Diameter Server 를 위한 관리시스템의 설계 및 구현

함영환, 정병호, 정교일
한국전자통신연구원 정보보호연구본부
e-mail : yhham@etri.re.kr

The Design and Implementation of Diameter Server Management System

Young-Hwan Ham, Byung-Ho Chung, Kyo-Il Chung
Information Security Research Division,
Electronics and Telecommunications Research Institute

요 약

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 이와 같은 무선랜환경에서 안전하게 사용자를 인증하고 서비스를 제공하기 위한 AAA 프로토콜로 Diameter Protocol 표준이 정의되었다. 이와 같은 Diameter base Protocol 표준의 관리를 위한 MIB 구조가 Diameter Base MIB 에 정의되어 있다. 본 논문에서는 무선단말 사용자를 인증시켜 주고 무선랜서비스를 허가해주는 Diameter Server 를 관리하기 위한 관리 시스템을 위의 MIB 을 기준으로 해서 설계하고 구현하였다

1. 서론

최근에 공공장소에서의 보다 안정적이고 고속의 무선 인터넷 접속에 대한 욕구가 커지면서 무선랜에 대한 수요가 많아지고 있고, 유무선 사업자들은 무선랜 시장을 선점하기 위해서 서비스를 서두르고 있다. 그리고 AP(Access Point)장비와 무선랜 단말사이의 안전한 인증과 서비스를 위하여 802.1x 표준이 정의되었다[1]. 802.1x 는 wireless lan 단말이 AP(Access Point)장비에 접속하여 서비스를 받고자 할 때 필요한 인증에 대한 방법을 제공한다.

802.1x 는 EAP(Extensible Authentication Protocol)만을 지원하고 인증기능을 수행하는 인증서버를 필요로 하고 여기서는 인증서버로써 Diameter 서버를 사용하는 것을 가정한다. EAP 프로토콜은 사용자의 인증을 위해서 MD5, TLS, SRP(Secure Remote Protocol)와 같은 다양한 인증메카니즘을 사용할 수 있게 한다[2][3][4][5][6]. 또한 인증서버(authentication server)를 EAP 서버와 분리시킬 수 있도록 함으로써, 보다 유연하고 확장가능한 시스템을 구축할 수 있다.이와 같은 Diameter Base Protocol 표준의 관리를 위한 MIB 구조가 Diameter Base MIB 에 정의되어 있다. Diameter Base MIB 은 크게 Host Configuration, Host Statistics, Peer Configuration, Peer Statistics, Realm Configuration, Realm Statistics 의 6 개의 테이블로 구성되어 있다[1][9].

본 논문에서는 무선단말 사용자를 인증시켜 주고 무선랜서비스를 허가해주는 authentication server 를 관리하기 위한 시스템을 위의 Diameter MIB 들을 기준으로 해서 설계하고 구현하였다.

2. Diameter Server 관리시스템의 설계

2.1 시스템의 구성요소

무선랜환경에서는 IEEE 802.1x 표준을 이용하여 인

증을 받기 위해서는 Supplicant(wireless terminal), AP 그리고 Authentication Server 가 필요하다. Authentication 서버로는 Radius 서버나 보다 확장되고 개선된 표준인 Diameter 서버를 이용하는 것을 가정하여 Diameter Server 를 Authentication Server 로 이용하는 것으로 가정한다[7][8].

802.1x 를 지원하는 AP 는 EAP 를 이용하여 authentication server 에게 인증을 요청하는데, 이때 AP 는 Supplicant 의 EAP 패킷을 받아 이것은 Diameter 패킷으로 Encapsulaton 한 다음 Diameter 서버에게 전달하는 역할을 한다. 반대로 Diameter server 의 응답메시지를 Decapsulation 한 다음 EAP 패킷을 Supplicant 에게 전달하는 역할을 수행한다.

