NETWORKING CONCEPTS

Bhupendra Pratap Singh

ACTS, CDAC, Pune

THE OSI MODEL

- Established in 1947, **the International Standards Organization** (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all **aspects of network communications is the Open Systems Interconnection (OSI) model**. It was first introduced in the late 1970s.

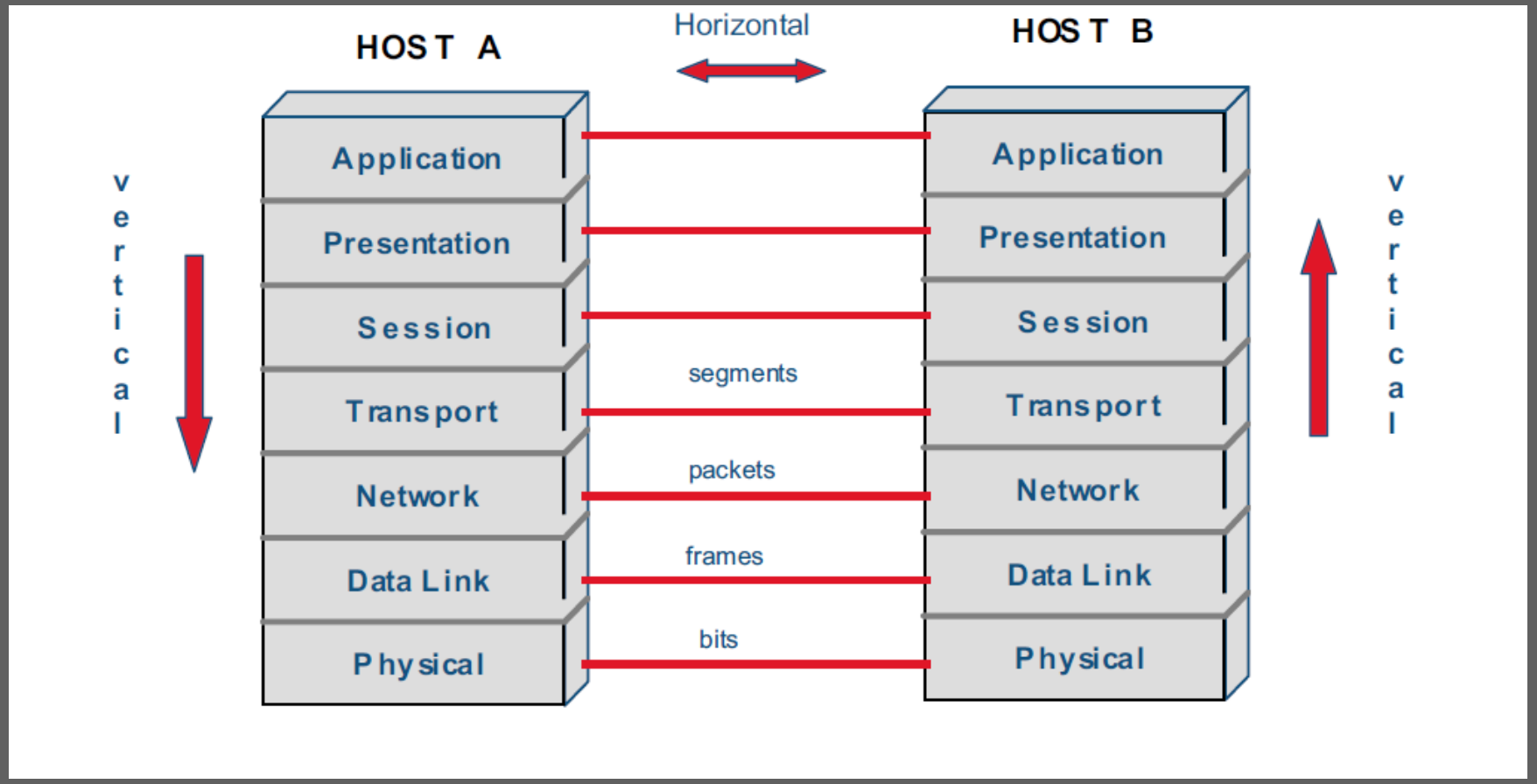
NOTE

- ISO is the organization.
- OSI is the model.

WHY OSI MODEL??

To guide vendors and developers so that digital communication products and software programs they create will interoperate.

SEVEN LAYERS OF OSI MODEL



APPLICATION LAYER

- This is the topmost layer in the seven OSI Layers.
- This is the layer that the end-user (can be a computer programmer, or a regular PC user) is actually interacting with.
- This layer allows access to network resources.
- Contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web.

PRESENTATION LAYER

- This is the layer in which the operating system operates with the data.
- Main functions of this layers includes
  - translation,
  - encryption
  - compression of data

SESSION LAYER

- Maintaining proper communication by establishing, managing and terminating sessions between two computers.
- For instance - when ever a user login to any banking website, a session is created and maintained for a specific period, if user doesn't logout, session automatically gets discarded/ended.

