EE 5516: Introduction to Networking (Fall, 2018)

Class locations and times

Teacher	Zhen Zhao, Ph.D.
Lecture times	Wednesday 5:30-8:00pm
Lecture room	Wachman 313

Week3 - HW1

1. Http programming: use any programming language you know, set a RESTful website, you don't have to make it public (just run it on your own laptop so it could be reached by http://localhost). Your website should be able to handle a http GET request and return corresponding http response.
2. Socket programming: use any programming language you know, code socket server and client program. Your socket server and client should be able to send plain text (strings) to each other.
3. Network security: use http flooding to try your own RESTful website and record the various http response grounded on your request profile.
4. Describe the workflow of watching a video station, specifying each step what the application layer's protocols are used.
5. Hash table:
   - Can I use hash key as an id? Specify the reason.
   - How to find the difference between two list of strings
   - How to handle the duplication of the hash code?
   - How to deal with an shared hash table being used on the web server?

Week4 - HW2

1. What are the transport layer protocols used for live video, file transfer, DNS and email, respectively?
2. Consider a TCP implementation with the Additive Increase (linear) and Multiplicative Decrease (AIMD) algorithm, ignoring the first phase where the ssthreshold is detected, assume the window size at the start of the slow start phase is 1 MSS and the ssthreshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the 4th transmission. Find the congestion window size at the end of the 8th transmission.

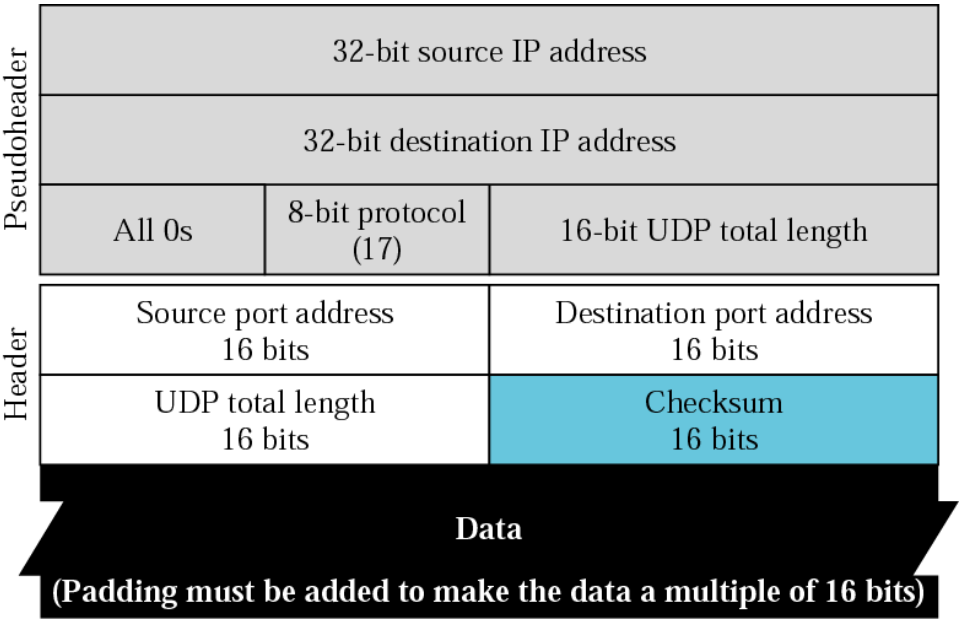

Figure 1: Data structure of UDP datagram for checksum calculation

3. UDP: Look into the following IP packet enclosing a UDP datagram. UDP checksum includes three sections: a pseudoheader, the UDP header, and payload – the data coming from the application layer. Pseudoheader and padding are only used to calculate checksum. After checksum is calculated, they are dropped. The figure. 1 is not a complete IP packet. It has the major info of the IP packet that has the UDP datagram and these info are what UDP checksum need to calculate. Now, assume we have

   - Source IP: 153.18.8.105
   - Destination IP: 171.2.14.10
   - The protocol is "UDP" (value is 17)
   - Source port: 1087
   - Destination port: 13
   - Payload: "TESTING".

   Please calculate the checksum for this packet. Hints:

   (a) When calculating the checksum, the value in the field "checksum" as the input of the calculation is "0".

