CCNA Routing and Switching

Chapter 1

Introduction

Introduction to Networking

- Computer network, or simply network
  - Refers to the connection of two or more computers by some type of medium

Why Do We Use Networks?

- This question can be answered in one word:
  - convenience People expect interoperability from electronic devices
- Computer networks allow:
  - For the transfer of files, data, and even shared applications without copying anything to floppy disk
  - Computers to share items such as printers, scanners, fax machines, processors, disk drives, and other resources
- Networked computers can share data and peripherals

Networking Terminology

- **Media**
  - Refers to the wire cabling that form the connections in most networks
  - Some networks use **wireless** transmission media, such as infrared or radio signals
- **Client/server** networks
  - **Servers** host the resources for the clients to use and provide security
  - A **client** is the computer that requests resources from the server

Networking Terminology

- **Client/server networks (continued)**
  - Types of servers include:
  - Print server
  - File server
  - Database server
  - Remote access server (RAS)
  - Web server
- **Peer-to-peer network**
  - When every computer on a network acts as both a client and a server
  - Also known as “workgroups”

Networking Terminology

- **LAN, WAN, MAN, SAN**
  - **Local area network (LAN)** is contained within a company or department and located in a single geographic area
  - **Wide area network (WAN)** spans multiple geographic areas and is usually connected by common telecommunication carriers
  - **Metropolitan area network (MAN)** refers to the intermediate stage between a LAN and a WAN

Networking Terminology

- **Storage area network (SAN)** refers to a series of storage devices that are networked together to provide very fast data storage for a network or subnetwork

- **Network Operating System (NOS)**
  - Allows communication, security, and distribution of data, files, and applications over a network

- **Network Interface Card (NIC)**
  - A device that allows a computer or other device to connect to a network through the media

Networking Terminology

- **Networking hardware**
  - Describes all the physical components of a network, such as the NIC, cable, hub, switch, router, and any related connectors or devices
- **Networking software**
  - The programs used to run a network
- **Virtual private networks**
  - Network that uses a public communications infrastructure (like the Internet) to facilitate private communication between a company LAN and remote employees

Networking Terminology

- **Virtual private networks**
  - **Extranet** is the part of the company's network that allows access to nonemployees
  - **Intranet** is the part of the company's network that allows access to employees
- **Firewalls:**
  - These devices are network security systems that monitor and control the incoming and outgoing network traffic based on predetermined security rules

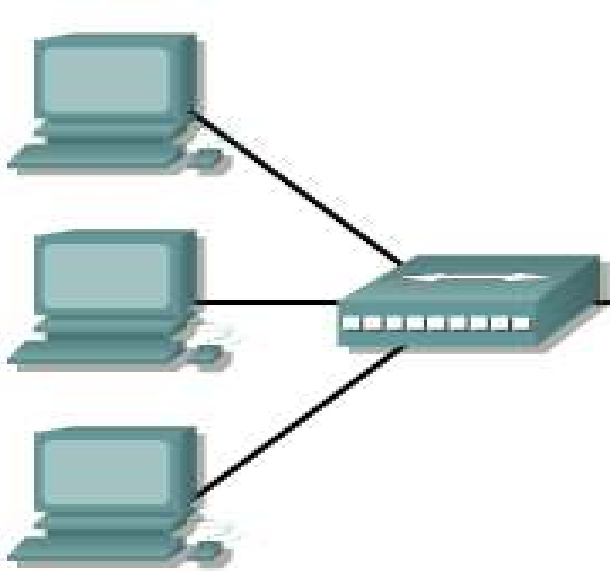
Internetworking

- **Networking Devices**
  - Equipment that connects directly to a network segment is referred to as a device.
- These devices are broken up into two classifications.
  - **End-user devices** include computers, printers, scanners, and other devices that provide services directly to the user.
  - **Network devices** include all the devices that connect the end-user devices together to allow them to communicate.

Internetworking

- A **hub** creates one collision domain and one broadcast domain

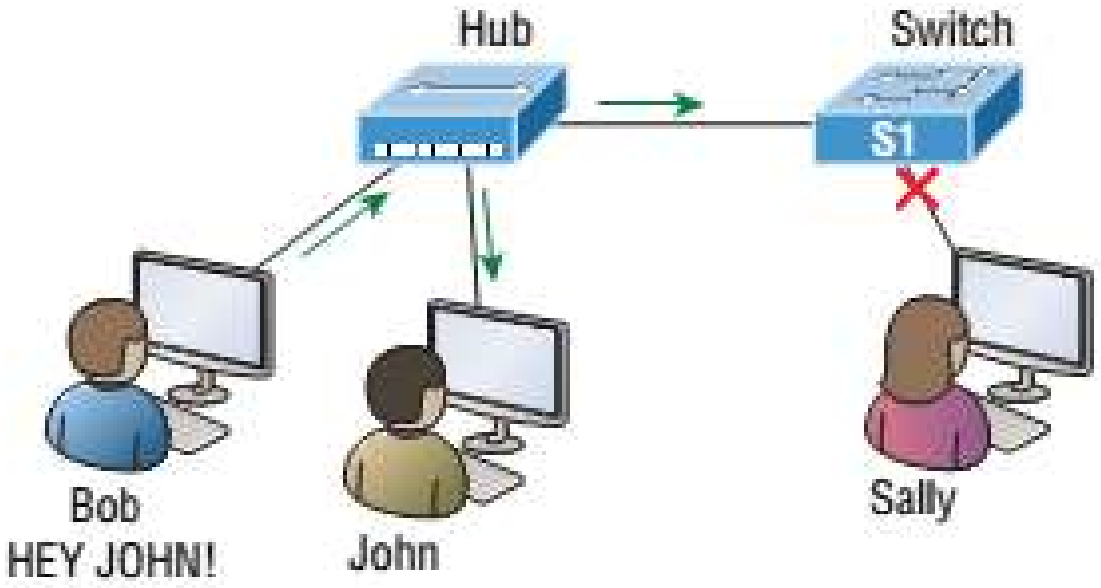
Connects a group of Hosts



Hub

Internetworking

- **Switch & Bridges** breakup collision domains



Internetworking

Switch

Internetworking

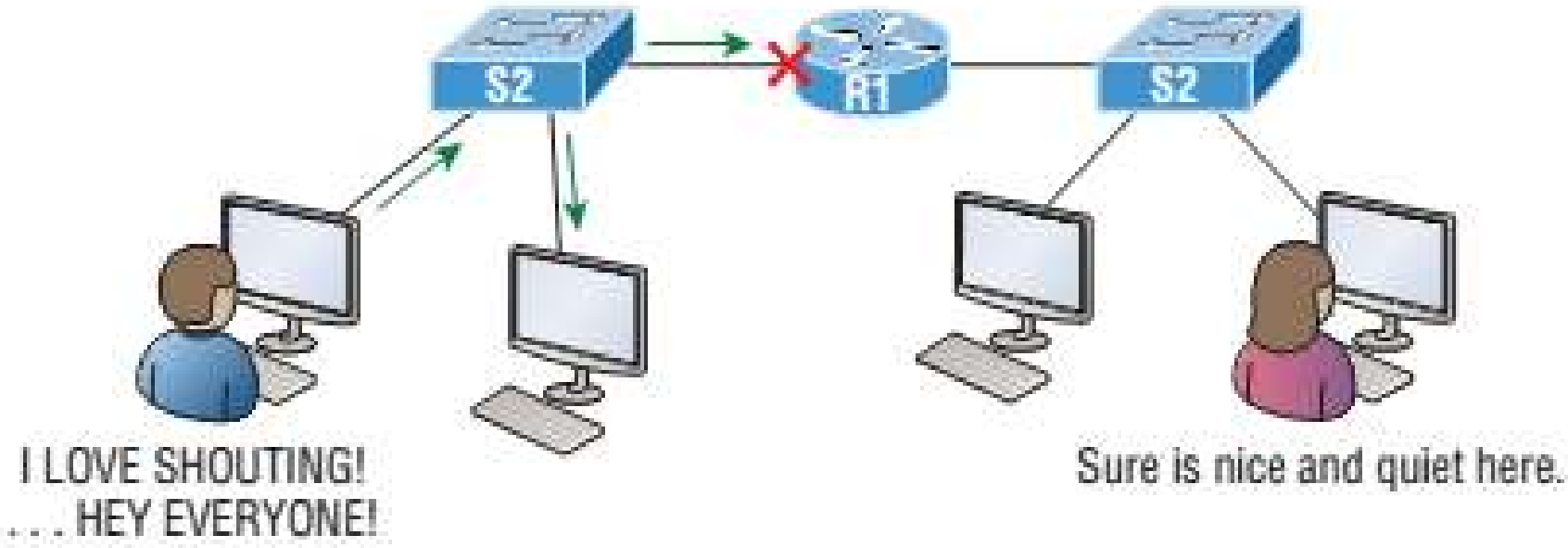
Bridges

Internetworking

- **Routers create Internetworks**
  - Routers are used to connect networks together
  - Route packets of data from one network to another
  - Cisco became the de facto standard of routers because of their high-quality router products
  - Routers, by default, break up a broadcast domain

