GPRS 망에서 원격 이동 가입자의 무선 인터넷 접속을 위한 PPP CHAP 개선

박 정 현[†]·김 영 진[††]·이 윤 주[†††]·양 정 모[††††]

요 약

원격 이동 가입자가 방문망에서 자신의 홈망 인증 서버를 접속하여 인증을 득하고 이를 통해 IP를 할당 받아 무선 인터넷 서비스를 받게 되는데 이 경우 보편적으로 PPP CHAP 인증 기능을 적용한다. 그러나 기존의 PPP CHAP 인증 기능을 GPRS 망으로 이동한 원격 이동 ISP 가입자에게 직접 적용할 수는 없다. 이에 본 논문에서는 GPRS 망으로 이동한 원격 이동 ISP 가입자에게 PPP CHAP 인증 기능을 통해 홈망의 인증 서버를 접속하여 인증을 득하고 IP를 할당 받아 이동 ISP 가입자가 GPRS 망에서 무선 인터넷 서비스를 받을 수 있는 방법을 제시한다. 이를 위해 본 논문에서는 GPRS 망으로 이동한 이동 ISP 가입자가 PPP CHAP 인증 기능을 통해 홈망의 인증서버로부터 인증을 득할 수 있도록 기존의 PPP CHAP 메시지 변경 구조와 MT에서의 PCO 메시지 구조, 그리고 GGSN과 ISP RADIUS 연동 메시지 구조 등을 제시한다. 또 제안된 PPP CHAP 방식을 통해 GPRS 망 GGSN에서 ISP망 내 RADIUS 서버 접속시 진행된 인증 시험 결과를 제시한다.

PPP CHAP (Challenge Handshake Authentication Protocol) Modification for Wireless Internet Access of Remote Mobile Subscriber on GPRS (General Packet Radio Service) Network

Jeong-Hyun Park[†]·Yeong-Jin Kim[††]·Yoon-Ju Lee[†††]·Jeong-Mo Yang[††††]

ABSTRACT

We usually applied PPP CHAP when the visited ISP subscriber accesses to authentication server in own home ISP network and IP Assignment for remote Internet service. But PPP CHAP doesn't support in case of visited ISP subscriber in GPRS network accesses to authentication server in own home ISP network for wireless Internet service. We suggest solution for this problem with PPP CHAP improvement. For this we propose the modified PPP CHAP message format, PCO Message format at MT, and interworking message and format between GGSN and RADIUS in home ISP network for wireless internet service of mobile ISP subscriber at GPRS network in this paper. We also show authentication results when visited mobile ISP subscriber via PPP CHAP at GPRS network accesses the RADIUS server in home ISP network.

Keywords : Wireless Internet, GGSN(Gateway GPRS Support Node), GPRS(General Packet Radio Service), PPP(Point-to-Point Protocol), CHAP(Challenge-Handshake Authentication Protocol), RADIUS(Remote Access Dial-in User Service)

1. 서 론

최근 인터넷 기술은 통신망 분야에서 새로운 개발 형태로 중요한 기반으로 나타나고 있다. 패킷 데이터 트래픽 양이 급속도로 증가되고 있으며 이런 트래픽 패턴의 변화에 대응하고자 사업자들은 IP에 기초한 통신망으로 모든 전략과 계획을 적용하고 있다. 분명한 것은 인터넷은 앞으로 오늘보다 더 우리의 일상 생활에 현저하게 자리를 잡아가게 된다는 사실이다.

한편 이동 통신망에서의 기하급수적인 트래픽 증가와 더불어 이용자들의 폭발적 증대 및 계속적인 응용 서비스 개발 증대는 기존 유선망에서의 통신 가입자 수와 통신 서비스 이용률을 앞서고 있다. 대표적으로 우리나라와 같은 몇몇 나라의 경우 이동통신 이용자수는 기존 전화 가입자 수를 초과했고 이런 놀라운 발전은 오늘날 우리가 사용하고 있는 2세대 이동통신 시스템을 개발한 1980년대 만 하더라도 기대하지 못했다. 인터넷과 이동통신망의 발전과 성장의 결합은 곧 무선 이동 인터넷 접속과 응용 서비스 증대로 이어질

† 정 회 원 : 한국전자통신연구원 책임연구원
†† 정 회 원 : 한국전자통신연구원 Global 무선 LAN 연구팀장(책임연구원)
††† 비 회 원 : 한국전자통신연구원 북경이동통신연구센터장(책임연구원)
†††† 비 회 원 : 중부대학교 정보통신공학부 교수
논문접수 : 2001년 11월 17일, 심사완료 : 2002년 7월 22일

것이다. 따라서 무선 이동 통신망이 인터넷 서비스의 효율적인 지원 기능을 갖추도록 하는 것은 매우 중요하다.

3GPP에서 표준화 되고 있는 제 3세대 이동통신 시스템인 UMTS(Universal Mobile Telecommunication System)는 인터넷과 같은 패킷 데이터 서비스를 제공하기 위해 GPRS (General Packet Radio Service)[1] 시스템을 정의하고 있다. GPRS 시스템은 패킷 스위치 기능을 수행하는 SGSN (Serving GPRS Support Node)과 GGSN(Gateway GPRS Support Node)간 통신을 위해 IP 기반의 자체 백본망을 가지고 있다. 또한 GPRS 시스템은 ISP(Internet Service Provider)망과의 연동을 통해 ISP 망 가입자에 대한 로밍 서비스를 제공하며, Mobile IP[2] 서비스의 제공을 위한 Mobile IP 시스템도 정의하고 있다. 3GPP TS 29.061[3]에 기술된 바에 의하면 GPRS 시스템은 IP를 기본으로 하는 외부 ISP 망과 연동하는 기능을 가진다. ISP 망 가입자가 GPRS 이동망에 접근하였을 때, GPRS 시스템은 3GPP 규격[1]에 정의된 바와 같이 Gi 인터페이스를 통해 GPRS 망 가입자가 아닐지라도 ISP 가입자에 대해 인증 과정 및 ISP내의 IP 할당과정을 대리적으로 수행하고 패킷 전송을 위한 베어러를 열어 주는 작업을 수행한다.

본 논문에서는 이동 ISP 가입자가 GPRS망에서 GGSN을 통해 이러한 인증 및 IP할당을 위해 ISP의 RADIUS(Remote Authentication Dial In User Service)서버 및 DHCP (Dynamic Host Configuration Protocol) 서버와 연동시에 야기되는 문제점을 찾아보고 그에 대한 해결책을 제시하고자 한다. 특별히, 본 논문에서는 ISP 망 가입자가 GPRS 망 접속을 통해 ISP 망에 대한 접속을 시도할 때 요구되는 인증 방법 중 CHAP을 이용한 패킷 구조와 인증 프로토콜을 제시한다.

본 논문은 논문 배경에 이어, 2장에서는 이동 ISP가입자가 TE를 통해 GPRS 망을 통해 홈 ISP망의 접속시 TE와 GPRS MT에서 고려되어야 할 사항과 GGSN에서 해결되어야 할 문제, 그리고 이때 사용되는 PPP CHAP메시지 구조를 살펴보고, 3장에서는 GPRS 망에서 이동 ISP 가입자의 무선 인터넷 접속 방안을 제안하고 이때 필요한 CHAP 메시지 개선 방안과 패킷 구조를 정의하고 있다. 4장에서는 제안된 방안에 대한 구현과 시뮬레이션 결과를 제시하였고 마지막으로 5장에서 본 논문의 특징과 효과에 대한 내용을 정리하였다.

2. CHAP 이용시 무선 이동 인터넷 접속 문제

이동 가입자가 홈 망을 벗어나 방문망의 이동 패킷 데이터 통신망을 경유하여 홈 망의 인증 서버를 접속하고 이를 통해 무선 인터넷 및 이동 패킷 데이터 서비스를 받기 위해 기존의 사용되는 PPP CHAP 방식을 그대로 적용하는데는 문제가 있다. 기존의 PPP CHAP 방식은 기본적으로 고정망 환경을 고려하여 정의된 하나의 링크 설정 및 인증 프로토콜로 이의 이동 통신망 환경에서의 적용을 위해서는 PPP CHAP 규격의 추가적인 변경과 정의가 필요하다. 이 단원에서는 PPP CHAP 방식을 간단히 확인하고 이것이 이동통신망 환경에서 적용시 고려되는 문제점을 살펴본다.

2.1 PPP(Point-to-Point Protocol)[8]

PPP는 점 대 점 링크상에서 네트워크 계층 프로토콜 정보를 엔캡슐레이션 할 표준 방법을 제공한다. PPP는 또한 광범위한 링크제어 프로토콜을 정의하므로 링크상에서 전송할 네트워크 계층 프로토콜을 처리하기 앞서 인증할 통신 상대를 위한 인증 프로토콜의 협상기능을 지원한다. PPP는 다음과 같이 3개의 주요 요소를 갖는다.

