CSE 425: Internet of Things

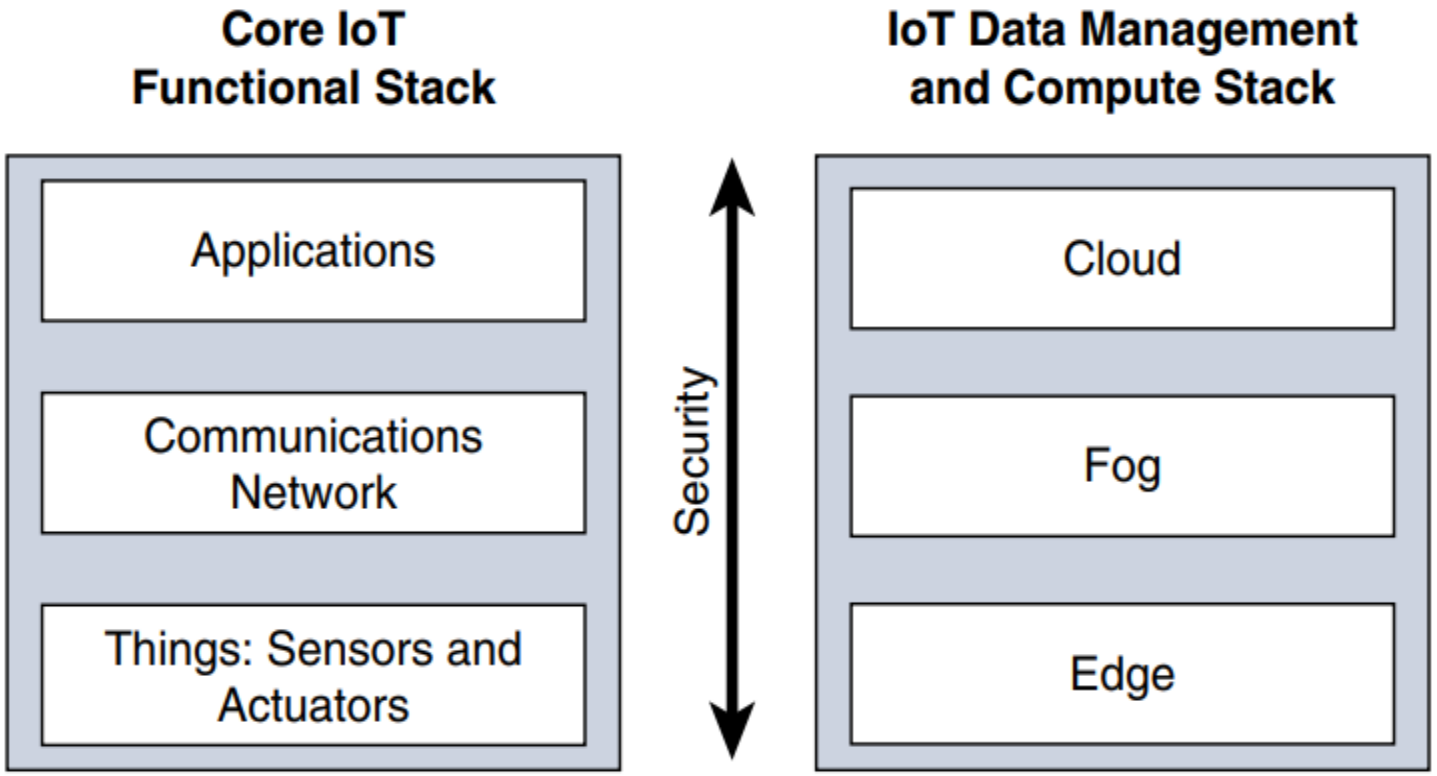
Dept. of CSE, BUBT| Summer 2021

Md. Hasibur Rahman

IoT Network Architecture and Design (Continue)

Courtesy: David Hanes and Co., Bahga & Madisetti, Many Websites, and Google

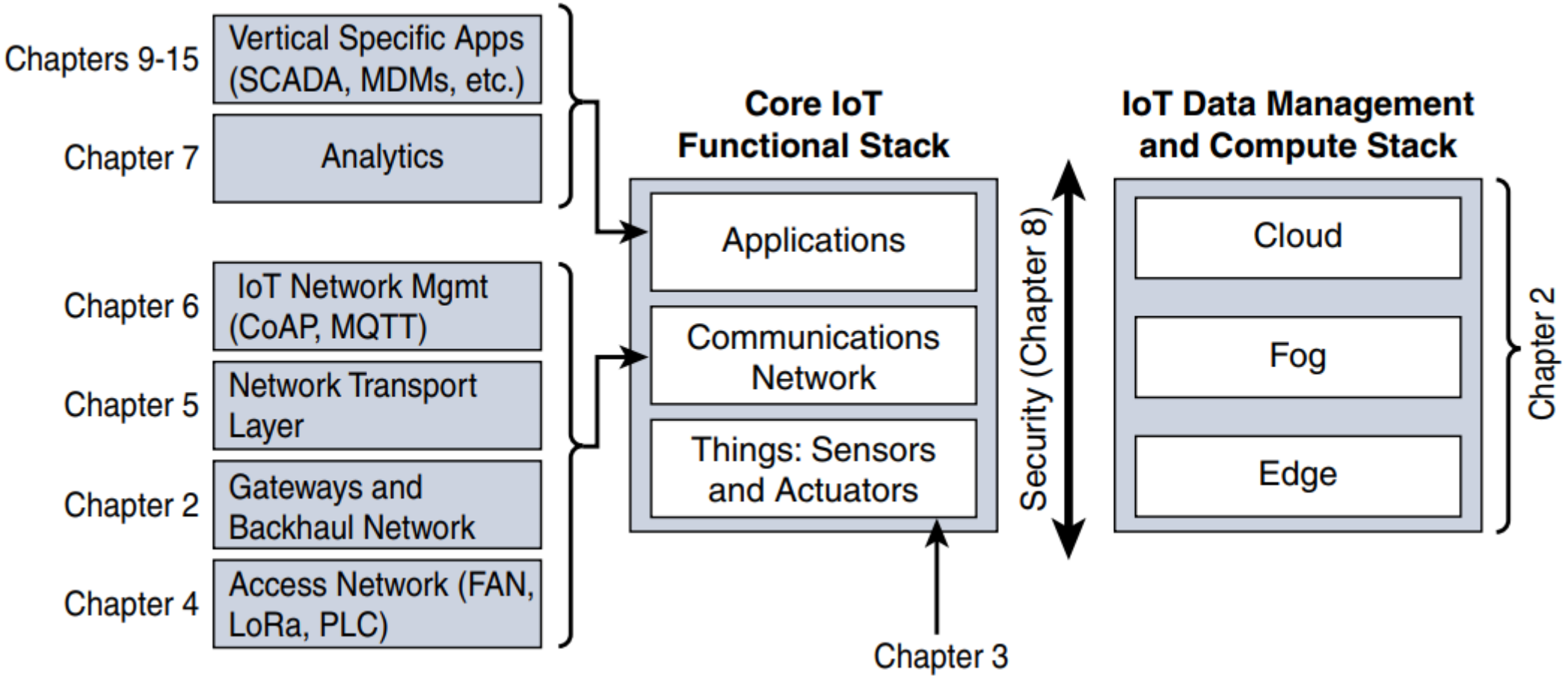
A Simplified IoT Architecture



Although differences exist between the aforementioned reference models, interconnection of the IoT endpoint devices to a network that transports the data where it is ultimately used by applications, whether at the data center, in the cloud, or at various management points throughout the stack.

This framework is presented as two parallel stacks: The IoT Data Management and Compute Stack and the Core IoT Functional Stack. Though it lacks detail necessary, our intention is to simplify the IoT architecture into its most basic building blocks. All the layers will still cover but they are grouped here in functional blocks that are easy to understand.

A Simplified IoT Architecture: Expanded View



Layer 2: Communications Network Layer

As you have already select the things for your IoT system, you are ready to connect the object and communicate.

Things selection attributes: transmission range, data volume and frequency, sensor density and mobility etc.

Compute and network assets used in IoT and their relation with physical environment in which the devices are deployed is a great concern of IoT. Some examples of the concerns are temperature variances, liquid environment, shock and vibration, dust, hazardous location etc.

