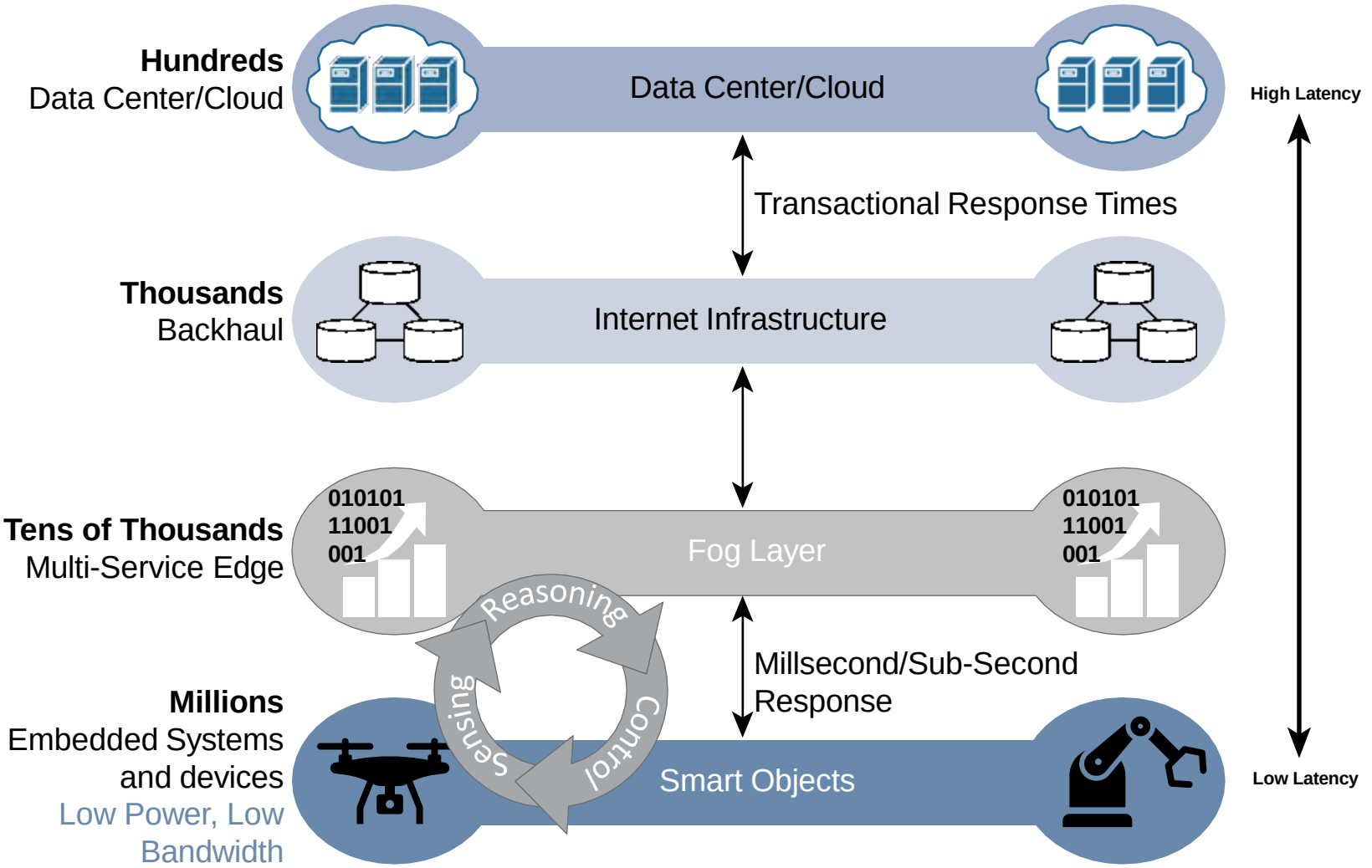
IoT Architecture

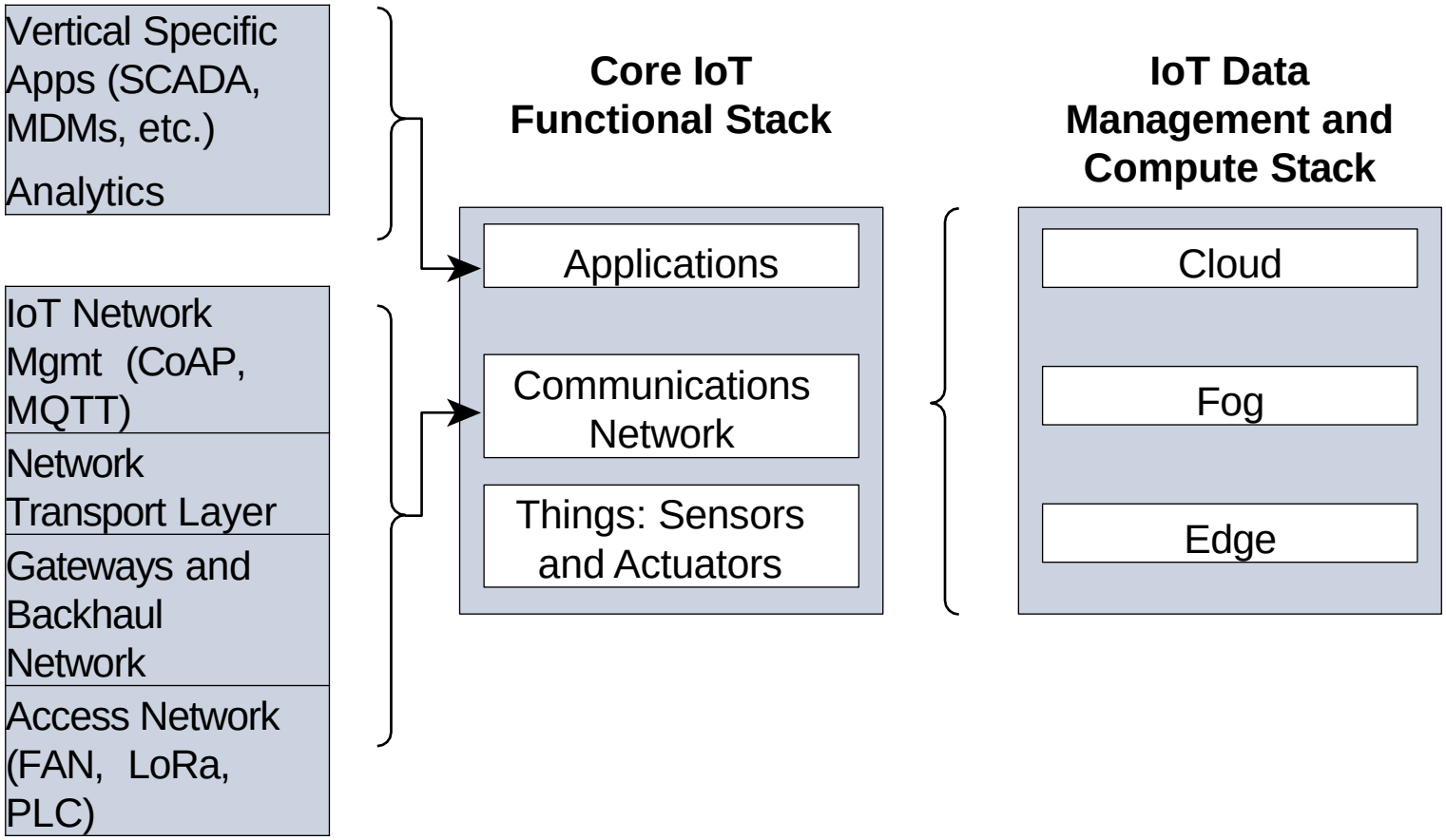
ΕΠΛ 428: IOT PROGRAMMING

Dr. Panayiotis Kolios
Assistant Professor, Dept. Computer Science,
KIOS CoE for Intelligent Systems and Networks
Office: FST 01, 116
Telephone: +357 22893450 / 22892695
Web: https://www.kios.ucy.ac.cy/pkolios/