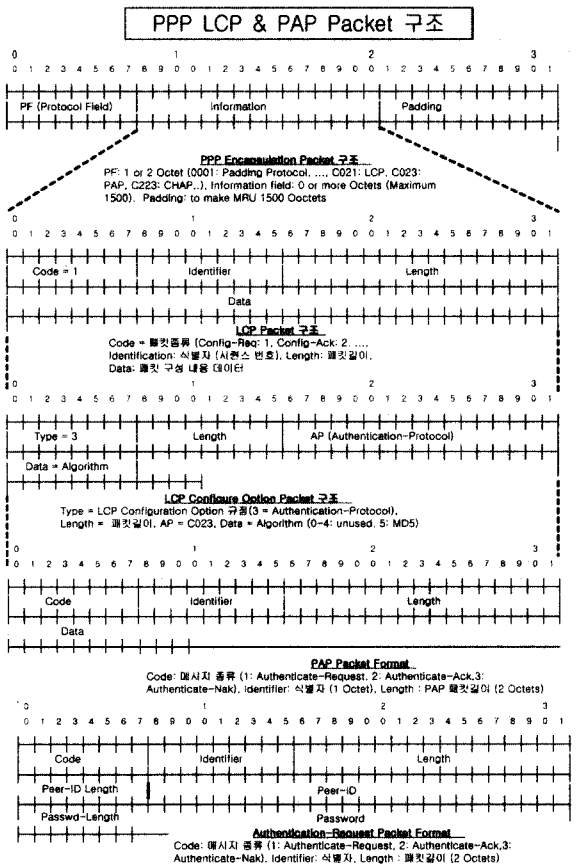
1) 시리얼 링크상에서 데이터 그램을 엔캡슐레이션하는 기능
2) 데이터 링크 접속을 설정하고, 구성하고 그리고 시험하기 위한 링크 제어 프로토콜(LCP, Link Control Protocol) 기능
3) 서로 다른 네트워크 계층 프로토콜을 설정하고 구성하기 위한 네트워크 제어 프로토콜의 슈트 (Network Control Protocol Suite) 기능

점 대 점 링크상에서 통신을 설정하기 위하여 PPP 링크의 각 끝점은 링크 설정 단계 중 데이터 링크를 구성할 LCP 패킷을 먼저 보내야 되며 링크가 설정되면 PPP는 네트워크 계층을 진행하기에 앞서 선택적인 인증 과정을 제공한다. 인증은 기본적인 의무사항은 아니나 만약 링크의 인증이 필요하다면 구현에서는 링크 설정 중에 인증 프로토콜 구성 옵션(Authentication Protocol Configuration Option)을 지정해야 한다. 이런 인증 프로토콜은 주로 회선 교환기나 전화선을 통해 연결을 시도하는 호스트나 라우터에 의해 사용하기 위한 것이지만 전용 링크에도 적용하기도 한다. 실제 PPP 인증 프로토콜로는 PAP(Password Authentication Protocol)과 CHAP(Challenge-Handshake Authentication Protocol) 2 가지 형태가 이용된다. 그 밖에 서버는 네트워크 계층과의 협상을 위한 선택 정보로 연결할 호스트나 라우터의 식별자(Identification)를 사용할 수 있다.

2.1.1 PPP PAP[14]

PAP은 2 방향 핸드쉐이크(2-Way Handshake)를 사용해 식별자를 확인하는 통신 상대를 위한 단순한 인증 방법이다. 이것은 초기 링크 설정에서 이루어진다. 링크 설정이

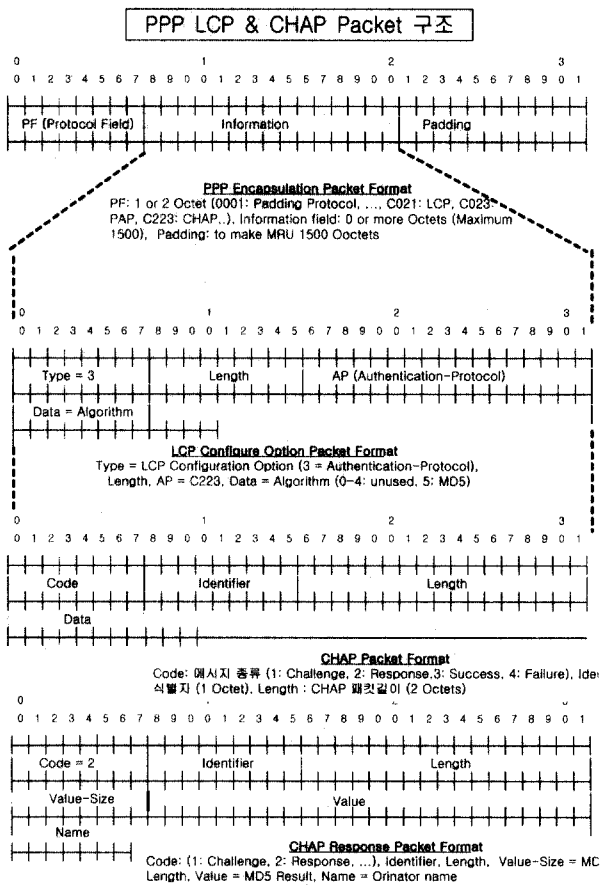
완료되면 사용자 ID와 패스워드는 통신 상대를 통해 인증 응답이나 접속 종료가 될 때까지 인증자로 반복해서 보내진다. PAP은 강한 인증 방법은 아니며 단순히 패스워드를 일반 통신회선을 통해 보내 진행되며 보통 재사용 형태 혹은 반복 시행 착오 시도 공격과 같은 것에 대해 보호되지 않는 방식이다. 통신 상대는 통신 시도 회수나 시간에 대한 조절 속에 있다. 따라서 구현 환경에 따라 PAP을 시도하기에 앞서 CHAP과 같은 좀더 강한 인증 방식을 진행하도록 하기도 한다. (그림 1)은 PPP LCP 및 LCP Option, 그리고 PPP PAP 메시지 구조와 각 메시지 필드에 대한 내용이다.



(그림 1) PPP LCP & PAP 메시지 구조

2.1.2 PPP CHAP[13]

CHAP은 3 방향 핸드쉐이크(3-Way Handshake)를 사용해 통신 상대의 식별자를 주기적으로 확인하는데 사용하는 인증 방법이다. 이것은 링크 설정 초기에 이루어지며 링크 설정이 된 후에도 언제든지 반복할 수 도 있다. 링크 설정이 완료된 후 인증자는 통신 상대에게 질의 메시지를 보내며 이에 대해 통신 상대는 일방향 해쉬 함수를 사용해 계산된 값으로 응답한다. 인증자는 기대한 해쉬 값에 대한 자신의 계산 결과를 가지고 응답을 검사한다. 그 값이 맞으면 인증자는 Ack 메시지를 보내며 그렇지 않으면 접속을 끊는다. CHAP은 식별자 변경과 랜덤값의 변경으로 재 사용 공격에 대처할 수 있다. 따라서 랜덤값의 반복 사용은 어떤 특정 공격에 대한 노출을 고려해 제한하도록 하여야 한다. 인증자는 랜덤값의 사용회수와 시기를 통제할 수 있다. 인증 방법은 인증자와 통신 상대만이 사전에 온라인 혹은 오프라인으로 통해 공급받아 알고 있는 비밀키 값에 의존하므로 비밀키 값은 링크 상을 통해 보내지는 않는다. CHAP은 많은 다른 시스템을 인증하는데 사용할 수 있기 때문에 가입자의 이름 부분은 비밀키를 보관하는 데이터 베이스의 인덱스로 사용될 수 있다. 이것은 또한 세션 중 언제든지 비밀키 변경을 할 수 있다. CHAP 알고리즘은 비밀키의 길이를 최소한 1 Octet 이상을 필요로 한다. 비밀키 값은 가능한 커야하며 예측이 안되는 특성을 갖을 수록 좋다. 또한 CHAP 방식에서는 비밀키를 암호화된 패스워드 데이터가 아닌 평문 형태로 받아 들여 사용하는 단점도 갖고 있다. 모든 가능한 비밀키를 링크의 양단끝에서 유지해야 하기 때문에 대규모 환경에서는 적합치 않을 수 있다. 그럼에도 PPP CHAP은 기존 유선망에서 전화선이나 회선 교환기를 통해 클라이언트가 인증 서버를 접속할 때 가장 보편적으로 적용되는 인증 방식이다. 아래 (그림 2)는 PPP CHAP Packet 구조와 각 필드에 대한 내용이다.



