Auteur: P. Petit	*Titre: TD DNS*	*Version: 1.2*
Date: 07/11/2006	Licence: Gnu Free Documentation Licence	Durée: 1h00

DNS

Objectifs

- installation et gestion d'un serveur DNS

Configuration initiale

Ce TD est à réaliser avec deux stations de travail windows Xp pro pro nommées **station1** et **station2** et un serveur windows 2k3 server nommés **serveur1**. Le serveur **serveur1** ne sera PAS contrôleur de domaine. **serveur1** aura deux cartes ethernet.

Prérequis

- configuration IP sous w2k
- notions théoriques sur le DNS
- utilisation d'un analyseur de trames

Exercice 1: configuration initiale

Vous travaillerez avec deux machines virtuelles vmware: une machine virtuelle windows 2k3 server **serveur1** et une machine windows Xp pro **station1**. **serveur1** aura l'adresse IP 192.168.2.2 sur vmnet5. **station1** aura l'adresse IP 192.168.2.11 sur vmnet5. Elle utilisera **serveur1** comme serveur dns et comme routeur par défaut.

Exercice 2: installation du serveur

Installez le serveur DNS de windows. Pour cela, vous avez deux solutions :

- à l'ancienne: panneau de configuration/Ajout de programmes puis composants windows puis services de mise en réseau puis détail et sélectionnez le serveur DNS.
- w2k3: dans « gérer votre ordinateu »: ajouter un rôle et choisissez ràf

Exercice 3: domaine, zone directe, inverse

Cet exercice est à faire sur papier uniquement

Expliquez la différence entre un domaine et une zone dns. Qu'est-ce qu'une zone inverse.

Domaine dns: tout ce qui est en dessous de univ-evry.fr est dans le domaine univ-evry.fr. ex. toto.univ-evry.fr, u2.ibisc.univ-evry.fr, www.ibisc.univ-evry.fr, www.info.univ-evry.fr, www.univ-evry.fr

Zone: ce qui est géré par un serveur donné. Les zones déléguées ne font pas partie de la zone. Exemple: ibisc.univ-evry.fr n'est pas géré par le dns de l'université. Le dns de l'université a délégué la gestion de cette zone fille au serveur dns d'ibisc. Donc ibisc.univ-evry.fr ne fait pas partie de la zone univ-evry.fr.

Remarque: s'il n'y a pas de délégation de domaine fils, la zone et le domaine, c'est la même chose.

Www.univ-evry.fr est dans la zone univ-evry.fr

comment déterminer à l'aide de requetes DNS que ibisc.univ-evry.fr n'est pas dans la zone univ-evry.fr.

Réponse: on liste les dns de univ-evry.fr. On liste les dns de ibisc.univ-evry.fr et on voit que ce ne sont pas les mêmes. Pour ça, on fait une requete de type NS.

Nos machines seront sur le domaine DNS cmell.shayol.org . Citez les deux zones que devra gérer votre serveur DNS.

La zone directe cmell.shayol.org et la zone inversée 2.168.192.in-addr.arpa (réseau 192.168.2.0/24) car aucun autre serveur ne gère cette zone inversée. Toute machine doit avoir au moins une entrée directe et une entrée inversée.

Exercice 4: configuration du serveur DNS

Ouvrez la console de gestion de l'ordinateur. En développant l'item Services, vous trouverez la console de gestion du serveur DNS. Votre travail consiste à:

- Créez la zone directe
  - clic droit sur zone directe/nouvelle zone puis zone principale standard puis indiquez le nom de la zone
  - dans les propriétés de la zone, onglet serveurs de nom, indiquez l'adresse IP du serveur DNS
- créez la zone inversée
- ajouter une entrée directe (clic droit sur la zone/nouvel hôte)
- ajouter une entrée inverse pour votre serveur (clic droit sur la zone inverse/nouveau pointeur)
- ajouter une entrée en une seule action une entrée directe et inverse pour **station1**
- ajouter un enregistrement CNAME nommé poste1 pointant vers station1.cmellNN.shayol.org (clic droit sur la zone/nouvel alias)
- ajoutez un enregistrement CNAME nomme test pointant vers un nom inexistant. La création a-t-elle été possible ?

Exercice 5:

Sur votre serveur, ouvrez une fenêtre de commande et tapez y la commande « ping station1.cmellNN.shayol.org ». Faites de même en tapant directement « ping station1 ». Que se passe-t-il ? Expliquez.

Poste1 n'existe pas sur le serveur. Ce qui existe, c'est poste1.cmell.shayol.org. Définir des suffixes dns permet à la machine de compléter les noms incomplets avec ces suffixes avant de faire sa requete dns. Elle essaie les suffixes dans l'ordre jusqu'à trouver un suffixe qui marche ou constater que le nom demandé n'existe pas.

Expliquez ce qu'est le suffixe dns par défaut. Peut-on ajouter plusieurs suffixes dns à une machine ?

Indication:

- Poste de travail/propriétés/identification/propriétés/autres

- tcp-ip/propriétés/avancé/dns/ajouter des suffixes dns

Le suffixe dns est la partie du nom de machine qui suit le premier point. ex. u2.ibisc.fr a comme nom de suffixe ibisc.fr. Lors d'une interrogation, le serveur dns s'attend à une requète sur le nom complet. L'utilisateur aimerait bien pouvoir abréger le nom en n'utilisant que le nom sans le nom de domaine (u2 au lieu de u2.ibisc.fr). Définir un ou plusieurs suffixes dns sur un poste permet de ne donner que u2. Le poste complètera par le suffixe dns avant d'envoyer sa requète au serveur dns. Si on définit plusieurs suffixe, il les essaiera dans l'ordre.

