Communication Technologies for IoT – Part 1
Wireless Network Technologies

Dr. Bibhas Ghoshal

IIIT Allahabad

Machine to Machine (M2M) Services

- Machine to Machine refers to networking of machines and devices for the purpose of remote monitoring and control and data exchange.
- M2M service refers to solutions that focus on remote collection and transfer of data from embedded sensors placed on remote assets that are fixed or mobile.
- Smart mobile devices are used to interact and control various machines (devices) using M2M technology.

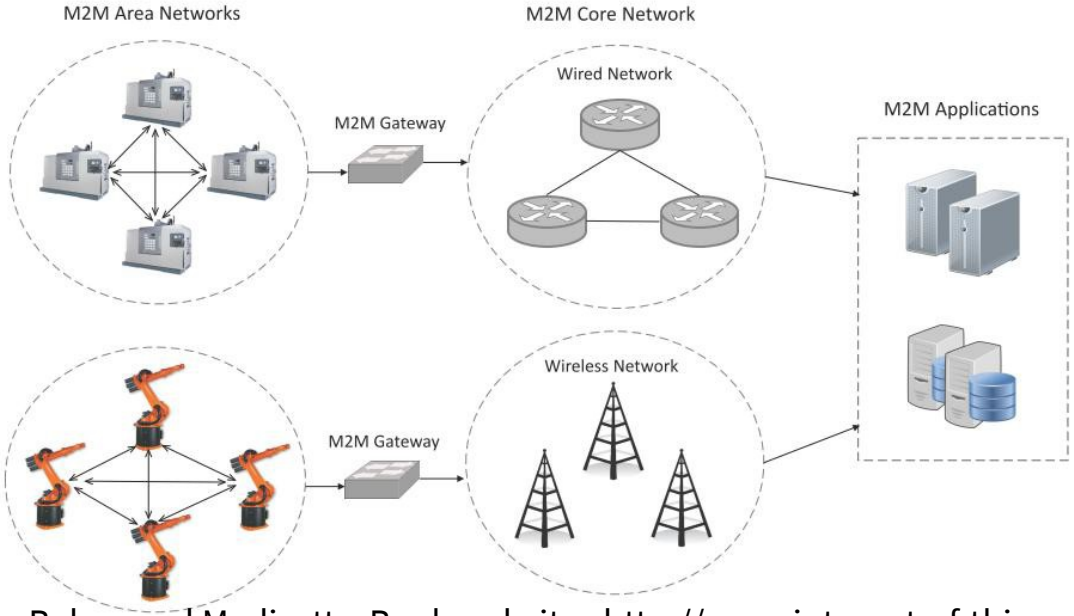
Machine to Machine (M2M) Technology

M2M area network comprises of machines (or M2M nodes) which have embedded hardware modules for sensing, actuation and communication.

Communication technologies used in M2M area network are Zigbee, Bluetooth, 6LoWPAN, IEEE 802.15.4. They use proprietary or non-IP based protocols

Communication network provides connectivity to M2M area network

Communication network uses IP based connectivity protocols

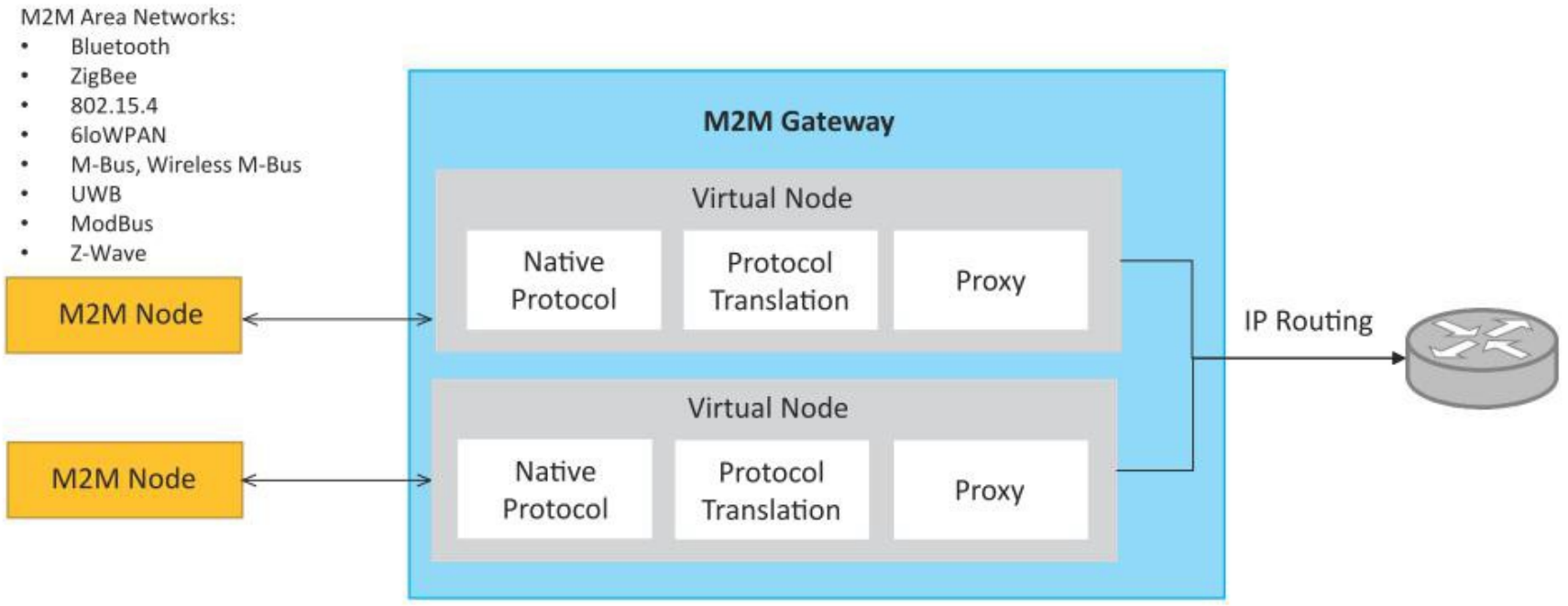


Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

Machine to Machine (M2M) Gateway

Since non-IP based protocols are used within M2M area networks, the M2M nodes within one network cannot communicate with nodes in an external network

To enable the communication between remote M2M area networks, M2M gateways are used.



