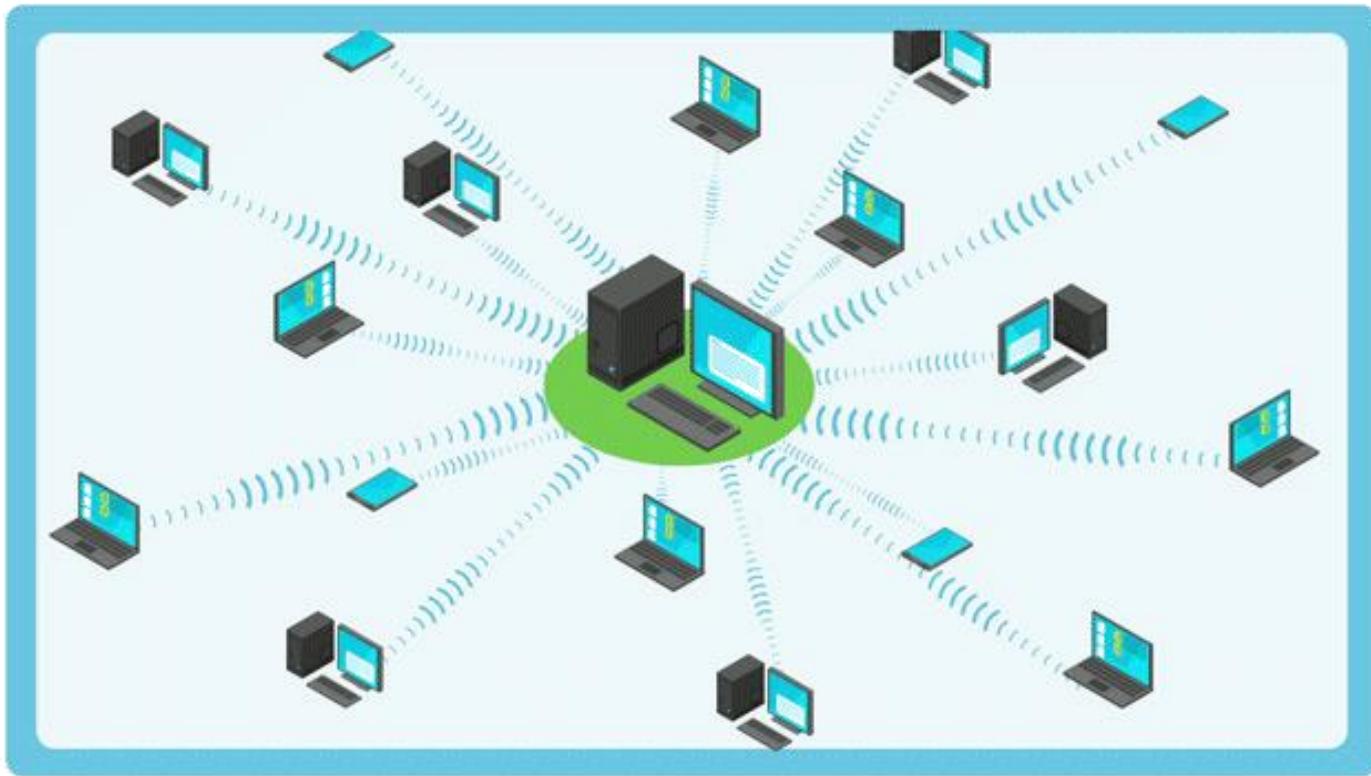
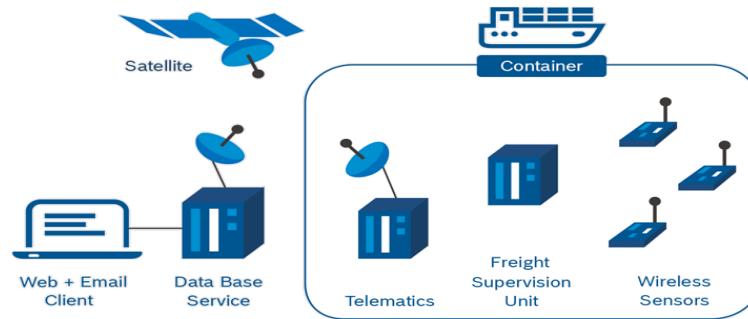


DATA and DIGITAL COMMUNICATIONS

INTRODUCTION TO NETWORK ENGINEERING
CHAPTER 2



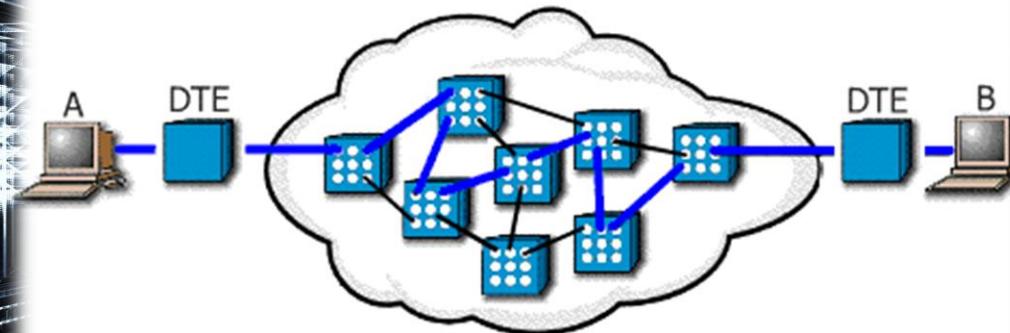
Chapter 2



Introduction to Network Engineering

- Principles of Data Communications
- Ethernet and Wi-Fi Technologies
- Computer Networks and the Internet
- Cybersecurity and Industry 4.0

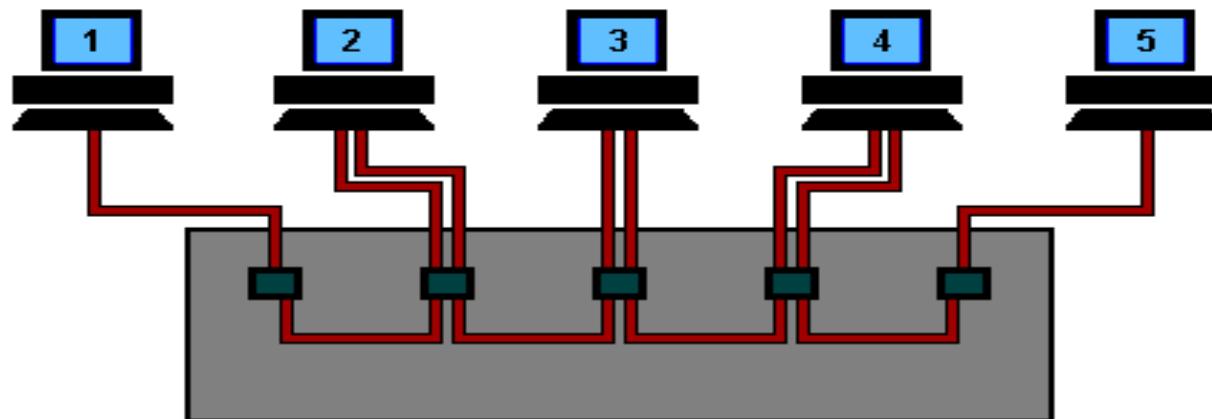
Module 5



Principles of Data Communications

Principles of Data Communications

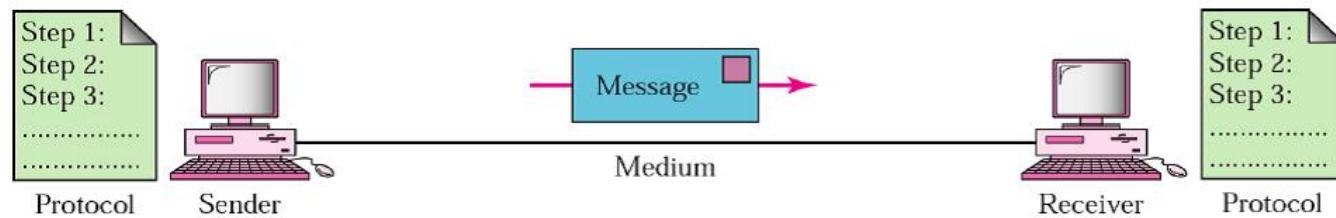
Data Communications is the transmission of digital data between two or more computers. It involves processes using computing and communication technologies to transfer data from one place to another, and vice versa.



Principles of Data Communications

Main Components of Data Communications

- Sender
- Receiver
- Medium
- Message
- Protocol



Data communications aims to provide the highest possible transmission rate of digital data between two or more computers at the lowest possible power and with the least possible noise. It is intended to provide the rules (protocols) and regulations (standards) that will allow computers with different disk operating systems, languages, and locations to share resources.

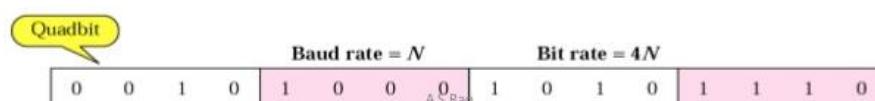
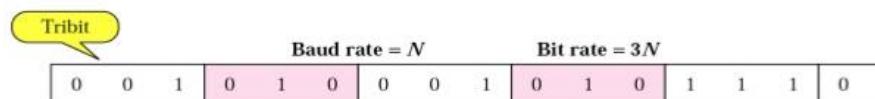
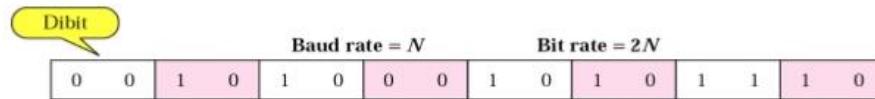
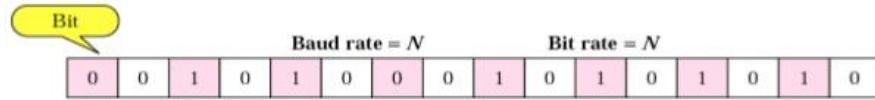
Principles of Data Communications

Data is information in numerical form that can be digitally transmitted or processed, while **signal** is a function that conveys information and can be used to transfer data from one device to another device. Both can have either an analog or a digital form.

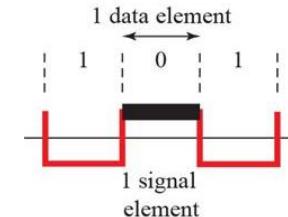
Term	Definition	Unit
Data Element	a single binary 1 or 0	Bit
Data Rate / Bit Rate	rate at which data elements are transmitted	Bits per second (bps)
Signal Element	part of a signal that occupies the shortest interval of a signaling code	Digital: voltage pulse of constant amplitude Analog: voltage pulse of constant amplitude, frequency, and phase
Signaling Rate / Baud Rate (Modulation Rate)	rate at which signal elements are transmitted	Baud

Principles of Data Communications

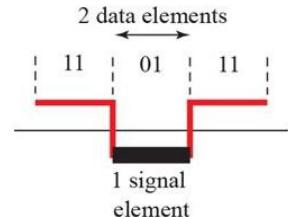
Bit Rate vs Baud Rate



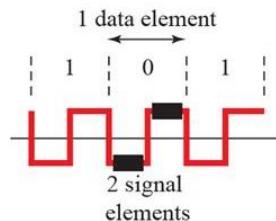
$$\text{transmission ratio } r = \frac{\text{no. of data elements}}{\text{1 signal element}}$$



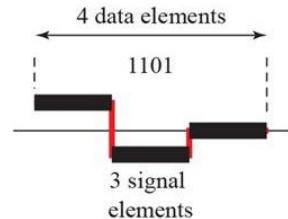
a. One data element per one signal element ($r = 1$)



c. Two data elements per one signal element ($r = 2$)



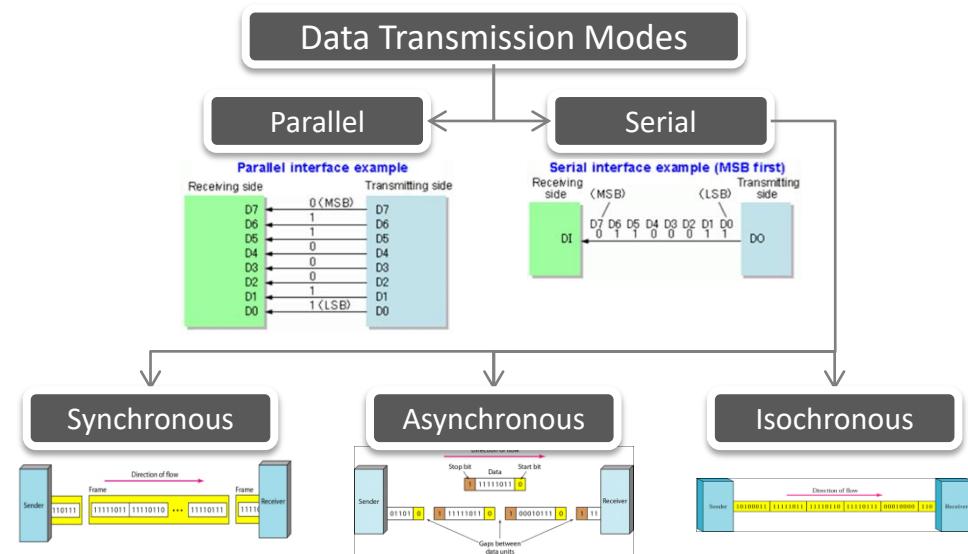
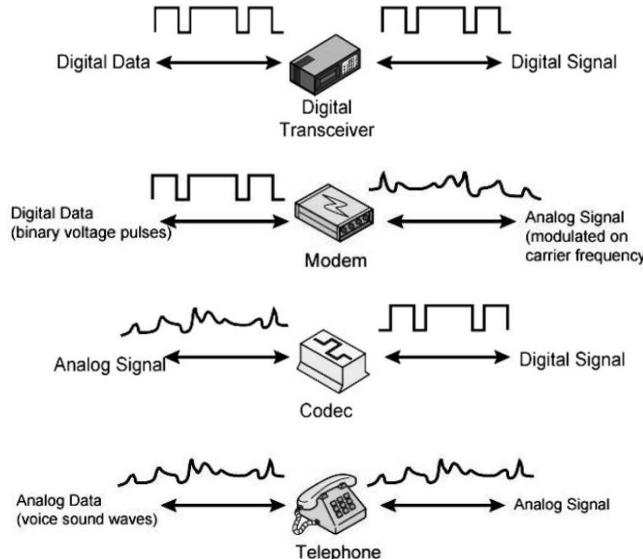
b. One data element per two signal elements ($r = \frac{1}{2}$)



d. Four data elements per three signal elements ($r = \frac{4}{3}$)

Principles of Data Communications

Data transmission is the process of transferring data between two or more digital devices. Data is transmitted from one device to another in analog or digital format.



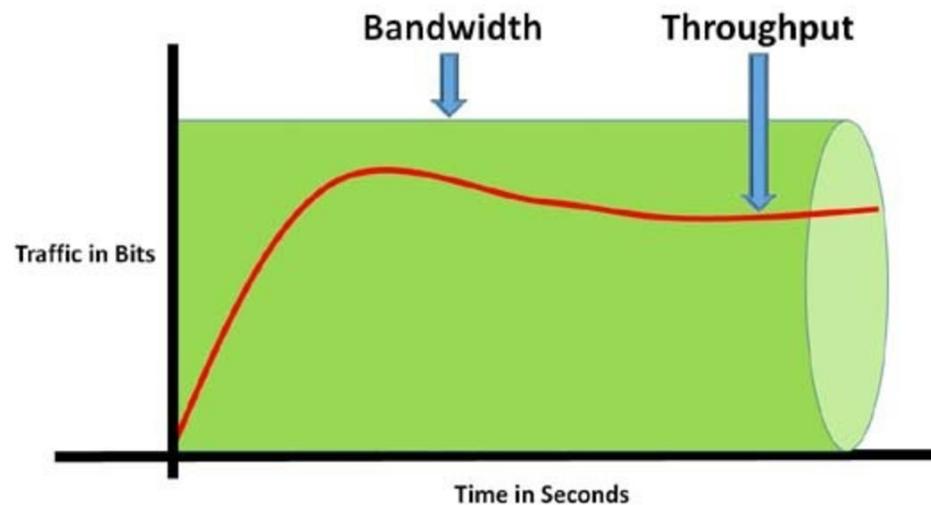
Principles of Data Communications

Throughput is an actual measure of transmission speed or how much data is successfully transferred per unit time, while **bandwidth** is a theoretical measure of how much data could be transferred from source to destination.

$$\eta = \frac{T_t}{T_t + 2T_p} \quad B = \frac{L}{T_t}$$

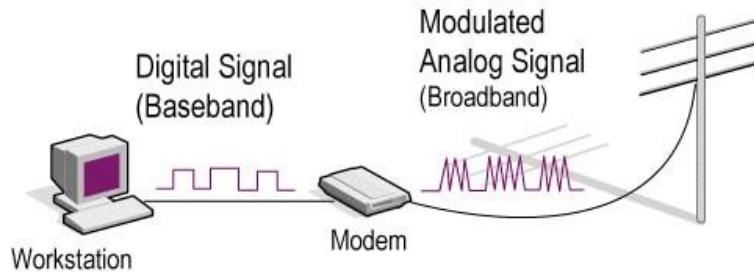
$$TP = \eta B \quad T_p = \frac{d}{v}$$

where:
 η = efficiency
 B = bandwidth
 TP = throughput
 T_t = transmission delay
 T_p = propagation delay
 d = propagation distance
 v = transmission speed



Principles of Data Communications

Baseband and Broadband Data Transmission



BASEBAND TRANSMISSION

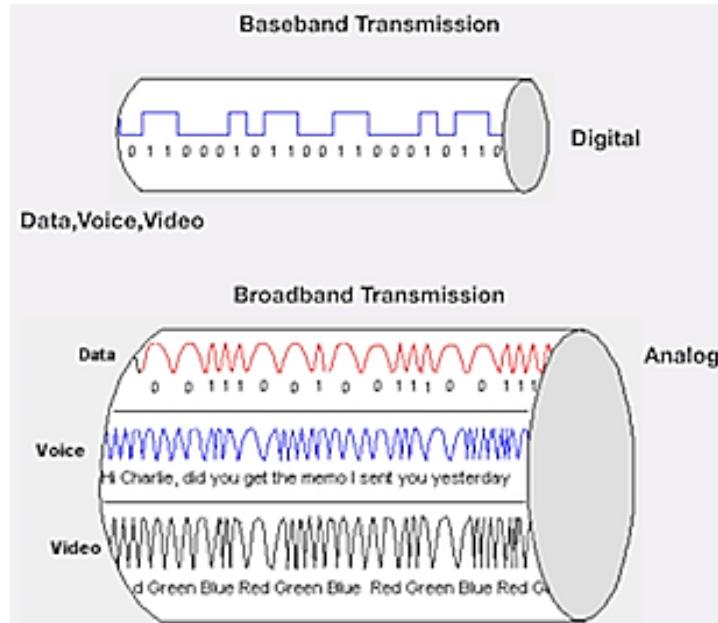
Baseband Transmission is a transmission technique that one signal requires the entire bandwidth of the channel to send data.

