International Journal of Engineering & Technology, 8 (1.6) (2019) 23-29

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Design and Implementation of Data and Voice Redundancy and Line Aggregation for VOIP with multiple links

Tun Tun Oo [1*], Africa Aaron Don[2]

Department of Electronics and Communications Engineering,
De La Salle University Manila, 2401 Taft Avenue, Manila, Philippines
**Corresponding author Email: tuntunoo@dlsu.edu.ph*

Abstract

In the previous wired PSTN (Public Switched telephone network), ADSL system has used to get the Internet. In the present, VOIP (Voice Over Internet Protocol) technology is used for communication to use internet by using packet switching technique. PBX (Private Branch Exchange) was launched to substitute over common PSTN systems. In old telephone network, PSTN is more consumed phone bills or oversea costs than VOIP talk service. In this paper, the VOIP is used redundancy technologies by going the performance secure network paths about some security techniques to secure a network. Ethernet gateway redundancy is based on the concept of redundancy group. A redundancy group can contain one or more bridge groups located on the same or different gateways. A redundancy group can operate in two modes. The first one, which is the default mode, is active-passive. In active-passive mode, only one bridge group is active and all others are in hot-standby state. In case the active bridge group fails, another member from the same redundancy group is selected and activated. In active-active mode, all bridge groups are active and load balancing is enabled. Load balancing allows the user to distribute the load of IB nodes among all bridge groups of the redundancy group. In case of a bridge group failure, the load of the IB nodes is redistributed among the remaining bridge groups.

Keywords: *ADSL; HSRP; OSPF; PSTN; PBX; VOIP*

1. Introduction

For many businesses, downtime in VoIP communication systems translates to company losses and lost opportunities. For this reason, VoIP network infrastructure and call continuity should be part of every company's communication plan. VoIP redundancy involves designing and implementing redundancy at both the VoIP and network infrastructure levels. A VoIP communications system has several components, each providing a specific function that helps deliver the necessary services to the enterprise and its customers. These components, subject to redundancy, are VoIP PBX, voice gateways and messaging and presence servers. The VoIP PBX, often called the "VoIP server," is the central processing system that handles call routing, IP phone registration, user accounts, dialing privileges and other similar functions. With modern systems, these servers often leverage virtualization technology to quickly restore a new hardware in the event of a failure.
This paper could have a layer three network model such Core, Distribution and Access layer for large business to a two layer network model (Core/distribution and access layer) for small business. Indeed, the core switches will distributed via the voice gateways and configured to automatically route calls from a voice gateway to another systems. The technology of VOIP (Voice Over Internet Protocol) has changed the our life's work and collaborate. Furthermore, a redundant design is considered especially for large enterprises network to increased reliability and technological evolution.
An effective design is to certain redundancy that the key ingredient is implemented at the VOIP voice call and other network infrastructure.
This paper is also implemented the EtherChannel technology. EtherChannel is a ports link aggregation technology developed by Cisco that it is supplied fault-tolerant highest data speed links between Switches, Routers, and Servers. EtheChannel technology allows multiple physical Ethernet links to combine into one logical channel. EtherChannel technology allows grouping of several physical Ethernet links to create one logical Ethernet link for the intending of supporting fault-tolerance and highest data speed links between switches, routers and servers. The main advantages of EtherChannel technology is that load sharing of traffic among the links is allowed in the channel as such as one or more links in the EtherChannel fail that it is redundancy in the event. EtherChannel is a Cisco Copyrighted term that it is also called "Link Aggregation".[2]

