Networking

Table of Contents

Update Notes

February 2, 2017 : Version 2

- Added Network Topologies
- Added the Index
- Declared Section 1: Network Fundamentals ***complete***
- Declared Section 2: Data Transmission ***complete***
- Declared Section 3: Wireless Networking ***complete***

February 1, 2017 : Version 1

- Contains a list of all objectives, Formative assessment topics and Summative assessment questions.
- Supports presentations for Networking Fundamentals, but does not contain answers to all 3.1.1 to 3.1.5 topics.
- Contains the section on OSI
- Distribution List
  - The table of contents which lists the Objectives
  - The Formative and Summative assessment pages
  - The section on the OSI Model

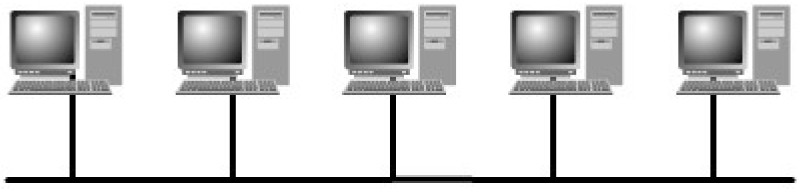
Network Fundamentals

A **computer network** is a collection of computing devices that are connected in various ways to communicate and share resources. Usually, the connections between computers in a network are made using physical wires and cables. However, some connections are wireless, using radio waves or infrared signals to transmit data.

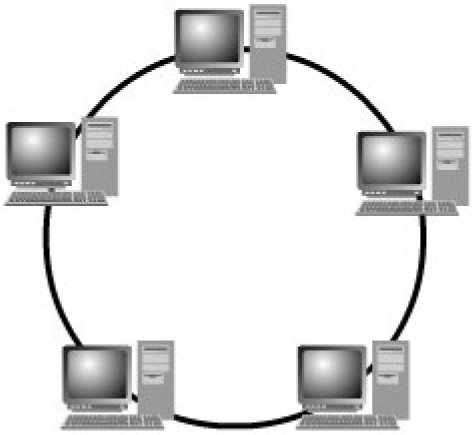
3.1.1 Identify different types of networks.

A network ***topology*** is the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology. Examples: Bus, star and ring

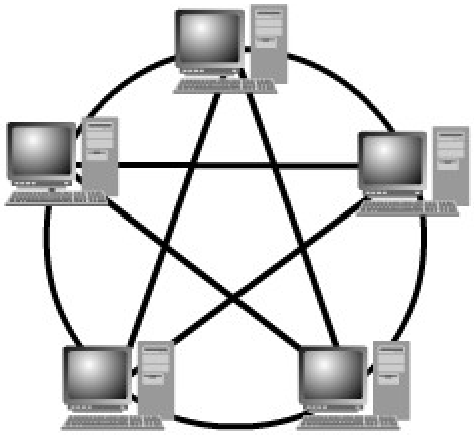
Computer Network Topologies – **Bus Topology**: Single Physical Layer



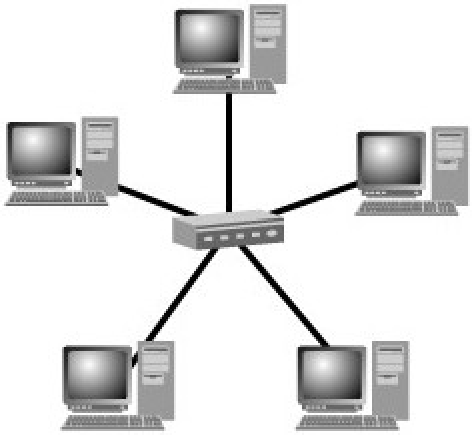
Computer Network Topologies – **Ring Topology**: No Centralized Point



Computer Network Topologies – **Mesh Topology**: Fully Connected



Computer Network Topologies - **Star Topology**: Centralized Point



Question: Describe the following types of networks: LAN, WAN, MAN, VLAN, SAN, VPN, PAN, AND P2P.

Local Area Network LAN

A network connecting a relatively small number of computers in a close geographic area. LANs are usually confined to a single room or building. They may sometimes span a few close buildings.

Wide Area Network WAN

A network that connects two or more local-area networks over a potentially large geographic distance. WANs use telephone lines, satellite dishes, or radio waves to span larger geographical areas than can be covered by a LAN. The Internet is an example of a WAN. The **Internet** is a vast collection of smaller networks that have agreed to communicate using the same protocols and to pass along messages so that they can reach their final destination.

Metropolitan Area Network MAN

A computer **network** that interconnects users with computer resources in a geographic **area** or region larger than that covered by even a large local **area network** (LAN) but smaller than the **area** covered by a wide **area network** (WAN).

Virtual Local Area Network VLAN

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

A VLAN can map workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

Storage Area Network SAN

A network of storage devices that can be accessed by multiple computers. Each computer on the network can access hard drives in the SAN as if they were local disks connected directly to the computer. This allows individual hard drives to be used by multiple computers, making it easy to share information between different machines.

While a single server can provide a shared hard drive to multiple machines, large networks may require more storage than a single server can offer. For example, a large business may have several terabytes of data that needs to be accessible by multiple machines on a local area network (LAN). In this situation, a SAN could be setup instead of adding additional servers. Since only hard drives need to be added instead of complete computer systems, SANs are an efficient way to increase network storage.

Virtual Private Network VPN

A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

Personal Area Network PAN

The interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

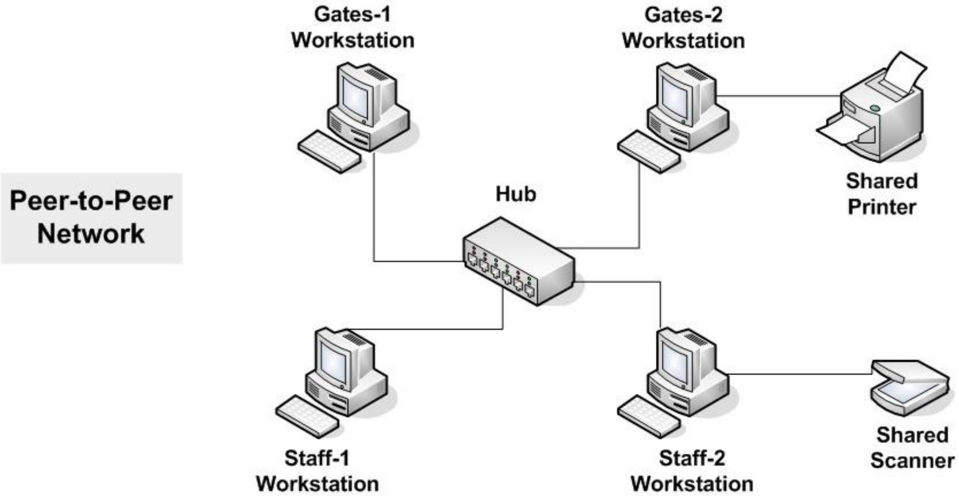
Peer to Peer Network P2P

In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

The only requirements for a computer to join a peer-to-peer network are an Internet connection and P2P software. Common P2P software programs include Kazaa, Limewire, BearShare, Morpheus, and Acquisition. These programs connect to a P2P network, such as "Gnutella," which allows the computer to access thousands of other systems on the network.

