

## Problem 1

Suppose an application generates chunks of 60 bytes of data, each chunk gets encapsulated in a TCP segment, and then an IP datagram.

1. What percentage of each datagram will be overhead, and what percentage will be application data?
2. What would be the overhead if each TCP segment include 100 of application chunks (i.e.,  $100 \times 60$  bytes), assuming the maximum size of an IP packet is 500 bytes and sending such big TCP payload would require fragmentation.

1. Since there is 40 bytes of header, the overhead is  $40/60+40 = 0.4$ . Application data is 0.6

2. I will not consider header as overhead here.

Overhead is  $500 - 100 = 400$  due to fragmentation.

## Problem 2

Consider the router trying to send the following IP packet:

4	5	TOS	6123			
123098			0	0	0	0
25		6	checksum			
10.1.1.1						
80.233.250.61						
data (6103 bytes)						

Figure 1: An IP packet.

Assuming that the maximum transmission unit that can be transferred over the link is 1400 bytes. For each of the fragment show the header length, total length, identification, flags, fragment offset, TTL, protocol fields, and IP payload size.

Write your answer using the table below

Header length	Total length	Identification	Flags	Fragment offset	TTL	Protocol	Data size
20 bytes	1400 bytes	123098	001	0	24	6	1376 bytes
20 bytes	1400 bytes	123098	001	172	23	6	1376 bytes
20 bytes	1400 bytes	123098	001	344	22	6	1376 bytes
20 bytes	1400 bytes	123098	001	516	21	6	1376 bytes
20 bytes	620 bytes	123098	000	688	20	6	600 bytes

## Problem 3

Calculate the network mask, the number of bits of the network, the number of endpoint addresses in the network (excluding special addresses), the network address, and the broadcast address of the network for the following:

1. 131.179.196.0/24
2. 169.232.34.48/30
3. 196.22.136.0/21
4. 93.181.192.0, netmask 255.255.224.0
5. 10.128.0.0, netmask 255.192.0.0

<p>1. network mask: 255.255.255.0. first 24 bits are high, others are low: 11111111.11111111.11111111.0000. number of bits of the network: 32 since it's ipv4 number of endpoint addresses: <math>2^{*(32 - 24)} - 2 = 254</math> network address: 131.179.196.0 10000011.10110011.11000100.00000000 broadcast address: 131.179.196.240 10000011.10110011.11000100.11110000</p> <p>2. network mask: 255.255.255.252. first 30 bits are high, others are low: 11111111.11111111.11111111.11111100. number of bits of the network: 32 number of endpoint addresses: <math>2^{*(32 - 30)} - 2 = 2</math> network address: 169.232.34.48 10101001.11101000.00100010.00110000 broadcast address: 169.232.34.51 10101001.11101000.00100010.00110011</p> <p>3. network mask: 255.255.248.0. first 21 bits are high, others are low: 11111111.11111111.11111000.0000. number of bits of the network: 32 number of endpoint addresses: <math>2^{*(32 - 21)} - 2 = 2046</math> network address: 196.22.136.0 11000100.00010110.10001000.00000000 broadcast address: 196.22.143.255 11000100.00010110.10001111.11111111</p> <p>4. network mask: 255.255.254.0. first 23 bits are high, others are low: 11111111.11111111.11111110.0000. number of bits of the network: 32 number of endpoint addresses: <math>2^{*(32 - 23)} - 2 = 510</math> network address: 93.181.192.0 01011101.10110101.11000000.00000000 broadcast address: 93.181.193.255 01011101.10110101.11000001.11111111</p> <p>5. network mask: 255.192.0.0. first 10 bits are high, others are low: 11111111.11000000.00000000.0000. number of bits of the network: 32 number of endpoint addresses: <math>2^{*(32 - 10)} - 2 = 4194302</math> network address: 10.128.0.0 00001010.10000000.00000000.00000000 broadcast address: 10.191.255.255 00001010.10111111.11111111.11111111</p>
--

## Problem 4

Why is the IP header checksum recalculated at every router?