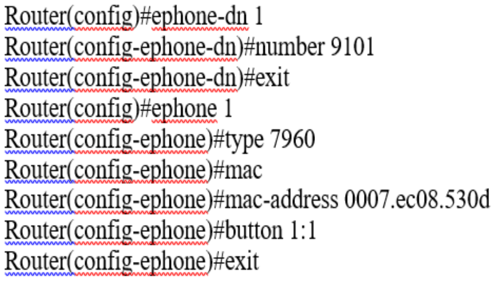
2. Significance and Statement of VOIP

This paper is significance for data redundancy and line aggregation (increase bandwidth) of VOIP (Voice Over Internet Protocol). The data redundancy is also called HSRP (Host Standby Routing Protocols).HSRP is the standard of Cisco of supporting the path of high data speed network availability. This is supporting first hop redundancy for Internet Protocol (IP) host. IEEE 802 LAN is configured with a default gateway IP address. IP traffic without relying on the availability of any single router is routed by HSRP. It enables a set of routers to operate with the appearance of a single virtual router or default gateway to the nodes via a Local Area Network (LAN). If HSRP is configured on a segment of network, it will support physical address (MAC) and logical Address IP that it is distributed among a group of networks or routers. Physical Address and logical address of a virtual router is allowed two more HSRP configuration routers to use MAC address. The virtual routers are configure to provide round robin or alternate to each other such as active and standby. One of the routers is choice to be the active router and the other router is standby router because one router of the group is failed that while another router is suddenly operated within 2 Sec.

This paper have discovered the problems that they are VOIP IPphone number assign problems, OSPF (Open Shortest Path Fast) routing Problem, Spanning Tree Protocol problem and Voice called connection problems via difference networks.

2.1. VOIP IPphone Number Assignment Problems

The purpose of this paper is to solve the impact of Voice Over Internet Protocol (VOIP). And then, the background knowledge on VOIP service will be provided. This problem have important things that they will be matched mac-address and ephone number assign.



```
Router(config)#ephone-dn 1
Router(config-ephone-dn)#number 9101
Router(config-ephone-dn)#exit
Router(config)#ephone 1
Router(config-ephone)#type 7960
Router(config-ephone)#mac
Router(config-ephone)#mac-address 0007.ec08.530d
Router(config-ephone)#button 1:1
Router(config-ephone)#exit
```

2.2. OSPF Routing and Switching Problems

OSPF (Open Shortest Path First) is one of Interior Gateway Protocol (IGP) that routes Internet Protocol (IP) packets within a single routing network domain only. OSPF (Open Shortest Path First) can calculate the best and shortest path of routers by using the Shortest Path First (SPF) algorithm. The O means open to the public and unrestricted corresponding routing protocols such as Cisco's IGRP and EIGRP. This algorithm can also communicate other routing protocols. Moreover, the correlation of RIPv1 to RIPv2 and then OSPFv3 cannot reverse direction with OSPFv2. Today, OSPFv3 is improving the significantly protocol than OSPFv2 to make Ipv6 migration.

Open Shortest Path First version 3 (OSPFv3) is precise in RFC 2740 that are some high level conformable between the transform of RIPv1 to RIPv2 and OSPFv3 to OSPFv2. In fact, OSPF v3 exert the same basic of routing information as OSPFv2 that are also work as the Shortest Path fast (SPF) algorithm, router ID, DR (designate router) election, areas ID. Timers and metrics are also the same that can be constant or variables. If the OSPF v3 wanted to use, the operation OSPFv2 would be understand as different and primarily operation and LSA (Link state Advertisement) formats. The differences between OSPF version 2 and OSPF version 3 are developed the link state Routing protocol from OSPF v2 and then specially exerted for IPv6 (Internet Protocols version 6) networking.

DR (Designate Router) and BDR (Backup Designate Router) are selected the following procedures. In the OSPF routing, DR and BDR are always defined because it is reduced the traffic and bandwidth. DR is mean Designate Route that it is mainly used LSDB systems. BDR is a backup DR that is secondary DR if DR fail or shutdown, it will be serve as DR (Designate router). The Designate router (DR) and (Backup Designate Router) BDR achieve the neighbor routers and permute routing information with all of routers on the same network and same area. In fact, the election of DR and BDR will make this time. If DR and BDR could not be choice the routers that they are low priority and router Id in the same area, they will be defined the DR others. DR others do not work any neighbor with each other. This reduces of the number of neighbor routers in broadcast and non-broadcast multiple access (NBMA) Networks. Indeed, this process are reducing of network traffic and saving bandwidth resources.

