. Ce peut être :
masque-source	permet d'ignorer certains bits de l'adresse source. Les bits ignorés sont positionnés à 1 dans le masque.

ip-destination	adresse ip d'un réseau ou d'une station. Ce peut être : • l'adresse précisée sur 32 bits, • **any** pour toutes les stations (équivaut à 0.0.0.0 255.255.255.255) • **host** destination pour une station particulière (équivaut à source 0.0.0.0)
masque-destination	permet d'ignorer certains bits de l'adresse destination. Les bits ignorés sont positionnés à 1 dans le masque.
port-destination	uniquement pour tcp et udp, expresion de type : • **eq** numéro de port : identique (égale) à ... • **gt** numéro de port : plus grand que... • **lt** numéro de port : plus petit que • **ne** numéro de port : différent de ... • **established** : dans le cas d'une connexion tcp établie. • **Range N° port début N° port fin** : Défini une plage de N° de port.
log	Créer un fichier journal (log) pour consigner l'événement.

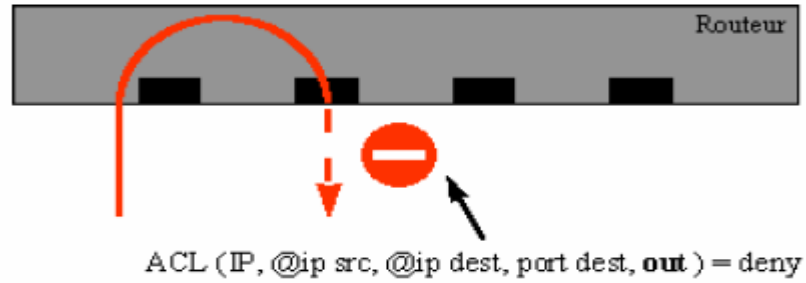
Activation de l'access-list

On associe à chaque interface du routeur une ACL.

Une ACL de type **in**, associée à une interface, contrôle le trafic qui entre dans le routeur par cette interface



Une ACL de type **out** associée à une interface contrôle le trafic qui quitte le routeur par cette interface.



Attention :

- les ACL ne s'appliquent qu'au **trafic en transit** et pas au trafic généré par le routeur lui-même. Par exemple, le trafic résultant d'une connexion telnet vers le routeur n'est pas soumis aux ACL.
- Implicitement la règle : **deny ip any any** est toujours appliquée à la fin de l'access-list, il n'est donc pas nécessaire de rajouter cette commande pour bloquer le reste du trafic.

L'activation d'une access-list sur une interface se fait par la commande :
ip access-group access-list-number {in|out}

access-list-number	numéro de l'access-list
in	filtre les paquets en entrée
out	filtre les paquets en sortie

Recommandations pour la configuration des routeurs :
Access-list contre le spoofing
L'access-list suivante interdit l'accès au réseau pour tous les datagrammes en provenance de l'extérieur, dont :
· l'adresse source est locale (127.0.0.0, 0.0.0.0)
· l'adresse source est privée (10.0.0.0, 172.16.0.0 et 192.168.0.0) (RFC 1918),
· l'adresse source est une adresse multicast (224.0.0.0) ou broadcast (255.255.255.255)
· l'adresse source est sur le réseau interne
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
interdire paquet ip de réseau 127.0.0.0 vers tout(toute station)
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.0.255.255 any
access-list 100 deny ip 224.0.0.0 31.255.255.255 any
access-list 100 deny ip host 255.255.255.255 any
access-list 100 deny ip host 0.0.0.0 any
access-list 100 permit ip any any
Cette access-list doit être appliquée sur toutes les interfaces externes :
ip access-group 100 in

Adresse IP et masque générique
Les ACL définissent des familles d'adresses IP à l'aide d'une **adresse IP** et d'un **masque générique**.
Pour vérifier si une adresse IP appartient à une famille :
· prendre l'adresse IP
· appliquer le masque générique, c'est-à-dire mettre à 0 dans l'adresse IP tous les bits qui sont à 1 dans le masque classique.
· comparer le résultat obtenu à l'adresse générique de la famille.
Exemples d'adresses génériques et de masques :
· 192.9.200.0 0.0.0.255 Toutes les adresses IP du réseau 192.9.200.0
· 192.9.200.1 0.0.0.0 L'adresse IP 192.9.200.1
· 0.0.0.0 255.255.255.255 Toute adresse IP.
· 192.9.200.0 0.0.0.63 Toutes les adresses IP comprises entre 192.9.200.0 et 192.9.200.63
· 147.210.0.254 0.0.255.0 Toutes les adresses IP de la forme 147.210.x.254

Annexe 2

Assignation de certains ports associés aux processus serveurs en fonction des protocoles de transport TCP et UDP.

Processus	Port	Protocole Description
ftp-data	20	File Transfer [Default Data]
ftp	21	File Transfer [Control]
ssh	22	SSH Remote Login Protocol
telnet	23	Telnet
smtp	25	Simple Mail Transfer
domain	53	Domain Name Server
bootpc	68	Bootstrap Protocol Client
tftp	69	Trivial File Transfer
http	80	World Wide Web HTTP
pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
sftp	115	Simple File Transfer Protocol
nntp	119	Network News Transfer Protocol
statsrv	133	Statistics Service
netbios-ns	137	NETBIOS Name Service
netbios-dgm	138	NETBIOS Datagram Service
netbios-ssn	139	NETBIOS Session Service
Imap2	143	Interim Mail Access Proto v2
snmp	161	Simple Net Mgmt Proto
https	443	MComhttps
Microsoft-DS	445	NETBIOS Datagram Service(Win2000)
P2P	6881 to 6889	client P2P

Corrigé Exonet N° 9

Question 1.1 Expliquer le rôle d'un firewall.

FW : Un pare-feu (appelé aussi coupe-feu ou firewall en anglais), est un système permettant de protéger un ordinateur des intrusions provenant d'un réseau (ex: Internet). Le pare-feu est en réalité un système permettant de filtrer les paquets de données échangés avec le réseau.

Question 1.2. Expliquer ce qu'est une DMZ.

DMZ : Une zone démilitarisée dit DMZ est un segment de réseau sur lequel des ressources internes sont accessibles par des clients externes.

Question 1.3. Citer 2 protocoles routables et 2 protocoles de routage.

Protocoles routables : **IP, IPX**
Protocoles de routage : **RIP, BGP, OSPF**

Question 1.4. Hormis celles filtrées, citer 2 types de trames qui ne sont pas routées par le routeur R-fw-dmz.

Les trames et les datagrammes IP que le routeur ne laisse pas passer sont :
- les trames de diffusion
- les datagrammes dont l'adresse de destination est inconnue.
- les datagrammes dont le TTL est à 1.

Question 2.1. En vous aidant des annexes 1 et 2 compléter le document réponse 1 qui concerne une partie de la configuration du routeur R-fw-dmz.

Partie de la configuration du routeur	***explications***
deny udp any range 6881 6889	*Interdire toutsegment udp de port 6881 à 6889 (peer to peer)*
deny tcp any any range 135 139	*Interdit tout segment tcp concernant le partage NETBIOS*
deny udp any any eq 445	*Interdit tout segment udp vers tout avec le port = 445 (partage 2000)*
deny tcp 10.0.0.0 0.255.255.255 any eq smtp log	*Interdit l'accès à toutes stations du réseau 10.0.0.0 au service smtp et création d'un journal*
deny ip any 172.16.0.0 0.15.255.255	*Interdit l'accès en IP à toutes stations du réseau 172.16.0.0/12 Anti spoofing*
deny ip 195.52.208.0 0.0.7.255 any	*Interdit tout paquet ip des réseaux 195.52.208.0/21vers tout*

Question 2.2. Pour les règles des lignes 4 et 6 du document réponse 1 calculer les plages d'adresses des réseaux concernés.

Ligne 4: la plage d'adresses concernée est 10.0.0.0 à 10.255.255.255 car le masque classique est 255.255.255.0 (masque générique: 0.255.255.255).
Ligne 6: la plage d'adresses concernée est 195.52.208.0 à 195.52.215.255 car le masque classique est 255.255.248.0 (masque générique: 0.0.7.255).

Question 2.3. Pourquoi toutes les access-lists présentes dans la configuration du routeur se terminent par "permit ip any any" ?

Par défaut, tout le trafic est bloqué donc si on veut au contraire autoriser tout ce qui n'a pas été interdit , il faut mettre la ligne suivante à la fin de l'acces-list : " permit ip any any"

Question 2.4. Si l'on souhaite interdire le service TFTP, quelle ligne faut il ajouter à la configuration du routeur dans l'access-list "dmz_in".

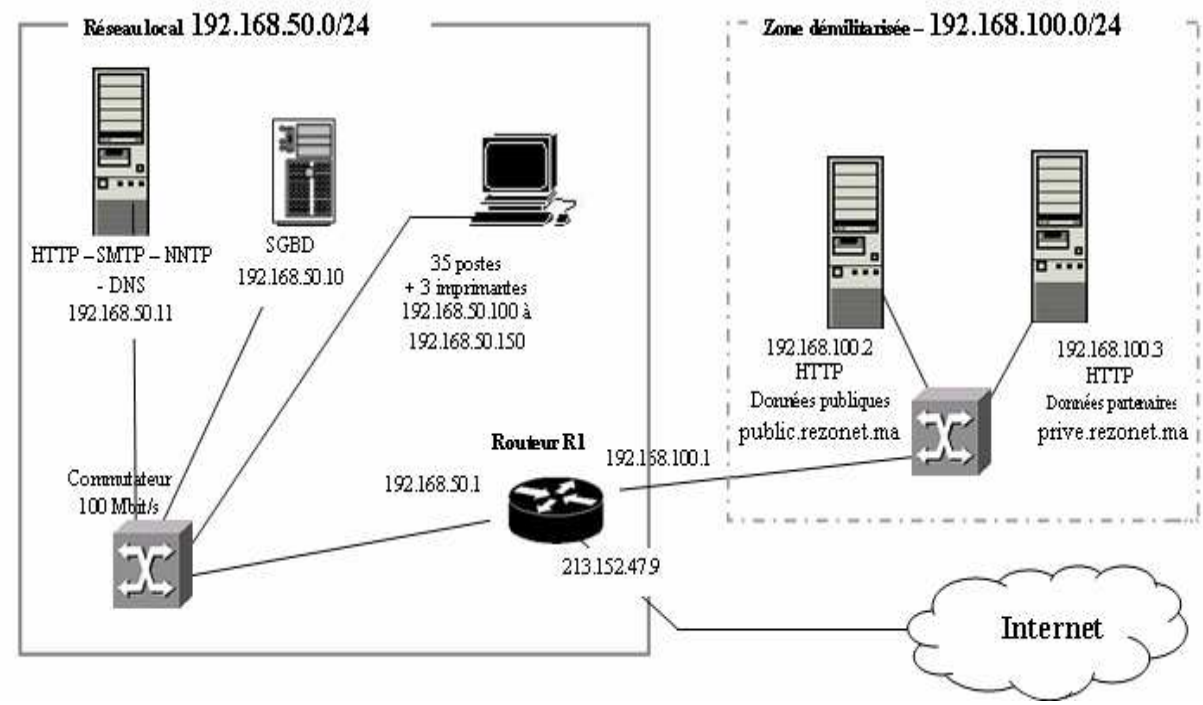
deny udp any any eq 69

EXONET N° 10

L’entreprise REZOnet externalisait ses serveurs HTTP, NNTP et SMTP pour l’Internet et l’extranet. Elle a décidé d’accueillir dans une zone démilitarisée ces serveurs. Ceci l’a conduit à revoir son architecture réseau et sa politique de sécurité.
Après avoir décidé dans un premier temps de créer une DMZ avec une adresse publique, l'administrateur décide d'utiliser aujourd'hui une adresse privée pour renforcer la sécurité.
Le routeur d’accès distant (R1) est un routeur filtrant, il permet d’interdire certains flux et en autoriser d'autres. Ce routeur prend aussi en charge la traduction d'adresses (NAT/PAT).
Les clients du réseau local ont un accès à Internet.
L’annexe 1 la structure schématique du nouveau réseau de l’entreprise.
L’annexe 2, des exemples de règles NAT/PAT appliquées par le routeur R1.
L’annexe 3 des exemples de règles de redirection appliquées par le routeur R1.

1. Pourquoi le routeur R1 masque-t-il les adresses du réseau 192.168.50.0/24 ?
2. Expliquer le rôle des règles de l'annexe 3.
3. Le routage porte-t-il sur les adresses substituées ou sur les adresses réelles ?
4. Pourquoi n'utilise-t-on pas le port standard 80 pour rediriger vers le serveur http partenaire de nom prive.rezonet.ma ?
5. Comment les clients http des partenaires doivent-ils adresser leur requête pour accéder au serveur http partenaire prive.rezonet.ma?
L'administrateur décide d'appliquer une politique de sécurité plus restrictive. Il veut empêcher tout trafic entre l'Internet et l'Intranet. Pour cela il va mettre en place un Proxy HTTP sur un serveur d'adresse 192.168.100.4 dans la DMZ qui écoutera sur le port 8080. Tous les utilisateurs devront passer par ce Proxy.
6. Comment fonctionne un Proxy-HTTP et quel est son intérêt ?
7. Proposer une solution pour permettre aux postes de l'Intranet d'utiliser le Proxy-HTTP de façon transparente.
8. Rédiger le(s) règle(s) permettant cette solution.

Annexe 1 : Structure schématique du réseau



Annexe 2 : exemples de règles NAT/PAT

Le type NP (NAT/PAT) s'applique en sortie de l'interface et substitue l'adresse IP source et le port source privés par une adresse IP publique et un port public. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

N°	Interface	Type	protocole	Adresse publique	port public	adresse privée	port privé
1	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.50.0/24	*
2	213.152.47.9	NP	TCP	213.152.47.9	*	192.168.100.0/24	*

Annexe 3 : exemples de règles de redirection

Le Type R (Redirection) s'applique en entrée de l'interface et substitue l'adresse IP destination et le port de destination publics par une adresse IP privée et un port privé. Cette règle génère une entrée dans une table interne du routeur qui permettra de gérer la substitution inverse.

N°	Interface	Type	protocole	Adresse publique	port public	adresse privée	port privé
3	213.152.47.9	R	TCP	213.152.47.9	80	192.168.100.2	80
4	213.152.47.9	R	TCP	213.152.47.9	4500	192.168.100.3	80

Corrigé Exonet N° 10

Question 1. Pourquoi le routeur R1 masque-t-il les adresses du réseau 192.168.50.0/24 ?

les adresses de classe C 192.168.x.x sont des adresses privées qui ne peuvent être routées sur Internet, il faut donc les substituer par une adresse publique (ici l'adresse publique du routeur).

Question 2. Expliquer le rôle des règles de l'annexe 3.

Les règles de l'annexe 3 redirigent vers les serveurs http de la DMZ les paquets dont l'entête TCP comporte les ports de destination précisés. L'adresse IP de destination qui est l'adresse publique du routeur sera substituée par l'adresse privée précisée. Le port de destination sera lui aussi substitué si cela est nécessaire. Ces substitutions sont faites avant d'entrer dans le processus de routage et de filtrage.

Question 3. Le routage porte t-il sur les adresses substituées ou sur les adresses réelles ?

Le processus de routage utilise l'adresse de destination d'un paquet pour prendre sa décision de routage. Cette décision ne peut être prise sur les adresses substituées car celles-ci ne correspondent pas aux adresses réelles du réseau local. Les règles suivantes sont donc appliquées :

- On substitue en entrée de l'interface les adresses et les ports de destination par les adresses et les ports privés. Cette substitution se fait avant le processus de routage et de filtrage qui va donc porter sur les adresses réelles.
- On substitue en sortie de l'interface les adresses et les ports sources par les adresses et les ports publics. Cette substitution se fait après le processus de routage et de filtrage qui a donc porté sur les adresses réelles.

Question 4. Pourquoi n'utilise t-on pas le port standard 80 pour rediriger vers le serveur http partenaire de nom prive.rezonet.ma ?

Il faut différencier les ports des serveurs. En effet une requête DNS sur public.sagi.fr ou prive.rezonet.ma renvoie l'adresse IP publique du routeur. On ne peut donc pas avoir deux fois le même port associé à la même adresse IP publique, car il est impossible de rediriger correctement la requête vers le serveur correspondant. On laisse ici les données publiques sur le port 80 (port standard du protocole http) mais on change le port http des données partenaires.

Question 5. Comment les clients http des partenaires doivent ils adresser leur requête pour accéder au serveur http partenaire prive.rezonet.ma?

Les clients des partenaires doivent connaître ces numéros de port (il faut saisir le numéro de port dans l'URL.) ex: HTTP://prive.rezonet.ma:4500

Question 6. Comment fonctionne un Proxy HTTP et quel est son intérêt ?

Le terme français pour désigner un Proxy est mandataire, c'est-à-dire celui à qui on confie un travail. Les proxys sont des relais. Ils jouent le rôle de serveur pour le client, et de client pour le serveur. Ils peuvent analyser les données dans le contexte de l'application et appliquer des filtres (sites interdits « blacklist », audit, etc.). Dans une configuration minimum un proxy http mettra en cache les pages HTML visitées optimisant ainsi leur utilisation. Un proxy peut permettre d'éviter les connexions directes depuis un réseau interne vers Internet. Sans routeur, il permet le partage de l'accès à Internet avec une interface publique.

Question 7. Proposer une solution pour permettre aux postes de l'Intranet d'utiliser le Proxy HTTP de façon transparente.

Deux solutions sont possibles :

- Configurer tous les navigateurs Internet pour paramétrer le Proxy. Cette solution n'est pas transparente et peut être contournée par les postes.
- Rediriger en entrée de l'interface 192.168.50.1 tout paquet avec l'adresse du port destination 80 vers le Proxy 192.168.100.4. C'est la technique dite du **"Proxy transparent".** Il faut bien sûr que le Proxy le permette c'est le cas de la plupart des Proxy du marché.

Question 8. Rédiger le(s) règle(s) permettant cette solution.

numéro	**Interface**	**Type**	**protocole**	**Adresse publique**	**port public**	**adresse privée**	**Port privé**
5	192.168.50.1	R	TCP	*	80	192.168.100.4	8080

Ici les requêtes http à partir du réseau local sont redirigées vers le proxy situé dans la DMZ. Le Proxy agira ensuite en tant que client Internet il utilisera donc un port client supérieur à 1024 pour ses échanges. Il n'y aura donc pas de confusion avec les échanges des serveurs de la DMZ.
Pour plus de sécurité il faudrait supprimer la règle 1 du NAT/PAT qui masque les adresses des postes du réseau local et leur permet l'accès à Internet.

EXONET N° 11

La filiale d'une société est reliée à son siège par l'intermédiaire de deux connexions distantes : une liaison spécialisée et une liaison de secours RNIS. Chaque liaison est gérée par un routeur différent: un routeur principal et un routeur de secours.
La disponibilité de la connexion est une nécessité pour la filiale. Vous êtes chargé d'étudier la mise en œuvre d'une solution qui permettrait de tolérer la panne du routeur principal.
Pour cela vous allez tout d'abord étudier ce qu'un administrateur devrait faire manuellement en cas de panne du routeur principal pour utiliser le routeur de secours.
Puis vous allez étudier la mise en œuvre de deux protocoles permettant d'assurer dynamiquement la tolérance de panne.
L'annexe 1 vous donne un schéma non exhaustif du réseau.
L'annexe 2 vous donne l'état initial de la configuration des différents éléments actifs du réseau avant la simulation de la panne.
L'annexe 3 présente sommairement les protocoles utilisés.
L'annexe 4 présente le cache ARP du poste 192.168.200.20 après la mise en place de HSRP et l'exécution d'une commande ping.
L'annexe 5 présente l'annonce de route faite par le routeur principal au routeur du siège après la mise en place du protocole de routage RIP.

Vous testez le fonctionnement du routeur principal en exécutant la commande suivante à partir du poste 192.168.200.20 : **ping 192.168.10.1**
Tout se déroule normalement.
Vous simulez une panne sur le routeur principal puis vous activez le routeur de secours sans modifier les configurations décrites dans l'annexe 2.

1. Quel sera le résultat de la commande « ping 192.168.10.1 » exécutée sur le poste 192.168.200.20 ?

2. Quelle doit être la nouvelle configuration du poste 192.168.200.20 pour utiliser le routeur de secours ?

3. La modification apportée sur le poste 192.168.200.20 ne modifie pas le résultat de la commande précédente, pourquoi ? Proposez une solution.

Vous mettez en place le protocole HSRP entre le routeur principal et le routeur de secours sur les interfaces 192.168.200.253 et 192.168.200.254.
Vous affectez aux deux routeurs l'adresse IP virtuelle suivante : 192.168.200.1 et l'adresse MAC virtuelle suivante 00-00-0c-07-ac-02.
Toutes les tables de routage restent dans l'état présenté par l'annexe 2.
Vous testez le fonctionnement du routeur principal en exécutant la commande suivante à partir du poste 192.168.200.20 : **ping 192.168.10.1**
Tout se déroule normalement.
Vous simulez de nouveau une panne sur le routeur principal.

4. Quelle doit être l'adresse du routeur par défaut utilisée par le poste 192.168.200.20 pour tolérer une panne du routeur principal ?

5. Doit-on vider le cache ARP du poste 192.168.200.20 avant d'exécuter de nouveau la commande ping 192.168.10.1 L'annexe 4 présente le contenu actuel du cache ARP.

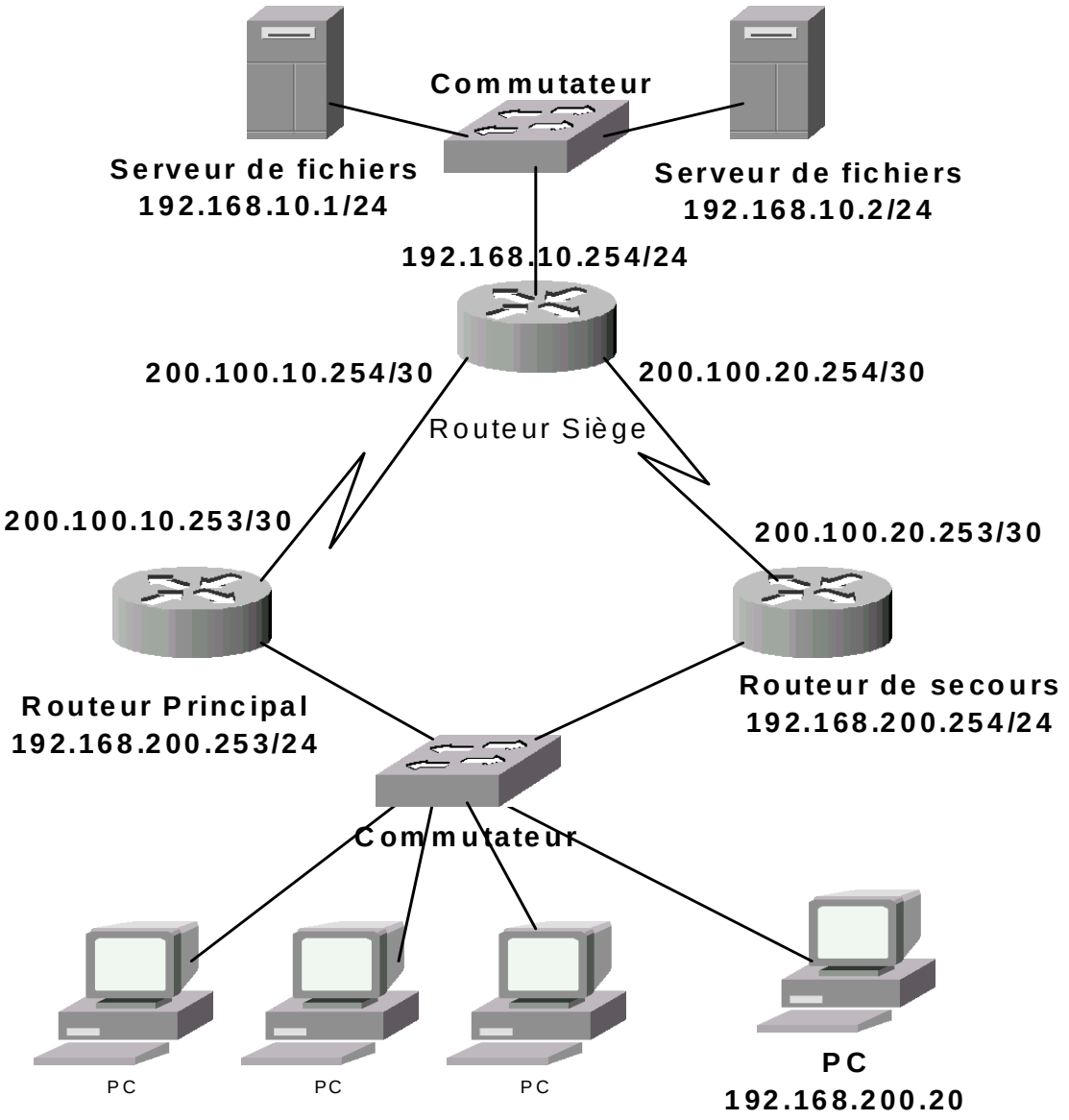
6. Quel sera le résultat de la commande « ping 192.168.10.1 » ?

7. Pourquoi ne met-on pas en œuvre HSRP entre les interfaces 200.100.10.253 et 200.100.20.253 ?

Pour automatiser la mise à jour des tables de routage notamment pour le routeur du siège, vous installez un protocole de routage à vecteur de distance sur les différents routeurs.
Dans un premier temps le routeur principal est actif et transmet des annonces de route au routeur du siège alors que le routeur de secours inactivé par HSRP ne transmet rien.
L'annexe 5 montre l'annonce transmise.
Vous simulez une panne sur le routeur principal. Le routeur du siège cesse de recevoir des annonces de la part du routeur principal mais en reçoit de la part du routeur de secours qui a été activé par HSRP.

8. Sur quelles interfaces doit-on activer le protocole de routage ?
9. Rajouter une colonne métrique aux tables de routage des routeurs.
10. Que contient l'annonce envoyée par le routeur de secours au routeur du siège ?
11. Quelle est la nouvelle table de routage sur le routeur du siège après réception de l'annonce ?

Annexe 1 : Schéma non exhaustif du réseau



Annexe 2 : la configuration des différents éléments actifs du réseau avant la simulation de la panne.

Table de routage du routeur siège

Réseau	Masque	Passerelle	Interface
192.168.10.0	255.255.255.0	192.168.10.254	192.168.10.254
200.100.10.252	255.255.255.252	200.100.10.254	200.100.10.254
200.100.20.252	255.255.255.252	200.100.20.254	200.100.20.254
192.168.200.0	255.255.255.0	200.100.10.253	200.100.10.254

Table de routage du routeur principal

Réseau	Masque	Passerelle	Interface
192.168.200.0	255.255.255.0	192.168.200.253	192.168.200.253
200.100.10.252	255.255.255.252	200.100.10.253	200.100.10.253
192.168.10.0	255.255.255.0	200.100.10.254	200.100.10.253

Le routeur Principal est actif

Table de routage du routeur de secours

Réseau	Masque	Passerelle	Interface
192.168.200.0	255.255.255.0	192.168.200.254	192.168.200.254
200.100.20.252	255.255.255.252	200.100.20.253	200.100.20.253
192.168.10.0	255.255.255.0	200.100.20.254	200.100.20.253

Le routeur de secours est inactif

Table de routage du poste 192.168.200.20

Réseau	Masque	Passerelle	Interface
192.168.200.0	255.255.255.0	192.168.200.20	192.168.200.20
0.0.0.0	0.0.0.0	192.168.200.253	192.168.200.20

Adresse MAC du routeur principal : 0D 0A C1 10 5B 2D
Adresse MAC du routeur de secours : 0D 0A C1 00 24 11

Cache ARP du poste 192.168.200.20

Adresse MAC	Adresse IP	Type
0D 0A C1 10 5B 2D	192.168.200.254	dynamique

Annexe 3 : Présentation des protocoles utilisés.

HSRP (Host Stanby Router Protocol)
HSRP est décrit dans la RFC 2281. Ce document est classé pour information ce qui veut dire qu'il n'est pas un standard Internet. C'est un protocole propriétaire CISCO. Il offre un mécanisme de tolérance aux pannes de la passerelle par défaut aux différentes machines du réseau incapables de découvrir dynamiquement les routeurs qui leur sont affectés (attention on ne fait pas référence ici à DHCP qui ne permet pas cela mais plutôt à des méthodes dynamiques comme IRDP ICMP Router Discovery Protocol).
HSRP permet à deux routeurs de partager une adresse IP virtuelle et une adresse MAC virtuelle. Le routeur actif répond aux requêtes ARP destinées à l'adresse commune comme s'il s'agissait de la sienne puis prend en charge les trames adressées à l'adresse MAC commune. Un échange de message réalisé en multicast permet aux routeurs de déterminer le routeur actif puis de vérifier la présence de l'autre routeur. Lorsque le routeur actif est défaillant, le deuxième routeur ne reçoit plus de message multicast de sa part, il devient alors actif et répond aux requêtes adressées aux adresses communes (IP et MAC).
D'autres protocoles sont bien sûr utilisables comme par exemple VRRP (Virtual Redundancy Router Protocol).

RIP V2 (Routing Information Protocol). La version 2 transmet les masques de sous-réseau.
Un protocole de routage permet de mettre à jour dynamiquement les tables de routage des routeurs.
Les routeurs s'envoient des messages contenant les réseaux qu'ils peuvent atteindre soit directement soit indirectement.
Pour atteindre un réseau, un routeur utilisant un protocole à vecteur de distance choisira toujours la route la plus courte.
La route la plus courte est celle qui traverse le moins de routeur.
Pour évaluer cette distance le routeur associe à chaque réseau une métrique sous la forme d'un entier. La valeur 1 correspond à une remise directe. Une valeur supérieure à 1 correspond à une remise indirecte.
Un routeur utilisant le protocole de routage RIP diffuse toutes les 30s la liste des réseaux qu'il peut atteindre avec leur métrique. Pour RIP la valeur 16 associée à une métrique invalide la route.
D'autres protocoles à vecteur de distance sont bien sûr utilisables par exemple IGRP (Internet Gateway Router Protocol) ou bien EIGRP (Extended Internet Gateway Router Protocol) de CISCO protocle Hybride entre les protocoles à vecteur de distance et ceux à états de lien.

Annexe 4

Cache ARP du poste 192.168.200.20 après la mise en place de ARP et la commande « ping 192.168.10.1 »

Adresse MAC	**Adresse IP**	**Type**
00-00-0c-07-ac-02	192.168.200.1	dynamique

Annexe 5

Annonce transmise par le routeur principal au routeur du siège

Réseau	**Masque**	**Métrique**
192.168.200.0	255.255.255.0	1

Corrigé Exonet N° 11

Question 1. Quel sera le résultat de la commande « ping 192.168.10.1 » exécutée sur le poste 192.168.200.20 ?

Le résultat sera "délai d'attente dépassé". Le paquet ICMP « echo » est parti mais le paquet ICMP « reply » n'est pas revenu dans le temps imparti.

Question 2. Quelle doit être la nouvelle configuration du poste 192.168.200.20 pour utiliser le routeur de secours ?

Il faut modifier la passerelle par défaut pour affecter l'adresse IP du routeur de secours 192.168.200.254

Question 3. La modification apportée sur le poste 192.168.200.20 ne modifie pas le résultat de la commande précédente, pourquoi ? Proposez une solution.

Le problème se situe sur la table de routage du routeur du siège sur « la route de retour ». En effet le paquet part du poste vers la nouvelle passerelle par défaut 192.168.200.254 qui transmet au routeur du siège. Celui-ci transmet au poste 192.168.10.1 qui répond via le routeur du siège. **Mais ce dernier continue à orienter vers le routeur principal qui est inactif.** Il faut donc remplacer la ligne obsolète par la ligne suivante :

192.168.200.0	255.255.255.0	200.100.20.253	200.100.20.254

Question 4. Quelle doit être l'adresse du routeur par défaut utilisée par le poste 192.168.200.20 pour tolérer une panne du routeur principal ?

L'adresse du routeur par défaut doit être l'adresse virtuelle IP 192.168.200.1

Question 5. Doit on vider le cache ARP du poste 192.168.200.20 avant d'exécuter de nouveau la commande ping 192.168.10.1 L'annexe 4 présente le contenu actuel du cache ARP.

Ce n'est pas nécessaire de vider le cache ARP car les deux routeurs utilisent la même adresse MAC virtuelle donc même si le poste ne refait pas de requête ARP pour résoudre l'adresse 192.168.200.1 le routeur de secours traitera bien les trames avec pour adresse MAC destinataire 00-00-0c-07-ac-02

Question 6. Quel sera le résultat de la commande « ping 192.168.10.1 » ?

Le résultat de la commande sera "délai d'attente dépassée" car la table de routage du routeur du siège n'a pas été mise à jour

Question 7. Pourquoi ne met on pas en œuvre HSRP entre les interfaces 200.100.10.253 et 200.100.20.253 ?

On ne peut mettre en œuvre HSRP que sur une même liaison réseau or ces deux interfaces ne sont pas sur une même liaison

Question 8. Sur quelles interfaces doit on activer le protocole de routage ?

Le protocole de routage doit être activé sur les interfaces : 200.100.10.254 200.100.20.254 200.100.10.253 200.100.20.253

Question 9. Rajouter une colonne métrique aux tables de routage des routeurs.

Table de routage du routeur siège

Réseau	**Masque**	**Passerelle**	**Interface**	**Métrique**
192.168.10.0	255.255.255.0	192.168.10.254	192.168.10.254	1
200.100.10.252	255.255.255.252	200.100.10.254	200.100.10.254	1
200.100.20.252	255.255.255.252	200.100.20.254	200.100.20.254	1
192.168.200.0	255.255.255.0	200.100.10.253	200.100.10.254	2

Table de routage du routeur principal

Réseau	**Masque**	**Passerelle**	**Interface**	**Métrique**
192.168.200.0	255.255.255.0	192.168.200.254	192.168.200.254	1
200.100.10.252	255.255.255.252	200.100.10.253	200.100.10.253	1
192.168.10.0	255.255.255.0	200.100.10.254	200.100.10.253	2

Table de routage du routeur de secours

Réseau	**Masque**	**Passerelle**	**Interface**	**Métrique**
192.168.200.0	255.255.255.0	192.168.200.254	192.168.200.254	1
200.100.20.252	255.255.255.252	200.100.20.253	200.100.20.253	1
192.168.10.0	255.255.255.0	200.100.20.254	200.100.20.253	2

Question 10. Que contient l'annonce envoyée par le routeur de secours au routeur du siège ?

Le routeur de secours envoie le même message qu'envoyait le routeur principal :

192.168.200.0	255.255.255.0	1

Question 11. Quelle est la nouvelle table de routage sur le routeur du siège après réception de l'annonce ?

Le routeur du siège invalide la route qui passait par le routeur principal car il ne reçoit plus d'annonce sur cette interface et la remplace par la route proposée par le routeur de secours.

Réseau	**Masque**	**Passerelle**	**Interface**	**Métrique**
192.168.10.0	255.255.255.0	192.168.10.254	192.168.10.254	1
200.100.10.252	255.255.255.252	200.100.10.254	200.100.10.254	1
200.100.20.252	255.255.255.252	200.100.20.254	200.100.20.254	1
192.168.200.0	**255.255.255.0**	**200.100.20.253**	**200.100.20.254**	**2**

EXONET N° 12

Une entreprise dispose de plusieurs routeurs dans son réseau. Un premier routeur (appelé SUPERNET) constitue le point d'entrée sur le réseau local, de tous les réseaux partenaires (filiales et clients). Il est interconnecté à un deuxième routeur (nommé PRIVANET) qui route vers les différents sous-réseaux internes de l'entreprise, en transmettant éventuellement les paquets à d'autres routeurs.
L'annexe 1 présente la table de routage de SUPERNET.
L'annexe 2 présente la table de routage de PRIVANET.

1. Indiquer, parmi les sous-réseaux de l'entreprise, ceux qui sont accessibles via le routeur SUPERNET
2. Indiquer quelles sont les lignes à rajouter dans la table de routage du routeur SUPERNET pour router vers les réseaux non accessibles.
3. Indiquer s'il est possible, avec une seule ligne dans la table de routage du routeur SUPERNET de router vers tous les réseaux.

Annexe 1 : Table de routage du routeur SUPERNET

Destination	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	184.10.20.254	184.10.20.200
200.100.32.0	255.255.224.0	10.0.0.1	10.0.0.2

Annexe 2 : Table de routage du routeur PRIVANET

Destination	Masque	Passerelle	Interface
0.0.0.0	0.0.0.0	10.0.0.2	10.0.0.1
200.100.18.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.31.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.32.0	255.255.255.0	200.100.32.254	200.100.32.254
200.100.33.0	255.255.255.0	200.100.33.254	200.100.33.254
200.100.34.0	255.255.255.0	200.100.34.254	200.100.34.254
200.100.48.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.49.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.50.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.66.0	255.255.255.0	200.100.33.250	200.100.33.254
200.100.98.0	255.255.255.0	200.100.33.250	200.100.33.254

Corrigé Exonet N° 12

Question 1. Indiquer, parmi les sous-réseaux de l'entreprise, ceux qui sont accessibles via le routeur SUPERNET

La deuxième ligne de la table de routage du routeur SUPERNET fait référence à un masque 255.255.224.0. Cela signifie que dans le troisième octet, les trois premiers bits sont à 1.
Toutes les adresses disposant donc des mêmes 19 premiers bits (8 + 8 + 3) seront routées. Il faut donc rechercher parmi l'ensemble des sous-réseaux contenus dans la table de routage de PRIVANET les adresses de réseau qui correspondent à cette propriété.
Pour répondre il faut convertir ces adresses réseaux en binaire :

200.100.18.0 11001000.11000100.**000**10010.00000000
200.100.31.0 11001000.11000100.**000**11111.00000000
200.100.32.0 11001000.11000100.**001**00000.00000000
200.100.33 0 11001000.11000100.**001**00001.00000000
200.100.34 0 11001000.11000100.**001**00010.00000000
200.100.48 0 11001000.11000100.**001**10000.00000000
200.100.49 0 11001000.11000100.**001**10001.00000000
200.100.50.0 11001000.11000100.**001**10010.00000000
200.100.66.0 11001000.11000100.**010**00010.00000000
200.100.98.0 11001000.11000100.**011**00010.00000000

Les réseaux 200.100.32.0, 200.100.33.0; 200.100.34.0; 200.100.48.0; 200.100.49.0; 200.100.50.0 sont ainsi accessibles. Car si on applique un masque qui restreint l'identifiant du réseau à ces 19 bits, avec une seule ligne dans la table de routage on route vers l'ensemble de ces réseaux. Ce qui implique bien un autre routeur (ici PRIVANET) qui distribue les paquets vers les bons sous-réseaux.
Créer des sur-réseaux (l'inverse des sous-réseaux) permet donc de limiter le nombre de lignes sur une table de routage, pour les routeurs "généraux" d'une entreprise.

Question 2. Indiquer quelles sont les lignes à rajouter dans la table de routage du routeur SUPERNET pour router vers les réseaux non accessibles.

Ligne à rajouter pour router vers 200.100.66.0 et 200.100.98.0

200.100.64.0 255.255.192.0 10.0.0.1 10.0.0.2

Il suffit en effet que les deux premiers bits du troisième octet soient égaux à 01 ($0x2^7 + 1x2^6 = 64$), et que le masque dispose d'un troisième octet commençant par 11 ($1x2^7 + 1x2^6 = 192$).

Ligne à rajouter pour router vers 200.100.18.0 et 200.100.31.0

Il faut que les trois premiers bits du troisième octet soient égaux à 000 ($0x2^7 + 0x2^6 + 0x2^5 = 0$), donc que le masque dispose d'un troisième octet commençant par 111 ($1x2^7 + 1x2^6 + 1x2^5 = 224$).

200.100.0.0 255.255.224.0 10.0.0.1 10.0.0.2

Il est aussi possible de restreindre la plage d'adresses routées en tablant sur les quatre premiers bits identiques (0001), ce qui donnerait l'adresse 200.100.16.0 et le masque /20 .

Question 3. Indiquer s'il est possible, avec une seule ligne dans la table de routage du routeur SUPERNET de router vers tous les réseaux.

On considère que toutes les adresses ont le troisième octet qui commence par 0 (adresse 200.100.0.0) ce qui donne un masque dans lequel le troisième octet commence par 1 (soit 128)

200.100.0.0 255.255.128.0 10.0.0.1 10.0.0.2

On pourrait aussi étendre la plage d'adresses routées en considérant que seuls les deux premiers octets sont identiques, ce qui donnerait une adresse identique, mais le masque /16 .

EXONET N° 15

La configuration proposée ne représente pas, loin s'en faut, une configuration idéale. Son étude a simplement pour objectif de balayer différentes fonctionnalités d'un DNS. L'annexe 1 vous permet de vous familiariser avec le vocabulaire et les concepts employés. L'annexe 2 fournit le plan d'adressage du réseau gberger.fr.

1. Compléter l'annexe 3 afin de positionner chaque machine référencée dans son domaine (associée à son adresse IP) à partir de l'analyse du fichier de configuration des zones gberger.fr, tsig.gberger.fr et tscg.gberger.fr (annexe 4). Faire apparaître pour chaque zone la liste des serveurs DNS.
Indiquer les hôtes du réseau gberger.fr qui ne sont pas encore référencés.

2. Répondre aux questions suivantes, en les justifiant :
2.1 Sur quelle machine est stocké le fichier de configuration de la zone tsig.gberger.fr ?
2.2 Quelle est la durée de validité de ses données en cache (exprimée en jours) ?
2.3 Quelle est l'adresse et le nom du serveur secondaire de la zone tscg.gberger.fr ?
2.4 Parmi ces deux zones (tsig.gberger.fr et tscg.gberger.fr), quelle est la zone qui a été le plus souvent modifiée ?
2.5 arle.tsig.gberger.fr est-elle une zone indépendante ?
2.6 Que faut-il faire pour que la résolution de nom pour la machine srv.gberger.fr, d'adresse 10.0.2.1 soit possible ?

3. En utilisant la même représentation que pour les fichiers de configuration fournis en annexe 4, lorsque cela est nécessaire, répondre aux questions suivantes :
3.1 Quel est le contenu du fichier de description de zone associé au serveur dns2.tsig.gberger.fr ?
3.2 Comment faire pour déclarer un nouveau serveur de noms pour la zone tscg.gberger.fr, de nom dns2 et d'adresse 10.0.2.13 ?
3.3 Comment faire pour que arle.tsig.gberger.fr devienne une zone indépendante ?

Annexe 1
Rappels de quelques définitions

Le rôle d'un serveur de noms de domaines est avant tout de permettre de "résoudre un nom", c'est-à-dire d'associer une adresse IP à un nom d'hôte.
L'espace des noms de domaines est découpé en **zones**. Ces découpes peuvent être réalisées entre deux nœuds adjacents quelconques. Chaque groupe de nœuds interconnectés devient ainsi une zone indépendante.
Du fait de la structure d'arbre (dans lequel chaque branche correspond à un domaine), chaque zone contient un nœud "de plus haut niveau" qui est plus proche de la racine que tous les autres nœuds de cette zone. Le nom de ce nœud est utilisé pour identifier la zone elle-même.
Chaque zone est gérée par une organisation, qui peut modifier ses données de façon unilatérale, créer des nouveaux sous-arbres à l'intérieur de la zone, supprimer des nœuds existants, ou encore déléguer la gestion de sous-zones à d'autres organisations plus locales.
Une zone contient donc un ensemble d'hôtes (noeuds). Les données décrivant une zone se divisent en quatre parties majeures :

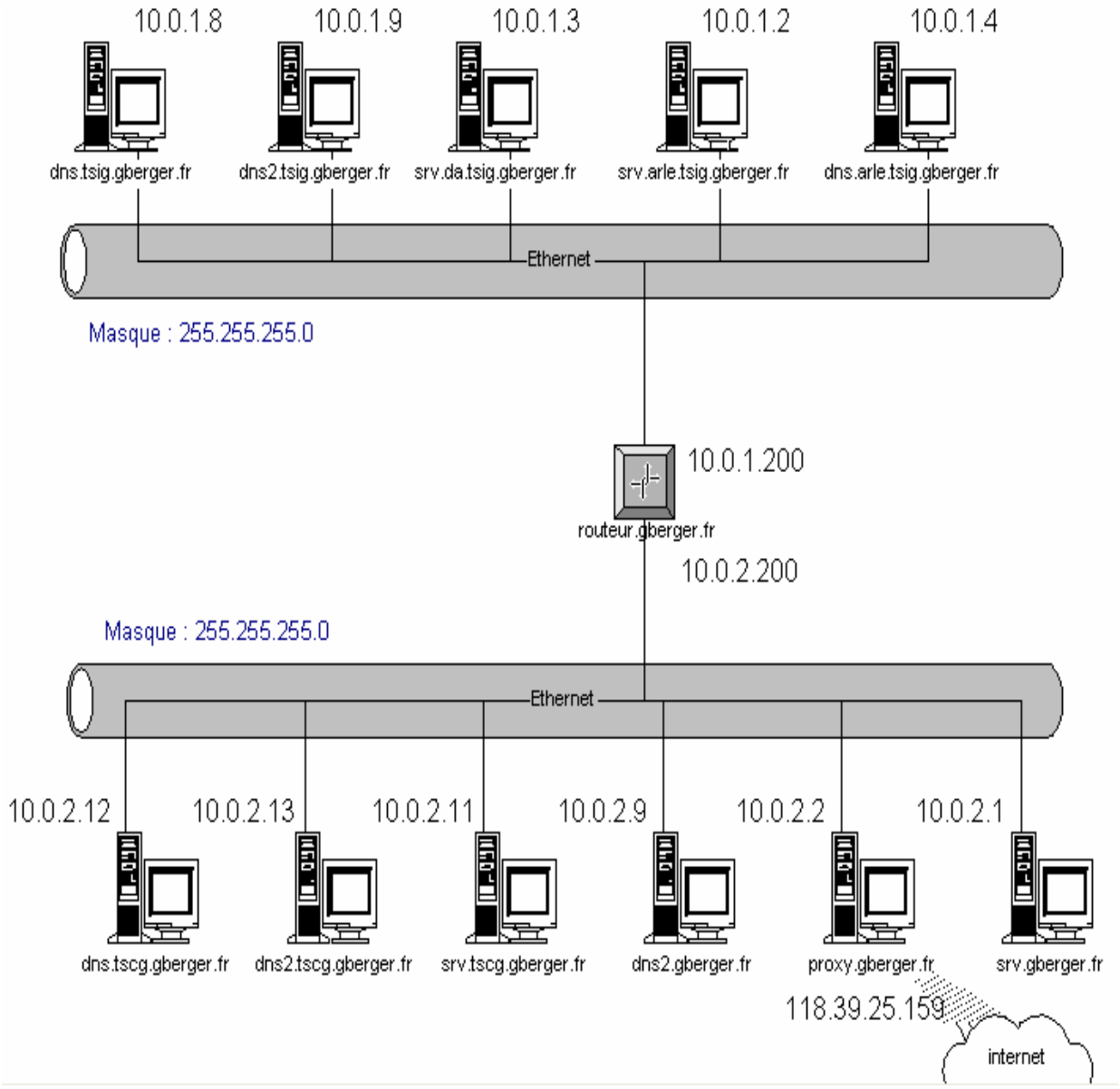
- Les données sur lesquelles le serveur fait autorité (pour tous les nœuds dans la zone).
- Des données définissant le nœud de plus haut niveau de la zone (qui fait partie des données sur lesquelles le serveur fait autorité).
- Des données décrivant les sous-zones déléguées, c'est-à-dire, les points de coupure dans les parties inférieures de la zone.
- Les données permettant l'accès aux serveurs de noms traitant les sous-zones déléguées (appelées souvent "glue data").

Toutes ces données sont exprimées dans un fichier sur le serveur primaire de la zone, sous forme d'enregistrements de ressources (en anglais Ressource Record : RR.)
Les principaux types d'enregistrements sont repérés par un code. On rencontre le plus souvent :
SOA (Start Of Authority) : identifie le début d'une "sphère d'autorité" (description d'une zone)
A (Address) : décrit une adresse d'hôte
NS (Name Server) : définit un serveur de noms faisant autorité sur la zone

Un serveur primaire d'une zone dispose du fichier de configuration de cette zone. Il fait référence sur cette zone.
Un serveur secondaire travaille sur une copie locale du fichier de configuration d'un serveur primaire, serveur qu'il contacte régulièrement pour mettre à jour les données qu'il possède sur la zone.
Chaque serveur dispose également d'un **cache** qui contient d'autres références (sur lesquelles il ne fait pas autorité) obtenues au cours des différentes opérations de résolutions de noms. Pour simplifier, on considérera que sa structure correspond à un ensemble de RR de type A.
Un serveur de cache ne travaille qu'avec un cache local qui contient les résultats des précédentes résolutions de noms. Cela évite une mise à jour périodique à partir du serveur primaire (moins de trafic réseau), mais peut entraîner beaucoup de trafic sur le réseau, notamment au départ, lorsque le cache est vide, et des erreurs, lorsque la durée de validité des informations est trop longue.

