International Journal of Computer Science and Software Engineering (IJCSSE), Volume 7, Issue 11, November 2018
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 255-259

Wireless Network Security Information System on Banking Company with Radius Server Using Authentication, Authorization, Accounting (AAA)

Janu Eka Setiawan

Business Information System, Gunadarma University, Jakarta Indonesia

greyfour59@gmail.com

ABSTRACT

BNI Coporate University (BNV) play an important role in improving the quality of employees in terms of learning. Therefore, the BNV continues to develop digital learning methods, so that the employee can do the expected learning whenever and wherever. The WLAN network connection is managed entirely by the Division of Management Information systems (MIS). There are constraints in the number of users who are not identified and the use of uncontrolled bandwidth on the network WLAN. Currently the WLAN network security applied by BNV uses encryption methods i.e. WEP (Wired Equivalent Privacy). WEP security system on a single keyword to all users of the WLAN encryption are used together. WLAN network security method is still not able to handle the number of WLAN users not entitled to that cause disruption of the available bandwidth capacity. Therefore required a network security method that can identify and authenticate the user using the WLAN. Then implemented by information system authorization networks WLAN by using the method of Authentication, Authorization and Accounting (AAA). By using the information system Authorization Networks WLAN by using the method of Authentication, Authorization And Accounting (AAA) bandwidth usage can fit to their use and increased network security.

Keywords: *Information System, Website, AAA, WLAN, Network, Security.*

1. INTRODUCTION

BNI Coporate University (BNV) play an important role in improving the quality of employees in terms of learning. BNV attempt to provide space for every employee of BNI in developing themselves with a variety of knowledge (the hard skills and soft skills). BNV has implemented a method of learning with digital learning. Current world banking including BNI already leads to digital banking. Therefore, the BNV continues to develop digital learning methods, so that the employee can do the expected learning whenever and wherever. To support this BNV continues to develop learning applications that are accessible by the internet. In addition to learning, employees can also become teachers to other employees by providing mentoring. One of management's efforts to improve the quality of our employees is through learning. Management expects the applied learning method is a method of learning with digital-based.

BNV has had an internet-based learning applications, so that employees can access the learning application BNV anywhere and anytime. In line with this, the BNV must provide access to the internet network to facilitate employees accessing the application of learning in an environment BNV. BNV has 4 locations i.e. BNV Town used as a workplace for BNV staff and as a place for training, BNV Mataram was made as a Center Assessment Center, BNV Slipi a place working for the leader, Deputy leader, Dean and some of the staff, besides BNV BNV Slipi is also used as a training and benchmarking, BNV Regional Learning Center (RLC) the RLC in Surabaya, Surabaya is the BNV for Surabaya and Indonesia region to the East, with the RLC Surabaya, The area around the eastern part of Indonesia there is no longer need to Jakarta to conduct training, due to the RLC has the quality and standard of Surabaya, which is the same as BNI Corporate University in Jakarta.

With the work location and place 4 of the training, then the BNV has to ensure the quality of internet network at 4 locations running smoothly and corresponding functions and needs. Network infrastructure in BNV divided into 2 IE intranet and the internet. For intranet technology completely managed by BNI, then internet network, internet network BNV is divided into 2 IE internet network with a Local Area Network and Wireless Local Area Networks (WLAN). BNV provides internet network using wlan. For the wlan network connection is managed entirely by the Division of Management Information systems (MIS) BNV. There are constraints in the number of users who are not identified and the use of uncontrolled bandwidth on the network wlan. This led to a large number of reports to

the Division of MIS. Wlan users can not access the internet properly around the work areas BNV. Wlan network security currently used in BNV using 2 encryption methods i.e. WEP (Wired Equivalent Privacy). On the security system using a single WEP key words Encryption to all users of the wlan is used together. This causes the WEP method being not suitable public System installed in addition to WEP is WPA (Wi-Fi Protected Access), WPA system has been able to shift the WEP method and result in better security. But both the wlan network security method is still not being able to handle the number of wlan users not entitled to that cause disruption of the available bandwidth capacity. Therefore require a network security method that can identify the user authentication and using the wlan. RADIUS (Remote Authentication Dial-In User Service) server that is used to set and authentication between the WLAN and the method of Authentication, Authorization and Accounting (AAA). So the use of wlan network at BNV can be arranged thoroughly using AAA.