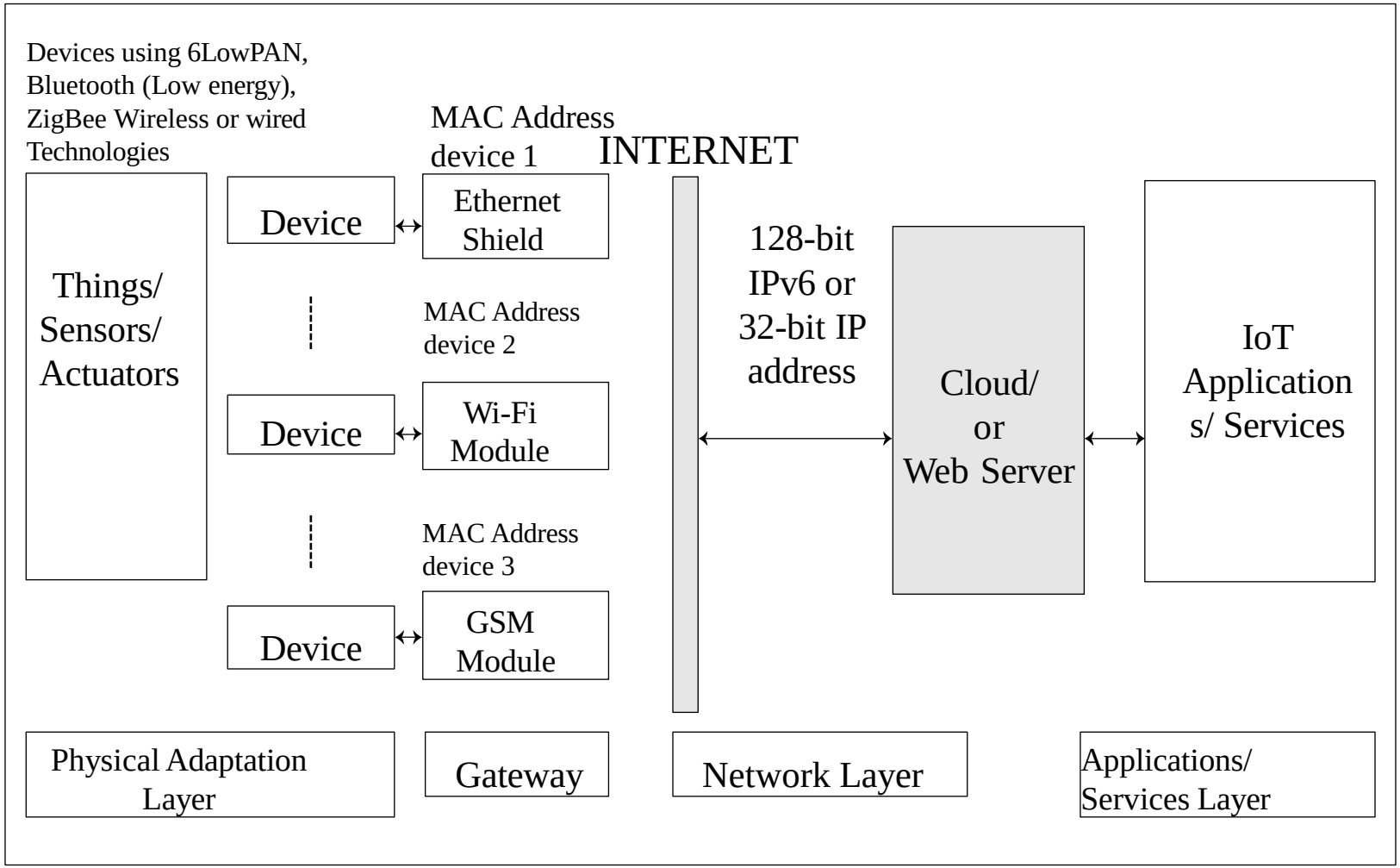
Πανεπιστήμιο Κύπρου

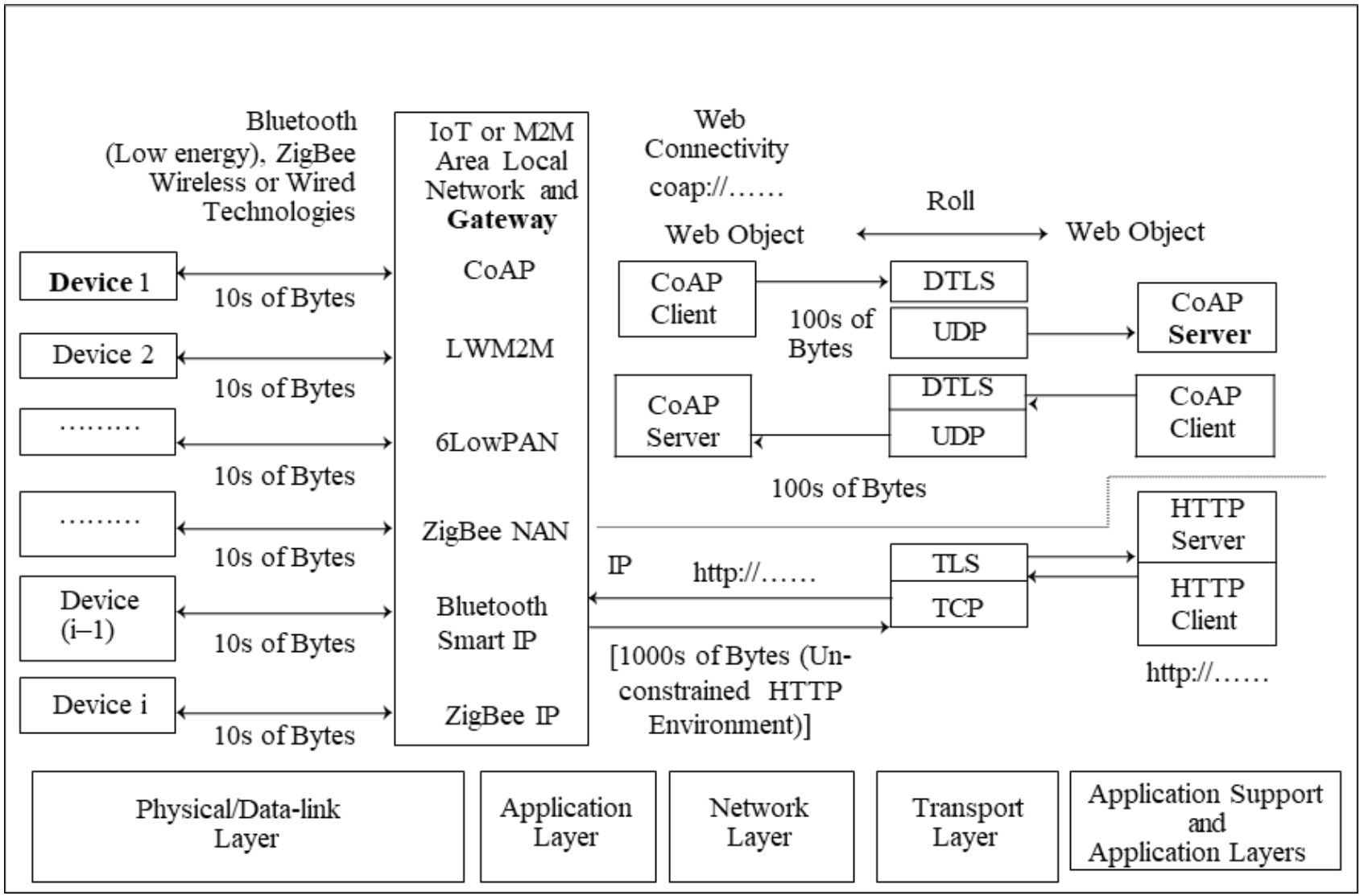


Πανεπιστήμιο Κύπρου



Πανεπιστήμιο Κύπρου


Devices using 6LowPAN, Bluetooth (Low energy), ZigBee Wireless or wired Technologies
Things/ Sensors/ Actuators
Device
Device
Device
MAC Address device 1
MAC Address device 2
MAC Address device 3
Ethernet Shield
Wi-Fi Module
GSM Module
INTERNET
128-bit IPv6 or 32-bit IP address
Cloud/ or Web Server
IoT Application s/ Services
Physical Adaptation Layer
Gateway
Network Layer
Applications/ Services Layer

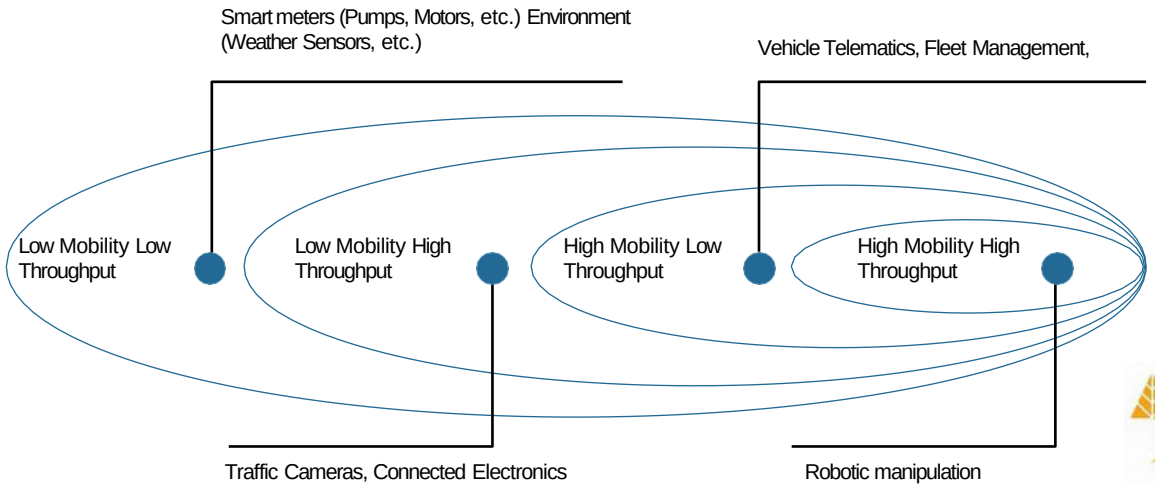


Πανεπιστήμιο Κύπρου

- Device consisting of hardware e.g. microcontroller (or SoC), sensors, actuators, and software for data processing and exchange
  - Sensors are electronic devices to quantify the environment (e.g. temperature, humidity, acceleration)
  - Devices consist of microcontroller units (MCUs) with processing, memory, and other hardware (ADC, PWM) interfaced together
- Gateways, edge/ fog devices middleware and services
- Server hardware and web software enabling web applications and web services (including storage, data analytics, predictive analytics)
- Connectivity and networking enabling internetworking

- **Battery-powered or power-connected**:
  - This classification is based on whether the object carries its own energy supply or receives continuous power from an external power source.
  - Battery-powered things can be moved more easily than line-powered objects.
  - However, batteries limit the lifetime and amount of energy that the object is allowed to consume, thus driving transmission range and frequency
- **Mobile or static**:
  - A sensor may be moving in a fluid or because it is attached to a moving object (for example, a location sensor on moving goods in a warehouse or factory floor).
  - The frequency of the movement may also vary, from occasional to permanent. The range of mobility (from a few inches to miles away) often drives the possible power source.

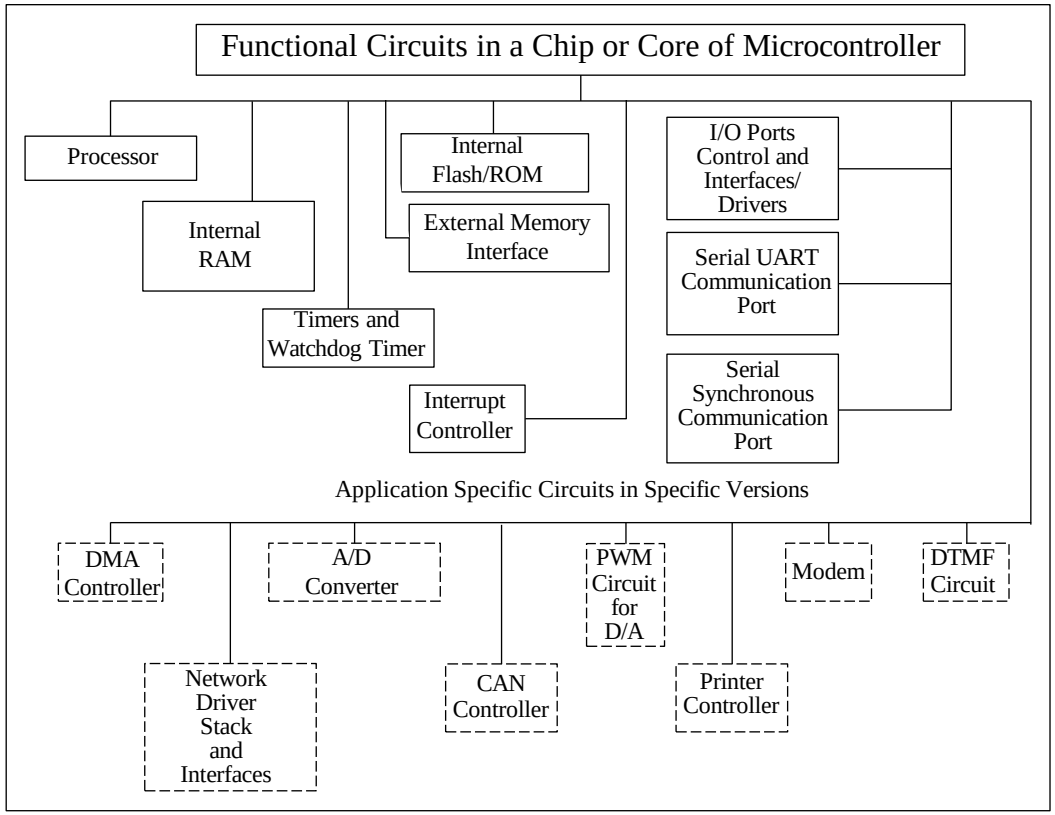
- **Low or high reporting frequency**:
  - A motion sensor may report acceleration several hundred times per second. Higher frequencies drive higher energy consumption, which may create constraints on the possible power source (and therefore the object mobility) and the transmission range.
- **Simple or rich data**:
  - Based on the quantity of data exchanged at each report cycle.
  - A humidity sensor in a field may report a simple daily index value (on a binary scale from 0 to 255), while an engine sensor may report hundreds of parameters,
  - Richer data typically drives higher power consumption.



Πανεπιστήμιο Κύπρου

- Hardware (Arduino, Raspberry Pi, etc)
- Integrated Development Environment (IDE) for software development, firmware and APIs
- Messaging Protocols (CoAP, MQTT, RESTful HTTP, XMPP (Extensible Messaging and Presence Protocol)
- Communication Technologies (Powerline Ethernet, RFID, NFC, ZigBee, Bluetooth, WiFi, 5G)
- Cloud Platforms/Data Centres (AWS IoT, CISCO IoT, Azure)

- Devices (embedded devices, sensors and systems) generate data
- Data needs computations and a system needs electronic circuits for computation and communication
- Embedded systems employ dedicated software into a computing platform to perform the computations and communication
- Microcontroller unit (MCU) is a single-chip unit with limited computational capabilities
    - MCU possesses memory, input-output capabilities and a number of on-chip functional units
    - e.g. Timer is one such unit which enables initiating new action(s) on timer start, on the clock inputs, timeouts or when the number of clock inputs equal to a preset value



- MCU is an Integrated Circuit with 8-bit, 16-bit, 32-bit etc architecture
- Clock frequencies can be 8 MHz, 16 MHz, 100 MHz, 200 MHz or higher
- A metric for performance is Million Instructions Per Second (MIPS)
- Or is Million Floating Point Operations Per Second (MFLOPS)

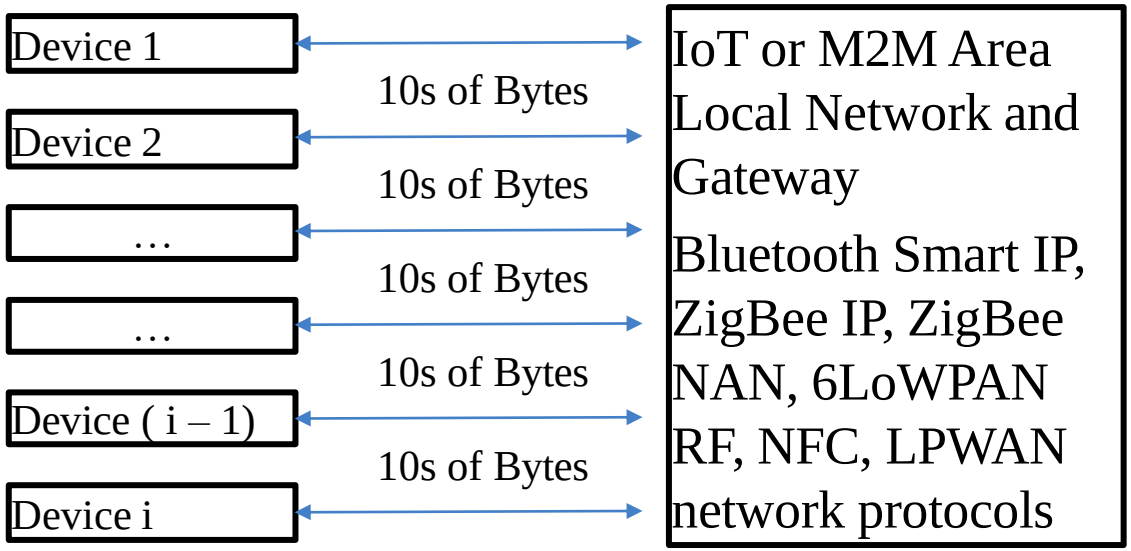
Πανεπιστήμιο Κύπρου

- Arduino boards, modules and shields are popular MCU
- Open source IDEs
- Analog input pins and PWM pins can connect sensors, actuators
- Digital I/O pins can connect On-Off states, set of On-Off states, digital inputs from sensors, digital outputs to actuators and other digital circuits
- Shield inserted for wireless connection to a ZigBee, Bluetooth LE, WiFi, GSM, or RF module or a wired connection to Ethernet LAN
- A programmer develops the codes using an IDE, the codes are pushed into the MCU using USB port of the board. The codes are pushed after developing-testing-debugging cycle(s)