Baseband Transmission uses digital signals.

BROADBAND TRANSMISSION

Broadband Transmission is a transmission technique that many signals with multiple frequencies transmit data through a single channel simultaneously.

Broadband Transmission uses analog signals.



Principles of Data Communications

Universal Asynchronous Receiver/Transmitter (UART)

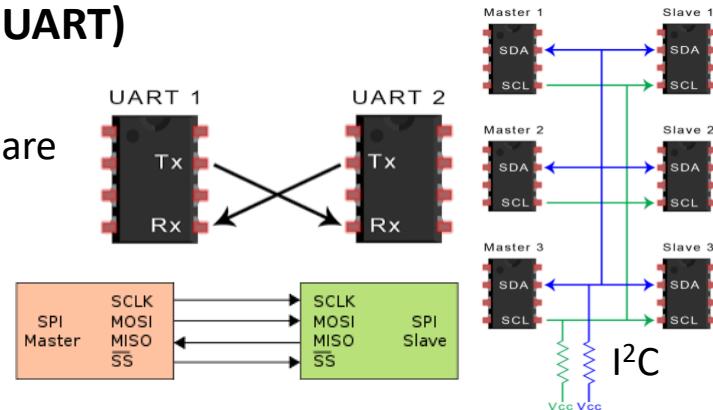
- device for asynchronous serial communication
configurable data format and transmission speeds are

Serial Peripheral Interface (SPI)

- synchronous serial communication interface
specification used for short-distance
communication, primarily in embedded systems

Inter-Integrated Circuit (I2C or I2C)

- serial protocol for 2-wire interface to connect
low-speed devices like microcontrollers and
other similar peripherals in embedded systems



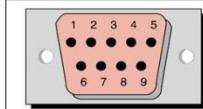
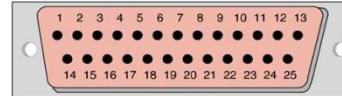
Standard	Tx Type	# Signal Wires	Data Rate & Distance	Hardware \$	Scalability	Application Example
UART	Asynchronous	2	20kbps @ 15m	Medium (transceiver)	Low (point-to-point)	Diagnostic display
LIN	Asynchronous	2	20kbps @ 40m	Medium (transceiver)	High (identifier)	Washing machine subsystem network
SPI	Synchronous	4+	25Mbps @ 0.1m	Low	Medium (chip selects)	High speed chip to chip link
I ² C	Synchronous	2	1Mbps @ 0.5m	Low (resistors)	High (identifier)	System sensor network

Principles of Data Communications

RS-232, RS-422, and RS-485 Standards



DB15

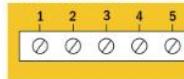


Pin Number	Signal Designation
1	Carrier detect
2	Receive data
3	Transmit data
4	Data terminal ready
5	Protective ground
6	Data set ready
7	Request to send
8	Clear to send
9	Ring indicator

Pin Number	Signal Designation	Pin Number	Signal Designation
1	Protective ground	14	Secondary transmit data
2	Transmit data	15	Transmit clock (DCE)
3	Receive data	16	Secondary receive data
4	Request to send	17	Receiver clock
5	Clear to send	18	Receiver bit clock
6	Data set ready	19	Secondary request to send
7	Signal ground	20	Data terminal ready
8	Carrier detect	21	Signal quality detector
9	Positive DC test voltage	22	Ring indicator
10	Negative DC test voltage	23	Data signal rate selector
11	Unassigned	24	Transmit clock (DTE)
12	Secondary carrier detect	25	Busy
13	Secondary clear to send		



Screw Terminals



DB9F Connector



RS422/485 Pinout

Screws	Signal	DB-9F
1	RX+	1
2	RX-	2
3	TX+/D+	4
4	TX-/D-	3
5	GND	5



- Mode of Operation
- Total Number of Drivers and Receivers on One Line
- Maximum Cable Length
- Maximum Data Rate @Max length
- Driver Output Signal Level (Loaded Min.)
- Driver Output Signal Level (Unloaded Max)
- Driver Load Impedance
- Max. Driver Current in High Z State
- Max. Driver Current in High Z State
- Slew Rate (Max.)
- Receiver Input Voltage Range
- Receiver Input Sensitivity
- Receiver Input Resistance

RS-232

SINGLE-ENDED

1 DRIVER	32 DRIVER
1 RECEIVER	32 RECEIVER
50 FEET	4000 FEET
20kb/s	100kb/s

RS-485

DIFFERENTIAL

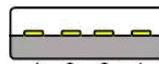
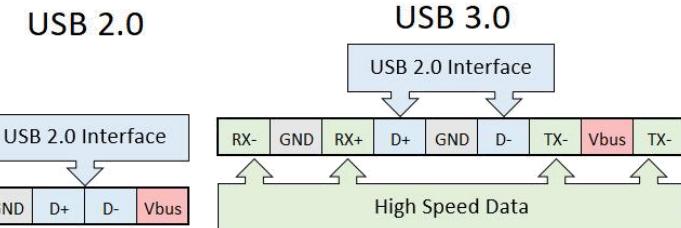
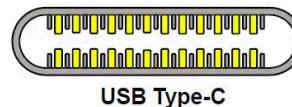
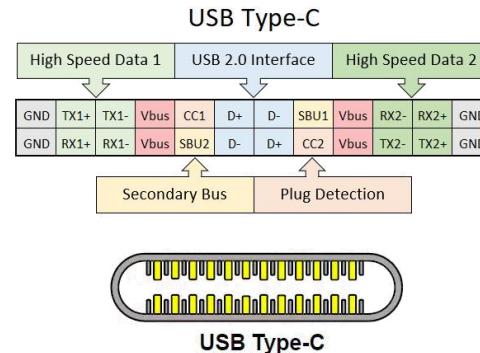
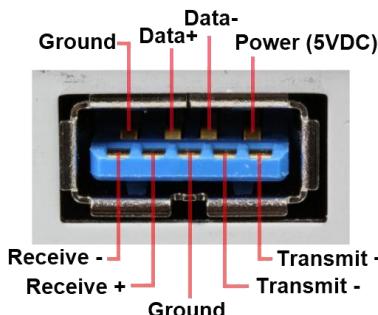
+/-5V to +/-15V	+/-1.5V
+/-25V	+/-6V
3kΩ to 7kΩ	54Ω
N/A	N/A
+/-6mA @ +/-2v	+/-100µA
30V/µS	N/A
+/-15V	-7V to +12V
+/-3V	+/-200mV
3kΩ to 7kΩ	≥ 12kΩ



Principles of Data Communications

Universal Serial Bus (USB)

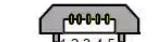
- enables communication between devices and a host controller such as a personal computer
- external bus standard that supports data transfer rates of 12 Mbps and can be used to connect up to 127 peripheral devices



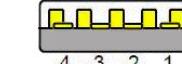
USB2.0 Type-A



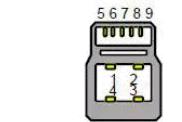
USB2.0 Mini-A



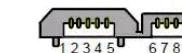
USB2.0 Micro-B



USB3.0 Type-A



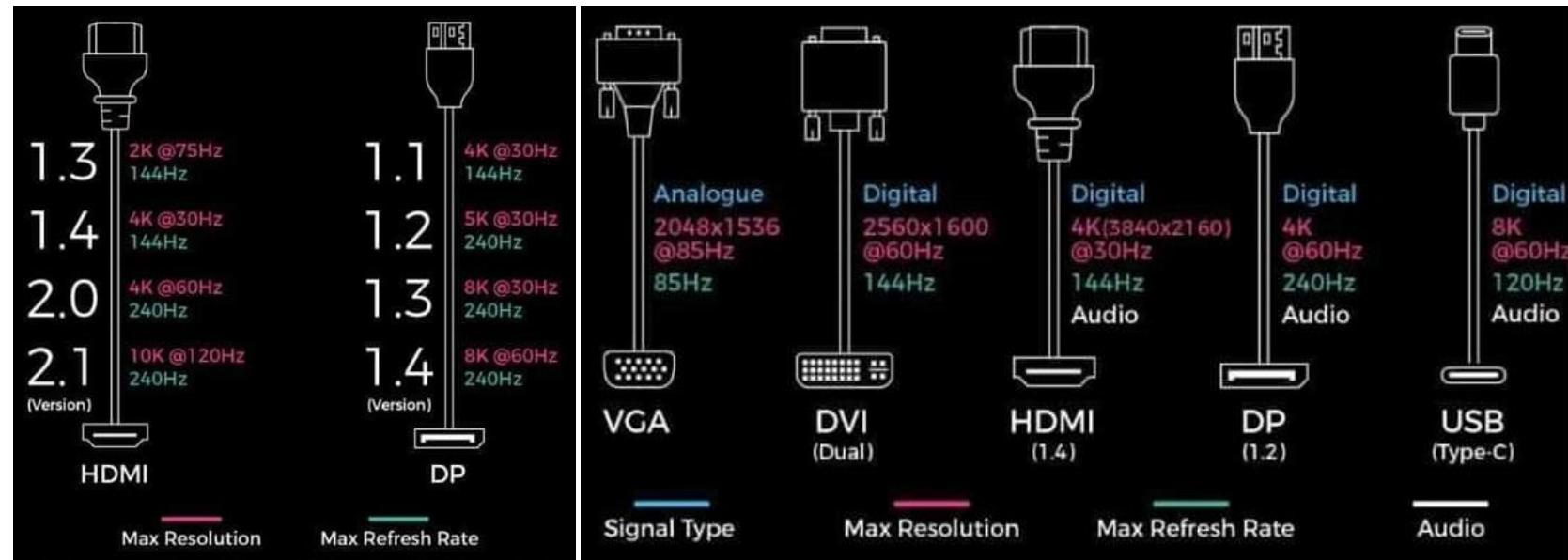
USB3.0 Type-B



USB3.0 Micro-B

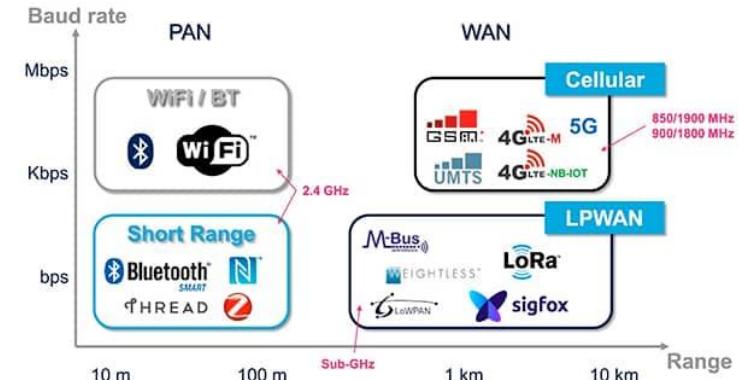
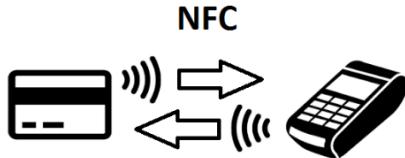
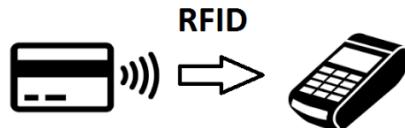
Principles of Data Communications

Data and Audio/Video Transmission Media



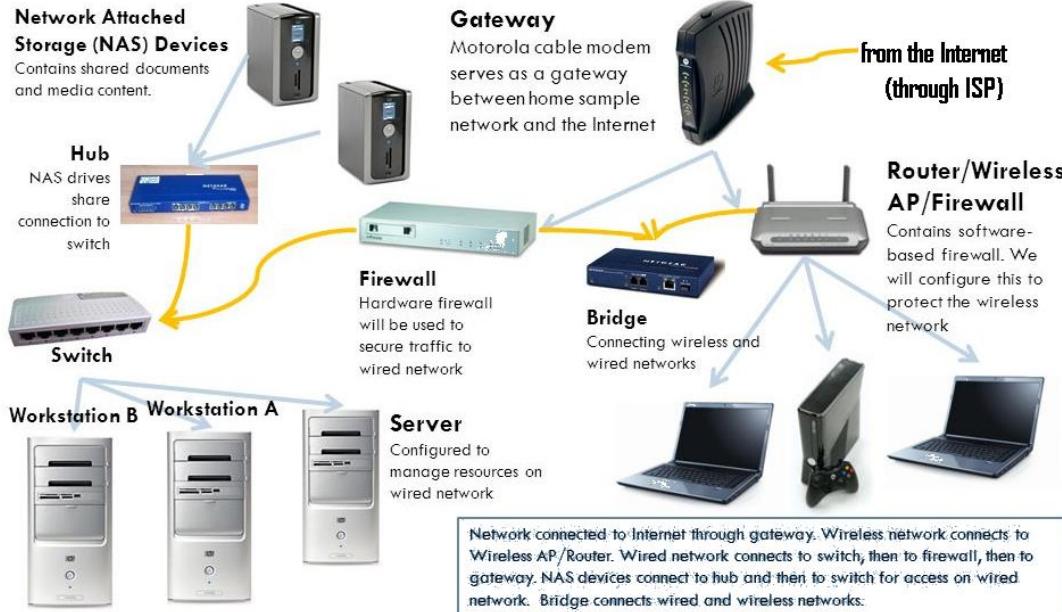
Principles of Data Communications

Short-Distance Wireless Data Transmission Technologies

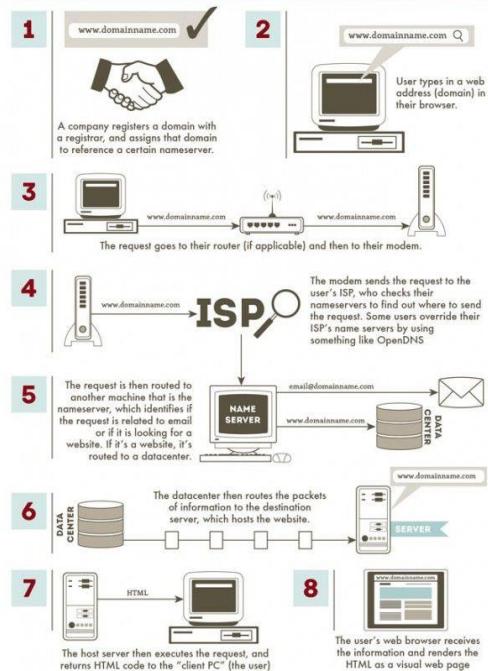


Principles of Data Communications

Computer Networks and the Internet



How the Internet Works



Principles of Data Communications

Common Data Communication Devices

- Gateway – allows data to flow from one discrete network to another
- Modem – allows devices to communicate with other remote devices by converting digital data into analog data and transmitting it over an analog telephone line
- Firewall – prevents unauthorized use and access to the network
- Router – responsible for sending data from one network to another
- Switch – uses the MAC address of a device to send data only to the port the destination device is plugged into
- Bridge – creates a single aggregate network from multiple communication networks or network segments
- Hub – similar to a switch, but it broadcasts data to all ports
- Wireless Access Point – allows Wi-Fi devices to connect to a wired network