Annexe 2
Plan d'adressage du réseau gberger.fr

Remarque : Seules les machines nécessaires à cet exercice sont visualisées sur ce document

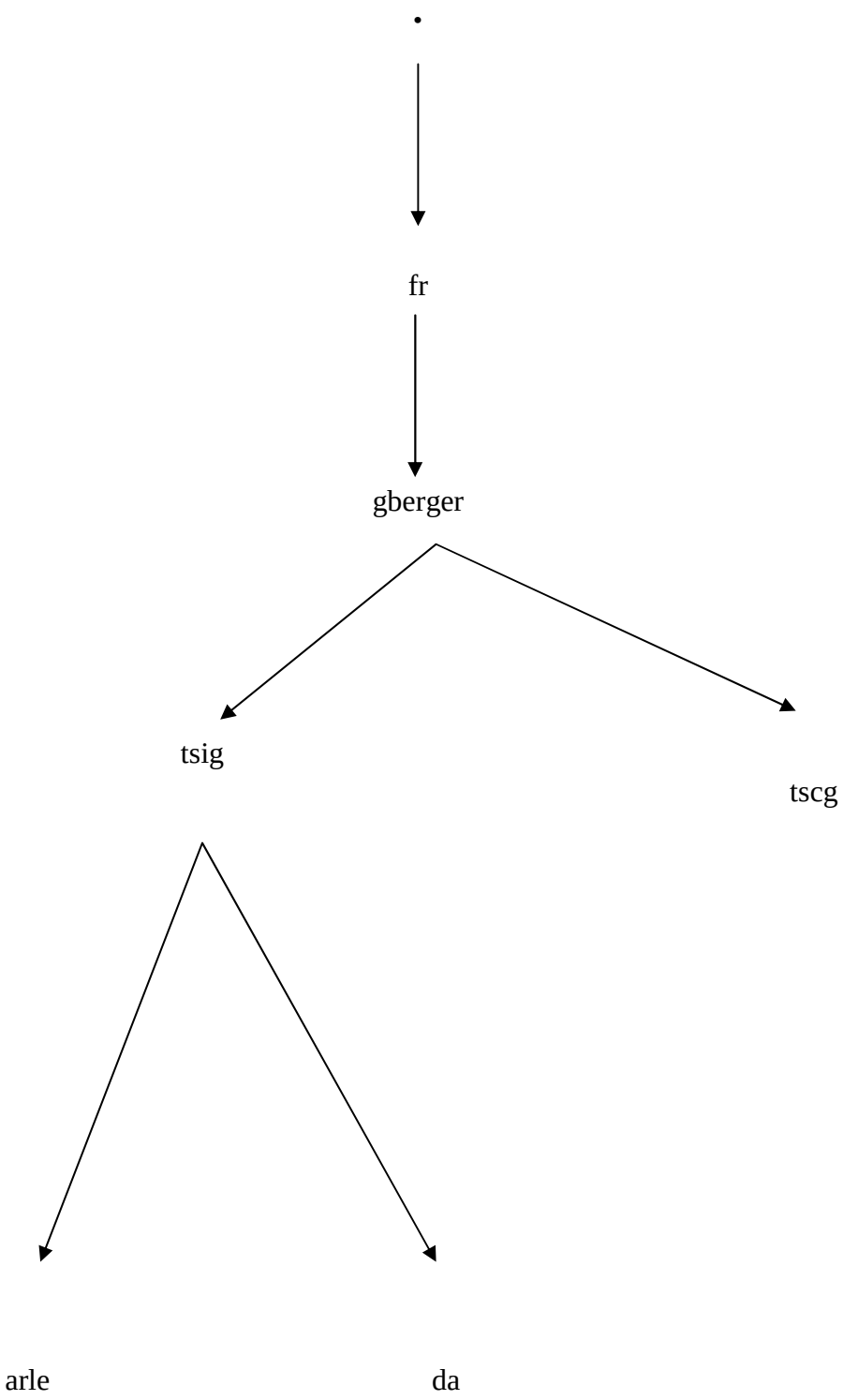


Le serveur proxy fait office de passerelle vers le Fournisseur d'Accès à Internet qui a fourni deux adresses de DNS : 118.39.5.53 et 118.39.17.26.

Les hôtes du réseau 10.0.2.0/24 ont pour passerelle par défaut 10.0.2.200.

Les hôtes du réseau 10.0.1.0/24 ont pour passerelle par défaut 10.0.1.200.

Annexe 3
Arbre de la zone gberger.fr



Annexe 4
Description de la zone gberger.fr

Configuration des postes

Chaque poste du réseau 10.0.1.0/24 dispose de la liste des serveurs DNS par défaut :
10.0.1.8
10.0.2.9

Chaque poste du réseau 10.0.2.0/24 dispose de la liste des serveurs DNS par défaut :
10.0.2.9
10.0.1.8

Contenu du fichier de configuration de la zone gberger.fr

```
; définition de la zone gberger.fr
; le serveur d'autorité est dns.tsig.gberger.fr (serveur primaire)
; il est administré par une personne qu'on peut joindre à l'adresse admgb@gberger.fr

gberger.fr.  IN      SOA    dns.tsig.gberger.fr.  admgb.gberger.fr. (
        3       ; numéro de version : permet aux serveurs secondaires de savoir s'ils doivent mettre à jour leur
                ; base
        36000   ; délai de mise à jour imposé aux serveurs secondaires (en secondes)
        3600    ; délai avant une autre tentative de mise à jour par un serveur secondaire (en secondes)
        360000      ; durée au-delà de laquelle les données de zones seront marquées comme obsolètes par un
                ;serveur
                ; secondaire (en secondes)
        86400); durée de validité en cache par défaut des enregistrements de zones (en secondes)

; avec deux serveurs de noms dans cette zone

                NS  dns.tsig.gberger.fr.
                NS  dns2.gberger.fr.

; et délégation de la zone tsig.gberger.fr avec trois serveurs de noms

tsig.gberger.fr.  IN    NS  dns.arle.tsig.gberger.fr.
                NS  dns2.tsig.gberger.fr
                NS  dns2.gberger.fr.

; et délégation de la zone tscg.gberger.fr avec deux serveurs de noms

tscg.gberger.fr.  IN    NS  dns.tscg.gberger.fr.
                NS  dns2.gberger.fr.
```

; déclaration des adresses faisant autorité

```
localhost.gberger.fr.       IN    A     127.0.0.1
dns2.gberger.fr.                  IN    A     10.0.2.9
proxy.gberger.fr.                 IN    A     10.0.2.2
routeur.gberger.fr          IN    A     10.0.2.200
routeur.gberger.fr          IN    A     10.0.1.200
```

; fin de la zone d'autorité
; glue data

```
dns.tsig.gberger.fr.        IN    A     10.0.1.8
dns.arle.tsig.gberger.fr          IN    A     10.0.1.4
dns.tscg.gberger.fr         IN    A     10.0.2.12
dns2.tsig.gberger.fr        IN    A     10.0.1.9
```

Contenu du fichier de configuration de la zone tsig.gberger.fr

```
tsig.gberger.fr. IN SOA dns.arle.tsig.gberger.fr. admig.gberger.fr. (19 18000 3600 72000 86400)
                    NS  dns.arle.tsig.gberger.fr.
                    NS  dns2.tsig.gberger.fr.
                    NS  dns2.gberger.fr.

localhost.tsig.gberger.fr.        IN    A     127.0.0.1
dns.arle.tsig.gberger.fr.         IN    A     10.0.1.4
dns2.tsig.gberger.fr.       IN    A     10.0.1.9
srv.arle.tsig.gberger.fr.         IN    A     10.0.1.2
srv.da.tsig.gberger.fr.     IN    A     10.0.1.3
```

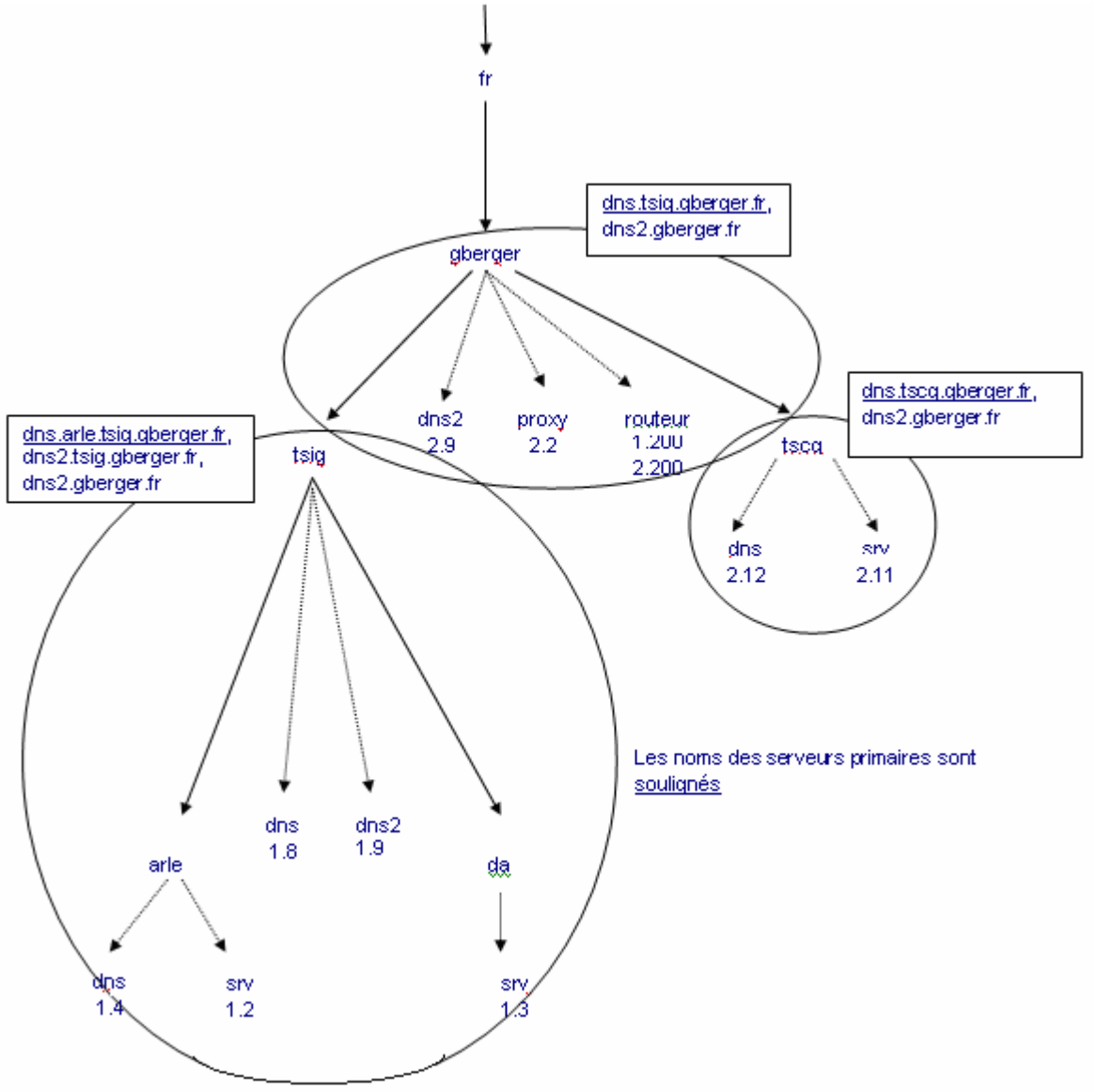
Contenu du fichier de configuration de la zone tscg.gberger.fr

```
tscg.gberger.fr. IN SOA dns.tscg.gberger.fr. admcg.gberger.fr. (13 54000 3600 108000 86400)
                    NS  dns.tscg.gberger.fr.
                    NS  dns2.gberger.fr.

localhost.tscg.gberger.fr.  IN    A     127.0.0.1
dns.tscg.gberger.fr.        IN    A     10.0.2.12
dns2.gberger.fr.                  IN    A     10.0.2.9
srv.tscg.gberger.fr.        IN    A     10.0.2.11
```

Corrigé Exonet N° 13

Question 1. Compléter l'annexe 3 afin de positionner chaque machine référencée dans son domaine (associée à son adresse IP) à partir de l'analyse du fichier de configuration des zones gberger.fr, tsig.gberger.fr et tscg.gberger.fr (annexe 4). Faire apparaître pour chaque zone la liste des serveurs DNS.
Indiquer les hôtes du réseau gberger.fr qui ne sont pas encore référencés.



les hôtes du réseau **gberger.fr** qui ne sont pas encore référencés sont :
srv.gberger.fr (adresse 10.0.2.1)
dns2.tscg.gberger.fr (adresse 10.0.2.13)

Question 2.1. Sur quelle machine est stocké le fichier de configuration de la zone tsig.gberger.fr ?

Sur **dns.arle.tsig.gberger.fr** (ligne SOA dans le fichier de configuration)

Question 2.2. Quelle est la durée de validité de ses données en cache (exprimée en jours) ?

86400 secondes, soit une journée (ligne SOA)

Question 2.3. Quelle est l'adresse et le nom du serveur secondaire de la zone tscg.gberger.fr ?

10.0.2.9, dns2.gberger.fr (deuxième ligne NS du fichier de configuration de **tscg.gberger.fr** : la première ligne correspond au serveur primaire (apparaissant dans la ligne SOA de la zone **tscg.gberger.fr**)

Question 2.4. Parmi ces deux zones (tsig.gberger.fr et tscg.gberger.fr), quelle est la zone qui a été le plus souvent modifiée ?

C'est la zone **tsig.gberger.fr** qui en est à la 19ème version (ligne SOA)

Question 2.5. arle.tsig.gberger.fr est elle une zone indépendante ?

non, car il n'y a pas de délégation de zone prévue , ni **dans gberger.fr,** ni dans **tsig.gberger.fr**

Question 2.6. Que faut il faire pour que la résolution de nom pour la machine srv.gberger.fr, d'adresse 10.0.2.1 soit possible ?

Il faut ajouter une ligne de type A dans le fichier de configuration de **gberger.fr** :

srv.gberger.fr. IN A 10.0.2.1

Question 3.1. Quel est le contenu du fichier de description de zone associé au serveur dns2.tsig.gberger.fr ?

Il contient la description de la zone **tsig.gberger.fr** pour lequel il est serveur secondaire.

Question 3.2. Comment faire pour déclarer un nouveau serveur de noms pour la zone tscg.gberger.fr, de nom dns2 et d'adresse 10.0.2.13 ?

Il faut ajouter une ligne NS dans le fichier de configuration de la zone gberger.fr (dans la partie correspondant à la délégation de cette zone : le nom de la zone peut être omis s'il est ajouté à la suite des deux lignes NS actuelles

tscg.gberger.fr. IN NS dns2.tscg.gberger.fr.

et une ligne A dans la zone des "glue data"

dns2.tscg.gberger.fr. IN A 10.0.2.13

ce qui donne le résultat suivant :

```
; et délégation de la zone tscg.gberger.fr avec trois serveurs de noms
tscg.gberger.fr.  IN    NS   dns.tscg.gberger.fr.
                        NS   dns2.gberger.fr.
                        NS   dns2.tscg.gberger.fr.

; déclaration des adresses sur lesquelles les serveurs font autorité

localhost.gberger.fr.          IN    A     127.0.0.1
dns.tsig.gberger.fr.           IN    A     10.0.1.8
dns2.gberger.fr.                     IN    A     10.0.2.9
proxy.gberger.fr.                    IN    A     10.0.2.2
routeur.gberger.fr.            IN    A     10.0.2.200
routeur.gberger.fr.            IN    A     10.0.1.200

; fin de la zone d'autorité
; glue data

dns.arle.tsig.gberger.fr.            IN    A     10.0.1.4
dns.tscg.gberger.fr.           IN    A     10.0.2.12
dns2.tsig.gberger.fr.          IN    A     10.0.1.9
dns2.tscg.gberger.fr.          IN    A     10.0.2.13
```

Question 3.3. Comment faire pour que arle.tsig.gberger.fr devienne une zone indépendante ?

Il faut créer une délégation de zone dans le fichier de configuration de tsig.gberger.fr, en déclarant au moins un serveur primaire et un serveur secondaire (pour améliorer la sécurité - tolérance aux pannes – et les performances – répartition des charges -) :

```
; délégation de la zone arle.tsig.gberger.fr
arle.tsig.gberger.fr    NS      dns.arle.tsig.gberger.fr
                        NS      dns2.tsig.gberger.fr
```

La ligne SOA permettra de déterminer le serveur primaire.

Les adresses étant déjà disponibles dans la zone autorisée, il n'est pas nécessaire d'ajouter de lignes d'adresse. Il faut enlever la ligne correspondant au serveur **srv.arle.tsig.gberger.fr**.

Contenu du fichier de configuration de la zone tsig.gberger.fr

```
tsig.gberger.fr.   IN  SOA dns.arle.tsig.gberger.fr.  admig.gberger.fr. (19 18000 3600 72000
86400)
                        NS  dns.arle.tsig.gberger.fr.
                        NS  dns2.tsig.gberger.fr.
                        NS  dns2.gberger.fr.

; délégation de la zone arle.tsig.gberger.fr avec deux serveurs

arle.tsig.gberger.fr.  NS     dns.arle.tsig.gberger.fr.
                       NS     dns2.tsig.gberger.fr.

localhost.tsig.gberger.fr.          IN    A     127.0.0.1
dns2.tsig.gberger.fr.       IN      A     10.0.1.9          ; adresse deuxième
serveur
srv.da.tsig.gberger.fr.     IN      A     10.0.1.3
~~srv.arle.tsig.gberger.fr.          IN    A     10.0.1.2~~          ; ligne à
supprimer

; "glue data"

dns.arle.tsig.gberger.fr.           IN    A     10.0.1.4    ; adresse premier
serveur
```

Il faut ensuite créer le nouveau fichier de configuration qui sera implanté sur le serveur primaire de la zone (**dns.arle.tsig.gberger.fr**)

Contenu du fichier de configuration de la zone arle.tsig.gberger.fr

```
arle.tsig.gberger.fr.   IN SOA dns.arle.tsig.gberger.fr. admarle.gberger.fr. (1 18000 3600
72000  86400)
                        NS  dns.arle.tsig.gberger.fr.
                        NS  dns2.tsig.gberger.fr.

localhost.arle.tsig.gberger.fr. IN      A     127.0.0.1
dns.arle.tsig.gberger.fr.           IN    A     10.0.1.4
dns2.tsig.gberger.fr.       IN      A     10.0.1.9
srv.arle.tsig.gberger.fr.           IN    A     10.0.1.2
```

EXONET N° 14

Une entreprise dispose d'un réseau Ethernet supportant le protocole TCP/IP et regroupant actuellement 66 hôtes (stations, serveurs, routeurs, passerelles,…). Vous êtes chargé(e) de proposer un plan détaillé pour automatiser l'attribution des configurations TCP/IP aux hôtes en respectant le cahier des charges rédigé par l'administrateur du réseau.

Cahier des charges

A. Données

- L'adresse du réseau est 193.250.17.0.
- L'entreprise est structurée en trois départements : Administratif, Commercial et Production.

Ces trois départements comportent respectivement 24, 16 et 18 hôtes ayant le rôle de postes de travail.

B. Contraintes

1. Chaque département doit être placé dans un sous-réseau IP distinct. On écarte les réseaux ayant une adresse "tout à zéro" ou "tout à un"
2. Les hôtes doivent pouvoir obtenir automatiquement leur configuration IP en en faisant la demande auprès d'un serveur DHCP.
3. Plusieurs serveurs offriront le service DHCP sur le réseau, l'indisponibilité de l'un d'entre eux ne doit pas totalement interrompre l'attribution des configurations TCP/IP aux hôtes qui en font la demande. On retient comme hypothèse que la panne d'un seul serveur DHCP sera assumée. Si un sous-réseau est privé de son serveur DHCP suite à une panne, 25% de ses hôtes doivent pouvoir obtenir une adresse IP valide auprès du serveur DHCP d'un autre sous-réseau.
4. La configuration des serveurs DHCP doit permettre l'ajout de nouveaux hôtes dans chaque sous-réseau.
5. Certains hôtes ayant un rôle de serveur doivent se voir attribuer des adresses IP toujours identiques. Les serveurs DHCP se voient attribuer l'adresse IP de numéro le plus haut utilisable dans chaque sous-réseau. Les serveurs et routeurs devront disposer d'adresses situées dans la partie haute de la plage d'adresses du sous-réseau. Les postes de travail se voient attribuer des adresses situées dans la partie basse de la plage d'adresses du sous-réseau

Liste des hôtes auxquels une adresse fixe doit être attribuée	
Hôte	Adresse MAC de l'hôte
Sous-réseau Administratif	
Serveur DNS	00-32-DE-5A-78-9C
Passerelle par défaut	1F-7A-90-02-F0-F0
Sous-réseau Commercial	
Passerelle par défaut	2B-14-62-91-C9-B1
Routeur	82-00-06-01-9B-7A
Sous-réseau Production	
Passerelle par défaut	1C-96-AA-F4-C2-91

6. Trois hôtes du département administratif ne sont pas clients DHCP.
7. Certains hôtes du domaine Production utilisés sur les chaînes de montage ne sont pas gérés par le service informatique. Une plage d'adresses leur a été réservée, elle recouvre les adresses 193.250.17.110 à 193.250.17.117.

1. Proposer un masque de sous-réseau pour le réseau de l'entreprise.
2. Calculer le nombre total d'hôtes que peut contenir chaque sous-réseau.
3. Affecter un numéro de sous-réseau à chaque département. Définir les plages d'adresses utilisables dans chaque sous-réseau.
4. Tracer un schéma du réseau de l'entreprise en faisant apparaître les hôtes du réseau et leur adresse IP.
5. Définir comment sera assurée l'attribution des configurations IP suite à une panne sur un des serveurs DHCP. Argumenter notamment sur la durée des baux. Noter les éventuelles contradictions vis à vis du cahier des charges.
6. Définir la configuration des serveurs DHCP pour chaque sous-réseau : étendue, durée du bail, options DHCP (passerelle par défaut, adresse de serveur DNS), adresses à exclure, réservations à prévoir. (voir annexe)

Annexe : Fiche de CONFIGURATION DHCP

CONFIGURATION DHCP DU DEPARTEMENT _____					
Étendue du sous-réseau IP : _____		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début					
Adresse fin					
Masque					
Durée du bail					
Options DHCP					
Nom	Valeur				
IP Fixes à attribuer					
Nom	Valeur				
Étendue de secours du sous-réseau IP : _____		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début					
Adresse fin					
Masque					
Durée du bail					
Options DHCP					
Nom	Valeur				

Corrigé Exonet N° 14

Question 1. Proposer un masque de sous-réseau pour le réseau de l'entreprise.

193.250.17.0 est une adresse de classe C, le dernier octet doit servir à coder les numéros de sous-réseau et les numéros d'hôtes dans chaque sous-réseau.
Pour coder trois numéros de sous-réseaux, sachant que les configurations "tout à zéro" et "tout à un" sont réservées, il est nécessaire d'utiliser 3 bits, d'où le masque de sous-réseau $(1110\ 0000)_2$ soit $(224)_{10}$.
Finalement le masque de sous-réseau complet est : 255.255.255.224.

Question 2. Calculer le nombre total d'hôtes que peut contenir chaque sous réseau.

Il reste 5 bits dans le dernier octet pour coder les numéros d'hôtes, soit $2^5 = 32$ possibilités auxquelles il faut retirer le numéro de sous-réseau ("tout à zéro") et l'adresse de diffusion dans le sous-réseau ("tout à un"), soit finalement 30 hôtes par sous-réseau.

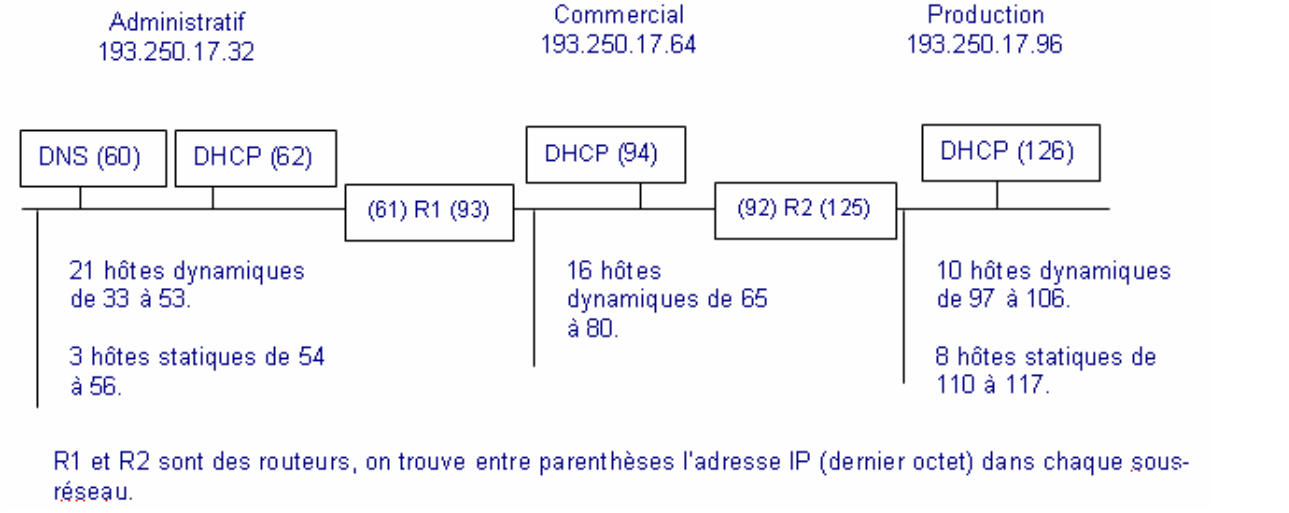
Question 3. Affecter un numéro de sous réseau à chaque département. Définir les plages d'adresses utilisables dans chaque sous réseau.

Le département Production dispose déjà d'un numéro de réseau puisque nous connaissons certaines adresses statiques dans ce sous-réseau :
Prenons l'adresse 193.250.17.110. Le dernier octet est 110 = $(0110\ 1110)_2$, donc le numéro de sous-réseau est $(011)_2$ sur 3 bits, d'où l'adresse de sous-réseau 193.250.17.96 pour le département Production.
Pour les départements Administratif et Commercial nous affectons respectivement les numéros de sous-réseau $(001)_2$ et $(010)_2$. Récapitulons :

Département	**Numéro binaire du sous-réseau**	**Adresse IP du sous-réseau**	**Adresses utilisables de… à … (dernier octet)**
Administratif	$(001)_2$	193.250.17.32	33 à 62
Commercial	$(010)_2$	193.250.17.64	65 à 94
Production	$(011)_2$	193.250.17.96	97 à 126

Question 4. Tracer un schéma du réseau de l'entreprise en faisant apparaître les hôtes du réseau et leur adresse IP.

L'énoncé stipulait : d'utiliser l'adresse la plus haute pour le serveur DHCP, les adresses en dessous pour les hôtes particuliers (serveurs, routeurs) avec souvent une réservation d'adresse et enfin les adresses les plus basses pour les postes de travail.



Question 5. Définir comment sera assurée l'attribution des configurations IP suite à une panne sur un des serveurs DHCP. Argumenter notamment sur la durée des baux. Noter les éventuelles contradictions vis à vis du cahier des charges.

En cas de panne d'un serveur DHCP, les hôtes doivent pouvoir solliciter une configuration auprès d'un autre serveur DHCP situé sur un autre sous-réseau, les requêtes en diffusion envoyées par ces hôtes doivent pouvoir passer les routeurs. Aussi, les routeurs R1 et R2 doivent être capables de router les datagrammes DHCP (BOOTP) ou un agent de relais DHCP doit s'exécuter sur chaque sous-réseau.
Chaque serveur DHCP se voit attribué une deuxième étendue d'adresse dans un autre sous-réseau dont il assure en quelque sorte le remplacement en cas de défaillance. Ces étendues "de sécurité" ne doivent pas entrer en conflit (comporter des adresses identiques) avec les plages d'adresses du serveur DHCP "titulaire" dans son sous-réseau car un risque d'attribution d'une adresse en double existerait.
Voici une proposition d'attribution de ces étendues de sécurité :

Le serveur DHCP du département…	Assure une redondance pour le département…	Nombre d'adresses (25% des hôtes dynamiques)	De… à… (dernier octet)
Administratif	Commercial	4	De 81 à 84
Commercial	Production	4	De 118 à 121
Production	Administratif	5	De 57 à 59 (*)

(*) seules trois adresses sont encore disponibles dans le sous-réseau Administratif, la règle des 25% ne peut être respectée.
Dans une telle configuration (nombre d'adresses très limité) la durée des baux sera plutôt longue de façon à limiter le nombre d'hôtes susceptibles de demander une nouvelle configuration à un moment donné. La durée peut être fixée à 24 heures de façon à laisser le temps de remettre en service le serveur DHCP. À l'inverse la durée de bail des étendues de secours sera plutôt brève de façon à minimiser le recours aux serveurs de secours.

Question 6. Définir la configuration des serveurs DHCP pour chaque sous réseau : étendue, durée du bail, options DHCP (passerelle par défaut, adresse de serveur DNS), adresses à exclure, réservations à prévoir. (voir annexe)

CONFIGURATION DHCP DU DEPARTEMENT Administratif					
Étendue du sous-réseau IP : 193.250.17.32		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.33	193.250.17.54	3 hôtes statiques	0032de5a789c	193.250.17.60
Adresse fin	193.250.17.61	193.250.17.56		1f7a9002f0f0	193.250.17.61
Masque	255.255.255.224	193.250.17.57	Étendue de secours		
Durée du bail	1 jour	193.250.17.59			
Options DHCP					
Nom	Valeur				
Serveur DNS	193.250.17.60				
Passerelle	193.250.17.61				
IP Fixes					
Serveur DHCP	193.250.17.62				
Hôtes statiques	193.250.17.54 … 56				
Étendue de secours du sous-réseau		Adresses exclues		Réservations	

IP : 193.250.17.64		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.81				
Adresse fin	193.250.17.84				
Masque	255.255.255.224				
Durée du bail	30 mn				
Options DHCP					
Nom	Valeur				
Passerelle	193.250.17.125				

Le tableau ci-dessus stipule des plages d'adresses d'exlusion. Cette fonctionnalité n'existe pas sur tous les systèmes et dans ce cas il serait nécessaire de faire plusieurs plages d'adresses pour un même sous-réseau. Ainsi sous linux on aurait l'équivalent des exclusions de windows sous la forme :

subnet 193.250.17.32 netmask 255.255.255. 224 {
range 193.250.17.33 192.168.0.53;
range 193.250.17.60 192.168.0.61; }

Dans la réalité l'administrateur s'arrangerait pour que sa planification n'oblige pas à de telles complications, il définirait une plage qui dès le départ n'intégrerait pas les adresses des hôtes statiques

CONFIGURATION DHCP DU DEPARTEMENT Commercial					
Étendue du sous-réseau IP : 193.250.17.64		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.65	193.250.17.81	Étendue de secours	2b146291c9b1	193.250.17.93
Adresse fin	193.250.17.93	193.250.17.84		820006019b7a	193.250.17.92
Masque	255.255.255.224				
Durée du bail	1 jour				
Options DHCP					
Nom	Valeur				
Passerelle	193.250.17.93				
IP Fixes					
Serveur DHCP	193.250.17.94				
Étendue de secours du sous-réseau IP : 193.250.17.96		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.118				
Adresse fin	193.250.17.121				
Masque	255.255.255.224				
Durée du bail	30 min				
Options DHCP					
Nom	Valeur				
Passerelle	193.250.17.125				

CONFIGURATION DHCP DU DEPARTEMENT Production					
Étendue du sous-réseau IP : 193.250.17.96		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.97	193.250.17.110	8 hôtes statiques	1c96aaf4c291	193.250.17.125
Adresse fin	193.250.17.125	193.250.17.117			
Masque	255.255.255.224	193.250.17.118	Étendue de secours		
Durée du bail	1 jour	193.250.17.121			
Options DHCP					
Nom	Valeur				
Passerelle	193.250.17.125				
IP Fixes					
Serveur DHCP	193.250.17.126				
Étendue de secours du sous-réseau IP : 193.250.17.32		Adresses exclues		Réservations	
		Plage De… A…	Commentaire	Adresse MAC	Adresse IP
Adresse début	193.250.17.57				
Adresse fin	193.250.17.59				
Masque	255.255.255.224				
Durée du bail	30 min				
Options DHCP					
Nom	Valeur				
Serveur DNS	193.250.17.60				
Passerelle	193.250.17.61				

EXONET N° 15

LaPointe SA est une entreprise de grande taille intervenant dans le secteur du Bâtiment et des Travaux Publics (BTP). Son siège social est localisé à Marseille.
Récemment elle a fusionné avec EuroBTP, une des premières entreprises européennes dans ce secteur d'activité. Pour être en conformité avec les méthodes d'EuroBTP, LaPointe SA est amenée à restructurer son réseau informatique et à modifier certaines pratiques de gestion.
Ainsi, tous les postes de travail et les serveurs de LaPointe SA doivent être raccordés directement à Internet. La société a obtenu la plage d'adresses IP 195.10.228.0/24 pour l'ensemble des machines du siège et des agences de LaPointe SA.
Vous êtes chargé(e) de participer à la refonte du réseau.

Le Directeur Financier rencontre un problème avec le nouvel ordinateur que vous lui avez installé la semaine dernière et qui est connecté au réseau de façon intermittente. Il a noté les messages qui sont apparus lors de ses deux dernières tentatives de connexion :
« Le système a détecté un conflit entre l'adresse IP 195.10.228.116 et l'adresse matérielle 00 :13 :B8 :3C :F7 :B2 »
« Le système a détecté un conflit entre l'adresse IP 195.10.228.116 et l'adresse matérielle 00 :13 :B8 :3C :F4 :D5 »
Son adresse IP fixe est 195.10.228.116/25 (soit un masque de 255.255.255.128).

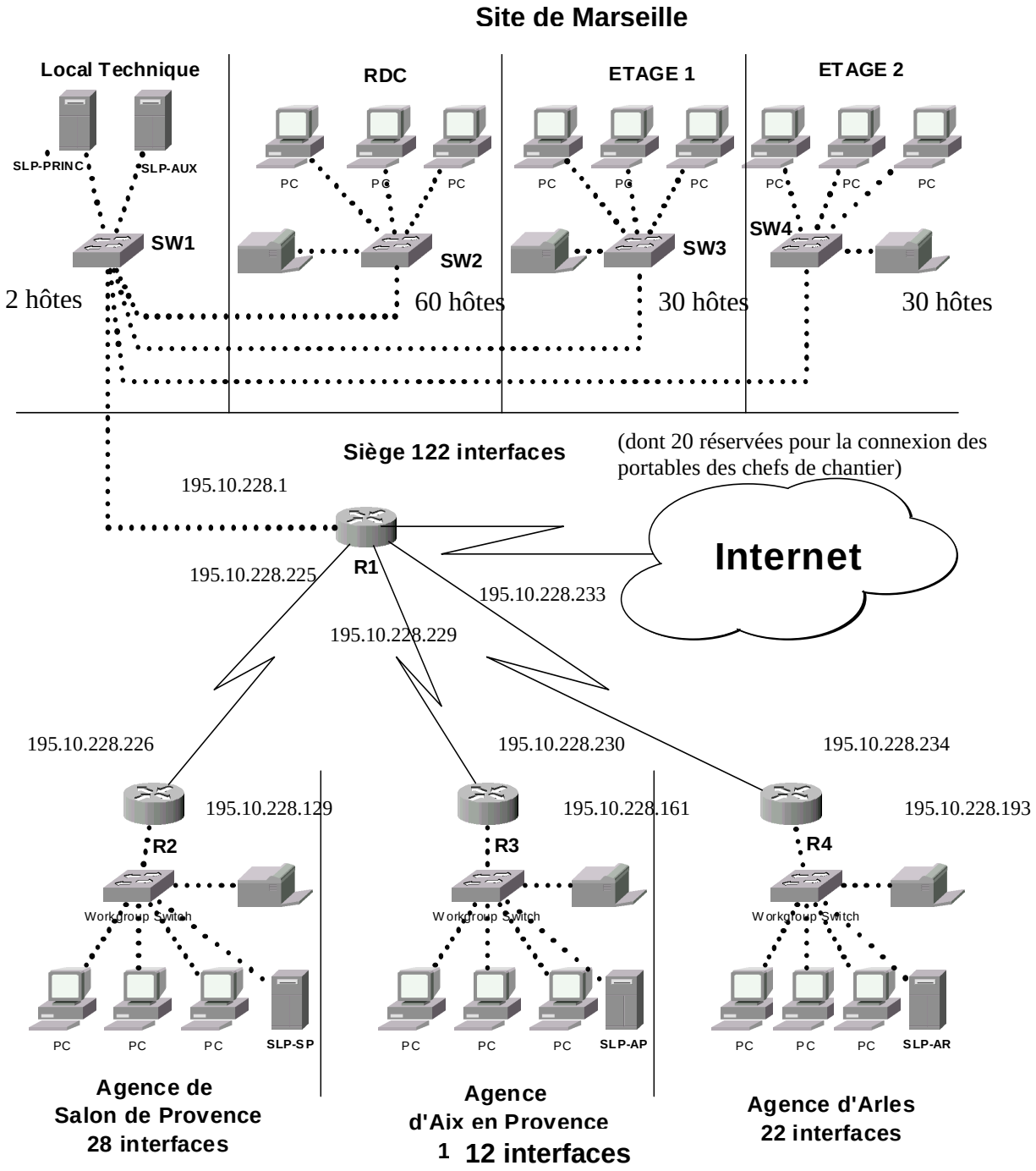
Votre responsable vous demande de résoudre ce problème, en vous appuyant sur les annexes 1 et 2.
1. Expliquer la cause du dysfonctionnement.
2. Proposer une solution pour éliminer ce dysfonctionnement.

En utilisant les annexes 1 et 2 vous êtes chargé(e) d'analyser le plan d'adressage de la société.
3. Vérifier que le plan d'adressage permet de prendre en charge le nombre d'interfaces nécessaire pour chaque site.

Vous êtes également chargé(e) de tester la configuration actuelle des routeurs R1, R2 et R3. Le routeur R4 a déjà été configuré et testé.
Deux commandes ont été lancées avec succès :
Commande 1 : À partir du poste d'adresse 195.10.228.15 : **ping 195.10.228.135**
Commande 2 : À partir du poste d'adresse 195.10.228.15 : **ping 195.10.228.164**
Une commande n'a pas abouti :
Commande 3 : À partir du poste d'adresse 195.10.228.135 : **ping 195.10.228.164**
4. Lister les équipements traversés lors de l'exécution de la commande 3, ainsi que les lignes des tables de routage utilisées et expliquer la raison de l'échec de cette commande.
5. Proposer la correction à apporter pour que la commande 3 fonctionne correctement.
6. Donner le contenu de la table de routage de R4.

Le service informatique a conçu une architecture DNS pour l'entreprise, le principe de cette architecture est fourni en **annexe 3**.
7. En justifiant votre réponse, donner l'adresse IP du serveur DNS sur lequel doit être défini le nom d'hôte www.marseille.lapointe.fr
8. Donner les paramètres de la configuration DNS des postes de travail du site d'Aix qui permettent d'accéder à l'ensemble des serveurs de l'entreprise en utilisant leur nom.
9. Indiquer quel est le rôle et l'intérêt des serveurs secondaires de la zone lapointe.fr

Annexe 1 : Architecture du réseau de LaPointe SA



R1, R2, R3 et R4 sont des routeurs qui relient les sites. SWn identifie les commutateurs (switch) installés dans les locaux de sous-répartition de chaque étage du site de Marseille, et dans le local technique (il n'y a pas plus de quinze mètres entre les locaux les plus éloignés).

Il s'agit de commutateurs 12 ou 24 ports 10/100 Mbps empilables avec un emplacement accueillant actuellement un adaptateur (transceiver) optionnel 10BASE 5, et qui disposent par ailleurs d'un emplacement libre permettant d'installer au choix un adaptateur 1000BASE-SX, 1000BASE-LX ou 1000BASE-T.

Annexe 2 : Extraits du plan d'adressage

Site ou liaison	Adresse réseau	Masque de sous-réseau
Marseille	195.10.228.0	255.255.255.128
Salon	195.10.228.128	255.255.255.224
Aix	195.10.228.160	255.255.255.224
Arles	195.10.228.192	255.255.255.224
R1-R2	195.10.228.224	255.255.255.252
R1-R3	195.10.228.228	255.255.255.252
R1-R4	195.10.228.232	255.255.255.252

Le sous-réseau de Marseille dispose de postes en adressage fixe, mais aussi de postes en adressage dynamique (les portables des chefs de chantier qui rapatrient les données enregistrées dans la journée à leur retour des visites de chantier).
Le serveur DHCP de Marseille gère la plage d'adresse suivante :
Plage d'adresses disponibles : 195.10.228.106 – 195.10.228.125

Exemples de configuration des postes dans chaque site

Site	Adresse d'un poste	Masque	Routeur par défaut
Marseille	195.10.228.4	255.255.255.128	195.10.228.1
Salon	195.10.228.135	255.255.255.224	195.10.228.129
Aix	195.10.228.167	255.255.255.224	195.10.228.161
Arles	195.10.228.201	255.255.255.224	195.10.228.193

Table de routage pour R1

Réseau	Masque	Routeur	Interface
195.10.228.0	255.255.255.128	195.10.228.1	195.10.228.1
195.10.228.128	255.255.255.224	195.10.228.226	195.10.228.225
195.10.228.160	255.255.255.224	195.10.228.230	195.10.228.229
195.10.228.192	255.255.255.224	195.10.228.234	195.10.228.233

Table de routage pour R2

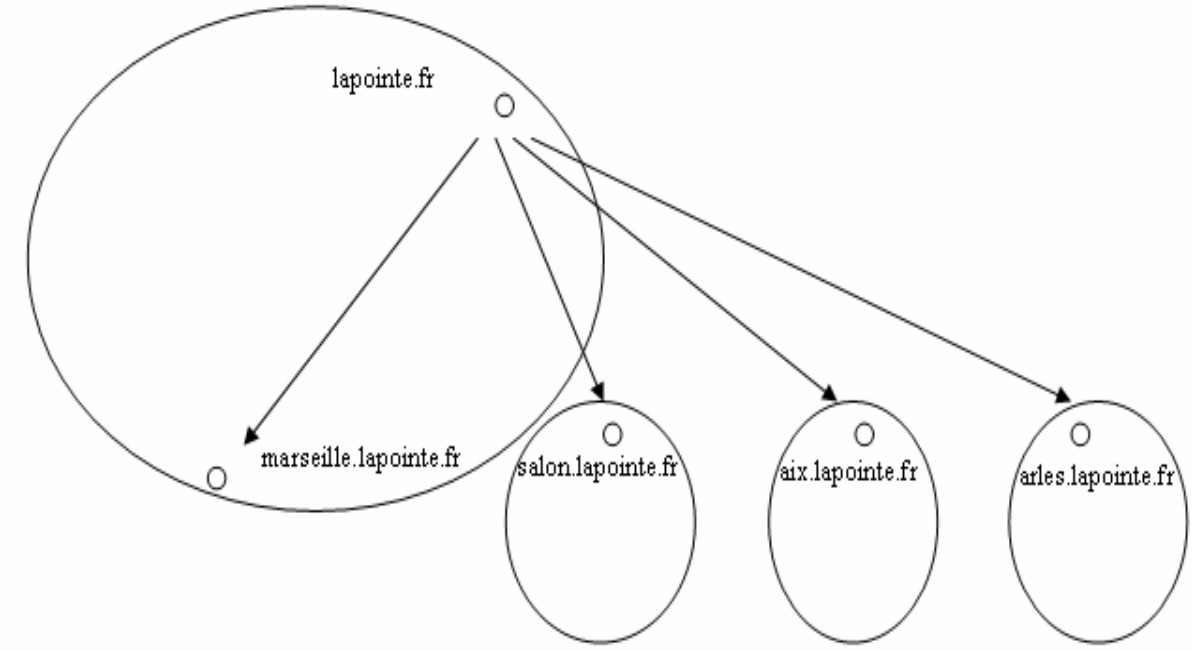
Réseau	Masque	Routeur	Interface
195.10.228.128	255.255.255.224	195.10.228.129	195.10.228.129
195.10.228.0	255.255.255.128	195.10.228.225	195.10.228.226
195.10.228.160	255.255.255.224	195.10.228.225	195.10.228.226
195.10.228.192	255.255.255.224	195.10.228.225	195.10.228.226

Table de routage pour R3

Réseau	Masque	Routeur	Interface
195.10.228.160	255.255.255.224	195.10.228.161	195.10.228.161
195.10.228.0	255.255.255.128	195.10.228.229	195.10.228.230
195.10.228.128	255.255.255.224	195.10.228.233	195.10.228.230
195.10.228.192	255.255.255.224	195.10.228.229	195.10.228.230

Annexe 3 : Architecture DNS du domaine lapointe.fr

Architecture administrative



- L'entreprise dispose du domaine lapointe.fr et chaque site, à l'exception de celui de Marseille, gère son propre sous-domaine.
- Chaque ovale correspond à une zone.

Architecture d'implémentation

Chaque ligne du tableau ci-dessous représente un serveur DNS et indique dans quel site il est implanté, quelle est son adresse IP, pour quelle zone il est serveur DNS primaire et pour quelle(s) zone(s) il est serveur DNS secondaire.

Site	Adresse IP du serveur DNS	Serveur primaire de	Serveur secondaire de
Marseille	195.10.228.2	lapointe.fr	salon.lapointe.fr aix.lapointe.fr arles.lapointe.fr
Salon	195.10.228.130	salon.lapointe.fr	lapointe.fr
Aix	195.10.228.162	aix.lapointe.fr	lapointe.fr
Arles	195.10.228.194	arles.lapointe.fr	lapointe.fr

Corrigé Exonet N° 15

Question 1. Expliquer la cause du dysfonctionnement

On est dans la situation où 2 machines utilisent la même adresse IP dans le même sous-réseau.
Le poste fixe d'adresse 195.10.228.116 entre en conflit avec d'autres machines, par exemple avec un portable connecté dans la plage d'adresse 195.10.228.106 et 195.10.228.125 (deux adresses MAC pour une seule adresse IP).

Question 2. Proposer une solution pour éliminer ce dysfonctionnement

Il faut donc changer l'adresse du poste pour qu'elle sorte de cette plage, sous réserve d'adresses disponibles (par exemple 195.10.228.126).
Il faut que l'adresse IP du poste du directeur soit unique sur le réseau et n'appartienne pas à une plage DHCP.
On peut conserver la plage du DHCP en indiquant simplement l'adresse du poste du directeur financier comme une adresse interdite.

Question 3. Vérifier que le plan d'adressage permet de prendre en charge le nombre d'interfaces nécessaire pour chaque site

Les masques de sous-réseau sont utilisés ici pour répartir les plages d'adresses en fonction des besoins de chaque site :

- Pour le site de Marseille on a besoin de 122 adresses (123 avec le routeur). Le dernier octet commençant par un 1 (255.255.255.128), on dispose donc de 126 adresses d'hôtes.
- Pour le site de Salon on a besoin de 28 adresses. Le dernier octet commençant par un 111 (255.255.255.224), on dispose donc de 30 adresses d'hôtes.
- Pour le site d'Aix on a besoin de 12 adresses. Le dernier octet commençant par un 111 (255.255.255.224), on dispose donc de 30 adresses d'hôtes.
- Pour le site d'Arles on a besoin de 22 adresses. Le dernier octet commençant par un 111 (255.255.255.224), on dispose donc de 30 adresses d'hôtes.

Question 4. Lister les équipements traversés lors de l'exécution de la commande 3, ainsi que les lignes des tables de routage utilisées et expliquer la raison de l'échec de cette commande.

La réussite des deux premières commandes permet de constater que les liaisons entre les sites de Marseille, Salon et Aix fonctionnent correctement.

Liste des équipements traversés et lignes des tables de routage utilisées :

Aller : Switch Salon, R2 (ligne 3), R1 (ligne 3), R3 (ligne 1), Switch Aix
Retour : Switch Aix, R3 (ligne 3)

Explication de la raison de l'échec de la commande :

- Pour la réponse, le poste d'adresse 195.10.228.164 envoie la réponse à la commande ping vers le routeur R3.
- Dans le routeur R3, la troisième ligne entraîne l'envoi de cette réponse sur l'interface 195.10.228.230 vers le routeur d'adresse 195.10.228.233, vers le sous-réseau 195.10.228.192
- L'adresse de ce routeur n'est pas accessible directement à partir de cette interface.

