Ensuring Reliability in Cloud Computing and Comparison on IPv6 Encouraged with Protocols

Arun Kumar Tripathi[1], Shweta Singh[2]
[1]mailtoaruntripathi@gmail.com, [2]shweta.vidudi272@gmail.com (Corresponding Author)
[1,2]KIET Group of Institutions, Ghaziabad, India

***Abstract*- In today's high-capacity networking environment, a need to an on-the-line computing has awakened i.e. a need to have an on-demand networking architecture. Architecture similar to this functionality is formally the famous Cloud Computing that provides a reliable basis to have access for the shared environment. This is accomplished through a connection-oriented network followed with some infrastructure with lesser maintenance and high performance. To accomplish this infrastructure OPNET IT GURU EDUCATIONAL VERSION 14.5 Modeler is being used. The reliability is encouraged by maintaining parameters for routing protocols such that throughput is increased as utilization is increased.**

Key Words: Cloud Computing, Delay, Utilization, TCP Connection, Throughput, PPP, Digital Signal, IP Routing Protocol, IPv6, RIPng, OSPF, IS-IS.

I. INTRODUCTION

Cloud Computing [1] is a mechanism that facilitates multiple connected devices in an Internet to get access to shared devices. These devices may be repeaters, hubs, switches, routers, etc. that help in exchanging the data packets in a network and along with this a certain factor to security is also needed, for that firewalls are required.

Cloud computing formally known as 'on-demand computing', enables an on-demand access to the shared resources and information that is usually managed by a third party situated at different geographical location. For cloud computing network, it is claimed that this technology enables to improve the access for applications in a faster way then to the before, enabling an improvement in manageability and maintainability factors, also, enables IT to adjust factors to shared resources so that they can easily met with fluctuating and unpredictable demands of business.

The main aspect that cloud computing provides is 'virtualization', which enables number of users to get their work done using virtual software, virtual hardware as and when needed. Since it is a Service-oriented Architecture (SOA) [1] that provides resources as aspects of services that facilitates for their use in consideration to well-established standards for global access in a standardized way.

Cloud computing is evolved by addressing the famous Quality-of-Service (QoS) [2] and reliability problems. Cloud computing facilitates following characteristics that will be analyzed in further analysis section. The characteristics can be a follows:

- **Cost**: The public-cloud architecture facilitates to claim high capital expenditures to operational expenditure.
- **Device and location independence**: This provides a facility to number of users to access resources or to operate through a web browser regardless of their geographic location.
- **Maintenance**: This is easy to use technology such that it doesn't need to be implemented onto every computer and can be operated from different places.
- **Performance**: It is made consistent by monitoring using loosely coupled architectures using web services as an interface with system.
- **Productivity**: Productivity is gradually increased as users are not intended to install applications onto their system every time they access.
- **Reliability**: Provides reliable methods for data recovery and backups, improves usage of redundant for multiple users.
- **Security**: The complexity of security is gradually increased when data is distributed onto a wider area or even over numbers of devices.

When is associated with security to a network or security concerned with autonomous systems operating in an unreliable or prone network, firewalls acts good to provide higher levels of security to an autonomous network. Firewall acts as a security factor for network where it is intended to sense, monitor and control every incoming and outgoing message or information or network traffic. Firewall relies to act as a barrier to allow only trusted network traffic to pass inside network and non-trusted outside network.

Rest of the paper is organized as follows. Section 2 deals with characteristics of TCP connection [2] (consisting of congestion-control and monitoring),

Point-to-Point (PPP) [3] protocol along with its characteristics and signaling scheme i.e. Digital Signal 1 (DS1) and Digital Signal 3 (DS3); protocols encouraged in Internet Protocol version 6(IPv6) [4] environment i.e. RIP next generation (RIPng) [5], Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS). Section 3 contains two scenarios on cloud based network. Section 3a environment with simple IPv6 scheme working underDS3link facilitating RIPng, section 3b represents environment with IPv6 scheme under RIPng, OSPF, IS-IS underDS3 link. Section 4 defines the simulation results that are made to the scenarios. Section 5 includes the conclusion and future work related to the further considerations to better up the working environment.

