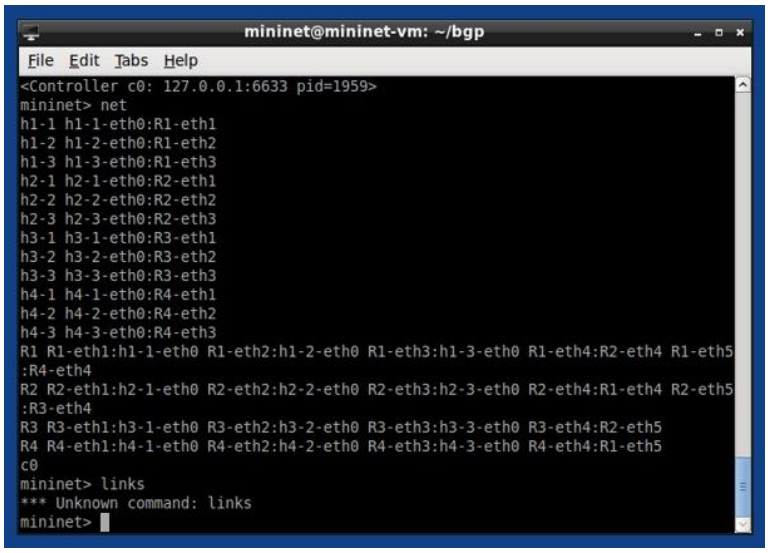
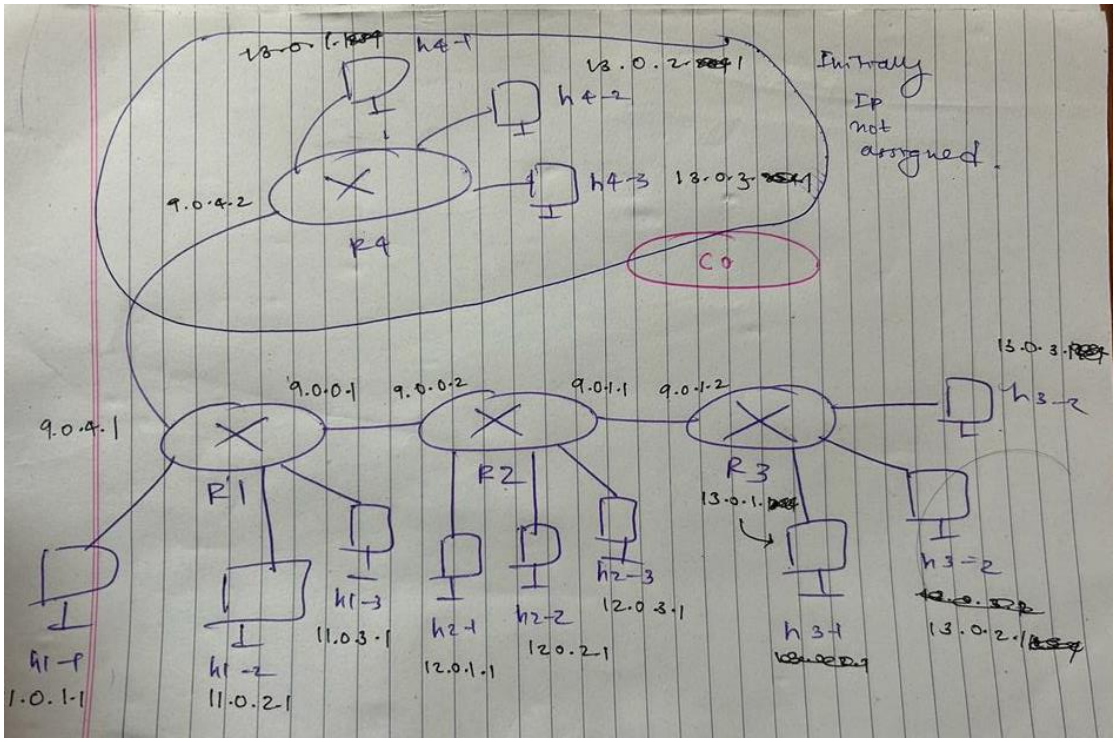
ACN Mininet Assignment: BGP Path Hijacking

Q1: Draw the topology diagram used for this demo. How many hosts are there and how many Routers are present in the emulated network inside mininet? How many hosts are present in each subnet? (Hint: Each router here represents an autonomous system)

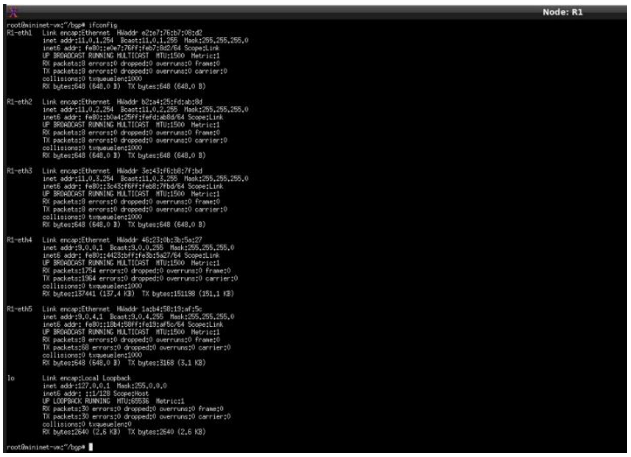
Ans:

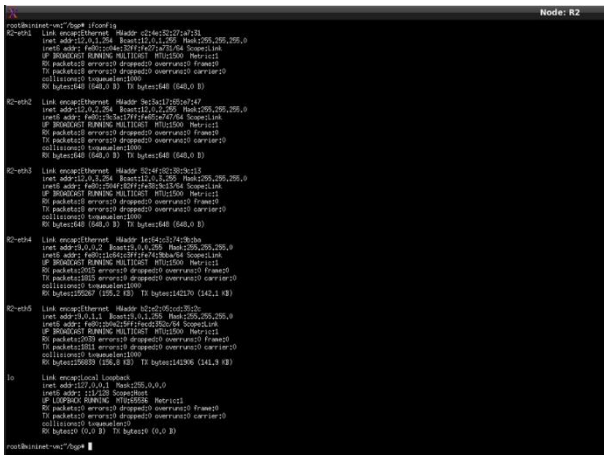


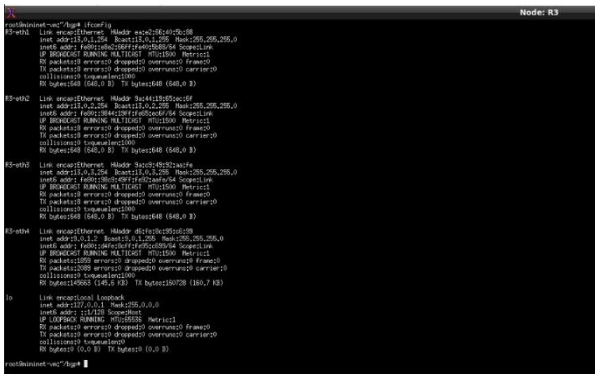


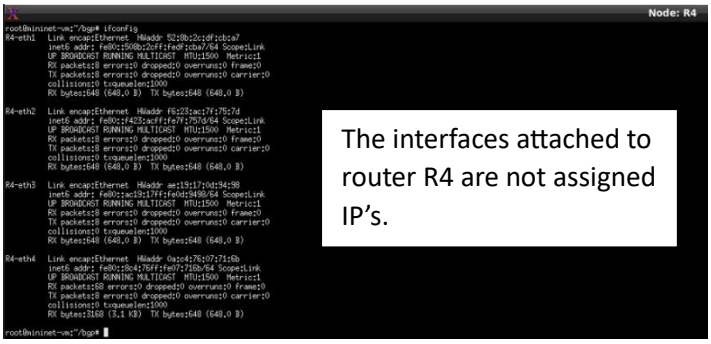
Q2: What are all the available interfaces (on both routers and hosts) and what are their IP addresses? (hint: use xterm to log into the host and find the answer). Include the IP addresses also in the topology diagram. If an interface does not have an IP address yet, mention it.

