Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 6, No. 1, June 2020, pp. 54~67
ISSN: 2338-3070, DOI: 10.26555/jiteki.v6i1.17105

Analyzing challenging aspects of IPv6 over IPv4

Shahzad Ashraf*[1], Durr Muhammad[2], Zeeshan Aslam[3]
[1]College of Internet of Things Engineering, Hohai University, Changzhou Jiangsu, China
[2]Department of Information Systems Management, Pakistan Steel Mills Karachi Pakistan
[3]Petroweld Erbil, Kurdistan Region Iraq

ARTICLE INFO

Article history's:

Received 01 July 2020,
Revised 15 July 2020,
Accepted 25 July 2020.

Keywords:

QoS,
Networking,
mitigating,
interoperability,
VPN.

ABSTRACT

The exponential expansion of the Internet has exhausted the IPv4 addresses provided by IANA. The new IP edition, i.e., IPv6 introduced by IETF with new features such as a simplified packet header, a greater address space, a different address sort, improved encryption, powerful section routing, and stronger QoS. ISPs are slowly seeking to migrate from current IPv4 physical networks to new generation IPv6 networks. The move from actual IPv4 to software-based IPv6 is very sluggish since billions of computers across the globe use IPv4 addresses. The configuration and actions of IP4 and IPv6 protocols are distinct. Direct correspondence between IPv4 and IPv6 is also not feasible. In terms of the incompatibility problems, all protocols can co-exist throughout the transformation for a few years. Compatibility, interoperability, and stability are key concerns between IP4 and IPv6 protocols. After the conversion of the network through an IPv6, the move causes several issues for ISPs. The key challenges faced by ISPs are packet traversing, routing scalability, performance reliability, and protection. Within this study, we meticulously analyzed a detailed overview of all aforementioned issues during switching into IPv6 network.

Corresponding Author:

Shahzad Ashraf,
College of Internet of Things Engineering, Hohai University, Changzhou Jiangsu, China
Email: nfc.iet@hotmail.com

1. INTRODUCTION

The fast growth of the Internet is taking place across the globe. After decades of struggle, due to speedy and appropriate technological advancement, a large number of technologies like 3G and 4G become a part of the Internet, which is supported by mobile devices. The fast changes of the Internet world enlarged the requirement for a unique IP address, which can be used for individual devices. Benefiting from the services of the Internet, the home users who are linked through smartphones can enjoy and take advantage of different services, and the billions of IP addressing can only be provided through IPv4, 32-bit addressing technique, which is about 4 billion [1]. The ISPs faced difficulties in providing Internet access to new users. Internet Assigned Number Authority (IANA) mentioned that IPv4 addresses are approximately ended [2]. The solution is to move on to the new IPv6 network. IPv6 was developed by Internet Engineering Task Force (IETF) with extra features, such as smaller header size, larger address space, new any-cast addressing type, integrated security, efficient routing, and better QoS [3]. It is a 128-bit architecture and can provide undecillion IP addresses. It is said to be a next-generation IP protocol. Both IP4 and IPv6 protocols are different in format and behavior and cannot communicate directly with each other. ISPs are moving towards Next Generation Network (NGN) [4], progressively and the changeover process is very sluggish due to billions of devices are working throughout the world. Therefore, it is not possible to replace the entire network with new IPv6 at once in a short span of time. According to a Google survey report, after over 25 years, the transition process is 25 % completed approximately. There are many reasons behind this slow conversion. The economic factor is also at a high rate. Hardware cost, more energy consumption, staff training, and else, altogether increases the economic cost [5]. The dual-stack technique and virtualized network architectures are introduced to overcome

the financial factor. Network Functions Virtualization (NFV) [6], is a new concept and an emerging network technology introduced. The primary objective of NFV is to eliminate hardware resources and provide networking services like routing, firewall, DNS, DHCP, etc. through a software- based virtual machine. Whereas in the dual-stack technique, new devices are supported to both functionalities of IPv4-IPv6 and can be communicated with both protocols easily. To support the IPv6 in the future, it is needed for ISPs to develop an independent and parallel IPv6 network with IPv4. It means, both protocols will co-exist for a long time during the transition.

By nature, the network topology is hybrid. The addressing method, compatibility issues, and operation methods of IP4 and IP6 are totally different [7]. Though, it generates a lot of problems for ISPs to translate IPv4 addressing techniques to IPv6 Network. During the changeover, it creates issues like security, traversing of the packet, scalability, and some performance-related problems faced by ISPs [8]. In packet traversing, the data communication is done by two IPv6 networks over an IPv4. For resolving such issues, the technique introduced is called Tunneling [9]. This technique is the only solution. The end nodes in tunneling implement dual IP layers in host and router means to support both IPv4 and IPv6 architecture called a dual-stack router. There are many techniques used in tunneling called static and dynamic [10]. In such techniques, static is suitable to implement while others are not in practice due to performance issues.

Routing is also a challenging task for network professionals when the network size is large, complex, heterogeneous, and scalable. Without a proper scalable routing system, a network does not provide better performance. The scalable routing system determines the best path from source to the destination quickly and efficiently if multiple paths exist in the large and complex network. Routing protocols are introduced to overcome routing and scaling issues. A variety of routing protocols is available for both IPv4 and IPv6 networks. IPv6 routing protocols are different from each other in terms of configuration, metrics, convergence speed, and other functionalities over IPv6 tunnels [11].

In any data network, the main risk is security. Even though the header of IPv6 offers incorporated security features which are able to decrease the Network threats, but still uncovered by many attacks, i-e Internet Control Message Protocol for IPv6 attack, Header attack for IPV6, and Reconnaissance Attack. The influence of some identified IPv4 attacks is not changed its appearance for the new IPv6 protocol. While, the attacks like sniffing, flooding, man-in-the-middle-attack (MITM) [12] can affect both IP addressing techniques (IPv4 and IPv6). It is required to change and design strong Network policies, and install some monitoring systems and implement some security tools like firewalls and IDS for external threats to reduce the security threats and minimize the risk.

The network functions which can be offered for NFV in case of firewalls, Storage Systems, Virtual Private Network (VPN), Gateways, DHCP, and Domain Name Service (DNS) can implement security in the course of software, not for hardware-based. The NFV architecture is comparatively reliable than a traditional architecture that can be suited for energy consumption, for some hardware, operating reliability, cost of equipment, and deploying of network topology [13].

2. COMPARISON BETWEEN IPV4 AND IPV6 HEADERS

The Internet Protocol is a routable protocol over the network. There is no surety to deliver a packet by IP. The IP Address tries its best to deliver a packet over the network in the best possible way through different routes [14]. Some application protocols such as FTP, SMTP, and HTTP have required a guarantee of packet delivery. The IP protocol is associated with TCP protocol on the transport layer to provide a guarantee of packet delivery services. The packets are moved on the network in an arbitrary path if multiple paths exist. On the network layer, a segment is encapsulated by an IP header before delivery. Source and destination IP addresses are enclosed in an IP header. The IANA has declared some blocks of IP address from different classes for private networking [15]. The 169.254.0.0/16 address is reserved for link-local addressing. All the reserved and private addresses are not routable over the Internet. The NAT was introduced to provide Internet access for private networks [20].