TRANSPORT LAYER

- The transport layer is responsible for the delivery of a message from one process to another.
- Segmentation and reassembly
- Connection control
- Flow control (how much information should be sent at a time).
- Error control
- multiplexing and demultiplexing of data among
- various applications, based on port numbers.
- additional reliability -- retransmission, reordering
- deduplication

NETWORK LAYER

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Logical addressing (IP based)
- Routing

DATA LINK LAYER

- This layer is responsible for organizing bits into frames and ensuring **hop to hop** delivery.
- Mapping of logical address(IP) -- ARP, RARP
- Error control -- checksum, Flow control, Access control
- The Data Link Layer is logically divided into two sublayers, The Media Access Control (MAC) Sublayer and the Logical Link Control (LLC) Sublayer.

CONT..

- Media Access Control (MAC) Sublayer determines the physical addressing of the hosts. The MAC sub-layer maintains MAC addresses (physical device addresses) for communicating with other devices on the network.
- MAC Addresses are also known as Physical addresses, Layer 2 addresses, or Hardware addresses.
- The Logical Link Control sublayer is responsible for synchronizing frames, error checking, and flow control.

PHYSICAL LAYER

- Concerned with the physical characteristics of electrical or optical signaling techniques which includes the voltage of the electrical current used to transport the signal.
- The media type (Twisted Pair, Coaxial Cable, Optical Fiber etc), impedance characteristics, physical shape of the connector, Synchronization etc.
- The Physical Layer is limited to the processes needed to place the communication signals over the media, and to receive signals coming from that media.
- Topology (star, bus, ring, mesh etc.)

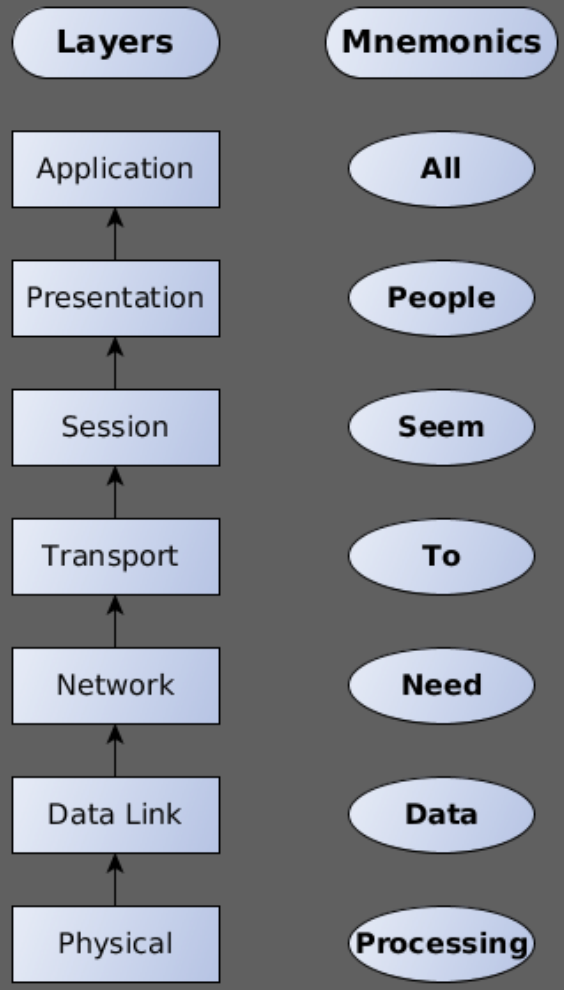
PROTOCOL DATA UNITS

- **Physical layer** - bits (raw/binary data)
- **Data Link layer** - frames
- **Network Layer** - packets or ip datagrams
- **Transport layer** - segments, user datagrams
- **Application/session/presentation** - message/payload

Application	Away
Presentation	Pizza
Session	Sausage
Transport	Throw
Network	Not
Data Link	Do
Physical	Please

