



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년03월12일
(11) 등록번호 10-1242995
(24) 등록일자 2013년03월06일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) H04L 12/14 (2006.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2011-7013105
(22) 출원일자(국제) 2009년11월10일
심사청구일자 2011년06월08일
(85) 번역문제출일자 2011년06월08일
(65) 공개번호 10-2011-0082620
(43) 공개일자 2011년07월19일
(86) 국제출원번호 PCT/US2009/063811
(87) 국제공개번호 WO 2010/054354
국제공개일자 2010년05월14일
(30) 우선권주장
61/112,873 2008년11월10일 미국(US)
(56) 선행기술조사문헌
US20060251049 A1
US20080270618 A1
US20050226174 A1

(73) 특허권자
리서치 인 모션 리미티드
캐나다 온타리오 워털루 필립 스트리트 295 (우편
번호 엔2엘 3더블유8)
(72) 발명자
몬테무로 마이클
캐나다 온타리오 엘4더블유 0비4 미시사우가 타회
불바드 4701
알렌 앤드류
미국 일리노이주 60060 먼텔레인 맥래 라인 1937
버클리 애드리안
미국 캘리포니아주 95376 트레이시 먼클레어 라인
413
(74) 대리인
신정건, 김태홍

전체 청구항 수 : 총 93 항

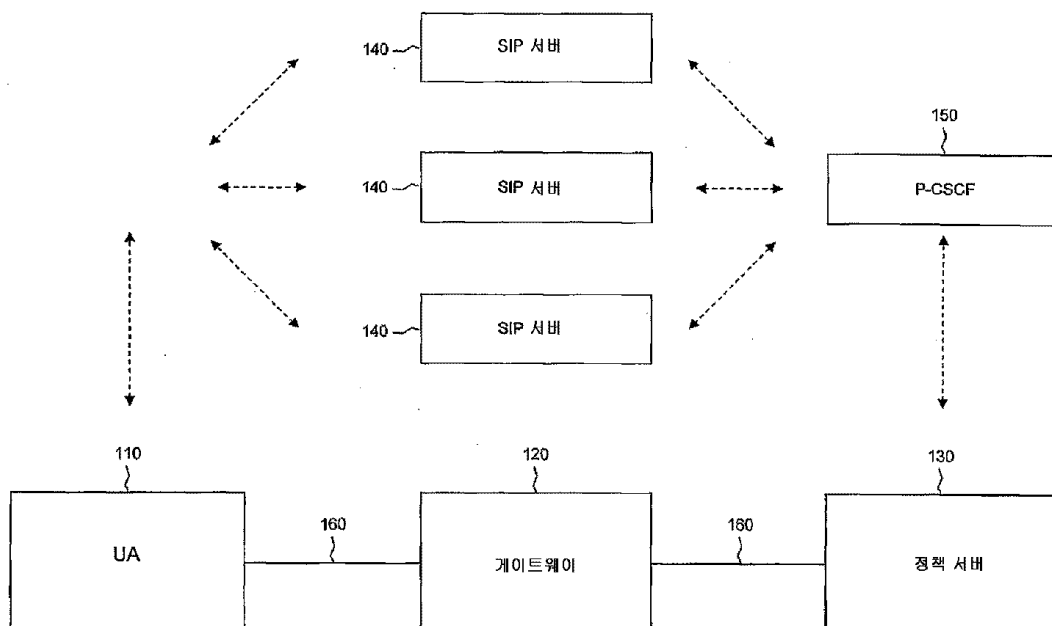
심사관 : 정은선

(54) 발명의 명칭 기존 허가 아키텍처 및 프로토콜을 이용하여 S I P 세션 정책을 지원하는 방법 및 시스템

(57) 요약

네트워크 컴포넌트로 세션 정책 요청을 전송하는 방법이 제공된다. 본 방법은 사용자 에이전트가 하위층 프로토콜을 이용하여 네트워크 컴포넌트에 세션 정책 요청을 전송하는 단계를 포함한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나이다.

대표도



특허청구의 범위

청구항 1

네트워크 컴포넌트에 세션 정책 요청(session policy request)을 전송하는 방법으로서,

사용자 에이전트가, 하위층 프로토콜을 이용하여 상기 세션 정책 요청을 상기 네트워크 컴포넌트로 전송하는 단계를 포함하고,

상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 2

제1항에 있어서, 상기 네트워크 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능부, 정책 제어 및 시행 기능부, 네트워크 액세스 서버, 게이트웨이, 및 라우터 중의 적어도 하나인 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 3

제1항에 있어서, 상기 세션 정책 요청은 상기 사용자 에이전트와 상기 네트워크 컴포넌트 사이의 중간 컴포넌트(intermediate component)를 통과하고, 상기 중간 컴포넌트는 게이트웨이, 액세스 포인트, 및 네트워크 액세스 서버 중의 적어도 하나인 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 4

제3항에 있어서, 상기 사용자 에이전트는 GPRS(General Packet Radio Service), GSM(Global System for Mobile Communications), EDGE(Enhanced Data rates for GSM Evolution), UTRAN(UMTS(Universal Mobile Telecommunications System) Terrestrial Radio Access Network), E-UTRAN(Evolved UTRAN), 3GPP UTRAN(Third Generation Partnership Project) UTRAN, 3GPP2 CDMA(Code Division Multiple Access), 802.11 WLAN(Wireless Local Area Network), 802.16 WMAN(Wireless Metropolitan Area Network), 802.20 WWAN(Wireless Wide Area Network), 802.22 WRAN(Wireless Regional Area Network), DOCSIS(Data Over Cable Service Interface Specification), 및 xDSL 패밀리를 포함하는 TISPAN (Telecoms and Internet converged Services and Protocols for Advanced Networks) 중의 적어도 하나를 포함하는 접속 액세스 네트워크를 통해 상기 중간 컴포넌트에 접속되는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 5

제3항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 상기 중간 컴포넌트 사이에서 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 상기 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 적어도 하나를 이용하여 상기 세션 정책 요청을 전송하는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 6

제1항에 있어서, 적어도 하나의 하위층 프로토콜의 유형-길이-값(type-length-value) 구조 능력(capability) 정보가 상기 세션 정책 요청을 표현하는데 사용되는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 7

제1항에 있어서, 상기 네트워크 컴포넌트는 상기 세션 정책 요청에 응답하여 상기 사용자 에이전트에 정책 문서를 제공하고, 상기 정책 문서는 이진수로 변환되어 사이즈를 줄이는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 8

제1항에 있어서, 상기 사용자 에이전트는 상기 사용자 에이전트에 의해 수신된 SIP(Session Initiation Protocol) 메시지 내의 URI(Uniform Resource Identifier)를 이용하여 상기 네트워크 컴포넌트에 접속하는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 9

제8항에 있어서, 상기 URI는 상기 SIP 메시지의 정책 접촉(Policy-Contact) 헤더 내에 있는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 10

제8항에 있어서, 상기 사용자 에이전트는 단일 네트워크 컴포넌트로 전송된 단일 세션 정책 요청을 통해 복수의 네트워크 컴포넌트에 접속하고, 상기 단일 네트워크 컴포넌트는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트와 접속하고, 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트로부터 정책 정보를 모으고(aggregating), 모든 정책 정보를 상기 사용자 에이전트로 제공하는 것인, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법.

청구항 11

네트워크 컴포넌트로의 세션 정책 요청(session policy request)을 위한 사용자 에이전트로서,

하위층 프로토콜을 이용하여 상기 세션 정책 요청을 상기 네트워크 컴포넌트로 전송하도록 구성되는 프로세서를 포함하고,

상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 사용자 에이전트.

청구항 12

제11항에 있어서, 상기 네트워크 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능부, 정책 제어 및 시행 기능부, 네트워크 액세스 서버, 게이트웨이, 및 라우터 중의 적어도 하나인 것인 사용자 에이전트.

청구항 13

제11항에 있어서, 상기 세션 정책 요청은 상기 사용자 에이전트와 상기 네트워크 컴포넌트 사이의 중간 컴포넌트를 통과하고, 상기 중간 컴포넌트는 게이트웨이, 액세스 포인트, 및 네트워크 액세스 서버 중의 적어도 하나인 것인 사용자 에이전트.

청구항 14

제13항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 상기 중간 컴포넌트 사이에서 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 상기 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 적어도 하나를 이용하여 상기 세션 정책 요청을 전송하는 것인 사용자 에이전트.

청구항 15

제13항에 있어서, 상기 사용자 에이전트는 GPRS(General Packet Radio Service), GSM(Global System for Mobile Communications), EDGE(Enhanced Data rates for GSM Evolution), UTRAN(UMTS(Universal Mobile Telecommunications System) Terrestrial Radio Access Network), E-UTRAN(Evolved UTRAN), 3GPP UTRAN(Third Generation Partnership Project) UTRAN, 3GPP2 CDMA(Code Division Multiple Access), 802.11 WLAN(Wireless Local Area Network), 802.16 WMAN(Wireless Metropolitan Area Network), 802.20 WWAN(Wireless Wide Area Network), 802.22 WRAN(Wireless Regional Area Network), DOCSIS(Data Over Cable Service Interface Specification), 및 xDSL 패밀리를 포함하는 TISPAN (Telecoms and Internet converged Services and Protocols for Advanced Networks) 중의 적어도 하나를 포함하는 접속 액세스 네트워크를 통해 상기 중간 컴포넌트에 접속되는 것인 사용자 에이전트.

청구항 16

제11항에 있어서, 적어도 하나의 하위층 프로토콜의 유형-길이-값(type-length-value) 구조 능력 정보가 상기 세션 정책 요청을 표현하는데 사용되는 것인 사용자 에이전트.

청구항 17

제11항에 있어서, 상기 네트워크 컴포넌트는 상기 세션 정책 요청에 응답하여 상기 사용자 에이전트에 정책 문서를 제공하고, 상기 정책 문서는 이진수로 변환되어 사이즈를 줄이는 것인 사용자 에이전트.

청구항 18

제11항에 있어서, 상기 사용자 에이전트는 상기 사용자 에이전트에 의해 수신된 SIP(Session Initiation Protocol) 메시지 내의 URI(Uniform Resource Identifier)를 이용하여 상기 네트워크 컴포넌트에 접촉하는 것인 사용자 에이전트.

청구항 19

제18항에 있어서, 상기 URI는 상기 SIP 메시지의 정책 접촉(Policy-Contact) 헤더 내에 있는 것인 사용자 에이전트.

청구항 20

제18항에 있어서, 상기 사용자 에이전트는 단일 네트워크 컴포넌트로 전송된 단일 세션 정책 요청을 통해 복수의 네트워크 컴포넌트에 접촉하고, 상기 단일 네트워크 컴포넌트는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트와 접촉하고, 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트로부터 정책 정보를 모으고, 모은 정책 정보를 상기 사용자 에이전트로 제공하는 것인 사용자 에이전트.

청구항 21

세션 정책을 제공하는 네트워크 컴포넌트로서,

하위층 프로토콜을 이용하여 전송된 세션 정책 요청을 수신하도록 구성되는 인증 컴포넌트를 포함하고,

상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 네트워크 컴포넌트.

청구항 22

제21항에 있어서, 상기 인증 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능부, 정책 제어 및 시행 기능부, 네트워크 액세스 서버, 게이트웨이, 및 라우터 중의 적어도 하나인 것인 네트워크 컴포넌트.

청구항 23

제21항에 있어서, 상기 세션 정책 요청은 사용자 에이전트로부터 중간 컴포넌트를 통해 상기 네트워크 컴포넌트로 전달되고, 상기 중간 컴포넌트는 게이트웨이, 액세스 포인트, 및 네트워크 액세스 서버 중의 적어도 하나인 것인 네트워크 컴포넌트.

청구항 24

제23항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 상기 중간 컴포넌트 사이에서 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 상기 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 적어도 하나를 이용하여 상기 세션 정책 요청을 전송하는 것인 네트워크 컴포넌트.

청구항 25

제23항에 있어서, 상기 사용자 에이전트는 GPRS(General Packet Radio Service), GSM(Global System for Mobile Communications), EDGE(Enhanced Data rates for GSM Evolution), UTRAN(UMTS(Universal Mobile

Telecommunications System) Terrestrial Radio Access Network), E-UTRAN(Evolved UTRAN), 3GPP UTRAN(Third Generation Partnership Project) UTRAN, 3GPP2 CDMA(Code Division Multiple Access), 802.11 WLAN(Wireless Local Area Network), 802.16 WMAN(Wireless Metropolitan Area Network), 802.20 WWAN(Wireless Wide Area Network), 802.22 WRAN(Wireless Regional Area Network), DOCSIS(Data Over Cable Service Interface Specification), 및 xDSL 패밀리를 포함하는 TISPAN (Telecoms and Internet converged Services and Protocols for Advanced Networks) 중의 적어도 하나를 포함하는 접속 액세스 네트워크를 통해 상기 중간 컴포넌트에 접속되는 것인 네트워크 컴포넌트.

청구항 26

제21항에 있어서, 적어도 하나의 하위층 프로토콜의 유형-길이-값(type-length-value) 구조 능력 정보가 상기 세션 정책 요청을 표현하는데 사용되는 것인 네트워크 컴포넌트.

청구항 27

제21항에 있어서, 상기 인증 컴포넌트는 상기 세션 정책 요청에 응답하여 사용자 에이전트에 정책 문서를 제공하고, 상기 정책 문서는 이진수로 변환되어 사이즈를 줄이는 것인 네트워크 컴포넌트.

청구항 28

제21항에 있어서, 사용자 에이전트는 상기 사용자 에이전트에 의해 수신된 SIP(Session Initiation Protocol) 메시지 내의 URI(Uniform Resource Identifier)를 이용하여 상기 인증 컴포넌트에 접속하는 것인 네트워크 컴포넌트.

청구항 29

제28항에 있어서, 상기 URI는 상기 SIP 메시지의 정책 접촉(Policy-Contact) 헤더 내에 있는 것인 네트워크 컴포넌트.

청구항 30

제28항에 있어서, 상기 사용자 에이전트는 단일 인증 컴포넌트로 전송된 단일 세션 정책 요청을 통해 복수의 인증 컴포넌트에 접속하고, 상기 단일 인증 컴포넌트는 상기 복수의 인증 컴포넌트 중 나머지 인증 컴포넌트와 접속하고, 상기 복수의 인증 컴포넌트 중 나머지 인증 컴포넌트로부터 정책 정보를 모으고, 모은 정책 정보를 상기 사용자 에이전트로 제공하는 것인 네트워크 컴포넌트.

청구항 31

네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법으로서,

상기 사용자 에이전트가, 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하는 단계를 포함하고,

상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 32

제31항에 있어서, 제1 URI는 SIP(Session Initiation Protocol) 기반 URI 및 SIPS URI(SIP Security URI) 중의 하나이며, 제2 URI는 상이한 프로토콜을 포함하는 다른 유형의 URI이고, 상기 제2 URI 및 상기 제1 URI는 동일한 정책 서버를 나타내는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 33

제32항에 있어서, 상기 사용자 에이전트는 URI 세트 중에서 복수의 URI 파라미터의 값을 비교하고, URI 세트의 2 이상의 URI 파라미터 간에 파라미터 값이 동일할 때, 상기 파라미터 값은 동일한 정책 서버를 나타내는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 34

제33항에 있어서, 상기 파라미터의 값은 상기 정책 서버의 호스트 이름, 상기 정책 서버의 도메인 이름, 상기 SIP 기반 URI, 상기 SIPS URI, 상기 URI 중의 하나와 관련된 인덱스, 및 상기 URI 중의 하나와 관련된 레이블 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 35

제31항에 있어서, 상기 사용자 에이전트가,

복수의 URI를 식별하는 단계,

상기 URI의 공통 파라미터에 기초하여 상기 URI에 포함된 값을 결정하는 단계; 및

상기 URI의 값들 중의 하나를 선택하여 정책 정보를 얻는 단계를 더 포함하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 36

제35항에 있어서, 상기 사용자 에이전트는 정책 채널 프로토콜을 이용하여 상기 정책 서버로부터 상기 정책 정보를 요청하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 37

제36항에 있어서, 상기 정책 채널 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 38

사용자 에이전트로서,

상기 사용자 에이전트가 네트워크에서 세션 정책으로의 액세스를 제공하는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하도록 구성되는 프로세서를 포함하고,

상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하는 것인 사용자 에이전트.

청구항 39

제38항에 있어서, 제1 URI는 SIP(Session Initiation Protocol) 기반 URI 및 SIPS URI(SIP Security URI) 중의 하나이며, 제2 URI는 상이한 프로토콜을 포함하는 다른 유형의 URI이고, 상기 제2 URI 및 상기 제1 URI는 동일한 정책 서버를 나타내는 것인 사용자 에이전트.

청구항 40

제39항에 있어서, 상기 사용자 에이전트는 URI 세트 중에서 복수의 URI 파라미터의 값을 비교하고, URI 세트의 2 이상의 URI 파라미터 간에 파라미터 값이 동일할 때, 상기 파라미터 값은 동일한 정책 서버를 나타내는 것인 사용자 에이전트.

청구항 41

제40항에 있어서, 상기 파라미터의 값은 상기 정책 서버의 호스트 이름, 상기 정책 서버의 도메인 이름, 상기 SIP 기반 URI, 상기 SIPS URI, 상기 URI 중의 하나와 관련된 인덱스, 및 상기 URI 중의 하나와 관련된 레이블 중의 적어도 하나인 것인 사용자 에이전트.

청구항 42

제38항에 있어서, 상기 사용자 에이전트는 또한,

복수의 URI를 식별하고,

상기 URI의 공통 파라미터에 기초하여 상기 URI에 포함된 값을 결정하고,

상기 URI의 값들 중의 하나를 선택하여 정책 정보를 얻도록 구성되는 것인 사용자 에이전트.

청구항 43

제42항에 있어서, 상기 사용자 에이전트는 정책 채널 프로토콜을 이용하여 상기 정책 서버로부터 상기 정책 정보를 요청하는 것인 사용자 에이전트.

청구항 44

제43항에 있어서, 상기 정책 채널 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 사용자 에이전트.

청구항 45

네트워크 컴포넌트로서,

상기 네트워크 컴포넌트가 네트워크에서 세션 정책으로의 액세스를 제공할 수 있는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 송신하도록 구성되는 프로세서를 포함하고,

상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하는 것인 네트워크 컴포넌트.

청구항 46

제45항에 있어서, 제1 URI는 SIP(Session Initiation Protocol) 기반 URI 및 SIPS URI(SIP Security URI) 중의 하나이며, 제2 URI는 상이한 프로토콜을 포함하는 다른 유형의 URI이고, 상기 제2 URI 및 상기 제1 URI는 동일한 정책 서버를 나타내는 것인 네트워크 컴포넌트.

