	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Partie 1 : Serveur DNS

Base de toutes les reconnaissances de machines, le service DNS se met en place au début afin d'identifier l'ensemble des composants de votre réseau et faciliter l'accès vers l'extérieur. Il constitue la carte d'identité première de l'entreprise par l'intermédiaire d'Internet. DNS sera identifié et utilisé par les clients, indifféremment sous Windows ou sous Linux.

1. Compréhension du système DNS

On ne présente plus le système DNS, hiérarchie de base de données distribuées, destiné à décrire les ordinateurs d'un réseau par la mise en relation d'une adresse IP avec un nom plus facilement reconnaissable pour un humain. On parlera de traduction d'adresses IP. Paradoxalement, chaque client est appelé un "résolveur" alors qu'il ne résout rien mais demande une résolution.

a. Pourquoi DNS est-il nécessaire ?

L'emploi du simple fichier /etc/hosts ne suffit pas pour de grands réseaux et a fortiori pour le réseau des réseaux : Internet. La taille de l'ensemble impose une base répartie de serveurs organisée en structure pyramidale (arbre inversé, la racine se trouvant en haut) pour mémoriser l'ensemble des données.

On nomme serveurs racines (ou "root") les serveurs dits de premier niveau au nombre de 13, s'occupant des domaines importants comme .com, .net, etc. Chaque serveur (ou nœud) à son niveau s'occupant d'une partie de l'arbre de connaissances pour sa zone.

L'utilisation du service DNS constitue la pierre angulaire de l'administration d'un réseau, il permet l'échange d'informations de beaucoup d'autres services.

b. Le vocabulaire DNS

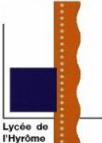
Le domaine inverse : résolution d'une adresse IP en nom de domaine avec l'ajout d'un domaine spécial in-addr.arpa à la fin. Par exemple :

Un réseau 10.1.0.0 et de masque 255.255.0.0 aura pour adresse inverse :
1.10.in-addr.arpa.

Le masque de classe B est volontairement associé à une adresse de classe A afin de montrer de façon claire que c'est le masque de sous-réseau qui détermine l'adresse inverse ; voici l'exemple avec une classique adresse de classe C :

Un réseau 192.168.1.0 et de masque 255.255.255.0 aura pour adresse inverse :
1.168.192.in-addr.arpa

La délégation : transfert de responsabilité dans l'administration d'une zone DNS avec autorité pour les serveurs de la zone de la résolution de noms.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Serveur primaire et serveur secondaire : transfert de zones entre serveur maître (primaire) et un autre serveur (secondaire), chacun ayant autorité sur la zone. Vis-à-vis d'un client, l'un ou l'autre répond en fonction de la vitesse du réseau.

Le cache : un serveur utilisant DNS construit sa propre base de données avec les noms résolus. On peut cantonner un serveur uniquement à ce rôle.

Serveur de type autoritaire : représente officiellement une zone :

Serveur de type non autoritaire : répond aux requêtes à partir du cache, informations non certaines

Serveur de type récursif : effectue des requêtes au nom du client jusqu'à la réponse ou l'erreur.

Serveur de type non récursif : renvoie à un autre serveur les requêtes sans réponse.

2. Installation du DNS

Vous allez mettre en place un service DNS sur le serveur SRVLAN. Il fournira le service DNS principal d'une zone nommée virtualux.local car au début votre entreprise ne dispose pas de son nom de domaine propre. L'extension .local ne portera pas à confusion vis-à-vis des serveurs DNS racines.

a. Installation du paquetage et fichier de configuration générale

Installez le paquetage BIND sous Ubuntu et ses dépendances :

```
sudo apt-get install bind9
```

Le service DNS démarre automatiquement à la fin de l'installation et d'après une configuration de base située dans les fichiers :

- /etc/bind/named.conf : fichier général (incluant les trois fichiers suivants).
- /etc/bind/named.conf/default-zones :

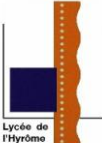
Ce fichier contient quatre zones particulières faisant référence à la zone de la boucle locale suivant la spécification RFC 1912 et dont l'utilité est de traiter les requêtes accidentelles (ou usurpées) pour le broadcast ou les adresses locales. Il contient également le fichier des serveurs racines (db.root) car n'oubliez pas que le service s'intègre dans une hiérarchie.

