LECTURE 3

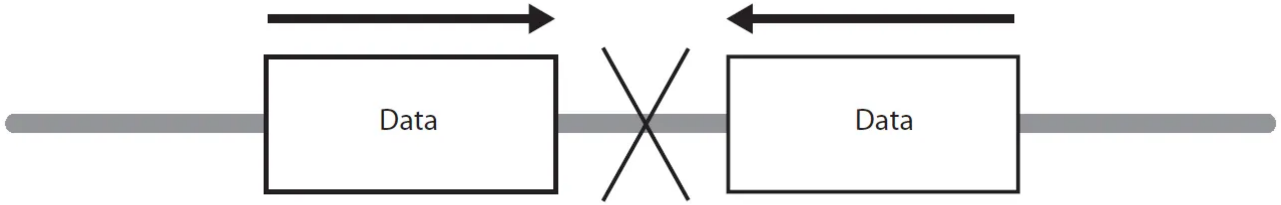
Dr. Mai Zaky

Overview of Networking Equipment

- **Broadcast domain** A data frame sent to every device on a network segment at the same time.
- Too many broadcasts in a network can cause
  - delays
  - reduce performance.
- A broadcast is usually sent when a data frame is trying to find a host in the network and doesn't know its current location.

- **Collision domain**, is an Ethernet term used to describe a network scenario wherein one device sends a packet on a network segment ,forcing every other device on that same segment to pay attention to it.

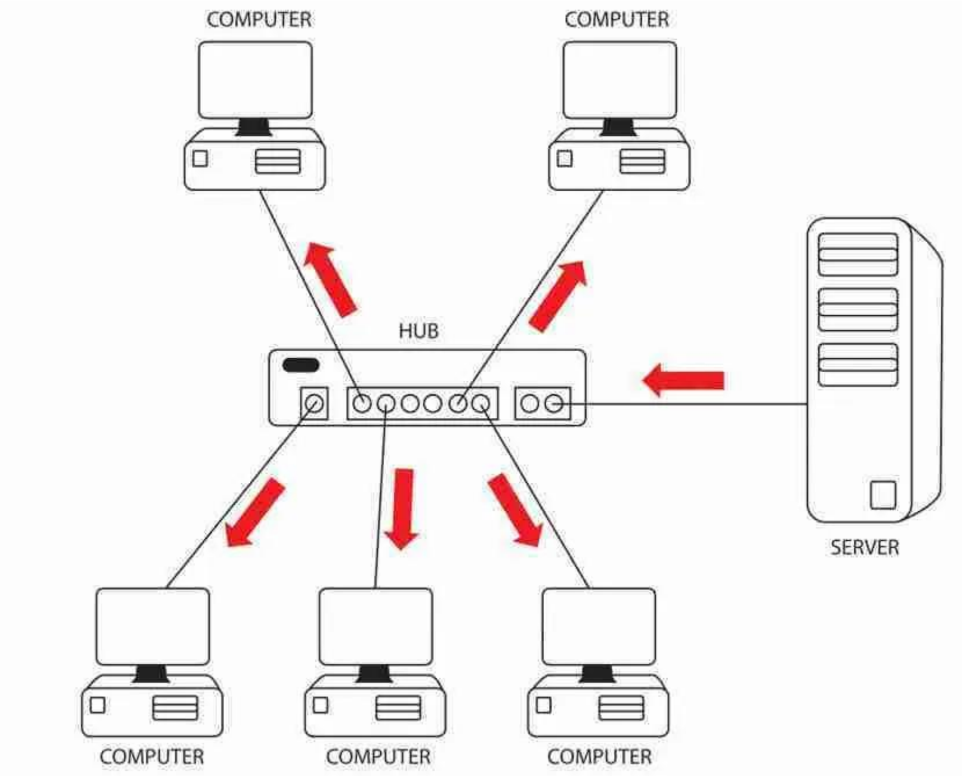
- At the same time, a different device tries to transmit, leading to a collision, after which **both** devices must **retransmit**, one at a time



Overview of Networking Equipment

Hub

- Hubs are **fairly rare nowadays**, they explain why we needed to change the way traffic is sent across a Local Area Network (LAN).
- A hub simply allows several networking devices to communicate.
- Each device plugs into a port on the hub using a network cable.
- Hubs have **no memory** or **hard drive**, so they **can never remember which device is plugged into which port.**
- When a hub receives data on one port, it just **forwards** it to **all the other ports**.
- This **causes a lot of unnecessary traffic** to pass through the network.

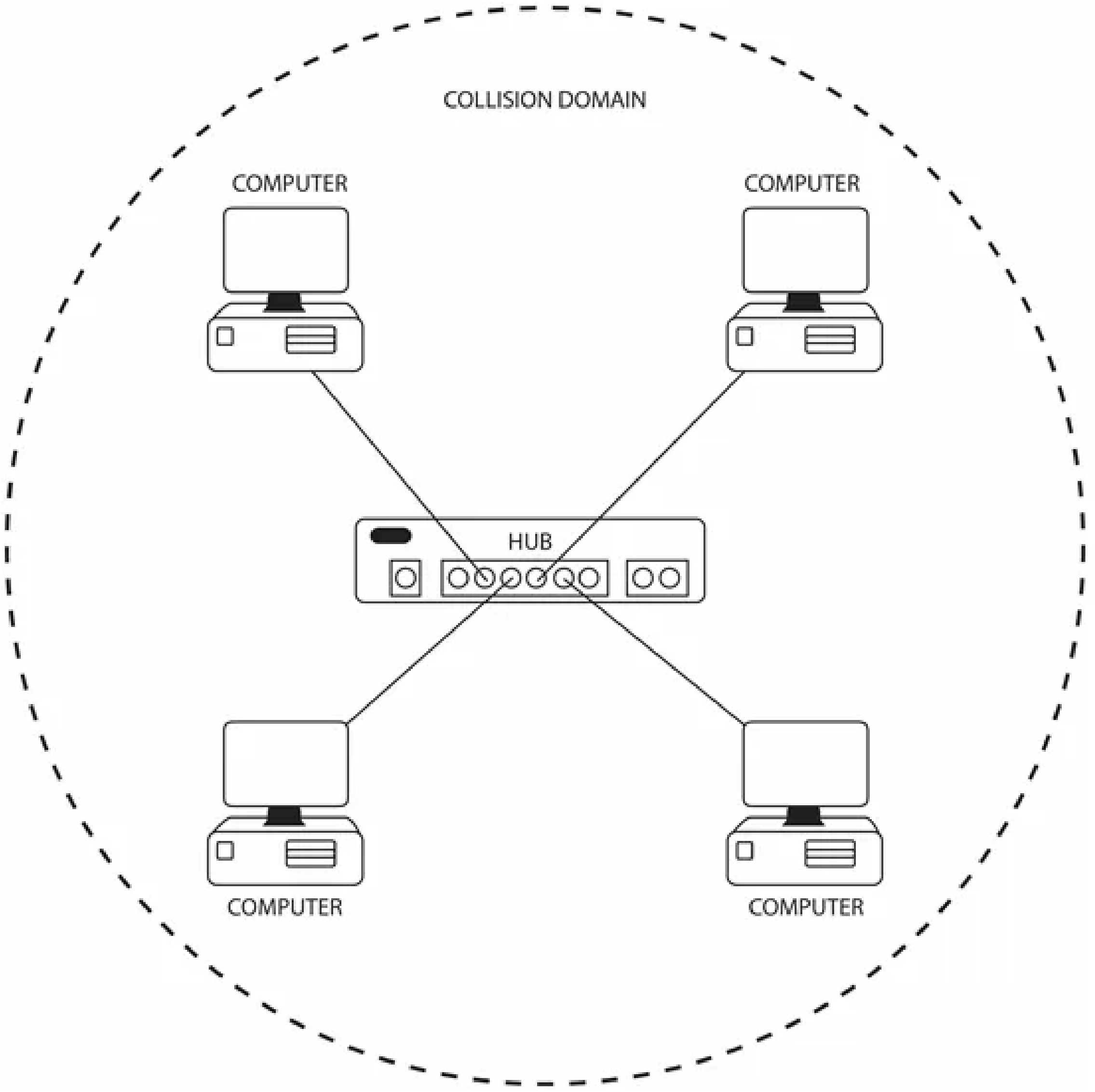


Every frame is received by every device when a hub is used

Overview of Networking Equipment

Hub

- A network hub that has created **one collision domain** (it's also **one broadcast domain** because there are no VLANs or routers present).
- If you ever see a hub in a network diagram referring to collision and broadcast domains, remember that the hub does not increase the number of collision domains or reduce the number of broadcast domains.

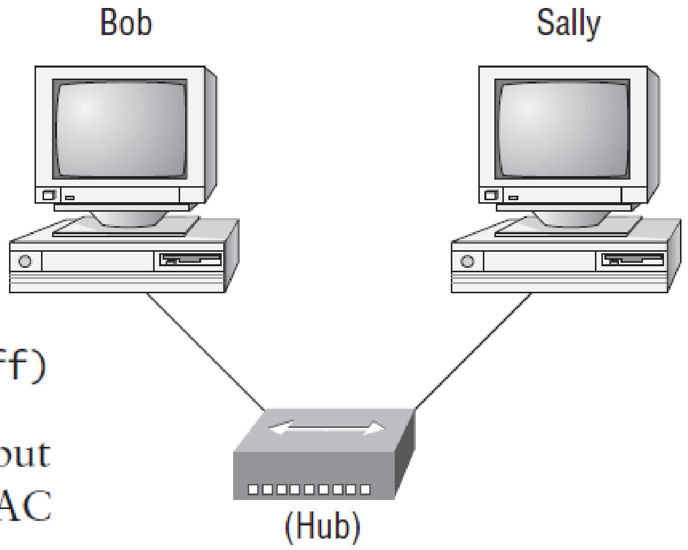


Hubs are in one collision domain

The basic network

This network is actually one collision domain and one broadcast domain.

Bob is actually going to use Sally’s MAC address (known as a hardware address), which is burned right into the network card of Sally’s PC



The basic network allows devices to share information.
The term computer language refers to binary code (0s or 1s).
The two hosts above communicate using hardware or MAC addresses.

