Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STUDY ON PORT BASED ON USER AUTHENTICATION SYSTEM USING IEEE 802.1X

[1]Young-Geun Yu, [2*]Koo-Rack Park, [3]Dong-Hyun Kim

[1]Dept. of Computer Engineering, Kongju National University, 31080, Rep. of Korea

[2*]Dept. of Computer Science & Engineering, Kongju National University, 31080, Rep. of Korea

[3]Dept. of Computer Engineering, Kongju National University, 31080, Rep. of Korea

E-mail: [1]ygyu@krict.re.kr, [2*]ecgrpark@kongju.ac.kr, [3]dhkim977@naver.com

ABSTRACT

Recently due to electronic weight lightening and miniaturization of devices, dissemination of devices such as smartphone is expanding abruptly. Concurrently with the convenience in carrying services using smartphone are increasing abruptly, leading us to many variations in life due to IOT environment realized. Especially as BYOD (Bring Your Own Device) ubiquitous environment is briskly realized, the business focused on use of internet is becoming the general trend in human living. Most of the businesses at government institutions, corporate or research laboratory, general households, are performed through network service. However, dependence on network is so high that any problem at network may cause paralysis of all businesses. Also operator maintaining the network requires much time and effort to resolve the problem of failure. Especially in case of any failure occurred in relation to security, the system to grasp the information comprising MAC, IP, access time, user etc in prompt and intuitive way is lacking, consuming much time in resolving problems. Recently as the IEEE 802.1x based wireless network expands, various services being provided. However, in the situation where many attacks through wireless network are occurring, this thesis proposes the authentication system that resolves the simple, repetitive problems which may occur between network user and the person in charge of network maintenance and can expedite user authentication, through user authentication based network design that can manage the authentication of dispersed network in centralized and flexible manner. Through the proposed system, threat to security would minimized and the user and network managers are anticipated to break from the simple, repetitive duties on internet service and management. Future studies shall be directed to the IP back tracking that can respond positively to the judgment and classification of wired-wireless traffic, and to the threat to security.

Keywords: *IEEE 802.1x, Authentication, Authorization, RADIUS, Firewall*

1. INTRODUCTION

Recently due to the development of information technology in overall industry, speedy changes are occurring. Especially various services through smart devices are rendered, and much variance is occurring in human living due to establishment of IOT environment. It is no exaggeration to tell that at the heart of these changes is the development of internet through information telecommunication network. These information telecommunication networks continuously grasp and improve past problems, and repeating sophistication by adding productivity. daily work and study activities of most corporates and research laboratories are being performed through information telecommunication network, which functions as the core infrastructure that would be paralyzed in all activities if in case of network failure. Due to brisk development of information telecommunication network, the duties of the worker in charge of telecommunication infrastructure are expanding vastly from basic simple work to the works requiring highly sophisticated technological capacities. Especially in case of any security related accident, due to lack of system that enables fast and intuitive grasp of Information such as MAC, IP, access time, user etc, much time and costs are invested to resolve such problems[1].

Especially any user intending to receive service using network, when accessing through wireless, cable, VPN(Virtual Private Network),

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

firewall etc, feels much difficulties in the access method through mutually different ID and Password, leaving much burden to the person in charge of network. Recently IEEE 802.1x based wireless LAN is briskly in expanded use. In case of access to internet using wireless LAN, less cost is incurred than cable based network composition and is convenient to use. Accordingly use of wireless LAN is briskly expanding at corporates and research institutions, campus, household etc. However any attacker attacking wireless LAN can perform various attack on wireless network, such as spoofing IP address and creating mass traffic identically with any attack of cable network. IEEE 802.1x is the framework that supplemented the weakness of 802.11b in user authentication [2],[3], and supports user authentication mechanism. However this is very vulnerable to attacks such as session hijacking etc due to lack of authentication and cryptogram mechanism to DoS (Denial of Service) attack and AP (Access Point), which was caused by structural reason in authentication protocol [4]. In this regard, this thesis proposes the method to use the port based user authentication and network information using IEEE 802.1x, in order to resolve the simple, repetitive problems which may occur between network user and the person in charge of network maintenance through user authentication based network design.

Through the proposed system, it is anticipated that mutual win-win is achievable in dynamic network environment and threat to security would minimized. Future studies shall be directed to the IP back tracking that can respond positively to the judgment and classification of wired-wireless traffic, and to the threat to security.

2. RELATED RESEARCH

2.1. 802.1x Architecture

IEEE 802.1x controls port based network approval in Ethernet network [5],[6]. At first this was introduced for cable network, but is recently used mainly at wireless 802.11 network. The following [Figure 1] is the adoption of composition element of AAA (Authentication, Authorization, Accounting) architecture in abstraction of 802.1x architecture by other nomenclature [6],[7].

