

Name: Chheang Sovanpanha

Lab - Observe DNS Resolution

Objectives

Part 1: Observe the DNS Conversion of a URL to an IP Address

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

Background / Scenario

The Domain Name System (DNS) is invoked when you type a Uniform Resource Locator (URL), such as **http://www.cisco.com**, into a web browser. The first part of the URL describes which protocol is used. Common protocols are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), and File Transfer Protocol (FTP).

DNS uses the second part of the URL, which in this example is **www.cisco.com**. DNS translates the domain name (**www.cisco.com**) to an IP address to allow the source host to reach the destination server. In this lab, you will observe DNS in action and use the **nslookup** (name server lookup) command to obtain additional DNS information.

Required Resources

1 PC (Windows with internet and command prompt access)

Part 1: Observe the DNS Conversion of a URL to an IP Address

- a. Open a Windows command prompt.
- b. At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org**. ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate **www.icann.org** into an IP address to know where to send the Internet Control Message Protocol (ICMP) packets.

The first line of the output displays **www.icann.org** converted to an IP address by DNS. You should be able to see the effect of DNS, even if your institution has a firewall that prevents pinging, or if the destination server has prevented you from pinging its web server.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.icann.org** to translate into an IPv4 address if desired.

Record the IP addresses for **www.icann.org**.

192.0.32.7

- c. Type the IPv4 addresses from step b into a web browser, instead of the URL. Enter **https://192.0.32.7** in the web browser. If your computer has an IPv6 address you can enter the IPv6 address. **https://[2620:0:2d0:200::7]** in the web browser.
- d. Notice that the ICANN home web page is displayed without using DNS.

Most humans find it easier to remember words, rather than numbers. If you tell someone to go to **www.icann.org**, they can probably remember that. If you told them to go to 192.0.32.7, they would have a difficult time remembering an IP address. Computers process in numbers. DNS is the process of translating words into numbers. Additionally, there is a second translation that takes place. Humans think

in Base 10 numbers. Computers process in Base 2 numbers. The Base 10 IP address 192.0.32.7 in Base 2 numbers is 11000000.00000000.00100000.00000111. What happens if you cut and paste these Base 2 numbers into a browser?

The website does not display anything.

- e. At a command prompt, **ping www.cisco.com**.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.cisco.com** to translate into an IPv4 address if desired.

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

```
C:\> ping -4 www.cisco.com
```

When you ping www.cisco.com, do you get the same IP address as the example? Explain.

Cisco hosts its web content on a series of mirror servers. Cisco uploads the exact same content spread out all over the world servers. When someone tries to reach www.cisco.com, the traffic is directed to the closest mirror server.

Type the IP address that you obtained when you pinged www.cisco.com into a browser. Does the web site display? Explain.

The Cisco web site does not display. There are at least two possible explanations for this: 1. Some web servers are configured to accept IP addresses sent from a browser and some are not. 2. It may be a firewall rule in the Cisco security system that prohibits an IP address from being sent via a browser. Depending on the Web Browser you can also get a message saying the connection is not secure or there is a certificate error.

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

- a. At the command prompt, type the **nslookup** command. Your result will be different than the example.

```
C:\> nslookup
```

What is the default DNS server used?

dns.google and 8.8.8.8

- b. Notice how the command prompt changed to a greater than (>) symbol. This is the **nslookup** prompt. From this prompt, you can enter commands related to DNS.

At the prompt, type **?** to see a list of all the available commands that you can use in **nslookup** mode.

- c. At the nslookup prompt, type **www.cisco.com**.

```
> www.cisco.com
```

```
Default Server:  one.one.one.one
```

```
Address:  1.1.1.1
```

```
Non-authoritative answer:
```

```
Name:      e2867.dsca.akamaiedge.net
```

```
Addresses: 2600:1404:a:395::b33
```

```
           2600:1404:a:38e::b33
```

```
           172.230.155.162
```

```
Aliases:  www.cisco.com
```

```
           www.cisco.com.akadns.net
```

```
           wwds.cisco.com.edgekey.net
```

```
           wwds.cisco.com.edgekey.net.globalredir.akadns.net
```

What is the translated IPv4 address?

96.16.100.137

Note: The IP address from your location will most likely be different because Cisco uses mirrored servers in various locations around the world.

Is it the same as the IP address shown with the **ping** command?

Yes, it is.

Under addresses, in addition to the 172.230.155.162 IP address, there are the following numbers: 2600:1404:a:395::b33 and 2600:1404:a:38e::b33. What are these?

IPv6 address at which the website is reachable.

- d. At the nslookup prompt, type the IP address of the Cisco web server that you just found. You can use **nslookup** to get the domain name of an IP address if you do not know the URL.

```
> 172.230.155.162
```

```
Default Server:  one.one.one.one
```

```
Address:  1.1.1.1
```

```
Name:      a172-230-155-162.deploy.static.akamaitechnologies.com
```

```
Address:  172.230.155.162
```

You can use the **nslookup** tool to translate domain names into IP addresses. You can also use it to translate IP addresses into domain names.

Using the **nslookup** tool, record the IP addresses associated with www.google.com.

The IP address are 2404:6800:4005:801::2004 and 172.217.24.228

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

- a. At the nslookup prompt, type **set type=mx** to use **nslookup** to identify mail servers.

```
> set type=mx
```

- b. At the nslookup prompt, type **cisco.com**.

```
> cisco.com
```

```
Server:  one.one.one.one
```

```
Address:  1.1.1.1
```

```
Non-authoritative answer:
```

```
cisco.com      MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
```

```
cisco.com      MX preference = 30, mail exchanger = aer-mx-01.cisco.com
```

```
cisco.com      MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

A fundamental principle of network design is redundancy (more than one mail server is configured). In this way, if one of the mail servers is unreachable, then the computer making the query tries the second mail server. Email administrators determine which mail server is contacted first by using **MX preference**. The mail server with the lowest **MX preference** is contacted first. Based upon the output above, which mail server will be contacted first when the email is sent to cisco.com?

alln-mx-01.cisco.com

- c. At the nslookup prompt, type **exit** to return to the regular PC command prompt.
- d. At the PC command prompt, type **ipconfig /all**.

Write the IP addresses of all the DNS servers that your school uses.

8.8.8.8 and 1.1.1.1

Reflection Question

What is the fundamental purpose of DNS?

DNS basically acts like the phonebook for the Internet. So DNS translates names to numbers. The numbers can be either IPv4 or IPv6.