DOI: 10.3969/j.issn.1673-5188.2016.01.009
http://www.cnki.net/kcms/detail/34.1294.TN.20151116.1025.002.html, published online November 16, 2015

A Software-Defined Approach to IoT Networking

Christian Jacquenet and Mohamed Boucadair
(France Telecom Orange, Cesson-Sévigné 35512, France)

Abstract

It is foreseen that the Internet of Things (IoT) will comprise billions of connected devices, and this will make the provisioning and operation of some IoT connectivity services more challenging. Indeed, IoT services are very different from legacy Internet services because of their dimensioning figures and also because IoT services differ dramatically in terms of nature and constraints. For example, IoT services often rely on energy and CPU-constrained sensor technologies, regardless of whether the service is for home automation, smart building, e-health, or power or water metering on a regional or national scale. Also, some IoT services, such as dynamic monitoring of biometric data, manipulation of sensitive information, and privacy needs to be safeguarded whenever this information is forwarded over the underlying IoT network infrastructure. This paper discusses how software-defined networking (SDN) can facilitate the deployment and operation of some advanced IoT services regardless of their nature or scope. SDN introduces a high degree of automation in service delivery and operation—from dynamic IoT service parameter exposure and negotiation to resource allocation, service fulfillment, and assurance. This paper does not argue that all IoT services must adopt SDN. Rather, it is left to the discretion of operators to decide which IoT services can best leverage SDN capabilities. This paper only discusses managed IoT services, i.e., services that are operated by a service provider.

Keywords

automation; dynamic service provisioning; Internet of Things; service function chaining; software-defined networking

1 Introduction

The Internet of Things (IoT) is a highly constrained, much larger networking infrastructure than legacy infrastructures that operators have known for decades. It is predicted there will be tens of billions of connected objects in the future, and IoT will be the de facto networking infrastructure for a plethora of emerging services [1]. Some of these services are seen by many operators as key business development opportunities that need to be further explored or industrialized. Some IoT services are being deployed in the home and in dense urban environments. Other IoT services, such as e-health and energy distribution services, are being deployed on a regional, national or even interplanetary scale and require large-scale networking, computation, and storage.

IoT connectivity services rely on elementary functions such as forwarding and routing, quality of service (QoS), and security.

One of the main differences between IoT connectivity services and legacy connectivity services such as Internet access is the constrained nature of some of the technologies involved. For example, a wireless sensor network (WSN) deployed in an IEEE 802.15.4 [2] network environment assumes a maximum transmission unit (MTU) of 127 bytes, with only 80 bytes allocated to the MAC payload for an average 250 kbps rate.

A WSN includes sensors that are constrained in terms of CPU and energy. This can affect how IoT service-driven policies are designed and enforced, especially when the data being transported, e.g., personal biometric data, requires a high degree of privacy in the forwarding and routing schemes. In addition, IoT dimensioning figures suggest a very different, much larger networking scale. Several thousand connected devices, with or without route computation capabilities, are likely to be the norm rather than the exception in urban and regional areas and even nationwide (**Table 1**).

The design and operation of an IoT connectivity service is complicated by the inherent dynamics of the networking infrastructure. For example, connected devices may be rapidly (re) grafted onto or pruned from the IoT network infrastructure according to their CPU loads or remaining energy. They may also be (re)grafted onto or pruned from the IoT network infrastructure because they are in motion, e.g., biometric sensor bracelets [3], they have been damaged by weather, or they have entered sleep mode.

