INTERNET OF THINGS (DESIGN PRINCIPLES FOR CONNECTED DEVICES)

By: Dr. Raj Kamal

Chapter 2

IoT Open Systems Interconnection (OSI) model, ITU-T Reference Model and ETSI High Level M2M Architecture

Learning Objectives

- Summarize recent initiatives of international organizations for design standardization of IoT/ M2M architectural layers and domain
- Explain wireless and wired communication technologies for physical cum data-link layer functions
- List functions of data-adaption later, and the device and gateway domain
- Discuss ease of designing and affordability of IoT devices

Introduction

- IoT or M2M device data refers to the data meant for communication to an application, service or process. Data also refers to data received by a device for its monitoring or for actions at actuator in it.

- Data stack denotes the data received after the actions at various in-between layers (or level or domains).

- Key terms:

  Layer: Physical Layer, Application Layer

  Level, Domain, Gateway, IP, Header, Packet, PDU, MTU

  Star Network, Mesh Network, End-Point Device or Node

  Coordinator, Master, Slave, Router, ISM Band, Application, Service, Process

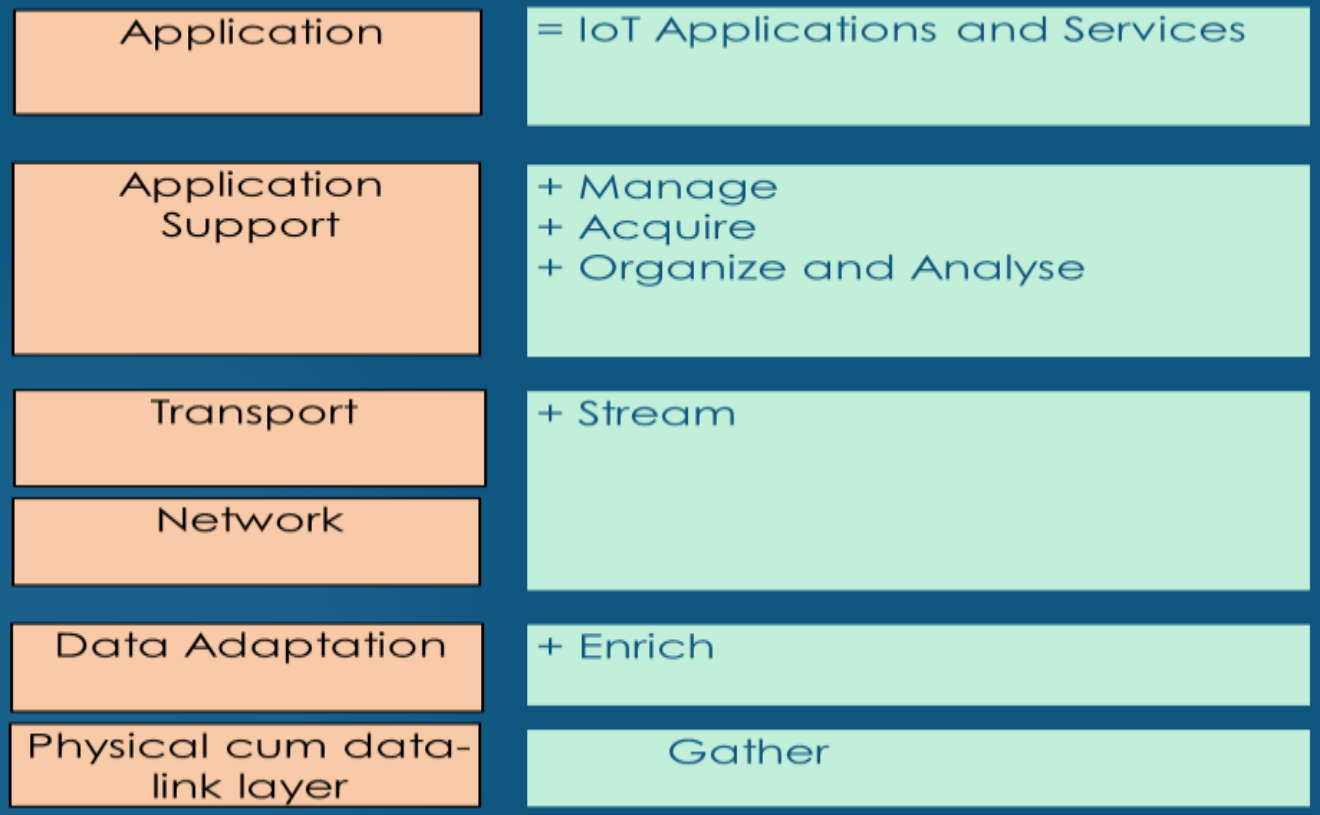
IETF Modified-OSI Six Layers

- Data communicate at source end from Application end (Layer 6) device-end (Layer 1)
- Stack means Data part + protocol header bits/words which transfer at one go
- Data stack creates by the processes at in-between layers from top layer 6 to bottom functional-layer 1 for communication

