



## Seamless Wireless Design With Single Service Set Identifier and Single Sign On Using Kerio Control

Sardjoeni Moedjiono<sup>1</sup>, Nada Maulana<sup>2</sup>, Aries Kusdaryono<sup>3</sup>  
Postgraduate Program, Budi Luhur University, Jakarta, Indonesia

**Abstract:** In the development of technologies that exist today and particular in the areas of networking, wireless technology began to be taken into account to develop the infrastructure in the industry, academia and the public. In an enterprise, Wi-Fi transmitter or access point can be installed more than 10-15 AP in it. The number of access points is proportional to the number of service set identification (SSID). The technological advances of the routers and access points can be combined to build a wireless controller to resolve the problem. Wireless controller also serves to ease the process of access points, took over the facility Dynamic Host Configuration Protocol (DHCP) and Security Password. By establishing a seamless wireless system with a single SSID, it can produce a quality network that include user activity when roaming and allows network administrators to perform monitoring and maintenance.

**Keywords:** Deadlock, Dynamic Host Configuration Protocol, Security Password, Service Set Identification, Wireless Controller

### 1. INTRODUCTION

In the development of technologies that exist today and in particular the areas of networking, wireless technology began to be taken into account to develop the infrastructure in the industry, academia and the public. Wireless networking is considered to be more efficient in doing the installation because it requires a lot of wires to form a local area network (LAN) in a particular place. An interesting finding was delivered in a survey is 85% of the number of Internet users in Indonesia use mobile devices while surfing in cyberspace. The second device is most often used are laptops, followed by PC / computer and the last tablet. While the majority of Internet users in Indonesia are workers and self-employed. From the employment sector, the majority used the Internet in Indonesia on trade and services sector [1]. By building a wireless network system is centralized, an admin can also perform monitoring and maintenance easier. It can also extend the range of the wireless signal with the seamless method, making it easier for the user to roaming without worrying disconnection when performing activities such as browsing or downloading.

### 2. RELATED WORK

In this section presented theories and literature used at the time of the study. These theories are taken from books and journal literature from the internet. Theories covered include the theory of the study of WLAN, Seamless Wireless, SSO, LDAP, Kerio Control, Firmware DD-WRT dan DHCP Forwarder.

#### 2.1 WLAN Standards

WLAN standard IEEE 802.11 refers to the first published in 1997. The IEEE (Institute of Electrical and Electronics Engineers) is an independent institution that focuses on the development and improvement of technological innovation for the good of man [2]. The development of the standard IEEE 802.11 WLAN where the development started in the standard-setting 802.11 in 1997 working at a frequency of 2.4 GHz and a maximum data rate of up to 2 Mbps, then in 1999 re-published standard IEEE 802.11b and 802.11a. Standard 802.11b working in 2.4 GHz band with a data rate of up to 11 Mbps, but have drawbacks likes the effect of interference due to the use of equipment with the same frequency. The 802.11a standard uses the 5 GHz frequency has a data rate of up to 54 Mbps, but has a weakness in the coverage area where its reach is lower than the 802.11b standard. In 2002, publishes IEEE 802.11g standard combines the advantages of 802.11a with 802.11b. The 802.11g standard works at a frequency of 2.4 GHz and has a data rate of up to 54 Mbps with coverage area closer to the range of 802.11b. The use of the same frequency between 802.11g with 802.11b makes the two standards are compatible, if implemented in wireless communication devices. The next development was marked by the publication WLAN 802.11n standard that combines 802.11b 802.11g technology. The technology used is known as MIMO (Multiple Input Multiple Output) which offers increased throughput, superior reliability, and increased client connected. IEEE 802.11a standard is a wireless WLAN protocol published in 1999. This standard work on the 5 GHz frequency band with a pattern of OFDM (Orthogonal Frequency Division Multiplexing) using 52 sub-carriers are modulated using techniques BPSK



(Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), 16-QAM (16-Quadrature Amplitude Modulation) or 64-QAM (64-Quadrature Amplitude Modulation). Data rate on IEEE 802.11a is 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps and up to 54 Mbps.

