International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Comparative study of Security Aspects of IPv6 Network in deployment on Virtual Private Cloud

Syed Amjad Ali[1], Dr. C Ram Singla[2], Dr Najmuddin aamer[3]

[1]*Research Scholar, Department of Electronics & Communication Engg; Shri JJT University Jhunjhunu Rajasthan*
[2] *Dean, Department of Electronics & Communication Engg; Shri JJT University Jhunjhunu Rajasthan*
[3]*HOD Computer Engineering Department Theem college of Engineering, Boisar*

Abstract: The core mandate of the development of IPv6 ideally has been to substitute and supplement IPv4 power as a salient principle of the present-day internet platform. Its birth is the desirable option to IPv4 since it can sustain the increased growth of applications and devices supporting the internet as well as unlock the security concerns posed by IPv4. Moreover, the deficiency and depletion of IPv4 pool of addresses and the dire requisite towards a strengthened generation of IP that is essentially dependable and secure. These are the reasons why IPv6 deployment has become urgent with emphasis on secure, larger address space, and better performance. The main point of this paper is about the peculiarities of IPv6 from a transition perspective and its performance differences compared to IPv4. The current state of IPv6 usage, IPv4 to IPv6 transition strategies/mechanisms, routing and optimization/performance perspective of this new protocol is the concern.

Keywords: IPv4, IPv6, Virtual Private Cloud, security, migration

1. INTRODUCTION

It is also evident that IPv6 network platform is maturing, albeit slowly despite the fact that it has been enforced on major networks and most operating systems (Repas, 2014). Most of the core Internet transit providers have utilized the platforms provided and deployed IPv6. However, the edge networks are lagging in the implementation (Amogh, 2012). Its implementation gave birth to challenges such as depletion of IPv4 address space, configuration intricacy, performance degradation and network operational excellence concerns at the protocol level to be addressed (ISOC, 2014).
Research has been carried out with regard to protocol design, connectivity and routing, and transition to IPv6. Methods have been recommended to evaluate performance degradation and platforms whose focal point is on hardware and IPv6 compatibility. Yagoub (2014), asserts a network whose key role is the provision of public services, its performance is a major concern and with IPv6 it is extremely complicated. (Ali, 2013). The IP fundamentally obligates logical addressing and IP header fragment coordination activities to facilitate communication over the Internet backbone. This backbone infrastructure utilizes addresses encapsulated in the TCP header to relay data units between two communicating entities i.e. the sender and recipient. The datagram component encapsulates IP header portion as well as the fundamental payload.

This section discussed IPv4, IPv6, transition mechanisms as well as other related technologies and models available today [1-4].

Internet Protocol Version 4

The IPv4 was established and operationalized in early 1980's (Ali, 2013). This is the Internet Protocol platform that is used extensively for logical addressing by Internet hosts. It resides at the internet layer (layer 2) of the TCP/IP stack that acts as a transmission link between entities. Subsequently, when considering the OSI model, it is operationalized at the Network layer (layer 3) fundamentally for logical addressing and routing of traffic between hosts. The IP address assignable to hosts in a network of this kind is identified as a 32-bit address space (Ali, 2013). According to (Ahmed, Mustafa, & Ibrahim, 2015), the contemporary 32-bit address space was considered adequate upon its establishment and operationalization. The 32-bit denotation is an unsigned binary digit, framed in a representation of dotted decimal grouped in 8 bits octet. The sequence of bits is automatically resolved to host names by the Domain Name System (DNS) for internet communication to take effect. The fourth version is comprised of 4,294,967,296 unique addresses assignable to hosts (Albkerat & Issac, 2014) that are classified into several classes as shown in Figure 1.

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental
Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.		

Figure 1: IPv4 classes (Source: (Albkerat & Issac, 2014)

The first three classes (A, B and C) vary the size of bit length addressable to nodes on the network. Consequently, range of addresses within class D are specially conserved to carry out multicast operations. Finally, range of addresses within class E bears the reservation tag for research-based activities and future work. Each of the class cadre has got networks and hosts as shown in Table 1 [5-8]. The internet protocol addressing mechanism include a subnet mask identifier to delineate the network identity segment from the host segment of the network address (Babatunde & Al-Debagy, 2014).

Table 1: The addressing scheme (Source: Babatunde & Al-Debagy, 2014).

