CSE5344 Computer Networks Project II

– Network Trace Analysis

Due Date: 12/04/2013 17:00PM

The aim of the project is to familiarize you with various network protocols, network trace analysis and related tools. The project will require you to capture live network traffic, analyze and deduce various protocol parameters and performance.

Various network packet analyzer tools are available. For the purpose of the project we use Wireshark. It can be downloaded and installed from http://www.wireshark.org/. The project is divided into three parts.

PART I (10 Marks)

1. Identify the IP address, subnet mask and default gateway of the interface of your host computer.
2. Identify the MAC address of your host computer.
3. What command did you use to accomplish the above two tasks?
4. Given your IP address, identify the network id (network address) of the network.
5. Which class of IP addresses does your IP address belong?
6. Is the IP address in public domain or private address space?

PART II (50 Marks)

Capture network traffic for few minutes. After you have started capturing the trace in your browser, open the website http://maps.google.com. After you stop capturing the network traffic; save the trace file with file name "Project II_Part II_Trace_<UTA ID>_<NAME>".

DNS Protocol (30 Marks)

1. Filter the trace for DNS protocol, what is your filter expression?
2. What transport layer protocol does DNS use?
3. Identify the pair of DNS query and response packet for the website you opened earlier (http://maps.google.com). Give their packet numbers. **Answer the following questions based on the indentified DNS query and response packets. Note: for the query packet, domain name is maps.google.com and type is A.**
4. What is the size of the DNS query packet at transport layer? What are the header length and the payload data unit (PDU) size?
5. What is the size of the DNS response packet at transport layer? What are the header length and the payload data unit (PDU) size?
6. What is the DNS server IP address?
7. For DNS query, what are the source port and destination port on host computers?
8. For the DNS query message header gather the following information.
    a. What is the transaction ID of the DNS query? Give the hexadecimal code of it.
    b. What is the length of this transaction ID field?
    c. What is this transaction ID used for?
    d. Identify the flag field in the DNS query. The DNS flag filed is made of multiple sub-fields. What is their value in bits and state the corresponding meaning of each sub-field given the value? Give the hexadecimal code for the flag field.

e. How many questions were asked in this query?
f. In the DNS queries field, what is the domain for which the query was sent? Give the string and equivalent hexadecimal representation of it. What is its field length?
g. State the query type and its meaning? Give the string and equivalent hexadecimal representation of it. What is its field length?
h. Give examples of different types of queries, their RR value and their description. Give at least six examples.
i. State the query class and its meaning. Give the string and equivalent hexadecimal representation of it. What is its field length?
j. Give examples of two other query classes and their meanings.

9. For the DNS response message header gather the following information
   a. Is the transaction ID same as the query?
   b. Identify the flag field in the DNS response. The DNS flag filed is made of multiple sub-fields. What is their value in bits and state the corresponding meaning of each sub-field given the value? Give the hexadecimal code for the flag field.
   c. How many replies are there to the query?
   d. Are there multiple answers to the query? If yes, can you suggest a reason for it?
   e. Does the website http://maps.google.com have an alias? What is it?
   f. Pick any one of the answers to the query. State the answer in RR format identifying each field. Give the meaning of each of the values in the sub-fields of the RR record.
   g. Study the answers in authoritative name server section. Why is the type field in all sections set to "NS"?
   h. How do you find the IP address of all the authoritative name servers specified in the authoritative name server section? State their IP addresses.

HTTP (20 Marks)

1. How many HTTP GET messages were sent by your browser? What is your filter expression? To what IP addresses were the GET messages sent?
2. How many HTTP RESPONSE messages did your browser receive? What is your filter expression?
3. Identify the pair of HTTP request and response messages for the website http://maps.google.com. Give the packet numbers. **Answer the following questions based on the indentified HTTP request and response packets. Note: for the request message, full request URI is http://maps.google.com/. Hint: you can find the response message number in the content of the request message.**
4. What version of the HTTP message are your browser and the HTTP server running.
5. What type of files, languages, encoding and character set (if any) does your browser indicate that it can accept to the server?
6. What is the status code returned from the server to your browser?
7. What is the content type, encoding and character encoding (if any) returned by the server?
8. How many bytes of content are being returned to your browser?
9. What is the source and destination port number in the HTTP GET message?
10. What is the source and destination port numbers in the HTTP RESPONSE message?

