Course Takeaways

(and inputs for your Portfolio ...)

1. IoT network characteristics and specificities

Hint : *List the major peculiarities of IoT physical networks. If needed, you can take the case of Low-Power Wireless Personal Area Networks (LP-WPAN) that we considered during the course and explain how they differ from conventional computer networks and what are the specific constraints that they are subject to.*

In general, IoT networks are subject to strong energy constraints. Sensors and actuators are often powered by batteries or other limited energy sources, which requires the use of extremely energy-efficient communication protocols in order to extend device lifetime. This requirement directly impacts network design: mechanisms that reduce transmission time, enable long sleep periods, and optimize exchanges to minimize power consumption are preferred.

LP-WAN technologies can cover several kilometers with minimal energy consumption, at the cost of lower throughput and less frequent transmissions.

Comparison with conventional networks:

Wi-Fi/Ethernet: High throughput, high energy consumption, larger range, fixed infrastructure.

IoT/LP-WPAN: Low throughput, low power consumption, short range, dynamic topology, loss tolerance.

Comparison table

Criterion	Traditional networks (Wi-Fi/Ethernet)	LP-WAN
Range	A few meters	Several km
Data rate	Mbps to Gbps	bps to kbps
Energy	High consumption	Ultra-low
Infrastructure	Local (routers)	Operators
Typical use	Broadband Internet	Long-range IoT

2. Rationale for adopting an IPv6 based architecture to support the communications of an IoT system or use case

Hint : *List the main benefits of adopting an IP based architecture in an IoT system, up the connected object (e.g. sensor, etc.).*

An IPv6-based architecture is particularly relevant for IoT communications because it provides several major benefits.

First, massive and unique addressing: IPv6 offers an almost unlimited address space thanks to 128-bit addresses, enabling billions of objects to be connected without the risk of address exhaustion. Each device can have a unique (potentially globally routable) IP address, which simplifies direct communication and reduces dependence on NAT.

Second, using IP as a common network layer ensures seamless integration with the Internet and existing networks. In addition, IPv6 simplifies address management and improves routing mechanisms, which is especially useful for large-scale and dynamic IoT deployments.

Unlike IPv4, IPv6 enables end-to-end communication between devices and servers, which significantly simplifies IoT architectures. This makes IPv6 well suited for Machine-to-Machine (M2M) services and use cases where devices must communicate directly without relying on complex gateways.

Finally, IPv6 can be adapted to IoT constraints through technologies such as:

1. 6LoWPAN, which compresses headers and handles fragmentation for low-power networks,
2. RPL, which optimizes routing in multi-hop, dense, and lossy environments.

3. IPv6 basics

Hint : First, from the experiments and traffic captures that you did during TD1, describe the different IPv6 initialisation steps that a host goes through, when switched on. Explain the rationale of the different steps, and the messages (with the types of IPv6 addresses) that are used to complete these steps. Then, derive some of the requirements of IPv6 (in terms of transmission capabilities of the physical network, and host availability) and enrich them with some other important characteristics of IPv6.

When an IPv6 host is powered on, several steps are required before it becomes operational on the network. These steps were observed during Lab/TD1 using Wireshark captures and Linux commands.

Main IPv6 initialization steps:

1. Interface activation and Link-Local address generation
   As soon as the interface (e.g., eth0) is enabled (ifconfig eth0 up), the host automatically configures a Link-Local address (prefix FE80::/10).

2. Duplicate Address Detection (DAD)
   The host sends a Neighbor Solicitation (NS) message to a dedicated multicast address in order to verify that its chosen address is not already in use.

3. Subscription to multicast groups
   The host joins essential IPv6 multicast groups (e.g., solicited-node multicast) to support Neighbor Discovery mechanisms efficiently.

4. Global address configuration
   The host receives network parameters via Router Advertisements (RA) sent by the router (stateless autoconfiguration / SLAAC), and configures a global IPv6 address accordingly.

5. Neighbor cache / neighborhood table update
   The host populates and updates its neighbor table (similar to ARP in IPv4, but using Neighbor Discovery in IPv6).

4. IPv6 adaptation and extensions in order to enable its use atop a physical IoT network

Hint :Without delving into the details, and relying on the experiment that you undertook during TD2, list the main additions, adjustments and optimizations of IPv6 that were defined for an application in the context of an IoT network.

IPv6, in its native form, is not directly suited to the constraints of IoT networks. For this reason, several adjustments and optimizations have been made to enable its use over physical IoT networks.