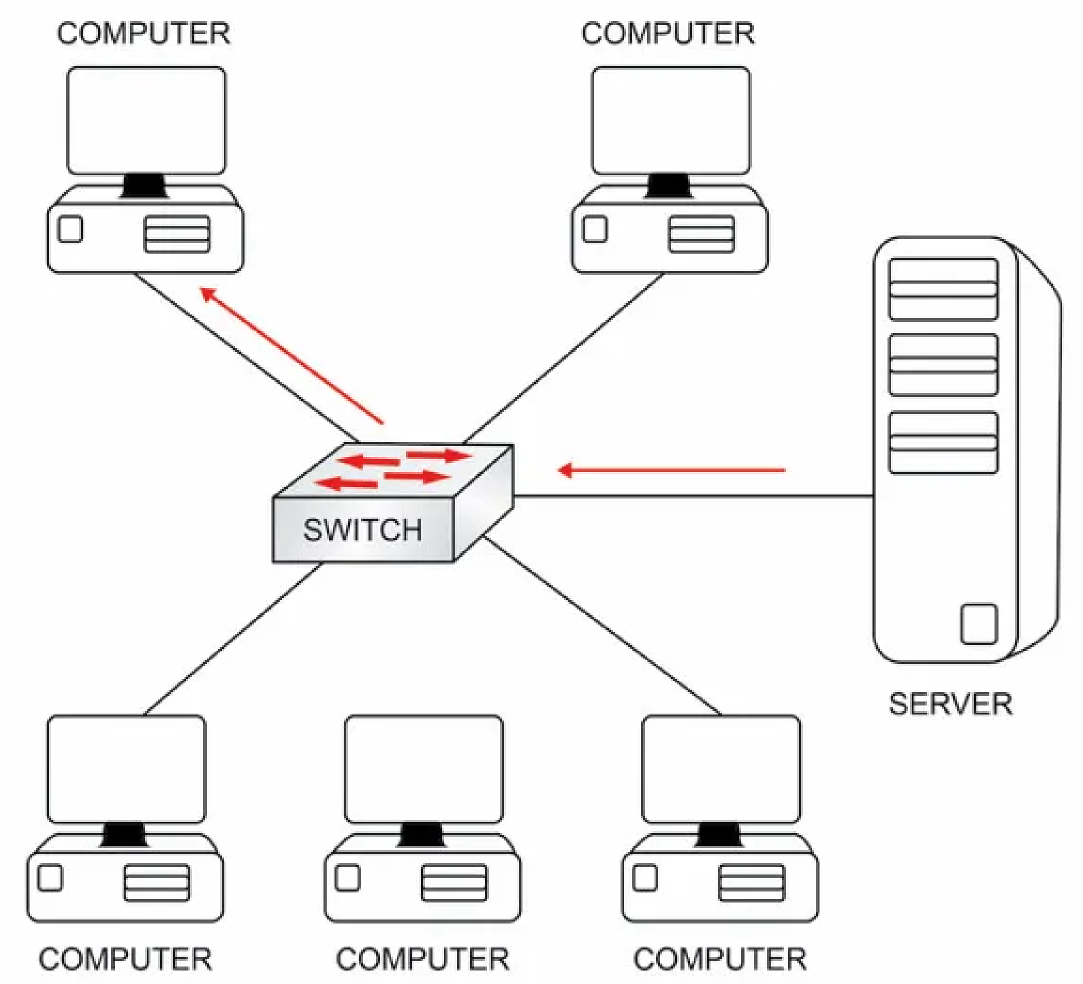
```
EthernetII,Src:192.168.0.2(00:14:22:be:18:3b),Dst:Broadcast (ff:ff:ff:ff:ff:ff)
```

What this output shows is that Bob knows his own MAC address and source IP address but not Sally’s IP address or MAC address, so Bob sends a broadcast address of all *f*s for the MAC address (a Data Link layer broadcast) and an IP LAN broadcast of 192.168.0.255.

Overview of Networking Equipment

Switch

- Switches operate by building a list **of which PCs are connected to which ports**, allowing the available bandwidth to be used a lot more efficiently.
- If a PC wants to send data to another PC via a switch, the switch will **forward the traffic only** to the port to which the intended recipient is connected.
- **If it doesn't know the port, it will send out a broadcast** to find out where in the network the PC is.
- Switches and hubs are designed to forward broadcast traffic as data frames addressed to every device in the network.

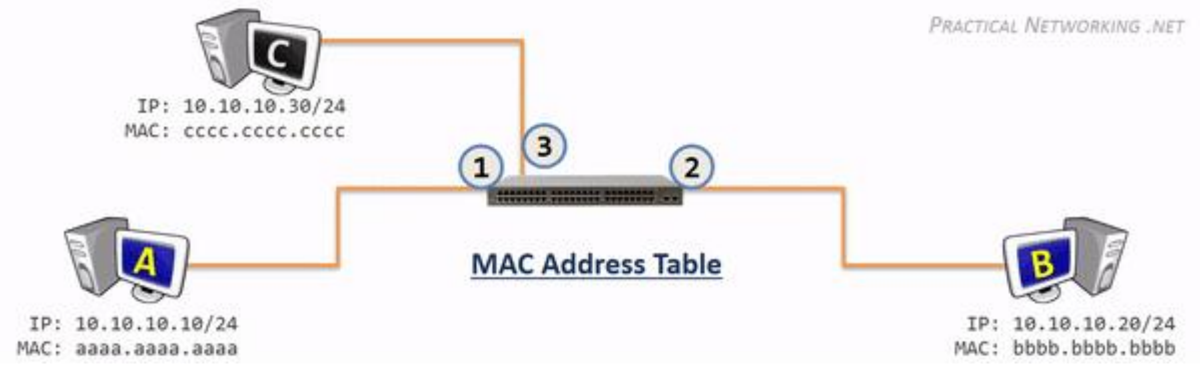


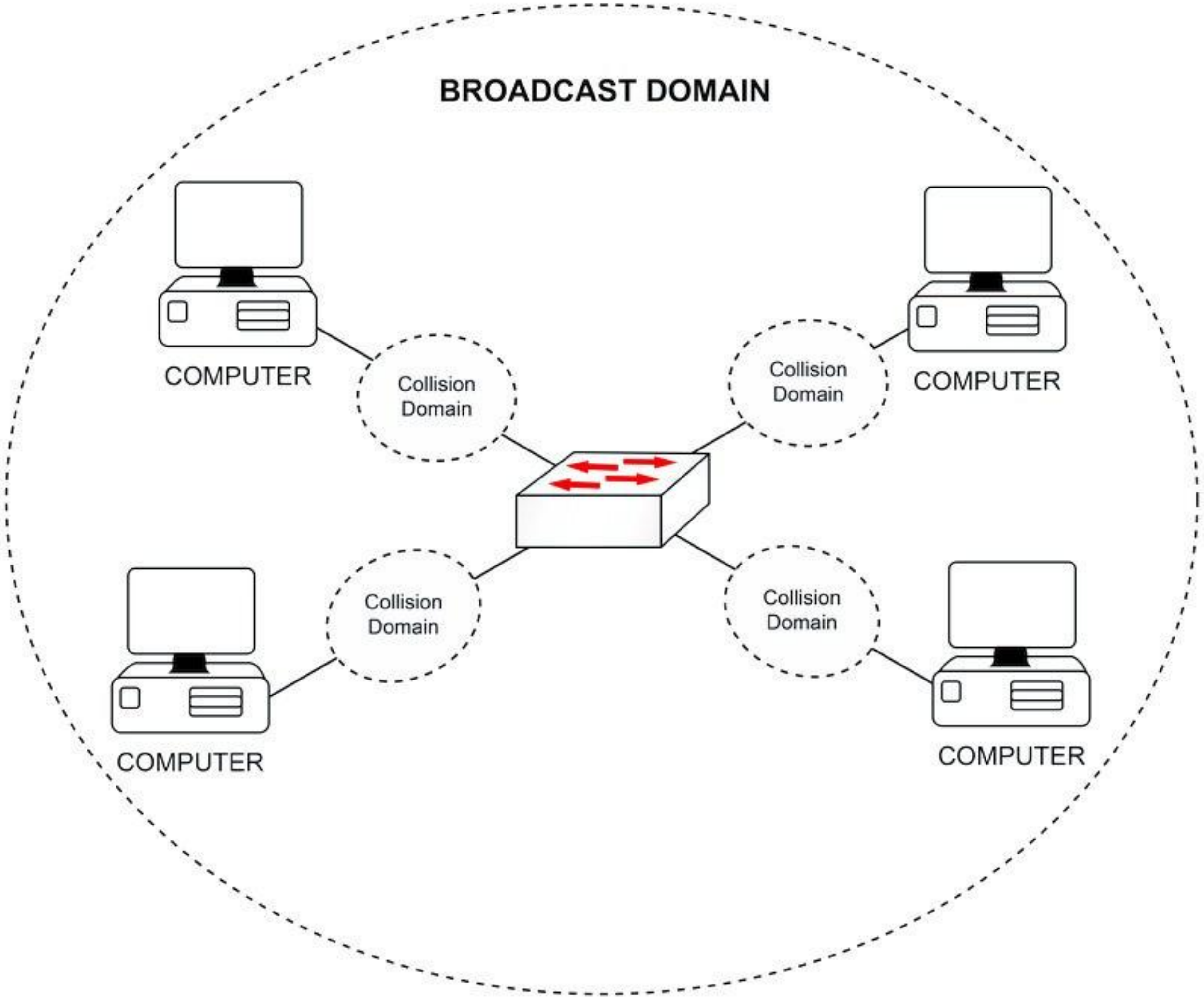
Switches forward frames only to the relevant port

Overview of Networking Equipment

Switch

- If you swapped the hub for a switch, you would have four collision domains (one per port used). All devices would still be in the same broadcast domain though.