II. RELATED WORK

In a cloud environment usually it is recommended to use a connection-oriented mechanism i.e. TCP connection. In TCP, the two communicating parties need to establish a connection at first by sending a series of messages to establish a network that is reliable and responsible to operate in-order delivery of a stream of bytes. The confirmation of messages to be delivered is controlled through ACK messages at routines.

Along with its mechanism, TCP provides a highly-tuned congestion control mechanism. The idea that works in congestion-control includes a monitoring process that defines the capacity available to the network, hence justifying that how much packets can be safely transmitted into the network.

TCP is an end-to-end transmission protocol that encourages higher levels of reliability in a network. Apart from this a protocol is also engaged along with the TCP mechanism so that authentication, transmission encryption and compression are also encouraged for maintaining the reliability of conversation taking place in between the integrated parties. PPP protocol is accomplished to provide these three facilities inside a network to make it secure and reliable from outside unreliable network.

PPP is a data link layer protocol which is used to establish a direct end-to-end connection in between two communicating entities. PPP is generally used in a physical manner in any network such as through serial cable, trunk line, phone line, cellular or may be as fibre optic cable like SONET. Generally PPP is used by Internet Service Providers (ISPs) to provide a dial-up connection to users. The circuit provided in PPP protocol environment is both synchronous and asynchronous in nature which is duplex in nature. Duplex circuit means the communicating entities will be maintaining a two-way communication mechanism.

There are certain configurations while working with PPP protocol, out these few can be as following:

- **Authentication**: This is accomplished by exchanging authentication messages while communication. Handshaking mechanism is encouraged to provide authentication.
- **Compression**: Compression techniques are mainly implemented to reduce the amount of data frames travelling along a network. This facilitates an effective throughput on PPP connections. Packets are then decompressed when received by receiver.
- **Error detection**: This is responsible to identify fault conditions, providing a loop-free data link and increased quality factor.
- **Multilink**: This characteristic provides with load balancing mechanism which uses multiple interfaces using PPP.

In telecommunication, information is shared in forms of digital signals that depend usually onto voltage of physical channel. In context to digital transmission, two types of digital signals are pursued that can be namely underlined in a T-carrier signalling scheme. T-carrier signalling scheme [3], [10] facilitates a carrier used to technological support in a cloud environment. The two very famous signalling mechanisms can be as stated below:

a) **Digital Signal 1**: The Digital Signal 1 scheme is formally known as DS1 signalling. This was well known as T-carrier signalling scheme which was used as E-carrier in place of T-carrier for countries mainly United States, South Korea and Japan. DS1 or T1 is basically a bit pattern that is used over a physical T1 line.

b) **Digital Signal 3**: The Digital Signal 3 is formally known as DS3 signalling. This is a 3 level T-carrier mechanism. It is also referred as T3 signalling mechanism. This level is an advanced version to the existing DS1 scheme as it is regarded that DS3 or T3 can transport 28 DS1 level signals within payload. This is more reliable scheme to be opted for a network to increase the productivity and reduces the querying delay.

Besides this, to communicate we need to configure protocols that are reliable and faster to perform. To communicate through the Internet facility, Internet protocols (IP) [6] are used. The two most familiar internet protocols are namely: Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). These protocols are intended to relay the

datagrams onto the boundaries of network. The since every version of protocol provides certain pattern to the address provided to each and every data packets which are intended to move across the stations so connected to communicate as:

- **IPv4**: This is a fourth version of IP. This version is a core protocol that is based on standard- based methods of networking. IPv4 is probably a connectionless protocol supporting packet-switched networking i.e. IPv4 provides some aspects of integrity for delivery of data packets by making use of best effort delivery model, but does not guarantee for accurate delivery or to prevent any duplicate delivery.

Besides all these factors, a new version (IPv6) was released to overcome allocation and address requirements by both private and public networks.

- **IPv6**: This is a recent version of IP providing with larger addressing space i.e. uses 128–bit address, much larger than used in IPv4. IPv6 provides technical benefits by providing much larger address space in a hierarchical way. Main features under IPv6 can be as:
  - For address assignment it uses stateless address auto-configuration
  - Provides a simplification in accordance to routers to deliver each packet at their prescribed destinations using fragmentation processes.
  - Creates a parallel and independent network facilitating an automatic mechanism to form host identifier from MAC address.

