STM JOURNALS

International Journal of
Satellite Remote Sensing

Volume 1, Issue 1, 2023
January–June
DOI (Journal): 10.37591/IJSRS

https://journals.stmjournals.com/ijsrs

Research IJSRS

Configuring Connectivity: Cisco Packet Tracer DHCP Server Best Practices

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

Abstract

In internet protocol (IP) networks, the dynamic host configuration protocol, or DHCP, is a network administration protocol that uses an architecture based on clients and servers to dynamically allocate internet protocol (IP) addresses and other interface characteristics to devices that are connected to the network. It explains routing between the ISP and the campus router uses a static route between the ISP and the gateway, and a default route between the gateway and the ISP. The loopback function domain on the ISP router identifies the ISP connection to the World Wide Web. You can use any router that satisfies the interface criteria. This covers the subsequent items and all conceivable pairings of them: 800, 1600, 1700, 2500 and 2600 series routers and identified the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. conduct the following steps on each router unless specifically instructed otherwise.

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

INTRODUCTION

Using an architecture consisting of client-servers, the Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in Internet Protocol (IP) networks that lets devices connected to the network automatically get IP addresses and other communication features. The technique does away with the need to manually configure each network device separately. It consists of two network components: a network DHCP server located in the centre of the network and client instances of the protocol stack on each computer or device. A client uses DHCP to ask the server for a set of parameters when it first connects to the network and then on a regular basis after that.

DHCP is compatible with all types of networks, including large university networks, tiny home networks, and local ISP networks. Numerous household gateways and routers can serve as DHCP servers. Most home network routers have a unique IP address issued to them within the ISP network. A DHCP server assigns a local IP address to each device connected to a local network. For networks utilizing IPv4 and IPv6 (Internet Protocol versions 4 and 6), DHCP services are offered. We refer to the DHCP protocol's IPv6 version as DHCPv6.I.

***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: August 22, 2023
Accepted Date: December 12, 2023
Published Date: December 23, 2023

Citation: Sanskruti Karnewaer, Sushil Bakhtar. Configuring Connectivity: Cisco Packet Tracer DHCP Server Best Practices. International Journal of Satellite Remote Sensing. 2023; 1(1): 29–35p.

Related Study

The goal of the Internet protocol's enhanced capabilities for differentiated services is to allow for scalable service discrimination over the network without requiring per-flow state and signaling at each hop [1]. A limited, well-defined collection of building blocks that are installed in network nodes

can be used to create a wide range of services. The services can be end-to-end or intradomain, and they can meet both relative performance-based (like "class" differentiation) and quantitative performance-based (like peak bandwidth) criteria. Combining the following methods can result in the construction of services: setting bits in an IP header field at network boundaries (hosts, internal administrative boundaries, autonomous system boundaries), utilizing those bits to control how packets are forwarded by network nodes, and conditioning the marked packets at network borders in compliance with the specifications or guidelines of each service; and using those bits to ascertain how packets are sent by the nodes inside the network.

A restricted shared set of Diffserv Codepoints (DSCPs) and Per-Hop Behaviours (PHBs) was specified by D. Black and R. Geib to be used at (inter)connections of two independently managed and run networks. Multiprotocol Label Switching (MPLS) is used by several network operators to connect their networks to one another. MPLS uses Treatment Aggregates for traffic annotated with various Diffserv Per-Hop Behaviours. They presented a straightforward interconnection methodology that could streamline Diffserv's functionality for network connectivity between MPLS-enabled and Short Pipe Model-applying providers. Their topology is applicable to both MPLS and non-MPLS networks, while it was inspired by the needs of MPLS network operators using Short Pipe Model tunnels [2]. McQuistin and Perkins discovered that 82.0% of the hosts that are reachable via TCP can negotiate and use ECN successfully in their research, support for using ECN with TCP has grown, and it is generally usable with UDP traffic [3]. Real-time applications that have specific performance needs and are susceptible to jitter (variation in delay) and packet loss can benefit from the highest priority class [4]. Several anomalies that appear in almost all traceroute-based measurements are described in the work of Augustin et al. They presented Paris traceroute; a novel publicly available traceroute that manipulates the contents of packet headers to get a more accurate image of the real pathways that packets traverse [5]. In a properly operating network, Bless et al suggested a differentiated services per-domain behaviour (PDB) whose traffic may be "starved" (but starvation is not necessarily needed) [6].

