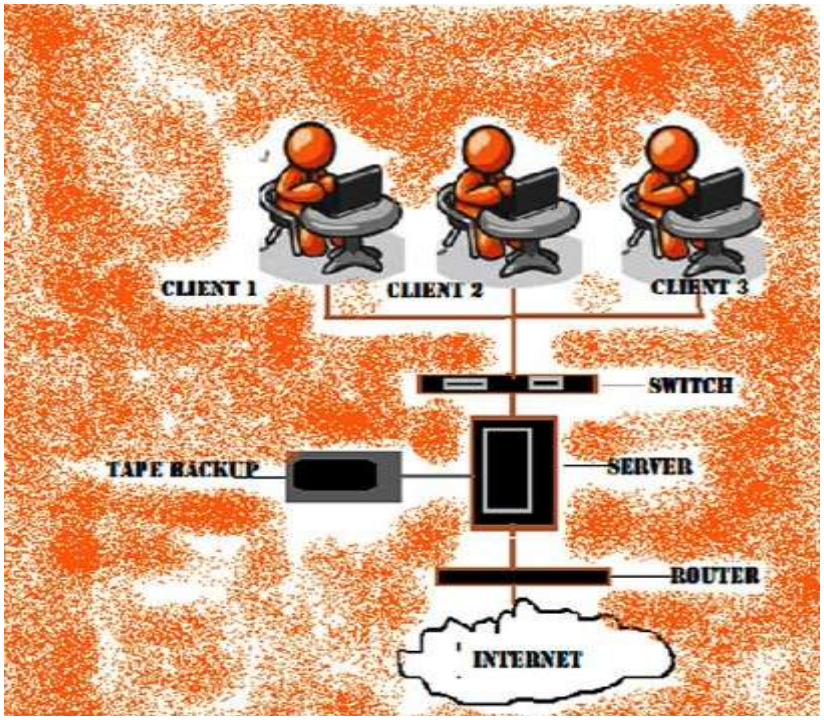
Information Technology

NVEQ Level 3 – Class XI

IT307-NQ2012-Computer Networks

Student’s Handbook



प.सु.श.केन्द्रीय व्यावसायिक शिक्षा संस्थान,श्यामला हिल्स, भोपाल

PSS Central Institute of Vocational Education, Shyamla Hills, Bhopal

PSS Central Institute of Vocational Education, 2012

Student Details

Student Name:________________________________

Student Roll Number:__________________________

Batch Start Date:_____________________________

Acknowledgements

The following partners were instrumental in providing the content:

1. Accenture India's Corporate Citizenship Program (Skills 4 Life) has provided the content material for English and have commissioned and developed as well as provided access to their implementing partners (Dr. Reddy's Foundation and QUEST Alliance).

2. The Wadhwani Foundation team involved in designing and building this curriculum and content include Ms. Sonia Kakkar, Mr Karthik Chandru, Ms. Toral Veecumsee, Ms. Rekha Menon, Mr. Ajay Goel and Mr. Austin Thomas.

3. The PSSCIVE's team was involved in guidance and editing the content.

4. In addition, various public domain sources have been leveraged to create materials and illustrations across module. The contributions of all these sources is gratefully acknowledged and recognized.

Preface

The National Curriculum Framework, 2005, recommends that children's life at school must be linked to their life outside the school. This principle makes a departure from the legacy of bookish learning which continues to shape our system and causes a gap between the school, home, community and the workplace.

The student workbook on "**Computer Networks**" is a part of the qualification package developed for the implementation of National Vocational Education Qualification Framework (NVEQF), an initiative of Ministry of Human Resource Development (MHRD), Government of India to set common principles and guidelines for a nationally recognized qualification system covering Schools, Vocational Education and Training Institutions, Technical Education Institutions, Colleges and Universities. It is envisaged that the NVEQF will promote transparency of qualifications, cross-sectoral learning, student-centred learning and facilitate learner's mobility between different qualifications, thus encouraging lifelong learning.

This student workbook, which forms a part of vocational qualification package for student's who have passed Class X or equivalent examination, was created by a group of experts. The IT-ITeS Skill Development Council approved by the National Skill Development Corporation (NSDC) for the IT/ITeS Industry developed the National Occupation Standards (NOS). The National Occupation Standards are a set of competency standards and guidelines endorsed by the representatives of IT Industry for recognizing and assessing skills and knowledge needed to perform effectively in the workplace.

The Pandit Sunderlal Sharma Central Institute of Vocational Education (PSSCIVE), a constituent of National Council of Educational Research and Training (NCERT) in association with Wadhwani Foundation has developed modular curricula and learning materials (Units) for the vocational qualification package in IT/ITes sector for NVEQ levels 1 to 4; level 1 is equivalent to Class IX. Based on NOS, occupation related core competencies (knowledge, skills, and abilities) were identified for development of curricula and learning modules (Units).

This student workbook attempts to discourage rote learning and to bring about necessary flexibility in offering of courses, necessary for breaking the sharp boundaries between different subject areas. The workbook attempts to enhance these endeavours by giving higher priority and space to opportunities for contemplation and wondering, discussion in small groups and activities requiring hands-on-experience. We hope these measures will take us significantly further in the direction of a child-centred system of education outlined in the National Policy of Education (1986). The success of this effort depends on the steps that school Principals and Teachers will take to encourage children to reflect their own learning and to pursue imaginative and on-the-job activities and questions.

Participation of learners in skill development exercises and inculcation of values and creativity is possible if we involve children as participants in learning, and not as receiver of information. These aims imply considerable change in school routines and mode of functioning. Flexibility in the daily time-table would be a necessity to maintain the rigour in implementing the activities and the required number of teaching days will have to be increased for teaching and training.

SESSION 1: INTRODUCTION TO NETWORKING

RELEVANT KNOWLEDGE

As you know, networking is widely used for accessing and sharing information; examples include web browsing, downloading & uploading, file sharing, printer sharing, etc. Today networking is popular with private and business users across the globe.

In today's world, it can be extremely difficult to live without networks, since resource sharing (printers, shared folders etc) and Internet connectivity have become an integral part of our daily activities.

A computer network, often simply referred to as a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.

Networking is widely used for sharing of resources and information & for communication purposes. Networks can also help in reducing costs; for example you can buy a single printer and share it across multiple users.

Network consists of one or more computers or devices connected in order to provide and access resources. Resources include a range of devices (example, Printer, CDROM, Hard Drives, etc.) and services (example, web service, mail service, etc.).

Networks based on size are classified into LAN & WAN.

- LAN: Local Area Network refers to group of computers networked within a limited geographical area such as schools, colleges, offices, etc.
- WAN: Wide Area Network refers to computers networked across geographical areas, in other words they connect LAN's between different locations. For example, computers or devices in a branch office could connect to the computer networks at the head office through telephone lines or satellites.

Ways to form a computer Network

There are several ways to form a network as listed below:

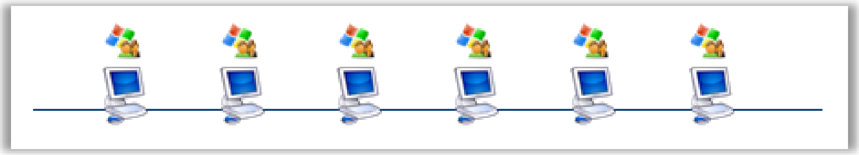
- Use a cross-over cable (also referred to as Peer-to-peer cable)
- Use Serial and Parallel ports
- Use Bluetooth
- Use Wi-Fi (for more than two computers)

- Use Hub or Network Switch (for more than two computers)
- SOHO Router or Wi-Fi Router (Commonly found in home & small business networks)

Though technically it is possible to connect computers using the above mentioned options, practices such as using a crossover cable, Wi-Fi or a network switch are most common methods. The technology or option choice is generally based on the number of connections, speed and distance constraints.

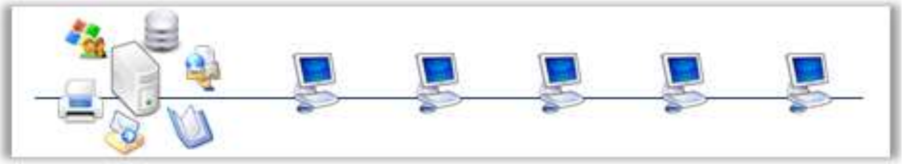
Networking Models

Peer-to-Peer(P2P): This is usually meant for a maximum of 10-20 computers. Herein, each computer can act both as a server as well as a client. P2P networks are simple to setup and use, normally home and small office networks fall in this category. P2P networks are also referred to as the Workgroup model and have their own security database, i.e. User accounts are present on each and every computer on a network.



Peer-to-Peer Network

Client / Server: These are large networks with 10 to hundreds of computers and may have dedicated servers and devices. Office networks that require centralized security and administration fall in this category. Common servers on these networks include File Servers, Print Servers, Messaging Servers, Database Servers, Domain controllers, etc.



Client-Server Network

Note: Clients are referred to as "Service Requestors" and Servers as "Service Providers". Any machine that request a service is called as the client and machines that fulfill the requests is called the client.

Networks can have a combination of both Client/Server models and Peer-to-Peer. For example, you may be using a centralized mail server and/or access files from other machines in the network.

Internet, Intranet & Extranet

Internet

Internet is a global system of interconnected networks; also referred to as network of networks, the Internet uses TCP/IP protocol suite (you will read more about this protocol later). Internet consists of millions of computers accessed by billions of users through a variety of devices for varying purposes such as browsing, electronic messaging, chatting, social networking, blogging, online shopping, Internet marketing, researching, data collection, downloading and uploading content, etc. It is the largest network in the world.

Intranet

Intranet refers to private computer network used by organizations for sharing resources; Intranets can be simple within a building or very large spread across the globe connected through various networking technologies. Intranets help employees of an organization to locate information much faster resulting in increased productivity. Though popularly referred to a company's internal website or portal, Intranet usually employs other protocols such as POP3, SMTP, FTP, etc. and may even offer a variety of services (you will read more about these in later sessions).

Extranet

Extranet is a computer network used outside the Intranet. For example, an organization may allow a vendor to view or access their resources such as their internal website for updating a product catalog or training material. However, this is highly restricted to Internet users (public). Extranets are usually accessed using VPNs (you will read more about this protocol later).

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Analyze the network requirement for your school or office setups available close to your vicinity. If a network is already present, understand the purpose of it. Share the inputs with rest of the class.

ASSESSMENT

Answer the following Questions

1. Explain the purpose of Networking
2. Explain Peer-to-Peer Networks
3. Explain Client Server networks
4. Explain any three methods for connecting two or more computers.
5. Explain Internet, Intranet & Extranet.

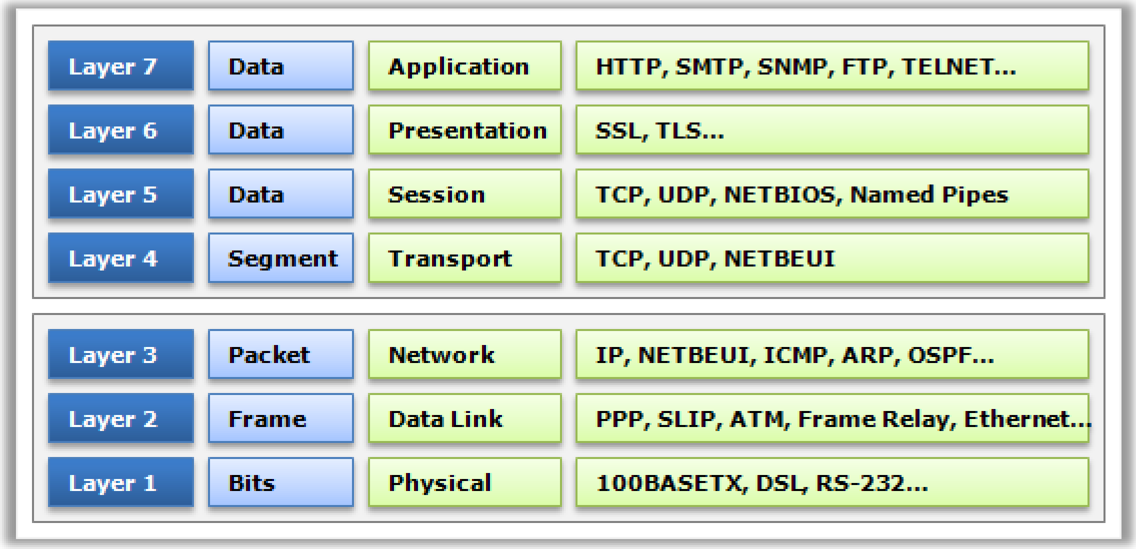
Fill in the blanks

1. Acronym for LAN ______________________________.
2. Acronym for WAN _____________________________.
3. In _________________ model, a computer can act both as a server and a client.
4. List any three resources that can be shared across a network. __________ , _________ & __________. __________
5. __________model uses centralized security database.
6. ____________________is also referred to as Service Requestors.
7. ___________________ is also referred to as Service Providers.
8. ___________________ is the largest network in the world.
9. ___________________ is commonly referred to as a private network by most organizations.

SESSION 2: THE OSI MODEL

RELEVANT KNOWLEDGE

In 1978, Open Systems Interconnect (OSI) model was introduced by the International Standards Organization (ISO) to provide a conceptual model for networking. OSI model servers the purpose in which the end user need not worry about using devices, protocols or services from different manufacturers as it lays out the guidelines for interoperability between network manufacturers. For example a network interface card manufacturer need not think about how the cables are manufactured, how protocols work or if an application would be compatible with the network interface card.



Layer 7	Data	Application	HTTP, SMTP, SNMP, FTP, TELNET...
Layer 6	Data	Presentation	SSL, TLS...
Layer 5	Data	Session	TCP, UDP, NETBIOS, Named Pipes
Layer 4	Segment	Transport	TCP, UDP, NETBEUI
Layer 3	Packet	Network	IP, NETBEUI, ICMP, ARP, OSPF...
Layer 2	Frame	Data Link	PPP, SLIP, ATM, Frame Relay, Ethernet...
Layer 1	Bits	Physical	100BASETX, DSL, RS-232...

The OSI Model defines how data communication occurs on networks. Most of the network communication protocols used today have a structure based on the OSI model. The OSI model defines the communications process into 7 layers, which divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is assigned to each of the seven OSI layers. Each layer can independently implement the tasks assigned. This enables solutions offered by one layer to be updated without adversely affecting the other layers.

Each layer addresses a specific set of functions as illustrated in the figure above. Layers 7 through 4 deal with end to end communications between data source and destinations. Layers 3 to 1 deal with communications between network devices. The seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (for example wires) and is responsible for placing data on the medium.

Data flow in the OSI Model

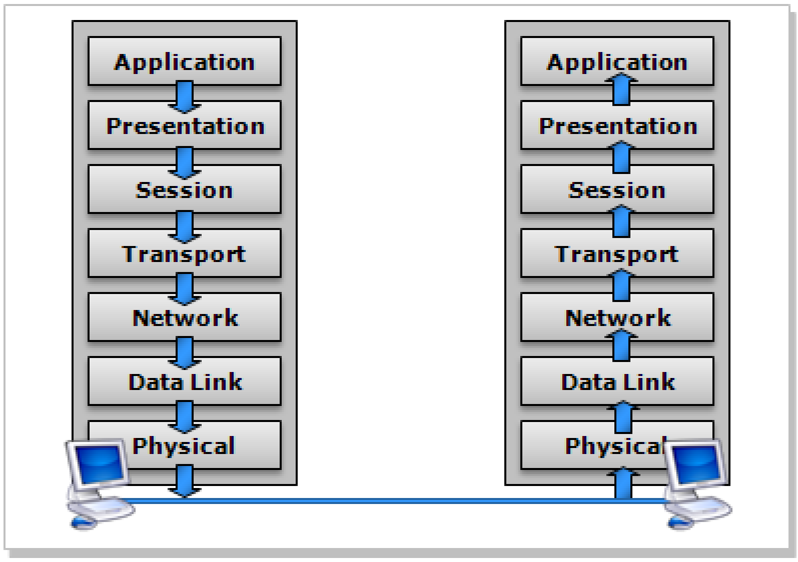
Data flows two ways in the OSI model, *Down* (data encapsulation) and *Up* (data decapsulation). For any data that needs to be sent from one computer to another, the OSI model ensures that everyone follows some guidelines and hence each computer is able to communicate with every other computer, regardless of whether one computer is a Macintosh and the other is a PC.

When data flows down the OSI model, every layer adds a header that ("encapsulation") and this is removed by the same layer on the other end of the session ("decapsulation"). These headers are layer specific.

The sending process passes the data to the application layer. The application layer attaches an application header and then passes the frame to the presentation layer. The presentation layer transforms data (if needed, such as by translating it) and adds a header. It gives the result to the session layer. The presentation layer is not concerned with which portion (if any) of the data received from the application layer is the application header and which portion is actually user data, because that information not necessary for the presentation layer's role.

The process of adding headers is repeated from layer to layer until the frame reaches the data link layer. Here, in addition to a data-link header, a data-link trailer is added. The data-link trailer contains a checksum and padding. The frame is then passed down to the physical layer, where it is transmitted to the receiving computer.

On the receiving computer, the various headers and the data trailers are stripped off one by one by each layer and passed on to the next upper layer till the packet finally reaches the receiving process.



Seven layers of OSI model are:

1. **Physical Layer** is the first (lowest) layer in the OSI Model and deals with media, signal and binary transmission. This layer:
    - Establishes and terminates connections to communication medium, controls modulation & demodulation of signals transmitted over wired (copper or fiber optic) or wireless media (such as radio wave).
    - Interfaces between the network medium and sending/receiving devices. (Hubs & Repeaters operate at this layer.)
    - Defines electrical, mechanical, and procedural interface to the transmission medium. Cables, connectors, voltages, topologies, etc. fall under the physical layer.
    - Protocols at this layer include 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX, DSL, ISDN, SONET, etc.
    - Unit of measurement (called as Protocol Data Units, PDU) at physical layer is bits such as Kbps, Mbps or Gbps.

2. **Data Link Layer** is the second (Layer 2) layer in the OSI Model. Data link layer is concerned with local delivery of frames between devices on the same LAN. Devices that operate at this layer include Network Interface Cards, Bridges and Switches. Communication happens through physical addressing; an address that is hardcoded into the network interface card (also referred to as MAC address).

Data Link Layer has the following two sub layers:

a. **Logical Link Control (LLC)** provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media.
b. **Media Access Control (MAC)** provides addressing and channel access control mechanisms for several network nodes to communicate in a shared medium such as the Ethernet.

The Data Link layer:

- Defines procedures for operating the communication links by physical addressing, framing, flow control, error control, media access control, etc.
- Frames packets
- Detects and corrects packets transmit errors
- Protocols at this layer include Ethernet, PPP, SLIP, Token Ring, etc.
- Unit of measurement in data link layer is ***frames*** (data packet).

3. **Network Layer**, is also referred to as Layer 3.This layer:
    - Determines how data moves between network devices by using logical addresses and routing functions in logical networks.
    - Routes packets using unique network device addresses as the IP (Internet Protocol) address. Routers operate at this layer
    - Protocols in this layer include IPv4, IPv6, IPX, RIP, OSPF, ICMP, IGMP, etc.
    - Unit of measurement in network layer is ***packets or datagram***.

4. **Transport Layer,** referred to as Layer 4, handles end-to-end communication and error-free transmission in conjunction with Layer 3. This layer:
    - Ensures end-to-end communication and error-free transmission
    - Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
    - Provides connection/connectionless oriented packet delivery
    - Protocols in this layer include TCP, UDP, etc.
    - The unit of measurement in transport layer is ***segments***.

5. **Session Layer,** referred to as Layer 5, is responsible for establishing, between network applications. This layer:
    - Manages user sessions and dialogues (Logon/Logoff is handled here).
    - Controls establishing, maintaining (synchronizing) and terminating sessions (conversations)/logic links between users/ network applications
    - Reports upper layer errors
    - Protocols in this layer include NetBIOS, PAP, PPTP, L2TP, etc.

6. **Presentation Layer** is also referred to as Layer 6. This layer:
    - Masks the differences of data formats between dissimilar systems
    - Specifies architecture-independent data transfer format
    - Encodes/decodes, encrypts/decrypts, compresses/decompresses data
    - Protocols in this layer include ASCII, EBCDIC, MIDI, SSL, TLS, etc.

7. **Application Layer**, referred to as Layer 7; protocols in this layer are responsible for process-to-process communication across an IP network. For example, if you initiate a web browser to visit a website, this layer initiates the HTTP protocol which in turn sends the data request to the underlying layers for communicating with the web server (HTTP) at the other end. To summarize, this layer:
    - Defines interface to user processes for communication and data transfer in network
    - Provides standardized services such as virtual terminal, file and job transfer and operations (provides services to end-users such as browsing, email, file transfers, etc.)
    - Protocols in this layer include HTTP, FTP, SMTP, POP3, DNS, DHCP, NNTP, etc.

Unit of measurement at Session, Presentation & Application layers is data.

IEEE 802 Standards

IEEE (Institute of Electrical and Electronics Engineers) is an international non-profit organization that set standards, IEEE 802 deals with LAN and WAN related technologies. Services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC).

Following table summarizes the IEEE 802 standards.

Standard	Description
IEEE 802.1	LAN / MAN Management
IEEE 802.2	LLC
IEEE 802.3	Ethernet
IEEE 802.4	Token Bus
IEEE 802.5	Token Ring
IEEE 802.6	Metropolitan Area Networks
IEEE 802.7	Broadband LAN
IEEE 802.8	Fiber Optic LAN / MAN
IEEE 802.9	Isochronous LAN
IEEE 802.10	LAN / MAN Security
IEEE 802.11	Wireless LAN
IEEE 802.12	Demand priority access method
IEEE 802.15	Wireless Personal Area Network
IEEE 802.16	Wireless Metropolitan Area Networks
IEEE 802.17	Resilient Packet Ring
IEEE 802.18	LAN/MAN Standards Committee
IEEE 802.22	Wireless Regional Area network

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Write the layers of OSI Model and list different protocols that match each layer. Refer to http://en.wikipedia.org/wiki/OSI_model for list of protocols at each layer. Use the following table to complete this activity:

Layer	Protocols

ASSESSMENT

Answer the following

1. Explain the purpose of OSI Model.
2. Explain Physical Layer of the OSI Model.
3. Explain Data Link Layer of the OSI Model.
4. Explain Network Layer of the OSI Model.
5. Explain Transport Layer of the OSI Model.
6. Explain Session Layer of the OSI Model.
7. Explain Presentation Layer of the OSI Model.
8. Explain Application Layer of the OSI Model.

Fill in the blanks

1. Acronym for ISO ____.
2. Acronym for OSI ____.
3. Seven layers of the OSI model are (write in correct order): _________________ , _________________ , ________________ , __________________, __________________, _______________ & ______________.
4. Sub layers of Layer 2 are: _________________ & _________________.
5. ______________ layer handles the function of logical addressing & routing.
6. ______________ layer deals with standards for cabling & connectors.
7. ______________ layer deals with standards for data formats, encryption & compression.
8. ___________, ___________ & _________ are examples of layer 1 protocols.
9. ___________, ___________ & _________ are examples of layer 2 protocols.
10. ___________, ___________ & _________ are examples of layer 3 protocols.
11. ___________, ___________ & _________ are examples of layer 4 protocols.
12. ___________, ___________ & _________ are examples of layer 5 protocols.
13. ___________, ___________ & _________ are examples of layer 6 protocols.
14. ___________, ___________ & _________ are examples of layer 7 protocols.
15. _________ layer is used for creating communication sessions between computers.
16. ____________ layer of the OSI model is used to encrypt and compress data.
17. __________ is the unit of measurement at Layer 1.
18. __________ is the unit of measurement at Layer 2.
19. _________ or __________ is the unit of measurement at Layer 2.
20. __________ is the unit of measurement at Layer 4.
21. __________ is the unit of measurement at Layer 7.

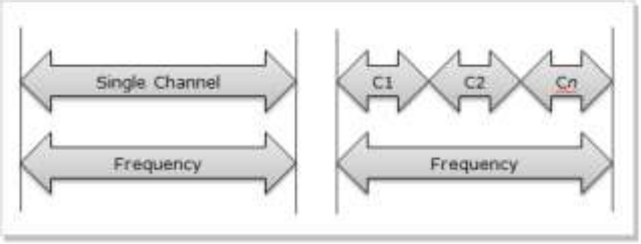
SESSION 3: TERMINOLGIES AND TECHNOLOGIES

RELEVANT KNOWLEDGE

Signaling Methods

In a network, communication happens between devices or computers through electrical, optical or radio-wave signals. Methods of signaling are widely categorized into *baseband* and *broadband*.

