Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network

Zeeshan Ashraf
Department of Computer Science and IT, The University of Chenab, Pakistan
zeeshan.np@gmail.com

Adnan Sohail
Department of Computing and Technology, IQRA University, Pakistan
adnan.sohail@iqraisb.edu.pk

Sohaib Latif
Department of Computer Science, Anhui University of Science and Technology, China
sohaib.latif@aust.edu.cn

Abdul Hameed
Department of Computing and Technology, IQRA University, Pakistan
hameed@iqraisb.edu.pk

Muhammad Yousaf
Department of Cyber Security, Riphah International University, Pakistan
muhammad.yousaf@riphah.edu.pk

Abstract: *The rapid proliferation of the Internet has exhausted Internet Protocol version 4 (IPv4) addresses offered by Internet Assigned Number Authority (IANA). The new version of the IP i.e. IPv6 was launched by Internet Engineering Task Force (IETF) with new features, such as a simpler packet header, larger address space, new anycast addressing type, integrated security, efficient segment routing, and better Quality of Services (QoS). Virtualized network architectures such as Network Function Virtualization (NFV) and Software Defined Network (SDN) have been introduced. These new paradigms have entirely changed the way of internetworking and provide a lot of benefits in multiple domains of applications that have used SDN and NFV. ISPs are trying to move from existing IPv4 physical networks to virtualized next-generation IPv6 networks gradually. The transition from physical IPv4 to software-based IPv6 is very slow due to the usage of IPv4 addresses by billions of devices around the globe. IPv4 and IPv6 protocols are different in format and behaviour. Therefore, direct communication between IPv4 and IPv6 is not possible. Both protocols will co-exist for a long time during transition despite the incompatibility issues. The core issues between IPv4 and IPv6 protocols are compatibility, interoperability, and security. The transition creates many challenges for ISPs during shifting the network toward a software-based IPv6 network. Packet traversing, routing scalability, the guarantee of performance, and security are the main challenges faced by ISPs. In this research, we focused on a qualitative and comprehensive survey. We summarize the challenges during the transition process, recommended appropriate solutions, and an in-depth analysis of their mitigations during moving towards the next-generation virtual IPv6 network.*

Keywords: *QoE, SDN, NFV, segment routing, security*.

Received November 16, 2019; accepted December 6, 2020
https://doi.org/10.34028/iajit/20/1/9

1. Introduction

Network technologies are constantly evolving. With the fast development of the Internet of Everything (IoE), the Internet is growing all over the world quickly in the last few years. Over the last decade, due to fast changes in technologies, millions of 4G and 5G supported mobile devices became part of the Internet. The speedy proliferation of the Internet increased the demand for a unique IP address for individual devices [75]. Home users are connected to the Internet through smartphones to enjoy different services. Internet Protocol version 4 (IPv4) is a 32-bit architecture and can only provide 4 billion IP addresses. The ISPs faced difficulties to provide Internet access to new users. Internet Assigned Number Authority (IANA) officially declared that IPv4 addresses have ended [39]. 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 Quality of Services (QoS) [24]. It is a 128-bit architecture and can provide undecillion IP addresses. It is said to be a next-generation IP protocol. Both IPv4 and IPv6 protocols are different in format and behavior and cannot communicate directly with each other. ISPs are moving towards Next Generation Network (NGN) progressively and the changeover process is very sluggish due to billions of devices working throughout the world. Therefore, it is not possible to replace all the networks with a new IPv6 at once in a short time. According to a Google survey report [40], after over 25 years, the transition process is 35 % 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, etc altogether increases the economic cost [37]. The dual-stack technique and virtualized network architectures such as Network Function Virtualization (NFV) and Software Defined Network (SDN) are introduced to overcome the financial factor. The NFV is a new paradigm and an emerging network technology introduced in 2012 [57]. The primary objective of NFV is to eliminate hardware resources and provide networking services like routing, firewall, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), etc through a software-based virtual machine. Whereas in the dual-stack technique, new devices are supported to both functionality of IPv4-IPv6 and can be communicated with both protocols easily [53]. To support IPv6 in the future, it is needed for ISPs to develop an independent and parallel IPv6 network with IPv4. It means, that both protocols will co-exist for a long time during the transition.

Currently, the network is hybrid. Both IPv4-IPv6 protocols are different in their architecture. Compatibility and interoperability are the core issues between IPv4-IPv6 protocols [46]. Therefore, it creates many challenges for ISPs to shift the existing IPv4 network towards a software-based IPv6 network. Packet traversing, routing scalability, a guarantee of performance, and security are the main challenges faced by ISPs during the transition process [54]. In packet traversing, communication is between two IPv6 networks over an IPv4 network. The tunneling technique is introduced to resolve the packet traversing issue [6]. Tunneling is a provisional solution. In tunneling, both end nodes are dual-stack routers. There are numerous IPv6 tunneling techniques. Some tunneling techniques are static while, others are dynamic [48]. Moreover, some tunneling techniques are not in practice due to their lack of performance. Static tunnels provide better performance [7].

Routing is also a challenging task for network professionals when the network size is large, complex, heterogeneous, and scalable. Without a proper scalable routing protocol selection, a network does not provide better performance [73]. The scalable routing protocol determines the best path from source to destination quickly and efficiently if multiple paths exist in the large and complex network. Routing protocols were introduced to overcome routing and scaling issues. A variety of routing protocols is available for both IPv4 and IPv6 networks. The routing protocols are different from each other in terms of configuration, metrics, convergence speed, and other functionalities [8].

Security is at high risk in any network architecture. Although, IPv6 provides a built-in security feature in the header. It reduced the security threats but was still exposed to several attacks like Reconnaissance Attack, ICMPv6 Attack, and IPv6 Routing Header Attack. Some IPv4 known attacks did not change their influence by the look of the new IPv6 protocol. Both IPv4-IPv6 networks are affected by the sniffing attack, flooding attack, and man-in-the-middle attack [25]. To overcome the internal/external security threats in networks during the transition process, it is needed to design and implement strong security policies, deploy monitoring systems within a network as well as implement proper security appliances, such as firewalls and Intrusion Detection Systems (IDS) which are used for external threats.

