10.48047/jocaaa.2023.31.01.30

Software-Defined Data Centers: Innovations in Network Architecture for High Availability

Bhupendra Singh[1]
bhupendra.research1@gmail.com,
Sr Network Engineer, Marriott International"
Shubh Prabhat[2]
prabhatshubh95@gmail.com
Architect, Globallogic
Ashish Anand[3]
gcp.ashish2020@gmail.com,
Director, Marriott International

Abstract

The advancement of next-generation networks (NGN) is largely attributable to the software-defined networking (SDN) revolution. Academics and businesses alike are very interested in software-defined networking (SDN) because of its "service provisioning on the fly" capabilities. An extensive overview of software-defined networking (SDN) improvements over traditional networks is offered in this article. The article delves into the growth of software-defined networking (SDN), the functional architecture of SDN and associated technologies, and the standards and protocols of OpenFlow, including the fundamental idea of how OpenFlow connects to network elements (NEs) like optical switches. There was also a chosen architectural survey. In order to better manage massive amounts of internet traffic and assist infrastructure and service providers in dynamically customising their resources, we have proposed an architecture based on software-defined heterogeneous networks. This architecture points towards new technology that will open up new vistas in the field of network technology. Additionally, in order to assess the progress towards standardisation of this technology, numerous standard development organisations (SODs) are now doing research and other activities to standardise SDN as NGN.

Keywords: OpenFlow Informational platform Plane of control Label switching that is applicable to several protocols Programs specify

1. Introduction

In order to meet the societal demands of an ever-increasing global population, networking connection speeds must increase to accommodate the growing need for big data analysis and the widespread usage of multimedia content. From 2014–2019, worldwide internet traffic is

10.48047/jocaaa.2023.31.01.30

predicted to increase at a CAGR of 23%, reaching 2.0 ZB/year or 168.0 EB/month in 2019 [1]. By 2016, this number might have risen to 1.1 ZB/year or 88.4 EB/month. By 2018, there will likely be 1.4 gadgets per capita, and by 2014, the number of mobile-connected devices will have surpassed that of the world's inhabitants [2, 3]. Furthermore, projections indicate that traffic originating from mobile and wireless devices will surge in the coming years. There will be a 66% growth in wireless traffic by 2019 (including Wi-Fi and mobile devices), whereas the percentage of wired traffic will fall from 54% in 2014 to 33% in 2019, according to this new Internet traffic forecast [1].

Still, it's worth noting that, according to some estimates, the number of Internet connections will outstrip the world's population by 2019, and that the amount of bandwidth sent by each individual would rise from 8 GB to 22 GB [1]. Approximately 980 million people in India use mobile devices, and 300 million have internet access [4]. Expanding Digital India Mission's reach to the remaining population is the next big goal. Hyper-capacity DWDM circuit switched optical networks are the main means to cope with the explosive network traffic beyond October 2023 [3]. The bandwidth demand generated by new and current ICT applications such as mobile computing, Internet of Things (IoT), cloud and fog computing, big data analytics, and Ultra High Definition (UHD) video-on-demand are insert reasons for the above-mentioned push. For network providers, operationally wise data delivery in such situations poses immense challenges in efficiency and cost.

Since most of the FN applications require dynamic provision of resources, Software-Defined Networking (SDN) has appeared as a metrology-based adaptive solution. SDN minimizes CAPEX and OPEX by separating hardware control from software logic and allowing centralized and programmable management of network resources [3].

SDN can be defined by three main characteristics:

- Separation of Control and Data Planes: The control plane is responsible for making decisions, while the data plane handles the packets forwarded according to that decision.
- Centralized Control: A logically centralized control plane allows unified management of multiple data-plane elements.

10.48047/jocaaa.2023.31.01.30

- Programmability through APIs: The SDN controller directly communicates with forwarding devices, such as switches and routers, via protocol-based interfaces like OpenFlow.

Thirdly, this design allows for global adjustments rather than device-centric configuration, which involves modifying each hardware item individually, and gives the networking administrator a bird's-eye perspective of the whole network. Nicira Networks first suggested this ground-breaking technology and idea, building on work they had done at UCB, Stanford, CMU, and Princwton [5, 6]. Research in software-defined networking (SDN) has recently focused on expanding its use to many types of networks, such as those in homes, businesses, cellular towers, Wi-Fi hotspots, and more.

2. SDN as a Progress Towards More Modern Network Architectures

To oversee routing paths, configure different NEs with each other in the network path, and monitor and control data flow, conventional networks use hardware components like application specific integrated circuits (ASICs) to implement a set of rules and algorithms[7]. The routing devices in a traditional network use a predefined set of rules stored in the firmware to determine the packet's destination address and the route it should take once it arrives at their location. Data packets are often processed in a consistent way and sent to the same location, all inside a very cheap routing device. In addition, a Cisco router or other specialised routing device may be able to handle packets differently based on their contents and characteristics. The administrator may use specialised local router code to indicate which flows are more important. Therefore, each router's queue size may directly control the flow of packets. With this kind of tailored local router configuration, operators may regulate traffic congestion and priorities more effectively. Due to heavy network traffic, existing network devices are unable to provide optimal network performance; this impacts the network's scalability, dependability, security, and speed. The present-day network nodes aren't dynamic enough to handle the many kinds of packets and the data they contain.

