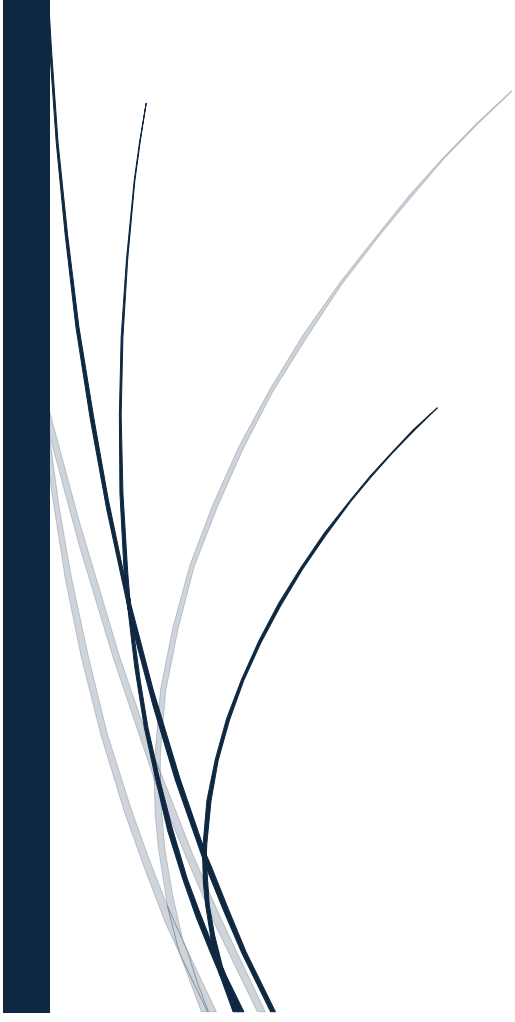
12/1/2025

Network & Security

Network Design and Related Aspects

CRN: 50251



Dewan Chowdhury
SGE515 @00773340

Table of Contents

Intelligent Transportation Systems

Intelligent Transportation Systems (ITS), a technology crucial for modernising our logistics and infrastructure operations. ITS integrates Information and Communication Technologies (ICT) into traditional transport infrastructure and vehicles to improve safety, efficiency, and sustainability. For non-technical management, ITS represents the fundamental shift from passive, reactive transport systems (e.g., fixed-timing traffic lights) to active, data driven networks that communicate and optimise themselves in real-time. This review will explain the core components, assess the operational benefits and deployment drawbacks, and specifically address the paramount security and ethical risks associated with large scale ITS adoption. The goal is to provide a comprehensive analysis supporting informed strategic investment decisions.

ITS is not a single product but a complex layer of integrated technologies designed to collect, process, and act upon real-time data to manage traffic flow, public transit, and freight logistics.

