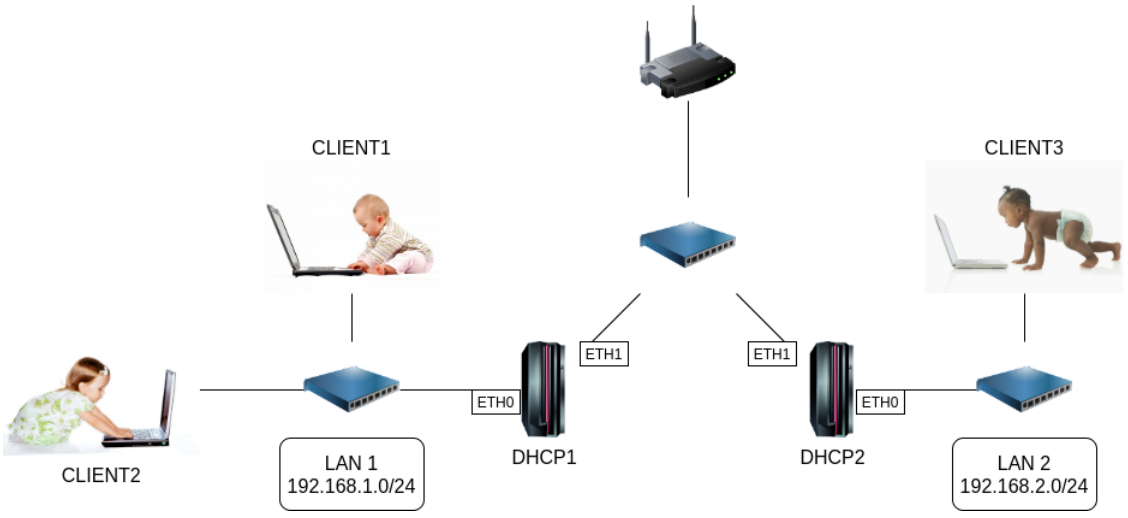
1 Objectifs

L'objectif de ce TP est de vous initier à la configuration d'un serveur **DHCP** afin d'automatiser la configuration IP d'un sous-réseau. Pour ce faire, vous allez utiliser un environnement virtuel émulant un réseau de machines sous *Debian*[1], c'est à dire la distribution que vous utilisez actuellement. L'environnement virtuel que nous allons utiliser est *NEmu*[2].

2 Le réseau

Nous allons travailler sur le réseau suivant :



Nous pouvons constater que ce réseau est composé de deux sous-réseaux : *LAN 1* et *LAN 2*. *LAN 1* est composé des machines *dhcp1*, *client1* et *client2*. *LAN 2* est composé des machines *dhcp2* et *client3*. Les deux machines *dhcp1* et *dhcp2* sont raccordées (sur leur interface *eth1*) à un réseau d'entreprise géré par un routeur externe. Les machines virtuelles vous sont livrées *nues*. C'est à dire qu'elles disposent uniquement des réglages élémentaires du système.

3 Avant de commencer...

- Dans un terminal régulier :
  - Pour lancer le réseau virtuel :
    `$ ~/iut-vms/vnet/nemu-vnet netdhcp`
  - Pour restaurer le réseau virtuel précédemment sauvegardé :
    `$ ~/iut-vms/vnet/nemu-restore ~/vnet/netdhcp.tgz`
- Dans le terminal de *NEmu* :
  - Pour quitter le réseau virtuel, tapez **quit()** dans le terminal principal
  - Pour sauvegarder le réseau virtuel, tapez **save()** et validez dans le terminal principal. Le réseau sera sauvegardé dans ∼ */vnet/netdhcp.tgz*
  - Pour redémarrer (violemment) l'ensemble du réseau virtuel, tapez **reboot()** et validez dans le terminal principal
  - Pour redémarrer une seule machine virtuelle : **RebootVNode('<nom de la VM>')**

1) Lancer le réseau virtuel comme indiqué ci-dessus. 5 fenêtres correspondant aux consoles de chacune des machines devraient apparaître.

