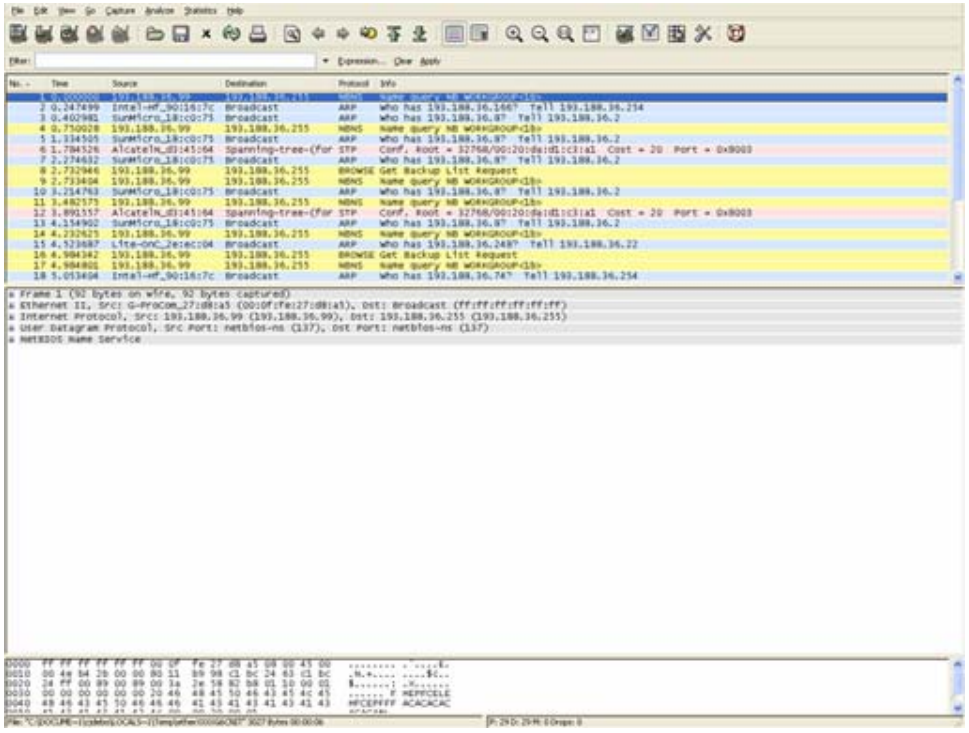
University of Malta
Department of Communications and Computer Engineering

Laboratory session 1: Using Ethereal to monitor a computer network

Name: _____
Date: _____

Objective: In this experiment you will learn how to use Ethereal, understand how name servers manage domain name information, and view port access.

Experiment 1: Familiarization with Ethereal



Ethereal has four major components:

1. The **command menus** are standard pulldown menus located at the top of the window. The menus that are important in this experiment are the File and Capture menus. The File menu will allow saving of captured packet data or

opening of a file containing previously captured packet data. From the Capture menu you will begin packet capture.

2. Inside the **packet-listing window** a one line summary for each packet captured, including the packet number, the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet, can be viewed. The protocol type field lists the highest level protocol that sent or received this packet.
3. The **packet-header details window** provides the details about the packet selected inside the packet listing window. The details displayed include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer details that will be displayed can be expanded or minimized as needed. If the packet has been carried over TCP or UDP, the protocol details will also be displayed. Finally, the details about the highest level protocol that sent or received this packet are also provided.
4. The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

To start the capturing of packets select the Capture pulldown menu and click on interfaces. In the new window you will see the possible network interfaces, click on the capture button of the interface showing a valid IP address. Leave running for 2 minutes and note the percentages of the type of packets captured. Click on stop and view the captured packets in the packet-listing window. Click on a few of the packets and view the details in the packet-header details window.

Experiment 2: HTTP

1. Start the Microsoft Explorer web browser.
2. Start Ethereal packet sniffer.
3. Enter http in the filter specification window. This will ensure that only http packets will be displayed.
4. Start Ethereal packet capture.
5. Enter the following in your browser: http://www.eng.um.edu.mt
6. Stop Ethereal packet capture.

The packet-listing window should contain the GET message from the browser to the server and the response message from the server to the browser. The detailed messages can be viewed in the packet-header details window.

