EDGE COMPUTING

1. What is edge computing?

Edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers.

Edge computing is a way of setting up a network so that business applications can process data right where it's created, rather than sending it all to a far-off cloud. This is done by using a distributed network of smaller servers, and IOT devices, that are closer to the location of the data creation.

2. Explanation of first question.

"Edge computing is a distributed computing framework..."

- **"Distributed Computing":**
  - This means that the computing work (processing data, running applications) isn't done in one central location (like a traditional data centre or the cloud). Instead, it's spread out across multiple computers or devices that are connected in a network.
  - Think of it like a team working on a project: instead of everyone working in one room, they're spread out in different locations but still collaborating.
- **"Framework":**
  - A framework is a structure or set of rules and guidelines that help you build and manage a system. In this case, it's the architecture that defines how the distributed computing works at the edge.
  - It is the underlying support structure.

"...that brings enterprise applications closer to data sources..."

- **"Enterprise Applications":**
  - These are software programs that businesses use for their operations. Examples include:
    - Manufacturing control systems
    - Inventory management software
    - Remote monitoring tools
  - These are the applications that a business depends on.
- **"Data Sources such as IoT devices or local edge servers ":**
  - These are where the raw data originates. In the context of edge computing, this often refers to:
    - **"IoT Devices":** Internet of Things devices, such as sensors, cameras, and actuators, that collect and generate data.

- **"Local Edge Servers":** Smaller, less powerful servers deployed closer the data sources. They provide local processing power, storage, and networking capabilities.

3. When this edge computing introduced?

- Edge Computing was introduced in 2010.
- After introducing 5G, edge computing is growing more. Powerful processors and energy efficient devices, edge computing will become a significant technology in the market.
- The explosive growth and increasing computing power of IoT devices has resulted in unprecedented volumes of data. And data volumes continue to grow as 5G networks increase the number of connected mobile devices.

4. Why we need Edge Computing?

In cloud computing, data storage and processing occur in a centralized cloud-based data centre. Data transforms back and forth via internet from these data centres. Due to long distance travel of data, bandwidth is poor and network latency increases.

5. Why is it important?

- **Reduced Latency:** Crucial for real-time applications (e.g., autonomous vehicles, industrial automation).
- **Bandwidth Efficiency:** Less data needs to be sent to the cloud, saving on bandwidth costs.
- **Improved Reliability:** Even with intermittent cloud connectivity, edge devices can function.
- **Enhanced Privacy:** Sensitive data can be processed locally, reducing the risk of exposure.

6. What will be the result of edge computing introduced in a project?

If data centre is created near the data generating source, then

- network latency will be reduced
- network's bandwidth will be optimised
- data processing time will be reduced
- sensitive data processed in local will be secured and privacy is ensured.

7. What is network latency?

Network Latency:

- Network latency is the delay or lag that occurs when data travels from one point to another over a network.
- Essentially, it's the time it takes for a data packet to reach its destination.
- Latency is typically measured in milliseconds (ms) .[1]

- High latency results in noticeable delays, which can negatively affect real-time applications like online gaming, video conferencing, and VoIP calls.[4]
- Low latency is crucial for applications that require immediate responses.[5]
- **Factors that affect Latency:**
    - Distance: The farther the data travels, the higher the latency.[6]
    - Network congestion: High traffic can slow down data transmission.[7]
    - Routing: Inefficient routing can increase the number of hops and delays.[8]
    - Hardware and software: The quality of network equipment and software can also play a role.[9]

Network Bandwidth:

- Network bandwidth refers to the maximum amount of data that can be transmitted over a network connection in a given period.[10]
- It represents the capacity of the network.[11]
- Bandwidth is measured in bits per second (bps) or its multiples, such as kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps).[12][13]
- **Impact:**
    - High bandwidth allows for the transmission of more data simultaneously, which is essential for activities like streaming high-definition video, downloading large files, and transferring large amounts of data.[14]
    - Low bandwidth can lead to slow downloads, buffering, and poor performance.[15]
- **Factors that affect Bandwidth:**
    - Network infrastructure: The type of network cables, routers, and switches used.
    - Internet service provider (ISP): The capacity of the ISP's network.[16]
    - Network congestion: High traffic can reduce available bandwidth.[17]

In simple terms:

- **Bandwidth** is like the width of a pipe: a wider pipe can carry more water at once.[18]
- **Latency** is like the time it takes for the water to travel through the pipe.

Both bandwidth and latency are important for network performance, but they affect different aspects of data transmission.[19]

Reference:

- https://www.classace.io/answers/demonstrate-understanding-of-the-lan-bandwidth
- What is Latency? - Latency Explained - AWS
- What Is Latency? | IBM
- Network Latency: Understanding the Impact of Latency on Network Performance | Kentik
- What is low latency and why is it needed? - Neos Networks
- Network performance: Bandwidth and latency | Google Cloud Skills Boost
- Network Latency - Common Causes & How to Fix Them
- What is Latency? Ways to Improve Network Latency
- Network Bandwidth: What Is Bandwidth in Networking? - IT Glossary | SolarWinds

