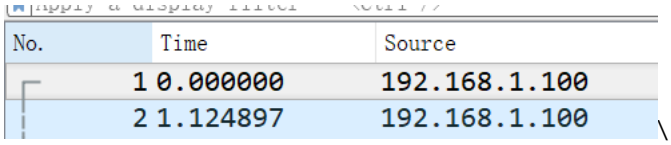
Exercise 1:

Question 1: What is the IP address of the client?

Answers:

The IP address of the client is **192.168.1.100.**

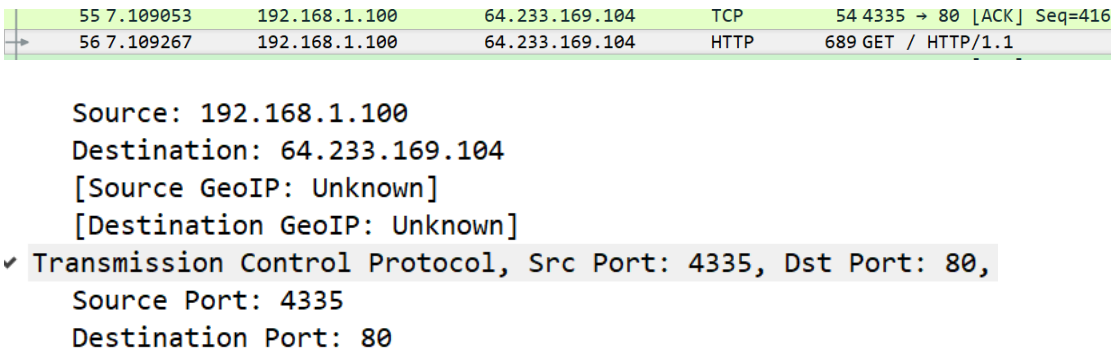


No.	Time	Source
1	0.000000	192.168.1.100
2	1.124897	192.168.1.100

Question 2: Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Answers:

Source IP Address: **192.168.1.100**, Port: **4335**
Destination IP Address: **64.233.169.104**, Port: **80**



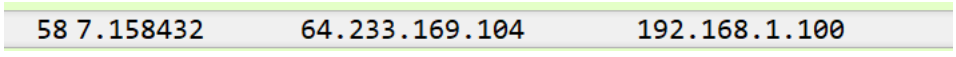
55	7.109053	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=416
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1

```
    Source: 192.168.1.100
    Destination: 64.233.169.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ Transmission Control Protocol, Src Port: 4335, Dst Port: 80,
    Source Port: 4335
    Destination Port: 80
```

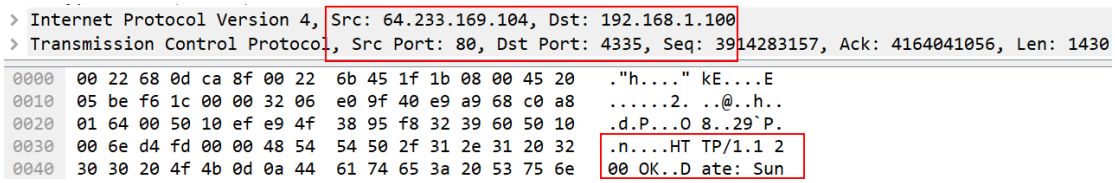
Question 3: At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Answers:

Time of the corresponding 200 OK HTTP message: **7.158432** seconds
Source IP Address: **64.233.169.104**, Port: **80**
Destination IP Address: **192.168.1.100**, Port: **4335**



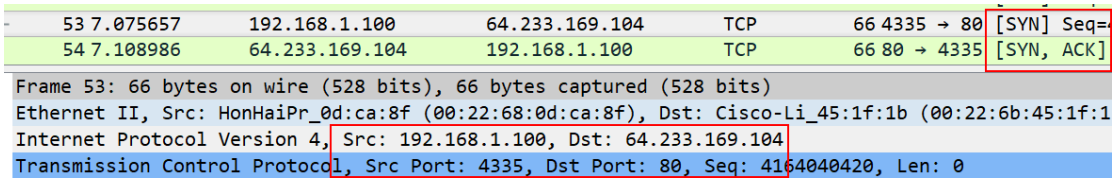
58	7.158432	64.233.169.104	192.168.1.100



