# Computer Networks

BCST -502 BCSP- 502

B.Tech (CSE) 5th Semester

Course Instructor: Dr Bishwajeet Pandey

# New 2020 Syllabus

**Unit –I**

Computer Network: Definitions, goals, components, Architecture, Classifications & Types.Layered Architecture: Protocol hierarchy, Design Issues, Interfaces and Services, ConnectionOriented & Connectionless Services, Service primitives, Design issues & its functionality. ISOOSI Reference Model: Principle, Model, Descriptions of various layers and its comparison with TCP/IP. Principals of physical layer: Media, Bandwidth, Data rate and Modulations

**Unit-II**

Data Link Layer: Need, Services Provided, Framing, Flow Control, Error control. Data Link Layer Protocol: Elementary &Sliding Window protocol: 1-bit, Go-Back-N, Selective Repeat, Hybrid ARQ. Protocol verification: Finite State Machine Models & Petri net models. ARP/RARP/GARP

**Unit-III**

MAC Sub layer: MAC Addressing, Binary Exponential Back-off (BEB) Algorithm, Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted- ALOHA), for Local-Area Networks (CSMA, CSMA/CD, CSMA/CA), CollisionFree Protocols: Basic Bit Map, BRAP, Binary Count Down, MLMA Limited Contention Protocols: Adaptive Tree Walk, Performance Measuring Metrics. IEEE Standards 802 series & their variant.

BIRLA INSTITUTE OF APPLIED SCIENCES
BIAS

# New 2020 Syllabus

**Unit-IV**

Network Layer: Need, Services Provided, Design issues, Routing algorithms: Least CostRouting algorithm, Dijkstra's algorithm, Bellman-ford algorithm, Hierarchical Routing,Broadcast Routing, Multicast Routing. IP Addresses, Header format, Packet forwarding,Fragmentation and reassembly, ICMP, Comparative study of IPv4 & IPv6

**Unit-V**

Transport Layer: Design Issues, UDP: Header Format, Per-Segment Checksum, CarryingUnicast/Multicast Real-Time Traffic, TCP: Connection Management, Reliability of DataTransfers, TCP Flow Control, TCP Congestion Control, TCP Header Format, TCP TimerManagement. Application Layer: WWW and HTTP, FTP, SSH, Email (SMTP, MIME, IMAP), DNS, Network Management (SNMP).

# ABOUT COURSE INSTRUCTOR

- PhD from Gran Sasso Science Institute, Italy
- PhD Supervisor Prof Paolo Prinetto from Politecnico Di Torino, World Rank 13 in Electrical Engineering
- MTech from Indian Institute of Information Technology, Gwalior
- Visited 32 Countries Across The Globe
- Written 200+ Research paper with 193 Researcher from 63 Universities
- Scopus Profile: https://www.scopus.com/authid/detail.uri?authorId=57203239026
- Google Scholar: https://scholar.google.com/citations?user=UZ_8yAMAAAAJ&hl=hi
- Contact: gyancity@gyancity.com, +91-7428640820 (For any help @ BIAS and Guidance for future MS from Europe and USA after BIAS)

# Course Objectives

- The course aims to develop an understanding of the fundamentals of Computer Network among the students

- The course explores different components of computer network, types of protocols, modern network technologies and their applications.

# Course Outcomes

After completing this course the student will be well equipped with the following concepts:

1. The student will be able to recognise the technological trends of Computer Networking.
2. The student will be able to discuss the key technological components of the Network and evaluate the challenges in building the network and find solutions for the same.
3. The student could understand the basic computer network technology as an isolating concept.

# Course Outcomes

4. The student will be thorough in concepts of Data Communication system and its components

5. The student will be able to identify and distinguish between different types of network topologies and protocols.

6. The student will have in depth knowledge of the the layers of the OSI model and TCP/IP and will able to explain the function(s) of each layer.

# Course Outcomes

7. The student will be able to identify the different types of network devices and their functions within a network

8. The student would have the skill to understand the building skills of subnetting and routing mechanisms.

9. Upon familiarity with the above concepts the student will be able to assist in network design and its implementation in real time.

