CS 224: Computer Networks
Assignment 3

Sambit Behera
190050104

April 4, 2021

Question 1a

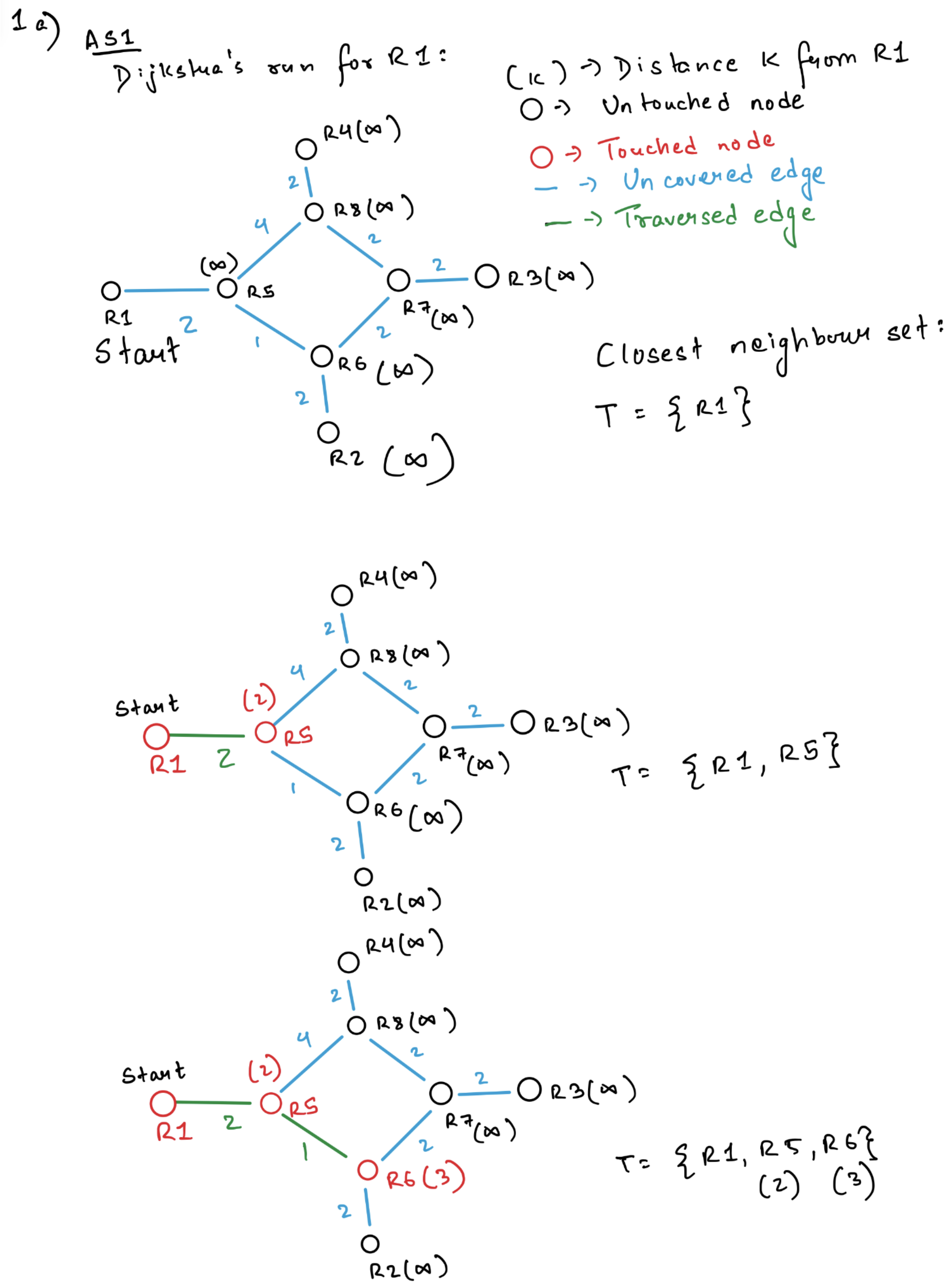