IN CISCO PACKET TRACER

The server is one of the many endpoints provided by the Cisco packet tracer that users can use to build networks. DHCP, email, FTP, HTTP, and many other services are all provided by this one server. To establish connectivity, the user must first assign the server a static IP address before turning on the DHCP service. The user will switch the IP configuration from static to DHCP since the PC needs to be set up to accept IPs from the DHCP server. To configure the DHCP service, the user needs to click on the DHCP tab and turn on the DHCP service. Pool's default name, serverpool, can be changed. If necessary, the user can configure DNS and the default gateway in accordance with their network configuration [7-11]. Establish the start IP address so that the server can assign an IP address based on the previously stated scope as shown in Figure 1. To prevent the server from leasing IP addresses to devices after the limit is met, the user must now specify the maximum number of users. Since the specified limit in this case is 10, even if the specified IP range scope contains many IP addresses, the server will only release 10 IP addresses as shown in Figure 1.

The server can have multiple pools included, and any pool that is not needed can be quickly eliminated. The server now has a lot more IP addresses to assign because pool1, an additional pool, was added with a different IP range. An IP address is assigned based on the server's chosen scope. The user has finished configuring the server's DHCP as shown in Figure 2. In the upcoming packet tracer lab, user must set up the router as a DHCP server.

To set up the routers with DHCP capabilities, the user must utilise the router's command-line interface, but it still needs to configure the same parameters on the router. In only four simple steps, it will configure DHCP on the Cisco router establishing and titling a swimming pool. We have called the DHCP pool in the lab "dynamic." As they can see, the router is now functioning as a DHCP server as the PC has received the IP address from it. DHCP Configuration (as shown in Figure 3) of a Router Using Packet Tracer.

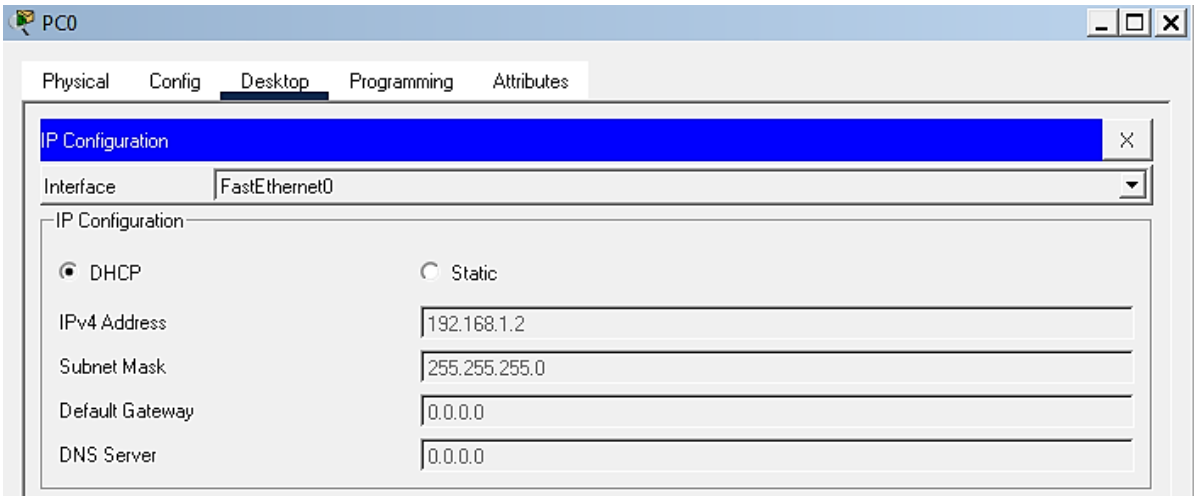

Figure 1. Pool adding.

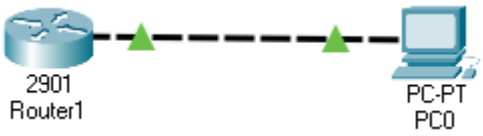

Figure 2. Router configuration.

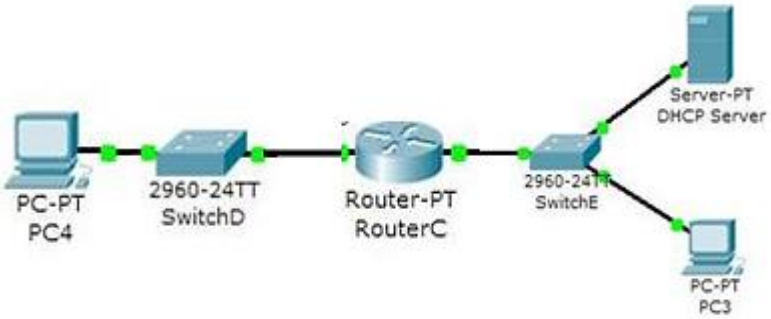

Figure 3. DHCP Configuration.