- **Baseband**: Data is sent as digital signals by using entire bandwidth of the media (Single Channel), supporting single communication at a time. Signals are sent over co-axial, twisted pair or fiber optic cables. Baseband supports higher transfer rates as compared to broadband; however, baseband is limited with distance. Baseband uses TDM (Time Division Multiplexing) to send multiple signals over a single cable. Example: Ethernet, Token Ring & FDDI.
- **Broadband**: Data is send as analog signals by using portion of a bandwidth. Broadband supports use of multiple signals at different frequencies (multiple channels). Signals are split into channels by using FDM (Frequency Division Multiplexing). Example: xDSL, where telephone lines are used for both voice (telephone) calls and data (Internet connectivity).



Baseband vs. Broadband

Channel Operation

Channel operation refers to the mode of communication between connected devices or computers. Channel operation can be *simplex, half-duplex* or *full-duplex*. Simplex is a one way communication, similar to that of a radio. Half-duplex is a two way communication but only one way at a time, similar to that of a walkie-talkie. Full-duplex is two way simultaneous communication (data can be received and sent at the same time), similar to that of a telephone.

Multiple Signaling Methods

When multiple devices or computers are connected in a network, they use multiple signals that are combined at the source and separated at the destination by use of a technique called *multiplexing*. For multiplexing, a device called the multiplexer is used for multiplexing / demultiplexing signals. Types of multiplexing include:

- **TDM (Time Division Multiplexing)** is a method in which multiple signals are combined and send over a single transmission media such as wires or radio waves. This is achieved by use of time sharing; multiple signals are transmitted for a defined amount of time in cycles. For example, a device sends and receives signals every alternate second.
- **FDM (Frequency Division Multiplexing)** is a method in which multiple signals are transmitted at different frequencies. Multiple signals can be sent at the same time over a single channel using this technique. For example, a device sends multiple signals at the same time using different frequencies similar to that of a radio (FM) or cable TV and the end device receives by tuning in to a particular channel.

Data Transmission methods

Data can be transferred over a network using the following techniques:

- **Circuit Switching**: In this method, a dedicated path is established between the endpoints before the data is transferred. Once a dedicated path is established, no other devices can use the circuit. Example: Dial-Up, ISDN.

- **Packet Switching**: In this method, data is divided into blocks referred to as packets. Multiple packets can be sent via different paths allowing more than two devices to communicate at the same time. Modes of operation can be connectionless or connection-oriented.

    - In connectionless mode, packets have source & destination address for routing that may take different paths. Example: Ethernet, IP, UDP.

    - In connection-oriented mode, connection is defined (a virtual circuit is created) before a packet is transferred. Packet switching supports variable packet sizes. Example: X.25, Frame Relay, TCP.

- **Cell Switching**: Cell switching method is similar to that of packet switching but has a fixed size for the cells transmitting data. Cell switching is efficient when large amounts of data need to transferred. Example: ATM.

Channel Access Methods

Channel access methods refer to how devices communicate using a shared medium such as bus networks, star networks, ring networks, hub networks & wireless networks. When multiple devices or computers are used in a shared medium, a pre-defined method of transmission needs to be defined. Channel access methods in circuit switching networks include FDM, TDM, etc and in packet switching networks include CSMA/CD, CSMA/CA, Token passing, etc.

Ethernet

Ethernet is a family of computer networking technologies for local area networks (LANs) and has largely replaced competing wired LAN technologies. Ethernet standard defines how communication happens between network interface cards, hub, switches, repeaters, etc. Devices on Ethernet networks use frames or Ethernet frames for communication. IEEE 802.3 standard defines the Media Access Control (MAC) portion of the data link layer and the physical layer of the OSI model. Ethernet protocols are covered by this standard.

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) as per IEEE 802.3 standard is a mechanism that defines how transmission takes place in a network. Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network before sending any packets in order to avoid data collisions. Collisions also decrease network efficiency on a collision domain. If two devices transmit simultaneously, a collision occurs, and both devices device will wait for a random amount of time before attempting to transmit again.

Collision domains are found in a hub environment where each host segment connects to a hub that represents only one collision domain and only one broadcast domain. Modern wired networks use a network switch to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full duplex links. Collision domains are also found in wireless networks such as Wi-Fi.; CSMA/CA is used in wireless networks.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle". It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is unreliable due to the hidden node problem.

Token Passing

Token passing is a channel access method where a signal called a token is passed between nodes that authorize the node to communicate. The most well-known examples are token ring and ARCNET.

Addressing methods

When multiple computers or devices are connected in a network, signals can be addressed as *unicast*, *multicasts* or *broadcasts*. Unicast refers to one-to-one communication, for example signal is sent from one computer to another. Multicast refers to one-to-may communication, for example signal from one computer or device is sent to selective set of computers or devices. Broadcast refers to one-to-all communication, for example single from one computer or device is sent to all devices and computers in a network.

ASSESSMENT

Answer the following

1. Explain the difference between baseband & broadband.
2. Explain TDM & FDM.
3. Explain CSMA/CD.
4. Explain CSMA/CA.

Fill in the blanks

1. Acronym for TDM ________________________________
2. Acronym for FDM ________________________________
3. Acronym for CSMA ____
4. In _________ a dedicated path is established before transmitting data.
5. In _________ method, data is divided into packets and can take different routes to reach the destination.
6. Define Unicast _____________________________.
7. Define Multicast _____________________________.
8. Define Broadcast _____________________________.
9. Simplex mode of communication ___________________.
10. Half-duplex mode of communication ___________________.
11. Full-duplex mode of communication ____________________.
12. IEEE Standard for CSMA/CD _________________.
13. ________ refers to digital signals that support single communication at a time.
14. ________ refers to analog signals that support multiple signals sent over a single cable.
15. _________ is the mechanism used in wireless networks.
16. X.25 and Frame Relay are examples of __________ methods.

SESSION 4: NETWORK TOPOLOGIES AND ACCESS METHODS

RELEVANT KNOWLEDGE

Network topology refers to the arrangement of computers or devices in a network.

Physical topology refers to the placement of network components including device location & cable installation. *Logical topology* refers to how data is sent or received in a network.

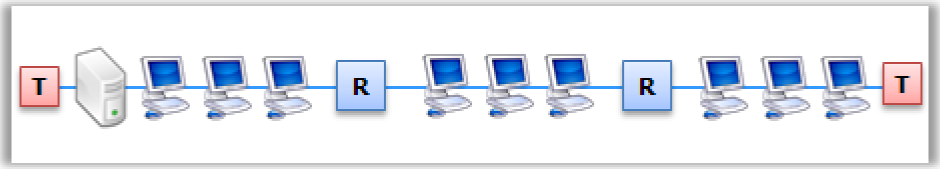
A graphical representation of a physical network is best illustrated through topology. Basic topologies include Bus, Star, Ring, Mesh and Hybrid.

Bus Topology

In bus topology, each node (computer) is connected through a single cable (known as backbone or trunk) used as a common transmission medium for communication. Signal from the source computer travels to all computers connected to the cable until the destination computer accepts the data; if not, the machines ignore the data.

In bus topology, the nodes are interconnected using co-axial cables through the T-Connector that splits the connection between nodes. Terminators are used at both ends to absorb the signal.

Advantages include ease of installation and low cost; however, since all the computers depend on a single cable, a single break or loose connection can cause the entire network to be down and troubleshooting can be difficult.



Bus or Linear Topology

Though bus topology is the simplest form for connecting multiple computers, issues may arise when two computers have a need to transmit at the same time. To handle such collisions, CSMA/CD protocol is used in Bus (Ethernet) implementations.

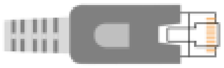
IEEE Standards related to bus topology are 10BASE2 (Thinnet) and 10BASE5 (Thicknet).

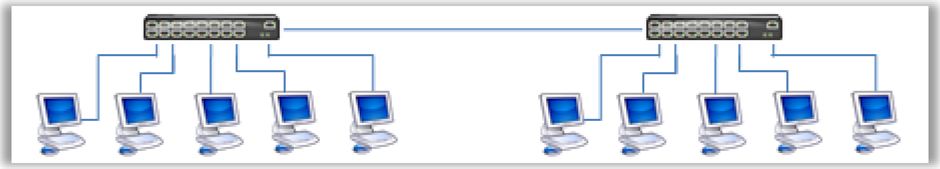
10BASE2 is a variant of Ethernet that uses Co-axial cable; with maximum segment length of 200 meters through practical limit is 185 meters. Maximum number of nodes within a segment is limited to 30. 10BASE5 is similar to 10BASE2 with the exception of distance up to 500 meters and maximum number of nodes up to 100. With the introduction of Ethernet over Twister pair, both 10BASE2 & 10BASE5 are obsolete with very rare exceptions.

Devices called repeaters are used to accommodate more number of computers on a segment. Repeaters amplify and retransmit weak signals to cover longer distances. However, the IEEE design guideline covers the use of repeaters and maximum segments through the 5-4-3 rule; this means that in a collision domain there can be a maximum of 5 segments connected through 4 repeaters, with 3 segments containing active senders. Note that rule is applicable only for 10BASE2 and 10BASE5 shared Ethernet networks (Not for switched Ethernet).

Star Topology

Star topology is the most common and widely used topology today. Each computer is connected to a centralized device called the hub or switch using dedicated cable such as the Twisted-Pair. All signals need to pass through the centralized device. Star topology is considered to be the easiest topology to design and implement as adding additional nodes is simple and easy to troubleshoot in case of single cable failure. However, entire network is affected if the hub or switch goes down.

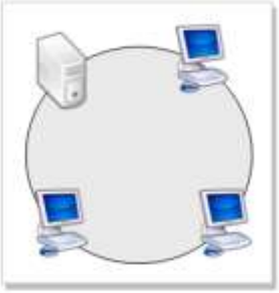
			
Hub	Switch	RJ-45	UTP



Ring Topology

In a ring topology, each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node. Data travels from node to node, with each node along the way handling every packet. Ring topology provides only one pathway between any two nodes, ring networks may be disrupted by the failure of a single link. A node failure or cable break can isolate every node attached to the ring. Ring topology uses physical star topology and logical ring for communication.

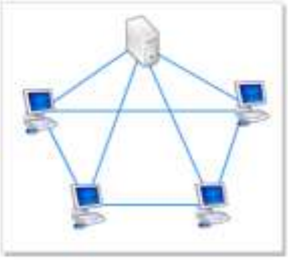
Devices used in ring topology include the Token Ring Network Interface card, Twister pair or fiber optic cables connected to a centralized device called the MSAU (Multistation Access Unit).



IEEE 802.5: IEEE 802.5 standard was derived from IBM token ring networks, this was originally developed by IBM. This has a logical ring topology and token based Media Access Control (MAC).

Mesh Topology

In a mesh topology, all nodes are connected to each other node. A full mesh requires complete connectivity between every node to ensure the data can be delivered one way or the other. This means that there is a high level of redundancy. Since this topology requires connectivity between every node, it is also the most expensive.



Hybrid Topology

Hybrid topology is a combination of two or more topologies mentioned above. For example, two physical star topology based network may be interconnected through a single bus topology.

Twisted Pair

Twisted-Pair cables are widely used in Local Area networks and telephone networks. In a twisted pair cable, two conductors of a single circuit are twisted together for canceling out electromagnetic interference (EMI) from external sources. Types include the UTP (Unshielded Twisted Pair) and STP (shielded Twisted Pair). UTP cables are found in Ethernet networks and telephone systems. RJ-45 (Registered Jack) connectors are used to connect the twisted pair cables to end-points on computer networks. RJ-11 is a connecter used on telephone networks.

IEEE Standards related to star topology are 10BASET, 100BASE-TX, 1000BASET & 10GBASET. Maximum distance supported by twisted pair is 100 meters.

Twisted-pair Ethernet cables can be wired "straight-through" or “Crossover”.

To connect a network interface card to a switch, hub or router, *straight-through* or patch cables are used.

To connect similar devices (network interface card on computer to another network interface on another computer, hub to hub or switch to switch), crossover cables are used.

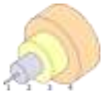
Fiber Optic

A fiber optic cable is a cable containing one or more optical fibers. Fiber-Optic cables are ideal for transmitting data over very long distances at great speeds as light is used for the medium for transmission. Fiber optic cables are not susceptible to any EMI, Near-end Crosstalk (NEXT), or Far-end Crosstalk (FEXT).

Note that you require special network interface cards & network switch that support the fiber optic interface which is usually expensive and common only in large enterprise networks or locations that are susceptible to EMI such as factories that use heavy machineries.

Fiber-Optic cables consist of a high quality glass or plastic strands and a plastic jacket made of Teflon or PVC that protects the cable.

Two types of Fiber-Optic cable exist: *Single-Mode Fiber (SMF)* used for longer distances and *Multi-Mode Fiber (MMF)* used for shorter distances. Signals are transmitted as light signals from source to destination. Either LED or Laser is used. In multi-mode fiber, light signals are transmitted in numerous dispersed path (single-mode fiber use single light source) and making it un-suitable for long distance transmissions.

	
1. Core, 2. Cladding, 3. Buffer, 4. Jacket	Fiber Optic Cable

In some cases, plenum rated cables are used that have a special jacket to protect against fire and emit less smoke than normal cables. However, this is rare and often seen only in industrial or manufacturing sites.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Identify hubs, switches, connectors & cables.
2.	Compare Straight-through & Crossover cables.

ASSESSMENT

Answer the following

1. Explain the devices used in Star Topology.
2. Explain the types of cables used in Star Topology.
3. Explain the advantages of fiber-optic cables.

Fill in the blanks

1. IEEE Standards related to bus topology are __________ & ____________.
2. 10BASE2 is referred as __________.
3. 10BASE5 is referred as __________.
4. ___________ topology is easy and simple to set up.
5. ___________ topology is redundant and considered expensive.
6. ___________ topology is the most widely used topology today.
7. Star topology uses__________ type of cable and _________ type of connectors.
8. Write any three IEEE standards that relate to star topology. _______________, ______________ & ________________.
9. ________ type of cable uses light as a medium of transmission.

10. __________ type of optic cables is used for long distances.
11. __________ cable can be used for connecting two computers without using a switch.
12. ________ cable is used for connecting dissimilar devices such as network switch & desktop.
13. ____________ are devices used for amplifying and retransmitting signals.
14. __________ is the most common cable used today on computer networks.
15. __________ is the category of UTP cable that supports minimum 100 Mbps.
16. __________ cable should be used in locations such as heavy machineries that have high EMI.
17. __________ cable should be used if fire protection is required.
18. __________ mode fiber supports longer distances than __________ mode fiber.
19. Acronym for MSAU ___________________________.
20. Acronym for NEXT ________________.
21. Acronym for FEXT ________________.
22. ___________ is a device used for testing patch cables and pins.

SESSION 5: NETWORK HARDWARE- NETWORK INTERFACE CARD

RELEVANT KNOWLEDGE

TCP/IP Utilities

On computers that have support for networking, a list of utilities is available to configure and troubleshoot network related issues. Often referred to as **TCP/IP utilities**, these utilities are bundled along with the operating system. Though the names of the utilities could vary in spelling, the underlying function is almost the same across operating systems. Given below is a list of utilities (with simple description) You will learn more about them in later sessions.

Utility	Description
IPCONFIG	Internet Protocol Configuration Utility
GETMAC	View MAC or Physical Address of an NIC
PING	Test network connectivity
TRACERT	Trace Route from source to destination
ARP	Resolve IP address to MAC address
Hostname	View computer name or hostname
NETSTAT	View TCP/IP statistics
Nbtstat	View NetBIOS over TCP/IP statistics
Nslookup	View DNS related information
Route	View or modify routing table
PATHPING	Trace packets and view detailed packet information

Note: Use /? for additional help/syntax for each command listed here. For example to know more about IPCONFIG, type IPCONFIG /?

Network devices such as NIC, hub, bridge, switch & routers are devices that help computers to network and communicate. There are a variety of network devices equipped with a wide range of functions.

Network Interface Card (NIC)

Network cards are devices that connect computers to the network. Network cards are both Layer 1 (Physical) & 2 (Data Link) devices as they provide physical access to the medium and also provide physical addressing through the MAC Address.

Network Interface Cards are available for desktop, laptop and server computers. A variety of interface such as PCI, CardBus, USB are available today. Most desktops, laptops, servers and motherboards have built-in NIC.

PCI Ethernet Card for use in Desktops	Cardbus Ethernet Card for use in older laptops	USB Ethernet Card (USB Ethernet converter)

Lab: View Network Interface card installed on a computer

Device Manager is a utility used for configuring & troubleshooting hardware devices such as Network Interface card, sound card, video card, etc. Device manager display the status of devices along with error codes if any. It is commonly used for updating device drivers, disabling/re-installing devices, etc.

Reference: http://support.microsoft.com/kb/310123

NIC's mostly work out of the box, but there might be instances where administrators need to configure or modify NIC settings to match their network environment. Common settings found in most NIC include settings for controlling speed & duplex modes, WOL settings, Power Management, VLAN settings, etc.

Network Interface cards have one or more LED (Light Emitting Diodes) to indicate network conditions like Link status, Network Speed, etc. Usually there are Light Emitting Diodes to indicate Link/Speed (labeled as LINK) and activity (labeled as ACT). For example solid green could mean the device is properly connected to a switch auto negotiated at 100 Mbps / full duplex, blinking orange could mean network activity, no light indicate a problem with network connection, etc.

Lab: View status indicators in a network interface card

Lab: View connectivity status through an Operating System

Lab: View settings of a Network Interface card

Changing duplex setting requires compatibility settings on the switch or hub as well; if the settings don't match, connection will never be made.

Auto-negotiation

Auto negotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support. Priority modes as per 802.3 standards are:

1. 1000BASE-T full duplex
2. 1000BASE-T half duplex
3. 100BASE-T2 full duplex
4. 100BASE-TX full duplex
5. 100BASE-T2 half duplex
6. 100BASE-T4
7. 100BASE-TX half duplex
8. 10BASE-T full duplex
9. 10BASE-T half duplex

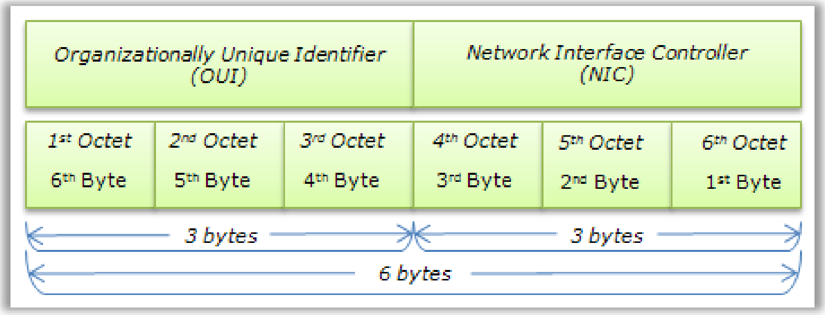
Devices choose the top most in the list if supported at both ends and if not, moves down the priority for other settings in the above mentioned list. Due to affordability of high speed devices (NIC & Switch), 100 or 1000 Mbps speed and full duplex settings are used usually through auto-negotiation, eliminating the need to configure this setting.

MAC Address

Also known as physical address, MAC Addresses are unique to each network interface card. MAC addresses are integrated with the NIC and usually not possible to change. On a network, each station is identified by the MAC Address.

MAC Addresses are governed by IEEE and use 48-bit (2^{48}) addressing scheme providing a total of 281,474,976,710,656 MAC addresses.

MAC Addresses are displayed in hexadecimal format, separated by hyphens. First three octets represent the organization that has been assigned an identifier (called as the *Organizationally Unique Identifier*) and the last three octets are assigned by the organization itself.



GETMAC is a command line utility used for viewing the MAC address of an NIC.

Lab: View MAC Address of a Network Interface Card using GETMAC

Lab: View MAC Address of a Network Interface Card using IPCONFIG

Lab: Identifying the OUI based on MAC address.

Power Management

You may have noticed that the monitor turns off when inactive to save power. This is automatically done by the Operating system for all devices that support Power Management capability. Power Management is a feature that helps in conserving power by turning off devices when not in use. Most NIC's have support for power management so that it can be turned off when not in use to save power.

Standby Mode refers to a low power mode to reduce power consumption; computers cut power to unneeded devices and remain in a low power state - just enough to wake up when required.

Lab: Enable / Disable Power Management

Boot ROM

Normally operating systems are installed on the computer. However, if the computer does not have an operating system installed, you can configure the computer to load an operating system from another computer on its network. To load an operating system from another computer on the network, these computers require a special chip called the BOOT ROM. Boot ROM can be added to the NIC through a special socket or in most cases today, it is often integrated within the NIC.

Computers that are not equipped with floppy disk drives or hard disk drives (diskless workstations) to save cost and to keep the network secure, can be used by loading necessary files from a remote computer on a network. Some computers such as public terminals used in libraries, schools, etc. rely on a centralized computer for processing and storing capabilities; referred to as *Thin Clients* these computers load their operating system and applications from a much powerful computer.

Lab: Change boot sequence to Network Boot

EXERCISE

Perform the following activities until you are confident:

S.No.	Activities
1.	Compare different models of wired network cards available from different vendors. Use the Wired Adapters Worksheet below:

Wired Adapters			
Vendor			
Model			
Interface			
PCI			
USB			
PCMCIA			
Cardbus			
PCI Express			
Number of Ports (RJ-45)			
Supported Speed (Mbps)			
10			
100			
1000			
Connectors			
RJ-45 (UTP)			
Fiber Optic			
Fiber Optic			
Features			
WOL Support (Yes / No)			
Boot ROM (Yes / No)			
Power Management (Yes / No)			

Operating Systems			
Microsoft Windows XP			
Microsoft Windows Vista / 7			
Linux			
IEEE Standards			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			

ASSESSMENT

Answer the following questions

1. Explain the purpose of NIC.
2. Explain the types of NIC's for use in Desktops.
3. Explain the types of NIC's for use in Laptops.
4. Explain MAC address with an example.
5. Explain the purpose of WOL
6. Explain the purpose of Boot ROM.

Fill in the blanks

1. __________ types of NICs are designed for use in desktop computers.
2. __________ types of NICs are designed for use in laptop computers.
3. __________ ype of NICs can be used in both desktop & laptop computers.
4. List any three manufactures of NICs. _______________ , _____________ & ____________.
5. MAC Addresses are displayed in _____________ format, separated by _________.
6. ____________ refers to the procedure through which the devices choose compatible network speed.
7. _____________ is also known as Physical address of an NIC.
8. _________ is a command line utility is used for viewing the physical address of an NIC.

SESSION 6: NETWORK HARDWARE- HUB, SWITCH & ROUTERS

RELEVANT KNOWLEDGE

While setting up a network, you will come across different types of hardware used. The commonly used hardware are hubs, switches and routers.

Hub

A hub is a device that connects multiple computers using a twisted-pair cable. Hubs operate at Layer 1 (Physical). The number of computers that can be connected to a hub depends on the number of ports available (typically 4 to 8). Whenever it receives data from one port, the hub broadcast data to all the devices connected to it, leading to collisions. Hence hubs are referred to as *multiport repeaters*. Since the evolution of SOHO routers and network switches, hubs are rarely used and considered obsolete.

Bridge

Bridge is a device that can connect network segments and separate network traffic based on broadcasts. Bridges examine the frames and selectively transfer frames according to their MAC address. Bridges operate at Layer 2 of the OSI Model.

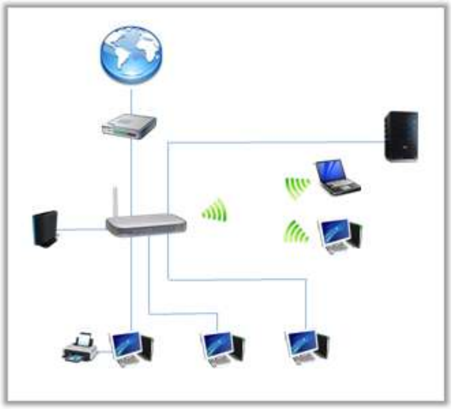
Switch

Switch is a device that allows multiple computers to be connected using twisted-pair cable. Switches (operating at Level 2 – OSI) manage traffic based on MAC (Media Access Control) addresses and are efficient in large networks. Switches are intelligent as they can build a table of MAC Addresses of all the devices connected to ports on the switch and create a virtual circuit for each attached device. Once a packet is received, it is analyzed and forwarded to only the destined station with matching MAC address based on the table.