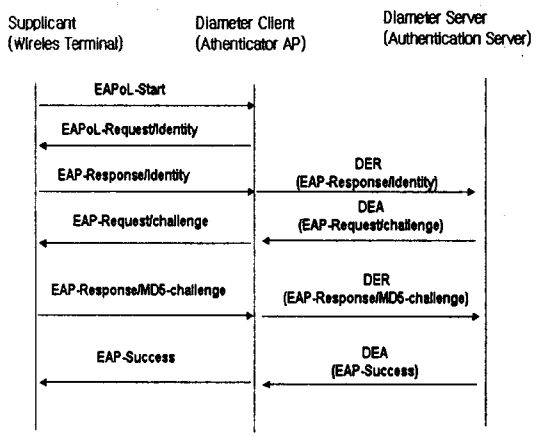

그림 1. 시스템의 구성요소

Diameter 서버 Supplicant 의 인증 기능을 수행하는 모듈이 들어가고, 또한 이를 관리하기 위한 MIB 변수 관리모듈 그리고 SNMP 프로토콜을 위한 SNMP Agent 모듈이 같은 시스템안에 들어가야 한다. 세가지 모듈을 동시에 하나의 프로세스로 설계하면 프로세스가 복잡해질 뿐만 아니라 개발 및 유지보수가 어렵기 때문에 SNMP Agent 모듈, Diameter 인증모듈과 MIB 관리모듈 을 각각 하나의 프로세스로 만들고 이를 IPC 를 이용하여 인터페이스하는 구조로 설계되었다.

2.2 프로세스간의 인터페이스

한 시스템내에서 프로세스간 통신(Inter Process Communication)을 하는 방법에는 Pipe, FIFO, Message Queue, Shared Memory 등의 방법이 있다. 이중에서 대용량에 대한 정보를 교환할 때 주로 사용되는 것이 shared memory 이다. 이 방법은 자료전달을 하고자 하는 프로세스끼리 같은 memory 에 접근하도록 하는데, 직접 메모리를 공유하므로 가장빠른 IPC 수단을 제공한다. 여기에서는 SNMP Agent 모듈과 AP 관리 모듈과의 인터페이스를 위해서 Shared Memory 를 사용하였다. 또한 한 프로세스가 Shared Memory 를 읽거나 쓸 때 다른 프로세스가 읽거나 쓰지 못하도록 보장하기 위해 Semaphore 를 사용했다.

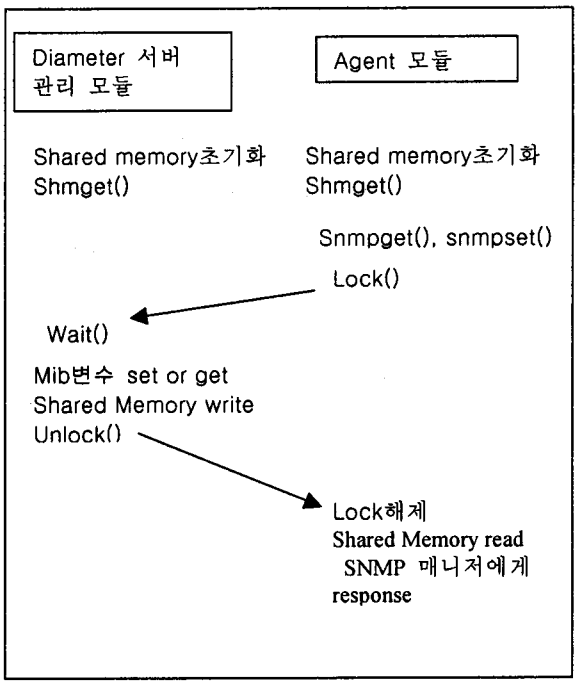

그림 2. Agent 모듈과 Diameter 서버 관리모듈과의 인터페이스

정의된 자료구조를 접근하기 위해서 자료구조를 임계영역으로 두고 두 프로세스가 임계영역 접근시마다 Lock()과 Unlock()을 반복하게 되는데, 우선권을 Agent 모듈에게 주어 명령의 시작은 Agent 모듈에서 시작하도록 한다. AP 관리 모듈은 임계영역에 대한 접근을 위해 세마포어 값이 0 이 되기를 기다린다(wait()). 세마포어 값이 0 이 되면, AP 관리 모듈은 임계 영역에 접근하고 Unlock 을 수행하여 Agent 모듈이 임계 영역에 접근하도록 허용한다. 위와 같은 구조로 SNMP 매니저의 Snmpget()이나 snmpset()명령이 Agent 모듈에 의해서 수행될 때, 정의된 자료구조를 임계영역이 되도록 보장함과 동시에 순차적인 자료구조 접근을 가능하도록 한다.