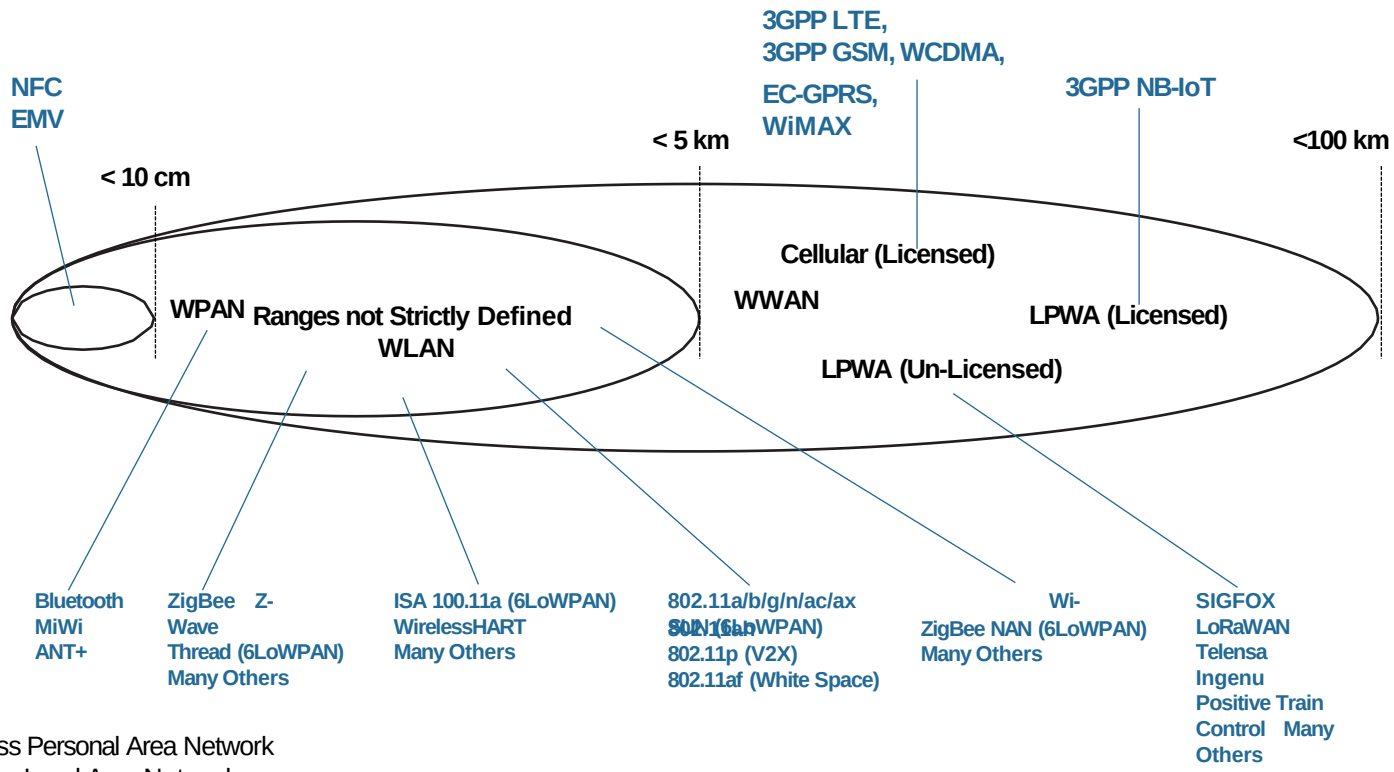
- Raspberry Pi single board SoC based computing and communication board
- RPi runs on the OSes (distributions of Linux such as Raspbian Ubuntu)
- RPi includes an OS - Ubuntu Core (also known as Snappy) - a stripped down version of Ubuntu, designed to run securely on IoT devices
- Based on the ARM Cortex quad core and includes a graphics card, onboard memory, card module etc

CONNECTIVITY FOR DEVICES

- Wireless Technologies
  - Bluetooth (Low Energy), ZigBee, NFC, RF link, WiFi, 5G
- Wired Technologies
  - I2C, SPI, UART



Physical/Data-link Layer



WPAN: Wireless Personal Area Network
WLAN: Wireless Local Area Network
WWAN: Wireless Wide Area Network

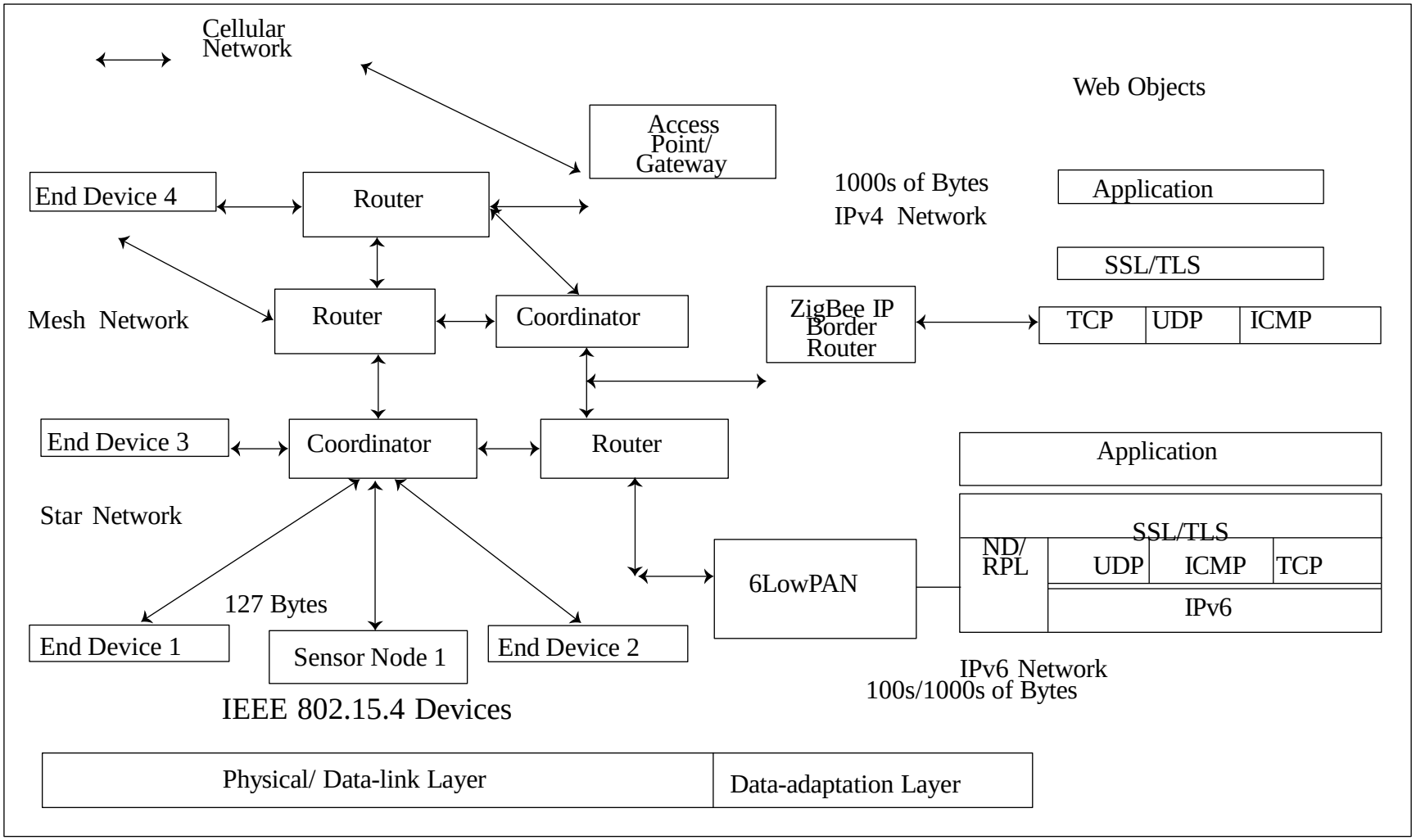
- Transmission distance is only one characteristic of wireless communications
- Wireless protocols use a specific frame format, transmission technique (**transmit power**, antenna gain) over a specific frequency (or **band**) for a specific **cost**
- These differences limit the amount of data throughput that each technology can achieve at a given distance, transmit power and bandwidth

Πανεπιστήμιο Κύπρου

- NFC short distance (20 cm) 2-way communication
- Setup time is 0.1 s. The device or its reader can generate RF fields for the nearby passive devices such as passive RFID.
- Data transfer rates are few hundred kbps
- Communication mode:
    - Point-to-point (P2P) mode: Both devices use the active devices in which RF fields alternately generate when communicating.
    - Card-emulation mode: Communication without interruption for the read and write
    - Reader mode: Using NFC the device reads passive RFID device. The RF field is generated by an active NFC device. This enables the passive device to communicate.
- Can interact with Bluetooth and WiFi

- BT employs IEEE 802.15.1 protocol standard and achieve ranges around 100 m at 10 mW power output, data transfer rate is 1 Mbps and setup time less than 6s
- BT devices form a WPAN network.
- Two operating modes BR/EDR (Basic Rate 1 Mbps/Enhanced Data Rate 2 Mbps and 3 Mbps) and Bluetooth low energy (BT LE 1Mbps).
- Bluetooth v4.2. BT LE is also called Bluetooth Smart providing the LE smaller data packet length, link layer privacy and secure connections, extended scanner and filter link layer policies and IPSP (Internet Protocol Support Profile)
- Bluetooth v5, has increased capacity by 800%, quadrupled the range and doubled the speed
- AES-CCM 128 authenticated encryption

- ZigBee implements IEEE 802.15.4 protocol standard for low-power, short-range (<200m) WPAN, low latency (< 10 ms) link
- Data transfer rate is <250 kbps (Ideal for smart meters)
- ZigBee devices form a WPAN network of embedded sensors, actuators, controllers
- The device can function in six modes
    - end point, ZigBee-ZigBee devices router, ZigBee network coordinator, ZigBee-IP coordinator, ZigBee-IP router and IP host.
- A ZigBee IP device is a Reduced Function Device (RFD). RFD means one that functions for the 'sleepy'/ battery-operated device. Sleepy means one that wakes up infrequently, sends data and then goes back to sleep.