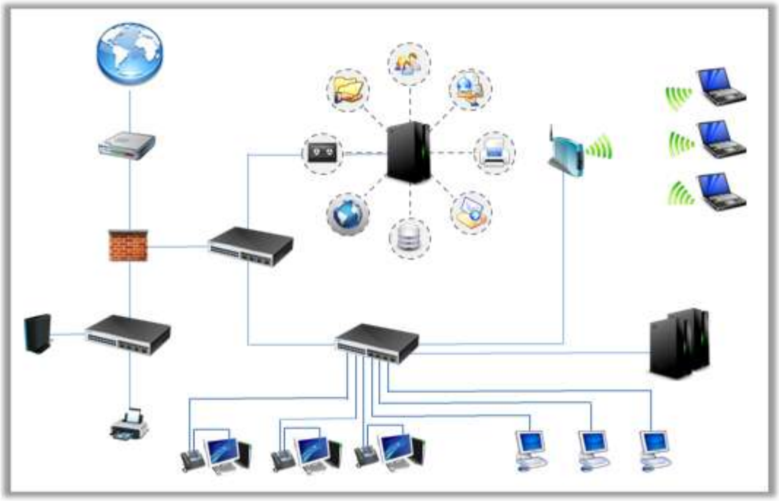
Using switches can eliminate collision as each port in the switch acts as a collision domain. Since switches isolate collision domains, they are referred to as *multiport bridges*. When forwarding frames, switches use Store and forward, cut through, Fragment free or Adaptive switching methods.

Unlike a hub that uses half-duplex communication, a network switch can send and receive at the same time (full-duplex mode) resulting in faster performance.

Number of computers that you can connect to a switch depends on the number of ports available (Typically 4 or 8 on SOHO switches designed for use in home and small business networks and 8 – 32 or 64 on switches designed for use in an enterprise network.). The networks can be extended by adding additional switches usually cascaded from the primary switch. Switches designed for larger networks are cascaded through a special port called the *Uplink* port.



Simple Small Office Home Office Network Setup



An Enterprise network with a variety of networking devices

Categories of switches include:

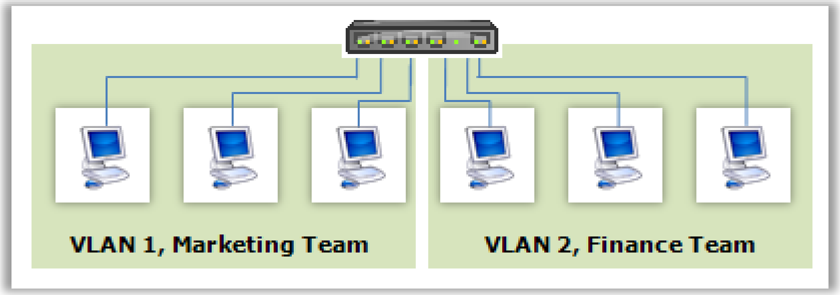
- **Unmanaged** switches are network switches used typically for homes or small offices requiring no administrative configuration.
- **Managed** switches are widely used in enterprise networks and ISP's. These need to be configured by the network administrator before it is used in a network.

VLAN

A single layer-2 network can be partitioned to create multiple distinct broadcast domains, enabling data to be exchanged only between the computers within the domain. This is referred to as VLAN or Virtual LANs. This is created for two primary reasons:

- to reduce collisions
- to implement security.

For example if all the computers in an organization are connected to a single switch, you can isolate them by creating VLAN's for each department resulting in restricted access across departments with maximum access between computers within departments. VLANs can be configured only on Managed switches.



Separate VLANs for marketing & finance team connected to a single switch

Power over Ethernet

PoE describes a standardized system to provide electrical power supply through Ethernet cables; generally, UTP cables carry only signals necessary for data communication. Switches that have support for PoE are generally expensive and in some cases only limited number of Ethernet ports are capable of supporting PoE. Advantages of PoE include the ability to provide power up to 25 watts and distance factor that allows devices to be connected up to 100 meters from the switch.

Router

Routers are Layer 3 devices that allow packets to be routed to different *logical networks*. Routers can discover and transfer packets based on routing table that are pre-determined or self-discovered. Routing tables are either managed by an administrator by manually defining the routes or automated through special configuration to exchange the routing tables with other routers on a logical network. Most common type of routers includes the SOHO router used at home or small office for sharing Internet connection; sophisticated routers are widely used in enterprise networks and ISP's. Similar to SOHO switches, SOHO routers do not need to be configured and routers designed for use in large networks require to be configured before they can be used.

SOHO Router	Enterprise Router

In general, a combination of several routers and switches are used in large networks. Notable manufacturers of routers include Cisco, Nortel Networks, Avaya, HP, Dell, Huawei, etc.

Routing

Routing is the process of selecting paths in a network when sending or receiving packets across computers or devices. Imagine if you are planning to send a parcel to someone; the parcel will travel through different offices, change routes if roadblocks are detected and finally be delivered to the recipient. Similarly when you browse the internet or send an email, packets take different routes (from your computer to your ISP, from your ISP to the next ISP, etc.) until it reaches its destination.

SOHO Router

Also referred to as a residential gateway, SOHO (Small Office Home Office) routers are devices designed for use in small to medium sized networks. Most SOHO routers have combinations of a switch, DSL or cable modem and an access point for Wi-Fi connectivity. These devices are used for two primary purposes:

- Connecting desktops & laptops across home or office.
- Sharing a single Internet connection across desktops & laptops.

Some models include support for connecting peripherals such as printers, USB hard disk drives, etc. through USB ports.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Compare different models of unmanaged switches available from different vendors.

Network Switch			
Vendor			
Model			
Details			
Managed / Unmanaged			
No. of Ports (Ethernet)			
No. of Ports (PoE)			
Speeds			
10 Mbps			
100 Mbps			
1000 Mbps			
IEEE Standards			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
Interface			
10BaseT			
100BaseTx			
1000BaseT			

ASSESSMENT

Answer the following questions

1. Explain the purpose of a Hub.
2. Explain the purpose of bridge.
3. Explain the purpose of network switch.
4. Explain the purpose of PoE.
5. Explain the purpose of a router.
6. Differentiate between hub, switch and router.

Fill in the blanks

1. Hubs operate at the _________ layer of the OSI Model.

2. Switch operates at the ________ layer of the OSI Model.

3. Router operates at the ___________ Network Layer of the OSI Model.

4. _________ are also referred to as multiport repeaters.

5. ___________ type of switches require no administrative efforts.

6. VLAN's, PoE, bandwidth restrictions can be used only on ___________ switches.
7. Acronym for VLAN _________________________.
8. Acronym for PoE ____________________.
9. ___________ layer of OSI Model is used for VLANs.
10. __________ is the process of selecting paths in a network when sending or receiving packets from one computer or device to another.
11. Switches use __________, _____________, ____________ or ____________ methods.
12. __________ switches are used to create VLANs.
13. __________ are also referred to as multiport bridges.

SESSION 7: PROTOCOLS

RELEVANT KNOWLEDGE

Protocols are a set of standards that allow network devices to communicate and exchange information. Protocols define how devices start, manage and end communication; most protocols are described by IETF (Internet Engineering Task Force) as RFC's (Request for Comments).

Protocols are set of rules for communication. In a computer network, all computers need to use the same protocol for communication. Protocols may include signaling, authentication and error detection and correction capabilities. Protocols address data formats, address formats, error detection techniques, sequence & flow control, routing and other requirements for communication. In a network, multiple protocols are used during communication. Examples of protocols at the network layer are *NetBEUI, IPX/SPX, TCP/IP, AppleTalk, etc*.

The NetBEUI protocol is used to connect and communicate between computers with Microsoft Windows as the operating system. Similarly AppleTalk protocol is used to connect and communicate among computers with MAC OS. However, when connecting computers with different operating systems you need to use a standardized protocol such as the TCP/IP protocol.

Proprietary & Open Standard Protocols

Proprietary protocols are communications protocol owned by a single organization or individuals. Usually proprietors enforce technical and licensing restrictions through patents to keep the specification as a trade secret. Examples include NETBEUI from Microsoft, IPX/SPX from Novell, AppleTalk from Apple, etc.

Open Standard protocols are communication protocols that are publicly available, have various rights to use associated with it, and may also have various properties of how it was designed. Example, TCP/IP.

NetBEUI

NetBEUI is a non-routable protocol used for Microsoft Networks. NetBEUI (NetBIOS Extended User Interface) is ideal for small networks. In this protocol, each device must have a unique name (referred to as the workstation name) of max 15 character length. NetBEUI is not efficient on large networks or routable, hence it is not used much today.

IPX/SPX

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) is a routable protocol used in Novell NetWare networks. IPX operates at the Network Layer and SPX at the Transport Layer. NWLink IPX/SPX is a protocol developed by Microsoft that is compatible with IPX/SPX Protocol.

AppleTalk

AppleTalk is a proprietary suite of networking protocols developed by Apple Inc. for their Mac computers. AppleTalk included a number of features that allowed local area networks to be connected with no prior setup or the need for a centralized router or server of any sort. Connecting together AppleTalk equipped systems would automatically assign addresses, update the distributed namespace, and configure any required inter-networking routing. It is a plug-n-play system.

TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) is a routable protocol suite that is also known as the Core Protocol of the Internet Protocol Suite. TCP/IP has gained popularity as it is very efficient in very large networks; most operating systems include support for TCP/IP.

Unlike many other protocols, TCP / IP have the following benefits:

- Open Standard (not tied to any vendor unlike proprietary protocols)
- Enable communication between different Operating Systems (almost every operating system including flavors of Unix, Windows, Mac OS support TCP / IP)
- Runs on any network framework (Ethernet, Token Ring, Dial-Up connections)
- Routable & a common addressing scheme.

TCP/IP protocol suite is the most widely used protocol today including LAN's and WAN's. Internet uses TCP/IP as its protocol.

IP

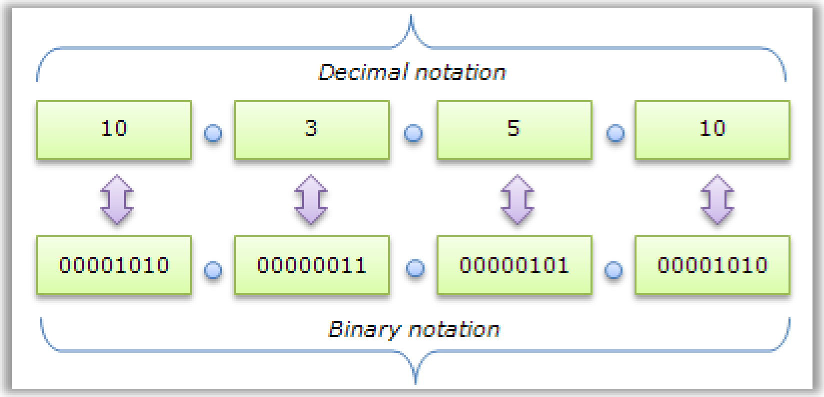
Internet Protocol is the primary communication protocol used for relaying data across network boundaries. Functions include logical addressing and routing. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the internet. Its successor is Internet Protocol Version 6 (IPv6), which is increasingly being used.

IPv4

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

IP (IPv4) use a 32-bit address that will provide 4,294,967,296 (2^{32}) possible addresses and has two parts: Network ID (Portion of the address that represents the network that a device belongs to) and Host ID (Portion of the address that represents the host on a particular network). Network & Host portion of an IP address is decided based on an additional value called the Subnet Mask. Each device on an IP network must have a unique IP address for communication.

IP addresses are binary numbers (image below), but they are usually stored in text files and displayed in human-readable notations such as 10.3.5.10 (image below).



IANA

Internet Assigned Numbers Authority (IANA) is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. IANA is a department operated by the Internet Corporation for Assigned Names and Numbers, also known as ICANN.

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

Classful Network

Classful network is an addressing schedule originally introduced in 1981 and used for several years until the introduction of CIDR method. In this method, the 32-bit address space is divided into five addresses classes namely A, B, C, D and E. Each class defines a fixed network size and number of hosts within networks.

Following table summarizes the classes of IPv4 addressing:

Class	Range	Subnet	No. of Networks	No. of Hosts / N
A	0.0.0.0 - 126.255.255.255	255.0.0.0	126	16,777,214
B	128.0.0.0 - 191.255.255.255	255.255.0.0	16,384	65,532
C	192.0.0.0 - 223.255.255.255	255.255.255.0	2,097,152	254
D	224.0.0.0 - 239.255.255.255	Multicast		
E	240.0.0.0 - 255.255.255.255	Reserved for future use		

Examples of Class A IP Addresses: 5.2.2.1, 12.1.1.14, 72.34.23.23

Examples of Class B IP Addresses: 129.1.2.3, 160.2.3.34, 190.2.3.4

Examples of Class C IP Addresses: 200.12.3.4, 202.13.14.15, 220.3.2.3

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	1. Identify the class for the following IP addresses: a. 7.1.2.3, Class ___ . b. 45.43.32.12, Class ___ . c. 183.12.34.22, Class ___ . d. 203.23.12.33, Class ___ . e. 219.44.34.23, Class ___ . f. 130.34.54.12, Class ___ .

ASSESSMENT

Answer the following questions

1. Explain Proprietary Protocols with an example.
2. Explain Open Standard Protocols with an example.
3. What is IP?
4. List the classes of IPv4.

Fill in the blanks

1. Protocols are set of rules for communication.
2. Examples of Proprietary Protocols ____________ , ___________ & ____________.
3. Acronym for NetBEUI ______________________.
4. Acronym for IPX/SPX ______________________.
5. Acronym for TCP/IP ________________________.
6. __________ is an example of a protocol that is Open Standard.
7. Versions of IP are ______ & ______.
8. _____ is a connectionless protocol used on packet-switched networks.
9. Acronym for IANA _______________________.
10. IPv4 uses ______ 32-bit addressing scheme
11. IP address classes are ______ , ______ , ________ , _________ & ________.
12. Number of logical networks in Class A _____ and host per network ________.
13. Number of logical networks in Class B _____ and host per network ________.
14. Number of logical networks in Class C _____ and host per network ________.
15. Range of IP Address Class A ___________________.
16. Range of IP Address Class B ___________________.
17. Range of IP Address Class C ___________________.
18. Range of IP Address Class D ___________________
19. Range of IP Address Class E ___________________.
20. _____________ class of IP addresses are reserved for multicasting.

SESSION 8: IP ADDRESS

RELEVANT KNOWLEDGE

As you have learnt about IP addresses in the previous session, you know that IP addresses are seen as numbers or numeric values such as 10, 192, 182, etc. However, computers use binary language and translate decimal to binary and vice versa behind the scene.

IP addresses assigned to a host or a computer can be public or private.

Public IP Address

Public IP addresses are IP addresses obtained from an ISP by organizations to provide services such as web hosting, email, etc. This is similar to that of a cell phone number that is required for your make and receive phone calls. If you want to provide a service such as free email for users (like Gmail) or an online shopping mall for your customers, you must have a public IP address assigned to the computer serving such requests.

Regional Internet Registry (RIR) is an organization that manages the IP address allocation and registration within particular regions across the world. Public IP addresses are allocated to ISP’s which in turn is allocated by the ISP to customers.

When you rent or lease an Internet connection from an ISP such as DSL, Cable, Dial-up, etc. you are given only a dynamic IP address that changes in most cases every time you re-connect; ISP’s issue the same IP address to different customers on a rotation basis to reduce the incurred cost. If you want to provide an Internet based service such as free mails or a website on your computer, you need to get a dedicated or static IP address which can be leased from the ISP for a fixed fee.

Private IP Address

Private IP addresses are addresses used in private networks such as homes and internal office networks. Private IP addresses need not be purchased as it is meant for private use and anyone can use the private address without approval from a regional Internet Registry (RIR); private IP addresses will not connect to public address and vice versa. This is similar to that of extension numbers that can be used only for calling each other telephone numbers with an office.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:

Class	IP address range	number of addresses
A	10.0.0.0 – 10.255.255.255	16,777,216
B	172.16.0.0 – 172.31.255.255	1,048,576
C	192.168.0.0 – 192.168.255.255	65,536

Most common use of private addresses is in residential networks; since most Internet service providers (ISPs) only allocate a single public IP address to each residential customer, but many homes has more than one computer or other Internet connected device, such as IP telephones or IP televisions. In this situation, a network address translator (NAT/PAT) gateway is usually used to provide Internet connectivity to multiple hosts that translates private to public IP address and vice versa.

Private addresses are also commonly used in corporate or enterprise networks, which for security reasons, are not connected directly to the Internet. Often a proxy, SOCKS gateway, or similar devices are used to provide restricted Internet access to internal users.

IPCONFIG is a command line utility used for managing IP configuration. IPCONFIG is used typically for viewing IP configuration of a computer; however, additional administrative tasks are also possible using this command.

Lab: Determine if the IP address is Private or Public using IPCONFIG

Lab: Converting from Binary to Decimal & vice versa.

Lab: Identifying Network & Host ID of the IP Addresses.

EXERCISE

Perform the following activities till you are confident:

<table>
<tr><th>S.No.</th><th>Activities</th></tr>
<tr><td>1.</td><td>Identify the Network & Host ID of the following IP Addresses with Subnet Masks.
<table>
<tr><td>Computer ID</td><td>IP Address</td><td>Subnet Mask</td></tr>
<tr><td>Computer A</td><td>10.1.1.3</td><td>255.0.0.0</td></tr>
<tr><td>Computer B</td><td>10.1.2.3</td><td>255.0.0.0</td></tr>
<tr><td>Computer C</td><td>10.23.1.3</td><td>255.0.0.0</td></tr>
<tr><td>Computer D</td><td>11.2.1.2</td><td>255.0.0.0</td></tr>
<tr><td>Computer E</td><td>11.2.3.2</td><td>255.0.0.0</td></tr>
<tr><td>Computer F</td><td>141.23.12.12</td><td>255.255.0.0</td></tr>
<tr><td>Computer G</td><td>202.13.14.12</td><td>255.255.255.0</td></tr>
</table>
</td></tr>
</table>

Answer the questions in the following sections:

Section 1:

1. Network ID of Computer A: ______________________
2. Network ID of Computer B: ______________________
3. Network ID of Computer C: ______________________
4. Network ID of Computer D: ______________________
5. Network ID of Computer E: ______________________

Section 2:

1. Host ID of Computer A: ______________________
2. Host ID of Computer B: ______________________
3. Host ID of Computer C: ______________________
4. Host ID of Computer D: ______________________
5. Host ID of Computer E: ______________________

Section 3:

1. Will Computer A be able to communicate with Computer B?
2. Will Computer A be able to communicate with Computer C?
3. Will Computer C be able to communicate with Computer D?
4. Will Computer D be able to communicate with Computer E?
5. Will Computer F be able to communicate with Computer G?
6. What is required for Computer A to be able to communicate with Computer E?

ASSESSMENT

Answer the following questions

1. Explain the purpose of Public IP address with an example.
2. Explain the purpose of Private IP address with an example.
3. Explain the purpose of Subnet Masks.
4. Explain the procedure to determine the network ID and host ID of an IP address with an example.
5. Explain the purpose of IPCONFIG utility with an example.

Fill in the blanks

1. Acronym for RIR ______________________________ .
2. ____________ IP addresses are required to communicate with other computers on the Internet.

3. ____________ IP addresses are used within Local Area Networks such as home or office networks.
4. _____________ , ________________ & _______________ are reserved ranges of Private IP Addresses.
5. ________ is a command line utility for working with IP configuration in a computer.
6. Device that is required for transmitting data across different logical networks ____________ Router.
7. 123.43.12.11 is an example of Class _____ IP address.
8. 223.143.112.18 is an example of Class _____ IP address.
9. 74.13.123.14 is an example of Class _____ IP address.
10. Identify the IP Address that can be assigned to a computer from the table below:

IP Address	Can be assigned, True / False
0.0.0.1	
1.0.1.1	
255.1.1.1	
254.1.1.1	
127.0.0.1	

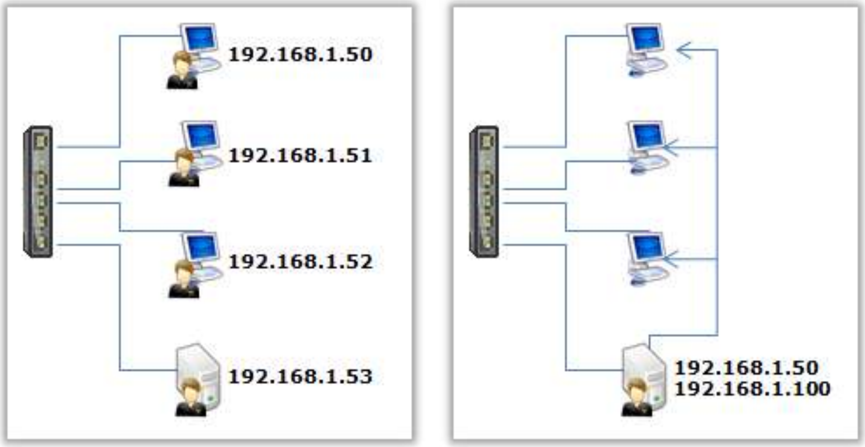
SESSION 9: IP ADDRESS ASSIGNMENT

RELEVANT KNOWLEDGE

You have learnt about identifying network & Host ID's of an IP address, public and private IP addresses in the previous session. IP addresses are assigned by administrators either manually or automated through DHCP servers. In this session, you will learn about IP address assignment. You will learn about DHCP servers later on.

IP Address Assignment

Internet Protocol addresses is assigned to a host either on booting (when on the OS starts), or permanently by a fixed configuration of its hardware or software. Administrators can allocate and assign unique non-changing IP addresses to hosts or computers. Such addresses are called *Static IP address*. On large networks, administrators automate the IP address assignment using a special service called the DHCP that assigns IP addresses automatically; such dynamically assigned addresses are called *Dynamic IP address*.



Static IP provided by Administrator for each computer or host (left) and a DHCP Server configured to assign a dynamic IP address through a pre-defined range.

If you want to host a website or provide email services to employees or users, generally you should use static IP addresses. If you want to provide Internet access to users, you can use dynamic IP address. Dynamic IP addresses are assigned by a network device such as SOHO Router or Servers that have DHCP capability.

Lab: Assign static IP address to computers.

PING is a command line utility used for testing network connectivity. PING operates using ICMP echo request packets for its response from another computer and measures the time taken by the packet from transmission to reception (referred to as Round-Trip). PING is widely used by administrators to understand and troubleshoot network related issues particularly at the network layer of the OSI model.

Lab: Check network connectivity using PING (LAN)

ARP or Address Resolution Protocol is used for resolving IP addresses to MAC address. When two computers communicate using IP address (Layer 3) on the same subnet, IP address will be resolved to MAC address (Layer 2) and they start communicating using MAC Address through Network Switch. Thus ARP, a layer 3 protocol serves as an intermediate between Layer 3 and Layer 2 establishing connectivity between network layer and the Ethernet.

Once resolved, mapping of IP Address to MAC addresses are stored in cache for some time for future use. Entries resolved automatically are referred as dynamic entries and is used most of the time.

Lab: ARP

Loopback IP Address

Loopback IP address is a special IP address reserved for testing local machine's NIC or device drivers or TCP/IP stack within the local computer. It cannot be assigned to any computer and is implemented at the software level. IP address in the range of 127.0.0.1 to 127.255.255.254 is reserved for loopback address. However, 127.0.0.1 is most commonly used for testing and management purposes by administrators.

Lab: Test Loopback IP

CIDR

Assigning numbers based on Classful network was easier during early stages of networking networks were smaller. As time evolved, due to explosive growth of the Internet, IP addresses were getting exhausted. An addressing scheme, CIDR (Classless Inter-domain Routing), was introduced for efficient use of IP addresses.

If you have noticed, a Class A IP address can accommodate 16 million hosts. However, in most organizations the number of computers will be probably in thousands and not millions. Assuming if an organization has around 2000 computers, imagine the wastage of number of IP addresses if Class A was used.

Similarly, a Class C IP address can accommodate only 254 host; and in the same situation, the IP address range is insufficient and multiple ranges from Class C will be needed. CIDR helps resolve these issues.

Lab: Use CIDR Method

Lab: Use the decimal to binary conversion to determine network ID & Host ID by using CIDR Method.

Special IPv4 Addresses

Given below is a list of special IP addresses that cannot be assigned to any computer as they are reserved for specific functions.