The major participation of NFV is to offer network functions like firewalls, gateways, storage, Virtual Private Network (VPN), DHCP, DNS, routing, etc through software-based instead of hardware appliances. Compared with traditional physical network architectures, NFV architecture provides several advantages over traditional network architecture, such as low energy consumption, minimum equipment cost, elimination of proprietary nature of the hardware, improved operating performance, operation efficiency, optimized network configuration, resource allocation, and flexible network function deployment [38].

This research study presents a qualitative and comprehensive survey of all the above-mentioned main challenges, which are faced by ISPs during the transition towards virtualized NGN, and a detailed analysis of their solutions. To compare with other survey articles, our work presents novel knowledge about various key issues and challenges that occur during the co-existence of both IPv4-IPv6 networks and suggests the best solutions according to circumstances.

2. Comparison of IPv4 and IPv6

The IP is a connectionless and routed protocol. It does not provide a guarantee of a packet delivery service. Indeed, IP protocol tries its best efforts to deliver the user's traffic through different routes from one network to another network based on IP addresses [76]. Some application protocols such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Hyper Text Transfer Protocol (HTTP) have required a guarantee of packet delivery. To provide a guarantee of packet delivery services, the IP protocol is associated with the TCP protocol on the transport layer. 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 sending [24]. Unique source and destination IP addresses are needed for communication over the Internet and are enclosed in an IP header. The IANA has declared some blocks of IP addresses from different classes for private networking [58]. The 169.254.0.0/16 address is reserved for link-local addressing [19]. All the reserved and private addresses are not routable over the Internet. The NAT was introduced to provide Internet access for private networks [67].

2.1. IPv4

IP version 4 (IPv4) still routes most Internet traffic today. The packet of IPv4 consists of a data unit and a header. When the data unit comes to the network layer, then a minimum of 20 bytes of the IPv4 header is encapsulated in data before its transmission over the network.

The IPv4 header consists of 14 fields. Its maximum size is 60 bytes. One field is optional. The first 4-bits of the header are versions. It indicates the IP version used. A Time To Live (TTL) 8-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. 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. The 32-bit IP address fields are used to store the source and destination IP addresses respectively. The public IP addresses may be changed in transition by NAT devices.

2.2. IPv6

IP version 6 (IPv6) is the latest. It is also said to be the next-generation IP protocol. It consists of a 128-bits architecture. It can be provided in 2^{128}, which is 340 undecillion, approximately 3.4×10^{38} IP addresses. Repeated zero sections are eliminated and replaced with a double colon. [42]. In IPv6, the standard size of a subnet is 2^{64} and it is almost double the total IPv4 address size. Due to the larger address space, it is no need for NAT. Some addresses are also reserved in IPv6 by IANA.

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 first 4-bits of the header is also version the 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 is increased to 128-bits. The Flow Label 20-bits field provides traffic engineering and QoS services.

IPv6 provides several advantages over IPv4. A new multicast implementation technique has been introduced in IPv6 [63]. A new feature Stateless Address Auto Configuration (SLAAC) is also introduced in IPv6 to eliminate additional configuration servers. It allows a host to generate its address using a combination of link-local addresses and information advertised by routers [69]. IPsec is used as a built-in security feature in IPv6 with the help of the extension header. IPsec is a mandatory part of all IPv6 protocol implementation [43]. The extension header carries optional information along with the IPv6 header [24]. The extension header provides support for fragmentation. There are several types of extension headers. In IPv4, when a mobile device such as a smartphone changes its location, the device losses its IP address. When a person with a smartphone travels in a bullet train then it is very difficult to sustain services. To eliminate this limitation in IPv4, IPv6 introduced the mobility feature. The MIPv6 allows a mobile node to maintain a connection while moving from one subnet to another.

The real-time comparison between IPv4 and IPv6 is presented in Table 1.

Table 1. IPv4 and IPv6 comparisons.

	IPv4	**IPv6**
Address Length	32 bits	128 bits
Header Size	20-60 bytes	40 bytes
Header Fields	14	8
Address Types	Unicast, Multicast, Broadcast	Unicast, Multicast, Anycast
Built-in Security	No	IPsec
Mapping	Uses ARP to map MAC	Uses NDP to map MAC
Flow Identification	Not available	Through Flow Label
Mobility Support	Not supported	Mobility Provided
Address Translation	Required	Not Required
VLMS Support	Required	Not Required

3. Next-Generation Virtual Networking

In modern days, thousands of new devices are increasing the size of ISPs. As a result, ISPs are purchasing new physical equipment like routers, switches, gateways, security appliances, dedicated servers, and controllers. It increases the expenditure costs as well as electricity consumption for ISPs. To reduce energy consumption and expenditure costs for proprietary hardware, virtualization concepts are introduced in networking [38]. Virtualization architectures made the transition process easy and quick as well as provided several benefits.

3.1. Network Services Virtualization (NSV)

The virtualization technique is successfully implemented in the form of Virtual Local Area Network (VLAN), VPN, Virtual Router Redundancy Protocol (VRRP), and Virtual Routing Forwarding (VRF). These virtualization concepts are called NSV and have benefits in terms of hardware elimination. VLANs divide a physical switch into multiple segments logically and segments act as separate networks. 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 [9]. 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 [12]. 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 [52]. The VRF technique creates multiple virtual routing tables in a single router. VRF splits a single router into multiple logical routers [56].

3.2. Virtual Machines

In computing, a Virtual Machine (VM) is the virtualization or emulation of a computer system. VMs are based on computer architectures and provide functionality just like a physical computer [29]. VM is classified into system virtual machine or process virtual machine based on functionality. 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. There is multiple virtualization software such as VMware, VirtualBox, Virtual Iron, QEMU, ESXi, etc. that are used to create and run virtual machines on different operating systems and offer a variety of "vServices" in terms of desktop computing, servers, cloud management, application management, storage management, networking, and security.

