

CA- C14L: COMPUTER NETWORK LAB
LAB MANUAL

CA- C14L: COMPUTER NETWORK LAB

PART – A

1. Execute the following commands:
Amp, ipconfig, hostname, netdiag, nerstat, nslookup, pathping, ping
route, tracert
2. Study of different types network of cables.
3. Practically implement the cross-wire cable and straight wired cable using crimping tool.
4. Study of network IP address configuration (Classification of address, static and dynamic address)
5. Study of network devices (switch, Router, Bridge)
6. Share the folder in a system and access the files of that folder from other system using IP address.

PART - B

1. Configure and connect the computer in LAN.
2. Block the website using “Windows Defender Firewall” in Windows 10.
3. Configuration the wifi hotspot, and connect other devices (mobile/laptop).
4. Configuration of switches.
5. Configuration of VLAN using Packet Tracer/GNS3.
6. Configuration of VPN using Packet Tracer/GNS3.

Reference:

Youtube.com/watch?v=rurs7cdT5cc

<https://www.youtube.com/watch?v= IOZ8 cPgu8>

<http://www.alphr.com/block-websites-windows/>

Youtube.com/watch?v=rurs7cdT5cc -

<https://youtu.be/kCf5sFnTB6U> - Configuration of VLAN using Packet Tracer/GNS3

<https://youtu.be/ya9R7yn23F0> - Basic Switch Configuration | Switch Basic Configuration | Cisco
Switch Assign IP Address

Experiment – 1: Execute the commands - netstat, nslookup, pathping, ping route, tracert,

Definitions & meanings of terms

ARP

Address Resolution Protocol (ARP) The Address Resolution Protocol is a layer 2 protocol used to map MAC addresses to IP addresses. All hosts on a network are located by their IP address, but NICs do not have IP addresses, they have MAC addresses. ARP is the protocol used to associate the IP address to a MAC address.

Ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

hostname

A host name is a unique name or label assigned to any device that is connected to a specific computer network. It facilitates the differentiation of different machines or devices connected to the Internet, a network and/or both.

Netdiag

The Netdiag command-line diagnostic tool helps to isolate networking and connectivity problems by performing a series of tests to determine the state of your network client.

Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

Nslookup

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name and find out the corresponding IP address or domain name system (DNS) record.

Pathping

This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router

Ping route

Ping is a simple command that can test the reachability of a device on the network. Traceroute is a command you use to 'trace' the route that a packet takes when traveling to its destination. It's useful for tracing network problems, discovering where connections fail, and tracking down latency problems.

Tracert

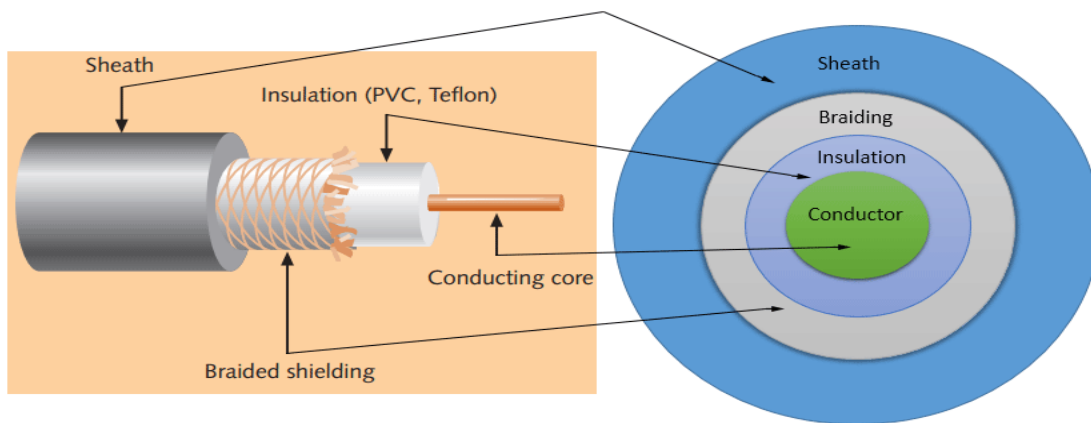
a command-line utility that you can use to trace the path that an Internet Protocol (IP) packet takes to its destination

Experiment – 2: Study of different types of network cables.

Network cables

In a computer network, to connect two or more computers or networking devices network cables are used. These cables are responsible for data transfer and also the propagation of signals for telecommunication.

1. **Coaxial Cables:** These cables contain a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.



- **Sheath** - The outer layer of the coaxial cable which protects the cable from physical damage.
- **Braided shield** - This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.
- **Insulation** - Insulation protects the core. It also keeps the core separate from the braided shield. Since both the core and the braided shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.
- **Conductor** - The conductor carries electromagnetic signals.

Coaxial cables have two types of transmission-

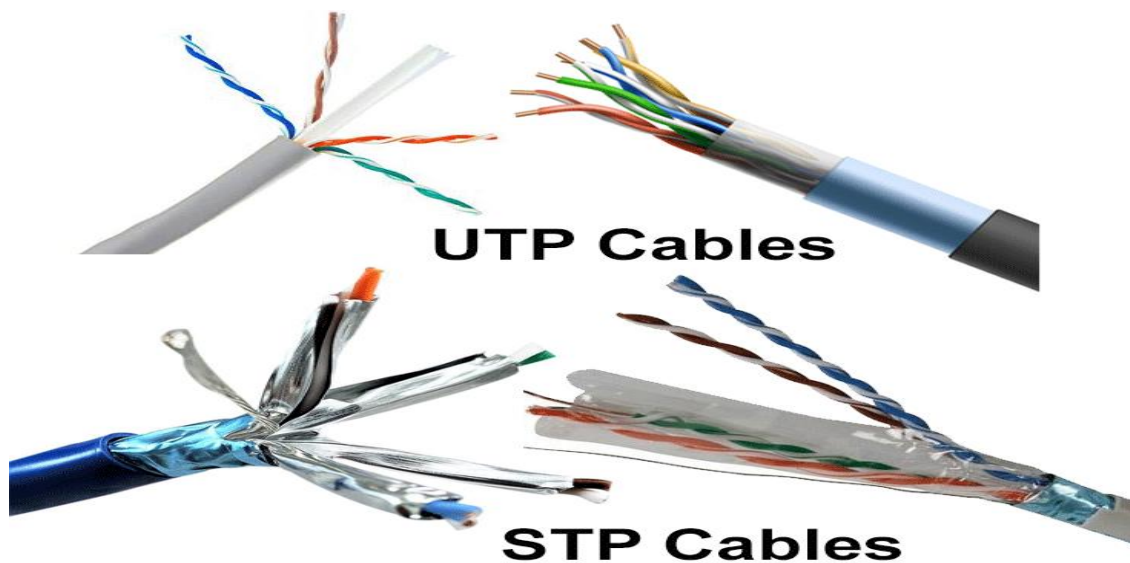
Baseband Transmission – It is the process of transmitting a single signal at high speed.

Broadband Transmission – It is the process of transmitting a multiple signals simultaneously.

Specifications of coaxial cables

Type	Ohms	AWG	Conductor	Description
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.
RG - Radio Guide to measure the materials used in shielding and conducting cores.				
Ohm - Impedance is the resistance that controls the signals. It is expressed in the ohms.				
AWG - AWG stands for American Wire Gauge. It is used to measure the size of the core.				

2. Twisted Pair Cables: The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable. This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.



STP (*Shielded twisted-pair*) cable - each pair is wrapped with an additional metal shield, and all pairs are wrapped in a single outer plastic sheath.

UTP (*Unshielded twisted-pair*) cable - all pairs are wrapped in a single plastic sheath.

Categories of twisted-pair cable.

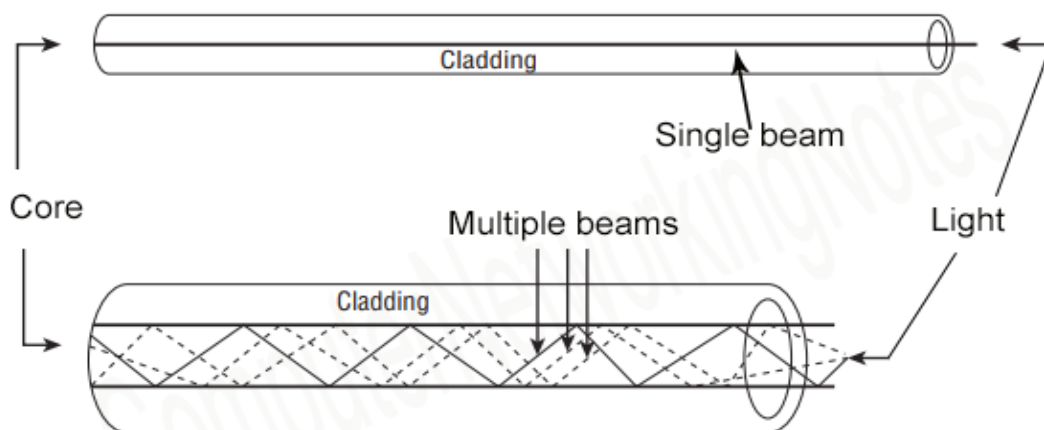
Category/name of cable	Maximum support speed	Bandwidth/support signals rate	Ethernet standard	Description
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.

Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pair and shields each pair by its plastic sheath.
Cat 1, 2, 3, 4, 5 are outdated and not used in any modern LAN network. Cat 7 is still a new technology and not commonly used. Cat 5e, 6, 6a are the commonly used twisted-pair cables.				

3. Fiber Optics Cables: This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance.



SMF (Single mode fiber) optical cable



MMF (multi-mode fiber) optical cable

The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket. Core carries the data signals in the form of light.

- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps. Fiber optic uses light to send data. It reflects light from one endpoint to another.