- Understanding Network Bandwidth: Definition, Importance & Impact | Performance Networks
- How to improve download speed: What it is and how to make it better – Microsoft 365
- What is network bandwidth? | LogicMonitor
- Key Factors That Affect Your Network Performance | M247
- Cisco Blog Detail
- Latency vs Bandwidth: the Key Differences

8. What does a good edge computing model possess or how can it be identified?

An effective edge computing model should address network security risks, management complexities and the limitations of latency and bandwidth. A viable model should help you:

- Manage your workloads across all clouds and on any number of devices
- Deploy applications to all edge locations reliably and seamlessly
- Maintain openness and flexibility to adopt to evolving needs
- Operate more securely and with confidence

9. What are the varieties of edge computing?

- cloud edge
- IoT edge
- mobile edge

10. What are the key capabilities of edge computing?

Key Capabilities of Edge Computing:

1. **Massive, Efficient Software Updates:**
    - Imagine needing to update software on thousands of devices spread across a city or factory. Edge computing lets you do this quickly and automatically, without needing a huge IT team running around.
    - **Think of it as:** Easily updating apps on thousands of phones, but for industrial machines or city sensors.
2. **Flexible and Adaptable Technology:**
    - Because there are so many different types of devices (sensors, cameras, machines), edge computing uses open-source technology. This means it can work with almost anything and you're not locked into one company's system.
    - **Think of it as:** A universal adapter that can connect to any device.
3. **Strong Security:**
    - Edge computing helps make sure that the right software is running on the right device, and that everything is secure. You can set rules and policies to protect your data.
    - **Think of it as:** A security guard that makes sure only authorized people and programs are allowed in.

4. **Reliable and Expert Support:**
    - Implementing edge computing can be complex, so you need a partner with experience. They can help you set up and manage your system, and make sure it's working at its best.
    - **Think of it as:** Having a skilled guide to help you navigate a complicated project.

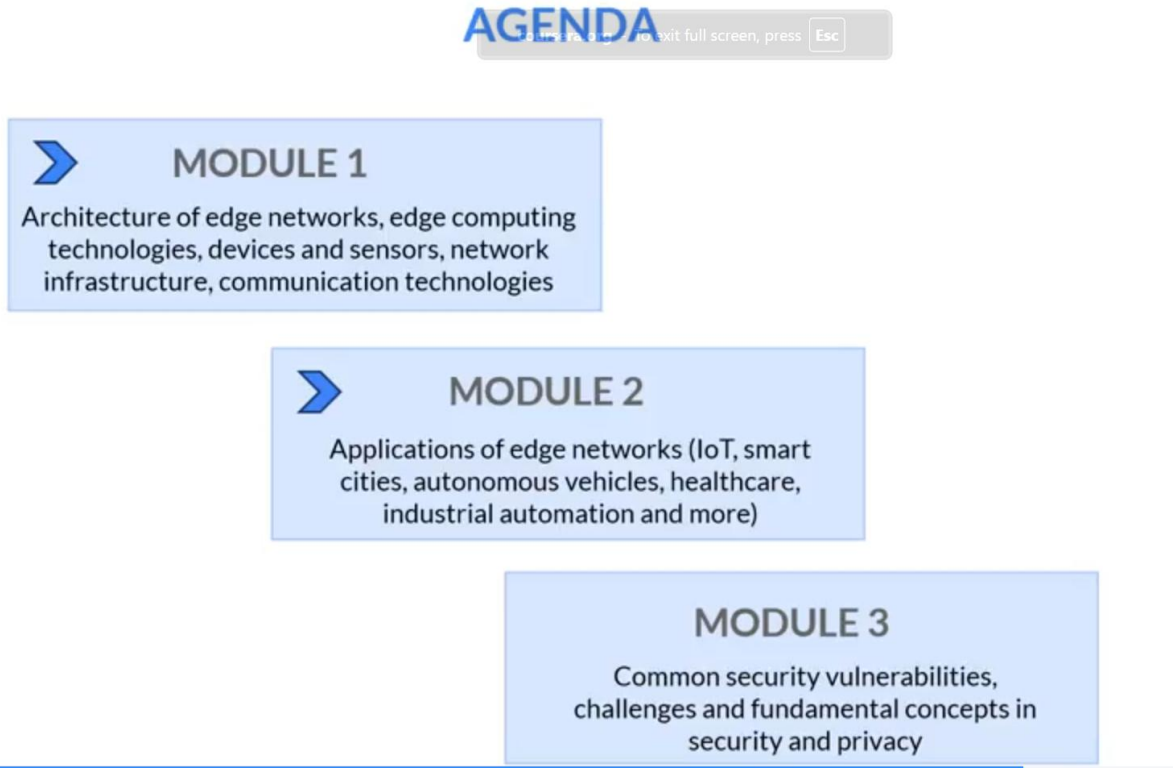
Essentially, edge computing allows you to manage a large amount of devices, and data processing, that are located far from a centralized data centre, in an efficient, secure, and scalable way.

Reference:

- What Is Edge Computing? | IBM

Edge Computing Course: Edge Computing Fundamentals | Coursera

11. Agenda of the course:



12. What will I learn in this course?

- Upon completion, learners will be able to:
- identify key architectural components of edge computing networks
- compare various types of devices and sensors utilized in edge computing
- identify challenges associated with edge networks
- compare key principles of cybersecurity
- identify potential security vulnerabilities in edge networks

- list security protocols
- explain data privacy and confidentiality

13. what are the modules and what they cover, what I am supposed to dive deep into?