A SIMPLE MNEMONIC FOR MEMORIZING THE NAMES OF OSI LAYERS

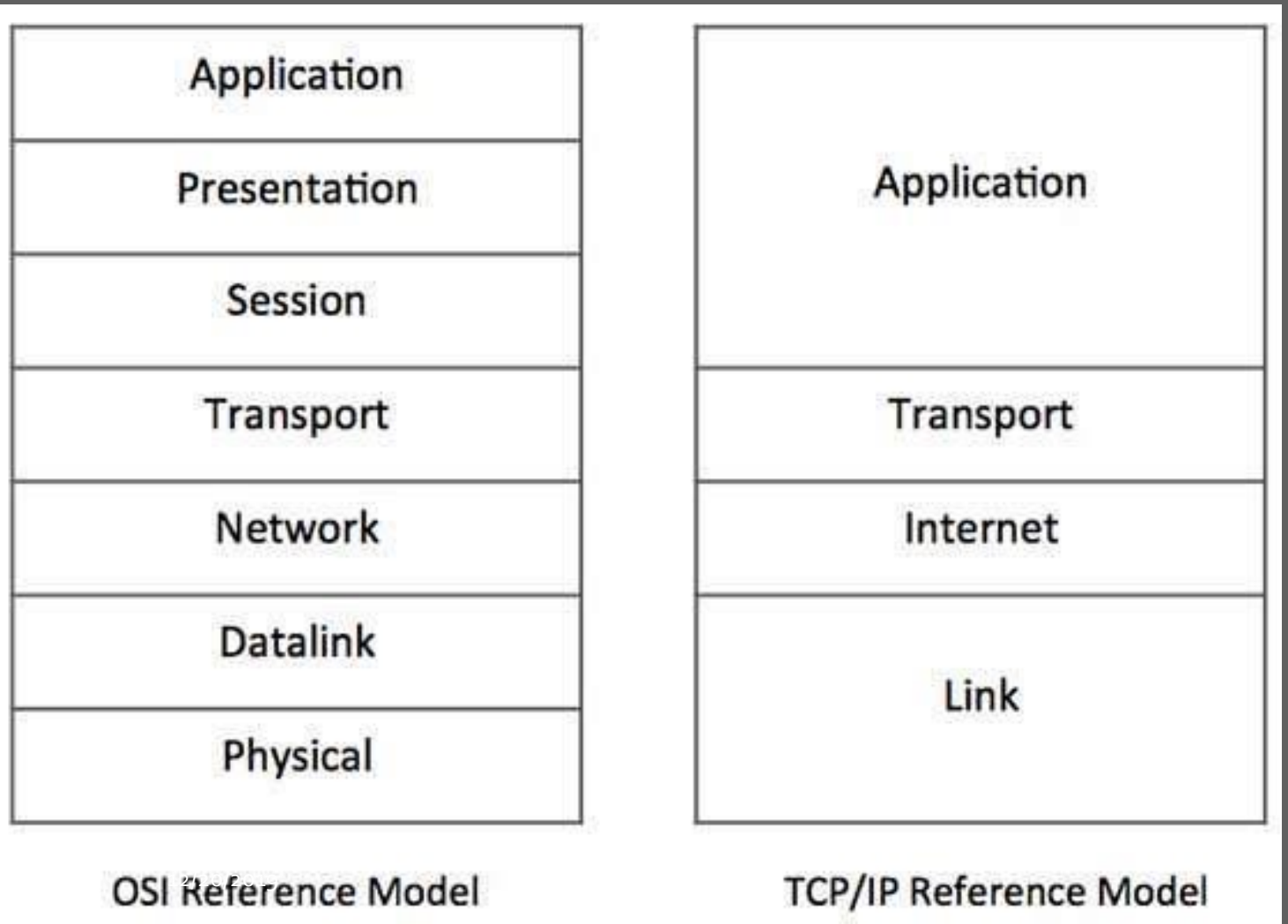
All People Seem To Need Data Processing



DIFFERENT LEVEL OF ADDRESSING

- Physical addressing -- MAC address
- Logical addressing -- IP address
- Port addressing -- transport layer

TCP/IP REFERENCE MODEL



Note : Link layer is also referred as Network Access Layer/Network Interface at many places.

WHICH CAME FIRST OSI OR TCP/IP ??

- **The TCP/IP model,** which is realistically the Internet Model, came into existence about **10 years before the OSI model.**
- Development of the OSI model began in the late 1970s, and the model was published in 1984.
- It can be said that the OSI model prescribes and TCP/IP model describes.

MAC ADDRESS

- Media Access Control (MAC address or Layer 2 addresses or physical address or hardware address) addresses are 48 bit (six bytes) binary addresses represented in hexadecimals.
- MAC addresses are typically locally specific, means that the scope of a MAC address is limited within a Local Area Network (LAN).
- For example, the MAC address 10101010.11110000.11000001.11100010.01110111.01010001 in binary can be represented as shorter hexadecimal equivalent AA.F0.C1.E2.77.51.

CONT..

- Every network card manufacturer gets a universally unique 3-byte code called the Organizationally Unique Identifier (OUI). Manufacturers agree to give all NICs a MAC address that begins with the assigned OUI. The manufacturer then assigns a unique value for the last 3 bytes, which ensures that every MAC address is globally unique.

TCP PROTOCOL

- TCP is connection-oriented, which means that, before data is sent, a connection between two hosts must be established. The process used to establish a TCP connection is known as the three-way handshake.
- It is known to provide reliable and error-free communication between end systems.
- It performs sequencing and segmentation of data.
- It is stream oriented, full – duplex, bi-directional protocol.
- It also has acknowledgment feature and controls the flow of the data through flow control mechanism.
- BYTE streaming.

