Implementation of IPv6 With MAC Basis In Wireless LAN Network

Fransiscus A.Halim[1], Pujianto Yugopuspito [2], Robert A.Suhim[3]
[1] Computer Engineering, Faculty of Computer Science, Universitas Pelita Harapan
[2]Informatics Engineering, Faculty of Computer Science, Universitas Pelita Harapan
[3] Computer Engineering, Faculty of Computer Science, Universitas Pelita Harapan
Fransiscus_halim@uph.edu[1], pujianto.yugopuspito@uph.edu[2], robert.suhim@gmail.com[3]
Tel : 021-5460901 Fax : 021-5460910

Abstract

It is now important to implement TCP/IP version 6 protocol (IPv6) in the network. Regarding to depletion of IPv4 address, the migration to IPv6 is crucial because the address space is shrinking day by day. Universitas Pelita Harapan (UPH) has a wireless LAN network which has been operating. Wireless LAN network is used as a facility to access the internet. UPH has implemented virtual LAN technology to accomodate a large number of users. Due to inefficient topology, VLAN cannot work efficiently. Wireless LAN network changes are necessary to overcome this inefficiency. The new design of wireless LAN network also considers the implementation of IPv6. The purpose of this thesis is to design the topology of wireless LAN in IPv6 basis.IPv6 implementation process is elaborated through creating an environment called test-bed. Test-bed is a small environment of network for testing purposes. All implementation processes are tested in this environment. Some testings were done to know the operating system's support, how much time is needed for host to get configuration and protocol testing.There are 3 conclusions that can be drawn from the experiments. The first conclusion is not all operating systems support IPv6 by default. The second conclusion is the time needed by the host to get IPv6 address is 194.76 milisecond at zero traffic and 328.13 milisecond at full traffic. The third conclusion is DHCPv6 relay agent is not necessary due to time delay. The new topology is designed and ready to be implemented.

***Keyword** : IPv6 implementation, medium access control, wireless LAN*

1. Introduction

The internet grows rapidly by increasing amount of users. With growth of the internet, the availability of public IP is decreased while the need of public IP is increased. It is predicted that someday public IPv4 can not accomodate growing number of users. According to Inetcore, a reasearch institute in Japan, IPv4 address will run out in 2011 with two percents of address space left.

Internet Protocol version 6 (IPv6) is a new protocol that designed to complement IPv4. IPv6 has address space of 128 bit while IPv4 has 32 bit. IPv6 helps the internet to grow and gives new features that IPv4 cannot gives. Migrations from IPv4 to IPv6 in wireless network need to be done smoothly and user-friendly so users have no trouble in setup the devices. DHCP presence in wireless LAN can help users to implement IPv6 in their devices.

Universitas Pelita Harapan has wireless LAN network to gives internet access to students and staff. Virtual LAN (VLAN) is used in Wireless LAN network. Vlan is segmented in each floor of the buildings, it means each floor has different Vlan. Each buildings has one or two switches. These switches are connected to core switch. This system has authentication method by using captive portal. The problem is bottleneck in Vlan trunking and authentication process.

Topology design changes are necessary to overcome the bottleneck problem. The changes in design is followed by Internet Protocol migration to IPv6. It is expected that the wireless network in Universitas Pelita Harapan can be better in term of quality of services, security, and mobility.

2. Research Method

The new network topology design offer some changes in the system and using IPv6 as protocol. Network will implement some new router with IPv6 capability. The network do not use any Network Address Translation (NAT) mechanism. The new router placed before building switch and perform layer 3 routing. Vlan is no longer necessary for the proposed system because it already has layer 3 routing mechanism. The proposed topology design is represented in figure 1.

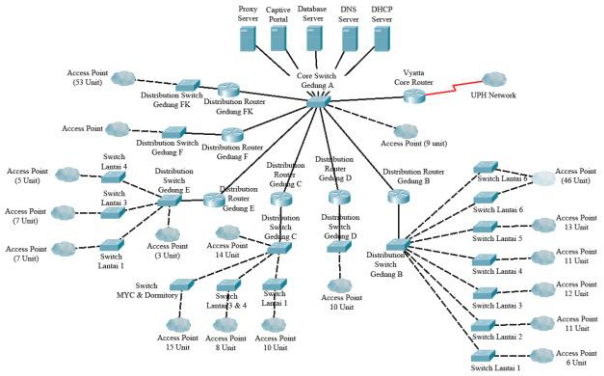

Figure 1. Proposed Topology

For experiment purpose, a smaller scope topology is created. This topology is called test-bed. Every testing and analysis is done to this test-bed. Experiment done to test-bed can be implemented in real topology because test-bed is part of the topology. The test-bed topology is represented in figure 2.

