INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
TOULOUSE

INNOVATIVE SMART SYSTEMS

An insight into Internet based technologies and protocols for Wirelessly connected things report

Diani Badr
5 ISS
2024/2025

Table of content

Introduction

The Internet of Things (IoT) is transforming our interaction with connected objects through low-power wireless networks and advanced communication protocols. To ensure the scalability, security, and energy efficiency of these systems, network architecture plays a key role, and the adoption of IPv6 emerges as an essential solution due to its vast address space and features tailored to IoT network constraints. This report explores the specificities of IoT networks, their differences from traditional computer networks, and the technical challenges they pose, particularly in terms of reliability, energy management, and latency. It also analyzes the benefits of an IPv6-based architecture, its adaptations for low-power networks such as 6LoWPAN and RPL, and its role in optimizing performance and security in IoT communications. Finally, it examines the impact of IoT technologies on sustainable development and their contribution to the United Nations' objectives.

1. IoT network characteristics and specificities

1.1. Characteristics of IoT Networks

IoT networks, such as Low-Power Wireless Personal Area Networks (LP-WPANs), stand out due to several unique features. First, they employ flexible topologies like star or mesh, enabling robust and adaptable connectivity based on coverage needs. These networks are optimized for low energy consumption, as devices often operate on batteries or limited power sources, making them ideal for applications requiring long autonomy. Additionally, their range is generally limited to reduce costs and conserve energy. They are also designed to be cost-effective, featuring simple devices that encourage large-scale adoption. Finally, their architecture simplifies the integration of new devices, while mesh networks provide self-maintenance in the event of local failures.

1.2. Differences with Conventional Computer Networks

IoT networks differ significantly from conventional computer networks due to their constraints and specific use cases. Unlike traditional networks, IoT devices have limited resources, such as processing power, memory, and storage, restricting their ability to handle complex data flows. These networks also exhibit increased security vulnerabilities, as their resource limitations prevent the implementation of sophisticated security protocols. Moreover, the transmission speed of LP-WPANs is slower since these networks prioritize energy efficiency over performance. IoT networks are heavily influenced by environmental factors, such as electromagnetic interference or physical obstacles, which can compromise their efficiency. Lastly, unlike traditional networks that manage complex applications, IoT networks focus primarily on simple data collected from sensors or sent to actuators.

1.3. Specific Constraints of IoT Networks

IoT networks face several specific constraints that affect their performance and usability. Reliability is a critical challenge, as these networks must maintain stable communication even in disrupted environments or when certain nodes fail. Managing delays and latency is also crucial, especially for critical applications like healthcare or industrial processes, where delays can have serious consequences. Energy consumption is a central constraint, requiring a balance between device autonomy and network performance. Additionally, the network's capacity to support a large number of devices while ensuring optimal quality of service is a constant challenge. These constraints demand innovative technical solutions to maximize the benefits of IoT networks while mitigating their limitations.

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

Adopting an IPv6-based architecture in an IoT system offers several benefits, especially for connected objects like sensors and other low-power devices.