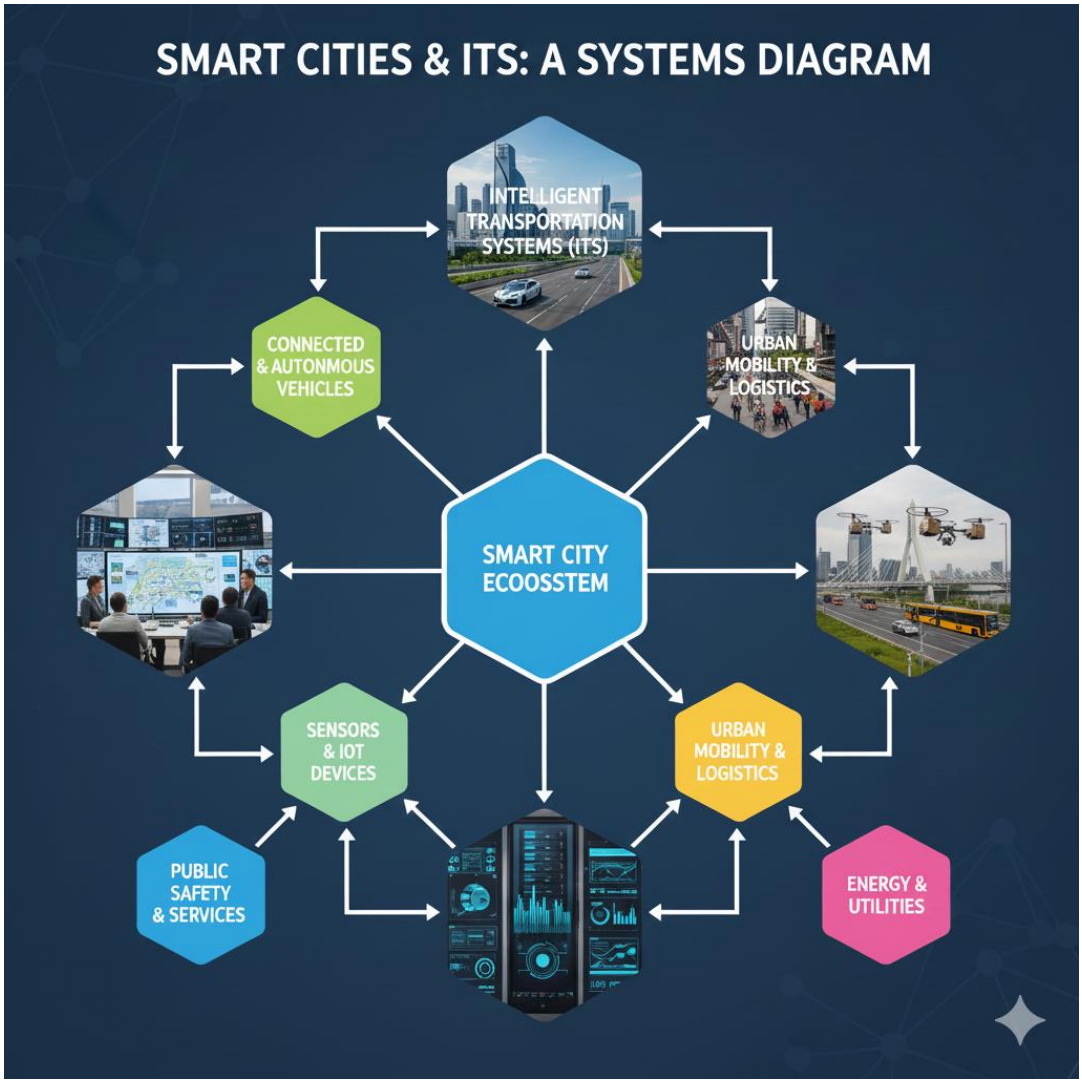
Core Components

- Data Collection (Sensors): This is the foundation. Data is gathered from various sources, including in-road sensors (inductive loops, cameras), mobile sensors (GPS data from public buses or private vehicles), and environmental data (weather).
- Processing (Control Centres): Dedicated Traffic Management Centres (TMCs) use powerful real-time analytics systems to process the collected data. They identify congestion, predict demand, and calculate optimal control strategies.
- Communication (V2X): The ability of systems to talk to each other is the defining feature of ITS. This is often called V2X (Vehicle-to-Everything) communication:
    - V2I (Vehicle-to-Infrastructure): Vehicles talk to traffic lights, road signs, and road-side units.
    - V2V (Vehicle-to-Vehicle): Vehicles talk directly to each other to share speed, position, and braking data for collision avoidance.
    - V2P (Vehicle-to-Pedestrian): Protecting vulnerable road users (e.g., smart crosswalks).
- Actuation (Control Systems): The output of the system includes Adaptive Traffic Control Systems (traffic lights that change timing based on real-time traffic flow), variable speed limits, electronic tolling, and dynamic route guidance transmitted to drivers.

Key Mechanisms

The system operates by constantly looping through four steps: Sense, Analyse, Communicate, and Act.

1. Sense: Traffic cameras detect an unusual build-up of vehicles on a major artery.
2. Analyse: The central control software calculates that the current traffic signal timing is inefficient for this volume and identifies alternate routes.
3. Communicate: The system uses Dedicated Short-Range Communication (DSRC) or Cellular V2X (C-V2X) to adjust the timing of the next five traffic signals and sends alerts to connected vehicles advising them of the congestion and suggesting a diversion.
4. Act: Drivers receive the updated information via their navigation systems, and the traffic signals adjust automatically, smoothing the flow and preventing gridlock.



ITS provides substantial operational, financial, and societal advantages compared to traditional static traffic management. These benefits are centred on safety enhancement and efficiency maximisation.