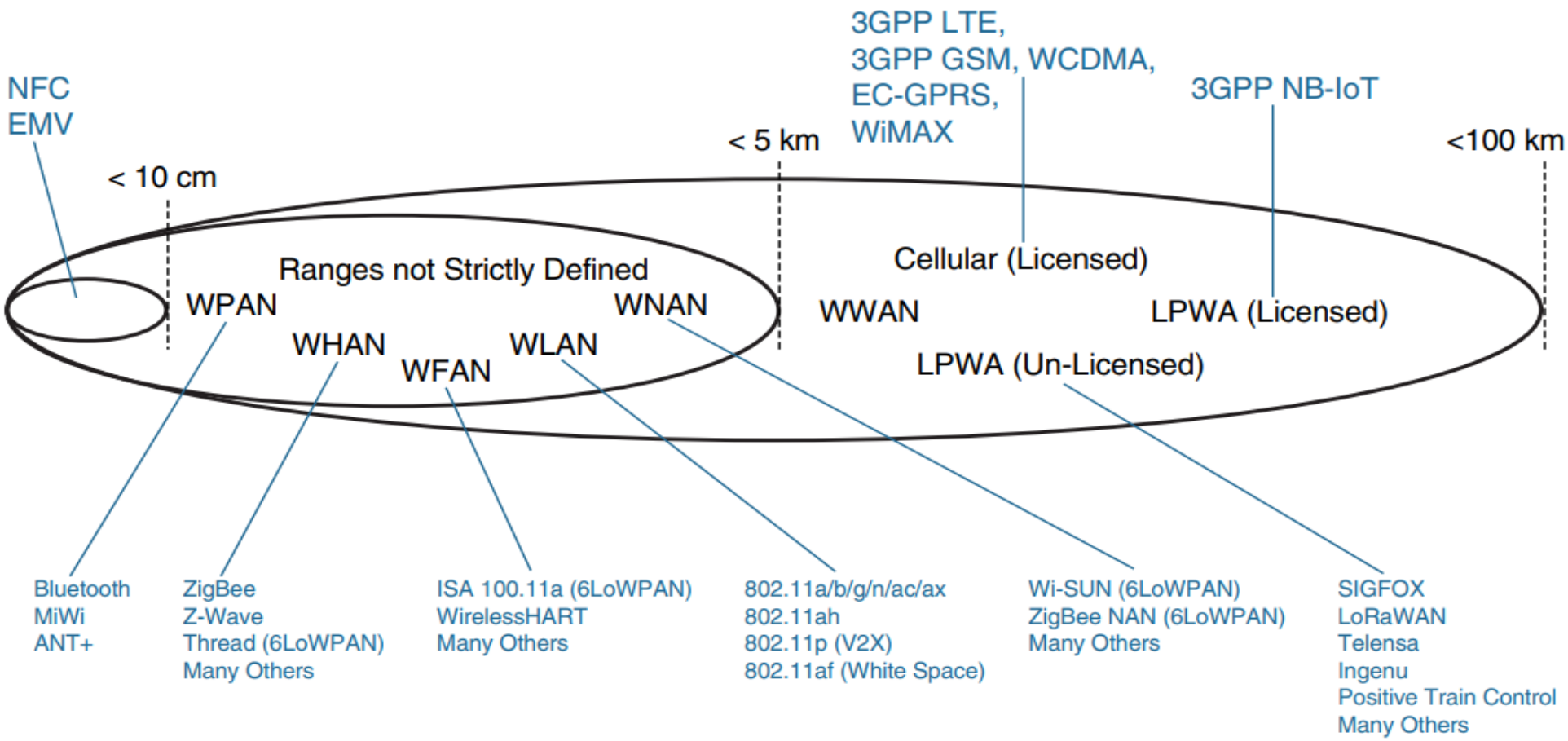
The equipment can impact the environment. For example, in a scenario in which volatile gases may be present, spark suppression is a critical design criterion.

Layer 2: Access Network Sublayer

There is a direct relationship between the IoT network technology you choose and the type of connectivity topology this technology allows. Each technology was designed with a certain number of use cases in mind (what to connect, where to connect, how much data to transport at what interval and over what distance). One key parameter determining the choice of access technology is the range between the smart object and the information collector.

> "One of the myths about the Internet of Things is that companies have all the data they need, but their real challenge is making sense of it. In reality, the cost of collecting some kinds of data remains too high, the quality of the data isn't always good enough, and it remains difficult to integrate multiple data sources."
>
> — Chris Murphy, Editor, Information Week

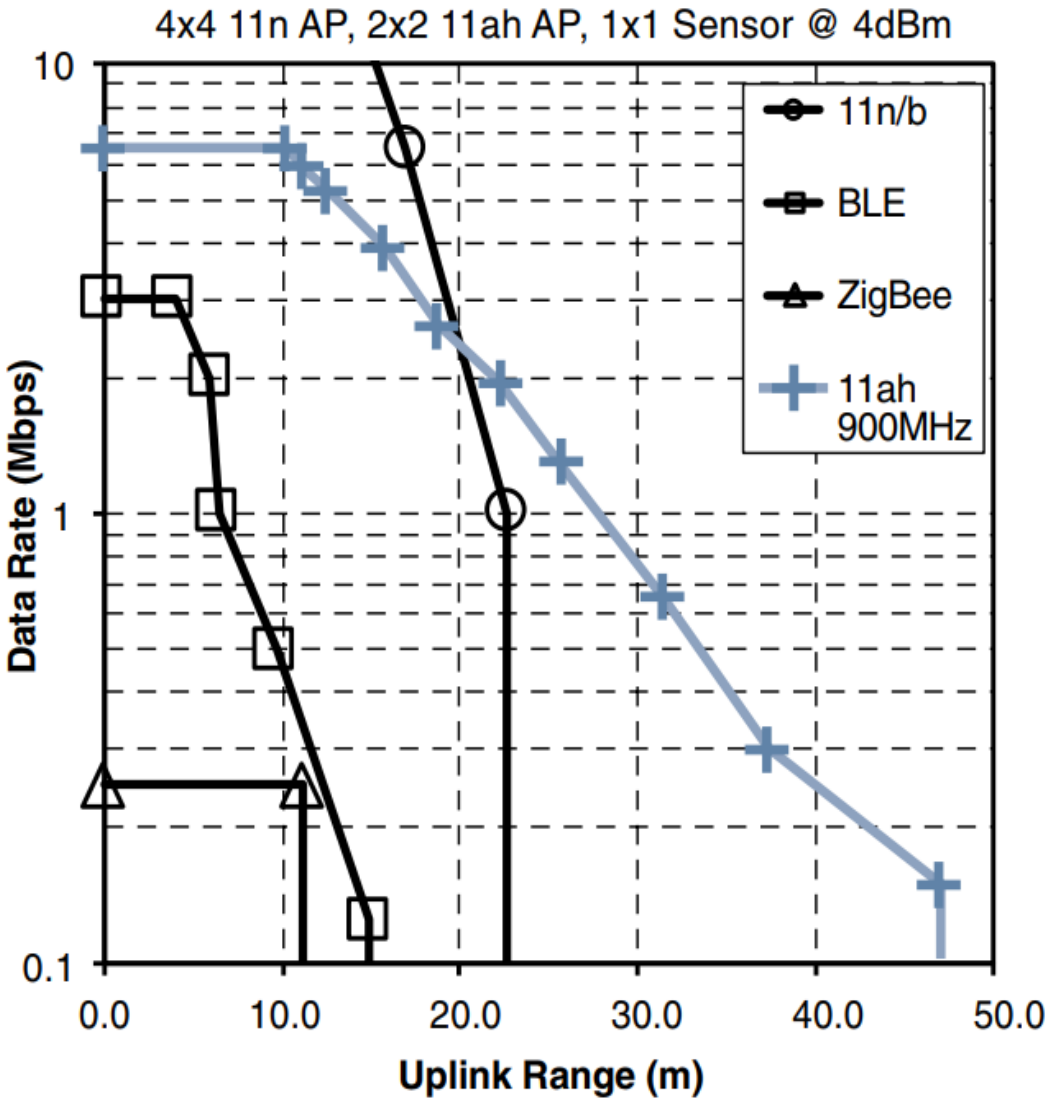
Access Network Sublayer: Access Technologies and Distances



