Emergence of IoT: Introduction, Evolution of IoT, Enabling IoT and the Complex Interdependence of Technologies, IoT Networking Components, Addressing Strategies in IoT.

Introduction to IoT

- **Definition**:
  - **Internet of Things (IoT)** refers to a system of interrelated physical devices embedded with sensors, software, and connectivity, enabling them to collect, exchange, and act on data without human intervention.
- **Key Features**:
  - **Interconnectivity**: Devices can communicate with each other and the cloud through internet protocols.
  - **Automation**: Many processes run without human interaction.
  - **Real-Time Data**: Sensors collect and provide real-time data for analysis and decision-making.
  - **Intelligence**: Integrated AI and analytics process data and offer smart responses.
- **Working of IoT**:
  - **Sensors/Devices**: Collect data (e.g., temperature, motion).
  - **Connectivity**: Data is transmitted to a central system via communication protocols like Wi-Fi, Zigbee, or cellular networks.
  - **Data Processing**: The cloud or local systems analyze data, often in real-time.
  - **Actions**: Systems respond, for example, turning off lights or adjusting temperatures.
- **Applications**:
  - **Smart Homes**: Devices like smart thermostats and lights automate home environments.
  - **Healthcare**: Wearables monitor health metrics and notify healthcare providers.
  - **Industrial IoT**: Factories automate processes using connected machines.
  - **Agriculture**: IoT monitors soil conditions, weather patterns, and crop health.
- **Importance**:
  - **Efficiency**: Automates routine tasks and reduces human intervention.
  - **Cost-Savings**: Helps optimize resource usage and reduce waste.
  - **Real-Time Monitoring**: Offers immediate feedback and allows quick action.
  - **Data-Driven Insights**: Helps organizations make better decisions using real-time data.
- **Challenges**:
  - **Security**: With more devices connected, the system becomes vulnerable to cyber threats.

- **Data Privacy**: Massive data collection raises concerns about personal data privacy.
- **Interoperability**: Devices from different manufacturers may use different communication protocols, which makes integration harder.
- **Energy Consumption**: IoT devices, especially those that are battery-powered, need efficient power management.

.

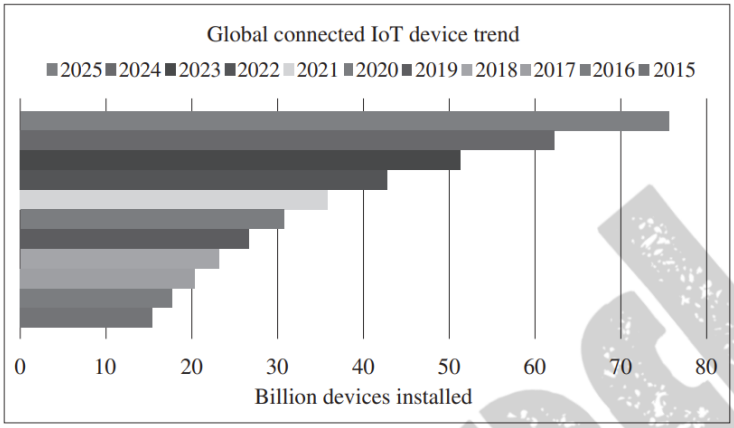
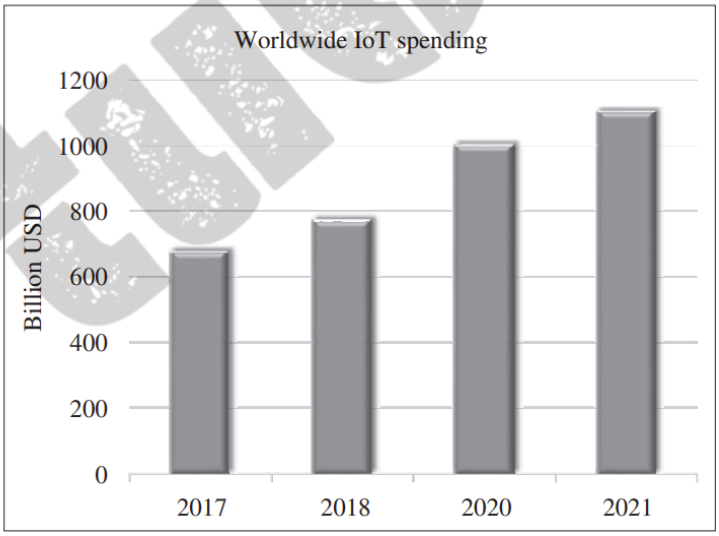


Figure 4.1 10-year global trend and projection of connected devices (statistics sourced from the Information Handling Services [7])



Evolution of IoT:

The **Internet of Things (IoT)** evolved through a series of technological advancements that laid the foundation for interconnected systems and seamless integration into everyday life. The emergence of IoT involved key developments in technology, automation, and communication that helped shape the current IoT landscape.