ADDRESSES – IPV4

32 bit IP address broken into 4 octets or 8 bit fields (0-255 value in decimal notation)

IP Address Classes and Representation

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

Class – D : Reserved for Multicasting while Class –E is reserved for R&D purposes

IPV4 PRIVATE ADDRESS SPACE

- Some address blocks in the unicast space were set aside and designated as private addresses. The private address space was intended for networks that are not connected to the public Internet. The following addresses are specific in RFC 1918 as part of the IPv4 private address space:

- 10.0.0.0 to 10.255.255.255 Class - A
- 172.16.0.0 to 172.31.255.255 Class - B
- 192.168.0.0 to 192.168.255.255 Class - C

SUBNET MASK

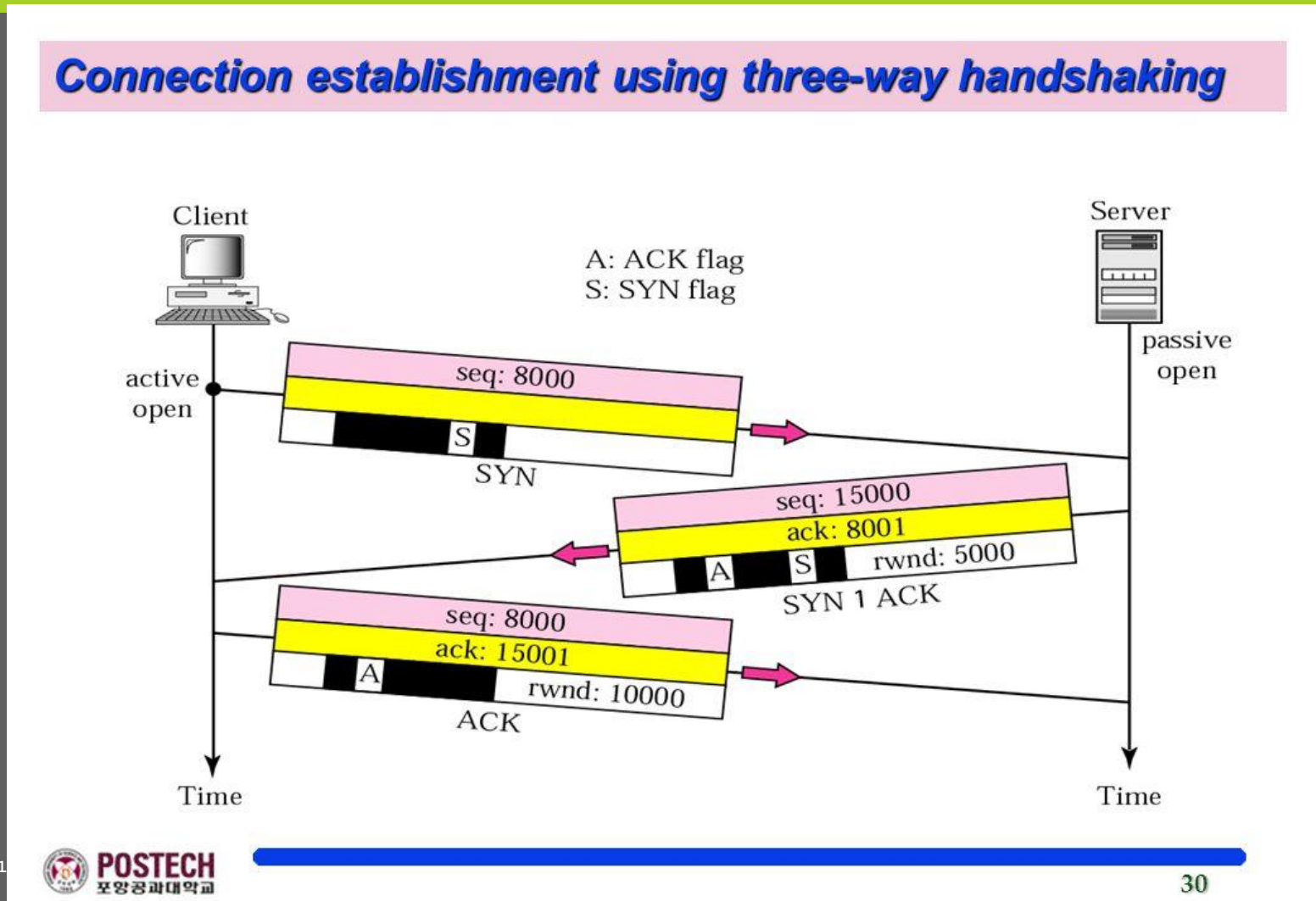
- An address the accompanies an IP address that indicates which portion of the IP address is the network ID and which portion of the IP address is host ID.

