STM JOURNALS

International Journal of
Radio Frequency Innovations

Volume 1, Issue 2, 2023
July–December
DOI (Journal): 10.37591/IJRFI

https://journals.stmjournals.com/ijrfi

Research IJRFI

Exploring DHCP Protocol Administration: A Packet Tracer Simulation Study

Sanskruti Karnewaer[1,*], Sushil Bakhtar[2]

Abstract

The following functions of DHCP are included to lessen network administration: TCP/IP setting that is automated and centralized. the capability of centrally defining TCP/IP setups. the use of DHCP options to allocate a complete range of additional TCP/IP configuration values. DHCP runs at the application layer of the TCP/IP stack. Although this essay will concentrate on Windows NT, another advantage of DHCP is that it is compatible with a wide range of hardware and software systems. The majority of TCP/IP client software implementations support DHCP, while DHCP server software is available on most operating systems. Moreover, connections can be established between any DHCP server and any DHCP client. It provides DHCP clients with TCP/IP setup information and dynamically assigns IP addresses to them. DNS addresses, subnet mask information, and IP addresses of default gateways are all included in this data.

Keywords: DHCP protocol, IP address, router, server, diffserv codepoints

INTRODUCTION

DHCP Defined

With DHCP, an Internet standards track protocol currently described in Request for Comments (RFC) 2131, a server on a TCP/IP network can supply configuration information to clients. This information includes the domain name, subnet mask, DNS, WINS, cookie, and/or time server addresses, as well as the default gateway (router). Additionally, DHCP specifies a method for assigning IP host addresses. Another benefit of DHCP is that it works with both hardware and software platforms, albeit this essay will focus on Windows NT. DHCP is supported by most TCP/IP client software implementations, and most operating systems have DHCP server software available. Furthermore, any DHCP server and any DHCP client can connect with one another [1, 2].

DHCP supports three different mechanisms for IP address allocation:

Automatic allocation: A client receives a permanent IP address from the server.

***Author for Correspondence**
Sanskruti Karnewaer
E-mail: sanskrutikarnewar21@gmail.com

[1]Student, Department of Electronics and Telecommunication, Prof Ram Meghe College of Engineering and management, Amravati, Maharashtra, India
[2]Assistant Professor, Department of Electronics and Telecommunication, Prof Ram Meghe College of Engineering and management, Amravati, Maharashtra, India

Received Date: April 08, 2024
Accepted Date: April 18, 2024
Published Date: April 29, 2024

Citation: Sanskruti Karnewaer, Sushil Bakhtar. Exploring DHCP Protocol Administration: A Packet Tracer Simulation Study. International Journal of Radio Frequency Innovations. 2023; 1(2): 1–11p.

Allocation dynamically: The server allots an IP address to a client for a predetermined amount of time (referred to as the lease) or until the client officially forfeits the address.

Manual allocation: The network administrator has specifically assigned the address that the server sends to the client [3, 5].

Any given site will employ one or more of these processes for address allocation, depending on the policies set out by the local network management. However, only dynamic allocation allows addresses that are no longer in use to be

© STM Journals 2023. All Rights Reserved

automatically reused. Because of this feature, DHCP can be a helpful and straightforward technique for giving client systems that are only momentarily connected to a network temporary addresses. For instance, dial-up hosts are nearly always allocated a temporary IP address by ISPs using DHCP, which ensures that the address is only assigned to the host for the duration of the connection. We will talk about this form of DHCP since it is the most frequently used [4–10].

DHCP Operation

The operation of DHCP is straightforward, and it operates on a relatively simple protocol. If an option such as Server issued IP address is selected or the IP address is set to 0.0.0.0, a host computer that supports DHCP will function as a DHCP client. These options won't be available if DHCP client software isn't present in a certain TCP/IP suite; Unix, OS/2, and Windows 95/98/NT systems all support DHCP as a native client service in the TCP/IP kernel. For instance, Figure 1 illustrates how to set up a Windows 95 TCP/IP client to use DHCP by choosing the TCP/IP Properties window's Obtain an IP address automatically option. Set up for DHCP on a client system (windows 95) is shown in Figure 1.

The messages exchanged during the four fundamental DHCP functioning phases are depicted in Figure 2. Similar to most TCP/IP programs, DHCP operates on a client-server architecture, with the client starting the session. All DHCP messages are sent as User Datagram Protocol (UDP) datagrams, even if they aren't displayed here. Messages sent from the client to the server are sent to UDP port 67 (DHCP server) at the server, and messages from the server to the client are sent to UDP port 68 (DHCP client) at the client [11-14].

When a client makes its first request for an IP address, the initialization step begins:

The client sends a DHCPDISCOVER message over the local IP network to identify the DHCP server(s). The client uses an IP broadcast address to send the message because it does not know the address(es) of the DHCP server(s). A DHCPOFFER message is returned by every DHCP server that is available.

The client must choose which server to use if there are multiple; generally, the first server to answer is chosen, though there is no hard-and-fast rule in this regard. The client broadcasts a DHCPREQUEST specifying the server that will be utilized (and indirectly informing all other servers that they won't be used), regardless of the number of servers that respond.

