Diploma Engineering

Laboratory Manual

Computer Networking

(4340703)

DCE SEM 4

Enrolment No	
Name	
Branch	
Academic Term	
Institute	

Directorate Of Technical Education Gandhinagar-Gujarat

DTE's Vision:

- To provide globally competitive technical education;
- Remove geographical imbalances and inconsistencies;
- Develop student friendly resources with a special focus on girls' education and support to weaker sections;
- Develop programs relevant to industry and create a vibrant pool of technical professionals.

Institute's Vision:

Institute's Mission:

Department's Vision:

Department's Mission:

Certificate

This is to certify that Mr./Ms. ……

…….. Enrolment No. …….. of …….. Semester of Diploma in *Computer Engineering* of Institute ……..

(GTU code: ……..) has satisfactorily completed the term work in course *Computer Networking (4340703)* for the academic year: …….. Term: …….. as prescribed in the GTU curriculum.

Place:……..

Date: ……..

Subject Faculty **Head of the Department**

Preface

Main motto of any laboratory/Practical/field work is for enhancing required skills as well as creating ability amongst students to solve real time problem by developing relevant competencies in psychomotor domain. By keeping in view, GTU has designed competency focused outcome-based curriculum -2021 (COGC-2021) for engineering diploma programmes. In that more time allotted to practical work than theory. It shows importance of enhancement of skills amongst students, and it pays attention to utilize every second of time allotted for practical amongst students, instructors and Lecturers to achieve relevant outcomes by performing rather than writing practice in study type. It is must for effective implementation of competency focused outcome- based green curriculum-2021, every practical has been keenly designed to serve as a tool to develop & enhance relevant industry needed competency in each and every student. These psychomotor skills are very difficult to develop through traditional chalk and board content delivery method in the classroom. Accordingly, this lab manual designed to focus on the industry defined relevant outcomes, rather than old practice of conducting practical to prove concept and theory.

By using this lab manual students can read procedure one day advance before actual performance day of practical experiment which creates interest and also they have idea of judgement of magnitude prior to performance. This in turn enhances pre-determined outcomes amongst students. Each and every experiment /Practical in this manual begins by competency, industry relevant skills, course outcomes as well as practical outcomes which serve as a key role for doing the practical. The students will also achieve safety and necessary precautions to be taken while performing practical.

This manual also provides guidelines to lecturers to facilitate student-centered lab activities through each practical/experiment by arranging and managing necessary resources in order that the students follow the procedures with required safety and necessary precautions to achieve outcomes. It also gives an idea that how students will be assessed by providing Rubrics.

Computers and computer networks are the sole of the computer-based information systems. In present times, whether it is small or big organization they own their private computer networks to handle computer-based information systems. Therefore in every organisation, establishing, commissioning (making operational) and maintaining secure computer networks has becomes one of the essential jobs of a diploma computer engineer too. This course is therefore designed to help the computer engineering diploma holders to develop this competency

Best efforts are being done from our side in designing this lab manual, but there is always scope of improvement. Any suggestions for improvement are welcomed.

Programme Outcomes (POs) to be achieved through Practical of this Course

Following programme outcomes are expected to be achieved through the practical of the course:

1. **Basic and Discipline specific knowledge:** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the computer engineering problems.

2. **Problem analysis**: Identify and analyse well-defined computer engineering problems using codified standard methods.

3. **Design/ development of solutions:** Design solutions for computer engineering well-defined technical problems and assist with the design of systems components or processes to meet specified needs.

4. **Engineering Tools, Experimentation and Testing:** Apply modern computer engineering tools and appropriate technique to conduct standard tests and measurements.

5. **Engineering practices for society, sustainability and environment:** Apply appropriate technology in context of society, sustainability, environment and ethical practices.

6. **Project Management:** Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.

7. **Life-long learning:** Ability to analyze individual needs and engage in updating in the context of technological changes in field of computer engineering.

Practical Outcome - Course Outcome matrix

Course Outcomes (COs):

a. **CO1** Classify various types of networks base on their construction, usage and scope

b. **CO2** Differentiate OSI and TCP/IP models

c. **CO3** Select proper transmission media and devices based on network requirements.

d. **CO4** Compare IPv4 and IPv6 addressing scheme

e. **CO5** Identify various types of network security threats

S. No.	Practical Outcome	CO1	CO2	CO3	CO4	CO5
1.	Assume six devices are arranged, if in: a) bus topology b) ring topology c) star topology d) mesh topology Find out number of cables (links), ports needed in each device and total number of ports needed in entire network for each of above stated topology.	√	-	-	-	-
2.	Study about OSI model network Layers.	-	√	-	-	-
3.	Prepare and Test Straight UTP Cable and Cross UTP Cable.	-	-	√	-	-
4.	Study and Test various Network devices available at Department/Institute. (Repeater, Hub, Switch, Bridge, Router and Gateway).	-	-	√	-	-
5.	Determine whether following IPv4 address are valid or invalid. If valid IPv4 addresses then find class, Network and Host ID of an IPv4 address. If invalid IPv4 address then write reason for the same. a) 1.4.5.5 b) 75.45.301.14 c) 111.56.045.78 d) 192.226.12.11 e) 130.45.151.154 f) 11100010.23.14.67 g) 221.34.7.8.20 h) 240.230.220.89	-	-	-	√	-
6.	Determine Class and Network Address for given IPv4 address and subnet mask. IPv4 address | Subnet Mask | Class | Subnet 172.16.2.10 | 255.255.255.0 | | 10.6.24.20 | 255.255.240.0 | | 10.30.36.12 | 255.255.255.0 | |	-	-	-	√	-
7.	Subnet the IP address 216.21.5.0 into 30 hosts in each subnet	-	-	-	√	-

8.	Identify valid IPv6 addresses and if invalid IPv6 address then write reason for the same. a) 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888 b): : c) 225.1.4.2 d) 2001: db8: : e): : 1234 : 5678 f) 2001 : db8: : 1234 : 5678 g) 2001:0db8:0001:0000:0000:0ab9:C0A8:0102 h) fe80:2030:31:24	-	-	-	**√**	-
9.	Study of firewall in providing network security.	-	-	-	-	**√**
10.	Run basic utilities and network commands: ipconfig, ping, tracert, netstat, pathping , route	-	-	-	-	-
11.	MicroProject					

Industry Relevant Skills

The following industry relevant skills of the competency "**Use Software and hardware technology to establish, commission (make operational) and maintain secure computer networks**" are expected to be developed in the student by undertaking the practical of this laboratory manual.

1. Select the layout of proper cabling
2. Design of Computer Network
3. Installation of Computer Network
4. Selection of proper internetworking device
5. Knowledge of Internet protocol for subnetting
6. Dealing with network security threats
7. Trouble shooting computer network with Network utilities command

Guidelines to Teachers

1. Teacher should provide the guideline with demonstration of practical to the students.
2. Teacher is expected to refer complete curriculum document and follow guidelines for implementation strategies.
3. Teacher shall explain prior concepts and industrial relevance to the students before starting of each practical
4. Involve all students in performance of each experiment and should give opportunity to students for hands on experience.
5. Teacher should ensure that the respective skills and competencies are developed in the students after the completion of the practical exercise.
6. Teacher is expected to share the skills and competencies to be developed in the students.
7. Finally give practical quiz as per the instructions. Utilise 2 hrs of lab hours effectively and ensure completion of write up with quiz also on same day.

Instructions for Students

1. Listen carefully the lecture, curriculum, learning structure, skills to be developed.
2. Organize the work in the group and make record of all observations.
3. Students shall develop maintenance skill as expected by industries.
4. Student shall attempt to develop related hand-on skills and build confidence.
5. Student shall develop the habits of evolving more ideas, innovations, skills etc.
6. Student shall refer technical magazines and databooks.
7. Student should develop habit to submit the practical on date and time.
8. Student should well prepare while submitting write-up of exercise.

Progressive Assessment Sheet

<table>
<tr><th>Sr.No.</th><th>Experiment/
Practical Outcome</th><th>Page</th><th>Date of
Perform</th><th>Date of
Submision</th><th>Marks
(10)</th><th>Dated Sign</th><th>Remarks</th></tr>
<tr><td>1</td><td>Assume six devices are arranged, if in:
a) bus topology b) ring topology
c) star topology d) mesh topology
Find out number of cables (links), ports needed in each device and total number of ports needed in entire network for each of above stated topology.</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>Study about OSI model network Layers.</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td>Prepare and Test Straight UTP Cable and Cross UTP Cable.</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td>Study and Test various Network devices available at Department/Institute. (Repeater, Hub, Switch, Bridge, Router and Gateway).</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td>Determine whether following IPv4 address are valid or invalid. If valid IPv4 addresses then find class, Network and Host ID of an IPv4 address. If invalid IPv4 address then write reason for the same.
a) 1.4.5.5 b) 75.45.301.14
c) 111.56.045.78 d) 192.226.12.11
e) 130.45.151.154 f) 11100010.23.14.67
g) 221.34.7.8.20 h) 240.230.220.89</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>Determine Class and Network Address for given IPv4 address and subnet mask.
<table>
<tr><th>IPv4 address</th><th>Subnet Mask</th><th>Class</th><th>Subnet</th></tr>
<tr><td>172.16.2.10</td><td>255.255.255.0</td><td></td><td></td></tr>
<tr><td>10.6.24.20</td><td>255.255.240.0</td><td></td><td></td></tr>
<tr><td>10.30.36.12</td><td>255.255.255.0</td><td></td><td></td></tr>
</table></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7</td><td>Subnet the IP address 216.21.5.0 into 30 hosts in each subnet</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>8</td><td>Identify valid IPv6 addresses and if invalid IPv6 address then write reason for the same.
a) 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888
b) : :
c) 225.1.4.2
d) 2001: db8: :
e) : : 1234 : 5678
f) 2001 : db8: : 1234 : 5678
g) 2001:0db8:0001:0000:0000:0ab9:C0A8:0102
h) fe80:2030:31:24</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>9</td><td>Study of firewall in providing network security.</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>10</td><td>MicroProject</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5">Total</td><td></td><td colspan="2"></td></tr>
</table>

Date: ……

Practical No.1:

Assume six devices are arranged, if in:

a) bus topology b) ring topology

c) star topology d) mesh topology

Find out number of cables (links), ports needed in each device and total number of ports needed in entire network for each of above stated topology.

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Problem analysis: (PO2)** Identify and analyse well-defined Computer Engineering problems using codified standard methods.
3. **Design/development of solutions: (PO3)** Design solutions for Computer Engineering well-defined technical problems and assist with the design of systems components or processes to meet specified needs.
4. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
5. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

1. Identify need of computer network.
2. Line Configuration identification skills.
3. Topology identification skills.

C. Relevant Course Outcomes

Classify various types of networks base on their construction, usage and scope.

D. Practical Outcome

1. To differentiate various line configuration
2. To design a computer network considering particular topology
3. To categorise computer network based on scope and connection.

E. Relevant Affective domain related Outcome(s)

- Follow safety measure.
- Follow ethical practices.

F. Prerequisite Theory:

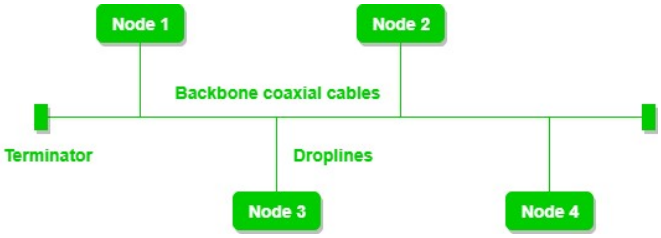
What is a Network Topology?

Topology defines the structure of the network of how all the components are interconnected to each other.

Main Types of Network Topologies

- Bus
- Star
- Ring
- Mesh

Bus:- Bus topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.



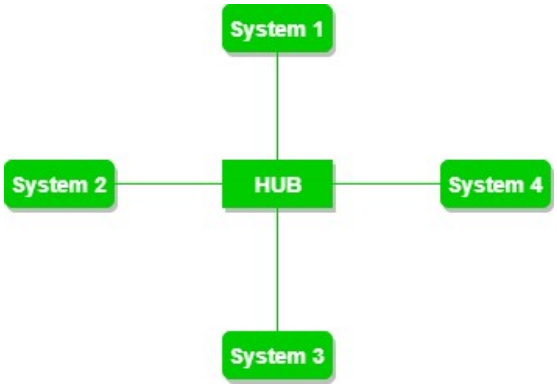
Advantages:-

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages:-

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both the ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.

Star:- In star topology, all the devices 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. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.



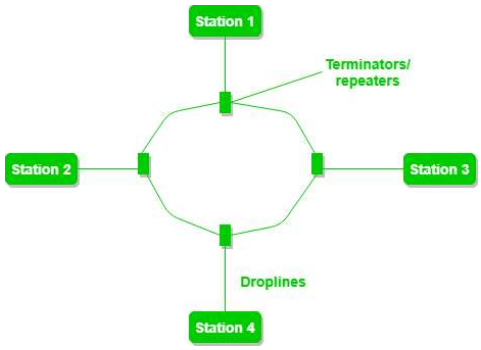
Advantages:-

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages:-

- Requires more cables length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than bus topologies because of the cost of the concentrators.
- Performance is based on the single concentrator i.e. hub.

Ring:- In ring topology where device are connected to make a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are called a ring network.



Advantages:-

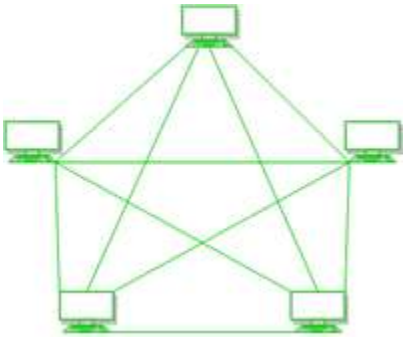
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages:-

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.

- Less secure.

Mesh:- Mesh topology is a type of network topology in which all devices in the network are interconnected.