Key Benefits of IPv6 in IoT Systems

- **Scalability with a Large Address Space**: IPv6 provides a vast address space (128-bit addresses), which is critical for accommodating the billions of devices expected in IoT ecosystems.
- **Address Auto-Configuration**: IPv6 supports automatic address configuration (stateless or stateful). This eliminates the need for manual configuration, which is ideal for large-scale deployments of IoT devices.
- **Efficient Routing and Communication**: IPv6 enhances routing efficiency with hierarchical address allocations and supports neighbor discovery, reducing the overhead in communication protocols like ARP.
- **Support for Low-Power and Lossy Networks (6LoWPAN)**: IPv6 integrates with 6LoWPAN, enabling it to operate efficiently over low-power wireless personal area networks (WPANs). This feature is vital for IoT systems where energy efficiency is critical.
- **Global Reachability**: IPv6 enables devices to communicate directly over the internet using globally unique addresses, facilitating seamless integration of IoT devices into broader networks.
- **Improved Security Features**: IPv6 inherently supports IPsec for secure communication, ensuring data integrity, confidentiality, and authentication—key requirements for sensitive IoT data.
- **Mobility Support**: IPv6 provides better mobility support through features like Mobile IPv6, allowing devices to move across networks without losing connectivity.
- **Energy Efficiency**: Protocols like 6LoWPAN and RPL (Routing Protocol for Low-power and Lossy Networks) are designed to work with IPv6 to optimize energy consumption in IoT environments.
- **Seamless Integration with Modern Network Infrastructure**: Many modern networks are transitioning to IPv6, making it easier for IoT devices to integrate into existing systems without additional translation or adaptation layers.
- **Support for Multi-Hop Communication**: IPv6 is well-suited for multi-hop networks, which are common in IoT applications. Protocols like RPL optimize routing in these scenarios, ensuring reliability and efficiency.

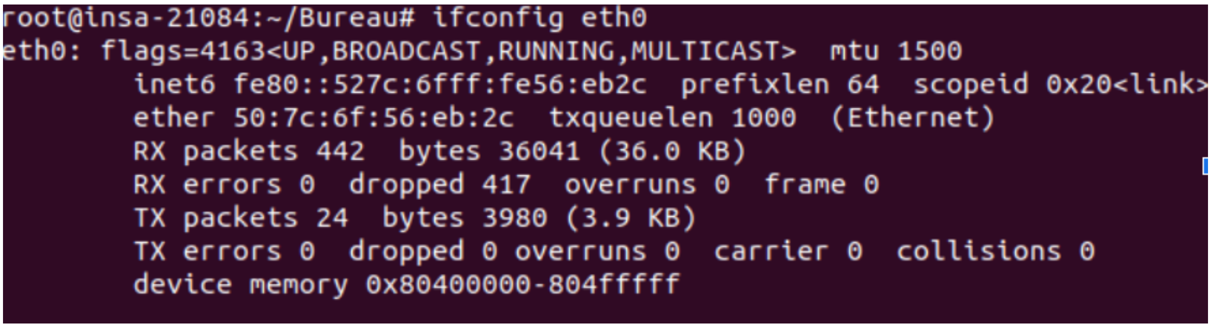
In summary, adopting IPv6 for IoT systems addresses critical challenges related to scalability, efficiency, security, and integration, ensuring the architecture is future-proof and capable of supporting diverse IoT applications.

3. IPv6 basics

3.1. Description of IPv6 Initialization Steps

a. Link-local Address Auto-configuration:

When a host's network interface (e.g., eth0) is activated using commands like ifconfig eth0 up or ip link set dev eth0 up, it automatically assigns a link-local IPv6 address within the fe80::/10 range. To ensure the uniqueness of this address on the local link, the host performs Duplicate Address Detection (DAD) by sending Neighbor Solicitation (NS) ICMPv6 messages to the multicast address ff02::1:ffXX:XXXX corresponding to the potential address. If no conflicts are detected, the address is confirmed, enabling local link communication without the need for a router or manual configuration. This process involves the exchange of NS and Neighbor Advertisement (NA) messages.