- In Module 1, you build the foundation by exploring **edge computing architecture**, communication technologies, and the devices that power them. From edge nodes and gateways to lightweight protocols like **MQTT** and **CoAP**, you master the components needed to optimize real-time data processing and reduce network congestion.
- In Module 2, the narrative intensifies as you delve into edge applications across healthcare, IoT, automation, and smart cities. You confront unique challenges, from safeguarding patient data in hospitals to synchronizing distributed data in industrial systems. Privacy and security concerns take centre stage, pushing you to develop innovative solutions to protect sensitive information and ensure operational efficiency.
- Finally, Module 3 places you at the heart of the action, defending edge networks against sophisticated threats. Armed with cybersecurity principles, you tackle vulnerabilities like **device tampering** and **DDoS attacks**, deploy secure protocols such as **TLS** and **SSH**, and implement advanced measures like **Two-Factor Authentication** and **Single Sign-On** to protect both data and users.

14. Key terms to learn:

- edge devices, edge data centres, edge Computing software, network connectivity, quality of service, distributed data management, edge to cloud integration, and management and monitoring tools.

15. What is edge computing?

- Edge computing is a distributed computing paradigm that processes data closer to the data source, reducing the need for centralized cloud computing.
- The word "paradigm" highlights the change in the way computing is done, the word "framework" highlights the structure that allows the change to happen.
- This proximity to data sources, such as IoT devices and sensors, enables real-time data analysis and actions, leading to improved responsiveness and efficiency.
- Edge devices are small computing devices placed close to data source like sensors, cameras or variables. They process data locally, reducing latency, and improving responsiveness. Edge devices play a critical role in enabling efficient and rapid data processing right where it's needed most. An edge data centre is a compact and self-contain

16. What are the 3 tiers of edge computing?

There are three tiers to edge computing,

- The first layer: the sensors and internet of things, IoT devices, collect and perform some basic processing on raw data.

- The middle layer: consists of edge nodes and servers. They are located strategically near the devices in order to perform higher-level processing and decision-making.
- The third layer: the cloud or central data centre takes care of source-intensive tasks like advanced analytics, machine learning, and long-term data storage that may not be practical at the edge.

17. How the 3 tiers work together?

From the initial data collection to the final analysis and storage:

1. The First Layer: Sensors and IoT Devices (Data Collection and Basic Processing)

- **What Happens:**
  - This is where data originates. Sensors (temperature, motion, light, etc.) and IoT devices (smart cameras, industrial machines, etc.) gather raw data from the physical world.
  - These devices often have limited processing power, so they perform only basic tasks:
    - Data collection: Gathering the raw information.
    - Simple filtering: Removing noise or irrelevant data.
    - Basic aggregation: Combining data points.
    - Sometimes very basic analysis.
- **Example:**
  - A smart traffic camera detects a car passing by. It records the time, speed, and a snapshot of the license plate. It might filter out blurry images or perform a basic check for excessive speed.
- **Output:**
  - Filtered and pre-processed data is sent to the next layer.

2. The Middle Layer: Edge Nodes and Servers (Local Processing and Decision-Making)

- **What Happens:**
  - Edge nodes and servers are located closer to the first layer, providing more computational power.
  - They perform more advanced processing:
    - Data aggregation and analysis: Combining data from multiple devices.
    - Real-time decision-making: Triggering actions based on immediate data.
    - Local data storage: Temporarily storing data for quick access.
    - Application execution: Running applications that require low latency.
  - This is the layer where time sensitive actions are taken.
- **Example:**
  - The edge server receiving data from the traffic camera analyzes the speed data, compares it to speed limits, and triggers a signal to a traffic light to adjust its timing if there's congestion. It may also send an alert to traffic management if a vehicle is speeding excessively.
- **Output:**

- Processed data and decisions are sent to the cloud, and/or actions are taken locally.

3. The Third Layer: Cloud or Central Data Centre (Advanced Analytics and Long-Term Storage)

- **What Happens:**
  - The cloud or central data centre handles resource-intensive tasks:
    - Advanced analytics: Running complex algorithms and machine learning models.
    - Long-term data storage: Archiving data for historical analysis and compliance.
    - Global data aggregation: Combining data from multiple edge locations.
    - Model training.
  - This is where the "big picture" analysis happens.
- **Example:**
  - The cloud analyzes traffic patterns from multiple edge locations to optimize traffic flow across the entire city. It also trains machine learning models to predict future traffic congestion. The cloud stores historical traffic data for urban planning and infrastructure development.
- **Output:**
  - Insights and models are sent back to the edge for improved local decision-making.

Flow of Information:

1. **Data Collection:** Sensors and IoT devices gather raw data.
2. **Local Processing:** Edge nodes and servers perform real-time analysis and decision-making.
3. **Cloud Analysis:** The cloud handles complex analytics and long-term storage.
4. **Feedback Loop:** Insights and models from the cloud are sent back to the edge to improve local performance.

This tiered approach allows for efficient data processing, reduced latency, and improved overall system performance.