A router that is using OSPF routing information will detect the lists of neighbors and do not care any router that is be haven a priority of zero that the router is neglected to become The Designate router (DR) or (Backup Designate Router) BDR. The all of OSPF (open shortest Path first) algorithm run that routers are having zero priority by removing the eligibility lists. Chronicle The Designate router (DR) or (Backup Designate Router) BDR in LSDB list that is all of neighbor routers.

(1) Examine the new DR and BDR from the list of LSA that select the one with the highest priority. When comparing priorities, then continue selection the highest router ID (IP address) exception of priority zero of router. Again, if a connected finds, select the one with the highest router ID.

(2) Determine the lists of router LSA that select the only one with the highest priority to choice the (Designate routers) DR from the lists of the highest router ID. If there are not selected DR that is lists of any routers, then promote the new BDR to become Designate routers (DR).

(3) The steps (2) and (3) need to repeat frequently until a router becomes the DR or BDR.

(4) If the router that it elected (Designate router) DR, the interface will set to DR, if the router that it elected (backup designate router) BDR, the interface will set to BDR. Differently, all of other router that may not elect in the lists of LSDB specified the interface state to designate router other (DR other).

(5) On the non-broadcast multiple access (NBMA) network, the routers that is elected DR and BDR must start sending hello packets and dead time interval to neighbors that are not eligible to change state DR.

(6) If the select routers that choice DR and BDR, any of high level priority and router ID will not be become DR and BDR that the routers is connected after selecting DR and BDR.

(7) If the Designate router (DR) and/or Backup Designate router (BDR) has break down states such as power shutdown and other damage, all of infrastructure by using same area will need to be changed and repeat election DR and BDR again.

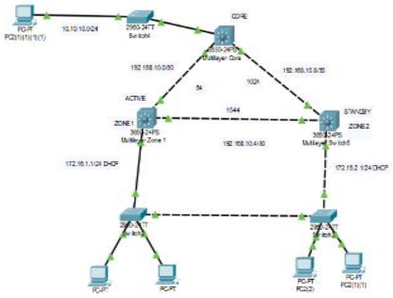
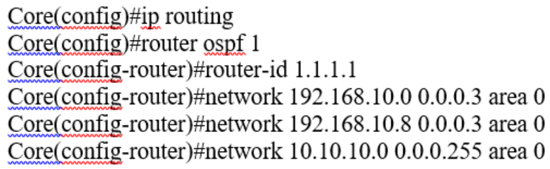


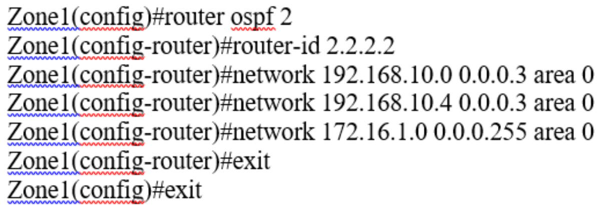
Fig 1: The OSPF Network Diagram with bandwidth

Core L3 Switch configuration commands



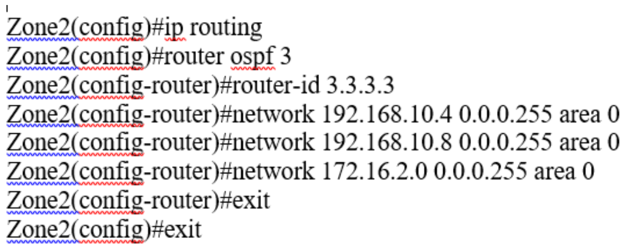
```
Core(config)#ip routing
Core(config)#router ospf 1
Core(config-router)#router-id 1.1.1.1
Core(config-router)#network 192.168.10.0 0.0.0.3 area 0
Core(config-router)#network 192.168.10.8 0.0.0.3 area 0
Core(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

Zone 1 L3 Switch Configuration