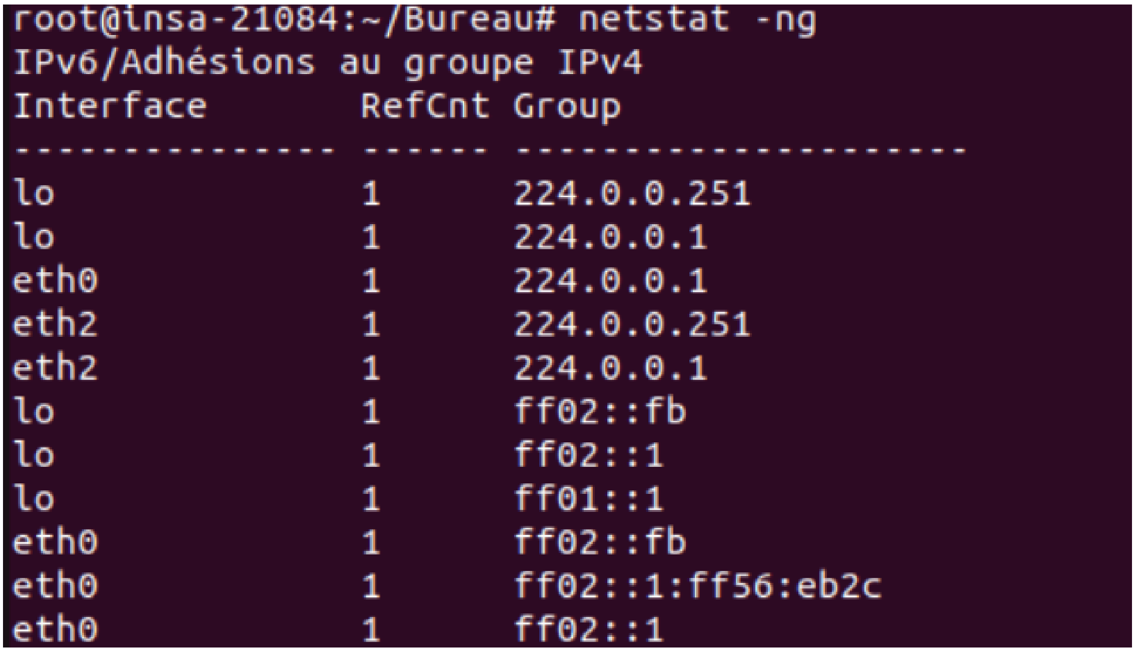
```
root@insa-21084:~/Bureau# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::527c:6fff:fe56:eb2c  prefixlen 64  scopeid 0x20<link>
        ether 50:7c:6f:56:eb:2c  txqueuelen 1000  (Ethernet)
        RX packets 442  bytes 36041 (36.0 KB)
        RX errors 0  dropped 417  overruns 0  frame 0
        TX packets 24  bytes 3980 (3.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x80400000-804fffff
```

b. Global Unicast Address Configuration:

To configure a global unicast address, the host sends Router Solicitation (RS) ICMPv6 messages to the multicast address `ff02::2`, requesting network configuration details. Routers respond with Router Advertisement (RA) messages, providing the necessary network prefix and optional DNS settings. The host then combines the received network prefix with its Interface Identifier, often derived from its MAC address, to generate a global unicast address. This automated process minimizes human intervention and ensures scalability for large networks by using RS and RA messages to streamline configuration.

c. Multicast Group Subscription:

By default, the host subscribes to several multicast groups, such as `ff02::1` (all nodes) and `ff02::2` (all routers), using Multicast Listener Discovery (MLD) messages. This subscription enables efficient network communication and device discovery by targeting specific groups of devices, eliminating the need for resource-intensive broadcasting to all devices on the network.



```
root@insa-21084:~/Bureau# netstat -ng
IPv6/Adhésions au groupe IPv4
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      224.0.0.251
lo              1      224.0.0.1
eth0            1      224.0.0.1
eth2            1      224.0.0.251
eth2            1      224.0.0.1
lo              1      ff02::fb
lo              1      ff02::1
lo              1      ff01::1
eth0            1      ff02::fb
eth0            1      ff02::1:ff56:eb2c
eth0            1      ff02::1
```

d. Neighbor Discovery Protocol (NDP):

IPv6 resolves addresses to MAC addresses using Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages, functioning similarly to the Address Resolution Protocol (ARP) in IPv4. This mechanism ensures that devices can discover each other and establish communication at the link layer, facilitating seamless connectivity within the network.

