SUTD 2021 50.012 Lab 6 Writeup Submission Document

> Project Group 2 Members:
>
> - James Raphael Tiovalen / 1004555
> - Velusamy Sathiakumar Ragul Balaji / 1004101
> - Han Xing Yi / 1004330
> - Huang He / 1004561
> - Qiao Yingjie / 1004514
> - Zhang Peiyuan / 1004539

Submission Answers

1. Chosen IP subnet for the hosts: `10.0.0.0/24`. This is indicated by the subnet mask `255.255.255.0`.

2. Yes, `srv1` and `srv2` are in the same subnet of `10.0.0.0/24`, since `srv1` has an IP address of `10.0.0.10` and `srv2` has an IP address of `10.0.0.11`.

3. Executing the command: `h1 tracepath srv1 -n` on the Mininet console, we are not able to observe the switch. This is because switches, which exist on the link layer, are transparent towards hosts. Instead, we were only able to trace the IP addresses of the hop router(s).

4. For servers `srv1` and `srv2`, the gateway is `10.0.0.1`. For hosts `h0`, `h1`, `h2`, `h3`, and `h4`, the gateway is `10.0.0.111`.

5. Executing the command `h1 ping 8.8.8.2` on the Mininet console, we get `Destination Host Unreachable` errors. Thus, `h1` is not able to ping/reach the `test.net` (`8.8.8.2`) server since the specified gateway in `h1` is wrong. ARP requests for `10.0.0.111` (which is the IP address of the first hop router/gateway for the hosts `h1` to `h4`) cannot be resolved as it does not exist and thus the packets are not going to the correct router.

6. Yes, the DHCP server is running on `10.0.0.10` (server `srv1`). This can be identified by running the command `h1 dhclient h1-eth0` on the Mininet console and intercept the packets via Wireshark on `h1`, which would allow us to see the DHCP DORA messages being exchanged between `10.0.0.10` (the DHCP server) and the client requesting the IP address, whose IP was initially set as `0.0.0.0` and the destination of the packets was set as the broadcasting IP address `255.255.255.255`.

7. Yes, the value for `dhcp-option` is wrong as it should be `3,10.0.0.1` (instead of `3,10.0.0.111`). The purpose of this line is to configure the IP address of the first hop router/gateway broadcasted to the hosts `h0` to `h4` to `10.0.0.1`, which actually exists and thus should allow the hosts to reach the server `test.net`.

8. Yes, `h1` is now able to ping and reach Google (`8.8.8.8`) as it is now able to reach the external gateway `extGW` through the switches.

9. Yes, `h1` is able to ping and reach `test.net`, which has the IP address: `8.8.8.2`. This is because when the DNS server was changed to `8.8.8.8`, that DNS server contains the DNS record (type `A`) for `test.net` with its associated IP address.

10. The `intGW` node. It converts the source internal IP address of `10.0.0.105` to `2.2.2.2` for host `h1` for outgoing packets, and vice versa for incoming packets via NAT.

11. The rule added was: `iptables -I FORWARD -s 10.0.0.11 -j DROP`. This rule uses the principle of match + action, where packets sent from the source IP address of `10.0.0.11` (`srv2`) will be dropped by the firewall.