Course Takeaways

1. 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.

SDN is fundamentally different from traditional networks as it separates the data plane from the control plane, making the last one entirely programmable.

Building an SDN network offers several advantages, such as redirecting data based on the received frames. For instance, this allows for enhancing network security by permitting only specific types of frames (TCP, UDP, ICMP, etc.) or specific addresses to pass through.

The main challenges of SDN lie in implementing rules that correctly address the network's requirements. This involves programming the control plane to manage these aspects effectively.

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

NFV enables the virtualization of network functions, such as firewalls, routers, etc., on standard servers instead of running them on dedicated hardware.

The opportunities offered by NFV include:

- **Rapid Deployment:** New network functions can be activated with just a few commands (or clicks).
- **Scalability:** Resources can be adjusted dynamically based on demand.
- **Cost Reduction:** Eliminates the need for investment in specialized hardware.
- **Flexibility:** New services can be tested and deployed without disrupting the network.

-

3. 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.

Assignments related to question 3 :

Hint : Select one of the papers listed below and answer the questions. A couple of criteria are provided to help you choose the paper that better meets your expectations.

Paper	Questions
Title : Building Resilience for SDN-Enabled IoT Networks in Offshore Renewable Energy Supply **Venue** : 9th World Forum on Internet of Things (WF-IoT), oct. 2023 **Keywords** *:* Internet of Things, software-defined networking, resilience, offshore wind farms, performance, QoS **Abstract** :Resilient software-defined Internet of Things (SDIoT) networks are critical in offshore renewable energy supply (such as offshore wind farms) for wide-area monitoring, protection, automation, and control (WAMPAC). Offshore wind farms transmit time-sensitive data about the turbine performance, power generation, environmental conditions, and critical equipment status to the wind farm offshore landing point or the remote control room. As such, there is a need to guarantee real-time communication to coordinate protection and control actions that maximize production and minimize inadvertent wind farm downtime. This research designs a deep Q-Network (DQN) resilience model that quickly detects disruptions and applies optimal traffic engineering actions at the software-defined network (SDN) controller to guarantee high performance. This resilience model improves the quality of service of the SDNenabled IoT networks in offshore wind farm communication networks. **required expertise in communication networks :** low **Link to the document** *:* here	1. Quel est le rôle joué par le réseau SDN dans l'architecture type du cas d'application ciblé par ce travail ? 2. Quels critères ont motivé l'adoption d'un réseau SDN ? Quelles en sont les limites/faiblesses ? Aurait-il été possible de faire la même chose avec un réseau conventionnel ?
Title : IoT Gateway Edge VNFs on uCPE **Venue** : IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2018 **Keywords** *:* IoT, NFV, microservices **Abstract** : With the emergence of 5G and Internet of Things technologies, there is an increasing trend of network services integrating the edge and centralized cloud computing for guaranteeing low latency, real-time processing, and better security/privacy. In this demo, we present an intelligent IoT edge solution with IoT virtual network functions (VNFs) running on uCPE. We demonstrate the system architecture and IoT VNFs on uCPE	Cet article (de plus de 6 ans) introduit une démonstration montrant l'utilisation des approches NFV (Network Function Virtualisation) dans un contexte domotique. 1. Quelle est la finalité de la solution technique qui fait l'objet de la démonstration ?