3.2. Requirements and Characteristics of IPv6

a. Requirements:

- IPv6 transmission relies on specific network capabilities to function efficiently. The underlying network must support multicast communication to enable processes such as Router Advertisements and Neighbor Discovery, ensuring targeted and efficient message delivery. Additionally, IPv6 requires a minimum Maximum Transmission Unit (MTU) of 1280 bytes for packet transmission, ensuring compatibility across diverse network segments. Support for ICMPv6 is also critical, as it facilitates essential functions like Duplicate Address Detection (DAD) and error reporting, which are integral to maintaining network stability and address uniqueness.

- Host availability is another important requirement in an IPv6 network. Devices must remain active to respond promptly to Neighbor Solicitations, ensuring continuous connectivity and address resolution. Moreover, hosts must support both stateless and stateful address configurations to adapt to dynamic networks, allowing seamless integration and automated configuration in environments with varying infrastructure and scale.

b. Key Characteristics:

- **Larger Address Space:** Supports 128-bit addresses, allowing virtually unlimited devices and efficient IoT deployment.
- **Built-in Security:** IPv6 includes IPsec as a mandatory feature for end-to-end encryption and data integrity.
- **Efficient Routing:** Simplified header structure and hierarchical addressing improve routing efficiency.
- **Autoconfiguration:** Supports both Stateless Address Autoconfiguration (SLAAC) and DHCPv6, reducing administrative overhead.
- **Improved Multicasting:** Eliminates IPv4's broadcast mechanism, using multicast for targeted communication.

c. Compatibility with IoT:

IPv6 is highly compatible with IoT due to its vast address space, which can accommodate billions of devices with unique identifiers, enabling large-scale deployments. It also supports efficient communication methods, such as multicast and anycast, which are essential for IoT devices operating in constrained environments by minimizing bandwidth usage and optimizing message delivery. However, IPv6 presents challenges, such as the need for a robust infrastructure to support multicast and comply with the minimum MTU requirements. Additionally, resource-constrained IoT devices may face increased processing and memory demands to handle the protocol's features and functionality.

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

4.1. Additions and Adjustments:

- **6LoWPAN :** 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is designed to enable the efficient use of IPv6 in low-bandwidth IoT networks. It achieves this through header compression, which significantly reduces the size of IPv6 headers to minimize overhead, making it suitable for constrained devices. Additionally, 6LoWPAN supports fragmentation and reassembly of IPv6 packets to accommodate the smaller Maximum Transmission Unit (MTU) of IoT networks, such as those based on IEEE 802.15.4. Furthermore, it simplifies IPv6 address assignment using address autoconfiguration, which is particularly beneficial for resource-limited devices and ensures seamless communication with link-local and private addresses.

- **RPL:** RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) leverages a Destination-Oriented Directed Acyclic Graph (DODAG) to create efficient routing topologies tailored for IoT networks. It supports diverse communication patterns, including multi-point-to-point, point-to-multi-point, and point-to-point, making it ideal for IoT's dynamic traffic requirements. Designed for energy efficiency, RPL minimizes control message overhead, reducing power consumption and enabling its use in battery-powered devices. Its adaptability to various traffic patterns, particularly multipoint-to-point communication common in sensing applications, ensures reliable and optimized routing in low-power and lossy network environments.

- **Link-Layer Adjustments:** IPv6 has been adapted to seamlessly integrate with low-power wireless networks through compatibility with the IEEE 802.15.4 standard, which is commonly used in IoT environments. This integration ensures that IPv6 can function effectively on networks with constrained resources by leveraging short-range, low-power radio interfaces optimized for IoT. These adjustments allow devices to communicate efficiently while minimizing energy consumption and addressing the limitations of bandwidth and processing power in such networks.

4.2. Optimizations

Optimizations in IPv6 for IoT networks focus on improving efficiency and performance in constrained environments. Compression mechanisms, including stateless and stateful address compression, significantly reduce IPv6 packet size, minimizing overhead in low-bandwidth networks. For resource-constrained devices, simplified neighbor discovery and routing functionalities are tailored to operate effectively within the limited processing power and memory of IoT devices. Additionally, traffic management is enhanced through the integration of the RPL protocol, which optimizes routing for diverse traffic patterns, reducing latency and ensuring reliable communication in IoT applications. These optimizations collectively enable IPv6 to function seamlessly in low-power and lossy network conditions.