Step Index Fiber – consists of a core surrounded by the cladding which has a single uniform index of refraction.

Graded Index Fiber - The refractive index of the optical fiber decreases as the radial distance from the fiber axis increases.

Plastic Optical Fibers – Polymethylmethacrylate is used as a core material for the transmission of light.

Glass fibers – consists of fine glass fibers.

Single mode fiber – used for long-distance transmission of signals.

Multimode – use for short distance transmission of signals.

Experiment – 3: Practically implement the cross-wired cable and straight wired cable using crimp tool.

Components: RJ-45 connector, Crimping Tool, Twisted pair Cable

Procedure:

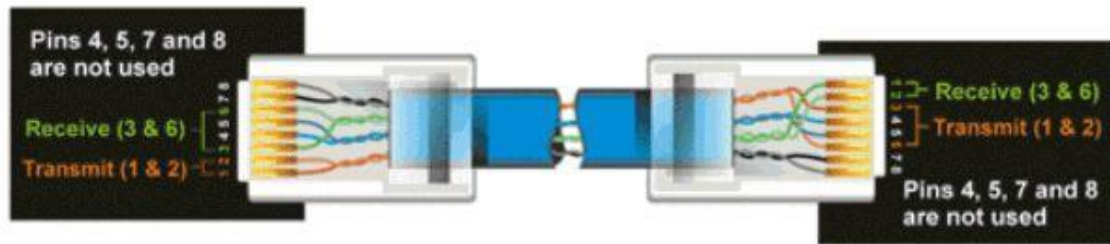
Step – 1: Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render it useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.

Step – 2: Spread the wires apart, Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.

Step – 3: You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end.

Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Diagram shows you how to prepare Cross wired connection



Pin number	Wire Color
Pin 1 ==>	Orange/White
Pin 2 ==>	Orange
Pin 3 ==>	Green/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Green
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Crossed-Over		
Wire		Becomes
1	→	3
2	→	6
3	→	1
6	→	2

Pin number	Wire Color
Pin 1 ==>	Green/White
Pin 2 ==>	Green
Pin 3 ==>	Orange/White
Pin 4 ==>	Blue
Pin 5 ==>	Blue/White
Pin 6 ==>	Orange
Pin 7 ==>	Brown/White
Pin 8 ==>	Brown

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

You Tube reference for Practical Session I Cross wired cable and straight through cable using clamping tool: <https://youtu.be/E5i8kRJXTw>

Experiment – 4: Study of network IP address configuration (Classification of address, static and dynamic address)

An IP address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication. IP address act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source.

IP address Full Form: Internet Protocol address

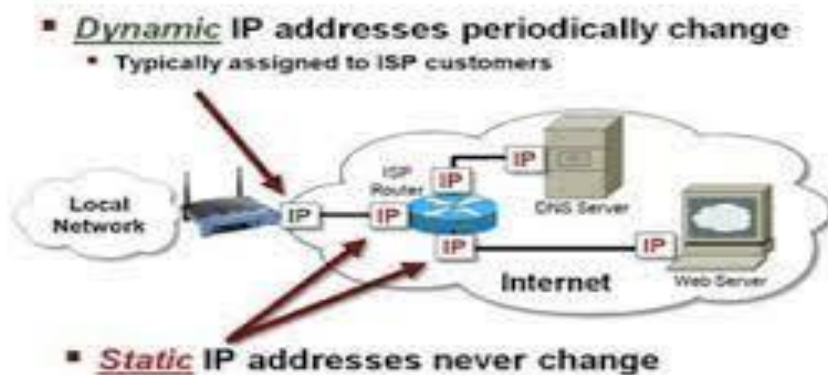
Classification of IP Address

TCP/IP defines five classes of IP addresses: Class A, B, C, D and E. Each class has a range of valid IP addresses.

Static IP address - it is also known as fixed or dedicated IP addresses which donot change. Once a device has been assigned a static IP address that number remains with the device as its internet identifier until the device is decommissioned or the network architecture is modified.

You can assign these static IP addresses on the device itself—using

- Windows' network settings on each computer
- or you can do it at the router level. If you do it through the router, it will likely be called a DHCP reservation.
- DHCP reservations allow you to easily set everything up in one place with all your computers left at their default settings.
- Your computer will ask for an IP address via DHCP, and your router will assign it the one you reserved, with your computer being none the wiser.



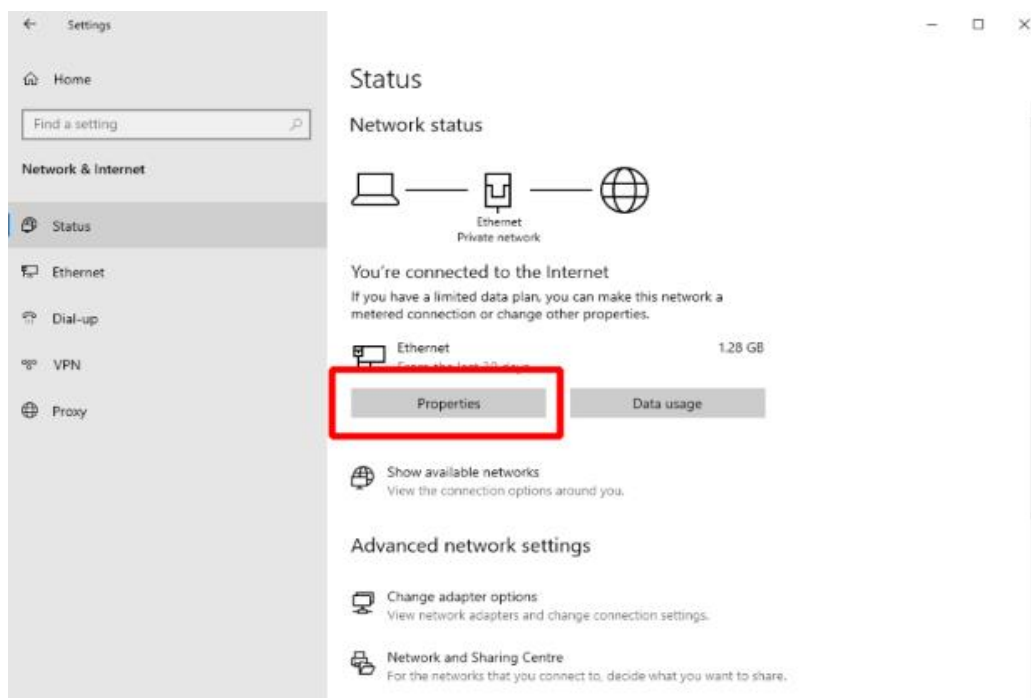
You tube link: <https://youtu.be/SOGaaGBwzxk>

How to set up a static IP address

You will need to contact your Internet Services Provider (ISP) for a static IP address. Once you receive this, setup is straightforward.

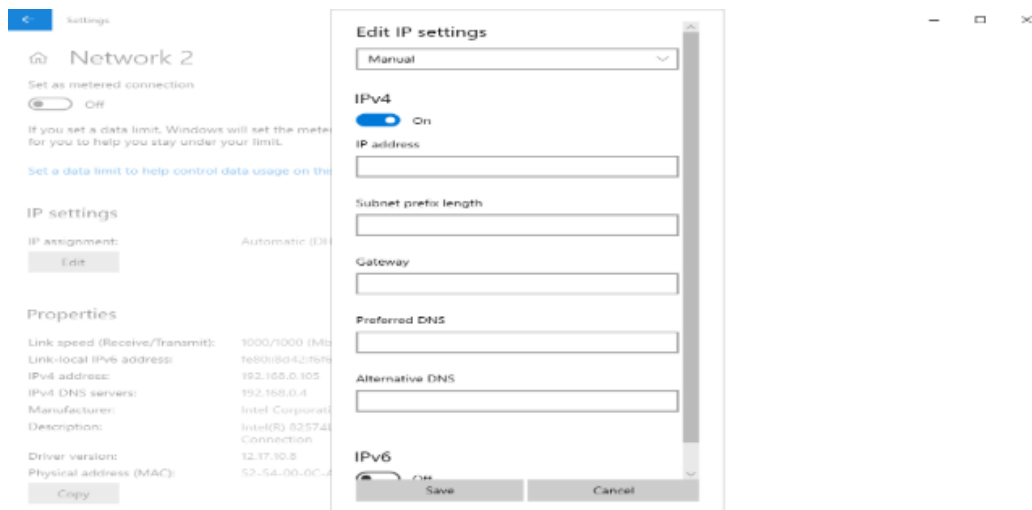
For Windows

- Open the **settings** app on your computer
- Choose **Network and Internet** option from the list on the left
- Select the connection you are using
- Find the IP assignment **manage known networks > properties > IP settings**



- Select **edit** under IP assignments
- Select **Manual** from the options
- Select **IPv4** and toggle to **on**

It's a simple process to switch to a static address, and for businesses and individuals with more complicated internet needs, it's a great decision.



- Enter the static IP address
- Enter **24** in the Subnet prefix length field
- Find your gateway and DNS by typing **ipconfig/all** into the command window
- Add the gateway information in the field
- Add the preferred DNS address and, if available, the alternate DNS address
- Remember to click save when you're finished

Dynamic IP address – it is an ever changing dynamic IP address, which is not permanently tied to a device. Dynamic IP addresses are used for a specific amount of time and then returned to an address pool so that other devices can use them. Dynamic IP addresses are the most common type of IP address; they are the default IP address type provided by internet service providers (ISPs). In addition, dynamic IP addresses are ideal for everyday internet users because they are easy to manage and don't require users to go through any additional setup or network configuration. An organization or home network should nearly always use a dynamic IP address.

