Regular paper
Journal of the KIECS. pp. 295-300, vol. 12, no. 2, Apr. 30 2017, t. 82, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.2.295

AAA가 적용된 네트워크의 인증에 대한 검증 사례연구

박성배* · 김노환**

A Verification Case Study about the Authentication of a Network using AAA

Sung-Bae Park* · No-Whan Kim**

요 약

AAA는 사용자에 대한 안전하고 신뢰성 있는 인증(Authentication)을 통해 사용자에게 주어진 권한과 서비스 수준을 결정하여 인가(Authorization)하고, 사용자 자원의 사용정보를 과금, 감사, 리포팅 등을 위한 계정관리(accounting) 기능을 체계적으로 통합 관리하는 정보보호 프로토콜이다.

본 논문에서는 RADIUS와 TACACS+가 적용된 라우터와 서버 기반의 네트워크를 설계하기 위해 토폴로지를 설계한 후 패킷 트레이서를 이용하여 공통 가상 망을 구현한 다음, 시뮬레이션을 통해서 인증에 대한 검증 구현 사례를 제시하였다.

ABSTRACT

AAA, an information-protective protocol authorizes the degree of service and rights to the user through a safe and reliable authentication. The protocol also systematically manages the accounting functions including billing, monitoring, and reporting using the user information.

After a topology was created to design a network based on a router and server using RADIUS and TACACS+, a common virtual network was made using a packet tracker. This paper presents cases showing valid authentication through simulations.

키워드

AAA, RADIUS, TACACS+, Authentication, Virtual Network, Packet Tracer
AAA, RADIUS, TACACS+, 인증, 가상 망, 패킷 트레이서

Ⅰ. 서 론

최근 네트워크 환경의 비약적인 발전으로 사용자의 다양한 요구와 새로운 서비스들이 본격적으로 전개되면서 신뢰성 있는 정보보호 인프라 구축의 중요성이 이 대두되고 있다.

네트워크상에서 비인가 접속은 각종 장비와 서비스에 대해 중대한 보안 위협을 줄 수 있으므로 안전한 접속 관리는 매우 중요하다 하겠다. 네트워크 서비스에 대한 불법적인 사용을 방지하고, 인가된 사용자에 대해 적절

* 경동대학교 간호학부(nadri_90@kduniv.ac.kr)
** 교신저자 : 경동대학교 간호학부
· 접 수 일 : 2017. 01. 12
· 수정완료일 : 2017. 04. 13
· 게재확정일 : 2017. 04. 24
· Received : Jan. 12, 2017, Revised : Apr. 13, 2017, Accepted : Apr. 24, 2017
· Corresponding Author : No-Whan Kim
School of Nursing, Kyungdong University
Email : nwkim@kduniv.ac.kr

한 권한을 부여하며 그 외 서비스 사용내역에 따른 과금을 부여하는 메커니즘 구축은 필수적이라 할 수 있다.

AAA(: Authentication 인증, Authorization 인가, Accounting 계정관리) 네트워크 보안 서비스는 라우터나 액세스 서버의 접근을 제어하는 프레임워크이다.

NAS(: Network Access Server)에 접속하는 사용자에 대한 안전하고 신뢰성 있는 인증(Authentication)을 통해 사용자에게 주어진 권한과 서비스 수준을 결정하여 인가(Authorization)하고, 사용자 자원의 사용정보를 NAS로부터 전달 받아 과금, 감사, 리포팅 등을 위한 계정관리(accounting) 기능을 체계적으로 통합 관리하는 정보보호 프로토콜이다.

본 논문은 관련연구로 해당 논문들을 검토한 후, 선행연구로 AAA를 검토하였으며, 본론에서는 토폴로지를 설계한 후, AAA를 적용한 서버와 라우터, 각 단말기에 IP 주소를 할당한 공통 가상 망을 구현하였다. 서버설정과 인증 실습과정을 연계한 시뮬레이션을 통해서 AAA가 적용된 라우터와 서버 기반 네트워크의 인증에 대한 효율적인 검증사례를 제시하였다.

II. 관련 연구

2.1 논문연구

지승구외 2인(2002)은 차세대 이동통신의 보안요구사항에 대해 검토하고 all-IP 기반의 개방적 이동통신 환경에서의 보안 구조상 취약점을 분석하였다[1].

