

RADIUS 인증 및 과금 서버를 이용한 IP 관리 방법

박 정 현[†]

요 약

GPRS 망으로 이동한 이동 ISP 가입자가 무선 인터넷 서비스를 제공 받기 위해 필요한 IP 할당과 인증 문제점을 알아보고 그 해결 방법으로 인증 및 과금 기능을 가진 RADIUS 인증 및 과금 서버를 이용한 IP 관리 기법을 제안하였다. 제안된 RADIUS 인증 및 과금 서버를 이용한 IP 관리 기법을 통해 GGSN은 할당된 IP의 갱신(할당시간 연장) 및 해제의 과정을 수행할 수 있도록 하고 지속적인 무선 인터넷 서비스 지원 및 IP 자원 관리를 가능하게 하며 이를 위해 ISP 내 RADIUS 서버와의 연동 신호를 정의하였다.

IP Management Method Using RADIUS Authentication and Accounting Servers

Jeong-Hyun Park[†]

ABSTRACT

This paper describes the requested IP assignment and authentication problem for wireless internet service of visited ISP subscriber on GPRS network, and proposes to use RADIUS authentication and accounting server for these problems. In this paper, we also define signals between GGSN and RADIUS, and between RADIUS authentication server and accounting sever for IP management and wireless internet service.

키워드 : RADIUS 인증 및 과금 서버(RADIUS Authentication and Accounting Server), DHCP, 동적 IP(Dynamic IP), GPRS/UMTS

1. 서 론

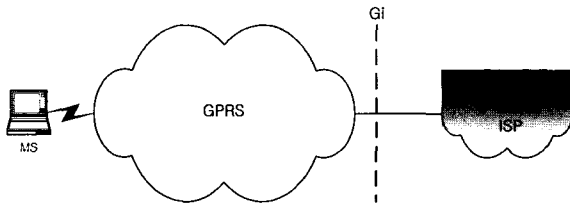
3GPP에서 표준화 되고 있는 제 3세대 이동통신 시스템인 UMTS(Universal Mobile Telecommunication System)는 인터넷과 같은 패킷 데이터 서비스를 제공하기 위해 GPRS(General Packet Radio Service)[1] 시스템을 정의하고 있다. GPRS 시스템은 패킷 스위치 기능을 수행하는 SGSN(Serving GPRS Support Node)과 GGSN(Gateway GPRS Support Node)간 통신을 위해 IP 기반의 자체 백본 망을 가지고 있다. 또한 GPRS 시스템은 ISP(Internet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

이어 GPRS 망 내 GGSN은 ISP 망내서 각각 별도로 관리 및 운영되고 있는 인증 서버와 IP 관리 서버를 통해

GPRS 망으로 이동한 이동 ISP 가입자의 인증과 IP 할당에 대한 처리를 지원한다. 이 경우 ISP 망내에서 운영되는 인증 및 과금 서버로 RADIUS를 이용할 수 있고, IP 관리 서버로는 DHCP를 이용할 수 있다. 그러나 고정 IP를 사용하는 이동 ISP 가입자의 경우는 ISP 내 DHCP 서버와의 연결 접속이 필요하지 않다. 그리고 동적 IP를 사용하는 이동 ISP 가입자는 ISP 내 RADIUS 서버를 통해 1차 인증을 거치고 이어 DHCP 서버를 통해 IP 할당을 받아야 한다. 이를 위해 ISP 망 RADIUS 서버와 DHCP 서버는 이동 GPRS 망으로 이동한 이동 ISP 가입자에게 무선 인터넷 서비스 제공을 위해 별도의 상호 신호 교환 기능이 필요하게 된다. 이후 GPRS 망으로 이동한 이동 ISP 가입자가 ISP 망 내 DHCP 서버를 통해 정해진 사용 시간에 대해 할당된 IP를 부여 받아 무선 인터넷 서비스를 받게 되며 이후 정해진 시간이 지나면, GPRS망 내 GGSN과 DHCP사이에는 IP 사용 시간 연장을 위한 신호 교환이 필요하다. 그러나 현재까지 정의된 DHCP 서버는 GPRS 망으로 이동한 이동 ISP 가입자에게 동적 IP를 부여하는 경우처럼 서로 다른 서브넷 상에서는 ISP 내 IP를 부여해 줄 수 없게 된다. 이를 위해 GPRS 망내 GGSN과 ISP 망내 별도의 특정 DHCP Relay가 필요하고 이 특정 DHCP Relay를 통해 GPRS 망 내 GGSN과 ISP 망내 DHCP서버와 상호 신호 연계를 하게 된다. 이런 불편함을 없애기

[†] 정 회 원 : 한국전자통신연구원 u-Logistics연구팀, 책임연구원
논문접수 : 2003년 1월 20일, 심사완료 : 2004년 9월 13일

위해 본 논문에서는 ISP 망내 인증 및 과금 서버인 RADIUS 서버에 IP 관리 기능을 부여하고 이를 위한 신호 정의를 제시한다. 또 GPRS 망으로 이동한 이동 ISP 가입자가 무선 인터넷 서비스를 위해 요구되는 동적 IP 할당 시 DHCP 서버 이용 문제점과 이에 대한 해결 방안도 제시하고 있다.



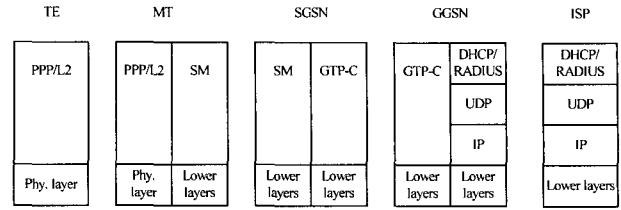
(그림 1) GPRS망과 ISP 연동

위 (그림 1)에서 GPRS 망에는 무선 액세스망과 정합되어 패킷 호 처리 및 세션 관리, 이동성관리 기능을 담당하는 SGSN이 있고, 세션 및 이동성 관리 기능을 담당하는 GGSN이 있다.