Address Classes	RANGE	Bit Pattern of 1 st byte	Decimal Range	Default Subnet Mask	Reserved for
A	1.0.0.0 to 126.255.255.255	0xxxxxxx	1 to 127	255.0.0.0	Governments
B	128.0.0.0 to 191.255.255.255	10xxxxxx	128-191	255.255.0.0	Medium Companies
C	192.0.0.0 to 223.255.255.255	110xxxxx	192-223	255.255.255.0	Small Companies
D	224.0.0.0 to 239.255.255.255	1110xxxx	224-239	Not Applicable	Reserved for Multicasting
E	240.0.0.0 to 255.255.255.255	11110xxx	240-255	Not Applicable	Experimental or future use

Experiment – 5: Study of network devices (switch, Router, Hub, Bridge)

Network Devices: Physical devices that allow hardware on a computer network to communicate and interact with one another.

Hub: An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

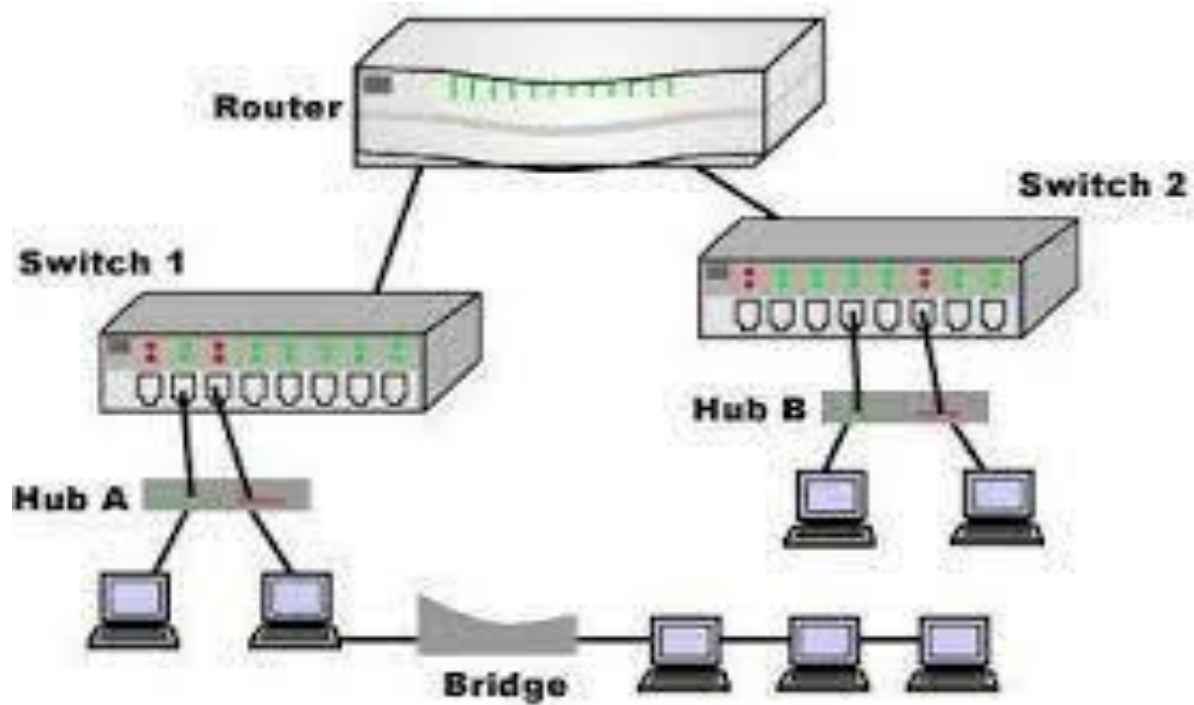
Switch: A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

Bridge: A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

Router: A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

Gate Way: In a communications network, a network node equipped for interfacing with another network that uses different protocols.

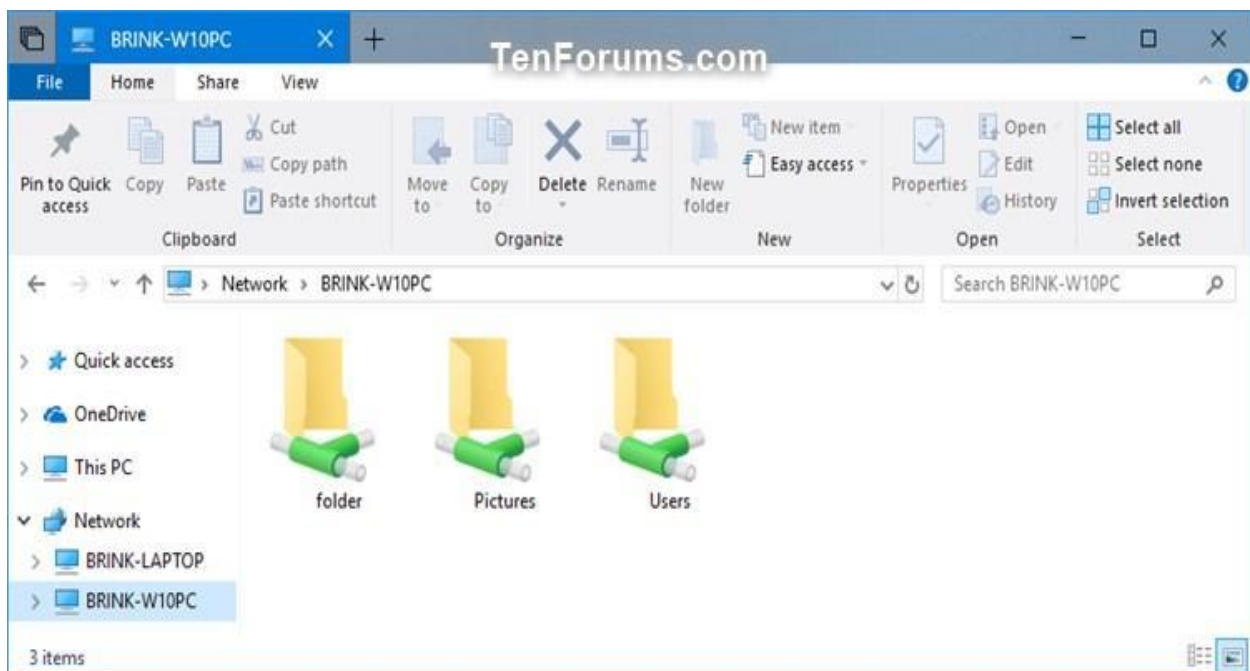
- A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
- A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

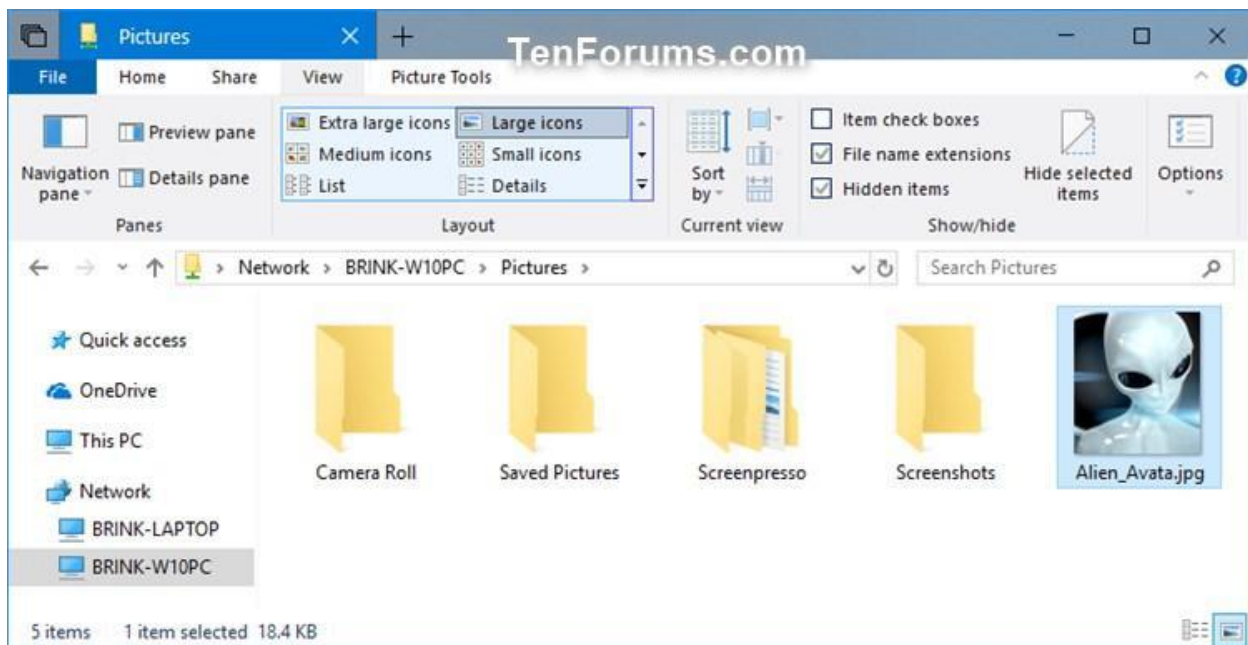


Experiment – 6: Share the folder in a system and access the files of that folder from other system using IP address.

Windows 10

- Set Up File Sharing on a Windows PC
- Share File or Folder using "Give access to" Context Menu
- Stop Sharing File or Folder using "Give access to" Context Menu
- Share File or Folder using Share tab in File Explorer
- Stop Sharing File or Folder using Share tab in File Explorer
- Share Folder using Sharing Properties
- Share Folder or Drive using Advanced Sharing
- Stop Sharing Folder or Drive using Advanced Sharing
- Share Folder or Drive using Shared Folder Wizard
- Stop Sharing Folder or Drive using Shared Folders MMC Snap-in





PART – B

Practical – 1: Configure and connect the computer in LAN.

There are two ways to configure and connect the computers in LAN depending on Operating SYSTEM, they are

1. Using wired connection
2. Using wireless connection

Procedure: On the host computer

Step -1: Log on to the host computer as Administrator or as Owner.