The designated IP address, any further network parameter assignments, and the lease—the duration of the address assignment—are sent back by the chosen server in a DHCPACK response.

The address renewal timer (T1) and the server rebinding timer (T2) are the two timers that the DHCP client keeps track of. T1 and T2 are initially configured to represent 50% and 87.5%, respectively, of the lease time. When the address is assigned, the host has the option to change the values of both timers (although T1 must be less than T2).

The client attempts to renew its address lease when the T1 period expires, entering the Renewal phase:

The client sends a DHCPREQUEST to the server that assigned the address.

The server responds with a DHCPACK and a new lease period.

As long as the server renews the address lease during the T1 period, the T2 timer will never expire. In the event that T2 does expire, the client enters the Rebind phase and searches for any other server that will renew the address:

© STM Journals 2023. All Rights Reserved

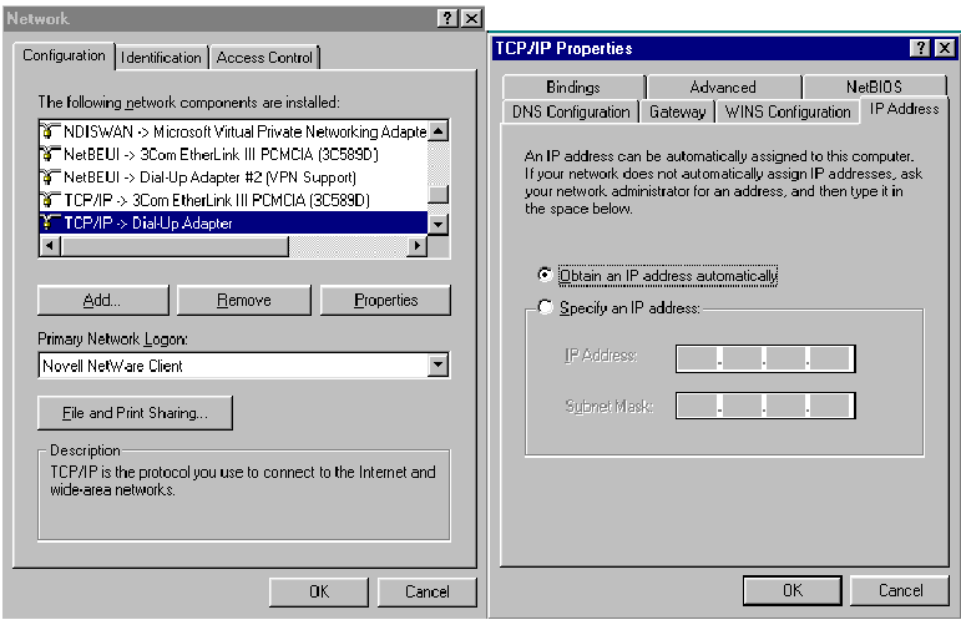

FIGURE 1. Setup for DHCP on a client system (Windows 95).

Figure 1. Set up for DHCP on a client system (windows 95).

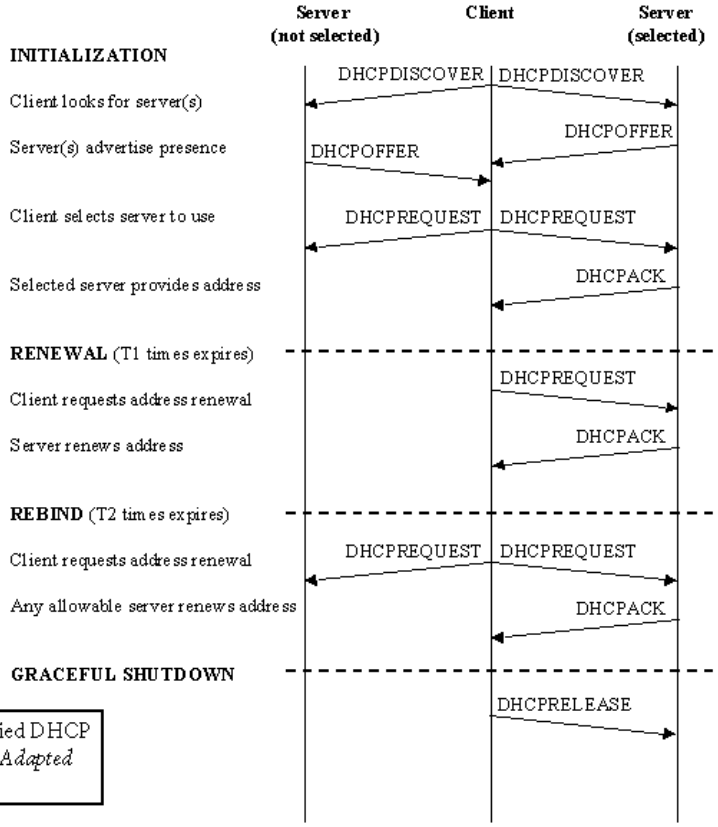

FIGURE 2. Simplified DHCP message exchange. *Adapted from RFC 2131.*

Figure 2. Simplified DHCP message exchange. Adapted From RFC2131.