- /etc/bind/named.conf.options : fichier contenant les options de BIND9.
- /etc/bind/named.conf.local : fichier contenant votre zone (vide pour l'instant).

Sauvegarder ces trois fichiers afin de pallier toute mauvaise manipulation en ajoutant une extension .sauv

Observer le contenu du fichier /etc/bind/named.conf

Observer le contenu et les adresses des serveurs racines dans le fichier /etc/bind/db.root

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Nous allons créer une zone correspondante à notre réseau local :

Remplir le fichier /etc/bind/named.conf.local avec vos zones :

```
// Les zones
zone "virtualux.local" IN {
    type master;
    file "db.virtualux.local";
    allow-update { none; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.virtualux.local";
    allow-update { none; };
};
```

Les 2 zones définissent 2 fichiers qui devront se trouver dans le répertoire par défaut (/var/cache/bind). La première zone permettra de définir les machines du réseau local pour la résolution d'adresses, la seconde zone permet la réalisation la résolution inverse. Notre serveur DNS sera le maitre de ces 2 zones.

b. Construction des fichiers de zones

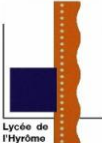
Vous trouverez dans les fichiers ci-dessous une référence à l'arobase soit @. Ce symbole indique un raccourci pour désigner le nom de la zone actuelle spécifié dans l'instruction zone du fichier /etc/bind/named.conf.

Créez le fichier pour la zone directe pour vos machines dans le fichier /var/cache/bind/db.virtualux.local

```
; Fichier pour la résolution directe
$TTL 86400
@ IN SOA srvlan.virtualux.local. root.virtualux.local. (
    2013020201      ;numero de serie
    1w              ;refresh
    1d              ;retry
    4w              ;expire
    1w )            ;negative cache ttl

@ IN NS srvlan.virtualux.local.
srvlan IN A 192.168.4.254
client IN A 192.168.4.1
```

Quelques explications :

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

\$TTL 86400 : spécifie la durée de validité de l'enregistrement (86400 s = 24h), c'est donc le délai maximum pendant lequel un enregistrement pourra être gardé en cache.

On trouve un enregistrement dit SOA pour start of authority, qui définit le nom du serveur, l'adresse électronique de l'administrateur (@ remplacé par un .), et quelques paramètres pour la gestion d'un éventuel serveur secondaire :

- **un numéro de série** que l'on ne doit pas oublier d'incrémenter à chaque modification du fichier. Ce numéro permet aux serveurs esclaves de savoir s'il y a du nouveau, et de modifier le contenu de leurs bases en conséquence. Il est d'usage de choisir un numéro du type yyyymmdd, suivi d'un numéro d'ordre, mais cela n'est nullement obligatoire, l'important étant que ces numéros soient toujours croissants.
- **Refresh, Retry, et Expire** sont des délais, exprimés en secondes, qui vont piloter le comportement des serveurs esclaves. A l'expiration du délai refresh, l'esclave va entrer en contact avec le maître ; s'il ne le trouve pas, il essaiera de nouveau à la fin du délai retry. Et si, au bout du délai expire, il n'est pas parvenu à ses fins, il considérera que le serveur maître a été retiré du service
- **Negative cache TTL** : la durée de vie minimum du cache pour le DNS secondaire

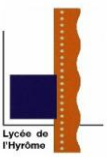
Les 3 dernières lignes ajoutent 3 enregistrements :

- Sur la première, on déclare srvlan.virtualux.local comme étant un serveur de noms de notre zone.
- La seconde, le nom srvlan est associé à l'adresse IP 192.168.4.254
- La troisième concerne la résolution du client

Créez ensuite le fichier pour la zone inverse : /var/cache/bind/rev.virtualux.local

```
; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA srvlan.virtualux.local. root.virtualux.local. (
    2013020201
    1w
    1d
    4w
    1w )
@      IN NS   srvlan.virtualux.local.
254    IN PTR  srvlan.virtualux.local.
1      IN PTR  client.virtualux.local.
```