This may be circumvented with the use of a software module that handles data rules appropriately. Efficient use of network resources will aid improve control over network traffic, which might lead to state-of-the-art technology called SDN [8]. Additionally, it facilitates the efficient creation of virtual flow slices, which allows users to make better use of cloud resources like storage, computation, bandwidth, and virtual machines (VMs). The purpose of software-

10.48047/jocaaa.2023.31.01.30

defined networking (SDN) is to provide a system that allows for the transparent and user-controlled administration of a network's transport devices. The number of controllers on the control plane could be one or more, depending on the size of the network. P2P setup allows for the formation of a distributed network control that is both fast and reliable, even in the presence of various controller environments. Every item in a flow table contains three fields: matching, counter, and instruction. As a result, the network's data processing, control, and administration capabilities are enhanced. This is because, rather of having to deal with each device in the network separately, an administrator may regulate data flow and make desired changes to the characteristics of the network's switching and routing devices from a central location using software modules (applications) .

Another way to look at SDN's progress is as an extraordinary evolutionary step; new services are added to the mix by using virtualisation, especially for optical transport network control and management, which boosts the network's efficiency and capacity.

Complex processes are engaged in the attempts to tackle varied societal issues in light of the technical breakthroughs of the Internet. To make NGN a reality, research and development are continuing at this very moment. The implementation of an all-optical network has great promise for FN. With its high-speed switching in a packet-based software-defined-network (SDN) architecture, this optical packet and circuit integrated network (OPCInet) provides a variety of services, increases functional flexibility, and reduces energy consumption in the metro/core network [9,10].

Table 1: Innovations in Network Architecture for High Availability

Category	Innovation	Description	Benefits for High Availability
Software-Defined Networking (SDN)	Centralized Control Plane	Decouples control from data plane via SDN controller	Enables dynamic rerouting and quick failure recovery
Network Function Virtualization (NFV)	Virtualized Network Services	Firewalls, load balancers, and routers deployed as virtual instances	Increases flexibility and redundancy
Overlay Networks	VXLAN, NVGRE	Encapsulates L2 traffic over L3 networks for multi-tenant environments	Simplifies network segmentation and improves fault isolation
Intent-Based Networking (IBN)	Policy-Driven Automation	Network behavior defined by high-level	Reduces manual errors and enables

10.48047/jocaaa.2023.31.01.30

		intent and enforced via automation	predictive failure management
Microsegmentation	Fine-Grained Security Policies	Logical segmentation of workloads at the VM or container level	Limits attack surface and contains breaches without impacting availability
Self-Healing Networks	AI/ML-Driven Network Monitoring	Uses machine learning for anomaly detection and predictive maintenance	Minimizes downtime through proactive remediation
Multi-Path Networking	Equal-Cost Multi-Path (ECMP), Link Aggregation	Uses multiple paths between source and destination	Load balancing and path redundancy improve fault tolerance
Disaggregated Infrastructure	Hardware Abstraction & Resource Pooling	Decouples compute, storage, and network resources	Enables dynamic resource allocation and redundancy
Zero Trust Architecture (ZTA)	Continuous Verification	Ensures identity-based access at every level of the network	

3 Motivation

The following facts should help to illustrate the rationale for using SDN technology as NGN:

• Investing in the network infrastructure to increase the capacity of the current computer network is necessary to meet the rapidly increasing traffic. Even a small business would need hundreds, if not thousands, of devices to keep up with the massive growth of the network. Managing networks is a hard task due to the heterogeneous structure of networks caused by the deployment of equipment, applications, and services offered by many suppliers, providers, and manufacturers.

Conventional methods of setup, optimisation, and troubleshooting would become ineffective and inadequate as a result of these challenges. Network function virtualisation (SDN) is promoted as a potential solution to the issues listed above. It does this by separating the control logic from the data plane, which enables software-based network administration and operation that is both flexible and efficient.

• In the early stages of software defined optical networks (SDONs), when control logic is offloaded from the switching node, scalability, reliability, and network performance are major

10.48047/jocaaa.2023.31.01.30

challenges for efficient operation. Several OpenFlow controller implementations, such as NOX-MT, Maestro, Beacon, etc., are able to handle at least 50,000 new flow requests per second, according to a research conducted on a large simulated network with 256 switches and 100,000 endpoints [11]. That means a single controller can manage an unexpectedly high volume of new flow requests. Therefore, issues with scalability, dependability, and network performance are effectively handled.

Implementing programmable traffic flow management and load balancing arrangements inside a data centre (DC) is made easier using optical-technology-based software-defined networking (SDN), which allows for on-demand mobility and service relocation.

Wherein the latency and bandwidth needed by various applications (varying traffic flows) are considered [12].

• The majority of existing networks are built to make the most efficient use of the underlying infrastructure, and the spectrum that has been allocated is more than enough. This led to the proposal of new elastic-optical networking (AEON) technologies in SDON. Without using a static wavelength grid, variable spectrum capacity is assigned to each data connection individually. It is a smart network that uses its resources with great optimisation [13] thanks to the flexible bandwidth network's allocation of spare spectrum to rerouted signals, which increases its adaptability.

• Additionally, SDN can integrate multiple transport technologies and multi network domains efficiently and effectively.