Question 5. Proposer la correction à apporter pour que la commande 3 fonctionne correctement

Il faut modifier la troisième ligne de la table de routage de R3

Table de routage pour R3

Réseau	**Masque**	**Routeur**	**Interface**
195.10.228.160	255.255.255.224	195.10.228.161	195.10.228.161
195.10.228.0	255.255.255.128	195.10.228.229	195.10.228.230
195.10.228.128	255.255.255.224	195.10.228.**229**	195.10.228.230
195.10.228.192	255.255.255.224	195.10.228.229	195.10.228.230

Question 6. Donner le contenu de la table de routage de R4

Réseau	**Masque**	**Routeur**	**Interface**
195.10.228.192	255.255.255.224	195.10.228.193	195.10.228.193
195.10.228.0	255.255.255.128	195.10.228.233	195.10.228.234
195.10.228.128	255.255.255.224	195.10.228.233	195.10.228.234
195.10.228.160	255.255.255.224	195.10.228.233	195.10.228.234

Question 7. En justifiant votre réponse, donner l'adresse IP du serveur DNS sur lequel doit être défini le nom d'hôte www.marseille.lapointe.fr.

Le domaine concerné est marseille.lapointe.fr, qui appartient à la zone lapointe.fr. Un nom d'hôte est enregistré sur le serveur DNS primaire de la zone à laquelle il appartient (cette zone pouvant être ensuite répliquée sur le ou les serveurs DNS secondaires). Le serveur primaire pour la zone lapointe.fr est situé à Marseille et d'après le tableau de l'annexe 3 il a pour adresse IP : 195.10.228.2.

Question 8. Donner les paramètres de la configuration DNS des postes de travail du site d'Aix qui permettent d'accéder à l'ensemble des serveurs de l'entreprise en utilisant leur nom.

Il faut, sur chaque poste de travail, l'adresse IP du serveur DNS d'Aix ou d'un autre serveur DNS .

- Préciser les adresses IP des serveurs à consulter : Aix (195.10.228.162) (serveur DNS d'Aix en priorité pour prendre en charge les résolutions de noms « au plus près ») puis celui de Marseille (195.10.228.2), qui stocke l'ensemble des références pour le domaine lapointe.fr (en tant que primaire de la zone lapointe.fr, et secondaire pour les domaines aix.lapointe.fr et salon.lapointe.fr)
- Donner un nom d'hôte
- Indiquer le nom de domaine par défaut : aix.lapointe.fr (ou lapointe.fr)

Question 9. Indiquer quel est le rôle et l'intérêt des serveurs secondaires de la zone lapointe.fr

Les serveurs secondaires stockent le fichier de configuration du serveur primaire, permettant d'une part une **répartition des charges** (le serveur primaire n'est pas le seul sollicité), d'autre part une **tolérance aux pannes** (la liaison avec le site de Marseille peut être défaillante, sans perturber la résolution de noms en local, quelque soit le site considéré).

EXONET N° 16

Le réseau local de la société Ludo utilise les protocoles TCP/IP (adresse réseau 192.168.1.0, masque 255.255.255.0). Les adresses IP des postes de travail sont attribuées dynamiquement par un serveur DHCP. Les serveurs possèdent des adresses statiques.
Pour prendre en charge les nouveaux serveurs et les routeurs, le FAI attribue à la société Ludo le réseau 179.169.10.96 avec le masque de sous-réseau 255.255.255.240.
Ce réseau doit être découpé en deux sous-réseaux afin de séparer les deux segments suivants :

- le lien entre le routeur d'accès R1 et le routeur R2,
- la partie comprenant le commutateur SW2 et les trois serveurs internet.

Pour pouvoir identifier les deux sous-réseaux, on donne la valeur 255.255.255.248 au masque de sous-réseau.
Sur le schéma du réseau (annexe 1) figurent les adresses IP des serveurs et des routeurs. Le routeur R1 est fourni pré-configuré par le fournisseur d'accès.

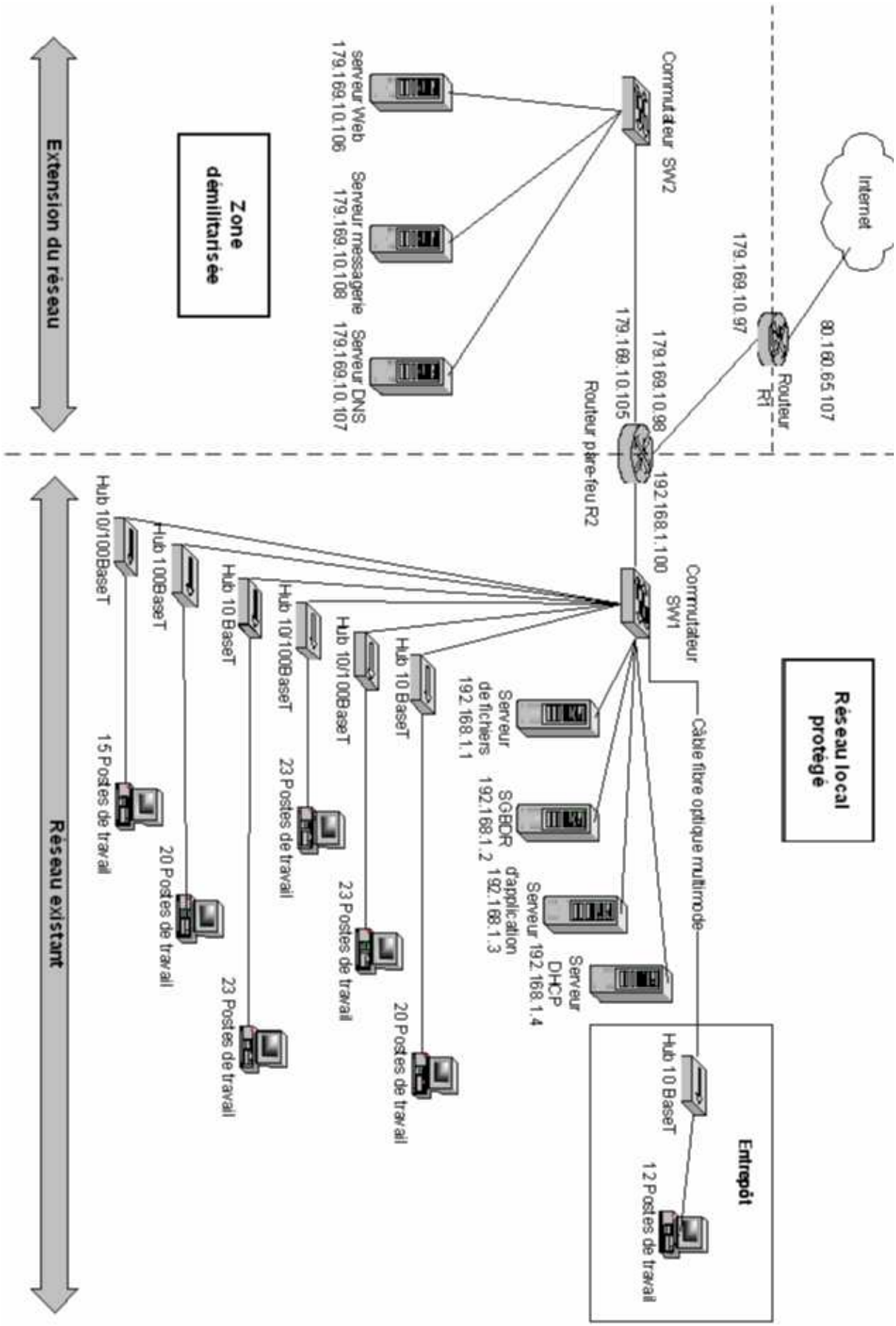
1. Indiquer le nombre d'adresses IP d'hôtes dont on dispose dans chaque sous-réseau avec ce découpage. Justifier la réponse et donner l'adresse IP de chacun des deux sous-réseaux.
2. Écrire la table de routage du routeur R2 en indiquant les valeurs à utiliser pour l'adresse réseau, le masque de sous-réseau, la passerelle et l'interface.
3. Expliquer le mécanisme mis en œuvre sur le routeur R2 pour assurer la correspondance entre les adresses IP utilisées dans le réseau local de l'entreprise et celles utilisées sur internet.
4. Expliquer ce qu'il faut faire pour que la configuration TCP/IP des postes permette à ceux-ci d'accéder à internet.

Le routeur R2 servira également de pare-feu et permettra d'isoler le réseau local de la zone contenant les trois nouveaux serveurs. Cette zone est appelée « zone démilitarisée ».
5. Justifier le choix d'avoir séparé le réseau en deux parties : « Zone démilitarisée » et « Réseau local protégé ».

Le routeur R2 est un routeur filtrant agissant au niveau paquet. Il filtre les paquets entrants et sortants sur toutes ses interfaces réseau en fonction de règles de filtrage définies par l'administrateur du réseau. Un extrait de sa table de filtrage ainsi que l'algorithme qu'il utilise pour la prendre en compte sont présentés en annexe 2.
6. Expliquer le rôle des deux règles de filtrage numéro 1 et numéro 4.

Le contrat de maintenance du site marchand prévoit la mise à jour du site pendant deux ans. Pour permettre au technicien de maintenance d'effectuer des mises à jour à distance sur le serveur Web, vous devez autoriser les connexions par le protocole SSH (Secure Shell) sur ce serveur, ceci uniquement en provenance de l'ordinateur d'adresse 195.65.21.4.
7. Ajouter la règle permettant d'autoriser ces connexions de maintenance en spécifiant sa position dans la table.

Annexe 1 : schéma du réseau



Annexe 2 : Filtrage du pare-feu

Algorithme de filtrage

Pour chaque paquet qui transite en entrée ou en sortie sur une interface du routeur, les règles sont examinées dans l'ordre à partir de la règle n° 1. La première règle dont les paramètres correspondent exactement au paquet reçu ou envoyé est appliquée, après quoi l'analyse des règles s'arrête. Si la fin de la table est atteinte sans qu'aucune règle ne soit applicable, le paquet est refusé.

Table de filtrage

N° règle	Interface	Sens	IP source	Port source	IP destination	Port destination	Action
1	**179. 169.10.98**	**Entrée**	**tous**	**tous**	**179.169.10.106**	**80**	**Autorise**
2	179. 169.10.98	Entrée	tous	tous	179.169.10.106	443	Autorise
3	179. 169.10.98	Entrée	tous	tous	179.169.10.107	53	Autorise
4	**179. 169.10.98**	**Entrée**	**tous**	**53**	**179.169.10.107**	**tous**	**Autorise**
5	179. 169.10.98	Entrée	tous	tous	179.169.10.108	25	Autorise
6	179. 169.10.98	Entrée	tous	25	179.169.10.108	tous	Autorise
7	179. 169.10.98	Entrée	tous	tous	tous	22	Interdit
8	179. 169.10.98	Entrée	tous	tous	tous	23	Interdit

Table de correspondance entre les protocoles d'application et les ports TCP ou UDP

protocole	port utilisé
SMTP	25
HTTP	80
SSL	443
DNS	53
Telnet	23
SSH	22

Corrigé Exonet N° 16

Question 1. Indiquer le nombre d'adresses IP d'hôtes dont on dispose dans chaque sous-réseau avec ce découpage. Justifier la réponse et donner l'adresse IP de chacun des deux sous-réseaux.

Avec le masque 255.255.255.248 appliqué au réseau 179.169.10.96 / 255.255.255.240, on obtient 1 bit pour le sous-réseau (donc deux sous-réseaux), et 3 bits pour l'adresse machine, donc $2^3 = 8$,
soit 8 – 2 = 6 machines dans chaque sous-réseau.
(1 pt par adresse de sous-réseau) Les sous réseaux sont 179.169.10.96 et 179.169.10.104 (masque 255.255.255.248)

Question 2. Écrire la table de routage du routeur R2 en indiquant les valeurs à utiliser pour l'adresse réseau, le masque de sous-réseau, la passerelle et l'interface.

Réseau	**Masque**	**Passerelle**	**Interface**
179.169.10.96	255.255.255.248	179. 169.10.98	179. 169.10.98
179.169.10.104	255.255.255.248	179. 169.10.105	179. 169.10.105
192.168.1.0	255.255.255.0	192.168.1.100	192.168.1.100
0.0.0.0	0.0.0.0	179.169.10.97	179. 169.10.98

Question 3. Expliquer le mécanisme mis en œuvre sur le routeur R2 pour assurer la correspondance entre les adresses IP utilisées dans le réseau local de l'entreprise et celles utilisées sur internet.

Le routeur pare-feu permet la traduction des adresses IP privées du réseau local (non routables sur Internet) en une adresse publique (ici 179.169.10.98, l'adresse IP de l'interface du routeur pare-feu reliée à Internet).
Le mécanisme NAT (Network Address Translation) ou PAT (Port Address Translation) qui utilise le champ « port source » pour faire la correspondance entre les paquets émis et reçus et leur adresse source ou destination dans le réseau local permet la traduction d'adresses de une à plusieurs (une IP publique pour plusieurs IP privées).

Question 4. Expliquer ce qu'il faut faire pour que la configuration TCP/IP des postes leur permettre d'accéder à internet.

On doit ajouter dans la configuration des postes l'adresse de la passerelle par défaut (par une option DHCP ou en « dur ») soit 192.168.1.100

Question 5. Justifier le choix d'avoir séparé le réseau en deux parties : « Zone démilitarisée » et « Réseau local protégé ».

Ces deux zones ne peuvent pas bénéficier du même niveau de sécurité. En effet, la partie « zone démilitarisée » doit être accessible d'Internet pour permettre la connexion des clients au serveur Web, la réception des requêtes de résolution de noms par le serveur DNS, la réception du courrier par le serveur POP. Par contre aucun utilisateur extérieur ne doit pouvoir accéder au réseau local.

Question 6. Expliquer le rôle des deux règles de filtrage numéro 1 et numéro 4.

a. Règle N° 1 : elle autorise les connexions des clients internet (IP source non spécifiée) au site Web (serveur 179.169.10.106) par le protocole http (port 80)
b. Règle N°4 : elle autorise l'entrée des réponses aux requêtes DNS (port source 53) à destination du serveur DNS (serveur 179.169.10.107) venant de n'importe quel serveur internet (IP source non spécifiée).

Question 7. Ajouter la règle permettant d'autoriser ces connexions de maintenance en spécifiant sa position dans la table.

La règle suivante doit être ajoutée dans la table avant la règle n° 7 :
ligne à insérer :

Interface	Sens	IP source	Port source	IP destination	Port destination	Action
179.169.10.98	Entrée	195.65.21.4	tous	179.10.169.106	22	Autorise

EXONET N° 17

L'entreprise DUGALDE édite des ouvrages spécialisés d'artisanat et d'art.
Ouverte au marché mondial depuis 1998, elle assure la traduction et l'impression d'ouvrages en langues étrangères : un service TRADUCTION a d'ailleurs été constitué à cet effet.
Devant gérer notamment les droits d'auteur et de reproduction d'images pour des œuvres et des auteurs originaires des cinq continents, elle a dû se doter d'un service JURIDIQUE conséquent.
Aujourd'hui, 500 personnes sont salariées de l'entreprise qui s'est implantée dans les deux premiers étages d'un grand bâtiment.
L'entreprise est maintenant largement informatisée, mais le fonctionnement du réseau et sa sécurité doivent être améliorés et la gestion de la qualité des projets doit désormais être prise en compte.
Le responsable informatique décide de vous en confier l'étude.

Au 1er étage se trouvent les services ÉDITION, JURIDIQUE et TRADUCTION, au 2ème étage le service ADMINISTRATIF et le service INFORMATIQUE. Le réseau informatique de l'entreprise est décrit en annexe 1.

1.a. Indiquer la classe et l'adresse du réseau exploité au 2ème étage de l'entreprise DUGALDE. Justifier la réponse.

1.b. Rechercher le masque de sous-réseau utilisé pour le 2ème étage. Veiller à prévoir le plus grand nombre de postes possible et tenir compte des 2 sous-réseaux existants.

1.c. Indiquer le nombre de sous-réseaux dont on pourrait disposer à cet étage. Justifier la réponse.

1.d. Rechercher l'adresse du sous-réseau auquel appartiendrait la machine d'adresse 172.16.132.2. Justifier la réponse.

Chaque étage dispose d'un ou de plusieurs serveurs DHCP. Le serveur nommé EDITI peut attribuer des adresses IP aux postes du 1er étage. Les serveurs ADMINI et INFORI attribuent, quant à eux, des adresses IP respectivement aux postes des deux sous-réseaux 4 et 5.

2. Expliquer le rôle des agents relais DHCP installés sur AGR1 et AGR2.

Des utilisateurs du sous-réseau 1 se plaignent parfois qu'ils n'arrivent pas à se connecter au réseau, un message leur signalant qu'une adresse IP existe déjà sur le réseau. Un contrôle a été réalisé permettant d'écarter les routeurs comme cause possible.

3. Donner une cause possible du problème rencontré par ces utilisateurs.

4. Proposer les paramètres de configuration du serveur DHCP EDITI afin d'assurer le bon fonctionnement de l'ensemble des postes du 1er étage.

L'entreprise située au 3ème étage déménage et la société DUGALDE profite de l'occasion pour y déplacer certains postes de travail du service ÉDITION qui manque actuellement cruellement de place.

5. Proposer une solution matérielle permettant d'assurer l'interconnexion avec un débit de 1 Gbit/s entre les postes du service ÉDITION déplacés au 3ème étage et les postes du service ÉDITION restés au 1er étage.

On prendra soin de ne modifier en aucun cas la configuration logicielle des machines.

On décide d'implanter également au 3ème étage un nouveau service qui aura pour adresse de sous-réseau 192.168.4.0 et qui devra être connecté au routeur AGR2.

6. Donner les lignes de la table de routage du routeur AGR2 qui permettront aux postes du sous-réseau 192.168.4.0 d'accéder à tous les autres sous-réseaux de l'entreprise. Seules les lignes précisant les accès aux sous-réseaux sont demandées.
Chaque ligne de la table de routage devra comporter l'adresse du réseau de destination, le masque de sous-réseau, l'adresse de passerelle et l'adresse d'interface.

Tous les services de l'entreprise doivent accéder à l'Internet, mais les droits d'accès aux différents services (web, courrier, etc.) ne sont pas les mêmes. Pour résoudre le problème et après avoir effectué une étude de marché, l'administrateur s'est doté d'un pare-feu (firewall) disposant également d'une fonction de translation d'adresses.
7. Expliquer en quoi la translation d'adresses est intéressante pour la sécurité de l'entreprise. On prendra soin de décrire le processus mis en œuvre.

Le pare-feu choisi gère les autorisations d'accès aux services de l'internet en regroupant les postes de travail qui ont des droits similaires. Pour créer un groupe de machines, on associe une plage d'adresses IP à son nom. Le responsable informatique a ainsi choisi de créer un groupe de machines par sous-réseau.
Voici un extrait partiel de la table actuelle des contrôles d'accès du pare-feu. Dans cette table, tout ce qui n'est pas explicitement autorisé est interdit.

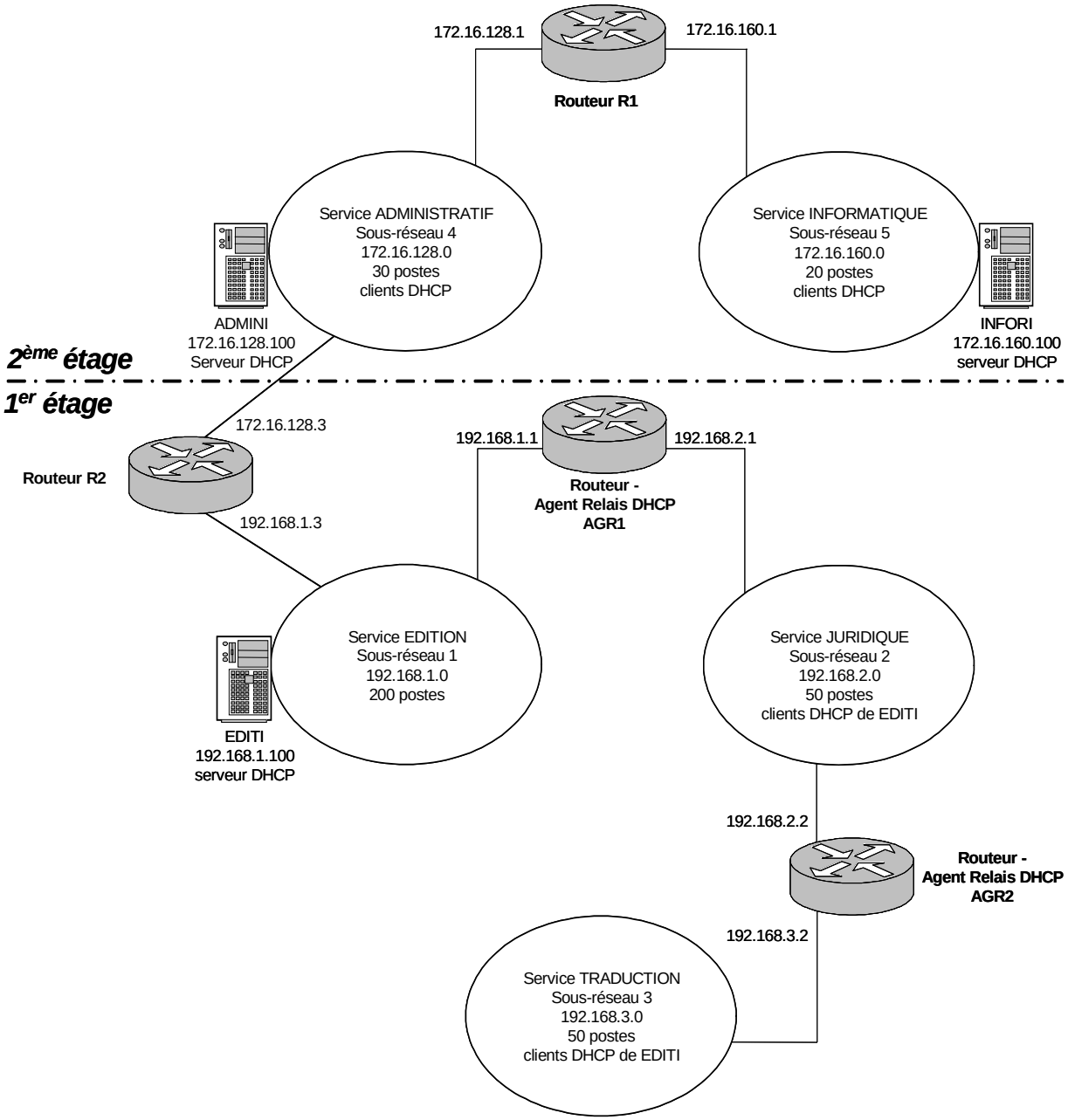
Groupe de machines	Protocoles autorisés
Sous-réseau 1	DNS, HTTP, …
Sous-réseau 2	DNS, HTTP, …
Sous-réseau 3	…
Sous-réseau 4	…
Sous-réseau 5	…

On souhaite que les postes de travail :
- du sous-réseau 1 puissent accéder au web et faire du transfert de fichiers,
- des sous-réseaux 2, 3 et 4 puissent accéder au web et utiliser le courrier électronique,
- du sous-réseau 5 puissent accéder à tous les services de l'internet, y compris les forums de discussion.

8. Présenter les contrôles d'accès du pare-feu à l'aide d'un tableau indiquant, pour chaque groupe de machines, la liste des protocoles autorisés.

On envisage d'autoriser les commerciaux à transmettre leurs commandes à distance à travers l'Internet, en utilisant les portables qui leur ont été fournis, équipés de cartes modem PCMCIA.
9. Indiquer comment assurer la sécurité et la confidentialité de ces transactions.

Annexe 1 : Réseau informatique de l'entreprise DUGALDE



Corrigé Exonet N° 17

Question 1.a. Indiquer la classe et l'adresse du réseau exploité au 2ème étage de l'entreprise DUGALDE. Justifier la réponse.
Question 1.b. Rechercher le masque de sous-réseau utilisé pour le 2ème étage. Veiller à prévoir le plus grand nombre de postes possible et tenir compte des 2 sous-réseaux existants.
Question 1.c. Indiquer le nombre de sous-réseaux dont on pourrait disposer à cet étage. Justifier la réponse.
Question 1.d. Rechercher l'adresse du sous-réseau auquel appartiendrait la machine d'adresse 172.16.132.2. Justifier la réponse.

1.a. 1er octet = 172 , compris entre 128 et 191 correspond à la classe B
Autre solution : en binaire 172 = **10**11 1110 **(10xx xxxx : classe B)**
L'adresse du réseau de l'entreprise DUGALDE est **172.16.0.0**

1.b. Le masque de réseau par défaut de la classe B est 255.255.0.0
Pour adresser des sous-réseaux, on dispose des 2 octets de poids faible.
Pour pouvoir disposer d'un réseau en x.y.160.0, il faut utiliser 3 bits sur les 2 octets de poids faible (160 base 10 = 1010 0000 base2). Les autres bits pourront être utilisés pour l'adressage des nœuds.
On a donc : 1111 1111. 1111 1111. **111**0 0000 . 0000 0000, soit **255.255.224.0**

1.c. 3 bits sont utilisés dans la partie hôte pour adresser les sous-réseaux.
$2^3 - 2 = 6$. On peut adresser **6 sous-réseaux**

1.d. Les 2 octets de poids faible ont pour valeur 132.2 , soit en binaire **100**0 0100 . 0000 0010. Les 3 premiers bits concernant le réseau (1000 0000 base 2 = 128), la machine d'adresse 172.16.132.2 appartient au sous-réseau d'adresse **172.16.128.0**

Question 2. expliquer le rôle des agents relais DHCP installés sur AGR1 et AGR2.

Les agents relais DHCP AGR1 et AGR2 sont situés entre un sous-réseau qui dispose d'un serveur DHCP et des sous-réseaux ne disposant pas de serveur DHCP ; les postes des sous-réseaux 2 et 3 doivent obtenir une adresse du serveur EDITI situé sur un autre sous-réseau ; l'agent relais va servir de passerelle avec le sous-réseau 1 ; il a dans sa configuration l'adresse IP du serveur DHCP EDITI et redirigera ainsi les requêtes de demandes d'adresse IP provenant des postes appartenant aux sous-réseaux 2 et 3 vers ce serveur DHCP. Inversement il relayera l'adresse IP attribuée vers la station qui en a fait la demande (il route les trames DHCP).

Question 3. Donner une cause possible du problème rencontré par ces utilisateurs.

Il se peut que la plage d'étendue DHCP proposée par EDITI n'ait pas exclu l'adresse du serveur lui-même ou celle du routeur. Un utilisateur faisant une demande peut donc se voir affecter une de ces adresses qui entre alors en conflit avec celle affectée de manière statique au serveur DHCP ou au routeur. Une autre cause éventuelle peut consister en une durée de bail trop longue ou trop courte. Une autre raison moins probable ici pourrait être la présence d'une adresse IP statique (fixe) sur quelques postes.

Question 4. Proposer les paramètres de configuration du serveur DHCP EDITI afin d'assurer le bon fonctionnement de l'ensemble des postes du 1er étage.

Le serveur DHCP EDITI doit attribuer des adresses aux 3 sous-réseaux 1, 2 et 3. Il doit donc gérer trois étendues.

Étendue de sous-réseau 1 :

Plage d'adresses à affecter: de 192.168.1.1 à 192.168.1.203

Adresse à exclure : 192.168.1.100 (adresse du serveur EDITI)
192.168.1.1 (adresse Agent Relais AGR1)
192.168.1.3 (adresse du routeur R2)

Masque de réseau : 255.255.255.0

Adresse de passerelle : 192.168.1.3

Étendue de sous-réseau 2 :

Plage d'adresses à affecter: de 192.168.2.1 à 192.168.2.52

Adresse à exclure : 192.168.2.1 (adresse Agent Relais AGR1)
: 192.168.2.2 (adresse Agent Relais AGR2)

Masque de réseau : 255.255.255.0

Adresse de passerelle : : 192.168.2.1

Étendue de sous-réseau 3

Plage d'adresses à affecter: de 192.168.3.1 à 192.168.3.51

Adresse à exclure : 192.168.3.2 (adresse Agent Relais AGR2)

Masque de réseau : 255.255.255.0

Adresse de passerelle : : 192.168.3.2

Question 5. Proposer une solution matérielle permettant d'assurer l'interconnexion avec un débit de 1 Gbit/s entre les postes du service EDITION déplacés au 3ème étage et les postes du service ÉDITION restés au 1er étage.
On prendra soin de ne modifier en aucun cas la configuration logicielle des machines.

Il s'agit ici de déplacer des machines sans toucher à leur configuration. Pas question donc de créer un autre sous-réseau au troisième étage. Il est exclu de fait, de relier les étages au travers d'un routeur, puisque toutes les machines conservent leur adresse IP et restent donc dans le même sous-réseau. La solution consiste alors à relier les deux étages (distance supposée inférieure à 25 m) à l'aide d'un brin supportant le 1 Gbit/s (catégorie 5e, 5+, 6 ou 7, voire fibre optique – obligatoire pour des distances supérieures à 25 m). On ne va pas, bien entendu, « tirer » autant de brins qu'on déplace de stations et il faut donc prévoir en plus, à l'étage, un équipement d'interconnexion des postes (en principe commutateur plutôt que concentrateur afin de limiter les collisions) qui sera relié à l'équipement actuel d'interconnexion. (on ignore son type, son débit actuel et donc s'il faut le changer). On ne demande pas à changer les cartes réseau.
On décide d'implanter également au 3ème étage un nouveau service qui aura pour adresse de sous-réseau 192.168.4.0 et qui devra être connecté au routeur AGR2.

Question 6. Donner les lignes de la table de routage du routeur AGR2 qui permettront aux postes du sous-réseau 192.168.4.0 d'accéder à tous les autres sous-réseaux de l'entreprise. Seules les lignes précisant les accès aux sous-réseaux sont demandées.
Chaque ligne de la table de routage devra comporter l'adresse du réseau de destination, le masque de sous-réseau, l'adresse de passerelle et l'adresse d'interface.

Réseau	**Masque**	**Passerelle**	**Interface**
…	…	..	..
192.168.1.0	255.255.255.0	192.168.2.1	192.168.2.2
192.168.2.0	255.255.255.0	192.168.2.2	192.168.2.2
192.168.3.0	255.255.255.0	192.168.3.2	192.168.3.2
192.168.4.0	255.255.255.0	192.168.4.2	192.168.4.2
172.16.128.0	255.255.224.0	192.168.2.1	192.168.2.2
172.16.160.0	255.255.224.0	192.168.2.1	192.168.2.2
…	…	…	…

Question 7. Expliquer en quoi la translation d'adresses est intéressante pour la sécurité de l'entreprise.
On prendra soin de décrire le processus mis en œuvre.

La translation d'adresses (NAT Network Address Translation, PAT Port Address Translation, …) permet de masquer au monde extérieur les adresses IP réellement utilisées dans l'entreprise, rendant ainsi plus difficiles les tentatives d'intrusion.
Quand un poste du réseau local émet une demande de service vers l'internet, le dispositif (pare-feu, routeur NAT, serveur mandataire ou proxy, …) disposant d'une fonction de translation d'adresses, remplace l'adresse IP du poste émetteur du paquet par sa propre adresse avant l'envoi sur l'internet. Il remplace de même le port de l'application cliente par une valeur particulière, en général située au delà de 61 000. Ces informations, adresse IP du poste émetteur, port d'origine de l'application cliente et port attribué, sont enregistrées dans une table. Lorsque la réponse du service invoqué arrive sur le pare-feu, ce dernier vérifie dans la table qu'il possède bien l'entrée correspondante, par rapport au port attribué, puis il réécrit dans les paquets l'adresse IP du poste émetteur et port initial de l'application cliente. Le paquet peut ainsi rejoindre sa destination dans le réseau local.

Question 8. Présenter les contrôles d'accès du pare-feu à l'aide d'un tableau indiquant, pour chaque groupe de machines, la liste des protocoles autorisés.

Groupe de machines	**Protocoles autorisés**
Sous-réseau 1	DNS, HTTP, FTP
Sous-réseau 2, 3 et 4	DNS, HTTP, SMTP, POP3, IMAP
Sous-réseau 5	DNS, HTTP, SMTP, POP3, IMAP, NNTP

Question 9. Indiquer comment assurer la sécurité et la confidentialité de ces transactions.

Une solution consiste à mettre en œuvre un tunnel à travers l'internet en utilisant un protocole comme PPTP ou L2TP (création d'un VPN).
Du côté de l'entreprise Dugalde, il faut installer un serveur d'accès distant et sur les portables des commerciaux, il faut configurer un client d'accès distant.
Le VPN sera créé entre le client et le serveur et les données seront cryptées lors des échanges.
Il est également possible d'envisager la transmission de fichiers cryptés en utilisant des outils PGP.
Le commercial pourra alors rédiger sa commande sur son portable et crypter le fichier concerné avant de l'envoyer. La fiabilité et la rapidité d'un tel cryptage est obtenu en combinant les principes des clés privées/publiques et des clés secrètes.

EXONET N° 18

Le groupement d'intérêt économique (GIE) SILVIA regroupe une dizaine de membres (appelés aussi clients) dans des domaines d'activité variés relevant de la filière bois.
Sa mission est de fournir à ses membres une expertise dans le conseil (gestion, informatique de gestion…) et de proposer également tous les services de traitement numérique (comptabilité, paie, ...)
Le GIE héberge sur ses propres machines toutes les applications informatiques de comptabilité, de gestion et de publication en ligne et propose à ses membres l'accès à ses services sous la forme d'un intranet.
Toutes les applications sont basées sur IPv4.
Sur le réseau du GIE, les postes clients ont comme passerelle par défaut l'adresse 172.16.0.253.

La liaison avec les réseaux des membres du GIE
Chaque nouveau membre se voit attribuer par le GIE une adresse de réseau de classe C privée prise dans la plage d'adresses de 192.168.0.0 à 192.168.255.0.
Les membres accèdent aux applications de l'intranet par une liaison dédiée louée à un opérateur.
Ils accèdent à Internet par un autre moyen (Numéris, ADSL, modem...) afin de ne pas surcharger la liaison louée et garantir la sécurité des données privées.
Sur les réseaux des membres, le cahier des charges prévoit que les postes utilisent :
– le serveur de nom qui est situé sur le réseau du GIE,
– l'adresse du routeur qui les relie au GIE comme passerelle par défaut.

Le GIE s'est doté d'un SIG (système d'information géographique) qu'il met à la disposition de ses membres. Il souhaite s'attacher les services du cabinet de géomètres Géom & Trie, situé à 25 km afin de renseigner le SIG à partir de relevés effectués sur le terrain.
Pour chaque parcelle de bois appartenant à un membre du GIE, le cabinet de géomètres devra numériser le plan cadastral correspondant, effectuer un relevé sur le terrain par système GPS (Global Positioning System), caractériser le boisement et alimenter le SIG.
La liaison entre le site du GIE et le site de Géom & Trie sera réalisée par une liaison louée Transfix.
Afin d'établir le besoin en bande passante, les techniciens du GIE consultent les statistiques d'utilisation des liaisons avec ses membres. Il en ressort que :

- Les applications de gestion basées sur le protocole HTTP représentent 75 % des flux. Elles nécessitent un débit de 10 Kbit/s par poste utilisateur pour garantir une qualité de service suffisante.
- Le reste des flux est constitué par les autres services (DNS, FTP...) de l'intranet.

1. Déterminer la bande passante minimum nécessaire, exprimée en Kbit/s, que devra supporter la liaison Transfix entre le site du GIE et celui de la société Géom & Trie.

Toutes les machines du réseau du GIE sont configurées pour utiliser le routeur « **rtr-ext** » comme passerelle par défaut. Ce routeur dispose d'une table de routage, dont voici un extrait :

Réseau	**Masque**	**Passerelle**	**Interface**
192.168.11.0	255.255.255.0	172.16.0.254	172.16.0.253
192.168.12.0	255.255.255.0	172.16.0.254	172.16.0.253
192.168.13.0	255.255.255.0	172.16.0.254	172.16.0.253

2. Proposer la ligne à ajouter dans la table de routage du routeur « rtr-ext » pour que les machines du réseau du GIE puissent atteindre le réseau de la société Géom & Trie.

3. Proposer la ligne qui permettrait, en remplaçant toutes les lignes précédentes, d'adresser tous les réseaux possibles des membres du GIE.

Un des géomètres semble rencontrer quelques dysfonctionnements à partir de la machine 192.168.62.11 alors que **tout fonctionne normalement sur les autres machines**. Il peut accéder à tous les services Internet, mais n'arrive pas à accéder aux applications situées sur la machine 172.16.0.10 de nom srv10.silvia.fr.
Afin de déterminer la cause du dysfonctionnement entre ces deux nœuds, vous souhaitez, à partir du poste 192.168.62.11, utiliser la commande « ping » pour vérifier le fonctionnement des éléments suivants :

- pile de protocoles TCP/IP sur lui-même,
- couche Physique et Liaison de données sur le réseau de la société Géom & Trie,
- couche Réseau entre le réseau de la société Géom & Trie et celui du GIE,
- résolution de nom en utilisant le protocole DNS.

4. Pour chacune des vérifications souhaitées, indiquer la commande « ping » à exécuter. Justifier la réponse pour chacune des quatre commandes employées.

Vous demandez au géomètre de taper la commande « **ping 172.16.0.10** » sur la machine qui ne fonctionne pas. La consultation du cache **arp** de cette machine donne le résultat suivant :

Adresse internet	**Adresse physique**	**Type**
192.168.62.253	00:D0:59:86:3B:68	dynamique

Vous demandez ensuite au géomètre de taper la commande « **ping 172.16.0.10** », depuis une autre machine d'adresse **192.168.62.12**. Après quoi, la consultation du cache **arp** de cette autre machine donne le résultat suivant :

Adresse internet	**Adresse physique**	**Type**
192.168.62.254	00:D0:59:82:2B:86	dynamique

5. Expliquer le rôle du protocole arp.
6. Expliquer le problème que l'analyse des caches arp révèle pour la machine 192.168.62.11.

Les fonctions de filtrage du routeur « **rtr-ext** » sont déjà activées sur les interfaces 193.252.19.3 et 195.115.90.15. Les tableaux ci-dessous donnent **un extrait** des tables de filtrage correspondant à chacune de ces interfaces :

Table de filtrage de l'interface 193.252.19.3 du routeur « rtr-ext » :

N° de règle	**Adresse source**	**Port source**	**Adresse destination**	**Port destination**	**Protocole transport**	**Action**
1	Toutes	Tous	195.115.90.1/32	25	TCP	Accepter
2	Toutes	Tous	195.115.90.1/32	110	Tous	Accepter
3	Toutes	Tous	195.115.90.1/32	53	Tous	Accepter
4	Toutes	Tous	195.115.90.2/32	80	TCP	Accepter
6	Toutes	Tous	195.115.90.0/28	22	Tous	Accepter
7	195.115.90.0/28	Tous	Toutes	Tous	Tous	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Tous	Refuser

Table de filtrage de l'interface 195.115.90.15 du routeur « rtr-ext » :

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole transport	Action
Défaut	Toutes	Tous	Toutes	Tous	Tous	Accepter

L'algorithme utilisé par le service de filtrage est équivalent à ceci :

1. Tant qu'il y a un paquet à traiter
    - En suivant l'ordre des règles de 1 à n, rechercher la première règle applicable.
    - Si une des règles est applicable, alors appliquer l'action au paquet et arrêter le parcours de la table.
    - Si aucune règle n'est applicable, appliquer la règle par défaut.

On souhaite remplir la table de filtrage sur l'interface **172.16.0.253** du routeur « **rtr-ext** » entre le réseau du GIE et la DMZ (zone démilitarisée), en appliquant les règles suivantes :

- L'accès au service DNS de la DMZ n'est autorisé que pour le serveur DNS du GIE.
- L'accès au service SSH est autorisé à partir de toutes les machines du GIE sauf pour le serveur d'adresse 172.16.0.10.
- Tout le reste est refusé.

7. Expliquer le rôle de la règle numéro 1 et celui de la règle numéro 6 dans la table de filtrage de l'interface 193.252.19.3.

8. Proposer une table de filtrage pour l'interface 172.16.0.253 afin de prendre en compte les contraintes exprimées ci-dessus. Vous respecterez la présentation adoptée pour les tables de filtrage présentées ci-dessus. Vous traiterez aussi bien les flux provenant du GIE en direction de la DMZ que les flux en retour.

Afin de réaliser des tests, vous mettez en place, avec un autre membre de l'équipe, un logiciel de capture de trames sur l'une des machines du réseau du GIE.

Capture de trames

```
0000  00 d0 59 82 2b 86 00 80  c8 7a 0a d8 08 00 45 00   .ÐY.+... Èz.Ø..E.
0010  00 40 8b 12 40 00 40 06  57 17 ac 10 00 64 ac 10   .@..@.@. W.¬..d¬.
0020  00 0a 11 0e 00 15 7e 09  c4 4a 7f 94 cb 33 80 18   ......~. ÄJ..Ë3..
0030  16 d0 28 b9 00 00 01 01  08 0a 04 45 57 06 00 1e   .Ð(¹.... ...EW...
0040  45 04 55 53 45 52 20 61  6e 6e 69 65 0d 0a         E.USER a nnie..
```

Cette capture **ne présente pas** le **préambule** de la trame Ethernet.

9. Indiquer l'adresse MAC (adresse physique ou Ethernet) de la machine destinataire de la trame capturée.

10. Donner en décimal l'adresse IP du destinataire du datagramme qui a été capturé.

Chaque membre du GIE dispose d'une base de données sur la machine 195.115.90.2. Ces données sont exploitées par le serveur HTTP pour la création dynamique de pages web.

11. Décrire, éventuellement à l'aide d'un schéma, le dialogue qui s'établit entre un client HTTP (navigateur Internet), un serveur HTTP et un serveur de bases de données lorsque le client soumet un formulaire au serveur HTTP et que celui-ci doit retourner des informations contenues dans la base de données.

Annexe 1 : Plan du réseau

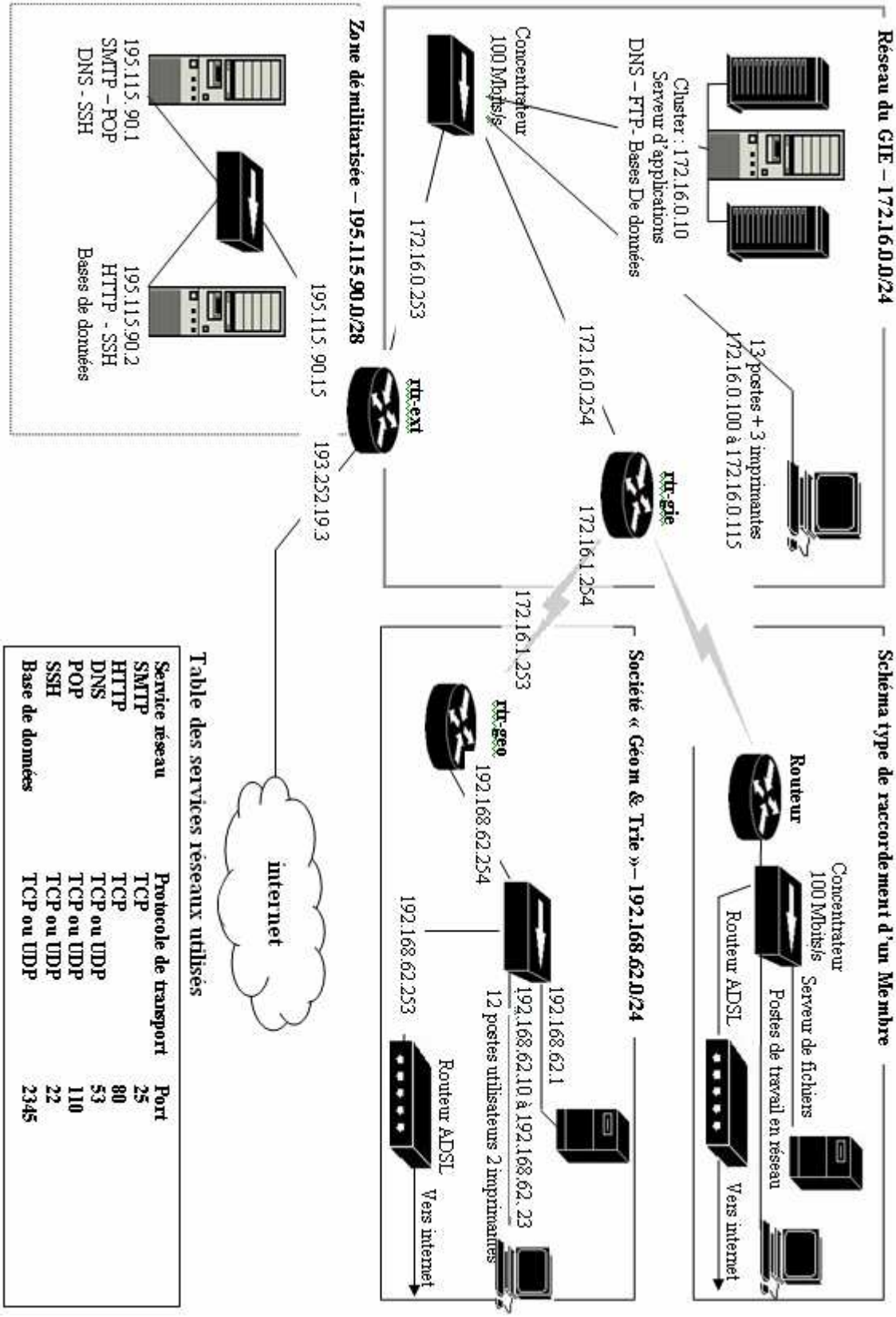
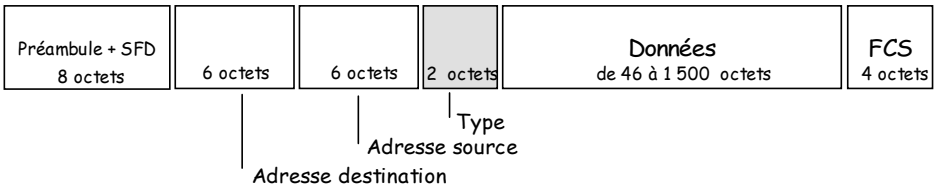


Table des services réseaux utilisés

Service réseau	Protocole de transport	Port
SMTP	TCP	25
HTTP	TCP	80
DNS	TCP ou UDP	53
POP	TCP ou UDP	110
SSH	TCP ou UDP	22
Base de données	TCP ou UDP	2345

Annexe 2 : Format des trames Ethernet et datagrammes IP

Format d'une trame Ethernet



SFD : Start Frame Delimiter indique le début de la trame
FCS : Frame Check Sequence ou code de contrôle CRC

Structure du datagramme IP (par lignes de 32 bits)

1 4	5 8	9 16	17 19	20 24	25 32
Version	IHL	TOS (Type Of Service)	Longueur du datagramme - TL (Total Length)		
ID (IDentification)			FO	Déplacement (Offset)	
TTL (Time To Live)		Protocole	Total de Contrôle (Header Checksum)		
Adresse IP Source					
Adresse IP Destination					
Options IP Éventuelles					Bourrage
Données (de 2 à 65 517o) …					

IHL : Internet Header Length ou longueur d'en-tête, en mots de 32 bits
FO : Fragment Offset indique si le fragment est suivi d'autres fragments

Corrigé Exonet N° 18

Question 1. Déterminer la bande passante minimum nécessaire, exprimée en Kbit/s, que devra supporter la liaison Transfix entre le site du GIE et celui de la société Géom & Trie.

Comme l'indique clairement le schéma du réseau (**annexe 1**), il y a douze postes dans la société « Géom & Trie ». Le texte mentionne de son côté « les applications de gestion… représentent 75 % des flux. Ces applications… nécessitent un débit de 10 Kbit/s par poste utilisateur… ».
Il faut donc : 10 Kbit/s * 12 postes soit 120 Kbit/s pour les applications de gestion. Ces applications de gestion « …représentent 75 % des flux ». Il faut donc rajouter les 25 % utilisés par les autres flux (DNS, FTP…) soit 40 Kbit/s (120/75*25), pour obtenir le débit total nécessaire.
Le débit total nécessaire est donc de 120+40 Kbit/s soit 160 Kbit/s.

Question 2. Proposer la ligne à ajouter dans la table de routage du routeur « **rtr-ext** » pour que les machines du réseau du GIE puissent atteindre le réseau de la société Géom & Trie.

