

Examen terminal UE9 - Réseaux et protocoles (INF09)

Durée 2 heures. Tous les documents sont autorisés

Chaque candidat doit, au début de l'épreuve, porter son nom dans le coin de la copie qu'il cachera par collage **après avoir été pointé**. Il devra en outre porter son numéro de place sur chacune des copies, intercalaires ou pièces annexées.

1 Introduction

On se place dans le cadre d'une entreprise qui possède un réseau informatique suffisamment important pour avoir un service informatique. Ce dernier gère bien entendu l'ensemble du réseau et des machines pour le fonctionnement interne de l'entreprise, mais aussi les serveurs publics classiques tels que serveur web, dns, mail.

Cette entreprise a choisi d'utiliser uniquement le protocole IPv6 en interne, seules les machines susceptibles d'accéder directement à l'extérieur posséderont une adresse IPv4 publique (essentiellement les serveurs publics).

2 Accès à l'Internet et plages d'adresses disponibles

Pour son accès à l'Internet, l'entreprise a passé un contrat avec un fournisseur. Ce dernier doit lui fournir un préfixe IPv4 du type "/29" et un préfixe IPv6 du type "/61", avec dans les deux cas des adresses publiques.

Question 2.0.1 – *Donnez un exemple de préfixe IPv4 et un exemple de préfixe IPv6 respectant ces exigences.*

- *Pour le préfixe IPv4 choisi, faites la liste complète des adresses IPv4 que l'entreprise pourra affecter à ses machines nécessitant un accès IPv4.*
- *Pour le préfixe IPv6 choisi, et en supposant que les adresses des machines de l'entreprise respecteront le schéma classique : 64 bits pour la partie "réseau" et 64 bits pour la partie "machine" de l'adresse, indiquez combien de sous-réseaux l'entreprise pourra utiliser pour son parc de machines, et là encore, faites-en la liste complète.*

3 Architecture du réseau

3.1 Niveau physique

L'entreprise est subdivisée en plusieurs départements, et souhaite, au niveau réseau, affecter un sous-réseau IPv6 à chacun d'eux. Mais la répartition géographique des machines ne correspond pas à ce découpage en départements, et il arrive souvent que des machines utilisées par des employés appartenant à des départements différents soient voisines, et par conséquent reliées au réseau par le même équipement (switch). Voir par exemple la figure 1.

Question 3.1.1 *Quelle fonctionnalité couramment disponible sur les switches permet de résoudre ce problème en forçant les machines appartenant à des départements différents de passer par le niveau réseau (donc par*

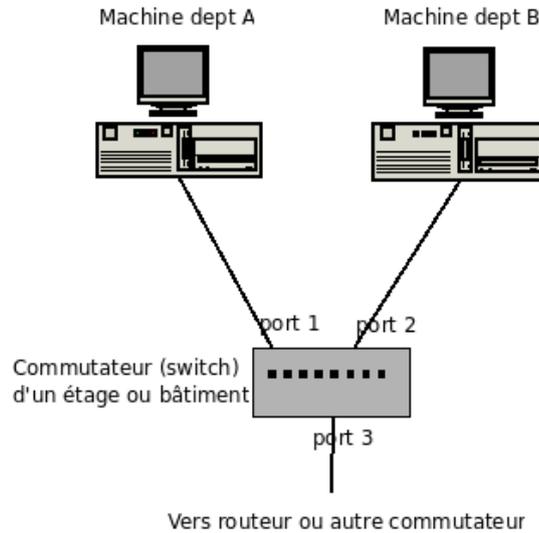


FIGURE 1 – Détail de configuration niveau physique

un routeur) pour communiquer entre-elles ? Dans le schéma de la figure 1, quel type d'ordre de configuration l'administrateur devra-t-il donner au switch ? (On ne demande pas de syntaxe précise, mais simplement l'idée)

3.2 Niveau réseau

On suppose que l'architecture logique du réseau de l'entreprise correspond à la figure 2. La zone marquée "P" est destinée à recevoir uniquement les serveurs publics de l'entreprise, qui auront à la fois une adresse IPv4 et une adresse IPv6.

