Lab - Observing DNS Resolution (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

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 host. In this lab, you will observe DNS in action and use the **nslookup** (name server lookup) command to obtain additional DNS information. Work with a partner to complete this lab.

Required Resources

1 PC (Windows 7, Vista, or XP with Internet and command prompt access)

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

a. Click the **Windows Start** button, type **cmd** into the search field, and press Enter. The command prompt window appears.

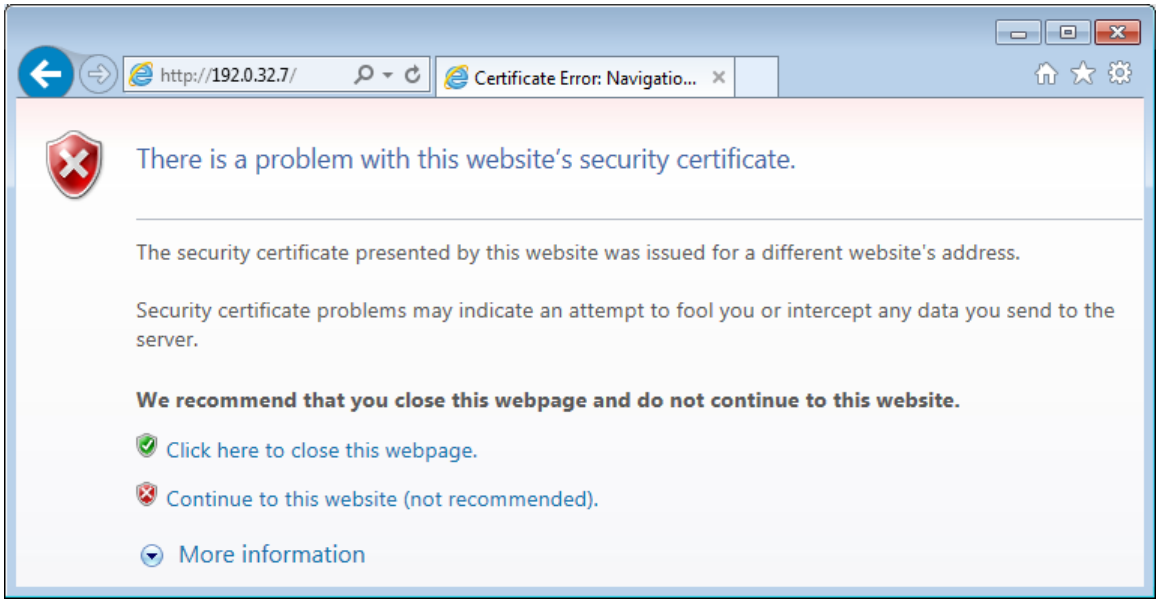
b. At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org**. ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate www.icann.org into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

c. 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.

