UE INF-2211
« Administration système/réseau »

Sujet de TP n°1 : configuration de stations Linux pour un fonctionnement en réseau

Informations préliminaires

L'objectif de cette séance de TP est de prendre en main les services réseau sur les machines que vous administrez, en acquérant une vision d'ensemble des répertoires et fichiers qui permettent le contrôle de ces services.

Lors de l'installation du système Linux sur votre machine, vous avez fait en sorte que cette machine reçoive des paramètres de configuration par défaut, en la configurant en tant que client DHCP. La configuration initiale de votre machine s'est donc faite avec l'aide des machines *phobos* et *deimos*, qui assurent notamment au sein de la salle *Cyber Lab* les fonctions de :

— serveur DHCP *(deimos)*, fournissant certains paramètres (adresses IP, adresses de serveurs DNS, etc.) aux machines qui en font la demande.
— routeur garde-barrière *(phobos)* pour le trafic entrant et sortant de la salle, et pour le trafic échangé entre les réseaux *saturne* et *uranus*.
— serveur HTTP *(deimos)*, hébergeant l'ensemble des paquets de la distribution Debian.

1 Analyse de la configuration initiale de votre machine

— En utilisant la commande *dmesg* et en examinant le fichier */var/log/s*yslog, identifiez l'interface (ou les interfaces) réseau détectée(s) lors du démarrage du système, ainsi que les modules logiciels utilisés pour exploiter chaque interface. Notez en particulier toute information pouvant être utile concernant l'interface Ethernet de votre machine (adresse DMA, numéro d'interruption, identité du pilote, identifiant de l'interface elle-même, etc.).
— En utilisant la commande *ip*, observez la configuration des interfaces réseau locale (i.e., interface de bouclage ou *loopback*) et Ethernet de votre machine. Prenez le temps de bien comprendre chacun des éléments d'information retournés par cette commande. Notez que chaque interface dispose à la fois d'adresses IPv4 et IPv6.
— Vérifiez qu'un processus *dhclient* tourne en tâche de fond sur votre machine. Consultez la page de manuel associé à ce programme, ainsi que le fichier de baux */var/lib/dhcp/dhclient.XXX.leases* (où XXX désigne l'interface réseau) dans lequel sont stockées les informations qu'il a collectées. La structure de ce fichier est décrite dans la page de manuel *dhclient.conf*.
— En utilisant la commande *ip*, observez l'état de la table de routage de votre machine à l'issue du démarrage du système (du point de vue du routage IPv4 et du routage IPv6). Cette fois encore, prenez le temps de bien comprendre les informations retournées par cette commande, et de jouer un peu avec les diverses options offertes.
— Installez le paquet Debian *net-tools*, qui apporte des commandes telles que *ifconfig*, *route*, *arp*, *netstat*, etc. Ces commandes sont aujourd'hui remplacées pour la plupart par la commande *ip*, mais utilisez-les pour répéter les opérations réalisées plus haut afin d'observer les possibilités de chaque commande.
Ceci fait, désinstallez le paquet *net-tools*, ce qui aura pour effet de faire disparaître les commandes *ifconfig*, *route*, etc. Vous pourrez ainsi vous concentrer sur l'apprentissage des nombreuses possibilités de la commande *ip*.

2 Reconfiguration du service de nommage

— Essayez de « pinguer » depuis votre machine une autre machine située hors de la salle *Cyber Lab* (avec IPv4, puis avec IPv6). Que constatez vous ?
— Identifiez le chemin suivi par les paquets IP au cours de cette manipulation. Pour ce faire vous pourriez avoir besoin d'installer le paquet *traceroute*. Notez par ailleurs que la commande *traceroute* réalise par défaut de l'émission de datagrammes UDP, qui sont souvent filtrés par certains pare-feux. En jouant sur les options de la commande on peut également obtenir que *traceroute* utilise des paquets ICMP ou des segments TCP SYN, les paquets ICMP n'étant en général pas filtré par les pare-feux.
— Essayez à présent de « pinguer » une autre machine de la salle (toujours avec IPv4 et IPv6). Que constatez vous ? Pouvez vous désigner la machine visée par son nom ? Pouvez vous la désigner par son adresse IP4 ? Par une adresse IPv6 ? Par son nom ? Qu'en déduisez vous ?
— En éditant les fichiers */etc/nsswitch.conf* et */etc/hosts,* faites en sorte que l'on puisse désigner toutes les machines de la salle par leur nom.
— Identifiez les adresses des serveurs DNS auxquels votre machine fait appel. Ces adresses ont été fixées par le serveur DHCP qui a permis à votre machine de démarrer sur le réseau.