Once connected to the network, P2P software allows you to search for files on other people's computers. Meanwhile, other users on the network can search for files on your computer, but typically only within a single folder that you have designated to share. While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads. Therefore, it is best to be on the safe side and only download software and music from legitimate websites.

EXAMPLE:



Shown above, there is a scanner that is connected to the Staff-2 Workstation, this scanner can be shared with the other workstations connected to the networking. Similarly, the Gates-2 Workstation has shared its printer.

3.1.2 Outline the importance of standards in the construction of networks.

Protocols

- Computer networks can consist of many computers that are different and distant from each other.
- These computers may have different platforms (PC, mainframe, or supercomputer).
- They may also have different processors, operating systems, and hardware.
- Because of this diversity in a computer network, rules are necessary for the computers to be able to communicate with each other. These rules are called protocols.
- A protocol is a set of rules that govern data communication. Because there are so many differences among computers, more than one rule is necessary.

A **network protocol** is a standard set of rules and procedures for computers to use when communicating with one another.

A protocol is a reference ensuring that all programs are written following the same format. It would be pointless to write a communications program in which the programmer invents his own series of codes and messages. Such a program would be unable to interact with any other. The program receiving the output of this original program would be unable to decipher the messages. For this reason all programs must follow common standards.

Networking is a field that particularly requires common protocols. These protocols or standards enable **compatibility** through a common language. Software and hardware producers need to ensure their products are compatible with each other. Open standards encourage diversity of production, which drives competition, lowers prices and generates innovation.

An example of a standard networking protocol is TCP/IP. This communication protocol enabled the proliferation of the Internet possible.

3.1.3 Describe how communication over networks is broken down into different layers.

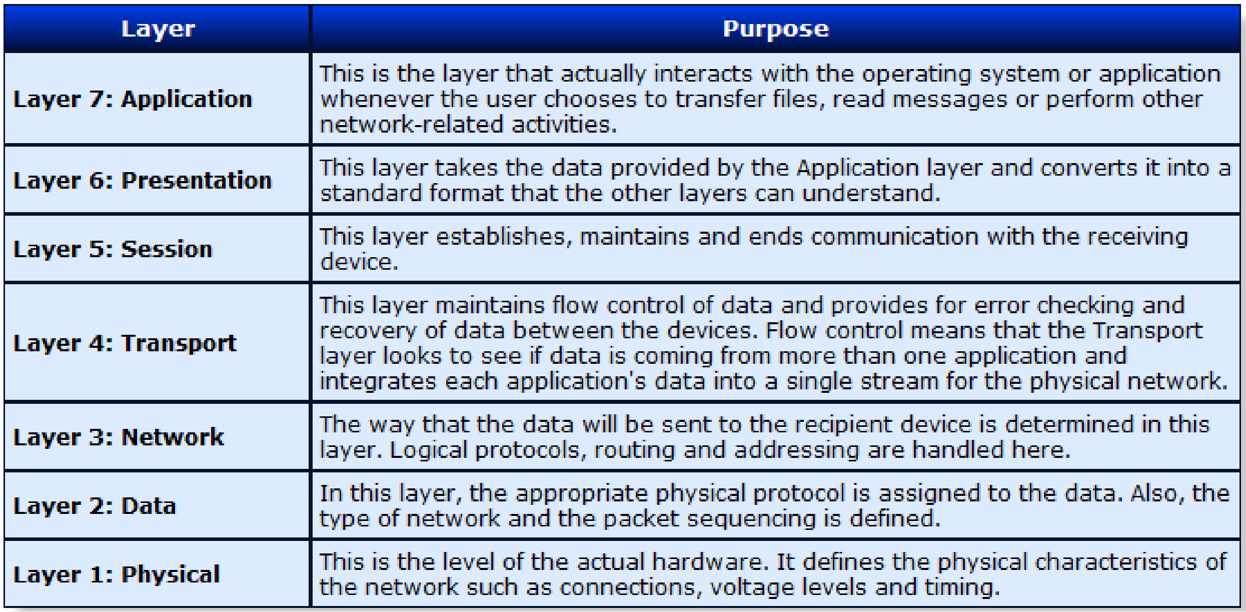
Perhaps no other standard has affected networking more than the **OSI model**. Virtually all networks in use today are based in some fashion on the Open Systems Interconnection (OSI) standard. OSI was developed in 1984 by the International Organization for Standardization (ISO), a global federation of national standards organizations representing approximately 130 countries.

Early in the development of computer networks, commercial vendors came out with a variety of technologies that they hoped businesses would adopt. The trouble was that the proprietary systems were developed with their own particular nuances and did not permit communication between networks of different types. As network technologies grew, the need for interoperability became clear; we needed a way for computing systems made by different vendors to communicate. The OSI model provided a standard way for this communication to take place.

> Interoperability - The ability of software and hardware on multiple machines and from multiple commercial vendors to communicate.

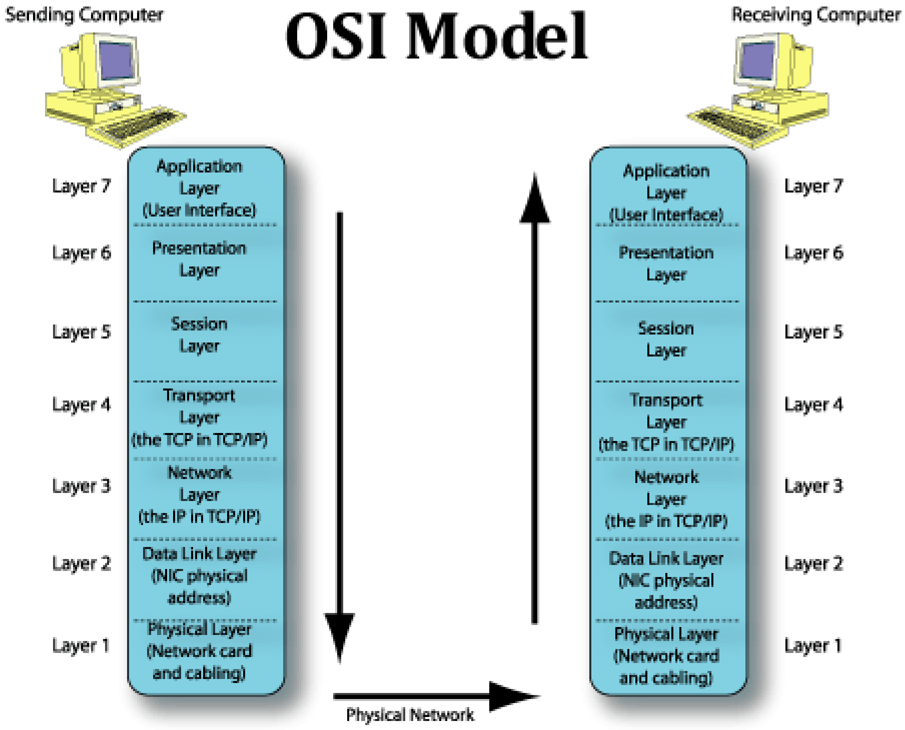
Every machine that can be connected to a network goes through similar process in transferring that data out on the wire. An application that we are running on that device generates some data that it wants to send to some other device on the network. The information must be placed in a format suitable for the application that will receive it on the other side. Once this is done, the machine goes through the process of encoding the data into a network-ready format. This is done by breaking the data up into small units called **packets**. The packet not only contains raw data (just a few bytes in each packet), but it contains other important information such as where the data will go.