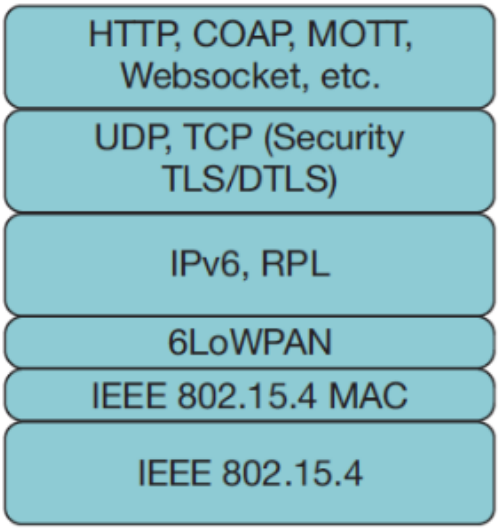
There is 6LoWPAN, an adaptation of IPv6 designed for IoT networks. This protocol provides IPv6 header compression, drastically reducing their size to fit the small MTU of IoT networks. It also includes a packet fragmentation mechanism to enable data transport despite frame size limitations. Finally, 6LoWPAN adapts the Neighbor Discovery protocol for sleeping

nodes, which spend most of their time in low-power mode, in order to minimize energy consumption while maintaining connectivity.

5. The IETF IPv6 based stack for IoT

Hint :Depict the protocol tack proposed by the IETF for IoT and then briefly describe the main network functions performed by the new layers. Also, provide a few words to describe the proposed application level protocols.

Below is the IPv6-based communication stack for IoT. The core idea is to keep IPv6 as the network layer, while adding a 6LoWPAN adaptation layer to make IPv6 efficient over radio links with small frames, and using a dedicated routing protocol (RPL).



Layer description (bottom-up)

Adaptation layer: 6LoWPAN

This layer sits between IEEE 802.15.4 and IPv6 to enable IPv6 over small frames.

It provides two main functions:

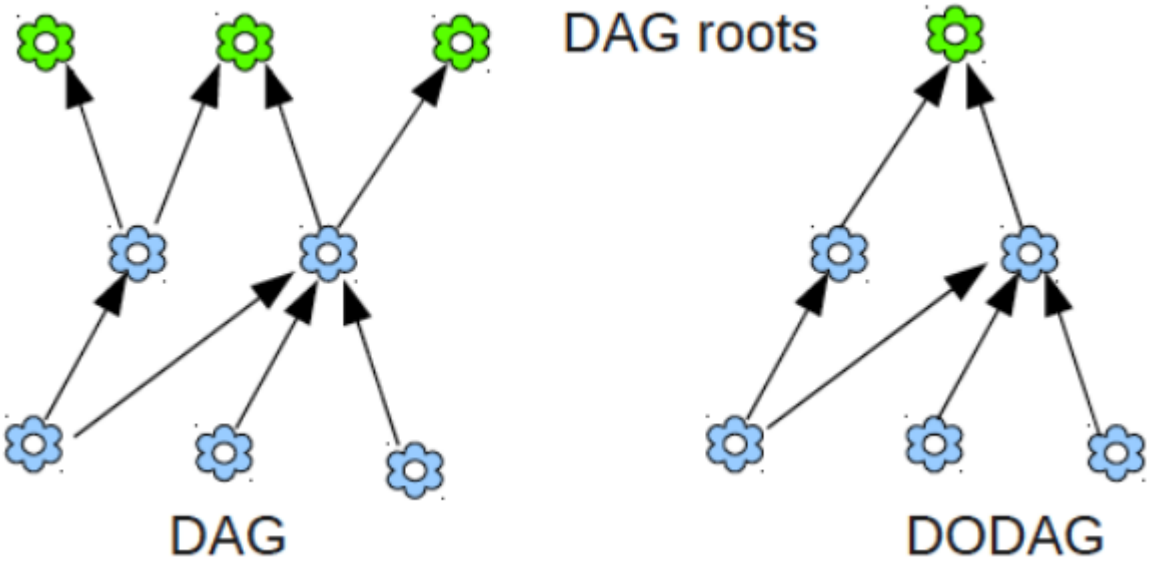
1. **IPv6 and UDP header compression**
   This significantly reduces header sizes. With IEEE 802.15.4, the maximum frame size is 127 bytes. Considering the MAC header (25 bytes) plus IPv6+UDP headers (48 bytes), the remaining application payload can be as low as 54 bytes without compression. Compression is therefore essential.

2. **Fragmentation**
   When an IPv6 packet does not fit into a single 802.15.4 frame, 6LoWPAN fragments it into multiple pieces and reassembles it at the receiver.

