무선 인터넷 환경에서 CHAP 인증 기법을 이용한 로밍 서비스 지원 방법

박정현* · 유승재** · 양정모**

요 약

본 논문에서는 무선 인터넷 환경에서 CHAP 인증 기법을 이용한 로밍 서비스 지원 방법을 기술한다. 이를 위해 특별히 GPRS 망으로 이동한 이동 ISP 망 가입자가 자신의 홈 ISP 망을 접속하여 인증을 받기 위한 기법을 제시한다. 또 이동 ISP 망 가입자의 단말에서 정의되어야 할 인증 메시지 구조와 GPRS 망 게이트웨이에서 구현될 메시지 구조를 제시한다. 아울러 GGSN과 ISP 망간의 인증 메시지 구조를 정의하며 이들 제안된 내용에 대해 시험 환경 구축을 통해 실제 시뮬레이션 결과를 보였다.

Roaming Service Support Technique using CHAP in Wireless Internet

Jeong-Hyun Park* · Seung-Jae Yoo** · Jeong-Mo Yang**

ABSTRACT

We describe CHAP authentication for roaming service method of visited ISP subscriber on GPRS network. We also illustrate how visited mobile ISP subscriber can access ISP server and authenticate RADIUS in home network via Gateway GPRS Support Node (GGSN) on GPRS/UMTS network for wireless internet service and roaming. For this we propose the modified CHAP message format, PCO Message format at MT, and interworking message and format betweenGGSN 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 CHAP at GPRS network accesses the RADIUS server in home ISP network.

Key words : Roaming Service, Wireless Internet, CHAP

* 한국전자통신연구원

** 중부대학교 컴퓨터공학부 정보보호학과

1. 서 론

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 ISP망 가입자에 대한 로밍 서비스를 제공하며, Mobile IP[2] 서비스의 제공을 위한 Mobile IP 시스템도 정의하고 있다.

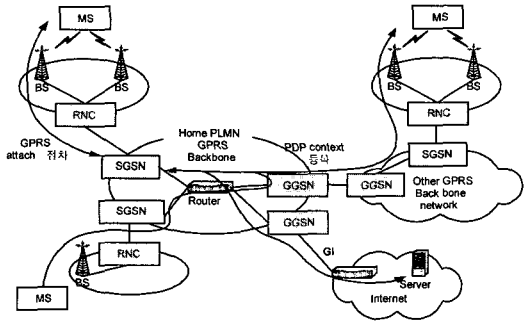
ISP 망 가입자가 GPRS 이동망에 접근하였을 때, GPRS 시스템은 3GPP 규격[1]에 정의된 바와 같이 Gi 인터페이스를 통해 GPRS망 가입자가 아닐지라도 ISP 가입자에 대해 인증 과정 및 ISP내의 IP 할당과정을 대리적으로 수행하고 패킷 전송을 위한 베어러를 열어 주는 작업을 수행한다. 이동 ISP 가입자가 무선 인터넷 서비스를 받기 위해 홈 ISP 망의 인증 서버를 통해 인증을 받는 기법은 기존 유선 통신망 환경에서와 다소 차이가 발생된다.

본 논문에서는 UMTS/GPRS망으로 이동한 이동 ISP 망 가입자가 자신의 홈 ISP(Internet Service Provider) 망 접속을 통해 무선 인터넷 서비스를 받기 필요한 인증 방법을 제시한다. 2장에서는 UMTS/ GPRS 망으로 이동 ISP 망 가입자의 무선 인터넷 접속에 대해 설명하고 3장에서는 UMTS/GPRS으로 이동한 이동 ISP 가입자의 무선 인터넷 서비스를 위한 인증 기법을 기술한다. 아울러 4장에서는 UMTS/GPRS으로 이동한 이동 ISP 가입자의 무선 인터넷 서비스를 위한 인증 방법을 검증하고 시험한 시험 환경과 시뮬레이션 결과를 제시하며 5장에서는 결론을 기술한다.

