Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2011, Vol. 3, No. 2

Handover Latency Measurement using Variant of Capwap Protocol

Muhammad Arif Amin

mamin@hct.ac.ae

Phone: 971-50-6120064, Fax: 971-2-4451571

Kamalrulnizam Abu Bakar, Abdul Hanan Abdullah and Rashid Hafeez Khokhar

{knizam, hanan, rkhokhar2}@utm.my

Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia

81310, Skudai, Johar, Malaysia

http://csc.fsksm.utm.my

Received: January 24, 2011 Accepted: April 6, 2011 DOI: 10.5296/ npa.v3i2.571

Abstract

The wireless LAN has become increasingly more popular over the last decade. Applications such as audio, video and voice have become important to users in a network environment. As the need for these real-time applications has increased, the handover latency during the movement of the mobile node (MN) has become crucial. A large number of wireless access points require a centralized architecture to manage, control and troubleshoot. The Control and Provision of Wireless Access Points (CAPWAP) Protocol designed by IETF allows Wireless Termination Points (WTP) to be managed centrally by an access controller (AC). This paper briefly describes the CAPWAP architecture and proposes a network setup in which the handover latency is reduced during the movement of mobile node. In particular, it shows if a Generic Routing Encapsulation (GRE) tunnel is produced between the access controllers, the Layer 3 handover latency is reduced. Results are obtained by implementing the Protocol in a test bed for Layer 2 and Layer 3 roaming for data and real-time video streaming.

Keywords: 802.11, CAPWAP, Handover, Mobility, Network Management, Wireless Networks.

1. Introduction

The demand for wireless communication continues to grow at a rapid pace. Many organizations have opted for wireless networks because of the ease of deployment and extension as compared to a wired network. Wireless communication provides freedom of access to a network at anytime and anywhere. However, it presents many challenges for the continuous communication of audio, video and voice applications. This has led to the concept of mobility in a network in which users can roam freely without realizing the network change on the node. Wireless Local Area Networks (WLAN) based on the IEEE 802.11 standard [1] has useful characteristics to provide mobility within and between networks.

Large networks require many access points (AP) and it is difficult to define a consistent strategy to manage, configure, control and troubleshoot. Due to these issues, many vendors started producing their solutions involving proprietary protocols in order to perform these functions. As a result, there is a challenge to the network world to design a system that is compatible with multiple vendors. This has led the research to develop a proprietary centralized solution, which can simplify the functionalities commonly requested by network administrators. In addition, it provides compatibility among different vendors. This also enables mobile users to move between different networks, thus allowing them to roam seamlessly as shown in Figure 1. Roaming depends on the movement between different wireless networks, and relies on the handover from one access point to another. A delay is associated with the handover process, which is the combination of the discovery phase, search or probe phase authentication, and finally the association phase. Many proposed solutions share two common elements: (i) functions that AP provides; and (ii) functions that can be centralized for management and monitoring purposes.

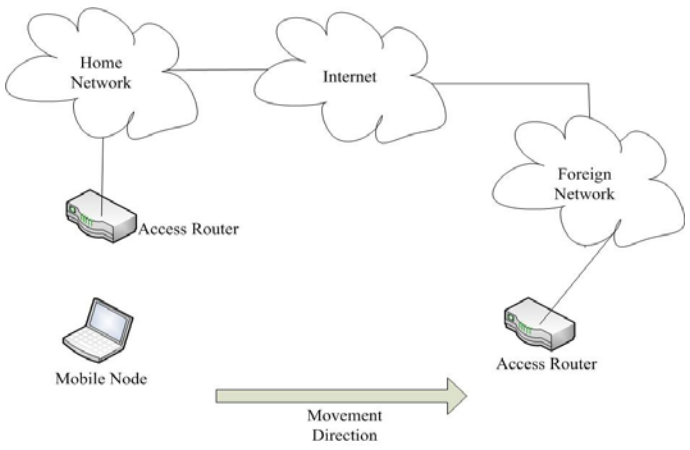

Figure 1. Mobility Process of a node moving between two different networks.

Legacy infrastructure involves access points to perform all the functions, such as channel selection, beaconing, authentication, association, re-association, encryption and management. This prevents the introduction of expensive network components to perform the interconnection. However, it places an enormous load on the management and control of the infrastructure. Centralized function involves expensive network components to perform more functions on behalf of the access point, which allow more control of the wireless infrastructure.

The CAPWAP working group within IETF began its activity with an aim to define standard solutions to the above-mentioned problems [2]. In particular, the focus of the group is to standardize a protocol to centrally manage access points and provide compatibility between multiple vendors in a large-scale environment. Thus, a standardized protocol called Control and Provision of Wireless Access Points (CAPWAP) [3] was designed to provide such functions and interoperability between different vendors, allowing mobile users to roam freely.