2.3 Diameter Base MIB 의 구성

Diameter Base MIB 은 크게 Host Configuration, Host Statistics, Peer Configuration, Peer Statistics, Realm

Configuration, Realm Statistics 의 6 개의 테이블로 구성되어 있는데, 크게는 설정에 관련된 MIB 변수(Configuration 관련 변수)와 통계 및 진단관련 MIB 변수로 구분할 수 있다. Configuration 관련 변수들은 Diameter 프로토콜 표준과 관련하여 서버에 관련된 설정환경을 나타내는 MIB 변수들의 집합이고 Host Configuration, Peer Configuration, Realm Configuration 등이 있다. Statistics 관리 관점에서의 관련 테이블은 Host Statistics, Peer Statistics, Realm Statistics 등의 테이블이 있다.

3. Diameter Server 관리 시스템의 구현

3.1 Diameter Server 관리 모듈

AP 관리 모듈은 AP 의 Authenticator 프로세스중의 하나의 모듈로서, 실제로는 하나의 쓰레드로 동작하면서 SNMP 에이전트의 get 또는 set 요청을 기다린다. AP 관리 모듈은 세마포어를 이용하여 에이전트를 명령을 기다리다가 에이전트의 명령이 발생하면, 인터페이스를 위한 공유메모리 구조체에 정의된 각각의 변수(mib 변수이름, 포트 번호, 플래그, 명령값)를 읽어들인다. 여기에서 플래그를 보고 이 명령이 snmpget 인지 snmpset 명령인지를 구분하고 이에 따라 해당 포트의 해당 mib 변수에 명령값을 "set"하거나 "read"한 다음 다시 명령을 기다리는 상태가 된다. 여기서 편의상 AP 관리 모듈의 함수이름 "SNMPMetaAgent()"로 정의하였고 이것을 pseudo code 로 나타내보면 아래의 그림과 같다.

```
/*   SNMPMetaAgent Pseudo Code */
int SNMPMetaAgent(void)
{
/* SNMP agent 에서 metaAgent 에게 요청시 사용 */
  struct sembuf lock = { 0, -1, SEM_UNDO } ;

/* SNMP metaAgent 에서 agent 의 요청을 기다림 */
  struct sembuf waiting = { 0,   0, SEM_UNDO } ;


/* SNMP metaAgent 가 agent 의 요청을 수행한 후 agent
에게 알릴 때 사용 */
  struct sembuf unlock = { 0,   1, SEM_UNDO } ;

  semid = semget(KEY, 1, SFLG) ;
  semctl( semaphore 값을 1 로 초기화) ;
  while(;;)
  {
    semop(semid, &waiting, 1) ;
    if(IPC_read(mib_var_name, port_no, flag, real_value))
    switch(falg) {
      case 0 :
        read the MIB_vars from IPC_read(real_value);
        get the real_value from global_vars;
        IPC_write(real_value);
        semop(semid, &unlock, 1);

        break;
      case 1 :
        read the MIB_vars from IPC_read(real_value);
        assign_fsmvar();
        IPC_write(real_value.success);
        semop(semid, &unlock, 1);
        break;
    }
}
```

그림 3. Diameter 서버 관리모듈의 Pseudo Code

3.2 매니저와 에이전트

매니저의 사용자 인터페이스는 자바기반으로 구현한다. 따라서 자바를 지원하는 모든 시스템에서 운영체제에 무관하게 운용될 수 있다. Java Web Start 는 Applet 처럼 웹 기반 어플리케이션이 가지는 장점들을 모두 가지며 Stand Alone Application 의 장점을 동시에 제공하는 자바 실행 프레임워크로 초기에 한번 전체 구성요소를 다운로드하고 서버에서 Java Web Start Application 을 구성하는 구성요소가 변경되면, 자동으로 다운로드하여 클라이언트에 설치한다. Servlet 을 통하여 SNMP Agent 의 MIB 변수를 GET 또는 SET 하기 때문에 클라이언트는 SNMP 와 관련없이 개발이 가능하다.

