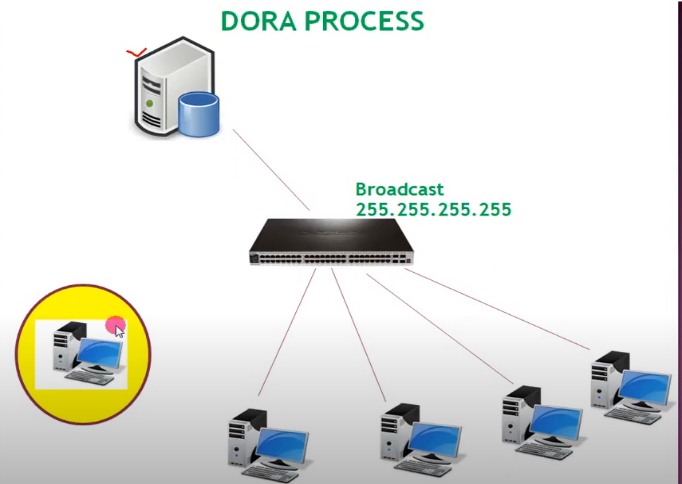
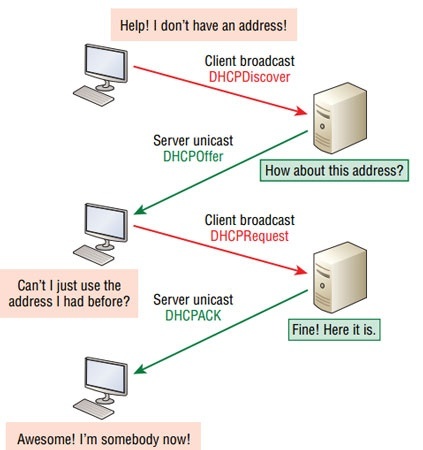
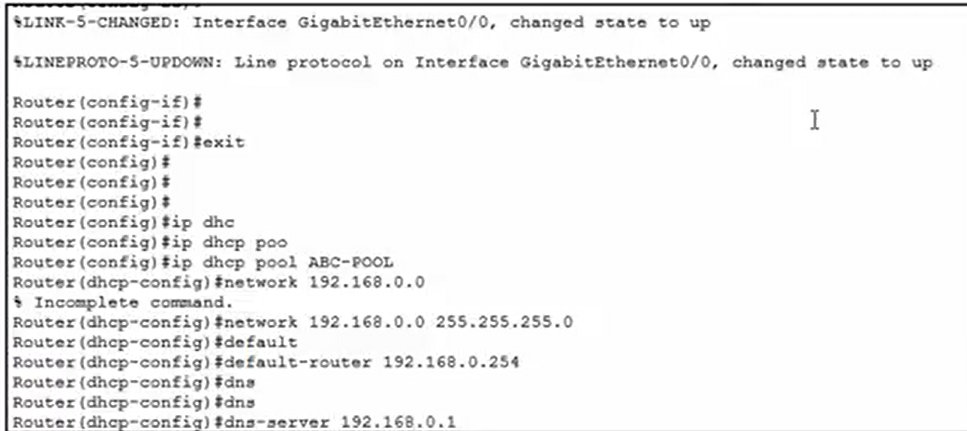
# **How DORA Works?**



**DHCP used UDP port no 67 and 68. DHCP provide services on 67 port no. and client listen on 68 port no. DHCP based on client-server model. DHCP used DORA process for working.**

1. **Discover:** The DHCP client sends a broadcast message on the network requesting an IP address lease.
2. **Offer:** DHCP servers on the network receive the broadcast and respond with an offer message, providing the client with an available IP address and other network configuration information.
3. **Request:** The DHCP client selects one of the offered IP addresses and sends a request message to the DHCP server.
4. **Acknowledge:** The DHCP server confirms the request and sends an acknowledgement message to the client, granting the client permission to use the offered IP address and network configuration information.

Once the DHCP client receives the acknowledgement message, it configures its network settings and begins using the IP address lease.