This paper presents a brief architecture of the CAPWAP Protocol and findings from handover delays associated with it. The Protocol is implemented in a test bed environment using physical switches, access controllers, access points and a mobile node. Two different networks are setup to measure the latency for the Layer 2 and Layer 3 handover. Several tests, including echo packets, file transfer and video streaming, are conducted in order to compare the results.

The rest of this paper is organized as follows. The next section highlights the CAPWAP Protocol and its functionalities in terms of the IEEE 802.11 standard. In Section 3, the handover process is described. Section 4 presents the performance evaluation. This is followed by the experimental results and discussion in Section 5. Finally, the paper concludes with some future directions in Section 6.

2. The CAPWAP protocol

Centralized WLAN architecture can simplify the deployment of large-scale networks by enabling network wide management, configuration, control, monitoring and troubleshooting. The CAPWAP architecture supports both legacy wireless access points, called “fat AP”, and Wireless Termination Points (WTP), also called “thin AP”. A centralized network controller terminating all the APs, called an Access Controller (AC), is used to perform management and control functionality. The CAPWAP is a recent standard defined by IETF to manage vendor free WTP radio technologies using the IEEE 802.11 standard. The CAPWAP Protocol aims to define the following as stated in [3].

- Centralized management, authentication and policy enforcement functions for the collection of WTP.
- The AC operates all the critical network functions, and the Protocol is independent of Layer 2.
- A generic encapsulation and transport mechanism are provided.

The CAPWAP defines an architecture in which AC is directly connected to several WTPs by a Layer 2 switch or Layer 3 routed network switch. It exchanges the traffic with WTP allowing a centralized management, as shown in Figure 2. The AC represents a control node, which makes it possible to manage many functionalities such as RF monitoring and configuration, WTP configuration, firmware loading, network wide user database and mutual authentication between AC and WTP. The advanced control functions require a regular exchange of control messages between AC and WTP; this is done using the UDP Protocol. CAPWAP uses separate UDP ports and are secured by Datagram Transport Layer Security (DTLS) [4]. CAPWAP architecture does not mandate only one AC to manage the WTP, but it is possible to distribute implementation across different devices or ACs in the network to improve services and redundancy. CAPWAP defines a discovery protocol to automatically detect WTP in the network. As soon as the WTP is attached on the network, it sends the Discovery Request Message to any AC on the same network that would listen to the request and respond with Discovery Response message. By exchanging this information, the WTP selects the AC, and then the AC adopts the WTP for bidirectional communication.

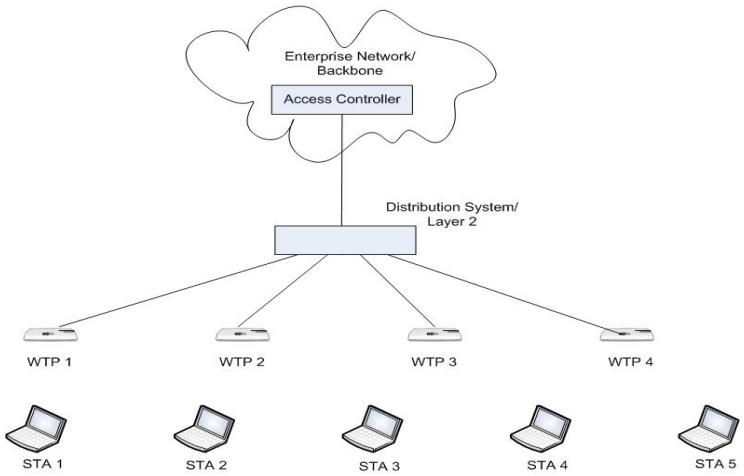

Figure 2. CAPWAP Architecture

The CAPWAP Protocol also defines two modes of operation: Split MAC (SM) and Local MAC (LM) [5]. In Split MAC, all Layer 2 wireless data and management frames are encapsulated via the CAPWAP Protocol and exchanged between AC and WTP. In Local MAC the distribution and integration functionalities reside on the WTP, or are bridged to AC

using 802.3 frames. However in both cases, the CAPWAP functionalities reside on the AC. In split MAC all user data is tunneled between the AC and the WTP, but in Local MAC not all the frames are sent to the AC. In both architectures the beacons and probe generation are implemented on the WTP. However, in the case of roaming, the WTP may send management frames to the AC, such as association and re-association, when used in Local MAC architecture.

