

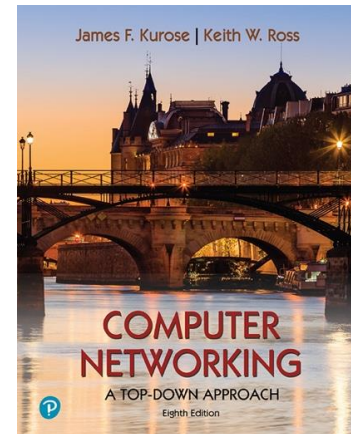
Laboratoire Wireshark :

DNS v8.0

Supplement to *Computer Networking: A Top-Down Approach*, 8e éd. , J.F. Kurose et K.W. Ross

« Dites-le moi et j'oublie. Montrez-moi et je me souviens.
Impliquez-moi et je comprends. Proverbe chinois

© 2005-2020, J.F Kurose et K.W. Ross, Tous droits réservés



Comme décrit dans la section 2.4 du texte, le système de noms de domaine (DNS) traduit les noms d'hôte en adresses IP, remplissant ainsi un rôle essentiel dans l'infrastructure Internet. Dans cet atelier, nous examinerons de plus près le côté client du DNS.

Rappelons que le rôle du client dans le DNS est relativement simple : un client envoie une ¹*requête* à son serveur DNS local et reçoit une *réponse*. Comme le montrent les figures 2.19 et 2.20 du manuel, beaucoup de choses peuvent se passer « sous les couvertures », invisibles pour les clients DNS, car les serveurs DNS hiérarchiques communiquent entre eux pour résoudre de manière récursive ou itérative la requête DNS du client. Du point de vue du client DNS, cependant, le protocole est assez simple – une requête est formulée sur le serveur DNS local et une réponse est reçue de ce serveur.

Avant de commencer cet atelier, vous voudrez probablement examiner DNS en lisant la section 2.4 du texte. En particulier, vous pouvez consulter le matériel sur les **serveurs DNS locaux**, la **mise en cache DNS**, les **enregistrements et messages DNS** et le **champ TYPE** de l'enregistrement DNS.

