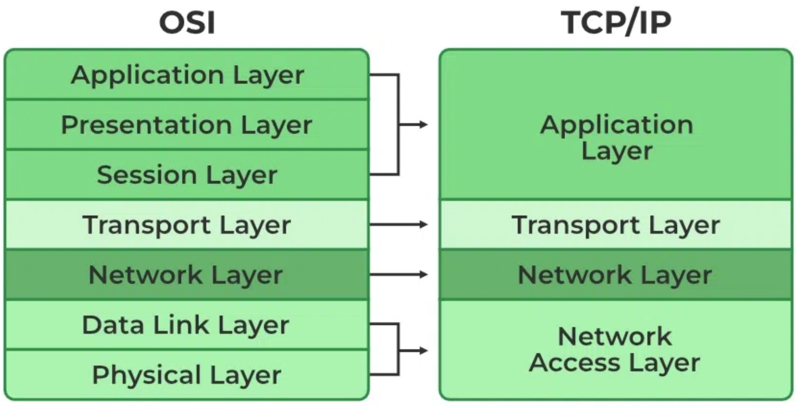
UNIT-2

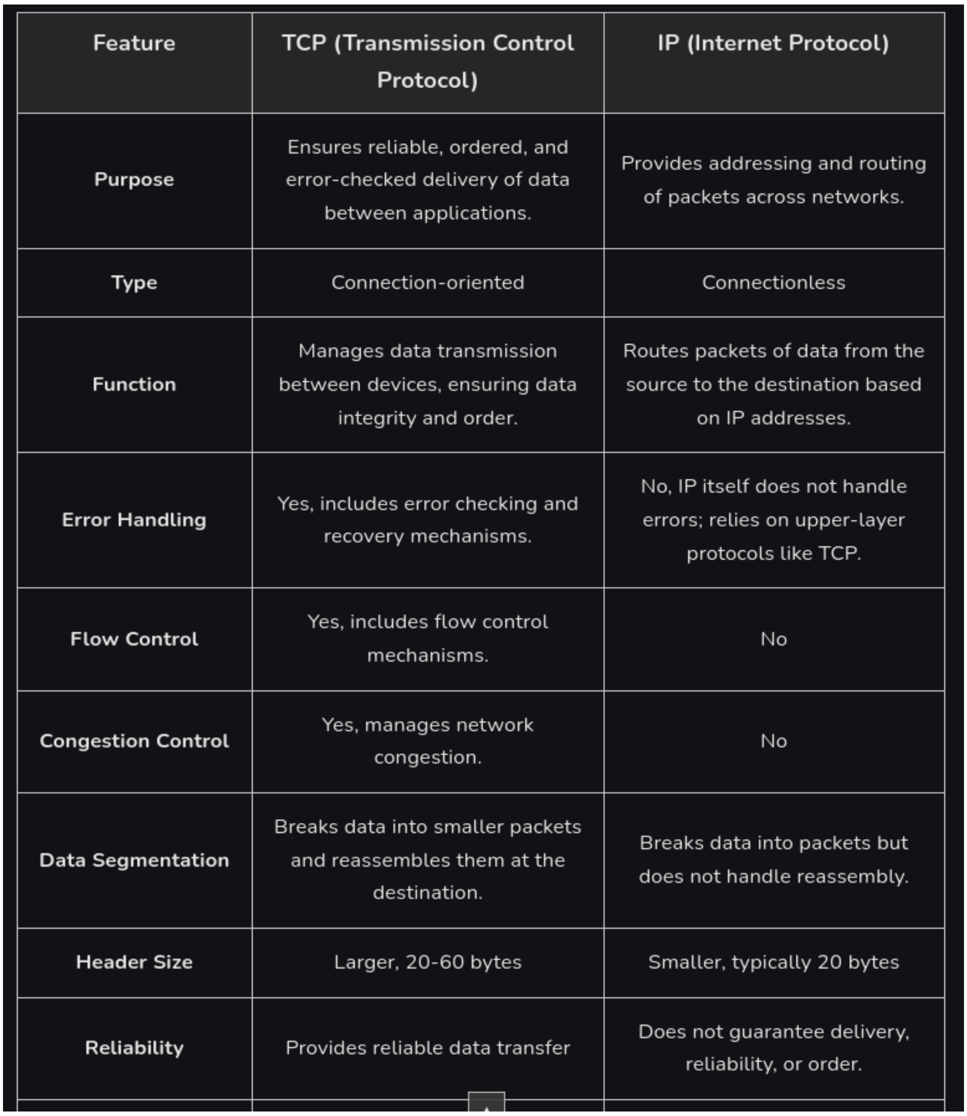
- network protocol
    - a set of rules that govern how data is transmitted b/w devices on a network
    - OSI is the most widely employed model communication b/w computers on a network
    - every layer communicates using a different protocol

