CS468 – Homework Assignment 1

February 27, 2014

Bing Hao

1. An organization has a class C network 200.1.1 and wants to form subnets for four departments, which hosts as follows: A – 72 hosts, B – 35 hosts, C – 20 hosts, D – 18 hosts. There are 145 hosts in all.

(a) Give a possible arrangement of subnet masks to make this possible. What is the network address, subnet mask, broadcast address, maximum number of hosts for each subnet. Please also show the available IP address range for each subnet.

(b) Suggest what the organization might do if department D grows to 34 hosts.

Answer

a. For A – 72 hosts, the nominal subnet size is 2^7, the subnet musk could be 11111111.11111111.11111111.10000000, For this problem we only need to consider the last byte of the IP address, thus a possible IP address assignment could be 0XXXXXXX (One subnet bit 0, seven host bits)

Possible subnets: $2^1 = 2$ subnets
Network address: 200.1.1.0
Subnet mask: 255.255.255.128
Valid subnets: block size = 256-128=128
Broadcast address: 200.1.1.127 (next the start of subnet -1)
Maximum number of hosts: $2^7 - 2 = 126$
IP address range: 200.1.1.1- 200.1.1.126

For B – 35 hosts, the nominal subnet size is 2^6, the subnet musk could be 11111111.11111111.11111111.11000000, For this problem we only need to consider the last byte of the IP address, thus a possible IP address assignment could be 10XXXXXX (Two subnet bits 10, 6 host bits)

Possible subnets: $2^2 = 4$ subnets (Two subnet bits)
Network address: 200.1.1.128
Subnet mask: 255.255.255.192
Valid subnets: block size = 256-192=64
Broadcast address: 200.1.1.191 (next the start of subnet -1)
Maximum number of hosts: $2^6 - 1 = 63$
IP address range: 200.1.1.128- 200.1.1.190

For C – 20 hosts, the nominal subnet size is 2^5, the subnet musk could be 11111111.11111111.11111111.11100000, For this problem we only need to consider the last byte of the IP address, thus a possible IP address assignment could be 110XXXXX (Three subnet bits 110, 5 host bits)

Possible subnets: $2^3 = 8$ subnets (Three subnet bits)

Network address: 200.1.1.192

Subnet mask: 255.255.255.224

Valid subnets: block size = 256-224=32

Broadcast address: 200.1.1.223 (next the start of subnet -1)

Maximum number of hosts: $2^5 - 1 = 31$

IP address range: 200.1.1.192- 200.1.1.222

For D – 18 hosts, the nominal subnet size is 2^5, the subnet musk could be 11111111.11111111.11111111.11100000, For this problem we only need to consider the last byte of the IP address, thus a possible IP address assignment could be 111XXXXX (Three subnet bits 111, 5 host bits)

Possible subnets: $2^3 = 8$ subnets (Three subnet bits)

Network address: 200.1.1.224

Subnet mask: 255.255.255.224

Valid subnets: block size = 256-224=32

Broadcast address: 200.1.1.255 (next the start of subnet -1)

Maximum number of hosts: $2^5 - 1 = 31$

IP address range: 200.1.1.224- 200.1.1.254

b. We could give A two subnets, the last byte of the IP address of subnets could be:
   A: 01XXXXXX (64 hosts) and 001XXXXX (32 hosts)
   B:10XXXXXX (64 hosts)
   C: 000XXXXX (32 hosts)
   D:11XXXXXX (64 hosts)

2. Calculate the effective throughput to transfer a 1,000KB file in the following case, assuming a round-trip time of 100ms, a packet size of 1KB data, and an initial 2*RTT of "handshaking" before data is sent.

(a) The bandwidth is 1.5 Mbps, and data packets can be sent continuously.

(b) The bandwidth is 1.5 Mbps, but after we finish sending each data packet, we must wait one RTT before sending the next.

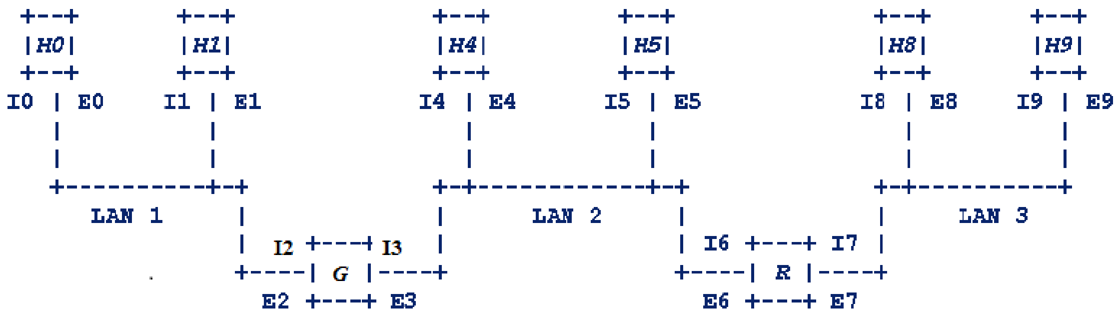
Answer

a. Throughput = TransferSize / TransferTime
   TransferTime = RTT + 1/Bandwidth * TransferSize

   TransferTime 2*0.1+ (1000*2^10*8)/(1.5*10^6)=5.661s
   Throughput =(1000*2^10*8)/ 5.661 = 1447094.15298 bps =1.447 Mbps

b. This means we need to wait 1 RTT for first 999 packets.
   TransferTime = 5.661s + 999*RTT =105.561 s
   Throughput =(1000*2^10*8)/ 105.561=77604.4182984 bps=0.077 Mbps

3. Consider the network topology below:



- **G is a gateway.**
- **R is an IP router.**
- **H0 , H1 , H4 , H5 , H8 & H9 are hosts.**
- **I0 ~ I9 are 32-bit IP addresses, as shown.**
- **E0 ~ E9 are 48-bit Ethernet MAC addresses, as shown.**

Suppose host H4 sends an IP packet to host H9. This packet will, of course, be encapsulated in an Ethernet frame.

