Computer Networks-Lab 02

Instructor: Hurmat Hidayat

CL30001 – Computer Networks-Lab

SEMESTER Fall 2022

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

Table of Contents

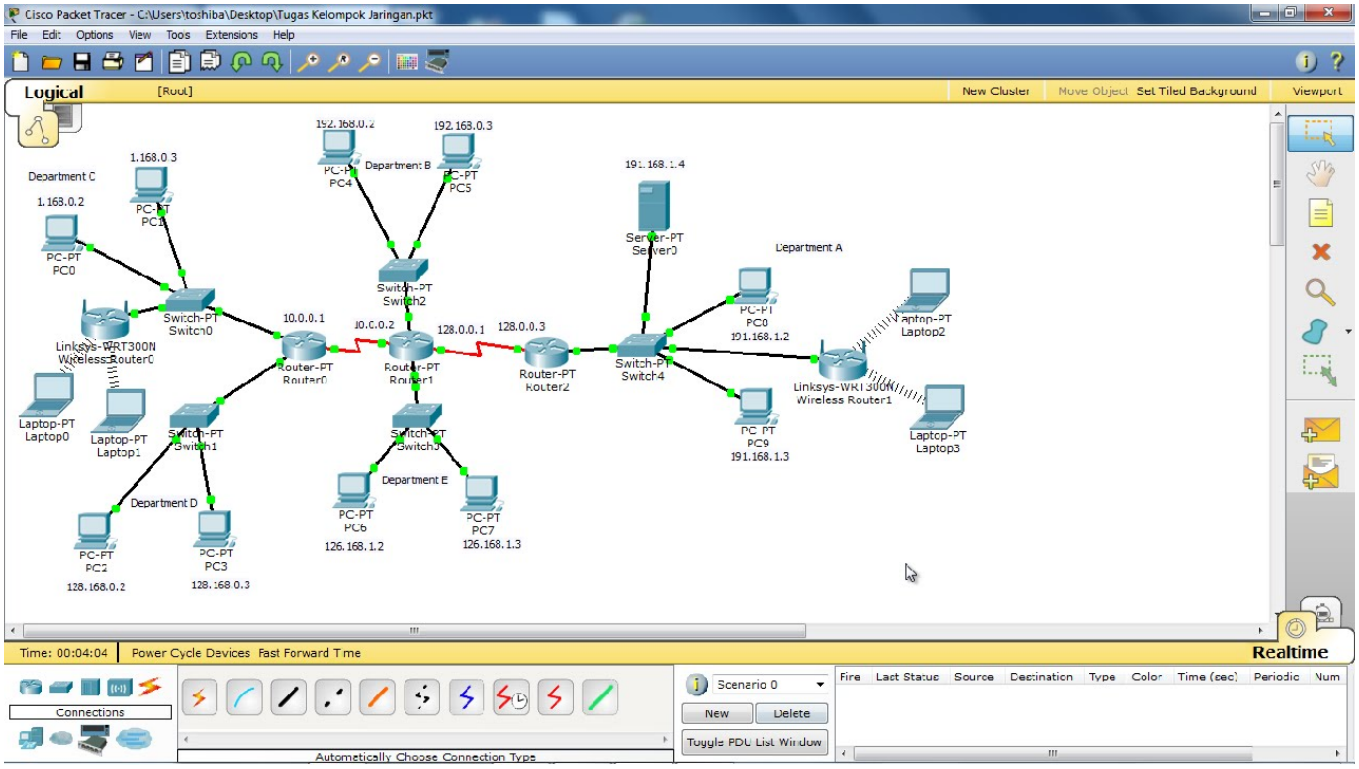
OBJECTIVES OF THE LAB

In this lab, we will cover the following:

- What Is CISCO Packet Tracer?
- Introduction to Transmission Media
    - Wired (guided)
    - Wireless(Unguided)
- 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
- Connecting two computers directly via Cross Over Cable
- Introduction to Network Devices
    - Hub, Switch ,Router, and Modem
- Performed Simulation of Hub and Switch with different scenarios on Packet tracer.

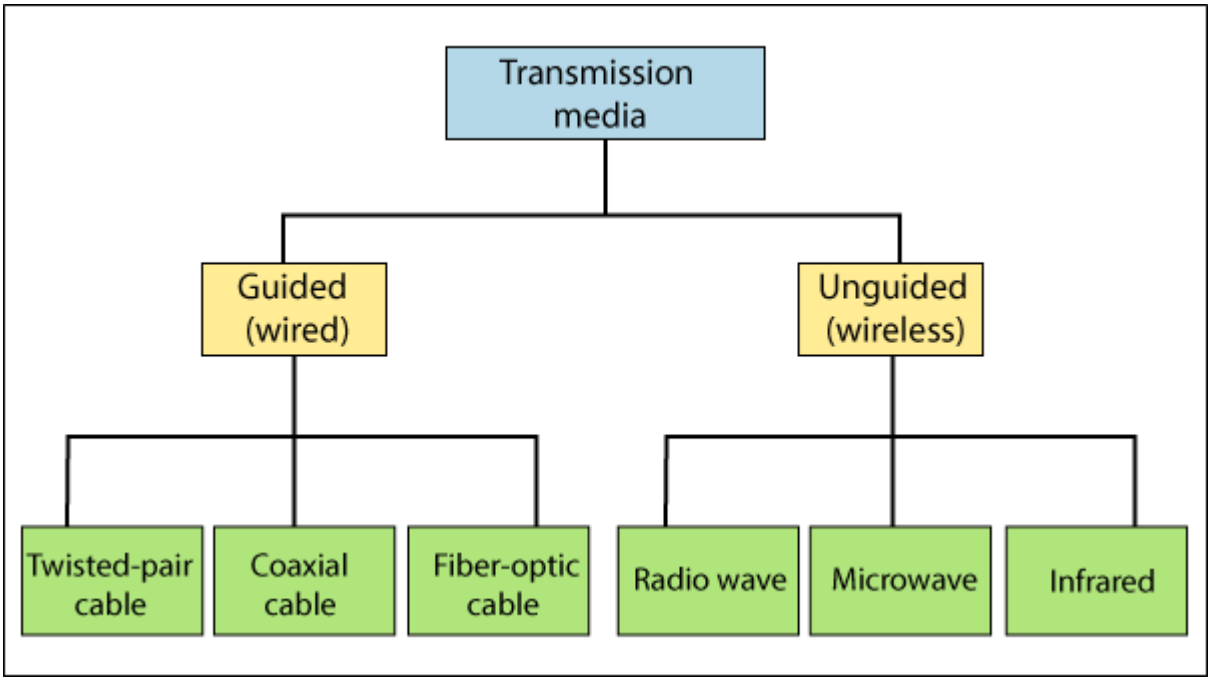
CISCO Packet Tracer

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.



Transmission Media

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. 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).

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

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)).

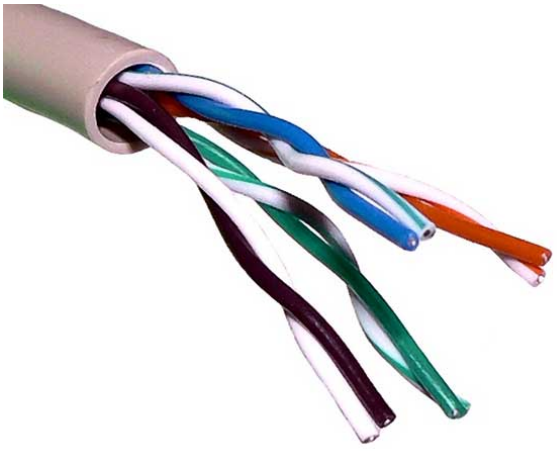


Figure 3.3. CAT6 Twisted pair cable

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

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.