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network

WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWA: Low Power Wide Area

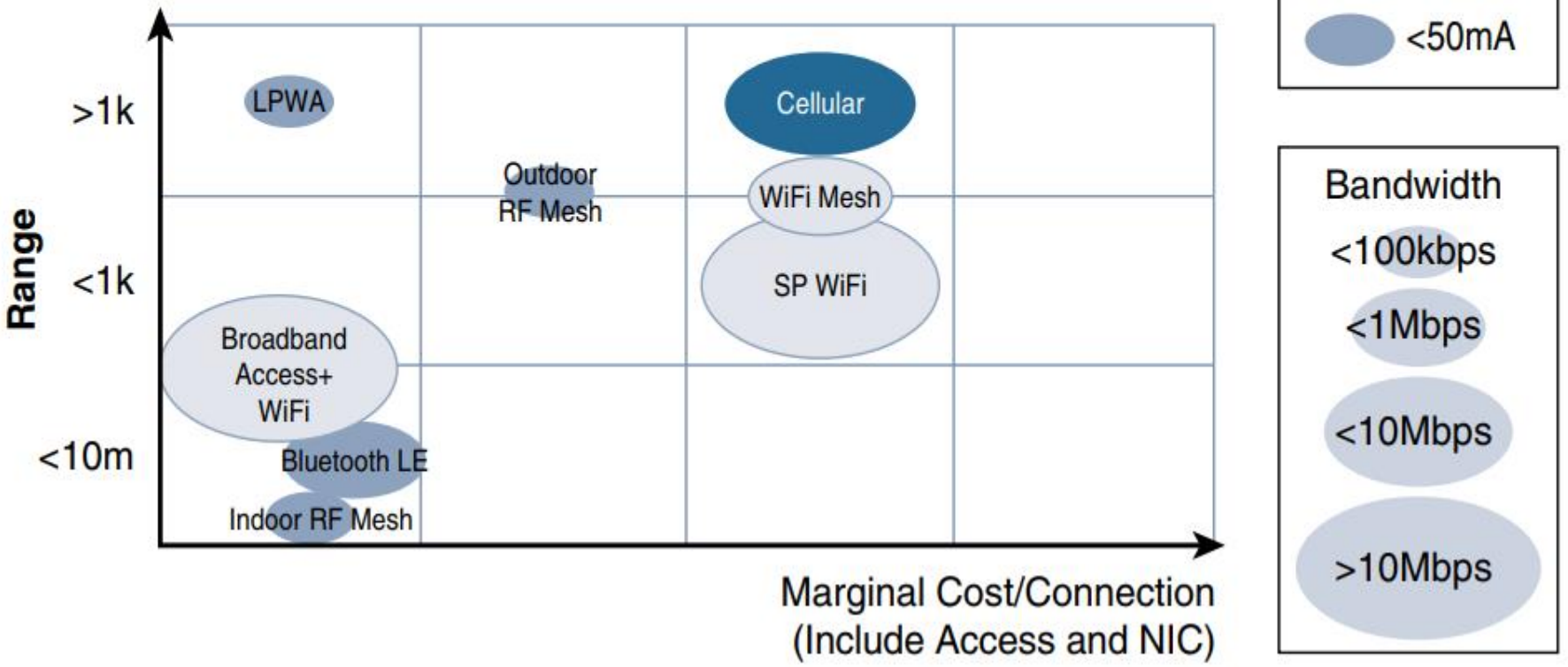
Access Network Sublayer: Access Technologies and Distances

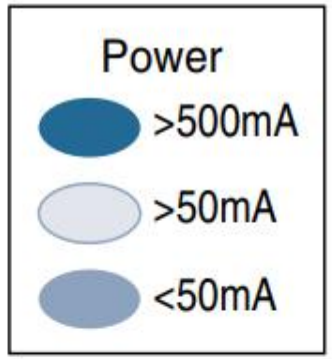


Similar achievable distances do not mean similar protocols and similar characteristics. Each protocol uses a specific frame format and transmission technique over a specific frequency (or band). These characteristics introduce additional differences. For example, Figure in left demonstrates four technologies representing WHAN (ZigBee and BLE) to WLAN (11n/b, 11ah) ranges and compares the throughput and range that can be achieved in each case. Figure in left, supposes that the sensor uses the same frame size, transmit power, and antenna gain. The slope of throughput degradation as distance increases varies vastly from one technology to the other. This difference limits the amount of data throughput that each technology can achieve as the distance from the sensor to the receiver increases.

Common Last-Mile Technologies in Terms of Range Versus Cost, Power, and Bandwidth

Last mile is used to refer to the final leg of the telecommunications network delivery components to the end user.



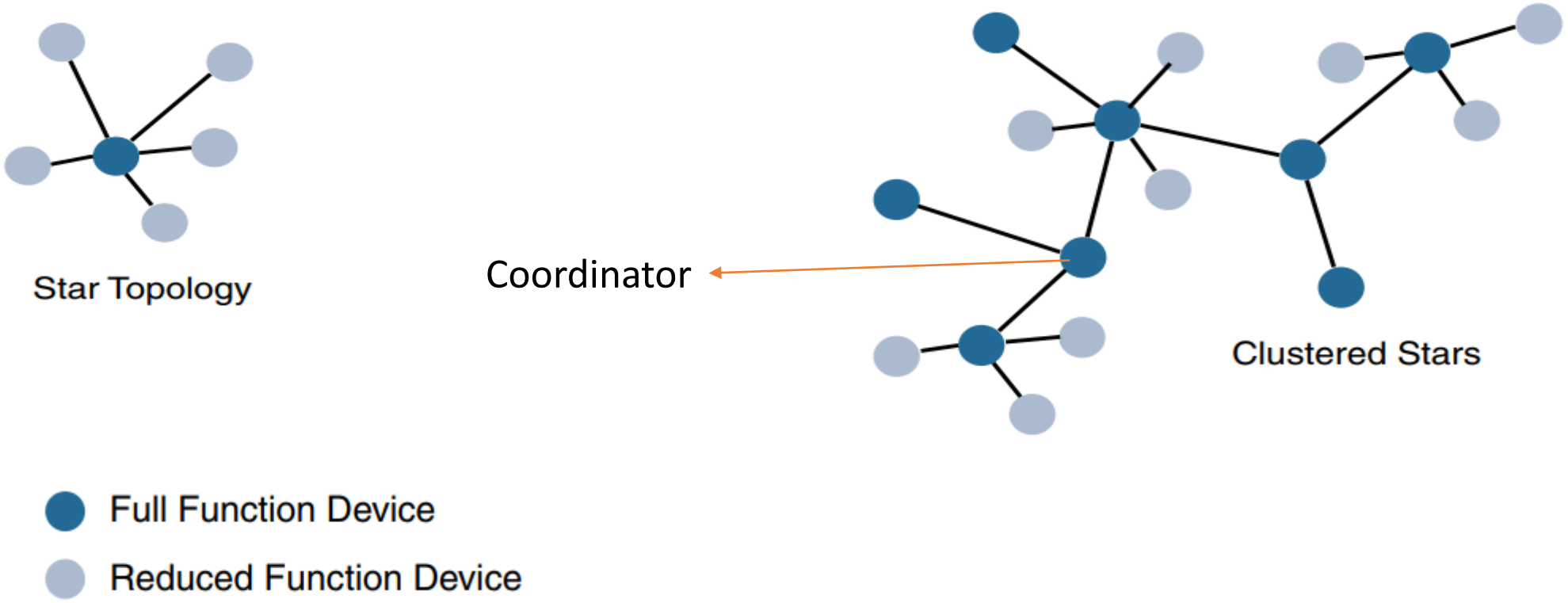


- Longest range
- Highest throughput
- Lowest power consumption
- Lowest Cost of Money

Access Network Sublayer: Topologies

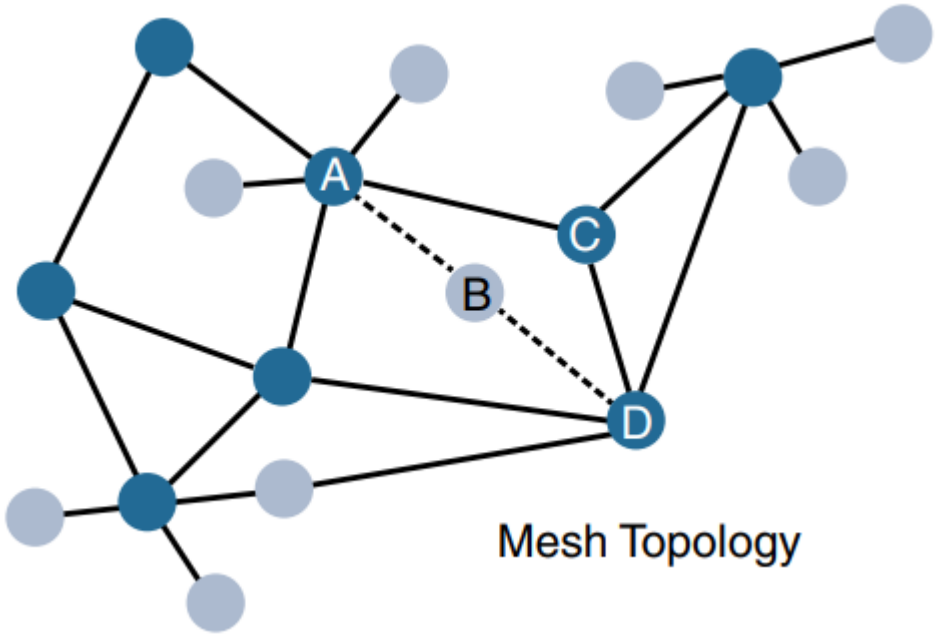
Similar ranges also do not mean similar topologies. Some technologies offer flexible connectivity structure to extend communication possibilities:

Point-to-point topologies: These topologies allow one point to communicate with another point.