The client sends a DHCPREQUEST to find any DHCP server that will extend the lease. A DHCPACK and a new lease period are returned by any server that is able to extend the lease for this address.

© STM Journals 2023. All Rights Reserved

The client is prepared to give up the address and cut off from the network at some point. The client will send a DHCPRELEASE to the server, relinquishing its claim to the IP, if it supports graceful shutdown.

Although it covers the DHCP protocol's fundamental functions, this explanation is intentionally condensed and omits a lot of information. It should be mentioned that DHCP is an insecure protocol because it is challenging to safeguard the systems that it is meant to support. Furthermore, a malevolent individual can quickly set up an unapproved DHCP server, which can subsequently provide clients with disruptive data like false or duplicate IP addresses, as well as inaccurate gateway or name server addresses.

Furthermore, a malevolent DHCP client has the ability to seize any address that is accessible and prevent other users from using it. DHCP use over a firewall should only be used when absolutely essential for these and other reasons.

RESULT

We will learn about configuring DHCP servers with Cisco Packet Tracer in this tutorial.

How to Use Cisco Packet Tracer to Configure and Check the DHCP Server:

Step 1: Open the Cisco Packet Tracer desktop first, then choose one of the devices listed below in Table 1.

- Now create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others as shown in Figure 3

Table 1. Devices use in the configuration of Cisco Packet.

S.N.	Device	Model Name	Unit
1.	PC	PC	5
2.	Switch	PT-Switch	2
3.	Router	PT-Router	1
4.	Server	Server-PT	1

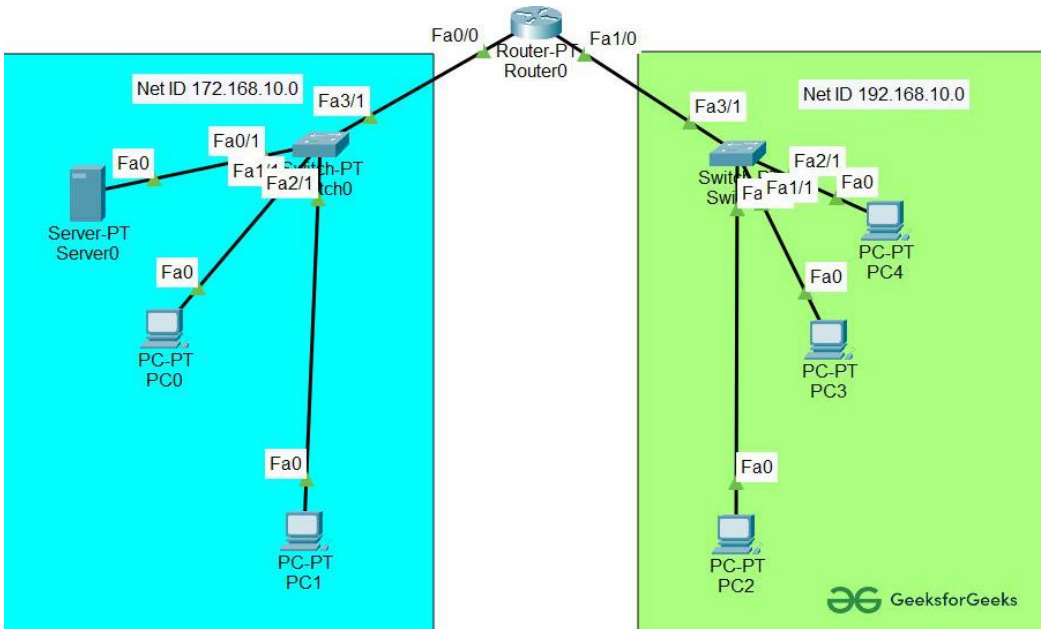

Figure 3. Connection of devices using automatic cable.

© STM Journals 2023. All Rights Reserved

Step 2: Configure the Server with IPv4 address and Subnet Mask according to the Data given below in Table 2.

- To assign an IP address in Server, click on Server-PT.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Add IPv4 address, subnet mask, and Default Gateway as shown in Figure 4.
- Assigning IP address using the ipconfig command as shown in Figure 5
- We can also assign an IP address with the help of a command.
- Go to the command prompt of the server
- Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

Table 2. Data to Configure the Server with IPv4 address and Subnet Mask

Parameters	Address value
IPv4 Address	172.168.10.2
Subnet Mask	255.255.255.0
Default-Gateway	172.168.10.1