Technological Advancements Shaping IoT:

1. **ATM (1974)**:
    - **Automated Teller Machines (ATMs)** were the first widely used connected machines that allowed remote access to banking services. ATMs dispense cash after verifying the identity of users with a specially coded card.
    - **Significance**: The first ATM connected online in 1974, showing the potential for connecting machines to deliver services beyond human operating hours.
2. **World Wide Web (1991)**:
    - The **Web** became operational in 1991, providing a global platform for information sharing and communication.
    - **Significance**: The Web's creation enabled rapid advancements in computing and communication, laying the groundwork for connected devices to interact over the internet.
3. **Smart Meters (Early 2000s)**:
    - **Smart Meters** were among the first devices capable of remote communication with power grids, allowing utilities to monitor usage, manage billing, and allocate power more efficiently.
    - **Significance**: They pioneered the concept of connected devices that could autonomously report data back to a central system.
4. **Digital Locks**:
    - **Digital locks** represented early home automation technology, allowing remote control of locks and security systems using smartphones. Modern digital locks can lock/unlock doors, manage key codes, and add users remotely.
    - **Significance**: This laid the foundation for smart home technology, automating simple tasks in households.
5. **Connected Healthcare**:
    - **Connected healthcare** devices include wearables and monitors that link patients to hospitals, doctors, and relatives in real-time. These devices track vitals (e.g., heart rate) and send alerts for emergencies, providing continuous monitoring.
    - **Significance**: Connected healthcare sped up access to medical records and enabled quicker responses to medical issues, improving healthcare quality.

6. **Connected Vehicles**:
    - **Connected vehicles** use sensors and communication technologies to monitor systems and communicate with other vehicles, or even with external sensors. They provide self-diagnosis and can alert owners to potential system failures.
    - **Significance**: These vehicles are precursors to autonomous vehicles and smart transportation systems.
7. **Smart Cities**:
    - **Smart cities** integrate smart systems (sensors, monitors, and actuators) across urban infrastructure. This interconnection enhances city-wide operations such as traffic management, parking, energy consumption, and transportation.
    - **Significance**: Smart cities optimize urban management, improving efficiency and sustainability in public services.
8. **Smart Dust**:
    - **Smart dust** refers to tiny, microscopic computers smaller than a grain of sand, used for applications such as environmental monitoring or medical diagnostics.
    - **Significance**: Smart dust extends IoT into new areas where traditional computers cannot function, offering highly specialized sensing capabilities.
9. **Smart Factories**:
    - **Smart factories** employ IoT systems to manage and monitor plant processes, assembly lines, and operations autonomously, reducing human error and improving efficiency.
    - **Significance**: Smart factories are key to the **Industry 4.0** revolution, which emphasizes automation and data exchange in manufacturing.
10. **UAVs (Unmanned Aerial Vehicles)**:
    - **UAVs** or drones are now used in agriculture, surveying, surveillance, delivery services, stock management, and asset monitoring.
    - **Significance**: UAVs showcase the ability of IoT to support unmanned, automated systems in diverse industries.

IoT Today:

The modern IoT spans various domains such as smart cities, healthcare, manufacturing, agriculture, and more. IoT is not limited to one industry but acts as a cross-domain technology enabler, supporting multiple sectors simultaneously. Examples include:

- **Smart Parking**: IoT sensors detect available parking spaces in real-time.
- **Smart Lighting**: Street lights adjust based on traffic or pedestrian presence.
- **Environmental Monitoring**: Sensors track pollution, radiation, or flood levels.
- **Supply Chain Optimization**: IoT systems track inventory and logistics in real-time.