청구항 47

제46항에 있어서, 상기 제1 URI 및 상기 제2 URI는 상기 정책 서버의 호스트 이름, 상기 정책 서버의 도메인 이름, 상기 SIP 기반 URI, 상기 SIP URI, 상기 URI 중의 하나와 관련된 인덱스, 및 상기 URI 중의 하나와 관련된 레이블 중의 적어도 하나를 공통으로 가짐으로써 동일한 정책 서버를 참조하도록 지정되는 것인 네트워크 컴포넌트.

청구항 48

네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법으로서,

상기 사용자 에이전트로부터 단일 네트워크 컴포넌트로 단일 세션 정책 요청을 전송하는 단계 - 상기 단일 네트워크 컴포넌트는 복수의 네트워크 컴포넌트에 접촉하고, 상기 단일 네트워크 컴포넌트로 상기 단일 세션 정책 요청을 전송하는 단계는 하위층 프로토콜을 이용하고, 상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나임 -;

정책 정보를 모으는 단계; 및

상기 사용자 에이전트로 상기 모은 정책 정보를 제공하는 단계를 포함하는 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 49

제48항에 있어서, 상기 모은 정책 정보는 상기 단일 네트워크 컴포넌트에서 수집된 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 50

제48항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 중간 컴포넌트 사이에서 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 상기 단일 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 하나를 이용하여 상기 세션 정책 요청을 전송하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 51

제48항에 있어서, 상기 세션 정책 요청은 PROXY-TO 파라미터를 포함하고, 상기 PROXY-TO 파라미터는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트 중의 하나 이상을 나타내는 적어도 하나의 URI를 포함하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 52

제48항에 있어서, 정책 서버들 간의 프로토콜을 이용하여 상기 복수의 네트워크 컴포넌트 사이에서 상기 모은 정책 정보를 송신하는 단계를 더 포함하는, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 53

제48항에 있어서, 상기 단일 네트워크 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능부, 정책 제어 및 시행 기능부, 네트워크 액세스 서버, 게이트웨이, 및 라우터 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 54

사용자 에이전트로서,

단일 세션 정책 요청의 전송에 응답하여 복수의 네트워크 컴포넌트에 대한 모은 정책 정보를 수신하도록 구성되는 프로세서를 포함하고,

상기 사용자 에이전트는 상기 세션 정책 요청을 하위층 프로토콜을 이용하여 단일 네트워크 컴포넌트에 전송하고, 상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 사용자 에이전트.

청구항 55

제54항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 중간 컴포넌트 사이에서 상기 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 단일 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 적어도 하나를 이용하여 상기 세션 정책 요청을 전송하는 것인 사용자 에이전트.

청구항 56

제54항에 있어서, 상기 세션 정책 요청은 PROXY-TO 파라미터를 포함하고, 상기 PROXY-TO 파라미터는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트를 나타내는 적어도 하나의 URI를 포함하는 것인 사용자 에이전트.

청구항 57

제54항에 있어서, 상기 사용자 에이전트는 또한, 정책 서버들 간의 프로토콜을 이용하여 네트워크 컴포넌트 사이에서 상기 모은 정책 정보를 송신하도록 구성되는 것인 사용자 에이전트.

청구항 58

네트워크 컴포넌트로서,

단일 세션 정책 요청을 수신하고 복수의 네트워크 컴포넌트로부터의 정책 정보의 모음에 응답하여 상기 모은 정책 정보를 전송하도록 구성되는 프로세서를 포함하고,

네트워크 컴포넌트가 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 하위층 프로토콜을 통해 사용자 에이전트로부터 상기 세션 정책 요청을 수신하는 것인 네트워크 컴포넌트.

청구항 59

제58항에 있어서, 적어도 하나의 하위층 프로토콜은 상기 사용자 에이전트와 중간 컴포넌트 사이에서 상기 세션 정책 요청을 전송하는데 사용되고, 적어도 하나의 하위층 프로토콜 프레임은 상기 중간 컴포넌트와 상기 네트워크 컴포넌트 사이에서 DIAMETER 프로토콜 및 RADIUS 프로토콜 중의 적어도 하나를 이용하여 상기 세션 정책을 전송하는 것인 네트워크 컴포넌트.

청구항 60

제58항에 있어서, 상기 네트워크 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능부, 정책 제어 및 시행 기능부, 네트워크 액세스 서버, 게이트웨이, 및 라우터 중의 적어도 하나인 것인 네트워크 컴포넌트.

청구항 61

네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법으로서,

상기 사용자 에이전트가 제1 네트워크 노드로 등록 메시지를 전송하는 단계; 및

상기 사용자 에이전트가 상기 등록 메시지에 응답하여 상기 제1 네트워크 노드로부터 정책 관련 정보를 수신하는 단계를 포함하고,

상기 정책 관련 정보는 상기 세션 정책, 상기 세션 정책을 지시하는 URI, 및 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 62

제61항에 있어서, 상기 제1 네트워크 노드는 서빙 콜 세션 제어 기능부 및 레지스트리(registrar) 중의 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 63

제61항에 있어서, 상기 제1 네트워크 노드를 통해 상기 정책 관련 정보를 포함하는 제2 네트워크 노드로의 등록이 이루어지고, 상기 사용자 에이전트는 상기 제2 네트워크 노드로부터 상기 정책 관련 정보를 수신하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 64

제63항에 있어서, 상기 제2 네트워크 노드는 SIP 서버 및 정책 서버 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 65

제63항에 있어서, 상기 제2 네트워크 노드가, 정책 관련 정보의 수신을 야기시키는 하위층 프로토콜 프레임 요청을 수행할 것을 상기 사용자 에이전트에게 통지하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 66

제65항에 있어서, 상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 67

제61항에 있어서, 상기 제1 네트워크 노드를 통해 상기 정책 관련 정보를 포함하는 제2 네트워크 노드로의 등록이 이루어지고, 상기 사용자 에이전트는 상기 제1 네트워크 노드로부터 정책 관련 정보를 수신하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 68

제67항에 있어서, 상기 제1 네트워크 노드가, 정책 관련 정보의 수신을 야기시키는 하위층 프로토콜 프레임 요청을

청을 수행하였음을 상기 사용자 에이전트에게 통지하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 69

제67항에 있어서, 상기 제1 네트워크 노드는 SIP 서버 및 정책 서버 중의 적어도 하나인 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 70

제61항에 있어서, 상기 사용자 에이전트는 단일 네트워크 컴포넌트로 전송되는 등록 메시지를 통해 복수의 네트워크 컴포넌트와 접촉하고, 상기 단일 네트워크 컴포넌트는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트와 접촉하고, 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트로부터 정책 정보를 모으고, 상기 사용자 에이전트에 상기 모은 정책 정보를 제공하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 71

제70항에 있어서, 상기 모은 정책 정보는 proxy-to 파라미터를 이용하여 제공되는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 72

제61항에 있어서, 상기 사용자 에이전트는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하고, 상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하고, 상기 사용자 에이전트는 상기 복수의 URI 중 어느 URI를 사용하여 상기 정책 서버로부터 정책 문서를 얻을지를 결정하는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 73

제72항에 있어서, 상기 복수의 URI의 임의의 것은 alternative_URI 파라미터에서 제공되는 것인, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 74

제61항에 있어서, 정책 서버들 간의 프로토콜을 이용하여 네트워크 컴포넌트들 사이에서 모은 정책 정보를 송신하는 단계를 더 포함하는, 네트워크에서 사용자 에이전트가 세션 정책을 액세스하는 방법.

청구항 75

사용자 에이전트로서,

상기 사용자 에이전트가 등록 메시지를 전송하고 상기 등록 메시지에 응답하여 제1 네트워크 노드로부터 정책 관련 정보를 수신하도록 구성되는 프로세서를 포함하고,

상기 정책 관련 정보는 상기 사용자 에이전트가 통신할 수 있는 네트워크에 대한 세션 정책, 상기 세션 정책을 지시하는 URI, 및 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나인 것인 사용자 에이전트.

청구항 76

제75항에 있어서, 상기 제1 네트워크 노드를 통해 상기 정책 관련 정보를 포함하는 제2 네트워크 노드로의 등록이 이루어지고, 상기 사용자 에이전트는 상기 제2 네트워크 노드로부터 정책 관련 정보를 수신하는 것인 사용자 에이전트.

청구항 77

제76항에 있어서, 상기 제2 네트워크 노드가, 정책 관련 정보의 수신을 야기시키는 하위층 프로토콜 프레임 요청을 수행할 것을 상기 사용자 에이전트에게 통지하는 것인 사용자 에이전트.

청구항 78

제77항에 있어서, 상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 사용자 에이전트.

청구항 79

제75항에 있어서, 상기 제1 네트워크 노드를 통해 상기 정책 관련 정보를 포함하는 제2 네트워크 노드로의 등록이 이루어지고, 상기 사용자 에이전트는 상기 제1 네트워크 노드로부터 정책 관련 정보를 수신하는 것인 사용자 에이전트.

청구항 80

제79항에 있어서, 상기 제1 네트워크 노드가 하위층 프로토콜 프레임 요청을 수행하였음을 상기 사용자 에이전트에게 알림으로써 정책 관련 정보를 수신하도록 하는 것인 사용자 에이전트.

청구항 81

제75항에 있어서, 상기 사용자 에이전트는 단일 네트워크 컴포넌트로 전송되는 등록 메시지를 통해 복수의 네트워크 컴포넌트와 접촉하고, 상기 단일 네트워크 컴포넌트는 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트와 접촉하고, 상기 복수의 네트워크 컴포넌트 중 나머지 네트워크 컴포넌트로부터 정책 정보를 모으고, 상기 사용자 에이전트에 상기 모은 정책 정보를 제공하는 것인 사용자 에이전트.

청구항 82

제81항에 있어서, 상기 모은 정책 정보는 proxy-to 파라미터를 이용하여 제공되는 것인 사용자 에이전트.

청구항 83

제75항에 있어서, 상기 사용자 에이전트는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하고, 상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하고, 상기 사용자 에이전트는 상기 복수의 URI 중 어느 URI를 사용하여 상기 정책 서버로부터 정책 문서를 얻을지를 결정하는 것인 사용자 에이전트.

청구항 84

제83항에 있어서, 상기 복수의 URI의 임의의 것은 alternative_URI 파라미터에서 제공되는 것인 사용자 에이전트.

청구항 85

네트워크 노드로서,

상기 네트워크 노드가 등록 메시지의 수신에 응답하여 사용자 에이전트로 정책 관련 정보를 전송하도록 구성되는 프로세서를 포함하고,

상기 정책 관련 정보는 상기 네트워크 노드가 컴포넌트인 네트워크에 대한 세션 정책, 상기 세션 정책을 지시하는 URI, 및 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나인 것인 네트워크 노드.

청구항 86

제85항에 있어서, 상기 네트워크 노드는 서빙 콜 세션 제어 기능부 및 레지스트러(registrar) 중의 하나인 것인 네트워크 노드.

청구항 87

제85항에 있어서, 중간 네트워크 컴포넌트를 통해 상기 네트워크 노드로의 등록이 이루어지고, 상기 네트워크 노드는 상기 정책 관련 정보를 포함하는 것인 네트워크 노드.

청구항 88

제85항에 있어서, 상기 네트워크 노드는, 상기 정책 관련 정보의 전송을 야기시키는 하위층 프로토콜 프레임 요청을 수행할 것을 상기 사용자 에이전트에게 통지하는 것인 네트워크 노드.

청구항 89

제88항에 있어서, 상기 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 것인 네트워크 노드.

청구항 90

제85항에 있어서, 상기 네트워크 노드는, 사용자 에이전트로부터 등록 메시지를 수신하면, 다른 복수의 네트워크 컴포넌트에 접속하고, 상기 다른 복수의 네트워크 컴포넌트로부터 정책 정보를 모으고, 상기 모은 정책 정보를 상기 사용자 에이전트에 제공하는 것인 네트워크 노드.

청구항 91

제85항에 있어서, 상기 네트워크 노드는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 사용자 에이전트로 전송하고, 상기 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용하고, 상기 사용자 에이전트는 상기 복수의 URI 중 어느 URI를 사용하여 상기 정책 서버로부터 정책 문서를 얻을지를 결정하는 것인 네트워크 노드.

청구항 92

제91항에 있어서, 상기 복수의 URI의 임의의 것은 alternative_URI 파라미터에서 제공되는 것인 네트워크 노드.

청구항 93

제85항에 있어서, 상기 네트워크 노드는 또한, 정책 서버들 간의 프로토콜을 이용하여 네트워크 컴포넌트들 사이에서 모은 정책 정보를 송신하도록 구성되는 것인 네트워크 노드.

명세서

배경 기술

[0001]

인터넷 프로토콜(IP; Internet Protocol) 멀티미디어 서브시스템(IMS; IP Multimedia Subsystem)은 이동 및 고정 사용자 에이전트(UA; user agent)에 멀티미디어 서비스 및 VoIP(voice-over-IP) 호를 제공하는 표준 아키텍처이다. SIP(Session Initiation Protocol)는 IMS 기반 호 또는 세션을 생성, 변경 및 종료하는 시그널링 프로토콜로서 IETF(Internet Engineering Task Force)에 의해 주로 표준화되고 관리되어 왔다. 여기에 사용된 바와 같이, “사용자 에이전트” 및 “UA”라는 용어는 어떤 경우에는 이동 전화, 개인 휴대 단말기, 핸드헬드 또는 랩탑 컴퓨터 및 텔레커뮤니케이션 능력을 갖는 유사 장치 등의 이동 장치를 지칭한다. 이러한 UA는 UA 및, 제한되지 않지만, SIM(Subscriber Identity Module (SIM) 애플리케이션, USIM(Universal Subscriber Identity Module) 애플리케이션 또는 R-UIM(Removable User Identity Module) 애플리케이션을 포함하는 UICC(Universal Integrated circuit Card) 등의 관련된 제거가능 메모리 모듈을 포함할 수 있다. 대안으로, 이러한 UA는 그러한 모듈이 없는 장치를 포함할 수 있다. 다른 경우, “UA”라는 용어는 고정 라인 전화, 데스크탑 컴퓨터, 셋탑 박스 또는 네트워크 노드 등의 유사한 성능을 갖지만 운반가능하지 않은 장치를 지칭할 수 있다. UA가 네트워크 노드이면, 네트워크 노드는 UA 또는 고정 라인 장치 등의 다른 기능을 대행할 수 있고 UA 또는 고정 라인 장치를 시뮬레이팅하거나 에뮬레이팅할 수 있다. 예를 들어, 임의의 UA에 대하여, 일반적으로 장치에 상주하는 IMS SIP 클라이언트가 실제로 네트워크에 상주하고 최적화된 프로토콜을 이용하여 SIP 메시지 정보를 그 장치로 중개한다. 즉, UA에 의해 전통적으로 수행되었던 임의의 기능은 원격 UA의 형태로 분산될 수 있고, 이 원격 UA는 네트워크 내의 UA를 나타낸다. ” UA”라는 용어는 또한, 제한되지는 않지만, SIP 세션을 포함할 수 있는 통신 세션을 종료할 수 있는 임의의 하드웨어 또는 소프트웨어 컴포넌트를 지칭할 수 있다. 또한, “사용자 에이전트”, “UA”, “사용자 기기”, “UE” 및 “노드”라는 용어는 여기에서 동의어로 사용될 수 있다.

도면의 간단한 설명

[0002]

본 개시물의 더 완벽한 이해를 위해, 첨부된 도면 및 상세한 설명과 연결하여 다음의 간단한 설명은 참조한다. 동일한 참조 번호는 동일한 부분을 나타낸다.

도 1은 종래 기술에 따른 SIP 세션의 확립을 위한 흐름도.

도 2는 종래 기술에 따른 정책(policy) 아키텍처를 나타내는 도면.

도 3은 종래 기술에 따른 정책 및 과금 제어 아키텍처를 나타내는 도면.

도 4는 본 개시물의 실시예에 따른 텔레커뮤니케이션 시스템을 나타내는 도면.

도 5는 본 개시물의 실시예에 따른 프로토콜 스택을 나타내는 도면.

도 6은 본 개시물의 실시예에 따른 액세스 네트워크를 나타내는 도면.

도 7은 본 개시물의 실시예에 따른 다른 액세스 네트워크를 나타내는 도면.

도 8은 본 개시물의 실시예에 따른 또 다른 액세스 네트워크를 나타내는 도면.

도 9는 본 개시물의 실시예에 따른 또 다른 액세스 네트워크를 나타내는 도면.

도 10은 본 개시물의 실시예에 따른 또 다른 액세스 네트워크를 나타내는 도면.

도 11은 본 개시물의 실시예에 따른 또 다른 액세스 네트워크를 나타내는 도면.

도 12는 본 개시물의 실시예에 따른 또 다른 액세스 네트워크를 나타내는 도면.

도 13은 본 개시물의 실시예에 따라 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법을 나타내는 도면.

도 14는 본 개시물의 실시예에 따라 사용자 에이전트가 네트워크에서 세션 정책을 액세스하는 방법을 나타내는 도면.

도 15는 본 개시물의 실시예에 따른 다수 접속된 정책 제어 및 과금 규칙 기능을 나타내는 도면.

도 16은 본 개시물의 다른 실시예에 따라 사용자 에이전트가 네트워크에서 세션 정책을 액세스하는 방법을 나타내는 도면.

도 17은 본 개시물의 다른 실시예에 따라 사용자 에이전트가 네트워크에서 세션 정책을 액세스하는 방법을 나타내는 도면.

도 18은 본 개시물의 몇 가지 실시예를 구현하는데 적합한 프로세서 및 관련 컴포넌트를 나타내는 도면.

발명을 실시하기 위한 구체적인 내용

[0003]

본 개시물의 하나 이상의 실시예의 구체적인 구현예가 이하에 제공되지만, 개시된 시스템 및/또는 방법은 현재 공지되거나 현존하는 임의의 수의 기술을 이용하여 구현될 수 있음을 이해해야 한다. 본 개시물은 여기에 기재되는 예시적인 설계 및 구현예를 포함하는 이하에서 설명하는 구체적인 구현예, 도면 및 기술에 한정되지 않으며, 첨부된 청구범위 및 그 동등물 내에서 변경될 수 있다.