## 2.2 WLAN Physical Architecture

WLAN physical architecture consists of two categories: architecture IBSS (Independent Based Service Set) and Infrastructure Architecture.

### 1. IBSS Architecture

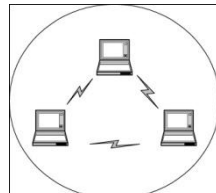


Figure1: IBSSArchitecture [3]

Figure 1 shows the architecture configuration IBSS or ad-hoc WLAN configuration which is a peer-to-peer, where two or more devices can be connected via a wireless network without requiring an access point. In this architecture, the device will configure itself on the same radio channel for communication to enable peer-to-peer [3].

### 2. Infrastructure Architecture

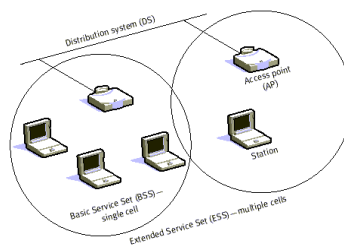


Figure2: Infrastructure Architecture [3]

In the architecture of the infrastructure there is an access point that works to serve the communication on the wireless network, where the access point is connected to a backbone DS (distribution system). BSS is an architectural configuration with an access point with a client that communicates in the coverage. A BSS has an ID (identifier) that is unique and different from other BSS. The device you want to connect to a WLAN are required to have the same ID value in accordance with the BSS id. Configuring two or more BSS connected to a backbone are the same then will form a subnet is seen as an ESS.

### 2.3 Failover/Load Balance

Load Balance in computer networks is a technique for dividing the load into multiple paths or links. This is done if for heading a network there are multiple paths (links). The purpose of load balancing is that there is no link to get a larger load than the other link. It is expected to share the burden in some of these links, it will be to achieve a balance the use of these links. There are various load balancing implementations are often encountered in the field, which most often is the application load balancing on a local network that has two or more internet connections. While Failover own technique is a technique that allows a link will replace another link tasks in case of failure or dropping connections. Failover and Load Balance are two different techniques, load balancing is a technique to divide the load while the failover refers to a technique for making a backup link. But the application of load balancing, in general, will be accompanied by a failover [4].

### 2.4 Seamless Wireless

Seamless roaming can be interpreted as the process move between wireless networks for communication takes place when not distracted or without re-authentication. The process includes seamless roaming services in the most seamless work by using Internet Protocol (IP) that is designed to provide mobility at the network level connection. In other words, the network itself continues to hold the user's IP address and get away from the connection to the other connection types, exchanged so smooth that there is no noticeable effect



on the user side [5]. If there are some areas in a room covered by more than one access point, then the cell coverage have to overlap. Each wireless station will automatically determine the best connection will arrest of an Access point. Area coverage overlapping an important attribute of the WLAN setting because it enables seamless roaming between overlapping cells.

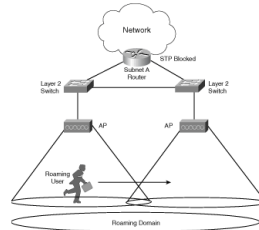


Figure 3: Seamless Roaming [6]