Class	Leading bits	Size of network number bit field	Number of Networks	Addresses per network	Start Address	End Address
A	0	8	126 (27-2)	16,777,216 (224)	0.0.0.0	127.255.255.255

B	10	16	16,382(214-2)	65,536 (216)	128.0.0.0	191.255.255.255
C	110	24	2,097,150(221-2)	256 (28)	192.0.0.0	223.255.255.255
D (multicast)	1110	Not defined	Not defined	Not defined	224.0.0.0	239.255.255.255
E (reserved)	1111	Not defined	Not defined	Not defined	240.0.0.0	255.255.255.255

Internet Protocol Version 5 (IPv5) (RFC 1190)

The Internet Stream Protocol (ST) was created in the late 1970's through experimental transmission of multimedia data and distributed simulation by (Krikorian, 2016) stipulated in 1979 in IEN 119 document (Wikipedia, 2016).

The protocol was amended and upgraded after two decades, to ST2 (Topolcic, 1990) defined in RFC 1190 and ST2+ implementation initiated into most of the commercial projects by popular companies such as Apple, IBM, NeXT, Sun, among others. These protocols were connection-oriented, unlike IPv4 suite which supported the connection-less strategy. This protocol guaranteed QoS to applications and services running on this platform. The naming convention for ST and ST+, were already given that magical "5" hence IPv5. The IPv5 was assigned to ST experimental protocol but failed to be introduced for use to the general public [9-13].

Internet Protocol Version 6 (IPv6) (RFC 2460)

This platform was established in 1994 with the main agenda for stakeholder implementations targeted by 1996. The specifications are defined in RFC 2460 of December 1998 (Deering & Hinden, 1998). It is the main successor version of IPv4 since IPv5 didn’t see the light of the day for implementation, deployment, and adoption. The design was considered an advancement of the Internet Protocol blueprint with both IPv6 and IPv4 still underutilized. The IPv6 implementation criteria is based on a 128-bit architecture accommodating an aggregate of 2128 addresses (Albkerat & Issac, 2014). The new blueprint is extensively defined in RFC 3513. The protocol evolved from IPv4 address platform. The founding conceptual blue print is considerably maintained with a couple of additional features integrated with the sole purpose to improve network operational excellence and provision of robust service delivery to internet clientele. This protocol fully supports stateless configuration (auto configuration) and NAT is excluded hence considered advantageous [14-18].

The IP address blends the MAC address for the interface and the prefix from the router or layer 3 device. The Dynamic Host Control Protocol is not utilized though it can be implemented in the presence of Domain Name System (Albkerat & Issac, 2014). The size of IPv6 address is 128 bits long, encompassing Hexadecimal digits capable of providing 3.8x1038 addresses. These range of discrete addresses are enough to assign a unique address to individual device for the present and the future. The four digits are separated by a colon which provides eight parts; the zeroes can be omitted to make the address smaller as shown in Figure 2.

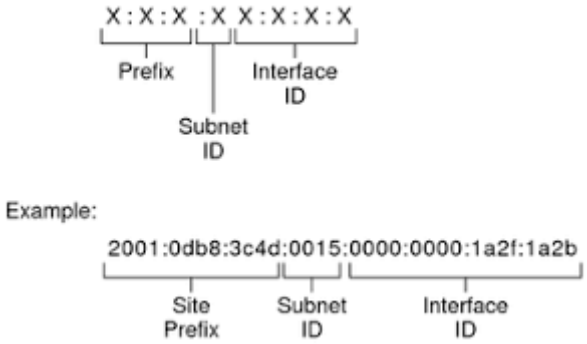

Figure 2: IPv6 addressing (Source: Albkerat & Issac, 2014)

IPv6 Features

Ibikunle & Oshin (2011), affirms that this version has specifically been designed with better features than the outgoing IPv4 address scheme. The successfully executed IPv4 functions were retained in the new scheme. However, new features were added to the IPv4 successful implementation functions to improve performance that is known of the new internet protocol. As a result, it translated into a number of merits over the depleted IPv4 pool as emphasized by (Govil, Govil, Kaur, & Kaur, 2008; Bradner & Mankin, 1995) and defined by IETF in RFC 1752 (Bradner & Mankin, 1995).

Larger address space

The fourth generation scheme of addressing utilizes a 32-bit address space assignable to the Internet whereas the next generation platform supports 128-bit address space. This address space has expanded to accommodate all possible end user devices. As a result, the depletion problem of hosts is squarely addressed and hosts reachable. Moreover, this addressing platform has completely eliminated the need for network addresses to be translated and hence reinstating the founding principle of end-to-end mechanism with the mandate of providing some applicable functionalities [19].

