université BORDEAUX
Master 1 *Sciences Technologies*

ANNÉE 2024-2025
Étape : Master Sciences Technologies (semestre 2)
Épreuve de : Administration des réseaux
Date : 22 Avril 2025
Heure : 9h00

SESSION DE AVRIL 2025
UE : 4TIN808U
Durée : 1h30
Documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Dans un réseau local, expliquer ce qui se passe lorsque deux machines ont la même adresse IP. Même question lorsqu'elles ont la même adresse physique (MAC).
2. Pourquoi le protocole DHCP est basé sur un mécanisme de broadcast ? Est il possible d'avoir plusieurs serveurs DHCP dans un même réseau local ? Comment cette situation est elle gérée par le protocole ?
3. Que se passe-t-il du point de vue du réseau lorsqu'un utilisateur saisit une URL dans son navigateur web dans le but d'en consulter le contenu ?
4. Quelles sont les principales différences entre IPv4 et IPv6. Qu'est ce qui freine le déploiement d'IPv6 ?
5. Quels sont les avantages de l'utilisation des VLANs pour la gestion d'un réseau local ? Justifiez votre réponse.

Exercices

6. Un système de translation d'adresses personnel (freebox,...) est utilisé pour donner accès à Internet à 15 postes de travail. Combien de connexions TCP simultanées sur le port 80 du serveur web www.google.com peuvent être supportées au plus ? Expliquez. Nous considérerons le cas où le serveur web n'a pas de mécanisme lui permettant de limiter le nombre de connexions simultanées.
7. L'utilitaire `ping` sert à envoyer un datagramme ICMP à une adresse IP et demande au destinataire d'envoyer un datagramme ICMP en réponse. Donnez une cause possible pour chacune des situations suivantes :
   (a) En retour de la commande `ping`, le message d'erreur *Destination host unreachable* est affiché.
   (b) En retour de la commande `ping`, aucun message n'est affiché et aucun paquet n'est reçu.
   (c) En retour de la commande `ping`, un message de type *ICMP time exceeded* est reçu.
   (d) En retour de la commande `ping`, un message de type *ICMP redirect* est reçu.
   (e) En retour de la commande `ping`, un message de type *Network unreachable*.
8. Considérons la topologie du réseau ci-dessous. Alice possède plusieurs PC chez elle (192.168.0.2-4) qui partagent une seule adresse IP publique (1.2.3.4) via un dispositif NAT. En outre, elle exploite un serveur de caméras de surveillance qui est directement connecté à Internet avec une adresse IP publique (5.6.7.8). La caméra transmet le signal vidéo en direct sous la forme d'un flux de paquets UDP avec le port source 1000 vers une adresse IP et un port de destination configurables.

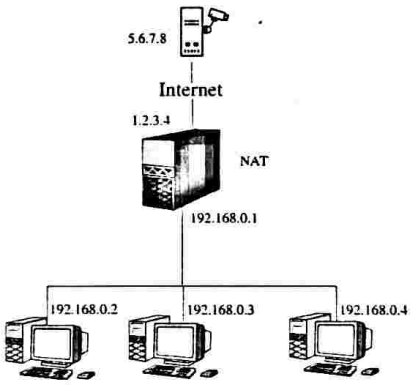

FIGURE 1 – Architecture du réseau.

   (a) Alice souhaite recevoir le flux vidéo en direct sur l'un de ses PC et configure donc la caméra pour qu'elle envoie le signal vidéo à vers l'adresse IP 192.168.0.3 et le port 1234. Cependant, elle ne le reçoit pas sur son PC. Pourquoi ? Où ce trafic est-il envoyé ?
   (b) Alice configure maintenant la caméra pour qu'elle envoie le signal vidéo à l'adresse IP 1.2.3.4 et au port 1234. Mais elle ne le reçoit toujours pas sur aucun de ses PC. Pourquoi ? Où ce trafic est-il envoyé ?
   (c) Que peut faire Alice pour recevoir le signal vidéo sur son PC à l'adresse IP 192.168.0.2 sur le port 1234 en supposant qu'elle ne puisse pas modifier la configuration de la passrelle NAT ? Décrivez étape par étape ce qu'elle peut faire si elle a les possibilités suivantes :

— envoyer un seul paquet UDP avec des adresses et des ports source et destination arbitraires à partir de chacune de ses PC.
— observer les paquets reçus sur chacun de ses PC ainsi que sur le serveur hébergeant la caméra.
— spécifier l'adresse IP et le port de destination pour le signal vidéo.

Problème

Soit le script de configuration d'`iptables` donné ci-dessous. Il correspond au réseau représenté par la figure 2 (le script étant exécuté sur la machine à trois interfaces réseau).

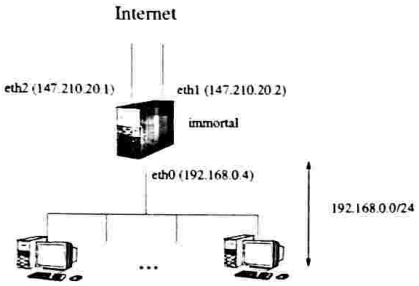

FIGURE 2 – Architecture du réseau.

```
#!/bin/sh
iptables -F
iptables -t nat -F

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP


[1] iptables -A OUTPUT  -o eth0 -j ACCEPT
[2] iptables -A OUTPUT  -o lo -j ACCEPT

[3] iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

[4] iptables -A INPUT -i eth2 -m state --state ESTABLISHED,RELATED -j ACCEPT

[5] iptables -A OUTPUT -o eth2 -j ACCEPT

[6] iptables -A FORWARD -i eth0 -s 192.168.0.0/24 -j ACCEPT


[7] iptables -A FORWARD -p tcp -i eth1 --dport 22 --sport 1024:65535  -m state --state NEW -j ACCEPT

[8] iptables -t nat -A PREROUTING -p tcp -i eth2 -d 147.210.20.2 --dport 22 --sport 1024:65535 -j DNAT --to 192.168.0.2:22
```

9. Détailler les modification que subit un paquet (correspondant à une ouverture de connexion) envoyé par l'hôte 212.27.48.10 à la machine d'adresse IP 147.210.20.2 (l'adresse de la passerelle NAT est 147.210.20.2) sur le port 22. Ce paquet est-il accepté ou détruit ? Expliquer. Proposer une solution dans le cas ou le paquet n'arriverait pas à destination.
10. Même question que précédemment lorsque 212.27.48.10 veut se connecter à la machine dont l'adresse IP est 147.210.20.1.
11. Nous souhaitons maintenant rendre accessible à partir d'internet le serveur `http` de la machine `www` dont l'adresse IP est 192.168.0.2. Que faut-il mettre en place ? Proposer un ensemble de règles qui répondraient à cette demande.
12. Est-il sûr de laisser le serveur `http` de la machine `www` dans le même réseau que nos machines internes ? Argumenter votre réponse. Proposer enfin une modification de l'architecture du réseau ainsi que le script ci-dessus pour pallier le problème.