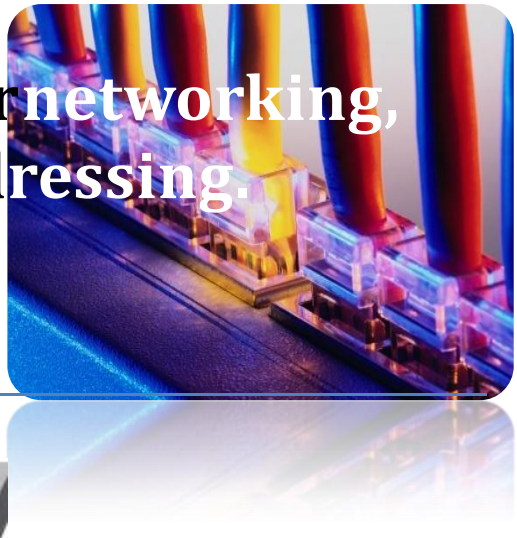
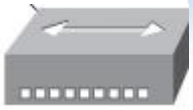
Introduction to internetworking, OSI, TCP/IP and Addressing.



Network Devices

❖ **Repeater (Hub)**



Hubs don't break collision and broadcast domains. So any packet will be forwarded to all ports.

❖ **Bridge (Switch)**

On the other hand switch can divide collision domain but not broadcast domain.

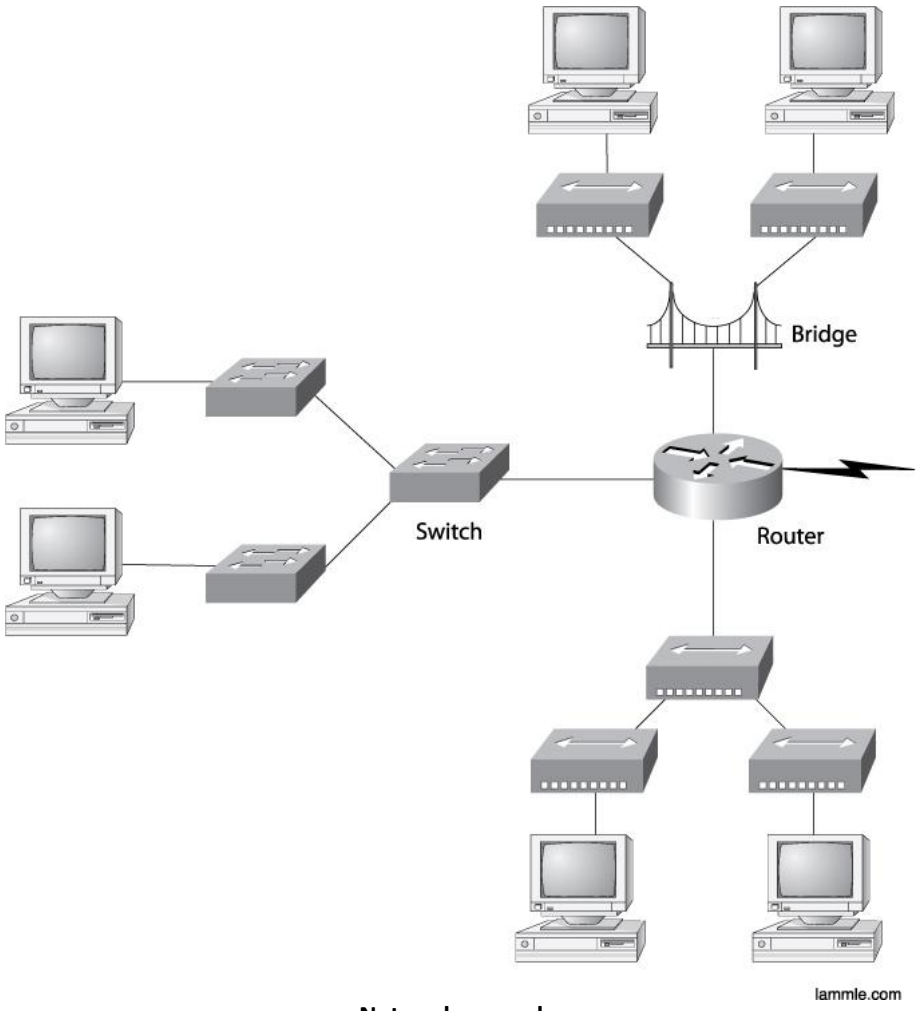
Drawbacks of using switches in a wrong way can include **Broadcast storms.**