> TCP/IP for packet routing and connections; BGP for route discovery; DNS for IP address discovery

- TCP/IP model
    - defines how data is transmitted over networks, ensuring reliable communication between devices
    - divides packets and one end, transfers them and assembles them at the other end
    - layers
        - app layer
            - functions - provides protocols for user-facing applications; HTTP, FTP, SMTP
            - sec challenges
                - vulnerable to attacks like phishing, buffer overflows and malware injection
                - weak or absent authentication
                - encryption is critical to protect sensitive data
        - transport layer
            - functions - manages end-to-end comm b/w devices; TCP and UDP
            - sec challenges
                - TCP susceptible to SYN flooding
                - session hijacking attacks can intercept and manipulate comm
                - TLS is used to encrypt data and provide secure communications
        - internet layer
            - functions - responsible for routing and addressing data packets using IP
            - sec challenges
                - IP spoofing allows attakers to impersonate others
                - fragmentation attacks can exploit the division and reassembling of packets
                - IPSec is used to authenticate and encrypt data packets
        - network access layer
            - functions - deals with physical and data link layers, ensuring transmission over physical media
            - sec challenges
                - ARP poisoning, MAC spoofing and VLAN hopping

        - strong authentication and encryption protocols can mitigate risks

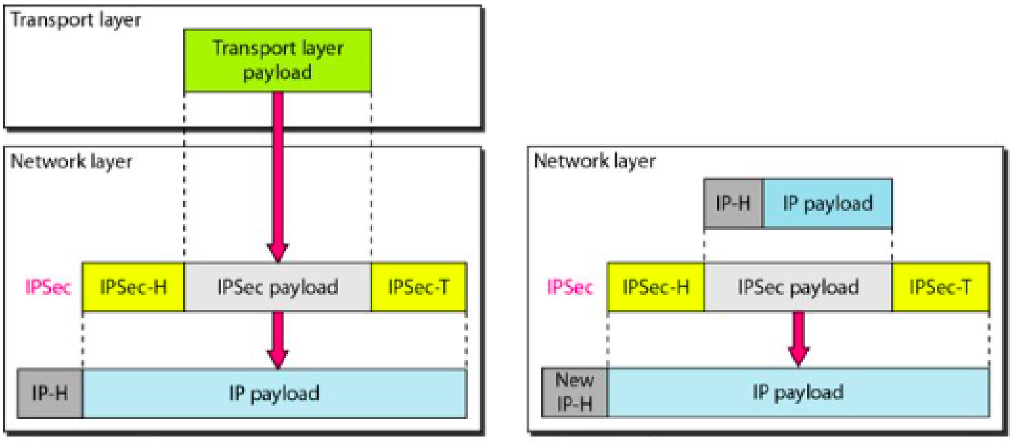




Feature	TCP (Transmission Control Protocol)	IP (Internet Protocol)
Purpose	Ensures reliable, ordered, and error-checked delivery of data between applications.	Provides addressing and routing of packets across networks.
Type	Connection-oriented	Connectionless
Function	Manages data transmission between devices, ensuring data integrity and order.	Routes packets of data from the source to the destination based on IP addresses.
Error Handling	Yes, includes error checking and recovery mechanisms.	No, IP itself does not handle errors; relies on upper-layer protocols like TCP.
Flow Control	Yes, includes flow control mechanisms.	No
Congestion Control	Yes, manages network congestion.	No
Data Segmentation	Breaks data into smaller packets and reassembles them at the destination.	Breaks data into packets but does not handle reassembly.
Header Size	Larger, 20-60 bytes	Smaller, typically 20 bytes
Reliability	Provides reliable data transfer	Does not guarantee delivery, reliability, or order.