2. BASIC THEORY

AAA issued by the IETF (Internet Engineering Task Force) to provide security, authentication and accounting, the current RFC2865, RFC2866 include:. Security management including key setting along between the RADIUS client and RADIUS server, to encrypt sensitive information, and use the authentication code to test the integrity of the data packet. The primary mechanism the protocols shown in the picture below.

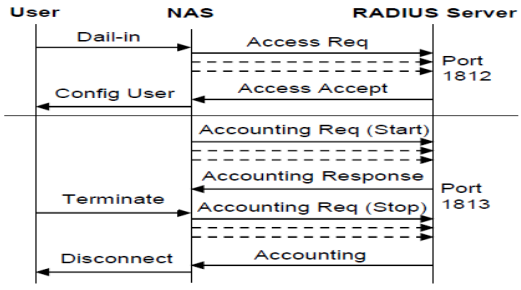

Fig. 1. AAA Comunnication

In the picture above, NAS represent the RADIUS client AAA Protocol in the workflow. The dotted line represents the re-transmission caused by timeout. For brevity, the retransmissions of the response message sent from the RADIUS server to the NAS is not shown. The RADIUS protocol is scalable, the attribute has a length of variables and can carry authentication, accounting and detailed configuration information. In this implementation, the new attributes can be added to expand the Protocol. In the picture above, NAS represent the RADIUS client AAA Protocol in the workflow. The dotted line represents the re-transmission caused by timeout. For brevity, the retransmissions of the response message sent from the RADIUS server to the NAS is not shown. The RADIUS protocol is scalable, the attribute has a length of variables and can carry authentication, accounting and detailed configuration information. In this implementation, the new attributes can be added to expand the Protocol.

Work system Authentication and Authorization when the Network Access Server (NAS) will authenticate users through RADIUS, the NAS sends the Access-Request packet to the RADIUS server. For this NAS sets the proper attributes that describe the information you need about the services required for RADIUS server and user. Password UserPassword attribute in the users are then sent by then encrypted and not sent in plain text. NAS also produces a unique Request Authenticator for requests and resetting the NAS identifier so that it can connect replied to the request. After receiving a request to this RADIUS server checks the list of clients that are in the database. If the request does not come from the user then requests are not continued and no error message is sent. If the user is expired, the RADIUS server to decrypt the user's password (if any) and this is the user checks the database for entries to ask users and checks if the user password is suitable. If the user is not found, the password does not match or the user is not allowed for a while.

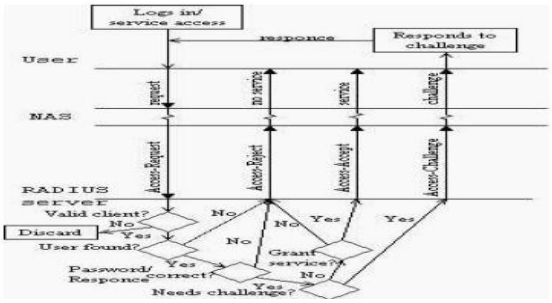

Fig. 2. AAA authentication procedure

When NAS receive a reply and in accordance with the request that uses the identifier. Then the NAS count response Authenticator to receive a reply in the same way a RADIUS server performs and compare this value to the response Authenticator in the message. If it matches, then the RADIUS server responya is confirmed and verified. The process of combining with the shared secret and enskripsi this is the hash of the response Authenticator. The response Authenticator can be used to check the truth to authenticate the RADIUS server. Accounting is done almost the same as authentication and authorization. When NAS receive a reply and in accordance with the request that uses the identifier.

Then the NAS count response Authenticator to receive a reply in the same way a RADIUS server performs and compare this value to the response Authenticator in the message. If it matches, then the RADIUS server responya is confirmed and verified. The process of combining with the shared secret and enskripsi this is the hash of the response Authenticator. The response Authenticator can be used to check the truth to authenticate the RADIUS server. Accounting is done almost the same as authentication and authorization. There are some differences. Accounting using UDP port 1813. There are also two RADIUS message code and 12 attributes to Accounting. Accounting starting with the NAS sends a packet with the Accounting-Request code have the Acct-Status-Type attribute to start to the RADIUS server. In accounting start request, attribute that contains information about the user and the services used. All attributes that can be used in Access-Request can also be used in the Accounting-Request with five exceptions. This is the User-Password, CHAP-Password, ReplyMessage, State and the CHAP-Challenge attribute.