Using this example of a DHCP Cisco Packet Tracer router, we have focused on DHCP implementation in Cisco Packet Tracer. Stated differently, we have examined how to set up a DHCP server using a Packet Tracer router. We wanted to go over some fundamental DHCP information before we started. DHCP utilizes UDP 67 and UDP 68 ports. For DHCP Server and DHCP Client communication, it has a messaging system. The following lists the messages and their types from these messaging systems:

- DHCP Discover (broadcast)
- DHCP Offer(broadcast)
- DHCP Request (broadcast)
- DHCP Ack (broadcast)
- DHCP Nak (unicast)
- DHCP Release (unicast)
- DHCP Decline (unicast)
- DHCP Inform (unicast)
    a. To begin with, a client broadcasts a "DHCP Discovery" message stating that it requires an IP address.
    b. Next, the client receives configuration offers from the DHCP servers via the "DHCP Offer" unicast message.

c. Next, using the "Transaction ID" of the first DHCP server to provide an offer, the DHCP client broadcasts a "DHCP Request" message to the network. The other servers are aware that the client desires to connect to the server that is associated with the "Transaction ID."
d. Lastly, the server either delivers a reject message known as "DHCP-NACK" or a unicast "Acknowledgment" message to the client stating that the IP assignment was completed successfully.

A Packet Tracer Router's DHCP configuration requires a few simple steps to follow.

Broadcast domains are a key component of this arrangement. Our task is easier if our topology has just one broadcast domain; if not, we need to use the "IP-helper address" function for assistance.

IP Helper Address Command

The command that assists us in persuading the router to allow broadcast packets through is IP helper address. Moving on, let's examine our two distinct configuration topologies and learn how to set up a DHCP server in packet tracer. One Broadcast Domain's DHCP Packet Tracer Configuration. The topology of our single broadcast domain is shown below in fig4. In addition to its routing capabilities, the router will serve as our DHCP server, and there is a switch for PCs.

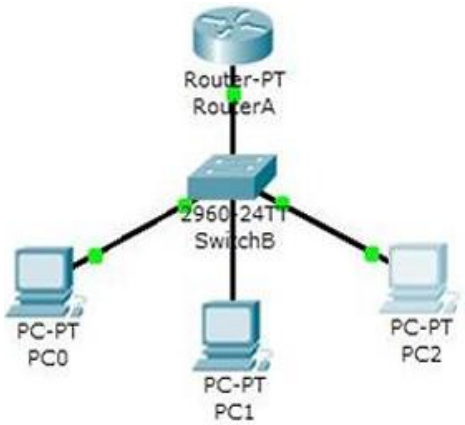

Figure 4. DHCP Example topology (One Broadcast Domain).

First, let's look at How to Set Up a Packet Tracer Router's DHCP Server for a Single Broadcast Domain. In the first scenario of our DHCP Cisco packet tracer example, our One Broadcast Domain structure appears as presented in Figure 4. Along with its routing functions, a router will also perform the duty of server. There's also a PC switch there.

The router connection on router A that is connected to the switch will first have an IP address assigned to it. Second, we're going to make an IPD DHCP pool. We shall provide the IP addresses that the DHCP clients will receive in this pool. The interface address of the router will then be set as the clients' default router address. Finally, in the final section, we will use the "ip dhcp excluded address" command to omit specific addresses that we do not want to utilize for the dynamic IP assignments. The specified addresses won't be used in the pool when the "ip dhcp excluded address" command is used. DHCP messaging system is shown in Figure 5.

Following this arrangement, 192.168.10.11 will be displayed when we check PC0's IP address. since it is the DHCP pool's first accessible address.

Both 10.10.0.0 and 192.168.1.0 require their own DHCP pools. The DHCP Server screenshot below illustrates how these allocations will be completed. As you can see, the DHCP server provides our PCs with their IP setup. IP addresses are assigned automatically.