AAA server is the authentication server system, and includes authentication server. This actually performs the role of allocating authentication and authority.

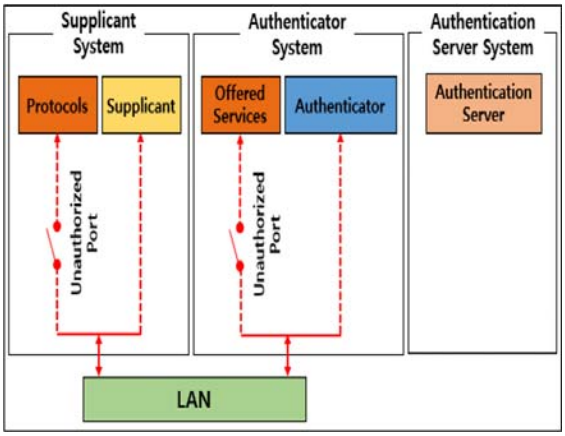

Figure 1 : Port based Authorization Model

The port within authentication supplicant and authenticator system may be deemed as abstract port entity. If authentication and authority grant is not successful, the supplicant system can only arrive at the authentication module in authentication system. 802.1x AA procedure always commence from the supplicant that transmits start message to authenticator, unauthenticated port is authenticated and authority grant is successfully completed. Also authentication server may inform whether access shall be allowed to authenticator in binary information, or provide the particular VLAN tag for expected user traffic [8],

The following [Figure 2] is the interaction between composition elements of classic 802.1x architecture, including all frontend and backend AA [9]. The frontend authentication between authentication supplicant and authenticator module is defined by the EAP (Extensible Authentication Protocol) [10], and the back end AA between the authenticator module and authentication server is performed by RADIUS (Remote Authentication Dial in User Service) protocol [11] and the Diameter protocol [12].

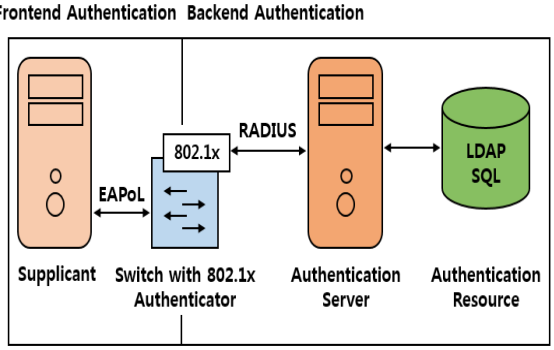

Figure 2 : Interaction of components in the classic 802.1x architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2. EAP and RADIUS in 802.1x

The following [Figure 3] is an example of 802.1x based authentication/authority grant flow. Authentication is granted mainly through 4 stages, and is the protocol most widely used in back end AA.

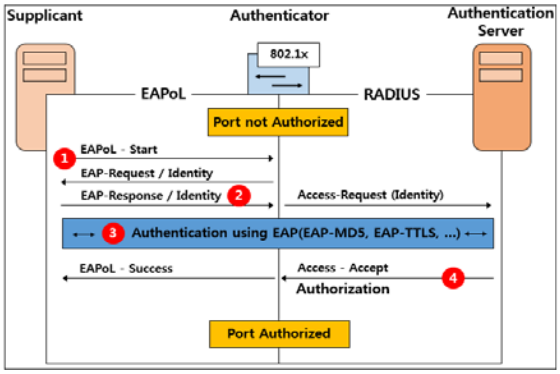

Figure 3 : Example of 802.1x based authentication/authority grant flow

First is the initialization stage of AA in 802.1x, where supplicant module in network client commences authentication and authorization by transmitting EAPoL start message. EAPoL (EAP over LANs) is the encapsulation to transmit EAP message in the Ethernet frame introduced concurrently with 802.1x. EAP facilitates telecommunication between supplicant and authenticator, and provides fixed request and response system exchanging authentication data.

Second is the identity based AA in 802.1x, where authenticator requests client's identity and transmits to RADIUS authentication server. RADIUS is the RADIUS server composed in multiple layers, with user identity connected to domain, and keeps information in the RADIUS server of relevant domain. Identity is the most relevant information in routing of AA trial within the RADIUS infrastructure.

Third is the 802.1x authentication, and authentication is performed between authentication supplicant and authentication server. The authenticator decapsulates EAP packet in EAPoL frame, and encapsulates again in RADIUS frame, and vice versa. Flexible message structure of EAP allows use of other authentication procedure. Simple access method delivers normal text identification information or simple MD5 -hashed password, and supports stable authentication procedure such as IKEv2 for EAP[13] and EAP tunneled TLS[14], EAP-TLS[15]. Also, as authenticator relays EAP message only by pass-through method, it is not necessary to realize the characteristics of EAP type.

