# A Study on Performance of IPv4, IPv6 on Wireless Network (IEEE 802.11ac) with Wireless Security Protocols (WEP, WPA and WPA2)

Thanaphon Pattanasophon[1],Sita Thanee[2],Sukrita Limpayaraya[3],Thongchai Kaewkiriya[4]

*Information Technology, Thai-Nichi Institute of Technology*
*1771/1, Pattanakarn Road, Suanluang, Bangkok, Thailand*
[1]Pa.thanaphon_st@tni.ac.th
[2]Th.sita_st@tni.ac.th
[3]Li.sukrita_st@tni.ac.th
[4]ThongChai@tni.ac.th

***Abstract*— Due to the rapid expansion of Mobile Device, which connected through wireless network. The replacing of Internet Protocol version 4(IPv4) to Internet Protocol version 6(IPv6). This study has an aim to compare data loss rate, transmission delay, and throughput over a wireless network. The first step is identifying wireless networking standard in IEEE 802.11ac. The second step is upload example large file on IPV4 with wireless security protocols test. The third step is an upload example multimedia file on IPV6 with wiles security protocols test. The fourth step is analyzing the performance of the IPV4, IPV6 on the wireless network. The last step is providing result. The result is the IPV4 network is more stable over IPV6.**

***Keywords*— Wireless Network , IPv4 , IPv6 , Wireless Security Protocols**

## I. INTRODUCTION

Nowadays, the internet has become very important for human life. The internet has used as well-known and it has more devised to connect the internet than before. And the each devised has to connect with the number of IP Addresses. Presently, we are using IPv4 and will be changing from IPv4 system to IPv6 system for supporting the devised to connect to the network. IPv4 can support the devised only number 232 but it is not enough for today to connect to the internet. IPv6 can support with devising up to number 2128 so it can help to support many devised. [1]

If it is working more and it is preparing to improve for changing IPv6, It is therefore necessary to study the performance of IPv6 the network for comparing with IPv4. In the current trial show the efficiency for analyzing of Delay (Round Trip time), Packet Lose and Throughput into IEEE802.11ac network. Using encryption by WEP, WPA and WPA2. In the case that does not have the background traffic to get the best comparison with Delay (round Trip time), Packet Loss and Throughput. The result of researching give us the experiment the concern with A study on performance IPv4, IPv6 and dual stack networks with QoS enabled, It showed that the efficiency work of IPv4 is better than IPv6 and Dual Stacks. However, the researcher makes the experiment for A Study on Performance of IPv4 and IPv6 on Wifeless Network (IEEE 802.11ac) with Wireless Security protocols (WEP, WPA and WPA2) to measure the happening of delay, packet loss and Throughput. The results can be applied to the design and use within the enterprise to achieve maximum efficiency.

## II. RELATED LITERATURE

### *A. Previous Work*

*1) A Study on Performance of IPv4, IPv6 and Dual-Stacks Networks with QoS Enabled* [2]

The behavior of the Internet uses a variety of results in the use of the Internet more to the number of the Internet Protocol are likely to be in the near future. The Investigator is the research that test compares the performance that test to compare the performance test the data by the value of the performance in 3 is packet loss, delay and throughput by the packet loss and delay is calculated from the results of the ping. To compare the packet loss from the trial found that while the network has a FTP load as the background traffic in the packet loss. When you make the case of packet loss much less. The part that does not have a background traffic rate of packet loss almost will not occur without that will do or do not make Qos. To compare the delay that does not have the background of the traffic network that do and do not make the QoS average delay, at least equal the section that has the background traffic found that the network that does not make the QoS is the average delay high but in the QoS setting delay is evenly. To compare the throughput does not have a background traffic in the network has a high rate of similar with background traffic. The Network IPV4, IPV6, and dual stack that does not have the QoS values will be throughput much less. A summary of the results of the test the performance of the network IPv4, IPv6, and dual stack that is made and does not make the QoS. It was found that the overall network IPV6 high-stability than IPV4 Networks and dual stacks.