3. Handover Process

To achieve successful mobility or roaming, an MN must perform Layer 2 (L2) and Layer 3 (L3) functions. L2 mainly depends on the MAC address exchange between MN and AP, but L3 depends on changing the IP address of the MN. However, L3 cannot be processed until the L2 process is finished successfully [6]. Since the L2 process is hardware dependent, it is mainly controlled by the manufacturer of the wireless network interface card (WNIC) and the driver. It may also depend on the signal strength or other environmental conditions. A passive scanning process at the WNIC driver level helps the MN find APs within the range and switch to a certain AP when required.

A Layer 2 handover can be achieved by connecting multiple access points to the same backbone switch, with each making a cell of its own called a Basic Service Set (BSS), which is similar to the cellular network as shown in Figure 3. Each cell is identified by a unique identifier called the BSS identifier (BSSID), which is represented by the access points. Each AP broadcasts a network name called a Service Set Identifier (SSID). When multiple APs are connected to the Layer 2 switch, if they broadcast similar SSIDs then they are called as Extended Service Set (ESS), as shown in Figure 4. Seamless roaming can be achieved using overlapping cells from different access points.

The process of a L3 switchover requires an IP change, infrastructure participation and configuration. This involves network devices exchanging signals with each other when the MN moves between old and new networks. These devices are called access routers, and are connected through a common network. Access routers are able to send information to the MN at local and remote locations using multiple routing protocols. To cater to IEEE 802.11 mobility, the following two types of mobility management protocols are designed by IETF.

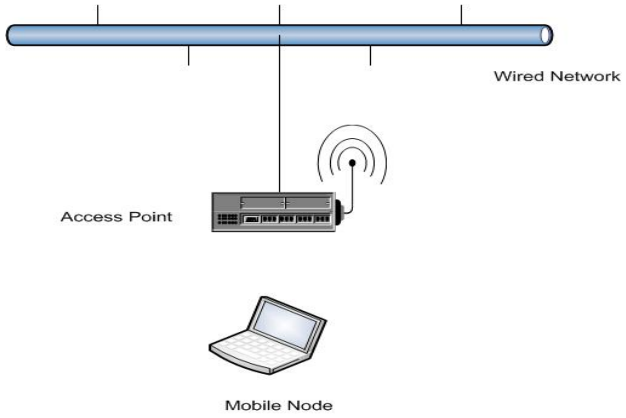

Figure 3. Basic Service Set Architecture

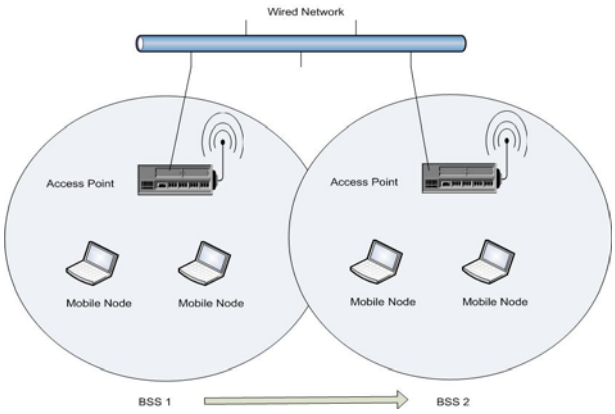

Figure 4. Extended Service Set Architecture

3.1 Host-based mobility.

Host mobility mainly depends on the signals initiated by the mobile node during roaming. These protocols include Mobile IP (MIP) [7] and Mobile IP version 6 (MIPv6) [8]. However, all of the protocols mentioned thus far operate inherently in their own environments. The protocols are designed to allow the MN to carry a home IP address, called home address (HoA), in the visiting network. When the MN is present in the foreign network it is assigned a new IP address called a Care of Address (CoA). A mapping between HoA and CoA is stored in the access router and the MN. When a node in the home network tries to communicate to the MN at the visiting network, packets are intercepted by the access router and routed to the foreign network based on the mapping. However, all the nodes at the foreign network communicate with the MN with its CoA. These protocols, however, were designed to provide mobility between two different networks or ISPs, but they do not provide efficient mobility solutions within the enterprise due to the large handover latency. Similarly many other extensions to the MIPv6 were designed to provide efficient handover within the enterprise, but still produce large latency that is not suitable for real-time applications.

3.2 Network-based mobility.

The IETF working group Network-Based Localized Mobility Management (NETLMM) is working toward providing mobility using network devices. Most of the handover signals are initiated by the network devices instead of mobile node. This group has standardized a protocol called the Proxy Mobile IPv6 (PMIPv6) [9]. PMIPv6 is designed to provide mobility within the same domain or enterprise; if a node moves out of the domain it must rely on MIPv6. Theoretically and mathematically, PMIPv6 produces less latency compared to MIPv6 and its extensions. However, practical implementations have not been tested and vendors have not yet started implementing the protocol in the devices yet. Both of the above mentioned mobility management protocols might provide better handover in the near future. However, none of them provide central management and control of the access points.

