Networks and Protocols (Week 1)

Dr Md Hasanuzzaman Sagor

m.h.sagor@qmul.ac.uk

School of Electronic Engineering & Computer Science

Queen Mary
University of London

Teaching Staff

- Week 1 & 2

Dr. Md Hasanuzzaman Sagor
m.h.sagor@qmul.ac.uk

- Week 3 & 4

Dr. Zhijin Qin (Module Organiser)
z.qin@qmul.ac.uk

Part 1 Introduction to Networks and IoT

Queen Mary
University of London

TERMINOLOGY

Communication System

- To convey information from one point to another e.g. Radio, TV and Telephone
- More complex systems could be those who guide aircraft or space craft or provide live news coverage around the globe through satellite
- **Data** refers to facts, concepts and instructions presented in whatever form is agreed upon by parties creating and using data.

Components of Comms. System

- **Message:** The message is the information (data) to be communicated
  - Consists of text, numbers, pictures, sound, video or any combination of these.

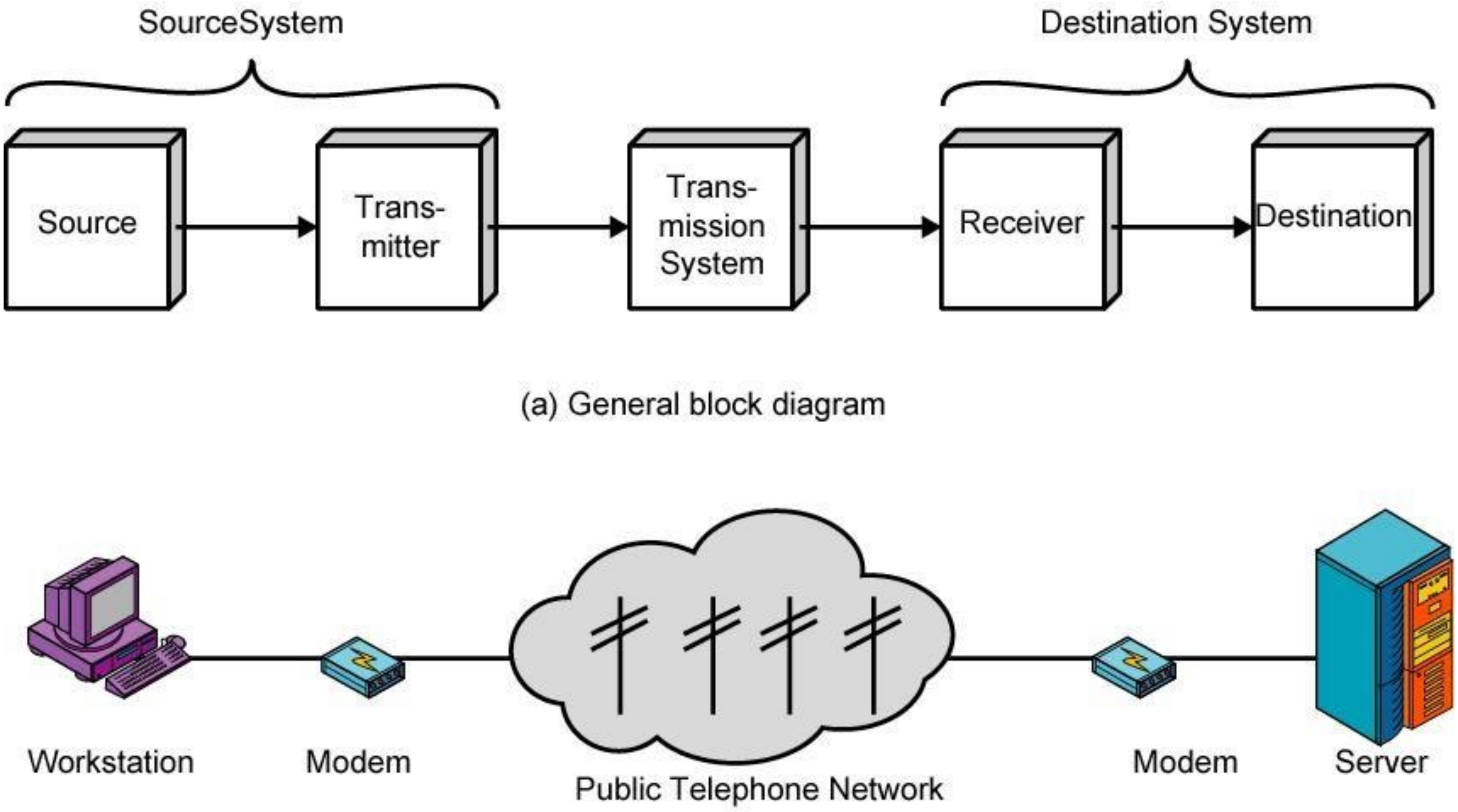
- **Sender:** The sender is the device that sends the data message
  - e.g. computer, telephone handset, video camera etc

- **Receiver:** The receiver is the device that receives the message
  - e.g. computer, telephone handset, television etc

Components of Comm. System

- **Medium:** The transmission medium is the physical path by which a message travels from sender to receiver.
  - e.g. twisted pair wire, coaxial cable, fiber-optic cable, laser, or radio waves (terrestrial or satellite microwave.
- **Protocol:** A protocol is a set of rules that govern data communication
  - Represents an agreement between the communicating devices
  - Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese. e.g.
  - HDLC, TCP/IP, IPX/SPX etc

Simplified Communications Model - Diagram



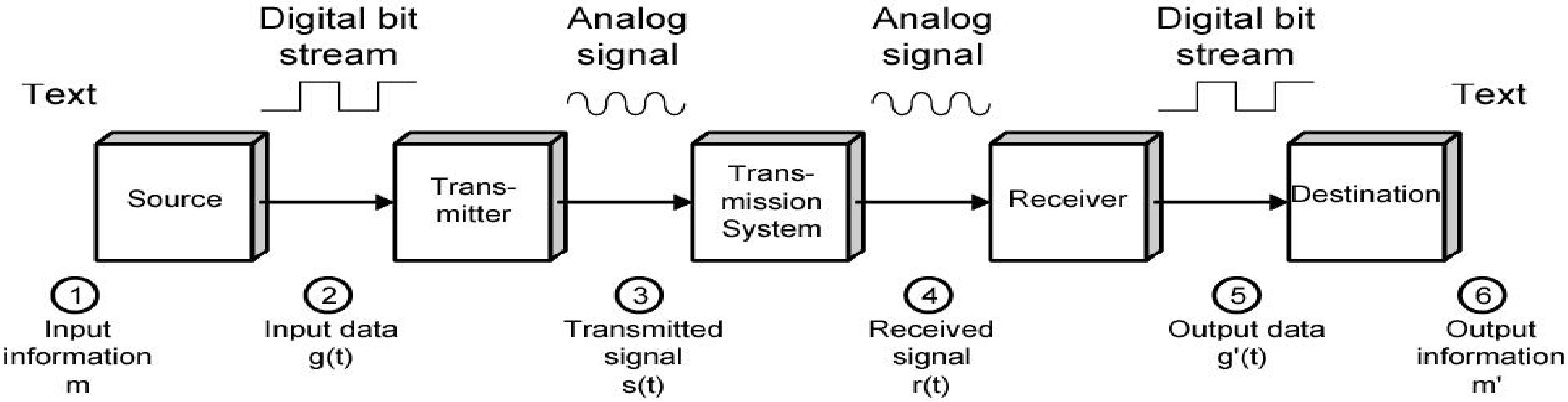
(a) General block diagram

(b) Example

A Communications Model

- Source
  - generates data to be transmitted
- Transmitter
  - Converts data into transmittable signals
- Transmission System
  - Carries data
- Receiver
  - Converts received signal into data
- Destination
  - Takes incoming data

Simplified Data Communications Model - Diagram



Data Communication deals with the transmission of signals in a reliable and efficient manner

Networking

- Networking deals with the technology and architectures of the communication networks used to interconnect communication devices
- Point to point communication is not usually practical
  - Devices are too far apart
  - Large set of devices would need impractical number of connections
- Solution is a communications network
  - Wide Area Network (WAN)
  - Local Area Network (LAN)
  - Personal Area Network (PAN)

Classification of Comms. Networks

- Determined by its network size, complexity, the distance it covers and its physical architecture.
- **Local Area Network (LAN)**
  - – Connects computers equipment and other terminals in a limited area e.g. university campus, office or factory etc.
  - – Usually privately owned, allows resources to be shared
  - – Traditionally have data rates 4-16 Mbps, now can reach 100Mbps with gigabit systems.
- **Metropolitan Area Network (MAN)**
  - – Used to connect No. of LANs spread around say in an entire city e.g. a cable television network
  - – May use high speed network using optical fiber connections

Classification of Comm. Networks

- **Wide Area Networks (WAN)**
  - Provides transmission of data over large geographical areas e.g. a city, a state, a country, a continent or even the globe.
  - Often require multiple communication connections, including microwave radio links and satellite.
  - WAN's are implemented on either of the two technologies: Circuit switching and Packet Switching.
  - Major roles have been assumed by frame relay and ATM.
  - Can you think about the world's largest WAN?

Classification of Comm. Networks

- **Personal Area Network (PAN)**
  - – Provides transmission of data over short range .
  - – Requires low power for transmission .
  - – Appropriate for low cost small networks.
  - – A part of larger Internet of Things (IoT) ecosystem.

Example?

Transmission Mode

- The mechanism of transferring data between two devices connected over a network.
- It defines the direction of signal flow between two linked devices.

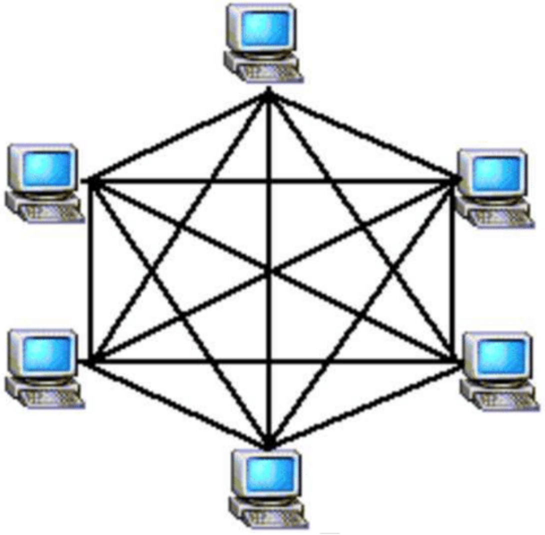
- **Simplex** is unidirectional i.e. signal flows only in one direction
- **Half-Duplex** is where each station can both transmit and receive, but one at a time
- **Full-Duplex** is where both stations can transmit and receive simultaneously

Line Configuration

- Refers to the way two or more communication devices attach to a link. A **link** is a physical communication pathway that transfers data from one device to another
- **Point-to-Point line configuration** provides dedicated link between two devices. Use the entire capacity of the channel e.g. TV remote using infrared
- **Point-to-Multipoint line configuration** is one in which more than two specific devices share a single link. The capacity of the link is shared.

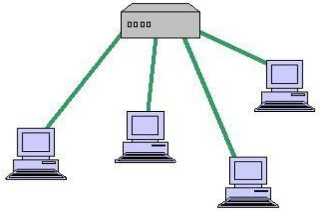
Topology

- Refers to the way a network is laid out, physically or logically. Two or more links form a topology.
- Topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to each other.
- **Peer-to-peer** (equal sharing) or **primary-secondary** relationship is possible.
- **MESH Topology**
  - Every device has a dedicated point
  - -to-point link to every other device
  - Eliminate traffic problem, is
  - robust and guarantees privacy

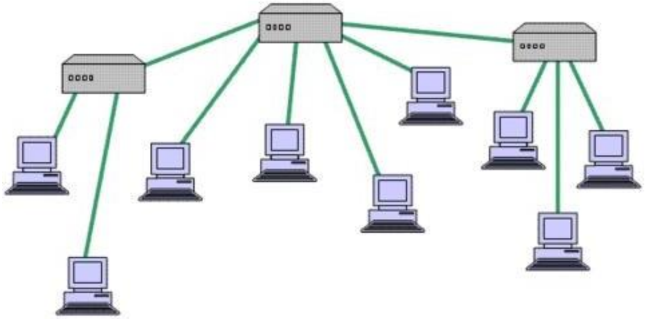


Topology

- **STAR Topology**
  - Each device has a dedicated point-to-point link only to a central controller called hub.
  - Less expensive, needs only one I/O port to connect to hub.
  - If one link is disconnected, that doesn't effect others.
  - If the hub fails, all connections are affected, and the entire network goes down.

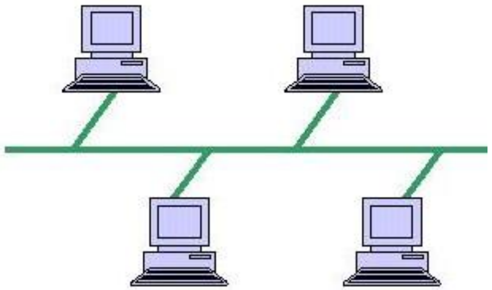


- **TREE Topology**
  - A variation of star as not all devices connect to central hub, but most devices connect to a secondary hub, which in turn connects to central hub.
  - Central hub is mostly an active hub i.e. it repeats the signals.
  - Example is cable TV

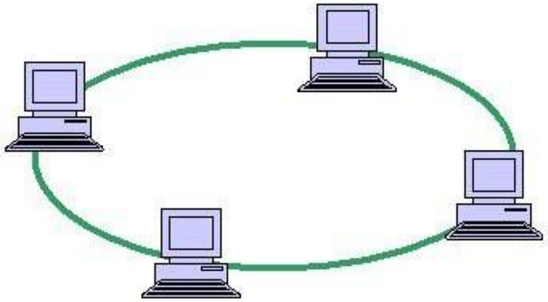


Topology

- **BUS Topology**
  - Nodes are connected to a bus cable by drop lines and taps
  - Has multipoint line configuration
  - Limits the no. of taps a bus can support
  - A fault in the cable will stop all transmission
  - Very old technique.

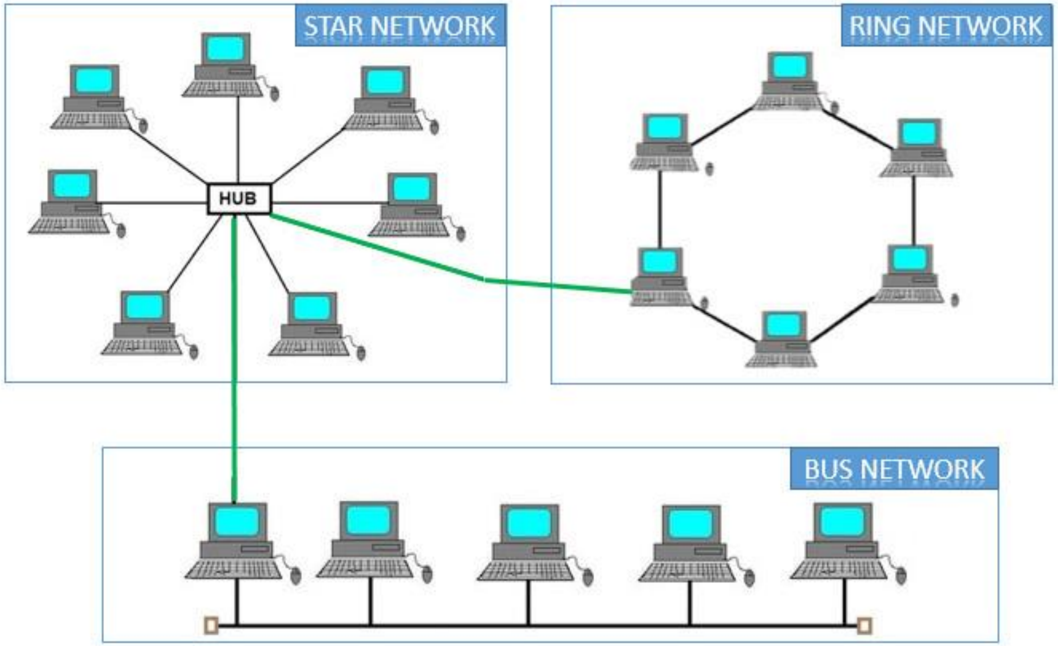


- **RING Topology**
  - Each device has a dedicated point-to-point line only with two devices on either side of it
  - Signal is passed in one direction along the ring
  - Put constraint on maximum ring length no. of devices
  - Any break in ring will disable the entire network
  - Easy to design, very old and rarely used today.