정구완외 3인(2003)은 IETF에서 권한관리 기반 구조의 표준으로 제시하고 있는 속성 인증서(Attribute Certificate)를 통해 Diameter 프로토콜에서의 효과적이고 표준화된 권한관리 메커니즘을 제안하고, 관련 Diameter 메시지 등을 정의하고 있다[2].

이덕규, 이임영(2006)은 각 디바이스의 접속통신에 맞도록 통신 메니저를 통해, 인증, 인가, 계정관리를 진행하고 서비스 매니저를 통해 서비스를 제공하는 방식의 AAA 기법을 설계하였다[3].

이덕규, 정교일(2007)은 인증과 인가에서 좀 더 효율적인 AAA가 될 수 있도록 사용자의 속성 정보를 제공하여 권한 관리가 가능하도록 하는 속성인증서 기술과 속성 인증서 발급, 저장, 유통으로 인가를 제공하는 메커니즘을 제안하고 있다[4].

T. LAKSHMIBAI 외 2인(2014)은 TACACS+ 서버가 원격 기반 서비스를 위한 사용자 인증 및 권한 부여, 계정 관련 서비스를 제공하고 있고 네트워크 및 피어 투 피어 통신망에서 알려지지 않은 사용자 및 공격자 정보를 식별하므로, 이전의 보안 지향 인증 방식에 비해 보다 효율적인 중앙 집중식 보안을 제공하고 있음을 분석하고 있다[5].

이들 논문은 AAA가 적용된 라우터와 서버 기반 네트워크의 보안구조, 권한관리 등을 분석한 후, 효율성, 메카니즘 등을 다양하게 제시하고 있지만, 학생들이 실습을 통해 구현하기에는 한계가 있으므로 제한적이지만 실습을 통해 구현 및 검증 가능한 AAA 구축방안을 제시하고자 한다.

2.2 선행연구

네트워크상에 연결되어 있는 각종 장비들의 계정(사용자의 아이디와 암호)을 각각 설정하여 인증하는 것은 매우 단순하면서도 번거로운 작업이다.

이러한 문제를 해결하기 위해서 라우터와 스위치의 인증을 AAA 서버를 통해 받도록 설정하고, AAA 서버에서 만들어진 계정은 별도의 설정 없이 라우터와 스위치에 바로 적용되어 관리가 용이해진다[6].

AAA 보안 프로토콜은 표 1 및 그림 1과 같이 크게 두 종류로 분류된다.

표 1. RADIUS와 TACACS+
Table 1. RADIUS vs. TACACS+

AAA Protocol	RADIUS	TACACS+
Authentication	User	Equipment
Protocol	UDP	TCP
Encryption	Password only	Entire body
Authentication Authorization	perform together	perform separately
Standard	open/IETF, Cisco	Cisco

RADIUS : UDP, Cisco - 1645, 1646 port, standard/IETF - 1812, 1813 port
TACACS+ : TCP 49 port

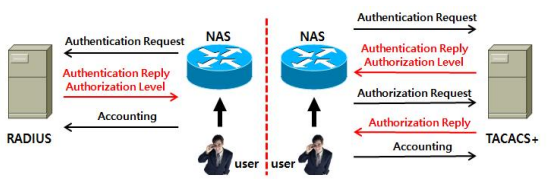


그림 1. RADIUS와 TACACS+
Fig. 1 RADIUS vs. TACACS+

2.2.1 RADIUS

RADIUS(: Remote Authentication Dial-In User Services)는 Dial-Up 네트워크 상에서 서버나 장비에 접속 시 보안을 위한 계정 및 권한 등에 대해 AAA 서버에서 중앙 관리하고자 하는 사용자 인증 프로토콜로 UDP 프로토콜 프레임을 사용하며, Client와 Server가 존재한다.

NAS 장비를 통해 인증과 인가를 하게 되며, TACACS+에 비해 CPU 부하, 메모리 사용량이 적으며, 대형부터 소형까지 모든 네트워크에 사용된다.

2.2.2 TACACS+

TACACS+(: Terminal Access Controller Access Control System +)는 트래픽 손실이 적은 TCP 프로토콜 프레임을 사용하며, RADIUS의 fail over, 오류처리 등의 단점을 극복하고 패킷 전체를 암호화하여 전송하는 보안이 강화된 새로운 정보보호 프레임워크로서 역시 Client와 Server가 존재한다.