Fourth is the 802.1x approval. After successful authentication, RADIUS server returns authentication data such as VLAN tag. The authenticator applies authentication data such as VLAN tag to particular physical port such as switch, and the authenticator confirms successful AA to supplicant using EAP's success message.

2.3. EAP Overview

2.3.1 EAP Protocol

EAP[16] is not a protocol, but a frame work based on other typed protocol with capacity to add new protocol easily to frame work, and is defined at RFC 3748[17]. EAP was developed originally for use as PPP (Point to Point Protocol), where Protocol at EQP frame work can be selected as package contract between client and server but both parties shall use identical protocol for authentication and telecommunication. The following [Figure 4] is major composition elements of EAP, classified into 3 main categories.

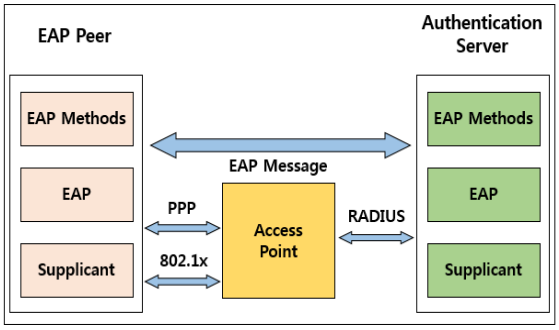

Figure 4 : Major EAP composition element

First is Client/Supplicant, which requests access to wireless network.

Second is AP (Access Point) which receives wireless signal and transmits to cable network, functioning as the relay between client and server. As identification of client has not been checked, any client accessing for the first time is cut off. This is composed of two logic ports of control port and non-control port. When the user has been authenticated, control port is used. If, user has not been authenticated, control port is used for telecommunication only.

Third is the AS (Authentication Server) called RADIUS as a kind of authentication server, which is a remote server with user account information in storage. When all users intend to be connected to server, the server verifies the existence

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of relevant user. If user has been authenticated, the authentication server transmits information to access point and sets up dynamic access control list.

2.3.2 Authentication Methods of EAP

Generally, authentication protocol using EAP may be classified in 4 categories mainly.

First is EAP-MD5[16], which is based on single direction hash function, and takes long input message arbitrarily to create the pseudo-random output called hash. The merit of hash is the difficulty in finding identical message that could create mathematically identical hash. Also DM5 message is not stored in general text type in the server side. When a user creates his/her account at the server and input cryptogram, the server brings the hash of relevant cryptogram and put in storage. Nextly when a user logs in the server, user shall input the cryptogram. MD5 protocol at the client side converts relevant cryptogram into hash value and then delivers to the server. The server receives hash from the client and compares the hash value so arrived. Realization of MD5 can be completed easier than in comparison with other protocol, and so is used for verification test for effectiveness of user. However, this has the demerit where WLAN attacker can easily sniff client ID and password hash, does not support mutual authentication, only verifying the effectiveness of client.

Second is EAP-LEAP (Light Weight Extensible Authentication Protocol)[18], developed by Cisco to resolve the weakness of WEP. This verifies effectiveness from both sides by providing mutual authentication based on challenge/response model. Temporary session key is derived, is computed promptly and is fungible with existing well known authentication method of EAP-TLS.

The third is EAP-TTLS (Tunnel Transport Layer Security)[19], which is the client authentication to overcome the demerits of TLS. This is similar to TLS, but third party's authentication certificate is required from server side. The tunnel has the merit of advance using legacy protocol in client authentication. By use of tunnel, client identity is hidden, and TTLS is composed by the following 2 stages, identically with other tunneling protocol.

- Server authentication certificate is used, to inspect server effectiveness and to set up encrypted tunnel in symmetry.
- Client ID is confirmed using other protocol. But verification of identity is implemented within the tunnel, so identity of client can be protected.

The fourth is EAP-PEAP (Protected Extensible Authentication Protocol)[20], also known as EAP inside EAP, as a tunnel method.

Identically with TTLS, this verifies the effectiveness of server using server authentication, and is used for TLS based tunnel 을 cryptogram 화 and providing authentication. As the message is encapsulated within tunnel, various typed attacks may be prevented. PEAP is mobilized in the following 2 stages.

- Client uses server authentication certificate to inspect server effectiveness, and then negotiates and sets up TLS session.
- Server inspects client effectiveness using EAP method rather than legacy.

In case the PEAP client used at WLAN inspects server effectiveness by authentication certificate, security tunnel is regarded as created.

3. PROPOSED SYSTEM

3.1 Status before of composition of authentication network

In case of cable network hub or sharer is used at lower of switch, it takes much time to grasp physical composition status and to resolve problems upon occurrence of failure. In case of wireless network and VPN network, separate authentication account is operated individually, and it was difficult to update password regularly to enhance security, users often forgot passwords. As the support load by network staffs are heavy, stresses at workplace is heightened.