Ans:





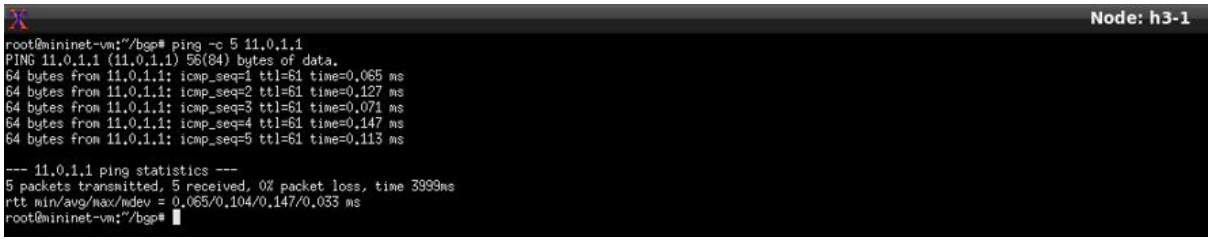


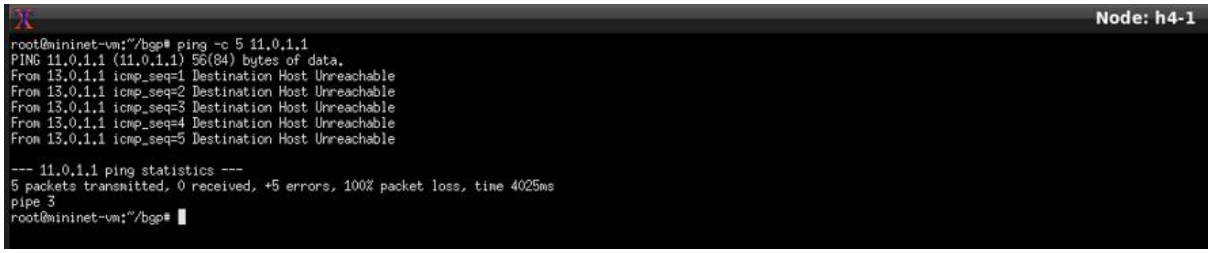


The interfaces attached to router R4 are not assigned IP's.

Q3: Check the reachability for host “h3-1” from at least three other hosts. Post screenshots as proof that you are able to communicate with “h3-1”. (hint: use xterm “hostname” to log in the host and test reachability)\

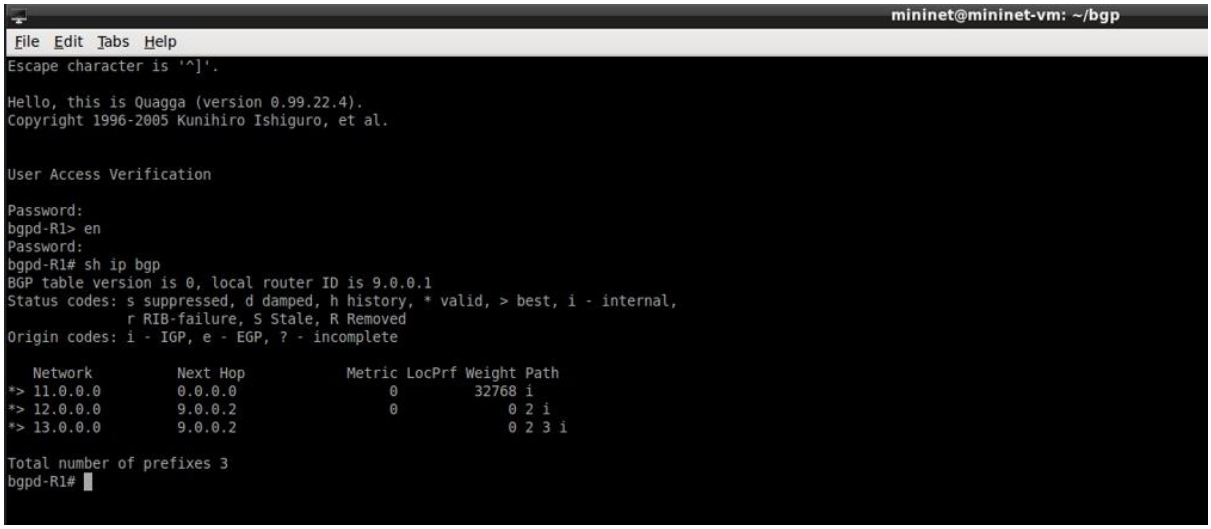
Ans:





Q4: What do you see at the router R1 (AS1). Explain your interpretation of the entries in the BGP table with screenshots.

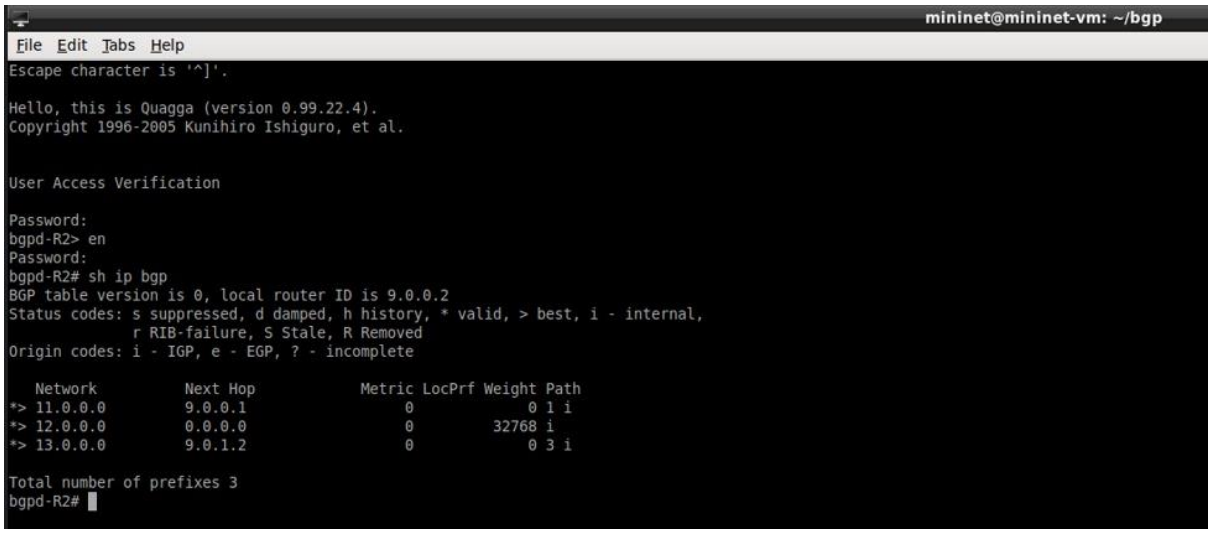
Ans: Based on the output I can interpret that if the destination IP is of current subnet, it will flow the packet onto the link which can be seen by the corresponding next hop entry 0.0.0.0 and if the destination network id are of subnet 2 and 3 it will pass it to the interface 4th of the subnet 2 : 9.0.0.2



Q5: Perform the same for the router R2. Post screenshot. Are the entries in the routers different from each other? Why? What do they signify?