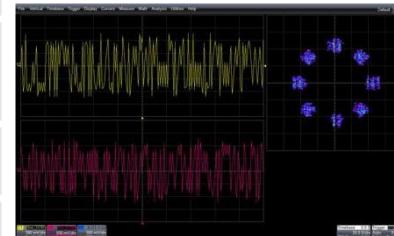
Principles of Data Communications

Ethernet and Wi-Fi

	WiFi	Ethernet
Speed	Slow data transfer speed	Faster data transfer speed
Reliability	Suffers from signal interference due to many environmental factors	Delivers a consistent speed
Security	Data flow needs to be encrypted	Data doesn't require to be encrypted
Latency	Higher	Lower
Deployment	Easy to install and deploy	Cable installation infrastructure is required



Ethernet Signals (via Cable)



Wi-Fi Signals (via Air)

Principles of Data Communications

International ICT-Related Organizations and Standards

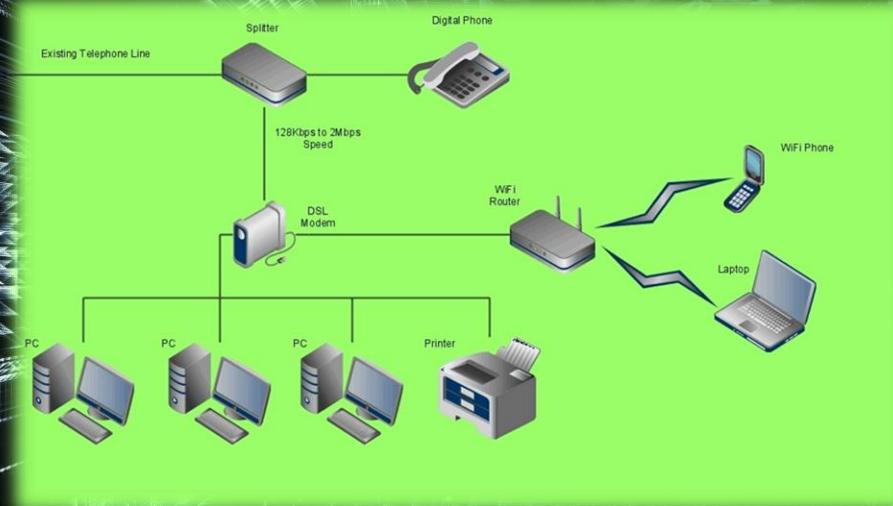
ANSI	American National Standards Institute
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunications Union
ISO	International Organization for Standardization
ISOC	Internet Society
IETF	Internet Society and the Internet Engineering Task Force
EIA/TIA	Electronic Industries Alliance and the Telecommunications Industry Association

Signaling rate	Example bus standard	Fundamental frequency	Optimum antenna length
100 kbits/s	TIA/EIA-423	50 kHz	1,500 meters
1 Mbit/s	TIA/EIA-422	500 kHz	150 meters
10 Mbits/s	TIA/EIA-485	5 MHz	15 meters
200 Mbits/s	IEEE 1394 Firewire	100 MHz	75 cm
400 Mbits	ANSI TIA/EIA-644 LVDS	200 MHz	50 cm
2 Gbits/s	IEEE 802.3 Gbit Ethernet	1 GHz	7.5 cm

IEEE 802 standards

Standard	Name	Explanation
802.1	Internetworking	Covers routing, bridging, and inter-network communications
802.2	Logical Link Control	Covers error control and flow control over data frames
802.3	Ethernet LAN	Covers all forms of Ethernet media and interfaces, from 10 Mbps to 10 Gbps (10 Gigabit Ethernet)
802.4	Token Bus LAN	Covers all forms of token bus media and interfaces
802.5	Token Ring LAN	Covers all forms of token ring media and interfaces
802.6	Metropolitan Area Network	Covers MAN technologies, addressing, and services
802.7	Broadband Technical Advisory Group	Covers broadband networking media, interfaces, and other equipment
802.8	Fiber-Optic Technical Advisory Group	Covers use of fiber-optic media and technologies for various networking types
802.9	Integrated Voice/Data Networks	Covers integration of voice and data traffic over a single network medium

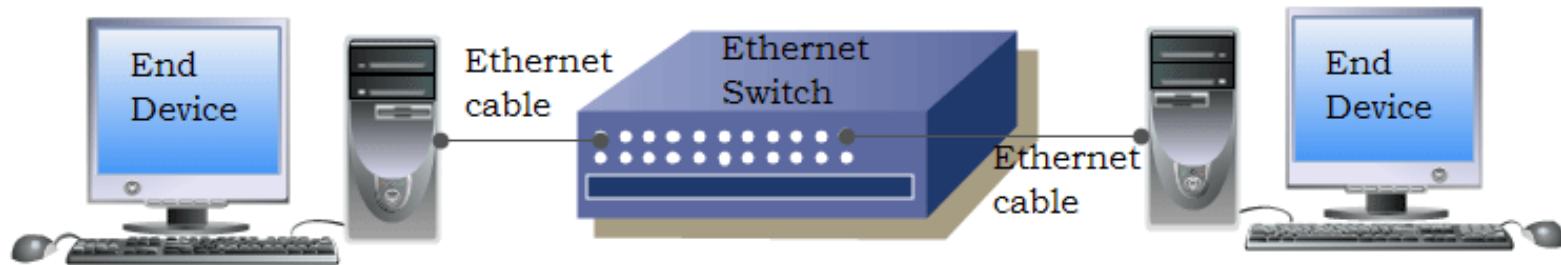
Module 6



Ethernet and Wi-Fi Technologies

Ethernet and Wi-Fi Technologies

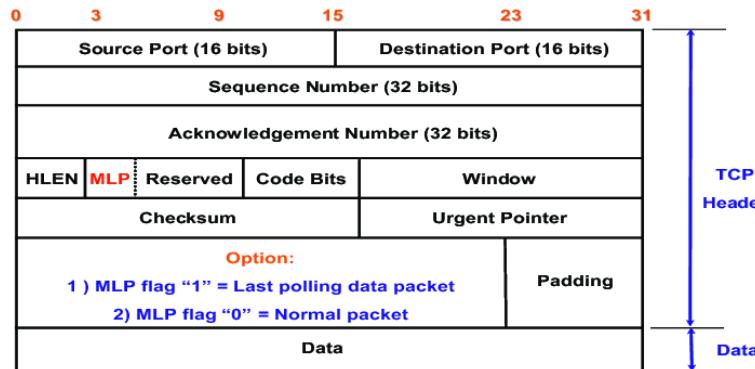
Ethernet is a widely deployed LAN technology standardized in IEEE 802.3. Its connector is the *network interface card* (NIC) equipped with 48-bit MAC address, which helps other Ethernet devices to identify and communicate with remote devices in Ethernet.



Ethernet and Wi-Fi Technologies

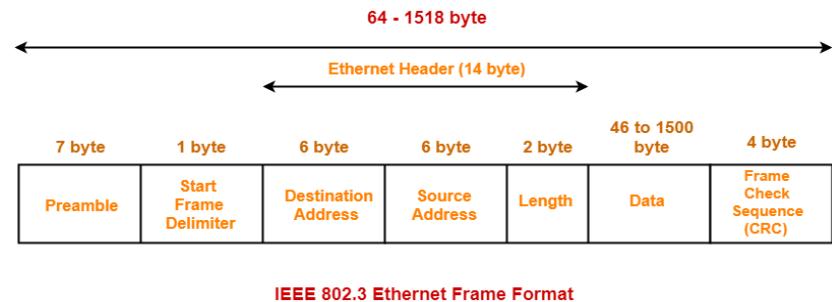
Network Packet

- formatted unit of data carried by a packet-switched network
- consists of control information and user data, which is also known as the payload



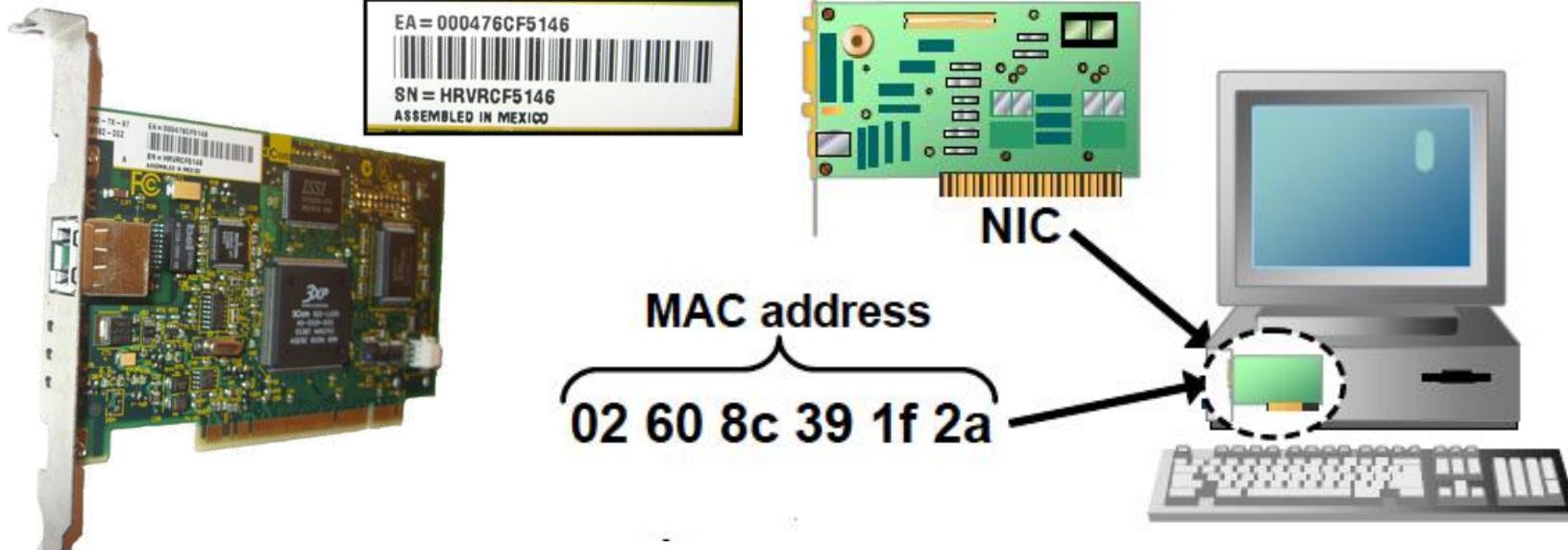
Ethernet Frame

- payload transported by a data unit on an Ethernet link
- data link layer protocol data unit that uses the underlying Ethernet physical layer transport mechanisms



Ethernet and Wi-Fi Technologies

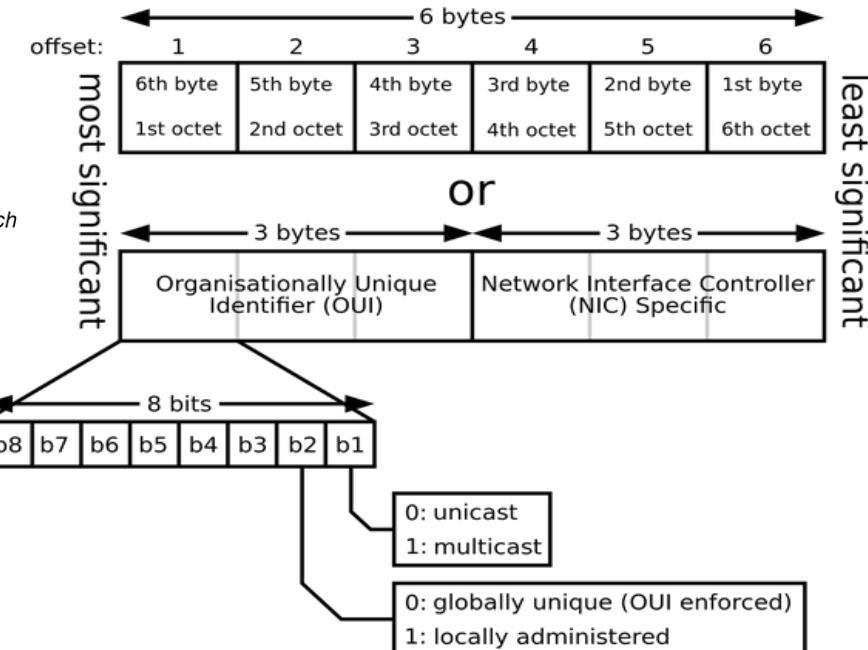
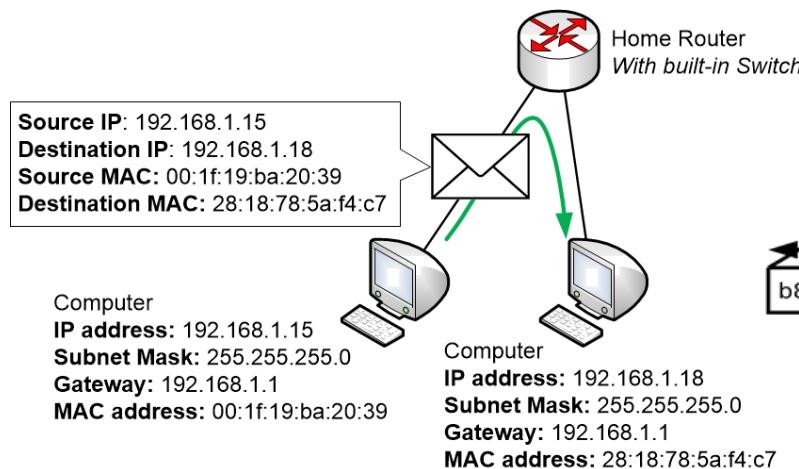
Network Interface Controller (NIC)



Ethernet and Wi-Fi Technologies

Media Access Control (MAC) Address

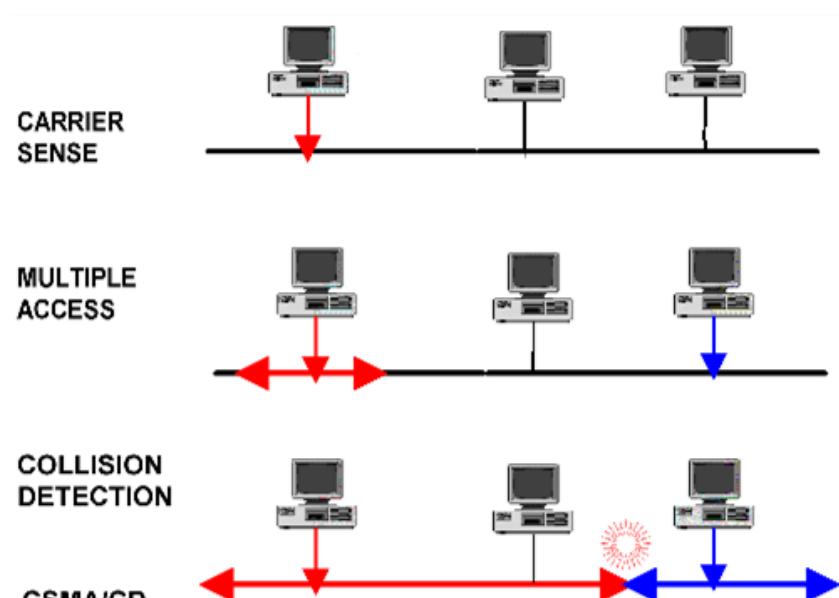
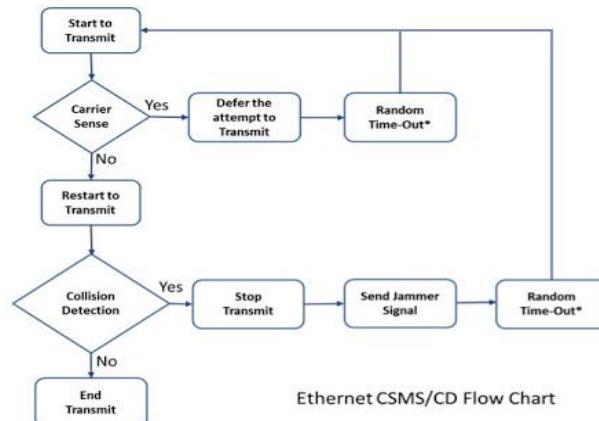
- also known as *physical address*
- unique in each NIC



Ethernet and Wi-Fi Technologies

Carrier-Sense Multiple Access w/ Collision Detection (CSMA/CD)

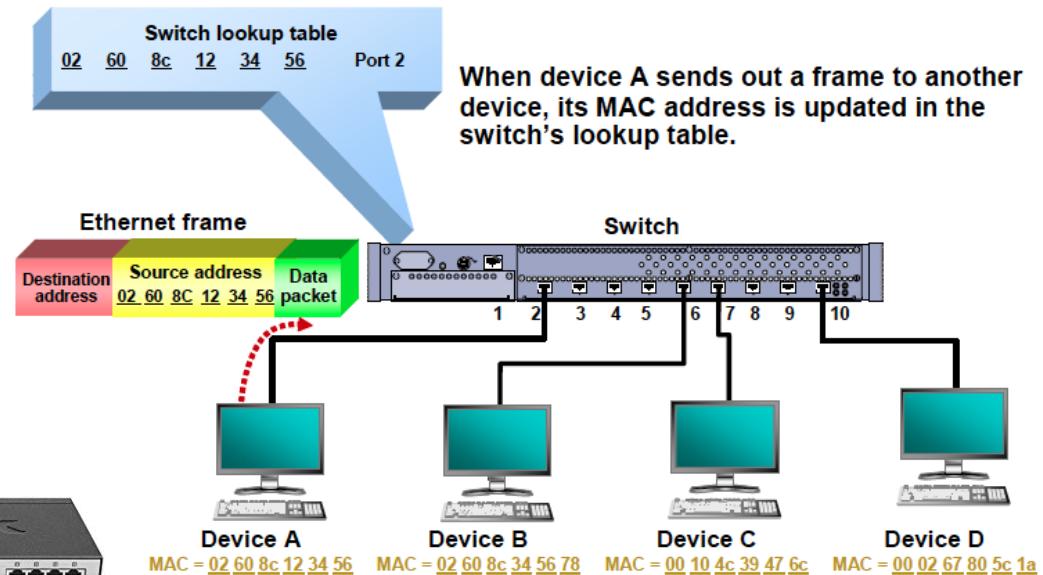
- MAC method that defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision



Ethernet and Wi-Fi Technologies

Ethernet Switch

- data link layer protocol data unit and uses the underlying Ethernet physical layer transport mechanisms
- payload transported by a data unit on an Ethernet link

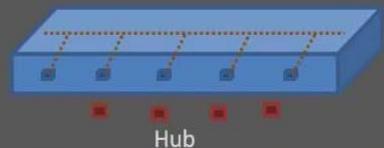


Ethernet and Wi-Fi Technologies

Hub is really a *repeater*

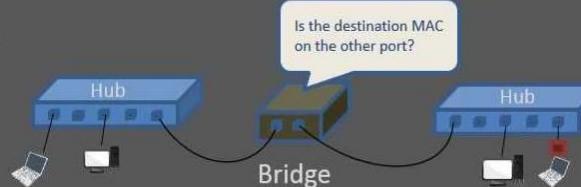
A message sent by one host is sent to all other hosts.