(a) What are source and destination Ethernet addresses in the Ethernet header of the frame when it traverses on LAN 2?

(b) What are source and destination IP addresses in the IP header of the packet when it traverses on LAN 2?

(c) What are source and destination Ethernet address in the Ethernet header of the frame when it traverses on LAN 3?

(d) What are source and destination IP address in the IP header of the encapsulated packet when it traverses on LAN 3?

Suppose host H1 wants to talk to H9 and H1 has never connected to H9 before.

(e) What H1 will do and what protocol will be used?

(f) How many machines will get this message and who they are?

(g) What address information (source/destination MAC and source/destination IP) in the protocol header of the packet when it traverses on LAN 1?

(h) What address information (source/destination MAC and source/destination IP) in the protocol header of the packet when it traverses on LAN 2?

(i) What address information (source/destination MAC and source/destination IP) in the protocol header of the packet when it traverses on LAN 3?

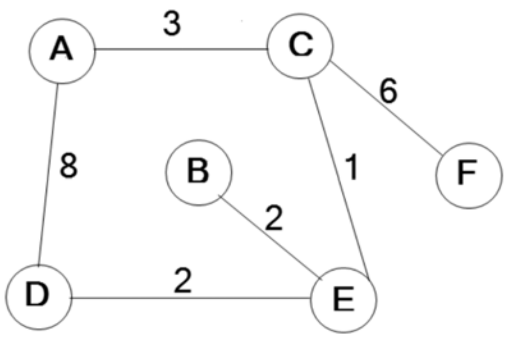
(j) What H9 will do when it receive the packet? What message it will reply and to whom? Please describe the details.

Answer

a. Source:E4
   Destination: E6
b. Source:I4
   Destination: I9
c. Source:E7
   Destination: E9
d. Source:I4
   Destination: I9
e. H1 noticed the H9 is not in its subnet, thus H1 needs to use the ARP protocol to get the MAC address E2 of G by using the IP I2. The data packet which need to be transferred to H9 will be sent to E2 of G, G will do the following transmission.
f. H0, G, R, H9 will get this message.
g. MAC source: E1
   MAC destination: E2
   IP source: I1
   IP destination: I9
h. MAC source: E3
   MAC destination: E6
   IP source: I1
   IP destination: I9
i. MAC source: E7
   MAC destination: E9
   IP source: I1
   IP destination: I9
j. If the UDP protocol is used, the H9 will do nothing after it received the packet. If the TCP protocol is used, an ACK message will be replay to H1. Since H1 is not in the same

subnet of H9, thus the ACK message will be sent to E7 of R, R will send it to E3 of G according to the routing table, finally E2 of G will send the ACK message to the E1 of H1.

4. For the network given below, give global distance-vector tables when



(a) Each node knows only the distances to its immediate neighbors.

(b) Each node has reported the information it had in the preceding step to its <u>immediate neighbors</u>.

(c) Apply (b) again.

<u>Answer</u>

a.

	A	B	C	D	E	F
A	0	Infinity	3	8	Infinity	Infinity
B	Infinity	0	Infinity	Infinity	2	Infinity
C	3	Infinity	0	Infinity	1	6
D	8	Infinity	Infinity	0	2	Infinity
E	Infinity	2	1	2	0	Infinity
F	Infinity	Infinity	6	Infinity	Infinity	0

b.

	A	B	C	D	E	F
A	0	Infinity	3	8	4	9
B	Infinity	0	3	4	2	Infinity
C	3	3	0	3	1	6
D	8	4	3	0	2	Infinity
E	4	2	1	2	0	7
F	9	Infinity	6	Infinity	7	0

c.

	A	B	C	D	E	F
A	0	6	3	6	4	9
B	6	0	3	4	2	9
C	3	3	0	3	1	6
D	6	4	3	0	2	9
E	4	2	1	2	0	7
F	9	9	6	9	7	0

5. For the network given in question 4, show how the link-state algorithm builds the routing table for node D.

Answer

Step	Confirmed	Tentative
1	D (0,-)	
2	D(0, -)	A(8,A) E(2,E)
3	D(0, -), E(2, E)	A(8, A), C(3, E), B(4, E)
4	D(0, -), E(2, E), C(3, E)	A(6, E), B(4, E), F(9, E)
5	D(0, -), E(2, E), C(3, E), B(4, E)	A(6, E), F(9, E)
6	D(0, -), E(2, E), C(3, E), B(4, E), A(6, E)	F(9, E)
7	D(0, -), E(2, E), C(3, E), B(4, E), A(6, E), F(9, E)	