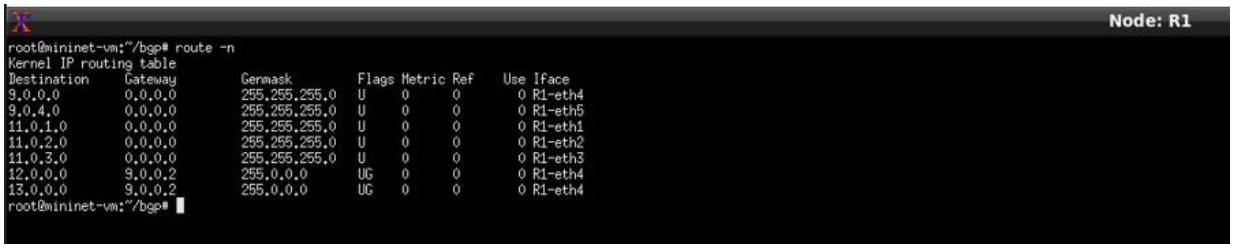
Ans: Based on the topological position of router R2, the entries of R1 and R2 will differ for each of the network ID.

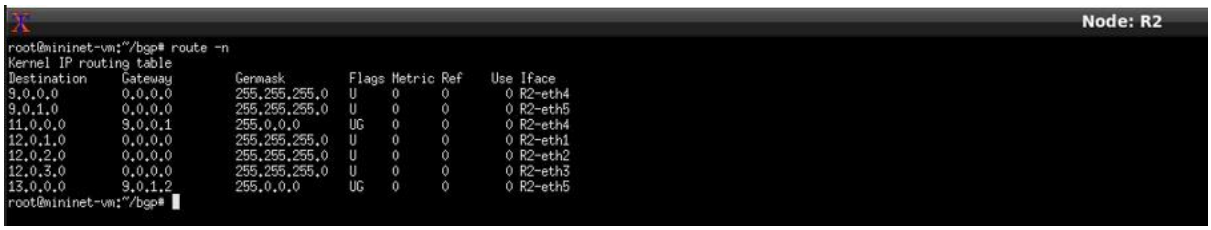
If the packet belongs to subnet 2, it will put it on the link. On the other hand for subnet 1 and subnet 2 it will forward to their respective interface.



Q6. Post contents of forwarding tables at R1 and R2 using “route -n” command by logging into respective routers. Explain the difference between R1’s BGP table and its forwarding table and how the BGP table is used to populate entries in the forwarding table of R1.

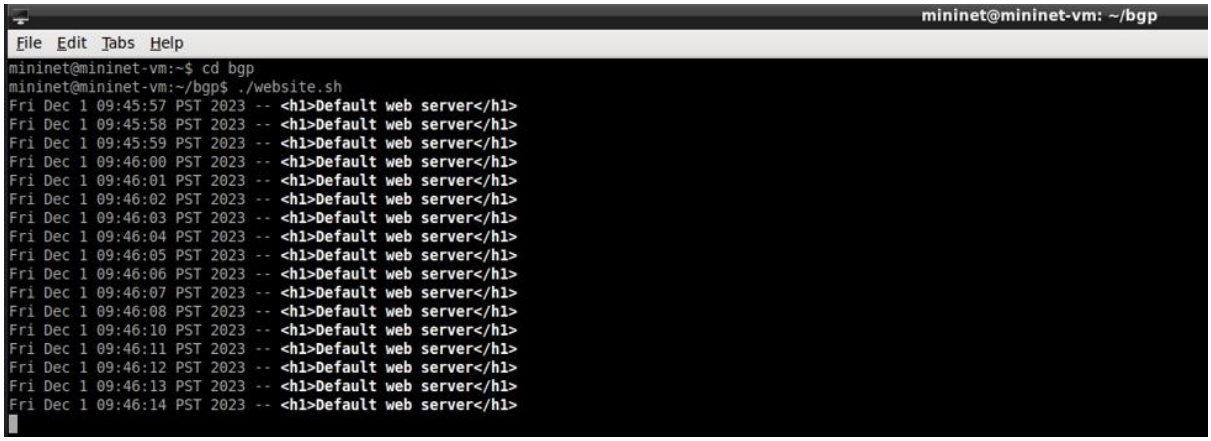
Ans: Each router will construct its forwarding table using their respective BGP tables. BGP table contains the information about neighbouring autonomous system whereas forwarding table used to do destination-based routing.
Here BGP table, tells how it can go to destination asynchronous system.

