

Travaux pratiques – Observation de la résolution DNS

Objectifs

- 1re partie : Observer la conversion DNS d'une URL en adresse IP
- 2e partie : Observer la recherche DNS à l'aide de la commande Nslookup sur un site Web
- 3e partie : Observer la recherche DNS à l'aide de la commande Nslookup sur des serveurs de messagerie

Contexte/scénario

Le système de noms de domaine (DNS) est invoqué lorsque vous tapez une URL, comme <http://www.cisco.com>, dans un navigateur Web. La première partie de l'URL décrit le protocole utilisé. Les protocoles courants sont le protocole HTTP (Hypertext Transfer Protocol), le protocole HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) et le protocole FTP (File Transfer Protocol).

Le système DNS utilise la deuxième partie de l'URL, en l'occurrence www.cisco.com. Il traduit le nom de domaine (www.cisco.com) en adresse IP pour autoriser l'hôte source à atteindre l'hôte de destination. Au cours de ces travaux pratiques, vous allez observer le système DNS en action et utiliser la commande **nslookup** (recherche de serveur de noms) afin d'obtenir des informations DNS supplémentaires. Travaillez avec un partenaire pour réaliser ces travaux pratiques.

Ressources requises

- 1 ordinateur (Windows 7, Vista ou XP, équipé d'Internet et d'un accès aux invites de commande)

1re partie : Observer la conversion DNS d'une URL en adresse IP

- a. Cliquez sur le bouton **Démarrer Windows**, tapez **cmd** dans le champ de recherche, et appuyez sur Entrée. La fenêtre d'invite de commandes s'affiche.
- b. À l'invite de commandes, envoyez une requête ping à l'URL de l'ICANN (Internet Corporation for Assigned Names and Numbers) à l'adresse **www.icann.net**. L'ICANN coordonne le DNS, les adresses IP, la gestion du système de noms de domaine de haut niveau et les fonctions de gestion du système de serveur racine. L'ordinateur doit convertir www.icann.net en adresse IP pour savoir où envoyer les paquets ICMP (Internet Control Message Protocol).
- c. La première ligne de l'écran affiche www.icann.net converti en adresse IP par le système DNS. Vous devez pouvoir voir l'effet du système DNS même si votre institution dispose d'un pare-feu qui empêche d'exécuter la commande ping, ou si le serveur de destination vous empêche d'effectuer ce type de commande sur son serveur Web.

```
C:\>ping www.icann.net

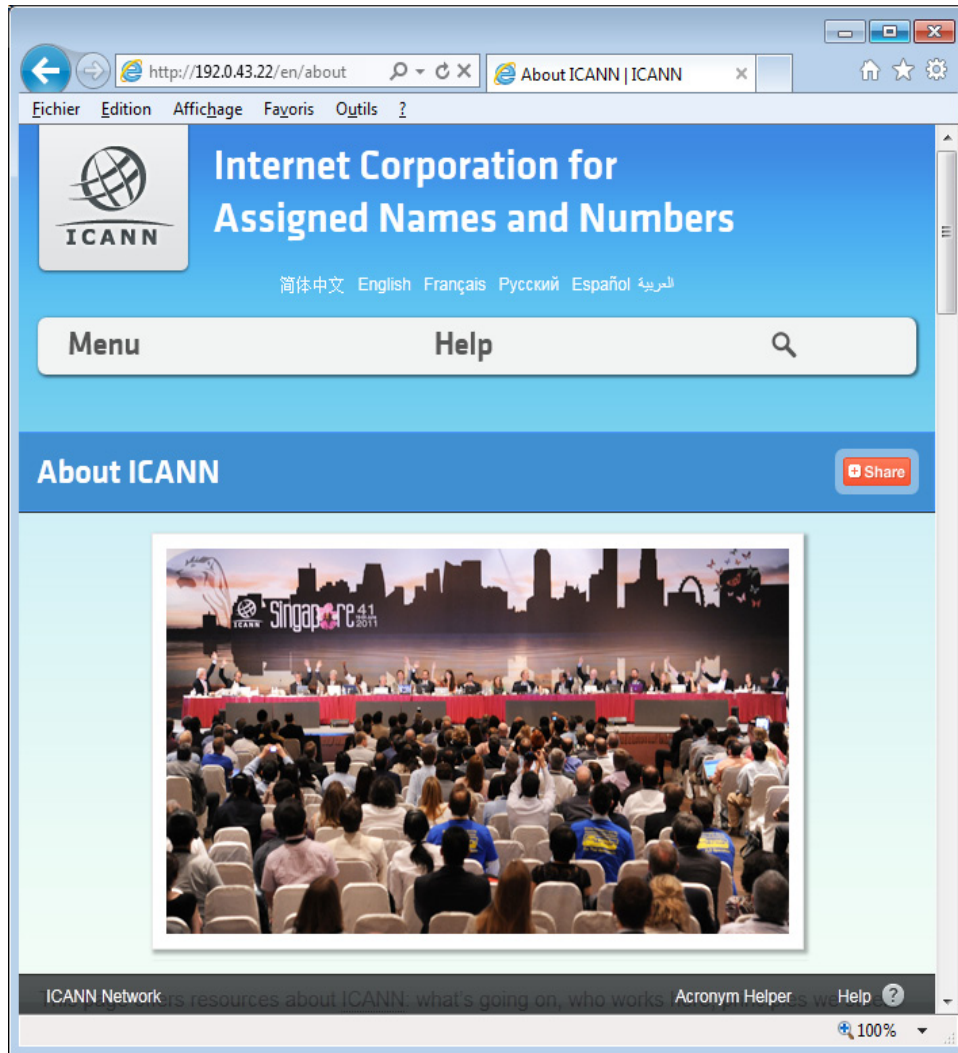
Pinging www.icann.net [192.0.43.22] with 32 bytes of data:
Reply from 192.0.43.22: bytes=32 time=112ms TTL=241
Reply from 192.0.43.22: bytes=32 time=119ms TTL=241
Reply from 192.0.43.22: bytes=32 time=113ms TTL=241
Reply from 192.0.43.22: bytes=32 time=115ms TTL=241

Ping statistics for 192.0.43.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 112ms, Maximum = 119ms, Average = 114ms
```