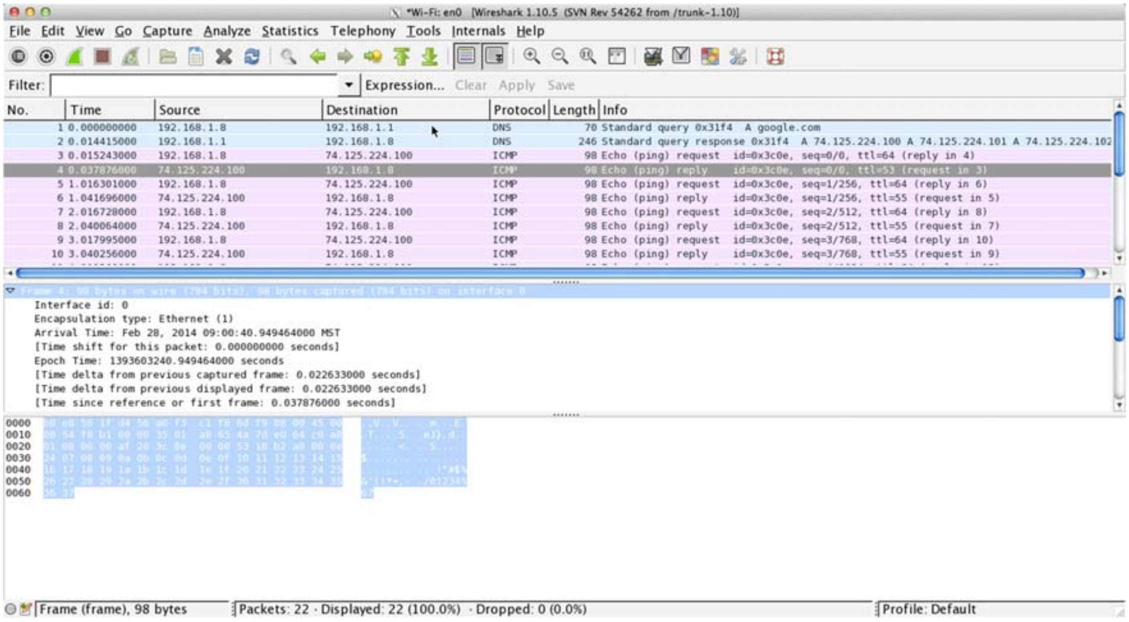
6. Consider three common network commands: ping, traceroute and nslookup,

(a) Give out when you want to use these three commands, what information you might get from these commands, and how they work. Please give your answer based on captured packets using Wireshark for each command.

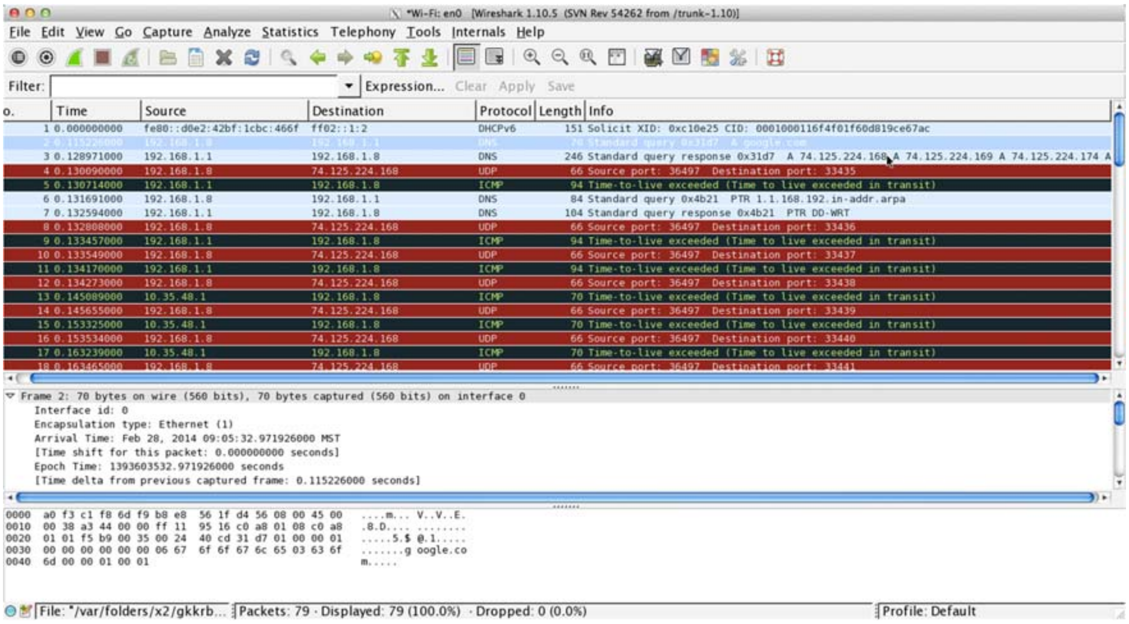
(b) I cannot access a remote machine (The machine's name is "boy", actually it is timeout when I use the command "ping boy"). Then you might derive the conclusions that the problems are 1) the name server is down, 2) the intermediate nodes is down, 3) the remote machine "boy" is down. Give your investigations that support your conclusion, specify clearly what command you use and what possible results that make you derive the conclusion.