The OSI Model uses seven layers to define the different stages that data must go through to travel from one device to another over a network. Each layer deals with a particular aspect of network communication. Think of the seven layers as the assembly line in the computer. At each layer, certain things happen to the data that prepare it for the next layer. The table below lists the seven layers along with a description of their purpose in the network communication process.



Layer	Purpose
Layer 7: Application	This is the layer that actually interacts with the operating system or application whenever the user chooses to transfer files, read messages or perform other network-related activities.
Layer 6: Presentation	This layer takes the data provided by the Application layer and converts it into a standard format that the other layers can understand.
Layer 5: Session	This layer establishes, maintains and ends communication with the receiving device.
Layer 4: Transport	This layer maintains flow control of data and provides for error checking and recovery of data between the devices. Flow control means that the Transport layer looks to see if data is coming from more than one application and integrates each application's data into a single stream for the physical network.
Layer 3: Network	The way that the data will be sent to the recipient device is determined in this layer. Logical protocols, routing and addressing are handled here.
Layer 2: Data	In this layer, the appropriate physical protocol is assigned to the data. Also, the type of network and the packet sequencing is defined.
Layer 1: Physical	This is the level of the actual hardware. It defines the physical characteristics of the network such as connections, voltage levels and timing.

The illustration below shows the flow of data from one computer to another through a network that uses the ISO standard.

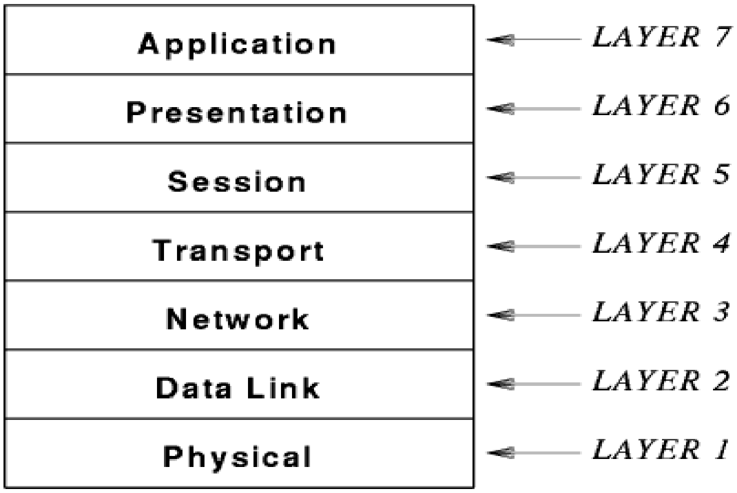

Sending Computer
OSI Model
Receiving Computer
Layer 7
Application Layer (User Interface)
Layer 6
Presentation Layer
Layer 5
Session Layer
Layer 4
Transport Layer (the TCP in TCP/IP)
Layer 3
Network Layer (the IP in TCP/IP)
Layer 2
Data Link Layer (NIC physical address)
Layer 1
Physical Layer (Network card and cabling)
Physical Network

Note: The IB curriculum states, "Awareness of the OSI seven layer model is required, but an understanding of the functioning of each layer is not."

ISO/OSI Model

- The International Standards Organization (ISO) Open Systems Interconnect (OSI) is a standard set of rules describing the transfer of data between each layer in a network operating system. Each layer has a specific function (i.e. the physical layer deals with the electrical and cable specifications)

- The OSI Model clearly defines the interfaces between each layer. This allows different network operating systems and protocols to work together by having each manufacturer adhere to the standard interfaces. The application of the ISO OSI model has allowed the modern networks that exist today. There are seven layers in the OSI model.



The ***Physical Layer***

- Establishes the physical characteristics of the network (e.g., the type of cable, connectors, length of cable, etc.)
- Defines the electrical characteristics of the signals used to transmit the data (e.g. signal voltage swing, duration of voltages, etc.)
- Transmits the binary data (bits) as electrical or optical signals depending on the medium.

The ***Data Link Layer***

- Defines how the signal will be placed on or taken off the NIC. The data frames are broken down into individual bits that can be translated into electric signals and sent over the network. On the receiving side, the bits are reassembled into frames for processing by upper levels.

- Error detection and correction is also performed at the data link layer. If an acknowledgement is expected and not received, the frame will be resent. Corrupt data is also identified at the data link layer.

- Because the Data-Link Layer is very complex, it is sometimes divided into sublayers (as defined by the IEEE 802 model). The lower sublayer provides network access. The upper sublayer is concerned with sending and receiving packets and error checking.

The ***Network Layer***

- Primarily concerned with addressing and routing. Logical addresses (e.g., an IP address) are translated into physical addresses (i.e., the MAC address) for transmission at the network layer. On the receiving side, the translation process is reversed.

- It is at the network layer where the route from the source to destination computer is determined. Routes are determined based on packet addresses and network conditions. Traffic control measures are also implemented at the network layer.

The ***Transport Layer***

- On the sending side, messages are packaged for efficient transmission and assigned a tracking number so they can be reassembled in proper order. On the receiving side, the packets are reassembled, checked for errors and acknowledged.

- Performs error handling in that it ensures all data is received in the proper sequence and without errors. If there are errors, the data is retransmitted.

The ***Session Layer***

- Is responsible for establishing, maintaining, and terminating a connection called a 'session'.

- A session is an exchange of messages between computers (a dialog). Managing the session involves synchronization of user tasks and dialog control (e.g., who transmits and for how long). Synchronization involves the use of checkpoints in the data stream. In the event of a failure, only the data from the last checkpoint has to be resent.

