جامعة الأهرام الكندية
AHRAM CANADIAN UNIVERSITY

Lecture (02)
Network
Protocols and Standards

Dr. Ahmed M. ElShafee

Agenda

- -
- -

Preface

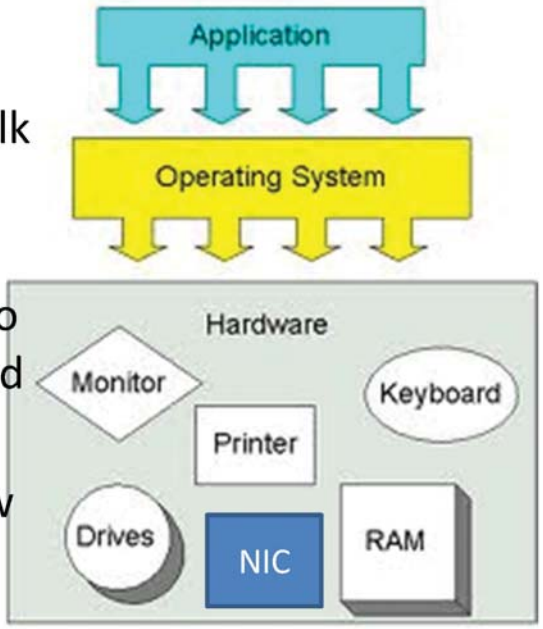
- Protocols and standards are what make networks work together.
- Protocols make it possible for the various components of a network to communicate with each other.
- Standards also make it possible for network components manufactured by different companies to work together.

Understanding Protocols

- A *protocol is a set of rules that enables effective communications to occur.*
- You encounter protocols every day: making a phone call
  - When you pick up a phone, you must listen for a dial tone before dialing the number. If you don't hear a dial tone, you know that either
    - (1) someone else in your family is talking on the phone
    - (2) something is wrong with your phone.
  - When you hear the dial tone, If the person you want to call is in the same area code as you, simply dial that person's digit phone number.

- If the person is in a different area code, you dial the area code, and the person's digit phone number.
- If you hear a series of long ringing tones, you wait until the other person answers the phone.
- If you hear a series of short tones, you know the other person is talking to someone else on the phone. So you hang up and try again later.
- If the phone rings a certain number of times with no answer, you hang up and try again later.
- If you hear a voice say, "Hello," you begin a conversation with the other party.

- Computer networks depend upon many different types of protocols in order to work.
  - Network cards must know how to talk to other network cards in order to exchange information,
  - operating systems must know how to talk to network cards in order to send and receive data on the network
  - and application programs must know how to talk to operating systems in order to know how to retrieve a file from a network server.



- ***Types of Protocols***
- At the lowest level, protocols define the type of electrical signal represents a ones and zeros.
- At the highest level, protocols defines how a computer user in United States can send an e-mail to another computer user in New Zealand.
- And in between are many other levels of protocols

- ***Protocol suits:***
- Various protocols tend to be used together in matched sets called *protocol suits.*
- *The two most popular protocol suits for networking are* ***TCP/IP*** *and* ***Ethernet****.*
- ***TCP/IP*** was originally developed for Unix networks and is the protocol of the Internet and most local-area networks
- ***Ethernet*** is a low level protocol that defines the electrical characteristics of the network hardware used by most local-area networks.

- A third important protocol is ***IPX/SPX****, which is an alternative to TCP/IP that was originally developed for* ***NetWare*** networks.
- In the early days of networking, IPX/SPX was widely used in local area networks, but TCP/IP is now the preferred protocol

Understanding Standards

- In the early days of computer networking, each computer manufacturer developed its own networking protocols.
- As a result, equipment s from different manufacturers can't work on a single network.
- Then along came standards to save the day.
- With standard protocols, different equipments from different manufacturer can work together in single network.
- organizations are involved in setting standards for networking.
  - **American National Standards Institute (ANSI) (USA)**
  - **Institute of Electrical and Electronics Engineers (IEEE) (**international organization**)**

- **International Organization for Standardization (ISO): (**international organization**)**
  - **Internet Engineering Task Force (IETF):** The organization responsible for the protocols that drive the Internet.
  - **World Wide Web Consortium (W3C):** An international organization that handles the development of standards for the World Wide Web

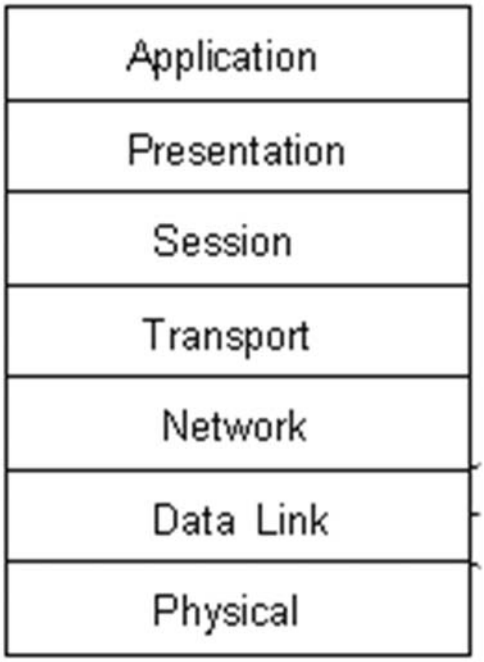
The Seven Layers of the OSI Reference Model

- Open Systems Interconnection Reference Model, affectionately known as the *OSI model.*
- The OSI model breaks the various aspects of a computer network into seven distinct layers.
- These layers are kind of like the layers of an onion: Each successive layer envelops the layer beneath it, hiding its details from the levels above.

- The OSI model is not a networking standard, it's a framework into which the various networking standards can fit
- the OSI model is sort of a standard of standards.

Layer	Name	Description
1	Physical	Governs the layout of cables and devices such as repeaters and hubs.
2	Data Link	Provides MAC addresses to uniquely identify network nodes and a means for data to be sent over the Physical layer in the form of packets. Bridges and switches are layer 2 devices.
3	Network	Handles routing of data across network segments.
4	Transport	Provides for reliable delivery of packets.
5	Session	Establishes sessions between network applications.
6	Presentation	Converts data so that systems that use different data formats can exchange information.
7	Application	Allows applications to request network services.