5. The IETF IPv6 based stack for IoT

The IETF (Internet Engineering Task Force) has developed a protocol stack specifically designed for IoT to ensure seamless communication in constrained environments, leveraging IPv6 as the foundation.

5.1. Main Network Functions of New Layers

Each of the new layers in this stack performs specific network functions:

6LoWPAN (Adaptation Layer)

- **IPv6 Header Compression**: Reduces overhead by compressing redundant IPv6 fields.
- **Packet Fragmentation & Reassembly**: Ensures IPv6 packets can be transmitted over IEEE 802.15.4 networks.
- **Efficient Neighbor Discovery**: Adapts IPv6 NDP to support sleepy nodes.

RPL (Routing Layer)

- **DODAG Construction**: Builds multi-hop routes in Low-Power Lossy Networks (LLNs).
- **Objective Functions**: Determines best paths based on link quality, energy, etc.
- **Routing Tables Optimization**: Stores minimal routing information to reduce memory usage.

Application Layer Protocols

- **CoAP**: Designed for constrained devices with a simple request/response model, supporting retransmissions for reliability.
- **MQTT**: Uses a broker-based publish/subscribe model for efficient IoT communication.
- **HTTP**: Used when web integration is necessary.

5.2. Key Network Functions of the New Layers

6LoWPAN (Adaptation Layer)

- Compresses IPv6 headers for efficient transmission.
- Manages fragmentation of large IPv6 packets to fit in IEEE 802.15.4 frames.

RPL (Routing Layer)

- Creates a topology suitable for low-power and lossy networks.
- Uses Directed Acyclic Graphs (DAGs) for hierarchical routing.
- Supports three modes: storing, non-storing, and hybrid to optimize routing memory and processing.

CoAP (Application Layer)

- Enables constrained devices to communicate efficiently.
- Uses a request-response model similar to HTTP.
- Works over UDP, reducing overhead and power consumption.

MQTT (Application Layer)

- Uses a publish-subscribe model, suitable for real-time and event-driven communication.
- Designed for minimal bandwidth and low power consumption.
- Commonly used in IoT scenarios such as smart homes and industrial monitoring.

6. Existing IPv6 based network technologies for IoT

This table lists the existing IoT network technologies that use IPv6, along with their associated application domains.

IPv6-based IoT Network Technology	Description	Application Domains
6LoWPAN	Enables IPv6 over low-power wireless networks (IEEE 802.15.4)	Smart Homes, Smart Cities, Industrial IoT, Healthcare
IPv6 over BLE	Allows Bluetooth Low Energy (BLE) devices to use IPv6	Smart Homes, Healthcare, Industrial IoT
Thread	IPv6-based mesh networking protocol for smart homes	Smart Homes, Smart Buildings
NB-IoT	Cellular LPWAN technology optimized for IoT applications	Smart Cities, Smart Agriculture, Asset Tracking
LTE-M	Cellular IoT technology supporting IPv6, optimized for mobility	Smart Transportation, Healthcare, Smart Agriculture
LoRaWAN with IPv6	LoRaWAN with SCHC enables IPv6 communication	Smart Agriculture, Smart Cities, Industrial IoT
5G	5G supports native IPv6 addressing for ultra-reliable IoT	Smart Manufacturing, Smart Cities, Healthcare

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

7.1. Description of our semester project
Our semester project, "Shared Access for Family Electrically-Assisted Tricycle", explores the integration of Ultra Wideband (UWB) technology for secure and intelligent vehicle access. In collaboration with Actia and NXP, our main objective was to characterize a UWB positioning system for keyless entry. Through real-world testing with different antenna configurations, we measured positioning accuracy and optimized triangulation algorithms. The results demonstrated that UWB provides reliable localization with centimeter-level precision, surpassing existing technologies such as Bluetooth and GPS.