18. What is an edge device?

- Edge devices are small computing devices placed close to data source like sensors, cameras or variables.
- They process data locally, reducing latency, and improving responsiveness.
- Edge devices play a critical role in enabling efficient and rapid data processing right where it's needed most.

19. What is edge data centre?

- An edge data centre is a compact and self-contained facility placed closer to the edge devices, often within the proximity of the end users or data sources.

- It acts as a bridge between the edge devices and the cloud, providing more computing power and storage at the edge of the network.
- Think of it as the mini data centres, catering specifically to needs of localized area, ensuring faster data processing, and more seamless experience of users.

20. What is edge computing software?

- Edge computing software, also known as edge computing platforms, ties everything together.
- It includes various tools and frameworks that facilitate data processing, analytics, and application deployment on edge devices and edge data centres.
- These software solutions allow developers to create applications that leverage the power of edge computing, enhance performance and user experience.
- They empower businesses to make real-time decision based on data insight collected from the edge, leading to more efficient operations and services.

21. Flow of data:

Data source (GPS or camera) -> Edge Device (Smartphone, does 1st level processing) -> Edge Data centre (captures data & edge computing s/w in this data centre will do the 2nd level processing)

22. What is edge node, edge server, edge data centre, and a data centre

It's important to differentiate these terms, as they represent different levels of computing infrastructure within the context of edge computing. Here's a breakdown:

1. Edge Node:

- This is a broad term that can refer to any device or point in the network where processing occurs closer to the data source.[1]
- It can encompass a wide range of devices, from simple IoT sensors to more powerful edge servers.[2]
- Essentially, an edge node is any point where data is processed "at the edge" of the network, rather than in a centralized location.[3]

2. Edge Server:

- An edge server is a specific type of edge node.
- It's a computer server located closer to end-users or data sources than traditional data centres.[4]
- Edge servers are designed to handle data processing, storage, and application execution locally, reducing latency and improving performance.[5]
- These servers are more powerful than basic IoT devices and are capable of running more complex applications.[6]

3. Edge Data Centre:

- An edge data centre is a smaller, localized data centre that brings computing resources even closer to end-users.[7]

- These data centres are strategically placed to minimize latency and improve the delivery of services.[8]
- They are smaller than traditional data centres and are often deployed in locations like:
    - Cell towers
    - Retail stores[9]
    - Industrial facilities
- They provide a location for many edge servers to operate from.

4. Data Centre:

- A data centre is a large, centralized facility that houses computer servers, storage systems, and networking equipment.[10]
- Traditional data centres are designed to handle large volumes of data and provide centralized computing resources.[11]
- They are typically located in purpose-built facilities and are used to support a wide range of applications and services.[12]
- They are normally very large-scale operations.

Key Differences:

- **Location:** Edge nodes, edge servers, and edge data centres are located closer to end-users or data sources, while traditional data centres are centralized.[13]
- **Scale:** Edge data centres are smaller than traditional data centres, and edge servers are less powerful than those found in large data centres.[14]
- **Purpose:** Edge computing infrastructure is designed to reduce latency and improve performance for real-time applications, while traditional data centres are designed for large-scale data processing and storage.[15]

In simple terms, think of it as a scale of processing power and location. An IOT device has the least power, and is the closest to the data source. An edge server has more power, and is located near IOT devices.[16] An edge data centre houses many edge servers. And a data centre is a very large building that houses very many powerful servers.[17]

Reference:

- What is an Edge Node? | Cribl Glossary
- Edge computing is transforming the way we process data
- What Is an Edge Server? | Akamai
- What is an Edge Server? | Supermicro
- Edge Computing for IoT
- What is an Edge Datacentre | Glossary | HPE India
- What Is an Edge Data Centre? - Interconnections - The Equinix Blog
- Retail store transformation with edge
- What is a Data Centre? - Cloud Data Centre Explained - AWS
- Data centre - Wikipedia
- Edge Data Centres: A Comprehensive Guide
- Edge Computing Guide: Transforming Real-Time Data Processing

- Inside a Data Centre with 90,000 Servers - YouTube

23. Flow of data in a typical client-server model:

Client (phone – NIC: digital signals -> modulated signals) -> (through cellular data / phone Wi-Fi / on radio waves) -> ISP (Airtel Network) -> internet -> server / data centre.

1. **The Client (Your Device):**
   - This is the device you're using to access the internet or a network. It could be your:
     - Computer
     - Smartphone
     - Tablet
   - When a request is initiated, then the application data is converted into modulated radio waves.
   - Application data -> TCP/IP layering -> data packets -> NIC modulation -> modulated radio waves.

2. **Modulated radio waves to ISP:**
   - **Wi-Fi Connection:** Via a Wi-Fi router.
   - **Cellular Data Connection:** Via a cellular tower.
   - **Wi-Fi:** Involves a Wi-Fi router to handle local network routing and a modem (if needed) to modulate signals for transmission over cable or phone lines.
   - **Cellular:** Bypasses your local network and connects directly to the ISP's cellular network.
   - **Fibre:** Bypasses the traditional modem, and uses a fibre optic modem to convert digital signals into light pulses.[6]

3. **The Internet Service Provider (ISP):**
   - The ISP is the company that provides you with internet access.
   - **What Happens:**
     - Your ISP's network receives the data packets from your router.
     - It routes the packets through its network to the destination server.
     - This routing involves multiple hops through various routers and networks.

