# Problem Set #2_Solutions

**Problem 1 (6 points)**

(a) Is 20.20.0.255/255.255.254.0 a valid IP address for a host? **[1pt]**
(b) Divide the 20.20.0.0/16 subnets into 10 large networks of 4096 IPs each, 16 medium-sized networks of 1024 IPs each, and 10 small sized networks of 128 IPs each. **[4pt]**
(c) Is 192.168.2/23 and 192.168.3/23 representing the same subnet? Please justify your answer. **[1pt]**

Solution

(a) Yes, it is a valid address for hosts
(b)

10 subnets of 4096 IPs
16 subnets of 1024 IPs
10 subnets of 128 IPs

We start with large subnets

20.20.0.0/20
20.20.16.0/20
20.20.32.0/20
20.20.48.0/20
20.20.64.0/20
20.20.80.0/20
20.20.96.0/20
20.20.112.0/20
20.20.128.0/20
20.20.144.0/20

Then work on subnets of 1024 IPs

20.20.160.0/22
20.20.164.0/22
20.20.168.0/22
20.20.172.0/22
20.20.176.0/22
20.20.180.0/22
20.20.184.0/22
20.20.188.0/22
20.20.192.0/22
20.20.196.0/22
20.20.200.0/22
20.20.204.0/22

20.20.208.0/22
20.20.212.0/22
20.20.216.0/22
20.20.220.0/22

Then work on subnets of 128 IPs

20.20.224.0/25
20.20.224.128/25
20.20.225.0/25
20.20.225.128/25
.
.
.
20.20.228.128/25

OR

20.20.240.0/25
20.20.240.128/25
20.20.241.0/25
20.20.241.128/25
.
.
.
20.20.244.128/25

(c) they do represent the same subnet of 192.168.2.0-192.1683.255

**Problem 2 (5 points)**

An organization has been assigned the prefix 212.1.0.0/23 and wants to form subnets for 4 departments which have the following number of hosts:

| | |
|---|---|
| Department A: | 140 hosts |
| Department B: | 124 hosts |
| Department C: | 62 hosts |
| Department D: | 31 hosts |

(a) Give a possible arrangement of subnet masks to make this possible. **[4pt]**
(b) Suggest what the organization might do if department C grows to 65 hosts. **[1pt]**

Solution:

(a)
A: 256 IPs subnet
B:128 IPs subnet
C:64 IPs subnet
D:64 IPs subnet(32IPs subnet can only support 30 hosts)
Ip range is 212.1.0.0-212.1.1.255
So
A: 212.1.0.0/24
B:212.1.1.0/25
C:212.1.1.128/26
D:212.1.1.192/26

(b) In this case, C need a 128 subnet, but there are no enough IP to do this, so the organization either can apply for more ip addresses or use private ip address space.

**Problem 3 (12 points)**

For the network given below in Figure. 1, give global distance-vector tables like those on textbook Table 3.10, 3.13 **WHEN:**

(a) Each node knows only the distance of its immediate neighbors. **[4pt]**
(b) Each node has reported the information it had in the preceding step to its immediate neighbors. **[4pt]**
(c) Repeat step (b) one more time. **[4pt]**

