# Telnet configuration in Cisco packet tracer

**In this Lab, we will learn about telnet configuration in Cisco packet tracer. Check out the steps for the working telnet connection.**

**Telnet –**Protocol developed in 1969, allow us to connect to the remote device using the command line interface, telnet protocol is part of the TCP/IP suite.

To use the telnet, the device should have a telnet client installed and the remote device should be configured to accept telnet connection so most of the devices like servers, routers, switches, firewalls, etc are configured to allow telnet connection.

We can use any telnet client to establish the connection; one of the famous free telnet clients is putty. Putty is used by many organizations as it is open source and it also works for the SSH connection.

In this packet tracer lab, we will set up a router for telnet access. And then use the command prompt on the computer to test our telnet connection.

To telnet the router from our PC we will have to assign an IP address to our PC. After that, we will assign the IP address to the router interface which is connected with that PC.

For establishing a successful telnet connection, our PC and router should be on the same network as the PC and router are connected directly.

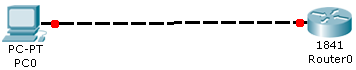
After assigning the IP addresses to both our devices, we have to enable the router for a telnet connection by configuring the VTY lines.

We will configure telnet lines 0-15 on the router, which will allow 16 simultaneous telnet connections to the router, this feature is helpful if more than one person wants to log in to the device at the same time, this type of practice is common if we have many administrators to look after the device.

Once we have configured both devices properly, we can try pinging the router from our PC to check the connectivity. If the router is responding to the ping command then we can establish a telnet connection from our PC’s command prompt.

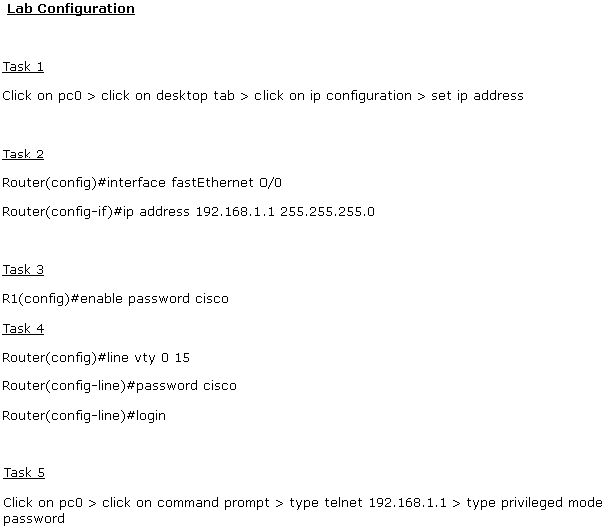
Once the telnet connection is initiated successfully, we will be prompted with the password to access the router via a telnet connection.

An important thing, we have to configure the privileged mode password. That’s because it is not possible to access the privileged mode through a telnet connection if the password for our privileged mode is not configured. if we will try to access privileged mode without the configuration of the password then we will see an error message saying ‘no password set’.



**Lab tasks**

1. Set pc0 IP address to 192.168.1.2/24
2. Set interface fast Ethernet 0/0 IP address to 192.168.1.1/24
3. Set privileged mode password to Cisco
4. Enable telnet lines on router
5. Test telnet connection via your PC



CDP packet tracer (Cisco Discovery Protocol)

**In this CDP lab, we will be using CDP protocol to find out neighbor information in Cisco packet tracer.**

CDP is a handy protocol. It is a fantastic tool for searching the details about directly connected devices. However, being Cisco propriety, it only works if the connected device is a Cisco device. It sends messages to the directly connected devices, these messages contain details about the host, devices, network, IOS, ports, etc. It is enabled by default on all Cisco devices.

CDP protocol generates messages every 60 seconds, these messages are received by the neighbor device and then the information is stored in the database.

CDP provides us with information that is quite useful if we do not have a complete diagram or have incomplete documentation about the network.

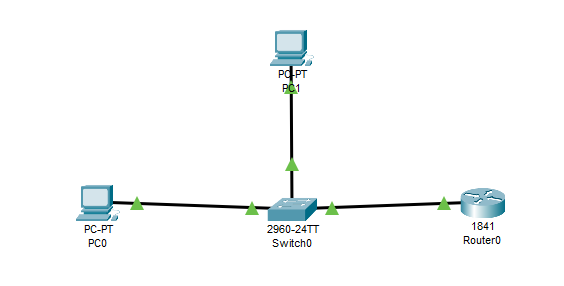
By using CDP we can find out the following information:

* The hostname of the remote devices
* Local and remote interfaces on which the devices are connected
* Type of device and the platform
* The IP address of the connected devices
* The version of IOS running

Although CDP provides good information about the directly connected devices however it can also pose a security threat to the network as hackers can identify and gather information very easily if any device in the network is compromised so it is the best practice to use this protocol very carefully and disable this protocol on highly secure devices. For e.g, we should not send CDP messages on the interface that is connecting outside of our network.