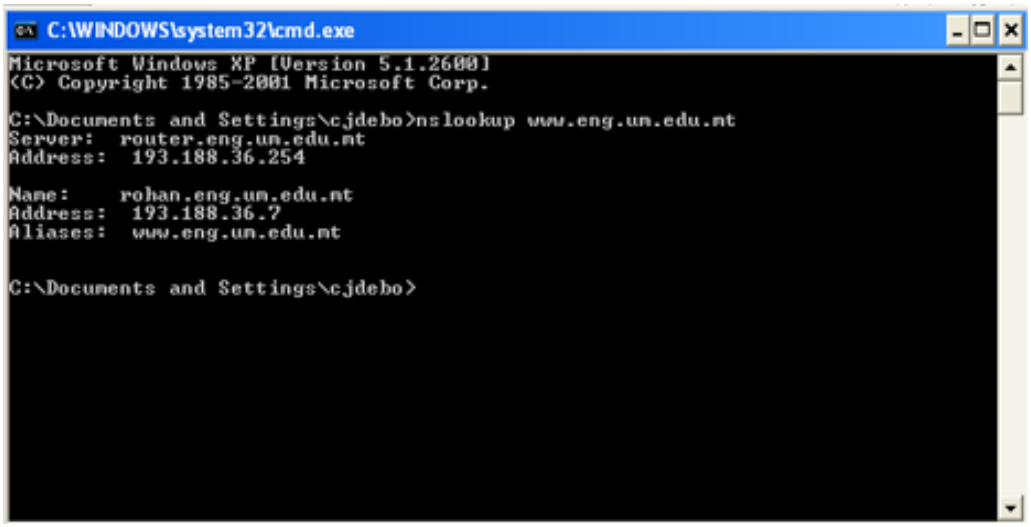
Answer the following questions:

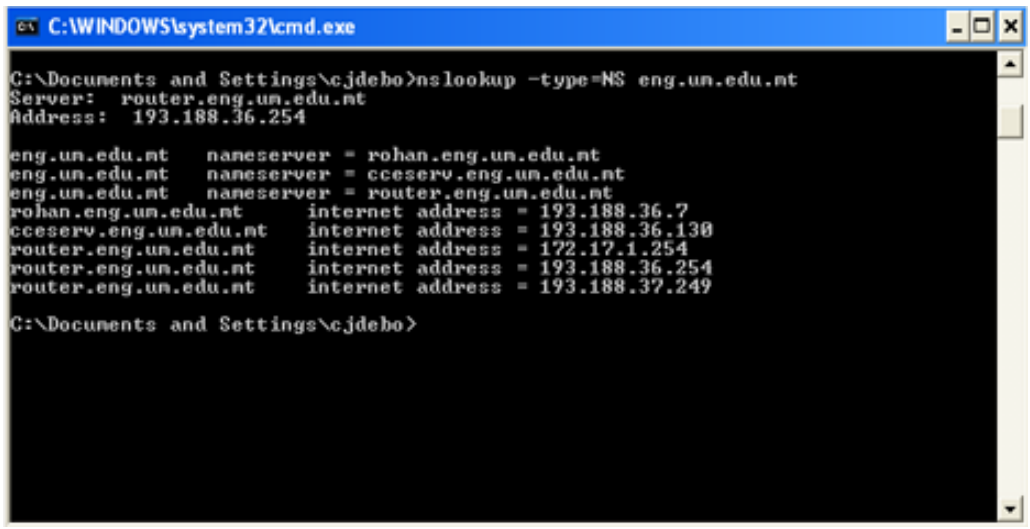
1. What version of http is the browser and server running? _____
2. How many requests have been done? _____
3. What applications does the browser accept? _____
4. What languages does the browser indicate that it can accept to the server? _____
5. What are the IPs of your computer and the server? _____
6. When was the file retrieved last modified? _____

7. What are the port numbers used in this transfer? _____
8. How many bytes of content are sent to the browser? _____

Experiment 3: Tracing DNS

The nslookup tool allows the user to query any specified DNS server for a DNS record. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result. An example is shown below.





The screenshots above show two types of nslookup queries. The first command:

nslookup www.eng.um.edu.mt

requests the default DNS server, in this case router.eng.um.edu.mt, to send the IP address for the host www.eng.um.edu.mt. The response from this command provides two pieces

of information: (a) the name and IP address of the DNS server; and (b) the answer itself. Note that although the response came from the local DNS server, it is possible that this local DNS server iteratively contacted several other DNS servers to get the answer.

Consider the second command:

nslookup –type=NS eng.um.edu.mt

The option "-type=NS" and the domain "eng.um.edu.mt" were used. This causes nslookup to send a query for a type-NS record to the default local DNS server. This command will request for the host names of the authoritative DNS for eng.um.edu.mt. The answer first indicates the DNS server that is providing the answer along with three nameservers. Finally, the answer also includes the IP addresses of the authoritative DNS servers available.