The following [Table 1] is the status of network composition.

Table 1 : Status of network composition

Section	Contents
Cable	Private network and institutional network mixed
Wireless	Wireless LAN controller / wireless IPS / authentication server
VPN	VPN local account in place
Firewall	IP based access list application

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 Network user / manager issue

Users intending to access network for authentication feels inconvenience in use of network as the access ID/Password for wired and wireless, VPN are different. In case of relocation of user, many inconveniences are experienced until the staff in charge resolves such issue.

The following [Table 2] shows the network user issues.

Table 2 : Network user issues

Section	Contents
Cable	Network installation request and IP user application received upon new subscription/relocation
Wireless	Wireless LAN user approval application received upon introduction of a new terminal
VPN	VPN user application
Firewall	Firewall access application received and re-application due to relocation and organizational restructuring

Also managers in charge of network are more fatigued due to simple, repeated works accompanying VLAN setting upon occurrence of new and relocating user, issue and re-issue of IP address, manual registration of MAC at WIPS device upon introduction of new wireless terminal, real time grasp of IP/MAC/user/access time/operation system accessed to network, client verification in processing information protection accident and network failure, cabling and network re-composition upon organizational restructuring.

Other than these works, they are engaged in other duties such as processing various official letters from external institutions, review on sophistication measures, inspection and preparation of responding measures upon occurrence of information protection accident, information security assessment to be processed in emergency etc.

The following [Table 3] shows network manager issues.

Table 3 : Network manager issues

Section	Contents
Cable Network	VLAN set up upon occurrence of new/relocation user
	IP address allocated upon occurrence of new/relocation user
	Manual IP ;management by Excel or dedicated system used
Wireless Network	MAC address manual registration at WIPS
Wire/Wireless, Firewall, VPN	Access ID/Password managed separately by media

3.3 The composition direction focused on manager/user

In this thesis, network is composed applying user oriented operational concept. Therefore, VLAN is automatically allocated based on user ID, IP address is automatically allocated though DHCP server, then user ID is a acknowledged through identity firewall, so that intuitive security policy is applied to user ID.

The following [Table 4] is the composition direction focused on manager.

Table 4 : Composition direction focused on manager

Section	Contents
VLAN	VLAN/IP automatically application according to user's headquarter/ branch/ department/cable/ wireless/ smart device
IP allocated	IP address is automatically allocated according to VLAN
Wireless Network	MAC information automatically linked between Authentication server and WIPS
Firewall	Organic ACL policy applied through user ID

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As for the direction of authentication network composition focused on manager, direction is set up focusing on automatic VLAN/IP application by user, automatic registration of MAC information from approved wireless terminal, intuitive ACL policy application at firewall based on user ID, and establishment of real time recognition system on user/IP/MAC/operation system/access time. Also as for direction of composition focused on *user*, direction is set up focusing on access method through identical ID and password by media, and prompt network use system.

The following [Table 5] shows the composition direction focused on *user*.

Table 5 : Composition direction focused on *user*

Section	Contents
Wired/ Wireless VPN	Identical ID/Password application
Wired/ Wireless	new/relocation when plug and play & mobility application
	internet user registration for visitor is approved by relevant department

3.4 Composition of authentication network

The following [Table 6] shows the preparations for composition of authentication network.

Table 6 : Preparations for composition of authentication network

Section	Contents
Authentication system	VLAN policy set up according to headquarter/branch/department/cable/wireless/smart device
	802.1x set up information automatically distributed according to user's OS(Windows, OSX, Linux, Smart Device)
Account System	Wired /wireless / VPN user integrated account prepared
firewall	Identity firewall
Access Witch	Hub, sharer removed
	1PC connection environment created to switch 1 port
DHCP Server	IP automatic distribution environment set up

By setting up 1 PC/port environment at access switch, only one VLAN can be set up at a single port, and single user can be accurately controlled.

The policy authentication system considers various case of use, in order to apply VLAN and IP address to be used in future. At the authentication system, after verification of user account, download 802.1x set up information to client and download VLAN, ACL to switch port. And the account system holds user account.

The following [Figure 5] is the composition diagram for authentication network as the proposed system. Logically, authentication system is placed at the center of the network, and network is composed and operated focusing on user's identity.