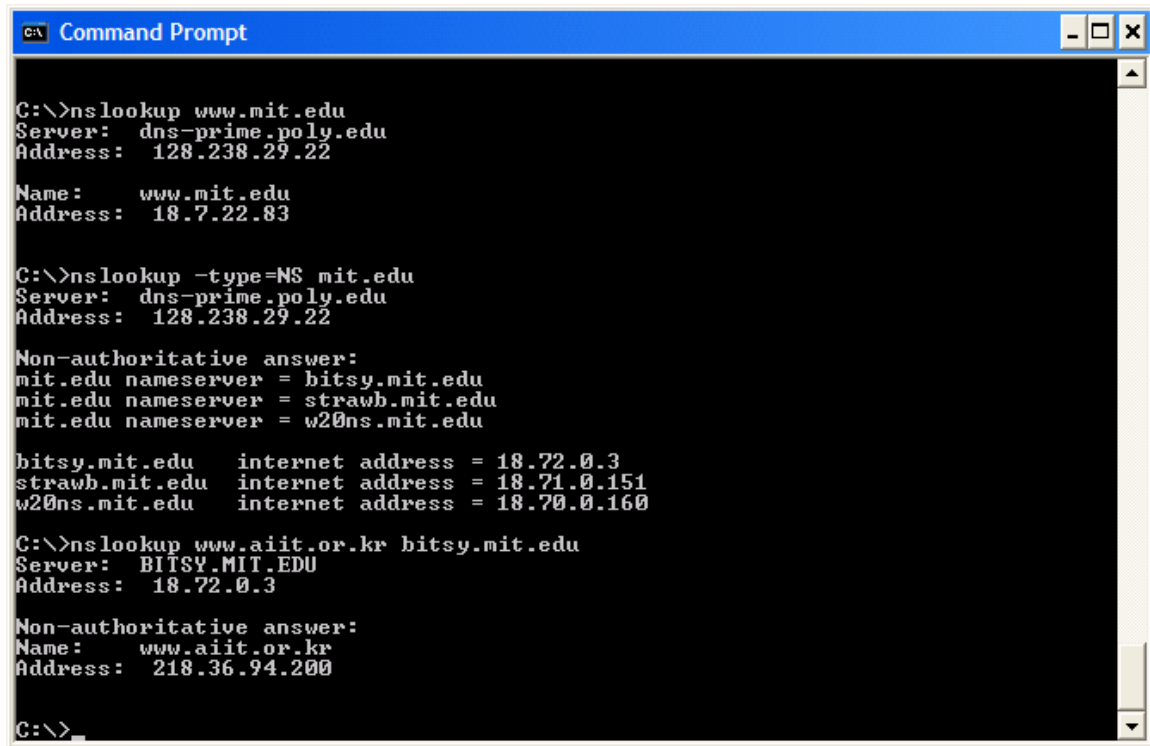
1. recherche

Dans cet atelier, nous utiliserons largement l'outil *nslookup*, qui est disponible dans la plupart des plates-formes Linux / Unix et Microsoft aujourd'hui. Pour exécuter *nslookup* sous Linux/Unix, il vous suffit de taper la commande *nslookup* sur la ligne de commande. Pour l'exécuter dans Windows, ouvrez l'invite de commandes et exécutez *nslookup* sur la ligne de commande.

Dans son opération la plus basique, l'outil *nslookup* permet à l'hôte exécutant l'outil d'interroger n'importe quel serveur DNS spécifié pour un enregistrement DNS. Le serveur DNS interrogé peut être un serveur DNS racine, un serveur DNS de domaine de premier niveau, un serveur DNS faisant autorité ou un serveur DNS intermédiaire (voir le

¹ Références à figures et sections sont pour le 8^{ième} édition de notre texte, *Réseaux informatiques, une approche descendante*, 8^{ième} Ed. J.F. Kurose et K.W. Ross, Addison-Wesley/Pearson, 20 ans 20.

manuel pour les définitions de ces termes). Pour accomplir cette tâche, *nslookup* envoie une requête DNS au serveur DNS spécifié, reçoit une réponse DNS de ce même serveur DNS et affiche le résultat.



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Name:    www.mit.edu
Address: 18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu  internet address = 18.71.0.151
w20ns.mit.edu   internet address = 18.70.0.160

C:\>nslookup www.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name:    www.aiit.or.kr
Address: 218.36.94.200

C:\>
```

La capture d'écran ci-dessus montre les résultats de trois commandes *nslookup* indépendantes (affichées dans l'invite de commandes Windows). Dans cet exemple, l'hôte client est situé sur le campus de l'Université polytechnique de Brooklyn, où le serveur DNS local par défaut est dns-prime.poly.edu. Lors de l'exécution de *nslookup*, si aucun serveur DNS n'est spécifié, *nslookup* envoie la requête au serveur DNS par défaut, qui dans ce cas est dns-prime.poly.edu. Considérez la première commande :

```
nslookup www.mit.edu
```

En mots, cette commande dit « s'il vous plaît envoyez-moi l'adresse IP de l'hôte *www.mit.edu* ». Comme le montre la capture d'écran, la réponse de cette commande fournit deux informations : (1) le nom et l'adresse IP du serveur DNS qui fournit la réponse ; et (2) la réponse elle-même, qui est le nom d'hôte et l'adresse IP de *www.mit.edu*. Bien que la réponse provienne du serveur DNS local de l'Université polytechnique, il est tout à fait possible que ce serveur DNS local ait contacté de manière itérative plusieurs autres serveurs DNS pour obtenir la réponse, comme décrit dans la section 2.4 du manuel.

Considérons maintenant la deuxième commande:

```
nslookup -type=NS mit.edu
```

Dans cet exemple, nous avons fourni l'option « -type=NS » et le domaine « mit.edu ». Cela entraîne l'envoi par *nslookup* d'une requête pour un enregistrement de type NS au serveur DNS local par défaut. En d'autres termes, la requête dit: « Veuillez m'envoyer les noms d'hôte du DNS faisant autorité pour mit.edu ». (Lorsque l'option -type n'est pas utilisée, *nslookup* utilise la valeur par défaut, qui consiste à interroger les enregistrements de type A.) La réponse, affichée dans la capture d'écran ci-dessus, indique d'abord le serveur DNS qui fournit la réponse (qui est le serveur DNS local par défaut) ainsi que trois serveurs de noms MIT. Chacun de ces serveurs est en effet un serveur DNS faisant autorité pour les hôtes du campus du MIT. Cependant, *nslookup* indique également que la réponse est « non autorisée », ce qui signifie que cette réponse provient du cache d'un serveur plutôt que d'un serveur DNS MIT faisant autorité. Enfin, la réponse inclut également les adresses IP des serveurs DNS faisant autorité au MIT. (Même si la requête type-NS générée par *nslookup* n'a pas explicitement demandé les adresses IP, le serveur DNS local les a renvoyées « gratuitement » et *nslookup* affiche le résultat.)

Considérons enfin la troisième commande:

```
nslookup www.aiit.or.kr bitsy.mit.edu 8.8.8.8
```

Dans cet exemple, nous indiquons que nous voulons que la requête envoyée au serveur DNS bitsy.mit.edu plutôt qu'au serveur DNS par défaut (dns-prime.poly.edu). Ainsi, la transaction de requête et de réponse a lieu directement entre notre hôte de requête et bitsy.mit.edu. Dans cet exemple, le serveur DNS fournit bitsy.mit.edu l'adresse IP de l'hôte www.aiit.or.kr, qui est un serveur Web de l'Advanced Institute of Information Technology (en Corée).

Maintenant que nous avons parcouru quelques exemples illustratifs, vous vous interrogez peut-être sur la syntaxe générale des commandes *nslookup*. La syntaxe est la suivante :

```
nslookup -option1 -option2 hôte-à-trouver dns-server
```

En général, *nslookup* peut être exécuté avec zéro, une, deux ou plusieurs options. Et comme nous l'avons vu dans les exemples ci-dessus, le serveur dns est également facultatif; si elle n'est pas fournie, la requête est envoyée au serveur DNS local par défaut.

Maintenant que nous avons fourni un aperçu de *nslookup*, il est temps pour vous de l'essayer vous-même. Procédez comme suit (et notez les résultats) :

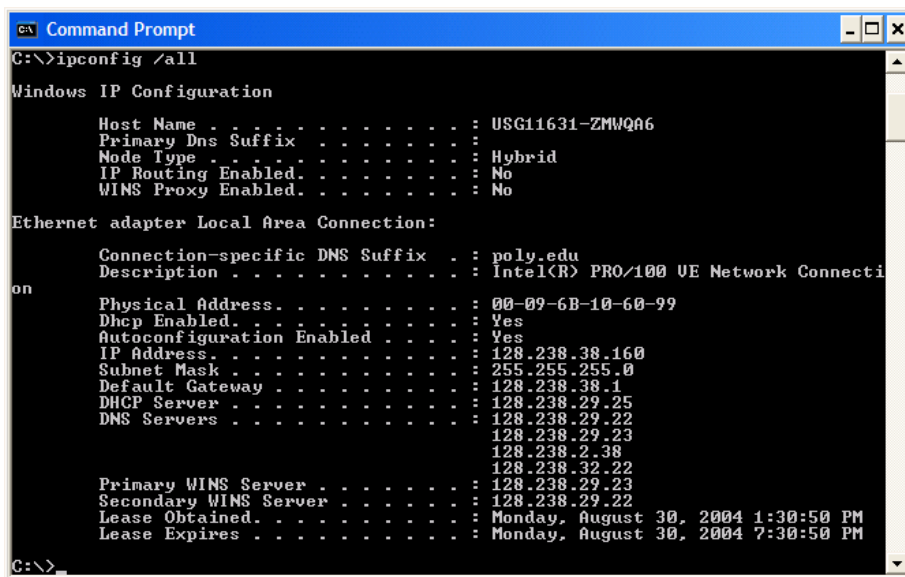
1. Exécutez *nslookup* pour obtenir l'adresse IP d'un serveur Web en Asie. Quelle est l'adresse IP de ce serveur ?
2. Exécutez *nslookup* pour déterminer les serveurs DNS faisant autorité pour une université en Europe.

2. ipconfig

ipconfig (pour Windows) et *ifconfig* (pour Linux/Unix) sont parmi les petits utilitaires les plus utiles de votre hôte, en particulier pour le débogage des problèmes de réseau. Ici, nous ne décrivons que *ipconfig*, bien que linux / Unix *ifconfig* soit très similaire. *ipconfig* peut être utilisé pour afficher vos informations TCP/IP actuelles, y compris votre adresse, les adresses de serveur DNS, le type d'adaptateur, etc. Par exemple, si vous toutes ces informations sur votre hôte simplement en entrant

`ipconfig \tout`

dans l'invite de commandes, comme indiqué dans la capture d'écran suivante.