Checksum is calculated at every router because datagram needs to be discarded if the data is corrupted, so in order to minimize incorrect information, incorrect data needs to be detected as soon as possible. Checking checksum at every router ensures early detection of incorrect data. Also, some fields in the header such as time to live changes at every router, so checksum needs to be performed before header is processed.

## Problem 5

Install *Wireshark* (<https://www.wireshark.org/>). Then, (i) start capturing a packet trace from your network interface, (ii) open a web browser, (iii) go to <https://www.cs.ucla.edu/>, (iv) and then stop capturing the trace.

Investigate any TCP packet from your network interface to the UCLA CS web server. What is the IP address of your network interface? What is the IP address of [www.cs.ucla.edu](https://www.cs.ucla.edu/)? Provide the screenshot that shows the IP addresses in the investigated packet.

My network interface IP address is 192.168.0.21

The IP address of ucla cs website is: 164.67.100.181

No.	Time	Source	Destination	Protocol	Length	Info
621	135.852288	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=6/1536, t...
622	135.871541	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=6/1536, t...
623	136.853770	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=7/1792, t...
624	136.873192	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=7/1792, t...
625	137.645637	192.168.0.23	192.168.0.255	BROWS...	257	Host Announcement BETTY-LIU-V20, Workstation,
626	137.646780	192.168.0.23	192.168.0.255	NBNS	110	Refresh NB BETTY-LIU-V20<20>
627	137.648382	192.168.0.23	192.168.0.255	NBNS	110	Refresh NB WORKGROUP<00>
628	137.649774	192.168.0.23	192.168.0.255	NBNS	110	Refresh NB BETTY-LIU-V20<00>
629	137.855340	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=8/2048, t...
630	137.874186	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=8/2048, t...
631	138.858251	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=9/2304, t...
632	138.876881	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=9/2304, t...
633	139.385224	fe80::16b7:f8ff:fe...	ff02::1	ICMPv6	134	Router Advertisement from 14:b7:f8:77:22:3e
634	139.861346	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=10/2560, t...
635	139.880535	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=10/2560, t...
636	140.864909	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=11/2816, t...
637	140.884085	192.168.0.21	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
638	140.884662	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=11/2816, t...
639	141.869954	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=12/3072, t...
640	141.884636	192.168.0.21	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
641	141.892877	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=12/3072, t...
642	141.945008	192.168.0.23	224.0.0.251	MDNS	117	Standard query 0x0000 PTR _afpovertcp._tcp.lo
643	141.946724	fe80::1033:a27:653...	ff02::fb	MDNS	137	Standard query 0x0000 PTR _afpovertcp._tcp.lo
644	142.049747	192.168.0.23	224.0.0.251	MDNS	416	Standard query response 0x0000 PTR Betty Liu
645	142.053839	fe80::1033:a27:653...	ff02::fb	MDNS	436	Standard query response 0x0000 PTR Betty Liu
646	142.871982	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=13/3328, t...
647	142.885040	192.168.0.21	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
648	142.889662	164.67.100.181	192.168.0.21	ICMP	98	Echo (ping) reply id=0x3a25, seq=13/3328, t...
649	142.969427	192.168.0.23	224.0.0.251	MDNS	175	Standard query 0x0000 PTR _afpovertcp._tcp.lo
650	142.971426	fe80::1033:a27:653...	ff02::fb	MDNS	195	Standard query 0x0000 PTR _afpovertcp._tcp.lo
651	142.974430	192.168.0.21	164.67.100.181	ICMP	98	Echo (ping) request id=0x3a25, seq=14/3584, t...