❖ **Router**

Routers are devices used to create internetworking and WAN networks. Routers divide both broadcast and collision domains.

Four router functions in your network can be listed as follows:

- Packet switching
- Packet filtering
- Internetwork communication
- Path selection



Network example

** Practice yourself of how many broadcast and collision domain in some network!

Broadcast and Collision domains

With hub networks, When any one pc places data on the wire it is automatically sent to all other ports (pc's) on that hub and any other hubs daisy chained to it. This is a collision domain because another PC could place data on the wire at the same time as another and thus cause a collision. It doesn't matter if either pc is sending unicast or broadcast packets everything gets sent to all ports because that is all a hub does. Hubs are also half duplex devices which means data can only from in one direction at a time.

A switch on the other hand can tell the difference between a broadcast and a unicast packet it receives. If an 8 port switch receives a packet

from one PC destined for another PC (unicast) it only sends that data down the wire the destination PC resides. This is why it's called a switch. It creates a virtual path between two devices. When a switch receives a broadcast it will forward out all ports except the port it received the broadcast on (no point in echoing back what you were just told) Now the reason this does not cause collisions is because switches are full duplex. They send and receive at the same time so it doesn't matter if a pc receives a broadcast at the same time they are sending data.

Unicast , Multicast , Broadcast

Unicast : one device calls another.

Multicast : one device calls a group of the network.

Broadcast : one Device calls all the network.