- IPSec
    - protocol suite designed by IETF for securing IP comm by authenticating and encrypting data packets
    - network layer security
    - modes
        - transport - encrypts payload of IP packet; onl;y protects info coming from transport layer

    - tunnel - encrypts entire IP packet

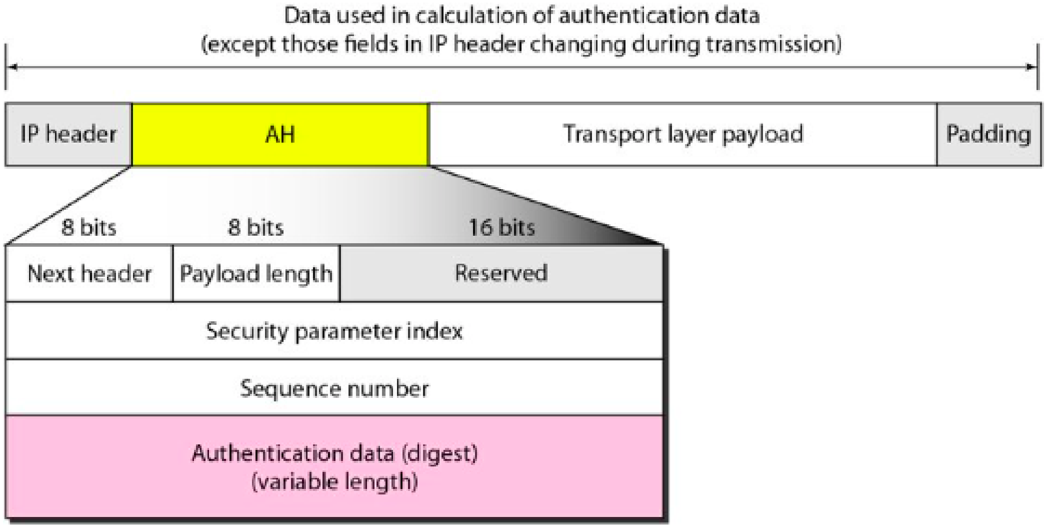


a. Transport mode

b. Tunnel mode

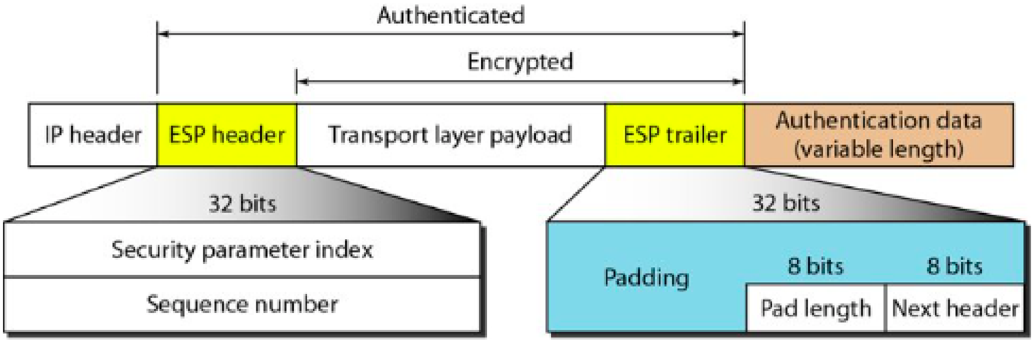
  - protocols
    - authentication header(AH) - procides authentication and data integirty but no privacy

