KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.9 pp.271~282 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.9.271

Implementation and Performance Analysis of Network Access Control Based on 802.1X for Effective Access Control on BYOD

Min Choul Lee† · Jeongho Kim††

ABSTRACT

In the business environment BYOD(Bring Your Own Device) is used and being expanded continuously. According to a survey conducted by Cisco in 2012 on 600 companies, 95% of them are already permitting the use of BYOD in their work environments so that productivity of their employees has improved as a result. Gartner predicted that the use of BYOD will be caused new security threat. They also suggested to introduce NAC(Network Access Control) to resolve this threat, to separate network zone based on importance of their business, to establish the policy to consider user authority and device type, and to enforce the policy. The purpose of this paper is to design and implement the NAC for granular access control based on IEEE(Institute of Electrical and Electronics Engineers) 802.1X and DHCP(Dynamic Host Configuration Protocol) fingerprinting, and to analyze the performance on BYOD environment.

Keywords : BYOD, DHCP, Fingerprint, IEEE 802.1X, Network Access Control

효율적인 BYOD 접근통제를 위한 802.1X 네트워크 접근통제 구현과 성능 해석

이 민 철† · 김 정 호††

요 약

비즈니스 환경에서 BYOD(Bring Your Own Device) 활용은 지속적으로 확대되고 있다. 시스코(Cisco)는 2012년 600개 기업을 대상으로 BYOD 활용에 관한 설문조사를 실시했다. 조사 결과 95%의 기업에서 이미 BYOD 사용을 허용하고 있으며, 업무 생산성이 향상된 것으로 나타났다. 가트너(Gartner)는 BYOD 도입으로 보안위협이 증가할 것으로 예측했으며, 보안위협 완화 방안으로 네트워크 접근통제(Network Access Control, NAC) 도입을 제안했다. 또한 접근통제 중요도에 따라 네트워크 영역을 나누고, 사용자 역할과 단말기 유형을 고려하여 접근통제 정책을 상세히 정의하고, 네트워크에 연결된 모든 단말기에 강제로 적용할 것을 주장했다. 본 논문에서는 IEEE 802.1X와 DHCP 핑거프린팅(fingerprinting)을 응용하여 네트워크 접근통제를 설계·구현하고, BYOD 환경에 적용하여 접근통제 성능을 해석하고자 한다.

키워드 : BYOD, DHCP, Fingerprint, IEEE 802.1X, 네트워크 접근통제

1. 서 론

비즈니스에 활용되는 단말기가 데스크톱, 랩톱 등의 PC 중심에서 BYOD(Bring Your Own Device)로 불리는 스마트폰, 태블릿 등의 스마트 기기로 확대되고 있다. 시스코(Cisco)는 2012년 600개 기업을 대상으로 실시한 설문조사 결과에서 95%의 기업이 기업 내 개인 소유 스마트기기 사용을 허용하고 있으며, 이는 업무 생산성 향상으로 이어졌다고 발표했다[1]. 그러나 기업은 생산성 향상이라는 긍정적 효과와 함께 보안위협 증가라는 새로운 문제에 직면한다[2].

가트너(Gartner)는 BYOD와 관련된 보안위협 경감 방안으로 네트워크 접근통제(NAC, Network Access Control) 도입을 제안한다. 또한 사용자의 역할과 권한, 단말기 유형에 따라 접근 가능한 네트워크 영역을 세분화하고, 영역별 접근통제 정책을 수립하여 강제적으로 적용할 것을 주장한다[3].

BYOD 통제를 위한 다양한 NAC가 출시되었으나, 국내에는 기존 네트워크 변경을 최소화하는 인밴드 또는 아웃오브밴드 방식이 대부분이다[4]. 이러한 NAC는 네트워크를 동적으로 결정하는 802.1X와 달리 이미 결정된 네트워크 위에서

† 준 회 원 : 한밭대학교 컴퓨터공학과 석사과정
†† 종신회원 : 한밭대학교 컴퓨터공학과 교수
Manuscript Received : June 22, 2015
First Revision : August 28, 2015
Accepted : August 31, 2015
* Corresponding Author : Jeongho Kim(jhkim@hanbat.ac.kr)

접근통제를 구현함에 따라 몇 가지 제약을 유발한다. 단말기 프로파일(사용자, IP 주소, 위치 등) 변경 시 접근통제 정책 변경이 필요하고, 단말기의 이동성을 제한하고, 유무선 네트워크에 별도의 접근통제 정책을 적용해야 하며, NAC 운영 중단 시 전체 네트워크의 접근통제 가용성을 해칠 수 있다. 이러한 제약을 해소하려면, BYOD 환경을 고려한 네트워크 분할, 접속 네트워크 동적 결정, 세분화된 접근통제 정책 설계와 적용 등의 개선이 요구된다[3, 5].

802.1X가 적용된 유무선 네트워크는 네트워크 접속을 시도하는 단말기의 사용자를 인증하고, 사용자에게 접근이 허가된 VLAN(Virtual Local Area Network)을 동적으로 할당할 수 있다. 이때 사용자 권한과 단말기 유형을 고려하여 네트워크를 동적으로 할당하려면, 802.1X 인증과 별도로 단말기 식별이 필요하다.

본 논문에서는 IEEE 802.1X PNAC(Port based Network Access Control)와 DHCP 핑거프린팅(fingerprinting)을 응용하여 사용자 역할과 단말기 유형에 따라 VLAN을 할당하고, 접근통제를 수행하는 네트워크 접근통제를 설계·구현한다. 그리고 BYOD 환경에 적용하여 네트워크 접근통제 성능을 해석한다.

이후 논문은 다음과 같이 구성된다. 2절은 접근통제 표준인 IEEE 802.1X와 단말기 식별에 사용되는 DHCP 핑거프린팅에 대해 기술한다. 3절에서는 네트워크 접근통제를 설계하며, 네트워크 구성, 접근통제에 사용되는 데이터베이스 구조, 인증 및 인가 절차, 접근통제 정책 등을 기술한다. 4절에서는 3절의 설계에 기반하여 네트워크 접근통제를 구현한다. 이 과정에서 DHCP 메시지를 이용한 단말기 핑거프린트 수집방법, 인증서버의 로직을 변경하여 사용자 권한과 단말기 유형에 따라 접근대상 네트워크를 결정하는 방법과 네트워크에 따른 접근통제 정책을 구현한다. 5절에서는 4절에서 구현한 접근통제의 성능을 해석한다. 6절에서는 본 논문의 결론과 향후 연구과제에 대해 기술한다.

2. 관련 표준 및 기술

본 절에서는 네트워크 접근통제에 관한 유일한 국제표준인 IEEE 802.1X와 수동적 운영체제(OS) 식별방법인 DHCP 핑거프린팅에 대해 기술한다.

2.1 IEEE 802.1X 포트기반 네트워크 접근통제

IEEE 802.1X는 네트워크 접속을 시도하는 단말기에 대한 인증메커니즘 제공을 목적으로 개발된 포트기반 네트워크 접근통제 표준으로, 포트기반 인증(Port based Authentication)이라고 한다[6].

2.1.1 802.1X 구성요소

802.1X는 Fig. 1과 같이 요청자, 인증자, 인증서버로 구성된다[6].

Fig. 1. Physical Elements of 802.1X

1) 요청자(Supplicant)

802.1X에서 요청자는 두 가지 의미로 사용된다. 첫 번째는 네트워크에 접근하고자 하는 단말기 또는 클라이언트를 의미하고, 두 번째는 단말기에서 인증을 위해 사용되는 클라이언트 소프트웨어를 의미한다[7].