Advantages:-

- Communication is very fast between the nodes.
- It is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages:-

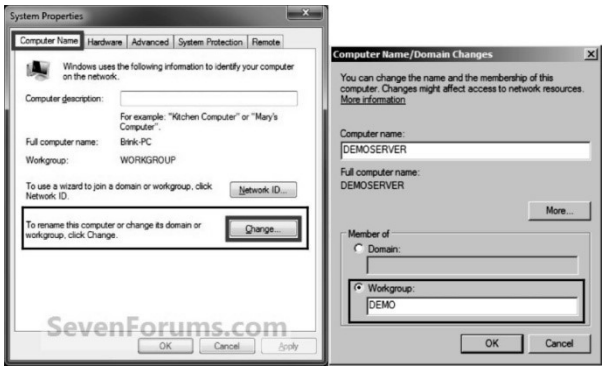
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

G. Resources Required

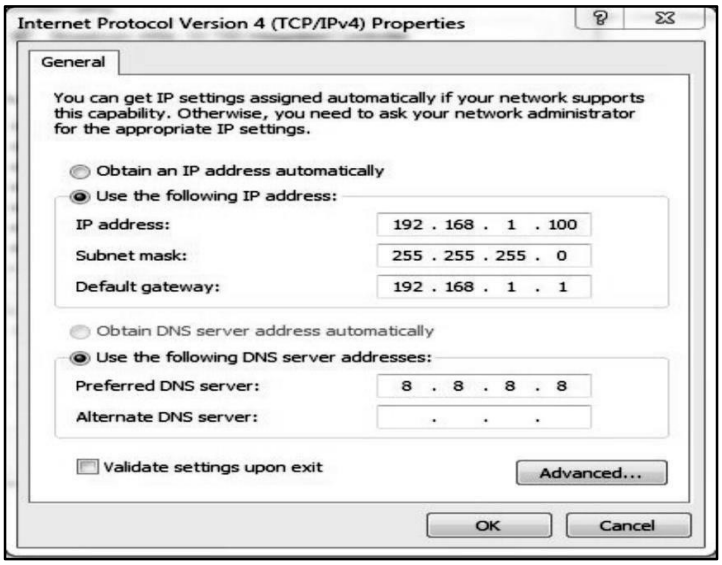
- A set of computers with updated configuration.
- Switch / Hub
- Transmission media and connector

H. Safety and necessary Precautions

1. Handle carefully network devices.
2. Follow safety Practices
3. Check workgroup of computer or write name of workgroup under which all computers are connected to eachother.



- Assign IP address to computer using TCP/IP configuration.



Note :

1. The computers connected to switch or Hub must come under same workgroup.
2. IP address of each computer must be unique.

- Use ping command to check whether computer connected in network.
- Once whole network is formed, then go to Network and check whether all computers are connected in network or not.

I. Procedure

Teacher shall explain structure, advantage and disadvantage of each topology.

- Physical formation of star topology:
  1. Power on the computers that want to connect in star topology and confirm whether operatingsystem and NIC card is properly working.
  2. Power on the central device i.e. switch or hub.
  3. Take cable and connect one end of one cable to port of the switch or hub and connect another end of the same cable to computer's NIC port.
  4. The lights on port of the switch or hub and computer's NIC port should turn on. (On some devices,the lights will flicker on and off; this is normal activity.)
  5. This is the physical formation of star topology.

J. Actual procedure followed (for remaining topology/ Find out number of cables (links), ports needed in each device and total number of ports needed in entire network for each of above stated topology)

……

……

……

……

……

……

……

……

……

……

……

……

K. Observations:

L. Conclusion

1. Components arrangement in network done in_____(Physical/Logical) topology.
2. In the laboratory computer is connected to_____(hub/switch) with_____ports to from star topology.
3. How many cables are required to connect 4 computers using following topologies?
   i. a. Bus - b. Ring - c. Star - d. Mesh –
4. Which topology is preferred if used want to connect 3 computers to each other? Why?

M. Practical related Quiz.

1. Define topology.

   ……

   ……

   ……

   ……

   ……

2. List out types of topology

   ……

.....

.....

.....

.....

3. How to check whatever physical formation of star topology completed or not?

.....

.....

.....

.....

N. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.2:

Study about OSI model network Layers.

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)**Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Life-long learning: (PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Understand concept of OSI model.
b. Describe functions of each layer.
c. Compare OSI and TCP/IP Model.

C. Relevant Course Outcomes

Select proper transmission media and devices based on network requirements.

D. Practical Outcome

a. To study OSI reference model
b. To compare OSI and TCP/IP model

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

The OSI Model is based on the proposal developed by international standard organization (ISO) as a first step towards international standardization of protocols used in various layers.

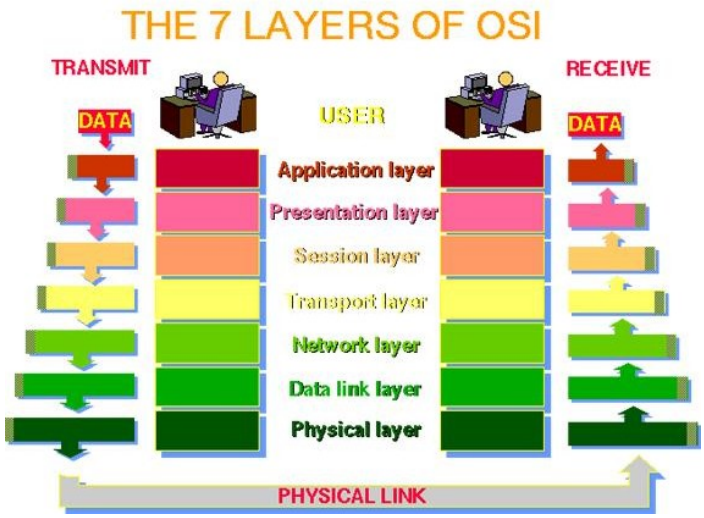
Model is called ISO OSI (open system interconnection) reference model, because it deals with connecting open systems (i.e. system that are open for communication with other systems).

OSI model has seven layers. The principles applied to the seven layers are as follows:

- A layer should be created where different level of abstraction is needed.
- Each layer define a well define function.
- The function of each layer should be chosen to minimize the information flow across the interface.
- The no of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwidely.

Note: the OSI model itself is not networking architecture because it does not specify exact services and protocols to be used in each layer. it just tells what each layer should do.

Various layers are shown in figure:



Physical layer:-
It is connected with transmitting raw bits over a communication channel.

The design issues have to do with making sure that when one side sends a 1 bit, other side as a 1bit not as a 0 bit receives it.

The volts used to represent a 1 or 0 bit, the direction of transmission, initial connection establishment, pins of NIW connector, function of each pins etc. point should be considered.

The design issues here largely deal with mechanical, electrical & procedural interfaces and physical transmission medium.

Data link layer:-

Main task to take a row transmission facility and transform it into a line that appears free of undetected transmission errors to N/W layers.

It accomplishes this map data up into data frames transmit the frames sequentially & process the acknowledgement frames sent back by the receiver.

Data link layer creates and recognizes frame boundaries.

Noise burst on line can destroy a frame completely. Data link layer s/w on source m/c can RETRANSMIT the frame. This layer also solves the problem caused by damaged, lost & duplicate frames.

Another issues that arise are how to keep the fast transmitter from drawing a slow receiver in data, how to deal if line is used to transmit data in both directions, how to control access toshared channel in case of broadcast networks.

Network layer:-

It is concerned with controlling operations of SUBNET. A key design issue is determining how packets ate routed from source to destination.

If too many packets in subnets at same time, they will get in each other's way. Forming bottlenecks. The controls such congestion also belongs to N/W layer.

Since operators of the subnet may well expect remuneration for their efforts there is often some accounting function built into n/w layer.

When a network travels from one n/w to another to get its destination, many problems can arise. It is up to n/w layer to overcome all this problems to allow heterogeneous n/w to be interconnected.

In broadcast n/w, routing problem is simple, so n/w layer is thin or even nonexistent.

Transport layer:-

This layer accept data from session layer, split it up into smaller units if need be pass these to n/w layer and ensure that the pieces all arrives correctly at other end.

Under normal condition, transport layer creates a distinct n/w connection required by session layer. If creating or, maintaining a n/w connection is expensive, the transport layer mightmultiplex several transport connections on to same n/w connection to reduce cost.

It also determines what types of services to provide session layer, and ultimately user of networks.

Transport layer is true end-to- end layer, from source to destination:

In other words, a program on source m/c carries on a conversation with a similar program on a destination m/c, using message header and control messages.

If hosts are multi programmed then need to be someone channel, the transport layer must take care of establishing and deleting connection across n/w. this requires naming mechanism and flow control.

Session Layer:-

It allows user on different m/c to establish session between them. A session allows ordinary data transport and also provide enhanced services useful in some applications. A session might be used to allow a user to log into a remote time sharing system or transfer file between 2 m/cs.

SERVICES:

- To manage dialogue control.
- Token management.
- Synchronization.

Presentation Layer:-

It performs function that is requested sufficiently often to warrant finding solution for them, rather then letting each user solve. It is concerned with SYNTAX and SYMENTEC of information transmitted.

SERVICES:

Encoding data in a standard agreed upon way. In order to make it possible for computers with different presentation to communicate, the data structure to be exchanged can be defined in abstracted way, along with a standard encoding to be used “on the wire”.

The presentation layer manages these abstract data structure and converts from representation used inside the computer to n/w standard representation and back.

Application layer:-

It contains a variety of protocols that are commonly needed.

There is hundreds of incompatible terminal type in the world. Consider the right of the full screen editor that all to work over n/w with many different terminal types with different screen layout, escape sequence for inserting and deleting text, moving cursor etc.

One solution is to define on abstract n/w VIRTUAL TERMINAL that editor and other programs can be written to deal with. All the virtual terminal software is in application layer.

Another function is FILE TRANSFER. Transferring file between two different systems requires handling incompatibilities. This work belongs to application layer.

G. Procedure

1. Teacher shall explain OSI model & function of each Layer
2. Teacher shall also explain TCP/IP mode
3. Teacher will enlist differences between OSI model and TCP/IP model

H. Actual procedure followed

……

……

………

………

………

………

……

………

……

………

……

………

………

………

………

………

………

………

……

………

………

………

………

………

………

………

……

………

………

………

………

I. Observations:

J. Conclusion

1. The acronym OSI stands for _____ in computer networking.
2. Who developed standards of OSI reference model?
3. How many layers are there in OSI reference mode of networking?
4. Choose the correct layer numbers and names of the OSI model below.
   A) Layer 7 - Application Layer, Layer 6 - Presentation Layer
   B) Layer 5 - Session Layer, Layer 4 - Transport Layer
   C) Layer 3 - Network Layer, Layer 2 - Data Link Layer, Layer 1 - Physical Layer
   D) All the above.

K. Practical related Quiz.

1. Write the list of protocols work at different layers

.....

.....

.....

.....

.....

.....

.....

2. Compare OSI model and TCP/IP model

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.3:

Prepare and Test Straight UTP Cable and Cross UTP Cable.

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Problem analysis: (PO2)** Identify and analyse well-defined Computer Engineering problems using codified standard methods.
3. **Design/development of solutions: (PO3)** Design solutions for Computer Engineering well-defined technical problems and assist with the design of systems components or processes to meet specified needs.
4. **Engineering Tools, Experimentation and Testing:** (**PO4)** Apply modern Computer Engineering tools and appropriate technique to conduct standard tests and measurements.
5. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.

B. Competency and Practical Skills

a. Identify different network cable.
b. Prepare straight and crossover network cable.
c. Test network cable.

C. Relevant Course Outcomes

Select proper transmission media and devices based on network requirements.

D. Practical Outcome

a. Understand Use and color code of network cable.
b. Understand use of connecter and crimping tool.
c. Understand the procedure to create straight cable and crossover cable.

E. Relevant Affective domain related Outcome(s)

- Follow safety measure.
- Follow ethical practices.

F. Prerequisite Theory:

1. Straight network cable

- It is a type of Ethernet cable used to connect computing devices together directly.
- Straight through or patch cables were used to connect from a host network interface controller (a computeror similar device) to a network switch, hub or router.
- Both sides (side A and side B) of cables have wire arrangement with same color.
- These are used when connecting Data Terminating Equipment (DTE) to Data Communications Equipment(DCE)

Pin ID	Side A	Side B
1	Orange - White	Orange - White
2	Orange	Orange
3	Green - White	Green - White
4	Blue	Blue
5	Blue - White	Blue - White
6	Green	Green
7	Brown - White	Brown - White
8	Brown	Brown

2. Crossover network cable :

- It is used to connect two devices of the same type : two computers or two switches to each other.
- Both sides (side A and side B) of cable have wire arrangement with different color.
- These are used when connecting Data Terminating Equipment (DTE) to Data Terminating Equipment (DTE) or Data Communications Equipment (DCE) to Data Communications Equipment (DCE)

Pin ID	Side A	Side B
1	Orange - White	Orange - White
2	Orange	Orange
3	Green - White	Green - White
4	Blue	Blue
5	Blue - White	Blue - White
6	Green	Green
7	Brown - White	Brown - White
8	Brown	Brown

BACKGROUND/PREPARATION:-

In this lab you will learn how to build a Category 5 (CAT 5) Unshielded Twisted Pair (UTP) Ethernet network patch cable (or patch cord) and test it for good connections and correct pin outs (correct colour wires on the correct pin). This will be 4-pair (8 wires) "straight through" cable, which means that the colour of wire on pin 1 on one end of the cable will be the same as pin 1 onthe other end. Pin 2 will be the same as pin 2, and so on. It will be wired to EIA/TIA 568-B or A standards which determines what colour wire is on each pin. This patch cable can be used in a workstation NIC to the wall plate data jack, or it can be used in the wiring closet to connect the patch panel (horizontal cross connect) to an Ethernet hub or switch. Patch cables are wired straight through because the cable from the workstation to the hub or switch is normally crossed over automatically at the switch or hub. Note that the ports on most hubs have an X next to them. This means the send and receive pairs will be crossed when the cabling reaches the switch. The pin outs will be T568-B, and all 8 conductors (wires) should be terminated with RJ45 modular connectors (only 4 of the 8 wires are used for 10/100Base-T Ethernet; all 8 are used for 1000Base-T Ethernet).

G. Resources Required

1. Two to three foot length of CAT5 cabling (one per person or one per team)
2. Two RJ45 connectors
3. RJ crimping tools to attach the RJ45 connectors to the cable ends
4. Ethernet cabling continuity tester that can test crossover type cables (T568-A to 568-B)
5. Wire cutters
6. Cable jacket stripper.

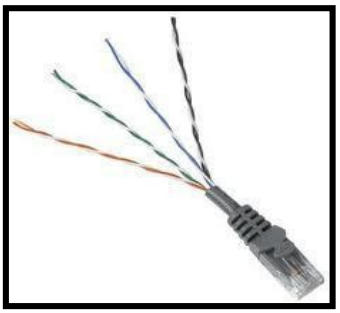


Figure 1: A short section of CAT 5 cable

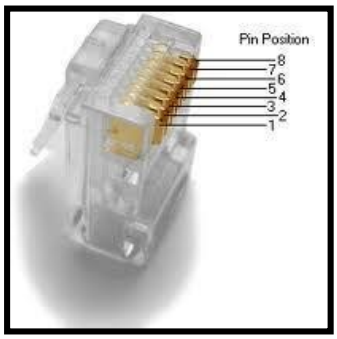


Figure 2: An RJ-45 connector

Figure 3: A combination wire stripping/crimping tool

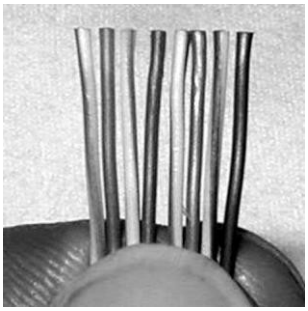
Figure 4: Cable testers

H. Procedure

- Prepare straight and crossover cable :
- Cut into the plastic sheath 1 inch from the end of cut cable. The crimping tool has a razor blade that will do trick.