Topology

- **HYBRID Topology**
  - A network may combine several topologies as subnetworks linked together in a larger topology
  - Three departments having ring, bus and star topology can get connected through a central hub

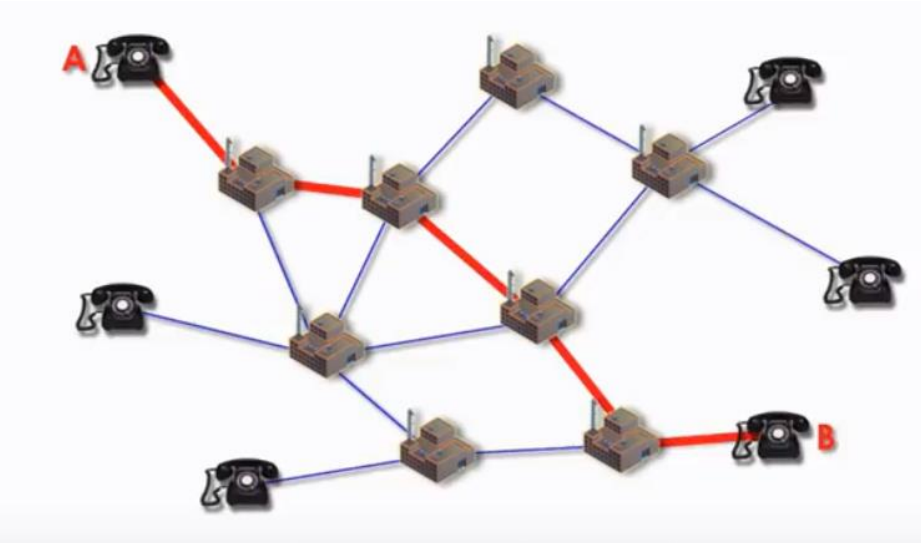


Alternative Technologies

Circuit switching and Packet switching

Circuit Switching:

- The communications between end devices (nodes) must be set up before they can communicate.
- Dedicated communication paths established for the duration of the conversation.
- e.g. telephone network



Alternative Technologies

Packet Switching:

- Data sent out of sequence
- Small chunks (packets) of data at a time
- Packets passed from node to node between source and destination
- Used for terminal to computer and computer to computer communications
- Original Packet switching networks were designed to provide 64 kbps .

Bits, Bauds, Symbols, and Bandwidth

What is a bit?

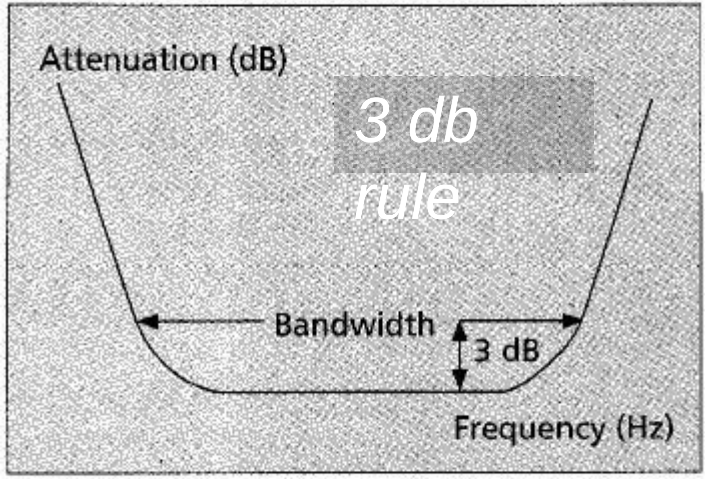
- A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1.

Profound insight:
All data can be represented up to arbitrary precision by bits

What is Bandwidth

- It can be defined as the range between the lowest and highest frequencies used for a particular application.
- The more bandwidth a data connection has, the more data it can send and receive at one time.
- Its unit of measure is hertz (Hz).

***Question:** Is all the signal power concentrated only within these frequencies?*



Spectral regulation agencies take a more strict view. 99% of the signal power has to be within the defined bandwidth.

Analog bandwidth (Hz) vs. Digital bandwidth (bps)

Relation of bitrate and bandwidth

Both are directly proportional, more BW means higher bitrate

Rate ∝ Bandwidth

As a first approximation,

we can think that we can transmit 1 bit/ Hz of BW (i.e., α =1) assuming a binary alphabet.

Harry Nyquis

Second approximation:

Nyquist (1924) established the upper bound on max. symbol rate as (2 x Bandwidth).

Symbol rate <= 2 B

Assuming binary alphabet , transmission can take place at max. of 2 bits/ Hz

Squeezing more bits/Hz

Pack more bits/Hz than allowed by Nyquist rate (of 2 bits/Hz) by having one symbol encode multiple bits

For digital transmission:

V	$\log_2 V$
1	0
2	1
3	1.6
4	2
8	3
16	4

Max symbol rate

$$R = 2B \log_2 V$$

Bits/ symbol

V = no. of possible symbols or levels

“Certain Factors Affecting Telegraph Speed”, Nyquist **(1924)**

Network performance [1]

- Transmission is subject to errors
- Across the network, data may be:
  - delayed
  - lost
  - mis-ordered
  - duplicated(!)

- Need to have mechanisms to deal with these
- QoS (Quality of Service):
  - to give some kind of assurance to an application

Network performance [2]

- An application’s QoS requirements?

  High data rate: video, graphics and quality audio

  - Interactive services:
    - 200ms round trip time (RTT)
    - low jitter for conversational services

- Delays:
  - Processing
  - Packetisation
  - Queuing
  - Transmission (data rate)
  - Propagation

Network performance [3]

Related to IoT or wireless sensor networks

- Energy consumption
  - – Energy spent to transmit, receive, sense, etc
- Network lifetime
  - – Time span from the deployment to the instant when the network is considered nonfunctional.
  - – E.g. the instant when the first sensor dies, a percentage of sensors die, the network partitions, or the loss of coverage occurs

Standardized Protocol Architectures

- Required for devices to communicate
- Customers can insist on standards-based equipment

- Two standards:
  - OSI Reference model
    - Never lived up to early promises
  - TCP/IP protocol suite
    - Most widely used

- Also: IBM Systems Network Architecture (SNA)

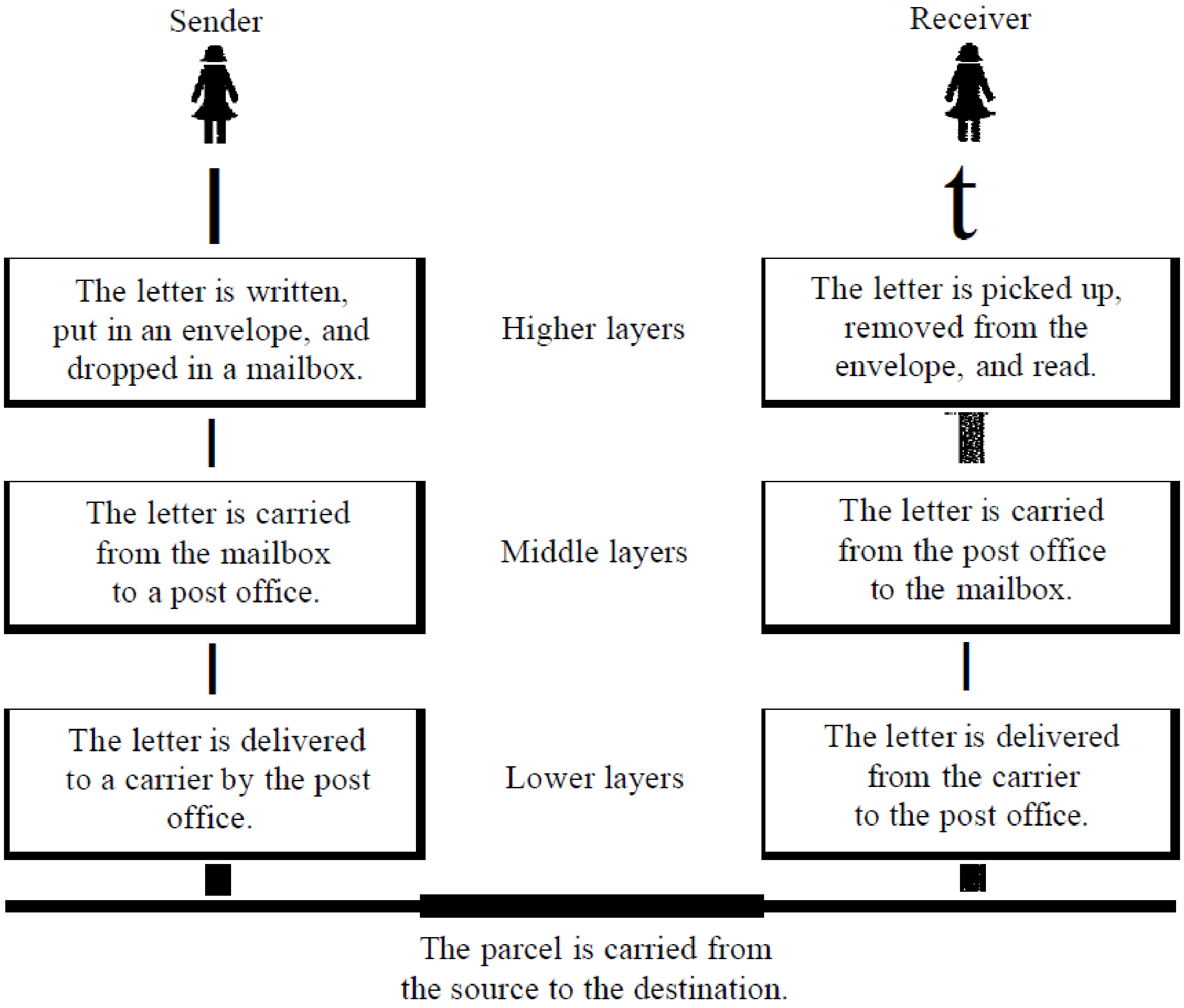
Open Systems Interconnection (OSI)

- Open System Interconnect is an ISO standard that covers all aspects of network communication.
- Developed by the International Organization for Standardization (ISO). International Standards Organization is a multinational body dedicated to worldwide agreement on international standards.
- An Open System is a model that allows any two different systems to communicate regardless of their underlying architecture.
- Seven layers
- A theoretical system delivered too late!
- TCP/IP is the de facto standard.

Basic Concepts

- OSI is a **Model** not a **Protocol,** rather it is a framework for developing protocol standards.
- OSI model uses the structuring technique known as layering.
- The layered framework is used for the designing of network systems that allows communication across all types of computer systems.
- The model is built of seven separate but related layers.
- Each layer performs a related subset of the functions required to communicate with another system.
- Each layer uses the services provided by its lower layer and provides service to its upper layer.
- Changes in one layer should not require changes in other layers.
- A protocol implements the functions of one or more of the OSI layers.

Example of Layered Task



Sender

Receiver

The letter is written, put in an envelope, and dropped in a mailbox.

Higher layers

The letter is picked up, removed from the envelope, and read.

The letter is carried from the mailbox to a post office.

Middle layers

The letter is carried from the post office to the mailbox.

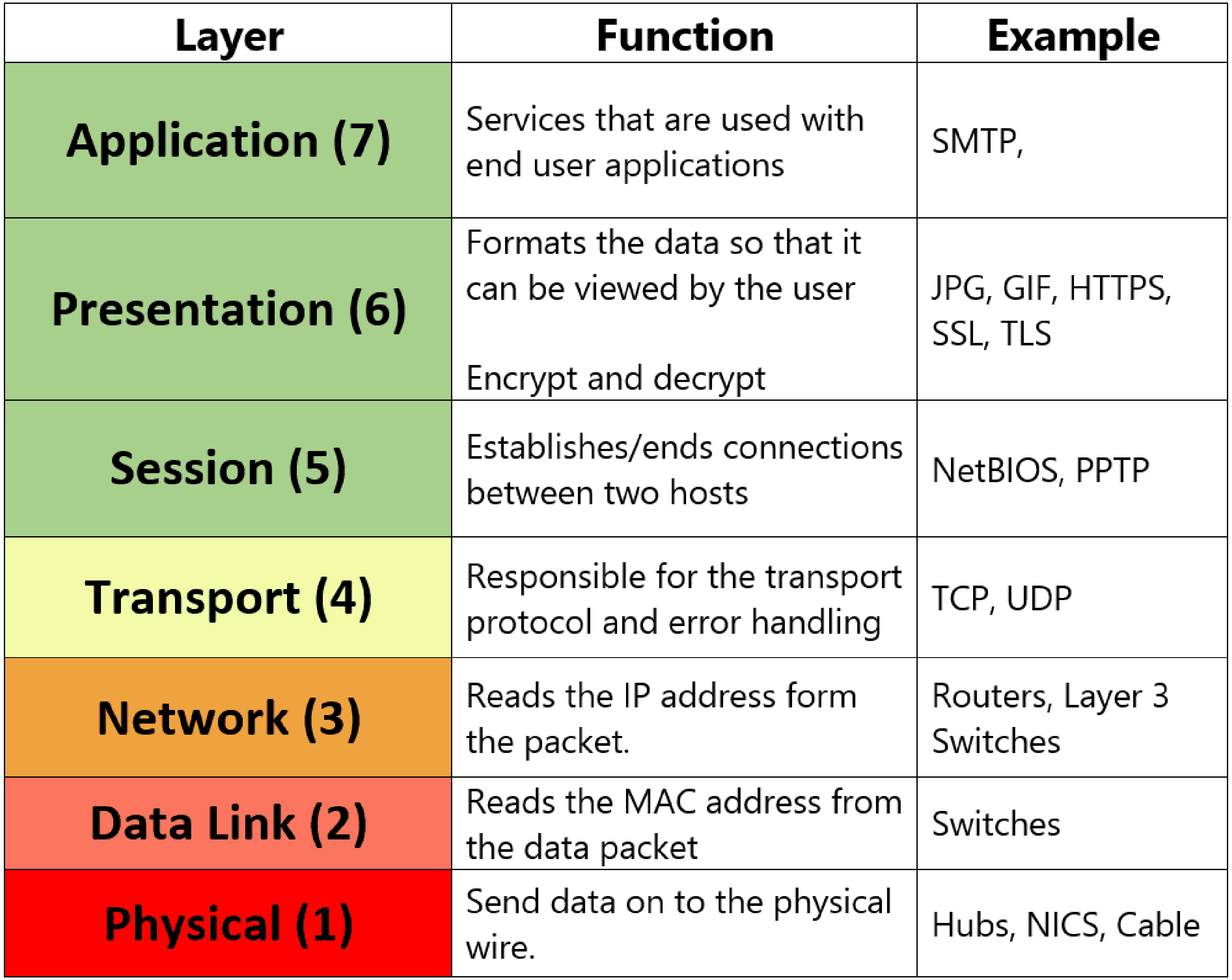
The letter is delivered to a carrier by the post office.

Lower layers

The letter is delivered from the carrier to the post office.