One of the simplest ways to create a network.



Bridge is a more intelligent form of Hub

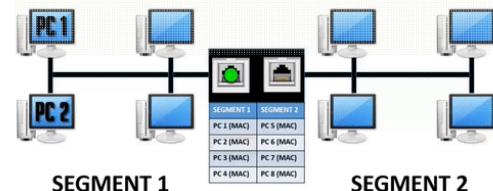
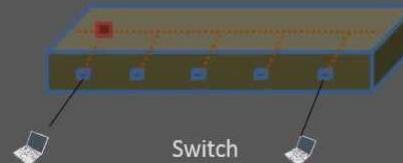
Packets are processed based on MAC address (Hardware Address) inside the incoming packet.



Switch = Bridge with more than 2 Ports

More scalable and practical

- Bridge is not very useful for end-computing devices
- Hubs cannot handle large data traffic

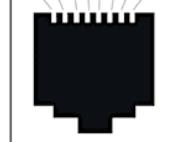


Ethernet and Wi-Fi Technologies

RJ-45 Connectors and Twisted-Pair Cables



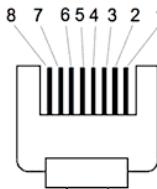
1 2 3 4 5 6 7 8



Rj-45 Jack
(Female)

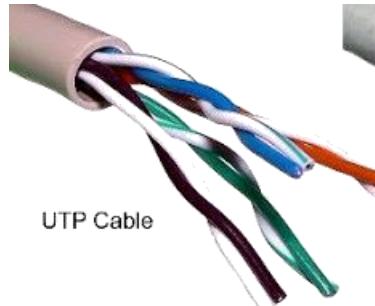


RJ45 Jack

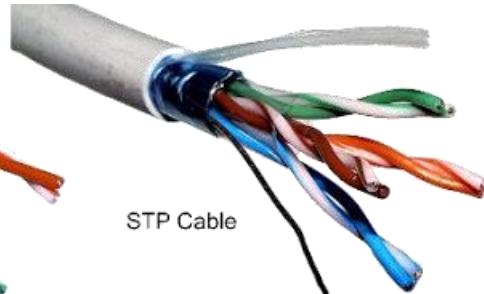


Rj-45 Plug
(Male)

Pin	Signal
1	CTS
2	DTR
3	TXD
4	SGND
5	SGND
6	RXD
7	DSR
8	RTS



UTP Cable

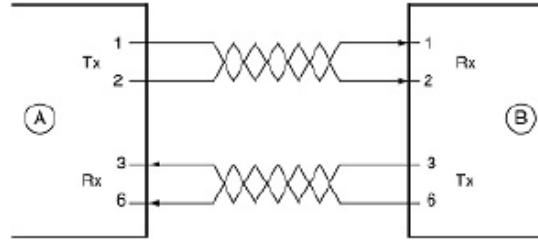


STP Cable

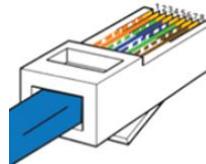
Parameters	UTP	STP
Full Form	Unshielded Twisted Pair	Shielded Twisted Pair
Structure	cable with wires that are twisted together.	Twisted pair cable enclosed in foil / shield.
Cost	Cheaper than STP	Costlier than UTP
Weight	Lighter than STP	Heavier than UTP
Noise & interference	Prone to Noise and interference	Less prone to noise and interference
Data Speed	Supports slower speed than on STP	Support higher speed than UTP
Grounding of cable	Not required	Required
Target deployments	Locations less prone to interference like offices and homes.	Locations prone to interference like factories and airports

Ethernet and Wi-Fi Technologies

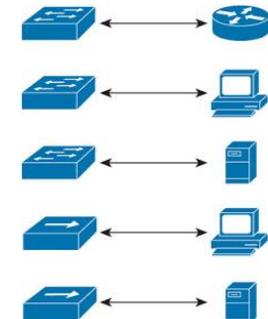
Straight-Through



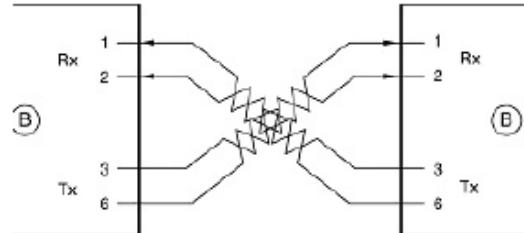
SIDE ONE



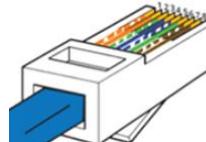
SIDE TWO



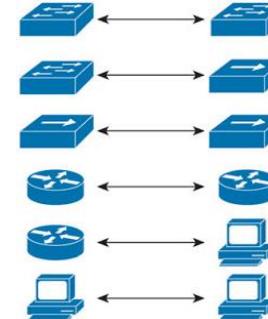
Crossover



SIDE ONE



SIDE TWO



Ethernet and Wi-Fi Technologies

UTP Cable Categories and Ethernet Standards

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Ethernet Type	Bandwidth	Cable Type	Max. Distance
10Base-T	10Mbps	Cat 3/Cat 5 UTP	100m
100Base-TX	100Mbps	Cat 5 UTP	100m
100Base-TX	200Mbps	Cat 5 UTP	100m
100Base-FX	100Mbps	Multi-mode fiber	400m
100Base-FX	200Mbps	Multi-mode fiber	2Km
1000Base-T	1Gbps	Cat 5e UTP	100m
1000Base-TX	1Gbps	Cat 6 UTP	100m
1000Base-SX	1Gbps	Multi-mode fiber	550m
1000Base-LX	1Gbps	Single-mode fiber	2Km
10GBase-T	10Gbps	Cat 6a/Cat 7 UTP	100m
10GBase-LX	10Gbps	Multi-mode fiber	100m
10GBase-LX	10Gbps	Single-mode fiber	10Km

Ethernet and Wi-Fi Technologies

Giga-Ethernet

- introduced in 1995, overtook Fast-Ethernet as it provides speed up to 1000 Mbits/seconds.
- IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables.
- IEEE802.3ah defines Giga-Ethernet over Fiber.



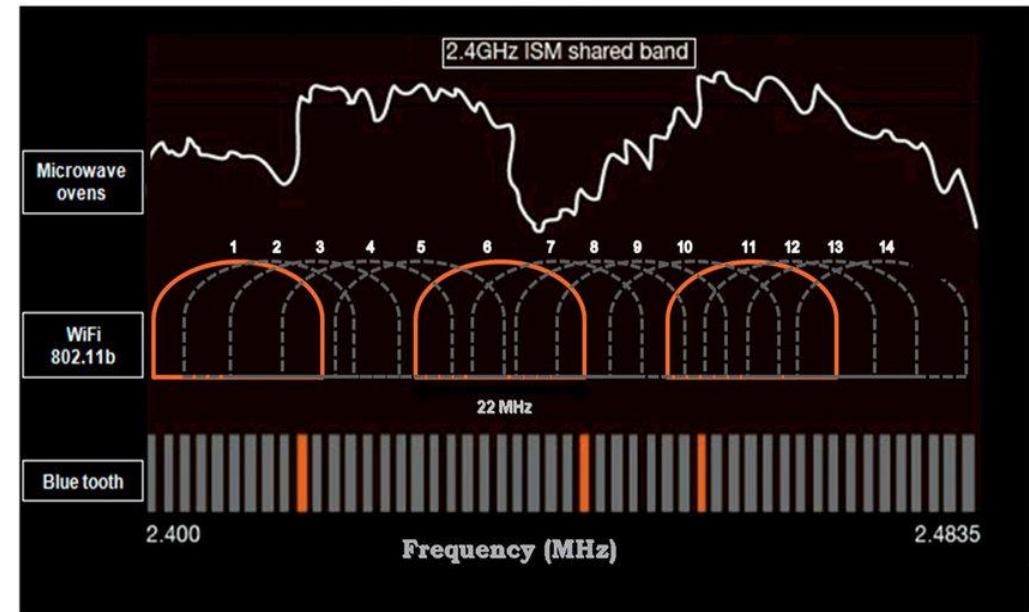
Cabling Standard	Cabling Type	Max Reach
10GBASE-SR	62.5µm OM3 multimode fiber	300m
	50µm OM4 multimode fiber	400m
10GBASE-LR	9µm single-mode fiber	10km
10GBASE-ER	9µm single-mode fiber	40km
10GBASE-ZR	9µm single-mode fiber	80km
	9µm single-mode fiber	10km
10GBASE-LX4	62.5µm multimode fiber	300m
	50µm multimode fiber	
10GBASE-LRM	9µm single-mode fiber	220m
10GBASE-T	Cat 6, Cat 6a or 7 twisted pair	30m
10G DAC/AOC	Copper RJ45	1-10m/up to 20m

Cable Type	Color
Multimode 50 µm and 62.5 µm (OM1, OM2)	Orange
Multimode 50 µm, laser optimized (OM3)	Aqua
Single-mode (OS1/OS2)	Yellow
Outside Plant (OSP) - MDPE	Black
Indoor/Outdoor (I/O)	Black

Ethernet and Wi-Fi Technologies

Wireless Fidelity (Wi-Fi)

- wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections
- based on the IEEE 802.11 family of standards and is primarily designed to provide in-building broadband coverage.



Ethernet and Wi-Fi Technologies

Technologies	Indoor/ Outdoor	Bitrate	Freq. bands	License	Bandwidth	Modulation	MIMO
IEEE 802.11	20m /100m	2 Mbps	2.4GHz	Unlicensed	20 MHz	FHSS and DSSS	—
IEEE 802.11b	35m/ 140m	11 Mbps	2.4GHz	Unlicensed	20 MHz	HR-DSSS	—
IEEE 802.11a	35m/ 119m	54 Mbps	5GHz	Unlicensed	20 MHz	OFDM	—
IEEE 802.11g	45m/ 90m	54 Mbps	2.4 GHz	Unlicensed	22 MHz	OFDM/ DSSS/ CCK	—
IEEE 802.11n	70m/ 250m	600 Mbps	2.4 GHz/ 5 GHz	Unlicensed	20 MHz/ 40 MHz	OFDM	4 X 4
IEEE 802.11ac wave	70m/ 250m	7000 Mbps	5 GHz	Unlicensed	80 MHz	64-QAM	MU-MIMO
IEEE 802.11ad	10m/ n/a	7000 Mbps	60 GHz	Unlicensed	2.16 GHz	Single Carrier/ OFDM	10 X 10
IEEE 802.11ac wave 2	70m/ 250m	7000 Mbps	5 GHz	Unlicensed	80 MHz/ 160 MHz	256-QAM	MU_MIMO 8 X 8

Wi-Fi Specifications

Ethernet and Wi-Fi Technologies

IEEE 802.3 vs 802.11 Frame Format

Ethernet (802.3) Frame Format							
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	Destination MAC Address	Source MAC Address	Type	Data (payload)	CRC	Inter-frame gap



For TCP/IP communications,
the payload for a frame is a
packet

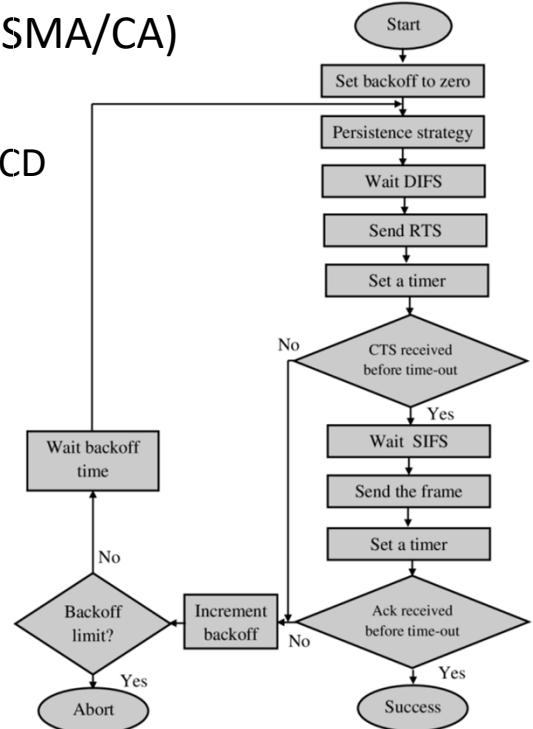
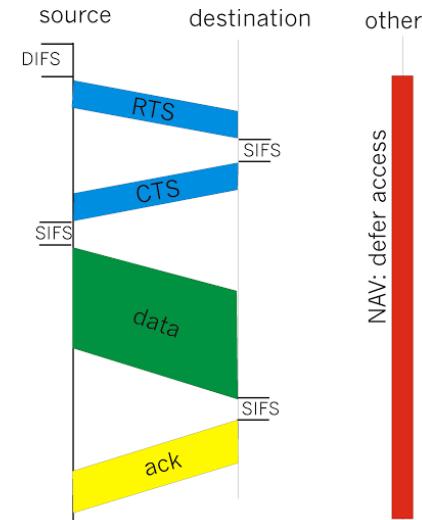
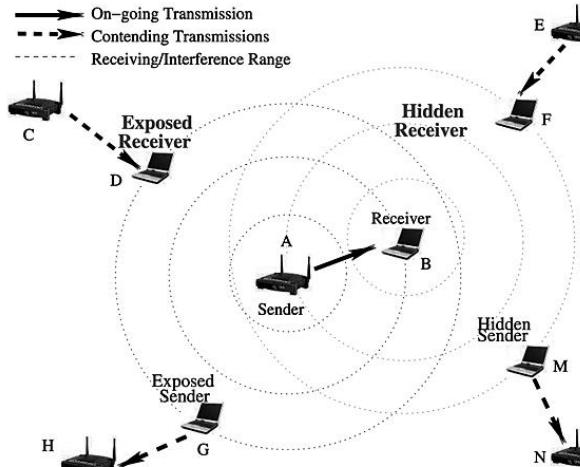
Wireless Encryption Protocol	Description	Encryption Level (Key Size)
WEP	Wired Equivalent Privacy	64-bit
WPA2	Wi-Fi Protected Access	256-bit
TKIP	Temporal Key Integrity Protocol	128-bit
AES	Advanced Encryption Standard	128-, 192-, and 256-bit

WiFi (802.11) Frame Format								
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

Ethernet and Wi-Fi Technologies

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

- protocol for carrier transmission in 802.11 (wireless) networks
- acts to prevent collisions before they happen, unlike in CSMA/CD