PART III (35 marks)

HTTP STREAMING

In this part you use your browser or any media player to stream to your host computer a video file over HTTP. The instructions for how to set up the streaming server and access it is provided at the end of the

document. Capture the network traffic for the duration of the video stream. Save the trace file with file name "Project II_Part III_Trace_<UTA ID>_<NAME>".

1. Filter the trace to only show interactions between your host computer and the HTTP server. Give the expression used.
2. How many HTTP GET request messages were sent by your browser? What is your filter expression?
3. How many types of HTTP RESPONSE messages did your browser receive? What is your filter expression? State the response code and their meaning?
4. What is the IP address of the HTTP server?
5. On what web server is the HTTP server hosted? How can you infer the information from the traces?
6. What is the content type specified in the HTTP RESPONSE message?
7. At the host computer what is your TCP window size. What is the window scaling factor at the host computer? What would be your window size if it is scaled once by the window scaling factor? Why is window scaling used in TCP?
8. At the HTTP server the sequence number of next packet is increased in fixed steps. Specify this fixed step value and explain the reason.
9. In the Time-Sequence Graph (Stevens) for all traffic from the HTTP server to the host computer, the sequence number of the packets increases in discrete steps. Do you notice a start-up delay in the capture traffic stream? The start-up delay is defined as the time from which the host computer sends a request to the server and the application starts playing the video file. Specify the start-up delay if any. Enclose a snapshot of the graph named as "Time-Sequence Graph (Stevens)".
10. What is the starting and ending sequence numbers at the server? Can you identify how many packets with application data were transmitted?
11. Consider the TCP segment containing the first application data as the first segment in the TCP connection. What are the sequence numbers of the first ten segments in the TCP connection? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the ten segments? What is the EstimatedRTT value after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment. Show the process of calculation. State your assumptions if any (You can suppose α=0.125). Enclose a snapshot of the graph named as "RTT graph".
12. Video streaming is constrained by its quality of service (QoS) requirements of delay and jitter. The delay and jitter requirements are given by the table below. One-way delay is the time duration between the packets transmitted from the source and received at the destination. Jitter is defined as the variance in delay. Based on the graph of observed RTT in question 15 of Part III can you comment on the delay and jitter experienced by the video stream. Can you relate the approximate values of delay and jitter that you perceive with the mentioned perceived quality and the video stream quality as observed by you in the vlc player. Comment on it.

One-way delay	Effect on perceived quality
< 100-150ms	Delay no detectable
150-200ms	Still acceptable quality, but a slight delay in or hesitation is noticeable
Over 250-300ms	Unacceptable delay, normal conversation impossible

Delay variation (jitter)	Effect on perceived quality
< 40ms	Jitter no detectable
40-75ms	Good quality, but occasional delay or jumble noticeable
Over 75ms	Unacceptable, too much jumble in conversation

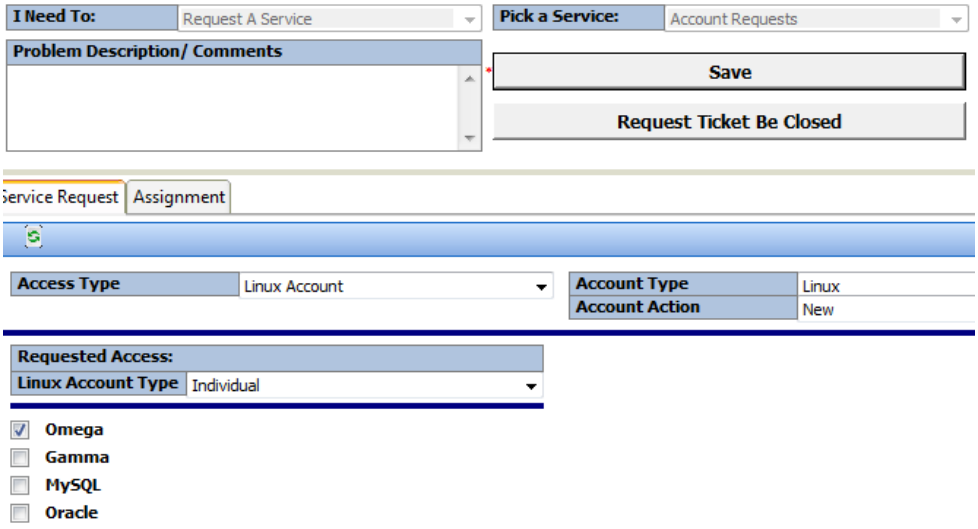
Source: E. Sedoyeka, Z. Huanti, and D. Tairo, "Analysis of QoS Requirements in Developing Countries," *International Journal on Computing and ICT Research*, vol. 3(1), pp. 18-31, 2009

13. Video streaming protocols prefer using UDP rather than TCP as the transport layer protocol, even though TCP ensures reliable delivery of data. Video streaming applications are characterized by high transmission rate than conventional applications. Can you identify and comment what feature of TCP makes it undesirable of real-time applications with stringent QoS constraints.