CAPWAP Protocol is best suited for the campus or enterprise network in which access points are centrally managed. It also produces better results for handover within the network and between two different networks. This paper only covers handover latency measurement using a pre-standard variant of the CAPWAP Protocol in an enterprise network. Experimental research results have shown that the total handover time can exceed two seconds, and different phases during handover can add to handover latency time [10]. An example would be context transfer during handover (reactive), which could increase the handover latency. However, proactive context transfer reduces the latency [11] because the process starts before handover. The Inter Access Point Protocol (IAPP) defined by the IEEE provides Layer 2 handover to transfer context and management signaling [12]. However, it can only perform these functions for the legacy access points and also generate large handover latency because of no infrastructure support. The CAPWAP Protocol allows access controllers to maintain mobile node stations status by controlling and managing the wireless termination points (WTP). Multiple ACs can be used to control multiple WTPs; each AC is configured with a wireless LAN (WLAN) similar to the other and defined as a peer so that they can share forwarding tables of the L2 and L3 switch. This allows each AC to track the mobile node and perform seamless roaming within and between different networks. However [13,14] has discussed Layer 2 handover in CAPWAP using network deployment and presented mathematical model, which shows handover latency of 85µsec. In [15, 16] an open source implementation of CAPWAP protocol is presented, the author tested reliability of the protocol using experimentations and presented association and configuration delays between WTP and AC, however the author did not measure total handover delay experienced by the node.

4. Performance Evaluation

This section presents the test bed setup and results obtained after experimentation. The test bed is setup in a lab containing the network devices and the mobile node. The lab is setup by

reducing the signal strength of the WTP so that no interference could be observed by any other access point in the area. A laptop with an external wireless network card is used to perform the experiment. A network sniffer captured the packet when the mobile node connected and disconnected from the network. Handover delays are measured by connecting and disconnecting the node to two different networks.

4.1 Experimental Setup.

The experimental test bed included two Layer 3 switches, 2 AC, 2 Layer 2 switches, 2 WTP, two Dynamic Host Configuration Protocol (DHCP) server, one media server and one wireless station. The switches, access controllers and WTP used are from HP Procurve networking; the DHCP server and the media server are HP desktop computer running windows 2003 operating system, the wireless station from HP small desktop computer with Linksys 802.11 b/g wireless network card and Windows XP professional with SP2 operating system. With this test bed, three sets of experiments were performed, each conducted five times to measure the latency:

- Ping packets from the station to the media server
- FTP from media server to the station
- Real-time video streaming from the media server to the station

Each of the above mentioned tests were run in two different topologies including Intra-Domain and Inter-Domain to measure handover latency. A virtual local area network (VLAN) configuration was used on the switches to simulate two different domains. An open source packet sniffing tool, Wireshark [17], was used in promiscuous mode to capture the packet at the station.

4.2 Layer 2 (L2) roaming.

Figure 5 shows the setup of the Layer 2 roaming in which the STA moved between the two WTPs with the same SSID and under a single domain (Intra-Domain). Here, the same VLANs, IP addressing and SSID were configured in both networks. The same SSID was mapped to the same VLAN on both ACs; therefore, no IP change was required during roaming. This was exactly the same setup as the legacy access points in a network. In this setup, the 802.11i standard was used, which includes a provision known as pre-authentication. This was developed for the benefit of independent access points. A station learns about the existence of another available AP, which supports the current WLAN by listening to beacons. When the station determines that it needs to roam toward another AP, it sends Extensible Authentication Protocol (EAP) [18] messages to the second AP, while still associated with the first. The information is transferred from the station through the first AP to the basic SSID (BSSID) that

represents the current WLAN on the second AP. The receiving AP stores this pre-authentication information using Pair-wise Master Key (PMK) Caching, enabling the station and the AP to establish all required encryption keys before the station initiates the roam. The pre-authentication implementation on the AC causes it to listen to BSSIDs of its adopted WTPs. The station can complete its authentication with the second AC before it initiates the roam to a WTP adopted by the second AC as if it were roaming between two independent APs. Table 1 shows the test bed configuration.

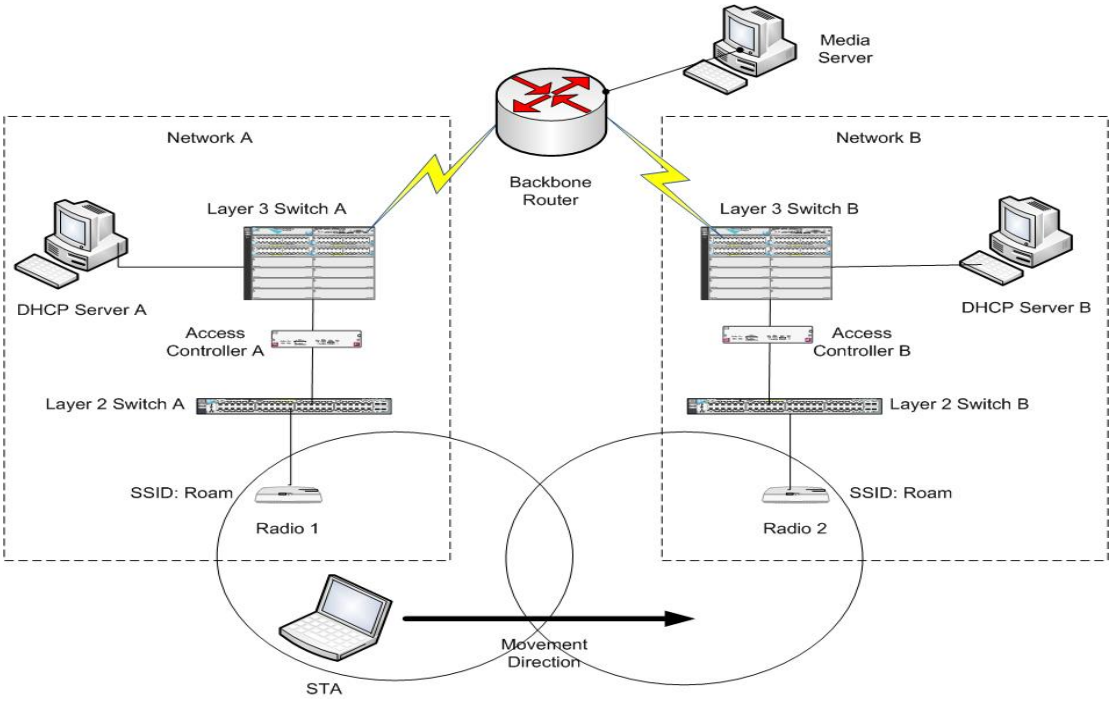

Figure 5. Layer 2 Test bed Topology

Table 1. Layer 2 roaming test bed setup configuration

Device	Network A	Network B
L3 Switch	10.1.1.1	10.1.1.2
Access Controller	10.1.1.10	10.1.1.20
L2 Switch	10.1.1.30	10.1.1.40
WTP	10.1.1.15	10.1.1.16
STA	10.1.1.8	10.1.1.8
DHCP	10.1.1.50	10.1.1.50
Backbone Router	10.0.100.10	10.0.100.10
VLAN Name	WirelessA	WirelessB
VLAN ID	1	1
SSID	Roam	Roam

4.3 Layer 3(L3) roaming

Fig 6 shows the setup of Layer 3 roaming. Here, the STA is moved between two different networks (Inter-Domain). However, the STA require a new IP address and re-authentication when moved from network A to network B. The pre-authentication method does not work because of L3 separations and routing requirements. Each AC controller is configured with a mapping of SSID to a VLAN, because there are two different networks with different VLAN IDs, on the access controller. Once the mapping is done, ACs are configured to be the peers of each other. A Generic Routing Encapsulation Tunnel (GRE) [19] is created between the ACs to share information between each other. This allows peers to share the WTP and STA information, which allow forwarding of the switching table. An overlap of 20% was created between the cell sizes of both WTPs to provide roaming. However, the STA was not moved physically between the cells in order not to include motion parameters during the handover, but placed between two WTPs inside the overlap area. The STA is associated with VLAN when its home AC receives an IP address from the DHCP server and communicates with the network. When the STA moves toward another WTP, the AC detects the home VLAN and starts to tunnel traffic to the home AC that allows seamless handover in a new network. Table 2 shows the configuration of the test bed.