1. http://www.debian.org
2. https://gitlab.com/v-a/nemu

Vincent Autefage
vincent.autefage@u-bordeaux.fr

4 Mise en jambe

4.1 Configuration IP des serveurs

Jusqu'à indication du contraire, nous ne considérerons que les interfaces **eth0** des machines serveurs pour le moment.

2) Choisir une adresse pour chacun des serveurs *dhcp1* et *dhcp2* sur leur sous-réseau respectif.

3) Afin de pouvoir redémarrer librement ces deux serveurs en conservant leur configuration IP, nous allons compléter le fichier `/etc/network/interfaces` de chacune des ces deux machines. Effectuer la configuration correspondante.

Rappel : Les lignes concernant l'interface de *loopback* ne doivent **en aucun cas** être modifiées.

4) Analyser l'effet des commandes **ifup eth0** et **ifdown eth0** sur les deux serveurs. Pour cela, regarder l'effet produit à l'aide des commandes **ifconfig** et **route**.

5) Éditer le fichier `/etc/default/isc-dhcp-server` sur les deux serveurs afin de n'activer le futur service DHCP que sur la première interface réseau (*i.e.* **eth0**), la seconde interface (**eth1**) étant gérée de façon externe :

```
INTERFACESv4="eth0"
```

4.2 Configuration IP des clients

6) Configurer les interfaces réseaux des machines *client1* et *client2* de manière perenne afin qu'elles obtiennent leur configuration IP en interrogeant un serveur DHCP.

Attention : Ne pas inclure de directive **auto** dans le fichier `/etc/network/interfaces` afin de pouvoir manuellement contrôler le cycle de vie des interfaces réseaux.

Exemple :

```
iface eth0 inet dhcp
```

7) Démarrer l'interface réseau de *client1* grâce à la commande **ifup eth0**. Vous devez normalement observer une erreur après une longue attente (environ 1 minute). En effet aucun serveur DHCP n'est encore configuré ; le sous-réseau n'est donc pas en mesure de fournir une adresse IP au client.

5 Configuration DHCP sur le premier réseau

5.1 Configuration silencieuse

Nous allons dans un premier temps configurer le serveur **dhcp1** afin qu'il n'ait aucune adresse IP à distribuer.

8) Pour cela, ajouter un bloc **subnet** vide dans le fichier `/etc/dhcp/dhcpd.conf` (ajouter le bloc en fin de fichier sans toucher aux autres lignes).

9) Redémarrer le service DHCP grâce à la commande suivante :

```
# systemctl restart isc-dhcp-server
```

Attention : Il faudra penser à redémarrer ce service après chaque modification du fichier de configuration du serveur DHCP.

Vincent Autefage
vincent.autefage@u-bordeaux.fr

10) Afin de vérifier que le service est bien démarré, vérifier son état à l'aide de la commande suivante :

```
# systemctl status isc-dhcp-server
```

Info : Les *logs* du service DHCP sont stockés dans le fichier `/var/log/syslog`. Il faudra vérifier le contenu de ce fichier à chaque redémarrage du service DHCP afin de s'assurer qu'aucune erreur silencieuse ne s'est produite. Ce fichier contenant les *logs* d'un grand nombre de services, il peut devenir extrêmement volumineux et donc difficile à analyser. Vous pouvez n'afficher que les N dernières lignes d'un fichier grâce à la commande suivante :

```
# tail -n <N> <file>
```

Exemple :

```
# tail -n 20 /var/log/syslog    # affiche les 20 dernières lignes du fichier /var/log/syslog
```

Le journal complet est également disponible via la commande suivante :

```
# journalctl --unit isc-dhcp-server
```

11) Passer en mode graphique grâce à la commande **startx** et démarrer **wireshark** sur l'interface **eth0**.

Rappel :

```
# wireshark -i eth0 -k
```

12) Nous allons démarrer l'interface réseau de *client1* en mode *debug* afin d'afficher toutes les étapes de la configuration grâce à la commande suivante :

```
# dhclient -d eth0
```

Info : Un *CTRL+C* permet d'arrêter le client DHCP.

13) Démarrer l'interface réseau de *client1* comme indiqué ci-dessus et observez les paquets des requêtes émises par ce dernier. Le serveur DHCP répond-il ? Pourquoi ?