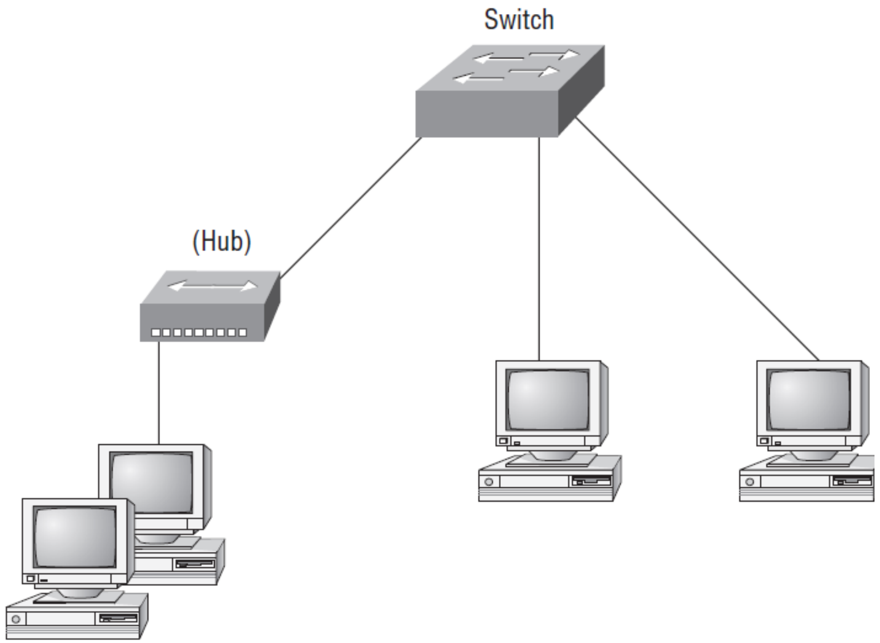




Each switch port creates a collision domain

Network segmentation

- Breaking the big network into a number of smaller ones, by using devices like routers, switches and bridges.
- Each network segment connected to the switch is **now a separate collision domain**
- But this network is still **one broadcast domain**.
- We replace the main hub with switch, because hubs don't segment a network, they just connect network segments together.
- Routers break up a broadcast domain - the set of all devices on a network segment that hear all the broadcast sent on that segment.



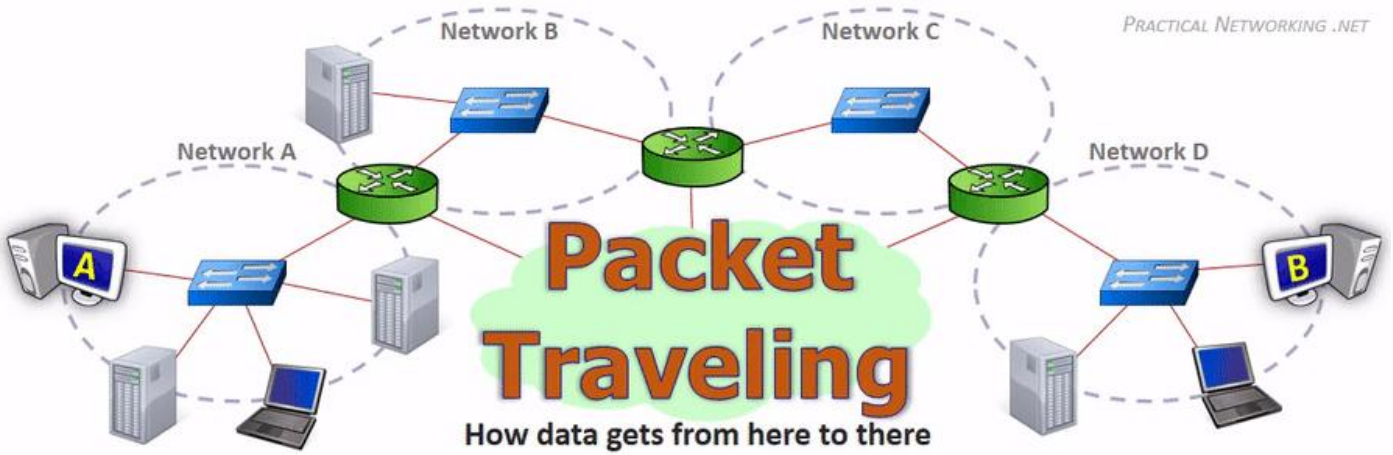
NOTE

Switches create separate collision domains but a single broadcast domain. Routers provide a separate broadcast domain for each interface.

Overview of Networking Equipment

Router

- A router is designed to **store** a directory of networks. Rather’s job is to find out **where** different networks are.
- It then sends the traffic via the **best path**. This path could be the **fastest**, most **reliable**, or **shortest**, or a **combination of these features**, depending on how you want traffic to be sent as the network administrator.
- If the router does not know how to get traffic to its intended destination, it will **either drop** the packet or **forward it to another router** that should know how to get it there.



Overview of Networking Equipment

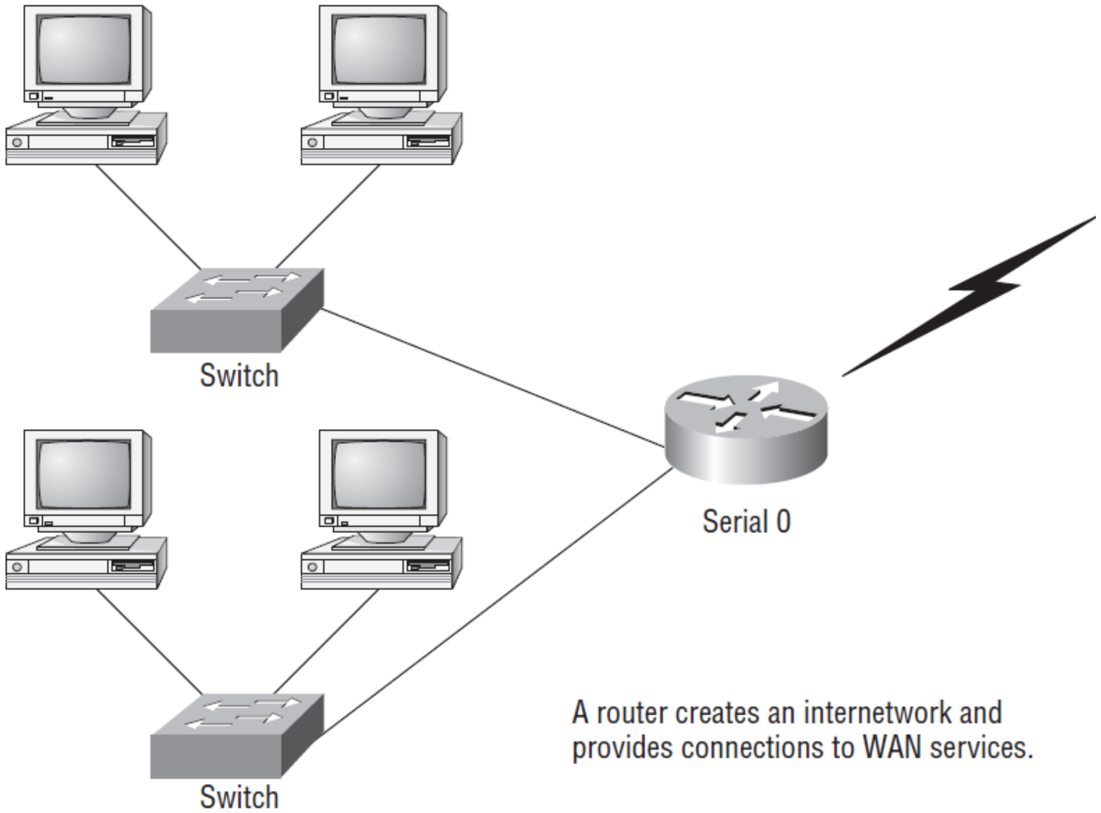
Router

- It is important to remember that by default, routers **do not forward broadcasts**.
- Because they do not forward broadcast information, routers are used to create broadcast domains. Broadcasts in the network will stop at the router (unless you configure it to forward them, which isn't recommended)

- **Remember** that switches segment collision domains. Every port on the switch is a separate collision domain.
- **Remember** also that routers segment broadcast domains, and every port on the router is a separate broadcast domain.
- **Finally**, all the ports in a hub are in ONE collision domain, while all the ports in a switch are in the same broadcast domain.

Network segmentation

- Each host is connected to **its own collision domain**
- The router has created **two broadcast domain.**
- Also the router provides connections to WAN services.

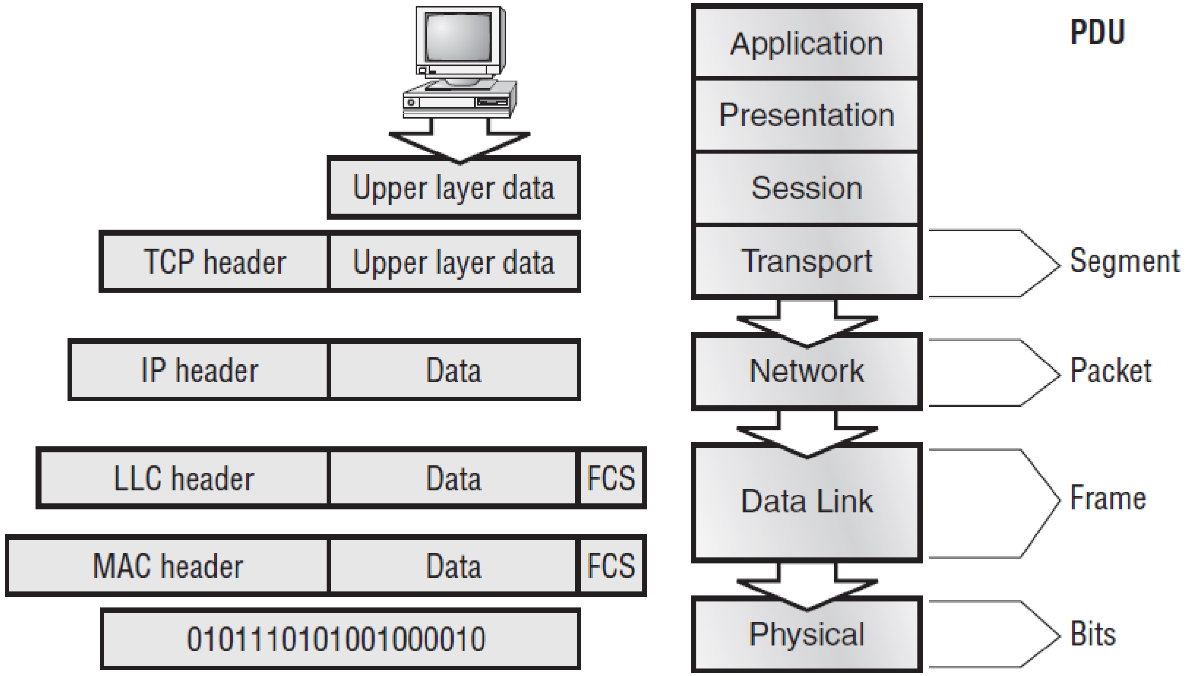


A router creates an internetwork and provides connections to WAN services.