Auto configuration of nodes

The advertisements of routes in the routing table is fundamentally based on auto-configuration with regard to link state addressing forwarded by the respective routers (Govil, Govil, Kaur, & Kaur, 2008). This auto-configuration approach has provided a robust, fast, effective, systematic and dependable network node. The Plug and Play hallmark facilitate automatic setup, installation and configuration of IPv6 network devices. The node connected on the network establishes a unique string of address identified uniquely derived from a prefixed network code and the associated MAC/physical address. The importance of this feature is that, the end user is only required to seamlessly connect a device to the network infrastructure backbone in the absence of technical experts. This kind of support is very important especially for connectivity of new smart devices. Therefore, network devices do not require any form of configuration for connectivity to the network/internet such as manual and dynamic configuration.

More levels of addressing hierarchy

The various addressing tiers considered by the next generation scheme arrangement guarantees satisfactory clustering of routes, more flexible assignment of discrete addresses to downstream nodes and more scalable global routing table suited for the public internet.

Simpler IP header

The intelligence of layer 3 network device helps in the execution of routing and switching capabilities in a faster, effective and efficient manner, with the key purpose improve network performance and optimize processes (Govil, Govil, Kaur, & Kaur, 2008). Therefore, the complexities associated with the IP header are entirely eliminated.

Mobility Support

With the next generation protocol, mobility provision isn't an exception. The mobile support capability allows network nodes to be assigned one unique IP address that permanently belongs to it regardless of where it is being used. In the process a mobile network device traverse networks i.e. from one network to another, a new IPv6 address is created by incorporating the devices unique IP address and the network's designation number (Ibikunle & Oshin, 2011). The MIPv4 fundamentally supports triangular routing while MIPv6 on the other hand abandon the routing experience. This capability aid Wireless-Fidelity hosts to pick a new router without renumbering option. As a result, a connection is established that support robustness, dependability and faster link with minimal network congetion and interrupts.

Security

The IPSec fabric implementation proved to be explicitly imperative in IPv6. The framework warrants network nodes of a protected network traffic transmission (RFC 1825). In addition, the embedded security features have no negative effects with regard to performance, speed and network efficiency (Govil, Govil, Kaur, & Kaur, 2008). The embedded security features to the IPv4 protocol were optionally implementation at the user level. The IPv6 platform use data encryption mechanism to secure inbound and outbound traffic. It scrutinizes the integrity of packets with key consideration for interoperability since it is an open standard providing network security policies for packet transmission. It is designed to provide functionality within the seven designated layers of the OSI fabric. During encapsulation and decapsulation process between the layers, it ensures that the entire block of data units enclosed within the packet is transmitted risk-free among internetworking devices. Therefore, the IPv6 architecture consists of a protocol stack that supports IPSec, enhance security of the network and dispense interoperability framework upon implementation of IPv6 networks. Nevertheless, the provision of IPSec in the next generation is primarily embedded in the extension headers making the execution and implementation optional.

Better Support for Quality of Service

The network Quality of Service sometimes is referred to as "best level of effort" service in the contemporary IPv4 networks and it is an essential ingredient for network performance. The contemporary implementation experienced drawbacks since it failed to prioritize applications. The criteria used doesn't distinguish between time-sensitive (streaming video or audio) and non-time-sensitive (file transfer) applications. Time-sensitive applications include streaming live video or audio while non-time-sensitive include applications such as file transfer. For example, in the process datagrams are impaired during transmission, it is evident the TCP segment recognizes the loss and forwards a request for retransmission hence considered a reliable form of transmission. However, regardless of the reliability evidenced, network delay is inevitable. The IPv6 embedded features enhances services delivery, boost security, and improve reliability of the network for better coexistence. The identification of traffic and handling of inbound and outbound transmission is defined in the IPv6 additional fields. In this arrangement, the Flow Label field contained within the IP header, facilitates data units in a flow to be uniquely identified and dealt with. Consequently, as the transmission is identified in the header, QoS is guaranteed and supported efficiently. Considering these enhancements, this next generation protocol supports applications to request handling with no delay across the wide area network. This provision allows time-sensitive data to be loaded with minimal latency as supported by the priority levels 0 to 7 as follows:

- Level 0 - No specify priority
- Level 1 - Background traffic (news)
- Level 2 - Unattended data transfer (email)

- Level 3 - Reserved
- Level 4 - Attended bulk transfer (FTP)
- Level 5 - Reserved
- Level 6 - Interactive traffic (Telnet, Windowing)
- Level 7 - Control traffic (routing, network management)

The implementation strategy considered eliminates fragmentation and reduces latency and extra bandwidth consumption for prompt arrival of packets to the destination. In the long run, this implementation approach may result to inefficient utilization of traffic-oriented and resource-oriented traffic [38].

