École de technologie supérieure
Département de génie logiciel et des TI

Responsable du cours : Mohamed Faten Zhani
Chargé de cours : Aris Leivadeas
Chargé de laboratoire : Firmin Mah
Session : E2024

GTI100 - Programmation et Réseautique en génie des TI

Laboratoire 6 : Ethernet, ARP et NAT

Durée = 1 séance de 3 heures

Objectifs

Ce laboratoire vous permettra de comprendre le fonctionnement des protocoles Ethernet et ARP ainsi que le traducteur d'adresse réseau (NAT).

Montage & Outils

- Système d'exploitation : *Windows*
- Outils et logiciels : *Wireshark*, *arp, Cisco Packet Tracer*

Notes

- Ce travail doit se faire individuellement.
- Le rapport de laboratoire est à remplir directement dans Moodle. Cliquez sur le test « Rapport laboratoire 6 » pour remplir votre rapport.
- Le symbole ☛ indique la manipulation à faire pour répondre aux questions.
- Veuillez joindre, s'il y'a lieu, les captures d'écran qui montrent les réponses aux questions. **Le symbole 🖵 indique que vous devez joindre une capture d'écran pour avoir les points.**

Partie I : Capture et analyse du trafic réseau

Protocole ARP

Le fichier « Labo6-ARP-Google.pcapng » contient la capture de paquet enregistré par Wireshark durant un échange arp et un ping vers *google.ca*

☛ Ouvrez le fichier « Labo6-ARP-Google.pcapng » dans Wireshark et filtrez les paquets capturés pour ne montrer que les paquets arp.

1. Répondez aux questions suivantes *(12 points)*

   - Quelle est l'adresse IP de la machine dont on cherche l'adresse physique ?
   - À quelle machine correspond cette adresse ?

- Quelle est l'adresse MAC destination de la requête ARP ?
- Que signifie cette adresse MAC ?
- De quel(s) nœud(s) provient la réponse ARP ?
- Quelle est l'information la plus importante retournée dans la réponse ARP ?
- Donnez la valeur de cette information.
- Dans quel type de paquet la requête ARP est encapsulée ?
- Quelle est la taille, en octets, de l'entête Ethernet ?
- Quelle est la taille totale de la trame contenant la requête ARP ?
- A quoi servent les octets de bourrage (padding) dans une trame Ethernet ?
- Combien d'octets de bourrage (padding) ont été ajoutés à la réponse ARP ?

☛ Filtrez les paquets capturés pour ne montrer que les paquets ICMP.

☛ Pour les questions suivantes, considérez seulement la trame qui contient la première requête ICMP.

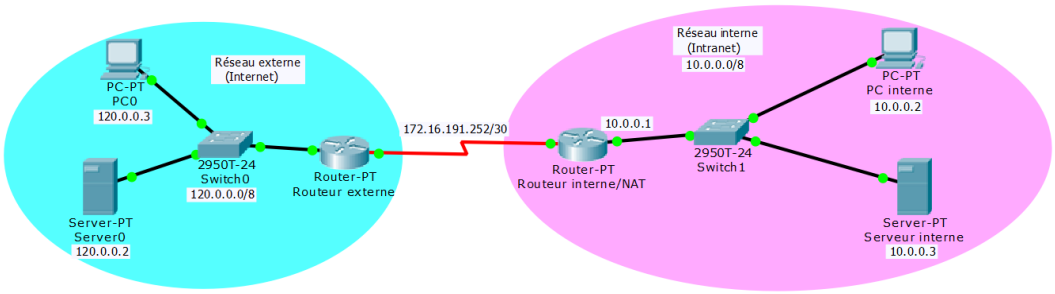
2. Répondez aux questions suivantes *(8 points)*
   - À quelle station correspond l'adresse IP destination de la première requête ICMP ?
   - À quelle station correspond l'adresse MAC destination de la première requête ICMP ?
   - Donnez la valeur hexadécimale du champ type de la trame Ethernet.
   - À quel protocole de couche supérieure cette valeur correspond ?

Partie II : Fonctionnement du NAT

3. Questions préliminaires : Répondez aux questions suivantes : *(5 points)*
   - Est-ce qu'actuellement votre poste communique avec google.ca avec sa propre adresse IP ?
   - Comment peut-on connaître l'adresse IP source et le numéro de port TCP source avec lesquels vos paquets arrivent à google.ca ?

Configuration du NAT :

Dans ce qui suit, nous allons configurer le NAT dans un routeur qui connecte un réseau privé d'une entreprise (appelé aussi Intranet) à un réseau externe (équivalent à internet). Le réseau privé utilise la plage d'adresses privées 10.0.0.0/8 à l'interne. À la sortie du réseau, le NAT doit convertir ces adresses privées en adresses publiques afin que les machines internes puissent communiquer avec internet. La plage d'adresses externes affectée à l'entreprise est 132.1.1.0/28.



4. D'après les plages d'adresses fournies ci-dessus, donnez les informations suivantes : *(4 points)*

   - Nombre d'adresses IP publiques disponibles pour l'entreprise
   - Nombre maximal d'hôtes qu'on peut avoir dans le réseau interne

Essayons maintenant de configurer le NAT au niveau du routeur interne.