*2) A Performance Comparison of Wireless Communication Over Standard* 802.11*n and WPA*2 [3]

WPA2 encryption for the most popular in the current on the wireless network that the popularity on the standard IPv4, the current Internet access the DVD player 4. Start to find that the number of the IPv4 will be used to is not

sufficient to the use of the internet in the future if occurred. This means that you will not be able to connect to the network device to the internet up again. This research summary for IPv4and IPv6, IPv4, and more effective IPv6 both the Operating System and the size of the most throughput will increase the size of the packet. Enable WPA2, the results of throughput, less than for both the IPv4 and IPv6 on Windows 7 and the Linux Ubuntu Operating System both 32-bit and 64-bit. Turn off the WPA2 encryption can be concluded that the increase of the rate of delays to both the IPV4and IPV6 Security System WPA2 will increase the amount of data sent and negatively impact the performance of the TCP throughput and round trip time on 802.11 n wireless LAN.

*B. Wireless Network (IEEE 802.11ac)*

802.11ac [4], the emerging standard from the IEEE, is like the movie The Godfather Part II. It takes something great and makes it even better. 802.11ac is a faster and more scalable version of 802.11n. It couples the freedom of wireless with the capabilities of Gigabit Ethernet.

*C. IPV4*

The Internet Protocol version 4 (IPv4) [5] is a protocol for use in packet-switched Link Layer networks. IPv4 provides an addressing capability of approximately 4.3 billion addresses.

*D. IPV6*

The Internet Protocol version 6 (IPv6) [6] is more advanced and has better features compared to IPv4. It has the capability to provide an infinite number of addresses. It is replacing IPv4 to accommodate the growing number of networks worldwide and help solve the IP address exhaustion problem.

*E. Wireless Security Protocols*

*1) Wireless Encryption Protocol (WEP)*

Wired Equivalent Privacy (WEP) [7] is a security mechanism for Wireless LAN. It was introduced in September 1999 as part of the IEEE 802.11 security standard. The purpose of Wired Equivalent Privacy (WEP) was to provide security comparable to that of wired networks. RC4 stream cipher is used by WEP to provide confidentiality and CRC-32 for data integrity. The standard specified for WEP provides support for 40 bit key only, but nonstandard extensions have been provided by various vendors which provide support for key length of 128 and 256 bits as well. A 24 bit value known as initialization vector is also used by WEP for initialization of the cryptographic key stream.

*2) Wi-Fi Protected Access (WPA)*

In order to overcome the flaws of WEP, Wi-Fi Protected Access (WPA) [8] was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance. WPA implements the majority of the IEEE 802.11i standard, thus it is an intermediate solution. WPA was intended to address the WEP cryptographic problems without requiring new hardware. WPA provides the following security features.

*3) WI-FI PROTECTED ACCESS 2 (WPA2)*

WPA2 [9] completely implements IEEE 802.11i standard and is an enhancement over WPA. The significant development was the introduction of Counter Mode with Cipher block Chaining Message Authentication Code Protocol(CCMP) which uses block cipher Advanced Encryption Standard(AES) for data encryption, but stream cipher TKIP is available for backward compatibility with existing WAP hardware. WPA2 authentication also has two modes: Pre-Shared Key and Enterprise similar to WPA. WPA2 key generation is achieved by 4-way handshake for deriving Pairwise Transient Key (PTK) and Group Transient Key(GTK) and Group Key handshake for Group Transient Key renewal or host disassociation.

*F. JPerf*

JPerf [10] [11] is a simple framework for writing and running automated performance and scalability tests. When have bad network performance and frequent interruptions are often because of an insufficient network infrastructure. Undersized or old network hardware, a wrong configuration or maybe hardware faults can be a bad influence for the performance in a network and make the work on the PC more difficult. Long waiting periods and even data loss are the consequences. With the application JPerf is possible to measure the information flow-rate (the bandwidth) in a network and to determine the specific weak point.

## III. CONCEPTUAL FRAMEWORK

The trial will test all six patterns by defining experimental IPv4 and IPv6 using encryption, WEP, WPA and WPA2, as well as performance in the Delay (Round Trip Time), Packet Lose and Throughput testing Delay and Packet Lose uses . Packet size 64 Bytes and 16,000 Bytes, and also to measure the performance of IPv4 and IPv6 Packet size Packet small or large.

