Unit-4

..Implementation of iot

- **Introduction to software defined network**
- **SDN of IOT**
- **Industrial of IOT**
- **Case study: Agriculture, Healthcare, Activity monitor**

Software-Defined Networking (SDN)

- SDN is a network architecture approach that enables the network to be intelligently and centrally controlled using software applications. This helps operators manage the entire network consistently regardless of the underlying network technology.
- This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic.
- SDN can create and control a virtual network – or control a traditional hardware – via software.
- In order to understand software defined networks, we need to understand the various planes involved in networking.

Data plane:

All the activities involving as well as resulting from data packets sent by the end user belong to this plane. This includes:

- Forwarding of packets
- Segmentation and reassembly of data
- Replication of packets for multicasting

Control plane:

All activities necessary to perform data plane activities but do not involve end user data packets belong to this plane. In other words, this is the brain of the network. The activities of the control plane include:

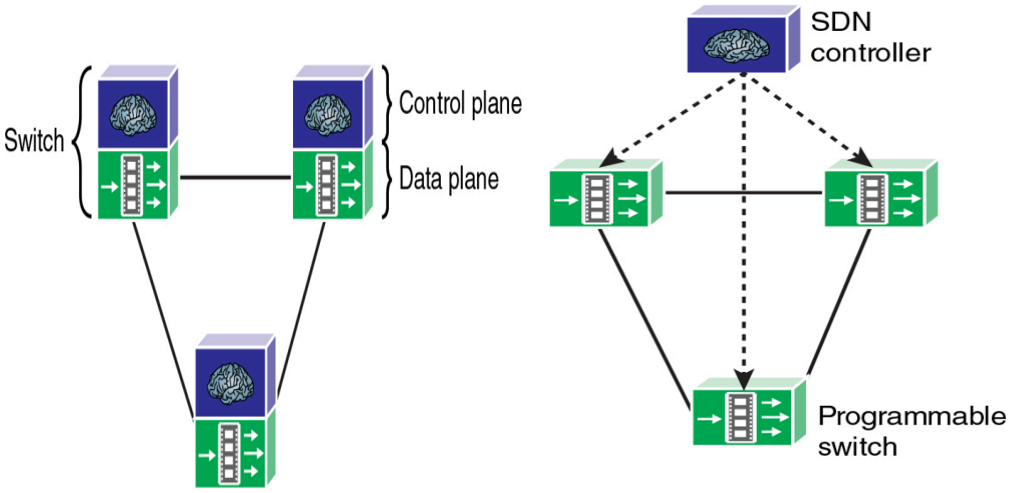
- Making routing tables
- Setting packet handling policies

In a traditional network, each switch or router has its own data plane as well as control plane. The control plane of various switches exchange topology information and hence construct a forwarding table which decides where an incoming data packet has to be forwarded via the data plane.

Software defined networking (SDN) is an approach via which we take the control plane away from the switch or router and assign it to a centralized unit called the SDN controller. Hence, a network administrator can shape traffic via a centralized console without having to touch the individual switches.

The data plane still resides in the switch and when a packet enters a switch, its forwarding activity is decided based on the entries of flow tables, which are pre-assigned by the controller.

A flow table consists of match fields (like input port number and packet header) and instructions. The packet is first matched against the match fields of the flow table entries.



Traditional networks SDN networks

SDN represents a substantial step forward from traditional networking, in that it enables the following:

- **Increased control with greater speed and flexibility:** Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.
- **Customizable network infrastructure:** With a software-defined network, administrators can configure network services and allocate virtual resources to

change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.

- **Robust security:** A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

How does Software-Defined Networking (SDN) work?