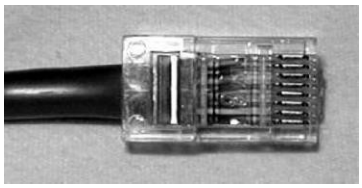
- Unwind it and pair of the similar colors.

- Pinch the wires between your fingers and straighten them out.



- Use scissors to make a straight cut across the wires 1/2 Inch from the cut sleeve to the end of the wires
- Push the wires into the connector.

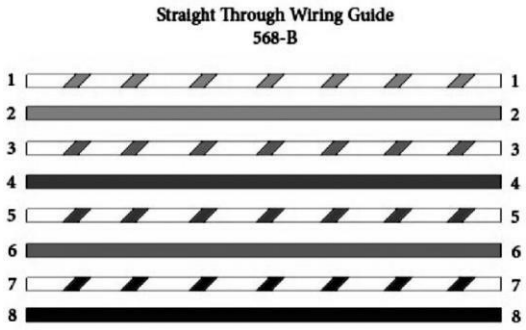
- A view from the top. All the wires are all the way in. There are no short wires.



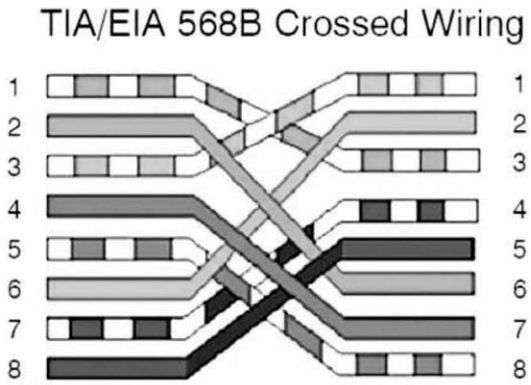
- CRIMPING THE CABLE: carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is alsoa locking tab that holds the blue plastic sleeve in place for a tight compression fit.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

- For a Straight cable, repeat all steps on the other end of the Ethernet cable exactly. For a cross-over cable.make sure to get the color order right as per given on next page :

Connector A		Connector B
Pin 1		Pin 1
Pin 2		Pin 2
Pin 3		Pin 3
Pin 4		Pin 4
Pin 5		Pin 5
Pin 6		Pin 6
Pin 7		Pin 7
Pin 8		Pin 8



Connector A		Connector B
Pin 1		Pin 3
Pin 2		Pin 6
Pin 3		Pin 1
Pin 4		Pin 7
Pin 5		Pin 8
Pin 6		Pin 2
Pin 7		Pin 4
Pin 8		Pin 5



- Make sure to test the cables using line tester before installing them. An inexpensive Ethernet cable testerdoes this quite well

G. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

H. Observations:

a. Prepare straight network and crossover network cable and write the name of color of each pins of both side in the table:

Pin no./id	Straight cable		Crossover cable	
	Side A	Side B	Side A	Side B
1	Orange-white	Orange-white		
2				
3				
4				
5				
6				
7				
8				

I. Conclusion

1. To connect switch to switch……(Straight/Crossover) cable is used.
2. UTP cables consist of…….. (2/4/8) pairs.

3. In crossover cable colors at both sides of cable are ..... (Same/different)
4. Complete the following table by writing type of the cable required to connect two devices.

Device	Switch	Router	computer
Switch	**Straight**		
Router			
Computer			

J. Practical related Quiz.

1. State the purpose to prepare straight network cable.

.....

.....

.....

.....

.....

.....

2. State the purpose to prepare cross network cable.

.....

.....

.....

.....

.....

.....

3. State the purpose to use RJ45 connector

.....

.....

.....

.....

.....

4. Give the names of RJ45 pinout for each pin along with pin number.

.....

.....

.....

.....

.....

K. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.4:

Study and Test various Network devices available at Department/Institute. (Repeater, Hub, Switch, Bridge, Router and Gateway).

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Engineering Tools, Experimentation and Testing:** (**PO4)** Apply modern Computer Engineering tools and appropriate technique to conduct standard tests and measurements.
3. **Life-long learning: (PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Identify need of connecting two computer networks
b. Internetworking devices identification skills.

C. Relevant Course Outcomes

Classify various types of networks base on their construction, usage and scope.

D. Practical Outcome

a. To differentiate various internetwork devices
b. Identify usage of various internetwork devices.

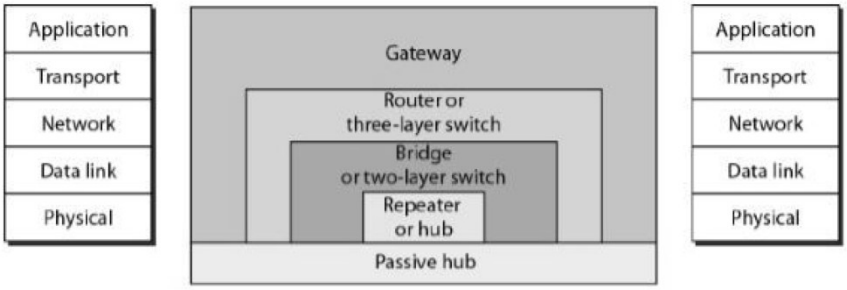
E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

When two or more separate networks are connected for exchanging data or resources, they become an internetworking (or internet). Linking number of LANs into an internet requires additional devices which are called as internetworking devices. Routers and Gateways these devices are designed to overcome obstacles to interconnection without

disrupting the independent functioning of the networks. Figure given below shows various internetworking devices.



Repeaters:

- Repeaters are network devices operating at the physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area. They are also known as signal boosters.
- Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern.
- A repeater can extend the physical length of a LAN.
- The location of a repeater on a link is vital. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of its bits.
- If the corrupted bit travels much farther, however, accumulated noise can change its meaning completely. At that point, the original voltage is not recoverable, and the error needs to be corrected.

Types of Repeaters: According to the types of signals that they regenerate, repeaters can be classified into two categories:

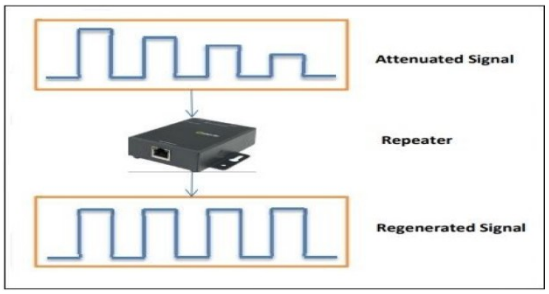
- Analog Repeaters − can only amplify the analog signal.
- Digital Repeaters − can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types:

- Wired Repeaters are used in wired LANs.
- Wireless Repeaters are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories:

- Local Repeaters − They connect LAN segments separated by small distance.
- Remote Repeaters − They connect LANs that are far from each other.



Advantages of Repeaters:

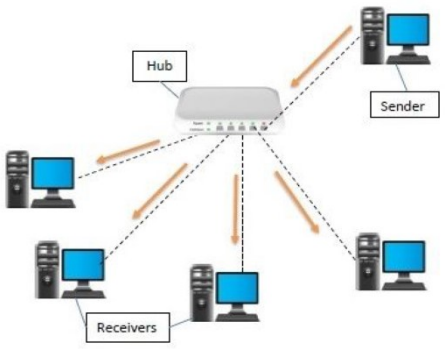
- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters:

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

Hub:

- A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
- A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.
- When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



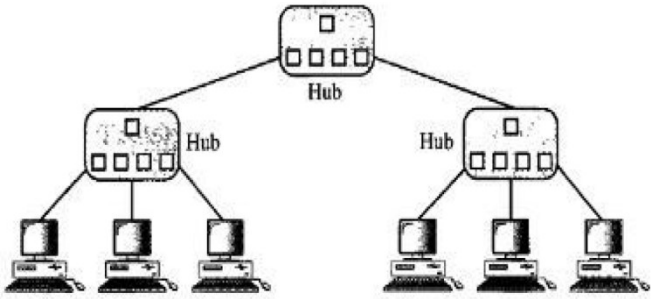
Types of Hubs:

Passive Hubs: A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.

This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Active Hubs: An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. However, hubs can also be used to create multiple levels of hierarchy, as shown in Figure. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).

Intelligent Hubs: Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc

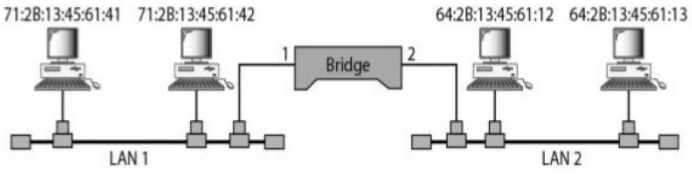


Bridges:

- A bridge operates in the physical layer as well as in the data link layer. It can regenerate the signal that it receives and as a data link layer device, it can check the physical addresses of source and destination contained in the frame.
- The major difference between the bridge and the repeater is that the bridge and the repeater is that the bridge has a filtering capability.
- That means it can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is forwarded, then the bridge should specify the port over which it should be forwarded.

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table



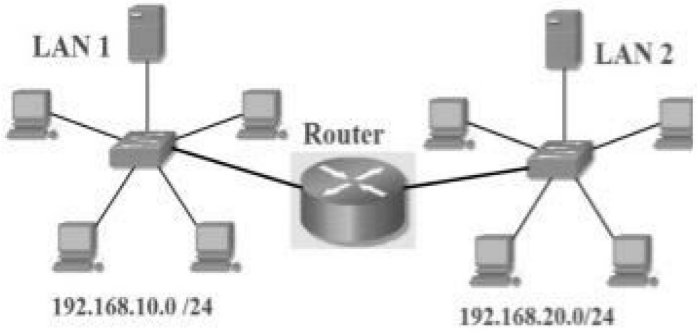
Types of Bridges :

Transparent Bridges:- These are the bridges in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations are unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges:- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can discover frames by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

Router:

- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.
- A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols. Data is grouped into packets, or blocks of data.
- Each packet has a physical device address as well as logical network address. The network address allows routers to calculate the optimal path to a workstation or computer.
- The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent
- A routing table typically contains the following entities −
  - IP addresses and subnet mask of the nodes in the network
  - IP addresses of the routers in the network
  - Interface information among the network devices and channels
- Routing tables are of two types –
  Static Routing Table − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
  Dynamic Routing Table − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large numbers of routers.



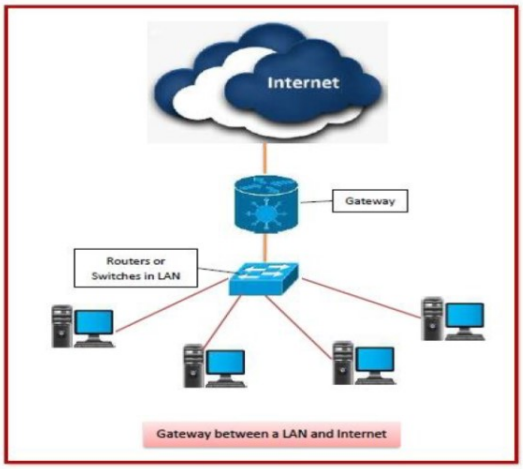
Types of Routers:

A variety of routers are available depending upon their usages. The main types of routers are as follows :-

- Wireless Router − They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while it's 300 feet for outdoor connections.
- Broadband Routers − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- Core Routers − They can route data packets within a given network, but cannot route the packets between the networks. They help to link all devices within a network thus forming the backbone of the network. It is used by ISP and communication interfaces.
- Edge Routers − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use the Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
- Brouters − Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Gateway:

- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model.
- However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model.
- It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway.
- Only the internal traffic between the nodes of a LAN does not pass through the gateway.
- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenarios, a gateway node may be supplemented as a proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses a packet switching technique to transmit data across the networks.



Types of Gateways :

On basis of direction of data flow, gateways are broadly divided into two categories −

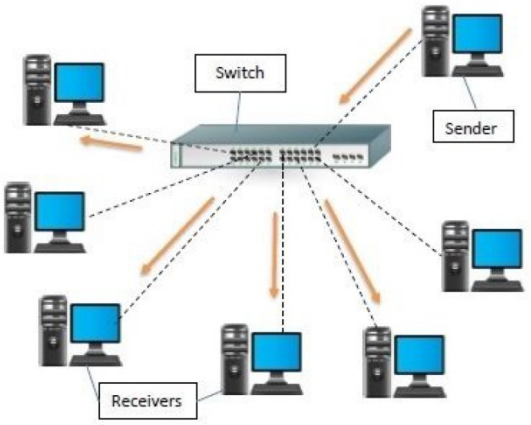
- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

- **Network Gateway** − This is the most common type of gateway that provides an interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.
- **Cloud Storage Gateway** − It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.
- **Internet-To-Orbit Gateway (I2O)** − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).
- **IoT Gateway** − IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud networks and user applications.
- **VoiP Trunk Gateway** − It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

Switch:

- A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.
- Like a hub, a switch also has many ports, to which computers are plugged in.



- However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s).
- Thus, it supports both unicast and multicast communications.
- We can have a two-layer switch or a three-layer switch.
- A three-layer switch is used at the network layer; it is a kind of router.
- The two-layer switch performs at the physical and data link layers.
- A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance.
- A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.
- This means no competing traffic (no collision, as we saw in Ethernet).
- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC Address of the frame it received.
- However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing.
- It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

G. Procedure

1. Teacher shall explain all internetworking devices
2. Teacher will give demo of testing various internetworking devices available in institute.

H. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

……

I. Observations:

J. Conclusion

1. _____ (Gateway/ Switch)device connects networks with different protocols.
2. _____ (Hub/Router) is used to connect a number of LANs.
3. Which networking device connect one LAN to other LAN using same protocol? (Switch/Router)

K. Practical related Quiz.

1. Why we need internetworking devices?

……

……

……

……

……

2. List out various internetworking devices.

……

……

……

……

……

3. How can you manage a network using a router?

.....

.....

.....

.....

.....

.....

.....

.....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.5:

Determine whether following IPv4 address are valid or invalid. If valid IPv4 addresses then find class, Network and Host ID of an IPv4 address. If invalid IPv4 address then write reason for the same.

a) 1.4.5.5
b) 75.45.301.14
c) 111.56.045.78
d) 192.226.12.11
e) 130.45.151.154
f) 11100010.23.14.67
g) 221.34.7.8.20
h) 240.230.220.89

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
3. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Learning basics of IPv4 addressing scheme.
b. Identify valid and invalid IPv4 address
c. Network class identification skills.