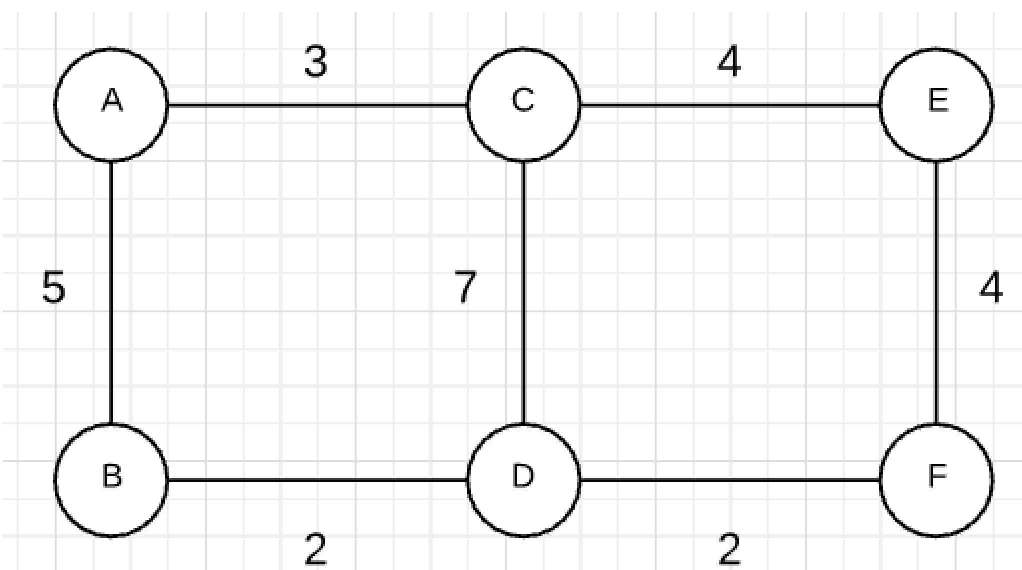



Figure. 1

Solution:

(a)

| | Distance to reach Node | | | | | |
|---|---|---|---|---|---|---|
| | A | B | C | D | E | F |
| A | 0 | 5 | 3 | Inf. | Inf. | Inf. |
| B | 5 | 0 | Inf. | 2 | Inf. | Inf. |
| C | 3 | Inf. | 0 | 7 | 4 | Inf. |
| D | Inf. | 2 | 7 | 0 | Inf. | 2 |
| E | Inf. | Inf. | 4 | Inf. | 0 | 4 |
| F | Inf. | Inf. | Inf. | 2 | 4 | 0 |

**(b)**

| | Distance to reach Node | | | | | |
|---|---|---|---|---|---|---|
| | A | B | C | D | E | F |
| A | 0 | 5 | 3 | 7 | 7 | Inf. |
| B | 5 | 0 | 8 | 2 | Inf. | 4 |
| C | 3 | 8 | 0 | 7 | 4 | 8 |
| D | 7 | 2 | 7 | 0 | 6 | 2 |
| E | 7 | Inf. | 4 | 6 | 0 | 4 |
| F | Inf. | 4 | 8 | 2 | 4 | 0 |

**(c)**

| | Distance to reach Node | | | | | |
|---|---|---|---|---|---|---|
| | A | B | C | D | E | F |
| A | 0 | 5 | 3 | 7 | 7 | 9 |
| B | 5 | 0 | 8 | 2 | 8 | 4 |
| C | 3 | 8 | 0 | 7 | 4 | 8 |
| D | 7 | 2 | 7 | 0 | 6 | 2 |
| E | 7 | 8 | 4 | 6 | 0 | 4 |
| F | 9 | 4 | 8 | 2 | 4 | 0 |

**Problem 4 (6 points)**

Again for the network graph in Figure. 1. Show how the link-state algorithm builds the routing table for node D.

(a) Show the detailed link-state algorithm. **[5pt]**

(b) Show the final routing table of node D. **[1pt]**

Solution:

In the beginning all

Node D use Dijkstra's Algorithm to build its routing table.

So:

Initialization:

D is starting node N' = {D}

B,C,F are D's neighbors

d(A,B,C,D,E,F) = (INF,2,7,0,INF,2)

Iteration 1:

Add B to N' since d(B)= 2 is smallest,N'={B,D}

d(A,B,C,D,E,F)=(7,2,7,0,INF,2)

Iteration 2:

Add F to N'     N'=[B, D, F]

d(A,B,C,D,E,F)=(7,2,7,0,6,2)

Iteration 3:

Add E to N'     N'=[B, D, E, F]

d(A,B,C,D,E,F)=(7,2,7,0,6,2)

Iteration 4:

Add  A to N'     N'=[A, B, D, E, F]

d(A,B,C,D,E,F)=(7,2,7,0,6,2)

Iteration 5:

Add C to N'     N'=[A,B,C,D,E,F]

d(A,B,C,D,E,F)=(7,2,7,0,6,2)

N' now contains all nodes, the algorithm is complete

| Destination | Next-hob | distance |
|---|---|---|
| A | B | 7 |
| B | B | 2 |
| C | C | 7 |
| E | F | 6 |
| F | F | 2 |

