**INDEPENDENT STUDY**

**ON**

**SOFTWARE DEFINED NETWORKING**



**Submitted to:**

Prof. Stephen Guhl

EECS department, WSU.

**Submitted by:**

Susmitha Neerubai

C534C335

Masters, Computer networking

Wichita state university

**TABLE OF CONTENTS:**

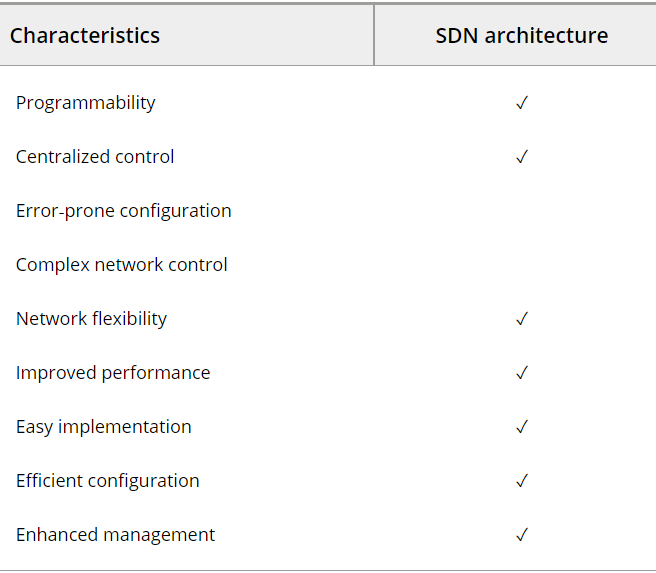
|  |  |
| --- | --- |
| Definition | 3 |
| Architecture of SDN | 3 |
| How SDN works | 4 |
| Challenges and issues of SDN | 5 |
| Agility | 6 |
| Scalability | 6 |
| Elasticity | 7 |
| Conclusion | 8 |

**Definition of software-defined networking**:

SDN lets you design, build, and manage networks, separating the control and forwarding planes. As a result, the control planes is directly programmable, and it abstracts the underlying infrastructure for applications and network services.

Network intelligence is logically centralized through programmable SDN controllers. Implemented in software, these controllers maintain a coherent view of the network domain. To applications and policy engines, SDN looks like a single logical switch.

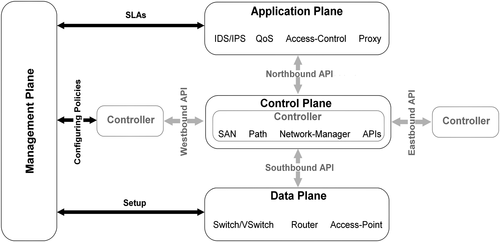
Software‐defined networking (SDN) is facilitating organizations to deploy applications and enable flexible delivery, offering the capability of scaling network resources in lockstep with application and data needs, and reducing both CapEX and OpEX. SDN is an innovative approach to design, implement, and manage networks that separate the network control (control plane) and the forwarding process (data plane) for a better user experience. This network segmentation offers numerous benefits in terms of network flexibility and controllability.



**ARCHITECTURE OF SDN:**

core architecture of SDN is divided into three layers. The upper layer of SDN architecture is an application layer that defines rules and offers different services such as firewall, access control, IDS/IPS, quality of service, routing, proxy service, and monitoring balancer. This layer is responsible of abstracting the SDN network control management through the northbound API. The second layer is known as the control plane, which is an abstraction of the network topology. The controller is the main component responsible for establishing flow tables and data handling policies as well as abstracting the network complexity and collecting network information through the southbound API and maintaining an up‐to‐date network holistic view. The southbound API communications can be deployed in two different scenarios:

* in‐band communication: In this scenario, the traffic between the controller and any network device should abide by the dictated flow rules.
* out‐of‐band communication: Here, the traffic does not follow flow rules. This type of deployment requires VLAN implementation to isolate the traffic flow from the communications, which depends on OpenFlow rules.



SDN architecture’s decouple network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services.

The OpenFlow protocol can be used in SDN technologies. The SDN architecture is:

* **Directly Programmable**: Network control is directly programmable because it is decoupled from forwarding functions.
* **Agile**: Abstracting control from forwarding likes administrators dynamically adjust network-wide traffic flow to meet changing needs.
* **Centrally** **managed**: Network intelligence is centralized in SDN controllers that maintain a global view of network.
* **Programmatically** **configured**: SDN let network manager configured, manage, secure and optimize network resources via dynamic, automated SDN programs.

**How SDN Works:**

SDN providers offer a wide selection of competing architectures. All SDN networks have some of an SDN controls, as well as southbound and northbound application program interfaces (APIs).

Controllers:

The “Brains” of the networks, SDN controllers offer a centralized view of overall network, enabling network administrators to dictate to underlying systems (like features and routers).

Southbound APIs:

SDN uses southbound APIs to relate information to the switches and routers “below”. OpenFlow, consider the first standard in SDN, was the original southbound API. While popular, it is no longer the only API available on the market.