네트워크 장비의 경우 일반 사용자 인증과 다르게 한 번의 인증과 여러 번의 권한 부여가 필요한데, AAA 구조가 개별화 되어 있어, 인증과 인가가 별도의 작업으로 가능하여 RADIUS 프로토콜에 비해 효율적이므로, 대규모 네트워크에서 라우터나 스위치의 인증을 일원화하기 위해 인증 서버로 사용한다.

III. 본 론

본 논문에서는 RADIUS와 TACACS+를 공통 적용할 수 있는 토폴로지에 기반 한 가상 망을 구현하고 해당 AAA를 구현하기 위해서, 그림 2와 같이 라우터와 RADIUS와 TACACS+ 서버를 설정한 후, ping, telnet 접속 등 시뮬레이션을 실시하여 검증하였다.

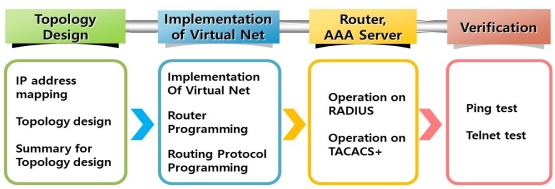


그림 2. RADIUS와 TACACS+의 검증 사례
Fig. 2 Verification cases of RADIUS & TACACS+

3.1 토폴로지 설계

RADIUS와 TACACS+의 검증 사례를 검토하기 위해, 그림 3과 같이 공통으로 적용할 수 있는 토폴로지를 200.100.1.0, 200.100.2.0, 200.100.10.0의 C 클래스 3개, 10.0.0.0의 A 클래스 1개로 설계하였다. 오른쪽 음영 부분은 시나리오-2 검증 시 추가되는 부분이다.

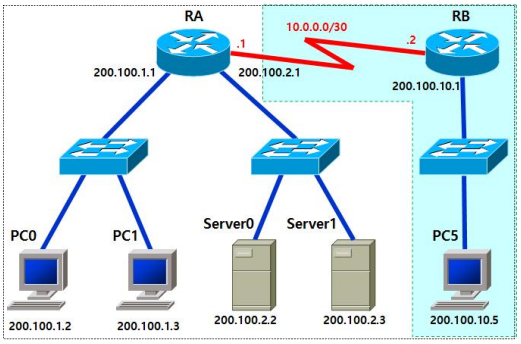
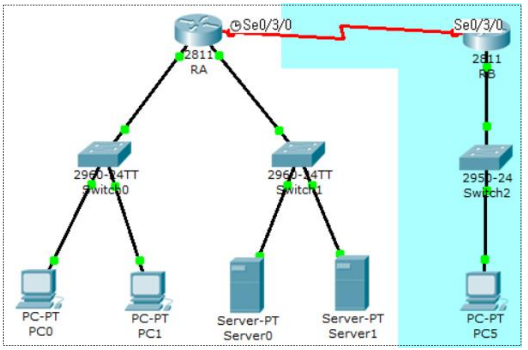


그림 3. 토폴로지 설계
Fig. 3 Topology design

3.2 공통 가상 망 구성

RADIUS와 TACACS+을 검증하기 위하여, 그림 3과 같은 토폴로지를 기반으로 그림 4와 같은 가상 망을 구현하였다[7-9].



IP/suffix	port	Equip.	IP/suffix	port	Equip.
200.100.1.1 /24	fa0/0	RA	200.100.1.3 /24		PC1
200.100.2.1 /24	fa0/1	RA	200.100.2.2 /24		Server0
200.100.1.2 /24		PC0	200.100.2.3 /24		Server1
10.0.0.1 /30	s0/3/0	RA	200.100.10.1 /24	fa0/0	RB
10.0.0.2 /30	s0/3/0	RB	200.100.10.5 /24		PC5

그림 4. 공통 가상 망 구현
Fig. 4 Implementation of common virtual networks

특히, 제안하고자 하는 네트워크는 서버가 1개인 경우 라우터에서 TACACS+ 원격 사용자 인증을 설정하고 검증한 후, TACACS+ 설정을 지운 다음 RADIUS를 설정하여 검증하거나 그 역으로 검증하면 번거롭고 오류의 가능성이 있으므로, RADIUS 서버와 TACACS+ 서버를 별도로 두었다.

