



Computer Networks-Lab 02



Instructor: Engr. Khuram Shahzad

CL30001 – Computer Networks-Lab

Summer 2022

JULY 18, 2022

NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES, FAST- PESHAWAR CAMPUS
Department of Computer Science & Software Engineering

Table of Contents

Utilities used to allow connect PC remotely:	3
Windows 10:	3
Allow Access to Use Remote Desktop Connection (RDP)	3
Option 1	3
Option 2:	7
Enable it and add your required user:	9
How to Use the Remote Desktop Connection Client	9
Step 1: Launch the Remote Desktop Connection Unit	9
Step 2: Enter the Remote Hosts IP Address or Name	11
How to Find the IP Address and Host Name	11
Step 3: Entering the RDP Credentials and Finalizing the Connection	12
Access remotely using Open SSH Server:.....	14
Server-side OS (window 10).....	14
Now come toward client OS (window /Linux etc.)	20
Straight-Through and Cross-Over Cable, Viewing Network Equipment like Hub, Ethernet Switch, Router and different Cables.....	22
OBJECTIVES OF THE LAB.....	22
WIRELESS.....	25
WIRED	26
STRAIGHT-THROUGH CABLE	28
CROSS-OVER CABLE	30
TESTING CABLES.....	31
CABLE TESTER.....	31
NETWORKING DEVICES	32
HUB	32
SWITCH.....	33
ROUTER	35
What should I buy for my network, Hub, Switch or Router?.....	36
OBJECTIVES	38
PRE-LAB READING ASSIGNMENT	38
EXPERIMENTS WITH DETAILS.....	38
How to Change the Cisco Router name	40

How to set the IP address to Cisco interface:..... 50

How to check the IP address of all interfaces:..... 50

STUDENT TASK-01..... 50

Utilities used to allow connect PC remotely:

1. Any Desk <https://anydesk.com/en/downloads/windows>
2. TeamViewer <https://www.teamviewer.com/en/download/windows/>
3. Remote Desktop Connection (RDP)
4. VPN and Open SSH
5. Cloud Services (AWS, Google cloud, Azure)

Windows 10:

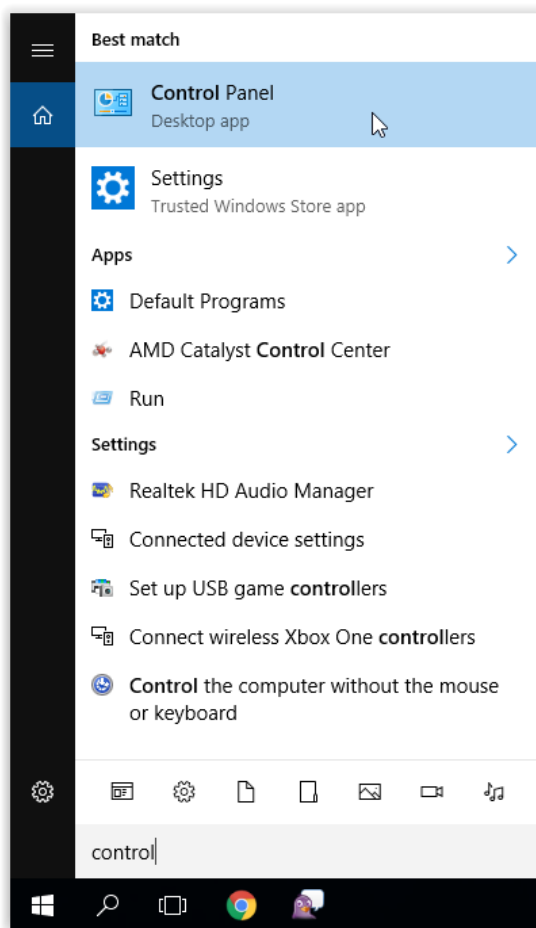
Allow Access to Use Remote Desktop Connection (RDP)

Allow Access to Use Remote Desktop Connection

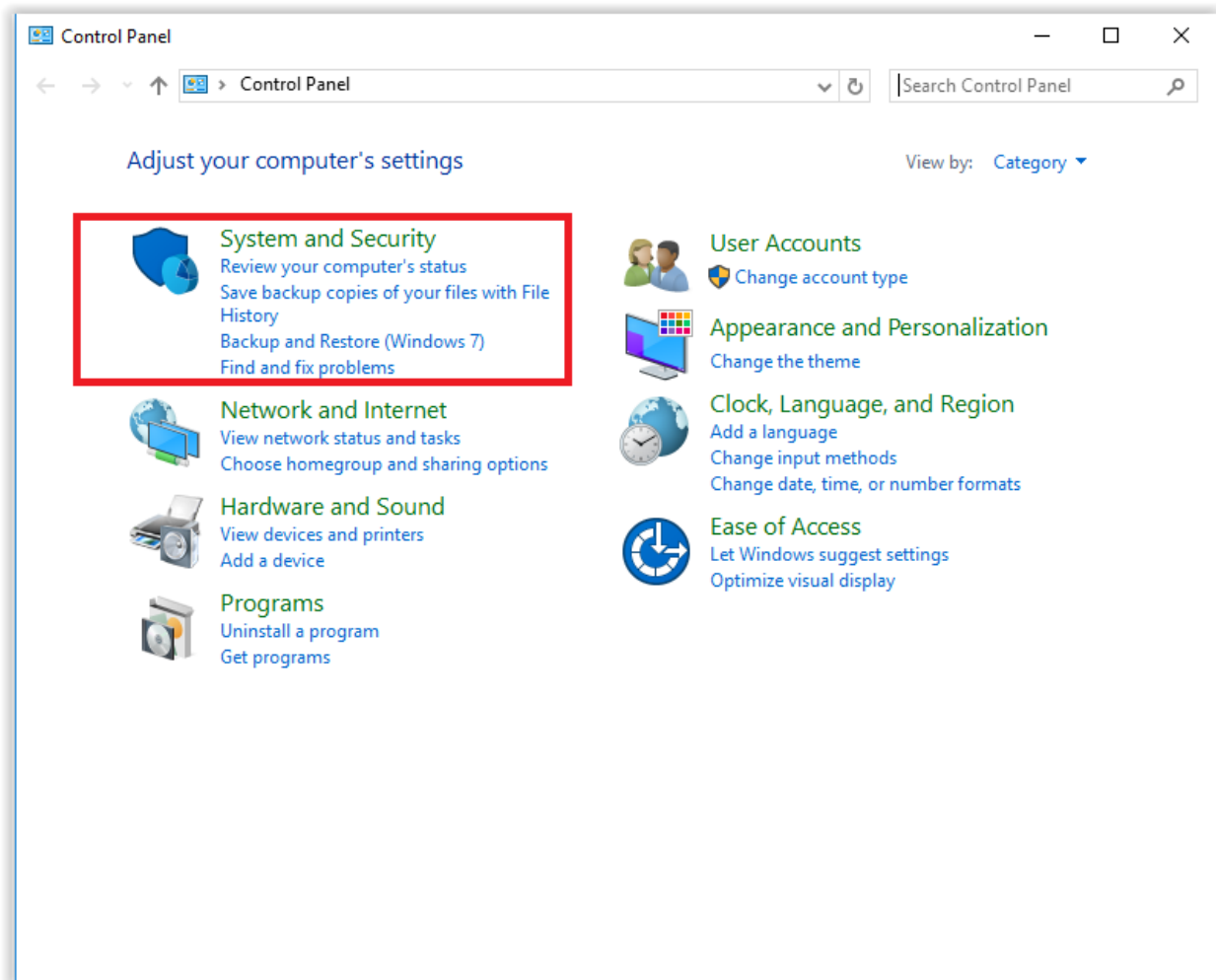
Before Remote Desktop can be used, permission has to be granted to the specific accounts that you would like to Allow to connect to your computer remotely. This is typically done on your *Office Computer*.

Option 1

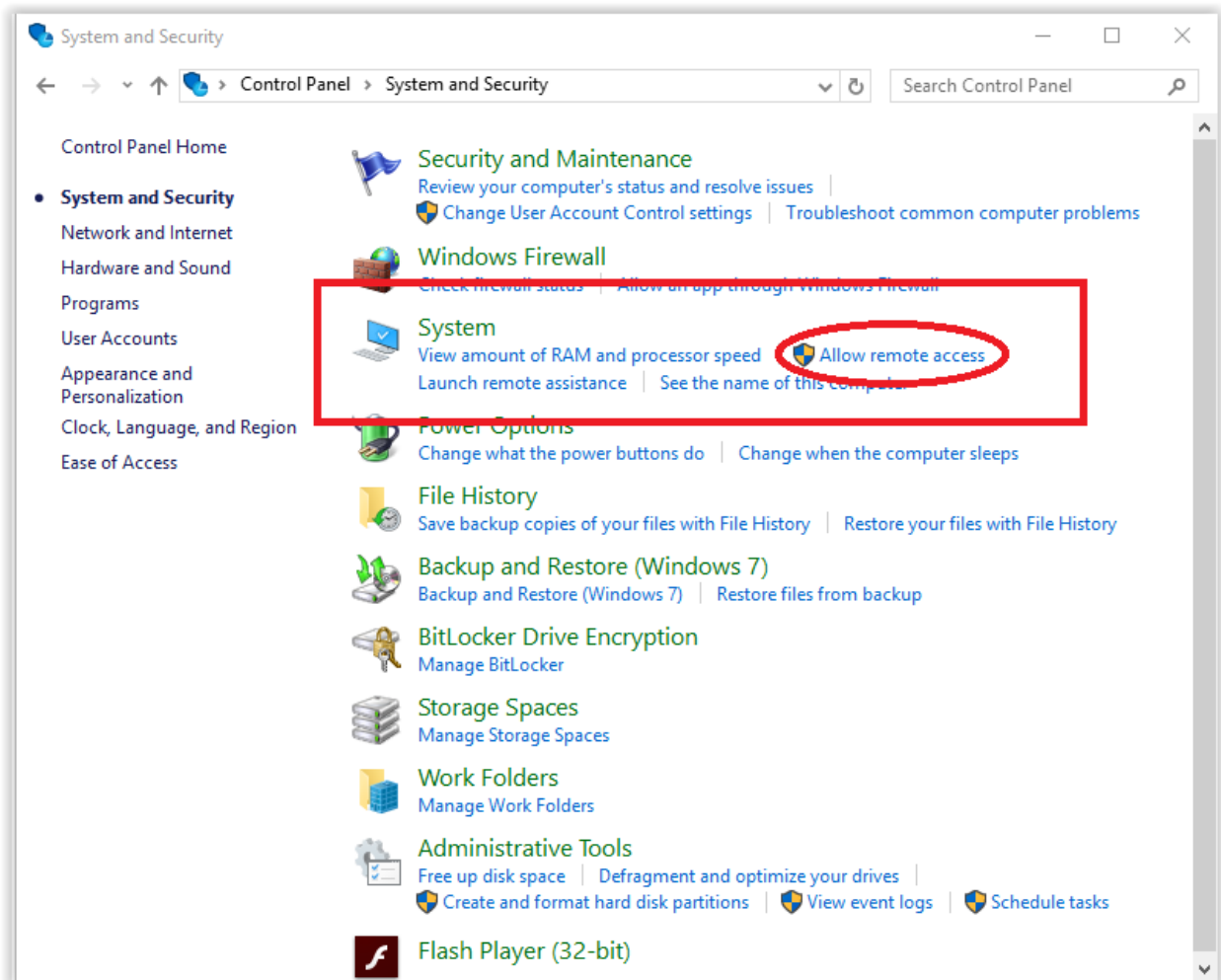
1. Click the **Start menu** from your desktop, and then click **Control Panel**.