3. REASEARCH METHOD

The first step to designing the system that is retrieved from a data analysis of the field and collect the necessary information or data on the material covered. The stages are done for research to design and manufacturing research. Stage performed in the planning stages, namely the study of the field and the study of literature.

1. Field Studies the data collection phase is held against the direct observation of the condition of the field that was in the banking company.
2. Did a study of literature through books and references obtained from either the library or the international journal. As for the book in question is a book related to computer networks AAA Radius Server, method, and software used in this study. Whereas the reference in question is the IEEE (Institute of Electrical and Electronics Engineers)

4. DISCIUSSION

Network to connect the internet network BNV, it is done to support the smooth running of day-to-day work in completing the BNV staff and smooth execution of the training in the city, the BNV BNV Slipi, RLC, and Assessment in Mataram. For the Wifi network in maintenance entirely by E.G. the BNV.

4.1 BNV Wifi Network Topology

Network interconnection BNV is a network-based VPN-MPLS connecting branches BNV throughout Indonesia. The network has a backbone of 1Gbps which are supported by the infrastructure of the optical property of BIZNET. This network using dynamic routing OSPF that supports rapid change and use of the ip address on a branch of the BNV. With the interconnection of this network then the radius server will be central in ter-BNV Jakarta City. Which facilitates data integration faster if the data changes on the primary database.

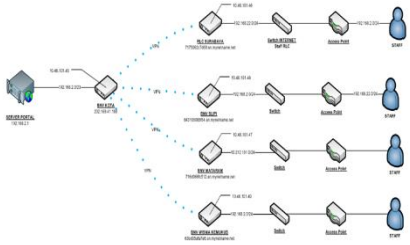

Fig. 4. BNV Interconnection Network Topology.

4.2 Topology Network Wifi BNV

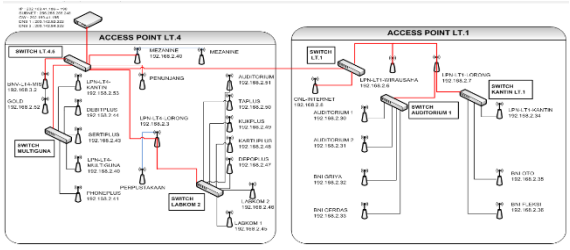

Fig. 5. BNV City Wifi Network Topology.

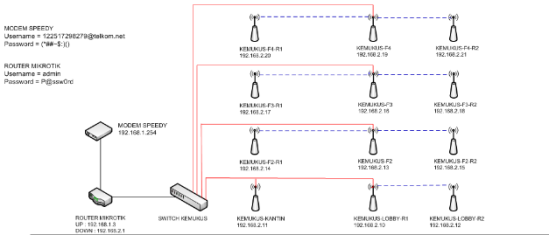

Fig. 6. BNV Kemukus Network Topology.

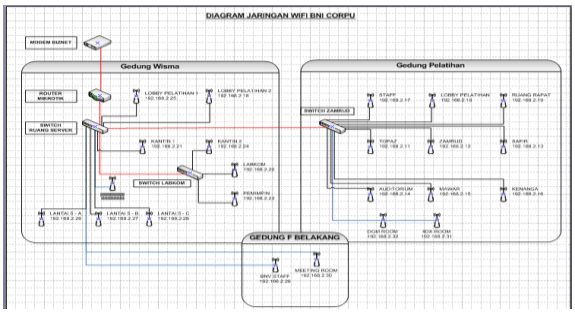

Fig. 7. BNV Slipi Network Topology.