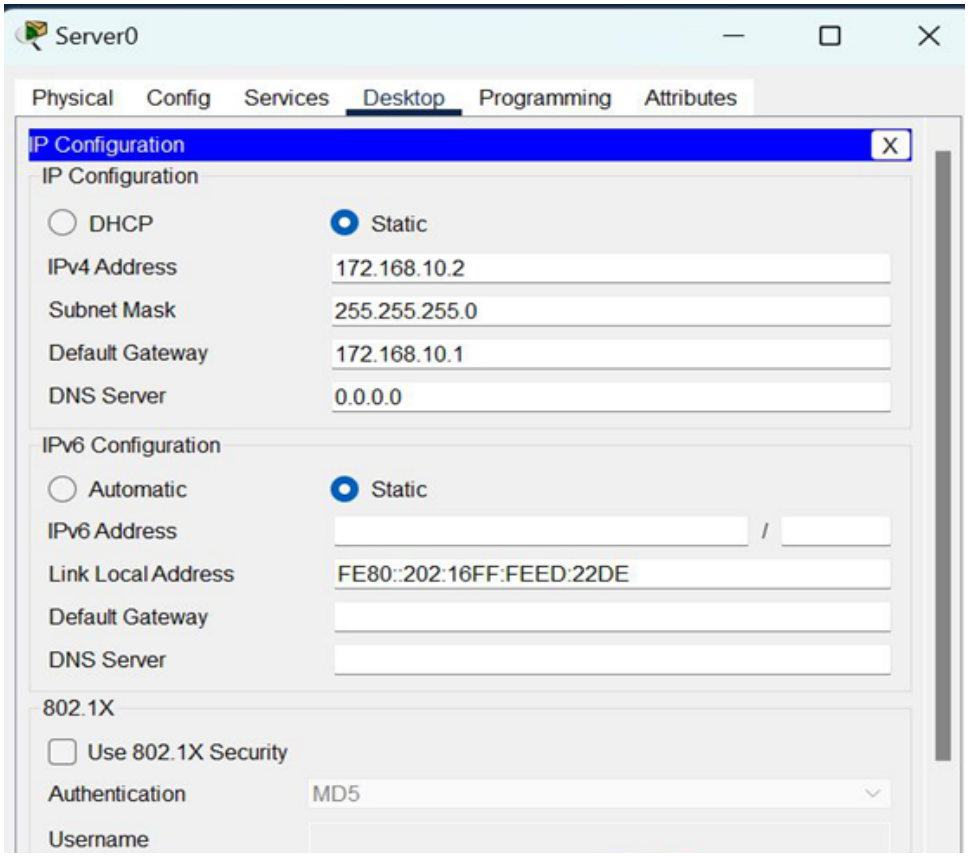

Figure 4. Configure the Server with IPv4 address and Subnet Mask according to the Data

Example

ipconfig 172.168.10.2 255.255.255.0 172.168.10.1

Step 3: Configuring the DHCP server as shown in Figure 6.

- To configure the DHCP server first,
- Click on Server then, Go to services.
- Click on DHCP and turn on the services and, configure the DHCP server with the help of the data given below in Table 3.

© STM Journals 2023. All Rights Reserved

- Delete the default values of Start IP Address and subnet Mask then save the info.
- Create two new pools.
- POOL1 and POOL2 and fill the data as shown in the images below.

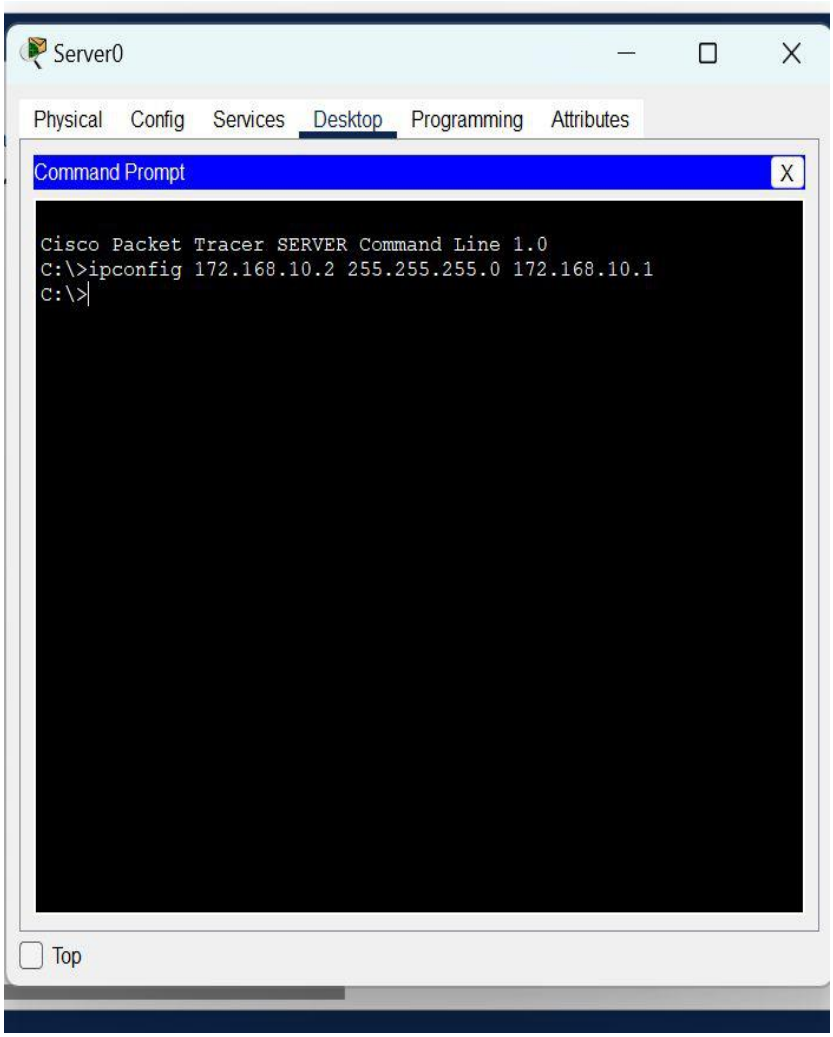

Figure 5. Assigning IP address using the ipconfig command.