[0004]

SIP RFC (Request for Comments) 3261은 멀티미디어 세션을 생성, 변경 및 종료하는 시그널링 프로토콜이다. SIP 내의 중심 요소는 프록시(proxy) 서버이다. 프록시 서버는 라우팅(routing), 랑데부(rendezvous), 인증(authentication), 허가(authorization), 이동성 및 다른 시그널링 서비스를 요청하는 중재자이다. 그러나, 프록시는 SIP가 확립한 실제 세션 - 오디오, 비디오, 및 세션 모드 메시지 -로부터 분리된다. 세션의 세부 사항은 SIP 메시지의 페이로드에서 전달되고 일반적으로 SDP(Session description Protocol) RFC 4566 및 RFC 3264로 기재된다.

[0005]

경험을 통해 세션의 형태에 영향을 주는 SIP 중재자가 필요하다는 것을 알 수 있다. 세션 파라미터는 일반적으로 세션 정책의 시행을 통해 제어된다. 예를 들어, SIP는 미디어 트래픽에 대한 제한된 리소스를 갖는 무선 네트워크에 이용될 수 있다. 활동성이 높은 기간 동안, 무선 네트워크 제공자는 각 사용자에게 이용가능한 대역폭의 양을 제한하기를 원한다. 세션 정책으로, 무선 네트워크의 중재자는 UA에게 이용가능한 대역폭을 알릴 수 있다. 이 정보는 UA가 세션에서 성공적으로 이용할 수 있는 스트림의 수, 미디어 유형, 및 코덱을 결정할 수 있도록 한다. 마찬가지로, 네트워크 제공자는 사용자가 사용할 수 있는 미디어 유형의 세트를 정의하는 사용자와의 서비스 레벨 협정을 가질 수 있다. 네트워크는 사용자 에이전트에 현재의 정책 세트를 전달하여 사용자

에이전트가 무심코 임의의 네트워크 정책을 어기지 않고 세션을 설정하도록 할 수 있다.

- [0006] 다른 예에서, SIP UA는 방화벽 또는 네트워크 경계 장치를 통해 공공 인터넷에 연결된 네트워크를 이용하고 있다. 네트워크 제공자는 미디어 스트림을 방화벽 또는 경계 장치 상의 특정 IP 어드레스 및 포트로 보내어 공공 인터넷에 도달하도록 할 필요가 있다는 것을 UA에게 전하기를 원한다. 이 정책을 알면, UA는 방화벽 또는 네트워크 경계를 건너 세션을 설정한다. 미디어 중재자를 삽입하는 다른 방법과 달리, 세션 정책의 사용은 SIP 메시징 바디의 검사 또는 변경을 필요로 하지 않는다.
- [0007] 도메인(domain)은 종종 자신의 세션 정책을 시행할 필요성을 갖는다. 예를 들어, 도메인은 비디오의 사용을 허용하지 않는 정책 및 비디오 인코딩을 포함하는 모든 패킷을 드롭(drop)하는 시행 메커니즘을 가질 수 있다. 불행하게도, 이들 시행 메커니즘은 통상 사용자에게 시행할 정책에 대하여 알리지 않는다. 대신에, 사용자가 어떤 일을 수행하는 것을 조용히 방지한다. 이것은 사용자가 이해할 수 없는 장치의 오작동을 초래할 수 있다. 세션 정책으로, 사용자는 현재의 네트워크 정책에 대하여 알고 정책에 따른 세션을 설정하거나 덜 엄중한 정책으로 간단히 도메인에 연결할 수 있다. 따라서, 세션 정책은 시행과 결합된 동의의 중요한 결합을 제공한다. 즉, 사용자는 정책을 파악하여 그에 대한 동작을 할 필요가 있지만, 제공자는 여전히 정책을 시행할 권리를 보유한다.
- [0008] IETF는 draft-sip-session-policy-framework-05에서 세션 정책 프레임워크를 정의하여 네트워크가 SIP UA로 현재의 정책 세트를 전달하도록 하여, SIP UA가 임의의 네트워크 정책을 무심코 어기지 않고 세션을 설정하도록 할 수 있다.
- [0009] 2가지 유형의 세션 정책, 즉, 세션-특정 정책 및 세션-독립 정책이 정의되었다. 세션-특정 정책은 세션의 설명(description)에 기초하여 특정한 하나의 세션을 위해 생성된 정책이다. 이 세션-특정 정책은 네트워크 중재자가 UA가 제안하는 세션의 설명을 검사하고 그 세션 설명에 대한 정책을 반환할 수 있다. 예를 들어, 중재자는 제안된 세션 설명에서 각각의 미디어 스트림에 대한 방화벽/NAT(network session translation) 내의 핀홀(pinhole)을 개방할 수 있다. 그 후, 중재자는 UA의 IP 어드레스 및 포트를 외부 소스로부터 도달할 수 있는 방화벽/NAT에서 개방된 것으로 대체하는 세션 설명에 대한 정책을 반환할 수 있다. 세션-특정 정책은 세션에 맞추어지기 때문에, 세션-특정 정책이 생성되는 세션에 세션-특정 정책이 적용된다. 세션-특정 정책은 세션이 확립될 때 세션 별로 생성된다.
- [0010] 반면에, 세션-독립 정책은 세션과 독립적으로 생성되어 UA에 의해 설정되는 모든 SIP 세션에 일반적으로 적용되는 정책이다. 세션-독립 정책은 예를 들어 UA에게 기존의 대역폭 제한 또는 미디어 유형 제한을 알리는데 사용될 수 있다. 이들 정책은 특정 세션 설명에 기초하지 않기 때문에, 세션 설정 시도와 무관하게 생성될 수 있고, 초기화될 때(예를 들어, 장치가 파워 온될 때) 및 정책이 변경될 때만 UA에 전달될 필요가 있다.
- [0011] 이하에서 설명하는 메커니즘은 세션-독립 정책 및 세션-특정 정책을 위해 사용될 수 있다. 세션-특정 정책(SIP 요청 또는 SIP 응답에 응답하여 제공되는 정책)을 위해, PolicyOffer(정책 제안) 또는 Policyanswer(정책 대답) 문서는 UA로 반환될 수 있다. 세션-독립 정책(세션 전에 UA에 제공되는 정책)을 위해, 세션 정책 문서가 복귀될 수 있다.
- [0012] 미디어 정책에 더하여, 여기에서 정의된 메커니즘은 UA에게 SDP 제안 또는 대답에 상이한 IP 어드레스를 이용하고, 방화벽 또는 NAT를 처리하고, 트랜스코더 또는 다른 미디어 릴레이를 통해 미디어를 라우팅한다는 것을 알리는데 사용될 수 있다.
- [0013] 3GPP(Third Generation Partnership Project)는 이동 또는 일반 전화 네트워크를 위한 멀티미디어 서비스에 대한 차세대 SIP/IP 기반 네트워크로서 IP 멀티미디어 서브시스템(IMS)을 표준화하였다. 3GPP IMS에 대한 아키텍처는 3GPP TS(Technical Specification) 23.228에 명시되어 있다. 3GPP TS 23.228에서는, S-CSCF(Serving Call session Control Function) 및 P-CSCF(Proxy Call Session Control Function)을 포함하는 IMS 요소의 기능이 명시되어 있다. S-CSCF는 SIP 레지스트라(registrar) 및 RFC 3261에 정의된 SIP 프로키로서 동작한다. P-CSCF는 SIP 프로키로서 동작한다. 3GPP IMS는 세션 시그널링을 위한 SIP를 이용하고, 상술한 바와 같이, IMS 네트워크 엔티티(P-CSCF 및 S-CSCF)는 (스트림의 수, 미디어 유형 및 코덱 등의) 세션의 형태에 영향을 줄 필요가 있다.
- [0014] 3GPP는 IMS 베어러(bearer) 리소스로의 UA 액세스를 위한 필요한 허가 및 회계 기능을 수행하는 정책 및 과금 제어(PCC)에 대한 아키텍처를 정의하였다. PCC 아키텍처는 정책 서버 및 다양한 소스로부터의 입력에 기초하여, (스트림의 수, 미디어 유형 및 코덱 등의) 세션의 속성 및 특성에 기초한 베어러 액세스에 대하여 어떤 UA

가 허용되는지를 결정하는 정책 제어 및 과금 규칙 기능(Policy Control and Charging Rules (PCRF) function)을 포함한다. PCRF는 가입 기반 정책에 대한 가입 프로파일 저장소(Subscription Profile Repository; SPR) 및 애플리케이션-특정 입력에 대한 AF(Application Function)와 인터페이스한다. IMS가 PCC와 함께 사용되면, AF는 SIP 세션 시그널링에 기초하여 PCRF에 영향을 줄 수 있는 SIP 프록시, P-CSCF이다. PCRF는 정책이 시행되도록 게이팅 및 필터링 기능을 제공하는 PCEF(Policy Control Enforcement Function)과 인터페이스한다. PCEF는 액세스 네트워크 특정 게이트웨이(예를 들어, GGSN, PDG, PDSN 또는 CMTS)와 통합된다. 이들 엔티티는 DIAMETER 또는 RADIUS 프로토콜을 이용하여 통신하고 AAA(Authentication Authorization Accounting) 인프라스트럭처의 일부를 형성한다. 여기에 기재된 정책 서버는 PCRF로 제한되지 않는다. P-CSCF와 통합된 정책 서버 등의 다른 실시예가 가능하다.

[0015] 현재, 3GPP는 TS 24.229에서 본래의 SIP INVITE 요청이 네트워크 정책이 허용하지 않는 미디어 유형 또는 코덱을 포함하면 SIP 488 응답을 보내는 SIP 프록시에 기반하여 IMS에 대한 세션 정책 감시 메커니즘을 정의하였다. RFC 3261 및 3GPP TS 24.229에 명시된 바와 같이, 488 응답은 호출하는 UA가 허용될 수 있는 SDP로 요청을 제시할 수 있도록 허용되는 미디어 유형 및 코덱의 SDP 설명을 포함한다. 그러나, 이러한 접근법은 SIP 요청이 각각의 도메인을 가로지르기 때문에 모든 도메인이 자신의 정책 세트를 가질 필요가 있다는 문제가 있다. 로밍 상황에서, 단일 SIP 요청이 4 이상의 상이한 IMS 도메인을 가로지를 수 있고 각각의 도메인에 의해 SIP 488 응답을 되돌려 보낼 수 있다. 잠재적으로, 각 도메인 내의 각 프록시는 SIP 488 응답으로 SIP INVITE 요청을 거절하여 SIP INVITE 요청이 호출되는 UA에 도달되기 전에 호출하는 UA가 5개 (또는 그 이상)의 SIP INVITE 요청을 전송(및 4개 이상의 SIP 488 응답을 수신)할 수 있다. 이것은 심하게 지연된 세션 설정을 초래한다.

[0016] 또한, 이 메커니즘은 RFC 3261에서 허용되는 SDP를 포함하지 않는 SIP INVITE 요청에 대하여 동작하지 않고, SDP가 없는 초기 SIP INVITE는 전송되고, 호출된 UA는 응답으로 SDP 제안을 되돌려 보낼 수 있고, 호출자는 ACK 요청에 SDP 대답을 반환한다. SIP 응답은 요청에 응답하여 전송될 수 있기 때문에, 응답은 488 응답으로 거절될 수 없다. 그러므로, 3GPP IMS는 (정책을 알고 있는) 네트워크 서버 및 SIP INVITE 요청이 발생하는 외부 IMS 네트워크로부터 들어오는 SIP INVITE 요청을 허용함으로써 제안없는 SIP INVITE 요청의 사용을 제한하였다. 이 경우, 세션이 정책과 반대의 코덱으로 확립되면, BYE로 즉시 종료된다. 이 상황은 만족스럽지 못하다.

[0017] 추가적으로, 3GPP PCC 아키텍처는 SIP 시그널링으로부터 SDP를 분석하는 P-CSCF에 의존하여 세션을 위한 베어러 리소스의 허가에 대한 PCRF로의 입력을 제공한다. 호출된 UA에 대하여, 호출된 UA에 의해 수락되는 미디어 유형 및 코덱에 기초하여 베어러 리소스를 허가하기 위하여, 응답으로 전송된 SDP 대답이 P-CSCF에 의해 요구된다. 이것은 호출된 UA는 대답을 전송하기 전에 SDP 대답을 포함하는 임시의(1xx) 응답을 전송할 필요가 있다는 것을 의미한다. IMS는 전제조건 프레임워크 RFC 3312를 이용하므로, 이 임시의 응답은 신뢰성있게 전송될 필요가 있다. 이것은 추가의 SIP PRACK 요청 및 200OK 응답이 교환되도록 하고 따라서, 끝에서 끝까지 교환되는 추가의 불필요한 SIP 메시지에 의해 호 설정 시간이 상당히 지연된다.

[0018] 도 1은 SIP 세션이 확립된 세션 정책 프레임워크의 기본 IETF SIP 아키텍처를 나타내는 draft-sip-session-policy-framework-05로부터의 흐름도이다. 이벤트(12)에서, 제1 UA_A(110_A)는 SDP 제안을 포함하는 SIP INVITE 메시지를 제1 프록시_A(120_A)로 전송한다. 이벤트(14)에서, 제1 프록시_A(120_A)는 정책 접촉 헤더를 포함하는 488 메시지를 제1 UA_A(110_A)로 전송한다. 제1 UA_A(110_A)는 제1 프록시_A(120_A)에게 ACK 메시지를 반환한다. 이벤트(16)에서, 제1 UA_A(110_A)는 InfoOffer(정보 제안)을 포함하는 PolicyChannel(정책 채널) 메시지를 제1 정책 서버_A(130_A)으로 전송한다. 이벤트(18)에서, 제1 정책 서버_A(130_A)은 PolicyOffer(정책 제안)을 포함하는 정책 채널 메시지를 제1 UA_A(110_A)로 전송한다.

[0019] 이벤트(20)에서, 제1 UA_A(110_A)는 SDP 제안을 포함하는 INVITE 메시지를 제1 프록시_A(120_A) 및 제2 프록시_B(120_B)를 통해 제2 UA_B(110_B)로 전송한다. 이벤트(22)에서, 제2 UA_B(110_B)는 InfoOffer(정보 제안) 및 InfoAnswer(정보 대답)를 포함하는 정책 채널 메시지를 제2 정책 서버_B(130_B)로 전송한다. 이벤트(24)에서, 제2 정책 서버_B(130_B)은 Policyoffer 및 PolicyAnswer를 포함하는 정책 채널 메시지를 제2 UA_B(110_B)로 전송한다. 이벤트(26)에서, 제2 UA_B(110_B)는 SIP 200OK 대답을 제2 프록시_B(120_B) 및 제1 프록시_A(120_A)를 통해 제1 UA_A(110_A)로 전송한다. 제1 UA_A(110_A)는 SIP ACK 메시지를 제2 UA_B(110_B)로 돌려보낸다. 이벤트(28)에서, 제1 UA_A(110_A)는 InfoAnswer를 포함하는 정책 채널 메시지를 제1 프록시_A(120_A)로 전송한다. 이벤트(30)에서, 제1 프록시_A(120

_A)는 PolicyAnswer를 포함하는 정책 채널 메시지를 제1 UA_A(110_A)로 전송한다.

- [0020] 다음의 엔티티, 즉, UA, 프록시, 정책 서버 및 가능하면 정책 시행 엔티티는 일반적으로 세션-특정 정책에 필요하다. 이들 엔티티에 대한 정책 아키텍처는 도 2에 도시된다. UA(110)는 SIP 시그널링(125)을 통해 프록시(120)와 통신하고 정책 채널(135)을 통해 정책 서버(130)와 통신한다. 미디어(145)는 UA(110) 및 정책 시행 컴포넌트(140) 사이에서 교환될 수 있다.
- [0021] 프록시(120)는 UA(110) 및 정책 서버(130)를 위한 랑데부 메커니즘을 제공한다. 이것은 각각의 UA(110)는 그 도메인 내에서 정책 서버(130)의 URI(Uniform Resource Identifier)를 얻어 정책을 검색할 위치를 알 수 있다. UA가 정책 서버 URI를 아직 수신하지 않은 경우(예를 들어, 이전의 호 또는 구성 등의 다른 수단으로) 프록시(120)는 정책 서버 URI를 UA(110)로 전달한다. 프록시(120)는 실제 정책을 UA(110)로 전달하지 않는다. 대신에, 프록시(120)는 UA(110)에 UA(110)가 정책 문서 또는 다른 정책 정보를 검색할 수 있는 정책 서버(130)에 대한 URI 또는 다른 식별자를 제공한다.
- [0022] 정책 서버(130)는 프록시(120)와 물리적으로 같은 위치에 위치할 수 있는 별도의 논리적 엔티티이다. 정책 서버(130)의 역할은 UA(110)에 세션 정책을 전달하는 것이다. 정책 서버(130)는 UA(110)로부터 세션 정보를 수신하고, 그 정보를 이용하여 세션에 적용되는 정책을 결정하고, 이 정책을 UA(110)로 반환한다.
- [0023] 세션 정책 프레임워크는 UA(110)가 프록시(120)로부터 정책 서버(130)의 URI를 수신하는 메커니즘으로서 (SIP 요청 및 응답에서 프록시(120)에 의해 포함될 수 있는) SIP 정책 접촉 헤더를 정의한다. 즉, 프록시(120)는 정책 접촉 헤더에 정책 서버(130)의 URI를 추가할 수 있다. UA(110)는 URI를 이용하여 정책 서버(130)에 접촉하고 정책 서버(130)에 현재 세션에 대한 (SDP(Session Description)을 포함하는) 정보를 제공한다. 그 다음 UA(110)는 응답으로 정책 서버(130)로부터 세션 정책을 수신한다. UA(110)는 또한 세션 중에 정책 서버(130)로부터 정책 업데이트를 수신할 수 있다. UA(110) 및 정책 서버(130) 간의 통신 교환은 정책 채널(135)로 정의된다.
- [0024] 현재의 세션 정책 프레임워크는 draft-ietf-sipping-policy-package-05에서 정의되는 이벤트 패키지 및 SIP 이벤트 프레임워크 RFC 3265에 기초하여 SIP 기반 메커니즘을 정의하여 정책 채널(135)을 이용하여 세션 정책을 UA(110)에 전달하고, SIP 정책 접촉 헤더 내에 프록시(120)에 의해 포함될 수 있는 URI로서 SIP 및 SIPS URI만을 현재 정의한다. 세션 정책 프레임워크의 전체 세부사항은 draft-sip-session-policy-framework-05에 정의된다.
- [0025] 3GPP는 도 3에 도시된 바와 같이 TS 23.203에서 정책 및 과금 제어(PCC) 아키텍처를 정의하였다. 도면에서, 정책 및 과금 규칙 기능(PCRF)은 정책 서버이다. 두꺼운 점선은 draft-sip-session-policy-framework-05에서 정의된 정책 채널이 동작할 필요가 있는 기준점을 나타낸다. 가입 프로파일 저장소(Subscription Profile Repository; SRP)는 또한 가입 관련 정책을 포함하지만 PCRF에 의해 PCRF 정책에 포함된다. TS 23.203은 또한 로밍 시나리오를 위한 방문한 PCRF로 다른 구성을 지지하지만, 이 경우, 단일 PCRF는 다른 정책 서버와 인터페이스한다. 정책 과금 시행 기능은 IP-CAN(IP-Connectivity Access Network)-특정 게이트웨이(예를 들어, GGSN, PDG, CMTS)에 포함된다. 3GPP IMS에서, P-CSCF는 AF(Application Function) 기능을 구현한다. AF는 Rx 기준점을 통해 PCRF와 통신한다. 3GPP IMS에서, IMS SIP 세션에 대한 베어러 리소스를 허가하기 위하여 P-CSCF는 PCRF와 인터페이스한다. PCRF는 PCEF가 세션 베어러에 적용되는 정책을 결정하는 기준 중의 하나로서 P-CSCF 정보를 이용한다. Gx 기준점은 PCEF 및 PCRF 간의 통신을 위한 프로토콜로서 DIAMETER를 이용한다. 마찬가지로, DIAMETER는 P-CSCF 및 PCRF 간의 Rx 기준점 상에서 사용되는 프로토콜이다.
- [0026] SIP 이벤트 프레임워크 RFC 3265는 기본 정책 및 네트워크 아키텍처에 독립적이고 모든 SIP UA(110)가 모든 정책 서버(130)와 인터페이스할 수 있도록 보장하기 때문에 양호한 일반 솔루션을 제공한다. 그러나, GSM(Global System for Mobile Communications), UMTS(Universal Mobile Telecommunications System), CDMA(Code Division Multiple Access) 및 E-UTRAN(Evolved UMTS Terrestrial Radio Access Network) 등의 제한된 대역폭 네트워크에 대하여, SIP 이벤트 프레임워크 RFC(3265)는 세션 설정시 UA(110)에 세션 정책을 전달하기에 너무 무겁다. SIP 이벤트 프레임워크는 최소로 세션 정책을 얻기 위해 전달될 다음의 SIP 메시지, 즉, SIP SUBSCRIBE 메시지, SIP 200OK 메시지, SIP NOTIFY 메시지 및 또 다른 SIP 200OK 메시지를 필요로 한다.
- [0027] 또한, 이들 메시지, 특히, SUBSCRIBE 메시지 및 NOTIFY 메시지는 IP 및 UDP에 헤더의 오버헤드를 포함하는 큰 텍스트 기반 메시지이다. 그러므로, 메시지는 100 바이트의 크기를 가질 수 있다. NOTIFY 메시지는 XML(Extensible Markup Language)-인코딩 정책 문서를 포함하기 때문에 특히 크다.