Access Network Sublayer: Topologies

Point-to-multipoint topologies: These topologies allow one point to communicate with more than one other point. Most IoT technologies where one or more than one gateways communicate with multiple smart objects are in this category.



Mesh Topology

Note: Figure shows a partial mesh topology, where a node can communicate with more than one other node, but not all nodes communicate directly with all other nodes. In a full mesh topology each node communicates with each other node.

Note: Do not confuse *topology* and *range*. Topology describes the organization of the nodes, while range is dictated by factors such as the frequency or operation, the signal structure, and operational bandwidth. For example, both IEEE 802.15.4 and LoRaWAN implement star topologies, but the range of IEEE 802.15.4 is a few tens of meters, while LoRaWAN can achieve a successful signal over many kilometers.

Gateways and Backhaul Sublayer

Data collected from a smart object may need to be forwarded to a central station where data is processed. As this station is often in a different location from the smart object, data directly received from the sensor through an access technology needs to be forwarded to another medium (the backhaul) and transported to the central station. The gateway is in charge of this inter-medium communication. It can be either a dedicated hardware appliance or software program.

Gateways and Backhaul Sublayer

Some of the most common uses for IoT gateways include:

- Connecting devices to one another
- Connecting devices to the cloud
- Translating communicate between IoT devices that are manufactured or operated by different companies
- Filtering data
- Mitigating security risks
- Intelligence at the edge

Gateway and Backhaul Sublayer

Architectural Considerations for WiMAX and Cellular Technologies:

Technology	Type and Range	Architectural Characteristics
Ethernet	Wired, 100 m max	Requires a cable per sensor/sensor group; adapted to static sensor position in a stable environment; range is limited; link is very reliable
Wi-Fi (2.4 GHz, 5 GHz)	Wireless, 100 m (multipoint) to a few kilometers (P2P)	Can connect multiple clients (typically fewer than 200) to a single AP; range is limited; adapted to cases where client power is not an issue (continuous power or client battery recharged easily); large bandwidth available, but interference from other systems likely; AP needs a cable
802.11ah (HaloW, Wi-Fi in sub-1 GHz)	Wireless, 1.5 km (multipoint), 10 km (P2P)	Can connect a large number of clients (up to 6000 per AP); longer range than traditional Wi-Fi; power efficient; limited bandwidth; low adoption; and cost may be an issue
WiMAX (802.16)	Wireless, several kilometers (last mile), up to 50 km	Can connect a large number of clients; large bandwidth available in licensed spectrum (fee-based); reduced bandwidth in license-free spectrum (interferences from other systems likely); adoption varies on location
Cellular (for example, LTE)	Wireless, several kilometers	Can connect a large number of clients; large bandwidth available; licensed spectrum (interference-free; license-based)

Layer 2: Network Transport Sublayer

This communication structure thus may involve peer-to-peer (for example, meter to meter), point-to-point (meter to headend station), point-to-multipoint (gateway or headend to multiple meters), unicast and multicast communications (software update to one or multiple systems). In a multitenant environment (for example, electricity and gas consumption management), different systems may use the same communication pathways. This communication occurs over multiple media (for example, power lines inside your house or a short-range wireless system like indoor Wi-Fi and/or ZigBee), a longer-range wireless system to the gateway, and yet another wireless or wired medium for backhaul transmission.

To allow for such communication structure, a network protocol with specific characteristics needs to be implemented. The protocol needs to be open and standard based to accommodate multiple industries and multiple media. Scalability (to accommodate thousands or millions of sensors in a single network) and security are also common requirements. IP is a protocol that matches all these requirements. The flexibility of IP allows protocols to be embedded in objects of very different natures, exchanging information over very different media, including low-power, lossy, and low-bandwidth networks.

Layer 2: IoT Network Management Sublayer

IP, TCP, and UDP bring connectivity to IoT networks. Upper-layer protocols need to take care of data transmission between the smart objects and other systems. Multiple protocols have been leveraged or created to solve IoT data communication problems. Some networks rely on a push model (that is, a sensor reports at a regular interval or based on a local trigger), whereas others rely on a pull model (that is, an application queries the sensor over the network), and multiple hybrid approaches are also possible.

Layer 3: Applications and Analytics Layer

- **Analytics Versus Control Applications:**

Analytics application: This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed.

Control application: This type of application controls the behavior of the smart object or the behavior of an object related to the smart object. For example, a pressure sensor may be connected to a pump. A control application increases the pump speed when the connected sensor detects a drop in pressure.

- **Data Versus Network Analytics:**

Data analytics: This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system. At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store.

For example, a machine or robot in a factory can report data about its own movements. This data can be used by an analytics application to report degradation in the movement speeds, which may be indicative of a need to service the robot before a part breaks.

Layer 3: Applications and Analytics Layer

- **Data Versus Network Analytics:**

Data analytics: This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system. At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store.

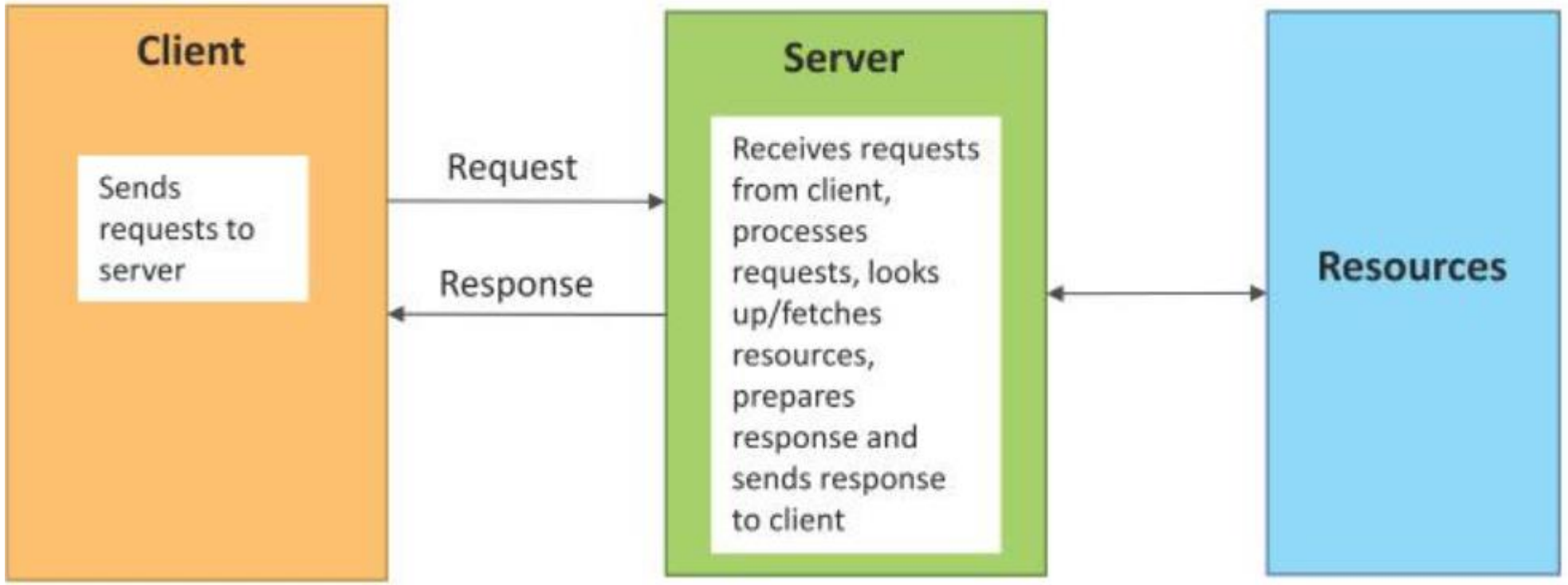
For example, a machine or robot in a factory can report data about its own movements. This data can be used by an analytics application to report degradation in the movement speeds, which may be indicative of a need to service the robot before a part breaks.