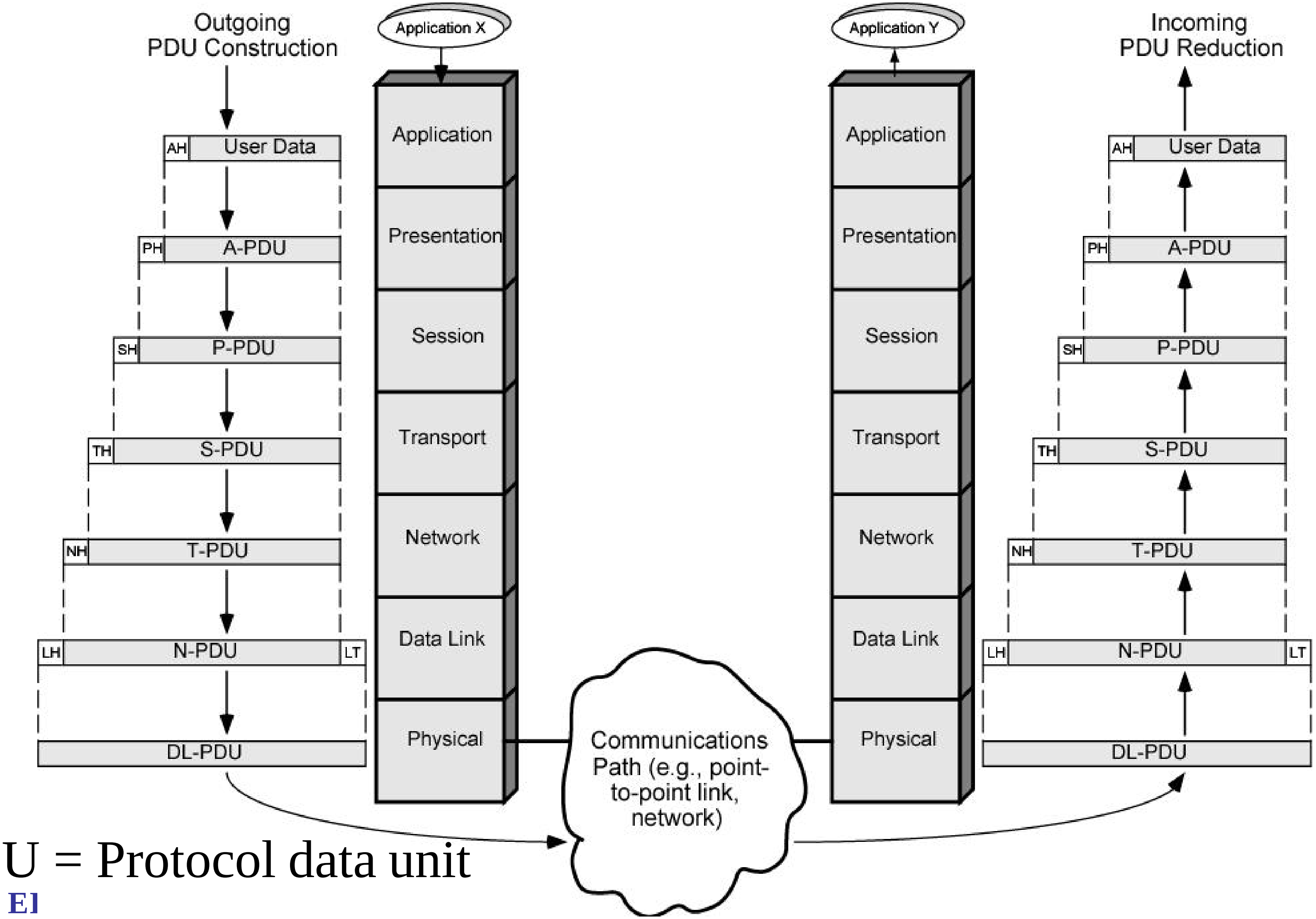
The parcel is carried from the source to the destination.

OSI Layers



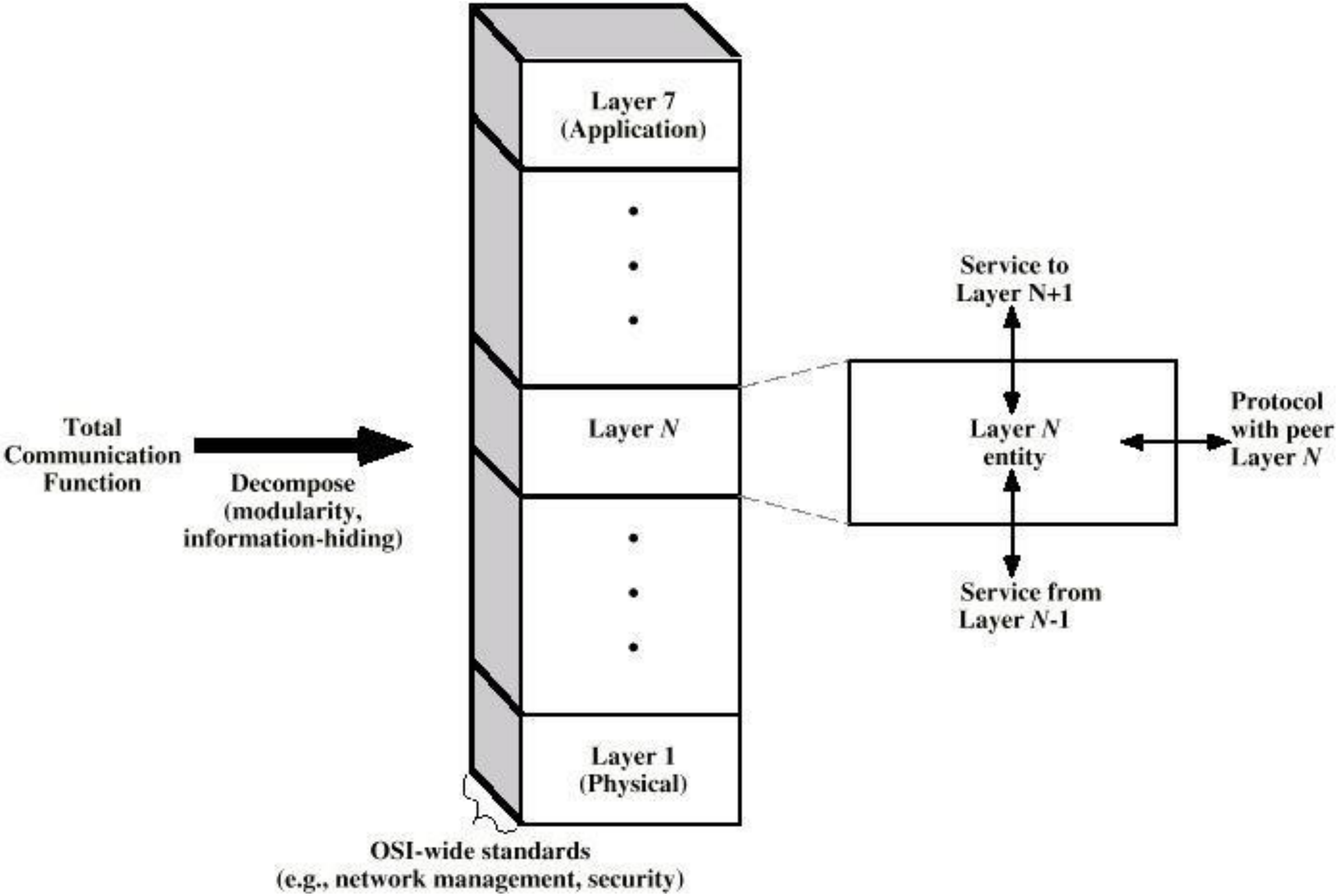
Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

The OSI Environment

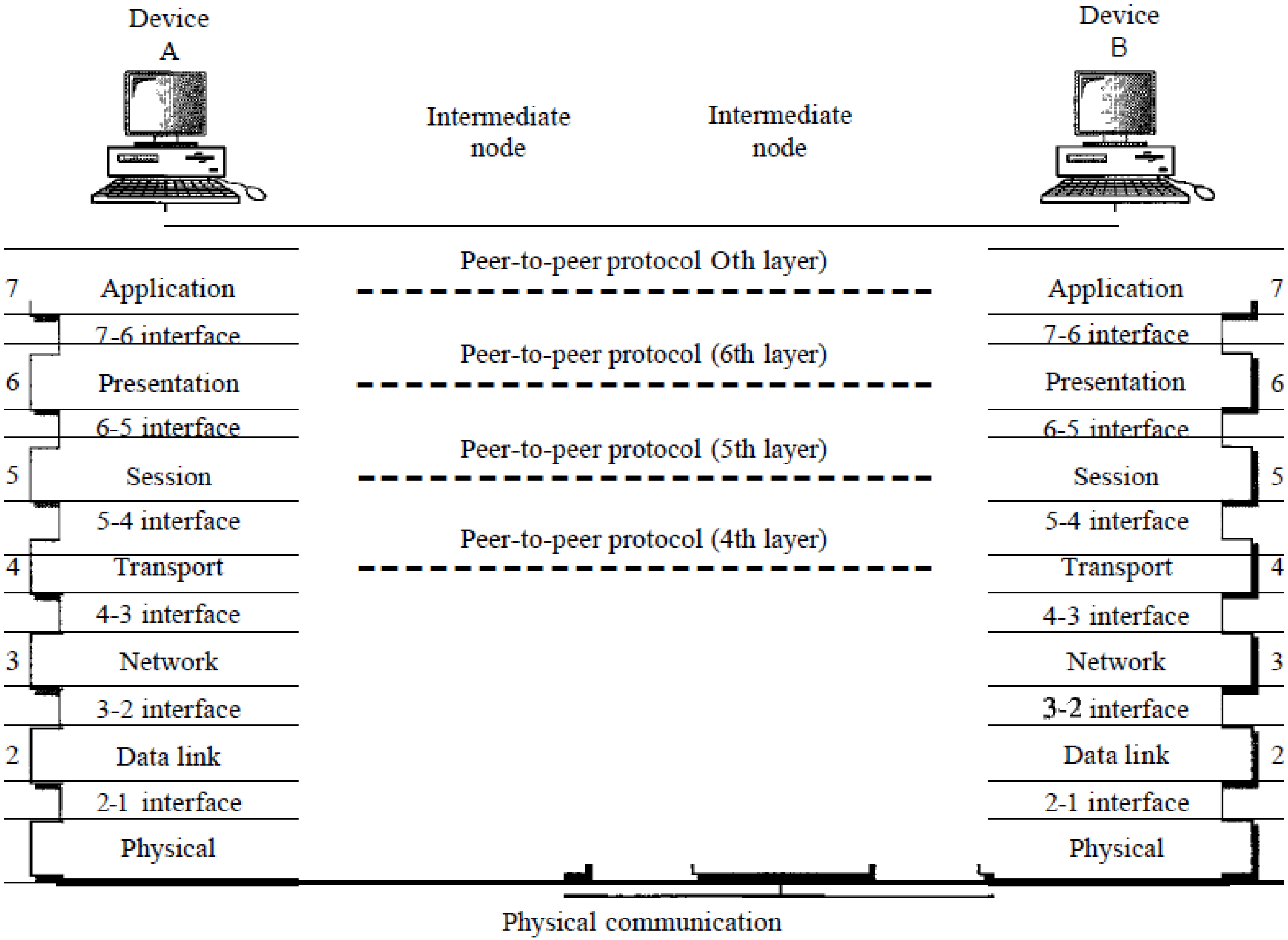


PDU = Protocol data unit

OSI as Framework for Standardization


Total Communication Function
Decompose (modularity, information-hiding)
Layer 7 (Application)
Layer *N*
Layer 1 (Physical)
OSI-wide standards (e.g., network management, security)
Service to Layer N+1
Layer *N* entity
Protocol with peer Layer *N*
Service from Layer *N*-1

Interactions between layers



Elements of Standardization

- Protocol specification
  - Operates between the same layer on two systems
  - May involve different operating system
  - Protocol specification must be precise
    - Format of data units
    - Semantics of all fields
    - allowable sequence of PDUs
- Service definition
  - Functional description of what is provided
- Addressing
  - Referenced by SAPs (Service access points)

OSI Layers (1)

- Physical
  - Physical interface between devices
    - Electrical & Mechanical level
    - Functional
    - Procedural
    - Provides the hardware means of sending and receiving data on a carrier
- Data Link
  - Means of activating, maintaining and deactivating a reliable link
  - Error detection and control
  - Higher layers may assume error free transmission

OSI Layers (2)

- Network
  - Transport of information
  - responsible for the source-to-destination delivery of a packet
  - Higher layers do not need to know about underlying technology
- Transport
  - Exchange of data between end systems
  - Error free
  - In sequence
  - No losses
  - No duplicates
  - Quality of service

OSI Layers (3)

- Session
  - Responsible for dialog control and synchronization.
  - Dialogue discipline
  - Establishes, manages and terminates connections between applications
  - Recovery
- Presentation
  - Data formats and coding
  - Responsible for interoperability between these different encoding methods.
  - Data compression and Encryption
- Application
  - Enables users to access the network
  - Means for applications to access OSI environment
  - Everything at this layer is application-specific

TCP/IP Protocol Architecture

- TCP/IP, or the Transmission Control Protocol/ Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet.
- Developed by the US Defense Advanced Research Project Agency (DARPA)
- Used by the global Internet
- No official model but a working one is as below:
  - Application layer
  - Host to host or transport layer
  - Internet layer
  - Network access layer
  - Physical layer

TCP/IP Protocol Layers

Physical Layer

- Physical interface between data transmission device (e.g. computer) and transmission medium or network
- Characteristics of transmission medium
- Signal levels, Data rates

Network Access Layer

- Exchange of data between end system and network
- Destination address provision
- Invoking services like priority

TCP/IP Protocol Layers

Internet Layer

- Systems may be attached to different networks
- Routing functions across multiple networks
- Implemented in end systems and routers

Transport Layer

- Responsible for maintaining end-to-end communications across the network
- Reliable delivery of data
- Include TCP and User Datagram Protocol (UDP)

TCP/IP Protocol Layers

Application Layer

- Combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.
- Facilitates the user to use the services of the network.
- Direct user interface
- Includes the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3) and others.

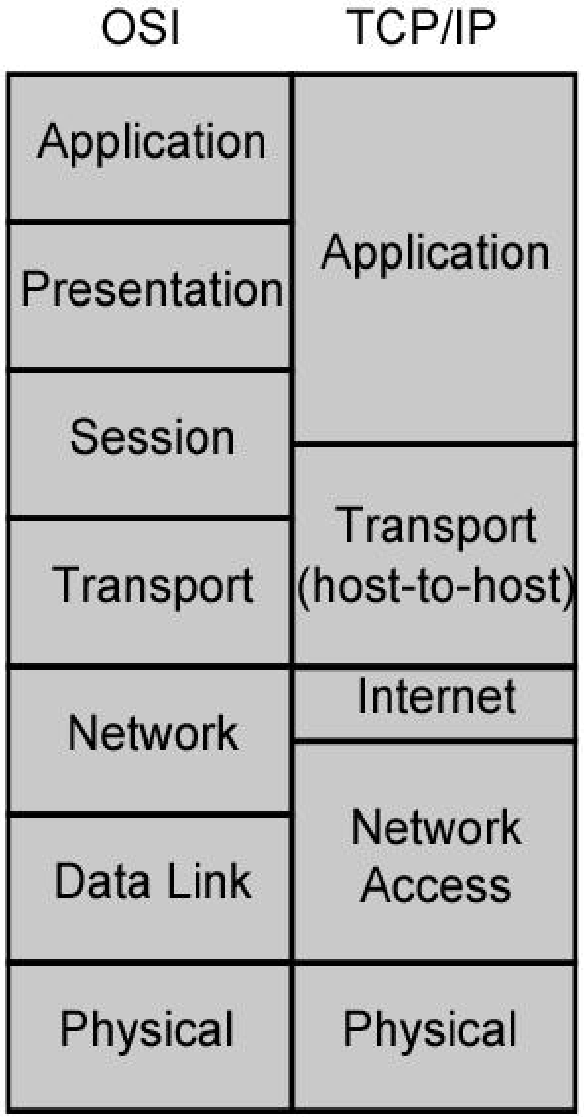
Layering

- Each layer only communicates with adjacent layers. For example, a software only needs to know how to request a connection with a remote host using the Transport layer. It doesn’t need to know how bits are encoded before transmission. That’s the Physical layer’s job.