Πανεπιστήμιο Κύπρου

- Wi-Fi implements IEEE 802.11 protocol standard enabling WLANs in the ISM Bands 2.4GHz/ 5GHz / etc
- Wi-Fi interfaces connect within themselves / an AP or wireless router
- Offers roaming across cells of range <100m and high data rates of hundreds of Mbps

- Cellular networks are Wireless Wide Area Networks(WWAN)
- Partition a geographical area into “cells”
  - Manage a subset of the total available channels
  - *Frequency reuse* between distant cells
  - Full duplex communication using downlink/uplink channels
  - OFDMA on allocated channels for digital communication
- Adaptive QAM modulation enables high data-rate at the expense of increased processing -> high energy consumption
- Adaptive retransmission and error correction to combat the wireless channel effects
- Short latencies achieved by streamlined 5G IP based architecture

- Wired communication
    - serial asynchronous communication (for example, UART interface)
    - synchronous serial communication (for example, SPI interface
    - parallel input, output and input-output ports at the devices).
- Wired communications can be over a bus when a number of components (chips, units, integrated circuits or ports or interfacing circuits) connect through a common set of interconnections
- A Bus provides a set of control, address and data signals such that the data signals are accepted by the device at destination address only from a source at an instance
- Bus signals may be sent in a serial or parallel manner. Communication is between a master at a given instance (sender) and the destined address computer (listener) at an instance.
    - Ethernet IEEE 802.2 bus specifications
        - MAC data frame defined
    - USB specification

- Universal Asynchronous Transmitter (UART) Serial Communication
- UART enables serial communication (transmission) of 8 bits serially with a start bit at the start of transmission of a byte on serial Transmitter Data (TxD) output line. Serial data present one after another at successive time intervals
- Asynchronous communication results in variation in time intervals for each frame or phase differences between successive bytes and in-between wait interval since clock information is not accompanying the data. Successive set of bytes may wait after transmission till an acknowledgement is received
- Transmit bit clock period T = 0.01 ms, and thus a byte's transfer rate is 1 MBps with Baud Rate 1/T
- Universal Synchronous Asynchronous Transmitter (USART) enables serial communication (transmission) in synchronous as well as asynchronous modes
    - Synchronous means all bytes in a frame transmit with equal time spacing or equal phase differences

- SPI is a widely used serial synchronous communication methods
- Master-Slave architecture where
    - Master is the source of serial synchronous com hich controls the synchronising clock
    - A receiver of serial synchronous input or output is called a slave
    - Four sets of signals, SCLK, MISO, MOSI, and SS (slave select) are used on four wires. When SS is active, then the device functions as a slave.
- Master Input Slave Output (MISO) / Master Output Slave Input (MOSI)
    - MOSI is output from master and input at slave and SCLK (clock information or signal) is from the master to slave
    - MISO is synchronous serial input at the master for the serial output from slave. Slave synchronises output as per SCLK of the master. Master synchronises the input as per SCLK of the master

- A number of device integrated circuits for sensors, actuators, flash memory and touchscreens need data exchanges in a number of processes
- ICs mutually network through a common synchronous serial bus, I2C
- 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 I2C and 400 kbps I2C
- I2C bus has two lines that carry the signals - one line is for the clock and one is for bidirectional data.
- I2C bus protocol has specific fields. Each field has a specific number of bits, sequences and time intervals between them

- Wired USB provides fast serial transmission and reception
- Maximum 127 devices can connect with a host.
- USB standard provides a fast (up to 12 Mbps) as well as a low-speed (up to 1.5 Mbps) serial transmission
- Features of a USB are:
    - USB data format and transfer serial signals are Non Return to Zero (NRZI) and the clock is encoded by inserting synchronous code (SYNC) field before each packet
    - four types of data transfer - controlled data, bulk data, interrupt driven and isosynchronous
- USB is a polled bus. Polling mode functions as: A host controller regularly polls the presence of a device as scheduled by the software. It sends a token packet. The token consists of fields for type, direction, USB device address and device end-point number.
- The device does handshaking through a handshake packet, indicating successful or unsuccessful transmission. A CRC field in a data packet permits error detection.
- A USB supports three types of pipes
    - Stream with no USB-defined protocol is used when the connection is already established and the data flow starts.
    - Default control is for providing access.
    - Message is for control functions of the device.
- The host configures each pipe with the data bandwidth to be used, transfer service type and buffer sizes.

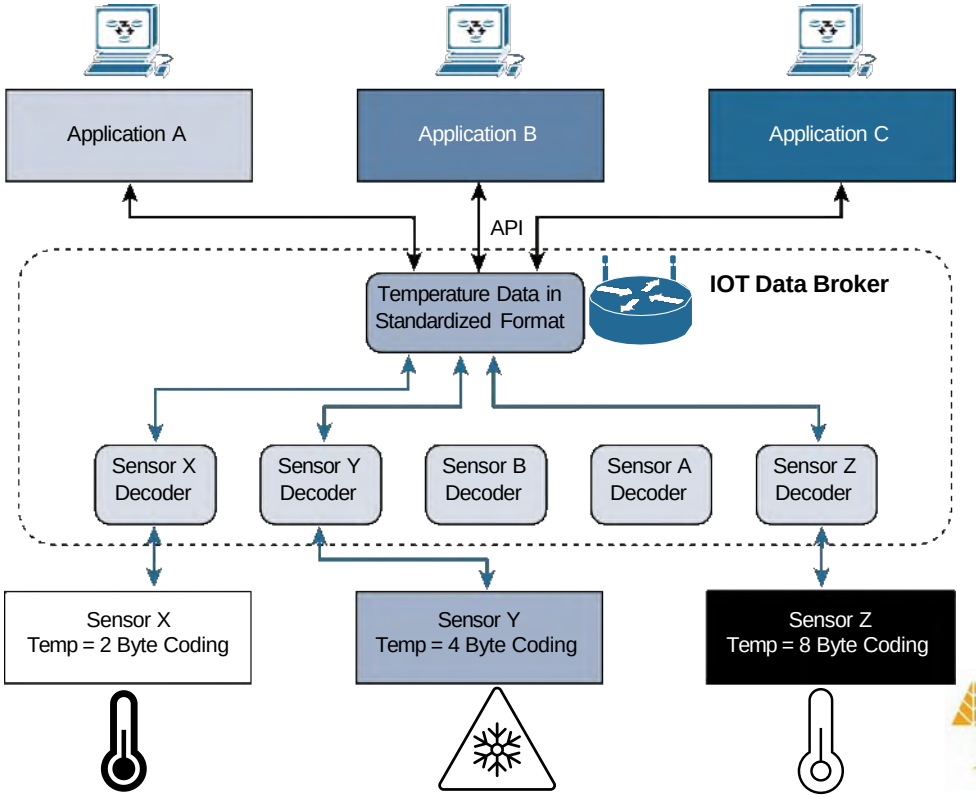
- Ethernet standard is based on IEEE 802.2 (ISO 8802.2) protocol for LANs (define header / payload size)
- Features of Ethernet are:
    - Uses passive broadcast medium
    - Formatting of frame (serially sent bits as PDU of MAC layer)
    - Uses 48-bit MAC address
    - Address Resolution Protocol (ARP) resolves a 32 bit IP address at
    - Reverse Address Resolution Protocol (RARP) resolves 48 bit destination host media address into 32 bit IP addresses for Internet communication.
- Transmission speeds are 10 Mbps, 100 Mbps (unshielded and shielded wires), 1 Gbps (high-quality coaxial cable), 4 Gbps (in twisted pair wiring mode) and 10 Gbps (fiber-optic cables)
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- Half-duplex meaning transmit (Tx) and receive (Rx) signals can be sent on the same wire or data path.
    - Each device listens and if the channel is idle then transmits.
    - If not idle, it waits and tries again.
- Preamble in the header is used to indicate start of a frame and synchronisation

Property	**NFC**	**BT LE**	**ZigBee IP**	**WLAN 802.11**
IEEE Protocol		802.15.1	802.15.4	802.11z
Physical Layer	848, 424, 212, 106 kbps	2.4 GHz (LE-DSSS)	2.4 GHz or 915 MHz, 868 MHz and 433 MHz DSSS MAC layer CSMA/ CA	2.4 GHz Two PHY layers MAC layer CSMA/CD
Data Transfer Rate	106 kbps	1 Mbps	250 kbps (2.4 GHz, 40 kbps 915 MHz, 20 kbps 868.3 MHz	11 Mbps/54 Mbps
Power Dissipation	Very low	Lower than ZigBee, much lower than WLAN 802.11	2 mW Router and 0.1 mW for end- device Much lower than WLAN 802.11	Much Higher than ZigBee
Set up/ Connection/ Disconnection Intervals	0.1 s	3s Connection time < 3 ms	20 ms Connection time < 10 ms	
Security	—	AES-CCM-128	AES-CCM-128	WEP
Network	Point to point between active and passive devices	Star topology, peer- to-peer piconet expended by inter- piconets data transactions and synchronisation	Low power, mesh or peer-to peer star networks using end devices, coordinator, router, ZigBee IP border router	LAN topology IBSS, BSS and distributed BSSs for WWLAN widely used for Internet connectivity of mobiles, tablets, desktops
Broadcast/ Multicast/Unicast	Unicast	Unicast	Unicast/ multicast	Unicast

APPLICATION PROTOCOLS

- Data acquisition from devices can be taxonomized in four modes:
  - Polling data from a device by querying the device
  - Event-based gathering refers to the data sought from the device on an event; for example, when the device reaches near an access point or a card reaches near the card reader or an initial data exchange for the setup of peer-to-peer or master-slave connection
  - Scheduled interval refers to the data sought from a device at select intervals
  - Continuous monitoring
- Data enrichment refers to adding value, security and usability of the data by introducing extra bits, meta-data (ID, timestamp, location, etc)

- Naïve approach is to adopt deployments with no application layer, **not recommended** due to lack of **management** and **maintenance**, **interoperability**
- Instead, use of data **brokers**: piece of middleware
    - standardizes device input/ output into a common format that can then be retrieved by applications



Πανεπιστήμιο Κύπρου

- IP, TCP, and UDP bring connectivity to IoT networks
- Upper-layer protocols take care of data transmissions
- Multiple protocols exists:
    - Push model (that is, a sensor reports at a regular interval or based on a local trigger)
    - Pull model (that is, an application queries the sensor over the network)
    - Hybrid approaches
- HTTP for data transfer has a client-server structure
    - sensor use the client part to establish a connection to app server
- Web-derived protocols have been suggested such as WebSocket
    - Provides a simple bidirectional connection over a single connection.
    - Often combined with other protocols, such as MQTT (described shortly) to handle the IoT-specific part of the communication
- Note that HTTP is a fat protocol and was not designed to operate in constrained environments with low memory, low power, low bandwidth, and a high rate of packet failures

- With the same logic of reusing well-known methods, Extensible Messaging and Presence Protocol (XMPP) was created
- XMPP is based on instant messaging and presence
- Allows the exchange of data between two or more systems and supports presence and contact list maintenance
- Can also handle publish/subscribe, making it a good choice for distribution of information to multiple devices
- A limitation of XMPP is its reliance on TCP, which may force subscribers to maintain open sessions to other systems and may be a limitation for memory-constrained objects

- Web App is a software to address application requirements
- Application Programming Interface (API) refers to
    - software component, which receives messages from one end; for example, from an application or client as input and initiates actions (send structured requests), to application software, server or a client at the other end
    - software components, which enable easier development of an application. An API defines the functionalities for a programmer, which puts the building blocks together to develop an application. A building block consists of the operations, inputs, outputs and underlying types.
- Web service uses web protocols, web objects or WebSockets; e.g. weather reports service
- Object refers to a collection of resources; for example, collection of data and methods (or functions or procedures) to operate on data
    - e.g. Time_Date object with second, minutes, hour, day, month and year fields and update methods.

- Broker denotes an object managing communication between two ends; e.g. between the message publisher and subscriber or for example taking the request from a source and sending the response received back for that source after arranging the response from another object
- Proxy refers to an application which receives a response from the server for usage of a client or application and which also receives requests from the client for the responses retrieved or saved at the proxy
- Web protocol is a protocol that defines the rules and conventions for communication between the web server and web clients. It is a protocol for web connectivity of web objects, clients, servers and intermediate servers or firewalls. It includes mechanisms for a web object to identify and make connections with other objects. The protocol also includes web object formatting rules that specify how that object packs into it the sent and received messages

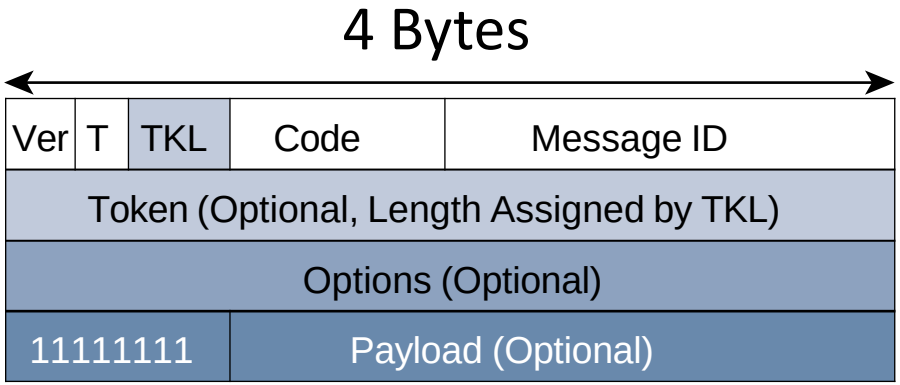
- Representational State Transfer (**REST**) is a software architecture referring to ways of defining the identifiers for the resources, methods, access methods and data transfer during interactions.
- REST is a software architecture which also specifies the practices, constraints, characteristics and guidelines for creating scalable web services.
- Scalable means can be used as per the size. The architecture is used during the design of web software components, clients and web APIs
- REST also refers to usage of defined resource types when transferring the objects between two ends—URIs or URLs for representations of the resources.
- REST also refers to the usage of use verbs (commands), POST, GET, PUT and DELETE and files of MIME types

