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.*

IoT networks, particularly LP-WPAN, are characterized by low power consumption, limited bandwidth (20-250 kbps), and reduced range (a few tens of meters). They prioritize energy efficiency and low-data-rate communications, with devices constrained in processing power and memory. IoT networks often use dynamic topologies and multi-hop communication, while addressing challenges such as security, interoperability, and interference in diverse environments.

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.).*

Adopting an IP-based architecture in IoT systems is beneficial because it allows devices to connect globally and communicate seamlessly over the internet. It ensures that devices from different manufacturers can work together through standardized protocols. With IPv6, it also supports a large number of devices, making the system scalable for future growth. Additionally, it enables direct communication between devices without needing intermediaries, making it an ideal choice for modern and large-scale IoT projects.

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.

Based on TD1, a host follows these initialization steps when switched on in an IPv6 network:

1. **Link-Local Address Configuration:**
   - Upon activation, the network interface (eth0) assigns a link-local address automatically
   - This process uses SLAAC. The link-local address is derived from the device's MAC address using the EUI-64 format
   - Purpose : to ensure that the device has a unique address for communication within the same local link without requiring a router
2. **Duplicate Address Detection (DAD):**
   - The host performs DAD to ensure that its link-local address is unique on the network
   - Message used: Neighbor Solicitation (NS) and Neighbor Advertisement (NA), sent to the multicast group
   - Purpose: To prevent address conflicts in the network
3. **Router Discovery and Global Unicast Address Configuration:**
   - The host sends Router Solicitation (RS) messages to the multicast address to discover an IPv6 router
   - The router responds with Router Advertisement (RA) messages, which provide network configuration details, including the network prefix and other settings
   - The host uses this information to configure its global unicast address
4. **Neighbor Discovery Protocol (NDP):**
   - The host maintains a table of neighbors' link-layer addresses via NDP
   - Purpose: Facilitates IPv6-to-MAC address resolution, replacing ARP from IPv4
   - Message Types: NS and NA messages

IPv6 has specific requirements for both the network and hosts to ensure proper functionality. The network must support multicast for Neighbor Discovery (NDP) and Router Advertisements (RA), handle larger headers due to the extended IPv6 address format, and ensure transmission reliability for Duplicate Address Detection (DAD) and NDP to work effectively. Hosts must support automatic address configuration and respond to periodic Router Solicitation (RS) and RA updates. Key features of IPv6 include a 128-bit address space, stateless (SLAAC) and stateful (DHCPv6) address configuration, enhanced security through mandatory IPsec, and multicast support, which is crucial for efficient IoT communication.

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.

To enable IPv6 in IoT environments, optimizations such as 6LoWPAN (header compression, fragmentation, and adaptation for IEEE 802.15.4) and RPL (efficient multi-hop routing, multipoint-to-point support, and energy-based routing optimization) have been implemented. These adaptations enhance energy efficiency, reduce unnecessary transmissions, and improve security with lightweight IPsec and DTLS. The goal is to ensure IPv6 compatibility, scalability, and efficient operation in resource-constrained IoT networks.

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.

The IETF proposed IoT protocol stack is designed for resource-constrained devices and low-power networks. It includes several layers:

- Physical and Data Link Layers: They handle the transmission of data over physical media, such as through IEEE 802.15.4 (used in Zigbee, 6LoWPAN).
- Network Layer: It uses 6LoWPAN for IPv6 transmission over low-power networks and RPL for efficient routing in low-power, lossy networks.
- Transport Layer: Protocols like COAP and UDP ensure lightweight, low-overhead communication suited for IoT environments.
- Application Layer: The Constrained Application Protocol (CoAP) enables efficient communication for M2M interactions in constrained devices, offering request-response and observation capabilities.

The proposed application level protocols :

- COAP: Lightweight, request-response protocol for constrained devices, optimized for low-power networks.
- MQTT: Publish/subscribe messaging protocol, efficient in low-bandwidth and high-latency environments.
- XMPP: XML-based protocol for real-time messaging and presence, suitable for IoT communication.

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))

Several IoT network technologies use IPv6 :

IoT network technologies	Application domains
6LoWPAN	Smart homes, healthcare, agriculture, industrial IoT
Zigbee	Smart homes, healthcare, agriculture, industrial IoT
LoRaWAN	Smart cities, agriculture, asset tracking
NB-IoT	Smart cities, healthcare, utilities
LTE-M	Fleet management, healthcare, smart cities
Thread	Smart homes, building automation, healthcare
Bluetooth 5	Smart homes, healthcare, retail
Wi-Fi	Smart homes, healthcare, retail applications
RPMA	Smart agriculture, smart cities, asset tracking

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.

My semester project with ACTIA focuses on using Ultra-Wideband (UWB) technology for secure car access with a key. The key uses UWB to precisely determine the user's position relative to the vehicle, enabling seamless unlocking and starting of the car.
The objectives are :

1. Positioning the user based on UWB antenna locations: The goal is to determine the user's position in relation to the car by using the locations of UWB antennas placed around the vehicle.
2. System limit testing: The system will be tested to evaluate its performance under different conditions, focusing on accuracy, range, and reliability in real-world environments.

Adopting IPv6 in my project is essential for scalable and secure communication between the UWB key and the car system. Its vast address space allows unique identification of devices, while built-in security features like IPsec ensure safe data transmission. IPv6 enhances the project's scalability, security, and future-proofing.