(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년01월29일
(11) 등록번호 10-2070275
(24) 등록일자 2020년01월20일

(51) 국제특허분류(Int. Cl.)
H04L 12/12 (2006.01) *H04L 12/24* (2006.01)
H04L 12/26 (2006.01) *H04L 29/08* (2006.01)
(21) 출원번호 10-2014-7002102
(22) 출원일자(국제) 2012년06월27일
심사청구일자 2017년06월01일
(85) 번역문제출일자 2014년01월24일
(65) 공개번호 10-2014-0040253
(43) 공개일자 2014년04월02일
(86) 국제출원번호 PCT/EP2012/062415
(87) 국제공개번호 WO 2013/000936
국제공개일자 2013년01월03일
(30) 우선권주장
11447015.6 2011년06월29일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US06021507 A*
US20070214262 A1*
US20110060822 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인터디지털 씨이 페이튼트 홀딩스
프랑스 75017 빠리 뤼 뒤 꼴로넬 몰 3
(72) 발명자
반 드 포엘, 더크
벨기에 2650 에드겜 프린스 보데위즌란 47 테크니컬러
(74) 대리인
양영준, 백만기

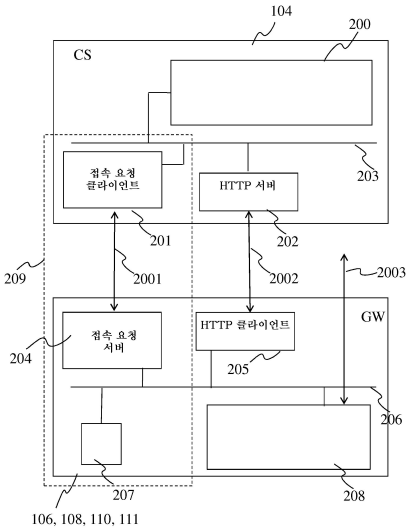
전체 청구항 수 : 총 8 항 심사관 : 이준석

(54) 발명의 명칭 **장치의 원격 관리**

(57) 요 약

본 발명은 장치의 원격 관리 분야 및 그 방법을 구현하는 장치에 관한 것이다. 특히, 본 발명은 원격 관리가능 장치에 대한 라이프라인 접속에 관한 것이고, 라이프라인 접속은 원격 설정 관리 서버와 원격 관리가능 장치 사이에서 손실된 통신을 재확립하는데 사용될 수 있다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

설정 서버 장치(configuration server device)(104)와 고객 지역 설비 장치(customer premises equipment device)(106, 108, 110, 111) 간의 통신 방법으로서,

상기 설정 서버 장치에서,

상기 설정 서버 장치가 상기 고객 지역 설비 장치와의 원격 관리 접속이 손실(lost)된 것으로 결정한 경우, 상기 설정 서버 장치는 더 이상 상기 고객 지역 설비 장치와의 관리 세션을 확립할 것을 상기 설정 서버 장치에 요청하도록 상기 고객 지역 설비 장치를 트리거할 수 없기 때문에,

상기 설정 서버 장치에 의하여, 상기 고객 지역 설비 장치의 재구성을 가능하게 하는 정보를 포함하는 메시지를 송신하는 단계; 및

상기 설정 서버 장치에 의하여, 상기 고객 지역 설비 장치와의 손실된 원격 관리 접속의 재확립에 대한 요청을 상기 고객 지역 설비 장치로부터 수신하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서, 상기 메시지는 상기 고객 지역 설비 장치의 미리 결정된 포트 번호에 송신되고, 미리 결정된 포트 번호 상에서 상기 고객 지역 설비 장치가 상기 고객 지역 설비 장치의 재구성을 가능하게 하는 정보를 포함하는 메시지들을 청취하는, 방법.

청구항 3

제1항 또는 제2항에 있어서, 상기 정보는 상기 설정 서버 장치의 어드레스를 포함하는 방법.

청구항 4

제1항 또는 제2항에 있어서, 상기 정보는 접속 요청 크리덴셜(connection request credentials)을 포함하는 방법.