The deployment of a wide range of IoT services—from "smart home" residential services and automated building services to advanced personal e-health services—has become a

▼Table 1. What makes IoT routing special

Internet Routing	IoT Routing
Nodes are routers	Nodes can be anything—sensors, actuators, routers, etc.
A few hundred nodes per network	1000+ nodes per network, depending on the nature of the service
Links and nodes are stable over time	Links are highly unstable and degrade communication. Nodes fail more often, e.g., exhausted batteries and CPU overload
No stringent routing constraints	Highly constrained environment
Routing is by default not application-aware	Routing must be application-aware, e.g., e-health services generate traffic that requires a high degree of privacy whereas energy-distribution services generate traffic that primarily requires low-latency routes

key strategy for operators. Such IoT services open up tremendous opportunities for operators to develop their businesses. The simultaneous development of cloud infrastructures and the introduction of automation techniques for service delivery and operation will likely boost IoT services.

Operators see IoT services as a key factor affecting business development and existing network infrastructures, from both a design standpoint and operational standpoint. The introduction of several hundred or even thousands of connected devices will distort the global routing system and affect traffic forwarding in access infrastructures but must not jeopardize the quality of legacy services.

Such effects are not only assessed from a dimensioning perspective, i.e., moving from several hundred network devices to several thousand connected objects with computing resources, but also from a traffic taxonomy perspective. IoT services typically demand the ability to compute (traffic-engineered) paths that can accommodate privacy characteristics of traffic. IoT services also involve other considerations that lead to complex, likely multimetric, multiconstrained routing objective functions that differ from current routing policies based on the classical hop-by-hop forwarding scheme.

Also, cloud-based resources, such as IoT service platforms, also affect the way IoT services are designed and operated. Operators now need to have skills in IT/network convergence, which suggests that current service delivery and operational procedures may need to be revised. The evolution of organizational practices is further affected by the introduction of advanced cross-platform, cross-segment residential, e-health, urban and corporate IoT services. These inevitably create new challenges because they have specific functional capabilities.

Software-defined networking (SDN) enables flexible, robust, scalable design and operation of IoT services. This paper discusses an original approach in which SDN is not limited to dynamic IoT resource allocation. IoT-specific policy provisioning information is exchanged between the SDN computation logic and some of the IoT service functions involved in the delivery and operation of the IoT service.

The proposed approach has a much broader scope: it can be used to dynamically expose and negotiate the parameters of an IoT service, and it can be used to assess whether the IoT services that have been dynamically delivered comply with what has been negotiated with the IoT application or service customer. This global, systemic, software-defined IoT networking approach is unique.

This paper is organized as follows. The following section introduces two cases where the design and operation of the IoT service are complicated by dimensioning and the nature of the traffic generated. Then, the paper discusses the benefits of SDN to IoT service delivery and operation. Furthermore, it discusses the nature of the various SDN building blocks used in the IoT service delivery procedure—from dynamic IoT service parameter exposure and negotiation to IoT resource allocation and service fulfillment. The conclusion discusses what could be next for SDN-based IoT networking and what could be the role of network operators and service providers in this area.

2 Two Use Cases

Here we introduce two IoT services that are typically in the portfolio of a service provider. They are also prime examples of the complexity involved in smartly combining very different elementary capabilities, i.e., service functions that are usually supported by network elements. Besides basic forwarding capabilities, these services can usually manipulate privacy data, which often affects how connected devices dynamically compute and select routes to convey IoT traffic.

These cases create specific challenges in terms of scale but also in terms of QoS. Forwarding of biometric data collected by e-health sensors to the nearest hospital requires robust, low-latency routes whereas forwarding of power meter readings for billing purposes requires more reliable routes so that data does not need to be retransmitted.

The different routing objectives in the following two cases imply the need for an advanced, presumably multimetric route-computation logic that is not only fed specific service requirements and constraints but also proactively (or reactively) adapts to any event that may alter the network conditions in a deterministic, scalable manner. In this way, IoT services cannot be disrupted.

2.1 E-Health Services

A typical service that illustrates the challenges raised by IoT is e-health. In some contexts, e-health may require a network infrastructure that is highly reliable and preserves data integrity. Unlike some IoT services, where connected devices are only responsible for sending data, some e-health services may require traffic bi-directionality, perhaps for receiving check instructions and tweaking threshold settings.