Network analytics: Most IoT systems are built around smart objects connected to the network. A loss or degradation in connectivity is likely to affect the efficiency of the system. Such a loss can have dramatic effects.

- **Data Analytics Versus Business Benefits**

Request-Response communication model

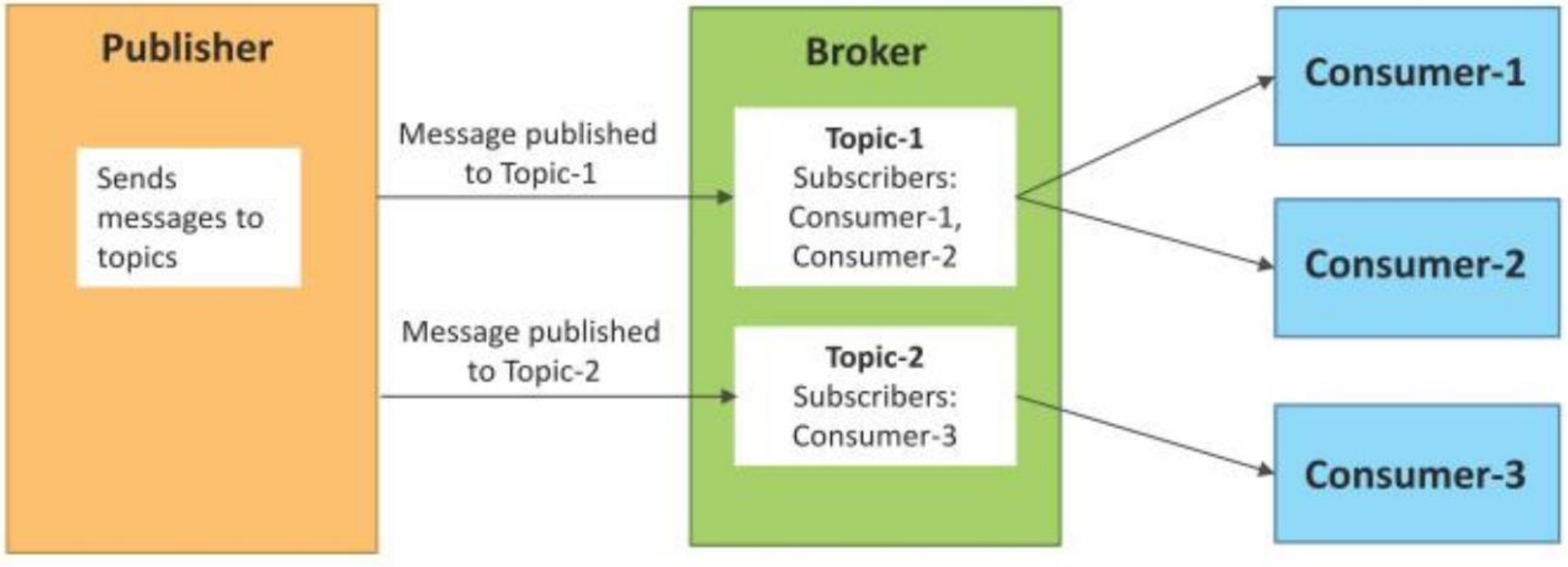
- Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.
- REST-based Communication APIs



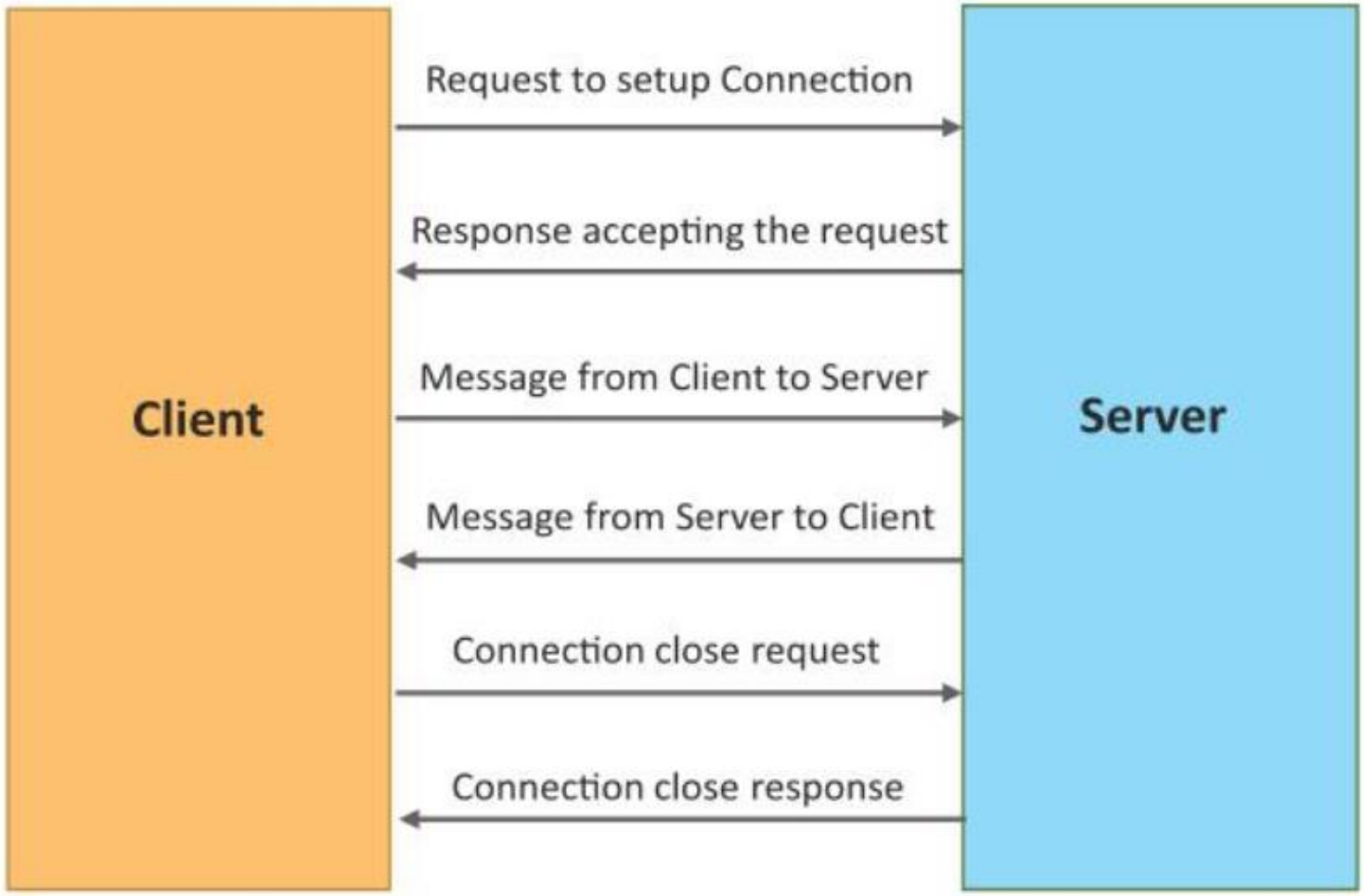
Publish-Subscribe communication model

- Publish-Subscribe is a communication model that involves publishers, brokers and consumers.
- Publishers are the source of data. Publishers send the data to the topics which are managed by the broker.