Breaking up a broadcast domain is important because when a host or server sends a network broadcast, every device on the network must read and process that broadcast—unless you've got a router. When the router's interface receives this broadcast, it can respond by basically saying, discard the broadcast without forwarding it

Data Encapsulation

- As data passes down each OSI layer, a **new header** is added to it; this process is called **encapsulation**.
- **The header contains information about how the data should be treated by the receiver.**
- As data is encapsulated while moving down the layers, it will be known by a **different name.**
- When the data is received at the destination, it is then **de-encapsulated**, a **process that removes each header**, and then the information is passed up to the next layer.



Upper layer data

TCP header | Upper layer data

IP header | Data

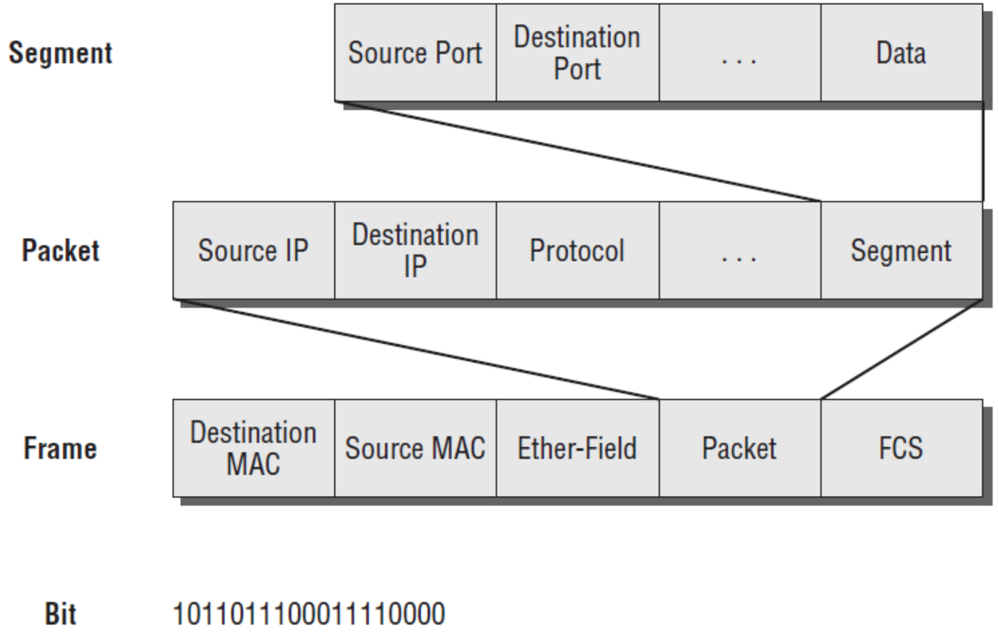
LLC header | Data | FCS

MAC header | Data | FCS

0101110101001000010

Application
Presentation
Session
Transport
Network
Data Link
Physical

PDU
Segment
Packet
Frame
Bits



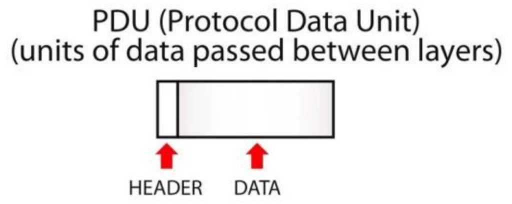
Segment: Source Port | Destination Port | . . . | Data

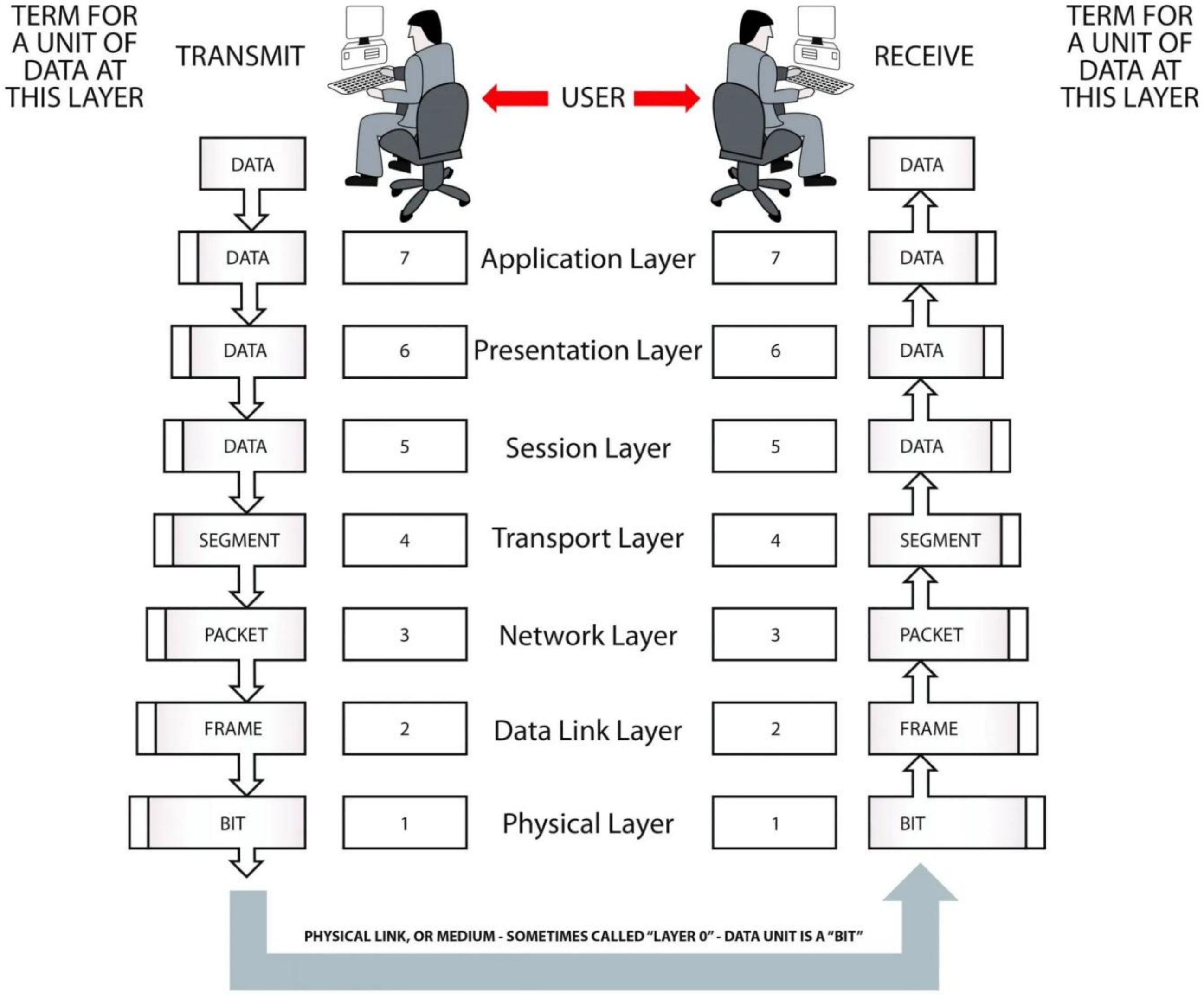
Packet: Source IP | Destination IP | Protocol | . . . | Segment

Frame: Destination MAC | Source MAC | Ether-Field | Packet | FCS

Bit: 1011011100011110000

Data Encapsulation





Application Layer

- Where most **users interact with the network**. The Application Layer interface directly interacts with application and **provides common web application services** such as web browser, email clients and file transfer.

- There are many services that operate at the application layer :
  - ✓ **World Wide Web (WWW)** – connects millions of users to servers and provides multimedia functions such as text, graphics, and sound
  - ✓ **E-mail (SMTP, POP)** – the standard used to send and receive e-mail all over the world
  - ✓ **File Transfer Protocol (FTP)** – provides a means to upload and download large files over networks.
  - ✓ **Telnet** – used to connect to networking devices remotely (connect to networking equipment many miles away from the actual physical location)

Presentation Layer

- The function of the presentation layer is to **present data to the application layer.**
- It converts coded data into a format the application layer can understand.
- It is also responsible for **data encryption**, **data decryption**, and, finally, **data compression**.

Session Layer

- In the session layer, **sessions or dialogs** between applications are **set up**, managed, and eventually terminated.
- A session is coordinated and synchronized to **prevent different applications**' data from becoming **mixed up during transfer**.

Transport Layer

- The transport layer takes data from the upper layers, **breaks it into smaller units** called **segments**, and **adds** logical transport information in the **header**.

- Before communication can take place, an end-to-end logical connection called a **virtual circuit** has to be established.

- The transport layer includes several protocols,
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

- which are a part of the TCP/IP (Internet Protocol) suite of protocols. The TCP/IP suite is the standard suite on which most of the Internet operations are based.