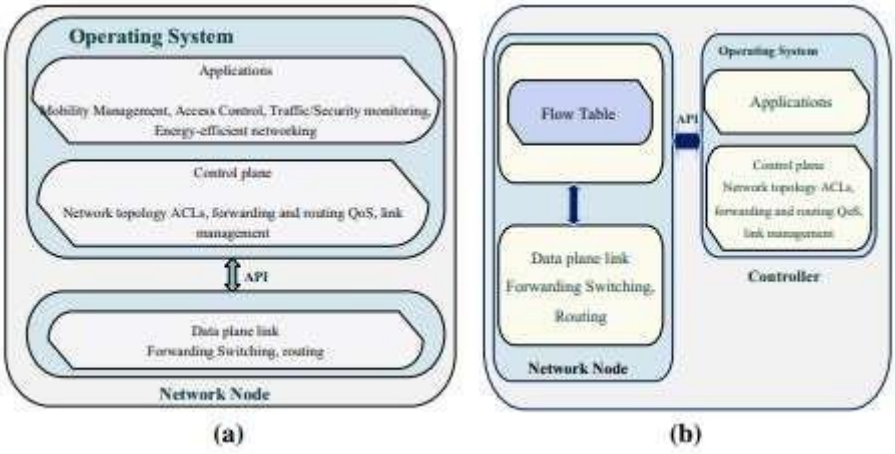

Figure 1: The SDN node in comparison to the traditional network node [9]. a traditional method (where each node in the network is independently managed on the control and

10.48047/jocaaa.2023.31.01.30

data planes). b. Software-defined networking (SDN) method (network nodes offload control logic to the controller)

4. Layer for Application

In the block architecture depicted in Figure 3, the top tier, positioned above the control layer, is known as the Application layer. This layer leverages high-level programming languages to interact with the network and abstract the global network state. SDN applications continuously retrieve and manipulate network information through southbound and northbound protocols such as the Extensible Messaging and Presence Protocol (XMPP). These applications enable dynamic control of the physical Network Elements (NEs), facilitating advanced network operations.

Key SDN applications within the Application layer include:

- **Energy-efficient networking**: Optimizing power consumption in network devices.
- **Security monitoring**: Enhancing network security through real-time threat detection.
- **Access control links**: Managing network access policies for end-users and devices.
- **Traffic engineering**: Ensuring optimal flow and bandwidth distribution across the network.
- **Path Computation Element (PCE)**: Dynamic routing and optimization of network paths.

These applications enable **programmable, flexible, and adaptive** management of modern networks, responding to dynamic traffic and operational conditions.

4.1 Dynamic Routing

Routing and packet switching are the two primary operations of every network. The current distributed method to packet switching and routing has its disadvantages, such as sluggish convergence, complicated implementation, and limited capacity to create adaptive control, among others. In contrast, software-defined networking (SDN) is based on closed-loop control, which allows for adaptive network management by continuously feeding applications information about the global network state. In software-defined networking (SDN), load balancing and cross-layer design are two common adaptive routing applications.

10.48047/jocaaa.2023.31.01.30

4.2 Managing Loads

When it comes to data centres, load balancing is the method of choice for optimising resource use. The deployment of a front-end load balancing in the DC allows for the direct routing of client requests to specific servers, which in turn increases throughput, decreases response time, and prevents network overload. It may be costly and lead to a bottleneck if all requests are handled by a dedicated load balancer. Whereas, SDN load balancing makes use of a number of algorithms for rules-based packet routing. Koerner et al. created and used a differentiated load balancing algorithm to manage various kinds of traffic, including online traffic and email traffic [14].

4.2.1 Design Cross-Layer

As in the OSI reference model, entities at different levels are allowed to communicate information inside each other; in layered architecture, the cross-layer design is in charge of enhancing the integration between different layers. This cross-layer architecture is ideal for deploying to increase the network's overall efficiency since SDN applications may access the network's status information. The cross-layer method proposed by [15] has the capacity to dynamically configure the underlying network element by using the re-configurability and high speed of software-defined networking (SDN) switching devices, such as optical switches. In order to take use of a device's multiple interfaces and multi-casting capabilities, developed a handover method that integrates WiFi and WiMax networks, which incorporates hoolock. Each client connection has its own unique basic service set identifier (BSSID) in another investigation using Odin. This method has little effect on HTTP downloading in both single and multiple handovers, low latency in re-association, and no throughput reduction by exchanging the BSSID of one Physical Wireless AP with another BSSID of a neighbouring AP during handover.

4.2.2 Upkeep of Networks

One of the most common causes of network failure due to configuration errors is human mistake. In this case, there is no automated or compressive solution for network maintenance that can be provided by individual diagnostic tools like ping, traceroute, tcpdump, or NetFlow. Configuration errors are mitigated by using the centralised and automated management approaches inherited from SDN. As soon as the controller detects a network breakdown,

10.48047/jocaaa.2023.31.01.30

provide a quick restoration method for software-defined networking (SDN) that involves calculating a new route for uninterpreted traffic flow using updated packet forwarding rules.

4.2.3 Secure Networks

Firewalls and proxy servers are now used to prevent physical breaches in networks. However, network operators have a significant issue when trying to authentically apply these strategies owing to the variety in network design. Alternatively, software-defined networking (SDN) offers a centralised control plane that is easy to design merge and verify rules to avoid security breaches.

4.2.4 Virtualisation of Networks

Virtualisation (NV) involves slicing a physical network into several virtual network entities, which are then assigned to different users and controllers. But, FlowVisor is the most popular tool in software-defined networking (SDN) for creating virtual networks for research experiments by slicing physical network resources including topology, flow space (the data flow table in switching), bandwidth, CPU of switching devices, and control channel.

OpenFlow is a key protocol in **Software-Defined Networking (SDN)** that enables the separation of the control and data planes. It allows a centralized **SDN controller** to manage network devices (like switches and routers) through standardized messaging.

Core Components:

- **Flow Tables**: Store rules with match fields (e.g., IP, ports), counters, and actions (e.g., forward, drop).
- **OpenFlow Messages**:
    - OFPT_PACKET_IN: Sent to the controller when no match is found.
    - OFPT_FLOW_MOD: Adds/modifies/deletes flow entries.
    - OFPT_PACKET_OUT: Controller instructs switch to forward a packet.
    - OFPT_STATS_REQUEST/REPLY: Used for network statistics.
- **Secure Channel**: Encrypted communication (typically over TLS) between controller and devices.
- **OpenFlow Agent**: Executes instructions on the device based on controller commands.

10.48047/jocaaa.2023.31.01.30

Key Benefits:

- **Centralized management**
- **Granular traffic control**
- **Rapid deployment of network innovations**
- **Interoperability across vendors**

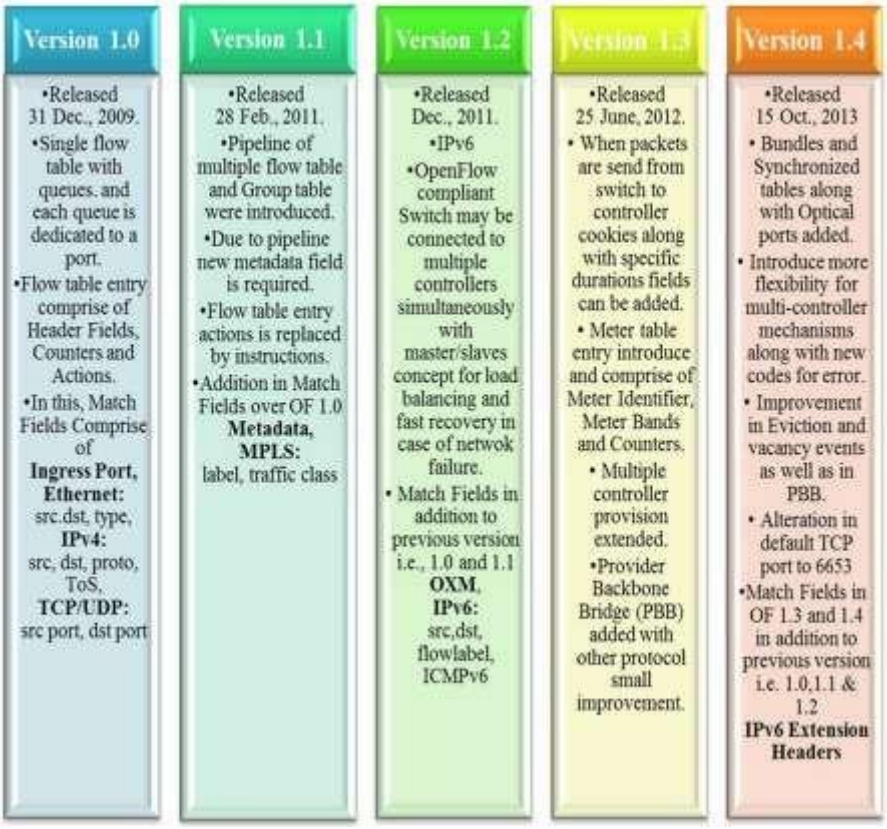

Figure 2: Advancement in OpenFlow in chronological order

4. How SDN Functions

Separate centralised controllers in SDN replace the individual network nodes as the source of control. Routing, visibility, provisioning, and orchestrating of network overlays are just a few of the many tasks carried out by this controller. Figure 3 shows that the network operations system (NOS) manipulates the forwarding plane by giving an abstract representation of the network topology to the software-defined networking (SDN) controller that hosts the different applications. This API, known as southbound, gathers information from the SDN switches. In

10.48047/jocaaa.2023.31.01.30

this way, the controller may optimise flow management by drawing on the network's detailed knowledge, which satisfies the needs of service users for scalability and flexibility. The application can do things like dynamically allocate bandwidth into the data plane.