While communicating in an unreliable network, some aspects of security should also be maintained out of which there are some routing protocols even. RIP [5]is one the protocol that is employing a routing hop count facility. RIP provides a facility to count and limit number of hops between source and destination devices. In an IPv6 environment routing is made at simpler levels for accordance of routers in a network. When RIP is implemented along with the IPv6 protocol address type, network probably performs in a better way as RIP provides route poisoning, split horizon and hold down facilities which prevents inaccurate routing information unnecessarily propagated in a network.

RIP is based on User datagram protocol (UDP) mechanism at the transport layer. RIPng is an extension to RIP version 2 that supports for IPv6 address configuration.

- **OSPF:** OSPF [7] is one the routing protocol for networks that follows IP. It works for an autonomous network such that it uses a link state algorithm that falls for interior group of routing protocols. The OSPF is responsible to collect information from all the routers available in an autonomous network and constructs a topology map of network. A topology is made in a form of routing table that defines all the link paths involved in a network then datagrams are sent solely to their defined destination IP address. OSPF doesn't use TCP/UDP transport protocol, but rather encapsulates into IP datagrams. It is indeed best in implementing its own error detection and correction functionality.
- **ISIS-IS:** IS-IS [7] is another designed routing protocol that rapidly and efficiently moves information in between the devices grouped or connected in a network via physical link. This follows packet-switch networking scheme. IS-IS and OSPF both the protocols act in one and the same manner by finding the lowest cost path from routing topology so maintained, rather IS-IS supports larger area than OSPF.

III. SIMULATION

The simulation [8]is performed to establish a reliable network that consists of TCP type connection for which, a point-to-point transmission protocol (PPP) is simulated for its working in an IPv6 environment using DS3 communication link. The fact on simulating these two scenarios is to get the maximum throughput in a cloud-based environment working under different routing protocols. Also, to reduce the delay caused while placing queries to get access or to operate onto a particular network.

In simulation, a cloud network is set up with basic linking methodologies *i.e.*, DS3 operated under point-to-point transmission protocol PPP.