Figure 1

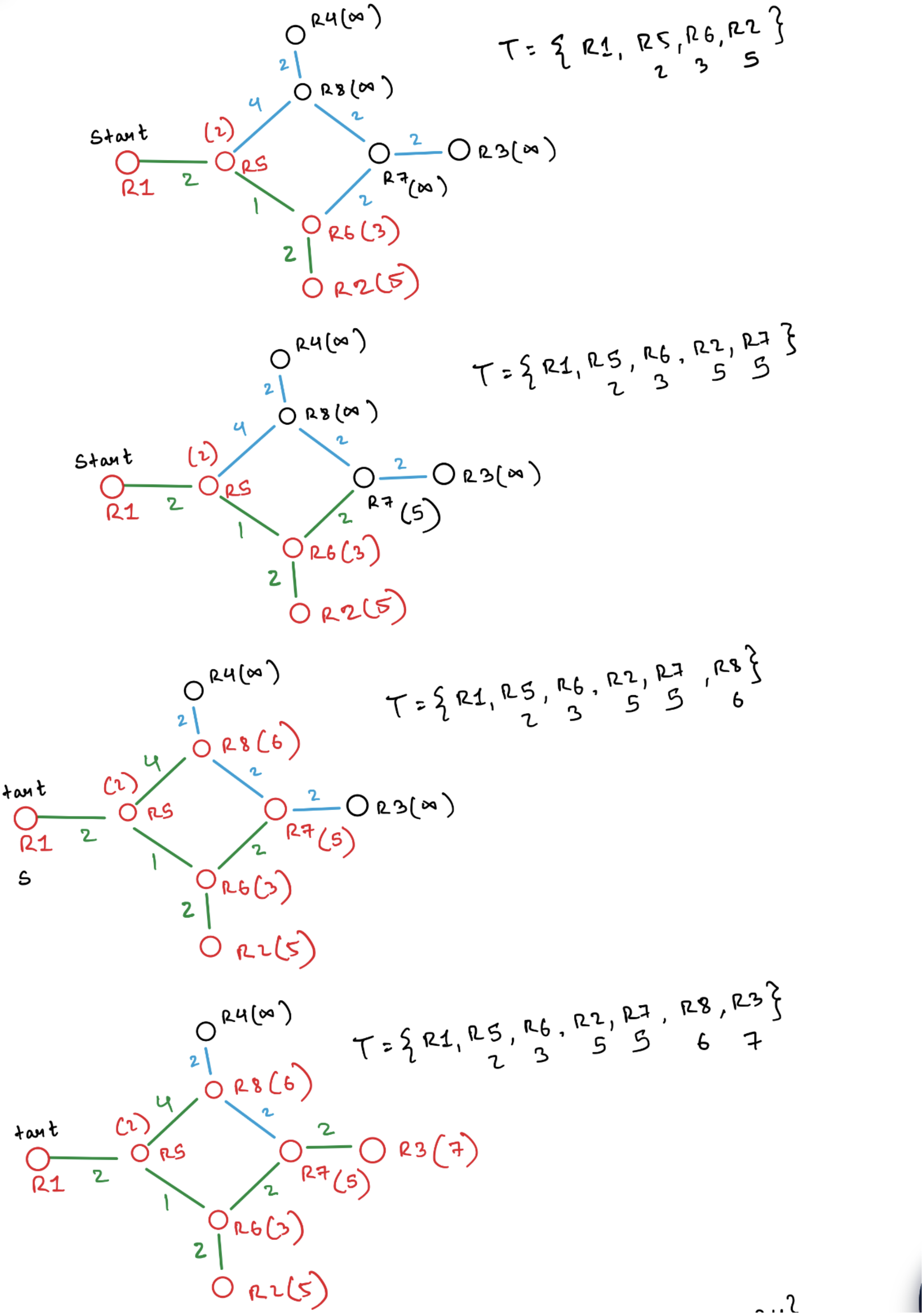
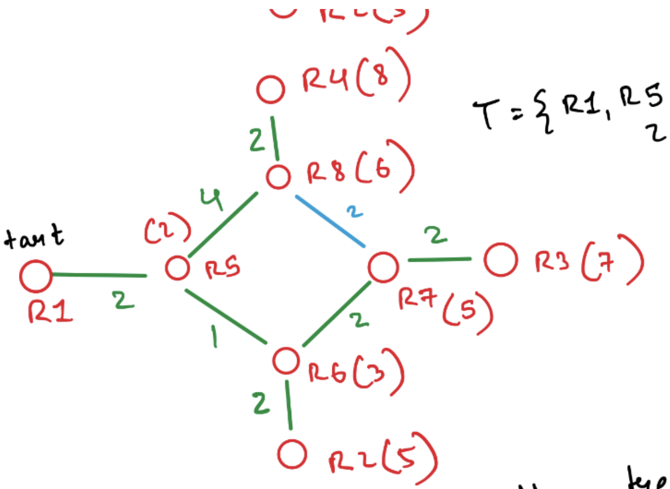
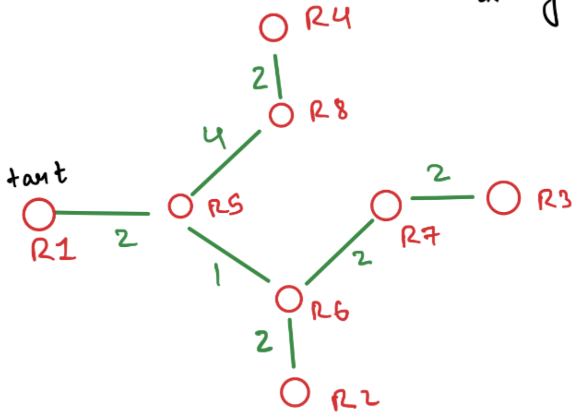