Problem Formulation

We aim to enable accountability and privacy in the IPv6 Internet while at the same time keeping the implementation lightweight and deployable. We have explained the motivations, resources, design goals, and adversary model in this section. A PKI certificate is required to confirm that a delegate is who they say they are prior to a verifier accepting their response. There will be an improvement in performance for verifiers with improved communication with delegates and improved verification of PKI certificates.

Motivation

Today, APIP and APNA are widely considered to be state-of-the-art approaches to balancing security and privacy in the network. Nevertheless, to be widely deployable, both of these tools require extensive modifications to the existing Internet infrastructures and protocols. Due to the introduction of APIP and APNA, protocols and infrastructures based on IP addresses (e.g., routing protocols and DNS) will need to be updated. Despite being deployable on today's Internet, there are some implementation constraints. In other words, when APIP adapts to today's Internet, PKI certificates are introduced and communication with routers' delegates is increased. For APNA, unless an AS completely adopts APNA, it will not be able to minimise the amount of privacy leaks associated with the presence of the local host addresses seen by an adversary. Routers in the AS should also keep a copy of the EphIDs that they forward the packets to, even if all routers are configured to use EphID for addressing. Computers in larger Internet service providers may require hundreds of thousands of flat entries, which would be a burden for router-based network devices. As such, we are interested in developing a protocol that is capable of starting to provide accountability and privacy for the Internet in its current state while avoiding the introduction of new communication identifiers and widespread alterations to existing infrastructures and protocols [39].

B. What We Have

Large IPv6 address space, existing standardised and well-maintained protocols, and adequate accountability of today's IPv6 Internet are available to help bootstrap new privacy and accountability measures.

1) Large IPv6 Address Space: the IPv6 address space is considerably larger than the IPv4 address space The IPv6 address space has 232 times the size of the IPv4 address space, even when just a single /64 prefix is assigned. Generally, a host configures two global unicast addresses within a /64 IPv6 prefix using stateless address autoconfiguration (SLAAC). 3 Typically, a DHCPv6 client obtains one global unicast IPv6 address from a /64 prefix. Even if we assume that each host has three global unicast addresses within a /64 sub-prefix, and that each address is actually assigned to a single host, the address space usage of the /64 sub-prefix is around 1.63 * 10−13, a number slightly greater than zero. It appears that we're not fully exploiting the IPv6 address space.

2) Multiple Addresses per Host: SLAAC and DHCPv6 addresses can be obtained per prefix for hosts. The SLAAC address used for outgoing connections may change over time (i.e., temporary address). For incoming connections, the other does not change over time (i.e., stays the same). Even if we assume that every host is assigned 100 addresses, a prefix with a thousand hosts would consume 5.42 × 10−12 units of space. Furthermore, the fact that RFC 7934 [20] makes mention of this is supported by RFC 4664 [6]. What this boils down to is that IPv6 address assignment practises help demonstrate that hosts may be assigned additional addresses for various purposes, such as for privacy purposes.

3) Standardized and Well-Maintained Protocols: Traditional and regularly updated protocols include DHCPv6 [19], SAVI [21], IPsec [22], and RPKI [23]. Reducing the amount of effort we need to use can be accomplished by using these protocols instead of creating new, similar ones. When working with a preexisting protocol, the same difficulties are encountered during the process of creating a new protocol. As an example, the certificate management issue found in APNA [10] is also present in IPsec.

C. Design Goals

1) Accountability: Accountability is referring to one's actions being held accountable to a governing body (specifically, a governing body who has the ability to act). In computing, accountability is defined as being able to reliably attribute all data packets to their senders. You have to follow a number of procedures to attain accountability on the Internet. First, data packets must be guaranteed to be authentic because they are used to keep track of senders who send bad data, and especially the header information. The second thing that must be done is for every senders on the network to have a unique identifier, and to be authenticated before accessing the network. Additionally, each data packet should have a specific sender identifier associated with it. There are numerous useful protocols that use accountability to help achieve a particular goal, such as blocking and filtering traffic, and calculating reputation scores for each source.

2) Privacy: It is accepted that there are four common notions of privacy at the network layer [9], [10], [25]. We have listed these four privacy goals for your consideration, as shown below.