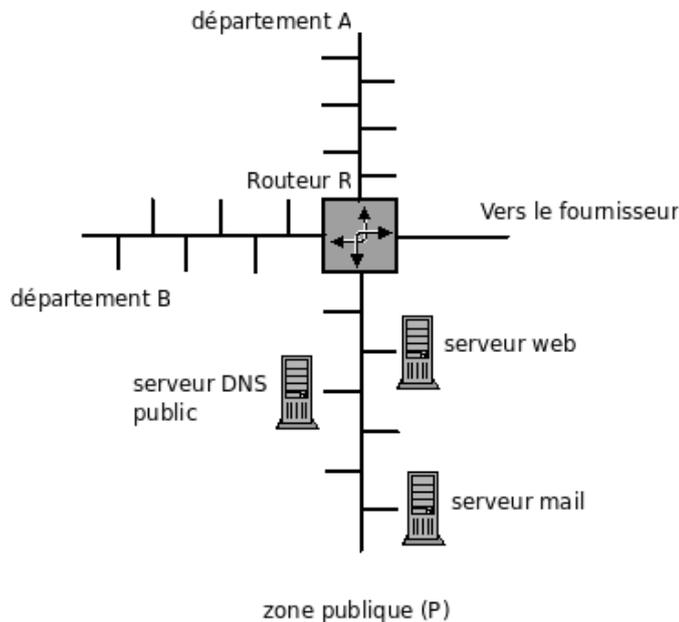


FIGURE 2 – Architecture logique réseau

Le routeur R est censé recevoir tout datagramme IPv4 ou IPv6 dont l'adresse destination correspond au préfixe IPv4 ou IPv6 attribué à l'entreprise par le fournisseur. Ce même routeur possède une route par défaut pour chacun de ces deux protocoles, lui permettant d'envoyer des datagrammes destinés à l'extérieur de l'entreprise.

Question 3.2.1 Complétez le schéma de la figure 2 avec les adresses de sous-réseau IPv6 pour chacun des départements, ainsi qu'avec les adresses IPv4 des serveurs publics. Donnez les tables de routage IPv4 et IPv6 du routeur correspondantes à cette répartition des adresses.

Question 3.2.2 Comment à votre avis les adresses (v4 ou v6) des serveurs publics, ainsi que les adresses v6 des machines des employés sont elles distribuées ? Manuellement ou automatiquement ? Justifiez vos choix. Dans le cas où on choisit la distribution automatique pour certaines machines, quelle configuration faut-il prévoir et sur quel(s) équipement(s) ? Même question pour le cas où on devrait distribuer des adresses v4 au lieu de v6.

3.3 Niveau transport

Tout en utilisant exclusivement des adresses publiques v6, on ne souhaite pas forcément que n'importe qui puisse accéder à toutes les machines ni tous les services de celles-ci.

Question 3.3.1 Quelle fonctionnalité doit-on mettre en place, et sur quel équipement, afin d'interdire ou d'autoriser certains accès ? Précisez par exemple quelles règles on doit prévoir pour :

- interdire tout accès depuis l'extérieur à toutes les machines d'un des départements de l'entreprise
- par exception à la règle précédente, autoriser l'accès à un serveur web sur une de ces machines. comment doit-on positionner cette règle par rapport à la précédente ?
- sur les machines serveurs publics (prenez un exemple, web ou mail ou autre) autoriser depuis l'extérieur seulement l'accès au service concerné, mais, depuis l'intérieur, autoriser aussi l'accès depuis la machine de l'administrateur système sur le port 22 (ssh) pour la maintenance.

NB : on ne demande pas ici la syntaxe précise des règles, mais simplement pour chacune les paramètres de filtrage et l'action à appliquer.

3.4 DNS

L'entreprise possède un nom de domaine et gère elle-même son serveur de noms.

Question 3.4.1 Quelles informations précises (noms, adresses) doit-on mettre dans le serveur DNS public de l'entreprise ? Pensez aux serveurs publics mais aussi à l'exemple de la question 3.3.1 concernant le serveur web situé sur une machine d'un des départements (se limiter à la conversion noms vers adresses).

Question 3.4.2 Pour ses besoins internes, l'entreprise a besoin de donner des noms à au moins une partie de ses machines, sans pour autant que ceux-ci soient connus de l'extérieur. Que doit-elle mettre en place pour cela ? Préciser comment doit être configuré sur les machines de l'entreprise l'accès à la résolution de noms.

3.5 Accès à l'Internet v4

Une partie au moins des machines des employés doivent avoir accès à des services de l'Internet, qui est majoritairement v4, tout en n'ayant qu'une adresse v6. En particulier :

- accès à des serveurs web v4
- envoi de mails à des correspondants uniquement en v4
- ponctuellement, quelques autres services pas forcément connus au préalable.

Question 3.5.1 – Comment peut-on résoudre simplement les deux premiers cas ? Précisez les éventuelles configurations nécessaires de certains logiciels clients sur les machines des employés concernées.

- Que peut-on mettre en place pour le troisième cas ?