C. Relevant Course Outcomes

Compare IPv4 and IPv6 addressing scheme

D. Practical Outcome

a. Know importance of IPv4 address
b. Know notation of IPv4 address
c. Identify valid and invalid IP addresses
d. Categorise IPv4 addresses according to types

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

IPv4 address

An IP (Internet Protocol) 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. The IP address is also called IP number or internet address. It helps you to specify the technical format of the addressing and packets scheme. Most networks combine TCP with IP.

IPv4 was the primary version brought into action for production within the ARPANET in 1983. The IPv4 addresses are represented in dot-decimal notation and has the following format: x . x . x . x where *x* is a decimal number (ranging from 0 to 255). These four numbers are separated by three dots. IPv4 addresses are 32-bit integers which will be expressed in decimal notation.

An example of a valid IP is: 129.142.30.56. IP Address is divided into two parts:

- Prefix: The prefix part of IP address identifies the physical network to which the computer is attached. . Prefix is also known as a network address.
- Suffix: The suffix part identifies the individual computer on the network. The suffix is also called the host address.

Parts of IPv4

- **Network part:** The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:** The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
- For each host on the network, the network part is the same, however, the host half must vary.
-

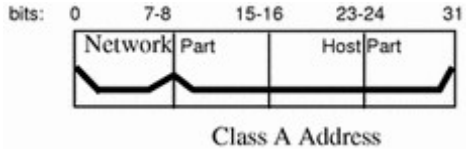
Network Classes

The first step in planning for IP addressing on your network is to determine which network class is appropriate for your network. After you have done this, you can take the crucial second step: obtain the network number from the InterNIC addressing authority.

Currently there are three classes of TCP/IP networks. Each class uses the 32-bit IP address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

Class A Network Numbers

Class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address, as illustrated in figure below.

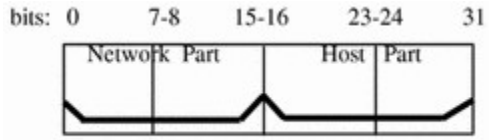


Class A Address

The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 classes A networks can exist. Each one of these numbers can accommodate up to 16,777,214 hosts.

Class B Network Numbers

A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the InterNIC, and comprise the network address. The last two bytes, 50.56, make up the host address, and are assigned at the discretion of the owner of the network number. Figure given below graphically illustrates a class B address.

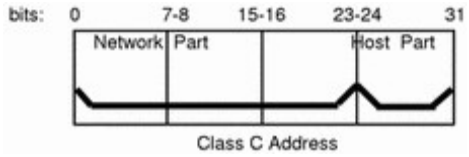


Class B Address

Class B is typically assigned to organizations with many hosts on their networks.

Class C Network Numbers

Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at the discretion of the network owners. Figure given below graphically represents the bytes in a class C address.



The first byte of a class C network number covers the range 192-223. The second and third each cover the range 1- 255. A typical class C address might be 192.5.2.5. The first three bytes, 192.5.2, form the network number. The final byte in this example, 5, is the host number.

Administering Network Numbers

If your organization has been assigned more than one network number, or uses subnets, appoint a centralized authority within your organization to assign network numbers. That authority should maintain control of a pool of assigned network numbers, assigning network, subnet, and host numbers as required. To prevent problems, make sure that duplicate or random network numbers do not exist in your organization.

Designing Your IP Addressing Scheme

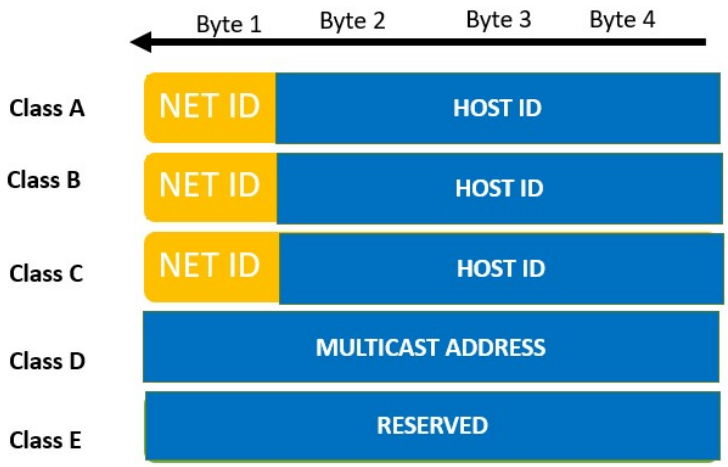
After you have received your network number, you can then plan how you will assign the host parts of the IP address.

Table given below shows the division of the IP address space into network and host address spaces. For each class, "range" specifies the range of decimal values for the first byte of the network number. "Network address" indicates the number of bytes of the IP address that are dedicated to the network part of the address, with each byte represented by *xxx*. "Host address" indicates the number of bytes dedicated to the host part of the address. For example, in a class A network address, the first byte is dedicated to the network, and the last three are dedicated to the host. The opposite is true for a class C network.

Table :Division of IP Address Space

Class	Range	Network Address	Host Address
A	0-127	*xxx*	*xxx.xxx.xxx*
B	128-191	*xxx.xxx*	*xxx.xxx*
C	192-223	*xxx.xxx.xxx*	*xxx*
D	224-239	Reserved for multicast groups	
E	240-254	Reserved	

The numbers in the first byte of the IP address define whether the network is class A, B, or C and are always assigned by the InterNIC. The remaining three bytes have a range from 0-255. The numbers 0 and 255 are reserved; you can assign the numbers 1-254 to each byte **depending on the network number assigned to you**.



G. Procedure

Teacher shall explain about

- Basics of IP addresses
- IPv4 addressing scheme
- How to identify valid and invalid IPv4 addresses
- How to classify IPv4 addresses in different classes

H. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

……

……

I. Observations:

J. Conclusion

1. Which of this is not a class of IP address?
   a) Class E
   b) Class C
   c) Class D
   d) Class F

2. Network addresses are a very important concept of _____
   a) Routing
   b) Mask
   c) IP Addressing
   d) Classless Addressing

3. The last address of IP address represents
   a)Unicast address
   b) Broadcast address
   c) Network Address
   d) None of these

K. Practical related Quiz.

1. Why IP addresses are needed?

.....

.....

.....

.....

.....

2. How to check IPv4 address on Windows and mobile phone?

.....

.....

.....

.....

.....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.6:

Determine Class and Network Address for given IPv4 address and subnet mask.

IPv4 address	Subnet Mask	Class	Subnet (network address)
172.16.2.10	255.255.255.0		
10.6.24.20	255.255.240.0		
10.30.36.12	255.255.255.0		

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Problem analysis: (PO2)** Identify and analyse well-defined Computer Engineering problems using codified standard methods.
3. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
4. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Learning importance of subnetting.

C. Relevant Course Outcomes

Compare IPv4 and IPv6 addressing scheme

D. Practical Outcome

a. Know importance of subnetting

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

Subnetting

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN).

Subnets were initially designed for solving the shortage of IP addresses over the Internet.

Each IP address consists of a subnet mask. All the class types, such as Class A, Class B and Class C include the subnet mask known as the default subnet mask. The subnet mask is intended for determining the type and number of IP addresses required for a given local network. The firewall or router is called the default gateway. The default subnet mask is as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

The subnetting process allows the administrator to divide a single Class A, Class B, or Class C network number into smaller portions. The subnets can be subnetted again into sub-subnets.

Dividing the network into a number of subnets provides the following benefits:

- Conservation of IP addresses: Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.
- Reduced network traffic: The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.
- Simplification: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

How to Subnet

To better understand the concept of subnetting, imagine a network with a total of 256 addresses (a Class C network). One of these addresses is used to identify the network address and another one is used to identify the broadcast address on the network. Therefore, we are left with 254 addresses available for addressing hosts.

If we take all these addresses and divide them equally into 8 different subnets we still keep the total number of original addresses, but we have now split them into 8 subnets with 32 addresses in each. Each new subnet needs to dedicate 2 addresses for the subnet and broadcast address within the subnet.

The result is that we eventually come up with 8 subnets, each one possessing 30 subnet addresses available for hosts. You can see that the total amount of addressable hosts is reduced (240 instead of 254) but better management of addressing space is gained.

Now that we have subnet mask explained, I'll now use a couple of examples to help explain how an IP address subnet mask can be calculated as clearly as possible, but first, here is a quick explanation of "What is a subnet mask?" An IP subnet mask is a number used for defining a range of IP addresses that are available within a network.

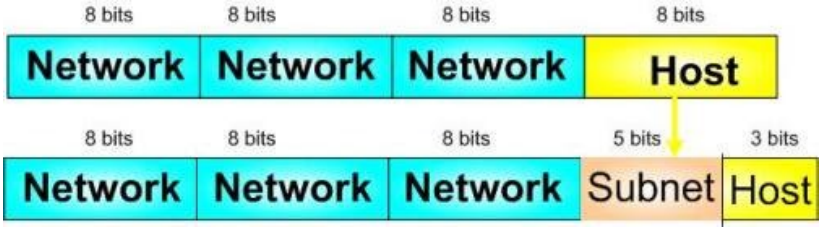
How to Subset a Class C Address Using the Binary Method

It can be helpful to know how to be your own subnet mask calculator. Subset a Class C address with the binary method by following these four steps (which will be explained in more detail below):

1. Convert to binary.
2. Calculate the subset address.
3. Find host range.
4. Calculate the total number of subsets and the hosts per subnet.

We will use a Class C address, which takes 5 bits from the Host field for subnetting and leaves 3 bits for defining hosts as shown in figure 1 below. Having 5 bits available for defining subnets means that we can have up to 32 (2^5) different subnets.

It should be noted that in the past using subnet zero (00000---) and all-ones subnet (11111---) was not allowed. This is not true nowadays. Since Cisco IOS Software Release 12.0 the entire address space including all possible subnets is explicitly allowed.



Let's use IP address 192.168.10.44 with subnet mask 255.255.255.248 or /29.

- Step 1: Convert to Binary

IP Address (Decimal)	**192.**	**168.**	**10.**	**44**
IP Address (Binary)	11000000	10101000	00001010	00101100
Subnet Mask (Binary)	11111111	11111111	11111111	11111000
Subnet Mask (Decimal)	**255.**	**255.**	**255.**	**248**

- Step 2: Calculate the Subnet Address

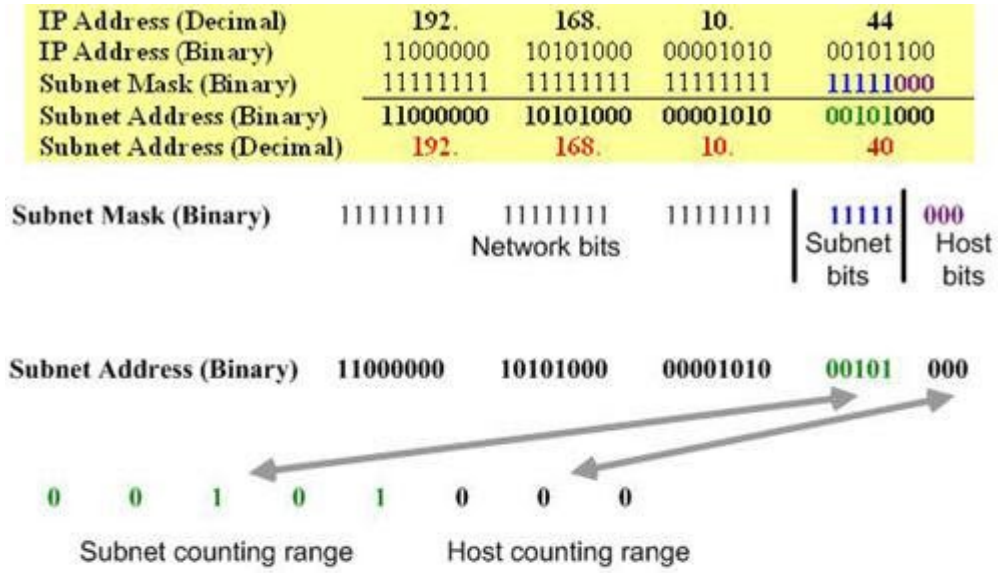
To calculate the IP Address Subnet you need to perform a bit-wise AND operation (1+1=1, 1+0 or 0+1 =0, 0+0=0) on the host IP address and subnet mask. The result is the subnet address in which the host is situated.

- Step 3: Find Host Range

We know already that for subnetting this Class C address we have borrowed 5 bits from the Host field. These 5 bits are used to identify the subnets. The remaining 3 bits are used for defining hosts within a particular subnet.

The Subnet address is identified by all 0 bits in the Host part of the address. The first host within the subnet is identified by all 0s and a 1. The last host is identified by all 1s and a 0. The broadcast address is the all 1s. Now, we move to the next subnet and the process is repeated the same way.

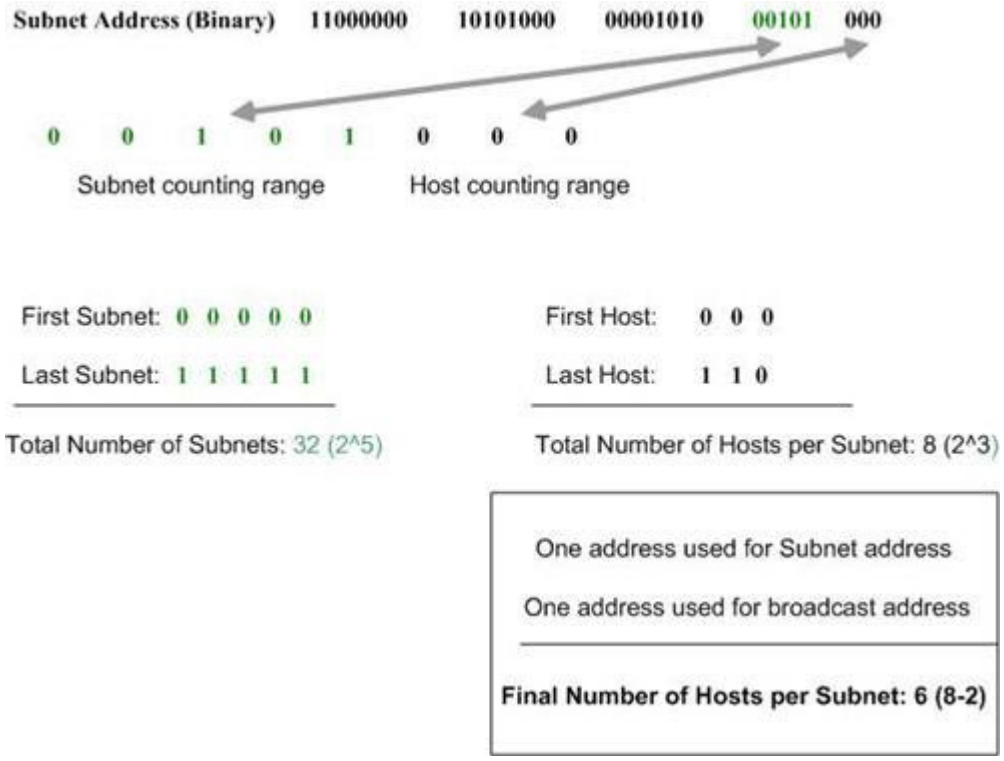
The following diagram clearly illustrates this process:



Subnet:	11000000	10101000	00001010	00101	000
Subnet:	192.	168.	10.	40	
First Host:	11000000	10101000	00001010	00101	001
First Host:	192.	168.	10.	41	
Last Host:	11000000	10101000	00001010	00101	110
Last Host:	192.	168.	10.	46	
Broadcast:	11000000	10101000	00001010	00101	111
Broadcast:	192.	168.	10.	47	
Next Subnet:	11000000	10101000	00001010	00110	000
Next Subnet:	192.	168.	10.	48	

- Step 4: Calculate the Total Number of Subnets and Hosts Per Subnet

Knowing the number of Subnet and Host bits we can now calculate the total number of possible subnets and the total number of hosts per subnet. We assume in our calculations that all-zeros and all-ones subnets can be used. The following diagram illustrates the calculation steps.