Answer

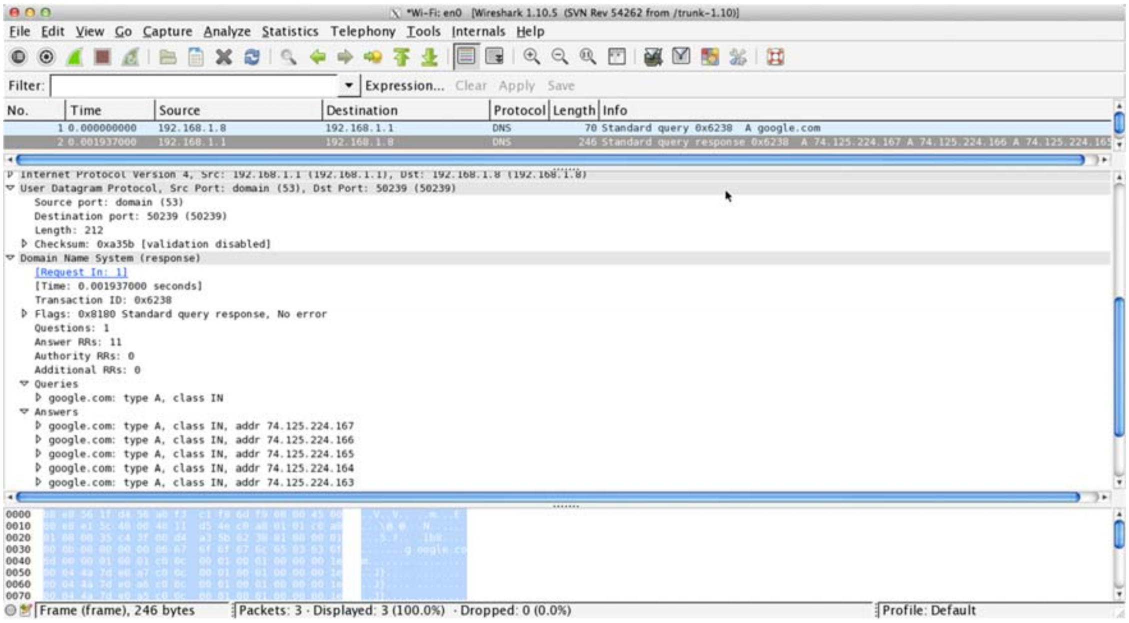
a.



Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. According to above screenshot of ping google.com, at first, the URL google.com was translated to IP address by the DNS, and then my computer sent echo request, the google.com replied the request one by one. That every request was replied means the connection quality is good and the RTT could be calculated based on the ICMP packet.



traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Above screenshot shows the traceroute tool finding out the route from my computer to google.com.



nslookup is a network administration command-line tool available for many computer operating systems for <u>querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record</u>. Above screenshot shows the result of command nslookup google.com. A standard query was sent to the DNS server, and then a standard query response was sent back with google.com's IP address.

b. If the operating system was assigned with a wrong DNS, the following message will be returned when make a ping query:

```
C:\Users\neil>ping google.com
Ping request could not find host google.com. Please check the name and try again
.
```

Therefore, the timeout problem could not be caused by the name server down.

If the ping boy returns timeout, we need to use traceroute tool to dig in the problem. If the traceroute could not reach the boy's IP which returned by DNS query, then the problem should be the intermediate nodes down. Otherwise, the problem is the remote machine "boy" down.

7. Mixed questions:

(a) Give three similarities of Ethernet, fast Ethernet and Gigabit Ethernet, and three differences among them.

(b) Why we need the hardware address, and why we need the IP address. Give three usages of these two addresses.

(c) What ARP stands for? When I use ping, traceroute and nslookup commands, do these commands will invoke ARP? When they will and when they will not?

(d) Can you use PING command only to simulate the function of TRACEROUTE? How? Please give a real example in your virtual machines.

(e) Why you need DNS? If you cannot connect to any DNS server, what you need to know and to do to connect to remote web server?

Answer

a. For 10BASE-T (Ethernet), 100BASE-TX (Fast Ethernet), 1000BASE-T (Gigabit Ethernet), the similarities are they are all use 8P8C connectors, they all support both full-duplex and half-duplex communication, they are all standards under IEEE 802.3.

   The differences could be 10BASE-T and 100BASE-TX only require two of the pairs, but 1000BASE-T uses all four cable pairs for simultaneous transmission in both directions. The speeds are different, 10BASE-T (Ethernet, 10 Mbit/s), 100BASE-TX (fast Ethernet; 100 Mbit/s) and 1000BASE-T (gigabit Ethernet; 1 Gbit/s). 10BASE-T (Ethernet, 10 Mbit/s) could use both Category 3 cable and Category 5 cable, but 1000BASE-T (gigabit Ethernet; 1 Gbit/s) could only use Category 5 cable.

b. A media access control address (MAC address, Hardware Address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model. MAC addresses aren't distributed across the internet in any order that would make them easy to locate with modern routers, thus it is used for communication on the LAN.

   An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there." Routers have routing tables that allow them to summarize what networks are in which direction, therefore when they receive a packet destined to say www.att.com at ip address 23.64.25.145 the routers know where that block of addresses is and send it in the correct direction.

c. Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.