- **Sender Anonymity.** The protection of sender anonymity. Anonymity of the sender is also provided by the first item on the list, which allows the sender to hide its identity from observers in any ASes, all the way to the recipient AS, while also concealing its source AS and route. With respect to LAN segment observers, we do not believe that sender anonymity is an issue because the sender already has the link layer address (address) they wish to send to. Additionally, we do not believe the requirement for sender anonymity is in opposition to the source AS, as it already knows the identity and network attachment of the sender.
- **Sender-Flow Unlinkability.** Also known as 'sender-flows anonymity' or 'sender-flow unrelevancy', our second privacy goal is sender-flow unlinkability, which means that an adversary cannot discover additional information about the source of a flow by examining a number of flows that originate from the same AS. The relativity of flows, according to the principle of flows, suggests the possibility of two flows originating from the same source. In the traditional networks, flow is the same for both the sender and receiver, but network devices and observers use a different meaning for the term. Since PAVI rewrites the source or destination addresses in the data packets as they move across the network, it changes how packets move across the network.
- **Sender-Receiver Unlinkability.** Thirdly, sender-receiver unlinkability must be achieved. Anyone who watches both the sender and the receiver can tell whether the two communicate in different flows. When one of the senders and one of the receivers knows the identity of the other, unlinkability means ensuring the privacy of the other's identity.

- **Data Confidentiality.** Fourth, data confidentiality is required for privacy. The payload in a packet can only be known by the recipient, and all other entities, including the source AS, must be in the dark. We use well-established protocols, such as IPsec, to protect the privacy of packet payload in this study.

3) Deployability: In relation to current protocol [9], [10], we are aiming to increase PAVI's deployability, and as a result, we are pursuing two sub-goals:

- **Lightweight Enhancements**: PAVI should only introduce lightweight Internet enhancements, and should not require major protocol or infrastructure changes as required by [9] and [10]. There should be a minimal performance cost to the Internet core deployed using PAVI.
- **Incrementally Deployable**: Legacy ASes can benefit from an AS/PAVI combination that is partially deployed; upgraded ASes, however, cannot immediately implement a PAVI.

D. Adversary Model

The adversaries' objective is to set up packets in the network without being discovered, while the objective of PAVI is to uncover the sender's identity. Because the adversary is presumed to be able to observe packet headers and payload, we assume that." Because the hosts could be compromised and used for attacks, it is assumed. Additionally, we predicted that transit ASes could be malicious. The adversary will not be able to access secret keys used in PAVI.

1. Virtual private cloud (VPC)

A virtual private cloud (VPC) is a secure private network inside a network cloud. A VPC is a secure, isolated private cloud that's hosted within a public cloud. The private cloud is hosted remotely by a public cloud provider, but customers have access to run code, store data, host websites, and perform other activities in an ordinary private cloud. (Many private clouds, though, aren't set up in this manner.) The various features of private cloud computing are included in VPCs, which combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.

What is a public cloud? What is a private cloud?

The public cloud is similar to a crowded restaurant; use it like that. A virtual private cloud, on the other hand, is a secluded table in that crowded restaurant. The party who made the reservation is permitted to use the table even though the rest of the restaurant is full. When there are a lot of cloud customers accessing computing resources, the public cloud is said to be crowded. On the other hand, a VPC (a type of Private Cloud) only allows one customer to use those resources.

How is a VPC isolated within a public cloud?

An Amazon VPC isolates your computing resources from the public cloud's other resources. A VPC needs the following technologies in order to isolate itself from the rest of the public cloud::

Subnets: A subnet is a portion of an IP network reserved for private use. Like IP addresses, which are visible to the public Internet, private IP addresses are not accessible in a VPC.

VLAN: The use of a VLAN for local area networks is a type of LAN. A VLAN is a virtual LAN. VLANs are similar to subnets in that they partition a network at a different layer of the OSI model, but this partitioning occurs at a different layer of the OSI model (layer 2 instead of layer 3).

VPN: A virtual private network (VPN) creates a private network within a public network by encrypting the data. As you can see, VPN traffic uses public infrastructure such as routers, switches, and so on, but it is encrypted and undetectable to anyone.

In the case of a VPC, only that VPC customer will have access to the dedicated subnet and VLAN that belong to the VPC. This keeps anyone from gaining access to VPC resources from

the public cloud. In other words, it places the "Reserved" sign on the table. VPC customers connect through a VPN to connect to their VPC, which allows for data to be sent into and out of the VPC without other public cloud users being able to see it.

Additional customization with VPCs is offered by a few VPC providers as given below:

- **Network Address Translation (NAT):** This feature allows you to find out if your computer is connected to the public Internet or a private network with your company's network address. It is possible to use a public-facing website or application in a VPC where NAT is in use.
- **BGP route configuration:** Customers who use BGP routing tables to connect their VPC to their other infrastructure have the option of tailoring the tables to meet their needs.