In some e-health scenarios, monitoring a set of biometric data may involve dynamically computing routes for conveying data (collected by the sensors) to the nearest hospital when a threshold has been reached or selecting the hospital that can provide the most suitable specialist care. Given the sensitive nature of biometric data and the need to rapidly react to health emergencies, such as a heart attack, specific constraints should be overcome by the underlying forwarding and routing schemes.

These constraints can be overcome by dedicated traffic engineering, such as dynamic route computation, that takes into account not-so-usual routing metrics, such as the nature of the traffic, energy or CPU consumption of the communication device, or network bandwidth resources.

Also, there are typical seasonal epidemics, such as the winter flu, that need to be dynamically monitored on a regional or even national scale so that authorities can take appropriate ac-

tion (e.g., launch a vaccine campaign targeting people at risk).

Moreover, dynamic monitoring of an epidemic requires carefully designed traffic-forwarding policies adapted to manage mobile communities that process emergency calls and collect statistics on the importance, severity, and scope of the epidemic.

These two examples of e-health services create network challenges in terms of:

- reliable identification and efficient addressing and naming schemes for many connected devices (typically health sensors)
- dynamic, multimetric, self-adaptive route-computation schemes for service performance, scalability and robustness
- privacy preservation, so that sensitive data is not leaked to illegitimate nodes or data consumers
- dynamic mobility management and self-adaptive interconnected design schemes that leverage existing network infrastructure (both wired and wireless) for the sake of service-inferred traffic-forwarding policies.

Indeed, e-health services that dynamically monitor biometric data are available to users who may be mobile. As such, monitoring traffic-forwarding policies should be able to take advantage of available network infrastructures. Network interconnects may be needed to forward traffic upstream in the network or ensure that commands sent by an actuator connected somewhere on the Internet are reliably transmitted to the relevant connected devices. These network interconnects should be able to accommodate various kinds of IoT traffic envelopes and ensure such traffic can coexist with other types of traffic in order to minimize the risk of service disruption.

Self-adaptation can then be implemented according to the nature of the service to be delivered and the subsequent resource allocation decisions, e.g., route computation and bandwidth reservation.

2.2 Energy Management and Distribution

Dynamic management of energy distribution is another area where large-scale IoT might be used. Data collected from power meters is forwarded to metro agencies (perhaps for billing) but also contributes to the management of energy distribution during peak seasons, such as winter.

Forwarding the corresponding traffic requires capillary and WSNs that are connected with metropolitan and core networks (assuming both wired and wireless infrastructures).

Because of the nature of this traffic, adequate traffic engineering policies have to be enforced. This ensures that the computed paths will not only accommodate the type and amount of available resources but also the typical traffic patterns—e.g., N:1 or P:1 group communication schemes as a function of traffic directionality; sensor-collected data forwarded to metro, regional, or national energy control centers; or commands generated by an energy-control center and forwarded to a group of sensors so that energy consumption can be better regulated.

This use case involves additional challenges besides those already mentioned for the deployment of robust e-health services. These challenges are related to:

- designing and dynamically enforcing multicast/broadcast traffic engineering policies on a large scale
- assessing the effect of corresponding traffic growth on the performance and scalability of core networking infrastructures from both a design and operation perspective. This results in the development of adapted traffic-forwarding paradigms.
- dynamically managing available bandwidth resources, such as radio channels in 802.15.4e environments.

3 Software-Defined Networking Can Help

The nature of some of IoT services encourages operators to be particularly flexible and agile during the service-delivery and operation phases. Some capabilities, such as firewall, that are needed to create, deliver, and maintain a feature of an IoT service may be hosted in various platforms typically located in a cloud infrastructure. Other capabilities, such as traffic forwarding and QoS, may be supported by in-network nodes such as dedicated service cards or devices with dedicated hardware.

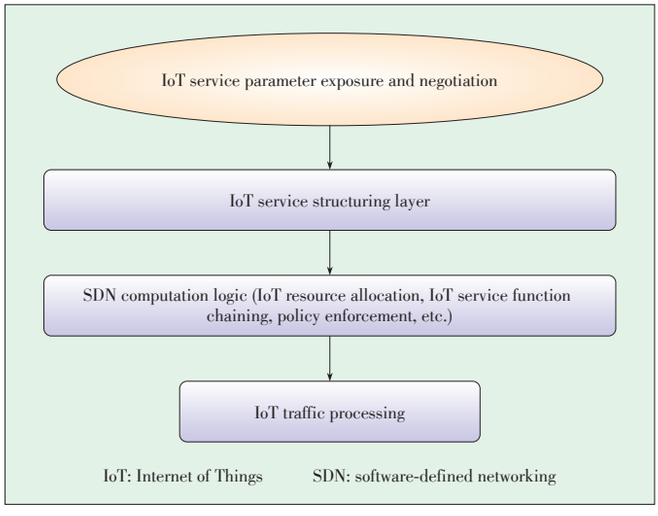
Selection of capabilities needed to dynamically orchestrate and deliver an IoT service therefore benefits from the flexibility of cloud-hosted service platforms and applications coupled with SDN techniques [4] that include dynamic service-inferred IoT resource allocation and policy enforcement as well as feedback mechanisms for IoT service fulfillment and assurance.

In recent years, SDN-related activities have mostly centered on how a logically centralized SDN computation logic, often designated as an SDN controller or orchestrator, can provide network devices with configuration information pertaining to the various features required to deliver a (connectivity) service.

Also recently, the application of SDN to IoT networking has been investigated [5], [6]. However, the focus has primarily been on dynamically enforcing a traffic-forwarding policy within an IoT network infrastructure according to abstract models and virtualized functions.

SDN combined with network function virtualization (NFV) and mass data analytics is a promising option for introducing high-degree automation into the overall IoT service-delivery procedure (**Fig. 1**)—from dynamic exposure and negotiation of IoT service parameters to resource allocation, policy enforcement, and service fulfillment and assurance.

Mass data analytics is required to optimize data aggregation and interpretation. SDN and data analytics can be used together to react to specific events and observed behaviors of the IoT underlying infrastructure. For example, they can be used to propose automated forwarding behaviors when there is an overload or failure. SDN and data analytics can also be used to offload some functions from the sensors and mediation servers



▲Figure 1. IoT service delivery procedure.

while meeting real-time requirements of data processes required by some IoT services. Because time synchronization is critical for some data retrieval, SDN can be used to synchronize the clocks of involved nodes.

With NFV techniques, SDN can instantiate new IoT controllers and concentrators whenever required and wherever they are located in the transport network. In this way, data received from connected devices can be handled appropriately. The location and dimensioning of these controllers are automatically fed by SDN intelligence, which is based on various service-specific criteria that reflect the business guidelines of the IoT service provider.

An SDN platform can be used to manage one or more IoT services. Whether one or several SDN controllers are required in a given network depends on the deployment strategy, which has to take into account the number, nature, and scope of the IoT services to be delivered. Although the application of SDN techniques to IoT services is attractive, the approach discussed in this paper does not necessarily benefit each and every IoT service. Rather, we suggest that a software-defined approach to IoT networking is primarily beneficial for IoT services that require sophisticated treatment and processing.

Sensors are no longer application-dependent and can be customized for an application. SDN can significantly help customize involved nodes at large to accommodate the design requirements of an IoT service portfolio, from smart home automation to advanced e-health or energy distribution services.

Structurally, IoT services often rely on complex, multifunctional network architectures that involve on-field hardware with embedded software, connectivity distributed systems, cloud software components, and third-party developers. Related challenges include: constrained resources, occasional massive amounts of signaling information, queries, and reduced computational resources. A typical IoT network of several thousand nodes (Table 1) requires new data processing schemes, stream processing, filtering, aggregation, and data mining.