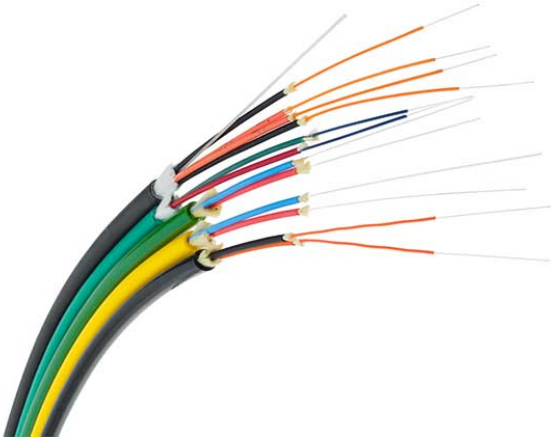


Figure 3.4. Fiber optic

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.

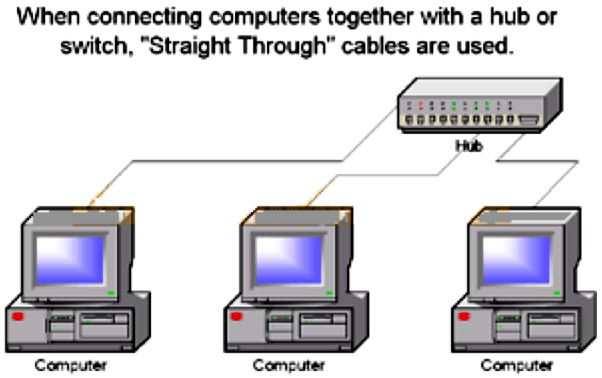


Figure 3.5. Straight-through Cable

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.

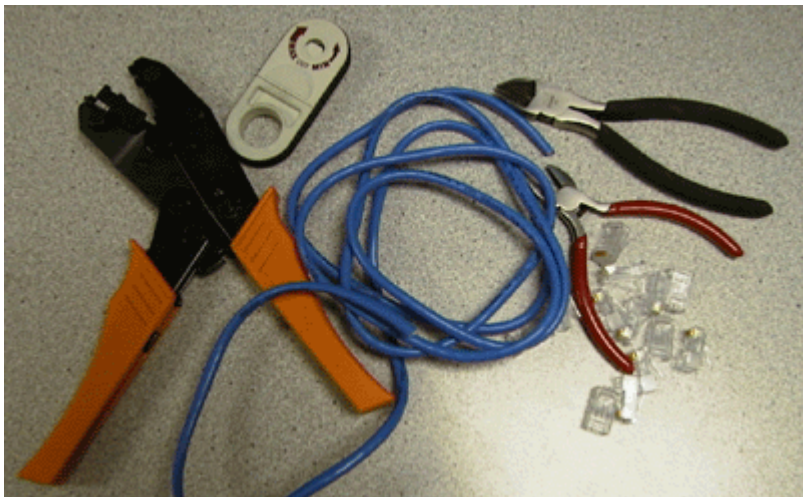


Figure 3.6. Tools Required for Cabling

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.

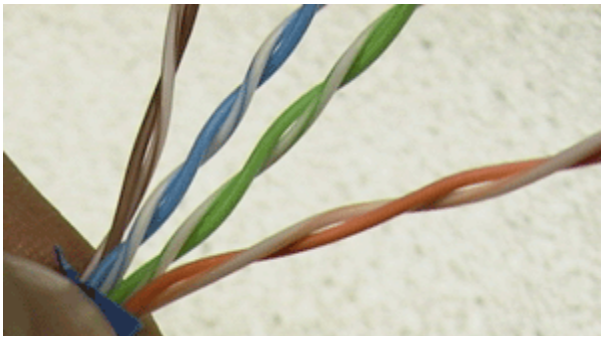
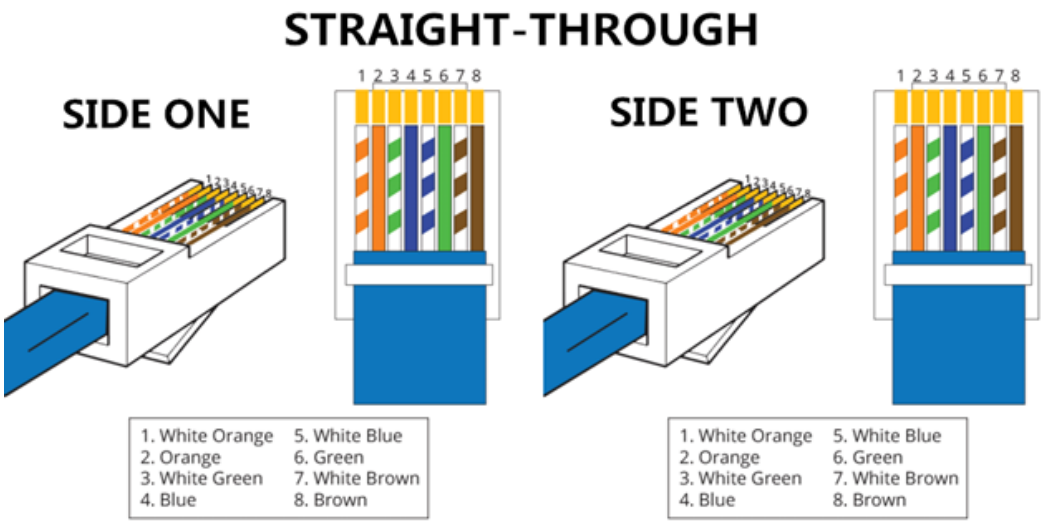


Figure 3.7. Cable Pairs

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.

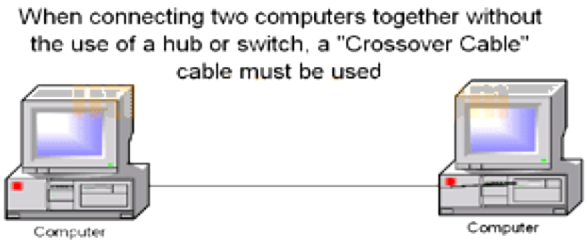


Figure 3.8. Cross-Over Cable

Tools Required

Same as used for making Straight-Through Cable.

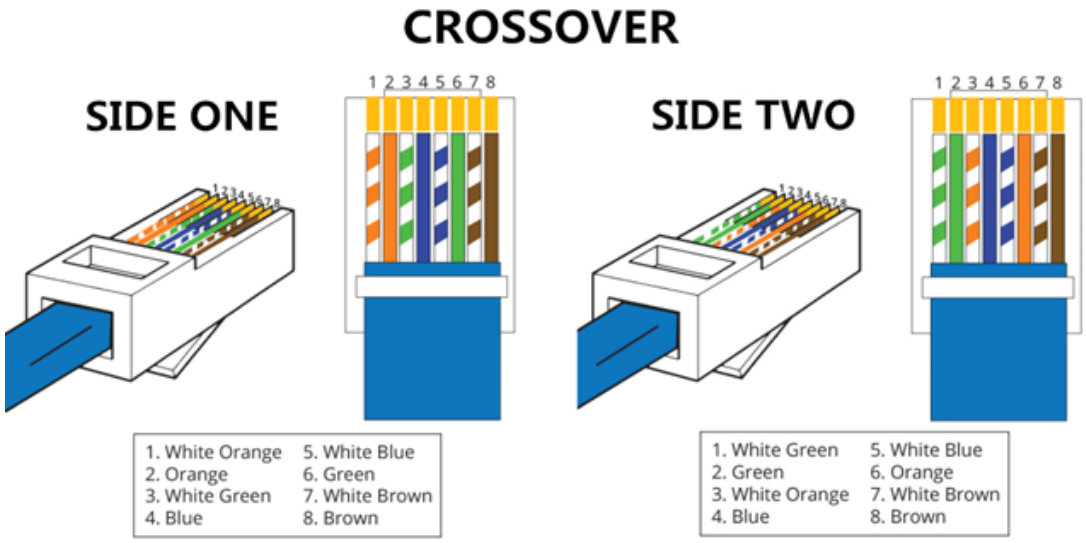
Procedure

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

Cisco packet tracer : Connecting Two PCs

We will look into how we can connect two computers/laptops using a virtual program called **CISCO Packet Tracer**.

Prerequisites:

- Laptop/Desktop
- CISCO Packet Tracer program

Run the Cisco Packet Tracer and Start the application.