7.2. Adoption of IPv6 in our semester project
L'adoption de l'IPv6 dans notre projet de semestre est pertinente pour améliorer l'évolutivité, la sécurité et la connectivité des systèmes d'accès aux véhicules basés sur l'UWB. Grâce à son espace d'adressage étendu, IPv6 permet l'intégration fluide de plusieurs dispositifs connectés, tels que les ancres UWB et les modules de communication des véhicules, assurant ainsi une expansion future sans contrainte. De plus, les fonctionnalités de sécurité intégrées, notamment IPsec, renforcent l'authentification et le chiffrement, offrant une meilleure protection contre les cybermenaces. En outre, les capacités de multidiffusion améliorées optimisent la transmission des données en temps réel entre les composants du véhicule, garantissant une gestion efficace du positionnement et du contrôle d'accès. L'utilisation de l'IPv6 permet ainsi de soutenir les applications IoT avancées, le diagnostic à distance et les mises à jour sécurisées, rendant notre système plus robuste et adaptable aux solutions de mobilité intelligente.

8. IoT and sustainability

8.1. One of the United Nations' Sustainable Development Goals and How IoT Can Help Achieve It

One of the United Nations' Sustainable Development Goals (SDGs) is Sustainable Cities and Communities. This goal aims to make cities more inclusive, safe, resilient, and sustainable.

IoT can play a crucial role in achieving this goal by optimizing urban infrastructure and reducing waste. For example:

- **Smart Traffic Management:** IoT-enabled sensors and AI-based traffic monitoring systems can optimize road traffic, reducing congestion and lowering CO2 emissions.
- **Energy-efficient Buildings:** IoT can regulate heating, cooling, and lighting based on real-time occupancy, reducing energy consumption.
- **Smart Waste Management:** IoT sensors in trash bins can notify waste collection services when bins are full, improving efficiency and reducing unnecessary fuel usage.
- **Air Quality Monitoring:** IoT devices can continuously track pollution levels, providing data for better urban planning and response strategies.

These applications contribute to reducing the environmental impact of cities while improving the quality of life for residents.

8.2. Main Guidelines to Design a Sustainable IoT Device/Product

The presenter emphasized several key guidelines for designing sustainable IoT devices to reduce e-waste and ensure long-lasting, efficient solutions:

- **Design Useful Devices:** Prioritize IoT solutions that serve meaningful purposes and contribute to societal benefits, rather than creating unnecessary gadgets.
- **Enable Easy Recycling:** Ensure that the components (electronics, batteries, etc.) can be easily separated and disposed of properly.
- **Implement Over-the-Air (OTA) Firmware Updates:** Allow remote software updates to fix security vulnerabilities, enhance performance, and extend device lifespan.
- **Ensure Robustness and Reliability:** Use adaptive networking protocols to minimize interference and maintain reliable communication, preventing devices from becoming obsolete too soon.
- **Avoid Hardcoded Dependencies on Cloud Services:** Design devices that can function even if the cloud service provider shuts down, preventing sudden obsolescence.
- **Minimize the Need for Additional Gateways:** Use **Cross-Technology Communication (CTC)** to allow direct communication between different IoT devices without requiring extra hardware.
- **Use Energy Harvesting Technologies:** Reduce reliance on batteries by designing devices that can harvest energy from the environment, such as solar or kinetic energy.

Conclusion

The Internet of Things (IoT) is revolutionizing communications and automation by leveraging wireless networks optimized for low energy consumption. The adoption of IPv6 in these environments is essential to ensure scalability, security, and communication efficiency, particularly through protocols such as 6LoWPAN and RPL. Despite challenges related to energy constraints, reliability, and latency, technological advancements continue to optimize IoT network performance and facilitate large-scale integration.