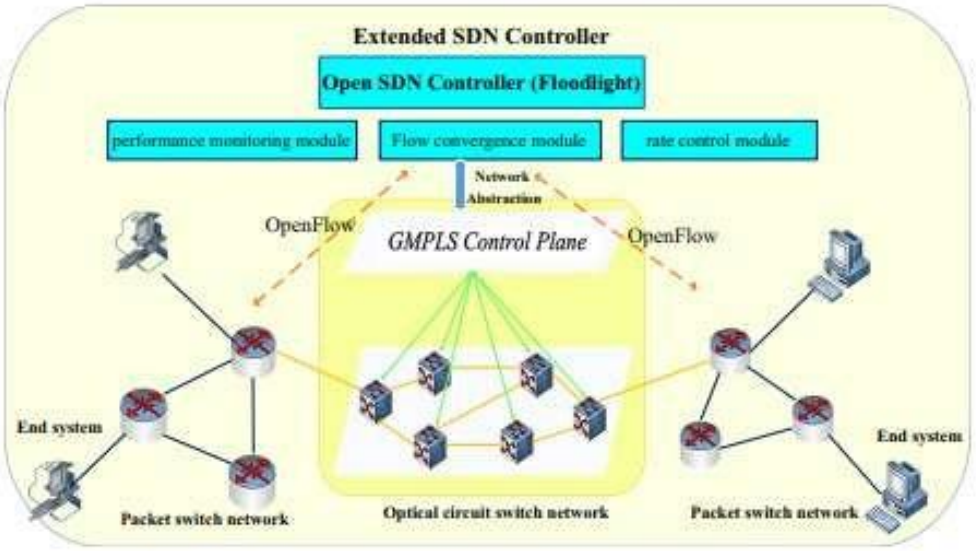

Figure 3: SDN Extended Controller

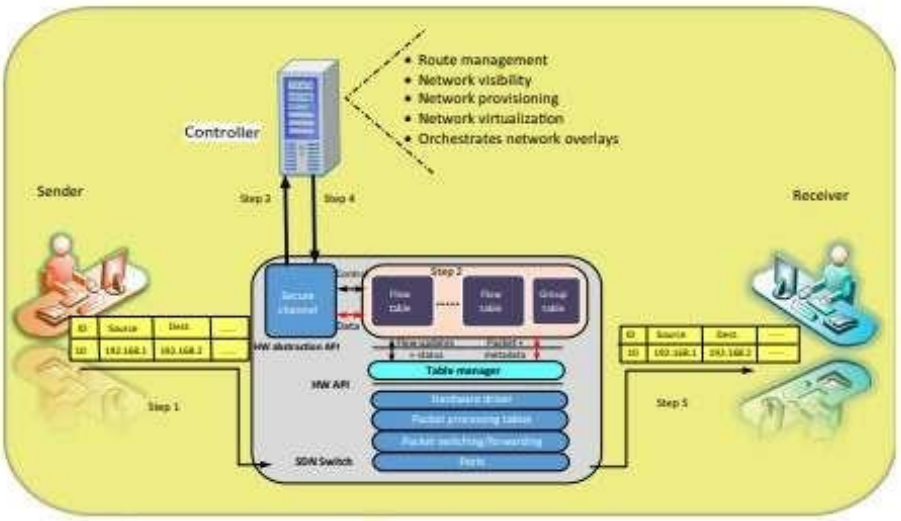

Figure 4: The SDN controller and switch.

In Figure 4, we can see that the first step in creating a new flow is for a packet to arrive at the switch from the sender. The second step is for the SDN switch to check if the packet matches a flow rule stored in the SDN cache. If it does, the instructions associated with that entry, such as those pertaining to the packet/match fields, update counter, metadata, and action set, are executed. Step 5 entails directing the packets to the appropriate recipient. Step 3 involves

10.48047/jocaaa.2023.31.01.30

sending the packet to the controller via a secure channel in the event that the match is not available in the switch's flow table. Step 4 involves the controller analysing the packet for its source and destination IP addresses. Based on this analysis, the entries in the flow tables of the switches along the route are updated using the southbound API, which includes protocols like PCE, ForCES, and OpenFlow. In step 5, the packet is sent to the recipient via the switch to the correct port [9].

5. Architecture for Software-Defined Heterogeneous Networks (SDHNs)

As illustrated in Figure 5a, our suggested SDHN as a FN design includes a controller, an OpenFlow switch, a packet switching network, an optical circuit switching network, and a base station/AP that allows for smooth communication with N clients. Figure 18a, b show the various network devices used in the data plane, including packet switches, optical switches, and wireless devices. The control plane in our proposed SDHN architecture communicates with the data plane through a south-bound interface, which includes the OpenFlow protocol and the OpenFlow agent/GMPLS. The controller performs functions such as route management, network visibility, and orchestrating network overlays.