- [0028] 따라서, 도 1의 세션 정책 흐름도에 도시된 시나리오에서, 세션을 확립하는데 필요한 9개의 SIP 세션 시그널링 메시지에 더하여 정책 채널 상의 SIP 이벤트를 이용하는 3개의 정책 채널 상호작용을 위해 12개의 SIP 메시지가 필요하다. 따라서, SIP 이벤트 프레임워크를 이용하는 SIP 시그널링 오버헤드는 SIP 세션 확립을 위해 필요한 SIP 시그널링보다 크다. 이것은 시그널링 대역폭을 낭비시킬 뿐 만 아니라 초당 수천 킬로비트의 시그널링 채널로 셀룰러 등의 네트워크의 대역폭을 제한하여, 세션 설정에서 상당한 지연을 초래한다.
- [0029] 또한, SIP 이벤트 프레임워크는 SIP 다이얼로그(dialog)를 확립하는 것을 의미하는 상태 기반이다. 이것은 네트워크 인프라스트럭처 엔티티에 대하여 큰 부하를 부과할 수 있다. 또한, 정책 서버(130)는 전통적으로 SIP를 구현하지 않지만 전송 정책을 위한 AAA (RADIUS 및 DIAMETER) 등의 다른 프로토콜을 사용하였다.
- [0030] 이 시나리오 하에서 전송될 필요가 있는 많은 수의 왕복 SIP 메시지 및 메시지 및 정책 문서의 큰 사이즈는 많은 오버헤드를 소비할 수 있는 수락가능하지 않게 효율적이지 않은 메카니즘을 초래할 수 있다. 이것은 시그널링 대역폭의 낭비를 초래하여 세션 설정에서 상당한 지연을 초래할 수 있다.
- [0031] 일 실시예에서, 3GPP PCC 또는 유사한 AAA 인프라스트럭처가 배치된 SIP 또는 SIPS URI 대신에, 정책 접촉 헤더에 AAA URI 또는 유사한 URI가 제공된다. 즉, SIP 메시지 층보다 낮은 층에 있는 통신 경로가 UA 또는 정책 서버 사이에서 생성되어 정책 채널로서 사용된다. UA는 하위층 프로토콜을 이용하여 이 정책 채널을 통해 세션 정책 요청을 정책 서버로 전송할 수 있다. 어떤 경우, 하위층 프로토콜은 EAP(Extensible Authentication Protocol)를 이용하는 RADIUS 프로토콜 또는 DIAMETER 프로토콜일 수 있다. EAP가 기재되었지만, 당업자는, 제한되지 않지만, PPP(Point to Point Protocol) 등의 다른 프로토콜을 선택할 수 있다. 다른 경우, 하위층 프로토콜은 무선 장치 및 네트워크 간의 데이터 베어러 채널을 생성한다. 예를 들어, 무선 장치는 정보를 포함하는 네트워크에 메시지를 전송하여 데이터 채널을 생성할 수 있다. 이것은 무선 장치로부터 SGSN이라 불리는 네트워크 노드로의 통신인 GPRS(General Packet Radio Service) 활성화 PDP(packet Data Protocol)일 수 있다. LTE 환경에서, ESM 메시지 내의 하위층 프로토콜은, 제한되지 않지만, 무선 장치로부터 MME로의 ATTACH 메시지 내에 또는 별도의 디폴트 메시지로서 터널링 및/또는 피기백될 수 있는 PDN_CONNECTIVITY_REQUEST 또는 BEARER_RESOURCE_MODIFICATION_REQUEST일 수 있다. RFC 3588에 대하여, 다음은 유효한 DIAMETER 또는 RADIUS 호스트 식별자
- [0032] aaa://host.example.com
- [0033] aaa://host.example.com:6666
- [0034] 의 예이다.
- [0035] 대안으로, AAA URI를 사용하는 대신, MPDF URI "mpdf:" 또는 "mpdfeap:" 등의 MPDF에 대하여 새로운 URI 포맷이 정의될 수 있다. 다른 URI 선택스가 또한 가능하다.
- [0036] 도 4는 UE가 EAP(Extensible Authentication Protocol)을 구현하고 EAP를 이용하여 PCRF로 정책 채널 프로토콜을 구현하는 방식으로 세션 정책 요청 및 정책 문서가 전송될 수 있는 시스템을 나타낸다. UA(110)는 게이트웨이, 액세스 포인트, 네트워크 액세스 서버, 프록시 또는 실질적으로 동등한 능력을 갖는 또 다른 컴포넌트일 수 있는 제1 유형의 네트워크 노드에 접속될 수 있다. 이하, 이 컴포넌트는 게이트웨이(120)라 한다. 게이트웨이(120)는 PCEF(Policy Charging Enforcement Function)을 포함할 수 있다. 이하에서, 게이트웨이(120)에 대한 참조는 게이트웨이(120)만을 지칭하거나, PCEF만을 지칭하거나 PCEF와 결합한 게이트웨이(120)를 지칭할 수 있다.
- [0037] UA(110)는 EAP 프로토콜 또는 유사한 하위층 프로토콜을 통해 게이트웨이(120)에 세션 정책 요청을 전송할 수 있다. 게이트웨이(120)는 정책 서버, 정책 및 과금 규칙 기능, 인증 서버 또는 유사한 컴포넌트일 수 있는 제2 유형의 네트워크 노드에 접속될 수 있다. 임의의 실시예에서, 이 컴포넌트는 독립 요소일 수 있다. 다른 실시예에서, 이 컴포넌트는 P-CSCF를 포함하는 SIP 프록시 등의 다른 컴포넌트와 결합될 수 있다. 이하에서, 이 컴포넌트는 정책 서버(130)라 한다. 단 하나의 정책 서버(130)만이 도시되지만, 다수의 정책 서버가 존재할 수 있다. 게이트웨이(120)는 RADIUS 프로토콜, DIAMETER 프로토콜 또는 실질적으로 동등한 능력을 갖는 다른 하위층 프로토콜을 통해 정책 서버(130)에 세션 정책 요청을 전송할 수 있다. 세션 정책 요청을 전송하고 정책 문서를 수신하는 이전에 설명된 기술의 절차의 상태가 도 4에서 점선으로 표시된다.
- [0038] UA(110)를 인증하는 프로세스에서, UA(110) 및 정책 서버(130) 사이에서 게이트웨이(120)를 통해 하위층 통신 경로(160)가 생성된다. 이 경로(160)는 정책 채널로서 사용될 수 있다. EAP 기반 요청이 UA(110)로부터 게이

트웨이(120)로 전송될 수 있는 다양한 기술은 EAP 프레임을 전송할 수 있는 RADIUS 또는 DIAMETER 기반 인프라 스트럭처를 가질 수 있다. 그러므로, EAP 기반 요청은 UA(110)로부터 정책 서버(130)로 게이트웨이(120)를 통해 전송될 수 있고, EAP 기반 응답은 정책(130)로부터 UA(110)로 전송될 수 있다.

[0039] 실시예에서, 정책 채널(160)은, UA(110)로부터 정책 서버(130)로 세션 정책 요청을 전송하고 정책 문서 또는 다른 정책 정보를 정책 서버(130)로부터 UA(110)로 전달하는데 사용될 수 있다. 정책 채널(160)은 draft-ietf-sip-session-policy-framework 드래프트에서 정의된 SUBSCRIBE 및 NOTIFY 메커니즘에 기초하여 정책 채널 메커니즘에 대한 대체물일 수 있다. 특히, 하나 이상의 EAP 프레임은 UA(110) 및 게이트웨이(120) 간의 RFC 5108 당 IP 기반 IKEv2(Internet Key Exchange version 2)를 통해 IP(Internet Protocol)-CAN(Connectivity Access Network)를 통해 전송될 수 있다. 대안으로, RFC 2284, 유선 IEEE 802 LAN (IEEE-802.1X), IEEE 802.11 무선 LAN (IEEE-802.11), UDP(L2TP [RFC2661] 및 IKEv2 [IKEv2]) 및 TCP(PIC)에 따라 PPP(Point-to-Point Protocol) 기반 전송 EAP 등의 다른 전송 프로토콜이 사용될 수 있다. 또한 다른 전송 프로토콜이 가능하다. 이들 전송 프로토콜 중의 임의의 것에서, 메시지가 SIP 메시지보다 더 낮은 프로토콜 층에서 전송되고, 일반적으로 애플리케이션층에서 전송된다.

[0040] 임의의 실시예에서, EAP에서 허용되는 유형-길이-값(type-length-value(TLV)) 구조는 정책 문서를 요청하는 쿼리를 삽입하는데 사용될 수 있다. 다른 실시예에서, 정책 접촉 URI는 사용자를 식별하는데 사용되어 왔던 RFC 4482 당 임의의 NAI에 첨부될 수 있다. 정책 서버 어드레스는 또한 SIP UA 및 EAP 프레임을 처리하는 홈 AAA 서버 사이의 공유키에 의해 암호화될 수 있다. 이것에 의해 정책 어드레스는 임의의 중간 노드에게 비밀로 할 수 있다.

[0041] 실시예에서, 게이트웨이(120)는 DIAMETER를 이용하여 Gx 기준점을 통해 EAP 프레임을 정책 서버(130)로 전달한다. 다른 실시예에서, RADIUS 또는 유사한 프로토콜이 이용될 수 있다. EAP 프레임은 UA(110) 및 게이트웨이(120) 및 정책 서버(130) 간의 세션 정보 문서 등의 정책 채널 문서를 전송할 수 있다. 세션 정보 문서는 InfoOffer, InfoAnswer, 및/또는 draft-ietf-sip-session-policy framework 및 관련 문서 또는 미래의 확장에서 정의된 다른 문서일 수 있다. UA(100)는 정책 서버(130)에 접근하여 정책 접촉 헤더 또는, 제한되지 않지만, 정책 접촉 헤더라 불릴 수 있는 새로운 헤더 내에서 제공되는 정책 접촉 URI(Uniform Resource Indicator)에 기초하여 정책 문서를 얻을 수 있다. 정책 서버(130)는 정책 문서 또는 다른 정책 정보를 UA(110)로 반환할 수 있다. 정책 정보는 요청과 동일한 프로토콜을 이용하여 동일한 경로를 따라, 요청에 사용된 것과 다른 프로토콜을 이용하여 동일한 경로를 따라, 요청에 사용된 것과 다른 상이한 경로를 따라 또는 임의의 다른 방식으로 반환할 수 있다. 세션-특정 정책에 대하여, 세션 정책이 세션동안 변하면(예를 들어, 이용 가능한 라디오 리소스에서의 변화 때문에), 정책 서버(130)는 동일한 DIAMETER 및 EAP 프로토콜을 이용하여 UA(110)에 변경된 정책 문서를 전송할 수 있다.

[0042] 도 5는 IP-CAN 액세스 게이트웨이를 통해 UA 및 DIAMETER 기반 PCRF 사이에서 EAP 및 IP 기반 미디어 정책 문서를 전송하는 제안된 프로토콜 스택의 실시예를 나타낸다.

[0043] 여기에 기재된 실시예가 구현될 때, UA(110)가 정책 문서를 요청하고 수신하는데 필요한 왕복 메시지의 수가 상술한 SIP 시나리오에 사용된 복수의 SIP 메시지에 비교하여 크게 감소할 수 있다. 또한, EAP 기반 세션 정책 요청은 상술한 SIP 메시지의 일부보다 상당히 작을 수 있다. 예를 들어, SIP 메시지의 오버헤드는 500 내지 1000 바이트일 수 있다. 반면, EAP 기반 메시지의 오버헤드는 50 바이트이다.

[0044] 또한, 실시예에서, 정책 문서는 이진수로 변환되어 더 작아질 수 있고, SIP 기반 방법으로 전송되는 큰 XML 기반 정책 문서 보다는 오히려, 더 작아진 정책 문서가 UA(110)로 전송될 수 있다. 세션 정책 문서의 XML 내용은 본 기술에서 공지된 다수의 방법에 의해 이진수 형태로 압축될 수 있다. ITU-T Rec. X.891에 명시된 바와 같이 XML 정보세트(Infoset)가 일 예일 수 있다.

[0045] 3GPP는 미디어에 대한 허가 요청이 SIP 시그널링과 링크되지 않는 목적을 갖는다. 여기에 기재된 세션 정책 요청은 미디어를 얻기 위한 허가를 요청하는 EAP 기반 메시지를 사용하고 따라서 미디어에 대한 허가 정책으로부터 SIP 시그널링의 분리를 달성할 수 있다.

[0046] 또한, EAP 기반 세션 정책 요청은 액세스 네트워크 불가지론자(agnostic)이다. 즉, UA(110)는 (GSM, EDGE, UTRAN, 및/또는 E-UTRAN를 포함하는) GPRS, 3GPP UTRAN, 3GPP2 CDMA, 802.11x WLAN, 802.16 WiMAX, 802.20 WLAN, DOCSIS (Data Over Cable Service Interface Specification), 및/또는 TISPAN(Telecoms and Internet converged Services and Protocols for Advanced Networks) NASS/RACS(Network Attachment Sub-

System/Resource and Admission Control System) 등의 몇 개의 상이한 무선 또는 유선 통신 기술을 통해 게이트웨이(120)에 접속할 수 있다. 이들 아키텍처는 DIAMETER 기반 또는 RADIUS 기반 정책 서버에 의존하므로, UA(110)는 여기에 기재된 바와 같이 이들 액세스 네트워크 중에서 무엇이 UA(110)를 게이트웨이(120)와 접속하는데 사용되는 지에 관계없이 게이트웨이(120)에 EAP 기반 세션 정책 요청을 제출할 수 있다.

[0047] 도 6은 (도 6 내지 12에서는 UE라 하는) UA(110)가 GPRS(GSM/EDGE/UTRAN/E-UTRAN) IP-CAN을 이용할 때 세션 정책 요청이 처리될 수 있는 방법을 나타낸다. IMS로의 3GPP 셀룰러 액세스(GSM/EDGE/UTRAN/E-UTRAN)은 GPRS를 이용한다. GPRS에 대하여, IP-CAN 베어러는 PDP에 콘텍스트이다. GPRS에서, 게이트웨이는 GGSN이고 PCEF는 GGSN과 동일 위치에 위치한다. PCEF 및 PCRF 간의 Gx 기준점 및 P-CSCF 및 PCRF 간의 Rx 기준점은 DIAMETER를 사용한다.

[0048] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 또는 PPP 기반 IKEv2를 통해 GGSN로 전송될 수 있다. 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 EAP 프레임은 Gx 기준점을 이용하여 DIAMETER를 통해 PCRF로 라우팅될 수 있다. PCRF는 UE로부터의 InforOffer 또는 InfoAnswer 메시지에 포함된 정책 정보, PCRF에 설치된 정책, SPR로부터 페치된 가입 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및 UE가 이용하는 액세스 네트워크의 지식 및 그 이용 가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF는 Gx 기반 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 GGSN로 전송하고 그 후 IP 또는 PPP 기반 IKEv2를 통해 UE로 전송되는 EAP 내에서 UE로 전달된다. 또한 다른 시나리오가 가능하다.

[0049] 도 7은 UE가 강화된 패킷 코어(EPC) IP-CAN으로 3GPP E-UTRAN 또는 다른 3GPP 액세스를 이용할 때 세션 정책 요청이 처리될 수 있는 방법의 일예를 나타낸다. 3GPP E-UTRAN 및 다른 3GPP 액세스는 IMS로 액세스하기 위한 EPC를 사용할 수 있다. EPC에 대하여, IP-CAN 베어러는 GPRS 또는 PMIP (Proxy Mobile IP)로부터 강화된 PDP 콘텍스트이다. EPC에서, 게이트웨이는 PDN GW이고 PCEF는 PDN GW와 동일 위치에 위치한다. PCEF 및 PCRF 간의 Gx 기준점 및 P-CSCF 및 PCRF 간의 Rx 기준점은 DIAMETER를 이용한다.