- The first three layers are sometimes called the *lower layers.*
- *They deal with* the mechanics of how information is sent from one computer to another over a network.



- Layers 4 through 7 are sometimes called the *upper layers.*
- They deal with how application software can relate to the network through application programming interfaces.

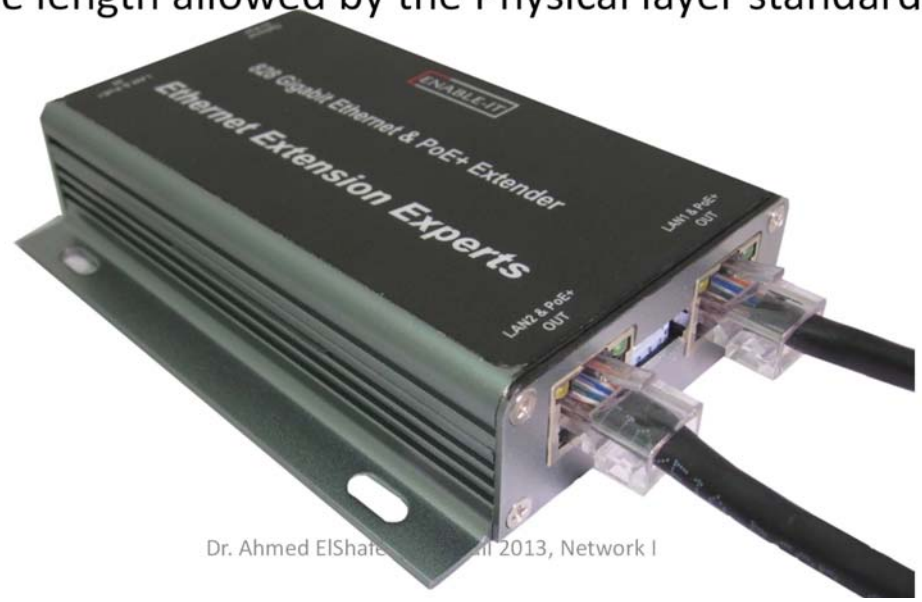
1. The Physical Layer

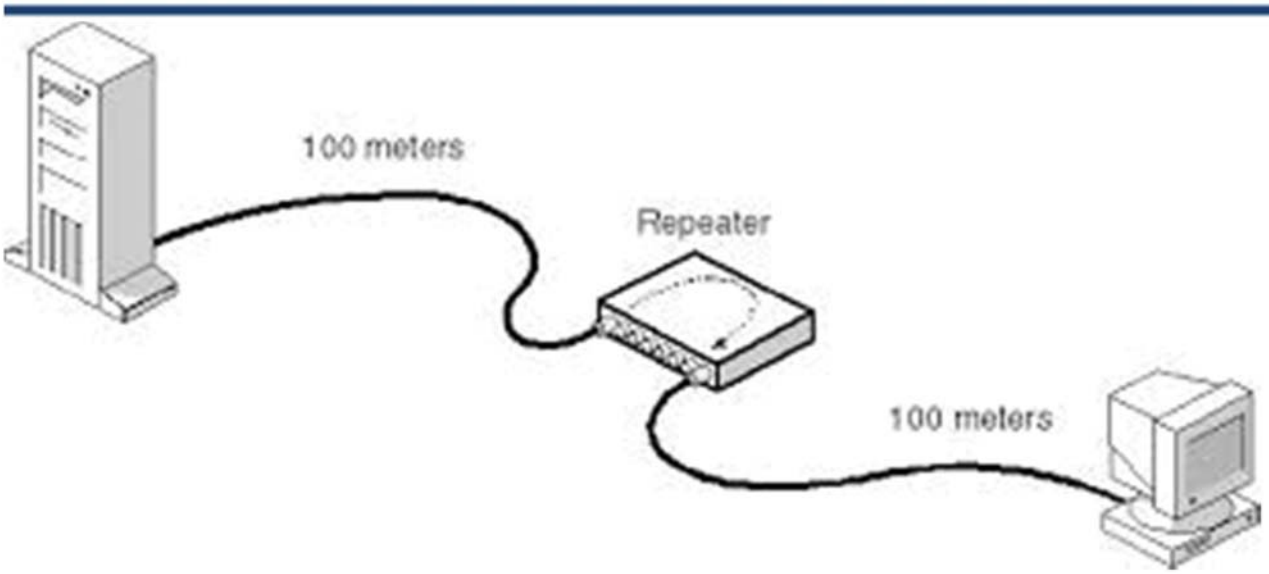
- addresses the physical characteristics of the network, like;
  - types of cables
  - types of connectors used,
  - how long the
  - network topologies like star, bus, ring, and mesh
  - electrical characteristics of the signals used to transmit data

Network Cable

- networks are constructed using a type of cable called *twisted-pair* cable, which looks a little like phone cable but is little different.
- other types of cable; coax cable, fiber-optic cables that span long distances at high speeds,

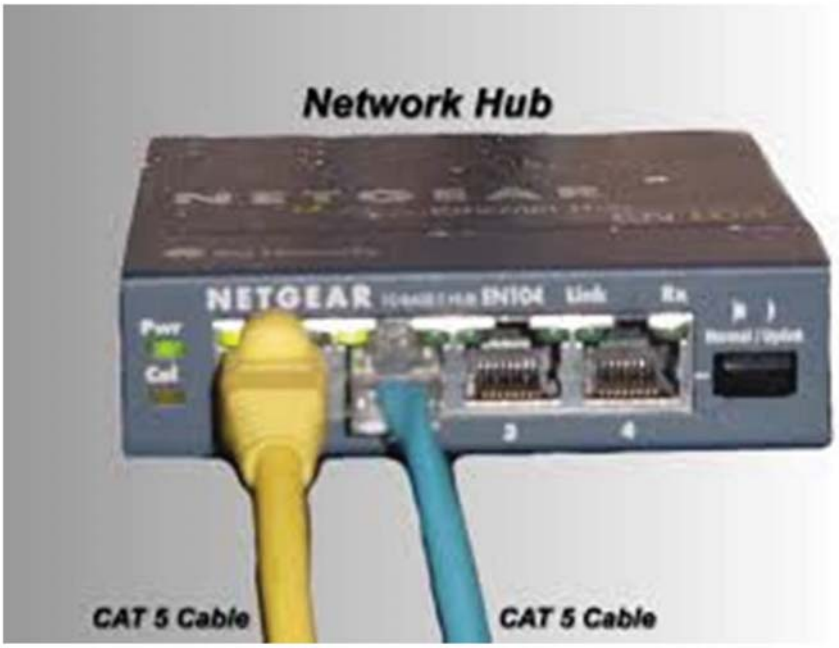
- ***repeater s***
- Example of a Physical layer device is a *repeater.*
- A repeater is used to regenerate the signal is the cable exceed the cable length allowed by the Physical layer standard





