Networking

Table of Contents

Update Notes

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.

Question: Describe the following 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.

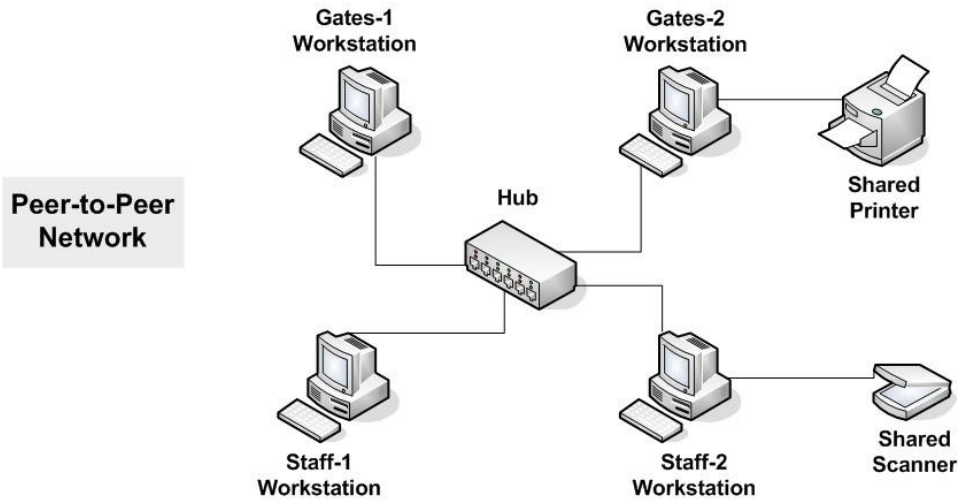
Peer to Peer Network P2P

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.

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.

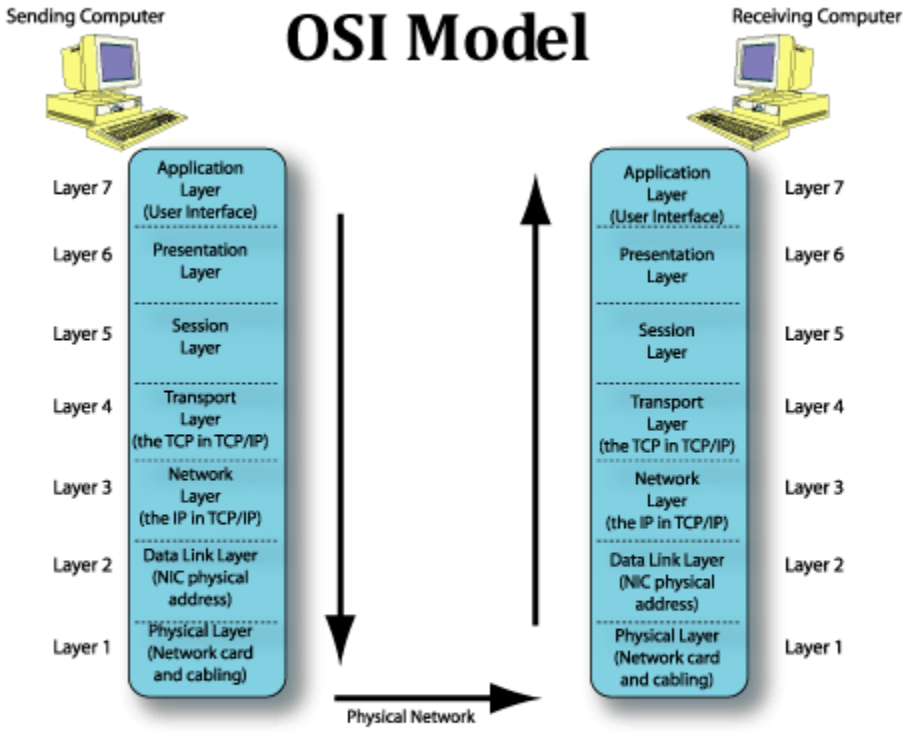
```
Interoperability - The ability of software and hardware on
multiple machines and from multiple commercial vendors to
communicate.
```

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.

