TCP/IP

Understanding TCP/IP is essential for anyone working in IT or networking. It forms the backbone of internet and network communications. This technical documentation is designed to provide a structured and detailed understanding of TCP/IP, covering fundamental concepts, protocols, and mechanisms. It suits learners at all levels, from beginners to advanced professionals.

1. TCP/IP Classes

TCP/IP defines different classes of IP addresses to organize the IP address space efficiently. Each class has a specific range of addresses, allowing for different sizes of networks. These are Class A, Class B, Class C, Class D, and Class E, each serving distinct purposes.

---

2. Private IP Addresses

Private IP addresses are used for communication within a local network. They are not routable on the Internet and help secure internal communications. They are often used in conjunction with NAT (Network Address Translation).

---

3. Data Protection in IP

IP does not inherently guarantee data protection or reliable delivery. Instead, it relies on transport layer protocols like TCP and UDP for:

- Checksum Mechanisms: Ensures data integrity.
- Error Detection and Correction: TCP uses acknowledgment and retransmission to ensure reliability, while UDP offers minimal error-checking capabilities.

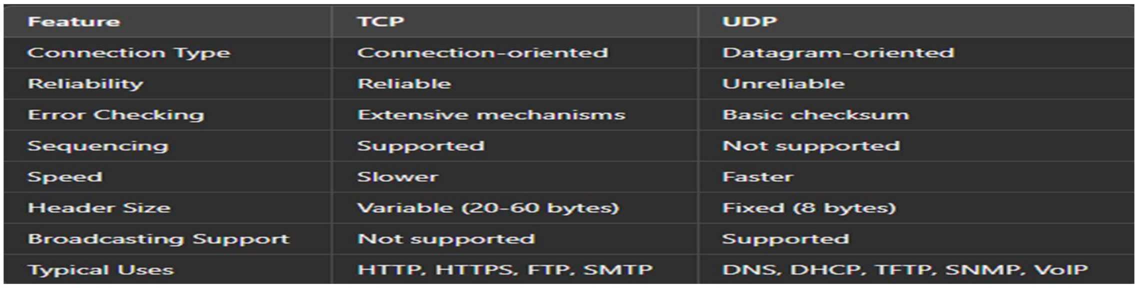
If the destination IP is unreachable, the packet's TTL (Time to Live) decreases until it reaches zero, at which point the packet is discarded.

---

4. Transport and Internet Layer Data Units

- Transport Layer: The protocol data unit is referred to as a "segment" (TCP) or "datagram" (UDP).
- Internet Layer: The protocol data unit is a "packet."

5. TCP vs. UDP



Feature	TCP	UDP
Connection Type	Connection-oriented	Datagram-oriented
Reliability	Reliable	Unreliable
Error Checking	Extensive mechanisms	Basic checksum
Sequencing	Supported	Not supported
Speed	Slower	Faster
Header Size	Variable (20-60 bytes)	Fixed (8 bytes)
Broadcasting Support	Not supported	Supported
Typical Uses	HTTP, HTTPS, FTP, SMTP	DNS, DHCP, TFTP, SNMP, VoIP

6. TCP Reliability Mechanisms

TCP ensures reliability through:

- **Checksum**: Detects errors in data.
- **Acknowledgments**: Confirms receipt of data.
- **Retransmission**: Resends lost or corrupted data.
- **Sequence Numbers**: Maintains the order of data.
- **Timers**: Ensures timely delivery.

---

7. TCP Services

Key services provided by TCP include:

- Process-to-process communication
- Stream orientation
- Full-duplex service
- Multiplexing
- Reliability

---

8. TCP Protocol Header Format

The TCP header includes fields such as:

- Source and Destination Ports
- Sequence Number
- Acknowledgment Number
- Flags (e.g., SYN, ACK, FIN)
- Window Size

---

9. TCP Flags

TCP headers include six primary flags:

1. **URG**: Indicates urgent data.
2. **ACK**: Valid acknowledgment number.
3. **PSH**: Request to push data.
4. **RST**: Reset connection.
5. **SYN**: Synchronize sequence numbers.