2.1 IPv4 Header

The majority of Network traffic is based on IPv4. In the IPv4 packet, the header and data unit is part of that packet. Before transmitting the packet over the network, the header of a minimum of 20 bytes is encapsulated with the Data Unit part of IPv4. The IPv4 header consists of 14 fields. Its maximum size is 60-bytes. One field is optional. The first4-bits of the header are version. It indicates the IP version used. A TTL8-bits field helps stop the packet from moving in the loop on the Internet. Whenever a packet arrives and crosses one node on the network, then its TTL field is decremented by one [16]. When the TTL field becomes zero, the node discards the packet. The header checksum 16-bits field is used for error checking of the header. When a packet reaches the router, the checksum of the header is calculated by the router. The router compares

both values. If the value does not match, the router discards the packet. The32-bits source and destination IP addresses fields are used to store the sender and receiver IP addresses, respectively. These addresses may be changed in transition by NAT devices.

2.2. About IPv6 Header

The most recent version for IP addressing is IPv6, which is supposed to be used for the coming generation. It is called 128-bit addressing architecture. Its total IP addresses can be calculated in 2^{128}, almost 3.4 x 10^{38} total IP addresses. Most repeated zeros can be reduced to double-colon [17]. Because of the large addressing volume, there is not necessary for Network Addressing Translation. However, some Addresses range can be reserved by its standard IANA.

In IPv6, a new multicast implementation technique has introduced. A new feature, Stateless Address Auto Configuration (SLAAC), is introduced in IPv6 to eliminate additional configuration servers. It allows a host to generate its own address using a combination of link-local addresses and information advertised by routers. IPsec is used as a built-in security feature in IPv6 with the help of the extension header [18]. It is a mandatory part of all IPv6 protocol implementation. The extension header carries optional information along with the IPv6 header. The extension header provides support for fragmentation. There are several types of extension headers.

The IPv6 header is simplified. Some fields are removed. It consists of only 8 fields. Its size is fixed, and that is 40-bytes. The first4-bits of the header is also version same as in IPv4. The TTL field is replaced with the 8-bits Hop Limit field. The Next Header 8-bits field in the fixed header indicates the type of the extension header. The size of the source and destination IP addresses fields are increased to 128-bits. The Flow Label20-bits field provides traffic engineering and QoS services.

3. VIRTUALIZATION IN NETWORKING

In the present era, by increasing the size of ISPs can increase the number of devices. Therefore, ISPs are continuously buying the physical items for increasing the size; as a result, the cost and electricity consumption is increasing. Virtualization concepts are introduced in networking for reducing energy consumption and expenditure costs for proprietary hardware.

3.1 Network Services Virtualization (NSV)

The Technique is effectively applied in some forms of virtual LAN, Virtual Router Redundancy Protocol, and virtual routing and forwarding. These NSV concepts are called virtualization and provide support after eliminating the hardware. VLANs is a subnetwork that can group collections of devices on separate physical local area networks (LANs). A single broadcast domain of the switch is separated into multiple broadcast domains through VLANs, which reduce the cost, split the size of the network into multiple networks, lessen broadcast traffic and improve security [19]. Similarly, VPNs provide a secure and logical connection over the public network by sending/receiving secure data over the public network with the use of VPNs. The VRRP provides availability and reliability with multiple redundant virtual routers as gateways on a single router for efficient traffic delivery. If one gateway is down, then the traffic is passed from another gateway [20]. The VRF technique creates multiple virtual routing tables in a single router. VRF splits a single router into multiple logical routers.

4. VMWARE INFRASTRUCTURE

The Dell Corporation is providing a VMware platform called for virtualization with the partnership of other companies to provide service. This VMware Workstation is used to manage IT Environment; it allows different users to set of connections of Virtual Machines (VMs) on a physical machine and communicate them simultaneously along with the original machine. A hypervisor is computer software or firmware used to create and run more than one VM as a guest machine on a physical machine. These VMs may run different types of guest operating systems like (Microsoft, Linux, and Mac) and share the virtualized hardware resources. Each VM can use up to 16-GB RAM and 4 CPUs with VMware Virtual Symmetric Multi-Processing (SMP). VMware offers a variety of software to provide “vServices” in terms of desktop computing, servers, cloud management, application management, storage management, networking, and security.

4.1 Cloud Computing

It is an on-demand technology that worked on virtualization concepts. It is a de facto standard based hosting and providing services to many users over the internet. This cloud computing technology has many

benefits over traditional techniques and adopting and implementing very fast by ISPs and end-users. More, it further benefits like saving cost, scheduling of jobs, energy efficiency, no limitation of storage, scalability, access ever time and anywhere of the globe, to tolerate the fault that occurs in the system. The next generation of cloud technology should be equipped with a mixture of traditional and non-traditional development [21], such as SDN, Nano Computing, Quantum Computing, Neuromorphic, etc.

5. CORE ISSUES DURING MOVING TOWARD NGN

The addressing method of IPv4 and IPv6 is totally different, which cannot be worked exchangeability. By using a dual-stack approach, the network became hybrid in nature. The co-existence of IPv4-IPv6 generated several core issues in different aspects. These issues are the main reason for decreasing the overall performance of ISPs. These issues are:

5.1. Packet Traversing

In the meantime, the Addressing Techniques, i.e., IPv4 and IPv6, are not well matched. The users or machine fit in the IPv4 method cannot communicate with the IPv6 technique. The two IPv6 networks cannot