2. UMTS/GPRS망으로 이동한 이동 ISP 가입자의 무선 인터넷 접속

3세대 이동 통신망은 음성 서비스와 패킷 데이터 서비스를 분리하여 서비스를 제공하며 핵심 망에 IP기반의 GPRS 망을 구성하고 다른 패킷 데이터망과 연동하여 종단간 패킷 데이터 서비스를 제공한다. 아래 (그림 1)은 GPRS 망에서 데이터 서비스를 나타내며 (그림 2)는 GPRS망으로 이동한 이동 ISP 가입자의 무선 인터넷 접속을 위한 사전 동작 절차를 나태 낸다.

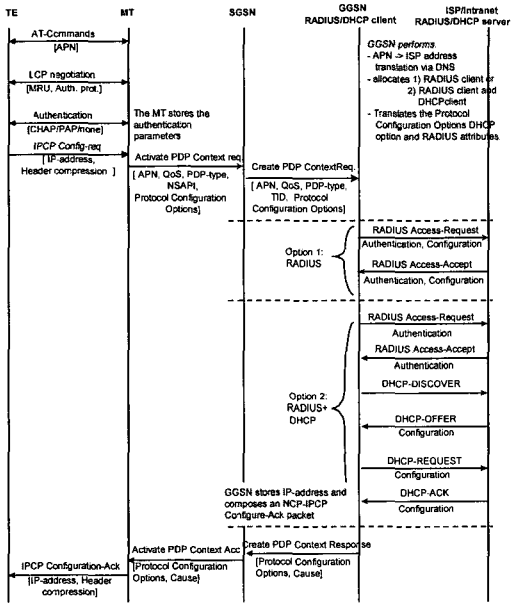
이동단말(MS : mobile station)은 MT(Mobile Terminal)와 MT에 응용서비스를 제공하는 TE (Terminal Equipment)로 구성되며 RNC(Radio Network Cont-roller)와 무선 채널로 연결되어 회선 및 패킷 모드의 서비스를 제공 받는다. SGSN은 이동단말의 MM(Mobility Management) context를 설정하여 이동단말의 위치 및 보안 정보를 관리하며 이동단말의 PDP(Packet Data Protocol) context를 설정하여 GTP 터널링을 통해 데이터 서비스를 한다. GGSN은 이동단말의 PDP context를 유지하고 외부 IP 망과 연동을 위해 이동단말의 IP 주소 할당 및 관리 등의 IP 라우팅 기능을 하는 게이트웨이 역할을 한다. PDP context에는 이동단말의 PDP type (e.g. IPv4, IPv6, X.25)과 주소정보, QoS 프로파일 등의 정보를 포함하고 있다. HLR은 이동단말의 서비스 프로파일을 복사 및 저장하는 홈 네트워크에 위치한 데이터 베이스이며, MSC는 회선 교환 서비스를 위한 스위칭과 위치 정보 관리 기능을 수행하며, VLR은 자신이 소속한 GPRS망에 존재하는 이동단말에 대한 정보를 일시적으로 저장하고 HLR과 동일한 데이터를 유지한다[1, 3]



(그림 1) UMTS/GPRS 데이터 서비스

이동 ISP 가입자가 GPRS망으로 이동해 온 경우 이동 ISP 가입자는 GPRS망을 통해 무선 인터넷 서비스를 받기에 앞서 홈 ISP 망에 속하여 먼저 인증과 IP 주소를 받아야 한다. 이러한 주소는 정적인 경우 인터넷 서비스 가입시에, 동적인 경우 GPRS망에서 PDP Context Activation시에 이루어진다. 이 경우 GPRS GGSN은 ISP의 RADIUS[4] 및 DHCP[5,6] 서버와의 직접적인 연동을 하는 기능을 가져야 한다. 이를 위해 이동 ISP 가입자는 PDP Context Activation시에 인증 요구 및 개인 정보를 GGSN에게 전달해야 하는데 이것은 GTP의 Information Element내의 PCO을 통하여 이루어 진다. GGSN은 외부 ISP의 RADIUS/DHCP 서버와 직접 연동하여 인증 및 주소 할당 과정을 수행한다. (그림 2)에서 이동 ISP가입자가 GPRS망을 통해 홈 ISP망내 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 저장 한다. 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 APN [9]을 해석하여 해당 ISP를 구분하고, 또한 이 ISP에 인증 및 IP할당을 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 부여 받는다. 이때 GGSN은 인증과 IP할당에 성공했을 경우, TE로부터 요청된 IPCP내의 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 IPCP결과에 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 동적 IP를 획득하여 TE에 전달할 경우 동적 IP에 대해 할당 시간(Lease Time)을 함께 부여 받게 되는데, 이 경우 GGSN은 세션이 종료되기 이전까지 해당 IP의 갱신(Renewing)을 위해 할당 시간을 계속적으로 연장하는 기능을 담당해야 한다. 이것은 할당시간이 만료되기 이전에 주소 할당 서버(RADIUS 혹은 DHCP)에 갱신 메시지를 보냄으로써 이루어 질