Implementation:

Follow the below steps to implement the connection:

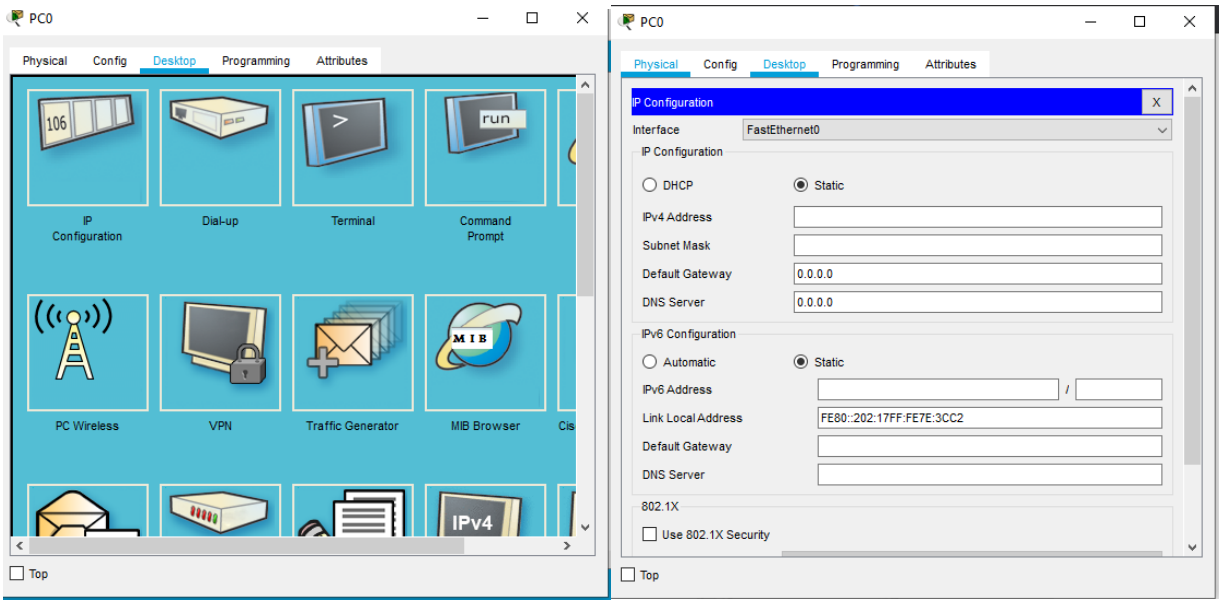
Step 1: From the bottom toolbar, click on ‘End Devices’ and select ‘PC’ and then click on the screen (for two PC’s do this step twice).

Bottom toolbar->End devices->PC

Step 2: Now to connect the PC's, we require a wire; we use cross-over wire to connect similar devices. Select Connections from the bottom toolbar, and select cross-over wire (that is the fourth wire).

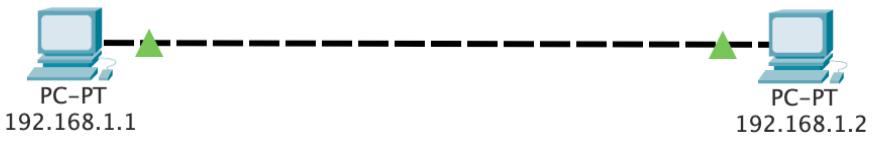
Step 3: After selecting the wire click on the computer on the screen(here PC0) and select FastEthernet0. Then, drag the wire to the other pc (here PC1) and do the same.

Step 4: Now, we will assign the IP address to both the PCs (PC0 & PC1). An **IP address** (Internet Protocol) is nothing but the numerical designation of the devices connected to the network, that use the Internet protocol as a communication medium. Click on PC0. A dialog box will appear on the screen, select Desktop and then select IP configuration :



After clicking on IP configuration this is what will appear. Now in IPv4 Address, write 192.168.1.1, Subnet mask will be 255.255.255.0. Similarly, assign 192.168.1.2 to PC1

We have successfully connected two computers.



Verify the connection using ping

Verify the connection by pinging the IP address of any host in PC0.

- Use the ping command to verify the connection.
- We will check if we are getting any replies or not.
- Here we get replies from a targeted node on both PCs. So, the connection is verified.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Understanding OUTPUT:

Interesting result from ping is round-trip time calculation. Measured in milliseconds, round-trip time indicates the delay between the sending of a ping request packet and the receipt of the corresponding response packet. The network delay or latency indicated by ping offers a good indicator of the responsiveness of network services on that remote host.

By default, ping waits Approximately 4,000 milliseconds (4 seconds) for each response to be returned before displaying the "Request Timed Out" message.

PING

The ping command is one of the most well-known tools available. Simply put, ping sends an "are you there?" message to a remote host. If the host is, in fact, there, ping returns a "yup, I'm here" message. It does this using a protocol known as ICMP, or Internet Control Message Protocol. ICMP was designed to be an error reporting protocol and has a wide variety of uses that we won't go into here.

Task: Using Packet Tracer connect two PCs as shown above and perform the following:

1. First Configure the PCs as shown above and verify the connection using ping command.
2. Configure PC1 as follow: IPv4: 192.168.1.1 Subnet mask: 255.255.255.0

   And PC2 as: IPv4: 192.168.2.1 Subnet mask: 255.255.255.0

3. Configure PC1 as follow: IPv4: 192.168.1.1 Subnet mask: 255.255.0.0

   And PC2 as: IPv4: 192.168.2.1 Subnet mask: 255.255.0.0

Verify each configuration using ping command and briefly describe the response.

NETWORKING DEVICES

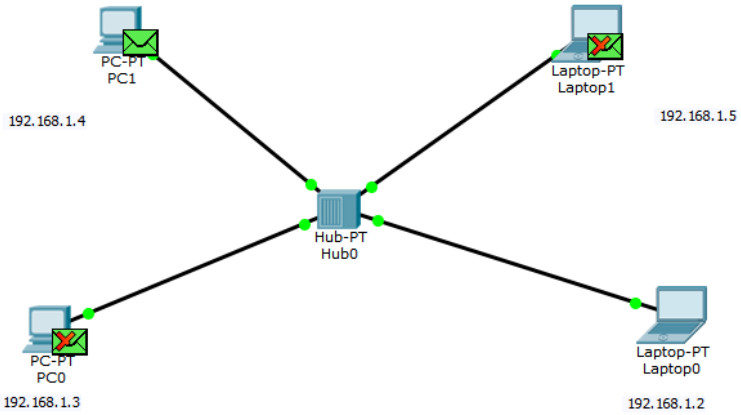
HUB

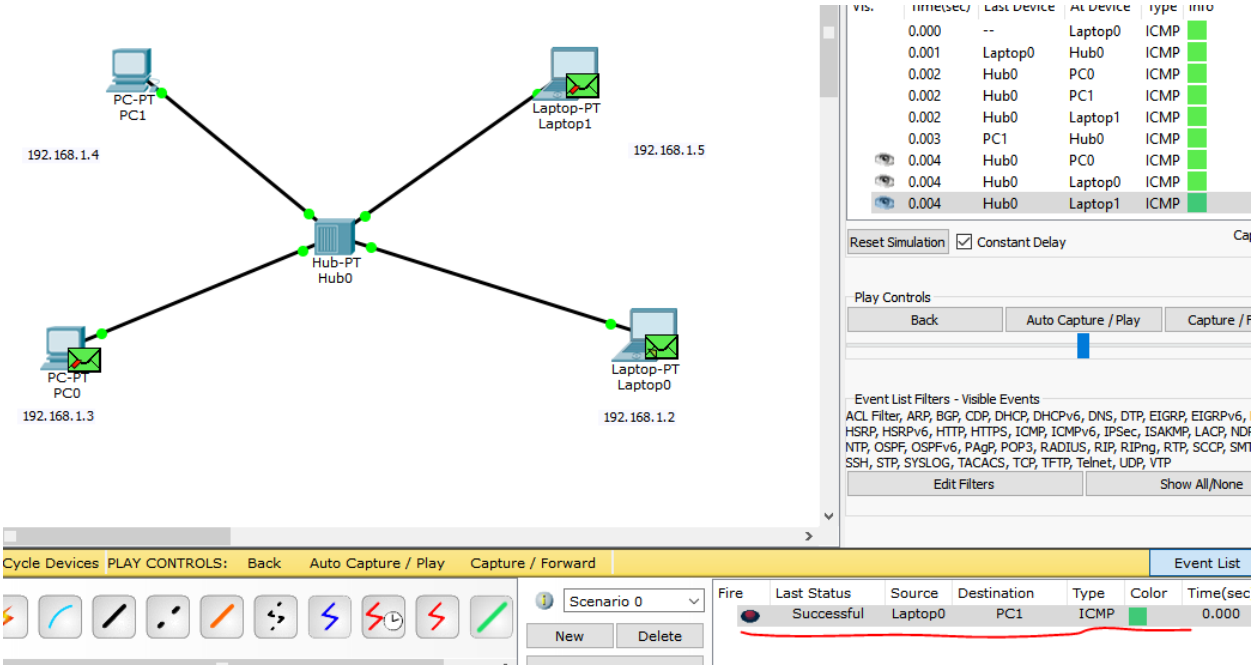
When referring to a network, a hub is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection. 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