- Here are the SDN basics: In SDN (like anything virtualized), the software is decoupled from the hardware. SDN moves the control plane that determines where to send traffic to software, and leaves the data plane that actually forwards the traffic in the hardware. This allows network administrators who use software-defined networking to program and control the entire network via a single pane of glass instead of on a device by device basis.
- There are three parts to a typical SDN architecture, which may be located in different physical locations:
- **Application**s, which communicate resource requests or information about the network as a whole
- **Controllers**, which use the information from applications to decide how to route a data packet
- **Networking devices**, which receive information from the controller about where to move the data
- Physical or virtual networking devices actually move the data through the network. In some cases, virtual switches, which may be embedded in either the software or the hardware, take over the responsibilities of physical switches and consolidate their functions into a single, intelligent switch. The switch checks the integrity of both the data packets and their virtual machine destinations and moves the packets along.

SDN architecture

- Basic components
    - SDN switches
    - Controller
    - Applications

SDN Switches

- SDN devices contain forwarding functionality
- Forwarding information is stored in a flow table

- The flow table resides on the network device and consists of a series of flow entries and actions to perform when a packet matches an entry
- If the SDN device finds a match, it takes the appropriate configured action (e.g. forward)
- If it does not find a match, it can either drop the packet or pass it to the controller

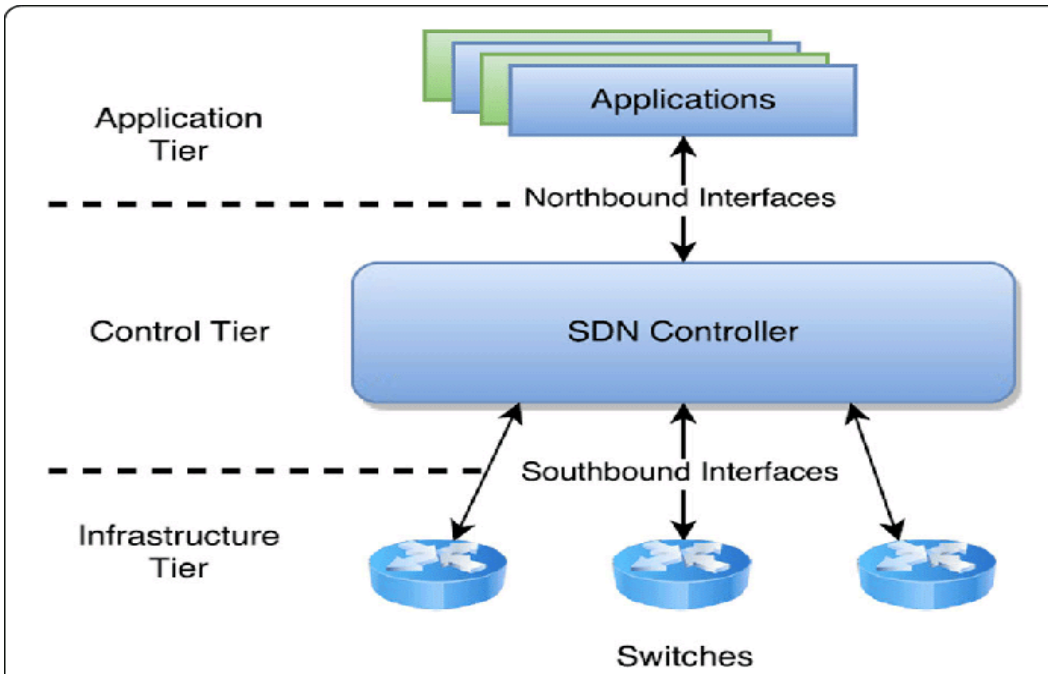
Controller

- It implements control plane functionality
- It presents an abstraction of the network to the SDN applications running above
- The controller allows the SDN application to define flows on devices and to help the application to respond to packets which are forwarded to the controller by devices
- It maintains a view of the entire network (global network view)

Applications

- SDN applications are built on top of the controller
- Software applications can implement forwarding, routing, overlay, multipath, access control, etc.
- The application is driven by events coming from the controller and from external inputs
- External inputs could include network monitoring systems, Netflow, IDS, or BGP peers

The layers communicate via a set of interfaces called the northbound APIs (between application and control layer) and southbound APIs(between control and infrastructure layer).



