Ifconfig Lab 1: Network & Protocols

Intro IT & Web Science - ITWS 1100

The purpose of this lab is to get you familiar with some basic networking concepts, protocols, and tools. We will start the lab in class. Please enter your answers in this document and save it as "Lab1-*YourFullName.docx*". It is due in the Assignment area by EoD on the next class-day.

1. **Basic Network Information**
   For the following exercises, open a "Command Prompt" console window on your laptop, enter each command as shown on the command line, and answer the questions provided. To copy from the Command Console, block text with your mouse and right-click or hit enter. (If you cannot block text directly, right-click and select "Mark" first). If you are using Linux/Unix/OS X, perform the equivalent command (shown in parentheses) in a terminal window.
   Hint: Read about Netstat (you can also search this site for other info ie ipconfig) for Windows here:
   https://technet.microsoft.com/en-us/library/bb490947.aspx
   Hint: Mac info is here:
   https://developer.apple.com/library/archive/documentation/System/Conceptual/ManPages_iPhoneOS/man3/getifaddrs.3.html
   Hint: If you are having issues retrieving IPv6 or v4 info from the commands – look up the options for ipconfig, etc

   a. **ipconfig /all** (Windows)
   ifconfig –a and **scutil --dns**, and **netstat -nr | grep default** (Mac)
   (Also on Mac – AppleMenu->About->MoreInfo->System report, ifconfig en1)
   (can also type hostname from the command line –mac/linux)

   For your LAN Ethernet adapter and your general IP configuration:
   i. What is your hostname? *DESKTOP-J3JJH90*
   ii. What is your MAC address? *00-05-9A-3C-7A-00*
   iii. Who is the vendor of your Ethernet adapter? *Cisco AnyConnect Secure Mobility Client*
   iv. What is your IPv4 address? *128.213.71.26*
   v. What is your IPv6 address? *fe80::3daa:e099:4e2e:1961%15*
   vi. What are the IP (v4) addresses of your DNS servers? *128.113.11.73, 128.113.26.250*
   vii. What is the IP (v4) address of your default gateway *N/A*

   b. **netstat –f** (netstat –f inet)
   i. What kind of transport layer protocols are in use? *TCP, UDP*
   ii. What kind of application layer protocols are in use? *http, https*

   c. **netstat –b** (netstat –b –f inet)
   i. What applications are using your network ports, and what application layer protocol are they using? (only name up to three) *(Discord.exe, https), (SearchApp.exe, http), (chrome.exe, https)*

d. **nslookup 192.0.32.10**

nslookup it allows you to look up IPs or hostnames against a name server (by default, the first DNS server configured in your network settings).

i. Upon running "nslookup 192.0.32.10", what is the host name of the name server you are using *reliance.net.rpi.edu*

ii. What name is associated with 192.0.32.10? What is the significance of this name? *ccnso.icann.org, It is significant because it is the website of the committee that decides which country gets which domain extension (USA -> .us, UK -> .uk, etc.)*

iii. Perform a "netstat –n" in your console (this tells netstat not to resolve names against the name server – notice that it's quicker). Do an nslookup on a foreign IP from your netstat results. What name did you uncover? (If the DNS server can't resolve the IP you picked, try another one.) *Uncovered 53.16.211.130.bc.googleusercontent.com.*

iv. Do an "nslookup 127.0.0.1". What name is returned? What is the significance of this name? *localhost. That is me.*

v. What is the IP address of lms.rpi.edu? *34.235.253.173*

vi. What is the IP address of www.rpi.edu? Is it IPv4 or IPv6? *2620:0:2820:4::2 it is IPv6*.

e. **tracert www.ucla.edu** (traceroute www.ucla.edu)

i. How many hops did it take for you to reach www.ucla.edu? *27 hops*

ii. From the tracert you just ran, locate an IPv4 address of a router along the path. Visit http://www.iplocation.net/ and enter the IPv4 address. Were you able to determine the router's location? If so, where is it? *99.82.176.74, (Ashburn, Virginia)*

iii. Enter your own IPv4 address in the website. What did you learn? *Based in Albany/Troy, ISP is Rensselaer Polytechnic Institute*

2. SSH to RCS-Linux

For this exercise you are going to create a terminal session onto another computer and run some network commands there.