How to Subset a Class C Address Using the Fast Way

Now let's see how to subnet the same Class C address using a faster method. Let's again use the IP address 192.168.10.44 with subnet mask 255.255.255.248 (/29).

The steps to perform this task are the following:

1. Total number of subnets: Using the subnet mask 255.255.255.248, number value 248 (11111000) indicates that 5 bits are used to identify the subnet. To find the total number of subnets available simply raise 2 to the power of 5 (2^5) and you will find that the result is 32 subnets. Note that if subnet all-zeros is not used then we are left with 31 subnets and if also all-ones subnet is not used then we finally have 30 subnets.

2. Hosts per subnet: 3 bits are left to identify the host therefore the total number of hosts per subnet is 2 to the power of 3 minus 2 (1 address for subnet address and another one for the broadcast address)(2^3-2) which equals to 6 hosts per subnet.

3. Subnets, hosts and broadcast addresses per subnet: To find the valid subnets for this specific subnet mask you have to subtract 248 from the value 256 (256-248=8), which is the first available subnet address. Actually the first available one is the subnet-zero

which we explicitly note. Next subnet address is 8+8=16, next one is 16+8=24 and this goes on until we reach value 248.

The following table provides all the subnet cal information. Note that our IP address (192.168.10.44) lies in subnet 192.168.10.40.

Subnet	0	8	16	...	40	...	248
First Host	1	9	17	...	41	...	249
Last Host	6	14	22	...	46	...	254
Broadcast	7	15	23	...	47	...	255

G. Procedure

Teacher shall explain about

- Basics of Subnetting
- How to subnet a given network?

H. Actual procedure followed

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

……

……

……

I. Observations:

J. Conclusion

1. If a host on a network has the address 172.16.45.14/30, what is the subnetwork this host belongs to?
   a) 172.16.45.0
   b) 172.16.45.4
   c) 172.16.45.8
   d) 172.16.45.12
2. What is the subnetwork address for a host with the IP address 200.10.5.68/28?
   a) 200.10.5.56
   b) 200.10.5.32
   c) 200.10.5.64
   d) 200.10.5.0
3. To test the IP stack on your local host, which IP address would you ping?
   a) 127.0.0.0
   b) 1.0.0.127
   c) 127.0.0.1
   d) 127.0.0.255

K. Practical related Quiz.

1. When calculating the maximum available valid host addresses in each subnet, why we always minus 2 addresses from total addresses?

   .....

   .....

   .....

   .....

   .....

2. Subnet the Network 203.10.93.0/24 into 25 Subnets. After Subnetting, is IP 203.10.93.30 a valid Host ID?

   1. YES
   2. NO

   .....

.....

.....

.....

.....

3. How many subnets and maximum hosts per subnet can we get from the subnet network 172.27.0.0/23?

.....

.....

.....

.....

.....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.7:

Subnet the IP address 216.21.5.0 into 30 hosts in each subnet

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Problem analysis: (PO2)** Identify and analyse well-defined Computer Engineering problems using codified standard methods.
3. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
4. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Learning importance of subnetting.

C. Relevant Course Outcomes

Compare IPv4 and IPv6 addressing scheme

D. Practical Outcome

a. Subnetting based on host requirement
b. Find number of networks (subnets)
c. Find number of hosts per network (subnet)

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

Subnetting based on host requirement

Five steps of subnetting are:

1. Identify class of IP address and note the Default Subnet Mask.

2. Convert Default subnet mask into binary
3. Note the number of hosts required per network and find the Subnet Generator(SG) and Octet position
4. Generate new Subnet Mask
5. Use SG and generate network ranges (subnets) into the appropriate octet position

Let's suppose we have purchased the address 192.168.100.0 we required to break that address into **62 hosts per network.**

Step 1: Identify class of IP address and note the Default Subnet Mask.

Here address 192.168.100.0 belongs to Class C and Default Subnet Mask of Class C is 255.255.255.0. In class C we have possibilities of 256 IP address but we can't use first IP address and last IP address as first IP address is network address and last IP address is broadcast address. So we have 254 IP addresses but here we need only 62.

Step 2: Identify Convert Default subnet mask into binary

255.255.255.0=11111111.11111111.11111111.00000000

Step 3: Note the number of hosts required per network and find the Subnet Generator(SG) and Octet position

No. of hosts per subnet = 62 (So convert 64 into binary)
62 = 111110 (6bits)

Reserve 6 bits in the subnet mask

So, we need 6 bits in the host portion of the address in our default subnet mask. Our default subnet mask is

255.255.255.0=11111111.11111111.11111111.00000000

Here we need to reserve from right to left in last octet of default subnet mask ie keeping rightmost 6 zeros and remaining bits are to converted to 1's
255.255.255.192=11111111.11111111.11111111.11000000

So the new subnet mask is 255.255.255.192 or /26. So, 62 hosts' needs 6 bits in the host portion.

SG is 64 as first one is at 6^{th} position and 2^6=64 and Octet where we find first one is 4^{th} octet so Octet position=4.

Step 4: Generate new Subnet Mask

The new subnet mask is 255.255.255.192 or /26 is already generated in the last step.

Step 5: Network Ranges (Subnets)

Now for finding the network ranges, our increment is 64 (ie value of SG).

Net	Network ID	Broadcast IP	Total IP Addresses
Net-0	**192.168.100.0** + 000.000.000.64	**192.168.100.63** + 000.000.000.64	64
Net-1	**192.168.100.64** + 000.000.000.64	**192.168.100.127** + 000.000.000.64	64
Net-2	**192.168.100.128** + 000.000.000.64	**192.168.100.191** + 000.000.000.64	64
Net-3	**192.168.100.192** +	**192.168.100.255** +	64

G. Procedure

Teacher shall explain about

- Basics of Subnetting
- How to subnet a given network based on host requirement?

H. Actual procedure followed

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

I. Observations:

J. Conclusion

1. What is broadcast address of third subnet of the problem given to you?

   .....

2. What is the network address of second subnet of the problem given to you?

   .....

K. Practical related Quiz.

1. Find number of networks (subnets) of the solved problem and problem given to you?

   .....

   .....

   .....

2. Find number of hosts per network (subnet) of the solved problem and problem given to

you?

3. Break 201.1.1.0 into networks of 40 hosts each.

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.8:

Identify valid IPv6 addresses and if invalid IPv6 address then write reason for the same.

a) 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888
b): :
c) 225.1.4.2
d) 2001: db8: :
e): : 1234 : 5678
f) 2001 : db8: : 1234 : 5678
g) 2001:0db8:0001:0000:0000:0ab9:C0A8:0102
h) fe80:2030:31:24

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
3. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Identifying need of IPv6 addressing.

C. Relevant Course Outcomes

Compare IPv4 and IPv6 addressing scheme

D. Practical Outcome

a. Know importance of IPv6 address
b. Know notation of IPv6 address
c. Identify valid and invalid IPv6 addresses
d. Difference between IPv4 and IPv6

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

What is an IPv6 Address?

Internet Protocol version 6 (IPv6) is the newest version of the Internet Protocol (IP), Similar to IPv4. IPv6 was introduced to remediate the problems and limitations of IPv4. IPv6 is also referred to as IPnext generation or IPng. IPv6 uses 128 bits to identify a host instead of IPv4's 32 bits. The 128 bits that IPv6 uses allows the address space up to 2^{128} which equates to over 340 undecillion numbers of IP available addresses. The address space of IPv6 is a staggering number compared to ipv4s address space. The number of connected devices to the internet has long outgrown the addressing capacity of IPv4. The adoption of IPv6 has been slow from a technological standpoint. Most Internet Service Providers (ISP) still use IPv4 so version four will still be around for some time. Despite computers supporting IPv6 from the Windows XP era.

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

```
0010000000000001 0000000000000000 0011001000111000 1101111111100001
0000000001100011 0000000000000000 0000000000000000 1111111011111011
```

Each block is then converted into Hexadecimal and separated by ':' symbol:

```
2001:0000:3238:DFE1:0063:0000:0000:FEFB
```

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

```
2001:0000:3238:DFE1:63:0000:0000:FEFB
```

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

```
2001:0000:3238:DFE1:63::FEFB
```

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

```
2001:0:3238:DFE1:63::FEFB
```

Examples of valid IPv6 addresses

The following list shows examples of valid IPv6 (Normal) addresses:

- 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888

- 2001 : db8 : 3333 : 4444 : CCCC : DDDD : EEEE : FFFF
- : : (implies all 8 segments are zero)
- 2001: db8: : (implies that the last six segments are zero)
- : : 1234 : 5678 (implies that the first six segments are zero)
- 2001 : db8: : 1234 : 5678 (implies that the middle four segments are zero)
- 2001:0db8:0001:0000:0000:0ab9:C0A8:0102 (This can be compressed to eliminate leading zeros, as follows: 2001:db8:1::ab9:C0A8:102)

Differences between IPv4 and IPv6

	IPv4	**IPv6**
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.

Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

G. Procedure

Teacher shall explain about

- Need of IPv6 address
- IPv6 address format
- Difference between IPv4 and IPv6 addresses

H. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

I. Observations:

J. Conclusion

1. What is address size of IPv6?
   a) 32 bit
   b) 64 bit
   c) 128 bit
   d) 256 bit

2. IPv6 stands for?
   a) Internet Protocol version 3
   b) Internet Protocol version 4
   c) Internet Protocol version 5
   d) Internet Protocol version 6

K. Practical related Quiz.

1. What are features of IPv6?

……

.....

.....

2. Which statement(s) about IPv4 and IPv6 addresses are true?
   1. An IPv6 address is 32 bits long, represented in hexadecimal.
   2. An IPv6 address is 128 bits long, represented in decimal.
   3. An IPv4 address is 32 bits long, represented in decimal.
   4. An IPv6 address is 128 bits long, represented in hexadecimal.

   a) 1 and 3 only
   b) 2 only
   c) 3 and 4
   d) 2 and 4

3. Which among the following features is present in IPv6 but not in IPv4?
   a) Fragmentation
   b) Header checksum
   c) Options
   d) Anycast address

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.9:

Study of firewall in providing network security.

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
3. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. Identify need of firewall

C. Relevant Course Outcomes

Identify various types of network security threats

D. Practical Outcome

a. To learn importance of Firewall.
b. To get acquainted with different types of Firewalls
c. To enable and disable Firewalls in Windows

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

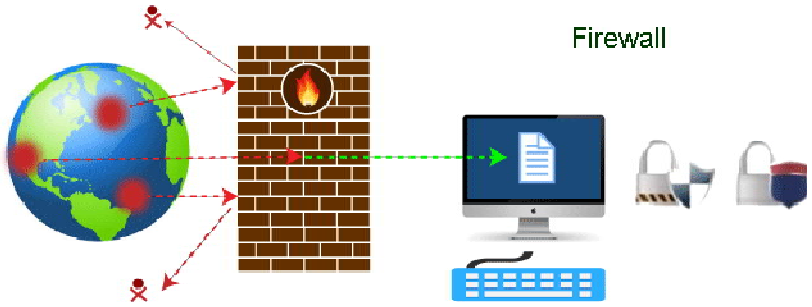
In current scenario, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and

external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

- **Open Access**
  If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks

coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

- **Lost or Comprised Data**
  Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

- **Network Crashes**
  In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again. Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

History of Firewall

Firewalls have been the first and most reliable component of defence in network security for over 30 years. Firewalls first came into existence in the late 1980s. They were initially designed as packet filters. These packet filters were nothing but a setup of networks between computers. The primary function of these packet filtering firewalls was to check for packets or bytes transferred between different computers.

Firewalls have become more advanced due to continuous development, although such packet filtering firewalls are still in use in legacy systems.

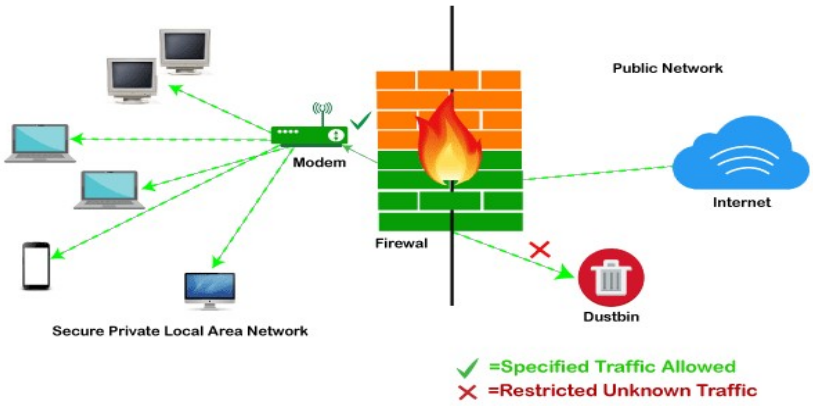
As the technology emerged, Gil Shwed from Check Point Technologies introduced the first stateful inspection firewall in 1993. It was named as FireWall-1. Back in 2000, Netscreen came up with its purpose-built firewall 'Appliance'. It gained popularity and fast adoption within enterprises because of increased internet speed, less latency, and high throughput at a lower cost.

The turn of the century saw a new approach to firewall implementation during the mid-2010. The 'Next-Generation Firewalls' were introduced by the Palo Alto Networks. These firewalls came up with a variety of built-in functions and capabilities, such as Hybrid Cloud Support, Network Threat Prevention, Application and Identity-Based Control, and Scalable Performance, etc. Firewalls are still getting new features as part of continuous development. They are considered the first line of defence when it comes to network security.

Working of Firewall

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Limitations of Firewall

When it comes to network security, firewalls are considered the first line of defence. But the question is whether these firewalls are strong enough to make our devices safe from cyber-attacks. The answer may be "no". The best practice is to use a firewall system when using the Internet. However, it is important to use other defence systems to help protect the network and data stored on the computer. Because cyber threats are continually evolving, a firewall should not be the only consideration for protecting the home network.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Therefore, it is recommended to keep all Internet-enabled devices updated. This includes the latest operating systems, web browsers, applications, and other security software (such as anti-virus). Besides, the security of wireless routers should be another practice. The process of protecting a router may include options such as repeatedly changing the router's name and password, reviewing security settings, and creating a guest network for visitors.