Step -2: Click Start, and then click Control Panel.

Step -3: Click Network and Internet Connections.

Step -4: Click Network Connections.

Step -5: Right-click the connection that you use to connect to the Internet.

Step -6: Click Properties.

Step -7: Click the Advanced tab.

Step -8: Under Internet Connection Sharing, select the Allow other network users to connect through this computer's Internet connection check box.

Step -9: If you are sharing a dial-up Internet connection, select the Establish a dial-up connection whenever a computer on my network attempts to access the Internet check box if you want to permit your computer to automatically connect to the Internet

Step -10: Click OK. You receive the following message:

When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

Step -10: Click Yes.

The connection to the Internet is shared to other computers on the local area network (LAN).

The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

On the client computer

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client computer.

Step – 1: Log on to the client computer as Administrator or as Owner.

Step – 2: Click Start, and then click Control Panel.

Step – 3: Click Network and Internet Connections.

Step – 4: Click Network Connections.

Step – 5 Right-click Local Area Connection and then click Properties.

Step – 6: Click the General tab, click Internet Protocol (TCP/IP) in the connection uses the following items list, and then click Properties.

Step – 7: In the Internet Protocol (TCP/IP) Properties dialog box, click Obtain an IP address automatically (if it is not already selected), and then click OK. Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. you can assign the following static IP address, subnet mask, and default gateway:

- IP Address: 192.168.31.202 9.

- Subnet mask: 255.255.255.0 10.

- Default gateway: 192.168.31.1 11.

In the Local Area Connection Properties dialog box and click OK.

Step – 8: Quit Control Panel.

Practical – 2: Block the website using “windows Defender Firewall” in Windows 10.

Windows Defender Firewall: helps and protects from unauthorized access.

Blocking the Websites on a Windows 10 PC with the Hosts File

Method – 1:

Step-1: Click on the Start menu and select “Windows Accessories.”

Step-2: Right-click on Notepad, select “More” followed by “Run as administrator.”

Step-3: When the Notepad opens, select “File” from the toolbar and “Open” from the drop-down menu.

Step-4: Go the “C:\Windows\System32\Drivers\etc” location.

Step-5: Make sure to select the “All files” option for the files to appear. Then open the “host” file.

Step-6: Scroll to the bottom of the page and click on the last line. Make sure to create space.

Step-7: Enter the URL you want to block.

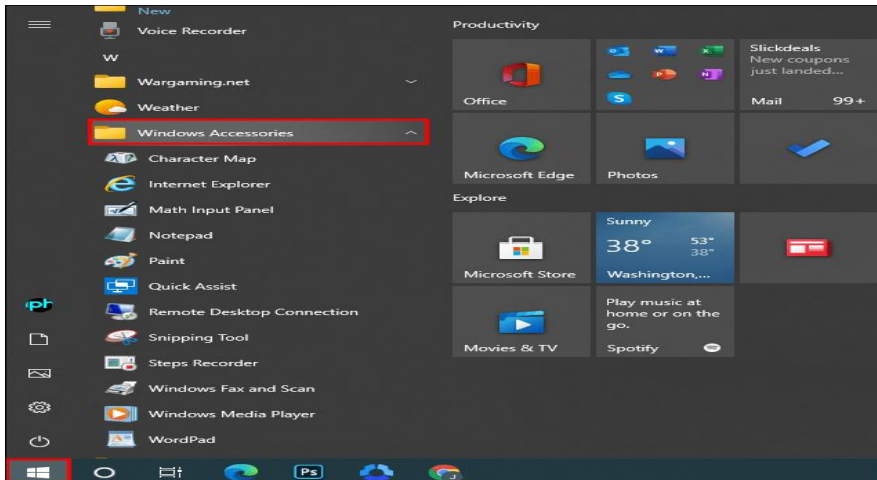
Step-8: Go to File and select “Save.”

Method – 2:

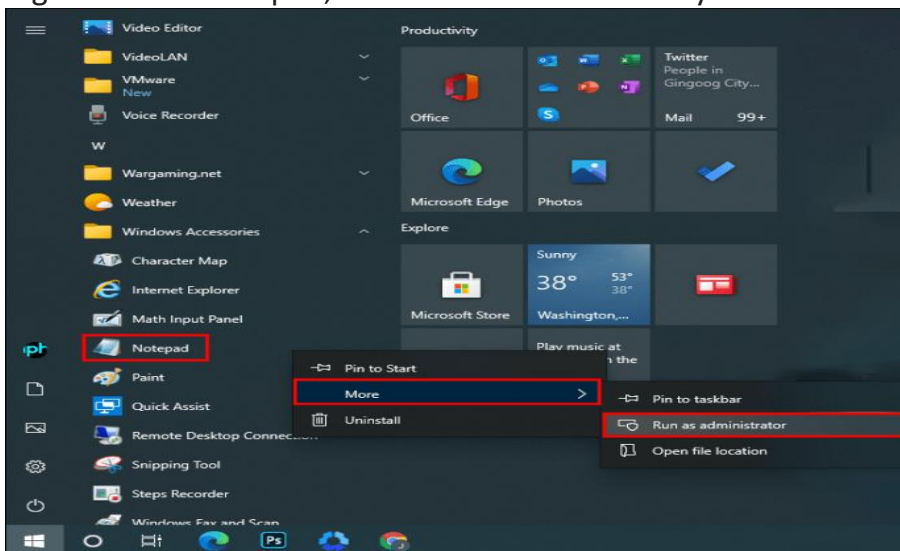
1. Launch the Control Panel on your computer.
2. Select “Windows Defender Firewall” followed by “Advanced Settings” on the left-side pane.
3. Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”
4. When a new window pops up, select the “Custom” option followed by “Next.”
5. On the next window, select “All programs” and again select “Next.”
6. Select ” These IP addresses ” option under “Which remote IP addresses does this rule apply to?”
7. Click on “Add” and enter the IP addresses you want to block. Then select “Next.”
8. Make sure to choose the “Block the connection” option and click on “Next.”
9. Choose whether the rule applies to Domain, Private, or Public. You can also select all three.
10. Select “Next,” add a name or description for this rule, and select “Finish” to complete the action.

The process is straightforward, and the steps are as follows:

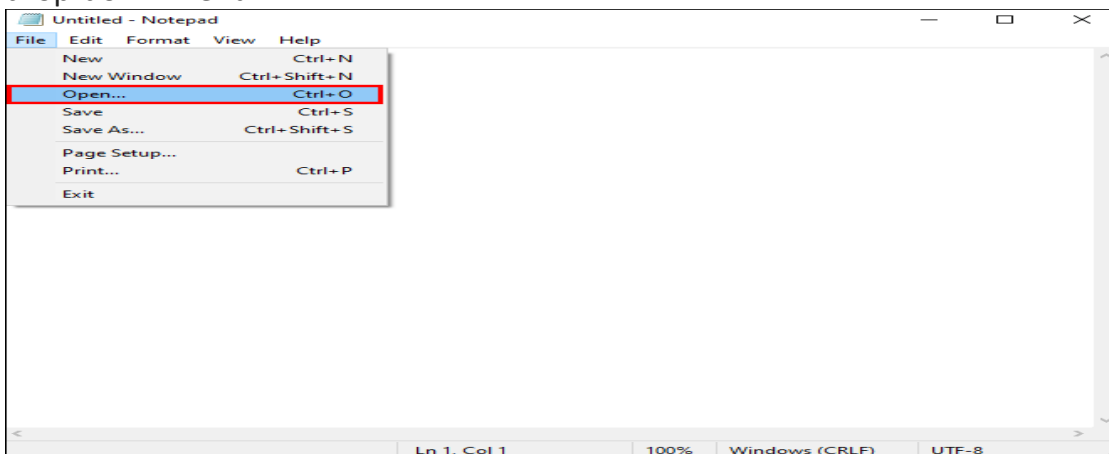
1. Click on the Start menu and select "Windows Accessories."



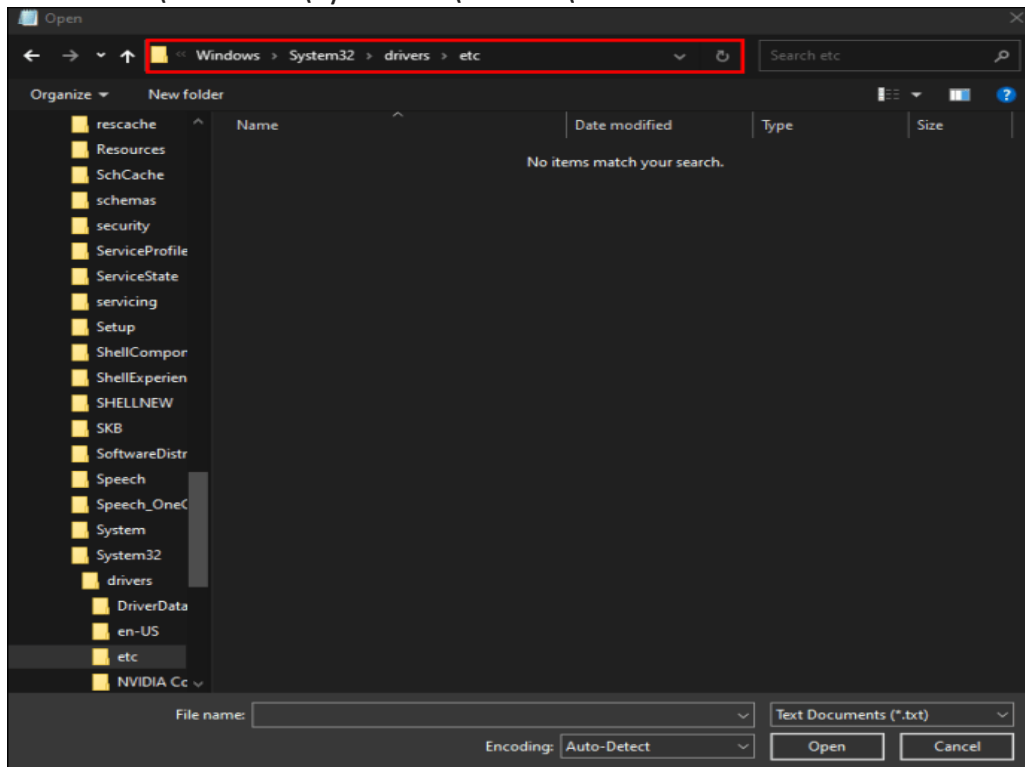
2. Right-click on Notepad, select "More" followed by "Run as administrator."