Step 4: Configuring Router with IPv4 Address and Subnet Mask.

- IP Addressing Table for Router:
- To assign an IP address in router0, click on router0.
- Then, go to config and then Interfaces, and make sure to turn on the ports.
- Then, configure the IP address in FastEthernet according to IP addressing Table as shown in Figure 7.

Table 3. Services to configure the DHCP server.

S.N.	Device	Interface	IPv4 Address	Subnet Mask
1.	router0	FastEthernet0/0	172.168.10.1	255.255.255.0
2	FastEthernet0/1	192.168.10.1	255.255.255.0	

Fill IPv4 address and subnet mask.

© STM Journals 2023. All Rights Reserved

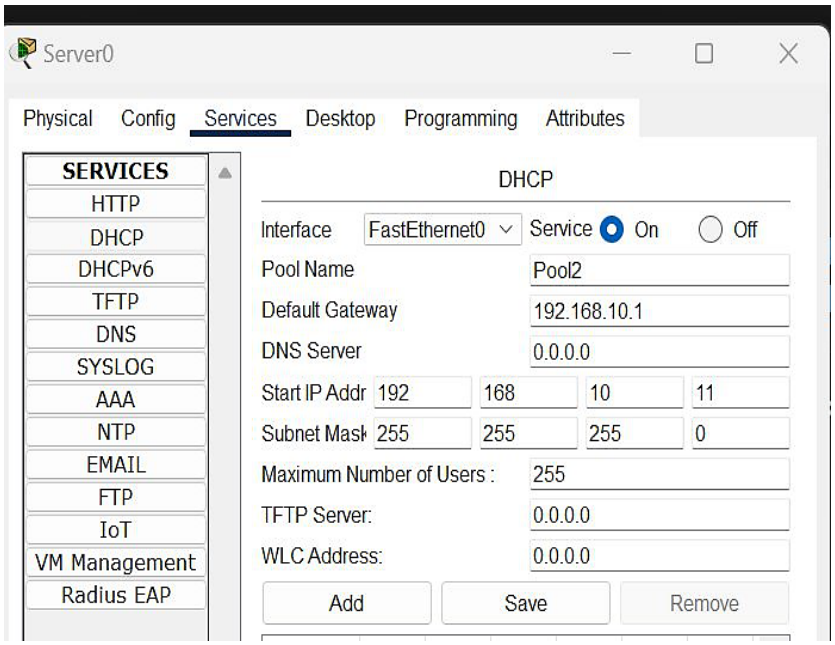

Figure 6. Configuring the DHCP.

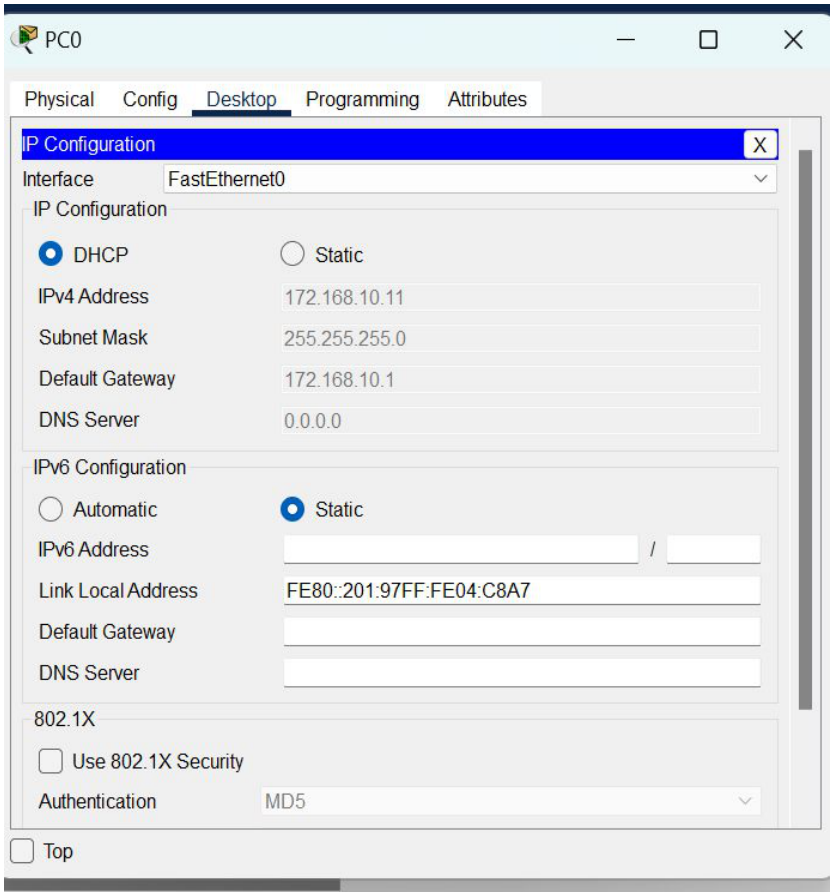

Figure 7. Configuring Router with IPv4 Address and Subnet Mask.