**Problem 5 (10 points)**

(a) Give Names of two Distance Vector Routing Protocols **[1pt]**
(b) Give names of two link-state routing protocols. **[1pt]**
(c) What is the main difference between these two types of protocols. **[2pt]**
(d) Comment on scalability, convergence time, computation overhead of these two types. **[2pt]**
(e) Which type do you think is more suitable for the scale of Internet level network, explain your answer. Give name of the popular protocol that is used by the Internet routers. **[4pt]**

Solution:

(a) RIP (both versions, in case someone mentions versions), IGRP, EIGRP.
(b) OSPF, IS-IS
(c) In Distance vector protocol, a router has a knowledge of neighbor's distance to the destinations and it believes the routing decisions sent by the neighbor. So basically, a routing by rumor. Whereas in the case of Link-state, each router has a knowledge of every router's links. It has a complete view of the topology, then it runs shortest path algorithm like Dijkstra's algorithm and computes the best path on its own.

    If people mention some other differences like frequency of updates, algorithm used, convergence time or computational complexity, give 1 point only.

(d) Scalability: Link state is not scalable because huge amount of information is transferred between each router. Thus, in larger networks, too much information will be sent over a network thus not scalable. However, in case of Distance Vector, less information is sent to neighbor router. Thus, it is more scalable protocol.

    Convergence time: In link state, Updates are sent immediately. Thus, changes are communicated faster and network converges faster. In Distance vector, updates are periodic. Thus, it takes more time to converge.

    Computation overhead: Link state requires too much processing power since it has to process all the information and calculate best paths. However, in DV, each router has to do less processing and has to just believe the information sent by its neighbor. Thus, overall overhead is less.
(e) Distance Vector is in right direction. (Students must explain it) Main reasons are Scalability and Less computational overhead which is necessary for router internet routers. Popular protocol: BGP

**Problem 6 (5 points)**

Consider this directional graph below in Figure 4. Use Dijkstra's algorithm to find the shortest path from node v3 to v5. Write down the **steps**. Do you have any comments on the result?

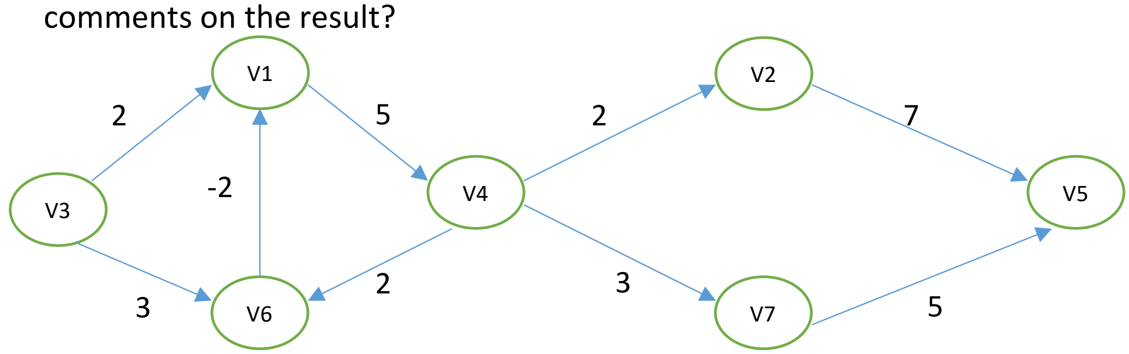



Figure. 4

Solution:

Initialization

N' = {V3}

D(V1,V2,V3,V4,V5,V6,V7)=(2,INF,0,INF,INF,3,INF)

Iteration1: Include V1

N'={V1,V3}

D(V1,V2,V3,V4,V5,V6,V7)=(2,INF,0,7,INF,3,INF)

Iteration2: Include V6

N'={V1,V3,V6}

D(V1,V2,V3,V4,V5,V6,V7)=(2,INF,0,7,INF,3,INF)

NOTE: although V6 have a negative link, but since it points into the set N', so it will not be used, because nodes inside N' will not get updates according to Dijkstra's algorithm

Iteration3: Include V4

N'={V1,V3,V4,V6}

D(V1,V2,V3,V4,V5,V6,V7)=(2,9,0,6,INF,3,10)

Iteration 4: Include V2

N'={V1,V2,V3,V4,V6}

D(V1,V2,V3,V4,V5,V6,V7)=(2,9,0,6,16,3,10)

Iteration 5: Include V7

N'={V1,V2,V3,V4,V6,V7}

D(V1,V2,V3,V4,V5,V6,V7)=(2,9,0,6,15,3,10)

So the final route by Dijkstra's algorithm is V3-V1-V4-V2-V5 which is not the optimal.
The optimal is: V3-V6-V1-V4-V2-V5
This is because Dijkstra's algorithm may not generate correct result if negative links are involved.