- Each layer needs to add some control information to the data in order to do it’s job.

- Once the lower layers deliver the data and control information - the peer layer uses the control information.

OSI v TCP/IP



OSI

Application

Presentation

Session

Transport

Network

Data Link

Physical

TCP/IP

Application

Transport (host-to-host)

Internet

Network Access

Physical

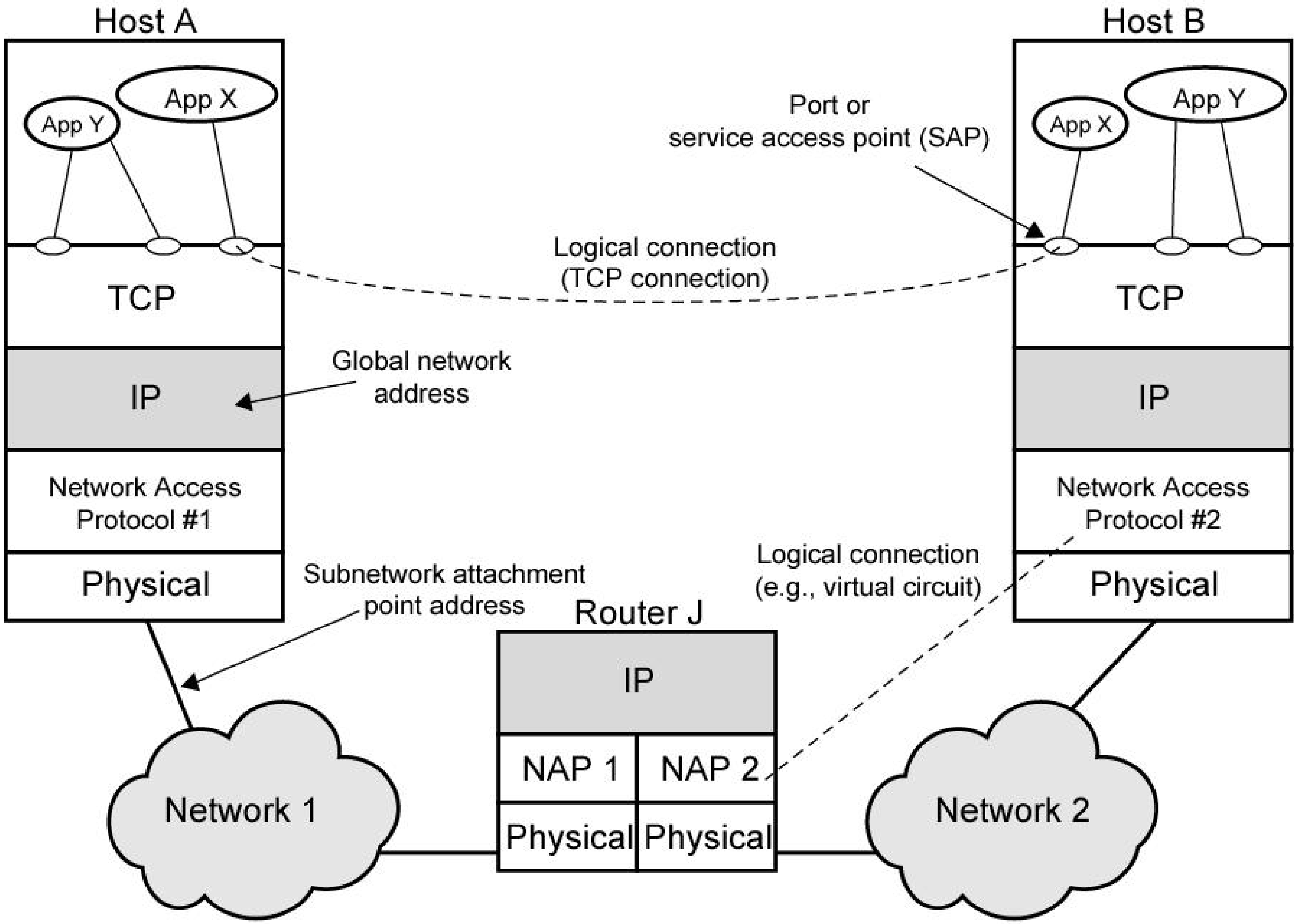
TCP

- Usual transport layer is Transmission Control Protocol
  - Reliable connection
- Connection
  - Temporary logical association between entities in different systems
- TCP PDU
  - Called TCP segment
  - Includes source and destination port (c.f. SAP)
    - Identify respective users (applications)
    - Connection refers to pair of ports
- TCP tracks segments between entities on each connection

UDP

- Alternative to TCP is User Datagram Protocol
- Unreliable Protocol
- Not guaranteed delivery
- No preservation of sequence
- No protection against duplication
- Minimum overhead
- Adds port addressing to IP

TCP/IP Concepts


Host A
App Y
App X
TCP
IP
Network Access Protocol #1
Physical
Port or service access point (SAP)
Logical connection (TCP connection)
Global network address
Host B
App X
App Y
TCP
IP
Network Access Protocol #2
Physical
Subnetwork attachment point address
Router J
Logical connection (e.g., virtual circuit)
IP
NAP 1
NAP 2
Physical
Physical
Network 1
Network 2

Addressing in TCP/IP

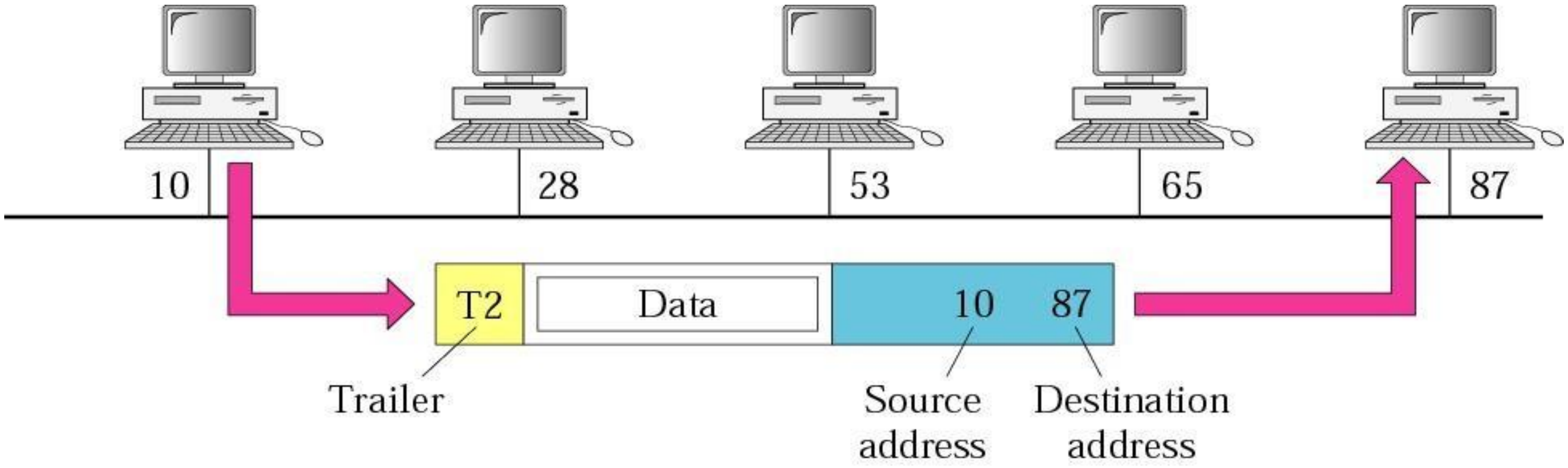
Four different levels of addresses are used in an internet employing the TCP/IP protocols:

Physical address

- Also known as the link address, is the address of a node as defined by its LAN or WAN

- **Logical address** (32-bit , IPv4)
  - logical (IP) addresses are for universal communications that are independent of underlying physical networks
- **Port address** (16-bit)
  - port addresses differentiate different processes
- **Application-specific address**
  - Some applications have user-friendly addresses that are designed for that specific application, such as email address, URL.

Physical Address



- Most local area networks (LANs) use a 48-bit (6 bytes) physical address written as 12 hexadecimal digits, with every 2 bytes separated by a colon as shown below:

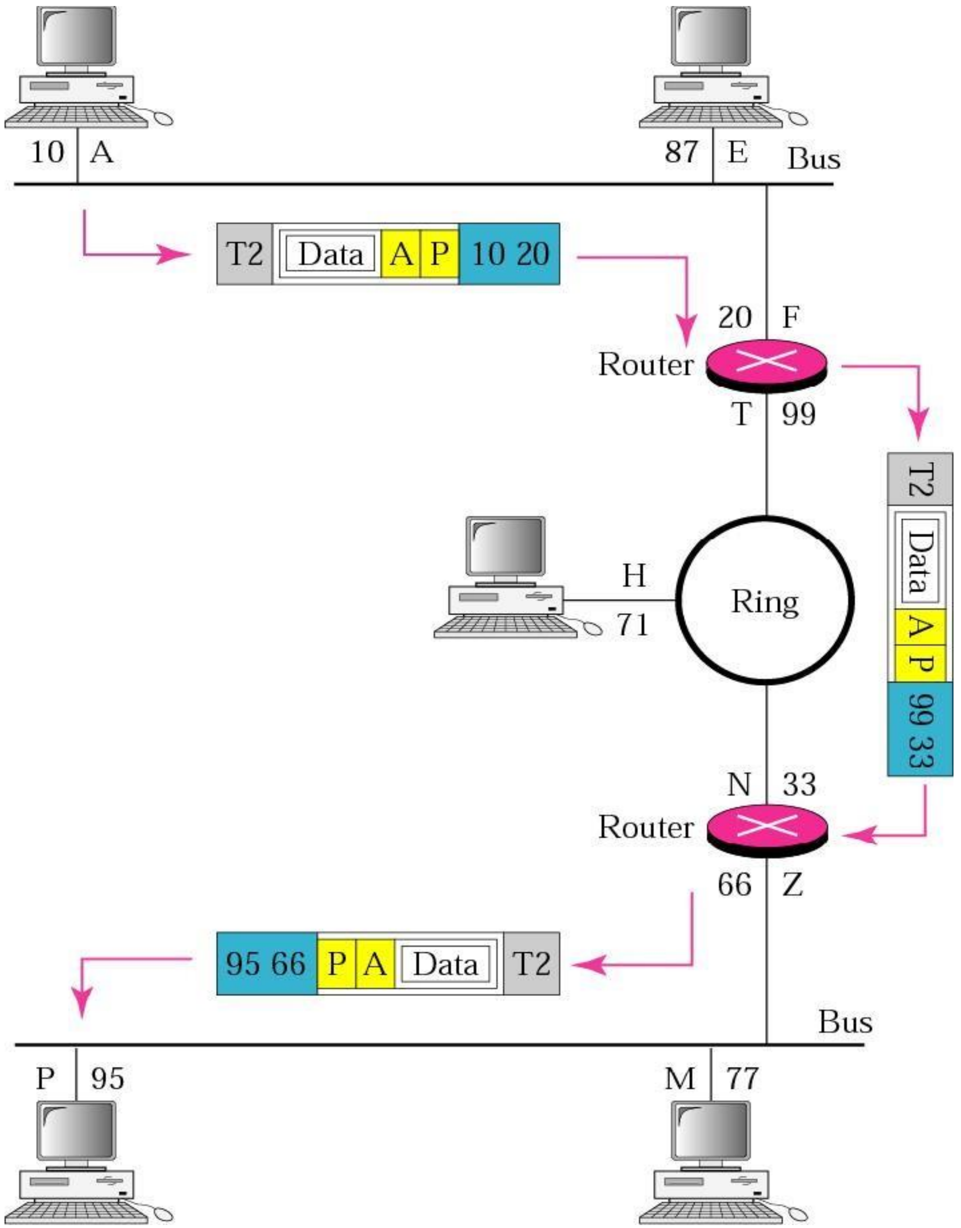
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address

Logical (IP) Address

- The physical addresses change from hop to hop, but the logical address remain the same.
- IPv4 address is 32 bits in length, normally written as four decimal numbers, with each number representing 1 byte

  i.e. 138.37.7.80



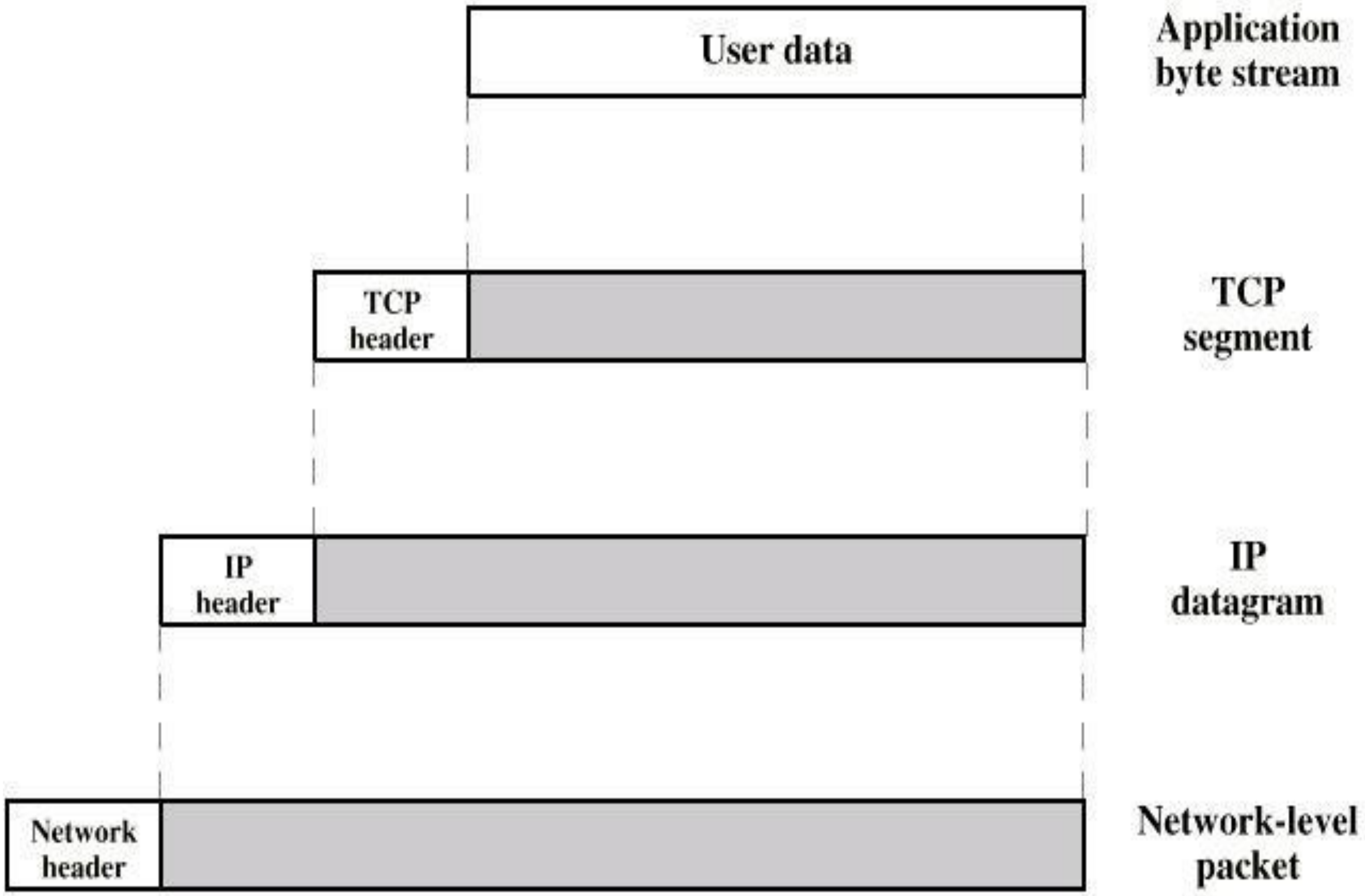
What are ‘Headers’?