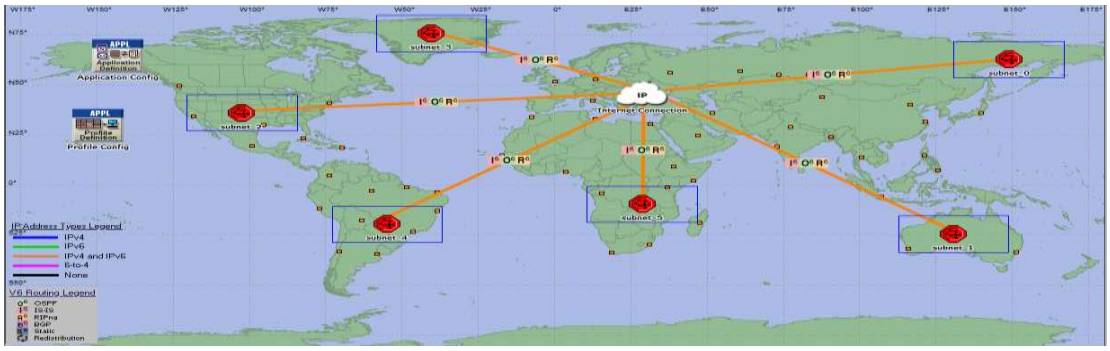

Figure 1. Internet Connection following cloud-based network

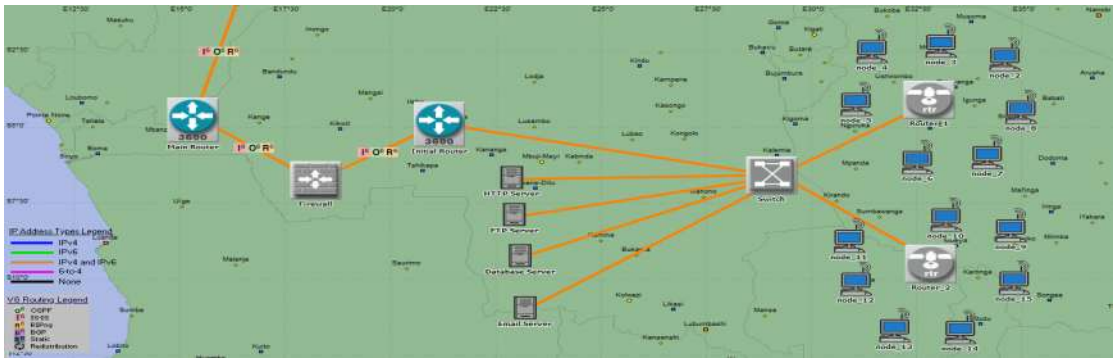

Figure 2. Simple Autonomous Network

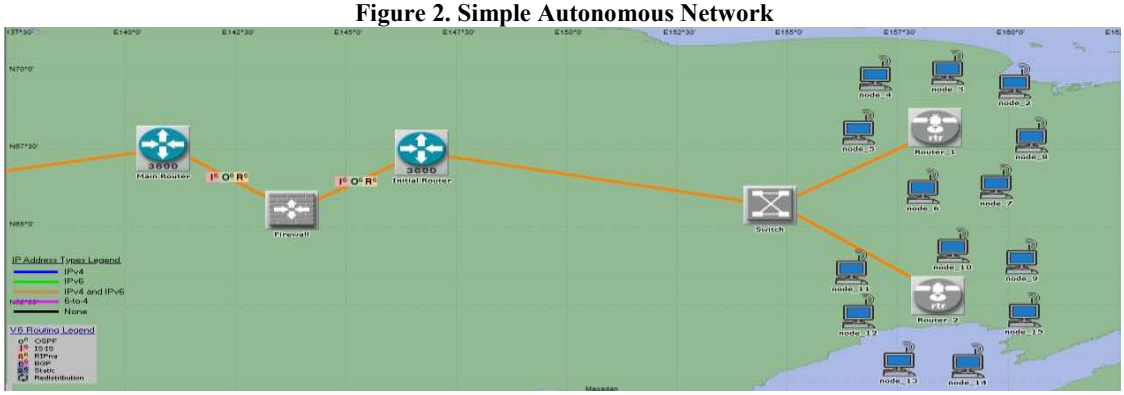

Figure 3. Autonomous Network defining Applications

A) Basic IPv6 environment with RIPng protocol This scenario is made to operate under IPv6 environment that uses only RIPng protocol to gather routing information. The autonomous networks are intended to connect via DS3 or T3 communication links with the ip_cloud.

B) Reliability to Basic IPv6 environment with RIPng This scenario is implemented in an IPv6 environment that supports its routing mechanism under RIPng protocol and also along with OSPF and IS-IS routing protocol in which stations are also connected via DS3 communication link.

The working environment consists of an ip_cloud, six subnets, out of which five subnets are made similar consisting of a wireless LAN (WLAN) using 100BaseT links connected with two routers (namely WLAN_Router1 and WLAN_Router2) and one Ethernet Switch, two CISCO 3640 Routers (one initial & one main router further interlinking to ip_cloud) and one firewall [11]; other one subnet is made as centralised autonomous network in which application servers are made to locate and are made to available for every access made), PPP protocol, connection links (to connect subnets to ip_cloud so that every autonomous network is allowed to

operate), Application Definition (consisting of description or definitions of applications so used) and Profile Definition (defining profiles of each application related to every client).

Fig. 1 depicts the overall schema of cloud- based network, along with this; Fig. 2 represents the architecture that defines to a particular autonomous network and saving their status at the corresponding servers. The corresponding servers are depicted in Fig. 3 respectively.

IV. ANALYSING THE SIMULATION

This section deals with analysis of simulations onto different scenarios and working environments. The results shown for the measuring factors such as delay, throughput, etc. are made to be taken with care. The simulating results will be as following:

A. **Queuing Delay:** Queuing Delay [9] can be defined as amount of time a data packet spends while waiting in a queue at a particular for its successful transmission or to achieve a positive delivery before timeout has occurred.

Fig. 4 and 5 represents the queuing delay factor in both scenarios.