4 IoT-Adapted SDN Mechanics

4.1 Dynamically Exposing and Negotiating IoT Service Parameters

An IoT connectivity service parameter (standard) template can be used for the dynamic negotiation procedure between a customer and IoT service provider [7]. In a biometric data-monitoring service that typically demands very low latency and privacy-preserving routes, such a template would include clauses about:

- sensor geolocation information, so that the SDN can find the most suitable routes to the nearest dispatch emergency center in a reliable and secure manner
- communication schemes and traffic patterns, e.g., a typical 1:N hose model where commands to collect biometric data during a daily duty cycle can be sent to *N* sensor bracelets from a controller in a monitoring center
- QoS guarantees and availability requirements, which may be expressed in terms of traffic loss or one-way delay metrics
- traffic isolation and privacy requirements. This typically requires encryption to ensure the privacy of personal data generated by biometric services.
- flow identification information, e.g., the IPv6 source address used by a given sensor to send data
- any relevant activation means (perhaps to dynamically graft a sensor to a specific Destination-Oriented Directed Acyclic Graph (DODAG) in a WSN that has Routing Protocol for Low Power and Lossy Networks (RPL) enabled [8].

4.2 Designing an IoT Service and Dynamically Allocating Resources

IoT resources can be dynamically selected and allocated according to the outcomes of the IoT service parameter negotiation and according to the information maintained by the SDN computation logic (Policy Decision Point) in an IoT resource repository, which stores the relevant IoT service data models [9].

Notifications originating from the IoT network may also affect the decision-making process of the SDN computation logic. For example, a sensor notifies the SDN computation logic that a 50% energy threshold has been reached, which leads to a decision to restrict it to only computing routes that are robust and reliable.

In the biometric data monitoring example mentioned previously, the outcomes of the service parameter negotiation feed the SDN computation logic, which derives the Objective Function [10] that locates the nearest grounded root in an RPL network environment. This grounded root could be hosted in a cloud service platform managed by the IoT service provider on behalf of the emergency dispatch center.

Depending on which RPL metrics best accommodate the IoT

service parameter negotiation results, the resulting DODAG topology may then look like either a high-quality link, battery-free routing environment, or low-latency link routing environment.

4.3 Dynamically Structuring IoT Service Function Chains

To differentiate traffic handling in an IoT infrastructure, SDN-computed service function chaining techniques may be used [11]. These techniques are designed to enforce differentiated traffic-forwarding policies within the IoT network infrastructure and satisfy a set of service-specific IoT requirements, such as delegated encryption, security control, traffic shaping and scheduling, message formatting (add/remove field, versioning, protocol adjustment), or privacy preservation. In such contexts, the SDN computation logic dynamically structures the various service function chains according to service requirements that need to be satisfied to deliver a specific IoT service.

In the biometric data monitoring example, a set of elementary service functions need to be invoked. Such functions include sleep mode and sensor duty cycle management, to optimize energy consumption in particular; encapsulation and MTU management, to adapt to various network environments (especially when traffic needs to reach an IoT controller located upstream in the network); and security management, to preserve data privacy.

Fig. 2 shows how two SDN-structured IoT service chains—SFC1 and SFC2—that are applied to traffic that crosses the IoT SFC domain.

- SFC1 = {Deep Packet Inspection (DPI), 6loWPAN encapsulating capability [12], RPL DODAG Information Object (DIO) trickle timer and Destination Advertisement Object (DAO) route lifetime settings, TLS Proxy, 6lo decapsulating capability}
- SFC2 = {DPI, 6lo near field communication (NFC) encapsulating capability, expected transmission count (ETX) setting, auto ACK enforcement, CoAP/HTTP proxy, 6lo decapsulating capability}.

The IoT infrastructure is operated according to policies that tell IoT devices which flows are to be bound with which service chain.