본 논문에서는 GPRS망으로 이동한 이동 ISP 가입자의 무선 인터넷 서비스 제공을 위한 일반적인 신호 절차와 프로토콜 스택을 2장에서 기술하고, GPRS 망으로 이동한 이동 ISP 가입자에게 무선 인터넷 서비스를 제공하기 위해 홈 ISP 망의 RADIUS(Remote Authentication Dial In User Service) 인증 서버 및 DHCP(Dynamic Host Configuration Protocol)와 GGSN과 연동시 야기되는 문제점을 3장에서 기술하며, 4장에서는 이런 문제점을 해결하기 위한 방안으로 RADIUS 인증 및 과금 서버를 이용하는 방법과 이에 필요한 세부 연동 신호 정의를 제시한다. 이어 마지막으로 5장에서 결론을 기술한다.

2. GPRS망으로 이동한 이동 ISP 가입자의 ISP 망 접속

이동 ISP 가입자가 GPRS 망을 방문하여 GPRS 망을 통해 무선 인터넷 서비스를 받기 위해서는 먼저 홈 ISP 망을 통해 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 PCO를 통하여 이루어진다. GGSN은 외부 ISP의 RADIUS/DHCP 서버와 직접 연동하여 인증 및 주소 할당 과정을 수행한다. (그림 2)는 GPRS망으로 이동한 이동 ISP 가입자가 GPRS망을 경유하여 ISP 접속의 경우 망의 각 노드에 대한 프로토콜 스택이며 (그림 3)은 이동 ISP가입자가 GPRS 망을 통해 홈 ISP 망 내 RADIUS 인증 서버와 DHCP 서버의 접속을 시도하는 경우에 대한 신호 절차이다.



(그림 2) GPRS망으로 이동한 이동 ISP가입자의 홈 ISP망 접속시 신호 프로토콜

Reject 메시지를 구성한다. 이후 GGSN은 이러한 IP 주소 정보를 저장하고 이 정보를 바탕으로 PCO를 구성하여 Create PDP Context Response를 SGSN으로 전송한다. SGSN은 Activate PDP Context Accept를 MT에 전송하고, 이후 MT는 PCO 내의 IP 주소 정보를 읽어 IPCP 결과에 따라 TE와 MT사이의 국부적인 협상을 통해 IP 주소를 전달하게 된다.

그런데 TE가 무선 인터넷 서비스를 받기 위해 동일 IP 주소를 계속적으로 사용하여 무선 인터넷 서비스를 받기 위해서는 IP 주소 사용에 대한 할당 시간(Lease time)이 만료되기 이전에 IP 주소 할당 시간을 연장하는 기능이 필요하다. 따라서 GGSN은 홈 ISP 내 DHCP서버를 통해 할당 받은 동적 IP 주소를 획득하여 TE에 전달한 경우 이러한 동적 IP에 대해 할당 시간을 함께 부여 받게 되는데 이 경우 GGSN은 세션이 종료되기 이전까지 해당 IP 주소의 갱신(Renewing : 할당 시간 연장)을 위해 할당 시간을 계속적으로 연장하는 기능을 담당해야 한다. 이것은 할당 시간이 만료되기 이전에 홈 ISP 망 내 IP 주소 할당 서버(DHCP)에 갱신 메시지를 보냄으로써 이루어 질 수 있다. 따라서 GGSN도 ISP망 내에서 할당 받은 동적 IP 주소에 대해 IP 주소 할당 시간 연장을 위해 내부적으로 타이머를 구동 시키며 주기적으로 할당 연장을 위한 메시지를 전송해야 한다.

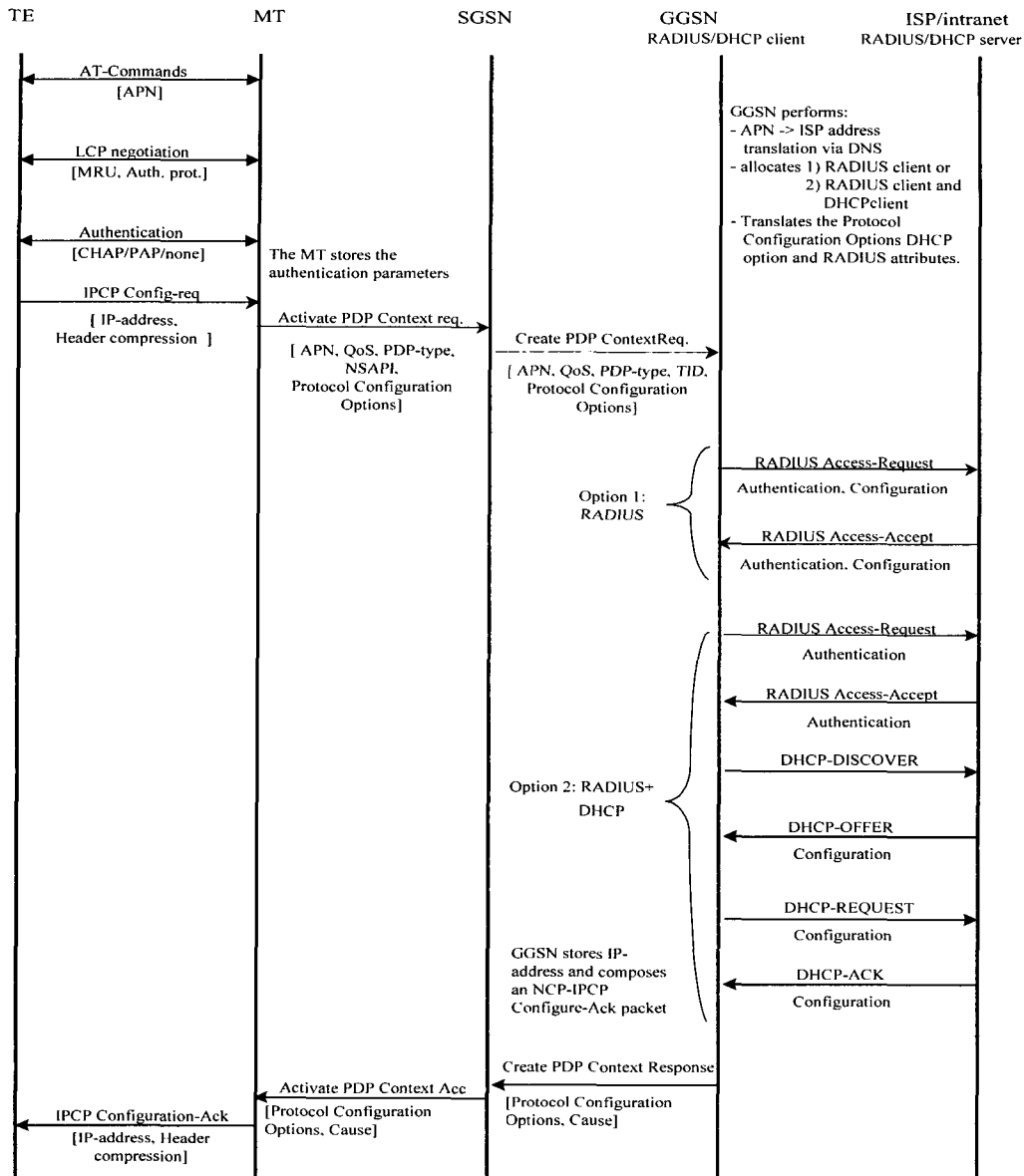
또한 TE가 세션을 종료한 경우 GGSN은 ISP의 자원 및 과금 관리 차원에서 해당 IP 주소 할당 서버에 IP 주소 해제 메시지를 전송하여야 한다. 이는 DHCP Release 메시지를 보냄으로써 이루어 질 수 있다.