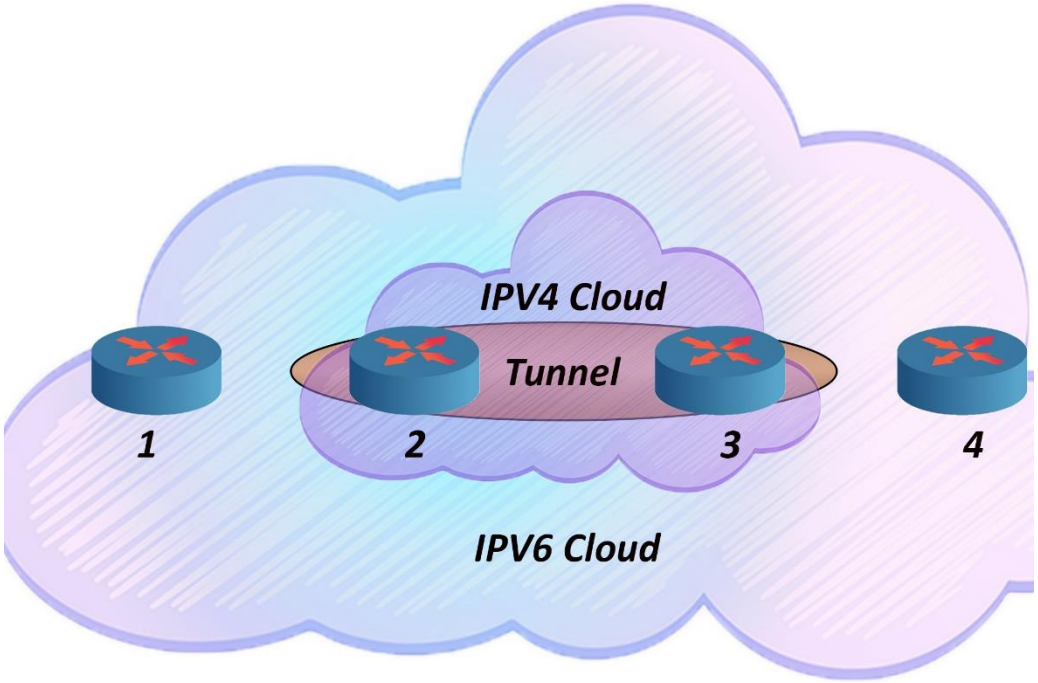

Fig. 1. Tunneling feature of IPv6

communicate with each other if the IPv4 network is involved between them. It creates a packet traversing issue. To resolve this issue, researchers adopted a smart solution. A tunnel is deployed when two IPv6 separate networks are directly connected with the IPv4 network and want communication with each other, as shown in Figure 1. In tunneling, a virtual connection is established between two networks over the middle of the network. Network-layer virtualization provides segregation to realize end-to-end connectivity. It joins two homogeneous networks through the virtual network [22]. It's a temporal solution until the entire network shifts to IPv6.

At the destination, the decapsulation process is executed. In the decapsulation process, it extracts the IPv4 header and delivers the originalIPv6 packet to its destination. It is used to achieve heterogeneous traversing. There are several IPv6 tunneling protocols like 6-in-4, 6-to-4, ISATAP, tredo, 6rd, 6over4, and GRE. These are different from each other in performance and configuration basis. The6in4, 6rd, and GRE tunneling protocols are static, while 6-to-4, 6over4, and ISATAP are dynamic. The static/ manual tunnel is a point-to-point while the automatic/dynamic tunnel is a point-to-multipoint. In the static tunneling method, source and destination IPv6 addresses of the tunnel are defined while in the dynamic method, the source address is assigned by the operator, and the destination address is found automatically [23]. The comparison of IPv6 tunneling protocols is shown in Table 1. The packet traversing issue is resolved by tunneling. Numerous research studies addressed IPv6 tunneling protocols in which researchers measured, compared, and analyzed the performance of the most common IPv6 tunneling protocols in the small and large sizes of VNs through different simulators.

Researchers concluded the results on the performance basis of theIPv6 tunneling protocols through different kinds of parameters such as convergence, throughput, jitter, end-to-end delay, RTT, and tunnel overhead. Detail comparison of the IPv6 tunneling protocols is displayed in Table 2. It shows that the performance of the 6-in-4 tunnel is better than all others in most of the above-mentioned parameters. Due to better performance, it is widely used. It is a static and point-to-point tunnel. Mostly, researchers measured the performance in a small size of VNs through simulators. Although IPv6 tunneling technique resolved packet traversing issue nevertheless it is not a secure virtual connection [24]. It is more vulnerable to a breach as compared to physical links. The IPv4/IPv6 source address of the encapsulating packet can be spoofed. The attacker can alter the encapsulated IPv6 packet anywhere on the Internet during transmission. With the wild development of IPv6 tunneling methods, certain types of attacks like tunnel injection, tunnel sniffing, reflector attack, and routing loop attack are noticed. To provide a secure virtual IPv6 connection, it is needed to combine the 6in4 tunnel with IPsec. The security association in IPsec is established to protect the traffic defined by IPv6-sourceand IPv6-destination during transmission over the Internet [25]. In this scenario, the tunnel's packet once again is encapsulated in the IPsec security header before the transition. On receiving end, two times decapsulation is performed. First for IPsec header and second is IPv6 tunnel's header that creates extra overhead for every tunnel's packet during encapsulation/decapsulation. A new IPv6 tunneling technique with security features needs to be addressed for reducing extra overhead with security features.

Table 1. IPv6 tunneling comparative analysis

IPv6 Tunnel	Advantages	Limitations	Deployment Pattern
6-in-4	Stable and simple link for regular communication. Easy to deploy. Allows transport of IPv6 packets over an IPv4 network. Available on most platforms	Management overhead. Must be manually configured	Site-to-site tunneling mechanism
6-to-4	It is site to multisite mechanism. Easy for IPv6 "islands" located in IPv4 networks.	Security Threats and vulnerabilities, the complexity of IPv4 and IPv6 in the routing table	Site-to-multisite tunneling
ISATAP	Low maintenance, easy incremental deployment of IPv6 to disparate nodes within AS (intra site) supported in many platform.	Monitoring of traffic is difficult works only over the intranet, can require more setup than other methods. Some security issues, designed for use within a local network only.	Designed for Intrasite use. Additional CPU load for encapsulation decapsulation
GRE	Generic support several types, can be used with routing protocol.	Firewall challenges (IP protocol type 47 for IPv4 datagram for inbound and outbound must be opened). Simple key authentication between the tunnel end point. Key transmitted in clear text.	For Site-to-site tunneling only.

Table 2. IPv6 tunnel comparative outcome details

IPv6 Tunnel	Routing	Convergence Speed (sec)	Throughput (kbps)	Jitter (ms)	End to end Delay (ms)	RIT (ms)	Routing Traffic sent (bps)	Tunnel Over Head (ms)
6to4	Static	X	468.83	0.0078	1.3103	0.719	X	X
ISATAP		X	495.11	0.0152	1.2427	0.551	X	X
6rd	Static	X	150.33	0.0912	2.7820	X	X	35.375
6to4		X	320.17	1.6779	4.5173	X	X	08.250
ISATAP		X	100.79	0.0010	0.0363	X	X	14.688
GRE		X	390.22	0.0004	0.8885	X	X	12.187
6to4	Static	0.00249	486.40	0.0225	1.3103	0.719	X	00.712
ISATAP		0.00226	497.02	0.0300	1.2427	0.551	X	00.568
6in4	RIPng	35.0	X	X	1.3103	X	80.00	X
6to4		8.9	X	X	1.2427	X	50.00	X
6in4	OSPFv3	23.3	X	X	30.150	8.230	33 (hello)	X
6to4		130.4	X	X	36.230	14.56	12 (hello)	X
ISATAP		38.4	X	X	31.730	13.04	11 (hello)	X

GRE	25.6	X	X	34.540	12.89	34 (hello)	x

5.2. Routing Scalability

The most necessary part of the network is routing. Lack of proper routing, the data cannot be sent to the destination host, and the network cannot function properly. The device named router decides to deliver the packet to the right machine after matching Mac with the routing table. If the path is matched from the table, then the destination host will receive data; otherwise, the packet will be discarded [26]. The routing table can store a large number of routes. A variety of routing protocols for IPv4 and IPv6 are available. The goal of routing protocol is to achieve accuracy, stability, redundancy, routing information integrity, manageable routing policy, and fast convergence. A comparison of IPv6 routing protocols is shown in Table 3. However, the routing process is performed by routing protocols. Routing protocols detect any change or failures easily if occurred in the network. IPv6 protocols are different in nature and performance. Researchers examined the performance of IPv6 routing protocols in small and medium sizes of networks through different simulators. Research studies may help ISPs to provide routing services on large scale next-generation virtualized IP networks. Detailed performance comparison of the IPv6 routing protocols on the basis of several parameters like convergence, throughput, jitter, packet loss, end-to-end delay, and RTT are displayed in Table 4.