3.3. Cloud Computing

Cloud computing is based on virtualization. It has been recognized as the de facto computing standard for hosting and delivering services over the Internet. Cloud computing is being quickly implemented by service providers and end-users because of its many benefits over traditional computing models such as cost-saving, scheduling, energy efficiency, scalability, unlimited storage, anytime anywhere access, and high fault tolerance capability [29].

The next generation clouds should also be ready to emerge from traditional or non-traditional architectures trends such as neuromorphic, quantum computing, adiabatic, nano computing, containerization, and Fog/Edge computing.

3.4. Network Function Virtualization (NFV)

The NFV concept was projected as new emerging technology. It is used to design, deploy, and manage network services with lower cost and lower energy consumption through decoupling physical proprietary network equipment [51] as is displayed in Figure 1.

The applications are performed and combined on standard IT platforms, high-volume servers, switches, routers, security appliances, and storage. In November 2012, seven world's leading Telecommunication Service Providers (TSPs) selected the European Telecommunications Standards Institute (ETSI) to be the home of the Industry Specification Group (ISG) for NFV [50].

NFV provides many benefits, such as reducing equipment cost, the openness of platforms, improved operating performance and operation efficiency, scalability, flexibility, and smaller development cycles [38].

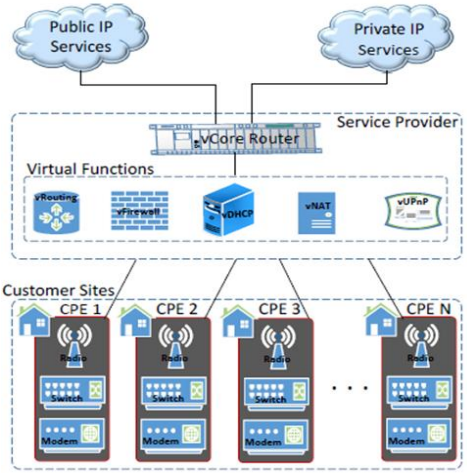

Figure 1. Network functions virtualization [50].

3.5. Software Defined Network (SDN)

The SDN is also a new programmable paradigm for next-generation virtual networks. In physical hardware switches, the control plane and data plane work together. The SDN is a programmable network approach that separates the control plane and data plane through standardized manners [36]. 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.

From a network management point of view, SDN architecture decouples network control and data forwarding functions. The network control plane is centrally managed by a directly programmable controller in the network. SDN was commonly associated with the OpenFlow protocol as a centralized controller that was used to communicate with network plane elements to determine the network paths for packets across network switches [55]. However, since 2012, many companies such as CISCO and NICIRA have introduced their proprietary controllers.

4. Core Issues During Moving Towards NGN

IPv4 and IPv6 protocols are not interoperable. So, IPv4 and IPv6 protocols will be run parallel until the transition is not completed. 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:

4.1. Packet Traversing

Meanwhile, IPv4-IPv6 protocols are not compatible. The users belonging to the IPv4 network cannot communicate with the IPv6 network. The two IPv6 networks cannot communicate with each other if the IPv4 network is involved between the two. It is known as a packet traversing or interoperability issue. To resolve the packet traversing issue, an artificial solution which is called tunneling is adopted. A tunnel is deployed when two IPv6 separate networks are directly connected with the IPv4 network and want to communicate with each other as shown in Figure 2.

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 between two communication ends. It joins two homogeneous networks through the virtual network [46].

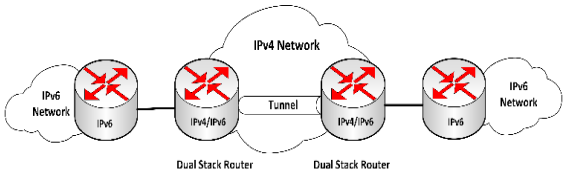

Figure 2. IPv6 tunneling.

Tunneling is a temporary solution until all the networks do not shift to IPv6. In tunneling, the IPv6 packet is encapsulated into the IPv4 header and then routed over the IPv4 network as highlighted in Figure 3.

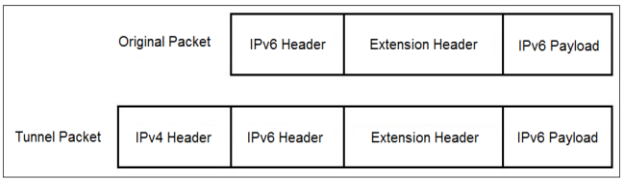

Figure 3. IPv6 tunnel packet.

At the destination, the decapsulation process is executed. In the decapsulation process, it extracts the IPv4 header and delivers the original IPv6 packet to its destination. It is used to achieve heterogeneous traversing. There are several IPv6 tunneling protocols like 6in4, 6to4, ISATAP, tredo, 6rd, 6over4, and GRE [48]. These are different from each other on a performance and configuration basis. The 6in4, 6rd, and GRE tunneling protocols are static, while 6to4, 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, the 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 [7]. The comparison of IPv6 tunneling protocols is shown in Table 2.

Table 2. IPv6 tunneling comparisons.

IPv6 Tunnel	Advantages	Limitations	Deployment Pattern
6in4	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.
6to4	It is a 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 on many platforms.	Monitoring 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 Intra-site use. Additional CPU load for encapsulation/ decapsulation.
GRE	Generic. Support several types. Can be used with routing protocols	Firewall challenges (IP protocol type 47 for IPv4 datagrams for inbound and outbound must be opened). Simple key authentication between the tunnel end-points. Key transmitted in cleartext.	For site-to-site tunneling only.