3. GPRS 망을 방문한 이동 ISP 가입자의 IP 할당시 문제점

본 절에서는 GPRS 망을 방문한 이동 ISP가입자가 무선 인터넷 서비스를 위해 요구되는 IP 할당시 문제점을 살펴본다.

가. RADIUS 인증 서버만을 이용하는 경우

ISP망을 사용하기 위해 RADIUS 인증서버에 접속하는 경우는 RADIUS 서버의 접속을 통해 인증 결과뿐만 아니라 IP 주소 정보도 함께 얻어내야 한다. 이러한 IP 주소 할당을 위해 RADIUS 메시지의 속성(Attribute) 중 Framed-IP 필드가 사용될 수 있다.



(그림 3) GPRS망으로 이동한 이동 ISP가입자의 홈 ISP 망 접속시 신호 절차

GGSN은 먼저 PCO(Protocol Configuration Options) 내에서 인증 종류(PAP or CHAP)와 인증 정보(사용자 이름 및 암호) 및 IP 정보(정적 IP 혹은 동적 IP)를 읽어 낸다. 이를 바탕으로 GGSN은 RADIUS 인증 서버에 Access-Request를 구성하고 그 속성에 인증 정보를 RADIUS 프로토콜 형식에 맞게 기입하고 요구된 IP가 있는 경우 Framed-IP에 이 값을 넣는다. 그러나 이러한 요구에 대해서 RADIUS 서버측에서는 인증정보 이외의 다른 정보는 서버 내에 기재되어있는 정보에 의해 결정되므로 이러한 클라이언트에서의 속성 설정은 참고 수준으로 끝나게 되어있다. 그래서 Access-Request를 받은 RADIUS 인증 서버는 인증정보를 통해 사용자의 인증을 시도하고 성공적인 결과가 나왔을 때 해당 사용자의 정보를 기초로 하여 Access-Accept 메시지의 속성을 결정한다.

이때 Framed-IP를 이용하여 할당된 IP를 전달한다. GGSN은 이 Accept메시지의 인증 결과 및 할당된 IP 주소를 바탕으로 SGSN에 세션 생성 성공을 보고한다.

그런데 만약 RADIUS 서버가 단말에 동적 IP 주소를 할당해야 하는 경우 RADIUS 서버는 특정 주소 할당 Pool내에서 동적 IP 주소 할당 기능을 수행하여야 한다. 이 경우 자체적으로 IP 주소 할당 기능을 하며 lease pool을 관리하고 또한 DHCP와 ISP망 내부적으로 연동하여 IP를 할당시킬 수 있어야 한다. 또 다른 방법으로 RADIUS 서버가 Framed-IP를 0xffffffff로 지정하여 NAS(Network Access Server)가 직접 지정토록 할 수 있다.

그러나 RADIUS 서버가 직접 IP를 할당하는 경우에 IP 주소 갱신 메시지에 대한 구체적인 방안이 마련되어야 하

며 특히 IP 해제 메시지에 대해서는 RADIUS 프로토콜로는 구현할 수가 없는 문제가 발생하게 된다. 또한 NAS가 할당하는 경우는 GGSN이 ISP의 IP 주소를 할당해야 하는 경우이므로 원칙적으로 불가능한 경우이다. 그러므로 RADIUS 서버만을 접속하는 경우는 동적 IP 할당에 대한 관리가 불가능하게 된다.

나. RADIUS와 DHCP 서버를 이용하는 경우

이동 ISP 가입자가 GPRS망을 경유하여 ISP망내 동적 IP 주소 할당을 받기 위해 RADIUS 인증 서버를 거친 후 독립적으로 존재하는 DHCP 서버를 접속하는 경우는 두 서버의 기능 구분이 비교적 명료하다. TE에서 세션 활성화요구가 들어오면 GGSN은 세션 생성 요구 메시지의 PCO 내에서 인증 정보 및 IP 주소 정보를 얻는다. 이 인증 정보를 통해 GGSN은 먼저 RADIUS 서버에 Access-Request 메시지를 보내어 인증을 요구한다. 이때 IP 주소 할당에 대한 정보는 메시지 속성 내에 기재하지 않는다. 이 인증이 성공한 경우 GGSN은 다시 DHCP 서버에 접속하여 IP 주소를 할당 받는 일련의 과정을 수행해서 동적 혹은 정적 IP 주소 할당 및 할당 시간을 부여 받는다. GGSN은 동적 IP 주소 할당인 경우 타이머를 구동하여 이 IP 주소의 할당 시간이 만료되기 이전에 IP 주소 연장 메시지(DHCP Request)를 주기적으로 전송한다. 또한 세션이 종료된 경우에는 IP 주소 해제 메시지(DHCP Release)를 보내어 IP 주소 사용이 끝났음을 DHCP 서버에 알리며 이후에는 IP 주소 연장 메시지를 보내지 않아야 한다.