4. **The Server (Where the Data Resides):**
   - A server is a powerful computer that stores and provides data or services.
   - **What Happens:**
     - The server receives the data packets from your ISP.
     - It processes your request (e.g., retrieves the webpage you requested).
     - It sends the response (the webpage) back to your device, following the same path in reverse.

5. The Data Centre:

- Servers are often housed in data centres, which are facilities designed to provide reliable power, cooling, and network connectivity.
- Data centres can be owned by:
    - Cloud providers (e.g., AWS, Google Cloud, Azure)
    - Companies that host their own servers

24. How application data is converted into modulated radio waves?

- You initiate a request (e.g., typing a website address, opening an app).
- Break the data into smaller chunks
- Adding headers to each chunk, which contain information like the source and destination IP addresses, port numbers, and sequence numbers.
    - The above 2 steps are part of the TCP/IP protocol suite, which is a set of rules that govern how data is transmitted over networks.
    - Specifically, these actions happen within the transport layer (TCP) and the network layer (IP) of the TCP/IP model of the OS.
    - The process is also referred to as "encapsulation."
    - Essentially, the original application data is wrapped in layers of headers, like putting a letter inside an envelope.
    - Each layer adds its own header, providing information needed for routing and delivery.
- Once the headers are added, the resulting chunks of data are indeed considered data packets.
    - There are further lower-level processes that occur, such as the data link layer adding a trailer to the end of the packet, to help with error checking, but the main creation of the data packet occurs in the steps you mentioned.
- Your device's network interface card (NIC) sends these data packets to your local network (e.g., your home Wi-Fi router).
    - Modulation is the process of changing the characteristics of a carrier wave to encode the digital data.
    - The NIC takes the digital data (the data packets or electrical signals) and uses it to modify a carrier wave.
    - This modification can involve changing the amplitude (strength), frequency, or phase of the carrier wave.
    - These variations in the carrier wave represent the bits of data.
    - The resulting modulated carrier wave is a radio wave that can be transmitted through the air.
- So, in short, the electrical signals are turned into modulated radio waves.

25. How does the modulated radio waves reach the ISP through Wi-Fi connection?

1. **Wi-Fi Router Reception:**
   - The modulated radio waves are received by your Wi-Fi router's antenna.
2. **Router Demodulation:**
   - The router's Wi-Fi chip demodulates the received modulated radio waves back into digital data packets. This is essential for the router to understand and process the data.
3. **Router's Decision:**
   - The router examines the destination IP address in the data packets.
4. **Two Possible Paths:**
   - **Local Network Destination:**
     - If the destination is another device on your local network (e.g., another computer, a smart TV), the router forwards the data packets directly to that device.
     - This stays within your home network.
   - **Internet Destination:**
     - If the destination is on the internet (e.g., a website, a remote server), the router proceeds to the next steps.
5. **NAT (Network Address Translation):**
   1. The router performs NAT to replace your device's private IP address (used within your home network) with your public IP address (assigned by your ISP).
   2. This is crucial because:
      1. Private IP addresses are not routable on the internet.
      2. NAT allows multiple devices on your local network to share a single public IP address.
      3. The router also makes a record of the private IP address and port that made the request, so that when the server responds, the router knows where to send the data back to.
      4. NAT is a routing function performed by the router.
      5. It happens after demodulation and before the data packets are sent to the modem/fibre connection.
      6. It's essential for enabling communication between devices on your local network and the internet.
2. **Internet Connection Paths (if destination is the internet):**
   1. **Modem Connection (Cable or DSL):**
      1. The modem receives the NATed data packets from the router.
      2. **Modulation (Cable/DSL):**
         1. **Cable Modem:** If you have a cable connection, the cable modem modulates the digital data packets into radio frequency signals that can be transmitted over the coaxial cable.

2. **DSL Modem:** If you have a DSL connection, the DSL modem modulates the digital data packets into analog signals that can be transmitted over telephone lines.
3. **Transmission:** The modem transmits the modulated signals to your ISP.

2. **Fibre Connection:**
    1. The router forwards the NATed data packets to your Fibre Optic modem.
    2. The fibre optic modem converts the electrical signals to light pulses, for transmission over fibre optic lines to your ISP.

3. **ISP (Internet Service Provider):**
    - The ISP receives the modulated signals (cable, DSL, or light pulses) from the modem.
    - The ISP demodulates the signals back into digital data packets.
    - The ISP's routers forward the data packets through their network to the internet.

26. How does the modulated radio waves reach the ISP through Cellular connection?

1. **Cellular Tower:**
    - The cellular tower's antenna receives the modulated radio waves from your device.[5]
    - The tower demodulates the radio waves back into digital data packets.
    - **Transmission:** The tower transmits the data packets to the ISP's core network.
2. **ISP (Cellular Network Provider):**
    - The ISP's core network receives the data packets.
    - The ISP's routers forward the data packets through their network to the internet.