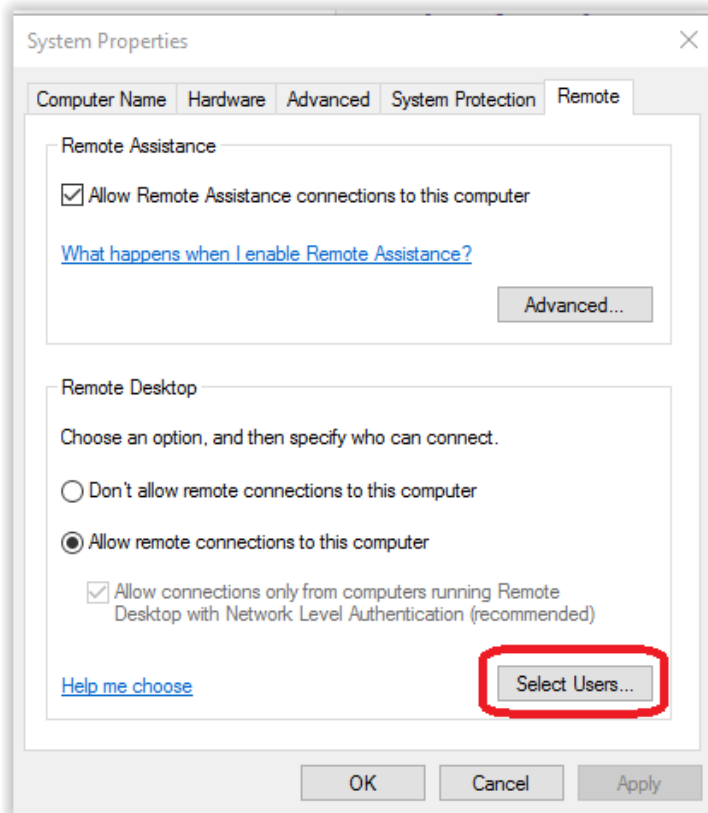
2. Click **System and Security** once the Control Panel opens.



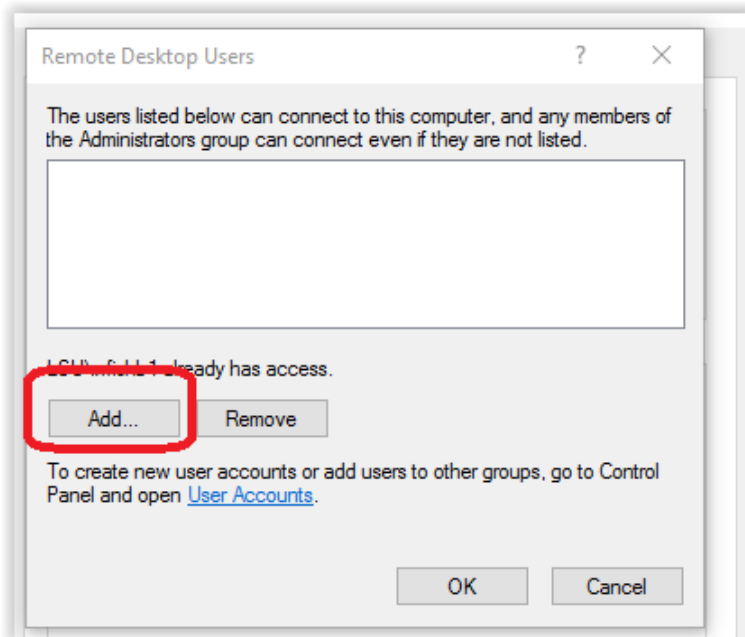
3. Click **Allow remote access**, located under the *System* tab.



4. Click **Select Users**, located in the *Remote Desktop* section of the *Remote* tab.

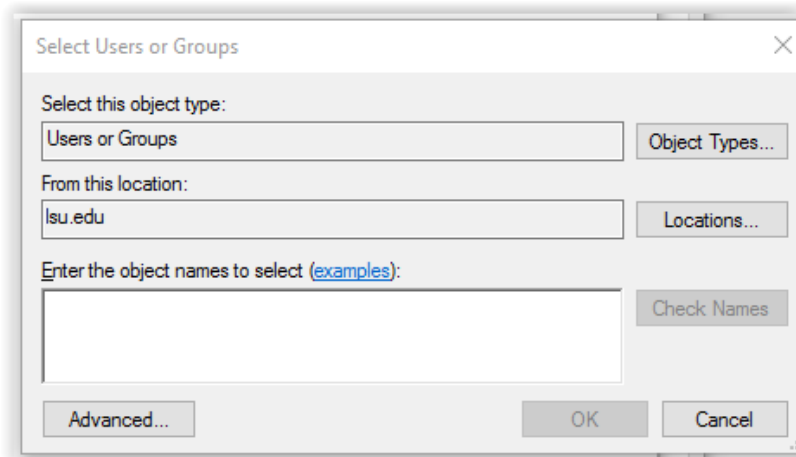


5. Click **Add** from the *System Properties* box.



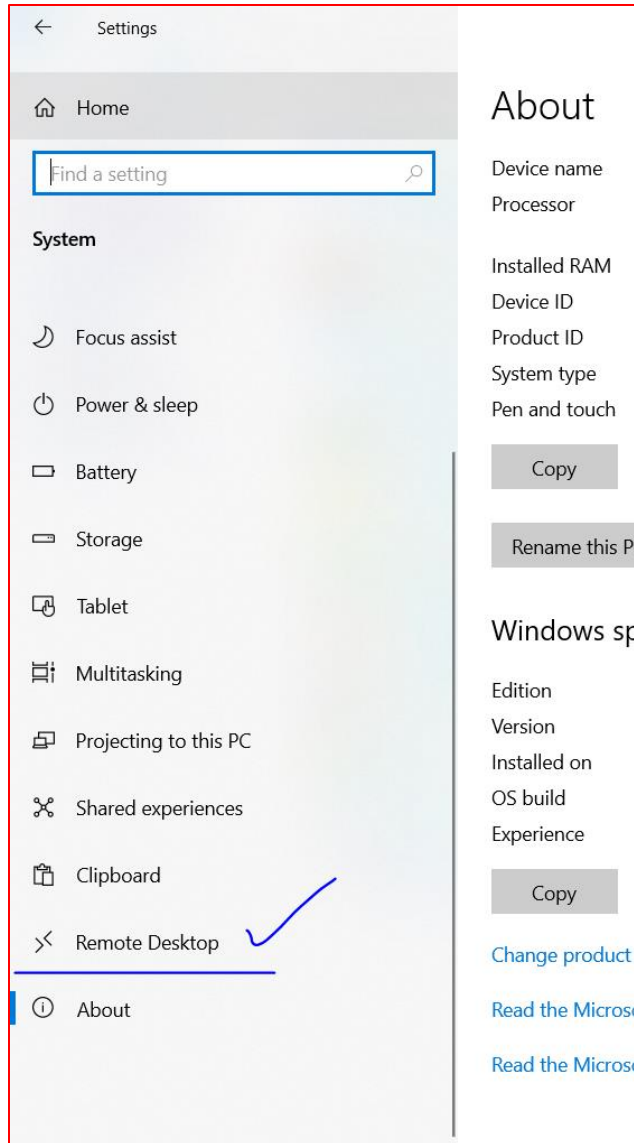
6. Type your **myLSU ID** and information for anyone else you would like to add. (This will allow *Remote Desktop* access to the computer which it is set.)

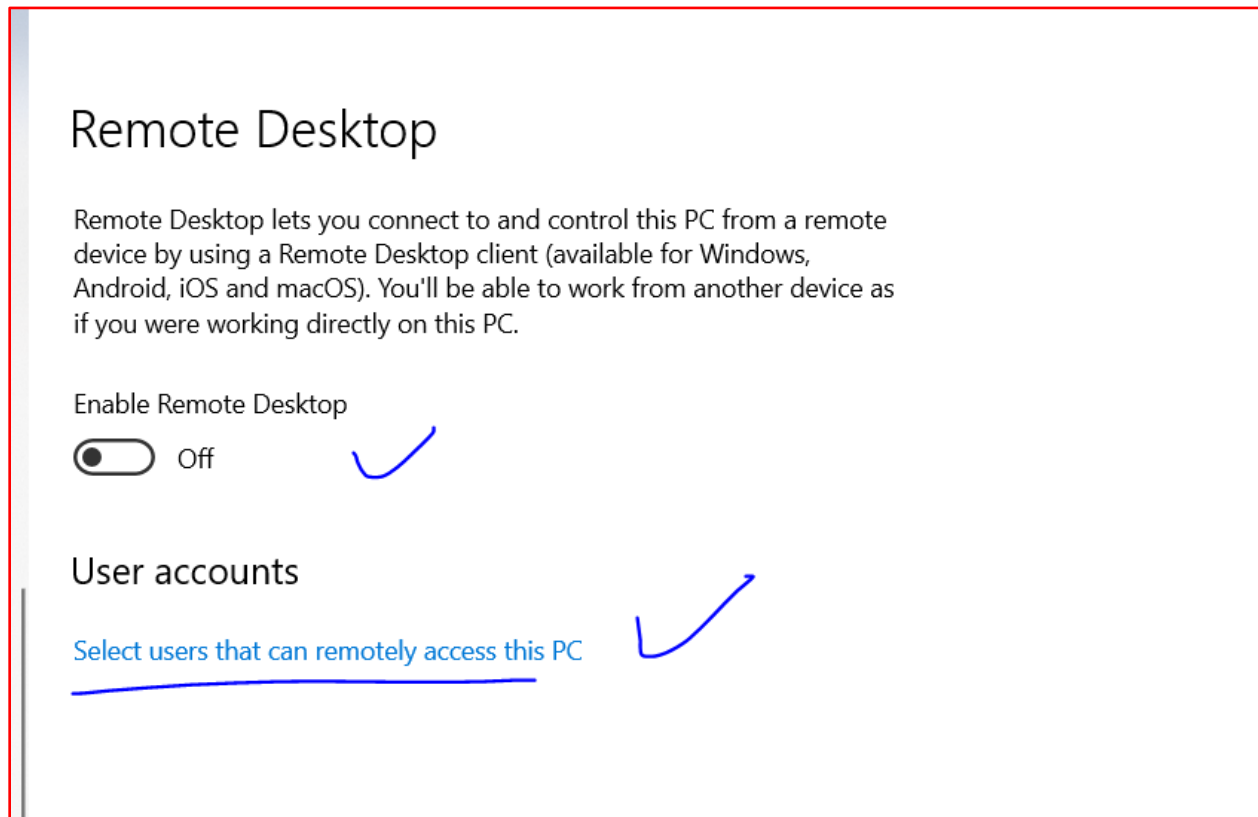
7. Click **OK** when finished.



Option 2:

Go to setting and allow remote desktop connection:



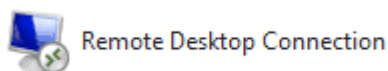
Enable it and add your required user:**How to Use the Remote Desktop Connection Client**

Using the Remote Desktop client is straightforward and you do not need to specifically configure Remote Desktop on the local computer. The steps below will work for all versions of Windows starting from Windows 7.