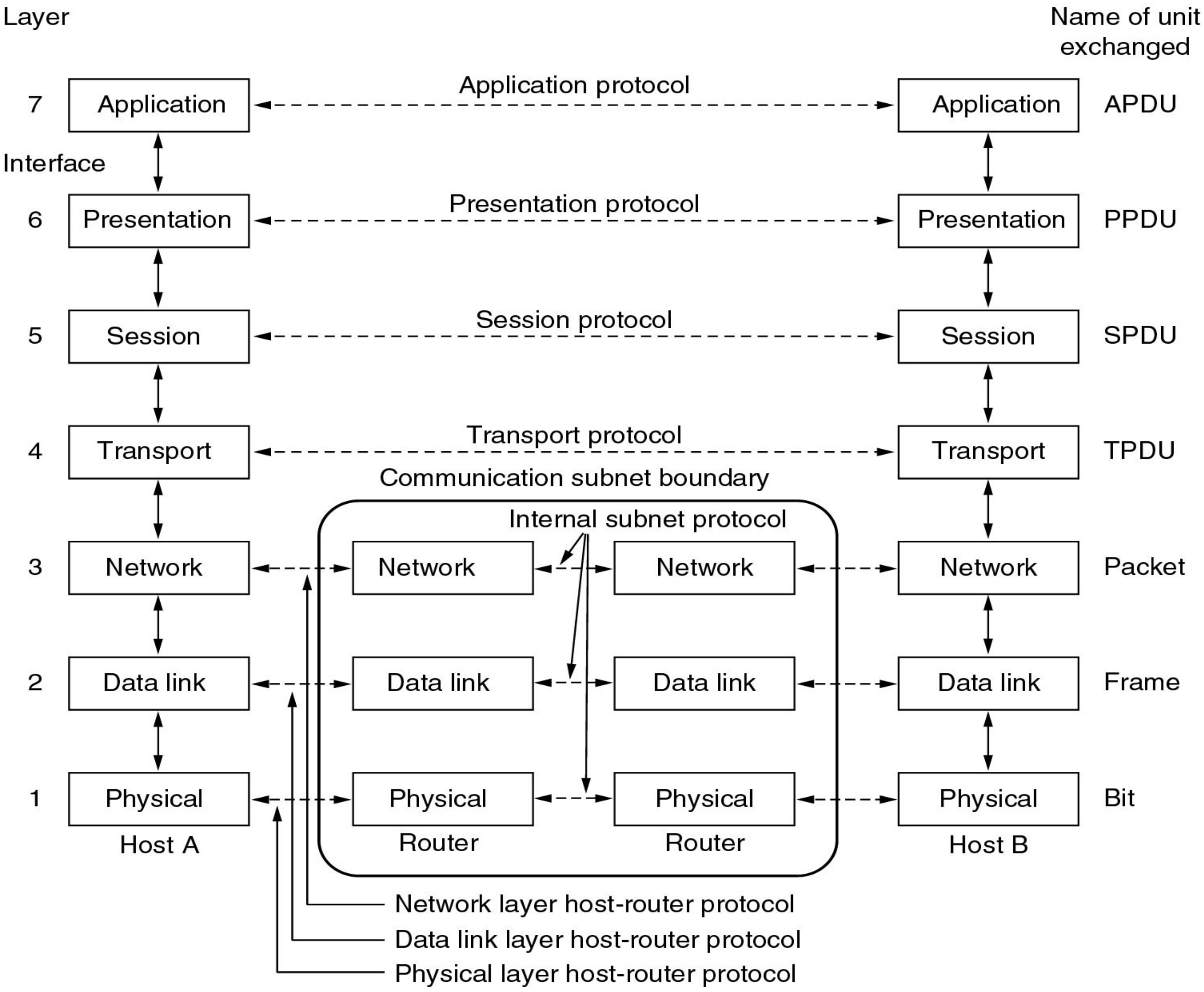
- Logon, name recognition and security functions take place at the Session Layer.

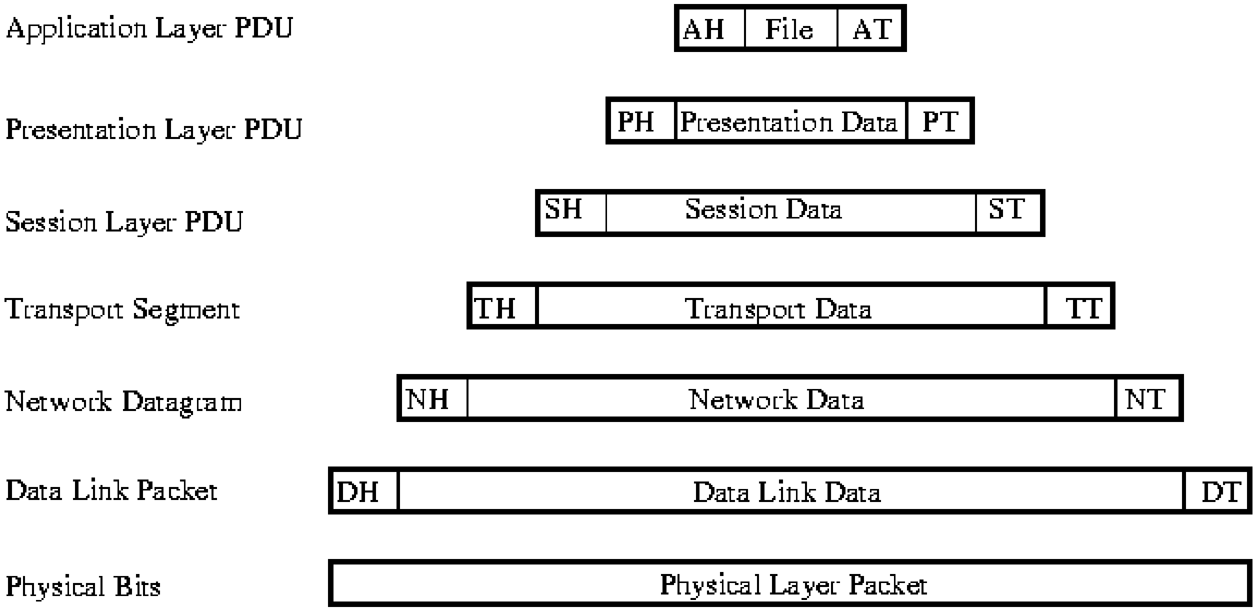
The ***Presentation Layer***

- It is responsible for data translation (formatting), compression, and encryption.
- The Presentation Layer is primarily concerned with translation; interpreting and converting the data from various formats. For example, EBCIDIC characters might be converted into ASCII. It is also where data is compressed for transmission and uncompressed on receipt. Encryption techniques are implemented at the Presentation Layer.
- The redirector operates at the presentation layer by redirecting I/O operations across the network.