Ethernet and Wi-Fi Technologies

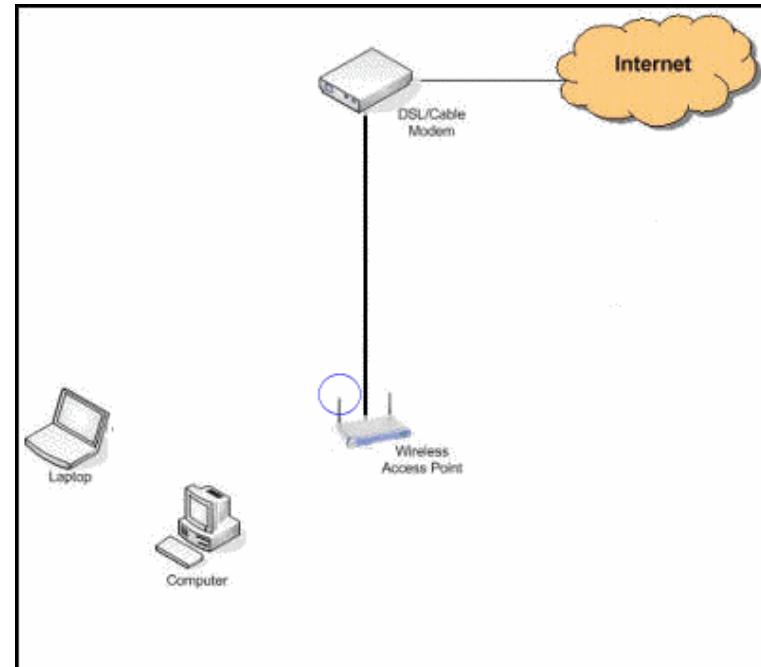
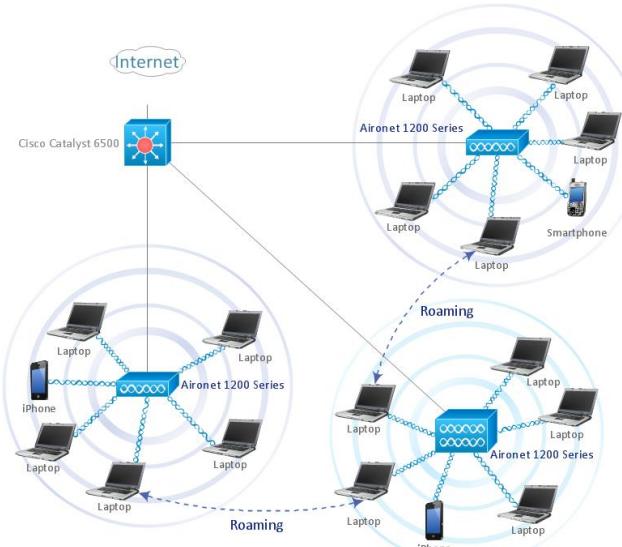


Wi-Fi Adapters and Modules

Ethernet and Wi-Fi Technologies

Wireless Access Point (WAP)

- network device that acts as a portal for devices to connect to a local area network



Ethernet and Wi-Fi Technologies



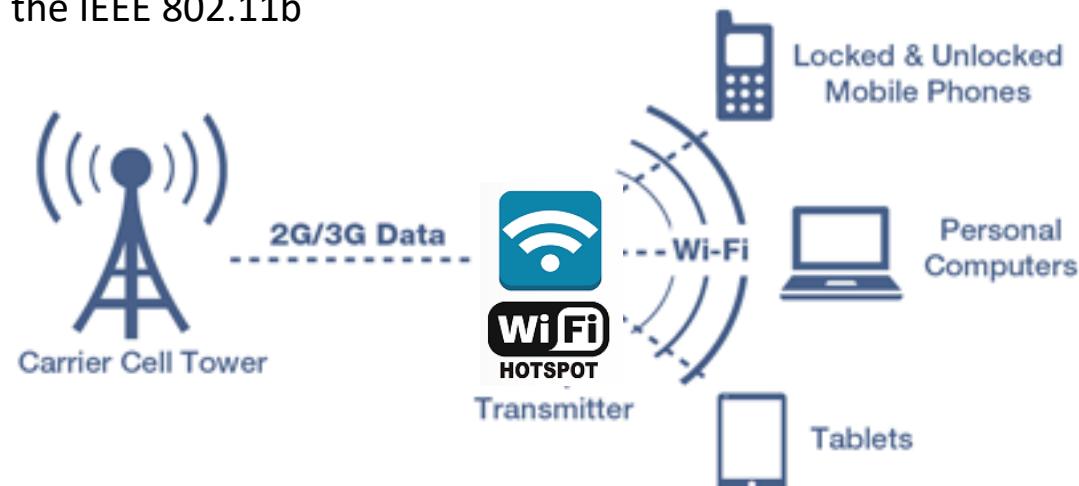
Different WAP Models

Ethernet and Wi-Fi Technologies

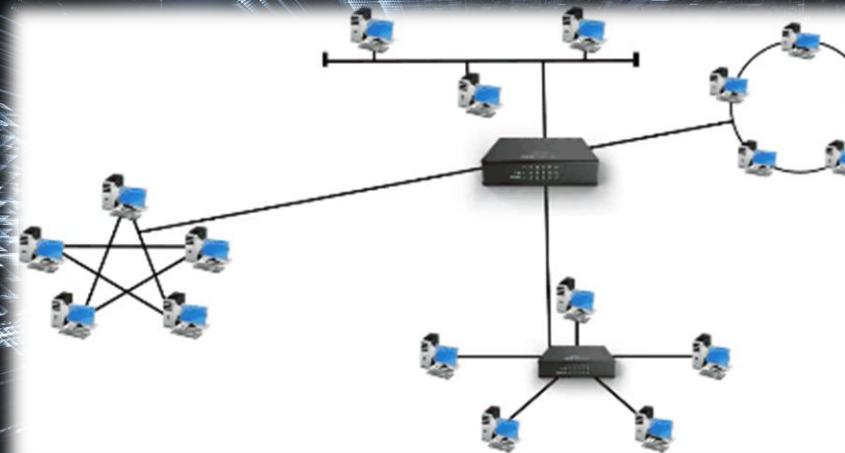
Wi-Fi Hotspots

- created by installing an access point to an internet connection
- transmits a wireless signal over a short distance typically around 300 feet
- most common specification is the IEEE 802.11b

The largest public WiFi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.



Module 7

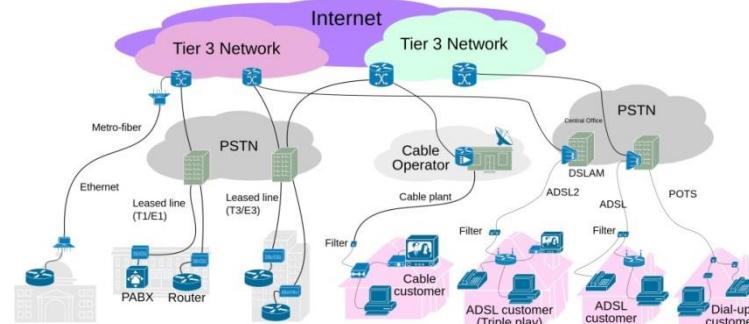


Computer Networks and the Internet

Computer Networks and the Internet

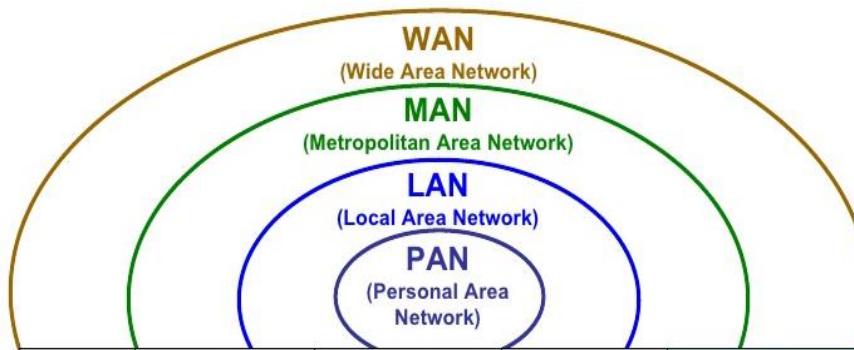
Computer Network (or *data network*) is a system that transfers data between network access points (nodes) through data switching, system control, and interconnection transmission lines.

The largest and most popular example is the *Internet*.



Computer Networks and the Internet

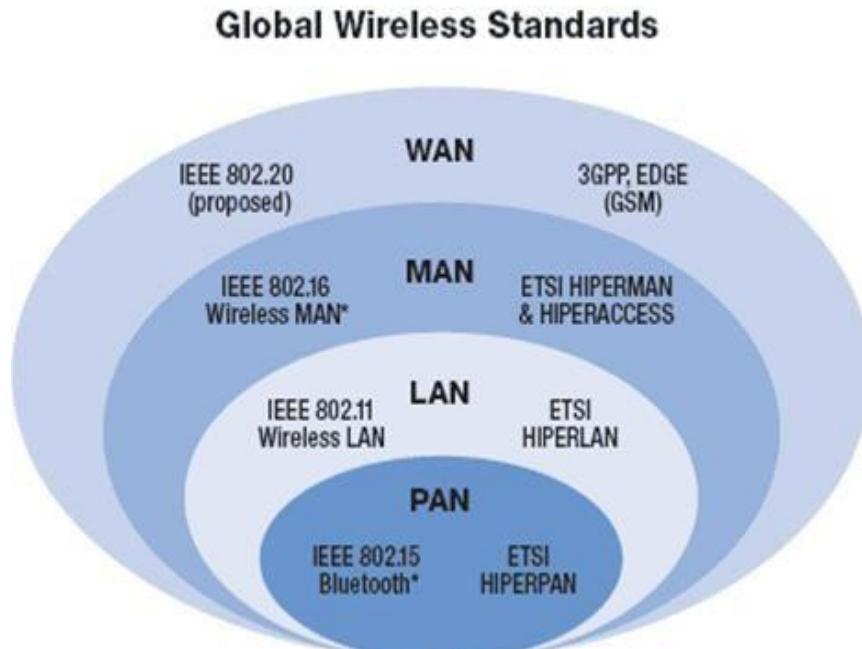
Types of Computer Networks



	PAN	LAN	MAN	WAN
Standards	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, cellular access



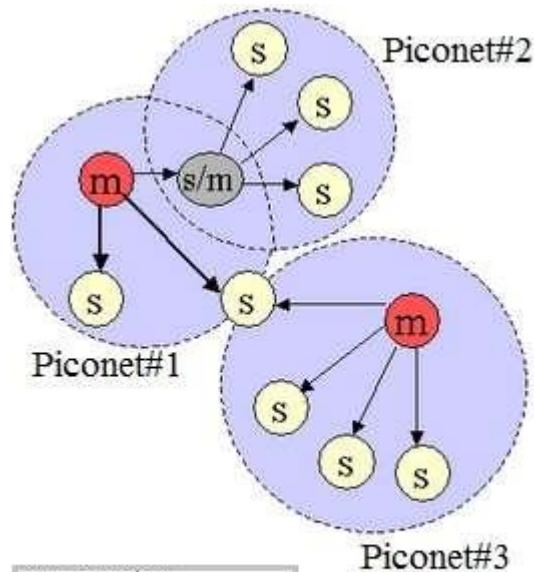
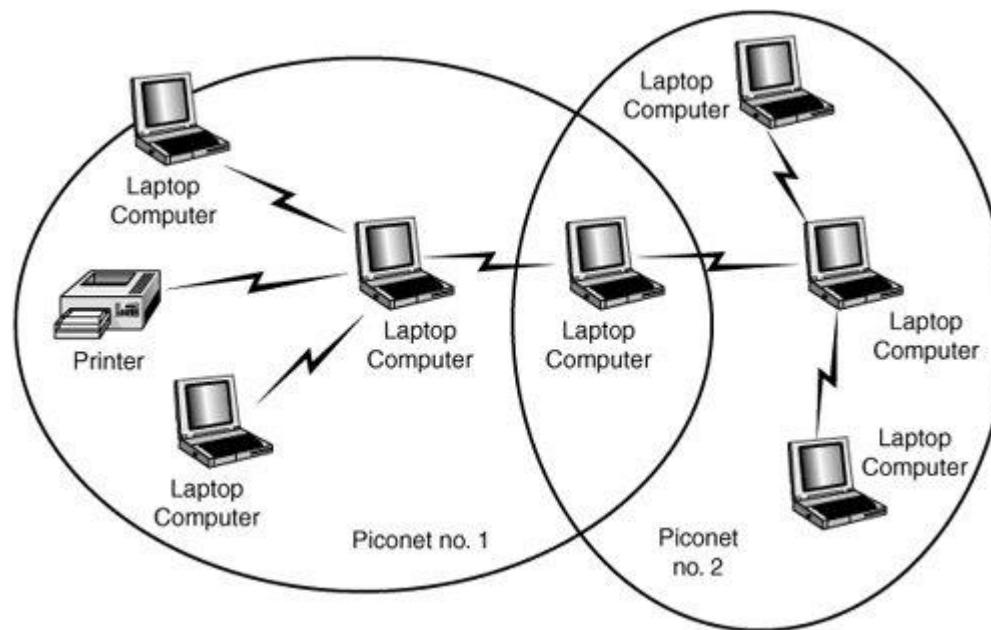
Computer Networks and the Internet



LAN	WAN	MAN
Short for local area network.	Short for wide area network.	Short for metropolitan area network.
Connects a group of computers within a limited geographic area.	Covers a large geographical area such as a state, country or a continent.	Confined to a city or town. Distance coverage is larger than LAN and smaller than WAN.
High bandwidth for data transfer.	Low bandwidth for data transfer.	Bandwidth is moderate for data transfer.
Owned by private companies or individuals.	Established under distributed ownership.	Ownership can be private or public.
Limited to 100 to 1000 meters.	Spans a huge area of 100,000 kilometers.	Distance coverage is up to 100 kilometers.
Lower setup cost due to inexpensive devices.	Higher setup cost than LAN and MAN.	Moderate installation costs.
Higher data transfer speeds with 10, 100, and 1000 Mbps high-speed Ethernet.	Low data transfer rates between 10 to 20 Mbps.	Speed can go up to 100 Mbps.

Computer Networks and the Internet

Piconet and Scatternet

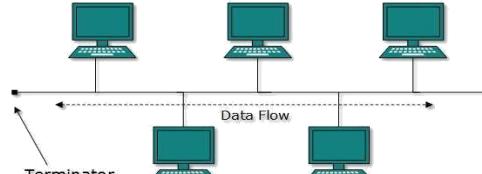


m-master
s-slave
s/m-slave/master

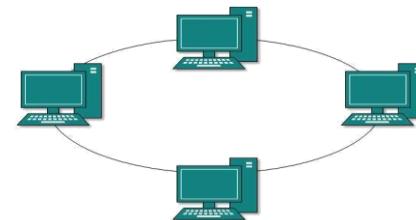
Scatternet

Computer Networks and the Internet

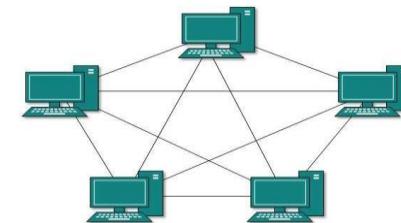
Computer Network Topologies



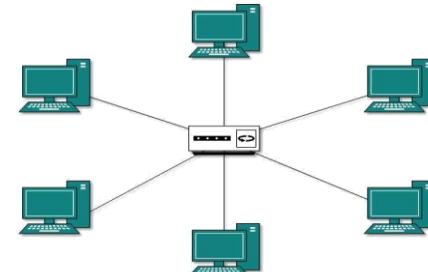
Bus Topology



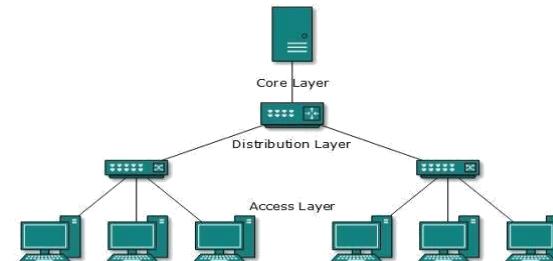
Ring Topology



Mesh Topology



Star Topology



Tree Topology

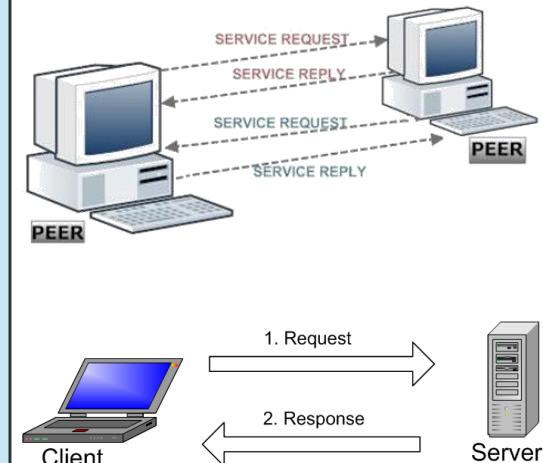
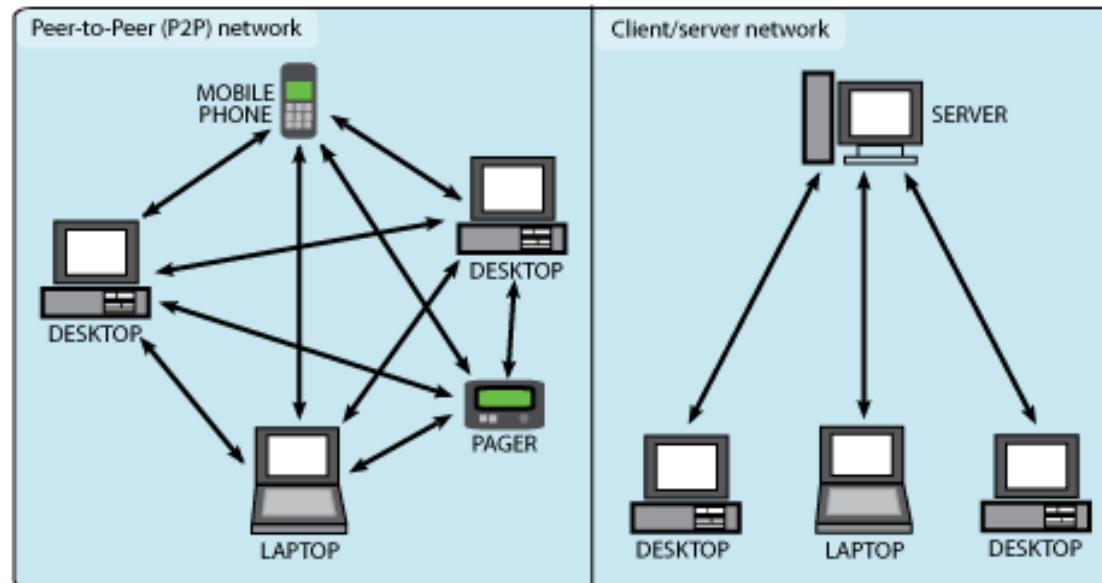
Computer Networks and the Internet