Top of Form

**Dynamic Host Configuration Protocol(DHCP)** uses the DORA. Dynamic Host Configuration Protocol is the protocol of the [application layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/). It is used to provide Subnet Mask, Router Address, DNS Address, and Vendor Class Identifier. In fact, DHCP provides an automatic IP address to Hosts which want to connect to a network.

DORA is the process that is used by [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/). DORA helps in providing an IP address to hosts or client machines. DORA is the process that follows some steps between the server and client. It gets the IP address from the centralized server. It consists of four-stage:

* **Discover**
* **Offer**
* **Request**
* **Acknowledge**

Now let’s see what happens when DHCP clients request a DHCP server an IP address. Let’s see what messages are exchanged between them in the process.

**Note**: *In the network layer, DHCP messages are always broadcast. In the data link layer also DHCP messages are broadcast.*

## **Step 1: DHCP Discover Message**

This is the first message in the DORA process which helps in finding the DHCP server of the network. DHCP client will find the server by sending DHCP discover message. The broadcast message is sent to the network. As the DHCP client doesn’t know the IP address of the server so the message is broadcast with a destination IP is 255.255.255.255. And the source IP will be 0.0.0.0 as the client does not have any IP address. Here the DHCP discover message in the data link layer and network layer is always broadcast.

Source IP address: 0.0.0.0

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP clients

Destination MAC address: FF:FF:FF:FF:FF:FF

## **Step 2: DHCP Offer Message**

DHCP server receives the discover message and it replays the DHCP client with the DHCP offer request. The server sends a DHCP offer message with filled information. It has information about the IP address and duration of time that a host can use. Here destination IP address will be 255.255.255.255 as the DHCP client still does not have its IP address. But this DHCP offer message is broadcast in the network layer and unicast in the data link layer.

Source IP address: IP Address of DHCP Server

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP Server

Destination MAC address: MAC address of DHCP clients

## **Step 3: DHCP Request Message**

DHCP clients send the request message to the server when it receives a DHCP offer message from the server. This message tells the server that it accepts the IP address given by the server. Here destination address will be 255.255.255.255 means it’s again broadcast. The reason for this is there might be many DHCP servers in the network so the client may receive multiple offer messages and it will accept the request that reaches him first and send a broadcast message to eliminate other DHCP servers. Here source IP address will be 0.0.0.0 as the DHCP server hasn’t yet assigned an IP address to the client. DHCP Request Message is also a broadcast message.

Source IP address: 0.0.0.0

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP clients

Destination MAC address: MAC address of DHCP server

## **Step 4: DHCP Acknowledge Message**

This is the last step or message in the DORA process. The DHCP server sends Acknowledge Message to the client when it receives the request message from the DHCP client. This message will contain the IP address and subnet mask that the server assigns to the client. Source IP address will be the IP address of the server. This will be again broadcast message as the destination IP address is 255.255.255.255. But it is unicast in the case of the data link layer.

Source IP address: IP Address of DHCP Server

Destination IP address: 255.255.255.255

Source MAC address: MAC address of DHCP server

Destination MAC address: MAC address of DHCP clients

So, this is the DORA process and when this process is over DHCP client will get its IP address. Here things to remember is

* **DHCP Discover Message**– Broadcast
* **DHCP Offer Message** – Broadcast in the network layer and unicast in the data link layer
* **DHCP Request Message** – Broadcast in the network layer and unicast in the data link layer
* **DHCP Acknowledge Message** – Broadcast in the network layer and unicast in the data link layer

**DHCP Server Configuration in Cisco**

DHCP is a network management protocol used in networks to dynamically assign IP addresses and other network configuration information like default gateway, mask, DNS server address, etc. It is an application layer protocol.