Les 2 dernières lignes permettent la résolution inverse de nos deux machines du réseau. 254 et 1 sont les 2 derniers octets de l'adresse IP.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Attribuez ces deux fichiers de zones au groupe bind afin de les rendre accessibles au serveur bind par :

```
sudo chgrp bind /var/cache/bind/*
sudo chmod 664 /var/cache/bind/*
```

c. Démarrage du serveur DNS

Modifier la deuxième ligne du fichier /etc/hosts du serveur srvlan :

```
192.168.4.254    srvlan.virtualux.local    srvlan
```

Modifier le fichier /etc/resolvconf/resolv.conf.d/head pour qu'il contienne les lignes suivantes :

```
domain virtualux.local
search virtualux.local
nameserver 192.168.4.254
```

Rappel : la directive domain fixe le domaine courant, search fait ajouter le domaine virtualux.local par défaut aux demandes avec un nom d'hôte non entièrement qualifié. Ensuite votre serveur DNS sera interrogé.

Redémarrer la carte réseau eth0 avec les commandes ifdown et ifup.
Observer le fichier /etc/resolv.conf qui contient les serveurs DNS de votre machine

Lancer l'utilitaire de vérification named-checkconf (si c'est bon il ne retourne rien) qui vérifie par défaut le fichier /etc/bind/named.conf :

```
sudo named-checkconf
```

Lancer le deuxième utilitaire de vérification named-checkzone sur vos fichiers de zone :

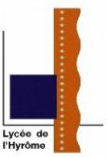
```
cd /var/cache/bind/
sudo named-checkzone -d virtualux.local db.virtualux.local
```

Cette commande retourne normalement :

```
loading "virtualux.local" from "db.virtualux.local" class IN
zone virtualux.local/IN: loaded serial 2013020201
OK
```

Ouvrir sur une autre console par la combinaison [Alt] [F2] et lancer la commande permettant de voir en temps réel le fichier de logs général :

```
sudo tail -f /var/log/syslog
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Revenir sur la première console cette fois par [Alt] [F1] et relancer le service bind9 par :

```
sudo /etc/init.d/bind9 restart
```

Visualiser les affichages de la deuxième console.

Si tout se passe bien, aucune erreur ne doit avoir lieu sur la première console et la deuxième console affiche les logs du service bind (named).

d. Test du serveur DNS

Un bon administrateur ouvre toujours une deuxième console afin d'y surveiller les journaux de logs, donc gardez la numéro deux ouverte. Sur le serveur vous allez utiliser des outils de vérification du service DNS : nslookup, host et dig.

nslookup :

La commande nslookup (disponible aussi sous windows) permet de faire des requête simple DNS à partir de la ligne de commande.

Tester et interpréter les résultats des commandes suivantes, normalement c'est votre serveur DNS qui répond.

```
nslookup srvlan  
nslookup srvlan.virtualux.local  
nslookup client  
nslookup www.facebook.fr
```

host :

La commande host est similaire mais fournit plus de détail avec l'option -v

Tester et interpréter les résultats des commandes suivantes :

```
host srvlan  
host -v client | more  
host -v www.facebook.fr | more
```

dig :

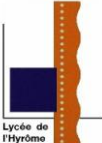
La commande dig est plus complète.

Tester et interpréter les résultats des commandes suivantes :