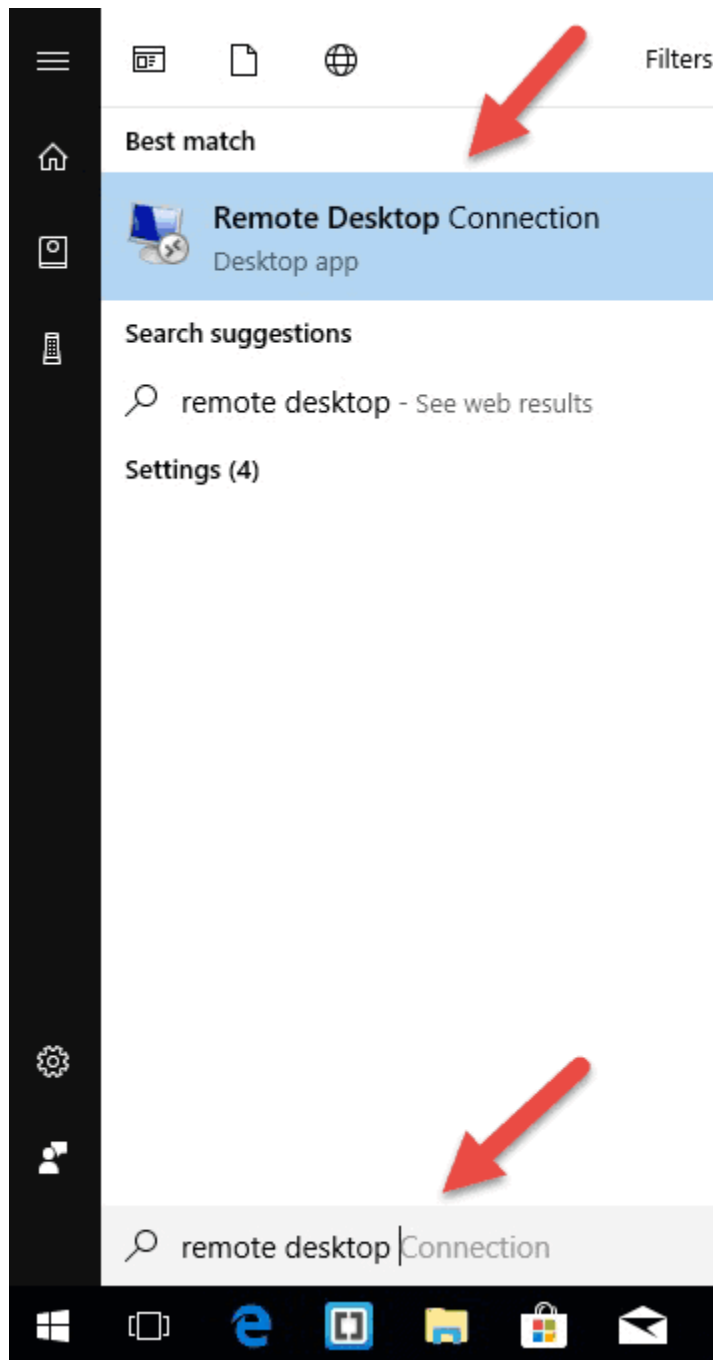
Step 1: Launch the Remote Desktop Connection Unit

On your local Windows computer, locate the Remote Desktop Connection application. You can find it in a couple of different ways:

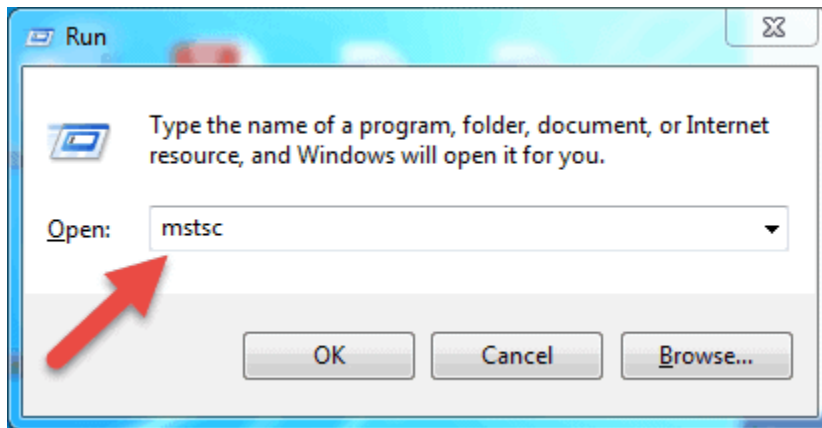
1. For Windows 7, click on Start -> All Programs, go to the 'Accessories' folder and click on Remote Desktop Connection. For Windows 10, Click on Start and locate the 'Windows Accessories' folder where you can also find the Remote Desktop Connection app.



2. Click on Start and type in Remote Desktop Connection in the search bar. You will receive search results as soon as you start typing. Click on the application when it shows up on the list.



3. Press Windows + R keys on your keyboard to get the “Run” box. Type in mstsc and hit Enter in the ‘Open:’ field to run the Remote Desktop client.



Step 2: Enter the Remote Hosts IP Address or Name

Once you launch the Remote Desktop Connection application, you will get a window where you can enter the **name** or the **IP address of a remote machine** you want to access.

In the **Computer** field, type in the corresponding name or IP address and click **Connect**.

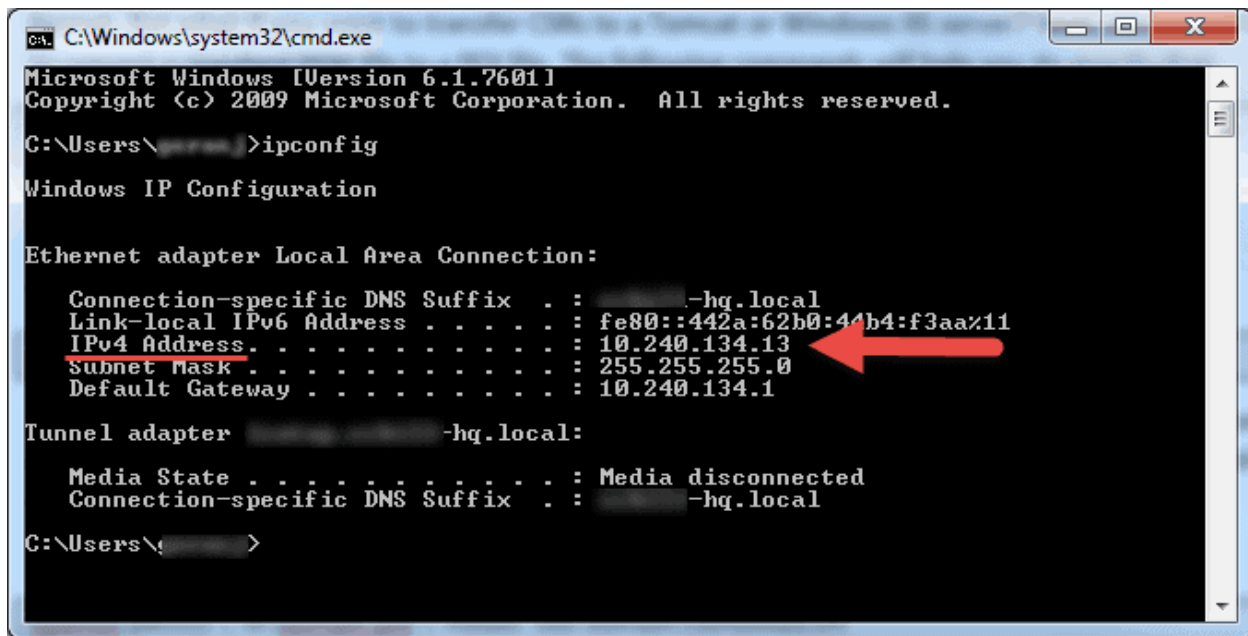


How to Find the IP Address and Host Name

There are many ways to locate the name, public or private IP address of a computer where you want to configure Remote Desktop service. Here are the quickest and easiest methods:

To determine a computer's private IP address:

1. Search for **CMD** from the start menu or press **Windows + R** on your keyboard, type in CMD and hit Enter to run the command prompt.
2. Type **ipconfig** in the command prompt and hit Enter.
3. You will see your computer's private IP address under the **IPv4 Address** line.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : -hq.local
    Link-local IPv6 Address . . . . . : fe80::442a:62b0:44b4:f3aa%11
    IPv4 Address. . . . . : 10.240.134.13
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.240.134.1

Tunnel adapter -hq.local:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : -hq.local