[0050] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 기반 IKEv2를 통해 PDN GW로 전송될 수 있다. 대안으로, 채널 InfoOffer는 PDN CONNECTIVITY REQUEST 등의 ESM 메시지내에 터널링, 피기백 또는 전송될 수 있고, ESM 메시지가 무선 장치로부터의 ATTACH 메시지에 포함되지 않는 경우, InforOffer는 MME를 통해 PDN GW로 전송될 수 있다. 정책 채널 InforOffer 및 InfoAnswer는 메시지를 포함하는 EAP 프레임 또는 MME로부터 예를 들어 정보 대답 메시지를 포함하는 생성 세션 응답 및 정보 제안을 포함하는 생성 세션 요청을 포함하는 EPC 베어러 채널을 생성하는 PDN으로의 메시지는 Gx 기준점을 이용하여 PCRF로 DIAMETER를 통해 라우팅될 수 있다. PCRF는 UE로부터의 InfoOffer 또는 InfoAnswer 메시지 내에 포함된 정책 정보, PCRF에 설치된 정책, SPR로부터 페치된 가입자 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및/또는 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용 가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF는 Gx 기반 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 PDN GW로 전송하고 IP 기반 IKEv2를 통해 UE로 전송되는 EAP 내에서 또는 PolicyAnswer를 포함하는 생성 세션 응답을 통해 UE로 전달된다.

[0051] 도 8은 UE가 3GPP2 CDMA IP-CAN을 이용할 때 세션 정책 요청이 처리될 수 있는 방법의 일예를 나타낸다. IMS로의 3GPP2 셀룰러 액세스(CDMA-1X, CDMA EVDO)는 이동 IP를 이용한다. 3GPP3 CDMA에서, 게이트웨이는 PDSN이고, PCEF는 PDSN과 동일 위치에 위치한다. PCEF 및 PCRF 간의 Gx 기준점 및 P-CSCF 및 PCRF 간의 Rx 기준점은 DIAMETER를 이용한다.

[0052] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 기반 IKEv2를 통해 PDSN으로 전송될 수 있다. 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 EAP 프레임은 Gx 기준점을 이용하여 PCRF로 DIAMETER를 통해 라우팅될 수 있다. PCRF는 UE로부터의 InforOffer 또는 InfoAnswer 메시지 내에 포함된 정책 정보, PCRF에 설치된 정책, (홈 네트워크에서 SPR 또는 홈 PCRF 또는 다른 정책 서버 등으로부터) 홈 네트워크로부터 페치된 가입자 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및/또는 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용 가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF는 Gx를 통해 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 PDSN으로 전송하고 IP 기반 IKEv2를 통해 UE로 전송되는 EAP 내에서 UE로 전달된다.

[0053] 도 9은 UE가 802.11x WLAN IP-CAN을 이용할 때 세션 정책 요청이 처리될 수 있는 방법의 일예를 나타낸다. IMS

로의 802.11x WLAN 액세스에서, 게이트웨이는 PDG이고, PCEF는 PDG과 동일 위치에 위치한다. PCEF 및 PCRF 간의 Gx 기준점 및 P-CSCF 및 PCRF 간의 Rx 기준점은 DIAMETER를 이용한다.

[0054] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 또는 802.1X 기반 IKEv2를 통해 PDG로 전송될 수 있다. 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 EAP 프레임은 Gx 기준점을 이용하여 PCRF로 DIAMETER를 통해 라우팅될 수 있다. PCRF는 UE로부터의 InforOffer 또는 InfoAnswer 메시지 내에 포함된 정책 정보, PCRF에 설치된 정책, SPR로부터 폐치된 가입자 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF는 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 Gx를 통해 PDG로 전송하고 IP 기반 IKEv2를 통해 UE로 전송되는 EAP 내에서 UE로 전달된다.

[0055] 도 10은 UE가 WiMAX/802.16 IP-CAN을 이용할 때 세션 정책 요청이 처리될 수 있는 방법의 일예를 나타낸다. WiMAX IP-CAN에서, (IEEE 802.16 표준에서 이동국 또는 MS라 한다)는 WiMAX ASN(Access Service Network)에 접속된다. ASN은 코어 네트워크 기능(예를 들어, 이동 IP HA, AAA 서버, DHCP, DNS 등)의 집합인 CSN(Connectivity Service Network)와 논리적으로 통신한다. ASN은 권한 부여된 UE에 대하여 트래픽 승인 및 스케줄링을 관리하고 QoS를 시행하고, UE에 대한 (세션, 플로우 또는 UE 당) 회계 기능을 수행한다. WiMAX PCEF는 WiMAX IP-CAN의 일부이며 WiMAX 포럼에 의해 정의된다. WiMAX PCEF는 PCRF로부터의 Gx 기준점을 종료하고 분산된 시행 아키텍처일 수 있다.

[0056] WiMAX IP-CAN으로의 PCC 기능 맵핑은 도 8에 도시되며, PCC Gx 및 Rx가 적용된다. Gx 및 Rx는 DIAMETER를 이용한다.

[0057] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 또는 802.1X 기반 IKEv2를 통해 또는 PCEF로 전송될 수 있다. 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 EAP 프레임은 Gx 기준점을 이용하여 PCRF로 DIAMETER를 통해 라우팅될 수 있다. PCRF는 UE로부터의 InforOffer 또는 InfoAnswer 메시지 내에 포함된 정책 정보, PCRF에 설치된 정책, SPR로부터 폐치된 가입자 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF는 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 Gx를 통해 WiMAX PCEF로 전송하고 IP 기반 IKEv2를 통해 UE로 전송되는 EAP 내에서 UE로 전달된다.

[0058] 도 11은 UE가 DOCSIS IP-CAN을 이용할 때 세션 정책 요청이 처리되는 방법의 일예를 나타낸다. DOCSIS IP-CAN에서, 각각의 UE는 HFC(Hybrid Fiber Coax) 액세스 네트워크를 통해 CMTS(Cable Modem Termination System)에 연결된 CM(Cable Modem)을 통해 네트워크에 연결된다. UE 및 CM은 동일한 물리적 패키지에 포함되거나 포함되지 않을 수 있지만, 이들은 개별 논리적 장치이다. 하나 이상의 UE는 단일 CM을 대할 수 있다(subtend). CMTS는 IP 접속성 및 트래픽 스케줄링을 제공하고 CM 및 그에 대한 UE에 대한 QoS를 관리하기 때문에, CMTS는 DOCSIS IP-CAN에 대하여 PCEF의 역할을 수행한다. DOCSIS IP-CAN에서, AM(Application Manager) 및 PC(Policy Server)는 PCRF의 역할을 수행한다.

[0059] DOCSIS IP-CAN을 통해 리소스를 액세스하면, Rx 인터페이스는 리소스를 요청하는데 사용될 수 있다. Rx 인터페이스는 DIAMETER를 이용한다. AM 및 PS 간 PS 및 CMTS 간의 통신은, COPS에 기초하고 J.179에 정의된 PKT-MM-2 인터페이스를 사용한다. COPS는 IP를 통해 관리하고 IKE 또는 키 관리를 위한 커버러스(Kerberos)를 이용하여 IPsec ESP를 이용한다.

[0060] PKT-MM-2 인터페이스는 Gx 인터페이스의 기능을 수행하지만 DIAMETER가 아닌 COPS를 이용한다. DOCSIS 시스템은 전체 3GPP PCC 구현을 나타내지 않고 그와 인터페이스할 수 있다.

[0061] DOCSIS는 UE 및 AM 간의 mm-7 인터페이스를 정의하여 UE가 AM과 인터페이스하도록 하고 QoS 리소스를 직접 요청하고 관리한다. 이 인터페이스는 패킷 케이블에 의해 아직 표준화되지 않았다.

[0062] EAP 프레임은 mm-7을 통해 점재적으로 전송되어 AM에 도달하고 AM을 통해 PS에 도달할 수 있다. 대안으로, DOCSIS는 또 다른 802.1X 구현예이므로, EAP 프레임은 802.1x에서처럼 전송되어 CMTS에 도달할 수 있고, PKT-MM-2 인터페이스 상의 COPS 프로토콜은 RADIUS 속성으로서 EAP 프레임을 중개하는데 사용될 수 있다.

[0063] 이 액세스 네트워크 시나리오에서, 정책 채널 InforOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 기반 IKEv2를 통해 PCRF/AM으로 mm-7을 이용하여 전송될 수 있다. PCRF(AM 및 PS)는 UE로부터의

InforOffer 또는 InfoAnswer 메시지 내에 포함된 정책 정보, PS에 설치된 정책, Rx를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. PCRF/AM은 IP 기반 IKEv2를 통해 UE로 전송되는 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서를 mm-7 또는 COPS 및 802.1x를 통해 전송한다.

[0064] 도 12는 UE가 TISpan NASS/RACS를 이용할 때 세션 정책 요청이 처리되는 방법의 일예를 나타낸다. TISpan NGN은 3GPP PCC를 이용하지 않는다. TISpan NGN에서, NASS(Network Attachment Sub-System) 및 RACS(Resource and Admission Control System)가 존재한다. RACS는 액세스 및 집합(aggregation) 네트워크에서 리소스 예약 및 승인 제어를 포함하는 정책 제어 요소이다. RACS는 애플리케이션에 정책 기반 전송 제어 서비스를 제공한다. 이들 서비스는 애플리케이션이 RACS의 범위 내에서 전송 네트워크로부터 전송 리소스를 요청하고 예약할 수 있게 한다. RACS는 SPDF 및 A-RACF로 구성된다.

[0065] SPDF는 P-CSCF로부터 수신한 리소스 예약 요청을 조정하는 기능 요소이다. SPDF가 수행하는 기능 중의 하나는, P-CSCF로부터 수신된 요청 정보가 SPDF에서 정의된 정책 규칙과 일치하는지를 판정하는 것이다. SPDF는 또한 SIP 세션에 대한 요청된 리소스를 허가한다. 그러기 위해, SPDF는 P-CSCF로부터 수신된 요청 정보를 이용하여 적절한 허가를 산출(즉, 소정의 미디어 컴포넌트를 허가)한다. 또한, SPDF는 요구된 전송 능력에 따라 A-RACF의 위치를 제공하고, A-RACF의 리소스를 요청하고, RACS의 세부사항 및 코어 전송층을 제어 아키텍처로부터 숨기고, 적절한 A-RACF를 향해 애플리케이션 기능으로부터의 요청을 맵핑함으로써 리소스 중재를 제공한다.

[0066] A-RACF는 승인 제어 및 네트워크 정책 어셈블리를 제공하는 기능 요소이다. 승인 제어를 위하여, A-RACF는 SPDF로부터 QoS 리소스에 대한 요청을 수신하고 수신된 QoS 정보를 이용하여 승인 제어를 수행한다. 그 후, 리소스에 대한 요청이 승인되었는지를 SPDF에 지시한다.

[0067] 액세스 네트워크 정책은 액세스 라인에 적용되어야 하는 정책을 특정하는 규칙 세트이다. 네트워크 정책 어셈블리를 위하여, 다수의 SPDF가 A-RACF에게 리소스를 요청할 수 있기 때문에, A-RACF는 SPDF로부터의 요청이 액세스 정책에 매칭하는지를 확인한다. A-RACF는 리소스를 요청한 SPDF로부터의 요청을 결합하여 모든 요청이 액세스 라인의 능력에 매칭되는지를 확인한다.

[0068] SPDF는 Rq 인터페이스를 통해 액세스 네트워크에서 리소스에 대한 요청을 발행한다. 이들 요청은 IP QoS 특성을 나타낸다. A-RACH는 IP QoS 정보를 이용하여 승인 제어를 수행하고 승인 제어 결정을 Rq 인터페이스를 통해 SPDF에 알려준다. RF 인터페이스는 DIAMETER를 이용한다. RACS는 3GPP PCC PCRF와 유사한 정책 제어 기능을 수행한다. P-CSCF는 Gq'를 이용하여 RACS와 통신하고 Gq'는 DIAMETER를 이용한다. Gq'는 3GPP PCC에서 Rx에 유사한 기능을 제공한다.

[0069] 3GPP PCC의 게이트웨이와 동등한 IP 에지 라우터는 3GPP PCC에서 PCEF에 동등한 기능을 수행하는 ACEF(Access Control Enforcement Function)을 포함한다. RACS 및 ACEF 간의 Re 인터페이스는 아직 표준화되지 않았다. IP 에지 라우터는 또한 NASS(기술적으로 AMF는 NASS의 일부이다)에 인터페이스하는 RADIUS 클라이언트인 AMF(Access Management Function)을 포함한다. AMF는 UE에 의해 전송된 네트워크 액세스 요청을 변환하고, IP 어드레스 및 네트워크의 할당을 위한 요청을 전달하고, 사용자 허가 요청을 UAAF(User Access Authorization Function)로 전달한다. 역방향으로, AMF는 NASS 내의 UAAF로부터의 응답을 UE로 전달한다.

[0070] NASS는 액세스 레벨에서의 등록 및 TISpan NGN 서비스로의 액세스에 대한 사용자 기기의 초기화를 제공한다. NASS는 네트워크 레벨 식별 및 인증을 제공하고, 액세스 네트워크의 IP 어드레스 공간을 관리하고 액세스 세션을 인증한다. NASS는 또한 TISpan NGN 서비스/애플리케이션 서브시스템의 접촉점을 사용자 장치에 발표한다. NASS를 통한 네트워크 부착은 암시적 또는 명시적 사용자 식별자 및 NASS에 저장된 인증 자격에 기초한다. NASS 내에는, 여기에 관련되지 않은 다른 기능과 함께 UAAF 및 CLF(Connectivity Session Location and Repository Function)가 있다. UAAF는 사용자 인증 및 허가 체크를 수행한다. UAAF는 사용자 인증 및 액세스 허가 정보를 PDBF(Profile Database Function)에 포함된 사용자 프로파일로부터 검색한다. UAAF는 또한 청구를 위한 회계 데이터를 수집한다. CLF는 UE에 할당된 IP 어드레스, 관련 네트워크 위치 정보 및 NACF에 의해 제공되는 지리적 위치 정보를 등록하고 모든 정보를 연관시킨다. CLF는 사용자의 식별자, 사용자 네트워크의 QoS 프로파일 및 위치 정보의 사용자 프라이버시 설정을 저장한다. CLF는 상위 서비스에 대한 위치 쿼리 기능을 제공한다. CLF는 RACS 내의 A-RACF와 e4 인터페이스를 통해 통신한다. e4 인터페이스는 DIAMETER를 이용한다. 인터페이스(a3)는 AMF 및 UAAF 사이에서 사용된다. 이 인터페이스는 AMF가 사용자를 인증하고 네트워크 가입 정보를 인증할 것을 UAAF에 요청할 수 있게 한다. 인터페이스(a4)는 UAAF 및 CLF 사이에서 사용된다. 이 인터페이스는 UAAF가 푸시(Push) 모드에서 사용자 네트워크 프로파일 정보 (예를 들어, QoS 프로파일) 뿐 만 아

나라 사용자 식별자 및 위치 정보의 사용자 프라이버시 설정 간의 연관성을 등록하도록 CLF에 요청할 수 있게 한다. 인터페이스(a4)는 CLF가 풀(Pull) 모드에서 UAAF로부터 사용자 네트워크 프로파일을 쿼리하도록 할 수 있다. 인터페이스(a3 및 a4)는 현재 표준화되어 있지 않다.

[0071] 이 액세스 네트워크 시나리오에서, 정책 채널 InfoOffer 및 InfoAnswer 메시지를 포함하는 UE로부터의 EAP 프레임은 IP 기반 IKEv2를 통해 IP 에지 라우터로 전송된다. 정책 채널 정보 제안 및 정보 대InfoOffer 및 InfoAnswer답 메시지를 포함하는 EAP 프레임은 a3 인터페이스를 이용하여 RADIUS를 통해 NASS(UAAF)로 라우팅된다. NASS(UAAF)는 RADIUS(a4) 및 DIAMETER(e4)를 이용하여 RACS(A-RACF)로 전달된다. RACS(A-RACF 및 SPDF)는 UE로부터의 InfoOffer 또는 InfoAnswer 메시지에 포함된 정책 정보, SPDF에 설치된 정책, Gq'를 통해 P-CSCF에 의해 설치된 서비스 기반 허가 정책 및 UE가 사용하고 있는 액세스 네트워크의 지식 및 그 이용가능한 리소스에 기초하여 미디어 정책 문서를 생성한다. RACS(A-RACF)는 e4를 통해 EAP 프레임 내의 PolicyOffer 또는 PolicyAnswer 메시지 내의 미디어 정책 문서 NASS로 전송하고, a4 및 a3를 통해 RADIUS를 이용하여 IP 에지 라우터로 전달하고, IP 기기 기반 Ev2를 통해 UE로 전송된 EAP 내에서 UE로 전달된다.

[0072] 도 13은 세션 정책 요청을 네트워크 컴포넌트로 전송하는 방법(400)의 실시예를 나타낸다. 블록(410)에서, UA는 EAP 프로토콜 또는, 제한되지 않지만, 활성화 PDP 콘텍스트 등의 유사한 프로토콜을 이용하여 네트워크 컴포넌트로 세션 정책 요청을 전송한다. 네트워크 컴포넌트는 정책 서버, 인증 서버, 정책 제어 및 과금 규칙 기능, SPR(subscription profile repository), 정책 제어 및 강화 기능, 네트워크 액세스 서버, 게이트웨이, 라우터, CSCF(예를 들어, P-CSCF 또는 S-CSCF) 등의 SIP 프록시 또는 유사한 컴포넌트일 수 있다. 어떤 경우, 세션 정책 요청은 이들 컴포넌트 중의 다른 것이 종료하기 전에 이들 컴포넌트 중의 하나 이상을 통과할 수 있다.

[0073] 어떤 경우, 하나 이상의 URI 방식이 기존 정책 접촉 헤더로 사용되어 draft-ietf-sip-session-policy-framework-05에 정의된 SIP 및 SIPS URI 방식만을 이해하는 기존의 SIP 사용자 에이전트와 역호환을 보장할 수 있다. 실시예에서, SIP 또는 SIPS URI에 더하여 정책 서버의 새로운, 대체, 년-SIP URI(예를 들어, AAA URI)를 추가함으로써 정책 접촉 헤더에 새로운 URI 방식이 포함된다. 예를 들어, 대체 URI는

[0074] Policy-contact: sip:host.example.com,

[0075] aaa://pcrf.example.com;alt-uri=host.example.com

[0076] 상술한 예는 2개의 PolicyContactURI가 정책 문서를 얻기 위하여 정책 채널 상의 상이한 프로토콜을 이용하는 동일한 정책 서버의 대체 URI이라는 실시예를 나타낸다. 이것은 접촉될 필요가 있는 2개의 상이한 정책 서버에 대하여 URI가 명시된 draft-ietf-sip-session-policy-framework-05의 기술의 현재 상태와 상반된다.