(그림 2) PPP LCP & CHAP 메시지 구조

2.2 CHAP 이용시 무선 이동 인터넷 접속 문제

대부분의 현존 ISP 업체는 가입자가 다이얼 업 모뎀을 통해 내부적으로 클라이언트와 서버간에 링크 설정 및 PPP PAP 혹은 CHAP을 통한 인증을 진행한 후 패킷 데이터 및 인터넷 서비스를 제공한다. 그러나 인터넷과 이동통신의 결합을 통한 무선 인터넷 및 이동 패킷 데이터 서비스 지원 시 기존 PPP CHAP 방식을 현존 이동통신과 인터넷이 결합한 환경에 직접 적용하기는 어렵다. 즉, 기존의 고정망을 통한 인증 서버 접속시 PPP CHAP의 처리 과정과 이동 통신망을 경유하여 인증 서버 접속시 PPP CHAP 처리는 다르다. 따라서 가입자가 이동 통신망을 경유하여 인터넷 및 무선 이동 패킷 데이터 서비스를 받을 때 기존의 PPP CHAP 처리 과정은 수정되어야 하며 필요에 따라 무선 패킷 이동 통신 서비스를 위한 기본적인 규약이 정해져야 할 것이다. 따라서 고정 가입자가 이동 통신망을 경유하여 자신의 홈 망의 인증 서버를 접속하고 이어 무선 이동 패킷 데이터 및 인터넷 서비스를 받기 위해서는 기존의 PPP CHAP은 먼저 TE(Terminal Equipment)와 이동 단말(MT)간의 처리 과정에서의 규약이 필요하고, 다음은 이동 단말에서 이동 통신망 게이트웨이로 보내는 PPP CHAP 메시지 전송 부분, 그리고 마지막으로 이동 통신망 게이트웨이에서 이동 가입자 홈 망내의 인증 서버로 보내는 메시지 처리 과정이 해결되어야 한다.

2.2.1 TE-MT(Mobile Terminal) 사이의 연계 문제

TE와 이동 통신 단말인 MT 사이에서 먼저 PPP 링크 설정 및 인증 메시지의 처리에 대한 절차가 정의되어야 한다. 이를 위해 MT는 TE 홈 망의 가상 인증 서버로 혹은 TE가 MT를 경유하여 홈 망의 인증 서버를 연결하는데 필요한 기능을 가져야 한다. 즉, 두 경우 MT에서 모든 지원 가능해야 하며 우선은 이동통신망의 무선 지연을 고려하여 MT를 홈 망의 가상 인증 서버로 고려하여 처리할 수 있는 방법이 고려된다. 이 경우 TE와 MT 사이의 링크 설정 과정과 PPP CHAP 처리 과정이 진행될 수 있어야 하며 이에 따른 MT에서 가상 인증 서버 기능이 지원되어야 한다.

2.2.2 MT에서 해결되어야 할 문제

MT가 홈 망의 가상 인증 서버로 동작될 경우 MT는 PPP CHAP 처리 및 중계 기능을 가지며 이때 필요한 메시지와 구조가 정의되어야 한다. 아울러 MT가 PPP CHAP 메시지 처리 및 중계 기능을 갖을 때 MT에서는 이동 패킷 통신망 환경에서 PPP CHAP 메시지를 이동 패킷 망 게이트웨이로 전달하는 기능이 있어야 한다.

2.2.3 MT와 GGSN에서 해결되어야 할 문제

MT에서 준비된 PPP CHAP 메시지나 이동 가입자 홈 망의 인증 서버에서 준비된 메시지의 중계 처리를 위해 MT와 무선 패킷 데이터 통신망 게이트웨이 사이에는 상호 중계 및 처리를 위한 메시지와 이의 구조 및 처리절차가 정의되어야 한다.

2.2.4 GPRS 망 게이트웨이노드 GGSN에서 해결되어야 할 문제

MT에서 보내온 PPP CHAP이 담긴 메시지의 해석과 이 메시지 내용을 이동 가입자 홈 망으로 보낼 수 있는 기능을 갖어야 한다. 이의 처리를 위한 메시지와 구조 및 처리 절차 정의가 필요하다.

2.2.5 GGSN과 이동 가입자 홈 망내 인증 서버 사이에서의 처리 문제

이동 패킷 데이터 통신망 게이트웨이 노드 GGSN과 이동 가입자 홈 망의 인증 서버 사이에는 상호 인증 관련 메시지 중계 및 처리할 수 있는 기능이 준비되어야 하며 이를 처리하기 위한 메시지 구조가 정의되어야 한다.

2.2.6 기타 과금/QoS 처리 문제

그 밖에 이동 가입자가 패킷 이동통신망을 경유하여 자신의 홈 망 내 인증 서버를 접속하여 무선 인터넷 및 이동 패킷 데이터 서비스를 받기 위해서는 무선 패킷 이동 데이터 통신망과 홈 망 사이에 이동 가입자별 서비스 지원 정의 문제 및 서비스별 품질을 처리 할 수 있는 QoS 지원 문제, 그리고 이동 패킷 데이터 통신망과 이동 가입자의 홈 망 사이에 이동 가입자 무선 인터넷 서비스 지원에 따른 과금 처리 문제와 이에 대한 기본적인 상호 협약이 선행되어야 할 것이다.

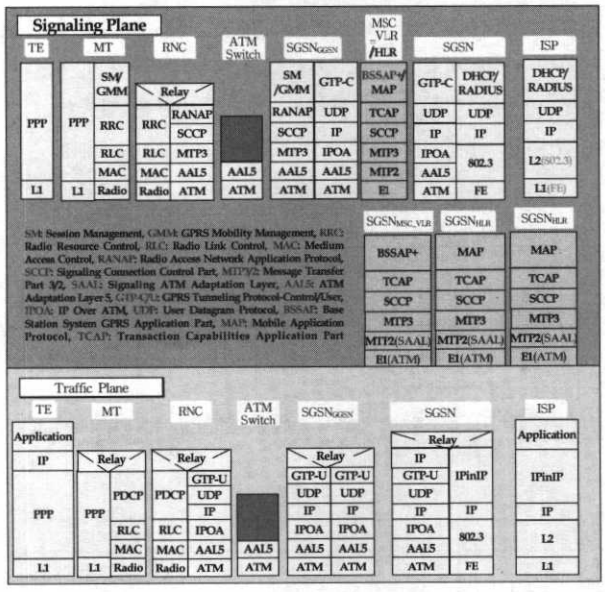
3. 이동 ISP 가입자의 무선 인터넷 접속 방안

GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 경유하여 홈 ISP 망을 접속하여 무선 인터넷 서비스를 받기 위해서는 이동 ISP 가입자 TE에서 보내는 PPP CHAP Response 메시지 내에 PPP CHAP Challenge 값이 포함되어야 한다. 또 GPRS MT에서 PCO(Protocol Configuration Option) 데이터 구조에 PPP CHAP Challenge 값을 별도 정의하여 GPRS GGSN으로 보내 홈 ISP 망내의 RADIUS 서버로 보내도록 할 수 있다. 본 절에서는 GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 경유하여 홈 ISP 망의 인증 서버를 접속할 때 필요한 프로토콜 스택과 접속 방법 그리고 PPP CHAP Challenge 값의 처리 방안 등을 제시한다.

3.1 프로토콜 스택 구조

(그림 3)은 이동 ISP 가입자가 GPRS 망을 통해 홈 ISP 망을 접속하여 무선 인터넷 서비스를 받을 때 이동 패킷망

노드에서 요구되는 프로토콜 스택 구조이다. TE와 MT사이는 PPP 링크 설정을 위한 PPP 클라이언트와 가상 PPP 서버가 있으며 MT는 가상 PPP 서버로서 받은 TE 관련 정보를 이동 접속 망을 경유하여 홈 ISP망 노선의 인증서버로 전달하기 위해 MT와 RNC 기지국 사이에는 PDCP (Packet Data Convergence Protocol), RNC와 SGSN 사이는 RANAP, SGSN과 GGSN 사이는 GTP(GPRS Tunneling Protocol)가 각각 있으며, 각 노드 프로토콜내에서 PCO 데이터가 포함되어 정의되어 전송된다. 게이트웨이 노드인 GGSN에서는 GTP내 PCO 정보를 끄집어 내어 홈 ISP 망의 인증서버로 필요한 정보를 보내어 이동 ISP 가입자의 실제 인증을 받게 되며 그 인증 결과를 다시 GTP 메시지내 PCO에 넣어 MT로 보낸다. 또한 이동 ISP망 가입자가 GPRS망을 통해 무선 인터넷 서비스를 받기위해 게이트웨이 노드와 ISP 망내 서버간에는 이동 데이터 전송을 위해 IP_in_IP로 엔캡슐레이션 및 디캡슐레이션하도록 하고 있다.