Safety Enhancement

ITS is a proactive safety tool. By enabling V2V communication, the system can provide warnings milliseconds before a human driver can react. This functionality is pivotal in mitigating high-risk scenarios:

- Reduced Accidents: Real-time data sharing and early warnings for hard braking, road hazards, or blind-spot threats significantly reduce the incidence and severity of collisions.
- Optimised Emergency Response: Smart signalling systems can prioritise ambulances and fire trucks, creating "green waves" that cut emergency response times, potentially saving lives.

Efficiency and Economic Gains

The system's real-time adaptability directly translates into major economic savings:

- Congestion Reduction: Adaptive Traffic Control dynamically adjusts signal timing to match actual traffic volume, leading to smoother flow and reduced idling. This can reduce travel time on major corridors by up to 20%.
- Fuel and Emissions Reduction: Less stop-and-go traffic means vehicles operate more efficiently, resulting in significant reductions in fuel consumption and, consequently, lower carbon emissions and air pollution. This aligns with corporate sustainability goals.
- Logistics Optimisation: ITS integration promises lower operational costs due to reduced driver delays and fuel use, and dramatically improved schedule reliability by proactively rerouting vehicles around incidents.
- Predictive Infrastructure Maintenance: ITS sensors monitor the physical wear and tear on roads and bridges in real-time. Data analytics can shift maintenance from a reactive schedule (repairing damage after it occurs) to a predictive schedule (repairing before failure), saving costs and minimising public disruption.

Benefit	ITS Advantage	Traditional Method Drawback
Efficiency & Congestion	Dynamic Route Optimisation: Reduces travel time by up to 20% by using real-time data to adjust signals and reroute traffic around incidents.	Fixed Timings: Traffic signals change regardless of traffic density, leading to unnecessary delays.
Safety	Real-time Collision Warning: V2V systems provide millisecond-latency warnings for hard braking or hazards around blind corners, reducing accident severity.	Passive Safety: Relies on driver awareness and fixed signage; no active pre-warning system.
Environmental	Reduced Fuel Consumption: Smoother traffic flow, less idling, and better route choices reduce carbon emissions and air pollution.	Excessive Idling: Stop-start traffic and prolonged waiting at signals increase fuel burn and emissions.

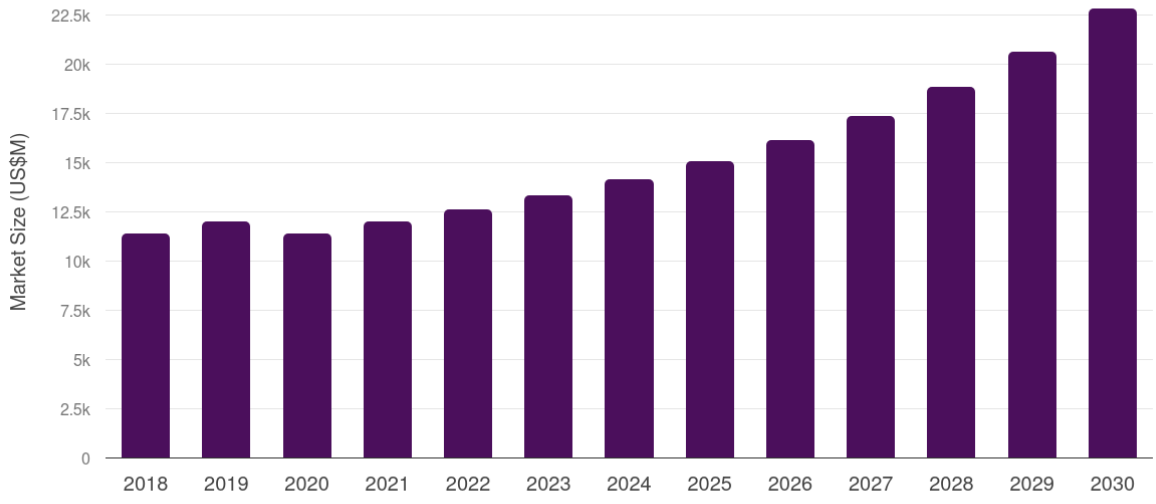
Despite the benefits, ITS implementation faces significant technical, financial, and political hurdles that management must consider.