Simulation of Hub with end devices

Task: Construct and simulate the following topology





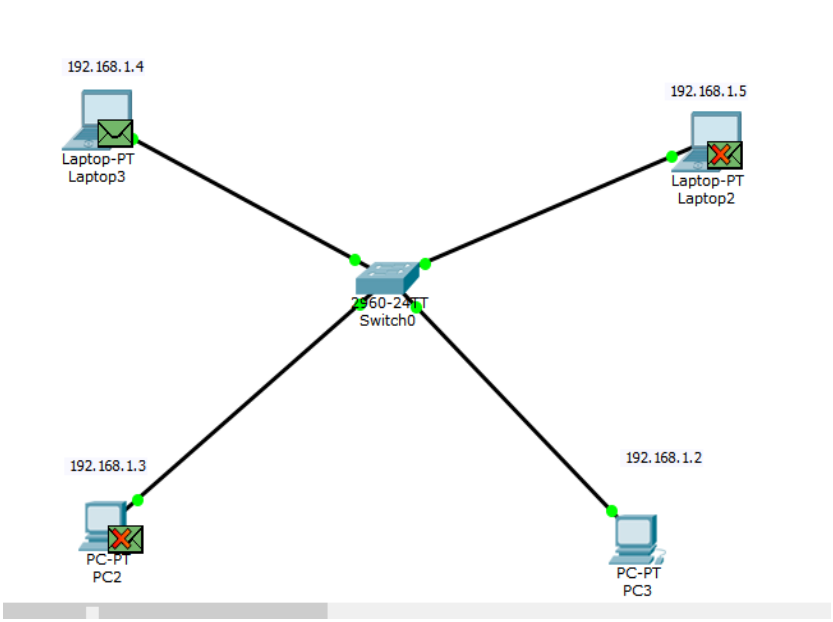
SWITCH

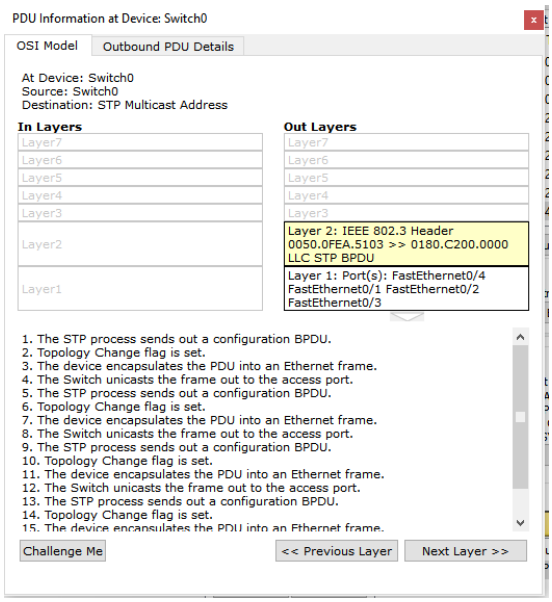
On a network, a switch is a hardware device that filters and forwards packets through the network, but often not capable of much more. The first network device that was added to the Internet was a switch called the IMP, which helped send the first message on October 29, 1969. A network switch is more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

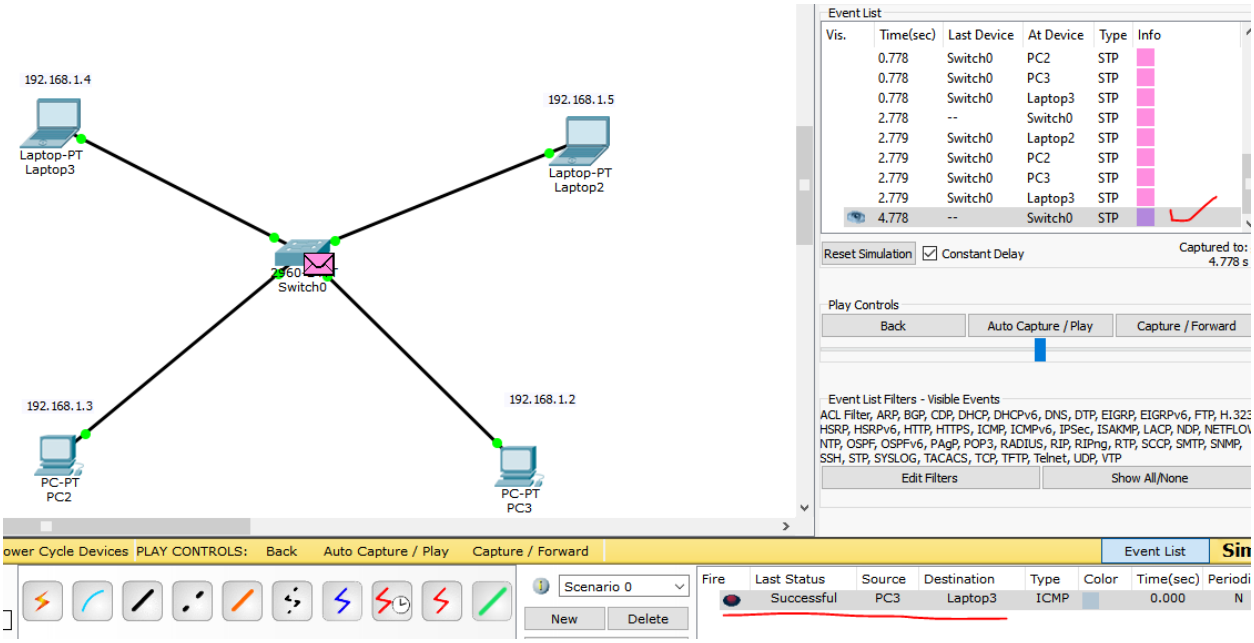
Figure 3.11. NETGEAR 5 Port Switch

Simulation of Switch with end devices

Task: Construct and simulate the following topology







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?

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

Q. List networking hardware vendors?

Connecting PCs Remotely

Utilities used to allow connect PC remotely:

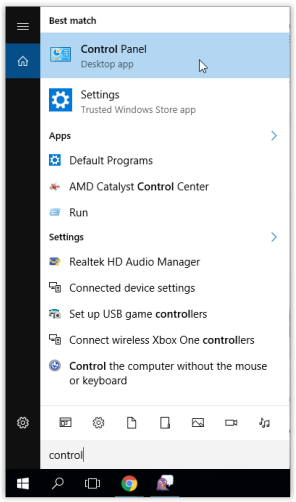
1. Any Desk https://anydesk.com/en/downloads/windows
2. TeamViewer https://www.teamviewer.com/en/download/windows/
3. Remote Desktop Connection (RDP)
4. VPN and Open SSH
5. Cloud Services (AWS, Google cloud, Azure)
    a. https://console.cloud.google.com/billing
    b. https://portal.azure.com/

Allow Access to Use Remote Desktop Connection (RDP): Windows 10

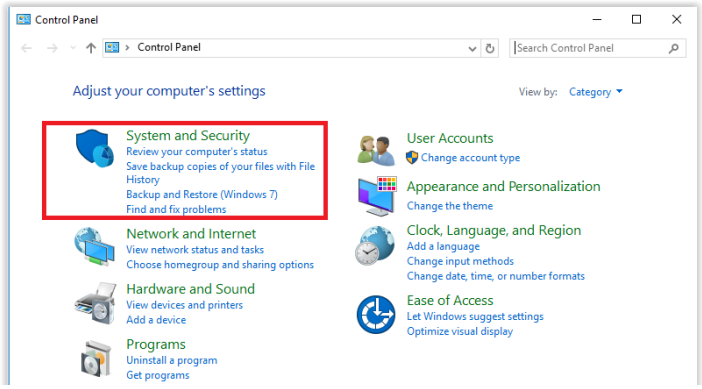
Before Remote Desktop can be used, permission has to be granted to the specific accounts that you would like to Allow to connect to your computer remotely. This is typically done on your *Office Computer*.