Table 3. IPv6 related routing protocols

Routing Protocol	Advantages	Limitations	Type
RIPng	Easy to configure. Best for the small size of the network. Single table.	The maximum size is 15. Senda broadcast the routing table every 30 seconds. Flat network. The administrative distance is 120.	Distance vector. The Bellman-Ford algorithm is used to calculate the best path. Metric is hop count.
EIGRPv6	Maximum hop counts 256. Support VLSM. Support un-equal load balancing. Route Summarization. MD5 and SHA-2 authentication.	Multiple tables. Flat network. Higher routing overhead. Not scalable.	Hybrid. The DUAL algorithm is used to calculate the route. Metrics are bandwidth and delay. The administrative distance is 90.
IS-IS	Support VLSM. Support authentication. Hello, messages.	Not popular.	Link state. Dijkstra's algorithm is used to calculate the best route. The administrative distance is 115.
OSPFv3	Support VLSM, Support authentication. Open standard. Hello, messages. Sends only incremental changes. More scalable.	Multiple tables. Support equal load balancing. Difficult configuration.	Link state. Dijkstra's algorithm is used to calculate the best route. Cost is the metric. The administrative distance is 110.

Table IV shows the detailed comparison of different IPv6 routing protocols in small and medium sizes of VNs. In this comparison, the RIPng has an advantage over the rest of the IPv6 routing protocols in most of the parameters. RIPng is a distance vector routing protocol and is not used in the large network [27]. EIGRPv6 and OSPFv3 are the best choices for a larger network. EIGRPv6 is developed by CISCO as a proprietary but later on, declared as an open standard. It is best for the flat network. When the network is moving towards a decoupling of hardware and virtualized network, then OSPFv3 is a better choice for routing. It is an open standard and hierarchical model routing protocol proposed by IETF. OSPFv3 becomes industry standard and most widely deployed protocol on the Internet due to its open standard feature, hierarchical nature and Optimized Link State Routing (OLSR). Its design focused on scalability and robustness against failures. In OSPF, the routing domain is divided into multiple areas and limiting the processing overhead of the protocol. Due to its hierarchical nature, it is a more scalable routing protocol in Multi-Protocol Label Switching (MPLS) and NGN.

In traditional IP routing, the router determines the path incrementally based on the destination IP address. Another alternative connection-oriented routing technique based on label switching is called MPLS. Segment routing (SR) is also a modern and fast form of routing introduced by IETF. It is a variant of traditional IP routing. It works within MPLS and IPv6 networks. In segment routing, an IPv6 ingress node prepends a new type of header SRH (Segment Routing Header), which contains a list of segments. In the MPLS network, segments are encoded as labels. While in the IPv6 network, segments are encoded as a list of IPv6 addresses.

In a distributed control plane, the segments are allocated by OSPF or BGP. SR decreases the lookup delay at every router. As a result, network performance is increased. SR increases network scalability, efficiency, and rerouting.

Table 4. IPv6 comparative performance

Ref	Routing Protocol	Convergence Speed (sec)	Throughput (kbps)	Jitter (ms)	End to end Delay (ms)	RIT (ms)	Packet Loss (%)
[14]	EIGRPv6	13.0	X	X	57.0	45.0	X
	OSPFv3	21.0	X	X	72.0	51.0	X
[40]	EIGRPv6	163.6	X	X	X	35.5	3.6
	OSPFv3	180.6	X	X	X	43.4	7.0
[41]	IS-IS	45.0	X	X	X	X	X
	OSPFv3	47.0	X	X	X	X	X
[42]	RIPng	X	856.3	6.5	13.1	X	X
	OSPFv3	X	775.2	303.9	629.2	X	X
[43]	RIPng	X	537.7	16.5	X	X	20.4
	EIGRPv6	X	714.1	14.2	X	X	2.5
	OSPFv3	X	674	15.9	X	X	2.7
[44]	RIPng	X	930.0	43.0	X	X	5.0
	EIGRPv6	X	920.0	47.0	X	X	6.0
	OSPFv3	x	820.0	58.0	X	x	14.2

The researcher [28] presents their design and implementation of routing function in a virtualized mode over an Open Flow network. Open Flow is the most common configuration protocol for enabling Software Defined Network (SDN) architecture. The SDN is a programmable network approach that separates the control plane and forwarding plane through standardized manners. It defines two types of communication devices. One is the controller, and the second is a switch. The controller handles the network forwarding elements while the switch is accountable for packet forwarding. The researchers emphasize the idea of routing service as NFV over an Open Flow network. The researchers achieved benefits on the basis of reducing routing devices, configuration, space, costs, energy consumption, and deployment time. By increasing the number of requests, the RTT lasts stable in unrelated proposed method extracted from the experiment. The performance and scalability are assured. More evaluations are needed to determine the robustness of the virtualized functions.

5.3. Network Performance Guarantee

The Virtualization of Network is a model to tackle different network challenges within a traditional network by decoupling the hardware by leveraging. It provides general-purpose services, such as servers, storage, switches, controllers, and security, through software implementation along with several emerging technologies like NFV, SDN, and cloud computing. Virtualized Data Center (VDC) provides better management flexibility, lower cost, scalability, better resource utilization, and energy efficiency through NFV. There are several technical challenges to network operators such as, how to migrate from the large scale as tight coupling exists in network infrastructure to NSV-based solutions smoothly and how to make sure the guarantee of network performance for virtual appliances during migration. Commercial data centers process a variety of services such as web services, real-time applications, gaming, audio, and video live streaming, etc. that demand high network bandwidth. It is the primary job of network operators to provide a guarantee of services to users and satisfy them. When moving towards virtualized technology implementation, network operators are reluctant due to performance issues throughput and latency. Virtualized data centers are capable of overcoming throughput and delay challenges. It divides a data center network into numerous logical networks. These logical networks independently achieve performance objectives. To achieve a guarantee of performance in virtualized data centers, multiple recommended architectures, namely, Second Net, Oktopus, Gatekeeper, Cloud NaaS, and Seawall, are available.

- **Second Net**: In [29], researchers offered Second Net VDC architecture as a resource allocator for multiple tenants in cloud computing. It provides service variation, computation, storage, and bandwidth guarantee among multiple VMs to define three basic service types type 0, type 1, and type 2, respectively. Type 1 service deals bandwidth guarantee. It is a highly scalable architecture and supports up to 232 VMs and achieves high scalability by distributing all the virtual-to-physical mapping, routing, and the bandwidth reservation from switches to server hypervisors. The authors designed architecture, implemented it on a simulated test-bed, and evaluated the performance. The designed algorithm achieved high network operations during experiments with low time complexity. Some limitations are highlighted in SecondNet architecture. First, its performance depends upon the physical arrangement of the network. Second, it does not consider the latency associated with the performance of the network.