The packet traversing issue is resolved by tunneling. Numerous research studies [1, 2, 5, 60] 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 base of the IPv6 tunneling protocols through different kinds of parameters such as convergence, throughput, jitter, end-to-end delay, Round Trip Time (RTT), and tunnel overhead. Detail comparison of the IPv6 tunneling protocols is displayed in Tables 3 and 4 respectively.

Results show that the performance of the 6in4 tunnel is better than all others in most of the above-mentioned parameters. Due to better performance, 6in4 is widely used. It is a static and point-to-point tunnel. Mostly, researchers measured the performance in small size of VNs through simulators. Although the IPv6 tunneling technique resolved the packet traversing issue nevertheless it is not a secure virtual connection [31]. 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 [44]. 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 [34]. 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-source and IPv6-destination during transmission over the Internet [33]. 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 the IPsec header and the second is the IPv6 tunnel's header that creates extra overhead for every tunnel's packet during encapsulation/decapsulation. To reduce extra overhead with security features, a new IPv6 tunneling technique with security features needs to be addressed.

The performance of IPv6 tunneling protocols is examined by static routing as it is better in the small size of the network, but not feasible in large and complex networks. For larger and complex networks, dynamic routing is best for time-saving [8].

Table 3. IPv6 tunnel's performance with static routing.

Ref	IPv6 Tunnel	Throughput (kbps)	Jitter (ms)	Delay (ms)	Tunnel Overhead (ms)
[1]	6to4	486.40	0.0225	1.3103	00.712
	ISATAP	497.02	0.0300	1.2427	00.568
[2]	6to4	468.83	0.0078	1.3103	×
	ISATAP	495.11	0.0152	1.2427	×
[60]	6rd	150.33	0.0912	2.7820	35.375
	6to4	320.17	1.6779	4.5173	08.250
	ISATAP	100.79	0.0010	0.0363	14.688
	GRE	390.22	0.0004	0.8885	12.187

Table 4. IPv6 tunnel's performance with dynamic routing.

Ref	IPv6 Tunnel	Routing Protocol	Convergence Speed (sec)	Delay (ms)	Routing Traffic Sent (bps)	RTT (ms)
[5]	6in4	RIPng	35.0	1.310	80.00	×
	6to4		8.9	1.242	50.00	×
[7]	6in4	OSPFv3	23.3	30.15	33 (hello)	8.23
	6to4		130.4	36.23	12 (hello)	14.5
	ISATAP		38.4	31.73	11 (hello)	13.1
	GRE		25.6	34.54	34 (hello)	12.8

4.2. Routing Scalability

Routing is an essential part of the network. Without proper routing, the network would be non-functional and the data cannot be delivered to the destination. The router performs decisions by consulting its routing table. If the path exists in its routing table, then the router sends data to its destination otherwise discards the packets [10]. A router can store billions of routes in the routing table.

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 [73]. A comparison of IPv6 routing protocols is shown in Table 5.

Scalability is the capability of the network to handle or accommodate a growing amount of work easily. It is a highly significant issue in networking and routing. Multiple times, source and destination addresses are changed in a large and complex network. Routing protocols can easily complete their routing tables quickly after any change occurs in the network.

Table 5. IPv6 routing protocol's comparisons.

Routing Protocol	Advantages	Limitations	Type
RIPng	Easy to configure. Best for the small size of the network. Single table.	The maximum size is 15. Send a broadcast 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 count 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.

Although, the routing process is easily performed by routing protocols. Routing protocols detect any change or failure 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 [3, 8, 11, 18, 41, 49, 71] may help ISPs to provide routing services on large-scale next-generation virtualized IP networks. Detailed performance comparisons of the IPv6 routing protocols based on several parameters like convergence, throughput, jitter, packet loss, end-to-end delay, and RTT are displayed in Table 6.

Table 6. IPv6 routing protocols performance.

Ref	Routing Protocol	Convergence Speed (sec)	Throughput (kbps)	Jitter (ms)	RTT (ms)	Packet Loss (%)
[3]	RIPng	×	537.7	16.5	×	20.4
	EIGRPv6	×	714.1	14.2	×	2.5
	OSPFv3	×	674.0	15.9	×	2.7
[8]	EIGRPv6	13.0	×	×	45.0	×
	OSPFv3	21.0	×	×	51.0	×
[11]	EIGRPv6	8	152.24	41.89	5.78	14
	OSPFv3	45	151.42	42.02	7.22	18
[18]	RIPng	×	856.3	6.5	13.1	×
	OSPFv3	×	775.2	303.9	629.2	×
[41]	IS-IS	45.0	×	×	×	×
	OSPFv3	47.0	×	×	×	×
[49]	RIPng	×	930.0	43.0	×	5.0
	EIGRPv6	×	920.0	47.0	×	6.0
	OSPFv3	×	820.0	58.0	×	14.2
[71]	EIGRPv6	163.6	×	×	35.5	3.6
	OSPFv3	180.6	×	×	43.4	7.0

Table 6 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 large networks [47]. EIGRPv6 and OSPFv3 are the best choices for a larger network. EIGRPv6 is developed by CISCO as proprietary but later on, declared an open standard in 2013 [62]. 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 [22]. OSPFv3 becomes the 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 [32]. 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 [70]. Segment Routing (SR) is also a modern and fast form of routing introduced by IETF [26]. 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 Segment Routing Header (SRH) 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 the result, network performance is increased. SR increases network scalability, efficiency, and rerouting. In the future, segment routing will be adopted for routing in NGN.

Batalle *et al*. [16], researchers present their design and implementation of the routing function in a virtualized mode over an OpenFlow network. OpenFlow is the most common configuration protocol for enabling SDN architecture [13]. The researchers emphasize the idea of routing service as NFV over an OpenFlow network. The researchers achieved benefits based on reducing routing devices, configuration, space, costs, energy consumption, and deployment time.

The experimental results show that the RTT remains steady in dissimilar proposed scenarios when the number of requests increases. The performance and scalability are assured. More evaluations are needed to determine the robustness of the virtualized functions.

