PNS SCHOOL OF ENGINEERING & TECHNOLOGY

Nishamani Vihar, Marshaghai, Kendrapara

LAB MANUAL

ON

NETWORKING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

4TH SEMESTER

PREPARED BY

Er. BALARAM DAS

LECTURER IN COMPUTER SCIENCE & ENGINEERING

# EXPERIMENT- 1
Aim of The Experiment:

Study about Network Topology

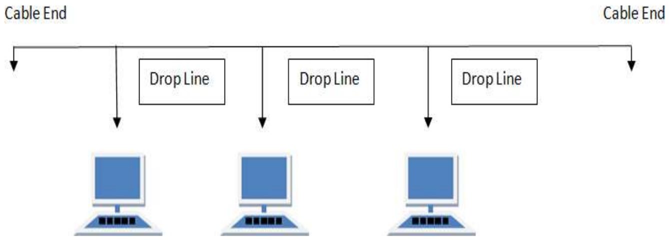
Resource Required-
PC with Windows OS and NIC.

Topology: -

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to another network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand by joining two cables together.

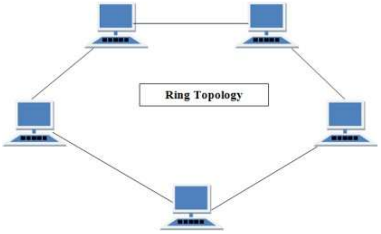
Disadvantages of Bus Topology

1. Cables fail, then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

Features of Ring Topology



1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.

3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner, that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1. Transmitting networks are not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

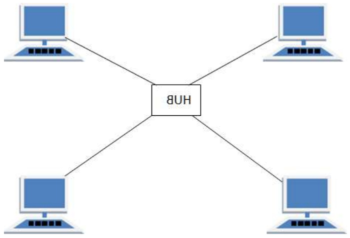
1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of Topology all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.



Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has `n(n-1)/2` physical channels to link `n` devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

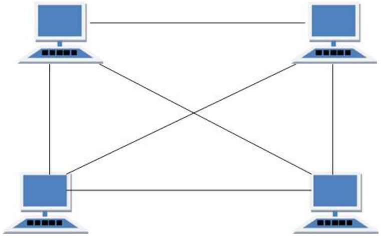
MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology



1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

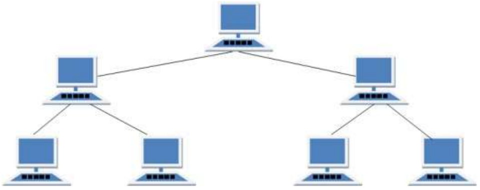
TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

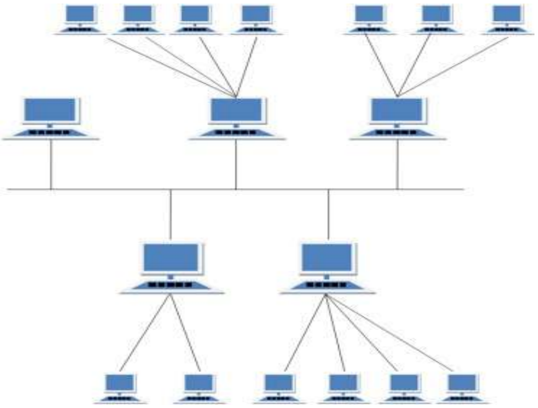


1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.

2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.



HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

# EXPERIMENT- 2

Aim of The Experiment:

Study about Network Cables & Connectors.

Resource Required-

Different types of Cables and connectors.

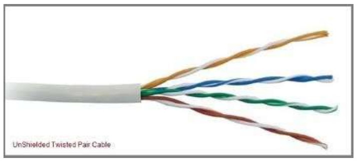
Network Cables:-

Guided media, which are those that provide a conduit from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fiber-Optic Cable**.

A signal travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. **Optical fiber** is a cable that accepts and transports signals in the form of light.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :



- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/KM @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference(noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver.

Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.

Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

Performance of Shielded Twisted Pair Cable

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. As shown in the below figure, a twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100kHz. Note that gauge is a measure of the thickness of the wire.

Applications of Shielded Twisted Pair Cable

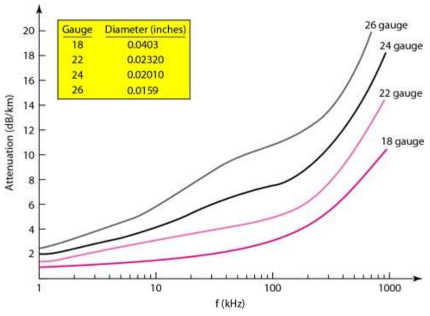
- In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as Centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

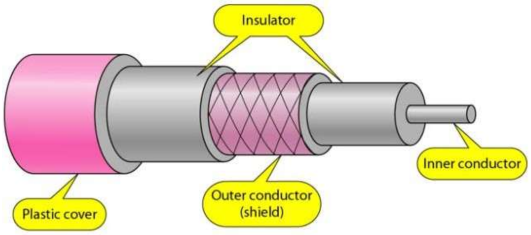


- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.

- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.

Coaxial Cable Standards

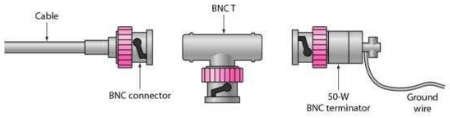
Coaxial cables are categorized by their Radio Government(RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:



Category	*Impedance*	*Use*
		et
		net

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. The below figure shows 3 popular types of these connectors: the BNC Connector, the BNC T connector and the BNC terminator.



The BNC connector is used to connect the end of the cable to the device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

There are two types of Coaxial cables:

1. BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

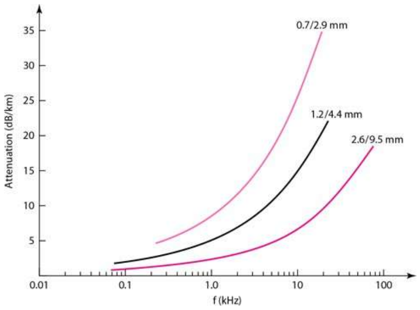
2. BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity.
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they

  have better shielding when compared to twisted pair cable



Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Performance of Coaxial Cable

We can measure the performance of a coaxial cable in same way as that of Twisted Pair Cables. From the below figure, it can be seen that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications of Coaxial Cable

- Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
- In traditional Ethernet LANs. Because of it high bandwidth, and consequence high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10Mbps with a range of 185 m.

Fiber Optic Cable

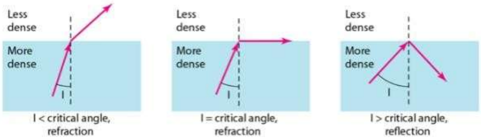
A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.

For better understanding we first need to explore several aspects of the **nature of light**.

Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.

Bending of a light ray

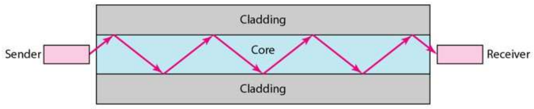

Less dense
More dense
I
I < critical angle, refraction
Less dense
More dense
I
I = critical angle, refraction
Less dense
More dense
I
I > critical angle, reflection

As the figure shows:

- If the **angle of incidence I**(the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.
- If the angle of incidence is **greater** than the critical angle, the ray **reflects**(makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

Note: *The critical angle is a property of the substance, and its value differs from one substance to another.*

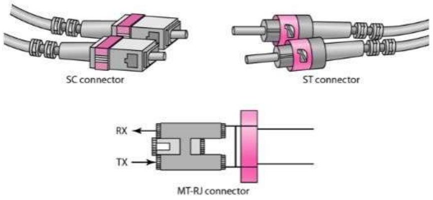
Optical fibres use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Internal view of an Optical fibre

Propagation Modes of Fiber Optic Cable

Current technology supports two modes(**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fibre with different physical characteristics. Multimode can be implemented in two forms: **Step-index** and **Graded-index**.



Connectors:-

A connector is a device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers.