- At each layer, a packet has two parts: the header and the body.
- The header contains protocol information relevant to that layer, while the body contains the data for that layer.
- **Physical Layer:** no header - just a bunch of bits.
- **Data Link Layer:**
- address of the receiving endpoints
- address of the sending endpoint
- length of the data

Headers in TCP/IP

- Each layer treats the information it gets from the layer above it as data and applies its own header to this data.
- At each layer, the packet contains all the information passed from the higher layer; nothing is lost. This process of preserving the data while attaching a new header is known as ***encapsulation***.

Headers in TCP/IP



Headers in TCP/IP

- At the application layer, the packet consists simply of the data to be transferred. As it moves to the transport layer, the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) preserves the data from the previous layer and attaches a header to it. At the next layer, IP considers the entire packet (consisting now of the TCP or UDP header and the data) to be data, and now attaches its own IP header. Finally, at the network access layer, Ethernet or another network protocol considers the entire IP packet passed to it to be data and attaches its own header.

IoT

Queen Mary
University of London

IoT-Introduction

- Internet Technology connecting devices, machines and tools to the internet by means of wireless technologies.
- Over 10 billion 'Things' connected to the Internet as of today.
- 'Things' connected to the internet are projected to cross 20 billion in near future.
- Unification of technologies such as low-power embedded systems, cloud computing, big-data, machine learning, and networking.

IoT- Enablers

- In a report commissioned by ITU in 2005, prospective IoT enablers include:
  - RFID
  - Nanotechnology
  - Sensors
  - Smart Networks
  - Augmented Intelligence

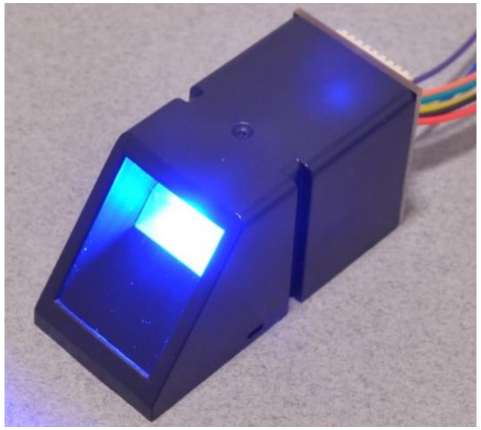
IoT Characteristics

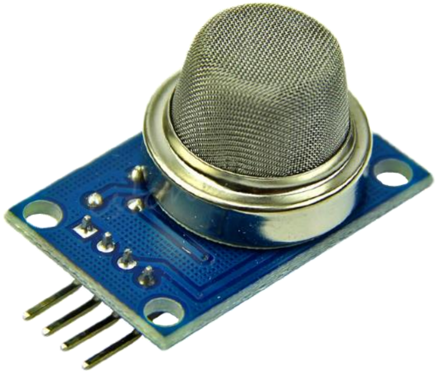
- Efficient, scalable, and associated architecture
- Unambiguous naming and addressing
- Abundance of sleeping nodes, mobile and non-IP devices
- Intermittent connectivity.

Reference: Teemu Savotainen, Jonne Soininen, and Balhanan Silverajan , “IPv6 Addresssing Strategies for IoT”, IEEE Sensors, Journal, Vol. 13, No. 10, October, 2013

IoT Component: Sensors

- To measure a physical phenomenon.
- Data centric creation of information without human intervention.
- A sensor converts a non-electrical input into an electrical signal that can be sent to an electronic circuit.


Fingerprint


Gas Leakage

Ultrasonic

IoT Component: Sensors

- Different sensors capture different types of information.

- Accelerometers measure linear acceleration, detecting whether an object is moving and in which direction, while gyroscopes measure complex motion in multiple dimensions by tracking an object's position and rotation.

- By combining multiple sensors, each serving different purposes, it is possible to build complex systems that exploit many different types of information.

IoT Component: Actuator

- The technological complement to a sensor is an **actuator**, a device that converts an electrical signal into action, often by converting the signal to nonelectrical energy, such as motion.

- An actuator requires a control signal and a source of energy.

Factors driving adoption in the IoT

- There are three primary factors driving the deployment of sensor technology:
  - price
  - capability
  - size.
- As sensors get less expensive, “smarter”, and smaller, they can be used in a wider range of applications and can generate a wide range of data at a lower cost.

Sensor Technology Challenges

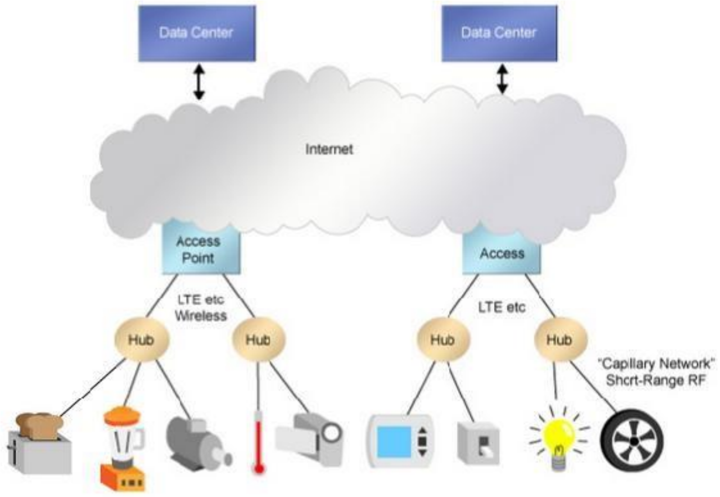
Among the challenges are power consumption, data security, and interoperability:

- **Power consumption:** Battery life, charging, and replacement, especially in remote areas, may represent significant issues.
- **Security of sensors:** Requires lightweight security algorithm. Data Integrity is a concern.
- **Interoperability:** Most of the sensor systems currently in operation are proprietary and are designed for specific applications.

NETWORKS IN THE IoT

Networks in the IoT

- Information that sensors create rarely attains its maximum value at the time and place of creation.



- The signals from sensors often **must be communicated to other locations** for aggregation and analysis.
- This typically involves transmitting data over a network.

Networks in the IoT

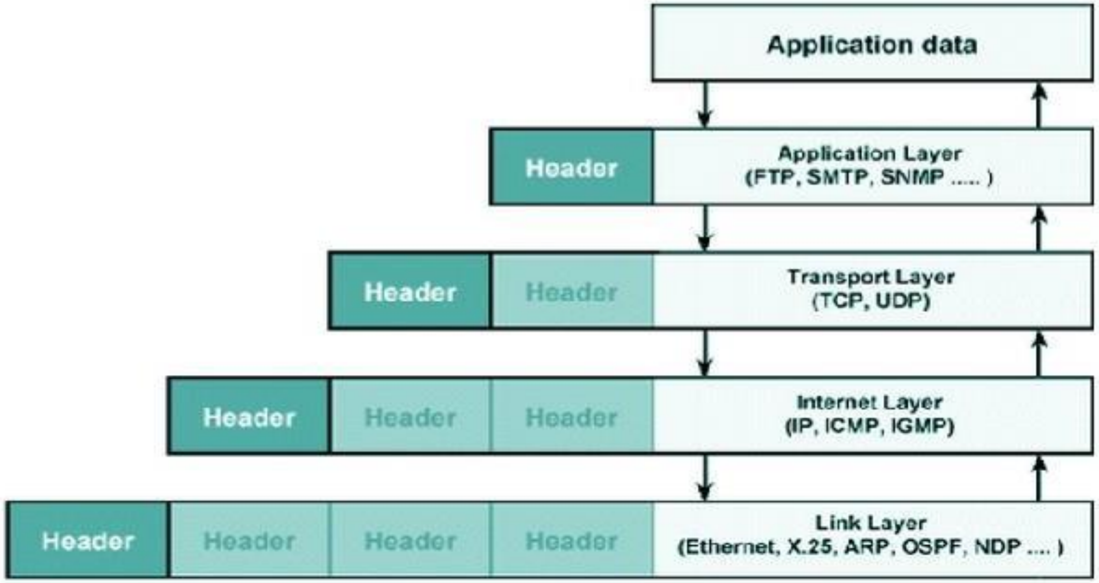
- Sensors and other devices are connected to networks using various networking devices such as **hubs, gateways, routers, network bridges, and switches**, depending on the application.
  - **Hubs:** Used to connect segments of a LAN.
  - Gateways: A network point that acts as an entrance to another network.
  - **Routers:** A device that forwards data packets along networks.
  - **Network bridges:** A network device that connects multiple network segments.
  - **Switches:** A computer networking device that connects devices together by using packet switching to receive, process, and forward data to the destination device.

Networks in the IoT

- The first step in the process of transferring data from one machine to another via a network is to uniquely identify each of the machines. The IoT requires a **unique name** for each of the **“things”** on the network.
- Network protocols are a set of rules that define how computers identify each other and subsequently execute the communication process.

Internet Protocol

- The Internet Protocol is an open protocol that provides **unique addresses** to various Internet-connected devices; currently, there are two versions of IP: IP version 4 **(IPv4)** and IP version 6 **(IPv6).**



Internet Protocol

- IP was used to **address computers** before it began to be used to address other devices.
- IPv4-32 bit addresses. Address space has depleted.
  - Total Address Space? - 2^32; i.e. approx. 4 billion.
- IPv6-128 bit addresses. Much larger address space facilitates in supporting billions of devices.
- More than 50 billion internet connected devices by 2020. Adoption of **IPv6 has served as a key enabler of the IoT.**

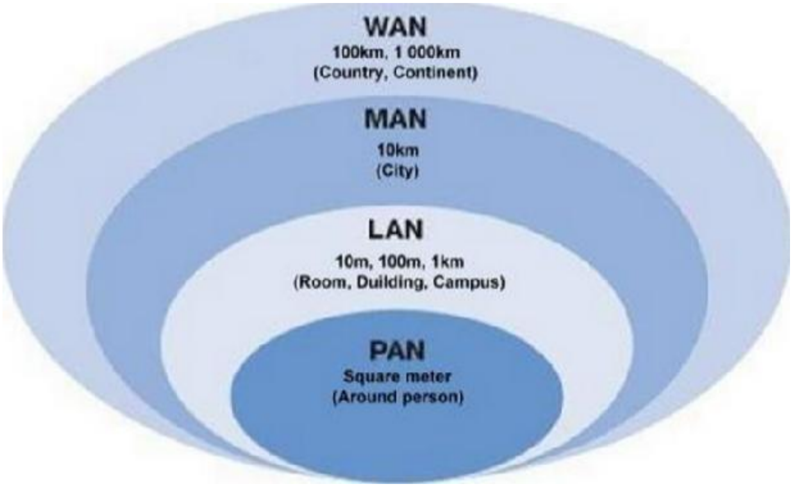
ENABLING NETWORK TECHNOLOGIES

Enabling Network Technologies

- Network technologies are classified broadly as **wired** or **wireless**.

- With the continuous movement of users and devices, wireless networks provide convenience through almost continuous connectivity, while wired connections are still useful for relatively more reliable, secured, and high-volume network routes.

Enabling Network Technologies



- The choice of network technology depends largely on the **geographical range** to be covered.
- When data have to be transferred over short distances (for example, inside a room), devices can use wireless **personal area network** (PAN) technologies such as **Bluetooth** and **ZigBee**, as well as wired connections through technologies such as Universal Serial Bus **(USB).**

Enabling Network Technologies

- When data have to be transferred over a relatively bigger area such as an office, devices could use **local area network** (LAN) technologies.
- Examples of wired LAN technologies include Ethernet and fiber optics.
- Wireless LAN networks include technologies such as **Wi-Fi**.

Enabling Network Technologies

- When data are to be transferred over a wider area beyond buildings and cities, an internetwork called **wide area network** (WAN) is set up by connecting a number of local area networks through routers.
- The Internet is an example of a WAN.
- Wireless LAN networks include technologies such as **WiMAX**.

Enabling Network Technologies

- **Data transfer rates** and **energy requirements** are two key considerations when selecting a network technology for a given application.
- Technologies such as **4G** (LTE, LTE-A) and **5G** are favourable for IoT applications, given their high data transfer rates.
- Technologies such as **Bluetooth Low Energy** and **Low Power Wi-Fi** are well suited for energy-constrained devices.

Bluetooth and Bluetooth Low Energy

- Introduced in 1999, Bluetooth technology is a wireless technology known for its ability to transfer data over short distances in personal area networks.
- Bluetooth Low Energy (BLE) is a recent addition to the Bluetooth technology and consumes about half the power of a Bluetooth classic device, the original version of Bluetooth.
- Key features of the Bluetooth protocol are
- **robustness**, **low power**, and **low cost**.

Bluetooth and Bluetooth Low Energy

- The energy efficiency of BLE is attributable to the **shorter scanning time** needed for BLE devices to detect other devices: 0.6 to 1.2 milliseconds (ms) compared to
- 22.5 ms for Bluetooth Classic.
- In addition, the efficient transfer of data during the transmitting and receiving states enables BLE to deliver higher energy efficiency compared to Bluetooth Classic.
- Higher energy efficiency comes at the cost of lower data rates: BLE supports 260 kilobits per second (Kbps) while Bluetooth Classic supports up to 2.1 Mbps.

Bluetooth and Bluetooth Low Energy

- Existing penetration, coupled with low devices costs, positions BLE as a technology well suited for IoT applications.
- However, **interoperability** is the persistent bottleneck here as well:
- BLE is compatible with only the relatively newer dual-mode Bluetooth devices.

Wi-Fi and Low Power Wi-Fi

- Wi-Fi is a wireless technology that is widely popular and known for its high-speed data transfer rates in personal and local area networks.
- Typically, Wi-Fi devices keep latency, or delays low by **remaining active** even when no data are being transmitted.

Wi-Fi and Low Power Wi-Fi

- Such Wi-Fi connections are often set up with a dedicated power line or batteries that need to be charged after a couple of hours of use.
- Lower-power Wi-Fi devices **“sleep”** when not transmitting data and need just 10 milliseconds to **“wake up”** when called upon.
- Low Power Wi-Fi with batteries can be used for remote sensing and control applications.

Worldwide Interoperability for Microwave Access (WiMAX) and WiMAX 2

- Introduced in 2001, WiMAX was developed by the European Telecommunications Standards Institute (ETSI) in cooperation with IEEE.
- WiMAX 2 is the latest technology in the WiMAX family. WiMAX 2 offers maximum data speed of 1 Gbps compared to 100 Mbps by WiMAX.

Worldwide Interoperability for Microwave Access (WiMAX) and WiMAX 2

- In addition to higher data speeds, WiMAX 2 has better **backward compatibility** than WiMAX: WiMAX 2 network operators can provide seamless service by using 3G or 2G networks when required.
- By way of comparison, Long Term Evolution (LTE) and LTE-A also allow backward compatibility.

Long Term Evolution (LTE) and LTE-Advanced

- Long Term Evolution, a wireless wide-area network technology, was developed by members of the 3rd Generation Partnership Project body in 2008.
- This technology offers data speeds of up to 300 Mbps.
- LTE-Advanced (LTE-A) is a recent addition to the LTE technology that offers still-higher data rates of 1 Gbps compared to 300 Mbps by LTE.