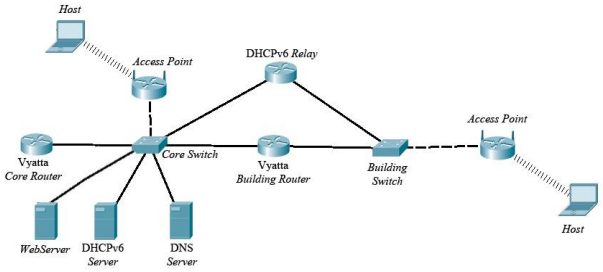

Figure 2. Test-bed Topology

IPv6 address used in test-bed network is global unicast address. This is a public IPv6 address that can be routed through the internet. The global unicast address is acquired from Freenet6 tunnel broker. The prefix given from Freenet6 tunnel broker service is 2406:a000:f003:8100::/56. It means the address has 2^8 equal to 256 subnets to make address segmentation. In experiment, connection to tunnel broker is disabled due to testing internal network.

From Figure 2, there are 2 network segments, core network and building network. This two networks has different addressing. Prefix given to core network is 2406:a000:f003:8101::/64 and prefix given to building network is 2406:a000:f003:8102::/64.

This test-bed is composed from several networking devices. The devices used in this test-bed is routers, switches, access points, servers, and hosts. Routers used in this network is Vyatta Core version 6.1. Switches used in this network is Linksys. Access points used in this network is Linksys WAP4400N. Server used in this network is Windows Server 2008 R2. Host used in this network is PC equipped with several operating system, Linux Ubuntu, Windows XP, Windows 7, and Mac OS X.

2.1 Operating Ssystem Test

Operating system test conducted to see how several operating systems fully support IPv6. Full support means operating system can exchange version 6 protocol messages like ICMPv6 and DHCPv6 to get address configuration. Operating systems tested are

Windows XP, Windows 7, Mac OS 10.6, and Linux Ubuntu.

Testings are done by analyzing every packet that come or leave the host. For example in testing host with Windows 7 operating system. Every packet come or leave the interface is being analyzed. If there are any ICMPv6 packet and DHCPv6 packet, then the host has supported IPv6.

2.2 ICMPv6 Protocol Test

ICMPv6 protocol test conducted to see how much time needed for a host to configure its own address. This configuration is called Stateless Automatic Address Configuration (SLAAC). Time is counted when host is connected to the network until it gets the address configured. Time is taken from the router advertisement packet that is caught by wireshark application. Testings are done in zero traffic condition and full traffic condition. To generate some traffic to the network, an application called IP Traffic Test & Measure is used.

2.3 DHCPv6 Leased-Time Test

DHCPv6 leased-time test conducted to see how much time needed for a host to configure its DNS address and domain search. Time is counted when a host is connected to the network and get its DNS configuration. Time is taken from DHCPv6 reply packet that contains DNS address and domain search.

Testings are done in two scenario. Scenario 1 is using DHCPv6 relay agent to relay DHCP messages in different segment of network. Devices outside the box are not used. This scenario is represented in figure 3. Scenario 2 is not using DHCPv6 relay agent so host can communicate with DHCPv6 server directly. Devices outside the box are not used. This scenario is represented in figure 4.

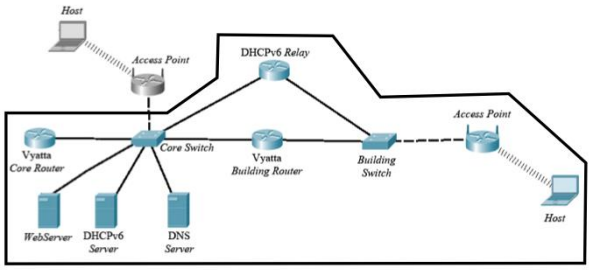

Figure 3. Scenario 1 DHCPv6 Protocol Test

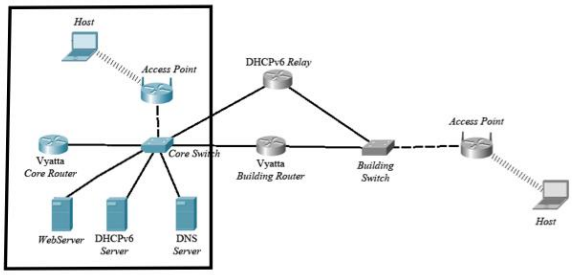

Figure 4. Scenario 2 DHCPv6 Protocol Test

2.4 DNS and HTTP Test

DNS and HTTP test conducted to test web browsing experience in IPv6. When a host access a domain name, that host will send out query to DNS server for asking the IP address. DNS server will reply by giving the proper IP address based on their database. After that a host will open HTTP page by accessing the IP address given from DNS server.

