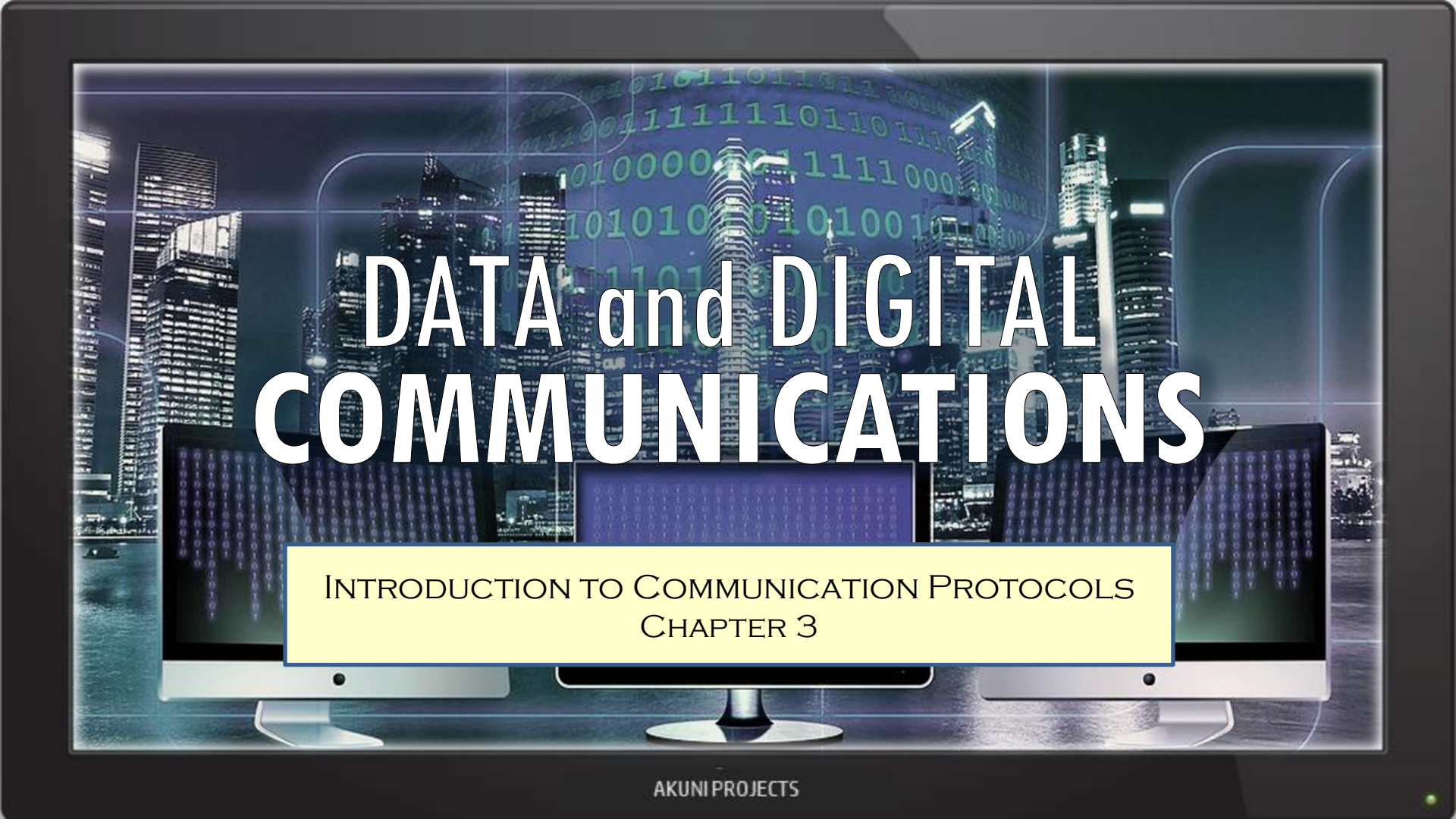
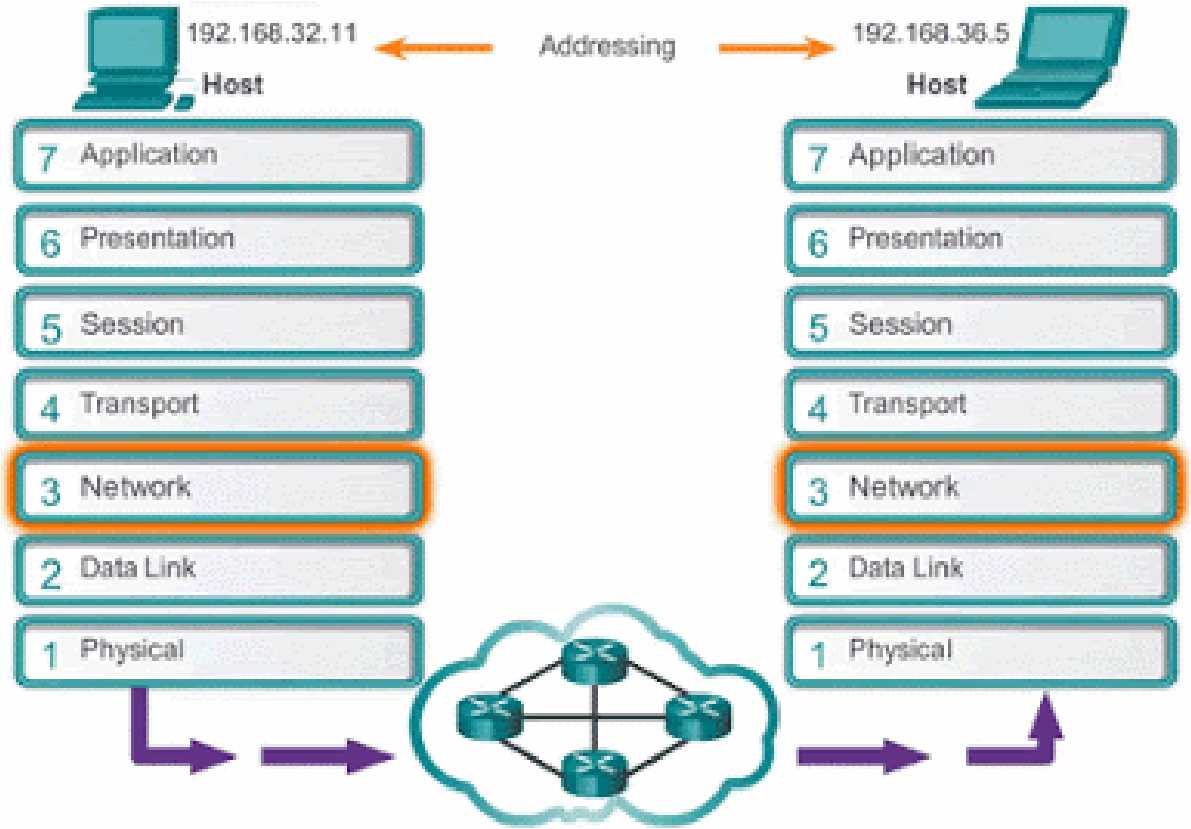
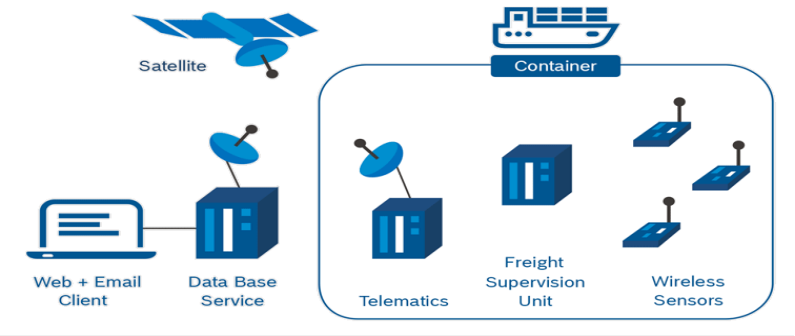

DATA and DIGITAL
COMMUNICATIONS
Introduction to Communication Protocols
Chapter 3
AKUNI PROJECTS



Chapter 3



Introduction to Communication Protocols

- Basic Concepts and the Physical Layer
- The Data Link and Network Layers
- The Transport and Session Layers
- The Presentation and Application Layers

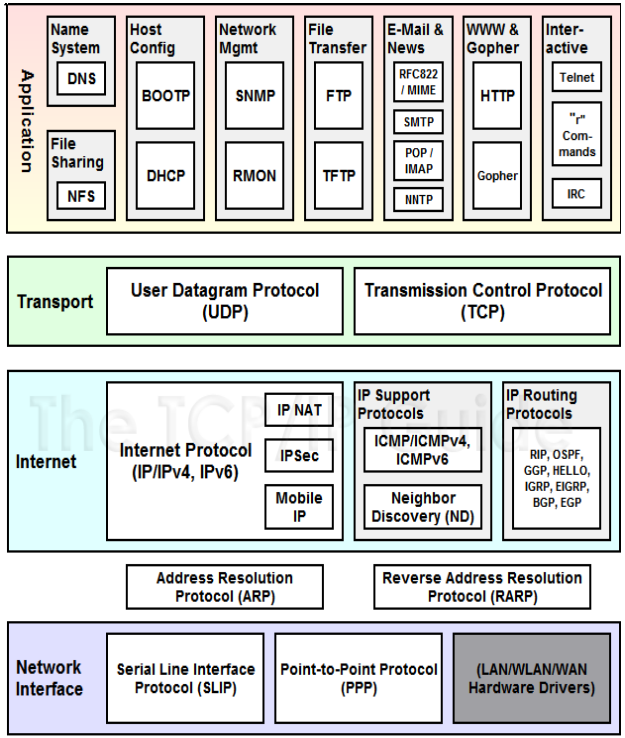
Module 9

Basic Concepts and the Physical Layer

Basic Concepts and the Physical Layer

Communication Protocols

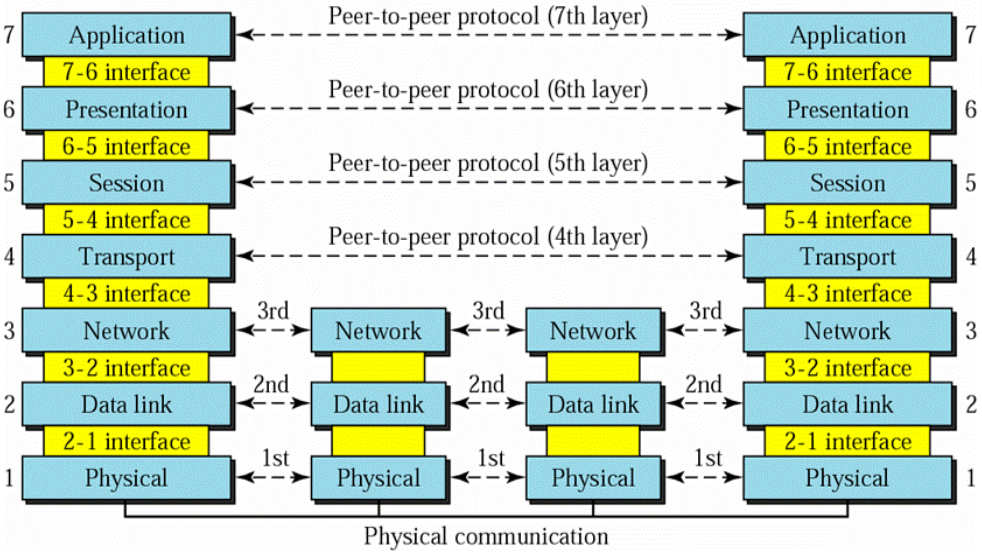
- formal descriptions of digital message formats and rules required to exchange messages in or between computing systems and are required in telecommunications
- rules, syntax, semantics and synchronization of communication and possible error recovery methods, as well as cover authentication, error detection and correction, and signaling



Basic Concepts and the Physical Layer

Open System Interconnect (OSI) is a conceptual model that enables diverse communication systems to communicate using standard protocols.

The OSI reference model guides developers and vendors so the digital communication and software products they create can interoperate, and to facilitate a clear framework that describes the functions of a network or a telecommunication system. Additionally, it is used trace how data is sent or received over a network



Basic Concepts and the Physical Layer

Transmission Control Protocol / Internet Protocol (TCP/IP) is a conceptual model and set of communications protocols used in the Internet and similar computer networks. It is composed of 4 layers (not including/separating the physical layer) instead of 7.

The TCP/IP Model helps

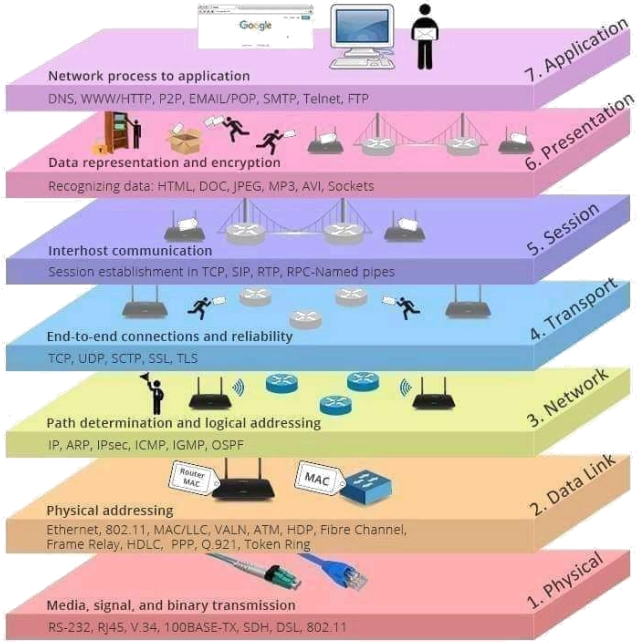
- determine how a specific computer should be connected to the internet and how data should be transmitted between them
- create a virtual network when multiple computer networks are connected together
- allow communication over large distances

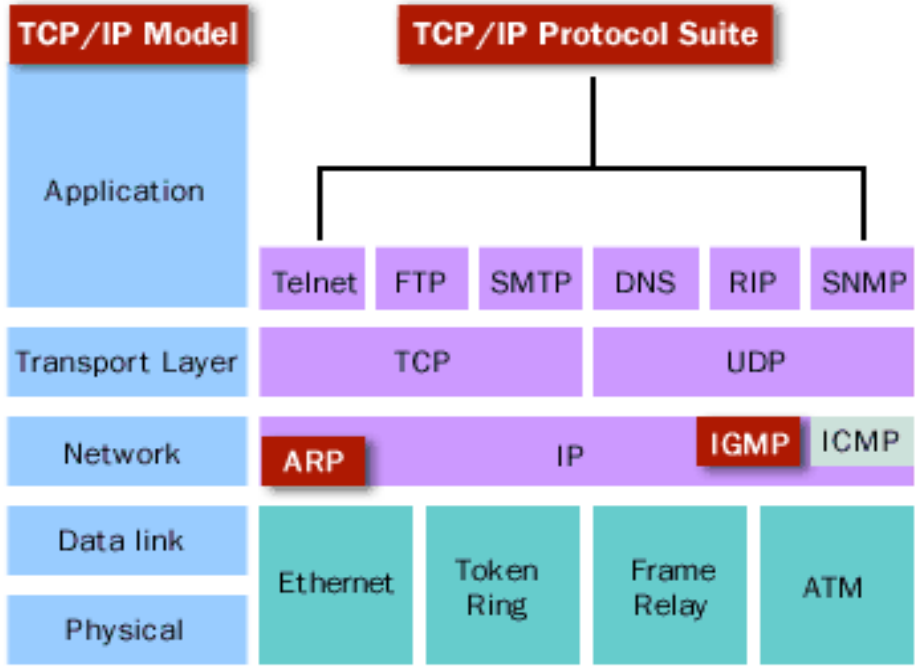
NETWORK LAYER	FUNCTIONS AND PROTOCOLS
Application Layer	Protocol that dictates the method used to send data such as HTTP & FTP (web-based), POP3 & SMTP (Email), SSL & TLS (Security) and SNMP (Network Management)
Transport Layer	Protocol responsible for dictating format of data sent, exactly where it is sent to and maintaining data integrity such as TCP and UDP.
Internet Layer	Purely transports data packets (datagrams) across network boundaries. Possible Internet layer include, IP, ICMP & IGMP.
Physical (Network Interface)	The physical/logical network components used to interconnect hosts or nodes in a network (only on host side). Examples include ISDN, Ethernet, ATM, Wi-Fi.

The ***TCP/IP suite*** is a set of protocols that provides an end-to-end connectivity by specifying how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network.