What are the advantages of using a VPC instead of a private cloud?

- **Scalability:** Customers can purchase additional computing resources on demand if a VPC is hosted by a public cloud provider.
- **Easy hybrid cloud deployment:** The process of connecting a VPC to the public cloud or on-premises infrastructure is rather simple.
- **Better performance:** Since cloud-hosted websites and applications typically perform better than those hosted on local on-premises servers, Cloud-hosted websites and applications typically perform better than local on-premises websites and applications.
- **Better security:** More resources for updating and maintaining the infrastructure, especially for small and mid-market businesses: public cloud providers that offer VPCs usually have. For large corporations and businesses that are subject to highly restrictive data security regulations, this feature is not quite as valuable.

Features

"Best of both worlds" cloud computing is an approach to virtual private cloud (VPC) offerings. They leverage public cloud resources and savings while offering many of the advantages of private clouds. VPC features include the following:

- **Agility:** Run a virtual network at your desired scale and provision cloud resources as required by your business. These resources can be scaled in real-time and dynamically.
- **Availability:** Redundant resources and highly fault-tolerant availability zone architectures ensure your applications and workloads are highly available.
- **Security:** You're data and applications will stay separate from other cloud customers' because the VPC is a logically isolated network. It is your discretion to access resources and workflows, and to whom.
- **Affordability:** The VPC customers can save on hardware costs, labour times, and other resources because of the public cloud's low costs.

Benefits

Everything a VPC has to offer benefits your business in a way that empowers agility, new innovation, and rapid growth.

- **Flexible business growth:** VPC customers can adapt to changes in business needs because cloud infrastructure resources, including virtual servers, storage, and networking, can be deployed dynamically.
- **Satisfied customers:** The customers who are happy with their service: In a "always-on" digital business environment, customers expect high availability ratios of nearly 100% Reliability in online experiences and trust in your brand are both achievable in VPC environments thanks to their consistent availability.

- **Reduced risk across the entire data lifecycle:** VPCs offer strong protection at the subnet or instance level, or both. This contributes to your sense of security and improves your customers' trust.
- **More resources to channel toward business innovation:** A greater range of resources that can be directed toward business innovation, especially with reduced IT costs and fewer demands on your internal IT team: You can devote yourself to achieving business goals and strengthening your core competencies while freeing up time and resources to act on your own interests.

Architecture

A VPC allows you to deploy cloud resources into an isolated virtual network in your own AWS account. There are three main classifications of cloud resources known as logical instances.

- **Compute:** Because virtual server instances (VSIs) are presented to the user as virtual CPUs (vCPUs) with a predetermined amount of computing power, memory, etc., they are referred to as virtual server CPUs (VS CPUs).
- **Storage:** VPC customers are given a storage quota for each account, and additional storage is available for purchase. To think of it, it's almost like buying additional hard drive space. Storage recommendations are based on the type of work you're doing.
- **Networking:** You can deploy virtual network functions such as firewalls, traffic-shaping, and IPsec features to virtual private cloud (VPC) accounts to grant or deny access to the resources of that VPC. Also, load balancers are useful because they distribute traffic across multiple VPCs to optimise both availability and performance. Direct or dedicated links help your enterprise IT environment or your private cloud and your VPC resources communicate quickly and securely with your public cloud.

Three-tier architecture in a VPC

Three-tier architecture: 80% of applications are based on this architecture, which consists of three tiers interlinked:

- The web or presentation tier, which handles requests from web browsers and utilises the information created or stored by the other layers to present information to end users.
- The business logic is concentrated in the application tier, where most processing occurs.
- The database tier, which includes database servers that store data processed in the application tier.

Assigning tiers their own subnets within a VPC results in each tier having its own IP address range. Assigned Access Control List (ACL) is created for each layer.

Security

In traditional data centres, the security features used to control access to resources are replicated and virtualized in order to create high levels of security. Virtual networks that customers can define are enabled by security features that provide them with the ability to set up virtual networks within logically separated sections of the public cloud, allowing them to control which IP addresses have access to which resources.

Two types of network access controls comprise the layers of VPC security:

- **Access control lists (ACLs):** The layers of VPC security comprise two varieties of network access controls: A form of access control. An ACL is a list of rules that govern which subnets users can access within your VPC. Subnets are subsections of your VPC, while the ACL determines the set of IP addresses or applications that are granted access to the subnet..
- **Security group:** A security group enables you to create groups of resources (and assign uniform access rules to them) that may be located in more than one subnet. You could set up all three of them so that they're publicly accessible on the Internet if you create a security group for them with the correct network configurations. Your virtual servers are assigned

security groups, which serve as virtual firewalls to control the flow of traffic no matter which subnet they are on.