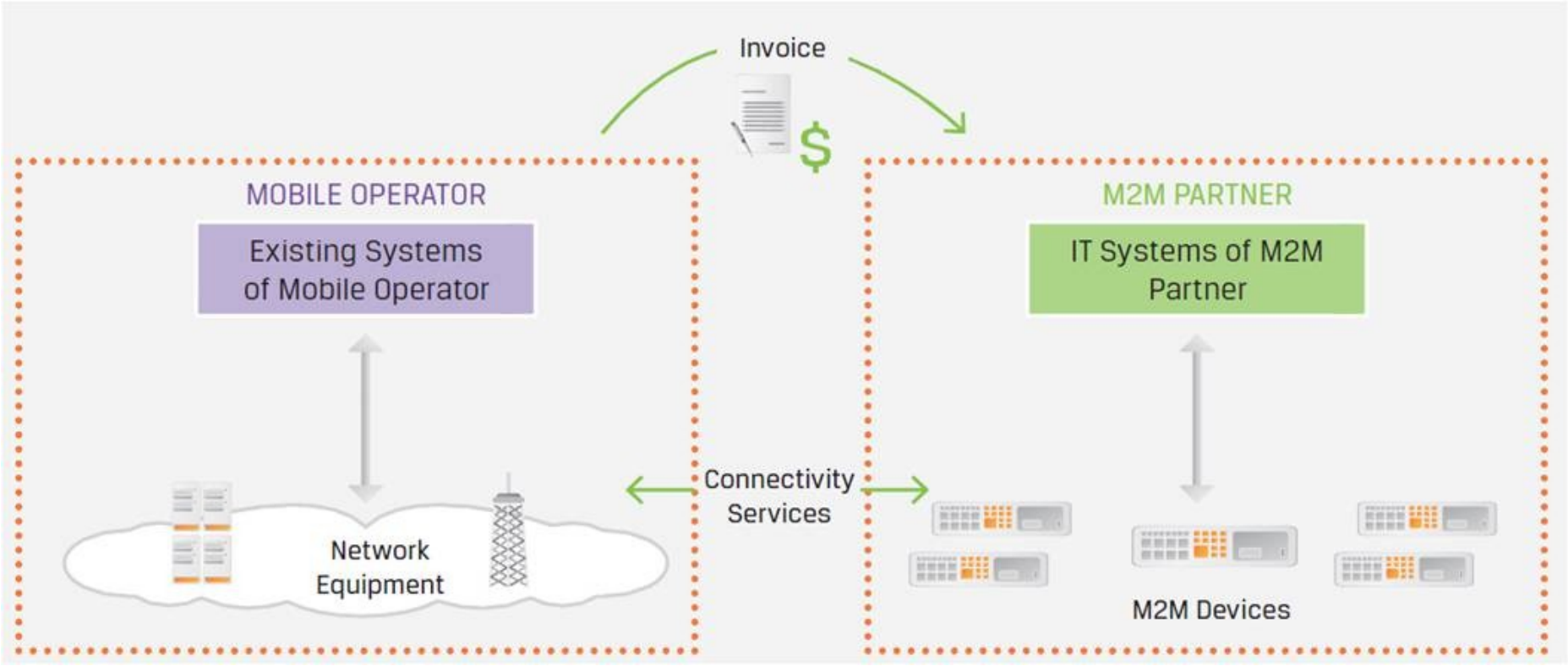
Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

Machine to Machine Vs. IoT

M2M	IOT
• Point-to-point connectivity frequently includes customer-site gear.	• A network consists of both remote and local devices that transmit information via IP.
• Many devices connect to networks via cellular or cable connections.	• The data delivered is through a cloud-based intermediary layer.
• Designed for small scale projects	• Can usually be scaled for large projects
• M2M devices do not always need to be connected to the internet	• In most circumstances, devices need continuous internet access.
• Because devices must adhere to the same communication protocols, integration choices are limited.	• There are endless integration possibilities, but you'll need a platform that can handle all of your communications.