Network and routing layer: IPv6 + RPL

IPv6 provides IP addressing and routing once adapted by 6LoWPAN. RPL is the routing protocol designed for IoT networks.

RPL finds and maintains efficient paths in mesh networks despite losses and IoT constraints. It organizes the network as a loop-free directed graph called a DODAG (Destination Oriented Directed Acyclic Graph), typically rooted at a gateway.



Network and routing layer

UDP is used because it is a connectionless and lightweight protocol, making it particularly well-suited to the constraints of IoT. DTLS provides confidentiality, integrity, and authentication to applications above the transport layer.

In cases where a connection-oriented use is required, it is possible to use the TCP and TLS protocols, which secure client-server exchanges against eavesdropping or tampering.

6. Existing IPv6 based network technologies for IoT

Hint : List the existing IoT network technologies that are using IPv6 and their associated vertical(s) (application domain(s))

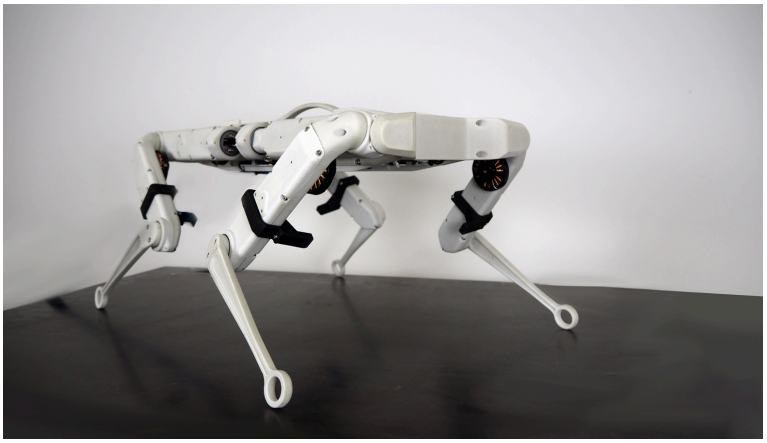
IoT protocols such as BLE, Zigbee, and NB-IoT are not natively based on IPv6, but they can integrate or support it through adaptation mechanisms suitable for constrained devices (e.g., 6LoWPAN).

IoT network technologies (IPv6)	Application domain
THREAD	Smart home / home automation
Bluetooth SMART	Personal devices / sensors / equipment
ZigBee®	Home automation, Energy management
NB-IoT™	Smart cities, Smart meters, Connected agriculture

7. Is an IPv6 based stack relevant for your semester project ?

Hint : After briefly describing your semester project, elaborate very shortly on the relevance of adopting IPv6 in your semester project.

Project (communication part):
The communication part of our project focuses on remotely controlling a quadruped robot (SOLO12). The robot is locally controlled by an FPGA, connected to a GSM module that provides the network link.



In our architecture, the robot initiates an outgoing connection to the cloud, and the control interface goes through the cloud. In this context, IPv6 does not necessarily provide a major benefit. However, IPv6 could become useful if we wanted to deploy a fleet of robots across multiple networks and manage large-scale addressing and end-to-end connectivity more cleanly.

8. IoT and sustainability (Optional, even if recommended)

Hint : After watching the presentation referred below,

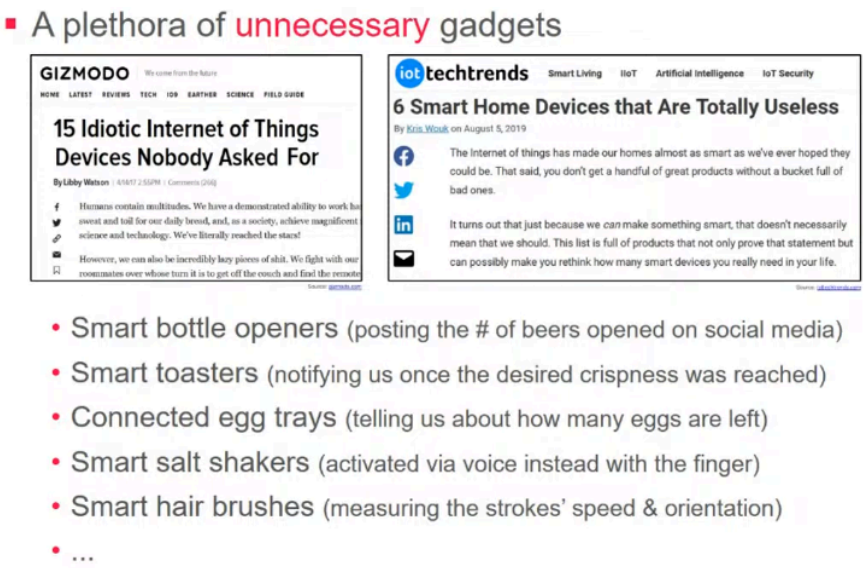
1. cite one of the United Nations' sustainable development goals, and briefly explain how IoT can help in achieving it ?