그러나 이 경우 DHCP의 속성상 몇 가지 문제점이 발생하게 된다. 일단 GGSN이 DHCP 클라이언트의 형식으로 홈 ISP망내의 DHCP 서버를 직접 접속하는 경우 DHCP 서버는 이 요청을 같은 서브넷 내부의 DHCP 클라이언트의 요청으로 간주하고, DHCP 속성에 따라 응답 메시지(DHCP OFFER)를 내부 서브넷에 방송(Broadcast)하게 된다. 결국 서브넷 내부에서만 방송되는 응답메시지는 GGSN에 도달되지 못하며 GGSN은 IP 주소 획득에 실패하게 된다. 또한 설사 GGSN이 DHCP 클라이언트로서 IP 주소를 할당 받을 수 있다 해도 GGSN 경우는 하나 이상의 IP 주소를 할당 받을 수 없어 GPRS망으로 이동한 ISP 가입자에게 홈 ISP망의 동적 IP 주소 할당에 대한 중계를 할 수가 없다.

다른 시도로서 GGSN을 DHCP Relay Agent 형식으로 사용할 수 있다. 이 때에는 DHCP Request 헤더내의 giaddr 필드에 GGSN의 IP 주소를 기입하여야 한다. 이 메시지를 받으면 DHCP 서버는 이를 DHCP Relay Agent에서 전송된 것으로 간주하고 IP 주소를 할당한 후 GGSN으로 직접 응답메시지(DHCP offer)를 unicast하게 된다. 그러나 이 경우 DHCP 속성상 DHCP 서버에서 할당된 IP 주소는 Relay agent가 속해 있는 서브넷 즉 GGSN이 속해 있는 서브넷의 IP pool내에서 할당된 값이 된다. 다시 말해 이러한 경우에 TE는 ISP 서브넷 내의 IP 주소가 아니라 GGSN의 서브넷 내의 IP 주소를 할당 받게 된다. 이것은 DHCP에 특별한 기

능 추가가 없는 한 이동성(Mobility)을 가진 단말에 서비스를 제공하지 못하는 한계를 가짐으로써 발생하는 상황이다. 결국 이러한 경우 GGSN은 ISP에서 할당하는 IP 주소를 제공 받지 못하게 된다. 이에 대한 해결책으로는 ISP망 내에 메시지 Relay를 설치하는 방안이 있을 수 있다. <표 1>에 위의 두 경우에 대한 기능 및 문제점을 나타내었다.

<표 1> RADIUS와 DHCP 서버 이용시 ISP망 IP 사용 기능 및 문제점

기능	RADIUS ONLY	RADIUS+DHCP
IP 할당	가능	가능
IP 갱신	방안제시 필요	가능
IP 해제	불가	가능
ISP망 IP사용	가능	불가

4. GPRS 망을 방문한 이동 ISP 가입자의 IP 할당 해결 방법

3장에서 지적한 문제점을 해결하는 방안으로 ISP망 내에 별도의 DHCP 서버가 없이 RADIUS 서버만 존재하는 경우와 주소 할당을 담당하는 DHCP 서버가 존재하는 경우에 대해 각각 그 IP 관리 과정을 제안한다.

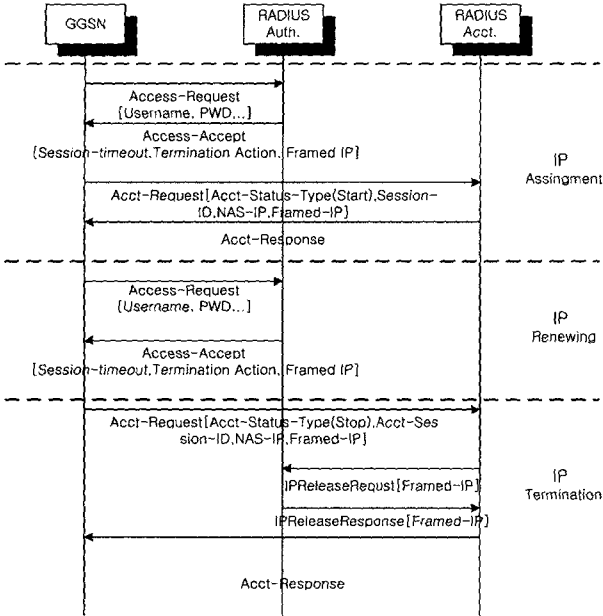
4.1 RADIUS 서버만을 이용한 처리 기법

RADIUS 서버만을 접속하는 경우 RADIUS 과금 서버와의 연동을 통해 IP 할당, 갱신 및 해체에 대한 기법을 제안한다. 이 때 RADIUS 과금 서버는 ISP망 사용에 대한 과금 정보 수집에도 사용되어질 수 있다.

■ RADIUS 서버를 통한 IP할당

(그림 4)에 RADIUS 인증 서버(RADIUS Auth.) 및 과금 서버(RADIUS Acct.)를 이용한 IP 할당, 갱신 및 해제 과정의 흐름을 나타내었다. 먼저 GGSN은 RADIUS 인증 서버에 Access-Request 메시지를 전송하여 인증을 요구한다. RADIUS 인증 서버는 그 이전에 이 GGSN에 대해 NAS로서의 정보를 가지고 있어야 하며, 이 정보를 통해 해당 GGSN과의 Shared Secret Key를 얻고 동적 IP 주소 할당을 요구할 수 있는 NAS임을 확인한다. 또한 사용자의 Username 및 암호를 통해 사용자 정보를 검색하여 사용자를 인증하고 또한 사용자 속성에 관한 부가적인 정보들을 얻는다. 이러한 사용자의 정보에 따라 IP 주소의 할당 여부 및 할당의 정적 혹은 동적 여부를 결정한다. 여기서 RADIUS 서버는 기존 NAS들과 GGSN과의 서비스의 구별을 위해 NAS별로 구분된 서비스를 설정할 필요가 있다. 예를 들어 사용자의 Framed-IP가 0xffffffe인 경우는 RADIUS 규격에 따라 IP 할당을 NAS (여기서는 GGSN)가 하는 경우이다. 이런 경우 GGSN에서는 ISP의 IP 주소를 할당할 수 없으므로 '정적 혹

은 동적 IP 주소 할당'으로 변경하여 RADIUS 자체적 혹은 DHCP연동을 통해 IP 주소를 할당할 수 있도록 서비스를 구별하는 방안이 제시될 수 있다.