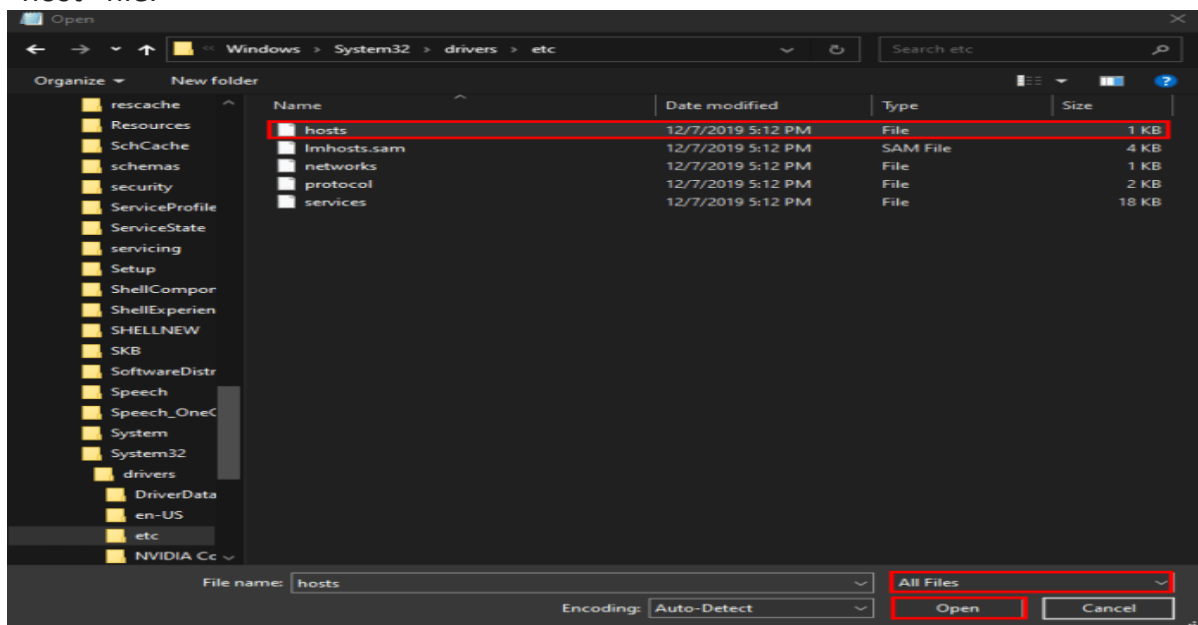
3. When the Notepad opens, select "File" from the toolbar and "Open" from the drop-down menu.



4. Go the “C:\Windows\System32\Drivers\etc” location.

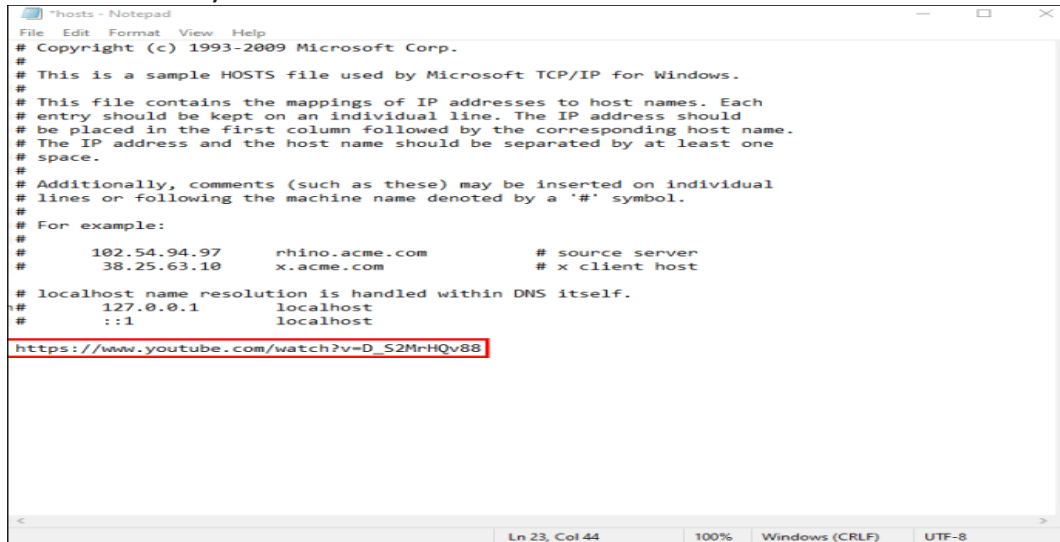


5. Make sure to select the “All files” option for the files to appear. Then open the “host” file.



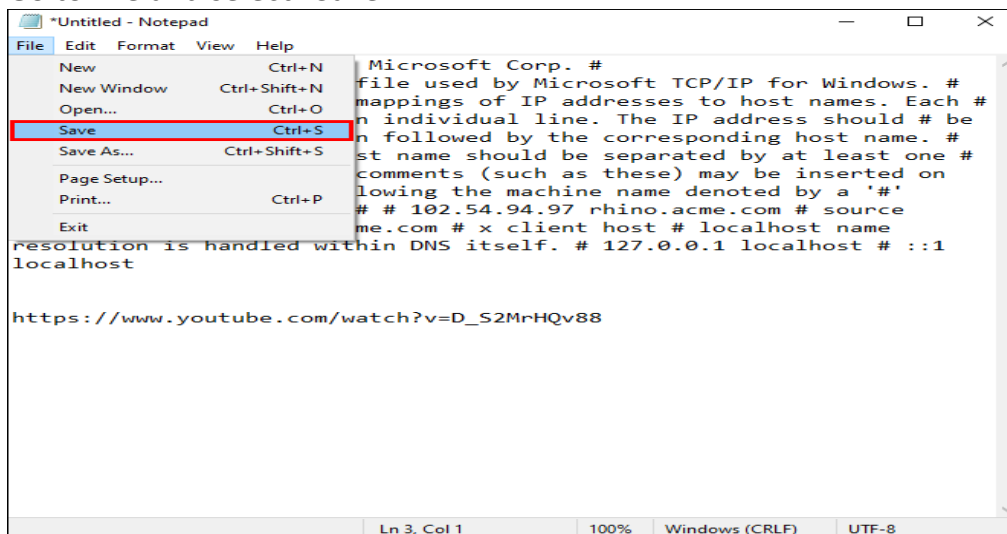
6. Scroll to the bottom of the page and click on the last line. Make sure to create space.

7. Enter the URL you want to block.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com        # source server
#       38.25.63.10       x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#
#       ::1               localhost
#
https://www.youtube.com/watch?v=D_S2MrHQv88
```

8. Go to File and select "Save."



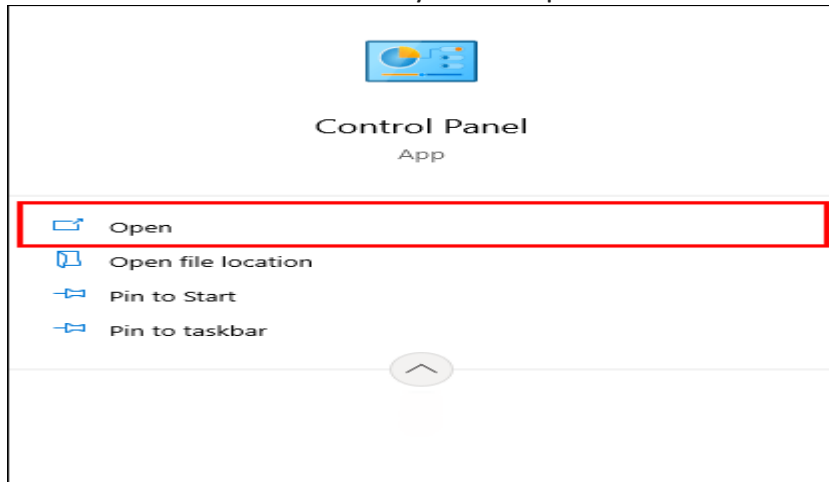
```
Microsoft Corp. #
file used by Microsoft TCP/IP for Windows. #
mappings of IP addresses to host names. Each #
n individual line. The IP address should # be
n followed by the corresponding host name. #
st name should be separated by at least one #
omments (such as these) may be inserted on
llowing the machine name denoted by a '#'
# # 102.54.94.97 rhino.acme.com # source
me.com # x client host # localhost name
resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1
localhost