```
Command Prompt
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : USG11631-ZMWQA6
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : poly.edu
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
    Physical Address. . . . . : 00-09-6B-10-60-99
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 128.238.38.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 128.238.38.1
    DHCP Server . . . . . : 128.238.29.25
    DNS Servers . . . . . : 128.238.29.22
                           128.238.29.23
                           128.238.2.38
                           128.238.32.22
    Primary WINS Server . . . . . : 128.238.29.23
    Secondary WINS Server . . . . . : 128.238.29.22
    Lease Obtained. . . . . : Monday, August 30, 2004 1:30:50 PM
    Lease Expires . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>
```

ipconfig est également très utile pour gérer les informations DNS stockées dans votre hôte. Dans la section 2.5, nous avons appris qu'un hôte peut mettre en cache les enregistrements DNS qu'il a récemment obtenus. Pour afficher ces enregistrements mis en cache, après l'invite `C:\>` fournissez la commande suivante :

```
ipconfig /displaydns
```

Chaque entrée affiche le temps de vie restant (TTL) en secondes. Pour vider le cache, entrez

```
ipconfig /flushdns
```

Le vidage du cache DNS efface toutes les entrées et recharge les entrées du fichier hosts.

3. Traçage DNS avec Wireshark

Maintenant que nous sommes familiers avec *nslookup* et *ipconfig*, nous sommes prêts à passer à des affaires sérieuses. Capturons d'abord les paquets DNS générés par l'activité de navigation Web ordinaire.

- Utilisez *ipconfig* pour vider le cache DNS de votre hôte.
- Ouvrez votre navigateur et videz le cache de votre navigateur. (Avec Internet Explorer, accédez au menu Outils et sélectionnez Options Internet, puis dans l'onglet Général, sélectionnez Supprimer les fichiers.)
- Ouvrez Wireshark et entrez "ip.addr == your_IP_address" dans le filtre, où vous obtenez your_IP_address avec *ipconfig*. Ce filtre supprime tous les paquets qui ne proviennent pas et ne sont pas destinés à votre hôte.
- Démarrez la capture de paquets dans Wireshark.
- Avec votre navigateur, visitez la page Web : <http://www.ietf.org>
- Arrêtez la capture de paquets.

Si vous ne parvenez pas à exécuter Wireshark sur une connexion réseau en direct, vous pouvez télécharger un fichier de trace de paquets qui a été capturé en suivant les étapes ci-dessus sur l'un des ordinateurs de l'auteur². Répondez aux questions suivantes. Dans la mesure du possible, lorsque vous répondez à une question ci-dessous, vous devez remettre une impression du ou des paquets dans la trace que vous avez utilisée pour répondre à la question posée. Annotez l'imprimé³ pour expliquer votre réponse. Pour imprimer un paquet, utilisez *Fichier->Imprimer*, choisissez Paquet sélectionné *uniquement*, Choisissez *Ligne récapitulative* des paquets et sélectionnez la quantité minimale de détails de paquet dont vous avez besoin pour répondre à la question.

3. Recherchez les messages de requête et de réponse DNS. Sont-ils ensuite envoyés via UDP ou TCP ?
4. Quel est le port de destination du message de requête DNS ? Quel est le port source du message de réponse DNS ?