3.3 시뮬레이션 결과

3.3.1 시나리오-1

시나리오-1은 RADIUS와 TACACS+ 서버를 on/off 할 수 있도록 서버를 2개로 구성한 후, 라우터의 스크립트를 설정하였다.

그림 5와 같이 Server0와 Server1을 각각 RADIUS 서버와 TACACS+ 서버로 설정하되, RADIUS 서버는 off, TACACS+ 서버는 on으로 설정하였다.

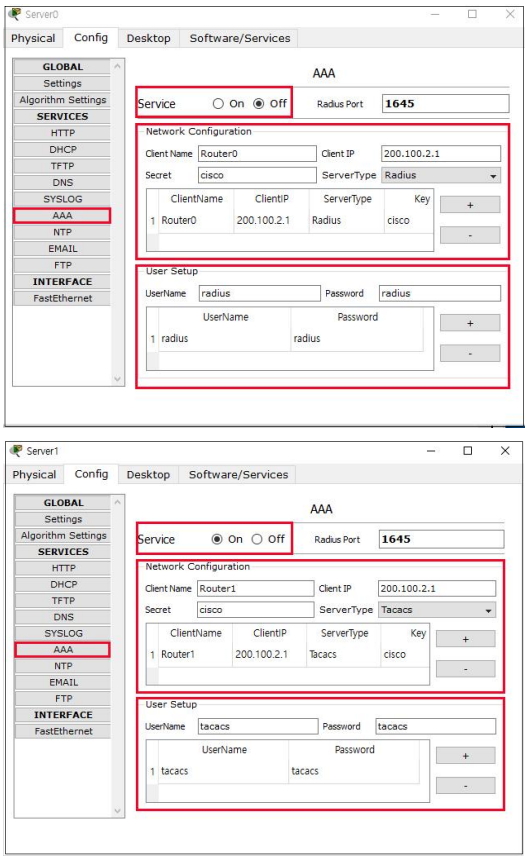


그림 5. RADIUS와 TACACS+ 서버 설정
Fig. 5 The server setting of RADIUS & TACACS+

다음으로, 라우터의 원격 인증을 AAA 서버를 통해 받도록 설정하기 위해서 라우터의 [CLI] 탭을 클릭하여 그림 6과 같이 IOS 명령을 입력하였다.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RA
RA(config)#aaa new-mode
RA(config)#aaa authentication login default
        group radius group tacacs+ local
RA(config)#enable secret aaa

RA(config)#radius-server host 200.100.2.2 key cisco
RA(config)#tacacs-server host 200.100.2.3 key cisco