Class	Default subnet mask	No. of networks	No. of hosts per network
A	255.0.0.0	256	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,777,216	126

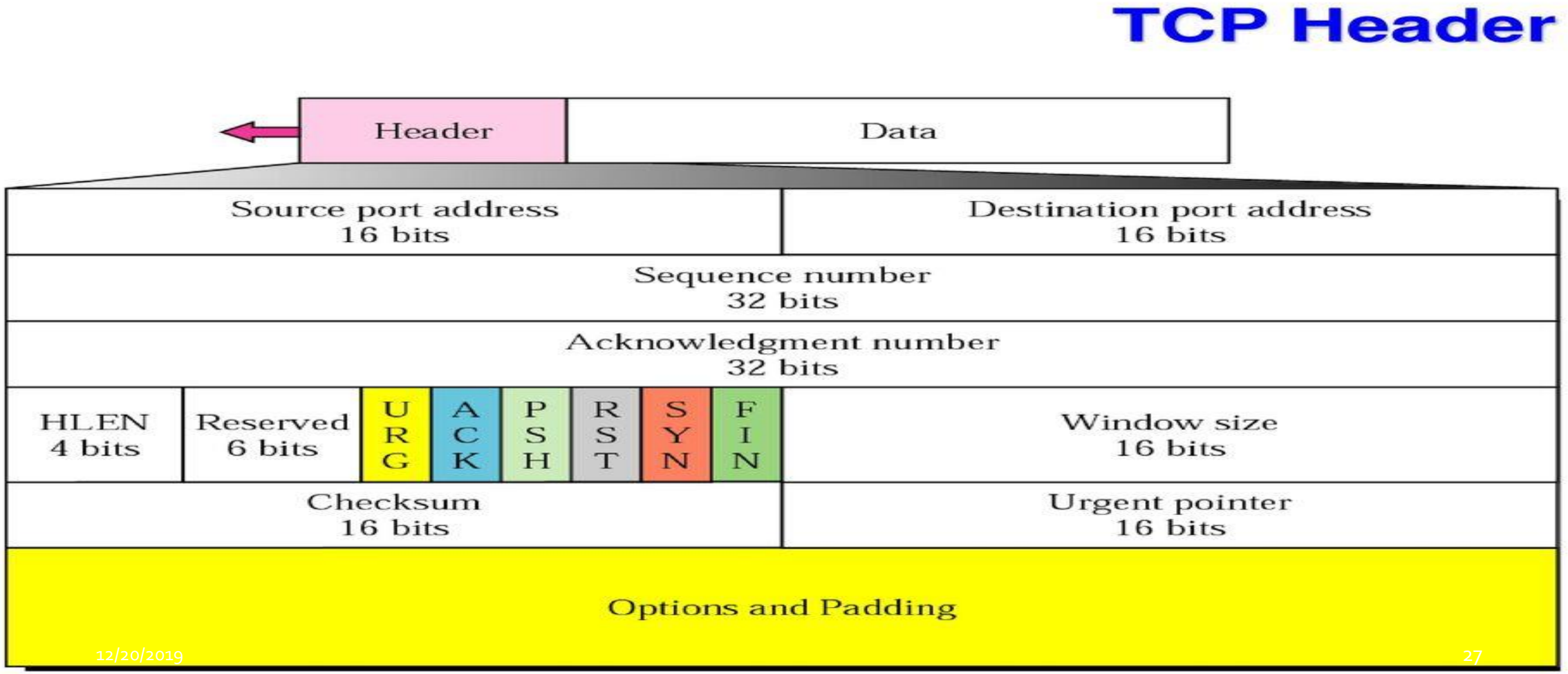
CIDR (CLASSLESS INTERDOMAIN ROUTING)

- In order to reduce the wastage of IP addresses a new concept of **Classless Inter-Domain Routing** is introduced.
- Representation: It is as also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.
- a . b . c . d / n
- Where, n is number of bits that are present in Block Id / Network Id.
- Example:
- 192.168.1.0/28
- If the Block size is 28 then, Host Id will contain 4 bits and Network will contain 32 – 4 = 28 bits.

TCP -THREE WAY HANDSHAKING



TCP HEADER (MIN 20 BYTES, MAX 60 BYTES)



CONT…

- **Source port** – the port number of the application on the host sending the data.
- **Destination port** – the port number of the application on the host receiving the data.
- **Sequence number** – used to identify each byte of data.
- **Acknowledgment number** – the next sequence number that the receiver is expecting.
- **HLEN (Header Length) – (**Scale of four**)** (Any value present inside will be multiplied by 4). {0101 to 1111}
- RESERVED - Reserved for future use. Must be zero

URG – (URGENT FLAG)

- This flag is used to identify incoming data as 'urgent'. Such incoming segments do not have to wait until the previous segments are consumed by the receiving end but are sent directly and processed immediately.
- This flag is set to 1 when it is used.

ACK (ACKNOWLEDGEMENT FLAG)

- The Acknowledgement flag is used to acknowledge the successful receipt of packets.
- ACK is set to 1 when we look for acknowledgements.

PSH (PUSH FLAG)

- The Push flag, like the Urgent flag, exists to ensure that the data is given the priority (that it deserves) and is processed at the sending or receiving end.
- When a host sends its data, it is temporarily queued in the TCP buffer, a special area in the memory, until the segment has reached a certain size and is then sent to the receiver.
- This design guarantees that the data transfer is as efficient as possible, without waisting time and bandwidth by creating multiple segments, but combining them into one or more larger ones.

CONT...