Advantages of SDN:

- Network is programmable hence can easily be modified via the controller rather than individual switches.
- Switch hardware becomes cheaper since each switch only needs a data plane.
- Hardware is abstracted, hence applications can be written on top of controller independent of switch vendor.
- Provides better security since the controller can monitor traffic and deploy security policies. For example, if the controller detects suspicious activity in network traffic, it can reroute or drop the packets.

Disadvantages of SDN:

The central dependency of the network means single point of failure, i.e. if the controller gets corrupted, the entire network will be affected.

SDN of IOT

Internet of Things (IoT), and Software Defined Network (SDN) are becoming popular technologies.

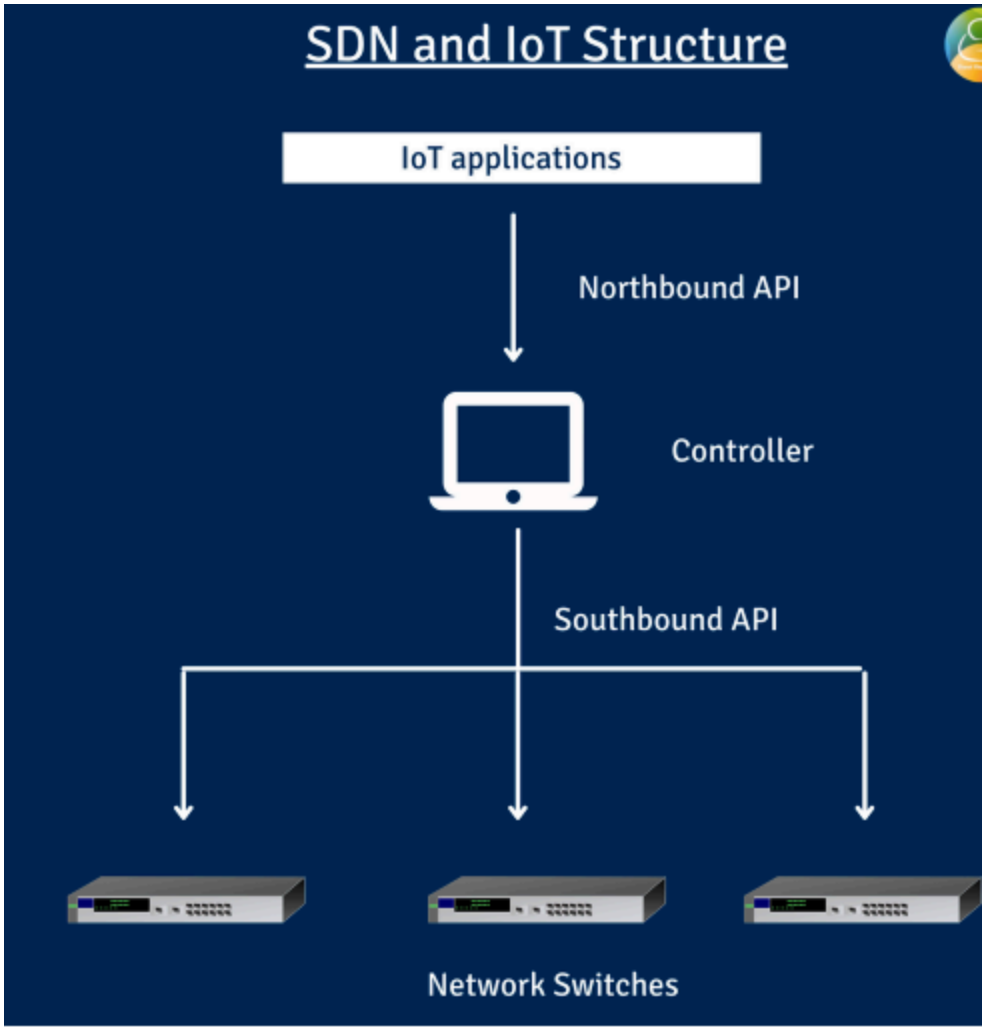
The main goal of IoT is to link electronic devices via the internet, meanwhile SDN facilitates network arrangement for management of a network by distinguishing the control layer and the data layer from each other.