2) 인증자(Authenticator)

인증자는 단말기와 인증서버의 중간에서 인증에 필요한 자격 정보를 전달하는 이더넷 스위치 또는 무선네트워크에

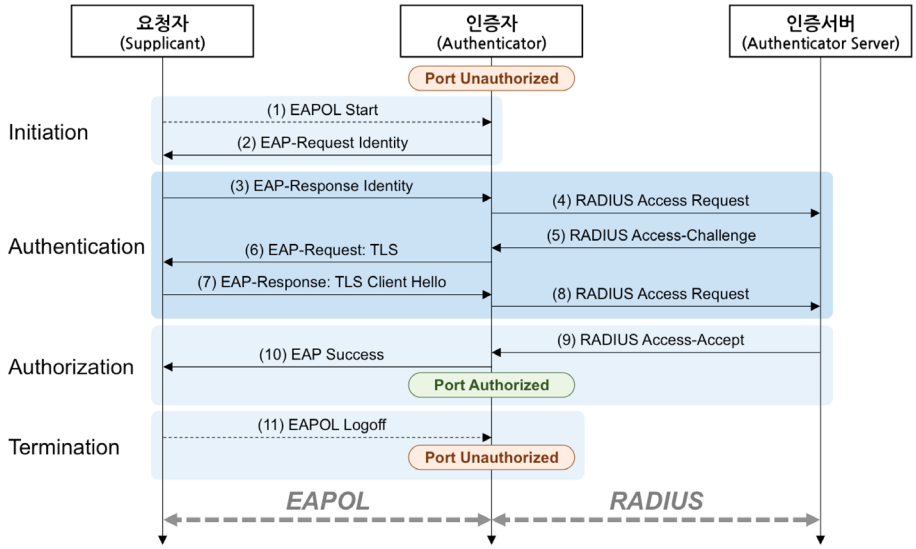

Fig. 2. 802.1X Authentication and Authorization Process[6]

서 사용하는 AP(Access Point) 같은 Layer 2 네트워크 장치를 의미한다[8].

3) 인증서버(Authentication Server)

인증서버는 사용자 인증에 필요한 정보를 저장하며, 요청자가 제공한 자격정보를 검증한다[7]. 또한, 인증자를 제어하는 속성정보(VLAN, ACL 등)를 관리한다. RADIUS(Remote Authentication Dial In User Service), AD(Active Directory) 등을 사용한다.

2.1.2 802.1X 인증절차

802.1X는 스위치의 물리적인 포트를 중심으로 단말기에 대한 인증과 접근대상 네트워크에 대한 인가를 수행한다[6]. Fig. 2는 802.1X에서 수행되는 사용자 인증과 네트워크에 대한 인가 절차를 나타내고 있으며, 802.1X 인증에 사용되는 EAP(Extensible Authentication Protocol), EAPOL(EAP Over Lan), 그리고 RADIUS와 같은 프로토콜을 나타낸다[8].

802.1X가 적용된 네트워크를 통해 다른 장치와 통신하기를 원하는 장치는 인증과 인가 절차를 반드시 거쳐야 한다.

802.1X에서 인증과 인가 절차는 개시(initiation), 인증(authentication), 인가(authorization), 종료(termination)의 4단계로 구분할 수 있다[5]. 개시단계는 인증을 준비하는 단계로, 단말기가 802.1X 인증을 지원하는지 확인하고, 인증에 필요한 정보를 요청한다. 인증단계는 단말기에서 제공된 인증정보를 이용하여 사용자의 자격을 검증한다. 결과에 따라 요청자의 네트워크 접근을 허용하거나 차단한다. 인가는 인증자가 수행하며 두 종류로 구분할 수 있다. 첫 번째는 스위치 포트의 상태를 “미인가”에서 “인가”로 변경하여 네트워크 접근을 허용하는 것이다[9]. 두 번째는 사용자별로 사전에 정의된 속성들을 이용하여 스위치 포트의 동작을 제어하는 것이다[9]. 마지막으로 종료단계는 네트워크 연결을 종료하고 스위치 포트의 상태를 미인가 상태로 변경한다. 연결 종료는 요청자의 명시적 또는 묵시적인 연결 종료 요청에 의해 처리된다.

2.2 DHCP 핑거프린팅

DHCP 핑거프린팅은 수동적(passive) OS 식별법이다. DHCP 클라이언트에서 IP 주소 할당을 요청하는 DHCPREQUEST 메시지에 포함된 독특한 데이터 패턴으로 OS를 식별한다[10]. 이는 NMAP, X-Prove 등의 능동적 방법에 비해 OS 식별이 용이하며, 식별률이 높다. 그리고 클라이언트의 보안정책에 관계없이 OS를 식별 가능한 장점이 있다[11]. 하지만 DHCP 환경에만 적용할 수 있다는 단점이 있다. 본 논문의 네트워크 접근통제는 사용자와 단말기 유형에 따라 접근대상 네트워크를 동적으로 할당하며, IP 주소 할당에 DHCP를 이용한다. 따라서 DHCP 핑거프린팅 기법은 적절한 OS 식별 기법이라 할 수 있다.

2.2.1 DHCP 메시지 구조와 OS 식별

Fig. 3의 DHCP 메시지에서 단말기 OS 식별에 사용하는 항목은 Options 필드이다.

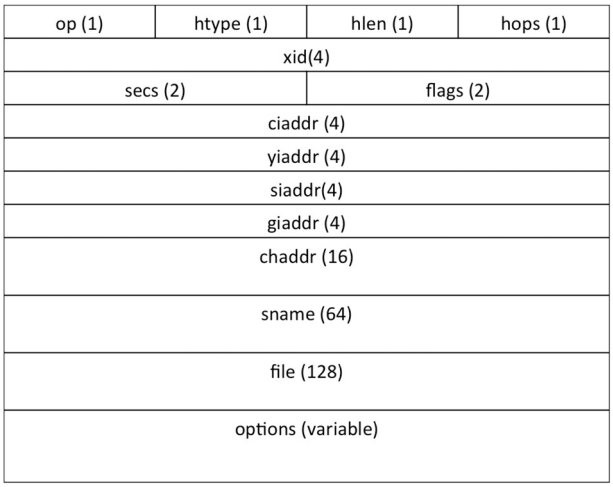

Fig. 3. DHCP Message Structure

Options에 포함된 옵션 중 55(Parameter Request List)와 60(Vendor Class Identifier)에는 OS별로 독특한 정보를 포함하고 있다. 이러한 정보의 차이를 이용하면 단말기에 설치된 OS를 식별할 수 있다.

1) Vendor Class Identifier

Option 60에서는 DHCP 클라이언트의 공급업체와 설정정보를 식별할 수 있다. Table 1과 같이 OS 공급업체의 이름과 버전정보를 포함한다. 다만 Option 60 필드는 선택사항으로 일부 클라이언트는 제공하지 않아 모든 단말기의 OS 식별에는 적합하지 않다.

Table 1. Vendor Class Identifier Value and OS

Data	OS
MSFT 5.0	Windows 2000 / XP
Linux 2.4.18-17.7.x	Linux (Kernel 2.4.18)
Mac OS J1-9.2.2	MacOS 9.2.2

2) Parameter Request List

Fig. 4는 DHCPREQUEST 메시지를 dhcpdump를 통해 해석한 결과이다.

Option 55는 Table 2와 같이 DHCP 클라이언트별로 요청값과 요청값의 순서가 달라 Option 60으로 OS를 특정하기 어려운 경우에도 OS 식별이 가능하다.

```
OPTION:  53 (  1) DHCP message type         3 (DHCPREQUEST)
OPTION:  61 (  7) Client-identifier         01:c8:d7:19:9f:11:bb
OPTION:  12 ( 10) Host name                 Cisco42045
OPTION:  60 ( 12) Vendor class identifier   udhcp 1.15.2
OPTION:  50 (  4) Request IP address        192.168.203.15
OPTION:  54 (  4) Server identifier         192.168.199.1
OPTION:  55 (  8) Parameter Request List      1 (Subnet mask)
                                              3 (Routers)
                                              6 (DNS server)
                                             12 (Host name)
                                             15 (Domainname)
                                             28 (Broadcast address)
                                             42 (NTP servers)
                                            212 (???)
```

Fig. 4. DHCP Option 55 Analysized by dhcpdump

Table 2. Parameter Request List Value and OS

Parameter Request List	OS
01,03,15,06,44,46,47	Windows 95
01,15,03,44,46,47,06	Windows NT 4.0
01,03,06,15,112,113,78,79	MacOS X

2.2.2 핑거뱅크(Fingerbank)

핑거프린트 자체로는 OS식별이 불가능하다. 이 때문에, 핑거프린트별 운영체제 데이터베이스가 필요하다. 핑거뱅크(http://www.fingerbank.org)는 단말기별 핑거프린트와 OS 목록을 ODBL(Open DataBase License) V1.0로 제공한다.

