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/mac/documentation/Darwin/Reference/ManPages/man8/ifconfig.8.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** (ifconfig –a) (Also on Mac – AppleMenu->About->MoreInfo->System report, ifconfig en1) (also type hostname form the command line –mac/linux)
      For your LAN Ethernet adapter and your general IP configuration:
      i. What is your hostname?
         DESKTOP-CFRKK7D
      ii. What is your MAC address?
         F8-59-71-7D-43-08

      iii. Who is the vendor of your Ethernet adapter?

         Intel(R) Ethernet Connection (4) I219-LM

      iv. What is your IPv4 address?

         129.161.49.23

      v. What is your IPv6 address?

         2620:0:2820:d04:80f9:9af:36fd:28e3

      vi. What are the IP (v4) addresses of your DNS servers?

         128.113.28.67

         128.113.26.77

      vii. What is the IP (v4) address of your default gateway

         129.161.49.254

b. **netstat –f** (netstat –f inet)

    i.   What kind of transport layer protocols are in use?

        TCP

    ii.   What kind of application layer protocols are in use?

        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)
Ffffffff

        Dropbox.exe, TCP

        Skype.exe, TCP

        chrome.exe, TCP

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

        dns4.net.rpi.edu

    ii.   What name is associated with 192.0.32.10? What is the significance of this name?

        ccnso.icann.org

        Country Code Names Supporting Organisation

    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.)

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

        localhost

        local machine

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

        128.113.0.1

    vi. What is the IP address of www.rpi.edu? Is it IPv4 or IPv6?

2620:0:2820:4::2, IPv6
128.113.0.2, IPv4

e. **tracert www.ucla.edu** (traceroute www.ucla.edu)
   i. How many hops did it take for you to reach www.ucla.edu?

   20

   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?

   No IPv4 address

   iii. Enter your own IPv4 address in the website. What did you learn?

   It gives the location of the IP address, even including latitude and longitude.

2. **SSH to RCS-Linux**
   For the next exercise, use PuTTy to 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

      ii. What application layer protocols do you see in use?

      TCP

   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?
         30
   d. In your Windows Command Prompt console use netstat (as in section 1.b) to find your current SSH
      connection.   Copy the netstat line showing the SSH connection to here.

      Mac users : Use command who –a

TCP   [2620:0:2820:2206:80f9:9af:36fd:28e3]:61675 rcs: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. *(OPTIONAL: not really, but not for credit) 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…)*

   a. Run WireShark and select "Capture Options, start a capture with detailed options".
      i. Set the Capture Filter to "tcp port 80" (or "tcp port http")
      ii. Set "Stop Capture after **4** packets"
      iii. Click "start"

   b. In your browser, visit http://m.rpi.edu/i/

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

         0x012

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

   ===

   HTTP/Requests:

Topic / Item Burst start	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate
--							
HTTP Requests by HTTP Host 0						100%	-

---rev2015-09-------------
-