Categories of Networks

Three categories of Networks

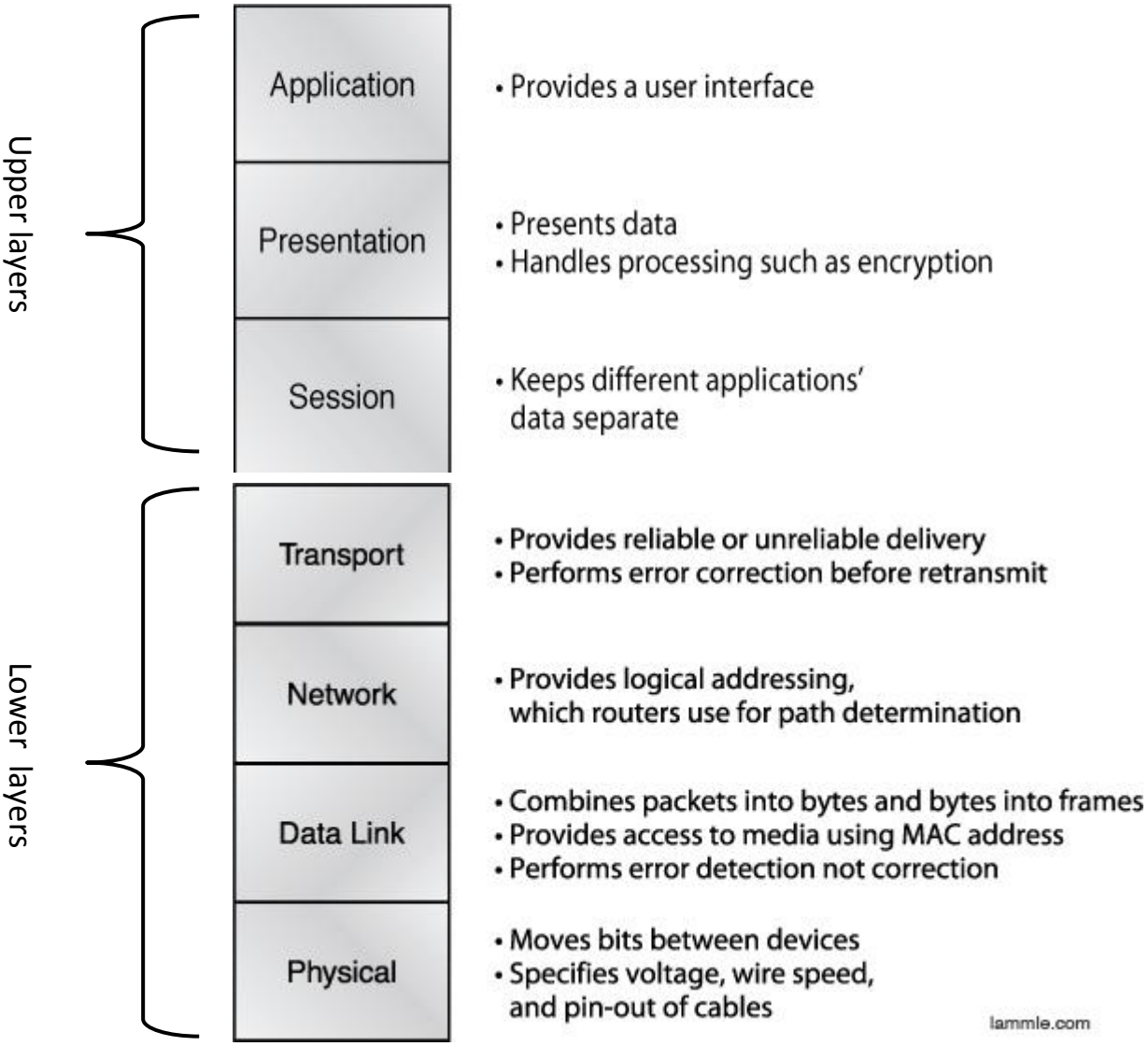
Local Area Network (**LAN**) limited to a few kilometers

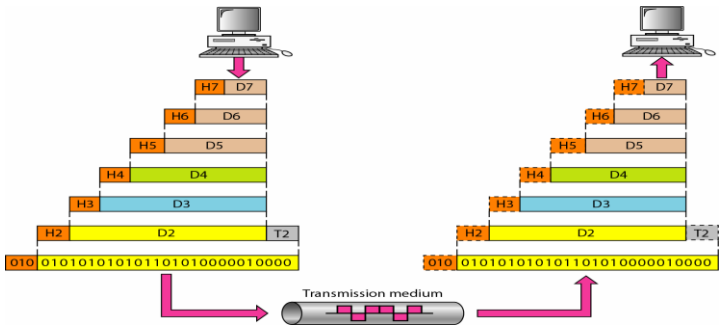
Metropolitan Area Network (**MAN**) tens of miles

Wide Area Network (**WAN**) worldwide.