IP Address	Description
0.0.0.0	Refers to unspecified IP address indicating the absence of an IP address.
255.255.255.255	Refers to the broadcast address, used for broadcasting in a network. IP broadcasts are used by DHCP & BOOTP clients.
127.0.0.1	Referred to as loopback address, it is assigned to the internal network adapter.
169.254.x.x	Reserved for Auto IP.

EXERCISE

Perform the following activities till you are confident:

<table>
<tr><th>S.No.</th><th>Activities</th></tr>
<tr><td>1.</td><td>Identify the Network & Host ID of the following IP Addresses with Subnet Masks.
<table>
<tr><th>Computer ID</th><th>IP Address</th><th>Subnet Mask</th></tr>
<tr><td>Computer A</td><td>10.13.1.3</td><td>255.255.0.0</td></tr>
<tr><td>Computer B</td><td>10.13.5.3</td><td>255.255.0.0</td></tr>
<tr><td>Computer C</td><td>10.23.1.3</td><td>255.255.255.0</td></tr>
<tr><td>Computer D</td><td>101.27.1.2</td><td>255.255.255.0</td></tr>
</table>
</td></tr>
</table>

Computer E	101.27.1.112	255.255.255.0
Computer F	192.168.2.5	255.255.0.0
Computer G	192.168.20.5	255.255.0.0

Answer the questions in the following sections:

Section 1:

1. Network ID of Computer A: ________________________
2. Network ID of Computer B: ________________________
3. Network ID of Computer C: ________________________
4. Network ID of Computer D: ________________________
5. Network ID of Computer E: ________________________

Section 2:

6. Host ID of Computer A: ________________________
7. Host ID of Computer B: ________________________
8. Host ID of Computer C: ________________________
9. Host ID of Computer D: ________________________
10. Host ID of Computer E: ________________________

Section 3:

7. Will Computer A be able to communicate with Computer B?
8. Will Computer A be able to communicate with Computer C?
9. Will Computer C be able to communicate with Computer D?
10. Will Computer D be able to communicate with Computer E?
11. Will Computer A be able to communicate with Computer E?
12. Will Computer E be able to communicate with Computer F?

2.	Assign Static IP address to computers, verify network connectivity.

ASSESSMENT

Answer the following questions

1. Explain the procedure of assigning a static IP address with an example.
2. Explain the PING utility with an example.
3. Explain the purpose of loopback IP address and its range with an example.
4. Explain the purpose of CIDR Method with an example.
5. Explain ARP.

Fill in the blanks

1. Acronym for ARP ________________________________.
2. Acronym for CIDR ____.
3. ______________ protocol is used by ping utility for displaying messages.
4. ICMP operate at _____________ layer of the OSI Model.
5. Acronym for ARP ____.
6. 22.123.12.255 is an example of ___________ address.
7. Number of bits in IPv4 address ____.
8. __________ is a command line utility used for testing network connectivity.
9. ___________ protocol is used for translating IP addresses to MAC addresses.
10. __________ is a command line utility used for managing ARP Cache.
11. IP address range reserved for loopback purpose ___________________.
12. IP address assigned through DHCP is referred to as ___________ IP addresses.

SESSION 10: TRANSPORT LAYER PROTOCOLS - TCP & UDP

RELEVANT KNOWLEDGE

You have learnt about IP Addressing and IP assignment in the earlier sessions. While network layer protocols are used for logical addressing and routing, transport layer protocols provide end-to-end communication between hosts or computers on a TCP/IP Network.

Transport Layer Protocols

Transport layer protocols (Layer 4 of OSI model) provide end-to-end communication services for applications. The transport layer provides convenient services such as connection-oriented data stream support, reliability, flow control, and multiplexing. Well-known protocols at this layer are TCP & User Datagram Protocol (UDP).

User Datagram Protocol (UDP) is a transport layer protocol that is used for sending messages to other hosts on the network without prior communications, to set up special transmission channels or data paths. UDP does not provide reliability, ordering, or data integrity. UDP assumes that error checking and correction is either not necessary or performed in the application, hence avoiding the overhead of such processing at the network interface level.

UDP's stateless nature is also useful for servers answering small queries from huge numbers of clients, such as Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP), IP tunneling protocols and many online games.

Transmission Control Protocol (TCP) provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on a different computer on the network.

TCP is the protocol used by major Internet applications such as the World Wide Web, email, remote administration and file transfer. UDP is used either by applications that have a built-in facility to check reliability or when transfers happen that do not require reliability. UDP has less overhead than TCP.

TCP	UDP
Reliable	Unreliable
Connection Oriented	Connectionless

Segment Sequencing	No Sequencing
Acknowledge Segments	No Acknowledgement
Segment retransmission and flow control	No retransmission

Ports & Sockets

Today computers use a variety of network applications such as browsers, email clients, chat software, etc. simultaneously and are assigned only a single IP address. To avoid conflicts, port numbers are standardized by IANA for most network applications. When a network application from a client attempts to connect to corresponding network application to a server, the operating system uses a combination of the assigned IP address along with a port number referred to as a *socket* for end-to-end communication.

Computers that have single IP address can host a variety of services using different port numbers eliminating the need for having multiple IP address. For example, a computer assigned with an IP address 12.1.1.1 can run a web server using port 80 and an ftp server using port 21.

Port numbers range from 0 to 65,535 as it uses a 16-bit scheme (2^{16} = 65,536). 0 is reserved and cannot be used and the actual range is between 1 to 65535.

Network applications are designed to use a single port number or range or port numbers. Some network applications such as network & Internet games, video conferencing software, etc. may use a dynamic range of port numbers for communication. For example Apple's QuickTime Streaming Server uses UDP as its transport protocol in the 6970-9999 range.

Note: To know about the port numbers and range for specific network application, refer to product manual or the vendor's website.

IANA Well-Known Ports

Port numbers in the range from 0 to 1023 are referred to as well-known ports. Look at the following table that summarizes the standardized port numbers for common application layer protocols:

Port Number	Transport	Description
0	TCP, UDP	Reserved
20	TCP	FTP (Data)

21	TCP	FTP (Control)
23	TCP	Telnet
25	TCP	SMTP
53	UDP	DNS Query
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
111	UDP	RPC
119	TCP	NNTP
137	UDP	NETBIOS Name Service
143	TCP	IMAP4
161	UDP	SNMP
389	TCP	LDAP
443	TCP	HTTPS

Note: Only partial list of port numbers are included in this table; See the *Service Name and Transport Protocol Port Number Registry* of IANA for complete list of assigned ports.

Port numbers from 1024 to 49151 are the registered ports and are assigned by IANA for specific applications from products from a variety of vendors. Port numbers above 49151 are dynamic or private ports.

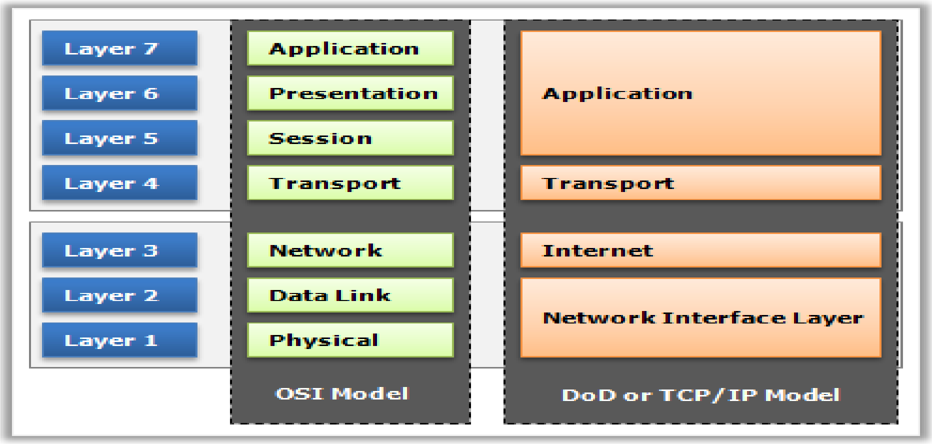
NETSTAT

NETSTAT (i.e. Network statistics), is a command line utility used for viewing port numbers used by network applications. This command is used to understand and troubleshoot any network or transport later issues.

Lab: Use NETSTAT to view Ports & status

TCP/IP model

DoD (Department of Defense) or TCP/IP Model simplifies the 7 layer OSI Model into a 4 layer model (figure below):



OSI (7 Layers) vs. TCP/IP Model (4 Layers)

1. *Network Interface or Link Layer* specifies how data is physically sent on a network using electrical, optical or radio waves. This layer includes devices such as NIC that directly interface with a network medium such as a UTP Cable.
2. *Internet Layer* specifies IP packets sent on a Packet Switched Network and is same as the Network Layer.
3. *Transport Layer* specifies how communication session takes place between computers and is the same as the Transport Layer discussed earlier.
4. *Application Layer* specifies how applications and protocols communicate between end points. This layer combines Session, Presentation & Application layers of the OSI Model.

Note: Different applications use several protocols that are a part of the *TCP/IP Protocol Suite* operating at each layer of the OSI model.

Lab: Refer to common protocols TCP/IP protocol suite.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Complete the following activity to understand using the NETSTAT Utility. 1) Open different websites in a web browser and… a. Use Netstat –n while it is loading the website & after b. Use Netstat –f while it is loading the website & after

	c. Use Netstat –n while it is loading the website & after 2) Open your email messaging software and… a. Use Netstat –n while it is loading the website & after b. Use Netstat –f while it is loading the website & after c. Use Netstat –n while it is loading the website & after Run the command several times and observe the results.

ASSESSMENT

Answer the following

1. Explain the purpose of Transport Layer Protocols.
2. Explain UDP.
3. Explain TCP.
4. Differentiate TCP & UDP
5. Explain sockets with an example.

Fill in the blanks

1. Acronym for TCP ________________________________.
2. Acronym for UDP ________________________________.
3. ____________ is a command line utility is used for viewing network statistics.
4. __________ is a transport layer protocol has less overhead and higher performance than TCP.
5. __________ is a transport layer protocol provides reliability.
6. Acronym for ARP ________________________________.
7. Acronym for IMAP ______________________________.
8. Acronym for LDAP ______________________________.
9. Acronym for FTP ________________________________.
10. Default port number for HTTP ________ .
11. Default port number for DNS Query ________ .
12. Default port number for POP3 ________ .
13. Default port number for SMTP ________ .
14. Default port number for IMAP4 ________ .
15. Default port number for LDAP ________ .
16. Default port number for HTTPS ________ .
17. Default port number for Telnet ________ .
18. Acronym for IGMP ___________________ .
19. Acronym for ARP ___________________.

20. Acronym for RARP ____________________ .
21. Acronym for DHCP____________________ .
22. Acronym for IMAP ____________________ .
23. Acronym for LDAP ____________________ .
24. Acronym for SNMP ____________________ .
25. Acronym for SSL ____________________ .
26. Well-known ports range from _____ to _______ ..
27. Dynamic ports start above __________ ..
28. DOD or TCP/IP model has __ layers.

SESSION 11: SERVER OPERATING SYSTEMS

RELEVANT KNOWLEDGE

Server Operating Systems(SOS) are system software that run on a server and enable the server to manage data, users, groups, security, applications, and other networking functions. SOS use the client/server architecture. Popular network operating systems are Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, several Linux distributions, Mac OS X, Novell NetWare, and BSD.

On a medium to large sized networks, special services are required for managing day-to-day operations such as data sharing, email & Internet access, printer access, etc. Hence, tight security may be needed to prevent unauthorized users from accessing or manipulating network resources.

Initially, multiple software were used to provide different networking functions. However, today these needs are taken care of by the server operating systems thereby eliminating the need to purchase additional software.

Advantages	Disadvantages
Centralized Management Higher Level of Security Can be accessed from remote locations	Initial cost can be high Requires special technical expertise Requires regular maintenance

Server Operating systems include support for a variety of functions (not limited to):

- Name Server (DNS, WINS, DDNS)
- Database Server
- Communications Server
- Mail Server
- File Server
- Print Server
- Proxy Server
- Web Server
- Remote Access Server
- Gaming Server
- Terminal Server, etc.

Generally, computers used for serving large number of requests and offering multiple services require powerful hardware. For example a server in a LAN environment, serving 20 – 30 users, would need comparatively less powerful hardware as against one serving millions of users. Servers used in medium to enterprise networks or ISP's need multiple processors, large working memory, extremely large storage and multiple network adapters and, the operating system installed on such computers should be capable of managing this hardware. Nowadays, popular server operating systems such as Microsoft Windows Server, Linux etc. offer features that support the latest, powerful hardware.

Some of the popular server or network operating systems are listed below:

Microsoft Windows Servers

Windows Servers refers to the brand of Server Operating Systems released by Microsoft. Following are the list of Server Operating Systems till date:

- Microsoft Windows NT 4.0 Server
- Microsoft Windows 2000 Server, Advanced Server & Datacenter Editions
- Microsoft Windows 2003 Web, Standard, Enterprise & Datacenter Editions
- Microsoft Windows 2008 Web, Standard, Enterprise & Datacenter Editions
- Microsoft Windows 2012 Foundation, Essentials, Standard & Datacenter Editions

UNIX

UNIX is a multitasking, multi-user computer operating system. UNIX operating system is widely used in servers, workstations, and mobile devices.
Based on UNIX Kernel, there are several variants available today. Following is a partial list of UNIX Variants:

- SUN Solaris
- IBM AIX
- BSD OS
- Digital Unix
- HP-UX
- MAC OS X Server, etc.

Linux

Linux is a Unix-like operating system assembled under the model of free and open source software development and distribution. Linux kernel was initially conceived and created by Finnish computer science student ***Linus Torvalds*** in 1991 and today, Linux kernel has received contributions from thousands of programmers across the globe.

It is one of the leading Operating System used on Servers, Mainframes, Smart Phone and Supercomputers. Users & administrators operate a Linux-based system through a command line interface (CLI) or a graphical user interface (GUI).

Linux is packaged in a format known as a Linux distribution through which users install Linux on their desktops or servers. Popular distributions include:

- Debian
- Redhat
- openSUSE
- Android
- Ubuntu
- Bharat
- Fedora, etc.

Debian

openSUSE

Redhat

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Discuss different distributions of Linux. Use the following links for reference: http://en.wikipedia.org/wiki/Linux http://en.wikipedia.org/wiki/Linux_distribution http://en.wikipedia.org/wiki/Red_Hat http://en.wikipedia.org/wiki/SUSE http://en.wikipedia.org/wiki/Ubuntu_(operating_system)
2.	Compare different editions of Server Operating Systems from Microsoft; use the following URL's for reference: http://en.wikipedia.org/wiki/Windows_Server_2003 http://en.wikipedia.org/wiki/Windows_Server_2008 http://en.wikipedia.org/wiki/Windows_Server_2012

ASSESSMENT

Answer the following questions

1. Explain the purpose of Server or Network Operating Systems.
2. Explain any five functions of a Server Operating System.
3. List the editions of Microsoft Windows 2008.
4. List any five variants of UNIX.
5. List any five distributions of Linux.

Fill in the blanks

1. Write five functions of a Server Operating System. ____________ , ____________ , ________________, ________________ & ________________.
2. List the editions of Windows 2003. ______________ , ________________ , _____________ & ______________.
3. List the editions of Windows 2008. ______________ , ________________ , _____________ & ______________.
4. List the editions of Windows 2012. ______________ , ________________ , _____________ & ______________.
5. List any 5 variants of UNIX. _____________ , ___________ , _____________ , _____________ & ______________.
6. List any 5 Linux distributions. _____________ , ___________ , _____________ , _____________ & ______________.

SESSION 12: NETWORKING SERVICES - DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

RELEVANT KNOWLEDGE

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure network devices to enable them to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate with other computers on the network and/or access the internet.

DHCP is widely used in enterprise networks and by ISP's as they usually serve a large number of computers. On large networks, using DHCP servers helps administrators to automate the procedure of assigning IP addresses to individual computers on the network.

DHCP infrastructure consists of:

- DHCP Servers
- DHCP Clients

DHCP server maintains a database of IP addresses and configuration information. When it receives a request from a client, the DHCP server allocates an IP address from a given range and sends the configuration information to the client. DHCP servers are preconfigured with a range of IP address and additional network configuration information by the administrator. Like other TCP/IP services, DHCP uses port numbers 67 & 68.

DHCP Process

DHCP follows a basic process to automatically configure a DHCP client, widely referred to as ***DORA***:

1. DHCP client sends a *DHCP **D**iscover* message.

2. DHCP server(s) responds with a *DHCP **O**ffer* message.

3. DHCP client selects an IP address offered and sends a *DHCP **R**equest* message to request use of this configuration.

4. DHCP server assigns the IP address and sends *DHCP Acknowledge* message to the client.

   The DHCP Request message identifies the server whose offer the DHCP client selected. The other DHCP servers which had sent offers, place their offered IPv4 addresses back into the available pool of addresses.

Lab: Install & configure DHCP Server
Lab: Configure clients for Dynamic IP
Lab: Check network connectivity using PING (LAN)

Auto-IP

Computers configured as DHCP clients receive an IP addresses from a DHCP server. If the DHCP server is unavailable or the DHCP has exhausted all its IP address, DHCP clients will never receive an IP address. This could lead to communication problems between computers on a network.

To addresses such issues, Auto-IP comes into effect. In this process, computers or hosts select a random IP address within a reserved range (built-in within the operating system) in order to communicate with other computers within that network. To ensure there are no IP conflicts in this automated process, hosts use ARP probes to determine if the address is already in use in the network; if there is a conflict, another random address within the range is selected. The IP address is used only when there are no replies to the ARP probe, indicating availability of the address.

Internet Engineering Task Force has reserved the address block 169.254.1.0 through 169.254.254.255 for Auto-IP reserve range in IPv4. Auto-IP is a feature found on most recent operating systems starting with the release of Microsoft Windows XP. Recent MAC OS and linux distributions also have support for Auto-IP.

Lab: APIPA demonstration

File and Print Sharing

Once you have setup the computer to work in a network, you can share files and printers among other computers in a network. You can use a variety of protocols for file and print sharing depending on the level of support that is available within the operating system. Likewise, you can use either static or dynamic IP addresses as well and share or access files across different computers in a network.

Lab: Share files on a computer

Lab: Access a shared folder from another computer

Lab: Share a printer attached to a computer

Lab: Access a shared printer

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Set up the DHCP Server to use the following details: IP Range: 10.1.1.1 to 10.1.1.50 Subnet Mask: 255.255.255.0 Gateway: 10.1.1.100
2.	Share different folders, share using Read & Full Control Permissions and access from other computers.
3.	Install different printer models, share and access from other computers.

ASSESSMENT

Answer the following questions

1. Explain the purpose of DHCP.
2. Explain the DORA Process.
3. Explain the procedure to install DHCP Server.
4. Explain the procedure to configure a DHCP Server with a Scope.
5. Explain the purpose of Auto-IP.
6. Explain the procedure to share a folder (based on lab).
7. Explain the procedure to access a shared folder (based on lab).
8. Explain the procedure to share a local printer (based on lab).
9. Explain the procedure to access a shared local printer (based on lab).

Fill in the blanks

1. Acronym for DHCP ____.
2. __________ protocol is used for automatic configuration of IP addresses.
3. Acronym for UNC ________________________________.
4. Acronym for APIPA _______________________________.

5. Computers that will be used as DHCP Servers must have a ________ IP address.
6. _____________________ through _______________ is reserved for Auto-IP by IETF.
7. With respect to file sharing, maximum number of simultaneous connections supported by Windows vista / 7 _____.
8. DORA Process ________, ___________, ___________ & _______________.
9. ________ IP addresses are assigned by a DHCP Server.
10. DHCP Port Number ___.
11. 169.254.123.33 is an example of _____ address.
12. _______ permission should be assigned if you do not want others to modify the documents or files when accessed over a network.
13. _______ permission should be assigned if you want others to modify the documents or files when accessed over a network.
14. _______ permission should be assigned if you want others to print when using a shared printer.

SESSION 13: NETWORKING SERVICES - NAME RESOLUTION

RELEVANT KNOWLEDGE

Name Resolution

Name resolution refers to the process of converting host names or domain names to an IP address. On an IP network, computers communicate using the IP address; however, computers are assigned names which are easy to remember. When a user attempts to access a computer by using the computer or hostname, it is automatically translated to the IP address assigned to it and then, the communication takes place.

Several methods are used for name resolution as described below:

- Using a HOSTS file
- Using DNS
- Using WINS
- Using DDNS

HOSTS File

The hosts file is a computer file used by the operating system to map host names to IP addresses. The hosts file is a plain text file and is conventionally named *hosts*.

***Note**: Though it's a plain text file, this file does not have extension as .TXT.*

HOSTS file contains lines of text mapping hostnames to IP addresses. HOSTS use a simple mechanism of separating hostnames and IP addresses by white space or tabs; this is very similar to that of a phonebook having entries of customers and their phone numbers. You can map friendly names such as John, PRINTSERVER, etc. that will be easier for users to remember; however for the computers to identify and connect, you need to map the name with respective IP address.

Following are the attributes of a host name:

- Host name can contain maximum 255 characters
- Multiple host names can be assigned to single host
- Host name need not match the NetBIOS computer name (Microsoft Windows)
- Comments can be included by including a hash character (#)

HOSTS file is located in:

Operating System	**Location**
Unix / Linux	/etc/hosts
Microsoft Windows XP / 7	%SystemRoot%\system32\drivers\etc\hosts
Mac OS X 10.2	/private/etc/hosts
Novell NetWare	SYS:etc\hosts
Android	/system/etc/hosts

Lab: View HOSTS file

DNS (Domain Name System)

Using HOSTS file for resolving names on large networks is practically impossible as the HOSTS file on each computer needs to be updated with entries of all other computers in the network – an impossible task for public networks such as the Internet.

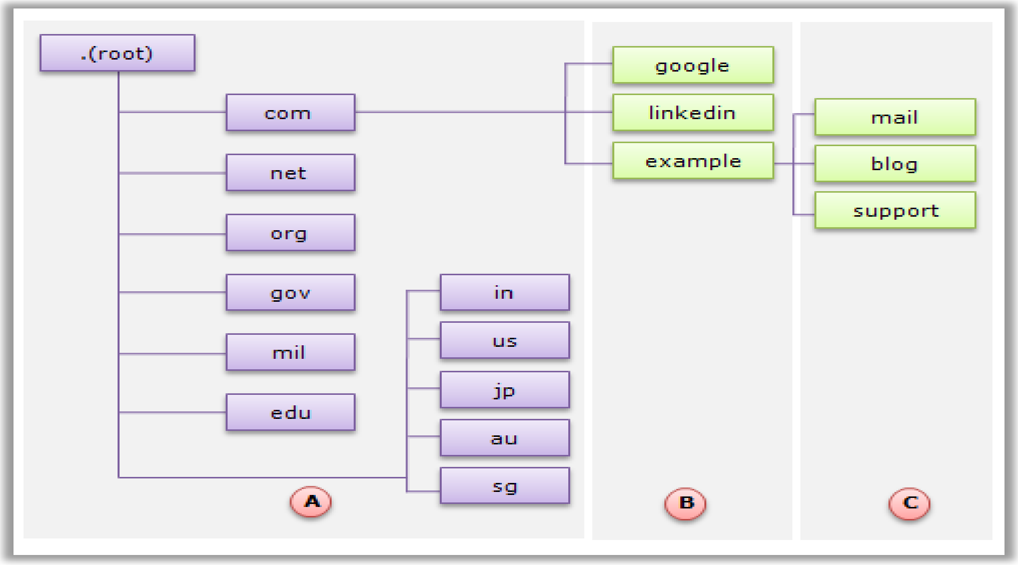
Hence, to address name resolution on large networks and the Internet, a hierarchical distributed naming system called as the DNS is used. Instead of storing information on each computer, entries are centralized to provide the name resolution for all computers in the network. This method helps reduce administrative costs and efforts, since only one machine has to be maintained for name resolution.

The method is analogous to retrieving phone numbers from a centralized service such as the Yellow pages instead of our personal phone books.

DNS provides a worldwide, distributed keyword-based redirection service and serves as an essential component for the functionality of the Internet. Unlike HOSTS file, DNS can be quickly updated and updates are distributed to other DNS servers across the globe.

Domain name space

Domain name space consists of trees *of domain names* and has multiple levels. For example, for a domain mail.google.com, *.com* refers to the top-level domain, *google* refers to second-level domain and *mail* refers to third-level domain. A single DNS zone may consist of one or more domains and sub-domains. Domain names are not case sensitive.