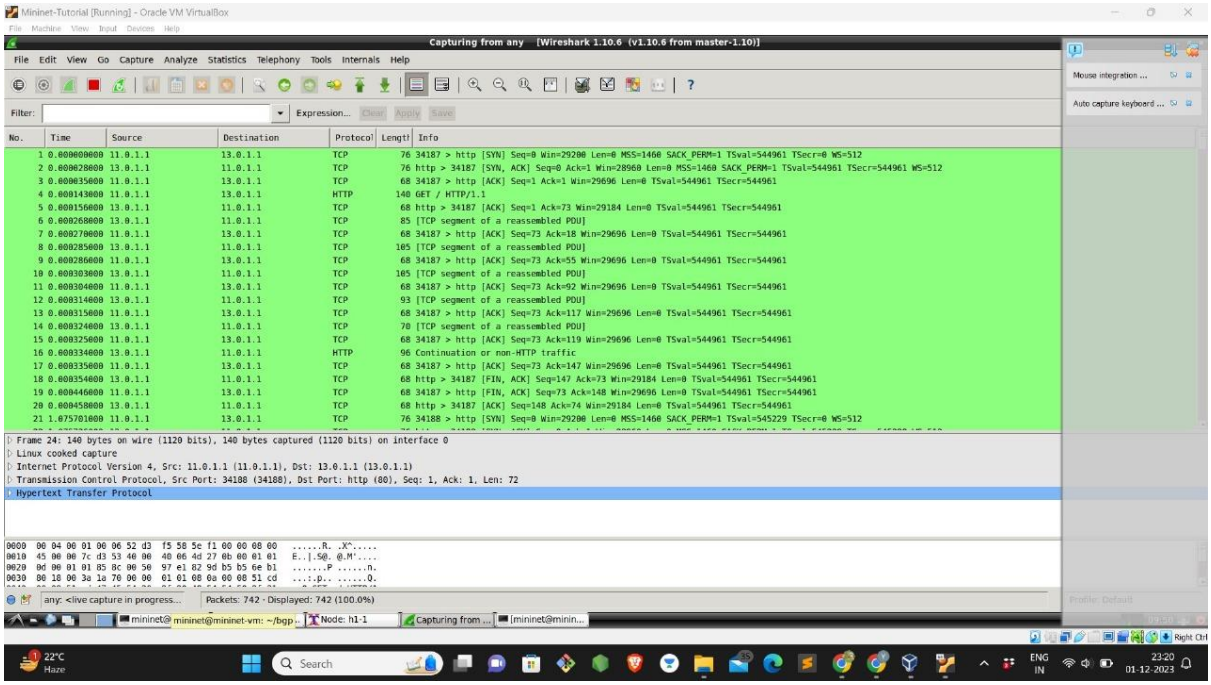




Q7: Open wireshark and listen to an interface (you have to choose the appropriate one). Post screenshots of the HTTP GET requests and the response you received. This should correspond to the output seen on the terminal window. (hint: to open wireshark: xterm into a host and type "`sudo wireshark &`"; ignore any error messages that pop up. Then choose an interface and listen to it.)

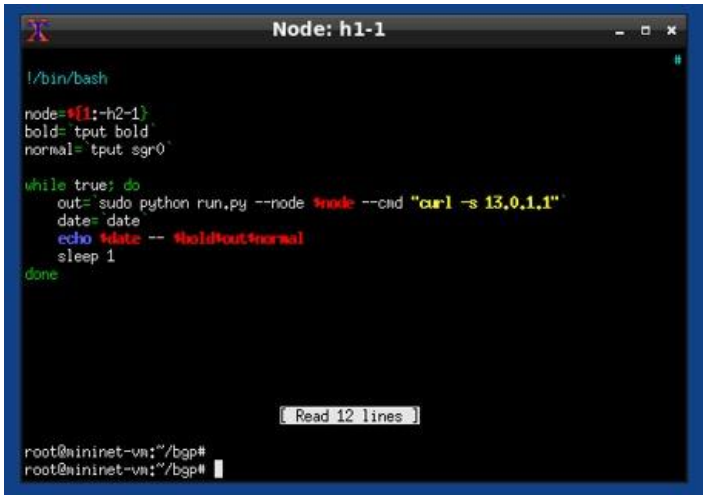
Ans:

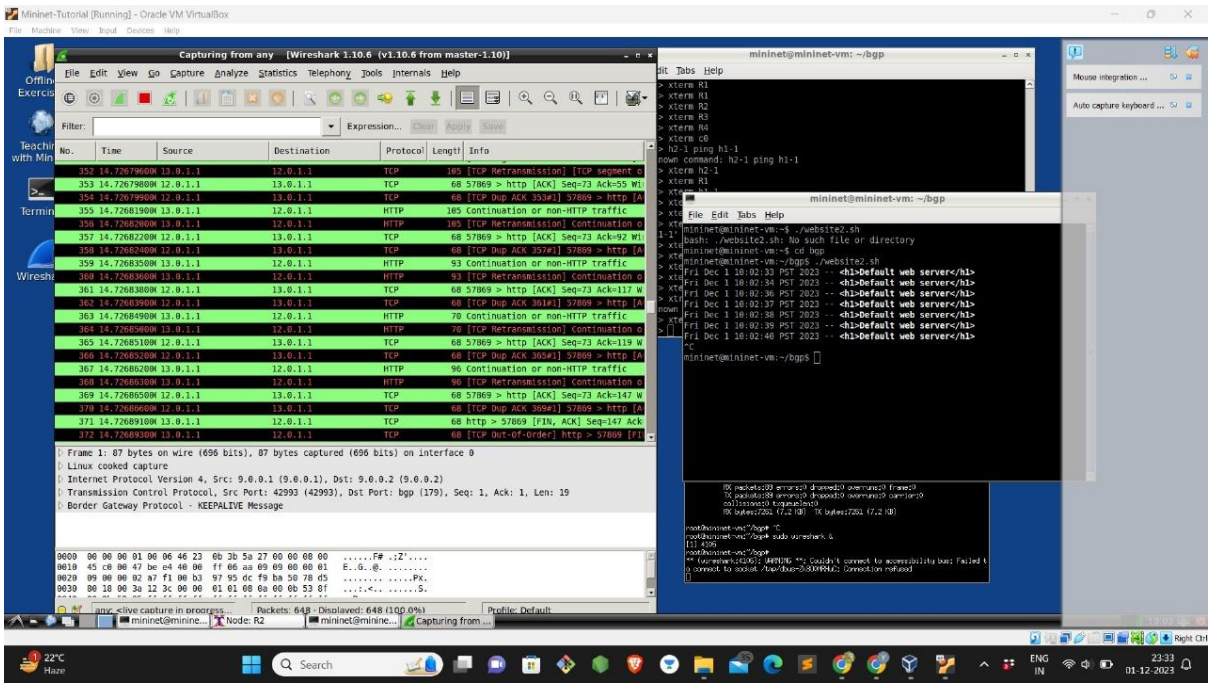




Q8: Modify `website.sh` (call it `website2.sh`) by choosing one of the hosts in AS2 to send GET requests to the webserver running on h3-1. Post a screenshot of CLI output and wireshark log as the proof.