3. 네트워크 접근통제 시스템 설계

본 절에서는 사용자 역할과 단말기 유형에 따른 네트워크 접근통제 구현에 필요한 네트워크 및 데이터베이스 구조, DHCP 핑거프린팅 절차, 사용자별 네트워크 접근 권한 등의 설계에 대하여 기술한다.

3.1 설계의 전제

802.1X에서 인증서버로 사용되는 FreeRadius는 기본적으로 사용자와 네트워크를 1:1로 맵핑 하여 한 사용자에게는 하나의 네트워크(VLAN)를 할당하도록 구현되어있다[12]. 이 때문에 사용자 역할과 단말기 유형에 따른 네트워크 접근통제 구현을 위해서는 조건에 따라 VLAN을 가변적으로 할당할 수 있도록 자료 구조와 VLAN 할당 절차를 변경해야 한다.

Fig. 5는 사용자 역할과 단말기 유형에 따른 네트워크 접근통제 절차를 나타낸다. 단말기가 네트워크 연결을 시도하면, 스위치는 단말기에 802.1X 인증에 필요한 환경설정 여부를 확인한다. 환경설정이 완료되지 않았거나 인증에 실패하면, 캡티브 포털 접속을 유도한다. 이때 DHCP 핑거프린팅을 이용해 단말기 유형을 식별하고, 결과를 데이터베이스에 저장한다.

인증서버는 인증에 성공한 단말기에 사용자 권한과 단말기 유형에 따라 접속이 허용된 VLAN을 할당한다. 만약 해당 단말기에 적절한 접근권한이 부여되지 않았다면, 최소권한 VLAN을 할당한다. 그리고 DHCP 서버는 단말기에 IP 주소를 할당한다. 이후 사전에 정의된 ACL을 통해 네트워크에 대한 접근을 통제한다.

3.2 네트워크 설계

네트워크 설계는 물리적 설계와 논리적 설계로 구분한다. 물리적 설계는 네트워크를 구성하는 물리적 장치들의 배치와 연결 방법 등을 결정하고, 논리적 설계는 물리적 네트워크 기반 위에서 VLAN을 활용하여 네트워크 세그먼트를 설계한다.

3.2.1 물리적 설계

물리적 네트워크는 Fig. 6과 같이 스타 토폴로지를 기반으로 설계하였다.

서버팜(Server Farm)도 업무 특성에 따라 VLAN을 통해 네트워크를 세그먼테이션 하였다[6]. 적용 대상은 350명의 직원이 2,000대가량의 단말기를 사용하는 정부출연 연구소로 하였다.

물리적 네트워크는 백본스위치, 스위치 및 AP, 무선랜제어기(Wireless LAN Controller), Radius 서버, DHCP 서버 등으로 구성되며 각 구성요소는 Table 3의 역할을 수행한다.

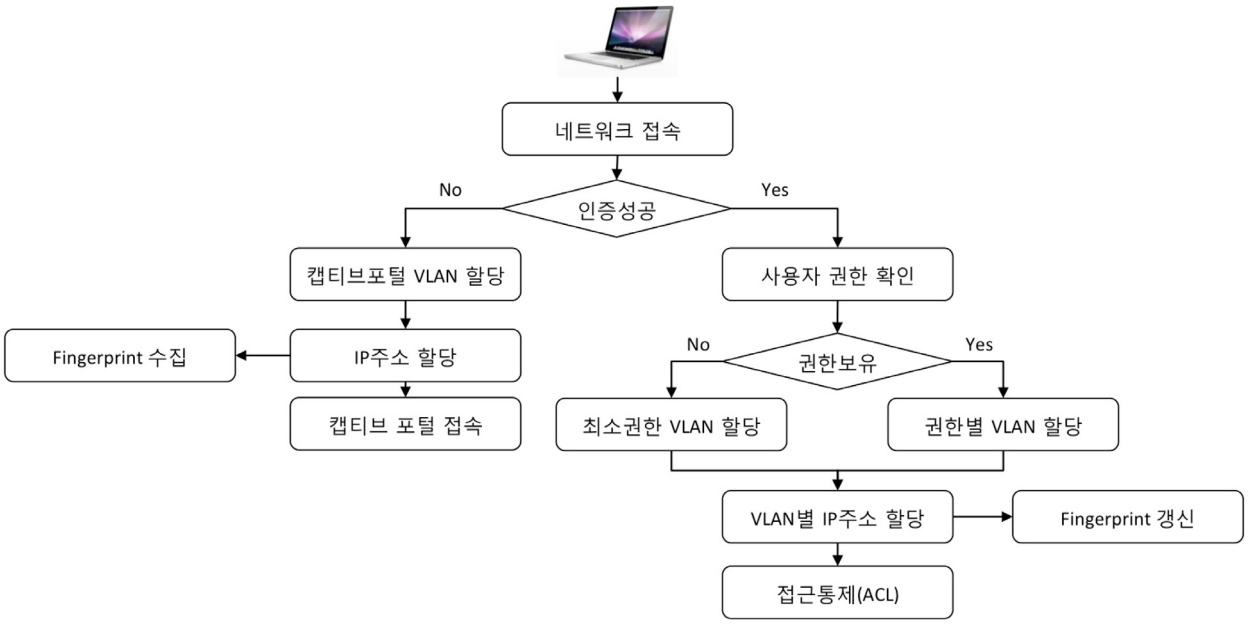

Fig. 5. Network Access Control Process

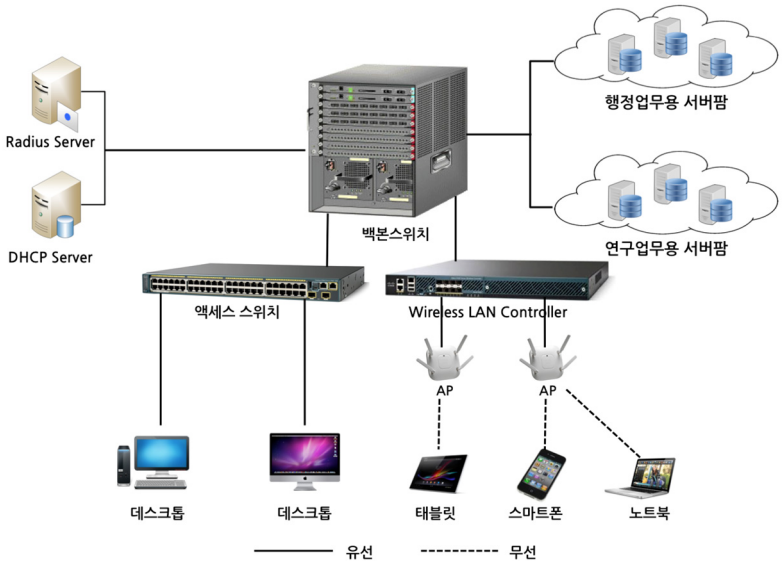

Fig. 6. Conceptual Design of Network

Table 3. Physical Elements and Each Role

구분	내용
백본스위치	- VLAN Aggregator와 게이트웨이 - ACL에 의한 VLAN별 접근통제
무선랜제어기	- AP 통합관리
AP · 스위치	- 802.1X 인증자 역할
Radius 서버	- 802.1X 인증서버 역할(자격정보 검증, 인증자 속성정보 전달)
DHCP 서버	- 서브넷별 IP 주소 할당 - 최초 IP 주소 할당 후, 동일한 IP 주소 할당보장

접근통제의 구현에는 Table 4의 오픈소스 소프트웨어를 사용했다.

Table 4. Opensource Software for Implementing NAC

구분	모델명	제조사
OS	Ubuntu 12.04 LTS	Ubuntu
인증시스템	FreeRadius 2	FreeRadius
DHCP 서버	ISC-DHCP	ISC
DBMS	MySQL 5.5.38	오라클/MySQL
개발언어	PHP 5	PHP

3.2.2 논리적 설계

본 논문에서는 네트워크를 Table 5의 기준에 따라 정적 네트워크와 동적 네트워크로 구분하였다[6].