Aidons nous du schéma de l'**Annexe 1** et plaçons nous mentalement « sur » le routeur **rtr-ext** dont il convient de compléter la table. La question indique que le réseau à atteindre est celui de société Géom & Trie « …puissent atteindre le réseau de la société Géom & Tri… » soit **192.168.62.0** comme l'indique clairement le schéma. Le masque de réseau est noté, dans cette même annexe, **/24** ce qui correspond à la notation CIDR (Classless InterDomain Routing) d'un masque de 24 bits à 1 soit, en notation traditionnelle : 255.255.255.0. Depuis le routeur **rtr-ext**, tous les paquets destinés au réseau Géom & Trie doivent donc être expédiés au routeur **rtr-gie** (dont le « travail » sera de les rediriger à son tour vers le réseau de la société…) et dont l'adresse de l'interface d'entrée est **172.16.0.254**. Pour cela, les paquets doivent sortir de notre routeur **rtr-ext** par l'interface de sortie **172.16.0.253**. Bien entendu le concentrateur n'a « rien à voir » avec un problème de routage puisqu'il est censé travailler au niveau 2 du modèle OSI et non pas au niveau 3 comme le routeur.
La ligne à rajouter dans la table de routage est donc en définitive :

Réseau à atteindre	Masque de ce réseau	« On doit s'adresser à »	« On sort du routeur par… »
Réseau	Masque	Passerelle	Interface
192.168.62.0	255.255.255.0	172.16.0.254	172.16.0.253

Question 3. Proposer la ligne qui permettrait, en remplaçant toutes les lignes précédentes, d'adresser tous les réseaux possibles des membres du GIE

A l'observation de la table de routage (complétée en principe par la ligne issue de la réponse à la question précédente) on constate que tous les réseaux appartiennent à la même plage d'adresses 192.168.x.y. On constate également que, quel que soit le réseau de destination, les valeurs de passerelle à atteindre et d'interface de sortie sont les mêmes. Comment « fusionner » toutes ces lignes en une seule ?
Si le masque de réseau appliqué aux paquets au niveau du routeur ne couvre que les deux premiers octets d'adresse, tous les paquets vont « sembler » appartenir au même réseau **192.168.0.0**. En effet, quand les décisions de routage sont prises, seuls les bits « couverts » par le masque de sous-réseau sont utilisés pour déterminer quel est le réseau à atteindre et donc, en appliquant un masque « tronqué » ou « sur-masque », toutes les adresses semblent faire partie du même réseau du point de vue du routage.
On doit donc utiliser ici un « sur-masque » **/16** alors que pour des réseaux de classe C on s'attend à avoir /24. Cette technique est largement utilisée par les opérateurs pour limiter la taille des tables de routage.

La ligne de remplacement des quatre lignes précédentes est donc en définitive :

Réseau	Masque	Passerelle	Interface
192.168.0.0	255.255.0.0	172.16.0.254	172.16.0.253

Question 4. Pour chacune des vérifications souhaitées, indiquer la commande « ping » à exécuter. Justifier la réponse pour chacune des quatre commandes employées.

- **Vérification 1** : « Pile de protocoles TCP/IP sur lui-même »

La commande **ping 127.0.0.1** permet de tester la pile TCP/IP de la machine, sans « descendre » au niveau de la carte. Un ping sur l'adresse IP du poste (**ping 192.168.62.11**) permet aussi de tester la pile TCP/IP sans descendre sur la carte mais teste en plus la validité de l'adresse. L'une ou l'autre de ces réponses est donc acceptable.

- **Vérification 2** : « Couche Physique et Liaison de données sur le réseau de la société « Géom & Trie »

La commande **ping 192.168.62.254** (ou sur toute autre adresse du réseau - 192.168.62.1 par exemple) suffit et permet de déterminer que la liaison fonctionne sur 2 nœuds adjacents. Cette commande permet de tester la carte réseau, le concentrateur et le câble de liaison. Par contre un « ping 127.0.0.1 » ou « ping 192.168.62.11 » est insuffisant à ce niveau car le paquet ne « sort » pas sur le réseau et donc la couche physique ne serait pas testée.

- **Vérification 3** : « Couche Réseau entre le réseau de la société « Géom & Trie » et celui du GIE »

Il s'agit de vérifier ici si le « routage » « …couche réseau… » se fait bien. Il faut donc un ping qui « concerne » les routeurs intermédiaires aux deux réseaux intéressés. Les commandes **ping 172.16.1.254** ou **ping 172.16.0.10** par exemple, sont valides. Ces commandes permettent de déterminer que le routage fonctionne entre les deux nœuds distants. Ces commandes testent le fonctionnement du routeur (configuration et table de routage) mais aussi celui de la table de routage du poste émetteur et de celle du poste récepteur. Là aussi la réponse doit normalement être positive puisque les autres postes accèdent au serveur.

- **Vérification 4** : « Résolution de nom en utilisant le protocole DNS »

Pour provoquer la résolution de nom en son adresse IP, il faut faire un ping qui utilise le nom d'hôte du poste. Ce nom est précisé dans le texte du sujet « …la machine 172.16.0.10 de nom srv10.silvia.fr… ». On fera donc un **ping srv10.silvia.fr**. On travaille ici dans les couches supérieures à la couche 3 (réseau), et donc au dessus du protocole de transport. On va ainsi tester la configuration DNS du poste ainsi qu'éventuellement le fichier de zone du serveur DNS contacté si le cache DNS sur le poste est vide, c'est-à-dire que cette résolution n'a pas déjà été faite antérieurement.

Question 5. Expliquer le rôle du protocole arp.

Le protocole **arp** permet la résolution d'adresse IP en adresse MAC adresse physique ou adresse Ethernet.

Question 6. Expliquer le problème que l'analyse des caches arp révèle pour la machine 192.168.62.11.

En clair, alors que les adresses MAC devraient être toutes les deux celles du routeur **rtr_geo**, une seule est la bonne. L'autre est donc celle du routeur ADSL qui répond au lieu du routeur **rtr_geo** attendu. La réponse est alors « évidente », le problème vient de ce que la passerelle par défaut (gateway) sur la machine « défectueuse » (**192.168.62.11**) correspond en fait à celle du routeur ADSL et non à celle du routeur **rtr_geo**.
Il faudrait modifier la passerelle par défaut du poste 192.168.62.11 en remplaçant la valeur actuelle 192.168.62.253 par la valeur correcte : **192.168.62.254**.

Question 7. Expliquer le rôle de la règle numéro 1 et celui de la règle numéro 6 dans la table de filtrage de l'interface 193.252.19.3.

En clair : La règle 1 autorise les requêtes « SMTP » à partir d'Internet sur la machine d'adresse 195.115.90.1
En clair : La règle 6 autorise les requêtes SSH sur toutes les machines appartenant au réseau DMZ (195.115.90.0/28)

Question 8. Proposer une table de filtrage pour l'interface **172.16.0.253** afin de prendre en compte les contraintes exprimées ci-dessus. Vous respecterez la présentation adoptée pour les tables de filtrage présentées ci-dessus. Vous traiterez aussi bien les flux provenant du GIE en direction de la DMZ que les flux en retour.

N° de règle	**Adresse source**	**Port source**	**Adresse destination**	**Port destination**	**Protocole transport**	**Action**
1	172.16.0.10/32	Tous	195.115.90.1/32	53	Tous	Accepter
2	195.115.90.1/32	53	172.16.0.10/32	Tous	Tous	Accepter
3	172.16.0.10/32	Tous	195.115.90.0/28	22	Tous	Refuser
4	172.16.0.0/24	Tous	195.115.90.0/28	22	Tous	Accepter
5	195.115.90.0/28	22	172.16.0.0/24	Tous	Tous	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Tous	Refuser

Question 9. Indiquer l'adresse MAC (adresse physique ou Ethernet) de la machine destinataire de la trame capturée.

00 : d0 : 59 : 82 : 2b : 86

Question 10. Donner en décimal l'adresse IP du destinataire du datagramme qui a été capturé

172.16.0.10

Question 11. Décrire, éventuellement à l'aide d'un schéma, le dialogue qui s'établit entre un client HTTP (navigateur Internet), un serveur HTTP et un serveur de bases de données lorsque le client soumet un formulaire au serveur HTTP et que celui-ci doit retourner des informations contenues dans la base de données.

1. Le client envoie la requête.
2. Les requêtes des clients arrivent sur le port HTTP (80 en général).
3. Le serveur HTTP transmet les valeurs (noms de champs + valeurs) à un script par une méthode get ou post.
4. Le serveur exécute un script (requête SQL encapsulée) et via un middleware la requête SQL est transmise au SGBD.
5. Le SGBD exécute la requête et renvoie le résultat au serveur http.
6. Le serveur http met en forme le résultat (HTML dynamique) et retourne au client (navigateur) ce résultat (page HTML).

EXONET N° 19

Le Domaine VISTE est un domaine qui possède vingt hectares d'orange, il produit environ 50 000 litres de jus d'orange par an.
VISTE dispose déjà d'un réseau informatique, reliant les bureaux, le dépôt (ou sont stockés les bouteilles de jus d'orange) et la cave, et d'un serveur HTTP en intranet.
VISTE est une petite entreprise ambitieuse qui cherche à se faire connaître en participant aux différents salons.
Récemment le propriétaire du domaine a loué un stand dans un salon qui va se dérouler à Meknés. Durant le salon, les commerciaux présents auront besoin d'obtenir en temps réel l'état des stocks et de se connecter sur le réseau du domaine. Il faut en effet offrir la possibilité aux visiteurs du salon de commander des jus d'orange présentés ou non sur le stand et disponibles en stock au domaine.

Dans le cadre de sa participation aux différents salons, le propriétaire du Domaine VISTE souhaite mettre en place un accès à sa base de données de gestion de stocks afin de faciliter la prise de commandes des produits non disponibles en quantité suffisante ou non présentés au salon.
Pour cela, il a contacté une société de services qui, après étude, lui propose d'abord de modifier le réseau existant afin d'en améliorer la sécurité. La proposition de modification est jointe en annexe 2.
Le propriétaire vous demande de valider les choix techniques et technologiques proposés par la société de services.

1. 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.

Le schéma proposé par la société de service indique la présence d'un serveur DHCP et d'un agent relais DHCP, dans la cave et dans le dépôt.

2. Indiquer en quoi une telle configuration est utile.

Pour assurer le bon fonctionnement de l'entreprise, il vous faut ensuite prévoir les tables de routage des routeurs afin que **Tous les hôtes** du réseau puissent communiquer entre eux et avec l'extérieur.

3. Établir la table de routage du routeur Général afin d'assurer le bon fonctionnement du réseau.

Pour maintenir la sécurité interne de l'entreprise VISTE, la société de service propose de ne pas mettre les serveurs HTTP et Mail sur le réseau interne. Sur le routeur Général, les règles suivantes ont été écrites
Règles NAT (Network Address Translation) **PAT** (Port Address Translation) **appliquées sur l'interface 172.16.0.129**

IP	Port
172.16.0.66	2020

←→

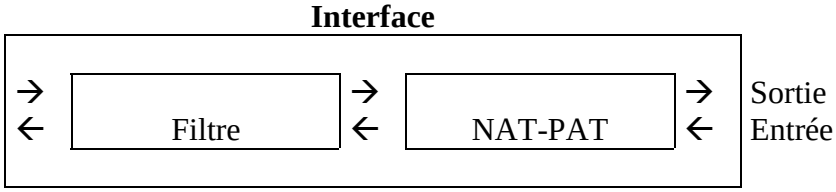
IP	Port
192.168.0.5	5600

Règles de filtrage appliquées sur l'interface 172.16.0.129

N° règle	Interface	IP Source	Port Source	IP Destination	Port Destination	Action
1	172.16.0.129	*	*	*	*	Refusé

Les règles de filtrage s'appliquent dans l'ordre de leur numéro.

Principes d'association des règles de filtrage et de NAT-PAT sur une interface.



- Sur un paquet **en sortie** d'une interface, on applique d'abord les règles de filtrage puis les règles NAT-PAT.
- Sur un paquet **en entrée** d'une interface, on applique d'abord les règles NAT-PAT puis les règles de filtrage.

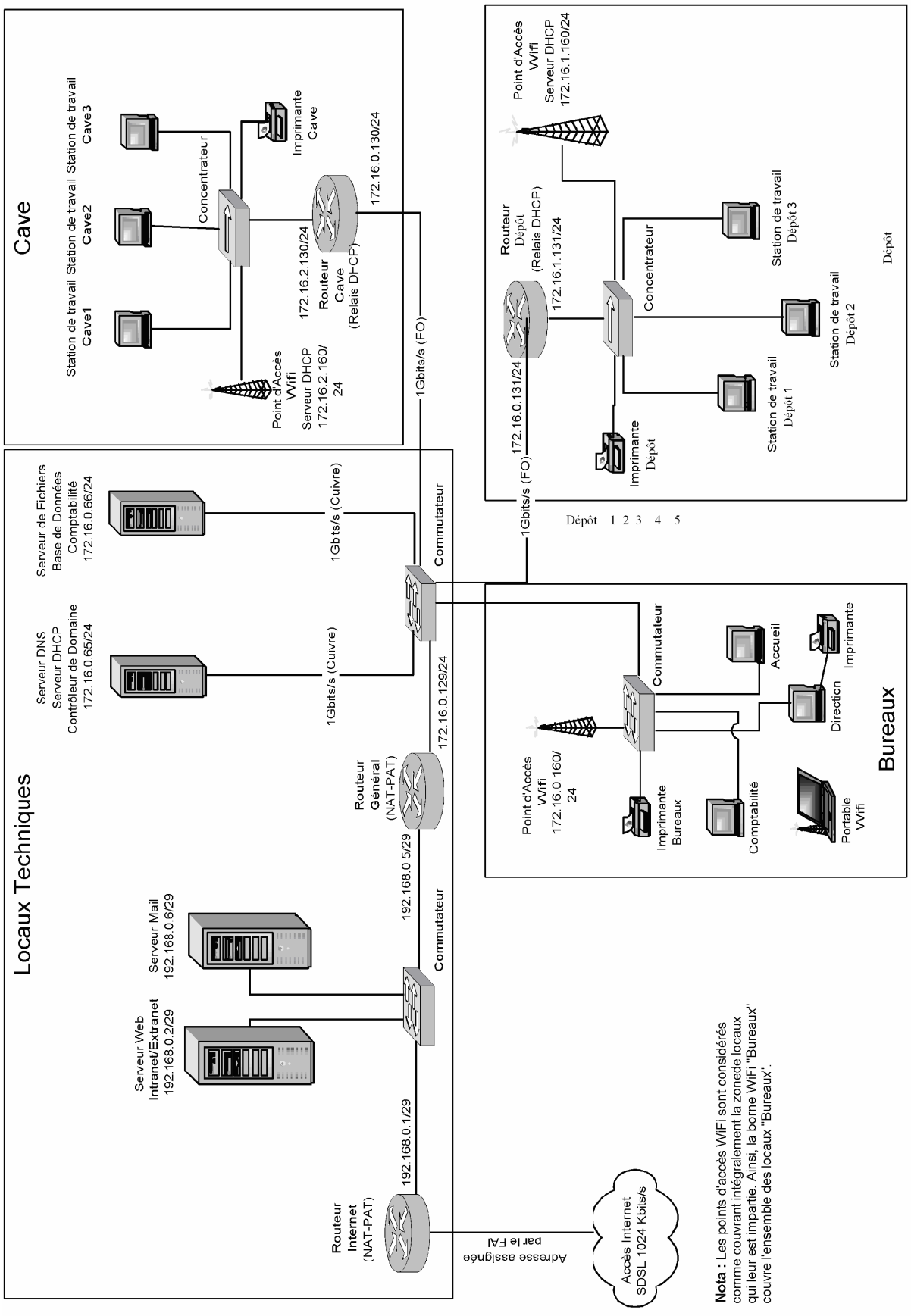
Le serveur HTTP utilise le **port 1060** pour communiquer et le serveur de bases de données le **port 2020**.

4. Donner les adresses IP et les ports source et destination d'un paquet envoyé par le serveur HTTP au serveur de bases de données. Vous justifierez votre réponse.
5. Rédiger la (ou les) règle(s) définie(s) sur l'interface 172.16.0.129, qui permet(tent) au serveur HTTP de communiquer avec le serveur de bases de données. Vous préciserez l'ordre de cette (ces) règle(s) par rapport à la règle actuelle.

Lorsque les commerciaux du domaine VISTE participent à un salon, ils doivent équiper le stand afin de pouvoir consulter le stock disponible. Pour assurer cette fonction, le domaine a fait l'acquisition de trois ordinateurs portables.
Ce matériel utilise les structures fournies par le salon pour accéder au serveur HTTP du domaine. Cette connexion sécurisée permet d'interroger, au travers d'une interface au format HTML, la base de données de gestion des stocks.
La solution technique proposée par la société de services a été mise en place. Lors d'un premier salon, les commerciaux ont dû installer leurs portables en paramétrant leur navigateur avec l'adresse IP du routeur Internet, adresse fournie par le fournisseur d'accès Internet (FAI) et relevée par la société de service. De plus, alors qu'en interne ils utilisent l'URL « http://catalogue.viste.fr », ils ont dû employer l'adresse IP fournie par le FAI comme adresse dans leur navigateur.
6. Expliquer pourquoi les commerciaux ont dû saisir l'adresse IP fournie par le FAI et non pas l'adresse IP du serveur HTTP.
7. Expliquer pourquoi ils ont dû saisir cette adresse IP au lieu d'une adresse URL, contrairement à ce qu'ils font en interne.

Quelques semaines plus tard, lors d'un autre salon, les commerciaux ont cherché en vain à utiliser cette même adresse IP mais elle ne fonctionnait plus ! Après contact d'urgence avec la société de services, ils ont dû employer une autre adresse IP.
8. Proposer une solution permettant aux commerciaux d'accéder au site web d'une manière conventionnelle (saisie soit de l'adresse URL du site web, soit d'une adresse IP stable).

Annexe 1 : schéma du réseau après modification



Corrigé Exonet N° 19

Question 1. 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 (dépôt), 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).

Question 2. Indiquer en quoi une telle configuration est utile.

En cas de défaillance du serveur DHCP, 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.

Question 3. Établir la table de routage du routeur Général afin d'assurer le bon fonctionnement du réseau.

A partir des documents fournis, on constate que les routeurs de la cave et du chai ne connaissent qu'une route par défaut sur le routeur général. Par conséquent il convient de passer par ce routeur pour atteindre les réseaux du dépôt et de la cave.

La table de routage du **routeur Général** sera donc de la forme suivante :

Destination réseau	Masque réseau	Adr. passerelle	interface	Métrique
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.5	1
172.16.0.0	255.255.255.0	172.16.0.129	172.16.0.129	1
172.16.1.0	255.255.255.0	172.16.0.131	172.16.0.129	1
172.16.2.0	255.255.255.0	172.16.0.130	172.16.0.129	1
192.168.0.0	255.255.255.248	192.168.0.5	192.168.0.5	1

Question 4. Donner les adresses IP et les ports source et destination d'un paquet envoyé par le serveur HTTP au serveur de bases de données. Vous justifierez votre réponse.

Le paquet est envoyé du serveur HTTP (192.168.0.2) sur le port 1060 comme l'indique le texte, et à destination du serveur de bases de données (172.16.0.66) pour le port 2020. Mais le paquet est pris en charge par le routeur NAT qui va assurer la translation de certaines valeurs. En effet l'adresse 172.16.0.66 et le port 2020 vont être convertis en l'adresse 192.168.0.5 et le port 5600. Les valeurs définitives seront donc :

- Adresse IP source : 192.168.0.2
- Port source : 1060
- Adresse IP Destination : 192.168.0.5
- Port Destination : 560

Question 5. Rédiger la (ou les) règle(s) définie(s) sur l'interface 172.16.0.129, qui permet(tent) au serveur HTTP de communiquer avec le serveur de bases de données. Vous préciserez l'ordre de cette (ces) règle(s) par rapport à la règle actuelle**.**

Il est nécessaire d'autoriser le dialogue dans les deux sens (serveur HTTP vers Serveur de bases de données et inversement). D'autre part on n'a pas à se préoccuper du NAT puisque les règles de filtrage s'appliquent AVANT ce NAT en sortie et après le NAT en entrée.

N° règle	Interface	IP Source	Port Source	IP Destination	Port Destination	Action
1	172.16.0.129	192.168.0.2	1060	172.16.0.66	2020	Accepté
2	172.16.0.129	172.16.0.66	2020	192.168.0.2	1060	Accepté
3	172.16.0.129	*	*	*	*	Refusé

Ces nouvelles règles seront placées AVANT la ligne actuellement présente dans la table de filtrage (dans un ordre qui importe peu) car la dernière ligne a pour objet de bloquer TOUTE transmission quels que soient les IP et ports de l'émetteur et de la destination.

Question 6. Expliquer pourquoi les commerciaux ont dû saisir l'adresse IP fournie par le FAI et non pas l'adresse IP du serveur HTTP.

Il n'est pas possible de saisir l'adresse IP du serveur HTTP car il s'agit d'une adresse de **classe privée** (192.x.y.z) et qui ne sera donc pas routée sur l'Internet. En conséquence les accès ne peuvent se faire que sur l'adresse IP fournie par le FAI, généralement obtenue à partir d'un serveur DHCP et « renouvelée » régulièrement.

En effet, lors du premier salon on a saisi l'adresse IP du moment, telle que le serveur DHCP du FAI l'avait affectée au client. Mais lors du deuxième salon cette adresse avait changé (bail expiré…) et on ne pouvait plus réutiliser la même.

Question 7. Expliquer pourquoi ils ont dû saisir cette adresse IP au lieu d'une adresse URL, contrairement à ce qu'ils font en interne.

En interne, les clients font appel au serveur DNS 172.16.0.65 pour résoudre le nom catalog.viste.fr en l'adresse IP du serveur web. Comme ce serveur DNS est situé **derrière** deux routeurs NAT et que de plus il est en adressage **privé**, il sera inaccessible de l'extérieur.

Question 8. Proposer une solution permettant aux commerciaux d'accéder au site web d'une manière conventionnelle (saisie soit de l'adresse URL du site web, soit d'une adresse IP stable).
Le domaine VISTE devra faire l'acquisition d'une adresse IP fixe et d'un nom de domaine.

EXONET N° 20

La SOVAMI est une société installée en France et spécialisée dans la collecte, le traitement et la valorisation de déchets d'équipements électriques et électroniques (DEEE).
La société possède son siège historique à Lyon. Il regroupe, outre les services administratifs et de direction, une unité de recherche et développement.
Une autre usine de traitement se situe à Fos. D'autres sites dits de prévalorisation existent à Toulouse, Tarbes et Bordeaux et un nouveau site doit ouvrir à Bussy en région parisienne ; ces sites servent de lieu de collecte et de première valorisation..
Le cœur du système d'information de la SOVAMI est à Lyon. Les autres sites accèdent au site de Lyon pour l'essentiel de leurs traitements.

Le réseau local du site de Lyon est vous est présenté en annexe 1.
Au siège de Lyon**,** on souhaite équiper une salle de réunion pour des visiteurs extérieurs équipés d'ordinateurs portables. Cette salle disposera de prises réseau, d'une imprimante en réseau et d'un point d'accès sans fil. L'ensemble sera relié à un commutateur capable de gérer des réseaux locaux virtuels (VLAN). Pour des raisons de sécurité, on veut pouvoir isoler momentanément le réseau de la salle de réunion du réseau du siège tout en autorisant des communications entre les équipements présents dans cette salle. Une présentation de la notion de VLAN est fournie en annexe 2.
1. Indiquer quel niveau de VLAN permettra de prendre en charge l'isolement temporaire du réseau de la salle de réunion du siège. Justifier la réponse.

En utilisant les annexes 1, 3 et 4, vous êtes chargé(e) d'analyser le plan d'adressage de la société.
2. Indiquer le nombre d'adresses IP encore disponibles dans le réseau IP de la zone "DMZ" du réseau. Justifier le résultat.

L'organisation du réseau interconnectant le siège de Lyon aux différents sites de la SOVAMI est conçue de telle sorte que chaque poste de n'importe quel site puisse se connecter au siège mais NE PUISSE PAS avoir accès aux autres sites.
Afin de vérifier que cette organisation est bien en place, vous effectuez la première série de tests suivante :
a) depuis une machine de Fos vers Bussy :
ping 10.192.1.254
vous obtenez le message **"Impossible de joindre l'hôte de destination ».**
b) depuis le serveur de fichiers de Lyon 10.0.1.1 vers Fos :
ping 10.128.1.254
vous obtenez le message **"Réponse de 10.128.1.254 : octets=32 temps<10 ms ...".**
c) depuis une machine utilisateur de Lyon vers Fos :
ping 10.128.1.254
vous obtenez le message **"Impossible de joindre l'hôte de destination".**
d) depuis une machine de Bordeaux vers Tarbes :
ping 10.130.1.254
vous obtenez le message **"Réponse de 10.130.1.254 : octets=32 temps<10 ms ...".**

3. Justifier les messages obtenus en réponse à chaque commande ping en analysant les tables de routage de l'annexe 4.
4. Proposer une solution pour empêcher les machines de Bordeaux de communiquer avec celles de Tarbes.

Au fur et à mesure de l'accroissement du nombre de sites connectés, les tables de routage des routeurs se sont complexifiées.

5. Proposer une solution pour réduire le nombre de lignes de la table de routage du routeur RLY2. Cette simplification ne doit pas modifier les règles de routage actuellement en place.

Les sites reçoivent souvent la visite de salariés itinérants qui utilisent leur ordinateur portable pour se connecter au réseau et travailler. C'est pourquoi il a été décidé de gérer de manière centralisée tout l'adressage IP de tous les postes clients de la SOVAMI à l'aide d'un serveur DHCP situé au siège de Lyon. Le service DHCP sera installé sur le serveur de fichiers. Dans chaque site, il existe un poste qui fait office de serveur d'impression. On souhaite que ce poste obtienne toujours la même adresse IP du serveur DHCP.

6. Indiquer quel service réseau doit être activé sur les routeurs pour que les postes des différents sites puissent obtenir une configuration IP du serveur DHCP.

7. Définir, pour le site de Lyon uniquement, l'étendue (plage d'adresses IP) qui est gérée par le serveur DHCP en précisant les exclusions strictement nécessaires.

8. Indiquer comment procéder pour que le serveur d'impression obtienne toujours la même adresse IP de la part du serveur DHCP.

Le routeur Internet nommé **«** RLY3 » a été installé par un prestataire de service qui a configuré sur l'interface 201.10.1.1 les règles de filtrage suivantes :

Table de filtrage de l'interface 201.10.1.1 du routeur « RLY3 » :

N° de règle	**Adresse source**	**Port source**	**Adresse destination**	**Port destination**	**Protocole transport**	**Action**
1	Toutes	Tous	201.10.1.10/32	80	TCP	Accepter
2	Toutes	Tous	201.10.1.10/32	53	Tous	Accepter
3	Toutes	Tous	201.10.1.11/32	25	Tous	Accepter
4	**Toutes**	**Tous**	**201.10.1.12/32**	**> 1024**	**Tous**	**Accepter**
5	201.10.1.8/29	Tous	Toutes	Tous	Tous	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Tous	Refuser

Table de correspondance entre les protocoles d'application et les ports TCP ou UDP

Protocole/application	**Port utilisé**
SMTP	25
HTTP	80
HTTPS	443
DNS	53
Telnet	23
SSH	22
POP3	110
IMAP	143

L'algorithme utilisé par le service de filtrage fonctionne selon le principe suivant :

Pour chaque paquet à traiter :

- En suivant l'ordre des règles de 1 à n, rechercher la première règle applicable,
- Si une des règles est applicable, alors appliquer l'action au paquet et arrêter le parcours de la table,

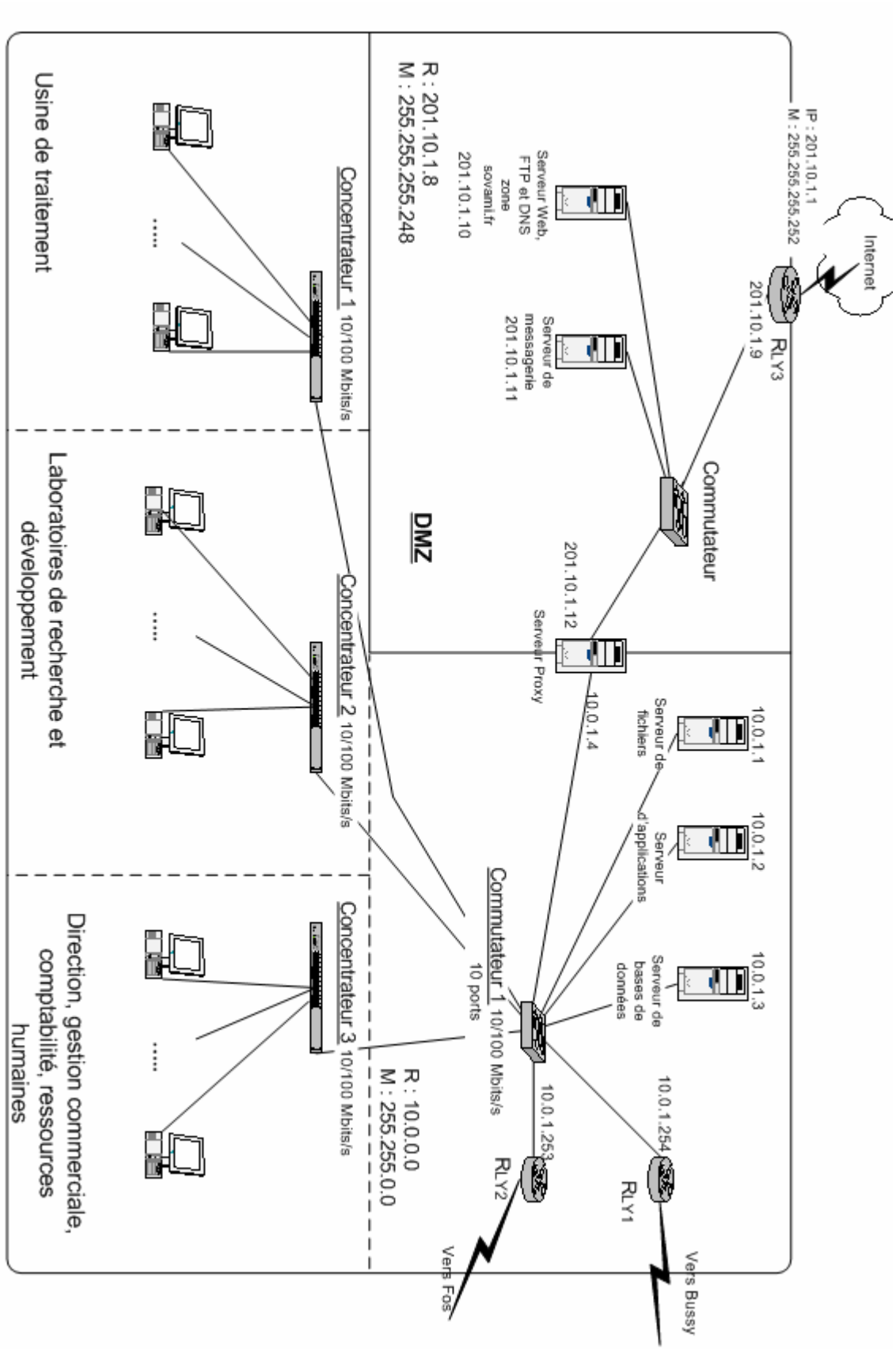
Si aucune règle n'est applicable, appliquer la règle par défaut.

9. Expliquer la règle de filtrage n° 4 et pourquoi le numéro de port de destination est supérieur à 1024.

Un utilisateur itinérant, qui consulte souvent ses messages électroniques depuis l'extérieur via des connexions RTC, par exemple à l'hôtel ou chez lui, se plaint qu'il ne peut pas rapatrier ses messages à l'aide de son logiciel client de messagerie habituel. Il accède à ses messages uniquement via son logiciel navigateur en mode « webmail », ceci au détriment du temps de connexion.

10. Expliquer la raison de l'impossibilité de l'utilisation du logiciel client de messagerie et proposer une solution à ce problème en intervenant sur les règles de filtrage.

Annexe 1 : Architecture du réseau local de la SOVAMI - site de Lyon



Annexe 2 : Présentation des réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce VLAN. Il existe différentes façons d'associer des trames et des ports à un VLAN, les principales sont les suivantes :

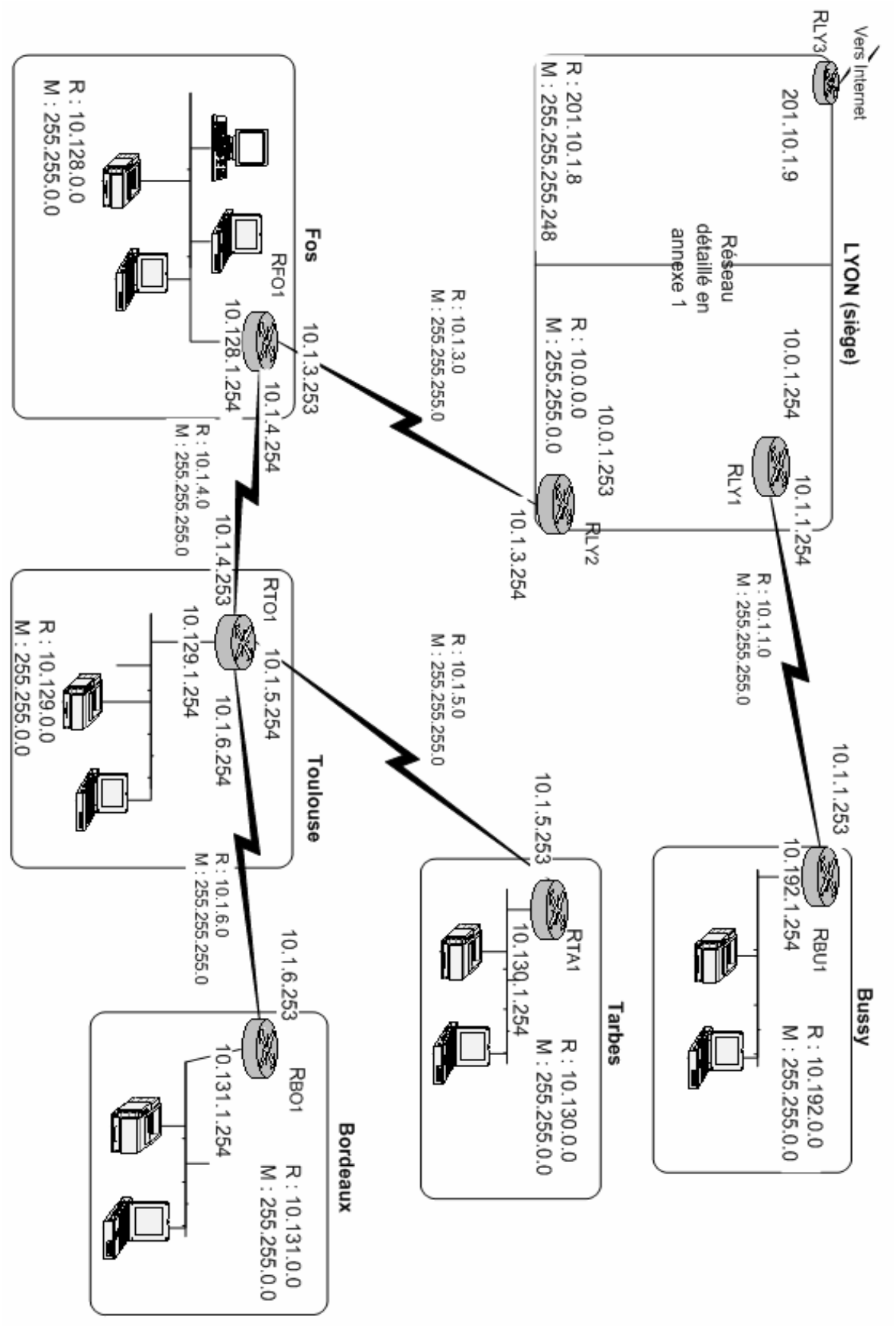
- **VLAN de niveau 1** ou VLAN par port : chaque port du commutateur est affecté à un VLAN, une trame en entrée sur ce port sera associée au VLAN du port.
- **VLAN de niveau 2** ou VLAN d'adresses MAC : chaque adresse MAC est affectée à un VLAN, donc chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse MAC émettrice contenue dans une trame en entrée sur ce port.
- **VLAN de niveau 3** ou VLAN d'adresses IP : chaque carte réseau est affectée à un VLAN en fonction de son adresse IP, donc chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse IP contenue dans le paquet transporté dans la trame en entrée.

Chaque VLAN peut être géré par un ou plusieurs commutateurs, un commutateur pouvant gérer plusieurs VLAN.

Les commutateurs identifient le VLAN auquel appartient une trame grâce au protocole 802.1q ; ils échangent ces trames via des ports d'interconnexion.

On considère qu'un port de commutateur ne sera associé qu'à un seul VLAN (à l'exception des ports d'interconnexion).

Annexe 3 : Architecture du réseau de la SOVAMI



Annexe 4 : Extrait du plan d'adressage et des tables de routage

Site ou liaison	Adresse réseau	Masque de sous-réseau
Lyon	10.0.0.0	255.255.0.0
Fos	10.128.0.0	255.255.0.0
Bussy	10.192.0.0	255.255.0.0
Toulouse	10.129.0.0	255.255.0.0
Tarbes	10.130.0.0	255.255.0.0
Bordeaux	10.131.0.0	255.255.0.0
RLY1-RBU1	10.1.1.0	255.255.255.0
RLY2-RFO1	10.1.3.0	255.255.255.0
RFO1-RTO1	10.1.4.0	255.255.255.0
RTO1-RTA1	10.1.5.0	255.255.255.0
RTO1-RBO1	10.1.6.0	255.255.255.0

Configuration des postes de travail dans chaque site

Site	Exemple d'adresse d'un poste	Masque	Routeur par défaut
Lyon - postes de travail	10.0.2.1	255.255.0.0	Pas de passerelle par défaut
Lyon - serveurs	10.0.1.1	255.255.0.0	10.0.1.253
Fos	10.128.1.1	255.255.0.0	10.128.1.254
Bussy	10.192.1.1	255.255.0.0	10.192.1.254
Toulouse	10.129.1.1	255.255.0.0	10.129.1.254
Tarbes	10.130.1.1	255.255.0.0	10.130.1.254
Bordeaux	10.131.1.1	255.255.0.0	10.131.1.254

Table de routage pour RLY2

Réseau	Masque	Routeur	Interface
10.0.0.0	255.255.0.0		10.0.1.253
10.1.3.0	255.255.255.0		10.1.3.254
10.128.0.0	255.255.0.0	10.1.3.253	10.1.3.254
10.129.0.0	255.255.0.0	10.1.3.253	10.1.3.254
10.130.0.0	255.255.0.0	10.1.3.253	10.1.3.254
10.131.0.0	255.255.0.0	10.1.3.253	10.1.3.254
10.192.0.0	255.255.0.0	10.0.1.254	10.0.1.253

Table de routage pour RFO1

Réseau	Masque	Routeur	Interface
10.0.0.0	255.255.0.0	10.1.3.254	10.1.3.253
10.1.3.0	255.255.255.0		10.1.3.253
10.1.4.0	255.255.255.0		10.1.4.254
10.128.0.0	255.255.0.0		10.128.1.254
10.129.0.0	255.255.0.0	10.1.4.253	10.1.4.254
10.130.0.0	255.255.0.0	10.1.4.253	10.1.4.254
10.131.0.0	255.255.0.0	10.1.4.253	10.1.4.254

Table de routage pour RTO1

Réseau	Masque	Routeur	Interface
10.0.0.0	255.255.0.0	10.1.4.254	10.1.4.253
10.1.4.0	255.255.255.0		10.1.4.253
10.1.5.0	255.255.255.0		10.1.5.254
10.1.6.0	255.255.255.0		10.1.6.254
10.129.0.0	255.255.0.0		10.129.1.254
10.130.0.0	255.255.0.0	10.1.5.253	10.1.5.254
10.131.0.0	255.255.0.0	10.1.6.253	10.1.6.254

Table de routage pour RTA1

Réseau	Masque	Routeur	Interface
0.0.0.0	0.0.0.0	10.1.5.254	10.1.5.253
10.1.5.0	255.255.255.0		10.1.5.253
10.130.0.0	255.255.0.0		10.130.1.254

Table de routage pour RBO1

Réseau	Masque	Routeur	Interface
0.0.0.0	0.0.0.0	10.1.6.254	10.1.6.253
10.1.6.0	255.255.255.0		10.1.6.253
10.131.0.0	255.255.0.0		10.131.1.254

La route par défaut sur les routeurs s'exprime à l'aide du numéro de réseau 0.0.0.0.

Corrigé Exonet N° 20

Question 1. Indiquer quel niveau de VLAN permet de prendre en charge l'isolement temporaire du réseau de la salle de réunion. Justifier la réponse.

On choisira le niveau 1 (VLAN par ports) en effet il suffira alors de modifier la configuration du commutateur pendant les réunions pour que les ports auxquels sont reliés les prises et la borne wi-fi ne soient pas affectés au VLAN donnant l'accès au réseau de l'entreprise
Le niveau 2 ne convient pas car il n'est pas facile de connaître les adresses MAC des portables des visiteurs. Par ailleurs, cette solution ne respecte pas la contrainte de lieu (accès limité à partir de la salle de réunion), en effet un ordinateur portable dont l'adresse MAC serait autorisée pourrait se connecter en dehors de la salle de réunion.
Le niveau 3 peut présenter un risque en terme de sécurité puisqu'une adresse IP valide peut être éventuellement choisie par un visiteur.

Question 2. Indiquer le nombre d'adresses IP encore disponibles dans le réseau IP de la zone "DMZ" du réseau. Justifier le résultat.

La zone DMZ a pour adresse de réseau 201.10.1.8 avec comme masque 255.255.255.248. Il y a donc 29 bits pour la partie réseau et 3 bits pour la partie hôte, soit 2^3-2= 6 adresses utilisables dans le réseau. 4 adresses sont déjà utilisées (3 serveurs et le 1 routeur), il reste donc **2 adresses IP disponibles**.

Question 3. Justifier les messages obtenus en réponse à chaque commande ping en analysant les tables de routage de l'annexe 4.

a) depuis une machine de Fos vers Bussy :

ping 10.192.1.254

vous obtenez le message **" Impossible de joindre l'hôte de destination ".**

Il n'y a pas de route vers le réseau de Bussy (10.192.0.0) ni de route par défaut dans la table de routage du routeur RFO1 (et idem pour RLY2). Le routeur envoie au poste une message ICMP indiquant que le destinataire est inaccessible.

b) depuis le serveur de fichiers de Lyon 10.0.1.1 vers Fos :

ping 10.128.1.254

vous obtenez le message **"Réponse de 10.128.1.254 : octets=32 temps<10 ms ...".**

Les routes sont bien définies entre le serveur de fichiers de Lyon et le réseau local de Fos. En effet les routeurs de Lyon ont comme passerelle par défaut 10.0.1.253(RLY2) RLY2 a une route indirecte vers 10.128.0.0 qui passe par le routeur 10.1.3.253 (RFO1) qui dessert directement le réseau de Fos. La route de retour ne pose pas de problème. La première ligne de la table de routage de RFO1 permet de retourner vers le réseau de Lyon Tant mieux puisque c'est ce que l'on veut !

c) depuis une machine utilisateur de Lyon vers Fos:

ping 10.128.1.254

vous obtenez le message **"Impossible de joindre l'hôte de destination".**

La communication est impossible entre une machine utilisateur de Lyon et le réseau local de Fos. La machine utilisateur ne possède pas de passerelle par défaut. Cela dénote là aussi une configuration conforme aux exigences (structure hiérarchique, les postes de Lyon n'ont pas besoin de routeur pour accéder aux serveurs de Lyon)).

d) depuis une machine de Bordeaux vers Tarbes:

ping 10.130.1.254

vous obtenez le message **"Réponse de 10.130.1.254 : octets=32 temps<10 ms ...".**
Les machines de Bordeaux peuvent atteindre le réseau local de Tarbes, ce qui ne devrait pas être possible (voir routeurs RTA1, RBO1 et RTO1). Les machines de bordeaux ont comme routeur 10.131.1.254 (RB01) . Celui-ci a une route par défaut qui renvoie à RT01 (10.1.6.254). RT01 a une route vers 10.130.0.0 via le routeur 10.1.5.253 (RTA1) . Les postes de Tarbes ont aussi une passerelle par défaut RTA1 qui dispose d'une route de retour vers Bordeaux via la route par défaut et le routeur RTO1.

Question 4. Proposer une solution pour empêcher les machines de Bordeaux de communiquer avec celles de Tarbes.

La configuration des routeurs **RTA1** et **RBO1** comporte une route par défaut qui rend accessible le réseau de Bordeaux pour le réseau de Tarbes et retour. La solution la plus simple pour répondre aux exigences de sécurité est de remplacer la ligne de la route 0.0.0.0 dans les routeurs RTA1 et RBO1 par une route qui permet l'accès au site de Lyon :
Pour RTA1 :

Réseau	**Masque**	**Routeur**	**Interface**
10.0.0.0	255.255.0.0	10.1.5.254	10.1.5.253

Et pour RBO1 :

Réseau	**Masque**	**Routeur**	**Interface**
10.0.0.0	255.255.0.0	10.1.6.254	10.1.6.253

Question 5. Proposer une solution pour réduire le nombre de lignes de la table de routage du routeur RLY2. Cette simplification ne doit pas modifier les règles de routage actuellement en place.

Le routeur RLY2 connaît la route de 4 réseaux dont les numéros sont consécutifs (10.128.0.0 à 10.131.0.0). Cela correspond pour le deuxième octet aux valeurs binaires 10000000 à 10000011, soit 6 bits communs.

Les 4 lignes concernant ces réseaux peuvent être condensées en une seule.

Réseau	**Masque**	**Routeur**	**Interface**
10.128.0.0	255.252.0.0	10.1.3.253	10.1.3.254

Les masques 255.192.0.0 à 255.252.0.0 sont également corrects.

Question 6. Indiquer quel service réseau doit être activé sur les routeurs pour que les postes des différents sites puissent obtenir une configuration IP du serveur DHCP.

Le service Agent de relais DHCP doit être activé pour relayer les requêtes DHCP des réseaux des sites vers le serveur DHCP du site de Lyon.

Question 7. Définir, pour le site de Lyon uniquement, l'étendue (plage d'adresses IP) qui est gérée par le serveur DHCP en précisant les exclusions strictement nécessaires.

Solution 1

Exclusions	**Étendue**
10.0.1.1 à 10.0.1.4 10.0.1.253 à 10.0.1.254	10.0.0.1 – 10.0.255.254 masque 255.255.0.0

Solution 2

Exclusions	**Étendue**
	10.0.0.1 – 10.0.1.0 masque 255.255.0.0 10.0.1.5 – 10.0.1.252 masque 255.255.0.0 10.0.1.255 – 10.0.255.254 masque 255.255.0.0

Question 8. Indiquer comment procéder pour que le serveur d'impression obtienne toujours la même adresse IP de la part du serveur DHCP.

Au niveau du serveur DHCP, il faut procéder à une **réservation**, c'est à dire associer l'adresse MAC de la carte réseau du serveur d'impression à l'adresse IP souhaitée.

Question 9. Expliquer la règle de filtrage 4 et pourquoi le numéro de port de destination est supérieur à 1024.

Cette ligne concerne l'accès depuis Internet au serveur proxy en réponse à des requêtes initiées par le serveur proxy à la demande des postes clients du réseau local, lesquels utilisent forcément un port supérieur à 1024 (Registered Ports) car de 0 à 1023 il s'agit des ports réservés à des processus système (Well Known Ports).
Les ports autorisés sont ceux qu'utilise le proxy pour les accès à Internet. On admettra les réponses qui indiquent que le proxy réalisant une translation d'adresses, les ports utilisés sont supérieurs à 1024.

Question 10. Expliquer la raison de l'impossibilité de l'utilisation du logiciel client de messagerie et proposer une solution à ce problème en intervenant sur les règles de filtrage.

L'accès au serveur de messagerie depuis l'extérieur est interdit pour un client de messagerie, car les protocoles POP3 (port 110) et IMAP (port 143) ne sont pas explicitement autorisés et sont donc bloqués par la règle de filtrage par défaut**.**

Pour l'autoriser, il faudrait ajouter la règle suivante :

N°	**Adresse source**	**Port source**	**Adresse destination**	**Port destination**	**Protocole transport**	**Action**
6	Toutes	Tous	201.10.1.11/32	110 ou 143	Tous	Accepter

EXONET N° 21

La société AHOLA est une société dont l'activité est centrée sur la conception d'équipements et de vêtements de surf. Elle emploie 74 personnes, chaque salarié est équipé d'un ordinateur. Les ordinateurs sont des machines de bureau. Toutes ces machines sont reliées au réseau local de l'entreprise.
Le réseau de distribution est constitué d'une centaine de concessionnaires implantés dans les principaux pays européens et de vingt agents commerciaux. Chacun d'eux dispose d'un ordinateur portable qui lui permet de se connecter à distance pour transmettre les commandes des clients et pour obtenir une mise à jour régulière des catalogues de produits. Les commerciaux viennent régulièrement travailler dans les locaux de l'entreprise.
Prenant conscience qu'il est temps de réorganiser totalement son réseau, l'administrateur décide d'étudier les principes d'une architecture Ethernet entièrement commutée et la mise en œuvre de réseaux locaux virtuels (VLAN).
Pour cela, il a fait l'acquisition d'un premier commutateur qu'il a relié provisoirement au réseau afin de l'étudier.
Sur ce commutateur, il a connecté différents concentrateurs comme le montre l'annexe 1.
Le commutateur mis en place peut gérer les réseaux locaux virtuels (VLAN), comme l'explique l'annexe 3.
Pour tester son commutateur, l'administrateur met en place provisoirement deux VLAN de niveau 1 (VLAN par ports). Les concentrateurs 3, 4 et 5 sont respectivement connectés au port 3, 4 et 5 du commutateur. L'administrateur déclare un VLAN pour le port 3 et 4 et un autre VLAN pour le port 5.
Avant cette manipulation, le poste de l'administrateur communiquait avec l'ensemble des serveurs et accédait à Internet sans problème.
à partir de son poste, l'administrateur exécute une commande qui vide son cache ARP puis exécute plusieurs commandes à l'aide de l'utilitaire ping.

