Lab 2: HTTP and DNS

HTTP Section:

In this first part of the lab we are going to have you examine some HTTP traffic using wireshark. To do this you will have to make use of the **Windows machines in BE301A.** Close all tabs (except the one you may be using to read this document) or programs that may create "noise" on the windows machine. Open wireshark and begin listening to traffic on Local Area Network. Using Firefox go to *"www.example.com"* . Set the display filter to only show HTTP packets.

1. **[5pts] What was the IP address of the "www.example.com" web server and what port number was the web server located on?**
2. **[5pts] What is a "Request URI"?**
3. **[5pts] What version(s) of HTTP is the server using? How do you know?**
4. **[10pts] Open another application on the Windows machine while capturing packets. Without filters added, what do you see this application doing? What evidence is given that this application is responsible for the traffic. Include the summary of the packet exchanges in your report.**

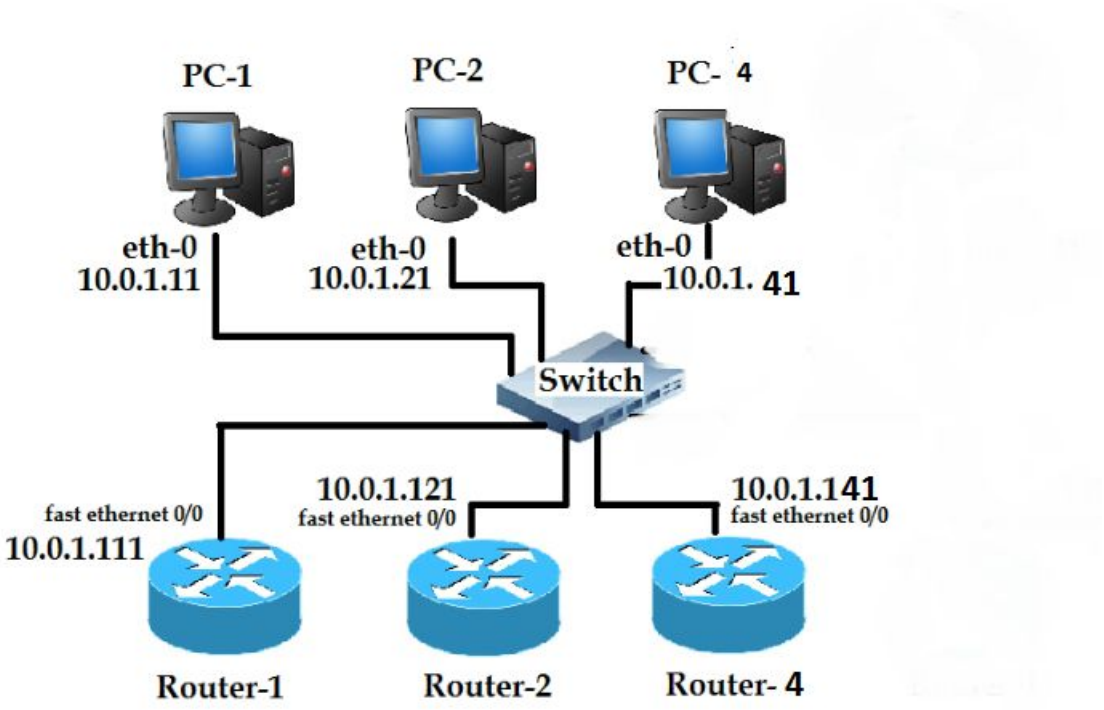
Now clear or restart your Wireshark capture, and travel to "http://www.soe.ucsc.edu". Ignore everything after the initial request.

5. **[10pts] What status code was returned in response to the initial request to "www.example.com"? What about when "www.soe.ucsc.edu" was requested?**

Again clear or restart your wireshark capture and now travel to "https://my.ucsc.edu". Filter your packets in Wireshark by "ssl".

6. **[5pts] What is the IP address and port number of the my.ucsc.edu web server?**
7. **[5pts] What is different about the 'payload' (the contents of the packet), from those of the example.com packet?**

DNS Section (part 1):



We will now switch over to using the **Linux PODS in BE301A.** In this part of the lab you will get a hands-on view of name resolution done by a DNS server on one of your 3 linux machines. Start by restarting any PCs or routers already on - we don't want to load bad settings, toggle the on/off switch for routers, wait a second before turning back on. Next we will be setting up the topology in the figure above and setting the IP addresses for the Linux PCs.

Reminders: that the PCs on the patch panel are label 1/0, 1/1, 2/0, etc. The first number indicates the PC number, and the second number indicates the device number (so 1/0 is PC1 eth0). Use the yellow ethernet cables to connect the PCs to the Switch, and the Router's fastEthernet port to the switch as well.