Top-level domains or TLD (A) are domains at the highest level in the hierarchical Domain Name System of the Internet. For all levels, it is the last portion of a domain name. Management of most top-level domains is delegated to responsible organizations by the *Internet Corporation for Assigned Names and Numbers (ICANN)*, which operates the *Internet Assigned Numbers Authority (IANA)* and is in charge of maintaining the DNS root zone. Second-level (B) domains are leased from a hosting provider for a fee. Third-level (C) domains are managed by administrators of the second-level domain and require no fee at all.

Internationalized country level code TLD's are also available and are specially encoded domain names. These when viewed in web browsers, the contents are displayed in the native language such as Arabic, Chinese, etc.

Note: For complete list of domain zones, visit http://www.iana.org/domains/root/db/

Resource Records

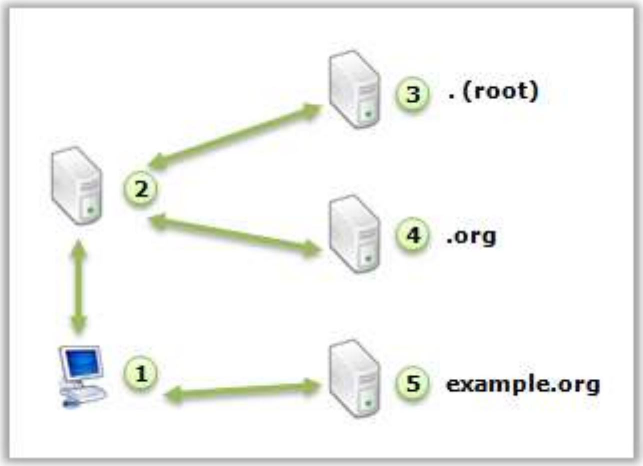
DNS zones contain resource records which hold information associated with a domain name such as services. For example, MX records are used for mail servers, CNAME records are used for pointing to an alias such as www or blog (www.google.com, blog.example.com), etc.

Address resolution mechanism

When you use an application such as web browser or mail client, the domain names (e.g. Wikipedia.org or mail.google.com) are translated to an IP address enabling your computer to communicate. Domain name resolvers determine the appropriate domain name servers responsible for the domain name to be accessed, by a sequence of queries, starting with the right-most (top-level) domain label.

DNS Process

The DNS process is explained below.



1. User opens an URL, www.example.org. Client sends a query to ISP's DNS for the IP address of www.example.org.
2. ISP's DNS searches its database or cache to find matching IP address. If not found, query is forwarded to the root server.
3. Root server traces the IP address of the .org DNS Server and sends it to ISP's DNS Server.
4. ISP's DNS Server contacts the .org DNS Server by its IP Address. The .org DNS Server responds to ISP's DNS Server with the IP address of www.example.org.
5. Client communicates with www.example.org using its IP address.

Authoritative & Non-Authoritative DNS Servers

Authoritative DNS Servers refers to DNS servers that have complete information about a domain and can provide answers to client queries directly. Non-Authoritative DNS Servers may have a copy of the answers or cache copies of DNS queries and provide the answer to DNS clients.

Lab: Install DNS Server

NSLOOKUP (Name Server Lookup)

NSLOOKUP is a command line utility used for querying DNS servers.

Lab: Use NSLOOKUP

Caching Name Server

Caching name servers store results of DNS queries for a period of time as per TTL (Time-to-live) configuration of each domain name record. Caching name servers can improve the efficiency of DNS traffic across the Internet and even increase the performance of end-user applications which use DNS. Caching name server need to be configured on the DNS Server.

DNS Client Resolver Cache (Microsoft Windows XP / 7)

DNS client resolver cache is a RAM-based table that contains entries of Hosts file and host names that Windows has tried to resolve through DNS. The DNS client resolver cache stores entries for both successful and unsuccessful DNS name resolutions. This in turn can improve performance as Windows can locate the destination IP address directly from Cache (RAM) instead of initiating another query to an internal or external DNS server.

Lab: View DNS Resolver Cache
Lab: Clear DNS resolver cache

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Use NSLOOKUP to resolve IP addresses of at least five different websites.
2.	View DNS Resolver Cache
3.	Clear DNS Resolver Cache

ASSESSMENT

Answer the following questions

1. List the methods used for name resolution.
2. Explain the procedure to create a record in HOSTS file.
3. Explain the DNS Process.
4. Explain the purpose of NSLOOKUP with an example.

Fill in the blanks

1. Hostname can be up to maximum of 255 characters.
2. Location of HOSTS file in Linux ___________________________.
3. Location of HOSTS file in Microsoft Windows _____________________________.
4. DNS uses a hierarchical distributed naming system.
5. __________ & ___________ can be used for resolving domain name to IP address.
6. Acronym for TLD _________________________.
7. Acronym for ICANN ____.
8. Acronym for IANA ____.
9. Examples of TLD ____________ , __________ & _____________.
10. Acronym for FQDN ____.
11. _______________ is a command line utility used for querying a DNS Server.
12. __________ is used for resolving IP address to domain name.
13. _______________ is used for clearing the DNS resolver cache.

SESSION 14: NETWORKING SERVICES - NETBIOS, WINS & DDNS

RELEVANT KNOWLEDGE

Computers that run Microsoft windows use computer names and need a unique name. They use NETBIOS Names which is 16 characters in length. (The 16th character is reserved for NETBIOS Suffix to represent service and as a result computer names are maximum 15 characters long.) Computer names use alphanumeric characters for naming convention and are assigned by the administrator.

On a Microsoft windows network that uses IP, computers can be accessed using computer names instead of IP addresses as these are easier to remember and identify.

Lab: View and Change Computer Name

HOSTNAME

Hostname is a command line utility that can retrieve computer name.

Lab: Use HOSTNAME

NetBIOS over TCP/IP

NetBIOS over TCP/IP (NBT, or sometimes NetBT) is a networking protocol that enables legacy computer applications (relying on the NetBIOS API) to run on modern TCP/IP networks. NetBIOS was developed in the early 1980s, targeting very small networks (about a dozen computers).

WINS

Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names. WINS is to NETBIOS Names just as DNS is to hostnames, providing name resolution services for computers running windows on a Microsoft Windows network.

Unlike DNS that requires static IP addresses, WINS supports name resolution mapping using dynamic IP addresses assigned to computers. For example a computer configured as a WINS client (for example, client01) registers itself with a WINS server (for example, winserver01) on joining the network with its NETBIOS name (Computer name) along with its IP address. Now, when another computer (for example, client02) needs to access client01, it contacts the WINS server to retrieve the IP address and communicates with the client01. This eliminates the

need for broadcasting to find the client and helps in reducing network traffic. Additionally, WINS clients can also work with static IP address environments.
Lab: Install WINS Server

NBTSTAT

NBTSTAT is a command line utility for viewing statistics of NetBIOS over TCP/IP.
Lab: Use NBTSTAT

DDNS

DNS requires hosts to be assigned static IP addresses. DNS is not suitable when using DHCP environments; as the IP addresses keeps changing over time and the DNS service requires permanent IP addresses for its records. For example if a consumer using a DSL or cable modem wants to host a website on their computers and to be made accessible to the public, it is not practically possible as their public IP address changes over shorter period of times. In such a scenario, DDNS can be used.

Similar to WINS, DDNS clients can make use of dynamic IP address and computers can be accessed using hostnames or domain names. How? For example, if you are initially assigned a dynamic public address of 202.1.2.3, your computer can be configured to update its IP address along with the hostname or domain name to a machine with DDNS. If the public address changes, the DDNS client will automatically contact and update the DDNS with the changed IP address.

Today, there are a many DDNS providers on the Internet, offering their service free or for a small fee. Examples of service providers include (not limited to):

- http://www.dnsdynamic.org
- http://www.changeip.com
- http://www.dyndns.com
- http://www.changeip.com
- http://freedns.afraid.org
- http://www.dnsmadeeasy.com

Lab: Sign up with one of the free DDNS providers.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Visit any three website that provides DDNS Service.

ASSESSMENT

Answer the following questions

1. Explain the procedure to change a computer name.
2. Explain the purpose of NBTSTAT with an example.
3. Explain the purpose of WINS.
4. Explain the purpose of DDNS.

Fill in the blanks

1. Computer names are ______ characters in length.
2. _________ is a command line utility that can retrieve computer name.
3. _________ is a command line utility for viewing statistics of NetBIOS over TCP/IP.
4. Acronym for WINS ___________________________________.
5. Acronym for DDNS ___________________________________.

SESSION 15: NETWORKING SERVICES - TERMINAL SERVICES & ACTIVE DIRECTORY

RELEVANT KNOWLEDGE

Terminal Services

Terminal service is a component of Windows Server Operating System that makes applications installed on the server accessible to computers in a network. Applications can be accessed from a variety of devices such as smart phones, laptops or desktops running different operating systems.

Terminal services are useful when you want to reduce hardware costs by hosting applications on the server and access them using thin client devices or computers that have older hardware. Terminal services also enhance application access security by installing the application on a particular computer and allowing access to selective users.

Terminal services accessed by using client software are referred to as Terminal Services Client or Remote Desktop Connection and is used in multiple operating systems.

Lab: Install Terminal Services

Terminal Services can also be used where an application is not compatible with an operating system. For example an application designed to run on Windows will not run on machines with MAC OS, UNIX or Linux. In such a case, you can install the terminal client software and access the application from a computer running terminal services enabling everyone to use the application irrespective of the operating system.

Terminal Server Licensing

Terminal Server though included as a component, requires separate licensing. By default, a 120 day trial is included.

Thin Clients

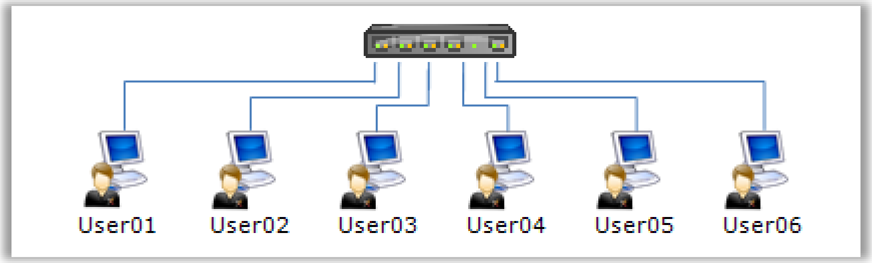
Thin client refers to computing devices that have minimum processing and storage capabilities. Thin clients depend on other powerful computer that takes care of such needs. Thin clients are not expensive and help organizations reduce cost.

Network Controllers

On medium to large sized networks, it is a practice to have centralized security. Network or Domain Controllers are used for authenticating user accounts and permissions are tightly controlled. This helps the administrators as everything is centralized and users can login to any of the computer within a network using a single username and password combination.

Workgroups

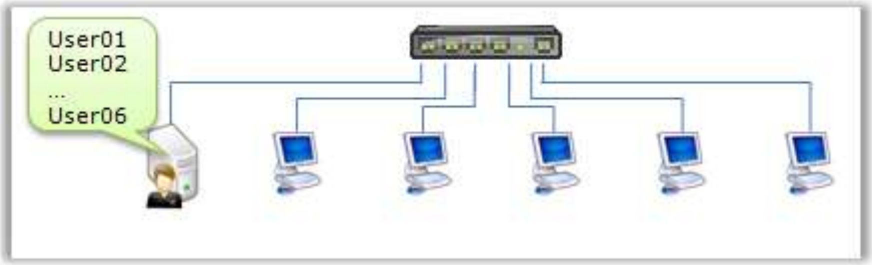
Workgroup or Peer-to-Peer computer network refers to decentralized model where the user name and password is stored on individual computers. Workgroup model is suitable for 10-15 computers or fewer numbers of users and requires additional administration as the number of computer or user grows. Since the permissions are managed locally at each computer, each user or owners of a computer act as an administrator.



Workgroup Model, User accounts on each computer

Domains

Domain refers to a centralized model where a centralized database stores all the credentials (usernames, passwords, security policies, etc.). Domain models assist administrators to control the computers in a network from a single station making it easier to administer. Permissions (or restrictions) to change wallpaper, access control panel items, etc. can be set across the network keeping all the computers secure. Domain models are suitable for small, medium to extremely large networks and can scale to thousands of users.



Domain Model, User Accounts on a Centralized computer (Domain Controller)

Active Directory

Active Directory is a directory service used in Microsoft Windows Domain networks. Here, a domain controller is configured to authenticate and authorize all users and computers in a network. Active Directory enforces security policies such as password length, password complexity, user restriction, etc. Active Directory or an equivalent directory service is widely used in medium to large corporate networks. Active Directory uses the LDAP Protocol for directory service, Kerberos protocol for authentication and DDNS for name resolution.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Setup Terminal services for the following applications: a. OpenOffice.org Suite b. Calculator c. Paint (MSPAINT)

ASSESSMENT

Answer the following questions

1. Explain the purpose of Terminal Services.
2. Explain the procedure to set up terminal services for an application with an example.
3. Describe Thin Clients.
4. Differentiate Workgroups vs. Domains.
5. Explain Active Directory.

Fill in the blanks

1. In _____________ model, security is decentralized.
2. In _____________ model, security is centralized.
3. ______ clients are computers that have limited processing capabilities and depend on powerful computer for processing needs.

   ___________ is an example of directory service included with server operating systems from Microsoft.

SESSION 16: WIRELESS NETWORKING

RELEVANT KNOWLEDGE

Introduction to Wireless Networking, RF Communication

Wireless network refers to a computer network that is not connected by any cables. Typically Wireless networking is used where wired connectivity is not possible or feasible due to technology costs or availability. Wireless telecommunications networks are implemented and administered using a transmission system called radio waves. This implementation takes place at the physical level (layer) of the OSI model network structure.

Types of wireless networks

- **Wireless personal area network (WPANs)** interconnect devices within a relatively small area usually within a person's reach. For example, usage of Bluetooth to connect a mobile phone to a laptop.
- **Wireless metropolitan area network (WMANs)** is a wireless network that connects several wireless LANs. WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard.
- **Wireless wide area network (WWANs)** is a wireless network that covers large areas, such as one between neighboring towns and cities, or city and its suburbs. This network can connect branch offices of business or function as a public internet access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2.4 GHz band, rather than Omnidirectional antennas used with smaller networks.

Omnidirectional antennas are types of antenna that radiates radio waves equally in all directions. Omnidirectional antennas oriented vertically are widely used for nondirectional antennas as they radiate equally in all horizontal directions.

Note: Though there are a variety of Wireless Networks, this course focuses only on Wireless LAN.

Wireless LAN

WLAN refers to connectivity between two or more devices within short distances such as homes or campus. WLAN uses spread-spectrum or OFDM technologies that enable users to have mobility within the coverage area. WLAN corresponds to IEEE 802.11 standards and are marketed commonly under the **Wi-Fi** brand name.

WNIC: Wireless network interface controller (WNIC) is a network interface controller using radio waves for connectivity instead of wires. WNIC is usually found integrated with mobile devices such as laptops; however, to use on a desktop, you may need a dedicated card.

PCI Wireless Card

CardBus Wireless Card

USB Wireless Card

WAP (Wireless Access Points): WAP are devices that connect WNIC to wired networks thus acting like a bridge between wired and wireless networks. WAP have built-in antennas for communicating with WNIC and other WAP’s. WAP are generally connected to a network switch or router providing internet connectivity to its client over wireless networks. Since wireless networks use radio waves, their transmission capability is limited. *Range extenders* are devices used for extending wireless LAN similar to that of repeaters used in wired networks. Most SOHO routers have integrated access point and they are commonly referred to as Wi-Fi or Wireless Routers.

Wireless Access Point

Wireless Range Expander

IEEE 802.11: IEEE 802.11 standard defines the Wi-Fi standard, used for wireless networks and is Sub classified into IEEE 802.11b, a, g and n.

Access method is CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance), before transmitting data, the station senses for activity on the channel for a pre-determined amount of time. If the channel is busy, the station does not transmit and waits for a random interval before attempting to transmit again.

IEEE 802.11x Standards

Due to ease of installation, wireless LANs have become popular in not only residences but also commercial complexes who offer wireless access to their customers; often for free. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard IEEE 802.11-2012 has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

IEEE 802.11 Standards

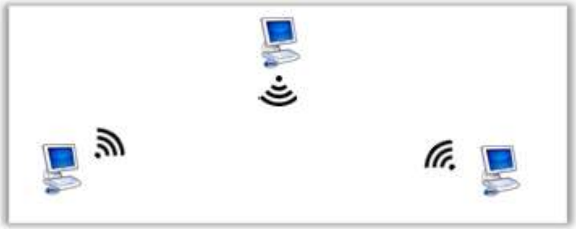
Standard	Radio Frequency	Speed	Range (Indoor)	Range (outdoor)
IEEE 802.11b	2.4 GHz	Up to 11 Mbps	Up to 35 m	Up to 140 m
IEEE 802.11a	5 GHz	Up to 54 Mbps	Up to 35 m	Up to 120 m
IEEE 802.11g	2.4 GHz	Up to 54 Mbps	Up to 38 m	Up to 140 m
IEEE 802.11n	2.4 / 5 GHz	Up to 600 Mbps	Up to 70 m	Up to 250 m

Note: IEEE 802.11 b, g & n are compatible with each other. IEEE 802.11n is compatible with IEEE 802.11a.

Types of Wireless LAN include the ADHOC & Infrastructure Network.

ADHOC

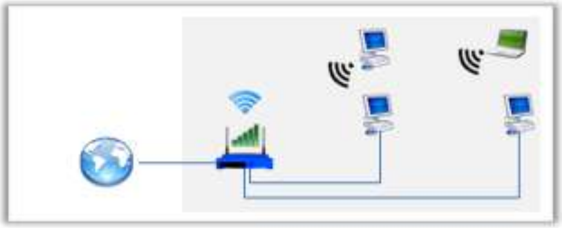
A wireless ad-hoc network is a decentralized type of wireless network. Also known as peer-to-peer (P2P) network, ADHOC mode allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points.



This method is usually used by two or more wireless computers that connect to each other to form a network. This is considered the quickest method as no other devices are required other than the WNIC and the procedure is straight-forward and simple.

Infrastructure Mode

In infrastructure mode, communication happens via a centralized device called the access point that serves as a bridge to a wired network infrastructure. Usually, this is used for utilizing resources on the wired networks.



For example, you may have an existing wired network with two desktops connected for Internet access; to add wireless clients such as a laptop, you can attach an access point to the network switch. All wireless clients will access the desktops and the Internet through the access point. You may also find SOHO routers (figure above) that has integrated access points for connecting wired and wireless devices in home or small business networks. Dedicated access points are used usually in enterprise networks.

SSID

SSID or Service Set Identifier is a unique alphanumeric name used for naming wireless networks. SSID’s can be 32 character’s long and is case-sensitive. Wireless clients continuously scan the wireless network for available SSID’s. Users or administrators can connect to a wireless network. Any wireless device can associate with only one SSID at a time (similar to that of cell phone associated with a single ISP or number).

Basic service set

The basic service set (BSS) is the basic building block of an 802.11 wireless LAN. In infrastructure mode, a single access point (AP) together with all associated stations (STAs) is called a BSS. An access point acts as a master to control the stations within that BSS. Each BSS is identified by a BSSID. The simplest BSS consists of one access point and one station.

Independent basic service set (IBSS)

With 802.11, it is possible to create an ad-hoc network of client devices without a controlling access point. This is called an independent basic service set (IBSS). In this case, the SSID is chosen by the client device that starts the network, and broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network.

Extended service set

An extended service set (ESS) is a set of one or more interconnected BSSs and integrated local area networks that appear as a single BSS to the logical link control layer at any station associated with one of those BSSs.

The set of interconnected BSSs must have a common service set identifier (SSID). They can work on the same channel, or work on different channels to boost aggregate throughput. The maximum length of the SSID can be 32 characters long.

Wireless Zero Configuration & Proprietary Utility

Wireless connection management utility refers to software provided by a vendor that is used for managing wireless network connections. Also referred to as proprietary utility, this is usually installed along with the drivers and accessed through a program shortcut. Mostly utilities from different vendors have different user interface that may be confusing to end users.

Wireless Zero Configuration (WZC), also known as Wireless Auto Configuration or WLAN AutoConfig, is a wireless connection management utility included with Microsoft Windows. You can use WZC to manage wireless network connections. It works with all wireless adapters. WZC is used for providing an interface that looks similar irrespective of the wireless card used. This is useful to consumers who work with different WNIC from a variety of vendors.

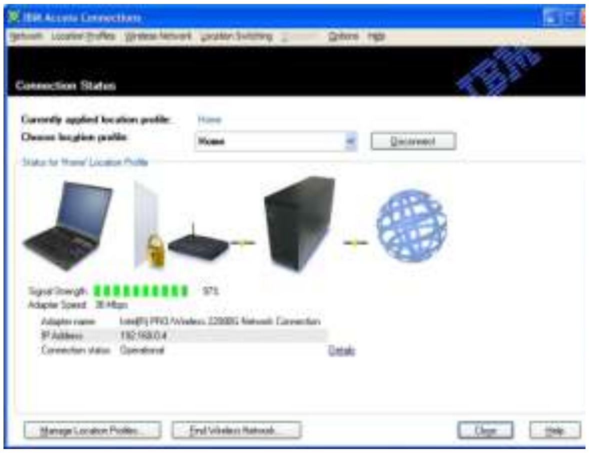
Setting up Wireless Networks

Lab: Set up a ADHOC network

Lab: Set up a Infrastructure Network

Wireless Site Survey

Before you implement a WLAN, you need to understand the requirements such as coverage, number of computers that will connect, roaming, data rates, etc. This process requires planning and designing, commonly referred to as Site Survey.


IBM Access Connections
Network Location Profiles Wireless Network Location Switching Options Help
Connection Status
Disconnect
Manage Location Profiles... Find Wireless Network... Close Help

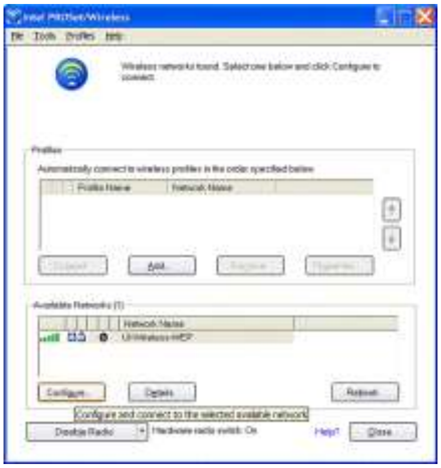
Currently applied location profile: Home
Choose location profile: Home

Status for 'Home' Location Profile

Signal Strength: 97%
Adapter Speed: 36 Mbps

Adapter name	Intel(R) PRO/Wireless 2200BG Network Connection
IP Address	192.168.0.4
Connection status	Operational

IBM WLAN Utility



Wireless networks found. Select one below and click Configure to connect.

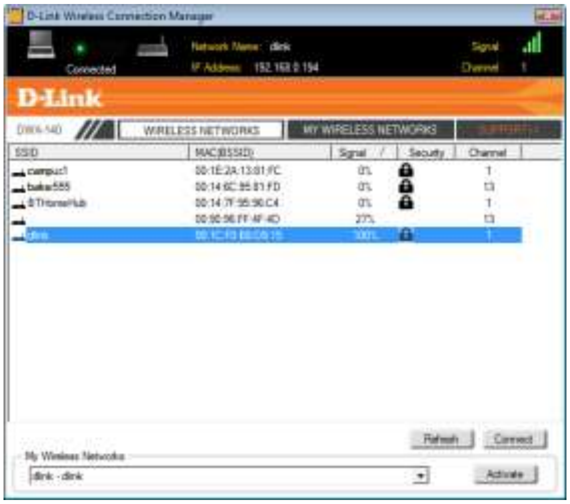
Automatically connect to wireless profiles in the order specified below.