청구항 5

상호접속된 고객 지역 설비 장치(106, 108, 110, 111)와 설정 서버 장치(104) 간의 통신 방법으로서,

상기 고객 지역 설비 장치에서,

상기 설정 서버 장치가 상기 고객 지역 설비 장치와의 원격 관리 접속이 손실(lost)된 것으로 결정한 경우, 상기 설정 서버 장치는 더 이상 상기 고객 지역 설비 장치와의 관리 세션을 확립할 것을 상기 설정 서버 장치에 요청하도록 상기 고객 지역 설비 장치를 트리거할 수 없기 때문에,

상기 고객 지역 설비 장치에 의하여, 상기 고객 지역 설비 장치의 재구성을 가능하게 하는 정보를 포함하는 메시지를 수신하는 단계;

상기 고객 지역 설비 장치에 의하여, 상기 고객 지역 설비 장치와의 상기 손실된 원격 관리 접속의 재확립에 대한 요청을 송신하는 단계

를 포함하는 방법.

청구항 6

제5항에 있어서, 상기 메시지는 미리 결정된 포트 번호 상에서 수신되고, 미리 결정된 포트 번호 상에서 상기 고객 지역 설비 장치가 상기 고객 지역 설비 장치의 재구성을 가능하게 하는 정보를 포함하는 메시지들을 청취

하는, 방법.

청구항 7

제5항 또는 제6항에 있어서, 상기 정보는 상기 설정 서버 장치의 어드레스를 포함하는 방법.

청구항 8

제5항 또는 제6항에 있어서, 상기 정보는 접속 요청 크리덴셜을 포함하는 방법.

청구항 9

삭제

청구항 10

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 장치의 원격 관리 분야 및 그 방법을 구현하는 장치에 관한 것이다. 특히, 본 발명은 원격 관리가능 장치와 원격 관리 서버 사이에서 원격 관리 통신이 손실되었을 때 사용될 수 있는 장치의 원격 관리에 대한 라이프라인(life-line) 접속에 관한 것이다.

배 경 기 술

[0002] 예를 들어, 소위 트리플 플레이 게이트웨이(VoIP(Voice Over Internet Protocol) 전화, 인터넷, IP 텔레비전) 등의 집에서의 서비스 가입자 장치의 출현으로, 서비스 가입자 장치가 서비스 오퍼레이터에 의해 제안된 서비스를 만족스러운 방식으로 정확하게 사용/수신할 수 있도록 구성하기 위하여, 이들 서비스 가입자 장치를 관리하는 방법에 대한 문제가 서비스 오퍼레이터에게 발생한다. 특히, 서비스 오퍼레이터는 빈번히 추가의 소프트웨어를 인스톨하거나, 펌웨어를 업그레이드하거나, 오퍼레이터에 의해 제공된 홈 게이트웨이 내의 기존의 소프트웨어 또는 하드웨어를 설정(configure)하여 새로운 서비스를 제공하거나 기존의 서비스를 개선할 필요가 있다.

[0003] 솔루션은 예를 들어 CPE 또는 서비스 가입자 장치의 원격 설정에 대한 TR-069 규격에 따라 전용 설정(configuration) 장치 또는 ACS(Auto Configuration Server)에 이들 서비스 가입자 장치를 접속하는 것을 포함하고, 여기서 ACS는 서비스 가입자 장치에 필요한 소프트웨어를 자동으로 배포하는 것을 담당한다. TR-069는 게이트웨이 및 라우터, 시청각 수신을 위한 셋탑 박스, VoIP(voice over IP) 전화 세트 및 NAS(Network Attached Storage) 등의 장치에 의해 지원된다.