4.3. Network Performance Guarantee

Network virtualization is a paradigm to address several technical challenges within a traditional network. Virtualization technologies decouple 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 [20]. Virtualized Data Center (VDC) provides better management flexibility, lower cost, scalability, better resource utilization, and energy efficiency through NFV [15]. 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 [37].

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 SecondNet, Oktopus, Gatekeeper, CloudNaaS, and Seawall are available [59].

1. *SecondNet*: Guo *et al*. [35], offered SecondNet 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 2^{32} VMs and achieves high scalability by distributing all the virtual-to-physical mapping, routing, and bandwidth reservations from switches to server hypervisors. The authors designed architecture, implemented it on a simulated testbed, 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.

2. *Oktopus*: Ballani *et al*. [14], developed a new Oktopus architecture to prove the practicability of VNs. It depends on two proposed VN abstractions. 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.
3. *Gatekeeper*: Rodrigues *et al*. [59], focused on the problem related to network performance segregation and designed a new model named Gatekeeper. The solution should be scalable, on the basis of the quantity of VMs, expected performance, and robust against malicious behaviors of tenants. Gatekeeper architecture emphasizes 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 that belong to the same tenant. The degree of incoming traffic is monitored by the virtual NIC (vNIC) of each receiving VM through a 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 being reduced. Researchers implemented a Gatekeeper prototype with 2 tenants and 6 physical machines and their results showed that Gatekeeper works well within simple scenarios. Gatekeeper does not focus on latency and is still in progress.
4. *CloudNaaS*: cloud Networking-as-a-Service (CloudNaaS) is a VN architecture. Professionals deploy and manage enterprise applications in clouds in a well-organized way by using this architecture. Benson *et al*. [17], 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 permits the deployment of a variety of middlebox appliances. The authors demonstrated the flexibility of CloudNaaS in the cloud using a multi-tier application model in a test-bed with commercial OpenFlow 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 delivery and a few paths for QoS traffic based on the type of service. It uses wildcard bits for aggregation of IP forwarding entries. The results show that CloudNaaS performs well in large numbers of provisioning requests. The limitation of CloudNaaS is the use of limited paths for QoS.
5. *Seawall*: seawall is another bandwidth allocation architecture that defines a mechanism of how the bandwidth will be shared among multiple tenants in virtualized data centers. Shieh *et al*. [65], 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 VM 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 qualitative comparisons of the aforementioned architectures based on forwarding scheme, bandwidth guarantee, scalability, QoS, and deployability factors are summarized in Table 7.

Table 7. Qualitative comparison of architectures of VNs.

Ref	Architecture	Forwarding Scheme	Bandwidth Guarantee	Scalability	QoS	Deployability
[14]	Oktopus	×	✓	High	✓	High
[17]	CloudNaaS	✓	✓	Low	✓	Low
[35]	SecondNet	✓	✓	High	✓	High
[59]	Gatekeeper	×	✓	High	✓	High
[65]	Seawall	×	×	High	×	High

In the above 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 [21]. QoS is achieved in all VN architectures except Seawall by allocating bandwidth for each virtual link. The Seawall shares bandwidth among tenants based on weights. It does not provide guaranteed bandwidth allocation and did 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 [68]. It is measured by surveys and Means

Opinion Scores (MOS) methods. It is qualitative [21]. 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 users' satisfaction levels 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-users 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, display size, etc. Third, context influences factors based on location, time, interpersonal relations, and economic context [64]. QoE is an emerging multidisciplinary field. It is an important metric in the design and implementation of video streaming systems. In video streaming systems, 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.

4.4. Security

Security is always an important issue in any network architecture. IPv6 offers built-in security features with an extension header to improve its security mechanism. Despite these improvements in IPv6, there are some threats. IPv6 network was disturbed due to some new types of attacks [74]. Network security is a significant issue, especially when moving towards virtualized NGN and during the co-existence of IPv4-IPv6 networks [23]. Some kind of attacks affects both IPv4-IPv6 architectures and did not discriminate by appearance. A few examples of such kinds of attacks are sniffing attacks, flooding attacks, man-in-the-middle attacks, and application-layer attacks [66]. A set of attacks with countermeasures are shown in Table 8.

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 [4]. 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 it to its destination if the data is not secure. IPv6 header has no security mechanism itself. 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 [28]. The attacks in the application layer are the most common in both IPv4 and IPv6 networks. Different types of viruses and worms are tried to destroy data. To avoid these types of attacks, updated anti-virus software is installed.

Although, 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:

1. *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 is helped, to find out an accessible system and port scanning. The larger subnet size of the IPv6 and some types 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 kinds of tools. Reconnaissance attacks can be mitigated to perform the following methods [30]. A suitable IPS is deployed at the border. IPv6 packet filtering is also applied where applicable. When using DHCPv6, avoid using sequential addresses. Configured Media Access Control (MAC) addresses manually when VM is employed.
2. *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 by an attacker. ICMPv6 attacks can be mitigated to enforce a proper IPv6 packet filtering technique.
3. *IPv6 Routing Headers*: all nodes of IPv6 are capable of processing, and routing headers according to the IPv6 protocol. An attacker sends a specific packet containing a "forbidden" address in routing headers to access hosts by bypassing 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.
4. *Security Issues during Transition*: dual-stack and tunneling mechanisms have solved the problems of interoperability. In the dual-stack mode, the network node deals with both IPv4-IPv6 protocols and

maintains two separate tables. The IPv4 packets are forwarded to the IPv4 network while IPv6 packets to the IPv6 network. Dual-stack nodes are classified into two types. The first type is supported only in both IPv4-IPv6 and does not provide tunneling while the second type provides support for tunneling [61]. In dual-stack, applications are threatened by IPv4 and IPv6 attacks. Tunneling mechanisms bring new danger and misuse possibilities. In the automatic tunneling method, an intruder can avoid ingress filtering checks. Network addresses within the IPv4 or IPv6 headers may be spoofed and can be used for DoS 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 the firewall is active then tunneling traffic may be blocked. Security specialist enables tunneling traffic by using a protocol field value that is 41 [31].