and show that, in addition to typical uCPE VNFs, IoT VNFs can be included to increase opportunities for new IoT services and revenues while using the same management/deployment platforms as typical VNFs. **required expertise in communication networks :** low **Link to the document :** here	2. Décrire en qcq lignes les principes de la solution proposée ? 3. Quels sont les bénéficiaires d'une telle solution ? (utilisateurs ? opérateur réseau ? les prestataires de services applicatifs ?)
Title : LoRa-SDN: Providing Wireless IoT Edge Network Functions via SDN **Venue** : *International Convention on Information, Communication and Electronic Technology , 2020* **Keywords** *:* LoRa; SDN; IoT; wireless edge networks **Abstract** : Large-scale Internet of Things (IoT) deployments such as smart cities and smart grids are becoming a reality. In these topologies, extensive numbers of wireless devices transmit data to gateways that forward the collected data to back-end systems over a fixed network infrastructure – the core network. It is expected that in the near future the core network will utilize software-defined networking (SDN), as has already happened in data centres and networks of service providers. This enables simplified deployment of network functions and dynamic reactions to observed network conditions. This paper explores how SDN mechanisms can be applied beyond the traditional core network to include wireless IoT edge networks as well. The most popular IoT technology – Long Range (LoRa) – was selected as the main use case technology. The paper describes the LoRa integration with SDN and proposes the LoRa-SDN integration architecture. **Sections to read :** I,III and V **required expertise in communication networks :** low **Link to the document :** here	1. A quelle fin proposent les auteurs d'utiliser SDN dans le contexte de réseaux LoRa ? Comment ce choix est-il motivé ? 2. Décrivez brièvement les grandes lignes de la proposition d'intégration d'une approche SDN dans un réseau IoT edge avec des accès LoRa ?
Title : SDN-Enabled Secure IoT Architecture **Venue** : IEEE Internet Things Journal, 2021 **Keywords** *:* Internet of Things (IoT) Security, Software Defined Network (SDN) Security, Policy based Secure IoT Architecture, IoT Authentication and Access Control. **Abstract** : The Internet of Things (IoT) is increasingly being used in applications ranging from precision agriculture to critical national infrastructure by deploying a large number of resource constrained devices in hostile environments. These devices are being exploited to launch attacks in cyber systems. As a result, security has become a significant concern in the design of IoT based applications. In this paper, we present a security architecture for IoT networks by leveraging the underlying features supported by Software Defined Networks (SDN). Our security architecture restricts network access to authenticated IoT devices. We use fine granular policies to secure the flows in the IoT network infrastructure and provide a lightweight protocol to authenticate IoT devices. Such an integrated security approach involving authentication of IoT devices and enabling authorized flows can help to protect IoT networks from malicious IoT devices and attacks. **required expertise in communication networks :** **Sections to read:** III **Link to the document** *:* here	1. Expliciter pour chacune des phases prises en charge par l'architecture de sécurité proposée (authentification, autorisation et communication (ou transfert de données)), l'apport de l'approche SDN ?

Paper number 3:

Explain for each of the phases supported by the proposed security architecture (authentication, authorization and communication (or data transfer)), the contribution of the SDN approach?

According to this paper, in the authentication phase, SDN provides centralized authentication for IoT devices and uses a lightweight protocol based on Elliptic Curve Cryptography (ECC). This ensures that only legitimate devices can access the network. Additionally, IoT device information, such as the device identifier, is transmitted to the controller through IoT gateways, enabling centralized management of device identity verification.

In the authorization phase, the SDN controller evaluates various requests from authenticated devices based on predefined security policies (Policy-based Security Application). An authorization module, called the “IoT Authorization Authority,” verifies whether the network services requested by devices comply with the established policies. If a request is determined to be valid during this phase, an authorization token, known as “OAuth” (Open Authorization), is generated and provided to the device.

As for the communication phase, data transit is secured as the SDN controller manages data flows between IoT devices and data services. It also has the capability to establish secure paths for sensitive data.

Paper number 2:

This article (over 6 years old) introduces a demonstration showing the use of NFV (Network Function Virtualisation) approaches in a home automation context.

1. *What is the purpose of the technical solution being demonstrated?*
2. *Describe in a few lines the principles of the proposed solution?*
3. *Who will benefit from this solution (users? network operators? application service providers?)?*

This paper describes a solution implementing a VNF in an IoT project. This VNF acts as a gateway at the edge, capable of collecting information from multiple connected devices that use different protocols as needed. The device hosting this VNF, the uCPE, allows the integration of IoT plugins for technologies such as LoRa, Zigbee, BLE, etc.

Such a device also enables traffic redirection to various cloud destinations, such as Microsoft Azure or IBM Cloud, where different applications can run to process and deliver the information to users.

Implementing such a device in an IoT network offers several advantages:

- **Security:** The data collected from IoT devices can be processed within the VNF, ensuring only non-sensitive data is sent. For instance, an image could be processed to blur users present in it before transmission.

- **Latency:** Since the VNF is located at the edge, data takes minimal time to reach it. Additionally, if the cloud hosting the user application goes offline, the data remains stored in the VNF and can be transmitted as soon as the service is restored.
- **Modularity:** A VNF is quick to implement and modify as needed. It also simplifies the addition of new sensors without requiring configuration changes on the cloud.

-