C:\Users\>
```

To determine which public IP address a computer is using:

1. From your web browser, go to **com** or use its search bar.
2. **Type in “what is my IP”** or simply **“my IP”** and hit Enter.
3. At the top of the page, Google will show you the public IP address your computer is using. If this is not working for your region, you can visit the first webpage in the search results and it will show you the IP address. Some websites such as www.whatismyip.com will even show you your private (local) IP address.

To find a computer’s name:

1. Right Click on **Computer**, or **This PC**, depending on the Windows OS version you are using.
2. Click on
3. You will find your full computer name under the **“Computer name, domain, and workgroup settings”** section.

Step 3: Entering the RDP Credentials and Finalizing the Connection

After you hit connect, the loading bar will appear. When it finishes initiating and configuring the remote session you will get a pop-up window that will look similar to this:



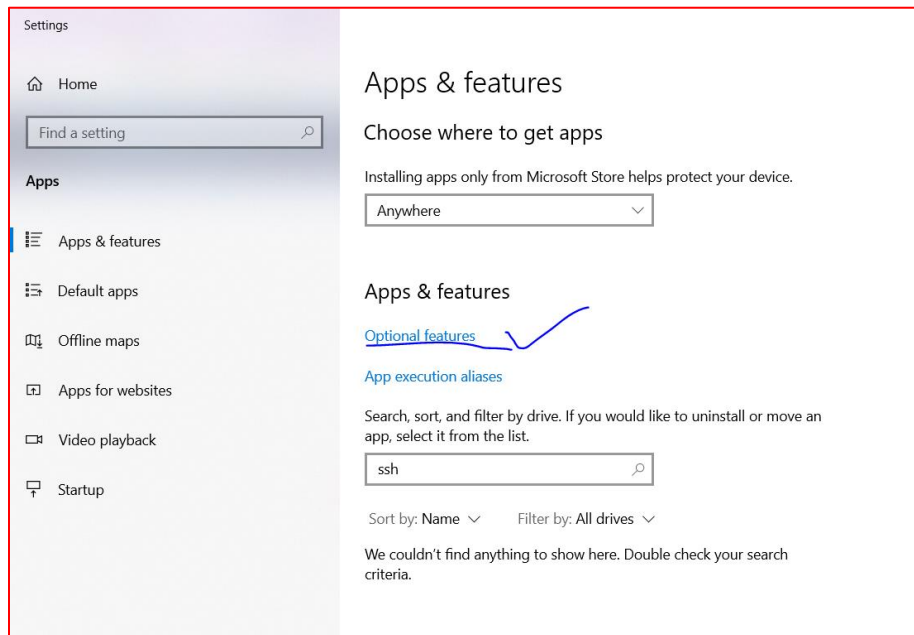
1. Enter the **password** for the selected username. You can use another account, if needed, and provide a different username and password.
2. Click **OK** when ready and you will get the security certificate warning.
3. Click **Yes** to continue.

Access remotely using Open SSH Server:

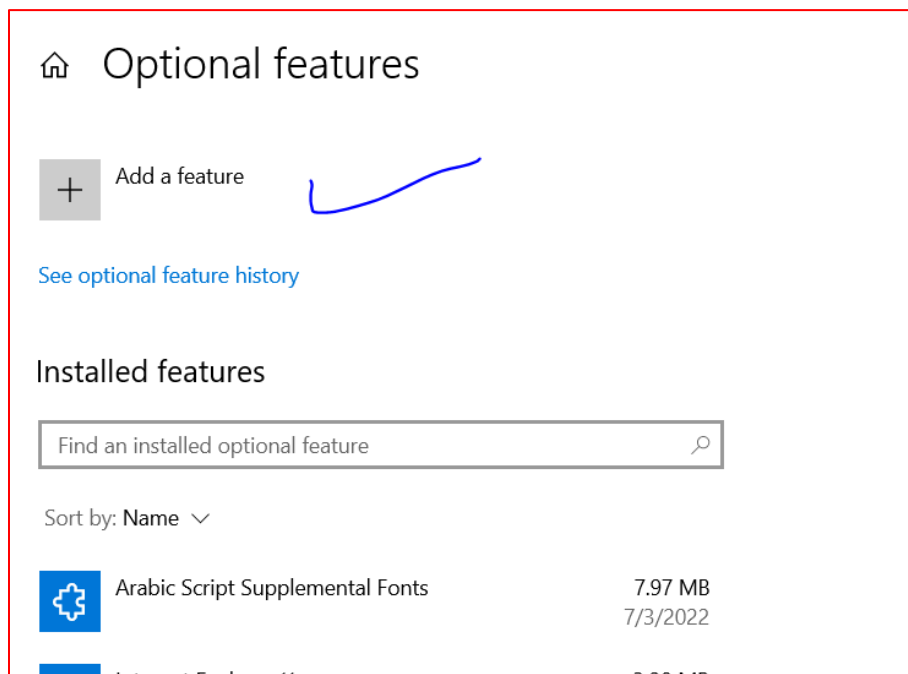
Server-side OS (window 10)

1. Go to the Apps and feature in Window setting (Server Window)

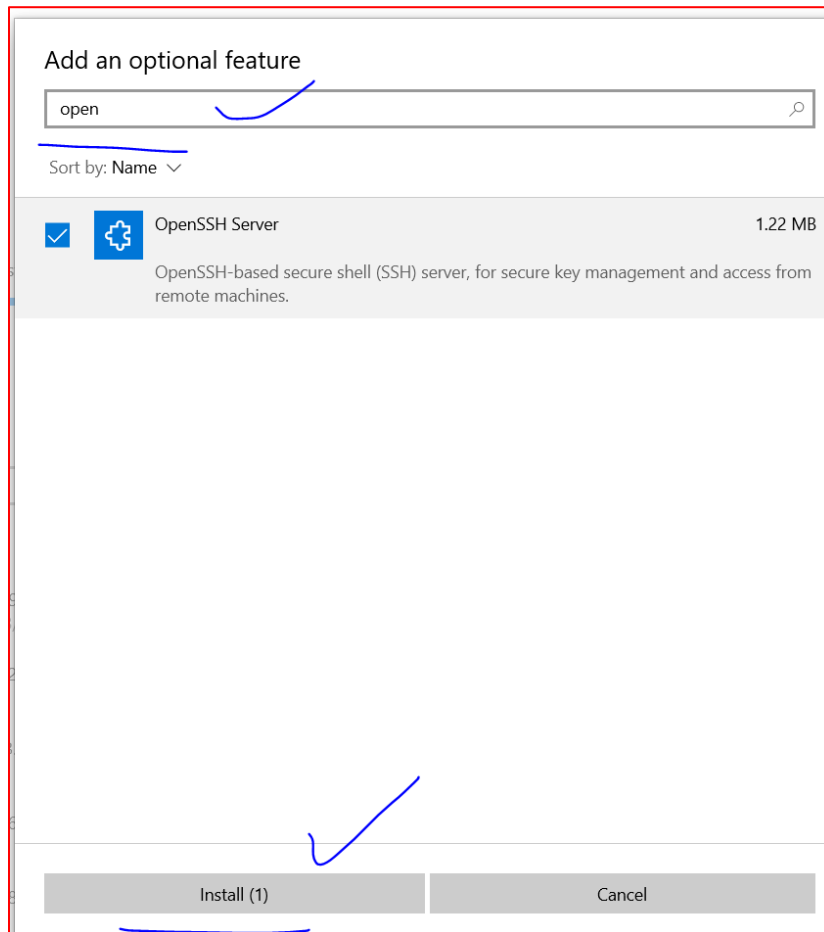
Click on Optional Features:

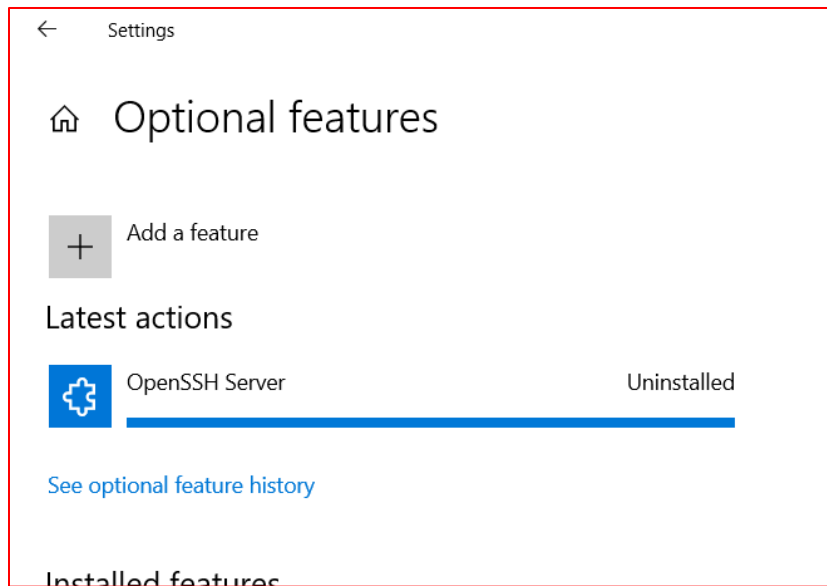


2. Click on Add a feature

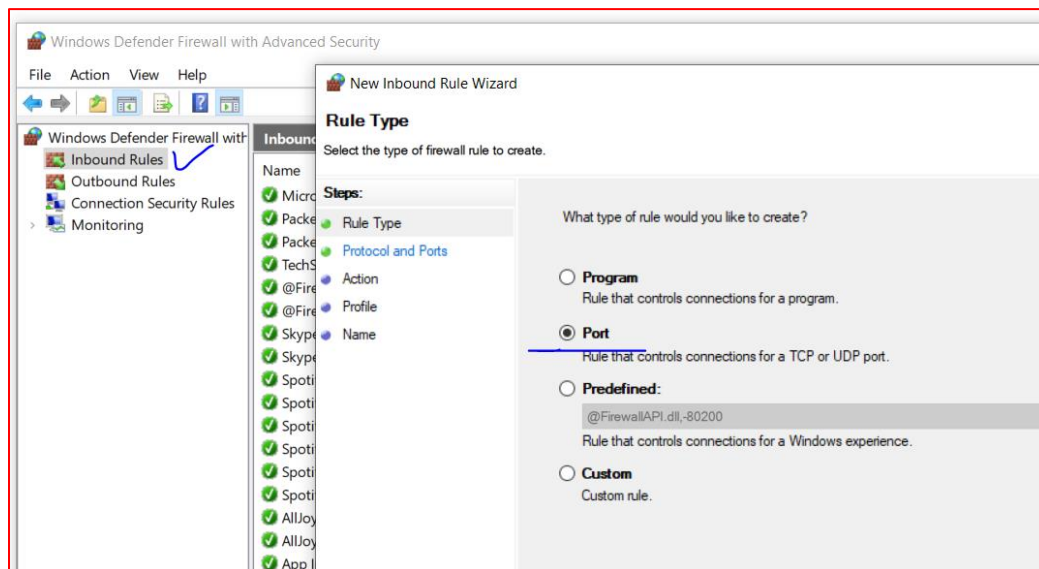


3. Search for Open SSH Server





4. Add inbound rule for port 22 in firewall on Server Window
Follow the step , which are given below



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP
☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports
☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

< Back Next > Cancel

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

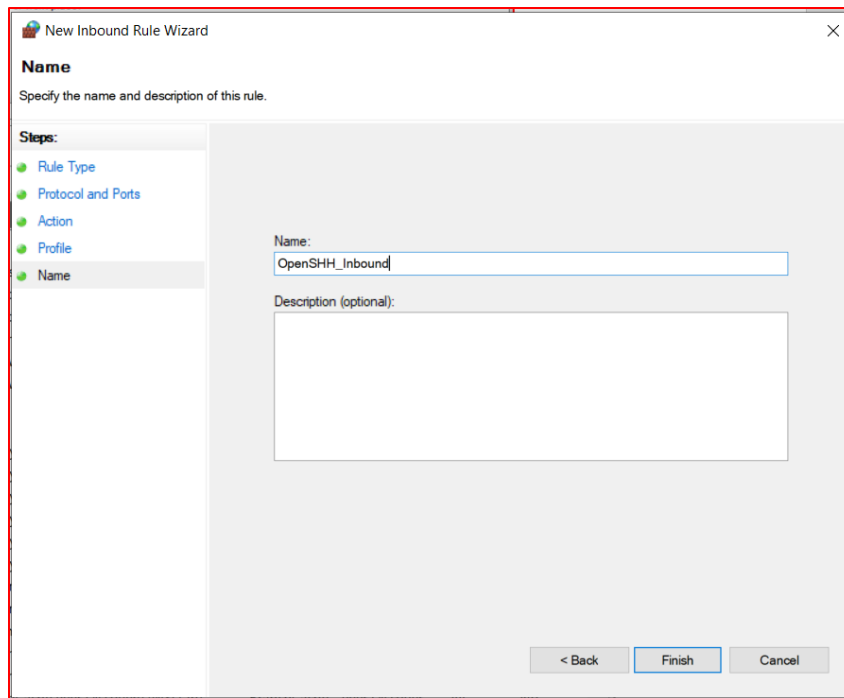
When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

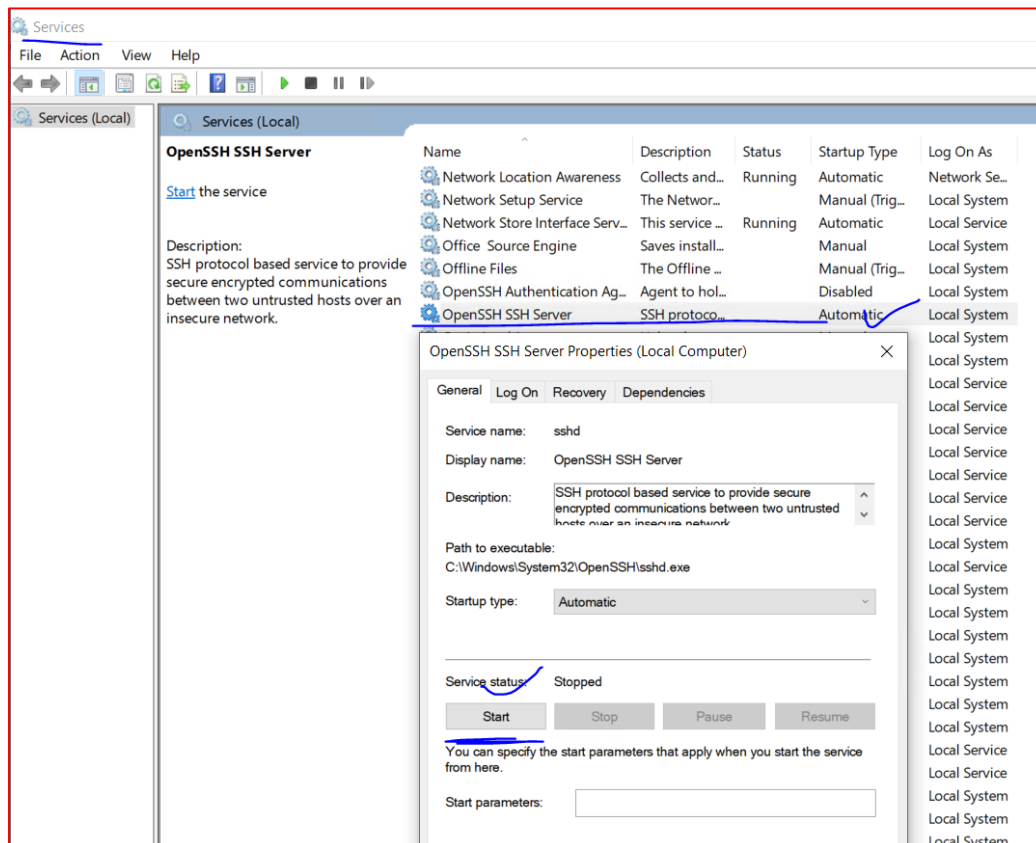
☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel



5. Now start the Open SSH from services:

Go to the services and find the Open SSH Server, right click on it and then start it.



6. Get the Ip address, username and password of Server-Side window.

Now come toward client OS (window /Linux etc.)

In my case:

Username is: Admission-04

Ip address is : 192.168.1.136

Open the cmd and type:

```
C:\Users\Khuram Shahzad>ssh Admission-04@192.168.1.136
Admission-04@192.168.1.136's password:
```

Enter the password

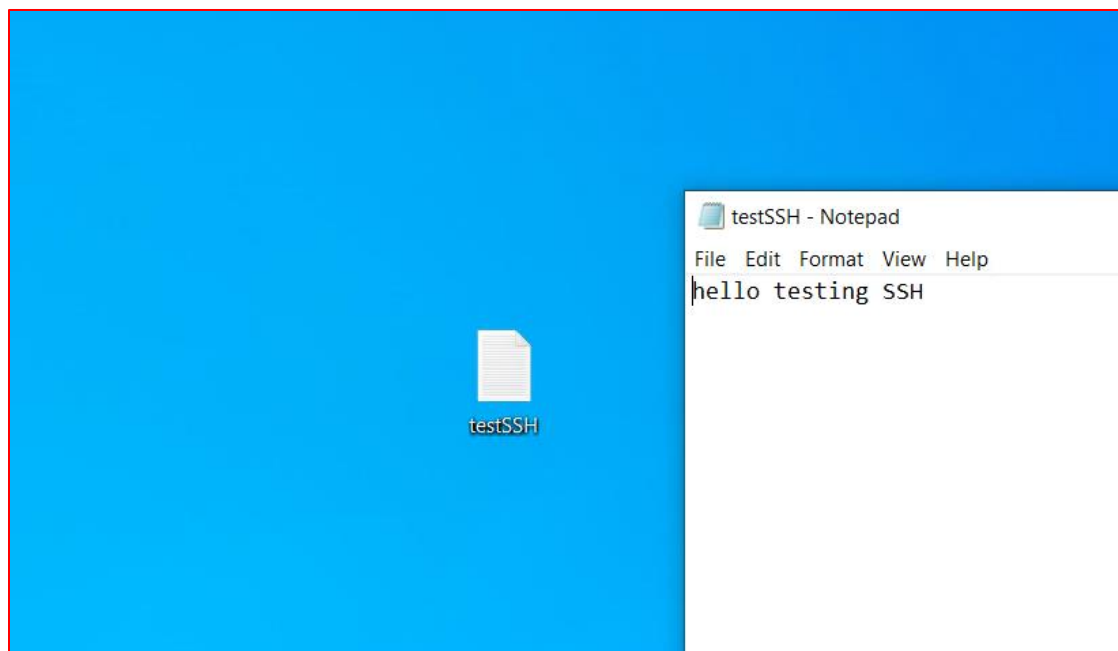
You will get access to the PC through console:

```
Administrator: C:\Windows\system32\conhost.exe
Microsoft Windows [Version 10.0.19044.1806]
(c) Microsoft Corporation. All rights reserved.

admission-04@DESKTOP-4I1B6K0 C:\Users\Admission-04>
```

Now you can access any send, receive ,add and delete any file or folder etc.