https://www.youtube.com/watch?v=D_S2MrHQv88
```

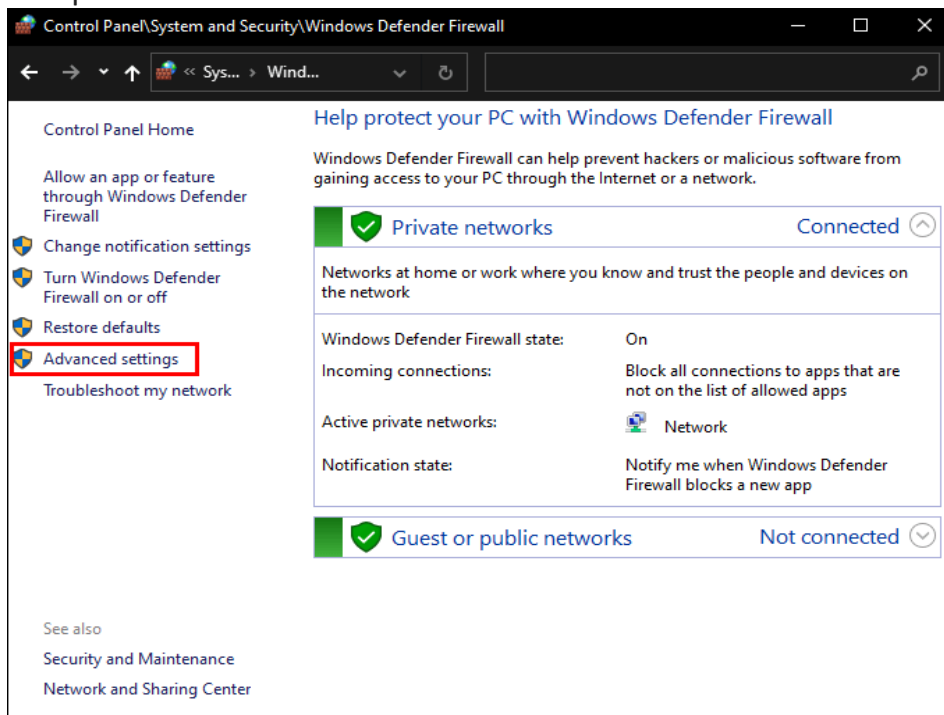
For this to work, you must have permission to access the host file. Also, make sure to restart your computer to ensure the website is blocked.

If the firewall permits access to questionable sites, you can set it up so no one in your home, school, or work opens it either. Here's how it works:

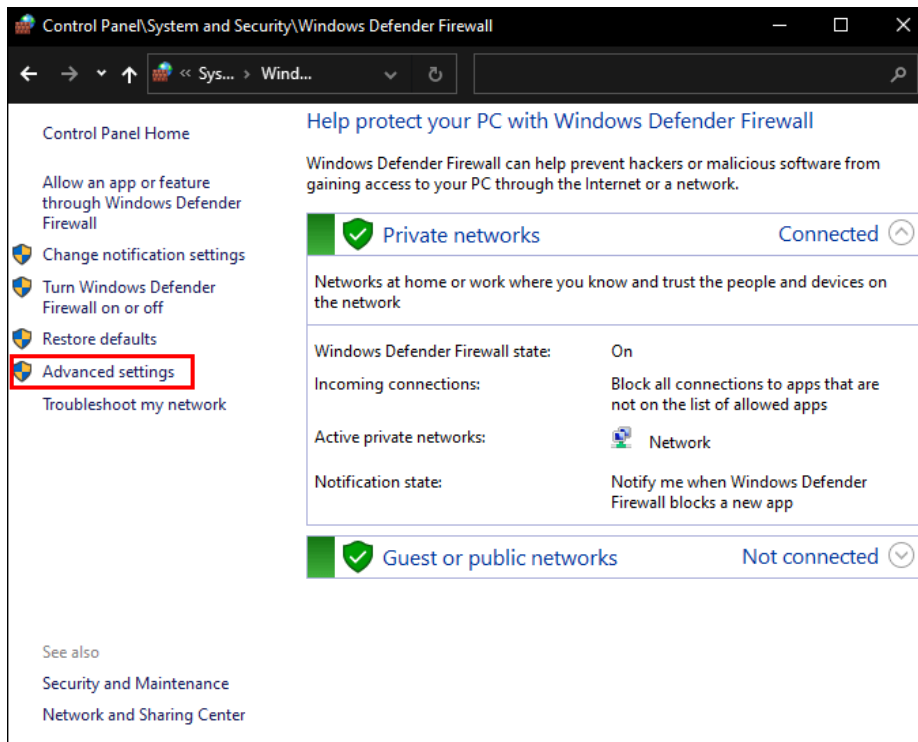
11. Launch the Control Panel on your computer.



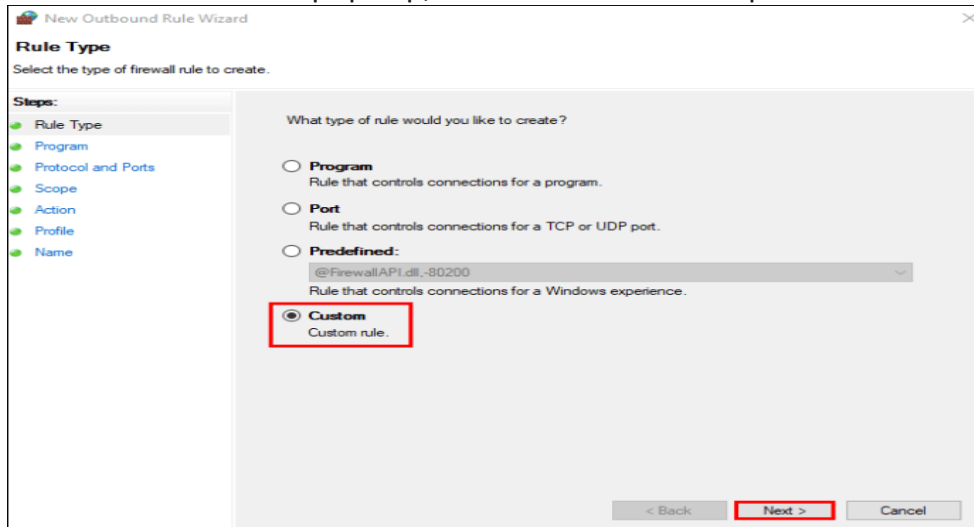
12. Select “Windows Defender Firewall” followed by “Advanced Settings” on the left-side pane.



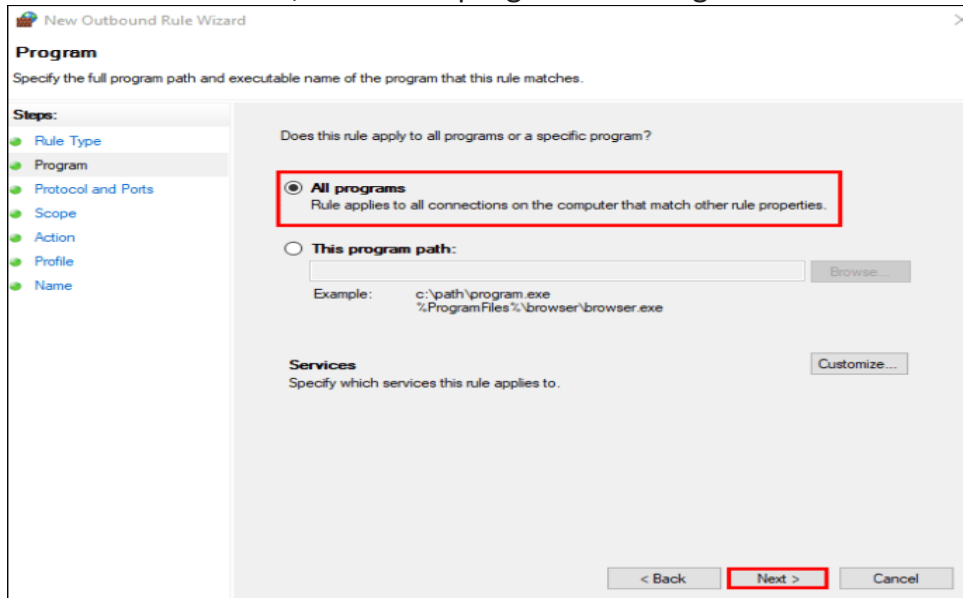
13. Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”



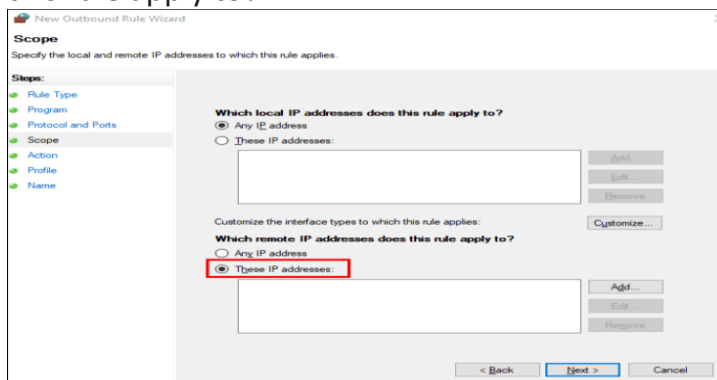
14. When a new window pops up, select the “Custom” option followed by “Next.”



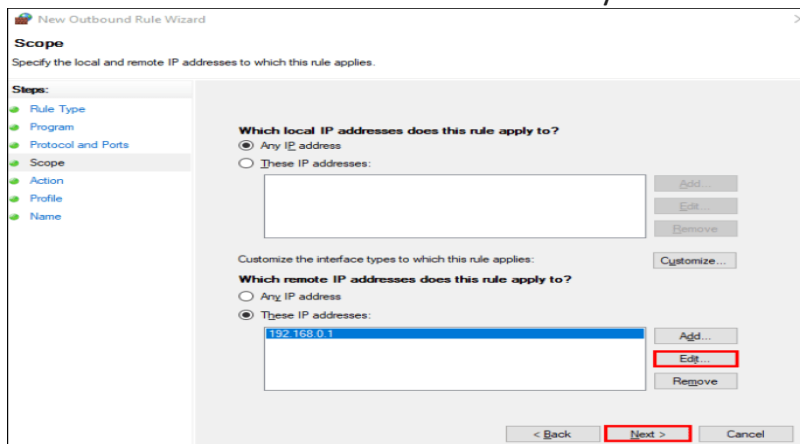
15. On the next window, select “All programs” and again select “Next.”



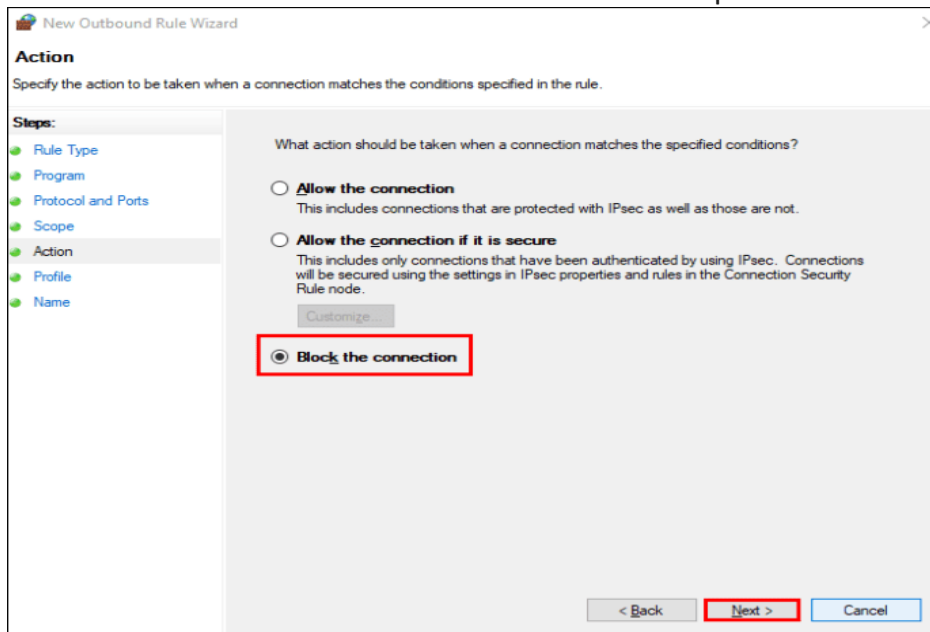
16. Select the “These IP addresses” option under “Which remote IP addresses does this rule apply to?”



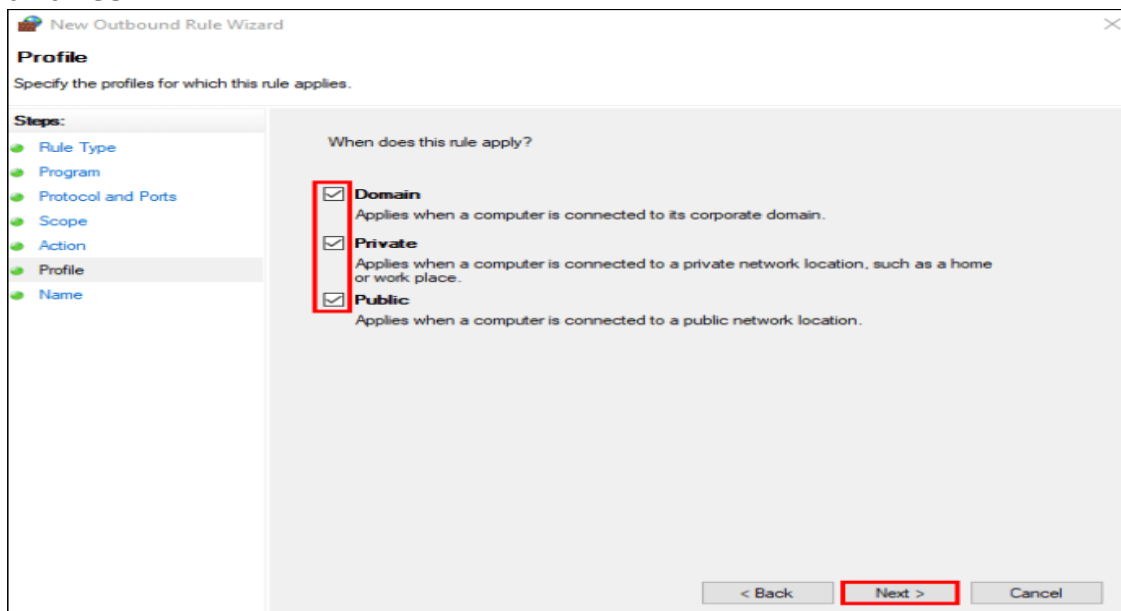
17. Click on “Add” and enter the IP addresses you want to block. Then select “Next.”



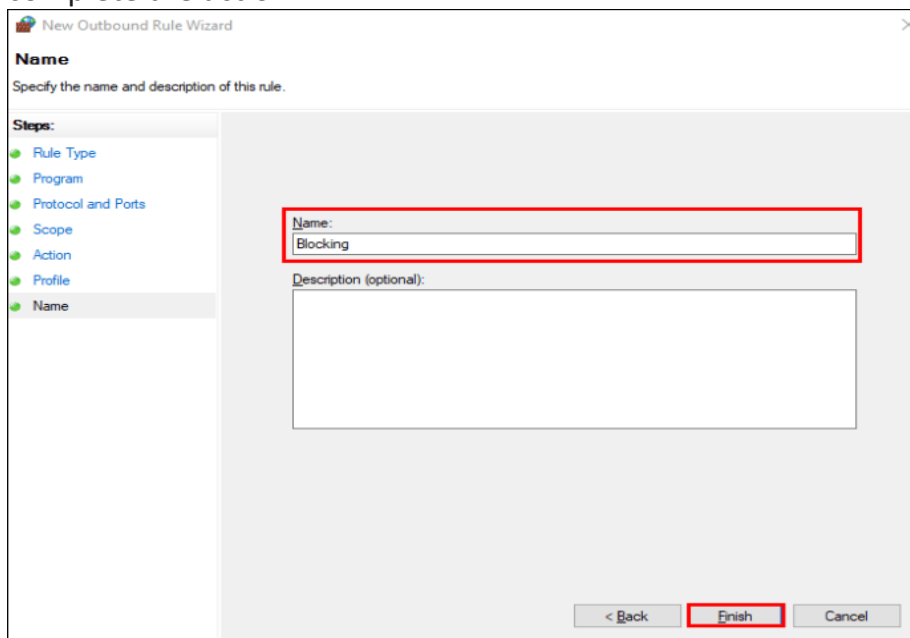
18. Make sure to choose the “Block the connection” option and click on “Next.”



19. Choose whether the rule applies to Domain, Private, or Public. You can also select all three.



20. Select “Next,” add a name or description for this rule, and select “Finish” to complete the action.



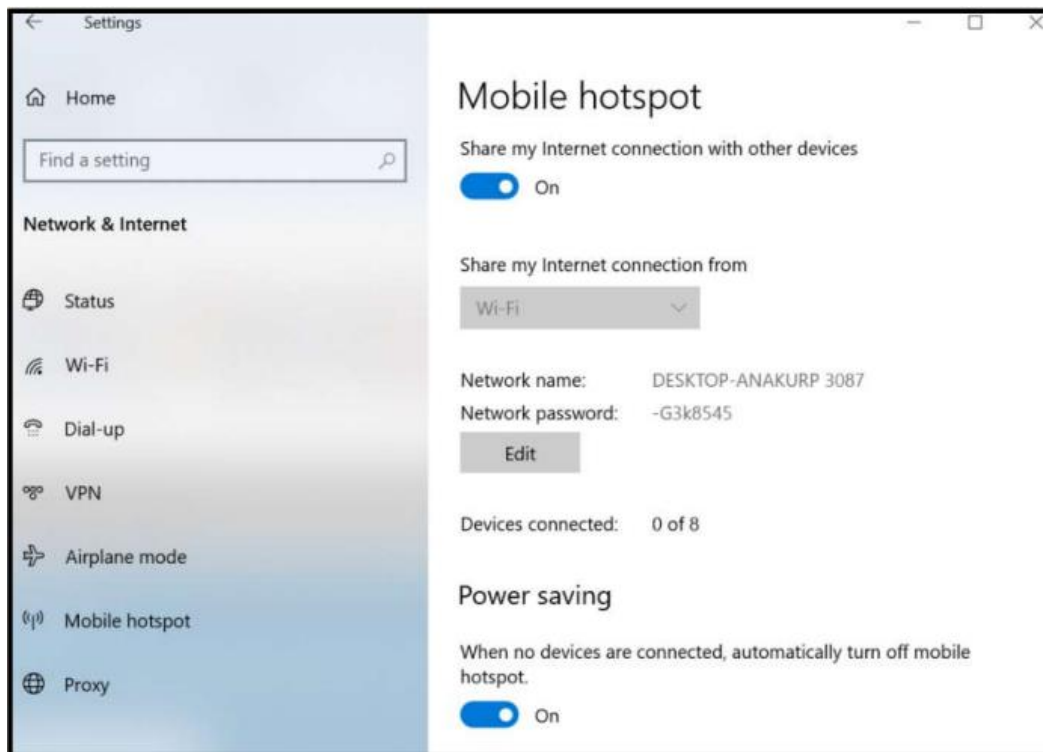
The image shows a screenshot of the 'New Outbound Rule Wizard' window, specifically the 'Name' step. The window title is 'New Outbound Rule Wizard'. The main heading is 'Name', and the instruction is 'Specify the name and description of this rule.' On the left, a 'Steps:' list shows the progression: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name (which is currently selected). The main area contains a 'Name:' text box with the word 'Blocking' entered, and a larger 'Description (optional):' text box below it. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red rectangle, indicating it should be clicked to complete the action.