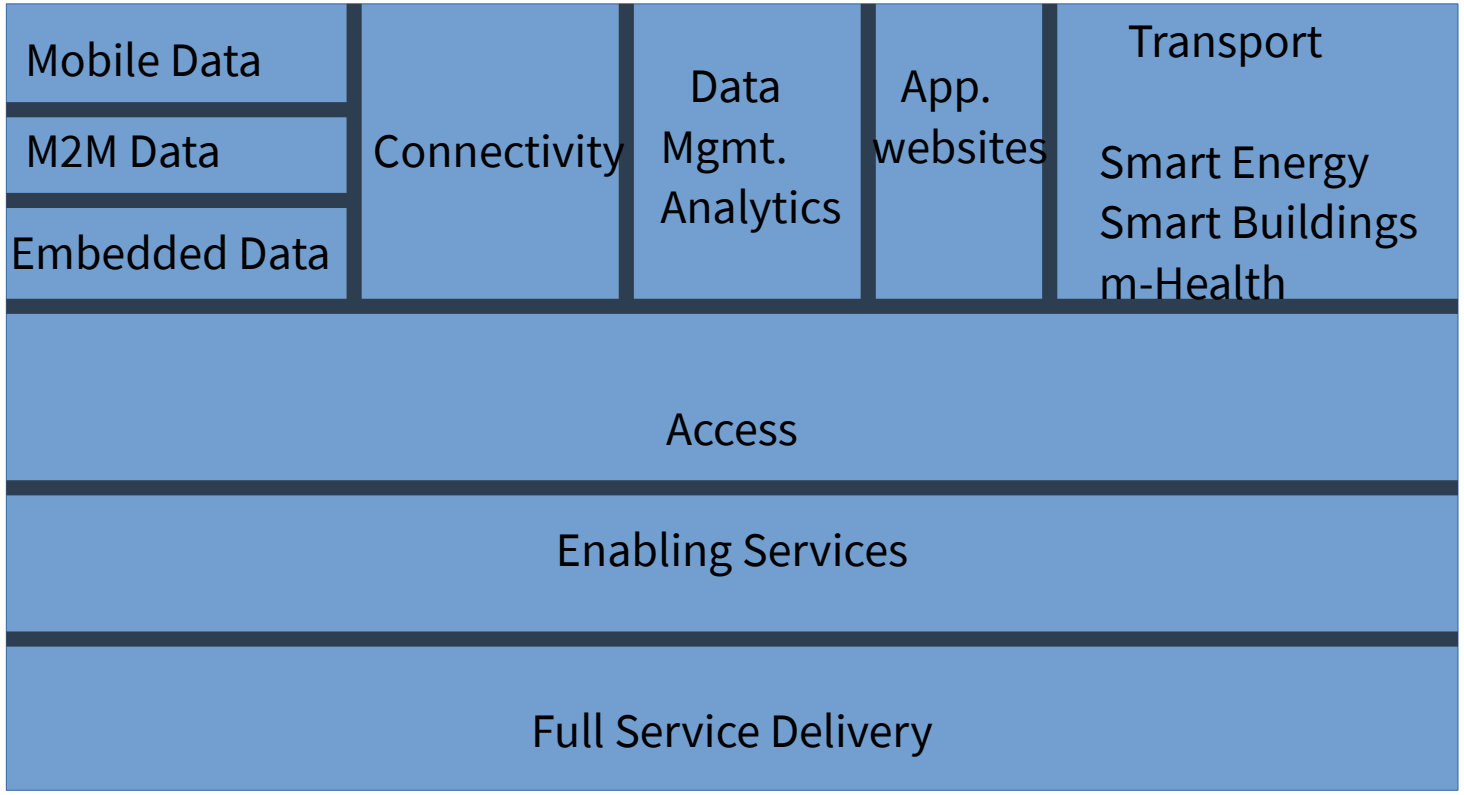
Source : Internet

Machine to Machine (M2M) Service Provision



Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

Architecture for IoT Using Mobile Devices



Architecture for IoT using mobile devices

Ref : The Internet of Things, Enabling Technologies, Platforms and Use Cases: Pethuru Raj and Anupama C. Rajan, CRC Press

Mobile Technologies for Supporting IoT Ecosystem

Requirements of mobile network to support IoT devices :

1. Support for massive number of devices(10-100 time more)
2. Support for high data rate (10-100 time more data rate)
3. Reduce latency between end-to-end devices
4. Provide consistent quality of experience (QoE)
5. Reduce capital operation cost

Key features in 5G networks in order to cater to the above Requirements :

1. Software Defined Networking (SDN)
2. Network Function virtualization

Software Defined Networking

Networking architecture that separates the control plane (network control) from the data plane (network devices) and centralizes the network controller (data embedded into the controller).

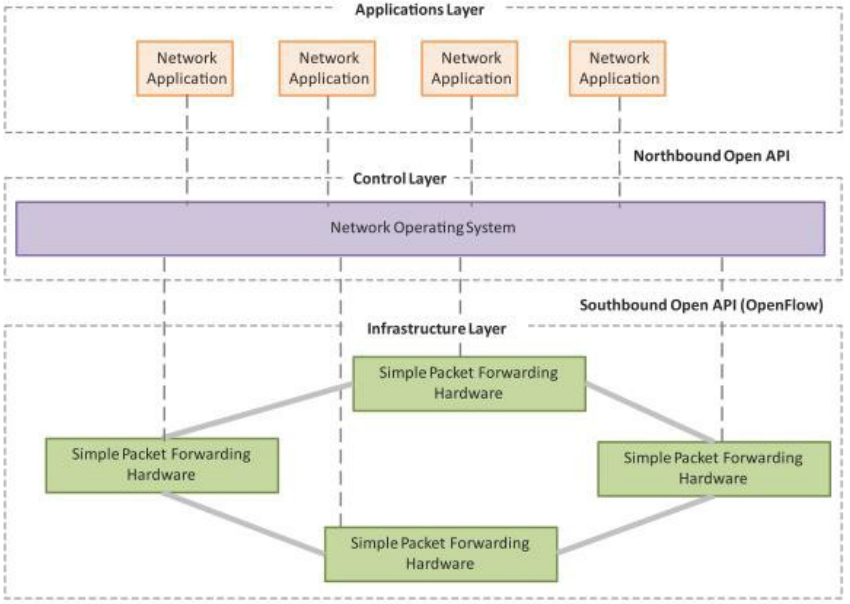
Separation of control enables network services to be abstracted from the underlying components and helps network to be treated as logical entity

SDN controllers maintain a unified view of the network and make configuration, management and provisioning simpler

Underlying infrastructure uses packet forwarding

Hardware as opposed to specialized hardware

In conventional networks



Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

The Internet's Landscape

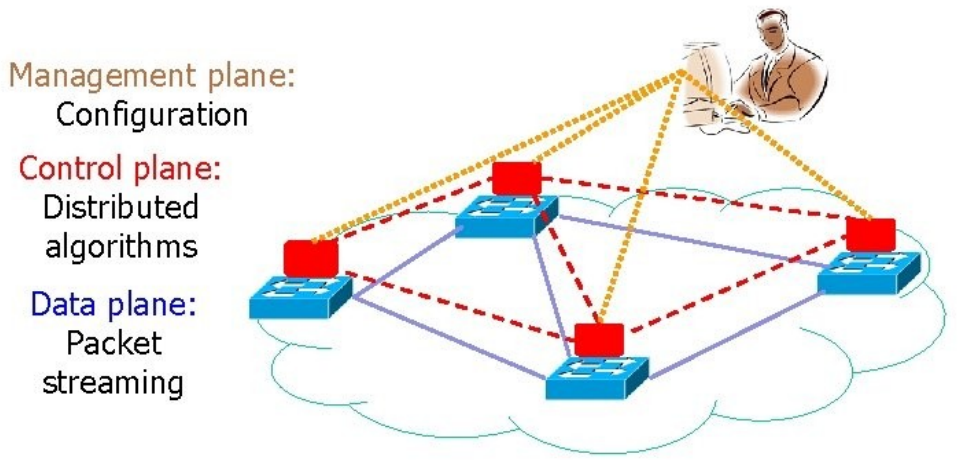
Innovation in Applications

Innovation in Technologies

Stagnant Internet Protocols **TCP/IP, BGP, DNS, OSPF**

Where is the Problem ?

Traditional Computer Networks



Proprietary software and vendor-specific configuration interfaces

A plane is an abstract conception of where certain processes take place.