(그림 4) RADIUS 인증 및 과금 서버를 이용한 IP 관리 과정

인증이 성공적으로 끝나고 사용자의 요구와 관계없이 서버에 기록된 사용자 정보 중 할당해야 할 IP 주소가 있는 경우(Framed-IP) RADIUS 인증 서버는 정적인 경우에는 지정되어 있는 IP 주소를 할당하고, 동적인 경우에는 이전에 해당 사용자에게 할당되었던 IP 주소 정보가 있는 경우 이를 할당하고 불가능할 경우 현재 관리하고 있는 IP pool에서 사용하지 않는 IP 주소를 할당한다. 이 때 IP 주소 할당은 ISP망 내에서 유일한 값을 가지는 Username과 쌍을 이루며 유일한 Pair를 가진다. RADIUS 인증 서버는 Session-Timeout 필드에 할당 시간(Lease Time)을 넣고, Termination-Action에 RADIUS-Request(Value : 1)을 지정하고 Framed-IP에는 할당된 IP를 넣어서 Access-Accept 메시지를 작성하여 전송한다. 할당 시간은 특별한 설정이 없는 한 사용자의 요구를 따라야 하나 RADIUS 속성상 Access-Request시에는 Session-timeout을 사용할 수 없으므로 이전에 할당된 값을 사용하며 이전에 할당된 값이 없는 경우 기본으로 설정된 값을 사용한다. 또한 정적 할당인 경우는 할당 시간을 0xffffffff (4byte)로 설정한다. Session-timeout은 서버가 특정 서비스를 제공하는 시간을 의미하며 Termination Action은 서비스가 끝났을 때 클라이언트가 취해야 할 행동을 나타내며 default(Value : 0), RADIUS-Request(Value : 1) 등이 있다. Framed-IP는 Framed Protocol에 대해 할당 되는 IP를 나타낸다. Access-Accept 전송이후 RADIUS 인증 서버는 할당된 IP 주소 및 할당 시간 정보를 저장하고 내부적으로 타이머를 구동하여 할당 시간을 관리하여 할당 시간 만료 시 종료와 갱신 시 할당 시간 연장 등의 작업을 수행하여야 한다. 한편

GGSN은 Access-Accept를 통해 인증 결과 확인 및 IP와 할당 시간을 할당 받고 이전에 요구되었던 IP(정적 IP)와 RADIUS 서버에서 할당한 Framed-IP를 비교하여 이가 다를 경우 IPCP NAK메시지를 구성한다. 물론 이 때에도 세션 활성화는 성공으로 간주되며 추가적인 협상은 TE와 MT간에 행하여진다. 만일 Access-Reject를 받은 경우는 세션 활성화 실패로 간주하고 이를 TE에 알린다.

IP 주소 할당에 성공한 경우 GGSN은 RADIUS 과금 서버에 Acct. Request 메시지를 전송한다. Acct. Request 메시지의 속성에는 과금의 시작을 알리는 Acct-Status-Type : START (Value : 1)가 포함되어 그 이외에 Charging-ID로 사용되는 Acct-Session-ID, NAS-IP(GGSN-IP) 및 할당된 IP가 기입되는 Framed-IP 등이 포함되어 전송된다. 과금 요청 메시지를 받은 RADIUS 과금 서버는 Acct. Response 메시지로 응답하고 전송된 과금 정보를 저장하고 과금을 관리한다. 과금 응답 메시지를 받은 GGSN은 SGSN쪽으로 Create PDP Context Response를 전송하고 세션을 활성화 시킨다.

■ RADIUS 서버를 통한 IP 갱신

동적으로 IP를 할당 받은 경우 TE가 동일 IP 주소로 계속적으로 서비스를 받기 위해서는 할당 시간이 만료되기 이전에 IP 주소 할당시간을 연장하는 기능이 필요하다. 이 경우 IP 주소 갱신 요청의 주체가 GGSN 혹은 RADIUS 서버가 될 수 있다. 그러나 RADIUS 서버가 주체가 될 경우 GGSN이 내부적인 이유로 TE로 해제 메시지를 보내지 못하는 경우나 일반적으로 해제 과정을 수행하지 않는 일반적인 클라이언트의 경우에 RADIUS 서버는 사용하지 않는 IP 주소에 대해 계속적으로 IP 갱신 과정을 수행하여야 하는 맹점이 있으므로 갱신 요청의 주체는 GGSN이 되는 것이 바람직하다 할 수 있다.

GGSN은 세션이 종료되기 전까지 RADIUS 인증 서버에 주소의 갱신을 요청하는 메시지를 정기적으로 전송하여야 한다. 이때 갱신 메시지 전송에 대한 연장 시간의 설정은 할당 시간이 만료되기 이전의 값으로 사용자에게 의해서 임의적으로 선택되어 질 수 있으며 RADIUS 서버로부터 응답이 없거나 실패인 경우 몇 번의 재전송이 가능하다. 갱신 메시지를 보내기 위해 GGSN은 IP 할당 시 지정되었던 Termination Action의 속성값에 의해 Access-Request를 전송한다. RADIUS 서버는 Access-Request의 사용자를 인증한 후 요청된 사용자에 대해 기 할당된 IP 주소가 있는지 확인하고 사용자에 대한 요청 IP 주소가 유효할 경우 이 요청 메시지를 갱신의 메시지로 간주하고 할당 시간만큼 IP 주소의 할당 시간을 새로 연장한다. 이때 할당 시간의 결정은 특별한 설정이 없는 한 이전에 할당된 값을 사용한다. 만약 사용자에 기 할당된 IP 주소와 요청된 IP 주소가 다른 경우 인증 서버는 갱신의 실패로 간주하고 GGSN에 Access-Accept 메시지를 보내되 그 Framed-IP를 0으로 설정한다. 이때 Session-Timeout(Lease Time) 속성은 보내지 않는다. GGSN은 Access-Accept 메시지에 Framed-IP가 요구된 IP

주소와 다른 경우 갱신이 실패임을 인지하고 해당 세션을 종료하고 이를 RADIUS 과금 서버 및 TE로 알린다.