- High Initial Cost: Deploying the necessary sensing infrastructure (cameras, roadside units, control software) requires immense upfront investment from government or public-private partnerships.
- Standardisation and Usability: Different manufacturers and regions may adopt competing communication standards (e.g., DSRC vs. C-V2X), leading to fragmentation. This can limit the effectiveness of V2X communication across borders or between different vehicle brands.
- Data Overload: The sheer volume and velocity of real-time data generated by thousands of sensors and vehicles present a Big Data challenge. Processing this data reliably with ultra-low latency is computationally intensive and costly.
- Regulatory Uncertainty: The legal and regulatory frameworks governing autonomous vehicles and liability in a V2V collision scenario are still evolving, posing legal risks for deployment.
- Public Acceptance: Implementing measures like congestion charging, detailed vehicle tracking, and invasive roadside surveillance can face significant public resistance and privacy concerns.

The complexity and high costs result in measured, steady adoption. The following figure illustrates the projected growth of the market in two key regions:

The complexity and high investment cost are reflected in the regional market adoption rates. The growth trends for Europe and Asia Pacific are illustrated in **Figure 1&2** below. The data confirms a steady, rather than exponential, growth rate, projecting a market size increase of roughly 100% in both regions over the period. While the European market starts at a slightly higher baseline, the Asia Pacific market demonstrates steeper growth post-2022, indicating a rapid acceleration in ITS infrastructure investment in that region. This trend suggests that while deployment barriers exist, regulatory commitment is leading to substantial long-term market expansion.

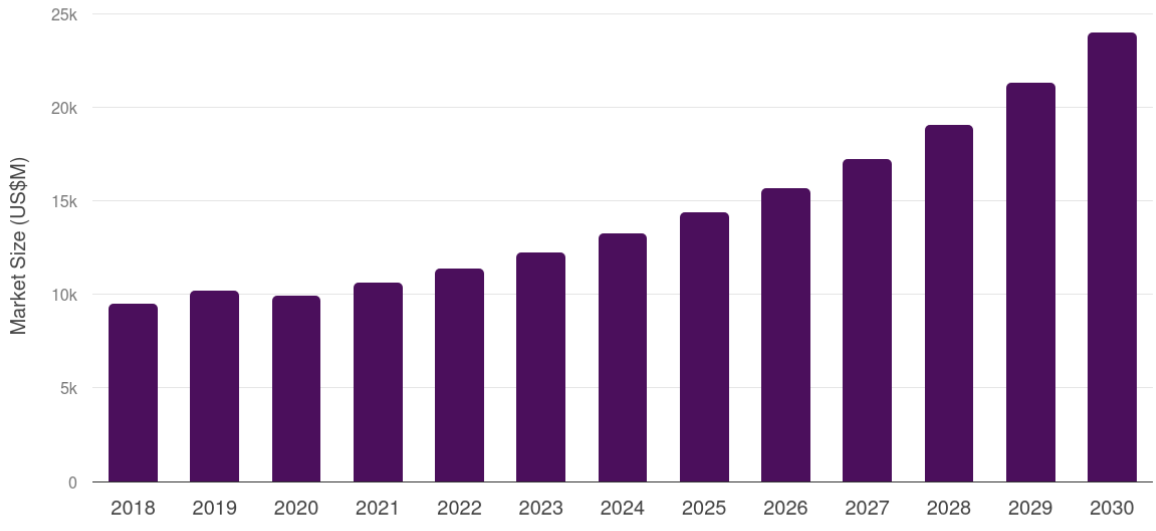
Europe intelligent transportation system market, 2018-2030



https://www.grandviewresearch.com/horizon/outlook/intelligent-transportation-system-market/europe

GRAND VIEW HORIZON

Asia Pacific intelligent transportation system market, 2018-2030



https://www.grandviewresearch.com/horizon/outlook/intelligent-transportation-system-market/asia-pacific

GRAND VIEW HORIZON

Figure 1&2: Projected Market Size of Intelligent Transportation Systems in Europe and Asia Pacific (2018–2030) This figure, generated from two charts provided by Grand View Research, illustrates that both the European and Asia Pacific ITS markets are projected to approximately double in value between 2018 and 2030.

The interconnected nature of ITS makes security the most critical consideration. An ITS network is a massive Internet of Things (IoT) ecosystem where a single compromised node can affect hundreds of vehicles and millions of commuters, potentially turning transport infrastructure into a weapon.