1. Après la mise en place des VLAN, dire quel sera le message émis à l'issue de l'exécution des commandes suivantes émises par le poste de l'administrateur :

- **ping 192.168.1.2**
- **ping 192.168.1.5**
- **ping 195.26.36.2**

Justifier les réponses.

2. Dire quel sera le contenu du cache ARP du poste de l'administrateur à l'issue de ces trois commandes. Utiliser l'annexe 2 pour répondre à cette question.

Après son test sur le commutateur, l'administrateur est revenu à la configuration sans VLAN présentée en annexe 1.
Les adresses des machines du réseau 192.168.1.0, autres que les serveurs et les routeurs, sont attribuées dynamiquement. Le serveur DHCP est paramétré pour distribuer des adresses aux 74 machines de bureau. Mais il faut prévoir aussi des adresses supplémentaires pour les commerciaux qui peuvent avoir besoin de connexion réseaux dans les locaux du siège.
Pour des raisons de sécurité, l'administrateur veut impérativement limiter la plage d'adresses IP aux seules adresses indispensables, il a défini la configuration DHCP suivante :
Adresse de début : 192.168.1.10
Adresse de fin : 192.168.1.93
Masque de sous-réseau : 255.255.255.192
Durée du bail : 30 jours 0 heure 0 minute
Mais le serveur DHCP refuse la valeur du masque de sous-réseau.

3. Expliquer la cause de cet échec et proposer un nouveau masque.

Après rectification, toutes les stations obtiennent maintenant une adresse mais la configuration DHCP n'est pas complète.

4. Définir les paramètres DHCP permettant aux stations de se connecter à Internet et de résoudre les noms d'hôte internet.

On estime qu'au plus 10 commerciaux par semaine peuvent être amenés à se connecter simultanément au siège de la société. Ils branchent leur portable sur les prises RJ45 disponibles dans les bureaux et restent au maximum 3 jours sur le site.
La première semaine suivant la mise en place de la configuration DHCP, 5 commerciaux se sont connectés sans problème.
La deuxième semaine, 3 autres commerciaux se sont connectés.
La troisième semaine, 6 commerciaux ont tenté de se connecter mais certains ont échoué.

5. Expliquer la cause de cet échec et proposer une solution.

Le choix des adresses réseau 192.168.1.0 et 192.168.2.0 pour le réseau d'AHOLA a amené l'administrateur à installer le service NAT (service de translation d'adresses IP) sur le routeur 192.168.1.254.

6. Justifier la nécessité du service NAT.

Le serveur du fournisseur d'accès à Internet (FAI), poste 200.12.200.12, est utilisé comme serveur mandataire (proxy) et serveur de messagerie. Il a été paramétré pour livrer des messages (protocole POP sur le port 110) et envoyer des messages (protocole SMTP sur le port 25).
Tous les salariés de l'entreprise (y compris ceux du dépôt de Benesse-Maremne) sont autorisés à utiliser le protocole HTTP (port 80) pour consulter les sites web disponibles sur le Net.
Le tableau suivant donne le filtre mis en œuvre par l'administrateur sur le routeur pour que les serveurs web extérieurs à l'entreprise puissent répondre :

N° règle	Interface d'arrivée	Action	Source	Port source	Destination	Port destination
1	195.26.36.2	accepte	*	*	192.168.1.0	>1024
2	195.26.36.2	accepte	200.12.200.12	80	192.168.2.0	> 1024
3	192.168.1.254	accepte	*	*	200.12.200.12	80
4	192.168.2.254	accepte	*	*	*	80

Le filtre s'applique après les opérations de translation d'adresses sur les adresses réelles et non sur les adresses substituées.

La première règle (règle n° 1) s'interprète ainsi :
Sur l'interface d'arrivée 195.26.36.2, quelle que soient l'adresse IP source et le numéro de port source du paquet, on accepte tous les paquets à destination du réseau 192.168.1.0 et d'un numéro de port supérieur à 1024.

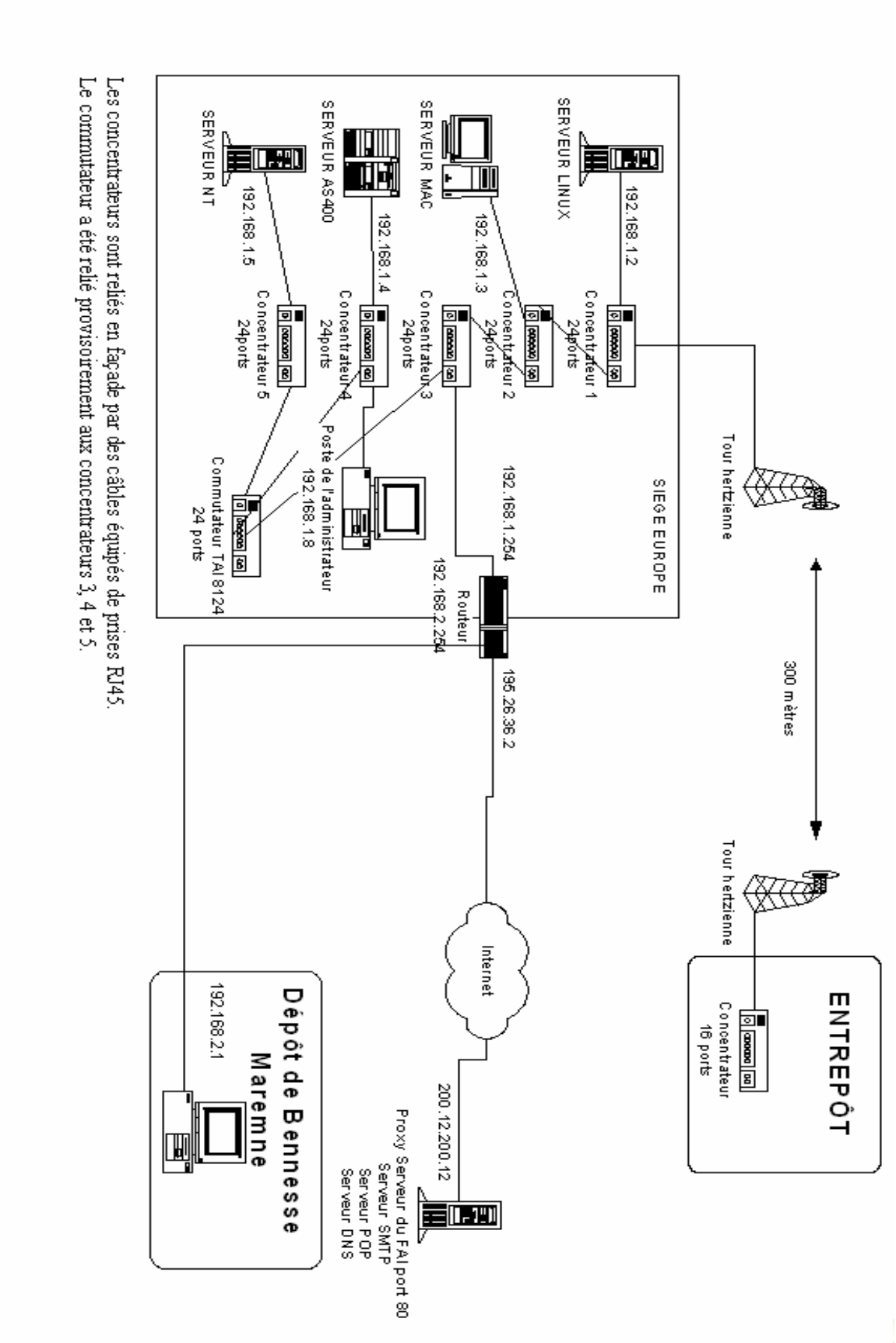
La deuxième règle (règle n° 2) s'interprète ainsi :
Sur l'interface d'arrivée 195.26.36.2, on accepte les paquets dont l'adresse IP source est 200.12.200.12, le port source 80 à destination du réseau 192.168.2.0 et d'un numéro de port supérieur à 1024.

Les règles générales de filtrage sont les suivantes :

- Pour chaque paquet qui transite par le routeur, les règles sont parcourues de la règle 1 à la règle 4.
- Dès qu'une règle s'applique, on arrête le parcours des règles.
- Tout ce qui n'est pas autorisé est interdit.

7.a. Dire en quoi les règles 1 et 2 expriment un fonctionnement différent en termes de sécurité et préciser quelle est la plus sûre.
7.b. Dire en quoi les règles 3 et 4 expriment un fonctionnement différent en termes de sécurité et préciser quelle est la plus sûre.
8. En respectant le formalisme proposé ci-dessus, rédiger la ou les règles qui permettent à tous les salariés de l'entreprise (dépôt de Benesse-Maremne compris) d'envoyer des messages électroniques (on ne tiendra pas compte des flux DNS et des flux POP ou IMAP).

Annexe 1 : Schéma du réseau



Les concentrateurs sont reliés en façade par des câbles équipés de prises RJ45.
Le commutateur a été relié provisoirement aux concentrateurs 3, 4 et 5.

Annexe 2 :Tableau de correspondance adresses IP adresses MAC

Adresses IP	Adresses MAC
192.168.1.2	**00-02-3f-23-9C-02**
192.168.1.3	**00-02-3f-23-3f-03**
192.168.1.4	**00-02-3f-23-40-04**
192.168.1.5	**00-02-3f-3a-80-05**
192.168.1.8	**00-02-3f-10-7d-08**
192.168.1.254	**00-02-3f-01-02-54**
192.168.2.254	**00-0b-cd-02-02-54**
195.26.36.2	**00-0b-cd-00-36-02**
200.12.200.12	**00-06-1b-02-00-12**

Annexe 3 : Principe de fonctionnement des réseaux locaux virtuels (VLAN)

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce VLAN. Il existe différentes façons d'associer des trames et des ports à un VLAN, les principales sont les suivantes :

- **VLAN de niveau 1** ou VLAN par port : chaque port du commutateur est affecté à un VLAN, une trame en entrée sur ce port sera associée au VLAN du port.
- **VLAN de niveau 2** ou VLAN d'adresses MAC : chaque adresse MAC est affectée à un VLAN, donc chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse MAC émettrice contenue dans une trame en entrée sur ce port.
- **VLAN de niveau 3** ou VLAN d'adresses IP : chaque carte réseau est affectée à un VLAN en fonction de son adresse IP, donc chaque port du commutateur se voit affecté dynamiquement à un VLAN en fonction de l'adresse IP contenue dans le paquet transporté dans la trame en entrée.

Chaque VLAN peut être géré par un ou plusieurs commutateurs, un commutateur pouvant gérer plusieurs VLAN.

Les commutateurs identifient le VLAN auquel appartient une trame grâce au protocole 802.1q ; ils échangent ces trames via des ports d'interconnexion.

On considère qu'un port de commutateur ne sera associé qu'à un seul VLAN (à l'exception des ports d'interconnexion).

Corrigé Exonet N° 21

Question 1. Après la mise en place des VLAN, dire quel sera le message émis à l'issue de l'exécution des commandes suivantes émises par le poste de l'administrateur :
- ping 192.168.1.2
- ping 192.168.1.5
- ping 195.26.36.2

Justifier les réponses.

Chaque ping sera précédé d'une requête ARP qui résoudra l'adresse IP en adresse MAC. Une requête ARP est transmise par une trame de diffusion. Chaque VLAN constitue un domaine de diffusion.
La commande "ping 192.168.1.2" aura des réponses "reply" car la requête de diffusion ARP parvient au poste 192.168.1.5 et l'échange ICMP echo/reply peut donc se faire. 192.168.1.2 fait partie du même VLAN que le poste de l'administrateur.
La réponse à la commande "ping 192.168.1.5" sera "délai d'attente dépassé" car la requête de diffusion ARP ne parvient pas au poste 192.168.1.5 qui ne fait pas partie du même VLAN que le poste de l'administrateur.
La réponse à la commande "ping 195.26.36.2" aura des réponses "reply" car la requête de diffusion ARP parvient au routeur 192.168.1.254 qui fait partie du même VLAN que le poste de l'administrateur

Question 2. Dire quel sera le contenu du cache ARP du poste de l'administrateur à l'issue de ces trois commandes. Utiliser l'annexe 2 pour répondre à cette question.

On trouvera dans le cache ARP les associations suivantes :
00-02-3f-23-9c-02 192.168.1.2
00-02-3f-01-02-54 192.168.1.254 // correspondant au ping 195.26.36.2 qui provoque le renvoi de l'adresse MAC du routeur
00-02-3f-3a-80-05 192.168.1.5 // cette association ne doit pas se trouver dans le cache ARP

Question 3. Expliquer la cause de cet échec et proposer un nouveau masque.

Le masque ne permet pas de gérer les 84 adresses que prétend offrir la plage d'adressage (6 bits dans la partie host → 64 – 2 = 62 adresses hosts). Il faut changer le masque. Les deux masques permettant de gérer au moins 84 adresses sont 255.255.255.0 et 255.255.255.128. Comme le routeur a pour adresse 192.168.1.254, et que l'adresse du réseau est 192.168.1.0 seul le masque 255.255.255.0 est acceptable.

Question 4. Définir les paramètres DHCP permettant aux stations de se connecter à Internet et de résoudre les noms d'hôte internet.

Il faut renvoyer l'adresse 192.168.1.254 pour le routeur et 200.12.200.12 comme adresse de serveur DNS.

Question 5. Expliquer la cause de cet échec et proposer une solution.

La plage d'adresses disponibles pour DHCP propose 84 adresses ; 74 postes de travail utilisent en permanence une adresse dynamique. La première semaine, 5 commerciaux pourront donc se connecter au réseau du siège sans soucis, la deuxième semaine trois autres. En revanche, la troisième semaine, seuls 2 des 6 commerciaux réussiront à se connecter. En effet, comme le bail est de trente jours, les adresses n'ont pas été libérées.
Il faut diminuer la durée du bail pour que les adresses soient libérées (attention car le renouvellement se fait avant l'expiration).

Question 6. Justifier la nécessité du service NAT.

Pour assurer la sécurité de son réseau, l'opérateur lui a conseillé d'opter pour des adresses de réseau privé. Ces adresses ne sont pas routables sur Internet. Il faut donc substituer, dans tous les paquets IP, ces adresses par des adresses routables. C'est ce que fait le service NAT sur le routeur. Ce service prend une adresse IP dans une plage d'adresses sur son réseau (195.26.36.0), ces adresses sont obligatoirement des adresses publiques.

Question 7.a. Dire en quoi les règles 1 et 2 expriment un fonctionnement différent en termes de sécurité et préciser quelle est la plus sûre.
Question 7.b. Dire en quoi les règles 3 et 4 expriment un fonctionnement différent en termes de sécurité et préciser quelle est la plus sûre.

En autorisant l'adressage des ports supérieurs à 1024, la première règle autorise des flux autres qu'en provenance de HTTP. La deuxième règle autorise des échanges avec le proxy sur le port 80 uniquement. La deuxième règle est donc plus sûre que la première.
La quatrième règle autorise des échanges HTTP qui ne passent pas par le proxy. La troisième règle est donc plus sûre.

Question 8. En respectant le formalisme proposé ci-dessus, rédiger la ou les règles qui permettent à tous les salariés de l'entreprise (dépôt de Benesse-Maremne compris) d'envoyer des messages électroniques (on ne tiendra pas compte des flux DNS et des flux POP ou IMAP).

N° règle	Interface d'arrivée	Action	Source	Port source	Destination	Port destination
1	195.26.36.2	accepte	*	*	192.168.1.0	>1024
2	195.26.36.2	accepte	200.12.200.12	80	192.168.2.1	
3	192.168.1.254	accepte		*	200.12.200.12	80
4	192.168.2.254	accepte		*		80
5	**195.26.36.2**	**accepte**	**200.12.200.12**	**25**	**192.168.0.0/16**	**>1024**
6	**192.168.1.254**	**accepte**	**192.168.1.0/24**	*****	**200.12.200.12**	**25**
7	**192.168.2.254**	**accepte**	**192.168.2.0/24**	*****	**200.12.200.12**	**25**

La notation employée sur les règles 5 est optimisée avec un supernetting, ce n'est pas bien sûr la notation exigée. Cette ligne peut être décomposée en deux lignes prenant en compte les réseaux 192.168.1.0 et 192.168.2.0.

EXONET N° 22

Le groupe polymousse est spécialisé dans la fabrication et la transformation de mousse de polyuréthanne.
Employant quelque 3 000 collaborateurs, le groupe polymousse est principalement présent sur le marché français mais il a récemment racheté dans différents pays plusieurs sociétés qui sont devenues des succursales.
La répartition de l'effectif des collaborateurs du groupe est désormais la suivante :
- France : 1 500
- Espagne : 800
- Allemagne : 400
- Belgique : 300

Cette évolution majeure nécessite de réaliser l'intégration des différents systèmes d'information présents au sein du groupe. Le système d'information (SI) ainsi obtenu doit garantir la disponibilité des applications informatiques dans l'ensemble du groupe.
Après l'acquisition des différentes succursales, le groupe polymousse est organisé en quatre divisions : France, Espagne, Allemagne et Belgique.
Chaque division regroupe plusieurs succursales :
- l'Espagne compte trois succursales,
- l'Allemagne huit succursales,
- la Belgique quatre succursales,
- la France comporte une succursale qui héberge les applications du groupe.

Dans un premier temps, les administrateurs du groupe désirent harmoniser le plan d'adressage pour l'ensemble des divisions. L'organisation du réseau et le plan d'adressage retenu pour le groupe polymousse sont décrits en annexe 1.
Pour optimiser les tables de routage, on utilise un plan d'adressage dans lequel chaque division se voit attribuer un sous-réseau dans le réseau d'adresse 10.0.0.0, qu'elle subdivise à son tour en sous-réseaux pour ses succursales.
La division Espagne doit regrouper à terme jusqu'à 11 succursales réparties sur l'ensemble du territoire de ce pays.

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.**
2. **Calculer le nombre maximum de divisions que le plan d'adressage permet de définir.**
3. **Donner le masque de sous-réseau qui permet d'adresser les 11 sous-réseaux des succursales de la division Espagne. Justifier la réponse.**
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.**
5. **Donner les lignes de la table de routage du routeur nommé R.Central qui donne accès à l'ensemble des divisions du groupe dans tous les pays.**

Après la mise en œuvre du plan d'adressage global au sein du groupe, il s'avère nécessaire de mettre en place un service privé de résolution de nom DNS. L'architecture DNS présentée en **annexe 2**, doit permettre de nommer les différents serveurs du groupe qui sont répartis sur l'ensemble des Divisions.

Le domaine appelé « polynet » constitue la racine du domaine privé du groupe. Chaque division gère son propre sous domaine et porte l'extension du pays. Ainsi la Belgique disposera du sous domaine « be.polynet »

6. Expliquer le principe et l'intérêt de la délégation de zone dans le système de résolution de nom DNS.
7. Donner l'adresse IP et le nom du serveur DNS sur lequel doit être défini le nom d'hôte sap.be.polynet. Expliquer ce choix.
8. Proposer une solution permettant d'améliorer la tolérance aux pannes du service DNS d'une division.

L'administrateur du réseau de la division France désire limiter les flux de diffusion aux services. Le commutateur installé permet de mettre en place une configuration basée sur les VLAN, dont le principe et les niveaux sont présentés en annexe 3. Dans un premier temps, l'administrateur ne prend pas en compte les problèmes liés à l'adressage IP. Il se demande si cette opération peut être réalisée immédiatement en conservant les concentrateurs existants.
9. Donner le nombre de domaines de collision et le nombre de domaines de diffusion présents dans le réseau de la division France avant la mise en place des VLAN. Justifier la réponse.
10. Expliquer s'il est possible d'isoler les flux des services en conservant les concentrateurs existants.

Dans l'étude menée pour l'interconnexion des réseaux des différentes divisions, il a été décidé que chaque division gérerait son propre accès à Internet.
Dans un premier temps on s'intéresse à la gestion de l'accès Internet du siège. Les administrateurs ont mis en place l'architecture représentée en annexe 4. Celle-ci est constituée d'un routeur filtrant (nommé RF) et d'un serveur mandataire (nommé proxy) pour le service HTTP. Ce serveur mandataire analyse les URL demandées pour ne retenir que celles qui ne comportent pas certains mots et qui n'appartiennent pas à une liste régulièrement mise à jour. Le routeur filtrant ne gère pas automatiquement les flux de retour.
L'ensemble du personnel à l'exception du poste de l'administrateur doit accéder à l'Internet en utilisant le serveur mandataire.

Règles de filtrage définies actuellement sur le routeur filtrant RF (interface S0)

règle	direction	IP source	Port source	IP destination	Port destination	Action
1	Sortie	10.1.0.50 / 32	Tous	Tous	Tous	Router
2	Entrée	Tous	Tous	10.1.0.50 /32	Tous	Router
3	Sortie	Tous	Tous	Tous	Tous	Bloquer
4	Entrée	Tous	Tous	Tous	Tous	Bloquer

11. Comparer la nature des actions de filtrage que peuvent réaliser le routeur filtrant RF d'une part et le serveur mandataire d'autre part, en prenant appui sur le modèle OSI.
12. Expliquer le rôle et l'ordonnancement des règles de filtrage définies sur le routeur RF.
13. Insérer correctement des nouvelles règles dans la table de filtrage de RF de façon à permettre au serveur mandataire de communiquer sur le web, sans tenir compte des flux DNS.
14. Indiquer la configuration requise sur les postes clients du siège pour leur permettre d'accéder à Internet avec le protocole HTTP.

L’infrastructure réseau du groupe polymousse permettant de relier l’ensemble des divisions au siège est actuellement construite sur des liaisons internationales louées à haut débit. Toutes les garanties de sécurité exigées par le groupe sont prises en charge par cette infrastructure, mais l’extension du groupe devrait augmenter considérablement les coûts de location des liaisons.
La solution envisagée prévoit l’exploitation du réseau public Internet avec une mise en œuvre de Réseaux Privés Virtuels (RPV, ou Virtual Private Network, ou VPN).
Dans un premier temps, une solution RPV va être testée entre les divisions France et Belgique qui disposent de routeurs implémentant les fonctions de RPV.

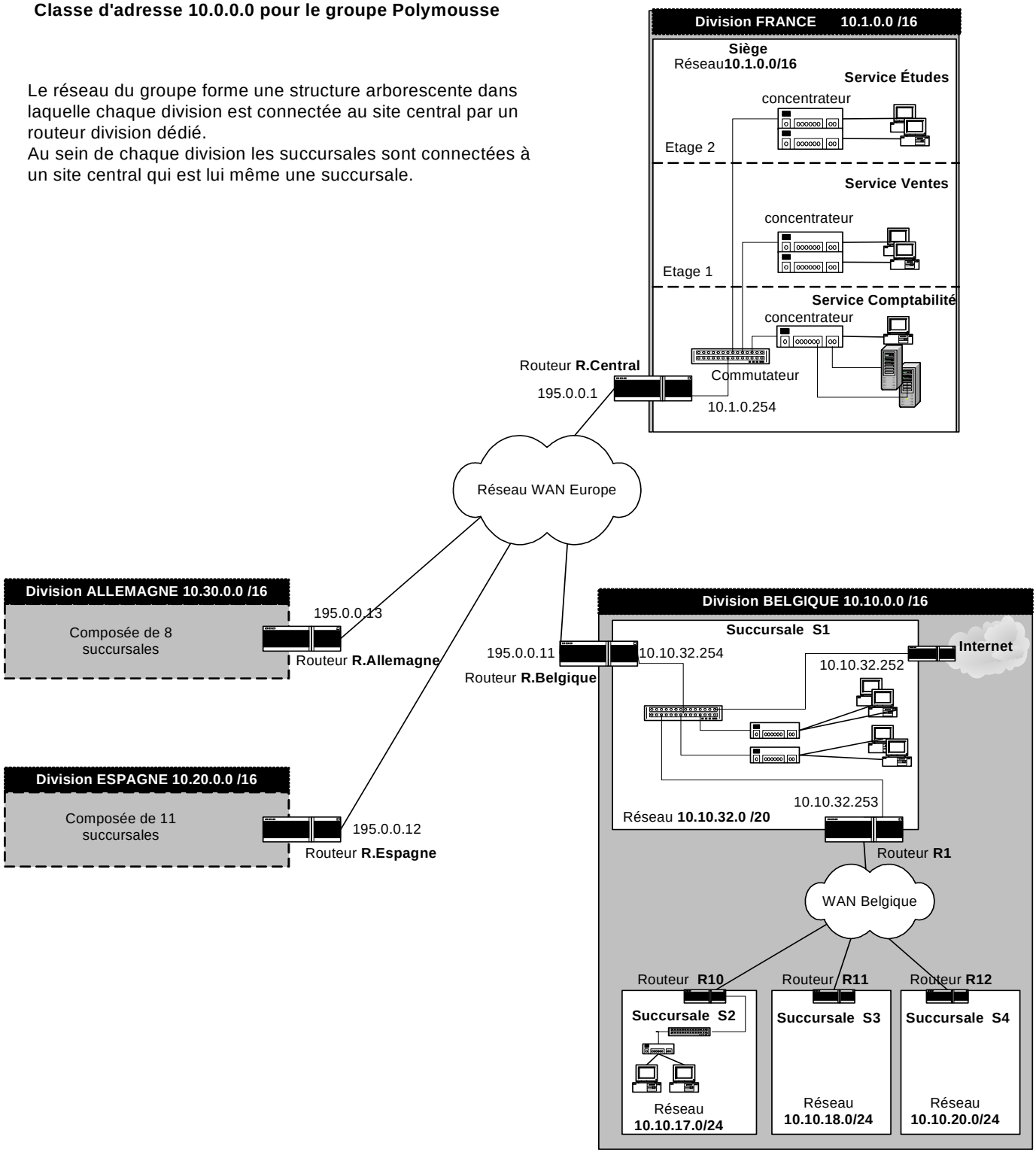
15. Décrire les différentes garanties qu’offrent les mécanismes de signature et de chiffrement.

16. Indiquer les clés nécessaires dans chacune des divisions en précisant leur rôle.

Annexe 1 : architecture du réseau du groupe POLYMOUSSE

Classe d'adresse 10.0.0.0 pour le groupe Polymousse

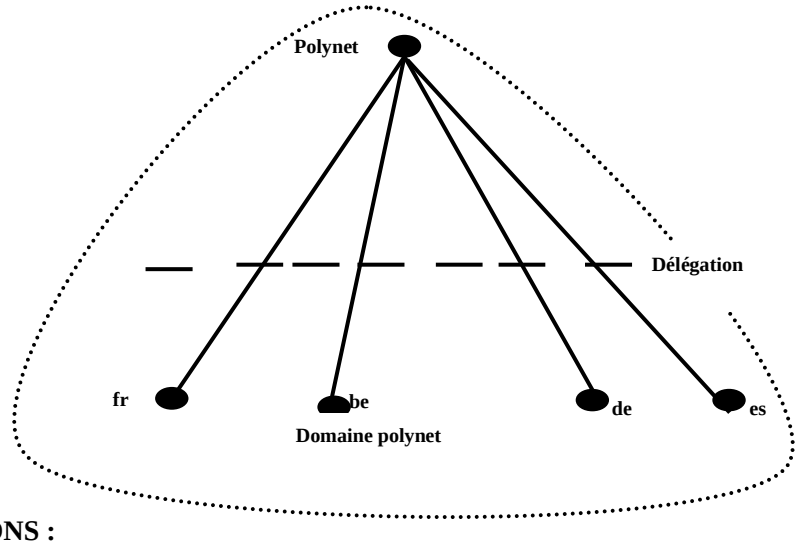
Le réseau du groupe forme une structure arborescente dans laquelle chaque division est connectée au site central par un routeur division dédié.
Au sein de chaque division les succursales sont connectées à un site central qui est lui même une succursale.



Extrait de la table de routage du routeur **R. Belgique**

ligne	Adresse réseau	Passerelle	Interface
1	10.10.16.0/20	10.10.32.253	10.10.32.254
2	10.10.32.0/20	10.10.32.254	10.10.32.254
…	…	…	…
n	défaut	10.10.32.252	10.10.32.254

Annexe 2 : organisation DNS du groupe



Liste des serveurs DNS :

pays	Zone	fonction	Nom du serveur	adresse IP
Belgique	**be.polynet**	**Primaire**	**dns.be. polynet**	**10.10.32.2**
Allemagne	**de. polynet**	**Primaire**	**dns.de. polynet**	**10. 30.32.2**
Espagne	**es. polynet**	**Primaire**	**dns.es. polynet**	**10. 20.32.2**
France	**fr. polynet**	**Primaire**	**dns.fr. polynet**	**10.1.0.2**
France	**polynet**	**Primaire**	**Racine.polynet**	**10.1.0.1**

Annexe 3 : présentation des réseaux locaux virtuels

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce Vlan. Il existe différentes façons d'associer des ports à un VLAN, les principales sont les suivantes :

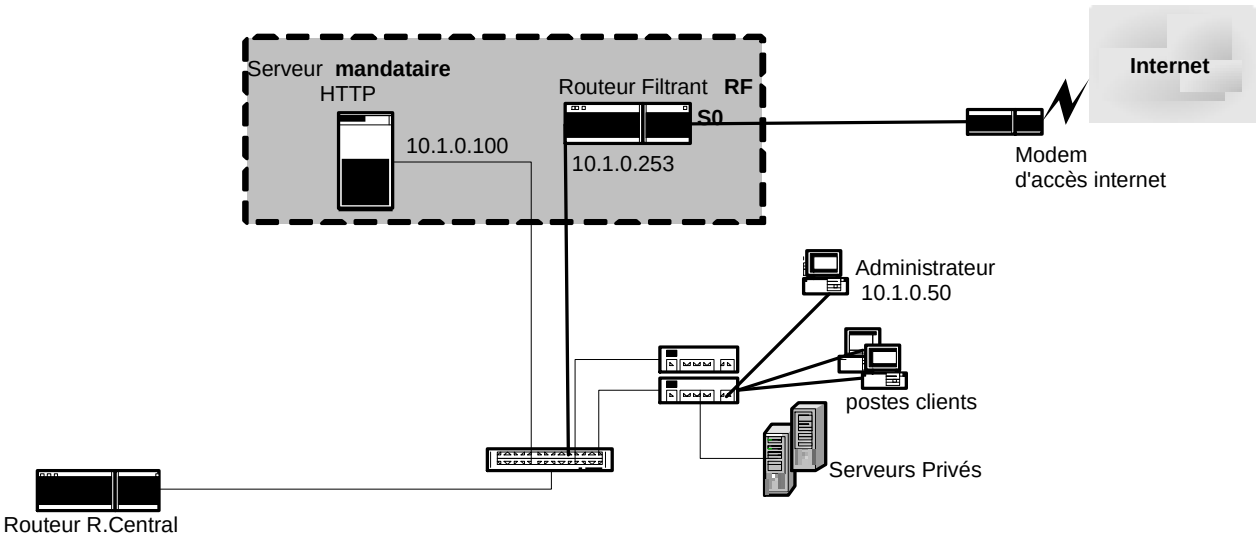
- **VLAN de niveau 1** ou VLAN par port : chaque port du commutateur est affecté à un VLAN, donc chaque carte réseau est affectée à un VLAN en fonction de son port de connexion.
- **VLAN de niveau 2** ou VLAN d'adresses MAC : chaque adresse MAC est affectée à un VLAN, donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse MAC de la carte réseau qui y est connectée.
- **VLAN de niveau 3** ou VLAN d'adresses IP : chaque carte réseau est affectée à un VLAN en fonction de son adresse IP, donc chaque port du commutateur se voit affecter dynamiquement à un VLAN en fonction de l'adresse IP de la carte réseau qui y est connectée

Chaque VLAN peut être géré par un ou plusieurs commutateurs, un commutateur peut gérer plusieurs VLAN.

Les commutateurs identifient le VLAN auquel appartient une trame grâce au protocole 802.1q, ils échangent ces trames via des ports d'interconnexion.

En pratique, un port de commutateur ne sera associé qu'à un seul VLAN (à l'exception des ports d'interconnexion).

Annexe 4 : architecture du réseau pour l'accès à l'Internet



Corrigé Exonet N° 22

Question 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.

Question 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.

Question 3. Donner le masque de sous réseau qui permet d'adresser les 11 sous réseaux des succursales de la division Espagne.

- 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

Question 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

Question 5. Donner les lignes de la table de routage du routeur nommé R.Central qui donne accès à l'ensemble des divisions du groupe dans tous les pays.

Table de routage du routeur **R.Central**

Adresse réseau	Passerelle	Interface
10.1.0.0 /16	10.1.0.254	10.1.0.254
10.30.0.0 /16	195.0.0.13	195.0.0.1
10.20.0.0 /16	195.0.0.12	195.0.0.1
10.10.0.0 /16	195.0.0.11	195.0.0.1

Question 6. Expliquer le principe et l'intérêt de la délégation de zone dans le système de résolution de nom DNS.

- Permet de diviser l'espace de noms et de déléguer la gestion d'une partie de l'espace de nom DNS à chaque Division. L'extension de l'espace de noms sera ainsi simplifiée et sous la responsabilité de chaque Division. La modification d'un nom d'hôte sera réalisée par la division qui gère la zone concernée.

Question 7. Donner l'adresse IP du serveur DNS sur lequel doit être défini le nom d'hôte, SAP.be.polynet. Expliquez ce choix.

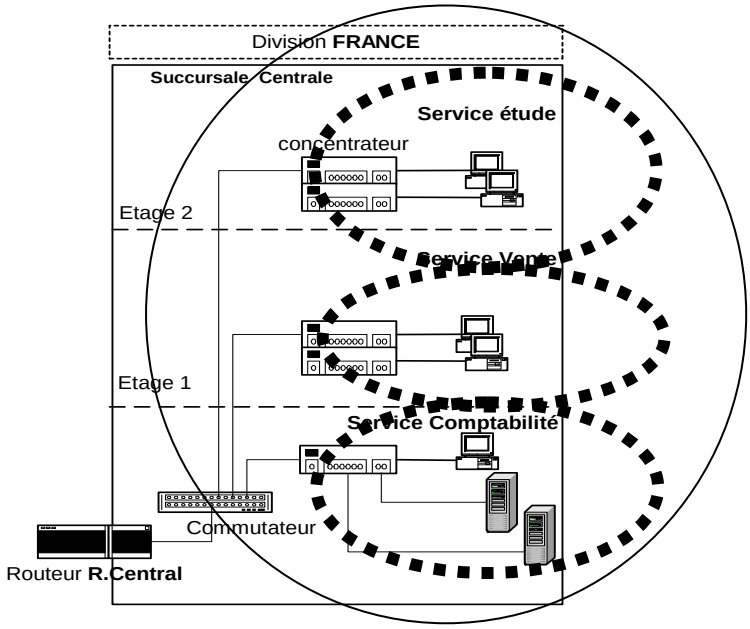
- Le nom d'hôte **sap.be.polynet** est situé dans le sous-domaine **be.polynet**. Le serveur primaire qui gère cette zone est situé en Belgique. Il a pour adresse IP 10.10.32.2 et pour nom dns.be.polynet.

Question 8. Proposer une solution permettant d'améliorer la tolérance aux pannes du service DNS d'une division.

- Un serveur DNS supplémentaire peut être rajouté au niveau de chaque succursale permettant ainsi d'offrir une redondance de zone. Les informations de zone seront répliquées sur chacun d'eux.
- Une autre solution consiste à utiliser le serveur racine (parent) de la zone Polynet pour répliquer l'ensemble des zones.

Question 9. Donner le nombre de domaines de collision et le nombre de domaines de diffusion présents dans le réseau de la division France avant la mise en place des VLAN. Justifier la réponse.

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

Question 10. Expliquer s'il est possible d'isoler les flux des services en conservant les concentrateurs existants.

Pour isoler les trois services, il est donc nécessaire de créer trois VLAN.
Tous les postes d'un service doivent appartenir au même VLAN pour communiquer ensemble. Ces postent sont reliés par des concentrateurs connectés sur un port du commutateur. Ces ports doivent donc être affectés à un VLAN.
Il est donc possible de conserver les concentrateurs existants. La solution est de configurer des VLAN de niveau 1 sur le commutateur existant en affectant le numéro de Vlan du service au port connecté au concentrateur du service. Mais le fait de conserver les concentrateurs impose que tous les postes appartiennent au même VLAN.

Remarque : le port connecté vers le routeur Central peut être affecté au même VLAN que celui correspondant au service comportant les serveurs accessibles depuis les autres Divisions.
Les VLAN de niveau 2 : nécessitent dans cette configuration de saisir toutes les adresses MAC des postes pour les affecter à un VLAN, mais dans cette configuration (avec concentrateur), c'est inutile. Un port appartient à un seul Vlan (non 802.1q), donc toutes les adresses appartiennent au VLAN correspondant au port connecté au concentrateur.
Les VLAN de niveau 3 : l'affectation des vlan dépend de l'adresse Ip d'un réseau. Même remarque que pour le niveau 2 avec les concentrateurs.
La question demande de ne pas prendre en compte les problèmes liés à l'adressage Ip. En effet, si la communication inter-VLAN est autorisée, il faut passer par la mise en place d'un routeur (avec une interface sur chaque VLAN) et donc des adresses réseaux différentes pour chaque VLAN.

Question 11. Comparer la nature des actions de filtrage que peuvent réaliser le routeur filtrant RF d'une part et le serveur mandataire d'autre part, en prenant appui sur le modèle OSI.

Le routeur filtrant agit aux niveaux 3 et 4 du modèle OSI. Les filtres sont basés sur l'analyse des adresses IP source et destination et les ports de protocole. Il n'est capable ni de comprendre le contexte du service qu'il rend, ni d'identifier le demandeur du service.
Le serveur mandataire agit au niveau application du modèle OSI. Le filtrage se situe donc au niveau applicatif. Les règles de filtrage peuvent être plus élaborées (discriminantes) et faire référence à l'identité de l'utilisateur ou à la nature du service fourni.

Question 12. Expliquer le rôle et l'ordonnancement des règles de filtrage définies sur RF.

Les règles 1 et 2 permettent au poste de l'administrateur d'adresse IP 10.1.0.50 d'accéder à tous les services disponibles sur Internet.
La règle 3 bloque en sortie tout autre trafic de façon à ce qu'il faille passer par le serveur mandataire (proxy) pour accéder à Internet.
La règle 4 bloque en entrée tout autre trafic provenant d'Internet.
Les règles 1 et 2 sont placées avant les règles 3 et 4 qui bloquent tout le trafic

Question 13. Insérer correctement des nouvelles règles dans la table de filtrage de RF de façon à permettre au serveur mandataire de communiquer sur le web, sans tenir compte des flux DNS.

Règle	direction	IP source	Port source	IP destination	Port destination	Action
1	Sortie	10.1.0.50 /32	Tous	Tous	Tous	Router
2	Entrée	Tous	Tous	10.1.0.50 /32	Tous	Router
3	**Sortie**	**10.1.0.100 /32**	**Tous**	**Tous**	**80 / HTTP**	**Router**
4	**Entrée**	**Tous**	**80 / HTTP**	**10.1.0.100 /32**	**Tous**	**Router**
5	Sortie	Tous	Tous	Tous	Tous	Bloquer
6	Entrée	Tous	Tous	Tous	Tous	Bloquer

Question 14. Indiquer la configuration requise sur les postes clients du siège pour leur permettre d'accéder à Internet avec les protocoles HTTP.

Il convient d'indiquer au niveau des applications, voire au niveau du système d'exploitation, que les accès se font via un serveur mandataire (**proxy**) dont on indiquera l'adresse IP ou le nom.

Question 15. Décrire les différentes garanties qu'offrent les mécanismes de signature et de chiffrement.

Les mécanismes de signature et de chiffrement permettent d'assurer les fonctions de confidentialité, d'authentification, de non-répudiation et d'intégrité.

- Le chiffrement assure la confidentialité : l'information échangée entre deux entités du réseau, ne doit pas être intelligible pour une tierce personne qui serait à l'écoute ou récupérerait le message.
- L'action de signer assure authentification et imputabilité (non-répudiation).
    - L'authentification (ou identification) permet de prouver que la provenance de l'information est bien celle qu'elle dit être.
    - La non-répudiation (ou non-désaveu) concerne la validité juridique des signatures. Émetteur et récepteur ne pourront nier l'émission et la réception de l'objet.
- Le chiffrement assure l'intégrité : le destinataire est assuré que l'information qui lui parvient est bien l'information qui a été transmise.

Question 16. Indiquer les clés nécessaires dans chacune des divisions en précisant leur rôle.

Lors d'un échange entre la succursale S1 et le siège, S1 utilisera la clé publique du destinataire (le siège) pour chiffrer le message. Puis le siège utilisera à réception sa clé privée pour déchiffrer. En outre S1 peut utiliser sa propre clé privée pour signer son envoi et garantir ainsi l'authentification du message. Toute transmission à l'initiative du siège générera un processus inverse quant à la mise en œuvre des clés.(chiffrage avec la clé publique de S1 qui déchiffrera avec sa propre clé privée, le siège utilisant éventuellement sa clé privée pour signer son envoi).

EXONET N° 2B

Le Conseil Général rassemble 43 élus. Il emploie environ 1 500 personnes dont 19 au service informatique, basé à la cité administrative.
L'infrastructure réseau se compose principalement d'une vingtaine de serveurs et environ d'un millier de postes de travail répartis sur plusieurs sites.
Le réseau dispose
-d'une zone démilitarisée (DMZ) publique comportant :
- un serveur DNS maître pour la zone cg96.fr, le serveur secondaire (esclave) étant hébergé par le fournisseur d'accès ;
- un serveur relais de messagerie/anti-virus de messagerie ;
- un serveur web public (www.cg96.fr).

-d'un réseau privé où sont situés :
- des serveurs d'infrastructure (DNS, DHCP, WWW, messagerie SMTP et POP3, annuaires d'authentification, serveurs de fichiers et d'impression, SGBD) ;
- des serveurs applicatifs ;
- les postes de travail.

L'organisation logique TCP/IP est basée sur le domaine Internet **cg96.fr**. L'adressage est effectué par des serveurs DHCP.

L'administratrice du réseau, Mme Simonet, veut mettre en place une infrastructure Wifi dans la salle du Conseil pour que les élus et les visiteurs, essentiellement des journalistes, puissent accéder à Internet depuis leur ordinateur portable lors des sessions du Conseil général.
Pour cela, elle dispose d'un point d'accès Wifi qui propose deux SSID (identifiant de réseau physique) associés chacun à un VLAN par le commutateur Wifi, ce qui permet la séparation complète des réseaux.
Le premier SSID n'est pas diffusé sur le réseau. Il est paramétré sur les portables des élus du CG96. Ce SSID a été configuré par le service informatique pour n'autoriser que certaines adresses MAC.
Le second SSID est diffusé sur le réseau. Il ne dispose d'aucune sécurité particulière et permet une connexion implicite pour un poste de travail configuré de manière standard. Les postes de travail utilisant ce SSID accèderont à Internet au moyen d'un accès ADSL classique. Les adresses MAC des portables des élus sont interdites sur ce SSID.
L'adressage sera effectué par deux serveurs DHCP (un pour chaque VLAN).
Le point d'accès est relié à un commutateur qui gère des VLAN. Selon la configuration d'un poste de travail portable, celui-ci se connectera sur le VLAN 1 (Élus) ou sur le VLAN 2 (Visiteurs).

1. Dire pourquoi les portables des visiteurs qui se connectent sur le second SSID obtiendront obligatoirement une adresse IP donnée par le serveur DHCP 192.168.1.33 et non par le serveur DHCP 172.16.108.2. Justifier la réponse en vous appuyant sur le protocole DHCP et les VLAN.

Pour le réseau VLAN2 (Visiteurs), Mme Simonet souhaite mettre en oeuvre un plan d'adressage IP limitant à 13 le nombre d'adresses hôtes utilisables dans le réseau. Le serveur DHCP d'adresse 192.168.1.33 fera aussi office de routeur NAT.

2. Donner en la justifiant la valeur du masque de sous-réseau en notation classique et en notation CIDR.

3. Donner la plage d'adresses utilisables par le serveur DHCP ainsi que les différents paramètres TCP/IP nécessaires au fonctionnement des postes de travail du réseau VLAN2 (Visiteurs).

Après avoir paramétré le serveur DHCP du VLAN 1 (Élus), Mme Simonet teste la connexion avec la cité administrative au moyen de commandes ping depuis un portable d'élu disposant de l'adresse 172.16.108.10 et dont la passerelle par défaut est 172.16.108.1. Les liaisons sont opérationnelles et les postes et routeurs sont actifs. Elle exécute les deux commandes suivantes.

ping 172.16.4.10

Réponse de 172.16.108.1 : impossible de joindre l'hôte de destination

le message sous Linux serait : Network Unreachable)

ping 192.168.8.1

Délai d'attente de la demande dépassé (le message sous Linux serait : Destination Host Unreachable)

En analysant les tables de routage de l'annexe 2 :

4. Justifier les réponses obtenues aux deux commandes.

5. Préciser quelles modifications sur les tables de routage Mme Simonet doit faire pour que la communication entre la salle du Conseil et la cité administrative fonctionne.

Mme Simonet doit installer un nouveau serveur d'application à architecture 3-tiers (serveur web, couche applicative et base de données relationnelle). Elle a commandé un serveur performant nommé

SRV-IM. Mais le fournisseur vient de la prévenir que la livraison sera retardée de trois semaines. Or, elle doit impérativement mettre ce serveur en production dès la semaine prochaine. En attendant, elle va donc installer le serveur sur une machine un peu ancienne nommé SRV-FIC.

L'application sera accessible sur SRV-FIC au moyen de l'URL suivante :

http://intra-marche.cg96.fr

Elle préparera ensuite SRV-IM, installera les outils et les applicatifs, réinstallera le contenu de la base de données, puis testera la nouvelle configuration. Les deux machines, SRV-FIC et SRV-IM devront donc fonctionner simultanément sur le réseau. Lorsque les tests seront concluants, elle lancera le basculement sans que cela modifie l'URL en mettant à jour le fichier de la zone **cg96.fr**.

6. Dire quelle modification doit être effectuée sur le fichier de zone cg96.fr du serveur Richelieu pour faire le basculement.

Mme Simonet décide d'installer un serveur DNS secondaire (**Milady**) pour le domaine **cg96.fr**.

7. Dire quel intérêt présente la mise en place d'un serveur DNS secondaire (esclave).

A l'issue des tests, le serveur secondaire est opérationnel pour la résolution de noms sur la zone **cg96.fr**. Les postes de travail de la cité administrative sont configurés pour utiliser le serveur DNS **Milady** en premier et le serveur DNS **Richelieu** en deuxième. Après l'installation d'un nouveau serveur applicatif (**g-equip**), Mme Simonet ajoute manuellement un enregistrement Adresse (ou Hôte) dans le fichier de zone **cg96.fr** du serveur maître (**Richelieu**), mais oublie d'incrémenter le numéro de version.

Pour tester le nouvel hôte, elle lance à partir d'un poste de travail de la cité administrative la commande suivante : **ping g-equip.cg96.fr**

8. Donner et justifier la réponse à cette commande en vous appuyant sur les fichiers de zone de l'annexe 3.

Le pare-feu externe est paramétré pour filtrer les flux en provenance d'Internet :
Extrait de la table de filtrage du pare-feu externe coté Internet

Règle	IP source	Port source	IP destinataire	Port destinataire	Etat TCP	Décision
9	*	*	*	> 1024	établi	Accepte
10	*	*	*	DNS (port 53)	SO	Accepte
11	*	*	*	WWW (port 80)	*	Accepte
12	*	*	*	SMTP (port 25)	*	Accepte
13	*	*	*	SSH (port 22)	*	Accepte
14	*	*	*	HTTPS (443)	*	Accepte
Défaut	*	*	*	*	*	Bloque

Remarques : les règles sont appliquées dans l'ordre. "> 1024" signifie tous les ports supérieurs à 1024. Une étoile (*) signifie "tout". "SO" signifie sans objet, c'est à dire que le paramètre n'a pas d'intérêt dans ce cas. L'état TCP établi correspond à une connexion TCP en cours.

