MIT World Peace University

Computer Networks
Second Year B. Tech, Semester 3

DHCP, DNS and Web Server configuration

Practical Report
Assignment 10

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

November 20, 2022

Contents

1 Aim and Objectives

Aim

To Configure network using Dynamic Host Configuration Protocol (DHCP), DNS and Web server Use Ping utility to test connectivity.

Objectives

1. To learn the DHCP installation and understand the practical use of DHCP, DNS and Web server.
2. To learn the mechanism to access the remote machine by using ping utility to test connectivity.

2 Devices

2.1 Devices Used

1. 1 Wireless Router WRT300N
2. 1 Switch 2950
3. 5 Generic PCs
4. 3 Laptops
5. 1 Web Server

2.2 Device Info and IP Addresses

Subnet Mask: 255.255.255.0

Name	Type	IP
PC0	PC	192.168.0.5
PC1	PC	192.168.0.2
PC2	PC	10.0.0.51
PC3	PC	192.168.0.6
PC6	PC	192.168.0.7
Laptop0	Laptop	192.168.0.3
Laptop1	Laptop	10.0.0.50

3 Cables

1. Straight LAN Cable to connect unlike Devices
2. Crossover LAN Cable to connect like Devices

4 Commands

```
Router>enable
Router#config terminal
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#ip dhcp pool MY_LAN
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.10
```

5 Theory

5.1 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture.

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed.

DHCP can be implemented on networks ranging in size from residential networks to large campus networks and regional ISP networks. Many routers and residential gateways have DHCP server capability. Most residential network routers receive a unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device.

DHCP services exist for networks running Internet Protocol version 4 (IPv4), as well as version 6 (IPv6). The IPv6 version of the DHCP protocol is commonly called DHCPv6.

5.2 The Need for DHCP

1. On an IP network, each device connected to the Internet must be assigned a unique IP address. DHCP helps network administrators to monitor and assign IP addresses in a centralized manner.

2. It can automatically assign a new IP address to a computer when it is moved to another location. DHCP automates the process of allocating IP addresses, which reduces the time required for device configuration and deployment, as well as the possibility of configuration errors.

3. A DHCP server can manage the configurations of multiple network segments. When the configuration of a network changes, an administrator only needs to update the corresponding configuration on the DHCP server.

It Offers the Following Advantages:

1. Reliable IP address configuration
2. Reduced IP address conflicts
3. Automatic IP address management
4. Efficient change management