정적 네트워크는 전통적인 네트워크 구성방식으로 설계와 구현이 용이하다. 그러나 단말기의 이동성이 동일 VLAN으로 제한되며, 단말기 위치가 VLAN을 벗어날 경우 IP 주소와 함께 단말기와 연계된 모든 보안정책도 변경해야 하는 단점이 있다.

동적 네트워크는 연결대상 네트워크를 사전에 결정하지 않고, 조건에 따라 가변적으로 할당하는 네트워크를 의미한다[6]. 이는 전송매체(유무선)에 관계없이 동적인 VLAN 할당과 일관된 접근통제를 가능하게 하고, 경계 없는 단말기 이동성을 보장하게 한다.

Table 5. Compare Static Network with Dynamic Network

구분	정적 네트워크	동적 네트워크
VLAN 설계 기준	공간(건물, 층)	업무, 역할
VLAN 할당 방식	정적/수동/ 인증 전 할당	동적/자동/ 인증 후 할당
IP 주소 할당 방식	정정/동적(DHCP)	동적(DHCP)
전송매체	유무선 분리	유무선 통합
단말기 이동성	동일 VLAN으로 이동성 제한	자유로운 이동성 보장

접근통제에 사용할 VLAN은 동적 네트워크 기준에 따라 사용자의 직위를 기준으로 설계하였다. Table 6은 사용자 직위에 따라 구성된 VLAN 설계를 나타낸다.

동적 네트워크는 서버팜에 대해서도 시스템 특성과 접근

Table 6. VLAN Design for User Network

직위	사용목적	VLAN ID	VLAN 그룹	IP 주소 서브넷
임원	단말허용	110	VLAN_110	172.16.110.0/24
	최소권한	119	VLAN_119	172.16.119.0/24
보직자	단말허용	120	VLAN_120	172.16.120.0/24
	최소권한	129	VLAN_129	172.16.129.0/24
임원	단말허용	130	VLAN_130	172.16.130.0/24
	최소권한	139	VLAN_139	172.16.139.0/24
연수생	단말허용	140	VLAN_140	172.16.140.0/24
	최소권한	149	VLAN_149	172.16.149.0/24

대상을 고려하여 네트워크를 세분화하여 네트워크 단위 접근통제를 구현할 수 있다. Table 7은 운영시스템을 기준으로 구성한 서버팜 VLAN 설계이다.

Table 7. VLAN Design for Server Farm Network

시스템	VLAN ID	VLAN 그룹	IP 주소 서브넷
경영자정보	210	VLAN_210	172.16.210.0/24
기관운영	220	VLAN_220	172.16.220.0/24
위원회	230	VLAN_230	172.16.230.0/24
그룹웨어	240	VLAN_240	172.16.240.0/24

3.3 데이터베이스 설계

동적인 네트워크 할당과 접근통제에 사용되는 사용자 권한, 단말기 핑거프린트, VLAN 등의 관리에 DB를 활용하였고, 테이블은 다음과 같이 설계하였다.

3.3.1 접근권한 정의 테이블 설계

사용자 권한과 단말기 유형별 접근권한 정의를 위해 Table 8과 같이 3개의 테이블을 설계하였다.

Table 8. Table Lists of Access Role Definition

테이블명	저장내용
nac_emp_info	사용자 정보(식별자, 부서, 직위)
nac_access_vlan	권한 레벨별 할당 VLAN
nac_access_allow_device	권한 레벨별 접근 허용 단말기

각 테이블의 상세 설계는 Table 9~Table 11과 같다.

Table 9. nac__emp__info

컬럼명	자료형	의미	기타
emp_id	VARCHAR(20)	직원 ID	주키
emp_name	VARCHAR(40)	성명	
dept_code	VARCHAR(10)	부서코드	
position_code	VARCHAR(10)	직위코드	

Table 10. nac__access__vlan

컬럼명	자료형	의미	기타
position_code	VARCHAR(10)	직위코드	주키
access_level	INT(11)	접근권한레벨	주키
vlan_group	VARCHAR(45)	할당 VLAN	

Table 11. nac__access__allow__device

컬럼명	자료형	의미	기타
access_level	INT(11)	접근권한레벨	주키
os_class_id	INT(11)	OS 그룹	주키

3.3.2 단말기 핑거프린트 저장 테이블

핑거프린트의 저장에는 Table 12와 같이 4개의 테이블을 이용한다. 첫 번째는 단말기의 맥 주소와 핑거프린트를 저장하고, 나머지 3개의 테이블은 핑거뱅크에서 제공하는 핑거프린트 데이터를 저장한다.

Table 12. Table Lists of Fingerprint Management

테이블명	저장내용
nac_device_fingerprint	단말기 핑거프린트 목록
nac_dhcp_os_fingerprint	핑거프린트별 OS 목록
nac_dhcp_os	OS 식별자와 이름 목록
nac_dhcp_os_class	OS 분류그룹과 OS 목록

각 테이블의 상세 설계는 Table 13~Table 16과 같다.

Table 13. nac__device__fingerprint

컬럼명	자료형	의미	기타
macaddr	VARCHAR(20)	맥주소	주키
fingerprint	VARCHAR(200)	핑거프린트	
os_id	INT(11)	OS ID	
os_class_id	INT(11)	OS 그룹	

Table 14. nac__dhcp__os__fingerprint

컬럼명	자료형	의미	기타
os_id	INT(11)	OS ID	주키
fingerprint	VARCHAR(200)	핑거프린트	주키

Table 15. nac__dhcp__os

컬럼명	자료형	의미	기타
os_id	INT(11)	OS ID	주키
os_class_id	INT(11)	OS 그룹	
os_desc	VARCHAR(150)	OS 이름	

Table 16. nac__dhcp__os__class

컬럼명	자료형	의미	기타
class_id	INT(11)	OS 분류	주키
class_desc	VARCHAR(100)	그룹 설명	주키

3.4 단말기 프로파일링

Fig. 7은 네트워크에 처음 연결하는 단말기에 대한 프로파일링 과정을 나타낸다.

네트워크 접속을 시도한 단말기는 802.1X 인증에 필요한 환경설정을 위해 캡티브 포털에 접속한다. 이때 IP 주소를 할당받는 과정에서, Fig. 7의 A와 같이 단말기의 맥 주소와 핑거프린트를 획득하여 DB에 등록한다. 이후 단말기는 Fig. 7의 2에서 802.1X 인증을 수행하고, Fig. 7의 B와 같이 단말

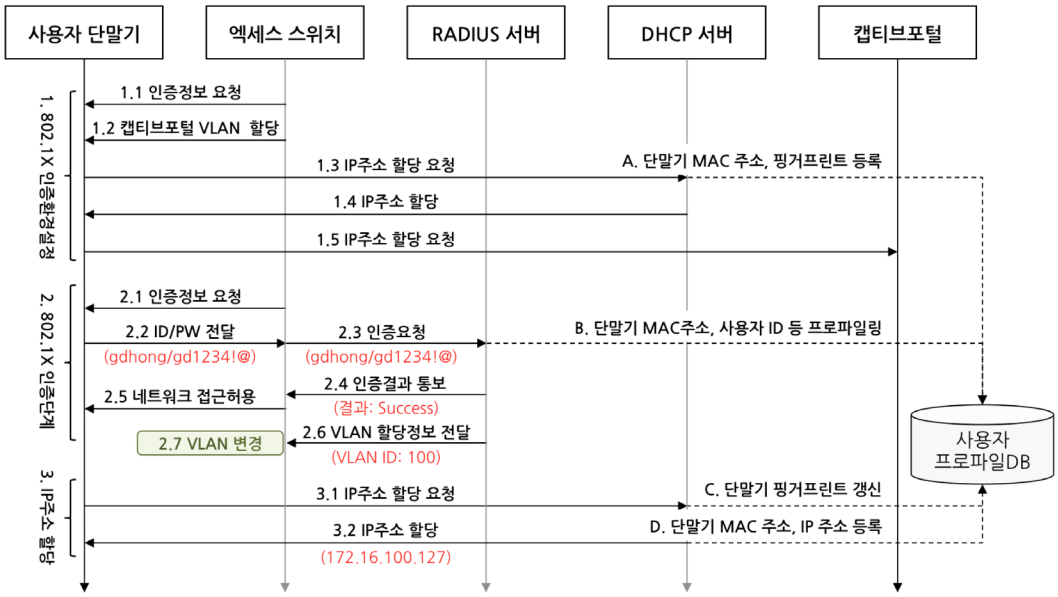

Fig. 7. User and Device Profiling Process

기의 맥 주소와 사용자 식별자를 추출하여 DB에 등록한다.