Security Risks

- Remote Vehicle Hacking: The most severe risk is a remote exploit that gains control over critical vehicle functions (braking, steering). This vulnerability often enters the system via external interfaces like infotainment or diagnostic ports, turning a vehicle into a potential weapon.
- GPS Spoofing and Timing Attacks: Attackers can feed false GPS coordinates or timing data to vehicles and infrastructure. This could be used to disrupt dynamic traffic light timings, cause systematic delays, or even reroute autonomous fleets into collision paths.
- Infrastructure Tampering: Roadside Units (RSUs) are vulnerable points. If an RSU is compromised, an attacker can broadcast false information (e.g., fake speed limits or congestion warnings) to entire vehicle networks, leading to chaos or accidents.
- Data Integrity: Ensuring the integrity of the sensor data is paramount. If a traffic flow input is deliberately corrupted, the Adaptive Traffic Control System will make dangerously wrong decisions, potentially causing gridlock instead of relief. Strong encryption, robust authentication protocols, and intrusion detection systems are mandatory at every layer.

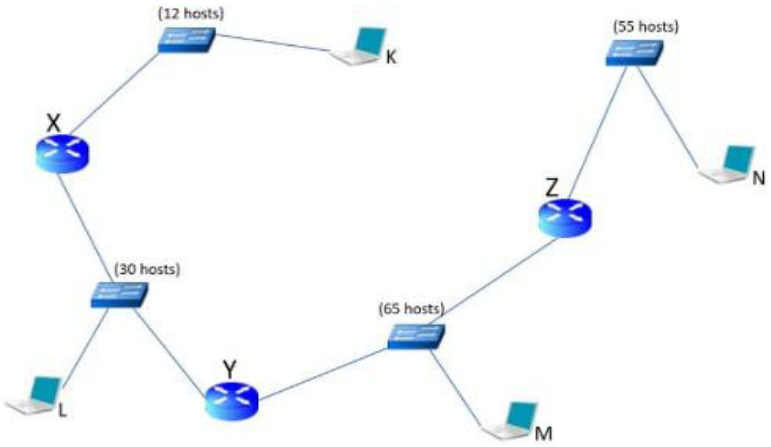
Ethical Dilemmas

- Privacy and Surveillance: ITS involves massive, continuous collection of mobility data, tracking the precise location and behaviour of drivers and vehicles. Ethical governance is mandatory to prevent the misuse of this data for non-transport related activities, such as profiling or surveillance. Public trust hinges on robust anonymisation and strict access controls.

- Autonomous Vehicle Decision-Making: For systems involving self-driving components, the developer must program decision-making algorithms for unavoidable accident scenarios (e.g., the Trolley Problem). The ethical choice (e.g., whether to prioritise the occupant's safety or the safety of external pedestrians) is complex, controversial, and requires careful regulatory oversight.

ITS represents a necessary and beneficial evolution towards smarter, safer urban environments. While the costs are high and ethical risks are complex, the long-term gains in efficiency and safety are undeniable. We recommend committing resources now to pilot a C-V2X deployment in a controlled fleet environment to build in-house expertise and develop a robust, secure data governance framework before full-scale adoption.

VLSM Subnetting Calculation



I am using Variable Length Subnet Masking (VLSM) by sorting the required subnets from largest to smallest. VLSM is used to maximise IP address efficiency by allowing subnets of different sizes within the same network, which helps avoid wasting addresses.

Network: 86.30.88.0/21

Available IP addresses: $2^{32-21} = 2^{11} = 2048$ address

Hosts required: 30 + 55 + 12 + 65 = 162 hosts

Subset D (65 hosts)

$2^6 = 64$, not enough bits

$2^7 = 128$, enough bits (7 host bits)

Subnet Mask: 255.255.255.128

Network Number: 86.30.88.0/25

First Address: 86.30.88.1

Last Address: 86.30.88.126

Broadcast Address: 86.30.88.127

Subset B (55 hosts)

2^5 = 32, not enough bits

2^6 = 64, enough bits (6 host bits)

Subnet Mask: 255.255.255.192

Network Number: 86.30.88.128/26

First Address: 86.30.88.129

Last Address: 86.30.88.190

Broadcast Address: 86.30.88.191

Subset A (30 hosts)

2^4 = 16, not enough bits

2^5 = 32, enough bits (5 host bits)