할당 시간 만료 이전까지 GGSN으로부터 갱신을 위한 메시지가 오지 않는 경우는 그 사용자에게 할당된 IP 주소 정보는 삭제되며 다른 사용자에게 할당 되어 질 수 있다. 만약 해제 이후에 Access-Request가 오면 RADIUS 서버는 이를 새로운 할당 메시지로 간주하고 이전에 할당했던 IP 주소를 할당하고 만약 불가능할 경우 새로운 IP 주소를 할당한다. 이 경우도 GGSN은 요구 IP 주소와 할당 IP 주소가 다른 경우 갱신 실패로 간주하고 해당 세션을 종료하고 이를 RADIUS 과금 서버 및 TE로 알린다.

■ RADIUS 서버를 통한 IP 해제

세션이 종료되었을 경우 GGSN은 해당 세션이 종료되었음을 ISP에 알려 해당 ISP가 할당된 IP 주소를 회수하고 관련 과금 기능을 수행할 수 있도록 해야 한다. 세션 종료

가 발생하면 GGSN은 RADIUS 과금 서버에 Acct-Request 메시지의 속성에 Acct-Status-Type : STOP(Value : 2) 및 Acct-Session-ID, NAS-IP(GGSN-IP), Framed-IP를 전송하여 세션이 종료되었음을 알린다. 과금 서버는 과금 종료 요청 메시지에 Framed-IP가 있는 경우 RADIUS 인증 서버에 IP Release Request 메시지에 해당 Framed-IP를 넣어 전송한다. RADIUS 인증 서버는 전송 받은 IP 주소를 검색하여 해당 IP 주소의 할당을 해제하고 IP Release Response 메시지를 과금 서버로 보낸다. 이 때 할당된 정보는 삭제되며 다른 사용자에게 할당되어질 수 있다. 인증 서버와 과금 서버 사이에 세션에 대한 식별자로서 Framed-IP 대신 Username이 사용되어 질 수 있다. 이 경우 초기 IP 주소 요청 시에 과금 서버에 대한 Accounting-Request 메시지에 Username을 넣어서 전송하여야 한다. 그러나 이는 속성 설정 중 선택 사항이므로 가급적 선택사항의 필수화를 줄이기 위해서는 Framed-IP를 사용하는 것이 바람직하다고 할 수 있다.

<표 2> RADIUS 인증 및 과금 서버의 메시지 속성 목록

서버	속 성(Attribute)	IP 할당		IP 갱신		IP 종료	
		요 청	응 답	요 청	응 답	요 청	응 답
RADIUS 인증서버	Username	○		○			
	Password or Chap pass	○		○			
	NAS-IP-Address	↓		↓			
	Framed-IP-Address	↓	○	○	○		
	Session-TimeOut		○		○		
	Termination-Action		○		○		
	Chap challenge	♣		♣			
RADIUS 과금서버	NAS-IP-Address	○				○	
	Framed-IP-Address	○				○	
	Acct-Status-Type	○				○	
	Acct-Session-Id	○				○	

○ : 필수적 ♣ : 조건적 ↓ : 선택적

인증 서버로부터 메시지를 받은 후 RADIUS 과금 서버는 Acct. Request 메시지를 GGSN에 전송하고 GGSN은 해당 세션의 종료되었음을 TE에 알린다. 이후에는 해당 IP 주소에 대한 GGSN으로부터의 주기적인 갱신 메시지 전송은 중지된다. 표 2에 RADIUS 인증 및 과금 서버의 메시지 에서 필요로 되는 속성을 나타내었다. GGSN 및 서버는 필요에 따라 추가적인 속성을 지정할 수 있다.

나. RADIUS 서버와 자체 DHCP 서버의 연동을 통한 IP 처리 기법

ISP 망 내에 IP 주소 할당을 담당하는 DHCP 서버가 존재하는 경우에 GGSN이 ISP 망 서브넷 내 해당 DHCP 서버를 찾지 못하고 또 DHCP 서버 IP 주소를 알지 못하는

등의 이유로 RADIUS 서버만 접속하여 처리하는 경우를 나타낸다. 이 경우 GGSN과 RADIUS 인증 및 과금 서버와의 흐름은 앞 절에서 설명한 과정과 동일하며 추가적으로 ISP 망 내 RADIUS 인증 및 과금 서버와 DHCP 서버와의 내부 연동 과정이 필요하다.

■ RADIUS 및 DHCP 서버를 통한 IP 할당

(그림 5)에 RADIUS 인증, 과금 서버 및 DHCP 서버를 이용한 IP 주소 할당 과정을 나타내었다. RADIUS 인증서버는 할당 시간을 관리하지 않으므로 갱신 메시지를 전송할 것인지 혹은 새로운 할당 메시지를 전송할 것인지에 대해 판별하는 작업만 수행하며 그에 대한 성공 여부는 모두 DHCP 응답에 의존한다. 먼저 GGSN은 RADIUS 인증서버에 Access-