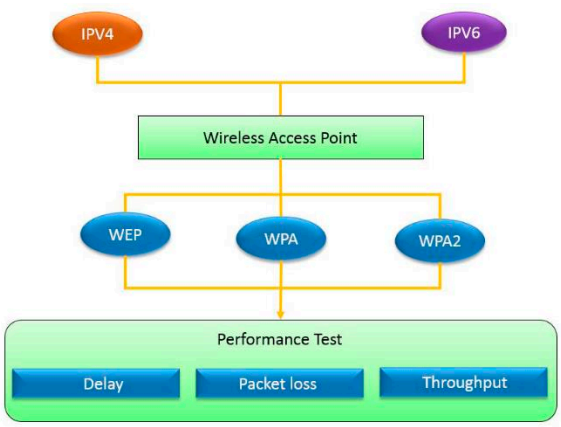


Fig. 1 Conceptual Framework

## IV. IMPLEMENTATION

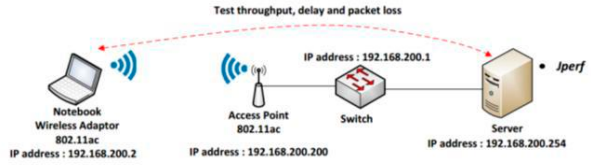


Fig. 2 IPV4 Performance Test

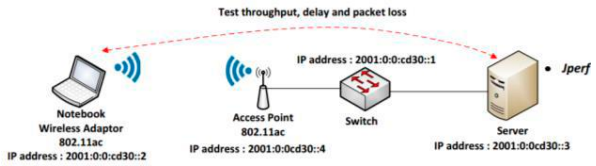


Fig. 3 Example of an image with acceptable resolution

The experiment has connected to a laptop with the network by log-in with password by WEP, WPA and WPA2. This is used for testing the efficiency of the network IEEE802.11ac by IPv4 (Picture 2) and IPv6 (picture 3) In the case of delay (round tip time), packet loss and throughput by log-in with a password, those 3 types can use the key that have maximum 10 characters that have to be same with all 3 types. The experiment is connected by connecting with layer 2 which can use to experiment by using the Ping to send to Packet in the space/side 64 bytes and 16,000 bytes for finding the Delay (round trip time) and Packet Loss. For throughput, the experiment is used by JPerf Program to find Maximum Throughput that will get from the connecting by IPv4 and IPv6.

## V. RESULTS

TABLE I
Wireless Security Protocols Delay Test

| Wireless Security Protocols | Delay | |
|---|---|---|
| | 64 Bytes | 16000 Bytes |
| IPv4 WEP | 1 ms | 10 ms |
| IPv6 WEP | 3.45 ms | 13.47 ms |
| IPv4 WPA | 5.2 ms | 5.8 ms |
| IPv6 WPA | 3.55 ms | 7.28 ms |
| IPv4 WPA2 | 5.4 ms | 5.6 ms |
| IPv6 WPA2 | 3.32 ms | 7.23 ms |

TABLE II
Wireless Security Protocols Packet Loss Test

| Wireless Security Protocols | Packet Loss | |
|---|---|---|
| | 64 Bytes | 16,000 Bytes |
| IPv4 WEP | 0.20% | 0.68% |
| IPv6 WEP | 3.20% | 6.40% |
| IPv4 WPA | 1.38% | 0.44% |
| IPv6 WPA | 1.80% | 2.00% |
| IPv4 WPA2 | 1.46% | 2.20% |
| IPv6 WPA2 | 1.20% | 4.80% |

TABLE III
Wireless Security Protocols Throughput Test

| Wireless Security Protocols | Throughput |
|---|---|
| IPv4 WEP | 21.70 Mbps |
| IPv6 WEP | 19.40 Mbps |
| IPv4 WPA | 119.00 Mbps |
| IPv6 WPA | 113.80 Mbps |
| IPv4 WPA2 | 118.00 Mbps |
| IPv6 WPA2 | 115.20 Mbps |