Basic Concepts and the Physical Layer

OSI and TCP/IP Models

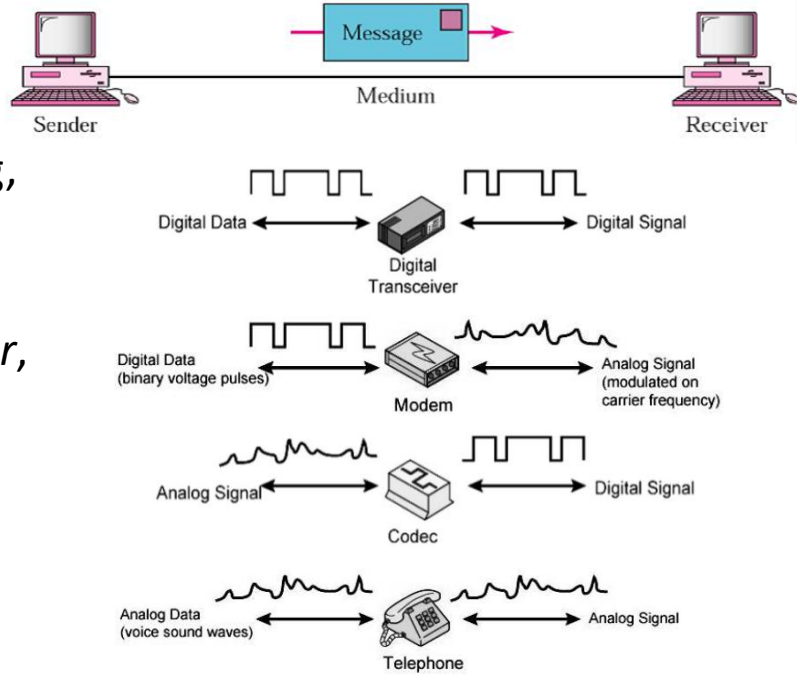




Basic Concepts and the Physical Layer

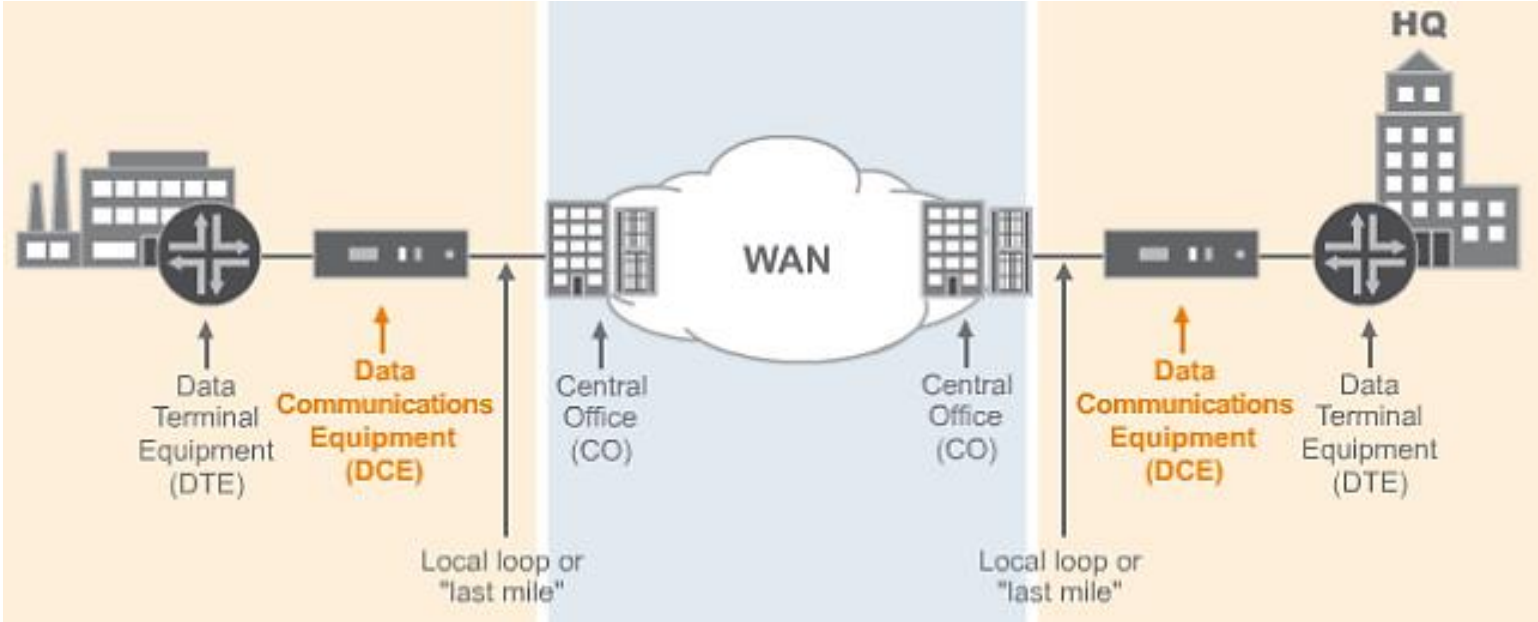
Physical Layer

- plays the role of interacting with actual hardware and signalling mechanism (defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.)
- provides its services to the *Data Link Layer*, which hands over *frames* to the physical layer; these frames are then converted by the physical layer to electrical pulses, which represent binary data that is then sent over the transmission media



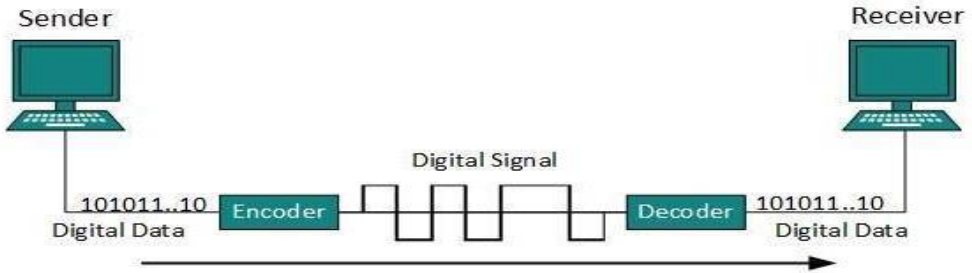
Basic Concepts and the Physical Layer

DTE and DCE

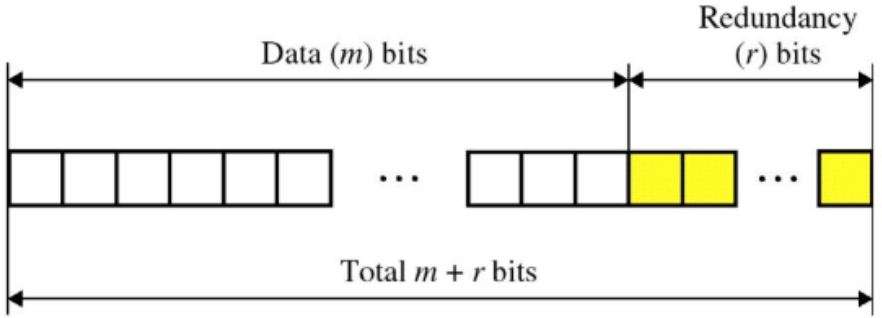


Basic Concepts and the Physical Layer

Digital transmission of digital data basically involves the ***line coding*** and ***block coding*** processes. Line coding is the process for converting digital data (binary bits) into digital signal.



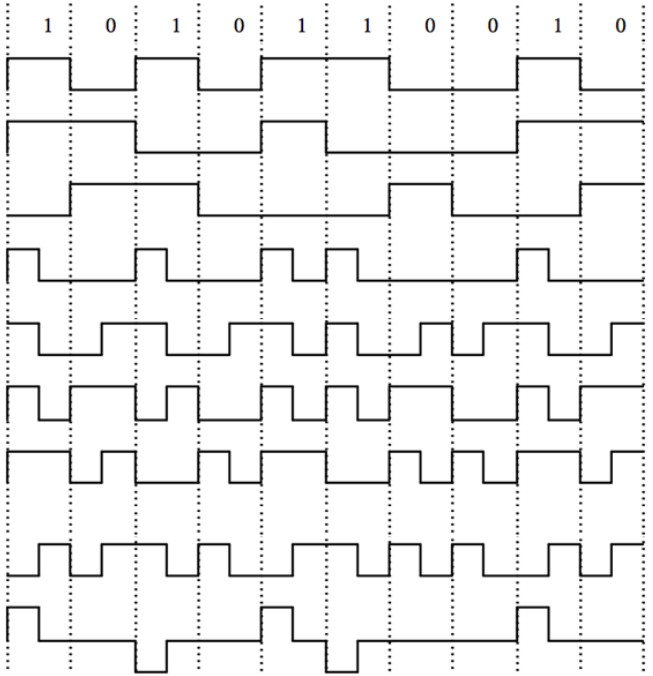
Furthermore, to ensure accuracy of the received data frame, block coding is done wherein ***redundant bits*** are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even and so the original number of bits is increased. Overall, line coding is necessary while block coding is optional,



Basic Concepts and the Physical Layer

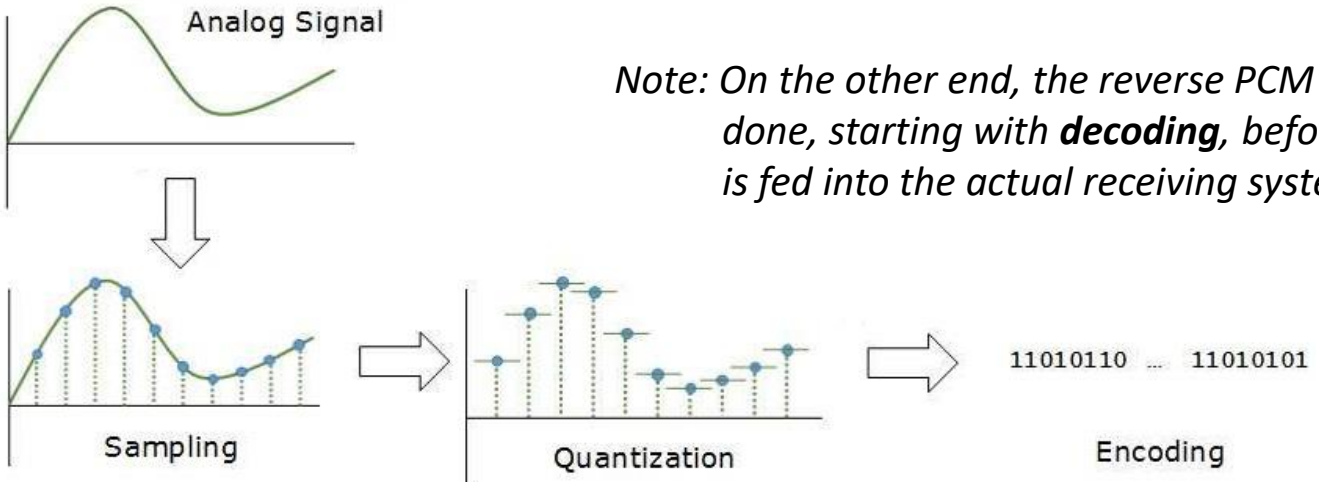
Common Types of Line Coding Schemes

Signal	Comments	1 state	0 state
NRZ–L	Non-return-to-zero level. This is the standard positive logic signal format used in digital circuits.	forces a high level	forces a low level
NRZ–M	Non-return-to-zero mark	forces a transition	does nothing (keeps sending the previous level)
NRZ–S	Non-return-to-zero space	does nothing (keeps sending the previous level)	forces a transition
RZ	Return to zero	goes high for half the bit period and returns to low	stays low for the entire period
Biphase–L	Manchester. Two consecutive bits of the same type force a transition at the beginning of a bit period.	forces a negative transition in the middle of the bit	forces a positive transition in the middle of the bit
Biphase–M	Variant of Differential Manchester. There is always a transition halfway between the conditioned transitions.	forces a transition	keeps level constant
Biphase–S	Differential Manchester used in Token Ring. There is always a transition halfway between the conditioned transitions.	keeps level constant	forces a transition
Differential Manchester (Alternative)	Need a Clock, always a transition in the middle of the clock period	is represented by no transition.	is represented by a transition at the beginning of the clock period.
Bipolar	The positive and negative pulses alternate.	forces a positive or negative pulse for half the bit period	keeps a zero level during bit period



Basic Concepts and the Physical Layer

In digital transmission of analog data, digitization must be done first. ***Pulse Code Modulation*** (PCM) is the most common method used and it comes in three steps:



*Note: On the other end, the reverse PCM is done, starting with **decoding**, before data is fed into the actual receiving system.*

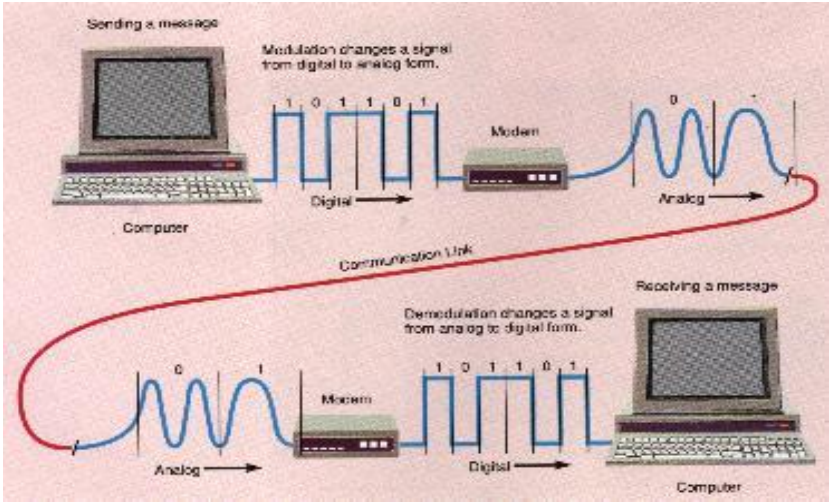
The same process with Line Coding happens in the encoding stage of PCM.

Basic Concepts and the Physical Layer

To transmit the digital data over an analog media, it must go through a digital-to-analog converter (DAC) first. It can be through bandpass filters (BPF) that allow only the frequencies of interest to pass, or through low-pass filters that allow to pass only frequencies that are below the cut-off.

Analog carrier signals are modified to reflect digital data. Thus, ***digital modulation*** or analog transmission of digital data can be in the form of:

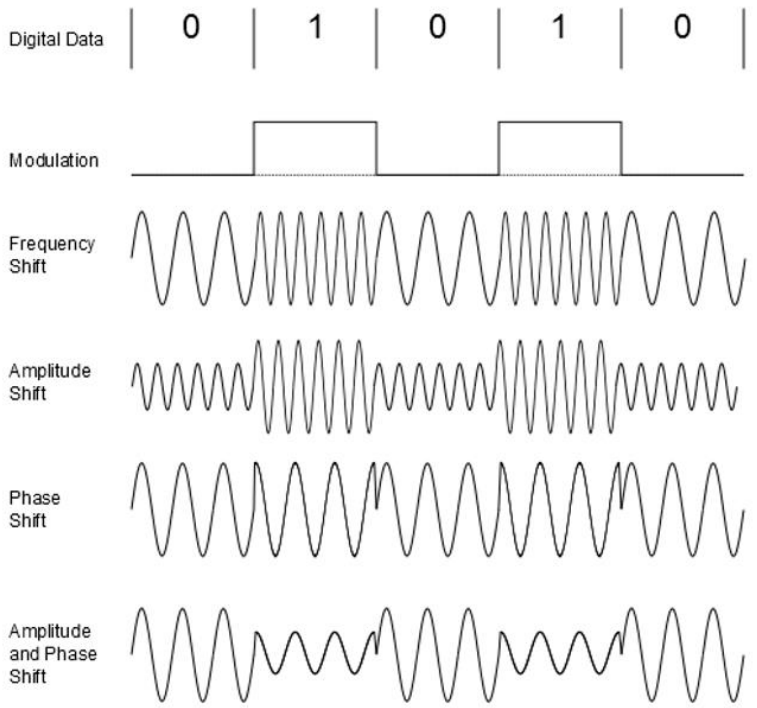
- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)
- Quadrature Amplitude Modulation (QAM)



Basic Concepts and the Physical Layer

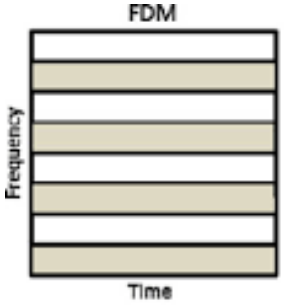
Types of Digital Modulation

Modulation	Units	Bits/Baud	Baud rate	Bit Rate
ASK, FSK, 2-PSK	Bit	1	N	N
4-PSK, 4-QAM	Dibit	2	N	2N
8-PSK, 8-QAM	Tribit	3	N	3N
16-QAM	Quadbit	4	N	4N
32-QAM	Pentabit	5	N	5N
64-QAM	Hexabit	6	N	6N
128-QAM	Septabit	7	N	7N
256-QAM	Octabit	8	N	8N

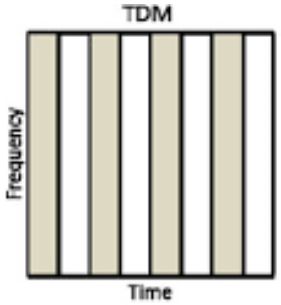


Basic Concepts and the Physical Layer

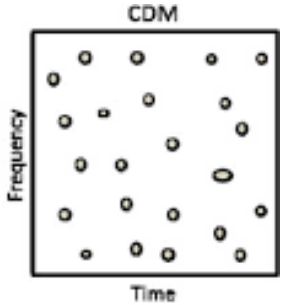
Multiplexing is a technique by which different streams of transmission can be simultaneously processed over a shared link. It divides the high capacity medium into low capacity logical medium which is then shared by different streams. The reverse of this process is called ***demultiplexing***.