The traditional network is moving towards software-based VNs. The network operators are decoupling hardware and trying to provide services through NSV, NFV, OpenFlow, and SDN. New security challenges also arise in this paradigm [45]. It is true that virtualization provided several benefits, and opens new dimensions of security threats for security specialists and professionals.

NFV allows network functions to be accomplished in VMs rather than in dedicated devices. It increases security risks and robustness issues due to the shared resources between VMs. These security challenges are divided into two categories. One is network function-specific security issues and the second is generic virtualization-related security issues [27]. 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 [72]. 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*: the 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. To overcome security threats in this domain, data should be encrypted and accessed only by the VNFs.
- *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 (vSwitches and vRouters) 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.

Table 8. Security threats and countermeasures.

Threat Name	IPv4	IPv6	Countermeasure
Sniffing Attack	√	√	IPsec
Flooding Attack	√	√	IPS
Man-in-the-Middle Attack	√	√	Encryption and Hashing
Viruses Attack	√	√	Anti-Virus
Reconnaissance Attack	×	√	Firewall and IPS
IPv6 Routing Headers Attack	×	√	Firewall
ICMPv6 Attacks	×	√	Firewall

5. Conclusions

IPv6 was launched as the next-generation internet protocol with several new features. ISPs have no choice but to shift their existing traditional IPv4 network towards IPv6. Several virtualized architectures were introduced in networking to overcome all the issues present in the physical network. The NFV, SDN, cloud computing, etc., were projected as new emerging technologies 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 virtualized IPv6 network architectures. The infrastructure and architecture of these two types of network models are different. The transition process is slow and cannot attain in a short period 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 qualitative and comprehensive survey, we focused on various key issues and challenges during the transition process from traditional IPv4 network to virtualized IPv6 network and provided corresponding solutions. Moreover, we highlighted limitations in all these corresponding solutions and

suggested some new research directions.

References

[1] Aazam M. and Huh E., "Impact of Ipv4-Ipv6 Coexistence in Cloud Virtualization Environment," *Annals of Telecommunications-Annales Des Télécommunications*, vol. 69, no. 9, pp. 485-496, 2014.

[2] Aazam M., Syed A., Shah S., Khan I., and Alam M., "Evaluation of 6to4 and ISATAP on a Test LAN," *in Procceding of IEEE Symposium on Computers and Informatics*, Kuala Lumpur, pp. 46-50, 2011.

[3] Al-Farizky R., "Routing Protocol Ripng, Ospfv3, And EIGRP on Ipv6 for Video Streaming Services," *in Proceeding of 5th International Conference on Cyber and IT Service Management*, Denpasar, pp. 1-6, 2017.

[4] Al-Mashhadani M. and Shujaa M., "IoT Security Using AES Encryption Technology based ESP32 Platform," *The International Arab Journal of Information Technology*, vol. 19, no. 2, pp. 214-223, 2022.

[5] Amr P. and Abdelbaki N., "Convergence Study of Ipv6 Tunneling Techniques," *in Proceeding of 10th International Conference on Communications*, Bucharest, pp. 1-6, 2014.

[6] Arkko J. and Baker F., Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment, Technical Report, *RFC 6180*, 2011.

[7] Ashraf Z. and Yousaf M., "Optimized Convergence of OSPFv3 in Large Scale Hybrid IPv4-IPv6 Network," *in Proceeding of 14th International Conference on Emerging Technologies*, Islamabad, pp. 1-6, 2018.

[8] Ashraf Z. and Yousaf M., "Optimized Routing Information Exchange in Hybrid IPv4-IPv6 Network using OSPFv3 and EIGRPv6," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, pp. 220-229, 2017.

[9] Ashraf Z. and Yousaf M., "Secure Inter-VLAN IPv6 Routing: Implementation and Evaluation," *Science International*, vol. 28, no. 3, pp. 3007-3014, 2016.

[10] Ashraf Z., *Ipv6 Routing: A Practitioner Approach*, LAP-LAMBERT, 2013.

[11] Ashraf Z., Sohail A., and Yousaf M., "Performance Analysis of Network Applications on IPv6 Cloud Connected Virtual Machine," *International Journal of Computer Network and Information Security*, vol. 11, no. 12, pp. 1-9, 2019.

[12] Ashraf Z., *Virtual Private Networks in Theory and Practice*, Grin Verlag, 2018.

[13] Balasubramanian V., Aloqaily M., and Reisslein M., "An SDN Architecture for Time Sensitive Industrial IoT," *Computer Networks*, vol. 186, p. 107739, 2021.

[14] Ballani H., Costa P., Karagiannis T., and Rowstron A., "Towards Predictable Datacenter Networks," *in ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 242-253, 2011.

[15] Bari M., Boutaba R., Esteves R., Granville L., Podlesny M., Rabbani M., Zhang Q., and Zhani, M "Data Center Network Virtualization: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 909-928, 2013.

[16] Batalle J., Riera J., Escalona E., and Garcia-Espin J., "On the implementation of NFV over an OpenFlow infrastructure: Routing function virtualization," *in Proceeding of IEEE SDN for Future Networks and Services*, Trento, pp. 1-6, 2013.

[17] Benson T., Akella A., Shaikh A., and Sahu S., "Cloudnaas: A Cloud Networking Platform for Enterprise Applications," *in Proceedings of the 2nd ACM Symposium on Cloud Computing*, Cascais, pp. 1-8, 2011.

[18] Chauhan D. and Sharma S., "Performance Evaluation of Different Routing Protocols in Ipv4 and Ipv6 Networks on The Basis of Packet Sizes," *Procedia Computer Science*, vol. 46, pp. 1072-1078, 2015.

[19] Cheshire S., Aboba B., and Guttman E., "Dynamic Configuration of Ipv4 Link-Local Addresses," *RFC 3927*, 2005.