**Problem 7 (7 points)**

(a) What is the difference between CSMA/CD and CSMA/CA [3 points]
(b) Why is collision detection more complex in wireless networks such as 802.11 compare to wired networks such as Ethernet. [2 points]
(c) How can hidden terminals be detected in 802.11 networks? Explain how it works. [2 points]

Solution

(a) CSMA CA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it. CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission and again it starts listening whether any data transmitting or not .

(b) This is the case in the hidden node problem, illustrated in Figure 2.30, in which A interferes with C's communication to B, and C interferes with A's communication to B.

(c) 802.11 uses the RTS-CTS mechanism to try to address hidden terminals. A node that has data to send begins by sending a short RTS packet indicating that it would like to send data, and the receiver responds with a CTS, which is also likely to be received by nodes that are in reach of the receiver but hidden from the sender. While this doesn't prevent collisions, the fact that RTS and CTS are short packets makes collisions less likely.

**Problem 8 (8 points)**

The network graph is shown in Figure. 2.

(a) Host H1 sends a packet to the destination 128.96.34.126. Explain how this packet traverses in the network described below. You need to describe who received the packet and what are their reactions. **[2pt]**

(b) Host H3 sends a packet to the destination 128.96.34.250. Explain how this packet traverses in the network. **[3pt]**

(c) The subnet of H1 has now two different teams and would like to split it into two subnets. Please add one more subnet and add R3 and change the network configurations as you need. Note that you are allowed to modify the network as least disruptive as possible. **[3pt]**

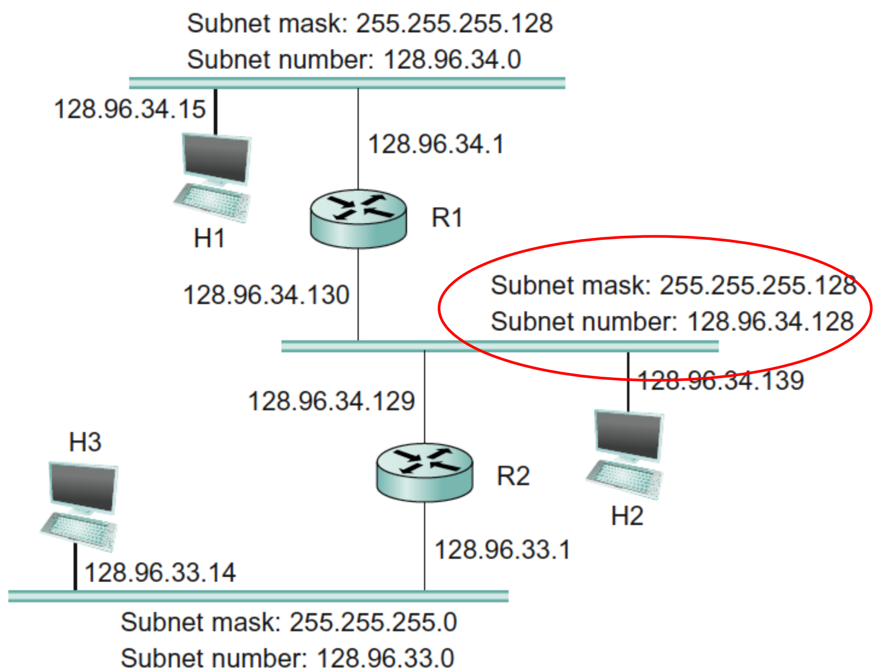


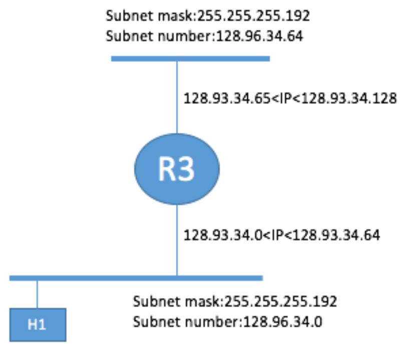

Figure 2.