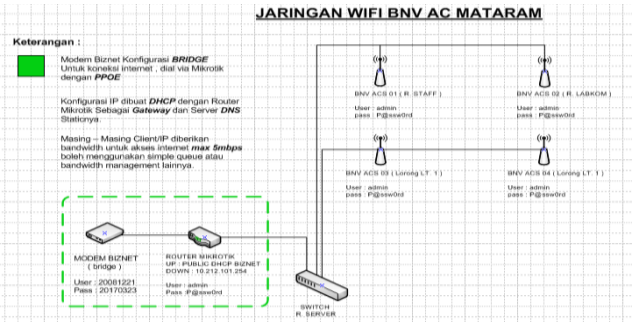

Fig. 8. Wifi Network Topology Assessment Center Of Mataram

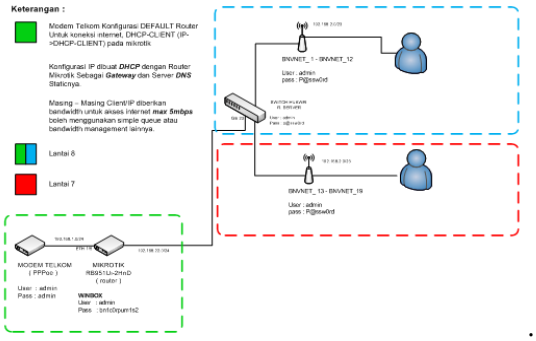

Fig. 9. RLC Surabaya Wifi Network Topology

4.3 Wlan Configuration to RADIUS AAA Server

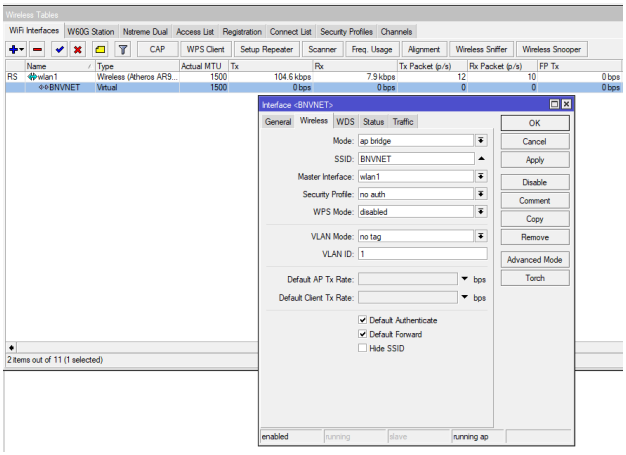

Fig. 10. The Configuration Of The Access Point

4.4 IP Address Configuration On The Access Point

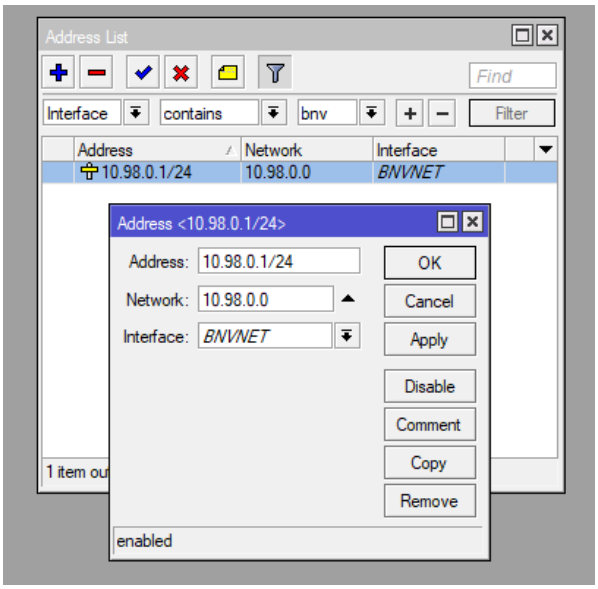

Fig. 11. IP Address Configuration On The Access Point

4.5 The Configuration Of The Radius Client Access Point

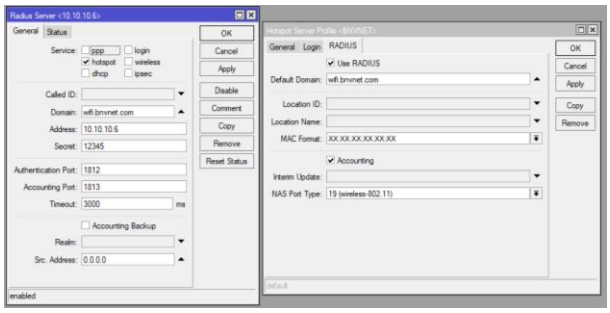

Fig. 12. The Configuration Of The Radius Client Access Point

4.6 Bandwidth Management Configuration

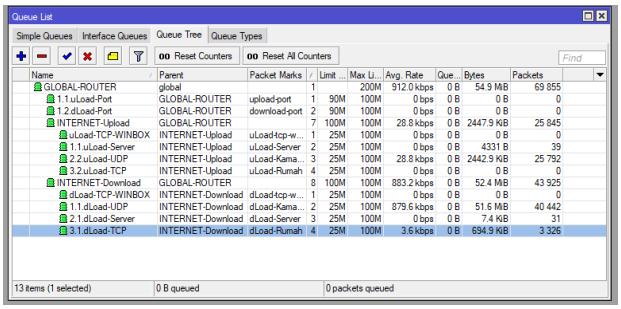

Fig. 13. Bandwidth Management Configuration

5. CONCLUSIONS

Based on the results of this research it causes that affect internet speed and bandwidth usage are high as well as the use of which is not in accordance with the last kebutuhanya, then diimplemtasikan into information system authorization network WLAN by using the method of Authentication, Authorization and Accounting (AAA) can pull the conclusion that:

a. By using the information system Authorization Networks Wlan by using the method of Authentication, Authorization And Accounting (AAA) bandwidth usage in accordance with their use and increased network security because there were safeguards the only additional registered in the system can access to the network.
b. The design by using the MySQL database table that generates mutually integrated between one another. So as to facilitate the collection of data is structured, accessible easily, quickly and accurately.

The bandwidth that is used after the implementation of the information system Authorization Networks Wlan by using the method of Authentication, Authorization And Accounting (AAA) yields the amount of 60% of the available bandwidth sehinggan bandwidth is still available can be used for other needs that can support the activities of BNI CORPORATE UNIVERSITY (BNV).

REFERENCES

[1] Aristiara dan Budihartanti. (2014). Otentikasi pengguna jaringan menggunakan radius windows 2008 server pada pt pertamina. Vol. XI No. 2. Jurnal Techno Nusa Mandiri.