Remember the notation for setting IPs is:

ifconfig eth0 10.0.1.X/24 **(replace X with the corresponding number in the diagram)**

To configure the routers we also need to connect the PC's console port labeled **console** on the patch panel with values 1-4 for each PC to the **console** port on the routers. Note it is probably easier to use 3 PCs to configure 3 Routers, with each PC setting up the below instructions.

Configuring the routers is slightly more difficult. Type each command listed in below beginning with Router 1.

1. Open a terminal on the Linux PC.
2. run the command: *kermit*
3. enter: *set line /dev/ttyS0* followed by return.
4. enter: *set carrier-watch off* followed by return
5. finally enter: *connect*

You should now be prompted with a "**Router >**" symbol. If the router prompts you with a "**rommon >**" prompt, type "reset" and wait for the router to reboot.

6. Now that we are logged in, we need to configure the router, so we need to get into a privileged mode, we do this with the command *enable*

Enable is used to change your permissions from user-level to a root-level access.

7. Enter the password on whiteboard. Then type out each command below
8. *configure terminal*
9. *interface fastEthernet0/0* (make sure you plugged in your cables to the correct port to the router labeled fastEthernet0/0.)
10. *ip address 10.0.1.X 255.255.255.0* (replace X with the corresponding value of the router 111, 121,141)
11. *no shutdown*
12. *end*
13. Then do the same For Routers 2&4.

Now we will begin Configuring the DNS server to do name resolution. All the PCs will have domain names in the form "PC#.mylab.com" where # is the PC number. Also these two things need to be done in advance:

1. Make sure that "*/etc/resolv.conf*" is empty.
2. Make sure the process "*named*" is stopped. (using *ps* and *kill* or *killall* - recall prelab 1)

Then run the following on each PC to specify a domain name given. Go to the PC's "*namedpackage"* directory in the home directory and run these 2 commands.

1. *chmod 755 named-installPC#* (# being the correct PC number)
2. *./named-installPC#* (# being the correct PC number)

On PC1&2 run the following commands so that PC 4 (10.0.1.41) will be used as the network's DNS server:

1. Change the line “hosts: files dns” in /etc/nsswitch.conf to “hosts: dns files”
2. Create /etc/resolv.conf with line “nameserver 10.0.1.41”
3. Verify /etc/hosts contains “127.0.0.1 localhost.localdomain localhost”
4. Now re-configure all the PC ip addresses using *ifconfig* just as before. If you did so earlier it will not affect the configuration.

On PC4 we will start the DNS server by running the following commands:

1. *cp /etc/named-part3.conf /etc/named.conf*
2. */etc/rc.d/init.d/named start*

Research what the command “host” does and run the following:

On PC4:

1. host –v PC2.mylab.com
2. host –v 10.0.1.21
3. host –v localhost
4. host –v tcpip-lab.net

On PC1:

5. host –v PC4.mylab.com
6. host –v 10.0.1.21
7. host –v localhost
8. host –v tcpip-lab.net

1. **[50 pts] List and explain the output of the host –v commands run on PC4 & PC1. Which names were resolved?**

Next, we will examine the exchange of DNS messages between DNS resolvers and DNS servers. Connect another Ethernet cable to PC 1 labelled 1/1 on the patch panel to port 23 of the switch, type in a new terminal run *ifconfig eth1 up* to turn on eth1, and start a Wireshark capture on eth1. **Make sure MAC name resolution, network name resolution, and transport name resolution are disabled.** Run these 4 ping commands and answer the questions below.