인증이 완료된 단말기는 네트워크 접속을 위해 IP 주소를 할당받는다. 이때 단말기의 핑거프린트를 Fig. 7의 C처럼 갱신한다. 그리고 Fig. 7의 D와 같이 단말기에 할당된 IP 주소를 DB에 등록한다.

프로파일링은 로그기반과 패킷기반으로 구분할 수 있다. 로그기반은 인증과 관련된 시스템로그 분석을 통해 단말기와 관련된 정보 획득 방법으로 Fig. 7의 B와 D가 이에 해당한다. 반면 패킷기반은 단말기에서 송신하는 TCP/IP 패킷을 분석하여 단말기 정보를 획득하는 방법으로 Fig. 7의 A와 C가 이에 해당된다.

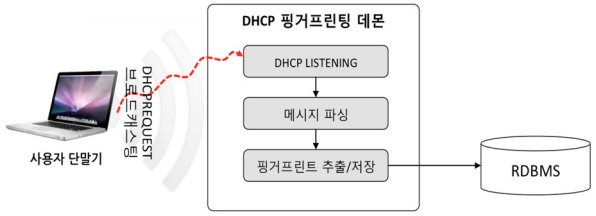

Fig. 8. Conceptual Diagram of DHCP Fingerprinting

본 논문의 로그기반 프로파일링에는 FreeRadius 인증로그와 DHCP 로그를 사용하였다[6]. 패킷기반 프로파일링을 위해서 DHCP 핑거프린팅을 구현하고자 한다. DHCP 핑거프린팅은 Fig. 8의 절차로 수행된다.

핑거프린팅 데몬은 DHCPREQUEST 메시지 수신을 위해 UDP 67번 포트(port)를 리스닝한다. Fig. 7의 "1. 802.1X 인증환경 설정" 또는 "3. IP 주소 할당" 과정에서 데몬이 단말기가 발송하는 DHCPREQUEST 메시지를 수신하면, 데몬은 메시지를 파싱하고 Option 55 파라미터의 값을 추출하여 DB에 저장한다.

3.5 사용자 권한과 접근통제 정책 설계

사용자 역할과 단말기 유형에 따라 네트워크 접근을 통제하려면 사용자와 단말기 유형에 따른 접근 권한을 정의하고 권한별 접근통제 정책을 설계해야 한다.

3.5.1 권한별 접근권한 정의

접근권한 정의를 위해 Table 17과 같이 사용자의 직위를 정의했다. 그리고 권한레벨에 따라 사용을 허가할 단말기(OS) 목록을 Table 18과 같이 정의하였다.

Table 17. User Grade

직위명	직위코드	비고
임원	G100	연구소장, 감사
보직자	G200	부장, 과장
직원	G300	임원/보직자를 제외한 직원
연수생	G400	석/박사 과정에 있는 학생

Table 18. Define Allow OS to Authority Level

권한레벨	접근허용 OS 분류 그룹
100	Windows, OS-X, Smartphones/PDAs/Tablets
200	Windows, OS-X
300	Windows, Linux
400	Windows

Table 19는 직위에 따라 할당할 권한레벨과 VLAN 그룹을 정의한다. 예를 들어 보직자는 권한레벨 "200"을 할당받아 "Windows, OS-X" 등의 단말기를 사용할 때 VLAN 120을 할당받는다.

그러나 권한레벨에서 허용하는 단말기 이외의 단말기를

사용할 때는 인터넷 연결만 가능한 최소권한 VLAN 129를 할당받는다.

Table 19. Assign Authority Level to User Grade

직위	직위코드	권한레벨	VLAN 그룹	비고
임원	G100	100	VLAN_110	
		미정의	VLAN_119	최소권한
보직자	G200	200	VLAN_120	
		미정의	VLAN_129	최소권한
직원	G300	300	VLAN_130	
		미정의	VLAN_139	최소권한
연수생	G400	400	VLAN_140	
		미정의	VLAN_149	최소권한

3.5.2 접근통제 정책

접근통제 정책은 다음 두 원칙에 따라 설계하였다. 첫째, IP 주소 중심이 아닌 VLAN 중심으로 네트워크와 시스템에 대한 접근을 통제한다. 둘째, VLAN 간의 접속은 배타적으로 차단한다.

Table 20. Access Control Matrix Between VLAN

출발지 \ 목적지			서버팜			
			210	220	230	240
사용자	임원	110	허용	허용	허용	허용
		119	차단	차단	차단	허용
	보직자	120	차단	허용	허용	허용
		129	차단	차단	차단	허용
	직원	130	차단	허용	차단	허용
		139	차단	차단	차단	허용
	연수생	140	차단	차단	차단	허용
		149	차단	차단	차단	차단

Table 20의 매트릭스는 사용자 네트워크에서 서버팜 네트워크로 시도하는 네트워크 접근통제 정책으로, IP 주소 기반이 아닌 네트워크 기반으로 설계하였다. VLAN을 기반으로 네트워크 중심의 접근통제를 설계함으로써, 사용자 환경 변화와 네트워크 접근통제의 운영 중단 시에도 일관된 접근통제가 가능하다.

4. 네트워크 접근통제 시스템 구현

본 절에서는 3절의 설계에 따른 네트워크 접근통제 시스템의 구현 방법과 적용 결과의 해석을 기술한다.

4.1 네트워크 접근통제 시스템 구현

본 논문의 네트워크 접근통제는 802.1X에 핑거프린트 추출을 위한 핑거데몬을 추가하고, 인증서버의 네트워크 할당 프로세스를 변경하고, 백본스위치에 접근통제 정책을 적용하는 절차로 구현하였다.

4.1.1 DHCP 핑거프린트 추출 프로그램

핑거데몬(finger daemon)은 두 단계에 의해 핑거프린트를 추출하고 OS를 식별한다. 첫 번째 단계에서는 DHCPREQUEST 메시지에서 핑거프린트를 추출한다. 두 번째 단계에서는 추출한 핑거프린트를 핑거뱅크 데이터와 비교하여 OS의 종류와 분류를 식별한다.

핑거프린트 추출에 사용되는 DHCPREQUEST 메시지의 옵션필드의 구조는 Fig. 9와 같다. 옵션필드는 매직코드, 옵션, 종료코드로 구분하며, 옵션필드의 처음과 마지막에는 매직코드와 종료코드가 위치한다. 매직코드는 옵션필드의 서두에 위치하는 4바이트의 고정된 값(99, 130, 83, 99)이다. 종료코드는 옵션필드의 끝을 알리는 값으로 255가 기록된다. 종료코드 이후의 옵션값은 무시된다. 중간에 위치하는 각 옵션들은 옵션코드(1바이트), 옵션길이(1바이트), 옵션데이터(n바이트)로 구성되며, 옵션 하나의 전체 크기는 옵션데이터의 크기에 2바이트를 더한 값과 일치한다.

Fig. 10은 DHCPREQUST 메시지에서 핑거프린트를 추출하는 절차이다. 핑거데몬이 UDP 67번 포트로 DHCPREQUEST 메시지를 수신(1)하면, 메시지에서 옵션필드 패킷을 추출(2)한다. 다음으로 인덱스변수 n을 이용하여 옵션코드가 55인지 확인(3)한다. 옵션코드가 55가 아니라면, 다음 옵션코드를 읽어들이기 위해 n값을 증가(4)시킨다. 옵션코드가 55라면, 옵션코드 뒤에 따라오는 옵션데이터에서 핑거프린트를 추출(6)하고, 데이터베이스에 저장(7)한다.

핑거프린트 저장이 완료되면, 데이터베이스는 트리거에 등록된 관계 대수 연산 R_1과 R_2를 실행하여 운영체제와 운영체제 그룹 식별자를 확인하여 등록한다.