Step 5: Configuring the PCs and changing the IP configuration.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.

© STM Journals 2023. All Rights Reserved

- Change its state from static to DHCP.
- It will automatically fetch the data and configure itself.

Output

The PCs will be configured and changing in IP configuration will takes place as shown in Figure 8.

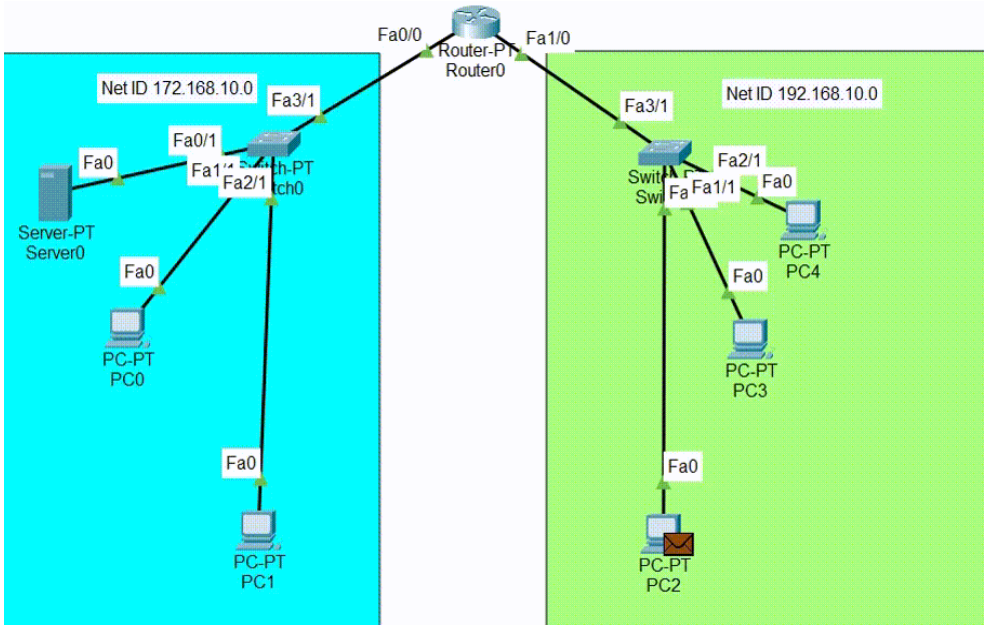

Figure 8. Configuring the PCs and changing the IP configuration.

Experimental Setup

How to configure DHCP server in Packet Tracer.

Hello and welcome! This tutorial will guide you on how to configure a DHCP server both on a router and on a generic server in Cisco Packet Tracer. In both cases, configuration is simple as long as you have a basic knowledge of IP addressing. On to it then!

Configuring DHCP server on a Router.

1. Build the network topology as shown in Figure 9.
2. On the router, configure interface fa0/0 to act as the default gateway for our LAN.
   - 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
3. Configure DHCP server on the Router. In the server we will define a DHCP pool of IP addresses to be assigned to hosts, a Default gateway for the LAN and a DNS Server.
4. Now go to every PC and on their IP configuration tabs, enable DHCP. Every PC should be able to obtain an IP address, default gateway and DNS server, as defined in step 2 and shown in Figure 10.

For example, to enable DHCP on PC1:

Click PC1->Desktop->IP configuration. Then enable DHCP:

© STM Journals 2023. All Rights Reserved

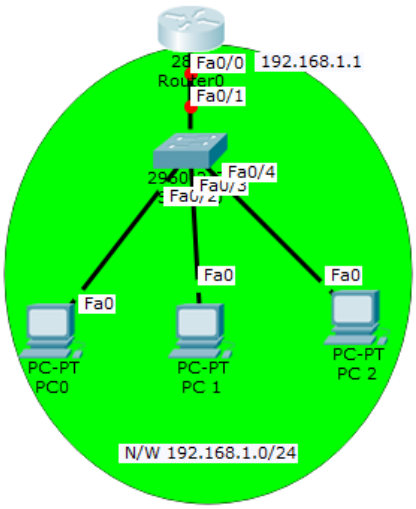

Figure 9. Network topology.