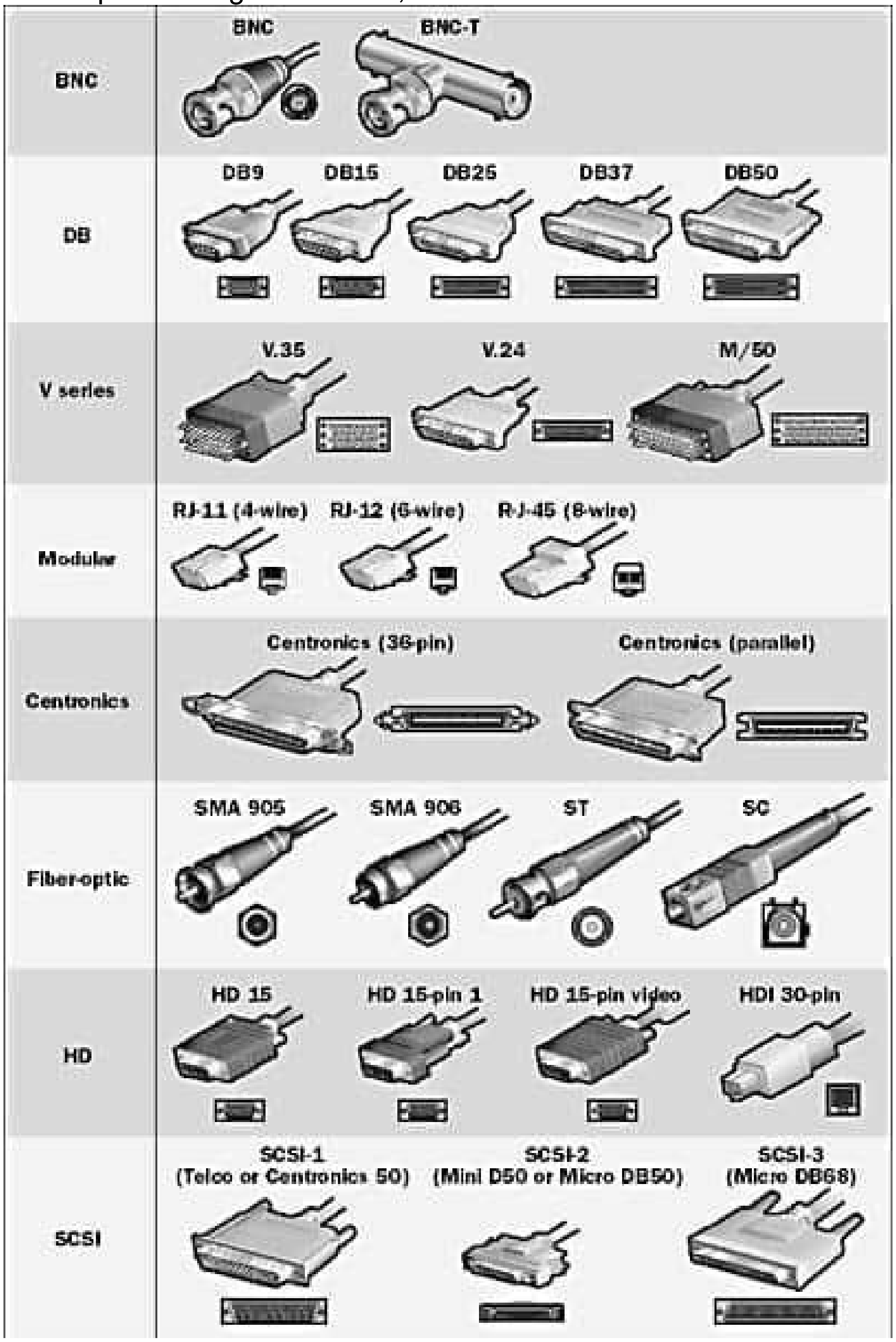
What is a Connector (device)?

A device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers. Connectors can be distinguished according to their physical appearance and mating properties, such as jacks and plugs (male connectors) or sockets and ports (female connectors).

They can also be distinguished by their different pinning configurations, such as DB9 and DB15 connectors, which have 9 and 15 pins, respectively.

In addition, connectors are distinguished by the kind of electrical interfaces they support. Examples of different types of connectors include:

- Connectors for serial interfaces, such as RS-232 and V.35
- Ethernet connectors, such as RJ-45 and BNC connectors
- Fiber-optic cabling connectors, such as SC and ST connectors



# EXPERIMENT- 3

Aim of The Experiment:

How to make Straight Through and Crossover Cable.

Resource Required-

Twisted pair Cable, connector, Crimping Tools, Cable Tester and Scissor.

HOW TO MAKE AN ETHERNET CABLE
Purchasing Ethernet cables can be quite expensive and pre-made lengths are not always the length you need. Making Ethernet cables is easy with a box of bulk Category 5e Ethernet cable and RJ-45 connectors that are attached to the cut ends of your preferred cable length.

Bulk Ethernet Cable - Category 5e or CAT5e

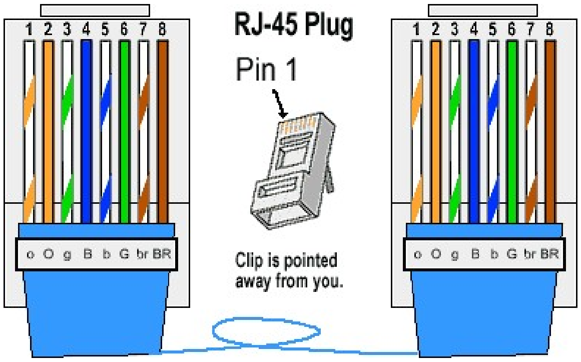
(You may also use Category 6 or CAT6 cabling which has higher performance specifications and is about 20% more expensive than CAT5e.)

Bulk RJ45 Crimpable Connectors for CAT-5e

or

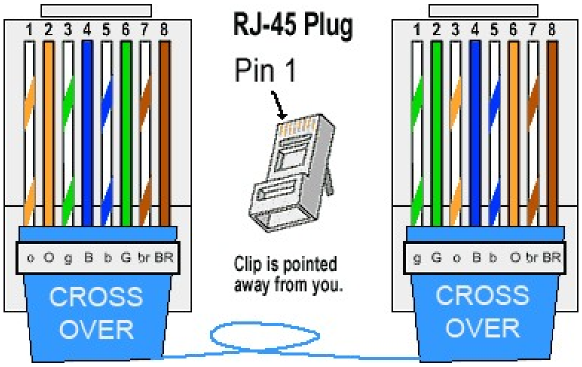
Bulk RJ45 Crimpable Connectors for CAT-6

RJ-45 Crimping tool



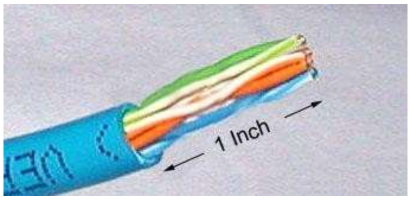
There are two kinds of Ethernet cables you can make, **Straight Through** and **Crossover**.

STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all purposes, and are often called "patch cables". It is highly recommend you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.

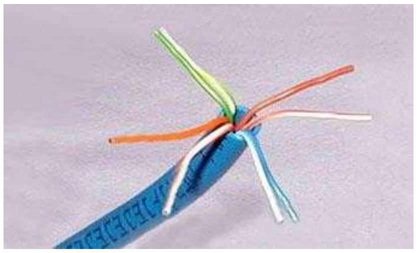


CROSSOVER CABLES - The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.

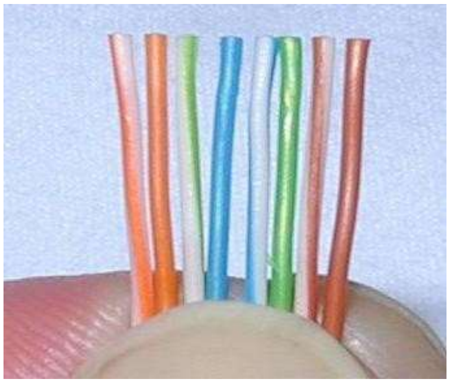
Here's how to make a standard cable:



Cut into the plastic sheath about **1 inch** (2.5 cm) from the end of the cut cable. The crimping tool has a razor blade that will do the trick with practice.

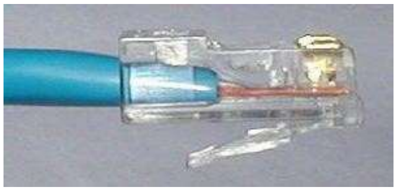


Unwind and pair the similar colors.

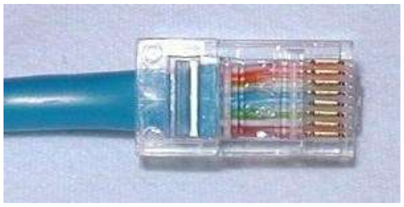


Pinch the wires between your fingers and straighten them out as shown. The color order is important to get correct.

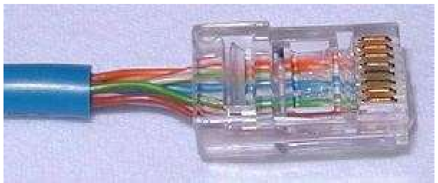
Use scissors to make a straight cut across the 8 wires to shorten them to **1/2 Inch** (1.3 cm) from the cut sleeve to the end of the wires.



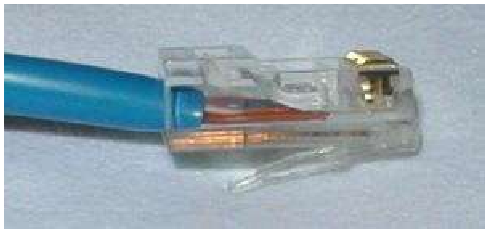
Carefully push all 8 unstripped colored wires into the connector. Note the position of the blue plastic sleeve. Also note how the wires go all the way to the end.



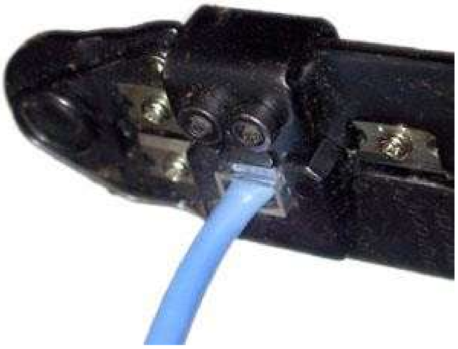
A view from the top. All the wires are all the way in. There are no short wires.



