IERG 5090

Advanced Networking Protocols and Systems

Homework Assignment 3

Due: Apr. 25, 2017

I am submitting the assignment for:

☐ an individual project or

☐ a group project on behalf of all members of the group. It is hereby confirmed that the submission is authorized by all members of the group, and all members of the group are required to sign this declaration.

I/We declare that: (i) the assignment here submitted is original except for source material explicitly acknowledged; (ii) the piece of work, or a part of the piece of work has not been submitted for more than one purpose (e.g. to satisfy the requirements in two different courses) without declaration; and (iii) the submitted soft copy with details listed in the <Submission Details> is identical to the hard copy(ies), if any, which has(have) been / is(are) going to be submitted.

I/We also acknowledge that I am/we are aware of University policy and regulations on honesty in academic work, and of the disciplinary guidelines and procedures applicable to breaches of such policy and regulations, as contained in the University website http://www.cuhk.edu.hk/policy/academichonesty/.

In the case of a group project, we are aware that each student is responsible and liable to disciplinary actions should there be any plagiarized contents/undeclared multiple submission in the group project, irrespective of whether he/she has signed the declaration and whether he/she has contributed directly or indirectly to the problematic contents.

It is also understood that assignments without a properly signed declaration by the student concerned and in the case of a group project, by all members of the group concerned, will not be graded by the teacher(s).

_____	_____
Signature(s)	Date
_____	_____
Name(s)	Student ID(s)
_____	_____
Course code	Course title

Problem 1: Experiments on IPv6 Tunneling [30 points + 15 bonus points]

a) Install a packet sniffing software (e.g. Wireshark on windows or tcpdump on Linux) on your local machine. You will need to use it to record the differences in the sizes and formats of the packets being sent out for the different connections in part b), c) and d) of this question.

b) Establish connectivity from your machine to the public IPv6 Internet by ONE of the following two ways:

(i) Use Tunnel Broker software to access the public IPv6 Internet.

- You can find some public tunnel broker server here:
  http://www.ipv6day.org/action.php?n=En.GetConnected-TB
  or
  https://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers
  Try to search the Internet to find what is the server software used by your selected tunnel broker and what is the corresponding client.
  [Hint: The server broker.aarnet.net.au had been tested to work correctly even with an NAT several years ago (don't know its latest status though). However, you need to download a tunnel client and must register and request a tunnel setup according to the instructions on the following webpage:
  http://broker.aarnet.net.au/

(ii) Use Teredo to access the public IPv6 Internet.

- You can get an overview of Teredo at
  http://en.wikipedia.org/wiki/Teredo_tunneling#Permanent_prefix.

- Teredo has been built in Windows XP/2003/Vista/7/8, and its usage can be found at
  http://www.microsoft.com/technet/network/ipv6/teredo.mspx
  and
  https://social.technet.microsoft.com/Forums/en-US/6764f46b-8b63-4672-b83b-d60835a7f467/teredo-isnt-working-anymore-using-microsofts-default-teredo-servers-in-windows-7-to-10?forum=win10itpronetworking

- Some public Teredo servers can be found at
  http://www.ipv6day.org/action.php?n=En.GetConnected-Teredo

c) Use ping6/tracert6 (or "ping -6" / "tracert -6" in some other versions of operating systems) and the IPv6 connection you established in b(i) **OR** b(ii) to contact 3 different dual-stack IP destinations of your choices. Record the required hop-count and Round Trip Time (RTT) for the IPv6 connection. Repeat the measurements for the same set of destinations using IPv4 (and ping/tracert) from the same machine. Tabulate and compare your results between the IPv4 and IPv6 connections in terms of Hop-count, RTT, packet-sizes and packet-header encapsulation formats.

You may need to use nslookup for IPv4 and/or IPv6 to resolve the IP address of the dual-stack destination.

- The command on Windows 8 for IPv6 DNS query is "nslookup www.xxx.net".
- You can find a list of "candidate" (possibly outdated) dual-stack IP hosts from:

http://mobitec.ie.cuhk.edu.hk/projects/IPv6/ReachableDualStackSites.html

d) [Bonus: 15 points] In part (b) and (c), you used one approach to setup the tunnel. Please re-do configuration in (b) and measurements in (c) with the other method that is not used before.

