CSIS 330 – Lab 11:

This lab is in two phases:

Phase 1: Troubleshooting–

OS Command Line Tools

*[Part I is adapted from Network Fundamentals CCNA Exploration Labs and Study Guide, by Rufi, Oppenheimer, Woodward, and Brady]*

**Background:**

**Netstat**: (<http://technet.microsoft.com/en-us/library/bb490947.aspx> )

The Netstat command (Network statistics utility) shows incoming and outgoing connections for TCP and UDP, host computer routing table information, and interface statistics. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, **netstat** displays active TCP connections.

**Ping:** (<http://en.wikipedia.org/wiki/Ping_%28networking_utility%29>)

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Ping operates by sending Internet Control Message Protocol (ICMP) *echo request* packets to the target host and waiting for an ICMP response. In the process, it measures the time from transmission to reception (*round-trip time*) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

**TRACERT:** (<http://support.microsoft.com/kb/162326>)

The TRACERT diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router should send an ICMP Time Exceeded message back to the source computer.   
  
TRACERT determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Note that some routers silently drop packets with expired TTLs and are invisible to TRACERT.   
  
TRACERT prints out an ordered list of the routers in the path that returned the ICMP Time Exceeded message.

**Ipconfig:** (<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ipconfig.mspx?mfr=true> )

**Ipconfig** displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for all adapters.

**Assignment Instructions:**

*[A Word template is provided for your answers and screen shots.]*

**Part I: Netstat Syntax**

Open a command prompt and type in the netstat command and its help functionality as follows:

**C:\> netstat /?**

Using the information displayed, fill in the table below:

|  |  |
| --- | --- |
| Command | Description |
| Example:  netstat -a | Displays all connections and listening ports |
|  | Displays addresses and port numbers in numeric form |
|  | Redisplays statistics every 5 second. Press Ctrl-C to stop redisplaying statistics. |
|  | Shows connections for the TCP protocol |
|  | Displays fully qualified domain names for foreign addresses. |
|  | Displays the routing table. |

**Part II: Netstat Routing Table**

Using netstat, display your routing table. Expand your screen such that only the **IPv4** routing table is shown. **Take a screen shot of this table and paste it in the appropriate section (Screenshot #1) of the Answer Template provided.**

**Answer the following question in the Answer template.**

Question #1: What does this table show you? Be specific. [Hint: Page 302 in your textbook provides some useful information.]

**Part III Netstat Output**

At the command prompt, type in the following:

**C:\>netstat -s -p tcp -f**

**Take a screen shot of the top section of your output and paste it in the appropriate section (Screenshot #2) of the Answer Template provided.**

Given your screen shot in Part IV above, answer the following questions:

1. How many active opens were recorded?
2. How many failed connection attempts were recorded?
3. How many segments were received?
4. How many segments were sent?
5. How many segments were retransmitted?

**Part IV: IPCONFIG**

At the command prompt, type IPCONFIG. **Take a screen shot of your output and paste it in the appropriate section (Screenshot #3) of the Answer Template provided.**

. **Answer the following questions in the template:**

1. What is your IPv4 address?
2. What is your subnet mask?
3. What is your default gateway address?

**Part V: PING**

At the command prompt, type

**ping 127.0.0.1**

**Take a screen shot of your output and paste it in the appropriate section (Screenshot #4) of the Answer Template provided and answer the following questions in the template:**

1. Were you able to ping this address?
2. How do you know?
3. How many packets were sent?
4. How many packets were received?
5. How many packets were lost?

The IP address 127.0.0.1 is called a loopback address. A loopback address is an IP address that refers to your own computer. It can be used to test if your TCP/IP configuration is working properly. You will learn about this in Chapter 8.

**Part VI: TRACERT**

At the command prompt, type

**tracert 127.0.0.1**

**Take a screen shot of your output and paste it in the appropriate section (Screenshot #5) of the Answer Template provided and answer the following questions in the template:**

1. Was the trace successful?
2. If the trace was successful, how many hops were performed to reach the destination?

**Deliverables:**

Save your Answer Template using the convention of [your first initial] + [your last name] + “\_Lab11”.

For example: Joe Smith will save his file template as JSmith\_Lab11A.doc .

Submit your **Answer Template** to Blackboard by attaching it to the appropriate assignment link.