6. **FIN**: Terminate the connection.

---

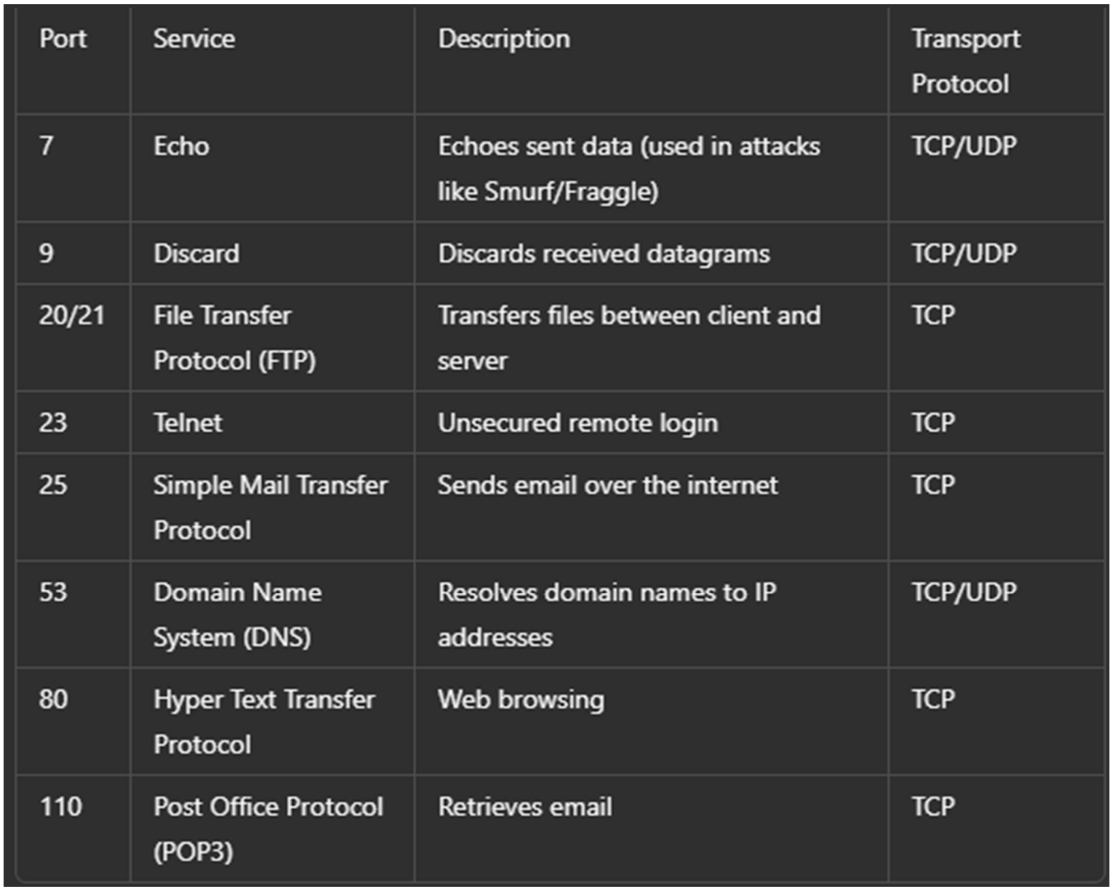
10. TCP Checksum Field

The 16-bit checksum field is mandatory in TCP and ensures error detection within transmitted data.

11. What is a PORT?

A port is an interface for communication between a computer and external devices or networks. For example, ports enable connections to printers, hard drives, and networks

12. Well-Known Ports used by TCP:



Port	Service	Description	Transport Protocol
7	Echo	Echoes sent data (used in attacks like Smurf/Fraggle)	TCP/UDP
9	Discard	Discards received datagrams	TCP/UDP
20/21	File Transfer Protocol (FTP)	Transfers files between client and server	TCP
23	Telnet	Unsecured remote login	TCP
25	Simple Mail Transfer Protocol	Sends email over the internet	TCP
53	Domain Name System (DNS)	Resolves domain names to IP addresses	TCP/UDP
80	Hyper Text Transfer Protocol	Web browsing	TCP
110	Post Office Protocol (POP3)	Retrieves email	TCP

13. Purpose of a DNS Server:

A DNS server translates human-readable domain names (e.g., www.google.com) into IP addresses, enabling access to websites and online services.