- Multipurpose Internet Mail Extensions or MIME refers to the type of files that are widely used on the Internet by web objects, applications and services
- **RESTful** refers to one which follows REST constraints and characteristics
- **WebSocket** denotes an API for bidirectional communication that has much less header size than HTTP communication and lower latency compared to HTTP approach of unidirectional communication at an instant
- **Framework** refers to provisions for a number of software libraries, and a number of APIs including those that can be selectively changed by user codes in applications
    - set of discrete objects, software components, protocols, that are easier to work with
    - implement code in a way that promotes consistent coding,
    - easier testing and debugging of code

- Constrained RESTful Environment (CoRE)
  - A device typically sends or receives small number of bytes
  - Data communicated when low power transceiver.
  - Devices duty cycle to conserve battery
  - Devices' connectivity may also break for long periods
- Hence the need for Constrained IoT protocols

- Constrained Application Protocol (**CoAP**) using REST
- Specialised web-transfer protocol
  - Defines **simple** and **flexible** ways to manipulate sensors and actuators for **data** or **device management**
- Features of CoAP are:
  - Application-support layer protocol
  - CoAP web-objects communicate using request/ response interaction model
- Object-model for the resources with single or multiple instances.
- Resource directory and resource-discovery functions
  - Resource identifiers coap://…

- Small message header



- ver (version)
- T (message type) [**confirmable**, **non-confirmable**, **acknowledgement** and **reset**]
- TKL (token length)
- code (request method or response code)
- message ID 16-bit identifier (Detects message duplication and used to match ACK and RST message types to Con and NON message types)
- token (correlates requests and responses)

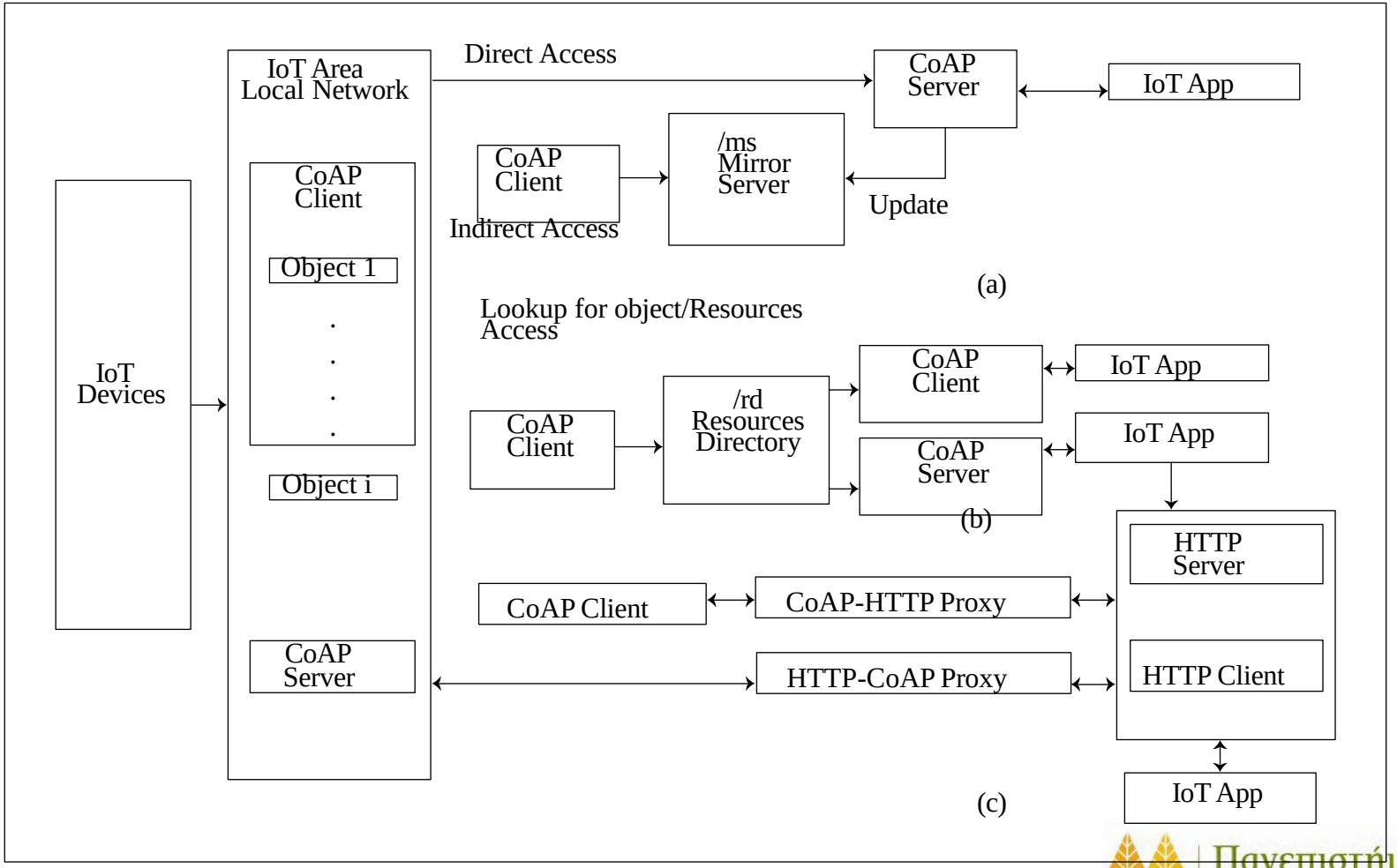
Πανεπιστήμιο Κύπρου

Communication over the network can take various paths

a. Direct and indirect accesses of CoAP client objects to a CoAP server

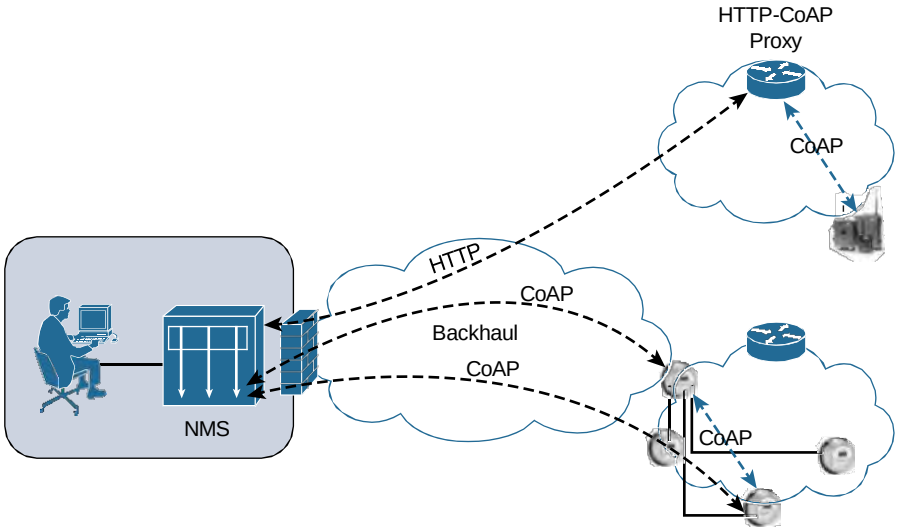
b. CoAP client for lookup of object or resource using resource directory

c. CoAP client and server access using proxies



Πανεπιστήμιο Κύπρου

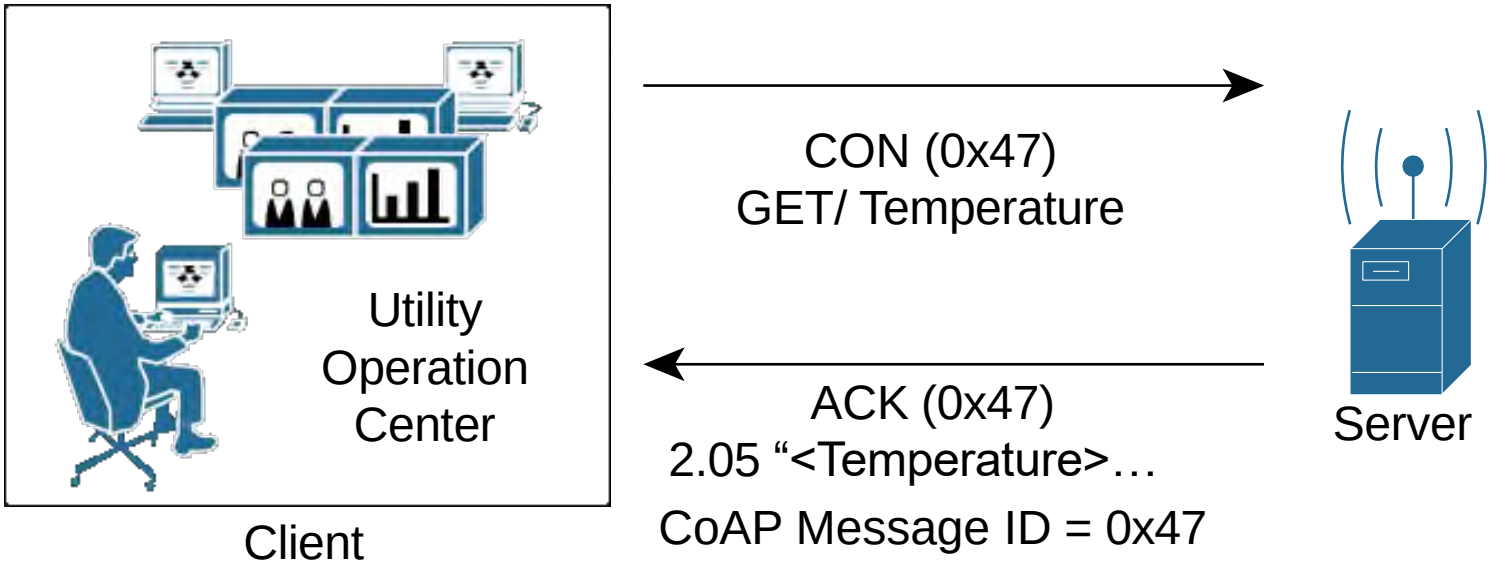
- Connections
  - between devices located on the same or different constrained network
  - between devices and generic Internet or cloud servers, all operating over IP



- Through the exchange of asynchronous messages:
  - a client requests an action via a method code on a server resource
- A uniform resource identifier (URI) localized on the server identifies resources
- The server responds with a response code that may include a resource representation
- The CoAP request/response semantics include the methods GET, POST, PUT, and DELETE
- CoAP URI format example:

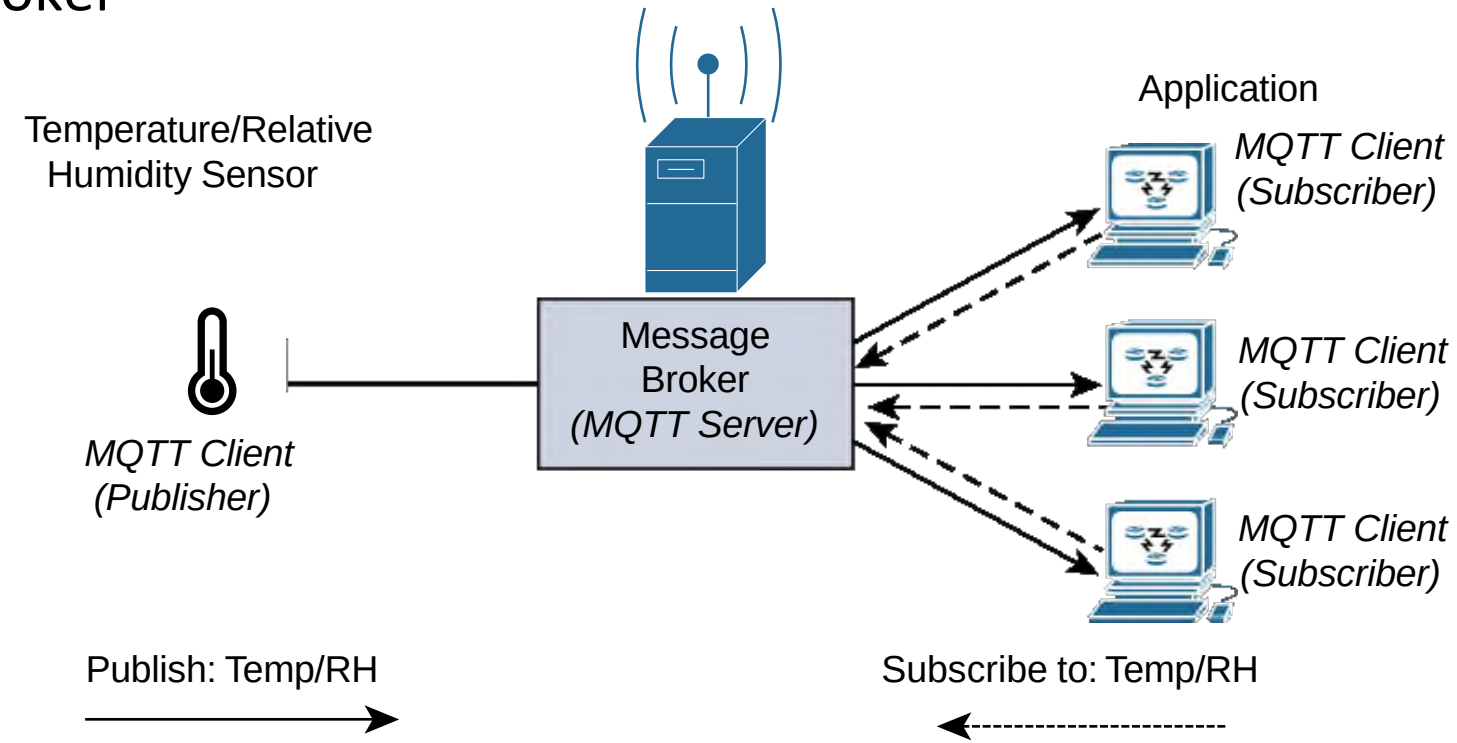
```
coap-URI = "coap:" "//" host [":" port] path-abempty ["?" query]
coaps-URI = "coaps:" "//" host [":" port] path-abempty ["?" query]
```