Subnet Mask: 255.255.255.224

Network Number: 86.30.88.192/27

First Address: 86.30.88.193

Last Address: 86.30.88.222

Broadcast Address: 86.30.88.223

Subset C (12 hosts)

2^3 = 8, not enough bits

2^4 = 16, enough bits (4 host bits)

Subnet Mask: 255.255.255.240

Network Number: 86.30.88.224/28

First Address: 86.30.88.225

Last Address: 86.30.88.238

Broadcast Address: 86.30.88.239

Explain what is meant by default and explicit routes

A router relies on its routing table to determine the optimal path for every incoming data packet. Within this table, the distinction between explicit routes and the default route is crucial for efficient and scalable network design. An explicit route, also known as a specific or static route, is a manually configured entry that directs traffic destined for a specific remote network to a designated next-hop router. These routes are essential for directing traffic to other known networks within a private organisation, or for providing redundancy by specifying a secondary path to a critical remote destination. Because the router performs a longest prefix match against the routing table, explicit routes, being highly specific, are checked and utilised first. The default route, often referred to as the Gateway of Last Resort, is the least specific route possible, designated by the network address and subnet mask. Its purpose is to handle all traffic for which a more specific explicit route is not found in the routing table. In typical network architecture, the default route points toward the Internet Service Provider (ISP) gateway, ensuring that traffic bound for any unknown external network (e.g., the public internet) is reliably forwarded off the local network. Without a default route, packets destined for unknown networks would be dropped, severely limiting connectivity.

Explain the differences between static and dynamic routing

The primary difference between static and dynamic routing lies in how the routing table is built, maintained, and how the network adapts to topology changes. Static routing requires the network administrator to manually enter and update every route in the router's table. This method offers high security because no routing information is advertised externally, and it consumes minimal router CPU/RAM resources and network bandwidth. However, static routing is inherently inflexible and does not scale well, it is highly error-prone in large or complex environments, as any topology change demands immediate, manual reconfiguration across all affected routers. This manual intervention leads to slow convergence times. Dynamic routing uses sophisticated protocols such as OSPF (Link-State) or RIP (Distance-Vector) to automatically discover and update network paths. Routers exchange routing information and use algorithms (e.g., Dijkstra's) to autonomously calculate the best path and maintain their routing tables. Dynamic routing is highly scalable, requires minimal administrative overhead after initial setup, and ensures rapid convergence by automatically rerouting traffic around link failures. The trade-off is higher resource consumption (CPU, bandwidth) and increased security risk, as routing information is actively broadcast across the network. Dynamic routing is the mandatory choice for large, complex, or rapidly changing internetworks, while static routing is reserved for simple stub networks or specialised scenarios like creating a manual backup path.

Compare the differences between the TCP and UDP protocols

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are the two foundational protocols of the Transport Layer in the TCP/IP suite. They reside directly above the Internet Layer (IP) and provide services that allow application processes to communicate across a network. Their fundamental difference lies in their approach to communication: TCP is connection-oriented and reliable, while UDP is connectionless and unreliable.

The defining feature of TCP is its connection-oriented nature. Before any data transmission occurs, TCP requires a formal handshake, the three-way handshake (SYN, SYN-ACK, ACK), to establish a logical, dedicated, full-duplex connection between the sender and receiver. This setup phase ensures that both parties are ready to communicate and negotiates initial sequence numbers. However, UDP is connectionless. It transmits data packets, called datagrams, without any pre-communication handshake or notification and treats each datagram independently.

TCP guarantees reliable, in-order delivery. To achieve this, it implements several mechanisms:

1. Sequencing: It assigns a sequence number to every segment, allowing the receiver to reassemble packets in the correct order, even if they arrive out of sequence.
2. Acknowledgment (ACK): The receiver sends explicit acknowledgments for successfully received segments.
3. Retransmission: If the sender does not receive an ACK within a specified timeout period, it assumes the segment was lost and automatically retransmits it.
4. Checksum: Used to detect errors in the header and data. If a corrupt packet is detected, it is discarded, and the sender must retransmit.

UDP offers no guarantees. It lacks sequencing, acknowledgments, and retransmission mechanisms. If a datagram is lost, duplicated, or arrives out of order, UDP does nothing; it is up to the receiving application to handle the error or simply tolerate the loss. For this reason, UDP is referred to as "unreliable" or "best-effort" service.