Technological Interdependencies in IoT:

IoT depends on several other networking paradigms, with each contributing to its success. These include:

1. **M2M (Machine-to-Machine Communication)**:
    - **M2M** enables devices and machines to communicate without human intervention, sharing updates about status, health, and tasks among connected machines.
    - **Example**: M2M is widely used in industrial automation where machines collaborate to complete tasks autonomously.
2. **CPS (Cyber-Physical Systems)**:
    - **CPS** integrates physical processes with computational feedback and actuation mechanisms, maintaining control loops (sensing, processing, and acting). Human involvement is minimal, with systems working autonomously.
    - **Example**: CPS-based smart factories optimize production processes with real-time monitoring and automation.
3. **IoE (Internet of Environment)**:
    - **IoE** focuses on reducing the environmental impact of connected technologies by promoting sustainable practices. It emphasizes energy-efficient systems, smart farming, and habitat conservation.
    - **Example**: IoE technologies are used in smart agriculture to minimize water and energy consumption.

4. **Industry 4.0**:
    - The **fourth industrial revolution** refers to the digitization of manufacturing and production processes. Smart factories rely on IoT and CPS for enhanced automation, resource management, and workforce optimization.
    - **Example**: Industry 4.0 enhances production lines with autonomous robots, data-driven decision-making, and real-time monitoring.
5. **IoP (Internet of People)**:
    - **IoP** aims to decentralize social interactions, payments, and transactions, maintaining privacy and security. It proposes limiting corporate and government control over personal data.
    - **Example**: IoP builds on decentralized technologies like **Bitcoin** to provide privacy-preserving alternatives to centralized internet services.

Comparison:

- **IoT vs. M2M**: M2M focuses on device-to-device communication, while IoT is broader, encompassing interactions between devices, people, applications, and data.
- **IoT vs. CPS**: CPS emphasizes control and feedback in a closed loop, while IoT focuses more on networking devices for data sharing and real-time monitoring.
- **IoT vs. WoT (Web of Things)**: WoT integrates IoT devices with web technologies using standards like RESTful APIs, extending IoT to the web

Aspect	IoT	M2M	CPS	WoT
Scope	Broad, connecting devices, people, and applications.	Focuses on direct device-to-device communication.	Closed-loop control of physical systems with feedback.	Web integration of IoT devices.

Core Technology	Cloud computing, wireless protocols, big data, and AI.	Cellular networks, embedded systems.	Sensors, actuators, feedback control systems.	Web technologies like RESTful APIs.
Internet Requirement	Essential; relies on IP-based networking.	Optional; uses telecom networks or private networks.	Not internet-focused; more about control systems.	Web-based interface is essential.
Data Handling	Data processed in cloud or edge environments.	Data processed locally for control or diagnostics.	Data used for real-time feedback and system adjustments.	Data accessed and controlled via the web.
Applications	Smart homes, healthcare, agriculture, etc.	Industrial automation, fleet management.	Industrial control, robotics, smart factories.	Web-based IoT device management.
Human Interaction	Minimal; most processes are automated.	Minimal, focused on machine communication.	Minimal, mostly supervisory.	Human interaction is through web interfaces.

Enabling IoT and the Complex Interdependence of Technologies

The **Internet of Things (IoT)** is a paradigm built upon a complex interdependency of technologies, including both legacy and modern systems. These technologies function across multiple layers or planes that collectively enable IoT applications.

Four Planes of IoT Paradigm

1. **Service Plane**:
    - **Components**: This layer includes the **devices (things)** and the **low-power connectivity** technologies that enable communication between devices and networks.

- **Functionality**:
  - Provides the basic setup for sensing, monitoring, and actuating IoT systems.
  - Devices could include wearables, smart appliances, vehicles, and industrial machinery.
  - Examples of low-power connectivity technologies include:
    - **Zigbee**, **Bluetooth**, **RFID**, **6LoWPAN**, **LoRA**, and **DASH**.
- **Characteristics**:
  - Utilizes protocols like **IEEE 802.15.4** for low-range, low-power communication.
  - Ensures devices can connect with nearby gateways for internet access.

2. **Local Connectivity Plane**:
   - **Components**: Responsible for distributing internet access to local IoT deployments (e.g., smart home devices).
   - **Functionality**:
     - Manages connectivity based on physical placements of devices, application domains, or service providers.
     - Manages traffic from multiple devices, merging it into a single gateway or router.
     - Helps conserve global IP addresses by assigning one global IP to multiple local devices (e.g., all devices in a smart home).
   - **Services Provided**:
     - Address management, device management, security, and sleep scheduling.
   - **Technologies**: Includes both legacy protocols (e.g., Wi-Fi, Ethernet) and modern wireless solutions.