The video highlights several United Nations Sustainable Development Goals (SDGs), particularly Goal No. 11, which focuses on sustainable cities and communities. This goal aims to make cities safer, more resilient, and more sustainable.

Some IoT solutions developed in the field of smart cities can contribute effectively to this objective. In particular, they can reduce energy waste in buildings by controlling heating and air conditioning according to demand, optimize public lighting through smart illumination, improve waste management through sensor-triggered collections, ease traffic flow for more efficient and less polluting transportation, and monitor air quality to help municipalities make informed decisions.

2. What are the main guidelines promoted by the presenter to design a sustainable IoT device/product?

The video presents several best practices for designing a sustainable IoT product. It notably emphasizes the importance of designing devices that are truly useful, avoiding the creation and production of unnecessary gadgets, and prioritizing real societal value.



It also recommends designing products in a way that facilitates recycling, for example by optimizing their ease of disassembly.

- Often hard to correctly dispose of IoT devices
  - Design flaw: not keeping recycling in mind
  - Electronics is hidden into an everyday object
  - Batteries hidden in the device
    (often not replaceable / hard to remove)

Supporting software updates is also essential: integrating update capabilities makes it possible to add new features, fix bugs, and improve performance over time.

Ability to keep IoT Devices up-to-date

- Many devices do not support any over-the-air firmware update capability
  - Cannot cope with changing customer demands

Finally, the video stresses the need to ensure the robustness and longevity of devices, and to avoid making them dependent on a single cloud service. If a company ceases operations or shuts down the service, the device could otherwise become unusable.

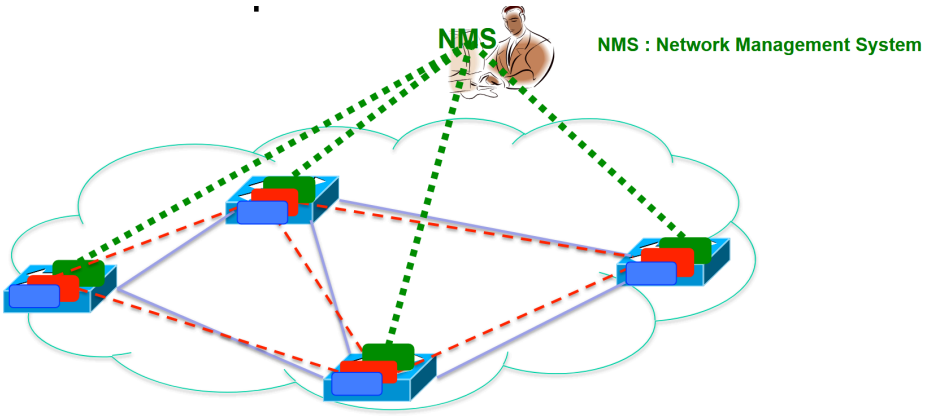
Title : The IoT and the two sides of Sustainability, 2023
Presenter : Carlo Boano, University of Graz, Austria

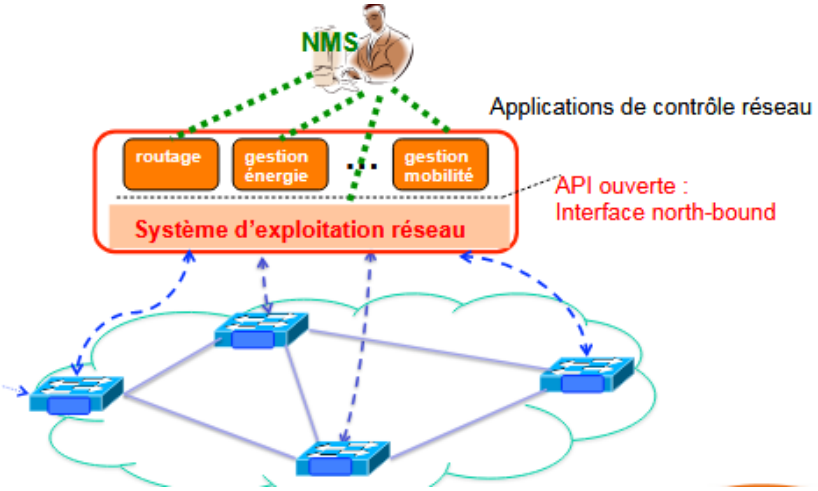
link to video : https://www.youtube.com/live/Sf70-Nb_hNI
Abstract : IoT systems are often portrayed as a key driver for sustainability and as an essential technology to achieve many of the seventeen United Nations' sustainable development goals by 2030. Among others, IoT systems can help improving health and well-being, building smart cities, promoting a responsible production and consumption, increasing awareness and visibility into energy and resource usage, as well as facilitating access to clean energy. At the same time, sustainability is often not a concern during the design of an IoT system: several IoT gadgets are unnecessary, many IoT products become quickly obsolete, and poorly-performing IoT devices are quickly dismissed. As a result, IoT hardware often ends up as e-waste into landfill after a very short lifespan, which is worrying considering the magnitude of IoT devices expected in the next decade. In this talk, I will illustrate this paradox with concrete examples and highlight the need to maximize the usability and lifetime of IoT systems, presenting technical solutions that could help in this regard