5.3 DHCP Message Format

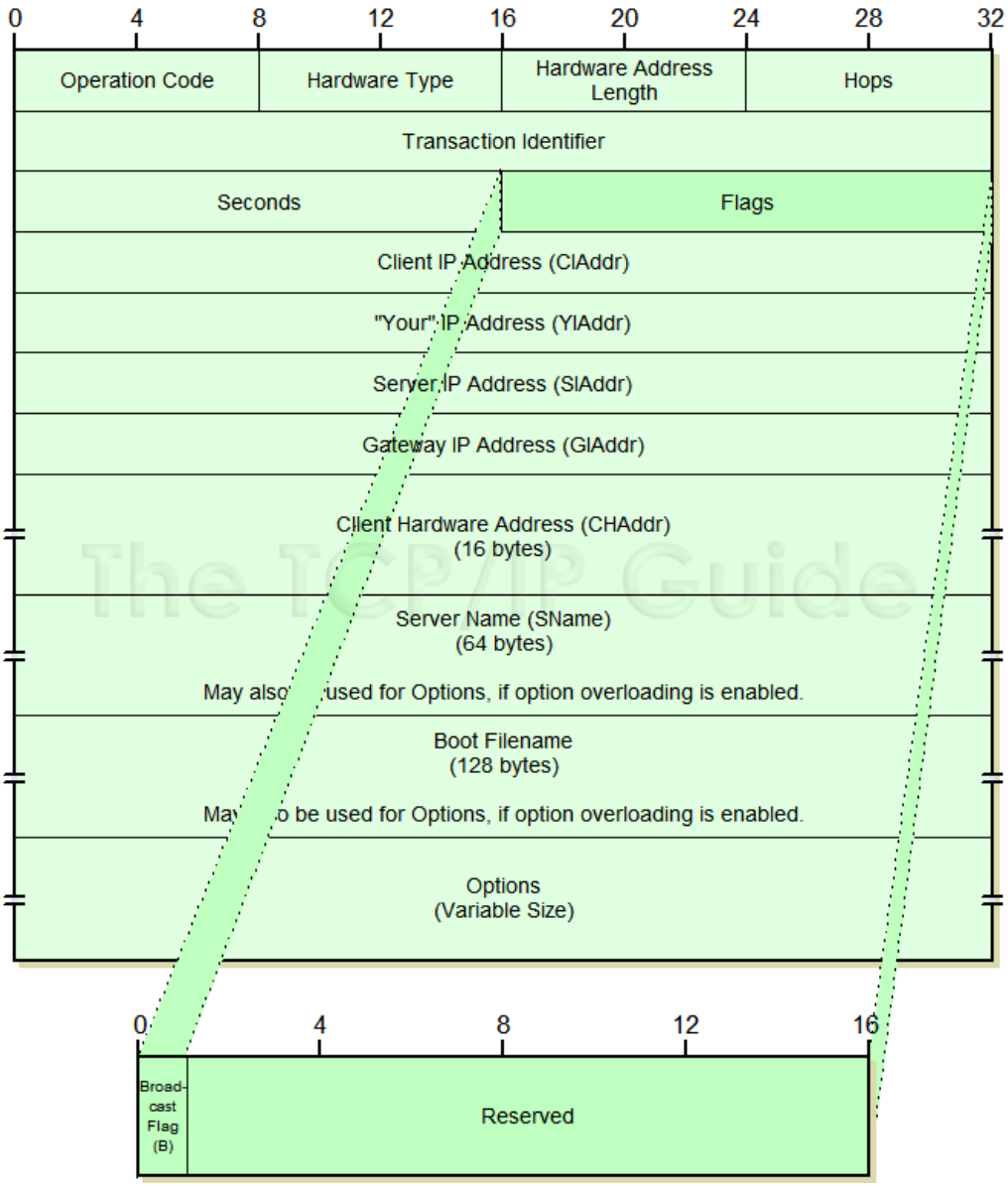


Figure 1: The DHCP Message Format

- *Operation Code*: Specifies the type of the Dynamic Host Configuration Protocol (DHCP) message. Set to 1 in messages sent by a client (requests) and 2 in messages sent by a server (response).
- *Hardware*: Type Specifies the network LAN architecture. For example, the ethernet type is specified when htype is set to 1.
- *Hardware*: Address Length Layer 2 (Data-link layer) address length (MAC address) (in bytes); defines the length of hardware address in the chaddr field. For Ethernet (Most widely used LAN Standard), this value is 6. Hops Number of relay agents that have forwarded this message.
- *Transaction*: identifier Used by clients to match responses from servers with previously transmitted requests.
- *seconds*: Elapsed time (in seconds) since the client began theDynamic Host Configuration Protocol (DHCP) process.
- *Flags*: Flags field is called the broadcast bit, can be set to 1 to indicate that messages to the client must be broadcast
- *ciaddr*: Client's IP address; set by the client when the client has confirmed that its IP address is valid.
- *yiaddr*: Client's IP address; set by the server to inform the client of the client's IP address.
- *siaddr*: IP address of the next server for the client to use in the configuration process (for example, the server to contact for TFTP download of an operating system kernel).
- *giaddr*: Relay agent (gateway) IP address; filled in by the relay agent with the address of the interface through which Dynamic Host Configuration Protocol (DHCP) message was received.
- *chaddr*: Client's hardware address (Layer 2 address).
- *sname*: Name of the next server for client to use in the configuration process.
- *file*: Name of the file for the client to request from the next server (for example the name of the file that contains the operating system for this client).

5.4 DHCP Operation

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the bootstrap protocol (BOOTP). UDP port number 67 is the port used by the server, and UDP port number 68 is used by the client.

DHCP operations fall into four phases: server discovery, IP lease offer, IP lease request, and IP lease acknowledgement. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgement.