Difference between a Firewall and Anti-virus

Firewalls and anti-viruses are systems to protect devices from viruses and other types of Trojans, but there are significant differences between them. Based on the vulnerabilities, the main differences between firewalls and anti-viruses are tabulated below:

Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.
Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.

Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats? for example- Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.

Types of Firewall

There are mainly three types of firewalls, such as **software firewalls, hardware firewalls, or both**, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.

A hardware firewall is a physical device that attaches between a computer network and a gateway. For example- a broadband router. A hardware firewall is sometimes referred to as an **Appliance Firewall**. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of firewall is also called a **Host Firewall**.

Besides, there are many other types of firewalls depending on their features and the level of security they provide. The following are types of firewall techniques that can be implemented as software or hardware:

- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

- **Packet-filtering Firewalls**

  A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network

traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations. Because these types of firewalls do not prevent web-based attacks, they are not the safest.

- **Circuit-level Gateways**

  Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.

  Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

- **Application-level Gateways (Proxy Firewalls)**

  Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.

  Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks. Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

- **Stateful inspection firewalls**

  Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.

  In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in

the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls. This is why stateful packet inspection is implemented along with many other firewalls to track statistics for all internal traffic. Doing so increases the load and puts more pressure on computing resources. This can give rise to a slower transfer rate for data packets than other solutions.

- **Next-generation Firewalls (NGFW)**

  Many of the latest released firewalls are usually defined as **'next-generation firewalls'**. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.

  NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance

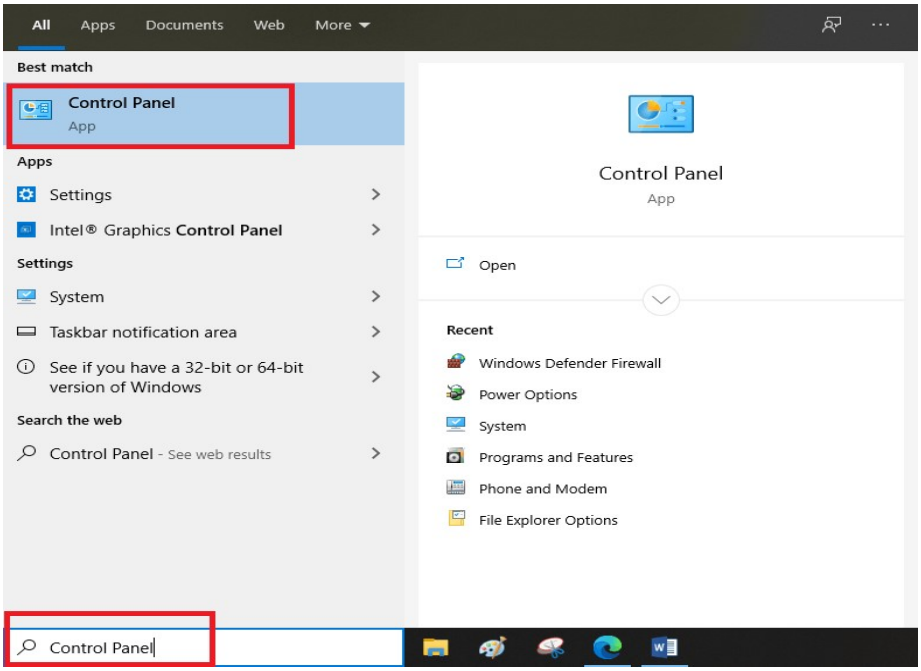
Working of Firewall with Windows

A firewall is the first line of control when it comes to the security of computers. It is designed to keep unauthorized users away from accessing files and resources stored on the computer system. There can be several reasons why a user might want to disable the firewall, especially when a user wants to try another firewall program.

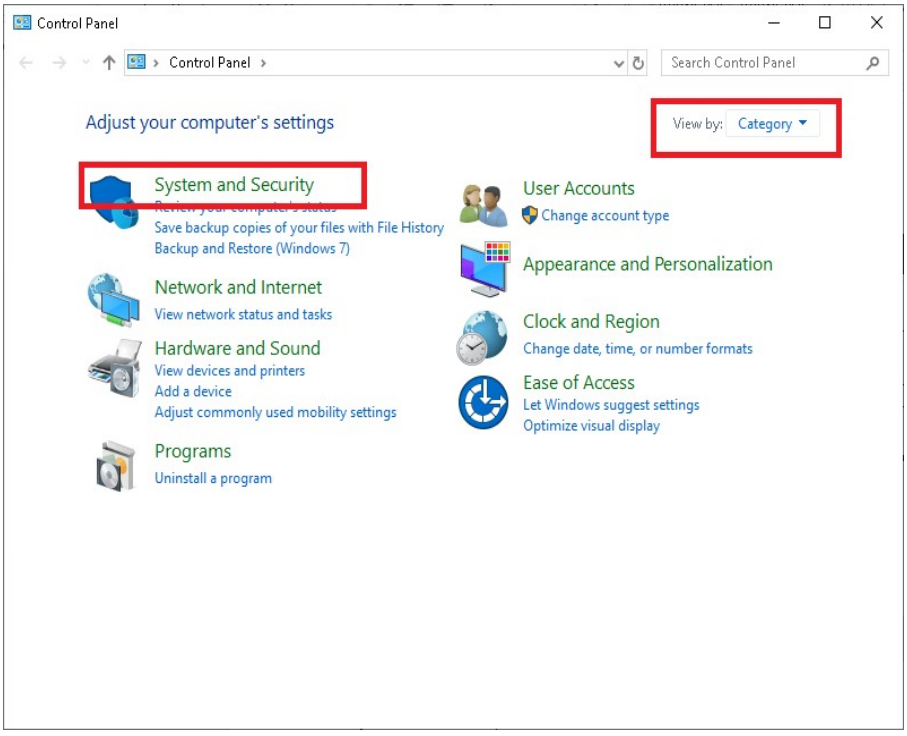
***Note**: It is not good to disable Windows Firewall unless there is another security program (with additional firewall support) running on the computer*

Following are steps to disable a firewall:

Step 1: First, we need to open the Control Panel. There are several ways to do this, but the easiest way is to use a search bar. Therefore, we need to click on the **Windows** search bar and enter the **'Control Panel'**. It will look like the following screen:

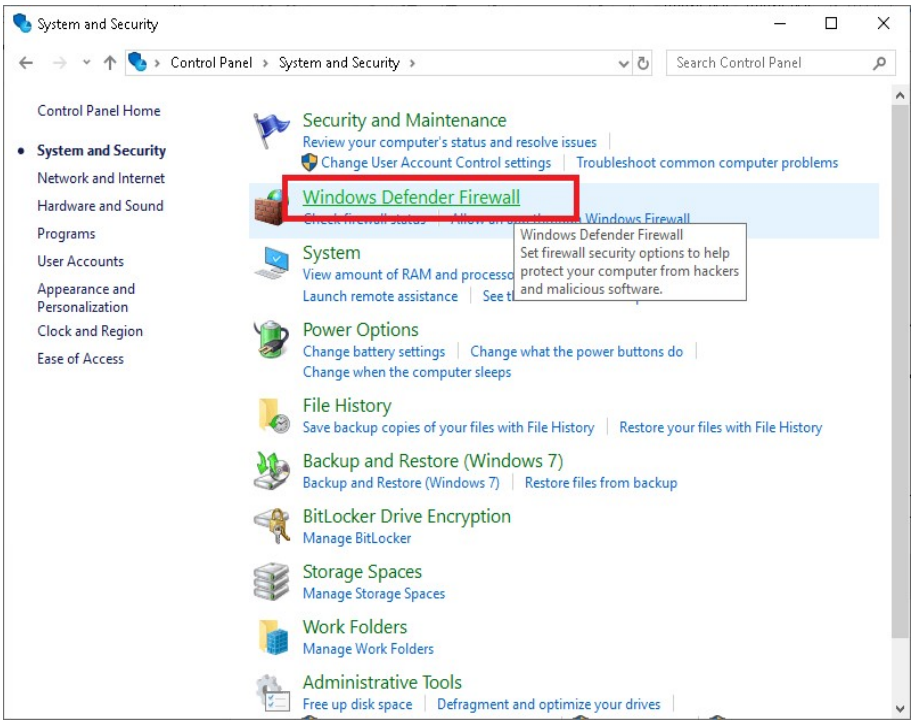


Step 2: After that, we are required to click on the Control Panel to open its settings. The control panel contains the following options:



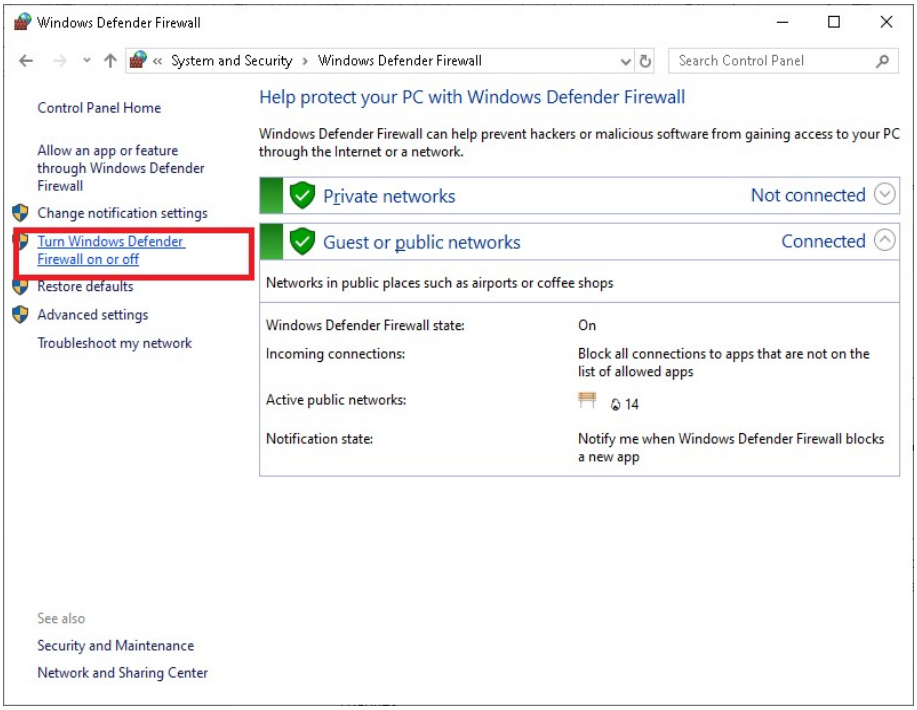
Here, we need to click on **'System and Security'**. This option is only visible if the 'view by:' option is set as 'Category'.

Step 3: Next, we need to click on **'Windows Defender Firewall'**, as shown below:

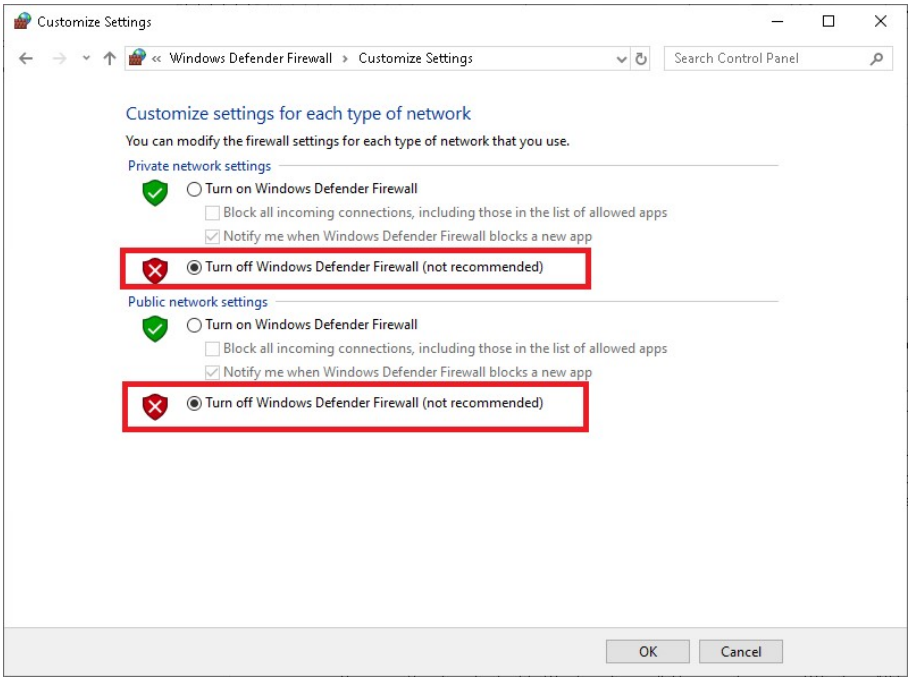


Note: In some computers, the option of 'Windows Defender Firewall' might instead be displayed as 'Windows Firewall'

Step 4: We are then required to click on **'Turn Windows Defender Firewall on or off'**. This option is shown in the left side panel of the screen:

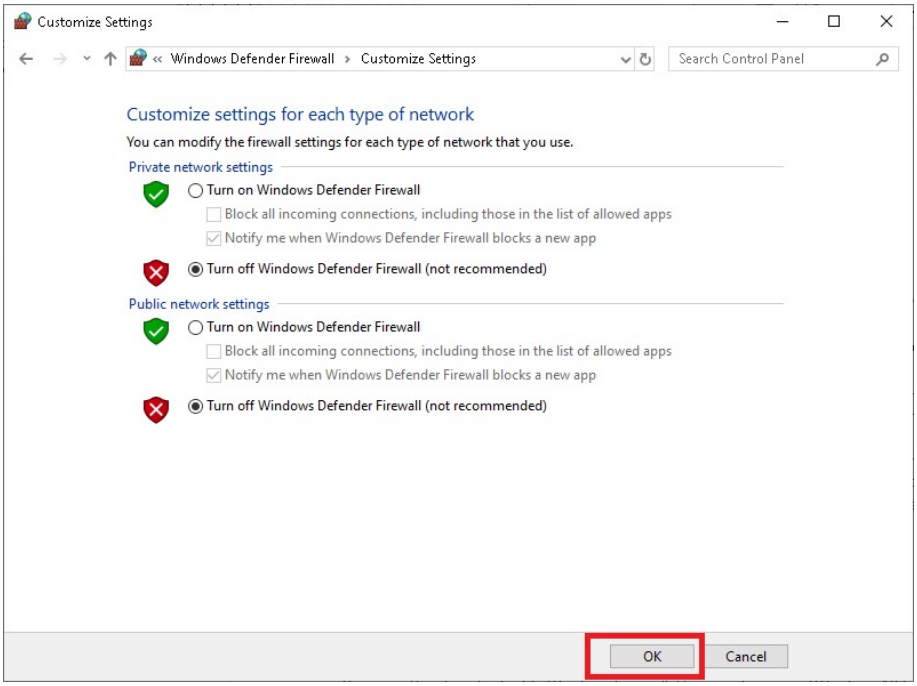


Step 5: On the next screen, we need to click on the circle radio button next to **'Turn off Windows Defender Firewall (not recommended)'**.