IETF Modified OSI Six Layers Architecture

- Data transmits from the device end (layer 1) from an Application, Service or Process end (Layer 6) and
- Data stack communicate between the physical layers at source and destination ends.
- Data stack receives at the device end (layer 1) and to an Application, Service or Process end (Layer 6)
- Data stack processes during the communication between the physical and application layers

Similarity between Generalised OSI and IETF Model



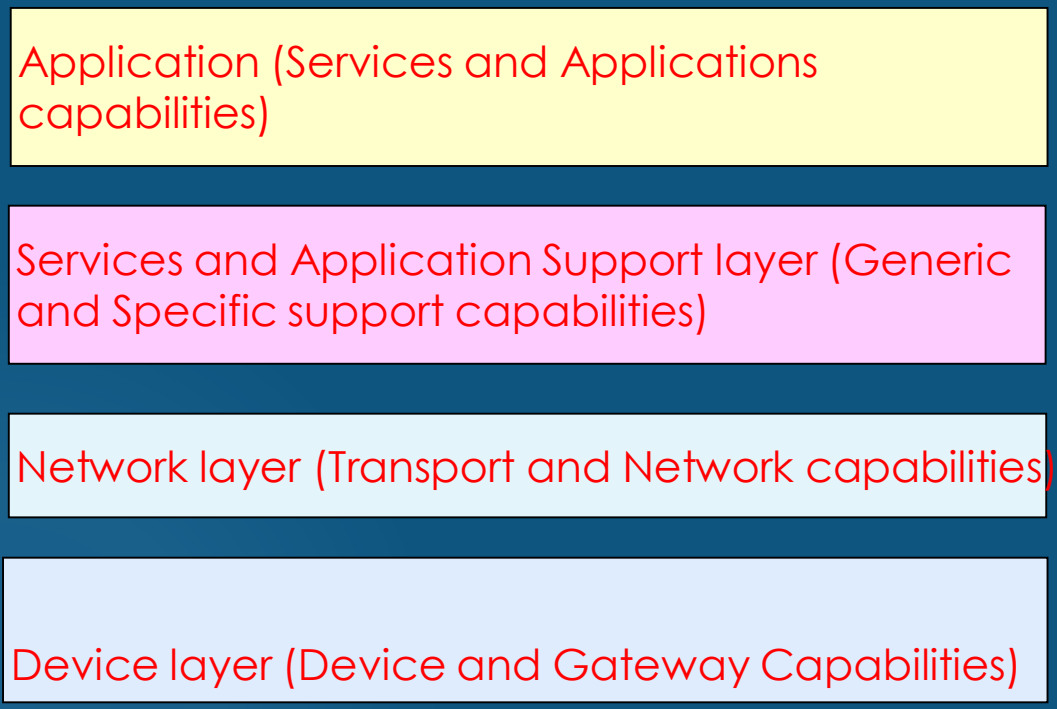
7-Layer Generalised OSI Model

IETF 6-Layer modified OSI Model

Example: Data Interchange in Streetlight

Layer 1	• Smart sensing and data-link circuit with each streetlight for transferring the sensed data to the layer 2
Layer 2	• Group controller controls a group of streetlights as per the program-commands from a Central station • Data Adaptation the group-controller receives data of each group through Bluetooth or ZigBee, then aggregates and compacts the data for communication to Internet,
Layer 3	• Network stream on the Internet to next layer
Layer 4	• Transport layer for device identity management, identity registry and data routing to next layer
Layer 5	• Application support by data managing, acquiring, organizing and analyzing
Layer 6	• Application a remotely stored service program which issues the commands or programs the firmware at the service controllers • Service controllers switch on-off, and monitor each group of streetlights in whole of the city.

ITU-T Reference Model



ITU-T Reference Model Four- Layers' Capabilities

- Data communicate from device-end (Layer 1) to Application end (Layer 4)
- Data stack creates by the processes at in-between layers; between the top layer 4 and bottom functional-layer 1.
- Stack means Data part + protocol header bits/words which interchanges between two layers
- Data also receives at the device layer (layer 1) from an Application, Service or Process end (Layer 4)
- Data stack processes bottom device layer to top functional-layer

ITU-T Reference Model - Details

Layer 1	Layer 2	Layer 3	Layer 4
Device • Device and Gateway Capabilities • (For example, Physical Devices' Functions in CISCO Reference Architecture)	**Network** • Transport and Network capabilities • For example, Connectivity layer in CISCO Reference Architecture)	**Services and Application Support** • Generic and Specific support capabilities • [For example, Data abstraction, Accumulation, Elements Analysis and Transformation (CISCO Reference Architecture)]	**Applications** • Services and Applications • (Collaboration, Processes and Application in CISCO Reference Architecture

Example: Internet of RFID

Layer 1

- Device and gateway capabilities
- RFID physical device-cum- RFID reader acquires the ID data, and communicate the enriched data according to a wireless protocol to an access point.

Layer 2

- Transport and Network capabilities
- Access network (access points and Internet connectivity to server)

Layer 3

- Services and application support layer capabilities at server
- RFID devices ID registry, ID management, RFIDs data routing to server or data center, data analysis for the time series device presence and device tracked positions.

Layer 4

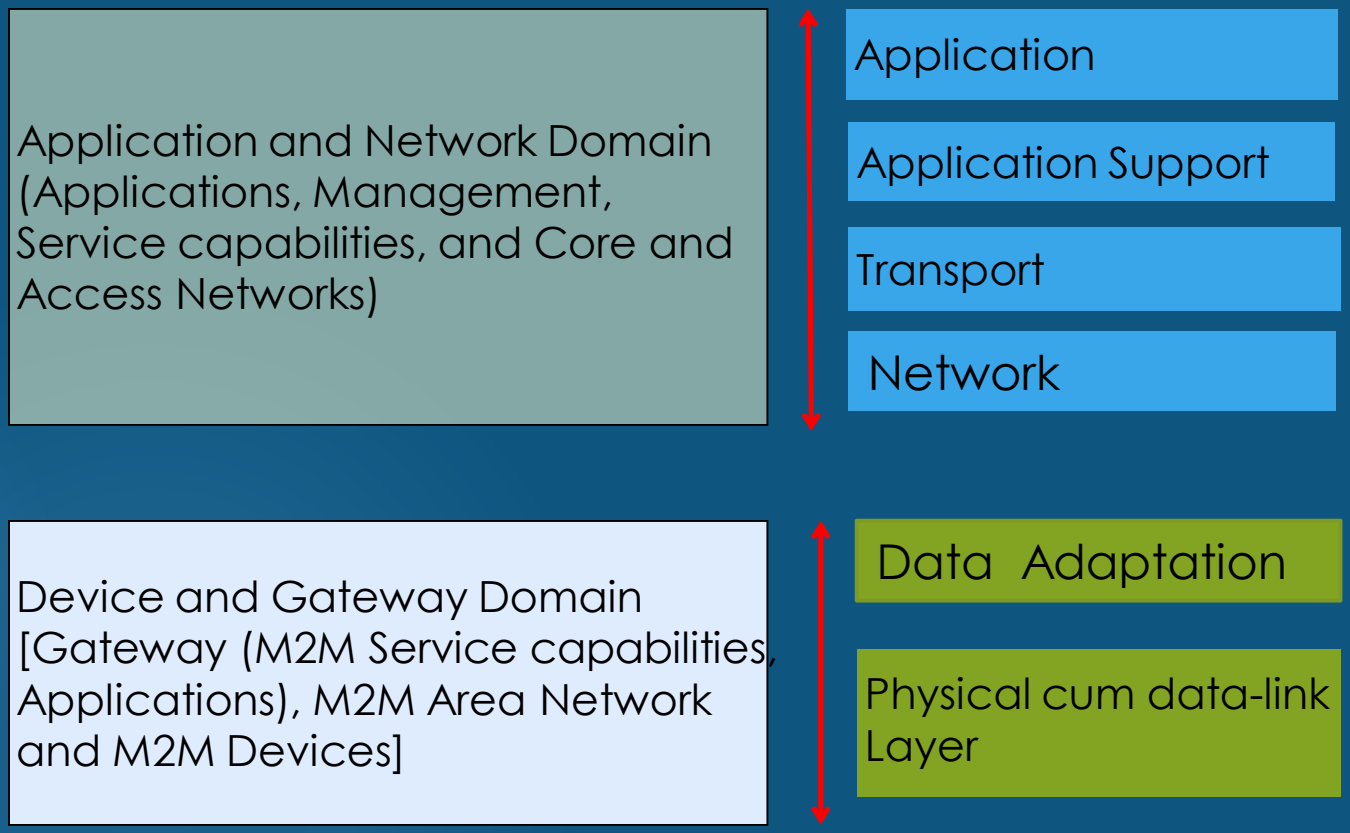
- **Application:** Services and Applications of RFIDs
- Tracking and inventory control of goods
- Business processes, for example, for the supply-chain management.

ETSI M2M Two Domains Reference Model

- Data communicate from device-end (Domain 1) to Application end (Domain 2)

The ETSI network domain has six capabilities and functions:

1. M2M applications
2. M2M service capabilities
3. M2M management functions
4. Network management functions
5. CoRE network (for example, 3G and IP networks, network control functions, interconnections among networks)
6. Access network (for example, LPWAN (low power wide area network), WLAN (Wi-Fi) and WiMax networks)



ETSI M2M-domains architecture and its High-level capabilities, and their correspondences with six layers of modified OSI reference model

Applications and Network Domain

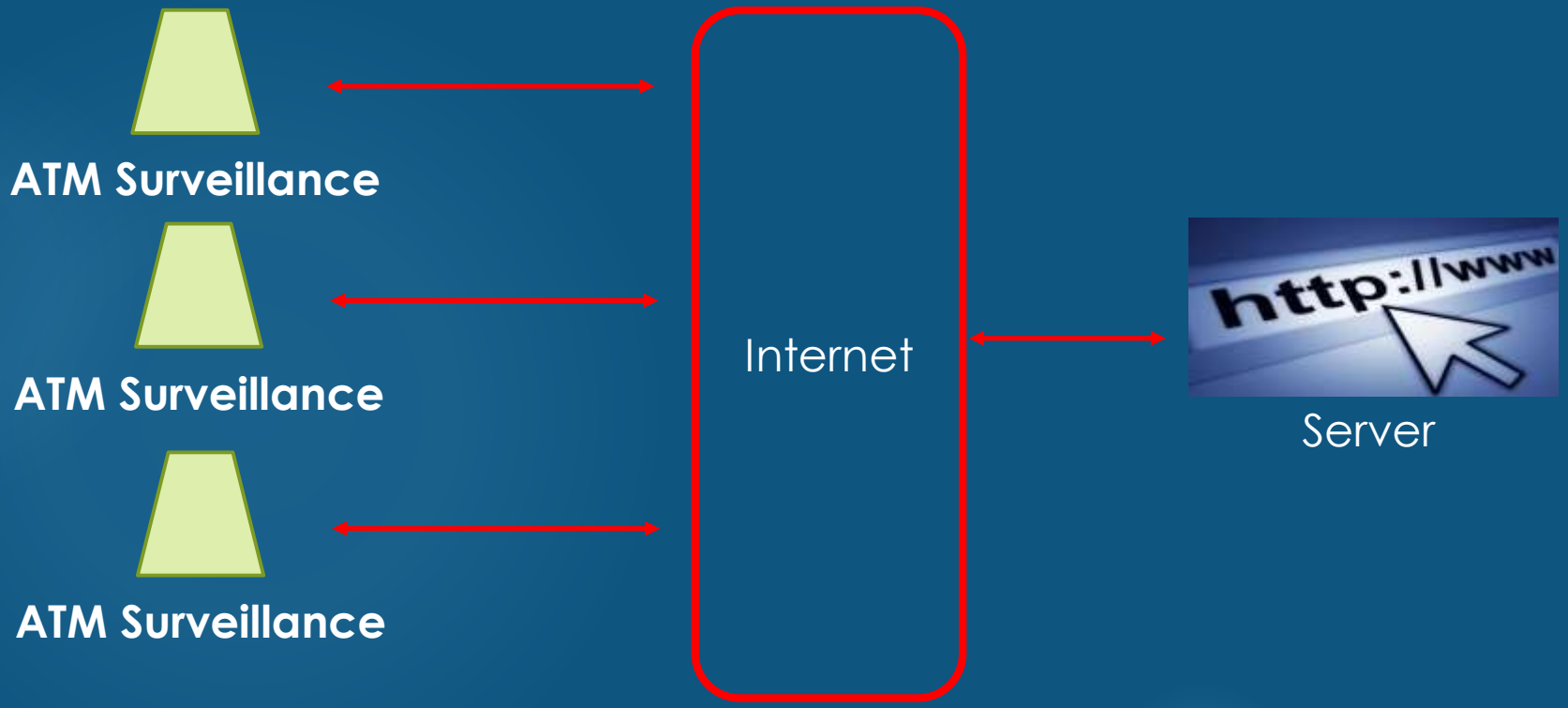
- M2M Applications, Service Capabilities, M2M Management functions
- Network Management Functions
- Core Network
- Access network

Devices and Gateway Domain

- Gateway between M2M area Network and core and access network
- M2M service capabilities and Applications.
- M2M Area Network
- M2M Device

Example: ETSI Domains and High Level Architecture

- Applications and services : ATMs-to-Bank Server



Applications and Network Domain

(Ref : Example)

- ATMs management functions
- Network management functions
- Banking Applications and Service capabilities for the ATMs
- Communicates with a core network
- Core connects the access networks of ATM gateways

Devices and Gateway Domain

(Ref : Example)

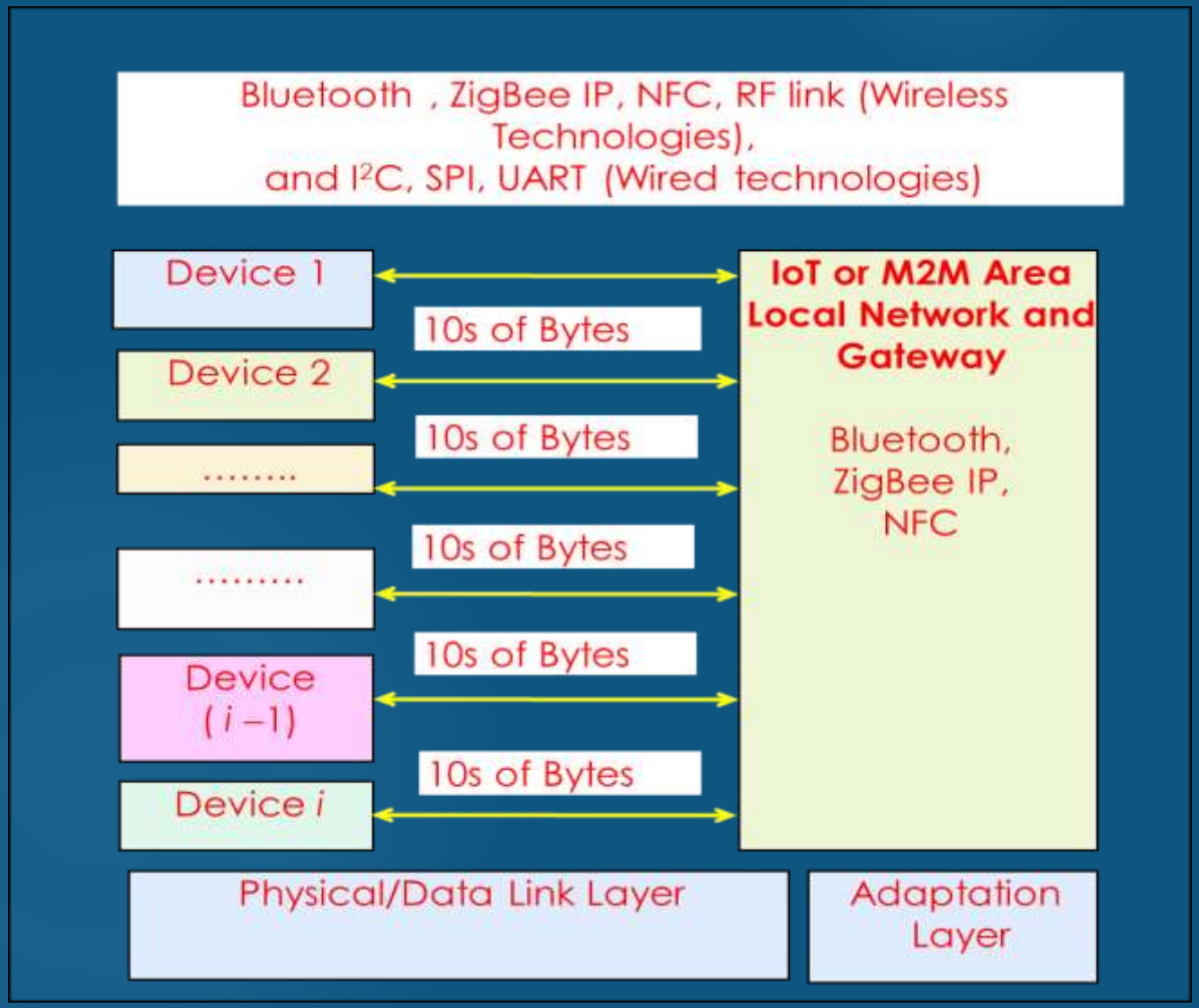
- Cards and ATMs
- ATM service capabilities and ATM applications
- ATM-gateway
- Cash dispensing system and a surveillance system

Connected Devices Communication to the Local Network and Gateway

- 1st to ith Connected devices connect to a Local Network and Gateway
- 10s of bytes communicate between a device and the local devices network

Physical/data-link Layer: Local Network and Connectivity

- Protocols RF, Bluetooth Smart Energy, ZigBee IP, ZigBee NAN (neighborhood area network), NFC, 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) or Mobile GSM



Connectivity of Connected devices 1st to ith and local Network and Gateway

NFC (Near Field Communication) wireless communication technology

- Short distance (10 cm-20 cm) Data exchange between devices
- Examples: proximity card reader/RFID/ IoT/ M2M/Mobile device, mobile payment wallet, Car electronic key, house or office entry key, Biometric passport reader.

NFC Devices

- Transmit and receive data at same instant
- Can generate RF fields for the nearby passive device such as passive RFID
- Check the RF field and detect collision of transmitted signal
- Check collision when the received signal does not match with the transmitted signal
- NFC device can receive and pass the data to a Bluetooth connection or standardized LAN or Wi-Fi using the information handover functions
- data transfer rates 106 kbps, 212 kbps, 424 kbps and 848 kbps
- Setup time 0.1s

Communication Modes

1. P2P (point to point) mode [Both devices use the active devices in which RF fields alternately generate when communicating],
2. Card-emulation mode
3. Reader mode [Device using NFC reads passive RFID device. The RF field is generated by active NFC de-vice. This enables passive device to communicate.]

RFID wireless Devices

- Transmit and receive data at same instant
- Can generate RF fields for the nearby passive device such as passive RFID
- Check the RF field and detect collision of transmitted signal
- Check collision when the received signal does not match with the transmitted signal

IC
Contains integrated circuit and antenna embedded or labeled onto the object

Type I
Passive device (without in-build power source) which gather charges from the received radiation and thus starts functioning

Type II
Active (with power source) [can on its own discover nearby node for data interchange]

Bluetooth

PROTOCOLS

- Bluetooth BR (Basic Rate 1)
- Bluetooth EDR (Enhanced Data Rate 2 Mbps and 3 Mbps)
- Bluetooth Low Energy (BT LE 1Mbps) two types of modes for the devices in the late

FEATURES

- Auto- synchronization between mobile and other devices when both use BT
- BT network uses features of self-discovery, self configuration and self-healing
- Support to NFC pairing for low latency in pairing the BT devices

ZigBee IP/ZigBee SE 2.0

FEATURES

- Self configuring
- Self healing
- Dynamic pairing mesh network
- Support for both multicast and unicast options

- Provides link level security using AES-CCM-128 (2.4 GHz ISM band frequency hopping spread spectrum (FHSS in BT BR/EDR)
- Direct sequence spread spectrum (DSSS in LE) 40-channel radio (2400 – 2483.5 MHz)

ZigBee IP/ZigBee SE 2.0 /2

PROTOCOLS

- Range is 10 to 200 m data transfer rate 250 kbps, low power operation
- ISM band frequencies direct sequence spread spectrum 16-channel radio

… Protocols for WPAN devices network

- ZigBee IP: an enhancement for the IPv6 connectivity
- ZigBee IP RFD (reduced function device) (functions for the 'sleepy'/ battery-operated device)
- Sleepy means one that wakes up infrequently, sends data then goes back to sleep

… Protocols for NAN and Smart Energy 2.0

- ZigBee NAN (Neighbourhood Area Network)
- A version for Smart Grid
- ZigBee SE 2.0 energy management and energy efficiency capabilities using the IP network

WiFi

An interface technology based on IEEE 802.11 protocol

- Wireless Local Area Networks (WLANs)
- Three main applications and connectivity through home access Point, public hotspots, enterprises, universities and offices.
- Wi-Fi enables Internet Connectivity of distributed WLAN networks

WiFi /2

FEATURES

- Generally the 2.4 GHz IEEE 802.11b adapter or 5 GHz (802.11a or 802.11g) or 802.11n or other 802.11 series protocols,
- Interfaces use 2.4 GHz or 5 GHz antenna,
- offers mobility and roaming
- have easy installation simplicity and flexibility,
- Easy installation simplicity and flexibility,
- Coverage range 30 m to 125 m,
- Limited coverage version 802.11a which coexists with b and g,
- Other versions 802.11b, 802.11g for high data rates up to 54 Mbps, and 802.11n
- Interoperability with wireless as well as wired infrastructure
- Ensures compatibility and enables easier access and hide complexity when enabling the wireless access to data, media and streams, applications and services

RF Transceivers and RF Modules

RF Modules

- Number of systems uses the RF modules
- Applications needing wireless connectivity
- Examples: security, telemetry, telematics, fleet management, home.

Simple RF circuits

- Transmitters, receivers, and transceivers
- An oscillator generates RF pulses of required active duty cycle and connects to a transmitter

GSM, GPRS, UMTS/ LTE and WiMax

- Mobile phones provisions for the USB wired port, BT and Wi-Fi devices
- Wireless Internet connectivity using GSM, GPRS, UMTS/ LTE and WiMax services of Mobile service provider and Wi-Fi using PCMCIA card

Wireless USB

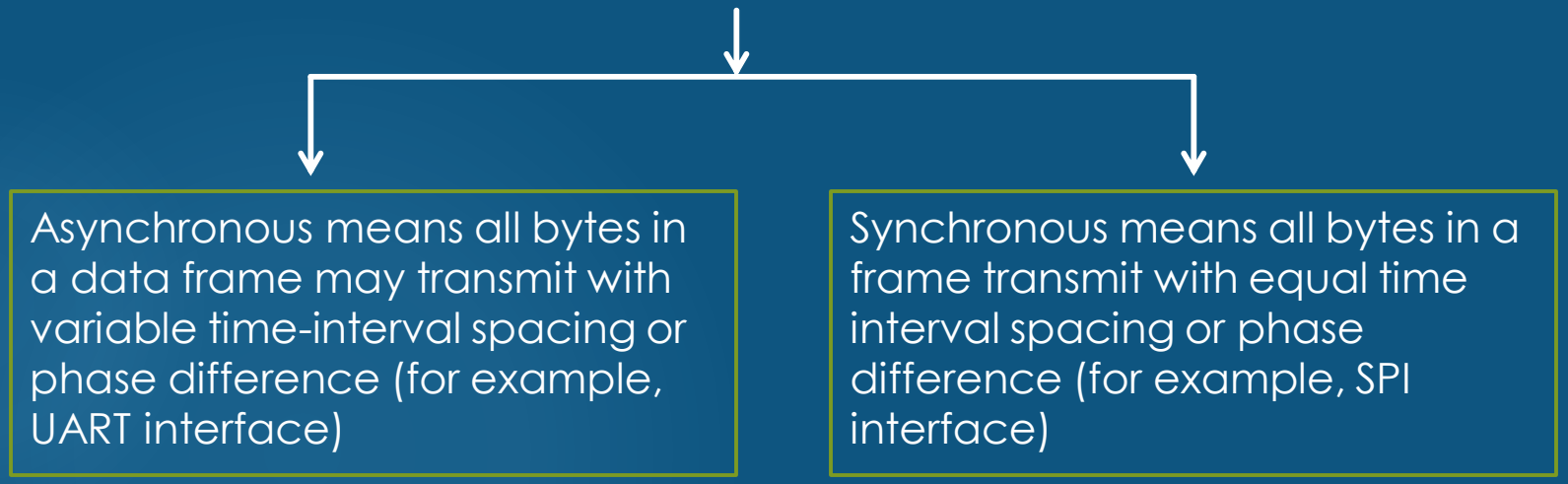
- Wireless extension of USB 2.0 and it operate at UWB (ultra wide band) 5.1 GHZ to 10.6 GHz frequencies. It is for short-range personal area network (high speed 480 Mbps 3 meter or 110 Mbps 10 meter channel).

FEATURES

- A host wire adapter (HWA) and a device wire adapter (DWA) wireless USB solution
- Supports the dual-role devices (DRDs). A device can be a USB device as well as limited capability host.

Serial and Parallel Communication

- Serial means one bit after another in successive time intervals over a wire



- Parallel all bits in a word at the same times communicate at different wires

Examples: Wired communication

- UART or USART
- SPI

UART (Universal Asynchronous Receiver and Transmitter)

- Serial asynchronous communication (transmission) of 8 bits serially
- A start bit at start of transmission of a byte on serial TxD (Transmitter Data) output line
- An additional bit appends between stop bit and last bit of the byte

USART (Universal Synchronous/ Asynchronous Receiver and Transmitter)

- Two modes: Synchronous/Asynchronous
- Mode 1: Synchronous means all bytes in a frame transmit with equal time interval spacing and a set of sync code bits between successive bytes;
- Mode 2: Asynchronous mode as UART

SPI (Serial Peripheral Interface) Bus

- ICs mutually network through four set of signals
- SCLK, MISO, MOSI, and SS (slave select) on four wires
- Master input slave output (MISO) and master output slave input (MOSI) for synchronous serial bits I/Os at the master and slave
- IOs are as per synchronizing clock of the master SCLK

Examples: Wired Communication / 2

- I2C (Inter-Integrated Circuit) Bus
- Ethernet Bus

I2C (Inter-Integrated Circuit) Bus

- ICs mutual network through a common synchronous serial bus
- Four potential modes of operation (master transmit, Master receive, slave transmit and slave receive)
- Three I2C bus standards: Industrial 100 kbps I2C, 100 kbps SM I^2C, and 400 kbps I2C
- I^2C Bus has two lines that carry the signals— one for the clock and one bi-directional data.

Ethernet Bus

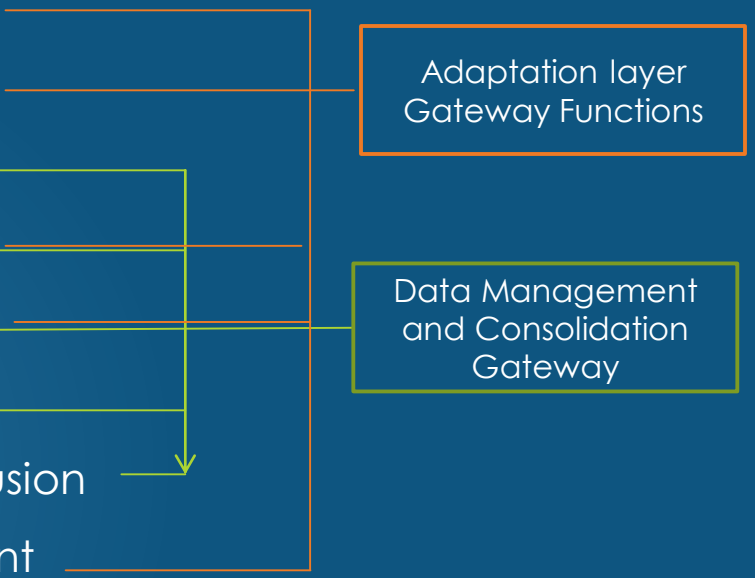
- Uses wired bus topology
- Transmission speeds: 10 Mbps, 100 Mbps (Unshielded and Shielded wires)
  - 1 Gbps (high-quality coaxial cable)
  - 4 Gbps (in twisted pair wiring mode)
  - 0 Gbps (fiber-optic cable)
- Uses 48-bit MAC addresses assigned distinctly to each device or computer on the LAN.
- Address Resolution Protocol (ARP) resolves 32 bit IP addresses at Internet Application into the 48 bit destination host media address when receiving data from Internet protocol.

Adaptation Layer

1. Data Management
2. Data Enrichment
3. Consolidation
4. Transcoding
5. Privacy,
6. Security,
7. Integration,
8. Compaction and Fusion
9. Device Management

Adaptation, Management and Gateway

1. Data Management
2. Data Enrichment
3. Consolidation
4. Transcoding
5. Privacy,
6. Security,
7. Integration,
8. Compaction and Fusion
9. Device Management



Data Source and Data Destination

- Each device and each device resource assigned an ID for specifying the data source
- Data destination Addressing
- Header fields add the destination address

Data Characteristics, Formats and Structures

- Taken into account when communication to next layer

Formatting:

- XML, JSON, TLV formats
- MIME type file for Internet

Device Management Functions

- Provisioning for the device ID or address,
- Device activation, and
- Device configuring.
- Accepting subscription for its resources

- Fault management: Course of actions and guidelines to be followed in case of a fault
- Forwarding function when DM server and device can interact without reformatting or structuring
- Does protocol conversion when device
- DM server using distinct protocols
- Does proxy function in case the an intermediate pre-fetch required in lossy environment or network environment needs

Device Configuring

- Managing device parameters and settings,
- Device registration,
- Device de-registration,
- Device attaching, (enabled to communicate) and
- Device detaching (disabled to communicate)

Data Privacy

- Examples: Patient medical data, data for a company supplies from and to different locations, and changes in inventories
- Privacy and protection from consciously or unconsciously transferring to untrustworthy destination using the Internet

Privacy Model

- Depends on following components:
  I. Device and Applications Identities management
  II. Authentication
  III. Authorisation
  IV. Trust and
  V. Reputation

Data Security Sub-layer for Confidentiality and Authorization

- A standard algorithm AES (Advanced Encryption Algorithm based on symmetric 128-bit block data encryption)
- CCM mode (Counter with CBC-MAC)
- CBC stands for cryptographic block cipher with a block length of 128 bits.
- CCM is method which provisions for the authenticated encryption algorithm for confidentiality and authentication

Data Gathering

- Data gathering means data- acquisition from the device(s)

Four modes of data gathering are:

1. Polling– means data sought from a device by addressing the device
2. Event based–
3. Scheduled interval–
4. Continuous monitoring

Data Dissemination: Prior Actions

1. Aggregation of joining together present and previously received data.
2. Compaction making information short without changing the meaning or context
3. Fusion means formatting the information received in parts through various data frames and several types of data (or data from several sources),

Energy Dissipation due to Data Dissipation

- Higher the data rate, the greater will be the energy consumed
- Higher is the radio frequency used, the greater will be the energy consumed
- Energy efficient computations by using concepts of data aggregation, compaction and fusion

Ease of Designing

- Design for connected devices for IoT Applications, Services and business processes
- Designer considers the ease in designing the devices physical, data link, adaption layers and gateway
- Means availability of sensors, actuators, controllers and IoT devices
- Low in cost and hardware
- Use preferably open source software components and protocols
- Device hardware should embed minimum of components
- Use ready solutions for ease in designing local devices personal area network
- Ensure the secure connectivity with the Internet

Affordability of IoT devices

For example, RFID or card

- The card: An embedded microcontroller, memory, OS, NFC peripheral interfaces, access point based device activation, RF module and transceiver and all that at low cost

For example, Wireless sensors use Mote (mobile terminal)

- Mote: Low cost devices with open source OS (tiny OS) and software components
- Provides ease and affordance in the WSN networks