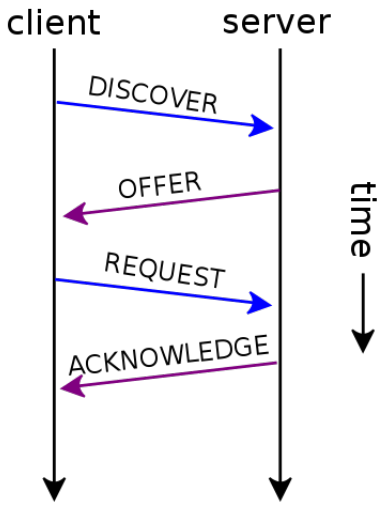


Figure 2: The DHCP Operations - DORA

5.5 DNS and Email server

DNS stands for Domain Name System or Domain Name Server. They are responsible for connecting domain names to web servers. Anytime you connect to the internet and go anywhere, you are using them.

The DNS records translate the domain into the IP address of the server that hosts it. The web server is then responsible for loading the site that matches the requested domain.

5.5.1 SMTP AND DNS

The **Domain Name System (DNS)** is a directory used by SMTP to convert a name, such as renovations.com, to a list of servers that can receive connections for that name and to find the IP address of a specific server. By looking up a destination server's address in the DNS, the sending server can properly route a message to a recipient.

DNS uses two kinds of records: **Mail Exchanger (MX)** records and A records. An MX record maps a domain name to the names of one or more mail hosts. An A record maps a host name to the IP address of a server.

Every email sent also generates a DNS lookup. And just like a domain name, each email address needs to map to an IP address

```
User ID at domain name = info@example.com
```

This format tells mail servers who and where the email should be delivered to. Without DNS, email could not function properly, which would be catastrophic for organizations that rely heavily on online correspondence.

Email runs on the following server types:

1. **SMPT**: Simple Mail Transfer Protocol (SMPT) is used for outgoing mail and is part of the TCP/IP application layer. This protocol works with the Mail Transfer Agent (MTA) running on your mail server to ensure messages are sent to the proper address.

2. **POP3**: Post Office Protocol, version 3 (POP3) is most commonly used for storing sent and received mail on local drives and/or servers. Once a user downloads the mail message, it is removed from the server.

3. **IMAP**: Internet Message Access Protocol (IMAP) stores copies of messages on the server, rather than on a computer or device. This lets a user access files from emails from any device, as well as lets them organize mail without downloading beforehand.

6 Procedure to Configure LAN

1. Create The network topology on the Packet tracer, that has a router, a few PCS near the router, and some connected to it via LAN cables.

2. Add a Web server which is connected to a switch that is connected to other end devices.

3. Run the commands on the router to configure it.

4. Go to the GUI tab in the router, and select the Wireless tab, where you can go to wireless security, and select security mode to WPA2, personal, and encryption to AE5. Assign a password.

5. To the PCs not connected to the router directly, install a wireless network card in them after turning them off, and then turn them back on.

6. Go the PC wireless in the Desktop Settings, and navigate to the Connect Tab. Here refersh the network, and add the WPA2 Passkey that you have assigned to the router.