Πανεπιστήμιο Κύπρου



- CoAP offers a reliable transmission of messages when a CoAP header is marked as "confirmable"
- CoAP supports basic congestion control with a default time-out, simple stop and wait retransmission with exponential back-off mechanism, and detection of duplicate messages through a message ID

- **MQTT** is an open-source protocol for IoT
- MQTT client can act as a publisher to send data (or resource information) to an MQTT server acting as an MQTT message broker

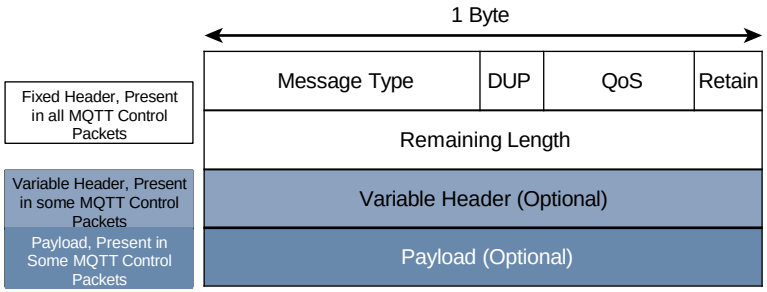


- **MQTT** is an open-source protocol for IoT
- MQTT Broker does the following:
  - Functions as a server storing messages from publishers and forwarding to subscribers
  - Receives topics from the publishers
  - Receives subscriptions from clients on the topics, matches subscriptions and publications
  - Recovers subscriptions on reconnect after a disconnection, unless the client explicitly disconnected
- Topic & levels (**#**:wildcard for specific levels):

adt/lora/adeunis/0018B20000000E9E

- Authentication by Username/Password in connect message and client security is made through SSL/TLS (port 8883) and WebSocket

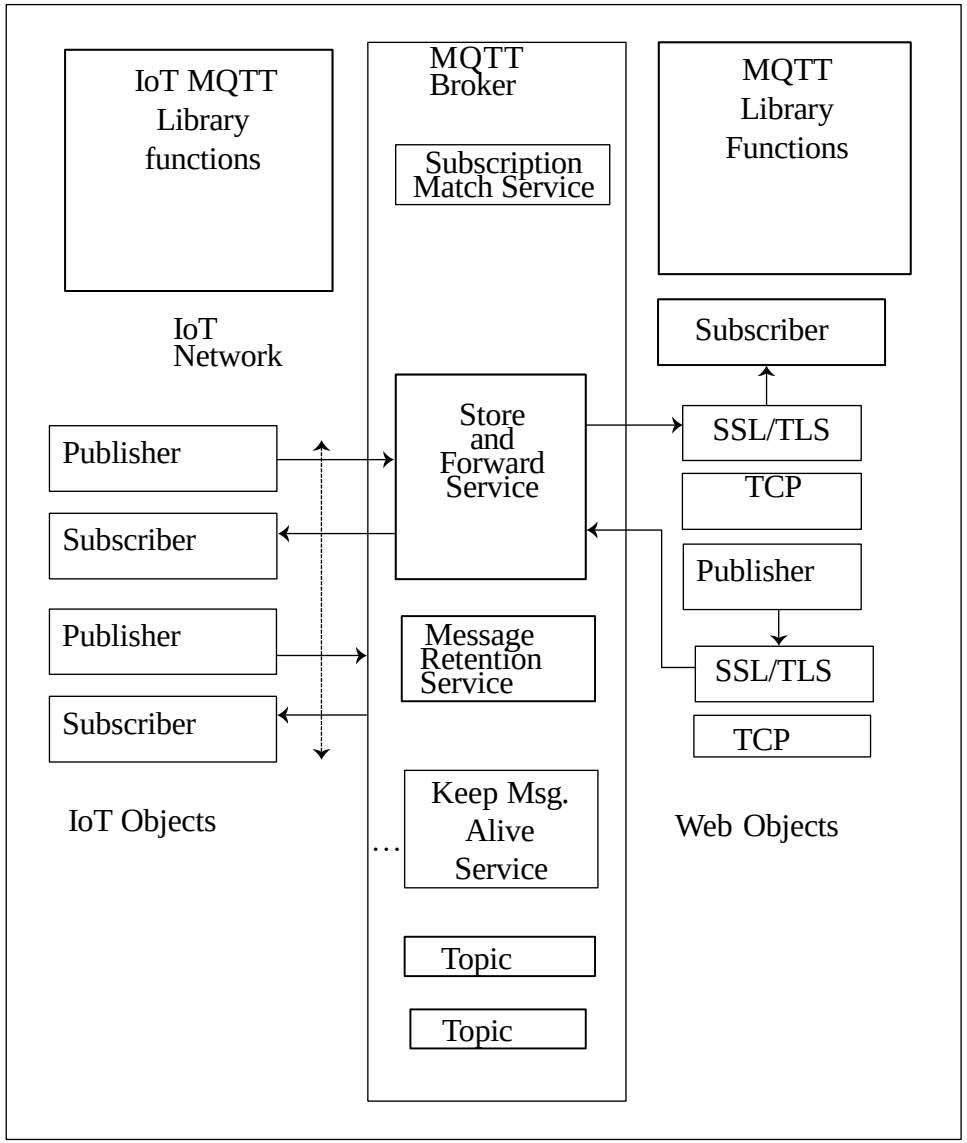
- MQTT is a lightweight protocol
- Each control packet consists of 2-byte fixed header with optional variable header fields and optional payload
- A control packet can contain **payload** up to 256 MB
- MQTT Message Format:



- MQTT sessions consist of four phases: session establishment, authentication, data exchange, and session termination

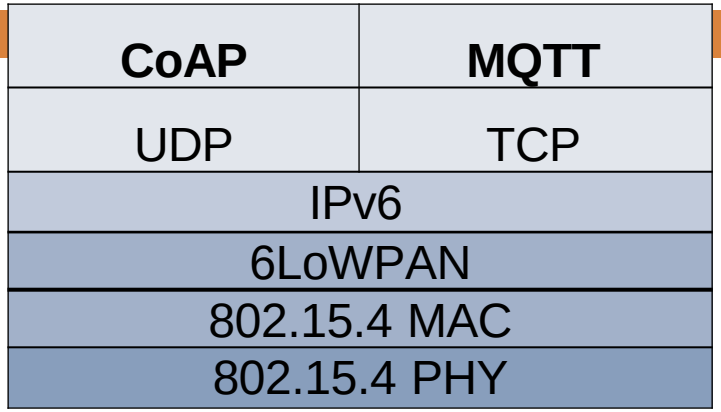
Πανεπιστήμιο Κύπρου

Messages interchange between devices (publisher and subscriber) and web objects (publisher and subscriber) using an MQTT Broker



Πανεπιστήμιο Κύπρου

- MQTT provides 3 levels of QoS
  - **QoS 0**: best-effort and unacknowledged service for "**at most once**" delivery. The publisher sends its message one time to a server, which transmits it once to the subscribers. No response is sent by the receiver, and no retry is performed by the sender. The message arrives at the receiver either once or not at all!
  - **QoS 1**: Ensures that the message delivery between the publisher and server and then between the server and subscribers occurs at least once. If message not acknowledged, it is sent again. This level guarantees "**at least once**" delivery!
  - **QoS 2**: No loss nor duplication of messages; increased overhead because each packet contains an optional variable header with a packet identifier. Requires a 2-step acknowledgement process. The first step is done through the PUBLISH/PUBREC packet pair, and the second is achieved with the PUBREL/PUBCOMP packet pair. This level provides a "guaranteed service" known as "**exactly once**" delivery, with no consideration for the number of retries as long as the message is delivered once!



Factor	CoAP	MQTT
Main transport protocol	UDP	TCP
Typical messaging	Request/response	Publish/subscribe
Effectiveness in LLNs	Excellent	Low/fair
Security	DTLS	SSL/TLS
Communication Model	One-to-one	many-to-many
Strengths	Lightweight and fast, with low overhead; uses a RESTful model; easy to parse and process for constrained devices; support for multicasting; asynchronous and synchronous messages	TCP and multiple QoS options provide robust communications; simple management and scalability using a broker architecture
Weaknesses	Not as reliable as TCP-based MQTT, so the application must ensure reliability	Higher overhead; TCP connections can drain low-power devices; no multicasting support

http://coap.technology/impls.html

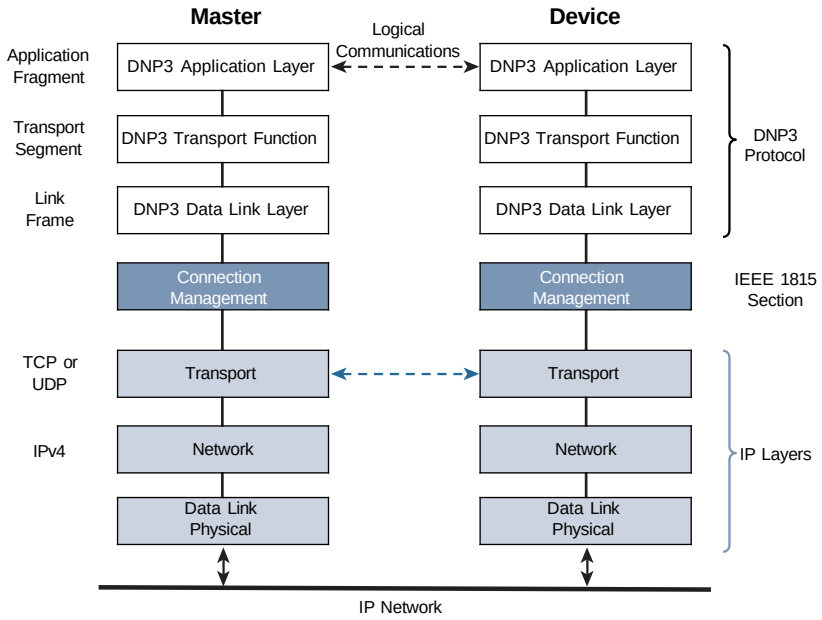
https://github.com/mqtt/

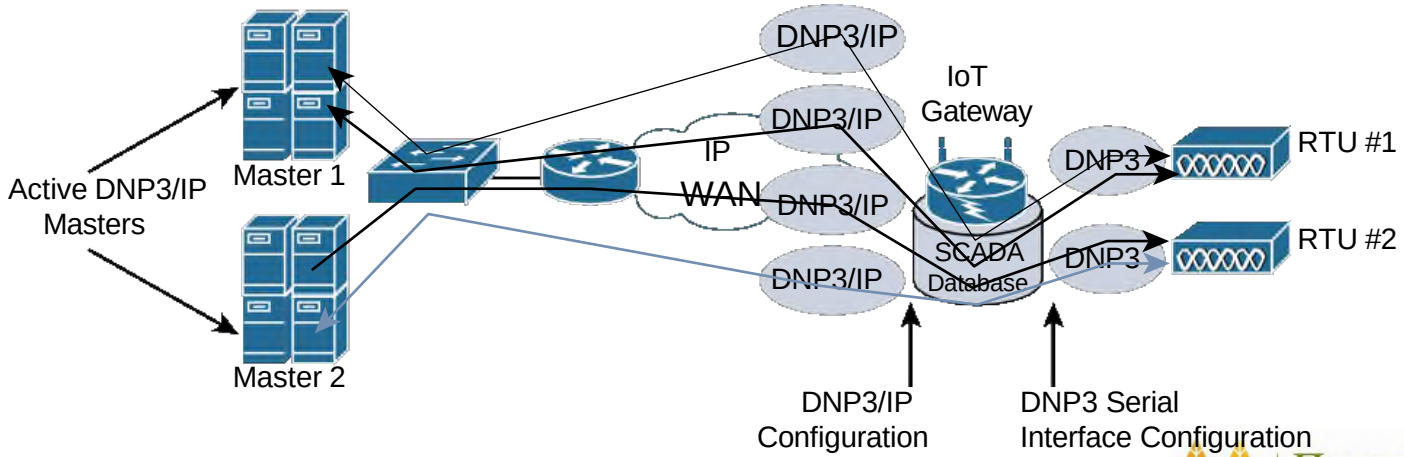
Πανεπιστήμιο Κύπρου

- SCADA is the most common industrial networking protocol for automation control systems
- Running directly over serial physical and data link layers
- Developed long before the days of IP, and it has been adapted for IP networks
- SCADA commonly uses **serial protocols** for communications between devices and applications
    - **Modbus** used to monitor and program remote devices via a master/slave relationship; using in building management /transport sectors
    - **DNP3** and International Electrotechnical Commission (**IEC**) **60870-5-101** used by utilities
- SCADA application layer protocols adapted to IP by assigning TCP/UDP port numbers to the protocols
    - e.g. Modbus messaging service utilizes TCP port 502