[2] Dhiman, D. (2014).Wlan security issues and solutions. IOSR Journal Of Computer Engineering (IOSR-JCE) E-ISSN: 2278-0661, P- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 67-75.
[3] Halvorsen, H.P. (2016). Introduction to database systems. University College Of Southeast Norway.
[4] Haq, Timur Dan Rahmadi. (2015). Implementasi aaa menggunakan radius sever pada jaringan vpn (study kasus: pt. forum agro sukses timur). Jurnal Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.
[5] Hoang-Tao. (2015). Fast authentication method for wireless local area network. International Journal Of Security And Its Applications Vol. 9, No. 6 (2015), Pp. 53-60.
[6] Jian dan Tian-Zhu. (2016). Design, extension and implementation of radius client International Journal Of Future Generation Communication And Networking Vol. 9, No. 5 (2016), Pp. 181-188
[7] Liu, C dan Yu, J. (2017). A solution to wlan authentication and association dos attacks. IAENG International Journal Of Computer Science, 34:1.
[8] M.D.L Siahaan, M.S Panjaitan, dan A.P.U Siahaan. (2016). Mikrotik bandwidth management to gain the users prosperity prevalent. International Journal Of Engineering Trends And Technology (IJETT), Volume-42 Number 5.
[9] Ndueso, J.S, Charles, N, Robert, O, dan Nwamara, U.A .(2013). Developed secure network model using radius server. International Journal Of Engineering Science And Innovative Technology (IJESIT) Volume 2, Issue 2
[10] R. Wulandari. (2016). Analisis qos (quality of service) pada jaringan internet (studi kasus: upt loka uji teknik penambangan jampang kulon – lipi). Jurnal Teknik Informatika Dan Sistem Informasi Volume 2 No`mor 2.
Rhodes, D.L Dan Bureau, C. (2012). The systems development life cycle (sdlc) as a standard: beyond the documentation.
[11] Support.Sas.Com/Resources/Papers/Proceedings12/194-2012.Pdf. Diakses 15 Februari 2018.
[12] Waliullah dan D. Gan. (2014). Wireless lan security threats & vulnerabilities: a literature review. (IJACSA) International Journal Of Advanced Computer Science And Applications, Vol. 5, No. 1.