The image shows two overlapping windows from a macOS desktop. The top window is titled "Network Utility" and has tabs for "Info", "Netstat", "Ping", "Lookup", "Traceroute", "Whois", "Finger", and "F". The "Traceroute" tab is selected. It prompts the user to "Enter an Internet address to trace the route to." with a text box containing "cs.ucla.edu" and a hint "(ex. 10.0.2.1 or www.example.com)". Below this, it says "Traceroute has started..." and displays the results of a traceroute to cs.ucla.edu (164.67.100.181), showing 64 hops max and 72 byte packets. The bottom window is a terminal titled "littlelotus — -bash — 80x24". It shows the last login time and the execution of a ping command to google.com (216.58.193.206), displaying 20 successful ping results with various response times.

Network Utility

Info Netstat Ping Lookup Traceroute Whois Finger F

Enter an Internet address to trace the route to.

cs.ucla.edu (ex. 10.0.2.1 or www.example.com)

Traceroute has started...

traceroute to cs.ucla.edu (164.67.100.181), 64 hops max, 72 byte packets

```

1 192.168.0.1 (192.168.0.1) 3.902 ms 2.192 ms 1.322 ms
2 142.254.236.89 (142.254.236.89) 11.035 ms 18.353 ms 10.697 ms
3 agg57.snmncaby02h.socal.rr.com (76.167.30.5) 13.766 ms 15.488 ms 16.771 ms
4 agg20.lamrcadq02r.socal.rr.com (72.129.10.130) 27.080 ms 23.714 ms 15.779 ms
5 agg28.tustcft01r.socal.rr.com (72.129.9.2) 13.741 ms 15.781 ms

```

littlelotus — -bash — 80x24

Last login: Wed Feb 27 20:18:17 on ttys001

Xiaohes-MacBook-Pro:~ littlelotus\$ ping google.com

PING google.com (216.58.193.206): 56 data bytes

```

64 bytes from 216.58.193.206: icmp_seq=0 ttl=54 time=17.540 ms
64 bytes from 216.58.193.206: icmp_seq=1 ttl=54 time=22.781 ms
64 bytes from 216.58.193.206: icmp_seq=2 ttl=54 time=18.599 ms
64 bytes from 216.58.193.206: icmp_seq=3 ttl=54 time=24.396 ms
64 bytes from 216.58.193.206: icmp_seq=4 ttl=54 time=17.624 ms
64 bytes from 216.58.193.206: icmp_seq=5 ttl=54 time=18.307 ms
64 bytes from 216.58.193.206: icmp_seq=6 ttl=54 time=19.488 ms
64 bytes from 216.58.193.206: icmp_seq=7 ttl=54 time=27.331 ms
64 bytes from 216.58.193.206: icmp_seq=8 ttl=54 time=29.768 ms
64 bytes from 216.58.193.206: icmp_seq=9 ttl=54 time=21.859 ms
64 bytes from 216.58.193.206: icmp_seq=10 ttl=54 time=22.932 ms
64 bytes from 216.58.193.206: icmp_seq=11 ttl=54 time=46.810 ms
64 bytes from 216.58.193.206: icmp_seq=12 ttl=54 time=27.576 ms
64 bytes from 216.58.193.206: icmp_seq=13 ttl=54 time=20.660 ms
64 bytes from 216.58.193.206: icmp_seq=14 ttl=54 time=34.867 ms
64 bytes from 216.58.193.206: icmp_seq=15 ttl=54 time=16.085 ms
64 bytes from 216.58.193.206: icmp_seq=16 ttl=54 time=19.169 ms
64 bytes from 216.58.193.206: icmp_seq=17 ttl=54 time=49.084 ms
64 bytes from 216.58.193.206: icmp_seq=18 ttl=54 time=28.096 ms
64 bytes from 216.58.193.206: icmp_seq=19 ttl=54 time=16.960 ms
64 bytes from 216.58.193.206: icmp_seq=20 ttl=54 time=18.680 ms

```

Problem 3 continued on next page.

Page 6 of 7

ation: Automatic

Status: **Connected** Turn Wi-Fi Off

Wi-Fi is connected to TC8715D3A and has the IP address 192.168.0.21.

Network Name: TC8715D3A

☒ Automatically join this network

☐ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.