Practical – 3: Configuration the wifi hotspot, and connect other devices (mobile/laptop).

1. PC as a mobile hotspot

Turn your Windows 10 PC into a mobile hotspot by sharing your Internet connection with other devices over Wi-Fi. You can share a Wi-Fi, Ethernet, or cellular data connection. If your PC has a cellular data connection and you share it, it will use data from your data plan.

1. Select **Start** , then select **Settings** > **Network & Internet** > **Mobile hotspot**.
2. For **Share my Internet connection from**, choose the Internet connection you want to share.
3. If desired, select **Edit** > enter a new network name and password > **Save**.
4. Turn on **Share my Internet connection with other devices**.
5. To connect on the other device, go to the Wi-Fi settings on that device, find your network name, select it, enter the password, and then connect.



2. Working with mobile hotspot

Activate Mobile Hotspot

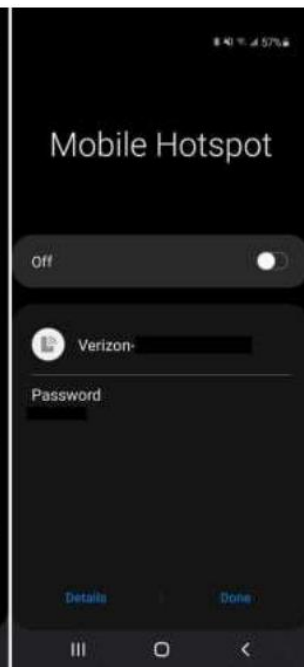
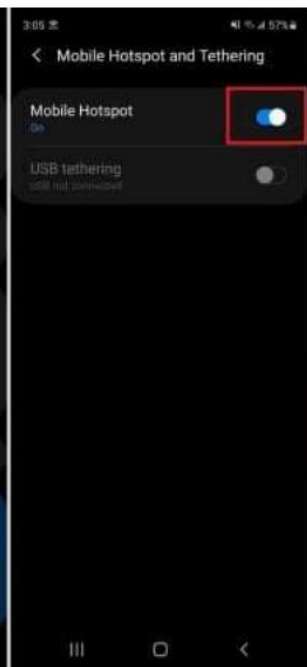
A Mobile Hotspot allows you to share your phone's mobile data connection with other devices. Follow the steps below to enable a Mobile Hotspot to share your internet connection with other devices.

Step 1. Launch the **Settings** app, and then select **Connections**.

Step 2. Tap **Mobile Hotspot and Tethering**.

Step 3. Tap the switch next to **Mobile Hotspot** to activate. The **Mobile Hotspot** icon appears on the status bar.

Step3. On the other device's screen, search for and select your phone from the Wi-Fi networks list.



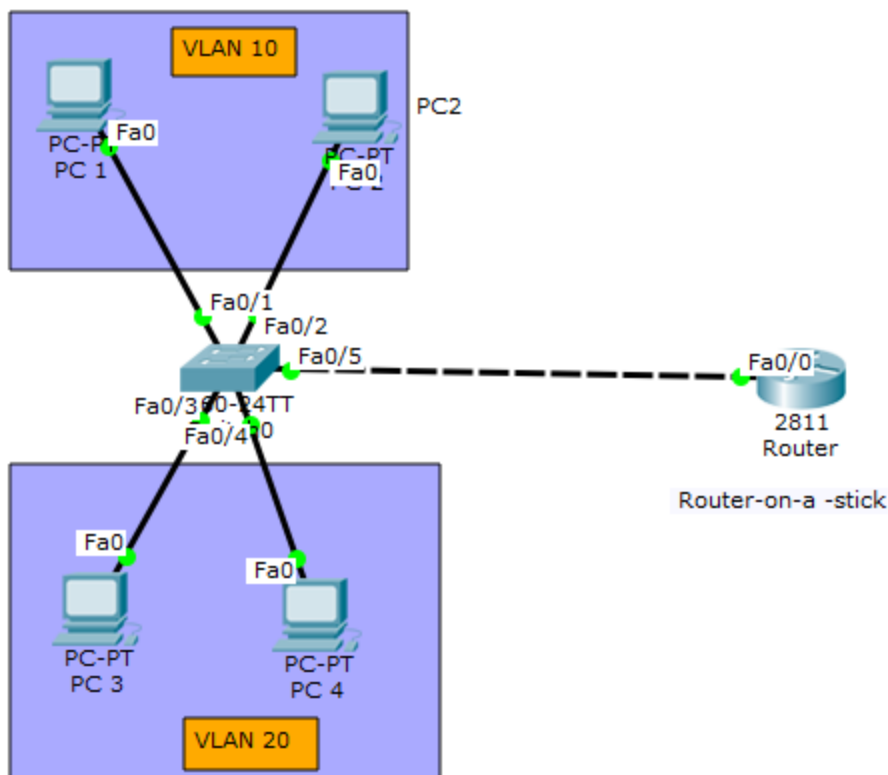
Practical – 3: Configuration of VLAN using Packet Tracer/GNS3.

Practical – 4: Configuration of VPN using Packet Tracer/GNS3.

Steps:

1. configure terminal. Enter global configuration mode.
2. interface vlan vlan-id. Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. ...
3. ip address { ip-address subnet-mask | dhcp } Configure the IP address.
4. exit. ...
5. show interfaces vlan vlan-id. ...
6. copy running-config startup-config.

1. In Cisco Packet Tracer, **create the network topology** as shown below:



2. Create 2 VLANs on the switch: **VLAN 10** and **VLAN 20**. You can give them custom names.