Read up on

- SSH: https://www.ssh.com/ssh/protocol/
- And how to use it on Windows; Here or here.
- On Mac or Unix you can use the normal terminal

If you are off-campus, you will need the VPN active on your computers; While it should be pre-loaded on your laptops from RPI already, you can find out more about it here https://itssc.rpi.edu/hc/en-us/articles/360008783172-VPN-Installation-and-Connection

Use SSH to *yourRCSid*@**rcs-linux.rpi.edu** (for those on Linux/Unix/OS X, ssh directly from your terminal). Log in with your RCS ID and password. You will arrive in your Rensselaer Computing System (RCS) home directory.

NOTE: If you are off-campus, you must connect to RPI's VPN (Virtual Private Network) to access rcs-linux.rpi.edu. This is accomplished by running a VPN client on your system such as the "Cisco AnyConnect VPN client" which is likely installed on your laptop already. For instructions on how to get the VPN client and information about VPN access, please see: http://helpdesk.rpi.edu/update.do?artcenterkey=556

a. **netstat -e**
   i. What transport layer protocols do you see in use? *tcp, tcp6, udp*
   ii. What application layer protocols do you see in use? *net, rpi, edu, nete, ldaps*

b. **host www.rpi.edu**
   i. What IPv4 addresses are used by www.rpi.edu? *128.113.0.2*

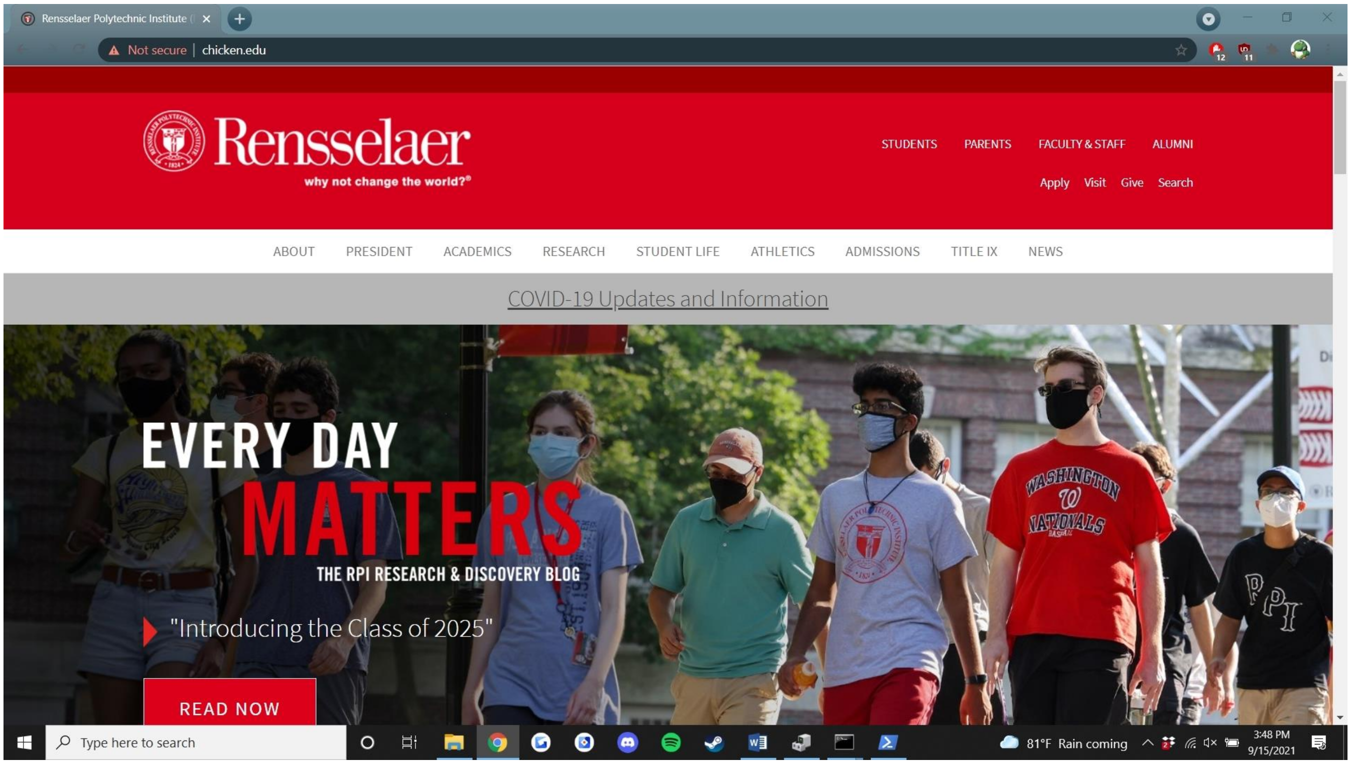
c. **traceroute www.google.com**
   i. How many hops did it take to get to Google? *9 hops*