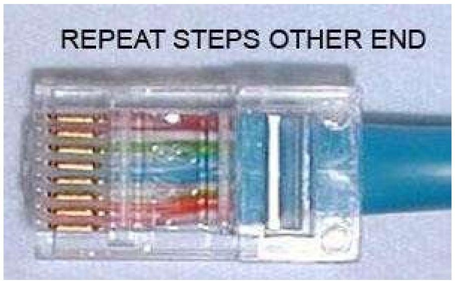
WRONG WAY - Note how the blue plastic sleeve is not inside the connector where it can be locked into place. The wires are too long. The wires should extend only 1/2 inch from the blue cut sleeve.



WRONG WAY - Note how the wires do not go all the way to the end of the connector.



CRIMPING THE CABLE ... carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the blue plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.



For a standard "Straight Through" cable, repeat all steps and wire color order on the other end of cable. For a cross-over cable, the other end will have a different color order as shown by the crossover picture above.

Make sure to test the cables before installing them. An inexpensive Ethernet cable tester does this quite well.

NOTE - The maximum cable length of CAT-5, CAT-5e or CAT-6 Ethernet cable is 328 feet or 100 meters.

<u># EXPERIMENT- 4</u>

Aim of The Experiment:

Install and configure a network interface card and Identify the IP address in a workstation.

Resource Required-

PC with Windows, NIC, Device driver.

Theory

If you want to add your computer to a network or a network device like a router then you need to install or configure your network card. Every new computer and motherboard you buy nowadays has a built in network port known as RJ45 socket. If you have an older computer or a motherboard that does not have a built in RJ45 socket then your only option is to add a PCI or USB network card if you wish to connect to a network. For this guide i will assume that you do not have a network card installed. If you already have a network card then you can skip step 1 to 3.

Step 1: Install a network card. This could be PCI card or USB network card adaptor.

If you are installing a PCI card you need to open your computer case and push the PCI network card into an empty PCI slot. It is quite simple and straight forward. If you are using a USB network adaptor you simply need to plug it into an empty USB port.

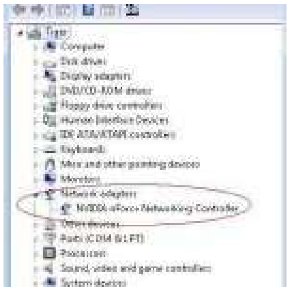
PCI Network card :

USB Network Adaptor:

Step 2: Install the device driver for the network card. Windows will detect that you have installed a new hardware. In most cases it will install the drivers automatically. If not, you need to install the drivers manually from the CD supplied with the network card. I am using Windows 7 operating system to demonstrate each step. If you are using Windows Vista the steps will be very similar. If you are using Windows XP it will be slightly different so<u> follow this guide instead</u>.

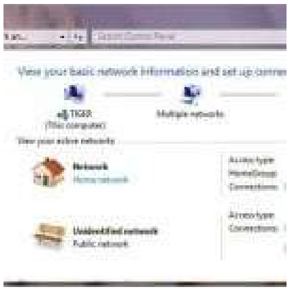
Step 3: After the drivers have been installed successfully you can see a network card listed under windows device manager. To go to the device manager click ***Start -> Control Panel -> System and Security -> Device Manager***.

You will see a network card listed under the device manager similar to the image below:



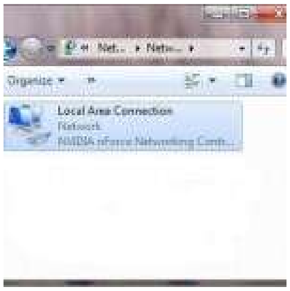
Step 4: Go to network sharing center by clicking ***Start -> Control panel -> Network and Internet -> Network and Sharing Center***. As you can see from the image below the

computer name tiger is connected to a network and has access to the Internet. This indicates that our network card is installed correctly and managed to get connection to our network. In this case it is connected to a ADSL router.

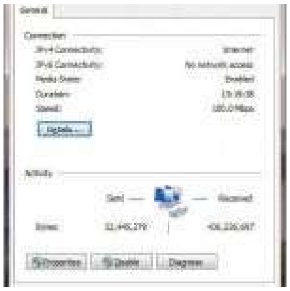


Step 5: Check your local area connections by clicking on ***change adaptor settings*** link on the left side of Network and Sharing center. You will get an icon similar to below:

Step 6: Double click on ***Local Area Connection*** icon which will display your LAN status. It shows the network connection duration, the speed of the connection, number of bytes sent and received etc.



Step 7: Click ***Details*** to see the Network connection details. You will see some very import connection details. Inside the red highlighted area you will see DHCP Enable is set to Yes and your IP Address listed. DHCP means (Dynamic Host Configuration Protocol). Basically its a feature built into most Routers or server operating systems which automatically assigns an IP address to the client computer. In our case the Router is the DHCP server and our computer is the client. Please note the dynamic IP address assigned by a DHCP server is random and can change next time you reboot your computer or the router.



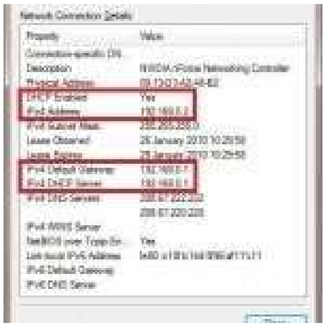
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	[illegible]
Speed:	100.0 Mbps

Activity

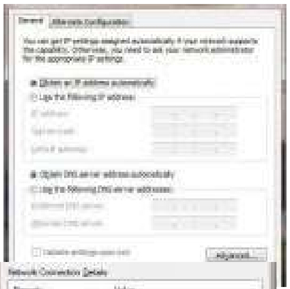
	Sent		Received
Bytes:	32,446,279		406,226,087

Step 8: Close the Network connection details. Click ***Properties -> (on Network area connections status) -> Internet protocol version 4 (TCP/IPv4) -> Properties***. As you can see everything is set to automatic. This means the DHCP server assigns everything automatically as mentioned above.



Property	Value
Connection-specific DN...	
Description	NVIDIA nForce Networking Controller
Physical Address	[illegible]
DHCP Enabled	Yes
IPv4 Address	192.168.0.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	26 January 2010 10:29:58
Lease Expires	[illegible] January 2010 10:29:58
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Servers	208.67.222.222 208.67.220.220
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	[illegible]
IPv6 Default Gateway	
IPv6 DNS Server	

Step 9: If you have many computers on a network i.e. your Desktop PC, Your Laptop, and your PS3 console its a good idea to fix the IP Address for each device. This is called static IP address. By fixing the IP address you can easily identify each computer on the network. This is what i will do below. I will choose my IP address as **192.168.0.100**. The subnet mask will be automatically set to **255.255.255.0**. Default gateway is **192.168.0.1**. The gateway IP address is normally the IP address of your router. Preferred DNS server is also the IP Address of your router, although you can use other DNS server like Open DNS IP address.



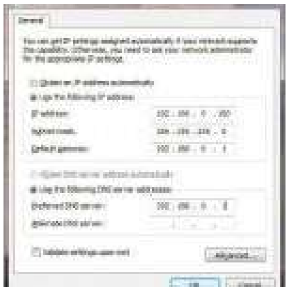
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

☐ Validate settings upon exit

Step 10: You can now check if the static settings have taken effect by clicking on ***Details*** on Local Area connection status as you have done on Step 6. Finally you will see all the settings that you have made in the previous step has taken effect. You will notice that the DHCP enable is set to No, as we have set each value manually.

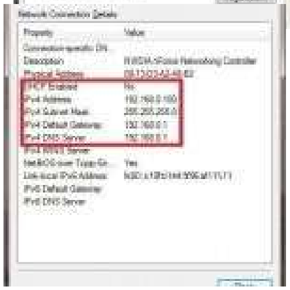


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:

☐ Validate settings upon exit



Property	Value
Connection-specific DN...	
Description	NVIDIA nForce Networking Controller
Physical Address	[illegible]
DHCP Enabled	No
IPv4 Address	192.168.0.100
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	[illegible]
IPv6 Default Gateway	
IPv6 DNS Server	

That's it, you have managed to install and configure your network device successfully. You have also learned how to use dynamic and static IP Address to connect to a network.

# EXPERIMENT- 5

Aim of The Experiment:

Manage User account on Windows, MAC, and Linux.

Resource Required-

Computer Installed with Windows, MAC or Linux.

Windows 10

1. Open the Control Panel.
2. Select **User Accounts**.

In the *User Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

Windows 8

1. From the Windows desktop, open the Charms menu by pressing the **Windows key + C key** and select **Settings**.
2. In the Settings window, select **Control Panel**.
3. Select **User Accounts**.

In the *User Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

Windows Vista and 7

1. Open the Control Panel.
2. Click **Add or remove user accounts**.

In the *User Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

Windows XP

1. Open the Control Panel.
2. Double-click the **User Accounts** icon.

In the *User Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

Windows 2000

Changing settings for a user account in Windows 2000 requires you to be logged in with an administrator account.

1. Open the Control Panel.

2. Double-click the **Users and Password** icon.

In the *Users and Passwords* window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.

Apple macOS X

macOS X 10.6 or later

1. Log in using an administrator account.
2. In the Apple menu, select **System Preferences**.
3. In the View menu, select **Users & Groups**.
4. You may need to click the lock button if it appears to be locked. Enter the administrator password.

In the *Users & Groups* window, you can add or remove user accounts. You can also select a user account and make any necessary changes.

macOS X 10.3 to 10.5.8

1. Log in using an administrator account.
2. In the Apple menu, select **System Preferences**.
3. In the *View* menu, select **Accounts**.
4. You may need to click the lock button if it appears to be locked. Enter the administrator password.