Topology	Advantages	Disadvantages
Mesh	Simplest and most fault tolerant.	Extremely difficult to reconfigure, extremely expensive, and very complex
Star/Tree	Cheap and easy to install, easy to reconfigure, and fault Tolerant	More expensive than bus
Ring	Efficient and easy to install.	Difficult to reconfigure and very expensive
Bus	Cheap and easy to install	Difficult to reconfigure, and break in bus disables entire network

Usage Factors	Very High	High	Moderate	Low	Very Low
Cost	Mesh Topology	Tree Topology	Star Topology	Ring Topology	Bus Topology
Security	Mesh Topology	Tree Topology	Star Topology	Ring Topology	Bus Topology
Privacy	Mesh Topology	Tree Topology	Star Topology	Bus Topology	Ring Topology
Use of cables	Mesh Topology	Tree Topology	Star Topology	Bus Topology	Ring Topology

Computer Networks and the Internet

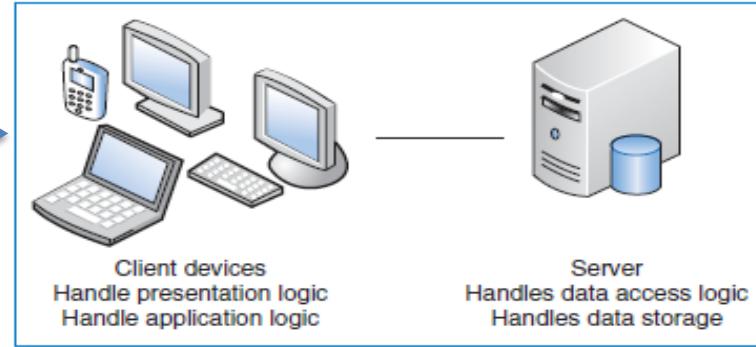
Types of Computer Network Architecture



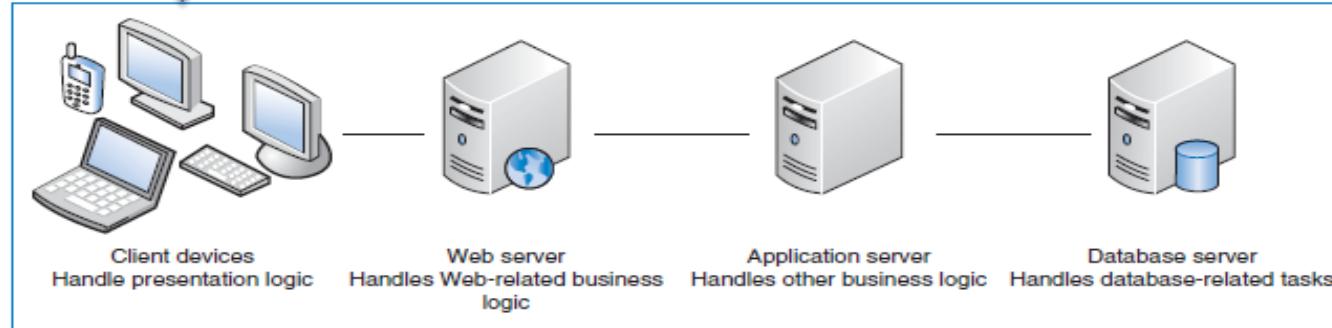
Computer Networks and the Internet

N-Tier Client-Server Architecture

1-Tier Architecture



3-Tier Architecture



Computer Networks and the Internet

Types of Servers

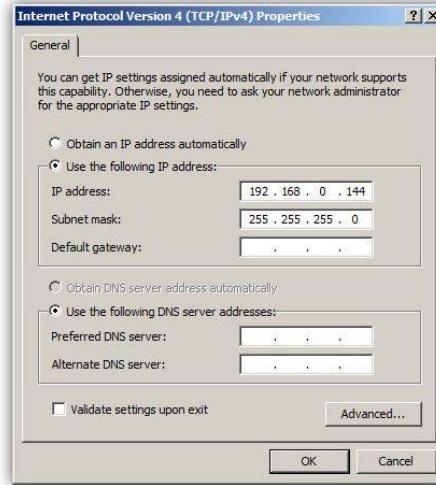
	<u>Purpose</u>	<u>Examples</u>		<u>Purpose</u>	<u>Examples</u>
Mail Server	E-mail Services	<ul style="list-style-type: none">• Microsoft Exchange Server• IBM Lotus Domino		Proxy Server	Filtering And Caching <ul style="list-style-type: none">• Microsoft Forefront Threat Management Gateway (ISA Server)• Apache HTTP Server• Apache Traffic Server
Application Server	An Environment To Run Certain Applications	<ul style="list-style-type: none">• Oracle WebLogic Server• Oracle Application Server• Oracle GlassFish Server• Zend Server		Print Server	Printer Services <ul style="list-style-type: none">• Microsoft Windows Storage Server (Built on the Microsoft Windows Server)
DNS Server	Translation of Domain Names Into IP Addresses	<ul style="list-style-type: none">• Microsoft Windows Server• BIND		<p>OTHER TYPES OF SERVERS:</p> <p>FTP Server, Chat Server, Fax Server, Game Server, Audio/Video Server</p>	

Computer Networks and the Internet

Dynamic Host Configuration Protocol (DHCP) Server

- network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices

IP Address is an identifier for devices on a TCP/IP network. It can be automatically assigned by the ISP (*dynamic IP address*) or manually assigned (*static IP address*). It has two versions: *IPv4* and *IPv6*



DNS SERVER

A device that locates the internet domain names and translates them into internet protocol (IP) addresses

DHCP SERVER

A device that dynamically assigns IP address and other network configuration parameters to each device on a network so that they can communicate with each other

Stands for Domain Name System Server

Maps the domain names to the corresponding IP addresses

Uses port number 53

Works in a decentralized manner

Helps to map the domain names to IP addresses; user does not need to memorize the IP addresses

Stands for Dynamic Host Configuration Protocol

Assigns IP addresses automatically to the devices when they connect to the network

Works on port number 67 and 68

Works in a centralized manner

Helps to assign IP addresses to the devices automatically, making it easier to manage a large network

Visit www.PEDIAA.com

Computer Networks and the Internet

Server Form Factors and Roles

Tower:

A tower server is a free-standing unit, similar to a large desktop pc in both size and shape.



Rack:

A rack server is specially designed to fit within a standardized 19" mounting rack.



Blade:

A blade servers are for use in blade enclosure that designed to fit within a standardized 19" mounting rack.



Server Manager > Dashboard

Select server roles

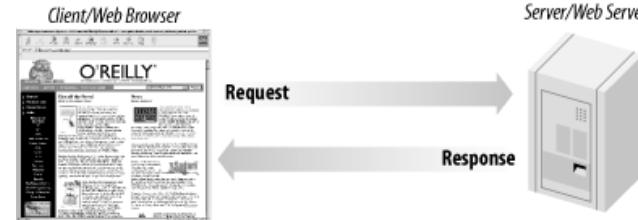
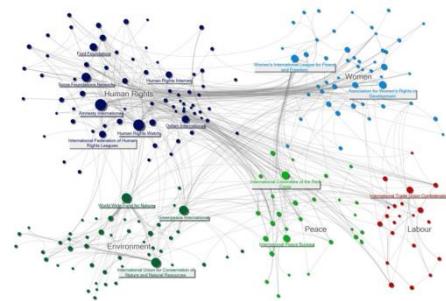
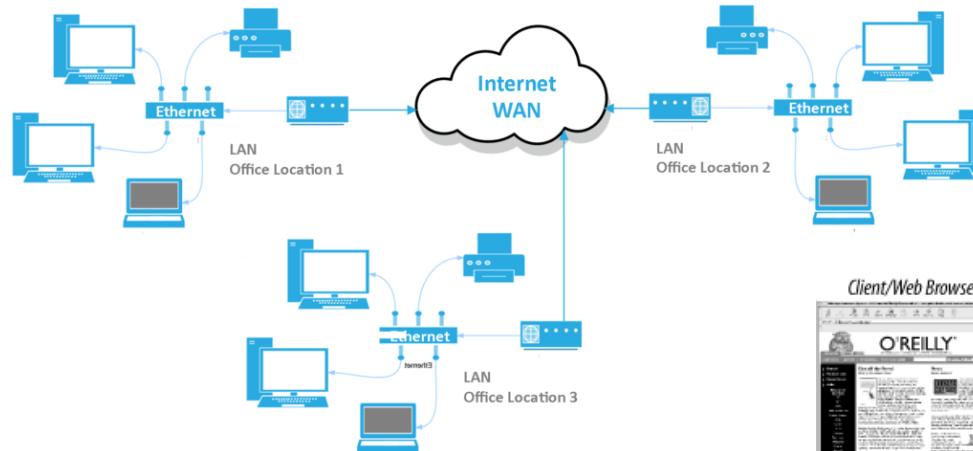
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

- Select one or more roles to install on the selected server.
- Roles**
- File and Storage Services (4 of 11 installed)
 - File Server (Installed)
 - BranchCache for Network Files (Installed)
 - DFS Namespaces (Installed)
 - DFS Replication
 - File Server Resource Manager
 - File Server VSS Agent Service
 - iSCSI Target Server
 - iSCSI Target Storage Provider (VDS and V)
 - Server for NFS**
 - Storage Services (Installed)
 - Work Folders
 - Hyper-V
 - Network Policy and Access Services



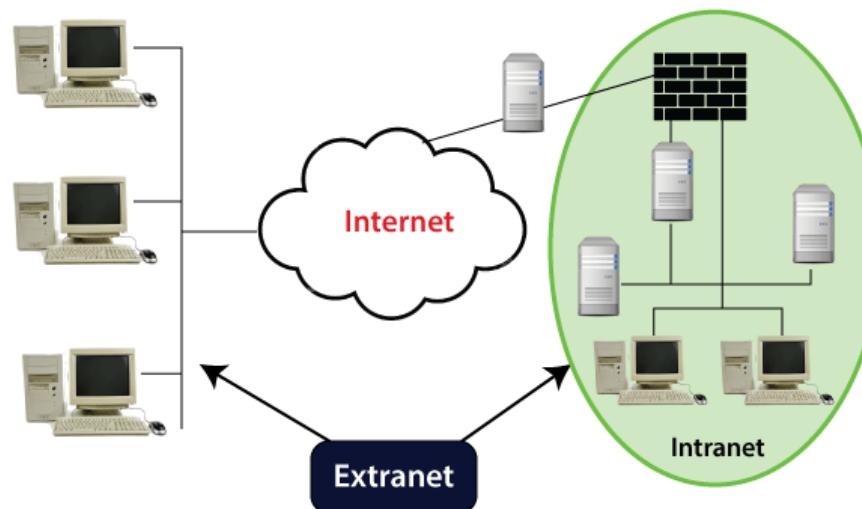
Computer Networks and the Internet

The **Internet** is the global system of interconnected computer networks that use the TCP/IP suite to link devices worldwide, while the **World Wide Web** (or web) is one of the services communicated over the Internet.



Computer Networks and the Internet

Intranet, Extranet, and Internet

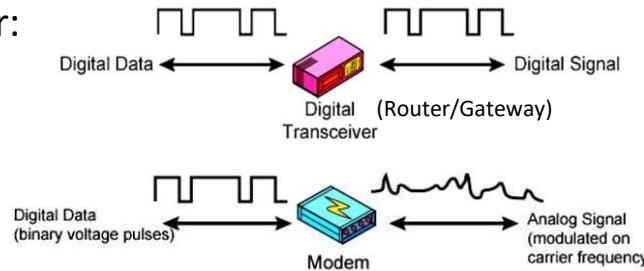


Parameter	Internet	Intranet	Extranet
Type of Network	Public	Private	Private/VPN
Size	Large number of connected devices	Limited number of connected devices	Limited number of connected devices over internet
Security	Depends on the device connected to the device	Firewall protected	Firewall separates Internet and Extranet
Policy	Internet Communication Protocols	Organizational Policies	Organizational policies, contractual policies and Internet Policies
Accessibility	Anyone	Authorized people	Authorized people
Information Sharing	Information can be shared across the world	Information can be shared securely within an Organization	Information can be shared between employees and external people
Owner	Not owned by anyone	Owned by a particular Organization	Owned by one or more Organizations
Example	World Wide Web, Email, Chat, Social Media	Internal Operations Network of an Organisation	Network of Collaboration between two Corporations

Computer Networks and the Internet

Modem and Gateway

Remember:



Router

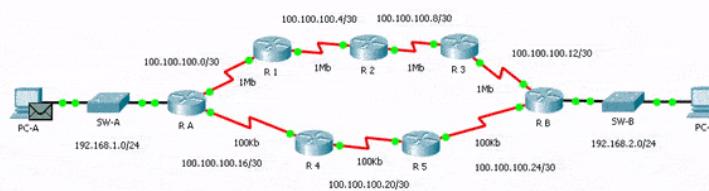
- forwards data packets connects both similar and dissimilar LANs with the same network protocols
- can provide modem, gateway, firewall, NAT, DNS, DHCP, and proxy server functions

Gateway	Modem
A gateway is a network device that acts as an entry point to another network.	A modem is a hardware component that allows any networking device to connect to the Internet.
It is a device that combines the functionality of both a modem and a router on the same box.	It is mainly used as a border device that enables a computer to transmit data over cable lines.
A gateway serves as a link between computers using different protocols, platforms or operating systems.	It converts or modulates an analog signal from a cable or telephone line to digital data that a computer can easily recognize and understand.
It can be a router, a firewall, server, or any other networking device that enables traffic flow in and out of the network.	Examples of modem include a cable modem or a DSL modem.