Phase 2: Packet Tracer

Network Representations (DNS and HTTP)

*[Activity from Cisco Networking Academy Lab Packet Tracer Activity 3.3.2 ]*

**This entire exercise comes from the Cisco Networking Academy.**

**Background:**

This Packet Tracer is a pre-programmed activity that includes embedded instructions as well as a partially built topology. Using the instructions that are embedded in the Packet Tracer, you will configure a Server to provide DNS services and to host a web page, configure a PC to use DNS services, and view how DNS and HTTP work together.

Because this Packet Tracer activity is part of the Cisco Networking Academy’s curriculum, there are differences between the point values reflected in the instructions and the actual points you can earn for this assignment in this class. Refer to the rubric in Blackboard for the number of points allocated to each task in this lab.

**Assignment Instructions:**

**Task 1: Configure Services and Support.**

To complete this part of the lab, refer to the instructions that are embedded within the Packet Tracer file for Task 1.

**When you have completed the configurations in this assignment, save your Packet Tracer file using the naming convention used for this class:**

[your first initial + your last name] + “\_Lab11b” (do not include the quotation marks)

For example, Joe Smith will save his file for this lab using the filename “JSmith\_Lab11b”.

**Tasks 2-3:**

Tasks 2 and 3 of the embedded instructions require you to perform activities in Packet Tracer that can only be graded by submitting screen shots of your results and answers to questions. To help you to know when to take screen shots, Tasks 2 and 3 are reproduced below with instructions regarding what screens to capture.

***[A Word template is also provided for your answers and screen shots.]***

**Task 2: Verify Connectivity in Realtime Mode**

**Step 1. Ping the server using the URL.**

Select the PC and click the **Desktop** tab. Click the **Command Prompt**button. A Command Prompt window opens. Type **ping www.example.com** (the URL of the Server) and press **Enter**.

**Take a screen shot of your output and paste it into the appropriate section (Screenshot #1) of the Word Answer Template provided.**

After the ping succeeds, close the Command Prompt window.

**Step 2. From the PC, Open a Web Page.**

From the PC desktop, click the **Web Browser** button. A simulated web browser opens. Type **www.example.com** (the URL of the Server) into the **URL** box and click the **Go** button. A web page should appear.

**Take a screen shot of your output and paste it into the appropriate section (Screenshot #2) of the Word Answer Template provided.**

Close the PC configuration window.

**Task 3: View how DNS and HTTP work Together using Simulation Mode**

**Step 1. From the PC, ping the Server using the URL**  
**Enter Simulation mode**. Click the PC Client. The PC configuration window opens. Click the **Desktop** tab. Click the **Command Prompt**button. A Command Prompt window opens. Type **ping www.example.com** (the URL of the Server) and press **Enter**. Minimize the simulated Command Prompt window. Use **Capture/Forward** to view the DNS and ICMP packets on the network. Each time you click the **Capture/Forward** button, the packet transfer process will proceed. During this process, you can click the colored square in the **Info** column to open the PDU information and view encapsulation and device processing details.

**Click the colored square in the Info column beside the SECOND PDU. (It should be a DNS PDU). Take a screen shot of the PDU information tab and paste it into the appropriate section (Screenshot #3) of the Word Answer Template provided.**

Close the Command Prompt window; click the**Reset Simulation** button.

**Step 2. From the PC, open a web page on the Server using the URL**

Click the **Web Browser** button. A simulated web browser opens. Type **www.example.com** (the URL of the Server) into the **URL** box and click the **Go** button. Minimize the simulated browser window. Use **Capture/Forward** to examine the DNS and HTTP packets. For each packet in the event list, click the colored square in the **Info** column to open the PDU information and view encapsulation and device processing details.

**Click the colored square in the Info column beside the LAST PDU. (It should be an HTTP PDU). Take a screen shot of the PDU information tab and paste it into the appropriate section (Screenshot #4) of the Word Answer Template provided.**

**Final Step: Save your Template**

Save your Answer Template using the convention of [your first initial] + [your last name] + “\_Lab11B”.

For example: Joe Smith will save his file template as JSmith\_Lab11B.doc .

**Deliverables**: **Submit your assignment by attaching your Packet Tracer file and your Answer Template to the appropriate assignment link in Blackboard. Both files must be uploaded to receive full credit for this assignment.**