Internetworking

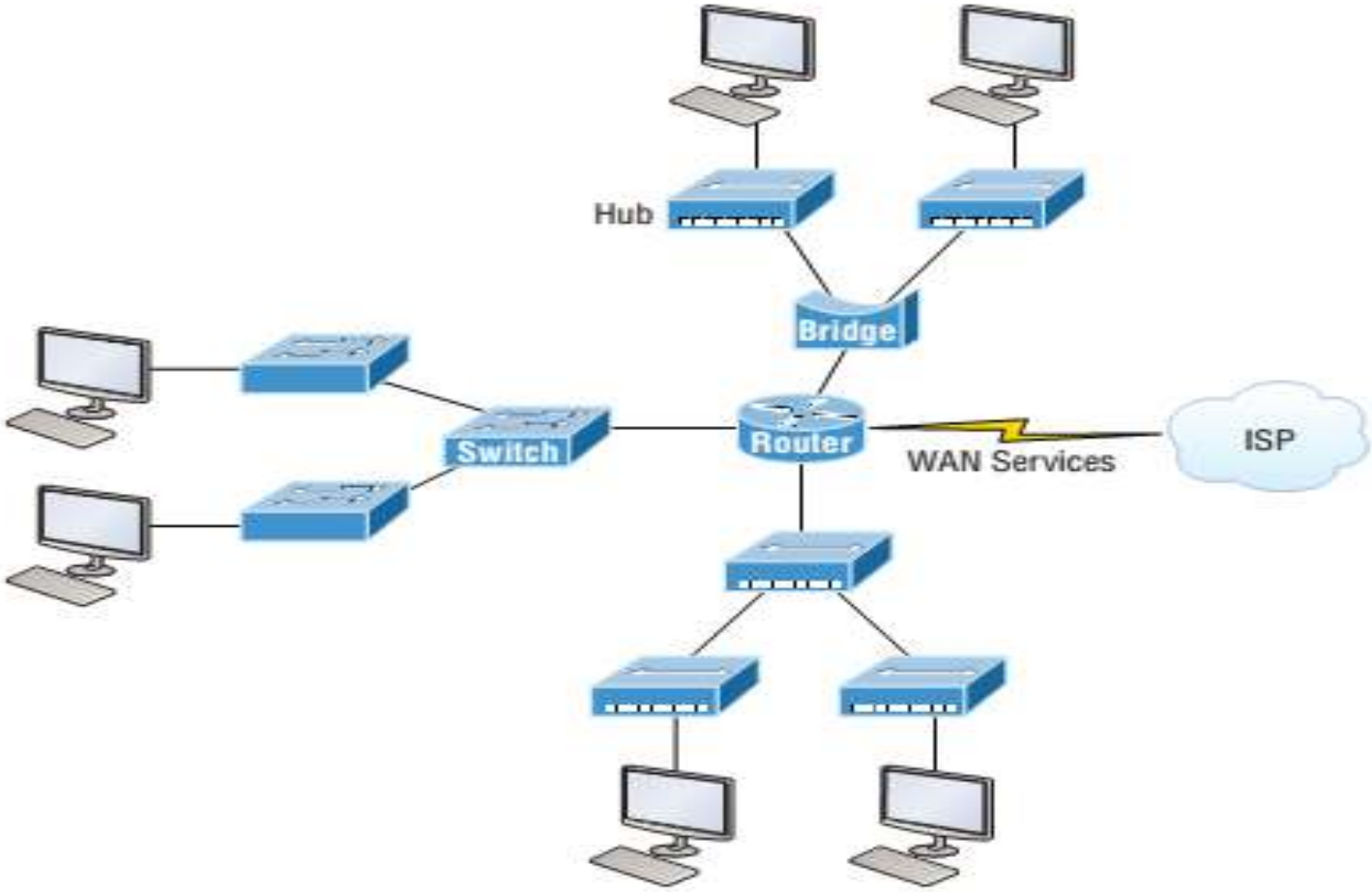
- **Routers create Internetworks**



Internetworking

Routers

Internetworking



Internetworking Models

- The **OSI** model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work in peaceable accord with each other
- When networks first came into being, computers could typically communicate only with computers from the same manufacturer
- The **OSI** model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer

OSI Model

Why do we need the OSI Model?

- To address the problem of networks increasing in size and in number, the International Organization for Standardization **(ISO)** researched many network schemes and recognized that there was a need to create a network model
- This would help network builders implement networks that could communicate and work together
- ISO therefore, released the OSI reference model in 1984.

OSI Model

Don't Get Confused.

ISO - International Organization for Standardization

OSI - Open System Interconnection

IOS - Internetwork Operating System

To avoid confusion, some people say "International Standard Organization."

The OSI Reference Model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

The OSI Model will be used throughout your entire networking career!

The OSI Reference Model

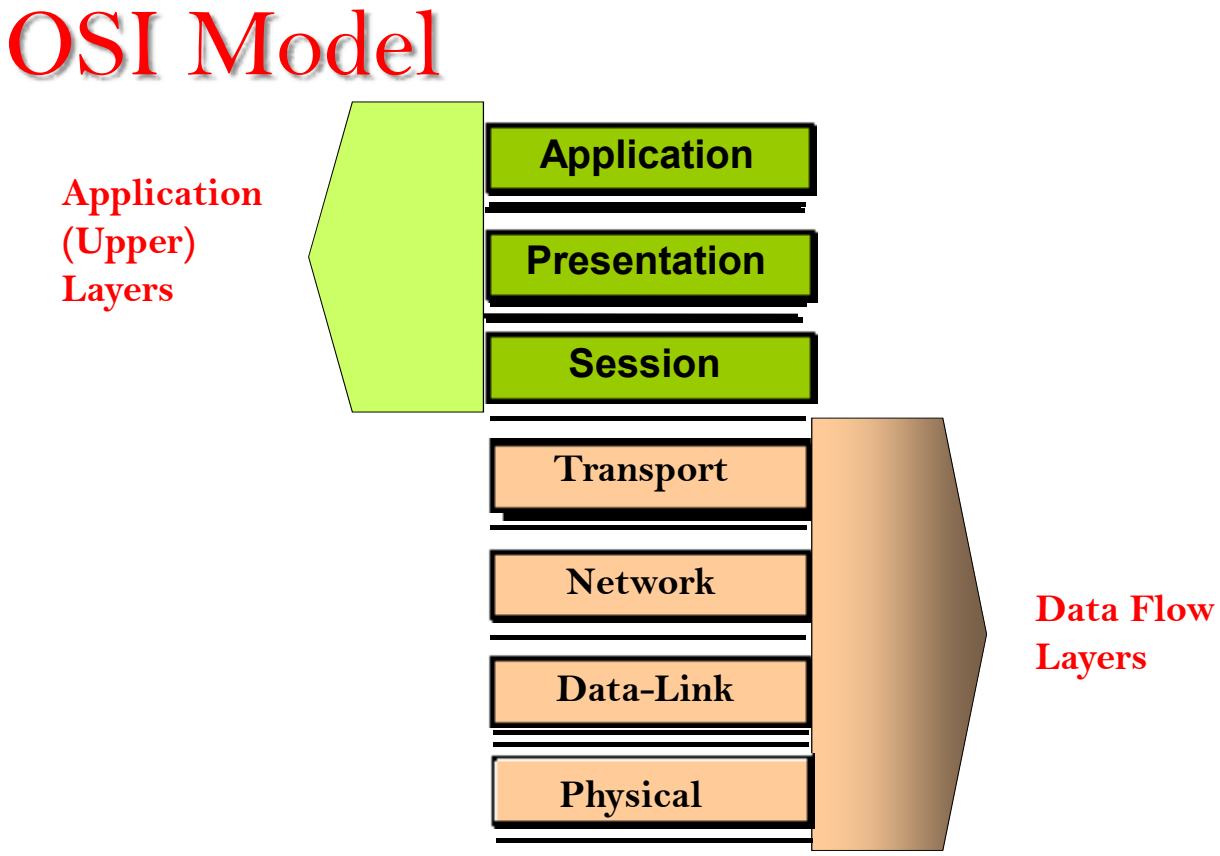
You need to know the seven layers in sequence, either top-to-bottom or bottom-to-top. Here are some mnemonic phrases to help you remember the layers of the OSI model.