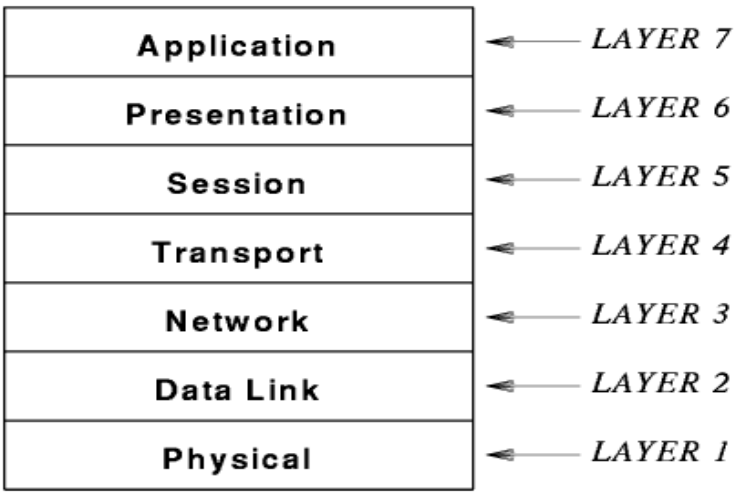
The illustration below shows the flow of data from one computer to another through a network that uses the ISO standard.



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***

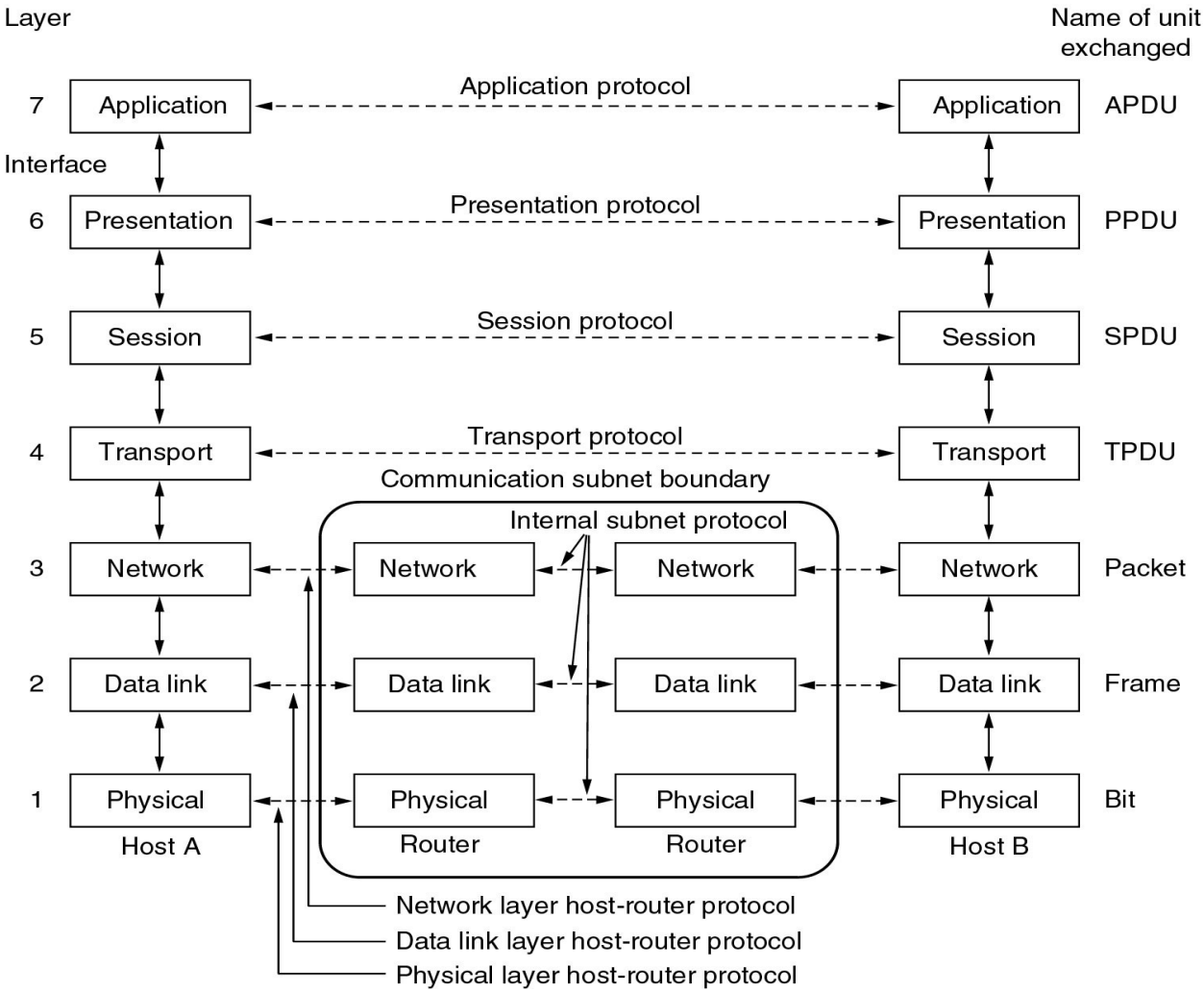
- Is responsible for establishing, maintaining, and terminating a connection called a 'session'.
- A session is an exchange of messages between computers (a dialog). Managing the session involves synchronization of user tasks and dialog control (e.g., who transmits and for how long). Synchronization 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.