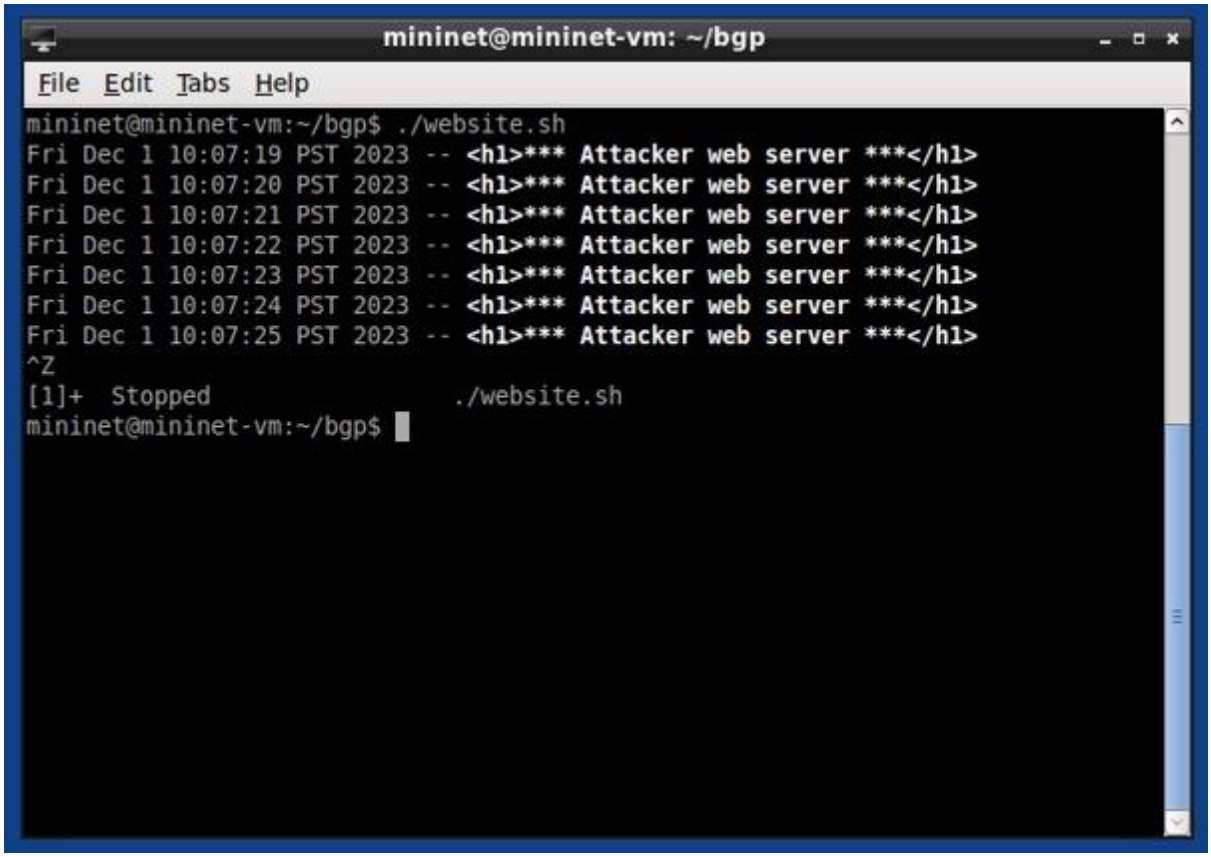
Ans:



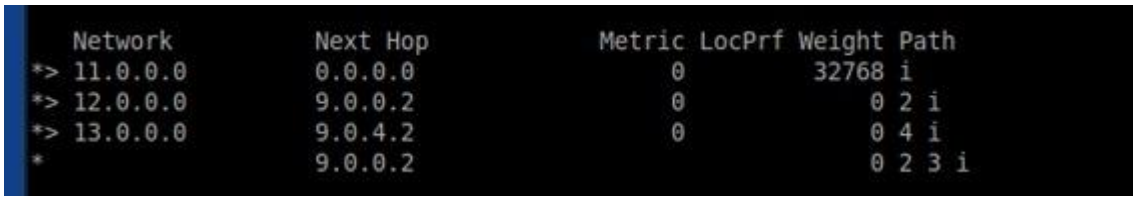


Q9: Do you see any change in the CLI output where you ran website.sh? If yes, post the screenshot. If not, post the screenshot. What do you think has happened?

Ans:

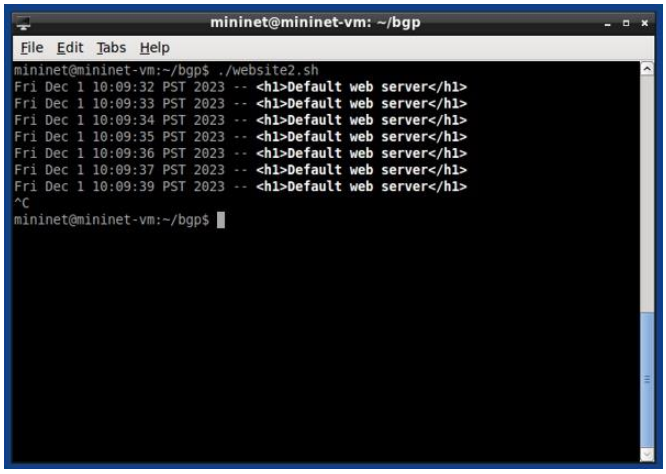


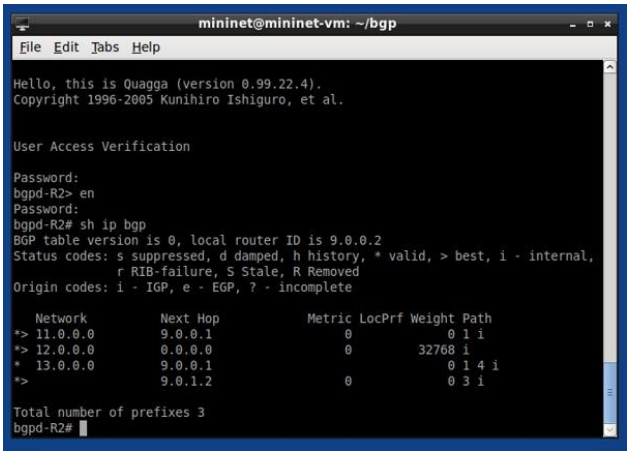
After running, start_rogue.sh, malicious AS4 will become the part of the network. So, it will advertise its existence to its autonomous system, as a result of which when AS1 receives the notification that it can reach AS3 in a less path, it will update its respective forwarding and BGP table. For reference the updated BGP table at R1 is shown below:



Q10: Do you see any change in the CLI output where you ran the modified script, website2.sh? If yes, post the screenshot. If not, post the screenshot. What do you think has happened?

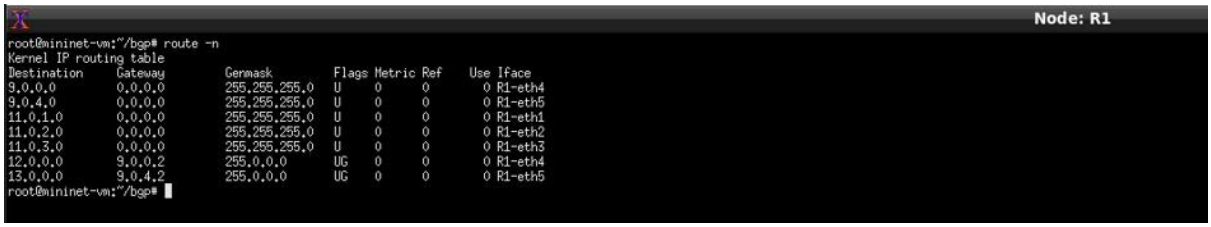
Ans: There would be no change in the forwarding table, but there would be change in the BGP table. As autonomous system 2 would be notified about the reachability of network 13.0.0 via AS1. But since AS_path via that route is longer than the previous AS_path so it won't change its forwarding table.

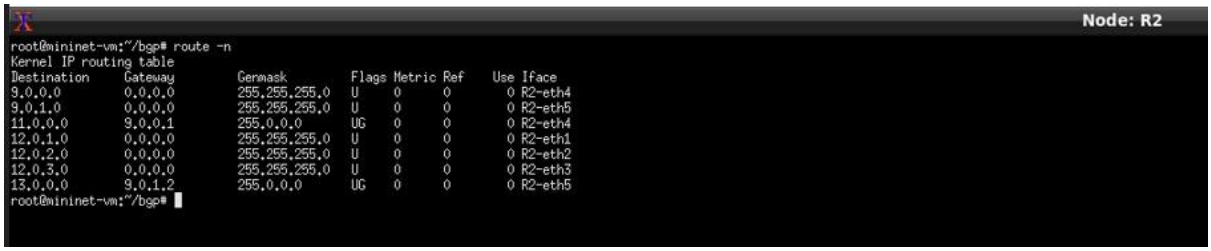




Q11: Log into the routers R1, R2. Are their BGP tables and forwarding tables different from before? If so, what is the difference? What has happened after bogus BGP advertisements by AS4 at AS1 and AS2?