The ***Application Layer***

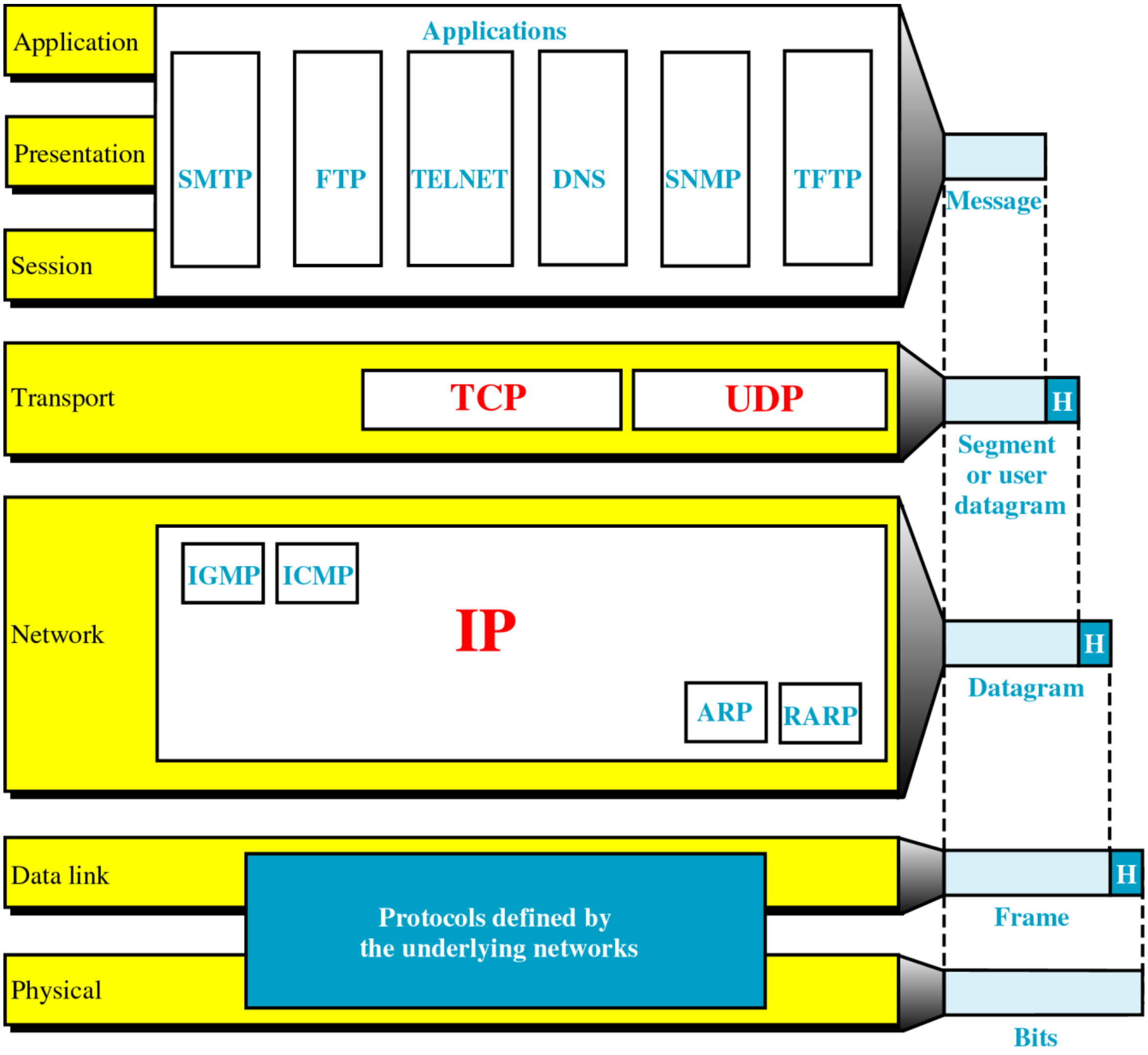
- Provides the operating system with direct access to network services.
- It serves as the interface between the user and the network by providing services that directly support user applications.


Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol
Physical layer host-router protocol



Each layer may add a Header and a Trailer to its Data (which consists of the next higher layer's Header, Trailer and Data as it moves through the layers). The Headers contain information that specifically addresses layer-to-layer communication. For example, the Transport Header (TH) contains information that only the Transport layer sees. All other layers below the Transport layer pass the Transport Header as part of their Data.

OSI vs. TCP/IP


Application
Presentation
Session
Applications
SMTP
FTP
TELNET
DNS
SNMP
TFTP
Message
Transport
TCP
UDP
H
Segment or user datagram
Network
IGMP
ICMP
IP
ARP
RARP
H
Datagram
Data link
Physical
Protocols defined by the underlying networks
H
Frame
Bits

3.1.4 Identify the technologies required to provide a VPN.

A **virtual private network (VPN)** is a technology that provides a secure and reliable private connection between computer networks over an existing public network, typically the **Internet**.

There are two components required to provide a VPN.

1. The first is a **network access server** (NAS, usually pronounced "nazz" conversationally). A NAS might be a dedicated server, or it might be one of multiple software applications running on a shared server. It's a NAS that a user connects to from the Internet in order to use a VPN. The NAS requires that user to provide valid credentials to sign in to the VPN. To authenticate the user's credentials, the NAS uses either its own authentication process or a separate authentication server running on the network.
2. The other required component of remote-access VPNs is **client software**. In other words, employees who want to use the VPN from their computers require software on those computers that can establish and maintain a connection to the VPN. Most operating systems today have built-in software that can connect to remote-access VPNs, though some VPNs might require users to install a specific application instead. The client software sets up the tunneled connection to a NAS, which the user indicates by its Internet address. The software also manages the encryption required to keep the connection secure. You can read more about tunneling and encryption later in this article.

Large corporations or businesses with knowledgeable IT staff typically purchase, deploy and maintain their own remote-access VPNs. Businesses can also choose to outsource their remote-access VPN services through an enterprise service provider (ESP). The ESP sets up a NAS for the business and keeps that NAS running smoothly.

The above information came from the howstuffworks website. It is a good article. You should read it.

http://computer.howstuffworks.com/vpn2.htm

3.1.5 Evaluate the use of a VPN.

A VPN is a way for companies to allow their employees to access company resources outside the office. The use of a VPN has led to changes in working patterns. Many companies are allowing their employees to work from home (telecommuting). While employees are traveling they can access company resources (files, application software, databases, printers).

Businesses are not the only ones that use VPNs. Many people subscribe to VPN services at home to protect their online privacy.

Data Transmission

3.1.6 Define the terms: protocol, data packet.

A **network protocol** defines rules and conventions for communication between network devices. A protocol is, in one sense, nothing more than an agreement that a particular type of data will be formatted in a particular manner. HTTP, FTP, POP3, SMTP, IMAP, TCP are all examples of network protocols.

A **data packet** contains data traveling over a network. It is a basic unit of binary data for communication over a digital network.

http://computer.howstuffworks.com/question525.htm

3.1.7 Explain why protocols are necessary.

Many protocols have been defined to assist in network communication. Some of these protocols were developed to help resolve communication problems like data integrity, flow control, deadlock, congestion, and error checking.

Define the following terms:

Data Integrity

Data integrity, in the context of networking, refers to the overall completeness, accuracy and consistency of data. Data integrity must be imposed when sending data through a network. In other words, how does a computer know that when it receives data over a network that it is complete, accurate, and consistent. This can be achieved by using error checking and correction protocols.

Flow Control

Flow control is utilized in data communications to manage the flow of data among two different network devices, especially in cases where the sending device can send data much faster than the receiver can digest.

Networks of any size have many different devices connected and each device has unique data transmission abilities. For instance, a router is built to manage the routing of data whereas a desktop, at the receiving end of that data, has far less sending/receiving abilities. These differences in sending/receiving abilities may lead to conflict if the sender starts transmitting data faster than the receiving devices's ability. To counteract this problem, a flow control protocol is used.