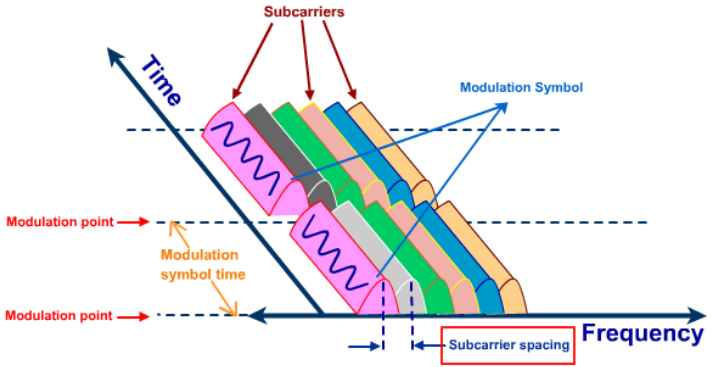
Frequency Division Multiplexing



Time Division Multiplexing



Code Division Multiplexing

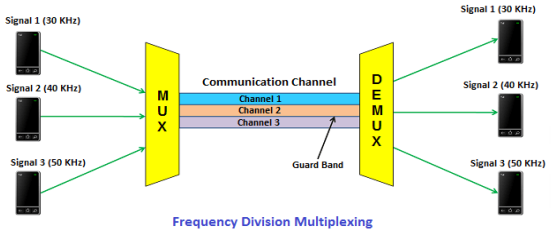


Orthogonal FDM (OFDM)

Basic Concepts and the Physical Layer

Frequency Division Multiplexing

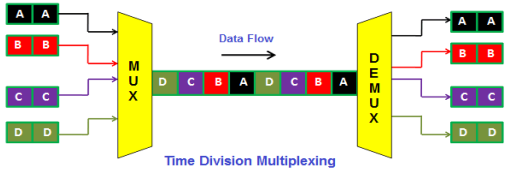
- used in analog TV and radio broadcast systems where the carrier bandwidth is divided into logical channels and allocates one user to each channel



Frequency Division Multiplexing

Time Division Multiplexing

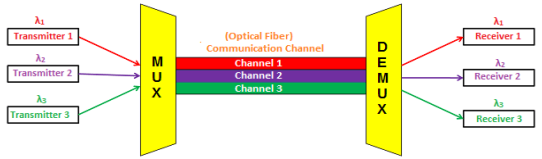
- used in telephone systems where shared channel is divided among its users by means of time slot where each user transmit data within the provided time slot only



Time Division Multiplexing

Wavelength Division Multiplexing

- used in fiber optic systems where multiple optical carrier signals are multiplexed by using different wavelengths

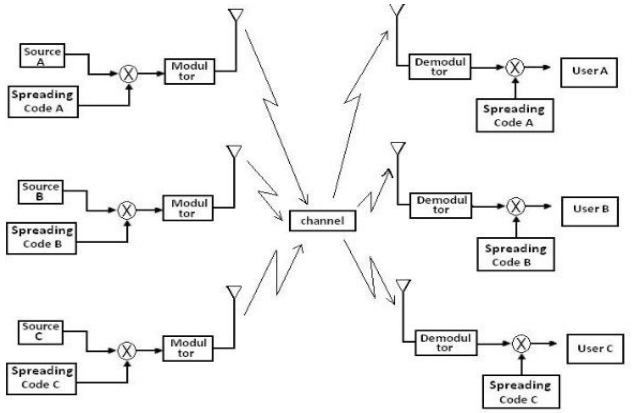


Wavelength Division Multiplexing

Basic Concepts and the Physical Layer

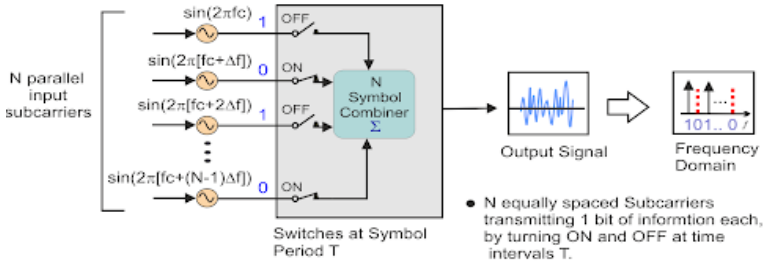
Code Division Multiplexing

- applied in TCP/IP communication to transmit multiple data signals over a single frequency but allows its users to full bandwidth and transmit signals all the time using an orthogonal code to spread the signals



Orthogonal Frequency Division Multiplexing

- single data stream is split across several separate narrowband channels at different frequencies to reduce interference and crosstalk
- used in digital TV and audio broadcasting, DSL internet access, wireless networks, power line networks, and 4G/5G mobile communications

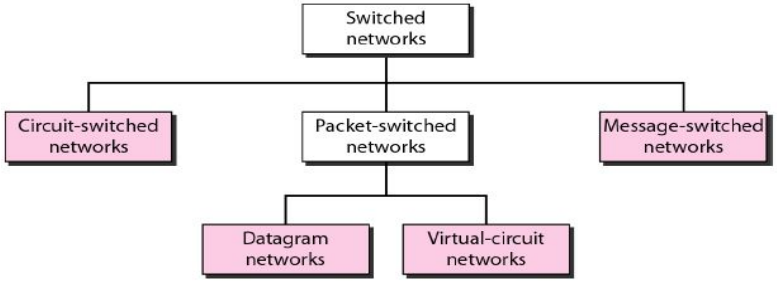


Basic Concepts and the Physical Layer

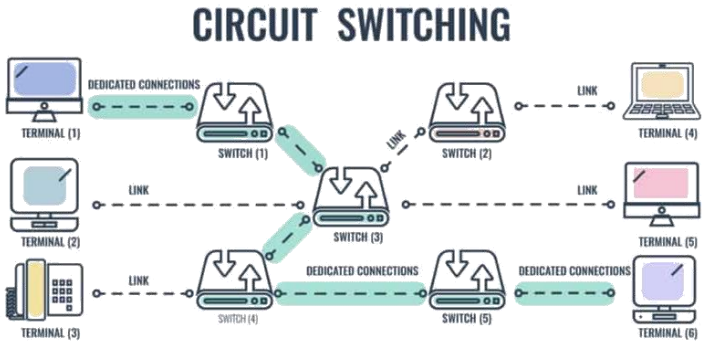
Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called **ingress**, and when data leaves a port or goes out it is called **egress**. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

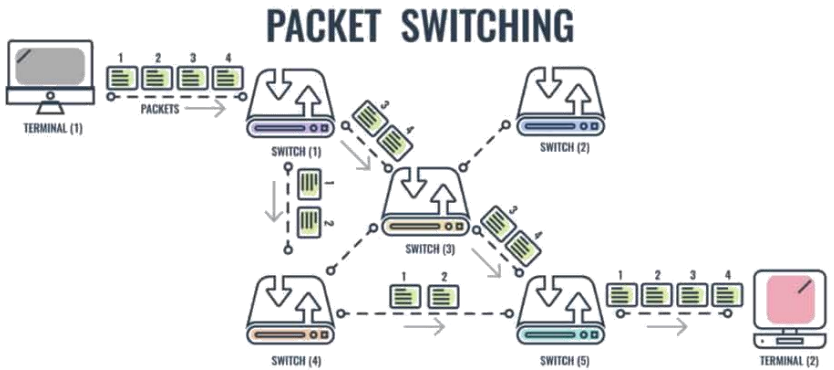
- Connectionless – data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- Connection-Oriented – Before switching data to be forwarded to destination, a pre-establish circuit along the path between both endpoints is required. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Basic Concepts and the Physical Layer

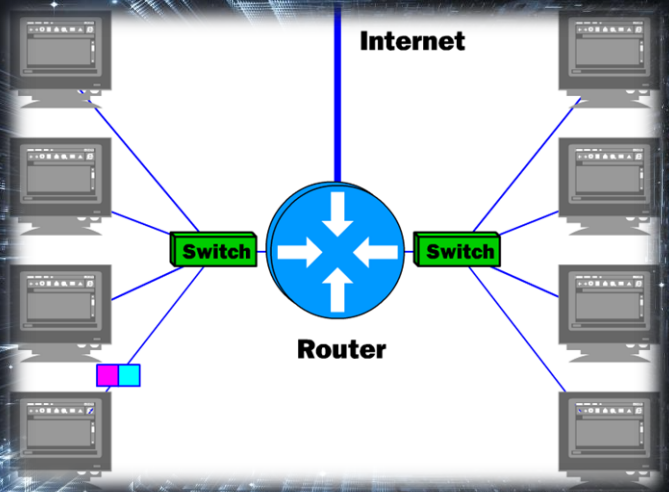


Parameter	Message switching	Circuit switching	Packet switching
Application	Telegraph network for transmission of telegrams	Telephone network for bi-directional, real time transfer of voice signals	Internet for datagram and reliable stream service between computers
End terminal	Telegraph, teletype	Telephone, modem	Computer
Information type	Morse, Baudot, ASCII	Analog voice or PCM digital voice	Binary information
Transmission system	Digital data over different transmission media	Analog and digital data over different transmission media	Digital data over different transmission media





Module 10

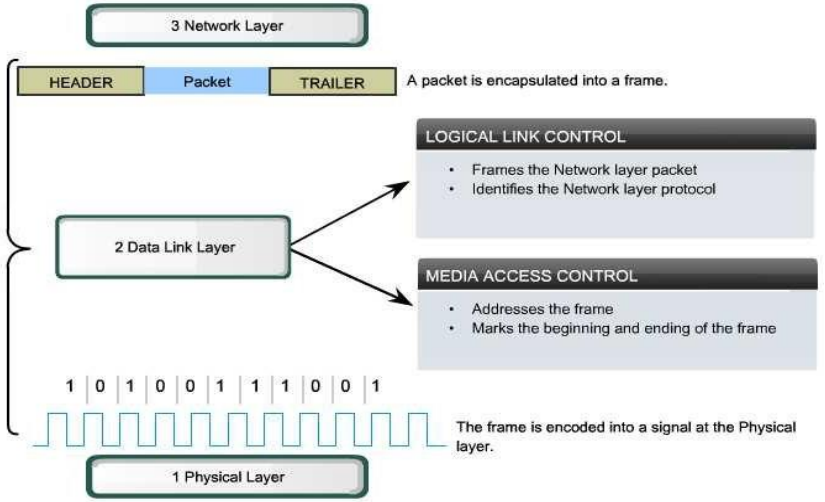


The Data Link and Network Layers

The Data Link and Network Layers

Data Link Layer

- responsible for the exchange of frames between nodes over a physical network media and ensures that all packets of information are passed on free of errors
- works between two hosts which are directly connected in some sense that could be point to point or broadcast; systems on broadcast network are said to be on same link
- its work tends to get more complex when it deals with multiple hosts on single collision domain

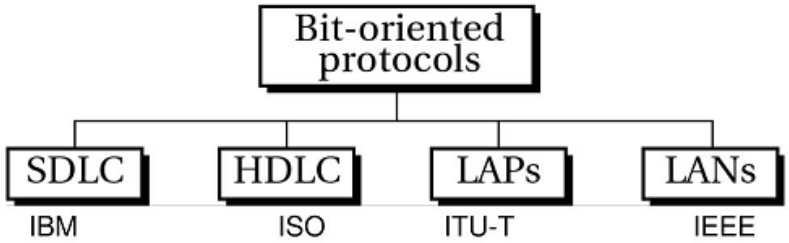


The Data Link and Network Layers

Frame Relay – telecommunication service designed for cost-efficient data transmission for intermittent traffic between LANs and between endpoints in WANs

Token Ring – networking technology used to build local area networks; it uses a special 3-byte frame (*token*) that travels around a logical ring of workstations or servers

Asynchronous Transfer Mode (ATM) – switching technique used by telecommunication networks that uses asynchronous TDM to encode data into small, fixed-sized cells



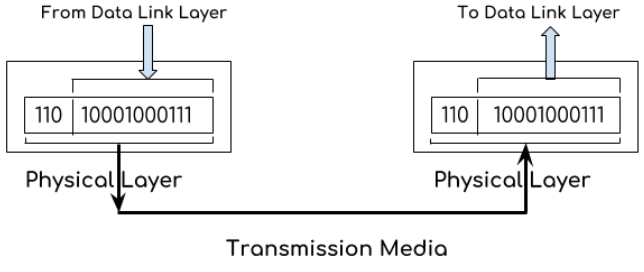
SDLC – Synchronous Data Link Control
HDLC – High-Level Data Link Control
LAPs – Link Access Protocols
LAN – Local Area Nelwork

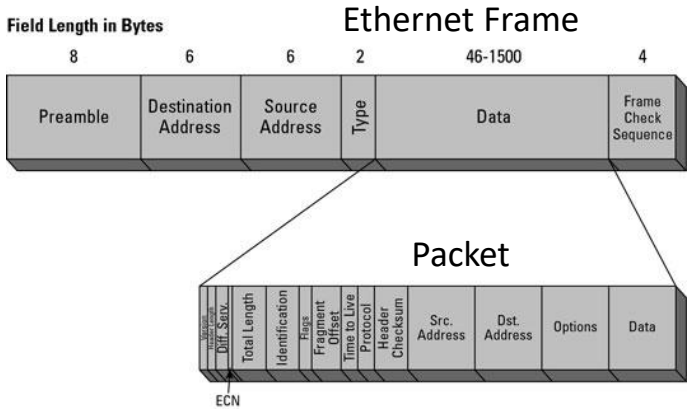
Point-to-Point Protocol (PPP) – provides a standard method for transporting multi-protocol datagrams over PPP links, as well as connection authentication, transmission encryption, and compression.

The Data Link and Network Layers

Services in the Data Link Layer

1. Framing – packets are taken from the network layer and encapsulated into ***frames***, which are then sent bit-by-bit to the physical layer
2. Addressing – data-link layer provides layer-2 hardware addressing mechanism in the form of MAC addresses
3. Synchronization – when data frames are sent on the link, both machines must be synchronized in order to transfer to take place





The Data Link and Network Layers

Services in the Data Link Layer

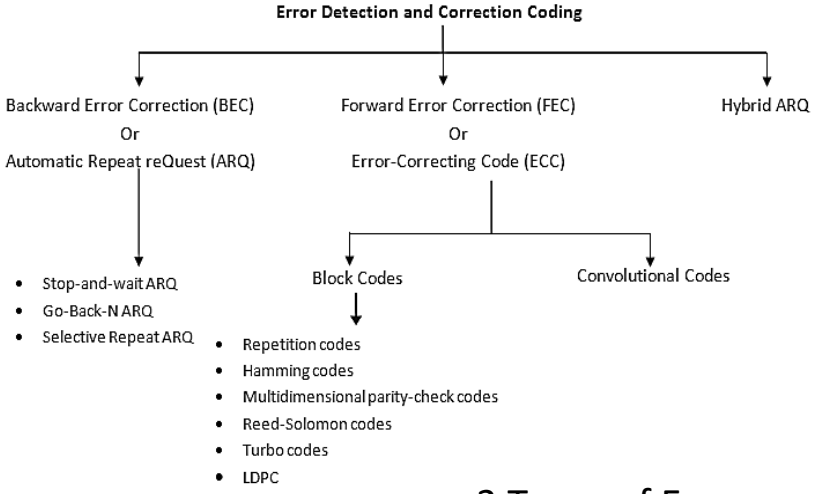
4. Error Control – signals may have encountered problem in transition and the bits are flipped; these errors are detected and the actual data bits are attempted to be recovered with an error reporting mechanism

Error detection
- Check if any error has occurred
- Don't care the number of errors
- Don't care the positions of errors

} Parity Check / CRC

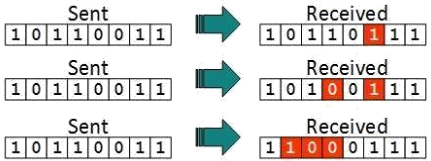
Error correction
- Need to know the number of errors
- Need to know the positions of errors
- More difficult

} BEC / FEC / ARQ



3 Types of Error

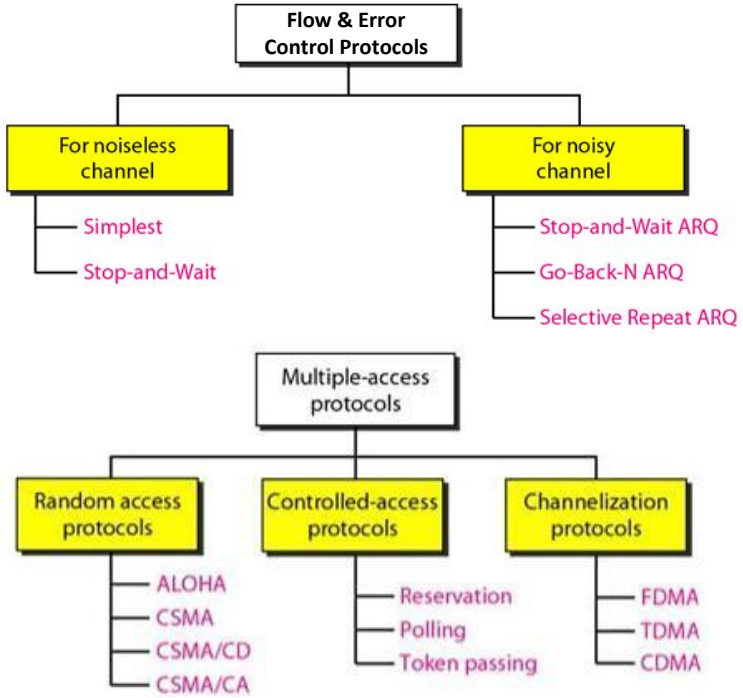
- Single-Bit Error
- Multiple-Bit Error
- Burst Error