Option 1

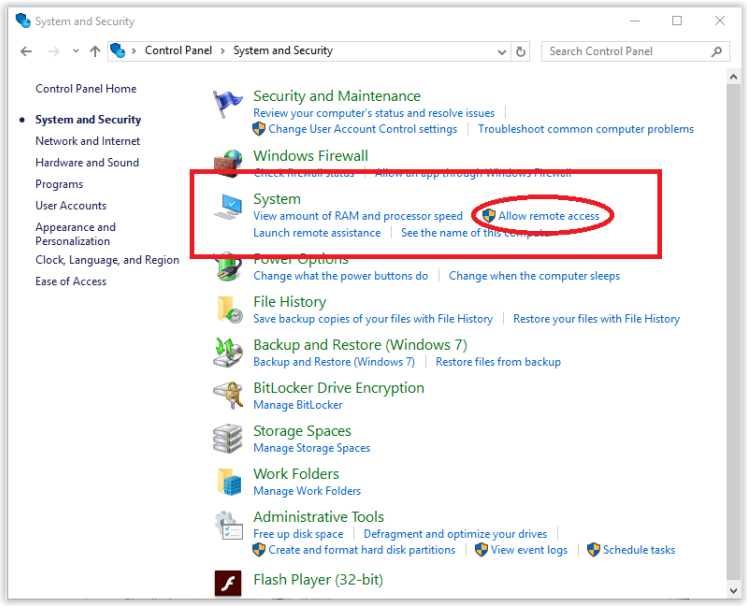
1. Click the **Start menu** from your desktop, and then click **Control Panel**.



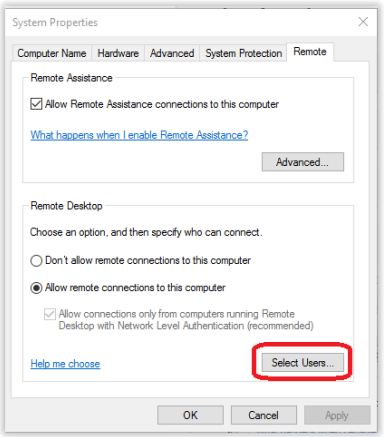
2. Click System and Security once the Control Panel opens.



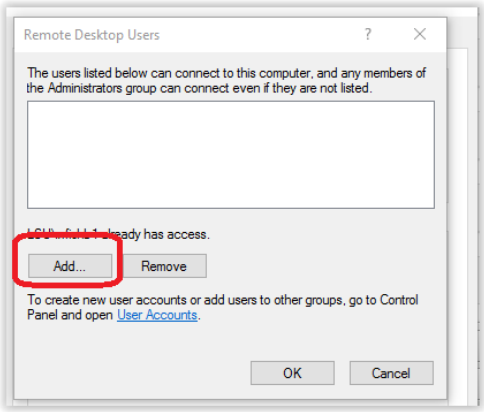
3. Click **Allow remote access,** located under the *System* tab.



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

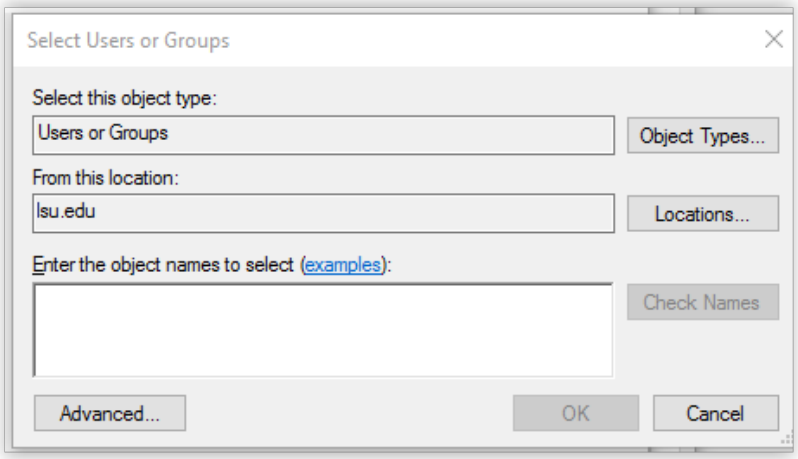


5. Click **Add** from the *System Properties* box.



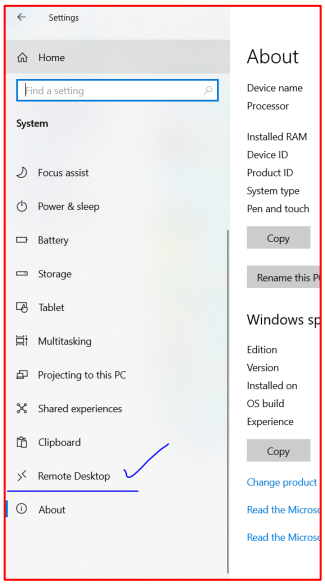
6. Type your **myLSU ID** and information for anyone else you would like to add. (This will allow *Remote Desktop* access to the computer which it is set.)

7. Click **OK** when finished.

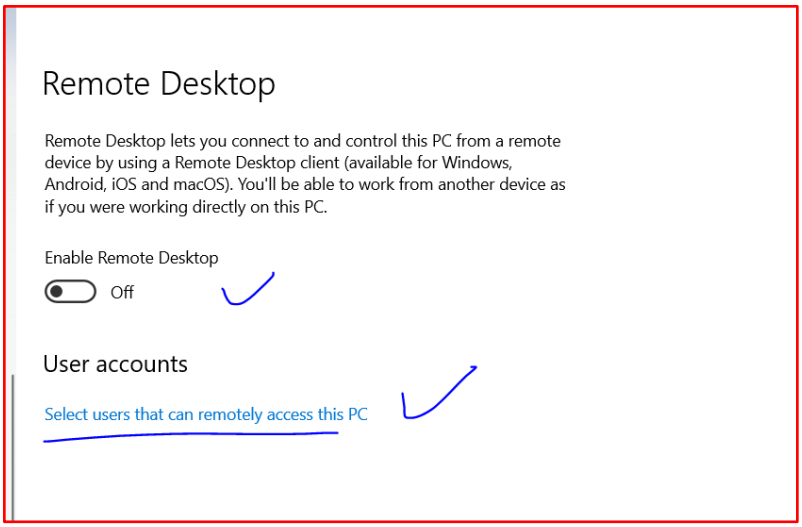


Option 2:

Go to setting and allow remote desktop connection:



Enable it and add your required user:



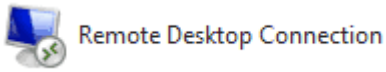
Remote Desktop Connection Client

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.