Problem 2: Video Streaming Protocols [25 points]

Surf the Internet (or with the help of Google) to find two web sites that use different protocols to support streamed/stored audio or video. For each site, use Wireshark to determine:

a) Whether metafiles are used
b) Whether audio/video is sent over UDP or TCP
c) Whether RTP is used
d) Whether RTSP is used
e) Whether the audio/video data packets are downloaded via an HTTP connection.

Problem 3 [30 points + 15 * 2 Bonus points]

This problem helps you to understand how SIP and some SIP like protocol/client works. The "Mandatory" part provides you a detailed guideline to conduct measurement studies. After learning the methodology and tools, you can conduct experiments for additional SIP-like protocols/clients for the bonus portion in a similar manner.

Mandatory Part: [30 points]

Conduct the following experiment steps and answer the corresponding questions:

a) Download Jitsi (SIP Communicator) [1] and install it.
b) Go to iptel.org [2] and register an account for using SIP services.
c) Open Wireshark [3], and start capturing SIP packets.
d) Launch Jitsi, add your registered account to network "iptel.org".
e) Can you capture SIP register messages? If yes, what's your IP address and SIP server address?
f) Which port number(s) do you use?
g) Show the packet content contains your account information.
h) Send text messages to another student.
i) What's your partner's IP address?
j) Which transport layer protocol is used?
k) Describe the packet header and content format Jitsi uses for text messages, and show some packets.

l) Form a group with other 2 or 3 students. Each group is required to conduct audio conference N times, where N is the size of the group. During each conference, one of the participants should be the conference leader in charge of the conference establishment inviting the participants and managing the conference; every group member should be the leader once. The duration of each conference is about 30 seconds. During the conference, every participant is required to catch the packets using Wireshark.

(1) Write down IP addresses and port numbers of all the participants' computers including yourself.

(2) Which transport layer protocol is used?

(3) Are there any conference participants behind the NAT? Find the IP addresses of these NATs.

(4) Describe steps to set up an audio conference, and use captured packets to support your description.

(5) What is the difference between text message packets and audio packets?

(6) What is the difference between when you are/aren't the conference leader?

m) Start a video chatting with the same partner in step (e), and capture packets.

(1) Which transport layer protocol is used?

(2) Describe the packet header and content format Jitsi uses for video chatting. What's the difference between video chatting and audio chatting?

(3) Show some packets.

[1] Jitsi (SIP Communicator): http://www.jitsi.org/
[2] iptel.org: http://serweb.iptel.org/user/reg/index.php
[3] Wireshark: http://www.wireshark.org/

Bonus Part 1: [15 points]

Apple's Facetime also uses a SIP-like protocol. Please measure the whole cycle of a video conference using Facetime. e.g. registry information exchange with server, call initiation, and audio/video data transmission. Describe your observation with supporting measurement evidence (e.g. using screenshots with highlighting).

Hints: We have several iMACs in the IE computing lab and the open meeting room on SHB 8th floor. You can launch Wireshark on those devices. If you have a MACBook Pro, you can also run both Facetime and Wireshark on it. Alternatively, you can use Facetime from an iPhone over an *insecure* WiFi link and then use Wireshark on a separate machine to sniff the Facetime signaling messages over the insecure WiFi link.

Bonus Part2: [15 points]

Starting version 4.0, many Android phones include a SIP client (under the Phone App) by default. You can register for free SIP accounts from some Voice-over-IP

service providers, such as:

- CallCentric, http://www.callcentric.com/

You can also use service providers other than CallCentric. After registration, try text message, audio calls and video calls. Measure how SIP initiates a session and what are the negotiated transmission parameters for audio and video data.

Hint: In order to do packet sniffing for you Android phone, you can:

- Root your phone and install tcpdump on it OR
- Set up your PC as an Access Point to offer an insecure WiFi link over which your Android phone can access the Internet and then use your PC to sniff on the SIP messages OR
- Connect your Android phone to the Internet via an unencrypted CUHK's WiFi services. Run Wireshark from your laptop to sniff over-the-air traffic by turning the laptop's WiFi interface to promiscuous mode .