- **Hubs**
- Hubs are also Physical layer devices.
- Technically, they're known as *multiport repeaters* because the purpose of a hub is to regenerate every packet received on any port on all of the hub's other ports
- Repeaters and hubs don't examine the contents of the packets that they regenerate

-



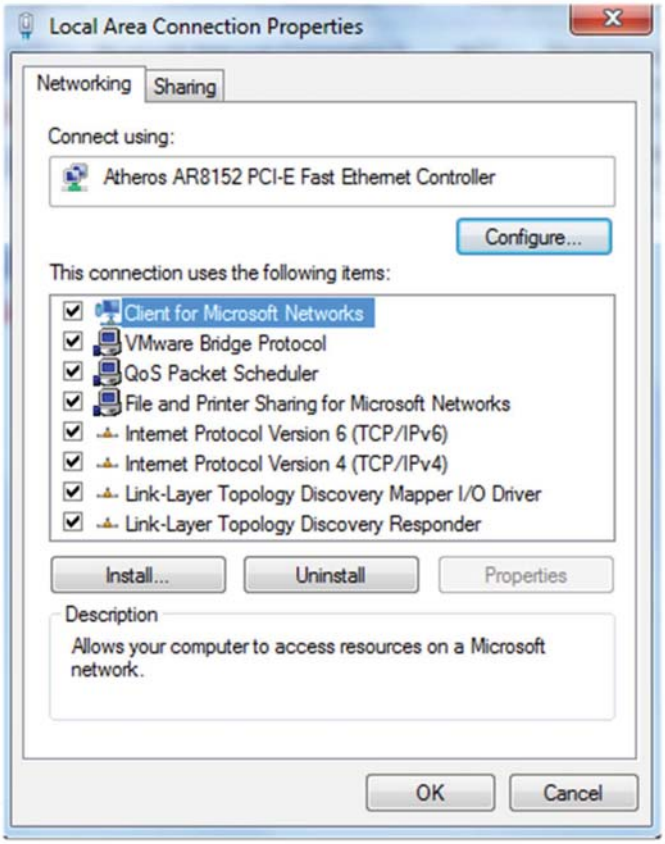
2. The Data Link Layer

- Data link protocols address things like
  - the size of each packet of data to be sent, a
  - addressing each packet so that it's delivered to the intended recipient,
  - Traffic management, make ensure that nodes don't try to transmit data on the network at the same time, and if so nodes detect error and recover it.

- basic error detection and correction to ensure that the data sent is the same as the data received
- If an uncorrectable error occurs, the data link standard specify how the node is to be informed of the error so that it can retransmit the data.

- ***network adapter***
- called a *network interface card or NIC*
- installed in each computer on the network
- You can display information about the network adapter (or adapters) installed in a Windows computer by displaying the adapter's Properties dialog box,

- To access this dialog box in Windows 7 or Vista,
  - open the Control Panel,
  - choose Network and sharing Center,
  - choose Change Adapter Settings.
  - Then, right-click the Local Area Connection icons and
  - choose Properties from the menu that appears.

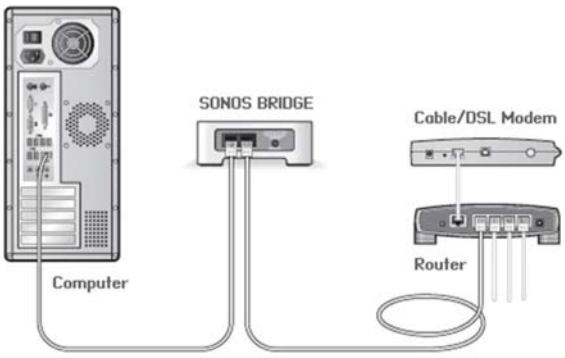


- ***MAC address***
- At the Data Link layer, each device on the network has an address known as the *Media Access Control (MAC) address.*
- MAC is hard-wired into every NIC by manufacturer
- MAC is unique per NIC

- You can see the MAC address for a computer's network adapter by opening a command window and running the ipconfig /all command