수 있다. 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 ISP의 IP 자원 관리 및 과금 관리 차원에서 해당 주소 할당 서버에 IP 해제 메시지를 전송하여야 한다. 이는 DHCP Release메시지를 보냄으로써 이루어 질 수 있다.



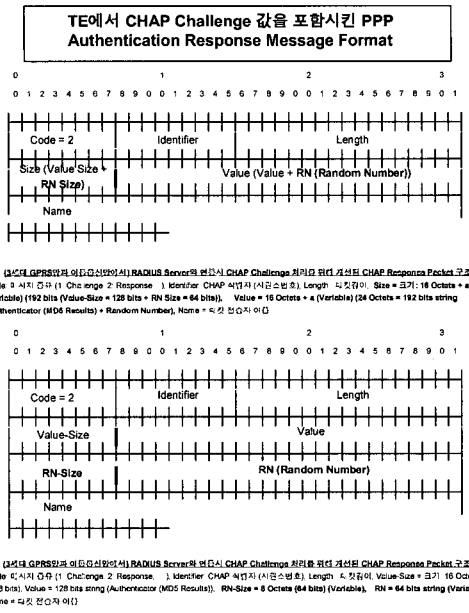
(그림 2) GPRS 망으로 이동한 이동 ISP 가입자의 무선 인터넷 접속

3. UMTS/GPRS으로 이동한 이동 ISP 가입자의 무선 인터넷 서비스를 위한 인증 기법

이동 ISP 가입자가 GPRS망을 통해 홈 ISP망의 접속하여 인증을 받기 위해 시도하는 PPP CHAP 메시지는 수정되어야 한다. 즉, 이동 ISP 가입자가 GPRS망을 경유하여 홈 ISP 망의 접속을 통해 무선 인터넷 서비스를 시도할 때 먼저 이동 ISP 가입자 TE와 GPRS의 MT사이에 PPP 링크 설정이 이루어지고 이어 PPP CHAP을 통해 GPRS에서 MT에서는 이동 ISP 가입자에 대한 가상 인증을 실행한다. 이어 MT는 TE에서 보내온 ISP 인증 정보를 GPRS망을 경유하여 홈 ISP망으로 보내 이동 ISP 가입자에 대한 실제 인증을 행한다. 이때 TE에서 MT로 보내는 PPP CHAP Response 메시지에는 ISP 홈 망 내 RADIUS 서버에서 이동 ISP 가입자의 실제 인증에 반드시 필요한 CHAP Challenge 값을 포함하고 있지 않다. 이를 위해 기존의 PPP CHAP Response 메시지는 수정되어야 하며 혹은 GPRS MT에서의 PCO 데이터 구조를 수정하여야 한다.

3.1 TE에서 PPP CHAP 메시지 변경

GPRS망으로 이동한 이동 ISP 가입자가 GPRS망을 접속할 때 이동 ISP 가입자 TE와 GPRS MT 사이는 PPP 링크 설정과 이동 ISP 가입자에 대한 가상 인증이 진행된다. 이때 TE는 PPP Client, MT는 PPP Server의 역할을 하게 되며 특별히 TE에 대한 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 ISP망의 RADIUS 서버로 보내져 이동 ISP 가입자에 대한 최종 인증이 진행되어야 한다. 아래 (그림 3)은 GPRS망으로 이동한 이동 ISP 가입자의 실제 인증을 위해 필요한 CHAP Challenge 값 처리를 위한 메시지 구조이다. (그림 3)에서 첫 번째 방안은 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.