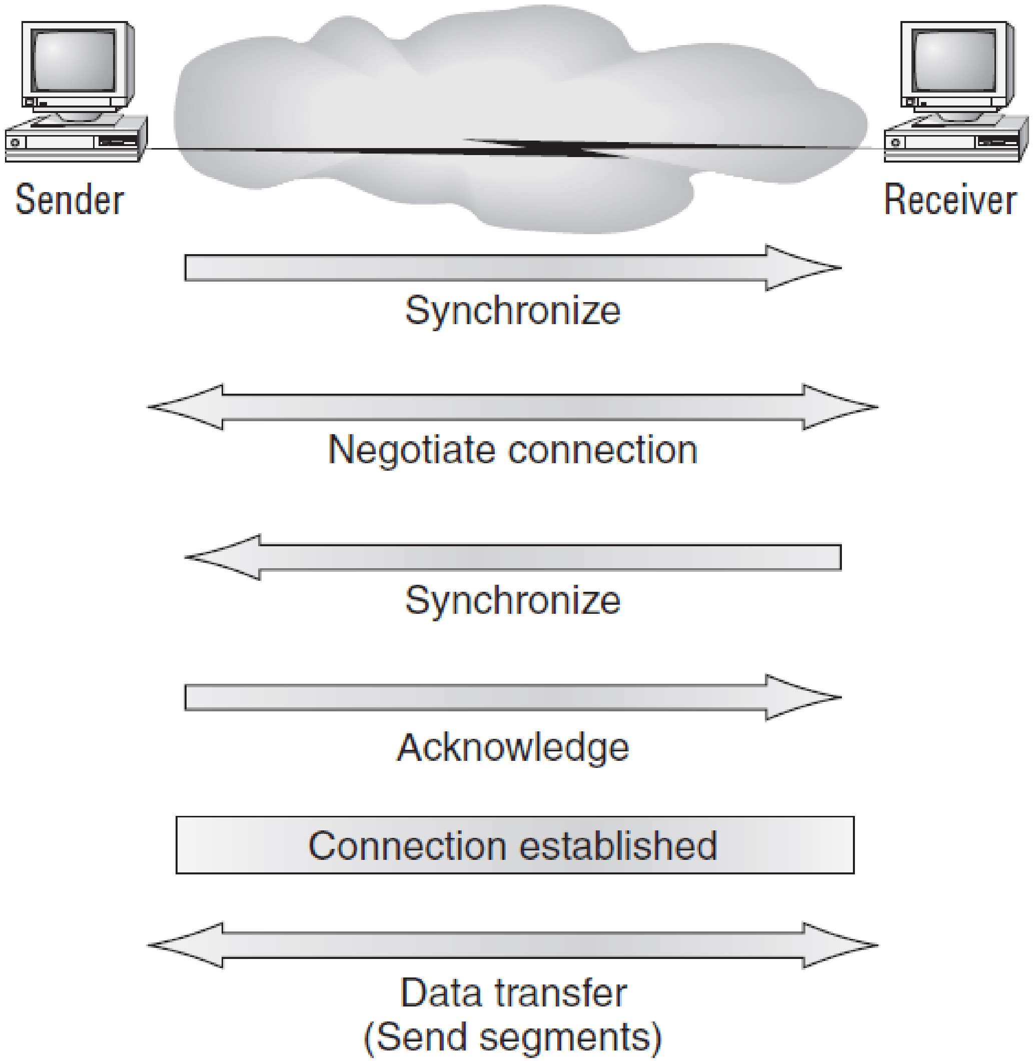
Transport Layer

Transmission Control Protocol (TCP)

- TCP is considered a **reliable connection-oriented** protocol.
- It uses reliable mechanisms to initiate and terminate connections.
- Many application layer protocols use TCP as the transport protocol. Some of them include **Telnet**, **HTTPS** (Hypertext Transfer Protocol Secure), and **FTP** (although they sit at the application layer, they do use TCP).

- In TCP, a **logical end-to-end connection** is achieved by each end-system agreeing that a connection is about to be initiated. This process is known as a **three-way handshake**.
- Data transfer using TCP as the transport protocol is considered to be reliable. This means that there is a guarantee that the data sent will reach the intended destination. This is accomplished by using three methods:
    - Flow control
    - Windowing
    - Acknowledgments

The Transport Layer
Connection-Oriented Communication

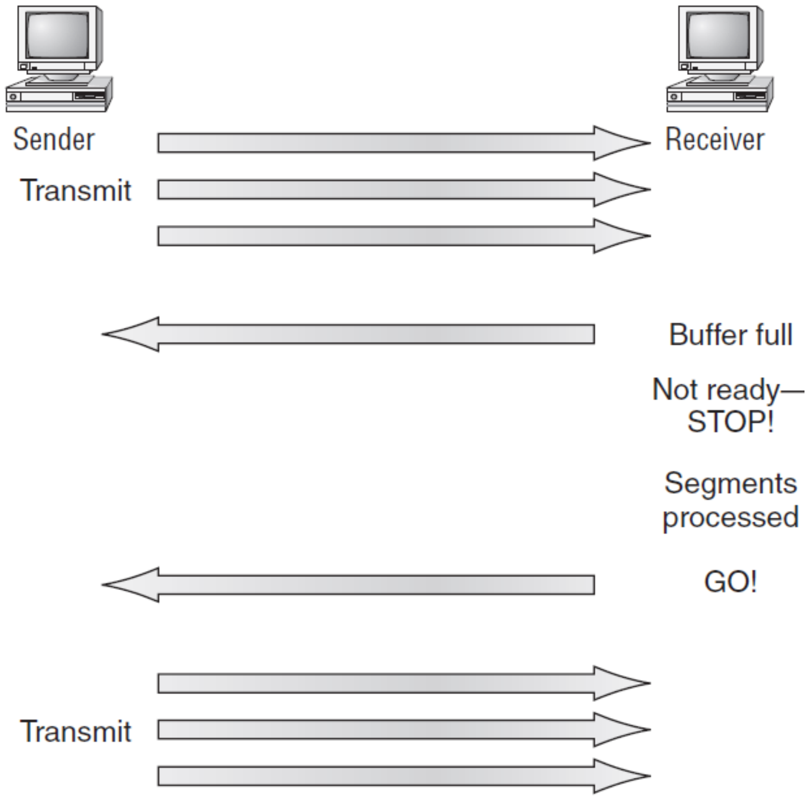


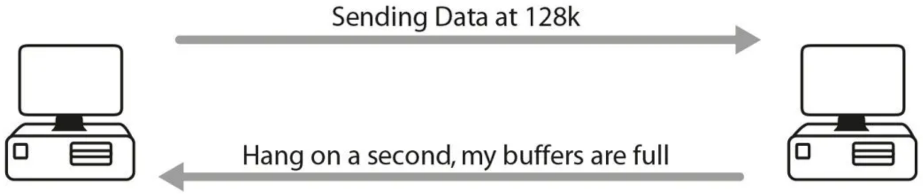
Transport Layer

Transmission Control Protocol (TCP)

Flow control

- If the receiver is sent more information than it can process, it will ask the sender to stop for a short while.
- An example of when this can occur is when both sides are using **different speeds**.



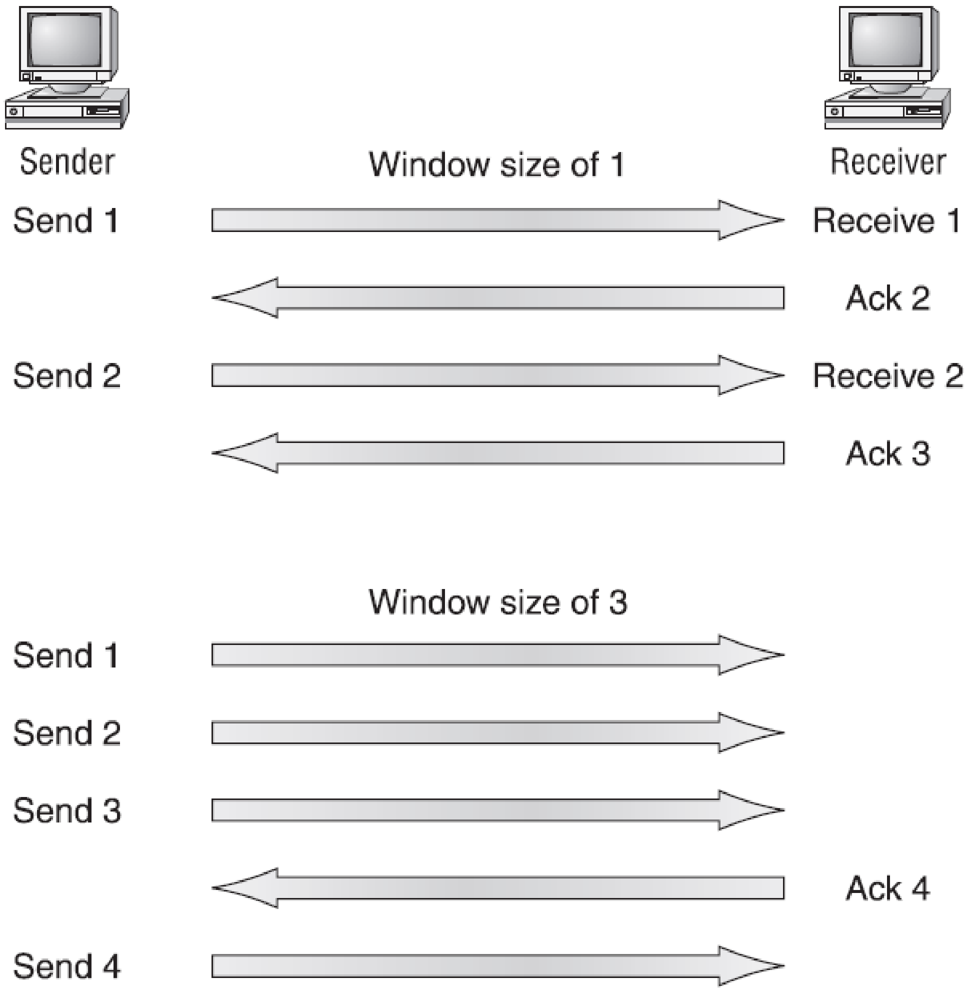


Transport Layer

Transmission Control Protocol (TCP)

Windowing

- The TCP window is the **amount of data that can be sent before an acknowledgment is required from the receiver.**
- The sender and receiver agree on the window size, and this can be scaled up and down as required.