R4(∞)
R8(∞)
Start
(2)
R5
R1
2
4
2
2
2
1
2
R7(∞)
R3(∞)
R6(3)
R2(5)
T = { R1, R5, R6, R2 }
2 3 5
R4(∞)
R8(∞)
Start
(2)
R5
R1
R7 (5)
R3(∞)
R6(3)
R2(5)
T = { R1, R5, R6, R2, R7 }
2 3 5 5
R4(∞)
R8(6)
tart
(2)
R5
R1
S
R7(5)
R3(∞)
R6(3)
R2(5)
T = { R1, R5, R6, R2, R7, R8 }
2 3 5 5 6
R4(∞)
R8(6)
tart
(2)
R5
R1
R7(5)
R3(7)
R6(3)
R2(5)
T = { R1, R5, R6, R2, R7, R8, R3 }
2 3 5 5 6 7

Figure 2



$T = \{R1, \underset{2}{R5}, \underset{3}{R6}, \underset{5}{R2}, \underset{5}{R7}, \underset{6}{R8}, \underset{7}{R3}, \underset{8}{R4}\}$

Hence, we get the routing tree for R1 as follows along with the corresponding distances shown

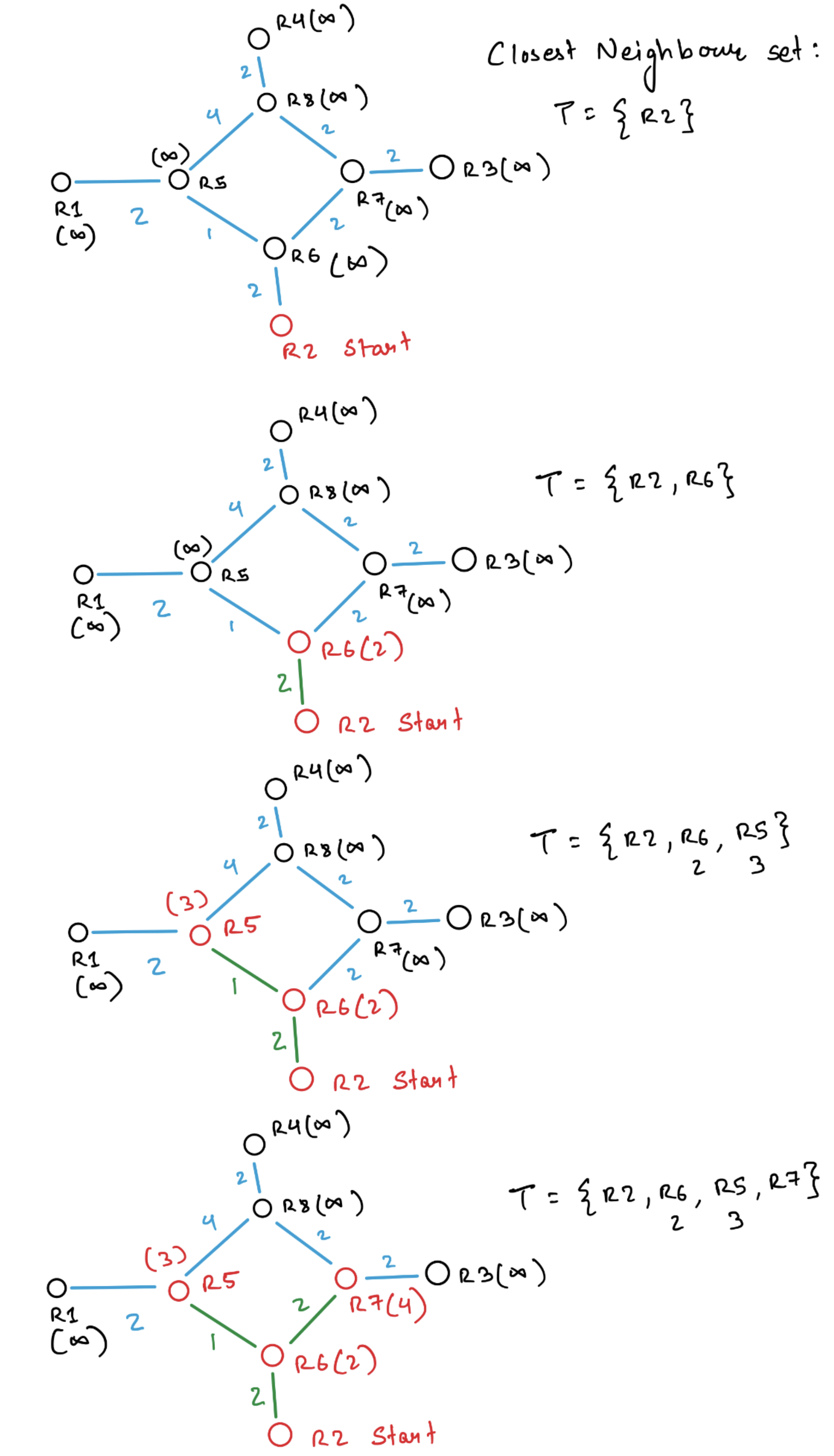


Routing table for R1.

Destination	Cost	Next hop
R2	5	R5
R3	7	R5
R4	8	R5
R5	2	R5
R6	3	R5
R7	5	R5
R8	6	R5

Figure 3

Djikstra's run for R2:



Closest Neighbour set:

$T = \{R2\}$

$T = \{R2, R6\}$

$T = \{R2, \underset{2}{R6}, \underset{3}{R5}\}$

$T = \{R2, \underset{2}{R6}, \underset{3}{R5}, R7\}$

Figure 4

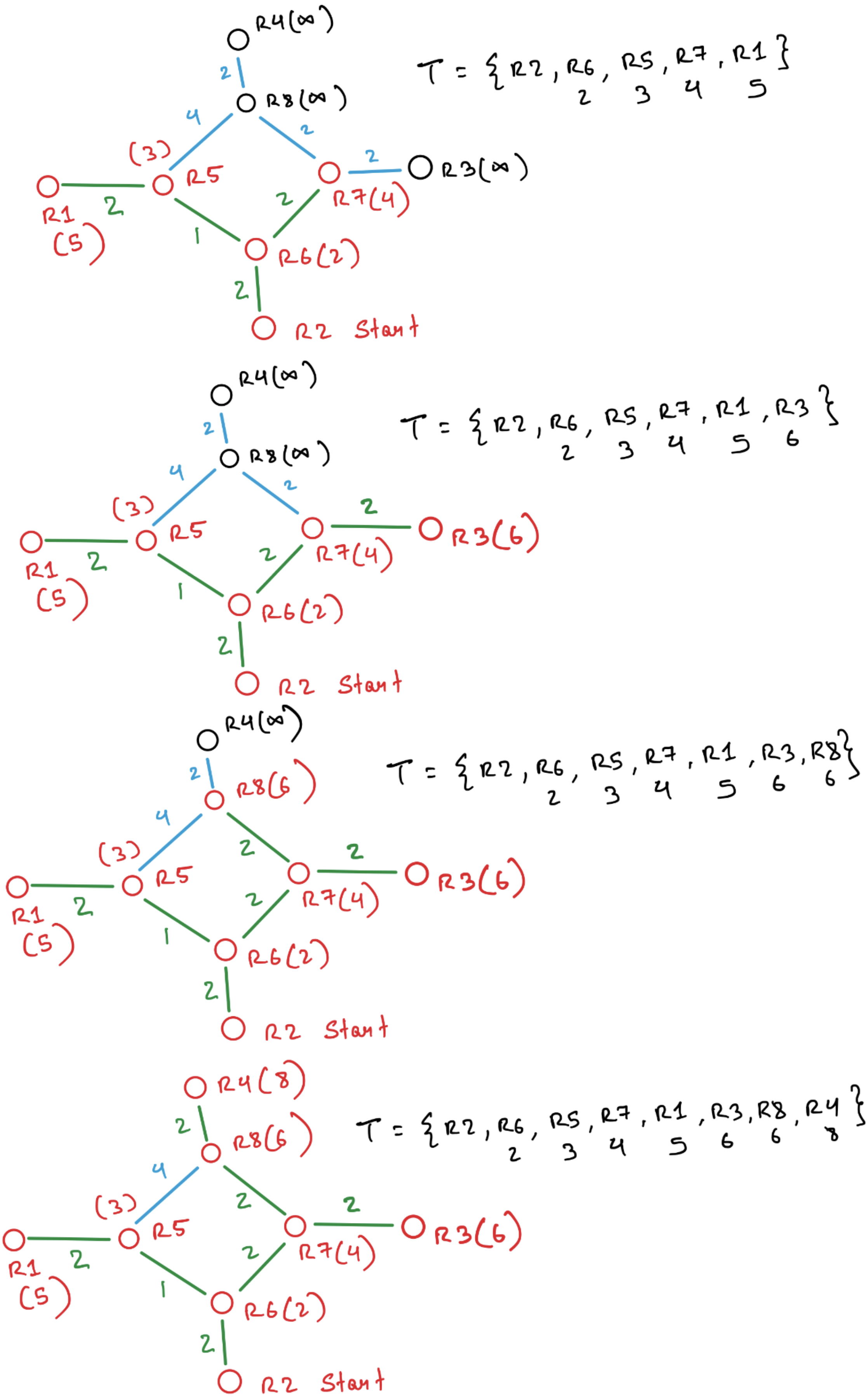
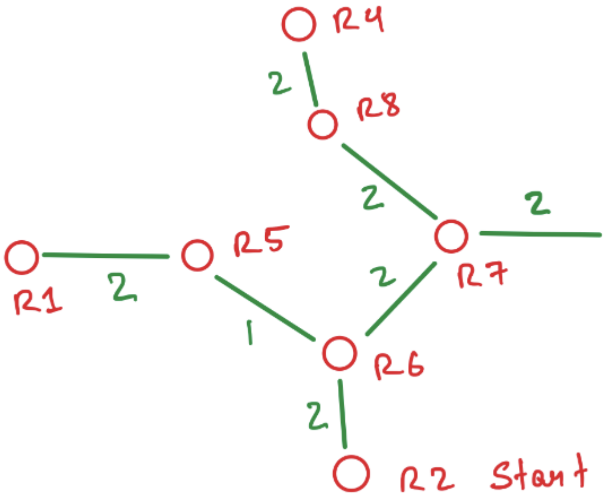

R4(∞)
2
R8(∞)
4
2
(3)
R5
2
R3(∞)
R1
2
R7(4)
2
(5)
1
R6(2)
2
R2 Start
T = {R2, R6, R5, R7, R1}
2 3 4 5
R4(∞)
2
R8(∞)
4
2
(3)
R5
2
R3(6)
R1
2
R7(4)
2
(5)
1
R6(2)
2
R2 Start
T = {R2, R6, R5, R7, R1, R3}
2 3 4 5 6
R4(∞)
2
R8(6)
4
2
(3)
R5
2
R3(6)
R1
2
R7(4)
2
(5)
1
R6(2)
2
R2 Start
T = {R2, R6, R5, R7, R1, R3, R8}
2 3 4 5 6 6
R4(8)
2
R8(6)
4
2
(3)
R5
2
R3(6)
R1
2
R7(4)
2
(5)
1
R6(2)
2
R2 Start
T = {R2, R6, R5, R7, R1, R3, R8, R4}
2 3 4 5 6 6 8