```
admission-04@DESKTOP-4I1B6K0 C:\Users\Admission-04>cd Desktop
admission-04@DESKTOP-4I1B6K0 C:\Users\Admission-04\Desktop>echo hello testing SSH > testSSH.txt
admission-04@DESKTOP-4I1B6K0 C:\Users\Admission-04\Desktop>
```



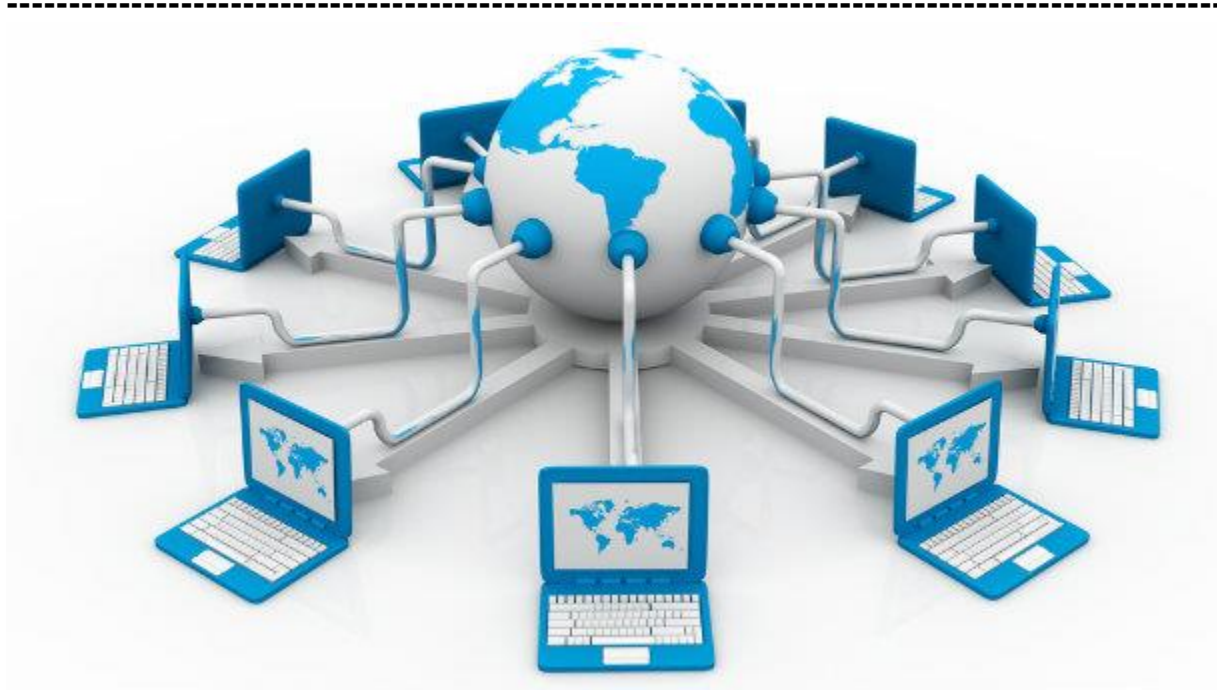
Straight-Through and Cross-Over Cable, Viewing Network Equipment like Hub, Ethernet Switch, Router and different Cables

OBJECTIVES OF THE LAB

In this lab, we will cover the following:

- Introduction to Computer Networks
- What Is CISCO Packet Tracer?
- Introduction to Transmission Media
 - Wired (gided)
 - Twisted Pair Cable (UTP, STP, Staright Cable , Crossover Cable)
 - Coaxil Cable
 - Fiber Optic
 - Wireless(Ungided)
 - Radio wave
 - Micro wave
 - Infrared
- Build a Category 6 (CAT 6) Straight-Through Ethernet network cable.
- Build a Category 6 (CAT 6) Cross-Over Ethernet network cable.
- Test both cables for good connection using Cable Tester.
- Connecting Computers via Switch using Straight Through Cable and Connecting two computers directly via Cross Over Cable
- Introduction to Network Devices
 - Hub
 - Switch
 - Router
 - Modem
- Performed Simulation of Hub, Switch and Router with difference senarios on Packet tracer.
- Introduction with Inbound & Outbound Rules in networking.
- How to allow or block an software/Program/Port from Firewall (Inbound & Outboud).

Replace all figures of devices with the real pictures you used during the lab

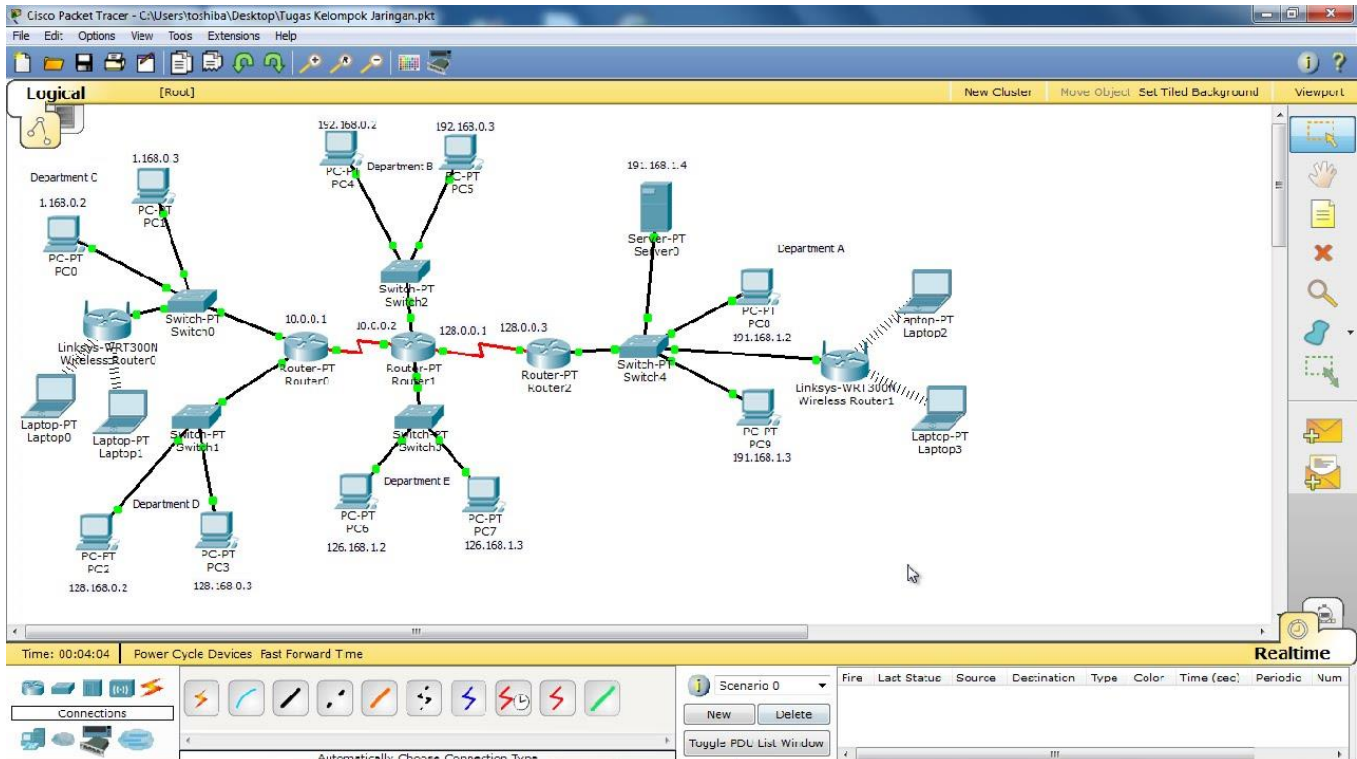
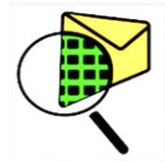


Computer Networks

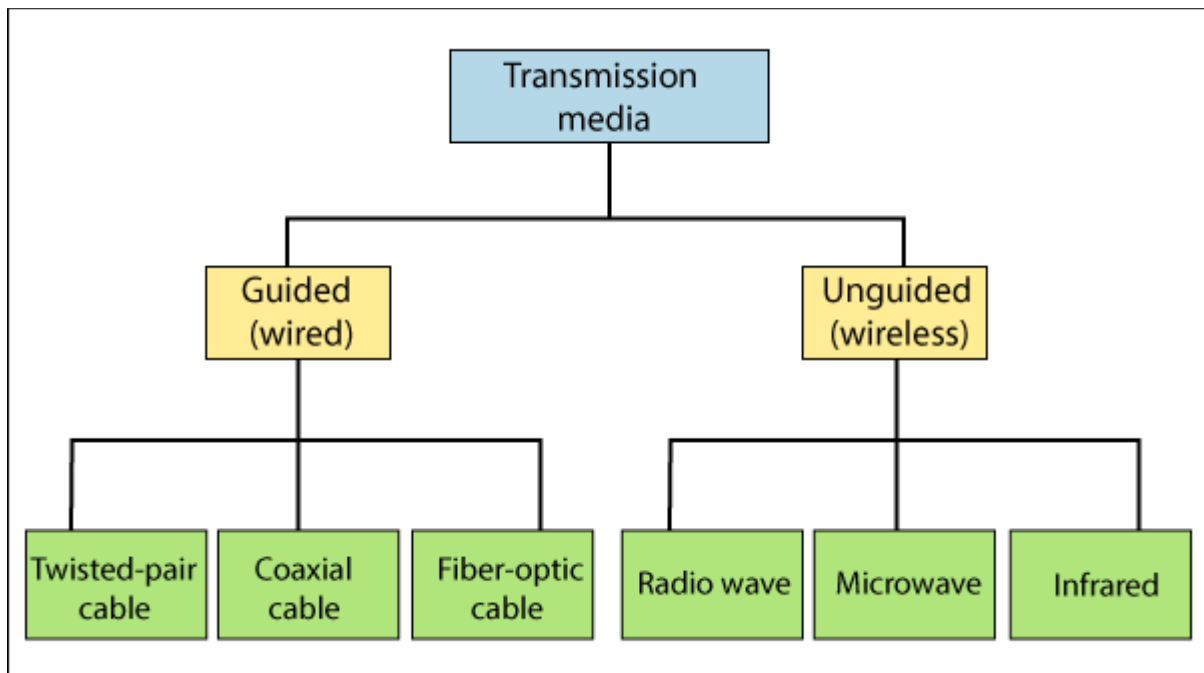
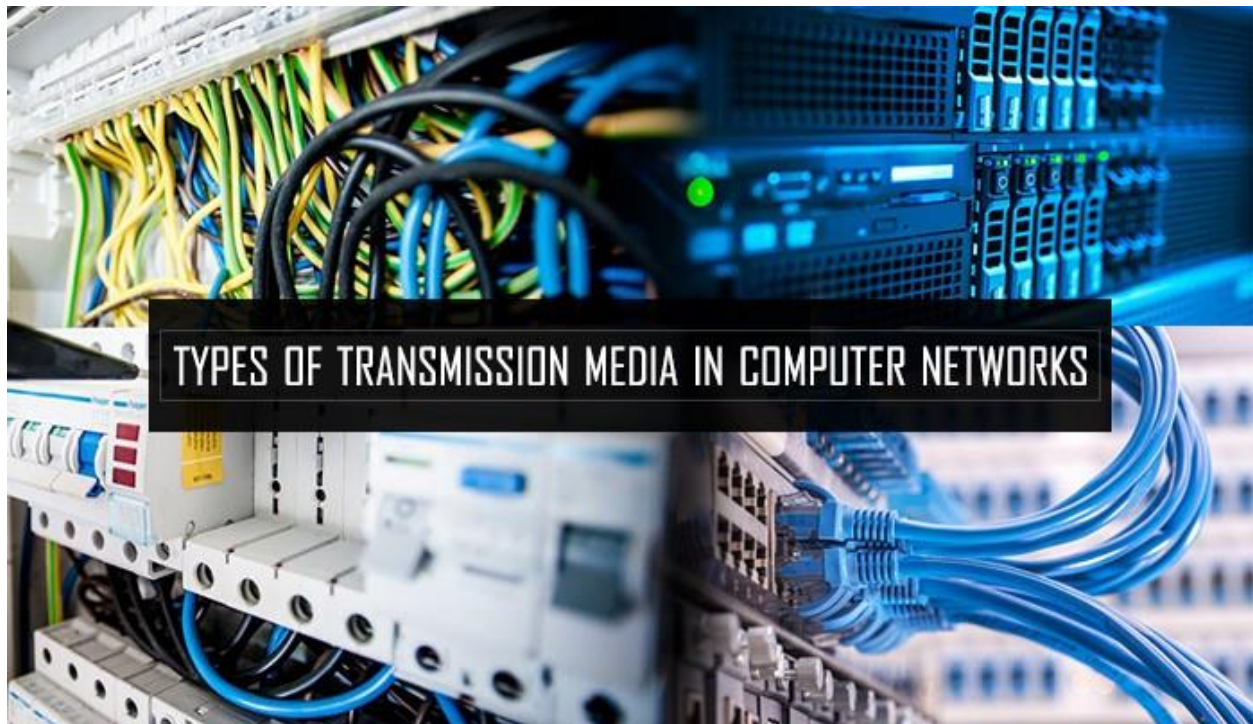
A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

What Is CISCO Packet Tracer?

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.



The transmission media is nothing but the physical media over which communication takes place in computer networks. The transmission of data over transmission media may be unguided (wireless) or guided (wired).



WIRELESS

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

WIRED

In wired communication a physical link is established between two devices. The link may be of different types.

CABLE

Alternatively referred to as a cord, connector or plug, a cable is one or more wires covered in a plastic covering that connects a computer to a power source or other device.

Networking cables are used to connect one network device to other network devices or to connect two or more computers to share printer, scanner etc. Different types of network cables like Coaxial cable, Optical fiber cable, Twisted Pair cables are used depending on the network's topology, protocol and size. The devices can be separated by a few meters (e.g. via Ethernet) or nearly unlimited distances (e.g. via the interconnections of the Internet).

I. COAXIAL CABLE

Coaxial lines confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them and though.

The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax).



Figure 3.2. Coaxial Cable

II. TWISTED PAIR CABLE

A cable made by intertwining two separate insulated wires. There are two twisted pair types: shielded and unshielded. A Shielded Twisted Pair (STP) has a fine wire mesh surrounding the wires to protect the transmission; an Unshielded Twisted Pair (UTP) do not. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. While twisted-pair cable is used by older telephone networks and is the least expensive type of local-area network (LAN) cable, most networks contain some twisted-pair cabling at some point along the network.

e.g. CAT6 (Category 6 UTP Cable (computer networks)).

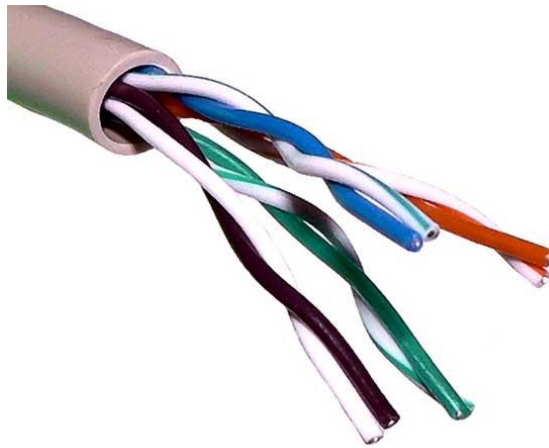


Figure 3.3. CAT6 Twisted pair cable

Q. Write note on CAT2, CAT3, CAT4, CAT5, CAT5e, CAT6, CAT7.

III. FIBER OPTICS

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.

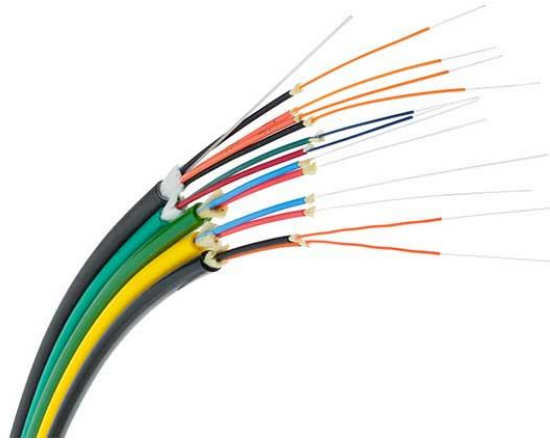


Figure 3.4. Fiber optic

Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

STRAIGHT-THROUGH CABLE

A straight-through network cable is just what the name suggests, a cable that passes data straight through from one end to another end. These cables are used for a variety of connections, for instance, connecting a computer to a hub or switch, connecting a computer to a cable/ISDN/DSL modem, and linking switches and hubs together. One such cable connection is shown in Figure 2.1.

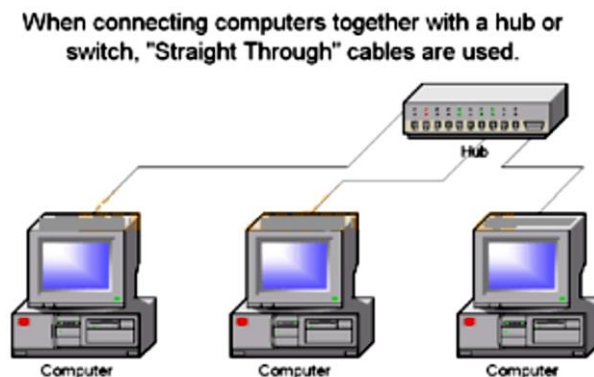


Figure 3.5. Straight-through Cable

Typically the ports on a hub are MDIX ports that allow the machine at the other end to utilize its MDI Port without the need for a crossover cable. Through these ports, hub automatically performs the crossover functions, which are required to properly align the cables with each other. When no hub or switch is used, cable itself must physically perform these crossover functions.

About Cabling

The two most common UTP (Unshielded Twisted-Pair) network standards are the 10 Mbps (10BASE-T Ethernet) and the 100 Mbps (100BASE-TX Fast Ethernet). In order for a cable to

properly support 100 Mbps transfers, Category 5 (or CAT 5) twisted pair cable must be used. This type of low loss extended frequency cable will support 10 Base-T, 100 Base-T and the newer 100VG-AnyLAN applications. Other types of cabling include Category 3 that supports data rates up to 16 Mbps, and Category 1 that only supports data rates up to 1Mbps.

Tools Required

The tools required to do this lab are:

- CAT 6 network cable
- RJ-45 Connectors
- Cable Cutter
- Crimping tool, &
- Cable tester.



Figure 3.6. Tools Required for Cabling

Procedure

Well, the wire has two sides. Let's call one side ... Side A and the other side ... Side B. Do the following steps with Side A of the wire.

1. Remove the plastic cover from the cable up to two inches. You will see 4 twisted pairs (total 8 wires). In each twisted pair, one wire will be colored and the other will be white. For example, one will be Green and the other will be White having Green marks. The latter is called Green-White. Similarly there will be Brown wire twisted with Brown-White, Blue wire twisted with Blue-White, Orange twisted with Orange-White. This can be seen in Figure 2.3.



Figure 3.7. Cable Pairs

2. Untwist the wires and make them smooth (don't remove the plastic covers from the metal wires).
3. Arrange the wires in the order: Orange-White, Orange, Green-White, Blue, Blue-White, Green, Brown-White, and Brown. The order is important since there is a wiring standard defined by the Telecommunications Industry Association (TIA) [<http://www.tiaonline.org>].
4. It's called the EIA/TIA-568 Commercial Building Telecommunications Wiring Standard, and you can find more information on it here: <http://www.digitaldelivery.com/Standards.htm#s5>
5. Cut the wires in straight fashion and insert in the RJ-45 Jack.
6. Using the Crimping tool, punch it properly. Perform Step 1-5 for Side B.

CROSS-OVER CABLE

A cross-over network cable is used to connect two computers directly. It is also used when you connect two hubs/Switches with a normal port on both hubs/Switches. (In other words, the cross cable is used relatively in a rare case.). It is used to connect similar devices.

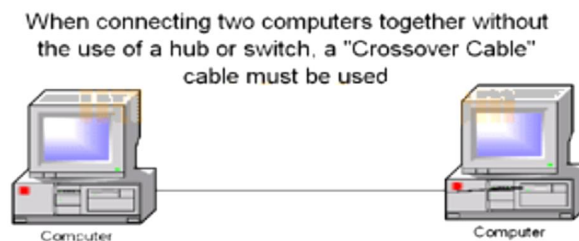


Figure 3.8. Cross-Over Cable

Tools Required

Same as used for making Straight-Through Cable.

Procedure

Side A

Perform Steps 1-5 mentioned above for making straight-through cable.

Side B

Arrange the wires as: green-white, green, orange-white, blue, blue-white, orange, brown-white, and brown. And punch it properly.

For Straight cables

For Cross cables

Pin #	Side A	Side B	Pin #	Side A	Side B
1	orange-white	orange-white	1	orange-white	green-white
2	Orange	Orange	2	Orange	green
3	green-white	green-white	3	green-white	orange-white
4	Blue	Blue	4	Blue	blue
5	blue-white	blue-white	5	blue-white	blue-white
6	Green	Green	6	Green	orange
7	brown-white	brown-white	7	brown-white	brown-white
8	Brown	Brown	8	Brown	brown