The Data Link and Network Layers

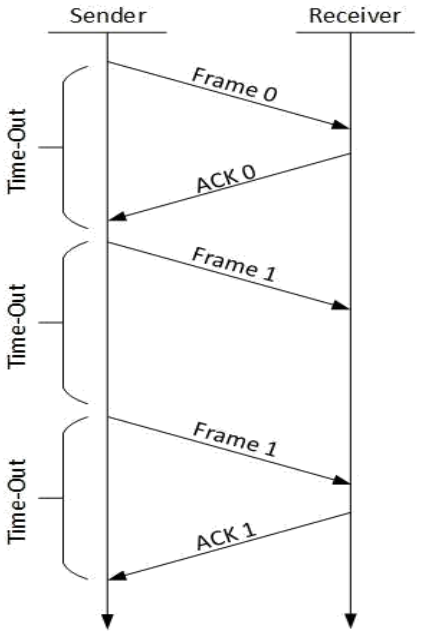
Services in the Data Link Layer

5. Flow Control – stations on same link may have different speed or capacity, and so the data-link layer ensures that both machine to exchange data on same speed
6. Multi-Access – when host on the shared link tries to transfer the data, it has a high probability of collision and hence, mechanism such as *CSMA/CD* and *CSMA/CA* are provided to equip capability of accessing a shared media among multiple systems

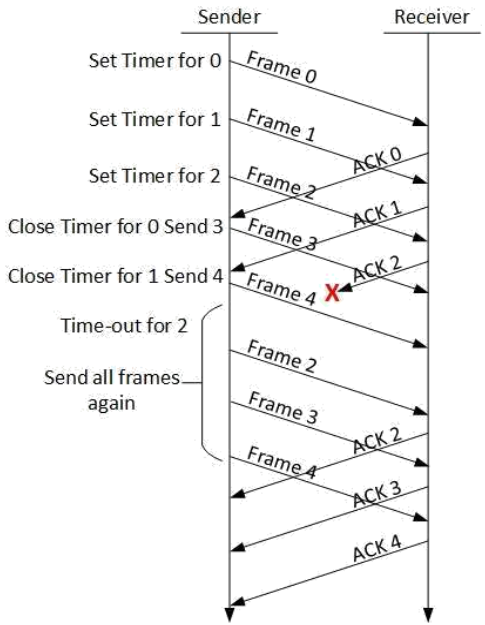


The Data Link and Network Layers

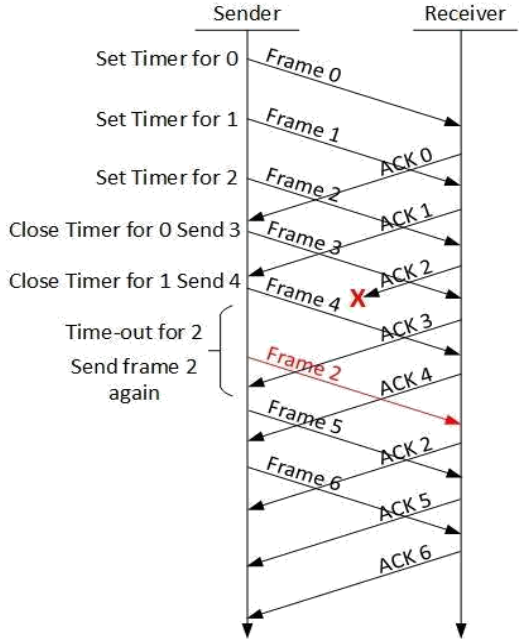
Stop-and-Wait ARQ



Go-Back-N ARQ



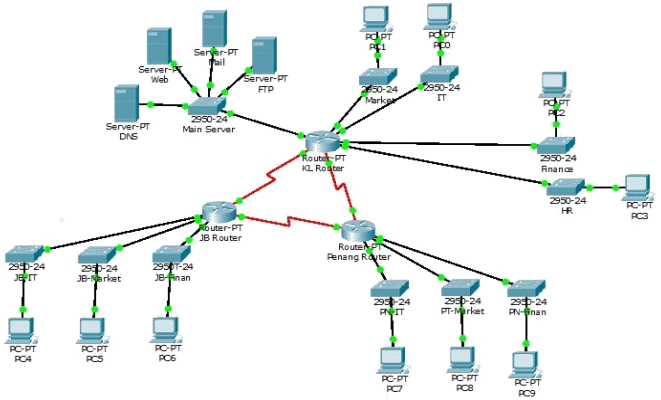
Selective ARQ

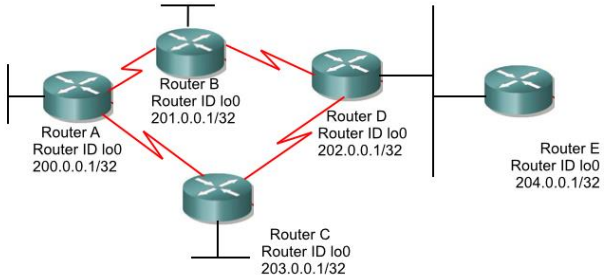


The Data Link and Network Layers

Network Layer

- provides services to allow end devices to exchange data across the network
- manages options pertaining to host and network addressing, managing sub-networks, and internetworking
- takes the responsibility for routing packets from source to destination within or outside a subnet
- divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels

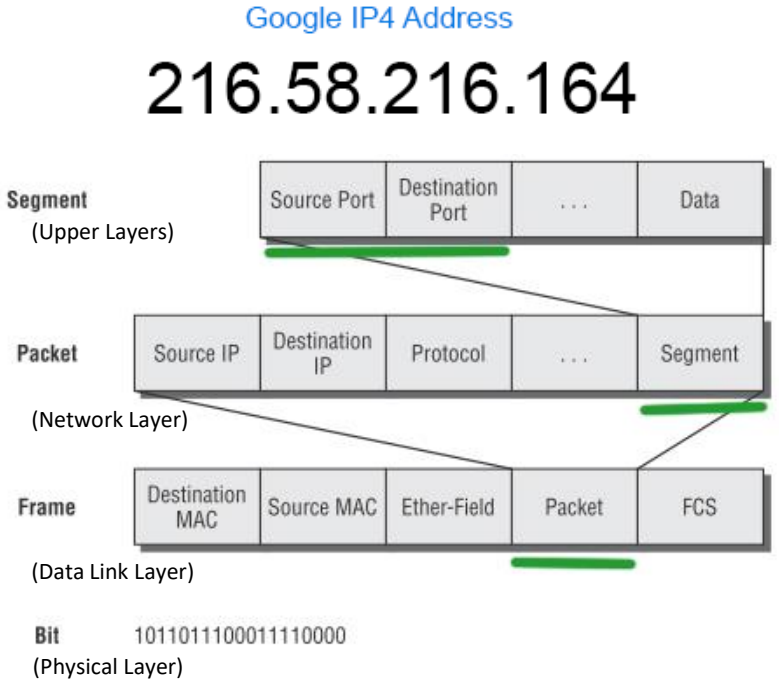




The Data Link and Network Layers

Services in the Network Layer

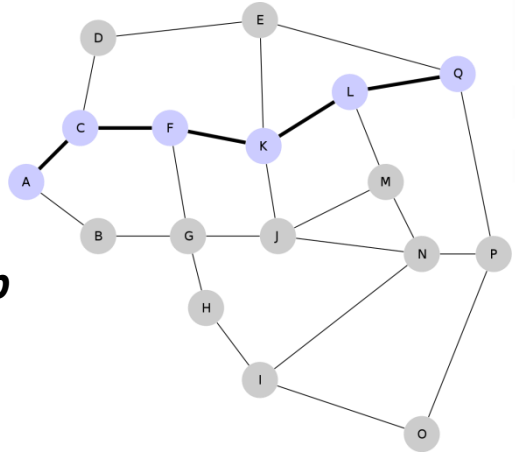
1. Addressing End Devices – in the same way that a phone has a unique number, end devices must be configured with a unique IP address for identification on the network as a ***host***
2. Encapsulation – the network layer receives a ***protocol data unit*** (PDU) from the transport layer and in a process called ***encapsulation***, it adds IP header information and the PDU becomes a ***packet***.

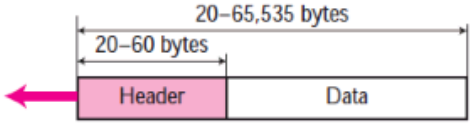


The Data Link and Network Layers

Services in the Network Layer

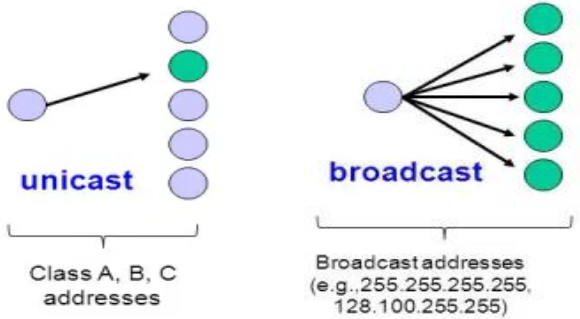
3. Routing – the network layer directs packets to a destination host on another network through a ***routing*** process wherein a router selects paths for and directs packets toward the destination host, and each route the packet takes to reach the destination host is called a ***hop***
4. De-encapsulation – when the packet arrives at the network layer of the destination host, the host checks the packet's IP header and if the destination IP address within it matches its own IP address, the header is removed and the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer



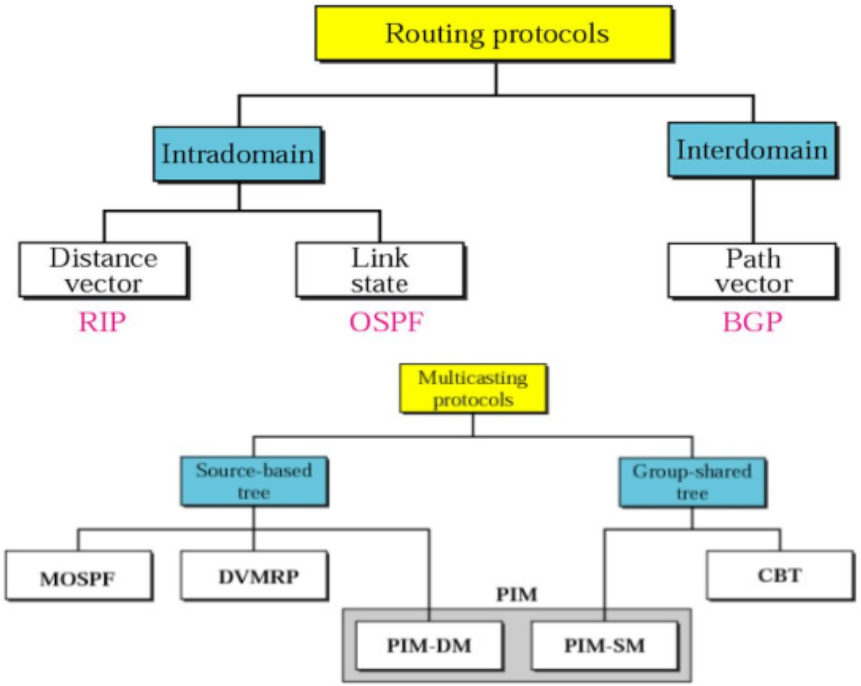


The Data Link and Network Layers

IP Routing Modes



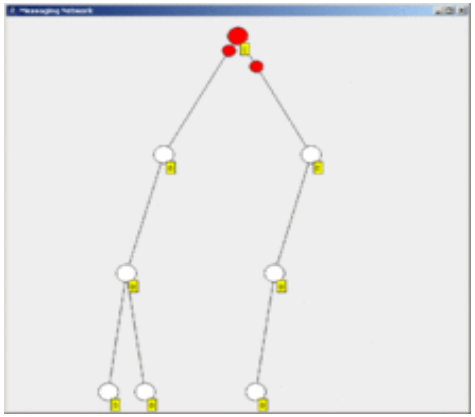
Unicast



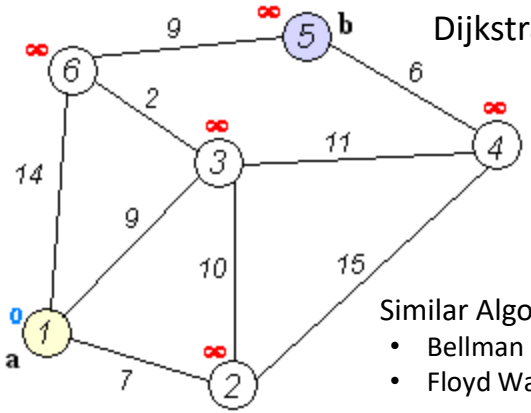
The Data Link and Network Layers

Routing Algorithms

- Flooding – simplest method packet forwarding; when a packet is received, the routers send it to all the interfaces except the one on which it was received.



- Shortest Path – routing decision in networks are mostly taken on the basis of cost between source and destination, considering the ***hop count***;



Dijkstra's Algorithm

Similar Algorithms

- Bellman Ford Algorithm
- Floyd Warshall Algorithm

The Data Link and Network Layers

Network Layer Protocols

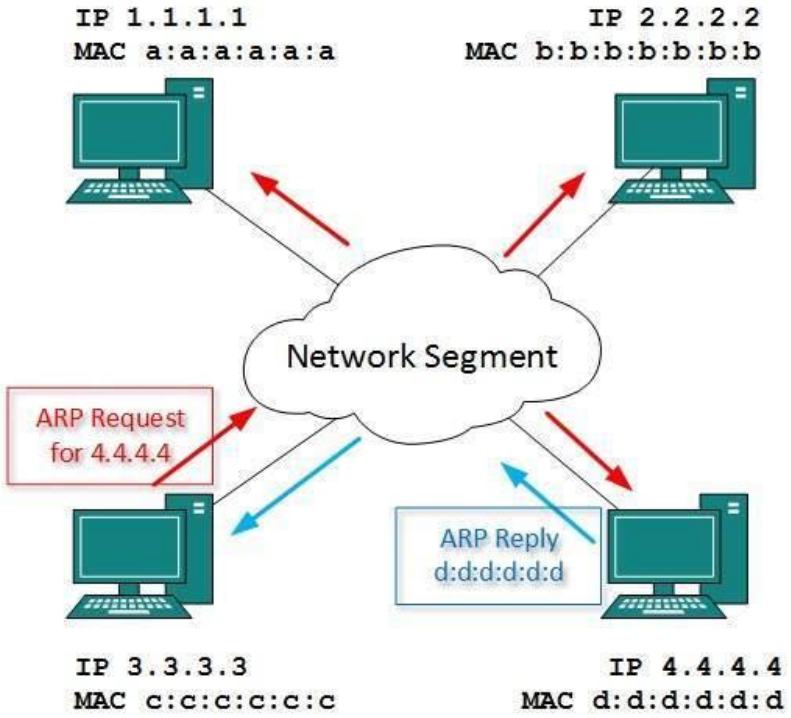
1. Internet Protocol (IP) – enables every host on the TCP/IP network to be uniquely identifiable; connectionless, best-effort, and media-independent protocol that provides only the necessary functions for delivering a packet from a source to a destination over an interconnected system of networks
2. Internet Control Message Protocol (ICMP) – network diagnostic and error reporting protocol that belongs to IP protocol suite and uses IP as carrier protocol to send back to the originating host any feedback about network such as *ICMP-echo* and *ICMP-echo-reply* messages encapsulated in an IP packet

	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} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

The Data Link and Network Layers

Network Layer Protocols

3. Address Resolution Protocol (ARP) – used to send out an ARP broadcast message asking, “Who has this IP address?” to know the MAC address of remote host on a broadcast domain; also includes the IP address of destination host (the sending host wishes to talk to) into a packet, so that when a host receives an ARP packet destined to it, it replies back with its own MAC address



The Data Link and Network Layers

Network Layer Protocols

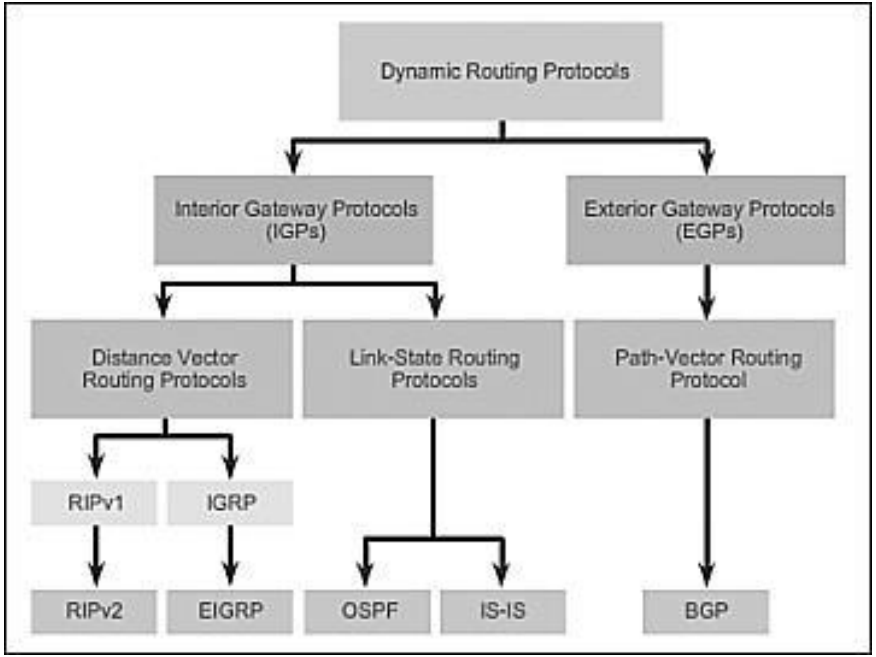
4. IP Routing Protocols – specify how routers talk to each other to distribute information so they can select routes between any two nodes on a network; ***Routing Information Protocol*** (RIP) is one the most common of these protocols

Protocol	Type	Scalability	Metric	IP classes
RIP-1	Distance vector	Small	Hop count	Classful
RIP-2	Distance vector	Small	Hop count	Classless
OSPF-2	Link state	Large	Cost	Classless
IS-IS	Link state	Very large	Cost	Classless
IGRP	Distance vector	Medium	Bandwidth, delay, load, MTU, reliability	Classful
EIGRP	Dual	Large	Bandwidth, delay, load, MTU, reliability	Classless
BGP	Distance vector	Large	Vector of attributes	Classless

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman-Ford		Dijkstra
Path Selection	Hop based		Shortest Path
Routing	Classful	Classless	Classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		*110*
Hop Count Limitation	15		No Limitation
Authentication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	RIP>OSPF		

The Data Link and Network Layers

Dynamic routing protocols are a solution that is used in large networks so as to reduce the complexity in configuration that would be occasioned by having to configure static routes. These are used to enable the routers exchange routing information, they allow routers to learn about remotely connected networks dynamically. This information is then added to their routing tables as a basis for forwarding packets.