d. In your Windows Command Prompt console use netstat (as in section 1.b) to find your current SSH connection. Mac users : Use command **who -a** as well as **netstat**

   Copy the netstat line showing the SSH connection to here.

   TCP [2620:0:2820:bc::3c7]:61622 rmtacc-r7b.rcs.rpi.edu:ssh ESTABLISHED

3. **Overriding DNS**
   Your machine has a local "hosts" file that maps IP addresses to host names and can be used to override DNS. (On some browsers, esp Chrome – the DNS information can be cached. Before and after this exercise, you should go into your browser's settings and empty your cache.)
   a. Use jEdit, notepad or some other text editor to edit your hosts file: C:\Windows\System32\drivers\etc\hosts (/etc/hosts on linux/unix). Using the examples in the comments at the top of the hosts file as a guide, give www.rpi.edu a new host name – you can use any IP address of www.rpi.edu for this exercise (you need only one IP).
   b. Visit the new hostname in your browser and capture a screenshot of the browser window. (CTRL-SHIFT-ALT PrntScrn)
   c. Paste the screenshot here.



d. (I'd encourage you to now return your hosts file to its original state. Then clear your Browser's cache).)

4. Do one of the following – or both if you're bored.

a. **(OPTION A – For those who are like – "I love this networking stuff") Take a look at some packets**
Download and install WireShark: http://www.wireshark.org/download.html
There are ports of this for most OSes – if you're not running Windows or Mac, scroll down on the Download page and look to the right. *(Note: I encourage you to run this only against your own machines. Also note that activities such as port scanning against RPI network devices will be noticed…)*

i. Run WireShark and select "Capture Options, start a capture with detailed options".

(1) Set the Capture Filter to "tcp port 80" (or "tcp port http")

(2) Set "Stop Capture after **4** packets"

(3) Click "start"

ii. In your browser, visit http://rpi.edu/

(1) Looking back at the WireShark output, look for the TCP three-way handshake.

iii. How are the SYN and ACK flags represented in the TCP header? (Feel free to investigate http://en.wikipedia.org/wiki/Transmission_Control_Protocol as well.)

iv. Look at the HTTP Request header. Copy your user-agent here (right-click to copy).

b. **(OPTION B – For those who are like – "I kind of get this, but are we there yet?"**

i. Explain in a Paragraph or two what this lab was trying to show and explain – in English – in detail, your own words, and proper grammar, answers to the following 3 questions

(1) What is the significance of the data we retrieved in #1?

The significance of the data retrieved in #1 of this lab is that it defines our PCs connection to the internet. Each of the different fields we were asked to retrieve: IPv4, IPv6, hostname, traceroute, etc. describes how our PC is uniquely identified when browsing the web and how our PC sees what it is connected to.

(2) What application protocol did you find and what is it? Why was it on the output?

The application layer protocol that I found was the Hypertext Transfer Protocol, or HTTP. It is a set of standards that allows internet users to exchange website information between one another. It was on the output because it was being used to describe what application protocol a particular TCP connection was using.

(3) What is happening when we override the DNS?

When we override the DNS, we tell our computers to go to an IP address that we designate instead of the default IP address when going to a site. For example, if we want to go to www.google.com**,** instead of using that address, we can change it to something else, like www.montanachicken.com. Then, when we go to that IP, our computer looks to see if it set to a different overridden IP, and goes to that site, while maintaining our new, changed IP address. So, when we go to www.montanachicken.com in this example, our computer checks the hosts file, and will instead go to google.com, but will display the IP address being used, www.montanachicken.com.