Control plane : how packets are forwarded;
Ex: process of creating routing tables

Data plane : how packets should forwarded;
Ex: access control, traffic monitoring

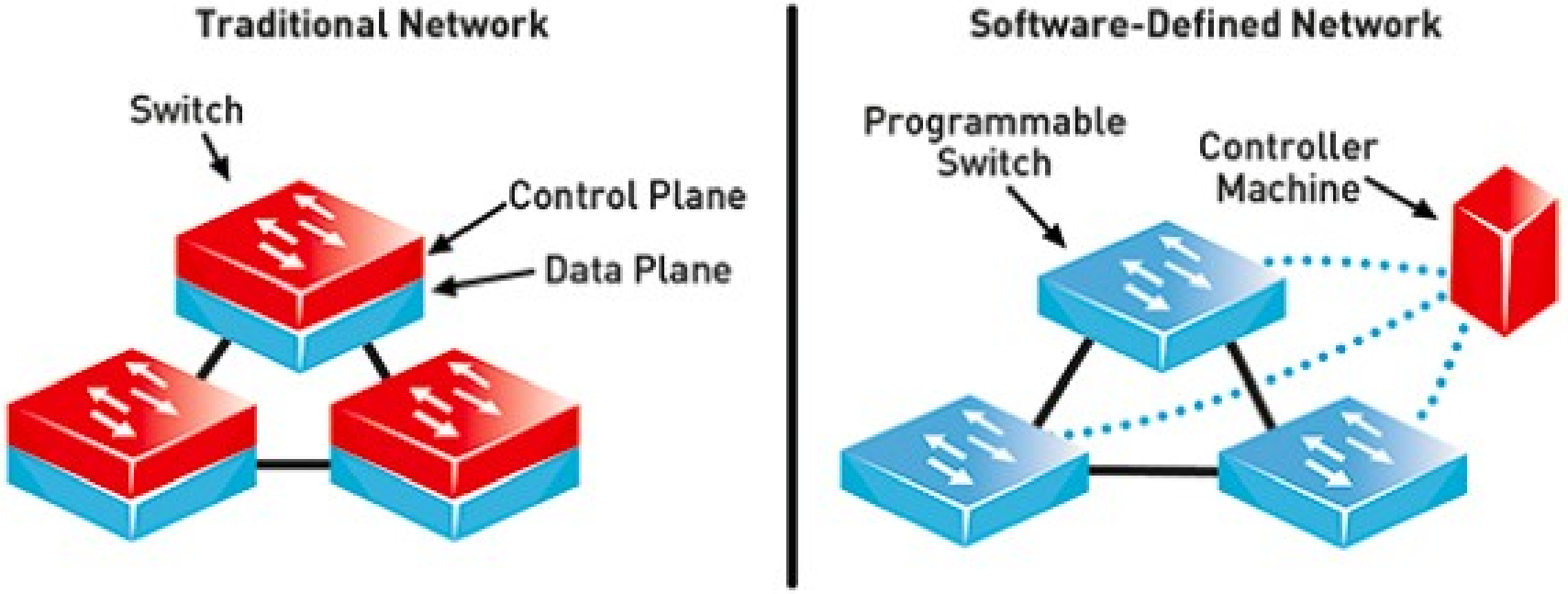
Management plane : collect, measure and configure equipments

1. **Closed equipment** - Software bundled with hardware ; Vendor specific interfaces

2. **Over Specified**
3. **Few people who innovate**
4. **Operating a network is expensive**
5. **Buggy software in the equipment**

Separating the Control and Data Plane

Vendors provide the hardware (data plane) and we decide control plane by writing custom logic - software



Why SDN?

Virtualization: Use network resource without worrying about where it is physically located, how much it is, how it is organized, etc.

Abstraction ⇒ Virtualization.

Orchestration: control and manage lot of devices with one command.

Programmable: able to change behaviour on the fly

Dynamic Scaling: able to change size, quantity

Virtualization ⇒ Scaling

Automation: minimize manual involvement - Troubleshooting, Reduce downtime, Policy enforcement

Why SDN?

- **Visibility: Monitor resources, connectivity**
- **Performance: Optimize network device utilization, Traffic engineering/Bandwidth management, Capacity optimization, Load balancing, High utilization, Fast failure handling**
- **Service Integration: Load balancers, firewalls, Intrusion**

Openness: Full choice of "How" mechanisms

⇒ Abstraction:

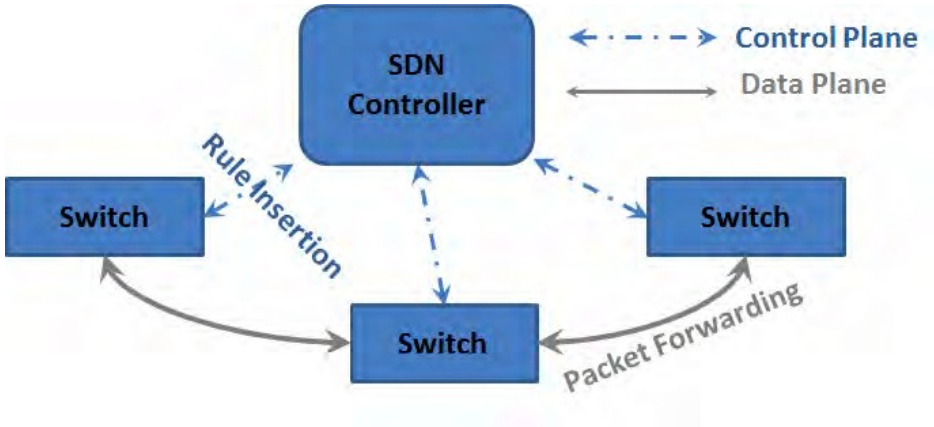
Abstract = Summary = Essence = General Idea ⇒ Hide the details