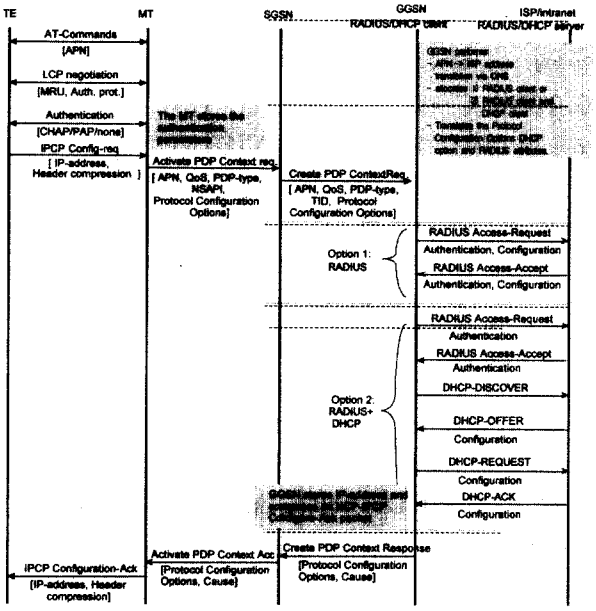


(그림 3) 이동 ISP 가입자가 GPRS 망을 통해 홈 ISP 망 접속시 신호 및 데이터 처리에 필요한 프로토콜 스택 구조

3.2 CHAP을 이용한 이동 ISP 가입자의 무선 인터넷 접속

이동 ISP 가입자가 GPRS 망으로 이동해 온 경우 이동 ISP 가입자는 GPRS 망을 통해 무선 인터넷 서비스를 받기에 앞서 홈 ISP 망에 접속하여 먼저 인증과 IP 주소를 받아야 한다. 이러한 주소는 정적인 경우 인터넷 서비스 가입시에, 동적인 경우 GPRS 망에서 PDP Context Activation시에 이루어진다. 이 경우 GPRS GGSN은 ISP 망내의 RADIUS[4] 및 DHCP[5, 6] 서버와의 직접적인 연동을 하는 기능을 가져야 한다. 이를 위해 GPRS 망을 방문한 이동 ISP 가입자는 PDP Context Activation시에 인증에 필요한 개인 정보를 GGSN에게 전달해야 하는데 이것은 GTP의 Information Element내의 PCO을 통하여 이루어진다. GGSN은 외부 ISP의 RADIUS/DHCP 서버와 직접 연동하여 이동 ISP 가입자를 위해 인증 및 주소 할당 과정을 수행한다. (그림 4)에서 이동 ISP 가입자가 GPRS 망을 통해 홈 ISP 망내 RADIUS 인증 서버와 DHCP 서버의 접속을 시도하는 경우에 대한 절차를 나타내고 있다. 먼저 TE는 MT에 AT-Command를 주고 받고, PPP모드에서 LCP 협상을 한다. 그리고 필요에 따라 CHAP 혹은 PAP 프로토콜을 이용하여 인증을 요구한다. 이때 MT는 임시적으로 인증 성공 응답을 TE쪽으로 주고, 이때 MT에서는 TE와 사용된 인증 정보를 저장한다. 이후에 MT는 IPCP[7] 메시지를 통해 IP요구 메시지를 보내어 정적 혹은 동적 IP의 할당을 요구한다. 이 과정이 끝나고 나면 MT는 세션활성화를 위한 다른 정보들과 함께, 인증 요구(CHAP or PAP) 및 IP할당 요구(IPCP) 메시지를 PCO[8]에 기록하여, SGSN에 세션활성화 메시지로 전송한다. SGSN은 해당 GGSN을 찾아 Create PDP Context Request 메시지를 전송한다. GGSN은 SGSN에서 온 Create PDP Centext Request 메시지내 APN[9]을 해석하여 해당 ISP를 구분하고, 또한 이 ISP에 인증 및 IP 할당을 위해 RADIUS 서버만을 접속할 것인지, RADIUS 및 DHCP를 접속할 것인지를 결정한다. 만약 RADIUS만을 접속하는 경우라면 GGSN은 PCO내의 정보를 분석하고 이를 통해 ISP의 RADIUS 서버에 접속하여 인증 및 IP를 취득한다. DHCP를 사용하는 경우는 먼저 RADIUS 서버의 접속을 통해 인증이 성공한 경우, 이후에 DHCP 서버에 접속하여 IP 및 관련정보를 부여받는다. ISP로부터 인증과 IP할당이 성공했을 경우, GGSN은 TE로부터 요청된 IPCP내 원하는 IP와 실제 ISP로부터 받은 IP를 비교하여 각각 IPCP-ACK, IPCP-NAK를 결정하며 인증 혹은 IP 할당에 실패한 경우는 IPCP-Reject 메시지를 구성한다. 이후 GGSN은 이러한 IP정보를 저장하고, 이 정보를 바탕으로 PCO를 구성하여 Create PDP Context Response를 SGSN으로 전송한다. SGSN은 Activate PDP Context Accept를 MT에 전송하고, 이후 MT는 PCO내의 IP 정보를 읽어 IPCP 결과에 따라 TE와 지역적인 협상을 통해 IP를 전달하게 된다. 그런데 이동 ISP TE한테 동일 주소로 계속적으로 서비스를 받기 위해서는 lease time이 만료되기 이전에 IP 할당시간을 연장하는 기능이 필요하다. GGSN에서 ISP로부터 동적 IP를 획득하여 TE에 전달한 경우 동적 IP에 대해 할당 시간(Lease Time)을 함께 부여받게 되는데, 이 경우 GGSN은 세션이 종료되기 이전까지 해당IP의 갱신(Renewing)을 위해 할당 시간을 계속적으로 연장하는 기능을 담당해야 한다. 이것은

할당시간이 만료되기 이전에 주소 할당 서버(DHCP)에 갱신 메시지를 보냄으로써 이루어 질 수 있다. 또 GGSN은 동적 IP에 대해 IP 할당 시간 연장을 위해 내부적으로 타이머를 구동시키며 주기적으로 할당 연장을 위한 메시지를 전송해야 한다. 또한 TE가 세션을 종료한 경우 GGSN은 ISP내의 IP 자원 관리 및 과금 관리 차원에서 해당 주소 할당 서버에 IP 해제 메시지를 전송하여야 한다. 이는 DHCP Release메시지를 보냄으로써 이루어 질 수 있다.



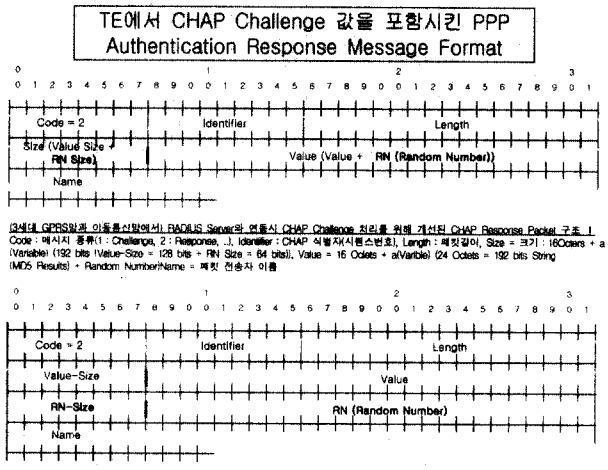
(그림 4) 이동 ISP 가입자가 GPRS 망을 통해 인증과 IP 주소를 할당 받는 과정

3.3 PPP CHAP 메시지와 PCO 데이터 변경

이동 ISP 가입자가 GPRS 망을 통해 홈 ISP 망을 접속하여 인증을 받기 위해 시도하는 PPP CHAP 메시지는 수정되어야 한다. 즉, 이동 ISP 가입자가 GPRS 망을 경유하여 홈 ISP 망 접속을 통해 무선 인터넷 서비스를 시도할 때 먼저 이동 ISP 가입자 TE와 GPRS의 MT사이에 PPP 링크 설정이 이루어지고, 이어 PPP CHAP을 통해 TE와 MT사이에 이동 ISP 가입자에 대한 가상 인증을 실행한다. 이어 MT는 TE에서 보내온 ISP 인증 정보를 GPRS 망을 경유하여 홈 ISP 망으로 보내 이동 ISP 가입자에 대한 실제 인증을 행한다. 이때 TE에서 MT로 보내는 PPP CHAP Response 메시지에는 홈 ISP 망 내 RADIUS 서버에서 이동 ISP 가입자의 실제 인증에 반드시 필요한 CHAP Challenge 값을 포함하고 있지 않다. 이를 위해 기존 PPP CHAP Response 메시지는 수정되어야 하며 혹은 다른 방법으로 GPRS MT에서의 PCO 데이터 구조를 수정하여 CHAP Challenge값을 ISP 인증 서버로 전달할 수 있어야 한다. 다음은 각 방안에 대한 구조와 설명이다.