```
dig client.virtualux.local  
dig  
dig ns virtualux.local  
dig www.google.fr +trace | more  
dig 4.168.192.in-addr.arpa. AXFR  
dig -x 8.8.8.8
```

Vérifier enfin la résolution DNS interne et externe avec :

- votre zone par un ping sur srvlan.virtualux.local
- votre client par un ping sur client.virtualux.local
- l'extérieur par un ping sur www.google.fr par exemple.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Il reste à tester le serveur depuis le client Lubuntu.

Modifier sur le client le fichier `/etc/resolv.conf` pour indiquer que `srvlan (192.168.4.254)` est votre serveur DNS.
Tester avec les commandes `DIG` et `ping` que votre serveur fonctionne correctement.

e. S'appuyer sur un DNS externe

Votre DNS fonctionne mais vous allez le rendre plus performant. Actuellement, il s'occupe des résolutions de la zone `virtualux.local` mais aussi des résolutions externes pour les machines de votre réseau et construit donc son cache. Notez que pour tout ce qui concerne les demandes de résolutions externes (par le biais de la récursivité comme par exemple `google.fr`), la tâche est dévolue aux serveurs racines (fichier `/etc/bind/db.root`) ce qui n'est pas a priori leur travail.

Afin de visualiser les requêtes DNS (port 53) récursives réalisées par votre serveur DNS, lancer une capture de trame avec `Wireshark` depuis votre machine hôte. En parallèle, lancer une commande depuis votre serveur `SRVLAN` permettant de faire une résolution de nom externe.
Observer les requêtes vers les différents serveurs DNS (racine, TLD ...) et les réponses associées

De façon à réduire la charge de travail de votre DNS (et surtout des autres), vous pouvez faire en sorte que cette seconde tâche soit dévolue au serveur DNS "au-dessus de lui", qui peut être celui de votre FAI ou de votre réseau physique dans notre cas.

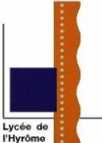
Commenter les lignes ayant trait aux serveurs racines dans le fichier `/etc/bind/named.conf.default-zones` de façon à ce qu'il ne puisse plus les "importuner" :

```
// Référence aux serveurs racines
//zone "." {
//  type hint;
//  file "/etc/binc/db.root";
//};
```

Décommenter et modifier la ligne suivante dans le fichier `/etc/bind/named.conf.options` :

```
options {
    forwarders { 172.16.0.1; };
};
```

Relancer votre serveur DNS, et observer à nouveau les requêtes/réponse DNS avec `Wireshark`.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Partie 2 : Serveur DHCP

Le serveur DHCP le plus utilisé sous Unix et Linux est un serveur fourni par l'ISC (Internet Software Consortium), l'organisme public qui gère Internet. Ce serveur est Open Source.

1. Principe de fonctionnement

Historiquement BootP (Bootstrap Protocol) a été le premier protocole de configuration complet. Il est devenu la base du protocole DHCP qui fonctionne sur les mêmes ports que BootP : UDP 67 et 68.

Le principe de base consiste à affecter dynamiquement une adresse IP à chaque client avec différents paramètres tels que serveur DNS, passerelle par défaut, etc. Cette allocation possède une durée limitée : le bail, renouvelé suivant un intervalle défini. De son côté, le client libère cette adresse quand la session se termine.

L'inconvénient majeur repose essentiellement sur la surcharge du réseau car le protocole utilise des trames de broadcast (diffusion multiple) pour rechercher le serveur DHCP sur le réseau.

À partir de la moitié environ de la durée du bail, le client cherchera à renouveler son bail directement auprès du serveur. Ceci entraîne deux choses :

- il ne faut pas poser une durée de bail trop courte sous peine de hausse du trafic réseau ;
- la plupart du temps le client conserve la même adresse.

Un peu avant la fin ($7/8^{\text{ème}}$ de la durée) et en cas d'échec le client renouvelle sa demande mais cette fois-ci sur le réseau entier.

2. Installation et configuration du service DHCP

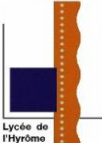
Vous allez monter un service DHCP sur le serveur SRVLAN pour les clients du réseau local avec intégration des inscriptions des clients dans le DNS. Cette installation se fera pour et à partir de l'interface eth1, celle branchée sur le LAN (réseau local).

Installer le paquet du serveur DHCP :

```
sudo apt-get update
sudo apt-get install dhcp3-server
```

Sauvegarder le fichier de configuration par défaut dhcpd.conf dans un fichier dhcp.conf.sauv

```
sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.sauv
```


	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Modifier en ajoutant ou en ajustant le fichier /etc/dhcp/dhcpd.conf comme suit :

```
#pas de mise à jour du DNS
ddns-update-style none;
option domain-name "virtualux.local"
option domain-name-servers 192.168.4.254;
# durée du bail par défaut sans demande express du client en secondes
default-lease-time 600;
# durée du plus long bail possible
max-lease-time 7200;
#serveur autoritaire
authoritative ;
#gestion des log maxi
log-facility local7;
```

Et ajouter à la fin du fichier :