Figure 5

Hence, we have the Routing tree for R2 as follows



Routing Table for R2 :

Destination	Cost	Next hop
R1	5	R6
R3	6	R6
R4	8	R6
R5	3	R6
R6	2	R6
R7	4	R6
R8	6	R6

Figure 6

Question 2

In the question it is given that only the border routers run BGP. Also, it is provided that AS1 has set LOCAL_PREF to the same value for all BGP advertisements and also assumed that MED attribute has not been set in any advertisement. We now apply BGP rules to choose routes in the following subsections.

i AS1 receives two advertisements for the IP address `151.128.32.0/24`. These are

- `151.128.32.0/24 AS2` received by R4 from R14. Hence by NEXT_HOP rule and iBGP protocol, R4 shares the info `151.128.32.0/24, AS2, IP add(R14)` to all the border routers of AS1.
- `151.128.32.0/24 AS3-AS4-AS2` received by R3 from R13. Hence R3 shares the info `151.128.32.0/24, AS3-AS4-AS2, IP add(R13)` to all the border routers of AS1.

This info is shared through iBGP. For all BGP routers of AS1, LOCAL_PREF has been set to same value, hence the first rule is same for both advertisements. But, The number of ASes in path is shorter for the advertisement with NEXT_HOP router R14 (1 AS) rather than R13(3 ASes). Hence all the border routers of AS1 choose R14 as the NEXT_HOP router to send packets to destination IP `151.128.32.0/24`

ii This part is similar to the first part. Here, the advertisements received for the destination IP address `130.12.1.0/24` are

- `130.12.1.0/24 AS4` received by R3 from R13. Hence by NEXT_HOP rule and iBGP protocol, R3 shares the info `151.128.32.0/24, AS2, IP add(R13)` to all the border routers of AS1.
- `130.12.1.0/24 AS2-AS4-AS3` received by R4 from R14. Hence R4 shares the info `130.12.1.0/24, AS2-AS4-AS3, IP add(R14)` to all the border routers of AS1.

Again, LOCAL_PREF is same for all routes, hence we check the number of ASes along each path. We can clearly see the advertisement by NEXT_HOP router R13 is shorter (1 AS) while R14 has 3 ASes. Hence, all border routers of AS1 choose R14 as the NEXT_HOP router for IP address `130.12.1.0/24`.

iii AS1 receives two advertisements of IP address `142.13.0.0/16`. These are

- `142.13.0.0/16 AS2-AS4` received by R4 from NEXT_HOP router R14. Hence, the info `142.13.0.0/16, AS2-AS4, IP add(R14)` is shared to all border routers of AS1 using iBGP
- `142.13.0.0/16 AS3-AS4` received by R3 from NEXT_HOP router R13. Hence, the info `142.13.0.0/16, AS3-AS4, IP add(R13)` is shared to all border routers of AS1 using iBGP

Now we apply the BGP rules to select routes. First, LOCAL_PREF is same for all routes. Next, both the advertisements have the same number of ASes (ie 2) in their path. Next, MED attribute is not set by AS1. Hence we move on to next rule. We know that R4 learns about the first advertisement from R14 through eBGP and about the second advertisement through iBGP. As per rule, eBGP is preferred over iBGP. Hence, R4 chooses R14 as its NEXT_HOP router. Similarly, R3 hears about first adv. through iBGP and about the second adv. from R13 through eBGP. Hence, it sets R13 as its NEXT_HOP router.

The remaining routers R1 and R2 both learn about the advertisements through iBGP. Hence, to break the tie we move to next rule, which is Hot Potato Routing. Now, we compare the lowest IGP metric (here, least distance to NEXT_HOP router). We use the routing table in Q1a to get the corresponding distance values. For router R1, $dist(R1, R4) = 8$ and $dist(R1, R3) = 7$. Hence, R1 chooses route to R3, that is R13 as its NEXT_HOP router because of lower distance metric. Similarly for router R2 we have, $dist(R2, R4) = 8$ and $dist(R2, R3) = 6$ Hence, R2 also selects route to R3 and R13 as its NEXT_HOP router because of lower distance metric.