Long Term Evolution (LTE) and LTE-Advanced

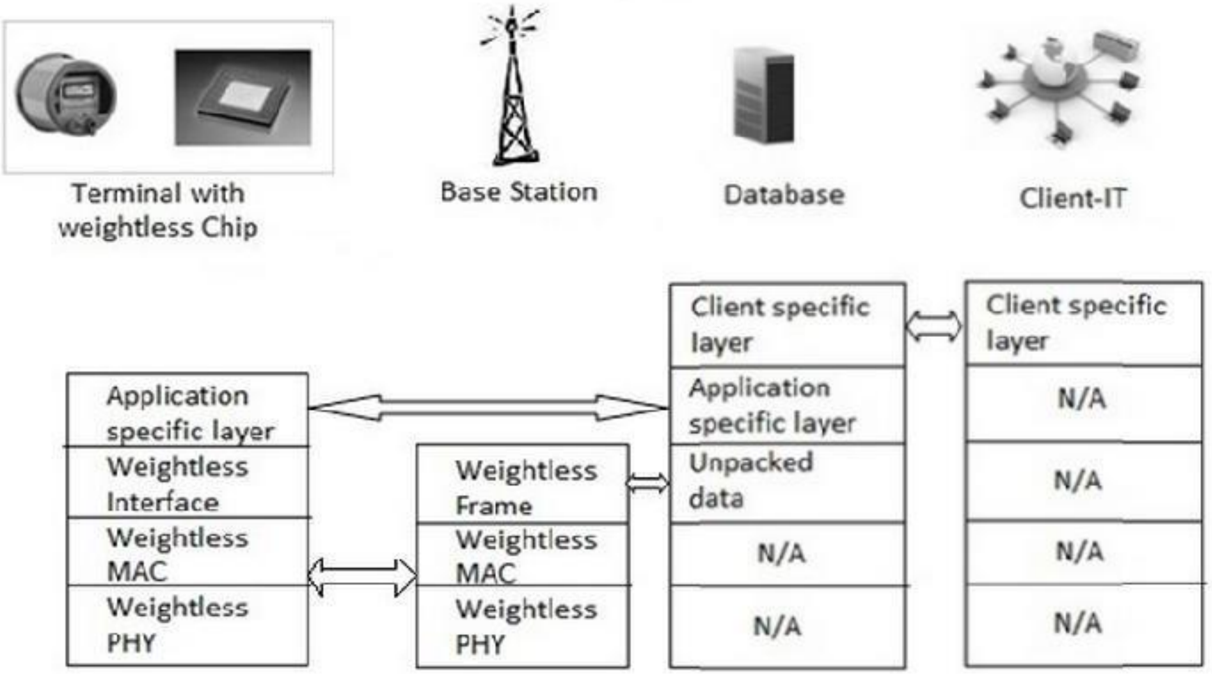
- There is debate among industry practitioners on whether LTE is truly a 4G technology: Many consider LTE a pre-4G technology and LTE-A a true 4G technology.
- Given its high bandwidth and low latency, LTE is touted as the more-promising technology for IoT applications;
- Uses advanced multiple access techniques i.e. OFDMA and SC-FDMA

Weightless

- Weightless is an open standard WAN technology introduced in early 2014.
- Uses Dynamic spectrum allocation.
- Uses unused bandwidth originally intended for TV broadcast.
- Can travel longer distances and penetrate walls.
- Supports Data rates of up to 16 Mbps in a wireless range of up to five kilometers, with batteries lasting up to 10 years

Weightless

- Devices remain in standby mode, waking every 15 minutes and staying active for 100 milliseconds to sync up and act on any messages
- Well suited for short message exchange in M2M Communications



IOT NETWORKS CHALLENGES

Challenges and Potential Solutions

- Even though network technologies have improved in terms of higher data rates and lower costs, there are challenges associated with:
  - **Data Explosion**,
  - **security**, and
  - **power consumption**.

Challenges and Potential Solutions: Data Explosion

- IoT devices generate tremendous amount of data.
- May become very costly to store data
- Need for efficient analytical algorithms for making use of the data.
- Recent focused on **Big Data, Artificial Intelligence, and Machine Learning.**

Challenges and Potential Solutions: Security

- Need for effective **Authentication and Access Control**
- **IPSec** is a potential solution. Requires large computational power. Is also defined as the encrypted, decrypted and authenticated packets
- Maintaining **data integrity** while remaining **energy efficient** stands as an enduring challenge.

Challenges and Potential Solutions: Power

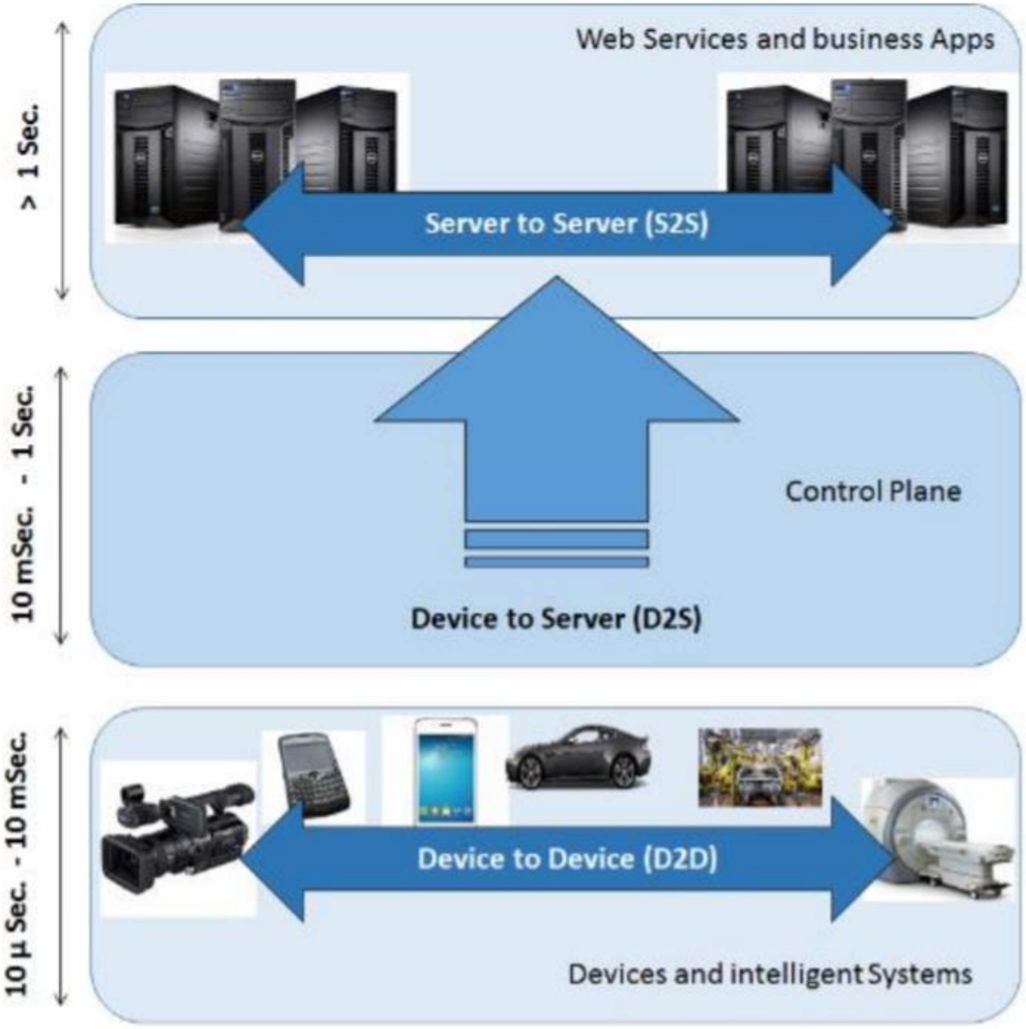
- Devices connected to a network consume power, and providing a **continuous power source** is a pressing concern for the IoT.
- Depending on the application, a combination of techniques such as **power-aware routing** and **sleep- scheduling protocols** can help to improve power management in networks.
- Power-aware routing protocols determine the routing decision based on the **most energy-efficient route** for transmitting data packets; **sleep-scheduling protocols** define how devices can "sleep" and remain inactive for better energy efficiency without impacting the output.

IOT ARCHITECTURES

IoT Communication Setup

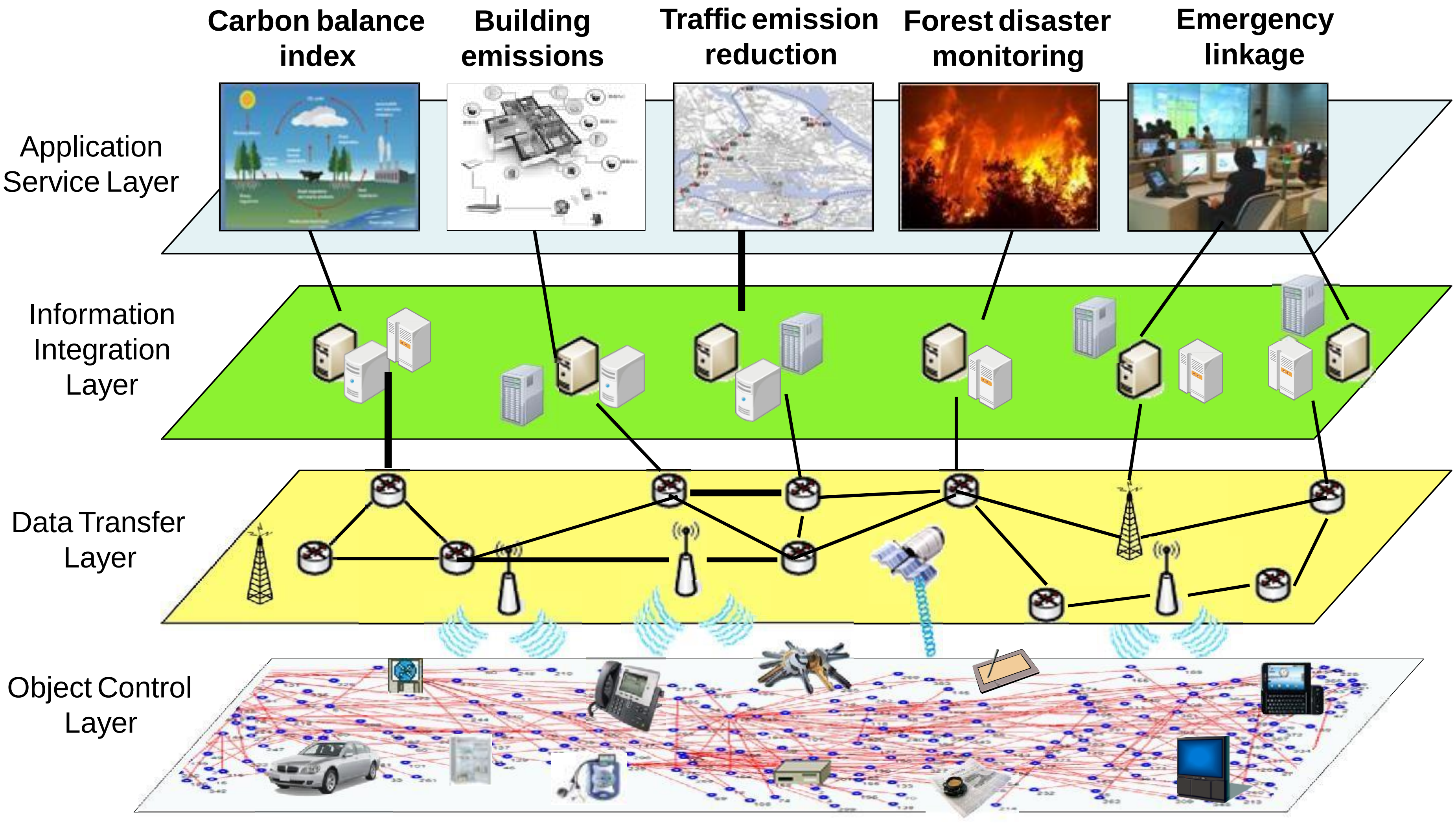
A common taxonomy:

- Devices must communicate with each other by Device to Device (**D2D**) setup.
- Then data collected from devices are transferred to the server infrastructure by Device to Server **(D2S).**
- The server infrastructure then share the device data by Server to Server **(S2S)**, possibly providing it back to devices, to analysis programs or to people.



Ref: R. Achary, J.S. Lalseta; *"Internet of Things: Essential Technology, Application Domain, Privacy and Security Challenges"* International Journal of Computer Applications, Vol. 157 – No 6, January 2017

IoT Network Structure/Architecture



Carbon balance index

Building emissions

Traffic emission reduction

Forest disaster monitoring

Emergency linkage

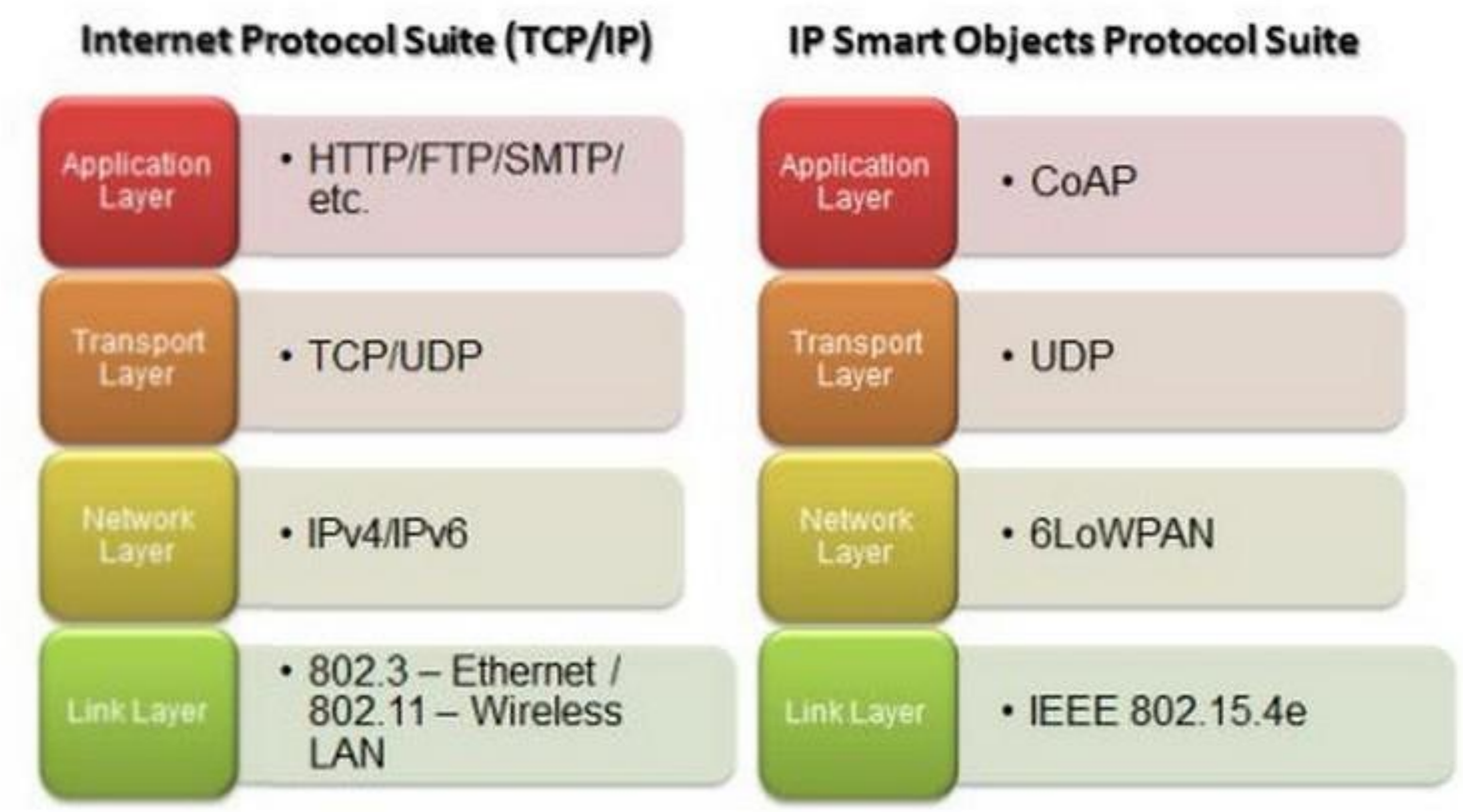
Application Service Layer

Information Integration Layer

Data Transfer Layer

Object Control Layer

IoT Protocol Stack, One Version!