Table 3.1 Straight-Through & Cross-Over Cable Connections

TESTING CABLES

Once both cables are ready, test it to make sure it works by means of a cable tester. Insert the two ends of the cable into the jacks on the tester and watch the lights. If they all light up, wire has a good connection and ready to use.

CABLE TESTER

A cable tester is a device that is used to test the strength and connectivity of a particular type of cable or other wired assemblies. There are a number of different types of cable testers, each able to test a specific type of cable or wire (some may be able to test different types of cables or wires). The cable tester can test whether a cable or wire is set up properly, connected to the appropriate source points, and if the communication strength between the source and destination is strong enough to serve its intended purpose. The picture is an example of a cable tester from TRENDnet.



Figure 3.9. TRENDnet Cable tester

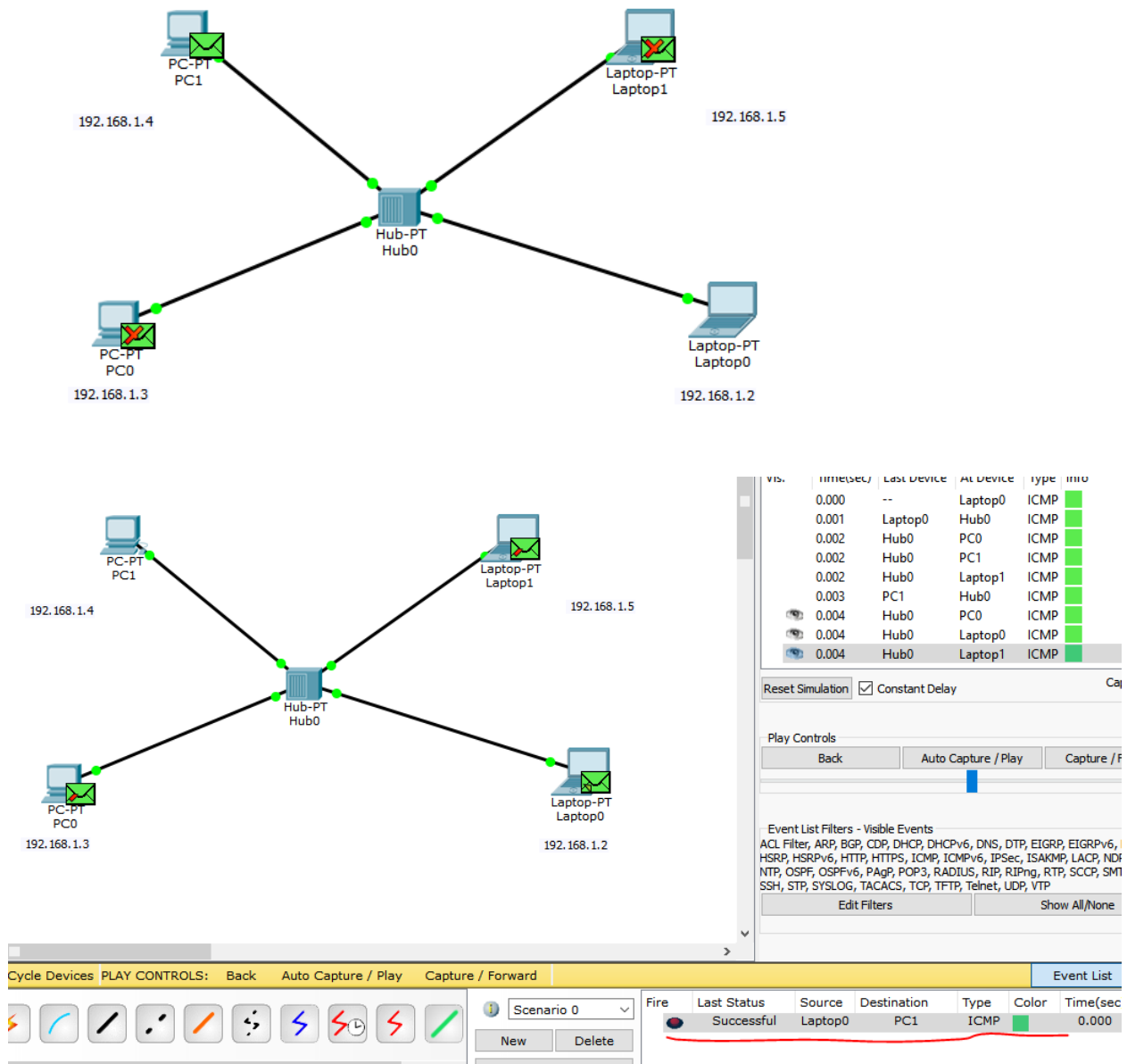
NETWORKING DEVICES

HUB

When referring to a network, a hub is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection. Most hubs can detect basic network errors such as collisions, but having all information broadcast to multiple ports can be a security risk and cause bottlenecks. In the past network hubs were popular because they were much cheaper than a switch and router, but today most switches do not cost much more than a hub and are a much better solution for any network.



Figure 3.10. Dlink 7 port HUB



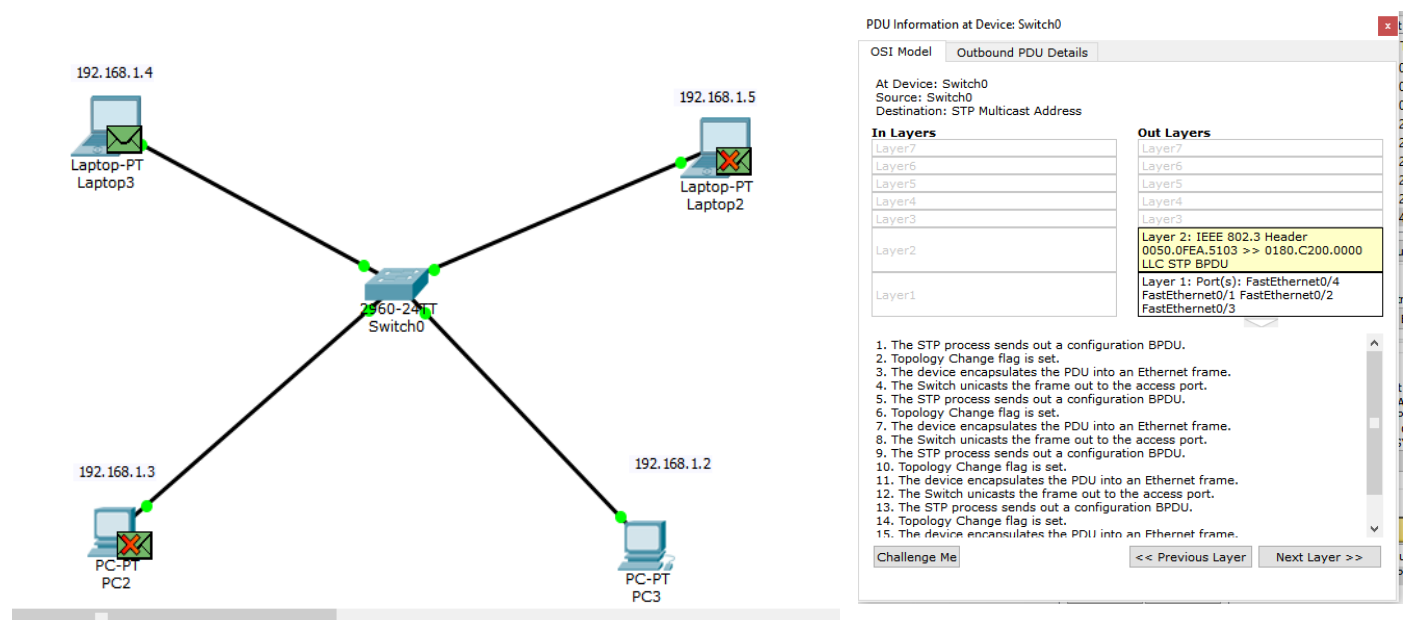
SWITCH

On a network, a switch is a hardware device that filters and forwards packets through the network, but often not capable of much more. The first network device that was added to the Internet was a switch called the IMP, which helped send the first message on October 29, 1969. A network switch is more advanced than a hub but not as advanced as a router. The picture shows an example of a NETGEAR 5 port switch.



Figure 3.11. NETGEAR 5 Port Switch

CiscoPacket Tracer Simulation of Switch with end devices



Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.778	Switch0	PC2	STP	
	0.778	Switch0	PC3	STP	
	0.778	Switch0	Laptop3	STP	
	2.778	--	Switch0	STP	
	2.779	Switch0	Laptop2	STP	
	2.779	Switch0	PC2	STP	
	2.779	Switch0	PC3	STP	
	2.779	Switch0	Laptop3	STP	
	4.778	--	Switch0	STP	

Reset Simulation ☒ Constant Delay Captured to: 4.778 s

Play Controls: Back Auto Capture / Play Capture / Forward

Event List Filters - Visible Events
 ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters Show All/None

Scenario 0 Fire Last Status Source Destination Type Color Time(sec) Period

Successful	PC3	Laptop3	ICMP		0.000	N
------------	-----	---------	------	--	-------	---

PDU Information at Device: Switch0

OSI Model Outbound PDU Details

PDU Formats

Ethernet 802.3

0		4		7		8		14		19		Bytes	
PREAMBLE: 1010 1010				S F		D		DEST ADDR: 0180.C200.0000				SRC ADDR: 0050.0FEA.5103	
LENGTH / TYPE: 0x3				DATA (VARIABLE LENGTH)						FCS: 0x0			

ROUTER

A hardware device designed to take incoming packets, analyze the packets, moving the packets to another network, converting the packets to another network interface, dropping the packets, directing packets to the appropriate locations, and performing any other number of other actions. The picture shows the Linksys BEFSR11 router and is what most home routers resemble.



Figure 3.12. Linksys BEFSR11 Router

A router has a lot more capabilities than other network devices such as a hub or a switch that are only able to perform basic network functions. For example, a hub is often used to transfer data between computers or network devices, but does not analyze or do anything with the data it is transferring. Routers however can analyze the data being sent over a network, change how it is packaged and send it to another network or over a different network. For example, routers are commonly used in home networks to share a single Internet connection with multiple computers.

Q. What is difference between Hub, Switch and Router?

What should I buy for my network, Hub, Switch or Router?

This question really depends on how you plan on using your network. For most users, a wireless network router is our recommendation. A wireless router allows wireless devices (e.g. your smartphone, tablet, wireless laptop) to connect to your network and because it is a router it also allows all devices to connect to the Internet.

If cost is a concern and you only want to connect a few computers to each other, a switch is the ideal solution since they are cheaper than a router.

In some situations you may need more than one router or switch. If you are in a big area such as an office you may need a router to connect all the computers to the Internet or other network and then use other routers, switches, or access points to connect other parts of the building to the same network.

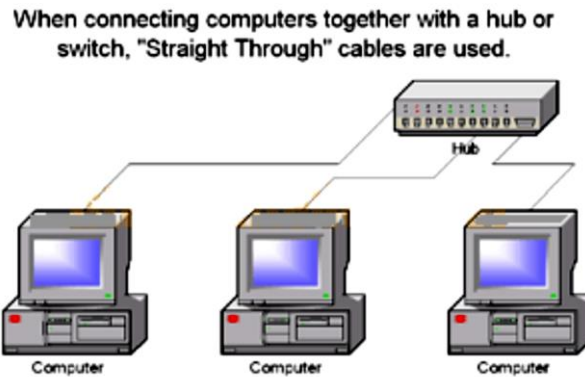
Q. List networking hardware vendors?

The Top 10 Intent-Based Networking Vendors Set to Disrupt Businesses in 2020

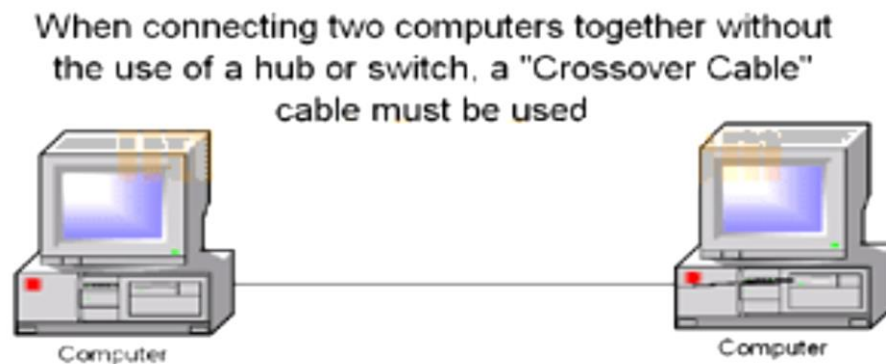
- Cisco. Finally, Cisco is probably the most notable company focused on IBN these days. ...
- Juniper. Juniper is a business making significant headway in the realm of IBN. ...
- Apstra. ...
- Huawei. ...
- Veriflow Systems. ...

- Indeni. ...
- Intentionet. ...
- Avi Networks.

Q. Connect the devices as follows and ping to show the connectivity



Q. Connect two computer directly as follows and ping to show the connectivity



OBJECTIVES

After these Lab students shall be able to perform

- Setting Router Modes on 2600 Series Routers
- Changing Hostname of the Router
- Configuring Date and Time on the Router (Clock Set Command)
- Setting a banner on the Router
- Displaying the Router's Running-Configuration and Start-Up Configuration
- Enable Password and Enable Secret Password with the Encryption Techniques/Levels
- Line Console Password Implementation on CISCO 2600 Series Router
- What is Telnet? How to Telnet? + Line VTY/Telnet Password

PRE-LAB READING ASSIGNMENT

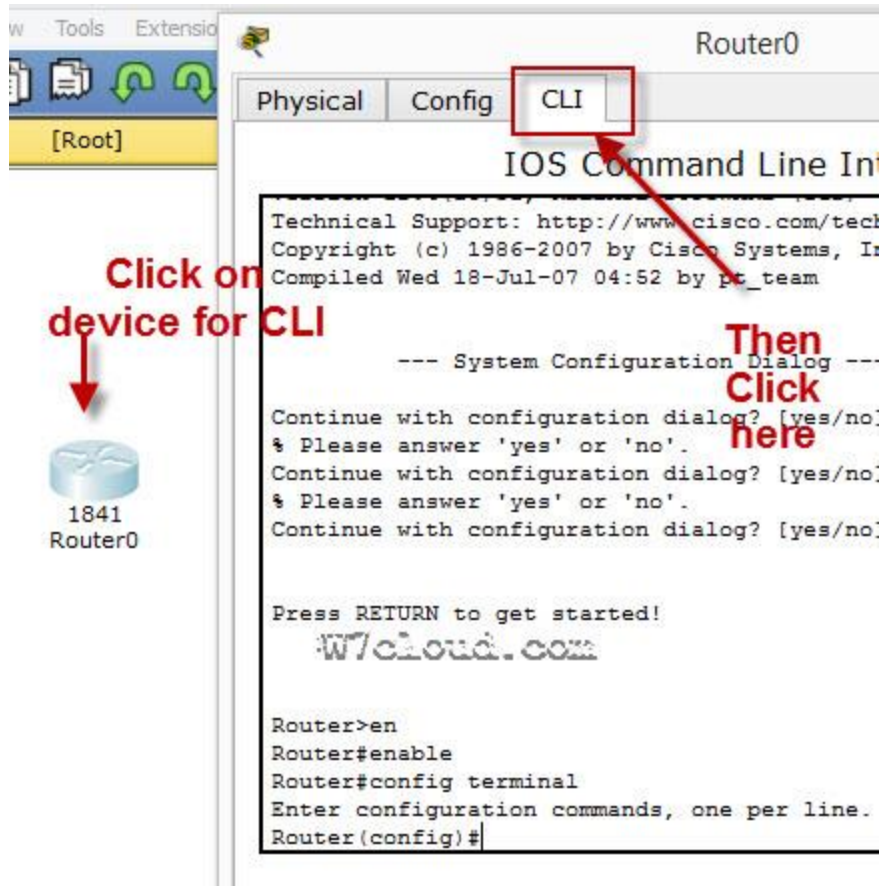
Remember the delivered lecture carefully.

EXPERIMENTS WITH DETAILS

Router>	- User EXEC mode
Router#	- Privileged EXEC mode
Router(config)#	- Configuration mode (notice the # sign indicates this is accessible only at privileged EXEC mode)
Router(config-if)#	- Interface level within configuration mode
Router(config-router)#	- Routing engine level within configuration mode
Router(config-line)#	- Line level (vty , tty, async) within configuration mode

Cisco Router Configuration Step By Step

To configure any device in packet tracer you are required to open or access its CLI. You can do it by clicking any device and then navigating to CLI tab. Once you are at CLI you can perform all Cisco Commands here.



Cisco IOS supports numerous command modes which can be practice with packet tracer, followings are the main command modes of cisco CLI with specific commands to navigate from one mode to other.

Mode	Symbol	How to access this mode	Command for leaving this mode
User EXEC Mode	Router >	Default mode after booting. Press enter for accessing this.	Use exit command
Privileged EXEC mode	Router #	Use enable command from user exec mode for entering into this mode	exit
Global Configuration mode	Router(config)#	Use configure terminal command from privileged exec mode	Exit or Ctrl+Z for user EXEC mode
Interface Configuration	Router(config-if)#	Use interface <interface name+number> command from global configuration mode	Use exit command to return in global mode

IOS commands are not case sensitive it means that you can use them in uppercase, lowercase, or mixed case, but passwords are case sensitive. Therefore make sure you type it in correctly. In any mode, you can obtain a list of commands available on that mode by entering a question mark (?).