4.4 Dynamic Discovery of IoT Resources

An SDN approach involves a bootstrapping procedure for dynamic discovery of the IoT network topology (including active nodes), platforms, and their respective capabilities. This is necessary to feed the SDN computation logic.

The acquired information is stored and maintained in the resource repository. IoT service-driven policy provisioning and configuration information is derived from this repository and forwarded to the components that participate in the delivery and operation of an IoT service.

5 Virtualization Techniques Can Help Commoditize IoT Devices

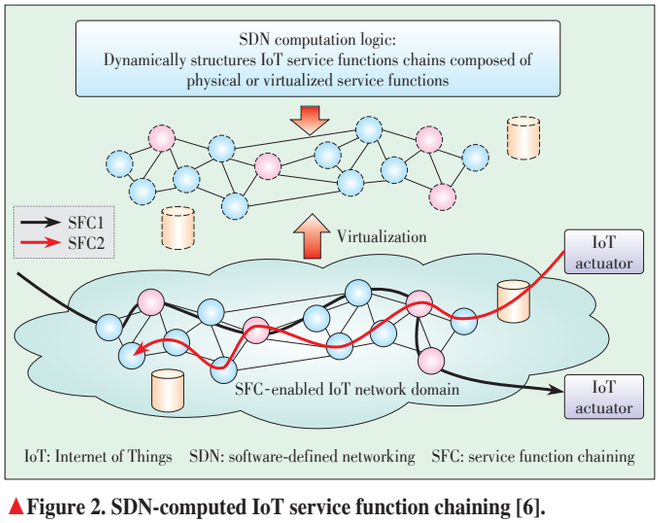
The lower layers, up to the Medium Access Control (MAC) layer, are embedded in commodity hardware. The upper layers, from the IPv6 network layer to the application layer (where Constrained Application Protocol (CoAP) [13] and HTTP reside) are virtualized and controlled by SDN (**Fig. 3**).

The SDN computation logic dynamically allocates virtual IPv6 forwarding and other RPL routing instances to master the flow of CoAP messages sent to a fleet of IoT devices for management purposes.

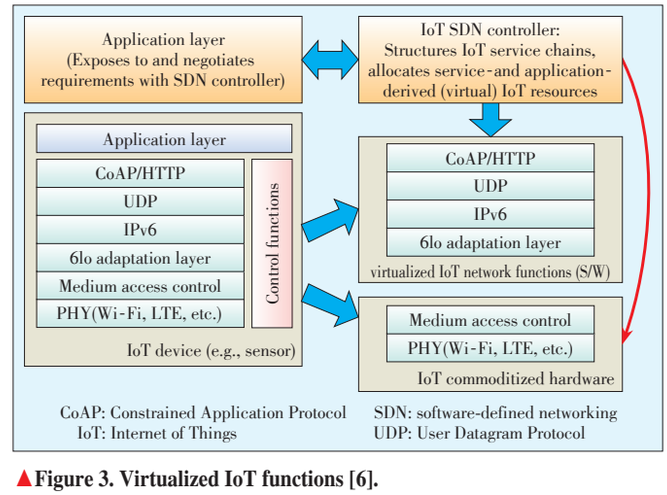
Such SDN-based deterministic flow mastery optimizes resource usage according to various parameters, such as location of IoT devices, whether these devices are mobile or not; acceptable ETX, to optimize duty cycle management; and data reception rate, to reduce energy consumption.

6 Conclusion and Next Steps

Combining SDN with virtualization is a likely precondition



▲Figure 2. SDN-computed IoT service function chaining [6].



▲Figure 3. Virtualized IoT functions [6].

to the mass adoption of robust, scalable IoT services. IoT service-delivery and operational procedures can leverage SDN—from service parameter negotiation to resource allocation and invocation.

Alongside ongoing academic research on SDN in IoT networking, vendors and operators are developing IoT-adapted protocols and data models as well as the computation logic that lies beneath the SDN intelligence. These are areas where operators can contribute significantly in the years to come.