27. How ISPs handle different connection types (cable, DSL, Fibre, Cellular)

1. Receive modulated signals at ISP (Physical Layer Differentiation):

- **Different Physical Interfaces:**
    - ISPs have different physical interfaces to receive different types of signals.
    - For cable connections, they have interfaces for coaxial cables.
    - For DSL connections, they have interfaces for telephone lines.
    - For fibre connections, they have optical receivers.
    - For cellular connections, they have cellular towers and base stations.
    - These physical interfaces are designed to handle specific signal types.
- **Signal Characteristics:**
    - Each connection type (cable, DSL, fibre, cellular) has distinct signal characteristics (frequency, modulation scheme, etc.).
    - The ISP's equipment can identify these characteristics to determine the connection type.

2. **Demodulate physical layer signal into data packets at various connections:**
    - Cellular:
        - Cellular Towers have specialized receivers and demodulators for cellular radio frequencies.
        - Cellular towers receive radio waves, demodulate them, and forward the data to the ISP's core network.
        - The ISP's cellular network handles authentication and mobility management.
        - The data packets are then routed to the internet.
    - Wi-Fi (via Modem/Fiber):
        - Cable/DSL Modems:
            - If you're using a cable or DSL modem, it modulates the digital data from your router into signals suitable for transmission over cable or phone lines.[1]
            - Cable ISPs (CMTS) use cable modems and headend equipment to demodulate radio frequency signals from coaxial cables.
            - DSL ISPs use DSLAMs (Digital Subscriber Line Access Multiplexers) to demodulate analog signals from telephone lines.
            - At the ISP's end, their equipment (CMTS for cable, DSLAM for DSL) demodulates those signals back into digital data packets.
        - Fiber Modems:
            - Fiber ISPs use optical receivers to convert light pulses into digital signals.
            - Fiber modems convert digital data into light pulses.[2]
            - At the ISP's end, optical receivers convert the light pulses back into digital data.
            - Then routes the data packets to the internet.
    - Key difference:
        - Medium of Transmission:
            - The key difference lies in the medium of transmission.
            - Cellular data uses radio waves directly to the tower, which handles the initial demodulation.[3]
            - Cable, DSL, and fiber connections use different physical media (coaxial cable, phone lines, fiber optic cables), requiring modems to adapt the digital data to those media.[4]
        - Point of Demodulation:
        - In cellular, the demodulation happens at the edge of the ISP's network (the tower).
        - In cable, DSL, and fiber, the demodulation happens closer to the ISP's core network.
    - In essence:

- ISPs use a combination of physical layer interfaces, signal analysis, and network layer protocols to differentiate and process incoming signals.
- This allows them to handle diverse connection types and route data packets efficiently.

3. **Network Layer Differentiation:**
   - **IP Addressing and Routing:**
     - Once the physical layer signals are demodulated into data packets, ISPs use IP addressing and routing protocols to determine the destination IP address.
       - Manage network traffic and ensure efficient delivery.
       - Cellular data, Wi-Fi, and wired connections all use IP protocols.
       - However, the way IP addresses are assigned and managed can differ.
       - For example, cellular networks often use different IP address ranges than fixed broadband networks.
     - Route the packets through their network and to the internet.
   - **Routing Tables:**
     - ISPs' routers maintain complex routing tables. These tables map IP addresses or IP address ranges to specific network paths.
       - These tables help the routers forward packets to the correct destination, regardless of the connection type.
     - The router looks up the destination IP address in its routing table.
   - **Next Hop:**
     - Based on the routing table, the router determines the "next hop," which is the next router or network device that should receive the data packets.

4. **Packet Forwarding:**
   - **Forwarding the Packets:**
     - The router forwards the data packets to the next hop.
     - This process is repeated at each router along the path to the destination.
5. **Internet Backbone:**
   - **Traveling the Internet Backbone:**
     - The data packets travel through the internet backbone, which is a high-speed network of interconnected networks.
     - The backbone consists of high-capacity fiber optic cables and powerful routers.
6. **Destination Network:**
   - **Reaching the Destination Network:**
     - Eventually, the data packets reach the destination network, which is the network where the destination server or device is located.
     - This may be another ISP, a corporate network, or a cloud provider's network.

7. **Destination Device:**
    - **Delivery to the Destination Device:**
        - The final router in the destination network delivers the data packets to the destination device.
        - The destination device's operating system reassembles the packets into the original data.
8. **Response (if applicable):**
    - **Sending a Response:**
        - If the request requires a response (e.g., loading a webpage), the destination device sends a response back to the originating device, following the same path in reverse.

28. What is a router?

- A router is a networking device that forwards data packets between computer networks.
- It analyzes the destination IP address in the data packets to determine the best path for them to travel.
- It acts as a gateway, connecting different networks (e.g., your home network to the internet).

29. What is the ultimate purpose of the routers?

- **Wi-Fi routers** do perform demodulation to convert received radio waves into data packets.
- **Core routers** within an ISP's network or the internet backbone primarily focus on forwarding data packets based on IP addresses.
- The primary purpose of a router is to route traffic.

30. Routing Vs Forwarding

- **Routing** is the process of determining the best path for data packets.
- **Forwarding** is the actual act of sending the data packets along that path.
- Core routers within the internet primarily perform forwarding based on routing tables.