- e.g. DNP3 is based on a master/slave relationship.
  - master is a powerful computer located in the control center of a utility
  - a slave is a remote device with computing resources found in a location such as a electricity substation
- Devices monitor and collect data indicating their state
  - Measure voltage, current, temperature, etc
  - Events: e.g. If a circuit breaker is on or off
- Data is transmitted to the master when it is requested, or events and alarms can be sent in an asynchronous manner
- Master issues control commands, such as to start a motor or reset a circuit breaker, and log the incoming data

- Protocol Stack for Transporting Serial DNP3 SCADA over IP



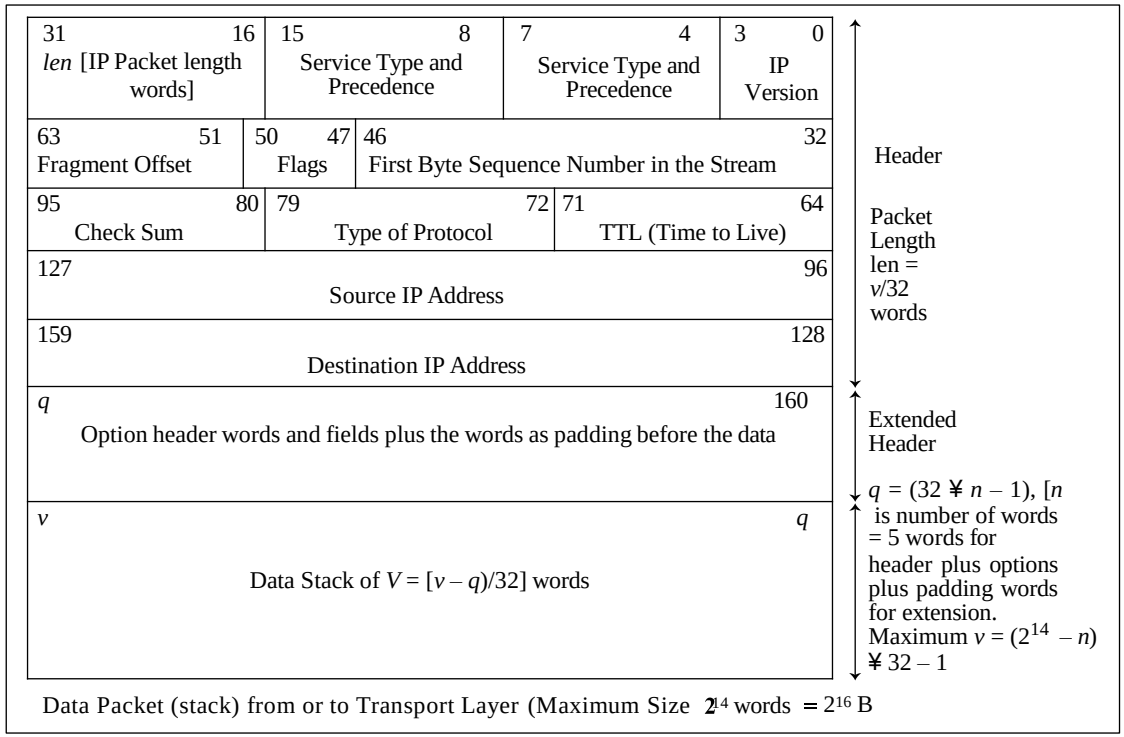


Πανεπιστήμιο Κύπρου

INTERNET CONNECTIVITY PRINCIPLES

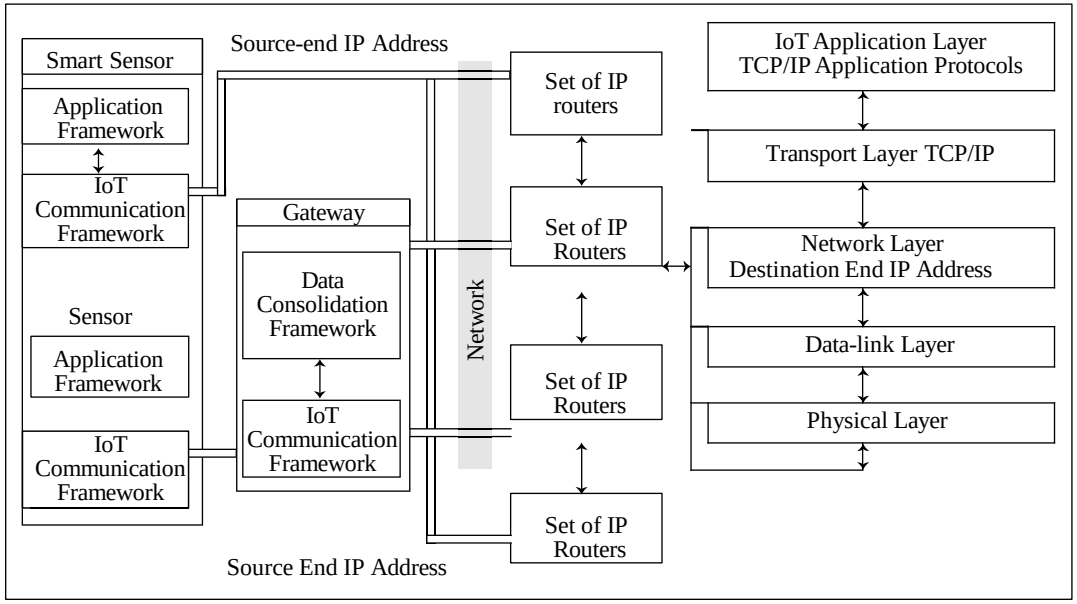
Πανεπιστήμιο Κύπρου

- Internet connected devices send data as packets (set of bytes), which are forwarded through a set of routers
- Devices monitor and control the flow using messages, data-stacks and commands
- IP Header are required for processing a received data at the Network layer
- TCP Header includes fields related to data processed at the Transport layer
- Protocol Data Unit (PDU) is the maximum number of bytes, which can be processed at a layer as per the protocol
- Port is an interface to the network from an application
- Socket is a software interface to the network that links a port protocol and an IP address



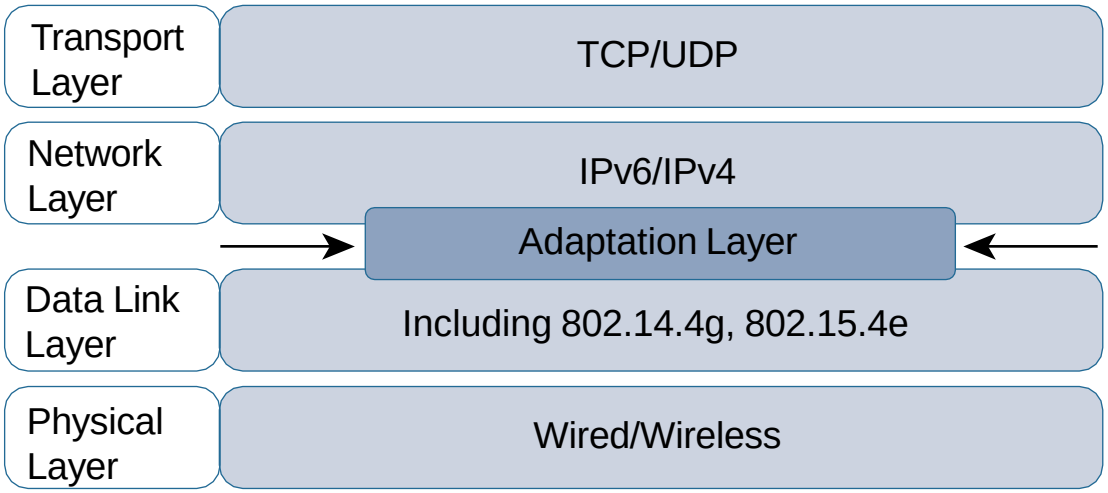
Πανεπιστήμιο Κύπρου

IoT networking through a set of IP routers from an IP address and communicating with an IoT application using TCP/IP suite of application protocols



Πανεπιστήμιο Κύπρου

- IP is key for the success of IoT but constrained nodes and constrained networks mandate optimization
- Adaptation Layer

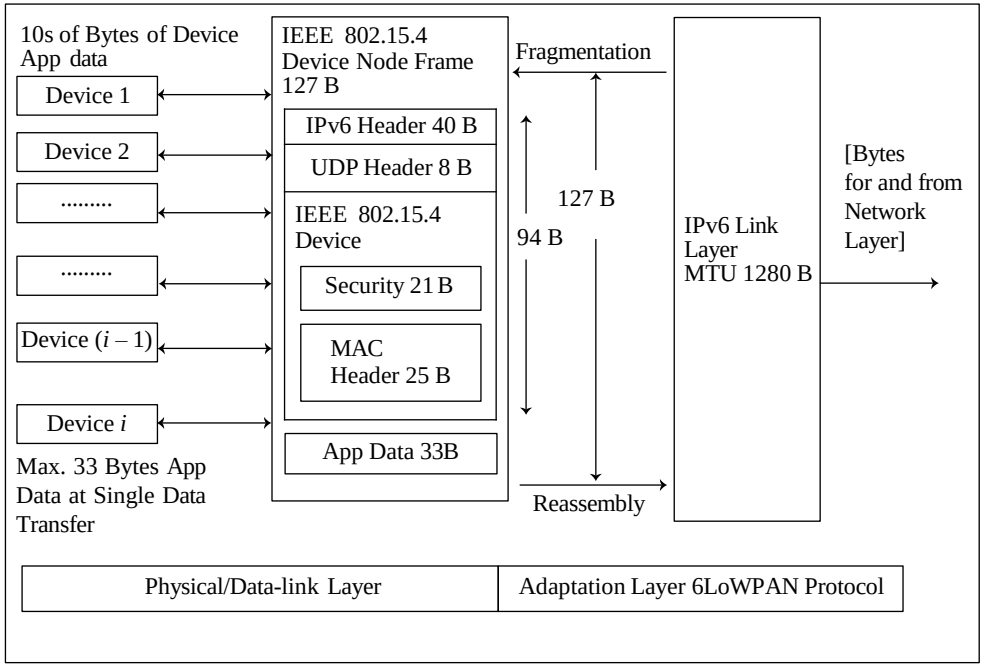


- 6LoWPAN adaptation (now 6Lo) for IoT
- Optimize transmission of IPv6 over constrained networks (such as IEEE 802.15.4)