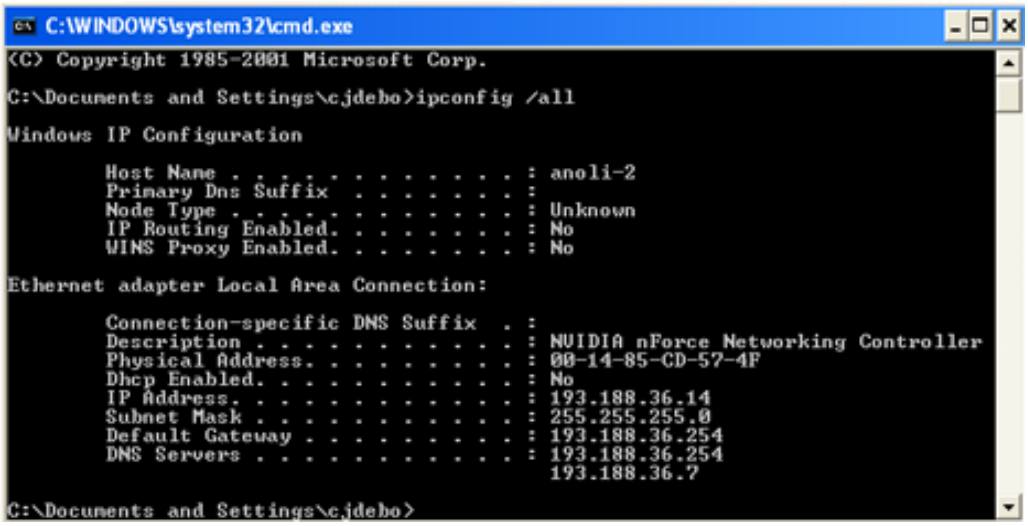
The general syntax of nslookup commands is:

nslookup –option1 –option2 host-to-find dns-server

In general, nslookup can be run with zero, one, two or more options, and the dns-server is optional as well.

Do the following (and write down the results):
1. Run nslookup to determine the authoritative DNS servers for a university in Italy.
2. Run nslookup so that one of the DNS servers obtained in Question 1 is queried for the Google servers.

Ipconfig is among the most useful utilities on the host, especially for debugging network issues. Ipconfig can be used to show the current TCP/IP information on the user's machine. It includes the IP address, DNS server addresses, adapter type and so on. Below is the output of ipconfig /all command.



Ipconfig is also useful in managing the DNS information stored in user's host. Remember that a host can cache DNS records it recently obtained. To see these cached records, provide the following command: ipconfig /displaydns

Each entry shows the remaining Time to Live (TTL) in seconds. To clear the cache, enter ipconfig /flushdns. Flushing the DNS cache will clear all entries and reload the entries from the hosts file.

Capture DNS packets generated by web browsing:

1. Empty the DNS cache of the computer.
2. Open the Internet browser and empty your browser cache.
3. Open Ethereal and enter "host your_IP_address" into the filter. This will remove all packets that neither originate nor are destined to the host.
4. Start packet capture in Ethereal.
5. Visit the web site: http://www.ieee.org
6. Stop Ethereal packet capture.

Answer the following questions:

1. Which protocol is used for DNS query and response? _____
2. What is the destination port for the DNS query message and the source port of DNS response message? _____
3. To what IP address is the DNS query message sent? _____
4. By examining the DNS query message, what "Type" of DNS query is it? _____
5. By examining the DNS response message, determine the number of "answers" provided? What does each of these answers contain? _____
6. Considering the subsequent TCP SYN packet sent by the host. Does the destination IP address of this packet correspond to any of the IP addresses provided in the DNS response message? _____
7. Before retrieving an image, does the host require a new DNS query? _____

Capturing nslookup

- Start Ethereal packet capture.
- Do an nslookup on www.eng.um.edu.mt
- Stop Ethereal packet capture.

To answer the following questions focus on the last query and response messages.

1. What is the destination port of the DNS query and what is the source port of DNS response? _____
2. To what IP address is the DNS query message sent? _____
3. Is this the IP address of your default local DNS server? _____

4. By examining the DNS query message, does the query message contain any "answers"? _____
5. By examining the DNS response message, how many "answers" are provided and what does each of these answers contain? _____

- Start Ethereal packet capture.
- Do an nslookup using the command nslookup –type=NS eng.um.edu.mt
- Stop Ethereal packet capture.

1. To what IP address is the DNS query message sent? _____
2. Is this the IP address of your default local DNS server? _____
3. By examining the DNS query message, does the query message contain any "answers"? _____
4. By examining the DNS response message, determine the nameservers available? _____

- Start Ethereal packet capture.
- Do an nslookup using the command nslookup www.ieee.org rohan.eng.um.edu.mt
- Stop Ethereal packet capture.

1. To which IP address is the DNS query message sent? _____
2. Is this the IP address of the default local DNS server? _____
3. By examining the DNS query message, what "Type" of DNS query is it? _____
4. By examining the DNS response message, what is the number of "answers" provided and what does each of these answers contain? _____

Experiment 4: Trace route

- Open a command prompt.
- Start Ethereal packet capture.
- Do a trace route command: tracert www.google.com
- Stop Ethereal packet capture.

1. What is the IP of the destination host? _____
2. Which protocols are used to execute the trace route? _____
3. What is indicated by the error packets? _____
4. What is the tracert measuring? _____
5. Identify some of the routers' location in the path. _____ _____
6. What are the delays of the links? _____ _____
7. Provide screenshots to confirm the above.

Comments: