NPTEL ONLINE
CERTIFICATION COURSES

Connectivity Technologies – Part II

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

6LoWPAN

Introduction

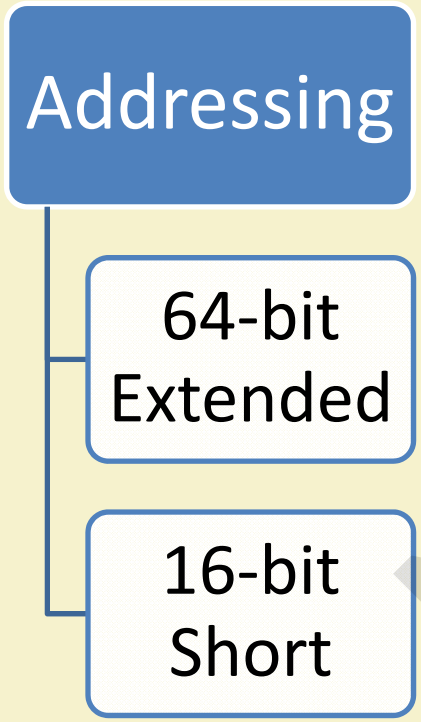
- ✓ Low-power Wireless Personal Area Networks over IPv6.
- ✓ Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- ✓ Allows low-power devices to connect to the Internet.
- ✓ Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

Features of 6LoWPANs

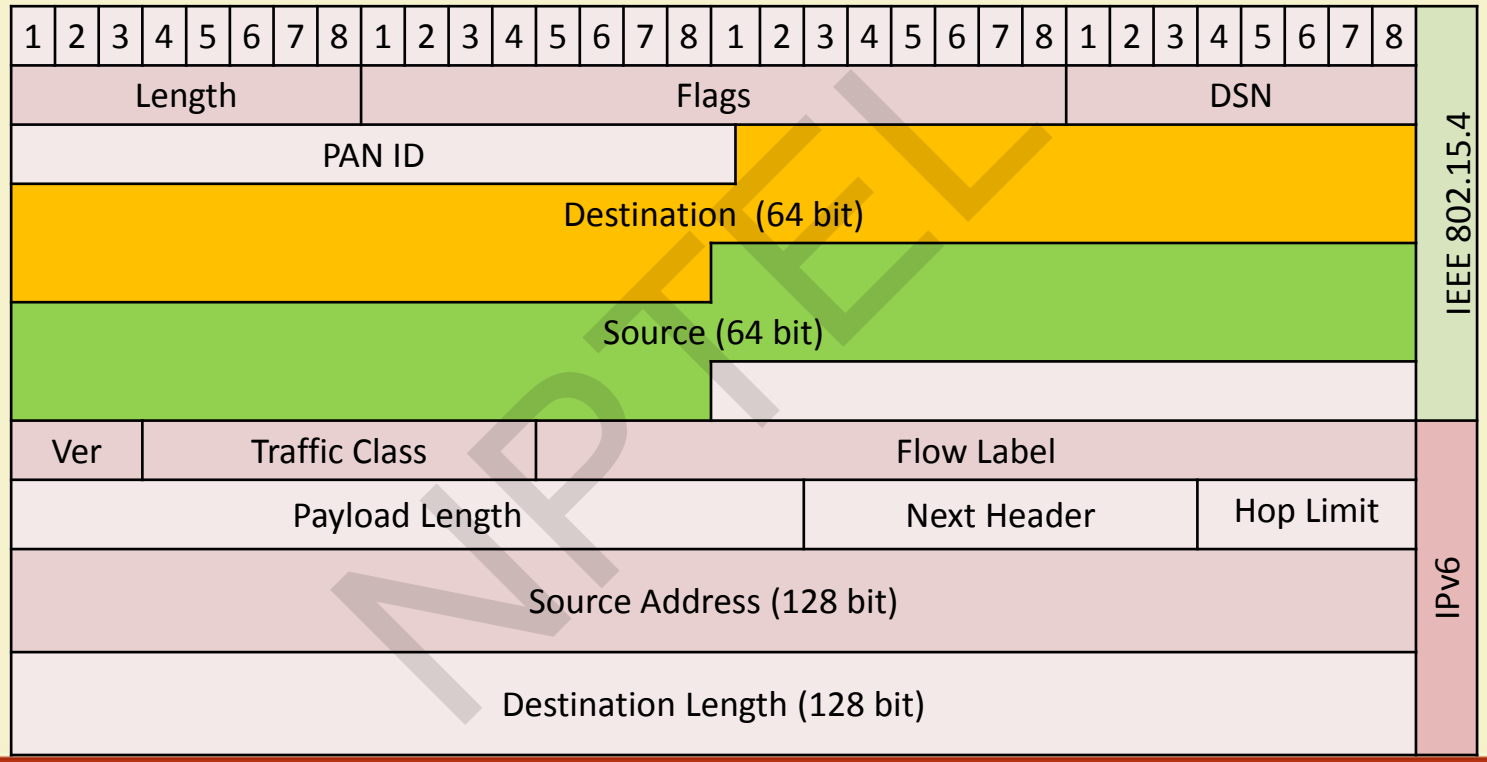
- ✓ Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).
- ✓ Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
- ✓ IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.
- ✓ Uses include IoT, Smart grid, and M2M applications.

Addressing in 6LoWPAN

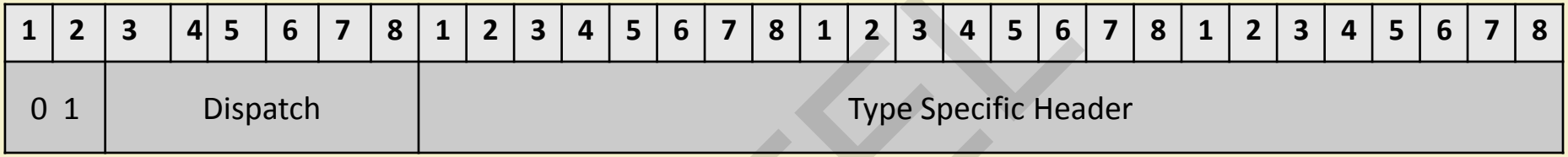


- 64-bit addresses: globally unique
- 16 bit addresses: PAN specific; assigned by PAN coordinator
- IPv6 multicast not supported by 802.15.4
- IPv6 packets carried as link layer broadcast frames

6LowPAN Packet Format

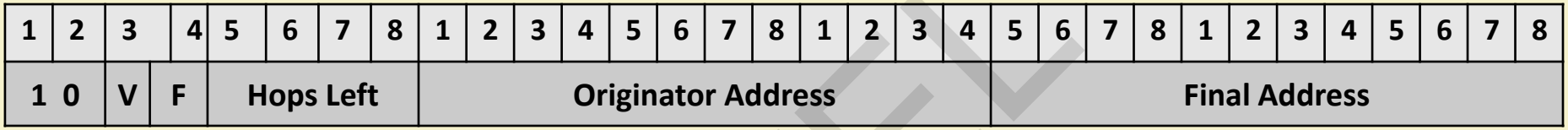


Header Type: Dispatch Header



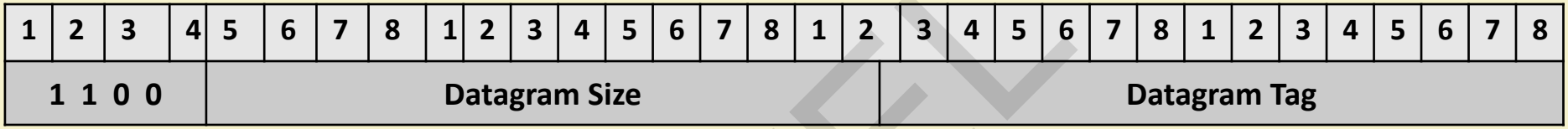
- **Dispatch:** Initiates communication
- **0,1**: Identifier for Dispatch Type
- **Dispatch**:
  - 6 bits
  - Identifies the next header type
- **Type Specific Header:**
  - Determined by Dispatch header

Header Type: Mesh Addressing Header

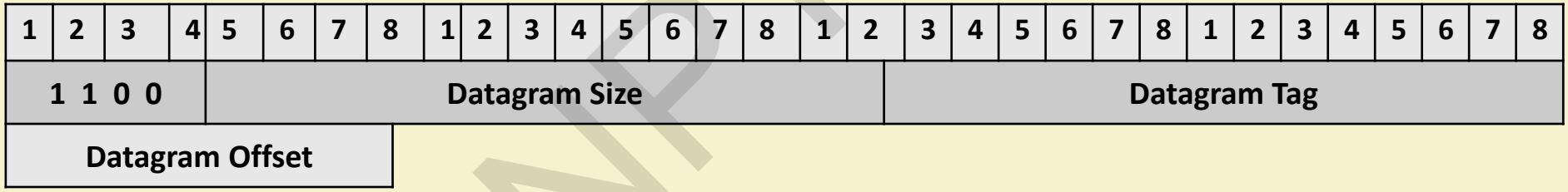


- **1,0**: ID for Mesh Addressing Header
- **V**: '0' if originator is 64-bit extended address, '1' if 16-bit address
- **F**: '0' if destination is 64-bit addr., '1' if 16-bit addr.
- **Hops Left**: decremented by each node before sending to next hop

Header Type: Fragmentation Header



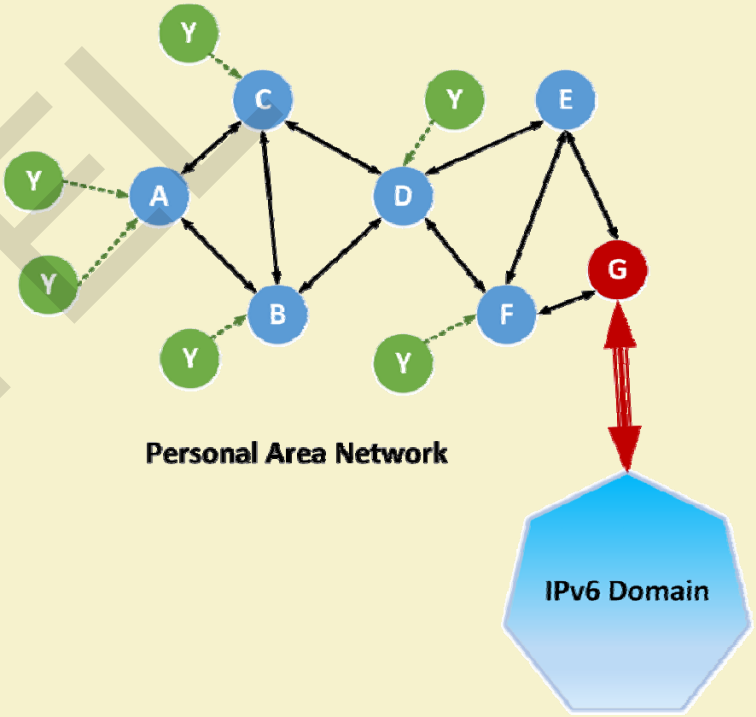
(a) First Fragment



(b) Subsequent Fragment

6LoWPAN Routing Considerations

- ✓ Mesh routing within the PAN space.
- ✓ Routing between IPv6 and the PAN domain
- ✓ Routing protocols in use:
  - **LOADng**
  - **RPL**



LOADng Routing

- ✓ Derived from AODV and extended for use in IoT.
- ✓ Basic operations of LOADng include:
  - Generation of **Route Requests (RREQs)** by a LOADng Router (originator) for discovering a route to a destination,
  - **Forwarding of such RREQs** until they reach the destination LOADng Router,
  - Generation of **Route Replies (RREPs)** upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)*. IETF. I-D draft-clausen-lln-loadng-14

- If a route is detected to be broken, a **Route Error (RERR)** message is returned to the originator of that data packet to inform the originator about the route breakage.
- **Optimized flooding** is supported, reducing the overhead incurred by RREQ generation and flooding.
- Only the destination is permitted to respond to an RREQ.
- Intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.
- RREQ/RREP messages generated by a given LOADng Router share a single unique, monotonically increasing sequence number.

Source: Clausen, T.; Colin de Verdiere, A.; Yi, J.; Niktash, A.; Igarashi, Y.; Satoh, H.; Herberg, U.; Lavenu, C. et al. (January 2016). *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)*. IETF. I-D draft-clausen-lln-loadng-14

RPL Routing

- ✓ Distance Vector IPv6 **routing protocol for lossy and low power networks.**
- ✓ Maintains routing topology using low rate beaconing.
- ✓ Beaconing rate increases on detecting inconsistencies (e.g. node/link in a route is down).
- ✓ Routing information included in the datagram itself.
- ✓ **Proactive**: Maintaining routing topology.
- ✓ **Reactive**: Resolving routing inconsistencies.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

- ✓ RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).
- ✓ RPL supports message confidentiality and integrity.
- ✓ Supports Data-Path Validation and Loop Detection
- ✓ Routing optimization objectives include
  - minimizing energy
  - minimizing latency
  - satisfying constraints (w.r.t node power, bandwidth, etc.)

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

- ✓ RPL operations require bidirectional links.
- ✓ In some LLN scenarios, those links may exhibit asymmetric properties.
- ✓ It is required that the reachability of a router be verified before the router can be used as a parent.

Source: T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik , JP. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", IETF, Standards Track, Mar. 2012

RFID

Introduction

- ✓ RFID is an acronym for “radio-frequency identification”
- ✓ Data digitally encoded in RFID tags, which can be read by a reader.
- ✓ Somewhat similar to barcodes.
- ✓ Data read from tags are stored in a database by the reader.
- ✓ As compared to traditional barcodes and QR codes, RFID tag data can be read outside the line-of-sight.

Source: “How does RFID work?” AB&R (Online)

RFID Features

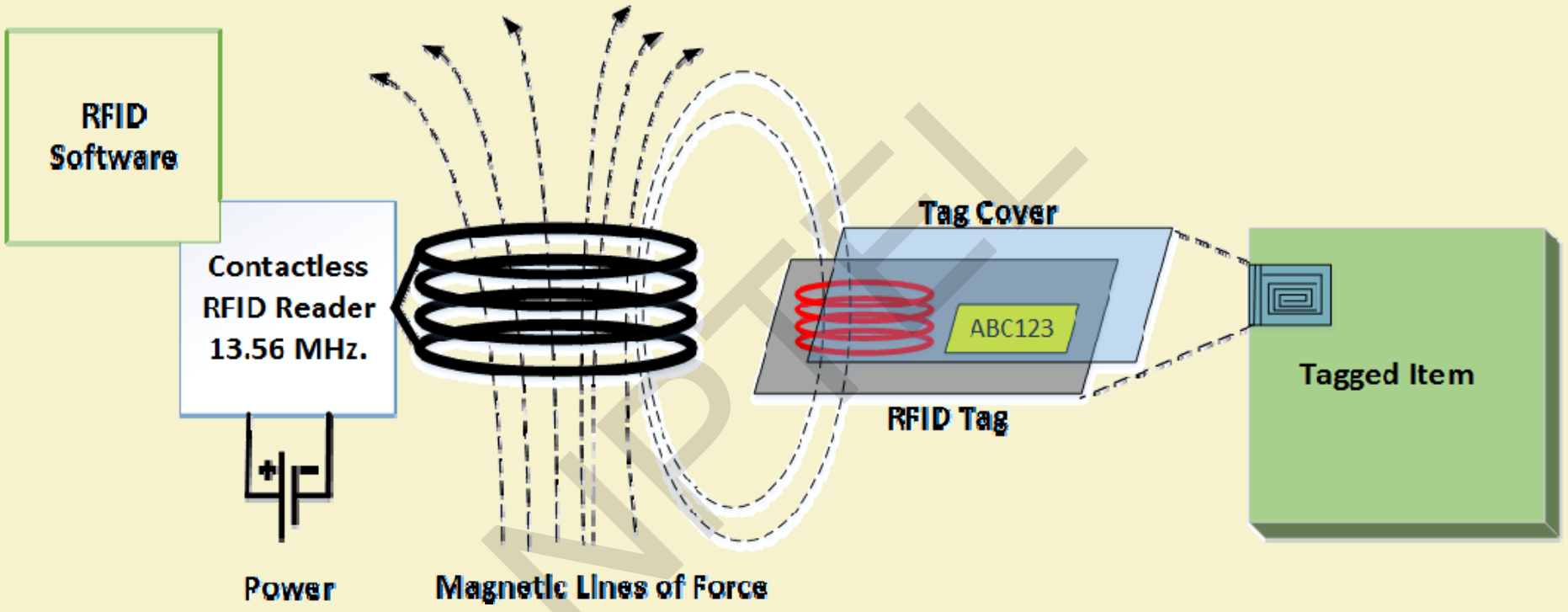
- ✓ RFID tag consists of an integrated circuit and an antenna.
- ✓ The tag is covered by a protective material which also acts as a shield against various environmental effects.
- ✓ Tags may be passive or active.
- ✓ Passive RFID tags are the most widely used.
- ✓ Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply.

Source: "How does RFID work?" AB&R (Online)

Working Principle

- ✓ Derived from Automatic Identification and Data Capture (AIDC) technology.
- ✓ AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.
- ✓ AIDC uses wired communication
- ✓ RFID uses radio waves to perform AIDC functions.
- ✓ The main components of an RFID system include an RFID tag or smart label, an RFID reader, and an antenna.

Source: "How does RFID work?" AB&R (Online)


RFID
Software
Contactless
RFID Reader
13.56 MHz.
Power
Magnetic Lines of Force
Tag Cover
ABC123
RFID Tag
Tagged Item

Applications

- ✓ Inventory management
- ✓ Asset tracking
- ✓ Personnel tracking
- ✓ Controlling access to restricted areas
- ✓ ID badging
- ✓ Supply chain management
- ✓ Counterfeit prevention (e.g. in the pharmaceutical industry)

Source: "How does RFID work?" AB&R (Online)

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Basics of IoT Networking – Part II

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

Functionality-based IoT Protocol Organization

- ✓ **Connectivity** (6LowPAN, RPL)
- ✓ **Identification** (EPC, uCode, IPv6, URIs)
- ✓ **Communication / Transport** (WiFi, Bluetooth, LPWAN)
- ✓ **Discovery** (Physical Web, mDNS, DNS-SD)
- ✓ **Data Protocols** (MQTT, CoAP, AMQP, Websocket, Node)
- ✓ **Device Management** (TR-069, OMA-DM)
- ✓ **Semantic** (JSON-LD, Web Thing Model)
- ✓ **Multi-layer Frameworks** (Alljoyn, IoTivity, Weave, Homekit)

Source: Internet of Things Protocols (Online)

MQTT

Introduction

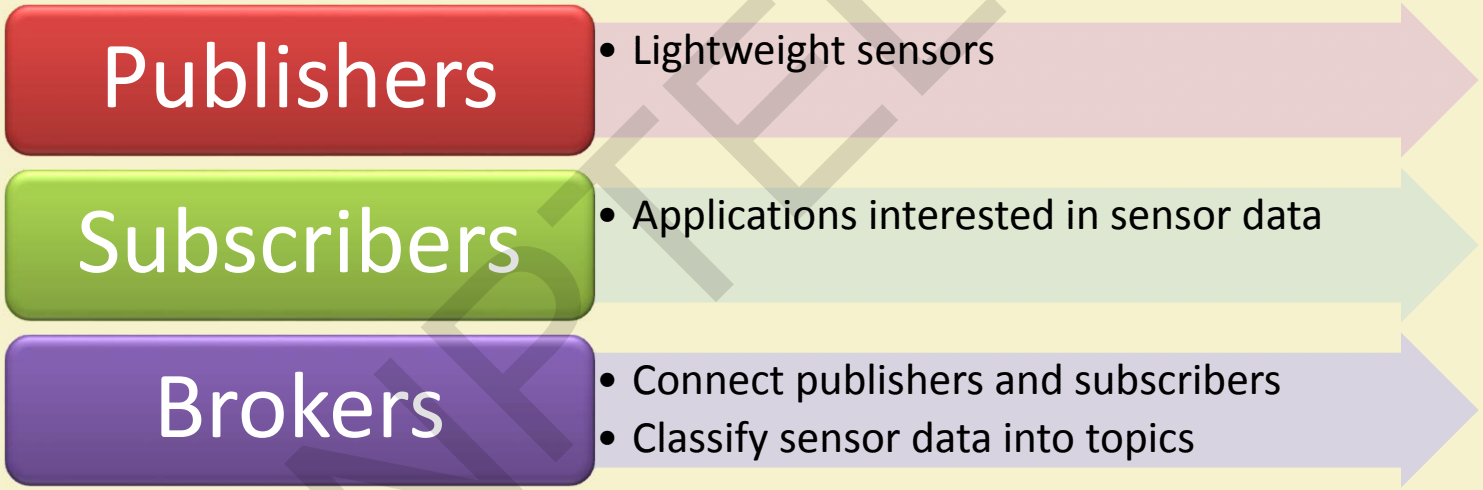
- ✓ **Message Queue Telemetry Transport.**
- ✓ ISO standard (ISO/IEC PRF 20922).
- ✓ It is a publish-subscribe-based lightweight messaging protocol for use in conjunction with the TCP/IP protocol.
- ✓ MQTT was introduced by IBM in 1999 and standardized by OASIS in 2013.
- ✓ Designed to provide connectivity (mostly embedded) between applications and middle-wares on one side and networks and communications on the other side.

Source: "MQTT", Wikipedia (Online)

- ✓ A message broker controls the publish-subscribe messaging pattern.
- ✓ A topic to which a client is subscribed is updated in the form of messages and distributed by the message broker.
- ✓ Designed for:
  - Remote connections
  - Limited bandwidth
  - Small-code footprint

Source: "MQTT", Wikipedia (Online)

MQTT Components

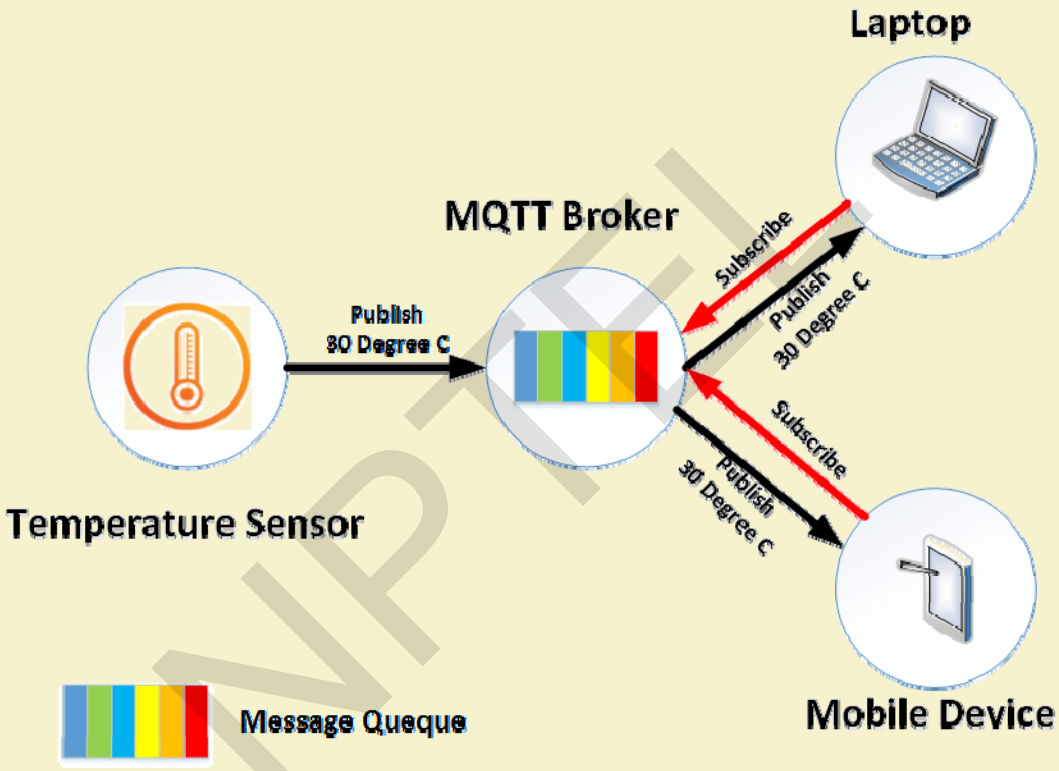


Source: "MQTT", Wikipedia (Online)

MQTT Methods

- Connect
- Disconnect
- Subscribe
- Unsubscribe
- Publish

Source: "MQTT", Wikipedia (Online)



Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

Communication

- ✓ The protocol uses a **publish/subscribe** architecture (HTTP uses a request/response paradigm).
- ✓ Publish/subscribe is **event-driven** and enables messages to be pushed to clients.
- ✓ The central **communication point is the MQTT broker**, which is in charge of dispatching all messages between the senders and the rightful receivers.
- ✓ Each client that publishes a message to the broker, includes a **topic** into the message. The **topic is the routing information for the broker.**

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

- ✓ Each client that wants to receive messages subscribes to a certain topic and the broker delivers all messages with the matching topic to the client.
- ✓ Therefore the clients don't have to know each other. They only communicate over the topic.
- ✓ This architecture enables highly scalable solutions without dependencies between the data producers and the data consumers.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

MQTT Topics

- ✓ A topic is a **simple string** that can have more hierarchy levels, which are separated by a slash.
- ✓ A sample topic for sending temperature data of the living room could be *house/living-room/temperature*.
- ✓ On one hand the client (e.g. mobile device) can subscribe to the exact topic or on the other hand, it can use a **wildcard**.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

- ✓ The subscription to *house/+/temperature* would result in all messages sent to the previously mentioned topic *house/living-room/temperature,* as well as any topic with an arbitrary value in the place of living room, such as *house/kitchen/temperature*.
- ✓ The plus sign is a **single level wild card** and only allows arbitrary values for one hierarchy.
- ✓ If more than one level needs to be subscribed, such as, the entire sub-tree, there is also a **multilevel wildcard** (#).
- ✓ It allows to subscribe to all underlying hierarchy levels.
- ✓ For example *house/#* is subscribing to all topics beginning with *house*.

Source: "MQTT 101 – How to Get Started with the lightweight IoT Protocol", HiveMQ (Online)

Applications

- ✓ **Facebook Messenger** uses MQTT for online chat.
- ✓ **Amazon Web Services** use Amazon IoT with MQTT.
- ✓ **Microsoft Azure** IoT Hub uses MQTT as its main protocol for telemetry messages.
- ✓ The **EVRYTHNG IoT platform** uses MQTT as an M2M protocol for millions of connected products.
- ✓ **Adafruit** launched a free MQTT cloud service for IoT experimenters called Adafruit IO.

SMQTT

- ✓ **Secure MQTT** is an extension of MQTT which uses encryption based on lightweight attribute based encryption.
- ✓ The main advantage of using such encryption is the broadcast encryption feature, in which one message is encrypted and delivered to multiple other nodes, which is quite common in IoT applications.
- ✓ In general, the algorithm consists of four main stages: setup, encryption, publish and decryption.

Source: M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751

- ✓ In the setup phase, the subscribers and publishers register themselves to the broker and get a master secret key according to their developer's choice of key generation algorithm.
- ✓ When the data is published, it is encrypted and published by the broker which sends it to the subscribers, which is finally decrypted at the subscriber end having the same master secret key.
- ✓ The key generation and encryption algorithms are not standardized.
- ✓ SMQTT is proposed only to enhance MQTT security features.

Source: M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in Fifth International Conference on Communication Systems and Network Technologies (CSNT 2015), April 2015, pp. 746-751

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE
CERTIFICATION COURSES

Basics of IoT Networking – Part III

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

CoAP

Introduction

- ✓ CoAP – **Constrained Application Protocol**.
- ✓ **Web transfer protocol** for use with constrained nodes and networks.
- ✓ **Designed for Machine to Machine** (M2M) applications such as smart energy and building automation.
- ✓ Based on **Request-Response model** between end-points
- ✓ Client-Server interaction is **asynchronous over a datagram oriented transport protocol** such as UDP

Source: Z. Shelby , K. Hartke, C. Bormann**, "The Constrained Application Protocol (CoAP)",** Internet Engineering Task Force (IETF), Standards Track, 2014

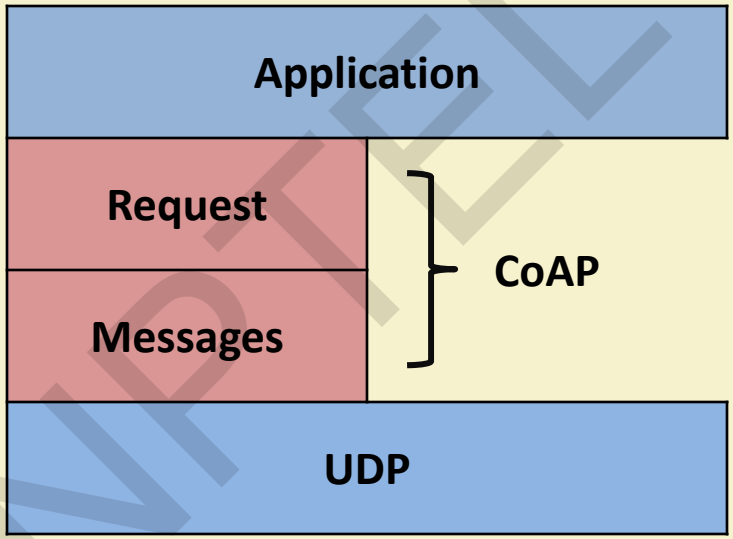
- ✓ The Constrained Application Protocol (CoAP) is a session layer protocol designed by IETF Constrained RESTful Environment (CoRE) working group to provide lightweight RESTful (HTTP) interface.
- ✓ Representational State Transfer (REST) is the standard interface between HTTP client and servers.
- ✓ Lightweight applications such as those in IoT, could result in significant overhead and power consumption by REST.
- ✓ CoAP is designed to enable low-power sensors to use RESTful services while meeting their power constraints.

Source: Z. Shelby , K. Hartke, C. Bormann**, "The Constrained Application Protocol (CoAP)",** Internet Engineering Task Force (IETF), Standards Track, 2014

- ✓ Built over UDP, instead of TCP (which is commonly used with HTTP) and has a light mechanism to provide reliability.
- ✓ CoAP architecture is divided into two main sub-layers:
  - Messaging
  - Request/response.
- ✓ The messaging sub-layer is responsible for reliability and duplication of messages, while the request/response sub-layer is responsible for communication.
- ✓ CoAP has four messaging modes:
  - Confirmable
  - Non-confirmable
  - Piggyback
  - Separate

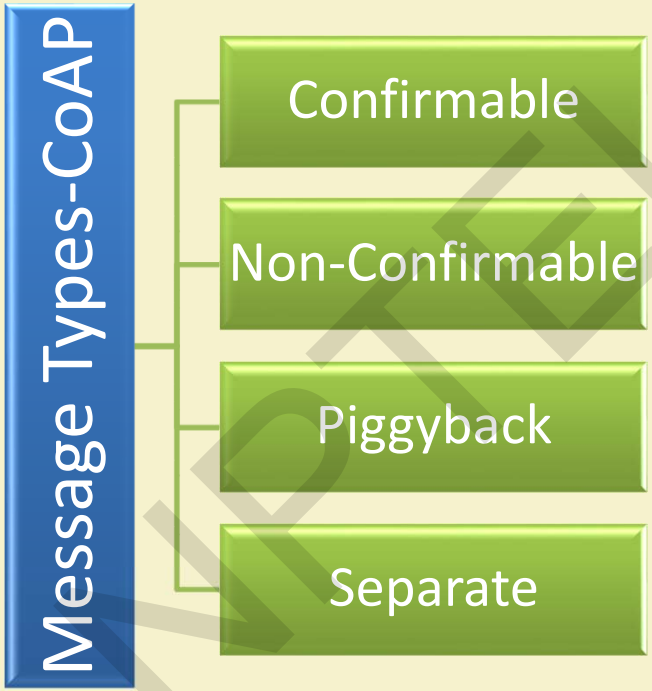
Source: V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

CoAP Position



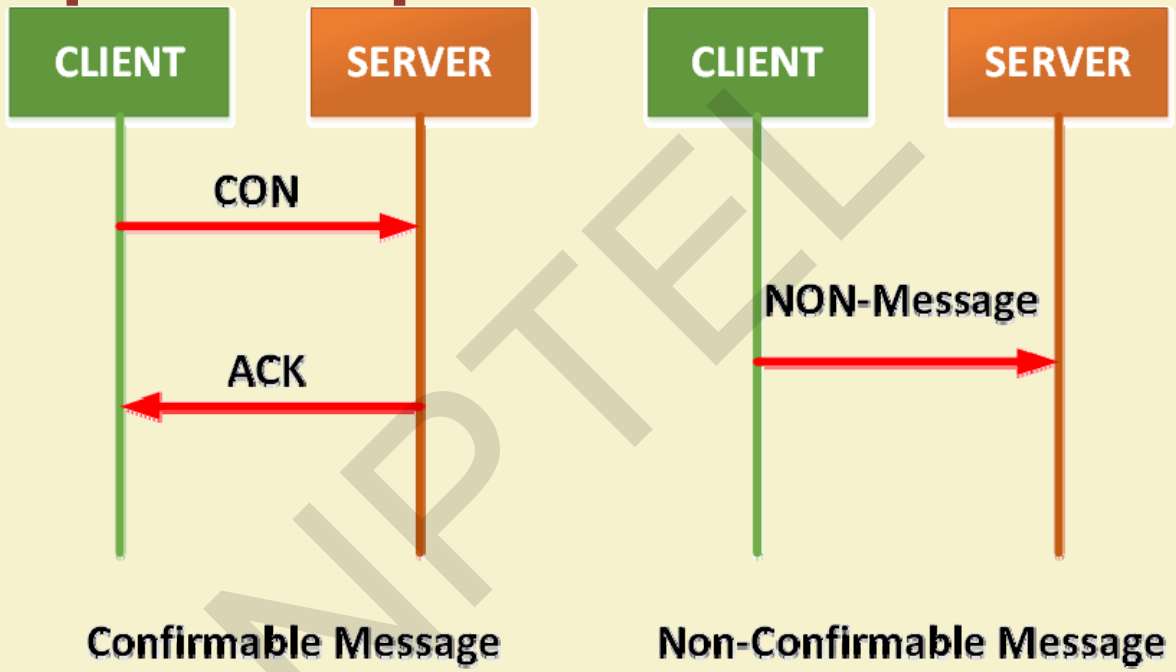
Source: Z. Shelby , K. Hartke, C. Bormann**, "The Constrained Application Protocol (CoAP)",** Internet Engineering Task Force (IETF), Standards Track, 2014

CoAP Message Types



Source: Z. Shelby , K. Hartke, C. Bormann**, "The Constrained Application Protocol (CoAP)",** Internet Engineering Task Force (IETF), Standards Track, 2014

CoAP Request-Response Model

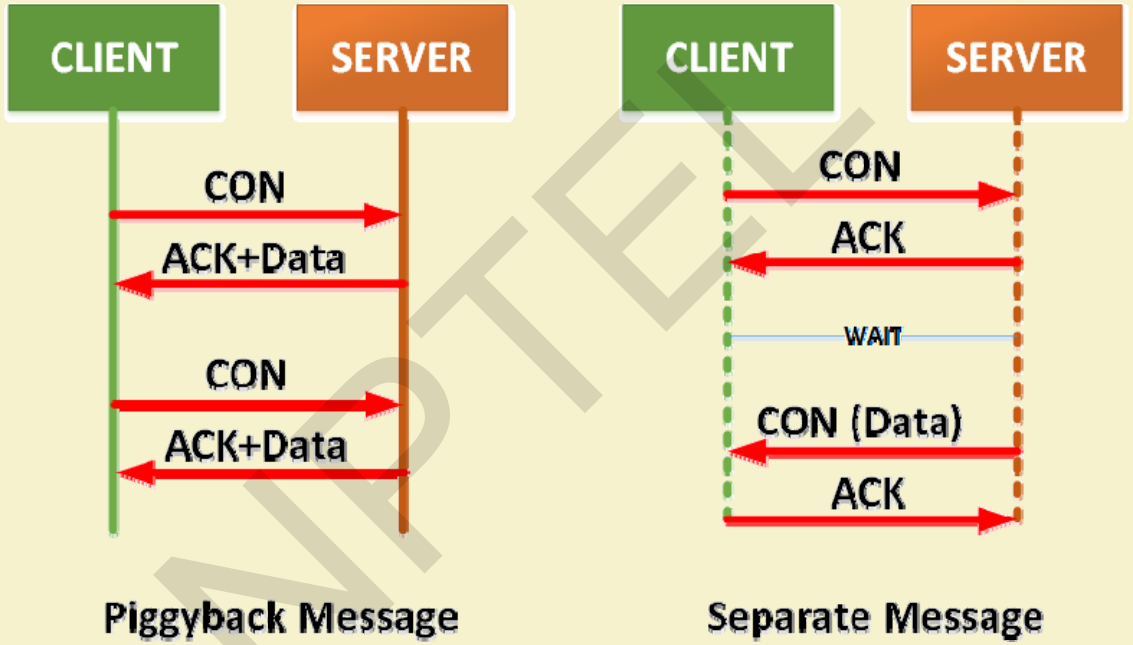


Source: V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

- ✓ Confirmable and non-confirmable modes represent the reliable and unreliable transmissions, respectively, while the other modes are used for request/response.
- ✓ Piggyback is used for client/server direct communication where the server sends its response directly after receiving the message, i.e., within the acknowledgment message.
- ✓ On the other hand, the separate mode is used when the server response comes in a message separate from the acknowledgment, and may take some time to be sent by the server.
- ✓ Similar to HTTP, CoAP utilizes GET, PUT, PUSH, DELETE messages requests to retrieve, create, update, and delete, respectively

Source: V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

CoAP Request-Response Model



Source: V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17, 2015

Features

- ✓ Reduced overheads and parsing complexity.
- ✓ URL and content-type support.
- ✓ Support for the discovery of resources provided by known CoAP services.
- ✓ Simple subscription for a resource, and resulting push notifications.
- ✓ Simple caching based on maximum message age.

Source: ”Constrained Application Protocol”, Wikipedia (Online)

XMPP

Introduction

- ✓ **XMPP – Extensible Messaging and Presence Protocol.**
- ✓ A communication protocol for **message-oriented middleware** based on XML (Extensible Markup Language).
- ✓ Real-time exchange of structured data.
- ✓ It is an open standard protocol.

Source: "XMPP", Wikipedia (Online)

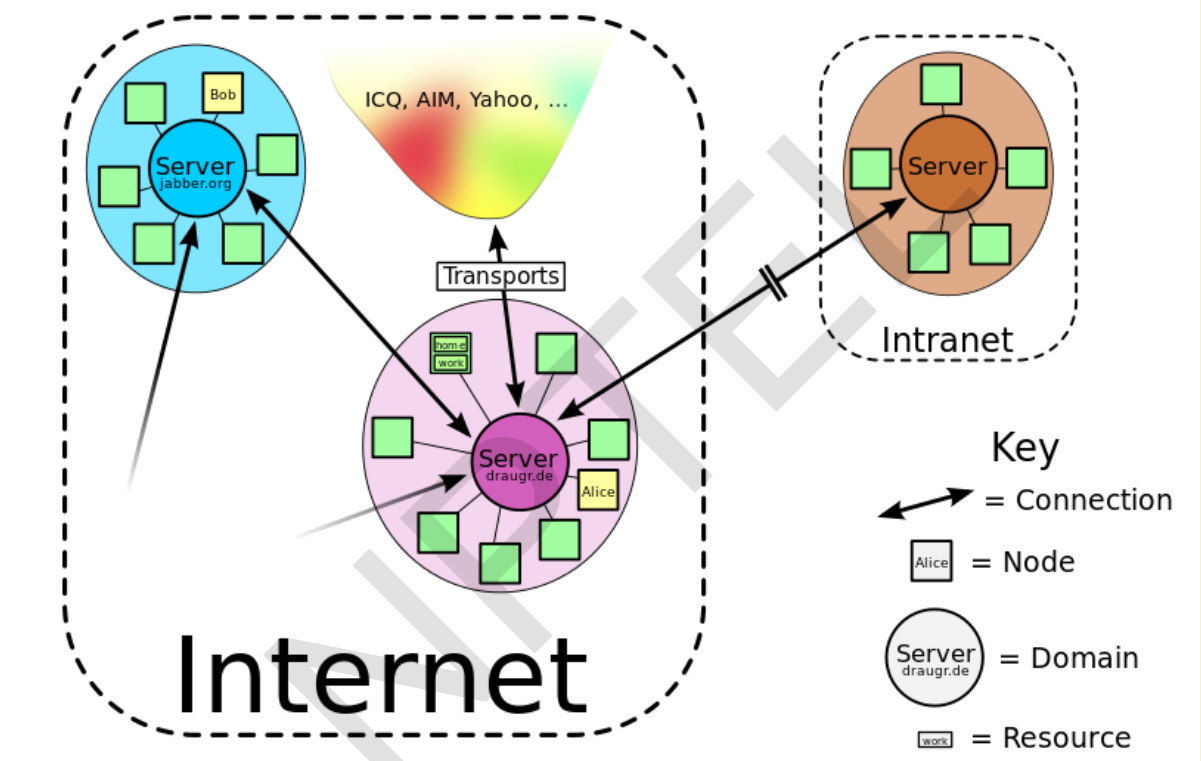
- ✓ XMPP uses a **client-server architecture**.
- ✓ As the model is **decentralized**, no central server is required.
- ✓ XMPP provides for the **discovery of services** residing locally or across a network, and the **availability information** of these services.
- ✓ Well-suited for cloud computing where virtual machines, networks, and firewalls would otherwise present obstacles to alternative service discovery and presence-based solutions.
- ✓ Open means to support machine-to-machine or peer-to-peer communications across a diverse set of networks.

Source: "XMPP", Wikipedia (Online)

Highlights

- ✓ Decentralization – No central server; anyone can run their own XMPP server.
- ✓ Open standards – No royalties or granted permissions are required to implement these specifications
- ✓ Security – Authentication, encryption, etc.
- ✓ Flexibility – Supports interoperability

Source: "XMPP", Wikipedia (Online)



Source: "JabberNetwork.svg", Wikimedia Commons (Online)

Core XMPP Technologies

Core
- information about the core XMPP technologies for XML streaming

Jingle
- multimedia signalling for voice, video, file transfer

Multi-user Chat
- flexible, multi-party communication

PubSub
- alerts and notifications for data syndication

BOSH
- HTTP binding for XMPP

Source: "XMPP: Technology Overview", XMPP.org (Online)

Weaknesses

- ✓ Does not support QoS.
- ✓ Text based communications induces higher network overheads.
- ✓ Binary data must be first encoded to base64 before transmission.

Applications

- ✓ Publish-subscribe systems
- ✓ Signaling for VoIP
- ✓ Video
- ✓ File transfer
- ✓ Gaming
- ✓ Internet of Things applications
  - Smart grid
  - Social networking services

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Basics of IoT Networking – Part IV

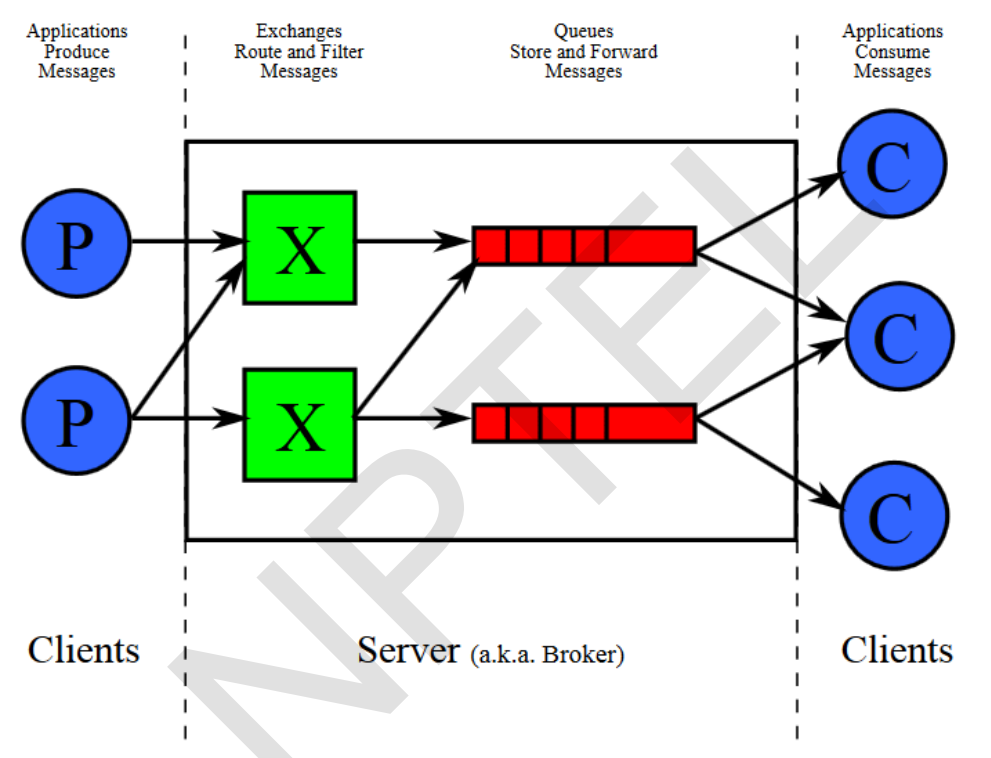
Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

AMQP

Introduction

- ✓ **Advanced Message Queuing Protocol.**
- ✓ **Open standard for passing business messages** between applications or organizations.
- ✓ Connects between systems and business processes.
- ✓ It is a binary application layer protocol.
- ✓ Basic unit of data is a *frame*.
- ✓ ISO standard: **ISO/IEC 19464**

Source: "Advanced Message Queuing Protocol", Wikipedia (Online)



Source: "The-amqp-model-for-wikipedia.svg", Wikimedia Commons (Online)

AMQP Features

Connects across

Features

- Security
- Reliability
- Interoperability
- Routing
- Queuing
- Open standard

Message Delivery Guarantees

- ✓ *At-most-once*
  - each message is delivered once or never
- ✓ *At-least-once*
  - each message is certain to be delivered, but may do so multiple times
- ✓ *Exactly-once*
  - message will always certainly arrive and do so only once

Reference: "OASIS AMQP version 1.0, sections 2.6.12-2.6.13". OASIS AMQP Technical Committee

AMQP Frame Types

- ✓ Nine AMQP frame types are defined that are used to initiate, control and tear down the transfer of messages between two peers:
  - Open (connection open)
  - Begin (session open)
  - Attach (initiate new link)
  - Transfer (for sending actual messages)
  - Flow (controls message flow rate)
  - Disposition (Informs the changes in state of transfer)
  - Detach (terminate the link)
  - End (session close)
  - Close (connection close)

Source: O.S. Tezer, "An advanced messaging queuing protocol walkthrough ", DigitalOcean (Online), 2013

Components

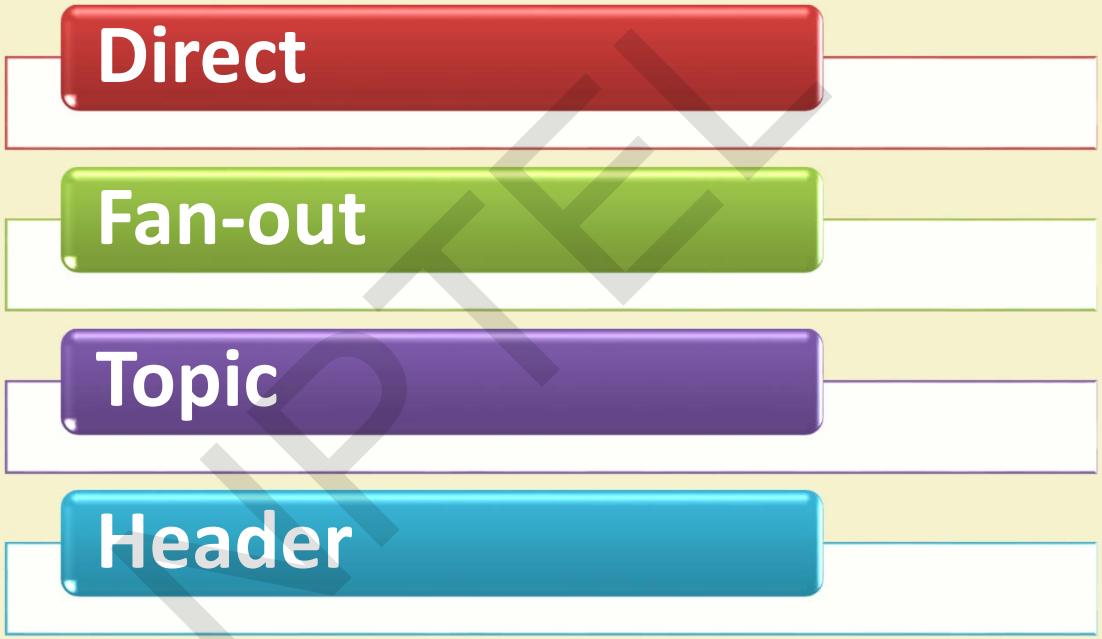
Exchange
- Part of Broker
- Receives messages and routes them to Queues

Queue
- Separate queues for separate business processes
- Consumers receive messages from queues

Bindings
- Rules for distributing messages (who can access what message, destination of the message)

Source: O.S. Tezer, "An advanced messaging queuing protocol walkthrough ", DigitalOcean (Online), 2013

AMQP Exchanges



Source: O.S. Tezer, "An advanced messaging queuing protocol walkthrough ", DigitalOcean (Online), 2013

AMQP Features

- ✓ Targeted QoS (Selectively offering QoS to links)
- ✓ Persistence (Message delivery guarantees)
- ✓ Delivery of messages to multiple consumers
- ✓ Possibility of ensuring multiple consumption
- ✓ Possibility of preventing multiple consumption
- ✓ High speed protocol

Source: O.S. Tezer, "An advanced messaging queuing protocol walkthrough ", DigitalOcean (Online), 2013

Applications

- ✓ Monitoring and global update sharing.
- ✓ Connecting different systems and processes to talk to each other.
- ✓ Allowing servers to respond to immediate requests quickly and delegate time consuming tasks for later processing.
- ✓ Distributing a message to multiple recipients for consumption.
- ✓ Enabling offline clients to fetch data at a later time.
- ✓ Introducing fully asynchronous functionality for systems.
- ✓ Increasing reliability and uptime of application deployments.

Source: O.S. Tezer, "An advanced messaging queuing protocol walkthrough ", DigitalOcean (Online), 2013

Thank You!!

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Connectivity Technologies – Part I

Dr. Sudip Misra
Associate Professor
Department of Computer Science and Engineering
IIT KHARAGPUR
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/

Communication Protocols

The following communication protocols have immediate importance to consumer and industrial IoTs:

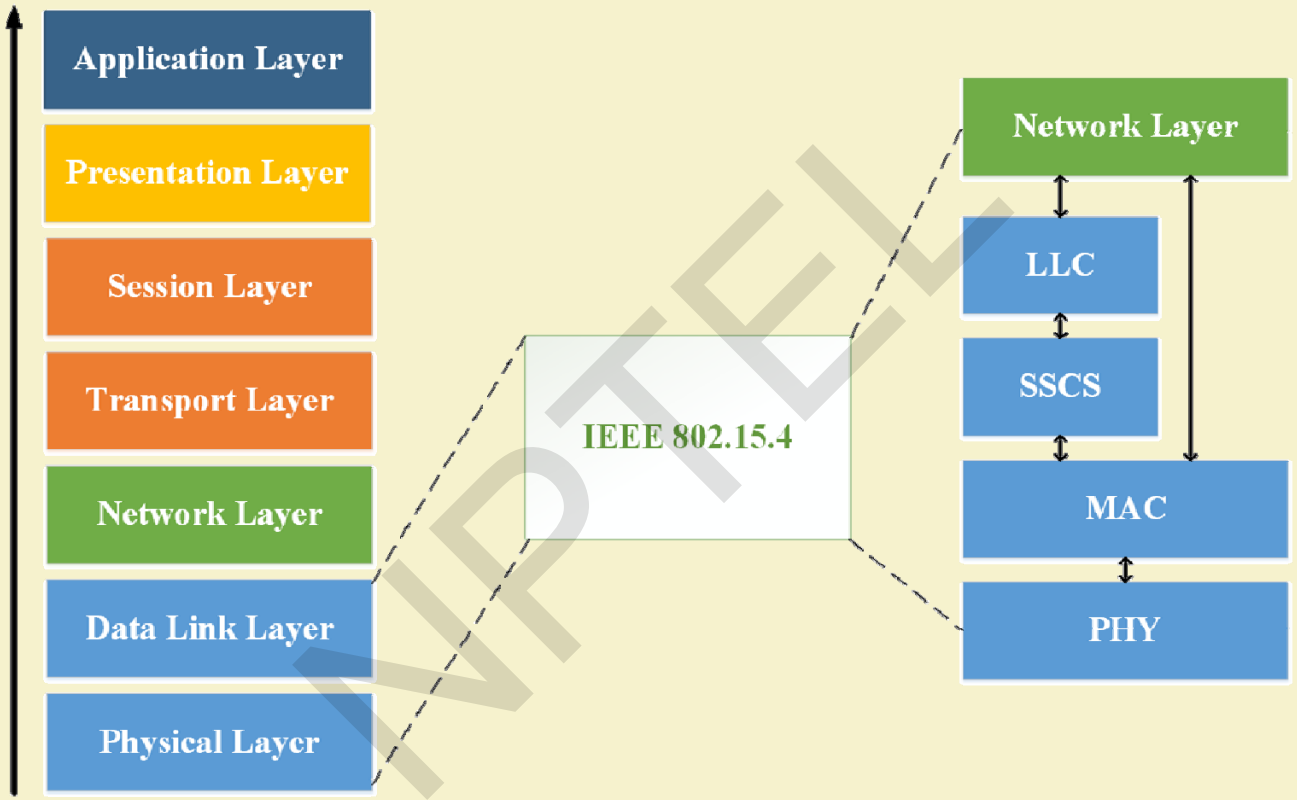
- ✓ IEEE 802.15.4
- ✓ Zigbee
- ✓ 6LoWPAN
- ✓ Wireless HART
- ✓ Z-Wave
- ✓ ISA 100
- ✓ Bluetooth
- ✓ NFC
- ✓ RFID

IEEE 802.15.4

Features of IEEE 802.15.4

- ✓ Well-known standard for low data-rate WPAN.
- ✓ Developed for low-data-rate monitoring and control applications and extended-life low-power-consumption uses.
- ✓ This standard uses only the first two layers (PHY, MAC) plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers
- ✓ Operates in the ISM band.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
IEEE 802.15.4
Network Layer
LLC
SSCS
MAC
PHY

- ✓ Uses direct sequence spread spectrum (DSSS) modulation.
- ✓ Highly tolerant of noise and interference and offers link reliability improvement mechanisms.
- ✓ Low-speed versions use Binary Phase Shift Keying (BPSK).
- ✓ High data-rate versions use offset-quadrature phase-shift keying (O-QPSK).
- ✓ Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access.
- ✓ Multiplexing allows multiple users or nodes interference-free access to the same channel at different times.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

- ✓ Power consumption is minimized due to infrequently occurring very short packet transmissions with low duty cycle (<1%).
- ✓ The minimum power level defined is –3 dBm or 0.5 mW.
- ✓ Transmission, for most cases, is Line of Sight (LOS).
- ✓ Standard transmission range varies between 10m to 75m.
- ✓ Best case transmission range achieved outdoors can be upto 1000m.
- ✓ Networking topologies defined are -- Star, and Mesh.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

IEEE 802.15.4 Variants

A/B
- Base version

C
- For China

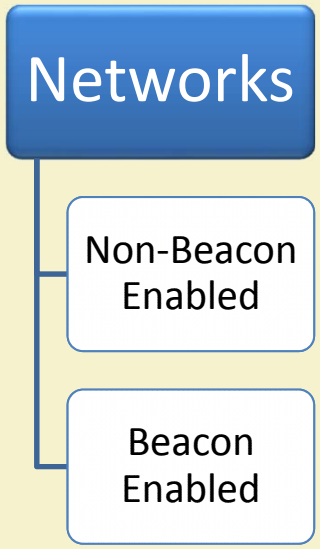
D
- For Japan

E
- Industrial applications

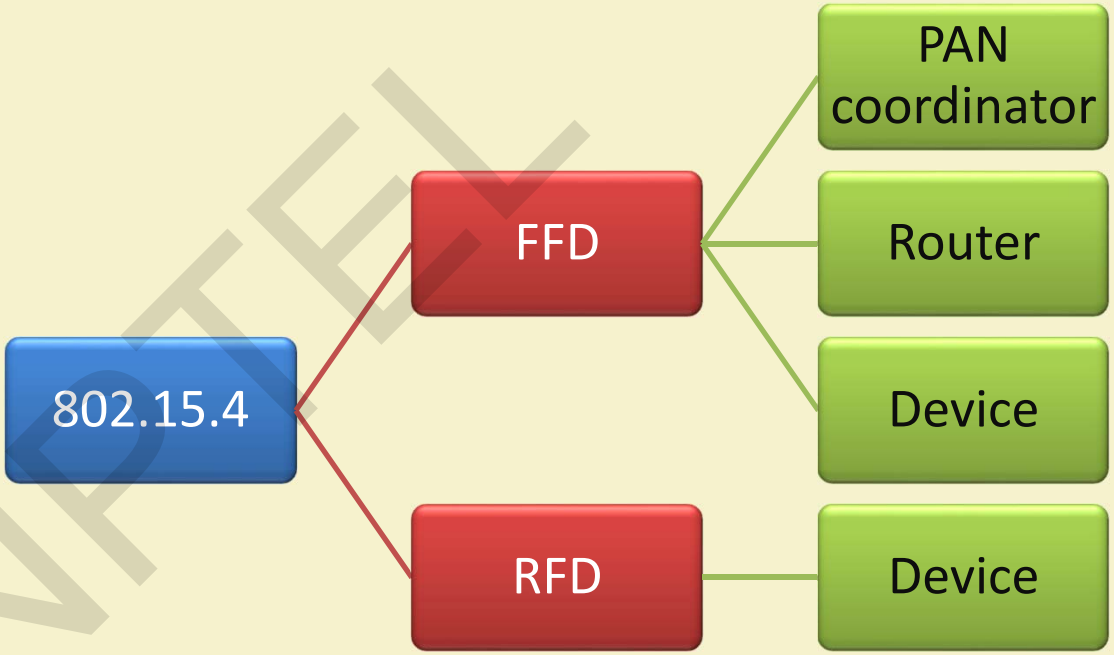
F
- Active RFID uses

G
- Smart utility networks (Smart Grids)

IEEE 802.15.4 Types



(a)

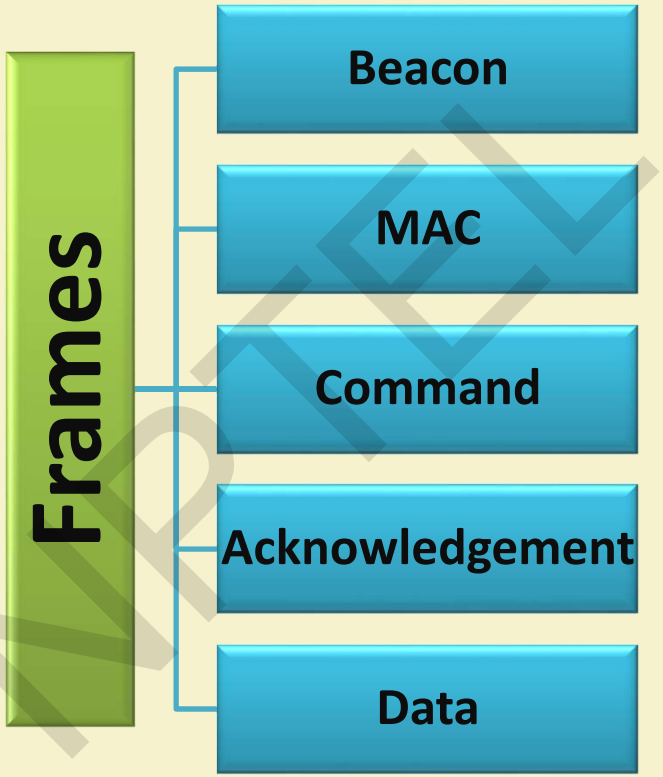


(b)

- **Full Function Device (FFD)**
  - Can talk to all types of devices
  - Supports full protocol

- **Reduced Function Device (RFD)**
  - Can only talk to an FFD
  - Lower power consumption
  - Minimal CPU/RAM required

IEEE 802.15.4 Frames



Beacon Enabled Networks

- Periodic transmission of beacon messages
- Data-frames sent via Slotted CSMA/CA with a super frame structure managed by PAN coordinator
- Beacons used for synchronization & association of other nodes with the coordinator
- Scope of operation spans the whole network.

Non-Beacon Enabled Networks

- Data-frames sent via un-slotted CSMA/CA (Contention Based)
- Beacons used only for link layer discovery
- Requires both source and destination IDs.
- As 802.15.4 is primarily, a mesh protocol, all protocol addressing must adhere to mesh configurations
- De-centralized communication amongst nodes

Zigbee

Features of ZigBee

- ✓ Most widely deployed enhancement of IEEE 802.15.4.
- ✓ The ZigBee protocol is defined by **layer 3 and above**. It works with the 802.15.4 layers 1 and 2.
- ✓ The standard uses layers 3 and 4 to define additional communication enhancements.
- ✓ These enhancements include authentication with valid nodes, encryption for security, and a data routing and forwarding capability that enables mesh networking.
- ✓ The most popular use of ZigBee is wireless sensor networks using the mesh topology.

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Zigbee
IEEE 802.15.4

Important Components

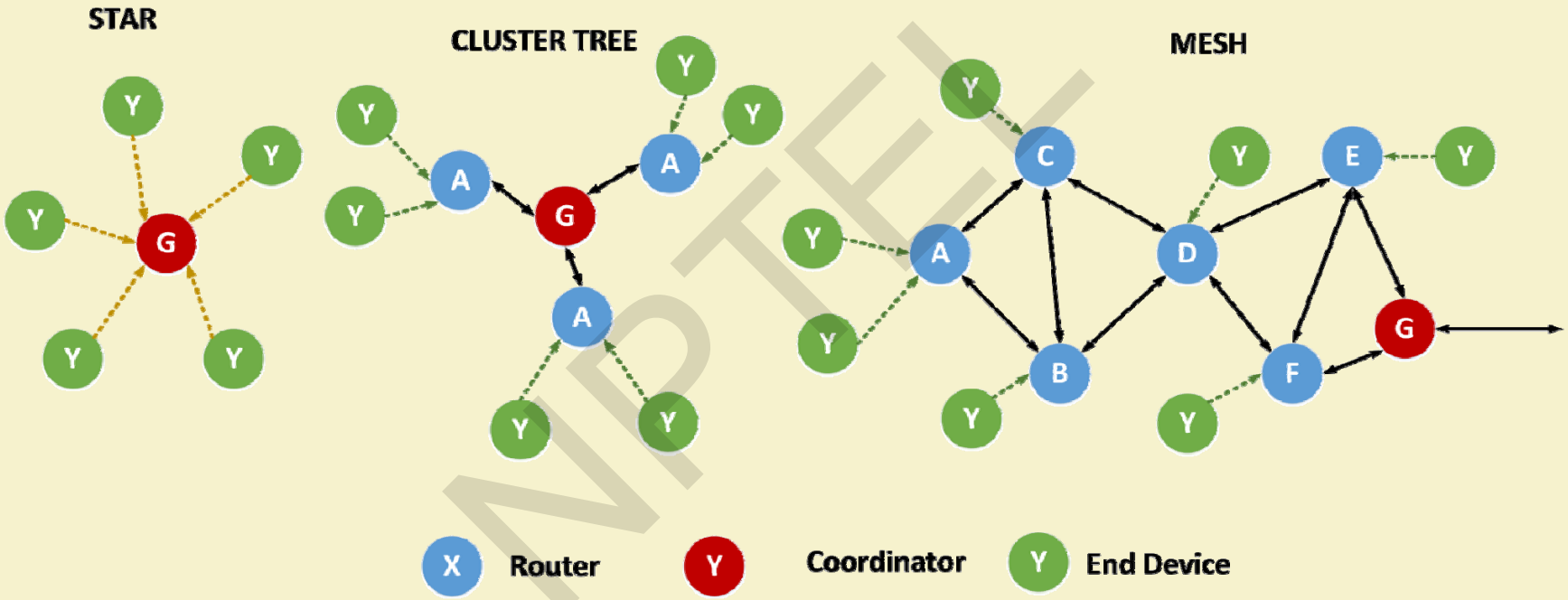
ZDO

- ZigBee Device Object
  (Device management, Security, Policies)

APS

- Application Support Sub-layer
  (Interfacing and control services, bridge between network and other layers)

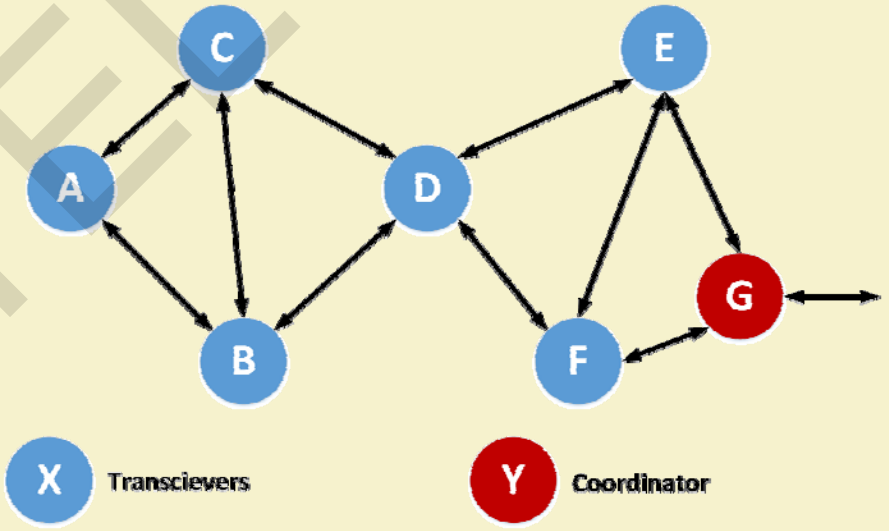
ZigBee Topologies



Source: T. Agarwal, "ZigBee Wireless Technology Architecture and Applications", Electronics Projects Focus (Online)

ZigBee Mesh

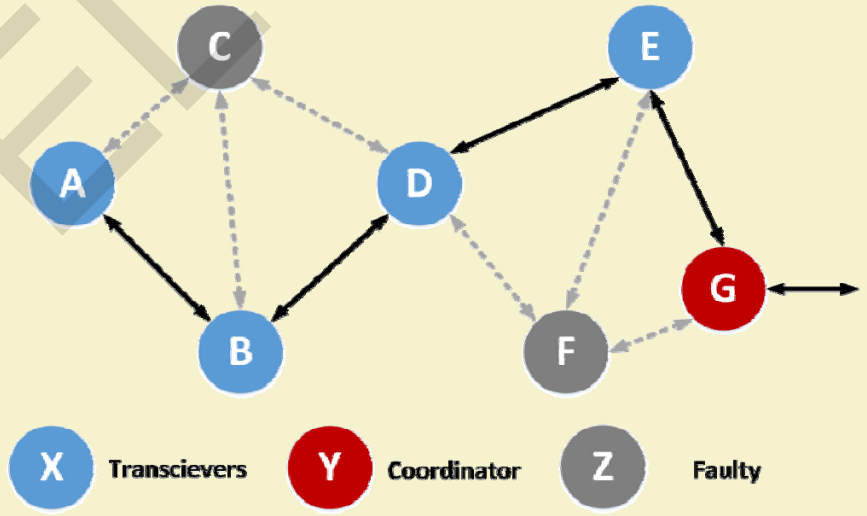
- ✓ In a mesh, any node can communicate with any other node within its range.
- ✓ If nodes are not in range, messages are relayed through intermediate nodes.
- ✓ This allows the network deployment over large areas.



Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

ZigBee Mesh (Contd.)

- ✓ Meshes have increased network reliability.
- ✓ For example, if nodes C and F are down, the message packets from A can still be relayed to G via B and E.
- ✓ ZigBee mesh networks are self-configuring and self-healing.



Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

ZigBee Types

- ✓ *ZigBee Coordinator (ZC)*:
  - The Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.
  - There is a single ZigBee Coordinator in each network, which originally initiates the network.
  - It stores information about the network under it and outside it.
  - It acts as a Trust Center & repository for security keys.

Sources:

- *"Wireless Sensor Networks Research Group". Sensor-networks.org. 2010-04-15.*
- *"Wireless Sensor Networks Research Group". Sensor-networks.org. 2009-02-05.*

ZigBee Types

- ✓ *ZigBee Router (ZR)*:
  - Capable of running applications, as well as relaying information between nodes connected to it.
- ✓ *ZigBee End Device (ZED)*:
  - It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.
  - This allows the node to be asleep a significant amount of the time thereby enhancing battery life.
  - Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.

Sources:

- *"Wireless Sensor Networks Research Group". Sensor-networks.org. 2010-04-15.*
- *"Wireless Sensor Networks Research Group". Sensor-networks.org. 2009-02-05.*

ZigBee Network Layer

- ✓ The network layer uses Ad Hoc On-Demand Distance Vector (AODV) routing.
- ✓ To find the final destination, the AODV broadcasts a route request to all its immediate neighbors.
- ✓ The neighbors relay the same information to their neighbors, eventually spreading the request throughout the network.
- ✓ Upon discovery of the destination, a low-cost path is calculated and informed to the requesting device via unicast messaging.

Source: "Zigbee", Wikipedia (Online)

Applications

- ✓ Building automation
- ✓ Remote control (RF4CE or RF for consumer electronics)
- ✓ Smart energy for home energy monitoring
- ✓ Health care for medical and fitness monitoring
- ✓ Home automation for control of smart homes
- ✓ Light Link for control of LED lighting
- ✓ Telecom services

Source: L.Fenzel, "What's The Difference Between IEEE 802.15.4 And ZigBee Wireless?", Electronic Design (Online), Mar. 2013

Thank You!!