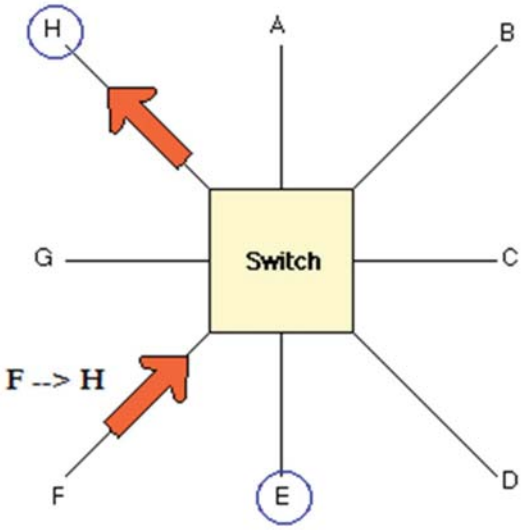
```
Administrator: C:\Windows\system32\cmd.exe

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11n Network Adapter
   Physical Address. . . . . . . . . : E8-39-DF-95-C6-F0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d5d:1de3:52cc:6c29%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 ??????, 2013 05:13:41 ?
   Lease Expires . . . . . . . . . . : 09 ??????, 2013 05:13:43 ?
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 384317919
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-14-AE-79-BF-00-26-6C-7E-A3-50

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

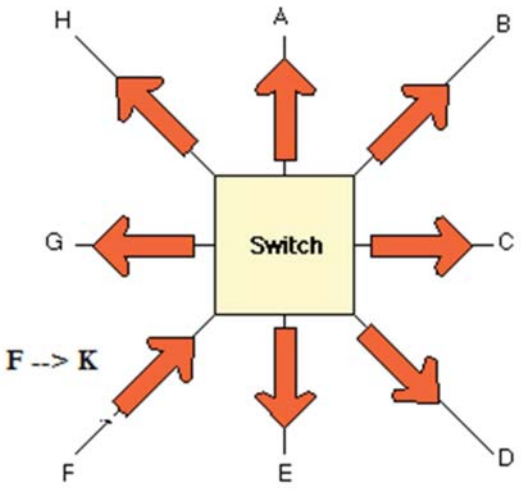
- ***Data Link layer devices***
  - bridges
  - Switches
- A *bridge* is an intelligent repeater that is aware of the MAC addresses of the nodes on either side of the bridge and can forward packets accordingly.



- A *switch* is an intelligent hub that examines the MAC address of arriving packets in order to determine which port to forward the packet to.

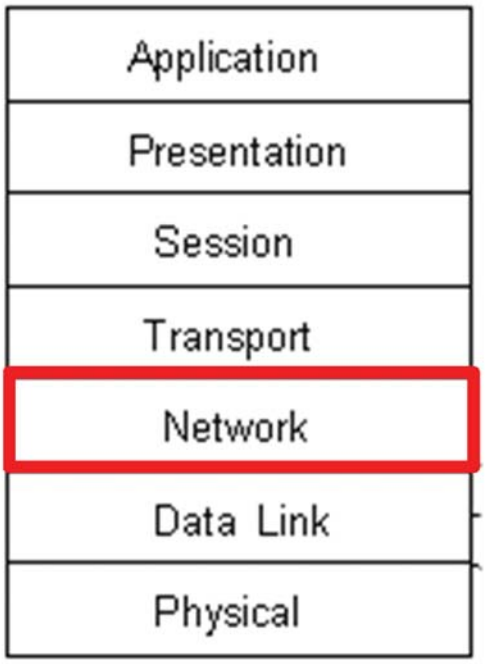
- Switch recognize the MAC address of devices connected to its ports.
- When a packet is received by switch port, switch can recognize the destination of packet.
- Switch search its MAC address table, if the machine is connected to one of its port, it directed that packet to destination machine only. If not, it broadcast packet to all ports.
- So it's some time called switching hub.





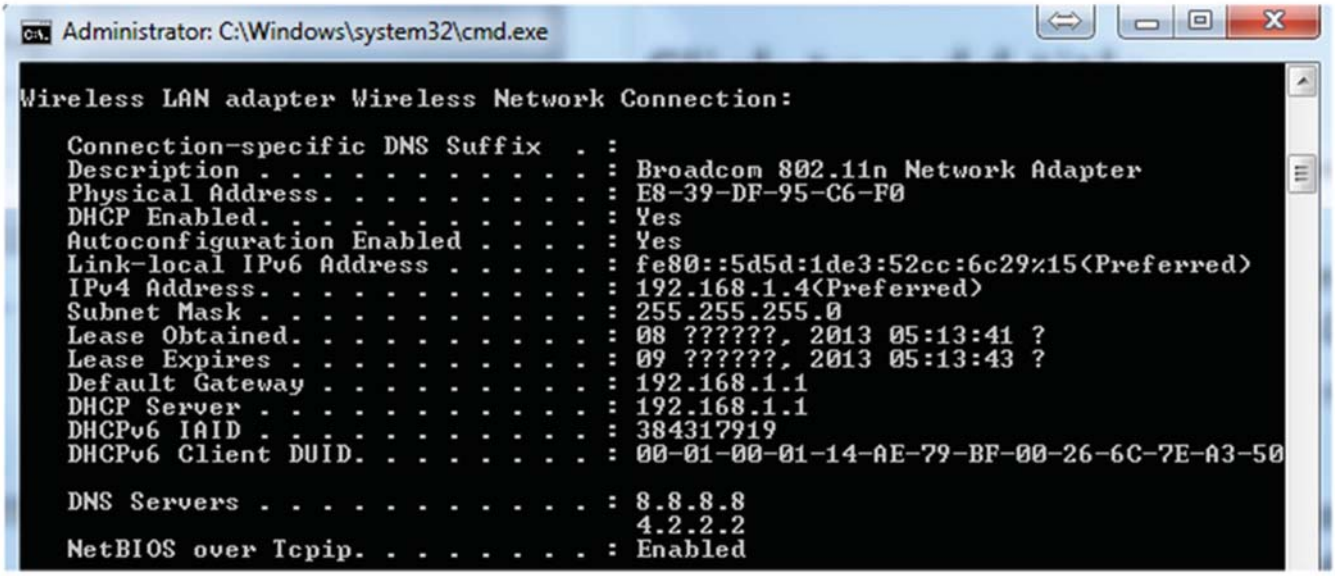
3. The Network Layer

- handles the logical address and routing network messages from one computer to another.
- The two most popular layer 3 protocols are
  - IP (which is usually paired with TCP)