Enregistrez l'adresse IP www.icann.net. _____

Travaux pratiques – Observation de la résolution DNS

- d. Saisissez l'adresse IP de l'étape c dans un navigateur web à la place de l'URL. Remarquez la page web d'accueil de l'ICANN qui s'affiche.



La plupart des gens ont plus de facilité à mémoriser des mots, plutôt que des chiffres. Si vous dites à quelqu'un de se rendre sur **www.icann.net**, il pourra probablement s'en souvenir. En revanche, si vous lui dites d'accéder à l'adresse 192.0.43.22, il aura plus de mal à se souvenir d'une adresse IP. Les ordinateurs utilisent des chiffres. Le DNS est un processus de traduction des mots en chiffres. Une deuxième traduction a lieu. Les humains pensent aux chiffres en base 10. Les ordinateurs traitent les chiffres en base 2. L'adresse IP en base 10 192.0.43.22 convertie en chiffres en base 2 correspond à 11000000.00000000.00101011.00010110. Que se passe-t-il si vous copiez et collez ces chiffres en base 2 dans un navigateur ?

- e. À présent, saisissez ping www.cisco.com.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.144.170] with 32 bytes of data:
Reply from 23.1.144.170: bytes=32 time=51ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58

Ping statistics for 23.1.144.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 51ms, Average = 50ms
```

- f. Lorsque vous envoyez une commande ping à www.cisco.com, est-ce que vous obtenez la même adresse IP que dans l'exemple ou obtenez-vous une autre adresse IP. Pourquoi ?

- g. Tapez l'adresse IP que vous avez obtenue lorsque vous avez envoyé votre requête ping www.cisco.com à partir d'un navigateur. Le site Web s'affiche-t-il ? Justifiez votre réponse.

2e partie : Observer la recherche DNS à l'aide de la commande Nslookup sur un site Web

- a. À l'invite de commandes, tapez la commande **nslookup**.