In the *Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes.

macOS X 10.2 to 10.2.8

1. Log in using an administrator account.
2. In the Apple menu, select **System Preferences**.
3. In the *View* menu, select **Accounts**.
4. You may need to click the lock button if it appears to be locked.

In the *Accounts* window, you can add or remove user accounts. You can also select a user account and make any necessary changes.

macOS X 10.1.5 or earlier

1. Log in using an administrator account.

2. In the Apple menu, select **System Preferences**.

3. In the *View* menu, select **Users**.

4. You may need to click the lock button if it appears to be locked.

In the *Users* window, you can add or remove user accounts. You can also select a user account and make any necessary changes.

Linux

To add a user account, use the **adduser** command. See the adduser command page for additional information about this command.

To remove a user account, use the **deluser** command. See the deluser command page for additional information about this command.

To change the user settings, such as group membership, default login shell, and home directory, use the **usermod** command. See the usermod command page for additional information about this command.

# EXPERIMENT- 6

Aim of The Experiment:

Use of Netstar and its Options.

Resource Required-

Computer Installed with Windows, MAC or Linux.

What is netstat?

Netstat — derived from the words *network* and *statistics* — is a program that's controlled via commands issued in the command line. It delivers basic statistics on all network activities and informs users on which **portsand addresses** the corresponding connections (TCP, UDP) are running and which ports are open for tasks. In 1983, netstat was first implemented into the **Unix** derivative BSD (Berkley Software Distribution), whose version 4.2 supported the first internet protocol family, TCP/IP. netstat has been integrated into **Linux** since its debut in 1991 and has been present in **Windows** since the appearance of version 3.11 (1993), which could also communicate via TCP/IP with the help of extensions. While the parameters of netstat's commands (as well as their outputs) differ from system to system, when it comes to their functions, the various implementations are very similar.

Essentially, netstat is a command line program and for this reason doesn't feature a graphical user interface. Programs like TCPView, which was developed by the Microsoft division Windows Sysinternals, makes it possible for statistics to be displayed graphically.

How do you use netstat?

In Windows operating systems, you can use the netstat services via the command line (cmd.exe). You can find them in the start menu under "All Programs" -> "Accessories" -> "Command Prompt". Alternatively, you can search directly for "Command Prompt" in the **start menu's search field** or start the command line via "Run" (Windows key + press "R" and enter "cmd"). The syntax of the netstat commands follows the following pattern:

```
netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p Protocol] [-r] [-s] [-t] [-x] [-y] [Interval]
```

The combination of the individual options works by stringing the individual parameters together, each separated by a space:

```
netstat [-OPTION1] [-OPTION2] [-OPTION3] …
```

The parameters are typically preceded by a **hyphen (-)**, but if you want to combine several options, you only have to place this hyphen in front of the first element. Instead of the variant shown above, you can also link different parameters as follows:

```
netstat [-OPTION1][OPTION2][OPTION3] …
```

In this case, it is important that you do not leave any spaces between the individual netstat options.

Netstat commands for Windows

[OPTION]	**Command**	**Description**
	netstat	Standard listing of all active connections
-a	netstat -a	Displays all active ports
-b	netstat -b	Displays the executable file of a connection or listening port (requires administrator rights)
-e	netstat -e	Shows statistics about your network connection (received and sent data packets, etc.)
-f	netstat -f	Displays the fully qualified domain name (FQDN) of remote addresses
-i	netstat -i	Brings up the netstat overview menu
-n	netstat -n	Numerical display of addresses and port numbers
-o	netstat -o	Displays the process identifier (PID) associated with each displayed connection
-p Protokoll	netstat -p TCP	Displays the connections for the specified protocol, in this case TCP (also possible: UDP, TCPv6, or UDPv6)
-q	netstat -q	Lists all connections, all listening TCP ports, and all open TCP ports that are not listening
-r	netstat -r	Displays the IP routing table
-s	netstat -s	Retrieves statistics about the important network protocols such as TCP, IP, or UDP
-t	netstat -t	Shows the download status (TCP download to relieve the main processor) of active connections
-x	netstat -x	Informs about all connections, listeners, and shared endpoints for NetworkDirect

-y	netstat -y	Displays which connection templates were used for the active TCP connections
Interval	netstat -p 10	Displays the respective statistics again after a selected number of seconds (here 10); can be combined as required (here with –p), [CTRL] + [C] ends the interval display

Netstat examples

In order to make the use of the listed netstat commands for Windows easier to understand, we will show you some example commands:

List of all connections for the IPv4 protocol

If you don't want to retrieve all active connections, but only all active IPv4 connections, you can do this using the netstat command:

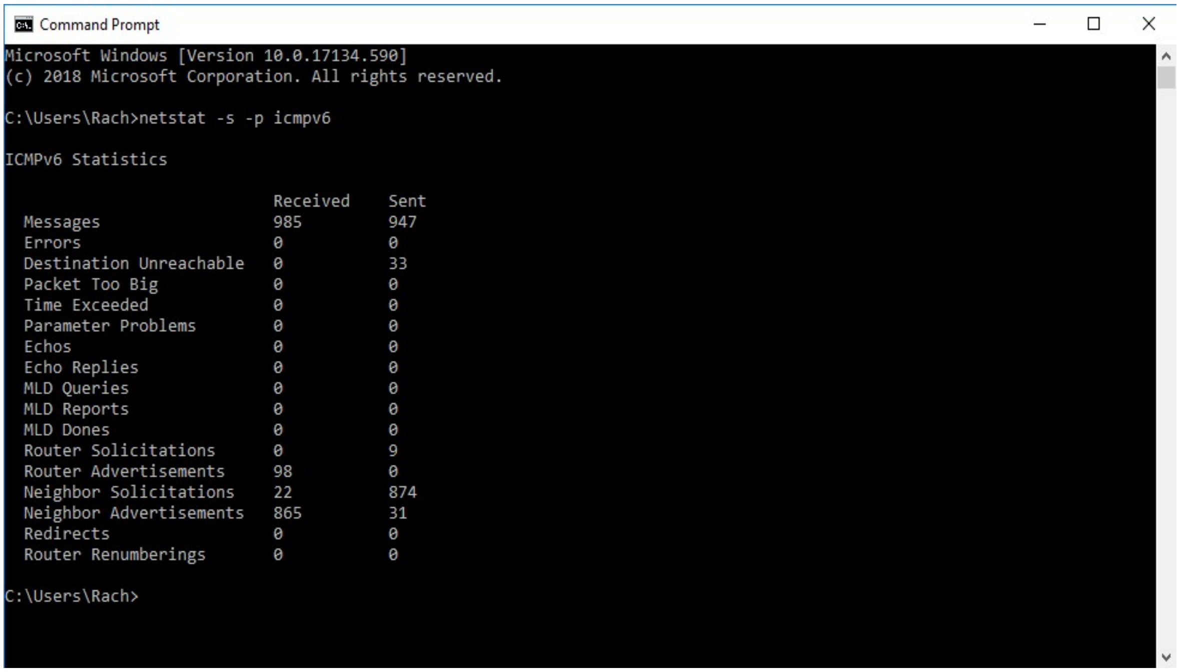
```
netstat -p IP
```

Accessing statistics using the ICMPv6 protocol

If you only want to obtain statistics on the ICMPv6 protocol, enter the following command in the command line:

```
netstat -s -p icmpv6
```

The output will then look something like this:



```
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Rach>netstat -s -p icmpv6

ICMPv6 Statistics

                            Received    Sent
  Messages                  985         947
  Errors                    0           0
  Destination Unreachable   0           33
  Packet Too Big            0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Echos                     0           0
  Echo Replies              0           0
  MLD Queries               0           0
  MLD Reports               0           0
  MLD Dones                 0           0
  Router Solicitations      0           9
  Router Advertisements     98          0
  Neighbor Solicitations    22          874
  Neighbor Advertisements   865         31
  Redirects                 0           0
  Router Renumberings       0           0

C:\Users\Rach>
```

To access the statistics for the previous ICMPv6 version 4, replace "icmpv6" with "icmp" in the command shown here.