14. Define the term Endpoint in TCP:

A TCP endpoint represents one side of a TCP connection, including the IP address and port. It enables communication between a client and a server.

15. Explain the error control mechanism in TCP:

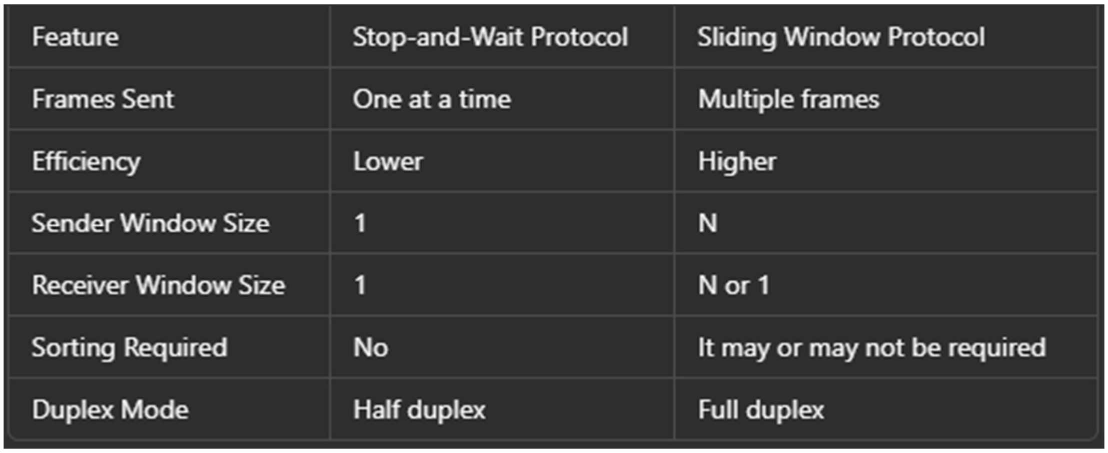
Error control is achieved using:

- **Checksum:** Detects errors in data
- **Acknowledgment:** Confirms receipt of data
- **Retransmission:** Resends lost/corrupted segments

16. What is Congestion?

Congestion occurs when network traffic exceeds capacity, slowing down data transmission. TCP manages congestion using algorithms like slow start and congestion avoidance.

17. Differences between Stop-and-Wait Protocol and Sliding Window Protocol:



Feature	Stop-and-Wait Protocol	Sliding Window Protocol
Frames Sent	One at a time	Multiple frames
Efficiency	Lower	Higher
Sender Window Size	1	N
Receiver Window Size	1	N or 1
Sorting Required	No	It may or may not be required
Duplex Mode	Half duplex	Full duplex

18. What is Round Trip Time (RTT)?

RTT is the time taken for a data packet to reach its destination and for the acknowledgment to return to the sender.

19. Significance of TCP Acknowledgments:

TCP acknowledgments confirm the successful receipt of data packets, ensuring reliable communication.

20. What is Retransmission?

Retransmission is the process of resending lost or corrupted data packets to ensure reliable delivery. It uses acknowledgment and timers to detect and resend missing packets.

21. Estimating TCP Round Trip Time (RTT)

If the TCP round trip time (RTT) is currently 30ms, and acknowledgments arrive after 26ms, 32ms, and 24ms, we calculate the new RTT estimate using the formula:

New RTT Formula:

Where:

- = 0.9

- Old RTT = 30ms
- Arrival RTT = 26ms (first calculation example)

Example Calculation:

Repeat this for subsequent arrival times (32ms and 24ms) to update the RTT iteratively.