Xon-Xoff is an example of a flow control protocol that syncs the sender with the receiver. It transmits a transmit off signal when the receiver no longer has space in its buffer(memory) and a transmit on signal when the receiver can resume taking data.

DeadLock

Computer networks are based on passing messages from computer to computer. The computers must have a protocol established that determines the order of communication. Without a proper protocol a situation called a deadlock can occur. A **deadlock** is a situation in which two or more communicating computers are each waiting for the other to send a message, and thus neither ever does. In a networking environment, deadlocks can occur due to lost or corrupt signals during communication. A protocol must be in place to handle these types of situations or the communicating will break down.

Congestion

Network devices have a memory location called a buffer that is used to store data that has been sent to them from another source. If this buffer becomes full and cannot handle any more data a problem known as congestion occurs. **Congestion** occurs when the source sends more data than the destination can handle. When this congestion occurs performance will degrade.

When congestion occurs, the destination device has only two options with the arriving data packets, to drop them or keep them. A protocol determines whether the destination device keeps the old packets and drops the new packets or it keeps the new packets and drops the old packets. In both the cases packets are dropped.

As an example, the TCP protocol is responsible for setting the policies for congestion that occurs with packets sent over the Internet.

Error Checking

Data that is transmitted over communication lines is subject to interference (noise) which can alter the nature of the data represented. Error checking protocols exist to check such errors and, if an error is detected the network, will try to recover the data, often by requesting a resend of the data packets.

Reduncancy

The central concept in detecting or correcting errors is redundancy. A redundancy check is extra data added to a message for the purposes of error detection. Several schemes exist to achieve error detection, and are generally quite simple. All error detection codes transmit more bits than were in the original data.

The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission.

Two common schemes used in redundant error checking are **parity checking** and **check sum.**

Parity Checking

Parity Checking is one of the easiest error checking methods to implement. In this technique, a redundant bit called a parity bit is added to every data unit so that the total number of 1's in the unit (including the parity bit) becomes even (or odd).

For example, suppose a sender wants to transmit the binary data 11000001. The sender starts by adding up all of the 1 bits. Since 11000001 contains three 1's the sum is an odd number. In an even parity scheme, a parity bit of 1 would be added to the data to make it add up to four, which is an even number.

110000011

In an odd parity scheme, a parity bit of 0 would be added to the data to retain the odd numbered sum.

110000010

A parity check can detect all single-bit errors. However, if any two bits change in transmission, the changes cancel each other and the data unit will pass a parity check even though the data is damaged.

Error Checking(Continued)

Checksum

The another simple method of verifying the integrity of digitally transmitted data is the checksum method. A checksum can be computed in many different ways, using different algorithms. For example, one algorithm computes a checksum value by adding together all the numbers in the input data. If the sum of all the numbers exceeds the highest value that a checksum can hold, the checksum equals the modulus of the total--that is, the remainder that's left over when the total is divided by the checksum's maximum possible value plus 1. In mathematical terms, a checksum is computed with the equation

Checksum = Total % (MaxVal + 1)

where Total equals the sum of the input data and MaxVal is the maximum checksum value you will allow.

Suppose the data whose contents you wish to verify is the following stream of 10 byte values:

36 211 163 4 109 192 58 247 47 92

If the checksum is a 1-byte value, then it can't hold a number greater than 255. The sum of the values in the above data is 1,159, so the 8-bit checksum is the remainder left when 1,159 is divided by 256, or 135. If the sender of the data calculated a checksum of, say, 135, and the receiver got a checksum of 246, then the data was damaged during transmission.

The problem with checksums is that although conflicting checksums are proof positive that transmitted data has been damaged, matching checksums doesn't necessarily prove that the data was not altered. You can reorder the numbers in the data set any way you want and the checksum won't change. Worse, you can change individual numbers and tweak others so that the checksum comes out the same. Therefore, more advanced checksum algorithms are typically used to verify data. These include cyclic redundancy check (CRC) algorithms and cryptographic hash functions.

http://computer.howstuffworks.com/encryption7.htm

3.1.8 Explain why the speed of data transmission across a network can vary.

Data transmitted over a network is packaged and transported in small pieces of data. The flow of these small pieces of data directly affects a user's experience. When data packets arrive in a smooth and timely manner the user sees a continuous flow of data; if data packets arrive with large and variable delays between packets the user's experience is degraded.

The **latency** of a network connection represents the amount of time required for data to travel between the sender and receiver. While all computer networks possess some inherent amount of latency, the amount varies and can suddenly increase for various reasons. People perceive these unexpected time delays as lag.

Here are some causes of lag:

- Length of the route that the packets have to take between sender and receiver.
- Type of media transporting the data.(e.g. fiber optics, satellite, wireless, metal wiring)
- Network congestion - causes data to be retransmitted.
- Traffic load - how many people are using network.
- Time of day - people use network more during peek times.
- Weather - satellite and wireless signal interference.

3.1.9 Explain why compression of data is often necessary when transmitting across a network.

Data compression is the process of encoding data to take up less storage space and less bandwidth for transmission. Digital data are compressed by finding repeatable patterns of binary 0s and 1s. The more patterns can be found, the more the data can be compressed. Text can typically be compressed to approximately 40% of its original size, and graphics files from 20% to 90%. Some files compress very little. It depends entirely on the type of compression algorithm used. As an example, the zip file format utilizes a common compression algorithm.

Data compression has enabled information to be disseminated more rapidly.

3.1.10 Outline the characteristics of different transmission media.

	Metal Conductor	Fiber Optics	Wireless
Description	Twisted Pair Cable Made of copper	Made of glass or plastic	Radio waves
Speed	CAT 5 - 100 Mbps to 1 Gbps	10 Gbps	Theoritical Speeds -------------------- 802.11b - 11 Mbps 802.11g - 54 Mbps 802.11n - 600 Mbps 802.11ac - 1300 Mbps Actual Speeds -------------------- 802.11b - 2-3 Mbps 802.11g - 20 Mbps 802.11n - 40-50 Mbps 802.11ac - 70-100 Mbps
Reliability	Extremely reliable, however, signal can only travel 1.2 miles before it needs to be regenerated or boosted.	Signal can travel 62 miles before it needs to be regenerated or boosted.	Somewhat reliable. Signal strength depends on hardware. On average a Wi-Fi signal can travel about 65 feet indoors. The disparity between theoretical and practical Wi-Fi performance comes from network protocol overhead, radio interference, physical obstructions on the line of sight between devices, and distance between devices. In addition, as more devices communicate on the network simultaneously, its performance will also decrease.
Cost	cheapest	most expensive	cost more than cooper but less than fiber
Security	Secure	More secure than copper	Potentially not as secure as wired media because signal travels through air. However, if proper authentication, encryption, and access control practices are followed it is very secure.