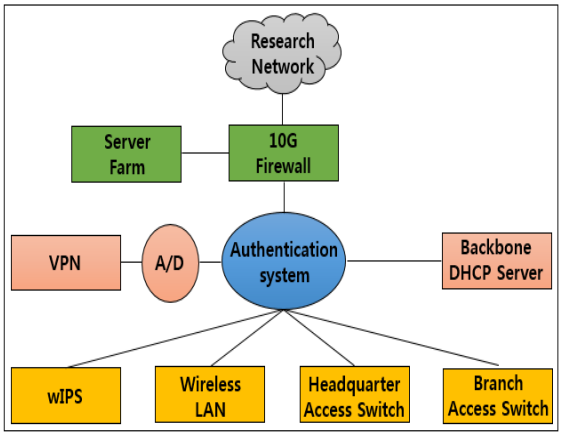

Figure 5 : Composition diagram of authentication network

3.5 Internal composition of authentication network

The following [Figure6] shows the internal composition of authentication system, which comprises 4 categories.

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

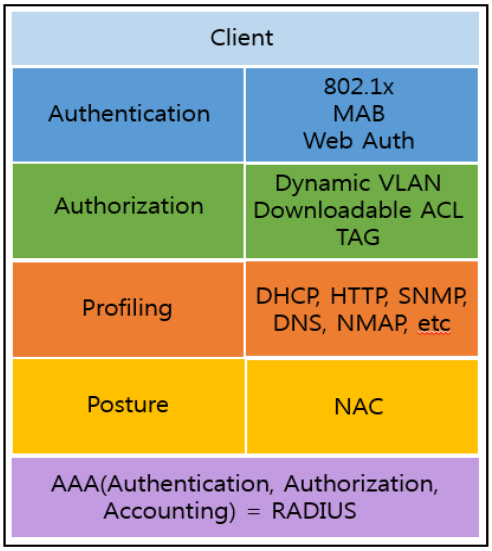

Figure 6 : Internal composition of authentication network

The authentication system is the system using RADIUS protocol and provides AAA function. Implementation module of authentication server is classified mainly in 4 categories.

First is Authentication, authentication method provides 802.1x authentication for user authentication in client system that can use internet browser, MAB authentication for system authentication such as printer and CCTV, and Web-Auth authentication method for uses without set up of 802.1x.

Second is Authorization, After authentication, authority grant function provides VLAN allocation function to authenticated user, port ACL allocation method to user, and the tag allocated function that supports mapping of user ID, IP address at firewall.

The third is Profiling, Various protocols are used to grasp detailed information on clients using the authentication system, capable of verifying the service port opened during use of NMAP.

Fourth is the Posture, which is a function usually named NAC. This function inspects whether security policy level has been observed before access of host to network, and controls network access.

3.6 Cable network authentication procedure

The following [Figure 7] is the flow chart for cable network authentication procedure, which shows the flow of authentication and network according to the situation of internal and external users in cable network authentication.

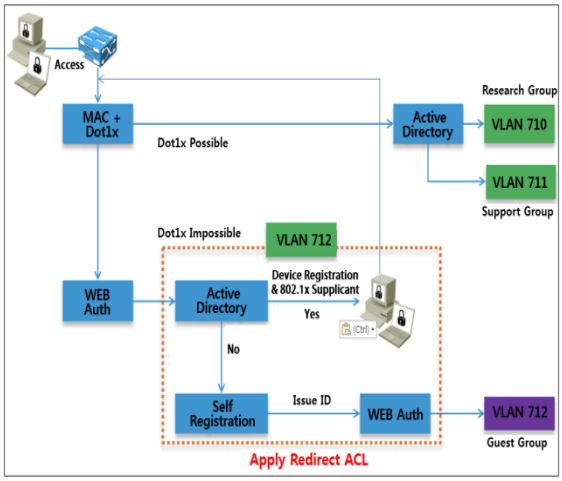

Figure 7 : Wired network authentication procedure flow chart

When authenticating wired network and in case of any internal user with active directory account, the condition for successful authentication is user PC MAC registration on authentication system and 802.1x set up at user PC. After application of VLAN set to user and IP address allocated and dACL, access to internet and necessary service is available. In case authentication failed, user is induced to web authentication, 802.1x supplicant is downloaded after verification of active directory account.

Subsequently by re- authentication process, MAC+Dot1x authentication would be successful. Thereafter, access to necessary service is possible. In case of external user, active directory account does not exist, and so is in the situation of not satisfying authentication condition. After failed authentication, composition is made to use limited telecommunication resources, and by registering independent account in authentication system, web authentication is enabled.

3.7 Wireless network authentication procedure

The following [Figure 8] shows the flow chart for wireless network authentication procedure, which shows the flow of authentication and network according to the situation of internal and external users in wireless network authentication.

When authenticating wireless network user, and in case of any initial access by internal user with active directory account, access is made wireless through GUEST_SSID.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

After implementation of user web authentication, active directory account is verified, then 802.1x supplicant is downloaded to proceed re-authentication process.

After success of Dot1x authentication, VLAN and IP address set up for user is allocated, and the telecommunication resource of the internet and internal user can be used.