Computer Networks and the Internet

Routing

- selecting a path for traffic in a network or between or across multiple networks



STATIC ROUTING

A form of routing that occurs when a router uses a manually-configured routing entry rather than information from a dynamic routing traffic

Static Routing is also called
non adaptive routing

The network administrator manually adds the routes in the routing table

Requires less bandwidth

Configuration is difficult

More secure

DYNAMIC ROUTING

A process where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a network

Dynamic Routing is also called adaptive routing

The routes are found automatically according to the changes in the network

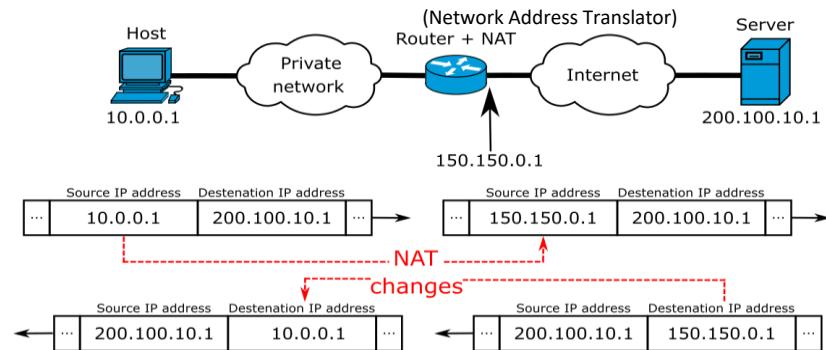
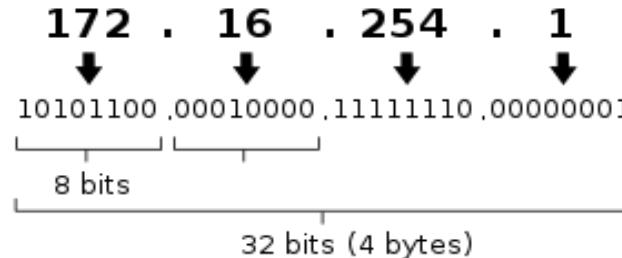
Requires more bandwidth

Configuration is easy

Less secure

Computer Networks and the Internet

IPv4 Address and Classful Addressing



CLASS	1 ST OCTET	BINARY RANGE	PUBLIC ADDRESS RANGE	PRIVATE ADDRESS RANGE	APPLICATION
A	0 – 127	00000000 – 01111111	0.0.0.0 – 126.255.255.255	10.0.0.0 – 10.255.255.255	Government Networks
B	128 – 191	10000000 – 10111111	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.31.255.255	Medium Companies
C	192 – 223	11000000 – 11011111	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255	Small Companies
D	224 – 239	11100000 – 11101111	224.0.0.0 – 239.255.255.255	N/A	For Testing
E	240 – 255	11110000 – 11111111	240.0.0.0 – 254.255.255.255	N/A	For Testing and Future Use

Computer Networks and the Internet

Types of IP Address

- **Network Address** – uniquely identifies a network; the first address of a class
- **Host Address** – uniquely identifies a host or node (computer or any IP-based device); somewhere between the network address and broadcast address of a class
- **Broadcast Address** – enables transmission to every node in a local network
- **Loopback Address** – special IP address (127.X.X.X) reserved for use in testing network cards

CLASS	NO. OF NETWORKS	NO. OF HOSTS	HOST ASSIGNMENT RANGE	N-H Representation	SUBNET MASK
A	$2^7 = 128$	$2^{24} - 2 = 16,777,214$	1.0.0.1 – 126.255.255.254	N – H – H – H	255.0.0.0
B	$2^{14} = 16,384$	$2^{16} - 2 = 65,534$	128.0.0.1 – 191.255.255.254	N – N – H – H	255.255.0.0
C	$2^{21} - 1 = 2,097,151$	$2^8 - 2 = 254$	192.0.0.1 – 223.255.255.254	N – N – N – H	255.255.255.0

Computer Networks and the Internet

Subnetting

- allows to create multiple *subnetworks* (*subnets*) or logical networks or that exist within a single Class A, B, or C network
- uses a *subnet mask* to determine what subnet an IP address belongs to

Classless Inter-Domain Routing (CIDR)

- set of IP standards used to create unique identifiers for networks and individual devices

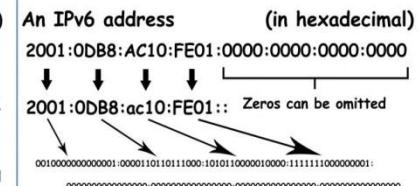
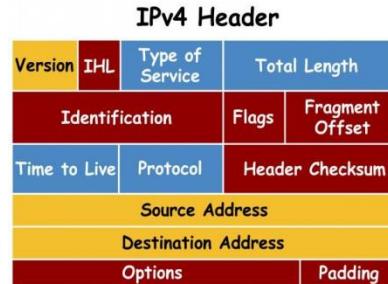
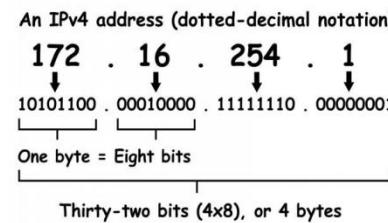
Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Address block	Present use
0.0.0.0/8	"This" network
14.0.0.0/8	Public-data networks
24.0.0.0/8	Cable television networks
39.0.0.0/8	Reserved but subject to allocation
128.0.0.0/16	Reserved but subject to allocation
169.254.0.0/16	Link local
191.255.0.0/16	Reserved but subject to allocation
192.0.0.0/24	Reserved but subject to allocation
192.0.2.0/24	Test-Net 192.88.99.0/24 6to4 relay anycast
198.18.0.0/15	Network interconnect device benchmark testing
223.255.255.0/24	Reserved but subject to allocation
224.0.0.0/4	Multicast
240.0.0.0/4	Reserved for future use

Computer Networks and the Internet

IPv4 vs IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0./24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,$ $920,938,463,463,374,$ $607,431,768,211,456$



Module 8

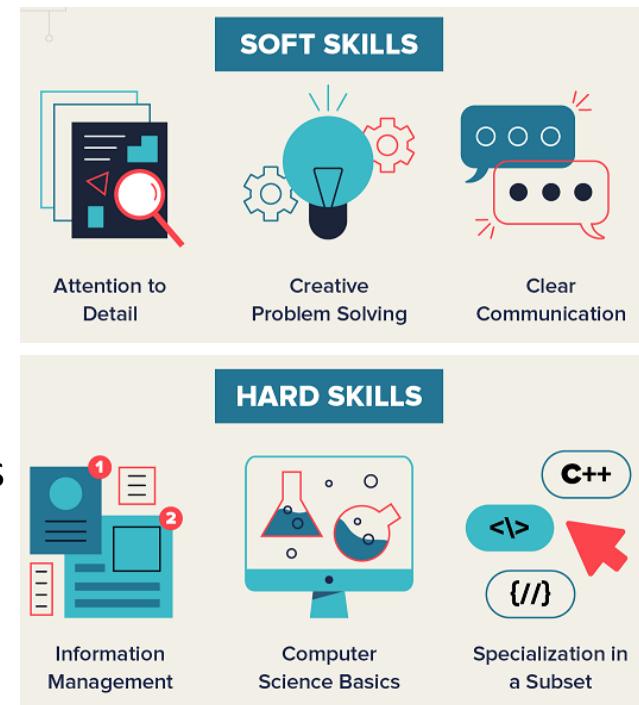


Cybersecurity and Industry 4.0

Cybersecurity and Industry 4.0

Cybersecurity

- measures for protecting computer systems, networks, and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction
- basically involves assessing, managing, and mitigating the risk, which are all continuous activities as long as the protected system exists
- basic objectives are to ensure the data confidentiality, integrity, and availability



Cybersecurity and Industry 4.0

Assessing Cybersecurity Risks



Point of Sale (POS) intrusions

Where retail transactions are conducted, specifically where card – present purchases are made.



Cyber Extortion

Crime involving an attack or threat of attack against your IT infrastructure , couple with demand for money to stop the attack.



Miscellaneous Errors

People make mistakes! Unintentional actions directly compromised a security attribute of an information asset.



Cyber Espionage

Unauthorised network or system access linked to state affiliated actors and / or exhibiting the motive of espionage.



Denial of Service

Intended to compromise the availability of networks and systems. Includes both network and application layer attacks.



Physical Theft and Loss

Any incident where an information asset went missing, whether through misplacement or malice.



Insider and Privilege Misuse

Any unapproved or malicious use of organisations resources. Mainly insider misuse or external (through collusion)



Web App Attacks

This includes exploits of a code – level vulnerabilities in the application as well as thwarting authentication mechanisms.



Payment Card Skimmers

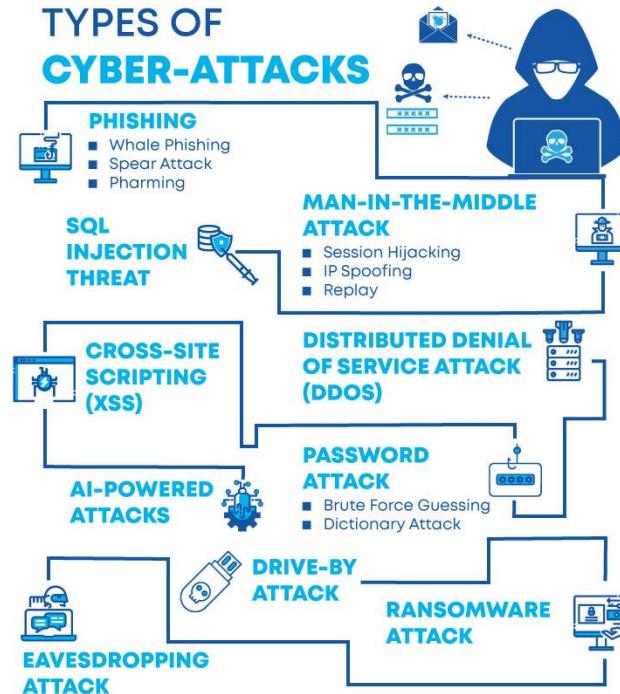
Where a skimming device is physically implanted on an asset that reads magnetic stripe data from a payment card



Crimeware

A form of malware. Primary goal is to gain control of systems to steal credentials

TYPES OF CYBER-ATTACKS



Cybersecurity and Industry 4.0

Managing Cybersecurity Risks



Risk Management Matrix

Cybersecurity and Industry 4.0

Mitigating Cybersecurity Risks

Each stage is designed to protect an organization from new workforce threats and build a cyber-resilient infrastructure for the future.



STEP 1 : Secure remote workforce

Enforce remote workforce security strategies and associated policies and processes. Assess and update perimeter security controls or leverage SaaS solutions.



STEP 2 : Protect digital identities and data

Continuously monitor digital identities and data, and establish alerts for potential threats. Review/update existing processes to strengthen your resilience.



STEP 3 : Cyber Threat Intelligence (CTI)

Extend your threat intelligence to cover your critical infrastructure and new attack vectors. Reduce external attack surface visibility with a remediation plan.

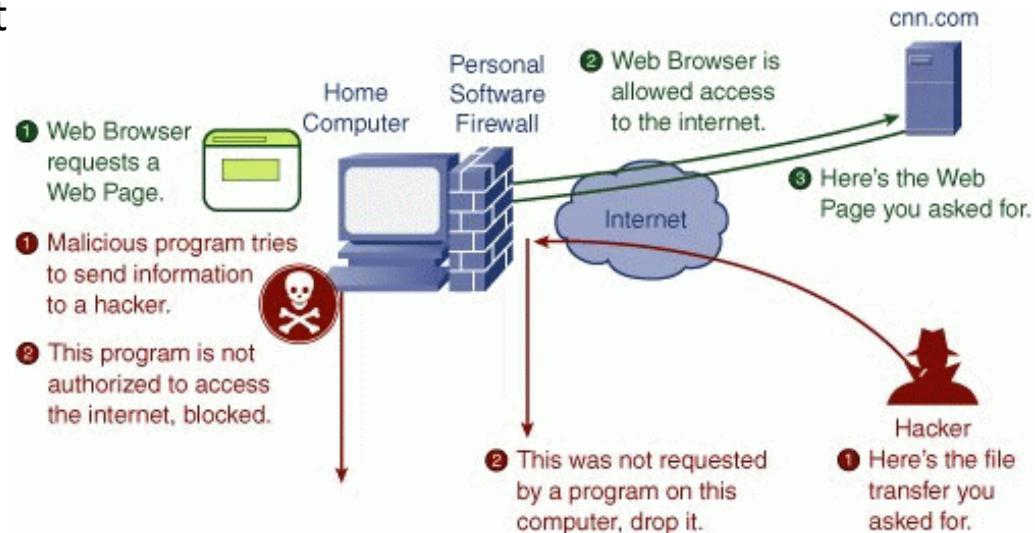
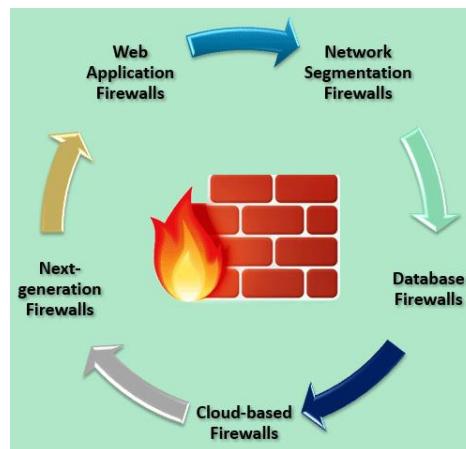


STEP 4 : Cyber Resiliency

Develop the repeatable ability to minimize the effect of cyberattacks on company operations, and create a culture of agility and responsiveness.

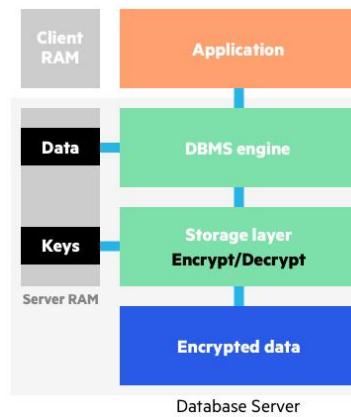
Cybersecurity and Industry 4.0

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet

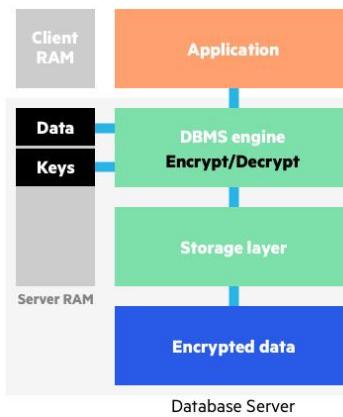


Cybersecurity and Industry 4.0

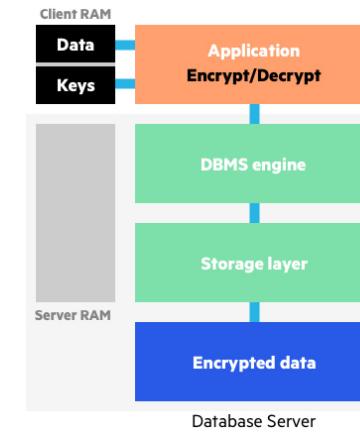
Encryption is a process that encodes a message or file so that it can be only be read by certain people. It uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. **Decryption** is the process of converting the encoded or encrypted text back into its original form.



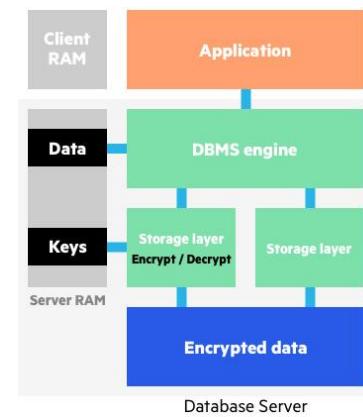
Storage-Level Encryption



Database-Level Encryption



Application-Level Encryption



File System-Level Encryption

Cybersecurity and Industry 4.0

Ethical Hacking

- act of intruding/penetrating into system or networks to find out threats, vulnerabilities in systems which a malicious attacker may find and exploit causing data loss, financial loss or other major damages
- done to improve the security of the network or systems by fixing the identified vulnerabilities

Types of Hackers

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes
.....
Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong
.....
Exploit security flaws for personal or political gain—or for fun



Cybersecurity and Industry 4.0



Cybersecurity and Industry 4.0

CpE-Related Laws and Standards



R.A. 10844

Department of Information and
Communications Technology Act of 2015



R.A. 10173

Data Privacy Act of 2012



R.A. 10175

Cybercrime Prevention Act of 2012



R.A. 8792

Electronic Commerce Act of 2000



R.A. 8293

Intellectual Property Code of the
Philippines

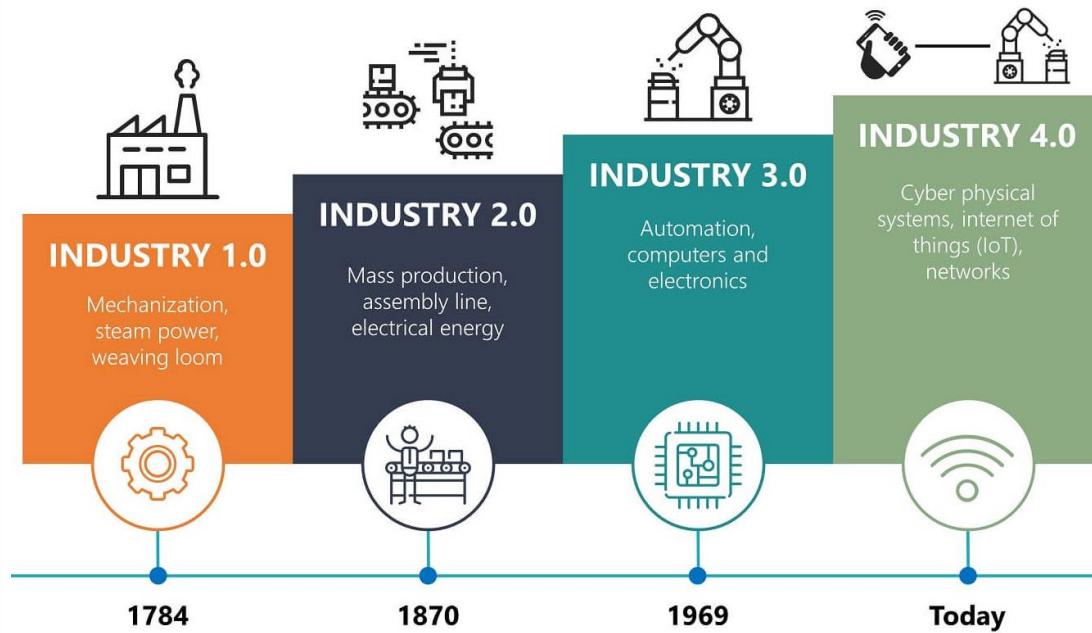


R.A. 8747

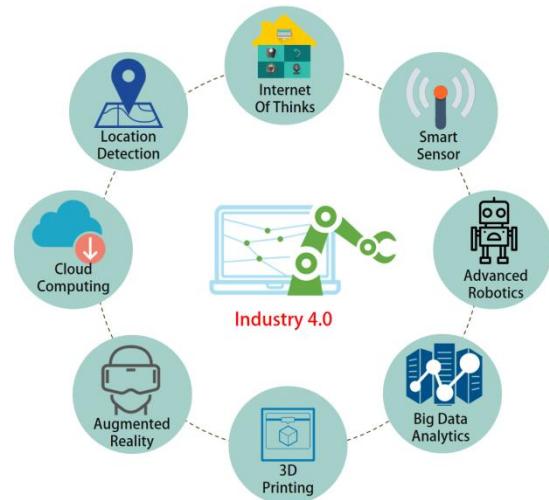
Philippine Year 2000 Disclosure and
Readiness Act