The Data Link and Network Layers

IP Packets

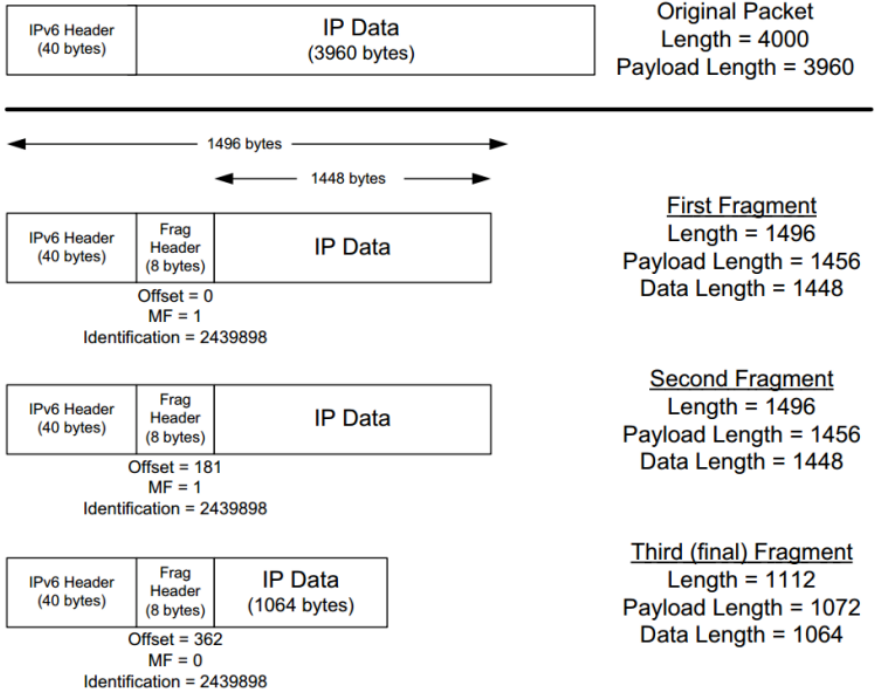
- **Payload** (IP Data) - contains the Layer 4 segment information and the actual data
- **IP Header** - identifies the packet characteristics; contains significant fields

Original IP Packet

Sequence	Identifier	Total Length	DF	MF	Fragment Offset
0	345	5140	0	0	0

IP Fragments

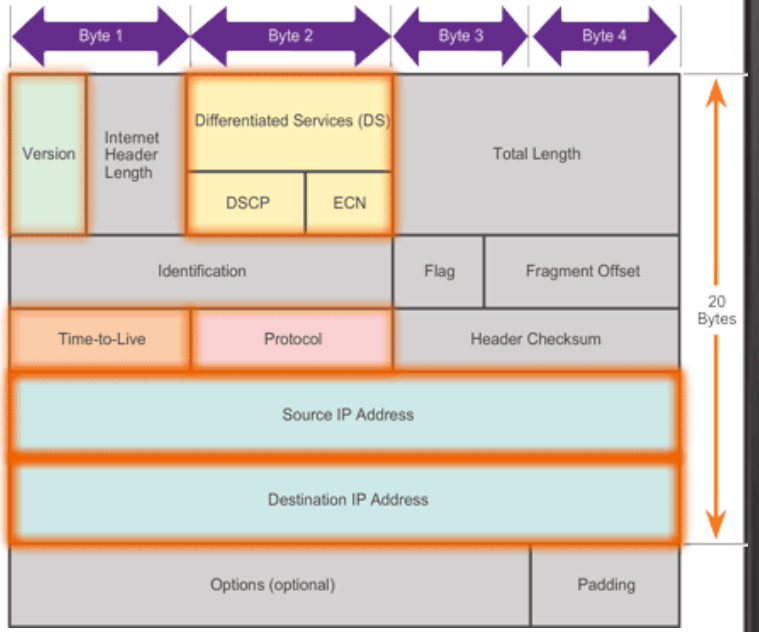
Sequence	Identifier	Total Length	DF Flag	MF Flag	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555



The Data Link and Network Layers

Significant Fields in an IPv4 Packet Header

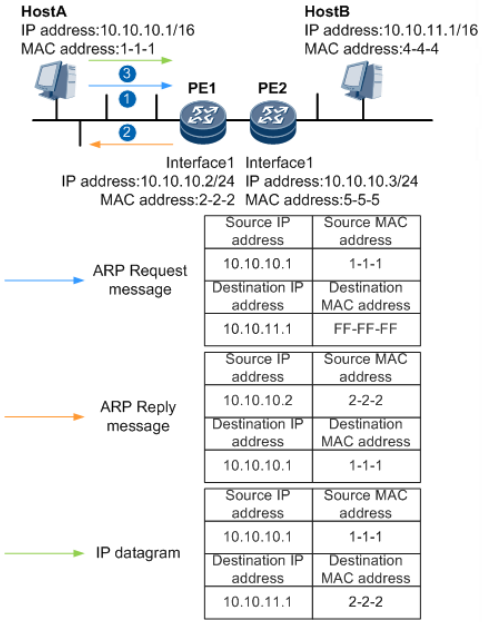
- Version – contains a 4-bit binary value identifying the IP packet version; always set to 0100
- Differentiated Services (DS) – 8-bit field used to determine the priority of each packet; the first 6 bits identify the *Differentiated Services Code Point* (DSCP) value used by a *quality of service* (QoS) mechanism, while the last 2 bits identify the *explicit congestion notification* (ECN) value that can be used to prevent dropped packets during times of network congestion; formerly called the *Type of Service* (ToS) field



The Data Link and Network Layers

Significant Fields in an IPv4 Packet Header

- Time-to-Live (TTL) - contains an 8-bit binary value used to limit the lifetime of a packet; specified in seconds but commonly referred to as *hop count;* the *traceroute* command uses this field to identify the routers used between the source and destination
- Protocol – 8-bit binary value that indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol; common values include ICMP (1), TCP (6), and UDP (17)
- Source IP Address – contains a 32-bit binary value that represents the source IP address of the packet.
- Destination IP Address – contains a 32-bit binary value that represents the destination IP address of the packet.

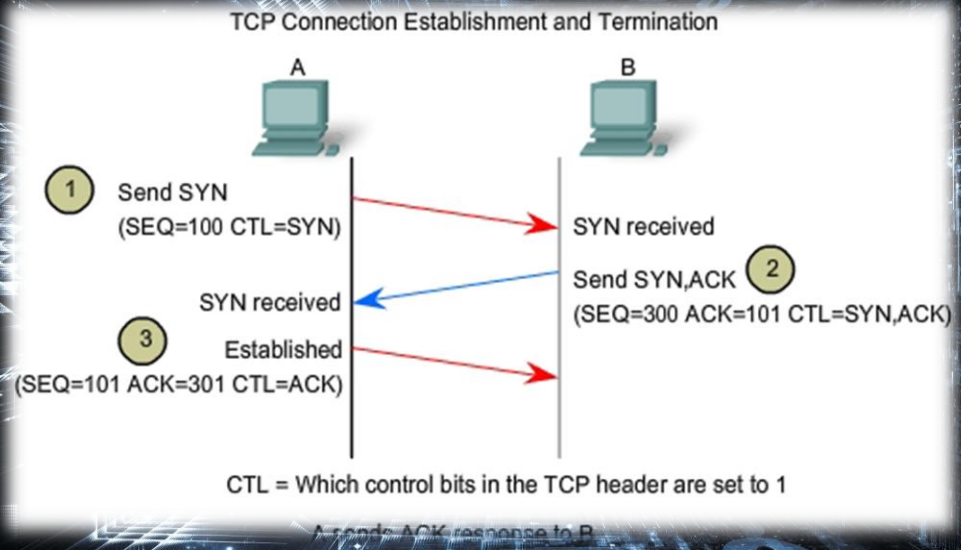


The Data Link and Network Layers

Significant Fields in an IPv6 Packet Header

- Version – contains a 4-bit binary value identifying the IP packet version; always set to 0110.
- Traffic Class – 8-bit field equivalent to the IPv4 DS field (contains 6-bit DSCP and 2-bit ECN)
- Flow Label – 20-bit field provides a special service for real-time applications
- Payload Length –16-bit field equivalent to the TL field in the IPv4 header that defines the entire packet (fragment) size, including header and optional extensions.
- Next Header – 8-bit field equivalent to the IPv4 Protocol field that indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol
- Hop Limit – 8-bit field that replaces the IPv4 TTL field
- Source Address –128-bit field that identifies the IPv6 address of the sending host
- Destination Address – 128-bit field identifies the IPv6 address of the receiving host

Module 11

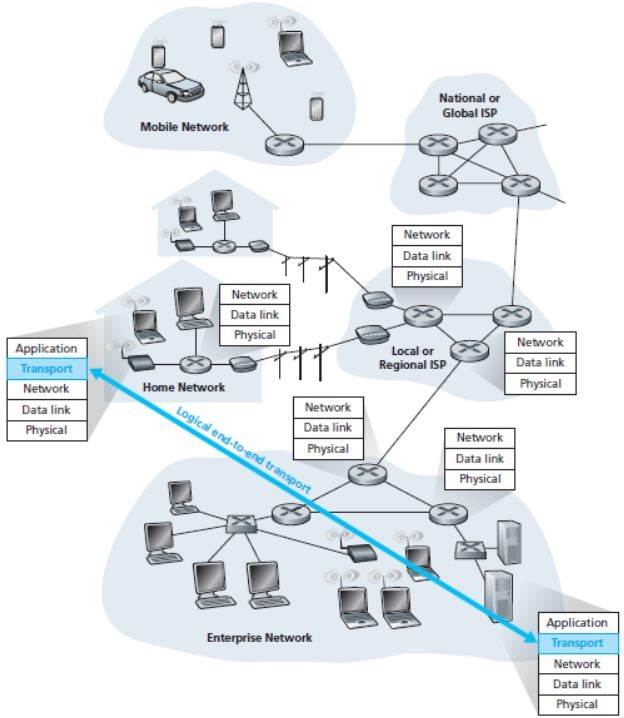


The Transport and Session Layers

The Transport and Session Layers

Transport Layer

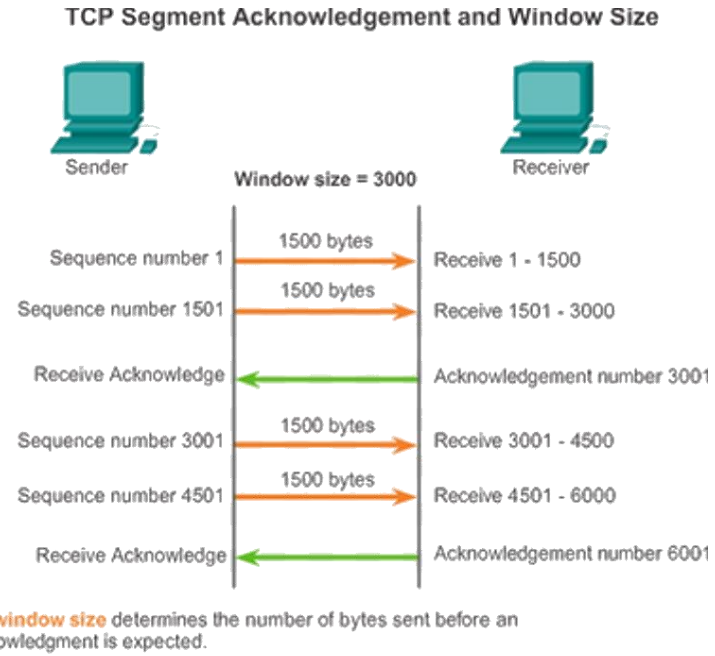
- offers peer-to-peer and end-to-end connection between two processes on remote hosts
- categorize all modules and procedures pertaining to transportation of data or data stream
- takes data from the upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to network layer for delivery
- controls the reliability of communications through flow control, segmentation, and error control



The Transport and Session Layers

Services in the Transport Layer

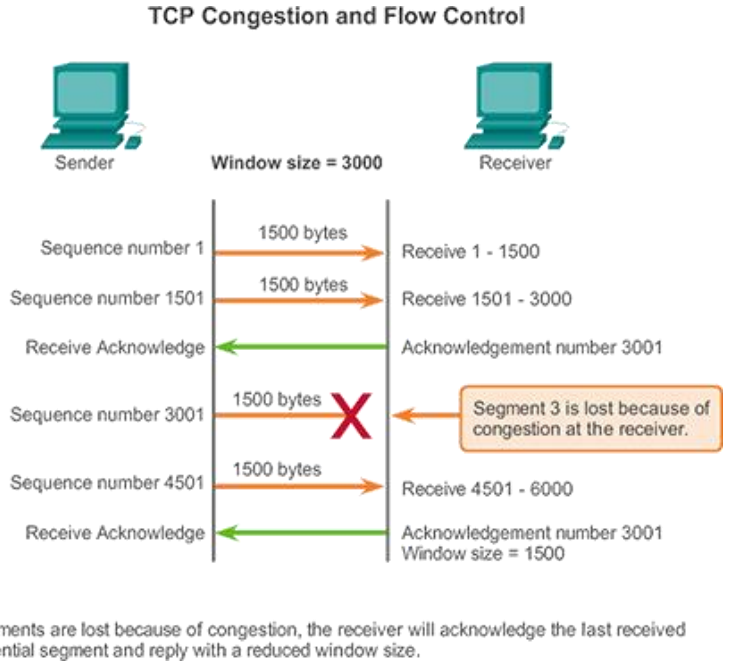
1. Connection-Oriented Communication – hosts at the end-points establish a ***handshake*** protocol to ensure a connection is robust before data is exchanged, but the repeated requests involved cause significant slowdown of network speed when defective byte streams are sent
2. Same Order Delivery – ensures that packets are always delivered in strict sequence by assigning them a number to fix any discrepancies in sequence



The Transport and Session Layers

Services in the Transport Layer

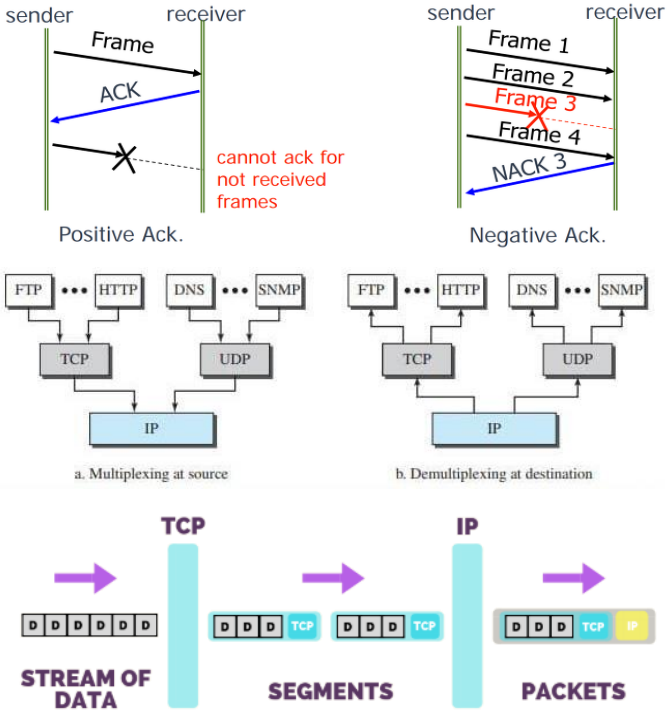
3. Data Integrity – using checksums, the data transmitted is guaranteed the same as the data received and that is not corrupt or missing
4. Flow Control – data can end up being sent faster than the speed at which the receiving device is able to buffer or process it, but this service ensures that the data is sent at a rate that is acceptable for both sides by managing data flow



The Transport and Session Layers

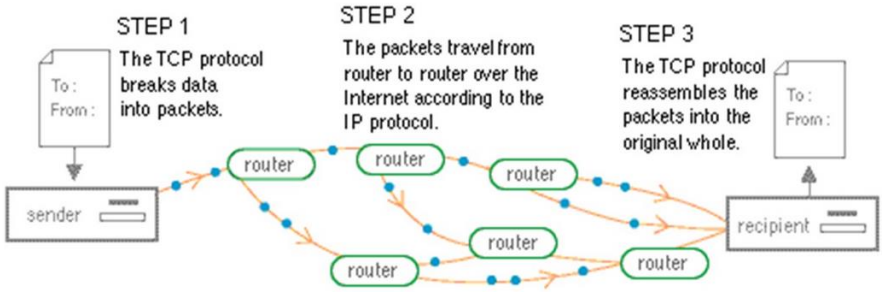
Services in the Transport Layer

5. Error Control – the transport layer can identify the symptoms of overloaded nodes and reduced flow rates and take the proper steps to remediate these issues
6. Multiplexing – allows the use of simultaneous applications over a network such as when different internet browsers are opened on the same computer
7. Byte orientation – allows applications that require to receive byte streams instead of packets



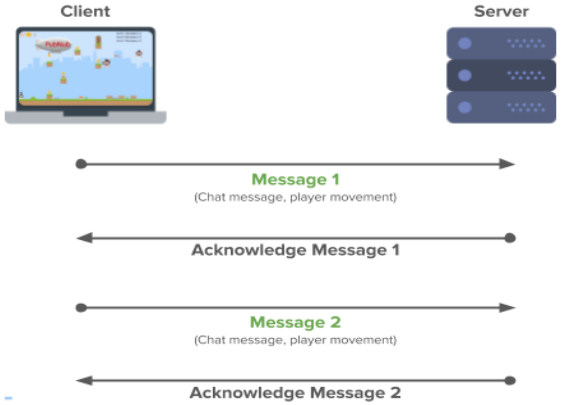
The Transport and Session Layers

Transmission Control Protocol (TCP) is the most widely used protocol for data transmission in communication network such as internet. It provides reliable communication between two hosts.