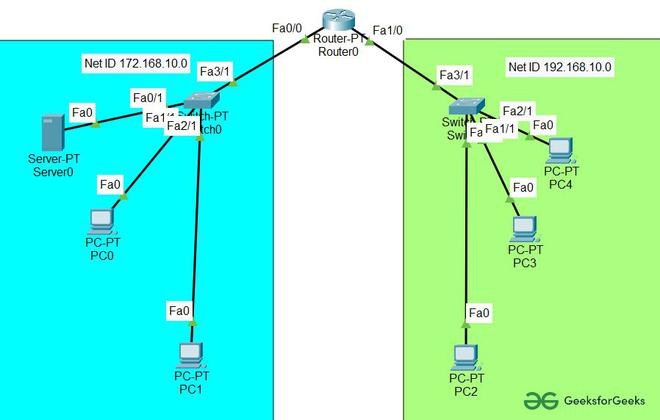
In this article, we will know about DHCP server configuration using Cisco Packet Tracer.

**Steps to Configure and Verify DHCP Server in Cisco Packet Tracer:**

**Step 1:**First, open the cisco packet tracer desktop and select the devices given below:

| **S.NO** | **Device** | **Model-Name** | **Unit** |
| --- | --- | --- | --- |
| **1.** | PC | PC | 5 |
| **2.** | Switch | PT-Switch | 2 |
| **3.** | Router | PT-Router | 1 |
| **4.** | Server | Server-PT | 1 |

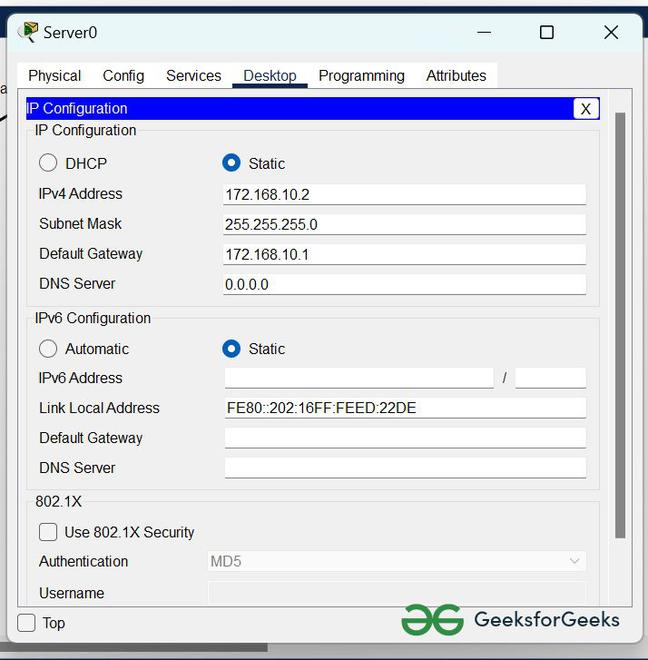
* Now create a network topology as shown below the image.
* Use an Automatic connecting cable to connect the devices with others.



**Step 2:** Configure the Server with IPv4 address and Subnet Mask according to the Data given above.

* 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.

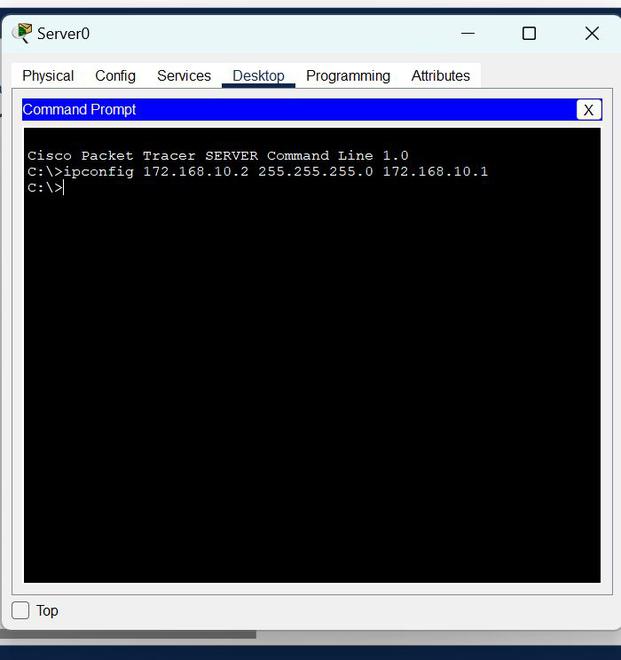
| **Parameters** | **Address value** |
| --- | --- |
| IPv4 Address | 172.168.10.2 |
| Subnet Mask | 255.255.255.0 |
| Default-Gateway | 172.168.10.1 |