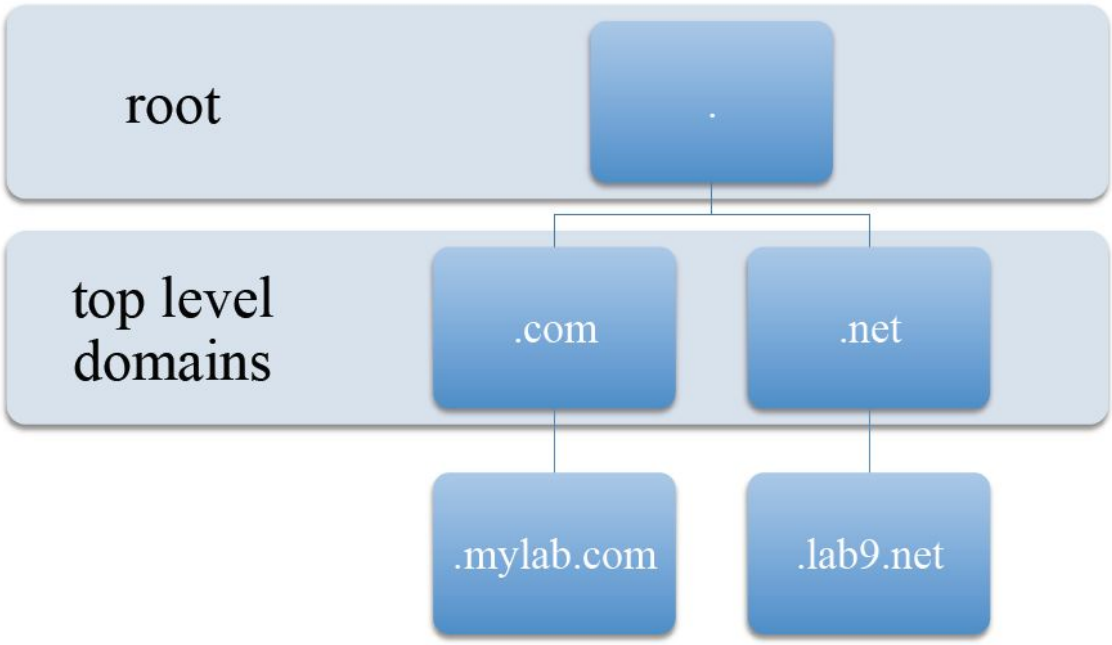
- ➔ ping –c 3 PC4.mylab.com
- ➔ ping –c 3 localhost
- ➔ ping –c 3 tcpip-lab.net
- ➔ ping –c 3 PC4.mylab.com (do so within a few minutes of #1)

Questions:

2. **[10 pts] Did all 4 ping commands generate a DNS message?**
3. **[20 pts] What happens if a DNS query that cannot be resolved is issued? Were all of the queries in the trace resolved?**
4. **[10 pts] When you repeated the ping to PC4, did PC1 issue another DNS request or was the previous response cached?**

DNS Section (part 2):

In real life, a single name server will not maintain entries for all addresses. DNS was designed to be a distributed system, and in this part we will see how multiple name servers interact to lookup and share address mappings. We will use the following hierarchy:



We will use the following assignment of IP addresses to domain names:

Linux PC	**IP Address**	**Domains**	**Domain Server for DNS Zones**
PC1	10.0.1.11	root-server.net	.
PC2	10.0.1.21	top-server.com	.com
PC3	10.0.1.31	top-server.net	.net lab8.net
PC4	10.0.1.41	nameserver.mylab.com	mylab.com
Router	**IP Address**	**Domain Names**	**Name Server**
Router1	10.0.1.111	R1.mylab.com	PC4 – 10.0.1.41
Router2	10.0.1.121	R2.mylab.com	PC4 – 10.0.1.41
Router3	10.0.1.131	R3.lab9.net	PC3 – 10.0.1.31
Router4	10.0.1.141	Router4.com	PC2 – 10.0.1.21

To configure this setup we first need to clean up what was done by the previous exercise. Comment/delete all lines in "*/etc/hosts*" & "/etc/resolv.conf". Then copy "*/etc/named-part6.conf*" to "*/etc/named.conf*" and restart the "*named*" process.

Now we need to again re-configure the routers by giving them a name server, on each router please run the following commands

1. *enable*
2. *configure terminal*
3. *ip name-server ip_address_of_nameserver* (see table above for each router)
4. *ip domain-lookup*
5. *end*
6. *show hosts*
7. *clear host **

We are now ready to examine how DNS queries are resolved in a hierarchical system. On PC1, make sure that eth1 is up and has been wired to port 23 of the switch (Verify your topology is correct). Start a wireshark session listening on eth1. Run the following ping commands from the routers:

On Router 1:

1. ping R2.mylab.com
2. ping R3.lab9.net
3. ping Router4.com

On Router 3:

4. ping R1.mylab.com
5. ping Router4.com
6. ping root-server.net

On Router 4:

7. ping R3.lab9.net

Kill the root name server on PC1. (service named stop)
Restart the nameserver on PC4. (service named restart)

On Router 2:

8. ping R3.lab9.net

1. [40 pts] For each command, explain how the observed DNS queries are resolved.
2. [10 pts] Which queries have the recursion-desired flag set?
3. [5 pts] List the authoritative servers for the .net and .com domains.
4. [10 pts] Do you observe recursive or iterative DNS queries, or both?

Reset all routers with the "reload" command. Do NOT save modified config!!!
Remember to save all your files from the PCs onto a flash drive, then please shutdown!