Therefore, R4 chooses R14 and R1,R2 and R3 choose R13 as their NEXT_HOP router to forward packets to destination IP `142.13.0.0/16`

iv To make all BGP routers choose R14, the administrator should set a higher LOCAL_PREF value to the R4-R14 route than the R3-R13 route. As this is the topmost rule in choosing a route, all the BGP routers of AS1 will choose the route with higher LOCAL_PREF value and hence set the NEXT_HOP router as R14.

Question 1c

We have a packet P1 which is forwarded to R1 of AS1 from AS5. Its destination IP address is `142.13.5.4`. Now, R1 can run BGP, hence has the BGP routing table with IP prefixes and corresponding exit routers. AS1 uses encapsulation as the solution for BGP-IGP interaction.

i R1 receives P1 and looks up the destination IP address in its BGP routing table. The destination IP address `142.13.5.4` belongs to the IP-prefix set `142.13.0.0/16` in the routing table. Hence, from Q1b iii, we can infer that R1 will choose NEXT_HOP router as R13 and the exit router in AS1 corresponding to this route is R3. Now, R1 has to encapsulate the packet with an IP header with source IP of R1 and destination IP of R3 to get packet P2 with whole of P1 as the payload. R3 receives the packet P2 and it finally de-encapsulates it, as P2 has the destination IP of R3. Then, R3 looks up its BGP routing table and gets R13 as its NEXT_HOP router and sends packet P1 to R13, which is then forwarded further.

ii R1 encapsulates P1 to get P2. Now, it looks up its IGP routing table for destination R3 and gets next hop router R5. Hence, it forwards it to R5. R5 receives P2 and looks up destination R3 in its IGP table. It finds the next hop router to be R6 and forwards to it. R6 receives P2 and looks up destination R3 in its IGP table. It gets next hop router to be R7 and forwards P2 to it. R7 receives P2 and looks up next hop router for destination R3. It gets R3 as the next hop and forwards to it. R3 receives P2 and as the packet is meant for R3, it de-encapsulates it and gets P1.

Hence, the routers R1, R5, R6 and R7 look up their IGP routing tables to forward **P2** (as asked in the subpart).

Other than that, R1 also looks up BGP routing table to get exit router R3 and R3 looks up BGP routing table to get NEXT_HOP router for **P1**.

Question 2

Network Address Translation is a method used to map an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. This method helps solving the problem of limited number of total IPv4 addresses. There are generally three types of NAT:-

1. Static NAT - This is a one-to-one conversion of a private IP address to a public IP address, and the conversion table is stored by the NAT device
2. Dynamic NAT - In this type of NAT, a private IP address is translated into a public IP address from a pool of public IP addresses. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses. This is used when the number of users who wants to access the Internet is fixed.

3. Port Address Translation (PAT) - This is a one-to-many type of NAT, which assigns a whole space of private IP addresses a single public IP address. The NAT translation table stores the IP addresses along with the port numbers the packets generated from and are being sent to, justifying its name. This is the most widely used type of NAT which will be discussed in details.