TCP Header

Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Sequence number																														
8	64	Acknowledgment number (if ACK set)																														
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size													
16	128	Checksum																Urgent pointer (if URG set)														
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																														



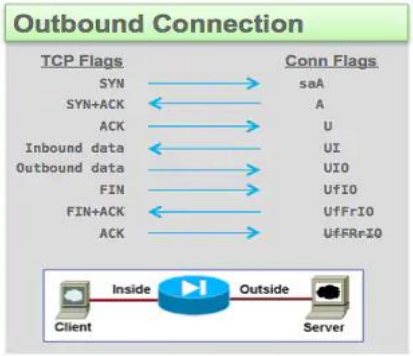
The Transport and Session Layers

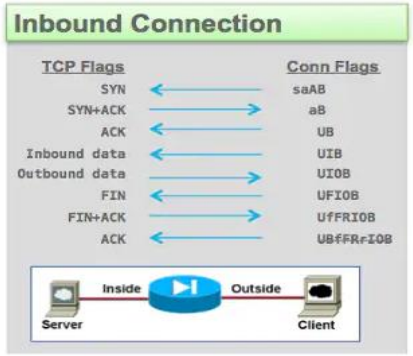
Fields in the TCP Header

- Source Port (16-bits) – identifies the source port of the sending device's application process
- Destination Port (16-bits) – identifies the destination port of the receiving device's application process
- Sequence Number (32-bits) – sequence number of data bytes of a segment in a session
- Acknowledgement Number (32-bits) – contains the next sequence number of the data byte expected when *ACK* is set, and works as acknowledgement of the previous data received
- Data Offset (4-bits) – implies both, the TCP header size (32-bit words) and the offset of data in current packet in the whole TCP segment
- Reserved (3-bits) – reserved for future use and all are set zero by default
- Flags (1-bit each) – indicate a particular state of connection or provide some additional useful information like troubleshooting or control purposes

The Transport and Session Layers

TCP Flags



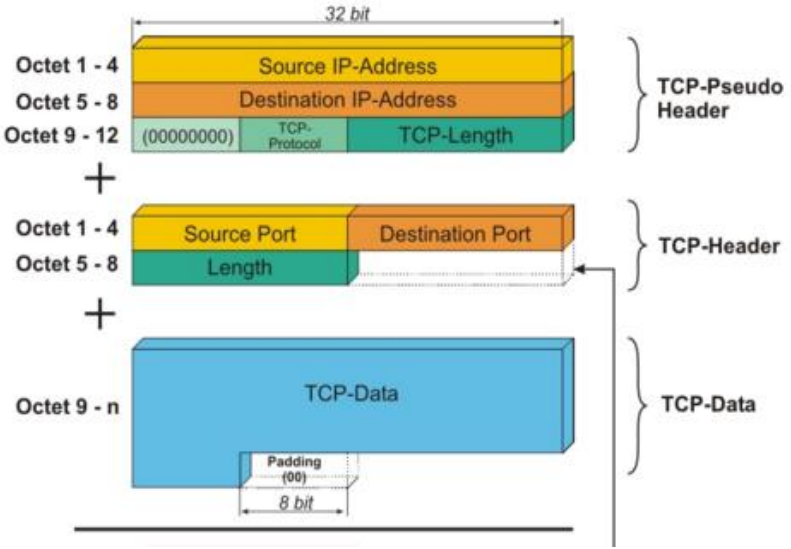


List of flags	Description	Decimal Value	Hex Value
CWR	Congestion Window Reduced (CWR) flag is set by the sending host to shows that it received a TCP segment with the ECE flag set	128	80
ECE	ECN-Echo indicate that the TCP peer is ECN capable during 3-way handshake	64	40
URG	Indicates that the urgent pointer field is significant in this segment.	32	20
ACK	Indicates that the acknowledgment field is significant in this segment.	16	10
PSH	Push function to transfer data	08	08
RST	Resets the connection.	04	04
SYN	Synchronizes the sequence numbers.	02	02
FIN	Last packet from sender which means there is no more data.	01	01
NS	Nonce Sum flag used for concealment protection.	00	00

The Transport and Session Layers

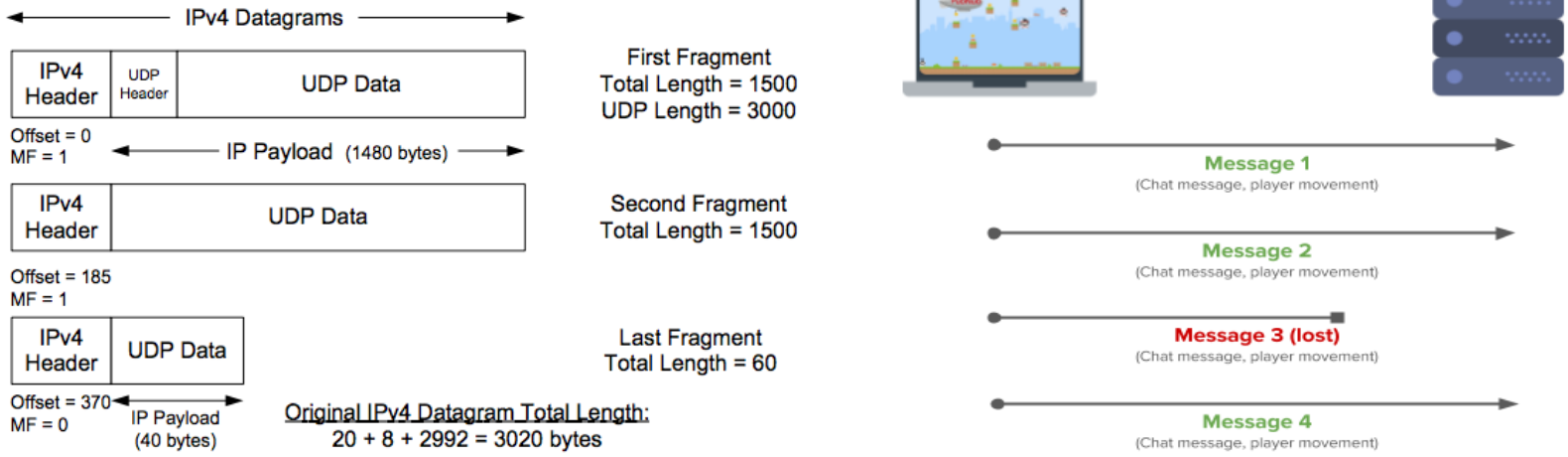
Fields in the TCP Header

- Windows Size – used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment
- Checksum – contains the checksum of *Header*, *Data* and *Pseudo Headers*
- Urgent Pointer – points to the urgent data byte if *URG* flag is set to 1
- Options – facilitates additional options which are not covered by the regular header; always described in 32-bit words (if less than 32-bit, padding is used to cover the remaining bits)



The Transport and Session Layers

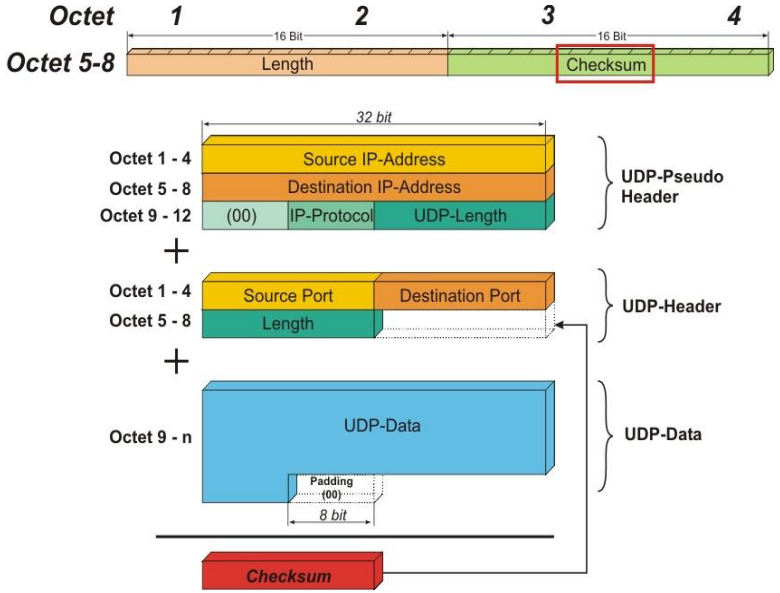
User Datagram Protocol is the simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. Though said to be an unreliable transport protocol, it uses IP services which provides best effort delivery mechanism.



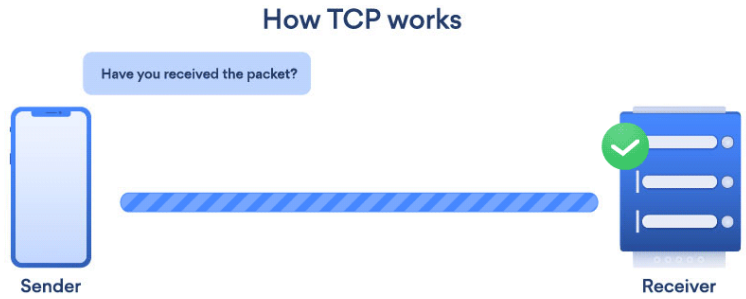
The Transport and Session Layers

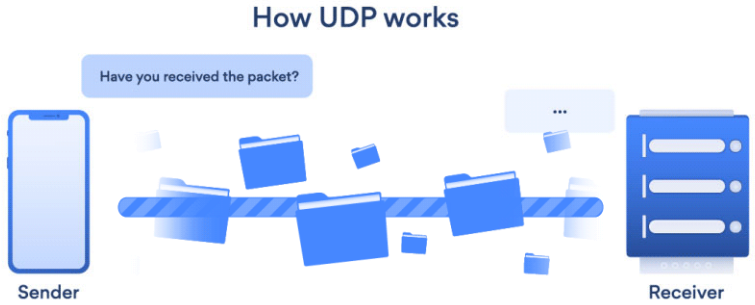
Fields in the UDP Header

- Source Port (16-bits) – used to identify the source port of the packet
- Destination Port (16-bits) – used to identify application level service on destination machine
- Length (16-bits) – specifies the entire length of UDP packet (including header)
- Checksum (16-bits) – stores the checksum value generated by the sender before sending; IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero



The Transport and Session Layers





TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

The Transport and Session Layers

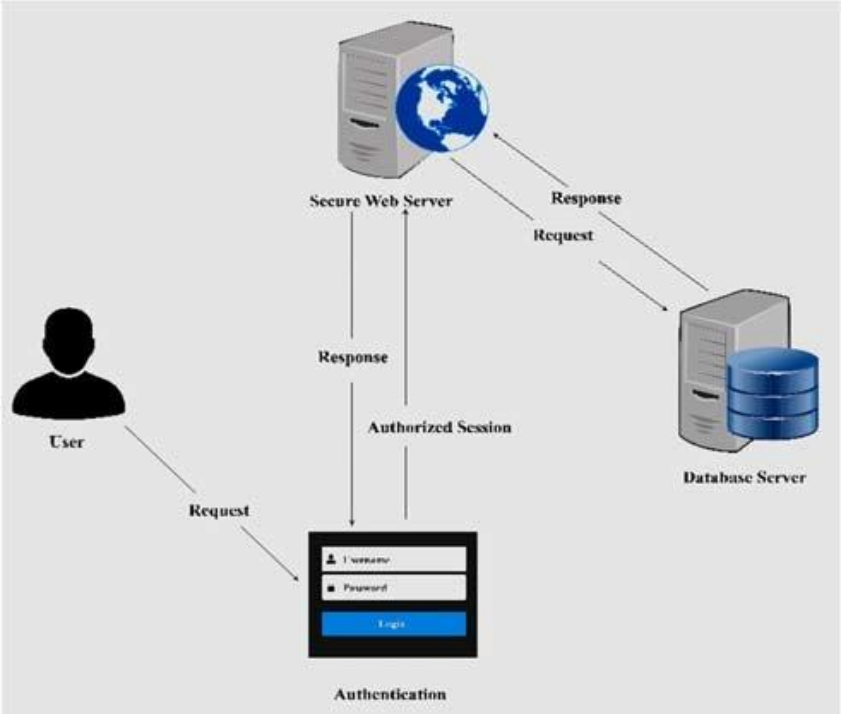
Other Transport Layer Protocols

1. Stream Control Transmission Protocol (SCTP) – ensures reliable, in-sequence transport of data and provides multi-homing support for transparent failover between redundant network paths
2. Datagram Congestion Control Protocol (DCCP) – minimal, general-purpose transport protocol that provides the establishment, maintenance and tear-down of an unreliable packet flow, as well as congestion control of that packet flow
3. Secure Sockets Layer (SSL) – encryption-based Internet security protocol for ensuring privacy, authentication, and data integrity in Internet communications
4. Transport Layer Security – successor of SSL designed to provide communications security over a computer network and all communications between their servers and web browsers

The Transport and Session Layers

Session Layer

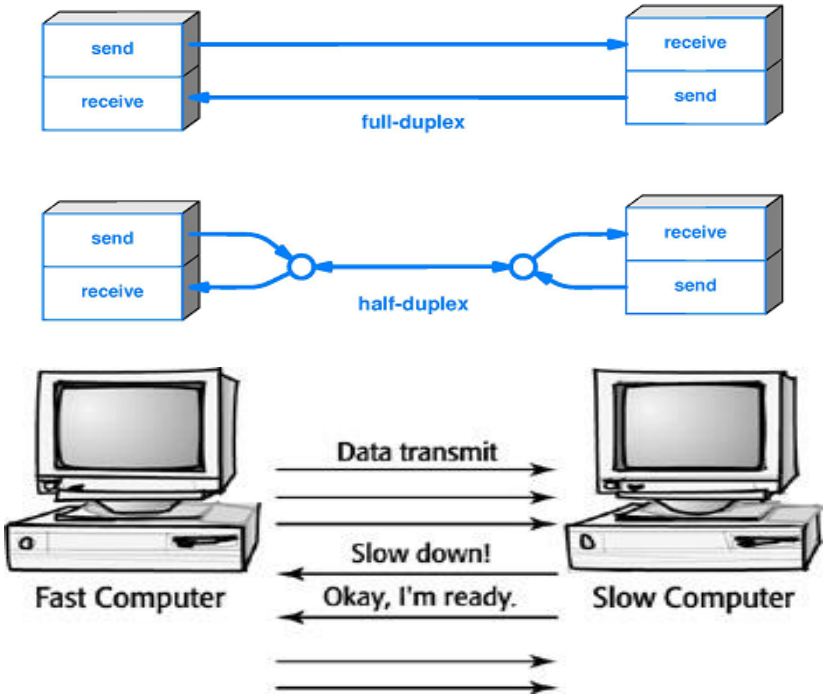
- controls the connections between multiple computers and tracks the dialogs between computers, called ***sessions***
- particularly useful for multimedia applications for which it is necessary to coordinate the timing of two or more types of data, such as voice and moving images, with a high degree of precision



The Transport and Session Layers

Services in the Session Layer

1. Dialog Control – the session layer behaves as a *dialog controller* that allows two communication machines to enter into a dialog in either half-duplex or full-duplex mode
2. Synchronization – process to add checkpoints which are referred to as ***synchronization points*** into the stream of data



The Transport and Session Layers

Services in the Session Layer

3. Token Management – through prevents the two users to simultaneously attempt access of the same critical operation by managing ***tokens***, which are basically ***session IDs***