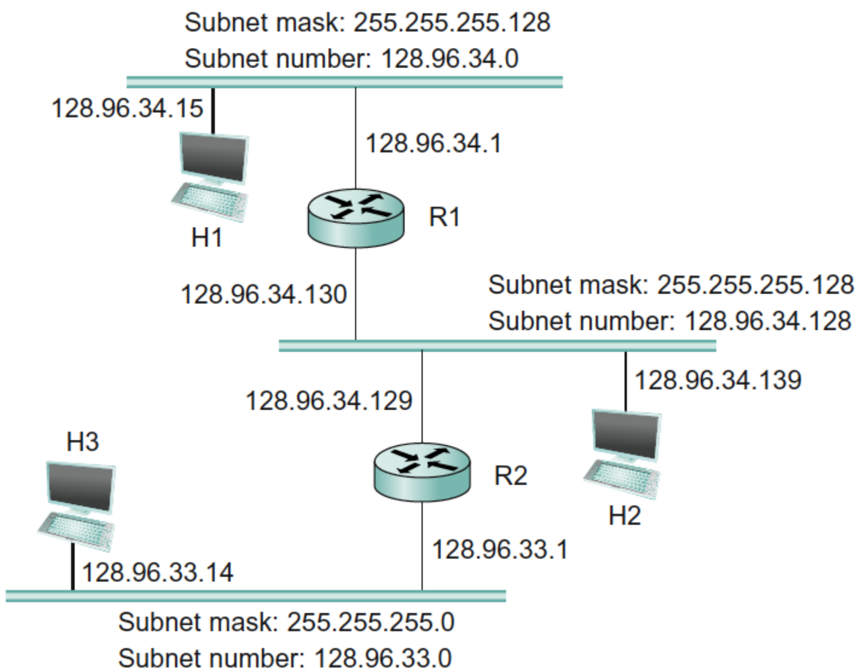
Solution

(a) The packet will reach destination at local Ethernet. Although R1 received the packet, R1 will not forward it, because R1 knows it belongs to local Ethernet.

(b) The destination belongs to the subnet in RED CIRCLE.
R2 will forward this packet to the next port connects to RED CIRCLE.
At this time the packet's source MAC will change to R2's MAC
The packet will reach the destination in the subnet marked by the red circle
R1 will hear this packet but will not forward it.

(c) The subnet of H1 will change to 128.93.34.0/255.255.255.192
Another Router R3 will connect the Ethernet with 128.93.34.0<IP<128.93.34.64
On the other side of R3 will have 128.93.34.65<ip<128.93.34.128 and with subnet 128.93.34.64/255.255.255.192 connected


Subnet mask:255.255.255.192
Subnet number:128.96.34.64
128.93.34.65<IP<128.93.34.128
R3
128.93.34.0<IP<128.93.34.64
H1
Subnet mask:255.255.255.192
Subnet number:128.96.34.0


Subnet mask: 255.255.255.128
Subnet number: 128.96.34.0
128.96.34.15
128.96.34.1
R1
H1
128.96.34.130
Subnet mask: 255.255.255.128
Subnet number: 128.96.34.128
128.96.34.129
128.96.34.139
H3
R2
H2
128.96.33.1
128.96.33.14
Subnet mask: 255.255.255.0
Subnet number: 128.96.33.0