UI-Wireless-WEP

Configure and connect to the selected available network

Hardware radio switch: On

Intel WLAN Utility

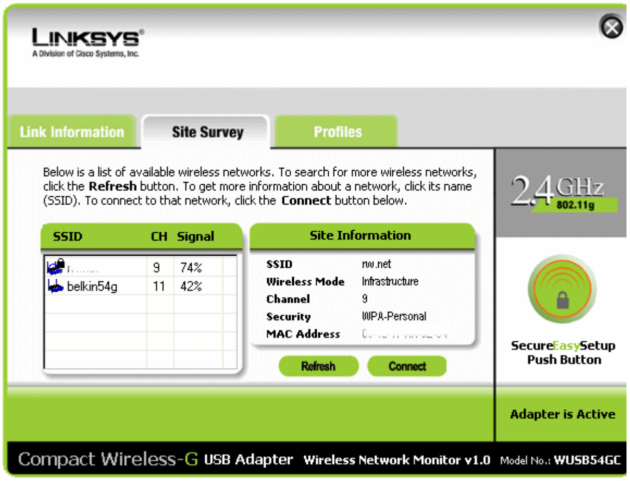


Network Name: dlink
IP Address: 192.168.0.194
Signal
Channel 1

SSID	MAC(BSSID)	Signal	Security	Channel
campus1	00:1E:2A:13:01:FC	0%	🔒	1
baker555	00:14:6C:85:81:FD	0%	🔒	13
BThomeHub	00:14:7F:95:90:C4	0%	🔒	1
	00:90:96:FF:4F:4D	27%		13
dlink	00:1C:F0:B8:C8:15	100%	🔒	1

dlink - dlink

D-Link WLAN Utility



Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To get more information about a network, click its name (SSID). To connect to that network, click the **Connect** button below.

SSID	CH	Signal
[illegible]	9	74%
belkin54g	11	42%

Site Information

SSID	nw.net
Wireless Mode	Infrastructure
Channel	9
Security	WPA-Personal
MAC Address	[illegible]

Linksys WLAN Utility

WLAN, since it uses radio waves they are prone to interference and the effect range can be determined only after a thorough study. You can analyze the signal strength, coverage, etc. by placing a WAP at a fixed location, move a client device to measure and conclude the actual requirements.

Channel Assignment

In wireless networks, channel allocation schemes are required to allocate bandwidth and communication channels to base stations, access points and terminal equipment.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Set up a ADHOC Network using different SSID’s
2.	Set up a Infrastructure Network using different SSID’s
3.	Compare different models of wired network cards available from different vendors. Use the Wired Adapters Worksheet below:

Wireless Adapters			
Vendor			
Model			
Interface			
PCI			
USB			
PCMCIA			
Cardbus			
PCI Express			
IEEE Standards			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			
IEEE 802.11n			
Supported Speed (Mbps)			
11			
54			
150			
300			
Operating Systems			
Microsoft Windows XP			
Microsoft Windows Vista / 7			
Linux			
Frequency			
2.4 GHz			
5 GHz			

Dual Band (2.4 + 5 GHz)			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
Antennas			
Single			
Double			
Detachable (Yes/No)			

ASSESSMENT

Answer the following questions.

1. Explain WLAN.
2. Explain IEEE 802.11 standards.
3. Explain Wireless Access Points.
4. Differentiate AHDOC & Infrastructure Networks.
5. Explain the procedure to setup a AHDOC Network.
6. Explain the procedure to setup a Infrastructure Network.
7. Differentiate Wireless Zero Configuration & Proprietary Utility.

Fill in the blanks

1. __________ are devices that acts like a bridge connecting wired & wireless networks.
2. Acronym for SOHO ____.
3. Acronym for WAP ____.
4. ___________ is used for identifying a WLAN.
5. ___________ mode in WLAN uses an AP.
6. ___________ mode in WLAN does not require an AP.
7. __________ type of SOHO routers have integrated WAP.
8. IEEE 802.11b can support maximum speed up to _____ Mbps.
9. IEEE 802.11a can support maximum speed up to _____ Mbps.
10. IEEE 802.11g can support maximum speed up to _____ Mbps.
11. IEEE 802.11n can support maximum speed up to _____ Mbps.
12. IEEE 802.11g is backward compatible with IEEE 802.11___.
13. IEEE 802.11b & g devices operate in the frequency range of _____.
14. IEEE 802.11a devices operate in the frequency range of _____.

SESSION 17: WIRELESS SECURITY

RELEVANT KNOWLEDGE

Overview of Wireless Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Due to affordability of Wi-Fi Routers, Internet access through wireless means have gained popularity. Today, almost every laptop and Smartphone is equipped with wireless cards enabling users to access network or the Internet through a wireless connection. Data transmitted over wireless LAN using radio waves can be trapped and unauthorized users can gain access to internal network resources or access to the Internet without the consent of the owner. In most cases, unprotected WLAN's acts like a free hotspot for wireless users.

You can protect WLAN's by using wireless security such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) to encrypt and decrypt network traffic.

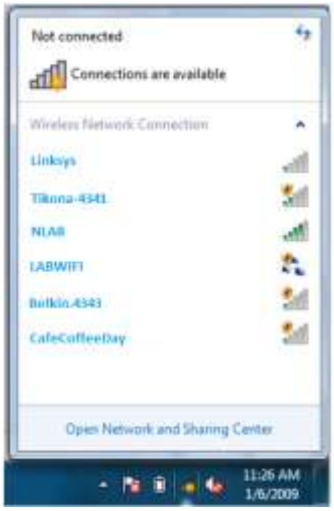
Piggybacking

Piggybacking refers to the practice of using wireless Internet connection subscribed by others. For example, a user can connect to his/her neighbor's WLAN and access the Internet without permission. Such practices are unethical and considered illegal in some countries.

Usually WAP's advertise their presence by broadcasting their SSID.

For example, look at the figure below listing all the wireless networks available within its range. Some of the connections could be far away from your computer; however, the WNIC will list every connection it can detect within its range. You may be able to establish a connection to one of the unsecured entries listed, though not owned by you!

Some businesses provide free or complimentary Internet access through WLAN's commonly referred to as a hotspot service. It is intended for their customers to avail Internet access during their visits. Such connections may also be listed here. For all you know, someone could also establish a connection to your WLAN and use your network resources or access the Internet without paying for it.


Not connected
Connections are available
Wireless Network Connection
Linksys
Tikona-4341
NLAB
LABWIFI
Belkin.4343
CafeCoffeeDay
Open Network and Sharing Center
11:26 AM
1/6/2009

Protecting WLAN

In order to protect wireless networks, there are a variety of methods available listed below (not limited to):

Note: Some of these methods may not be possible if the WAP or SOHO router with integrated AP lacks such capabilities.

1. Use MAC address authentication / filtration: You can add the list of MAC addresses of computers or devices to the WAP. Connection to the WAP will be allowed only if the WAP finds matching MAC address.

   Lab: Use MAC Address authentication / filtration

2. Implement WEP

   WEP (Wired Equivalent Privacy)

   WEP is a widely used security algorithm and is often the first security choice. Although its name implies that it is as secure as a wired connection, due to numerous flaws and has lost out to newer standards such as WPA2. WEP uses 64-bit or 128-bit encryption.

   Methods of Authentication

   WEP uses two methods of authentication: Open System authentication and Shared Key authentication.

   In *Open System authentication*, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs hence no security at all - anyone can connect!

In *Shared Key authentication*, the WEP key is used for authentication in a four step challenge-response handshake:

1. The client sends an authentication request to the Access Point.
2. The Access Point replies with a clear-text challenge.
3. The client encrypts the challenge-text using the configured WEP key, and sends it back in another authentication request.
4. The Access Point decrypts the response. If this matches the challenge-text the Access Point sends back a positive reply.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

Lab: WEP

3. Implement WPA

WPA (Wi-Fi Protected Access) & WPA2 (Wi-Fi Protected Access II)

WPA and WPA2 are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

WPA protocol implements a lot of the IEEE 802.11i standard, especially the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key, i.e. it dynamically generates a new 128-bit key for each packet thus preventing attacks which compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard.

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.

WPA operates in two modes:

a. First mode to provide different keys to each user through a 801.x authentication server.

b. Second mode, a less secure PSK mode. PSK or Pre-shared Key mode is designed for home and small business networks that may not have 801.x authentication servers. In this case, every user has the same pass phrase.

Unlike WEP that is widely supported by almost all WLAN devices, support for WPA or WPA2 may not be available on certain devices. In some cases, vendors provide a firmware upgrade which can provide support for WPA/WPA2. Also the WNIC's must support these standards.

Lab: WPA / WPA2

4. Disabling SSID broadcasts: If SSID broadcast is disabled, SSID's will not be displayed when computers attempt to discover WLAN's.

   Lab: Disable SSID broadcast

5. Implement Wireless intrusion detection systems and monitor your network for any intruders attempting to access your network through WLAN. This method is most expensive as it involves use of special devices.

To summarize, it is best to use a combination of methods to keep the network secure. Though there is no guarantee of 100% protection, the discussed methods definitely make it difficult for unauthorized users to penetrate and access the network.

Troubleshooting Wireless Networks

Given below are guidelines to optimize and troubleshoot wireless networks based on best practices:

- WLAN's use radio waves that is limited in distance. If the end device such as desktop or a laptop is quite far away from the WAP, the signal would be weak. It is advisable to either move the devices as close as possible or to place the devices (at least the WAP) at a higher level to avoid interference from obstacles such as cupboards, etc. Anything made of wood, steel, concrete, glass, etc. absorbs signals resulting in poor signals.
- When you require roaming facilities, you can use a wireless extender to amplify the signal and thus increase the coverage area. You can also configure some SOHO routers to work only as an access point.
- WLAN's use radio waves and may be disturbed by other radio waves using the same frequency within the area. For example, many consumer devices such as cordless telephones, Car alarm, wireless cameras, microwave oven, baby monitors use the same frequency (2.4 GHz) at which Wi-Fi standards 802.11b,

802.11g and 802.11n operate. This can cause a significant decrease in speed, or sometimes total blocking of the Wi-Fi signal. You can use devices such as spectrum analyzers to find the source of interference. If Such devices are not available, then you need to analyze and find out the probable devices that might use the same frequency. You can also move away from the interference by shifting channels (11 to 6, 6 to 1) as it will change the frequency of the WLAN devices.

- WLAN's use Omni-directional antennas that radiate strong signals horizontally but are weak in upward or downward directions. It is recommended to get WAP's with external antennas as the position can be changed to provide adequate signals. You can also use directional antennas if connecting WAP's between two buildings across a road or within a facility. Check with the product specification for details on signal strength and range it can provide.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Compare different models of access points available from different vendors. Use the Wired Adapters Worksheet below:
2.	Setup WLAN security by: a. Using 64-bit WEP b. Using 128-bit WEP c. Using different Pass Phrase d. Using WPA-PSK (AES) e. Using WPA2-PSK (AES)

Wireless Access Point			
Vendor			
Model			
Details			
Default SSID			
Default Password			
Default IP address			
IEEE Standards			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			

IEEE 802.11n			
Supported Speed (Mbps)			
11			
54			
150			
300			
Frequency			
2.4 GHz			
5 GHz			
Dual Band (2.4 + 5 GHz)			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
WPS (Yes/No)			
Antennas			
Single			
Double			
Detachable (Yes/No)			

ASSESSMENT

Answer the following Questions

1. Explain Wireless security.
2. Explain piggybacking with an example.
3. List any three methods that can be used for protecting WLAN with an example.
4. Explain WEP.
5. Explain WPA.

Fill in the blanks

1. _____________ refers to the practice of using wireless Internet connection that others have subscribed.
2. Acronym for WEP _____________________________________.
3. _____ WEP key is entered as a string of 10 hexadecimal characters
4. _____ WEP key is entered as a string of 26 hexadecimal characters
5. Acronym for WPA _____________________________________.
6. ____________ is the most secure wireless encryption standard.

SESSION 18: WIDE AREA NETWORKS CONCEPTS

RELEVANT KNOWLEDGE

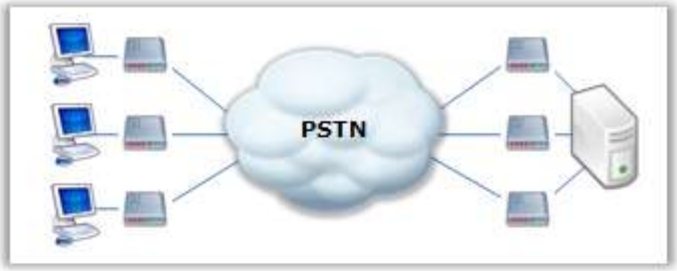
A Wide Area Network (WAN) is a network that covers a broad area (metropolitan, regional, or national boundaries) using private or public network transports. Using WANs, data can be transmitted over very long distances.

There are a variety of WAN technologies available offering temporary (pay as per usage) and permanent (24/7 availability) connectivity. Some of the common connectivity includes:

- Dial-Up
- ISDN
- DSL
- Cable
- Satellite
- Wireless

Dial-up

A Dial-up connection is a form of network connectivity using telephone networks. In the initial stages of networking, dial-up connections were used to connect to the ISP for Internet connectivity. In this, computers are connected over telephone networks using a device called the MODEM (a device used for modulating and demodulating signals from analog signals to digital signals and vice versa).



Dial-up connections have a maximum theoretical speed of 56 Kbps through the practical speeds are considerably less. Major disadvantages of dial-up are the inability to use telephone lines for calls during Internet or network connectivity and painfully slow speeds. Dial-up connectivity usage has become limited due to popularity, speed and wide availability of broadband technologies such as DSL & Cable Modem. However, you may still find people using dial-up connections for Internet Access or for connecting to offices in remote location.

To set up a dial-up connection, two parts are involved: RAS & Dial-Up Clients. One computer needs to be setup for accepting connections and the other, for connecting to a remote computer. Computers that are setup for accepting remote connections are referred to as *Remote Access Servers (RAS)* and computers that connect to remote computers are referred to as *Dial-up clients (DUN)*.

Lab: Install a MODEM on both computers

Lab: Setup computer to accept incoming connection

Lab: Create a Dial-up Connection for connecting to a remote computer or ISP.

Protocols used in dial-up networking are SLIP & PPP.

SLIP or Serial Line Internet Protocol is a protocol designed to work over serial ports and modem connections. SLIP needs static IP addresses before the hosts can be connected and supports only TCP/IP Protocol. SLIP has been largely replaced by PPP.

PPP or Point-to-Point Protocol supports TCP/IP and also multiple other protocols such as NETBEUI, IPX/SPX. PPP also supports dynamic IP addressing and is widely used for dial-up access to Internet. PPP supports multi-links (use of more than one modem simultaneously to increase bandwidth), authentication, encryption and compression.

RRAS (Routing & Remote Access Server)

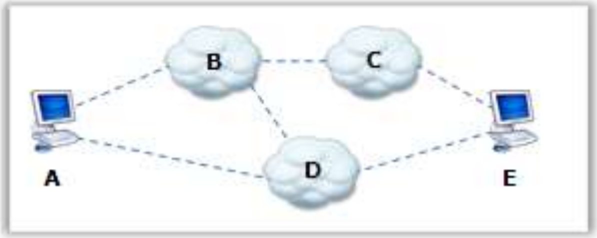
RRAS (Routing & Remote Access Server) is a feature that is used for managing remote connections. RRAS supports a variety of connections including Dial-up & VPN(Virtual Private network – you will read about this later) and usually support tens to hundreds of incoming connections. This is usually used by large organizations and ISPs.

Lab: Install and configure RRAS

Lab: Install a MODEM on the Server (Use previous procedure)

On packet switching networks, routers use static or dynamic methods:

- In ***Static routing***, packets are transmitted through a fixed route. Manual route entries of different routes are added to the routing table by the administrator to define the routing path. Packets are transmitted by the router only through the path set in the routing table. If there is a problem with a particular route, packets will never reach the destination through other routes. In such cases, administrators need to alter the routes to ensure packets are delivered to the destination. It is not fault-tolerant as it can lead to a single point failure; however, as the route path is known to the administrator, static route is considered to be secure. For example if the route is fixed to travel only through B & D from A to E, packet will never be delivered if there is a broken link between B & D (refer figure below) even though connectivity is still available between A to E through B & C or D.
- ***Dynamic routing*** refers to the capability where the routes are determined by the router automatically based on conditions. Packets may take alternate routes in case of a change in network condition. For example, if the packet has to travel between A to E (image below), packets may be transmitted typically through D as it is the shortest path, if there is a problem through D packet will be delivered through alternate route B & C even though if it is lengthier.



Dynamic routing path

When you specify an IP address and a subnet mask, you also need to specify an IP address in the default gateway column. Routing takes place when a packet is identified for delivery to a remote network. Once the packet is determined not a part of the local network, it is forwarded to the default gateway. Such packets forwarded to the default gateway, are routed and sent to the destination network.

Routing Protocols

In dynamic routing, routing tables are created and managed by routing protocols that automatically run on a router. Routing protocols enable routers to exchange the routing table between them periodically or when there is a change in network condition. Two categories of dynamic routing protocols are ***Distance-vector*** protocols and ***Link-state*** protocols.

- ***Distance-vector*** routing protocols such as RIPv1, RIPv2 & IGRP use some form of distance to calculate the route metric; for example the number of hops required between the source and the destination. Complete routing tables are periodically (for example, every 30 seconds) exchanged between neighboring routers and use algorithms such as Bellman-Ford to determine shortest path. *Routing Information Protocol (RIP)* uses hop count as its metric and *Interior Gateway Routing Protocol (IGRP)* uses a combination of bandwidth & delay as its metric.

- ***Link-state routing*** protocols such as OSPF & IS-IS operate by building topology table based on links and its status from neighboring routers. In case of any change in a link or its status, an advertisement about the change is sent to all routers within the area to adjust the topology table which in turn is used to determine the new best route.

RIP (Routing Information Protocol)

RIP is a distance-vector routing protocol that uses hop count as a routing metric. RIP is limited to 15 hops beyond which it is considered infinite distance and inoperable.

IGRP(Interior Gateway Routing Protocol)

IGRP is a proprietary distance-vector routing protocol invented by Cisco. IGRP overcomes the limitation of RIP by supporting up to a maximum of 255 hops (default 100).

OSPF (Open Shortest Path First)

OSPF is a link-state routing protocol is the most widely used IGP (Interior Gateway Protocol) in large enterprise networks. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

IS-IS (Intermediate System to Intermediate System)

IS-IS is a Interior Gateway protocol used within an administrative domain or network and is the de facto standard for large service provider network backbones.

IGP (Interior Gateway Protocol)

IGP is a routing protocol that is used to exchange routing information within an autonomous system (AS).

EGP (Exterior Gateway Protocol)

EGP is a routing protocol used to exchange routing information between autonomous systems. This exchange is crucial for communications across the Internet.

BGP (Border Gateway Protocol)

BGP is the protocol used for making routing decisions on the Internet today. ISP’s must establish communication with each other router using BGP and it serves as one of the most important protocols on the Internet.

Routing Commands

TRACERT

TRACERT is a command line utility used for displaying path taken by a packet and measuring transmit delays across an IP network. If you want to know the routes taken by a packet from your computer to the destination, you can use the TRACERT command. TRACERT uses ICMP.

Lab: Use TRACERT command

ROUTE

Route is a command line utility that is used for viewing and manipulating routing tables. Routing table on computers is automatically built based on the IP configuration of your computer. Route command is also used by administrators to make manual entries in the routing table to define static routes.

Lab: Use Route Command

PATHPING

PATHPING is a command line utility that combines the power of both PING and TRACERT. PATHPING can provide PING-like statistics between each host traced through TRACERT.

Lab: Use PATHPING

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Practice by creating additional dial-up connections.
2.	Use Tracert command to trace route for at least five websites

ASSESSMENT

Answer the following questions

1. Explain the purpose of Dial-up connections.
2. Explain the procedure to set up a dial-up connection.
3. Differentiate SLIP and PPP.
4. What is RRAS?
5. Explain Static routing with an example.
6. Explain Dynamic routing with an example.

Fill in the blanks

1. Acronym for SLIP ____.
2. Acronym for PPP ____.
3. Acronym for RRAS ____.
4. __________ is a command line utility used for viewing the route taken by a packet.
5. Acronym for RIP ____.
6. Acronym for OSPF ____.
7. Acronym for IGRP ____.
8. Acronym for BGP ____.
9. ___________ is used for indicating IP packets to be routed.

10. __________ is a command line utility used for viewing and manipulating routing table.
11. __________ is a command line utility that combines the power of both PING and TRACERT.
12. ________ is a command line utility can be used for viewing the route taken by a packet.
13. ________ is a command line utility can be used for viewing the routing table.
14. List any two distance-vector routing protocols. _________ & __________.
15. List any two distance-vector routing protocols. _________ & __________.

SESSION 19 : DIFFERENT WIDE AREA NETWORKS

RELEVANT KNOWLEDGE

ISDN (Integrated Services Digital Network)

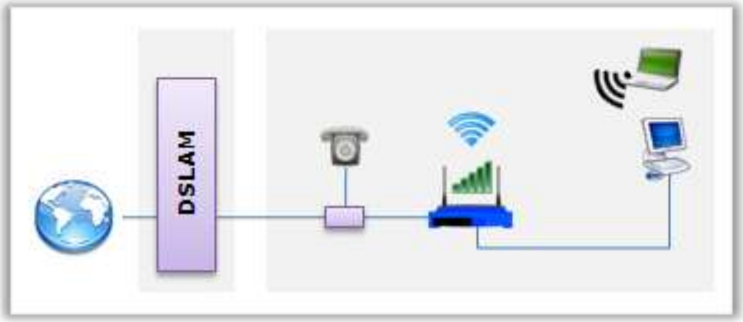
ISDN is a circuit switched network that enables digital transmission over telephone lines. It allows data, voice; video transmissions over a single line and multiple devices can use the same communication line. ISDN is widely used for high speed Internet access in most countries.

ISDN access is offered as *Basic Rate Interface (BRI)* & *Primary Rate Interface (PRI)*. ISDN offers speed in increments of 64 Kbps. BRI offers 128 Kbps delivered over standard copper telephone lines. With a payload of 144 Kbps, it is broken into two 64 Kbps (bearer channels, referred to as channel "B") and one 16 Kbps signaling channel (bearer channels, referred to as channel "D"). In short, BRI is 2B+1D. PRI is delivered on T1 carriers as 23B channels (64 Kbps each) and 1D Channel (64 Kbps) for signaling in North America. However, the configuration varies across locations as displayed below:

Region	ISDN PRI Configuration	Speed
North America	23B + 1D	1.544 Mbps (T1)
Japan	23B + 1D	1.544 Mbps (T1)
Europe	30B + 1D	2.048 Mbps (E1)
Australia	30B + 1D	2.048 Mbps (E1)
India	30B + 1D	2.048 Mbps (E1)

DSL

Digital subscriber line is a family of technologies that provide Internet access by transmitting digital data over telephone network. This is achieved by using different frequencies for voice and data.



The service is offered by installing a *DSLAM* (Digital Subscriber Line Access Multiplexer) (at telephone exchanges) and a *DSL filter* (at customer's premises) to split voice and data thereby enabling simultaneous transmission of voice and data. Since multiple signals are sent over pairs of wires at different frequencies, this is categorized as *broadband*. DSL uses PPPoE (Point-to-Point Protocol Over Ethernet).

DSL used today widely represents ADSL a variant that provide varying speeds in the range of 128 Kbps to over 40 Mbps downstream depending on the technology, line conditions and service-level implementations.

Following is a summary of xDSL standards:

Technology	**Rate (kbit/s)**	**Rate (kbyte/s)**
IDSL (dual ISDN + 16 kbit/s data channels)	144 kbit/s	18 kB/s
HDSL	1,544 kbit/s	193 kB/s
MSDSL	2,000 kbit/s	250 kB/s
SDSL	2,320 kbit/s	290 kB/s
SHDSL (ITU G.991.2)	5,690 kbit/s	711 kB/s
ADSL (G.Lite)	1,536/512 kbit/s	192/64 kB/s
ADSL (G.DMT)	8,192/1,024 kbit/s	1,024/128 kB/s
ADSL2	12,288/1,440 kbit/s	1,536/180 kB/s

Technology	Rate (kbit/s)	Rate (kbyte/s)
ADSL2+	24,576/3,584 kbit/s	3,072/448 kB/s
UDSL	200,000 kbit/s	25,000 kB/s
VDSL (ITU G.993.1)	52,000 kbit/s	7,000 kB/s
VDSL2 (ITU G.993.2)	100,000 kbit/s	13,000 kB/s

DSL is offered by vendors with a variety of options and sometimes with usage restrictions based on quota and/or bandwidth.

For example, an ISP may offer a download speed of 2 Mbps and configure it in a way that it steps down automatically to 512 Kbps or lower once you reach a download limit of 10 GB. However, this depends on the plan taken from an ISP.