Question 4: Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

Answers:

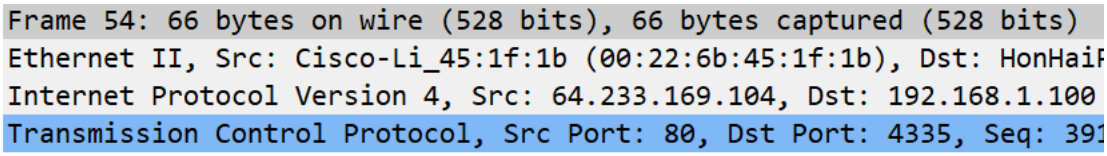
Time: **7.075657** seconds
Source IP Address: **192.168.1.100**, Port: **4335**
Destination IP Address: **64.233.169.104**, Port: **80**



Question 5: What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client?

Answers:

Source IP Address: **64.233.169.104**, Port: **80**
Destination IP Address: **192.168.1.100**, Port: **4335**
Time: **7.108986** seconds

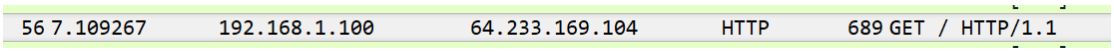


Question 6: At what time does this message appear in the NAT_ISP_side trace file?

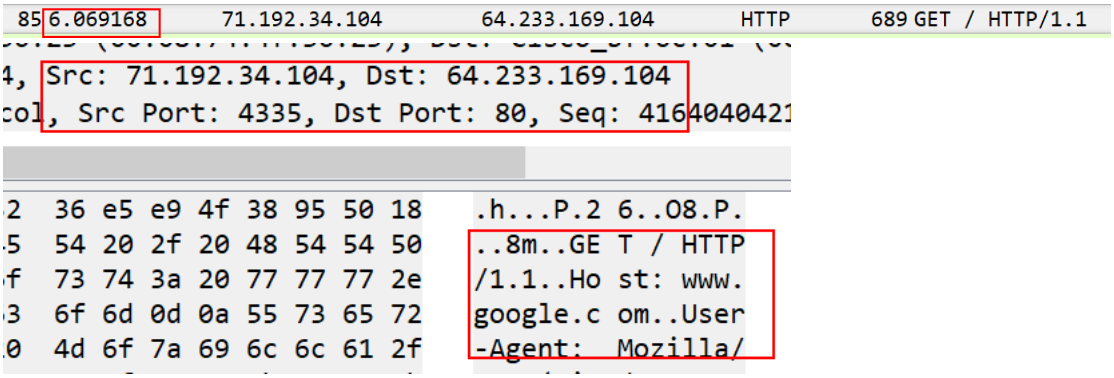
Answers:

Time: **6.069168** seconds

In the NAT_home_side trace file



In the NAT_ISP_side trace file



Question 7: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?

Answers:

Source IP Address: **71.192.34.104,** Port: **4335**
Destination IP Address: **64.233.169.104**, Port: **80**
Compare with the fields of Question 2, **source IP address** is different.

Question 8: Are any fields in the HTTP GET message changed?

Answers:

HTTP GET message has **not changed.**

Question 9: Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Answers:

Version and Header Length, Flags have **not** changed.
Header checksum changed from **0xa94a (Home)** to **0x022f (ISP)**. Because source IP address has changed from 192.168.1.100 to 71.192.34.10. (**Time to live**, **source IP address** has changed.)