Internet Protocol Suite (TCP/IP)

Application Layer	• HTTP/FTP/SMTP/ etc.
Transport Layer	• TCP/UDP
Network Layer	• IPv4/IPv6
Link Layer	• 802.3 – Ethernet / 802.11 – Wireless LAN

IP Smart Objects Protocol Suite

Application Layer	• CoAP
Transport Layer	• UDP
Network Layer	• 6LoWPAN
Link Layer	• IEEE 802.15.4e

Figure 1 TCP/IP Stack and IP Smart Objects Protocol Stack

Part 1.2 Data link

Queen Mary
University of London

Wired and Wireless LAN/PAN Attributes

- Ownership by a single organisation
- Medium to high data transmission rates
- Limited range of operation
- Shared transmission medium
- Low data error rates
- Inexpensive transmission media
- High to total connectivity and access
- De-centralised control and distributed operation
- Device, control, and manufacturer independence

Data link Layer

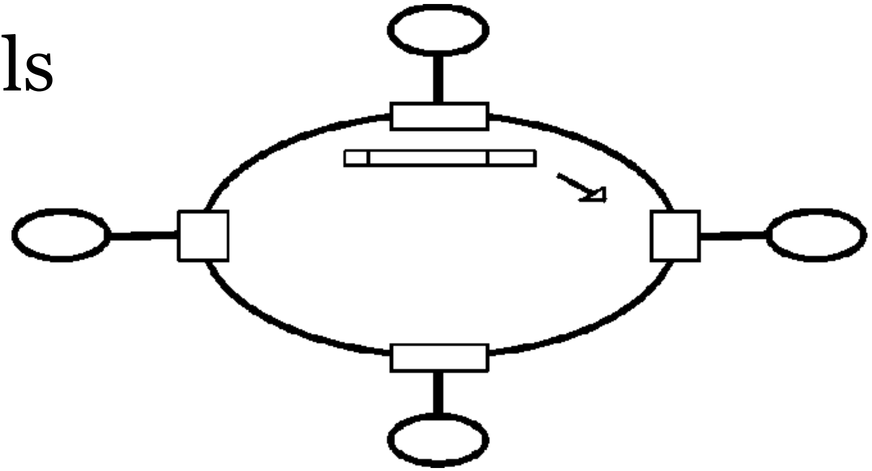
- MAC Sublayer
  - Access control to shared medium
  - Reliable data transmission
- Logical Link Control Sublayer
  - Provides the link between the higher layers and the communications media.
  - LLC provides three classes of service:
    - Unacknowledged connectionless service
    - Connection oriented service
    - Acknowledged connectionless service

Types of MAC Protocol

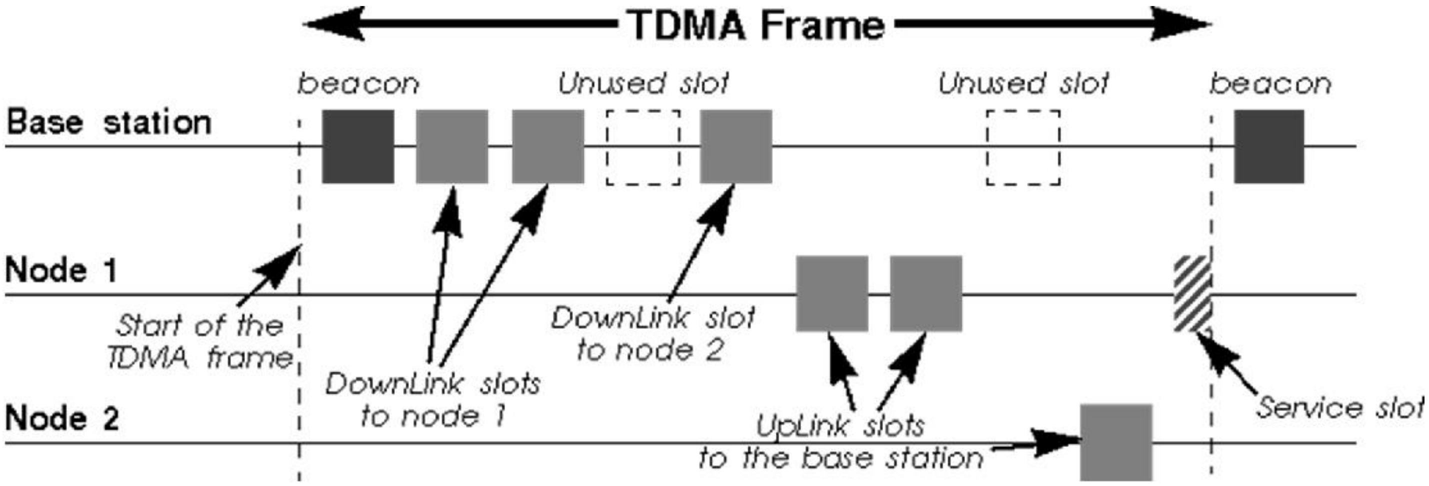
- Reservation based protocols
  - Required knowledge of network topology
  - Schedule for each end node
    - Fairness, priority
  - E.g. Token Ring and Time division Multiple Access (TDMA)
- Contention based protocols
  - No requirement for synchronization and topology knowledge
  - Nodes compete for resources
  - E.g. ALOHA and Carrier Sense Multiple Access

Token Ring Concept (Old technology)

- Access is controlled by gaining possession of a token, a special short frame.
- Token circulates around a ring in sequence
- Each node transmits its information in burst of maximum number of frames
- Operates at 4 - 16 Mbps
- Supports 8 priority levels

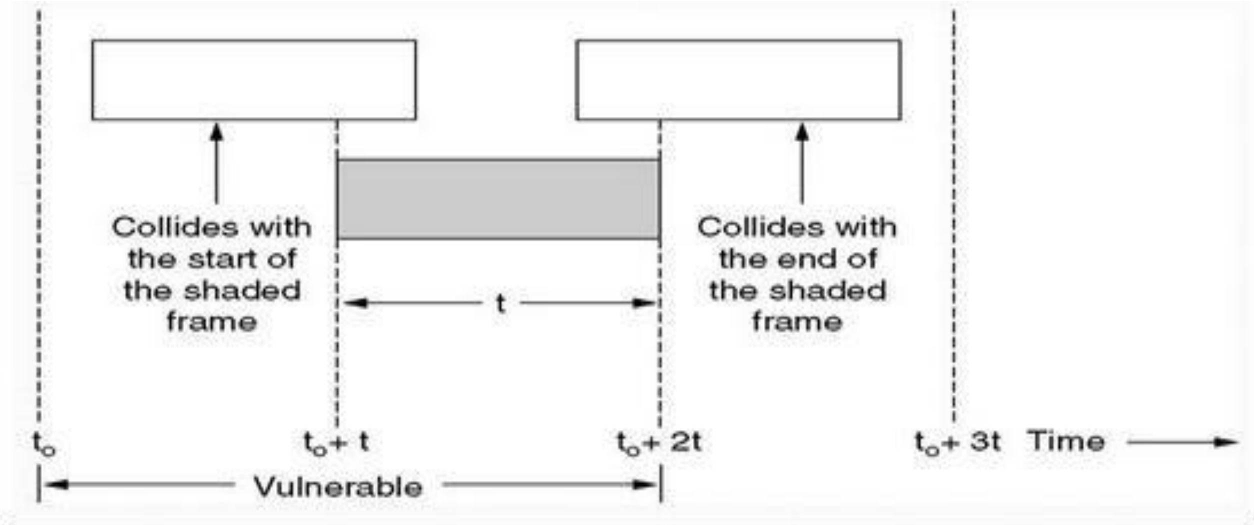


Time Division Multiple Access



- Needs centralized control synchronization between nodes and base station/access point.
- Access to channel in “rounds”
- Each node gets fixed length slot (length = pkt trans time) in each round
  - Beacon slot is for frame management
  - Service slot is used for nodes to request connection

Unslotted ALOHA


Collides with the start of the shaded frame
Collides with the end of the shaded frame
t
t_o
t_o+ t
t_o+ 2t
t_o+ 3t
Time
Vulnerable

EFFICIENCY OF ALOHA

- Transmit data whenever there is a data to be transmitted.
- If frame transmitted successfully, the next frame will be transmitted.
- If frame fail to transmit then the source will resend the same frame again.

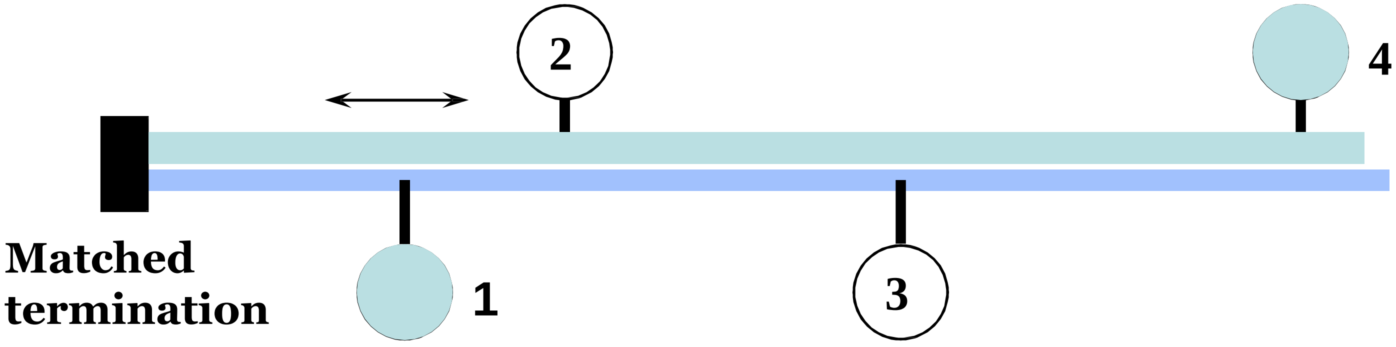
Slotted ALOHA

- Time is divided into equal size slots, time to transmit one frame
- Requires synchronization
- All stations need to wait until the beginning of each frame to transmit
- If two or more nodes transmit in slot, all nodes detect collision
- When node obtains fresh frame, it transmits in next slot
- No collision, node can send new frame in next slot
- If collision occurs, node retransmits frame in subsequent slot with probability p until success

CSMA/CD Access Protocol (Part I)

- Carrier Sense Multiple Access with Collision Detection
- The CSMA/CD access protocol is most easily described by employing an analogy
- i.e. the protocol used in a meeting between polite people
  - Listen before talking
  - Don’t talk while someone else is talking
  - Don’t ramble on incessantly
  - Stop and back-off if you find yourself starting to speak at the same time as someone else
  - Acknowledge the integrity of messages received

CSMA/CD Example



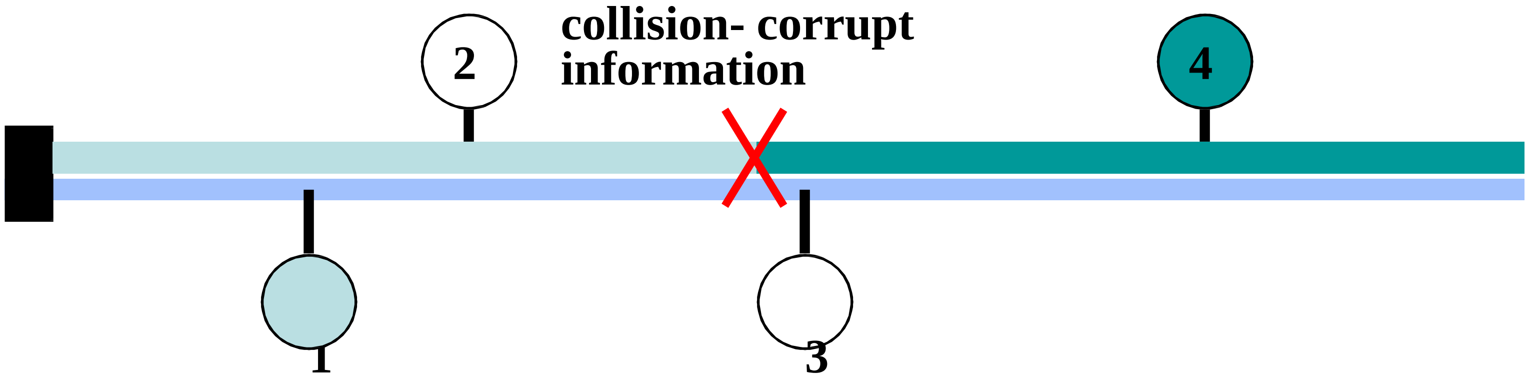
No reflection because of matched termination

1 wishes to transmit information to 4 - it waits until the medium is quiet and then transmits a frame which propagates along the medium

4 recognises that the frame is for it and reads the information.

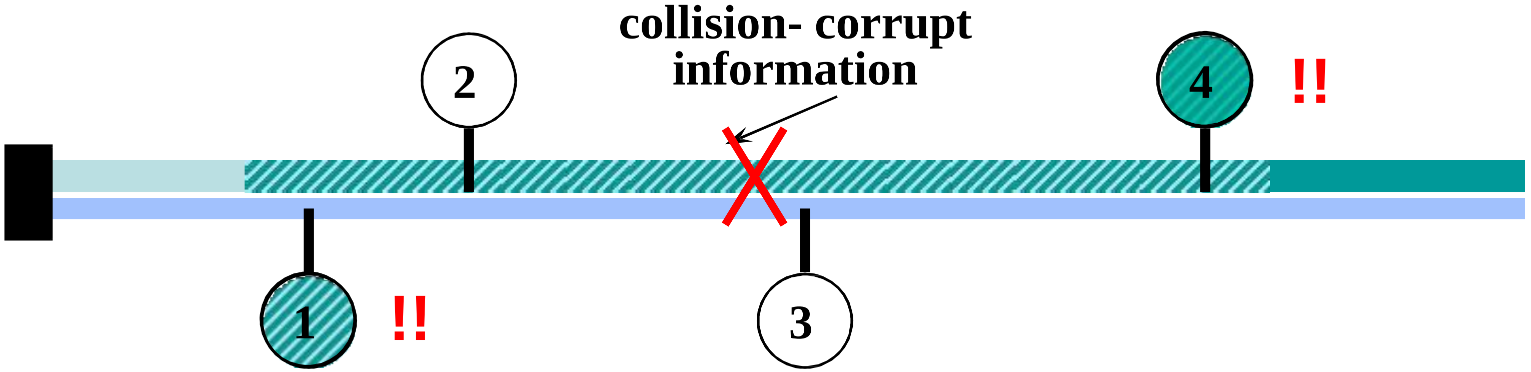
CSMA/CD Example

What happens when two stations transmit concurrently?