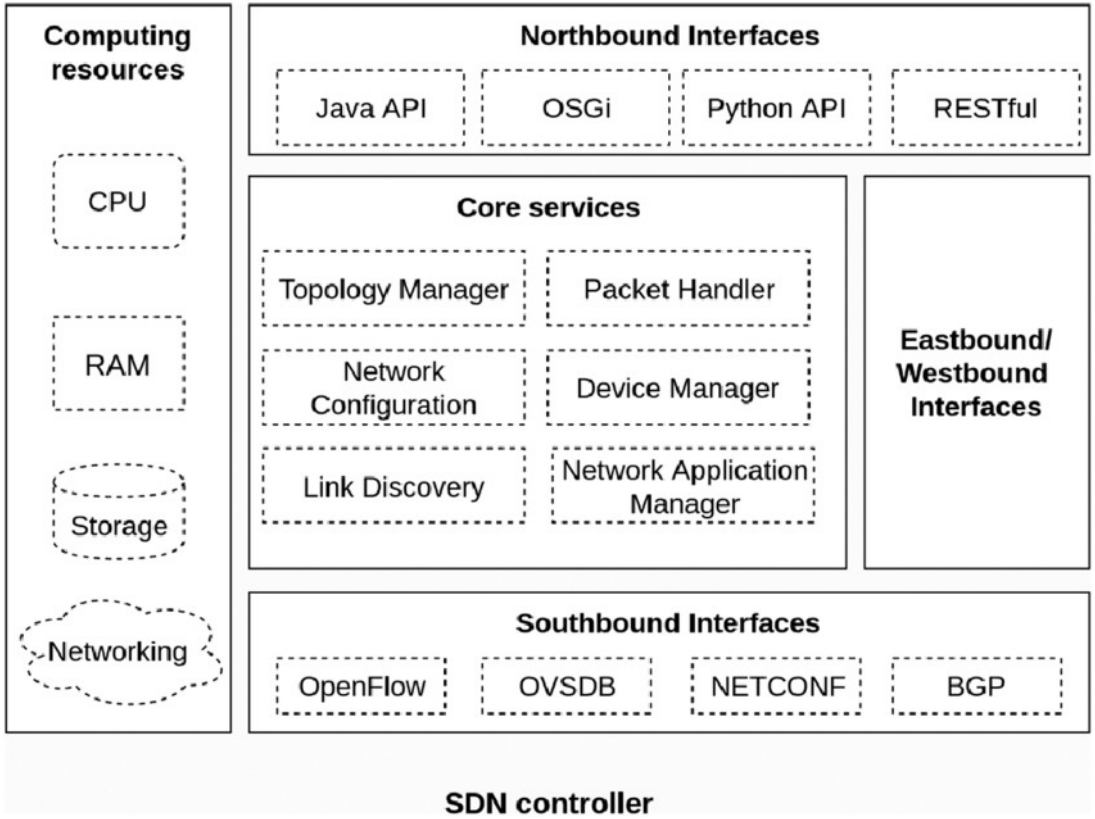
Define tasks by APIs and not by how it should be done.

SDN Controller

An application that manages flow control to enable intelligent networking

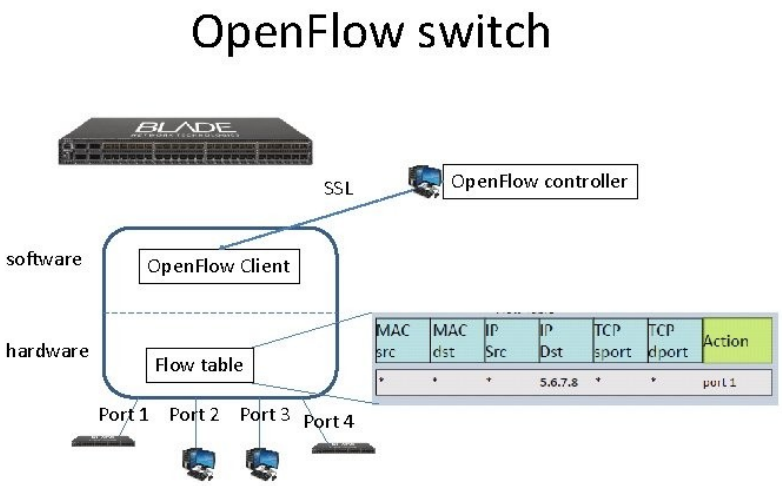
They are based on protocols such as Open flow that allow servers to tell switches where to send packets

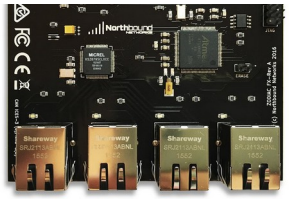




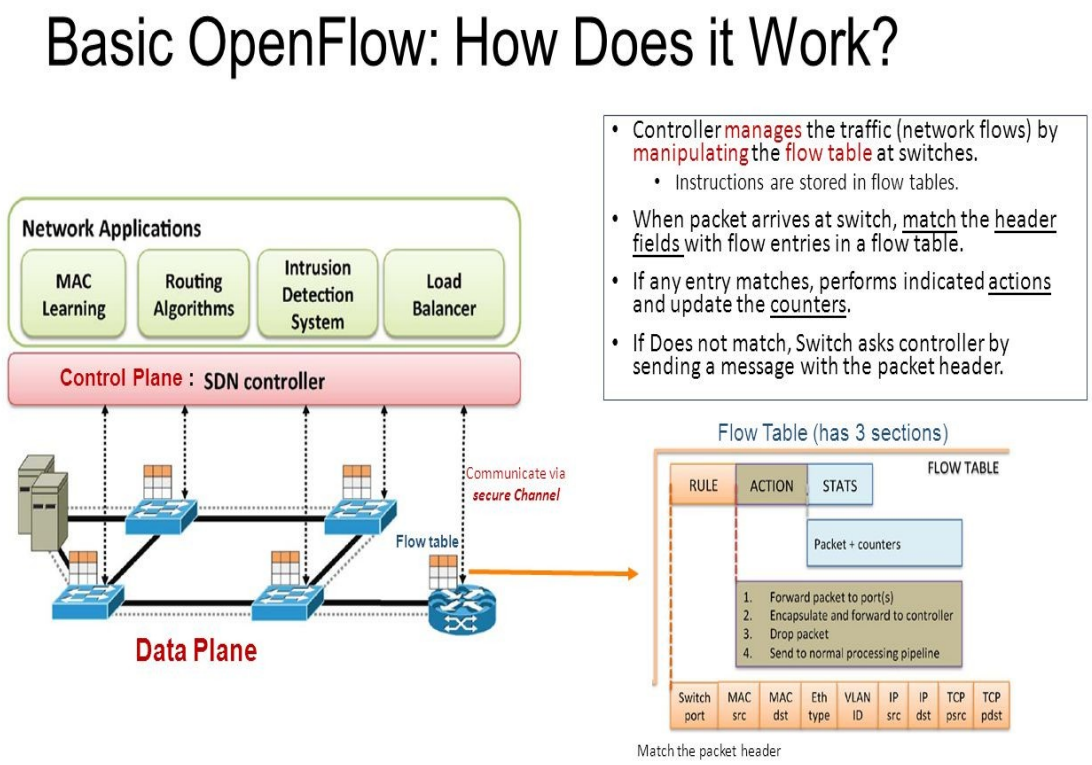
Open Flow

- **Protocol for controlling the forwarding behaviour of ethernet switches in a SDN**
- **Specifications maintained by Open Networking Forum**