```
#definition de notre reseau local
subnet 192.168.4.0 netmask 255.255.255.0 {
    # passerelle par défaut soit srvlan
    option routers 192.168.4.254;
    # masque de sous-réseau
    option subnet-mask 255.255.255.0;
    # étendue de la plage DHCP
    range 192.168.4.11 192.168.4.100;
}
```

On peut si on le désire réserver une ou plusieurs adresses IP de la plage d'adresses dans le cas par exemple d'une imprimante ou de serveur dont les adresses ne doivent pas changer.

Exemple de réservation en fonction de l'adresse MAC (en dehors de la plage d'attribution) :

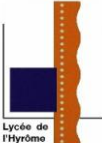
```
host le_nom {
    hardware ethernet 00:A0:78:8E:9E:AA; # exemple
    fixed-address 192.168.4.101; # exemple
}
```

Afin de spécifier l'interface d'écoute du serveur DHCP, modifier le fichier /etc/default/isc-dhcp-server avec :

```
INTERFACES="eth1"
```

Démarrer le serveur :

```
sudo service isc-dhcp-server start
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

Actuellement les log du serveur DHCP sont inscrits dans le fichier de logs général du système : le fichier /var/log/syslog.

Visualiser ce fichier avec la commande cat.

Afin de séparer les logs dans un autre fichier, modifier le fichier /etc/rsyslog.d/50-default.conf en ajoutant la ligne :

```
local7.* /var/log/dhcpd.log
```

Redémarrer le service syslog avec la commande :

```
sudo service rsyslog restart
```

Redémarrer le service dhcp et vérifier que les logs se trouvent bien maintenant dans le fichier /var/log/dhcpd.log

```
sudo service isc-dhcp-server restart
```

3. Tests du serveur DHCP

Sur le client Lubuntu :

- modifier la configuration de l'interface eth0 pour la configurer en dhcp.
- Redémarrer la carte réseau avec les commandes ifdown et ifup. Observer les messages liés au client dhcp.
- Vérifier que la configuration réseau du client est conforme (adresse ip, passerelle, serveur DNS)
- Observer les baux attribués au client dans le fichier /var/lib/dhcp/dhclient.leases

Afin de visualiser les trames DHCP :

Installer wireshark sur le client.

Lancer une capture de trame avec un filtre sur les ports udp 67 et 68.

Observer les trames DHCP générées par la commande suivante :

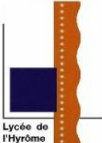
```
sudo dhclient -r eth0
```

Puis avec la commande :

```
sudo dhclient eth0
```

Sur le serveur srvlan :

- observer les logs syslog du serveur DHCP
- Observer les baux attribués aux clients dans le fichier /var/lib/dhcp/dhcpd.leases

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 2 SRVLAN : DNS et DHCP	Réseaux informatiques
BTS IRIS		TP

4. DNS dynamique

Le serveur DHCP peut communiquer avec le serveur DNS pour mettre à jour les enregistrements en fonction des adresses IP distribuées au client DHCP.

Il faut configurer le serveur DNS afin d'autoriser les mises à jour depuis le serveur DHCP qui se trouve sur la machine locale :

Modifier le fichier `/etc/bind/named.conf.local` en modifiant 2 lignes :

```
allow-update { 127.0.0.1; };
```

Redémarrer le serveur DNS

Il faut intervenir également sur le serveur DHCP :

Ajouter ou modifier les lignes ci-dessous au début du fichier `/etc/dhcp/dhcpd.conf` comme suit :

```
# méthode dynamique pour la mise à jour
ddns-update-style interim;
# autorisation de la mise à jour
ddns-updates on;
#specifie le nom de domaine
ddns-domainname "virtualux.local" ;

# donne précisément quel DNS à mettre à jour
zone virtualux.local. { primary 127.0.0.1; }
zone 4.168.192.in-addr.arpa. { primary 127.0.0.1; }
```

Redémarrer le serveur DHCP

Observer les log DHCP et DNS générés par les commandes suivante exécutées sur le client :

```
sudo dhclient -r eth0
```

Puis avec la commande :

```
sudo dhclient eth0
```

Observer les modifications automatiques dans les fichiers zones dans `/var/cache/bind` et tester les nouveaux enregistrements DNS.