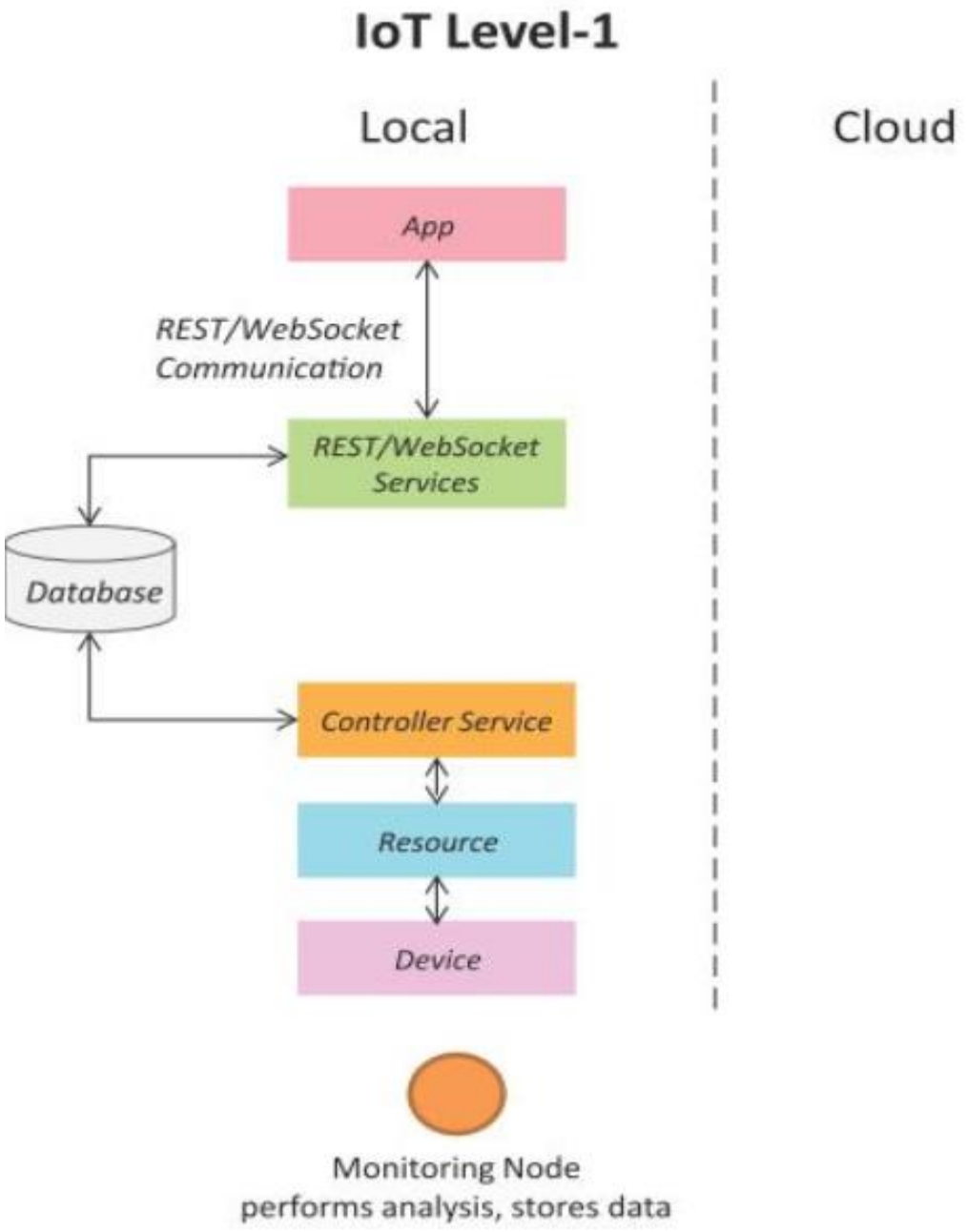
  Publishers are not aware of the consumers.
- Consumers subscribe to the topics which are managed by the broker.
- When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.