Top-to-bottom: "All people Seem To Need Data Processing"

Bottom-to-top: "Please Do Not Throw Sausage Pizza Away"

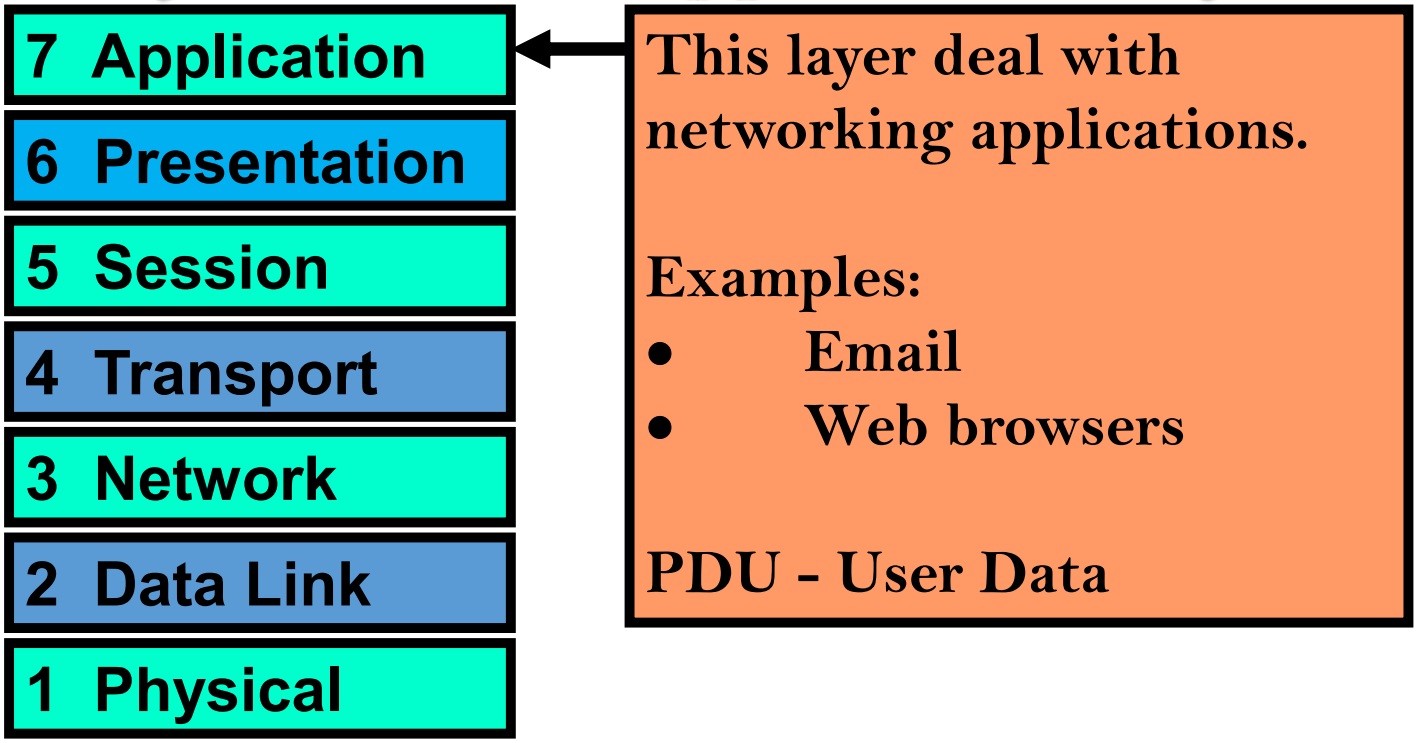
Memorize it!

OSI Model


OSI Model
Application
(Upper)
Layers
Application
Presentation
Session
Transport
Network
Data-Link
Physical
Data Flow
Layers

OSI Model

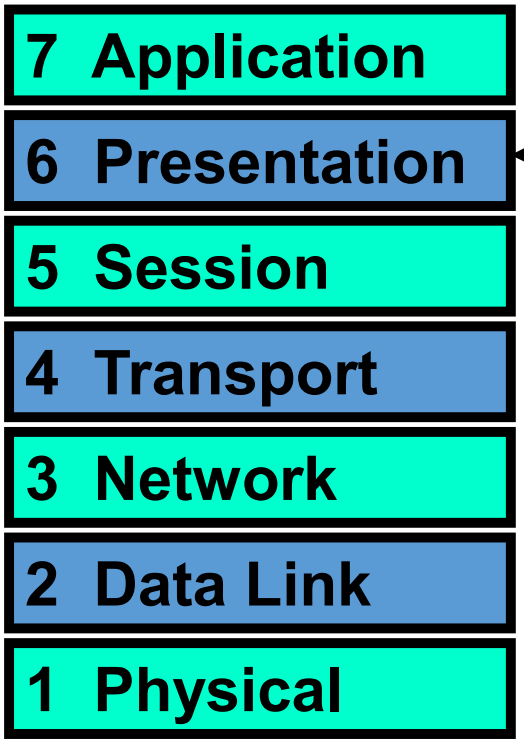
Layer 7 - The Application Layer



Each of the layers have Protocol Data Unit (PDU)

OSI Model

Layer 6 - The Presentation Layer



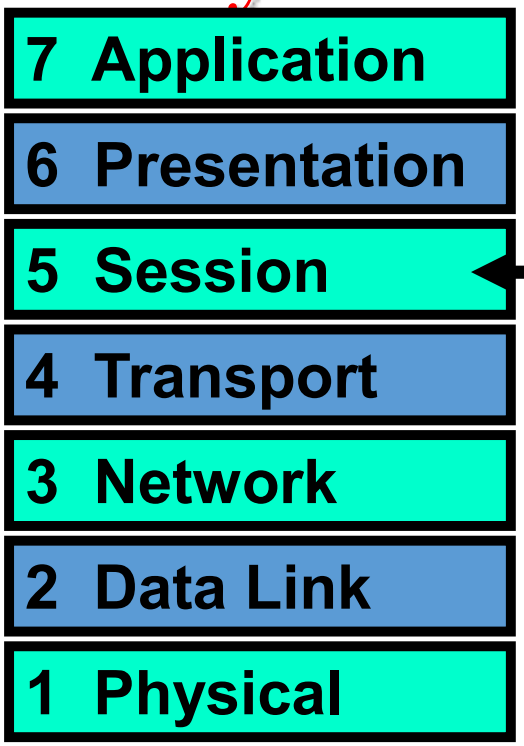
This layer is responsible for presenting the data in the required format which may include:

- ❑Code Formatting
- ❑Encryption
- ❑Compression

PDU - Formatted Data

OSI Model

Layer 5 - The Session Layer



- This layer establishes, manages, and terminates sessions between two communicating hosts.
- Creates Virtual Circuit
- Coordinates communication between systems
- Organize their communication by offering three different modes
  - Simplex
  - Half Duplex
  - Full Duplex

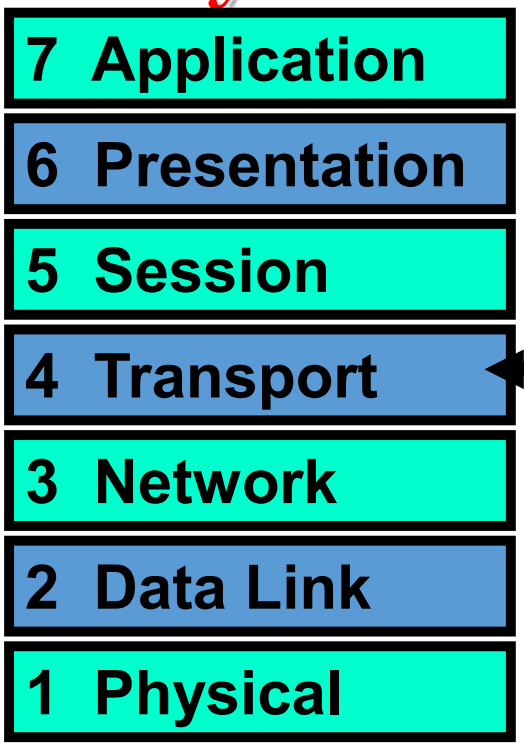
Example:

- **Client Software (Used for logging in)**

PDU - Formatted Data

OSI Model

Layer 4 - The Transport Layer

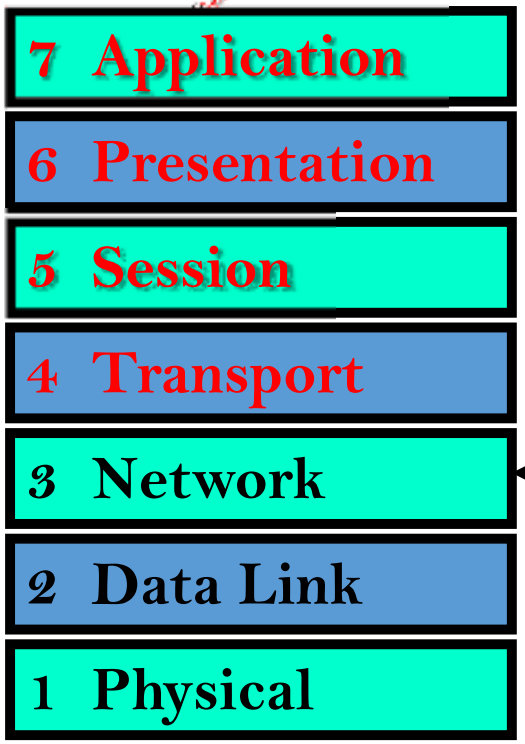


- This layer breaks up the data from the sending host and then reassembles it in the receiver.
- It also is used to insure reliable data transport across the network.
- Can be reliable or unreliable
- Sequencing
- Acknowledgment
- Retransmission
- Flow Control

PDU - Segments

OSI Model

Layer 3 - The Network Layer

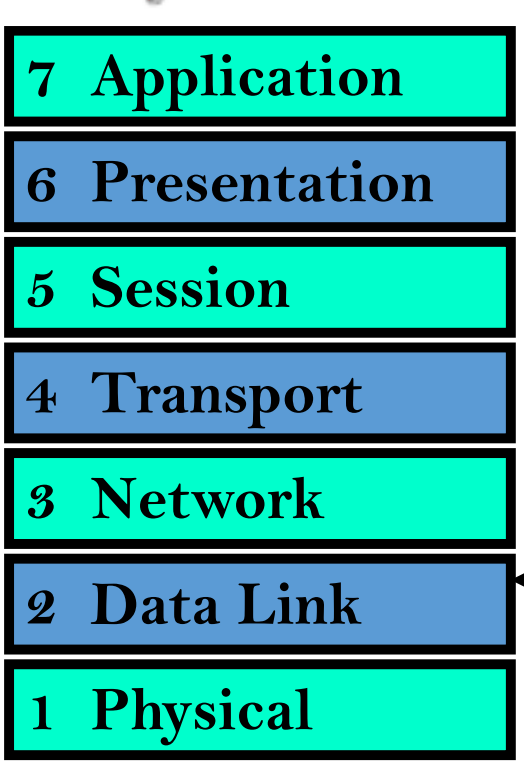


- Sometimes referred to as the "Cisco Layer".
- End to End Delivery
- Provide logical addressing that routers use for path determination
- Segments are encapsulated
- Internetwork Communication
- Packet forwarding
- Packet Filtering
- Makes "Best Path Determination"
- Fragmentation

PDU – Packets – IP/IPX

OSI Model

Layer 2 - The Data Link Layer



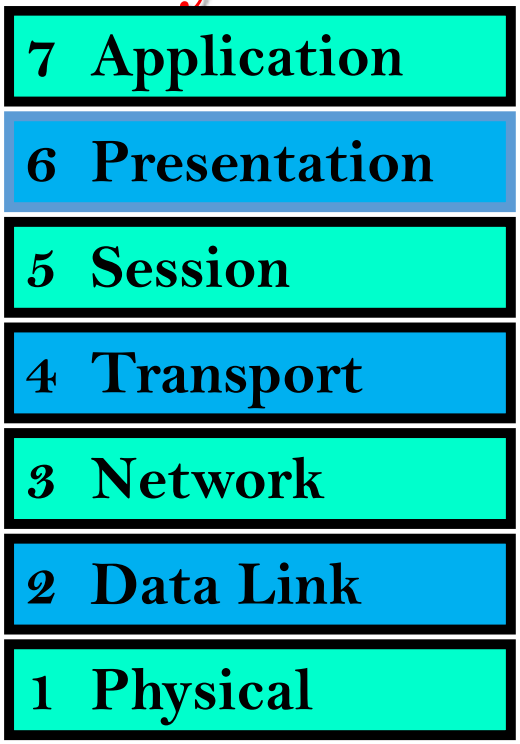
- Performs Physical Addressing
- This layer provides reliable transit of data across a physical link.
- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection, not correction
- LLC and MAC
- Logical Link Control performs Link establishment
- MAC Performs Access method

PDU - Frames

Preamble	DMAC	SMAC	Data length	DATA	FCS

OSI Model

Layer 1 - The Physical Layer



- This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.
- Move bits between devices
- Encoding

PDU - Bits

OSI Model

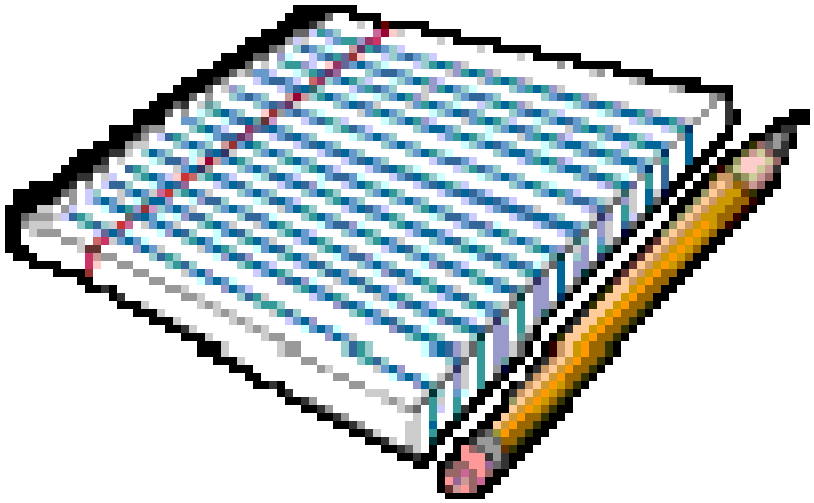
OSI Model Analogy
Application Layer – Source Host

After riding your new bicycle a few times in Mogadishu, you decide that you want to give it to a friend who lives in BAIDOA, BAY.

NB: I borrowed this example from apparently Indian teacher whose name I did not find. I thank him for the good analogy

OSI Model

OSI Model Analogy
Presentation Layer - Source Host



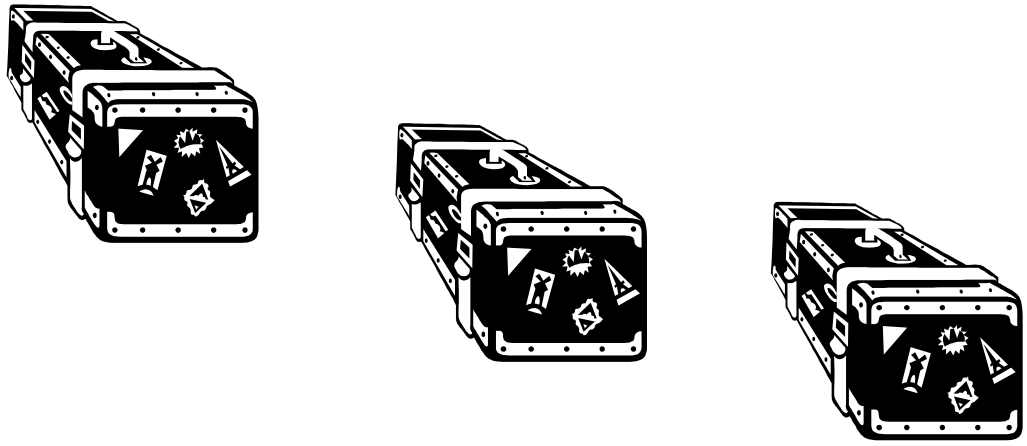
Make sure you have the proper directions to disassemble and reassemble the bicycle.

35

OSI Model Analogy
Session Layer – Source Host

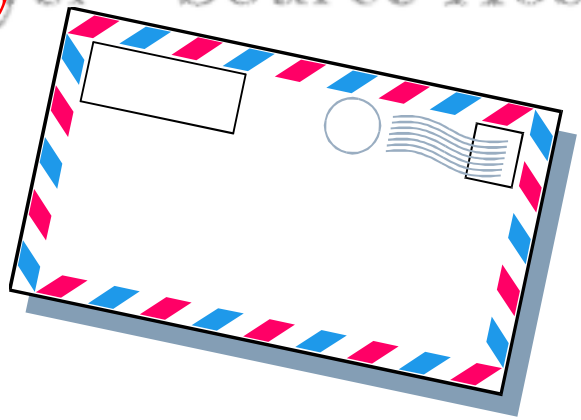
Call your friend and make sure you have his correct address.