For more details, refer to the **What is RTT** article.

---

22. Features of TCP

- **Connection-oriented:** Applications request and use a connection to transfer data.
- **Stream Data Transfer:** Data is transferred as a continuous stream, packaged into TCP segments for transmission.
- **Reliable:** Ensures data recovery in case of errors like corruption or duplication.
- **Point-to-Point:** Provides end-to-end delivery.
- **Interoperability:** Works across different platforms.
- **Error and Flow Control:** Manages error-checking and data flow.
- **Name Resolution:** Resolves human-readable names into IP addresses.
- **Routability:** TCP/IP supports routing.
- **Full Duplex:** Enables bidirectional communication.

For more details, read the **TCP/IP Model** article.

---

23. SCTP Protocol

SCTP (Stream Control Transmission Protocol):

- Connection-oriented protocol allowing full-duplex communication.
- Transmits multiple streams of data simultaneously.
- Ideal for applications like telephony and multimedia.
- Designed to support reliable connections over wireless networks.
- Standardized by RFC 2960 and developed by IETF.

---

24. Three-Way Handshake Protocol

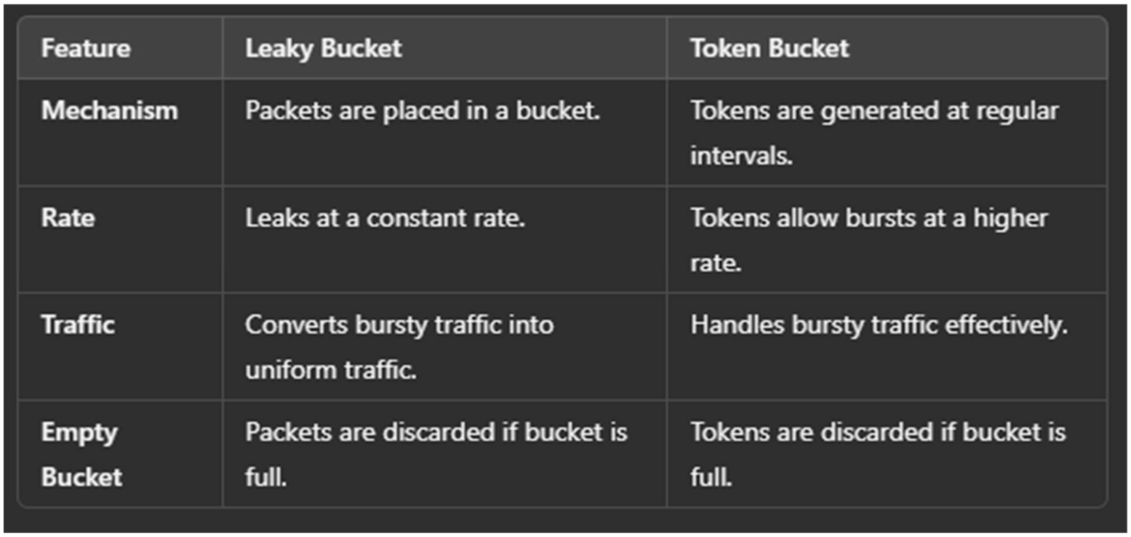
Steps:

1. **SYN:** Client sends a SYN segment to initiate connection.
2. **SYN + ACK:** Server responds with SYN-ACK, acknowledging the SYN and starting its own sequence.

3. **ACK:** Client sends an ACK to complete the handshake.

This process establishes full-duplex communication.