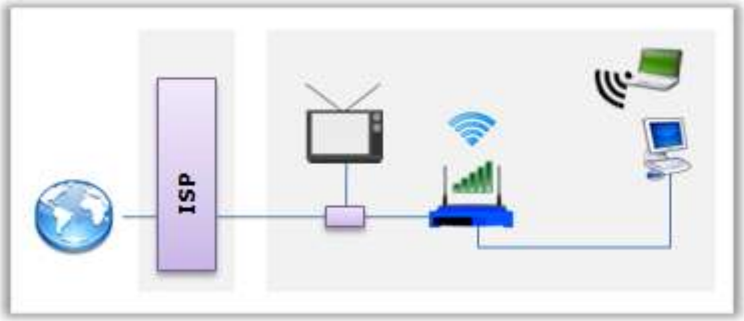
Lab: Set up a DSL Connection

Note : Your facilitator can demonstrate to set up a DSL connection only if a DSL router and an active internet connection is available. You need an active DSL connection from an ISP, a DSL Modem and a computer to use DSL.

1. Connect the DSL Modem to the splitter
2. Turn on the DSL Modem
3. Open the web browser, type the IP address of the Router and login
4. View DSL Connection properties (Use the Router Product Manual)

Cable Internet Access

Cable Internet access is a form of broadband communication that uses cable television infrastructure. Like DSL, cable Internet access is provided through co-axial or fiber optic cables from the ISP to customer's premises. Unlike DSL that provides dedicated bandwidth, cable Internet users share the available bandwidth.



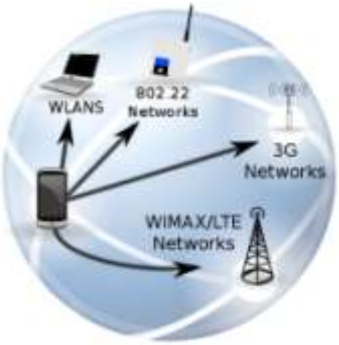
Cable Internet access is multiplexed at ISP and splitters are used to provide signals to TV and Cable MODEM. Many cable TV providers often bundle Internet access along with cable TV channel subscriptions. Depending on the provider, varying speeds are offered in the range of 1 Mbps to over 400 Mbps.

PPPoE

PPPoE or Point-to-Point Protocol over Ethernet is a protocol that is commonly used in broadband services such as DSL & Cable Modems. PPPoE encapsulates PPP frames within Ethernet Frames.

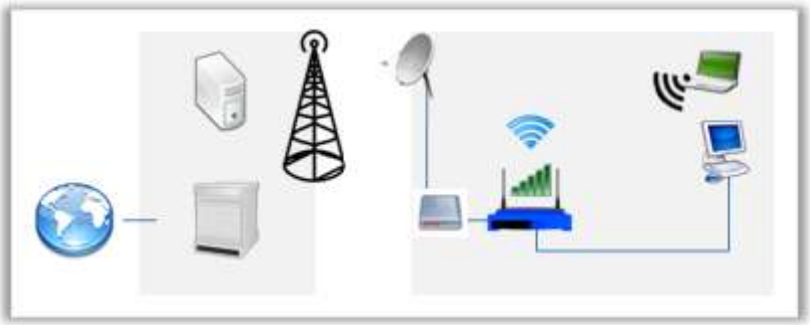
Wireless WAN

Wireless Internet access is used where wired connectivity is not possible or for remote locations. Wireless WAN uses technologies such as LTE, WiMAX, GSM, CDMA, etc. for providing connectivity.



WiMAX

WiMAX or Worldwide Interoperability for Microwave Access is a wireless communication standard used for providing Internet Access to fixed stations. WiMAX is used where wired Internet access such as DSL or Cable is not possible or available.



As compared to other wireless technologies, WiMAX is preferred as it economically viable and easier to implement. WiMAX can provide speeds of 30 to 40 Mbps with current trend at around 1 Gbps; however, the actual speed offered depends on the ISP.

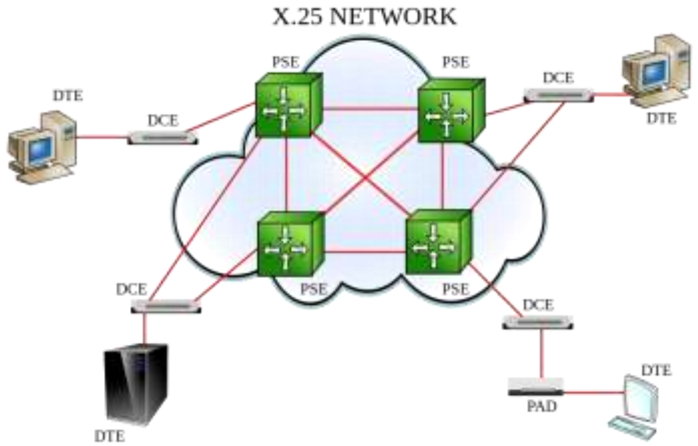
PPPoE

PPPoE or Point-to-Point Protocol over Ethernet is a protocol that is commonly used in broadband services such as DSL & Cable Modems. PPPoE encapsulates PPP frames within Ethernet Frames.

X.25

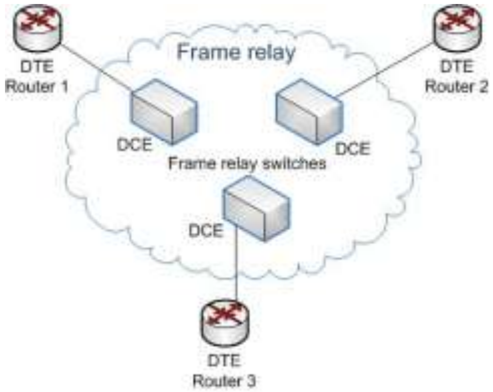
X.25 is a packet switching technology used in Wide Area Networks. In X.25, a Packet Assembler/ Dis-assembler (PAD) assembles and disassembles packets during transmission.

An X.25 WAN consists of packet-switching exchange (PSE) nodes as the networking hardware, and leased lines, telephone service connections or ISDN connections as the physical links. X.25 is a family of protocols that was popular during the 1980s with telecommunications companies and in financial transaction systems such as automated teller machines. X.25 supports speeds up to 2 MB.



Frame Relay

Frame relay is a packet switching technology originally designed for ISDN infrastructure but also used in many other network interfaces. Though X.25 provides quality of service and error-free delivery, Frame Relay relays data as quickly as possible over low error networks and hence supersedes X.25.

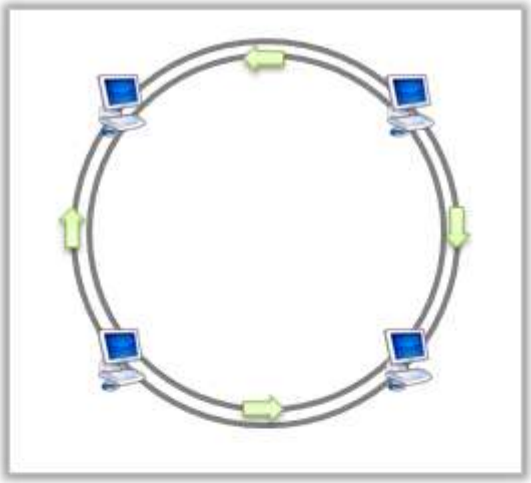


ATM

Asynchronous Transfer Mode or ATM is a packet switching technology using fixed cell size of 53 bytes between end points over a virtual circuit. ATM uses asynchronous TDM and is designed to handle voice, data and video signals.

FDDI

Fiber Distributed Data Interface or FDDI is a token ring based network using optical fiber. FDDI provides speed up to 100 Mbps and distance up to 200 kilometers. FDDI operates through two rings, one acting as a backup in case the primary one fails.



SONET

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized protocols that transfer multiple digital bit streams over optical fiber using lasers light from light-emitting diodes (LEDs). Optical Carrier transmission rates are a standardized set of specifications of transmission bandwidth for digital signals that can be carried on SONET. Base Unit is 51.84 Mbps and offered in multiples of base units (Table below).

SONET OCx	Payload (Mbit/s)	Line rate (Mbit/s)
OC-1	50,112	51,840
OC-3	150,336	155,520
OC-12	601,344	622,080
OC-24	1,202,688	1,244,160
OC-48	2,405,376	2,488,320
OC-192	9,621,504	9,953,280
OC-768	38,486,016	39,813,120

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Compare different DSL Plans
2.	Set up a DSL connection for Internet Connectivity
3.	Compare different Cable Modem Plans
4.	Compare different WiMAX Plans

Internet Connection Plans			
Vendor			
Plan			
Details			
Bandwidth (Kbps)			
Free Usage Limit (Per Month)			
Monthly Charges			
Modem (Free / Paid)			

ASSESSMENT

Answer the following questions

1. Explain ISDN.
2. Explain DSL.
3. Explain Cable Internet Access.
4. Explain WiMAX.

Fill in the blanks

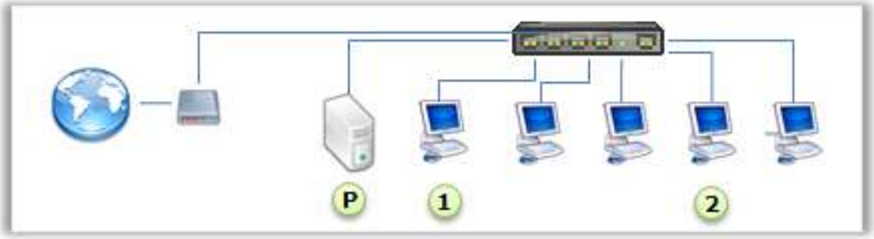
1. Acronym for ISDN. ______________________________.
2. Acronym for DSL.______________________________.
3. Acronym for WiMAX. ______________________________.
4. Acronym for ATM ________________________________.
5. Acronym for PAD ________________________________.
6. Acronym for DSLAM ____.

SESSION 20: NETWORKING SERVICES - PROXY SERVERS & ADDRESS TRANSLATION

RELEVANT KNOWLEDGE

Proxy Server

A proxy server is an application that acts as an intermediate between internal and external networks for processing requests. Proxy servers hide internal networks and hence provide an additional layer of security. They are used to share internet connections across multiple computers such as an Internet Café. Some proxy servers' cache resources such as web pages, videos to prevent content being re-downloaded thus saving network bandwidth referred to as caching proxies. Proxy servers can also be used to restrict or bypass Internet access.

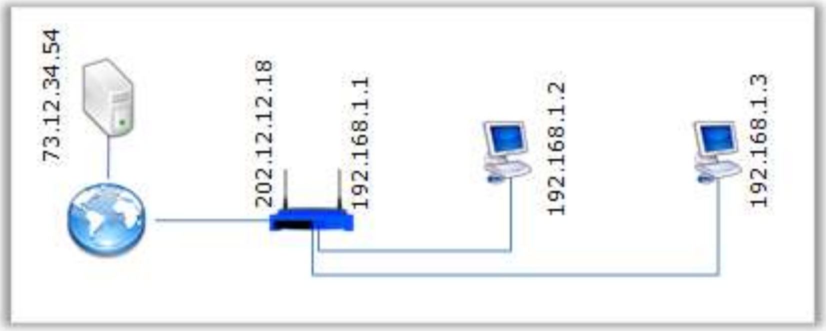


For an example on Caching Proxy, look at the above illustration. All clients and the Proxy Server are connected to a centralized switch which in turn is connected to the Internet. When Client 1 requests a website, it will be forwarded to the Proxy Server. If the content is not available in its cache, the Proxy Server will forward the request outside this network and provide Client 1 with corresponding content once it receives and stores it in its cache. When Client 2 requests for the same website, Proxy Server will search its cache and if available, it will be instantly provided to Client 2. This saves network traffic as the request is processed internally..

Notable proxy servers include Winproxy, Wingate, Microsoft Proxy Server, Squid, etc.

NAT

Network Address Translation or NAT is the process of modifying a private IP address to a public address and vice versa. NAT is commonly used where a single public address is used for sharing Internet access to multiple computers hence, multiple private IP addresses. NAT is a feature used widely in home, small & medium to enterprise networks for more than a decade due to IPv4 address exhaustion. Classic example includes the Internet Café (referred to as browsing centers) which uses a single public IP among multiple clients having private IP addresses.



For example, look at the illustration. ISP has issued a Public address of 202.12.12.18 for this connection (WAN Interface) that is connected to a NAT device. NAT device's internal IP address (LAN Interface) is 192.168.1.1 and the clients are assigned 192.168.1.2 and 192.168.1.3 which are private IP addresses. Clients cannot send any request directly to 73.12.34.54 as it's a public IP address. Listed below is the NAT process in this case:

1. Client 1 sends a request to 73.12.34.54.
2. LAN interface assigned with IP 192.168.1.1 receives the request.
3. NAT software on the Router replaces 192.168.1.1 with 202.12.12.18 and sends the request to 73.12.34.54.
4. 73.12.34.54 replies to 202.12.12.18.
5. NAT software replaces 202.12.12.18 with 192.168.1.1 based on its NAT table.
6. Reply is sent to 192.168.1.2.

The process is repeated for all other clients in the network. Thus though they are assigned Private IP addresses, computers in a network can access the Internet by using a single public IP address.

SOHO Routers are NAT devices widely found in home and small business networks. Since routing happens between public & private IP addresses and vice versa depicting the function of routing, NAT devices are commonly referred to as Routers.

SOHO Routers usually have:

- WAN Port, for connecting to the Internet
- LAN Ports, for connecting 4 to 8 computers using RJ-45 & UTP

- Access Point (Wireless Router Models), for connecting computers using WLAN

Lab: Work with NAT Device

Internet Connection Sharing (ICS)

Internet Connection Sharing is a feature in Windows Operating System that enables you to share Internet access with other computers on a network. ICS can be used when there is no availability of Wi-Fi Routers or other NAT Devices and also on dial-up, DSL, Cable, WiMAX and other connections.

Lab: Use ICS

ICS has a built-in DHCP service that automatically allocates IP address, gateway IP address, DNS IP address to other computers when they connect. ICS DHCP uses the reserved range of 192.168.0.2 to 192.168.0.254 and this range cannot be changed.

When the second computer connects (or is turned on), ICS automatically assigns an IP address from the ICS reserved range and allows the second computer to use the Internet connectivity available on the first computer.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Configure your computer for allowing remote access.
2.	Compare different models of wired routers available from different vendors. Use the Wired Adapters Worksheet below:

Wireless Routers			
Vendor			
Model			
Details			
Default IP			
Default Username			
Default Password			
Default SSID			
WPS (Yes/No)			
IEEE Standards			
IEEE 802.3			

IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			
IEEE 802.11n			
Supported Speed (Mbps), Wired			
10			
100			
1000			
10000			
Supported Speed (Mbps), Wireless			
11			
54			
150			
300			
Frequency			
2.4 GHz			
5 GHz			
Dual Band (2.4 + 5 GHz)			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
Antennas			
Single			
Double			
Detachable (Yes/No)			
Ports			
WAN			
LAN			
USB			
Serial			

ASSESSMENT

Answer the following questions

1. Explain the purpose of a Proxy Server with an example.
2. Explain NAT.
3. Explain ICS.

Fill in the blanks

1. Acronym for NAT ___________________________.
2. ____________ remaps private to public IP addresses and vice versa.
3. Port used by RDP _____.
4. Acronym for ICS ____.
5. IP address range reserved for ICS, from ____________ to _____________.

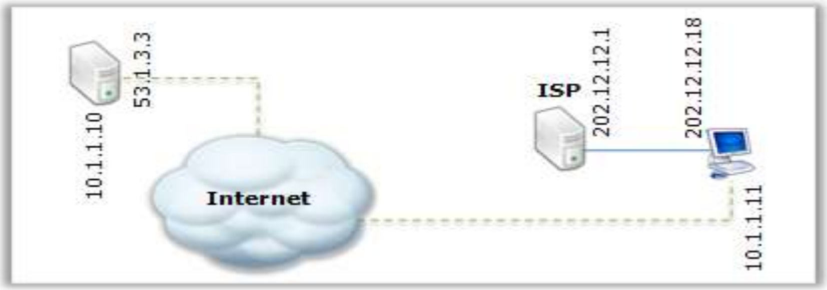
SESSION 21: NETWORK INFRASTRUCTURE – VPN & IPV6

RELEVANT KNOWLEDGE

VPN

Virtual Private Network (VPN) allows private network (LAN) to be extended outside the network. Users of VPNs access resources as if they are present locally though actually they are located remotely. A VPN connection is created through a WAN link such as the Internet but appears as a private link to the end-users hence the name Virtual Private Network. Though accessed through the Internet in most cases, high level of security is maintained between the host computer and the network through use of tunneling protocols and encryption.

For example, look at the following scenario where an employee is allowed to access their office network from a remote location:



1. Employee connects to the ISP to gain access to the Internet.
2. ISP assigns a public IP address to the employee’s computer.
3. Employee connects to the office using VPN.
4. VPN server validates, authorizes and allows employee to connect to office network. At this stage, a private IP address from the VPN DHCP is issued to the employee’s computer and a secure tunnel between the VPN client software and server is established.
5. Employee uses the resources available at office network as if it is available locally.
6. Information is sent and received using encryption mechanisms as defined by the administrator.

VPN uses one of the following two protocols:

- *PPTP* or *Point to Point Tunneling Protocol* operates using TCP (port 1723) to encapsulate PPP packets and can work with variety of other protocols such as IP, IPX & NetBEUI. PPTP relies on authentication protocols such as *PAP, SPAP, CHAP, MS-CHAP, EAP* for secure authentication and *MPPE* to create the VPN tunnel. Support for PPTP is widely available in most client operating systems making it easier to implement. However, PPTP has many security flaws and is considered insecure.

- *L2TP* or *Layer 2 Tunneling protocol* operates using UDP (port 1701) and uses IPSec for security and is considered more secure than PPTP. Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. L2TP also supports multiple protocols but as compared to PPTP, uses strong encryption algorithms.

Server Operating Systems usually include support for setting up VPN connections.

Lab: Setting up a VPN connection

VPN Client

When you want to connect to a VPN, you need to set up a VPN connection on the client computer. You can either use the VPN client software built-in with the operating system or use 3rd party VPN software.

Lab: Set up VPN Connection (Client)

Some client operating systems include support for setting up the computer as VPN Servers typically for Home or Small Office Solutions that is affordable.

Lab: Setup VPN on Client Operating System (Accepting incoming VPN Connection)

IPv6

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), intended to replace IPv4. IPv6 was developed by IETF to address the IPv4 issue of address exhaustion. IPv6 uses a 128-bit address, allowing for 2^{128}, or approximately 3.4×10^{38} addresses, or more than 7.9×10^{28} times more than IPv4.

IPv6 addresses consist of eight groups of four hexadecimal digits separated by colons, for example: 2001:0db8:85a3:0042:1000:8a2e:0370:7334.

Majority of the Operating systems support both IPv4 and IPv6, though use of IPv4 is popular.

IPv4 to IPv6 Tunneling

In situations when you want to connect IPv4 networks using IPv6, IPv6 packets can be encapsulated in IPv4 packets, a process referred to as IPv4 to IPv6 Tunneling.

This is useful in situations when routers between the networks do not understand IPv6.

Stateless address auto-configuration (SLAAC)

One major advantage of IPv6 is the ability to configure itself on an IPv6 network, though IPv6 can be assigned manually by the administrator.

Lab: View or Install IPv6

NETSH

NETSH is a command line utility that is used for viewing and modifying network configurations of a local or remote computer.

Lab: Use NETSH

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Setup VPN on a client operating system
2.	View IPv6 settings and configuration

ASSESSMENT

Answer the following questions

1. Explain VPN with an example.
2. Explain IPv6 with an example.
3. Explain the purpose of NETSH.

Fill in the blanks

1. Acronym for PPTP ____.
2. Acronym for L2TP ____.
3. Acronym for VPN ____.
4. _____________ is a command line utility used for modifying network connection.
5. Number of bits in IPv6 address ____.

6. 2001:2322:0000:12AC:0000:0000:0000:1231 is an example of IP version _ address.
7. _____ is used for connecting computers to corporate networks via the Internet.
8. _____________ protocol is used in VPN for encrypting L2TP data.
9. _______ & _______ are tunneling protocols used in VPN.
10. PPTP uses port number _____.
11. PPTP authentication protocols include _____ , _____ , _____ & _____ .
12. L2TP uses port number _____.
13. Acronym for IPSec __________________.
14. Acronym of SLAAC___________________________________.

SESSION 22: NETWORK SECURITY I

RELEVANT KNOWLEDGE

Network security refers to the practice of securing computers and devices in a network from unauthorized users and attacks. Network security can range from simple procedure such as using a username and password to using complex network devices to protect a network.

When you connect to the Internet, your computer and/or network is exposed to a public network where anyone could possibly attack and gain access to resources including data.

Following are some of the common types of host & network based attacks:

Spoofing

Spoofing is a method that refers to use of forged IP address, MAC address, E-mail address, etc. falsifying and gaining data. For example someone could send a packet from an IP address such as 10.1.1.1 but appears as if it was sent from another IP address thereby allowing the packet to enter into network, thus resulting in gaining access to someone's network without their consent.

Root kits

Root kits are special programs that take control of a computer by replacing critical system files and usually do undetected. Most of root kit programs are kernel-based, they act like parasites and attach themselves with the operating system. Though it is difficult to detect, you can observe change in patterns and check integrity of the operating system to see if it's affected by a root kit and take appropriate action.

Denial of service

Denial of service is a kind of attack that causes services to become unavailable when they are expected. For example a website under DOS (Denial of service) attack will cause itself to halt and affect the users by not providing the necessary service such as access to email or online shopping.

To prevent unauthorized users from gaining access through any method, you need to implement a variety of security measures such as using a firewall, scanning your computer or network for weakness, apply security patches, use IDS, etc.

Firewall

Firewalls are software or hardware devices that protect a computer and/or a network by analyzing and controlling both incoming and outgoing network traffic. Firewalls act like a window between internal and external network allowing authorized users to access resources.

Most operating systems include a software firewall and are configured to keep your computer secure. While software firewalls are sufficient for home and smaller networks, hardware firewalls are essential for larger networks as it offers a higher level of protection and can scale to larger network traffic from tens to hundreds of computers.

Firewall generations:

- First generation: Firewalls use Packet filters, a mechanism in which each packet is analyzed based on a combination of source and destination IP address, ports and decide if the packet should be passed on or discarded.
- Second generation: Firewalls use stateful filters, a mechanism in which each packet is analyzed to track the state of network connection travelling through it. Only packets that match the active connection is allowed or else discarded. *Stateful Packet inspection (SPI)* used in this method is considered most secure as it allows packets to be transmitted to the internal network as the firewall checks if the response packet is originated based on the request sent from the internal network.
- Third generation: Firewalls provide application layer filtering by working closely with the applications (browsers, email software, etc.) and protocols (http, ftp, smtp, etc.). This is useful when unwanted network application software or protocol attempts to use network bandwidth, causing harm to the computer or flood the network traffic and need to blocked or never allowed.

Note: Packet filtering alone does not provide enough protection. In order to effectively block peer-to-peer-related network traffic, what is needed is a firewall that does application filtering, which can be regarded as an extension to stateful packet inspection. Stateful packet inspection can determine what type of protocol is being sent over each port, but application-level filters look at what a protocol is being used for. For example, an application-level filter might be able to tell the difference between HTTP traffic used to access a Web page and HTTP traffic used for file sharing, whereas a firewall that is only performing packet filtering would treat all HTTP traffic equally.

Types of Firewalls

- **Personal Firewalls** are usually shipped with an operating system and protect only the computer on which it is installed. Personal Firewalls are designed to control network traffic generated by applications such as web browsers, file transfer software, email software, etc. installed on a computer. When an application tends to transmit or receive, the firewall looks up the policy defined in the firewall settings and allows or denies network traffic accordingly. If you do not have a personal firewall installed on your computer or you want to use a more advanced firewall software with advanced management capabilities, you can purchase a commercial firewall software or a hardware firewall.

  Notable software firewalls include Windows Firewall (shipped with most versions of Microsoft Windows), ZoneAlarm, Comodo Internet Security Plus, etc. Some Anti-virus vendors bundle firewall software to provide complete protection such as McAfee Internet Security, Kaspersky Internet Security, Norton Internet Security, etc.

- **Enterprise Firewalls** are suitable for organizations that have thousands of users or for networks that need high level of security such as banks. Enterprise Firewalls are usually hardware based, expensive, require additional technical expertise but offer greater levels of protection and scale to larger network traffic without affecting stability in performance. Enterprise firewalls can protect the entire network and operate at the network layer scanning each packet that transmits through them. Notable vendors for enterprise firewalls include Cisco, HP, IBM, Microsoft, Juniper networks, etc.

Barracuda NG Firewall

Check Point Firewall

Zone Alarm, Free Software Firewall

Windows Firewall

Windows Firewall is a built-in firewall software bundled and installed by default on most Microsoft Windows Operating systems like Windows XP, Vista & 7.