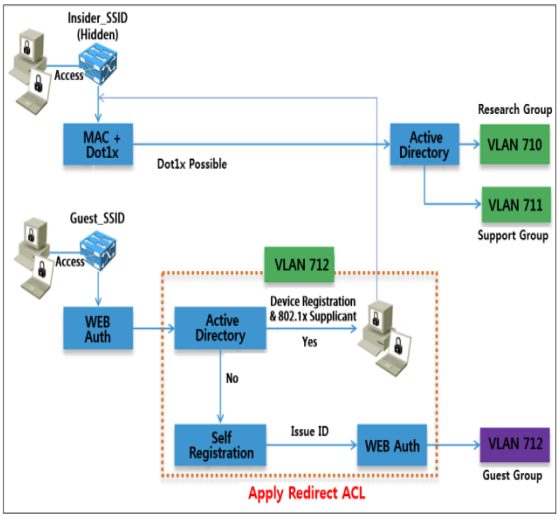

Figure 8 : Wireless network authentication procedure flow chart

The following [Figure 9] is the access authentication flow chart in case of internal user after initial access of wireless LAN is implemented.

After initial access, continuous use is available by access to wireless through internal Insider_SSID.

In case of external user, access is done through Guest_SSID, and use is possible after registration of independent account by implementation of user web authentication to the authentication system, and composition is made to use limited telecommunication resources.

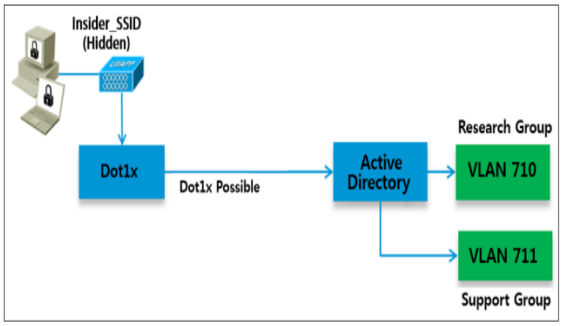

Figure 9 : Wireless initial access authentication flow chart

3.8 Authentication system

In order to implement 802.1x authentication, switch port environment and whole band of switch are set up at the user L2 switch.

Next is set up of switch port environment and whole band of switch.

The switch port type set up and concurrent use of IP phone is set up. Upon IP access, basic ACL access policy is established. In case of failed set up, re-booting of phone device occurs. Also in case of failed authentication, the next authentication procedure is implemented, and guest VLAN is declared to induce self-service portal.

```
switchport mode access
switchport voice vlan 304
ip access-group Voice-Allow in
authentication event fail action next-method
authentication event server dead action authorize vlan 592
authentication event server alive action reinitialize
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict mab
dot1x pae authenticator
dot1x timeout tx-period 5
dot1x max-req 1
dot1x max-reauth-req 3
dot1x timeout auth-period 2
spanning-tree portfast
```

```
aaa new-model
!
!
aaa group server radius krict
server-private xxx.xxx.xxx.xxx auth-port 1812 acct-port 1813 key 7 0208024902475E731F1A
server-private xxx.xxx.xx.xxx auth-port 1812 acct-port 1813 key 7 11071F171E535A5E577E
```