- **Oktopus**: In [30], researchers developed a new Oktopus architecture to prove the practicability of VNs. It depends on two proposed VN abstraction. It captures the exchange between the performance guarantees offered to multi-tenants and costs. It increases the performance of applications and provides better flexibility. In this architecture, renters find stability between higher application performance and lower cost. Renters are involved in metrics like reliability, bandwidth, and latency between VMs and failure resiliency of the path between VMs. The researchers deployed it on a 25-node two-tier test-bed through simulation. Researchers confirmed that abstraction is a practical, better approach. Moreover, they find out that abstractions can reduce tenant costs by up to 74%. The limitation of Oktopus is the support of tree topologies, and research is needed on implementation for other types of topologies.

- **Gatekeeper**: The researchers focused on the problem related to network performance segregation [31], and designed a new model named Gatekeeper. The solution should be scalable, on the basis of the quantity of VMs, expected performance, robust against malicious behaviors of tenants. Gatekeeper architecture emphasizes on providing assured bandwidth among VMs in multi-tenant data centers by attaining a high bandwidth consumption. It is a point-to-point protocol and generates one or more logical switch, which is connected with VMs who belong to the same tenant. The degree of incoming traffic is monitored by the virtual NIC (vNIC) of each receiving VM through different counter's set. If congestion occurs during the transmission process, the sender's vNIC is informed. The traffic controller uses this information and tries to control the traffic rate resulting in the level of congestion to be reduced. Researchers implemented a Gatekeeper prototype with 2 tenants and 6 physical machines; their results showed that Gatekeeper works well within simple scenarios. Gatekeeper does not focus on latency and still under progress.

- **Cloud NaaS:** It is a VN architecture; thereby, professionals deploy and manage enterprise applications in clouds in a well-organized way by using this architecture [32]. The researchers designed, presented, implemented, and evaluated a networking framework model of the cloud. The model provides the facility to deploy their applications on the cloud to access VNFs. It also gives permission to deploy a variety of middlebox appliances. The authors demonstrated the flexibility of Cloud NaaS in the cloud using a multi-tier application model in test-bed with commercial Open Flow enabled network devices to support several network functions. In this model, several techniques are used to reduce the number of entries in each switch. It uses a single path for traffic delivering and few paths for QoS traffic based on the type of service. It uses wildcard bits for aggregation IP forwarding entries. The results show that Cloud NaaS performs well in large numbers of provisioning requests. The limitation of Cloud NaaS is the use of limited paths for QoS.

- **Seawall:** Seawall is another bandwidth allocation architecture [33] that defines a mechanism of how the bandwidth will be shared among multiple tenants in virtualized data centers. The researchers presented Seawall, which is a bandwidth allocation system. It divides the network size according to a specified policy set by the administrator. It assigns weights to each VN and process. It allocates bandwidth according to weights. Congestion-control tunnels are used for bandwidth sharing between pairs of networks. For improving efficiency in Seawall, the end-to-end congestion control technique could be used. After the evaluation of the Seawall prototype, the researchers observed that it adds little overhead and achieves strong performance isolation. It does not address failures explicitly. The first prototype of Seawall was implemented on Windows 7 and Hyper-V.

Detailed quantitative comparisons of the architectures mentioned above based on the forwarding scheme, bandwidth guarantee, scalability, QoS, and deployment ability factors are summarized in Table 5.

Table 5. Quantitative comparison

Architecture	Forwarding Scheme	Bandwidth Guarantee	Scalability	QoS	Deployment ability
SecondNet	V	V	High	V	High
Oktopus	X	V	High	V	High
Gatekeeper	X	V	High	V	High
CloudNaaS	V	V	High	V	High
Seawall	X	X	High	X	High

In Table 5 comparison, all the architectures provide QoS in VNs except Seawall. QoS is measured after the calculation of the network performance. It purely focuses on technology-driven perspective measurement. It is evaluated using classical network performance metrics such as latency, jitter, and throughput. QoS and application-specific performance metrics are quantitative. QoS is achieved in all VN architectures except Seawallby allocating bandwidth for each virtual link. The Seawall shares bandwidth among tenants on the basis of weights. It does not provide guaranteed bandwidth allocation and does not expect performance. It is needed to focus on a new performance paradigm along with QoS, and that is Quality of Experience (QoE).

- **QoE:** QoE is positive feedback given by users based upon services provided by a system. User feedback is dependent on how much the user is satisfied in terms of usability, accessibility, and integrity of the QoS. It is measured by surveys and Means Opinion Scores (MOS) methods. It is qualitative. It is not only based on QoS but also based on non-technical aspects, such as end-user feelings and reactions. Nowadays, national or International service provider companies inquire about user's satisfactory level after their services by directly engaging users with the help of different online applications. Overall, the quality of the system is dependent on both QoS and QoE. Multi-user may have perceived different qualities provided by the same service on the same system. Practically, the calculation of QoE is a more challenging task due to the dependency on three factors. First, the human influence factor is based on age, gender, and user's mood. Second, the system influence factor is based on the responsiveness of the system, bandwidth, delay, jitter, screen resolution, packet loss, and display size, etc. Third, context influences factors are based on location, time, interpersonal relations, and economic context. QoE is an emerging multidisciplinary field. It is an important metric in the design and implementation of video streaming systems. In video streaming systems, due to high traffic demands and worst network performances may highly affect the user's experience. In live audio/video streaming and online game applications, packet loss affects QoE.

5.4. Security

Security plays a vital role in any Network where IPv6 provides a built-in security feature. Despite these security facets, the IPv6 network faces many challenges; the challenges in IPv6 are some new types of attacks. Network security is a significant issue, especially when moving towards virtualized NGN and during the co-existence of IPv4-IPv6 networks. Some kind of attacks affected both IPv4-IPv6 architectures and did not discriminate by appearance. A few examples of such kind of attacks are sniffing attacks, flooding attacks, man-in-the-middle attacks, and application-layer attacks. A set of attacks with countermeasures are shown in Table 6.

Table 6. Threats preventive measures

Threat Name	IPv4	IPv6	Countermeasure
Sniffing Attack	V	V	IPsec
Flooding Attack	V	V	IPs
Man-in-the-Middle Attack	V	V	Encryption and Hashing
Viruses Attack	V	V	Anti-virus
Reconnaissance Attack	X	V	Firewall and IPS
IPv6 Routing Header Attack	X	V	Firewall
ICMPv6 Attacks	X	V	Firewall

In a sniffing attack, an intruder can easily capture private data sent in plain text form with the help of some sniffer tools during transmission over the network. A sniffing attack can be avoided by using proper encryption techniques. Several encryption techniques, like DES, 3DES, and AES are available for data

confidentiality. In a flooding attack, the attacker hits network devices, routers, and servers. The network device is engaged with a large amount of network traffic and became out of service. It is also called a DoS attack. A proper IPS is used to avoid a DoS attack. In a man-in-the-middle attack, an intruder can easily capture data, alter it, and then transmit to its destination if data is not secure. IPv6 header has no security mechanism itself. The hashing technique is used to attain data integrity. Hashing and encryption algorithms are used within the IPsec protocol to protect data from intruders during transmission. The attacks in the application layer are the most common attacks in both IPv4 and IPv6 networks. Different types of viruses and worms tried to destroy data. Updated anti-virus software is installed to avoid these types of attacks. However, IPv6 introduced and implemented a built-in security feature in the form of an extension header. Some new security threats directly related to IPv6 networks arise. Some of them are:

- Reconnaissance Attacks: In this type of attack, an intruder collects essential data about the targeted network by using investigation and engaging with systems. The intruder uses different approaches, such as active methods, different scanning techniques, or passive data mining, for gathering information. This information can use in further attacks. The intruder tries to trace IP addresses, which are used in a network with the help of "PING sweeps". The "PING" command helps to find out an accessible system and port scanning. The larger subnet size of the IPv6 and some type of multicast addresses are helped to identify resources in the network easily. A software tool "Nmap" is used to discover hosts and services. Attacker misuses such kind of tools. Reconnaissance attacks can be mitigated to perform the following methods. A suitable IPS is deployed at the border. IPv6 packet filtering is also applied where applicable. When using DHCPv6, avoid using sequential addresses. Configured MAC addresses manually when VM is employed.
- ICMPv6 Attacks: In IPv6 networks, the neighbor discovery mechanism depends on some types of ICMPv6 messages. Therefore, we cannot block ICMPv6 messages completely the same as in IPv4. We need to allow some types of ICMPv6 messages for proper network operations. It can be misused for an attacker. ICMPv6 attacks can be mitigated to enforce a proper IPv6 packet filtering technique.
- IPv6 Routing Headers: All nodes of IPv6 are capable of processing, routing headers according to the IPv6 protocol. An attacker sends a specific packet containing a "forbidden" address in routing headers to access hosts through bypass the network security devices. The accessible host will forward the packet to a destination address even though that destination address is filtered. This publicly accessible host can easily use a DoS attack by an intruder. Mobile IPv6 requires routing headers. Enforcing a firewall can be mitigated attacks.
- Security Issues during Transition: In conjunction with each other has been solved by Dual Stack and Tunneling Methods. In Dual stack, IPV4 and IPv6 work at the same period and at the same time, two separate tables are being maintained. The packets of every addressing technique are sent to their respective mode. This dual-stack has two categories; the first one is to maintain both IPv4 and IPv6 but does not support Tunneling, while the second one provides Tunneling support. The IPv4 and IPv6 are also facing the vulnerability of attacks in dual-stack, while tunneling mechanism has the possibility to misuse. The intruder can avoid entering filtering the checkup. So the network address IPv4 or IPv6 can be hacked and used for Daniel of Service Attacks.

Network designers and security specialists need to understand the security implications of transition mechanisms. To minimize the security threats during the co-existence of IPv4-IPv6 networks, dedicated security appliances such as firewalls and IPS are used in networks. When firewall actives, then tunneling traffic may be blocked. Security specialist enables tunneling traffic by using protocol field value that is 41. The NFV allows network functions to be accomplished in VMs rather than in dedicated devices. When different Virtual Machines (VMs) share the resources, the vigor issues and different attacks may increase. These attacks are two types the first types are network-based security challenges, and the others are VM related issues. Network function-specific threats refer to attacks on network functions or resources, for example, spoofing, sniffing, and DoS. These threats are related to the attacker's abilities and physical agreement of the network. To overcome these threats by using packet filtering firewalls and IDS. General virtualization-related threats refer to security issues related to virtualized infrastructure. Physical infrastructure is shared virtually among multiple entities and brings new security vulnerabilities. The infrastructure of NFV is divided into three domains: computing domain, hypervisor domain, and network domain. Security threats related to these domains are in the following section.

- Computing Domain: Computing domain refers to generic servers and storage. In this domain, multiple VMs can be shared CPU and memory of physical infrastructure. It creates a high risk of data vulnerability. Data should be encrypted and accessed only by the VNFs to overcome security threats in this domain.
- Hypervisor Domain: Hypervisor domain moves the physical machines to the VMs. In this domain, unauthorized access and data leakage are security threats. A protected hypervisor should be used to prevent any unauthorized access or data leakage. Isolation of the served VM's space and VMs are only available to authentication controls.
- Network Domain: Network domain manages the VNFs, which refers to shared logical-networking layers (vSwitchesandvRouters) and shared physical NICs. It creates security threats due to sharing multiple logical network layers against a single physical NIC. To overcome security threats by adopting secured networking techniques such as TLS, IPsec, or SSH.

6. INCREDULOUS PERFORMANCE

A meticulous performance result has been achieved by transferring a data file over IPv6 and IPv4. It can be shown that during the transfer of data, the IPv6 protocol created a higher deletion level compared to IPv4, as seen in Figure 2. It has been analyzed that IPv4 is still generally faster than IPv6, but for a significant fraction of measurements, IPv6 is the faster protocol. Further, the size of the file transfer data itself also affects the speed performance both on IPv6 and IPv4. Several variables might affect and lower the output during file transfer over IPv6 tunneling compared to IPv4, which are:

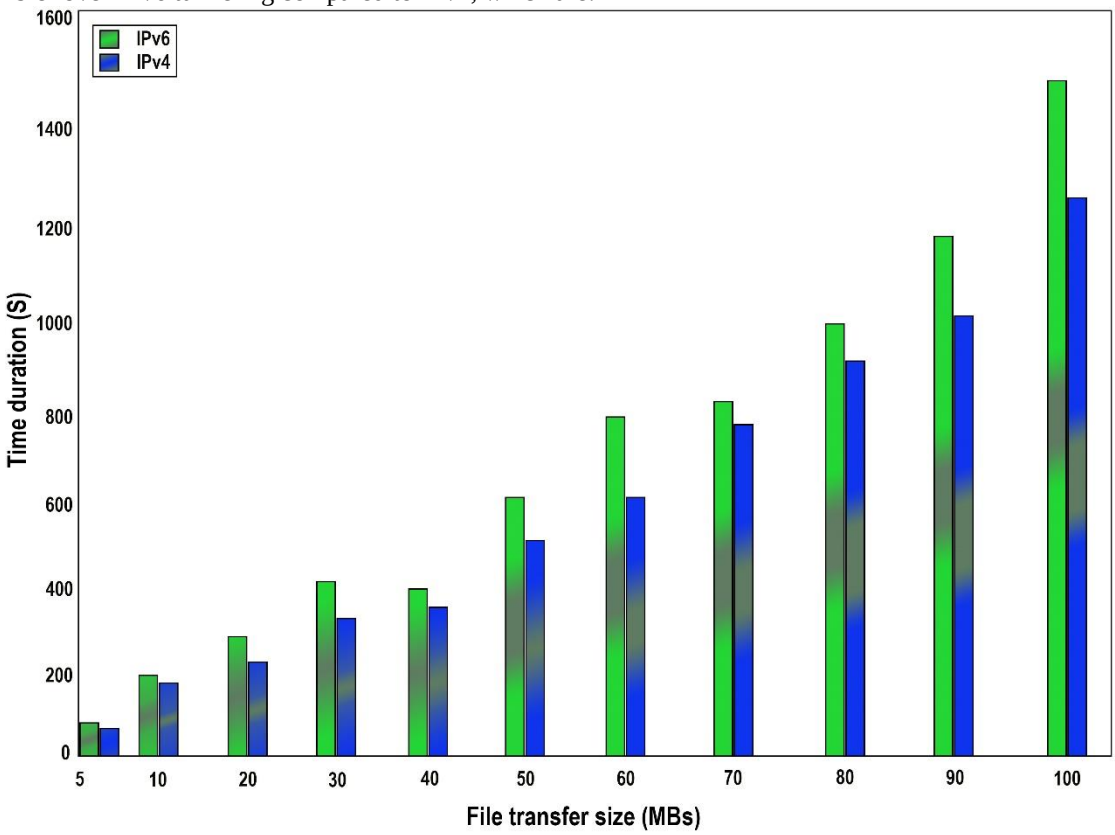

Fig. 2. Performance metric of IPv6 over IPv4 during file transfer

- Packet header size: the packet header size for IPv6 is much wider than the IPv4 standard. The implementation of IPv6 therefore introduces concerns related to extended packet headers. In this situation, the IPv4 packet header size is multiplied from 20 bytes to at least 40 bytes of IPv6.
- Number of hops: the number of hops often impacts and therefore decreases the efficiency as the file size moves down the network route to the expected destination. In fact, the main cause of this delay is due to factors such as serialization, packetization, coder, and propagation, dejitter buffer and processing.

7. CONCLUSIONS

IPv6 launched as the next-generation Internet protocol with several new features. ISPs have no choice to shift their existing traditional IPv4 network towards IPv6. A traditional network is based on proprietary hardware, and it provides services through dedicated devices. It increases the expenditure costs, high electricity consumption, difficult management, and controlling services. The virtualization paradigm is introduced in networking to overcome all the issues present in the physical network. The NFV idea was projected as a new emerging technology to design, deploy, and manage networking services with lower cost and lower energy consumption through the decoupling of physical proprietary network equipment. It also provides many benefits in terms of openness of platforms, improved operating performance, operation efficiency, scalability, and flexibility. The network operators are trying to shift the traditional IPv4 physical network to a virtualized IPv6 network. The infrastructure and architecture of these two types of network models are different. The transition process is slow and cannot attain in a short time due to billions of devices all over the world. Therefore, IPv4 and IPv6 will co-exist for a long time. The co-existence has created several core issues like packet traversing, routing scalability, a guarantee of network performance, and security during the transition. In this comprehensive survey, we focused on all these challenges during the transition process and provided corresponding solutions. Moreover, we highlighted limitations in all these corresponding solutions and suggested some new research directions.

REFERENCES

[1] C.-H. Chen, Y.-A. Lin, W.-T. Wu, Y.-T. Huang, and C.-C. Chu, "Design and Implementation of IPv4 and IPv6 Provisioning Technologies for VPC Architecture," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Sep. 2019, pp. 1–4, doi: 10.23919/APNOMS.2019.8892911.

[2] S. Ashraf, M. Gao, Z. Chen, S. Kamran, and Z. Raza, "Efficient Node Monitoring Mechanism in WSN using Contikimac Protocol," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, 2017, doi: 10.14569/IJACSA.2017.081152.

[3] R. K. CV and H. Goyal, "IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark," in *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, Mar. 2019, pp. 1–6, doi: 10.1109/ViTECoN.2019.8899746.

[4] X. Shen *et al.*, "AI-Assisted Network-Slicing Based Next-Generation Wireless Networks," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 45–66, 2020, doi: 10.1109/OJVT.2020.2965100.

[5] S. Ashraf, S. Saleem, A. H. Chohan, Z. Aslam, and A. Raza, "Challenging strategic trends in green supply chain management," *Int. J. Res. Eng. Appl. Sci. JREAS*, vol. 5, no. 2, pp. 71–74, 2020. Online

[6] R. Casellas, R. Vilalta, R. Martínez, and R. Muñoz, "Highly available SDN control of flexi-grid networks with network function virtualization-enabled replication," *IEEEOSA J. Opt. Commun. Netw.*, vol. 9, no. 2, pp. A207–A215, Feb. 2017, doi: 10.1364/JOCN.9.00A207.

[7] S. Ashraf, T. Ahmed, A. Raza, and H. Naeem, "Design of Shrewd Underwater Routing Synergy Using Porous Energy Shells," *Smart Cities*, vol. 3, no. 1, pp. 74–92, Feb. 2020, doi: 10.3390/smartcities3010005.

[8] X. Wu *et al.*, "State of the Art and Research Challenges in the Security Technologies of Network Function Virtualization," *IEEE Internet Comput.*, vol. 24, no. 1, pp. 25–35, Jan. 2020, doi: 10.1109/MIC.2019.2956712.

[9] S. Blawid, D. Neves, and R. Moura, "Exploring Quantum Tunneling in Ultrathin Transistors with Multiple Top Gates," in *2020 IEEE Latin America Electron Devices Conference (LAEDC)*, Feb. 2020, pp. 1–4, doi: 10.1109/LAEDC49063.2020.9072965.

[10] S. Ashraf, T. Ahmed, S. Saleem, and Z. Aslam, "Diverging Mysterious in Green Supply Chain Management," *Orient. J. Comput. Sci. Technol.*, vol. 13, no. 1, pp. 22–28, May 2020, doi: 10.13005/ojcst13.01.02.

[11] J. Beeharry and B. Nowbutsing, "Forecasting IPv4 exhaustion and IPv6 migration," in *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Aug. 2016, pp. 336–340, doi: 10.1109/EmergiTech.2016.7737362.

[12] S. Ashraf and T. Ahmed, "Dual-nature biometric recognition epitome," *Trends Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 008–014, Jun. 2020, doi: 10.17352/tcsit.000012.

[13] S. S. Kolahi, V. S. Hora, A. P. Singh, S. Bhatti, and S. R. Yeeda, "Performance Comparison of Cloud Computing/IoT Virtualization Software, Hyper-V vs vSphere," in *2020 Advances in Science and Engineering Technology International Conferences (ASET)*, Feb. 2020, pp. 1–6, doi: 10.1109/ASET48392.2020.9118185.

[14] G. Liu, W. Quan, N. Cheng, H. Zhang, and X. Shen, "VLI: Variable-Length Identifier for Interconnecting Heterogeneous IoT Networks," *IEEE Wirel. Commun. Lett.*, pp. 1–1, 2020, doi: 10.1109/LWC.2020.2982641.

[15] S. Ashraf and T. Ahmed, "Machine Learning Shrewd Approach for an Imbalanced Dataset Conversion Samples," *J. Eng. Technol. JET*, vol. 11, no. 1, Jun. 2020, Accessed: Jul. 05, 2020. Online

[16] N. Roddav, K. Streit, G. D. Rodosek and A. Pras, "On the Usage of DSCP and ECN Codepoints in Internet Backbone Traffic Traces for IPv4 and IPv6," 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909187

[17] F. K. Al-Fayyadh, "Performance of Wireless Network IEEE 802.11 under Dual-Stack Environment," in *2018 International Conference on Engineering Technology and their Applications (IICETA)*, May 2018, pp. 13–18, doi: 10.1109/IICETA.2018.8458070.