Le serveur DNS Athos ayant été victime d'attaques sur le port SSH, Mme Simonet a trois objectifs :
· éviter momentanément toute connexion SSH ;
· continuer à autoriser l'accès au DNS, au relais de messagerie et au serveur WWW de la DMZ ;
· continuer à permettre la navigation sur Internet des postes du réseau interne.
Pour cela elle envisage la solution suivante :
Supprimer les règles 9, 10, 11, 12, 13 et 14, puis n'autoriser dans un premier temps en entrée du pare-feu externe (à partir d'Internet) que les requêtes TCP établies (c'est à dire postérieures à une requête de connexion TCP préalable). Pour cela elle modifie la table de filtrage ainsi :
Extrait de la nouvelle table de filtrage du pare-feu externe coté Internet :

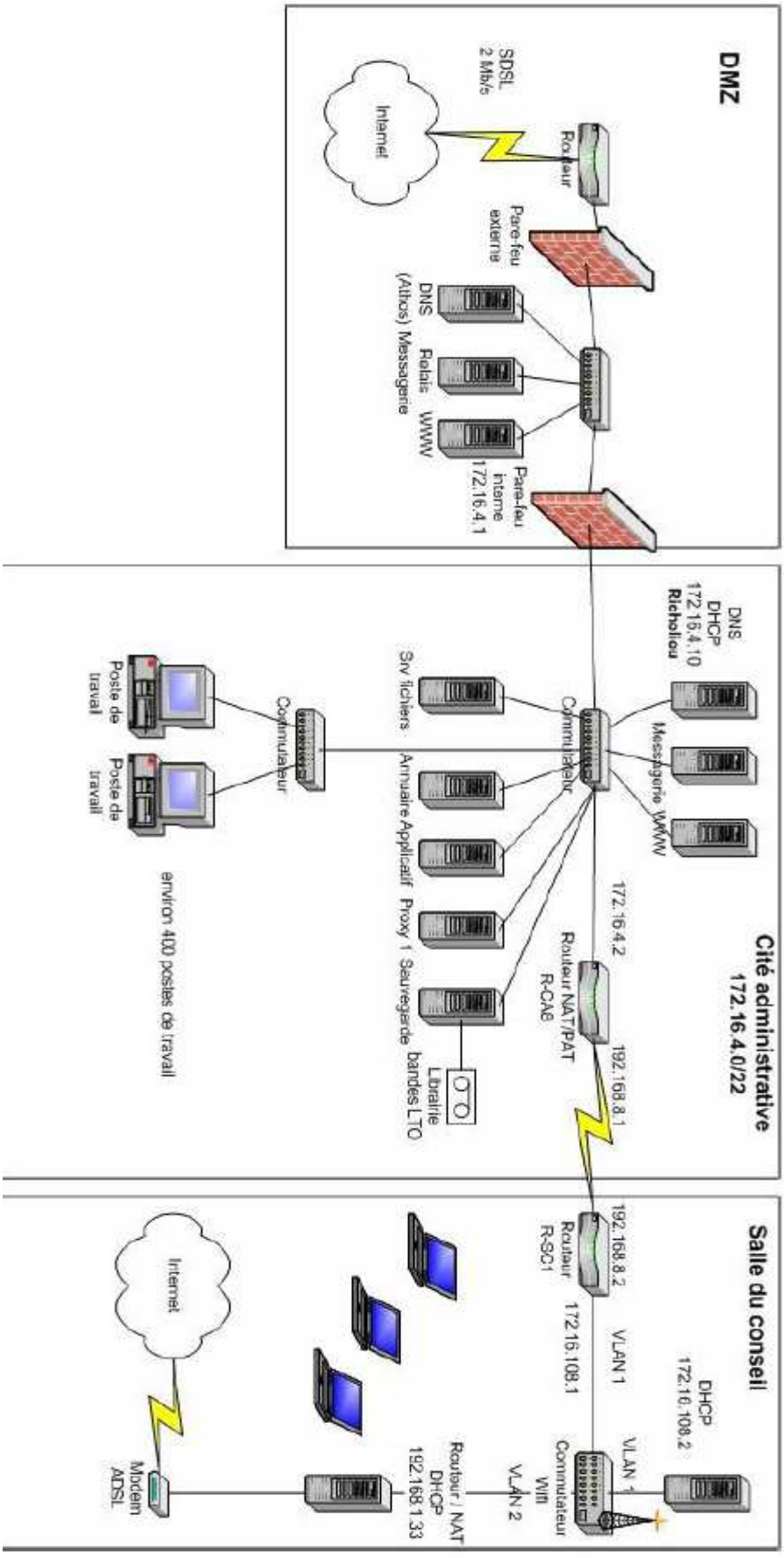
Règle	IP source	Port source	IP destinataire	Port destinataire	Etat TCP	Décision
9	*	*	*	*	établi	Accepte
Défaut	*	*	*	*	*	Bloque

9. Dire si cette table de filtrage répond aux trois objectifs. Justifier la réponse pour chaque objectif.

Non satisfaite par cette solution, Mme Simonet revient à la table de filtrage initiale.
10. Proposer une deuxième solution respectant les trois objectifs. Justifier la réponse.

La politique de sécurité interne implique l'utilisation d'un serveur mandataire (proxy) pour accéder à Internet. Les postes de travail de la cité administrative auront comme passerelle par défaut le routeur **R-CA8** d'adresse 172.16.4.2. La solution de paramétrer les navigateurs sur les postes n'a pas été retenue car elle n'offre pas une garantie suffisante. Mme Simonet a paramétré **PROXY1** en proxy transparent. Un proxy transparent est un proxy dont l'existence n'est pas connue par les navigateurs.
PROXY1 écoute les requêtes HTTP sur le port 8080, les navigateurs envoient leurs requêtes sur le port 80.
11. Dire quel mécanisme doit mettre en oeuvre l'administratrice pour que les requêtes HTTP des postes de travail soient envoyées à PROXY1.

Annexe 1 : schéma simplifié du réseau



Annexe 2 : Adresses des serveurs DNS des réseaux sans fil et tables de Routage

Réseau VLAN1 (Élus)
Serveur DNS interne : 172.16.4.10

Réseau VLAN2 (Visiteurs)
Serveur DNS du fournisseur d'accès Internet : 201.110.47.38

Table de routage du routeur R-SC1

Adresse/Masque	Masque	Passerelle	Interface
192.168.8.0	255.255.255.0	192.168.8.2	192.168.8.2
172.16.108.0	255.255.252.0	172.16.108.1	172.16.108.1

Table de routage du routeur R-CA8

Adresse/Masque	Masque	Passerelle	Interface
172.16.4.0.	255.255.252.0	172.16.4.2	172.16.4.2
192.168.8.0	255.255.255.0	192.168.8.1	192.168.8.1
172.16.108.0	255.255.252.0	172.16.108.1	192.168.8.1
0.0.0.0	0.0.0.0	172.16.4.1	172.16.4.2

Annexe 3 : Fichiers de zones DNS des serveurs Richelieu et Milady

Serveur Richelieu : extrait du contenu du fichier de configuration de la zone cg96.fr (toutes les portions de texte précédées par un point virgule (;) sont des commentaires).

```
; définition de la zone cg96.fr
; le serveur d'autorité est richelieu.cg96.fr (serveur primaire)
; il est administré par une personne qu'on peut joindre à l'adresse simonet@cg96.fr
; le serveur esclave est milady.cg96.fr (serveur secondaire)

        cg96.fr.  IN  SOA  richelieu.cg96.fr. simonet.cg96.fr. (
      136 ; numéro de version : permet aux serveurs secondaires de savoir s'ils doivent mettre à
          ; jour leur base, une incrémentation de ce numéro provoque un transfert de zone entre
          ; primaire et secondaire(s)
      36000 ; délai de mise à jour imposé aux serveurs secondaires (en secondes)
      3600 ; délai avant une autre tentative de mise à jour par un serveur secondaire (en secondes)
      360000 ; durée au-delà de laquelle les données de zones seront marquées comme obsolètes par
             ; un serveur secondaire (en secondes)
      86400); durée de validité en cache par défaut des enregistrements de zones (en secondes)

; avec deux serveurs de noms dans cette zone
              NS richelieu.cg96.fr.
              NS milady.cg96.fr.
; déclaration des adresses faisant autorité (extrait)
richelieu.cg96.fr.   IN A  172.16.4.10 ; déclaration des différents nom d'hôte
milady.cg96.fr.      IN A 172.16.12.10
srv-im.cg96.fr.      IN A 172.16.4.100
srv-fic.cg96.fr.     IN A 172.16.4.50
g-equip.cg96.fr.   IN A 172.16.4.97 ; ligne rajoutée dans la nouvelle version
r-sc1.cg96.fr.       IN A 192.168.8.2
r-ca8.cg96.fr.      IN A 172.16.4.2
intra-marche.cg96.fr. IN CNAME srv-fic.cg96.fr.  ; declaration d'un alias

; fin de la zone d'autorité
```

Serveur Milady : extrait du contenu du fichier de configuration de la zone cg96.fr du serveur Milady (les commentaires ont été effacés)

```
              cg96.fr. IN SOA richelieu.cg96.fr. simonet.cg96.fr. (136 36000 3600 360000 86400)
              NS richelieu.cg96.fr.
              NS milady.cg96.fr.
richelieu.cg96.fr.    IN A 172.16.4.10
milady.cg96.fr       IN A 172.16.12.10
srv-im.cg96.fr.      IN A 172.16.4.100
srv-fic.cg96.fr.      IN A 172.16.4.50
r-sc1.cg96.fr         IN A 192.168.8.2
r-ca8.cg96.fr        IN A 172.16.4.2
intra-marche.cg96.fr. IN CNAME srv-fic.cg96.fr.
```

Corrigé Exonet N° 23

Question 1. Dire pourquoi les portables des visiteurs qui se connectent sur le second SSID obtiendront obligatoirement une adresse IP donnée par le serveur DHCP 192.168.1.33 et non par le serveur DHCP 172.16.108.2. Justifier la réponse en vous appuyant sur le protocole DHCP et les VLAN.

Les VLAN définissent logiquement des domaines de diffusion. Ces domaines sont hermétiques.
Le protocole DHCP est basé sur des diffusions (broadcast). La requête DHCPDISCOVER envoyée par un portable de journaliste sur le VLAN 2 ne parviendra jamais au serveur DHCP 172.16.108.2.

Question 2. Donnez en la justifiant la valeur du masque de sous-réseau en notation classique et en notation CIDR.

13 adresses +1 (serveur)
Au total 14 + 2 (Adr. Diffusion + Réseau) = 16 adresses possibles
Il faut donc 4 bits pour adresser ces 16 adresses, car 24 = 16
Il reste donc 4 bits pour adresser les sous-réseaux
Ce qui donne **255.255.255.240**.
Ou encore un masque à **28 bits** ce qui donne la notation CIDR suivante **192.168.1.32/28**

Question 3. Donnez la plage d'adresses utilisables par le serveur DHCP ainsi que les différents paramètres TCP/IP nécessaires au fonctionnement des postes de travail du réseau VLAN2 (Visiteurs).

Plage d'adresses utilisable pour les postes de travail : 192.168.1.34 à 192.168.1.46
Paramètres DHCP :
masque de sous-réseau : 255.255.255.240
passerelle par défaut : 192.168.1.33
serveur DNS : 201.110.47.38
L'adresse 172.16.4.10 n'est pas acceptable.
durée du bail : 4 h (durée d'une session du Conseil)

Question 4. Justifier les réponses obtenues aux deux commandes.

a)Le poste de travail 172.16.108.10 peut joindre la passerelle par défaut 172.16.108.1, mais ensuite le routeur R-SC1 ne dispose pas de route vers le réseau 172.6.4.0. Le ping ne peut pas aboutir, donc ce routeur envoie un message ICMP au poste indiquant qu'il ne connaît pas de route vers ce réseau.
b)Il y a un problème pour le retour sur le routeur R-CA8. Le poste de travail 172.16.108.10 peut joindre la passerelle par défaut 172.16.108.1, le routeur R-SC1 connaît la route vers 192.168.8.1 mais la route vers le réseau 172.16.108.0 est fausse.

Question 5. Préciser quelles modifications sur les tables de routage Mme Simonet doit faire pour que la communication entre la salle du conseil et la cité administrative fonctionne.

Il suffit d'ajouter la route 172.16.4.0/255.255.255.252 passerelle 192.168.8.1 sur R-SC1 et de modifier la route
vers 172.16.108.0/255.255.252 passerelle 192.168.8.2 sur le routeur R-CA8.

Table de routage du routeur R-CA8

Adresse/Masque	Masque	Passerelle	Interface
172.16.4.0	255.255.252.0	172.16.4.2	172.16.4.2
192.168.8.0	255.255.255.0	192.168.8.1	192.168.8.1
172.16.108.0	***255.255.252.0***	***192.168.8.2***	***192.168.8.1***
0.0.0.0	0.0.0.0	172.16.4.1	172.16.4.2

Table de routage du routeur R-SC1

Adresse/Masque	Masque	Passerelle	Interface
192.168.8.0	255.255.255.0	192.168.8.2	192.168.8.2
172.16.108.0.	255.255.252.0	172.16.108.1	172.16.108.1
172.16.4.0.	***255.255.252.0***	***192.168.8.1***	***192.168.8.2***

Question 6. Dire quelle modification doit être effectuée sur le fichier de zone cg96.fr du serveur Richelieu pour faire le basculement.

; déclaration des adresses faisant autorité (extrait)
richelieu.cg96.fr. IN A 172.16.4.10
milady.cg96.fr IN A 172.16.12.10
srv-im.cg96.fr. IN A 172.16.4.100
srv-fic.cg96.fr. IN A 172.16.4.50
g-equip.cg96.fr. IN A 172.16.4.97
r-sc1.cg96.fr IN A 192.168.8.2
r-ca8.cg96.fr IN A 172.16.4.2
intra-marche.cg96.fr. IN CNAME srv-im.cg96.fr.
Il faut modifier l'enregistrement CNAME en le faisant maintenant pointer vers la nouvelle machine.

Question 7. Dire quel intérêt présente la mise en place d'un serveur DNS secondaire (esclave).

Un serveur secondaire (esclave) permet :
· La tolérance de pannes en permettant de résoudre les noms (pendant un certain temps) même si le serveur maître est en panne
· L'équilibrage de charge en répartissant les requêtes DNS.

Question 8. Donner et justifier la réponse à cette commande en vous appuyant sur les fichiers de zone de l'annexe 3.

La résolution de noms ne se fait pas. Milady répond qu'il n'a pas d'association pour ce nom donc les clients ne vont pas interroger Richelieu.
Le fichier du secondaire n'a pas été mis à jour à cause de l'erreur sur le numéro de version.
Les postes du site équipement sont configurés pour interroger d'abord le DNS Milady puis si celui-ci ne répond pas et uniquement si celui-ci ne répond pas, Richelieu.

Question 9. Dire si cette table de filtrage répond aux trois objectifs. Justifier la réponse pour chaque objectif.

En bloquant les flux entrants ne correspondant pas à des connexions TCP établies en interne, on obtient le résultat suivant :
· On ne peut plus se connecter de l'extérieur sur le service SSH car il n'est pas explicitement autorisé la ligne 13 est supprimée la ligne par défaut bloque et la ligne 9 n'autorise que les connexions établies de l'intérieur ;
· mais on ne peut plus se connecter sur le relais de messagerie et sur le serveur WWW qui nécessite une connexion TCP et on ne peut plus se connecter non plus au serveur DNS y compris avec UDP car la règle par défaut bloque l'accès ; les lignes 10 11 12 ont été supprimées ;
· par contre les utilisateurs peuvent utiliser Internet avec leur navigateur parce qu'ils établissent la connexion
Cette solution ne répond donc pas aux trois objectifs.

Question 10. Proposer une deuxième solution en respectant les trois objectifs. Justifier la réponse.

Il suffit de supprimer (ou de mettre sa décision à l'état « bloquer ») la ligne 13 car cette ligne autorise la connexion SSH.

Règle	IP source	Port source	IP destinataire	Port destinataire	Etat TCP	Décision
9	*	*	*	> 1024	établi	Accepte
10	*	*	*	DNS (53)	SO	Accepte
11	*	*	*	WWW (80)	*	Accepte
12	*	*	*	SMTP (25)	*	Accepte
14	*	*	*	HTTPS (443)	*	Accepte
Défaut	*	*	*	*	*	Bloque

Cette table répond aux trois objectifs

· on ne peut plus se connecter de l'extérieur sur le service SSH car la règle par défaut s'applique ;

· mais on peut se connecter aux autres services ;

· et les utilisateurs peuvent utiliser Internet.

Question 11. Dire quel mécanisme doit mettre en oeuvre l'administratrice pour que les requêtes HTTP des postes de travail soient envoyées à PROXY1.

Il faut mettre en place sur le routeur R-CA8 une redirection de port

EXONET N° 24

La mairie de la ville de L. est chargée de la gestion de 47 restaurants scolaires.
Ces restaurants sont regroupés en cinq secteurs, supervisés par des responsables de secteur, chargés de la gestion pratique des restaurants et de l'organisation des équipes. Les responsables de secteur disposent chacun d'un ordinateur utilisé pour des travaux de bureautique. Ces responsables de secteur sont situés dans un local distant de l'hôtel de ville, bâtiment principal de la mairie.
La gestion administrative de ces restaurants scolaires est assurée par le « Service des Affaires Générales ». Ce service, situé dans les locaux de la mairie, s'occupe ainsi de la gestion du personnel et de l'établissement du planning des équipes.
Monsieur Franck DUBOIS, attaché administratif au « Service des Affaires Générales », veut interconnecter le réseau principal de la mairie au réseau des responsables de secteur afin d'améliorer l'organisation et la gestion administrative du personnel.

Vous êtes amené(e) à installer et à configurer deux routeurs R2 et R3 pour relier le réseau principal de la mairie au réseau des responsables de secteur.

1. Expliquer la ligne 2 de la table de routage du routeur R3 (Annexe 2)

Il est décidé que les responsables de secteur connectés au réseau principal de la mairie doivent aussi avoir la possibilité de se connecter au serveur de messagerie de la mairie.

2. Indiquer l'adresse de passerelle qui doit être définie sur chaque ordinateur des responsables de secteur.

Ces modifications faites, il s'avère que les ordinateurs des responsables de secteur n'ont toujours pas accès au serveur de messagerie 192.168.200.130.
À partir du serveur Windows NT4 d'adresse 172.30.16.3, vous exécutez la commande ping 192.168.200.130. La commande s'exécute correctement.
À partir de l'ordinateur du responsable du secteur 1 d'adresse 172.30.32.1, vous exécutez la commande ping 172.30.16.3. La commande s'exécute correctement.
À partir de l'ordinateur du responsable du secteur 1 d'adresse 172.30.32.1, vous exécutez la commande ping 192.168.200.130. Cette fois la réponse est « Impossible de joindre l'hôte de destination ».

3. Indiquer, en justifiant votre réponse, le routeur qui est la cause du dysfonctionnement.

Vous avez la possibilité d'utiliser, pour modifier les tables de routage, la commande route.
On considérera que la syntaxe de la commande route se limite à :
route {[ADD] | [PRINT] | [DELETE] | [CHANGE] } destination MASK masque passerelle
Exemple : route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.1

4. Préciser, en justifiant votre réponse, la commande que vous devez employer pour mettre à jour la table de routage du routeur incriminé, de façon à obtenir une réponse correcte à la commande ping précédente.

Le serveur de messagerie de la mairie est désormais accessible par les responsables de secteur.
On vous demande d'appliquer sur le routeur **R3**, la commande suivante :
route add 0.0.0.0 mask 0.0.0.0 172.30.128.254
Une commande route print montre qu'une ligne supplémentaire a été créée dans la table de routage du routeur **R3**.

	0.0.0.0	0.0.0.0	172.30.128.254	172.30.128.253

5. Indiquer la raison pour laquelle on a décidé d'insérer une telle ligne dans la table de routage de R3.

On a mis en place sur le routeur **R1** connecté à Internet des règles de sécurité.
Après étude de la documentation technique du routeur **R1** et de la configuration existante, vous devez mettre à jour les fonctions de filtrage définies en **Annexe 3**pour autoriser aux responsables de secteur l'accès aux serveurs web et de messagerie.

6. Indiquer, en justifiant votre réponse, si le serveur web de la DMZ est accessible à partir d'Internet.

7. Ajouter une nouvelle règle qui autorise les responsables de secteur à accéder au serveur web de la DMZ en passant par le réseau principal de la mairie.

Le « Service des Affaires Générales» est réparti sur les 1er et 2ème étages qu'il partage avec d'autres services. Le « Service des Administrés », quant à lui, occupe à lui seul la totalité du rez-de-chaussée.
Le responsable informatique souhaite isoler chacun de ces deux services en mettant en œuvre des réseaux locaux virtuels (VLAN).
Le commutateur actuellement installé dans les bâtiments de la mairie est un commutateur administrable ne gérant que les VLAN de niveau 1 .
Après observation du schéma du réseau (**Annexe 1**), l'administrateur s'aperçoit que, dans l'état actuel de l'installation, il peut créer un VLAN de niveau 1 pour isoler le « Service des Administrés » mais qu'il ne peut pas en créer pour le « Service des Affaires Générales ».

8. Expliquer pourquoi il est possible de créer un VLAN de niveau 1 pour le « Service des Administrés ».

9. Expliquer pourquoi il n'est pas possible de créer un VLAN de niveau 1 pour le « Service des Affaires Générales ».

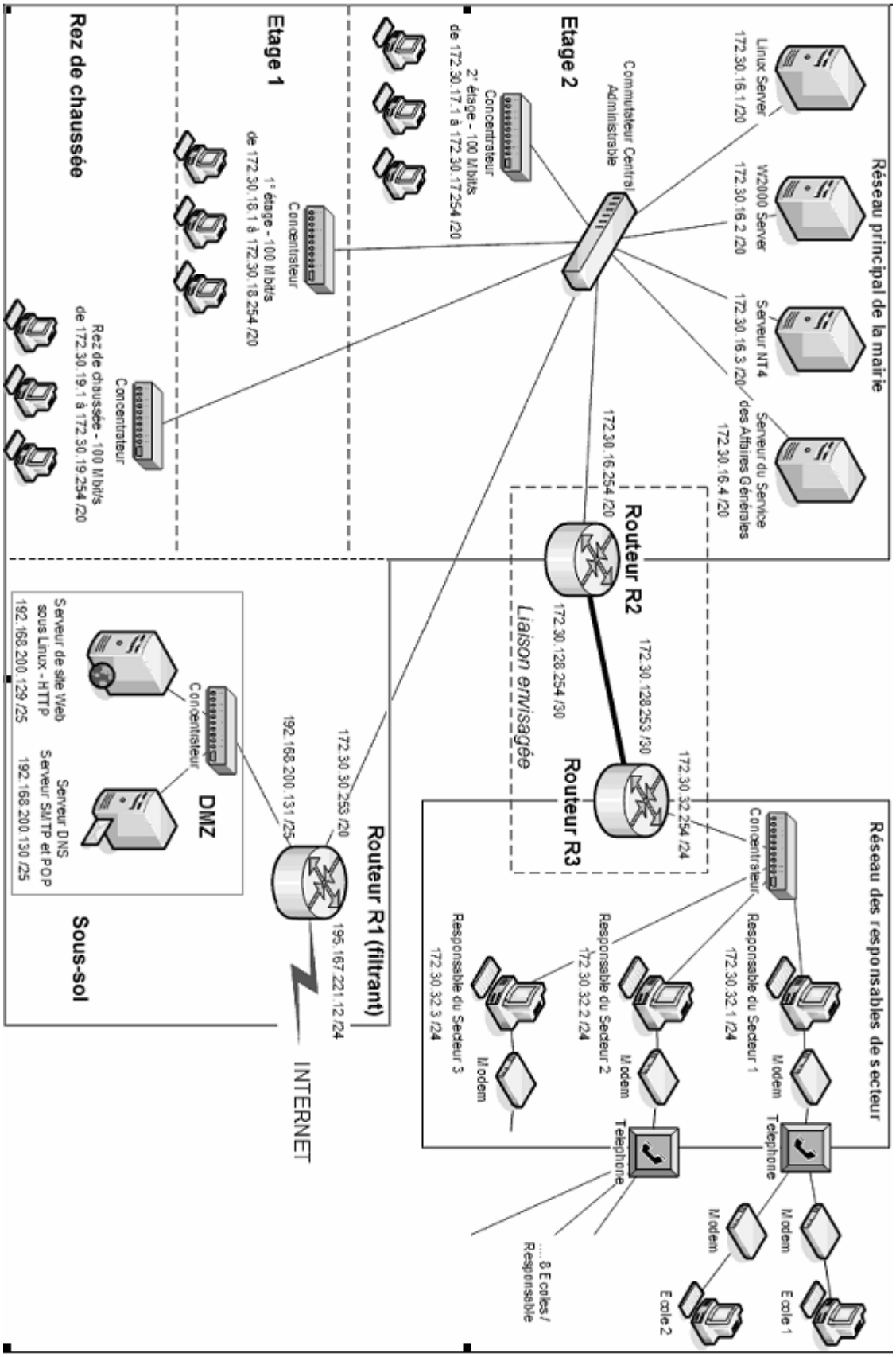
Les responsables de secteur se plaignent de recevoir de nombreux pourriels (spams).

10. Définir la notion de pourriel (spam) et préciser en quoi ils constituent une gêne pour l'entreprise.

Le responsable informatique vous demande de filtrer la réception des messages, afin de bloquer certaines sources (adresses électroniques, noms de domaine, adresses IP). Dans cette optique, la mairie adhère à un service de liste noire anti-pourriels (blacklist anti-spam) hébergé sur un serveur **DNSBL** (DNS BlackList).

11. Expliquer, en vous aidant éventuellement d'un schéma, le principe de fonctionnement de l'interrogation par l'entreprise d'une liste de type « Blacklist anti-spam » lors de la procédure de réception d'un message.

Annexe 1 : schéma du réseau



Annexe 2: Tables de routage

Table de routage du routeur R1

	Adresse destinataire	Masque	Passerelle	Interface
1	195.167.221.0	255.255.255.0	195.167.221.12	195.167.221.12
2	192.168.200.128	255.255.255.128	192.168.200.131	192.168.200.131
3	172.30.16.0	255.255.240.0	172.30.30.253	172.30.30.253
4	172.30.32.0	255.255.255.0	172.30.16.254	172.30.30.253
5	0.0.0.0	0.0.0.0	195.167.221.12	195.167.221.12

Table de routage du routeur R2

	Adresse destinataire	masque	Passerelle	Interface
1	172.30.128.0	255.255.128.0	172.30.128.254	172.30.128.254
2	172.30.16.0	255.255.240.0	172.30.16.254	172.30.16.254
3	172.30.32.0	255.255.255.0	172.30.128.253	172.30.128.254
3	192.168.200.128	255.255.255.128	172.30.30.253	172.30.16.254
4	195.167.221.0	255.255.255.0	172.30.30.253	172.30.16.254
5	0.0.0.0	0.0.0.0	172.30.30.253	172.30.16.254

Table de routage du routeur R3

	Adresse destinataire	Masque	Passerelle	Interface
1	172.30.128.0	255.255.128.0	172.30.128.253	172.30.128.253
2	172.30.16.0	255.255.240.0	172.30.128.254	172.30.128.253
3				
4				

Annexe 3: Politique de sécurité de la mairie

Le routeur **R1** est un routeur filtrant. Il agit au niveau des couches 3 et 4 du modèle OSI et assure des fonctions de translation d'adresses et de ports (NAT/PAT). Cette translation est assurée après filtrage. À titre d'exemple, voici une des règles NAT/PAT appliquées sur l'interface d'entrée 195.167.221.12 du routeur R1, à l'adresse IP de destination du paquet.

Avant Translation		**Après Translation**	
Adresse	Port	Adresse	Port
195.167.221.12	80	192.168.200.129	80

Chaque paquet arrivant sur une interface du routeur est analysé et les règles de filtrage sont traitées séquentiellement.

Règles de filtrage pour R1

N° de Règle	Interface d'arrivée	Adresse Source	Port Source	Adresse Destination	Port Destination	Numéro de Protocole	Action
1	195.167.221.12	Any	Any	195.167.221.12	80	6	accepté
2	172.30.30.253	172.30.16.0 /20	Any	192.168.200.130	25	6	accepté
3	195.167.221.12	Any	Any	Any	23	6	rejeté
Défaut (1)	Any	Any	Any	Any	Any	Any	rejeté

(1) Tout ce qui n'est pas autorisé est interdit.

Principaux protocoles et ports associés

Protocole	Port réservé	Numéro de Protocole
FTP	21	
Telnet	23	
SMTP	25	
HTTP	80	
NNTP	119	
SNMP	161	
DHCP	68	
DNS	53	
ICMP		1
TCP		6
UDP		17

Corrigé Exonet N° 24

Question 1. Expliquer la ligne 2 de la table de routage du routeur R3 (Annexe 2).

Rappelons qu'une ligne de la table de routage s'interprète de la manière suivante : pour atteindre le réseau **w.x.y.z**, défini par le masque **m.m.m.m**, il faut transmettre les paquets à l'adresse **w.x.y.z** et pour cela quitter le routeur ou le poste par l'interface **w.x.y.z**.
Pour atteindre le réseau 172.30.16.0, défini par le masque 255.255.240.0, il faut transmettre les paquets à l'adresse 172.30.128.254 (passerelle : point d'entrée dans ce sens là du routeur **R2**) et pour cela quitter le routeur (**R3** dans notre cas) par l'interface 172.30.128.253.

Question 2. ndiquer l'adresse de passerelle qui doit être définie sur chaque ordinateur des responsables de secteur.

La passerelle doit avoir pour valeur le point d'entrée dans le routeur **R3**, côté réseau des responsables de secteur, soit l'adresse **172.30.32.254**.

Question 3. Indiquer, en justifiant votre réponse, le routeur qui est la cause du dysfonctionnement.

Comme le ping passe depuis le serveur NT4 vers le serveur SMTP, on peut en déduire que le routeur **R1** n'est pas en cause. Il nous reste donc à préciser qui, des routeurs **R2** ou **R3**, est en cause.
A l'observation des tables de routage, on constate que le routeur **R3** ne dispose d'aucune ligne concernant le réseau 192.168.200.128 /25. Il ne peut donc atteindre les postes de ce réseau. Il faut lui rajouter cette ligne.

Question 4. Préciser, en justifiant votre réponse, la commande que vous devez employer pour mettre à jour la table de routage du routeur incriminé, de façon à obtenir une réponse correcte à la commande ping précédente.

L'adresse du réseau à joindre est 192.168.200.128, ce qu'on détermine en appliquant le masque /25 à l'adresse du Serveur SMTP/POP (192.168.200.130).
La commande à appliquer au routeur R3 est donc :
route ADD 192.168.200.128 MASK 255.255.255.128 172.30.128.254

Question 5. Indiquer la raison pour laquelle on a décidé d'insérer une telle ligne dans la table de routage de R3.

Rappelons que la ligne de commande qui a été exécutée sur le routeur R3 est :
route add 0.0.0.0 mask 0.0.0.0 172.30.128.254
Ce qui a pour effet d'insérer la ligne :

	0.0.0.0	0.0.0.0	172.30.128.254	172.30.128.253

La ligne insérée indique donc au routeur **R3** qu'il doit rediriger les flux sortants (toutes adresses « inconnues ») vers le routeur suivant **R2** (interface d'entrée 172.30.128.254). Ici, cette ligne permet aux postes des responsables de secteur d'accéder à Internet en passant par les routeurs R3, R2 et R1.

Question 6. Indiquer, en justifiant votre réponse, si le serveur web de la DMZ est accessible à partir d'Internet.

Rappelons la règle 1 de la table de filtrage :

N° de règle	Interface d'arrivée	Adresse Source	Port Source	Adresse Destination	Port Destination	Protocole	Action
1	195.167.221.12	Any	Any	195.167.221.12	80	6	accepté

D'après cette règle, tout accès (quelle que soit la source et quel que soit le port) en provenance d'Internet (interface d'arrivée 195.167.221.12), à destination de 195.167.221.12 avec le port 80 est **accepté**.

Rappelons la table de « translation » :

Avant Translation		**Après Translation**	
Adresse	Port	Adresse	Port
195.167.221.12	80	192.168.200.129	80

Du fait de l'application de la règle de translation, l'adresse de destination 195.167.221.12 est substituée en l'adresse 192.168.200.129 du serveur Web de la Mairie, qui est donc bien **accessible** depuis Internet.

Question 7. Ajouter une nouvelle règle qui autorise les responsables de secteur à accéder au serveur web de la DMZ en passant par le réseau principal de la mairie.

Donc, quel que soit le port source, tout flux en provenance du réseau des responsables de secteur (172.30.32.0 /24) arrivant sur l'interface 172.30.30.253, à destination du serveur web (192.168.200.129) doit être **accepté**.

La règle doit être placée avant la règle par défaut :

N° de règle	Interface d'arrivée	Adresse Source	Port Source	Adresse Destination	Port Destination	Protocole	Action
4	172.30.30.253	172.30.32.0 /24	Any	192.168.200.129	80	6	accepté

Question 8. Expliquer pourquoi il est possible de créer un VLAN de niveau 1 pour le « Service des Administrés » .

Toutes les machines du rez-de-chaussée doivent être isolées. Donc, si l'on affecte le **port** du commutateur sur lequel est connecté le concentrateur du rez-de-chaussée à un VLAN (VLAN par port ou de niveau 1), toutes les machines situées derrière le concentrateur vont appartenir à ce VLAN.

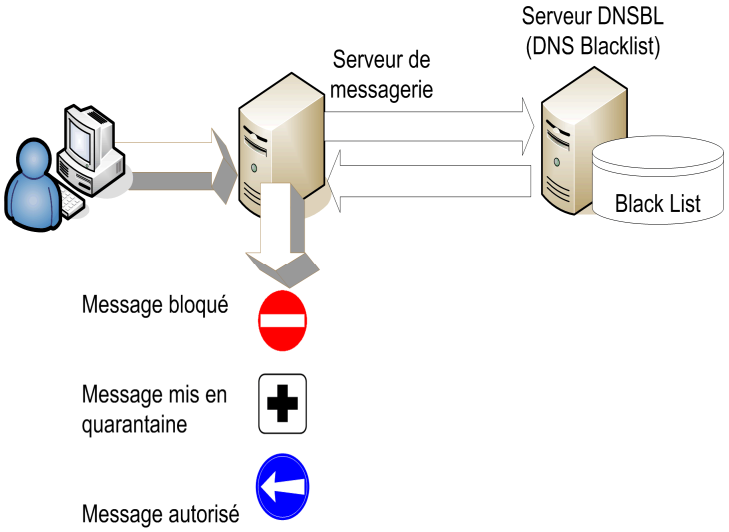
Question 9. Expliquer pourquoi, il n'est pas possible de créer un VLAN de niveau 1 pour le « Service des Affaires Générales ».

Il n'est plus possible d'utiliser des VLAN par port sans bloquer, dans un unique VLAN, toutes les machines situées derrière le concentrateur. Or certaines doivent appartenir à un VLAN et d'autres à un autre. On ne peut donc pas mettre en place de VLAN de niveau 1 pour le Service des Affaires Générales.

Question 10. Définir la notion de pourriel (spam) et préciser en quoi ils constituent une gêne pour l'entreprise.

Pourriel (spam, pollupostage…) : désigne les communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes. Les pourriels polluent les boites aux lettres des usagers des messageries et nécessitent de leur part un temps de traitement parfois non négligeable (tri, suppression…). Par ailleurs ils sont parfois porteurs de virus, chevaux de Troie, espiogiciels… ce qui peut nuire à l'efficacité des systèmes (destruction de données, ralentissement des systèmes…).

Question 11. Expliquer, en vous aidant éventuellement d'un schéma, le principe de fonctionnement de l'interrogation par l'entreprise d'une liste de type « Blacklist anti-spam » lors de la procédure de réception d'un message.



EXONET N° 25

Consciente de l'importance de modifier nos habitudes nutritionnelles et de protéger notre environnement, la société ESN a développé l'enseigne Espace Santé Nature qui offre une large gamme de produits issus de l'agriculture biologique, labellisés et contrôlés par des organismes agréés.
Pour accompagner le développement de son enseigne Espace Santé Nature la société a décidé de faire évoluer son système d'information.
Les locaux du siège de la société ESN accueillent un réseau informatique d'architecture « FastEthernet », entièrement commuté et distribué sur deux bâtiments principaux (A et B). Au moment de votre collaboration, le projet d'évolution de l'architecture du réseau local est en cours de réalisation.
L'ensemble des serveurs et le cœur de l'électronique active ont été migrés vers un nouveau bâtiment appelé « local technique général ». Celui-ci permet de bénéficier de locaux mieux adaptés notamment en termes de sécurité d'accès physique (utilisation de badges), de climatisation, de système anti-incendie et de tolérance aux pannes.

Chacun des trois bâtiments dispose d'un commutateur : CA, CB et CG (annexe 1).
Pour gérer la tolérance aux pannes des liaisons, l'administrateur a relié les trois commutateurs entre eux en formant un circuit. Pour éviter les **tempêtes de diffusion**, il a activé le protocole 802.1d. Ce protocole utilise un algorithme d'arbre de recouvrement minimum (spanning tree) pour transformer un circuit en arbre. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison. L'administrateur influe sur le choix des liaisons invalidées en pondérant chaque liaison. Les serveurs sont situés dans le local technique général. Il n'y a pas de trafic réseau entre les postes du bâtiment A et ceux du bâtiment B.

1. Expliquer ce qu'est une « tempête de diffusion » et sa cause.

2. Identifier le lien qui doit être invalidé par le protocole 802.1d en justifiant la réponse.

La séparation des flux entre bâtiments est assurée par la mise en place de réseaux locaux virtuels (VLAN) sur les commutateurs. Le commutateur CG dispose également d'une fonction de routage qui n'est pas activée. L'annexe 2 présente la configuration des réseaux virtuels et IP de la société.

3. Expliquer pourquoi les ports d'interconnexion entre commutateurs doivent être étiquetés.

4. Expliquer s'il est nécessaire d'activer le routage sur le commutateur CG pour permettre la communication entre un poste du bâtiment B et le serveur SRV-ESN.

Tous les postes obtiennent dynamiquement leur configuration IP (adresse, routeur, DNS) à partir du serveur SRV-ESN. Mais un commercial connecté avec son portable à un point d'accès sans fil du bâtiment A n'a pas pu accéder au serveur SRV-SAGE. La liaison entre le portable et le point d'accès est pourtant opérationnelle.

5. Définir les adresses IP des passerelles par défaut affectées aux postes fixes du bâtiment A et du bâtiment B pour aller vers Internet.

6. Expliquer la cause du dysfonctionnement observé sur l'ordinateur portable.

Afin de remplacer des serveurs de données obsolètes, on a fait l'acquisition d'un unique serveur nommé SRV-NAS plus performant, dont les caractéristiques sont présentées en annexe 3. Il dispose notamment de caractéristiques matérielles permettant d'assurer la continuité d'exploitation en cas de panne.

7. Comparer les solutions RAID 0, RAID 1 et RAID 5 de ce serveur :

- en terme de volume utile à justifier par un calcul,

- en terme de tolérance aux pannes.

8. Dire quels sont les autres éléments du serveur NAS qui permettent d'assurer la continuité de service et la tolérance aux pannes.

La société ESN a mis en place un catalogue en ligne accessible à tous sur Internet. Mais elle a aussi développé pour son réseau commercial de boutiques un accès web permettant de passer des commandes en ligne.
Les sites web public et privé sont installés sur le serveur SRV-3W. Ils se distinguent par des numéros de port différents (80 et 8000). Le SGBDR utilisé par le site web est situé sur le serveur SRV-SAGE.
Dans le cadre de son nouveau contrat d'accès à Internet, la société ESN bénéficie d'une liaison haut débit SDSL à 2 Mbps, d'une plage d'adresses IP sur le sous-réseau 217.167.171.128 de masque 255.255.255.248 et d'un nom de domaine géré par le fournisseur d'accès (**espace-sante-nature.com**).
9. Justifier le choix d'une offre d'accès à Internet de type SDSL.
10. Déterminer la classe, le nombre d'adresses et la plage d'adresses IP offertes par le FAI (fournisseur d'accès Internet) à ESN.

Les boutiques sont identifiées par la plage d'adresses 195.200.10.65 à 195.200.10.126 réservée auprès du FAI.
Dans un premier temps, l'administrateur n'a pas mis en place de DMZ, il a utilisé les fonctionnalités NAT/PAT et de redirection du routeur SDSL pour rendre accessibles le site public et le site privé. Puis sur le pare-feu SRV-WALL, il a élaboré les règles de filtrage suivantes sur l'interface externe (annexes 1 et 2 uniquement) :
Extrait de la table de filtrage qui ne montre pas les flux bidirectionnels :
(Information sur les ports utilisables : DNS (53), HTTP site public (80), HTTP site privé (8000), SMTP (25), POP3 (110) et SGBDR (3306), tous(ports > 1024))

N°	Source		Destination		Décision
	IP	Port	IP	Port	
…	**….**	**…**	**…**	**…**	**…**
20	**Toutes**	**Tous**	**192.168.0.7/32**	**80**	**Accepter**
30	**Toutes**	**Tous**	**192.168.0.7/32**	**8000**	**Accepter**
40	Toutes	Tous	192.168.0.9/32	25	Accepter
41	Toutes	Tous	192.168.0.9/32	110	Accepter
Défaut	Toutes	Tous	Toutes	Tous	Bloquer

11. Donner la signification de la règle n° 20.
12. Donner la signification de la règle n° 30 et expliquer pourquoi cette règle ne répond pas précisément aux contraintes d'accès.

Dans un deuxième temps, l'administrateur a décidé de créer une zone démilitarisée (DMZ) pour améliorer la sécurité des accès Internet (annexe 4).
Les deux interfaces du routeur SDSL sont configurées avec l'adresse IP 217.167.171.126 sur l'interface externe et 217.167.171.133 sur l'interface interne. Les adresses IP affectées aux serveurs SRV-MAIL et SRV-3W sont désormais 217.167.171.129 et 217.167.171.130. Sur le routeur SDSL les fonctionnalités NAT/PAT et de redirection ne sont plus nécessaires.
13. Donner la table de routage du pare-feu SRV-WALL.

Le pare-feu du routeur SDSL et le pare-feu SRV-WALL disposent désormais des règles de filtrage permettant l'accès au site web public et au serveur SMTP et POP. L'administrateur vous demande d'écrire les nouvelles règles qui permettent l'accès **au site web privé depuis les boutiques** pour la mise à jour des commandes dans la base de données.

14. Établir la nouvelle règle de filtrage sur l'interface externe 217.167.171.126 du routeur SDSL.

15. Établir la règle de filtrage sur l'interface externe de SRV-WALL sachant que le SGBDR (implanté sur le serveur SRV-SAGE) écoute sur le port 3306.

Le serveur SRV-MAIL assure les services SMTP et POP. Ces deux services ont été testés et fonctionnent correctement. Ils utilisent les mêmes mots de passe de connexion.

Depuis un poste du service informatique dans le réseau local, l'administrateur a configuré un compte de messagerie existant ainsi :

SMTP : 217.167.171.129

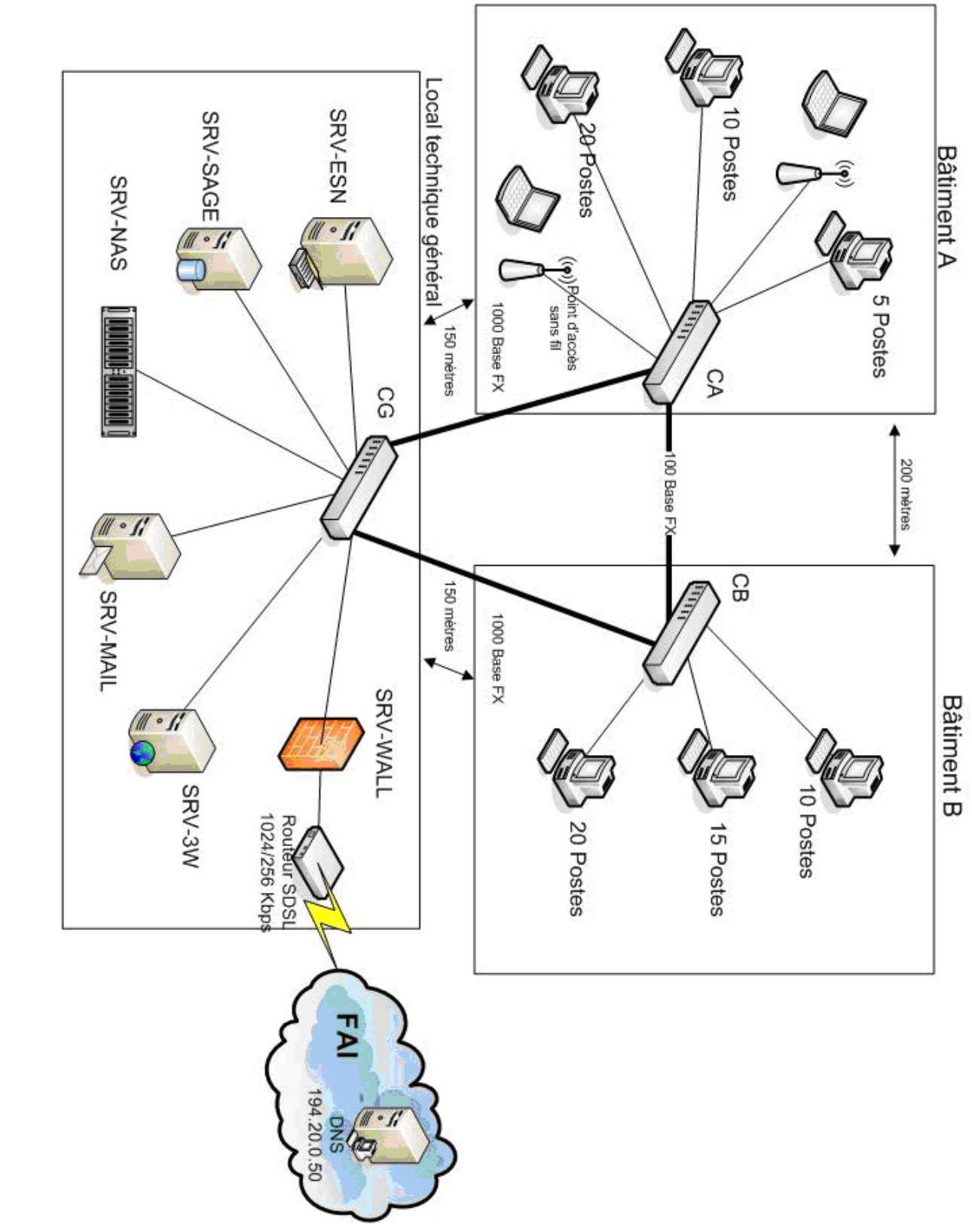
POP : pop.espace-sante-nature.com

Il envoie les courriels avec succès, mais il ne parvient pas à en recevoir. Le logiciel client de messagerie affiche l'erreur suivante :

Échec de la connexion au serveur. Compte : 'admin', Serveur : 'pop.espace-sante-nature.com', Protocole : POP3, Port : 110

16. Expliquer la cause de l'échec de réception du courriel, sachant que le FAI n'a pas été informé du nouveau plan d'adressage.

Annexe 1 : Nouvelle architecture du réseau



Annexe 2 : Configuration des réseaux virtuels et IP de la société

Architecture générale de l'interconnexion : Chaque bâtiment (A, B et local technique général) dispose d'un commutateur principal qui s'interconnecte avec les commutateurs principaux des autres bâtiments.

Architecture des VLAN

Commutateurs principaux	CA	CB	CG
Emplacement	Bâtiment A	Bâtiment B	Local Technique général
VLAN gérés	1,100, 200	1,100, 200	1,100, 200

Remarque : Le commutateur CG est un commutateur / routeur. À chaque VLAN défini sur le commutateur peut être associée une adresse IP qui permet le routage entre VLAN. Cette fonction de routage n'est pas activée.

Tableau d'affectation Ports - VLAN avec statut 802.1q des ports

	VLAN 1	**VLAN 100**	**VLAN 200**	**Etiquetés 802.1q (taggés)**
Ports de connexion des points d'accès sans fil du bâtiment A	X			NON
Ports de connexion des postes fixes filaires et des autres équipements du Bâtiment A		X		NON
Ports de connexion des postes fixes filaires et des autres équipements du bâtiment B			X	NON
Ports de connexion des serveurs et des équipements du local technique général		X	X	OUI
Ports d'interconnexion des commutateurs CA, CB et CG	X	X	X	OUI

Adresse IP du sous-réseau associé à chaque VLAN

VLAN 1 (par défaut)	VLAN 100	VLAN 200
Pas d'adresse IP affectée	192.168.0.0/24	192.168.1.0/24

Adressage IP des postes de travail : Tous les postes des bâtiments A et B doivent obtenir une adresse dynamiquement à partir du serveur DHCP SRV-ESN. Ce serveur gère deux plages d'adresses, une pour chaque réseau IP.