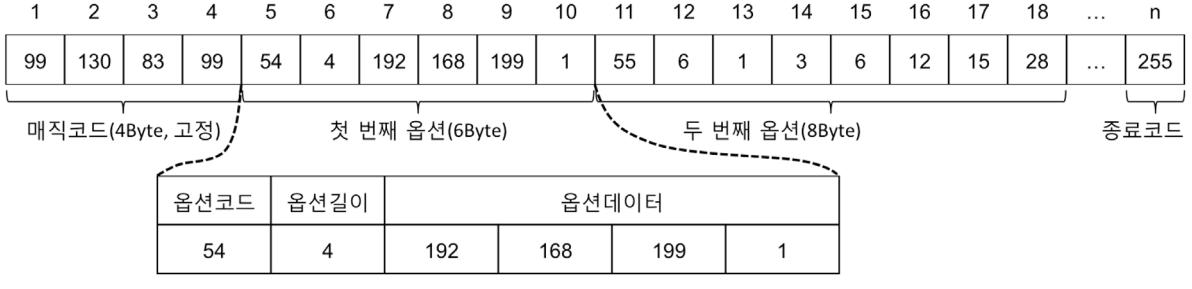

Fig. 9. DHCP Option Fields Structure

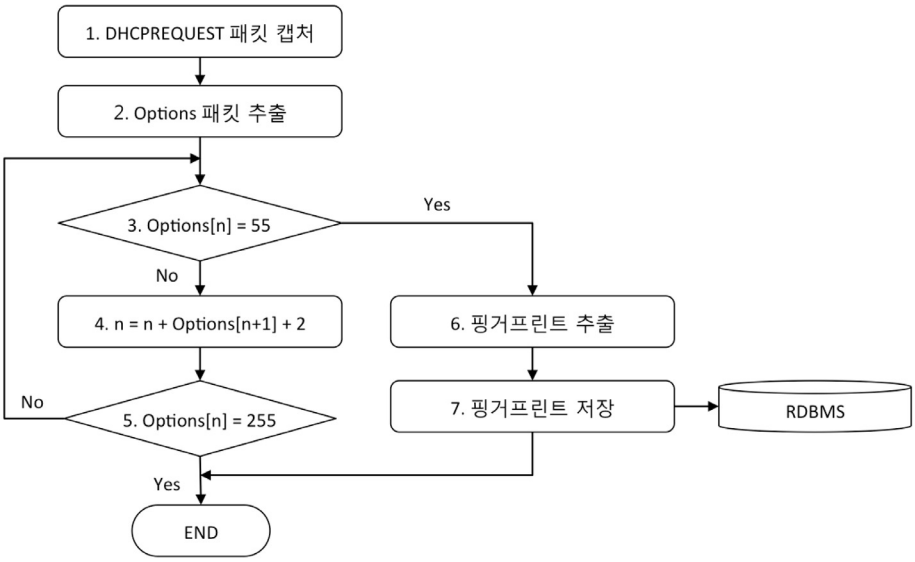

Fig. 10. DHCP Fingerprint Extraction Process

[관계 대수 연산 R_1과 R_2]

$R_1 \leftarrow F_{MIN\ OS\_ID}(\sigma_{FINGERPRINT='핑거프린트'}$
$(NAC\_DHCP\_OS\_FINGERPRINT))$

$R_2 \leftarrow F_{MIN\ CLASS\_ID}(NAC\_DHCP\_OS \triangleright\triangleleft_{OS\_ID=OS\_ID} R_1)$

Fig. 11은 핑거데몬이 수집한 핑거프린트이다.

4.1.2 네트워크(VLAN) 할당 프로세스 변경

본 논문에서 인증서버로 사용하는 FreeRadius는 인증이 완료된 사용자에게 하나의 VLAN만 할당하도록 구현되어있다. 이를 조건(사용자 권한, 단말기 유형 등)에 따라 VLAN을 가변적으로 할당하도록 하려면, 인증서버의 VLAN 할당 절차를 변경해야 한다.

Fig. 12는 인증서버의 기본적인 VLAN 할당 절차로, 사용자 식별자에 할당된 groupname을 선택(2)하고, groupname이 지정하는 AVP(Attribute Value Pairs) 정보를 선택(3)하여 사용자 단말기가 연결된 스위치 포트 또는 AP의 Association에 할당(4)한다.

사용자 권한과 단말기 유형에 따라 VLAN을 가변적으로 할당하기 위하여 Fig. 12에서 groupname을 선택하는 절차(2)를 Fig. 13으로 변경하였다.

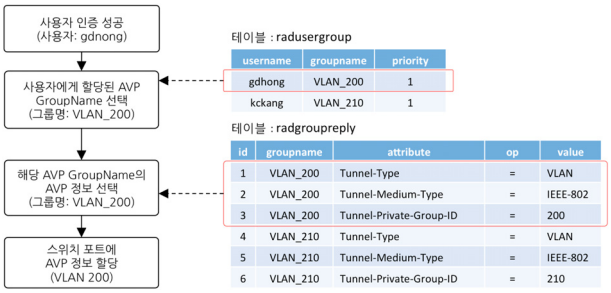

Fig. 12. VLAN Assign Process in FreeRadius[6]

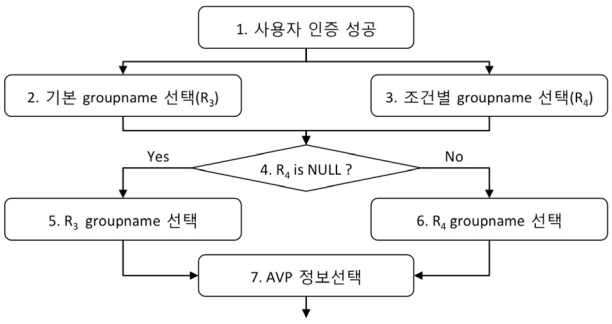

Fig. 13. Dynamic Groupname Selection Process by Condition

macaddr	fingerprint	os_id	os_class_id	detect_date	update_date
00:01:36:35:61:94	1,3,6,12,15,28,44	402	4	2014-09-05 13:45:13	2014-09-20 13:48:09
00:01:8e:b8:36:1a	1,3,6,15,119,95,252,44,46	202	2	2014-09-03 17:07:41	2014-09-22 09:14:51
00:08:9b:c0:49:92	1,3,6,12,15,17,23,28,29,31,33,40,41,42	504	5	2014-09-06 13:36:08	2014-09-17 14:16:01
00:08:9f:da:b1:97	1,15,3,6,44,46,47,31,33,121,249,43,252	107	1	2014-09-04 13:52:49	2014-09-18 00:20:20
00:08:ca:ae:a5:07	1,15,3,6,44,46,47,31,33,121,249,43,252	107	1	2014-09-02 08:39:53	2014-09-23 18:05:10
00:0b:ab:7f:6f:42	1,15,3,6,44,46,47,31,33,121,249,43,252	107	1	2014-09-12 09:50:50	2014-09-12 10:06:55
00:0e:35:4e:95:37	1,15,3,6,44,46,47,31,33,121,249,43,252	107	1	2014-09-02 09:49:48	2014-09-23 17:52:47
00:0f:e4:90:62:d2	1,3,6,12,15,28,33,51,58,59,119,121	1105	11	2014-09-02 08:59:10	2014-09-23 13:48:58
00:11:85:19:15:72	1,3,44,6,7,12,15,22,54,58,59,69,18,144	800	8	2014-09-02 15:09:30	2014-09-17 15:58:38

Fig. 11. Fingerprint List from Finger Daemon

사용자 인증이 완료되면, Fig. 13의 2와 3에서 관계 대수 연산 R_3과 R_4를 실행하여, groupname 두 개를 선택한다. R_3의 groupname은 Fig. 12의 2와 동일한 방법으로 결정되며, 사용자에게 최소 접근권한을 부여하기 위해 사용된다. R_4의 groupname은 사용자 권한과 단말기 유형에 따른 접근권한 부여에 사용되며, groupname 결정에는 앞서 설계한 사용자 권한과 핑거프린트가 이용된다. R_3와 R_4 중에서 선택의 우선순위를 R_4가 갖고 있다. R_4가 NULL이 아니면, 항상 R_4가 선택되고, R_4가 NULL이라면 R_3가 선택된다.