```
Braunch_office_router(config)#router ?
  bgp      Border Gateway Protocol (BGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf     Open Shortest Path First (OSPF)
  rip      Routing Information Protocol (RIP)
Braunch_office_router(config)#router |
```

How to Change the Cisco Router name

You can change the cisco router name by using command **hostname** in global configuration mode.

```
Router(config)#hostname HR-Router
HR-Router(config)#
```

ROUTER MODES

Router> enable

Note: This command allows you to enter into Privileged exec mode/enable mode, where you can have more options for show and other commands. The next prompt looks like this:

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Note: This command allows you to enter into global configuration mode, where you can configure a range of commands. The prompt for this command looks like this:

```
Router(config)#
```

```
Router(config)# exit
```

```
Router#exit
```

```
Router>
```

CHANGING HOSTNAME

To specify or modify the host name for the router, global configuration command HOSTNAME is used. HOSTNAME is case sensitive. The host name is used in prompts and default configuration filenames. The factory-assigned default host name is router.

```
Router> enable
```

```
Router#configure terminal
```

```
Router(config)#hostname NP
```

```
Router(config)# exit
```

```
NP#
```

CONFIGURATION OF DATE & TIME

The system clock runs from the moment the system starts up and keeps track of the current date and the time based on coordinated Universal Time(UTC), also known as Greenwich Mean Time(GMT). The system clock can be set from a number of sources, and in turn can be used to distribute the current time through various mechanisms to other systems. To manually set the system clock, use one of the formats of the clock set Exec command.

```
NP#clock set ?
```

```
Hh:mm:ss current time
```

Note : Allow you to see the format of complete command.

```
NP#clock set 12:15:00 ?
```

```
<1-31> Day of the month
```

```
Month Month of the year
```

NP#clock set 12:15:00 17 ?

Month Month of the year

NP#clock set 12:15:00 17 March ?

<1993-2035> Year

NP#clock set 12:15:00 17 March 2021

Verification:

NP#show clock

12:16:56. 441 UTC Wed Mar 17 2021

SETTING A BANNER

When someone connects to the router, the MOTD (Message of the Day) banner appears before the login prompt.

NP>enable

NP#configure terminal

NP(config)#banner motd # welcome to Networks Professionals #

NP(config)#exit

NP#

Note: # is a delimiting character. It is used before the start and ending of a message. You can use any character.

Verification:

NP#exit

NP con0 is now available

Press return to get started

Welcome to Networks Professionals

NP>

DISPLAYING RUNNING-CONFIGURATION

NP#show running-config

Building configuration.

Current configuration : 599 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname NP

!

!

ip cef

no ipv6 cef

!

spanning-tree mode pvst

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

shutdown

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

```
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!

banner motd ^C Welcome To Networks Professionals ^C
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
end
```

LINE CONSOLE PASSWORD

The router has a number of ports that allow access to the router, on each of these ports you can specify passwords to provide a layer of security to the router. There is also the option of disabling login password checking to any of the ports by entering the command to get to the Router (config-line)# section of the port and entering the no login command.

The console port is on the back of the router and is used to directly connect a console to the router for configuring the router. This port should allow logins with passwords if the router is physically secured. The port should be disabled if it is not regularly used or the router is not secured. To specify a password on a line, use the password line configuration command. The first character cannot be a number. The string

can contain any alphanumeric characters, including spaces, up to 80 characters. Console password is needed when logging into router at user EXEC mode from console.

```
NP>enable
NP#configure terminal
NP(config)#line console 0
NP(config-line)#password NP123
NP(config-line)#login
NP(config-line)#end
```

Verification:

```
NP#exit
NP con0 is now available
Press RETURN to get started
Welcome To Networks Professionals
User Access Verification
Password: NP123
NP>enable
```

LINE VTY / TELNET PASSWORD

virtual terminal lines (vty) are used to allow remote access to the router (by telnet through its interfaces). The router has variable virtual terminal lines depending upon the model of router.

```
NP# configure terminal
NP(config)# line vty 0 4
NP(config-line) # password NP456
NP(config-line)# login
NP(config-line)# exit
NP(config)# exit
```

NP#

AUXILIARY LINE PASSWORD

The auxiliary port is on the back of the router and is commonly used to connect a modem to. It is used to allow a remote user access to the configuration of the router. If a modem is connected to the port, it should definitely have a password specified for it.

NP #configure terminal

NP(config)# line aux 0

NP(config-line)# password NP@786

NP(config-line)# exit

NP(config-line)#login

NP(config)# exit

NP#

PASSWORD FOR PRIVILEGED MODE

To set a local password to control access to various privilege levels, use the enable password global configuration command. An enable password is defined as follows:

It must contain uppercase and lowercase alphanumeric characters from 1 to 25. Must not have a number as the first character.

Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.

NP# configure terminal

NP(config)# enable password NP222

NP(config)# exit

NP#

Verification:

NP con0 is now available

Press RETURN to get started.

Welcome To Networks Professionals

NP>

NP>enable

Password:NP222

NP#

```
NP#SHOW RUNNing-config
Building configuration...

Current configuration : 623 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname NP
!
!
!
enable password NP222
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
```

SECRET (ENCRYPTED) PASSWORD FOR PRIVILEGED MODE

The enable secret password is the password in encrypted form and is used to gain access to enable mode and to the global configuration mode on the router. The enable password is used when you do not specify an enable secret password. The enable password should be different from the enable secret password.

NP#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

NP(config)#enable ?

password Assign the privileged level password

secret Assign the privileged level secret

NP(config)#enable secret NP333

NP(config)#exit


```
NP(config-line)#no login
NP(config-line)#no password
NP(config-line)#end
NP#
```

REMOVING AUXILIARY LINE PASSWORD

```
NP>enable
NP#configure terminal
NP(config)#line aux 0
NP(config-line)#no login
NP(config-line)#no password
NP(config-line)#exit
NP(config)#exit
NP#
```

REMOVING PASSWORD FOR PRIVILEGED EXEC MODE

```
NP>enable
NP# configure terminal
NP(config)#no enable password
NP(config)# exit
NP#
```

REMOVING SECRET PASSWORD

```
NP>enable
NP# configure terminal
NP(config)#no enable secret
NP(config)# exit
NP#
```

How to set the IP address to Cisco interface:

You can set the IP address to any Cisco device interface by using the following commands:

```
Router(config)#interface <interface name&number>
Router(config-if)#ip address <IP address> <subnet mask>
```

How to enable a port or interface

```
Router(config-if)#no shut
```

Example:

```
Router(config)#interface fastEthernet 4/0
Router(config-if)#ip address 192.168.77.88 255.255.255.0
Router(config-if)#no shut
```

How to check the IP address of all interfaces:

You can use the “**show ip interface brief**” command in Privileged EXEC mode for checking the IP address of all interface of Cisco device.

```
Router#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet1/0	unassigned	YES	NVRAM	administratively down	down
Serial2/0	unassigned	YES	NVRAM	administratively down	down
Serial3/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet4/0	192.168.77.88	YES	manual	down	down

STUDENT TASK-01

Students should make the physical scenario exactly given in the lab objectives. Implement the connectivity between router and computer and then manipulating with the different modes of the CISCO IOS. Students shall implement the security techniques used to secure the routers. Submit a final report after doing the mentioned task physically.