3.3.1 TE에서의 PPP CHAP Response 메시지 변경

GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 접속할 때 이동 ISP 가입자 TE와 GPRS MT사이는 PPP 링크 설정과 이동 ISP 가입자에 대한 가상 인증이 진행된다. 이때 TE는 PPP Client, MT는 PPP Server의 역할을 하게 되며 특별히 TE에 대한 가상 인증으로 TE와 MT에서는 PPP CHAP Request와 CHAP Response를 주고 받는다. 그러나 이동 ISP 가입자에 대한 최종 인증은 홈 ISP 망 내 RADIUS 서버에서 이루어지며 CHAP Request에서 사용된 CHAP Challenge 값은 홈 ISP 망의 RADIUS 서버로 보내져 이동 ISP 가입자에 대한 실제 인증이 진행되어야 한다. 아래 (그림 5)는 GPRS 망으로 이동한 이동 ISP 가입자의 실제 인증을 위해 필요한 CHAP Challenge값 처리를 위한 메시지 구조이다. (그림 5)에서 첫 번째 방안은 TE에서 보내는 CHAP Response 메시지 내 Random Value Field에 CHAP Challenge 길이와 값을 넣어서 처리하는 방안이고, 두 번째 방안은 CHAP Response 메시지 내에 별도의 필드를 두어 CHAP Challenge 길이와 값을 정의하여 처리하는 방안이다. 이렇게 하므로 CHAP Challenge 값은 홈 ISP 망의 RADIUS 서버로 보내져 GPRS 망으로 이동한 이동 ISP 가입자에 대한 실제 인증을 가능케하고 이를 통해 GPRS 망으로 이동한 이동 ISP 가입자는 홈 ISP 망을 접속하여 무선 인터넷 서비스를 제공받게 된다.

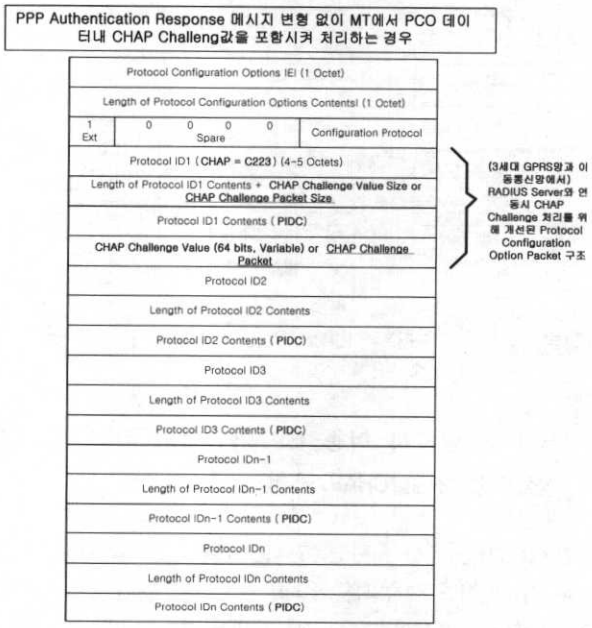


(그림 5) TE에서 PPP CHAP Response 메시지 구조

3.3.2 MT에서의 PCO 데이터 구조

GPRS 망으로 이동한 이동 ISP 가입자 인증시 필요한 CHAP Challenge 값을 MT의 PCO 데이터 구조에서 정의하여 처리하는 방안도 가능하다. 원래 MT는 TE에서 보내온 CHAP Response 메시지를 그대로 PCO 필드에 넣어 GPRS 망 게이트웨이 노드인 GGSN으로 보내게 되는데 이때 TE에서 보내온 CHAP Response 메시지 내에는 CHAP

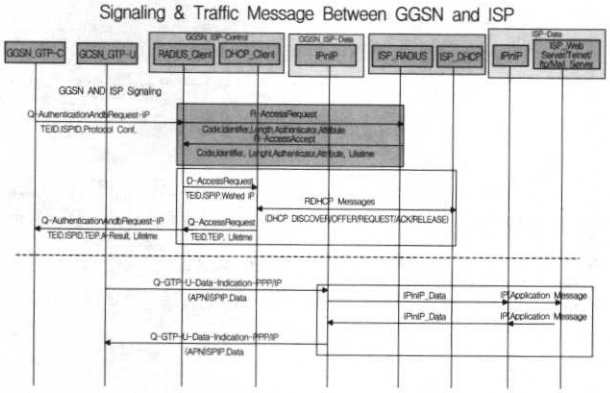
Challenge 값이 포함되지 않는다. 따라서 이를 위해 앞에서 제안 한 것처럼 CHAP Response 메시지를 변경하여 CHAP Challenge 값을 처리하는 방안이 있다. 그러나 이 방안은 기존의 PPP CHAP Response 메시지 구조를 변경해야 하는 사항이 따르고 이는 RFC의 변경까지도 고려되어야 한다. 또한 기존 PPP 단말도 GPRS 망으로 이동한 경우 새로운 형태의 PPP CHAP Response 메시지의 처리가 가능해야 하는 어려움도 따르게 된다. 이에 PPP CHAP Challenge 값을 GPRS MT의 PCO 데이터 필드에서 정의하여 처리하면 앞의 번거로움 없이 GPRS 망으로 이동한 이동 ISP 가입자에 대한 인증 정보 처리가 가능하다. (그림 6)은 PCO 데이터 구조에서 CHAP Challenge 값을 처리하는 방안이다. 첫 번째 방안은 기존의 CHAP PIDC 필드의 길이와 값에 CHAP Challenge 길이와 값을 포함시켜 처리하는 방안이고, 두 번째 방안은 CHAP PIDC(Protocol Identification Content) 필드 다음에 별도의 CHAP Challenge 필드를 두어 CHAP Challenge 길이와 값을 정의하여 처리하는 방안이다.



(그림 6) MT PCO 구조에서 PPP CHAP Challenge 값의 처리 구조 정의

3.4 GPRS GGSN과 ISP RADIUS/DHCP 서버간의 메시지 처리

GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 경유하여 홈 ISP 망 접속을 시도한 경우 먼저 홈 ISP 망내 인증 서버인 RADIUS 서버를 통해 인증을 득하고, 이어 홈 ISP 망 내 IP 주소 할당 서버를 통해 IP 주소를 할당받게 된다. 이때 GPRS 게이트웨이 노드인 GGSN은 MT에서 보내온 PCO 데이터를 통해 TE에서 올라온 이동 ISP 가입자에 대한 인증 정보를 추출해 RADIUS Client 메시지로 변형하여 이를 다시 홈 ISP 망내의 RADIUS 서버로 보낸다. (그림 7)은 MT의 PCO 데이터 구조를 통해 TE에서 올라온 가입자 인증 정보를 홈 ISP RADIUS 서버로 보내기 위해 GGSN에서 정의된 메시지이며 (그림 8)은 RADIUS Client 메시지 구조이고 (그림 9)는 소켓을 사용하여 GGSN에서 홈 ISP RADIUS/DHCP 서버로 보내는 RADIUS/DHCP Client 메시지 구조이다.



(그림 7) GPRS GGSN과 ISP RADIUS/DHCP 사이의 인터워킹 메시지

(그림 7)은 GPRS 망으로 이동한 이동 ISP 가입자의 무선 인터넷 서비스를 위해 진행되는 이동 ISP 가입자의 인증과 IP 주소 할당 관련 GGSN과 ISP내 RADIUS/DHCP 서버 사이에서 순차적으로 주고받는 메시지이며 그 과정은 다음과 같다.

단계 1 : GGSN_GTP-C -> GGSN_ISP_Control : Authentication_IP_Assignment_Request(GGSN GTP에서 ISP RADIUS 서버로 보내는 RADIUS Client 메시지를 생성하여 보내도록 하는 이동 ISP 가입자 TE의 인증 및 IP 할당 요구 메시지)

단계 2 : TE에 대한 인증과 정적 IP 사용 확인만을 필요로 하는 경우는 아래 단계 2-2과 단계 2-3은 필요하지 않다.