1	0.00000000	Vmware_b4:cb:20	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.11
2	0.00016500	Vmware_b4:cb:20	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.11
3	0.00054200	Tp-LinkT_f8:6d:f9	Vmware_b4:cb:20	ARP	60	192.168.1.1 is at a0:f3:c1:f8:6d:f9
4	0.00055300	192.168.1.11	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
5	0.00137600	192.168.1.11	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
6	0.06541500	8.8.8.8	192.168.1.11	DNS	124	Standard query response 0x0001 PTR google-public-dns-a.go
7	0.06731400	192.168.1.11	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
8	0.06745800	192.168.1.11	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
9	0.11521800	8.8.8.8	192.168.1.11	DNS	246	Standard query response 0x0002 A 74.125.224.38 A 74.125.2
10	0.11634300	192.168.1.11	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
11	0.11650200	192.168.1.11	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
12	0.16957000	8.8.8.8	192.168.1.11	DNS	98	Standard query response 0x0003 AAAA 2607:f8b0:4007:800::1

Above screenshot is for executing command nslookup google.com when ARP table is empty. The first 3 records used ARP to query the Gateway (192.168.1.1)'s MAC address.

For ping, traceroute and nslookup commands, the ARP will be used if it need to communicate with a host in the LAN but the host is not in the ARP table yet. Typically, those commands need to use the MAC address of the Gateway to send out the information on the LAN. The similar things also happen in every LAN which the packets get through, since in the LAN the IP address must be translated to MAC address for delivering the information in LAN.

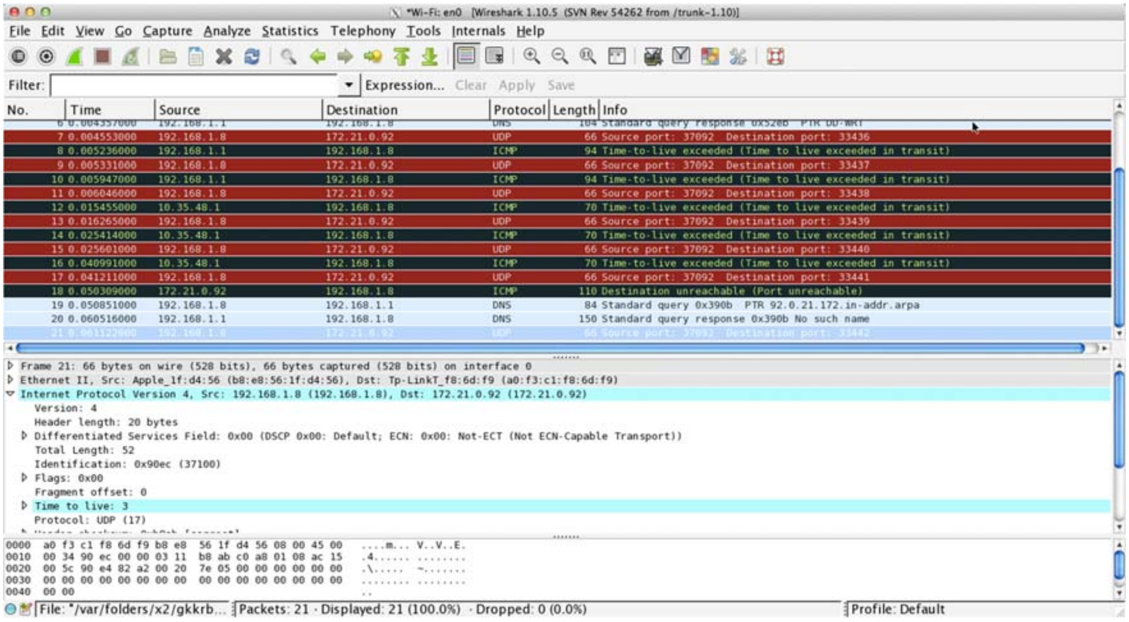
d. At first we need to know how TRACEROUTE works:

Traceroute works by sending packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

binghao — bash — 80×24

```
bings-air:~ binghao$ traceroute 172.21.0.92
traceroute to 172.21.0.92 (172.21.0.92), 64 hops max, 52 byte packets
 1  dd-wrt (192.168.1.1)  2.856 ms  0.724 ms  0.667 ms
 2  10.35.48.1 (10.35.48.1)  9.887 ms  10.455 ms  11.965 ms
 3  172.21.0.92 (172.21.0.92)  14.077 ms *  12.303 ms
bings-air:~ binghao$
```