Instructions for Setting up the HTTP Streaming Server

Create an account on the omega server.

Go to http://www.uta.edu/oit/cs/accounts/requests.php, click on https://ithelp.uta.edu to create a Linux Individual Account. Enter your NET ID and password when asked. On the order page enter the required information. Typically creation of account takes few business days, so do this well in advance and not few days before the submission deadline.



Once your account is created log on to the omega server using your NET ID and password. Select the video file you want to stream (typically of size around a minute) and copy it to the "public_html" folder on the server.

For linux and MAC users:
Assume your NET ID is "xxx0000".

In the bash shell enter the following command and then the password:
> ssh xxx0000@omega.uta.edu
xxx0000@omega.uta.edu's password:
Check if the "public_html" folder exists or not. If not create the folder and give it the following permissions
> mkdir public_html
> chmod 755 public_html
Go to the folder
> public_html
Check the folder location using "pwd".
> pwd
/home/x/xx/xxx0000/public_html
Now copy the video file to this directory. From a separate shell give the following command
> scp file-location/file-name xxx0000@omega.uta.edu: /home/x/xx/xxx0000/public_html

For Windows users:
Download the SSH Secure Shell Client from http://www.uta.edu/oit/cs/software/downloads.php. Log in on the omega server using Host Name as "omega.uta.edu" and user name as your NET ID. Follow the instructions discussed above for Linux and MAC users for creation of the directory and the copy of the video file in the shell.

Assuming you uploaded the video file given by the name "test.avi". The URL to access the file from your browser is http://omega.uta.edu/~xxx0000/test.avi

Playing the Media Stream at the Host Computer

Install VLC media player from http://www.videolan.org/vlc/.

Open the VLC client. Click File->Open Network Stream

In the window enter the URL as shown above replacing "xxx0000" with your Net ID. Click play to start streaming and watch the video.

Instructions for capturing the HTTP stream

1. Create an account on the omega server.
2. Copy the video file as instructed.
3. On the host computer start Wireshark and start capturing network traffic.
4. Open the VLC client and play the media stream as instructed.
5. After completion of the media stream stop the capture.
6. Save the trace file.

Instructions for Submission

1. The submission must include the following files
    a. Trace file captured in Part II of the project.
    b. Trace file captured in Part III of the project.
    c. A Word or PDF file with answers to questions. **(A hard copy of the answers should be submitted to the instructor on 12/04/2013 in class)**

2. The file name of the final submission must strictly follow the following naming scheme: <course number>_<project number>_<student ID>.zip, such as: CSE5344_project2_1000650001.zip.
3. **Upload the compressed file to the omega server in the folder "public_html". Copy the file only into the "public_html" folder and not any sub-folders that you may have. E-mail me the link to your file and your NET ID. Please do not send me the submission file via email.**
4. Late and incomplete submission will be penalized. Make sure you are able to access and download the file from the link before sending it to me. A broken link will be considered as an incomplete submission.
5. Follow the naming convention of the file strictly as it will help me identify your submission. Failure to follow the naming convention will be considered as incomplete or non submission and be penalized accordingly.

Marking Scheme

Part I – 10 Marks
Part II – 50 Marks
Part III – 35 Marks
Follow Submission Instruction – 5 Marks

Online References

1. Wireshark, http://www.wireshark.org/docs/
2. IP address, http://en.wikipedia.org/wiki/IP_address
3. Domain Name System (DNS), http://en.wikipedia.org/wiki/Domain_Name_System
4. Domain Name Service (DNS).
http://www.comptechdoc.org/independent/networking/guide/netdns.html
5. Hypertext Transfer Protocol (HTTP), http://www.w3.org/Protocols/rfc2616/rfc2616.html
6. Transmission Control Protocol (TCP), http://en.wikipedia.org/wiki/Transmission_Control_Protocol