[0077] (alt-uri 파라미터로서 도시된) 파라미터는 동일한 정책 서버의 SIP URI에 포함된 호스트이름을 포함함으로써 다른 PolicyContactURI(sip:host.example.com) 내의 동일한 정책 서버의 대체 URI라는 것을 나타낸다. draft-ietf-sip-session-policy-framework-05에서 지시된 것으로서 기존 SIP UA가 이해할 수 없는 PolicyContactURI URI 방식을 무시한다고 가정하면, 세션 정책을 지원하는 모든 UA는 정책 문서를 얻기 위한 SIP 및 SIPS 방식을 지원할 필요가 있다. SIP 및 SIPS URI 방식을 지원하는 UA는 다른 URI 방식을 이용하는 PolicyContactURI를 무시한다. 새로운 URI 방식 및 alt-uri 태그를 이해하고 지원하는 SIP UA는 aaa://pcrf.example.com이 sip:host.example.com에서 동일한 정책 서버의 대체 URI 또는 어드레스라는 것을 이해할 것이다.

[0078] 당업자는 파라미터 "alt-uri"는 하나의 policycontactURI가 또 다른 policycontactURI의 대안의 URI이고 파라미터의 이름이 상이한 실시예에서 다를 수 있다는 것을 나타내는데 사용된다는 것을 인식해야 한다. 다른 가능한 실시예는 파라미터의 값으로서 호스트 이름을 포함하지 않을 수 있다. 이들은 SIP URI 또는 policycontactURI의 인덱스를 포함하는 임의의 다른 지시를 포함할 수 있다. 예를 들어, "1"은 제1 policycontactURI를 나타내거나 파라미터 "prev"는 이전의 policycontactURI를 나타낼 수 있다.

[0079] 또 다른 가능한 실시예에서, 파라미터는 다수의 policycontactURI가 동일한 정책 서버를 위한 것이라는 것을 나타내는 레이블(label)을 포함할 수 있다. 예를 들어, 다음과 같다.

Policy-Contact: sip::host1.example1.com; label="A",
 aaa://pcrf1.example1.com; label="A",
 sip::host2.example2.com; label="B",
 aaa://pcrf2.example2.com; label="B"

[0080]

[0081] 또 다른 가능한 실시예에서, SIP UA는 호스트 이름의 도메인 이름 부분 또는 URI의 FQDN(fully qualified domain name)을 단순히 비교하여, 그들이 동일하면, UA는 그들이 동일한 정책 서버에 대한 상이한 policycontactURI라고 상정한다. 동일한 정책 서버에 대한 대안의 policycontactURI가 존재하면, SIP UA는 정책 서버에 접촉하는 어떤 policycontactURI가 이용될지를 결정할 수 있다.

[0082] 도 14는 UA가 네트워크에서 세션 정책을 액세스하는 방법(500)의 실시예를 나타낸다. 블록(510)에서, UA는 응답 메시지의 헤더 필드에서 정책 서버에 대한 다수의 URI를 수신한다.

[0083] DIAMETER 또는 RADIUS에 기초하여, 3GPP PCC 아키텍처는 정책 서버 간의 도메인간 통신을 지원한다. IMS 세션에서, 4개의 도메인(발신 방문(Originating Visited), 발신 홈(Originating Home), 종료 홈(Terminating Home), 종료 방문(Terminating Visited)이 세션 설정에 포함될 수 있다 (수송 네트워크가 포함된다면, 더 많이). 이들 도메인의 각각은 잠재적으로 세션에 적용되는 정책(미디어 유형, 코덱 등)을 가질 수 있다.

[0084] 또한, 3GPP에 의해 정의된 현재의 세션 정책 메카니즘으로, 각 도메인의 각 프록시는 SIP 488 응답으로 SIP INVITE 요청을 거절하여 SIP INVITE 요청이 호출된 UA에 도달하기 전에 호출하는 UA가 5개의 SIP INVITE 요청을 보내야 한다 (4개의 SIP 488 응답을 수신). 또한, SIP 서버는 복수의 정책 서버 중의 각각에 접촉하여 정책 정보를 얻을 필요가 있다. 이것은 호 설정을 지연시킬 수 있고 UA 배터리를 소모시킬 수 있다.

[0085] IETF 세션 정책 프레임워크는 SIP 프록시에 대한 메카니즘을 제공하여 발신 또는 종료 UA에 세션에 적용되는 세션 정책을 알린다. 이것은 정책 서버의 URI를 정책 접촉 헤더에 추가하는 프록시에 의해 수행된다.

[0086] DIAMETER 및 RADIUS는 하나의 도메인 내의 정책 서버가 (서비스 제공자 사이에 합의가 이루어진) 다른 도메인 내의 정책 서버와 통신하도록 한다. 일 실시예에서, 이 능력은 다른 정책 서버와 접촉하는 제1 정책 서버로 또는 계층 트리에서 다수의 정책 서버가 UA로부터의 단일 요청을 통해 접촉하도록 하는데 사용된다. 예를 들어, UA는 정책 서버(A)와 접촉하고, 정책 서버(A)는 정책 서버(B) 및 정책 서버(C)와 접촉하고, 정책 서버(B)는 정책 서버(D) 및 정책 서버(E)와 접촉한다. 반환된 정책 문서는 단일 정책 문서로 결합되어 UA로 반환된다. 이것을 달성하기 위하여, SIP 프록시는 UA에게 정책 접촉 헤더 내에 URI가 이미 열거된 다른 정책 서버가 그 도메인에서 정책 서버를 통해 접촉될 수 있다는 것을 지시한다.

[0087] draft-ietf-sip-session-policy-framework-05는 다음과 같이 정책 접촉 헤더 필드의 선택스를 정의한다

```
Policy-Contact = "Policy-Contact" HCOLON policyContactURI
                  *(COMMA policyContactURI)
policyContactURI = ( SIP-URI / SIPS-URI / absoluteURI )
                  [ SEMI "non-cacheable" ] *( SEMI generic-param )
```

[0088]

[0089] 정책 접촉 URI는 추가의 파라미터(RFC 3261에서 정의된 일반 파라미터)를 허용한다. RFC 3261로부터

```
generic-param = token [ EQUAL gen-value ]
gen-value     = token / host / quoted-string
host          = hostname / IPv4address / IPv6reference
hostname      = *( domainlabel "." ) toplabel [ "." ]
domainlabel   = alphanum
               / alphanum *( alphanum / "-" ) alphanum
toplabel      = ALPHA / ALPHA *( alphanum / "-" ) alphanum
```

[0090]

[0091] 따라서, 상기 배커스 나우어 형식(Backus-Naur Form)을 이용하여, 다음의 정책 접촉 헤더가 구성될 수 있다.

```
Policy-Contact: <aaa://host1.example1.com:1813>,  
<aaa://host2.example2.com:3868>; proxy-to= host1.example1.com,  
<aaa://host3.example3.com:1727>;>;  
proxy-to= host1.example1.com; proxy-to= host2.example2.com
```

[0092]

[0093] 상술한 예에서, 도메인 example1.com에 대한 SIP 프록시는 그 정책 서버 URI "aaa://host1.example1.com:1813"을 포함한다. 도메인 example2.com에 대한 SIP 프록시는 그 정책 서버 URI "aaa://host2.example2.com:3868"을 추가하고, example1.com에 대한 정책 서버가 그 정책 서버를 통해 도달될 수 있다는 것을 결정하고, example1.com(host1.example1.com)에 대한 정책 서버의 호스트 이름과 동일하게 설정된 파라미터 "proxy-to"를 추가한다. 마찬가지로, 도메인 example3.com에 대한 SIP 프록시는 그 정책 서버 URI "aaa://host3.example3.com:1727"을 추가하고, example1.com에 대한 정책 서버 및 example2.com에 대한 정책 서버가 그 정책 서버를 통해 도달될 수 있다는 것을 결정하고, example1.com에 대한 정책 서버의 호스트 이름과 동일하게 설정된 파라미터 "proxy-to" 및 example2.com에 대한 정책 서버의 호스트 이름과 동일하게 설정된 파라미터 제2 "proxy-to"를 추가한다.

[0094] UA가 상기 정책 접촉 헤더를 포함하는 SIP 488 응답 또는 SIP INVITE 요청을 수신하면, URI의 리스트를 스캔한다. 리스트 내의 URI가 정책 접촉 헤더 내의 다른 URI에서 나타나는 하나 이상의 호스트 이름 또는 도메인 이름을 포함하는 하나 이상의 "proxy-to" 파라미터와 관련되면, UA는 EAP InfoOffer 또는 InfoAnswer 메시지를 포맷할 때 정책 접촉 헤더 내에 열거된 URI와 관련된 "proxy-to" 파라미터에 호스트 이름 또는 도메인 이름이 나타난 정책 접촉 헤더로부터 정책 서버의 AAA URI를 포함하는 Also-Contact 파라미터 등의 파라미터를 포함할 수 있다. EAP InfoOffer 또는 InfoAnswer 메시지는 또한 draft-ietf-sipping-media policy-dataset-06에서 정의된 의도된 제안 또는 대답을 포함한다.

[0095] 제1 정책 서버가 Also-Contact 파라미터를 포함하는 InfoOffer 또는 InfoAnswer 메시지를 포함하는 정책 채널 메시지를 수신하면, Also-Contact 파라미터에서 식별된 정책 서버로 DIAMETER 요청을 어드레싱하고 임의의 "proxy-to" 파라미터로부터의 URI를 요청 내의 Also-Contact 파라미터에 포함시킨다.

[0096] 제1 정책 서버가 다른 정책 서버로부터 정책 문서를 수신하면, 수신된 모든 정책 문서를 자신의 정책 문서와 함께 단일 정책 문서로 만들고 그 단일 정책 문서를 PolicyOffer 또는 PolicyAnswer 메시지로 요청자에게 반환한다. 제1 정책 서버는 또한 PolicyOffer 또는 PolicyAnswer 메시지 내의 Policy-Contributor 파라미터 내의 포함된 정책 문서에 기여하는 모든 정책 서버의 모든 AAA URI를 포함한다.

[0097] UR가 PolicyOffer 또는 PolicyAnswer 메시지를 수신하면, Policy-Contributor 파라미터를 체크하고 정책 문서가 EAP InfoOffer 또는 InfoAnswer 메시지 내에 표시된 모든 정책 서버로부터의 정책을 나타낸다는 것을 보증한다. 따라서, draft-ietf-sip-session-policy에 따르면, "발견된 정책 서버 중의 하나로 정책 채널을 설정하는 것이 실패하면, UA는 이 정책 서버에 접촉하지 않고 세션의 개시를 계속할 수 있다.". 그러나, 정책 서버가 접촉되지 않으면, UA는 SIP 요청 또는 응답 내의 Policy-ID 헤더에 정책 서버의 URI를 포함하지 않는다. UA는 정책 서버가 정책 문서에 기여했다는 확인을 수신한 정책 서버만을 포함한다.

[0098] 대안으로, UA는 상술한 통합된 접근법을 이용하는 대신에 EAP/AAA 인프라스트럭처를 이용하여 개별적으로 병렬로 모든 정책 서버와 접촉할 수 있다.

[0099] 다른 실시예에서, P-CSCF 또는 다른 SIP 프록시(예를 들어, S-CSCF, 등)는 Also-Contact 파라미터를 이용하여 다른 정책 서버 업스트림의 정책 접촉 URI를 그들의 정책 서버에 알림으로써 정책 서버가 다른 정책을 얻도록 하거나 P-CSCF 또는 다른 SIP 프록시(예를 들어, S-CSCF, 등)가 (예를 들어, SIP 기반 정책 채널 또는 DIAMETER 또는 RADIUS, 등을 이용하여) 다른 정책 서버로부터 정책 문서를 얻어 그 정책 서버를 그들의 정책 서버에 제공하도록 할 수 있다. 정책 서버는 다른 정책 서버의 정책의 모음(aggregation)에 기초하여 모은 정책 문서를 생성하고 정책 채널을 통해 정책 문서를 요청하면 모은 정책 문서를 UA에 제공한다. 정책 서버는 또한 PolicyOffer 또는 PolicyAnswer 메시지 내의 Policy-Contributoer 파라미터 내의 포함된 정책 문서에 기여한 모든 정책 서버의 모든 AAA URI를 포함할 수 있다.

[0100] 간략화를 위해 위에서는 AAA URI가 사용되었지만, URI 방식의 실제 신택스는 UA 또는 SIP 프록시(P-CSCF, S-CSCF, 등)가 EAP/DIAMETER/RADIUS 인프라스트럭처를 통해 정책 서버에 접촉하도록 하는 임의의 URI 방식이 충분

함에 따라 상술한 실시예와 관련되지 않는다.

- [0101] 도 15는 DIAMETER를 이용하여 상이한 도메인 내의 다수의 PCRF가 상호 접속하는 방법 (유사한 접속이 RADIUS를 이용하여 제공될 수 있다) 및 상이한 도메인 내의 다수의 SIP 프록시(P-CSCF 및 S-CSCF)가 그들의 반환된 정책으로의 세션 기반 입력을 PCRF에 제공하는 방법을 나타낸다. 예를 들어, 사용자의 홈 네트워크 내의 S-CSCF는 SIP 요청에 포함된 IMS 통신 서비스 식별자에 기초하여 정책에 영향을 줄 수 있다.
- [0102] 이 기술을 이용하여, 제1 정책 서버에 단일 세션 정책 요청이 이루어질 수 있고, 그 정책 서버는 다른 정책 서버에 세션 정책 요청을 중개할 수 있다. 제1 정책 서버는 다른 정책 서버로부터 정책 문서를 모아 단일 정책 문서를 UA로 전달할 수 있다. 구체적으로, 일 실시예에서, DIAMETER 및 RADIUS 프로토콜은 (정책 서버 등의) AAA 서버가 도메인을 넘어 서로 인터페이스하도록 하므로, 단일 정책 서버가 SIP 세션이 단일 정책 채널 교환에서 가로지르는 다수의 정책 서버로부터의 정책들의 복합 정책을 제공할 수 있다. 정책 채널 메커니즘이 기존의 3GPP PCC 메커니즘 또는 DIAMETER 또는 RADIUS 기반 정책 서버에 인터페이스하는 IETF 세션 정책 프레임워크에 기초하는 것이 바람직하다.
- [0103] 도 16은 네트워크에서 UA가 세션 정책에 액세스하는 방법(600)의 실시예를 나타낸다. 블록(610)에서, UA는 단일 네트워크 컴포넌트로의 단일 세션 정책 요청을 통해 복수의 네트워크 컴포넌트에 접속한다.
- [0104] 다른 구현예에서, SIP UA가 SIP 인프라스트럭처, 예를 들어, IMS 네트워크로부터 서비스를 얻기를 원하면, SIP UA는, 제한되지는 않지만, SIP REGISTER 등의 메시지를 송신한다. 네트워크 노드가 S-CSCF iFC(initial Filter Criteria) 트리거 등의 SIP REGISTER를 수신하면, 제한되지는 않지만, SIP 서버 또는 정책 서버일 수 있는 또 다른 네트워크 노드로 제3자 등록이 이루어진다. SIP 서버는 SIP UA에 의해 요구된 세션 정책 정보를 포함하는 노드이다. SIP 서버는 SIP 푸쉬, SMS, USSD, 셀방송, 또는 MBMS를 통해 SIP로 정책 정보를 전송한다. 상기 예에서, 정책 정보는 등록 인코딩되거나 OMA DM 관리 객체일 수 있다.
- [0105] SIP REGISTRATION은 임의의 시간에 발생할 수 있고, 무선 액세스 기술 또는 그 능력을 변경할 때 등록을 수행하도록 SIP UA에 제공될 수 있다. 이 등록 정보는 상술한 바와 같이 SIP 서버에 의해 수신되면 정책 정보의 업데이트를 트리거할 수 있다. 이 업데이트는 SIP UA 능력 등의 새로운 정보 또는 Reg Event 패키지에 가입한 SIP 서버를 통해 또는 제3자 등록에서 전송될 수 있는 P-Network-Access-Info 헤더 정보에 기초할 수 있다.
- [0106] 다른 실시예에서, SIP REGISTRATION 및 제3자 등록은 SIP 서버가 SIP UA에 메시지를 전송하도록 하여 EAP 프레임 요청을 수행함으로써 정책 정보를 모으도록 한다.
- [0107] 또 다른 실시예에서, S-CSCF 등의 네트워크 노드가 2000K를 전송하면, 2000K가 정책 정보를 포함하거나 정책 정보를 얻을 수 있는 위치를 지정하는 URL을 포함할 수 있다. URL은, 제한되지는 않지만 SIP 헤더에 포함되거나 XML에 삽입될 수 있다.
- [0108] 또 다른 실시예에서, S-CSCF/레지스터는 REGISTER에 대한 SIP 2000K에서 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더를 반환할 수 있다. SIP REGISTER의 경로 상의 P-CSCF 등의 다른 SIP 프록시는 SIP REGISTER 내에서 직접 또는 간접으로 SIP REGISTER로의 SIP 2000K 내의 정책 서버의 policyContactURI를 포함하는 정책 접촉 헤더를 포함할 수 있다. policyContactURI가 SIP REGISTER에 포함되면, S-CSCF/레지스터 또는 다른 프록시는 직접 정책 문서를 얻어 그 문서를 자신의 정책 서버에 제공하여 모은 정책 문서를 생성하거나 다른 정책 서버(들)의 policyContactURI를 제공하여 상술한 메커니즘을 이용하여 모은 정책 문서가 정책 서버에 의해 생성될 수 있도록 한다. SIP REGISTER에서 수신된 정책 접촉 헤더는 SIP REGISTER에 대한 SIP 2000K에서 SIP UA에 제공될 수 있다.
- [0109] policyContactURI가 대안의 URI(예를 들어, alt-uri 파라미터)이고 정책 문서가 또 다른 정책(예를 들어, proxy-to 파라미터)을 통해 얻을 수 있다는 것을 식별하는 상술한 메커니즘은 SIP REGISTER 및 SIP 2000K 실시예와 함께 사용되어 다수의 정책 서버에 접속하지 않고 상술한 메커니즘을 이용하는 정책 채널을 이용하여 단일 정책 서버를 접촉함으로써 SIP UA가 효율적인 방식으로 모은 정책을 얻을 수 있도록 한다.
- [0110] draft-ietf-sip-session-policy-framework-05는 SIP REGISTER 또는 SIP 2000K에서 사용되는 정책 접촉 헤더를 현재 정의하지 않아 본 실시예는 draft-ietf-sip-session-policy-framework-05에 대한 SIP 확장으로서 구현될 수 있다. 이 확장에 대한 지원을 나타내기 위해, SIP UA는 SIP REGISTER 요청 내의 옵션-태그 "정책" 등의 옵션 태그를 포함하는 지원 헤더를 포함할 수 있다. 이 옵션 태그에 기초하여, 제3자 등록을 통한 프록시, S-CSCF/레지스터 및/또는 애플리케이션 서버는 SIP UA가 SIP REGISTER에 대한 SIP 2000K 내의 수신 정책 접촉

헤더를 지원하는 것으로 결정할 수 있다.

[0111] 또 다른 실시예에서, UA는 네트워크로 제1 허가 유형의 메시지를 송신할 수 있고, 제1 허가 유형은, 제한되지는 않지만, EAP, GPRS 활성화 PDP 컨텍스트 또는 SIP REGISTER일 수 있다. 제1 허가 유형 메시지 내에, SIP UA 등의 정보, InfoOffer 정보 및 공공 사용자 식별자 등의 가입자 식별자 등을 식별하는 파라미터 세트가 존재할 수 있다. 용어 세트는 잘 정의된 개별 객체의 모음이며, 여기서 이들 정의된 개별 객체 또는 정보 요소의 수는 제로 내지 다수일 수 있음을 당업자는 인식할 것이다. 다음은 UA로부터 네트워크로의 메시지의 예이다.

EAP Code: 1 (Request)

Type: 125* SessionPolicy

Length: Variable

Value:

[NAI]

[info offer]

[info answer]

<MIC>

[0113]

[0114] NAI는 네트워크로 인증하기 위하여 UA에 의해 사용되는 식별자이다. 식별자의 포맷은 RFC 4282에 정의되어 있다. NAI 내용은 AAA 서버(RADIUS 또는 DIAMETER)에 의해 사용되어 정책 요청을 적절한 정책 서버로 라우팅한다. EPA "유형"은 EAP 내용을 라우팅하는데 사용된다.

[0115] 제1 허가 유형 메시지는, 제한되지는 않지만, AAA 서버, GGSN 또는 CSCF일 수 있는 네트워크 노드에 의해 수신될 수 있다. 이 네트워크 노드는 제1 허가 유형 정보 세트를 받아, 제한되지는 않지만, RADIUS, DIAMETER 또는 SIP REGISTER일 수 있는 제2 허가 유형 메시지에 포함시킬 수 있다. 제1 하위층 메시지는 전부 제2 하위층 메시지에 배치될 수 있다. 제2 하위층 메시지는 필요한 정책 정보를 제1 네트워크 노드로 반환할 수 있는 제2 네트워크 노드로 전송될 수 있다. 제1 네트워크 노드는 역 변환을 수행하고 제1 허가 유형의 확인 응답을 정책 정보를 포함하는 UA로 반환할 수 있다. 다음은 네트워크로부터 UA로의 메시지의 일 예이다.

EAP Code: 2 (Response)

Type: 125* SessionPolicy

Length: Variable

Value:

[NAI]

[policy offer]

[policy answer]

<MIC>

[0116]

[0117] 정책 제안(policy offer), 정책 대답(policy answer), 정보 제안, 및 정보 대답은 <http://www.ietf.org/internet-drafts/draft-ietf-sipping-media-policy-dataset-06.txt>에 정의되어 있다.

- [0118] 인증을 위해 사용되는 (EAP-SIM 또는 EAP-AKA 등의) EAP 방법은 EAP 키잉 프레임워크(RFC 5247)에 순응하면, MIC는 위조 또는 재전송 공격에 대하여 세션 정책 요청/응답을 보호하는데 사용될 수 있다. 대안으로, 세션 정책 요청/응답은 공유키로 보호될 수 있다.
- [0119] 도 17은 UA가 네트워크에서 세션 정책을 액세스하는 방법(700)의 실시예를 나타낸다. 블록(710)에서, UA는 등록 메시지를 제1 네트워크 노드로 전송한다. 블록(702)에서, UA는 정책 관련 정보를 수신한다.
- [0120] UA(110) 및 상술한 다른 컴포넌트는 상술한 동작에 관련된 명령을 실행할 수 있는 프로세싱 컴포넌트를 포함할 수 있다. 도 18은 여기에 개시된 하나 이상의 실시예를 구현하기에 적합한 프로세싱 컴포넌트(1310)를 포함하는 시스템(1300)의 일예를 나타낸다. (중앙 처리 장치 또는 CPU라 불릴 수 있는) 프로세서(1310)에 더하여, 시스템(1300)은 네트워크 접속 장치(1320), 랜덤 액세스 메모리(RAM)(1330), 리드 온리 메모리(ROM)(1340), 제2 저장 장치(1350), 및 입출력(I/O) 장치(1360)를 포함할 수 있다. 이들 컴포넌트는 버스(1370)를 통해 서로 통신할 수 있다. 어떤 경우, 이들 컴포넌트의 일부가 존재하지 않거나 서로 다양한 조합으로 조합되거나 도시되지 않은 다른 구성요소와 조합될 수 있다. 이들 컴포넌트는 단일의 물리적 엔티티 또는 하나 이상의 물리적 엔티티에 위치할 수 있다. 프로세서(1310)에 의해 취해지는 여기에 기재된 임의의 동작은 프로세서(1310) 단독으로 수행되거나 디지털 신호 프로세서(DSP)(1380) 등의 도시되거나 도시되지 않은 하나 이상의 컴포넌트와 결합하여 프로세서(1310)에 의해 수행될 수 있다. DSP(1380)가 별도의 컴포넌트로서 도시되어 있지만, DSP(1380)는 프로세서(1310)에 통합될 수 있다.
- [0121] 프로세서(1310)는 네트워크 접속 장치(1320), RAM(1330), ROM(1340), 또는 (하드 디스크, 플로피 디스크, 광 디스크 등의 다양한 디스크 기반 시스템을 포함할 수 있는) 제2 저장 장치(1350)로부터 액세스될 수 있는 명령, 코드, 컴퓨터 프로그램 또는 스크립트를 실행할 수 있다. 하나의 CPU(1310)만이 도시되어 있지만, 다수의 프로세서가 존재할 수 있다. 따라서, 명령이 프로세서에 의해 실행되는 것으로 기재되어 있지만, 명령은 하나 또는 다수의 프로세서에 의해 동시에, 순차적으로 또는 다른 방법으로 실행될 수 있다. 프로세서(1310)는 하나 이상의 CPU 칩으로서 구현될 수 있다.
- [0122] 네트워크 접속 장치(1320)는 모뎀, 모뎀 뱅크, 이더넷 장치, USB(universal serial bus) 인터페이스 장치, 시리얼 인터페이스, 토큰 링 장치, FDDI(fiber distributed data interface) 장치, 무선 LAN 장치, 코드 분할 다중 액세스(CDMA) 장치 등의 무선 트랜시버 장치, GSM(global system for mobile communications) 무선 트랜시버 장치, WiMAX(worldwide interoperability for microwave access) 장치, xDSL(digital subscriber line) 장치, DOCSIS(data over cable service interface specification) 모뎀, 및 또는 네트워크에 접속하기 위한 다른 공지된 장치의 형태를 취할 수 있다. 이들 네트워크 접속 장치(1320)는 프로세서(1310)가 인터넷 또는 하나 이상의 텔레커뮤니케이션 네트워크 또는 프로세서(1310)가 정보를 수신하거나 프로세서(1310)가 정보를 출력할 수 있는 다른 네트워크와 통신하도록 할 수 있다.
- [0123] 네트워크 접속 장치(1320)는 또한 무선 주파수 신호 또는 마이크로파 주파수 신호 등의 전자파의 형태로 무선으로 데이터를 송신 및/또는 수신할 수 있는 하나 이상의 트랜시버 컴포넌트(1325)를 포함할 수 있다. 대안으로, 데이터는 전기 도체의 표면 내 또는 전기 도체의 표면 상, 동축 케이블 내, 도파관 내, 광섬유 등의 광 매체 내 또는 다른 매체 내에서 전파할 수 있다. 트랜시버 컴포넌트(1325)는 별도의 수신 및 송신 유닛 또는 단일 트랜시버를 포함할 수 있다. 트랜시버 컴포넌트(1325)에 의해 송신 또는 수신되는 정보는 프로세서(1310)에 의해 프로세싱될 데이터 또는 프로세서(1310)에 의해 실행될 명령을 포함할 수 있다. 이러한 정보는 예를 들어 컴퓨터 데이터 베이스밴드 신호 또는 반송파에 포함되는 신호의 형태로 네트워크로부터 수신되거나 네트워크로 출력될 수 있다. 데이터는 데이터를 프로세싱 또는 생성하거나 데이터를 송신 또는 수신하기에 바람직하도록 상이한 시퀀스에 따라 정렬될 수 있다. 베이스밴드 신호, 반송파에 포함된 신호 또는 현재 사용되거나 이후 개발되는 다른 유형의 신호는 전송 매체로 지칭될 수 있고 당업자에게 공지된 몇 개의 방법에 따라 생성될 수 있다.
- [0124] RAM(1330)은, 휘발성 데이터를 저장하고 프로세서(1310)에 의해 실행되는 명령을 저장하는데 사용될 수 있다. ROM(1340)은 제2 저장 장치(1350)의 메모리 용량보다 작은 메모리 용량을 갖는 비휘발성 메모리 장치이다. ROM(1340)은 명령 실행시 판독될 수 있는 데이터 및 명령을 저장하는데 사용될 수 있다. RAM(1330) 및 ROM(1340)으로의 액세스는 제2 저장 장치(1350)로의 액세스보다 빠르다. 제2 저장 장치(1350)는 일반적으로 하나 이상의 디스크 드라이브 또는 테이프 드라이브로 구성되고 RAM(1330)이 모든 작업 데이터를 유지하기에 충분히 크지 않을 때 데이터의 비휘발성 저장장치 또는 오버플로우 데이터 저장 장치로서 이용될 수 있다. 제2 저장 장치(1350)는 프로그램이 실행용으로 선택될 때 RAM(1330)으로 로딩되는 프로그램을 저장하는데 사용될 수 있다.

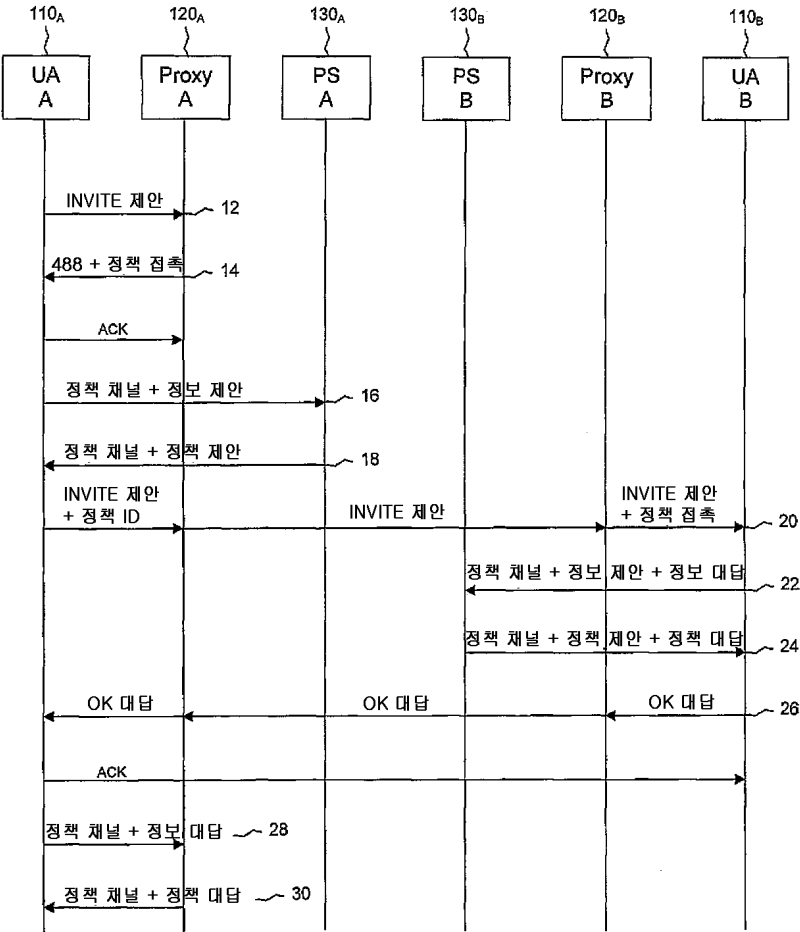
- [0125] I/O 장치(1360)는 액정 표시 장치(LCD), 터치 스크린 디스플레이, 키보드, 키패드, 스위치, 다이얼, 마우스, 트랙볼, 음성 인식기, 카드 판독기, 페이퍼 테이프 판독기, 프린터, 비디오 모니터 또는 다른 공지된 입출력 장치를 포함할 수 있다. 또한 트랜시버(1325)는 네트워크 접속 장치(1320)의 컴포넌트의 대신에 또는 그에 추가하여 I/O 장치(1360)의 컴포넌트로 간주될 수 있다.
- [0126] 다음의 IETF 인터넷 드래프트가 전부 재현된 것처럼 참고로 여기에 포함된다.
- <http://www.ietf.org/internet-drafts/draft-ietf-sip-session-policy-framework-05.txt>
<http://www.ietf.org/internet-drafts/draft-ietf-sipping-media-policy-dataset-06.txt>
<http://www.ietf.org/internet-drafts/draft-ietf-sipping-config-framework-15.txt>
- [0127] <http://www.ietf.org/internet-drafts/draft-ietf-sipping-policy-package-05.txt>
- [0128] 또한 다음의 3GPP 문서가 전부 재현된 것처럼 참고로 여기에 포함된다: RFC 2284, RFC 2661, RFC 3264, RFC 3265, RFC 3261, RFC 3312, RFC 3588, RFC 4282, RFC 4482, RFC 4566, RFC 5108, RFC 5247, TS 23.203, TS 23.228, TS 23.229 및 TS 24.229.
- [0129] 또한 IEEE 802.11, IEEE 802.16 및 IEEE 802.20이 전부 재현된 것처럼 참고로 여기에 포함된다.
- [0130] 실시예에서, 네트워크 컴포넌트에 세션 정책 요청을 전송하는 방법이 제공된다. 방법은 사용자 에이전트가 하위층 프로토콜을 이용하여 세션 정책 요청을 네트워크 컴포넌트로 전송하는 단계를 포함한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나일 수 있다.
- [0131] 다른 실시예에서, 사용자 에이전트가 제공된다. 사용자 에이전트는 하위층 프로토콜을 이용하여 세션 정책 요청을 네트워크 컴포넌트로 전송하는 프로세서를 포함한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나일 수 있다.
- [0132] 다른 실시예에서, 네트워크 컴포넌트가 제공된다. 네트워크 컴포넌트는 하위층 프로토콜을 이용해 전송된 세션 정책 요청을 수신하는 인증 컴포넌트를 포함한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나일 수 있다.
- [0133] 다른 실시예에서, 사용자 에이전트가 네트워크에서 세션 정책을 액세스하는 방법이 제공된다. 방법은 사용자 에이전트가 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하는 단계를 포함하고, 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용한다.
- [0134] 다른 실시예에서, 사용자 에이전트가 제공된다. 사용자 에이전트는 사용자 에이전트가 네트워크에서 세션 정책으로의 액세스를 제공하는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 수신하도록 구성된 프로세서를 포함하고, 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용한다.
- [0135] 다른 실시예에서, 네트워크 컴포넌트가 제공된다. 네트워크 컴포넌트는 네트워크 컴포넌트가 네트워크에서 세션 정책으로의 액세스를 제공할 수 있는 정책 서버에 대한 복수의 URI를 응답 메시지의 헤더 필드에서 송신하도록 구성된 프로세서를 포함하고, 복수의 URI의 각각은 상이한 정책 채널 프로토콜을 이용한다.
- [0136] 다른 실시예에서, 사용자 에이전트가 네트워크에서 세션 정책에 액세스하는 방법이 제공된다. 방법은 사용자 에이전트로부터 단일 네트워크 컴포넌트로 단일 세션 정책 요청을 전송하는 단계, 단일 네트워크 컴포넌트가 복수의 네트워크 컴포넌트에 접속하는 단계를 포함하고, 단일 세션 정책 요청을 단일 네트워크 컴포넌트로 전송하는 단계는 하위층 프로토콜을 이용한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나일 수 있다. 방법은 정책 정보를 모으는 단계 및 사용자 에이전트에 모은 정책 정보를 제공하는 단계를 더 포함한다.
- [0137] 다른 실시예에서, 사용자 에이전트가 제공된다. 사용자 에이전트는 단일 세션 정책 요청의 송신에 응답하여 복수의 네트워크 컴포넌트에 관한 모든 정책 정보를 수신하는 프로세서를 포함하고, 상기 사용자 에이전트는 하위층 프로토콜을 이용하여 단일 네트워크 컴포넌트에 세션 정책 요청을 전송한다. 하위층 프로토콜은 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio

Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나일 수 있다.