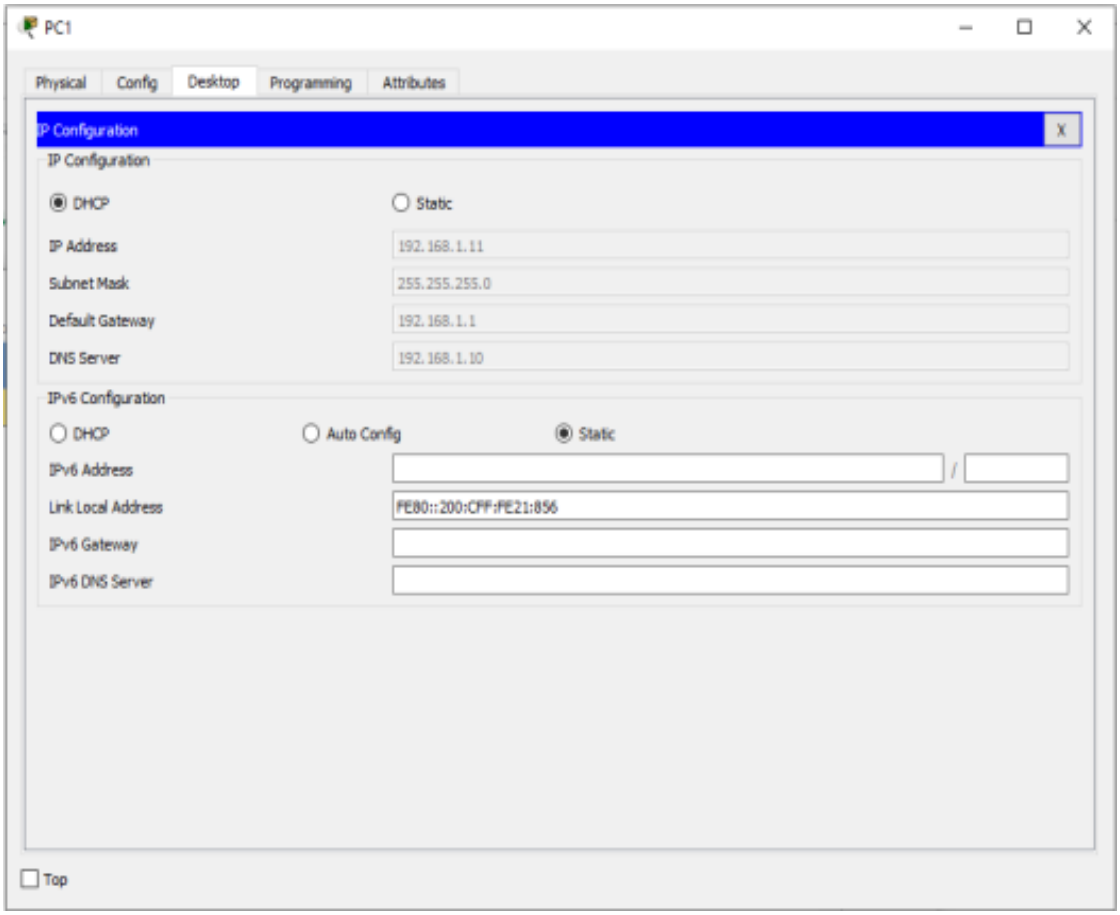

Figure 10. Window to show the process of enable DHCP.

1. Build the network topology in packet tracer is shown in Figure 11.
2. Configure static IP address on the server (192.168.1.2/24). Now configure DHCP service on the generic server as shown in Figure 12
3. To do this, click on the server, then click on Services tab. You will pick DHCP on the menu. Then proceed to define the DHCP network parameters as follows:
4. Here are the configurations on the server:
5. Once you've configured everything, turn ON the DHCP service.