TCP uses mechanisms like the sliding window protocol for flow control. The window size advertised by the receiver dictates how much data the sender can transmit before receiving an acknowledgment, preventing a fast sender from overwhelming a slow receiver. TCP incorporates sophisticated congestion control algorithms to adjust the transmission rate based on network congestion, reducing packet loss and improving overall network efficiency. UDP provides no such mechanisms. Data is sent as fast as the application generates it, regardless of the network state or the receiver's capacity, making UDP a potential contributor to network congestion if not managed carefully by the application layer.

Due to its complex mechanisms, TCP carries a significant header overhead (typically 20 bytes) and requires processing time for connection management, sequencing, and control. UDP is lightweight and minimalist, featuring a smaller header (only 8 bytes) and no connection management time. This low overhead makes UDP significantly faster and more efficient for applications where speed is prioritised over guaranteed delivery.

Feature	**TCP (Transmission Control Protocol)**	**UDP (User Datagram Protocol)**
Connection Type	Connection-Oriented (Virtual Circuit)	Connectionless (Datagram)
Reliability	Reliable (Guaranteed delivery, in-order)	Unreliable (Best-effort; no guarantee)
Error Control	Uses Sequence numbers, ACKs, and Retransmission.	No built-in error recovery; checks only header integrity.
Flow/Congestion Control	Yes (Sliding Window and Congestion Algorithms).	No (Can lead to network congestion).
Overhead	High (Minimum 20-byte header).	Low (Fixed 8-byte header).
Applications	Web Browsing (HTTP/HTTPS), Email (SMTP/IMAP), File Transfer (FTP).	DNS Lookups, Video/Voice Streaming (VoIP), Gaming, DHCP.

Explain how TCP/IP works

The TCP/IP 4-Layer Model is the practical networking architecture that forms the foundation of the modern Internet. It evolved from the theoretical OSI 7-Layer Model and is simpler and more concise, designed to facilitate end-to-end data communication across networks. The model breaks the complex task of networking into four manageable layers, with each layer performing a specific function and passing data to the layer above or below it.

Application Layer

This is the highest layer and the one users and application processes directly interact with. Its responsibility is to provide protocols that enable communication between applications running on different hosts. The Application Layer handles data formatting, presentation, and session management. Key protocols residing here include:

- HTTP/HTTPS: For accessing the internet.
- SMTP: For sending email.
- FTP: For file transfer.
- DNS: For translating domain names to IP addresses.
- The data unit at this layer is typically called the Message or Data.

Transport Layer

The Transport Layer provides the host-to-host communication service, managing the end-to-end delivery of data between application processes. It handles the crucial function of multiplexing and demultiplexing, allowing multiple applications to share the same network connection using Port Numbers. This layer contains the two main protocols:

- TCP: Provides reliable, connection-oriented service (used for applications where data integrity is paramount).
- UDP: Provides fast, unreliable, connectionless service (used for applications where speed/latency is critical).
- The data unit is called the Segment (TCP) or Datagram (UDP).

Internet Layer

The Internet Layer is the core of the TCP/IP suite. Its primary responsibility is logical addressing and routing data packets (datagrams) across different networks. It defines the path the data should take from the source host to the destination host, potentially passing through many routers.

- The dominant protocol here is the Internet Protocol (IP), which defines the universally unique IP addresses (IPv4 and IPv6).
- Routing protocols (like OSPF or EIGRP) also operate to maintain the routing tables.
- The data unit is called the IP Datagram or Packet. The Internet Layer is connectionless and best-effort.

Network Access Layer

The Network Access Layer, sometimes called the Link Layer or Physical Layer, is the lowest layer. It is responsible for the actual physical transmission of data between devices on the same link. It combines the OSI model's Data Link and Physical layers. Its functions include:

- Defining physical addressing (e.g., MAC addresses for Ethernet).
- Managing the physical medium (cables, radio waves).
- Encoding and decoding data into electrical or optical signals.
- Protocols here include Ethernet, Wi-Fi (802.11), and ARP (Address Resolution Protocol).
- The data unit is called the Frame.

In summary, the TCP/IP model works by encapsulation, as data moves down the stack from the Application Layer, each layer adds its own header information (like a TCP port header or an IP address header). When the data reaches the destination host, the process is reversed, and the headers are stripped off as the data moves up the stack until the original data is delivered to the correct application.