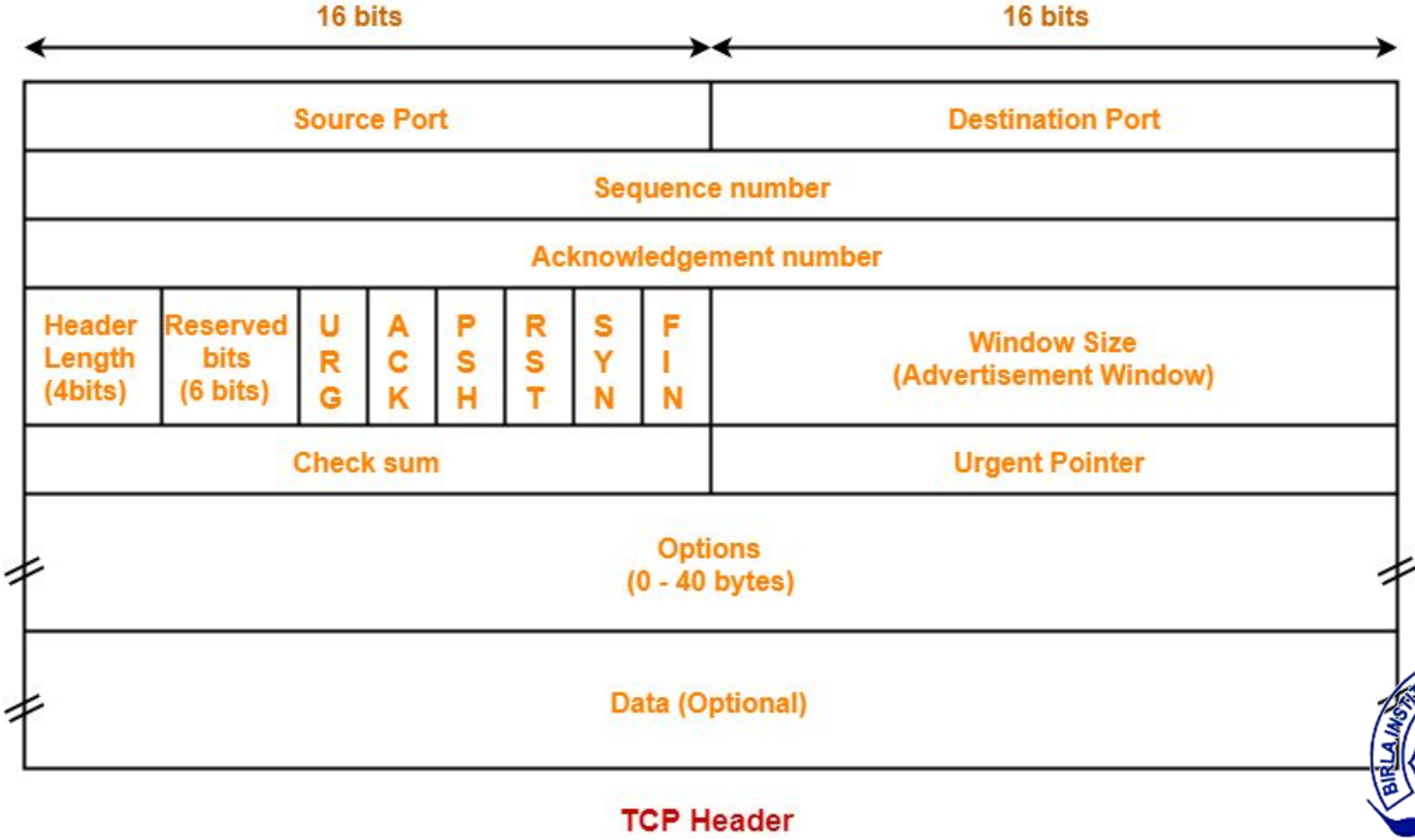
# About Course Outline

- UNIT 1:
  - Theory Lecture No 1-4, Lecture 29
  - Lab on Vivado: Lecture 9-11
- UNIT 2: Theory Lecture No 5-8
- UNIT 3: Theory Lecture No 14-18
- UNIT 4:
  - Theory Lecture No 12-13, 19-21, 36
  - Lab on Packet Tracer and C: Lecture 24-28
- UNIT 5: Theory Lecture No 30-35
- Student Assignment Presentation: 22-23
- Lecture No 37-42: Discuss Previous Year Question of UTU

LECTURE 32

# TCP Header Format

# TCP Header Format




TCP Header

# TCP Header Format: 1. Source Port

- Source Port is a 16 bit field.
- It identifies the port of the sending application.

# TCP Header Format: 2. Destination Port

- Destination Port is a 16 bit field.
- It identifies the port of the receiving application.
- It is important to note-
  - A TCP connection is uniquely identified by using-Combination of port numbers and IP Addresses of sender and receiver
  - IP Addresses indicate which systems are communicating.
  - Port numbers indicate which end to end sockets are communicating.

# TCP Header Format: 3. Sequence Number

- Sequence number is a 32 bit field.
- TCP assigns a unique sequence number to each byte of data contained in the TCP segment.
- This field contains the sequence number of the first data byte.

# TCP Header Format: 4. Acknowledgement Number

- Acknowledgment number is a 32 bit field.
- It contains sequence number of the data byte that receiver expects to receive next from the sender.
- It is always sequence number of the last received data byte incremented by 1.

# TCP Header Format: 5. Header Length

- Header length is a 4 bit field.
- It contains the length of TCP header.
- It helps in knowing from where the actual data begins.
- The length of TCP header always lies in the range-
    - [20 bytes , 60 bytes]
- The initial 5 rows of the TCP header are always used.
- So, minimum length of TCP header = 5 x 4 bytes = 20 bytes.
- The size of the 6th row representing the Options field vary.
- The size of Options field can go up to 40 bytes.
- So, maximum length of TCP header = 20 bytes + 40 bytes = 60 bytes.