```
Zone1(config)#router ospf 2
Zone1(config-router)#router-id 2.2.2.2
Zone1(config-router)#network 192.168.10.0 0.0.0.3 area 0
Zone1(config-router)#network 192.168.10.4 0.0.0.3 area 0
Zone1(config-router)#network 172.16.1.0 0.0.0.255 area 0
Zone1(config-router)#exit
Zone1(config)#exit
```

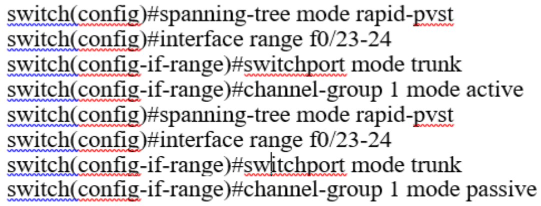
Zone 2 L3 Switch Configuration



```
Zone2(config)#ip routing
Zone2(config)#router ospf 3
Zone2(config-router)#router-id 3.3.3.3
Zone2(config-router)#network 192.168.10.4 0.0.0.255 area 0
Zone2(config-router)#network 192.168.10.8 0.0.0.255 area 0
Zone2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Zone2(config-router)#exit
Zone2(config)#exit
```

2.3. Spanning Tree Protocols Problems and Etherchannel

The Spanning Tree Protocol (STP) is a layer-2 protocol of OSI model that it is avoided network loop for any bridged LAN and switch. It is also called loop-free topology. SPT allows the network infrastructure that it is include redundant links to provide automatic backup lines. If an active link fails with the damage of bridge loops or the need for manual disable/enable of the back links. The switch that it is connected like ring or other multiple links must be avoided spanning tree because they will be in flooding the network. The Spanning Tree Protocol (STP) is the IEEE standard 802.1D. IEEE 802 is mean for Institute of Electrical and Electronics Engineers and 802 at 1980 February rule. STP creates a loop within the mesh, ring or star network of layer-2 bridges is connected between Ethernet switches that it is also operate bridges. And then it will disables these links that are not part of the tree, leaving a single active line between any two or more network nodes.
Spanning-tree and ether channel LACP (Line Aggregation Control Protocol) solution commands



```
switch(config)#spanning-tree mode rapid-pvst
switch(config)#interface range f0/23-24
switch(config-if-range)#switchport mode trunk
switch(config-if-range)#channel-group 1 mode active
switch(config)#spanning-tree mode rapid-pvst
switch(config)#interface range f0/23-24
switch(config-if-range)#switchport mode trunk
switch(config-if-range)#channel-group 1 mode passive
```

2.4. Voice Called Connection Problems via Difference Networks

This problem is carefully controlled to each difference network infrastructure because this issue is very important to called voip voice via difference networks.

The solution of the voip voice call via difference network command.