31. Internet Vs networks

- A network is a collection of interconnected devices that can communicate with each other. It facilitates the sharing of resources and information between these devices.
- These devices can be Computers (desktops, laptops), Smartphones, Tablets, Servers, Routers, Switches, Modems, Printers, Smart TVs, IoT devices (sensors, cameras, etc.
- The internet is a network of networks.
- It can be imagined as interconnected networks, with various levels of nesting.
- This hierarchical structure allows for scalability and efficient routing.

32. What is a Network Interface Card (NIC)?

- A Network Interface Card (NIC) is a hardware component that allows a device (like your computer or smartphone) to connect to a network.
- It's the physical interface between your device and the network cable (or Wi-Fi antenna).
- It translates the digital data from your device into signals that can be transmitted over the network and vice versa.
- In modern devices, especially smartphones and laptops, Wi-Fi capabilities are also integrated into the NIC.
- Think of it as the device that allows your computer to speak the language of the network.

33. Is Internet Service Provider (ISP) mean like Airtel, Jio, etc...?

- Yes, exactly. Airtel, Jio, Verizon, Comcast, etc., are all examples of Internet Service Providers (ISPs).
- They provide the infrastructure and services that allow you to access the internet.

34. Is the internet network also a network? Which we call as the internet? That we paid for online services to Airtel, Reliance, or Jio?

- Yes, the internet is a vast, global network of interconnected networks.
- It's a "network of networks."
- When you pay for internet service from Airtel, Jio, etc., you're paying for access to their network, which is then connected to the larger internet.
- They are essentially providing you with a "gateway" to the internet.
- The internet itself is not owned by any one company.

35. What is a DSL connection?

DSL (Digital Subscriber Line):

- DSL is a type of internet connection that uses existing telephone lines to transmit data.
- Older telephone lines were designed to carry analog voice signals. DSL technology allows digital data to be transmitted over those same lines.
- That's why a DSL modem is needed: it converts the digital data from your router into analog signals that can travel over the phone lines.

36. My phone doesn't contain any cable, so why the data in the router needs to be changed into an analogous signal?

1. Traditional Telephone Lines:

- These are the copper wires that were originally laid down for analog voice calls.

- They were designed to carry analog signals, which are continuous waves that represent sound.
- Devices that used these lines:
    - Landline telephones (the old-fashioned phones plugged into the wall)
    - Fax machines
    - Older dial-up modems (for internet access)
    - DSL modems

2. Analog vs. Digital Signals:

- **Analog:**
    - Continuous waves that vary in amplitude and frequency.
    - Think of the sound waves produced by your voice.
    - Traditional telephone lines carry analog signals.
- **Digital:**
    - Discrete values represented by bits (0s and 1s).
    - Computers and modern devices use digital signals.
    - Cellular data, Wi-Fi, and fibre optic connections use digital signals.

3. DSL and Analog Conversion:

- **DSL (Digital Subscriber Line):**
    - DSL technology allows digital data to be transmitted over traditional telephone lines.
    - However, because the phone lines were designed for analog signals, the digital data needs to be converted.
    - This is where the DSL modem comes in. It:
        - Converts digital data from your computer or router into analog signals for transmission over the phone line.
        - Converts analog signals from the phone line back into digital data for your devices.
- **Why Your Phone Doesn't Need Analog Conversion:**
    - **Cellular Data (4G, 5G):**
        - Uses radio waves to transmit digital data.
        - Radio waves are a form of electromagnetic radiation, but they carry digital information, not analog voice signals.
        - Your phone's cellular modem handles the conversion between digital data and radio waves.
    - **Wi-Fi:**
        - Also uses radio waves to transmit digital data.
        - Your phone's Wi-Fi adapter handles the conversion between digital data and radio waves.
    - **No Traditional Phone Lines:**
        - Your smartphone doesn't connect to traditional copper telephone lines.

        - Therefore, there's no need for analog conversion.

In simpler terms:

- Imagine a highway.
    - Traditional phone lines are like an old, narrow highway designed for horse-drawn carriages (analog signals).
    - DSL is like adding a new lane to that highway for modern cars (digital data), but you still need a special vehicle (DSL modem) to convert between the two.
    - Cellular data and Wi-Fi are like entirely new, modern highways designed for high-speed cars (digital data) from the start.

Reference:

- Understanding DSL: How Digital Subscriber Lines Function and Their Key Benefits
- Evolution of Business Internet Services: From DSL to Fibre
- Best Internet Connection for Small Businesses: Pros and Cons of Different Types | actcorp
- Does My Small Business Need Backup Internet Service? | Teal
- Digital subscriber line - Wikipedia
- " Experience Faster Internet with a DSL Modem Connection" | Lenovo US
- High-speed fibre grows as DSL declines - report - Optical Connections News

37. While NIC can translate the digital data from your device into signals that can be transmitted over the network and vice versa. but if the phone's digital signal can be sent via radio waves, then why the digital data should be translated? what signal doesn't change into? also translation means conversion right? and here by digital data into signal you mean digital data into digital signal where the natural human language is converted into bits (0's and 1's)?