Figure 32.6 ***Authentication Header (AH) Protocol in transport mode***

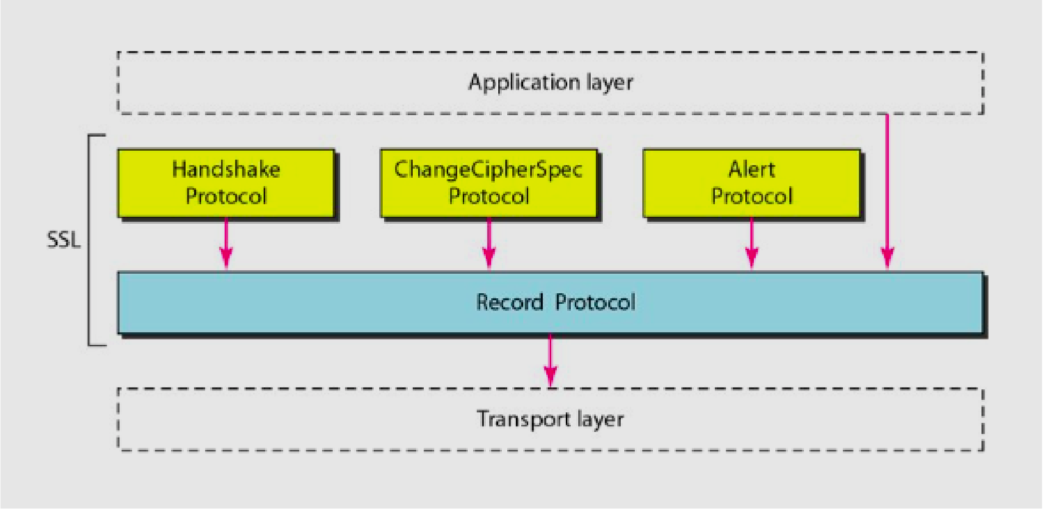


        - encapsulating security payload(ESP) - provides authentication, intergrity and privacy

          Figure 32.7 ***Encapsulating Security Payload (ESP) Protocol in transport mode***

- SSL/TLS
    - protocol suite to establish secure communciation channel b/w 2 parties across a network
    - transport layer security
    - SSL - cryptographic protocol for secure communication over the Internet
        - protocols
            - Handshake protocol - involves key exchange b/w client and server
            - ChangeCipherSpec protocol
            - Alert protocol
            - Record Protocol

    - TLS - ensures secure communication by encryptng data in transit using protocols like HTTPS
    - features
        - encryption
        - authentication
        - integrity
- SFTP

  - secure file transfer protocol
  - built on SSH
  - features
    - encryption of data under transfer
    - authentication via SSH keys/passwords
    - protection against eavesdropping and data tampering

- SSH

  - cryptograpic protocol for secure remote login and command exec
  - features
    - strong encryption for communication; public key authentication
    - protection against DNS spoofing and IP spoofing

- DNS

  - domain name system
    - DNS resolver
    - root nameserver
    - TLD server
    - authoritative nameserver
  - a system to translate domain names to the respective servers' IP addresses
  - vulnerabiliteis
    - DNS spoofing - manipulating DNS repsonses to redirect users to malicious sites
    - cache poisoning - injecting false data into a DNS resolver's cache
  - authentication occurs with the help of a random 16-bit TXID, abd response stays in cache only if teh TXID is the same at each stage; attackers guess TXID to deceive the resolver into thinking the response is valid
  - DNSSEC - adds cryptographic signatures to DNS records to ensure data integrity and authentication
    - types
      - public key
      - symmetric key
    - features
      - does nothing to imporve DNS availability
      - does nothing to improve DNS confidentiality
      - can still lead to buffer overflows

- routing protocols

  - routing
    - intradomain - within an autonomous system
      - distance vector - RIP
      - link state - OSPF
    - interdomain - b/w autonomous systems
      - path vector - BGP
  - RIP
    - routing information protocol

        - least cost route b/w 2 nodes is min distance; each node maintains a vector of min distances to every node; each node shares routing table with its immedaite neighbours periodically and when there is a change
        - uses UDP services on port 520
        - vulnerable to route poisoning and spoofing due to lack of authentication
    - OSPF
        - open shortest path first
        - uses Dijkstra's algo to build a routing table where each node has the entire topology of the domain
        - types of links
            - p2p
            - transient
            - stub
            - virtual
        - packets are encapsulated in IP datagrams
        - susceptible to attacks if authentication is not properly configured
    - BGP
        - border gateway protocol
        - similar to distane vector routing; atleast one "speaker" node in an AS that creates routing table and broadcasts to speaker nodes in neighbouring ASs
        - supports classless addressing
        - uses TCP services on port 179
        - vulnerable to prefix hijacking, route leaks and session hijacking due to the trust-based architecture it employs