```
Router(config)#dial-peer voice 9100 voip
Router(config-dial-peer)#session target ipv4:172.16.1.3
Router(config-dial-peer)#destination-pattern 91..
```

3. Methodology of data redundancy and line Aggregation for VOIP

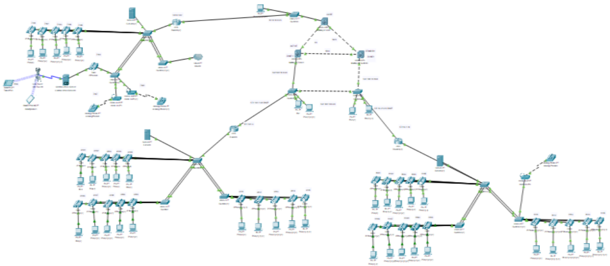


Fig 2: Data and Voice Redundancy and Line Aggregation of VOIP network infrastructure

The system that it is emphasized data redundancy and line aggregation methodology in this paper is included three group VOIP (Eg. Number 71.. , 81… and 91….), L2 Switch that it is used line aggregation (etherchannel) , L3 switch routing that it is used OSPF (Open Shortest Path Fast) and HSRP (Host Standby Routing Protocol). Moreover, the server would to also use DNS , Web server(HTTP) and Log of the system.

Each system of three group VOIP has one cisco 2811. This cisco router is configured DHCP (Dynamic Host Configuration Protocol) and sub-interface technology. There are three sub-interfaces that they are three IP such as 192.168.10.x for voice , 192.168.20.x for Data and 192.168.30.x for other management.

Table 1: The Metric Cost of OSPF

Interface type	bandwidth	Cost
Fast Ethernet and faster	100 Mb/s and higher	1
Ethernet	10 Mb/s	10
E1	2 Mb/s	48
T1	1.544 Mb/s	64
128bps	128bps	781
64kbps	64kbps	1562
56kbps	56kbps	1785

Cost = Reference bandwidth / Interface bandwidth in bps.

Cisco uses 100Mbps(10^8) bandwidth is the reference bandwidth. Reference bandwidth mean that it is arbitrary value in RFC(2339) OSPF.

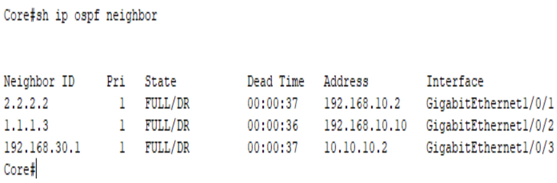
The cost of a link in OSPF can be verified using the "show ip ospf interface <interface name> <interface ID>" command.

At the OSPF, the L3 switch is used as the router configuration instead the router because the switch is more powerful routing and switching than ordinary router. In the OSPF system, the cost calculation would be used to calculate caudal the cable cost and port of fastethernet or gigabitethernet.

$$\text{Cost} = 10^8/\text{interface bandwidth in bps}$$

4. Data and Result of VOIP

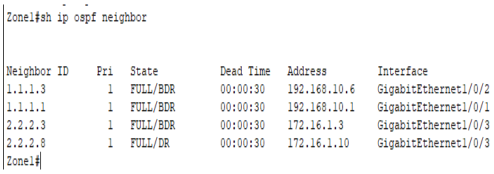
The neighbor of OSPF is showed the following figure. The Zone1 L3 switch has more neighbor than other L3 switch because the zone1 L3 is active situation of HSRP system.



```
Core#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:37    192.168.10.2    GigabitEthernet1/0/1
1.1.1.3           1   FULL/DR         00:00:36    192.168.10.10   GigabitEthernet1/0/2
192.168.30.1      1   FULL/DR         00:00:37    10.10.10.2      GigabitEthernet1/0/3
Core#
```

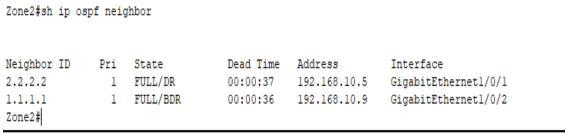
Fig 3: OSPF Neighbour of Core L3 Switch



```
Zone1#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.3           1   FULL/BDR        00:00:30    192.168.10.6    GigabitEthernet1/0/2
1.1.1.1           1   FULL/BDR        00:00:30    192.168.10.1    GigabitEthernet1/0/1
2.2.2.3           1   FULL/BDR        00:00:30    172.16.1.3      GigabitEthernet1/0/3
2.2.2.8           1   FULL/DR         00:00:30    172.16.1.10     GigabitEthernet1/0/3
Zone1#
```

Fig 4: OSPF Neighbour of Zone1 L3 Switch