# TCP Header Format: 6. Reserved Bits

- The 6 bits are reserved.
- These bits are not used.

# TCP Header Format: 7. URG Bit

- URG bit is used to treat certain data on an urgent basis
- When URG bit is set to 1,
- It indicates the receiver that certain amount of data within the current segment is urgent.
- Urgent data is pointed out by evaluating the urgent pointer field.
- The urgent data has be prioritized.
- Receiver forwards urgent data to the receiving application on a separate channel.

# TCP Header Format: 8. ACK Bit

- ACK bit indicates whether acknowledgement number field is valid or not.
- When ACK bit is set to 1, it indicates that acknowledgement number contained in the TCP header is valid.
- For all TCP segments except request segment, ACK bit is set to 1.
- Request segment is sent for connection establishment during **Three Way Handshake**.

# TCP Header Format: 9. PSH Bit

- PSH bit is used to push the entire buffer immediately to the receiving application.
- When PSH bit is set to 1,
- All the segments in the buffer are immediately pushed to the receiving application.
- No wait is done for filling the entire buffer.
- This makes the entire buffer to free up immediately.

# TCP Header Format: 9. PSH Bit

It is important to note:

- Unlike URG bit, PSH bit does not prioritize the data.
- It just causes all the segments in the buffer to be pushed immediately to the receiving application.
- The same order is maintained in which the segments arrived.
- It is not a good practice to set PSH bit = 1.
- This is because it disrupts the working of receiver's CPU and forces it to take an action immediately.

# TCP Header Format: 10. RST Bit

- RST bit is used to reset the TCP connection.

When RST bit is set to 1,

- It indicates the receiver to terminate the connection immediately.
- It causes both the sides to release the connection and all its resources abnormally.
- The transfer of data ceases in both the directions.
- It may result in the loss of data that is in transit.

This is used only when-

- There are unrecoverable errors.
- There is no chance of terminating the TCP connection normally.

# TCP Header Format: 11. SYN Bit

- SYN bit is used to synchronize the sequence numbers.

When SYN bit is set to 1,

- It indicates the receiver that the sequence number contained in the TCP header is the initial sequence number.
- Request segment sent for connection establishment during Three way handshake contains SYN bit set to

# TCP Header Format: 12. FIN Bit-

- FIN bit is used to terminate the TCP connection.

When FIN bit is set to 1,

- It indicates the receiver that the sender wants to terminate the connection.
- FIN segment sent for **TCP Connection Termination** contains FIN bit set to 1.

# TCP Header Format: 13. Window Size-

- Window size is a 16 bit field.
- It contains the size of the receiving window of the sender.
- It advertises how much data (in bytes) the sender can receive without acknowledgement.
- Thus, window size is used for **Flow Control**.

It is important to note-

- The window size changes dynamically during data transmission.
- It usually increases during TCP transmission up to a point where congestion is detected.
- After congestion is detected, the window size is reduced to avoid having to drop packets.

# TCP Header Format: 14. Checksum-

- Checksum is a 16 bit field used for error control.
- It verifies the integrity of data in the TCP payload.
- Sender adds CRC checksum to the checksum field before sending the data.
- Receiver rejects the data that fails the CRC check.

# TCP Header Format: 15. Urgent Pointer-

- Urgent pointer is a 16 bit field.
- It indicates how much data in the current segment counting from the first data byte is urgent.
- Urgent pointer added to the sequence number indicates the end of urgent data byte.
- This field is considered valid and evaluated only if the URG bit is set to 1.

# TCP Header Format: 15. Urgent Pointer-

## USEFUL FORMULAS

- **Formula-01:**

Number of urgent bytes = Urgent pointer + 1

- **Formula-02:**

End of urgent byte = Sequence number of the first byte in the segment + Urgent pointer

# TCP Header Format: 16. Options-

- Options field is used for several purposes.
- The size of options field vary from 0 bytes to 40 bytes.

Options field is generally used for the following purposes-

1. Time stamp
2. Window size extension
3. Parameter negotiation
4. Padding

# 16.1. Time Stamp

When wrap around time is less than life time of a segment,

- Multiple segments having the same sequence number may appear at the receiver side.
- This makes it difficult for the receiver to identify the correct segment.
- If time stamp is used, it marks the age of TCP segments.
- Based on the time stamp, receiver can identify the correct segment.

# 16.2 Window Size Extension-

- Options field may be used to represent a window size greater than 16 bits.
- Using window size field of TCP header, window size of only 16 bits can be represented.
- If the receiver wants to receive more data, it can advertise its greater window size using this field.
- The extra bits are then appended in Options field.

# 16.3 Parameter Negotiation-

Options field is used for parameters negotiation.

Example- During connection establishment,

- Both sender and receiver have to specify their maximum segment size.
- To specify maximum segment size, there is no special field.
- So, they specify their maximum segment size using this field and negotiates.

## 16.4 Padding-

- Addition of dummy data to fill up unused space in the transmission unit and make it conform to the standard size is called as padding.

- Options field is used for padding.