**Problem 9 (8 points)**

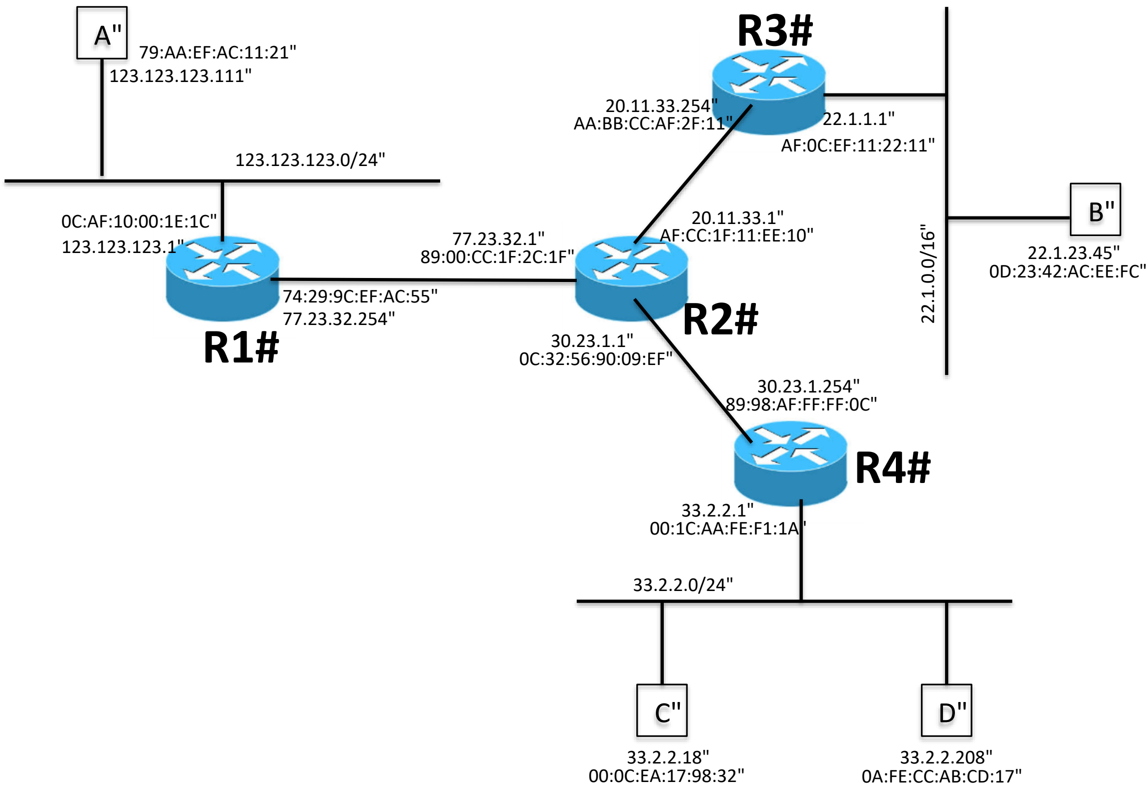



Figure. 3

Above in Figure 3 is the network graph with 4 routers (R1, R2, R3, R4) and 4 hosts (A, B, C, D). Each router interfaces and hosts are labeled with both IP and MAC address, Routing is enabled so that any two hosts can communicate with each other and also the default gateway of each host is set to its gateway router.

(a) Suppose that B send an IP packet to C through R1, R2, R4. Write down the IP packet's content (src MAC, dst MAC, src IP, dst IP) along the path in the Table given below: **[8pt]**

Solution

| | src MAC | dst MAC | src IP | dst IP |
|---|---|---|---|---|
| A-> R1 | A MAC | R1 MAC | A IP | D IP |
| R1 -> R2 | R1 MAC | R2 MAC | A IP | D IP |
| R2 -> R4 | R2 MAC | R4 MAC | A IP | D IP |
| R4 -> D | R4 MAC | D MAC | A IP | D IP |

**Problem 10 (5 points)**

Suppose a router has built up the routing table shown in the Table 2 shown below. The router can deliver packets directly over interfaces 0 and 1, or it can forward packets to routers R2, R3, or R4. Assume the router does the longest prefix match. Describe what the router does with a packet addressed to each of the following destinations:

(a) 128.96.171.92.

(b) 128.96.167.151.

(c) 128.96.163.151.

(d) 128.96.169.192

(e) 128.96.165.121

**Table 3**

| SubnetNumber | SubnetMask | NextHop |
|---|---|---|
| 128.96.170.0 | 255.255.254.0 | Interface 0 |
| 128.96.168.0 | 255.255.254.0 | Interface 1 |
| 128.96.166.0 | 255.255.254.0 | R2 |
| 128.96.164.0 | 255.255.252.0 | R3 |
| _default_ | | R4 |

(a) Applying the subnet mask 255.255.254.0, we get 128.96.170.0. Use interface 0 as the next hop.

(b) Applying subnet mask 255.255.254.0, we get 128.96.166.0 (next hop is Router 2). Applying subnet mask 255.255.252.0, we get 128.96.164.0 (next hop is Router 3). However, 255.255.254.0 is a longer prefix. Use Router 2 as the next hop.

(c) None of the subnet number entries match, hence use default Router R4.