```
C:\>nslookup
Default Server:  dslrouter.westell.com
Address:  192.168.1.1
>
```

Quel serveur DNS par défaut est-il utilisé ? _____

Remarquez que l'invite de commandes est devenue un symbole plus grand que (>). Il s'agit de l'invite **nslookup**. Dans cette invite, vous pouvez entrer des commandes liées au système DNS.

À l'invite de commandes, tapez ? pour afficher la liste de toutes les commandes disponibles pouvant être utilisées en mode **nslookup**.

- b. À l'invite **nslookup**, tapez **www.cisco.com**.

```
> www.cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: e144.dscb.akamaiedge.net
Addresses: 2600:1408:7:1:9300::90
           2600:1408:7:1:8000::90
           2600:1408:7:1:9800::90
           23.1.144.170
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

Quelle est l'adresse IP convertie ? _____

Est-ce la même adresse IP que celle affichée avec la commande **ping** ? _____

En dessous des adresses, en plus de l'adresse IP 23.1.144.170, il y a les nombres suivants : 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9800::90. De quoi s'agit-il ?

- c. À l'invite, tapez l'adresse IP du serveur Web Cisco que vous venez de trouver. Vous pouvez utiliser **nslookup** pour obtenir le nom de domaine d'une adresse IP si vous ne connaissez pas l'URL.

```
> 23.1.144.170
Server: dslrouter.westell.com
Address: 192.168.1.1

Name: a23-1-144-170.deploy.akamaitechnologies.com
Address: 23.1.144.170
```

Vous pouvez utiliser l'outil **nslookup** pour convertir les noms de domaines en adresses IP. Vous pouvez également l'utiliser pour convertir les adresses IP en noms de domaine.

À l'aide de l'outil **nslookup**, enregistrez les adresses IP associées à www.google.com.

```
> www.google.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400c:c01::93
           173.194.75.147
           173.194.75.105
           173.194.75.99
           173.194.75.103
           173.194.75.106
           173.194.75.104
```

3e partie : Observer la recherche DNS à l'aide de la commande Nslookup sur des serveurs de messagerie

- a. À l'invite, tapez **set type=mx** afin d'utiliser **nslookup** pour identifier les serveurs de messagerie.

```
> set type=mx
```

- b. À l'invite, tapez **www.cisco.com**.

```
> cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
cisco.com      MX preference = 10, mail exchanger = rcdn-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = alln-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = ams-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = rtp-mx-01.cisco.com

ams-mx-01.cisco.com  internet address = 64.103.36.169
rcdn-mx-01.cisco.com internet address = 72.163.7.166
```

Un principe fondamental en matière de conception de réseau est la redondance (plusieurs serveurs de messagerie doivent être configurés). De cette manière, si l'un des serveurs de messagerie est inaccessible, l'ordinateur envoyant la requête essaie le deuxième serveur de messagerie. Les administrateurs de messagerie électronique déterminent le serveur de messagerie qui est contacté en premier au moyen de **MX preference** (voir l'illustration ci-dessus). Le serveur de messagerie avec la valeur **MX preference** la plus basse est contacté en premier. D'après le résultat ci-dessus, quel serveur de messagerie sera-t-il contacté en premier lorsque des e-mails sont envoyés à cisco.com ?

-
- c. À l'invite de commandes nslookup, tapez **exit** pour revenir à l'invite de commandes normale.
- d. À l'invite de commandes du PC, tapez **ipconfig/all**.
- e. Indiquez les adresses IP de tous les serveurs DNS qu'utilise votre établissement.
-

Remarques générales

Quelle est la principale fonction du service DNS ?