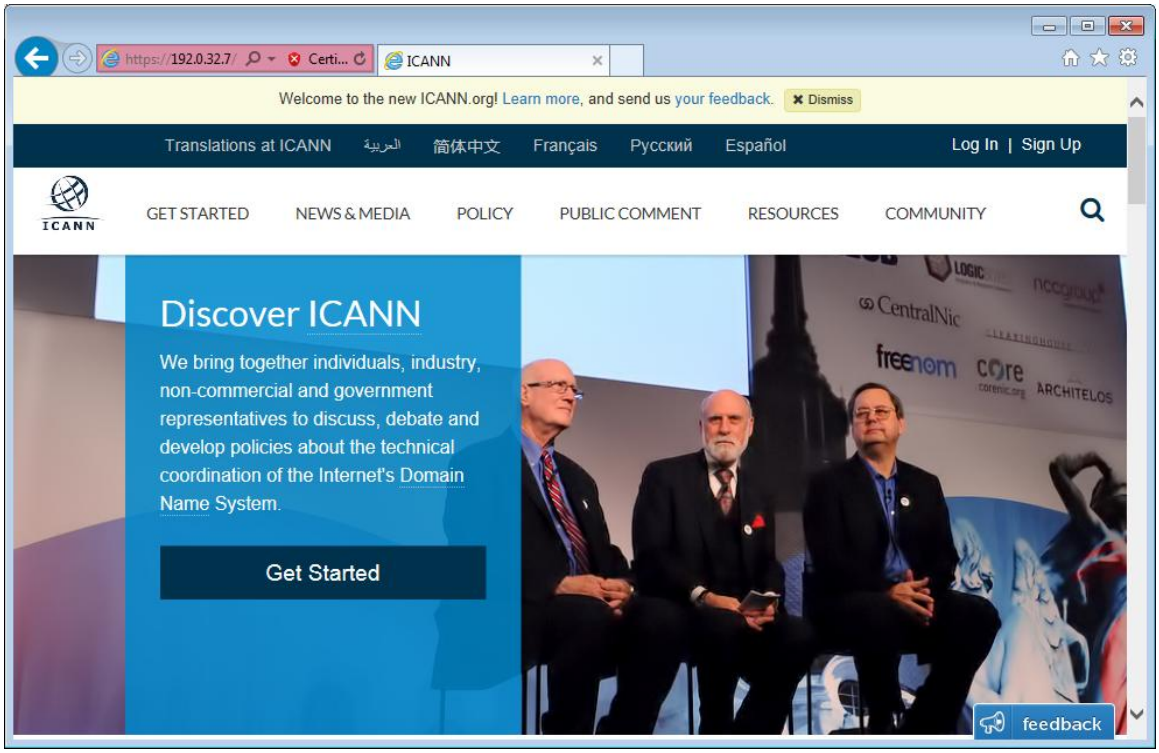
```
C:\>ping www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=24ms TTL=246
Reply from 192.0.32.7: bytes=32 time=28ms TTL=246

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 28ms, Average = 24ms
```

Record the IP address of www.icann.org. _____ 192.0.32.7

d. Type IP address from **step c** into a web browser, instead of the URL. Click **Continue to this website (not recommended).** to proceed.



e. Notice that the ICANN home web page is displayed.



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. 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 web site does not come up. The software code used in web browsers recognizes Base 10 numbers. It does not recognize Base 2 numbers.

f. Now type **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
```

g. When you ping www.cisco.com, do you get the same IP address as the example, or a different IP address, and why?

Answer will vary depending upon where you are geographically. Cisco hosts its web content on a series of mirror servers. This means that Cisco uploads the exact same content to geographically diverse (spread out all over the world) servers. When someone tries to reach www.cisco.com, the traffic is directed to the closest mirror server.

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

The **cisco.com** web site does not come up. There are at least two possible explanations for this: 1. Some web servers are configured to accept IP addresses sent from a browser; some are not. 2. It may be a firewall rule in the Cisco security system that prohibits an IP address being sent via a browser.

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

a. At the command prompt, type the **nslookup** command.

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

>
```

What is the default DNS server used? _____

Site dependent

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.

b. At the **nslookup** prompt, type **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
```

What is the translated IP address? _____

From a specific location, 23.1.144.170. 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

Under addresses, in addition to the 23.1.144.170 IP address, there are the following numbers: 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9800::90. What are these?

_____

IPv6, or IP version 6, IP addresses at which the web site is reachable.

c. At the 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.

```
> 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
```

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.

_____

Answer may vary. At the time of writing, the IP addresses are 173.194.75.147, 173.194.75.105, 173.194.75.99, 173.194.75.103, 173.194.75.106, 173.194.75.104.

```
> 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
```

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

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

```
> set type=mx
```

b. At the prompt, type **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
```

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 using **MX preference** (see above image). The mail server with the lowest **MX preference** is contacted first. Based upon the output above, which mail server will be contacted first when email is being sent to cisco.com?

_____

rcdn-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**.

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

_____

Site-dependent

Reflection

What is the fundamental purpose of DNS?

_____

_____

_____

People process in words. Computers process in numbers. People have a difficult time remembering a long string of numbers. Therefore, DNS exists to translate the “numbers” world of computers to the “word” world of people.