Repetitive query of interface statistics (every 20 seconds)

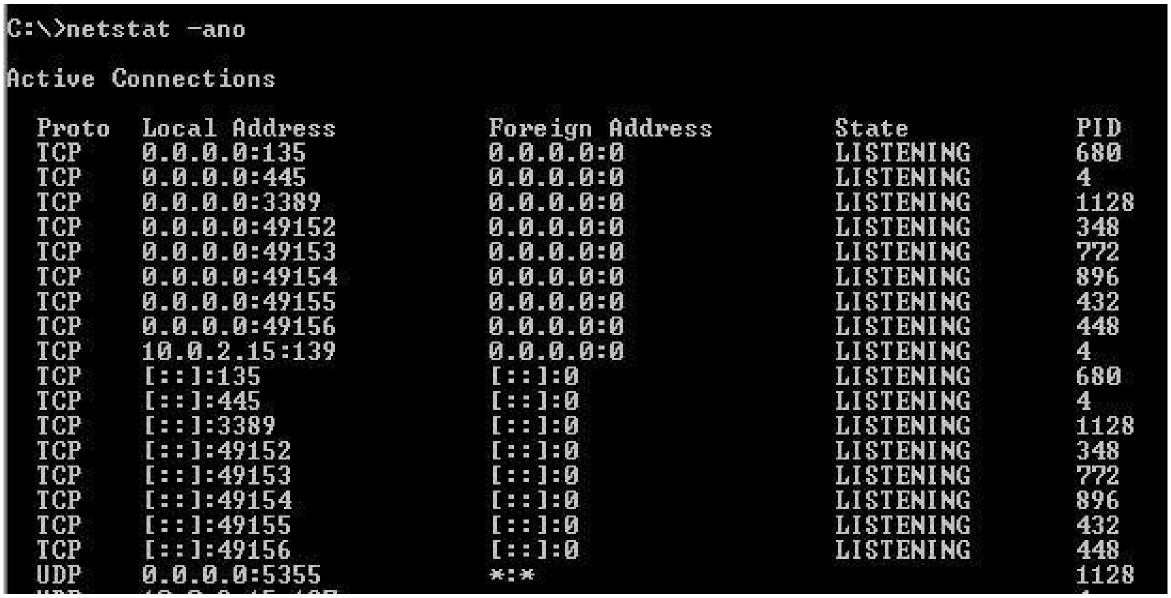
Use the following netstat command for a repeated query of the interface statistics, which returns new values every 20 seconds on received and sent data packets:

```
netstat -e 20
```

Display of all open ports and active connections (numeric and process ID included)

One of the most popular netstat commands is undoubtedly to query all open ports and active connections (including process ID) in numeric form:

```
netstat -ano
```



```
C:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1128
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       348
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       896
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       448
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       680
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1128
  TCP    [::]:49152             [::]:0                 LISTENING       348
  TCP    [::]:49153             [::]:0                 LISTENING       772
  TCP    [::]:49154             [::]:0                 LISTENING       896
  TCP    [::]:49155             [::]:0                 LISTENING       432
  TCP    [::]:49156             [::]:0                 LISTENING       448
  UDP    0.0.0.0:5355           *:*                                    1128
```

The command netstat -ano lists all open ports and active connections numerically, including process ID.

Why using netstat makes sense

When dealing with excessive traffic and malicious software it’s advantageous to be informed about the inbound and outbound connections to your computer. These are created via their respective **network addresses** that indicate which ports were preemptively opened for exchanging data. Once a port is opened, it receives the status ―LISTEN‖ and waits for connection attempts. One problem of having these ports remain open is that your system is then left vulnerable to malware. What’s more, there’s also a chance that Trojan viruses already found in your system may install a backdoor, opening up a corresponding port in the process. For this reason, **you should always regularly check the ports opened by your system**, a task for which netstat is particularly well suited. Thanks to the fact that you’ll be able to find the diagnosis tool on virtually every system, whether it be Unix, Linux, Windows, or Mac, this program offers a unified solution for all computers and servers.

Possible infections can be caught based on unknown opened ports or unknown IP addresses. In order to obtain an informative result, all other programs, such as your internet browser, should be turned off. This is due to the fact that these are often connected with computers that possess **unknown IP addresses**. Thanks to the detailed statistics, users also receive information on the packets that have been transferred since the last system start as well as notices of any errors that have occurred. The routing table, which delivers information on the paths data packets takes through the net, can be displayed with the help of the system-specific netstat command.

# EXPERIMENT- 7

Aim of The Experiment:

Troubleshooting using PING, IPCONFIG, NSLOOKUP and TRACERT.

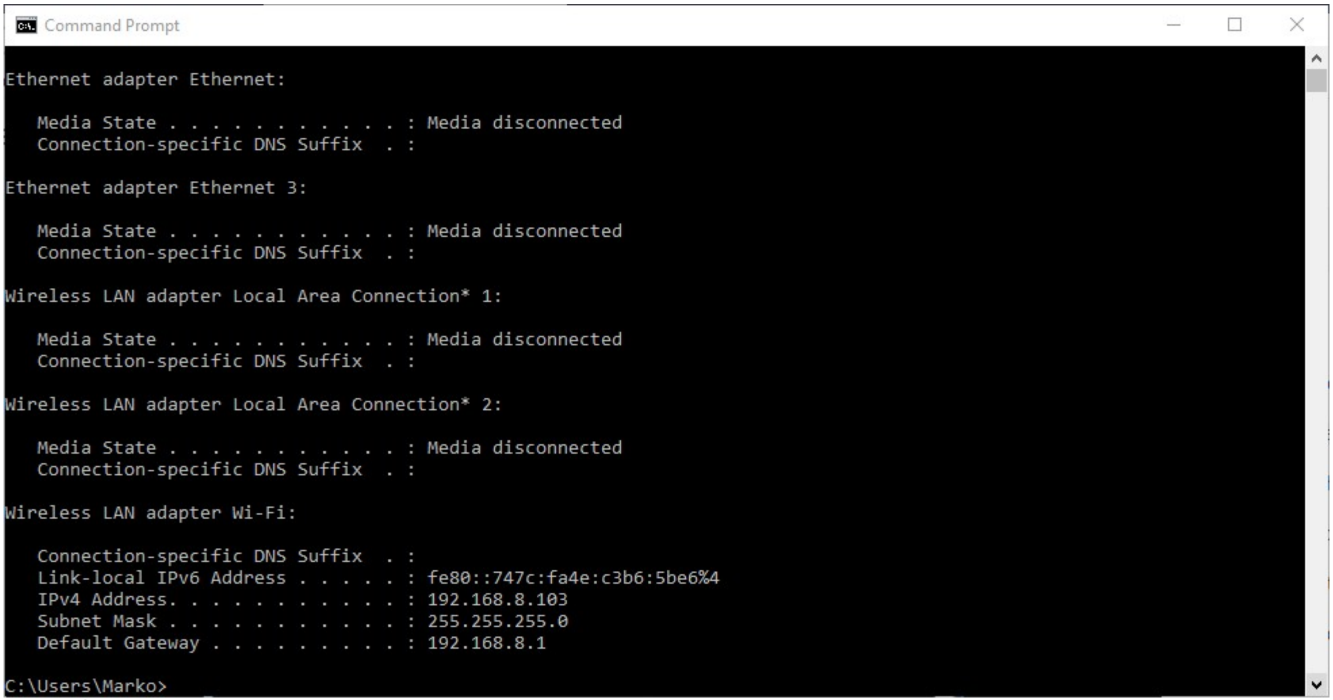
Resource Required-

Computer Installed with Windows, MAC or Linux.

This is about a series of network troubleshooting tools that you can use in command prompt to troubleshoot and gather information about your network. We're going to go over four commands: ―ipconfig‖, ―nslookup‖, ―ping‖, and ―tracert‖.

Ipconfig

The ―ipconfig‖ displays the current information about your network such as youryour IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers. Let's see the basic output of ―ipconfig‖:

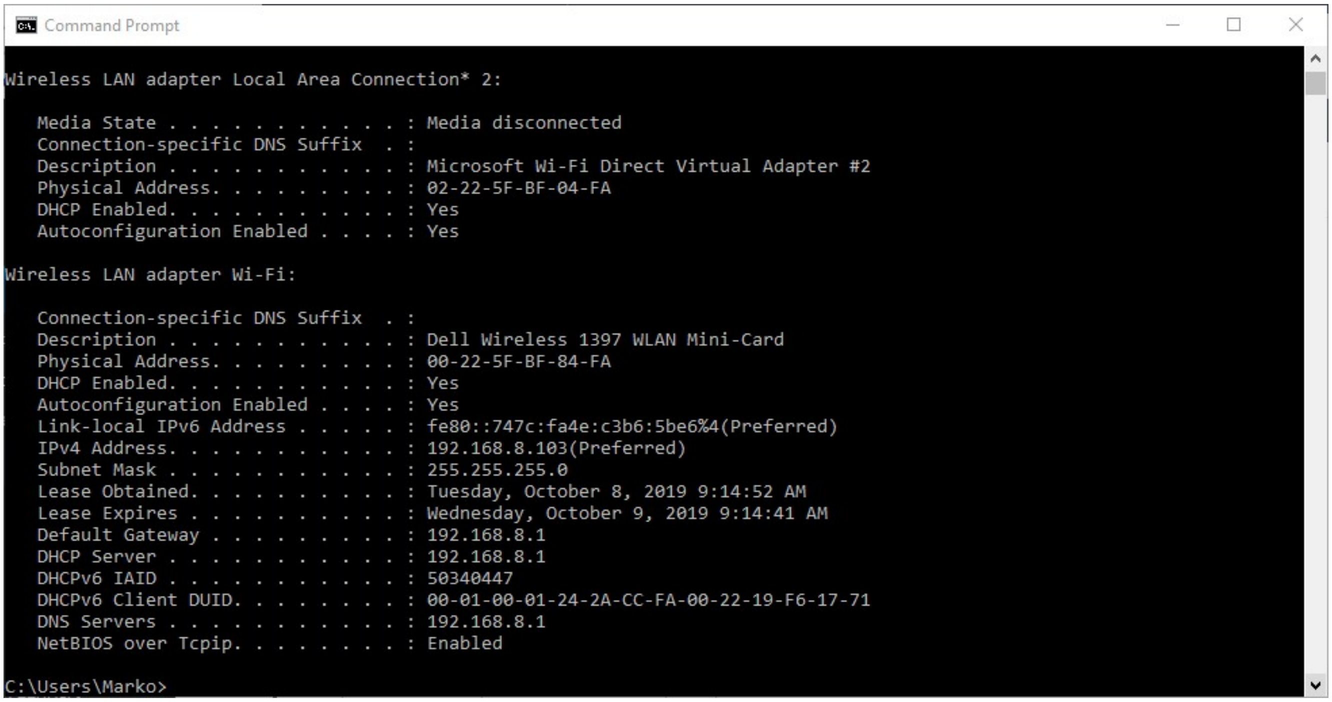


```
Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 3:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::747c:fa4e:c3b6:5be6%4
   IPv4 Address. . . . . . . . . . . : 192.168.8.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.1

C:\Users\Marko>
```

ipconfig output

Depending on your network connection type, you may see different output for different connection. For example, if you are connected to the network using Ethernet (you plug in your network cable to the RJ45 jack), you'll see IP information in the ―Ethernet adapter‖ section. In our case we are connected to the WIFI (wireless) connection so we our information there. In our case, the local IP (IPv4) of our computer is 192.168.8.103. We also see the Subnet Mask (255.255.255.0) which we can use to find the network address. We also see the Default Gateway IP (192.168.8.1), which is our router

