ARIZONA STATE UNIVERSITY

CSE 434, SLN 70569 — **Computer Networks** — Fall 2021

Lab #2

Available Sunday, 10/17/2021; due electronically before 11:59pm on Sunday, 10/31/2021

This lab includes two tutorials: One on TCP congestion control, and the other on basic home gateway services, specifically on DHCP, DNS, and NAT. Both tutorials in this lab use GENI. Expect the time to complete the experiments in the first tutorial to be around 60 minutes, and around 120 minutes for the second.

To ease grading:

1. Your report must consist of a **single file**, *i.e.*, you should import any figures and/or screen shots directly into your report. Always include your ASUrite id as part of any screen shot.
2. Include your group number and group member(s) on the title page of your report.
3. Label each exercise by its number, and provide your solution to the exercises in order.

1 TCP Congestion Control

TCP is arguably one of the most important Internet protocols, as it carries a much higher volume of traffic on the Internet than any other transport-layer protocol. Because of the importance of TCP congestion control, it is continuously undergoing improvement and refinement as the Internet and the characteristics of Internet traffic changes.

In this TCP Congestion Control tutorial, you'll work through experiments examining different variants of TCP congestion control. These include:

1. An early variant of TCP congestion control (TCP Reno) that uses a basic additive increase, multiplicative decrease (AIMD) rule.
2. The TCP Cubic variant, which is the current default on Linux servers used in much of the Internet.
3. Comparing a loss-based congestion control algorithm (Reno) with a delay-based congestion control algorithm (Vegas).
4. Using explicit congestion notification (ECN) with active queue management to try to reduce congestion before a router starts dropping packets.

Exercise 1.1: Configure the topology as described in the "Run my experiment" section of the tutorial. Follow the section "Exercise" to create a plot of the congestion window size for each TCP Reno flow over the duration of the experiment (see Fig. 1). Use the script provided to analyze the results of your experiment. Download the `sender-ss.svg` image file to your computer.

Annotate your plot (see Fig. 2) to show the periods of slow start and congestion avoidance, any instances where multiple duplicate ACKs were received (which trigger fast recovery), and any instances of a timeout.

For your lab report:

1. Include your annotated plot of the three flows sharing the bottleneck link using TCP Reno.
2. Using your plot and/or experiment data, explain the behaviour of TCP Reno in the slow start and congestion avoidance phases. In addition, explain what happens to both the congestion window and the slow start threshold when multiple duplicate ACKs are received.

Exercise 1.2: Under the "Optional: Other Congestion Control Algorithms" section of the tutorial, repeat the steps in the "Generating Data" section using the TCP Cubic variant. Download the updated `sender-ss.svg` image file to your computer.

Study the TCP Cubic algorithm and use it to annotate your plot, as you did in Exercise 1.1 for TCP Reno.

For your lab report:

1. Include your annotated plot of the three flows sharing the bottleneck link using TCP Cubic.
2. Using your plot and/or experiment data, explain the behaviour of TCP Cubic.
3. Why does TCP Cubic reach the available bandwidth faster than TCP Reno?

Exercise 1.3: Under "Optional: Low Delay Congestion Control" section of the tutorial, repeat the steps in the "Generating Data" section using the TCP Vegas variant.

Make a note of the `iperf3` throughput and the RTT estimated by `ping` during the TCP Vegas flow.

TCP Vegas does not work well when it shares a bottleneck link with a flow using a loss-based algorithm, *e.g.*, TCP Reno. To help understand the problem, you will send one TCP Reno flow and one TCP Vegas flow through the bottleneck router.

For your lab report:

1. Make a note of the throughput reported by `iperf3` for the TCP Reno flow and the TCP Vegas flow.
2. Using your throughput measurements, and knowledge of the congestion control mechanisms used by each algorithm, can you explain why TCP Vegas does not work well in this scenario?

You are welcome to try the experiment using TCP BBR, a more recent congestion control proposed by Google, but it is not required for this lab.

Exercise 1.4: Under "Optional: Explicit Congestion Notification (ECN)" section of the tutorial, use active queue management to configure a queue in both directions on the router, and enable ECN in TCP on each host. Prepare to capture the TCP flow on each host, and then start the experiment. When the experiment finishes, transfer the packet captures (*i.e.*, the `.pcap` files) to your computer using `scp`.