  - IPX (normally paired with SPX for use with Novell and Windows networks).

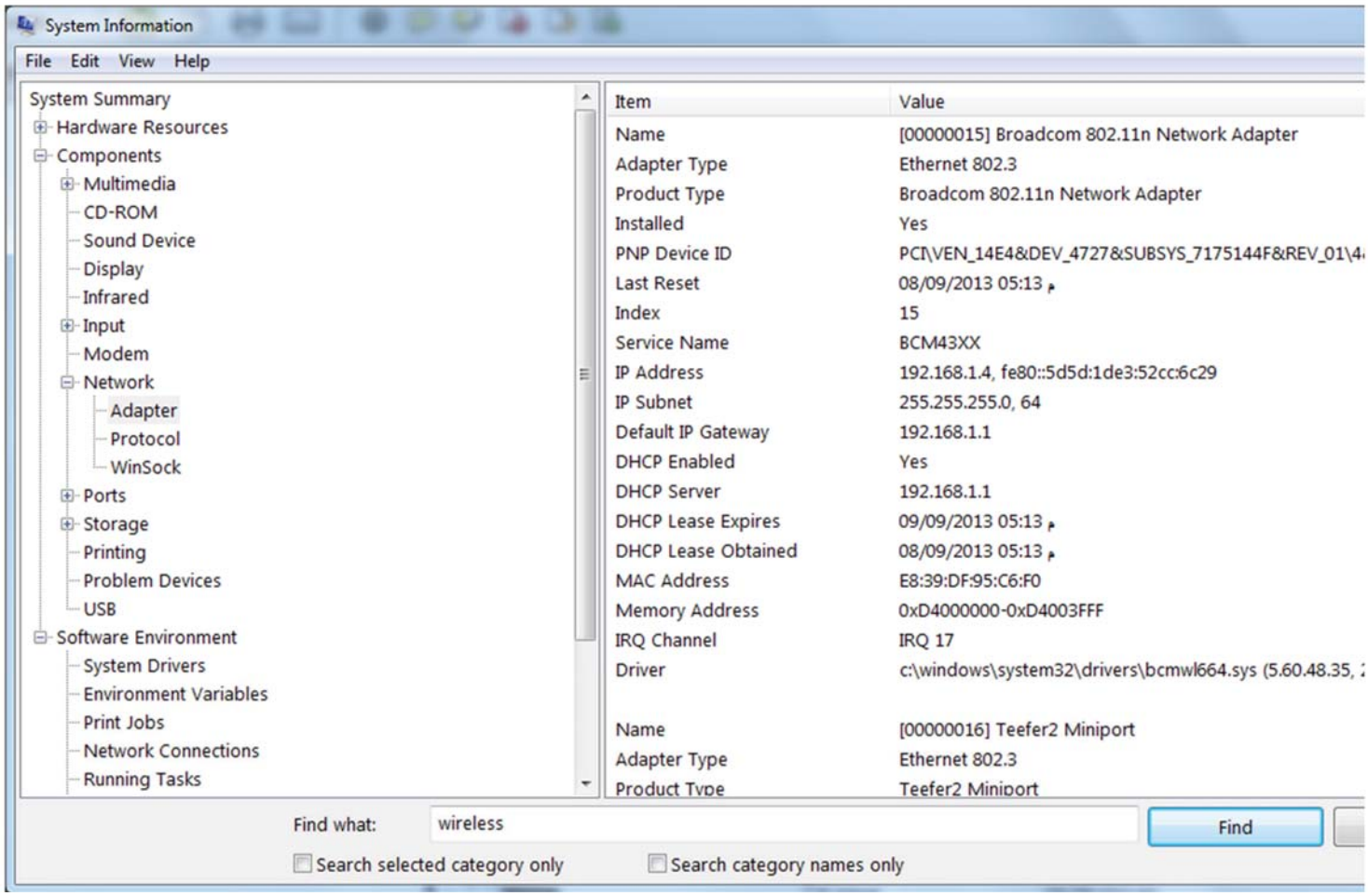


- **Logical addressing**
- logical address lets you access a network device by using an address that you assign.
- Logical addresses are created and used by Network layer protocols such as IP or IPX.
- The Network layer protocol translates logical addresses (IP address) (PC) to MAC addresses (NIC).
- if you use IP as the Network layer protocol, devices on the network are assigned IP addresses such as 192.168.1.2 (PC).
- Because the IP protocol use a Data Link layer protocol to actually send packets to devices (NIC), IP must know how to translate the IP address of a device to the device's MAC address.

- You can use the ipconfig command to know the IP address of your computer.

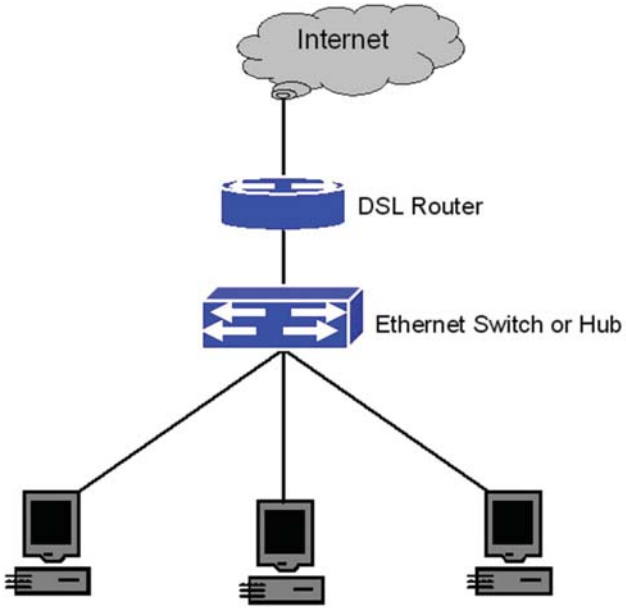


- Another way to display this information is to use the System Information command
  - Start ➪ System Information.
  - Components ➪ Network ➪ Adapter

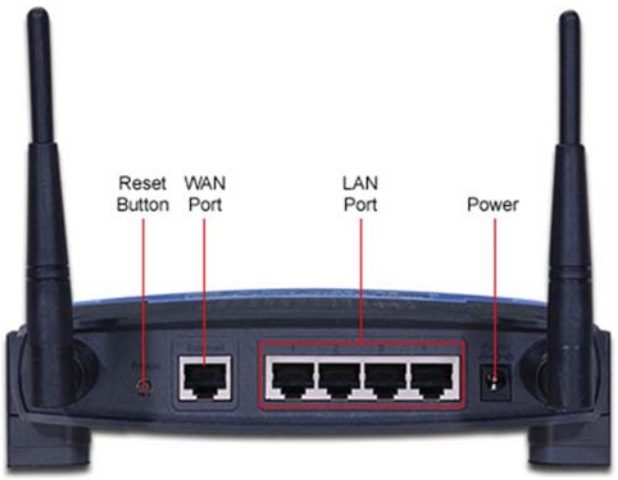


- most protocols divide the logical address into two parts:
  - a network address
  - and a device address.
- For example, in a typical IP address, such as 192.168.1.102, the network address is 192.168.1, and the device address (called a *host address* in IP) is 102.
- In an IPX address, the node address is the same as the MAC address.
- As a result, IPX doesn't have to translate between layer 3 and layer 2 addresses.

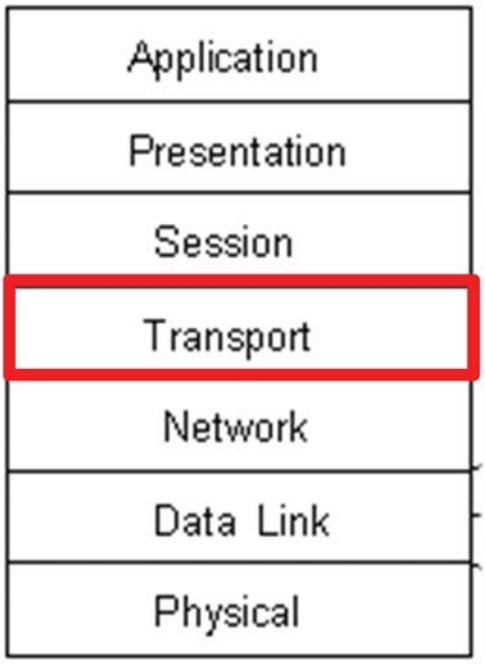
- **Layer 3 devices (Router)**
- a *router* is used to transfer packets between different networks, a packet may actually have to travel through several intermediate networks in order to reach its final destination network.