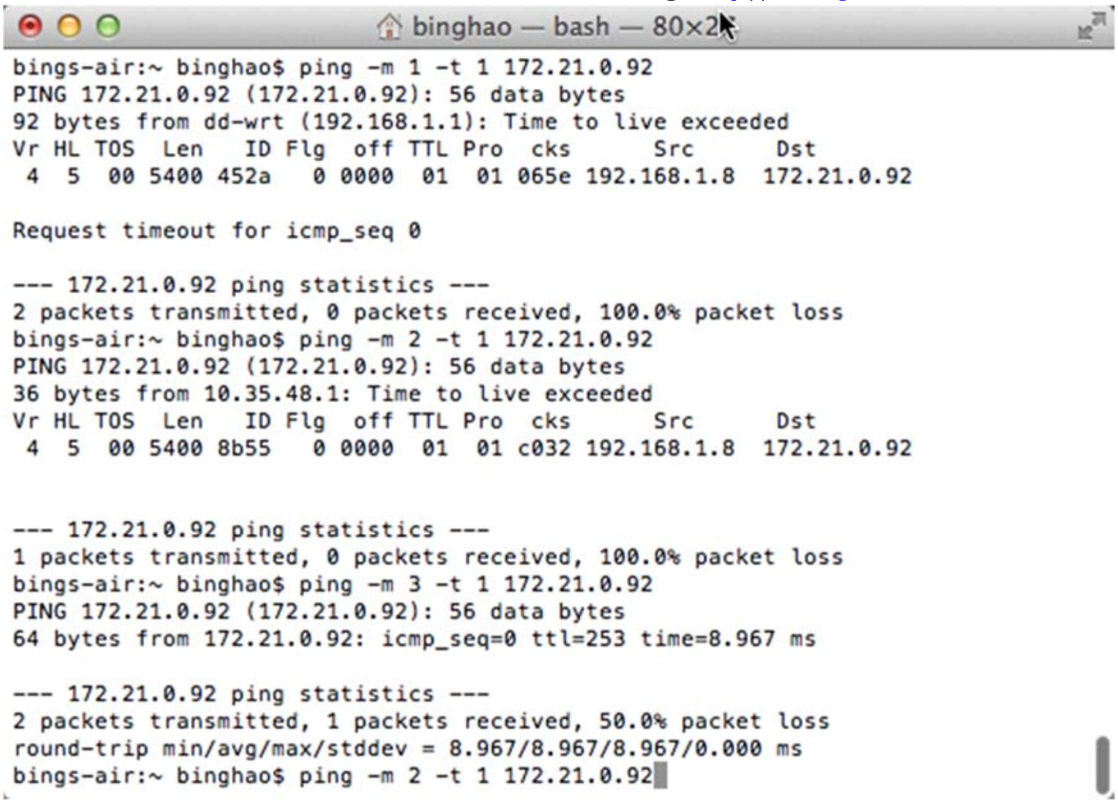
(The traceroute 172.21.0.92 command executing process)



(The wireshark screenshot for the traceroute command executing process)

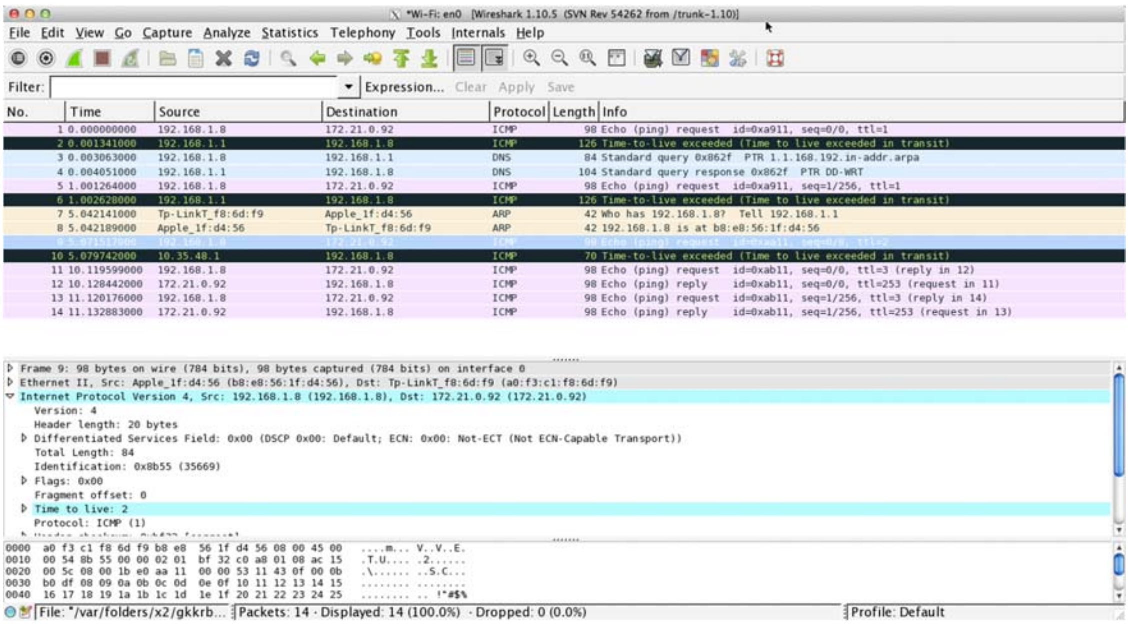
According to above screenshots, at first the traceroute tool sent a UDP packet to 172.21.0.92 with TTL =1, it was abandoned by my router 192.166.1.1, the router replied an ICMP packet which includes its IP address 192.166.1.1. The traceroute tool sent a new UDP packet to 172.21.0.92 with TTL =2, it was abandoned by the 10.35.48.1. Finally, The traceroute tool sent a new UDP packet to 172.21.0.92 with TTL =3, this UDP packet reached the host 172.21.0.92.