In the NAT_home_side trace file

Wireshark · Packet 56 · NAT_home_side

```
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]
```

In the NAT_ISP_side trace file

Wireshark · Packet 85 · NAT_ISP_side

```
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c
v Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]
```

Question 10: In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

Answers:

Time: **6.117078** seconds.

```
88 6.117078    64.233.169.104    71.192.34.104    TCP    1484 80 → 4335 [ACK]
89 6.
90 6.
91 6.
93 6.
94 6.
95 6.
96 6.
```

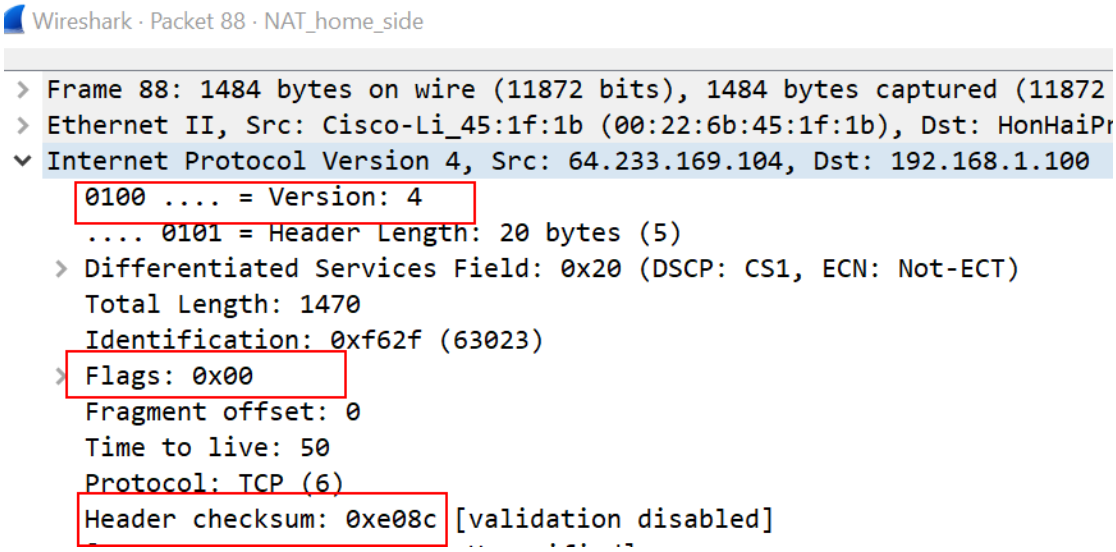
Wireshark · Packet 88 · NAT_ISP_side

```
0000  00 08 74 4f 36 23 00 0e  d6 bf 6c 01 08 00 45 20   ..tO6#.. ..l...E
0010  05 be f6 1c 00 00 33 06  37 84 40 e9 a9 68 47 c0   ......3. 7.@..hG.
0020  22 68 00 50 10 ef e9 4f  38 95 f8 32 39 60 50 10   "h.P...O 8..29`P.
0030  00 6e 2c e2 00 00 48 54  54 50 2f 31 2e 31 20 32   .n,...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 75 6e   00 OK..D ate: Sun
```