- When the segment arrives at the receiving end, it is placed in the TCP incoming buffer before it is passed onto the application layer. The data queued in the incoming buffer will remain there until the other segments arrive and, once this is complete, the data is passed to the application layer that's waiting for it.

CONT…

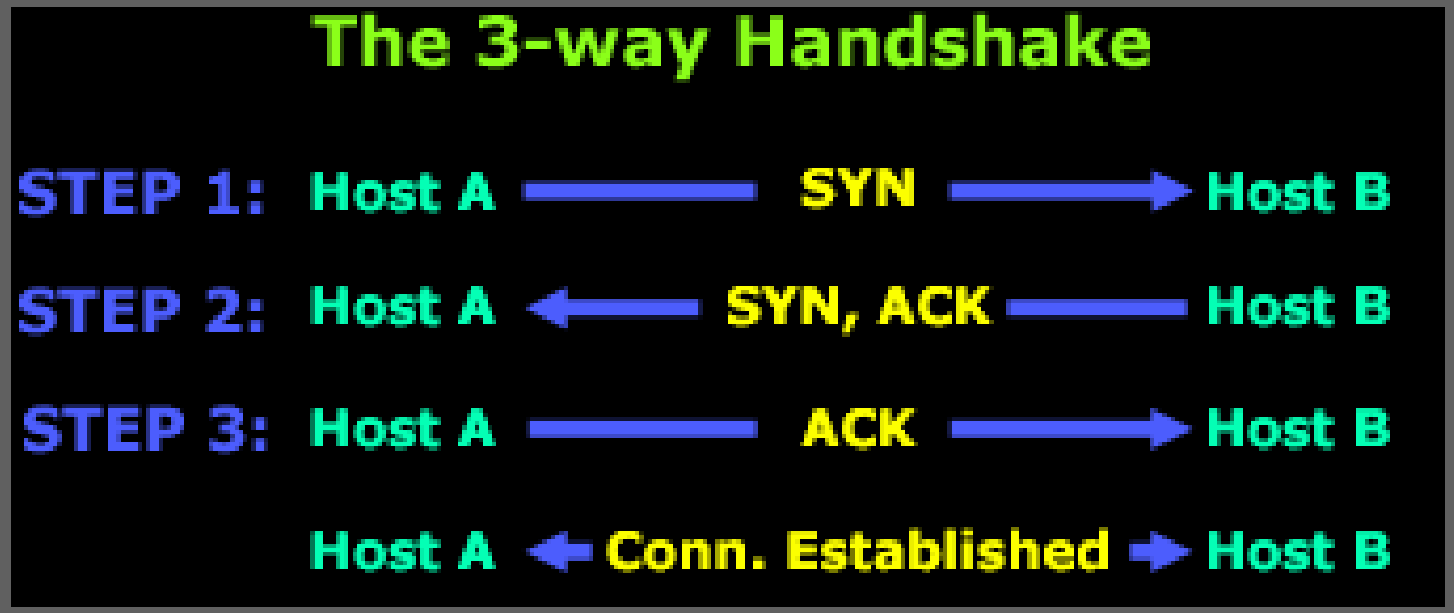
- While this procedure works well in most cases, there are a lot of instances where this 'queueing' of data is undesirable because any delay during queuing can cause problems to the waiting application. **A simple example would be a TCP stream, e.g real player**, where data must be sent and processed (by the receiver) immediately to ensure a smooth stream without any cut offs
- **Push flag is usually set on the last segment of a file to prevent buffer deadlocks.**

RST (RESET FLAG)

- The reset flag is used when a segment arrives that is not intended for the current connection. In other words, if you were to send a packet to a host in order to establish a connection, and there was no such service waiting to answer at the remote host, then the host would automatically reject your request and then send you a reply with the RST flag set. This indicates that the remote host has reset the connection.

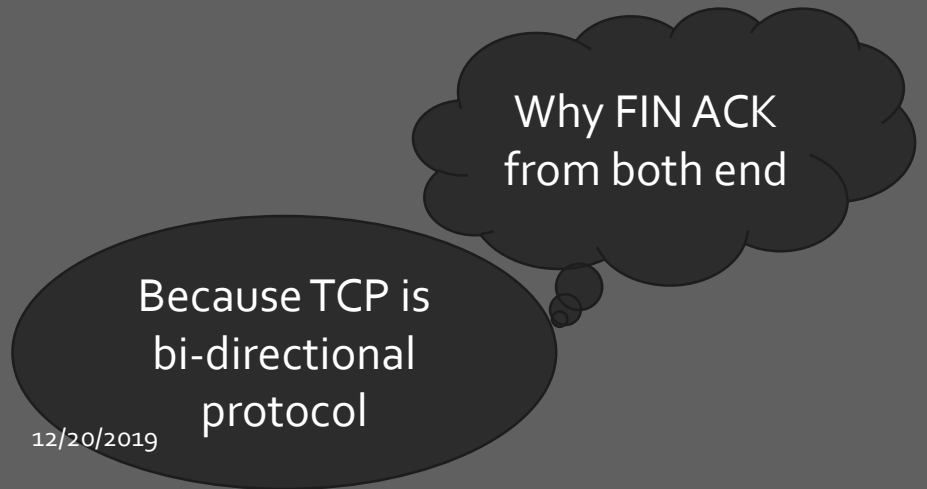
SYN (SYNCHRONISATION FLAG)