Using PING command only to simulate the function of TRACEROUTE:




```
bings-air:~ binghao$ ping -m 1 -t 1 172.21.0.92
PING 172.21.0.92 (172.21.0.92): 56 data bytes
92 bytes from dd-wrt (192.168.1.1): Time to live exceeded
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 5400 452a   0 0000  01  01 065e 192.168.1.8  172.21.0.92

Request timeout for icmp_seq 0

--- 172.21.0.92 ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
bings-air:~ binghao$ ping -m 2 -t 1 172.21.0.92
PING 172.21.0.92 (172.21.0.92): 56 data bytes
36 bytes from 10.35.48.1: Time to live exceeded
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 5400 8b55   0 0000  01  01 c032 192.168.1.8  172.21.0.92


--- 172.21.0.92 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
bings-air:~ binghao$ ping -m 3 -t 1 172.21.0.92
PING 172.21.0.92 (172.21.0.92): 56 data bytes
64 bytes from 172.21.0.92: icmp_seq=0 ttl=253 time=8.967 ms

--- 172.21.0.92 ping statistics ---
2 packets transmitted, 1 packets received, 50.0% packet loss
round-trip min/avg/max/stddev = 8.967/8.967/8.967/0.000 ms
bings-air:~ binghao$ ping -m 2 -t 1 172.21.0.92
```

(Ping 172.21.0.92 three times with different TTL values, 1,2 and 3)



(The wireshark screenshot for the Ping 172.21.0.92 commands executing process)

According to above screenshots, the first ping sent an ICMP packet to 172.21.0.92 with TTL =1, it was abandoned by my router 192.166.1.1, the router replied an ICMP packet which includes its IP address 192.166.1.1. The second ping sent a new ICMP packet to 172.21.0.92 with TTL =2, it was abandoned by the 10.35.48.1. Finally, The third ping sent a new ICMP packet to 172.21.0.92 with TTL =3, this UDP packet reached the host 172.21.0.92.

e. The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide.

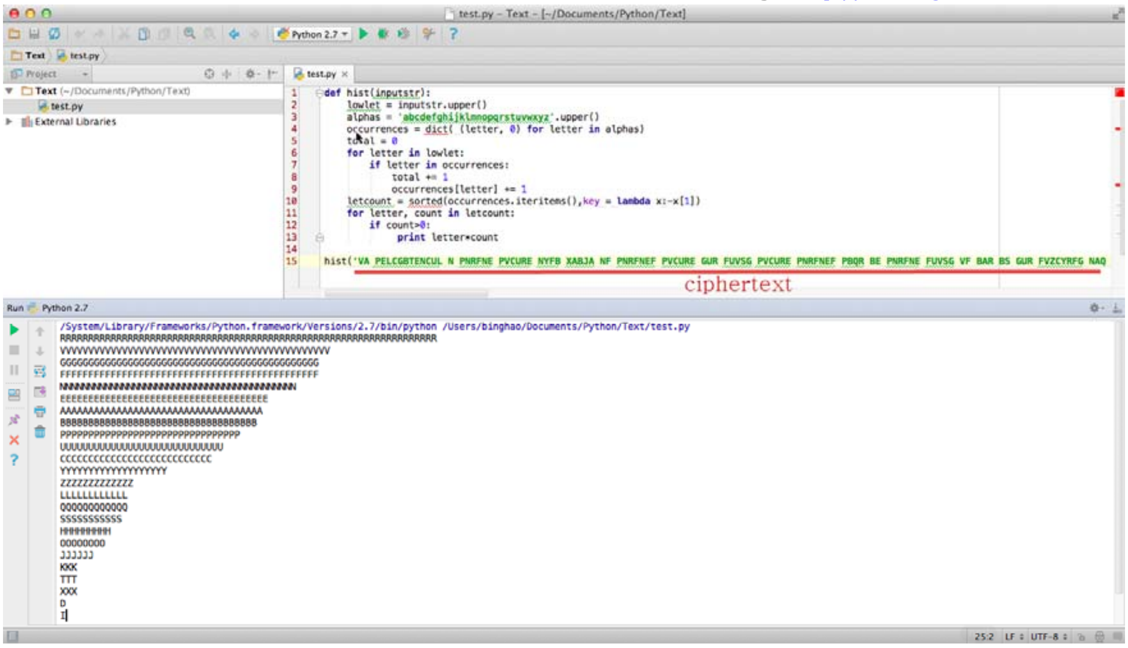
If I cannot connect to connect to any DNS server, then I have to know the web server's IP address to connect to it.
For example:

If I cannot connect to connect to any DNS server, then google.com could not be translated to 74.125.224.36. I have to access 74.125.224.36 directly.

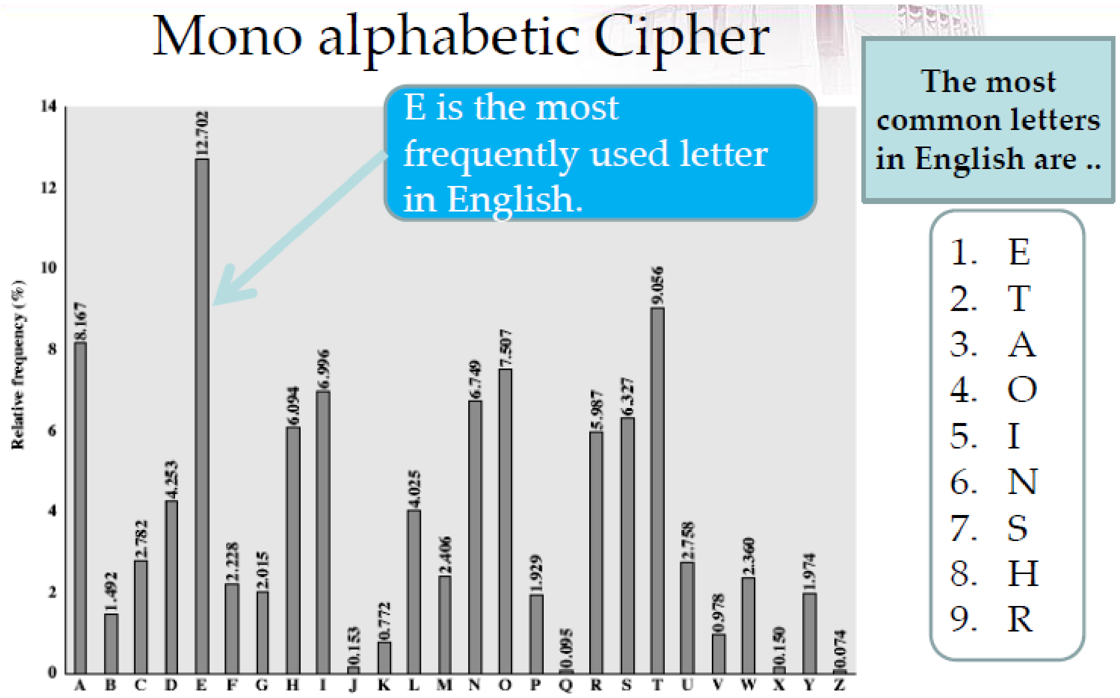
8. Please decrypt the following ciphertext to plaintext, describe your approach in detail.