9. What makes SDN different from legacy computer networks ? What are the appealing opportunities that it paves the way for ? What are its main challenges ?

Hint : Shortly, list the SDN principles that do not hold for legacy computer networks. Briefly, elaborate on these principles to sketch some of the opportunities that SDN brings.

In legacy networks, each device embeds both the control plane and the data plane. SDN introduces an architecture in which the control plane is decoupled from the data plane and made programmable.





With SDN, the control logic is extracted from network devices and centralized in a controller. The devices mainly become forwarding elements responsible for packet routing. In contrast, in a legacy architecture, control and forwarding functions are tightly coupled within each device.

SDN makes the network directly programmable: applications interact with the controller via APIs, and the controller drives the network devices through control interfaces. SDN notably enables forwarding management using match/action rules (as seen in lab sessions), thus providing very fine-grained traffic control.

As a result, SDN simplifies network management operations, since it is no longer necessary to intervene directly on each device: configuration and control are performed through network software. It also enables greater network automation, the use of simpler devices with minimal embedded software, better interoperability between devices, and greater flexibility of network infrastructures.

10. What does NFV (Network Function Virtualization) stand for ? What are the opportunities that it paves the way for ?

NFV consists in virtualizing network functions by implementing them as independent software modules. These functions are no longer executed on dedicated proprietary hardware devices, but on standard servers within virtual machines or containers.

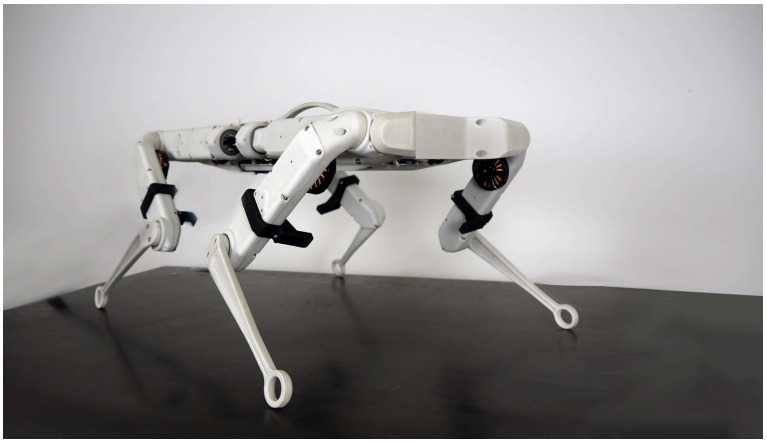
This approach brings two major benefits. First, it significantly improves network flexibility and agility: it becomes possible to modify system behavior simply through software deployment or updates, without changing the hardware. It also allows dynamic adjustment of resources according to demand and load, by increasing or decreasing the number of instances.

Second, NFV helps reduce costs, simplifies operations, and facilitates automation, while offering better economies of scale thanks to resource pooling and the use of standard hardware.

11. Are SDN and/or NFV relevant for your semester project ? If not, choose one of the assignments below ?

Hint : After briefly describing your semester project, elaborate very shortly on the relevance of adopting SDN and/or NFV in your semester project. Alternatively, choose one of the papers below, which propose some concrete applications of SDN/NFV in the IoT context. Read the recommended sections and answer the corresponding questions.
Brief project description (communication part):

The communication part of our project focuses on the remote control of a quadruped robot (SOLO12). The robot is locally controlled by an FPGA, to which a GSM module is connected to provide network connectivity.



In our project, NFV can be relevant because we have a “cloud” component that could host virtualized network functions around robot/cloud communication.

For example, to secure communications, one could deploy in the cloud a software function acting as a VPN and/or filtering service to secure access to the robot and limit its exposure.