Adressage IP des serveurs : Le protocole 802.1q est activé sur les interfaces réseau des serveurs. Ces interfaces sont associées au VLAN 100 et au VLAN 200 et disposent d'une adresse IP par VLAN. Les cartes réseaux de ces serveurs sont donc multi-adresses. Elles associent à un VLAN la trame reçue en fonction de l'étiquette contenue dans la trame et remettent le paquet à l'adresse IP correspondante. En émission, elles étiquettent la trame en fonction du VLAN d'émission.

Tableau d'affectation serveurs / VLAN et adressage IP des serveurs (avant le déplacement dans la DMZ des serveurs SRV-3W et SRV-MAIL)

	VLAN 100	VLAN 200
SRV-ESN (serveur d'authentification – DHCP – DNS cache)	192.168.0.1	192.168.1.1
SRV-SAGE (serveur d'applications de gestion et SGBDR)	192.168.0.3	192.168.1.3
SRV-NAS (stockage des fichiers et des bases de données)	192.168.0.5	192.168.1.5
SRV-3W (serveur web interne et externe)	192.168.0.7	192.168.1.7
SRV-MAIL (serveur de messagerie interne et externe)	192.168.0.9	192.168.1.9
SRV-WALL (pare-feu, accès Internet des postes sur l'interface interne)	192.168.0.254	192.168.1.254

NB: le pare-feu SRV-WALL dispose de l'adresse IP 217.167.171.134 sur l'interface externe.

Annexe 3 : Informations techniques sur le serveur NAS

Le **serveur NAS** est une solution simple pour ajouter du stockage disque en réseau. Le NAS est un périphérique réseau de stockage (serveur de fichiers). Il se connecte sur un réseau Ethernet et se comporte comme un serveur autonome de fichiers. Sa simplicité d'installation et d'administration, la redondance de ses composants en font une solution fiable et efficace pour le stockage et la sauvegarde des données sur un réseau hétérogène.

Caractéristiques du serveur NAS

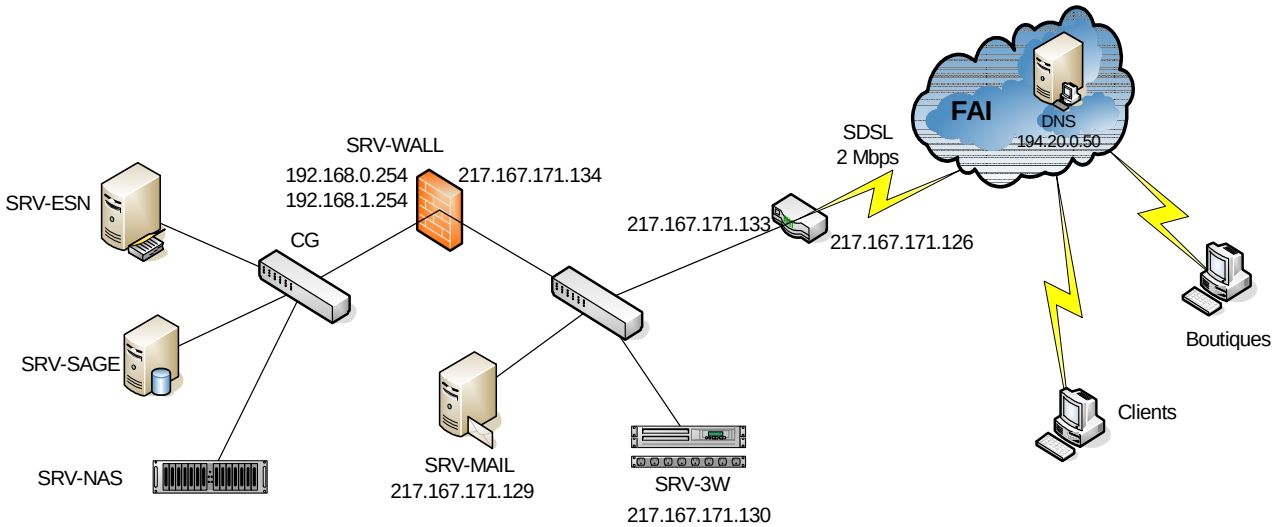
Matériel

- Pentium 4 2.8GHz avec 512KB L2 cache et 2 DIMM slots for 2GB ECC DDR 266/333 memory,
- 2 interfaces intégrées Intel Gigabit Ethernet
- 8 disques SATA hot-swappable (250 GB chacun)
- RAID 0, 1, 5
- Gravure sur CD-R/RW et DVD+RW (Option)
- Alimentation redondante et compatibilité UPS

Administration et Compatibilité

- Microsoft Windows NT/2000/2003 support Domaine et Active Directory
- UNIX, Solaris, FreeBSD, Linux, support Network Information Service (NIS),
- MacOS 8.x, 9.x, OS X
- TCP/IP, AppleTalk, IPX
- HTTP, CIFS/SMB, NFS v3, NCP, FTP, AFP
- BOOTP, RARP, DHCP, DNS, WINS, SMTP, SNMP, NTP, SSL

Annexe 4 : Schéma de la DMZ



Corrigé Exonet N° 25

Question 1. Expliquer ce qu'est une « tempête de diffusion ».

Le commutateur segmente le domaine de collision, il laisse cependant passer les diffusions de trames Ethernet (MAC FF-FF-FF-FF-FF-FF).
L'architecture en annexe présente une interconnexion des commutateurs en boucle.
Conséquences :
Les commutateurs mettent à jour leur table de correspondance port source = @mac à partir de la trame qui arrive. Les trames de diffusion et de multidiffusion sont acheminées par inondation vers tous les autres ports du commutateur et donc vers tous les commutateurs interconnectés. La trame boucle indéfiniment (pas de TTL), il y a inondation de la bande passante et surcharge de tous les noeuds connectés sur tous les ports.

Question 2. Identifier le lien qui doit être invalidé en justifiant la réponse

Le lien a invalider doit être CA CB, pour deux raisons, le débit est plus faible et il n'y a pas de flux échangés entre le bâtiment A et le bâtiment B, tous les flux sont destinés au local technique général où sont placés tous les serveurs.

Question 3. Expliquer pourquoi les ports d'interconnexion entre commutateurs doivent être étiquetés (taggés).

Les ports d'interconnexion appartiennent à plusieurs VLAN. Pour pouvoir associer une trame à un VLAN il faut donc rajouter l'étiquette 802.1q dans la trame.

Question 4. Expliquer s'il est nécessaire d'activer le routage sur le commutateur CG pour permettre la communication entre un poste du bâtiment B et le serveur SRV-ESN.

Non car le serveur SRV-ESN a deux adresses IP sur son interface où le protocole 802.1q est actif. Les trames émises et reçues par lui sont "étiquetées" puis associer à la bonne adresse IP en fonction du VLAN. Le serveur et le poste sont donc dans le même réseau IP et dans le même VLAN, on n'a donc pas besoin de router.

Question 5. Définir les adresses IP des passerelles par défaut affectées aux postes du bâtiment A et du bâtiment B pour aller vers Internet.

L'accès à Internet se faisant par le pare-feu SRV-WALL, on utilise l'interface de celui-ci associée au VLAN correspondant :

- Pour le bâtiment A il s'agit de 192.168.0.254 (VLAN 100).
- Pour le bâtiment B il s'agit de 192.168.1.254 (VLAN 200).

Question 6. Expliquer la cause du dysfonctionnement observé sur l'ordinateur portable.

Les points d'accès Wi-Fi sont associés au VLAN par défaut. Ils ne peuvent communiquer avec les autres Vlan directement. Il s'agit soit d'une erreur de configuration, soit d'une volonté d'isoler le flux des portables.

Question 7. Comparer les solutions RAID0, RAID1 et RAID5 de ce serveur :
- en terme de volume utile justifié par un calcul,
- en terme de tolérance aux pannes.

RAID0 : on utilise tous les disques, donc la totalité du volume (2000 G0) est disponible mais on n'a aucune tolérance aux pannes.
RAID1 : (mirroring) la moitié de l'espace est disponible pour l'utilisateur (1000GO) et celle-ci est dupliquée sur l'autre moitié, la tolérance de panne est assurée. Après une perte de disque la remise en service est très rapide puisqu'on dispose d'un disque identique au disque perdu.

RAID5 : un disque est utilisé pour le contrôle de parité. Donc l'espace disponible est de (7 X 250 = 1750) pour l'utilisateur et la tolérance aux pannes est assurée. La remise en service nécessite la reconstruction du disque perdu à partir des autres disques.

Question 8. Dire quels sont les autres éléments du serveur NAS qui permettent d'assurer la continuité de service et la tolérance aux pannes.

- Disques durs hot-swappable (branchement à chaud) en RAID 0 à 5
- Alimentation redondante et compatibilité UPS (l'arrêt se fera proprement à partir de l'onduleur)
- Mémoire vive de type ECC (contrôle d'erreur),
- 2 interfaces intégrées Intel Gigabit Ethernet (tolérance de panne possible)

Question 9. Justifier le choix d'une offre d'accès à Internet de type SDSL.

Symetric Digital Subscriber Line, liaison haut débit symétrique en descente et en montée. Les besoins de l'entreprise sont effectivement un haut débit bidirectionnel puisque l'accès à Internet est offert sur le réseau local et le serveur web hébergé en local est ouvert à l'extérieur.

Question 10. Déterminer la classe, le nombre d'adresses et la plage d'adresses IP offertes par le FAI (fournisseur d'accès internet) à ESN.

217.167.171.128 : classe C publique (réseau de $192.0.0.0_{10}$ à $223.255.255.0_{10}$ soit $110\ldots_2$ au 1er octet)
IP : 217.167.171.$\mathbf{128}_{10}$ → …**1000 0**000_2
Masque : 255.255.255.$\mathbf{248}_{10}$ → …1111 1**000**$_2$
Plage : …**1000 0**001_2 à …**1000 0**110_2 → 217.167.171.$\mathbf{129}_{10}$ à 217.167.171.$\mathbf{134}_{10}$
Nombre d'adresses : il reste trois bits pour la partie poste (host-id) donc $2^3 - 2 = 6$

Question 11. Donner la signification de la règle n° 20.

Les internautes (tout le monde) accèdent aux pages web publiques (port standard 80) du serveur SRV-3W.

Question 12. Donner la signification de la règle n° 30, et expliquer pourquoi cette règle ne répond pas précisément aux contraintes d'accès.

Tout le monde accède aux pages web privées du serveur SRV-3W. Les internautes devront néanmoins connaître le port non standard utilisé (http://www.espace-sante-nature.com:8000)
Ceci ne répond pas explicitement aux besoins. Au niveau du pare-feu, rien ne permet la sécurité d'accès aux pages privées (extranet) réservées exclusivement aux boutiques.

Question 13. Donner la table de routage du pare-feu SRV-WALL.

Destination	Masque	Passerelle	Interface
192.168.0.0	255.255.255.0	192.168.0.254	192.168.0.254
192.168.1.0	255.255.255.0	192.168.1.254	192.168.1.254
217.167.171.128	255.255.255.248	217.167.171.134	217.167.171.134
0.0.0.0	0.0.0.0	217.167.171.133	217.167.171.134

Question 14. Établir la nouvelle règle de filtrage sur l'interface externe 217.167.171.126 du routeur SDSL.

N°	Source		Destination		État
	IP	Port	IP	Port	
10	Toutes	53	217.167.171.134/32	Tous	Accepter
20	Toutes	Tous	217.167.171.130/32	80	Accepter
30	**195.200.10.64/26**	**Tous**	**217.167.171.130/32**	**8000**	**Accepter**
40	Toutes	Tous	217.167.171.129/32	25	Accepter
41	Toutes	Tous	217.167.171.129/32	110	Accepter
Défaut	Toutes	Tous	Tous	Tous	Bloquer

Adresses : 195.200.10.**65** à 195.200.10.**126** → … .**01**00 0001_2 à … .**01**111 1110_2
Masque : … .**11**00 0000_2 → 255.255.255.192
Réseau 195.200.10.64/26

Question 15. Établir la nouvelle table des règles de filtrage sur l'interface externe de SRV-WALL sachant que le SGBDR (implanté sur le serveur SRV-SAGE) écoute sur le port 3306.

N°	Source		Destination		État
	IP	Port	IP	Port	
10	217.167.171.134/32	53	Toutes	Tous	Accepter
20	**217.167.171.130/32**	**Tous**	**192.168.0.3/32**	**3306**	**Accepter**
30	217.167.171.130/32	80	192.168.0.0/24	Tous	Accepter
40	217.167.171.129/32	25	192.168.0.0/24	Tous	Accepter
41	217.167.171.129/32	110	192.168.0.0/24	Tous	Accepter
Défaut	Toutes	Tous	Tous	Tous	Bloquer

Question 16. Expliquer la cause de l'échec de réception du courriel, sachant que le FAI n'a pas été informé du nouveau plan d'adressage.

Les noms de domaine smtp.espace-sante-nature.com et pop.espace-sante-nature.com doivent être réaffectés à l'adresse 217.167.171.129 dans la zone espace-sante-nature.com administrée par le DNS primaire (SOA) du FAI.

EXONET N° 26

La société A'CLICK est spécialisée dans la production et la distribution de logiciels pédagogiques destinés aux enfants.
La société dispose aussi d'un service rédaction pour l'élaboration de magazines quotidiens pour enfants.
L'impression des magazines et fascicules est réalisée par un imprimeur situé à 160 km environ.
Vingt personnes de la société A'CLICK collaborent à l'élaboration des logiciels, dont quatre en télétravail (à partir de leur domicile) et trois autres chez l'imprimeur pour la mise en forme des magazines et fascicules.
La société A'CLICK dispose déjà d'un réseau informatique reliant les collaborateurs à domicile (essentiellement des développeurs) et l'imprimeur.

Vous disposez du plan du réseau de la société (annexe 1).
Le réseau de la société A'CLICK dessert le rez-de-chaussée et le premier étage de deux bâtiments distants d'une trentaine de mètres.
Les serveurs principaux sont placés au premier étage du bâtiment A dans un local technique. Les personnels sont répartis sur les deux bâtiments.
Les développeurs sur site travaillent essentiellement dans le bâtiment B.
La société a mis en place un réseau basé sur une architecture Ethernet 100 Mbit/s commutée bidirectionnelle avec des liaisons fibres optiques entre les commutateurs ayant un débit de 1 Gbit/s.
Pour la configuration des commutateurs, l'administrateur a choisi une solution basée sur des **VLAN** (Virtual Local Area Network) de niveau 1 (annexe 2).

1. Présenter les critères qui plaident en faveur de l'utilisation de réseaux locaux virtuels.

Le plan d'adressage IP en fonction des réseaux locaux virtuels et la configuration actuelle des commutateurs sont spécifiés dans les annexes 3 et 4.

2. Indiquer la classe, l'adresse réseau et le masque par défaut correspondant au plan d'adressage spécifié à l'annexe 3. Justifier les réponses.

3. Calculer le nombre d'hôtes que peut accueillir chacun des réseaux virtuels avec ce plan d'adressage.

4. Donner le nombre de domaines de diffusion (broadcast) mis en place par la configuration des commutateurs C2, C3, C4 et C5.

L'administrateur du réseau souhaite modifier la configuration des commutateurs (annexe 4).
L'administrateur connecte un poste (appartenant au réseau IP 192.168.10.32/27 et configuré sans passerelle) sur le port libre **c2e8** du commutateur **C2** pour le configurer. Il lance ensuite la commande **http://192.168.10.33** pour accéder à la page d'accueil de l'outil d'administration du commutateur C2.
Il obtient le message **"page web non disponible hors connexion" "terminé".**
Pour comprendre la nature du problème, il effectue les trois tests suivants :
Test1 : Il lance la commande **ping 192.168.10.33**
Il obtient le message **"Délai d'attente de la demande dépassé".**

Test2 : Depuis le poste il branche un câble console sur le commutateur C2 et lance une connexion série avec les propriétés **(**Bits par seconde : 9600, Bits de données : 8, Parité : Aucun, Bits d'arrêt : 1, Contrôle de flux : Matériel**).**
Il obtient le message de connexion « **Login : …… »** permettant d'accéder à l'outil d'administration.

Test3 : Il connecte alors directement le poste (en Ethernet) sur le port libre c3e8 du commutateur C3 et lance la commande **http://192.168.10.34**
Il obtient la page web d'accueil de l'outil d'administration du commutateur C3.
5. Donner la raison pour laquelle l'administration du commutateur C2 ne peut se faire actuellement que par le câble console. Proposer une solution pour résoudre ce problème.

Suite à une réorganisation des équipes de projet, il est nécessaire de déplacer le poste de travail d'un développeur, identifié **Dev5**, pour l'installer au rez-de-chaussée du bâtiment **B**. Ce poste est relié par l'intermédiaire d'une prise murale, au port **c4e7** du commutateur **C4**.
Après ce changement, l'administrateur constate que le poste **Dev5** ne peut plus communiquer avec son serveur d'applications **Sappl**. Il réalise différents tests à partir de la prise et en conclut que ce n'est pas un problème de connexion physique.
6. Expliquer pourquoi ce déplacement a généré ce problème. Proposer une solution pour que le poste Dev5 puisse de nouveau communiquer avec son serveur d'applications à partir de son nouvel emplacement.

Tous les postes du réseau peuvent communiquer entre eux grâce à la fonction de routage activée sur C2 qui est un commutateur de niveau 3. Cependant, l'administrateur n'a pas encore ajouté dans la table de routage de C2, la route par défaut pour accéder à Internet. La syntaxe de la commande pour ajouter une route dans la table de routage de C2 est décrite dans l'annexe 4.
7. Écrire l'instruction qui ajoute une route dans la table de routage de C2 pour autoriser tous les postes du réseau à accéder à Internet.

L'étude des flux sur les réseaux montre qu'après le redémarrage de l'ensemble des commutateurs une multitude de trames de diffusion ARP parviennent au portable de l'administrateur.
Celui-ci entreprend des recherches sur Internet et obtient des réponses lui expliquant un problème de "tempête de broadcast".
8. Expliquer l'expression "tempête de broadcast" et ce qui a provoqué ce problème. Indiquer quel protocole (ou algorithme) l'administrateur doit activer sur les commutateurs pour résoudre ce problème.

Les pages des magazines sont stockées dans une base de données. Elles sont composées de textes et d'images numérisées et d'attributs de mise en forme. Les flux de communication avec l'imprimeur sont de simples transferts de données composant le magazine : texte, images et attributs de mise en page.
La solution utilisée actuellement pour relier l'entreprise à la société A'CLICK repose sur une liaison à distance Numéris à 64 Kbit/s point à point.
L'impression quotidienne des magazines pour enfant étant en constante augmentation, l'adaptation de la ligne de communication reliant la société A'CLICK à l'imprimeur devient une priorité.
Le responsable du réseau estime en effet que le transfert des pages d'un magazine est trop long. Ainsi, pour le transfert d'une page de 300 Ko à laquelle s'ajoute 15 % de données de gestion (des différents protocoles mis en œuvre lors du transfert), il faut près de 44 secondes.
9. Déterminer la bande passante minimum nécessaire, exprimée en Kbit/s, que doit supporter la liaison pour ramener le temps de transfert d'une page à environ 10 secondes (justifier la réponse, prendre 1 Ko = 1 000 octets).

L'administrateur constate que pour obtenir des temps de transfert de pages et un coût acceptables, il va falloir augmenter considérablement les débits de transfert.
Lors d'une réunion, la direction de la société a donné son accord pour augmenter les débits via Internet.
Pour améliorer les capacités d'accès, l'administrateur propose la mise en place d'une technologie **ADSL** pour les développeurs à domicile et d'une technologie **SDSL** pour l'imprimeur.

10. Expliquer les principales différences techniques qui existent entre l'ADSL et le SDSL proposées par l'administrateur.

La connexion devra se faire de manière cryptée, virtuelle, point à point, avec une passerelle **VPN** (Virtual Private Network) dite aussi **RPV** (Réseau Privé Virtuel), située sur le routeur **Rte_A'click** de la société. Elle offrira ainsi aux développeurs et à l'imprimeur une extension du réseau privé.
Les développeurs à domicile pourront se connecter à Internet, puis établir une connexion VPN vers le réseau de la société.
Pour la mise en place de ce tunnel VPN, le routeur **Rte_A'click** doit posséder une adresse IP publique fixe, utiliser un pare-feu effectuant de la translation d'adresses et être capable de rediriger une demande vers une adresse IP privée (annexes 1 et 5).

11. Expliquer la démarche que doit suivre l'administrateur du réseau pour obtenir une adresse IP publique fixe.

12. Lister les avantages (en dehors des débits) d'une solution DSL/VPN

Après ces démarches, l'adresse IP attribuée à l'interface publique est **66.101.21.12.** En plus des accès à Internet, les données circulant sur le routeur **Rte_A'click** proviennent des échanges entre l'imprimeur et le serveur de base de données **Ssgbd** ainsi que des échanges entre les développeurs à domicile et le serveur Intranet **Sweb.**

13. Écrire la table de routage du routeur Rte_A'click, à partir des informations de l'annexe 1.

Les fonctions de filtrage du routeur **Rte_A'click** sont déjà activées sur l'interface publique 66.101.21.12 et sur l'interface privée 172.16.120.253. Les tableaux ci-dessous donnent un extrait des tables de filtrage correspondant à chacune de ces interfaces :

Table de filtrage de l'interface publique (66.101.21.12) du routeur Rte_A'click

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole	Action
1	Toutes	Tous	66.101.21.12/32	tous	GRE	Accepter
2	**66.101.21.12/32**	**1723**	**Toutes**	**tous**	**TCP (établi)**	**Accepter**
3	**Toutes**	**Tous**	**66.101.21.12/32**	**1723**	**TCP**	**Accepter**
4	Toutes	Tous	66.101.21.12/32	500	UDP	Accepter
6	Toutes	Tous	66.101.21.12/32	1701	UDP	Accepter
7	Toutes	Tous	66.101.21.12/32	4500	UDP	Accepter
…	…					
Défaut	Toutes	Tous	Toutes	Tous	Tous	Bloquer

Table de filtrage de l'interface privée (172.16.120.253) du routeur Rte_A'click

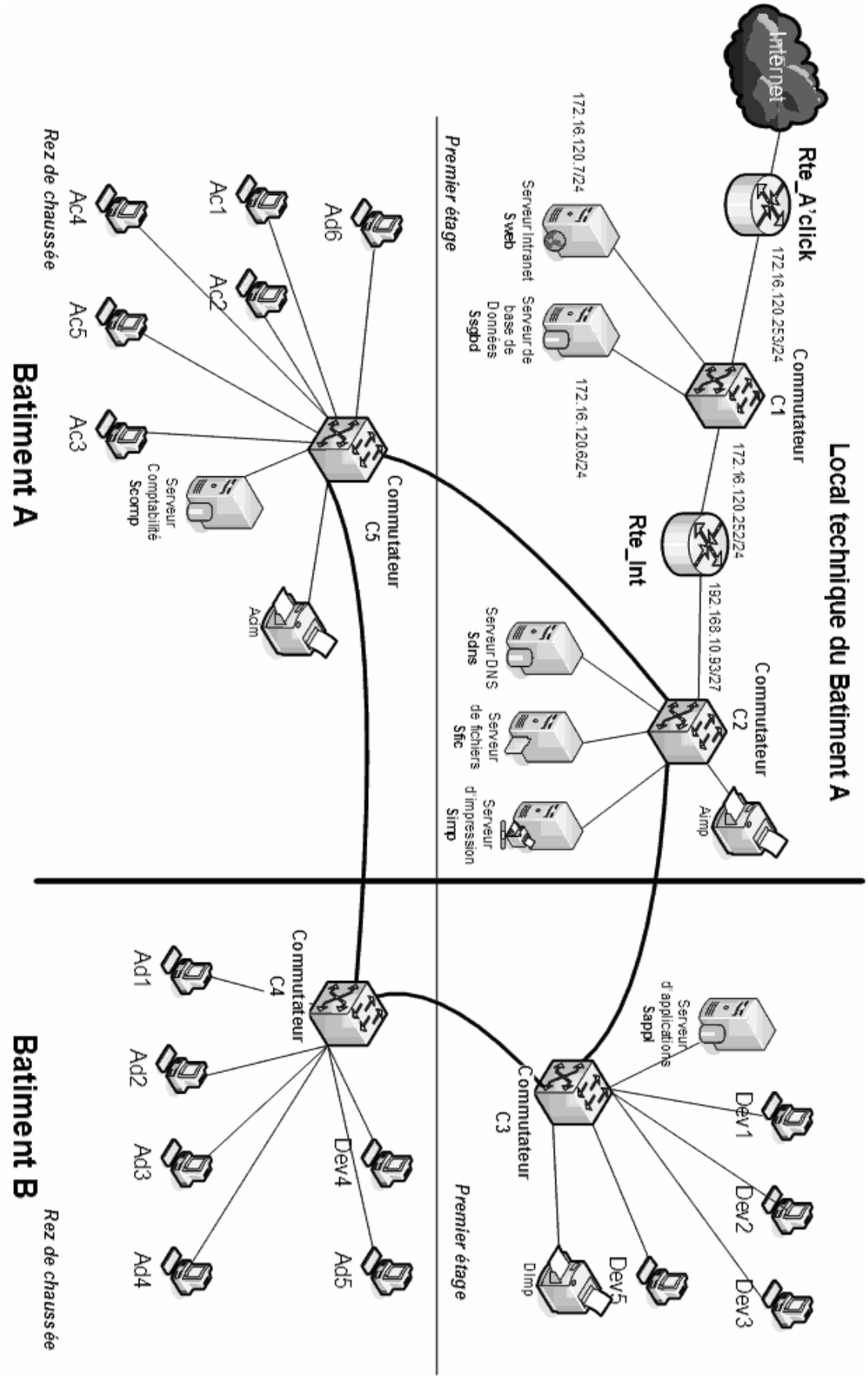
N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole	Action
…	…					
Défaut	Toutes	Tous	Toutes	Tous	Tous	Accepter

14. Expliquer les règles de filtrage 2 et 3 appliquées sur l'interface publique.

Lors de la mise en place du tunnel à la connexion, le serveur VPN doit attribuer aux développeurs à domicile une adresse IP, prise sur une étendue statique allant de **172.16.120.8** à **172.16.120.15**. L'imprimeur, quant à lui, doit toujours recevoir l'adresse IP **172.16.120.100**.
Les développeurs à domicile ont accès au serveur de base de données **Ssgbd** et au serveur Intranet **Sweb**, mais en aucun cas l'imprimeur ne pourra accéder au serveur Intranet **Sweb**.
Ni les développeurs à domicile, ni l'imprimeur ne doivent avoir accès au réseau interne de la société.

15. Ajouter la (les) règle(s) de filtrage à mettre en place sur l'interface 172.16.120.253 du routeur Rte_A'click, afin de respecter les accès précisés ci-dessus, sachant que l'action de la règle par défaut est « Accepter ».

Annexe 1 : Réseau Ethernet de la société A'CLICK



Annexe 2 : Rappel sur les VLAN

Les réseaux locaux virtuels (VLAN) permettent de créer des domaines de diffusion, gérés par des commutateurs. Une trame ne peut être associée qu'à un VLAN et cette trame ne peut être diffusée que sur les ports du commutateur associés à ce VLAN. Une trame ou un port peuvent être associés à un VLAN de manière statique ou dynamique :

- **Statique** : chaque port du commutateur est affecté à un VLAN par l'administrateur, une trame en entrée sur ce port sera associée au VLAN du port. On parle de **VLAN de niveau 1** ou VLAN par port.
- **Dynamique** : chaque port du commutateur se voit affecté dynamiquement à un VLAN à partir d'une information contenue dans la trame en entrée sur ce port. Cette affectation peut être définie en fonction de l'adresse MAC émettrice, de l'adresse IP émettrice, d'un protocole, etc. contenues dans la trame. On parle de **VLAN de niveau 2** (VLAN d'adresse MAC) **de niveau 3** (VLAN d'adresse IP) ou de **niveau applicatif** (VLAN basé sur les protocoles d'application).

On considère qu'un port de commutateur ne sera associé qu'à un seul VLAN à l'exception des ports d'interconnexion 802.1q. Un port 802.1q (dit tagged port) transporte des trames étiquetées avec un en-tête 802.1q qui permet d'associer la trame à un VLAN. Ce port est généralement réservé à la communication entre commutateurs.

Une trame ne peut être associée qu'à un seul VLAN. Chaque VLAN peut être géré par un commutateur ou par plusieurs et un commutateur peut gérer un ou plusieurs VLAN.

Lorsqu'un commutateur reçoit une trame de diffusion (broadcast), il la transmet d'une part à l'ensemble des ports sur lesquels sont reliés les postes appartenant au même VLAN que l'émetteur, d'autre part aux ports 802.1q affectés à ce VLAN.

Annexe 3 : Plan d'adressage IP en fonction des réseaux locaux virtuels

Chaque VLAN correspond à un sous-réseau IP.

- VLAN 1 (VLAN par défaut) : Pour les postes du service administratif, adresse réseau 192.168.10.32 masque 255.255.255.224
- VLAN 2 : Pour les postes du service de comptabilité, adresse réseau 192.168.10.64 masque 255.255.255.224
- VLAN 3 : Pour les postes du service développement et serveurs, adresse réseau 192.168.10.96 masque 255.255.255.224

La communication entre les VLAN est assurée par la fonction de routage activée sur C2, commutateur de niveau 3. Pour constituer la table de routage de C2, une adresse IP est affectée à chaque VLAN sur le commutateur C2, soit :

VLAN 1 : 192.168.10.62/27 VLAN 2 : 192.168.10.94/27 VLAN 3 : 192.168.10.126/27

Chaque poste du réseau est configuré avec une passerelle par défaut qui est l'adresse IP du VLAN correspondant, mis en place sur le commutateur C2, soit :

- Service administratif, VLAN 1 (VLAN par défaut), passerelle par défaut : 192.168.10.62
- Service de comptabilité, VLAN 2, passerelle par défaut : 192.168.10.94
- Service de développement et serveurs, VLAN 3, passerelle par défaut : 192.168.10.126

Annexe 4 : Configuration des commutateurs et des réseaux locaux virtuels

Commutateur C2 :
Administrable sur le VLAN2, 192.168.10.33/27
Protocole 802.1q activé, ports : c2f1, c2f2
Routage activé
Table gérée du C2

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c2e1	Aimp	c2e2	Rte_Int	c2e3	Sdns
c2e6				c2e4	Sfic
c2e7				c2e5	Simp
c2e8					
c2e9					
c2ea					
c2eb					
c2ec					

Commutateur C3 :
Administrable sur le VLAN1, 192.168.10.34/27
Protocole 802.1q activé, ports : c3f1, c3f2
Table gérée du C3

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c3e7				c3e1	Sappl
c3e8				c3e2	Dev1
c3e9				c3e3	Dev2
c3ea				c3e4	Dev3
c3eb				c3e5	Dev5
c3ec				c3e6	Dimp

Commutateur C5 :
Administrable sur le VLAN3, 192.168.10.97/27
Protocole 802.1q activé, ports : c5f1, c5f2
Table gérée du C5

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c5e1	Ad6	c5e2	Ac1	c5e8	Scomp
c5e9		c5e3	Ac2		
c5ea		c5e4	Ac3		
c5eb		c5e5	Ac4		
c5ec		c5e6	Ac5		
		c5e7	Acim		

Commutateur C4 :
Administrable sur le VLAN1, 192.168.10.35/27
Protocole 802.1q activé, ports : c4f1, c4f2
Table gérée du C4

VLAN1		VLAN2		VLAN3	
Port	Poste	Port	Poste	Port	Poste
c4e1	Ad1			c4e6	Dev4
c4e2	Ad2				
c4e3	Ad3				
c4e4	Ad4				
c4e5	Ad5				
c4e7					
c4e8					
c4e9					
c4ea					
c4eb					
c4ec					

Chaque commutateur dispose d'au moins une adresse IP et est administrable **sur un seul VLAN**.
Seul C2 est un commutateur de niveau 3 qui possède une fonction de routage. Il est configuré pour assurer la communication entre les réseaux locaux virtuels.
La commande pour ajouter une route dans la table de routage de C2 est la suivante :
Syntaxe :

ADD IP ROUTE=ipadd1 **INTERFACE**=vlan **NEXTHOP**=ipadd2 [**MASK**=ipadd3]

Paramètres :

ROUTE ipadd1 : définit l'adresse IP du réseau destinataire (0.0.0.0 pour la route par défaut).
INTERFACE vlan : définit le VLAN sur lequel est associée la route à ajouter (par exemple : INTERFACE=vlan1).
NEXTHOP ipadd2 : définit l'adresse IP du prochain saut (routeur) pour cette route.
MASK ipadd3 : définit le masque associé à cette route (réseau destinataire). Ce paramètre est facultatif. S'il n'est pas défini, c'est le masque de la classe de l'adresse IP du réseau destinataire qui est utilisé (0.0.0.0 pour la route par défaut).

Annexe 5 : Le réseau VPN (Virtual Private Network)

Ce réseau VPN utilise soit le protocole **PPTP** (Point to Point Tunneling Protocol), soit le protocole **L2TP** (Layer Two Tunneling Protocol) pour établir une connexion.
Le serveur VPN : Le serveur VPN doit posséder une **adresse IP publique fixe** afin que les clients VPN puissent utiliser cette adresse ou un nom DNS correspondant pour établir leur connexion VPN.
Lors de la demande de connexion du client VPN, le serveur VPN attribue aux clients VPN une adresse IP privée prise sur une étendue statique prédéfinie.
Les paquets VPN entrent sur l'interface publique du serveur VPN. Après vérification des filtres en entrée, celui-ci les désencapsule du tunnel crypté (déchiffrement des données) et envoie le datagramme IP privé en sortie sur l'interface privée qui applique les filtres avant de transmettre le paquet vers le réseau privé.

Le filtrage du serveur VPN :
Le pare-feu doit laisser entrer sur l'interface publique les paquets VPN suivants :

- **Pour un tunnel PPTP (Point to Point Tunneling Protocol) :**

Adresse IP source : adresse IP publique du client VPN source
Adresse IP destination : adresse IP publique du serveur VPN destination
Port de destination : TCP/1723 (pour l'établissement et la maintenance du tunnel)
ID de protocole : GRE/47 (protocole spécifique pour les données encapsulées dans le tunnel)

- **Pour un tunnel L2TP/IPSec (Layer Two Tunneling Protocol / Internet Protocol Security) :**

Adresse IP source : adresse IP publique du client VPN source
Adresse IP destination : adresse IP publique du serveur VPN destination
Port de destination : UDP/500 (pour la gestion des clés d'authentification utilisées pour sécuriser les informations)
Port de destination : UDP/1701 (trafic L2TP)
Port de destination : UDP/4500 (IPSec NAT-Transversal)

Corrigé Exonet N° 26

Question 1. Présenter les critères qui plaident en faveur de l'utilisation de réseaux locaux virtuels.

Le responsable du réseau a décidé de mettre en œuvre des réseaux locaux virtuels pour isoler les flux entre les différents services (chaque VLAN étant associé à un réseau IP) et améliorer ainsi la sécurité des échanges (les postes de même VLAN communiquent entre eux) et optimiser l'utilisation de la bande passante (broadcast).

Question 2. Indiquer la classe, l'adresse réseau et le masque par défaut correspondant au plan d'adressage spécifié à l'annexe 3. Justifier les réponses.

Classe : C car 192 en binaire commence par 110 - Adresse réseau : 192.168.10.0 car on trouve par exemple une adresse 192.168.10.33 et qu'en classe C on considère les 3 premiers octets comme l'adresse de réseau. Masque par défaut 255.255.255.0

Question 3. Calculer le nombre d'hôtes que peut accueillir chacun des réseaux virtuels avec ce plan d'adressage.

Masque des sous-réseaux : 255.255.255.224, soit le dernier octet en binaire : 1110 0000.
Donc 3 bits pour les sous-réseaux, reste 5 bits pour les postes, soit 2^5-2 = 30 hôtes possibles par VLAN.

Question 4. Donner le nombre de domaines de diffusion (broadcast) mis en place par la configuration des commutateurs C2, C3, C4 et C5.

Il y a trois VLAN, donc trois **domaines de diffusion**.

Question 5. Donner la raison pour laquelle l'administration du commutateur C2 ne peut se faire actuellement que par le câble console. Proposer une solution pour résoudre ce problème.
Que se passe-t-il ? L'administrateur ne peut pas administrer le commutateur C2.
Justification :
Car le commutateur C2 est administrable uniquement sur le **VLAN2**.
Or, lorsque l'on se connecte sur le port **C2e8** le portable est rattaché au **VLAN1** ce qui implique une impossibilité d'administrer le commutateur C2.
Solutions :
1. Sur le commutateur C2 : changer le VLAN d'administration (passé du VLAN2 en VLAN1)
2. Sur le commutateur C2 : changer le port c2e8 en VLAN2 (avec cette solution, l'IP du commutateur n'est pas compatible avec le VLAN2).

Question 6. Expliquer pourquoi ce déplacement a généré ce problème. Proposer une solution pour que le poste Dev5 puisse de nouveau communiquer avec son serveur d'applications à partir de son nouvel emplacement.

Justification :
Avant le déplacement, le poste Dev5 appartient au VLAN3, port c3e5 du commutateur C3.
Après le déplacement, il est connecté sur le port c4e7 du commutateur C4, qui appartient au VLAN1.
Dev5, placé dans le VLAN1, ne peut plus communiquer directement avec le VLAN3 et sa configuration IP ne permet pas de communiquer avec le VLAN3 en utilisant sa passerelle par défaut (routage activé sur C2).
Solution :
Sur le commutateur C4 : Configurer le port c4e7 en VLAN3.

Question 7. Écrire l'instruction qui ajoute une route dans la table de routage de C2 pour autoriser tous les postes du réseau à accéder à Internet.

L'instruction est :
ADD IP ROUTE=0.0.0.0 INTERFACE=vlan2 NEXTHOP=192.168.10.93

ou (le masque est facultatif pour la route par défaut)
ADD IP ROUTE=0.0.0.0 INTERFACE=vlan2 NEXTHOP=192.168.10.93 MASK=0.0.0.0

Question 8. Expliquer l'expression "tempête de broadcast". Indiquer quel protocole (ou algorithme) l'administrateur doit activer sur les commutateurs pour résoudre ce problème.

Explication de l'expression
Les liaisons redondantes entraînent que chaque trame parcourant des chemins différents passent plusieurs fois par le même commutateur qui régénère de nouvelles trames etc. On appelle ça une « tempête de broadcast ».
Choix de l'algorithme :
Les liaisons redondantes doivent être invalidées (suite à la formation de liaison inter-commutateur) sous peine de diffuser en plusieurs exemplaires des trames de broadcast et d'autres trames.
Pour y remédier il faut s'assurer que les commutateurs gèrent un algorithme de gestion des redondances comme **STP** (Spanning Tree Protocol) ou protocole **802.1d** et l'activer sur tous les commutateurs.

Question 9. Déterminer la bande passante minimum nécessaire, exprimée en Kbit/s que doit supporter la liaison pour ramener le temps de transfert d'une page à environ 10 secondes (justifier la réponse, prendre 1 Ko = 1 000 octets).

Bande passante à déterminer :
Bande passante : Soit 15 % de données de gestion : 300 * 1,15 = 345 ko pour une page de magazine.
Le temps de transfert actuel est de 43,12 secondes : [(345 * 1000 * 8) / (64 * 1000)], soit 345 / 8.
Pour ramener à 10 secondes :
10 = [(345 * 1000 * 8) / (d * 1000)]
d = (345 * 8) / 10
Il faut un débit réel de 276 kbit/s.

Question 10. Expliquer les principales différences techniques qui existent entre l'ADSL et le SDSL proposées par l'administrateur.

ADSL (Asymetric DSL) est la technique utilisée actuellement. Les canaux (la voie descendante allant de l'abonné vers le réseau et la voie montante allant du réseau vers l'abonné) sont asymétriques c'est-à-dire que leur débit est différent.
SDSL (Symetric DSL ou Single line DSL) est une version monoligne de HDSL. Les canaux (la voie descendante allant de l'abonné vers le réseau et la voie montante allant du réseau vers l'abonné) sont symétriques c'est-à-dire que leur débit est identique.

Question 11. Expliquer la démarche que doit suivre l'administrateur du réseau pour obtenir une adresse IP publique fixe.

Faire une demande d'adresse IP Publique fixe auprès du fournisseur d'accès Internet.

Question 12. Lister les avantages (en dehors des débits) d'une solution DSL/VPN.

Connexion permanente du fait de la liaison DSL, coût forfaitaire et indépendant de la distance
Sécurité liée au VPN : encapsulation de la trame cryptée et authentification.

Question 13. Écrire la table de routage du routeur Rte_A'click, à partir des informations de l'annexe 1.

Table de routage pour Rte_A'click

Réseau	Masque	Routeur	Interface
0.0.0.0	0.0.0.0	**@IP_FAI_A'Click**	66.101.21.12
192.168.10.0	255.255.255.0	172.16.120.252	172.16.120.253
172.16.120.0	255.255.255.0	172.16.120.253	172.16.120.253

On acceptera en lieu et place de l'adresse @IP_FAI_A'Click une adresse publique cohérente.

Question 14. Expliquer les règles de filtrage 2 et 3 appliquées sur l'interface publique.

Le pare-feu doit laisser entrer les flux VPN sur l'interface publique.
Les règles de filtrage 2 et 3 servent à l'établissement et le maintien du tunnel VPN, à la connexion des clients VPN.

Question 15. Ajouter la (les) règle(s) de filtrage à mettre en place sur l'interface 172.16.120.253 du routeur Rte_A'click afin de respecter les accès précisés ci-dessus, sachant que l'action de la règle par défaut est « Accepter ».

Table de filtrage de l'interface 172.16.120.253 du routeur Rte_A'click :

N° de règle	Adresse source	Port source	Adresse destination	Port destination	Protocole transport	Action
1	172.16.120.100/32	Tous	172.16.120.7/32	Tous	Tous	Bloquer
2	172.16.120.100/32	Tous	192.168.10.0/24	Tous	Tous	Bloquer
3	172.16.120.8/29	Tous	192.168.10.0/24	Tous	Tous	Bloquer
…	…					
Défaut	Toutes	Tous	Toutes	Tous	Tous	Accepter

EXONET N° 27

La société Tholdi est implantée dans plusieurs installations portuaires européennes. Elle est spécialisée dans la gestion de containeurs destinés au transport de marchandises. Son siège social est situé en région parisienne et ses zones d'activités dans les ports de :

- Le Havre (France) ;
- Marseille (France) ;
- Hambourg (Allemagne) ;
- Anvers (Belgique) ;
- Rotterdam (Pays-Bas).

Chacune des implantations comporte un système informatique organisé en réseau local. Ces réseaux sont interconnectés afin de permettre l'échange d'informations en temps réel entre tous les sites.

Le réseau de cette entreprise est basé sur un protocole unique : TCP/IP V4. Les réseaux locaux utilisent une technologie Ethernet à 100 Mb/s pour la connexion des postes de travail et à 1 Gb/s pour tous les serveurs. Les différents sites sont reliés au siège par des liaisons spécialisées.

Tous les utilisateurs des différents sites accèdent aujourd'hui à l'Internet via le serveur *proxy* du siège.

La société THOLDI, toujours soucieuse de diminuer ses charges d'exploitation, décide de tester une solution RPV (Réseau Privé Virtuel) ou VPN (*Virtual Private Network*), pour remplacer ses actuelles liaisons louées reliant tous les ports au site de Paris. Le site pilote choisi pour ce projet est le site de Rotterdam. Vous êtes chargé de cette mission par l'administrateur réseau de la société.
Ce dernier vous a fourni le plan de la solution à mettre en place en **annexe 1** et le plan d'adressage en **annexe 2.**

1. Indiquer, en observant le plan d'adressage, de quelle classe d'adresses il s'agit. Expliquer s'il s'agit d'adresses privées ou publiques. Justifier les réponses.

Le projet commence par l'installation du routeur d'accès à l'Internet qui doit remplacer le routeur gérant la liaison louée avec Paris. Celui-ci possède une fonction NAT (Network Address Translation) et une adresse publique en 82.216.198.161/29.

2. Donner l'adresse de réseau public de Rotterdam. Justifier la réponse.

3. Déterminer le nombre d'hôtes pouvant être adressés sur ce sous-réseau. Donner les adresses utilisables pour ces hôtes ainsi que l'adresse de diffusion. Justifier la réponse.

Il s'agit maintenant d'installer le serveur RPV et de configurer les éléments du réseau indispensables à la réalisation de ce projet. Pour faciliter votre travail, l'administrateur réseau vous a fourni une documentation sur les RPV. Elle est disponible en **annexe 3**.
La configuration suivante a été retenue pour la mise en place du RPV entre le site de Rotterdam et le site de Paris :

- Le serveur RPV du réseau de Rotterdam, paramétré pour faire du routage et de la « tunnelisation », est installé à l'adresse réelle 172.30.192.100/19. Ce serveur RPV possède une carte virtuelle d'adresse 10.7.124.240/8.
- L'administrateur réseau s'est chargé de l'installation du serveur RPV de Paris. Ce dernier est installé sur la machine hébergeant le serveur DHCP. L'adresse virtuelle du serveur RPV de Paris est 10.119.255.97/8.
- Les paquets transportés par le RPV utilisent le protocole UDP et le port 1500.

- Le routeur Internet du site de Paris possède l'adresse 83.225.12.17/30. Pour autoriser la redirection des paquets reçus sur le routeur Internet de ce site vers le serveur RPV de ce même site, l'administrateur réseau a mis en place une redirection de port ou DNAT (*Destination Network Address Translation*).

Vous êtes chargé(e) d'effectuer un paramétrage similaire sur le routeur Internet du site de Rotterdam. Pour effectuer ce travail vous utiliserez le modèle de tableau présenté ci-dessous.

Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
	DNAT					

4. Écrire, en utilisant le modèle de tableau présenté ci-dessus, la règle à mettre en place.

L'**annexe 4** vous présente la table de routage du serveur RPV de Rotterdam.

5. Indiquer, en observant la table de routage du serveur RPV de Rotterdam, si le site de Paris et le site de Rotterdam sont bien reliés par un tunnel d'adresse de réseau 10.0.0.0/8. Justifier la réponse.
6. Compléter la table de routage pour que le site de Rotterdam puisse communiquer avec le site du Havre via le serveur RPV de Paris.
7. Simplifier la table de routage obtenue en proposant une agrégation de routes. Justifier la réponse.
8. Indiquer l'adresse de passerelle qui doit être définie sur chaque ordinateur du site de Rotterdam.

Pour tester votre RPV, vous connectez votre portable à l'adresse 172.30.192.1/19 et vous exécutez la commande *ping*, en continu, vers le portable de l'administrateur réseau situé à Paris à l'adresse 172.30.32.1/19. Vous lancez alors une capture de paquets sur la carte réseau réelle du serveur RPV de Rotterdam. Cette capture est présentée en **annexe 5**.
9. Expliquer, en utilisant la capture de paquets de l'annexe 5, pourquoi les adresses IP d'origine et de destination des paquets en entrée et en sortie du serveur RPV (routeur chiffrant) sont différentes alors qu'il s'agit pourtant du même message (*ping request* pour les lignes 1 et 2).

Vous testez maintenant le fonctionnement global de l'interconnexion du site de Rotterdam avec le site de Paris depuis un poste fixe de Rotterdam. Vous constatez que le serveur DHCP de Paris n'arrive pas à vous fournir une adresse IP.
10. Indiquer la fonctionnalité qui n'a pas été mise en place sur le site de Rotterdam. Justifier la réponse.

Après la mise en place de l'architecture décrite en **annexe 1**, on se préoccupe maintenant des accès *Wi-Fi* pour le site de Rotterdam.

Les conducteurs d'engins du port maritime sont équipés de PDA (*Personal Digital Assistant* ou Assistant Personnel) de type HP iPAQ hx2490, qui ne supportent que le chiffrement en mode *Wep*. Les informations sur chaque transport sont ainsi saisies en temps réel.

Le réseau *Wi-Fi* de la société THOLDI respecte la norme 802.11g et offre un débit théorique de 54 Mbits/s (26 Mbits/s réels) sur la bande de fréquence 2,4 GHz. Cette norme offre une compatibilité descendante avec la norme 802.11b. Le mode de fonctionnement utilisé est le mode infrastructure, centralisé autour d'un seul point d'accès *Wi-Fi* pour le site. Ce point d'accès joue également le rôle de commutateur et dispose de six ports RJ45 dont trois sont libres.

11. Donner les avantages du mode point d'accès (infrastructure) par rapport au mode d'égal à égal (ad hoc).

12. Expliquer ce qu'est un SSID.

Le point d'accès *Wi-Fi* a été paramétré ainsi :

- Non diffusion du SSID du réseau ;
- Chiffrement Wep activé ;
- Activation du filtrage par adresse MAC.

13. Citer les paramètres *Wi-Fi* à enregistrer sur les PDA pour pouvoir se connecter au commutateur *Wi-Fi*.

Pour accentuer la sécurité des LAN du site, l'administrateur réseau envisage de mettre en place des VLAN. Il espère ainsi mieux gérer le trafic généré par les PDA des camionneurs. Il pense installer deux VLAN : un VLAN « Wifi » pour les seuls PDA et un VLAN « Lan » pour le reste du site. Le commutateur *Wi-Fi* permet d'associer un SSID à chaque VLAN et permet de gérer des VLAN par port.