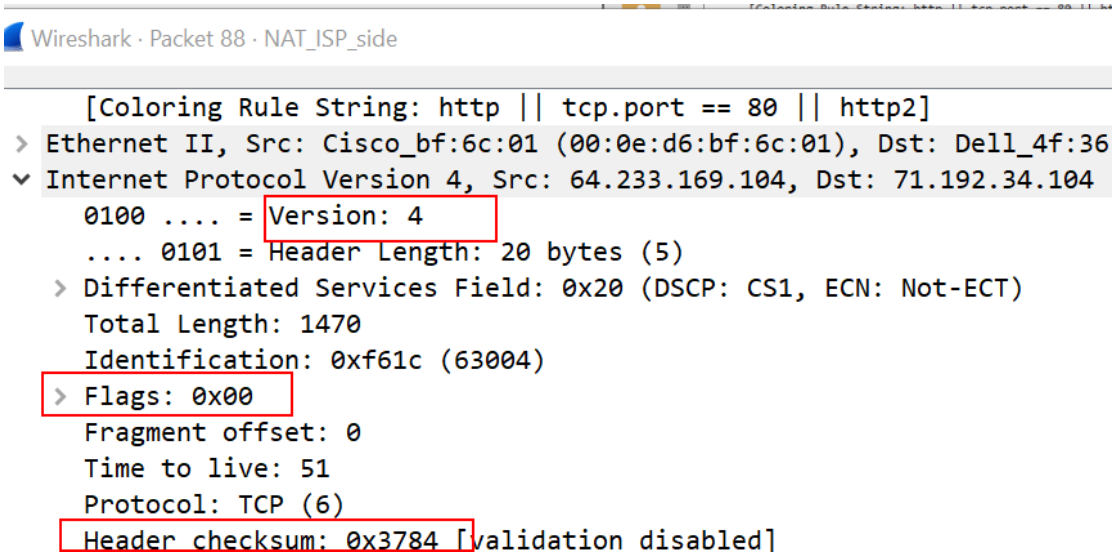
Question 11: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?

Answers:

Source IP Address**: 64.233.169.104,** port**: 80**
Destination IP Address**: 71.192.34.104,** port**: 4335**
Destination port, source IP address and port has not changed
(Version and Flags have not changed.)
Destination IP address has changed
(Header checksum, Time to live have changed.)
In the NAT_home_side trace file:



In the NAT_ISP_side trace file:



Question 12: In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in Question 4 and 5 above captured?

Answers:

SYN time: 6.035475 seconds
ACK time: 6.067775 seconds.

82	6.035475	71.192.34.104	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=416
83	6.067775	64.233.169.104	71.192.34.104	TCP	66 80 → 4335 [SYN, ACK] Se

Question 13: What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?

Answers:

SYN :
Source IP Address**: 71.192.34.104,** ports**: 4335**
Destination IP Address**: 64.233.169.104,** ports**: 80**
Destination IP address, port and **Source** port has not changed.
Source IP address has changed.
(Time to live, Header checksum have changed.)

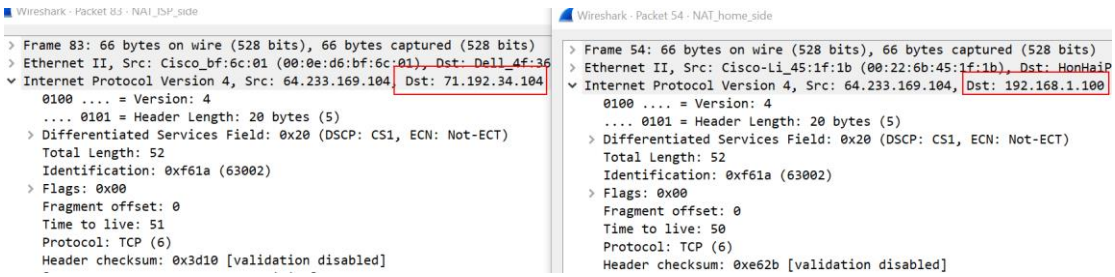
Wireshark · Packet 53 · NAT_home_side

```
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:
Internet Protocol Version 4, Src: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: C
    Total Length: 52
    Identification: 0xa2aa (41642)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xabbb [validation disabled
    [Header checksum status: Unverified]
    Source: 192.168.1.100
```

Wireshark · Packet 82 · NAT_ISP_side

```
    [Coloring Rule String: http || tcp.port =
  > Ethernet II, Src: Dell_4f:36:23 (00:08:74:4
  v Internet Protocol Version 4, Src: 71.192.34
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP
      Total Length: 52
      Identification: 0xa2aa (41642)
    > Flags: 0x02 (Don't Fragment)
      Fragment offset: 0
      Time to live: 127
      Protocol: TCP (6)
      Header checksum: 0x04a0 [validation disab
      [Header checksum status: Unverified]
```

ACK:
Source IP Address**: 64.233.169.104,** ports**:80**
Destination IP Address**: 71.192.34.104,** ports**: 4335**
Source IP address, port and **Destination** port has not changed.
Destination IP address has changed.
(Time to live, Header checksum have changed.)