10.48047/jocaaa.2023.31.01.30

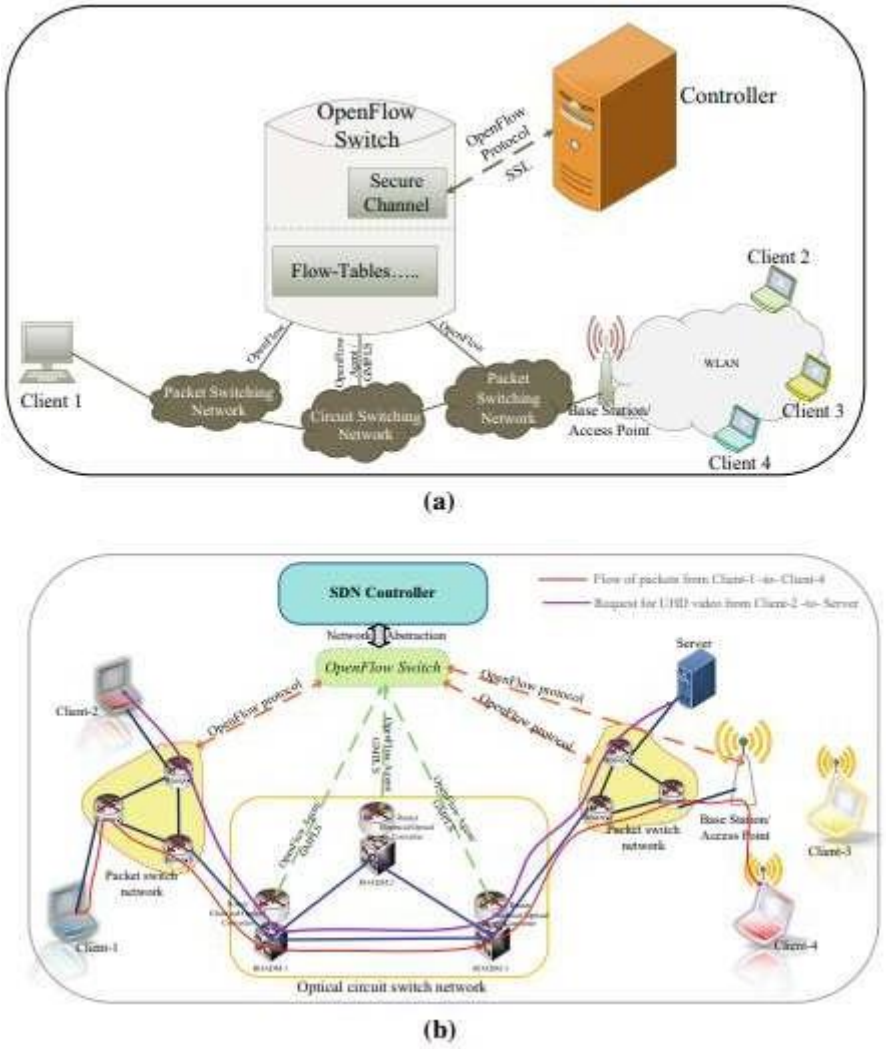

Figure 5: a. The SDHN's proposed block diagram, b. The SDHN's suggested architecture

Ingress network device Router-1 is the access point to the data plane when data gets transmitted from source to destination, like from Client-1 to Client-4. Router-1 receives the packet, processes the header and then looks it up against the flow table entries. If it finds an entry matching that flow, it executes the corresponding actions such as forwarding, modifying, or dropping the packet as defined by the match-action rule.The packet shall then be made to traverse the other routers and switches in the data plane, with each intermediate device applying similar such logic through its flow tables until the packet reaches its destination. The new flow usually indicated if there is not a single matching flow entry in the ingress device such as Router-1. The switch encapsulates the packet in a PACKET_IN message for forwarding to the SDN controller. The controller first performs a global network-level analysis, develops an appropriate flow rule, and then responds with a FLOW_MOD message to change the ingress

10.48047/jocaaa.2023.31.01.30

device's flow table. In this way, subsequent packets of the flow can be managed by these devices instead of being sent to the controller.

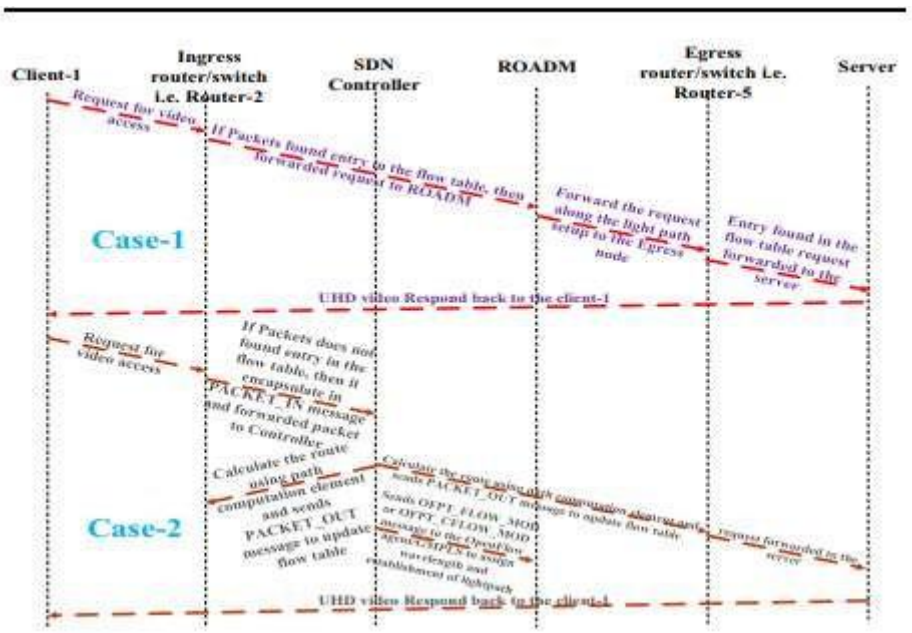

Figure 6: Show how the server is notified of a number of events that occur when client-2 requests on-demand ultra-high definition video access.