[관계 대수 연산 R_3]

$R_3 \leftarrow \pi_{GROUPNAME}(\tau_{PRIORITY}(\sigma_{USERNAME='사용자\ 식별자'}(radusergroup)))$

[관계 대수 연산 R_4]

$A \leftarrow nac\_access\_vlan$

$B \leftarrow nac\_access\_allow\_device$

$C \leftarrow \sigma_{MACADDR='단말기\ 맥주소'}(nac\_device\_fingerprint)$

$D \leftarrow \sigma_{EMP\_ID='사용자\ 식별자'}(nac\_emp\_info)$

$SubQuery \leftarrow {}_{F\ MIN\ ACCESS\_LEVEL}(A \triangleright\triangleleft_{POSITION\_CODE=POSITION\_CODE} D)$

$V_0 \leftarrow \pi_{ACCESS\_LEVEL}(B \triangleright\triangleleft_{OS\_CLASS\_ID=OS\_CLASS\_ID} C)$

$V_0 \leftarrow \pi_{ACCESS\_LEVEL}(V_0 \triangleright\triangleleft_{ACCESS\_LEVEL=ACCESS\_LEVEL} SubQuery)$

$V_0 \leftarrow \pi_{POSITION\_CODE,\ VLAN\_GROUP}(A \triangleright\triangleleft_{ACCESS\_LEVEL=ACCESSL\_LEVEL} V_0)$

$R_4 \leftarrow \pi_{VLAN\_GROUP}(V_0 \triangleright\triangleleft_{POSITION\_CODE=POSITION\_CODE} D)$

4.1.3 접근통제 정책 적용

네트워크 접근통제 정책의 구현과 적용은 백본스위치에서 제공하는 Named ACL을 이용한다. (Fig. 14)는 사용자 네트워크와 서버팜 VLAN간에 수행되는 ACL을 이용한 접근통제를 나타낸다.

서버팜 VLAN은 사용자의 불필요한 접근을 차단하고, 허용된 서비스에 대한 접근만을 허용한다. (Fig. 14)의 서버팜 VLAN 220은 접근이 허용된 사용자 VLAN에 대하여 HTTP (80)과 HTTPS(443)과 같이 제한된 서비스에 대한 접근만 허용할 수 있다.

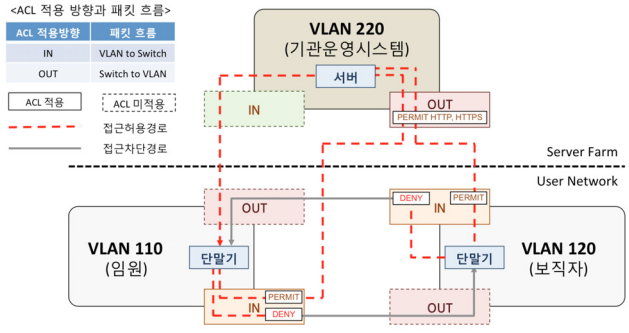

Fig. 14. Access Control Diagram by ACL

사용자 VLAN은 상호 간 접근을 배타적으로 차단하며, 서버팜에 대한 접근도 부여된 권한에 따라 접근을 허용하거나 차단한다. 이러한 양방향 접근통제는 어느 한쪽의 정책에 문제가 발생해도 접근통제의 가용성을 보장할 수 있게 한다.

5. 네트워크 접근통제 적용 결과에 대한 해석

본 논문에서 구현한 네트워크 접근통제는 사용자 역할과 단말기 유형에 따라 네트워크·시스템에 대한 접근통제, 단말기 이동성 보장뿐 아니라, 정보보안에 미치는 다음 세 가지 긍정적 해석을 도출할 수 있었다.

5.1 유무선 네트워크 접근 단말기 투명성 강화

가트너는 기업들이 자사 네트워크에 연결된 단말기 중에서 오직 80%에 대해서만 인식한다고 추정했다[3]. 20%의 투명하지 않은 단말기 사용은 기업정보의 비정상적인 유통을 유발하고, 중대한 보안사고로 이어질 수 있다. 이를 개선하기 위해서는 Table 21과 같이 네트워크 접근 투명성 확보에 필요한 요소를 정의하고, 이에 대한 지속적인 변경관리가 요구된다.

Table 21. Network Access Visibility Elements

구분	획득 방법
사용자 ID	인증로그 및 Radius 어카운팅 분석
단말기 Mac 주소	인증로그 및 Radius 어카운팅 분석, DHCP 핑거프린팅
단말기 제조사	단말기 맥주소의 OUI 검색
IP 주소	DHCP 로그 및 ARP 분석
단말기 OS	DHCP 핑거프린팅
단말기 위치	Radius 어카운팅 정보
사용시간	Radius 어카운팅, SNMP Trap 정보

802.1X 방식이 아닌 NAC와 자산관리 시스템에서도 Table 21에서 제시하는 요소들을 획득할 수 있지만, 단말기에 별도의 에이전트를 설치하거나, 사용자가 직접 정보를 등록해야 하는 문제점이 있다.

본 논문에서 구현한 네트워크 접근통제를 적용한 결과 Table 22와 같이 단말기 식별률을 95% 이상으로 향상시킬 수 있었다.

Table 22. Device Identification Ratio according to the Access Control

기관	탐지 단말 수	식별 단말 수	식별비율
A	2,386	2,310	96.8%
B	2,570	2,508	97.6%

국내에서 운영 중인 802.1X가 적용되지 않은 네트워크에서는 Fig. 15와 같이 유무선 네트워크에 따라 상이한 연결과정과 인증을 진행한다.

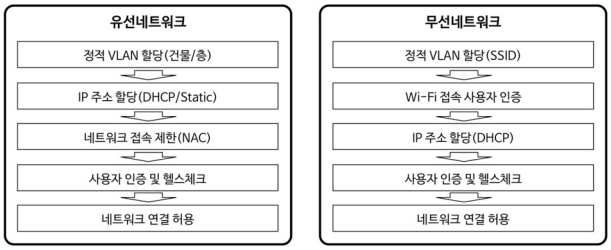

Fig. 15. Differences of Connecting and Authentication Process Between Wired and Wireless Network

이로 인해 네트워크 유형에 따른 별도의 사용자 인증과 프로파일링을 요구하며, 일부 장치(프린터, IP-CCTV 등)는 인증과 프로파일링이 어렵거나 불가능하다. 그러나 본 논문에서는 802.1X와 DHCP를 네트워크에 적용하여 네트워크 유형에 관계없이 Fig. 16과 같은 일원화된 네트워크 연결과 인증 절차를 구현하였다. 이 때문에 네트워크에 접속하는 모든 단말기는 네트워크 접속 이전에 반드시 사용자 인증과 네트워크 할당, IP 주소 할당 절차를 거치게 되고, 각 과정에서 단말기 및 운영체제 유형에 관계없이 Table 21의 항목에 대한 프로파일링을 수행하여 단말기 식별률을 향상시킬 수 있었다. 이는 기업 비즈니스에 사용되는 모든 단말기 현황을 투명하게 관리할 수 있음을 의미하고, 이를 통해 정보의 흐름을 투명하게 유지하며, 정보보안사고 발생 시 단말기의 추적성을 향상시킴을 의미한다.

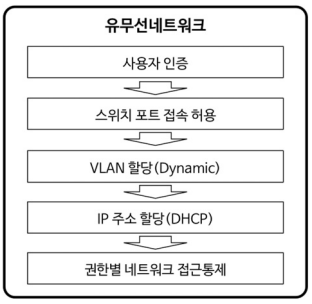

Fig. 16. Simplified Process

5.2 네트워크 접근통제 성능 향상

국내에서 도입된 인밴드 또는 아웃오브 밴드 방식의 NAC는 802.1X와 달리 사전에 결정된 네트워크 환경에서 운영된다. 이 때문에 Fig. 15와 같이 네트워크 유형에 따라 각각 네트워크 접근통제를 구축해야 하며, 네트워크 연결 이후 통제를 수행한다. 또한, 네트워크가 이미 결정된 상태이기 때문에, 사용자의 역할과 권한에 의한 접근통제가 아닌, IP・MAC 주소와 단말기 유형 등에 의한 통제를 수행할 수밖에 없다. 이 때문에 접근통제 정책의 복잡성이 증가하고, 다음과 같은 접근통제 예외 대상 장치와 접근통제 우회 기법이 안정적인 접근통제의 걸림돌로 작용한다.