```
Zone2#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:37    192.168.10.5    GigabitEthernet1/0/1
1.1.1.1           1   FULL/BDR        00:00:36    192.168.10.9    GigabitEthernet1/0/2
Zone2#
```

Fig 5: OSPF Neighbour of Zone2 L3 Switch

The result of VOIP voice calling procedure is the following test.

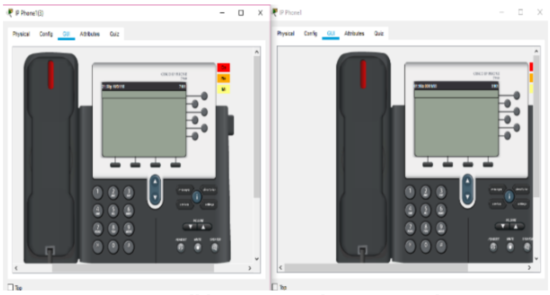


Fig 6: VOIP Call between numbers 9101 and 7101

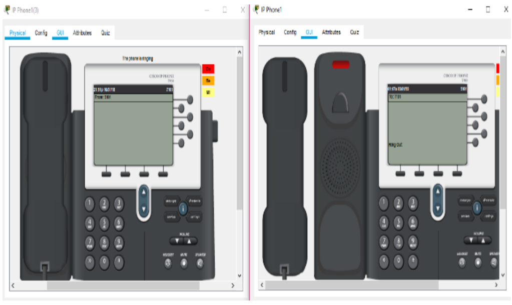


Fig 7: VOIP dial and Ring Process between numbers 9101 and 7101

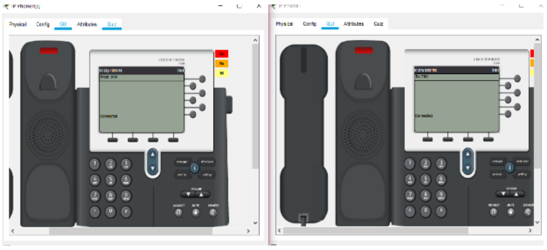


Fig 8: VOIP Pick up between numbers 9101 and 7101

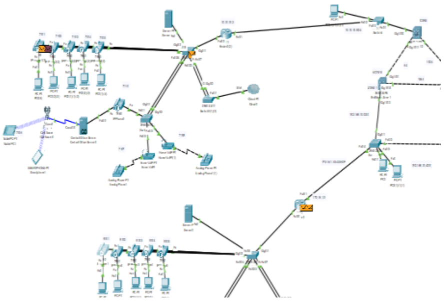


Fig 9: VOIP data flow simulation between numbers 9101 and 7101

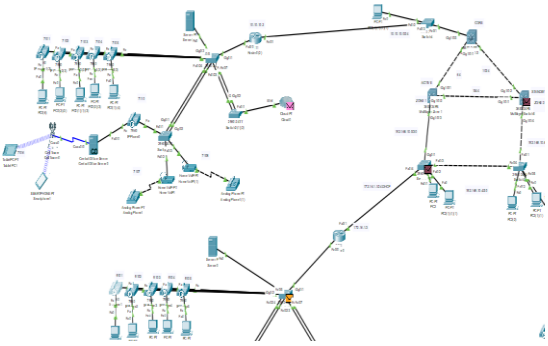
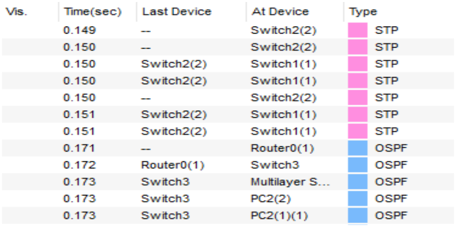
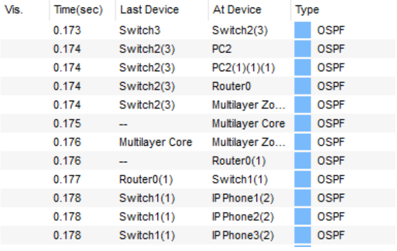


Fig 10: VOIP Packet flow simulation between numbers 9101 and 7101



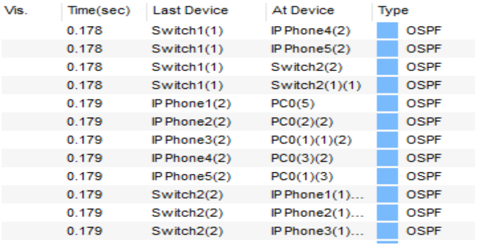
Vis.	Time(sec)	Last Device	At Device	Type
	0.149	--	Switch2(2)	🟪 STP
	0.150	--	Switch2(2)	🟪 STP
	0.150	Switch2(2)	Switch1(1)	🟪 STP
	0.150	Switch2(2)	Switch1(1)	🟪 STP
	0.150	--	Switch2(2)	🟪 STP
	0.151	Switch2(2)	Switch1(1)	🟪 STP
	0.151	Switch2(2)	Switch1(1)	🟪 STP
	0.171	--	Router0(1)	🟦 OSPF
	0.172	Router0(1)	Switch3	🟦 OSPF
	0.173	Switch3	Multilayer S...	🟦 OSPF
	0.173	Switch3	PC2(2)	🟦 OSPF
	0.173	Switch3	PC2(1)(1)	🟦 OSPF

Fig 11: VOIP Data flow Process between numbers 9101 and 7101



Vis.	Time(sec)	Last Device	At Device	Type
	0.173	Switch3	Switch2(3)	🟦 OSPF
	0.174	Switch2(3)	PC2	🟦 OSPF
	0.174	Switch2(3)	PC2(1)(1)(1)	🟦 OSPF
	0.174	Switch2(3)	Router0	🟦 OSPF
	0.174	Switch2(3)	Multilayer Zo...	🟦 OSPF
	0.175	--	Multilayer Core	🟦 OSPF
	0.176	Multilayer Core	Multilayer Zo...	🟦 OSPF
	0.176	--	Router0(1)	🟦 OSPF
	0.177	Router0(1)	Switch1(1)	🟦 OSPF
	0.178	Switch1(1)	IP Phone1(2)	🟦 OSPF
	0.178	Switch1(1)	IP Phone2(2)	🟦 OSPF
	0.178	Switch1(1)	IP Phone3(2)	🟦 OSPF

Fig 12: VOIP Data flow Process between numbers 9101 and 7101



Vis.	Time(sec)	Last Device	At Device	Type
	0.178	Switch1(1)	IP Phone4(2)	🟦 OSPF
	0.178	Switch1(1)	IP Phone5(2)	🟦 OSPF
	0.178	Switch1(1)	Switch2(2)	🟦 OSPF
	0.178	Switch1(1)	Switch2(1)(1)	🟦 OSPF
	0.179	IP Phone1(2)	PC0(5)	🟦 OSPF
	0.179	IP Phone2(2)	PC0(2)(2)	🟦 OSPF
	0.179	IP Phone3(2)	PC0(1)(1)(2)	🟦 OSPF
	0.179	IP Phone4(2)	PC0(3)(2)	🟦 OSPF
	0.179	IP Phone5(2)	PC0(1)(3)	🟦 OSPF
	0.179	Switch2(2)	IP Phone1(1)...	🟦 OSPF
	0.179	Switch2(2)	IP Phone2(1)...	🟦 OSPF
	0.179	Switch2(2)	IP Phone3(1)...	🟦 OSPF

Fig 13: VOIP Data flow Process between numbers 9101 and 7101

5. Review of the Related Literature