Lab: View Windows Firewall Status

Windows Firewall protects the computer by using the default settings (firewall rules) that can be modified anytime. Most commonly used network applications such as web browsers, email client software, etc. work without the need for modifying the settings on the firewall. Some network applications may not work as intended if it is blocked by the firewall (for example, an antivirus software may not be able to update itself from the Internet); in such cases, you need to add the application to the exception list indicating that the application is permitted to use the network or the Internet.

Lab: Add a program to the Exception List in Windows Firewall
Lab: Turn on or off the Windows Firewall.

Port Scanner

You have learnt about port numbers in earlier sessions. Though there are 65,536 ports available, few port numbers are allowed to be used on computer having a firewall installed. However a user can get into a network or a computer using one of the open ports. In such cases it is advisable to block all unused ports.

For us to understand the ports that are open on a computer, you can use port scanner software that scans and provides a detailed report on used and unused ports. This can help you in determining if the computer is prone to any possible security attacks.

Lab: Use Advanced Port Scanner (3rd party software)

TELNET

Telnet is a client-server protocol used for established connections to a remote host. Terminal Emulation or Telnet is still widely used by administrators for troubleshooting network applications. TELNET can be used for connecting to remote computers, switches and routers as well. Telnet provides bi-directional text-oriented communication using a virtual terminal connection. Telnet uses TCP and port number 23.

TELNET Service is built-in with most operating system but may need to be installed or started for accepting incoming connections.

Lab: Connecting to a remote computer using Telnet
Lab: Use TELNET for troubleshooting.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Add at least three network applications to the firewall exception list.
2.	Use Port scanner to scan different computers and observe the results.

ASSESSMENT

Answer the following questions

1. Explain Network Security.
2. What is spoofing?
3. What is a Root kit?
4. Explain Denial of service.
5. Explain Firewall.
6. Explain the procedure to add a program to the exception list of a firewall.
7. Explain the purpose of Port scanner with an example.
8. Explain the purpose of TELNET.

Fill in the blanks

1. Acronym for DOS in computer security context ________________________.
2. ________ is a software application or hardware device that protects computers or network by monitoring network traffic.
3. Acronym for SPI ____________________________________.
4. Acronym for TELNET _________________________________.
5. Telnet uses port number ___.

SESSION 23: NETWORK SECURITY II

RELEVANT KNOWLEDGE

Patch Management

When you install an Operating System or applications, they may have flaws, also referred to as security holes. This can be an opportunity for people who can manipulate and gain control of a computer or network resources using these flaws.

Operating systems and applications may have vulnerabilities (weakness) that can be corrected using by applying security patches, a process referred to as Patch Management.. Since presence of flaws is considered as a security risk & threat, these vulnerabilities must be addressed as quickly as possible. Most vendors analyze weaknesses and provide updates called as patches on a periodic basis. In most cases, the updates are automatically downloaded and updated by corresponding applications. However, it is a recommended practice to analyze a computer or computers on a network for any potential flaws and take necessary steps to correct them.

Belarc Advisor is a software utility that builds a detailed profile of installed software and hardware, missing security patches, anti-virus status, security configurations, and displays the results in a Web browser.

Lab: Download and use Belarc Advisor

Microsoft Baseline Security Analyzer (MBSA) is another utility that can be used for scanning vulnerabilities by checking an operating system if appropriate security patches are applied or not. MBSA checks most products such as the operating system itself, Internet Explorer, IIS, SQL Server, etc. and is restricted to products from Microsoft.

Packet Analyzer

Packet Analyzer is a software or hardware that can be used for monitoring network traffic passing over wired or wireless networks. As data flows over the network, each packet is captured, decoded and contents are analyzed. Packet analyzers are used for analyzing network problems, network utilization and to even detect network misuse by internal or external users. Popular packet analyzers include Wireshark, Microsoft Network Monitor, TCPDUMP, SniffPass, Capsa Free Network Analyzer, etc.

Lab: Network Monitor

IDS (Intrusion Detection System)

IDS is a software application or a hardware device used for monitoring a computer or a network for any malicious activities or violations and reports to a management system. IDS are used by administrators to receive an alert when any suspicious attempt is made to a computer or a network and to prevent further access to the computer or the network. IDS can be host based or network based.

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Use MBSA to analyze your computer and computers within your network. Refer to MBSA help file for instructions.

ASSESSMENT

Answer the following Questions

1. Explain Patch Management.
2. Explain Packet Analyzers.
3. Explain the procedure to use Network Monitor with an example.
4. What is IDS?
5. Explain MBSA.

Fill in the blanks

1. List any two utilities that can be used for analyzing vulnerabilities.
2. List any three Packet Analyzers.
3. Acronym for IDS ________________________________.
4. Acronym for MBSA ____.

SESSION 24: TROUBLESHOOTING NETWORKS

RELEVANT KNOWLEDGE

Troubleshooting Networks

You have learnt a variety of utilities and concepts. When you manage a network, it is quite common to face a number of issues related to network or Internet connectivity. Always check for any recent changes made to a computer or network before starting to troubleshoot; it's most likely that you find a clue that will save time.

Some of the well-known error messages include:

- **Network cable unplugged**: Indicates issue with cable; check if the cables are properly connected to both computer and network switch or SOHO Router. Use alternate cables to confirm.
- **Limited or No Network Connectivity**: Indicates issue with network card or IP settings, later more common. Check if the computer is configured as a DHCP client and verify its IP address, gateway and other relevant settings.
- **The Network Path cannot be found**: Indicates issue with network card, IP settings or Name resolution problems. Use the File and Print Sharing troubleshooting procedure.
- **Windows has detected an IP address conflict**: Indicates issue with IP address; assign another static IP address that is different than the one assigned to other computers within the same network.
- **A duplicate name exists on the network**: Indicates two or more computers in a network have the same name; assign another computer name that is different than the one assigned to other computers.

Use the following checklist and scenarios as a general guideline when troubleshooting:

- Unable to connect to a network (LAN)

If you are unable to connect to another computer on the same network, do the following:

1. Verify the cables are connected properly at both ends.
   a. Use a cable tester if required.
   b. Replace RJ-45 Jacks or use different cable if possible.

   c. Check LED indicators on the NIC to verify connectivity status, interpret based on NIC product manual.
2. Check if the NIC is installed and working properly using Device Manager.
   a. Sometimes the device drivers may be updated when operating system downloads and installs updates automatically. In some cases, updated drivers may be pushed through special software bundled along with device drivers. Typically updated drivers work properly as they address technical issues caused in earlier versions. In rare cases, these device drivers cause problems and need to be replaced with the drivers that worked earlier. .
      i. Use device manager to find if the driver was updated to a most recent one and if that's causing the problem; if yes, try using Rollback driver to replace the current driver with the previous device driver.
      ii. If Rollback driver did not fix the problem, re-install device drivers from the original compact disc. If original compact disc is not available, then download the drivers from Vendor's website and complete the installation. Verify if the issue is fixed.
      iii. Always use device drivers intended for the correct version of the operating system. Device drivers designed for 32-bit operating systems are NOT compatible with 64-bit operating systems and vice versa.
      iv. Download drivers ONLY from the manufacturer's website; never download drivers from 3rd party websites that may be modified internally and may cause major problems. Contact the vendor for correct or compatible device drivers.
3. Check if the NIC settings are proper (if altered) using Device Manager.
   a. In general, settings are managed automatically and usually not modified in home, small business or enterprise networks. Sometimes, network card settings are modified to match a network environment and incorrect settings can lead to problems in network connectivity.
   b. Use Device Manager to verify if settings such as duplex settings, etc. are intact. If unsure, reset the settings to the default value indicated as Auto; refer to NIC's product manual.
4. Check if the computer has a Valid IP address (Use IPCONFIG).
   a. Computers are usually configured to receive IP address from DHCP in most networks to ease administration. If there are issues with the DHCP server, computers configured as DHCP clients will not receive

any IP address resulting in network issue. In home and small business networks, devices such as SOHO routers provide IP addresses to client computers.

   i. Check if the DHCP Service is functional by logging to the SOHO router.
   ii. If all other computers configured as DHCP clients receive IP address from DHCP Service, then do the following (try each step and verify if the issue is resolved):
      1. Use IPCONFIG/RENEW.
      2. Disable and enable Network Adapter (Local Area Connection).
      3. Check if any firewall or startup program is blocking (Use MSCONFIG to reduce startup programs and check firewall settings).
      4. Test the affected computer by assigning a static IP address in the same subnet. Verify if the issue is resolved.

- Unable to connect to Internet (WAN).

Always verify if the issue is associated with a particular program or all programs on a computer. You can save time by proper probing to understand the exact issue. For an example, if you hear a complaint like "*Internet not working*", it could actually refer to an issue when a user is unable to use their email client, a web browser, video conferencing software or a game.

In addition to the above mentioned procedure (Unable to connect to a network (LAN)), use the following guidelines.

1. Test if the computer is able to communicate with the gateway (Ping gateway's IP address).
2. Test if the computer is able to communicate with the DNS server (Ping DNS Server's IP address).
   a. If you receive request timed out or extremely delayed response from your external DNS servers, try using other DNS Server' IP address such as one of the Public DNS servers. Using Public DNS Servers can improve performance and resolve issues related to DNS name resolutions; for example, Google provides free Public DNS to be used as alternate to DNS Servers. Typically ISP's provide Primary and alternate DNS's server's IP address pushed along with your IP address when you subscribe; if you have performance or name resolution issues with your ISP's DNS Servers, then it is recommended to use

the Public DNS Server's IP address. For example, to use Google's Public DNS Servers on a computer, do the following:

i. Click ***Start > Run > Type ncpa.cpl > Click OK***.
ii. Right-click ***Local Area Connection***, select ***properties***.
iii. Select ***TCP/IP (TCP/IPv4)***, select ***Properties***.
iv. Enter ***8.8.8.8*** and ***8.8.4.4*** as ***primary*** and ***alternate*** DNS Servers, click ***OK***.

Now your computer will use the Google's Public DNS servers for name resolution instead of your ISP's DNS Server. You can also specify the Google's Public DNS Server's IP address in your SOHO Router, if you want to use Google's Public DNS Servers for all computers and devices within your network; refer to SOHO router's product manual to alter this setting.

v. Use NSLOOKUP to verify name resolution functionality.

b. You can also use OpenDNS, a name resolution service that is offered for free. As compared to public DNS servers, OpenDNS offers additional facilities such as Phishing & Botnet Protection, Web Content Filtering, etc., refer to OpenDNS for more information.

3. If you do not have issues with name resolution, but a problem associated with a specific program such as a web browser or an email client, do the following:

   a. Try using programs of similar nature. For example, if the issue is related to a web browser such as Mozilla Firefox, try using Google Chrome or Internet Explorer.

      i. If it works fine with other browsers.

         1. Clear the browser's cache; web browsers store cached copies of content when you visit websites that could lead to problems.
         2. Check the settings of the web browser that related to this issue. Reset it to defaults or the value associated with the issue. Refer to browser's help file for further instructions.
         3. Web browser add-on's or plug-gin's offer additional functionality; some addons cause problems when in use. In such cases, you can disable the particular addon by using the addon settings within the web browser. If you are not sure of the addon that is causing the problem, try disabling all addons and verify if the issue

is resolved. If the issue appears fixed, then try enabling each addon to confirm the issue with an addon.

b. If the issue is related to a email client such as Microsoft outlook configured to download copies of emails from a service provider such as Gmail, Live or Yahoo!. Or custom email messaging providers, do the following:

    i. Check if any other programs are using the network or Internet bandwidth; stop or exit all other network applications that consume bandwidth for testing.

    ii. Check Username & password combinations, if you are unable to login; some services require just the username (SOMENAME) and some require username along with domain name suffix (SOMENAME@EXAMPLE.COM) for login names. Verify password as well; check if the password was recently changed.

    iii. Check if this the ports are blocked by a firewall by using TELNET

    iv. Verify the email client POP3/SMTP settings of the email client by referring to the settings as required by the ISP.

    v. Some ISP's offer complimentary email addresses when customers avail web hosting services; usually the POP3/SMTP settings are different than the conventional port numbers or settings, contact ISP for exact details if required. Check if the ports are accessible using TELNET.

    Tip: Most ISP's allow email access through a web browser pointing to customer's domain names, commonly referred to as webmail such as *mail.domainame.extension*. Check customers webmail to verify the status of mail service and to provide alternate access until the actual issue is resolved.

c. If the issue is related to a chat software or video conferencing software such as Skype, do the following:

    i. Verify and confirm if other applications are working

    ii. Some video conferencing software use TCP or UDP ports that may be disallowed by default in the firewall settings of a local computer. Open the firewall and the application to the exception list and verify if it is working.

    iii. If you are using a computer behind a SOHO Router, you may have to open certain port numbers or port range for the application to work. Usually port numbers required by such applications are documented and labeled as "Port

Forwarding” by respective vendors. Refer to the application software and the SOHO router to configure.

iv. In certain cases you may have to expose all port numbers for a particular computer in a network; for example, multiplayer games designed for use in the Internet or an organization providing a range of services from set of computers or hosts. Demilitarized Zone or DMZ, is a perimeter network that separates a single computer or a network from the LAN (though it is a part of the LAN) allowing access to a specific computer or the network. Computers that belong to DMZ typically used in SOHO Routers are exposed to the Internet, prone to direct attacks. Refer to SOHO Router manual for further reference.

- Unable to connect to a network share (File & Print Sharing).

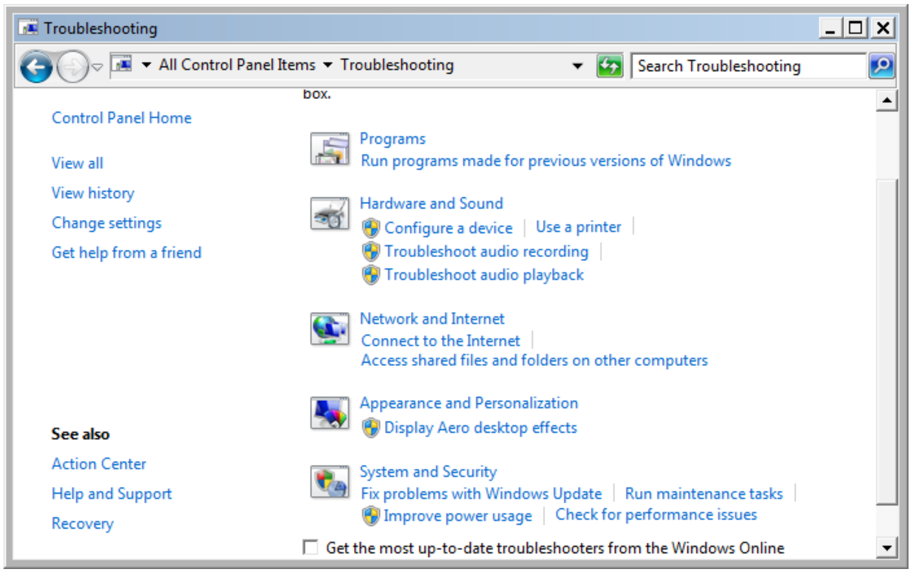
    1. File and Print sharing service is widely used in most networks, especially on Microsoft Windows Networks. On a Microsoft Windows Network, computers are accessed each other by computer names. For example, a folder with a share name “MYSHARE” on a computer named “DESKTOP01” is accessed through the UNC path, \\DESKTOP01\MYSHARE. If you are unable to access shares, do the following:
        - a. Confirm the share name and computer name.
        - b. Check if its computer or network specific; for example, if this share is not accessible only a particular computer or the entire network.
            - i. If it is across the entire network, then do the following on the computer that is configured to act as a server:
                1. Check network adapter & IP address settings.
                2. Check if File and Printer Sharing is allowed in Windows Firewall or 3rd party firewall.
            - ii. If it is only on a single computer, then do the following on the computer where the share is being accessed:
                1. Check network adapter & IP address settings.
                2. Check if you are able to access the computer by IP address instead of computer name.
                    - a. If you are able to access the computer by IP address but not by computer name, it indicates a problem with name resolution. Add the remote computer along with its IP address in the HOSTS file for quick resolution.

b. Check if NETBIOS over TCP/IP is enabled (Advanced Settings of TCP/IP Properties).
c. Check Firewall settings. If unsure, disable firewall and verify.

Note: On computers running vista/7/8 additional procedures may be required, refer to the manual for detailed instructions.

Some operating systems include built-in facilities for fixing issues automatically. For example, you may use the ***Repair*** or ***Diagnose*** option to fix network issues automatically. This could be useful for users who do not have sufficient knowledge to fix network issues or even understand their network setup. Network troubleshooter designed to run series of tests and present friendly messages that is understandable by non-technical persons. To repair your network connection automatically, do the following:

1. Click ***Start*** > ***Control Panel*** > ***Troubleshooting***.



box.

Control Panel Home

View all
View history
Change settings
Get help from a friend

See also
Action Center
Help and Support
Recovery

Programs
Run programs made for previous versions of Windows

Hardware and Sound
Configure a device | Use a printer |
Troubleshoot audio recording |
Troubleshoot audio playback

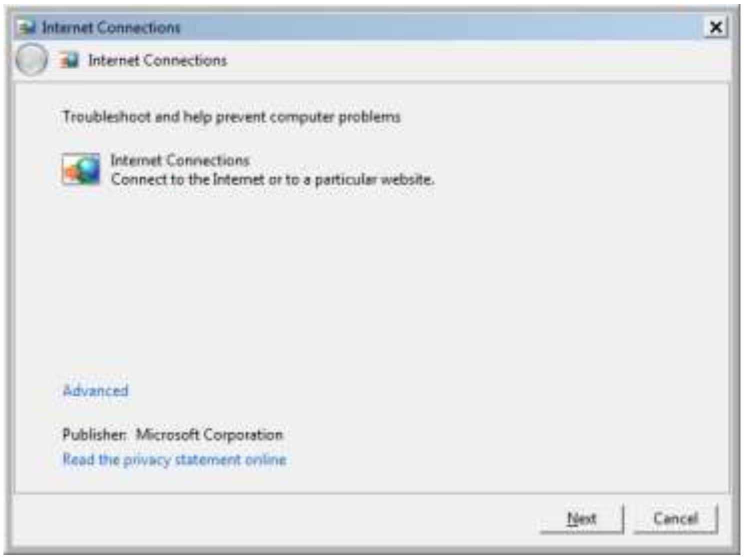
Network and Internet
Connect to the Internet |
Access shared files and folders on other computers

Appearance and Personalization
Display Aero desktop effects

System and Security
Fix problems with Windows Update | Run maintenance tasks |
Improve power usage | Check for performance issues

□ Get the most up-to-date troubleshooters from the Windows Online

2. To troubleshoot issues related to Internet connectivity, select *Connect to the Internet*.



Troubleshoot and help prevent computer problems

Internet Connections
Connect to the Internet or to a particular website.

Advanced

Publisher: Microsoft Corporation
Read the privacy statement online

3. Click *Next*. Follow the on-screen instructions.

Remote Desktop

Remote Desktop is a feature that enables computers to be managed remotely from other computers. This feature is commonly used by administrators to take remote control of a computer for performing administrative tasks such as installing or removing software, managing user accounts, troubleshoot application issues, etc. The functions are similar to that of normal system administration, except these are all done remotely.

Remote Desktop uses the Remote Desktop Protocol (RDP) for communication and TCP port 3389.

Lab: Remote Desktop

Remote Assistance

Remote Assistance is a GUI utility that can help you take control of a remote computer. You can use Remote assistance to perform maintenance or to troubleshoot a remote computer. This could be useful in situations when you want to connect to a customer's computer present in a remote location immediately saving time and travel.

Note: Both Remote Desktop & Remote Assistance has the same purpose; while Remote Desktop is used by administrators, Remote Assistance is meant for home users or consumers who have less technical knowledge. Also screen sharing (ability to see what a technician is doing on your computer) is available only in Remote Assistance. Remote Desktop does not require invitations to be sent like in Remote Assistance.

Lab: Remote Assistance

You can also use other 3rd party software such as VNC, TeamViewer, GoToAssist, Ammyy admin, GoToMyPC, LogMeIn, Radmin, Symantec pcAnywhere, Google Chrome Remote Desktop, etc. for taking remote control of a computer.

Troubleshooting Model

As general practice, you need to adopt a troubleshooting model that can help you stay organized and troubleshoot effectively. Following is a general guideline:

1. Gather Information about the Issue or Statement.
    a. Probe to differentiate if it is a request or an issue.
    b. Probe to find out if it is affecting single computer or an entire network.
2. Determine if any recent changes were made.
    a. Examples: was any software downloaded and installed with or without their knowledge, any settings was changed, any hardware device added or removed, etc.
3. Determine the most probable cause.
4. Create an action plan.
5. Verify the result and apply preventive measures.
6. Document the resolution.

Though this gives you a broad picture about troubleshooting, you may have to use additional resources in certain situations. Use the following guidelines to enhance your knowledge on troubleshooting further:

- Most product manuals or help files include detailed instructions for completing most tasks. It is highly recommended to read the product manual to understand features and limitations prior to troubleshooting. Sometimes, you may also find late-breaking information (most recent issues when the product is about to be shipped out) usually documented in a file labeled as Readme.txt or Readme.htm.
- Vendors also provide additional Self-help through community forums setup for each product or feature at their websites. You may submit your question or issue that may be answered by experts for a possible resolution. Be aware that you may even receive an answer from a normal registered user who may or

may not be 100% competent in the particular area; if the answer is vague, try validating the answer from another expert in such cases.

- Paid or Free Support is offered by a variety of vendors; some vendors offer free support through email or chat while charge a fee for voice support. Research by visiting the website and find out if there is a way to get your solution, either for free or for a small fee.
- Make use of free eBooks or training materials that are widely available on the Internet. Use free resources such as Wikipedia, eHow.com, about.com, etc. for articles on networking, troubleshooting, etc.

FTP

File Transfer Protocol or FTP is a network protocol used for transferring files between local and remote computers. FTP (executable) is a command line utility used in most operating systems for file transfers.

Lab: Use FTP

EXERCISE

Perform the following activities till you are confident:

S.No.	Activities
1.	Use the following remote administration tools to take remote control of a computer: a. Download, install and use TeamViewer b. Download, install and use Google Chrome Remote Desktop c. Download, install and use Ammyy admin
2.	Discuss different network scenarios and how to troubleshoot

ASSESSMENT

Answer the following questions:

1. Explain any three well-known error messages and cause of the error messages.
2. Explain the procedure to troubleshoot:
   a. If you are unable to connect to another computer within a LAN
   b. If you are unable to connect to the Internet
3. Explain the procedure to use remote desktop.
4. Explain the purpose of Remote Assistance with an example.

5. Explain any two remote administration tools.

Fill in the blanks

1. __________ is a built-in utility that is used for connecting and troubleshooting issues on a remote computer.
2. List any five free remote administration utilities. ______________ , ___________ , ____________, ____________ & _______________.
3. Shortcut (executable) for Remote Assistance __________.
4. ___________ is a command line utility used for transferring files between remote computers.
5. FTP uses port number __.
6. Remote Desktop uses ________________ protocol.
7. RDP uses port number ____.
8. Shortcut (executable) for Remote Desktop __________.

LIST OF CONTRIBUTORS

Advisors:

1. Mr. Ajay Mohan Goel, Director - Skills College, Wadhwani Foundation.
2. Mr. Austin Thomas, Director – Skills College Initiative, Wadhwani Foundation.
3. Prof. R.B. Shivagunde, Joint Director, PSSCIVE, Bhopal.
4. Dr. Vinay Swarup Mehrotra, Head, Curriculum Development and Evaluation Centre, PSSCIVE, Bhopal.

Subject Matter Experts:

1. Ms. Sonia Kakkar. Wadhwani Foundation.
2. Mr. Karthik Chandru, Wadhwani Foundation.
3. Ms. Toral Veecumsee, Wadhwani Foundation.
4. Mr. Ajay Goel, Wadhwani Foundation.
5. Mr. Austin Thomas, Wadhwani Foundation.

Editing:

1. Ms. Sonia Kakkar, Wadhwani Foundation.
2. Dr. Vinay Swarup Mehrotra, Head, Curriculum Development and Evaluation Centre, PSSCIVE, Bhopal.

Coordination:

1. Ms Rekha Menon, Wadhwani Foundation.
2. Mr. Ajay Goel, Wadhwani Foundation.
3. Mr. Austin Thomas, Wadhwani Foundation.