# 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 ?

**Differences between SDN and Legacy Computer Networks:** SDN, or Software-Defined Networking, is different from traditional networks because it separates the control and data planes. This means that instead of each device making its own decisions, a central controller manages everything. This centralization makes the network more flexible and easier to manage. Unlike legacy networks where each device operates independently, SDN provides a global view of the network, making it easier to implement policies efficiently. Plus, SDN allows for programmability through software, which means we can automate tasks and make real-time adjustments, making the network more agile and responsive.

**Opportunities Provided by SDN:** SDN offers many opportunities. With centralized control, network management becomes much simpler, making it easier to configure, monitor, and troubleshoot the network while reducing human errors. This centralized approach also improves network agility and flexibility, allowing us to quickly deploy new services and adjust policies to meet changing needs. Additionally, SDN optimizes resource utilization by dynamically routing traffic, which helps reduce congestion and improve bandwidth efficiency. This not only lowers operational costs but also enhances overall network performance.

**Main Challenges of SDN:** Despite its benefits, SDN does face some challenges. Managing large-scale networks with a single controller can be difficult, and while distributed controllers can help, they add complexity. Reliability is another concern because the centralized nature of SDN introduces a single point of failure, so redundancy and failover mechanisms are essential. Lastly, integrating SDN with legacy networks can be complex and requires significant standardization and compatibility efforts to ensure seamless integration.

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

**Network Function Virtualization (NFV**): NFV stands for Network Function Virtualization. It means we can run important network functions like routing, firewalls, and data compression

as software on regular servers instead of using special, expensive hardware. These functions are like independent software modules that can be managed more easily and flexibly. These network functions include routing, firewall, NAT, DPI, IDS, DHCP, and compression.

**Opportunities Provided by NFV:** NFV gives us a lot of opportunities. First, it makes the network flexible because we can change how it works on the fly and adjust resources based on what we need at the moment. This means we can quickly set up new services and use our resources more efficiently. Another great featuure is that we can chain these virtual functions together, so data packets go through a series of steps to get processed. This makes the network more efficient and customizable, helping us innovate and improve how the network works overall.

## 3. Are SDN and/or NFV relevant for your semester project ? If not, choose one of the assignments below ?

**Relevance of SDN and NFV for "What a Leak Detection" Project**

**SDN (Software-Defined Networking):** For our "What a Leak Detection" project, SDN is really useful because it helps manage the network in a smart way. Since we have multiple nodes (sensors) that need to communicate with each other to send data about leaks, SDN can centralize control and make the network more flexible. This means we can easily adjust how data flows between the sensors and the main monitoring system. If there's a lot of data or if something goes wrong, SDN can quickly change the network settings to keep everything running smoothly.

**NFV (Network Function Virtualization):** NFV is also really important for our project. It allows us to run network functions like routing and security as software on standard servers instead of using special hardware. This makes it easier to adjust the network as needed. For example, we can use virtual routers to manage how data moves between the sensors or virtual firewalls to keep the data secure. By chaining these virtual functions together, we can make sure that the data from our leak detection sensors is processed correctly before it reaches the monitoring system. This helps keep our data accurate and secure.