25. Leaky Bucket vs. Token Bucket Algorithm

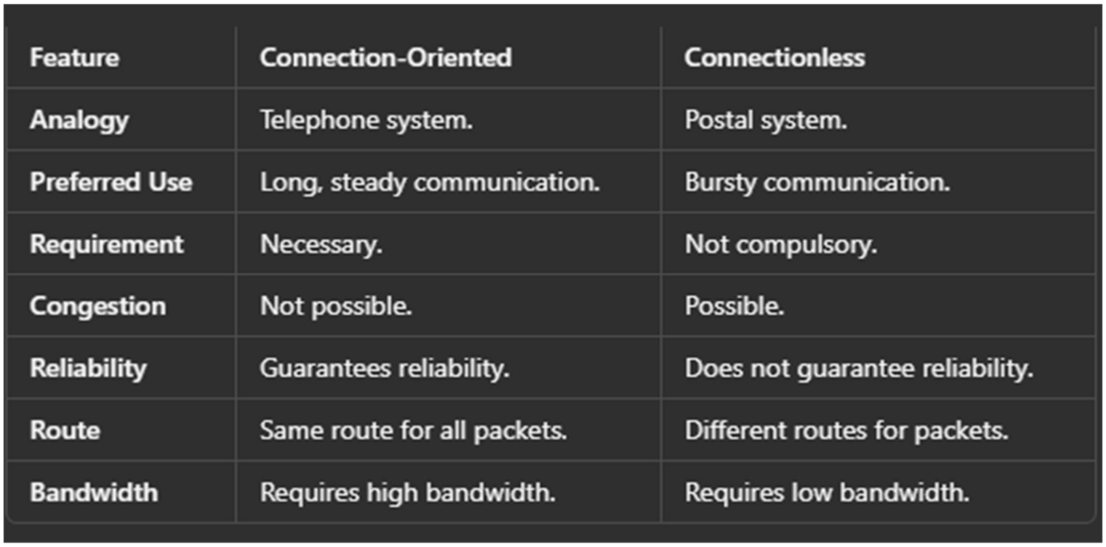


Feature	Leaky Bucket	Token Bucket
Mechanism	Packets are placed in a bucket.	Tokens are generated at regular intervals.
Rate	Leaks at a constant rate.	Tokens allow bursts at a higher rate.
Traffic	Converts bursty traffic into uniform traffic.	Handles bursty traffic effectively.
Empty Bucket	Packets are discarded if bucket is full.	Tokens are discarded if bucket is full.

26. Advantages of Token Bucket Over Leaky Bucket

- **Tokens are discarded, not packets, when the bucket is full.**
- **Allows large bursts of traffic at faster rates.**

27. Connection-Oriented vs. Connectionless Services



Feature	Connection-Oriented	Connectionless
Analogy	Telephone system.	Postal system.
Preferred Use	Long, steady communication.	Bursty communication.
Requirement	Necessary.	Not compulsory.
Congestion	Not possible.	Possible.
Reliability	Guarantees reliability.	Does not guarantee reliability.
Route	Same route for all packets.	Different routes for packets.
Bandwidth	Requires high bandwidth.	Requires low bandwidth.

28. TCP Connection Phases

1. **Connection Establishment: Three-way handshake.**
2. **Data Transfer: Full-duplex communication.**
3. **Connection Termination: Gracefully ends the connection.**

29. Features of TCP Sliding Window

- Variable-sized windows for flow control and reliable transfer.
- Full-duplex communication with simultaneous data transfer.
- Allows devices and routers of varying speeds to communicate effectively.]

30. Maximum and Minimum Size of TCP Header

- Maximum Size: 60 bytes
- Minimum Size: 20 bytes

31. Port Addresses and Their Uniqueness

- Port addresses are managed by the transport layer of the OSI Model (Layer 4).
- Port addresses are shorter than IP addresses because there are fewer protocols than devices.
- IP addresses identify devices, while port addresses identify specific protocols or services.

32. Reliability of UDP vs. IP

- UDP: Unreliable and connectionless.
- IP: Relies on upper-layer protocols for reliability (e.g., TCP).
- UDP is more reliable than IP regarding data integrity because its checksum covers the entire segment, while IP's checksum only covers the header.

---

33. Definition of Datagram

A datagram is a logical unit of data transfer that includes:

- Header: Contains metadata for routing.
- Data Payload: The actual data being sent.

Characteristics:

- Does not guarantee delivery.
- No prior information about the path between source and destination.
- Frequently divided into smaller parts for transmission.