14. Décrire le principe de fonctionnement d'un VLAN par port.

Avant de mettre en œuvre cette solution, l'administrateur souhaite étudier ses conséquences sur la configuration actuelle du réseau du site de Rotterdam.

15. Donner le nombre de domaines de diffusion ainsi défini sur le site.

16. Déterminer si l'administrateur réseau peut conserver le plan d'adressage IP des PDA. Justifier la réponse.

17. Exposer une solution permettant au PDA du VLAN « Wifi » de communiquer avec les postes du VLAN « Lan » (*les commutateurs Wi-Fi sont conservés mais un matériel peut être ajouté*). Préciser les configurations à mettre en place sur le commutateur *Wi-Fi* et sur les PDA.

L'objectif attendu par l'administrateur réseau est la limitation d'écoute passive par un portable pirate disposant d'une liaison *Wi-Fi* et ayant cassé la clé *Wep*.

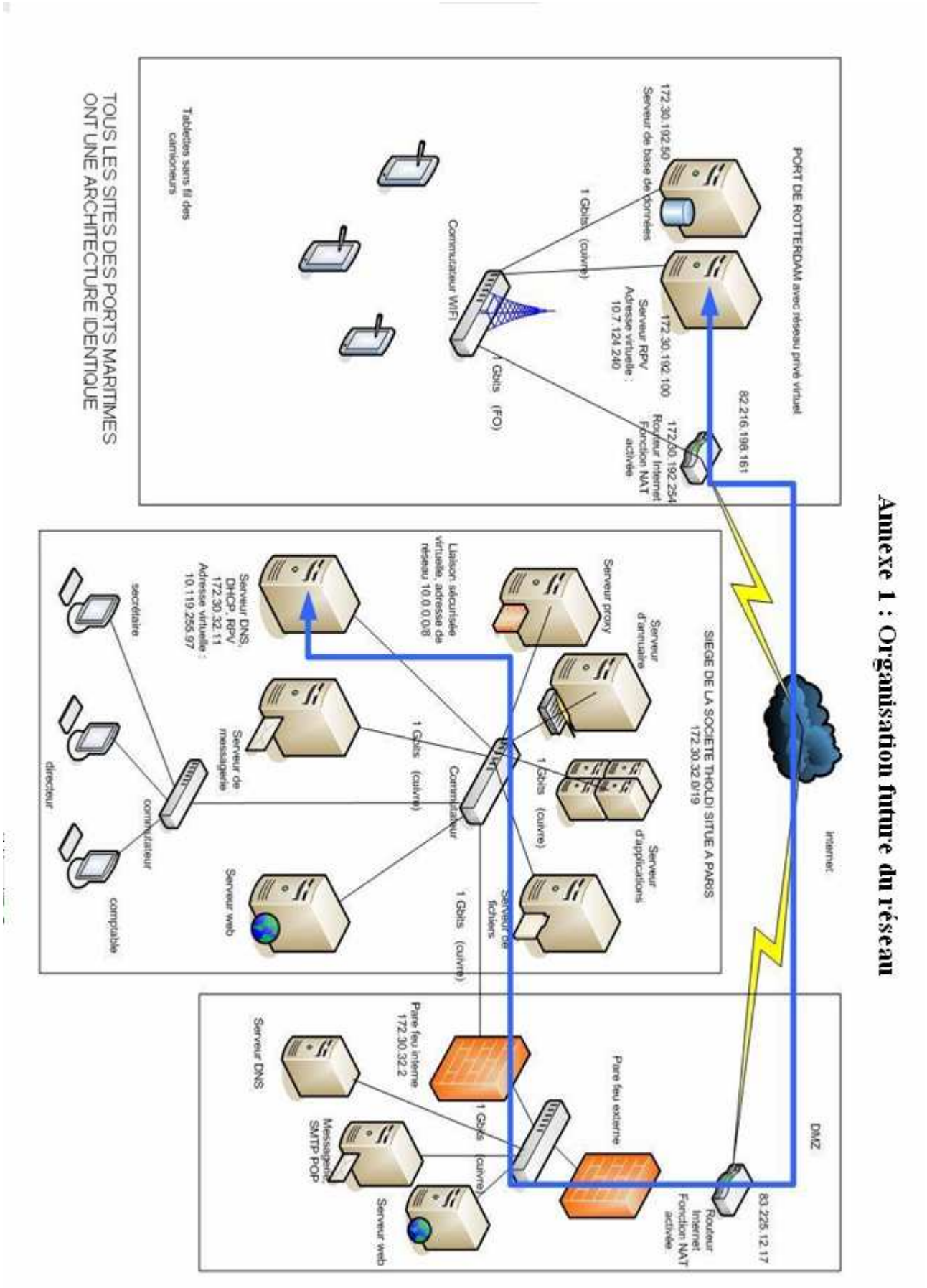
18. Indiquer, avant la mise en œuvre des VLAN, la nature des échanges entre les serveurs du port maritime pouvant être capturés par un portable pirate disposant d'une liaison Wi-Fi. Justifier la réponse.

19. Indiquer, après la mise en œuvre des VLAN, la nature des échanges entre les serveurs du port maritime pouvant être capturés par un portable pirate disposant d'une liaison Wi-Fi. Justifier la réponse.

Après cette étude préalable l'administrateur réseau décide d'abandonner la mise en place des VLAN estimant que la solution n'est pas techniquement et financièrement adaptée.

20. Proposer une autre solution permettant de réduire les risques d'écoute passive et ses conséquences sur les équipements actuels

Annexe 1 : Organisation future du réseau



Annexe 2 : Plan d'adressage réseau de la société THOLDI

172.30.32.0/19 réseau du siège à Paris
172.30.64.0/19 réseau du port du Havre
172.30.96.0/19 réseau du port de Hambourg
172.30.128.0/19 réseau du port d'Anvers
172.30.160.0/19 réseau du port de Marseille
172.30.192.0/19 réseau du port de Rotterdam

Annexe 3 : Fonctionnement d'un RPV (Réseau privé virtuel)

Le RPV correspond à une interconnexion de réseaux locaux via une technique de « tunnel ». On parle de RPV lorsqu'un organisme interconnecte ses sites via une infrastructure partagée avec d'autres organismes. C'est sur Internet et les infrastructures IP que se sont développées les techniques de « tunnel ».
Le RPV utilise Internet comme support de transmission en utilisant un protocole de « tunnelisation » qui encapsule les données à transmettre, données qui sont elles-mêmes chiffrées. On parle alors de RPV pour désigner le réseau ainsi créé, qui est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet) et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du RPV peuvent accéder aux données en clair.
Le RPV permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie, il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public, donc non garanti.

Annexe 4 : Table de routage du serveur RPV de Rotterdam

Destination réseau	Masque réseau	Adresse de Passerelle	Adresse Interface
0.0.0.0	0.0.0.0	172.30.192.254	172.30.192.100
10.0.0.0	255.0.0.0	10.7.124.240	10.7.124.240
172.30.32.0	255.255.224.0	10.119.255.97	10.7.124.240
172.30.192.0	255.255.224.0	172.30.192.100	172.30.192.100

Annexe 5 : Capture de paquets sur le serveur RPV de Rotterdam

No.	Sens	Source	Destination	Protocol	Info
1	Entrée	172.30.192.1	172.30.32.1	ICMP	Echo (ping) request
2	Sortie	172.30.192.100	83.225.12.17	UDP	Source port: 1500 Destination port: 1500
3	Entrée	83.225.12.17	172.30.192.100	UDP	Source port: 1500 Destination port: 1500
4	Sortie	172.30.32.1	172.30.192.1	ICMP	Echo (ping) reply

Corrigé Exonet N° 27

Question 1. Indiquer, en observant le plan d'adressage, de quelle classe d'adresses il s'agit. Expliquer s'il s'agit d'adresses privées ou publiques. Justifier les réponses.

Il s'agit de classe B car les valeurs de 128 à 191 pour le premier octet définissent la classe B.
Il s'agit d'adresses privées car de 172.16.0.0 à 172.31.255.255 ce sont des adresses privées.

Question 2. Donner l'adresse du réseau public de Rotterdam. *Justifier la réponse*.

L'adresse du routeur internet est 82.216.198.161/29. Avec un masque de 29 on utilise les cinq premiers bits du dernier octet pour adresser les sous-réseaux et les trois derniers pour adresser les hôtes du sous-réseau.
Les adresses réseau des sous-réseaux varient donc de 8 en 8.
soit 0,8,16,32,40,48,56,64,72,80,88,96,104,112,120,128,136,144,152,160,168. L'adresse du sous-réseau public de Rotterdam est donc 82.216.198.160/29.

Question 3. Déterminer le nombre d'hôtes pouvant être adressés sur ce sous-réseau. Donner les adresses utilisables pour ces hôtes ainsi que l'adresse de diffusion. *Justifier la réponse*.

Les 3 bits restant permettent d'adresser 2^3-2 = 6 hôtes. Premier hôte 82.216.198.161, dernier hôte 82.216.198.166, adresse de diffusion 82.216.198.167.

Question 4. En utilisant le modèle de tableau présenté ci-dessous, donner la règle à mettre en place.

Interface	Type	Protocole	Adresse publique	Port public	Adresse privée	Port privé
82.216.198.161	DNAT	UDP	82.216.198.161/29	1500	172.30.192.100/19	1500

Question 5. Indiquer, en observant la table de routage du serveur RPV de Rotterdam, si le site de Paris et le site de Rotterdam sont bien reliés par un tunnel d'adresse de réseau 10.0.0.0/8. *Justifier la réponse*.

Destination réseau	Masque réseau	Adr. Passerelle	Adr. Interface	Métrique
0.0.0.0	0.0.0.0	172.30.192.254	172.30.192.100	20
10.0.0.0	255.0.0.0	10.7.124.240	10.7.124.240	20
172.30.32.0	255.255.224.0	10.119.255.97	10.7.124.240	1
172.30.192.0	255.255.224.0	172.30.192.100	172.30.192.100	20

On constate bien que pour atteindre le réseau de Paris situé en adresse 172.30.32.0/19 on sort par l'interface 10.7.124.240 pour atteindre la passerelle 10.119.225.97. Cette adresse de passerelle est en fait l'adresse virtuelle du serveur RPV de PARIS. Tous les paquets à destination de Paris passeront donc bien par le tunnel RPV d'adresse de réseau 10.0.0.0/8.

Question 6. Compléter la table de routage pour que le site de Rotterdam puisse communiquer avec le site du Havre via le serveur RPV de Paris.

Il faut rajouter la ligne suivante :

172.30.64.0	255.255.224.0	10.119.255.97	10.7.124.240

Question 7. Simplifier la table de routage obtenue en proposant une agrégation de routes. *Justifier la réponse.*

Les routes concernant le site de Paris et du Havre peuvent être regroupées car elles ont une partie commune en binaire sur le troisième octet :
32 00100000
64 01000000

172.30.0.0	255.255.128.0	10.119.255.97	10.7.124.240

Question 8. Indiquer l'adresse de passerelle qui doit être définie sur chaque ordinateur du site de Rotterdam.

Les communications intersites doivent passées par le RPV. L'adresse de passerelle des hôtes de Rotterdam doit être l'adresse du serveur RPV soit 172.30.192.100. Comme le montre la table de routage si le réseau de destination est inconnu, le serveur RPV route le paquet vers sa passerelle par défaut, le routeur internet. Les accès à l'Internet ne sont donc pas perturbés par la mise en place de cette passerelle par défaut.

Question 9. Expliquer, en utilisant la capture de paquets de *l'annexe 5*, pourquoi les adresses IP d'origine et de destination des paquets en entrée et en sortie du serveur RPV (routeur chiffrant) sont différentes alors qu'il s'agit pourtant du même message (*ping request* lignes 1 et 2).

No.	Sens	Source	Destination	Protocol	Info
1	Entrée	172.30.192.1	172.30.32.1	ICMP	Echo (ping) request
2	Sortie	172.30.192.100	83.225.12.17	UDP	Source port: 1500 Destination port: 1500
3	Entrée	83.225.12.17	172.30.192.100	UDP	Source port: 1500 Destination port: 1500
4	Sortie	172.30.32.1	172.30.192.1	ICMP	Echo (ping) reply

Un serveur RPV encapsule les paquets d'origine pour les faire transiter dans le tunnel. La ligne 1 est le premier *echo request* de la commande *ping* émise par le portable de Rotterdam à destination du portable de l'administrateur réseau de Paris. Ce paquet est traité par le serveur RPV de la façon suivante : il y a chiffrement et encapsulation

Paquet reçu en premier par le serveur RPV

172.30.192.1	172.30.32.1	ICMP	Données

Le premier paquet pour pouvoir voyager sur internet est encapsulé dans ce deuxième paquet

172.30.192.100	83.255.12.17	1500	UDP	Données

La ligne 2 est donc le paquet qui encapsule les données chiffrées du « ping » de la ligne 1.

L'adresse 83.255.12.17 est l'adresse du routeur internet du site de Paris.
L'adresse 172.30.192.100, adresse du serveur RPV de Rotterdam, sera «natée» par le routeur internet de Rotterdam et deviendra 82.216.198.161.
Il existe donc dans les fichiers de configuration du serveur RPV, une correspondance entre son adresse virtuelle, son adresse réelle et son adresse publique.

Question 10. Indiquer la fonctionnalité qui n'a pas été mise en place sur le site de Rotterdam. *Justifier la réponse.*

Le site de Rotterdam et le site de Paris ne sont pas sur le même réseau. Le serveur DHCP est situé à Paris. Il est donc nécessaire d'installer un serveur relais DHCP sur le site de Rotterdam. En effet le serveur relais DHCP permet de relayer les demandes et les attributions d'adresses dans le port de Rotterdam depuis le serveur DHCP du site de Paris.

Question 11. Donner les avantages du mode point d'accès (infrastructure) par rapport au mode d'égal à égal (ad hoc).

	coût	Sécurité	Mise en œuvre
Infrastructure	Plus élevé	Très bonne avec un routeur	Point d'accès ou routeur wifi Cartes wifi
Ad hoc	Peu élevé	Peu sécurisé	Très simple Cartes wifi

Il s'agit ici du réseau d'une entreprise, le mode infrastructure est donc le mode le plus approprié.

Question 12. Expliquer ce qu'est un SSID.

Service Set Identifier, identifiant de 32 caractères de long au format ASCII servant de nom pour le réseau. La connaissance du SSID est nécessaire pour qu'une station puisse se connecter au réseau.

Question 13. Citer les paramétrages *Wi-Fi* à enregistrer sur les PDA pour pouvoir se connecter au commutateur *Wi-Fi*.

Il faut configurer le SSID sur le poste puisqu'il n'est pas diffusé.
Il faut définir la clé WEP utilisée par le point d'accès.

Question 14. Décrire le principe de fonctionnement d'un VLAN par port.

C'est l'association dans le commutateur d'un port à un numéro de VLAN. Toutes les trames émises et reçues sur le port ne seront commutées que vers un port appartenant au même VLAN. *Si plusieurs VLAN sont définies sur le port il faut que les trames soient étiquetées.*

Question 15. Donner le nombre de domaines de diffusion ainsi définis sur le site.

Deux domaines de diffusion sont gérés sur chaque site. Un par Vlan.

Question 16. Déterminer si l'administrateur réseau peut conserver le plan d'adressage IP des PDA. *Justifier la réponse.*

Les deux VLANS sont isolés. On peut conserver le même plan d'adressage IP mais dans ce cas on ne pourra jamais communiquer entre les deux Vlans. En effet pour communiquer en IP entre les deux VLANs il faut un routeur ce qui implique que les réseaux IP sur chaque Vlan soient différents.

Question 17. Exposer une solution qui permettrait au PDA du VLAN « Wifi » de communiquer avec les postes du VLAN « Lan » (*les commutateurs Wi-Fi sont conservés mais un matériel peut être ajouté*). Préciser les configurations à mettre en place sur le commutateur *Wi-Fi* et sur les PDA.

Il faut un routeur. Ce routeur aura deux cartes réseaux (réelles ou virtuelles) avec une adresse IP sur chacun des réseaux.
Si le routeur possède deux cartes réelles, il faut associer chacune de ces cartes à un VLAN et donc mettre à jour sur le commutateur *Wi-Fi* les associations VLAN <-> port (une carte sur *Wi-Fi* et une carte sur LAN).
Si le routeur ne possède qu'une carte réelle mais deux cartes virtuelles, il faut sur le commutateur *Wi-Fi* installer le protocole 802.1Q sur le port où est connectée cette carte réelle.
Sur les PDA, il faut paramétrer l'adresse IP de la carte réseau du routeur située sur le même VLAN comme passerelle.

Question 18. Indiquer, avant la mise en œuvre des VLAN, la nature des échanges entre les serveurs du port maritime pouvant être capturés par un portable pirate disposant d'une liaison *Wi-Fi*. *Justifier la réponse*.

Les échanges entre les serveurs sont commutés. Les échanges unicast ne seront pas capturables car non transmis par le point d'accès par contre les échanges *broadcast* le seront.

Question 19. Indiquer, après la mise en œuvre des VLAN, la nature des échanges entre les serveurs du port maritime pouvant être capturés par un portable pirate disposant d'une liaison *Wi-Fi*. *Justifier la réponse*.

Cela ne change pas grand chose. Les échanges entre les serveurs sont toujours commutés. Les échanges unicast ne seront pas capturables car non transmis par le point d'accès et isolés dans un VLAN. Par contre les échanges de *broadcast* ne seront pas transmis par le point d'accès car le SSID a été associé au VLAN Wifi.

Question 20. Proposer une autre solution permettant de réduire les risques d'écoute passive et ses conséquences sur les équipements actuels.

Il faut passer à un mode de chiffrement plus difficile à craquer que le chiffrement Wep, le chiffrement WPA par exemple. On peut aussi envisager la mise en place d'un serveur Radius et une authentification des PDA par certificats électroniques.

Le choix de chiffrement WPA impose le changement des PDA.

EXONET N° 28

La société FEFORT, installée en France, est spécialisée dans la torréfaction et l'assemblage de cafés.

Activité de l'entreprise
FEFORT possède des unités de production en Afrique, Amérique Centrale et Amérique du Sud qui s'occupent de la collecte de la matière première, « la cerise de café », auprès des producteurs locaux. Cette matière première est ensuite lavée et « dépulpée » sur place. Une fois séchés, les grains verts qui résultent de l'opération précédente traversent l'Atlantique, en bateau, jusqu'au Havre.
La société procède en France à la torréfaction des grains verts. Ceux-ci, grillés dans des fours, libèrent alors l'arôme attendu. Les laboratoires réalisent aussi, si nécessaire, l'assemblage des différentes variétés de café, tous les consommateurs n'ayant pas les mêmes attentes du produit, souvent en fonction de leurs habitudes culturelles.
Son client principal est la grande distribution sous sa propre marque ou sous la marque du distributeur.

Implantation géographique
Le siège de la société est situé en région PACA (Provence-Alpes-Côte d'Azur). Il regroupe les services administratifs et de direction, un service « qualité, recherche et développement » (Q–R&D) intégrant un laboratoire chargé de tester de nouveaux produits. Le service qualité est chargé de veiller à la qualité des processus de l'entreprise, aussi bien administratifs, que de production.
Le centre informatique principal est implanté au siège de la société. Les autres sites y accèdent pour l'essentiel de leurs traitements.
Le réseau et le parc informatique ont pris de l'ampleur au fil des années et il est nécessaire de le rationaliser.
Jeune diplômé(e), vous travaillez en tant que technicien(ne) sur le site principal, dans l'équipe « réseau et systèmes», chargée de l'architecture et de la sécurité de celui-ci.

Le réseau principal du siège regroupe un grand nombre de stations clientes (environ 250) et de serveurs. Bien que ce réseau s'appuie sur une arborescence de commutateurs, les diffusions sont nombreuses et pénalisent lourdement le réseau. De plus, la direction souhaite que les échanges de données entre les postes d'un même service ne soient pas, pour des raisons de confidentialité, accessibles aux autres services. Pour sécuriser et alléger la charge du réseau, Monsieur Godard, le directeur du service informatique envisage deux solutions :

- La première consiste à créer 8 sous-réseaux (7 services plus la liaison vers le pare-feu) en remplaçant le commutateur central (voir *annexe 1*) par un routeur IP à 8 interfaces. *Monsieur Godard vous demande d'étudier dans un premier temps la faisabilité de cette solution.*
- La seconde solution fait appel aux VLAN et *sera envisagée dans le dossier suivant.*

Étude de la première solution
Chaque service correspondra à un sous réseau. Monsieur Godard a choisi d'utiliser un masque de sous-réseau de 20 bits.

1. Donner l'écriture décimale pointée de ce masque et indiquer combien de sous réseaux pourront être créés à l'aide de celui-ci.
2. Proposer une adresse IP de réseau pour chacun des services. *La proposition doit être compatible avec les adresses statiques existantes indiquées dans l'annexe 2.*

3. Donner l'adresse de la passerelle par défaut des postes du service commercial, sachant qu'il s'agit de l'adresse disponible la plus élevée pour ce sous-réseau.

Suite à cette modification, les postes des différents services configurés en DHCP ne reçoivent plus leurs paramètres IP.

4. Expliquer la raison de ce dysfonctionnement et préciser les modifications à apporter, d'une part au serveur DHCP, d'autre part au nouveau routeur.

Pare-feu : Filtrage du trafic réseau

En complément de la protection des accès à l'entreprise prise en charge par le fournisseur d'accès Internet, le DSI envisage de filtrer le trafic réseau entre le siège et les unités du groupe.

Le pare-feu du siège doit être configuré pour :

- permettre à tous les utilisateurs l'accès à la navigation *web* via le serveur mandataire (*proxy*) du FAI (port 3128) ;
- limiter l'accès des unités du groupe uniquement au service informatique ;
- donner au service informatique (et donc au poste de l'administrateur) accès à l'ensemble des services et sites distants.

5. En utilisant le formalisme donné en *annexe 4*, donner les règles applicables en entrée de l'interface concernée permettant de respecter les consignes données. *Vous veillerez à limiter le nombre de règles à définir.*

DHCP : Création d'une étendue de secours

Chaque unité dispose de son propre serveur DHCP. L'administrateur du réseau souhaite introduire un dispositif de tolérance de panne s'appuyant sur le serveur DHCP du siège.

En cas de dysfonctionnement d'un serveur local, le serveur du siège devra donc pouvoir fournir leurs paramètres IP aux stations distantes qui en font la demande.

Vous avez été chargé(e) de tester la solution sur le site de Villeurbanne.

Le serveur DHCP local possède la configuration suivante :

Étendue : Villeurbanne
Plage d'adresses : 172.22.0.1 à 172.22.0.149
Masque : 255.255.0.0
Options
Passerelle : 172.22.250.204 (adresse interne du routeur 4)
DNS : 172.16.200.2

6. Indiquer les modifications à apporter afin de distribuer des adresses valides aux stations de Villeurbanne, sur une étendue de même taille.

DNS : Mise en place d'une délégation de zone

Le serveur DNS du siège prend en charge les résolutions de noms pour l'ensemble du groupe. La charge importante pour ce serveur et l'utilisation des liaisons distantes pénalisent les temps de réponse. Il a donc été décidé de mettre en place des serveurs DNS locaux sur le principe des délégations de zone. Chaque site gèrera sa propre zone dépendante de la zone principale du groupe.

L'arborescence souhaitée est donnée en *annexe 6*.

7. Apporter les modifications nécessaires au fichier de la zone *fefort.loc* (*annexe 5*) et écrire le fichier de la zone *villeurbanne.fefort.loc.*

Pour améliorer la tolérance aux pannes, il a été décidé que le serveur DNS du siège serait serveur secondaire pour chacun des domaines *fils*. En cas de défaillance d'un serveur DNS, les clients du site pourront alors utiliser les services du serveur DNS du siège.
Une première expérimentation de ce dispositif doit être mise en œuvre sur le site de Villeurbanne.

8. Expliquer les modifications à apporter au serveur DNS du siège d'une part et à celui du site de Villeurbanne d'autre part.

Le directeur vous suggère de mettre en place une solution basée sur l'utilisation de réseaux locaux virtuels (VLAN). Cette solution permettra de réduire le périmètre des domaines de diffusion et de sécuriser les échanges entre les services. L'acquisition d'un nouveau commutateur est nécessaire pour remplacer le commutateur actuel, notamment pour :

- Gérer les VLAN et la priorité des flux ;
- Éviter les tempêtes de diffusion ;
- Supporter la redondance de liens avec un autre commutateur de même type ;
- Administrer à distance le commutateur en mode console ainsi qu'à l'aide d'outils de supervision de réseau.

9. Déterminer la configuration matérielle et préciser les protocoles que devra supporter le nouveau commutateur. *Le rôle des fonctions et protocoles qu'il prendra en charge sera expliqué.*

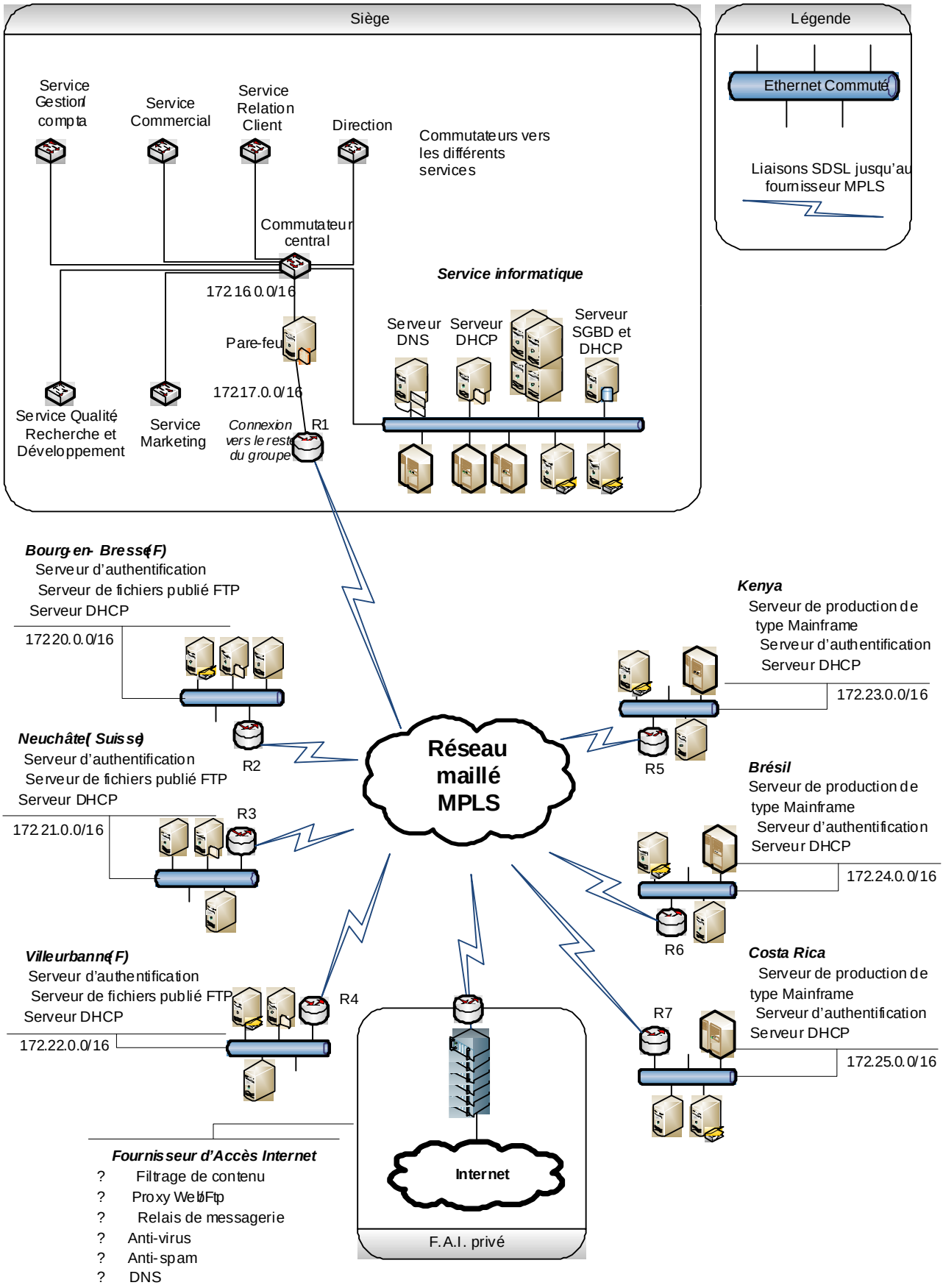
En vous documentant sur les VLAN afin de monter le dossier, vous vous apercevez que « l'étanchéité » qu'offrent les VLAN ne permettra plus aux postes de communiquer avec les serveurs du service informatique.

10. Proposer une solution matérielle complémentaire pour permettre aux postes de travail des différents services d'accéder aux serveurs du service informatique. Expliquer brièvement comment elle doit être mise en œuvre.

Une fois cette solution mise en place, un problème survient. Le service d'assistance téléphonique interne au groupe est débordé d'appels : les différents sites ne peuvent plus accéder aux serveurs. L'origine de la panne est trouvée : le routeur R1 est hors service.
Le problème est réglé par le remplacement du routeur défaillant par un nouveau routeur qu'il a fallu configurer. Le dépannage a nécessité une journée de travail. Après avoir reçu les chiffres de la perte d'exploitation générée par cette rupture de liaison, le DSI cherche à éviter qu'une telle interruption de service puisse à nouveau survenir. Ce dernier vous demande de proposer une solution permettant de garantir la continuité du service d'accès aux serveurs du siège lorsqu'une panne identique se présente.

11. Proposer une solution permettant de garantir la continuité du service d'accès aux serveurs du siège lors d'une panne du routeur. Expliquer les principes de fonctionnement de votre solution.

Annexe 1 – Schéma du réseau de la société FEFORT



Annexe 1 (suite)

Les sites du groupe sont interconnectés par un réseau professionnel MPLS. Le réseau et son adressage sont gérés par le fournisseur. Le groupe FEFORT peut à tout moment observer le fonctionnement de celui-ci, détecter les goulets d'étranglement et éventuellement demander le redimensionnement de certaines liaisons « sites vers MPLS ». C'est pour cela qu'il est important d'économiser la bande passante inter-sites.

Plan d'adressage du groupe FEFORT

Classe B privée : 172.16.0.0/16 à 172.25.0.0/16
Le siège possède 2 réseaux : 172.16.0.0 (services siège), 172.17.0.0 (liaison PF-Routeur)
Chaque service dispose d'un maximum de 50 stations.
Seuls le service informatique et le pare-feu utilisent des adresses statiques.

Pour information : MPLS (*Multi-Protocol Label Switching*)

Un réseau MPLS est mis en place par un opérateur spécialisé, il permet à des entreprises très étendues d'interconnecter leurs sites très facilement comme s'ils appartenaient à un réseau local. Le protocole MPLS intervient au niveau 2 du modèle OSI. On s'y connecte le plus souvent avec une liaison SDSL.

Différentes entreprises peuvent emprunter les mêmes chemins, car « l'étanchéité » entre les différents « clients » de ce réseau est assurée, en partie, par un « marquage » des trames. La marque (*tag*) est unique pour une entreprise.

Annexe 2 : Adresses statiques attribuées au siège

Machine	**@ IP**	**F.Q.D.N.**
Serveur d'authentification	172.16.200.1	logon.fefort.loc
Serveur DNS	172.16.200.2	ns.fefort.loc
Serveur DHCP	172.16.200.3	dhcp.fefort.loc
Serveur de messagerie	172.16.200.4	mail.fefort.loc
Serveur de développement	172.16.200.5	dev.fefort.loc
Serveur de fichiers	172.16.200.6	fichiers.fefort.loc
Serveur de sauvegardes	172.16.200.7	backup.fefort.loc
Serveur d'impressions	172.16.200.8	imp.fefort.loc
Serveur de bases de données	172.16.200.9	bdd.fefort.loc
Ferme de serveurs d'applications	172.16.200.10	appli.fefort.loc
Poste admininistrateur	172.16.200.200	poste_admin.fefort.loc
Pare-feu	172.16.220.1 172.17.0.1	
Routeur 1 (R1)	172.17.0.201	

Annexe 3 : Configuration du serveur DHCP du siège

Étendue : Siège FEFORT
Plage d'adresses distribuées : 172.16.0.1 à 172.16.2.255
Masque : 255.255.0.0
Options
Passerelle par défaut : 172.16.220.1
Serveur DNS : 172.16.200.1

Annexe 4 : Structure de la table de filtrage

N° de règle	***Adresse source***	***Port source***	***Adresse destination***	***Port destination***	***Protocole transport***	***Action***

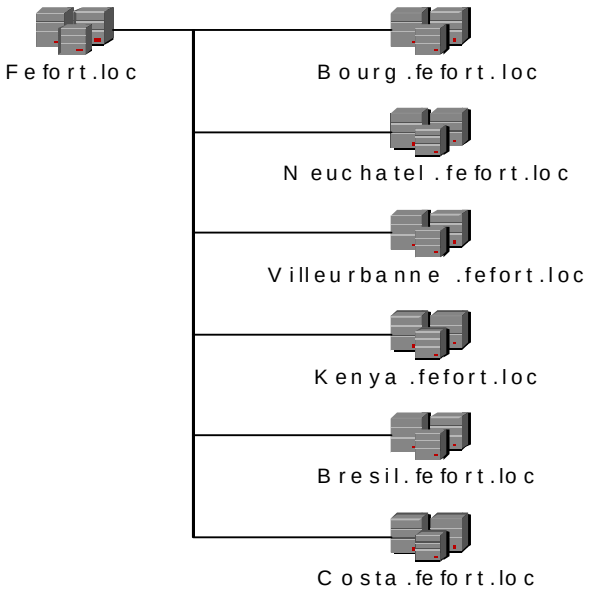
Chaque adresse sera indiquée au format *xxx.xxx.xxx.xxx/nn* où nn est le nombre de bits à « 1 » du masque.

Annexe 5 : Contenu du fichier de configuration de la zone fefort.loc

```
; définition de la zone fefort.loc
; le serveur d'autorité est dns.fefort.loc (serveur primaire)
; il est administré par une personne qu'on peut joindre à l'adresse admin@fefort.loc

fefort.loc.  IN      SOA    ns.fefort.loc.  admin.fefort.loc. (3; 36000; 3600; 360000; 86400)
             NS ns.fefort.loc. ; nom du serveur DNS primaire
; déclaration des adresses faisant autorité
; serveurs du siège
localhost.fefort.loc.  IN   A    127.0.0.1      ; serveur local
logon.fefort.loc.      IN   A    172.16.200.1   ; serveur d'authentification
ns.fefort.loc.  IN   A    172.16.200.2   ; serveur de nom
dhcp.fefort.loc.       IN   A    172.16.200.3   ; serveur dhcp
mail.fefort.loc.       IN   MX   172.16.200.4   ; serveur de messagerie
dev.fefort.loc. IN   A    172.16.200.5   ; serveur de développement
fichiers.fefort.loc.   IN   A    172.16.200.6   ; serveur de fichiers
backup.fefort.loc.     IN   A    172.16.200.7   ; serveur de sauvegardes
imp.fefort.loc. IN   A    172.16.200.8   ; serveur d'impressions
bdd.fefort.loc. IN   A    172.16.200.9   ; serveur de bases de données
appli.fefort.loc.      IN   A    172.16.200.10  ; serveurs d'applications
poste_admin.fefort.loc.     IN   A    172.16.200.200    ; station de l'administrateur
; serveurs de Villeurbanne
log-vi.fefort.loc.     IN   A    172.22.200.1   ; serveur d'authentification
dhcp-vi.fefort.loc.    IN   A    172.22.200.3   ; serveur dhcp
fic-vi.fefort.loc.     IN   A    172.22.200.6   ; serveur de fichiers
; serveurs des autres sites
;  …
; fin de la zone d'autorité
```

Annexe 6 : Arborescence DNS



Corrigé Exonet N° 28

Question 1. Donner l'écriture décimale pointée de ce masque et indiquer combien de sous réseaux pourront être créés à l'aide de celui-ci.

255.255.240.0
4 bits ==> 2^4 = 16 sous-réseaux possibles (*on tolère 16-2 – obsolète depuis 1995…*)

Question 2. Proposer une adresse IP pour chacun des services. *La proposition doit être compatible avec les adresses statiques existantes indiquées dans l'annexe 2.*

Tous les sous-réseaux commencent par 172.16 et se terminent par 0.
Ils s'écrivent donc sous la forme 172.16.x.0/20 où x représente un nombre multiple de 16 (puissance de 2 correspondant au dernier bit à 1 du masque de sous-réseau) :
0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 et 240.
Tous les ordinateurs du service informatique sont en 172.16.200.x : ils doivent donc appartenir au sous réseau 172.16.192.0 car celui-ci va jusqu'à l'adresse 172.16.207.255.
Le pare-feu possède une adresse 172.16.220.1 : il est donc dans le réseau 172.16.208.0
Pour les différents services, puisqu'ils n'ont que des adresses dynamiques fournies par le DHCP, on peut choisir n'importe quel autre sous-réseau non encore attribué.

sous-réseaux	**services**	
172.16.0.0		Au choix
172.16.16.0	Gestion/comptabilité	
172.16.32.0	Commercial	
172.16.48.0	Relation Client	
172.16.64.0	Marketing	
172.16.80.0	Direction	
172.16.96.0	Q, R & D	
172.16.112.0		
172.16.128.0		
172.16.144.0		
172.16.160.0		
172.16.176.0		
172.16.192.0	Service informatique	Obligatoire
172.16.208.0	*Accès pare-feu (pour information : non exigé)*	
172.16.224.0		
172.16.240.0		

La liste complète des sous réseaux possibles n'est pas demandée et les deux derniers réseaux sont aussi utilisables.

Question 3. Donner l'adresse de la passerelle par défaut des postes du service commercial, sachant qu'il s'agit de l'adresse disponible la plus élevée pour ce sous-réseau.

172.16.47.254
L'adresse fournie doit être cohérente avec l'adresse du sous réseau retenue pour le service commercial (ici 172.16.32.0).

Question 4. Expliquer la raison de ce dysfonctionnement et préciser les modifications à apporter, d'une part au serveur DHCP, d'autre part au nouveau routeur.

Raison

En l'état actuel des choses, le routeur ne laisse pas passer les paquets DHCP *Discover* qui sont des paquets de diffusion générale (adresse 255.255.255.255). Seuls les clients du service informatique sont susceptibles de recevoir leurs paramètres IP.

Mise à jour du routeur

Sur le routeur, il faut :

- attribuer au routeur une adresse dans chaque sous-réseau (fait à la question précédente donc pas exigée);
- activer le relais DHCP sur toutes les interfaces du routeur sauf celle du service informatique; *La citation de l'agent relais est exigée mais pas sa présence sur toutes les interfaces.*
- lui indiquer l'adresse du serveur DHCP : 172.16.200.3.

Mise à jour du serveur

Sur le serveur DHCP, il faut :

- supprimer l'étendue existante (*pas exigée*);
- créer une étendue par sous-réseau utilisé, donc par service

Par exemple, pour le service Comptabilité/Gestion :
Étendue : 172.16.16.1 à 172.16.16.100 (doit contenir au moins 50 adresses)
Masque : 255.255.240.0
Options :
Passerelle : 172.16.31.254 (adresse de routeur sur ce sous-réseau)
serveur DNS : 172.16.200.2
Il n'était pas demandé d'exemple. Une simple phrase précisant une création d'étendue par sous-réseau sera donc admise.

Question 5. En utilisant le formalisme donné en *annexe 4*, donner les règles applicables en entrée de l'interface concernée permettant de respecter les consignes données. Vous veillerez à limiter le nombre de règles à définir.

Interface concernée (pas demandé) :
172.16.220.1 (côté siège) en entrée pour la communication siège vers sites distants
172.17.0.1 (côté site) en entrée pour la communication retour
Ou bien une de ces interfaces en entrée et en sortie (on n'exige pas les deux).

N° de règle	***Adresse source***	***Port source***	***Adresse destination***	***Port destination***	***Protocole transport***	***Action***
1	Toutes	Tous	proxy	3128	TCP	Accepter
2	*Adresse proxy*	*3128*	*Toutes*	*Tous*	*TCP*	*Accepter*
3	172.0.0.0/8	Tous	172.16.192.0/20	Tous	Tous	Accepter
4	*172.16.192.0/20*	*Tous*	*172.0.0.0/11*	*Tous*	*Tous*	*Accepter*
Défaut	Toutes	Tous	Toutes	Tous	Tous	Refuser

1ère consigne : les règles 1 et 2 permettent les échanges entre le siège et le proxy du fournisseur d'accès.
2ème consigne : la règle 3 permet aux unités d'envoyer des paquets à tous les services disponibles du service informatique et la règle 4 permet les réponses.
3ème consigne : la règle 4 permet au service informatique de contacter les unités et la règle 3 permet les réponses.
La règle finale (non exigée) par défaut interdit tout trafic non spécifiquement autorisé donc les échanges directs entre les services du siège et les unités du groupe. Le pare-feu n'intervient pas dans les échanges entre les services du siège.

On acceptera :

- *toute adresse proxy cohérente.*
- *toute façon cohérente d'exprimer le mot "tous".*
- *tout masque de sur-réseau cohérent (/11, /12, et avec deux lignes /14 et /15)*
- *Une solution avec une ligne spécifique pour le poste de l'administrateur (/32).*

La ligne par défaut n'est pas exigée.

Question 6. Indiquer les modifications à apporter afin de distribuer des adresses valides aux stations de Villeurbanne, sur une étendue de même taille.

Il faut créer une étendue pour Villeurbanne, par exemple :
Plage d'adresses : 172.22.1.1 à 172.22.1.149
Masque : 255.255.0.0
Options Passerelle : 172.22.250.204 (adresse interne du routeur 4)
DNS : 172.16.200.2
La seule modification par rapport à l'étendue du serveur DHCP de Villeurbanne concerne la plage d'adresses distribuées.
Bien évidemment, il faudra activer le relais DHCP du routeur 4 et lui indiquer l'adresse du serveur DHCP du siège … mais cela n'est pas demandé.

Question 7. Apporter les modifications nécessaires au fichier de la zone *fefort.loc* (*annexe 5*) et écrire le fichier de la zone *villeurbanne.fefort.loc*.

Il faut ajouter le serveur DNS de Villeurbanne. Ce serveur aura **par exemple** les caractéristiques suivantes :

Machine	**@ IP**	**F.Q.D.N.**
serveur DNS	172.22.200.2	ns.villeurbanne.fefort.loc

Exemple avec BIND :
Dans la zone fefort.loc :

- il faut rajouter une ligne de délégation de zone pour chaque unité ainsi qu'une ligne de déclaration de l'adresse du serveur. Exemple pour villeurbanne

villeurbanne.fefort.loc. IN NS ns.villeurbanne.fefort.loc.
ns.villeurbanne.fefort.loc. IN A 172.22.200.2

On n'exige qu'une seule zone.

- il faut supprimer la déclaration des serveurs de Villeurbanne (sauf le serveur DNS déclaré ci-dessus bien sûr)

Le fichier zone de villeurbanne.fefort.loc. ressemblera à ceci :

```
villeurbanne.fefort.loc.        IN      SOA   ns.villeurbanne.fefort.loc.      admin.fefort.loc.
        (3; 36000; 3600; 360000; 86400)
        IN  NS      ns.villeurbanne.fefort.loc.
; serveurs de Villeurbanne
log-vi  IN      A       172.22.200.1  ; serveur d'authentification
dhcp-vi         IN      A       172.22.200.3  ; serveur dhcp
fic-vi  IN      A       172.22.200.6  ; serveur de fichiers
ns      IN      A       172.22.200.2  ; serveur de nom
```

Exemple sur un serveur MS-Windows :
Dans la zone fefort.loc :

- Sélectionner la zone fefort.loc
- Créer une nouvelle délégation
- Saisir le nom de la sous-zone (ici : “villeurbanne”)
- Ajouter le nom (ns.villeurbanne.fefort.loc) et l'adresse IP (172.22.200.2) du serveur DNS qui a obtenu la délégation.

Ajout de la zone de villeurbanne.fefort.loc :

2. Sélectionner les zones de recherche directes
3. Ajouter une nouvelle zone principale
4. Saisir le nom de la zone (ici : “villeurbanne.fefort.loc”).

Question 8. Expliquer les modifications à apporter au serveur DNS du siège d’une part et à celui du site de Villeurbanne d’autre part.

Exemple avec BIND :
Au siège :
Sur le serveur du siège, il faut ajouter l'information selon laquelle il sera serveur « esclave » pour la zone « villeurbanne.fefort.loc ».

```
zone "villeurbanne.fefort.loc" {
        type slave;
        masters {
        172.22.200.2;
        };
};
```

À Villeurbanne :
Sur le serveur DNS de Villeurbanne, il faut ajouter une ligne NS pour le serveur ns.fefort.loc, ce qui nous donne :

```
villeurbanne.fefort.loc.    IN    SOA    ns.villeurbanne.fefort.loc.    admin.fefort.loc.
        (3; 36000; 3600; 360000; 86400)
        IN    NS        ns.villeurbanne.fefort.loc.
        IN    NS        ns.fefort.loc
```

Exemple sur un serveur MS-Windows :
Au siège :
●Sélectionner “Zones de recherche directes”.
●Définir une nouvelle zone secondaire
●Saisir le nom de la zone (ici : “villeurbanne.fefort.loc”).
●Saisir l'adresse IP du serveur DNS principal (ici : 172.22.200.2)

À Villeurbanne :

- Sélectionner la zone “villeurbanne.fefort.loc”
- Ajouter un serveur de nom
- Saisir nom et adresse IP du nouveau serveur NS.

Question 9. Déterminer la configuration matérielle et préciser les protocoles que devra supporter le nouveau commutateur. ***Le rôle des fonctions et protocoles qu’il prendra en charge sera expliqué.***

Exemple de réponse :

Fonctions/protocoles	**Rôle, explication**
Configuration matérielle : 8 ports au moins + ports de liaison	Connectivité
Supporter la redondance de lien en évitant les tempêtes de diffusion *Protocole 802.1D, STP*	Arbre de recouvrement (Spanning tree), Tolérance de panne par agrégation de liens
Gérer les VLAN *Protocole 802.1q*	Marquage de trames pour identifier les VLAN
Gérer la priorité de flux *Protocole 802.1p*	Gestion de la priorité de trames
Protocoles SNMP, Telnet, HTTP	Accès en mode administrateur

Question 10. Proposer une solution matérielle complémentaire pour permettre aux postes de travail des différents services d'accéder aux serveurs du service informatique. Expliquer brièvement comment elle doit-être mise en œuvre.

Pour la solution basée sur un routeur, il faut soit une interface réelle par VLAN sans nécessité de taguer les trames soit une interface virtuelle par VLAN dans ce dernier cas le routeur doit taguer les trames.
Pour la solution basée sur des serveurs multidressés , il faut une interface virtuelle par VLAN et le serveur doit taguer les trames.
Pour la solution basée sur un commutateur-routeur il y a une interface réelle par VLAN, il n'est pas nécessaire de taguer.
Il existe aussi une réponse non détaillée ici avec des VLAN asymétriques?
Réponses possibles :
Prise en charge de la fonction de routage par l'ajout d'un routeur avec une interface taguée multi adressée afin d'interconnecter logiquement tous les VLAN.
Une solution avec un commutateur de niveau 3 peut assurer l'ensemble de ces fonctionnalités. Chaque port du commutateur s'interconnectant à un autre commutateur est associé à un VLAN et on affecte une adresse IP. Les liaisons ne gérant pas plusieurs VLAN il n'est pas nécessaire de taguer.
Si les serveurs gèrent les VLAN (protocole 802.1Q) on peut multiadresser les serveurs en définissant une interface virtuelle par VLAN, dans ce cas la liaison entre les commutateurs et les serveurs doit être taguée.

Question 11. Proposer une solution permettant de garantir la continuité du service d'accès aux serveurs du siège lors d'une panne du routeur. Expliquer les principes de fonctionnement de votre solution.

Exemples :
Mettre en place un routeur de secours et le protocole VRRP (Virtual Redondancy Router Protocol) (HSRP pour Cisco) pour activer/désactiver le routeur de secours.
Prévoir une redondance des routeurs avec répartition de charges
On accepte une solution qui n'assure pas la continuité de service mais la reprise rapide de service
Par exemple :
Prévoir un routeur de secours avec une reprise d'activité basée sur modification dynamique de l'adresse de passerelle sur les postes …
VRRP permet à deux routeurs R1 et R1' de partager une adresse IP virtuelle. De même pour leur adresse MAC. L'un des routeurs est actif comme s'il était seul. Mais s'il tombe en panne l'autre le détecte. (Arrêt des échanges mutuels de messages signalant leurs présences). R1' ne reçoit plus de messages, il devient alors actif et répond aux requêtes adressées aux adresses communes (IP et MAC).