- [0138] 다른 실시예에서, 네트워크 컴포넌트가 제공된다. 네트워크 컴포넌트는 단일 세션 정책 요청을 수신하고 복수의 네트워크 컴포넌트로부터의 정책 정보 모음에 응답하여 모은 정책 정보를 송신하는 프로세서를 포함한다. 네트워크 컴포넌트는 EAP(Extensible Authentication Protocol), PPP(Point to Point Protocol), 및 GPRS(General Packet Radio Service) 활성화 PDP(Packet Data Protocol) 컨텍스트 중의 적어도 하나인 하위층 프로토콜을 통해 사용자 에이전트로부터 세션 정책 요청을 수신한다.
- [0139] 다른 실시예에서, 사용자 에이전트가 네트워크에서 세션 정책을 액세스하는 방법이 제공된다. 방법은 사용자 에이전트가 제1 네트워크 노드에 등록 메시지를 전송하는 단계를 포함한다. 방법은 또한 사용자 에이전트가 등록 메시지에 응답하여 제1 네트워크 노드로부터 정책 관련 정보를 수신하는 단계를 더 포함한다. 정책 관련 정보는 세션 정책, 세션 정책을 지시하는 URI, 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나일 수 있다.
- [0140] 다른 실시예에서, 사용자 에이전트가 제공된다. 사용자 에이전트는 사용자 에이전트가 등록 메시지를 송신하고 등록 메시지에 응답하여 제1 네트워크 노드로부터 정책 관련 정보를 수신하도록 구성된 프로세서를 포함한다. 정책 관련 정보는 사용자 에이전트가 통신할 수 있는 네트워크에 대한 세션 정책, 세션 정책을 지시하는 URI, 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나일 수 있다.
- [0141] 다른 실시예에서, 네트워크 노드가 제공된다. 네트워크 노드는 네트워크 노드가 등록 메시지의 수신에 응답하여 사용자 에이전트에 정책 관련 정보를 송신하도록 구성된 프로세서를 포함한다. 정책 관련 정보는 네트워크 노드가 네트워크 노드가 컴포넌트인 네트워크에 대한 세션 정책, 세션 정책을 지시하는 URI, 정책 문서에 대한 policyContactURI를 포함하는 정책 접촉 헤더 중의 하나일 수 있다.
- [0142] 이들 주제와 관련된 추가의 정보는 제목이 "System and Method for Indicating Supported Session Policy URI Schemes Extensions"이고 2008년 2월 18일에 제출된 앤드류 알렌 등의 미국 가출원 번호 제61/029,522호 및 제목이 "System and Method for Resolving Extensions for the SIP Session Policy Framework"이고 2008년 2월 18일에 제출된 앤드류 알렌 등의 미국 가출원 번호 제61/029,523호에 개시되어 있으며, 이는 참조로 포함된다.
- [0143] 본 개시물에는 몇 가지 실시예가 제공되지만, 본 개시물의 사상 및 범위를 벗어나지 않고 개시된 시스템 및 방법이 다른 많은 특정 형태로 구현될 수 있음을 이해해야 한다. 본 예들은 설명하기 위한 것으로 제한적인 것은 아니며, 여기에 기재된 세부항목으로 제한되지 않는다. 예를 들어, 다양한 요소 또는 컴포넌트는 다른 시스템에서 조합 또는 통합되거나 특정 특징이 생략되거나 구현되지 않을 수 있다.
- [0144] 다양한 실시예에 별도로 기재된 기술, 시스템, 서브시스템 및 방법은 본 개시물의 범위를 벗어나지 않는 한도 내에서 다른 시스템, 모듈, 기술, 또는 방법과 조합 또는 통합될 수 있다. 서로 직접 결합되거나 서로 통신하는 것으로 기재된 다른 항목들이 전기적, 기계적 또는 다른 방법에 관계없이 간접적으로 결합되거나 임의의 인터페이스, 장치 또는 중간 컴포넌트를 통해 통신할 수 있다. 변경, 대체, 변형의 다른 예가 당업자에 의해 확인될 수 있으며 본 개시물의 사상 및 범위를 벗어나지 않는 한도 내에서 구현될 수 있다.

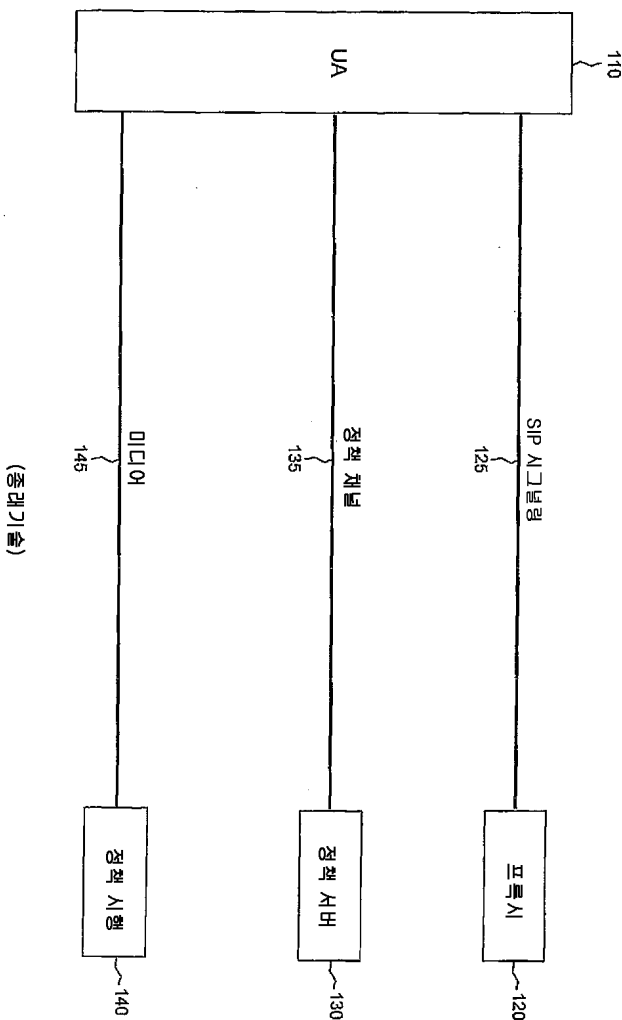
도면

도면1

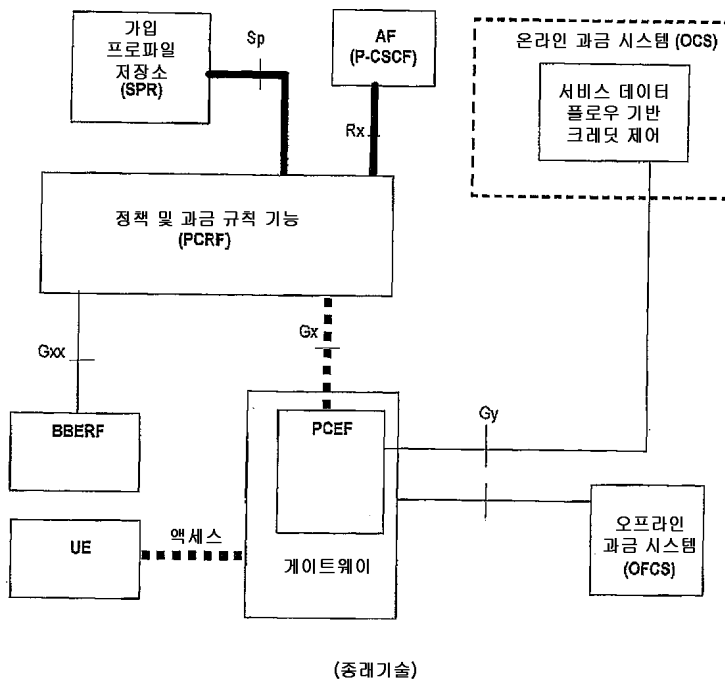


(종래기술)

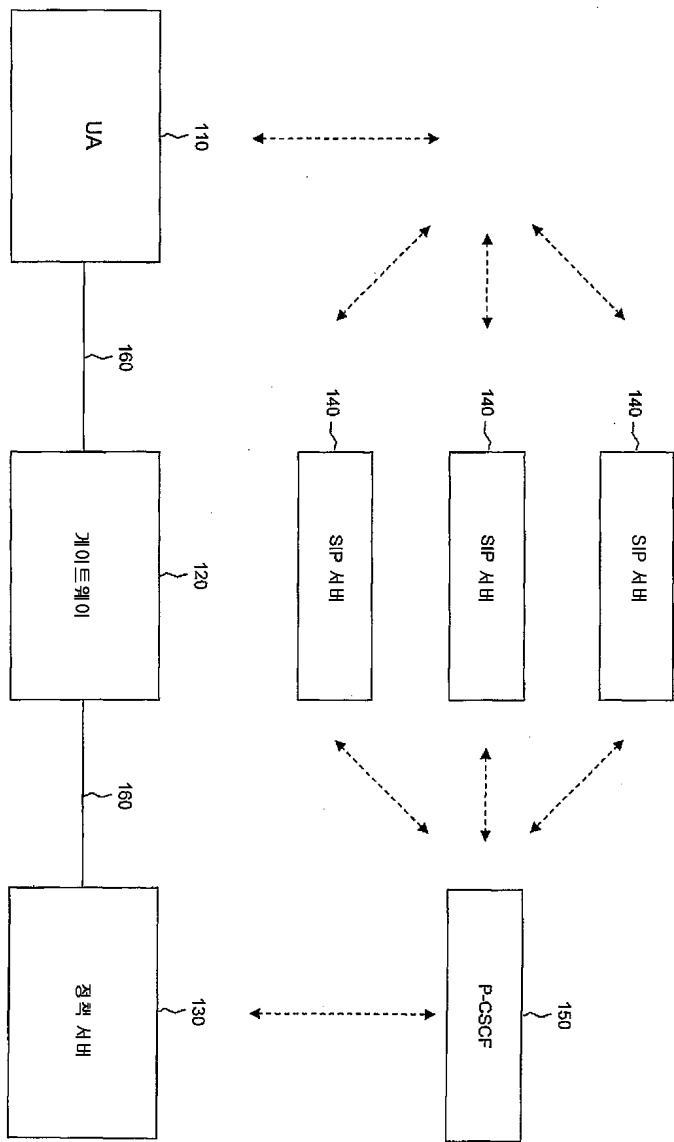
도면2



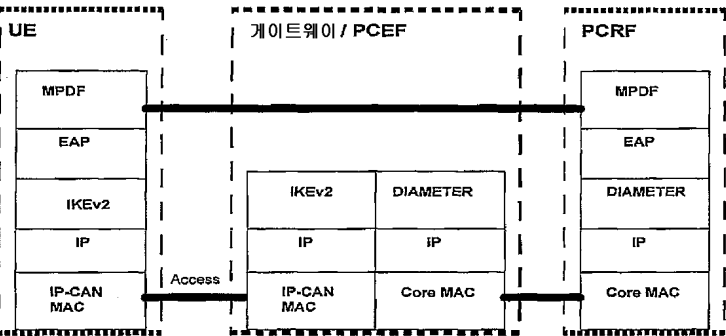
도면3



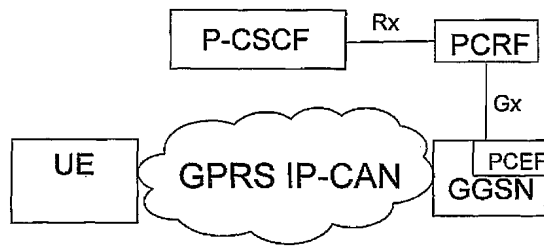
도면4



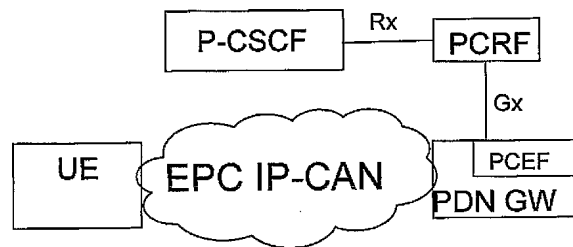
도면5



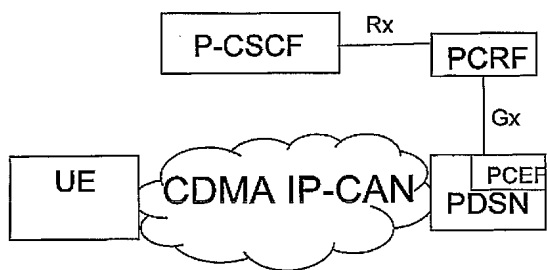
도면6



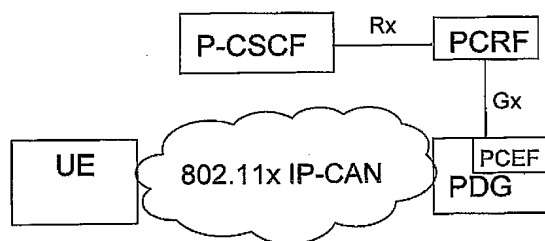
도면7



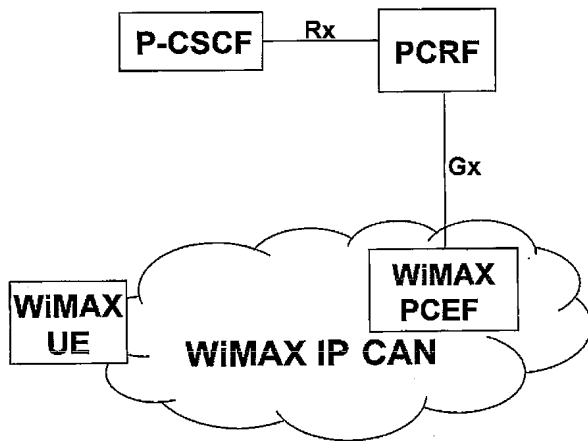
도면8



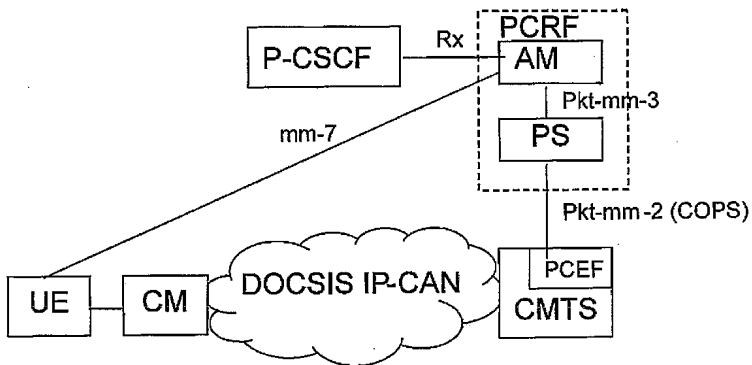
도면9



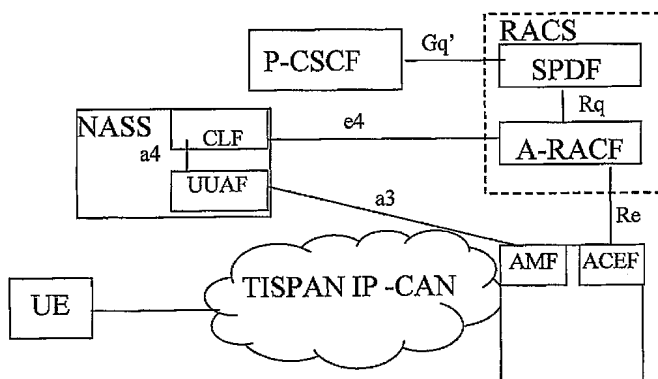
도면10



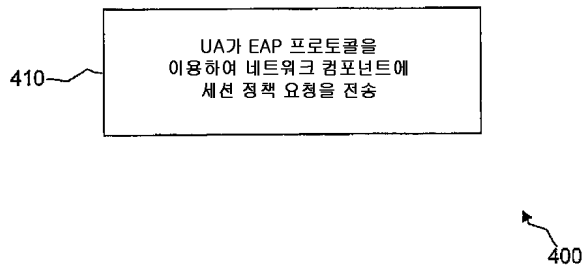
도면11



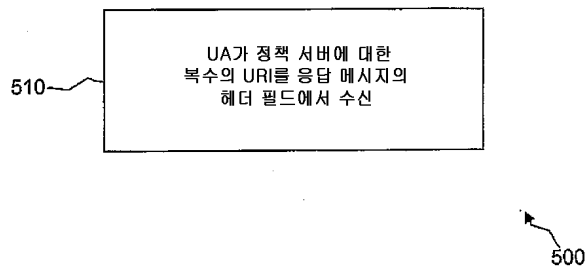
도면12



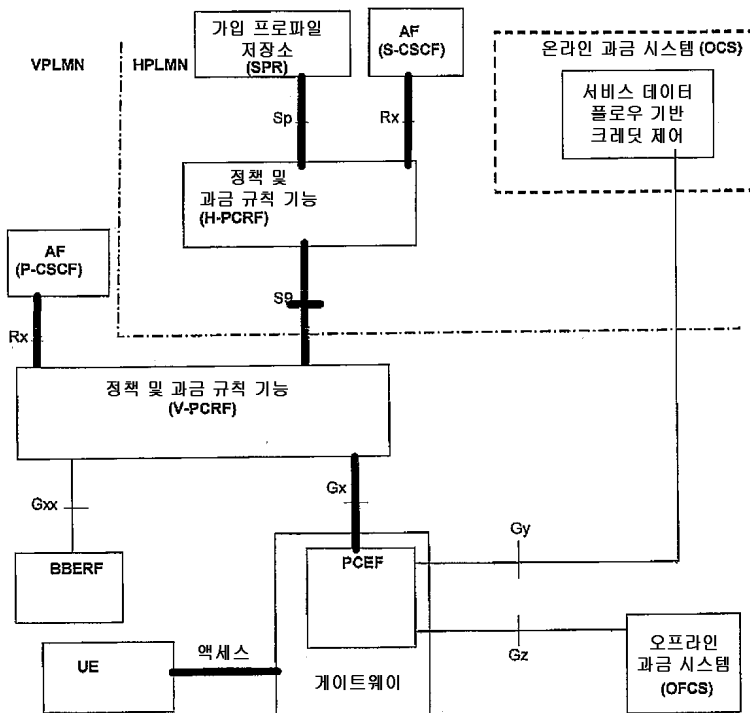
도면13



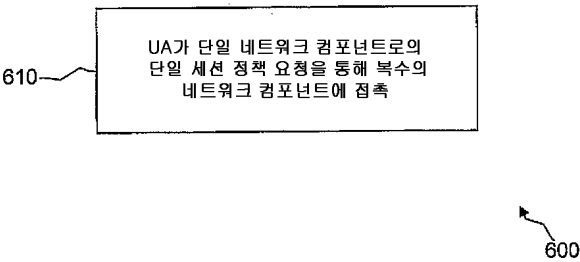
도면14



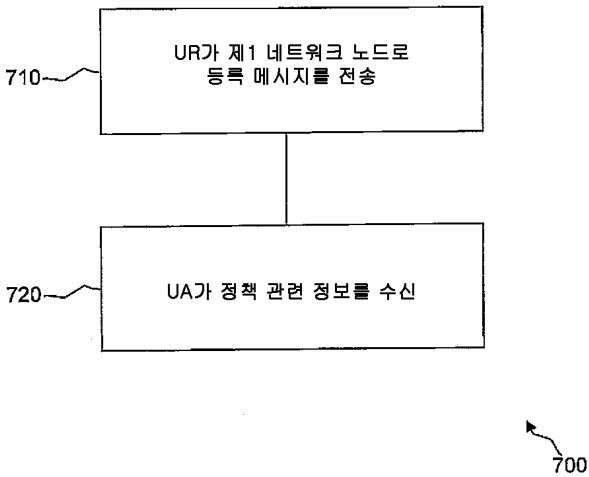
도면15



도면16



도면17



도면18