Here, we can select the firewall settings for different types of networks. Using this screen, we can turn off or disable the firewall for private networks, public networks, or both. We need to select the circle radio button next to 'Turn off Windows Defender Firewall (not recommended)' under both the private and the public network settings.

Step 6: After selecting the radio buttons, we are required to click on the **'OK'** button to keep the changes.



These are the steps to disable Windows Firewall. Here, we have used Windows 10 to describe the complete step by step tutorial. The processes will be the same on Windows 7/8/8.1; however, the user interface may be slightly different.

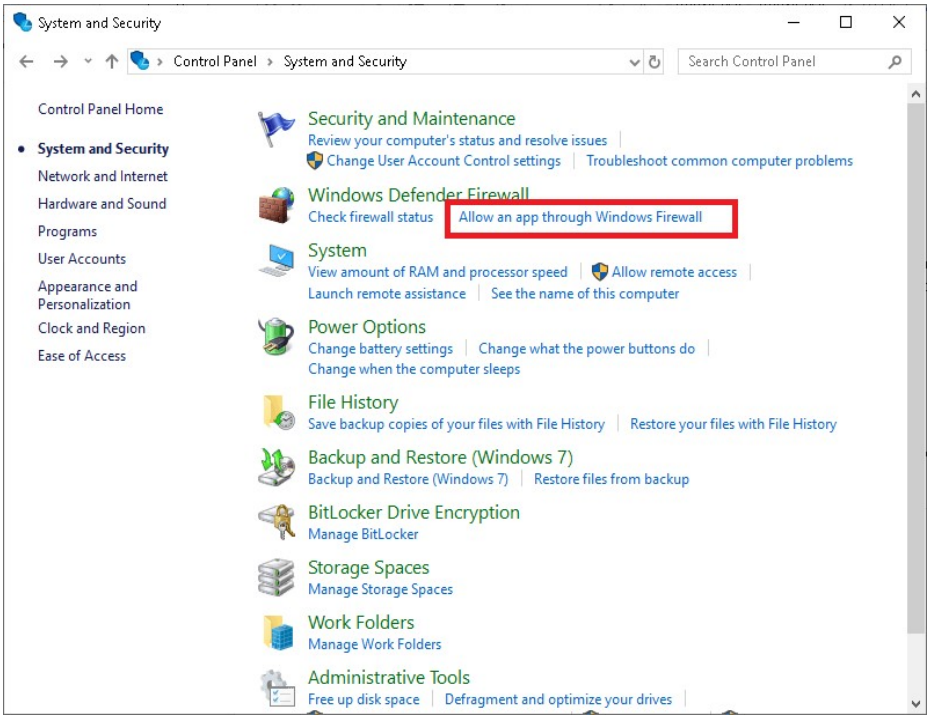
Caution

Suppose there is any program that is unable to access the Internet. In that case, it is better to allow that specific program through the firewall rather than disabling the entire firewall system. Here are the steps to allow any program through Windows Firewall:

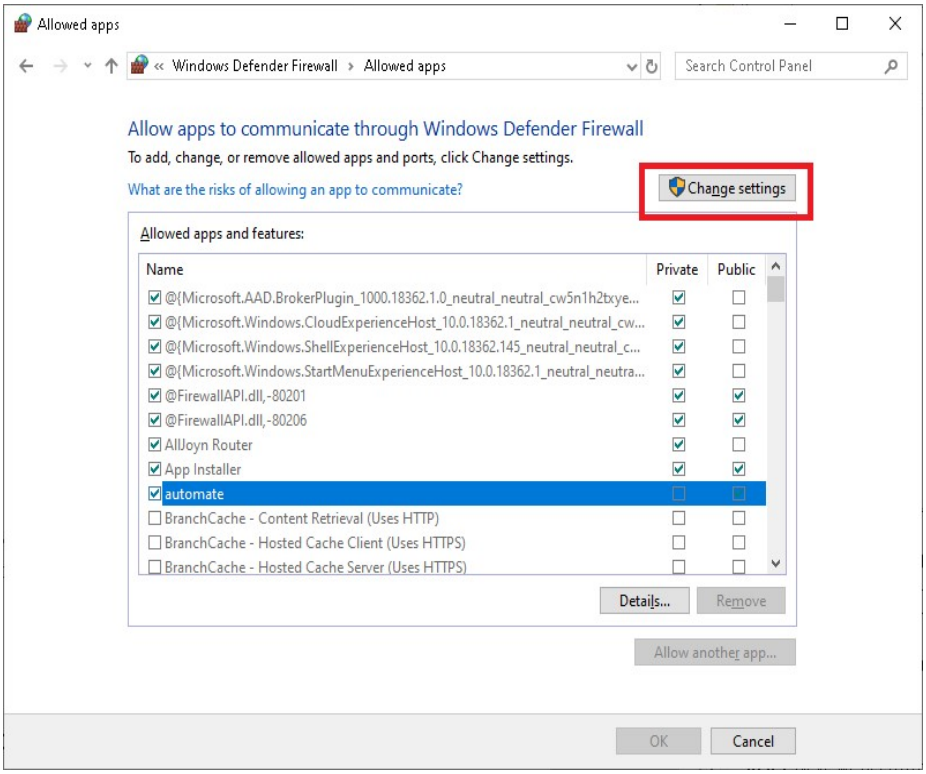
Step 1: First, we need to open a Control Panel.

Step 2: On the next screen, we need to click on **'System and Security'**.

Step 3: After that, we are required to click on **'Allow an app through Windows Firewall'**. This option is displayed under **'Windows Defender Firewall'** option, as shown below:



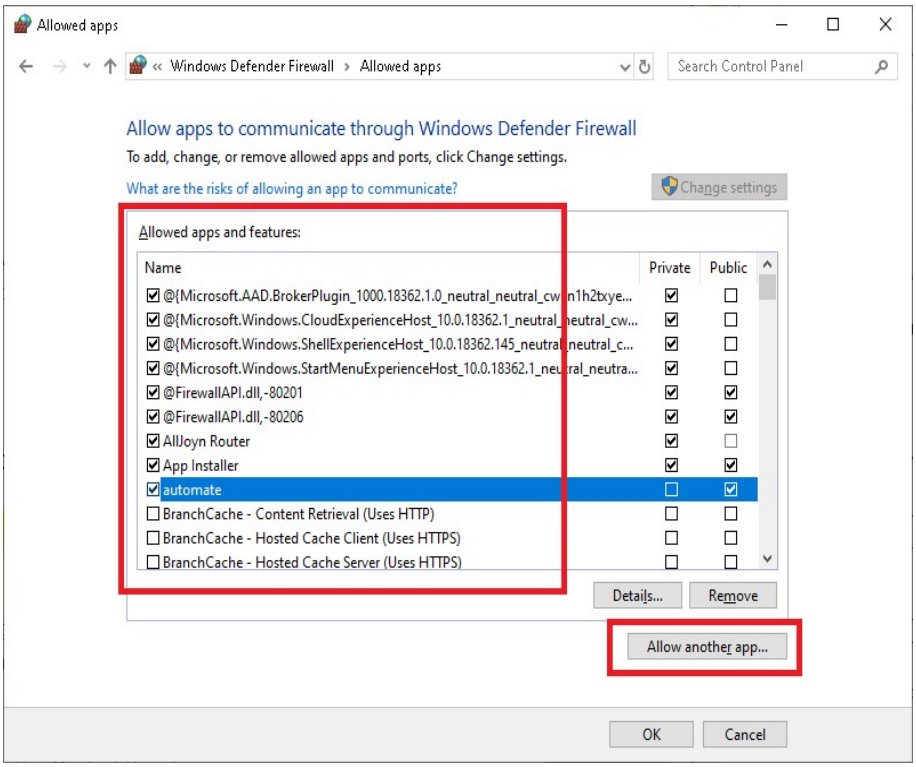
Step 4: After completing the above step, we will get the following screen:



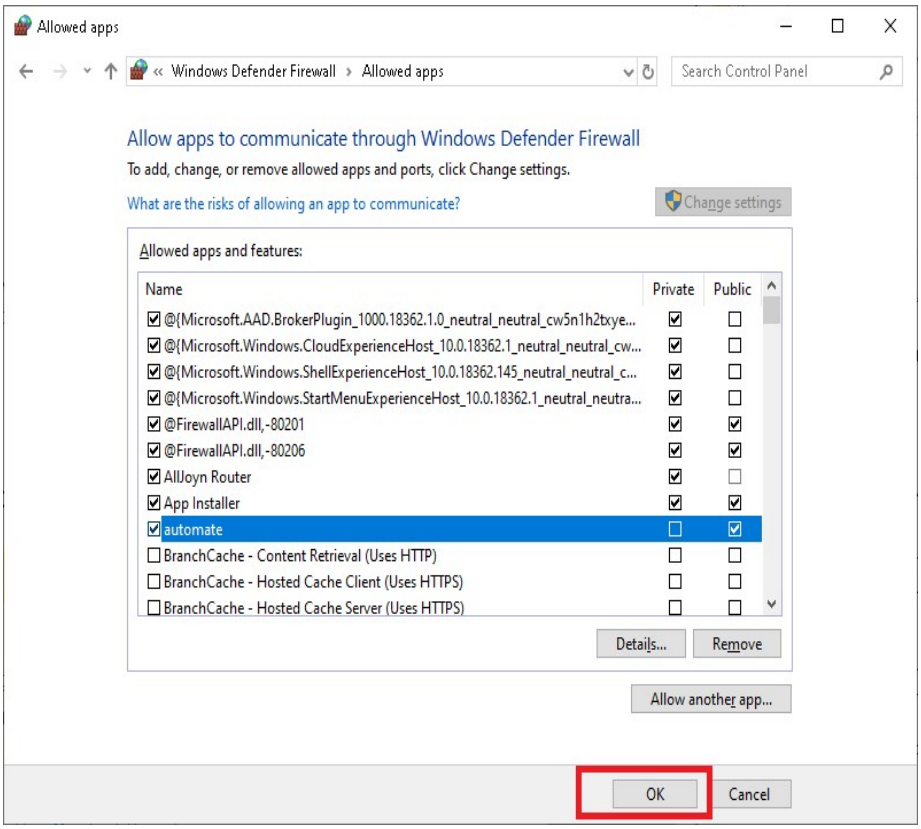
Here, we need to click on the **'Change settings'** button. This will allow us to access the list and modify its settings.

Step 5: Under the list of **'allowed apps and features'**, we can find a specific program to which we want to grant access through the Windows Firewall. After that, we need to select the checkboxes next to that particular program.

Here, we also get options to manage firewall settings for the private network and public network separately. The private box is mostly used for games based on a local area network, while the public box is used to allow the program to access the Internet. Besides, if we don't see a required program in the list, we can use the **'Allow another app'** button to add it manually.



Step 6: Next, we need to click on the **'OK'** button to keep the changes.



By using this method, we can enable or disable Windows Firewall for specific software. In simple words, the method helps us specify rules for individual programs to allow access to the Internet.

G. Procedure

Teacher shall explain about

- Importance of Firewall
- Working of Firewall
- Enabling and Disabling Firewall in Windows

H. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

I. Observations:

J. Conclusion

1. A firewall is a network security device
   a) it accepts, rejects, or drops that specific traffic.
   b) which monitors all incoming and outgoing traffic
   c) establishes a barrier between secured internal networks and outside the untrusted networks
   d) All of the above
2. _____ come by-default with operating systems.
   a) Hardware Firewall
   b) Software Firewall
   c) Stateful Inspection Firewall
   d) Microsoft Firewall

3. A proxy firewall filters at.
   a) Physical layer
   b) Application layer
   c) Network layer
   d) Data link layer

K. Practical related Quiz.

1. Whether a firewall is able to block some specific pages in a web application? Explain.

   .....

   .....

   .....

   .....

   .....

2. What is a Stateful Inspection Firewall?

   .....

   .....

   .....

   .....

   .....

3. Which type of firewall is more secure, packet filtering firewall or circuit-level gateway, and Why?

   .....

   .....

   .....

   .....

   .....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date

Date: ……

Practical No.10:

Run basic utilities and network commands: ipconfig, ping, tracert, netstat, pathping , route

Practical Significance:

A. Relevant Expected Program Outcomes(POs)

1. **Basic and Discipline specific knowledge: (PO1)** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the Computer Engineering problems.
2. **Engineering practices for society, sustainability and environment: (PO5)** Apply appropriate technology in context of society, sustainability, environment and ethical practices.
3. **Life-long learning:** (**PO7)** Ability to analyse individual needs and engage in updating in the context of technological changes in field of engineering.

B. Competency and Practical Skills

a. To study basic TCP/IP utilities.
b. To run networking commands

C. Relevant Course Outcomes

Not applicable

D. Practical Outcome

a. Understand basic of TCP/IP utilities.
b. Understand networking commands

E. Relevant Affective domain related Outcome(s)

- Follow ethical practices.

F. Prerequisite Theory:

Network Command-line Utilities

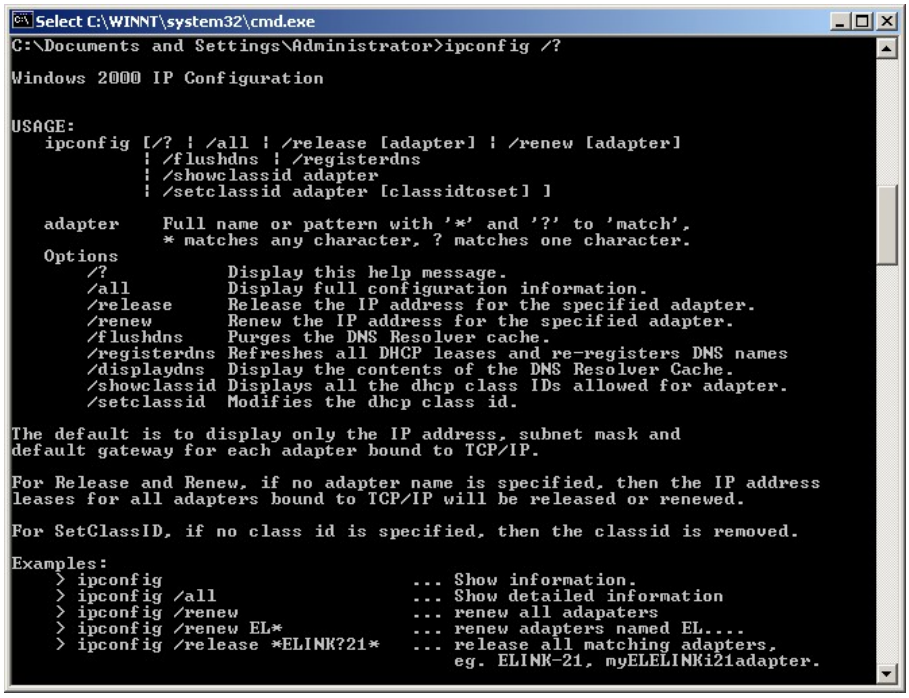
These utilities must be run at the prompt of the Cmd.exe command interpreter. To open Command Prompt, click Start, click Run, type cmd, and then click OK. Some command-line tools require the user to have administrator-level privileges on source and/or target computers.