The number of electronic devices over the internet is increasing constantly, therefore it is a complicated process to manage and control especially over the huge distributed network.

IoT network can be reasonably flexible and programmable through the SDN without introducing any trouble to the previously implemented network infrastructure.

In the IoT with SDN structure, the SDN controller allows up to separate the network into isolated subnets. Furthermore, the SDN Controller communicates with the IoT application using a unique application programming interface (API) known as the ‘Northbound API'. The latter analyses network traffic and take actions depending on the rules that have been specified.

The controller, on the other hand, communicates with network switches using another API (referred to as the "Southbound API") depending on configured rules. Overall, the combination of IoT with SDN improves IoT operations and security by allowing full and remote control of network setup without requiring direct contacts with IoT devices.



SDN and IoT structure

How does SDN work with IOT?

- SDN is implemented via the Openflow Protocol. The SDN switch uses a flow table, which is similar to the routing table used by traditional routers. It does, however, support chaining and allows for the matching of a broader variety of fields, with each flow having its own set of actions.

- When a packet arrives at a switch, it is compared to the flow table; if a match is detected, the relevant actions are carried out.
  If no match is identified, as is expected with a newly inserted device, the received packet is transferred to the SDN controller through the Southbound API.

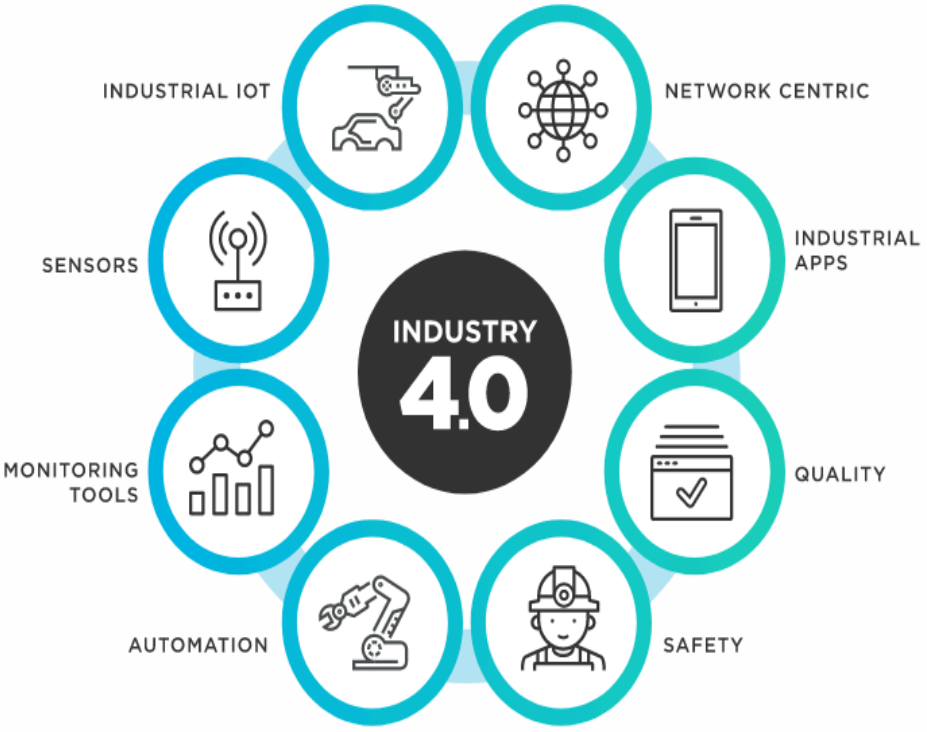
- The controller then inspects the packet and takes appropriate action. It may create a new flow on the switch to allow subsequent packets to be routed without the involvement of the controller. The SDN application will be notified via the Northbound API.

Industrial Internet of Things (IIoT)

Industrial IoT, or the **Industrial Internet of Things (IIoT)**, is a vital element of Industry 4.0. IIoT harnesses the power of smart machines and real-time analysis to make better use of the data that industrial machines have been churning out for years.