**2.**Assigning IP address using the ipconfig command.

* 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)

example: ipconfig 172.168.10.2 255.255.255.0 172.168.10.1

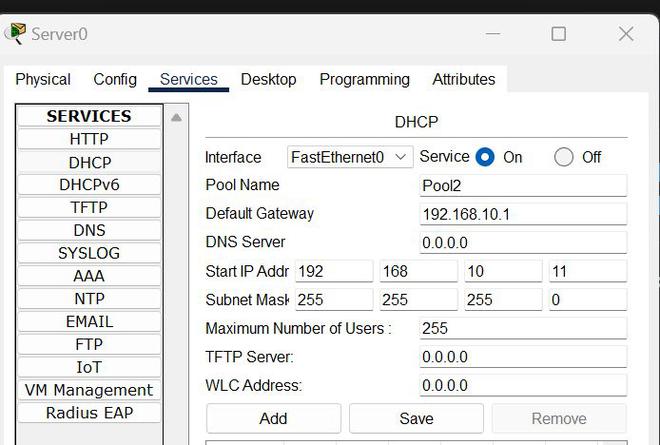


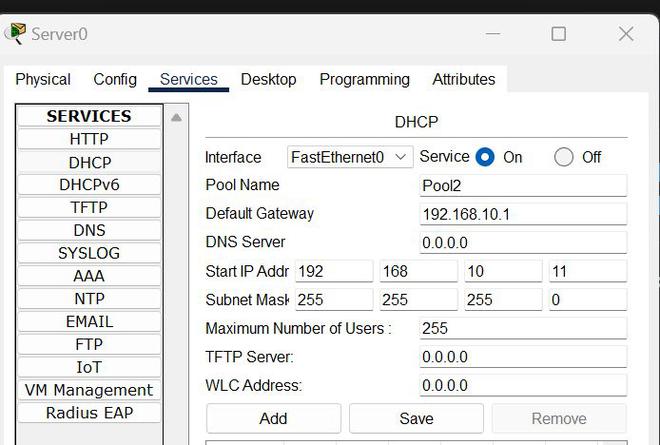
**Step 3:** Configuring the DHCP server.

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.
  + 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.





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

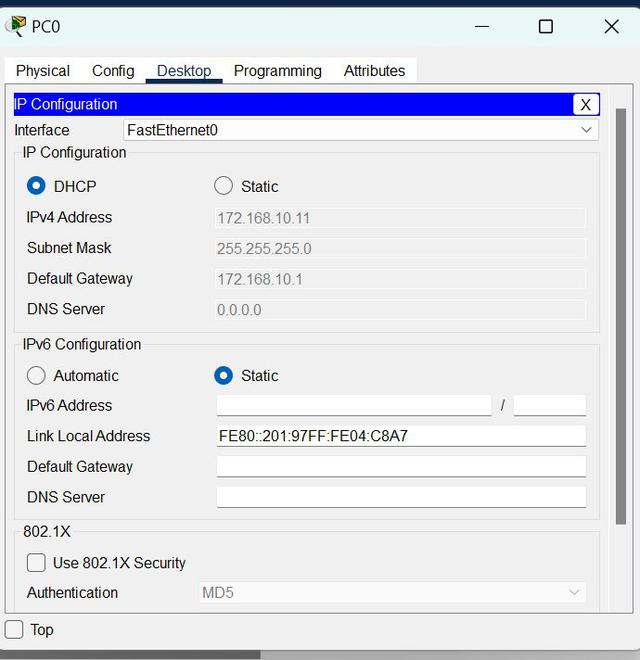
**IP Addressing Table for Router:**

| **S.NO** | **Device** | **Interface** | **IPv4 Address** | **Subnet Mask** |
| --- | --- | --- | --- | --- |
| **1.** | router0 | FastEthernet0/0 | 172.168.10.1 | 255.255.255.0 |
| FastEthernet0/1 | 192.168.10.1 | 255.255.255.0 |

* 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.
* Fill IPv4 address and subnet mask.