Authentication
verifies the user

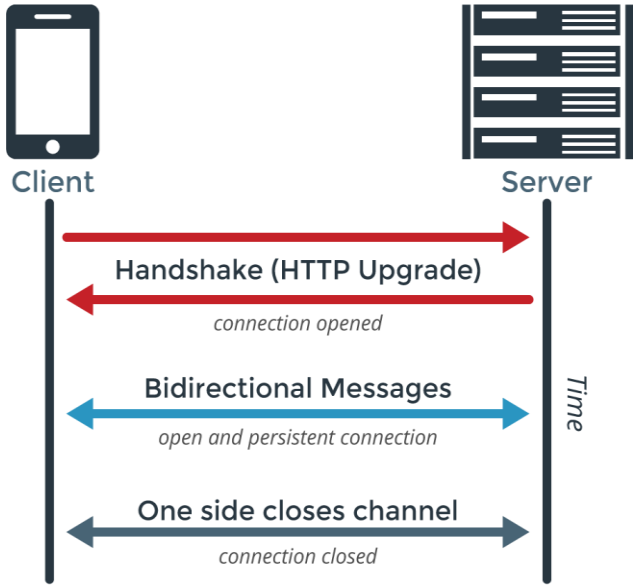
Authorization
determines user's access level

Session Restoration
checkpointing and recovery

The Transport and Session Layers

Network Layer Protocols

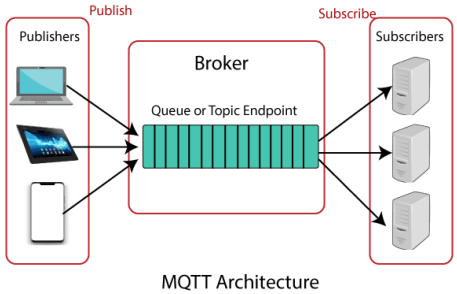
1. X.225 (or ISO 8327) – tries to recover lost connection, and refreshes one that is not used for a long period; also provides synchronization points in the stream of exchanged messages
2. Session Control Protocol (SCP) – method of creating multiple light-duty connections from a single TCP connection
3. Zone Information Protocol (ZIP) – AppleTalk protocol that coordinates the name binding process and maintains mappings of zone names to network numbers on internet routers



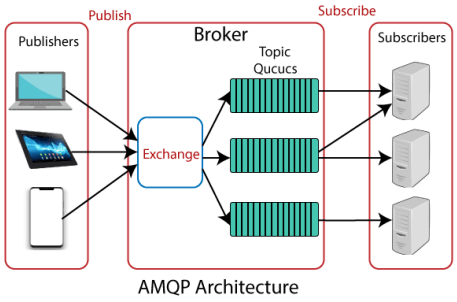
The Transport and Session Layers

Network Layer Protocols

4. Message Queue Telemetry Transport (MQTT) – protocol used for remote monitoring in IoT to collect statistics of many devices and the delivery of its infrastructure
5. Secure MQTT (SMQTT) – extended form of MQTT that uses encryption based on lightweight attribute-based encryption for a more secure data transmission
6. Advanced Message Queuing Protocol (AMQP) – designed for the financial industry, which also runs on TCP and provides a publishing/subscription architecture, but the broker is broken into two main components: ***exchange*** and ***queues***.



MQTT Architecture

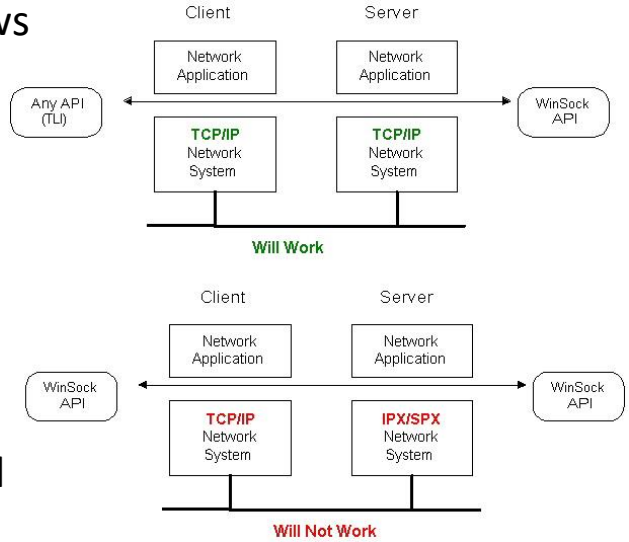


AMQP Architecture

The Transport and Session Layers

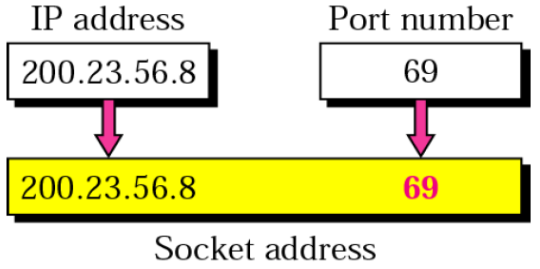
These session-layer tools are normally provided to higher layer protocols through command sets often called ***application program interfaces*** (API). Common APIs include *NetBIOS*, *TCP/IP Sockets*, and *Remote Procedure Calls* (RPCs).

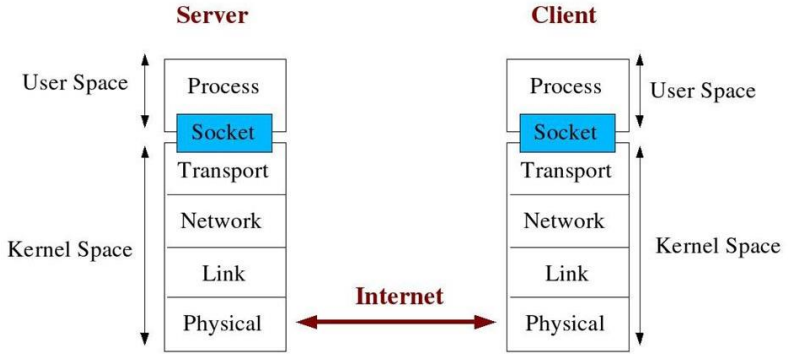
- Network Basic Input/Output System (NetBIOS) – allows applications on different computers to communicate within a local area network (LAN)
- TCP/IP Sockets – internal endpoint for sending or receiving data within a node on a computer network; combination of IP address plus port
- Remote Procedure Call (RCP) – protocol used to request a service from a program located in another computer on a network without having to understand the network's details.

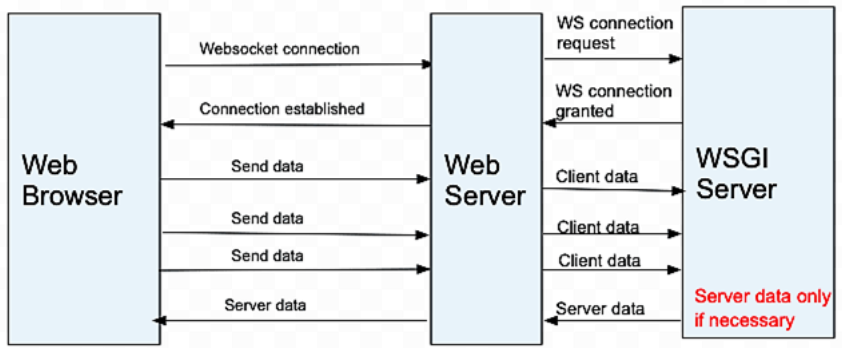


The Transport and Session Layers

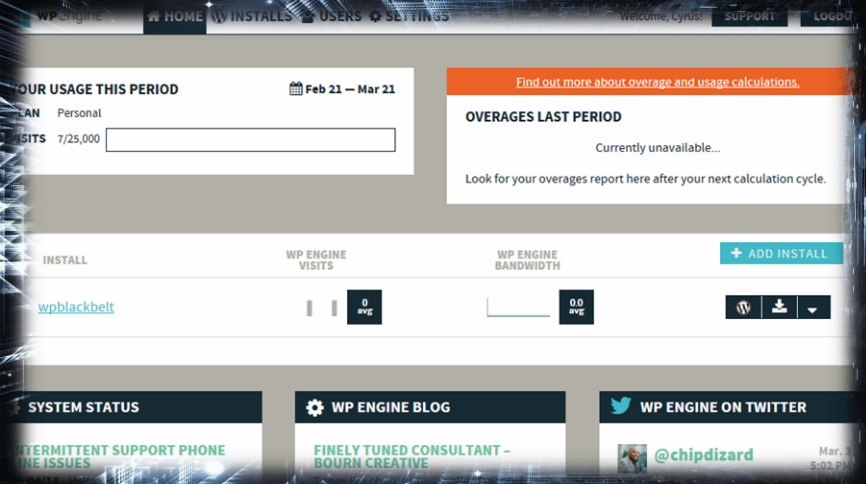
A TCP ***socket*** is an endpoint instance defined by an IP address and a ***port*** in the context of either a particular TCP connection or the listening state. ***Kernel space*** is where the *kernel* (i.e., the core of the operating system) runs and provides its services where the user is not allowed to interfere with.







Module 12



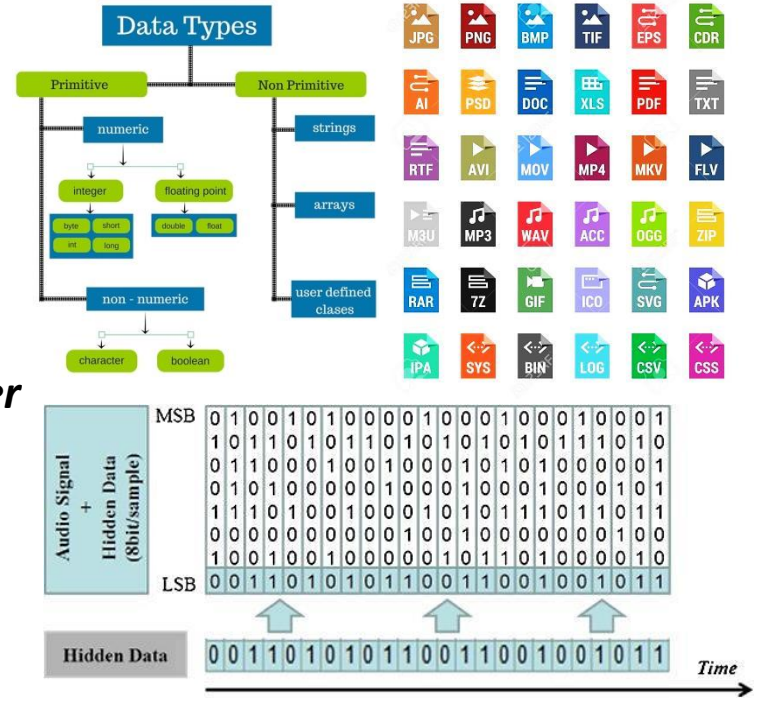
The Presentation and Application Layers

AKUNI PROJECTS

The Presentation and Application Layers

Presentation Layer

- responsible for the delivery and formatting of information to the application layer for further processing or display
- deals with syntactical differences in *data representation* within the end-user systems; hence, it's sometimes called the ***syntax layer***
- responsible for data encryption/decryption and for data compression/decompression
- many of its protocols also belong to the application layer



The Presentation and Application Layers

Services in the Presentation Layer

1. Translation – process of ensuring interoperability between encoding methods as different computers use different encoding methods
2. Encryption – process that encodes a message or file so that it can be only be read by certain people or program
3. Compression – process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less space on disk or transmission bandwidth

File extension	File type name
Text files	
Microsoft Word (Office 97-2003)	
.DOC	Word document
.DOT	Word document template
.WBK	Word backup document
Microsoft Word Open XML (introduced in Office 2007)	
.DOCX	Word document
.DOCM	Word macro-enabled document
.DOTX	Word document template
.DOCB	Word binary document
Other types of text files	
.ODT	OpenDocument text document
.PAGES	Pages document
.RTF	Rich text format file
.TXT	Plain text file
.WPD	WordPerfect document
.WPS	Microsoft Works word processor file
Data files	
.CSV	Comma-separated values file
.ODC	Office data connection file
.ODF	Apache OpenOffice math file

The Presentation and Application Layers

Data Representation refers to the form in which data is stored, processed, and transmitted. It also describes how data types are structured such as how signs are represented in numerical values and how strings are formatted (enclosed in quotes, terminated with a null, etc.).

A ***computer file*** is a computer resource for recording data discretely in a computer storage device. A ***file type*** or a *filename extension* is an identifier specified as a suffix to the name of a computer file.

Data Representation as Text

- ASCI (American Standard Code for Information Interchange)
- Unicode
- UTF-8 (8-bit Unicode Transformation Format)

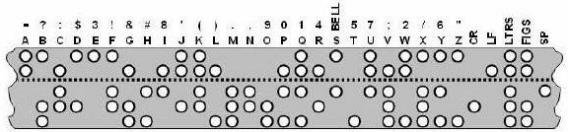
Characters:	h	o	p	e
Binary Values:	01101000	01101111	01110000	01100101

The Presentation and Application Layers

ASCII Code

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Baudot Code



Morse Code

A	·−	N	−·
B	−···	O	−−−
C	−·−·	P	·−−·
D	−··	Q	−−·−
E	·	R	·−·
F	··−·	S	···
G	−−·	T	−
H	····	U	··−
I	··	V	···−
J	·−−−	W	·−−
K	−·−	X	−··−
L	·−··	Y	−·−−
M	−−	Z	−−··
0	−−−−−	5	·····
1	·−−−−	6	−····
2	··−−−	7	−−···
3	···−−	8	−−−··
4	····−	9	−−−−·
PERIOD	·−·−·−		
COMMA	−−··−−		

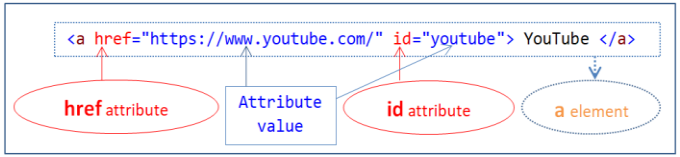
Discrete Code

2D Code

The Presentation and Application Layers

Data Representation and Syntax in Web Pages

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h *n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
...	Brackets an item in an ordered or numbered list
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink



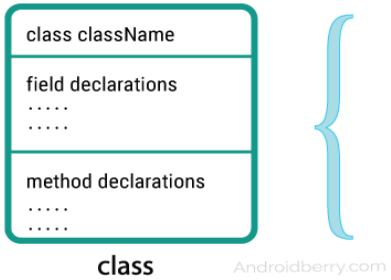

```
<HTML>
<script type="text/javascript">
/**
 * This is a multiple-
 * line comment
 */
var index = 0;
var arr = [];

function push(elem) {
    // This comment may span only this line
    arr[index++] = elem;
}
</script>
</HTML>
```

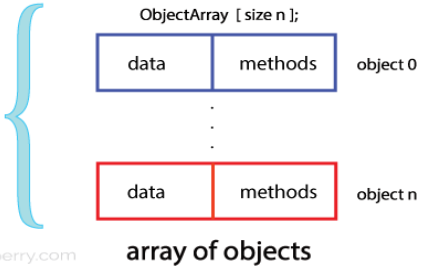
XML

```
<empinfo>
  <employees>
    <employee>
      <name>James Kirk</name>
      <age>40</age>
    </employee>
    <employee>
      <name>Jean-Luc Picard</name>
      <age>45</age>
    </employee>
    <employee>
      <name>Wesley Crusher</name>
      <age>27</age>
    </employee>
  </employees>
</empinfo>
```

JSON

```
{ "empinfo" :
  {
    "employees" : [
    {
      "name" : "James Kirk",
      "age" : 40,
    },
    {
      "name" : "Jean-Luc Picard",
      "age" : 45,
    },
    {
      "name" : "Wesley Crusher",
      "age" : 27,
    }
              ]
  }
}
```





Data Type
byte
sbyte
short
ushort
int
uint
long
ulong
float
double
decimal
char
string
bool
object

The Presentation and Application Layers

Audio File Formats

Uncompressed Formats

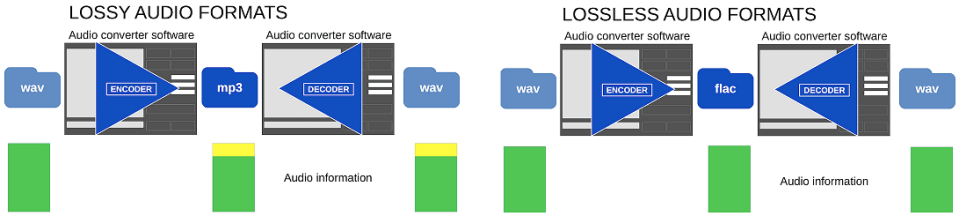
- **WAV** (Waveform)
- **AIFF** (Audio Interchange File Format)

Compressed, Lossless Formats

- **FLAC** (Free Lossless Audio Codec)
- **ALAC** (Apple Lossless Audio Codec)

Compressed, Lossy Formats

- **MP3** (MPEG Audio Layer III)
- **AAC** (Advanced Audio Coding)
- **M4A** (Audio Only MPEG-4 file)
- **Vorbis** (a.k.a. Ogg Vorbis)
- **WMA** (Windows Media Audio)



AudioDirector Produce Formats			
Format	Bit Rate	Sample Rate	File Size
WAV (PCM)	1536 kbps	48.0kHz	43.4MB
FLAC (FLAC)	759kbps	48.0kHz	21.5MB
APE (Monkey's Audio)	670kbps	48.0kHz	18.9MB
WMA (WMA)	128kbps	48.0kHz	3.65MB
MP3 (MPEG)	128kbps	48.0kHz	3.62MB
M4A (AAC)	127kbps	48.0kHz	3.58MB