In the Internet new era, Traditional Public Switched Telephone network (PSTN) services technology is needed to understand how they are work and the new Internet services can coexist. Internet is used in ADSL lines by using PSTN that it is limited to distance. The best-effort based IP will have to maintain the service that it is expected customers from PSTN because PSTN network wired can cause the line broken, noise and attenuation effort. The new contribution is analyzed the model VOIP traffic with multiple data and voice traffic. This model is based on the stochastic fluid flow mode. The VOIP traffic to a data and voice link is also considered the effect that it is delay and loss. Moreover, the capacity of traffic will be requirement to maintain a certain Qos (Quality of Service).[4]

The VOIP configuration is simple and easy configuration. But, the match of mac address and phone number is carefully assignment. If the VOIP technology is improve than PSTN, it will decrease toll call cost and maintain cost. Furthermore, their cable is used only fiber and RJ45 to maintain the garnishment of city, road and township. The author will be expected the next paper about wire and wireless effort between PSTN cable and VOIP cable. And then security issue of VOIP.

The VOIP promises to be a disruptive an application in relative short lifespan of the Internet. However, VoIP users and service providers must become familiar with develop defense against and counter measures for the litany that can be perpetrated against VoIP applications, devices that host host these applications, and the communications services that connect them. So, the security risk is also considered issue.

It brings many advantages to subscribers and operators, such as flexibility, cost reduction, and quality of service for all types of applications. VoIP is one of the most used applications until today. In this paper, we evaluated the performances of VoIP in Next-Generation Networks taking into account various codecs and transport protocols while increasing the number of users.[1]

6. Conclusions

The global can change (Internet Protocol Version 4) IPv4 to IPv6 transition that can provide developing the ISP (Internet Services Provider) or IXP (Internet Exchange Provider) with equipment and technologies for low cost VOIP network. An IPv4 VOIP can serve the carriers to realize future the issue for a new VOIP development. If the IPv4 to IPv6 projects is succeed, governments may find those project attractive for future funding and change the cable natures and equipment of corresponding changed cables.