3. **Global Connectivity Plane**:
   - **Components**: Comprises the broader internet infrastructure, including the web, cloud services, and data centers.
   - **Functionality**:

        - Enables global IoT applications by facilitating connections between devices, users, controllers, and applications.
        - Determines how, when, and where data is stored, processed, and forwarded.
    - **Key Technologies**: Includes cloud platforms, web services, and IoT management tools.
    - **Fog Computing**: This paradigm exists between local and global connectivity. It processes data closer to the source (at the edge) to reduce latency and decrease the load on the central internet infrastructure.
4. **Processing Plane**:
    - **Components**: This layer focuses on the analytics and processing of data collected from IoT devices.
    - **Functionality**:
        - Converts raw data into human-readable information.
        - Analyzes and visualizes data trends, providing actionable insights.
    - **Sub-Domains**:
        - **Intelligence**: Using AI and machine learning to derive insights from data.
        - **Data Conversion**: Cleaning and formatting data for analysis.
        - **Cognition**: Recognizing patterns and correlating them with known data.
        - **Visualization**: Creating graphs and charts for easy understanding of trends.
    - **Technologies**: Involves big data analytics, machine learning algorithms, and data visualization tools.

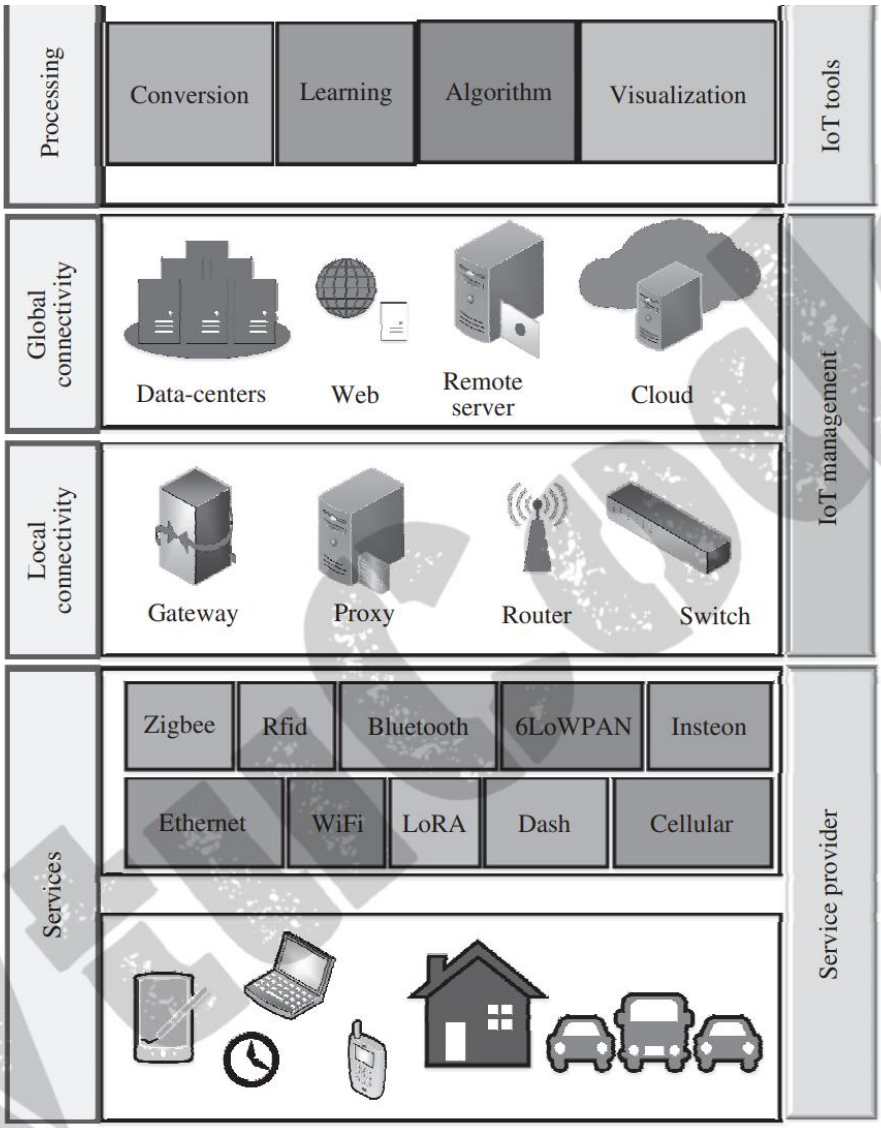


Figure 4.8 The IoT planes, various enablers of IoT, and the complex interdependencies among them

IoT Networking Components

An IoT implementation consists of several essential components that vary depending on application domains. The following are the six broad categories of IoT networking components:

1. **IoT Node**:
    - **Definition**: These are the fundamental devices within an IoT Local Area Network (LAN).
    - **Composition**: Each IoT node typically includes:
        - **Sensors**: Collect data from the environment (e.g., temperature, humidity).
        - **Processors**: Process data and control operations.