- Routers are used to connect networks that use different layer 2 protocols.



- For example, a router can be used to send a packet from an Ethernet to a Token Ring network.
- As long as both networks support the same layer 3 protocol, it doesn't matter whether their layer 1 and layer 2 protocols are different.



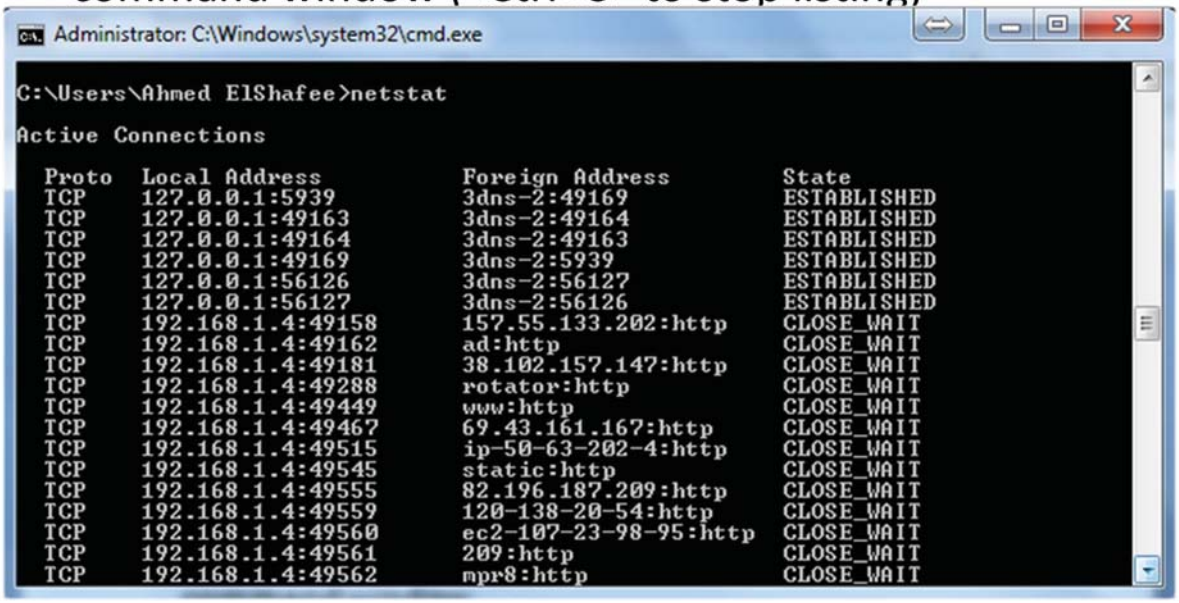
- **The Transport Layer**
- Definition:
  - the Transport layer is concerned with the transportation of information from one computer to another.



- Function:
  - ensure that packets are transported reliably and without errors.
  - establishing connections between network devices, acknowledging the receipt of packets,
  - resending packets that aren't received or are corrupted when they arrive.
  - divides large messages into smaller packets that can be sent over the network efficiently
  - reassembles the message on the receiving end,

- Examples:
  - TCP (normally paired with IP)
    - a connection oriented Transport layer protocol
  - *UDP* :
    - A connectionless protocol doesn't go to the trouble of establishing a connection before sending a packet. Instead, it simply sends the packet.
  - SPX (normally paired with IPX).

- Testing
  - To get information about the status of TCP and UDP connections by running the Netstat command from a command window (<Ctrl+C> to stop listing)



- **The Session Layer**
- **Definition**
  - The *Session layer establishes conversations known as sessions between networked* devices.
- **Function**
  - A single session include exchanging (transporting) data chunks between the two computers

- After a session between two computers has been established, it is maintained until the computers agree to terminate the session.