VA PELCGBTENCUL N PNRFNE PVCURE NYFB XABJA NF PNRFNEF PVCURE GUR FUVSG PVCURE PNRFNEF PBQR BE PNRFNE FUVSG VF BAR BS GUR FVZCYRFG NAQ ZBFG JVQRYL XABJA RAPELCGVBA GRPUAVDHRF VG VF N GLCR BS FHOFGVGHGVBA PVCURE VA JUVPU RNPU YRGGRE VA GUR CYNVAGRKG VF ERCYNPRQ OL N YRGGRE FBZR SVKRQ AHZORE BS CBFVGVBAF QBJA GUR NYCUNORG GUR RAPELCGVBA FGRC CRESBEZRQ OL N PNRFNE PVCURE VF BSGRA VAPBECBENGRQ NF CNEG BS ZBER PBZCYRK FPURZRF FHPU NF GUR IVTRARER PVCURE NAQ FGVYY UNF ZBQREA NCCYVPNGVBA VA GUR EBG13 FLFGRZ NF JVGU NYY FVATYR NYCUNORG FHOFGVGHGVBA PVCUREF GUR PNRFNE PVCURE VF RNFVYL OEBXRA NAQ VA ZBQREA CENPGVPR BSSREF RFFRAGVNYYL AB PBZZHAVPNGVBA FRPHEVGL

Answer

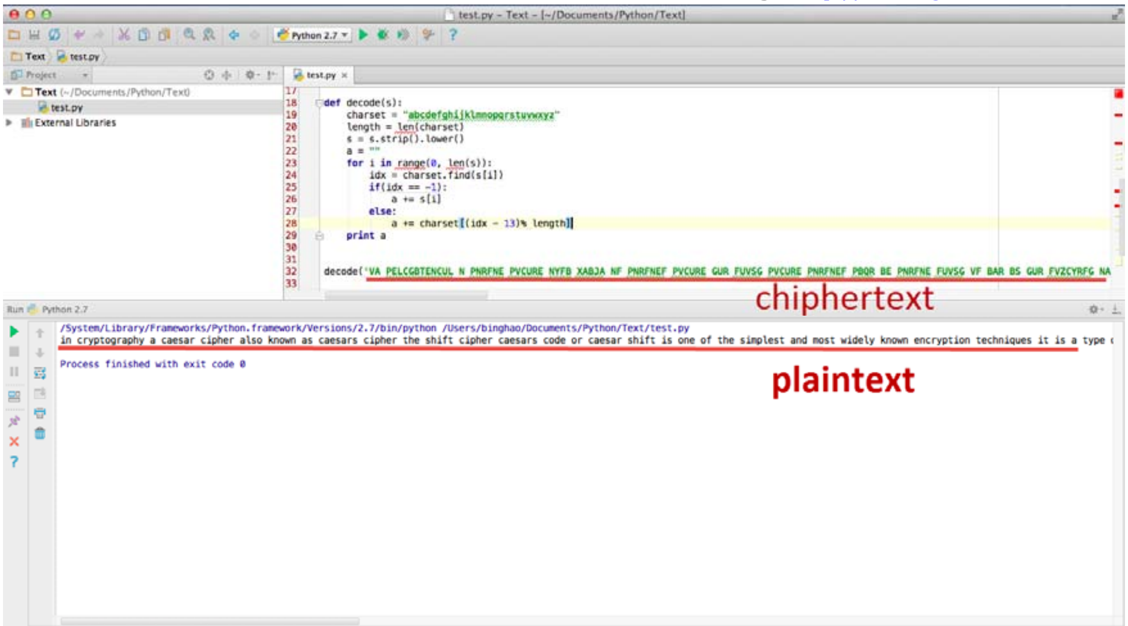


I used a python program to do the letters frequency computation for the chiphertext. According following table of the most common letters in English:



At first, I assume R -> E. The difference between R and E is 13.

Let us write a program to shift all letters by 13:



The plaintext is:

in cryptography a caesar cipher also known as caesars cipher the shift cipher caesars code or caesar shift is one of the simplest and most widely known encryption techniques it is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet the encryption step performed by a caesar cipher is often incorporated as part of more complex schemes such as the vigenere cipher and still has modern application in the rot13 system as with all single alphabet substitution ciphers the caesar cipher is easily broken and in modern practice offers essentially no communication security