Working

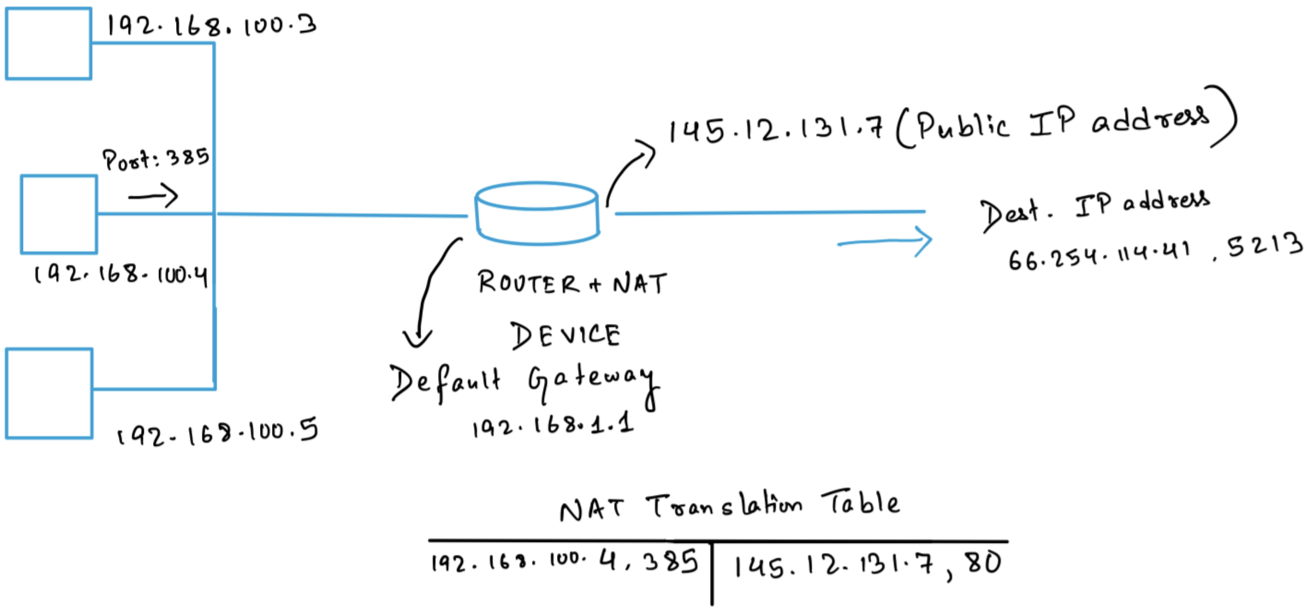


Figure 7

In the figure, we have a private network which is connected to the internet by a Router+NAT device. The device is allocated a public IP address by its Internet Service Provider(ISP). The device also has a private IP address which belongs to the private IP space of the local network. All the hosts in this LAN have a unique private IP address assigned to them. in the figure, host with IP `192.168.100.4` and port number 385 has to send packets to a public IP address `66.254.114.41` and port number 5213. Hence it generates a packet with the above source and destination in IP header and forwards it to the routing device. The router receives this packet and modifies the source IP address to `145.12.131.7` and then forwards it further to the internet. The router has a **NAT translation table** which keeps track of all the private IP addresses and their port numbers and map with the public IP address used instead. Storing port number clears up any ambiguity when the router receives a packet from the internet meant for some host in the private network.
When the router receives a packet from the internet, it picks the destination port number and looks up the NAT table to get the corresponding private IP address. Next, it modifies the destination IP address to this private IP address and forwards it to the local network.

Security

Although NAT isn't specifically used for its security benefits, it inherently functions as a very effective hardware firewall (with a few caveats examined below). As a hardware firewall it prevent "unsolicited", unexpected, unwanted, and potentially annoying or dangerous traffic from the public Internet from passing through the router and entering the user's private LAN network.

Since the NAT router links the internal private network to the Internet, it sees everything sent out to the Internet by the computers on the LAN. It memorizes each outgoing packet's destination

IP and port number in a NAT table and assigns the packet its own IP and one of its own ports for accepting the return traffic. Finally, it records this information, along with the IP address of the internal machine on the LAN that sent the outgoing packet, in the NAT table.

When any incoming packets arrive at the router from the Internet, the router scans its NAT table to see whether this data is expected by looking for the remote IP and port number in the current connections table. If a match is found, the table entry also tells the router which computer in the private LAN is expecting to receive the incoming traffic from that remote address. So the router re-addresses (translates) the packet to that internal machine and sends it into the LAN. If the arriving packet does not exactly match traffic that is currently expected by the router, the router figures that it's just unwanted "Internet noise" and discards the unsolicited packet of data. If the NAT router isn't already expecting the incoming data, because one of the machines on the LAN asked for it from the Internet, the router silently discards it and your private network is never bothered.

NAT also allows you to display a public IP address while on a local network, helping to keep data and user history private. Other than that, any outsider also has no idea which computer in the LAN had sent the packet or needs to be sent one, as all data is with the NAT router. This has proved a valuable feature on hardware firewalls for saving public IP addresses and also a countermeasure for some types of attacks such as a reconnaissance attack.