Seamless wireless solutions proposed seek to improve the three main points, namely: scanning Optimizations, adding topology discovery and handover predicting. SyncScan algorithm [7] proposed to be based on the data synchronization beacon access points that work in different channels. Thanks to the mobile station (MS) realizes approximate arrival beacons on certain channels. MS can switch to the correct channel before the manual that came and accelerate how to search. The algorithm requires knowledge of the configuration of another access point, such as the current operating channel and transmit beacon interval. Additionally, access points should have access to perform synchronous timing source. Smooth Handoff Algorithm [8] to modify the legacy of active scanning procedure. MS scan a number of channels and come back to the transmission line. This procedure is repeated until all channels are scanned. The scanning time is extended but most can resume transmitting MS during the process. The author states that scanning should begin at some time before the MS is disconnected from the access point but does not present a practical methodology to start Smooth Handoff. Single channel scanning can take more than 50 milliseconds, so that even a single channel scan and return to the transmission line may not meet the requirements of multimedia services. Another group of algorithms proposed in the literature about the use of information access points in the vicinity, called neighbors. Neighbor Graph [9] is a directed graph with each end represents the path between the node mobility, namely the AP. For any given AP, neighbors represent a set of potential access points. Neighbors can be obtained from the current access point or collected as a station across the network. NG and NGPruning algorithms [9] is the first published algorithm that uses neighbor graph to improve the efficiency of handover. Neighbor graph constructed by each access point based on the 802.11 reassociation request frame received from the MS which contains an old BSSID of the access point. NGPruning algorithms scanning procedure is only for those channels that are known to be used from the Neighbor graph. NGPruning algorithms eliminate overlapping access points from the scan list. Two access points overlap when the location when MS can communicate with them both with the quality of the received link. NGPruning algorithms cut all access points that are non-overlapping with affordable access point. Assuming that AP1 and AP2 are non-overlapping, if MS receives probe responses from AP1 there is no reason to wait for the response investigation of AP2. Because the scan time may be reduced by skipping AP2 scanning. RSS-based Indoor Tracking System (RITS) [10] is another example of an algorithm that facilitates the delivery by using neighbor graph. MS gather information RSSID of beacon frames sent by access points that operate on the same channel. In order to gather knowledge on access points that operate on a different channel MS also actively scan the selected channel. The authors state that a non-overlapping channel is selected for scanning, but it is not clear how the selection was made. Build a mobile station that stores RadioMAP RSSID and BSSID of the access point is scanned at a given moment. When the station intends to perform handover, it is listening for beacons on the current channel. If the station is able to determine the location based RSSID of the beacon, the station RadioMAP search for neighboring access points and performing handover. If not, the station must perform additional scanning. Algorithm introduces additional requirements on the network topology. The access point should operate on overlapping channels that allow the detection of the location but deteriorated transmission conditions.

## 2.5 Single Sign On (SSO)

SSO is a technology that has the ability to enter the same id and password to log into multiple applications within a company. Such as password authentication is the most secure mechanism, known as the SSO has now been reduced sign-on (RSO) since more than one type of authentication mechanisms used in accordance with the firm's risk models. For very large networks and heterogeneous, where the user is prompted to enter information themselves on any application which you want to access needed SSO. SSO system does not



require user interaction, to access all the services applications without having to log in and type in the password repeatedly. SSO authentication of users clicking on all applications that have diauthorized to be accessed. This eliminates the authentication request again when users switch applications during a session applies [11]. SSO also allows the authentication information and identifying a subject in order to avoid double login on the system or group of systems reliable. SSO system can also centralize service of the relevant system parameters at the same time and improve the overall usage. Service users may prefer the SSO system from the regular sign-on system. SSO system architecture has two main parts: the agent residing on the web server/application services and a dedicated SSO server that will be described as follows:

1. Agent: each HTTP request that goes to a web server will be translated by the agent. In every web server there is one agent as a host of application services. This agent will interact on the SSO server on the other side of the application and interact with the web browser of the user side.
2. SSO server: In providing temporary cookies session management function (temporary) use the SSO server. User-id, session creation time, session expiration time, and so forth is no information on cookies.

## 2.6 Lightweight Directory Access Protocol (LDAP)

LDAP is a protocol that defines how data can be accessed over a network directory. LDAP is used to store a variety of centralized information that can be accessed by multiple machines or applications from the network. The use of LDAP within the system will make information search become an integrated and very easy. For example, LDAP is often used to store usernames and passwords contained in the system centrally [12]. Basically for information storage on a storage LDAP with relational databases such as MySQL applications is the same. LDAP also make the process change and demand on data or information as is done by the RDBMS applications. But LDAP is not a relational database application, because LDAP is only optimized for finding information fast and not to process the data changes on a large scale and significantly faster. According to Imam Cartealy, there are three definitions are very important in that LDAP schema, object classes and attributes. Whereby the three inter-related definitions and become the backbone of LDAP, that is:

1. Scheme: Schemes can be likened to a packaging system for object classes and attributes. Each object classes and attributes must be defined within the scheme, and the scheme must be declared in the configuration file `deamonslapd, slapd.conf`.
2. Object Class: Object class is a container that serves to categorize attributes. Object class will determine whether an attribute must exist, or is optional.
3. Attribute: Attributes are the smallest structures of the scheme which is the object of the class members. An attribute has a name and also have a discount nilaidan every attribute can be more than one value.