3.1.11 Explain how data is transmitted by packet switching.

Packet switching is a network technology that breaks up a message into smaller chunks (packets) for transmission. Unlike circuit switching in traditional telephone networks, which requires the establishment of a dedicated point-to-point connection, each packet in a packet-switched network contains a destination address. Thus, all packets in a single message do not have to travel the same path. As traffic conditions change, they can be dynamically routed via different paths in the network, and they can even arrive out of order. The destination computer reassembles the packets into their proper sequence.

Below are the steps used to send packets over a network using packet switching:

1. The sending computer chops data into small packets, with an address on each one telling the network devices where to send them.
2. Each packet is assembled with a small piece of an e-mail, music file or whatever type of file is being transmitted inside the packet.
3. The sending computer sends the packet to a nearby router and forgets about it. The nearby router sends the packet to another router that is closer to the recipient computer. That router sends the packet along to another, even closer router, and so on.
4. When the receiving computer finally gets the packets (which may have all taken completely different paths to get there), it uses instructions contained within the packets to reassemble the data into its original state.

Packet switching is very efficient. It lets the network route the packets along the least congested and cheapest lines. It also frees up the two computers communicating with each other so that they can accept information from other computers, as well.

Transport Control Protocol/Internet Protocol (TCP/IP) is an example of a packet switching protocol. Some mobile phone technologies also use packet switching technologies.

Wireless Networking

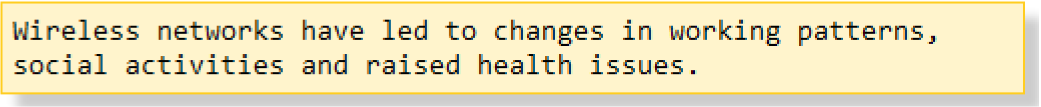
3.1.12 Outline the advantages and disadvantages of wireless networks.

Advantages of wireless networks

- **Convenience** - The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (a home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
- **Mobility** - With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
- **Productivity** - Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
- **Deployment** - Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
- **Expandability** - Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
- **Cost** - Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

Disadvantages of wireless networks

- **Security** - To combat security issues, wireless networks may choose to utilize some of the various encryption technologies available. Some of the more commonly utilized encryption methods, however, are known to have weaknesses that a dedicated adversary can compromise. Novice home users may make themselves vulnerable by not utilizing proper security precautions when setting up a wireless network at home.
- **Range** - The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly.
- **Reliability** - Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference.
- **Speed** - The speed on most wireless networks (typically 1-54 Mbps) is far slower than even the slowest common wired networks (100Mbps up to 1 Gbps).



Wireless networks have led to changes in working patterns, social activities and raised health issues.

3.1.13 Describe the hardware and software components of a wireless network.

Hardware

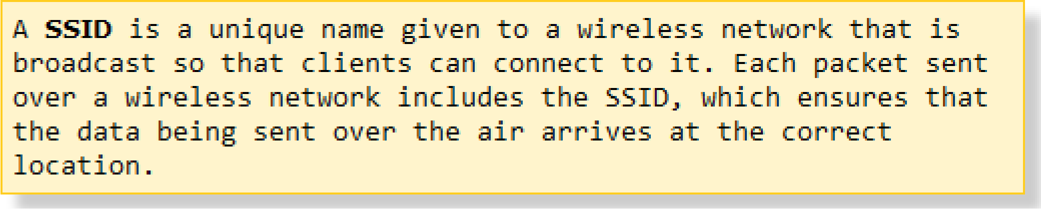
- **Wireless router** - A router is network device that determines where data packets should go and sends them to their destination by the shortest, most efficient route. A **wireless router** is a router that uses radio waves to transmit data.

- **Wireless adapter** - A wireless network adapter connects a computer to a wireless network so that they can communicate. Virtually all laptop and smaller computing units come with a built-in wireless adapter. If you want to convert your desktop computer to a wireless unit, you have to obtain a wireless adapter. The adapter slips into a slot inside the computer, with an antenna that projects out the back of the computer. You can also buy adapters that plug into a usb port.

- **Extender** - Wireless networks have a finite range. If you find that your signal is not strong enough to cover the areas you want, a wireless extender can fix the problem. A wireless extender captures the router signal and rebroadcasts it. Plug your extender into a wall socket about halfway between the router and where you are having difficulty picking up the wireless signal.

Software

Router Software - routers contain built-in software that can be accessed using any web browser software. This software is used to configure the router. You can perform tasks like assigning a router's SSID and setting security and firewall parameters.



A **SSID** is a unique name given to a wireless network that is broadcast so that clients can connect to it. Each packet sent over a wireless network includes the SSID, which ensures that the data being sent over the air arrives at the correct location.

http://www.howstuffworks.com/wireless-network1.htm

3.1.14 Describe the characteristics of wireless networks.

Question: Describe the characteristics of the following wireless networks: WIFI, WIMAX, LTE, and LTE-Advanced.

WiFi

- Wireless network that uses radio waves to transmit and receive data.
- Effect range relatively short, about 65 ft.
- Currently has higher average data speeds compared to other wireless network technologies (WiMax, LTE).
- Speed is effected by interference and distance from router.
- Easy setup.

WiMax (Worldwide Interoperability for Microwave Access)

- It is similar to Wi-Fi, but it can enable usage at much greater distances.

- Provides a wireless alternative to cable, DSL, and satellite Internet service. It is essentially a wireless broadband.

- ISPs can deliver Internet connections without running expensive cables to every home, and speeds often run between 5-10Mbps.

- Primarily due to its much higher cost, WiMAX is not a replacement for Wi-Fi home networking or Wi-Fi hotspot technologies.

- Current WiMax availability is limited.

- WiMax lost out to the competing LTE technology in the cell phone industry.

http://computer.howstuffworks.com/wimax1.htm

LTE (Long Term Evolution)

- Technology adopted by majority of mobile carriers.
- Uses packet switching technology for both data and voice.
- Capable of 300Mbps download speeds and 75Mbps upload speeds.
- Most 4G networks use this technology.

3G mobile

- "3rd Generation" cell phone technology first avaliable in cell phones in 2003.
- Depending upon carrier 3G networks use either EDGE, EV-DO or HSPA data protocols.
- Speeds range between 400 kilobits and 2Mbps, depending on the carrier and region.

4G mobile

- "4rd Generation" cell phone technology first avaliable in cell phones in 2008.
- Depending upon carrier 4G networks use either Wi-Max, HSPA+ or LTE data protocols.
- Most carriers have moved or are moving to LTE.
- Speeds currently range between 3.5Mbps and 19Mbps, depending on the carrier and region.
- There is currently very little standardization in 4G technologies. In some cases, one company's 4G speeds could be inferior to another carrier's older 3G network.

Future Networks

- **LTE-Advanced (Long Term Evolution-Advanced)** is the next generation cellular networking standard that offers higher throughput than its predecessor, LTE standard.
- LTE-Advanced networks can deliver up to 1 GBps of data, compared to a maximum of 300 MBps over LTE networks.
- Uses multiple-input, multiple-output (MIMO) technology to deliver data faster via more than one signal. MIMO requires multiple antennas to receive those signals, which can limit its use in compact mobile devices such as smartphones and tablets.