Northbound APIs:

SDN uses northbound APIs to communicate with the applications and business logic “above”. This help network administrators to shape traffic and deploy services through program instead of by manual configuration.

**CHALLENGES AND ISSUES IN SDN:**

In particular, the challenges and issues that appear of paramount importance in the SDN environment are the following:

1. ***Scalability*:** This defines the ability of SDN to, more specifically in the control plane, handle and process an increasing workload. Scalability aims at enlarging the capacity of the SDN by implementing mechanisms such as devolving [16](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0016), clustering [17](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0017), and high processing [18](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0018) to cope with the growing load.
2. ***Reliability*:** The SDN is considered reliable when it notifies of delivery failures of the data in real time. In such network, there should be a specified minimum reliability for the delivery of critical data. In today's implementations, SDN controllers [19](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0019) must be capable of meeting real‐time requirements for reliable delivery and timeliness.
3. ***High availability***: HA is an important aspect of today's services that should be available each time a customer requests a given service or resource. Availability is usually expressed as a percentage of uptime in a given year. Unavailability of services can generally occur owing to network outages or system crashes [20](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0020), [21](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0021). Network providers generally deploy backup services to offer HA by implementing redundant server hardware, server OS and network components, and so on.
4. ***Elasticity***: Elasticity is the ability of SDN to dynamically adapt its capacity by scaling up or down the available resources [22](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0022), [23](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0023) in order to meet the variation and fluctuation of the workload. Generally, elasticity is often focused on the control plane and might be referred to as scalability.
5. ***Security***: SDN security consists of protecting the information from theft or damage to the hardware and the software as well as from disruption of the services [24](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0024), [25](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0025). Securing SDN encompasses physical security of the hardware, as well as preventing logical threats that may come from the network or data. SDN vulnerabilities are the entrance door to security attacks being intentional or accidental.
6. ***Performance***: Performance refers to the amount of tasks achieved by SDN components compared with the time/resources (e.g., CPU and RAM) being used [26](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0026). There are many different ways to measure [27](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0027), [28](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0028) the performance of a network, as each network is different in nature and design. As far as SDN is concerned, the important measures are bandwidth, throughput, latency, and jitter.
7. ***Resilience***: Resilience in SDN is the capability to ensure and maintain an acceptable level of service even in case of a service, network or node failure. When an SDN element is faulty, the network should provide a continuous operational service with the same performance. In order to increase the resilience of SDN, potential challenges/risks have to be identified and addressed to protect the services [29](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0029).
8. ***Dependability***: The dependability of SDN is strongly tied to availability and reliability terms. SDN dependability aims mainly at preventing faults and implementing fault tolerance mechanisms to guarantee service delivery even at a degraded level [30](https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1737#sec1737-bib-0030). In addition to HA and reliability, integrity and maintainability are also two important dependability attributes.

**Gaining agility with SDN:**

Network intelligence, agility and flexibility are among the top difficulties of a product characterized administrator, particularly with regards to client experience, as indicated by Luigi Licciardi, head of Standards, IPR and Research Coordination at Telecom Italia Group.

Talking on the "Period of a product characterized administrator" board at TM Forum's Digital Disruption occasion in San Jose, Calif., a week ago, Licciardi said understanding the knowledge as of now in a fixed system, and how to change that system into something that is progressively dexterous and can pursue distinctive client and administrations necessities is the main test of the present specialist organizations as they move to a product characterized arrange (SDN).

"But on the other hand it's the best chance," he noted, including that while SDN and system capacities virtualization (NFV) are significant from a cost-decrease angle, they are similarly as significant from the point of view of having the option to convey administrations and applications on request, start to finish.

What this means is that we are separating and disaggregating the customer applications or services from the network infrastructure. This is more like a sandbox or private network for each application that is on an existing network.

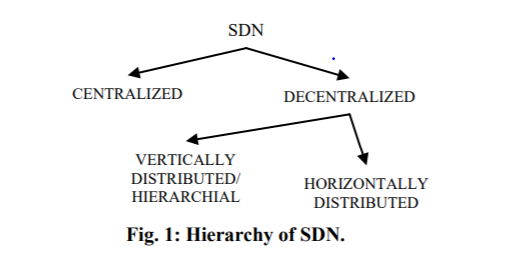
**Scalability:**

It means that a data center should be able to house thousands of tenants and several thousands of tenants networks.

In the infrastructure layer, scalability is enhanced by modifying the hardware and software of the network or forwarding device means it depends on memory size and processing speed of CPU.

HIERARCHY OF SDN AND THEIR SCALABILITY ISSUES:

The SDN has centralized and decentralized architectures.



SCALABILITY EVALUATION OF DIFFERENT MODELS OF SDN:

a metric which evaluates scalability of different models of SDN i.e. centralized control plane, vertically distributed/hierarchical control plane and horizontally distributed control plane.