However, we don't see DHCP and DNS information. To see detailed IP information we can use the ―/all‖ switch together with ―ipconfig‖ command (ipconfig /all).



```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 02-22-5F-BF-04-FA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1397 WLAN Mini-Card
   Physical Address. . . . . . . . . : 00-22-5F-BF-84-FA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::747c:fa4e:c3b6:5be6%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.8.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 8, 2019 9:14:52 AM
   Lease Expires . . . . . . . . . . : Wednesday, October 9, 2019 9:14:41 AM
   Default Gateway . . . . . . . . . : 192.168.8.1
   DHCP Server . . . . . . . . . . . : 192.168.8.1
   DHCPv6 IAID . . . . . . . . . . . : 50340447
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-2A-CC-FA-00-22-19-F6-17-71
   DNS Servers . . . . . . . . . . . : 192.168.8.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Marko>
```

ipconfig /all

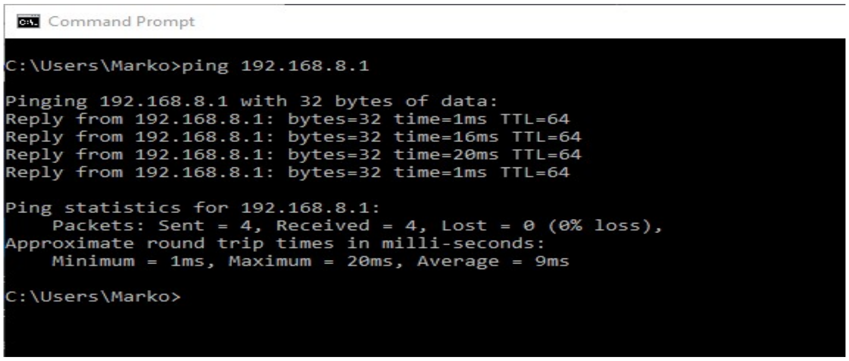
This time there's much more information present. The IP address, the Subnet Mask and and the Default Gateway address is still here, but this time you can also see your DHCP server and DNS server. In our case the DHCP IP address is the same as the router address, which means that DHCP server is currently residing on the router. DNS server is also the same as router address which means it is also DNS server.

Information gathering is a part of troubleshooting. For example, if you're trying to troubleshoot the DNS server, you can beforehand type in the —ipconfig‖ command and find where the DNS server is.

Network troubleshooting with ping

The —ping‖ command ping command allows you to send a signal to another device, and if that device is active, it will send a response back to the sender. The —ping‖ command is a subset of the ICMP (Internet Control Message Protocol), and it uses what is called an —echo request‖. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.

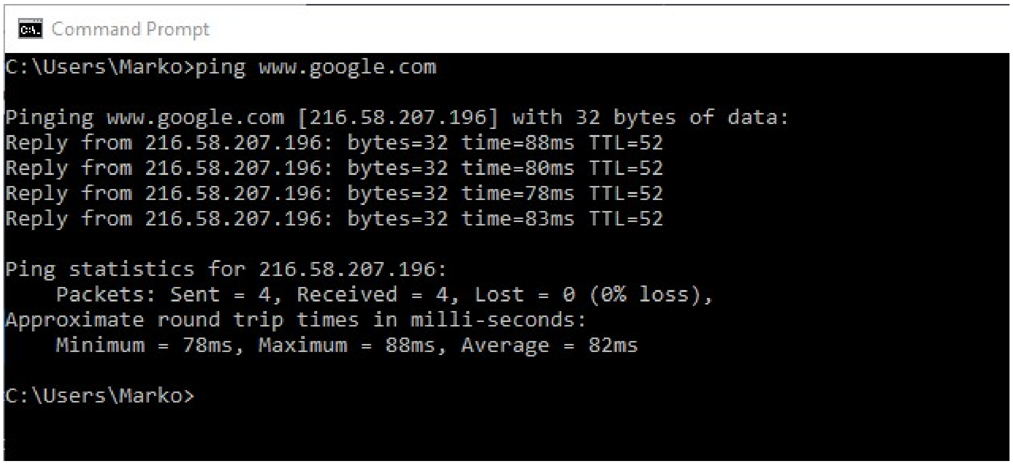
For example, if your local computer has Internet connectivity issues, you can try to ping your router. If you get no response then you know that the router is what is giving you problems. Let's ping our router IP, which is 192.168.8.1 in our example, and let's analyze the the printout.



```
C:\Users\Marko>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time=1ms TTL=64
Reply from 192.168.8.1: bytes=32 time=16ms TTL=64
Reply from 192.168.8.1: bytes=32 time=20ms TTL=64
Reply from 192.168.8.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 9ms

C:\Users\Marko>
```

ping command

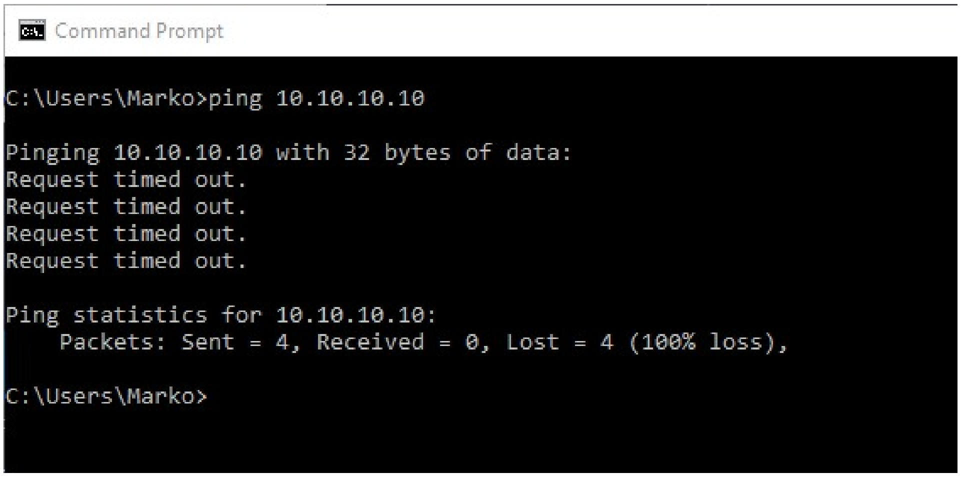
What happens is we send out four packets to the destination and the destination responds back with the same four packets. We sent out 32 bytes of data and we got back 32 bytes of data, and we got it back in 9 milliseconds average. From this we see that the device is alive and see the connection stability (4 of 4 packets received). Let us ping www.google.com and see what happens.



```
C:\Users\Marko>ping www.google.com

Pinging www.google.com [216.58.207.196] with 32 bytes of data:
Reply from 216.58.207.196: bytes=32 time=88ms TTL=52
Reply from 216.58.207.196: bytes=32 time=80ms TTL=52
Reply from 216.58.207.196: bytes=32 time=78ms TTL=52
Reply from 216.58.207.196: bytes=32 time=83ms TTL=52

Ping statistics for 216.58.207.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 88ms, Average = 82ms

C:\Users\Marko>
```

ping www.google.com

We got a similar printout, however, since we used domain name, we now see the resolved IP address of www.google.com. We sent out 32 bytes of data but, because Google server is far away it took 82 milliseconds to send and receive 4 packets from Google. We sent and received 4 packets so the connection was stable. Finally let's ping a device that doesn't exist.