The proposed system of VOIP is cost-effective , scalable and can extend IPV4 VOIP devices by giving developing country lowest cost VOIP network with a free prospective for global connectivity.

The VoIP application may be interested the users who they use Internet because they do not need to any cost for toll call by using the Internet. In fact, the VoIP would be appropriately ESIM. ESIM is one phone number between various mobile carriers in the country.[3]

The next contribution is experted the basic features of VOIP,QoS and IPv6 by using BGP (Border Gateway Protocol). Issues associated with VOIP and QoS as well as reasons as to IPv6 will help in addressing QoS issues in VOIP as against IPv4 have been highlighted and BGP is communicated to the difference routing protocols.[2]

The sniffer program provides for data breach through man in the middle attacks as it helps to sniff IP Source and Destination address and helps in identifying the geographic locations of endpoints of connections. Risk analysis and Quality of service using VoIP management protocols and its study will be the scope of further research in the SIP network.[6]

Acknowledgement

This paper was strongly supported by Dr Aaron Don M. Africa, Associate Professor, Department of Electronic and Communication Engineering, GOKONGWEI College of Engineering.
I thank my colleagues from GOKONGWEI College of Engineering, De La Salle University who provided insight and expertise that greatly assisted the research.

References

[1] Ayoub BAHNASSE, Abdelmajid BADRI, Fatima Ezzahraa LOUHAB, Mohammed TALEA, Azeddine KHIAT , Bishwajeet PANDY “Behavior analysis of VOIP performances in next-generation networks” International Journal of Engineering & Technology, 7 (3.15) (2018) 353-359

[2] E.M. Dogo, A. Ahmed and O.M. Olaniyi “Cross-Layer Integration Approach for Improving QoS for IPv6 Based VOIP” International Journal of Engineering and Technology Volume 4 No. 9, September, 2014

[3] Olga S. Mill “Managing IPv4 / IPv6 VOIP Interoperability Using Server-to-Server Approach”2012

[4] Shenquan Wang ; Z. Mai ; Dong Xuan ; Wei Zhao "Implementation of QoS-Provisioning system for voice over IP" Real-Time and Embedded Technology and Applications Symposium, 2002. Proceedings. Eighth IEEE , 24-27 Sept. 2002

[5] http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-etherchannel-in-cisco-switches-and-routers.php

[6] Ms. Toshima Singh Rajput , Ms. Kamini Maheshwar “VOIP PACKET ANALYZER FOR DETECTING THREATS IN SIP NETWORK” International Journal of Advanced Research in Computer Science Volume 8, No. 9, November-December 2017