3.1.15 Describe the different methods of network security.

There are several methods used to provide security for a wireless networking. The most common ones are encryption, authentication, and MAC address filtering.

Encryption

Encryption is the process of encoding data sent wirelessly between your device and the router, essentially scrambling the information and restricting open access. There are three main types of encryption: WEP, WPA, and WPA2.

- **Wired Equivalent Privacy (WEP)** - is an older network security method from the late 1990's that is still available to support older devices, but it is no longer recommended. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

- **Wi-Fi Protected Access (WPA)** - first used in 2003 to improve on or replace the flawed WEP encryption. WPA provides much stronger encryption than WEP and addresses a number of WEP weaknesses.

- **WPA2** - in 2006 WPA2 replaced WPA to again improve security by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations) in the original WPA implementation. WPA2 uses the AES (Advanced Encryption Standard), which provides government-grade encryption capabilities that are stronger than the TKIP (Temporal Key Integrity Protocol) used by WPA. In fact, AES is thought to be uncrackable by even the most skilled hacker.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In a wireless network authentication is commonly done through the use of logon passwords or passphrases.

WPA/WPA2 utilize two different protocols for network authentication.

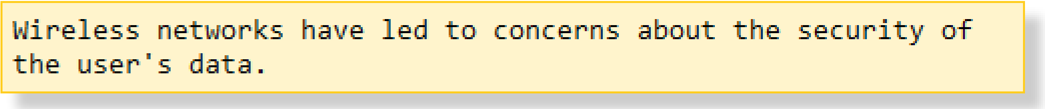
- **WPA2-PSK** is intended for home and very small office networks. Each wireless device is authenticated by the same 256-bit key. With this mode, you set an encryption passphrase that must be entered by each user when connecting to the network. This passphrase can be stored on each computer, but it must be entered for each device. All users share a locally stored passphrase, which can be found and copied from a computer by anyone. This makes WPA2-PSK less secure than the WPA2-ENT mode.

- **WPA2-ENT** is made for the enterprise network, but it's a smart choice for any business network. It provides security against more attacks than WPA2-PSK and separates users from the router's passphrase to the network. WPA2-ENT creates new encryption keys each time users log on to the network with their unique passwords, and the passphrase to the network is not stored locally. It also allows for centralized control over users' access to the wireless network, which makes management easier than with the WPA2-PSK mode.

MAC address filtering.

A MAC address (Media Access Control address) is a unique identifier assigned to a network adapter by the manufacturer for identification.

MAC address filtering allows only machines with specific MAC addresses access to a network. You specify which addresses are allowed in the router software.



Wireless networks have led to concerns about the security of the user's data.

3.1.16 Evaluate the advantages and disadvantages of each method of network security.

[Question: Evaluate the effectiveness of encryption, authentication, and MAC address filtering as they relate to wireless networking.]

MAC Address filtering will discourage the casual user from accessing your network but it will do very little to deter knowledgeable hackers who can use software to scan for MAC Addresses of legitimate devices currently accessing your network and then spoof their own MAC into a validated one.

The best way to secure a wireless network is combine both encryption and authentication technology using the WPA2 standard. However, for authentication to be effective a **strong password** must be used.

http://ipoint-tech.com/wireless-networking-wi-fi-advantages-and-disadvantages-to-wireless-networking/
http://networking.answers.com/wifi/necessary-hardware-for-a-wireless-network

Vocabulary

address
authentication
compression
conductor
congestion
construction
data
deadlock
encryption
error
fiber
filtering
flow
LAN

layers
lte
mac
MAN
media
mobile
model
network
networking
networks
optics
OSI
P2P
packet
PAN
protocol

SAN
standards
switching
VLAN
VPN
WAN
wifi
wimax
wireless

Question Banks

Formative Assessments (Quizzes)

1. Describe the following networks: LAN, WAN, VLAN, SAN, VPN, PAN, AND P2P.
2. Vocabulary Quizzes
    a. Network Fundamentals
        i. standard
        ii. protocol
    b. Data Transmission
        i. data packet
        ii. data integrity
        iii. flow control
        iv. deadlock
        v. congestion
        vi. error checking
        vii. packet switching
    c. Wireless Networks
        i. hardware components
        ii. software components
        iii. WIFI
        iv. WIMAX
        v. LTE
        vi. LTE-Advanced
        vii. encryption
        viii. authentication
        ix. MAC address filtering
3. Differentiate between standards and protocols
4. Identify the technologies required to provide a VPN.
5. Outline the characteristics of different transmission media
6. Outline the advantages and disadvantages of wireless networks.
7. Identify the hardware and software components of a wireless network.
8. Describe the characteristics of the following wireless networks: WIFI, WIMAX, LTE, and LTE-Advanced.
9. What are 3G and 4G mobile networks? What about 5G Networks?
10. Describe encryption, authentication, and MAC address filtering.

Summative Assessments (Test Question Bank)

Network Fundamentals

1. Outline the importance of standards in the construction of networks
2. Explain why protocols are necessary
3. What is the purpose of the OSI Model?
4. Draw a diagram of the OSI Model showing how data flows through the seven layers
5. Evaluate the use of a VPN.

Data Transmission

6. Explain why the speed of data transmission across a network can vary
7. Explain why compression of data is often necessary when transmitting across a network
8. Evaluate the use of a VPN
9. Explain how data is transmitted by packet switching

Wireless Networking

10. Evaluate the effectiveness of encryption, authentication, and MAC address filtering as they relate to wireless networking
11. Evaluate the effectiveness of encryption, authentication, and MAC address filtering as they relate to wireless networking.

References

- Networking topic resources : http://bwagner.org/
- Networking topics and activities: http://hwmath.net/IBCS/
- VPN: http://computer.howstuffworks.com/vpn2.htm
- MAN: http://searchnetworking.techtarget.com/definition/metropolitan-area-network-MAN
- Andrew S. Tanenbaum – Computer Networks, ISBN: 0-13066102-3
- J Glenn Brookshear "Computer Science – An Overview", ISBN: 0-321-54428-5
- Eugene Blanchard "Introduction to Networking and Data Communications"
- Computer Science Illuminated, Nell B. Dale, John Lewis, 4th Edition
- http://www.ehow.com/facts_7351195_network-protocols-important_.html
  http://www.netguru.net/ntc/NTCC6.htm
  http://www.webopedia.com/quick_ref/OSI_Layers.asp
  http://computer.howstuffworks.com/osi.htm
  http://computer.howstuffworks.com/vpn2.htm
- Network Services at Suffolk University, Boston:
  http://www.suffolk.edu/explore/52725.php

INDEX

Matching

Topology	Network Type	Network Architecture	OSI Model	Protocol
Mesh	VPN	Ethernet	Data Link Layer	FTP
Bus	WAN	Token Ring	Transport	HTTP
Star	Metropolitan Area Network			

HTTP

Star