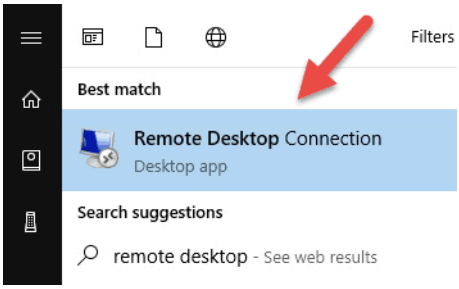
Step 1: Launch the Desktop Connection Unit

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

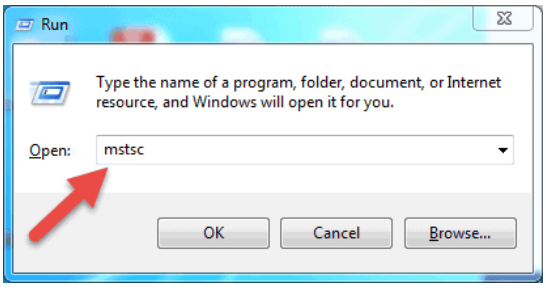
1. For Windows 7, click on Start -> All Programs, go to the 'Accessories' folder and click on Remote Desktop Connection. For Windows 10, Click on Start and locate the 'Windows Accessories' folder where you can also find the Remote Desktop Connection app.



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.

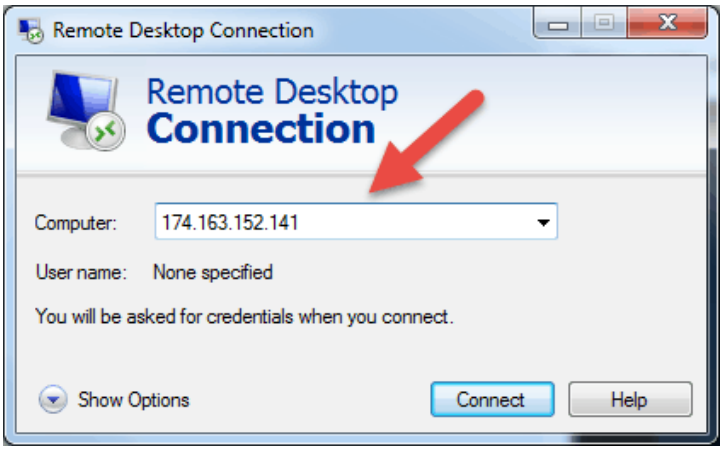


3. Press Windows + R keys on your keyboard to get the "Run" box. Type in mstsc and hit Enter in the 'Open:' field to run the Remote Desktop client.



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**.

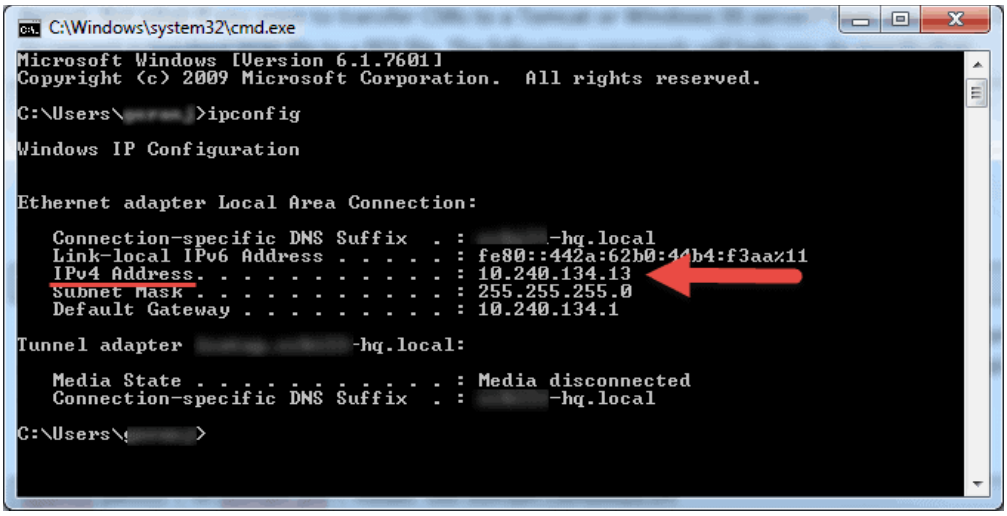


How to Find the IP Address and Host Name

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. Your will see your computer's private IP address under the **IPv4 Address** line**.**



To determine which public IP address a computer is using:

From your web browser, go to com or use its search bar. Type in "what is my IP" or simply "my IP" and hit Enter.

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:

Right Click on Computer, or This PC, depending on the Windows OS version you are using. Click on

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

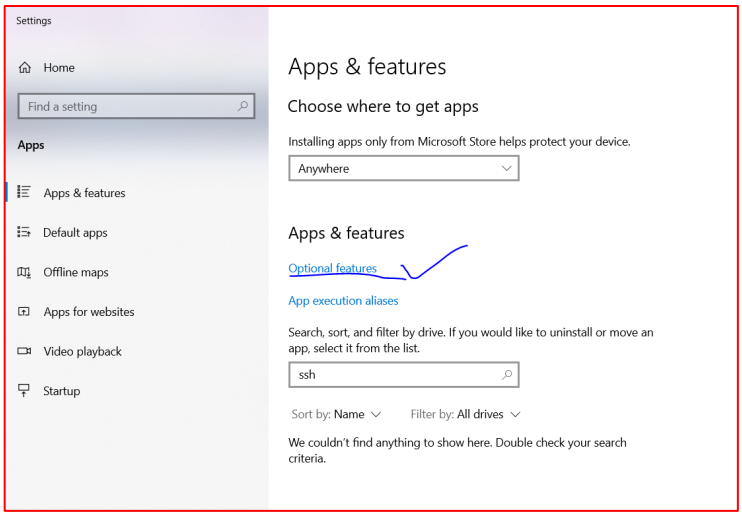
After you hit connect, the loading bar will appear. When it finishes initiating and configuring the remote session you will get a pop-up window that will look similar to this:

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.

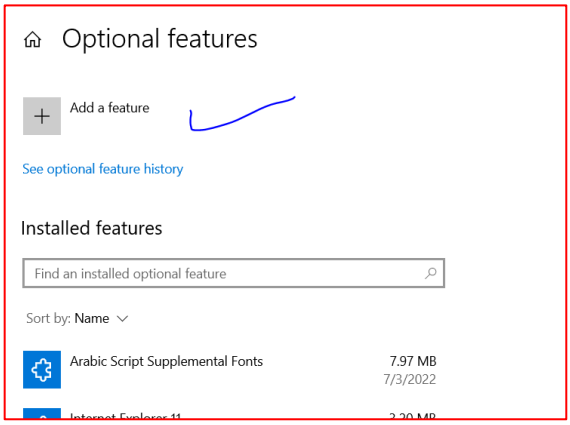
Access remotely using Open SSH Server:

Server-side OS (window 10)

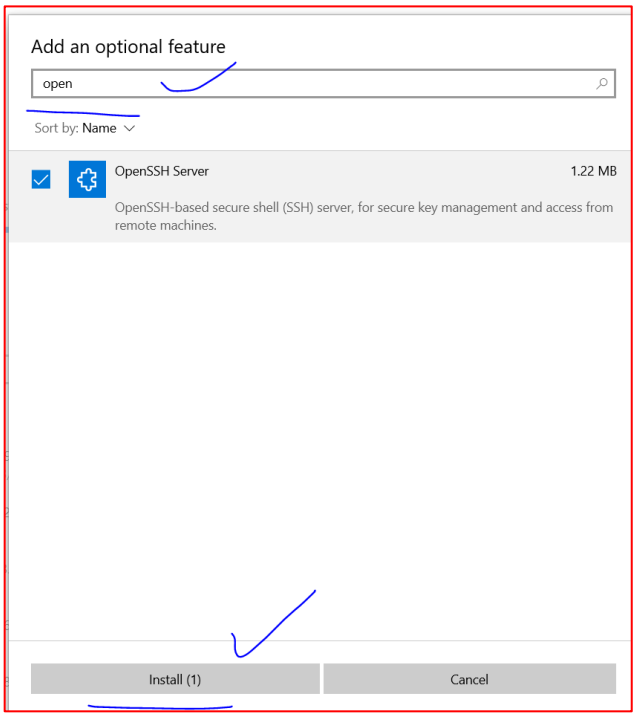
Go to the Apps and feature in Window setting (Server Window). Click on Optional Features:

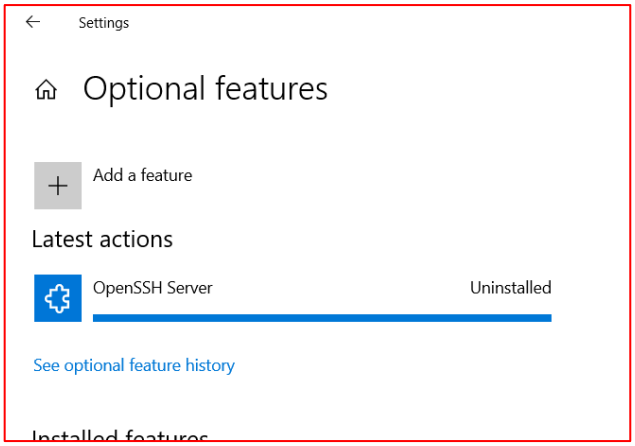


Click on Add a feature

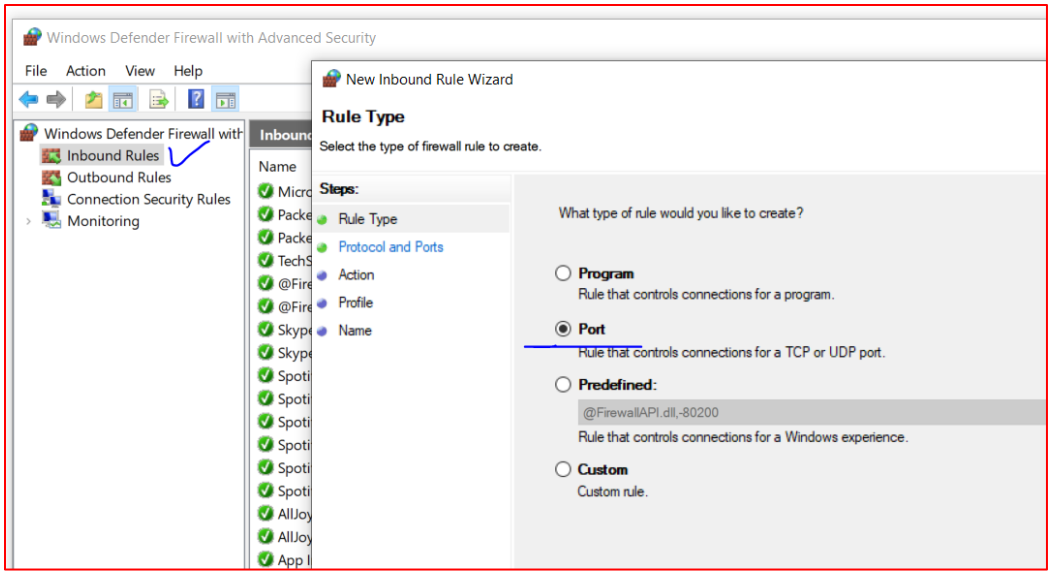


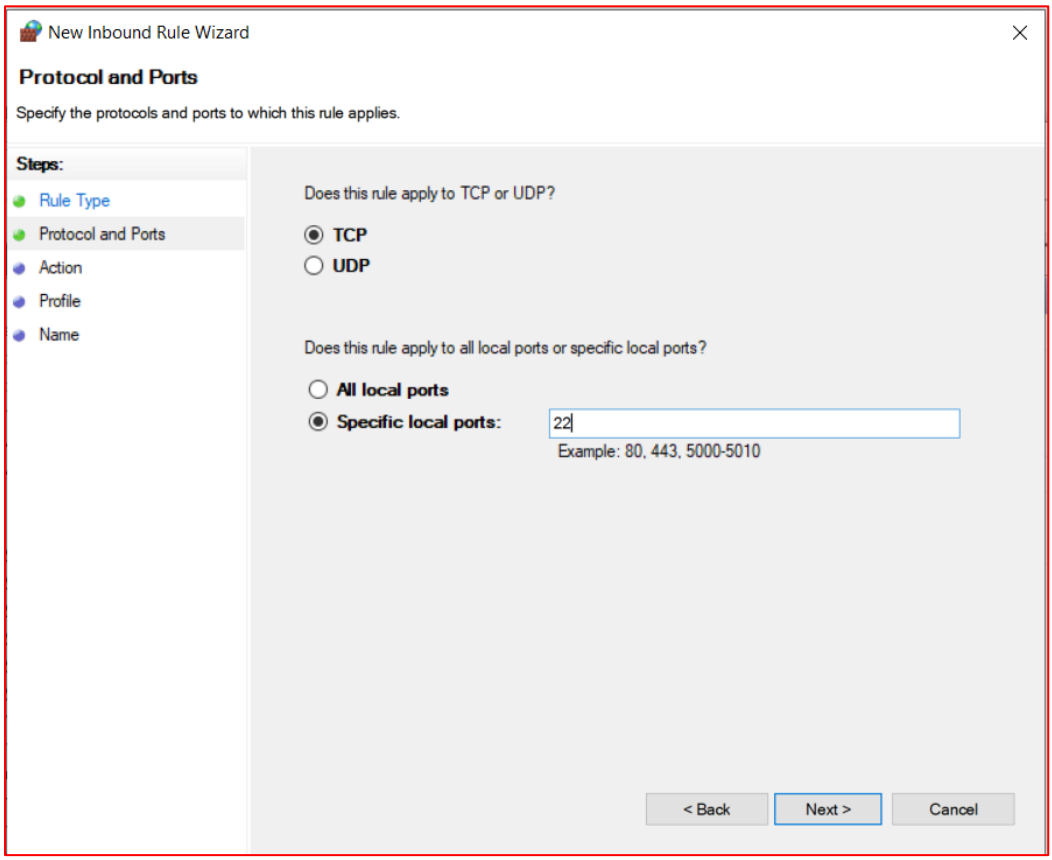
Search for Open SSH Server

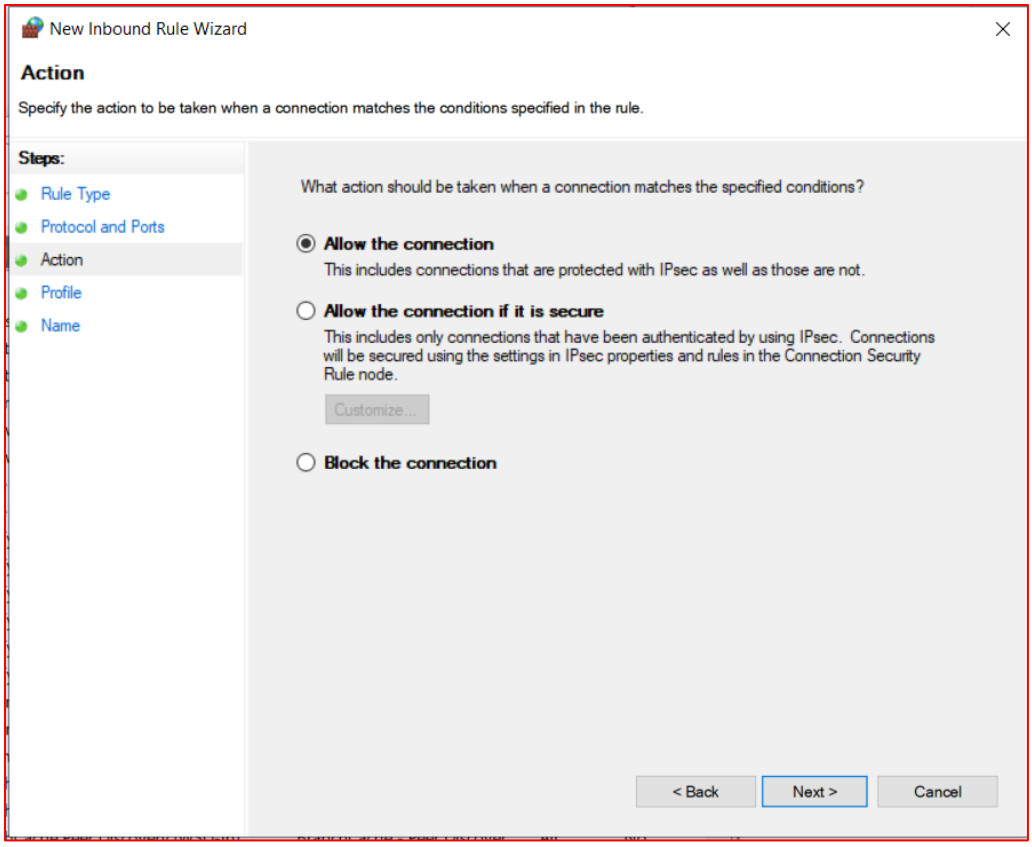


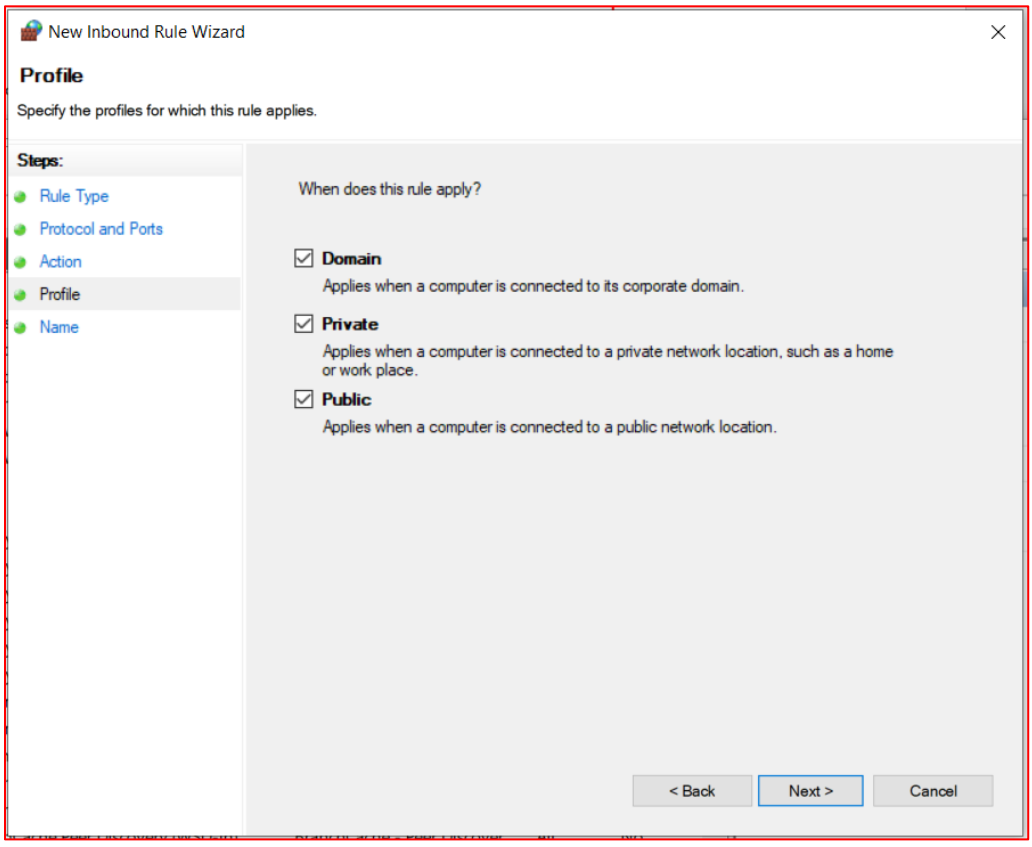


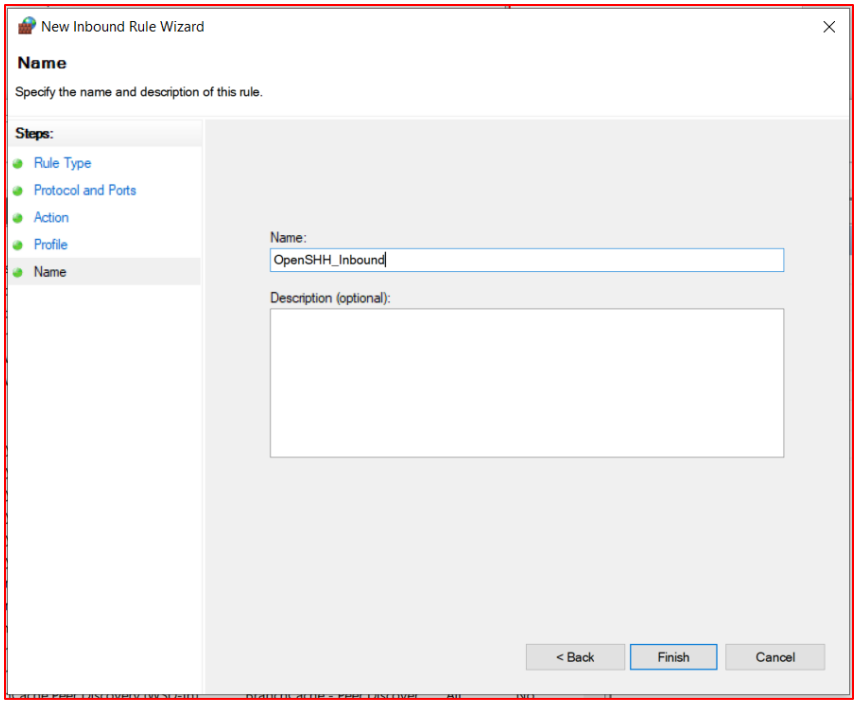
Add inbound rule for port 22 in firewall on Server Window. Follow the step , which are given below


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.
Custom
Custom rule.


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:
22
Example: 80, 443, 5000-5010
< Back
Next >
Cancel

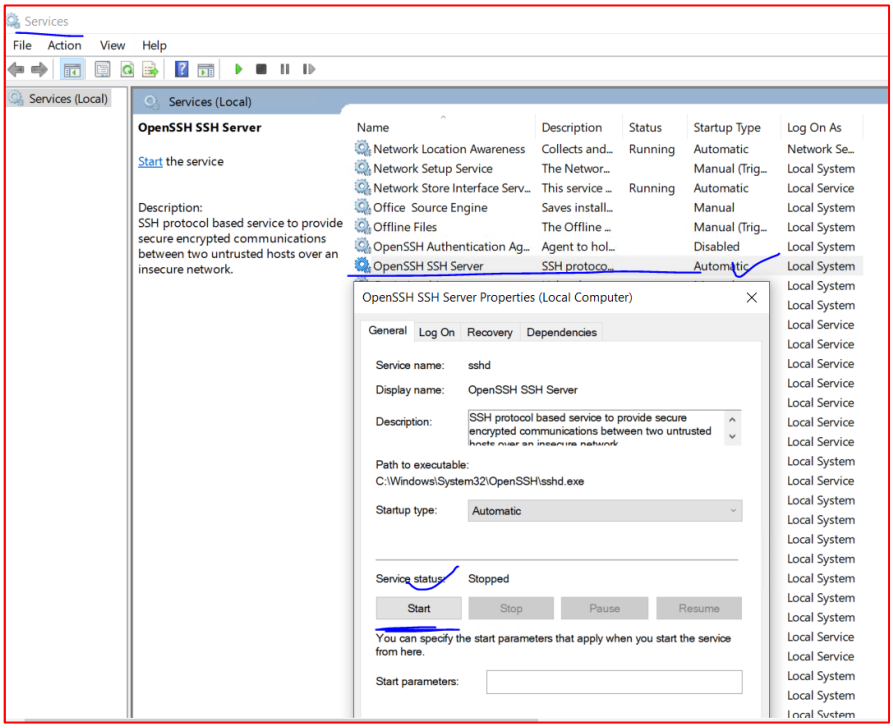

New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections 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



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.



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

Client OS (window /Linux etc.)

Now come toward Client OS, 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-4I1B6KO C:\Users\Admission-04>
```

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

```
admission-04@DESKTOP-4I1B6KO C:\Users\Admission-04>cd Desktop

admission-04@DESKTOP-4I1B6KO C:\Users\Admission-04\Desktop>echo hello testing SSH > testSSH.txt

admission-04@DESKTOP-4I1B6KO C:\Users\Admission-04\Desktop>
```

Echo hello testing SSH > testSSH.txt