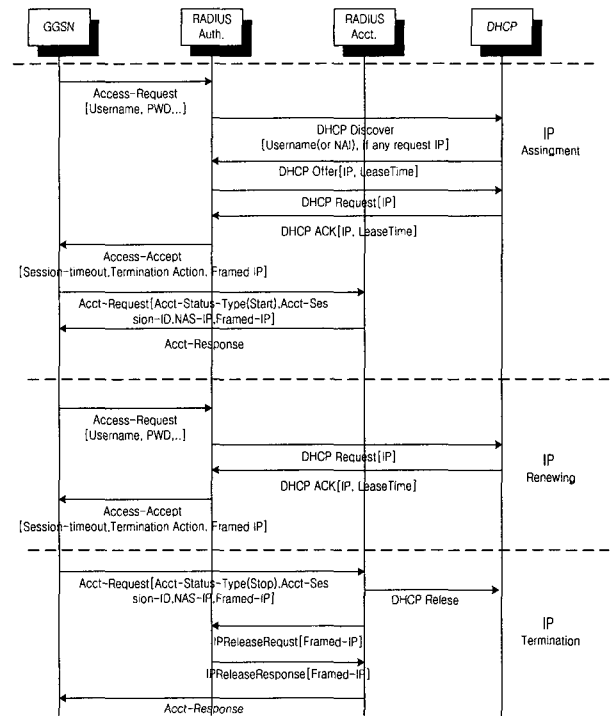
Request 메시지를 전송하여 인증을 요구한다. RADIUS 인증 서버는 사용자를 인증하고 속성에 Framed-IP가 있는 경우 DHCP와의 연동 작업을 수행한다. IP 주소 할당을 위해 RADIUS 서버는 DHCP에 IP 주소 할당 요구 메시지인 DHCP-Discover를 전송한다. RADIUS 서버는 DHCP 서버와 같은 서브넷에 속하는 경우라도 DHCP Relay Agent로서 작동하여 DHCP Discover 메시지 필드 중 giaddr에 RADIUS 서버 자신의 주소를 기입하여 메시지를 전송해야 한다. 이때 DHCP 속성상 RADIUS 서버는 할당 IP 주소의 서브넷에 속하는 IP 주소를 적어도 하나 이상 가지고 있어야 한다. RADIUS 서버가 DHCP Relay로 작동하는 이유는 하나 이상의 클라이언트 IP를 받아내야 하기 때문이며 부가적으로 망 내의 불필요한 Broadcast을 막을 수 있다. 클라이언트에 대한 유일한 ID로서 Username 혹은 NAI(Network Access Identifier)를 DHCP Discover의 옵션 필드의 Client Identifier에 지정한다. 또 정적 IP 주소의 할당 요구인 경우 옵션의 Request IP 필드에 해당 IP 주소를 지정하여 전송한다. 이후 일련의 과정이 끝나면 RADIUS 인증서버는 IP 주소와 할당 시간을 할당 받게 된다. IP 주소 및 할당 시간을 할당 받고 나면 일정 과정을 통해 RADIUS 과금 서버에 접속하고 세션을 활성화한다. 이 때 RADIUS 인증 서버는 할당 해제 메시지가 올 때까지 사용자 및 할당된 IP 정보를 저장하고 있어야 하며 필요에 따라 할당 시간을 관리할 수 있다.

■ RADIUS/DHCP 서버를 통한 IP 갱신

앞서 서술한 바와 같이 동적으로 할당된 IP 주소의 지속적인 사용을 위해 GGSN은 IP 주소 갱신 메시지를 전송한다. 이때 갱신을 위한 연장 시간은 DHCP[5]에 규정된 내용을 따르며 응답이 없을 경우 여러 번 전송할 수 있다. GGSN의 Access-Request 메시지가 전송되면 RADIUS 인증 서버는 사용자 인증 후 요청된 사용자에 대해 기 할당된 IP 주소가 있는지 확인하고 IP 주소가 할당된 사용자일 경우 이 요청 메시지를 갱신의 메시지로 간주한다. RADIUS 인증 서버는 DHCP 서버에 갱신을 위한 ciaddr에 갱신할 IP 주소를 넣고 DHCP Request 메시지를 전송하여 새로 할당 시간 연장을 요구한다. 성공적으로 DHCP ACK 메시지를 받은 경우 RADIUS 인증 서버는 Access-Accept를 GGSN에 전송한다. 만약 실패한 경우(DHCP NAK)를 받은 경우는 해당 IP 주소의 계속적인 사용에 실패한 경우로 RADIUS 인증 서버는 Access-accept 내에 Framed-IP를 DHCP 서버로부터 전송된 값인 0으로 설정하여 GGSN에 보낸다. GGSN은 메시지내의 Framed-IP가 요청된 IP 주소와 다른 경우 갱신에 실패한 것으로 간주하고 이를 RADIUS 과금 서버 및 TE에 알리고 관련된 세션을 종료한다. 비정상적 경우로 만약 갱신 시에 Access-Request의 사용자의 요청된 IP 주소가 기 할당된 IP 주소와 다른 경우 요청된 IP 주소로써 DHCP 갱신 메시지를 구성하여 DHCP 서버가 갱신의 성공 및 실패를 판단하게 해야 한다.

DHCP와 연동하는 경우 기본적으로 인증서버가 할당 시

간에 관리 없이 GGSN의 요청에 수동적으로 응하며 연장 시간만을 처리하는 것으로 구성되나 필요에 따라 내부적으로 타이머를 구동하여 할당 시간에 대한 연장 시간과 재 속박 시간(Rebinding Time)을 설정[5]하고 이에 따라 GGSN의 Access-Request를 갱신 혹은 재속박 메시지로 인식하여 처리할 수 있다. Rebinding은 DHCP 클라이언트가 주소 할당 서버로부터 갱신에 대한 응답이 없을 경우 주소 할당 정보의 연동이 가능한 다른 서버를 찾아 갱신 메시지를 발송하는 기능을 의미한다.



(그림 5) RADIUS 및 내부 DHCP 서버를 이용한 IP 관리과정

■ RADIUS/DHCP 서버를 통한 IP 해제

세션 종료가 발생하면 GGSN은 RADIUS 과금 서버에 Acct-Request 메시지의 속성에 Acct-Status-Type : TOP(Value : 2) 및 Acct. Session ID, NAS-IP(GGSN-IP), Framed-IP를 전송하여 세션이 종료되었음을 알린다. 과금 서버는 과금 종료 요청 메시지에 Framed-IP가 있는 경우 DHCP서버에 DHCP Release 메시지를 보내고 RADIUS 인증 서버에 IP Release Request 메시지에 해당 Framed-IP를 넣어 전송하여 해당 IP 주소의 할당 해제를 알린다. RADIUS 인증 서버는 전송 받은 IP 주소를 검색하여 해당 IP 주소의 할당을 종료하고 할당된 정보를 삭제한 뒤 IP Release Response 메시지를 과금 서버로 보낸다. RADIUS 과금 서버는 Acct-Request 메시지를 GGSN에 전송하고 GGSN은 해당 세션의 종료되었음을 TE에 알린다. 이후에는 해당 IP 주소에 대한 GGSN으로부터의 주기적인 갱신 메시지 전송은 중지된다.