Zodiac FX Open Flow SDN switch

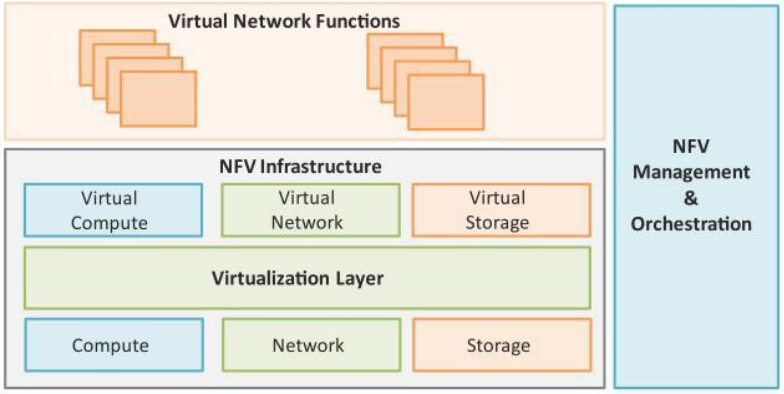


Network Function Virtualization (NFV)

Network Function Virtualization (NFV) is a technology that leverages virtualization to consolidate the heterogeneous network devices onto industry standard high volume servers, switches and storage.

Example : Virtual firewalls, load balancers, WAN accelerators, intrusion detection services

NFV can provide the infrastructure on which SDN can run.



Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

Key Elements of NFV

Virtualized Network Function (VNF) : VNF is a software implementation of a network function which is capable of running over the NFV Infrastructure (NFVI)

- **NFV Infrastructure (NFVI) :** NFVI includes compute, network and storage resources that are virtualized.

- **NFV Management and Orchestration :** NFV Management and Orchestration focuses on all virtualization-specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs.

Internet of Things, Bahga and Madisetty. Book website : http://www.internet-of-things-book.com

5G Architecture

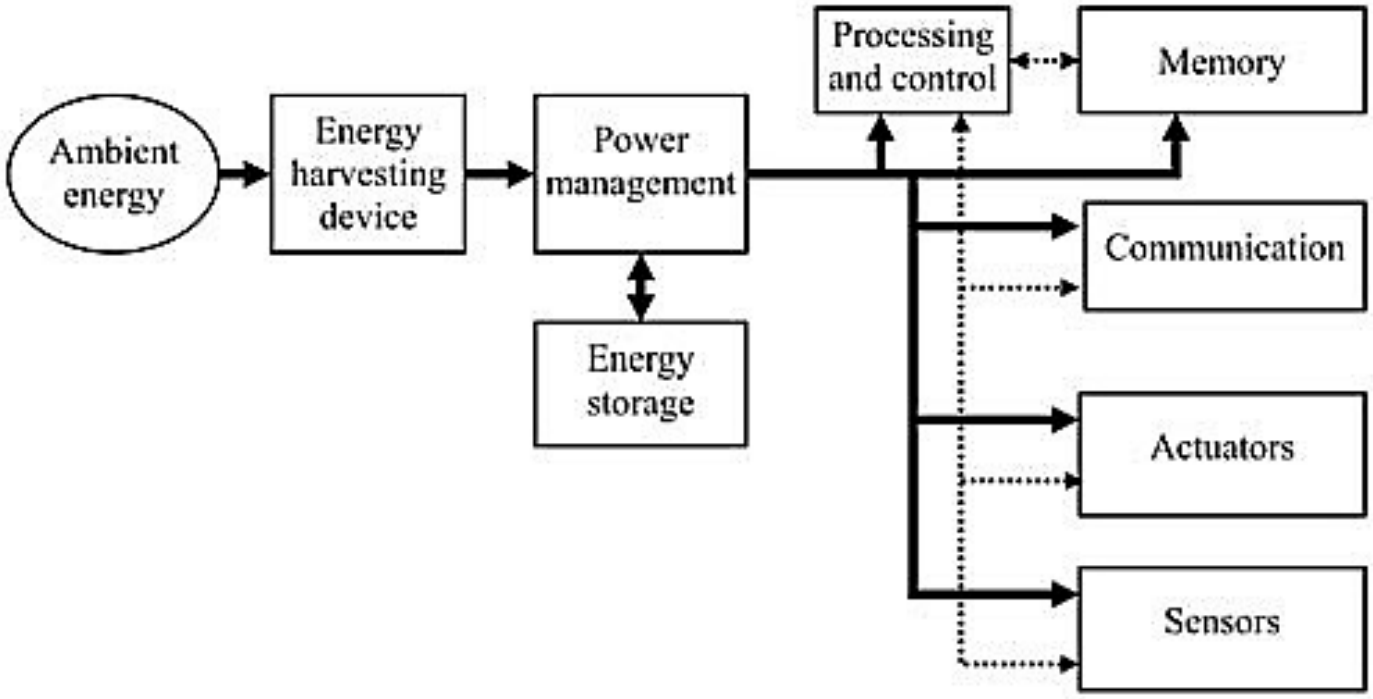
**High Frequency Band - ** Propagation Loss, Limited coverage Ex: Small cells
Solution : Small cells are overlaid on the coverage of large cells (operating at low frequency band)