## 2.7 Kerio Control

Previously called KerioWinRoute Firewall is a software developed by the gates of the Kerio firewall technology formerly known as the small software. Equipped with a vpn server, Sophos anti-virus (optional), web filtering, bandwidth limiter, internet and monitor user-specific Internet access management, Kerio Control can be installed on windows and linux. Kerio Control is very helpful to the defense network of small and medium organizations [13].

## 2.8 DD-WRT

Firmware can also be referred to as the operating system, because the firmware is a bridge for the hardware can run a software. However, this firmware is different from the operating system embedded in a computer such as Windows, Linux requires a large storage medium. So the firmware can be regarded as a software or any software that is embedded in the flash memory (Flash ROM) as an example in the motherboard is the BIOS (Basic Input Output System). DD-WRT is a popular alternative firmware for the Access point hardware. This firmware include some useful features, including client radio mode, transmit power settings, various captive portal, VPN, WDS, QoS support, and more. Firmware is using web-based configuration that is not encrypted or via HTTPS, and also provides SSH and Telnet access. [14]

# 3. METHODOLOGY AND RESEARCH DESIGN

## 3.1 Metodology

In designing a computer network, used methods Network Development Life Cycle (NDLC). Where this method is a method that relies on a previous development process such as strategic business planning, life cycle application development and analysis of data distribution. If the implementation of network technologies implemented effectively, it will provide information system that will meet strategic business objectives, then the top-down approach can be taken [15]. Here are the stages of NDLC:

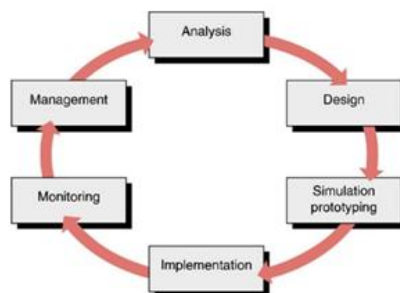


Figure 4: Network Development Life Cycle (NDLC) [15]

### 3.2 Research Design

Model design of this study aims to provide a comparative analysis between the current existing topology and topology with the proposed method. The comparative analysis covering the duration of the time reauthentication seamless process, when the process SSO with LDAP protocol, signal interference among the access point, the process of internet connections with load balancing and failover.

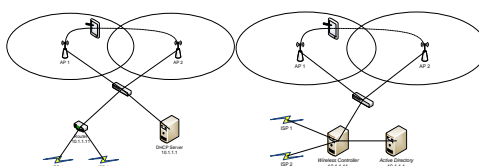


Figure 5: Topology a) Existing Topology, b) Topology with Wireless Controller

## 4. IMPLEMENTATION AND EVALUATION

### 4.1 Test Location



Figure 6: Map Location Test System

Table 1: Description of Location system testing

| Description                   | Information |
|-------------------------------|-------------|
| Spacious Room                 | 30x30 meter |
| Barrier                       | Glass 8 mm  |
| Distance between access point | 16.2 meter  |

### 4.2 Device Testing

Table 2: Device Testing

| Spec | Picture | Type            | Standards   | Frequency | Max Link Rate |
|------|---------|-----------------|---|-----------|---------------|
| AP 1 |         | Linksys WRT54GL | IEEE 802.3<br>IEEE 802.3u<br>IEEE 802.11g<br>IEEE 802.11b | 2.4 Ghz   | 54 Mbps       |
| AP 2 |         | Linksys WRT54GL | IEEE 802.3<br>IEEE 802.3u<br>IEEE 802.11g<br>IEEE 802.11b | 2.4 Ghz   | 54 Mbps       |

### 4.3 Unit Testing

Tests proved unit of Monitoring Kerio Control, software Speedtest, Wireshark, Acrylic Wi-Fi Professional and Who's On My Wifi.

1. Authentication user process





The process of the user authentication process by the Kerio control system that uses the username and password of the active directory domain.