Ans: Yes, BGP tables of both are different. Forwarding table of R1 differs while R2 will remain same. When bogus BGP advertisement happened by AS4 at AS1 and AS2. AS2 will not have a change in its forwarding table as for it to reach network 13.0.0.1 is just a one hop journey whereas the forwarding table of AS1 will have a change as it finds a shorter tour then previous to reach the same network tho it's faulty.

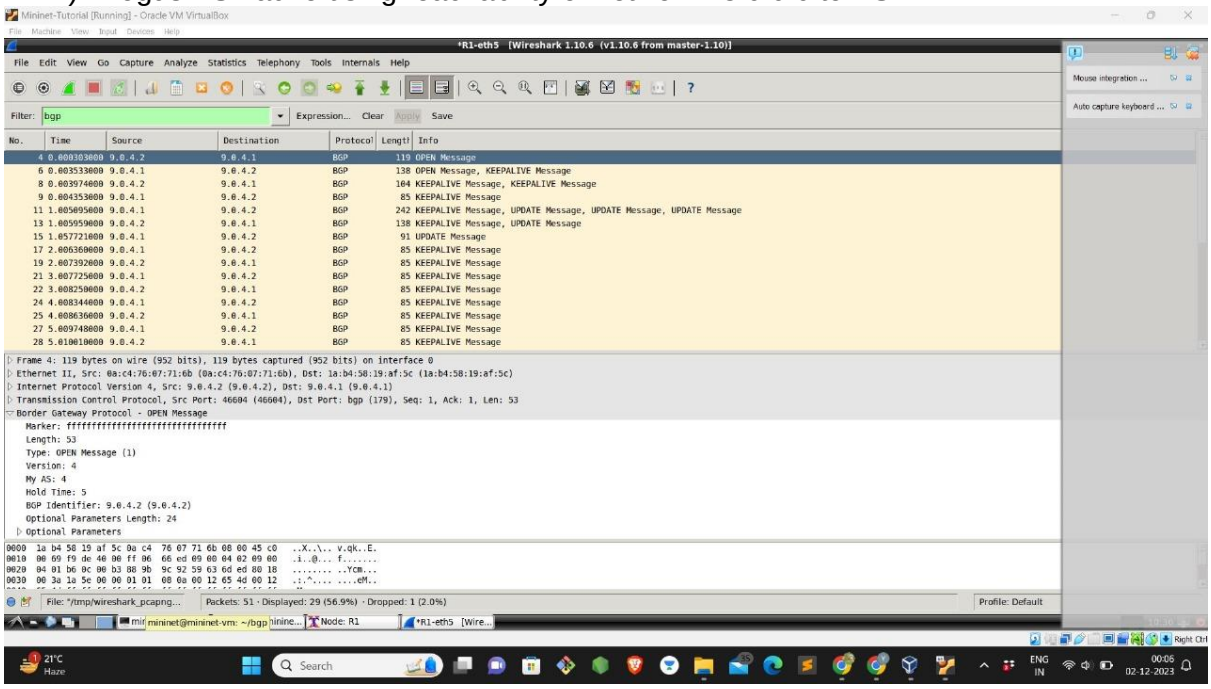




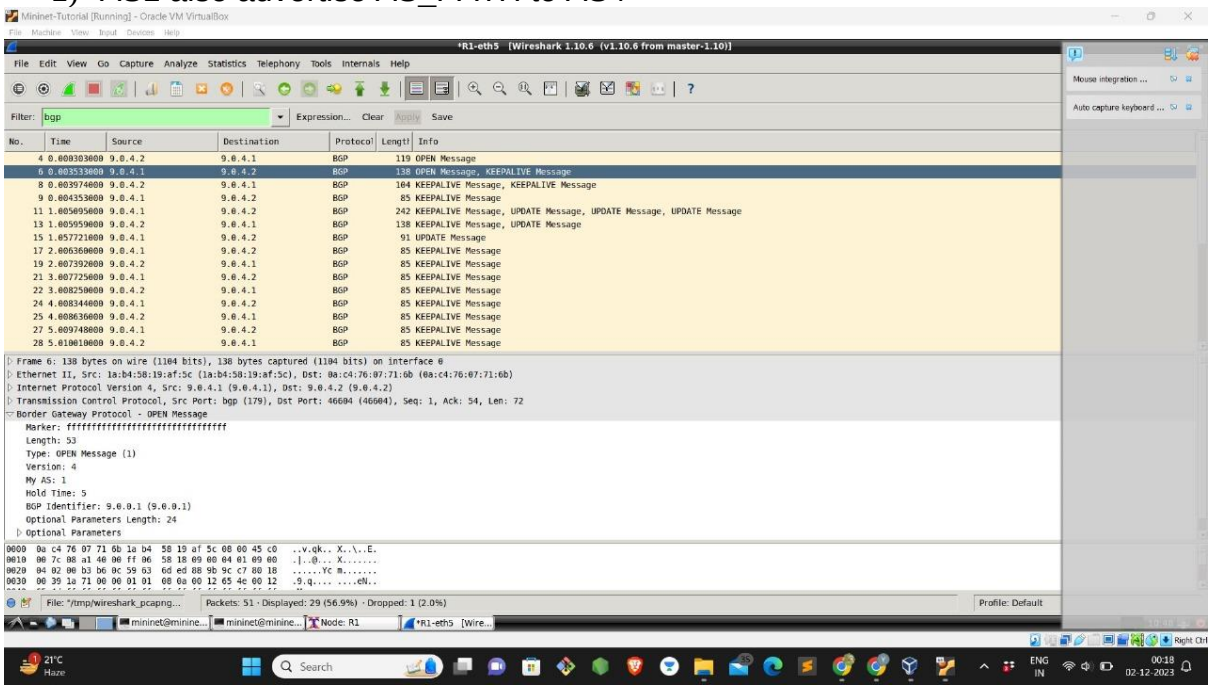
Q12: But this time open the xterm of the appropriate hosts and listen to the appropriate interfaces (figure out these interfaces) on wireshark in order to listen to the traffic. Now run the `start_rogue.sh` script. Do you see any BGP message sequence in the wireshark captures? Pin point which BGP message contains the rogue BGP update and post the screenshot. Expand the packet and post the screenshot. Explain the message contents, especially prefixes being advertised. Correlate this message with the screenshot taken earlier.