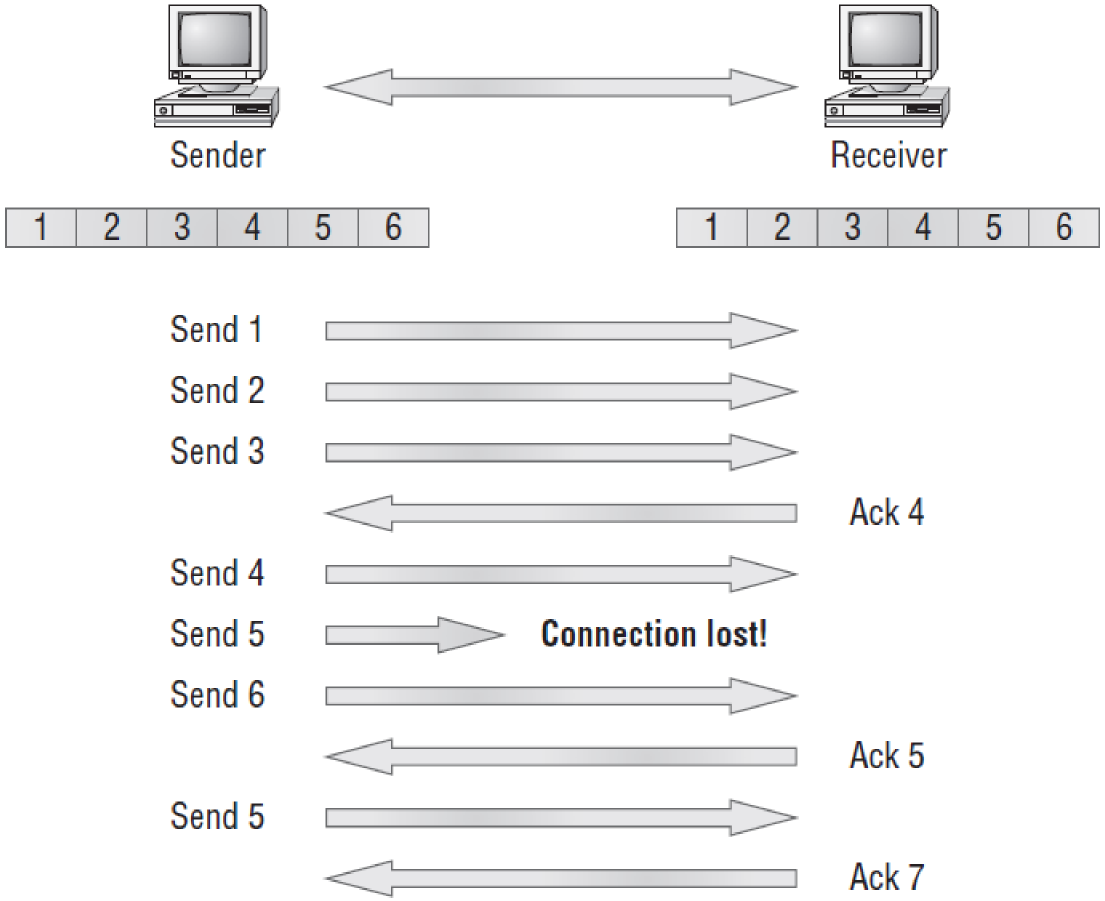


Transport Layer

Transmission Control Protocol (TCP)

Acknowledgement

- Acknowledgments are **messages indicating the successful receipt of TCP segments**.
- If a sender does not receive acknowledgments for the segments sent after a certain period, then it knows there is something wrong.



Transport layer reliable delivery

Transport Layer

User Datagram Protocol (UDP)

- UDP, on the other hand, is a **connectionless** protocol.
- In other words, it **does not care** about **sequencing** or **acknowledgments**, and it does not have all the fancy mechanisms that TCP uses to ensure that its segments reach their **destination safely**.
- This means that applications using UDP must be responsible for their own reliability.

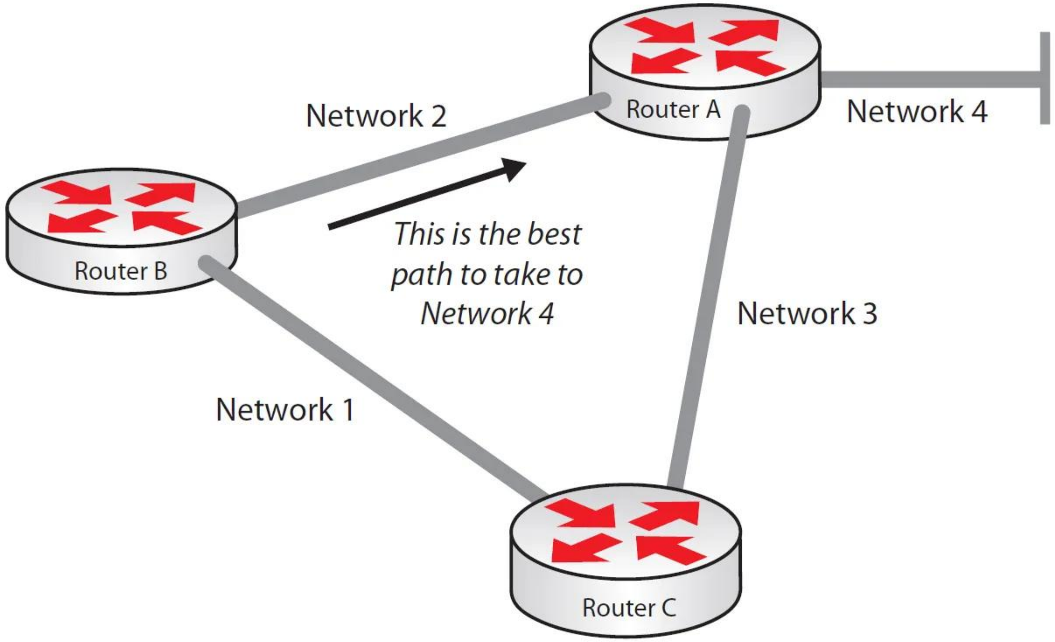
Why is UDP used at all?

- Unlike TCP, UDP is **lightweight**. Because it does not have to initiate a connection using a three-way handshake, UDP can be used for applications where **speed and bandwidth are a concern.**
- In some cases, these issues are more important than the reliability that TCP provides.
- Protocols carried on UDP include SNMP (Simple Network Management Protocol) and TFTP (Trivial File Transfer Protocol).

The Network Layer

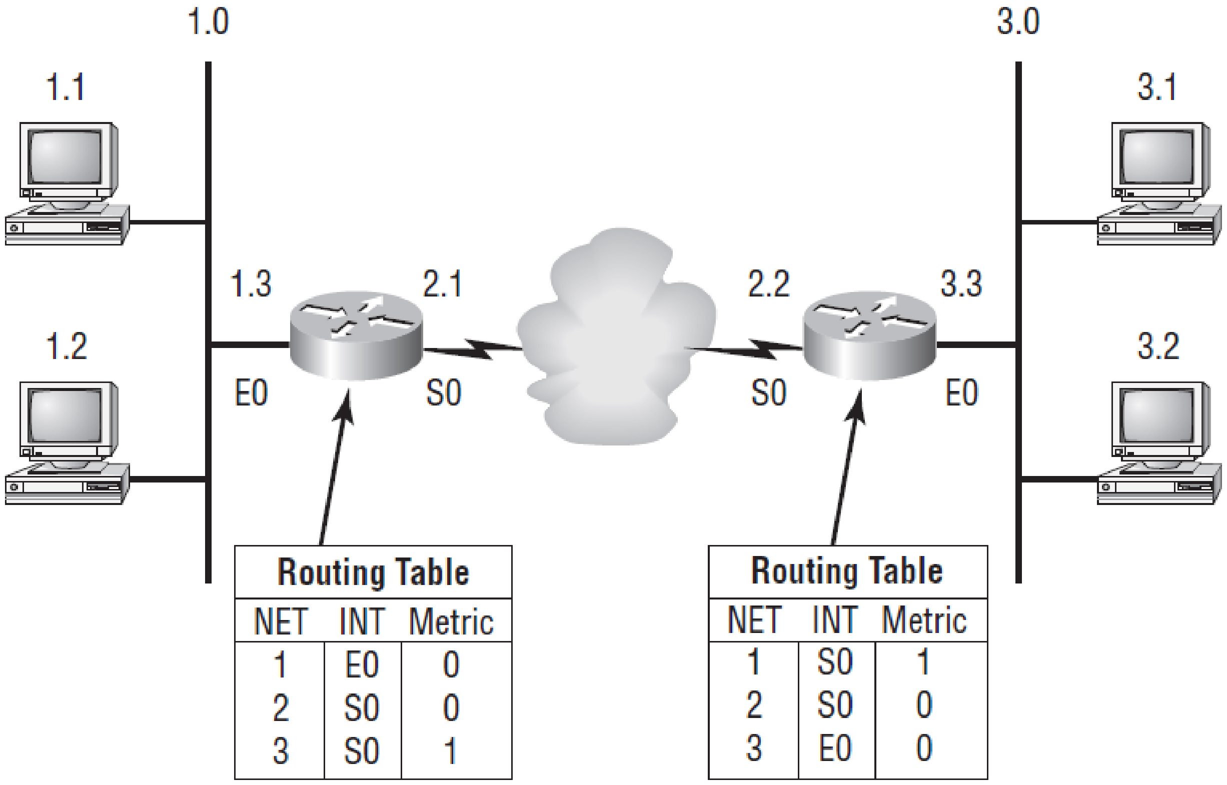
- The role of the network layer is to determine **the best path** or route for data to take from one network to another.
- Data are assembled into packets at this layer.

- logical addressing also takes place at the network layer.
- The most popular form of network addressing today is IP addressing using IPv4 or IPv6.



The Network Layer

- **Routers** (layer 3 devices) are specified at the Network layer and provide the **routing services** within an internetwork.
- Each router stores a table of which networks are directly connected and how to get to the networks that are not.
- When a packet arrives at a router interface, the router looks at the destination network address and decides whether that network is directly connected. If it is not, the router looks at its routing table to see which exit interface it should leave by.



Routing Table

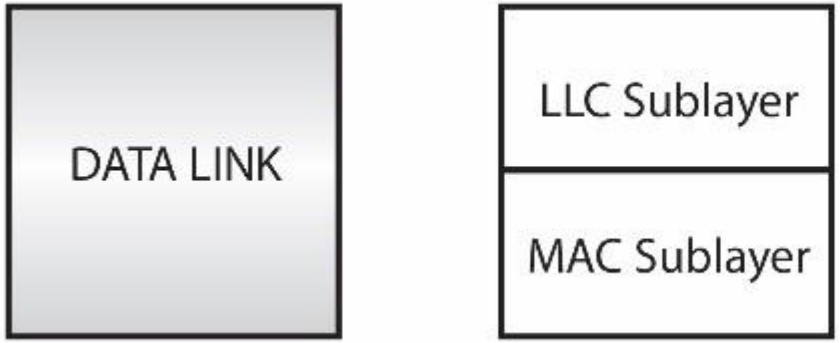
NET	INT	Metric
1	E0	0
2	S0	0
3	S0	1

Routing Table

NET	INT	Metric
1	S0	1
2	S0	0
3	E0	0

Data Link Layer

- The data link layer is divided into two sublayers—LLC and MAC
- The data link layer **takes packets from the network layer and divides them into smaller units known as frames**.
- Frames are then transported across a physical medium (i.e., wires).
- The data link layer has its own way of addressing known as **hardware addressing**. While the network layer determines where **networks** are located, **the data link layer determines where hosts are located on a particular network.**
- The MAC address allows devices to have a unique layer 2 address and allows communication to take place at layer 2 Switches.
- The MAC, or hardware, address is a 48-bit (6-byte) address written in a hexadecimal format.