The Presentation and Application Layers

Image File Formats

Vector Formats

- **AI** (Adobe Illustration Program)
- **EPS** (Encapsulated Postscriped File)
- **PDF** (Portable Document Format)

Raster Formats

- **PNG** (Portable Network Graphics)
- **JPG** (Joint Photographic Experts Group)
- **TIFF** (Tagged Image File Format)
- **GIF** (Graphics Interchange Format)
- **PSD** (Adobe Photoshop Program)

IMAGE FORMAT	AVAILABLE COLORS	COMPRESSION	FILE SIZE	BEST FOR
RAW	Billions	No	Very big (<10MB)	Editing
JPEG	16,1 million	Lossy	Small (<1MB)	Websites and storage
GIF	256	Lossless	Small (<1MB)	Animation
PNG	16,1 million + transparency	Lossless	Big (<3MB)	Websites, editing, storage
TIFF	Variable	Variable	Big (<3MB)	Editing and printing
BMP	Variable	Lossless	Big (<3MB)	-

The Presentation and Application Layers

Video File Formats

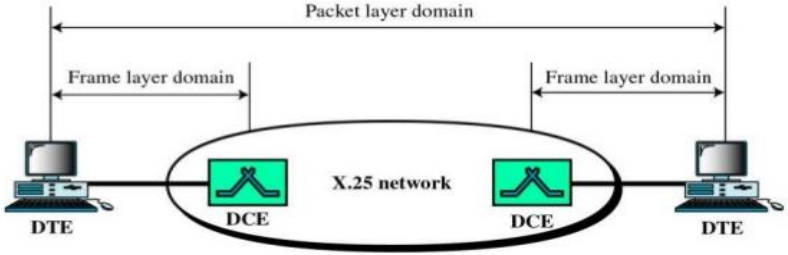
- **ASF** (Advanced System Format)
- **AVI** (Audio Video Interleave)
- **FLV** (Flash Video)
- **M4V** (iTunes Video)
- **MKV** (Matroska Video)
- **MP4** (MPEG-4)
- **MOV** (Apple QuickTime)
- **MPG** (Moving Picture Experts Group)
- **SWF** (Shockwave Flash)
- **VOB** (DVD Video Object)
- **WMV** (Windows Media Video)

	Category	H.264	H.265
General	Names	MPEG 4 Part 10 AVC (Introduced in 2004)	MPEG-H, HEVC, Part 2 (Approved in Jan 2013)
	Industry adoption	Dominant and accepted video codec for Terrestrial, Cable, Satellite and IPTV broadcast. (ATSC/DVB/ISDB) Widely used across Blu-Ray, security systems, videoconferencing , mobile video, media players, video chat etc.	Implementation demonstration across NAB, IBC and other events starting 2012 from companies e.g. ATEME, Broadcom, Thomson , Harmonic (Cisco), Ericsson, Qualcomm etc.. Increased R&D across Encoder/Decoder /CE vendors for software and hardware based solutions
	Key Improvement	• 40-50% bit rate reduction compared to MPEG -2 • Led the growth of HD content delivery for Broadcast and Online	• 40-50% the bit rate reduction at the same visual quality compared to H.264 • Potential to realize UHD, 2K, 4K for Broadcast and Online (OTT)
	Progression	Successor to MPEG-2 Part	Successor to MPEG 4 AVC, H.264
TECHNICAL	Compression Model	Hybrid spatial-temporal prediction model • Flexible partition of Macro Block (MB) , sub MB for motion estimation • Intra Prediction (extrapolate already decoded neighboring pixels for prediction) • Introduced multi-view extension • 9 directional modes for intra prediction • Macro Blocks structure with maximum size of 16x16 • Entropy coding is CABAC and CAVLC	Enhanced Hybrid spatial-temporal prediction model • Flexible partitioning, introduces Coding Tree Units (Coding, Prediction and Transform Units -CU, PU, TU) • 35 directional modes for intra prediction • Superior parallel processing architecture, enhancements in multi-view coding extension • CTU supporting larger block structure (64x64) with more variable sub partition structures • Entropy coding is only CABAC
	Specification	Support Up to 4K (4,096×2,304) Supports up to 59.94 fps 21 profiles ; 17 levels	Up to 8K UHDTV (8192×4320) Supports up to 300 fps 3 approved profiles, draft for additional 5 ; 13 levels
	Drawbacks	Unrealistic for UHD content delivery due to high bit rate requirements. Frame rate support restricted to 59.94	Computationally expensive (~ 300 % +) due to larger prediction units and expensive Motion Estimation (Intra prediction with more nodes, asymmetric partitions in Inter Prediction).

The Presentation and Application Layers

Presentation Layer Protocols

1. Secure Shell (SSH) – protocol for secure remote login between computers
2. Internet Message Access Protocol (IMAP) – used by clients to retrieve email messages from a mail server over a TCP/IP connection
3. X.25 Packet Assembler/Disassembler (PAD) – defines how DTEs communicate with the network and how packets are sent over that network using DCEs



The Presentation and Application Layers

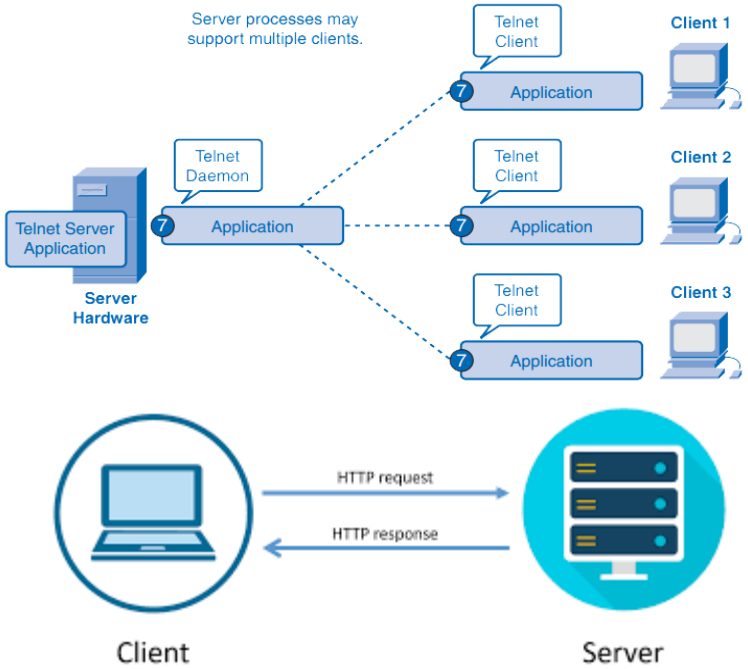
Presentation Layer Protocols

4. Network Data Representation (NDR) – implementation of the presentation layer in the OSI model
5. eXternal Data Representation (XDR) – specification protocol for a standard representation of various data types
6. Lightweight Presentation Protocol (LPP) – describes an approach for providing "stream-lined" support of OSI application services on top of TCP/IP-based network for some constrained environments
7. Apple Filing Protocol (AFP)
8. Independent Computing Architecture (ICA)
9. NetWare Core Protocol (NCP)
10. Tox Protocol

The Presentation and Application Layers

Application Layer

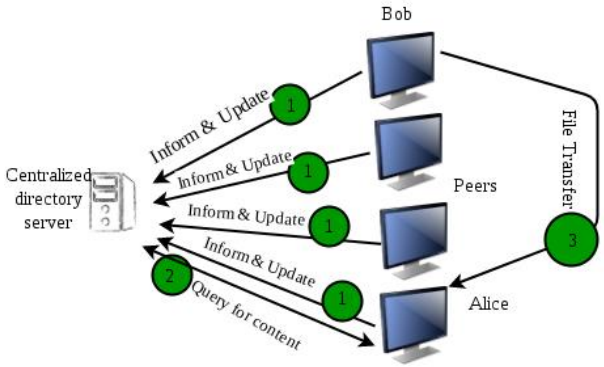
- primarily intended for interacting with user and user applications
- specifies the shared communications protocols and interface methods used by hosts in a communications network
- contains the communications protocols and interface methods used in process-to-process communications across an Internet Protocol (IP) computer network

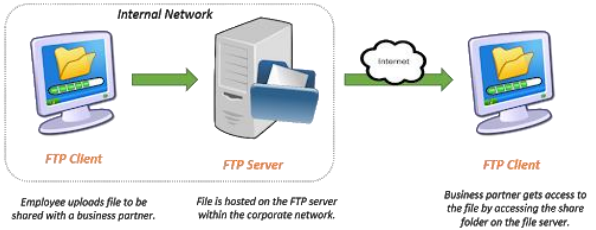


The Presentation and Application Layers

Services in the Application Layer

1. Directory Services – mapping between name and its value, which can be variable value or fixed
2. File Services – include sharing and transferring files over the network
   - ***File Sharing*** – users can upload a file to a specific server or to its own computer and provide access to intended users
   - ***File Transfer*** – users can copy or move file from one computer to another or to multiple computers through the network that enables them to locate other users in the network and transfer files.





The Presentation and Application Layers

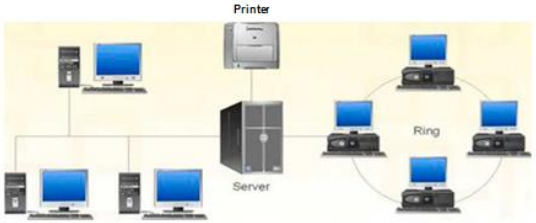
Services in the Application Layer

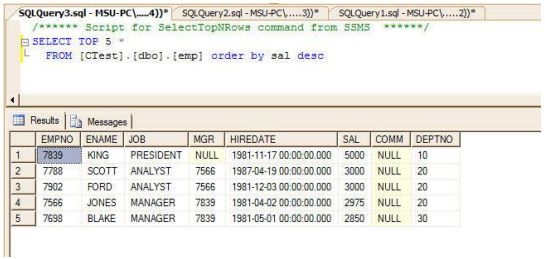
3. Communication Services
   - ***Email*** – the basis of today's internet features; all its users are provided with unique IDs and users can send an email through an email server
   - ***Social Networking*** –people can use it to find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos
   - ***Internet Chat*** – provides instant text or multimedia transfer services between two hosts
   - ***Discussion Boards*** – provide a mechanism to connect multiple peoples with same interests so that users can put queries, questions, suggestions etc. which can be seen by all other users and responded to
   - ***Remote Access*** – enables user to access the data residing on the remote computer; this feature is known as *Remote desktop*, which can be done via some remote device

The Presentation and Application Layers

Services in the Application Layer

4. Application Services – providing network based services to the users such as web services, database managing, and resource sharing
   - ***Resource Sharing*** – to use resources (servers, printers, and storage media , etc.) efficiently and economically, network provides a mean to share them
   - ***Databases*** – store data, processes it, and enables the users to retrieve it efficiently by using queries to help organizations make decisions based on statistics
   - ***Web Services*** (WWW) – used to connect to the internet, and access files and services from the internet servers

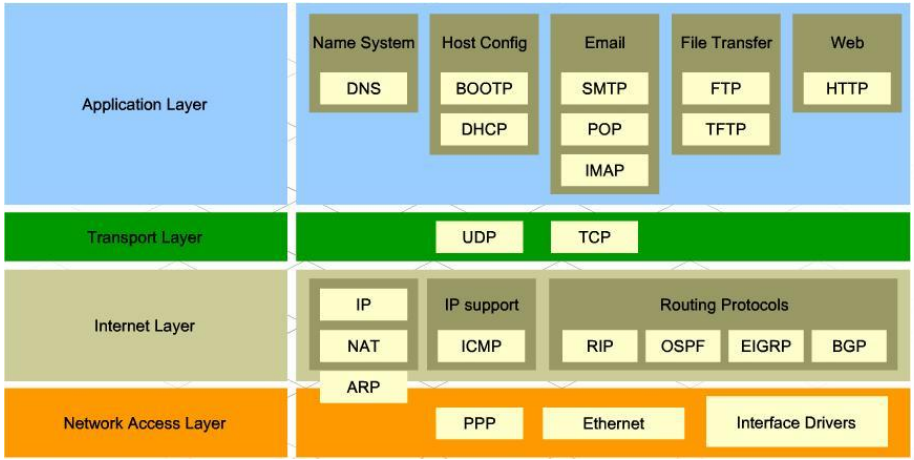




The Presentation and Application Layers

Categories of Application Layer Protocols

1. Protocols which are used by users.
2. Protocols which help and support protocols used by users.



Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name Server (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP
123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP

The Presentation and Application Layers

Common Application Layer Protocols

1. Hyper Text Transfer Protocol (HTTP) – works on client server model, being the foundation of WWW; hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents
2. Domain Name System (DNS) – works on Client Server model using UDP protocol for transport layer communication; the DNS server is configured with FQDN and email addresses mapped with their respective IP addresses
3. Simple Mail Transfer Protocol (SMTP) – used to transfer electronic mail from one user to another by means of email client software (User Agents) the user is using
4. Post Office Protocol version 3 (POP 3) – a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server

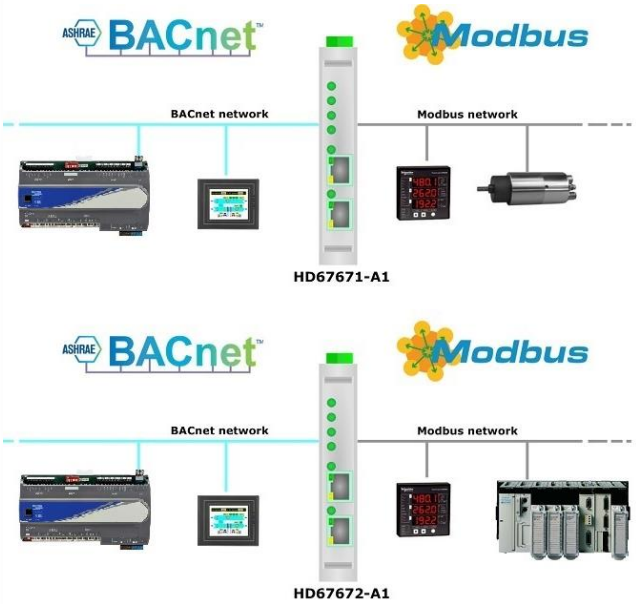
The Presentation and Application Layers

Common Application Layer Protocols

5. File Transfer Protocol (FTP) – standard network protocol used for the transfer of computer files between a client and server on a computer network
6. Telnet – client-server protocol that can be used to open a command line on a remote computer, typically a server
7. Internet Relay Chat (IRC) – protocol that facilitates communication in text form
8. Internet Protocol Security (IPsec) – secure network protocol suite that authenticates and encrypts the packets of data for security purposes
9. Dynamic Host Configuration Protocol (DHCP) – used on IP networks to dynamically assign an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks

The Presentation and Application Layers

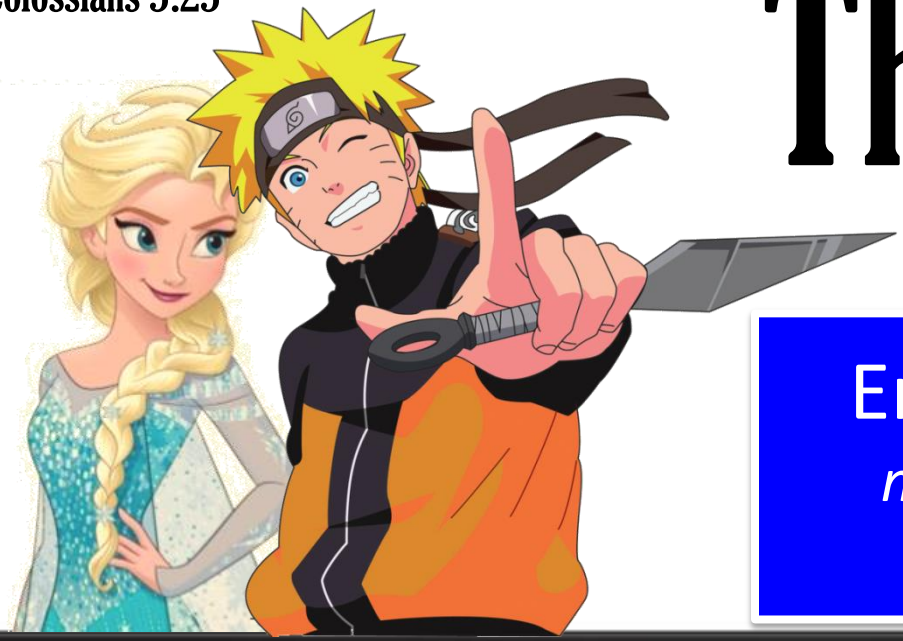
BMS and IoT Protocols



	IoT Stack		Web Stack
TCP/IP Model	IoT Applications	Device Management	Web Applications
Data Format	Binary, JSON, CBOR		HTML, XML, JSON
Application Layer	CoAP, MQTT, XMPP, AMQP		HTTP, DHCP, DNS, TLS/SSL
Transport Layer	UDP, DTLS		TCP, UDP
Internet Layer	IPv6/IP Routing 6LoWPAN		IPv6, IPv4, IPSec
Network/Link Layer	IEEE 802.15.4 MAC IEEE 802.15.4 PHY / Physical Radio		Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN (IEEE 802.11), Wi-Fi

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