- **Both wait until the medium is quiet and then each transmits a frame which each propagates along the medium.**
- **When the 2 propagating frames meet there is a "collision" - the corrupt collision information now propagates.**

CSMA/CD Example



- When the 2 propagating frames meet there is a “collision” - the corrupt collision information now propagates.
- Individual nodes cannot unscramble the mixed signals
- Eventually the corrupt information reaches one of the transmitting nodes; this is still transmitting and detects that information on the bus is not the same
- Enter Binary Exponential Backoff and then Retry

CSMA/CD Access Protocol (Part II)

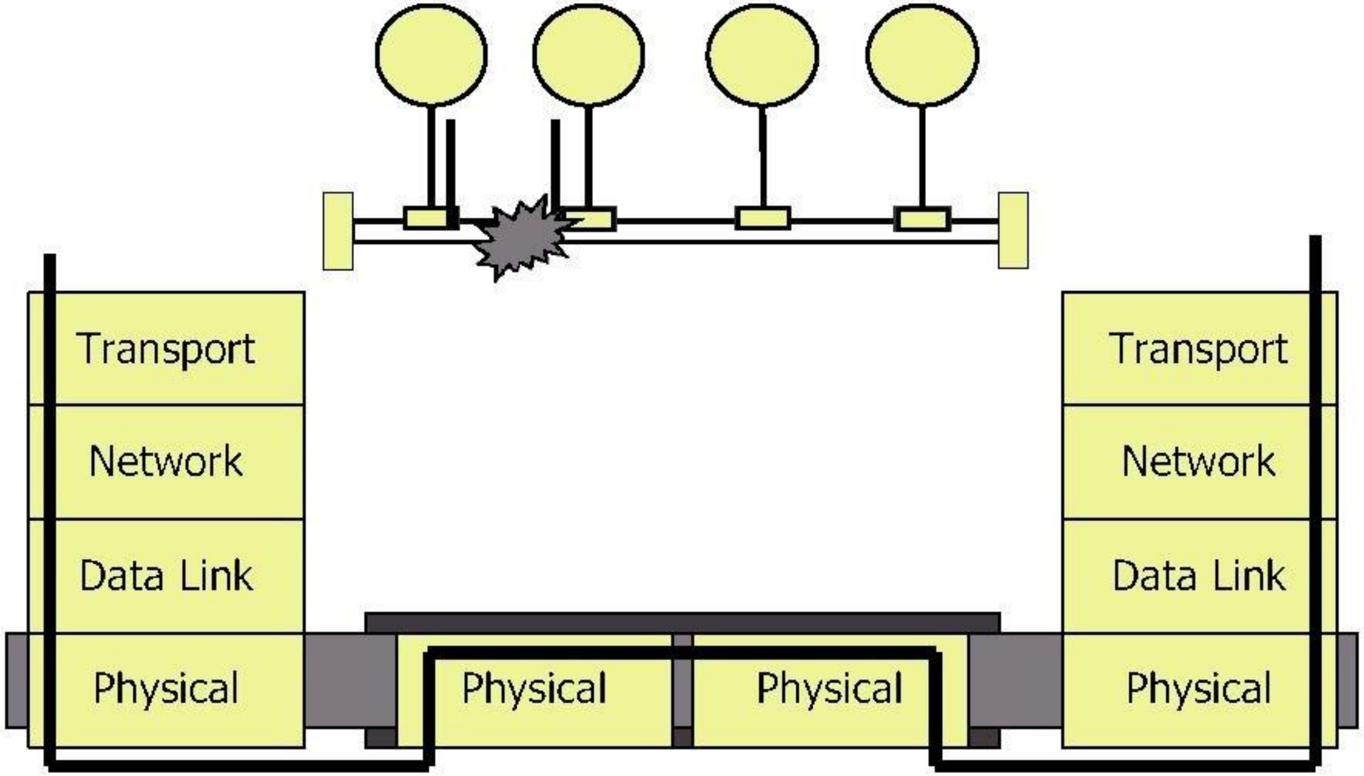
- Collision Detection
- Collision Window
  - Related to end-to-end propagation delay
- Minimum packet size must be greater than collision window

CSMA/CD Access Protocol (Part III)

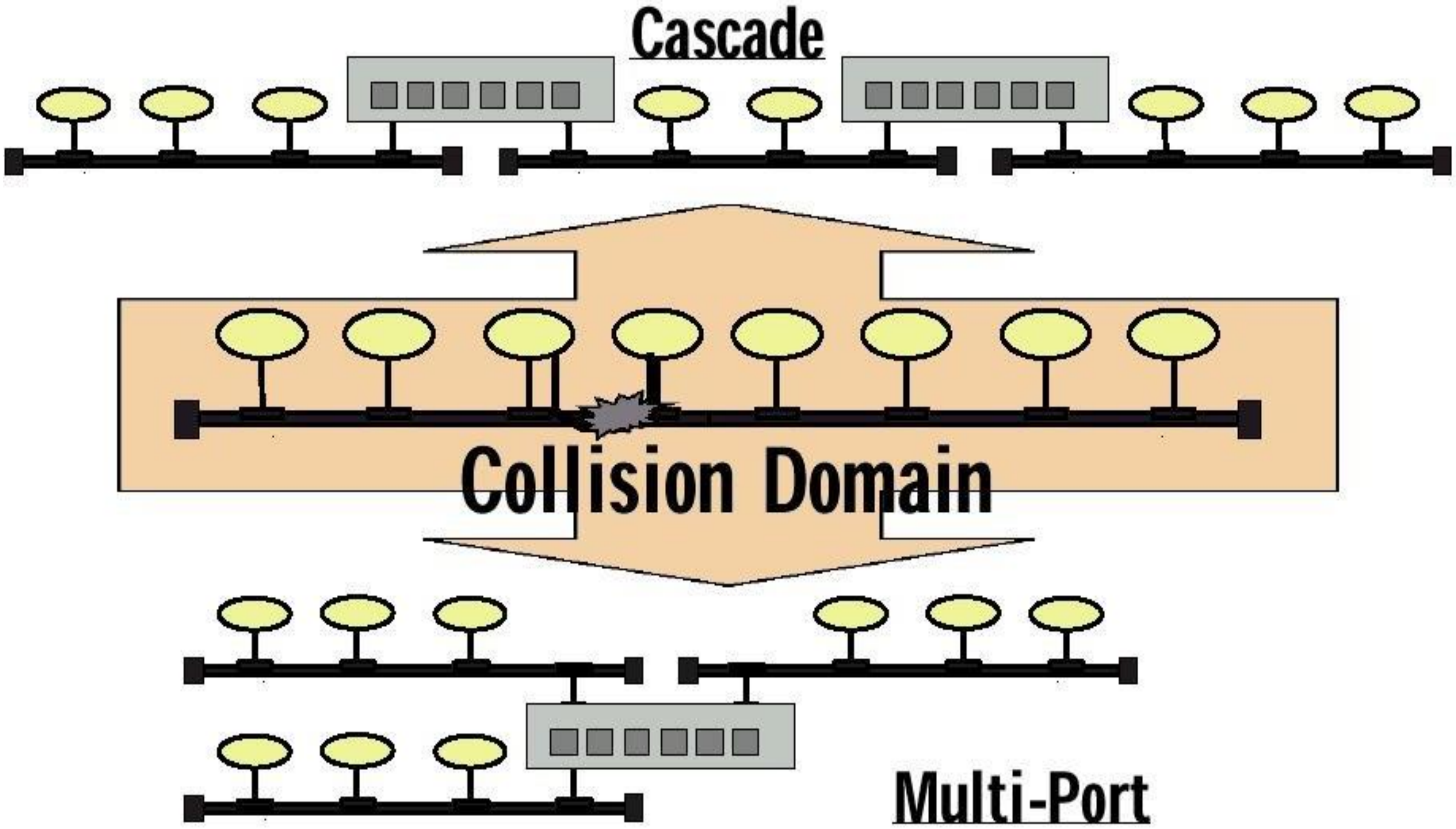
- Back-Off
  - Nodes wait a random time before attempting to retransmit data.
  - Truncated Binary Exponential Back-Off Algorithm.
  - After a collision, a node waits X slot-times* where X is a Random number taken from the following distribution:
  - [0, $(2^N -1)$] $0 \leq N \leq 10$
  - [0, 1023] $11 \leq N \leq 16$ N = number of retransmission attempts
- After 16 attempts, frame is lost. LLC problem!

One slot time is the round-trip time associated with a minimum sized frame, i.e. 51.2uS

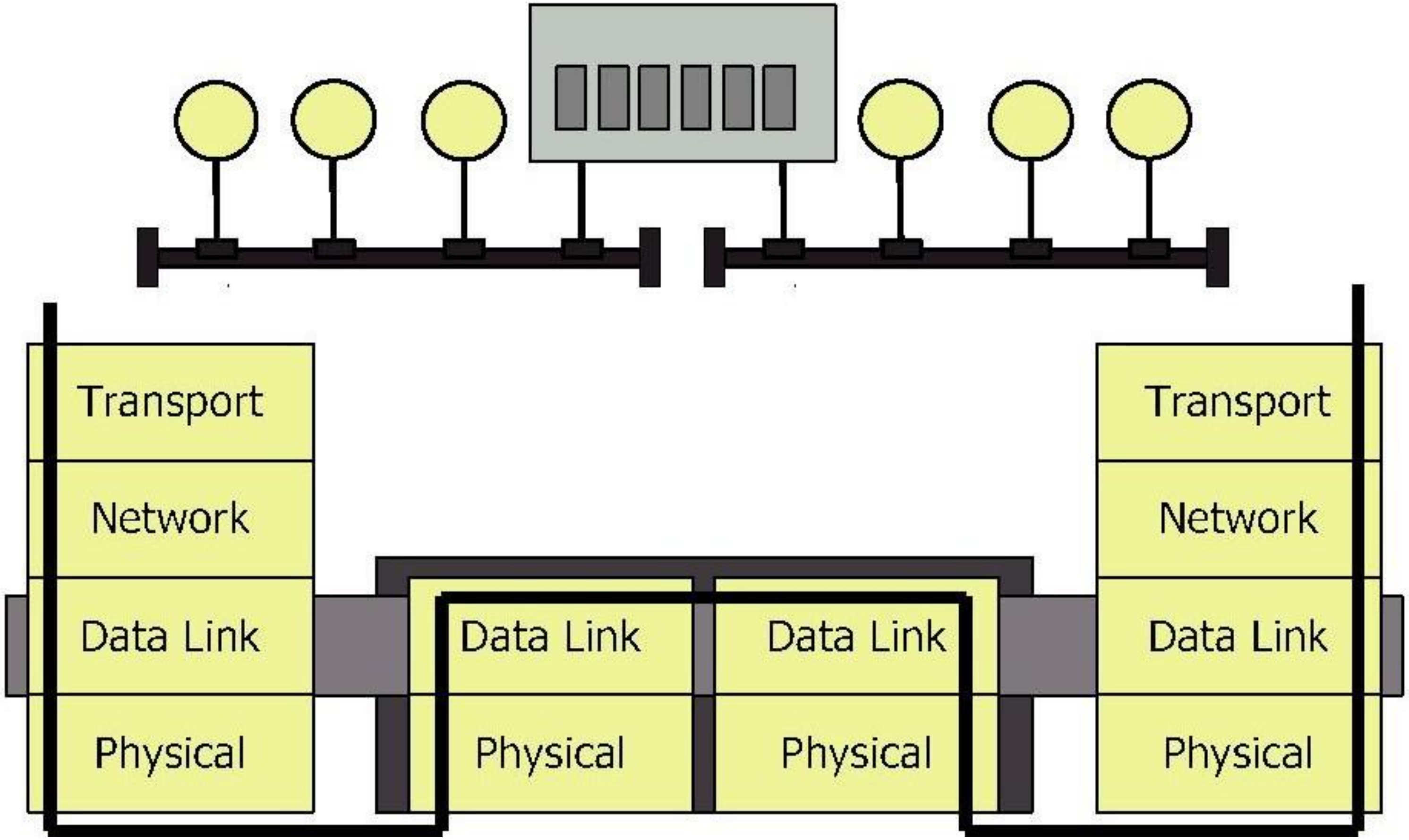
Inter-Networking – Physical Layer



Inter-Networking – Repeaters

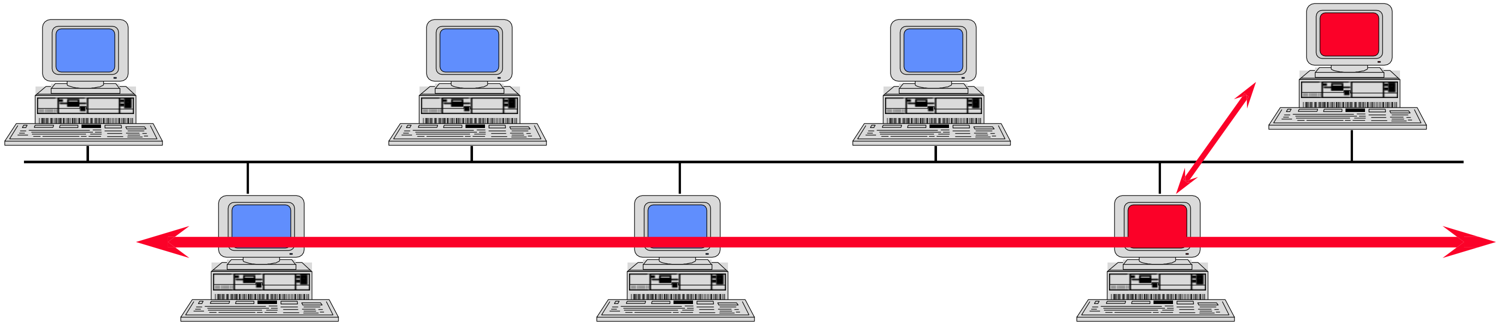


Inter-Networking – Data-Link Layer

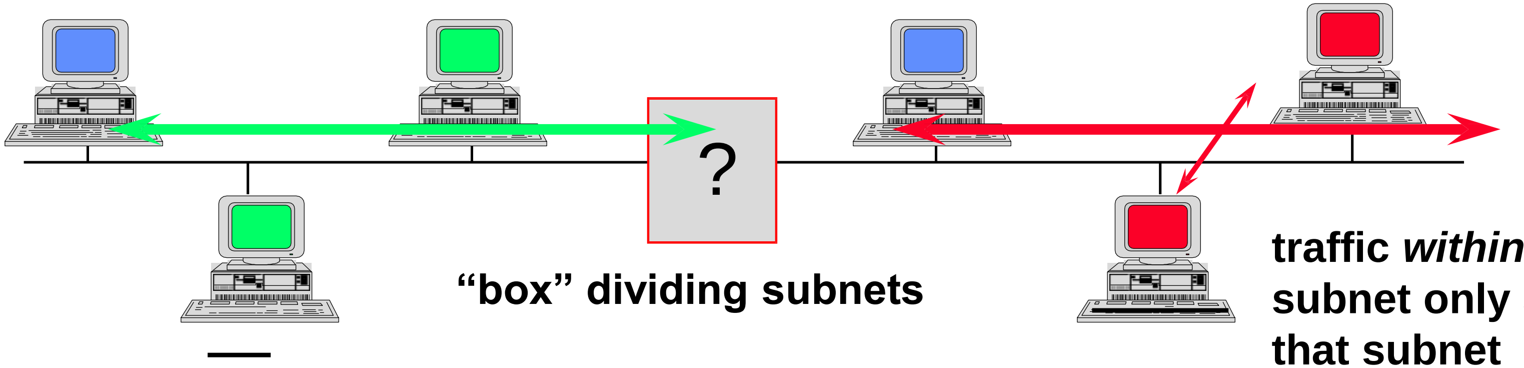


Traffic Flows - Reducing Collisions

We aim to segregate traffic flows to avoid congestion



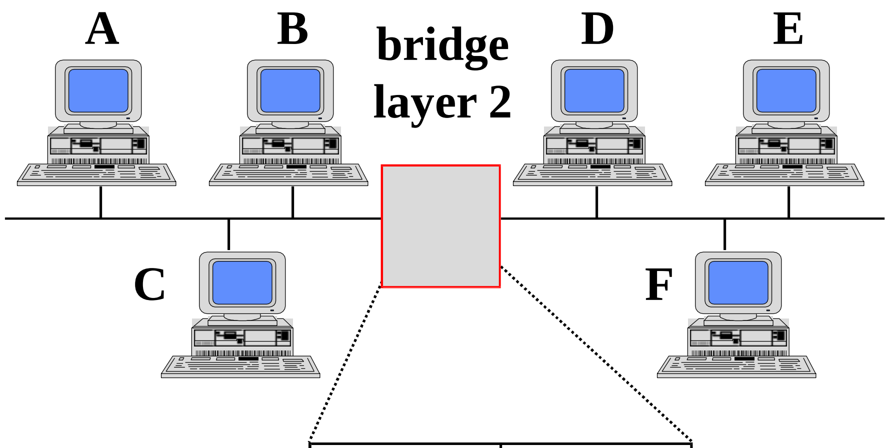
one network - traffic between 2 machines carried over whole network



“box” dividing subnets

traffic *within* a subnet only affects that subnet

Bridge Filtering by MAC Address



Bridge:

Layer 2 function works on MAC addresses cannot do routing can do filtering of traffic

Tables can be static and entered by a management process or the bridge can be self-learning

MAC table 1	MAC table 2
A	D
B	E
C	F

Bridge recognises whether MAC address of destination is on same side as source - if so it does not transmit it through the bridge - note that this is based on hardware MAC addresses, not IP addresses