- Ouvrez le fichier *Cisco Packet Tracer* « Labo6-NAT.pkt».
- Connectez-vous au routeur interne.
- Effacez un éventuel contenu de la table de correspondance du NAT à l'aide de la commande :

  clear ip nat translation *

- Identifiez quelle interface est connectée au réseau interne. Passez en mode interface de l'interface en question et exécuter la commande suivante :

  ip nat inside

- Identifiez quelle interface est connectée au réseau externe. Passez en mode interface de l'interface en question et exécuter la commande suivante :

  ip nat outside

- Passez au mode configuration et définissez la plage d'adresses externes à utiliser par le NAT. Commande à utiliser :

  ip nat pool <*nomPlage*> <*premièreAdresse*> <*dernièreAdresse*> **netmask** <*masqueReseau*>

  où *nomPlage* : nom que vous choisissez pour cette plage d'adresses externes,

  premièreAdresse et dernièreAdresse : la première et la dernière adresse dans cette plage,

  masqueReseau : le masque réseau à utiliser.

- Définissez une liste pour les adresses privées utilisées dans le réseau interne. Commande à utiliser :

  access-list <*numéroListe*> **permit** <*adresseRéseau*> <*masqueGen*>

  où *numéroListe* : numéro de la liste que vous choisissez (par exemple 1),

  adresseRéseau : adresse du réseau privé,

  masqueGen (wildcard) : l'inverse du masque sous-réseau (par exemple, pour un réseau ayant un masque 255.255.255.0, le masque générique est 0.0.0.255).

☛ Reliez la plage d'adresses internes à la plage d'adresses externes :

ip nat inside source list <*NuméroListe*> **pool** <*NomDeLaPlage*>

☛ Pour s'assurer que le NAT est fonctionnel, envoyez deux pings (PC interne vers Serveur0) et (serveur interne vers Serveur0). Si le NAT est bien configuré, les deux pings doivent être réussis.

☛ Exécutez les commandes suivantes en mode privilégié pour obtenir quelques statistiques et information sur le fonctionnement de votre NAT :

show ip nat translations

show ip nat statistics

5. Donnez la correspondance entre adresses internes/externes et identifiants ICMP internes/externes maintenue par le NAT. *(4 points)* Note : Prendre les résultats de 2 lignes quelconques si vous en avez plusieurs. Les résultats sont sous la forme @IP:identifiantICMP.

   Supposons maintenant que la plage d'adresses externes affectée à l'entreprise contient une seule adresse 132.1.1.1/28 et que le nom de la plage est *PlageNo1*

6. Parmi les commandes ci-dessous laquelle permet de préciser que seulement cette adresse est disponible comme adresse publique ? *(2 points)*

   ip nat pool PlageNo1 132.1.1.1 132.1.1.1 netmask 255.255.255.0

   ip nat pool PlageNo1 132.1.1.1 132.1.1.1 netmask 255.255.255.240

   ip nat pool PlageNo1 132.1.1.1 132.1.1.2 netmask 255.255.255.240

   ip nat pool PlageNo1 132.1.1.1 132.1.1.1 netmask 0.0.0.240

   ip nat pool PlageNo1 132.1.1.1 132.1.1.1 netmask 255.255.0.0

   ip nat pool Plage1 132.1.1.1 132.1.1.1 netmask 255.255.255.240

☛ Configurez le NAT pour que la plage d'adresses externes affectée à l'entreprise contient une seule adresse 132.1.1.1/28.

☛ Envoyez deux pings <u>en même temps</u> (du PC interne vers Serveur0) et (du serveur interne vers Serveur0). Pour bloquer le temps afin de préparer les pings à envoyer, il faut passer en mode simulation. Quand vous retournez au mode Real Time, le temps va avancer normalement et les deux pings vont être envoyés.

7. Est-ce que les 2 pings atteignent le Serveur0 ? Dites pourquoi. *(3 points)*

☛ Effacez le contenu de la table de correspondance du NAT à l'aide de la commande suivante :

clear ip nat translation *

- Afin de permettre à toutes les machines du réseau privé de communiquer avec l'extérieur, on doit configurer le NAT à utiliser la même adresse publique pour toutes les machines internes (appelé surcharge – o*verloading*). Pour ce faire, ajoutez le paramètre « overload » à la commande qui relie la plage d'adresses internes à la plage d'adresses externes :

ip nat inside source list <*NuméroList*> **pool** <*NomDeLaPlage*> **overload**

- Envoyez deux pings en même temps (du PC interne vers Serveur0) et (du serveur interne vers Serveur0). Pour bloquer le temps afin de préparer les pings à envoyer, il faut passer en mode simulation. Quand vous retournez au mode Real Time, le temps va avancer normalement et les deux pings vont être envoyés.

8. Donnez la correspondance entre adresses internes/externes et identifiants ICMP internes/externes maintenue par le NAT. *(4 points)* Note : Prendre les résultats de 2 lignes quelconques si vous en avez plusieurs. Les résultats sont sous la forme @IP:identifiant ICMP.

- Effacez le contenu de la table de correspondance du NAT à l'aide de la commande suivante :

clear ip nat translation *

Nous allons maintenant envoyer du trafic TCP à partir du réseau interne vers le réseau externe afin de voir comment le NAT procède avec le trafic TCP.

- Passez en mode Simulation afin de bloquer le temps et de bien configurer les générateurs de trafic. Pour générer du trafic à partir d'une machine, double clic sur la machine > Desktop> Traffic Generator. Dans notre cas, on génère du trafic http à partir du PC interne et du serveur interne vers Serveur0. Remplissez les champs nécessaires mais assurez-vous que le port source dans les deux cas est égal à 2000. Cliquez sur « Send ».
- Passez en mode Realtime pour débloquer le temps.

9. Donnez la correspondance entre adresses internes/externes et port source TCP interne/externe maintenue par le NAT. *(4 points)* Note : Prendre les résultats des lignes avec les ports 2000 et 1024 Les résultats sont sous la forme @IP:numéroDePort.

10. Combien de connexions TCP le NAT peut supporter simultanément ? Expliquez comment vous avez calculé cette valeur. *(4 points)*