Cybersecurity and Industry 4.0



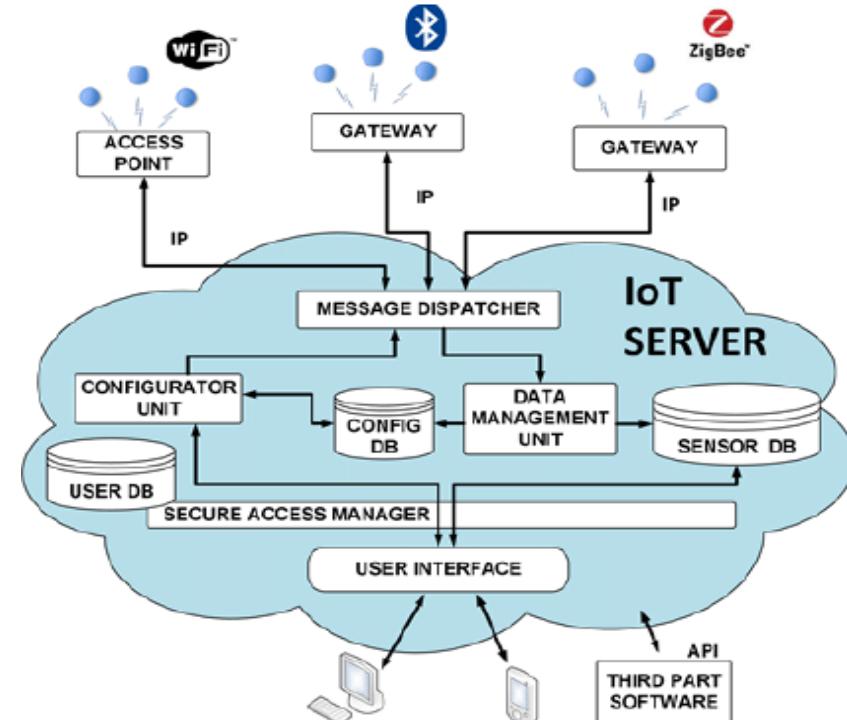
INDUSTRY 4.0 FRAMEWORK – THE DIGITAL TECHNOLOGIES



Cybersecurity and Industry 4.0

Internet of Things (IoT)

- system of interrelated computing devices and machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction
- creates opportunities for more direct, integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions



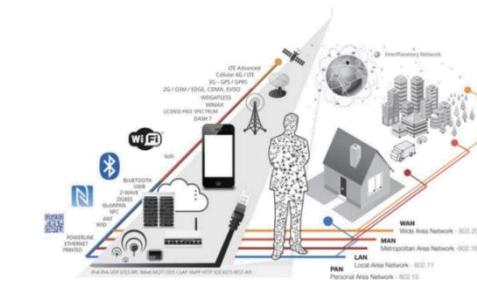
Cybersecurity and Industry 4.0

Components of IoT (3 Cs)



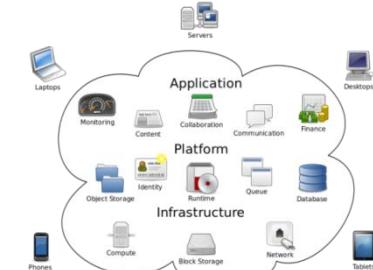
Components

Connecting the Real World to the Internet



Connections

Holding the System Parts Together



Cloud

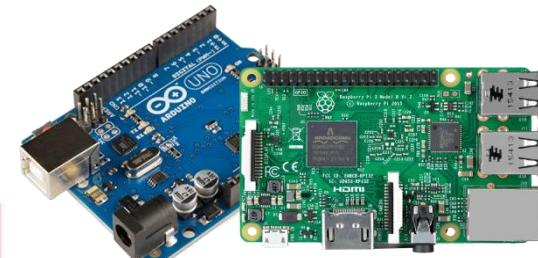
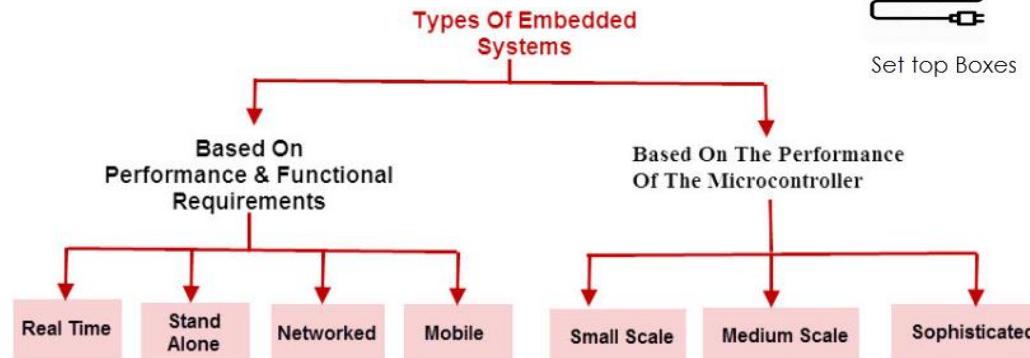
Storing and securing all the System Data



Cybersecurity and Industry 4.0

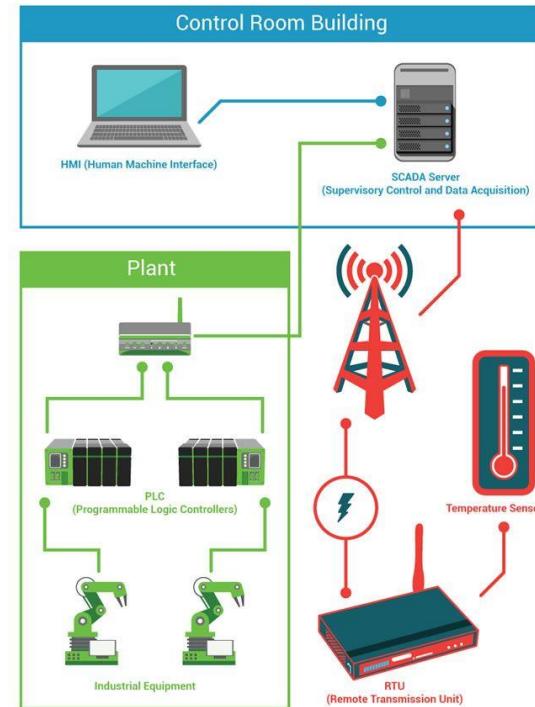
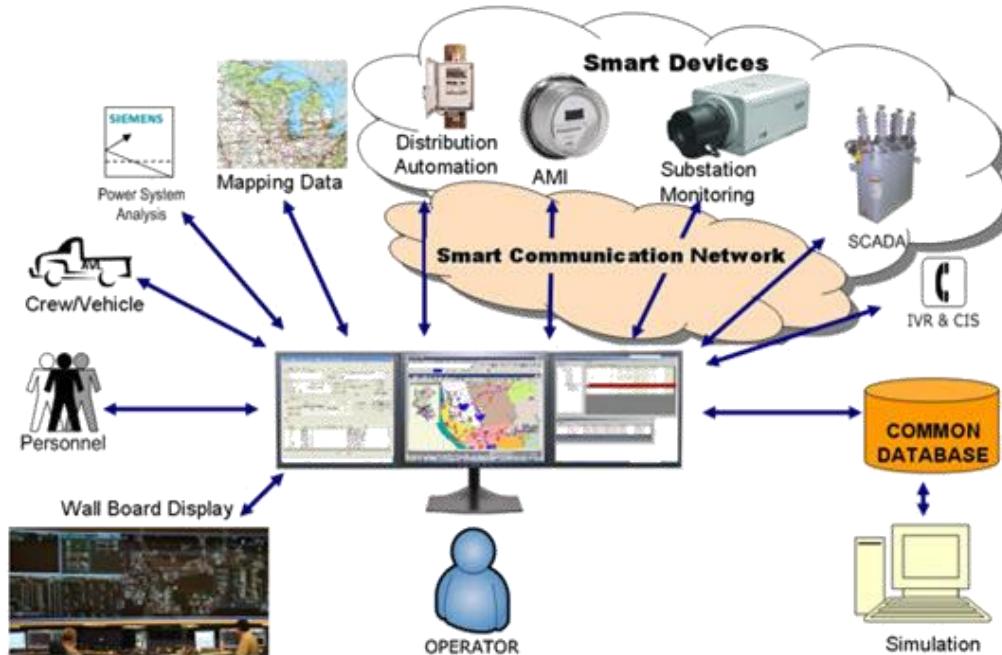
Embedded Systems

- controller with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints
- embedded as part of a complete device often including hardware and mechanical parts



Cybersecurity and Industry 4.0

Supervision Control and Data Acquisition

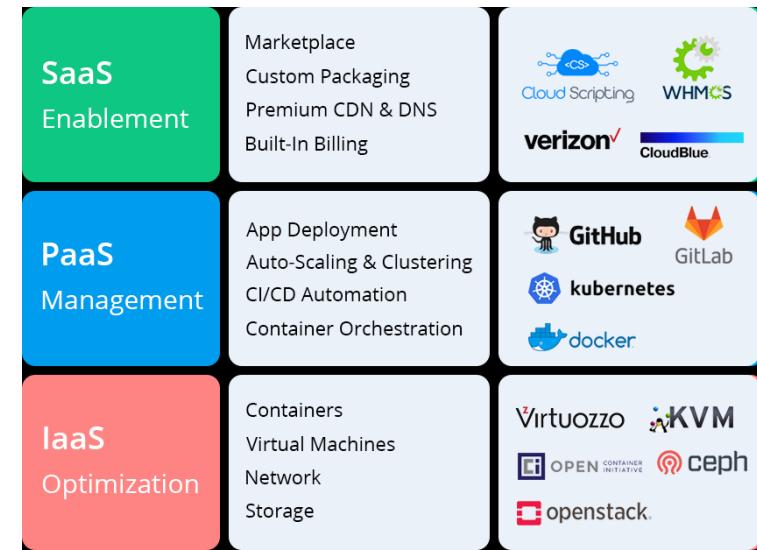


Cybersecurity and Industry 4.0

Cloud Computing is everything, from computing power to computing infrastructure, applications, business processes to personal collaboration— can be delivered as a service wherever and whenever needed.

The “*cloud*” is a set of hardware, networks, storage, services, and interfaces that combine to deliver computing as a service. *Cloud services* include the delivery of software, infrastructure, and storage over the Internet based on user demand.

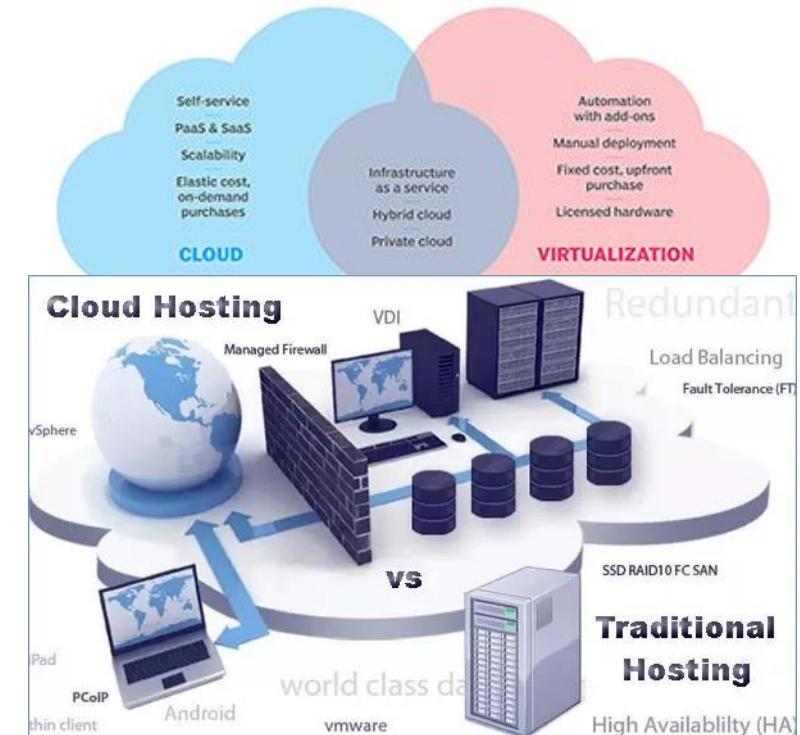
- Public Clouds – services provided via Internet
- Private Clouds – services deployed via a hosted data center or a company intranet
- Hybrid Clouds – combine the power of both public and private clouds



Cybersecurity and Industry 4.0

Advantages of Cloud Computing

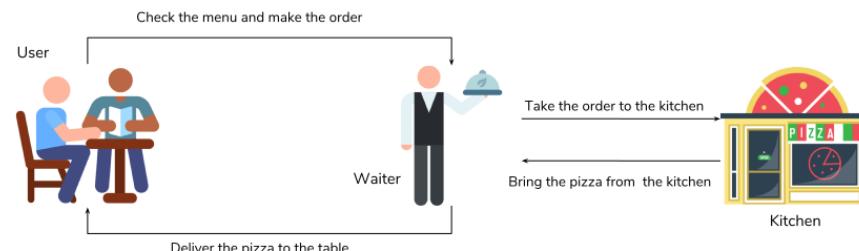
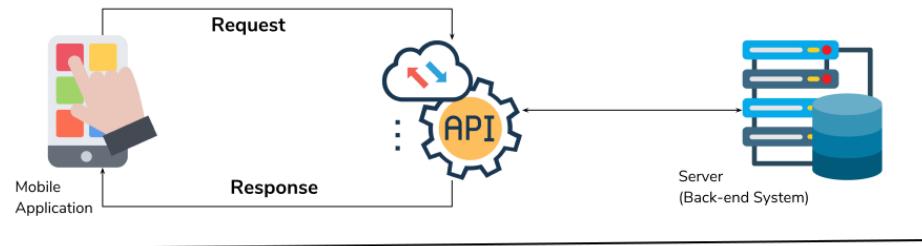
- Elasticity – makes the cloud scalable so that the resources allocated can be increased or decreased based upon demand.
- Efficiency – cloud resources can be obtained in a straightforward fashion and can be released if no longer required.
- Standardized APIs – communication among programs or data sources and linkages between cloud services is easier
- Resources Billing – usage is measured and customers pay only for resources used



Cybersecurity and Industry 4.0

Application Programming Interface (API)

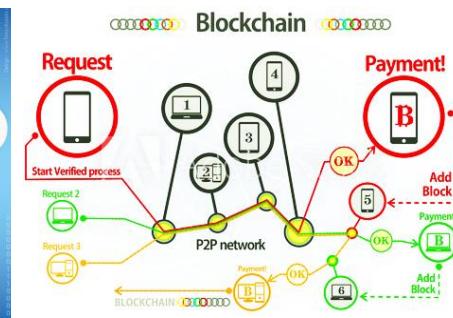
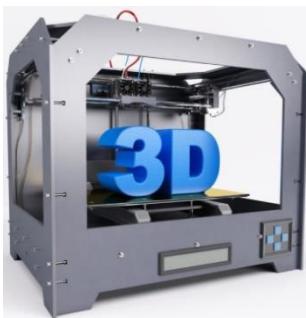
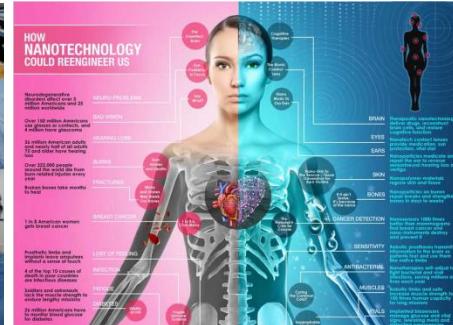
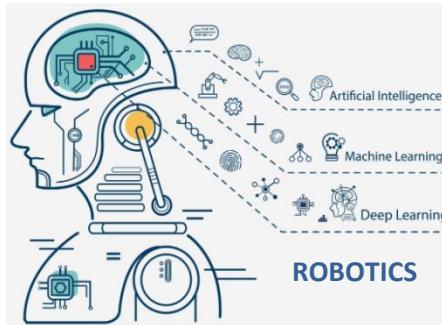
- set of routines, protocols, and tools for building software applications, as well as for communication among various components and interaction among software components



Web APIs are the defined interfaces through which interactions happen between an enterprise and applications that use its assets, which also is a *Service Level Agreement (SLA)* to specify the functional provider and expose the URL or service path for its API users

Cybersecurity and Industry 4.0

Other Technologies that Make the Industry 4.0



**Whatever you do, work heartily,
as for the Lord and not for men**

Colossians 3:23



Thank You!

Engr. Marvin De Pedro

marvin.depedro@gmail.com

09673873810