In the described SDN-enabled optical network architecture, the data plane dynamically updates its flow tables when Clients 1 through 4 initiate communication using a Path Computation Element (PCE) to transmit PACKET_OUT messages to the OpenFlow switch. These switches store flow entries derived from interdomain flow tables, ensuring efficient forwarding decisions across domain boundaries. Simultaneously, for the optical transport layer, wavelength assignment is coordinated by the SDN controller through interaction with the OpenFlow agent or Generalized Multiprotocol Label Switching (GMPLS) controller. This is achieved using OFPT_FLOW_MOD messages—either standard OpenFlow messages for mapping solutions or custom OpenFlow extensions—enabling the controller to specify flow rules tailored to optical transport requirements. Upon receipt of these flow modification instructions, the OpenFlow agent/GMPLS translates the directives into Transaction Language
1 (TL1) commands required by the Reconfigurable Optical Add-Drop Multiplexers (ROADMs) to establish the necessary optical lightpaths. These lightpaths ensure proper packet traversal through the optical layer in alignment with SDN policy.

In the specific use case, the data flow destined for Client-4 traverses the following devices: Router-1, Router-3, ROADM-1, ROADM-3, Router-4, and Router-6, reflecting a multi-layer

10.48047/jocaaa.2023.31.01.30

path computation across both IP and optical domains. Software-Defined Data Centers have transformed the infrastructure of the conventional data centers into completely virtualized and programmable facilities. It uses compute, storage and networking resources as abstract services. The basic technology that drives this evolution is Software-Defined Networking, which is related to decoupling of the control and data planes, leading to centralized policy enforcement and dynamic traffic engineering along with granular resource management. In the context of high availability (HA), SDN-based architectures are the most agile and fault-tolerant architectures possible, due to automated failover, link redundancy, real-time traffic rerouting, and proactive monitoring of the network. SDDCs deploy network function virtualization (NFV), with which essential services: firewalls, load balancers, intrusion detection systems are implemented as virtualized network functions (VNFs) increasing resilience and improvement of scalability. Thus, the services could be programmed and elastric so that they could be dropped off to ensure service continuity and fast recovery in failure. They are the main compositions to support mission-critical applications and cloud-native deployment. New inventions in the control plane intelligence, intent-based networking, and their AI driven orchestration are quickening the march of SDDCs into a more autonomous self-healing future network infrastructure. As depicted in Figure 6, the sequence of events is illustrated when Client-2 requests on-demand Ultra High Definition (UHD) video content from the server. This triggers an end-to-end service provisioning workflow encompassing flow table population, wavelength assignment, and dynamic path configuration across the hybrid SDN-optical network fabric

6. Ongoing Studies and SDN Standardizations as NGN

The following section elucidates the advancements in Software-Defined Networking (SDN) technologies, particularly in the context of standardization efforts aimed at facilitating Next Generation Network (NGN) deployments. A pivotal milestone in this domain was the establishment of the Open Networking Foundation (ONF) in 2011 by leading technology companies including Deutsche Telekom, Facebook, Google, Verizon, Microsoft, and Yahoo. The ONF was founded with the objective of accelerating the adoption of SDN and fostering the development of networks driven by the OpenFlow protocol. OpenFlow has since evolved into a central component of the SDN ecosystem, which is now supported by a robust and expanding community comprising both academic researchers and industry stakeholders. The synergy between academia and industry has led to the continuous development and deployment

10.48047/jocaaa.2023.31.01.30

of OpenFlow-based systems and software frameworks. A broad range of network equipment manufacturers consistently release OpenFlow-compliant hardware and software solutions, reflecting the protocol's increasing maturity and adoption the OpenFlow specification has undergone multiple iterations, each introducing enhanced capabilities and extended functionalities to accommodate evolving network demands. With every release, new features have been integrated, including advanced flow table structures, improved match-action fields, and extended support for diverse protocols. This iterative refinement has led to the emergence of numerous SDN controllers and switching devices that fully comply with OpenFlow standards, fostering interoperability and contributing to the widespread standardization of SDN across heterogeneous networking environments.

6.1 Current Research Activities

The majority of existing research in the field of Software-Defined Networking (SDN) has been conducted within the confines of Local Area Networks (LANs). However, Wide Area Network (WAN) environments are increasingly being recognized as viable candidates for SDN deployment. Emerging studies support the notion that WAN functionality can be realized through the integration of OpenFlow-based infrastructures, enabling centralized control over geographically distributed network elements.

In the context of wireless networks and mobility management, researchers have identified limitations associated with traditional distributed control plane architectures. These limitations manifest in the inefficient handling of constrained resources such as radio spectrum, suboptimal handover mechanisms, and inadequate inter-cell load balancing. In contrast, SDN-centric architectures offer a centralized and programmable approach that enhances wireless network management. Key features include dynamic spectrum management, the instantiation of virtual access points (VAPs) on demand, seamless handover orchestration, and optimized base station resource allocation—such as time-frequency resource blocks in Long-Term Evolution (LTE) and Orthogonal Frequency Division Multiple Access (OFDMA) systems—tailored to per-user requirements.

Furthermore, SDN provides a programmable substrate that accelerates the deployment of innovative network applications and services. This programmability is instrumental in the development of next-generation heterogeneous 5G wireless networks, where critical

10.48047/jocaaa.2023.31.01.30

functionalities such as network slicing, virtual network provisioning, and Network Function Virtualization (NFV) are essential for supporting diverse service demands and performance metrics.