[18] S. Ashraf, Z. A. Arfeen, M. A. Khan, and T. Ahmed, "SLM-OJ: Surrogate Learning Mechanism during Outbreak Juncture," *Int. J. Mod. Trends Sci. Technol.*, vol. 6, no. 5, pp. 162–167, May 2020, doi: 10.46501/IJMTST060525.

[19] A. Khatiri and G. Mirjalily, "Resource Balanced Service Chaining in NFV-enabled Inter-Datacenter Elastic Optical Networks," in *2020 12th International Conference on Knowledge and Smart Technology (KST)*, Jan. 2020, pp. 168–171, doi: 10.1109/KST48564.2020.9059321.
[20] S. Ashraf, A. Raza, Z. Aslam, H. Naeem, and T. Ahmed, "Underwater Resurrection Routing Synergy using Astucious Energy Pods," *J. Robot. Control JRC*, vol. 1, no. 5, 2020, doi: 10.18196/jrc.1535.
[21] A. Sharma, "Mission Swachhta: Mobile application based on Mobile Cloud Computing," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 133-138. doi: 10.1109/Confluence47617.2020.9057926
[22] M. Welzl, S. Islam, R. Barik, S. Gjessing, and A. Elmokashfi, "Investigating the Delay Impact of the DiffServ Code Point (DSCP)," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2019, pp. 612–616, doi: 10.1109/ICCNC.2019.8685538.
[23] S. Ashraf, Z. Aslam, A. Yahya, and A. Tahir, "Underwater Routing Protocols Analysis of Intrepid Link Selection Mechanism, Challenges and Strategies," *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 8, no. 2, pp. 1–9, Apr. 2020, doi: 10.26438/ijsrcse/v8i2.19.
[24] S. Mehraban, Komil. B. Vora, and D. Upadhyay, "Deploy Multi-Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF)," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, May 2018, pp. 543–548, doi: 10.1109/ICOEI.2018.8553949.
[25] S. Ashraf, A. Ahmad, A. Yahya, and T. Ahmed, "Underwater routing protocols: Analysis of link selection challenges," *AIMS Electron. Electr. Eng.*, vol. 4, no. 3, pp. 234–248, 2020, doi: 10.3934/ElectrEng.2020.3.234.
[26] P. L. Ventre, M. M. Tajiki, S. Salsano and C. Filsfils, "SDN Architecture and Southbound APIs for IPv6 Segment Routing Enabled Wide Area Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 4, pp. 1378-1392, Dec. 2018, doi: 10.1109/TNSM.2018.2876251.
[27] S. Ashraf, M. Gao, Z. Mingchen, T. Ahmed, A. Raza, and H. Naeem, "USPF: Underwater Shrewd Packet Flooding Mechanism through Surrogate Holding Time," *Wirel. Commun. Mob. Comput.*, vol. 2020, pp. 1–12, Mar. 2020, doi: 10.1155/2020/9625974.
[28] N. M. Tri and M. Tsuru, "Locating Deteriorated Links by Network-Assisted Multicast Proving on OpenFlow Networks," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2019, pp. 1–6, doi: 10.1109/ISCC47284.2019.8969739.
[29] F. Yan, T. T. Lee, and W. Hu, "Congestion-Aware Embedding of Heterogeneous Bandwidth Virtual Data Centers with Hose Model Abstraction," *IEEEACM Trans. Netw.*, vol. 25, no. 2, pp. 806–819, Apr. 2017, doi: 10.1109/TNET.2016.2606480.
[30] Z. Shao, K. Zhang, and H. Jin, "Improving fairness of network bandwidth allocation for virtual machines in cloud environment," in *2016 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Jun. 2016, pp. 1–5, doi: 10.1109/BlackSeaCom.2016.7901600.
[31] K. Cassady *et al.*, "Network segregation varies with neural distinctiveness in sensorimotor cortex," *NeuroImage*, vol. 212, p. 116663, May 2020, doi: 10.1016/j.neuroimage.2020.116663.
[32] T. Benson, A. Akella, A. Shaikh, and S. Sahu, "CloudNaaS: A Cloud Networking Platform for Enterprise Applications," *SOCC '11: Proceedings of the 2nd ACM Symposium on Cloud Computing*, pp. 1-13, October 2018. doi: 10.1145/2038916.2038924
[33] Da Fonseca, Nelson LS, and Raouf Boutaba, eds. Cloud services, networking, and management. John Wiley & Sons, 2015. Online

BIOGRAPHY OF AUTHORS

SHAHZAD ASHRAF received B.E. degree in Computer Systems Engineering, and M.E. in Communication System and Networks from Mehran Engineering & Technology University, Jamshoro Pakistan in 2004, and 2014 respectively. He got Ph.D. degree in Information and Communication Engineering with the College of Internet of Things of Engineering, Hohai University Changzhou China in 2018. From 2005 to 2016, he served as an Assistant Professor at NFC Institute of Engineering and Technology Multan, Pakistan.

His area of interest includes computer engineering, wireless communication, robotics and control, signal processing, grid and distributed computing, computer hardware and networks, vector graphics designing, artificial intelligence, machine learning, neuro-fuzzy systems, computer architecture, solid state devices, and web engineering.

He is an active and prominent reviewer of many renowned international journals including IEEE Access, ACM, wireless personal communications, IET, IETE, international journal of distributed sensor networks, international journal of microwave and wireless technologies, journal of robotics and control, international journal of data science and analytics, international journal of computers & technology, Technium: romanian journal of applied sciences and technology, iran journal of computer science, international arab journal of

information technology, emerald: sensor review, international journal of pervasive computing and communications, journal of engineering and technology, i manager: journal on wireless communication networks, international journal of advanced research in computer and communication engineering, advances in science, technology and engineering systems journal, and IGI global.

DURR MUHAMMAD received BSc degree in Computer Systems Engineering from NFCIET Multan, Punjab, Pakistan and M.E. in Electronic Systems Engineering from Mehran Engineering & Technology University, Jamshoro Pakistan in 2009 and 2014 respectively. He is currently working as Assistant Executive Engineer in Pakistan Steel Mills Karachi, Pakistan which is a country large Industrial Complex of Pakistan and previously worked as visiting Instructor in Dadabhoy Institute of Higher Education Karachi, Pakistan from Jan-2014 to 29th of October 2016.
His Area of Research is Computer Networks and Data Communication, Information Systems Security, Computer Architecture and organization, Wireless Sensor Networks, pervasive computing and communications, robotics and control and Network Automation. He is also a Cisco Certified Network Associate in routing and switching and Network Security.

ZEESHAN ASLAM received B.E degree in Electrical (Computer System) Engineering from Bahauddin Zakariya University, Multan and M.S in Electrical (Power) Engineering from Institute of Southern Punjab Multan in 2015, and 2018 respectively. He is currently serving as a Site HSE Manager in Petroweld Oilfield Services Kurdistan region Iraq since 2019.He served as an Electrical and HSE Engineer in Volka Food International Multan Pakistan as an Electrical Engineer from 2015-2019. He also served as a Visiting Faculty in NFC Institute of Engineering and Technology Multan, Pakistan 2017-2018.