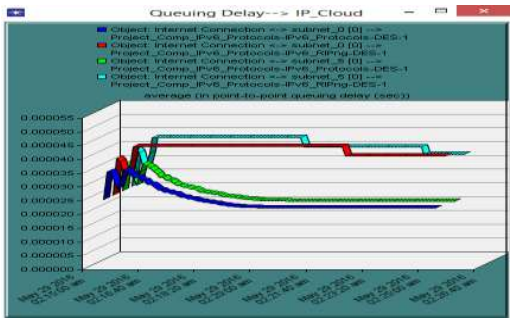

Figure 4.Internet Connection (Subnet 0 and Subnet 5): Queuing Delay

Fig. 4 depicts a queuing delay, in both scenarios, caused while entering a query into an ip_cloud. This represents delay that has caused when multiple users from different networks are trying to get information by sending queries. Out of these four graphs it has been analysed that IPv6 with OSPF and IS-IS works better than simple RIPng.

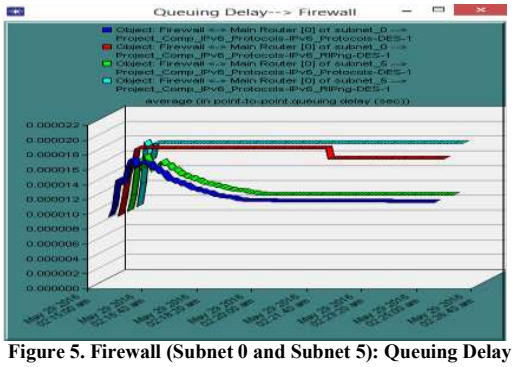

Figure 5. Firewall (Subnet 0 and Subnet 5): Queuing Delay

Fig. 5 depicts queuing delay on firewall of the subnet (Subnet 0 and Subnet 5) in both scenarios onto point-to-point connection link between Main Router and firewall while queries are fired onto it by different network domains. Delay has reduced when dealt with OSPF and IS-IS in IPv6 environment.

B. **Throughput:** Throughput [2] can be defined as a measurement of rate of production while communication. It depicts rate of successful delivery of data packets. Fig. 6 and 7 represents the load factor in both scenarios.

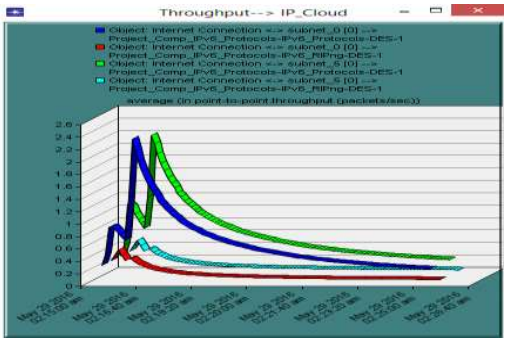

Figure 6. Internet Connection (Subnet 0 and Subnet 5): Throughput

Fig. 6 depicts throughput while receiving requested information through Internet Connection that is made to an ip_cloud. It can be seen very clearly that IPv6 performs better with OSPF and IS-IS i.e. there is a gradual in throughput and reliability is achieved.

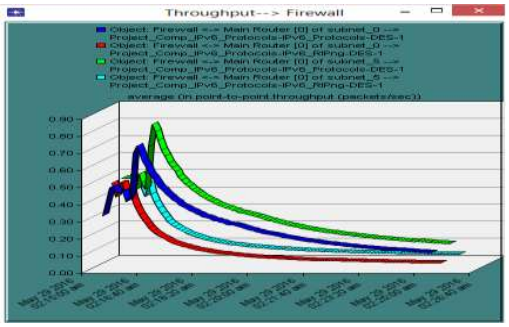

Figure 7. Firewall (Subnet 0 and Subnet 5): Throughput

Fig. 7 depicts throughput in a network while multiple users are making access to the channel. Throughput is increased with respect to numbers of packet in OSPF and IS-IS scheme.

C. **Utilization**: Utilization [12] is a measurement tool which is responsible to measure the performance success of any communication. The utilization proves for the best throughput factor achieved in any aspect. Fig. 8 and 9 depicts the utilization in a network consisting of both scenarios.