- transmission modes:
  - **Simplex:** In this mode, data flows in only one direction.
  - **Half-duplex:** In this mode, data flows in both directions, but only in one direction at a time.
  - **Full-duplex:** In this mode, data flows in both directions at the same time.

- **The Presentation Layer**
- **Definition**:

  responsible for how data is represente to applications.
- **Function**:

  1. Coding conversion
  - Most computers (windows, linux, apple) use the American Standard Code for Information Interchange (ASCII) to represent data
  - Some computers (IBM mainframe computers) use a different code, known as Extended Binary Coded

Decimal Interchange Code (EBCDIC).

- ASCII and EBCDIC aren't compatible with each other.
- To exchange information between a mainframe computer and a Windows computer, the Presentation layer must convert the data from ASCII to EBCDIC and vice versa.

2. Data compression

- Apply compression techniques so that fewer bytes of data are required to represent the information when it's sent over the network. At the other end of the transmission, the Presentation layer then uncompresses the data.

3. Scrambling data

– scramble the data before it is transmitted and unscramble it at the other end by using a sophisticated encryption technique

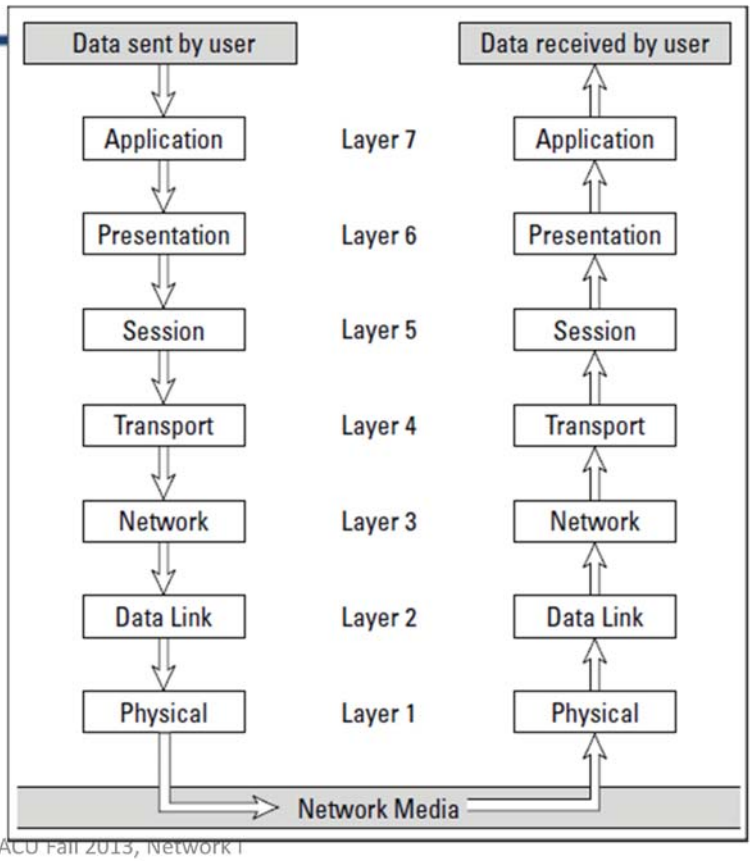
- **The Application Layer**
- **Definition**
- Application layer represents the programming interfaces that application programs such as Microsoft Office or QuickBooks use to request network services.

- Examples of Application layer protocols are
  - DNS (Domain Name System) for resolving Internet domain names.
  - FTP (File Transfer Protocol) for file transfers.
  - SMTP (Simple Mail Transfer Protocol) for e-mail.