Figure 7: Authentication user process

2. Connection process to active directory

In the proposed system needs in order to run the SSO, username and password is done by using the user account name of the Active Directory Domain (ADD). Periodically Kerio Control and ADD will synchronize using the LDAP protocol as in Figure 8.

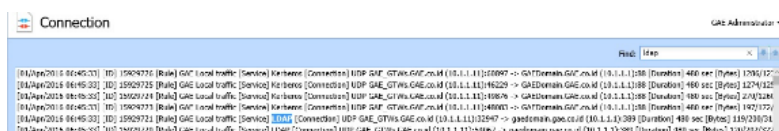


Figure 8: Kerio Control Sync Process and ADD with LDAP protocol

3. Failover/Load Balance process

Testing is done with the illustrations as if one of the Internet network attached have dropped connection or downtime. As for testing the function of load balancing, bandwidth testing performed using Speedtest.



Figure 9: Bandwidth Testing a) Without Load Balance, b) With Load Balance

4. Seamless wireless process

Testing is done with mobile devices to connect to the SSID radiated beginning GAE and then simulation roaming away from the nearest AP to another AP. Observed the process of authentication and reassociation process in Figure 10.



Figure 10: Reauthentication and Reassociation process to SSID

4.4 System Testing Results

From the test results failover/load balancing results to be the underdog of the proposed method is the process by which the time of testing the connection by testing internet connection speed. It can be deduced by calculating the average of testing each variation testing is as follows:

Table 3: Session of Results Testing Failover/Load Balance

| Scheme | Testing Variation | Testing 1 (Mbps) | Testing 2 (Mbps) | Testing 3 (Mbps) | Average (Mbps) |
|--------|-------------------|------------------|------------------|------------------|----------------|
| Old    | 1                 | 51               | 49.2             | 50.4             | 50.2           |
|        | 2                 | 6.2              | 5.9              | 6.1              | 6.06           |
|        | 3                 | 50.5             | 49.5             | 49.2             | 49.73          |
|        | 4                 | 5.9              | 6.2              | 5.8              | 5.96           |
| New    | 1                 | 56.3             | 56.7             | 57.1             | 56.7           |
|        | 2                 | 56.9             | 56.8             | 56.7             | 56.8           |
|        | 3                 | 50.2             | 51.1             | 50.8             | 50.7           |
|        | 4                 | 6.4              | 5.9              | 6.1              | 6.13           |

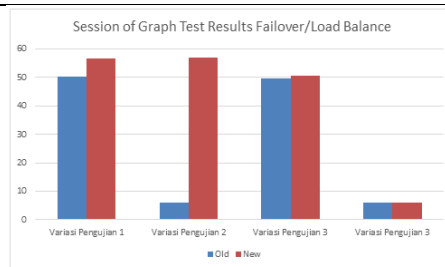
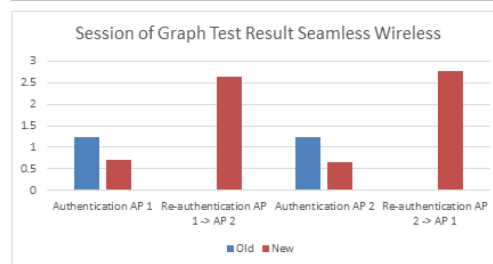


Figure 11: Session of Graph Test Results Failover/Load Balance

From the test results Seamless Wireless seen a significant difference between the old method and the proposed method. Where is contained in the device when the user re-authentication of AP1 to AP2 or vice versa. It can be concluded with an average process time of testing is as follows:

Table 4: Session of Results Testing Seamless Wireless

| Scheme | Authentication AP 1 | Re-authentication AP 1 -> AP 2 | Authentication AP 2 | Re-authentication AP 2 -> AP 1 |
|--------|---------------------|--------------------------------|---------------------|--------------------------------|
| Old    | 1.2286 ms           | RTO                            | 1.2405 ms           | RTO                            |
| New    | 0.6954 ms           | 2.6482 ms                      | 0.6458 ms           | 2.7576 ms                      |



Gambar 12: Session of GraphTest Result Seamless Wireless

From Table 3 and Figure 11 can be inferred old methods can not perform a re-authentication process resulting in a value of 0 or RTO. Aside from the process, there is no difference when the authentication process on each AP. Although the resulting value or time is not significant enough. Visible on the test results of testing in Table 4 and Figure 12, where the test of time when the process of authentication methods to AP 1 time average of 1.2286 ms and testing the new method gets an average of 0.6954 ms. Also visible on old methods when testing authentication process to the AP 2 received an average of 1.2405 ms and testing the new method gets an average of 0.6458 ms.