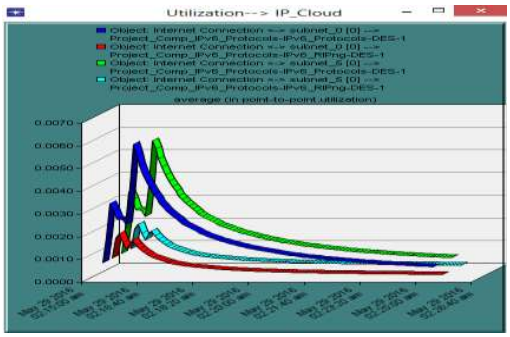

Figure 8.Internet Connection (Subnet 0 and Subnet 5): Utilization

The graph in Fig. 8 depicts utilization in both the scenarios. It can be seen very clearly that here also IPv6 with OSPF and IS-IS works in much better manner than simple RIPng.

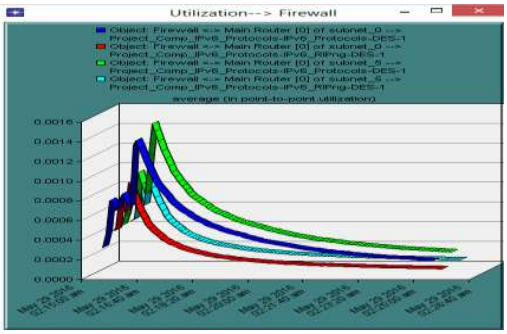

Figure 9.Firewall (Subnet 0 and Subnet 5): Utilization

Fig. 9 is recognized for its results where graph seems to produce better results while performing in IPv6 environment under OSPF and IS-IS protocols.

V. CONCLUSION

The simulation in the proposed paper is based on working of stations in an IPv6 environment in which the stations in each of the autonomous network system is intended to share information via DS3 communication links. The analysis can be clearly seen by all the graphs so generated. The gradual increase in throughput under OSPF and IS-IS protocol schemes can be said as on reliable basis. This is because when simple RIPng protocol is used, it just maintains the routing information and doesn't encourage such efforts so as to increase throughput and utilization. Rather, when it is talked about OSPF and IS-Is protocols, they maintain a dynamic routing table and makes a topology then after. This topology makes possible to automate a lowest path i.e. least cost and least maintenance path whenever there is change in topology. Hence, in this way a factor of reliability is attained while dealing with OSPF and IS-IS routing protocols.

REFERENCES

[1] "Cloud Computing: Clash of the Clouds", The Economist, 2009

[2] Shweta Singh, Priyanka Mudgal, Priyadarshini Chaudhary and Arun Kr. Tripathi, "Comparative Analysis of Packet Loss in Extended LAN Environment", International Journal of Computer Applications (IJCA), ISSN NO: 0975-8887, 2015

[3] www.en.wikipedia.org/wiki/Point-to-Point _Protocol

[4] "IPv6 Address Allocation Management", Internet Architecture Board, 1995

[5] G. Malkin, R. Minnear, "RIPng for IPv6", The Internet Society, 1997

[6] Smith, Lucie, Lipner and Ian, "Free Pool of IPv4 Address Space Depleted", 2011

[7] R. Coltun, D. Ferguson, J. Moy and A. Lindem, "OSPF for IPv6", The Internet Society OSPFv3, 2008

[8] Asmussen, Søren, Glynn and W. Peter, "Stochastic Simulation: Algorithms and Analysis", Springer Series Stochastic Modeling and Applied Probability, Volume 57, 2007

[9] Shweta Singh and Arun Kr. Tripathi, "Analysis of Delay and Load Factors in Wired and Wireless Environment", Second International Conference on Recent Trends in Science, Technology, Management and Social Development (RTSTMSD-15), IJSTM, and ISSN NO: 2321-1938, 2015

[10] J.R. Davis and A. K. Reilly, "T-Carrier Characterization Program – Overview", Bell System Technical Journal, Volume 60, Issue 6, 1981

[11] www.en.wikipedia.org/wiki/Firewall _(computing)

[12] www.colasoft.com/capsa/network_bandwidth_ analyzer.php