The OSI Model

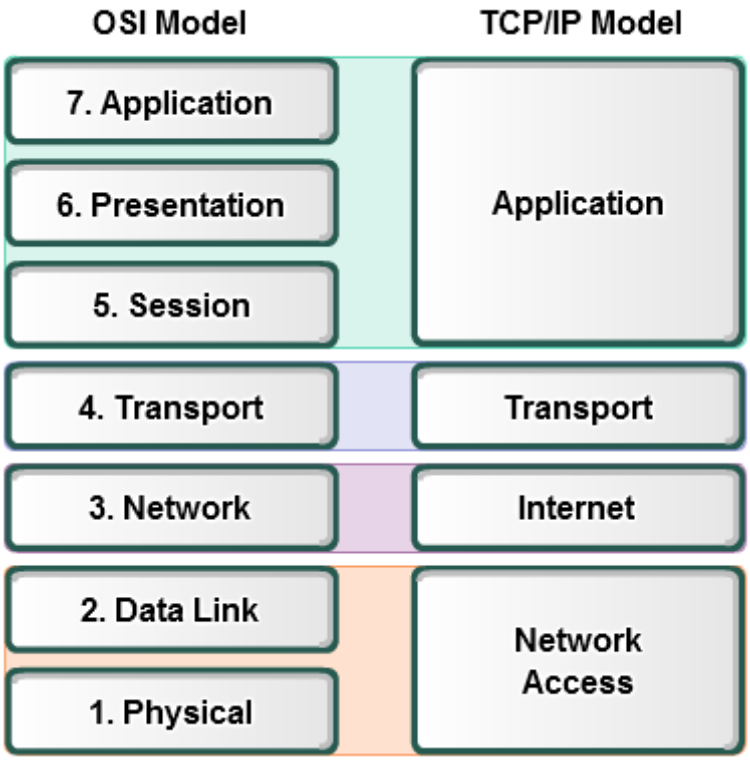
- Open Systems Interconnection (OSI) consists of seven separate but related layers.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.



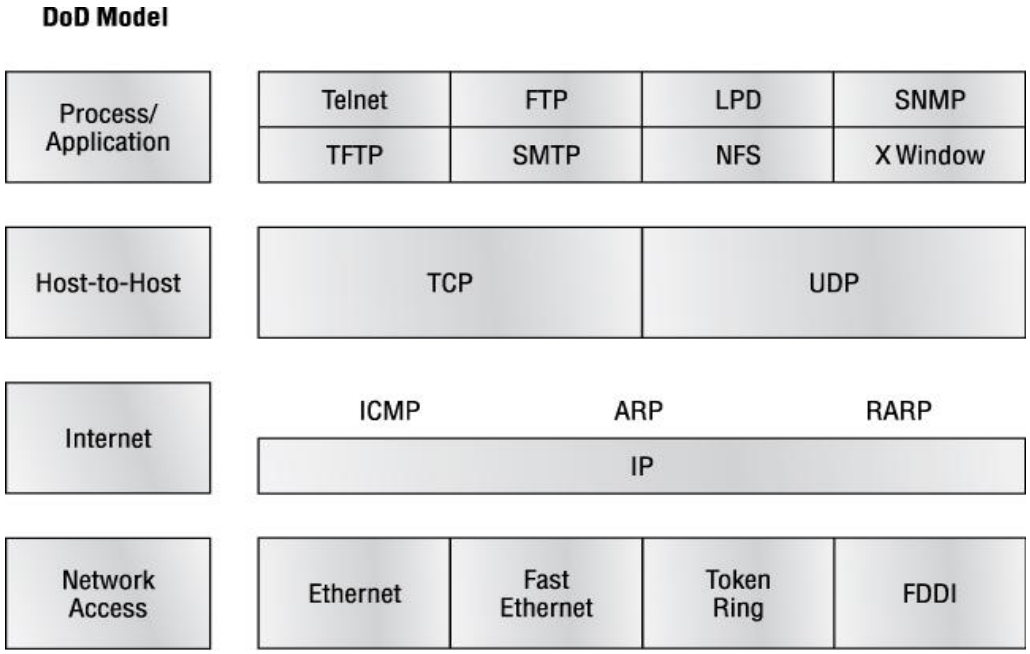


TCP/IP Model (DoD Model)

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a descriptive framework for the Internet Protocol Suite of computer network protocols created in the 1970s by the United States Department of Defense.



The TCP/IP Protocol Suite



**You have to know the uses of all these protocols by the end of semester !

Ports

A port number is a way to identify a specific **process** to which an Internet or other network message is to be forwarded when it arrives at a server.