The principal driver of IIoT is smart machines, for two reasons.

- The first is that smart machines capture and analyze data in real-time, which humans cannot.
- The second is that smart machines communicate their findings in a manner that is simple and fast, enabling faster and more accurate business decisions.



IIoT is used across a range of industries from manufacturing, logistics, oil and gas, transportation, mining, aviation, energy, and more.

Its focus is to optimize operations--particularly the automation of processes and maintenance.

IIoT capabilities enhance asset performance and better manage maintenance. In the long run, it moves the industry toward a demand service model, increases customer intimacy, and creates new revenue streams--which all contributes to the digital transformation of industries.

Applications of IIoT

IIoT is a game-changer for any industry in manufacturing that produces physical products or manages product transportation. IIoT can increase operational efficiencies, which in turn paves the way to create completely new business models. It has a range of applications in a cross-section of industries.

Production

Currently production sectors use IIoT technology the most. Smart machines, enabled with IIoT, can self-monitor and anticipate possible production hurdles. This results in lowered downtime and better efficiency.

Supply Chain

While keeping up production numbers is important, smooth delivery across the supply chain is also crucial. With IIoT, orders can automatically replenish stocks when needed. This reduces waste, maintains stock numbers, and makes sure the right amount of raw materials are always available. With the automation of supply chains and ordering, employees can focus on more complex areas of functioning.

Building Management

Most building management issues can be addressed with IIoT technology. Sensor-driven climate control removes all the uncertainty related to managing a building's internal climate and takes all needed factors into consideration--such as the number of people, ventilation spots, machinery, and more. IIoT enhances building security with smart devices that assess possible threats from any entry points of a building.

Healthcare

Healthcare has embraced smart devices for a long time now. Healthcare professionals can remotely monitor patients and are alerted by any status change. This makes healthcare more precise and personal. In the future, artificial intelligence may be able to assist with diagnoses, enabling doctors to treat patients more accurately and effectively.

Retail

IIoT technology in retail enables quick marketing decisions specific to each store. Companies can update storefronts based on region-specific consumer interests, and they can target audiences with smarter promotions. These data-driven insights make a store stand out from its competition.

Sensors are not new technology as companies have used them to track goods or monitor machines for years. The difference in IIoT is the ability to adopt these changes on a larger scale due to the lowered costs of sensors, comprehensive wiring networks, and big-data analytics.

Globally, manufacturers spend $197 billion yearly on IIoT, according to tech analyst IDC. Transport companies alone have invested around $71 billion in it. Companies are setting aside budgets for IIoT, but how they spend these budgets varies from one company to another, based on their priorities.

How Does IIoT Work and the Benefits

IoT is a network of smart devices and via networks that are linked to databases. These devices monitor, collect, exchange, and analyze data. A typical IIoT system comprises of:

- Smart equipment that measures, stores, and communicates information
- Public or private internet networks that serve as a data communication structure
- Analytical applications that process raw data into data insights for optimized processes
- Tools that help decision-makers and employees utilize data for better business outcomes

Dataflow is crucial to ensuring that IIoT applications work optimally. To aid dataflows, companies use a databus to distribute and manage real-time data. This technology paves the way for applications and devices to work together as a cohesive unit. While a database manages historical data at rest, a databus manages data in motion.

IIoT streamlines and automates processes, which increases business productivity. It improves operational efficiency, lowers operational costs, and increases income-generation. Better automation levels enhance product quality, and this, combined with efficient operations, assists with predictive maintenance.

With IIoT, the chances of creating new revenue streams is much higher. Data insights can provide information into how an efficiently run operation can resolve little-known inefficiencies to enhance productivity. Performance or usage data leads to newer products or services. For example, manufacturers can work out asset-sharing models with other manufacturers. This resource sharing optimizes space and production capabilities while saving costs. Similarly, IIoT devices can monitor and better manage an HVAC system.

IIoT works on improving productivity and quality, without burdening resources. This helps immensely with business expansion.