2. Need of Study

The adoption of next generation internet protocol IPv6 is mushrooming and has been on exponential scale since the last decade. The transition mechanisms are only seen as short term interim measures for interoperability between IPv4 and IPv6.However till migration phase completes, networks need to be optimized and secured. The users cannot tolerate internet downtime and reliability of the network. The operation of transition mechanism will act as bridge between two heterogeneous protocols but at the same time will introduce performance bottlenecks. For example; tunneling mechanism suffers from encapsulation and decapsulation delays, dual stacks require higher computational and processing power among the nodes. Also it's anticipated that the next generation internet protocol (IPng) will introduce vulnerabilities in addition to those inherent in IPv4. While the current security infrastructure like IPSec, SSL, PKI, and DNSSec are adequate for IPv4, it must be investigated and analysed as to whether it will suffice for IPv6 and migration networks. This is because there is much more research that needs to be done to learn more about IPv6 and Migration networks.

Programs and systems built to run on the IPv4 standard are not able to communicate with those that were built to run on the IPv6 standard. IPv4 systems are everywhere, and this is not about to change "overnight" with the roll-out of IPv6 systems. The need to upgrade the network causes the application to cease functioning until the transition mechanisms have been smoothed out. With IPv6, the address space is dramatically increased, which gives a lot more freedom in assigning addresses. By eliminating the need to use network address translation to avoid address exhaustion, the extended address length (Nakajima and Kobayashi 2004) also simplifies aspects of address assignment and renumbering when changing providers. While IPsec is an essential part of the base protocol suite in IPv6, in IPv4 it is an optional component (but usually implemented). IPSec is widely used today for securing traffic between IPv6 Border Gateway Protocol routers, but is not widely implemented because of the relative rarity of IPv6 BGP routers.

2. CONCLUSION

This research focuses largely on the performance metrics of the IPv6 transition strategies in network. Besides this the other network issues such asSecurity are included in this synopsis and deploying this IPv6 network on cloud with the help of Cloud BOSS. IPv6 network in wireless or in satellite communication has not beenincluded. The routing and performance comparisons of various IPv6 Transition strategies in a wired network set up are important to understand and for this purpose the focus on the choice of parameters of IPv6 transition strategies parameters is limited to Round-trip-time, throughput, end-to-end delay, and end-to-end jitter.

There are few other strategies that might be useful to the technical society that are not studied in this research due to limitations of Packet tracer, GNS3 and OMNeT++. At present, packet tracer and GNS3 do not support transition strategies such as Teredo, Tunnel Broker, 6RD and IPv6. Therefore, these mechanisms are not considered in this research.

3. REFERENCES

[1] S. E. Deering, ''Internet protocol, version 6 (IPv6) specification", 1998.