---

34. Registered and Dynamic Ports

- Registered Ports: Range from 1024 to 49151. Not assigned by IANA but can be registered to avoid duplication.
- Dynamic Ports: Range from 49152 to 65535. Neither assigned nor registered and can be used freely.

35. Importance of TTL Field

The TTL (Time-to-Live) field:

- **Specifies the lifetime or hop count for a packet in the network.**
- **Prevents packets from circulating indefinitely by discarding them after the TTL expires.**

36. IPv4 Packet Rejection Example

An IPv4 packet with the first 8 bits as 01000010 is rejected because:

- **The first 4 bits (0100) indicate IPv4.**
- **The next 4 bits (0010) represent the header length, calculated as 2 × 4 = 8 bytes, which is invalid (should be 20-60 bytes).**

37. IPv4 Header Options Calculation

If the IPv4 header length (HLEN) is 1000 in binary:

- **HLEN = 8**
- **Header size = 8 × 4 = 32 bytes**
- **Options size: 32 - 20 = 12 bytes (since the minimum header size is 20 bytes).**

38. Open-Loop vs. Closed-Loop Congestion Control

- **Open-Loop: Prevents congestion before it happens (handled by source/destination).**
- **Closed-Loop: Alleviates congestion after it occurs.**

39. Fields Changing in IPv4 Header from Router to Router

- **Total Length Field**
- **Header Checksum**

40. What is a Firewall?

A firewall is a security system that controls what data can enter or leave a computer or network. It acts like a wall, blocking unwanted or harmful traffic that doesn't meet predefined rules and allowing safe data to pass through.

If the value of the HLEN field is 7, then there are 28 (since 7 × 4 = 28) bytes included in the header.

---

41. Explain the Concept of NAT (Network Address Translation)

NAT (Network Address Translation) is a process used by routers to change the IP address of data as it moves between a private network and the internet. When a device sends data, the router changes its address to a public address from a private address. When the data returns, the router sends it back to the right device.

---

42. IPv4 Datagram Identification Example

If a source is sending 100 datagrams and the first datagram identification number is 1024, then the identification number of the last datagram will be:

---

43. Reason for Elimination of Checksum in IPv6 Header

The checksum is eliminated in IPv6 because it is provided by upper-layer protocols; it is therefore not needed at this level.

---

44. Strategies for IPv4 to IPv6 Transition

1. **Dual-Stack**
2. **Tunneling**
3. **Header Translation**

---

45. What is Tunneling?

Tunneling is an internetworking technique used when the source and destination networks of the same type are to be connected through a network of a different type.

---

46. Purpose of ARP Protocol

The ARP (Address Resolution Protocol) is used to find the physical address (MAC address) of a device when only its IP address is known. When a device wants to send data to another device on the same network, ARP resolves the IP address of the destination device into its MAC address. This information is then used to send data frames directly to the target device.

---

47. What is Fragmentation?

Fragmentation is an important function of the network layer. It is a technique in which gateways break up or divide larger packets into smaller ones called fragments. Each fragment is then sent as a separate internal packet. Each fragment has its own separate header and trailer. Sometimes, a fragmented datagram also gets fragmented when it encounters a network that handles smaller fragments.

Thus, a datagram can be fragmented several times before it reaches its final destination. The reverse process of fragmentation is difficult. Reassembly of fragments is usually done by the destination host because each fragment has become an independent datagram.

---

48. Minimum Frame Size in Ethernet

Given:

- Transmission Speed = 10 Mbps
- Round Trip Propagation Delay = 46.4 ms
- 48-bit jamming signal

The minimum frame size is calculated as:

---

49. Slow Start Phase in TCP Congestion Control

In the slow start phase of the TCP congestion control algorithm, the size of the congestion window increases exponentially.

---

50. Maximum Window Size in Selective Reject Protocol

The maximum window size for data transmission using the Selective Reject protocol with an n-bit frame sequence number is:

2^(n-1).