[20] Chowdhury N. and Boutaba R., "Network Virtualization: State of The Art and Research Challenges," *IEEE Communications Magazine*, vol. 47, no. 7, pp. 20-26, 2009.

[21] Clark A. and Claise B., "Guidelines for Considering New Performance Metric Development," *RFC 6390*, 2011.

[22] Coltun R., Ferguson D., Moy J., and Lindem A., "OSPF for IPv6," *RFC 5340*, 2008.

[23] Davies E., Krishnan S., and Savola P., "Ipv6 Transition/Co-Existence Security Considerations," *RFC 4942*, 2007.

[24] Deering S. and Hinden R., "Internet Protocol, Version 6 (Ipv6) Specification," *RFC 8200*, 2017.

[25] Durdağı E. and Buldu A., "Ipv4/Ipv6 Security and Threat Comparisons," *Procedia-Social and Behavioral Sciences*, vol. 2, no. 2, pp. 5285-5291, 2010.

[26] Filsfils C., Previdi S., Ginsberg L., Shakir R., Decraene B., and Litkowski S., "Segment Routing Architecture," *RFC 8402*, 2018.

[27] Firoozjaei M., Jeong J., Ko H., and Kim H., "Security Challenges with Network Functions Virtualization," *Future Generation Computer Systems*, vol. 67, pp. 315-324, 2017.

[28] Frankel S. and Krishnan S., "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," *RFC 6071*, 2011.

[29] Gharehpasha S., Masdari M., and Jafarian A., "Virtual Machine Placement in Cloud Data Centers Using A Hybrid Multi-Verse Optimization Algorithm," *Artificial Intelligence Review*, vol. 54, no. 3, pp. 2221-2257, 2021.

[30] Gont F. and Liu W., "Security Implications of Ipv6 On Ipv4 Networks," *RFC 7123*, 2014.

[31] Gont F. and Chown T., "Network Reconnaissance in IPv6 Networks," *RFC 7707*, 2016.

[32] Goyal M., Soperi M., Baccelli E., Choudhury G., Shaikh A., Hosseini H., and Trivedi K., "Improving Convergence Speed and Scalability in OSPF: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 443-463, 2012.

[33] Graveman R., Parthasarathy M., Savola P., and Tschofenig H., "Using IPsec to Secure IPv6-in-IPv4 Tunnels," *RFC 4891*, 2007.

[34] Gu K., Zhang L., Wang Z., and Kong Y., "Comparative Studies of IPv6 Tunnel Security," *in Proceeding of the 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Guilin, pp. 2799-2804, 2017.

[35] Guo C., Lu G., Wang H., Yang S., Kong C., Sun P., Wu W., and Zhang Y., "Secondnet: A Data Center Network Virtualization Architecture with Bandwidth Guarantees," *in Proceedings of the 6th International Conference*, Philadelphia, pp. 1-12, 2010.

[36] Haleplidis E., Pentikousis K., Denazis S., Salim J., Meyer D., and Koufopavlou O., "Software-Defined Networking (SDN): Layers and Architecture Terminology," *RFC 7426*, 2015.

[37] Han B., Gopalakrishnan V., Ji L., and Lee S., "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90-97, 2015.

[38] Hawilo H., Shami A., Mirahmadi M., and Asal R., "NFV: State of the Art, Challenges and Implementation in Next Generation Mobile Networks (vepc)," *IEEE Network*, vol. 28, no. 6, pp. 18-26, 2014.

[39] IPv4 Address Report", https://ipv4.potaroo.net, Last Visited, 2022.

[40] "IPv6 Adoption", http://www.google.com/intl/en/ipv6/statistics.html, Last Visited, 2022.

[41] Jaafar A., Salim S., Tiron L., and Hussin Z., "Performance Evaluation of OSPFv3 and IS-IS Routing Protocol on ipv6 Network," *in Proceeding of the International Conference on Engineering Technology and Technopreneurship*, Kuala Lumpur, pp. 1-5, 2017.

[42] Kawamura S. and Kawashima M., "A Recommendation for IPv6 Address Text Representation," Technical Report *RFC 5952*, 2010.

[43] Kent S. and Seo K., "Security Architecture for the internet protocol," *RFC 4301*, 2005.

[44] Krishnan S., Thaler D., and Hoagland J., "Security Concerns with IP Tunneling," *RFC 6169*, 2011.

[45] Lal S., Taleb T., and Dutta A., "NFV: Security Threats and best Practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211-217, 2017.

[46] Lu T., Wu C., Lin W., Chen H., and Hsueh K., "Comparison of IPv4-Over-IPv6 (4over6) and Dual Stack Technologies in Dynamic Configuration for IPv4/IPv6 Address," *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, vol. 63, pp. 259-269, 2017.

[47] Malkin G. and Minnear R., "RIPng for IPv6," *RFC 2080*, 1997.

[48] Manimozhi S. and Jayanthi J., "Performance Study of IPv6/IPv4 MANET (64MANET) Architecture," *in Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications*, Coimbatore, pp. 645-658, 2019.

[49] Masruroh S., Robby F., and Hakiem N., "Performance Evaluation of Routing Protocols RIPng, OSPFv3, and EIGRP in an IPv6 Network," *in Proceedings of International Conference on Informatics and Computing*, Mataram, pp. 111-116, 2016.

[50] Mijumbi R., Serrat J., Gorricho J., Bouten N., De Turck F., and Boutaba R., "Network Function Virtualization: State-Of-The-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 236-262, 2016.

[51] Morton A., "Considerations for Benchmarking Virtual Network Functions and Their Infrastructure," *RFC 8172*, 2017.

[52] Nadas S., "Virtual Router Redundancy Protocol (vrrp) version 3 for ipv4 and IPv6," *RFC 5798*, 2010.

[53] Nordmark E. and Gilligan R., "Basic Transition Mechanisms for Ipv6 Hosts and Routers," *RFC 4213*, 2005.