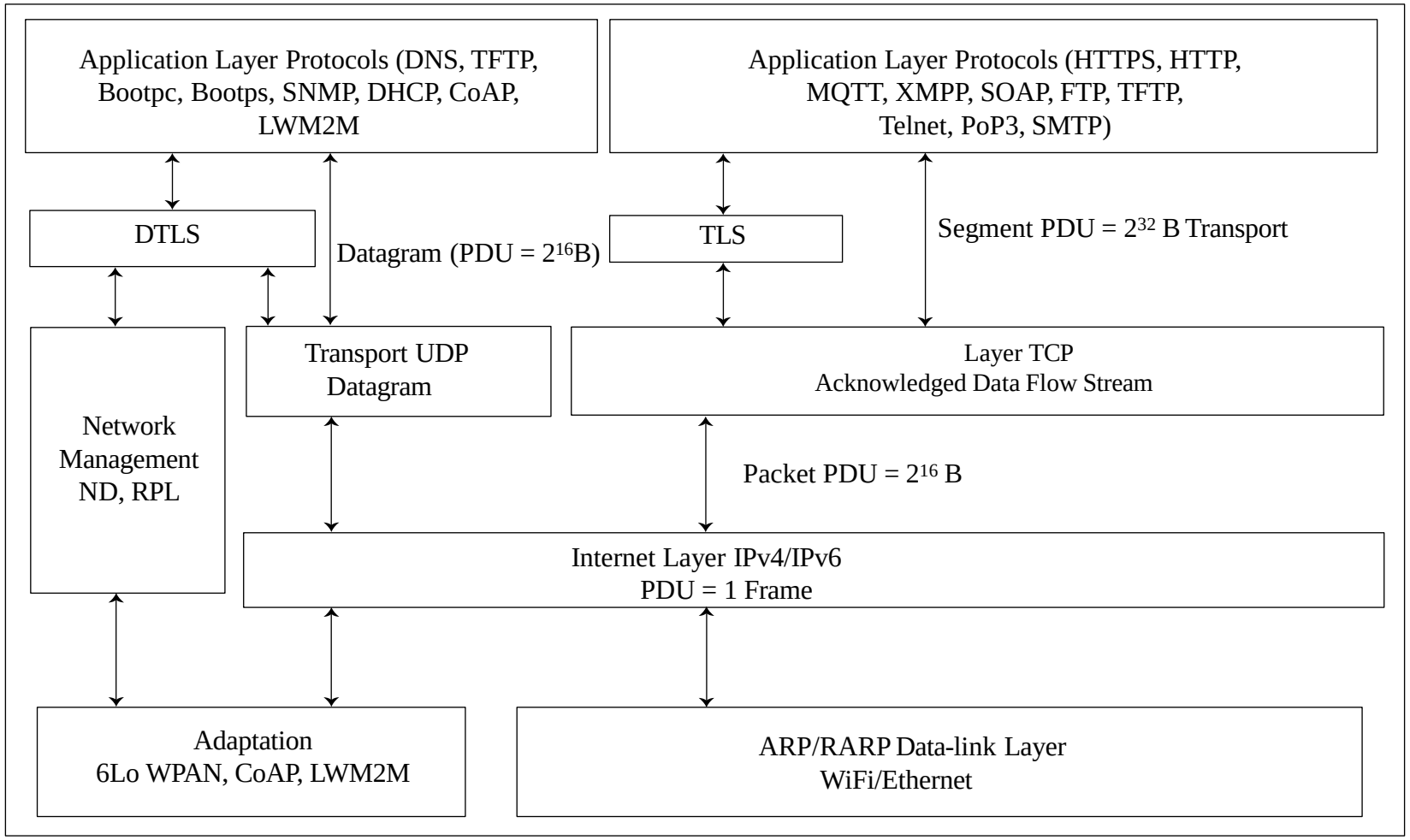
- 6LoWPAN (IPv6 Over Low Power Wireless Personal Area Network) is an adaptation-layer protocol
- IEEE 802.15.4 WPAN device use it to forward IPv6 traffic
- Features of 6LoWPAN include **header compression**, **fragmentation** and **mesh addressing**

IoT Protocol Stack with 6LoWPAN Adaptation Layer

Application Protcols	
UDP	ICMP
IPv6	
LoWPAN	
IEEE 802.15.4 MAC	
IEEE 802.15.4 PHY	

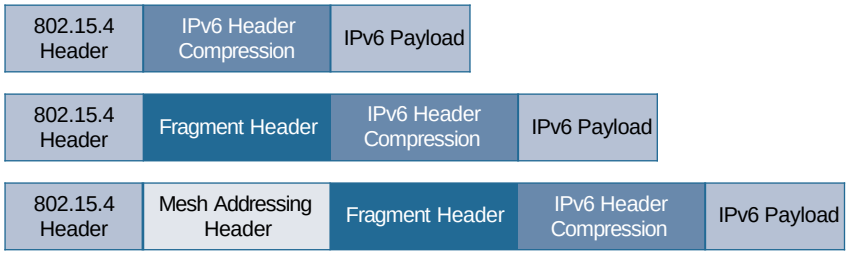


Πανεπιστήμιο Κύπρου

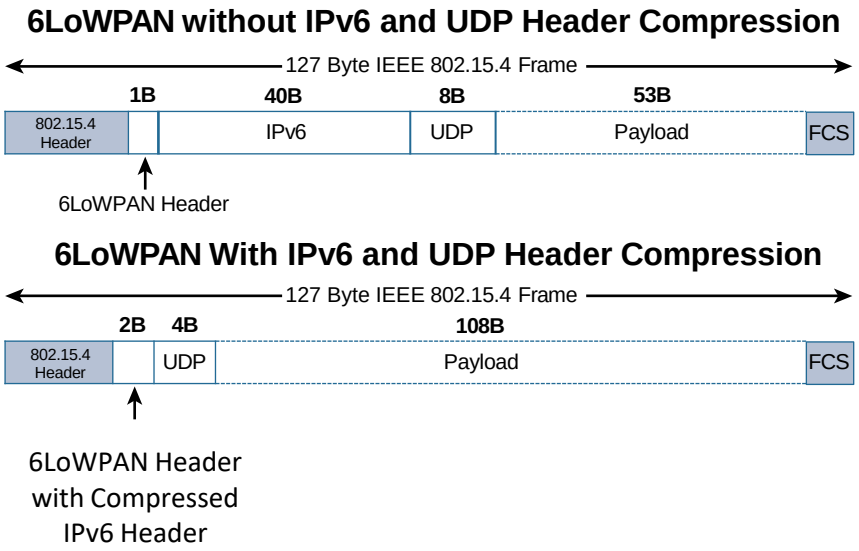


Πανεπιστήμιο Κύπρου

- 6LoWPAN Header Stacks

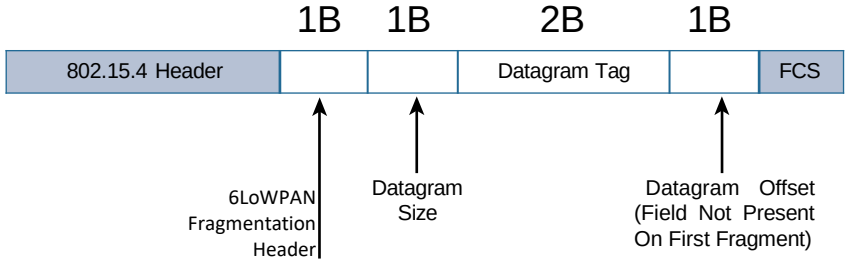


- Header compression
  - shrinks IPv6's 40-byte and UDP's 8-byte headers down as low as 6 bytes combined



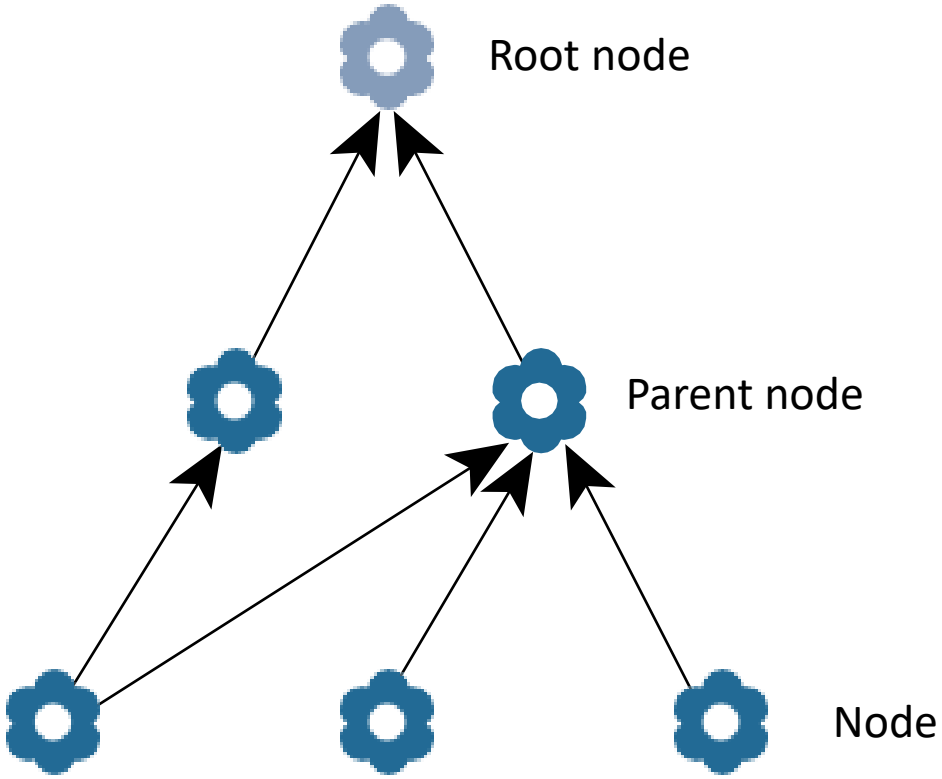
Πανεπιστήμιο Κύπρου

- IPv6 maximum transmission unit (MTU) 1280 bytes
  - MTU defines the size of the largest protocol data unit that can be passed
- IEEE 802.15.4 MTU is 127 bytes
- Hence large IPv6 packets fragmented across multiple 802.15.4 frames at Layer 2
- Fragment header has three primary fields, **Datagram Size**, **Datagram Tag**, and **Datagram Offset**
  - Datagram Size (1-byte) specifies total size of unfragmented payload
  - Datagram Tag identifies the set of fragments for a payload
  - Datagram Offset indicates how far into a payload a particular fragment occurs

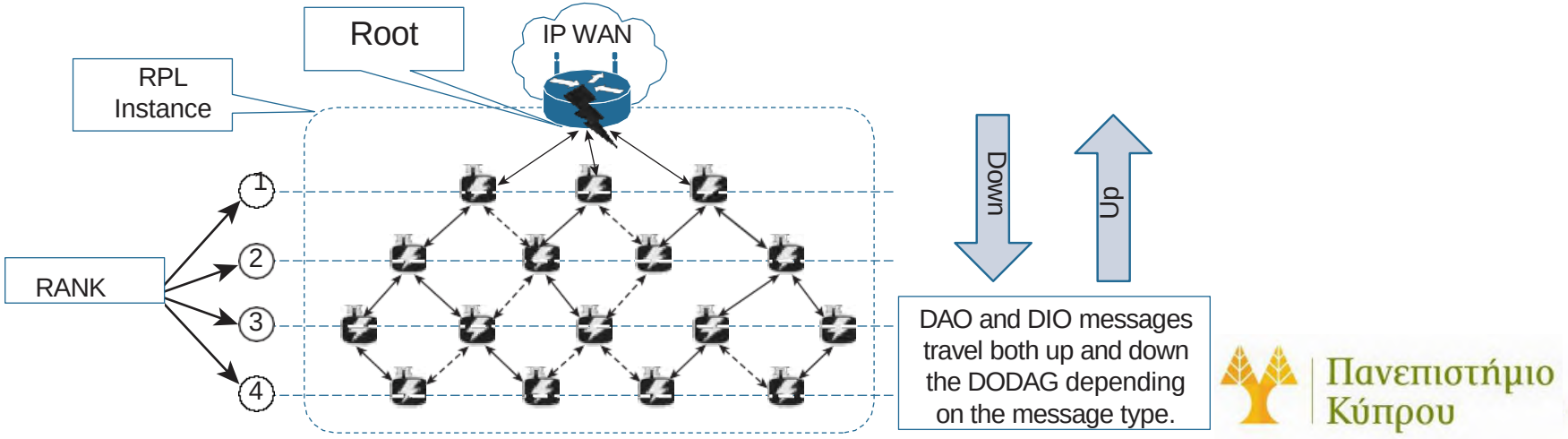


- Mesh enables forwarding of packets over multiple hops
- Addressing Header: **Hop Limit**, **Source/ Destination Address**
  - hop limit provides limits forwarding times
  - Each hop decrements value by 1
  - Once hits 0, dropped and no longer forwarded
- IPv6 Routing Protocol for LLNs (**RPL**)
  - each node acts as a router
  - routing is performed at the IP layer
  - Each node determines the next-hop destination based on the information contained in the IPv6 header
- To cope with the constraints of computing and memory operates:
  - **Storing mode**: full routing table
  - **Non-storing mode**: Border router(s) use full routing table. All other nodes in the domain only maintain their list of parents. A node forwards its packets to the border router

- RPL forms a directed acyclic graph (DAG)
- No cycles exist and all edges are arranged in paths oriented toward and terminating at one or more root nodes



- Routing graph created using message exchange
- Upward routes are discovered and configured using DAG Information Object (DIO) messages
  - Nodes listen to DIOs to handle changes in the topology
  - Determine parents and best path to root
- Downward routes set by nodes advertising their parent set using a Destination Advertisement Object (DAO) message
  - DAO messages allow nodes to inform their parents of their presence and reachability to descendants
- RPL DIO and DAO messages run on top of IPv6



Πανεπιστήμιο Κύπρου