Cover Page

Lab 7 Preparation
Name: Wei Lin
Student#: 999595193

1. Explain why NAT is often mentioned as a solution to counteract the depletion of IP addresses on the global Internet? Which alternatives to NAT exist that address the scarcity of available IP addresses?

NAT is a router function where private network IP addresses (and possibly port numbers) of IP datagram are replace with public network IP addresses at the boundary of a private network. IP masquerading in NAT allows enterprises or ISP to masquerade private network address space with only one IPv4 public network address on a customer premises router, which dramatically reduces the occupancy of public network IP addresses. Therefore, it is a solution to counteract the depletion of IP addresses. The alternatives to NAT is IPV6.

2. What does the following comment refer to: "NAT destroys the ability to do host-to-host communication over the Internet"?

The comment refers to the concern that NAT breaks universal end-to-end connectivity of hosts on the Internet. A host in the public Internet often cannot initiate communication to a host in a private network, because the communication channel need to be always initiated by the host in the private network first for setting up the address translation table. The issue is worse when two hosts that are in different private networks need to communicate with each other. This is causes by the fact NAT translate all private network IP address to a public IP address. When a sender in a private network sends a packet to a receiver in another private network, NAT will replace the source address of the packet with a public IP address assigned to the NAT router. In that case, the receiver only be able to identify the source address of the packet as the IP address of NAT router but not the IP address of the actual sender.

3. Explain the following terms which are used in the context of Network Address Translation：

a. Static NAT:
Static NAT is a type of NAT in which a private IP address is always mapped to a same public IP address

b. Dynamic NAT:

Dynamic NAT is a type of NAT in which a private IP address is mapped to an arbitrary public IP address from a pool of registered public IP addresses

c. NAT with IP overload:

NAT with IP overload is a modified form of dynamic NAT where the number of inside local addresses is greater than the number of inside global addresses. It allows overloading or the mapping of more than one inside local address to the same inside global address by adding port number and protocol type to the address translation table.

d. Port Address Translations:

Port Address Translations is an extension to NAT that allows multiple hosts on a private network to be mapped to a single public IP address by modifying the port number of outgoing traffic.

e. IP Masquerading

IP masquerading is a kind of NAT that allows internal computers to communicate with the outside without knowing the IP address of outside. It allows one machine to act on behalf of other machines.

4. Refer to RFC 1918 and list the IP address blocks that are reserved for use in private networks. Why is there a need to specify IP addresses for private networks?

Reserved IP address space for private internets:
10.0.0.0 - 10 .255.255.255 (10/8)
172.16.0.0 - 172.31.255.255 (172.16/12)
192.168.0.0 - 192.168.255.255 (192.168/16)

The reason for the separate private address space is that it will not conflict with any public IP addresses on the internet. It means if some hosts use some public IP addresses as their private IP addresses, they will not be able to reach those public IP addresses on Internet anymore.

5. The utility netfilter and the command iptables provide support for NAT in Linux systems. Explain the relationship between the netfilter utility and the iptables command?

netfilter is a packet filtering framework. It is the API that the Linux kernel offers to view and manipulate network packets.

iptbales is an interface that uses netfilter to classify and manipulate packets.

6. Describe the following terms which are used in the iptables command:

a. Chain:

Each chain is a list of rules which can match a set of packets. A rule specifies what to do with a packet that matches.

b. Postrouting

Postrouting refers to the state that the forwarded packet has finished routing and is about to leave the machine

c. Prerouting

Prerouting refers to the state that the packet just arrives at the network interface and no routing decision has taken place.

7. Consider a NAT device between a private and the public network. Suppose the private network uses addresses in the range 10.0.1.0-10.0.1.255, and suppose that the interface of the NAT device to the public network has IP address 128.143.136.80.

a. Write the iptables command so that the addresses in the private network are mapped to the public IP address 128.143.136.80.

iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -j SNAT --to-source 128.143.136.80

b. Write an IOS command so that the addresses in the private network are mapped to the public IP address 128.143.136.80.

ip nat inside source static 10.0.1.0/24 128.143.136.80

8. Explain the meaning of the "magic cookie" in the DHCP protocol.

DHCP messages are an extension of BOOTP message, so they formatted in an identical way. Magic cookie is used to differentiate between a BOOTP and a DHCP message. The fixed magic cookie, 99.130.83.99, indicates that the message is a DHCP message, and everything after the magic number is DHCP options.

9. If the command dhcpd is issued (without arguments) on a Linux PC with multiple network interfaces, which network interfaces does the DHCP server listen on?

If no arguments are specified, dhcpd will identify all network interfaces that are up and listen on all of them.