5.2 Configuration dynamique

Nous allons maintenant configurer le serveur **dhcp1** afin qu'il puisse distribuer des adresses IP de façon dynamique.

14) Compléter le bloc **subnet** afin de permettre la distribution d'un bloc de 10 adresses IP.

Attention : L'adresse IP du serveur DHCP **ne doit jamais** être contenue dans le pool d'adresses distribuables. Vous risqueriez sinon d'avoir un client ayant la même adresse IP que le serveur, ce qui rendrait l'adressage et le routage incohérents.

15) Redémarrer **wireshark** sur le serveur *dhcp1* et démarrer l'interface réseau du *client1* à l'aide la commande **ifup eth0** afin de visualiser les trames réseaux émises et reçues.

Astuce : **wireshark** permet de filtrer les paquets par famille. DHCP reposant sur le protocole **udp**, vous pouvez indiquer ce protocole dans la barre de filtre afin de ne pas être pollué par des paquets d'autres protocoles.

16) Vérifier la configuration réseau du *client1* grâce aux commandes **ifconfig** et **route**.

17) Vérifier que *dhcp1* et *client1* arrivent à communiquer entre eux grâce à la commande **ping**.

18) Les baux DHCP sont stockés dans le fichier `/var/lib/dhcp/dhcpd.leases` pour le serveur et dans le fichier `/var/lib/dhcp/dhclient.leases` (avec **dhclient** <**iface**>) ou `/var/lib/dhcp/dhclient.<iface>.leases` (avec **ifup** <**iface**>) pour le client. Observer le contenu des ces fichiers.

Info : Le client peut indiquer la libération du bail DHCP grâce aux commandes suivantes :

```
# dhclient -r eth0    # si l'adresse a été obtenue avec la commande : dhclient -d eth0
# ifdown eth0         # si l'adresse a été obtenue avec la commande : ifup eth0
```

19) Libérer le bail DHCP du *client1*.

5.3 Configuration statique

Nous allons maintenant configurer le serveur **dhcp1** afin qu'il puisse distribuer des adresses IP de façon statique.

20) Relever l'adresse MAC de *client2* grâce à la commande **ifconfig**.

21) Compléter le bloc **subnet** avec un sous-bloc **host** afin de permettre l'affectation d'une adresse IP particulière à cette machine.

Attention : Les adresses IP distribuées de façon statique **ne doivent jamais** être contenues dans le pool d'adresses dynamiques. Vous risqueriez sinon d'avoir deux clients partageant la même adresse IP, ce qui rendrait l'adressage et le routage incohérents.

22) Démarrer les interfaces réseaux de *client1* et *client2* à l'aide la commande **ifup**.

23) Vérifier la configuration réseau de *client1* et *client2* grâce aux commandes **ifconfig** et **route** et vérifier le contenu des fichiers de baux sur le serveur et sur les clients.

24) Vérifier que *dhcp1*, *client1* et *client2* arrivent à communiquer entre eux grâce à la commande **ping**.

25) Libérer les baux DHCP sur les deux clients.

5.4 Extension de bail

26) Dans le fichier de configuration du serveur DHCP, fixer une durée de bail DHCP de 30 secondes, puis relancer le service.

27) Relancer les clients DHCP en mode *debug* depuis *client1* et *client2* en observant les paquets reçus et émis.

28) À quelle rythme le bail est-il renouvelé ?

29) Les clients récupèrent-ils les mêmes adresses ?

5.5 Réallocation forcée

30) Tout en laissant tourner les clients DHCP en mode *debug*, couper le service DHCP sur le serveur *dhcp1* à l'aide de la commande suivante :

```
# systemctl stop isc-dhcp-server
```

31) Décrire le comportement des deux clients DHCP ? Votre analyse doit se faire au minimum sur une à deux minutes.

Vincent Autefage
vincent.autefage@u-bordeaux.fr

32) Sans couper les clients DHCP, relancer le serveur puis décrire le comportement des clients amenant à la récupération de la configuration réseau.

33) Libérer les baux DHCP sur les deux clients.