3 Configuration IP statique

On se contentera pour cette partie de gérer manuellement la configuration IPv4 des machines de la salle.

Dans la phase de démarrage d'une machine tournant sous Debian (avec support *SysInit*), le script */etc/init.d/networking* est invoqué avec l'option *start*. Au cours d'une phase de *shutdown* ou de *reboot*, ce même script est invoqué avec l'option *stop*.

Consultez attentivement le script *networking*. Identifiez les fichiers de configuration et autres scripts ou commandes sur lesquels il s'appuie pour réaliser la configuration des interfaces réseau. Examinez attentivement ces différents fichiers, et consultez les pages de manuel pour identifier le rôle de chaque commande invoquée.

Vous devriez à présent avoir repéré le fichier permettant de configurer l'interface Ethernet de votre machine. Pour l'instant ce fichier spécifie que l'interface doit être configurée par DHCP lors du lancement du système. Il vous faut donc le modifier afin d'obtenir une configuration statique de l'interface (i.e., ne faisant plus appel au serveur DHCP). L'objectif est qu'après cette opération l'interface soit configurée statiquement, en adoptant les mêmes adresses et masques de réseau que ce qui était jusqu'à présent obtenu par DHCP.

Après cette modification, stoppez le service client DHCP, qui tourne en tâche de fond sur votre machine. Relancez ensuite les services réseau de votre machine, et assurez vous que tout fonctionne bien, avec cette fois une configuration statique.

Remarque 1 : Notez qu'il n'est absolument pas nécessaire, pour relancer exclusivement les services réseau, de redémarrer entièrement la machine. Prenez donc l'habitude de ne pas faire rebooter sans cesse votre machine. Un redémarrage complet ne se justifie *réellement* qu'en cas de changement du noyau du système d'exploitation, c'est-à-dire presque jamais. Dans pratiquement tous les autres cas, il n'y a pas matière à redémarrer sans cesse votre machine : il suffit de faire redémarrer le ou les services appropriés (avec les options appropriées).

Remarque 2 : Lors de la prochaine séance de TP le serveur DHCP de *deimos* sera désactivé. Il est donc *impératif* qu'au terme de cette séance votre machine soit en mesure de démarrer avec une configuration réseau statique.

4 Installation d'outils de *monitoring* réseau

Installez sur votre machine les paquets *tshark* et *wireshark*, en autorisant la capture de trafic par des utilisateurs autres que *root*. Ces paquets contiennent des programmes permettant la capture et l'analyse de trafic réseau. Vous devez vous familiariser avec leur utilisation, car vous serez amenés à les utiliser fréquemment au cours des séances de TP à venir.

Familiarisez vous tout d'abord avec l'utilisation de la commande *tshark*, et avec ses nombreuses possibilités de paramétrage. Cherchez par exemple à faire de la capture sélective de trafic, tel que le trafic à destination ou en provenance d'une adresse Ethernet donnée, d'une adresse IP donnée, d'une plage d'adresses IP donnée, ou encore le trafic spécifique à un protocole donné (e.g., ICMP, ARP, IP, UDP, TCP, DNS, SSH...). Apprenez également à enregistrer des traces de trafic dans un fichier, et à les rejouer par la suite.

Lancez ensuite l'application *wireshark* (qui est la version graphique de *tshark*), et prenez le temps de vous familiariser avec elle comme vous l'avez fait avec *tshark*.

Attention : notez que ces outils de monitoring sont très puissants, mais que leur maîtrise n'est pas aisée. Pour vous en convaincre, regardez les pages de manuel intitulées *tshark*, *wireshark*, *wireshark-filter*, etc. Il n'est pas nécessaire que vous appreniez à maîtriser toutes les possibilités de ces outils, mais vous devez au moins être capables d'effectuer avec eux de la capture sélective de trafic, et de l'analyse du trafic capturé.