5. À quelle adresse IP le message de requête DNS est-il envoyé ? Utilisez *ipconfig* pour déterminer l'adresse IP de votre serveur DNS local. Ces deux adresses IP sont-elles identiques ?

² Télécharger le fichier zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> et extrayez le fichier **dns-ethereal-trace-1**. Les traces dans ce fichier zip ont été collectées par Wireshark en cours d'exécution sur l'un des ordinateurs de l'auteur, tout en effectuant les étapes indiquées dans le laboratoire Wireshark. Une fois que vous avez téléchargé la trace, vous pouvez la charger dans Wireshark et afficher la trace à l'aide de l'option *Ligne* menu déroulant, sélection *Ouvrir*, puis en sélectionnant l'application **Fichier de trace dns-ethereal-trace-1**.

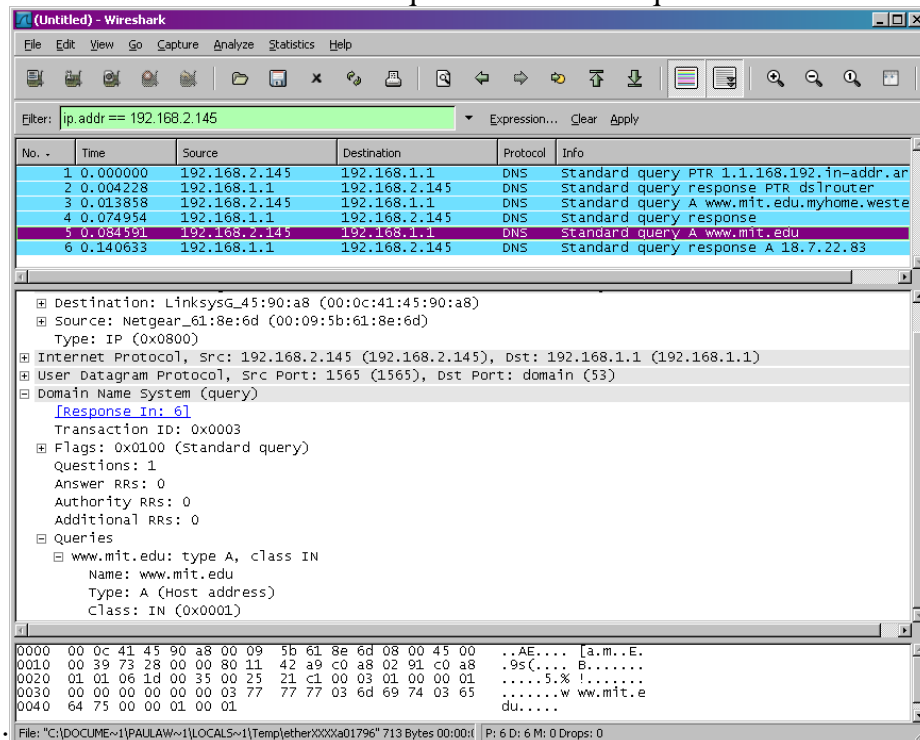
³ Qu'entendons-nous par « annoter » ? Si vous remettez une copie papier, veuillez mettre en évidence l'endroit où vous avez trouvé la réponse dans l'impression et ajouter du texte (de préférence avec un stylo de couleur) en notant ce que vous avez trouvé dans ce que vous avez mis en évidence. Si vous remettez une copie électronique, ce serait génial si vous pouviez également mettre en évidence et annoter.

- Examinez le message de requête DNS. De quel « Type » de requête DNS s'agit-il ? Le message de requête contient-il des « réponses » ?
- Examinez le message de réponse DNS. Combien de « réponses » sont fournies ? Que contiennent chacune de ces réponses ?
- Considérez le paquet TCP SYN suivant envoyé par votre hôte. L'adresse IP de destination du paquet SYN correspond-elle à l'une des adresses IP fournies dans le message de réponse DNS ?
- Cette page Web contient des images. Avant de récupérer chaque image, votre hôte émet-il de nouvelles requêtes DNS ?

Maintenant, jouons avec *nslookup*⁴.

- Démarrez la capture de paquets.
- Faites une *recherche sur* `www.mit.edu`
- Arrêtez la capture de paquets.

Vous devriez obtenir une trace qui ressemble à ce qui suit



Nous voyons sur la capture d'écran ci-dessus que *nslookup* a en fait envoyé trois requêtes DNS et reçu trois réponses DNS. Aux fins de cette affectation, en répondant aux questions suivantes, ignorez les deux premiers ensembles de requêtes/réponses, car ils sont spécifiques à *nslookup* et ne sont normalement pas générés par des applications

⁴ Si vous ne parvenez pas à exécuter Wireshark et à capturer un fichier de trace, utilisez le fichier de trace `dns-ethereal-trace-2` dans le fichier zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

Internet standard. Vous devez plutôt vous concentrer sur les derniers messages de requête et de réponse.

10. Quel est le port de destination du message de requête DNS ? Quel est le port source du message de réponse DNS ?
11. À quelle adresse IP le message de requête DNS est-il envoyé ? S'agit-il de l'adresse IP de votre serveur DNS local par défaut ?
12. Examinez le message de requête DNS. De quel « Type » de requête DNS s'agit-il ? Le message de requête contient-il des « réponses » ?
13. Examinez le message de réponse DNS. Combien de « réponses » sont fournies ? Que contiennent chacune de ces réponses ?
14. Fournissez une capture d'écran.

Maintenant, répétez l'expérience précédente, mais émettez plutôt la commande:

```
nslookup -type=NS mit.edu
```

Répondez aux questions suivantes⁵ :

15. À quelle adresse IP le message de requête DNS est-il envoyé ? S'agit-il de l'adresse IP de votre serveur DNS local par défaut ?
16. Examinez le message de requête DNS. De quel « Type » de requête DNS s'agit-il ? Le message de requête contient-il des « réponses » ?
17. Examinez le message de réponse DNS. Quels serveurs de noms MIT le message de réponse fournit-il ? Ce message de réponse fournit-il également les adresses IP des nommeurs mit ?
18. Fournissez une capture d'écran.

Maintenant, répétez l'expérience précédente, mais émettez plutôt la commande:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Répondez aux questions suivantes⁶:

19. À quelle adresse IP le message de requête DNS est-il envoyé ? S'agit-il de l'adresse IP de votre serveur DNS local par défaut ? Si ce n'est pas le cas, à quoi correspond l'adresse IP ?
20. Examinez le message de requête DNS. De quel « Type » de requête DNS s'agit-il ? Le message de requête contient-il des « réponses » ?
21. Examinez le message de réponse DNS. Combien de « réponses » sont fournies ? Que contient chacune de ces réponses ?

⁵ Si vous ne parvenez pas à exécuter Wireshark et à capturer un fichier de trace, utilisez le fichier de trace **dns-ethereal-trace-3** dans le fichier zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

⁶ Si vous ne parvenez pas à exécuter Wireshark et à capturer un fichier de trace, utilisez le fichier de trace **dns-ethereal-trace-4** dans le fichier zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>