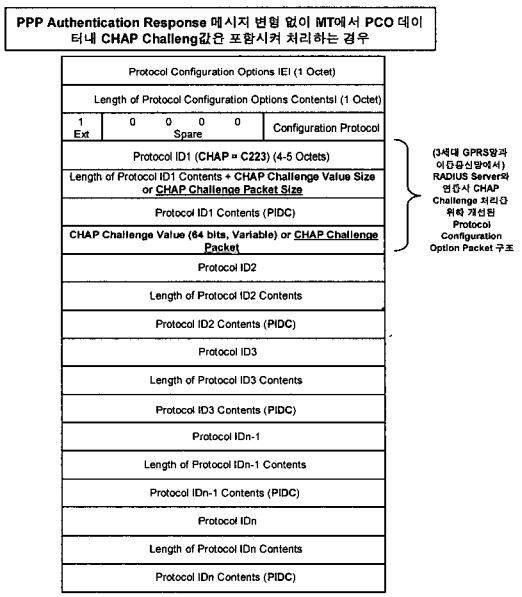


(그림 3) TE에서 PPP CHAP Response 메시지 구조

이렇게 하므로 CHAP Challenge 값은 ISP 홈 망의 RADIUS 서버로 보내져 GPRS망으로 이동한 이동 ISP 가입자에 대한 실제 인증에 사용되고 이를 통해 GPRS 망으로 이동한 이동 ISP 가입자는 홈 ISP망을 접속하여 무선 인터넷 서비스를 제공 받게 된다.

3.2 MT의 PCO 데이터 구조 변경

GPRS망으로 이동한 이동 ISP 가입자에 대해 홈 ISP망 내 RADIUS 서버에서 실제 인증시 필요한 CHAP Challenge 값을 MT의 PCO 데이터 구조에서 정의하여 처리하는 방안도 가능하다. 원래 MT는 TE에서 보내온 CHAP Response 메시지를 그대로 PCO 필드에 부쳐 GPRS 망 게이트웨이 노드인 GGSN으로 보내게 되는데 이때 TE에서 보내온 CHAP Response 메시지 내에는 CHAP Challenge 값이 포함되지 않는다. 따라서 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 GPRS망으로 이동한 경우 새로운 형태의 PPP CHAP Response 메시지의 처리가 가능해야 하는 어려움도 따르게 된다. 이에 PPP CHAP Challenge 값을 GPRS MT의 PCO 데이터 필드에서 미리 정의하여 처리하면 앞의 번거로움 없이 GPRS 망으로 이동한 이동 ISP 가입자에 대한 인증 정보 처리가 가능하다. (그림 4)는 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.

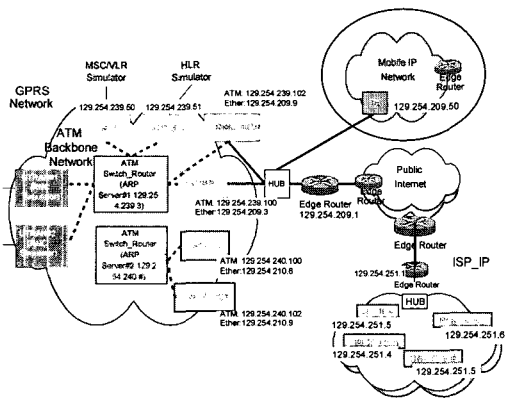


(그림 4) MT PCO 구조에서 PPP CHAP Response 처리 구조

4. 무선 인터넷 환경에서 CHAP 인증 기법을 이용한 로밍 서비스 지원 기법 구현

4.1 환 경

SGSN과 GGSN을 구현과 RNC 시뮬레이터를 통해 GPRS 핵심망 환경 구축을 하였고 ISP 내 인증 서버와 웹 서버 구현을 통해 ISP망 환경을 구축하였다. 그리고 RNC 시뮬레이터는 MT대신 가상의 PPP 인증 서버 역할을 대신하며 그 결과로 PPP PCO 데이터를 준비하며 이는 SGSN으로 보내는 PDP Context 메시지 내 포함하여 SGSN과 GGSN으로 전송하도록 하였다. 또 SGSN과 GGSN사이는 155Mbps ATM 인터페이스로 링크가 설정되었고 GGSN과 ISP망 사이는 IP를 기준으로 Fast Ethernet 으로 구성하였다. 아래 (그림 5)는 PPP CHAP을 통해 SGSN, GGSN, 그리고 ISP 인증 서버까지의 통신 환경을 보여준다.