Problem : Frequent control signalling between small cells and large cells in a heterogeneous network
Solution : Control (C-plane) and User plane (U-Plane) Decoupled Architecture; C-Plane at low frequency bands and U-Plane at available high frequency bands. This improves the efficiency of 5G architecture

Salient features of new 5G architecture :

1. Presence of 2 logical layers
2. Dynamic deployment of scaling network functions of the network cloud using SDN and NFV
3. Lean protocol stack by removing redundant functionalities

Energy Harvesting for Power Consumption in IoT Systems



Energy Harvesting in WSN

LPWAN Technologies

Low Power Wide Area Network (LPWAN) - Suitable for connecting devices that send small amounts of data over a long range with better battery efficiency
Ex : sensors

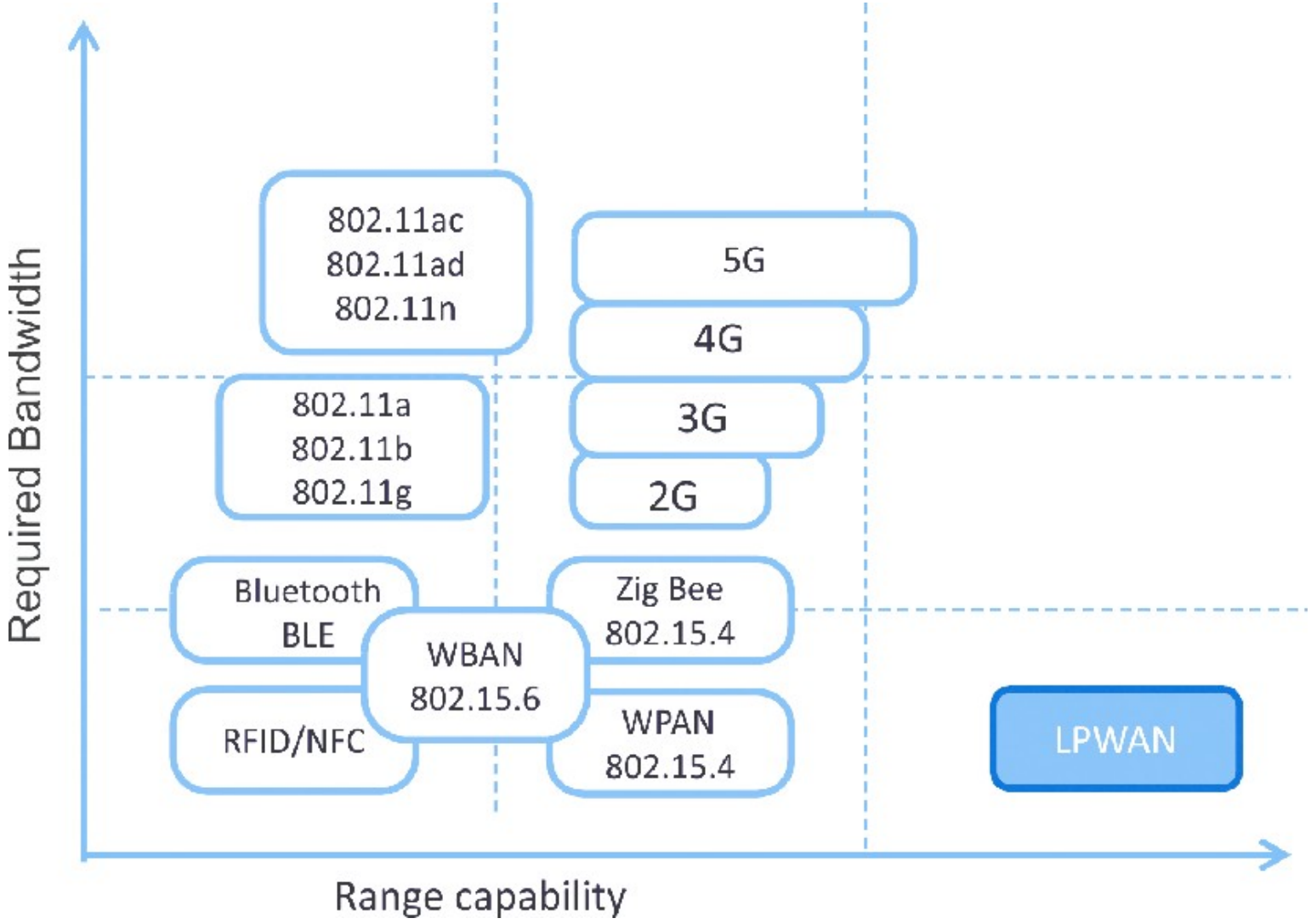
Key Features :

Long Range Communication – support nodes at distance of > 10 km from gateway
Low Transmission Data Rate - < 5000 bits of data / sec
Low Power Consumption – long battery life (~ 10 years)