Pour le voir, une méthode consiste à définir plusieurs suffixe et à faire une capture de trame durant une requete. On voit clairement les diverses demandes que fait le client au serveur.

Si mes suffixes sont cmell.shayol.org, lip6.fr et ibisc.fr. Quand j'utilise le nom u2, le poste client essaie u2.cmell.shayol.org, u2.lip6.fr et u2.

Exercice 6: interrogation du dns avec nslookup

Sous windows, la commande nslookup permet d'interroger le dns. Sous unix, cette commande existe mais elle est considérée comme obsolète et on lui préfère la commande host qui est plus polyvalente.

La description qui suit est celle de la syntaxe de la commande nslookup de windows (W2K+). La commande nslookup peut s'utiliser en mode interactif ou non interactif.

Par défaut, nslookup utiliser le serveur dns du poste. Il est possible d'utiliser un autre serveur dns en le précisant comme second argument sur la ligne de commande ou en utilisant la commande server en mode interactif. Exemple: « nslookup www.univ-evry.fr 194.199.90.1 ».

En mode interactif, on peut sélectionner le type de requête à l'aide de la commande « set type=RR ». En mode non interactif, on le précise avec l'option « -query-type=RR ». Exemple: pour obtenir les serveurs dns de la zone univ-evry.fr: « nslookup -query-type NS univ-evry.fr ». Le tableau suivant, extrait de la documentation de windows Xp indique les types possibles :

Valeur	*Description*
A	Spécifie l'adresse IP d'un ordinateur.
ANY	Spécifie tous les types de données.
CNAME	Spécifie un nom canonique d'alias.
GID	Spécifie un identificateur de groupe d'un nom de groupe.
HINFO	Spécifie le type de système d'exploitation et d'unité centrale d'un ordinateur.
MB	Spécifie un nom de domaine d'une boîte aux lettres.
MG	Spécifie un membre d'un groupe de messagerie.
MINFO	Spécifie des informations sur une liste de messagerie ou une boîte aux lettres.
MR	Spécifie le nom de domaine de la messagerie renommée.
MX	Spécifie le serveur de messagerie.
NS	Spécifie un serveur de noms DNS pour la zone nommée.
PTR	Spécifie un nom d'ordinateur si l'interrogation correspond à une adresse IP. Dans le cas contraire, spécifie le pointeur vers d'autres informations.
SOA	Spécifie le début d'autorité d'une zone DNS.

TXT	Spécifie les informations de texte.
UID	Spécifie l'identificateur de l'utilisateur.
UINFO	Spécifie les informations de l'utilisateur.
WKS	Décrit un service connu.

Utilisez la commande nslookup pour obtenir les informations suivantes :

- le contenu du RR SOA de la zone cmell.shayol.org
- la liste des serveurs dns de la zone cmell.shayol.org
- l'adresse ip de station1.cmellNN.shayol.org
- le nom de la machine qui a comme adresse ip 192.168.202.2
- l'adresse ip de poste01.cmellNN.shayol.org

Auteur: P. Petit	*Titre: TD DNS*	*Version: 1.2*
Date: 07/11/2006	Licence: Gnu Free Documentation Licence	Durée: 1h00

Exercice 7: installation d'un dns secondaire

Pour cette partie du TD, il vous faut une seconde machine windows server **serveur3** dont vous mettrez la carte réseau sur vmnet5. Son IP sera 192.168.2.3.

On souhaite que **serveur3** soit serveur dns secondaire pour la zone cmell.shayol.org. Rappelez ce qu'est un serveur secondaire et quel est l'intérêt d'en avoir un.

Un serveur secondaire pour une zone donnée est un serveur qui a accès en lecture seule à une copie de la zone. Il peut prendre le relais en cas de panne du serveur primaire. Il prend en charge une partie des requètes (répartition de charge entre tous les serveurs). Un secondaire ne sera connu que s'il y a une entre NS pointant vers lui dans la zone.

Que doit-on créer sur serveur3 pour qu'il soit serveur dns secondaire ?

On doit créer une zone secondaire standard cmell.shayol.org. Sur serveur1, on doit s'assurer :

- **que serveur3 a une entrée A dans la zone (et une entrée dans la zone inversée)**
- **que server3 est listé comme dns de la zone (propriétés de la zone/onglet serveurs de noms)**
- **que serveur3 est autorisé à réalisé des transferts de zone (propriétés de la zone/ongle transfert de zone/cocher « autoriser les serveurs dns listés dans l'onglet serveurs dns ».**

Les informations présentes sur **serveur3** sont-elles les mêmes que celles présentes sur le serveur dns primaire ?

Exercice 8: mise à jour du secondaire

Lancez un outil de capture de trame sur serveur3 (wireshark ou ethereal par ex.).

Ajoutez une entrée dans la zone dns de serveur1 et étudiez le trafic qui sert à la mise à jour.

Quelle requete dns permet de savoir que serveur3 est dns secondaire de la zone ? Le voit-on ?

Une requete NS car elle permet de demander les serveurs dns d'une zone (cmell.shayol.org dans notre cas) : nslookup query-type=NS cmell.shayol.org. On doit obtenir 2 réponses : serveur1 et serveur3.

Si vous avez oublié de déclarer serveur3 comme dns de la zone, faites le.

Propriétés de la zone puis onglet « serveur de noms ».

Ajoutez une entrée dans la zone dns de serveur1 et étudiez le trafic qui sert à la mise à jour.

Une fois que le transfert de zone a eu lieu, oui. Si lance un analyseur de trame et qu'on modifie des choses dans la zone, on voit que serveur1 notifie serveur3 du changement et que serveur3 lance un transfert de zone incrémental (IXFR) pour récupérer les modifications.