7. To the webserver, add a Fast ethernet port to connect it.

8. Configure the Web Server, and add the Default gateway as 10.0.0.1

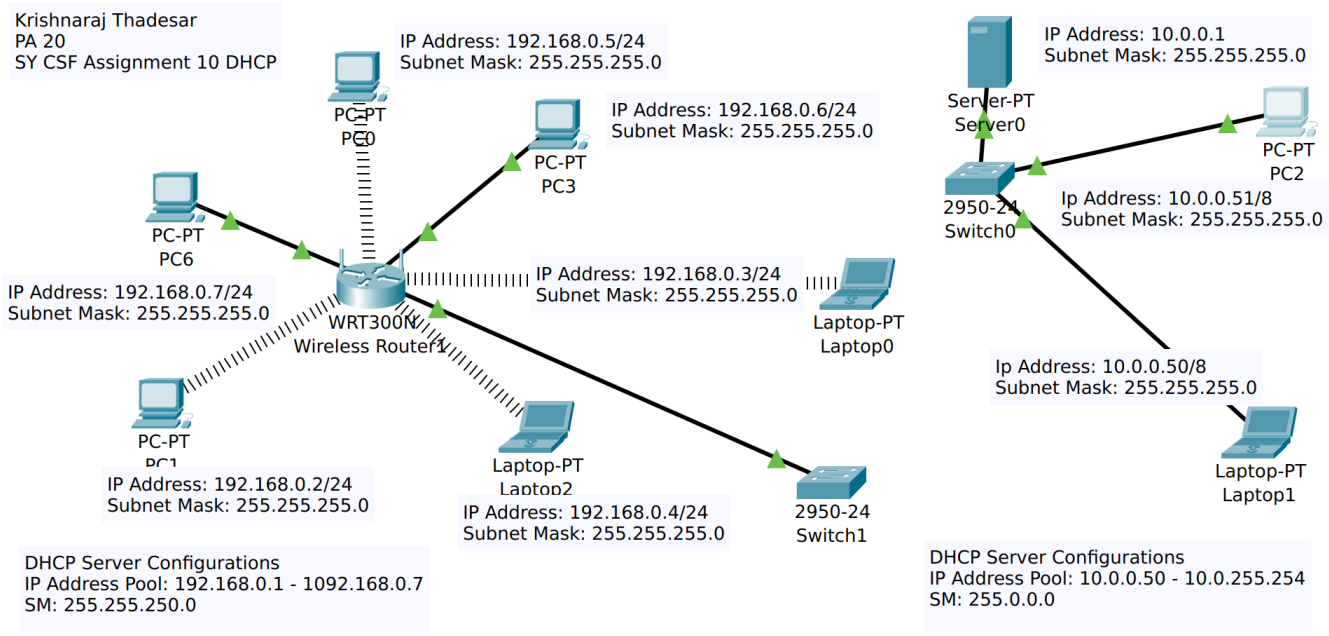
9. Go to the services tab in the web server, and in DHCP, turn it on, and configure the starting and the ending IP addresses. Save.

10. Assign IP Addresses to all the other computers, by selecting on the DHCP Radiobutton instead of the static one, and wait for it to query and assign the IP. Ping and check.

7 Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code
Programs Used: Cisco Packet Tracer v8.2

8 Connection Screenshot



9 Conclusion

DHCP, DNS and Web Server configurations were implemented and understood successfully.

20/11/22

DHCP - DNS - Security

CN Assignment - 10

Krishnaraj PT
Batch - A1
PA20
1032210888

FAQs

Q.1 Ways to check IP address on your machine.

→ (1) Public IP using google

just googling "What is my IP" would get you your public IP address assigned by the ISP to your PC.

(2) Control Panel → View Network Connections to see your local IP

(3) 'ipconfig' on Windows terminal

or 'ip addr' on Linux bash shell.

to see local IPV4 & IP V6 address.

(4) By opening your router's admin page

Q.2 What are the different ways to assign IP address?

→ (1) Static way: Manually configuring it on PC.

Static IP is more reliable and dependable. It is also secure. At

(2) Dynamic: Usually for computers that would log in temporarily. It is assigned on each session on the internet.

(Q.3) What is meant by public and private IP addresses?

→ Private IP Address: The address used to communicate within the same network.

- Scope is local
- free of cost
- only on LAN
- Uniform
- 10.0.0.0 — 10.255.255.255
  172.16.0.0 — 172.31.255.255
  192.168.0.0 — 192.168.255.255

  The rest can be public.
- eg. 192.168.1.1
- Secure
- Require Natting

Public IP: IP used to communicate with the outside network and Internet.

- global scope
- uniform / non-uniform
- Controlled by ISP
- Not free of cost
- eg. 17.5.7.8
- unique ~~to each system~~. ~~and~~ unique code.
- No security.

8.4

DHCP	DNS
Dynamic host control Protocol	Domain Name server
port 53	port 67 & 68.
Supports TCP & UDP	only ~~UP~~ UDP
Decentralized system	Decentralized System
unreliable Configuration of IP	Reliable
Used to allocate IPs to machines	Used to translate IP addresses to ~~name~~ names