For your lab report:

1. Compare the delay performance of Reno with ECN to that from the experiment (Exercise 1.3) showing the delay performance without ECN.
2. Look for the ECN-related fields in the IP header and TCP header, during connection establishment and during data transfer. Annotate your packet capture files by drawing a circle or a box around the fields to show:
   (a) The ECN handshake, *i.e.*, the `ECN-setup SYN` packet and corresponding `ECN-setup SYN-ACK`.
   (b) Select a data packet and show the two ECN bits in the IP header set to either either 01 or 01.
   (c) Find an instance of a "congestion experienced" signal, *i.e.*, the two ECN bits in the IP header set to 11, and subsequent "congestion window reduced" (CWR) flag in the TCP header of the next packet.

   Note: You may cut/paste select portions from your `.pcap` files; there is no need to include the entirety of each trace file.

You are now finished with the resources that you reserved for this tutorial. Please delete them now to free them for use by other experimenters.

2 Basic Home Gateway Services: DHCP, DNS, NAT

Most Internet-connected homes use a home network gateway to connect a local area network (LAN) in the home, to a wide area network (WAN) such as the Internet. Services on these gateways include:

- Routing between the LAN and WAN,
- DHCP, to provide hosts in the home network with IP addresses,
- DNS, to respond to name resolution queries from hosts in the home network, and
- NAT (Network Address Translation), to map one public IPv4 address to internal (private) IP addresses assigned to hosts on the home network.

The focus of this tutorial on Basic Home Gateway Services is on DHCP, DNS, and NAT.

Configure the topology as described in the "Run my experiment" section of the tutorial. This experiment mimics clients connecting to a residential gateway and using the network services provided by that gateway. The clients in our experiment are already set up to use a university gateway for those services. (Otherwise, they would not have a functional network connection and we would not be able to get in to them over `ssh`.)

To run this experiment, we will tell the clients not to use the university gateway for anything except our `ssh` session. However, once you do this, you should plan to finish the rest of the experiment involving these resources in the same `ssh` session. Otherwise, if you stop and then resume the experiment from a new `ssh` session in a new location, you won't be able to access the clients any longer.

Exercise 2.1: Reset the configuration of the clients to mimic connecting to a residential gateway. Follow the instructions in the section "Observe a DHCP Request and Response."

For your lab report:

1. Take a screen shot showing the DHCP discover message sent by the client to try and find DHCP servers on the LAN. What are the source and destination IP addresses in this request? Why are these addresses used?
2. Take a screen shot showing the DHCP offer sent by the server. What IP address does the server offer? What is the range of addresses that the server in our experiment may offer? (You can refer to the `dnsmasq` configuration file.)
3. Take a screen shot showing the DHCP request sent by the client. What is the destination address in this request? Why?
4. Take a screen shot showing the DHCP acknowledgement sent by the server to complete the configuration.
5. Take a screen shot showing the configuration of the client's `eth1` interface after receipt of the DHCP acknowledgement. Annotate your screenshot by drawing a circle or a box around the configuration to show the IP address and subnet mask the client is using. Does this correspond to the IP address in the request and in the acknowledgement? What, if any, other information did the server offer to the client?

Exercise 2.2: Now follow the instructions in the section "Observe a DNS Query and Response."

For your lab report:

1. For the basic DNS resolution (not the one with `+trace`) take a screen shot showing the `dig` command and its output. Also show the DNS query and response from the `tcpdump` output. Answer the following questions using the output gathered (no explanation is required).
   (a) What is the hostname that you tried to resolve?
   (b) What is the DNS record type associated with your query? (See this list of DNS record types.)
   (c) What is the address for the hostname you asked to resolve?
   (d) Give the name of the first "authoritative" server listed for this name, and the IP address of that "authoritative" server.
   (e) What is the IP address of the server that the DNS response is from?
2. For the hierarchical DNS resolution with `+trace`, take a screen shot of the `dig` command and its output. Draw a diagram showing how the hostname was resolved recursively, starting from the implied "." at the end and moving toward the beginning.
   (a) At the top, show the name servers for the root domain. Highlight the one that you queried for the top-level domain (as shown in the `dig +trace` output).
   (b) At the next level, show the name servers for the top-level domain. Highlight the one that you queried for the second-level domain.
   (c) At the next level, show the name servers for the second-level domain. Highlight the one that you queried for the subdomain.
   (d) Repeat until you have shown how the complete hostname is resolved.

Exercise 2.3: Follow the instructions in the section "Use NAT" set up the `gateway` to use NAT.

For your lab report:

1. Take screen shots to show the three-way TCP handshake for a connection between `client` and `website` as seen by `tcpdump` at the website, and as seen by `tcpdump` at the gateway (on the LAN). Make sure you can see the IP addresses and port numbers used in the connection.
2. Draw a diagram showing how NAT is used between `client` and `website`, similar to this diagram but with the IP addresses, hostnames, and ports from *your* experiment.

You are now finished with the resources that you reserved for this tutorial. Please delete them now to free them for use by other experimenters.