[54] Ordabayeva G., Othman M., Kirgizbayeva B., Iztaev Z., and Bayegizova A., "A Systematic Review of Transition from IPv4 To IPv6," *in Proceedings of the 6th International Conference on Engineering and MIS*, Almaty, pp. 1-15, 2020.

[55] Prabakaran D., Nizar S., and Kumar K., *Design Methodologies and Tools for 5G Network Development and Application*, IGI Global, 2021.

[56] Rahman R., Zahari N., Kassim M., and Yusof M., "Virtual Routing and Forwarding-lite Traffic

Management over Multi-protocol Layer Switching-Virtual Private Network," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 8, no. 3, pp. 107-113, 2016.

[57] Ray P. and Kumar N., "SDN/NFV Architectures for Edge-Cloud Oriented Iot: A Systematic Review," *Computer Communications*, vol. 169, no. 4, pp. 129-153, 2021.

[58] Rekhter Y., Moskowitz B., Karrenberg D., de Groot G., and Lear E., "Address Allocation for Private Internets," *RFC 1918*, 1996.

[59] Rodrigues H., Santos J., Turner Y., Soares P., and Guedes D., "Gatekeeper: Supporting Bandwidth Guarantees for Multi-tenant Datacenter Networks," *in Proceedings of the 3rd Conference on I/O Virtualization*, Portland, pp. 1-6, 2011.

[60] Saraj T., Hanan A., Akbar M., Yousaf M., Qayyum A., and Tufail M., "Ipv6 Tunneling Protocols: Mathematical and Testbed Setup Performance Analysis," *in Proceedings of Conference on Information Assurance and Cyber Security*, Rawalpindi, pp. 62-68, 2015.

[61] Sathu H., Shah M., and Ganeshan K., "Performance Comparison of Video Protocols Using Dual-Stack and Tunnelling Mechanisms," *in Proceedings of International Conference on Advances in Computing and Communications*, Berlin, pp. 501-511, 2011.

[62] Savage D., Ng J., Moore S., Slice D., Paluch P., and White R., "Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)," *RFC 7868*, 2016.

[63] Savola P. and Haberman B., "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast address," *RFC 3956*, 2004.

[64] Serral-Gracià R., Cerqueira E., Curado M., Yannuzzi M., Monteiro E., and Masip-Bruin X., "An Overview of Quality of Experience Measurement Challenges for Video Applications in IP Networks," *in Proceeding of the International Conference on Wired/Wireless Internet Communications*, Luleå, pp. 252-263, 2010.

[65] Shieh A., Kandula S., Greenberg A., Kim C., and Saha B., "Sharing the Data Center Network," *in Proceeding of the 8th USENIX Symposium on Networked Systems Design and Implementation*, Boston, pp. 23-23, 2011.

[66] Shiranzaei A. and Khan R., "IPv6 Security Issues-A Systematic Review," *Next-Generation Networks*, vol. 638, pp. 41-49, 2018.

[67] Srisuresh P. and Holdrege M., "IP Network Address Translator (NAT) Terminology and Considerations," *RFC 2663*, 1999.

[68] Tesfamicael A., Liu V., Foo E., and Caelli B., "QoE Estimation Model for a Secure Real-Time Voice Communication System in the Cloud," *in Proceeding of the Australasian Computer Science Week Multiconference*, Sydney, pp. 1-10, 2019.

[69] Thomson S., Narten T., and Jinmei T., "IPv6 Stateless Address Autoconfiguration," *RFC 4862*, 2007.

[70] Wahanani H., Saputra W., and Freitas E., "Performance Analysis of Video on Demand and Video Streaming on the Network MPLS Traffic Engineering," *Geomate Journal*, vol. 15, no. 50, pp. 141-148, 2018.

[71] Whitfield R. and Zhu S., "A Comparison of OSPFv3 and EIGRPv6 in a Small IPv6 Enterprise Network," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 1, pp. 162-167, 2015.

[72] Yang W. and Fung C., "A Survey on Security in Network Functions Virtualization," *in Proceeding of the IEEE NetSoft Conference and Workshops*, Seoul, pp. 15-19, 2016.

[73] Yu J., "Scalable Routing Design Principles," *RFC 2791*, 2000.

[74] Žagar D., Grgić K., and Rimac-Drlje S., "Security Aspects in IPv6 Networks-Implementation and Testing," *Computers and Electrical Engineering*, vol. 33, no. 5-6, pp. 425-437, 2007.

[75] Zhan J., Dong S., and Hu W., "IoE-supported Smart Logistics Network Communication with Optimization and Security," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102052, 2022.

[76] Zimmermann H., "OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on communications*, vol. 28, no. 4, pp. 425-432, 1980.

Zeeshan Ashraf is a Ph.D. candidate at IQRA University Islamabad Campus, Islamabad, Pakistan. Currently, he is serving as a permanent faculty member of the Computer Science and IT department at The University of Chenab, Gujrat, Pakistan. His interests includes next-generation virtual IP network, IPv6 Routing, IoT, and security.

Adnan Sohail has received a Ph.D. degree in Electrical Engineering and Information Technology from the Institute of Telecommunications, Vienna University of Technology, Vienna, Austria. Currently, he is serving as an Associate Professor in the Computing and Technology department of IQRA University Islamabad Campus, Islamabad, Pakistan.

Sohaib Latif is a Ph.D. scholar in Information Security Engineering at the Anhui University of Science and Technology, Huainan, China. His research interest includes Wireless Sensor Networks, MANET's, Petri net, Deep Learning, and Internet of Things.

Abdul Hameed is an associate professor in the Computing and Technology department of IQRA University Islamabad Campus, Islamabad, Pakistan. He received his Ph.D. degree in Video Quality Assessment from North Dakota State University, USA.

Muhammad Yousaf is an associate professor and head of the Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan. He completed his Ph.D. Computer Engineering from CASE, University of Engineering and Technology, Taxila, Pakistan in 2013.