        - **Communication Radio**: Enables the node to communicate with other devices and the network.
    - **Functionality**: Nodes can directly connect to other nodes or through a gateway for communication outside the LAN. They usually possess locally unique identifiers (LU-x) for identification within the network.

2. **IoT Router**:
    - **Definition**: A networking device responsible for directing data packets between different devices within the IoT network.
    - **Functionality**:
        - Ensures proper traffic flow within the network.
        - Can be enhanced to function as a gateway, allowing it to connect multiple networks.

3. **IoT LAN (Local Area Network)**:
    - **Definition**: A localized network that allows devices to connect and communicate over a limited geographic area, typically within a single building or organization.
    - **Characteristics**:
        - Composed of short-range connectivity technologies (e.g., Wi-Fi, Zigbee).
        - May or may not be connected to the Internet.
    - **Purpose**: Facilitates communication and data exchange among IoT nodes in close proximity.

4. **IoT WAN (Wide Area Network)**:
    - **Definition**: Connects multiple IoT LANs over a broader geographic area, potentially spanning kilometers to hundreds of kilometers.
    - **Functionality**:
        - Provides Internet access to the connected LANs and enables communication over large distances.
    - **Example**: A network that connects several factory locations to a central management system.

5. **IoT Gateway**:

- **Definition**: A device that connects an IoT LAN to a WAN or the Internet, acting as a bridge between local devices and external networks.
- **Functionality**:
  - Manages data transmission between local devices and the Internet.
  - Responsible for forwarding packets between LANs and WANs using Layer 3 of the OSI model.
- **Significance**: Gateways help manage network traffic, ensure security, and facilitate communication between different types of networks.

6. **IoT Proxy**:
   - **Definition**: An application layer device that performs intermediary functions between IoT nodes and other network entities.
   - **Functionality**:
     - Provides additional security features, such as firewalls and packet filtering.
     - Extends the addressing range of the network, allowing more devices to connect.
   - **Use Cases**: Used in scenarios requiring secure communication between devices and the cloud or other services.

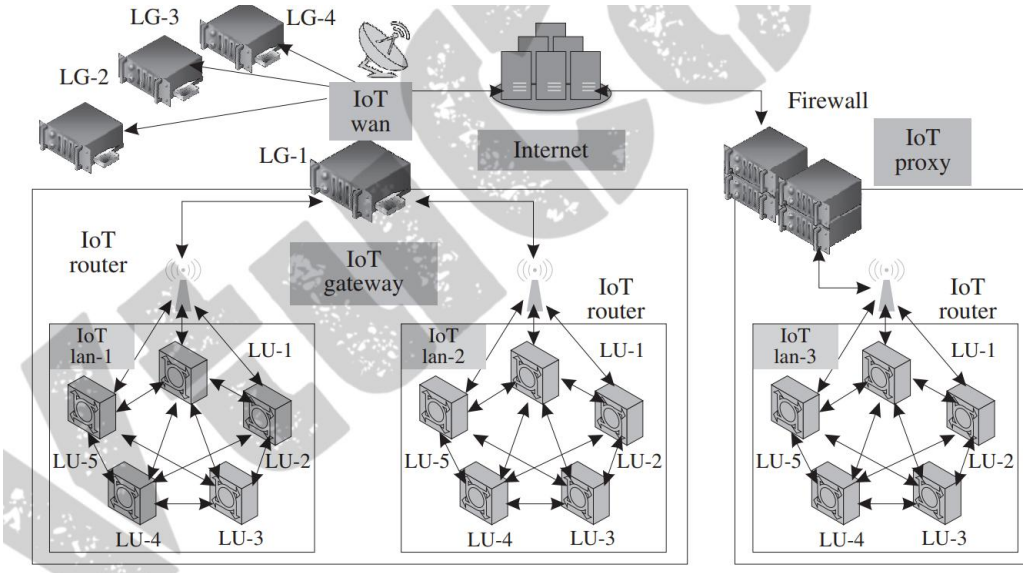


Figure 4.9 A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

Key Points:

- Each IoT LAN is identified uniquely, and while device identifiers are unique within a LAN, they may be repeated in other LANs.
- Routers act as linking points between different LANs and facilitate traffic flow to gateways or proxies.
- The reliance on **wireless technology** in IoT deployments is crucial due to the extensive number of devices involved, making it impractical to use wired connections.