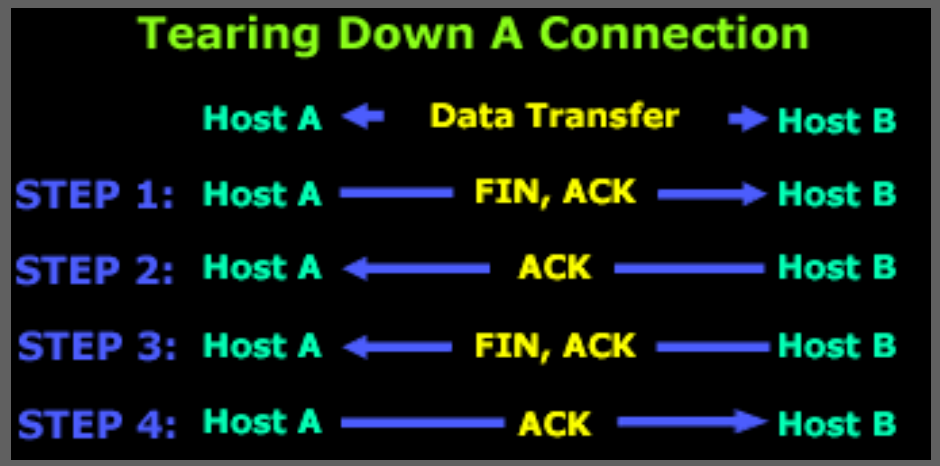
- The SYN flag is initially sent when establishing the classical 3-way handshake between two hosts.



FIN (FINISH FLAG)

- This flag is used to tear down the virtual connections created using the previous flag (SYN), so because of this reason, the FIN flag always appears when the last packets are exchanged between a connection.





WINDOWS SIZE (USE AT RECEIVING END)

- Window size (Total capacity) is advertised during the three way handshake.
- Basically used for flow control.
- 16 bits (possible values between zero to 65535).
- Suppose B (receiver) has advertised its window size as 10000 to A(sender), it means that we can not accept any value beyond this point.

CHECKSUM AND URGENT POINTER

- CHECKSUM – used for error control
- **URGENT POINTER**
- Whenever URG flag is set, so we look for the values which are urgent. The values can be between 0 to 65535.
- Values present inside urgent pointer will be processed at the urgent basis.

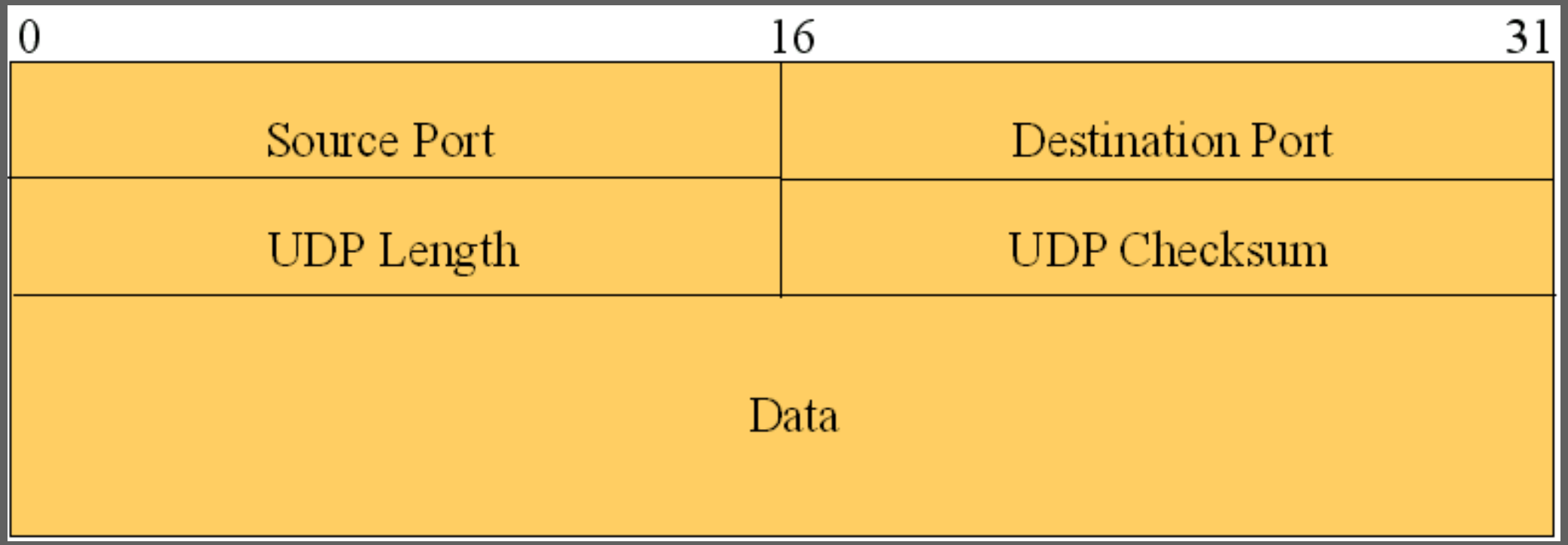
OPTIONS AND PADDING (40 BYTES)

