3/3 4/

Assignment 4

Problem Statement: Installing and configure DHCP server and write a program to install the software on remote machine.

Learning Objective:

1. To install DHCP server
2. To configure DHCP server

Learning Outcome: Students will be able to

- Demonstrate DHCP installation and configuration
- Install software on remote machine

Requirements:

- Open source linux based OS
- Eclipse IDE or Python interpreter

Theory

Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocol designed to provide the four pieces of information for a diskless computer or a computer that is booted for the first time. DHCP is a successor to BOOTP and is backward compatible with it. Although BOOTP is considered deprecated, there may be some systems that may still use BOOTP for host configuration. The DHCP client and server can either be on the same network or on different networks.

DHCP Packet format

- Operation code: This 8-bit field defines the type of DHCP packet: request (1) or reply (2).

- Hardware type: This is an 8-bit field defining the type of physical network. Each type of network has been assigned an integer. For example, for Ethernet the value is 1.

• Hardware length: This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.

• Hop count: This is an 8-bit field defining the maximum number of hops the packet can travel.

• Transaction ID: This is a 4-byte field carrying an integer. The transaction identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.

• Number of seconds: This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.

• Flag: This is a 16-bit field in which only the leftmost bit is used and the rest of the bits should be set to 0s. A leftmost bit specifies a forced broadcast reply (instead of unicast) from the server. If the reply were to be unicast to the client, the destination IP address of the IP packet is the address assigned to the client. Since the client does not know its IP address, it may discard the packet. However, if the IP datagram is broadcast, every host will receive and process the broadcast message.

Flag Format:

• Client IP address: This is a 4-byte field that contains the client IP address. If the client does not have this information, this field has a value of 0.

• Your IP address: This is a 4-byte field that contains the client IP address. It is filled by the server (in the reply message) at the request of the client.

• Server IP address: This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.

• Gateway IP address: This is a 4-byte field containing the IP address of a router. It is filled

by the server in a reply message.

• Client hardware address: This is the physical address of the client. Although the server can retrieve this address from the frame sent by the client, it is more efficient if the address is supplied explicitly by the client in the request message.

• Server name: This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this field with data, the server must fill it with all 0s.

• Boot filename: This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.

• Options: This is a 64-byte field with a dual purpose. It can carry either additional information (such as the network mask or default router address) or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present, the next 60 bytes are options. An option is composed of three fields:
a 1-byte tag field, a 1-byte length field, and a variable-length value field. The length field defines the length of the value field, not the whole option.

DHCP client transition
INIT State :
When the DHCP client first starts, it is in the INIT state (initializing state). The client broadcasts a DHCPDISCOVER message using port 67.

SELECTING State:
After sending the DHCPDISCOVER message, the client goes to the selecting state. Those

servers that can provide this type of service respond with a DHCPOFFER message. In these messages, the servers offer an IP address. They can also offer the lease duration. The default is 1 hour. The server that sends a DHCPOFFER locks the offered
IP address so that it is not available to any other clients. The client chooses one of the offers and sends a DHCP REQUEST message to the selected server. It then goes to the requesting state.
However, if the client receives no DHCPOFFER message, it tries four more times, each with a span of 2 seconds. If there is no reply to any of these DHCP DISCOVERs, the client sleeps for 5 minutes before trying again.

REQUESTING State:
The client remains in the requesting state until it receives a DHCPACK message from the server that creates the binding between the client physical address and its IP address. After receipt of the DHCPACK, the client goes to the bound state.

BOUND State:
In this state, the client can use the IP address until the lease expires. When 50 percent of the lease period is reached, the client sends another DHCPREQUEST to ask for renewal. It then goes to the renewing state. When in the bound state, the client can also cancel the lease and go to the initializing state.

RENEWING State:
The client remains in the renewing state until one of two events happens. It can receive a DHCPACK, which renews the lease agreement. In this case, the client resets its timer and goes back to the bound state. Or, if a DHCPACK is not received, and 87.5 percent of the lease time expires, the client goes to the rebinding state.

REBINDING State:
The client remains in the rebinding state until one of three events happens. If the client receives a DHCPNACK or the lease expires, it goes back to the initializing state and tries to get another IP address. If the client receives a DHCPACK, it goes to the bound state and

resets the timer.

Configuration Steps:

1. To install DHCP server on ubuntu, Type following command on terminal. – sudo apt-get install isc-dhcp-server
2. Now we should configure DHCP server. Configuration file is stored at locatio net//dhcp/dhcpd.conf .

Use gedit to edit dhcpd.conf

```
# A slightly different configuration for an internal subnet.
subnet 172.16.5.0 netmask 255.255.255.0 {
range 172.16.5.2 172.16.5.5;
option domain-name-servers 8.8.8.8;
option routers 172.16.1.1;
option broadcast-address 172.16.5.255;
default-lease-time 600;
max-lease-time 7200;
}
```

3 Now restart service by using following command. – sudo service isc-dhcp-server restart
4. Now on client computer, in network configuration setting just choose automatic configuration. Thats it client get IP address automatically

Steps for installation of Software on Remote Machine:

1. Type following command for installation of ssh in command prompt- – >sudo apt-get install ssh
2. Proceed with installation steps on Remote machine
3. After installation, for obtaining remote access, type following command- – >sudosshhostname@ipaddress – For Example. >sudossh student@172.25.28.60
4. Enter the password for host machine then enter the password for remote machine.
5. After login for installation of any package such as SBCL package type following command:- – >sudo apt-get installpackage_name.

3/3 4/

Conclusion:

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. Hence we installed and configured DHCP and studied installation of software on remote machine.