The SDN approach to IoT networking described in this paper is being further assessed through simulation and prototyping. The preliminary results of development activities on multi-metric IoT route computation, cross-platform IoT networking, and IoT-specific service function chaining will be communicated in 2016.

References

[1] O. Mazhelis, H. Warma, S. Leminen, *et al.*, "Internet-of-things market, value networks and business models: state-of-the-art report," University of Jyväskylä, Jyväskylä, Finland, Tech. Rep. TR-39, 2013.
[2] J. T. Adams, "An introduction to IEEE STD 802.15.4," in *IEEE Aerospace Conference*, Big Sky, MT, USA, 2006. doi: 10.1109/AERO.2006.1655947.
[3] N. Noury, A. Fleury, R. Nocua, *et al.*, "eHealth sensors, biomedical sensors, algorithms and sensor networks," *Innovation and Research in BioMedical Engineering*, IRBM vol. 30, no. 3, pp. 93–103 , June 2009.
[4] *Software-Defined Networking: A Perspective from within a Service Provider Environment*, IETF RFC 7149, Mar. 2014.
[5] Z. Qin, G. Denker, C. Gianneli, *et al.*, "A software defined networking architecture for the internet-of-things," in *IEEE Network Operations and Management Symposium (NOMS)*, Krakow, Poland, 2014, pp. 1–9. doi: 10.1109/NOMS.2014.6838365.
[6] M.-K. Shin, Y. Hong, and C. Y. Ahn, "A software-defined approach for end-to-end IoT networking," in *Proc. IETF91 SNDRG Working Group Meeting*, Honolulu, USA, Nov. 2014.
[7] *IP Connectivity Provisioning Profile (CPP)*, IETF RFC 7297, Jul. 2014.
[8] *RPL: IPv6 Routing Protocol for Low Power and Lossy Networks*, IETF RFC 6550, Mar. 2012.
[9] R. Sudhaakar and P. Zand, "6tiSCH resource management and interaction using CoAP," IETF, draft-ietf-6tisch-coap, Mar. 2015.
[10] *Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)*, IETF RFC 6552, Mar. 2012.
[11] J. Halpern and C. Pignataro, "Service function chaining (SFC) architecture," IETF, draft-ietf-sfc-architecture, Aug. 2015.
[12] IETF. *IPv6 over Networks of Resource Constrained Nodes (6lo) Working Group* [Online]. Available: https://datatracker.ietf.org/wg/6lo/charter/
[13] *The Constrained Application Protocol (CoAP)*, RFC 7252, Jun. 2014.

Manuscript received: 2015-10-19

Biographies

Christian Jacquenet (christian.jacquenet@orange.com) graduated from the Ecole Nationale Supérieure de Physique de Marseille, a French school of engineers. He joined Orange in 1989, and he is currently the director of the Strategic Program Office For Advanced IP Networking, Orange Labs. He is responsible for Orange's IPv6 program, which aims to define and drive the the Group's IPv6 strategy. He also conducts development activities in the areas of software-defined networking and service function chaining. He has authored and co-authored several Internet drafts and IETF RFC standards on dynamic routing protocols and resource allocation techniques. He has also authored papers and books on IP multicasting, traffic engineering, and automated IP service delivery techniques.

Mohamed Boucadair (mohamed.boucadair@orange.com) is an IP networking strategist at France Telecom. He previously worked as a senior IP architect at FT and worked in the corporate division of FT, which made recommendations on the evolution of IP/MPLS core networks. He has worked for FT R&D and has been part of the team working on VoIP services. He has been involved in IST research projects, working on dynamic provisioning and inter-domain traffic engineering. He has also worked as an R&D engineer in charge of dynamic provisioning, QoS, multicast and intra/inter-domain traffic engineering. He has authored many journal articles and has written extensively on these subjects. He holds several patents on VoIP, IPv4 service continuity, and IPv6.