They define scalability of controller contains number of nodes varies from 𝑁1 to 𝑁2 as follows

𝜑(𝑁1 , 𝑁2) = 𝐹(𝑁1)/ 𝐹(𝑁2)

where, 𝐹(𝑁1) and 𝐹(𝑁2) ≡ productivity of control plane having nodes 𝑁1 and 𝑁2 respectively

Productivity of control plane is defined as 𝐹(𝑁) = 𝜑(𝑁) × [𝑇(𝑁)/𝐶(𝑁)]

where, 𝜑(𝑁) ≡Throughput of control plane for processing network requests

𝑇(𝑁) ≡average response time for each request

𝐶(𝑁) ≡ cost of deployment of control plane

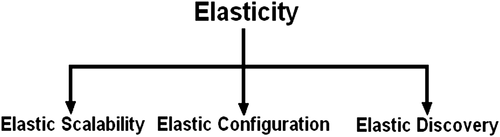
𝑁 ≡ Number of nodes in the network

SDN is easy to program, manageable and less complex as compared to the conventional network but the basic centralized nature of SDN is bottleneck for scalability of this network and it can be enhanced by decentralizing the control plane and modifying hardware and software of forwarding device and controller for load balancing, routing, traffic engineering etc. We further works on placement of controllers in the network so as to get maximum throughput and efficiency with less cost.

**ELASTICITY:**

Elasticity is another challenge facing cloud providers to manage and adapt responsiveness of SDN demands in real time. In addition to this, cloud providers should offer more elastic access to computing and network resources. Elasticity can be seen from three dimensions.

1. **elastic scalability**: aims at ensuring the growth depending on network requirements. SDN can scale dynamically in case of high demands.
2. **elastic configuration**: gives an opportunity to add, edit, and delete configuration to meet new network requirements and respond to new challenges in terms of bandwidth and throughput.
3. **elastic discovery*:*** anticipates discoveries as well as becoming aware of possible emerging technological opportunities and threats at the right time to react and meet the new requirements and trends. The main purpose is to identify irrelevant tendencies and think of acquiring new efficient techniques/strategies that might help in improving the SDN. The observations should be made quickly and the action must be taken in real time to take advantage of new possible network features and/or remove potential threats by deploying novel countermeasures.

[](https://onlinelibrary.wiley.com/cms/attachment/2608957d-5e32-4821-981b-417e2739c916/sec1737-fig-0004-m.jpg)

**Table:**Elasticity issues, solutions, and challenges.

|  | **Proposal** | **Main purpose/challenge** | **Elasticity (technique)** |
| --- | --- | --- | --- |
|  | ElastiCon is an elastic distributed controller architecture in which the controller pool dynamically expands or shrinks to automatically balance the load across controllers | Addressing the load imbalance issues to offer elasticity and load‐balancing equity | Load‐balancing/distribution |
|  | FreeFlow (split/merge) is a system that allows transparent and balanced elasticity for stateful virtual middleboxes to have the ability to migrate flows dynamically | Providing elasticity by the execution of virtual middleboxes | Load‐balancing |
|  | Hierarchical SDN is an architectural solution that offers a new way for the forwarding and control planes. Small forwarding tables are used in the network nodes to determine paths | Achieving elasticity and enabling more agile mechanisms for disaster recovery/fast restoration | Hierarchical |
|  | Elastic distributed SDN controller tailored for mobile cloud computing and FMC‐based systems where the SDN/OpenFlow control plane is repartitioned on a two‐level hierarchical architecture: a first level with a global FMC controller and a second level with several local FMC controllers | Ensuring elasticity with better control plane management, performance maintenance and network resources preservation | Distribution |

**CONCLUSION:**

On investigating the issues/challenges as well as the solutions for SDN in terms of scalability, elasticity, dependability, reliability, high availability, resiliency, security, and performance. As SDN is a new networking approach, several solutions to classical network problems have been revisited using this architecture, and many problems continue to be challenging. In this paper, we tried to simplify and explain each SDN issue and provided an overall view. It is important to note that the landscape of SDN‐related issues changes according to the advances in SDN development.

Research must focus more on the control plane to come up with novel solutions for controllers, which are the brains of the SDN architecture. The control plane is a point of failure of the whole network, and many security measures should be considered. Also, new HA and performance mechanisms should be implemented to abide by the SLA and deliver services accordingly. Service providers are willing to meet carrier‐grade SDN requirements by ensuring scalability, reliability, and resilience of their infrastructure. However, by adopting an extensive range of sophisticated features into their networks, reliability of SDN becomes a challenging goal. In fact, this is challenging when it comes to sticking with service requirements and respect today's telecommunication and network commitments in terms of fast fault management, detection and recovery, prevention from unauthorized access and Dos attacks, high throughput, very low latency, and software upgrades and patches.

Figure below summarizes all SDN challenges to be considered when designing a resilient SDN network, which is still an open research area. To achieve resilience, the service providers must deploy secure components/policies and reliable mechanisms. As for dependability, both highly available and reliable infrastructures are required to ensure a continuous and reliable service delivery to end costumers. Elasticity and scalability are also two important goals in designing carrier‐grade networks, but those can be only established in a highly available network with low latencies and high performance.

