Course Takeaways

(and inputs for your Portfolio ...)

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 differs from legacy networks by :

- Separating the control and data planes :
  - In legacy networks, the control plane and the data plane are tightly integrated within networking devices.
  - SDN separates these planes, centralizing control in an SDN controller while maintaining distributed data forwarding.
- Enabling centralized network management through a controller and allowing dynamic programmability via software :
  - SDN uses a logically centralized controller to manage the network, unlike distributed control in legacy networks.
  - This centralization simplifies configuration, monitoring, and troubleshooting.

These principles facilitate real-time optimization, scalability, cost efficiency using commodity hardware, and enhanced innovation and security through global network visibility. However, SDN faces challenges such as scalability limitations, controller reliability, integration with legacy systems, and potential security risks from its centralized architecture.

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

NFV virtualizes network functions like firewalls and load balancers, replacing specialized hardware with software running on standard servers. This approach reduces costs, accelerates service deployment, improves agility, and optimizes resource utilization. It also supports multi-tenancy and seamless disaster recovery.

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.

I choose the paper titled “Building Resilience for SDN-Enabled IoT Networks in Offshore Renewable Energy Supply”

- **Quel est le rôle joué par le réseau SDN dans l’architecture type du cas d’application ciblé par ce travail ?**

In SDN-enabled IoT networks for offshore wind farms, the SDN controller plays a key role by centralizing control and managing critical data flows. It enables:

- Adjustments to optimize the transmission of time-sensitive data, like measurements and control signals.
- Prioritization of important data to meet QoS standards.
- Quick responses to disruptions using a Deep Q-Network (DQN) agent, which detects issues and adjusts traffic to keep the network running smoothly.

- **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 ?**

Motivations for adopting an SDN network:

- Flexibility and centralization: SDN allows centralized control of network resources, which is important in remote areas like offshore wind farms.
- Programmability: The use of programmable interfaces facilitates the implementation of resilience solutions.
- Performance and QoS: SDN can dynamically manage traffic and prioritize critical data to meet quality of service requirements.

Limitations of SDN:

- Scalability issues: The centralized setup may become a bottleneck in large-scale systems.
- Dependence on the controller: The SDN controller is a single point of failure, so redundancy is needed.
- Integration challenges: Connecting to old systems and implementing advanced algorithms like DQN can be complex.

Achieving similar functionality with a conventional network would be highly challenging. Legacy networks lack the programmability, dynamic adaptability, and centralized management needed to meet the real-time and resilience requirements of offshore wind farm operations.

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 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	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 ? 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	1. A quelle fin proposent les auteurs d'utiliser SDN dans le contexte de réseaux LoRa ? Comment ce choix est-il motivé ?

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	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 resourceconstrained 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 ?