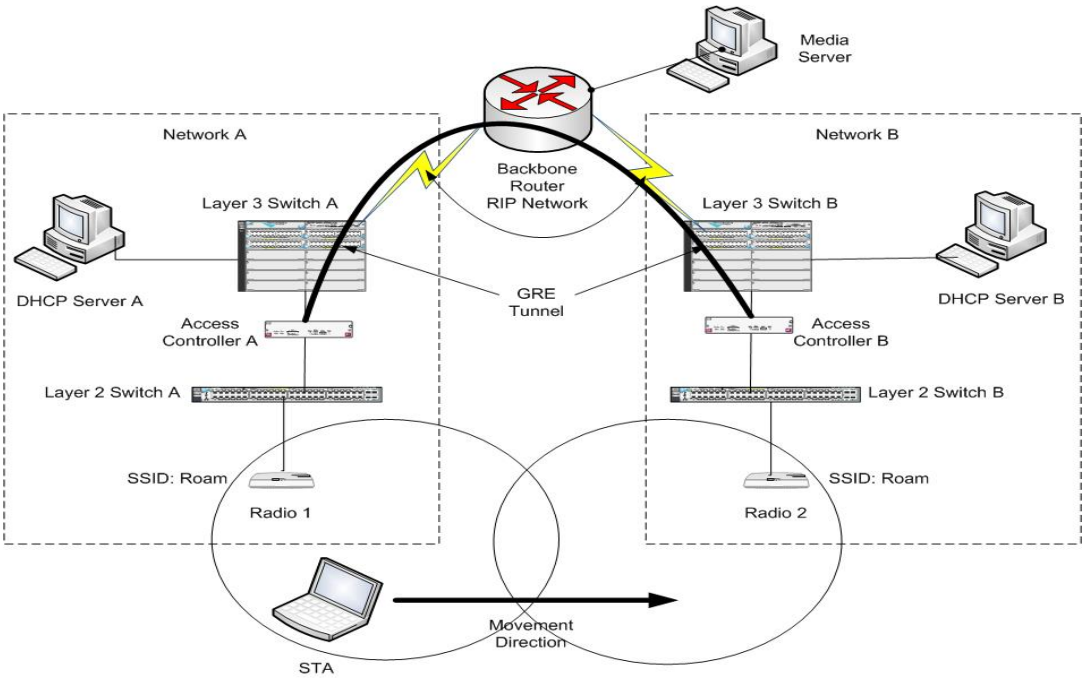

Figure 6. Layer 3 Test bed Topology

Table 2. Layer 3 roaming test bed setup configuration

Device	Network A	Network B
L3 Switch	10.1.1.1	10.2.1.1
Access Controller	10.1.1.10	10.2.1.20
L2 Switch	10.1.1.30	10.2.1.40
WTP	10.1.1.15	10.2.1.16
STA	10.1.1.8	10.1.1.8
DHCP	10.1.1.50	10.2.1.50
Backbone Router (RIP)	10.0.100.10	10.0.100.10
VLAN Name	WirelessA	WirelessB
VLAN ID	1	2
SSID	Roam	Roam

5. Experimental Results

In this section, we present experimental results about the performance of the pre-standard CAPWAP Protocol. The results shown are ping, ftp and video streaming handover latency recorded at the STA. In order to get the approximate reading we attached the STA with one WTP, started the packet sniffer, and then disconnected from the first WTP so that the STA could attach to the second WTP. Once the STA attached and started communicating with the second network, the sniffer was stopped and packets were analyzed and measured. The measurement includes the time period between the disconnection of STA and the re-connection. A continuous ping to the media server was generated from the station with a standard 32 byte of data. FTP was used to copy 3 GB of data from the media server to the STA. The VLC player [20] was used to do unicast video streaming from the media server to the STA. The media server was connected to the backbone network of the enterprise, which was different than network A and B. All these tests were run at least five times to measure L2 and L3 handover latencies and station cache.

The NetBIOS and IP address were refreshed before each test in order not to overlap the results. Figure 7 shows the results of Layer 2 handover latencies. The minimum handover latency time for Ping requests was 297 msec, maximum 922 msec, and average 651 msec. At least two echo replies were timed out for each test. For FTP, the minimum latency was 3770 msec, maximum 4375 msec, and average 4077 msec. After reconnection, multiple retransmission requests were sent to the server for the continuation of the data copy. In real-time video streaming, 309 msec was lowest, 840 msec highest, and 516 msec average. Observing Layer 2 results, the FTP latency was the largest compared to Ping and video streaming. It was almost 33% more than ping and 38% more than video streaming. Theoretically, the Ping should take less latency than video streaming, but due to the unicast

streaming the latency was lower. It might have produced different results if the multicast streaming had been used instead of unicast streaming.

Layer 3 handover latency results are presented in Figure 8. The results show that the minimum handover latency for the Ping request is 283 msec, maximum 731 msec, and average 584 msec. FTP results show that the minimum latency was 1727 msec, maximum 3179 msec, and average 2353 msec. In real-time video streaming, the minimum is 288 msec, maximum 498 msec, and average 386 msec. Layer 3 handover latencies are lower than the Layer 2 because of the tunnel created, which allows the other Access Controller to cache all the MAC addresses even if the STA is not linked to it.