Question 14: The discussion on NAT in the Week 8 lecture slides shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.

Answers:

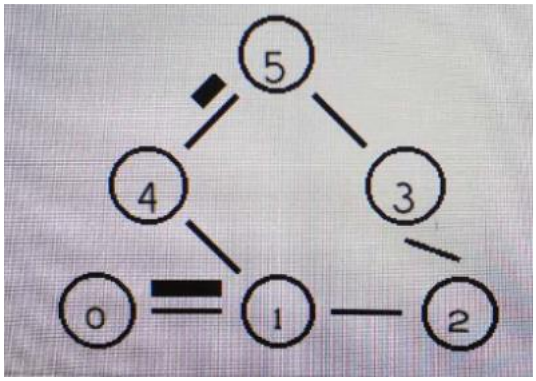
NAT translation table	
WAN side address, port	**LAN side address, port**
71.192.34.104,4335	**192.168.1.100,4335**

Exercise 2:

Question 1: Which nodes communicate with which other nodes? Which route do the packets follow? Does it change over time?

Answers:

Node 0 send packet to node 5. The route of packet is 0-1-4-5 and does not change over time.

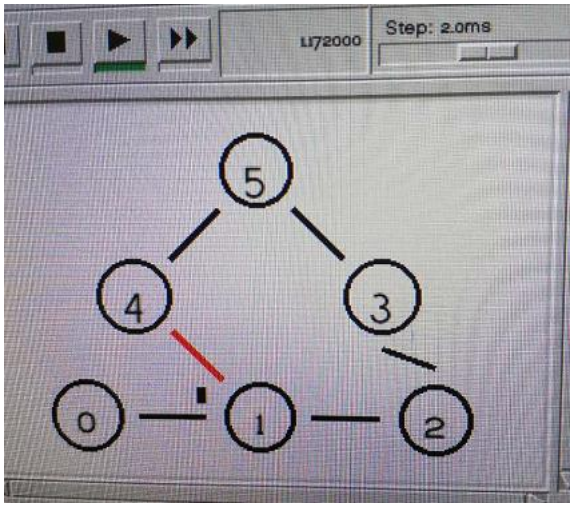


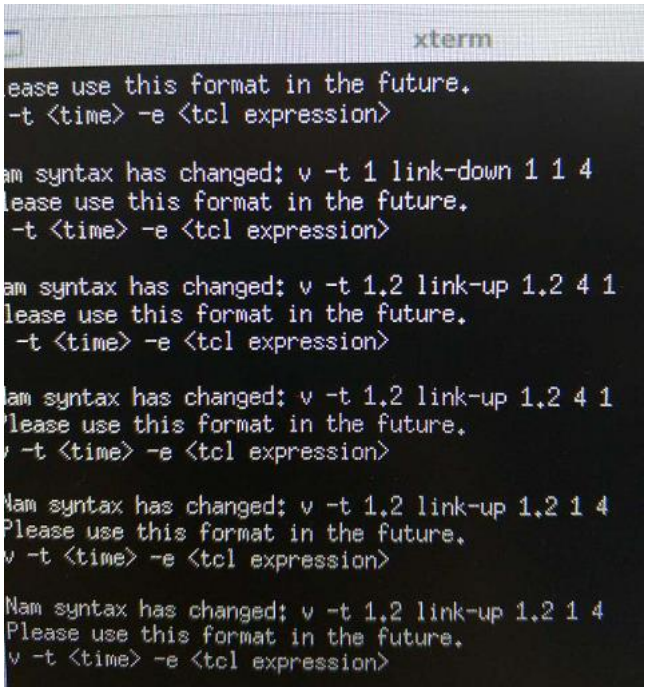
Question 2: What happens at time 1.0 and at time 1.2? Does the route between the communicating node change as a result of that?