Well known ports : The port numbers in the range from **0 to 1023** are the well-known ports. They are used by system processes that provide widely-used types of network services

So, when you implement your own network application choose a port number greater than 1023 and less than 65535 (2^{16})

TCP		**UDP**	
Telnet	23	SNMP	161
SMTP	25	TFTP	69
HTTP	80	DNS	53
FTP	21		
DNS	53		
HTTPS	443		

IP Addressing

- An IP address is a numeric identifier(4 bytes) assigned to each machine on an IP network.
- It designates the specific location of a device on the network.
- IP addressing was designed to allow hosts on one network to communicate with a host on a different network regardless of the type of LANs the hosts are participating in.

IP Terminology

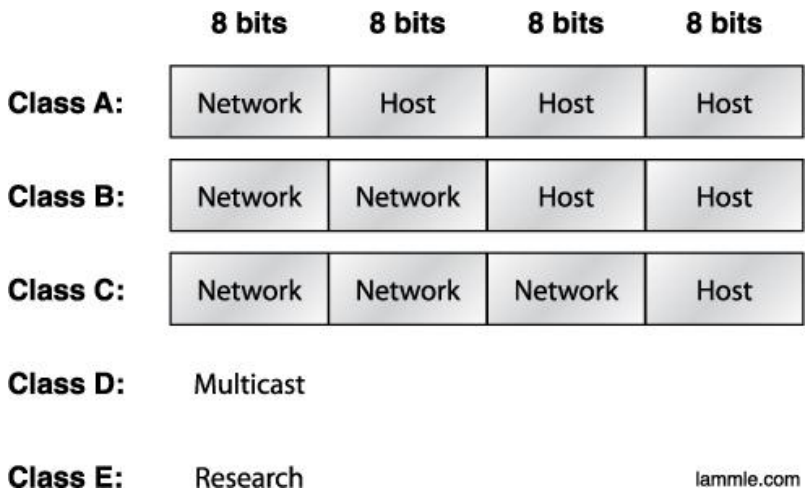
BIT: A bit is one digit, either a 1 or a 0.

BYTE: A byte is 7 or 8 bits, depending on whether parity is used. For the rest of this chapter, always assume a byte is 8 bits.

OCTET: An octet, made up of 8 bits, is just an ordinary 8-bit binary number. the terms byte and octet are completely interchangeable.

Network Addressing

Subdividing an IP address into a network and node address is determined by the class designation of one's network. All devices in a network share the same network address



How to know the class of an IP address?

From the left-most octet

Class A : left-most octet starts with 0
0000 0000 : 0
0111 1111 : 127

Class B : left-most octet starts with 10
1000 0000 : 128
1011 1111 : 191

Class C : left-most octet starts with 110
1100 0000 : 192
1101 1111 : 223

Class D : left-most octet starts with 1110

1110 0000 : 224
1110 1111 : 239

Class E : left-most octet starts with 1111
1111 0000 : 240
1111 1111 : 255

But ,,,

Not all IP addresses in this range are valid

Reserved Addressing

IP	Meaning
Network address of all 0s	Interpreted to mean “this network or segment.”
Network address of all 1s	Interpreted to mean “all networks.”
Network 127.0.0.1	Reserved for loopback tests (localhost)
Node address of all 0s	Interpreted to mean “network address”
Node address of all 1s	“all nodes” on the specified network
Entire IP address set to all 0s	default route.
Entire IP address set to all 1s	Broadcast to all nodes on the current network

Summery

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0
D	224-239	11100000-11101111	NA (multicast)	
E	240-255	11110000-11111111	NA (experimental)	

Private and public addressing

- Ideally, all PC at the world will have an IP address, but since IP addresses are 4 bytes long then the total IP addresses = 2^{32} =4,294,967,296 IP (small number comparing to number of PCs !)
- Private IP addresses are used to enable us to reuse an IP address in many locations.
- Under one public IP address we could run a complete network without having to assign an IP to every single PC.
- IP addresses can be used in private network but they are not routable through the Internet.
- To map Private to Public IPs and vice versa we use NAT (Network Address Translation).

Private Address Ranges

Address Class	Reserved Address Space
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255