(d) Applying subnet mask 255.255.254.0, we get 128.96.168.0. Use interface 1 as the next hop.

(e) Applying subnet mask 255.255.252.0, we get 128.96.164.0. Use Router 3 as the next hop

**Problem 11 (8 points)**

Consider the simple network in Figure 5 below, X, Y and Z are switches and link cost as specified. Assume Distance Vector algorithm is used and have converged. Now Y's and Z's Routing table will look like Table. 3.

(a) Now Let assume the cost of link X-Y suddenly changed to 60. Please write down the Y's and Z's routing table regarding distance to X, after Y updates this information to Z and then Z updates its information back. **[2pt]**
(b) Please write down the Y's and Z's routing table regarding X after Y updates this information to Z again and then Z updates back again. **[2pt]**
(c) How many updates did Y get until its distance to X have converged with Distance Vector algorithm? **[4pt]**

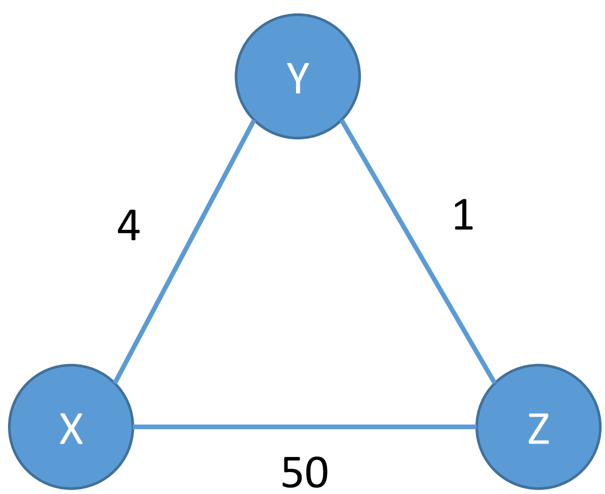



Figure. 5

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 4 | 6 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 5 |

**Solution:**

(a)

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 60 | 8 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 7 |

(b)

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 60 | 10 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 9 |

(c) 1st update we got x via z =8.

2nd update we got x via z = 10

22th update we got

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 60 | 50 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 49 |

23th update we got

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 60 | 51 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 51 |

Then Y update its information to Z, and the status converges as below:

| Node Y/Distance | Via X | Via Z |
|---|---|---|
| X | 60 | 51 |
| | | |
| Node Z/Distance | Via X | Via Y |
| X | 50 | 52 |

So the answer is 23

**Problem 12: (20 Points) Wireshark Exercise.**

(a) If everything went correctly, your Wireshark capture should have a copy of all protocols mentioned before. Using Wireshark answer the following questions by inserting a small screenshot of your findings for each: **[10 points]**

- What is the MAC address of your PC?
- What is the IP address of your Default gateway? What is its MAC address?
- What is the IP address was given to your PC via DHCP?
- Who is your DNS Server?
- What protocol is used by your web browser? What port numbers it uses?
- What is the IP address of the server hosting [www.colorado.edu](http://www.colorado.edu)?
- What other application protocols did Wireshark captured? (Other than http)

**(b)** Explain the steps involved after you turn on the adapter till the web page for e.g. [www.yahoo.com](http://www.yahoo.com) is rendered on the browser. What is the order of operation between all protocols? What happened first, second, third and so on? (hint: Wireshark captures them sequentially). Explain what did each one of the protocols do to serve your basic web browsing request? **[10 Points]**

DHCP Process → ARP→DNS→HTTP request →HTTP response

DHCP: Used to learn the IP address, Subnet, Default gateway, DNS server's address.

ARP: To learn the MAC address of default gateway. PC knows the IP address of the default gateway. ARP finds out the corresponding MAC address so that ethernet packet can be forwarded. (This is done to send packet for a DNS request, but it will have to reach default gateway first. Thus, first ARP will be used to reach default gateway)
(2 points)

DNS: Since the computer doesn't know the IP address of www.yahoo.com, it sends a DNS query to the DNS server IP obtained from DHCP server. It receives the IP address for www.yahoo.com from the DNS server. (2 points)

Then HTTP request is sent to the destination IP address and correct port number.
It receives the HTTP response packet containing the webpage and displays it in the browser. (1 point)