The results, we can know that the delay and packet loss happen in IPv4. And it will increase the delay and packet loss when we changed password of log-in from WEP to be WPA and WPA2, But IPv6 show that all 3 typed of log-in thru password, the delay will get approximated to 3.45, 3.55 and 3.32 of the followed. For throughput, IPv4 will give throughput better than IPv6 but not much. In the delay and packet loss will be increased by the packet of sending and receiving the information. From the table 1 and table 2 showed that the side/space of 64 bytes of the packet will get delayed. And packet is smaller than the space/side of 16,000 bytes of the packet.

## VI. CONCLUSIONS

Referring to our testing, we had found the Delay and Packet loss. Throughput for sending and receiving information in the network by IEEE802.11ac We found from IPv4 is the lesser than IPv6 in all types of micro packet and macro packet. And the types that have to get through password (Encryption) WEP, WPA and WPA2. It had the effect of delay and packet loss in the network. Referring to the table, we can see that the type of log-in with a password of WEP, it is the smallest to make an effect of delay and packet loss. And Log-in with a password of WPA2, is the most making delay and packet loss of throughput. In table for IPv4 and IPv6 that get very less because the log in with a password by WEP can connect to only the technology IEE802.11a. For throughput of log in with a password by WPA and WPA2 will have Throughput in the same level. IPv4 will have throughput more than IPv6. And the side/space of Packet that will be suitable for making the smallest effective of delay and Packet Loss, is sending and receiving the information by the side/space of micro packet will help to make a less an effect of delay and packet loss than using the side of the macro packet to send and receive information. The result is the IPV4 network is more stable over IPV6.

## ACKNOWLEDGMENT

We are thankful to our colleagues Thai-Nichi institute of technology who provided expertise that greatly assisted the research, although they may not agree with all of the interpretations provided in this paper. Without their precious support it would not be possible to conduct this research.

## REFERENCES

[1] N. Kathleen, B. David L., B. Steven, and B. Fred, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, Dec-1998.

[2] J. Kairat, "A study on performance of IPv4, IPv6 and Dual-Stacks networks with QoS enabled," *Science and technology Journal Thammasat University*, vol. 22, no. 6, pp. 914–924, 2557.

[3] K. K. and B. S., "A Performance Comparison of Wireless Communication Over Standard 802.11n and WPA2," presented at the The Eighth National Conference on Computing and Information Technology, Bangkok, Thailand, 2012, pp. 347–352.

[4] G. Kelly. (2014, December 30) *802.11ac vs 802.11n Wifi: What's The Difference* [Online]. Available: https://www.forbes.com/sites/gordonkelly/2014/12/30/802-11ac-vs-802-11n-wifi-whats-the-difference/#26cb1eb83957

[5] S. Mohd Khairil and H. Rosilah, "Impact of TCP Window Size on IPv4 and IPv6 Performance IJCSNS," *International Journal of Computer Science and Network Security*, vol. 9, no. 12, pp. 129–133.

[6] J. Xie and U. Narayanan, "Performance Analysis of Mobility Support in IPv4/IPv6 Mixed Wireless Networks", IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 962-973, 2010.

[7] A. H. Lashkari et al., "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in *2nd IEEE International Conference on Computer Science and Information Technology*, Bangkok, Thailand, 2009, pp. 48–52.

[8] I. Mohammad and A. Syed A., Eds., *Handbook of Wireless Local Area Networks: Applications, Technology, Security, and Standards*, 1st ed. Boca Raton: CRC Press, 2005.

[9] S. Choudhuri. (28 Mar 2012). *Understanding the Difference Between Wireless Encryption* [Online]. Available: http://blogs .cisco.com/smallbusiness/understanding-the-differenc e-between-wireless-encryption-protocols

[10] Cisco Meraki. (3 Feb 2015). *Troubleshooting client speed and traffic shaping using Jperf* [Online]. Available: https:// documentation.meraki.com Sampa

[11] S. Reeves. (21 Feb 2012). *Using JPerf to check network performance* [Online]. Available: http://www.techrepublic.com