DIAMETER 프로토콜

DIAMETER Protocol

김수창(S.C. Kim) Mobile IP연구팀 선임연구원
전학성(H.S. Jeon) Mobile IP연구팀 책임연구원
김성희(S.H. Kim) Mobile IP연구팀 책임연구원, 팀장

AAA는 복잡한 Inter-domain 응용 서비스의 등장으로 인해 이들 서비스들을 신뢰성 있고 안전하게 관리하기 위해 사용된다. IETF에서는 AAA를 위해 Remote Authentication Dial-In User Service(RADIUS)와 DIAMETER 프로토콜을 제안하고 있다. DIAMETER는 기존의 PPP와 Roaming, Mobile IP 같은 새로 출현하는 정책과 AAA 서비스를 위한 확장 기능을 제공하기 위한 Peer 기반의 가벼운 AAA 프로토콜이다. 본 논문에서는 DIAMETER 프로토콜에 대한 개요 및 메시지, 형식, 그리고 라우팅 방식에 대해서 기술한다.

I. 서 론

AAA는 다중 네트워크와 플랫폼상에서 인증(Authentication), 권한검증(Authorization), 과금(Accounting) 등의 기능들을 조정하는 프레임워크이다. DIAMETER는 이러한 AAA 서버에서 사용되는 프로토콜이다[1].

AAA는 복잡한 Inter-domain 응용 서비스의 등장에 따라 이들 서비스들을 신뢰성 있도록 하고, 안전한 관리를 위해 사용된다[1, 2]. IETF에서는 AAA를 위해 Remote Authentication Dial-In User Service(RADIUS)[3]와 DIAMETER 프로토콜을 제안하고 있다[1].

DIAMETER는 기존의 PPP와 Roaming, Mobile IP 같은 새로운 정책과 AAA 서비스를 위한 확장 기반을 제공하기 위한 가벼운 Peer 기반의 AAA 프로토콜이다[1].

가장 널리 알려지고 많이 사용되는 AAA 프로토콜은 RADIUS인데 DIAMETER는 RADIUS의 약점을 보완하고 서버간 통신(Inter-Server communication)을 지원한다. IETF에서는 DIAMETER를 위한 프로토콜을 정의하고 있다.

II. DIAMETER 기본 프로토콜

DIAMETER 기본 프로토콜(DIAMETER Base Protocol)은 독립적으로 사용되지 않고 특정한 응용들을 위해 확장된 형태로 사용된다. 현재까지의 DIAMETER 확장으로는 NASREQ, Mobile IP, Accounting Extension, Resource Management 그리고 Strong Security가 있다[4-9].

기본 DIAMETER 프로토콜은 자체 능력협상, Peer 간 메시지 송수신 방법과 종료 방법을 규정한다. 또한, 다른 DIAMETER 사이에 교환되는 모든 메시지에 대한 규칙을 규정한다. 이 프로토콜은 IP 보안 같이 하위 보안 프로토콜이 없을 경우 응용 레벨의 보안 AVP(Integrity-Check-Value)를 선택적으로 사용할 수 있도록 하였다.

DIAMETER의 Peer간 통신은 한쪽에서 다른 한쪽으로 메시지를 보내는 것으로 시작된다. DIAMETER 메시지에 사용되는 AVP(Attribute Value Pairs)들의 집합은 DIAMETER 응용 또는 DIAMETER 확장에 의해 결정된다.

사용자의 인증 및 권한검증을 위해 초기 요청에 사용되는 것은 Session-Id이며, Session-Id는 사용자의 세션을 구분하기 위해 이후의 모든 메시지에 포함된다. 상대측은 요구를 수락하거나 오류가 있으면 Result-Code AVP를 포함하여 응답한다. 요구를 받은 DIAMETER 서버나 클라이언트의 동작은 그 서버에서 사용되는 DIAMETER 확장에 따른다.

III. DIAMETER 프로토콜 형식

1. 헤더 형식

기본 DIAMETER 프로토콜은 SCTP(Stream Control Transmission Protocol)를 이용하며[10], 포트 1812상에서 운용된다. 송신 포트는 어떤 것이라도 상관없지만 수신 포트는 반드시 1812번 포트를 통해서 이루어져야 한다. 요구 수신 후 응답을 보내기 위해서는 송신과 수신 포트가 반대로 바뀐다. 요구와 응답에 사용되는 송신지 및 목적지 주소는 Peer의 유효한 IP 주소들 일수도 있다.

DIAMETER의 한 프로세스는 프로세스를 구분하기 위해 모든 메시지를 보냄에 있어 같은 포트를 사용해야만 한다. 한 DIAMETER 안에 여러 개의 프로세스가 있을 수 있으며 이때 송신 프로세스의 포트 번호로 그 프로세스를 구분한다.

DIAMETER 데이터 형식은 <표 1>과 같다. 이 필드는 네트워크 바이트 순서로 전송된다.

<표 1> DIAMETER 헤더 형식

0 1 2 3 0123456789012345678901234567890 1			
RADIUS PCC=254	Flags	Ver	Message Length
Identifier			
AVPs …..			

• RADIUS PCC

RADIUS Packet Compatibility Code(PCC)는 RADIUS와의 역 호환성을 유지하기 위하여 사용된다. 한 옥텟이며 값은 254를 가진다.

• Flags

5비트이며 현재는 사용되지 않고, 반드시 0으로 셋되어야 한다.

• Version

DIAMETER 버전 1을 나타내기 위해 1로 셋되어야 한다.

• Message Length

헤더 필드를 포함한 DIAMETER 메시지의 길이를 나타내며 2옥텟이 사용된다.

• Identifier

4옥텟으로 구성되며 요구와 응답을 매칭시키기 위해 사용된다. 송신측이 보내는 메시지를 특정한 시간에 내부적으로 유일하게 구별하는 데 필요하며, 재부팅이 되기까지 유효하다. Identifier는 일반적으로 임의로 발생시킨 숫자에서 증가하는 형태를 가진다. DIAMETER 서버는 메시지를 유일하게 식별하기 위해 송신 주소, 송신 포트 그리고 메시지의 Identifier 필드를 사용한다.

• AVPs

AVP는 DIAMETER 메시지에 관련된 정보를 Encapsulation하는 방법이며, 이후 자세히 기술한다.

2. AVP 형식

DIAMETER AVP는 요구와 응답 같은 메시지 형식은 물론 인증, 과금 및 권한검증정보, 보안정보를 실어 나르는 데 사용된다. 어떤 AVP들은 필요시 한 번 이상 사용될 수 있다.

AVP 형식에는 String, Data, Address, Integer32, Integer64, Complex 그리고 Time이 있는데, String과 Data 타입 AVP는 32비트 단위로 정렬하기 위해 Null로 패딩되어야 한다. 패딩의 길이는 AVP 길이 필드에 포함되지 않는다.

가. AVP 헤더

AVP 형식은 <표 2>와 같으며 네트워크 바이트 순서로 전송된다.

<표 2> DIAMETER AVP 헤더 형식

0 1 2 3 0123456789012345678901234567890 1						
AVP Header						
AVP Length	Reserved	P	T	V	R	M
Vendor ID(opt)						
Tag(opt)						
Data ...						

• AVP Code

AVP Code는 애트리뷰트를 유일하게 식별한다. 만일 Vendor-Specific 비트가 셋되었다면, AVP 코드는 벤더의 사설 주소 체계에 따라 할당된다. AVP 번호 256은 RADIUS와의 역 호환성을 위해 예약되어 있고, DIAMETER에서는 256 이상의 값을 사용하며 IANA(Internet Assigned Numbers Authority)에서 할당한다[11].

• AVP Length

2옥텟을 사용하며 AVP Code, AVP Length, AVP Flag, Reserved, Vendor ID 필드(존재한다면), AVP 데이터를 포함하는 애트리뷰트의 길이를 나타내는 데 사용된다. 만일 수신된 메시지가 올바르지 않은 애트리뷰트 길이를 가졌으면 메시지가 거절된다.

• AVP Flags

AVP Flag는 각 애트리뷰트들을 어떻게 다루어야 하는지를 상대 DIAMETER 호스트에게 알려주는 역할을 한다. 추가적인 DIAMETER 확장을 위해서 이러한 비트들을 정의할 수 있으며 인식되지 않는 비트는 오류로 처리된다.

'R'과 예비 비트들은 사용되지 않고, 0으로 셋되며, 수신측에서는 무시한다.

'P' 비트는 Strong Security Extension에서 정의한다.

필수 비트인 'M' 비트는 해당 AVP가 반드시 지원되어야 함을 나타낸다. 만일 수신측이 이 비트가 셋된 AVP를 받았으나 지원할 수 없는 경우 메시지는 반드시 거절되어야 한다. 이 AVP를 지원하지 않는 수신측이 받은 경우 이 AVP는 무시한다.

'V' 비트는 Vendor-Specific 비트이다. 이 비트가 셋되면 AVP 헤더에 Vendor ID 선택 필드가 사용된다. 이때 AVP 코드는 해당 Vendor Code 주소에 따른다.

'T' 비트는 Tag 비트이고, AVP의 집합을 묶어서 사용하는 데 사용된다.

나. 선택 헤더 정보요소(Optional Header Elements)

AVP 헤더는 여러 개의 선택 필드로 구성된다. 이 필드들을 사용하기 위해서는 해당 비트 플래그가 셋되어야만 한다.

• Vendor ID

이 필드는 AVP 플래그 필드 V가 셋되면 사용된다. 선택 사항인 이 필드는 IANA가 할당한 Structure and Identification of Management Information for TCP/IP-based Internets(SMI)[RFC1155]를 포함하는 4옥텟으로 이루어진다. DIAMETER 확장을 구현하려는 벤더는 반드시 자신의 Vendor ID를 사용해야 하며 자신의 AVP 주소를 이용하여야 한다.

• Tag

태그 필드는 길이가 4옥텟이며 같은 메시지 내에서 애트리뷰트들을 묶어서 사용하는 데 필요하다. 'T' 비트와 함께 사용된다.

3. AVP Value 형식

데이터 필드는 0개 이상의 옥텟으로 구성되며 특정 애트리뷰트에 대한 정보로 구성된다. 데이터 필드의 형식과 길이는 AVP Code와 AVP Length 필드에 의해 결정된다. 이 필드의 형식은 아래와 같은 7개의 데이터 타입 중의 하나에 해당한다.

• Data

가변 길이의 임의의 데이터를 포함한다. 다른 언

급이 없으면 AVP Length 필드는 최소한 9로 셋되어야 한다.

• String

Universal Character Set Transformation Formats(UTF)-8 문자 집합을 사용하는 NULL로 끝나지 않는 가변 길이 스트링을 포함한 데이터를 말한다. 다른 언급이 없으면 AVP Length 필드는 최소한 9로 셋되어야 한다.

• Address

32bit(IPv4)인지 128bit(IPv6) 주소인지를 나타내는 중요한 옥텟이다. IPv4 주소인 경우 AVP Length 필드는 12가 되고, IPv6인 경우 24가 된다.

• Integer32

32bit 값을 가진다. AVP Length 필드는 12가 된다.

• Integer64

64bit 값을 가진다. AVP Length 필드는 16이 된다.

• Time

Network Time Protocol(NTP)로부터 반환되어 온 4옥텟으로 이루어진 32비트의 부호없는 정수 값이다. AVP Length 필드는 12이다.

• Complex

Complex 데이터 타입은 복수개의 정보 필드를 포함하는 AVP들을 위해 예약되어 있다. 따라서 위에 정의한 AVP들과 다르다. Complex AVP는 데이터 형식과 AVP의 예상 길이를 나타낸다.

4. DIAMETER 프로토콜 기본 AVP

<표 3>은 DIAMETER 기본 프로토콜에 정의된 AVP와 AVP Code 값, 타입을 나타낸다.

이외에도 표준 DIAMATER 확장 AVP로서 NASREQ Extension, Mobile IP Extension, Strong Security Extension, Accounting Extension에서 사용되는 표준 AVP들이 있다.

5. 필수 AVP

모든 DIAMETER 메시지에 항상 사용되는 DIAMETER AVP는 <표 4>와 같다.

<표 3> DIAMETER 기본 프로토콜 AVP

AVP Name	Code	Type
User-Name	1	String
Session-Timeout	27	Integer32
Proxy-State	33	Complex
Command-Code	256	Integer32
Host-IP-Address	257	Address
Extension-Id	258	Integer32
Integrity-Check-Value	259	Complex
Encrypted-Payload	260	Complex
Nonce	261	Data
Timestamp	262	Time
Session-Id	263	Data
Host-Name	264	String
Vendor-Name	266	String
Firmware-Revision	267	Integer32
Result-Code	268	Complex
Destination-NAI	269	String
Failed-AVP	279	Data
Redirect-Host	278	Address
Redirect-Host-Port	277	Integer32

가. Command-Code AVP

Command-Code AVP(AVP Code 256)는 Integer32 타입이며 DIAMETER 헤더에 이은 첫번째 AVP이다. DIAMETER 메시지는 최소한 1개의 Command-Code AVP를 가져야 하고, 메시지와 관련된 명령어를 주고 받기 위해 사용한다. Command Code 32-bit 주소는 IANA에 의해 관리된다. DIAMETER 기본 프로토콜 및 확장에서 사용되는 Command Code는 다음과 같다.

나. Host-Name AVP

Host-Name AVP(AVP Code 32)는 String 타입이며 Peer DIAMETER에게 누가 송신한 것인가를 알려 주기 위해 사용된다. 모든 DIAMETER 메시지는 Host-Name AVP를 포함해야 하고, DIAMETER 메시지 발신자의 호스트 이름을 포함하며, NAI(Network Access Identifier) 작명 규칙을 반드시 따라야 한다[12].

<표 4> DIAMETER 필수 AVP

Command-Name	단축명	Code
Device-Reboot-Ind	DRI	257
Message-Reject-Ind	MRI	259
Session-Termination-Ind	STI	274
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	276
AA-Mobile-Node-Request	AMR	260
AA-Mobile-Node-Answer	AMA	261
Home-Agent-MIP-Request	HAR	262
Home-Agent-MIP-Answer	HAA	263
AA-Request	AAR	265
AA-Answer	AAA	266
AA-Challenge-Ind	ACI	267
DIAMETER-EAP-Request	DER	268
DIAMETER-EAP-Answer	DEA	269
DIAMETER-EAP-Ind	DEI	270
Accounting-Request	ACR	271
Accounting-Answer	ACA	272
Accounting-Poll-Ind	ACP	273
Accounting-Status-Ind	ASI	279
Session-Resource-Query	SRQ	277
Session-Resource-Reply	SRR	278

6. AVP 태그 방법

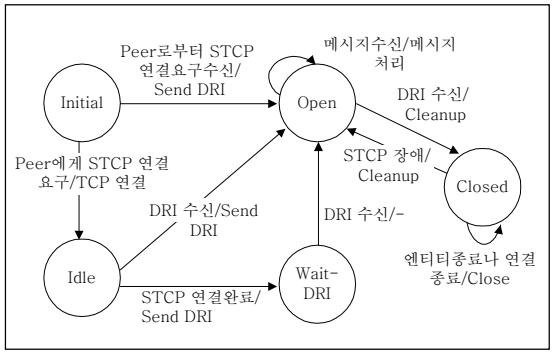
AVP를 서로 그룹화 하기 위해 T 비트를 사용한다. 같은 태그 값을 가진 모든 AVP는 '태그된 AVP 집합'이다. 태그 값의 사용에 대해서는 정해진 규칙이 없다. 태그는 하나 이상의 호스트에 대한 정보를 한 요청에 포함하는 것을 허용한다. 여러 개의 AVP들이 특정 인증 규칙을 나타내는 것이 필요할 때 태깅이 적절하다. 만일 하나 이상의 규칙이 필요한 경우 태깅 메커니즘은 AVP의 집합을 쉽게 그룹화 할 수 있도록 해준다.

다음은 DRI 메시지에서의 태그 사용 예를 보여준다.

<Device-Reboot-Ind>::=
<DIAMETER Header>
<Command Code AVP>
(<Tagged AVP #1>
<Tagged AVP #2>
<Tagged AVP n>)

IV. DIAMETER 동작

DIAMETER 구현시 Peer와의 통신을 위해 모든 DIAMETER가 가지는 상태는 (그림 1)과 같다.



(그림 1) DIAMETER 상태 천이도

로컬에서 STCP가 연결단계 동안 데이터 피기백을 처리할 수 있다면 Initial과 Idle 상태는 합쳐질 수 있다[13]. Cleanup 동작이 시작되면, DIAMETER 노드는 대체서버(Alternate Server)로 ACK를 받지 못한 채 중지된 모든 요구와 응답을 전달한다. 만일 어떤 메시지의 최종 목적지가 더 이상 접근이 불가능한 호스트일 경우 그 메시지는 Result-Code AVP 내에 DIAMETER_UNABLE_TO_DELIVER로 셋된 채 응답된다.

1. DIAMETER 동작 시작

가. Device-Reboot-Ind

AAA 서버가 새로 부팅되었을 경우 그 사실을 알리기 위해 DIAMETER가 Peer에게 DRI를 보낸다. 이때 Host-IP-Address AVP를 반드시 포함한다. 또한 지원되는 프로토콜 버전 번호나 Mobile IP 확장 등 능력협상을 위해서도 사용된다. DRI는 응답을 필요로 하지 않는 메시지이다. 일단 트랜스포트 연결이 설정되면 수신측이 수동으로 구성되었는지 또는 동적인 방법으로 발견되었는지의 여부에 관계없이 DRI를 보내며 프로토콜 처리기능에서는 Peer측이 보낸 이 메시지를 받고 해석해 보았을 때 오류가 있다고

판단되면 MRI(Message-Reject-Ind)를 보낸다. 동적인 방법으로 Peer를 발견하는 것은 Service Location Protocol(SLP)이나 다른 방법에 의해 가능하다.

DRI 메시지의 형식은 다음과 같다.

<Device-Reboot-Ind> ::=
<DIAMETER Header>
<Command Code AVP = 257>
<Host-Name AVP>
<Host-IP-Address AVP>
<Vendor-Name AVP>
<Extension-Id AVPs>
[<Firmware-Revision AVP>]
[<Timestamp AVP>
<Nonce AVP>
<Integrity-Check-Value AVP>]

나. Vendor-Name AVP

Vendor-Name AVP(AVP Code 266)는 String 타입이고, Peer DIAMETER에게 DIAMETER 디바이스의 제조업자명을 알리기 위해 사용된다.

다. Firmware-Revision AVP

Firmware-Revision AVP(AVP Code 267)는 Integer32 타입이고, DIAMETER Peer에게 자신의 디바이스의 펌웨어 버전을 알리는 데 사용된다.

DIAMETER SW 모듈이 실행되는 범용 컴퓨터와 같이 펌웨어 버전 정보를 갖지 않는 디바이스인 경우 DIAMETER SW 모듈 버전이 대신 사용될 수 있다.

라. Extension-Id AVP

Extension-Id AVP(AVP Code 258)는 Integer32 타입이고, DIAMETER 확장을 식별하기 위해 사용한다. 이 AVP는 로컬에서 지원되는 확장이 무엇인지를 Peer DIAMETER에게 알리기 위해 DRI 내에 포함된다.

각 DIAMETER 확장은 IANA가 할당한 확장 ID를 가져야만 한다. DIAMETER Device-Reboot-Ind 메시지 안에는 여러 개의 Extension-Id AVP가 사용될 수 있다. Extension-Id 값은 다음과 같다.

NASREQ	1
Strong Security	2
Resource Management	3
Mobile-IP	4
Accounting	5

마. Host-IP-Address AVP

Host-IP-Address AVP(AVP Code 4)는 Address 타입이며, 송신측 IP 주소를 DIAMETER Peer에게 알리기 위해 사용된다. SCTP 상에서 사용될 모든 송신 IP 주소는 매 주소마다 Host-IP-Address AVP를 포함한 DRI를 통해 방송되어야 한다. 이 AVP는 Device-Reboot-Ind 메시지에서만 사용된다.

2. 사용자 세션

사용자가 망을 사용하고자 할 때 DIAMETER 클라이언트는 로컬 서버에 인증 및 인가 요청을 보낸다. 이때 Session-Id AVP를 포함하며 이 Session-Id는 그 사용자의 세션에서 이후의 권한검증과 과금 메시지 등에 사용된다. Session-Id AVP를 통해 클라이언트와 서버 사이의 특정 사용자 세션의 메시지를 구별할 수 있다.

가. Session-Id AVP

Session-Id AVP(AVP Code 263)는 Data 타입이며, 세션을 식별하는 데 사용된다. 특정 세션 동안의 모든 메시지는 하나의 Session-Id AVP만 사용되어야 하며, 그 세션 동안 같은 값이 사용되어야 한다. 특정 세션에 관련이 없는 메시지들은 T 비트가 셋되어 여러 개의 Session-Id AVP가 나타날 수 있다. Session-Id는 세션이나 흐름을 식별하기 위해 서버에서 사용되므로 일정시간 내에서 전역적으로

유일해야만 한다. Session-Id의 형식은 다음과 같다.

<송신측 Host-Name> <송신측 포트번호> <단순 증가 32bit 값>< optional value>

재시동 후 Session-Id가 겹치는 문제를 피하기 위해 단순증가 32비트 값은 재시동시 0에서 시작해서는 안되고, 임의의 수에서 시작해야 한다. Optional Value는 구현에 따라 다르지만 모뎀의 장치 Id, 계층 2 주소, Timestamp 등을 포함할 수 있다.

Session Id는 세션을 시작하는 DIAMETER 장치에 의해 만들어진다. 대부분의 경우 클라이언트에 의해 이루어진다. 하나의 Session-Id는 하나 이상의 확장에 의해 사용될 수 있다(예를 들면 특정 서비스에 대한 인증과 과금).

나. Session-Timeout AVP

Session-Timeout AVP(AVP Code 27)는 Integer32 타입이며, 세션 종료 시까지 사용자에게 주어지는 서비스에 대한 최대 시간(초 단위)을 의미한다. 이 값이 0인 경우는 종료 때까지 무한 시간을 갖는다는 것을 의미한다.

이 AVP는 클라이언트가 허용할 수 있는 최대 시간의 참조일 뿐이다.

다. User-Name AVP

User-Name AVP(AVP Code 1)는 String 타입이며, NAI 규칙에 따르는 User-Name을 말한다[4]. 모든 DIAMETER 시스템은 최소한 72옥텟의 사용자 이름을 지원해야 한다.

3. 세션 종료

더 이상 세션이 필요 없을 경우 세션 종료를 요구할 수 있으며 이것은 Session-Terminate-Request (STR)와 Session-Terminate-Answer(STA)에 의해 이루어진다. STR을 수신하면 DIAMETER 서버는 Session-Id AVP에 의해 식별되는 해당 세션의 모든 자원을 회수한다.

가. Session-Termination-Ind

STI는 명령어 코드 274를 가지며, 특정 세션이 완료되었음을 알려주기 위하여 DIAMETER 서버에 의해 송신되는 메시지이다.

메시지 형식은 다음과 같다.

<Session-Termination-Ind>::=
<DIAMETER Header>
<Command-Code AVP = 274>
<Session-Id AVP>
<Host-Name AVP>
<User-Name AVP>
<Destination-NAI AVP>
[<Proxy-State AVP>]
[<Timestamp AVP>
<Nonce AVP>
<Integrity-Check-Value AVP>]

나. Session-Termination-Request

STR에는 Destination-NAI AVP가 필요하며, 해당 세션에서 인증/권한검증된 응답(AAA, HAA, AMA)의 Host-Name AVP 안의 값으로 셋되어야 한다.

STR을 수신하면 DIAMETER는 Session-Id AVP에 의해 식별되는 해당 세션의 모든 자원을 회수한다. 필요하다면 Proxy-Chain에서 중간 서버의 자원도 해제할 수 있다.

메시지 형식은 다음과 같다.

<Session-Termination-Request>::=
<DIAMETER Header>
<Command-Code AVP = 275>
<Session-Id AVP>
<Host-Name AVP>
<User-Name AVP>
<Destination-NAI AVP>
[<Proxy-State AVP>]
[<Timestamp AVP>
<Nonce AVP>
<Integrity-Check-Value AVP>]

다. Session-Termination-Answer

STA는 DIAMETER에서 STR에 대한 응답으로 보내는 메시지이다. Result-Code AVP가 반드시 사용되어야 하며 STR 처리중에 오류가 발생했는지를 나타내는 정보를 포함할 수 있다.

메시지 형식은 다음과 같다.

<Session-Termination-Answer>::=
<DIAMETER Header>
<Command-Code AVP = 276>
<Result-Code AVP>
<Session-Id AVP>
<Host-Name AVP>
<User-Name AVP>
<Destination-NAI AVP>
[<Proxy-State AVP>]
[<Timestamp AVP>
<Nonce AVP>
<Integrity-Check-Value AVP>]

4. 신뢰성 있는 전송

상대 Peer의 장애를 신속히 발견하고 강력한 재전송 기능을 가지며, 신속한 처리를 위해 DIAMETER 메시지는 SCTP 상에서 송・수신되어야 한다. TCP는 위에서 요구한 사항을 가지고 있지는 못하지만 신뢰성 있는 전송이 가능하므로 DIAMETER Peer는 TCP를 사용할 수도 있다.

5. 오류처리

DIAMETER에는 <표 5>와 같이 5개의 오류형태가 있다. 정확하지 않은 형식이나 인식할 수 없는 형식을 가진 DIAMETER 메시지로 인한 잘못된 메시지 오류, 지원되지 않는 Command-Code AVP를 수신한 경우, 송신측에서 보낸 필수 AVP를 수신측에서 알려지지 않은 AVP라고 응답하는 경우, 그리고 아직 알려지지 않거나 허용되지 않는 값을 수신한 경우 등이다.

<표 5> DIAMETER 오류

오류 종류	동 작
Bad Message	메시지 무시
Unknown Command	MRI 송신
Unknown AVP	MRI 송신
Bad Value	MRI 송신
Extension Error	Extension Response+ Result-Code

오류의 종류 및 동작은 다음과 같다.

'Extension Response + Result-Code'는 Peer에게 어떤 문제가 있다는 것을 알려주기 위해 Result-Code AVP들을 포함한 응답 메시지를 보내야 한다는 것을 뜻한다.

가. Message-Reject-Ind Command

MRI는 명령어 코드 259를 가지며, 트랜잭션이 완벽하게 수행되지 못하고 오류가 있을 때 사용되는 메시지이다. 메시지를 해석한 결과 오류가 있을 경우, 응답 메시지가 적절치 않을 때, 체크할 수 없는 메시지가 수신되었을 때 및 지원할 수 없는 확장이 요구된 경우 MRI를 보낸다.

MRI 메시지의 형식은 다음과 같다.

<Message-Reject-Ind message>::=
<DIAMETER Header>
<Command-Code AVP = 259>
<Host-Name AVP>
[<Session-Id AVP>]
<Result-Code AVP>
<Failed-AVP AVP>
[<Timestamp AVP>
<Nonce AVP>
<Integrity-Check-Value AVP>]

나. Failed-AVP AVP

Failed-AVP AVP(AVP Code 279)는 데이터 타입이고 AVP 안의 오류 정보로 인해 거절되거나 처리되지 않은 경우에 디버깅 정보를 제공한다. Re-

sult-Code AVP는 Failed-AVP AVP에 대한 원인 정보를 제공한다.

다. Result-Code AVP

Result-Code AVP(AVP Code 268)는 Complex 타입이며 요청한 것이 끝까지 잘 처리되었는지 또는 오류가 발생했는지를 알려주는 역할을 한다. Response나 Answer 타입의 모든 메시지는 IANA에서 관리되는 하나의 Result-Code AVP를 가진다.

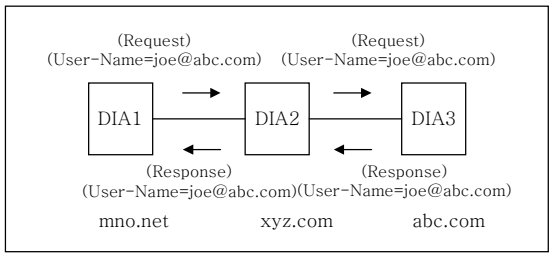
V. DIAMETER 메시지 라우팅

DIAMETER 기본 프로토콜은 라우팅을 위해 프록시 방법과 브로커링의 2개의 방법을 사용한다. DIAMETER 프록시는 사용자의 ID를 기반으로 하거나 다른 방법에 의해 단지 요청을 전해주는 서버이다. DIAMETER 브로커는 직접 상호작용 하기 위해 모든 서버를 하나의 로밍 컨소시엄 형태로 허용하여 서비스를 재전달하는 서버이다. DIAMETER 메시지 라우팅이 수행되는 방법은 다음과 같다.

1. NAI 기반 메시지 라우팅

DIAMETER 메시지 라우팅은 NAI의 사용 그리고 관련된 realm 라우팅 테이블을 통해 행해진다. NAI는 user@realm과 같은 형식을 가진다. 내부에서 지원되지 않는 realm을 포함하는 메시지를 받았을 경우 그 메시지는 라우팅 테이블 안에 구성되어 있는 DIAMETER 엔티티에 프록시 된다.

(그림 2)는 DIA1이 joe@abc.com이라는 사용자를 인증하기 위한 요청을 수신한 예를 보여준다. DIA1은 자신의 내부 realm 라우팅 테이블에 abc.com을 찾은 후 그 메시지는 DIA2에 프록시 되어야 함을 안다. DIA2도 같은 방법으로 찾아본 후 DIA3로 프록시 한다. DIA3도 같은 방법으로 자신의 라우팅 테이블을 찾아보고 그 realm은 내부적으로 지원이 된다는 것을 안다. DIA3는 그 인증요청을 처리하고 응답을 보낸다.



(그림 2) NAI 기반 라우팅

2. 메시지 프록시

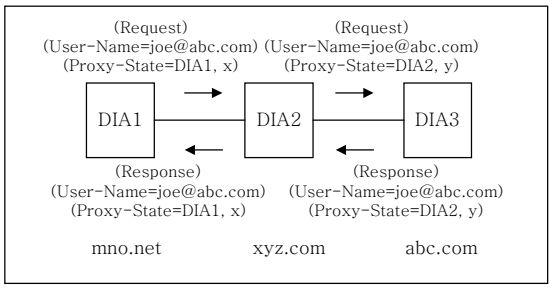
DIAMETER 프록시는 다른 DIAMETER 서버로 메시지를 전달하는 서버이다. 프록시는 기본적으로 몇 개의 DIAMETER 서버가 사용자 인증과 권한검증을 할 수 있는 계층적 DIAMETER 망이 구축될 경우 사용된다. 예로써 로밍 컨소시엄이 있으며, 각 ISP는 인증 및 권한검증을 할 수 있는 사용자 베이스를 가진다. 프록시 서버는 DIAMETER 메시지 내에서 AVP들을 순서 배치를 새로 해서는 안 된다. 프록시를 통해 DIAMETER 메시지를 라우팅하는 방법은 Proxy-State와 Destination-NAI의 2가지가 있다.

가. Proxy-State AVP

Proxy-State AVP(AVP Code 33)는 요청을 전달하는 데 사용하며, 응답을 후에 처리하기 위해 프록시에 의해 사용되는 불분명한 데이터를 포함한다. 이러한 데이터는 응답에 추가되는 AVP들, 다운스트림 Peer에 대한 정보 등을 포함할 수 있다.

DIAMETER 노드는 Proxy-State AVP를 요청에 추가하고 응답시 동일한 AVP가 포함될 것을 기대한다. 그리고 하나의 DIAMETER 메시지 안에 하나 이상의 Proxy-State AVP가 사용될 수 없다.

(그림 3)과 같이 DIA2가 DIA3로부터 응답을 받았을 때 DIA2는 Proxy-State를 조사해서 DIA1에서 만들어짐을 안다. DIA2는 DIA1과 통신할 수 있으므로 DIA2는 메시지를 DIA1으로 보낸다. Proxy-State AVP의 주소 필드는 128비트이며, 그 AVP를 생성한 시스템의 IP 주소를 갖는다. Proxy-State



(그림 3) Proxy-State AVP 이용 라우팅

AVP가 로컬 호스트를 위한 것인지를 결정하기 위해 호스트들을 돕는 데 사용된다.

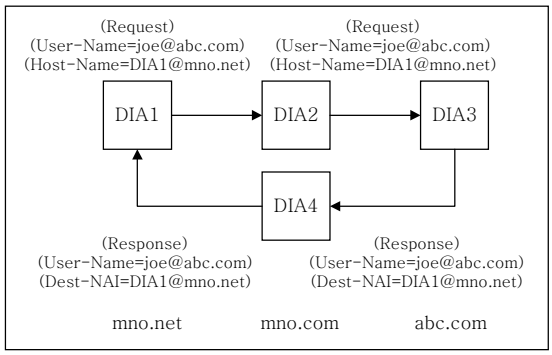
나. Destination-NAI AVP

Destination-NAI AVP(AVP Code 269)는 String 타입이고, 요청시 포함될 수 있으며, 응답 메시지 안에는 반드시 포함되어야 한다. Destination-NAI는 NAI 규격과 일치해야 한다. 응답 메시지의 Destination-NAI AVP는 요청시 사용되었던 Host-Name AVP의 값이 포함되어야 한다.

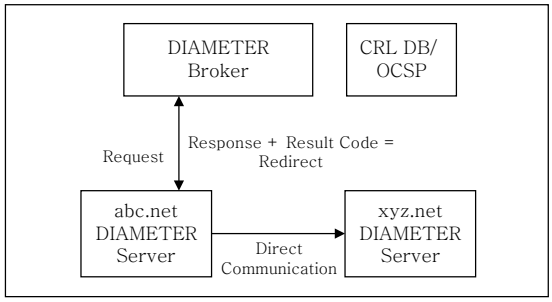
Destination-NAI AVP는 DIAMETER 노드가 특정한 realm을 처리할 수 있는 많은 Peer 중의 하나에게 메시지를 보낼 수 있는 더욱 탄력적인 DIAMETER 망을 허용한다. (그림 4)에서 DIA3는 응답을 생성한다. DIA3는 요청 메시지의 Host-Name AVP 값을 가지고 Destination-NAI를 응답 메시지에 넣는다. DIA3는 DIA1과 직접 통신할 수는 없지만 mno.com 망을 통해 Peer와 통신할 수 있다. 그러므로 DIA3는 mno.com 망 안의 아무 Peer에게 응답을 보낸다. DIA4는 응답을 수신하고, Destination-NAI AVP를 조사하며, DIA1과 직접 통신할 수 있는지를 결정한 후 응답을 DIA1으로 보낸다.

3. 메시지 재지정(Message Redirection)

브로커로 알려져 있는 DIAMETER 프록시는 요청이 있을 시 (그림 3)과 같이 메시지를 전달하는 대신에 다른 서버와 직접 접촉한다. 브로커가 홈 DIAMETER 서버 주소 해석 서비스에 대해 단순 NAI를



(그림 4) Destination-NAI 이용 라우팅



(그림 5) Redirect Indication을 반환하는 DIAMETER 브로커

마련할 경우 기본적으로 이루어진다.

(그림 5)의 예와 같이 abc.net의 DIAMETER 서버는 자신의 브로커로 요청을 보낸다. 브로커는 DIAMETER_REDIRECT_INDICATION을 Result-Code AVP에 셋해서 응답으로 보낸다. DIAMETER 서버는 이 값이 셋된 Result-Code를 응답으로 받으며, 이 메시지 내에는 하나 이상의 Redirect-Host AVP가, 옵션으로 Redirect-Host-Port AVP가 포함되어 있다. Redirect-Host AVP는 요청이 직접 전달되어야 하는 IP 주소를 포함한다.

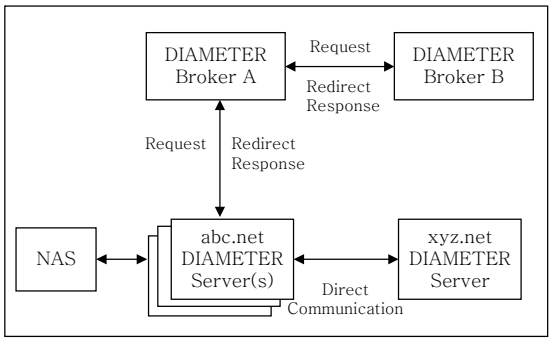
특정한 realm을 사용하는 홈 DIAMETER 서버를 식별하기 위해 브로커는 모든 메시지를 접촉하는 것이 요구된다. 브로커를 접촉하는 것은 부가적인 대기 시간이 필요하므로 같은 realm을 갖는 여러 메시지 처리를 위해 브로커를 접촉하는 점을 제거하기 위해 구현 시에는 브로커가 보낸 정보를 캐시할 수도 있을 것이다. 캐시의 유효한 기간을 Peer에게 알려주기 위해 브로커는 재전달 응답 메시지 안에 Session-

Timeout AVP를 포함할 수 있다. Peer는 브로커로부터의 캐시 유효기간 정보를 참고만 하지 강제적인 사항은 아니다.

Redirect-Host AVP가 태그되면 브로커는 특정 호스트에 대한 캐시 만기를 알리기 위해 Session-Timeout AVP에 태그를 추가한다.

DIAMETER_REDIRECT_INDICATION이 셋된 Result-Code를 가진 응답 메시지를 반환할 때 브로커는 요청 서버와 목적지 서버 양측에 대한 인증서를 포함할 수 있다. 이 인증서는 CMS-Data AVP 안에 포함된다. 요청 서버는 그 다음의 요구 안에 자신의 인증서를 홈 DIAMETER 서버에게 전달해야 한다.

(그림 6)은 요청이 두번째 브로커(브로커간 통신)에 전달되는 더 복잡한 망을 보여준다. NAS와 Edge DIAMETER 서버(브로커와 통신하는 역할) 사이의 다수의 프록시를 가지는 구조이다. 브로커 A가 브로커 B로부터 재전달된 정보를 포함하는 응답을 수신하면, A는 abc의 DIAMETER 서버로 전해주고, abc의 DIAMETER 서버는 xyz의 서버와 직접 통신하게 된다.



(그림 6) 프록시 망에서의 브로커간 재지정

가. Redirect-Host AVP

Redirect-Host AVP(AVP Code 278)는 Address 타입이고, DIAMETER_REDIRECT_REQUEST가 셋된 Result-Code AVP를 가진 응답의 형태로 반환된다. 이 AVP는 요청이 재전달되어야 하는 DIAMETER 호스트의 IP 주소를 포함한다. 같은 태그 값을 가진 여러 개의 태그된 Redirect-Host AVP가 있으면 그 주소의 모든 메시지는 동일한 호스트에 대한 접촉에 사용될 수 있음을 의미한다. 여러 AVP가 태그되지 않거나 다른 값으로 태그된 채 존재하면 이들 AVP들은 서로 다른 호스트들을 나타낸다. 이러한 Result-Code와 이 AVP를 수신하면 DIAMETER 호스트는 이들 호스트 중 하나에게 직접 요청을 보낸다.

나. Redirect-Host-Port AVP

Redirect-Host-Port AVP(AVP Code 277)는 Integer32 타입이며 Redirect-Host AVP와 함께 사용될 수 있다. 이 AVP가 사용되지 않았을 경우 예약 확보된 포트가 사용된다.

VI. DIAMETER 메시지 보안

DIAMETER 기본 프로토콜은 3가지 방법에 의해 보호된다. 첫번째 방법은 DIAMETER 프로토콜에 어떤 보안 체계도 사용하지 않는 대신 IP Security 같은 기본적인 보안체계를 사용하는 것이다. 두번째 방법은 모든 DIAMETER 구현에서 지원되어야 하는 Hop-by-Hop Security를 사용하는 방법이다. 마지막 방법은 옵션으로 공개 키 방식을 이용하는 것이다.

Hop-by-Hop Security는 메시지 무결성과 AVP 암호화를 제공한다. Hop-by-Hop Security는 RADIUS 프로토콜에 의해 사용된 방법과 유사한 형태의 미리 구성된 shared secret를 가지는 통신 엔티티를 필요로 한다. 이 방법은 공개 키 기반 보안(Public Key Infrastructure: PKI)과는 달리 적용하기가 매우 어렵고 대형 망에서는 관리하기 어려우며, 상호 신뢰를 필요로 한다. PKI는 종단간 DIAMETER 보안에 사용되고, 세부 사항은 DIAMETER Strong Security Extension에 정의되어 있다[6]. Hop-by-Hop Security는 대칭 암호기법으로 충분하거나 PKI를 사용할 수 없는 환경에 바람직하다.

VII. 결 론

이상과 같이 DIAMETER 기본 프로토콜에 대해 살펴 보았다. DIAMETER 기본 프로토콜의 표준화는 아직 IETF에서 Draft 형태로 추진되고 있지만 RADIUS와 호환성을 가지면서도 RSDIUS나 TACACS+ 같이 현재 사용되는 AAA 프로토콜의 한계를 극복할 수 있는 장점을 가지고 있으므로 향후 AAA 서버의 유력한 프로토콜로 거론되고 있다. 그리고 Mobile IP 같이 도메인 간의 이동성을 보장하는 응용 등 새로운 정책과 AAA 서비스가 필요한 곳에 많이 사용될 것으로 보인다.

참 고 문 헌

[1] Christopher Metz, "AAA Protocols: Authentication, Authorization and Accounting for the Internet," IEEE Internet Computing, Nov. 1999.

[2] Calhoun, Zorn and Pan, Akhtar, "DIAMETER Framework," draft-calhoun-diameter-framework-08.txt, IETF work in progress, June 2000.

[3] Rigney *et al*., ia, "RADIUS," RFC 2138, Apr. 1997.

[4] P. Calhoun, W. Bulley and A. Rubens, J. Haag, "DIAMETER NASREQ Extension," draft-calhoun-diameter-nasreq-03.txt, IETF work in progress, Apr. 2000.

[5] P. Calhoun and C. Perkins, "DIAMETER Mobile IP Extensions," draft-calhoun-diameter-mobileip-08.txt, IETF work in progress, June 2000.

[6] P. Calhoun, W. Bulley and S. Farrell, "DIAMETER Strong Security Extension," draft-calhoun-diameter-strong-crypto-03.txt, IETF work in progress, Apr. 2000.

[7] Pat R. Calhoun, "DIAMETER Base Protocol," draft-calhoun-diameter-15.txt, IETF work in progress, June 2000.

[8] Arkko, Calhoun and Patel, Zorn, "DIAMETER Accounting Extension," draft-calhoun-diameter-accounting-06.txt, IETF work in progress, June 2000.

[9] P. Calhoun and N. Greene, "DIAMETER Resource Management," draft-calhoun-diameter-res-mgmt-03.txt, IETF work in progress, Apr. 2000.

[10] R. Stewart *et al*., "Stream Control Transmission Protocol," draft-ietf-sigtran-sctp-13.txt, IETF work in progress, July 2000.

[11] Narten and Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 2434, Oct. 1998.

[12] Aboba and Beadles "The Network Access Identifier," RFC 2486, Jan. 1999.