- ipconfig
- ping
- tracert
- pathping

- netstat
- route

ipconfig

This ipconfig command is used for finding the IP address and default gateway of your network. 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 the IP address, subnet mask, and default gateway for all adapters.



This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

Syntax of ipconfig

ipconfig [/all]
[/renew [Adapter]]
[/release [Adapter]]
[/flushdns]
[/displaydns]
[/registerdns]
[/showclassid Adapter]
[/setclassid Adapter [ClassID]]

Examples of ipconfig

1) To display the basic TCP/IP configuration for all adapters, type:

ipconfig

2) To display the full TCP/IP configuration for all adapters, type:

ipconfig /all

3) To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

ipconfig /renew "Local Area Connection"

4) To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:

ipconfig /flushdns

5) To display the DHCP class ID for all adapters with names that start with Local, type:

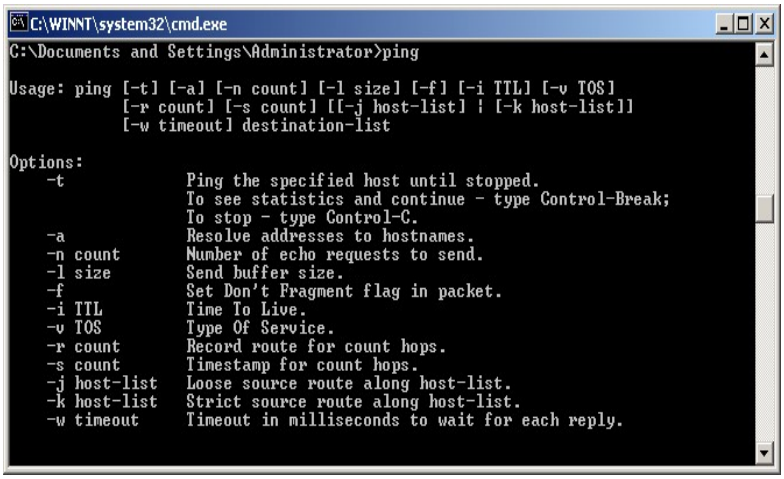
ipconfig /showclassid Local*

6) To set the DHCP class ID for the Local Area Connection adapter to TEST, type:

ipconfig /setclassid "Local Area Connection" TEST

Ping

The ping (packet Internet groper) command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. Used without parameters, ping displays help.



Ping command can be used to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

Syntax of ping

ping [-t]

[-a]
[-n Count]
[-l Size]
[-f]
[-i TTL]
[-v TOS]
[-r Count]
[-s Count]
[{-j HostList | -k HostList}]
[-w Timeout]
[TargetName]

Examples of ping

The following example shows ping command output:

C:\>ping example.microsoft.com
Pinging example.microsoft.com [192.168.239.132] with 32 bytes of data:

Reply from 192.168.239.132: bytes=32 time=101ms TTL=124

Reply from 192.168.239.132: bytes=32 time=100ms TTL=124

Reply from 192.168.239.132: bytes=32 time=120ms TTL=124

Reply from 192.168.239.132: bytes=32 time=120ms TTL=124

1) To ping the destination 10.0.99.221 and resolve 10.0.99.221 to its host name, type:

   ping -a 10.0.99.221
2) To ping the destination 10.0.99.221 with 10 Echo Request messages, each of which has a Data field of 1000 bytes, type:

   ping -n 10 -l 1000 10.0.99.221
3) To ping the destination 10.0.99.221 and record the route for 4 hops, type:

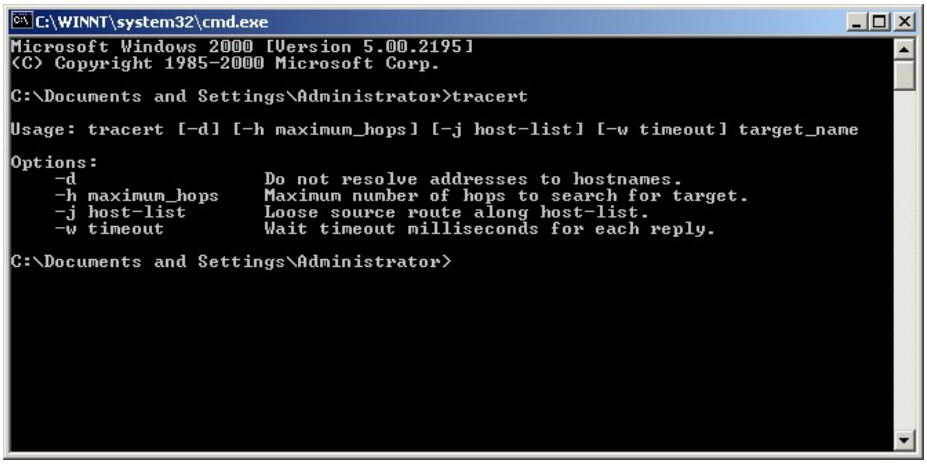
   ping -r 4 10.0.99.221
4) To ping the destination 10.0.99.221 and specify the loose source route of 10.12.0.1-10.29.3.1-10.1.44.1, type:

   ping -j 10.12.0.1 10.29.3.1 10.1.44.1 10.0.99.221

Tracert

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.

Used without parameters, tracert displays help



This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the -h parameter. The path is determined by examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (*) is displayed for that hop.

Syntax of tracert

tracert [-d]
[-h MaximumHops]
[-j HostList]
[-w Timeout]
[TargetName]

Examples of tracert

1) To trace the path to the host named corp7.microsoft.com, type:

   tracert corp7.microsoft.com

2) To trace the path to the host named corp7.microsoft.com and prevent the resolution of each IP address to its name, type:

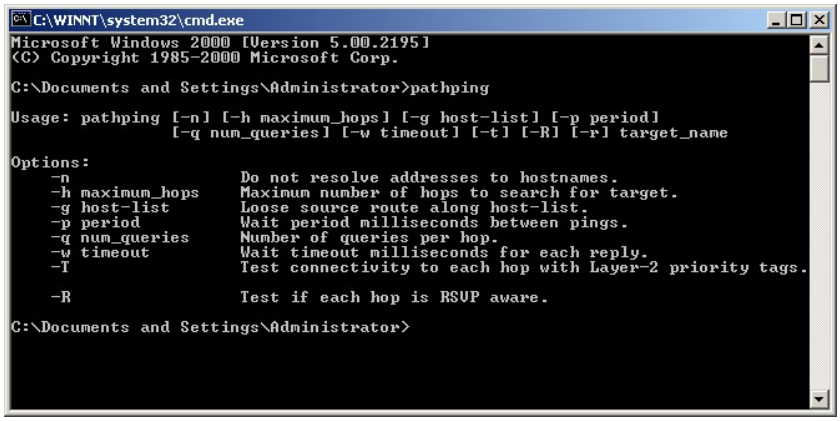
   tracert -d corp7.microsoft.com

3) To trace the path to the host named corp7.microsoft.com and use the loose source route 10.12.0.1-10.29.3.1-10.1.44.1, type:

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 corp7.microsoft.com

Pathping

Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping 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. Because pathping displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Pathping performs the equivalent of the tracert command by identifying which routers are on the path. It then sends pings periodically to all of the routers over a specified time period and computes statistics based on the number returned from each. Used without parameters, pathping displays help.



Syntax of pathping

pathping [-n]
[-h MaximumHops]
[-g HostList]
[-p Period]
[-q NumQueries]
[-w Timeout]
[-T]
[-R]
[TargetName]

Examples of pathping

The following example shows pathping command output:

D:\>pathping -n corp1
Tracing route to corp1 [10.54.1.196]

over a maximum of 30 hops:

0 172.16.87.35

1 172.16.87.218

```
2   192.168.52.1
3   192.168.80.1
4   10.54.247.14
5   10.54.1.196
Computing statistics for 125 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0                                           172.16.87.35
                                 0/ 100 = 0%   |
1  41ms    0/ 100 = 0%     0/ 100 = 0%     172.16.87.218
                               13/ 100 = 13%  |
2  22ms   16/ 100 = 16%    3/ 100 = 3%   192.168.52.1
                                 0/ 100 = 0%   |
3  24ms   13/ 100 = 13%    0/ 100 = 0%   192.168.80.1
                                 0/ 100 = 0%   |
4  21ms   14/ 100 = 14%    1/ 100 = 1%   10.54.247.14
                                 0/ 100 = 0%   |
5  24ms   13/ 100 = 13%    0/ 100 = 0%   10.54.1.196
Trace complete.
```

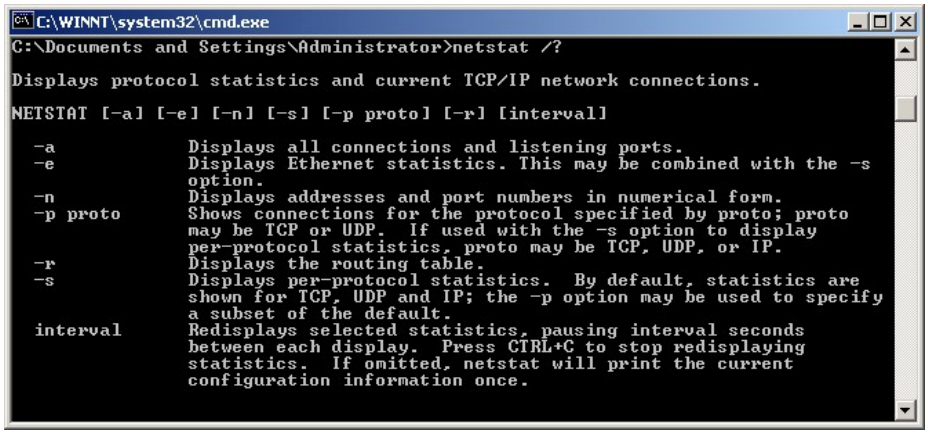
When pathping is run, the first results list the path. This is the same path that is shown using the tracert command. Next, a busy message is displayed for approximately 90 seconds (the time varies by hop count). During this time, information is gathered from all routers previously listed and from the links between them. At the end of this period, the test results are displayed.

In the sample report above, the This Node/Link, Lost/Sent = Pct and Address columns show that the link between 172.16.87.218 and 192.168.52.1 is dropping 13 percent of the packets. The routers at hops 2 and 4 also are dropping packets addressed to them, but this loss does not affect their ability to forward traffic that is not addressed to them.

The loss rates displayed for the links, identified as a vertical bar (|) in the Address column, indicate link congestion that is causing the loss of packets that are being forwarded on the path. The loss rates displayed for routers (identified by their IP addresses) indicate that these routers might be overloaded.

Netstat

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. Used without parameters, netstat displays active TCP connections.



Syntax of netstat

netstat [-a]
[-e]
[-n]
[-o]
[-p Protocol]
[-r]
[-s]
[Interval]

Examples of netstat

1) To display both the Ethernet statistics and the statistics for all protocols, type the following command:

   netstat -e -s

2) To display the statistics for only the TCP and UDP protocols, type the following command:

   netstat -s -p tcp udp

3) To display active TCP connections and the process IDs every 5 seconds, type the following command:

   netstat -o 5

4) To display active TCP connections and the process IDs using numerical form, type the following command:

   netstat -n -o

Route

Manipulates network routing tables.

Syntax of route

ROUTE [-f] [-p] [-4|-6] command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

-f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.

-p When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.

-4 Force using IPv4.

-6 Force using IPv6.

command One of these:
PRINT Prints a route
ADD Adds a route
DELETE Deletes a route
CHANGE Modifies an existing route
destination Specifies the host.
MASK Specifies that the next parameter is the 'netmask' value.
netmask Specifies a subnet mask value for this route entry.
If not specified, it defaults to 255.255.255.255.
gateway Specifies gateway.
interface the interface number for the specified route.
METRIC specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard, (wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only matching destination routes are printed. The '*' matches any string, and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Pattern match is only allowed in PRINT command.
Diagnostic Notes:

Invalid MASK generates an error, that is when (DEST & MASK) != DEST.

Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1

The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples of route

> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157* .... Only prints those matching 157*

> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
destination^ ^mask ^gateway metric^ ^
Interface^

If IF is not given, it tries to find the best interface for a given gateway.

> route ADD 3ffe::/32 3ffe::1

> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

CHANGE is used to modify gateway and/or metric only.

> route DELETE 157.0.0.0
> route DELETE 3ffe::/32

G. Procedure

Teacher shall explain and give demonstration of various network commands as listed above.

H. Actual procedure followed

……

……

……

……

……

……

……

……

……

……

……

……

……

……

I. Observations:

J. Conclusion

1. Which command is used for identifying the MAC address of a system?
    a) ipconfig
    b) ifconfig
    c) ping
    d) getmac
2. Which command helps to identify whether a given system is connected to a network?
    a) ping
    b) netstat
    c) ipconfig
    d) getmac
3. Which of the following best describes what traceroute is?
    a) It is the name of a tool used to determine the path of communication between two computersApplication layer
    b) It is how the distance between two cities is determined on a map.
    c) It is a website that allows users to see how far away they are from a specified computer.
    d) It is a way for network administrators to send the details of their network routers to other administrators.

K. Practical related Quiz.

1. What is netstat?

    .....

    .....

    .....

    .....

    .....

2. What do you understand by ping command?

    .....

    .....

    .....

    .....

    .....

3. What is a use of pathping command?

.....

.....

.....

.....

.....

L. Assessment-Rubrics

Rubrics ID	Criteria	Marks	Good (2)	Satisfactory (1)	Need Improvement (0)	Mark Scored
RB1	Regularity	2	High (>70%)	Moderate (40-70%)	Poor (0-40%)	
RB2	Problem Analysis	2	Apt & Full Identification of the Problem	Limited Identification of the Problem	Very Less Identification of the Problem	
RB3	Development of the Solution	2	Complete Solution for the Problem	Incomplete Solution for the Problem	Very Less Solution for the Problem	
RB4	Testing of the Solution	2	Correct Solution as required	Partially Correct Solution for the Problem	Very less correct solution for the problem	
RB5	Mock viva test	2	All questions responded Correctly	Delayed & partially correct response	Very few questions answered correctly	

Signature with Date