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
!
!
aaa authentication login default group radius
local
aaa authentication login LINE-CON none
aaa authentication dot1x default group krict
aaa authorization network default group krict
aaa accounting dot1x default start-stop group
krict
!
!
aaa server radius dynamic-author
client xxx.xxx.xxx.xxx server-key 7
0701275E474848574446
client xxx.xxx.xxx.xxx server-key 7
04550D1406601D1C5A4D
```

The authentication system is realized so that authentication status may be accurately monitored through set up of user authentication scenario and switch device environment.

And authentication information can be monitored in real time. The following [Figure 10] is the dashboard of authentication server as the proposed system.

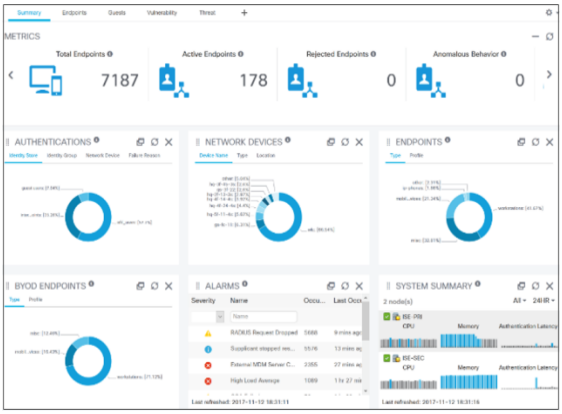

Figure 10 : Authentication server Dashboard

The following [Figure 11] is the overview of authentication server after completed user authentication, where user name, endpoint ID, profile, Authentication and Authorization policy may be confirmed.

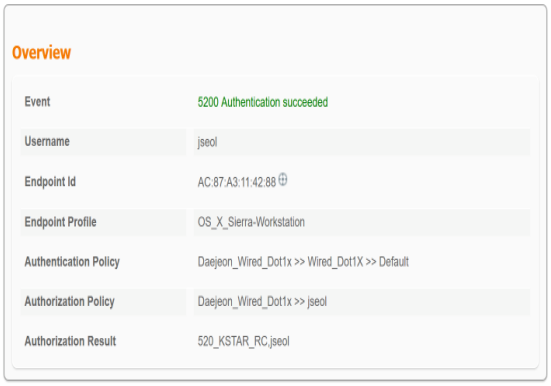

Figure 11 : Overview of user port authentication

4. EXPERIMENTS AND DISCUSSION

4.1 Anticipated effect of authentication system

After setting up authentication network, work performance form of users and managers has been improved in positive direction. In case of user, network access method and process was simplified. In case of managers, simple, repeated works were removed, with the capacity for real time monitoring of user access information.

At the firewall, managers can perform ACL management intuitively by user. However in case of wireless network, due to security issue, external network is separated and operated as independent network. The following [Figure 12] shows the comparison between before and after user authentication network.

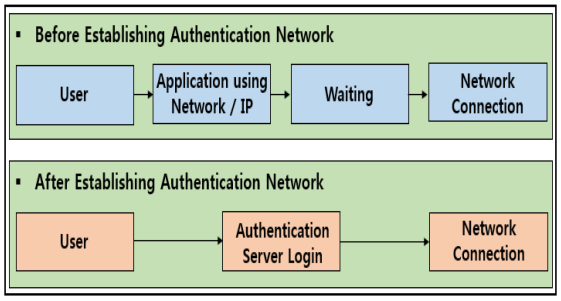

Figure 12 : Comparison between before and after set up of authentication network

In case of external user, immediately upon approval by the department in charge, network connection and service is available. Upon user's request, the person in charge of network maintenance used to grant VLAN set up and IP address, and notified the same to user, so as to permit access. Now immediate service is possible through the authentication system monitoring, so simple, repeated labors are avoided.

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The following [Figure 13] shows the work duty changes in case user requests network connection to the person in charge.

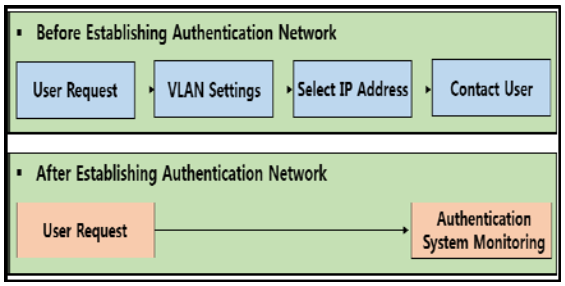

Figure 13 : Work duty change upon user request

4.2 Additional use of authentication system

Recently, infringement accidents due to smart devices are increasing. When Internet traffic occurs in iOS and Android based smart devices using wireless LAN, it can be bypassed to the ADSL network instead of the institution's internet network by using authentication system.

The following [Figure 14] is a conceptual diagram for additional use of the authentication system.

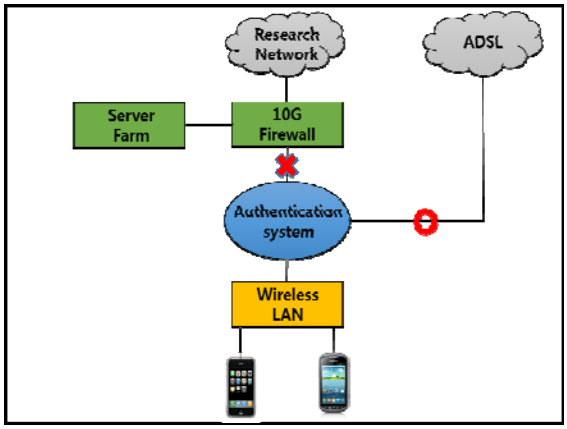

Figure 14 : Conceptual diagram for additional use of the authentication system

4.3 User verification of authentication system

The effectiveness of the authentication server system proposed in this thesis was verified by user satisfaction level.

The following [Table 7] shows the result of satisfaction level survey. The user satisfaction level, system effectiveness, system efficiency were surveyed to 83 users comprising internal network user and manager, external user, over 90% responded with satisfaction or higher, showing overall positive satisfaction level.

Table 7 : Survey Results

File Name	System Efficiency	System Effectiveness	User Satisfaction
Very Good	63	59	67
Satisfaction	12	13	13
Normal	4	6	2
Dis-Satisfaction	4	5	4
Very Dis-Satisfaction	0	0	0

5. CONCLUSION AND FUTURE DIRECTIONS

As the result of information technology development, the overall industry is experiencing diverse changes. Due to weight lightening and miniaturization of electronic devices such as smartphone. Concurrently with the convenience in carrying, services using smartphone are increasing briskly, and establishment of IOT environment is causing much change in human living. Especially it is not exaggerating to tell that at the core of the services of telecommunication terminal devices, is the use of internet through information telecommunication network. Also most works at each corporates or research laboratory etc are implemented through network service.