Answers:

At time 1.0, between 1 and 4 is link-down, but the route does not change. However, packets cannot reach node 5 from node 0.

At time 1.2, between 1 and 4 is link-up. Route does not change and packets can reach node 5 from node 0 via node 1 and node 4.



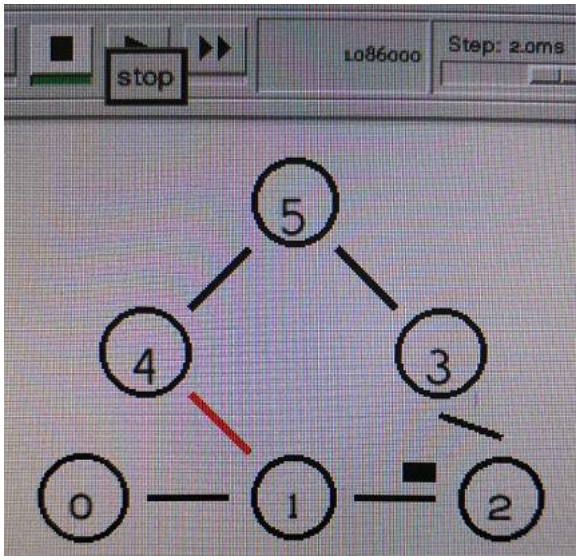


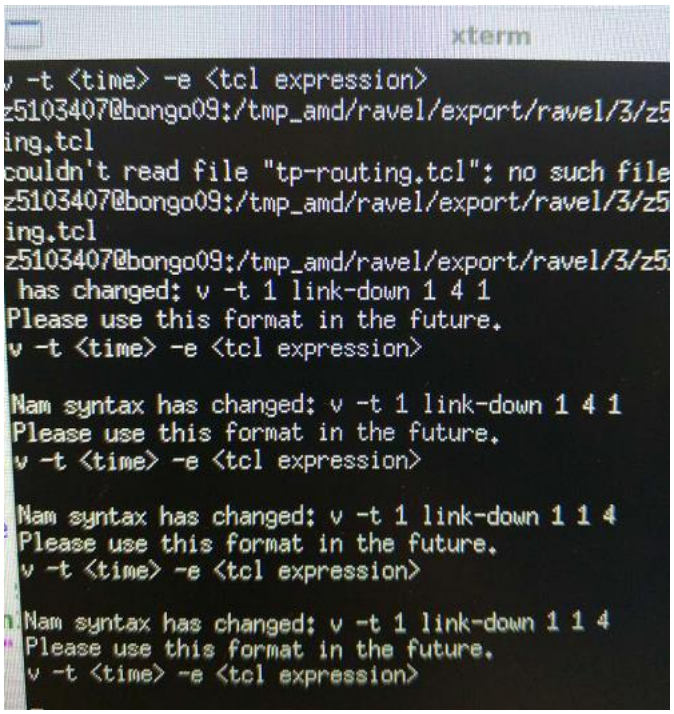
Question 3: How does the network react to the changes that take place at time 1.0 and time 1.2?

Answers:

At time 1.0, between 1 and 4 is link-down. At this moment, the routing protocol send packets from another route (0-1-2-3-5)

At time 1.2, between 1 and 4 is link-up. Because the cost of original route (0-1-4-5) is lower than current route (0-1-2-3-5), so the routing protocol will use the original route (0-1-4-5).





Question 4: How does this change affect the routing? Explain why.

Answers:

This change means the cost between node 1 and node 4 is 3. This makes the flow choose the route 0-1-2-3-5, because the cost of this route is lower than 0-1-4-5.

Question 5: Describe what happens and deduce the effect of the line you just uncommented.

Answers:

Because it changes the cost to 2 between node and node 4. So, route 1 (0-1-2-3-5) and route 2 (0-1-4-5) have equal cost. Due to using the multipath, when flow reaches node 1, its traffic will be split on both route equally.