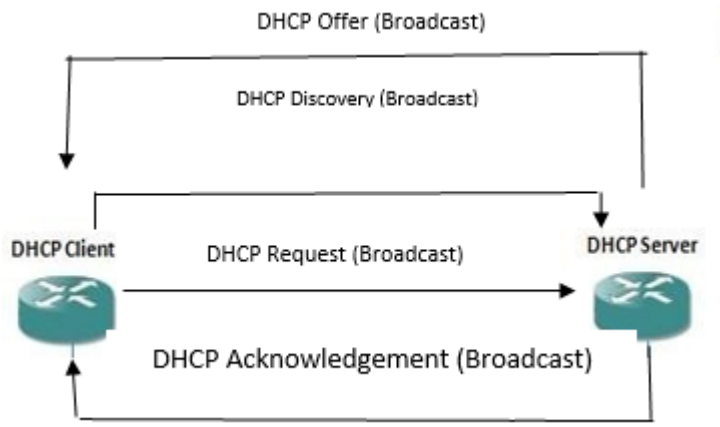

Figure 5. DHCP Messages.

Packet Tracer Router Configuration Basics

I'd like to share with you some information regarding essentially configuring a Cisco router using Packet Tracer. These are necessary for router configuration, although they are not part of the DHCP configuration. Here, we'll cover setting up our laptop to connect to a router, renaming a router, configuring console access, setting passwords on Cisco routers, and setting up basic static routing settings step-by-step.

Setting Up a laptop to Connect to a Router

Routers can be immediately clicked and connected in Cisco Packet Tracer. However, you may use a laptop and router to accomplish this via a console connection, much like in the real world, if you'd prefer. You must first configure the laptop's terminal software before connecting the laptop and router via a console cable. You will see several tabs when you click on laptop in Cisco Packet Tracer. One may find the terminal configuration under the desktop tab. The terminal settings will appear when you click it. To establish a connection with a router, adjust the configuration as follows:

- Bits Per Second: 9600
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Once these variables are completed, you can connect your router to the packet tracer.

Start Configuration on a Cisco Router

To begin the router configuration, there are unique configuration commands in every router. This is also standard with Cisco routers. The first command we should use while configuring a router on packet tracer is "enable." After receiving administrator privileges as a result, we can start configuring our packet tracer router by using the command "configure terminal." This lengthy version or even "conf t" can be used for this purpose. To begin the router configuration, there are unique configuration commands in every router. This is also standard with Cisco routers. The first command we should use while configuring a router on packet tracer is "enable." After receiving administrator privileges as a result, we can start configuring our packet tracer router by using the command "configure terminal." To accomplish this, you can either use this lengthy version or even "conf t." Terminal Configuration window is shown in Figure 6.

Configure Router Name

Every router has an initial name. However, in most cases, this name is altered to reflect more significant router names. These router names can display a router's position, priority, level, and other

details. We can provide the routers on packet tracer unique names by using one or more words. Using "hostname" commands, we may assign a router name to a Cisco router on a packet tracer. This command can be used in Cisco router setup mode. Here, we can enter XYZ as the name of our router.