1. "Translation" in the Context of NICs:

- "Translation" here essentially means "conversion." But it's not simply about changing from human language to bits. It's about changing the form of the digital data to match the medium of transmission.
- Here's a more accurate way to think about it:
    - The NIC takes the digital data (bits) that your device generates and transforms it into a modulated signal that can be sent over the network medium.
    - "Modulation" is the process of encoding digital information onto a carrier wave.

2. Why the encoding needs in short please

In short, encoding digital information onto a carrier wave (modulation) is necessary because:

- Efficient Transmission:
    - Raw digital signals (like square waves) don't travel well over long distances, especially through radio waves.
    - Carrier waves, with their specific frequencies, allow for more efficient and reliable transmission.
- Multiplexing:
    - Modulation allows multiple signals to be transmitted simultaneously over the same medium (e.g., radio frequencies) by assigning different frequencies or modulation schemes.
- Range and Interference:
    - Modulation helps to improve the range of transmission and reduce interference from other signals.
    - It allows the signal to be tuned to a frequency that travels well.
- Compatibility:
    - It allows the digital data to be made compatible with the physical medium that it must travel through.

3. Why Digital Data Needs to Be "Translated" (Modulated):

- **Not All Digital Signals Are Created Equal:**
    - While both your device and the network use digital data, the way that data is represented electrically or electromagnetically needs to be compatible with the physical medium.
    - For example:
        - Inside your computer, digital data is represented as electrical pulses on wires.
        - Over Wi-Fi, digital data is represented as variations in radio waves.[1]
        - Over ethernet cable, digital data is represented as variations of electrical signals.
    - Therefore, the NIC needs to convert the internal digital representation into the appropriate signal for the network medium.
- **Radio Waves and Modulation:**
    - In the case of Wi-Fi or cellular data, the NIC uses modulation techniques to encode the digital data onto radio waves.
    - This involves changing the amplitude, frequency, or phase of the radio waves to represent the bits.[2]
    - This modulation is necessary because raw digital pulses cannot travel efficiently over radio waves.
- **Ethernet and Electrical Signals:**
    - In the case of ethernet cable, the NIC changes the voltage of the electrical signals that are sent over the wire, to represent the binary 1's and 0's.

3. What Signal Doesn't Change Into?

- The fundamental information (the bits) doesn't change.

- The NIC doesn't change the content of the data, but it changes the form of the data.
- It's like taking a message written in English and translating it into Morse code. The message itself remains the same, but the way it's represented changes.

4. Human Language to Bits:

- That conversion (human language to bits) happens at a higher level of the software stack, within the operating system and applications.
- The NIC deals with the lower-level physical transmission of those bits.

In summary:

- The NIC's "translation" is about modulating digital data into a form suitable for the network medium.
- It's not about changing the content of the data, but about changing its representation.
- The type of modulation depends on the network medium (Wi-Fi, Ethernet, etc.).

Reference:

- https://www.britannica.com/story/how-does-wi-fi-work
- https://www.taitradioacademy.com/topic/how-does-modulation-work-1-1/

38. What is the difference between data centre, cloud and server?

1. Server:

- **Definition:**
  - A server is a computer or software program that provides services to other computers or devices (clients).
  - It's designed to handle requests and deliver data or resources.
  - Servers can be physical hardware or virtual machines.
- **Role:**
  - Hosts websites, applications, databases, and other services.
  - Responds to client requests.

2. Data Centre:

- **Definition:**
  - A building filled with many servers and supporting equipment (power, cooling, etc.)
  - A data centre is a physical facility that houses servers, storage systems, networking equipment, and other computing infrastructure.
  - It provides the necessary environment for these components, including power, cooling, and security.
- **Role:**
  - Provides the physical space and infrastructure to support servers and other IT equipment.
  - Ensures the reliability and availability of IT services.

3. Cloud:

- **Definition:**

    - A service that lets you access and use servers and other computing resources over the internet, often from large, distributed data centres.
    - Cloud computing is the delivery of on-demand computing services—including servers, storage, databases, networking, software, analytics,[1] and intelligence—over the internet ("the cloud").[2]
    - It's a model for delivering IT resources as a service.
- **Role**:
    - In this context, "cloud" refers to the distributed network of data centres and servers that are managed and operated as a single, cohesive infrastructure.
    - It's the overall architecture that allows for the provision of scalable and reliable computing resources.
- **Relationship**:
    - A cloud is made up of many data centres, which in turn contain many servers.
    - The "cloud" is the concept of a very large distributed data centre. It is the network of data centres.
    - Cloud providers (like AWS, Azure, and Google Cloud) operate large data centres that house the servers and infrastructure that power their cloud services.

Key Differences Summarized:

- **Server:** A piece of hardware or software (Individual machines).
- **Data Centre:** A physical facility (buildings that house these machines).
- **Cloud Computing:** The "cloud" is the interconnected network of those buildings and machines, managed as a unified infrastructure.

Reference:

- 20 Sep 2020: UPSC Exam Comprehensive News Analysis: A. GS 1 Related B. GS 2 Related C. GS 3 Related | PDF | Crispr | Deep Learning
- GMR Varalakshmi Foundation offers Free Course for Underprivileged in 'Cloud Computing'
- 05.10. Cloud Computing and Mobile Computing – Auditing Information Systems

39. Read later:

- What Is Edge Computing? Everything You Need to Know

40.