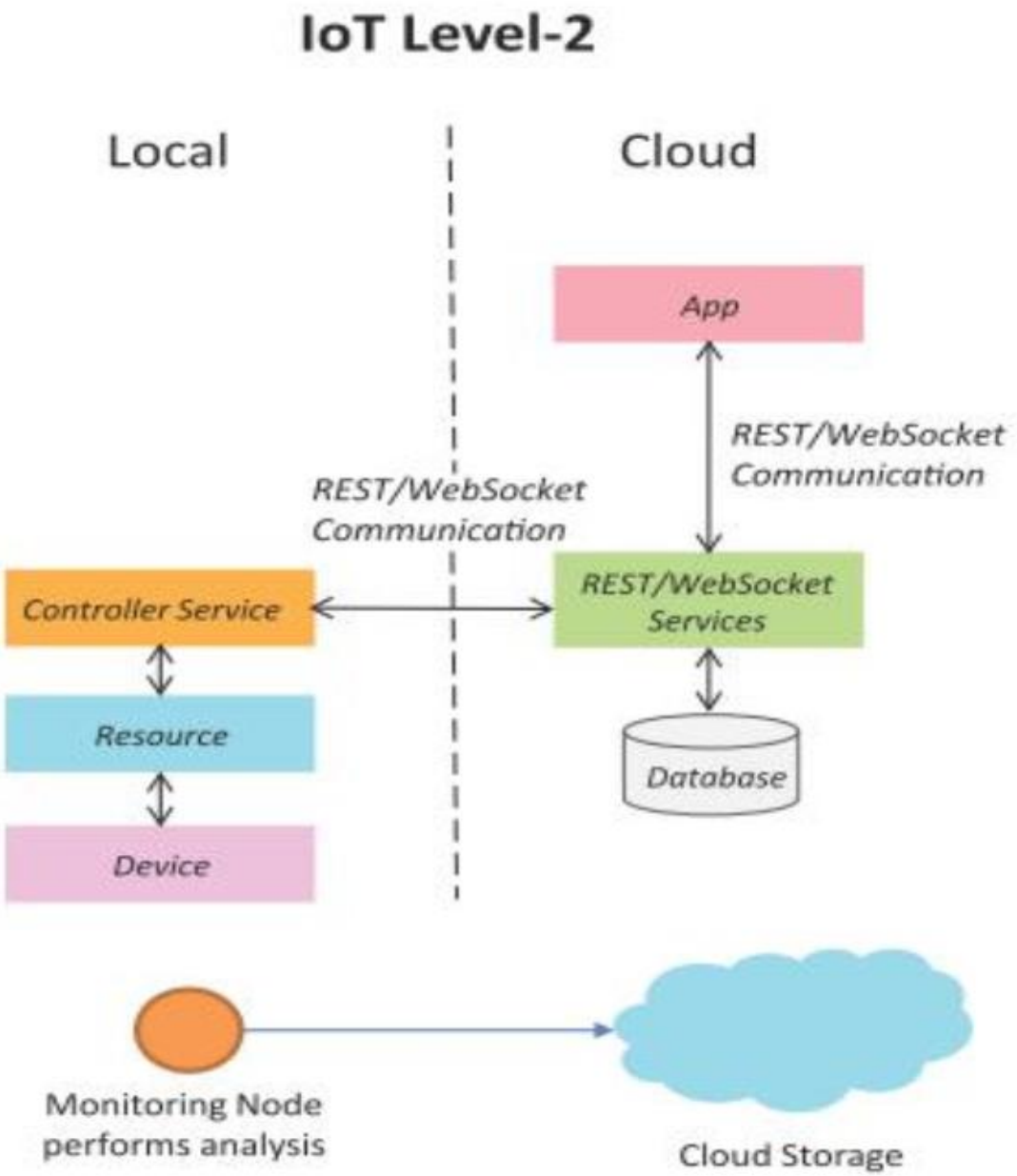
Exclusive Pair communication model



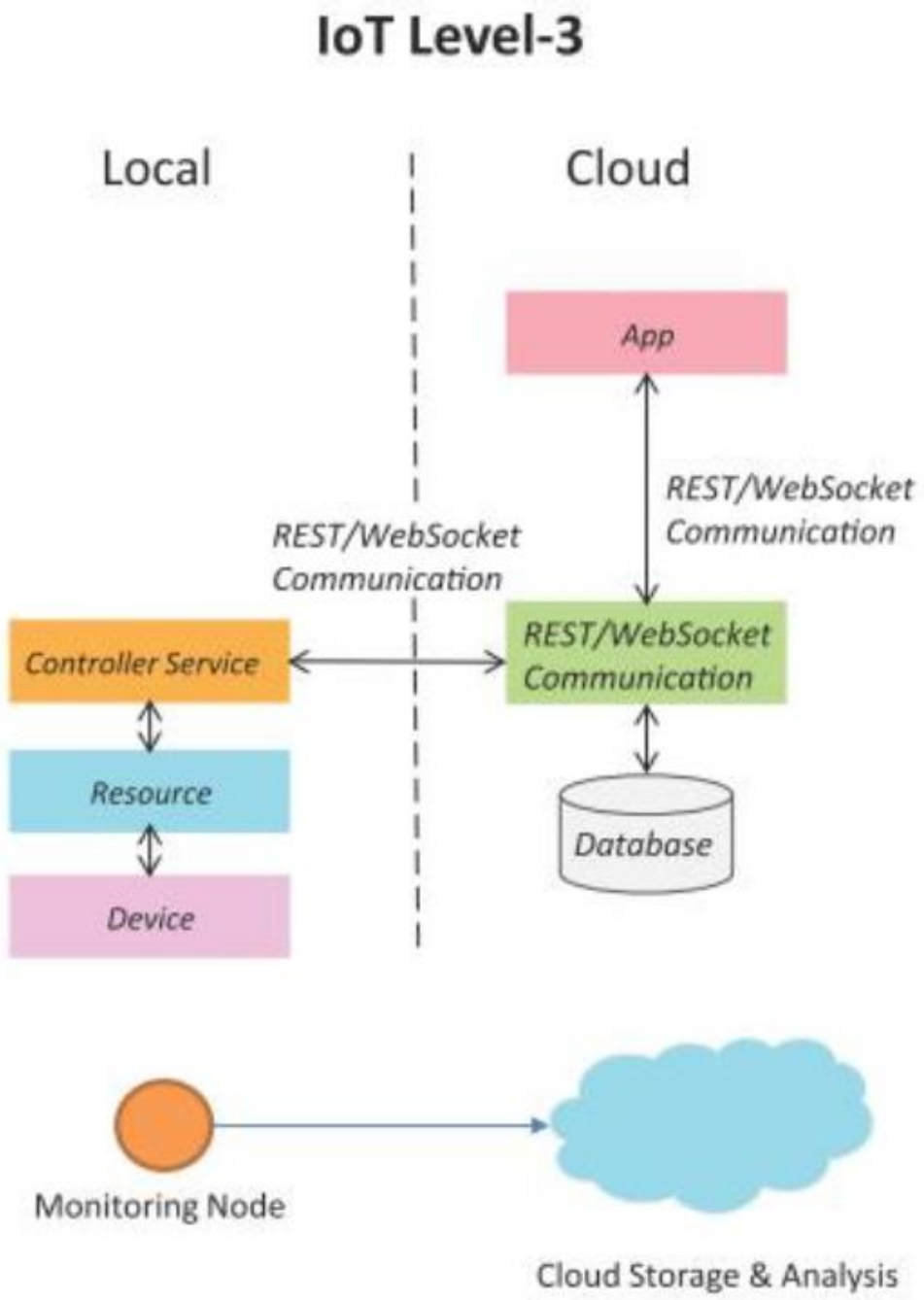
- Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server.
- Once the connection is setup it remains open until the client sends a request to close the connection.
- Client and server can send messages to each other after connection setup
- WebSocket-based Communication APIs


IoT Level-1
Local
Cloud
App
REST/WebSocket
Communication
REST/WebSocket
Services
Database
Controller Service
Resource
Device
Monitoring Node
performs analysis, stores data

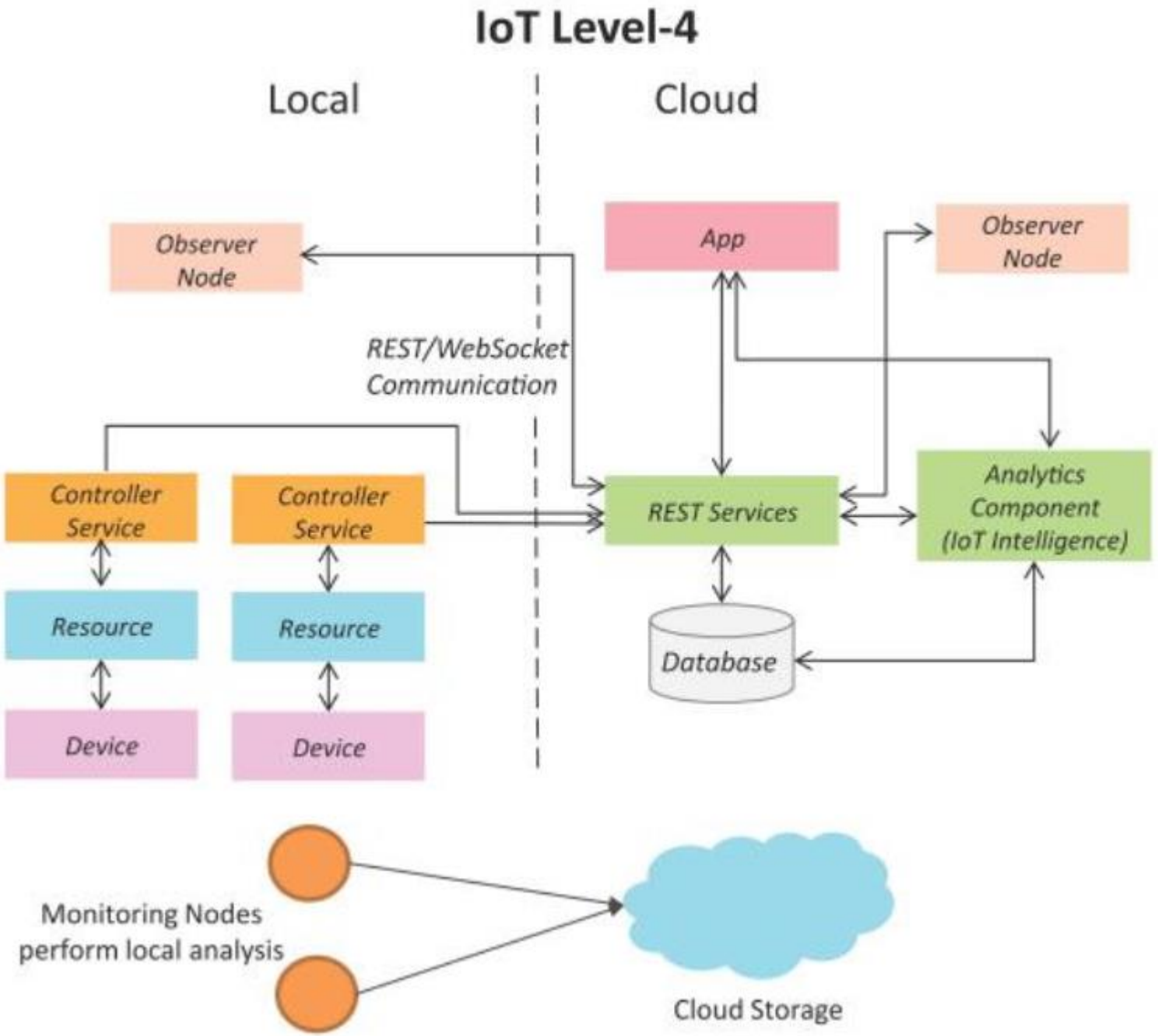
IoT Level 1


IoT Level-2
Local
Cloud
App
REST/WebSocket
Communication
REST/WebSocket
Communication
Controller Service
REST/WebSocket
Services
Resource
Database
Device
Monitoring Node
performs analysis
Cloud Storage