Layer 3 results shows less latency compared to Layer 2 results. However, similar to the Layer 2 results, FTP was the largest with 23% and was higher: 17% more than Ping and 22% more than video streaming. Comparing both Layer 2 and Layer 3 results, in Layer 3 Ping was 0.8% less, FTP was 17% less and video streaming was 1.25% less than Layer 2.

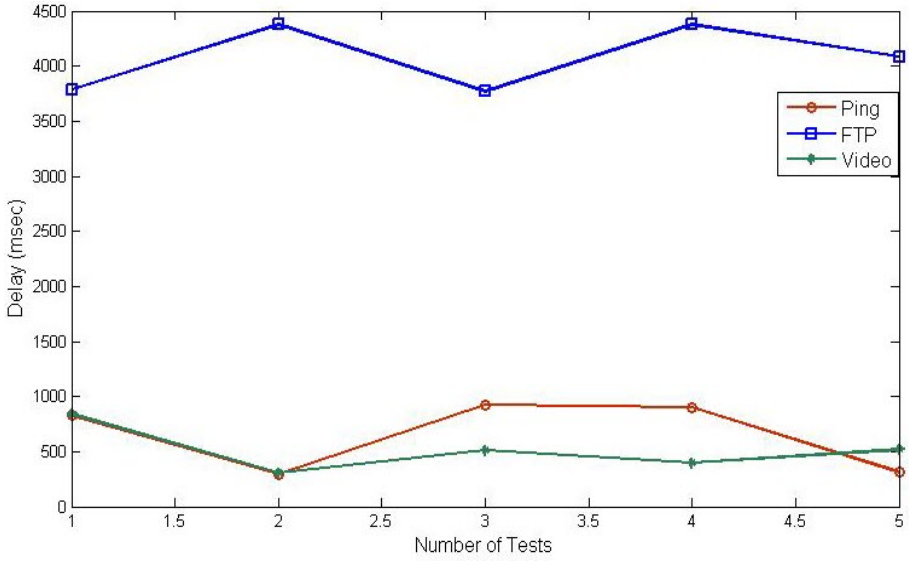

Figure 7. Layer 2 Handover Latency Results

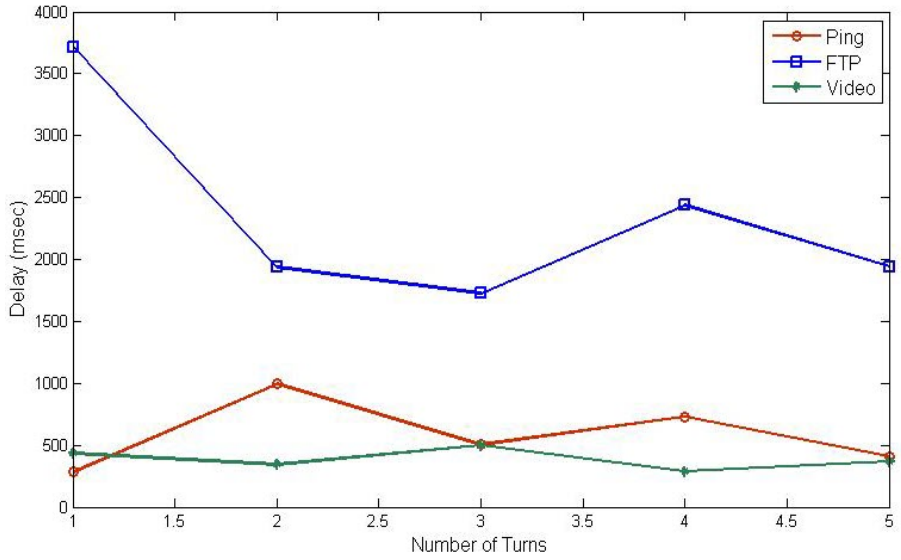

Figure 8. Layer 3 Handover Latency Results

6. Discussion

The CAPWAP Protocol was designed by the IETF to provide seamless mobility within the enterprise network as well as for Hot-Spot installations. Most of the protocols available are targeted to solve the problem of real-time applications; yet, their basic design is based on fixed nodes, not mobile nodes. They produce large handover latency during movement. Much research is underway to reduce the latency during movement. Due to the fast growth and demand in real-time applications using mobile nodes, the vendors proposed different strategies to solve this issue. CAPWAP provides an ideal solution for management; however, it also provides seamless mobility architecture to support audio, video and data. In this paper we presented the architecture for implementing CAPWAP within the enterprise network and used the topology to provide seamless handover during mobility. We focused mainly on the problem of handover latency that leads to disconnection from the network during movement.