```
Switch#config terminal
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name SALES
```

```
Switch(config-vlan)#vlan 20
```

```
Switch(config-vlan)#name IT
```

3. Assign switch ports to the VLANs. Remember each VLAN is viewed as separate broadcast domain.

And just before you configure, have in mind that switch ports could be either [access](#) or [trunk](#).

- An [access port](#) is assigned to a single VLAN . These ports are configured for switch ports that connect to devices with a normal network card, for example a PC in a network.
- A [trunk port](#) on the other hand is a port that can be connected to another switch or router. This port can carry traffic of multiple VLANs.

So in our case, we'll configure switch interfaces **fa 0/1** through **fa 0/4** as access ports to connect to our PCs. Here, interfaces **fa 0/1** and **fa 0/2** are assigned to **VLAN 10** while interfaces **fa 0/3** and **fa 0/4** are assigned to **VLAN 20**.

Switch *Interface* **fa0/5** will be configured as trunk port, as it will be used to carry traffic between the two VLANs via the router.

```
Switch>enable
```

```
Switch#config terminal
```

```
Switch(config)#int fa0/1
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 10
```

```
Switch(config-if)#int fa0/2
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 10
```

```
Switch(config-if)#int fa0/3
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 20
```

```
Switch(config-if)#int fa0/4
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 20
```

Worth noting: We could have configured all the above interfaces as access ports using *interface range* command as shown below:

```
Switch(config-if)#int range fa0/1-4
```

```
Switch(config-if-range)#switchport mode access
```

In the above commands, we have specified an interface range and then proceeded to configure all the ports specified as access ports.

Interface **fa0/5** is configured as *trunk* and will be used to for inter-VLAN communication.

```
Switch(config)#int fa 0/5
```

```
Switch(config-if)#switchport mode trunk
```

The next thing is to:

4 . Assign static IP addresses to the four PCs which are located in the separate VLANs. PC1 and PC2 fall in VLAN 10 while PC3 and PC4 fall in VLAN 20.

PC1 IP address 192.168.1.10 Subnet mask 255.255.255.0 Default gateway 192.168.1.1

PC2: IP address 192.168.1.20 Subnet mask 255.255.255.0 Default gateway 192.168.1.1

PC3: IP address 192.168.2.10 Subnet mask 255.255.255.0 Default gateway 192.168.2.1

PC4: IP address 192.168.2.20 Subnet mask 255.255.255.0 Default gateway 192.168.2.1

And now it's very clear that we treat a VLAN just like a physical LAN when assigning IP addresses.

At this point let's try to test connectivity **within** VLANs and **between** VLANs

To test communication between hosts in the same VLAN:

Ping PC2 from PC1 both in VLAN 10. Ping test should be successful.

To test connectivity between hosts in different VLANs:

Ping PC3 in VLAN 20 from PC1 in VLAN 10. Ping here will definitely fail. Why? Because **inter-VLAN routing** is not yet enabled. Hope you can see how we've used VLANs to place the hosts into two logical networks which can be viewed as separate broadcast domains.

Now, in order to allow the hosts in the two VLANs to communicate, we need to do something extra. And you can guess what. We'll configure the router to permit inter-VLAN communication. Let's do that right away.

5. Configure **inter-VLAN routing** on the router

We'll configure the router so that it will enable communication between the two vlans via a single physical interface. How is this made possible? We'll divide the single physical interface on the router into logical interfaces (sub interfaces). Each sub-interface will then serve as a default gateway for each of the VLANs. This scenario is called **router on a stick** (R.O.A.S) and will allow the VLANs to communicate through the single physical interface.

Wort noting: We **can't** assign an IP address to the router's physical interface that we have subdivided into logical sub-interfaces. We'll instead assign IP addresses to the sub interfaces.

So let's do router configurations:

```
Router>enable
```

```
Router#config terminal
```

```
Router(config)#int fa0/0
```

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

```
Router(config-if)#int fa0/0.10
```

```
Router(config-subif)#encapsulation dot1q 10
```

```
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
```

```
Router(config-subif)#
```

```
Router(config-subif)#int fa0/0.20
```

```
Router(config-subif)#encapsulation dot1q 20
```

```
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
```

As you can notice from above, the routers physical interface **fa0/0** was subdivided into two sub-interfaces(**fa0/0.10** and **fa0/0.20**) , which are then configured as *trunk* interfaces and given IP addresses.

Finally,

6. Test **inter-VLAN** connectivity.

Here we'll test connectivity between computers in different VLANs . Don't forget that its the router that enables inter-VLAN routing.

Ping PC3 in **VLAN 20** from PC1 in **VLAN 10**. If everything is well configured, then ping should work perfectly.