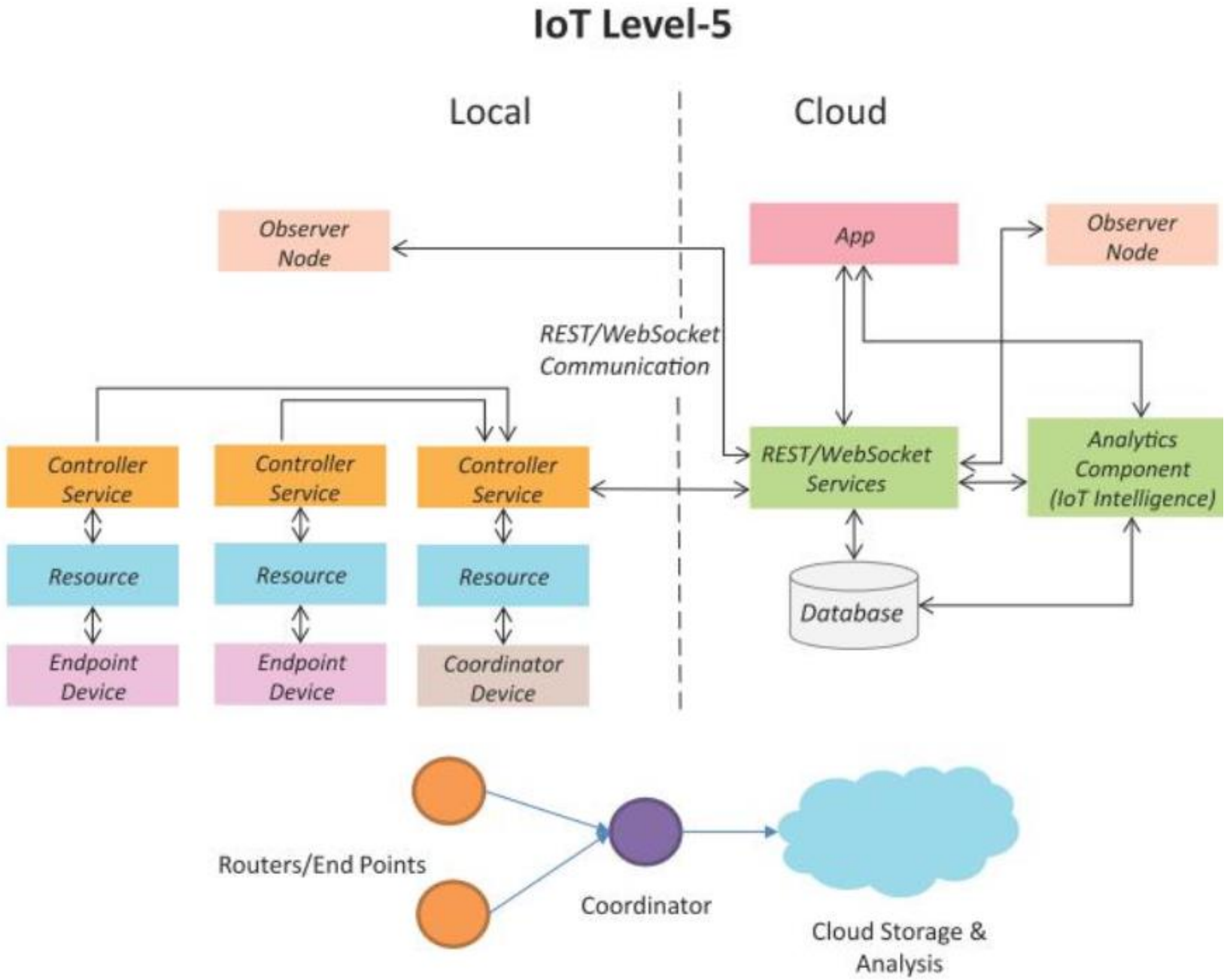
IoT Level 2


IoT Level-3
Local
Cloud
App
REST/WebSocket
Communication
REST/WebSocket
Communication
REST/WebSocket
Communication
Controller Service
Resource
Device
Database
Monitoring Node
Cloud Storage & Analysis

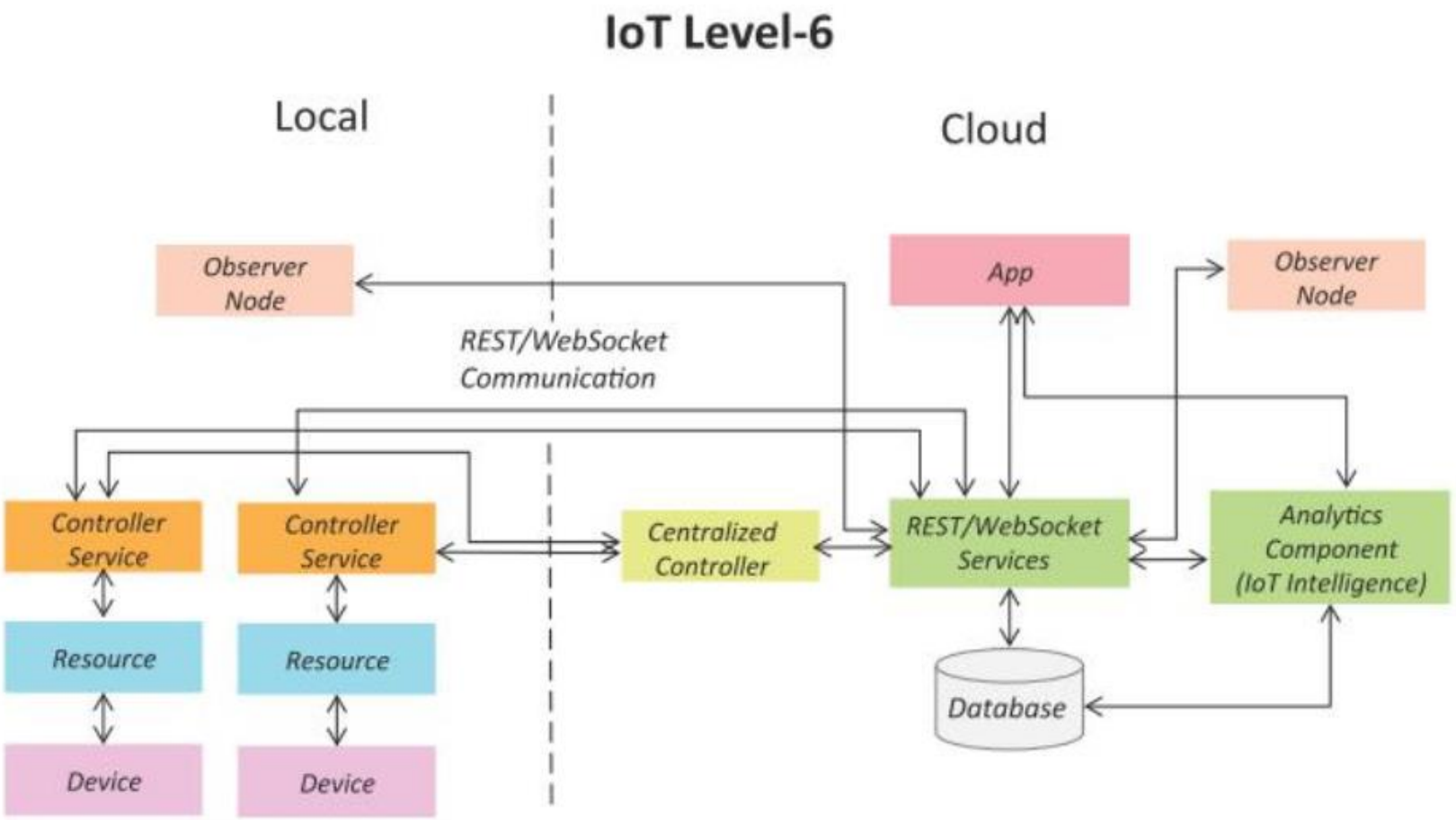
IoT Level 3

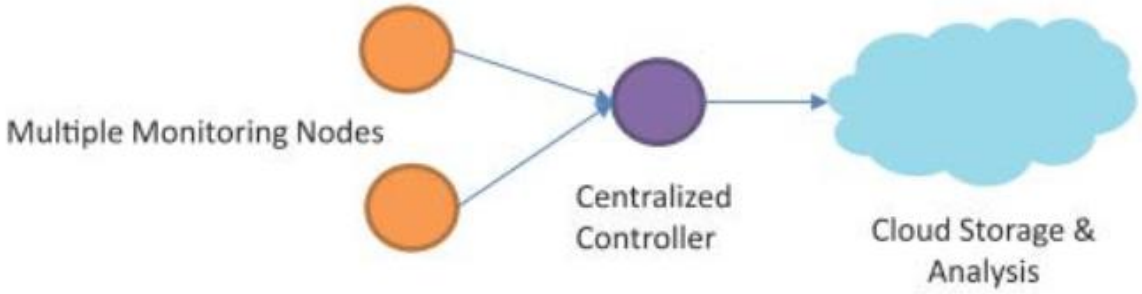

IoT Level-4
Local
Cloud
Observer Node
App
Observer Node
REST/WebSocket Communication
Controller Service
Controller Service
REST Services
Analytics Component (IoT Intelligence)
Resource
Resource
Database
Device
Device
Monitoring Nodes perform local analysis
Cloud Storage

IoT Level 4


IoT Level-5
Local
Cloud
Observer Node
App
Observer Node
REST/WebSocket Communication
Controller Service
Controller Service
Controller Service
REST/WebSocket Services
Analytics Component (IoT Intelligence)
Resource
Resource
Resource
Database
Endpoint Device
Endpoint Device
Coordinator Device
Routers/End Points
Coordinator
Cloud Storage & Analysis

IoT Level 5


IoT Level-6
Local
Cloud
Observer Node
App
Observer Node
REST/WebSocket Communication
Controller Service
Controller Service
Centralized Controller
REST/WebSocket Services
Analytics Component (IoT Intelligence)
Resource
Resource
Database
Device
Device


Multiple Monitoring Nodes
Centralized Controller
Cloud Storage & Analysis

IoT Level 6