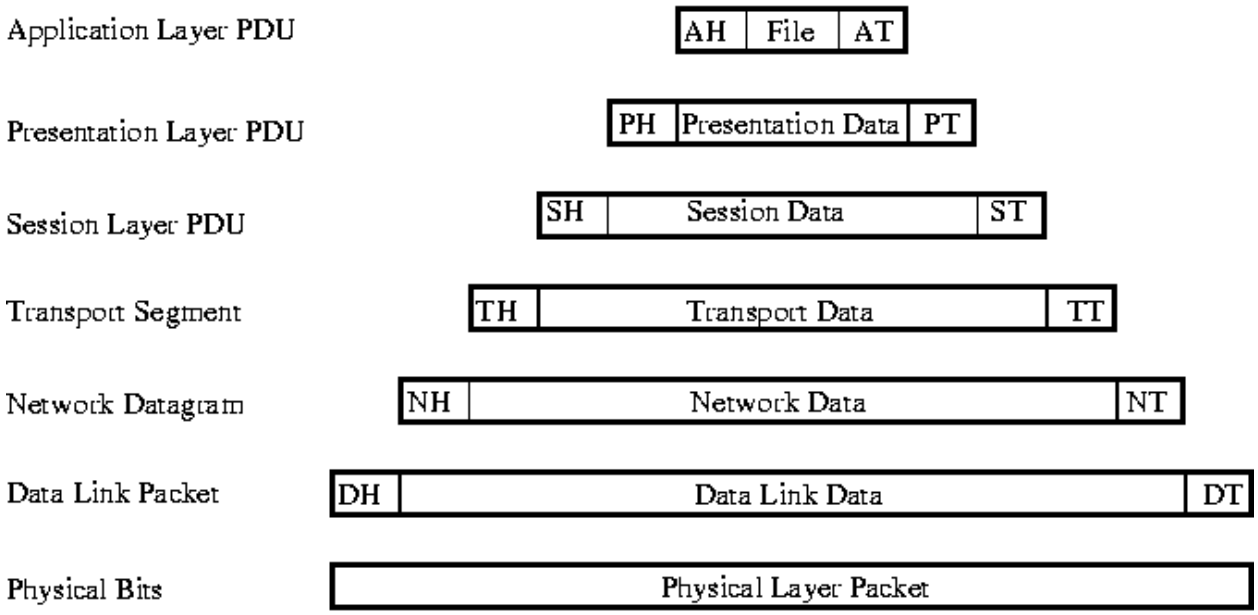
The ***Presentation Layer***

- 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***

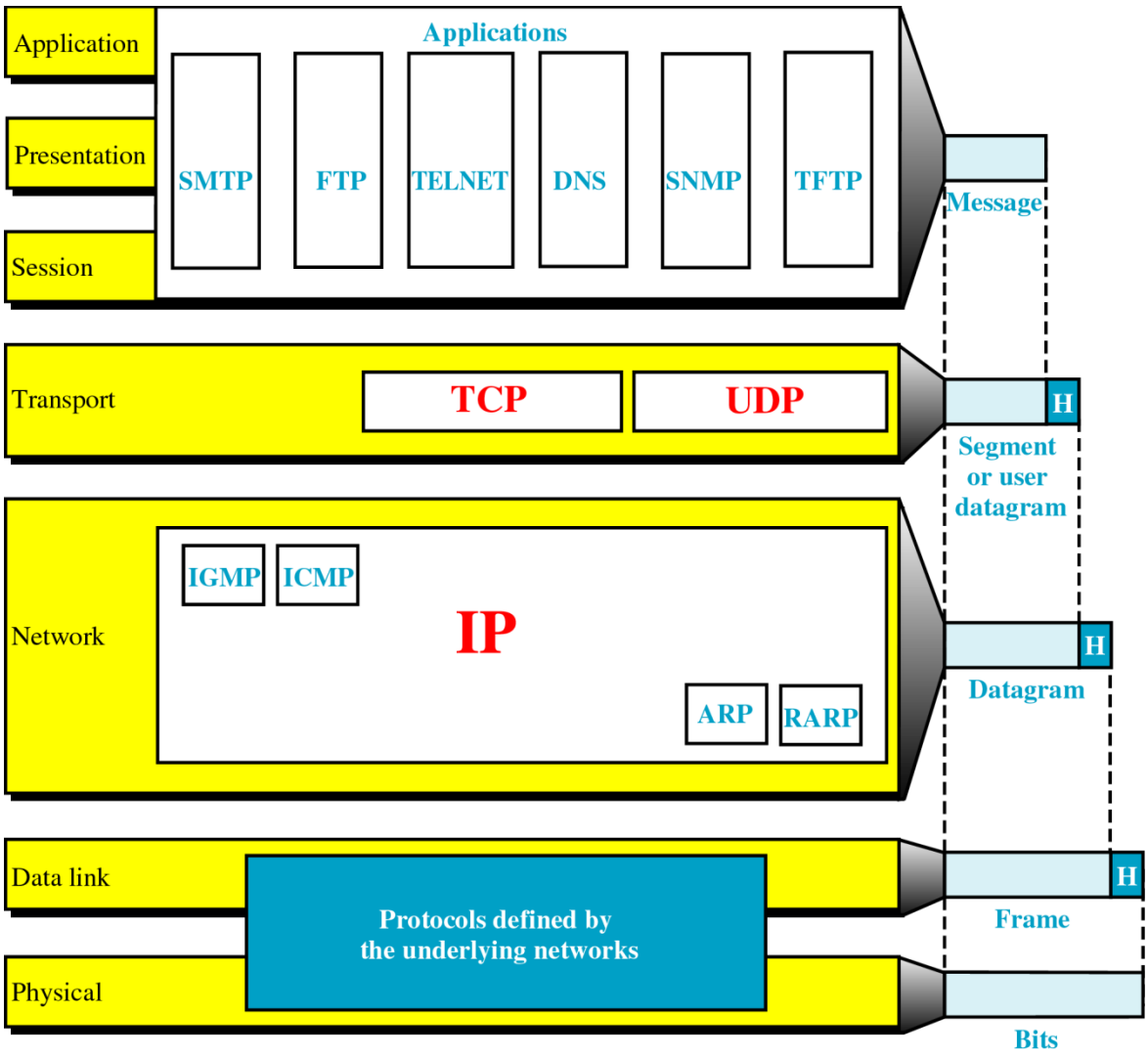
- Provides the operating system with direct access to network services.
- It serves as the interface between the user and the network by providing services that directly support user applications.


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
Protocols defined by
the underlying networks
H
Frame
Physical
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.

3.1.7 Explain why protocols are necessary.

Define the following terms:

data integrity

flow control

deadlock

congestion

error checking

Question: Explain why protocols are necessary.

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

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

.

3.1.10 Outline the characteristics of different transmission media.

	Metal Conductor	Fiber Optics	Wireless
Speed			
Reliability			
Cost			
Security			

3.1.11 Explain how data is transmitted by packet switching.

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).

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

3.1.14 Describe the characteristics of wireless networks.

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

Question: What are 3G and 4G mobile networks?

3.1.15 Describe the different methods of network security.

Question: Describe encryption, authentication, and MAC address filtering.

encryption

authentication

MAC address filtering.

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.

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

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