To facilitate experimental research in mobile and wireless SDN environments, platforms such as OpenRoads have been proposed. OpenRoads is considered a wireless analog to OpenFlow and incorporates multiple wireless technologies, including WiMAX and Wi-Fi, within its architecture. It enables fine-grained control over wireless access infrastructure, thereby serving as a foundational testbed for evaluating SDN-driven wireless mobility solutions.

7. Conclusion

Network traffic is experiencing an exponential rise, presenting a challenge to the technological infrastructure presently existent-in effect, it becomes difficult to provide efficient solutions. In this regard, the quest for innovation continues unabated. Software-Defined Networking (SDN) allows a younger avenue of thought when one regards separating the control plane from the data plane with respect to conventional networking architectures. Such separation brings about much higher levels of scalability, reliability, and overall performance of the selected network. This article presents an extensive overview of programmable networking and its developments through a period of about two decades. The emphasis is placed on some of the important advancements and professional opinions, from early programmable network framework designs to modern-day deployments of SDN. A fairly technical treatment of the SDN architecture is presented, with special consideration given to OpenFlow protocols and their applicability in talking to network elements (NEs). Some studies showed that some optical devices do not support the OpenFlow protocol; hence, researchers are considering alternate solutions such as virtual Ethernet interfaces (veths), OpenFlow agents, Generalized Multiprotocol Label Switching (GMPLS), and hybrid solutions. A critical analysis has been conducted on selected SDN architectures based on service capabilities, interfacing methodologies for network elements, and resource optimization strategies. Our proposed Software-Defined Heterogeneous Network (SDHN) as Future Network (FN) architecture features a centralized SDN controller that interfaces with a heterogeneous data plane comprising packet switches, optical transport elements, and wireless devices. The controller is responsible for tasks such as dynamic route computation, network visibility, policy enforcement, and orchestration of network overlays. Furthermore, ongoing research initiatives have significantly contributed to the standardization process of SDN technologies, outlining

10.48047/jocaaa.2023.31.01.30

their practical applications and deployment strategies. Looking ahead, it is anticipated that the architecture of the future Internet will conform to the Infrastructure-as-a-Service (IaaS) model. Under this framework, traditional Internet Service Providers (ISPs) will be restructured into two primary roles: Infrastructure Providers (InPs), who own and maintain the physical network infrastructure, and Service Providers (SPs), who offer end-to-end services by deploying network protocols. Within this ecosystem, Virtual Network Providers (VNPs) aggregate virtualized resources from multiple InPs, enabling the deployment of Virtual Networks (VNs) by Virtual Network Operators (VNOs) tailored to the specific requirements of SPs. Leveraging SDN in conjunction with Network Functions Virtualization (NFV) allows for programmable, on-demand provisioning and dynamic service chaining.

In conclusion, SDN emerges as a transformative networking technology, enabling granular control, programmability, and adaptability. It empowers network operators to dynamically configure infrastructure based on application-specific demands, thereby optimizing resource utilization and reducing both capital expenditures (CapEx) and operational expenditures (OpEx). As SDN continues to mature, its full potential—especially at a global scale—has yet to be fully realized, ensuring its relevance and applicability well into the foreseeable future.

Reference

1. Azari, M. M., Solanki, S., Chatzinotas, S., Kodheli, O., Sallouha, H., Colpaert, A., ... & Ottersten, B. (2023). Evolution of non-terrestrial networks from 5G to 6G: A survey. IEEE communications surveys & tutorials, 24(4), 2633-2672.
2. Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., Montoya, J. F. M., ... & Goussetis, G. (2023). Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials, 23(1), 70-109.
3. Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.
4. Barakabitze, A. A., Ahmad, A., Mijumbi, R., & Hines, A. (2023). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, *167*, 106984.

10.48047/jocaaa.2023.31.01.30

5. Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2023). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE access, 6, 3619-3647.
6. Erdelj, M., Natalizio, E., Chowdhury, K. R., & Akyildiz, I. F. (2023). Help from the sky: Leveraging UAVs for disaster management. *IEEE Pervasive Computing*, *16*(1), 24-32.
7. Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2023). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1761-1804.
8. Wijethilaka, S., & Liyanage, M. (2023). Survey on network slicing for Internet of Things realization in 5G networks. *IEEE Communications Surveys & Tutorials*, *23*(2), 957-994.
9. Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2023). Internet of things: Security and solutions survey. Sensors, 22(19), 7433.
10. Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2023). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion, 102, 102060.
11. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2023). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.
12. Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., ... & Das, S. K. (2023). Edge-computing-driven internet of things: A survey. ACM Computing Surveys, 55(8), 1-41.
13. Ahmad, S., Shakeel, I., Mehfuz, S., & Ahmad, J. (2023). Deep learning models for cloud, edge, fog, and IoT computing paradigms: Survey, recent advances, and future directions. Computer Science Review, 49, 100568.
14. Modupe, O. T., Otitoola, A. A., Oladapo, O. J., Abiona, O. O., Oyeniran, O. C., Adewusi, A. O., ... & Obijuru, A. (2023). Reviewing the transformational impact of edge computing on real-time data processing and analytics. Computer Science & IT Research Journal, 5(3), 603-702.
15. Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2023). A survey on security and privacy issues in edge-computing-assisted internet of things. IEEE Internet of Things Journal, 8(6), 4004-4022.