- 프린터, IP-CCTV, 지문인식 단말기 등 인증에 필요한 UI(User Interface)를 제공하지 않는 장치 예외처리
- 접근통제를 위해 사용하는 ARP 스푸핑, IP 스푸핑 기법에 대한 우회
- 인증대상 단말기의 IP 주소와 MAC 주소를 인증받은 단말기 또는 예외처리된 단말기의 주소로 변조
- 에이전트 설치 유무에 따른 접근통제 성능 편차가 발생하며, 모든 운영체제에 에이전트 설치 불가

그리고 접근통제 정책이 사용자에 종속되어 사용자의 역할이 변경되면 해당 사용자가 사용하는 단말기와 관련된 모든 접근통제 정책 변경을 유발한다.

본 논문의 네트워크 접근통제는 Fig. 16과 같이 네트워크 접속유형과 단말기 유형에 관계없이 단일한 절차에 따라 모든 단말기에 대해 예외 없는 접근통제를 수행한다. 그리고 사용자 역할과 권한, 단말기 유형, 네트워크 세그먼트를 중심으로 접근통제 정책을 구성하여, 앞서 언급한 접근통제 우회를 방지한다. 또한, 접근통제 정책이 사용자에 종속되지 않도록 사용자의 역할에 할당하여 사용자의 역할이 변경되어도 접근통제 정책 변경을 최소화한다. 이는 기존 네트워크 접근통제와 비교하여 유무선 네트워크 접근통제 절차 통합 및 간소화, 접근통제 우회 차단, 접근통제 정책의 항구성 유지 등의 관점에서 접근통제 성능이 향상됨을 의미한다.

5.3 네트워크를 통한 악성코드 확산 범위 최소화

정적 VLAN 기반의 엔터프라이즈 네트워크 환경에서는 악성코드 유입에 따른 확산 범위를 전체 네트워크로 간주할 수 있다. 이는 네트워크 설계 시 건물 또는 층에 따라 네트워크를 구분하고, 각 네트워크 세그먼트 간의 접근을 통제하지 않기 때문이다. 이 때문에 지능형지속공격(APT, Advanced Persistent Threat) 또는 제로데이공격(Zero-day Attack) 같은 고도화된 공격의 경우 보안시스템 유무에 관계없이 전체 네트워크로 공격 범위가 확대된다.

본 논문에서 구현한 접근통제는 조직의 업무 특성에 따라 VLAN을 활용하여 네트워크 세그먼트를 구분하고, 사용자 권한과 단말기 유형에 따라 네트워크 접근을 통제한다. 이 때문에 악성코드 유입에 따른 확산과 공격 범위를 단말기가 소속된 네트워크 세그먼트로 최소화할 수 있었다. 이는 기업 네트워크 환경에서 네트워크 세그먼테이션 범위의 조정과 세그먼트 간 접근통제만으로도 악성코드 유입에 의한 피해 범위를 단일 네트워크 세그먼트로 최소화할 수 있음을 의미한다.

6. 결 론

비즈니스 수행에 BYOD 도입이 확대되면서 기업 내 IT 환경에 보안위협이 증가하고 있다. 가트너는 이에 대한 대응으로 NAC를 도입하고, 세분화된 접근통제 정책에 따라 접근 가능한 네트워크 영역을 나누고, 접근통제 정책을 강제로 적용할 것을 주장하였다.

본 논문에서는 IEEE 802.1X와 DHCP 핑거프린팅을 응용하여 BYOD의 효과적인 통제를 위한 네트워크 접근통제를 설계・구현하고 성능을 해석하였다.

세분화된 접근통제 정책은 권한레벨을 통해 정의했다. 각 권한레벨은 사용을 허가할 단말기와 권한별로 할당할 VLAN

을 지정한다. 권한레벨은 사용자의 직위에 할당되고, 직위별로 접근통제 정책을 정의한다.

단말기가 네트워크 연결을 시도하면 인증서버는 사용자별 권한레벨에 따라 접속을 허용할 네트워크를 결정하고, 스위치 포트(또는 AP와 단말의 연계)에 할당한다. 이때 단말기는 DHCP 핑거프린팅으로 식별하고, 사용자 인증과 네트워크 할당은 802.1X이 수행한다. 권한레벨에 따른 네트워크와 서버팜에 대한 접근은 백본스위치에 정의된 접근통제 리스트가 통제한다.

이러한 접근통제는 유무선 네트워크에 관계없이 사용자의 역할과 단말기 유형으로 접속 네트워크를 동적으로 결정하고, 일관된 접근통제와 단말기의 이동성 보장이 가능했다. 또한, IP 주소가 아닌 네트워크 단위의 접근통제로 네트워크를 통한 악성코드 확산과 유포를 최소화할 수 있었다. 그리고 사용자와 단말기 프로파일링을 통해 95% 이상의 단말기를 식별할 수 있었다.

BYOD의 보다 효과적인 관리 및 통제를 위해서는 MDM (Mobile Device Management), MAM(Mobile Application Management) 등의 솔루션과 연계한 네트워크 접근통제에 관한 후속 연구가 필요하다.

References

[1] Eun Byol Koh, Joohyung Oh, and Chaete Im, "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment," *IMECS 2014*, Vol.II, pp.634-639, 2014.

[2] Prashant Kumar Gajar, Arnab Ghosh, and Shashikant Rai, "Bring Your Own Ddevice (BYOD): Security Risks And Mitigating Strategies," *JGRCS*, Vol.4, No.4, pp.62-70, 2013.

[3] Lawrence Orans and John Pescatore, "Strategic Road Map for Network Access Control," Gartner, 2011.

[4] 이정우 et al, "네트워크접근통제(NAC) 기술동향 파악 및 시험방법론 개발 최종 연구보고서", 한국정보통신기술협회, 2012.

[5] ForeScout, "CounterACT: 802.1X and Network Access Control," [Internet], http://www.forescout.com/wp-content/media/FS- 8021X_and_NAC_Tech_Note.pdf.

[6] 이민철, "네트워크 접근통제 시스템 구축", 에이콘출판, 2015.

[7] Broadford Networks, "802.1X and NAC: Best Practices For Effective Network Access Control," Broadford Networks [Internet], http://www.cadinc.com/wp-content/uploads/2010/11/CAD_ Bradford_Network_Access_Control_802.1X.pdf.

[8] Jim Geier, "Implementing 802.1x Security Solutions for Wired and Wireless Networks," Wiley Publishing, Inc., 2008.

[9] Edwin Lyle Brown, "802.1X Port-Based Authentication," Auerbach Publications, 2006.

[10] Shin Shirahata, Yasuo Tsuchimoto, and Jun Murai, "New scheme for passive OS fingerprinting using DHCP message," *IPSJ SIG Notes*, Vol.18, pp.41-46, 2003.

[11] David LaPorte and Eric Kollmann, Using DHCP for Passive OS Identification, Black Hat Japan 2007, [Internet], http://chatteronthewire.org/download/bh-japan-laporte-kollmann-v8.ppt.

[12] Drik van der Walt, "FreeRadius Beginner's Guide," Packt Publishing, 2011.

이 민 철

e-mail : way.of.cross@gmail.com
2004년 한밭대학교 컴퓨터공학과(학사)
2004년~2014년 극지연구소 선임기술원
2014년~현 재 한밭대학교 컴퓨터공학과 석사과정
관심분야 : 정보보안, 네트워크 접근통제

김 정 호

e-mail : jhkim@hanbat.ac.kr
1980년 경북대학교 전자공학(공학사)
1983년 경북대학교 전자공학(공학석사)
1994년 단국대학교 컴퓨터공학과 (공학박사)
1983년~1996년 한국전자통신연구소 책임연구원, 실장
1989년 정보처리기술사
1990년 공업계측제어기술사
1991년 정보통신기술사
1996년~현 재 한밭대학교 컴퓨터공학과 교수
관심분야 : 네트워크와 데이터통신, 정보보호