OSI Model Analogy
Transport Layer – Source Host



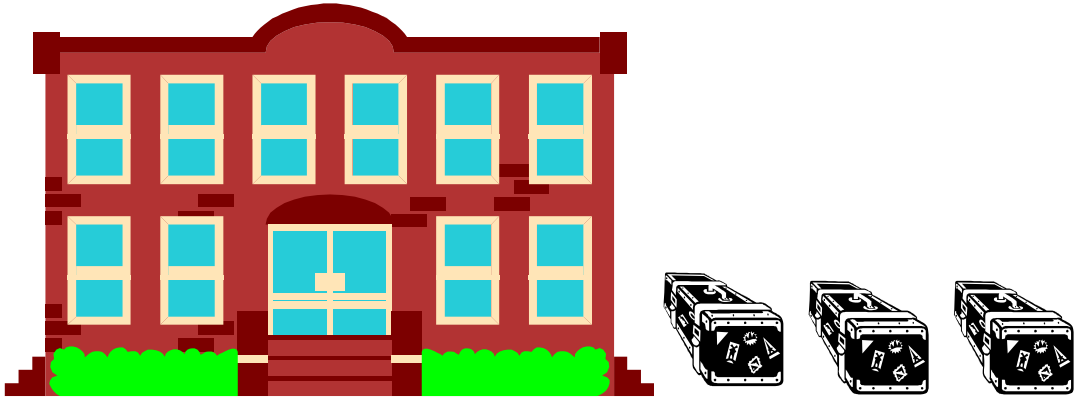
Disassemble the bicycle and put different pieces in different boxes. The boxes are labeled "1 of 3", "2 of 3", and "3 of 3".

OSI Model Analogy
Network Layer - Source Host



Put your friend's complete mailing address (and yours) on each box.Since the packages are too big for your mailbox (and since you don't have enough stamps) you determine that you need to go to the post office.

OSI Model Analogy
Data Link Layer – Source Host



Mogadishu post office takes possession of the boxes.

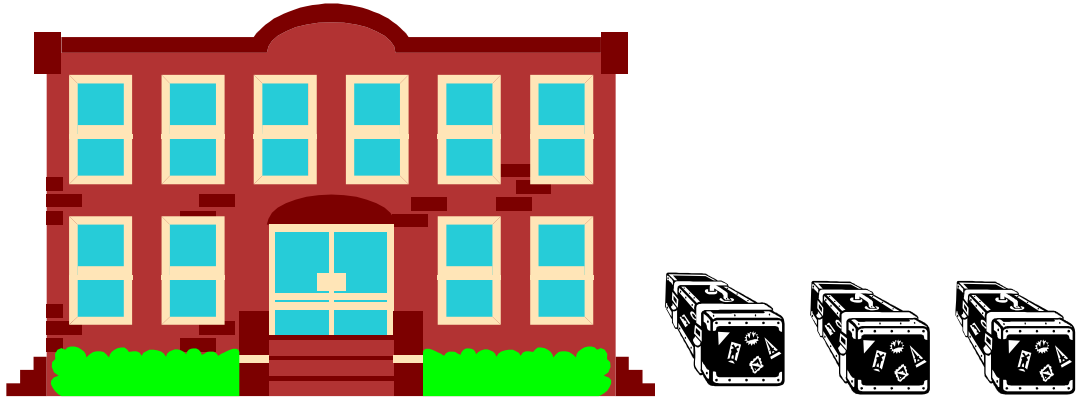
39

OSI Model Analogy
Physical Layer - Media

The boxes are flown from Mogadishu to BAY.

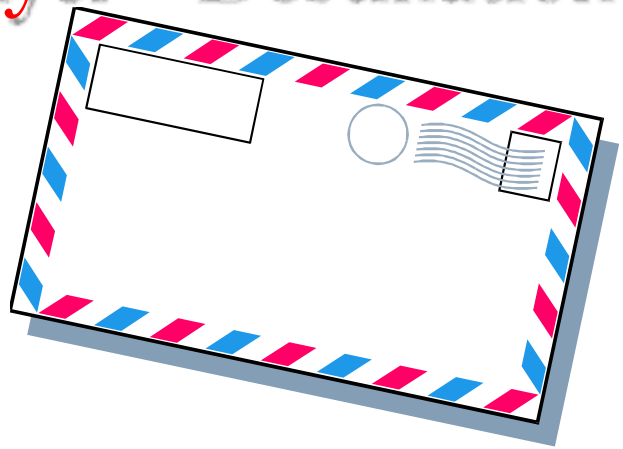
OSI Model

OSI Model Analogy
Data Link Layer - Destination



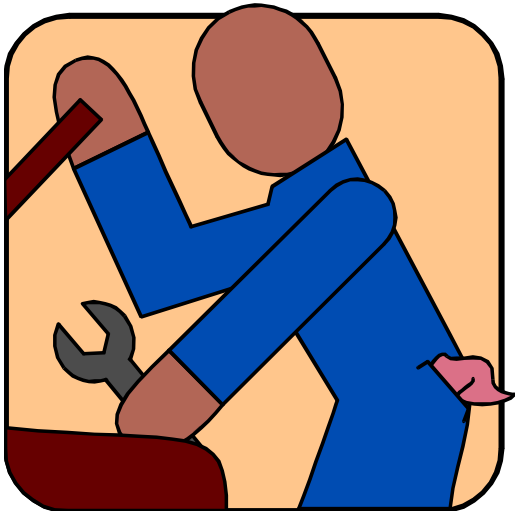
BAIDOA post office receives your boxes.

OSI Model Analogy
Network Layer - Destination



Upon examining the destination address, BAIDOA post office determines that your boxes should be delivered to your written home address.

OSI Model Analogy
Transport Layer - Destination



Your friend calls you and tells you he got all 3 boxes and he is having another friend named Ali reassemble the bicycle.

OSI Model Analogy
Session Layer - Destination

Your friend hangs up because he is done talking to you.

OSI Model Analogy
Presentation Layer - Destination

Ali is finished and "presents" the bicycle to your friend. Another way to say it is that your friend is finally getting him "present".

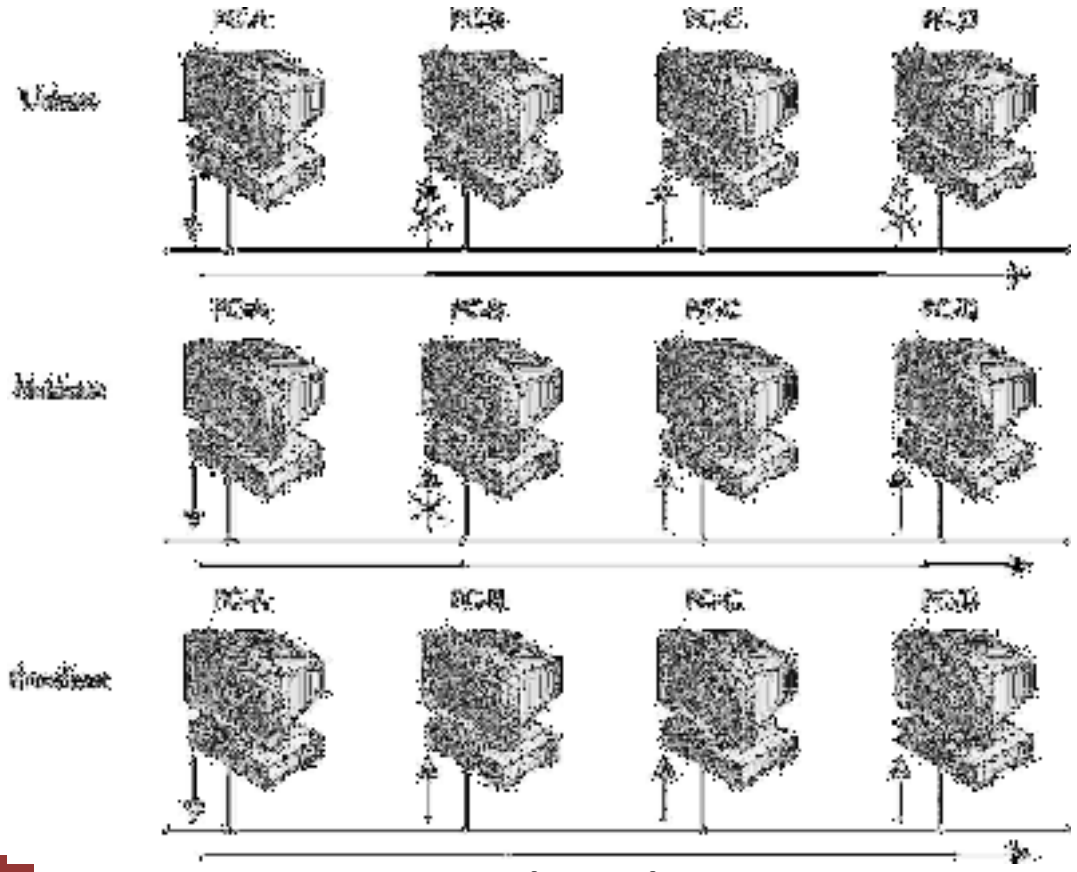
OSI Model Analogy
Application Layer - Destination

Your friend enjoys riding his new bicycle in BAIDOA.