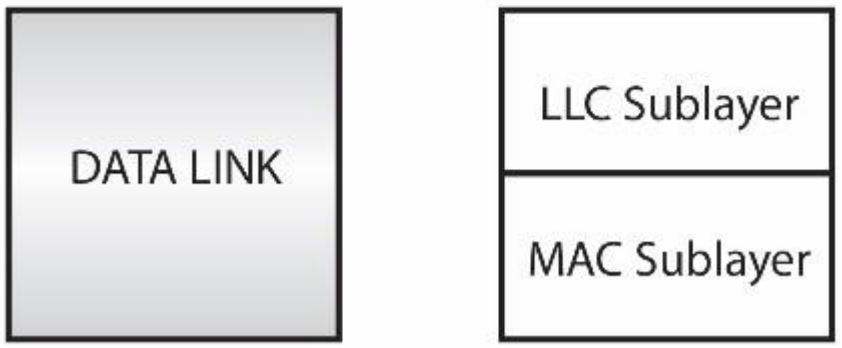
Data Link Layer

Logical Link Control Sublayer (IEEE 802.2)

- The LLC sublayer **interfaces with the network layer**
- Identifies network protocols, performs **error checking** and **synchronizes frames**

Media Access Control Sublayer (IEEE 802.3)

- The MAC layer directly interfaces with the physical layer. This is **where the physical address of the interface or device is stored.**
- A MAC address is a 48-bit address expressed as 12 hexadecimal digits.
- This address identifies **both the manufacturer** of the device and the **specific host**.



Physical Layer

- The physical layer takes frames from the data link layer and converts them into bits.

- The physical layer has to use bits (binary digits) since data on a wire can be sent only as a pulse of electricity or light—that is, only as one of two values, either a 1 or a 0

- **Hubs operate at the physical layer** of the OSI model. Hubs take the bits, strengthen the signal if it has been degraded, and send them out to every device connected to the ports.

Binary to Decimal and Hexadecimal Conversion

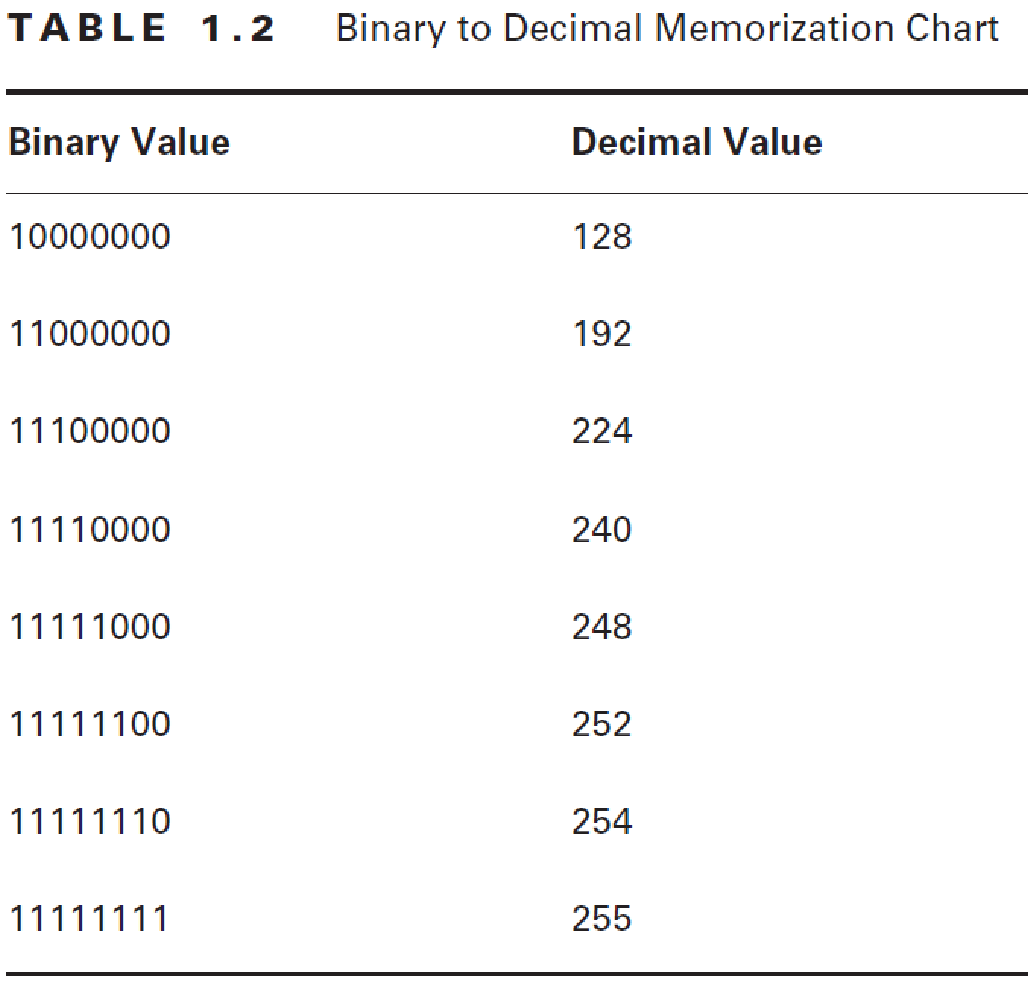


TABLE 1.2 Binary to Decimal Memorization Chart

Binary Value	Decimal Value
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

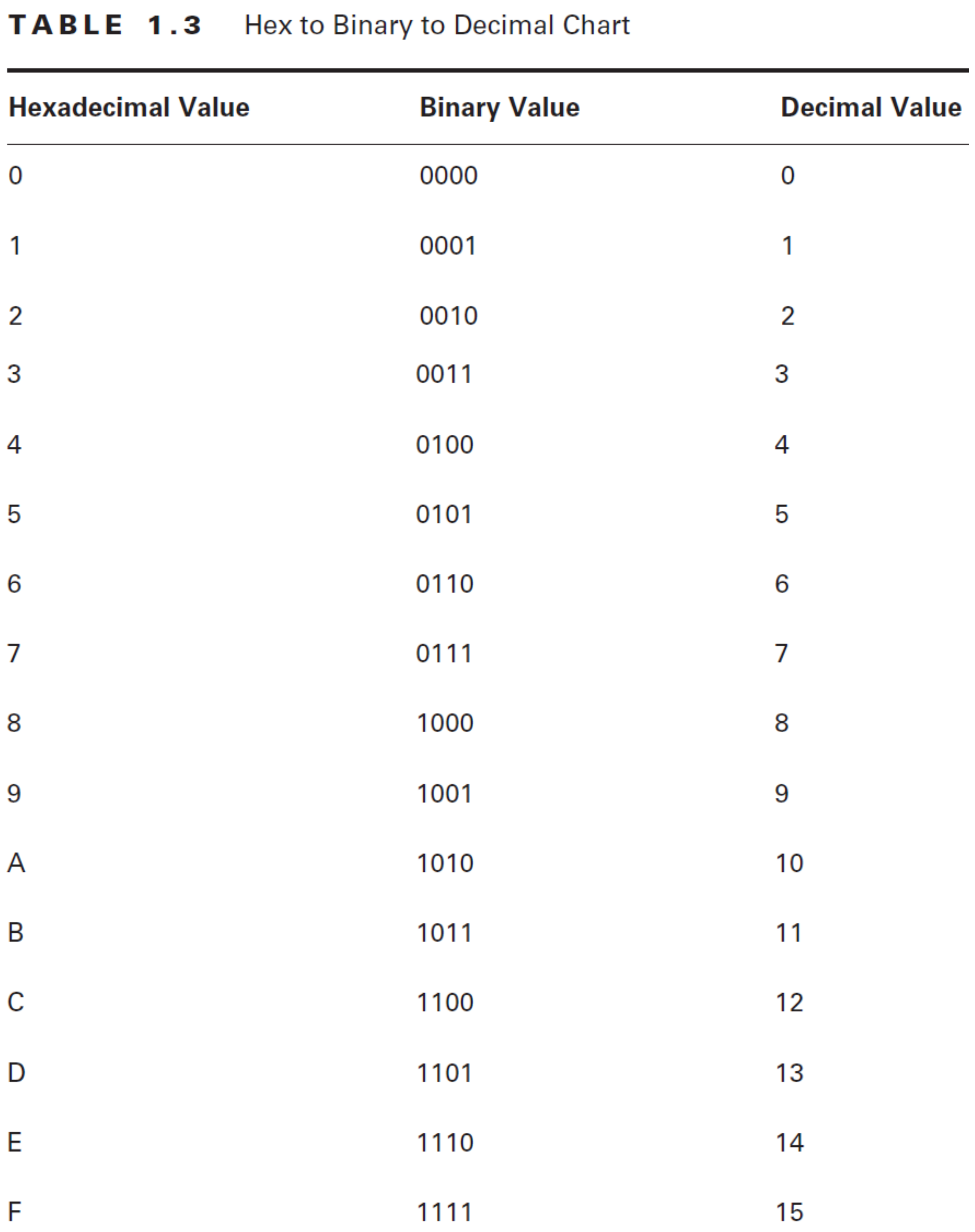
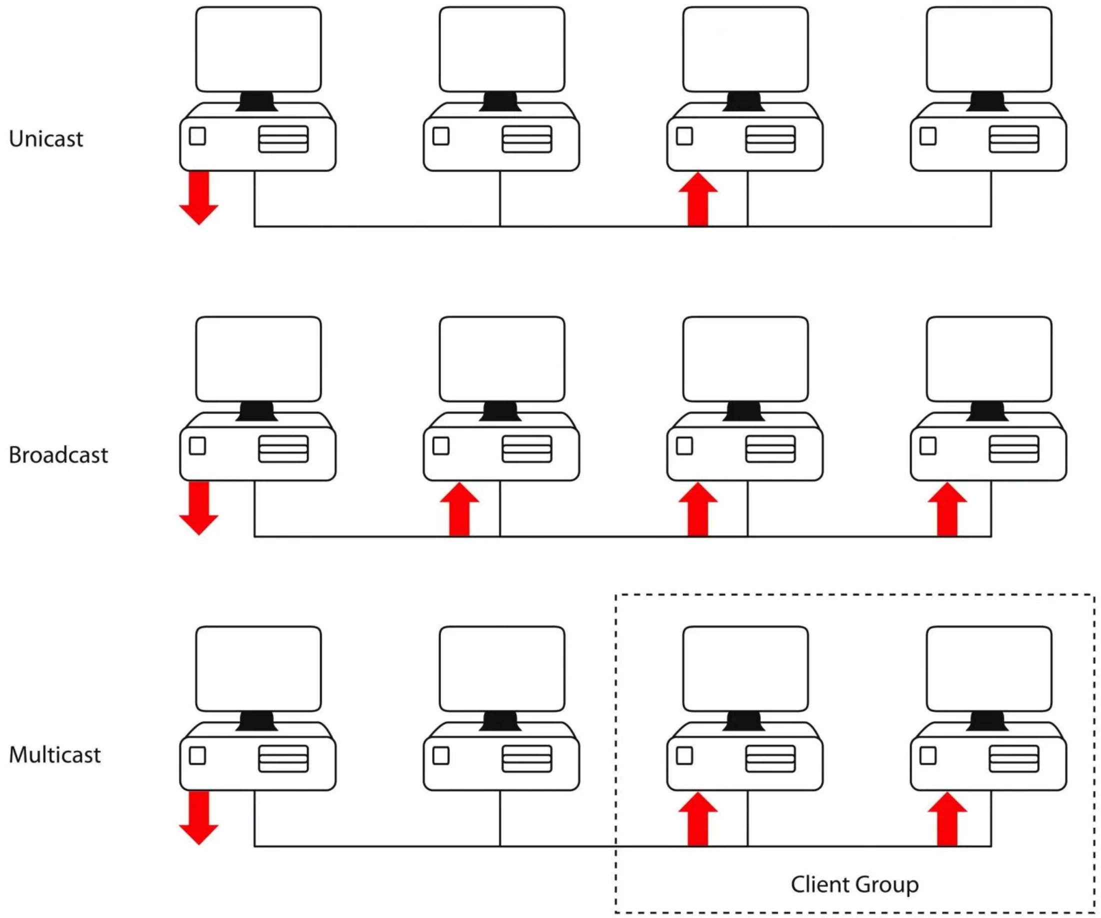