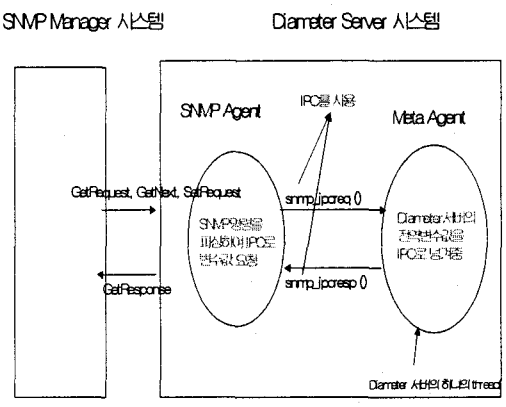

그림 4. Diameter 서버 관리 매니저와 에이전트

관리시스템의 자바 인터페이스를 위한 웹 서버는 Apache Tomcat 4.0 을 사용하여 개발됐다. SNMP Agent

와의 통신은 자바 기반 SNMP 라이브러리(Westhawk's Java SNMP stack)을 사용하여 개발됐다. 기본적으로 UCD-SNMP 는 MIB II 를 제공하며 추가적인 MIB 을 제공하기 위해서는 확장된 MIB 을 관리하는 Sub Agent 를 별도로 작성하여 UCD-SNMP Master Agent 와 상호 작용하도록 한다. Master Agent 와 Sub Agent 간의 상호작용은 Shared Library 형태 또는 각각 별도의 프로세스로 작동하고 AgentX 라는 프로토콜을 사용하여 상호 통신하는 방법이 있다. 본 논문에서는 보다 안정적인 구현을 위해 Shared Library 형태로 Agent 을 구현하였다. 동일 Diameter 서버 플랫폼에 Agent 프로세스가 구현되어있고 또한 관리모듈은 Authenticattion Server 프로세스안의 하나의 모듈(정확히는 하나의 Thread)로서 Agent 프로세스와 IPC 를 통해 통신하도록 구현되어있다.

4. 결론

AP 장비와 무선랜 단말사이의 안전한 인증과 서비스를 위하여 802.1x 표준이 정의되었다. 802.1x 는 wireless lan 단말이 AP 장비에 접속하여 서비스를 받고자 할 때 필요한 인증에 대한 방법을 제공한다. 이와 같은 이와 같은 무선랜환경에서 안전하게 사용자를 인증하고 서비스를 제공하기 위한 AAA 프로토콜로 Diameter Protocol 표준이 정의되었다. Diameter Base MIB 은 크게 Host Configuration, Host Statistics, Peer Configuration, Peer Statistics, Realm Configuration, Realm Statistics 의 6 개의 테이블로 구성되어 있다
본 논문에서는 위의 Diameter 서버를 Authentication Server 기능을 수행하는 관리객체로서 보고 이를 관리하기 위한 시스템을 위의 MIB 테이블들을 기준으로 해서 설계하고 구현하였다. 구현된 시스템을 통하여 관리자는 802.1x 기반의 인증을 수행하는 AuthenticationServer 의 중요한 관리변수를 설정하거나 읽을 수 있고 통계,진단, 에러 정보등을 현재의 활성화된 포트별로 확인할 수 있게 함으로써 효율적이고 정확한 관리를 할 수 있다.

참고문헌

[1] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", June 2001.
[2] W.Simpson, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.
[3] W.Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.
[4] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP) ", RFC2284, March 1998.
[5] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.
[6] T.Wu, "The SRP Authentication and Key Exchange System", RFC2945, September 2000.
[7] C.Rigney, "Remote Authentication Dial In User Service(RADIUS)" RFC 2138, April 1997.
[8] C.Rigney, "RADIUS Accounting" RFC 2139, April 1997.
[9] K.McCloghrie, D. Perkins, "Structure of Management Information for Version2 of the Simple Network Management Protocol(SNMPv2)" RFC 2578, April 1999.