6 Configuration DHCP sur le second réseau

34) Configurer le serveur *dhcp2* afin de permettre à *client3* de récupérer une configuration IP valide depuis le serveur DHCP *dhcp2*.

7 Raccord des deux sous-réseaux

Afin de permettre aux différents clients de pouvoir communiquer entre eux, nous allons modifier la configuration des deux serveurs DHCP afin qu'ils puissent indiquer à leurs clients la passerelle par défaut à utiliser.

35) Les deux serveurs sont pourvus d'une interface **eth1** raccordée à un réseau d'opérateur fournissant un serveur DHCP. Sur les deux serveurs, modifier le fichier `/etc/network/interfaces` afin de configurer leur interface **eth1** respective comme client DHCP.

Attention : Penser à activer l'IP forwarding sur les deux serveurs afin qu'ils soient en mesure de retransmettre les paquets des clients.

36) Démarrer l'interface **eth1** de chaque serveur grâce à la commande **ifup**.

37) Relever les adresses IPs des deux serveurs ainsi que leurs routes grâce aux commandes **ifconfig** et **route**.

38) Vérifier que les deux serveurs arrivent à communiquer entre eux grâce à la commande **ping**.

39) Modifier le bloc subnet du serveur *dhcp1* afin d'indiquer à ses clients que la passerelle par défaut est l'adresse IP de l'interface **eth0** de *dhcp1*.

40) Modifier le bloc subnet du serveur *dhcp2* afin d'indiquer à ses clients que la passerelle par défaut est l'adresse IP de l'interface **eth0** de *dhcp2*.

41) Relancer les services DHCP sur les deux serveurs.

42) Démarrer les interfaces réseaux de l'ensemble des clients grâce à la commande **ifup**.

43) Vérifier sur l'ensemble des clients que la configuration est correcte grâce aux commandes **ifconfig** et **route**.

44) Vérifier que les clients arrivent tous à communiquer entre eux grâce à la commande **ping**.

8 Mise en place d'une attaque de type *Man In The Middle* via *DHCP Spoofing*

8.1 Principe

Comme nous l'avons vu précédemment, le protocole DHCP, outre l'attribution d'adresse IP, permet d'indiquer aux clients un certain nombre d'informations de configuration supplémentaires comme un serveur de nom, un serveur d'impression ou encore une passerelle par défaut. Les clients DHCP acceptent généralement la première proposition de configuration reçue sans vérifier l'identité du serveur l'ayant émise. Couplé au fait que l'ensemble

des messages sont envoyés en clair, il assez aisé pour un attaquant de créer un serveur DHCP éphémère afin de forcer les clients à utiliser une passerelle par défaut illégitime sur laquelle le trafic peut être capturé. L'attaque se base ici sur une altération de la table de routage et non sur une altération de la table de correspondance ARP comme c'est le cas pour une attaque de type *ARP Spoofing*.

Nous allons tenter de simuler une attaque de type *DHCP Spoofing* depuis *client2* afin de forcer *client1* à croire que la passerelle par défaut est *client2*.

8.2 A l'abordage !

45) Il est tout d'abord nécessaire de relâcher la configuration réseau du *client1* (victime) afin de d'effectuer un cycle de configuration DHCP complet.

```
# dhclient -r eth0
```

46) Passer en interface graphique sur *client2* (attaquant) et lancez l'attaque *DHCP Spoofing* dans un terminal dédié :

```
# ettercap -Tzq -M dhcp:/255.255.255.0/<IP DHCP1>
```

47) Activer le client DHCP du *client1*.

48) Vérifier que votre attaque a fonctionner en consultant la table de routage du *client1*.

49) Renseignez-vous sur la fonctionnalité *DHCP Snooping* et expliquez comment cette technique peut apporter une certaine protection contre cette attaque.

9 Fin

50) Éteindre chaque machine correctement à l'aide de la commande **halt**. Vous pouvez ensuite sauvegarder votre session à l'aide de la commande **save()** et quitter l'environnement avec la commande **quit()** dans le terminal principal.

Vincent Autefage
vincent.autefage@u-bordeaux.fr