Addressing Strategies in IoT

As IoT continues to expand, efficient addressing strategies are critical to managing the increasing number of connected devices. This section focuses on **IPv6** addressing schemes, which are essential for accommodating the vast number of devices in the IoT landscape.

IPv4 vs. IPv6

Key Differences:

Feature	**IPv4**	**IPv6**
Developed by	IETF (1974)	IETF (1998)
Address Length	32 bits	128 bits
Number of Addresses	2^32 (approximately 4.3 billion)	2^128 (approximately 340 undecillion)
Notation	Dotted decimal	Hexadecimal
Dynamic Address Allocation	DHCP	DHCPv6, SLAAC
IPSec	Optional	Mandatory
Header Size	Variable	Fixed
Header Checksum	Yes	No
Broadcast Addresses	Yes	No
Multicast Addresses	Yes	Yes
Focus	Reliable transmission	Addressing

Observations:

- IPv6 was designed to handle the growing need for addresses due to the increase in connected devices.

- Unlike IPv4, which prioritizes reliable packet delivery, IPv6 emphasizes address allocation and routing.

IPv6 Address Format

- An **IPv6 address** is 128 bits long and structured as follows:
    - **Global Prefix**: The first 48 bits are globally unique and identify the network segment.
    - **Subnet Prefix**: The next 16 bits identify the subnet within that network.
    - **Interface Identifier (IID)**: The last 64 bits are used to identify the specific device or interface, often derived from the device's MAC address or generated randomly.

IPv6 Address Example:
2032:8A6F:3456:4F55:3342:AA43:3434:2267

Types of IPv6 Addresses

1. **Global Unicast Address (GUA)**:
    - Assigned to individual IoT devices, enabling them to communicate directly with the Internet.
    - Used for gateways, proxies, or WANs in IoT deployments.
2. **Multicast Address**:
    - Allows sending messages from one source to multiple destinations simultaneously, facilitating efficient data distribution.
3. **Link Local Address (LL)**:
    - Valid only within a single network segment (LAN) and cannot be routed outside it.
    - Commonly used for communication between devices on the same local network.
4. **Unique Local Address (ULA)**:
    - Similar to LL addresses but designed for internal communication within a network, not routable on the Internet.
    - Provides a way to communicate within a specific organization or area.

5. **Loopback Address**:
    - Used for testing and diagnostics; it refers to the device itself (localhost).
6. **Unspecified Address**:
    - All bits set to zero, indicating no specific destination address.
7. **Solicited-node Multicast Address**:
    - Used for neighbor discovery, allowing a node to join a multicast group based on its IPv6 address.

Addressing Strategies for Mobility

Addressing strategies are crucial for maintaining connectivity and avoiding address clashes when IoT nodes move between networks. The following strategies are commonly employed:

1. **Global Prefix Changes**:
    - When a node moves from one network to another, its global prefix may change, requiring reconfiguration of its address.
    - Static IP addresses are often preferred for resource-constrained IoT nodes to avoid conflicts during this transition.
2. **Prefix Changes within WANs**:
    - If a WAN changes its global prefix, devices must adapt to the change. This is typically managed by gateways and proxies that use Unique Local Addresses (ULAs) for internal communication.
3. **Remote Anchoring**:
    - This strategy maintains the IoT node's global address even if it moves across different networks or prefixes.
    - A remote anchoring point allows the node to keep its original global address through tunneling, ensuring stable connectivity despite changes in local network conditions.

Points to Ponder

- **Multihoming in IoT Networks**:
    - Multihoming involves connecting a node or network to multiple networks simultaneously for improved reliability.
    - Proxies can manage multiple IP addresses and link them to Link Local (LL) addresses in small IoT deployments.
- **Tunneling**:
    - A method of sending data from private networks over public networks through encapsulated packets.
    - Tunneling protocols, like VPNs and SSH, ensure secure communication for IoT devices, especially when using incompatible protocols across different networks.