- Concept of MSS (maximum segment size is used).
- Maximum Segment Size (MSS)
- Window Scaling
- Selective Acknowledgements (SACK)
- Timestamps (RTT)
- Note : Window Scaling option can be a maximum of 30 bits in size, which includes the original 16 bit Window size field covered in the previous section. So that's 16 (original window field) + 14 (TCP Options 'Window Scaling') = 30 bits in total
- **Note -** Each segment, including the TCP header, must fit in the 65535 byte IP payload, and the TCP header is **20 bytes** at least, so the maximum payload of a TCP segment is 65535-20=**65515 bytes**.

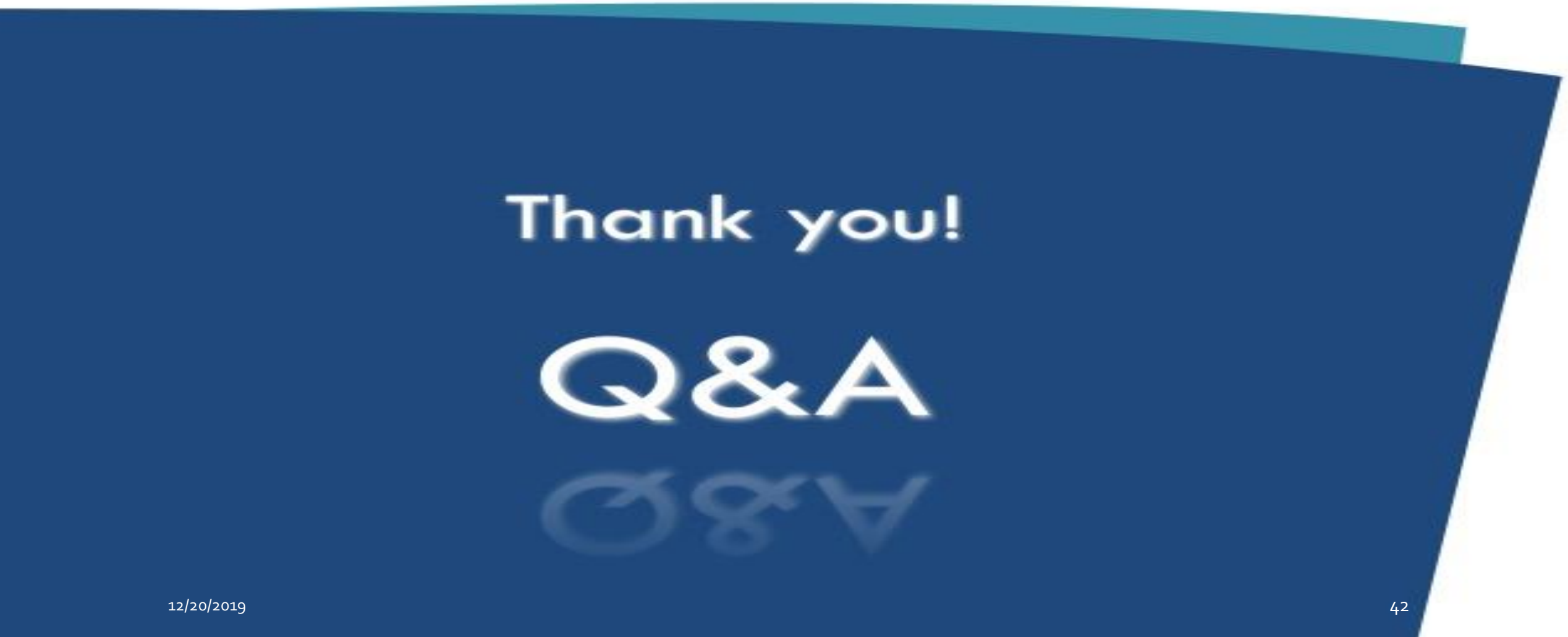
UDP (USER DATAGRAM PROTOCOL)

- User Datagram Protocol (UDP) is a connectionless protocol, which means UDP is not a reliable protocol and no sequence ordering.
- User Datagram Protocol (UDP) is capable of performing fundamental error checking. The UDP header includes a checksum field that the destination device can use to check the integrity of the data.

UDP HEADER FORMAT (FIXED 8 BYTES)



UDP LENGTH = UDP HEADER + LENGTH , UDP HEADER = 8 BYTES, PAYLOAD = 65535-8 = 66527 BYTES


Thank you!
Q&A