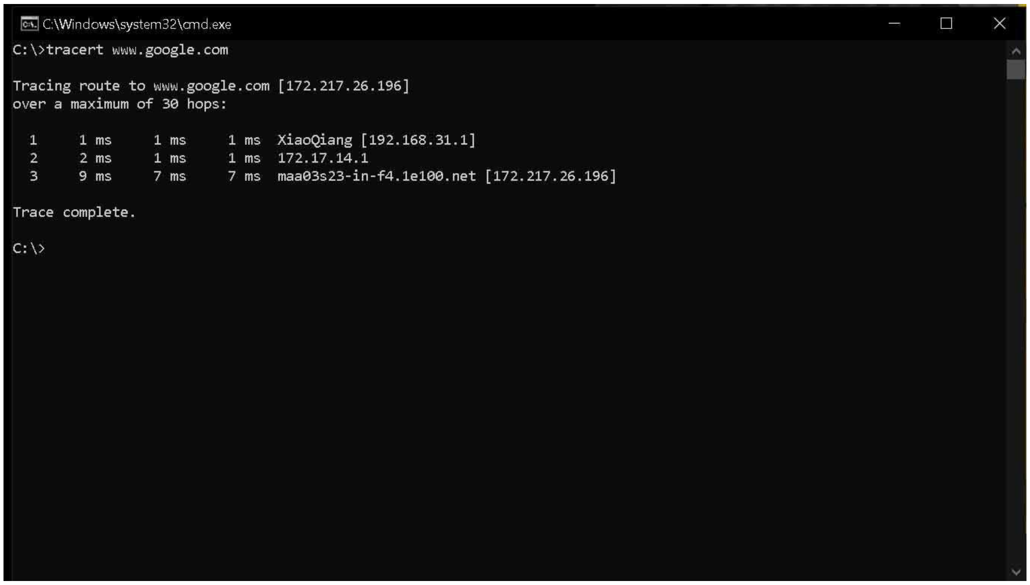
```
C:\Users\Marko>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Marko>
```

ping non existing device

We get a ―Request timed out‖ response. This is going to yield the same kind of results if a device wasn't actually working. As you can see at the summary, wee sent four and received zero, so it was a hundred percent lost. That means the system you're trying to reach is not connected to the network.

tracert

This command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term ―hops‖ instead of routers. Let's run the command and see what kind of results we get.



```
C:\>tracert www.google.com

Tracing route to www.google.com [172.217.26.196]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  XiaoQiang [192.168.31.1]
  2     2 ms     1 ms     1 ms  172.17.14.1
  3     9 ms     7 ms     7 ms  maa03s23-in-f4.1e100.net [172.217.26.196]

Trace complete.

C:\>
```

tracertwww.google.com

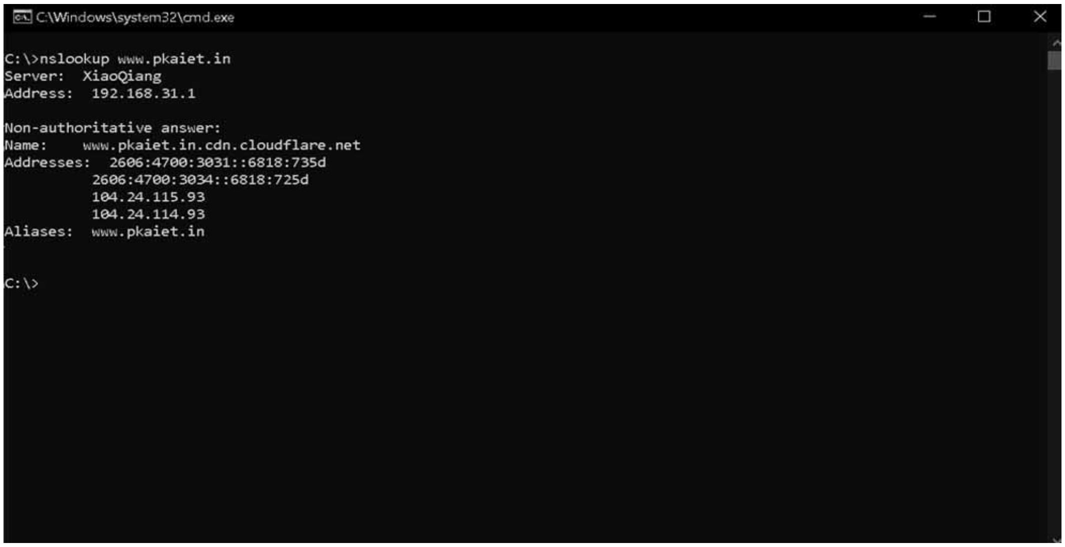
We have traced the route to www.google.com, and we're getting a list of each of the routers that we're hitting. At the end we see the IP address for utilizewindows.com server so the trace is complete. In our case we have 13 hops before we actually reached the intended server.

So what is the significance of this? Let's say your home network was perfectly fine but there was a problem with some router in the between, for example with your ISP router. If there's any problems it will try to indicate what the problem is. It could say things like —request timed out‖, —destination unreachable‖ or similar. However, different messages don't necessarily mean that there is a real problem with the device. There are several reasons why a —Request timed out‖ message may appear at the end of a trace route. This is typically because a device doesn't respond to ICMP or traceroute requests. Also, the device firewall or other security device could be blocking the request. Here is article with more details about tracert command.

nslookup

The nslookup command will fetch the DNS records for a given domain name or an IP address. Remember the IP addresses and domain names are stored in DNS servers, so the nslookup command lets you query the DNS records to gather information.

Let's say you wanted to know the IP address of www.pkaiet.in. You could simply type in nslookup and type in www.pkaiet.in. Let'sanalyze this printout.



```
C:\>nslookup www.pkaiet.in
Server:  XiaoQiang
Address:  192.168.31.1

Non-authoritative answer:
Name:    www.pkaiet.in.cdn.cloudflare.net
Addresses:  2606:4700:3031::6818:735d
          2606:4700:3034::6818:725d
          104.24.115.93
          104.24.114.93
Aliases:  www.pkaiet.in


C:\>
```

nslookupwww.pkaiet.in

The first two lines show you which DNS server was used to get these results. Our DNS server happens to reside on our router, so our router is also our DNS server. The answer that we got was the IP address of the www.pkaiet.in server.

EXPERIMENT- 8

Aim of The Experiment:

What is NOS (Network Operating System) and its use.

Resource Required-

Computer Installed with NIC, NOS software.

Network operating system (NOS)

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

The composition of hardware that typically uses a NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to then provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.

Due to earlier versions of basic operating systems not being designed for network use, network operating systems emerged as a solution for single-user computers.

Types of network operating systems

There are two basic types of network operating systems, the peer-to-peer NOS and the client/server NOS:

1. Peer-to-peer network operating systems allow users to share network resources saved in a common, accessible network location. In this architecture, all devices are treated equally in terms of functionality. Peer-to-peer usually works best for small to medium LANs and is cheaper to set up.
2. Client/server network operating systems provide users with access to resources through a server. In this architecture, all functions and applications are unified under one file server that can be used to execute individual client actions regardless of physical location. Client/server tends to be most expensive to implement and requires a large amount of technical maintenance. An advantage to the client/server model is that the network is controlled centrally, makes changes or additions to technology easier to incorporate.

Common features of network operating systems

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality. This includes:

- Basic support for operating systems like protocol and processor support, hardware detection and multiprocessing.
- Printer and application sharing.
- Common file system and database sharing.
- Network security capabilities such as user authentication and access control.
- Directory
- Backup and web services.
- Internetworking.

Examples of network operating systems

True network operating systems are categorized as software that enhances the functionality of operating systems by providing added network features. A few examples of these network operating systems and their service providers are:

- Artisoft's LANtastic- This is a simple, user-friendly NOS that supports most PC operating systems.
- Banyan's VINES- This uses a client-server architecture to request specific functions and services.
- Novell's NetWare- This was the first network operating system to be released and is designed based on XNS protocol architecture.
- Microsoft's LAN Manager- This operates as a server application and was developed to run under the Microsoft OS. Now, most of the functionality of LAN Manager is included in the Windows OS itself.

In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS come with capabilities that enable them to be described as a network operating system. Further, the most popular operating systems like Windows, Unix, Linux and Mac include built-in networking functions that may not require additional network services.

# EXPERIMENT- 9

Aim of The Experiment:

WAN concepts and Configure and forward Traffic in WAN.

Resource Required-

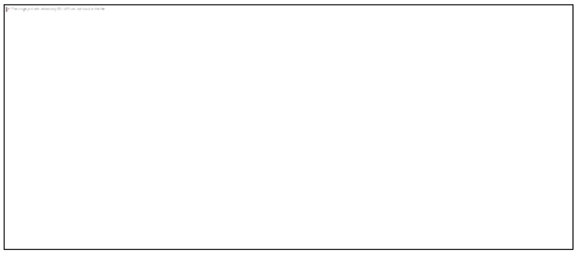
PC with Internet connectivity.

Introduction to WANs (Wide Area Network)

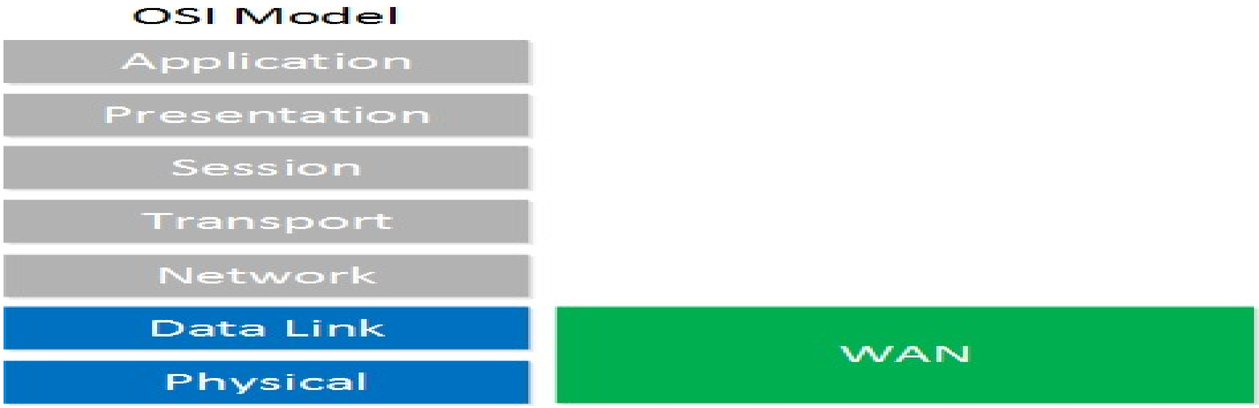
Our own networks are called LANs (Local Area Network). We **own and operate these networks**. It's called a ―local‖ area network since all devices that make up the LAN are close to each other. Perhaps in one building or a few buildings close to each other (called a campus).