Especially, most are the cases where any failure in network failure would paralyze all businesses. In case of network failure, network staffs spend huge costs and time to recover from such failure. Especially in case of any security related accident, huge time and costs are spent for recovery, due to lack of the system that can grasp the information comprising MAC, IP, access time, user etc in fast and intuitive way. Also users without the opportunity for professional training are experiencing many difficulties in access methods such as wired, wireless, VPN. This again brings big workload to the network staffs.

Recently as IEEE 82.1x based wireless network expands, numerous internet services became available. However, attackers attacking wireless network can maneuver various attacks on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the wired network. 802.1x is the framework that supplemented the vulnerability of user authentication, supporting user authentication mechanism. This thesis proposes the authentication system that can resolve the simple and repeated problems that may occur between network users and the person in charge of network maintenance through user authentication based network design, and can expedite user authentication.

Through the proposed system, it is anticipated that any threat to security would be minimized, and users and network managers are relieved from simple, repeated labors on internet service and management. Also to verify the proposed system, user satisfaction level was surveyed. According to the survey result, more than 90% of respondents were satisfied.

IEEE 802.1x authentication does not provide Pre or Post authentication provided by general network access control (NAC). Future research should continue to study the IP backtracking that can interoperate with IEEE 802.1x authentication and the functions provided by general NAC, identify and classify wired and wireless traffic, and actively respond to security threats.

REFERENCES:

[1] Y. G. Yu, K. R. Park, D. H. Kim, S. H. Park, M. S. Yoon, "The Study on Methods for User Authentication based on Port using 802.1x and Utilization of Information", *The 2nd International Conference on Computing Convergence and Applications*, August 17-20, 2017, pp. 173-176.

[2] Arunesh Mishra, William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", *University of Maryland*, 2002, pp. 1-12.

[3] P. Funk, S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", *IETF PPPEXT Working Group*, 2005.

[4] S. P. Hong, S. J. Han, "Wireless LAN System based on IEEE 802.1x EAP-TLS Authentication Mechanism", *Journal of Korea Institute of Information and Communication Engineering*, Vol. 16, No. 9, 2012, pp. 1983-1989.

[5] IEEE, "802.1X-2010 IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control", 2010.

[6] IEEE, "802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control", 2004.

[7] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic AAA Architecture", *RFC 2903 (Experimental)*, August 2000.

[8] P. Congdon, M. Sanchez, and B. Aboba, "RADIUS Attributes for Virtual LAN and Priority Support," *RFC 4675 (Proposed Standard)*, September 2006.

[9] HAUSER, Frederik; SCHMIDT, Mark; MENTH, Michael., "Establishing a session database for SDN using 802.1 X and multiple authentication resources", In: *Communications (ICC), 2017 IEEE International Conference on. IEEE*, 2017, pp. 1-7.

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

[11] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", *RFC 2865 (Draft Standard)*, Jun 2000.

[12] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn, "Diameter Base Protocol", *RFC 6733 (Proposed Standard)*, 2012.

[13] H. Tschofenig, D. Kroeselberg, A. Pashalidis, Y. Ohba, and F. Bersani, "The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method", *RFC 5106 (Experimental)*, Feb 2008.

[14] P. Funk and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", *RFC 5281 (Informational)*, Aug 2008.

[15] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol," *RFC 5216 (Proposed Standard)*, 2008.

[16] Jyh-Cheng and Yu-Ping Wang "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", *IEEE*, Dec 2005, ISSN 0163-6804/05.

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

[18] Kshitij R.Mawale, Dhananjay M.Dakhane and Ravindra L.Pardhi, "Authentication Methods for WiFi Networks", *International Journal of Application or Innovation in Engineering & Management(IJAIEM)*, Vol. 2, Issue 3, ISSN 2319-4847, March 2013, pp. 356-360.

[19] Khidir M.Ali and Ali Al-Khalifah "A Comparative Study of Authentication Methods for Wi-Fi Networks", *3rd ICCICSN*, November 2011.

[20] Bakytbek Eshmurzaev and Gokhan Dalkilic "Analysis of EAP-FAST Protocol", *34th int. Conf. on Information Technology Interfaces Cavtat, Croatia*, 2012.