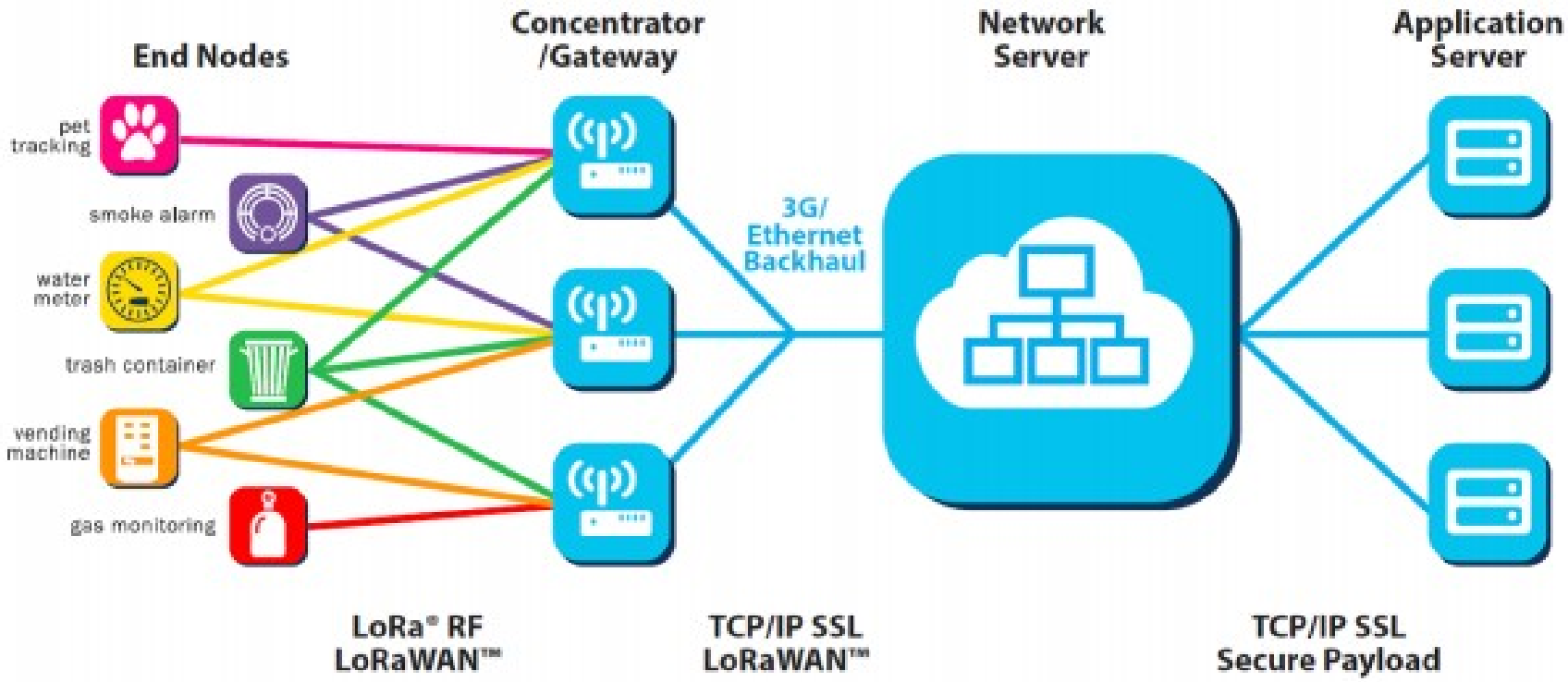
Suited For :

Fixed, medium to high density connections
Long life, battery powered applications

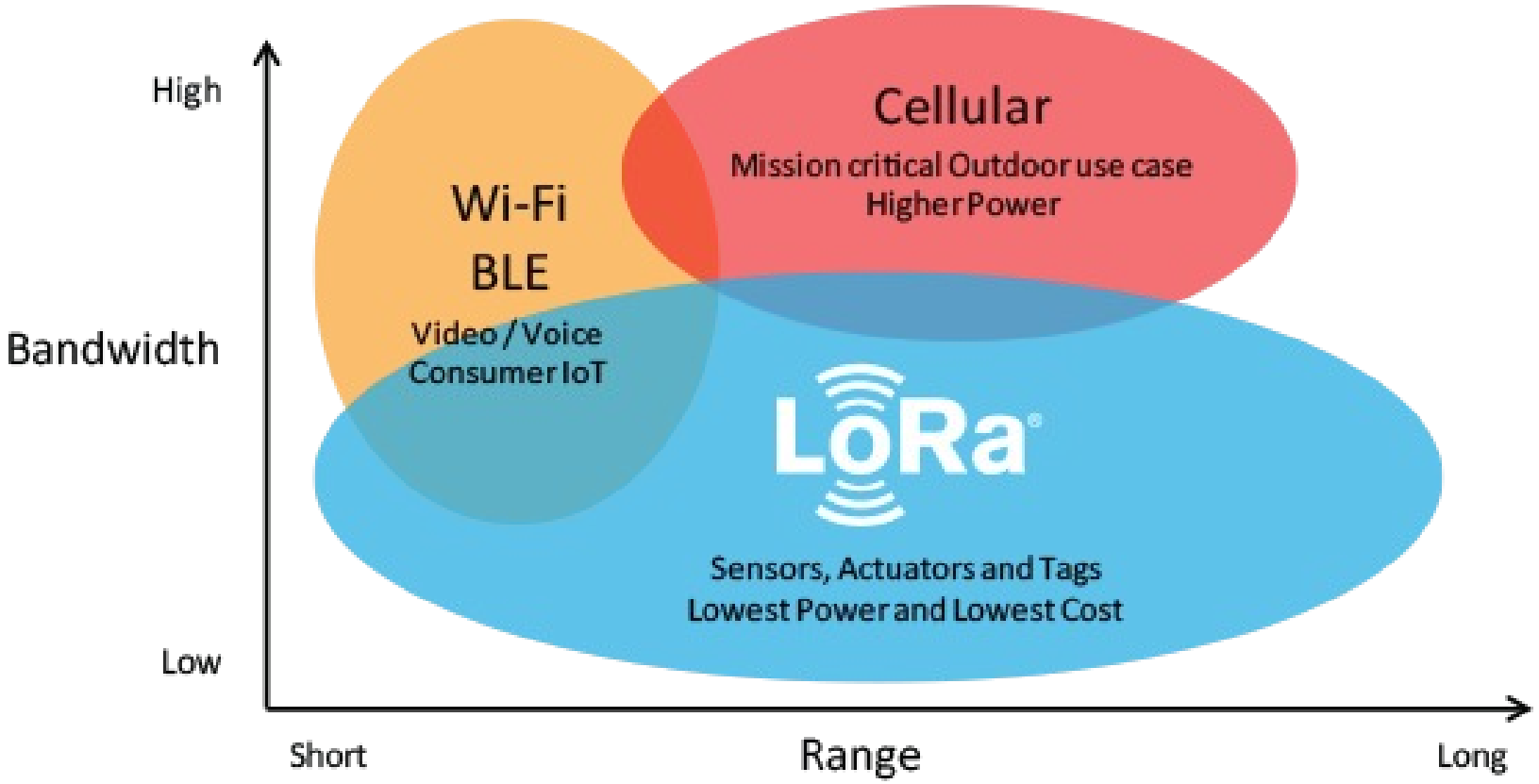
Bandwidth Requirements of LPWAN Network Topologies



LPWAN Network Topologies



LoRaWAN


High
Bandwidth
Low
Short
Range
Long
Wi-Fi
BLE
Video / Voice
Consumer IoT
Cellular
Mission critical Outdoor use case
Higher Power
LoRa
Sensors, Actuators and Tags
Lowest Power and Lowest Cost