RA(config)#line vty 0 4
RA(config-line)#login authentication default
RA(config-line)#transport input telnet
RA(config-line)#exit
RA(config)#
```

그림 6. 라우터의 AAA 설정 스크립트
Fig. 6 AAA setting script in the router

여기서, “aaa new model”은 aaa 서버 시작을 의미하고, “aaa authentication login default group radius group tacacs+ local”은 RADIUS와 TACACS+ 인증을 거쳐 설정한 사용자 이름과 암호로 접속한다는 의미하며, Server0와 Server1을 각각 RADIUS 서버와 TACACS+ 서버로 설정하면서 주소와 키 값을 설정하였다. 또한 “line vty 0 4”는 텔넷접속을 5명(0,1,2,3,4)으로 지정하고 “login authentication default”는 텔넷으로 접속 시 위의 정책을 적용하여 사용자 명과 암호를 입력하도록 했다.

이때, RADIUS 서버는 off, TACACS+ 서버는 on으로 하고 PC0에서 AAA Router에 ping test 후 telnet 접속을 시도하면 그림 7과 같이 TACACS+ 서버만 접속이 가능하며, 역으로는 RADIUS 서버만 접속이 가능함을 검증하였다.

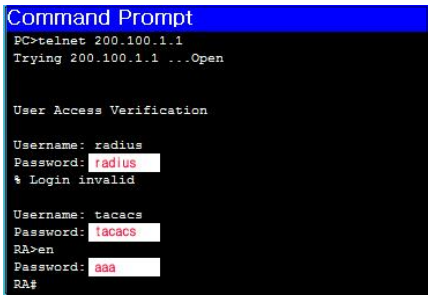


그림 7. 인증을 통한 접속 화면
Fig. 7 Access to the network screen through authentication

3.3.2 시나리오-2

시나리오-2는 시나리오-1의 네트워크에 라우터 RB가 추가된 네트워크로서, RADIUS와 TACACS+ 서버를 구성한 후 라우터와 AAA 서버를 설정하였다.

그림 8과 같이 기 설정된 Server0와 Server1에 PC5에서 텔넷이 가능하도록 Network Configuration에 RB를 추가하고 User Setup의 계정을 “tacacs2”로 각각 설정하였다. 이때 기존 라우터 RA의 User Setup의 계정은 “tacacs1”으로 각각 변경하였다.

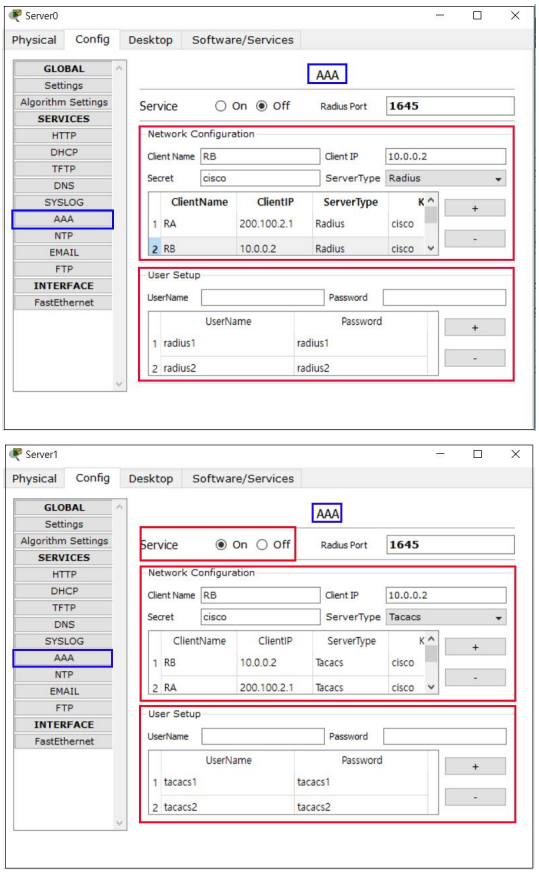


그림 8. RB 추가에 따른 각 서버 설정
Fig. 8 Setting change in each server after RA addition

다음으로, 라우터 RB의 원격 인증을 AAA 서버를 통해 받도록 설정하기 위해서 라우터 RB를 선택한 후 [CLI] 탭을 클릭하여 그림 9와 같이 IOS 명령을 입력하였다.

```
RB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RB(config)#
RB(config)#line vty 0 4
RB(config-line)#login authentication default
RB(config-line)#transport input telnet
RB(config-line)#radius-server host 200.100.2.2 key cisco
RB(config)#line vty 0 4
RB(config-line)#login authentication default
RB(config-line)#taca3s-server host 200.100.2.2 key cisco
RB(config-line)#tacacs-server host 200.100.2.2 key cisco
RB(config)#aaa new-model
RB(config)#aaa authentication login default group radius group tacacs+
RB(config)#enable secret aaa