   (b) Yes, the UDP total length field seems duplicated but remember the pseudoheader will be dropped after the checksum calculation.

   (c) The payload must be multiple of 16 bits so if needed, you should pad "0"s.

   (d) When counting the length, you should count the number of byte (8-bit). Also, pseudoheader is not included. The padding 0s in the payload is not counted.

   (e) Find the ASCII for the characters in the payload and use binary.

4. Network security: install nmap on your laptop, you can find the info here: https://nmap.org. Play around nmap and try something like this:

$nping –tcp-connect -p 8000 -rate 100000 -q x.x.x.x where x.x.x.x is the ip address of your RESTful API website built in HW3. Describe what you saw. Note: you need explore how to use nping with checking the nmap.org website, you will probably need change the parameters in the above example according to your own website's configuration. Nmap is a very powerful tool that many security applications are built on.
****If you haven't done your week3 hw, try this:
$ nmap localhost You will see something like what I saw:
Starting Nmap 7.70 (https://nmap.org) at 2018-09-21 15:20 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00069s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 969 closed ports, 26 filtered ports
PORT STATE SERVICE
22/tcp open ssh
88/tcp open kerberos-sec
631/tcp open ipp
3283/tcp open netassistant
5900/tcp open vnc
This let you know that the protocols like SSH are all open on the localhost Mac. If you don't have your own RESTful API website ready, don't worry. Please use the nmap tool to scan and list a range of your local network IPs like
$nmap -sP 192.168.0.1-16. Describe what you saw.

Week5-7 Network layer - HW3

1. Use LInk-state and distance vector algorithms to find the short paths from the "source" node to other nodes in fig. 2. Describe each of your steps of the algorithms. Coding is not required.

2. Assume if you are a user connecting to the node "source", and you want to browse a web page of a server connecting to one node in this network fig. 2. Describe each step with what protocols you use and what those protocols are doing for your browsing, like we did in class.

3. Assume you would like to set a VPN to connect to another node in this network fig. 2, how do you do it? Again describe each step.

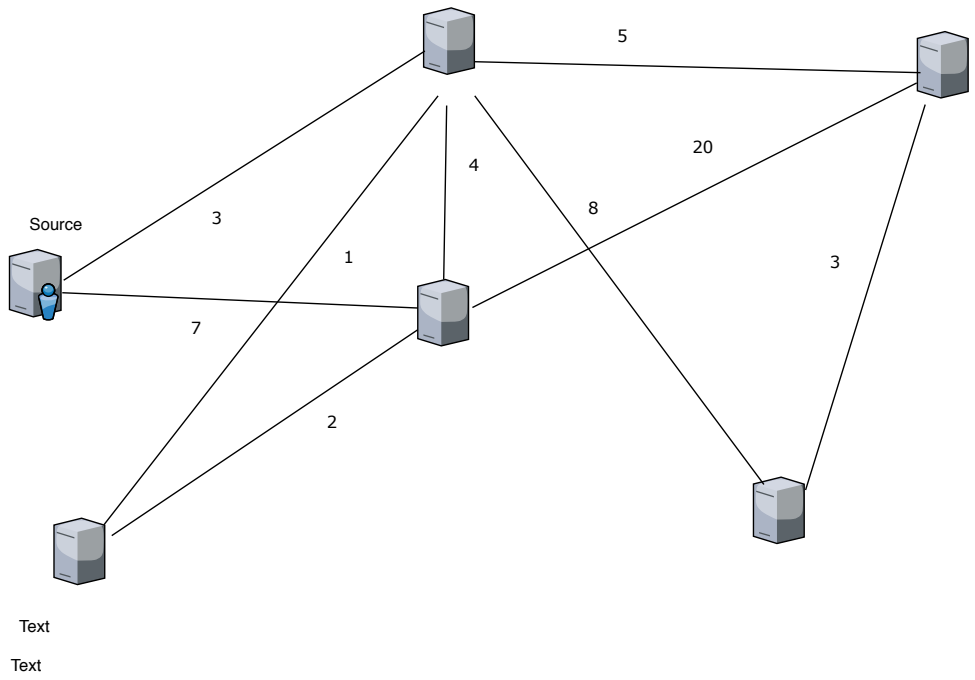

Figure 2: network topology