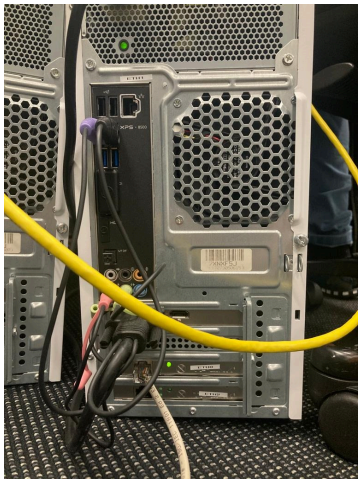
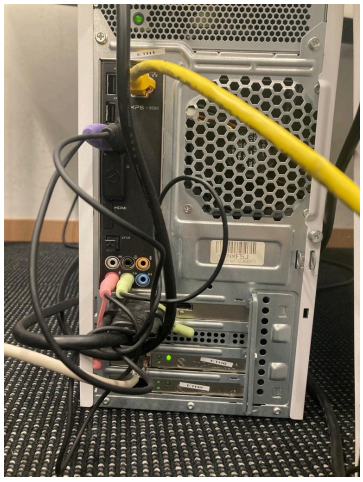
Communication Systems Lab

Exercise 2

September 27, 2022

Group2: Songyi Han and Mohamed Zahir Mohamed Wazeer

Our Topology

- Client1 : { interface: epn3s0, address: 10.1.2.2}
- Route : {interface: epn3s0, address: 10.1.2.1}

2.3. What is the command to add the route?

`$ ip route add default via 10.1.2.1`

2.5. Which hosts are reachable?

Client1 to ping the Router (`$ ping 10.1.2.1`) works. Whereas ping a server from the internet (`$ ping` www.google.com) does not work before allowing packet forwarding on the router

2.6. What does this iptables command do?

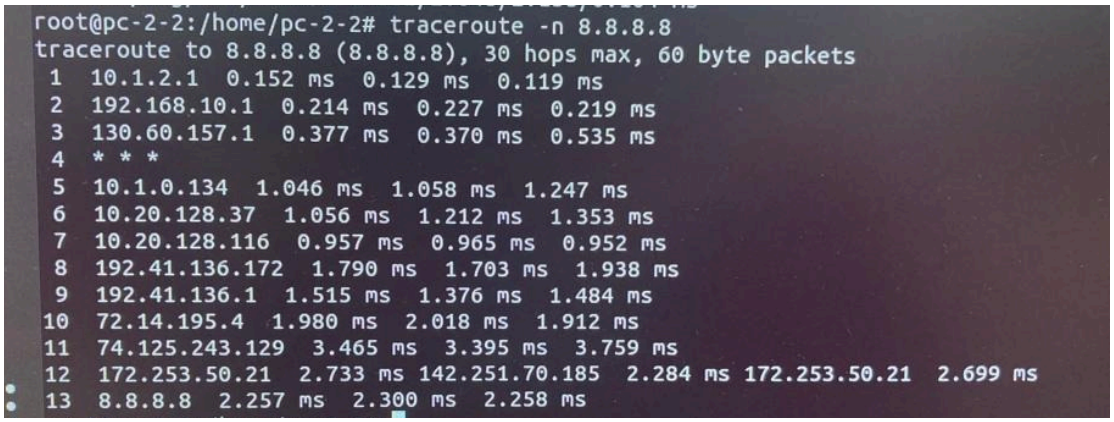
`$ iptables -t nat -A POSTROUTING -s 10.1.2.0/24 -o enp4s0 -j MASQUERADE`

Iptables is used to set up, maintain, and inspect the tables of IPv4 and IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

2.7. Which ones are reachable?

After configuring step 6, sever from the internet is also reachable by domain name

2.8 What does `traceroute -n 8.8.8.8` **output show?**



Traceroute allows to detect the route of the ip packets to the given host. It displays ip addresses, domains and countries of intermediate hops. If hop did not reply it will be shown as asterisk. Traceroute is often used to find problems in packet routing such as unexpected hops, routes longer than expected or even loops in the route.

2.9 Which protocol is used to resolve the MAC address of a host in the same subnet?
ARP(Address Resolution Protocol)

3.2 Questions

(a) What are the benefits of DHCP?

One of the biggest advantages of using the DHCP is that it allows the automatic management of IP addresses. It also offers reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time. It reduces network administration and has a smaller chance that two devices will use the same IP address. It allows for quick, on-the-fly changes. Lastly, you don't have to be onsite to make changes to devices on the network.

(b) What messages are exchanged between the DHCP server and client?

As soon as a client joins the network, it tries to configure its interface with an IP address by exchanging four messages with the DHCP server. These messages are DISCOVER, OFFER, REQUEST and ACK. DHCP is a client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools. DHCP-enabled clients send a request to the DHCP server whenever they connect to a network.

(c) To which destination address is the DHCP request sent?

The DHCP client broadcasts a DHCP DISCOVER message on the network subnet using the destination address 255.255. 255.255 (limited broadcast) or the specific subnet broadcast address (directed broadcast). A DHCP client may also request its last known IP address.

(d) The client sends a DHCP request to obtain an IP address to use. How can it do so without having an IP address in the first place? i.e., what is the source address that is used for the request?

The client discovers a DHCP server by broadcasting a discover message to the limited broadcast address (255.255. 255.255) on the local subnet. If a router is present and configured to behave as a BOOTP relay agent, the request is passed to other DHCP servers on different subnets. DHCP runs at the application layer of the Transmission Control Protocol/IP (TCP/IP) stack to dynamically assign IP addresses to DHCP clients and to allocate TCP/IP configuration information to DHCP clients.

(e) Which port does the DHCP server use?

UDP port number 67 is the port used by the server, and UDP port number 68 is used by the client

(f) Given a network of hosts, how is decided which host is the DHCP server? How can clients find the authoritative DHCP server?

The authority or the entity who runs the network decides which one will be the DHCP though in an ISP level it may get complicated.The client discovers a DHCP server by broadcasting a discover message to the limited broadcast address (255.255. 255.255) on the local subnet. If a router is present and configured to behave as a BOOTP relay agent, the request is passed to other DHCP servers on different subnets.

(g) Based on the previous question - are there any security concerns involved in the operation of DHCP?

An attacker could take over or spoof the DHCP server and hand out bad information to legitimate end users, sending them to a fake site. Or it could hand out legitimate IP addresses to unauthorized users. This could lead to man-in-the-middle attacks and denial of service attacks. Unauthorized DHCP servers can issue incorrect TCP/IP configuration information to DHCP clients. DHCP servers can overwrite valid DNS resource records with incorrect information. DHCP can create DNS resource records without ownership defined.