단계 2-1 : GGSN_ISP_Control <-> ISP_RADIUS : Access-Request/Access-Accept/Accept-Reject (GGSN_ISP와 ISP RADIUS 서버간에 주고받는 RADIUS Client 메시지)

단계 2-2 : GGSN_ISP_(RADIUS) <-> GGSN_ISP_(DHCP) : ISP_MN_Request and ISP_MN_Response(GGSN 내에서 RADIUS Client 부분과 DCHP Client간에 주고 받는 메시지로 TE의 동적 IP 주소 할당을 요구할 때 필요하다)

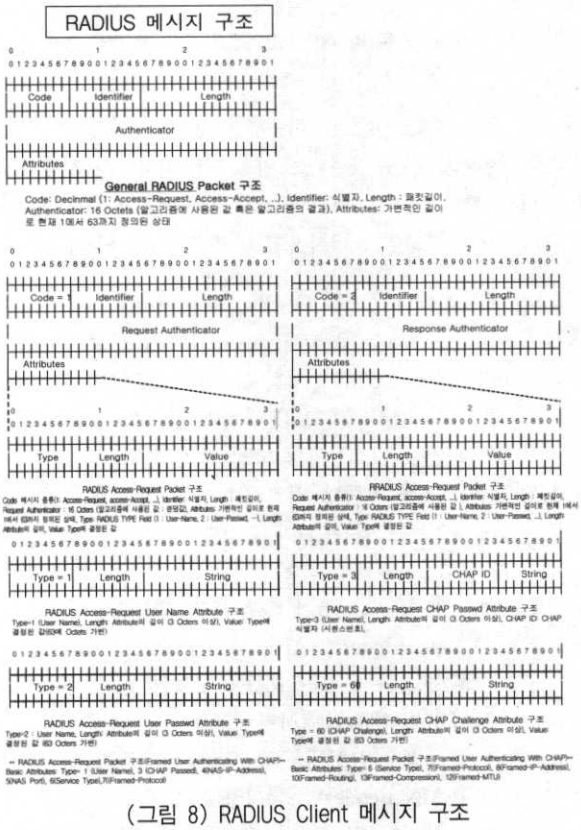
단계 2-3 : GGSN_ISP_Control <-> ISP_DHCP : DHCP Discover/Offer/Request/Ack. (GGSN_ISP와 ISP DHCP 서버간에 주고받는 DHCP Client 메시지)

단계 3 : GGSN_ISP_Control -> GGSN_GTP-C : Authentication_IP_Assignment_Response (GGSN_GTP에서 보내온 이동 ISP 가입자 TE의 인증 및 IP 할당 요구에 대한 응답 메시지)

단계 4 : GGSN_GTP-C -> GGSN_ISP_Control : Termination_Extension_Request (GGSN_GTP에서 보내온 이동 ISP 가입자에게 부여된 IP 주소의 갱신 및 종료 요구 메시지)

단계 5 : GGSN_ISP_Control -> GGSN_GTP-C : Termination_Extension_Response. (GGSN_GTP에서 보내온 이동 ISP 가입자에게 부여된 IP 주소의 갱신 및 종료 요구에 대한 응답메시지)

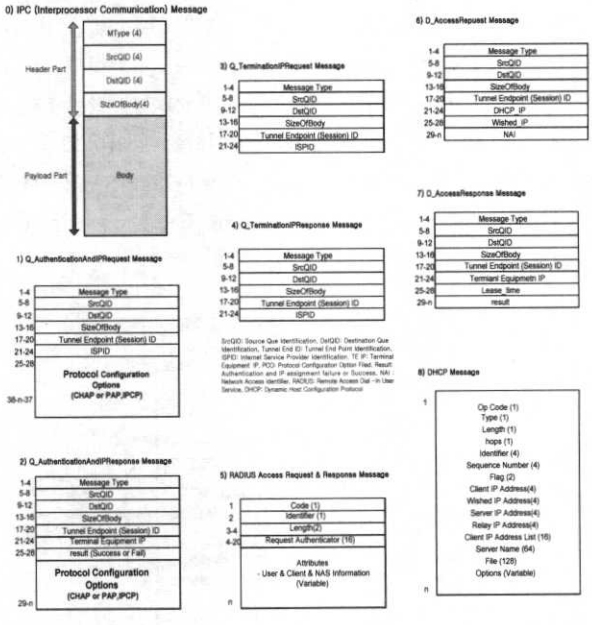
(그림 8)은 GPRS 망으로 이동한 이동 ISP 가입자가 ISP 망 내 RADIUS 서버를 접속하여 인증을 득하기 위해 TE에서 올라온 이동 ISP 가입자 인증 정보를 GGSN에서 RADIUS Client 메시지에 담아 ISP RADIUS 서버로 보내는 RADIUS Client 메시지 구조이다.



(그림 8) RADIUS Client 메시지 구조

(그림 9)는 GGSN에서 소켓을 사용하여 RADIUS/DHCP Client 메시지를 ISP RADIUS/DHCP 보낼 때 정의한 RADIUS/DHCP Client 소켓 메시지 구조와 GGSN_GTP에서 GGSN_ISP 부분으로 IPC(Inter Processor Communication)를 사용하여 보내는 이동 ISP 가입자의 인증과 IP 할당 및 해제에 대한 요구/응답 메시지 구조이다.

0) Basic IPC(Inter Processor Communication) 메시지 구조
1) Authentication_IP_Assignment_Request 메시지
2) Authentication_IP_Assignment_Response 메시지
3) Authentication_IP_Termination_Extension_Request메시지
4) Authentication_IP_Termination_Extension_Response메시지
5) RADIUS Client
6) ISP_MN(TE)_Request 메시지
7) ISP_MN(TE)_Response 메시지
8) DHCP Client



(그림 9) GPRS GGSN과 ISP RADIUS/DHCP 서버 간의 소켓 메시지 구조

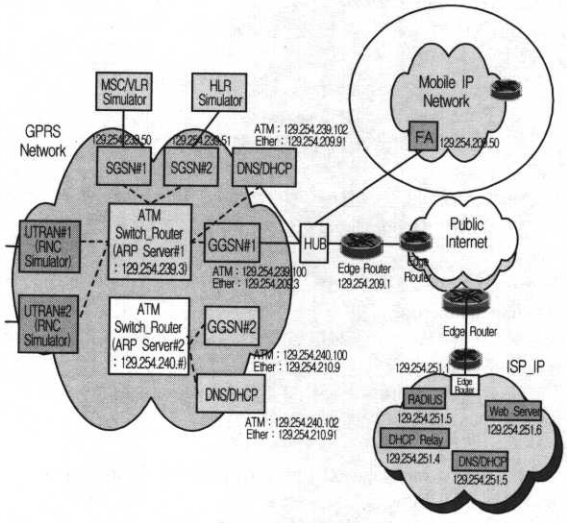
4. GPRS 망에서 이동 ISP 가입자의 무선 인터넷 접속을 위한 CHAP 구현

본 절에서는 제안한 PPP CHAP Challenge 처리 방식과 정의한 인터페이스 메시지를 이용해 실제 환경을 구축하고 구현하여 3세대 GPRS 망 Testbed에 적용한 내용을 기술한다.

4.1 환 경

SGSN과 GGSN의 구현과 RNC 시뮬레이터 구현을 통해 GPRS 핵심망 Testbed 환경 구축을 하였고, ISP 내 인증 서버와 DHCP서버 그리고 웹 서버 구현을 통해 솔라리스 환경에서의 ISP 망을 구축하였다. 그리고 RNC 시뮬레이터는 MT대신 가상의 PPP 인증 서버 역할을 대신하여 PPP PCO 데이터를 준비하며 이는 SGSN으로 보내는 PDP Context 메시지 내 포함하여 SGSN과 GGSN으로 전송하도록 하였다. 또 SGSN과 GGSN사이는 155 Mbps ATM 인터페이스로 네트워크가 구성되었고 GGSN과 ISP 망 사이는 IP

를 기준으로 Fast Ethernet 으로 구성하였다. 아래 (그림 10)은 PPP CHAP을 통해 SGSN, GGSN, 그리고 ISP 인증 서버까지의 통신 환경을 보여 준다.



(그림 10) 시뮬레이션 환경

4.1.1 TE에서 정의한 정보

시뮬레이션을 위해 TE에서 정의한 이동 ISP 가입자에 대한 정보는 사용자 ID와 패스워드 그리고 CHAP Challenge Value이다. 아래 내용은 실제 시험에 사용된 값이다.

- 사용자 ID : bari123
- 사용자 패스워드 : testing
- CHAP Challenge :
- CHAP Response = 사용자 ID ⊕ CHAP Challenge

4.1.2 MT에서 PCO 메시지 정보

또 MT에서 정의되는 PCO 메시지는 아래 값들로 사용하였으며 본 시험에서는 CHAP Challenge 값을 MT PCO에서 정의하여 처리하는 방안으로 시험하였다.