  - SMB (Server Message Block) for file sharing in Windows networks.
  - NFS (Network File System) for file sharing in Unix networks.
  - Telnet for terminal emulation.

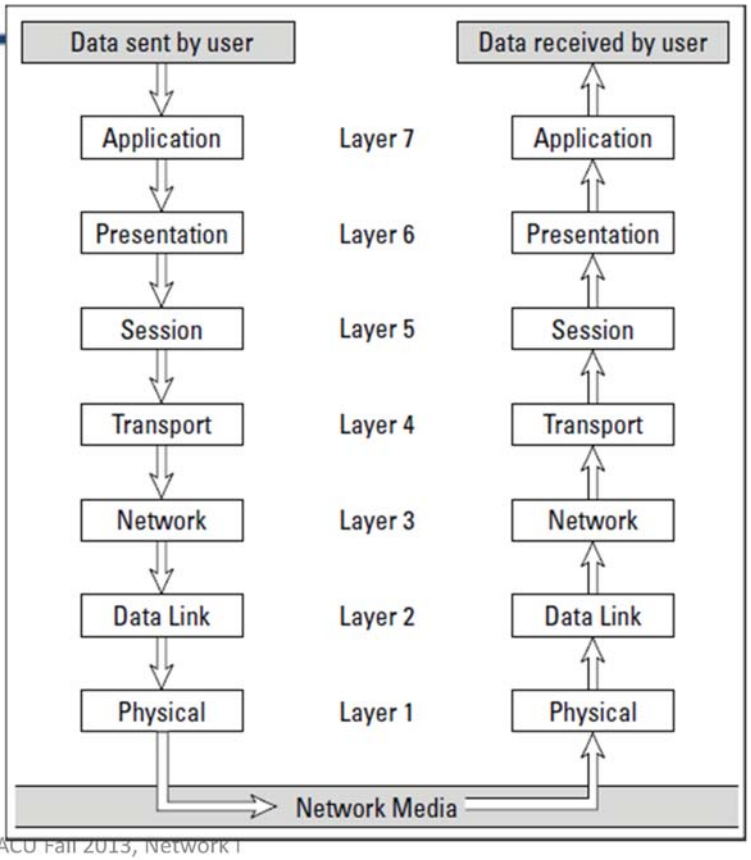
Following a Packet through the Layers

1. The end-user application sends data to another network computer.
2. The data enters the network through an Application layer interface, such as SMB.

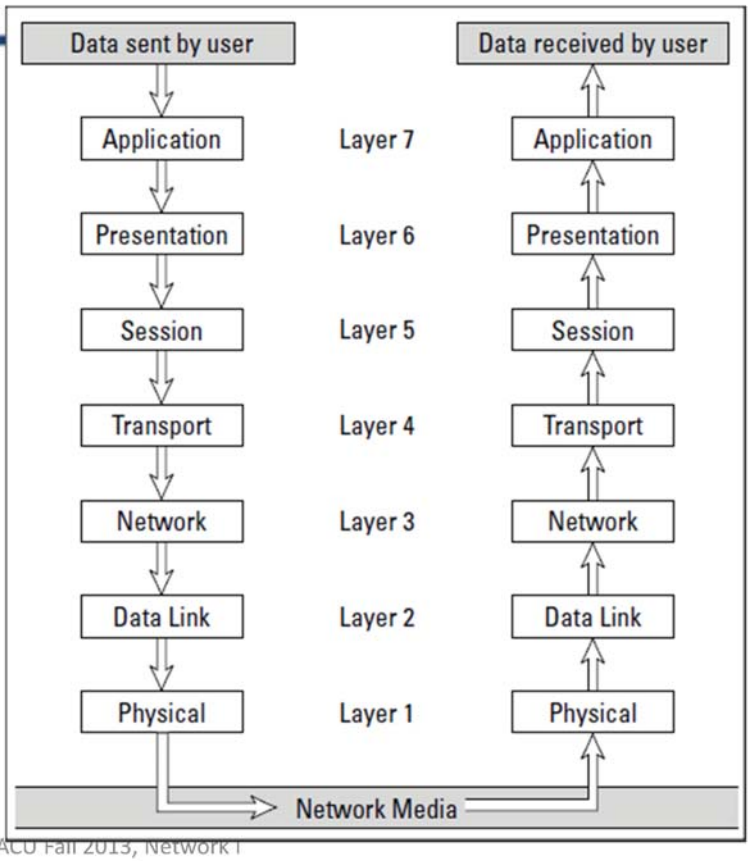
* Server Message Block (SMB), known as Common Internet File System (CIFS) operates as an application-layer network protocol, mainly used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network.



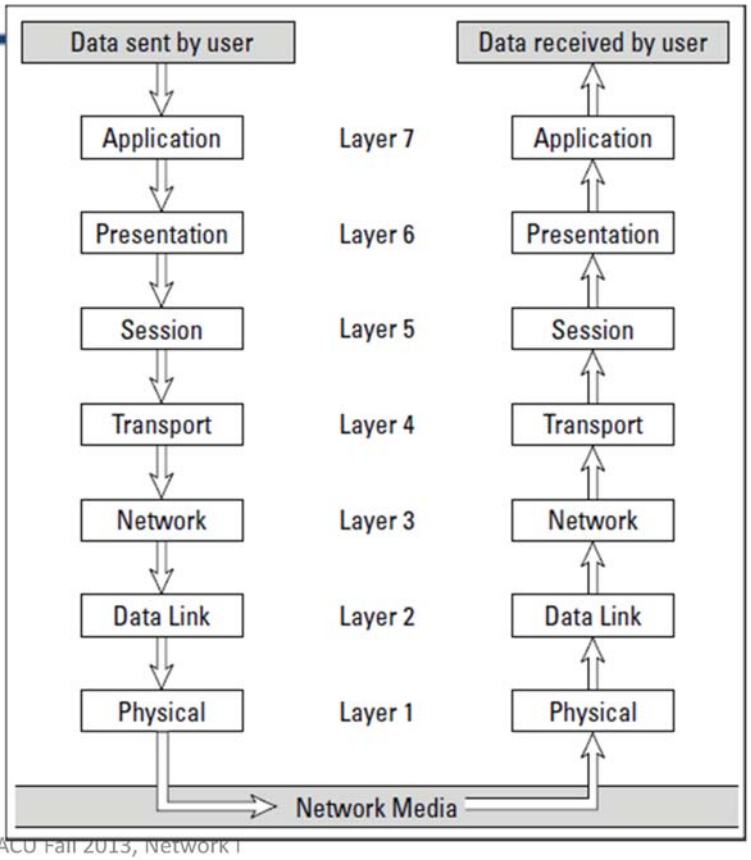
- The data then works its way down through the protocol stack.
- The protocol at each layer manipulates the data by adding header information, converting the data into different formats, combining/splitting packets to form larger/smaller packets, and so on.



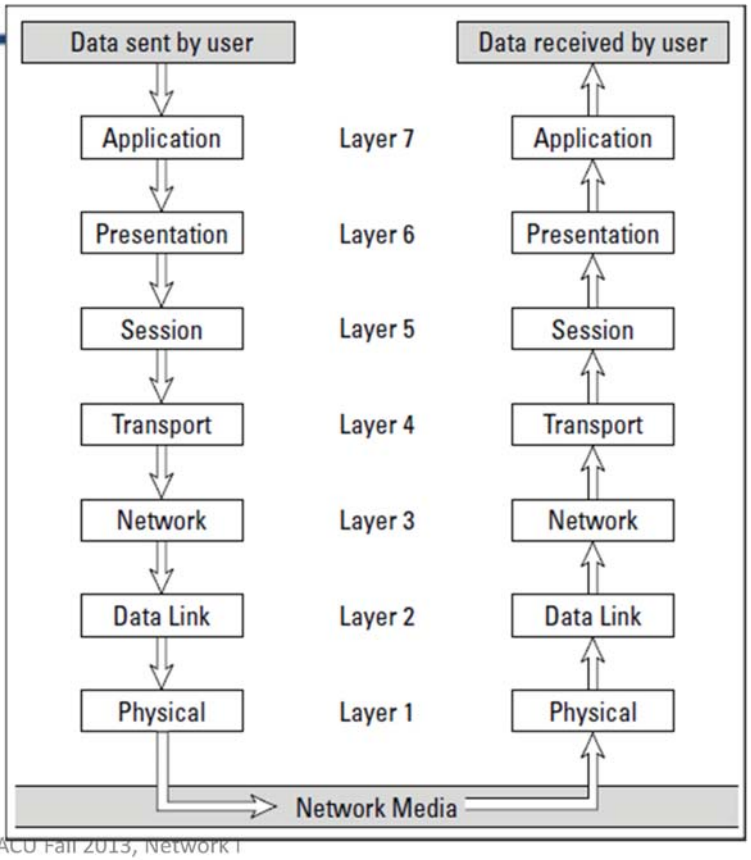
- When the data reaches the Physical layer protocol, it's actually placed on the network media (in other words, the cable) and sent to the receiving computer



- When the receiving computer receives the data, the data works its way up through the protocol stack.
- Then, the protocol at each layer reverses the processing that was done by the corresponding layer on the sending computer.



- Headers are removed, data is converted back to its original format, packets that were split into smaller packets are recombined into larger messages, (vice versa) and so on.
- When the packet reaches the Application layer protocol, it's delivered to an application that can process the data.



Thanks,..

See you next week (ISA),…