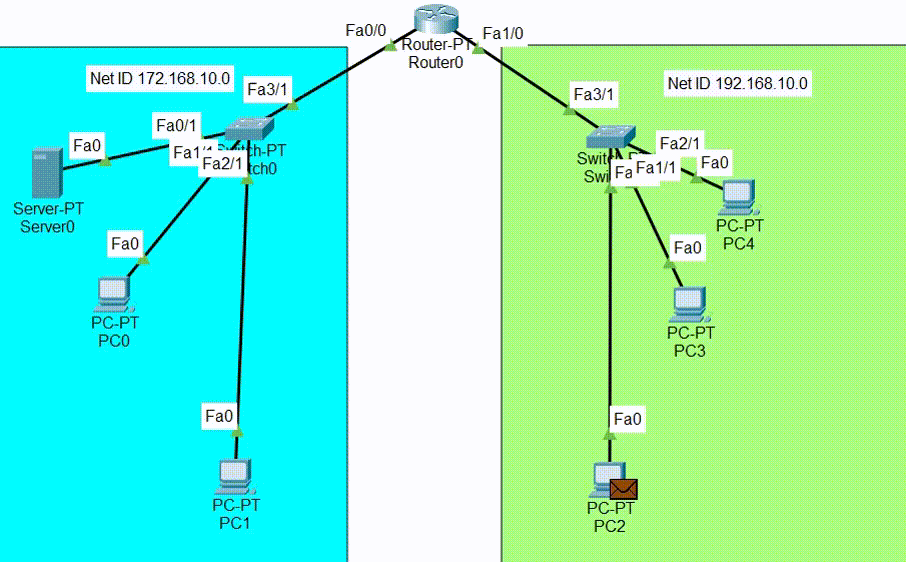
**Step 5:**Configuring the PCs and changing the IP configuration.

* To assign an IP address in PC0, click on PC0.
* Then, go to desktop and IP configuration and there you will find IPv4 configuration.
* Change its state from static to DHCP.
* It will automatically fetch the data and configure itself.



* Repeat the same procedure with other PCs to configure them thoroughly.

**Output:**



an example of how to configure DHCP in Cisco Packet Tracer:

1. First, open Cisco Packet Tracer and create a network topology.
2. Add a router and a switch to the topology.
3. Connect a PC to the switch using a straight-through cable.
4. Configure the IP address and subnet mask of the PC by going to the Desktop tab, clicking on IP Configuration, and entering the following values:

IP address: 192.168.1.10 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 DNS server: 8.8.8.8

1. Configure the router by opening its CLI (Command Line Interface) and entering the following commands:

enable

configure terminal

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

ip dhcp pool MYPOOL

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 8.8.8.8

exit

In the above configuration, we have created a DHCP pool named "MYPOOL" and specified the network range for DHCP clients, the default gateway (which is the router's IP address), and the DNS server (which is Google's public DNS server).

1. Configure the switch by opening its CLI and entering the following commands:

enable

configure terminal

interface FastEthernet0/1

switchport mode access

switchport access vlan 10

exit

vlan 10

name MYVLAN

exit

ip dhcp snooping vlan 10

exit

In the above configuration, we have created a VLAN named "MYVLAN" and enabled DHCP snooping for this VLAN to prevent rogue DHCP servers from assigning IP addresses to clients.

1. Verify that DHCP is working by going to the PC and releasing and renewing its IP address. To do this, right-click on the PC and select "Desktop". Then click on "IP Configuration", and click on the "DHCP" button. This will release the PC's current IP address and request a new one from the DHCP server. If everything is configured correctly, you should see that the PC gets an IP address in the range specified in the DHCP pool.