- 사용자 ID : bari123
- 사용자 패스워드 : testing
- CHAP Challenge :
- CHAP Response :
- Wished IP : none
- Total Size : 0x46
- PCO 데이터 구성(Hex) : 0x1, 0x46, 0x80, 0xc0, 0x21, 0x9, 0x1, 0x1, 0x0, 0x9, 0x3, 0x5, 0xc2, 0x23, 0x5, 0xc2, 0x23, 0x2d, 0x2, 0x1, 0x0, 0x1c, 0x10, 0x7, 0x5a, 0x3d, 0x30, 0xff, 0x62, 0xa6, 0x4c, 0xd9, 0xf5, 0x4, 0xee, 0xe3, 0x59, 0x68, 0x76, 0x79, 0x61, 0x63, 0x68, 0x61, 0x37, 0x33, 0x10, 0x7e, 0x46, 0x55, 0x97, 0x3, 0x8d, 0x11, 0x19, 0x8, 0xd3, 0xcc, 0x9c, 0xe, 0x1a, 0x88, 0x1e, 0x80, 0x21, 0x6, 0x3, 0x6, 0x0, 0x0, 0x0, 0x0

4.1.3 RADIUS 서버 환경

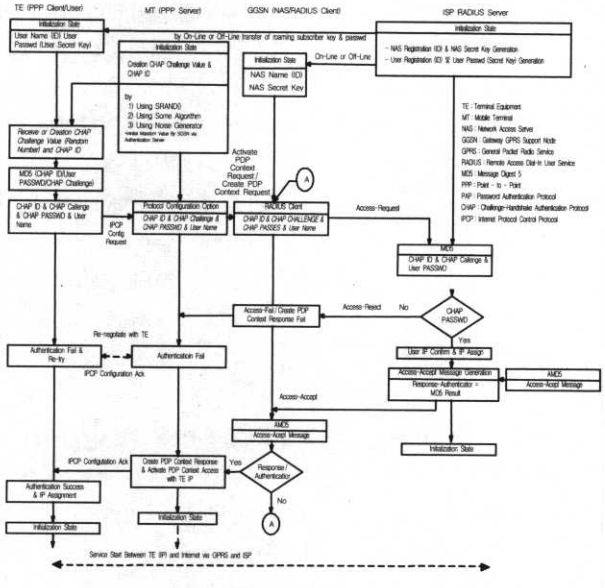
홈 ISP 망 내에서 RADIUS 서버는 Solaris 2.7 환경에서 구축하였고 실제 시험을 위해 RADIUS 서버의 환경은 아래와 같이 구성하였다.

- Bari Auth-Type = local, Password = "bari"
  service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 129.254.251.33,
  Framed-IP-Netmask = 255.255.255.0,
  Framed-MTU = 1500,
- Yacha73 Auth-Type = local, Password = "testing"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 129.254.251.34,
  Framed-IP-Netmask = 255.255.255.0,
  Framed-MTU = 1500,

ISP는 자신의 인증 서버에 가입자가 서비스 등록 시 가입자 관련 정보를 등록하고 관리하게 된다. 즉, 이동 ISP 가입자는 bari라는 이름으로 홈 ISP 망의 RADIUS 서버에 등록이 되어 있고, bari는 129.254.251.33 정적 IP 주소의 사용자로 되어 있다. 그밖에 bari외 또 다른 사용자의 등록이 가능하며 yacha73의 가입자가 129.254.251.34 정적 IP 사용자로 등록이 되어 있는 경우를 보여 준다.

4.2 동작 절차

(그림 11)은 ISP 가입자의 서비스 등록과 이에 따른 가입자 관련 초기 정보 준비 단계, 그리고 ISP 가입자가 GPRS 망으로 이동하여 홈 ISP 망의 접속을 통해 무선 인터넷 서비스를 받기 위해 이동 ISP TE에서 진행되는 내용, GPRS MT에서 준비하는 내용, GPRS GGSN에서 인증 관련 동작하는 과정, ISP RADIUS 서버에서 TE의 인증을 위해 진행하는 MD5 인증 처리 절차 등을 나타내고 있다.



(그림 11) 동작 절차

단계 1 : MT가 TE로 인증 요구 메시지를 보내면 TE는 자신의 ID와 비밀키 값에 랜덤값을 입력으로 MD5를

돌려 CHAP ID를 생성한다.

단계 2 : MT는 TE에서 온 CHAP Response와 CHAP Challenge 값을 PCO에 넣어 RNC/SGSN을 통해 GGSN으로 보낸다.

단계 3 : GGSN에서는 PCO 메시지 내 있는 TE ID와 CHAP ID, CHAP Challenge 값을 끄집어 내어 RADIUS Access-Request 메시지 내에 넣어 ISP RADIUS 서버로 보낸다.

단계 4 : ISP RADIUS 서버는 자신이 갖고 있는 TE에 대한 비밀키 값과 TE의 ID 그리고 CHAP Challenge를 입력으로 MD5를 돌려 GGSN에서 온 CHAP ID 값과 같은지 비교한다.

단계 5 : ISP RADIUS 서버는 MD5의 결과가 일치하면 인증 성공 결과와 TE에게 부여된 정적 IP 주소 값을 RADIUS Access-Accept에 넣고 이 Access-Accept 메시지 내용과 GGSN (NAS)의 비밀키 값을 입력으로 MD5를 돌려 그 결과를 Access-Accept 메시지 내의 Authenticator 값으로 채워 넣어 GGSN으로 보낸다.

단계 6 : GGSN에서는 수신한 Access-Accept 메시지에서 Authenticator를 뺀 나머지 값과 ISP RADIUS 서버에 등록된 GGSN-NAS 비밀키 값을 입력으로 MD5를 돌려 Authenticator 값과 같은지를 비교한다. 인증 값이 같지 않으면 몇 번의 시도를 계속하다 계속적인 실패가 오면 인증 실패 내용을 MT를 거쳐 TE에게 알린다.

단계 7 : 인증 값이 일치하면 ISP RADIUS 서버에서 얻은 인증 결과와 정적 IP 주소를 GGSN에서 Create PDP Context Message내에 넣어 SGSN/RNC를 통해 MT로 보내고, 이를 다시 TE에게 인증 성공 결과와 부여된 정적 IP 사용 확인으로 처리한다.

단계 8 : 이후 TE는 자신이 갖고 있는 홈 ISP 망의 정적 IP를 이용해 GPRS 망 게이트웨이 노드 GGSN을 거쳐 자신의 홈 ISP 망을 접속하여 무선 인터넷 서비스를 받는다.

4.3 시뮬레이션 결과[11]

GPRS 망으로 이동한 이동 ISP 가입자가 TE에서 MT로 자신의 인증 및 개인정보를 보낼 때 포함되어야 하는 정보는 SGSN에 연결된 RAN 시뮬레이터를 통해 처리하였다. 이어 RAN 시뮬레이터를 통해 입력된 정보는 SGSN GTP를 통해 GGSN으로 전달되고 GGSN에서는 GTP 내 입력된 PCO 정보를 끄집어 낸다. 아래는 RAN 시뮬레이터를 통해 입력되는 이동 ISP 가입자 정보이고 이는 편의상 사용자 인터페이스를 통해 선택하도록 하였다.

```
• INPUT SOME CONFIGURATON
  DATA(CHAP = 1, PAP = 2, IP RELEASE = 3) : 1
• Username : bari
• Password : bari
• Wished IP (if you don't have,j ust Enter) :
• Debug level : 3
    1 : Print Just Result
    2 : Print basic Debug Message
    3 : Print All Message(MQ,Socket)

  Auth Method = CHAP Username : bari Password : bari
  WishedIP : Debug level : 3

  Are you sure?(OK = 1, NO = 2) : 1
  chap challenge =
   235bf9f1 28a2b573 2de970f6 33302c78
  chap_resp =
   c4f675b7 744634d1 82ed1c5d 106a5ebd
  cont_chap.length = 25

  Sending a message 92 bytes from RNC Simulator =>
  RADIUS Client

   1406011 005af 00836 0004c
   0001 00011 4380c021 9113c
   935c2 235c223 2a210 1910c4f6
   75b77446 34d182ed 1c5d106a 5ebd6261
   72691023 5bf9f128 a2b5732d e970f633
   302c7880 21636 0000

  Receiving a message from RADIUS Client…
  Receiving message 63

   1406012 00836 005af 0002f
   0001 81fefb21 0001 2380c223
   15310 15415554 48454e54 49434154
   494f4e20 4f4b8021 63681 fefb21

  |*************************************************|
   |TEID = 1 ISPID = 17 : AUTHENTICATION_ACCEPT!
    => Getted IP = 129.254.251.33
  |*************************************************|
   receving protocol id =
   c223

  CHAP MESSAGE = AUTHENTICATION OK

  Get IP in PCO is 129.254.251.33
```

시뮬레이션에서 CHAP Challenge 값은 PCO 데이터 구조 정의에서 처리하도록 하였고 이는 다시 SGSN과 GGSN GTP를 통해 GGSN_ISP 부분까지 전달 되도록 하여 이를 다시 ISP 인증 서버로 보내 인증 결과를 받아오도록 한 것이다. 실제 구축한 환경에서 시뮬레이션을 통해 얻은 인증 결과와 정적 IP 사용 확인 대한 결과가 성공적으로 진행된 것을 위에서 보여주고 있다.