그러나 이러한 DHCP 서버와의 연동의 경우 RADIUS 인증 서버의 IP 주소와 할당 받고자 하는 IP 주소의 서브

넷이 일치해야 하는 제약이 존재한다. 즉 이 경우 두 개 이상의 서브넷에 속하는 IP 주소의 할당은 불가능하며 이를 해결하기 위해서는 할당 범위의 서브넷들에 속하는 하나 이상의 IP 주소 및 인터페이스를 갖고 있어야 한다. <표 3>에 RADIUS 인증, 과금 및 DHCP 서버를 사용하는 경우의 기능에 대해 나타내었다.

<표 3> RADIUS/내부 DHCP 서버 이용시 IP 사용 기능

기 능	RADIUS Auth.+Acct.	RADIUS Auth.+Acct.+ DHCP
IP 할당	가능	가능
IP 갱신	가능	가능
IP 해제	가능	가능
ISP망 IP사용	가능	가능
Rebinding	불가	가능
두개이상의 서브넷 IP 할당	가능	조건부 가능

다. 제안 내용 요약

GPRS 망을 방문한 이동 ISP 가입자의 IP 할당시 RADIUS 서버만 이용하는 경우와 RADIUS 및 DHCP 서버를 이용하는 경우 각각의 문제점을 정의하고, 이의 해결 방안을 제시하였다. 해결 방안으로는 RADIUS 서버만을 이용하는 경우 요구되는 RADIUS 인증 서버와 과금 서버 사이의 동작 절차와 연동 신호를 정의하였으며, RADIUS와 DHCP 서버를 이용하는 경우는 GGSN과 RADIUS 서버, 그리고 RADIUS 서버와 DHCP 서버간의 요구되는 동작 절차와 연동 신호를 각각 정의하였다.

RADIUS 서버에 접속하여 인증과 더불어 IP를 할당 받는 경우 GGSN은 해당 IP 주소에 대한 할당 및 동적 IP 주소인 경우 갱신, 해제 등의 기능이 추가되게 되는데 이를 위하여 RADIUS 메시지의 속성(Attribute)을 이용하여 IP 주소 및 할당 시간 등의 정보를 받고 종료 시에 인증 서버 및 과금 서버의 연동에 따라 IP 주소 할당 해지의 과정을 수행할 수 있다. 또한 갱신의 경우 할당시간의 만료 이전에 또 다른 인증 요구를 통해 갱신 작업을 수행 할 수 있다.

그리고 ISP내에 IP 주소 할당을 담당하는 DHCP가 존재하는 경우에도 이와의 연동을 통해 IP 주소 할당 및 관리의 과정을 수행할 수 있도록 하고 있다.

5. 결 론

본 논문에서는 UMTS시스템에서 GGSN과 ISP 연동 시 RADIUS 인증 및 과금 서버를 이용하여 IP 주소를 할당 받고 이를 관리하는 기법을 제안 했다. 즉 RADIUS 서버를 통해 이동 ISP 가입자에 대한 동적 IP 주소의 할당 방식으로 ISP내 RADIUS 서버 자체만으로 지원하는 방식과 RADIUS와 DHCP서버를 연계해서 처리하는 방식을 제안하였고, IP 갱신 및 종료시 RADIUS 과금 서버를 통해 처리

하는 방식을 제안하였다.

본 논문에서 제안한 기법은 GGSN이 RADIUS 서버 혹은 RADIUS와 DHCP서버와 접속하는 경우 발생하였던 문제를 해결하고 기존의 인증 및 과금 전용인 RADIUS서버간의 연동을 통해 IP 할당, 갱신 및 해제의 작업을 수행할 수 있게 하여 UMTS 시스템에서 이동 ISP 가입자의 로밍을 위한 IP 주소 관리 작업을 가능하게 할 수 있다. 그러나 외부망으로 이동한 이동 ISP 가입자에게 홈 ISP 망의 동적 IP 주소 할당시 홈 ISP 망내에서 RADIUS 인증 및 과금 서버가 DHCP와 연계하는 경우 여전히 RADIUS가 할당하고자 하는 IP 주소와 항상 같은 서브넷에 존재해야 한다는 제약이 있으며 이러한 경우 할당 IP 주소의 모든 서브넷을 관리하는 게이트웨이에 RADIUS 서버를 설치하는 등의 여러 가지 해법들이 있을 수 있으며 향후에 더 많은 연구가 요구 된다. 또한 이러한 인증 및 IP 주소 할당 과정 중에 RADIUS 인증 및 과금 서버와 DHCP 서버, 그리고 실제 ISP 내에서 사용자를 관리하고 데이터 전송을 담당하는 서버간의 연동 관계도 지속적인 연구 필요성이 있다.

참 고 문 헌

- [1] 3GPP, "General Packet Radio Service(GPRS); Service Description; Stage 2," 3G TS 23.060 version 3.4.0, July, 2000.
- [2] IETF RFC 2002, "IPv4 Mobility Support", C.E.Perkins, October, 1996.
- [3] 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.
- [4] IETF RFC 2865, "Remote Authentication Dial In User Service(RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson, June, 2000.
- [5] IETF RFC 2131, "Dynamic Host Configuration Protocol", R. Droms, March, 1997.
- [6] IETF RFC 2132, "DHCP Options and BOOTP Vendor Extensions", S. Alexander, R. Droms, March, 1997.

박 정 현



e-mail : jh-park@etri.re.kr
 1982년 숭실대학교 전자공학과(학사)
 1985년 숭실대학교 대학원 전자공학과(석사)
 1997년 충북대학교 대학원 전자계산학과(박사)
 1994~1995년 캐나다 MPR Teltech 방문 (DBS 시스템 공동 개발)
 1982년~현재 한국전자통신연구원 u-Logistics연구팀 책임연구원.

관심분야 : 정보보호 프로토콜, IMT-2000 시스템 및 DBS/VSAT 위성 통신 시스템 보안, 무선 LAN 보안, 무선이동 패킷 망 간 인터워킹, 우정 정보화 기술 및 RFID 응용 개발