

TP1 DNS - NON ENCADRE

Remarques :

Dans votre compte rendu, vous devrez joindre :

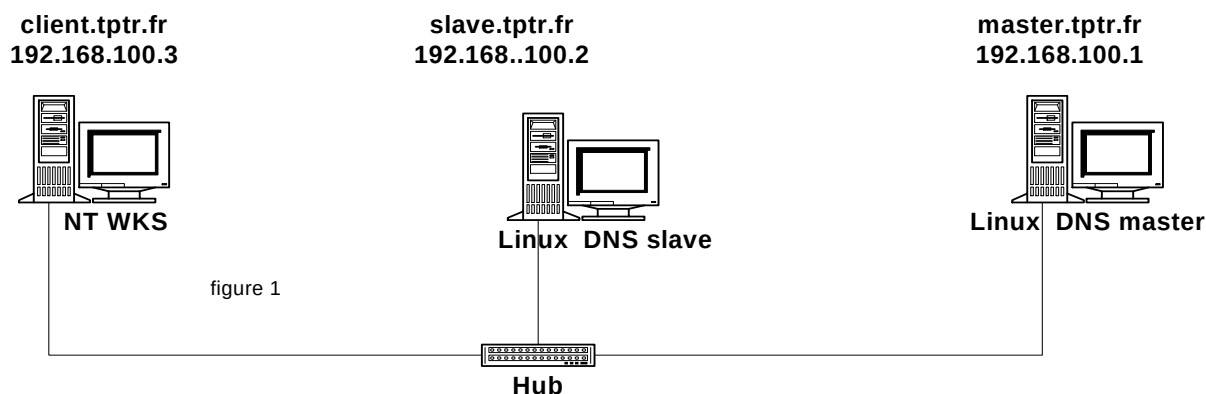
- Les fichiers de configuration des serveurs ;
- Les résultats obtenus en sortie d'écran ;
- Les trames capturées à l'aide de tcpdump ou wireshark;
- Les commandes exécutées sur le poste client.

1. Objectif

- Comprendre le fonctionnement et l'organisation du système de nommage sur Internet
- Etudier le protocole DNS,
- Etudier les rôles serveurs primaire, secondaire et cache.
- Configurer deux stations linux en tant que serveur de noms et une troisième comme client.
- Analyser les flux à l'aide de l'outil [wireshark](#), analyseur de protocoles.

2. Matériel ou Gns et Vmware

Hardware	Software
3 PC équipés de cartes intel	Linux
3 câbles UTP5	Bind9
1 Hub ou Switch	wireshark

3. Architecture

La configuration des machines est effectuée en tant que **root**. Le mot de passe associé est **efreitr**.

4. Liens - Documents

<http://coagul.org/drupal/article/installation-d%E2%80%99serveur-dns-bind-9-sur-debian>

<http://www.debian.org/doc/manuals/network-administrator/ch-bind.html>

DNS-Annexe-Complément

Configurations, Tests

- 1) Configurez le serveur DNS primaire en vous appuyant sur l'annexe ou en consultant les liens indiqués.
- 2) Testez son fonctionnement en local (commandes : **nslookup** ou **dig** - utilisez man)
Exemple :
#nslookup primaire.tptr.fr
#nslookup secondaire.tptr.fr
- 3) Configurez le client (utiliser l'annexe 2) et raccordez les deux postes au hub.
- 4) Interrogez le serveur primaire à partir du client et testez son fonctionnement.
- 5) La machine qui servira de serveur DNS secondaire n'est pas connectée au hub :
 - Configurez cette machine en tant que serveur secondaire (Annexe 4).
 - Exécutez la commande **ifconfig eth0 down**. Quelle est l'utilité de cette commande ?
 - Sur le client, lancez tcpdump (pour capturer les trames qui seront échangées lors du redémarrage du serveur DNS secondaire).
 - Connectez le serveur secondaire au réseau, réactivez l'interface (ifconfig eth0 up) et lancez le service de nom sur le serveur DNS secondaire
- 6) Vous sauvegarderez les trames échangées et proposerez un diagramme temporel .
- 7) Modifiez le fichier resolv.conf du client pour que :
 - le premier serveur de nom interrogé soit le serveur secondaire ;
 - le deuxième le serveur de nom primaire.
- 8) Le serveur primaire étant désactivé, lancez une interrogation à partir du client. Les trames échangées devront être sauvegardées et représentées sur un diagramme temporel.
- 9) Réactivez le serveur primaire, désactivez le secondaire. Formulez une nouvelle interrogation. Sauvegardez les trames échangées.
- 10) Analysez les trames capturées dans la question 9).
- 11) Sur quels protocoles s'appuie le DNS ? Définissez brièvement le rôle de ces protocoles ?
- 12) Quel est le port utilisé par le service DNS ?
- 13) Proposez quelques interrogations à l'aide de la commande nslookup ou dig.

Annexes – DNS – A titre d'exemple**Activation DNS - Logiciel named (bind)**

Lancer votre dns par la commande :
`/etc/init.d/bind9 restart`

Vérifier qu'il fonctionne
`ps -aef | grep named`

Puis examiner le fichier log `/var/log/syslog` pour vérifier que le lancement c'est bien déroulé grâce à la commande :
`less /var/log/syslog | grep named`

Dans le même temps on vérifiera avec quelles options est lancé named.

Test1 DNS

Mettre à jour le fichier `resolv.conf` avec l'adresse de votre dns.
Interroger votre dns par les commandes ou nom représente le nom mis précédemment
`dig nom.fr`
`dig -t any nomsrv.fr`
`dig nomsrv.fr mx`
`dig nomsrv.fr any`

Lancer [wireshark](#), puis essayer d'autres commandes en écoutant localhost.

Se mettre sur une autre machine, mettre à jour `/etc/resolv.conf`, puis lancer wireshark pour visualiser les trames échangées sur l'interface réseau, puis effectuer des tests identiques.

Test2 DNS

Faire
`ping voisin.nom.fr`
Faire
`ping www.nom.fr`
Que remarquez-vous? Pourquoi

Faire
`ping voisin`
Qu'obtenez-vous?

Modifier votre fichier `/etc/resolv.conf` en ajoutant la ligne:
`domain nom.fr`

Faire
`ping voisin`
Qu'obtenez-vous? Pourquoi?