Ans:

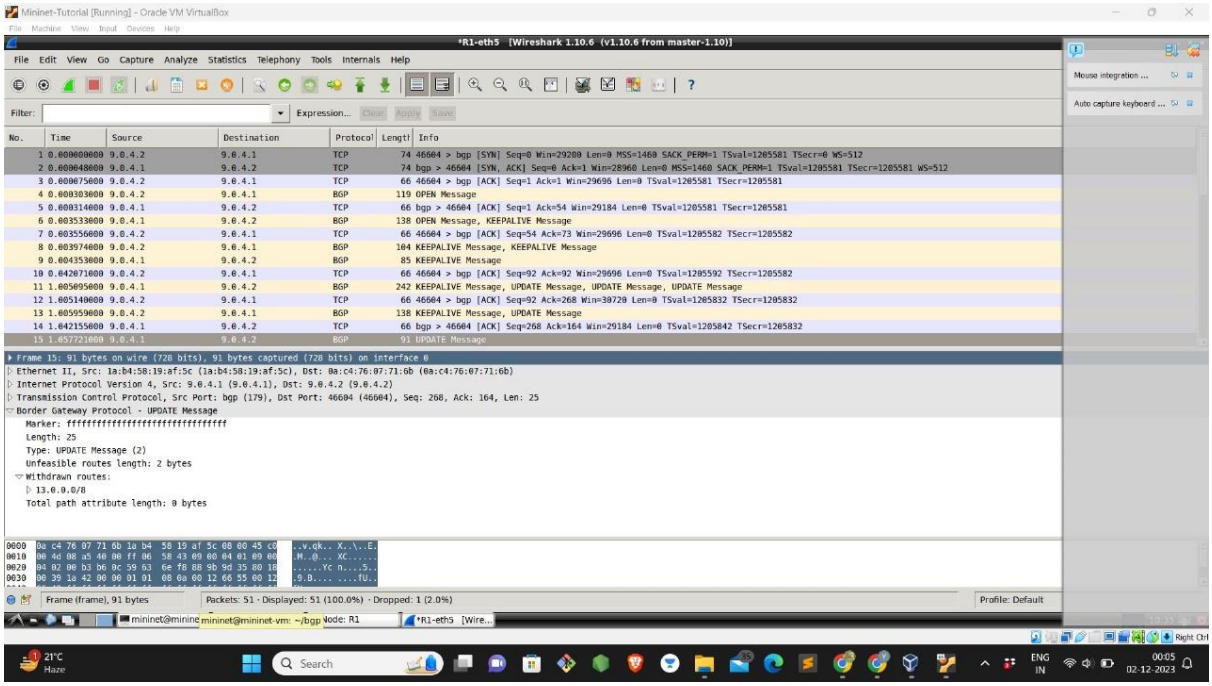
1) Bogus AS4 advertising reachability of network 13.0.0.0 to AS1



2) AS1 also advertise AS_PATH to AS4



3) AS1 finds shortest path and updates its BGP table to reach 13.0.0.0



Q13: Now put the sequence of events together and explain in clear steps what has occurred from start to finish. Is rogue AS succeeded in fooling the hosts (and then directing them to a fake website running at the hijacked host/web server) present in all other ASs or only a subset of them? List out the hosts that got fooled by the rogue AS.

Ans: When AS4 becomes the part of network, it will have impacts on the BGP tables of entire network router but only the forwarding table of R1 will have a change because it thinks AS4 as AS3 and finds it one hop away. As a result of which all the hosts of AS1 which are willing to communicate AS3 will now be redirected to bogus AS4. But AS2's and AS3's forwarding table will not have any changes as they already know shortest path to reach AS3 and so only a part of the network(AS1) will be poisoned because of inclusion of bogus AS4.

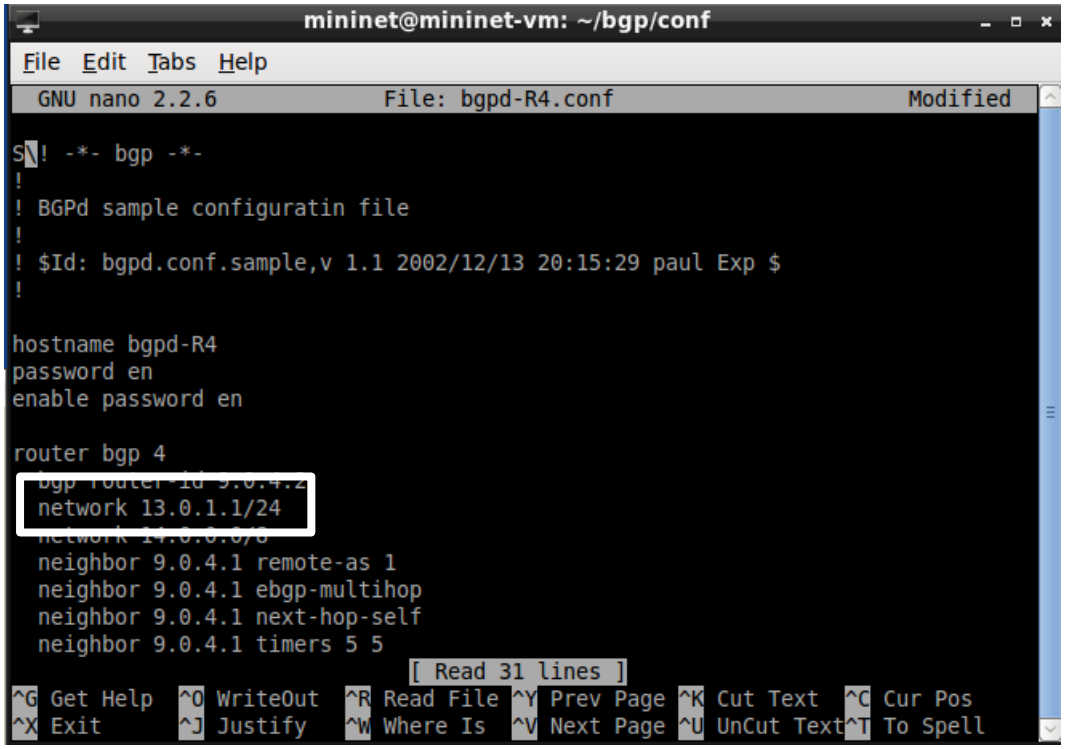
Q14. When hosts present in AS1 ping hosts in AS3, observe RTT before running `start_rogue.sh` script and after running `start_rogue.sh` script. Do you find any difference, explain. Did the rogue AS (AS4) hijack all the hosts in AS3 or a subset of them?

Ans: It was clearly seen that the RTT before inclusion of bogus RS4 is more than after its inclusion. This is because of the simple fact that before for AS1 to reach AS3 it was two hop away and when bogus AS4 that mimics AS3 comes into the picture then for AS1 to reach AS4 or say AS3 is just one hop tour.