When we need access to other remote networks, connect two LANs together or give others access to our LAN, we need a WAN (Wide Area Network). As the name implies, WANs cover **large geographical areas**. This could be a network between two cities or as large as the Internet.

WANs are operated by companies like phone/cable companies, service providers, or satellite companies. They build large networks that span entire cities or regions and lease the right to use their networks to their customers.



On the LAN, the dominant protocol that we use is Ethernet. For wide area networks, there are dozens of technologies and protocols we can choose from. Most WAN technologies describe layer one and two of the OSI model:



On the physical layer, we use different hardware, cables, connectors and interfaces. On the data link layer, there are a number of different WAN protocols that we can use.We'll discuss these.

Physical Layer Terminology

When you read about WAN technologies and protocols, there is a lot of terminology you might encounter. Let’s look at a picture:

The picture above is what a WAN solution in general looks like. Let me walk you through the different items in the picture:

- On the left side in the green box, we have the customer network that is paying for the services of the WAN service provider.
- On the right side, in the blue box, we have the WAN service provider with its hardware.
- The **CPE (Customer Premises Equipment)** are all devices, wiring, and hardware that are located at the site of the customer. These devices are connected to the WAN of the WAN service provider. The CPE might be owned by the customer or leased from the service provider. A combination is also possible. Perhaps the router is owned by the customer and the modem is leased from the service provider.
- All hardware and devices that belong to the service provider is called the **service provider equipment**.
- The **demarcation point (demarc)** is where the service provider’s wiring ends and where the customer’s wiring begins. Depending on which country you live in, this could be a so-called meter box/meter cupboard inside or outside your house or building.
- The **DTE (Data Terminal Equipment)** is the customer device that forwards data from the customer’s network to the WAN. This can be a router, computer or sometimes a switch.
- The **CSU/DSU (Channel Service Unit / Data Service Unit)** is a device that sits in between the router and WAN connection. It converts digital signals from the WAN into a digital signal the router understands and vice versa. For example, the CSU/DSU might be connected to the router with a DTE serial cable, so it has to speak a language the router understands. On the other side, the CSU/DSU is connected to a two pair cable to the WAN service provider which speaks another language. Back in the days, the CSU/DSU was a separate device. Nowadays this is integrated in router interfaces.
- The **DCE (Data Circuit-terminating Equipment)** is the device that receives data from the DTE, modulates into an analog signal and forwards it onto the wire to the service provider. It also demodulates analog signals that it receives on the wire into digital signals. This device is a modem and nowadays often integrated in interfaces or routers.
- The **local loop** is the physical link that connects from the demarcation point at the customer to the edge of the service provider network. It’s also often called the —last mile‖.
- The **CO (Central Office)** is the building where all lines from local loops to the customers end up. In this building, we will find CO switches where the lines terminate. The kind of CO switch used depends on the technology that is used (telephony, DSL, cable, etc.).

WAN Technologies

There are a number of different methods how we can forward data on a network:

- Circuit switching
- Packet switching
- Cell switching

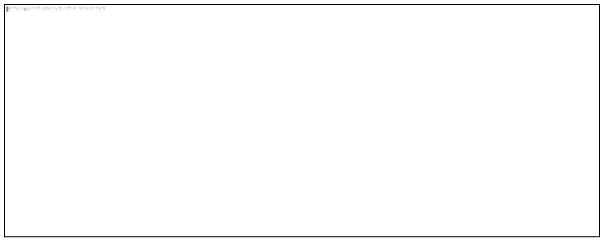
Let me explain these and show you some examples.

Circuit Switching

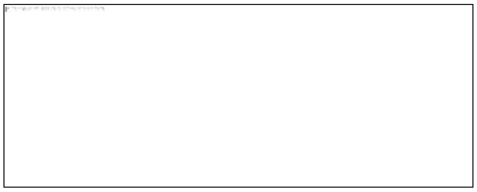
To understand circuit switching, it’s best to look at how telephony worked back in the 60s:

The phone network used telephone switchboards that were operated by switchboard operators who connected calls by plugging in phone plugs in the required phone jacks. To connect long distance calls, operators had to work together with operators in other offices.

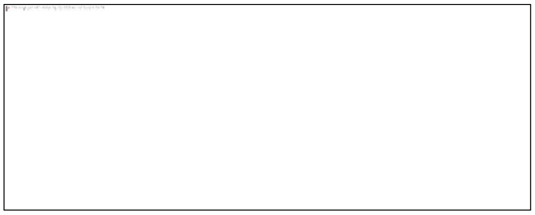
Once the correct plugs were connected, a circuit was established between two callers which allowed them to talk to each other. Here's a visualization:



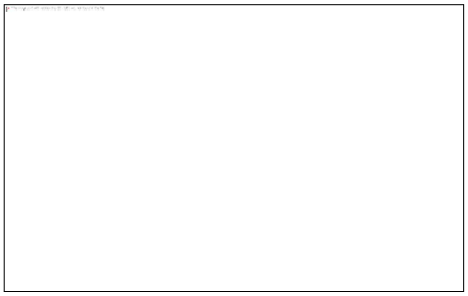
Above we have four users, the cloud is the phone network with two switchboards. Let's say user 1 and user 3 would like to talk to each other. The operators would plug in the required phone plugs to establish a circuit like this:



The circuit that is established is used exclusively by user 1 and user 3. It doesn't matter if they talk a lot or enjoy each other's silence, nobody else can use this circuit. User 2 and user 4 would also like to talk to each other. After connecting the right phone plugs, the circuit is established:



We now have two circuits and the network is at 100% capacity. It doesn't matter how much —datall our users are generating by talking or not. What if we had a fifth user?



The fifth user has to wait since there is no available capacity in our network. We will have to wait until one of the calls is completed so the circuit can be disconnected.

Later, the operators were replaced by electromechanical automatic telephone exchanges but circuit switching was still used to establish analog phone calls on our PSTN (Public Switched Telephone Network) which is also known as POTS (Post Office Telephone Service or Plain Old Telephone System).

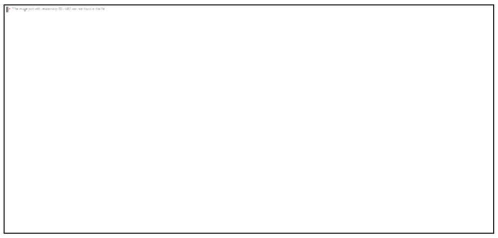
ISDN (Integrated Services Digital Network) also used circuit switching and supported data rates of 64 kbps per data channel.

The example above explains the limitations of circuit switching. Once the circuit is established, the **capacity is reserved** for that circuit.

The problem with circuit switching is the limited capacity that it offers. Once the circuit is established, you make a reservation in the network and you end up with a fixed capacity for the circuit. It doesn't matter how much data you transmit or not, the circuit will be there for you. This also means that you waste a lot of unused resources…

Packet Switching

The idea behind it is that we break our data down in —chunksll. Each chunk is a packet that is sent



on the network. This is what we mostly use on our networks nowadays. Here’s a visualization:

Above you can see that host 2 wants to send 4500 bytes of data. This is broken down in 3x 1500 byte packets. One packet is sent on the top link, the other two on the bottom link. With packet switching, there’s no fixed path in the network. Once host 4 receives all packets, it can extract and reassemble the data.

The packet size is variable, there is no fixed size.

Packet switching has mostly replaced circuit switching. One of the advantages is that because there are no fixed circuits, we can more effectively use the capacity that the network has to offer. We don’t waste any unused resources.

Cell Switching

Cell switching is very similar to packet switching with the exception that we use a fixed for our size for our cells. Here’s an example:

Above you can see that each computer sends some data. Whatever they send gets encapsulated in cells with a fixed size, 53 bytes in my example. ATM (Asynchronous Transfer Mode) was a popular WAN protocol that used cell switching.

WAN Technology

So far, we talked about some physical layer terminology and different methods to forward data on a network. Let’s look now at some actual WAN technologies that we use or used in the past.

Leased Lines

Leased lines are one of the older WAN options. Imagine we have a LAN in New York and another LAN in Miami. Somehow, we need to connect these two networks. A leased line is a point-to-point link that we **exclusively** use, often offered by a phone company. Leased lines have been out there for awhile so there are a bunch of other names we use for this:

- T1 / T3 / E1 / E3
- Point-to-point link
- Serial link
- Leased circuit

This point to point link will only be used by the customer that is paying for it, which makes it an expensive option. From the customer’s perspective, it looks like this:

On each site, we use a router with the point-to-point connection in between. In reality, there is no single connection that spans the ~1300 miles between New York and Miami.The phone company has multiple buildings throughout the country with their equipment, called COs (Central Office). These COs are connected to most buildings in a city, hoping that they can sell their services some day. When a customer requires a leased line, the phone company creates a connection between COs to build a point-to-point link:

Conclusion

You have now learned the basics of WANs (Wide Area Network):

- The difference between LANs and WANs.
- The terminology that is used when talking about the WAN physical layer.
- The difference between circuit switching, packet switching, and cell switching.
- Some examples of WAN technologies like leased lines& Ethernet.