Types of Transmission

- Unicast
- Multicast
- Broadcast

Types of Transmission



Broadcast Domain

- A group of devices receiving broadcast frames initiating from any device within the group

- Routers do not forward broadcast frames, broadcast domains are not forwarded from one broadcast to another.

Collision

- The effect of two nodes sending transmissions simultaneously in Ethernet. When they meet on the physical media, the frames from each node collide and are damaged.

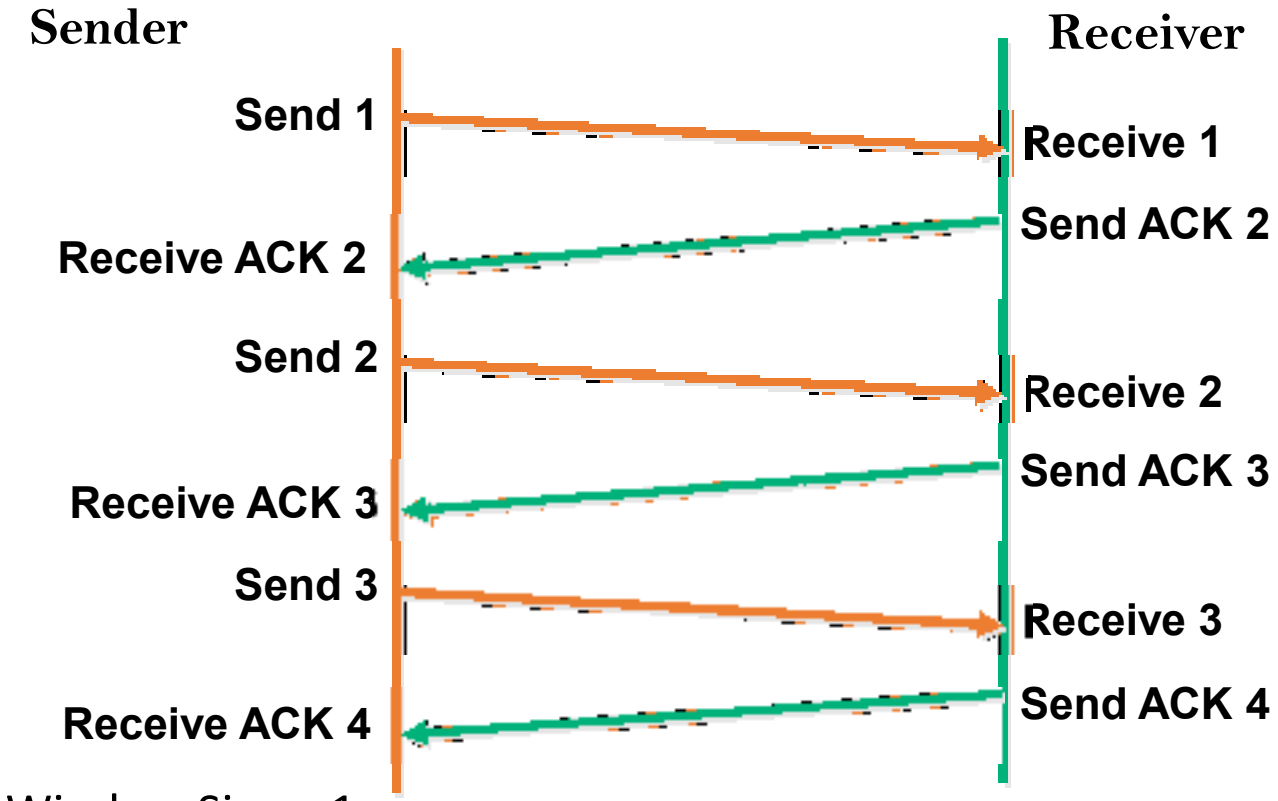
Collision Domain

- The network area in Ethernet over which frames that have collided will be detected.
- Collisions are propagated by hubs and repeaters
- Collisions are Not propagated by switches, routers, or bridges

Windowing

- Windowing in networking means the quantity of data segments which is measured in bytes that a machine can transmit/send on the network without receiving an acknowledgement

TCP Simple Acknowledgment



Chapter 3

TCP/IP

Introduction to TCP/IP & DoD Model

Why Another Model?

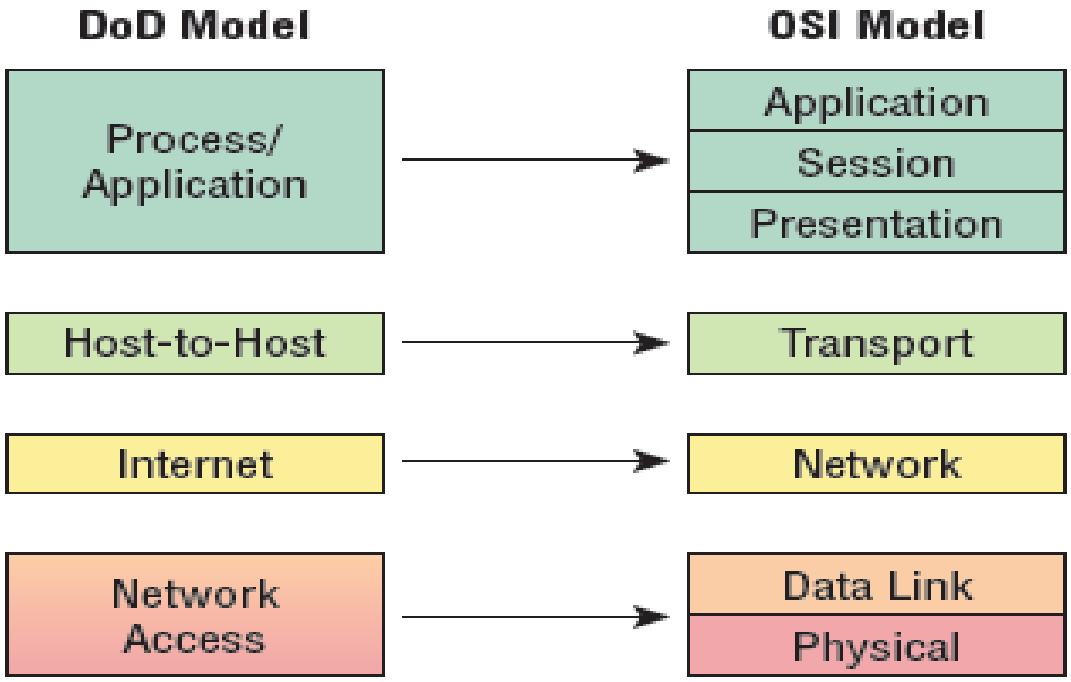
Although the OSI reference model is universally recognized, the historical and technical open standard of the Internet is Transmission Control Protocol / Internet Protocol (TCP/IP).

The TCP/IP reference model and the TCP/IP protocol stack make data communication possible between any two computers, anywhere in the world, at nearly the speed of light.

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions, even a nuclear war.