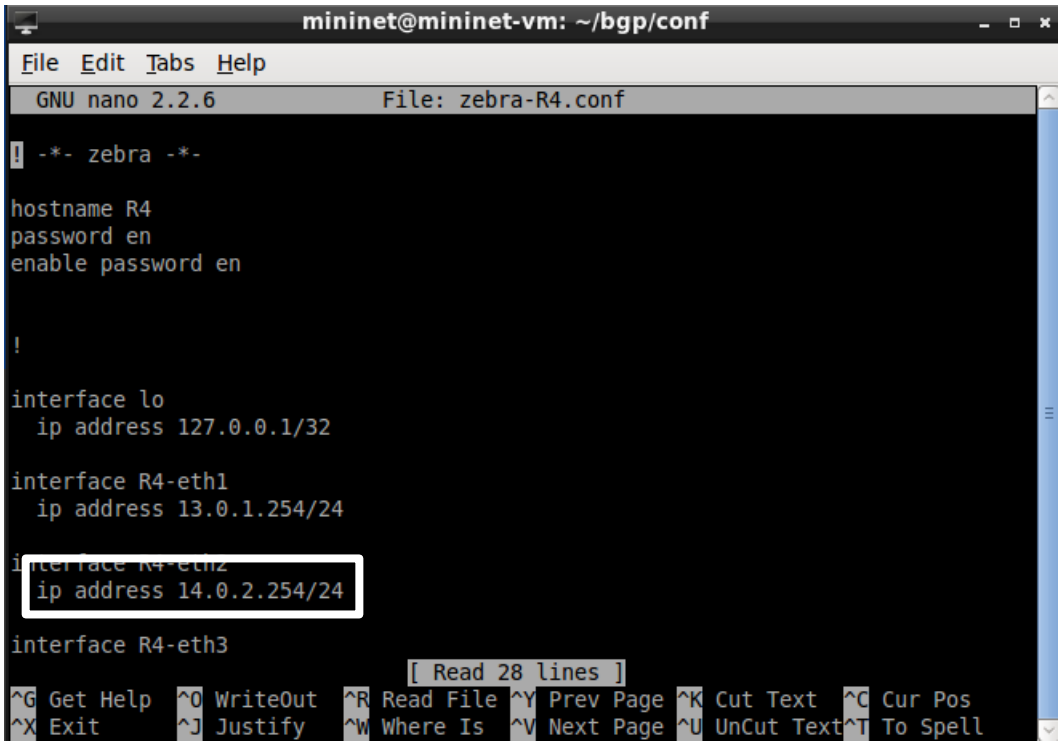
Q15. This is an advanced task. Modify the scripts given in the code base in a way the rogue attacker (AS4) only hijacks the host "h3-1" but not other hosts present in AS3. Explain how to launch this targeted BGP path hijack attack on the target host "h3-1" and demonstrate it with step-by-step instructions with screenshots

Ans:

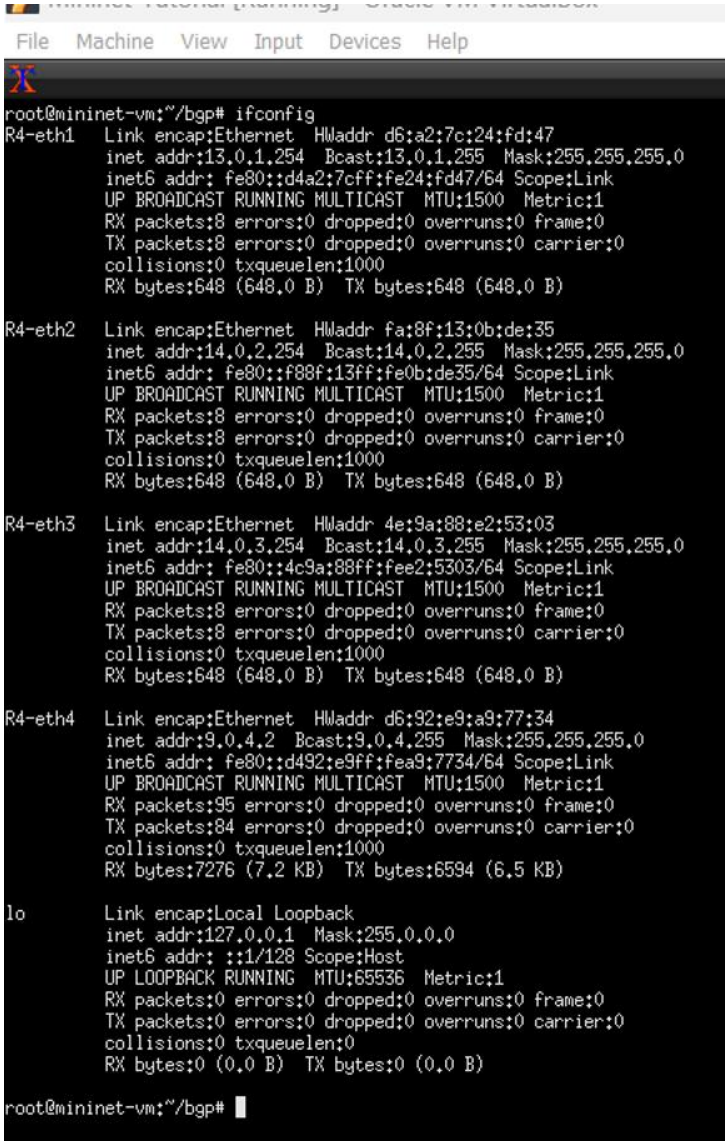
Changes to bgpd-R4.conf



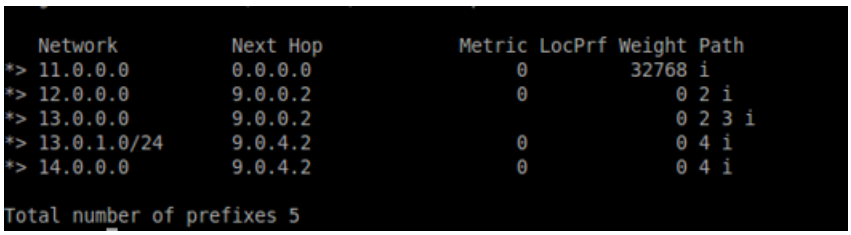
Changes to zebre-R4.conf

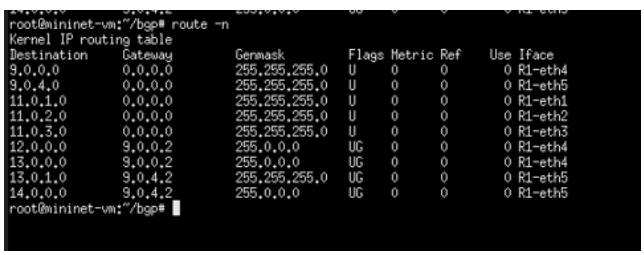


Changes to R4's interface IP's



Change to the R1 BGP and Forwarding Tables





Output comparison:

While trying to hit 13.0.1.1 from host H1-1

While trying to hit 13.0.2.1 from host H1-1

ANTI-PLAGIARISM Statement

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. Additionally, we acknowledge that we may have used AI tools, such as language models (e.g., ChatGPT, Bard), for assistance in generating and refining my assignment, and we have made all reasonable efforts to ensure that such usage complies with the academic integrity policies set for the course. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, we understand our responsibility to report honour violations by other students if we become aware of it.

Name: Yug Patel, CS23MTECH14019
Somya jain, CS23MTECH12011
Anil Kumar, CS23MTECH13001

Date:02/12/2023
Signature: Yug Patel, CS23MTECH14019
Somya jain, CS23MTECH12011
Anil Kumar, CS23MTECH13001