User Access Verification

Username: tacacs2
Password:
RB>en
Password:
RB#
```

그림 9. 라우터 RB의 AAA 설정 스크립트
Fig. 9 AAA Setting script in the router RB

여기서, RADIUS 서버는 off, TACACS+ 서버는 on으로 하고 PC5에서 PC0까지 ping test 후, AAA Router에 telnet 접속을 시도하면 그림 10과 같이 TACACS+ 서버만 접속이 가능하며, 역으로는 RADIUS 서버만 접속이 가능함을 검증하였다.

그림 10. 인증을 통한 접속 화면
Fig. 10 Access to the network screen through authentication

Ⅳ. 결 론

본 논문에서는 컴퓨터 네트워크 교과목에서 다루고 있는 AAA가 설정된 라우터와 서버 기반의 네트워크 관련하여 토폴로지에 기반 한 공통 가상 망을 구현한 다음 RADIUS와 TACACS+를 각각 라우터와 서버에 적용한 후, 시뮬레이션을 통해서 AAA가 적용된 라우터와 서버 기반 네트워크의 인증에 대한 효율적인 검증사례를 제시하였다.

제시된 구현 사례 중 시나리오-1은 2개의 호스트와 1개의 라우터 및 2개의 Server를 갖는 2개의 네트워크로 구성한 토폴로지를 기반으로 하고, 시나리오-2는 1개의 호스트와 1개의 라우터가 추가 구성된 4개의 네트워크로 구성한 토폴로지를 기반으로 하며, 이후 패킷 트레이서 시뮬레이터를 활용하여 공통 가상 망을 구현한 후, 라우터와 서버에 RADIUS와 TACACS+를 설정하였다.

시뮬레이션 결과, RADIUS 서버와 TACACS+ 서버를 on/off 하면서 PC0, PC1과 PC5에서 AAA Router에 telnet 접속을 시도하여 공통 가상 망이 인증에 대해 정상적으로 동작함을 확인하였다.

따라서, 구현 사례는 토폴로지 상에서 기존 이론 중심의 AAA를 검토한 후 대부분의 수업에서 누락된 서버설정과 인증 실습과정을 연계하여 AAA를 쉽게 이해할 수 있으므로 우수한 학습 결과가 기대된다.

향후, 제시된 AAA가 설정된 라우터와 서버를 갖는 네트워크에 관한 구현 사례를 실제 수업에 적용하여 문제점을 도출하고 취약점을 보완해야 하며, 평가 도구를 개발하고 분석하여 제시된 각 사례의 네트워크 효율성 평가를 검증하는 등의 보다 다양한 분야를 비교 및 분석하는 연구가 필요하다.

Reference

[1] S. Ji, K. Han, and S. Park, “An Implementation of AAA for Next Generation Mobile Communications,” *Symp. of the Korean Institute of Communications and Information Sciences*, July 2002, pp. 1962-1965.

[2] G. Jung, J. Song, H. Ryu, and H. Kim, "A study on Attribute Certificate Based AAA Protocol,” *Conf. of Korean Institute of Information Scientists and Engineers*, Seoul, Korea, vol. 30, no. 2, Oct. 2003, pp. 739-741.

[3] D. Lee and I. Lee, "An AAA Design for Roaming on Ubiquitous Network,” *J. of Security Engineering*, vol. 3, no. 1, Feb. 2006, pp. 55-61.

[4] D. Lee and K. Jeong, "A Study on Efficient AAA Using Attribute Certification,” *J. of Security Engineering*, vol. 4, no. 1, Feb. 2007, pp. 41-57.

[5] T. Lakshmibai, B. Chandrasekaran, and C. Parthasarathy, "A Survey of Different Networks for Traffic Flow Control,” *J. of Int. Academic Research for Multidisciplinary*, vol. 2, no. 5, June 2014, pp. 765-775.

[6] I. Yoon and J. Kim, *Complete Conquest for Packet Tracer,* Seoul: Kyung-Hee University Press, Jun., 2013.

[7] J. Jang and N. Kim, “The case study for Implementation and verification of Network based on VLSM,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 11, Dec. 2014, pp. 1267-1276.

[8] N. Kim, “The case study for Implementation and verification of Dynamic NAT and PAT,” *J. of the Korea Institute of Electronic Communication Science*s, vol. 10, no. 10, Oct. 2015, pp. 1131-1137.

[9] N. Kim, “The case study to verify of a network based on router applying an ACL(: Access List),” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 5, May 2016, pp. 491-498.

저자 소개

박성배(Sung-Bae Park)

1994년 단국대 영어영문과(문학사)
2001년 University of Central Missouri 졸업(영문학석사)
2006년 Southern Illinois University Carbondale (교육학 박사)
2014～현재 : 경동대학교 간호학부 교수
※ 관심분야 : 영어교육

김노환(No-Whan Kim)

1978년 숭실대학교 전자공학과 졸업(공학사)
1983년 연세대학교 산업대학원 전자전공 졸업(공학석사)
2002년 강원대학교 대학원 전자공학과 졸업(공학박사)
1993～현재 : 경동대학교 간호학부 교수
※ 관심분야 : 컴퓨터네트워크