In particular, we concentrated on reachability using Ping, file transfer using FTP and real-time video streaming using VLC software. We presented an architecture in which the SSID for both networks was the same, but mapped to different VLANs. Both the access controllers were defined peers of each so that they could share the forwarding tables by creating a GRE tunnel. Due to this configuration, when the STA moved between two different networks a fast handover took place. The experiment results show great differences between the handover latency generated during the movement. Theoretically, Layer 2 roaming must produce better results than Layer 3; however the difference in the figures is due to the exchange of the MAC addresses and building the forwarding table in the switch. When Layer 2 roaming was performed, the visiting switch did not know about the MAC address of

the STA; also, it was not possible to predict when the STA would perform handover initiation. In Layer 3, since the GRE tunnel is established between the ACs, both switches stored the forwarding tables of each other. When the STA moved to a new network, the AC immediately started to tunnel the packets to the home AC of the STA without any delay.

7. Conclusion

The problem of handover latency during movement in the wireless network has become very important. The current IEEE 802.11 products designed for the campus, office, hot-spot and enterprise networks do provide support for a large number of access point deployments and seamless mobility. A new protocol is required that allows easy management, configuration, control and troubleshooting. In this study, we implemented a pre-standard variant of the newly standardized CAPWAP Protocol. In particular, we ran the Protocol in a test bed and measured the handover latency by conducting several tests. Moreover, the set of results were presented to support the real world implementation scenario. Future work aims to measure the handover latency by proposing the standardized protocols and compare them against well-known protocols such as MIP and MIPv6 and extensions.

References

[1] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirement. Part 11: wireless LAN medium access control (MAC) and Physical layer (PHY) specifications. Amendment 2: higher-speed physical lyaer (PHY) extension in the 2.4 GHz band - corrigendum 1," *IEEE Std 802.11b-1999/Cor 1-2001*, 2001.

[2] B. O' Hara, P. Calhoun, and J. Kempf, "Configuraiton and Provisioning of Wireless Access Points Problem Statement," in RFC 3990, February 2005.

[3] P. Calhoun, M. Montemurro, and D. Stanley, " Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", in RFC 5415. March 2009.

[4] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1," in RFC 4346, April 2006.

[5] P. Calhoun, M. Montemurro, and D. Stanely, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11," in *RFC 5416*, March, 2009.

[6] R. Koodli and C. Perkins, "Mobile Internetworking with IPv6 Concepts, Principals, and Practices". Wiley-Interscience, 2007.

[7] C. Perkins, "IP Mobility Support for IPv4", in RFC 3344, Aug. 2002.

[8] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," in RFC 3775, October, 2009.

[9] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213,

Aug. 2008.

[10] H. Velayos and G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time", IEEE International Conference on Communications (ICC 2004). Paris, France. 20-24 June 2004. Pp. 3844-3848. DOI: 10.1109/ICC.2004.1313272

[11] A. Mishra, M. Shin, and W. A. Arbaush, "Context caching using neighbor graphs for fast handoffs in a wireless network". The 23rd Conference of the IEEE Communications Society (IEEE INFOCOM 2004) , Hong Kong, March 2004. DOI: 10.1109/INFCOM.2004.1354508

[12] "IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting ieee 802.11 operation," IEEE Std 802.11F-2003, 2003.

[13] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *SIGCOMM Comput. Commun. Rev.* Vol. 33, pp. 93-102, 2003. DOI: 10.1145/956981.956990

[14] T. Clancy, "Secure handover in enterprise WLANs: capwap, hokey, and IEEE 802.11R" *IEEE* Wireless Communications. Vol. 15, pp. 80-85, Oct. 2008. DOI: 10.1109/MWC.2008.4653136

[15] M. Bernaschi, F. Cacace, G. Iannello, M. Vellucci and L. Vollero, “OpenCAPWAP: An open source CAPWAP implementation for the management and configuration of WiFi hot-spots”. Computer Networks. Computer Networks, Vol. 53. Pp. 217–230. 2009. DOI: 10.1016/j.comnet.2008.09.016

[16] M. Bernaschi, F. Cacace, G. Iannello, M. Vellucci and L. Vollero, “OpenCAPWAP: an open-source CAPWAP implementation for management and QoS support”. 4th International Telecommunication NEtworking WorkShop on QoS in Multiservice IP Networks (QoSIP-IT-NEWS), Venice, Italy, February 2008. DOI: 10.1109/ITNEWS.2008.4488132

[17] Wireshark. [Online]. HYPERLINK "http://www.wireshark.org/" http://www.wireshark.org/

[18] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," in *RFC 3748*, 2004.

[19] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic Routing Encapsulation (GRE)," in *RFC 2784*, March, 2000.

[20] VLC Media Player. [Online]. HYPERLINK "http://www.videolan.org/vlc/" http://www.videolan.org/vlc/

Copyright Disclaimer