## 5. CONCLUSION

Based on the description that has been described in previous chapters, it can be concluded as follows:

1. Wireless Controller can be made using a router Kerio Control that has a function as a server AAA (Authentication, Authorization, and Accounting) as RADIUS (Remote Authentication Dial-In User Service).
2. A system of single SSID can be made by modifying the Access Point firmware using open source firmware DD-WRT and utilizes the DHCP Forwarder..
3. SSO system can be implemented by performing periodic sync between the Wireless Controller and Server AD using the techniques of mapping the LDAP protocol.

The suggestion from this study are as follows:

1. Before the development of a seamless wireless systems on multi-domain.
2. Further studies regarding the use of the device and the access point firmware different.
3. Further studies regarding device performance user access point to use the excess.
4. In the design of their systems need software and hardware support and is compatible with existing systems.



---

## REFERENCES

- [1] PUSKAKOM, 2014. *Profil Pengguna Internet di Indonesia*.
- [2] IEEE, 2012. *IEEE Standards Association, Wireless LAN*. [Online] Available at: <http://standards.ieee.org/about/get/802/802.11.html> [Accessed 16 July 2016].
- [3] Singh, J., 2009. Quality of Service in Wireless LAN Using OPNET MODELER. *Patiala: Computer Science and Engineering Department Thapar University*.
- [4] Towidjojo, R., 2013. *Mikrotik Kung Fu*. Kitab 2 ed. s.l.:Jasakom.
- [5] Lacoma, T., 2009. *What Is Seamless Roaming?*. [Online] Available at: [http://www.ehow.com/about\\_6324648\\_seamless-roaming\\_.html](http://www.ehow.com/about_6324648_seamless-roaming_.html) [Accessed 20 August 2016].
- [6] Charter, D., 2008. *Konsep Dasar Wireless LAN*. [Online] Available at: <http://ilmukomputer.org/wp-content/uploads/2008/02/charter-konsepwlan.pdf> [Accessed 24 October 2016].
- [7] Ramani, I. & Savage, S., 2005. *SyncScan: Practical Fast Handoff for 802.11*. Miami: Proceedings of the IEEE Infocom Conference.
- [8] Liao, Y. & Gao, L., 2006. *Practical Schemes for Smooth MAC Layer Handoff in 802.11 Wireless Networks*. s.l.:Mobile and Multimedia Networks.
- [9] Mishra, A., Shin, M. & Arbaugh, W. A., 2004. *Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network*. Hong Kong: Proceedings of Twenty Third Conference of the IEEE Communications Society.
- [10] Lee, C. & Seo, S., 2008. *An Indoor Tracking-based Handoff Mechanism for VoIP Applications in IEEE 802.11 WLAN's*. Seoul: J.Song Yonsei University.
- [11] Rudy, R. O. G., 2009. *Integrasi Aplikasi Menggunakan Single Sign On Berbasiskan Lightweight Directory Access Protocol (LDAP) dalam Portal binus@ccess (BEE-PORTAL)*.
- [12] Cartealy, I., 2013. *Linux Networking*. Jakarta: Jasakom.
- [13] Kerio, 2015. *Kerio Control, Network Security for your Business, Kerio Technologies*. [Online] Available at: <http://www.kerio.com/products/kerio-control> [Accessed 12 September 2016].
- [14] DD-WRT, 2015. *DD-WRT Unleash Your Router, Firmware*. [Online] Available at: <http://www.dd-wrt.com/site/index> [Accessed 12 September 2016].
- [15] Stiawan, D., 2009. *network development cycles*. [Online] Available at: [http://deris.unsri.ac.id/materi/jarkom/network\\_development\\_cycles.pdf](http://deris.unsri.ac.id/materi/jarkom/network_development_cycles.pdf) [Accessed 12 September 2016].