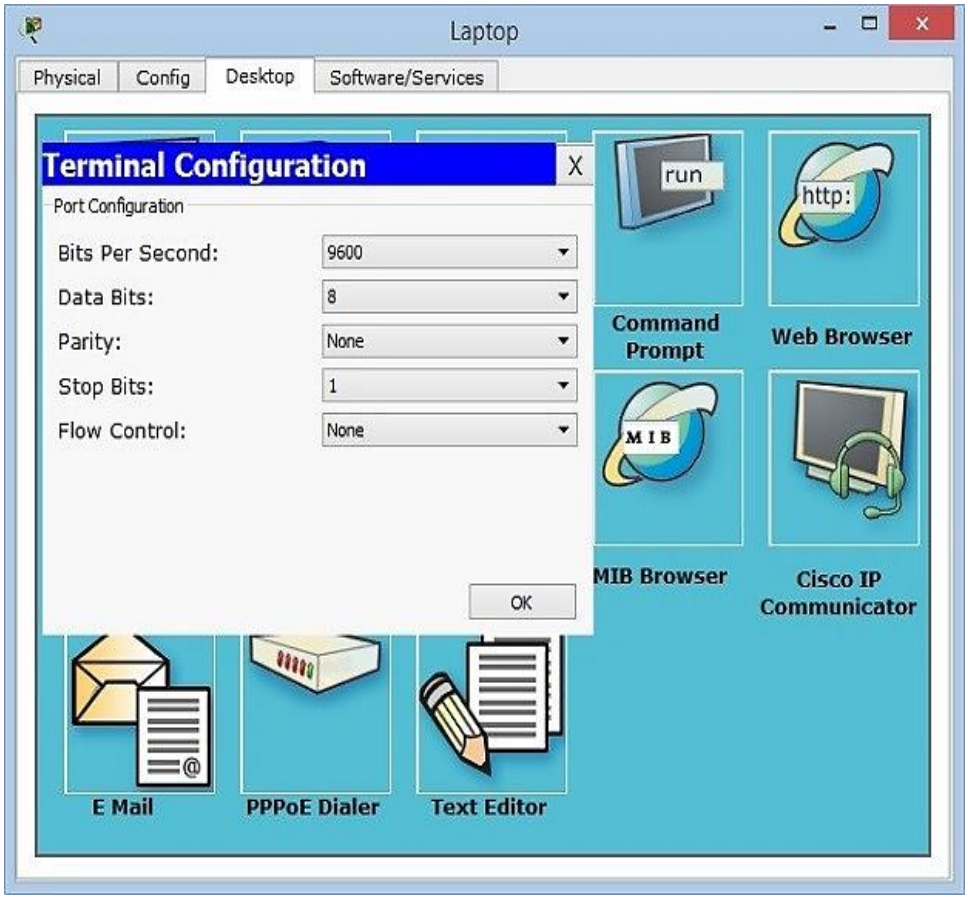

Figure 6. Terminal configuration.

Configure Enable Secret Password

We must first set a password on our router to safeguard it. Various passwords are utilized in Cisco routers. "Enable password" is one of the standard passwords used in routers. The password that preserves the password's clear text format is this one. However, there is an additional password known as "enable secret password." This password is more secure because it uses MD5. The value of the enable password is plainly visible in the configuration, however the enable secret password is not shown there. Let's set our enabled secret password to be abc123 now.

CONCLUSION

This research includes novel large-scale measurements employing fixed-core and mobile edge networks, as well as a new technique for observing DSCP alteration disorders. Our findings investigate a variety of DSCP values and modification pathologies during the packet's end-to-end journey. The most important finding is that many networks alter the DSCP value, even if we only saw a small number of instances where networks rejected packets containing a certain codepoint. Nevertheless, we advise applications to provide a DSCP and offer guidance. Although there is proof of operator configuration using DixServ, a large portion of the observed observations seem to originate from routers configured with outdated ToS semantics. This can occasionally lead to a priority inversion. It is highly advised to upgrade or reconfigure these routers to increase the possibility of utilising DiffServ along the whole network path. Additionally, we advise continuing to measure DSCP remarks to profile access networks as well as the core/server sections of the network.

REFERENCES

1. Nichols K, Blake S, Baker F, Black D. Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers. 1998 Dec.
2. R. Geib, D. Black, Diffserv-interconnection classes, and practice, 2017, (RFC 8100 (Informational)). (2017-03-09). [Online]. Available from https://datatracker.ietf.org/doc/rfc8100/
3. S. McQuistin, C.S. Perkins, Is explicit congestion notification usable with UDP? IMC '15: Proceedings of the 2015 Internet Measurement Conference October 2015. Pages 63–69. https://doi.org/10.1145/2815675.2815716
4. AT&T, Class of service data collection document for AT&T managed internet service (mis), 2010. https://carecentral.att.com/downloads/Class_of_Service.pdf
5. Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, Renata Teixeira. Avoiding traceroute anomalies with Paris traceroute. IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement October 2006; Pages 153–158. ACM Digital Library. https://doi.org/10.1145/1177080.1177100
6. R. Bless, K. Nichols, K. Wehrle, A lower effort per-domain behavior (PDB) for differentiated services, 2003, RFC 3662 (IETF). The Internet Society (2003). [Online]. Available from https://www.rfc-editor.org/rfc/rfc3662
7. Terzis, B. Braden, S. Vincent, L. Zhang, RSVP diagnostic messages, 2000, (RFC 2745). (Proposed Standard))
8. T. Flach, E. Katz-Bassett, R. Govindan, Quantifying violations of destination-based for-warding on the internet, in: Proc. of ACM IMC'12, Boston (USA), pp. 265–272.
9. I.R. Learmonth, A. Lutu, G. Fairhurst, D. Ros, Ö. Alay, Path transparency measurements from the mobile edge with PATHspider, in: Proc. of IEEE/IFIP TMA'17, Dublin, pp. 1–6
10. D. Murray, T. Koziniek, The state of enterprise network traffic in 2012, in: IEEE APCC 2012, Berlin, pp. 179–184
11. Detal G, Hesmans B, Bonaventure O, Vanaubel Y, Donnet B. Revealing middlebox interference with tracebox. In Proceedings of the 2013 conference on Internet measurement conference 2013 Oct 23 (pp. 1-8).