3. Results and Discussion

There are four experimental results, each derived from each test. The results are operating systems that support IPv6, how much time needed for a host to get IPv6 address configuration, how much time needed for a host to get DNS address configuration, and how can a host browse a HTTP content on the web.

Operating system evaluation is necessary to see what operating systems that support IPv6 by default. Operating systems that support IPv6 by default need no additional software so users do not have to install any additional software. Table 1 presents the IPv6 support from various operating systems.

Table 1 Operating System Support

Operating Systems	IP Address Configuration	Gateway Configuration	DNS Address Configuration	domain configuration
Windows XP	Y*	Y*	N	N
Windows 7	Y	Y	Y	Y
Mac OS 10.6.5	Y	Y	N**	N**
Linux Ubuntu Desktop 10.10	Y	Y	N**	N**

Operating system support can be seen from figure 5. “Y” sign represents that operating system can get the configuration while “N” state the opposite. “*” sign represents support but not whole. “**” sign represent that operating systems will support IPv6 with additional software.

From table 1 it can be concluded that all of operating system being tested can support ICMPv6 protocol. All of them can get IPv6 address configuration from router advertisement message. But not all operating systems can support DHCPv6 protocol. DHCPv6 protocol is needed for a host to get DNS address configuration and domain search.

When a host connected to the network for the first time, a host will exchange several message to get IP address configuration. First process is generating its link-local address based on its Medium Access Control (MAC) address. On the second process, a host search for its neighbor by sending a multicast message called neighbor solicitation. After that, it is third process, router that catch neighbor solicitation message will send out neighbor advertisement stated that there is a router exist. Finnaly router will send out router advertisement message to multicast address and every neighbor will get one. After a host get a router advertisement message, it will generating IP address based on its MAC address. The steps of this proccess is represented in figure 5.

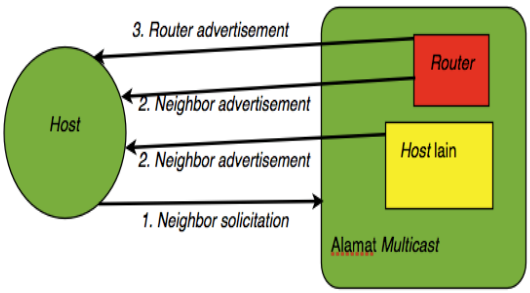

Figure 5. Address Configuration Process Scheme

Testings are done in zero traffic condition and in full traffic condition. There are 100 testings done to each of condition. Table 2. represents the first ten results of this testing.

Table 2. Testing Results of ICMPv6 Protocol Test

Zero Traffic		Full Traffic	
Test	Time (milisecond)	Test	Time (milisecond)
1	204.812	1	213.544
2	250.343	2	359.765
3	100.327	3	417.707
4	171.836	4	242.806
5	127.271	5	232.419
6	155.949	6	413.591
7	111.305	7	334.256
8	289.216	8	205.337
9	280.364	9	425.179
10	256.194	10	436.668
Average of 100 tests	192.190	Average of 100 tests	320.584

From Table 2, it can be concluded that traffic have effect on the time for host to get address configuration. In zero traffic condition, a host can get address configuration in 192.19 milisecond while in full traffic condition, a host can get address configuration in 320.584 milisecond.

In order to access internet content, a host need to have DNS server address configured. It is necessary to resolve domain name into IP address. DNS server address is not included in router advertisement message, so DHCPv6 server is needed to provide DNS server address to a host.

A host know that it has to request DNS server address to DHCPv6 server by receiving ‘O’ flag in router advertisement. ‘O’ flag means other configurations than IP address and gateway are acquired through a DHCPv6 server. If a host receive router advertisement with ‘M’ flag, it means that host has to request IP address, gateway address, and DNS address to DHCPv6 server. The ‘M’ flags means Statefull Automatic Address Configuration is used.

There are several steps to get DNS server address from DHCPv6 server. If there is no DHCPv6 relay agent, there are two steps.

- The first step is a host send out DHCPv6 information request message in order to search DHCPv6 server.
- If there are any DHCPv6 server, then DHCPv6 server will reply the message by send out DHCPv6 reply.

If there is a DHCPv6 relay to relay DHCP message, then there are four steps.

- The first step is a host send out DHCPv6 information request message in order to search DHCPv6 server.
- The second step is the DHCPv6 relay will relay the message by sending out DHCPv6 relay forward to another network segment.
- The third step is when DHCPv6 server hear the relay message and reply to relay agent. It is called DHCPv6 relay reply.