TABLE 1.3 Hex to Binary to Decimal Chart

Hexadecimal Value	Binary Value	Decimal Value
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

LAN Traffic

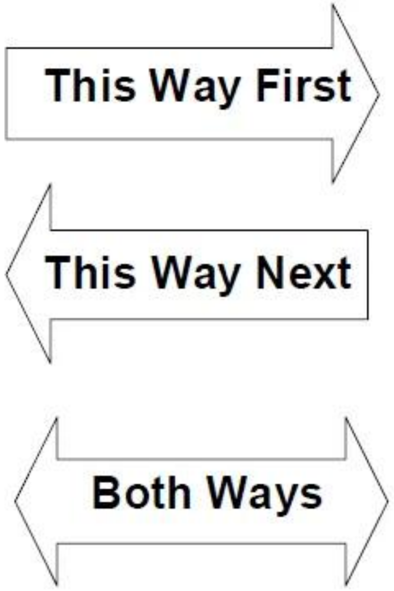
- **Unicast (one-to-one)** – a single LAN interface is the recipient
- **Broadcast (one-to-all)** – all devices on the LAN are the recipients
- **Multicast (one-to-many)** – a subset of all devices are the recipients



Half- and Full-Duplex Ethernet

- **Half-duplex Ethernet** it uses only one wire pair with a digital signal running in both directions on the wire.
- It also uses the CSMA/CD protocol to help prevent collisions and to permit retransmitting if a collision does occur.

- **full-duplex Ethernet** uses two pairs of wires instead of one wire pair like half duplex.
- with full-duplex data transfer, you get a faster data transfer compared to half duplex. And no collisions will occur.



This Way First

This Way Next

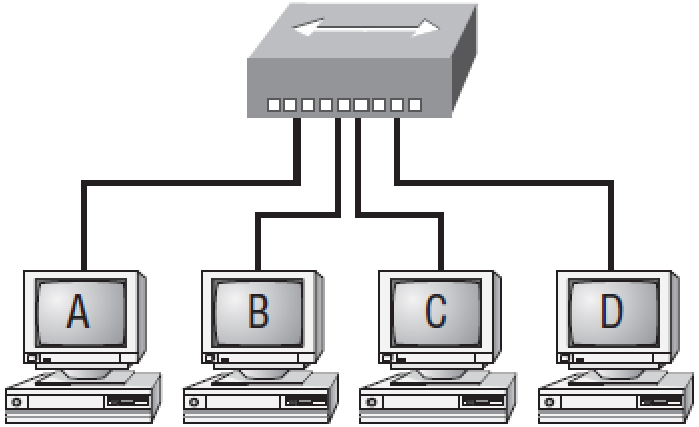
HALF DUPLEX -
ONE WAY AT A TIME

Both Ways

FULL DUPLEX -
BOTH DIRECTIONS
AT THE SAME TIME

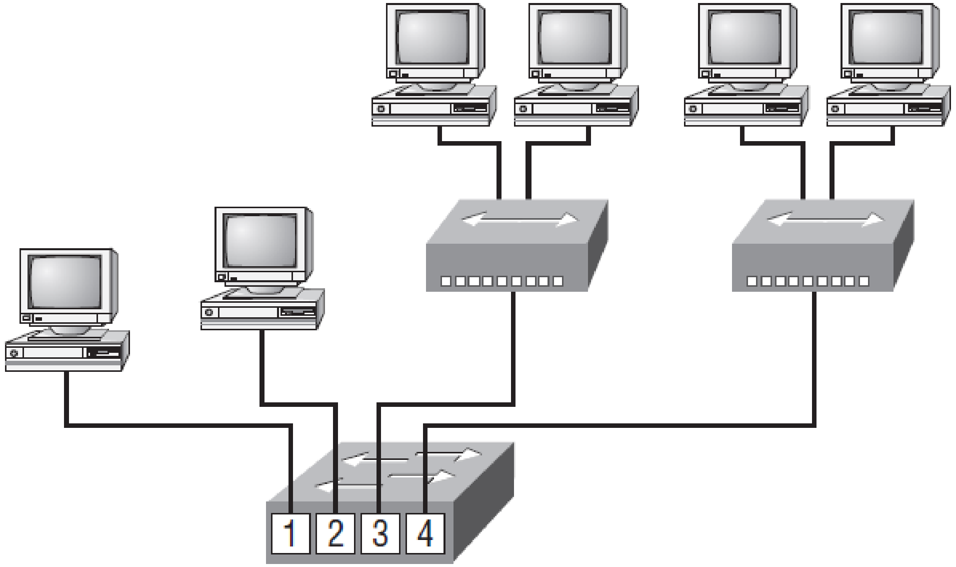
Hub in a network

Switch in a network



All devices in the same collision domain.
All devices in the same broadcast domain.
Devices share the same bandwidth.

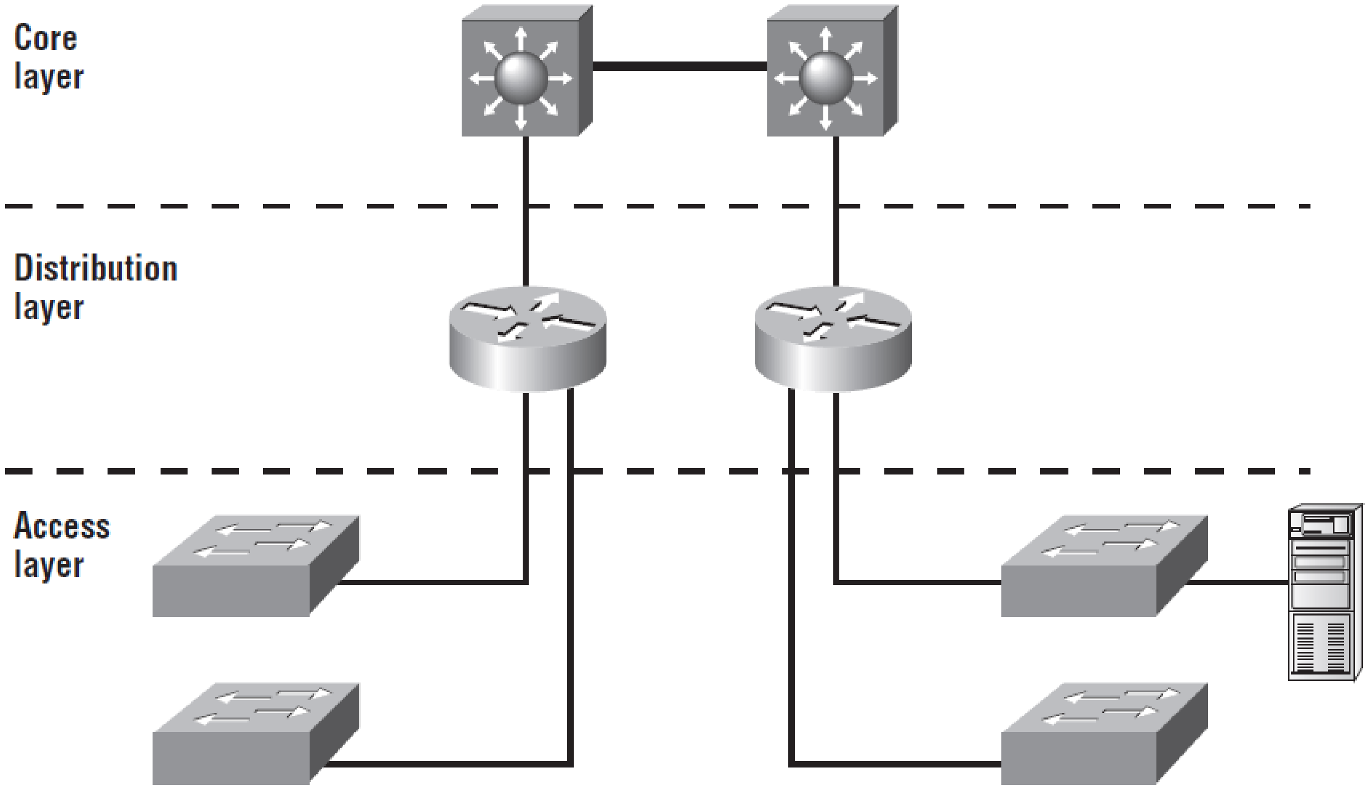
Hub is half duplex



Each segment has its own collision domain.
All segments are in the same broadcast domain.

Switch is full duplex

Cisco hierarchical model



CORE	Transport Network
DISTRIBUTION	Transport Network
ACCESS	Application Presentation Session Transport

The following are the three layers and their typical functions:

- The core layer: backbone
- The distribution layer: routing
- The access layer: switching