TCP/IP Protocol Stack

The DoD and OSI models

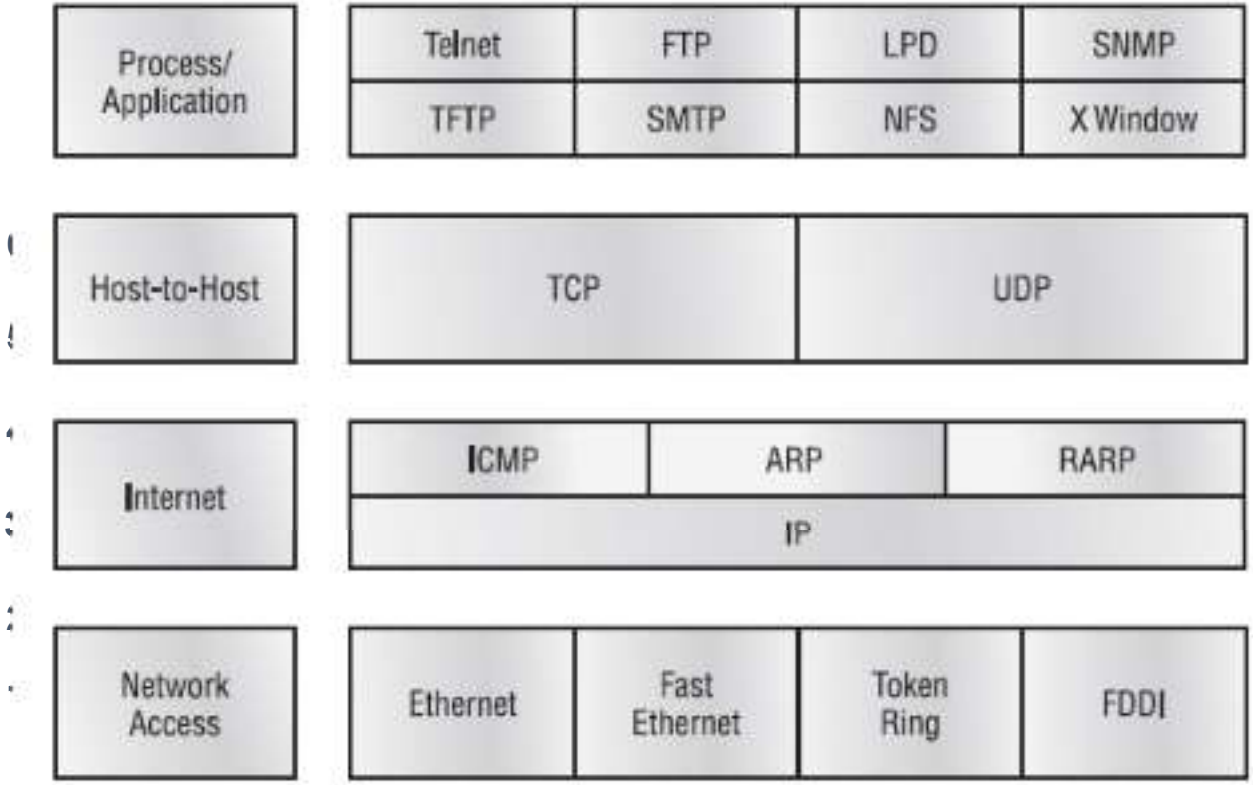


57

The Process/Application Layer Protocols

- Telnet
- SSH
- FTP
- TFTP
- SNMP
- HTTP
- HTTPS
- NTP
- DNS
- DHCP/BootP

Department of Defense DoD Model



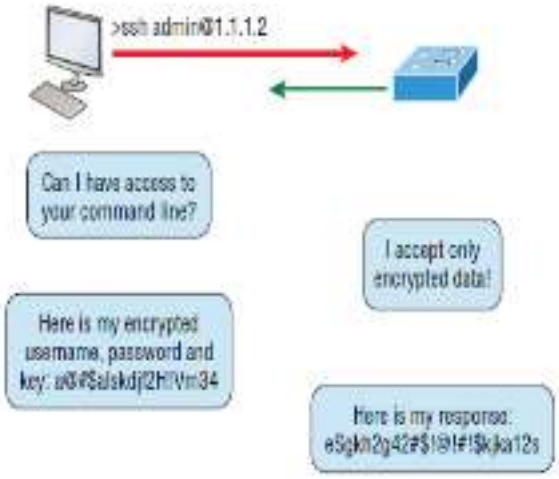
59

Telnet

- Telnet was one of the first Internet standards, developed in 1969, and is the chameleon of protocols—its specialty is terminal emulation. It allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server, in order to access a command-line interface.

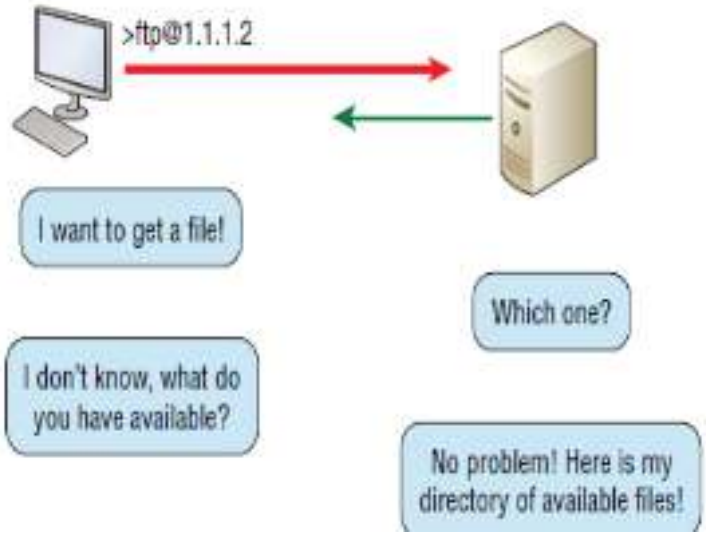
Secure Shell (SSH)

- Secure Shell (SSH) protocol sets up a secure session that's similar to Telnet over a standard TCP/IP connection and is employed for doing things like logging into systems, running programs on remote systems, and moving files from one system to another. And it does all of this while maintaining an encrypted connection.



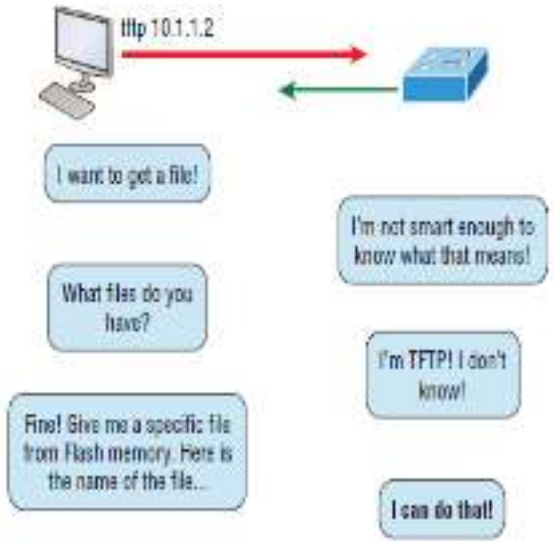
File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) actually lets us transfer files, and it can accomplish this between any two machines using it. But FTP isn't just a protocol; it's also a program. Operating as a protocol, FTP is used by applications. As a program, it's employed by users to perform file tasks by hand. FTP also allows for access to both directories and files and can accomplish certain types of directory operations, such as relocating into different ones



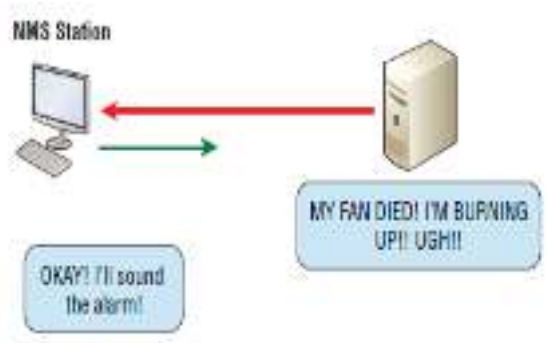
Trivial File Transfer Protocol (TFTP)

- File Transfer Protocol (FTP) actually lets us transfer files, and it can accomplish this between any two machines using it. But FTP isn't just a protocol; Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it because it's fast and so easy to use!
-



Simple Network Management Protocol (SNMP v1, v2, v3)

- Simple Network Management Protocol (SNMP) collects and manipulates valuable network information. It gathers data by polling the devices on the network from a network management station (NMS) at fixed or random intervals, requiring them to disclose certain information, or even asking for certain information from the device. In addition, network devices can inform the NMS station about problems as they occur so the network administrator is alerted. SNMP receives something called a. This protocol can also stand as a watchdog over the network, quickly notifying managers of any sudden turn of events. These network watchdogs are called agents, and when aberrations occur, agents send an alert called a trap to the management station.



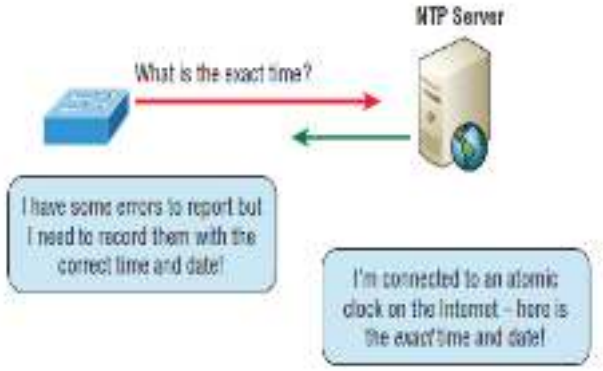
Hypertext Transfer Protocol (HTTP)

- It's used to manage communications between web browsers and web servers and opens the right resource when you click a link, wherever that resource may actually reside.
- In order for a browser to display a web page, it must find the exact server that has the right web page, plus the exact details that identify the information requested.