5. 결 론

이동 인터넷 시대, 글로벌 로밍 시대에서 정보화 서비스,

그 중에서도 이동통신망을 통한 무선 인터넷 서비스의 시공간을 초월한 사용 환경 제공을 위한 인터넷과 이동통신망의 결합 추세는 가속화되고 있다. 이동통신 시장의 반 이상을 장악하고 있는 유럽의 비동기 이동 통신 시스템에서도 인터넷과의 통합 환경 구축을 서두르고 있다. 실제 유럽의 패킷 이동통신 서비스 환경으로 제안되고 있는 3세대 GPRS 시스템, 이를 바탕으로 하는 4세대 UMTS 시스템에서는 인터넷 가입자의 이동통신망 접속화 및 All IP 망 구축화 형태로 이미 3GPP 규격화 회의를 통해 상당히 정립되고 있는 실정이다. 이에 본 논문에서는 유선 인터넷 PPP 가입자가 유럽의 패킷 이동통신망인 GPRS 망으로 이동해서 자신의 홈 ISP망에 접속하여 무선 인터넷 서비스를 받으려 할 때 고려되는 문제점을 검토하였다. 대표적으로 ISP 망 가입자가 GPRS 망으로 이동하여 PPP CHAP을 시도하여 홈 ISP 망의 RADIUS 서버 접속을 시도할 때 발생되는 문제로 PPP CHAP Challenge 값의 처리였다. 이에 본 논문에서는 GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 경유하여 ISP RADIUS 서버를 접속할 때 필요한 PPP CHAP 메시지 처리와 이와 관련되어 PPP CHAP과 RADIUS 서버간의 연동 처리 방안을 제시하고 있다. 먼저, 이동 ISP 가입자의 TE에서 PPP CHAP Response 메시지에 CHAP Challenge Value를 넣어 처리하는 방안과 GPRS MT에서 PCO 데이터에 CHAP Challenge Value를 넣어 처리하는 메시지 구조를 제안하였다. 또 GPRS GGSN에서 GTP에 포함된 PCO 데이터에서 MT를 통해 보내온 CHAP Challenge, CHAP ID, 가입자 ID 처리 방안과 이를 ISP RADIUS 서버에 보내기 위한 데이터 구조도 제시했다. 그 밖에 본 논문에서는 GPRS 망으로 이동한 이동 ISP 가입자가 GPRS 망을 통해 홈 ISP 망을 접속하여 무선 인터넷 서비스를 받기 위해 요구되는 이동 패킷 데이터 통신망 노드의 프로토콜 스택과 동작 절차 및 GGSN과 ISP RADIUS/DHCP 서버간에 연동에 필요한 메시지 및 데이터 구조도 제시하고 있다. 또 본 논문에서 제시한 이동 패킷 데이터 통신망에서의 PPP CHAP Challenge Value 처리방안의 가능성 확인을 위해 SGSN과 GGSN, RAN 시뮬레이터, 그리고 ISP RADIUS/DHCP 환경구축을 통해 시뮬레이션을 진행했고 그 내용도 본 논문에서 기술하였다. 따라서 본 논문에서 제안된 내용을 통해 유선 ISP 가입자는 GPRS 망으로 이동했을 경우도 이동성 및 로밍 서비스 지원을 받을 수 있게 되며 나아가 이동 ISP 가입자의 무선 이동 인터넷 서비스 지원도 가능하다. 아울러 기존 유선 인터넷 환경에서 적용되던 PPP CHAP 방식은 본 논문에서 제시한 CHAP Challenge Value 처리와 새로운 패킷 구조를 적용하므로 이동 패킷 통신 환경, 특별히 GPRS 환경에서도 방문 ISP 이동 가입자에게 사용이 가능하다.

참 고 문 헌

[1] 3GPP, "GPRS Service Description, Stage 2," 3G TS 23.060 version 3.3.0, March, 2000.

[2] 3GPP, "GPRS Service Description, Stage 1," 3G TS 22.060 version 3.3.0, March, 2000.

[3] 3GPP, "Combined GSM and Mobile IP Mobility Handling in UMTS IP CN," 3G TR 23.923 version 3.0.0, May, 2000.

[4] 3GPP, "Interworking between the Public Land Mobile Network(PLMN) supporting Packet Based Services and Packet Data Networks(PDN)," 3G TS 29.061 version 3.3.0, March, 2000.

[5] 3GPP, "Mobile radio interface layer 3 specification ; Core Network Protocols-Stage 3," 3G TS 24.008 version 3.4.1, July, 2000.

[6] R. Droms, "Dynamic Host Configuration Protocol(DHCP)," RFC 2131, March, 1997.

[7] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service(RADIUS)," RFC 2865, June, 2000.

[8] William Allen Simpson, "The Point-to-Point Protocol(PPP)," RFC1661, July, 1994.

[9] C. Perkins, "IP Mobility Support," RFC2002, Oct., 1996.

[10] C. Perkins, "IP Encapsulation within IP," RFC2003, Oct., 1996.

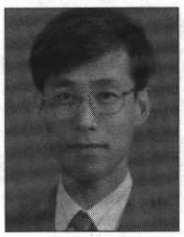
[11] Richard Stevens, "UNIX Network Programming ; Networking APIs : Sockets and XTI Volume 1," 1997.

[12] G McGregor, "The PPP Internet Protocol Control Protocol (IPCP)," RFC1172, May, 1992.

[13] W. Simpson, "PPP Challenge Handshake Authentication Protocol(CHAP)," RFC1994, August, 1996.

[14] W. Simpson, "PPP Authentication Protocols(PAP)," RFC1334, October, 1992.

[15] B. Aboba, "The Network Access identifier," RFC 2486, Jan., 1999.



박 정 현

e-mail : jh-park@etri.re.kr

1982년 숭실대학교 전자공학과 졸업(학사)

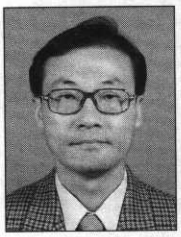
1985년 숭실대학교 대학원 전자공학과 졸업(석사)

1997년 충북대학교 대학원 전자계산학과 졸업(박사)

1994년~1995년 캐나다 MPR Teltech DBS공동 개발 방문연구원

1982년~현재 한국전자통신연구원 책임연구원

관심분야 : 정보보호 프로토콜, IMT-2000 시스템 및 DBS/VSAT 위성 통신 시스템 보안, 무선LAN 보안, 무선 이동 패킷망 간 인터워킹, 우정 정보화 기술 응용 개발



김 영 진

e-mail : yjkim@etri.re.kr

1981년 고려대학교 전자공학과 졸업(학사)

1983년 고려대학교 대학원 전자공학과 졸업 (석사)

1989년~1991년 벨기에 BTM 방문 연구원

1983년~현재 한국전자통신연구원 Global 무선 LAN 연구팀장(책임연구원)

관심분야 : CDMA 시스템, IMT-2000 시스템, IP기반 이동통신 시스템, 무선LAN

이 윤 주

e-mail : yjlee@etri.re.kr, yjlee@bj-etri.com

1974년 숭실대학교 전자공학과 졸업(학사)

1989년 숭실대학교 대학원 전자공학과 졸업 (석사)

1998년 숭실대학교 대학원 전자공학과 졸업 (박사)

1975년 민성전자 주식회사 사원

1977년 대한통신주식회사 사원

1991년~1992년 미국 Virginia Polytech. 대학교 방문연구원

1979년~현재 한국전자통신연구원 북경이동통신연구센터장 (책임연구원)

관심분야 : 로밍 및 연동 방식, IMT-2000 시스템, 이동 통신망 구조

양 정 모

e-mail : jmyang@mail.joongbu.ac.kr

1984년 동국대학교 수학과(학사)

1989년 동국대학교 대학원 수학과 졸업 (석사)

1997년 단국대학교 대학원 수학과 졸업 (박사)

1995년~현재 중부대학교 정보통신공학부 부교수

관심분야 : 응용 수학, 정보 분석, 암호학, 정보통신 보안, 암호 알고리즘 설계