(그림 5) 시뮬레이션 환경

• TE에서 정의한 정보

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

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

• MT에서 PCO 메시지 정보

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

• RADIUS 서버 환경

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

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

- 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,

4.2 시뮬레이션

시뮬레이션을 위해 GPRS망으로 이동한 이동 ISP 가입자의 TE에서 MT로 자신의 인증 및 개인정보를 보낼 때 포함되는 정보를 SGSN에 준비된 RAN 시뮬레이터를 통해 처리하였다. 이어 RAN 시뮬레이터를 통해 입력된 정보는 SGSN GTP를 통해 GGSN으로 전달되고 GGSN에서는 전달된 GTP에서 RAN 시뮬레이터에서 입력한 PCO 정보를 끄집어 낸다. RAN 시뮬레이터를 통해 입력되는 이동 ISP 가입자의 정보이고 이는 편의상 사용자 인터페이스를 통해 선택하도록 하였다.

시뮬레이션 결과는 CHAP Challenge 값을 PCO 메시지에 정의하여 처리하도록 하였고 이를 구현한 SGSN과 GGSN GPT를 통해 GGSN ISP 부분까지 전달되도록 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.

INPUT SOME CONFIGURATON DATA
(CHAP = 1, PAP = 2, IP RELEASE = 3) : **1**
Username : **bari**
Password : **bari**
Wished IP (if you don't have, just Enter) :
Debug level : **3**
1 : Print Just Result
2 : Print basic Debug Message
3 : Print All Message(MQ,Socket)
AuthMethod=CHAP Username:bari
Password : bari WishedIP : Debuglevel : 3
Are you sure?(OK = 1, NO = 2) : 1
chapchallenge=
235bf9f1 28a2b573 2de970f6 33302c78
chap_resp=
c4f675b7 744634d1 82ed1c5d 106a5ebd
cont_chap.length=25
SendingamessageofbytesfromRNC
Simulator=>RADIUSClient
1406011 005af 00836 0004c
0001 00011 4380c021 9113c
935c2 235c223 2a210 1910c4f6
75b77446 34d182ed 1c5d106a 5ebd6261
72691023 5bf9f128 a2b5732d e970f633
302c7880 21636 0000
ReceivingamessagefromRADIUSClient....
Receiving message 63
1406012 00836 005af 0002f
0001 81fefb21 0001 2380c223
15310 15415554 48454e54 49434154
494f4e20 4f4b8021 63681 fefb21
TEID = 1ISPID = 17:AUTHENTICATION_
ACCEPT!=>GettedIP=129.254.251.33
recevingprotocolid=c223
CHAPMESSAGE=AUTHENTICATIONOK
GetIPinPCOis129.254.251.33

5. 결 론

본 논문에서는 GPRS망으로 이동한 이동 ISP 가입자가 GPRS망을 경유하여 ISP RADIUS 서

버를 접속할 때 필요한 PPP CHAP 메시지 처리와 이와 관련되어 PPP CHAP과 RADIUS 서버간의 연동 처리 방안을 제시하고 있다. 이를 위해 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. 본 논문에서 제시한 PPP CHAP Challenge 방안은 구현되어 SGSN과 GGSN, RAN 시뮬레이터, 그리고 구축한 ISP RADIUS/DHCP 환경을 통해 시뮬레이션을 진행했으며 그 결과도 본 논문에서 보였다.

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.

박 정 현

1997년 충북대학교 전자계산학과 이학박사

1982년~현재 한국전자통신연구원 물류기술연구팀장 (책임연구원)

유 승 재

1998년 동국대학교 수학과 이학박사

1997년 현재 중부대학교 정보보호학과 부교수

양 정 모

1997년 단국대학교 수학과 이학박사

1995년~현재 중부대학교 정보보호학과 부교수