**Configuring a Syslog server** in Cisco Packet Tracer is very similar to setting it up in a real lab environment. You can follow these steps to configure a Syslog server in Cisco Packet Tracer:

1. Drag and drop a server device from the "End Devices" section onto your Packet Tracer workspace.
2. Double-click the server device to open its configuration window.
3. Under the "Services" tab, select "Syslog" from the dropdown menu.
4. Set the IP address of the Syslog server to a static IP address by clicking on the "Config" button next to the "IP Configuration" field.
5. Configure the Syslog server software to listen for syslog messages on UDP port 514. This can usually be done through the software's configuration file.
6. Determine the IP addresses of the devices that will send syslog messages to the Syslog server. These devices could be routers, switches, firewalls, or any other network device that supports syslog.
7. Configure each device to send syslog messages to the Syslog server's IP address on UDP port 514. This can usually be done through the device's configuration interface.
8. Verify that the Syslog server is receiving syslog messages from the devices. You can check the Syslog server's logs or use a network protocol analyzer such as Wireshark to view the incoming syslog messages.
9. Configure the Syslog server software to store the syslog messages in a format that is easy to search and analyze. This may involve configuring the software to use a specific log file format, such as syslog or CSV.
10. Set up a backup strategy for the Syslog server's logs to ensure that they are not lost in case of hardware failure or other issues.

Following these steps will enable you to configure a Syslog server in Cisco Packet Tracer and start collecting syslog messages from your network devices.

**Here is an example of configuring a Syslog server in Cisco Packet Tracer using CLI commands:**

1. Drag and drop a server device from the "End Devices" section onto your Packet Tracer workspace.
2. Double-click the server device to open its configuration window.
3. Under the "Services" tab, select "Syslog" from the dropdown menu.
4. Set the IP address of the Syslog server to a static IP address by clicking on the "Config" button next to the "IP Configuration" field. In this example, we'll use the IP address 192.168.1.100 for the Syslog server:

ip address 192.168.1.100 255.255.255.0

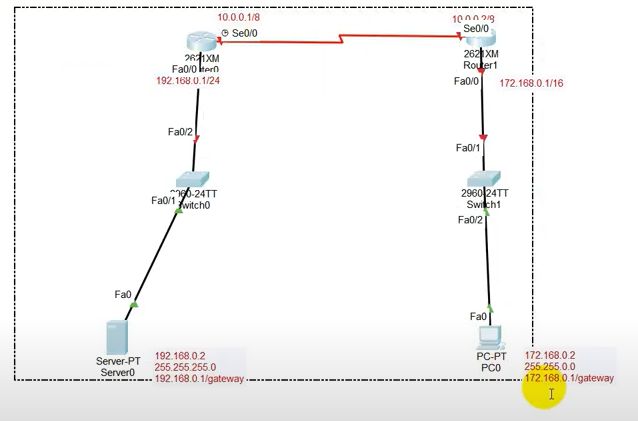
1. Configure the Syslog server software to listen for syslog messages on UDP port 514. This can usually be done through the software's configuration file. In Packet Tracer, this step is already done for you.
2. Determine the IP addresses of the devices that will send syslog messages to the Syslog server. These devices could be routers, switches, firewalls, or any other network device that supports syslog.
3. Configure each device to send syslog messages to the Syslog server's IP address on UDP port 514. For example, on a Cisco router, you would use the following command:

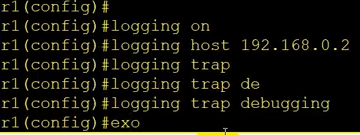
logging 192.168.1.100

This command tells the router to send syslog messages to the Syslog server at IP address 192.168.1.100.

1. Verify that the Syslog server is receiving syslog messages from the devices. You can check the Syslog server's logs or use a network protocol analyzer such as Wireshark to view the incoming syslog messages.
2. Configure the Syslog server software to store the syslog messages in a format that is easy to search and analyze. This may involve configuring the software to use a specific log file format, such as syslog or CSV. In Packet Tracer, this step is already done for you.
3. Set up a backup strategy for the Syslog server's logs to ensure that they are not lost in case of hardware failure or other issues. In Packet Tracer, you can simply save the Packet Tracer project file to back up the Syslog server's logs.

Overall, configuring a Syslog server in Cisco Packet Tracer is a straightforward process that involves setting a static IP address for the Syslog server, configuring the devices to send syslog messages to the server, and verifying that the server is receiving the messages.





R1# ping 192.168.0.2