- Hypertext Transfer Protocol Secure (HTTPS) is also known as Secure Hypertext Transfer Protocol. It uses Secure Sockets Layer (SSL). Sometimes you'll see it referred to as SHTTP or S-HTTP,

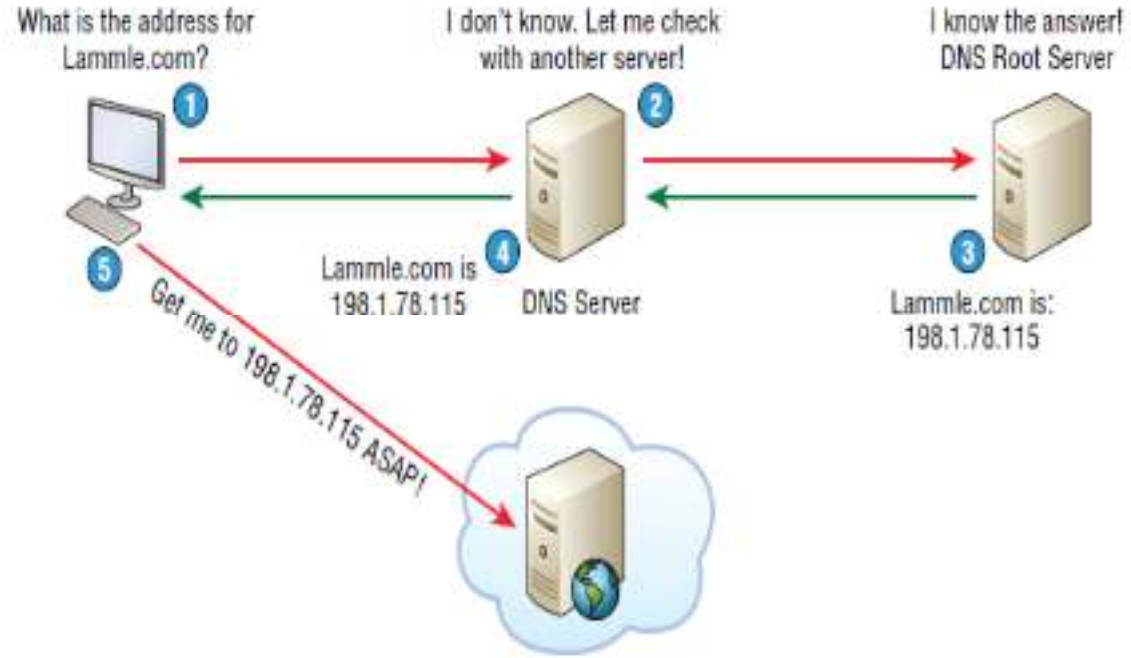
Network Time Protocol (NTP)

- used to synchronize the clocks on our computers to one standard time source (typically, an atomic clock). Network Time Protocol (NTP) works by synchronizing devices to ensure that all computers on a given network agree on the time



Domain Name Service (DNS)

- Domain Name Service (DNS) resolves hostnames.



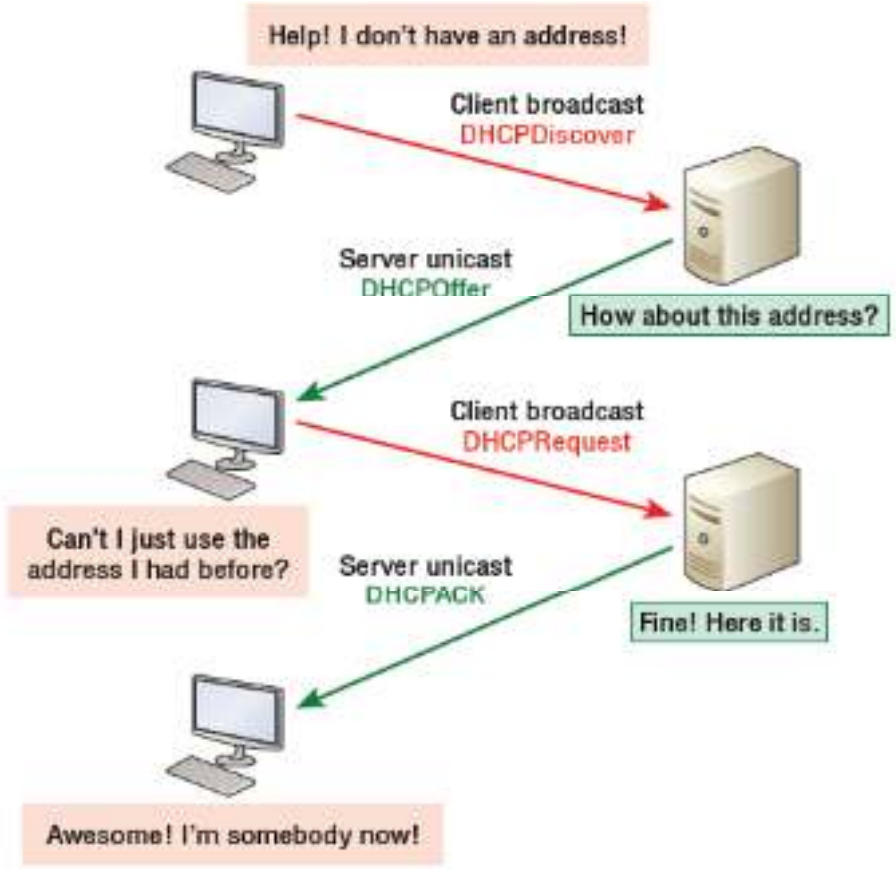
Dynamic Host Configuration Protocol (DHCP)/Bootstrap Protocol (BootP)

- Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts. It allows for easier administration and works well in small to very large network environments.
- DHCP differs from BootP in that BootP assigns an IP address to a host but the host's hardware address must be entered manually in a BootP table. You can think of DHCP as a dynamic BootP. But remember that BootP is also used to send an operating system that a host can boot from. DHCP can't do that.

  DHCP server can provide:

  - IP address
  - Subnet mask
  - Domain name
  - Default gateway (routers)
  - DNS server address
  - WINS server address

DHCP client four-step process



Automatic Private IP Addressing (APIPA)

- **Windows operating systems provide a feature called Automatic Private IP Addressing (APIPA). With APIPA, clients can automatically self-configure an IP address and subnet mask—basic IP information that hosts use to communicate—when a DHCP server isn't available. The IP address range for APIPA is 169.254.0.1 through 169.254.255.254.**

The Host-to-host Layer Protocols

There two main protocols at this layer:

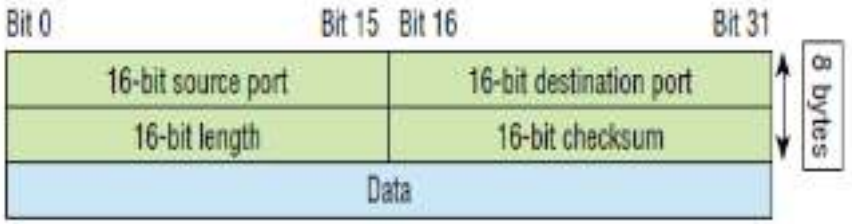
- Transmission Control Protocol (TCP) (connection oriented)
- User Datagram Protocol (UDP) (connectionless)

- Transmission Control Protocol (TCP) takes large blocks of information from an application and breaks them into segments. It numbers and sequences each segment so that the destination's TCP stack can put the segments back into the order the application intended.
- After these segments are sent on the transmitting host, TCP waits for an acknowledgment of the receiving end's TCP virtual circuit session, retransmitting any segments that aren't acknowledged.

71

User Datagram Protocol (UDP) (Connectionless protocol)

- **User Datagram Protocol (UDP) is basically the scaled-down economy model of TCP, which is why UDP is sometimes referred to as a thin protocol. Like a thin person on a park bench, a thin protocol doesn't take up a lot of room—or in this case, require much bandwidth on a network.**



Key protocols that use TCP and UDP

TCP	UDP
Telnet 23	SNMP 161
SMTP 25	TFTP 69
HTTP 80	DNS 53
FTP 20, 21	BooTPS/DHCP 67
DNS 53	
HTTPS 443	
SSH 22	
POP3 110	
NTP 123	
IMAP4 143	