- The fourth step is DHCPv6 relay agent send back the message from DHCPv6 server to host.

This process is represented in figure 6.

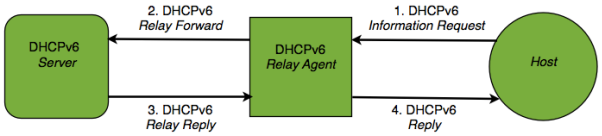

Figure 6. DHCPv6 Messages Scheme

Testings are done in two scenario. Scenario 1 is using DHCPv6 relay agent to relay DHCP messages in different segment of network. Scenario 2 is not using DHCPv6 relay agent so host can communicate with DHCPv6 server directly. Table 3 represents the results of this testing.

Table 3. Testing Results of DHCPv6 Leased-time

Scenario 1		**Scenario 2**	
Test	**Time (Second)**	**Test**	**Time (Second)**
1	15.703	1	3.143
2	15.670	2	4.363
3	15.519	3	3.997
4	15.455	4	4.050
5	15.577	5	4.360
6	16.534	6	4.367
7	15.785	7	4.175
8	15.925	8	3.970
9	15.302	9	3.491
10	18.264	10	4.317
Average of 100 Tests	15.766	Average of 100 Tests	3.683

From Table 3, it can be concluded that DHCPv6 relay agent causing a serious time delay. In scenario 1, from 100 tests conducted, a host have to wait at about 15.766 second to receive DNS server address configuration. In scenario 2, from 100 tests conducted, a host have to wait at about 3.683 second to receive DNS server address configuration.

If a host can get a DNS server address configured, then it can browse internet content. A host can resolve domain name using DNS address and access a webpage by exchanging HTTP message.

From several tests conducted, the new topology can be determined. DHCPv6 protocol testing results show that existance of DHCPv6 relay agent cause a timedelay. So by this factor, a new topology is being recommended. The new topology is represented in figure 7.

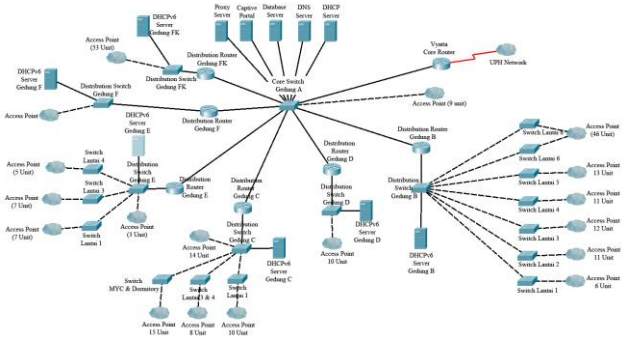

Figure 7. New Wireless LAN Network Topology based on experiments

The newly designed topology has several advantages. These are the advantages:

- VLAN system is not used anymore so bottleneck problem in VLAN trunking have been removed
- This network support IPv6 natively. Users can get IP address configuration easily. Implementation of Stateless Automatic Address Configuration (SLAAC) make user can get address configuration in miliseconds.

5. Conclusion

Not all operating system fully support IPv6. Windows XP operating system not fully support IPv6. Windows 7 operating system has fully support on IPv6. Mac OS 10.6 and Linux Ubuntu Desktop 10.10 has support for IPv6 but need some additional software to get DNS server address.

Time for host to get IP address configured based on router advertisement is 192.19 milisecond at zero traffic condition and is 320.584 milisecond at full traffic condition. The Stateless Automatic Address Configuration can run smoothly.

Time for host to get DNS server address configured directly from DHCPv6 server is 3.683 second. Time for host to get DNS server address configured based on DHCPv6 relay message is 15.766 second. This gap cause by delay that is produced from message relaying through DHCPv6 relay agent.

DNS and HTTP configuration can run on this topology. A host can resolve domain name and can access HTTP site to IPv6 webserver.

A wireless LAN network based on IPv6 composed of devices and represented in test-bed topology proved to be function properly. Therefore each device in test-bed can be implemented in real wireless LAN network of Universitas Pelita Harapan.

However an advance study about network security and mobility can improve this design. The network security covering anti DNS spoof and rock-solid authentication method. Study about mobility can enhance the user experience in using the wireless network.

References

Standards :

[1] R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Specification”, RFC 2460, Internet Engineering Task Force, December 1998.

[2] A. Conta, S. Deering, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC 2463, Internet Engineering Task Force, December 1998

[3] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney,. “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, Internet Engineering Task Force, July 2003

Textbooks :

[1] M. Blanchet,. “Migrating to IPv6”, England:John Wiley & Sons, Ltd, 2006.