[2] (13/2/2018). IPv6 Adoption – Google Internet Statistics. Available: https://www.google.com/intl/en/ipv6/statistics.html.
A. Shubair, Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms, Int. J. Secur. Netw. 12 (2) (2017) 83–102.
[3] J.H. Jafarian, E. Al-Shaer, Q. Duan, An effective address mutation approach for disrupting reconnaissance attacks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2562–2577.
[4] J.M. Ehrenfeld, Wannacry, cybersecurity and health information technology: a time to act, J. Med. Syst. 41 (7) (2017) 104.
[5] F. Gont, ‘‘A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) RFC No 7217”, 2014.
[6] S. Hagen, IPv6 Essentials, third ed., O’Reilly Media Inc, California, USA, 2014.
[7] F. Gont and T. Chown, Network reconnaissance in IPv6 networks RFC No 7707, 2016.
[8] R. Asati, H. Singh, W. Beebee, C. Pignataro, E. Dart, and W. George, Enhanced Duplicate Address Detection RFC No 7527, 2015.
[9] H. Rafiee and C. Meinel, ‘‘SSAS: A simple secure addressing scheme for IPv6 autoconfiguration,” in Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, 2013, pp. 275-282: IEEE
[10] S. Groat, M. Dunlop, R. Marchany, J. Tront, ‘‘The Privacy Implications of Stateless IPv6 Addressing,”, in: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ACM, 2010, p. 52.
[11] T. Savolainen, J. Soininen, B. Silverajan, Ipv6 addressing strategies for iot, IEEE Sensors J. 13 (10) (2013) 3511–3519.
[12] T. Narten R. Draves S. Krishnan ‘‘Privacy Extensions for Stateless Address Autoconfiguration in IPv6 RFC No 4941,” 2007.
[13] W. Haddad, E. Nordmark, F. Dupont, M. Bagnulo, B. Patil, Privacy for mobile and multi-homed nodes: MoMiPriv problem statement, Internet Draft (2005).
[14] R. Koodli ‘‘IP Address Location Privacy and Mobile IPv6: Problem Statement RFC No 4882,” 2007.
[15] A.O. Ade-Ibijola, A simulated enhancement of Fisher-Yates algorithm for shuffling in virtual card games using domain-specific data structures, Int. J. Comput. Appl. 54 (11) (2012).
[16] C.C. Zou, D. Towsley, W. Gong, On the performance of Internet worm scanning strategies, Perform. Eval. 63 (7) (2006) 700–723.
[17] F. Gont, W. Liu, A Method for Generating Semantically Opaque Interface Identifiers (IIDs) with the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC No 7943, 2016
[18] Deering, S., & Hinden, R. (December1998). Internet Protocol Version 6 (IPv6) Specification, IETF RFC 2460.
[19] Madhav Panthee, Dr. Yogesh Kumar Sharma, Review of E-Government Implementation, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 6, Issue 1, March 2019, pp. 26-30
[20] Narten, T., Nordmark, E., Simpson, W., & Soliman, H. (September 2007). Neighbor Discovery for IP version 6 (IPv6),IETF RFC 4861.
[21] Thomson, S., Narten, T., & Jinmei, T. (September 2007). IPv6 Stateless Address Autoconfiguration, IETF RFC 4862 .
[22] Conta, A., Deering, S., & Gupta, M. (March 2006). Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification),IETF RFC 4443.

[23] Hinden, R., & Deering, S. (February 2006). IP Version 6 Addressing Architecture, , IETF RFC 4291.
[24] Kent, S., & Seo, K. (December 2005). Security Architecture for the Internet Protocol , IETF RFC 4301.
[25] Ziring N. (May 2006). Router Security Configuration Guide Supplement - Security for IPv6 Routers. [Online]. Available:www.nsa.gov/ia/_files/routers/I33-002R-06.pdf
[26] Hermann, P.-Seton (2002). Security Features in IPv6. [Online]. Available: www.sans.org/reading_room/whitepapers/.../security_features_in_ipv6_380
[27] Sotillo, S. (2006). IPv6 Security Issues. [Online]. Available: www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf
[28] Sailan, M.K., Hassan, R., & Patel, A. (2009). A Comparative Review of IPv4 and IPv6 for Research Test Bed. 2009 International Conference on Electrical Engineering and Informatics, Selangor, Malaysia.
[29] Caicedo, C.E., Joshi, J.B.D., & Tuladhar, S.R.(2009). IPv6 Security Challenge. Computer, 42, 36-42.
[30] Dr. Yogesh Kumar Sharma and Dr. Surender (2013), "Future Role of Zigbee Technology in Wireless Communication System", Paper published in Grip - The Standard Research International Referred Online Research Journal, ISSN-2278-8123, Issue No. XVI, Pp. 18-31.
[31] Davies, J. (2003). Understanding IPv6, Microsoft Press.
[32] Kanda, M. (2004). IPsec: a basis for IPv6 security. [Online]. Available:http://www.ipv6style.jp/en/tech/20040707/index.shtml.
[33] Radwan, A.M. (2005). Using IPSec in IPv6 Security. [Online]. Available:http://www.uop.edu.jo/csit2006/vol2%20pdf/pg471.pdf
[34] Saito, Y. (December 2003). IPv6 and New Security Paradigm. NTT Communications, Doc. No. 79
[35] Dr.Yogesh Kumar Sharma, Rokade Monika D, Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic, National Conference on "Recent Innovations in Engineering and Technology" MOMENTUM-19 63-69 Sharadchandra Pawar College of Engineering, Dumbarwadi, Tal-Junnar, Dist-Pune-410504
[36] Cisco Systems Report (2004). IPv6 SECURITY Session Sec-2003.
[37] Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., & Verma, K. D. (2021). Secure Cloud Data Storage System Using Hybrid Paillier-Blowfish Algorithm. CMC-Computers Materials & Continua, 67(1), 779-798.
[38] Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2020). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, e4108
[39] Oh, H., Chae, K., Bang, H., & Na, J. (February 2006). Comparisons analysis of Security Vulnerabilities for Security Enforcement in IPv4/IPv6. Advanced Communication Technology, 2006. ICACT 2006.