© STM Journals 2023. All Rights Reserved

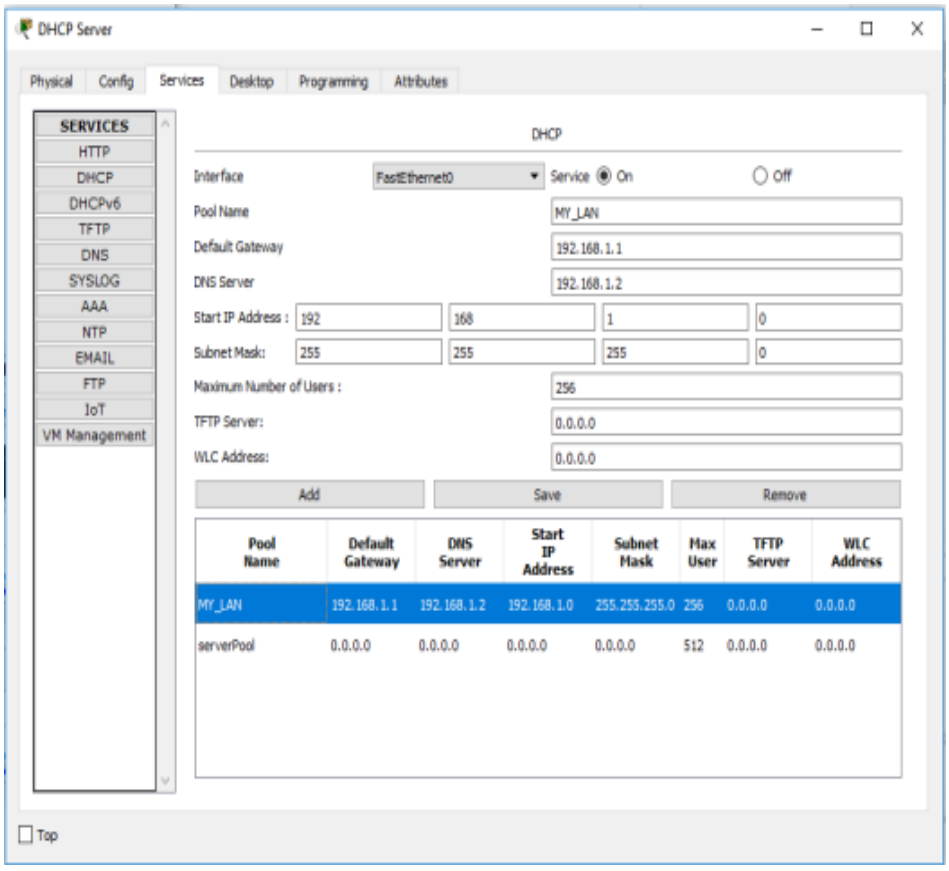

Figure 11. Building of Network topology in packet tracer.

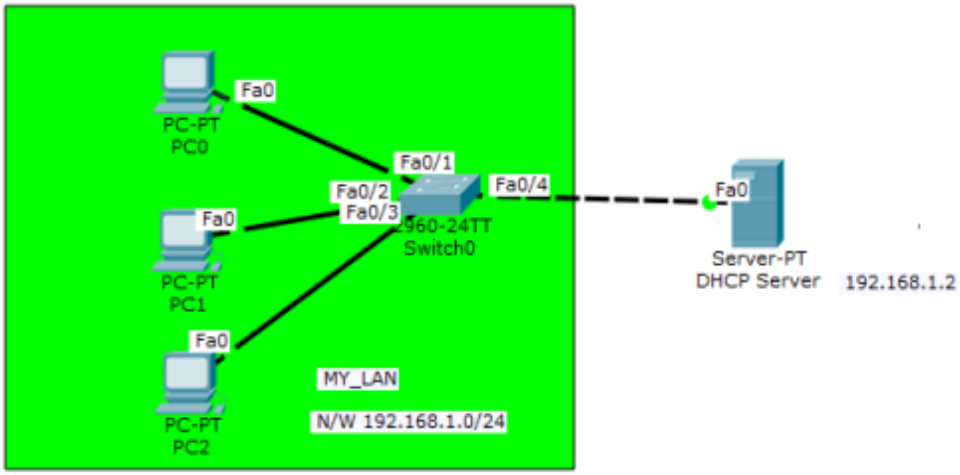

Figure 12. Configuration of static IP address.

Experimental Result

Finally, enable DHCP configuration on each PC. The three PCs should get automatically configured.

CONCLUSION

Network resources are made available to mobile hosts, like notebook computers, via DHCP. The current DHCP protocol does not take security into account. Every client can use the network provided they configure network resources such IP addresses. The Dynamic Host Configuration Protocol

© STM Journals 2023. All Rights Reserved

(DHCP) is used to setup network devices for connections on IP networks. Through the DHCP protocol, a DHCP server gives a DHCP client configuration information, such as an IP address, a default route, and one or more DNS server addresses.

REFERENCES

1. Lin, C. Su, T. and Wang, Z., 2011, "Summary of high-availability DHCP service solutions," in 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), Shenzhen, pp. 1–5.
2. Senecal, L., 2006, "Understanding and Preventing Attacks at Layer 2 of the OSI Reference Model," in 4th Annual Communication Networks and Services Research Conference, pp.6–8.
3. 2002, "DHCP servers subject to remote takeover," Network Security, vol. 2002, no. 5, p. 3.
4. Wilson, P., 2003, "Rogue Servers," Network Security, vol. 2003, no. 8, pp. 16–18.
5. Duangphasuk, S., Kungpisdan S., and Hankla, S., 2011 "Design and implementation of improved security protocols for DHCP using digital certificates," in 17th IEEE International Conference on Networks (ICON), pp. 287–292.
6. Brik, V., Stroik, J., & Banerjee, S. (2004). Debugging DHCP Performance. ACM, 257–262.
7. Dai, J.-W., & Chiang, L.-F. (2007). A New Method to Detect Abnormal IP Address on DHCP. IEEE.
8. Mcauley, A. J., & Manousakis, K. (2000). Self-Configuring Networks. IEEE, 315–319.
9. Park, C.-J., Ahn, S.-J., Chung, J.-W., Lee, C.-H., & Park, C.-S. (1997). The Improvement for Integrity between DHCP and DNS. IEEE, 511–516.
10. Wang, J.-H., & Lee, T.-L. (2002). Enhanced Intranet Administration in a DHCP-enabled Environment. IEEE.
11. Droms, R., 1999, "Automated configuration of TCP/IP with DHCP," IEEE Internet Computing, vol. 3, no. 4, pp. 45–53.
12. "CoovaChilli", http://coova.github.io/CoovaChilli.
13. Yaibuates, M. and Chaisricharoen, R., 2014, "ICMP Based Malicious Attack Identification Method for DHCP," in 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), Chiang Rai, pp. 1–5.
14. Braden, R., 1989, "Requirements for Internet Hosts-Communication Layers", RFC 1122, pp. 42.

© STM Journals 2023. All Rights Reserved