If we do not have the cisco device on the other end then the CDP protocol will not work however we can use the LLDP (Link Layer Discovery Protocol) as an alternative since it is a non-proprietary protocol so most of the vendors support this protocol. It is an industry-standard protocol with the same functionality.

In this lab, you will be required to find information about directly connected devices. To find complete information and details of all the devices, you have to use telnet because CDP can only provide information about directly connected devices. In the below lab, ‘device0’ does not have a direct link to all Cisco devices. And finally, we have to disable the CDP on the fast Ethernet 0/5 interface of router 5 – which is connected with the ISP router – because we do not want to pass our internal network information to the internet service provider (ISP).



Lab Tasks

1. Use CDP commands to find out Cisco devices 1 to 5  
2. Disable CDP on interface FastEthernet 0/1 of device 5

Lab Configuration

Task 1

Router#show cdp neighbors

Router#show cdp neighbors detail

Task 2

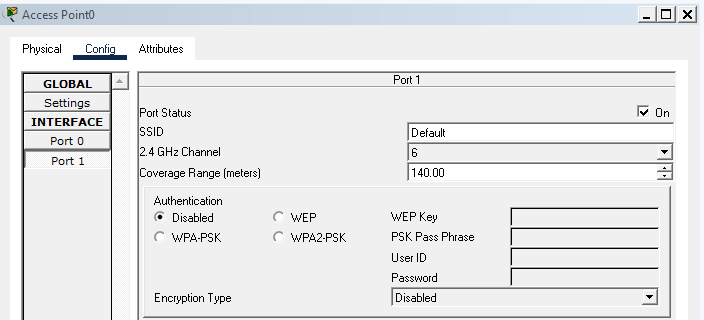
Router(config)#interface fastethernet 0/1

Router(config-if)#no cdp enable

# Configure access point in Cisco packet tracer

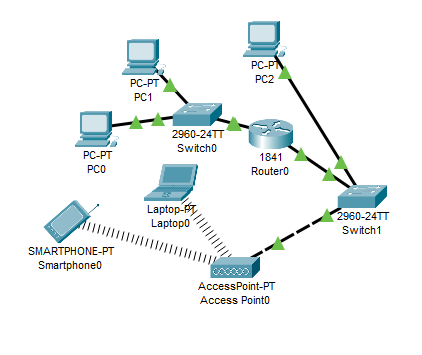
In this lab, we will configure a wireless access point in the Cisco packet tracer, and devices like phones, tabs, and laptops will be connected to the network.

A wireless access point allows devices to connect to the network wirelessly so to connect different devices to the access point, we have to configure the access point for basic settings.

We can configure port 1 for the wireless-related settings.

By default, SSID is configured as default and authentication is disabled and the same is configured on available end devices so we just have to add the devices to the packet tracer and they will connect to the access point immediately because the devices are preconfigured with the settings required to connect with the access point. However, If we have changed the SSID and enabled the authentication then we have to configure the device with the available SSID and also for authentication, the password must be entered.

To connect the Laptop or PC, we have to remove the Ethernet module and add the wireless module so these devices can support wireless connectivity while the other two devices in the image below have the wireless module preinstalled.



**Router Vs access point**

Usually, routers provide more functionality as compared to access points for e.g. routers can be configured with an access list and many more services like the quality of service, DNS, MAC address filtering, etc.

Routers available in the market these days have the ability to behave like an access point as well but normally in a large organization, access points are preferred due to their specific role and ease of configuration.

In big organizations, multiple access points are used to cover a large area so that access can be provided to users at every location.

The wireless router has the ability to assign dynamic IP addresses however in most cases, access point cannot assign IP addresses so to establish connectivity between different devices; we have to assign an IP address from the same network range.

If we want to assign the IP addresses dynamically then we can either add a wireless router to the network or configure a DHCP server.

We can also define the wireless range on the access point. By default, the access point is configured with a range of 140 meters so to reduce or increase the range, we can modify this setting.