[0004] 그러나, 기존의 솔루션은 ACS와 CPE 장치 간의 통신이 확실히 손실되었을 때 실패하는데, 예를 들어, TR-069의 경우에는, CPE 장치가 ACS(auto configuration server)와 관리 세션을 확립할 책임이 있다. ACS는 임의의 시간에 CPE를 트리거하여 소위 "접속 요청"에 의해 관리 세션을 확립할 수 있다. 인증 등의 추가의 보안 조치를 포함하고 원격 관리가 가능한 이 비교적 복잡한 수단은 원격 관리의 보안을 확보한다. TR-069가 견고한 프로토콜(robust protocol)로 설계되더라도, ACS가 CPE를 트리거하여 그와 원격 관리 접속을 확립하는 것을 성공하지 못하는 상황이 발생한다. 이 실패의 이유는 CPE가 ACS를 더이상 신뢰하지 못하여 ACS와의 관리 접속을 확립하는 것을 거절하는 TLS(Transport Layer Security) 인증서 만료; 예를 들어, CPE가 ACS URL(Uniform Resource Locator)를 손실했거나, CPE가 잘못된 ACS 인증 크리덴셜(ACS authentication credentials)을 갖는 경우 등의 CPE 상의 설정 문제; CPE가 긴 시간 동안 파워 오프 상태에 있어서 CPE 장치로 전달되지 않은 네트워크 토폴로지 변화; 또는 심지어 예를 들어 CPE 장치를 통해 제어를 획득하기 위한 이유로 원격 관리를 디스에이블하는 해킹(hacking)에 의한 자발적인 엔드 사용자 개입(intervention)을 포함한다. 원격 관리 접속이 모니터, 진단, 설정 관리 또는 심지어 펌웨어 업데이트를 위해 사용되기 때문에, 원격 관리 접속의 이 손실은 서비스 제공자에 대하여 큰 문제점을 제기한다. 더이상 관리할 수 없는 장치는 QoS(Quality of Service), 보안 또는 방화벽 서비스, IPTV(Internet Protocol Television) 등의 서비스; VoIP의 추가 및 전화 번호 설정 등의 새로운 서비스; 나쁜 접속성, 나쁜 서비스 품질 등의 임의의 보고 문제에 대한 진단 또는 트러블슈팅(troubleshooting); 및 새로운 장치 성능을 도입하거나 버그를 해결하기 위한 자동화된 펌웨어 업그레이드를 이용하는데 요구되는 설정

업데이트를 더이상 수신할 수 없다. CPE가 ACS의 정확한 위치(어드레스)를 잃어버렸거나 유효한 인증 정보를 잃어버렸다면, CPE가 서버에 대한 관리 접속을 성공적으로 확립할 수 없기 때문에 CPE는 ACS를 "손실"한 것으로 간주된다. 이 경우, 서비스 오퍼레이터와 가입자 장치 간의 통신은 확실히 손실되고 사용자에게 지시하거나 또는 사용자의 지역(premises)으로 엔지니어를 보내는 등의 오퍼레이터의 수동 개입에 의해서만 복원(restore)될 수 있다.

[0005] 2003년 12월 23일자 문헌 WO 03/107133 A2 "Secure Remote Management Appliance"(SMRA)는 네트워크 서비스로의 기존 접속의 손실 및 다른 인터페이스를 통한 네트워크 서비스로의 접속의 재확립을 기재한다. 그러나, 또 다른 추가의 네트워크 인터페이스 상의 네트워크 관리 스테이션을 접촉하려고 시도하는 것은, 네트워크 인터페이스의 변화가 이러한 실패 이유를 제거하지 않기 때문에, 상술한 문제 중의 하나가 발생하는 경우(상기 참조: "이 실패의 이유는 ~ 포함한다") SMRA가 네트워크 관리 스테이션에 여전히 접촉하지 못하게 한다.

[0006] 2009년 9월 10일자 문헌 US 2011/060822 A1 "Apparatus and method for managing communications"는 이웃 게이트웨이가 대신 관리 접속을 셋업하도록 요청함으로써 WAN 접속의 손실을 관리하는 게이트웨이를 기재한다. 이것은, 예를 들어, 적절한 크리덴셜을 제공하는 것을 실패하는 경우에, 실패한 게이트웨이가 대안의 관리 접속을 셋업할 수 없기 때문에, 상술한 문제점 중의 하나가 발생하는 경우, 게이트웨이가 WAN 접속을 복원할 수 없다. 또한, 이 솔루션은 실패한 게이트웨이가 이웃 게이트웨이와 통신할 수 있도록 요구하는데, 이는 네트워크 토폴로지가 변했을 때 불가능할 수 있다.

[0007] 따라서, 서비스 제공자의 관점으로부터 "손실(lost)"된 것으로 간주되는 장치에 대한 원격 관리 접속의 재확립을 지원하고 고객 개입에 대하여 또는 장치의 비용이 많이 드는 물리적 교체에 대한 필요성을 방지하기 위하여, 고객의 집에 배치된 오퍼레이터의 서비스 가입자 장치의 원격 설정 관리의 최적화가 필요하다.

발명의 내용

[0008] 본 발명의 목표는 종래 기술의 불편함 중의 적어도 일부를 완화하는 것이다.

[0009] 더 정밀하게, 본 발명은 서비스 오퍼레이터의 서비스 가입 장치 또는 CPE의 최적화된 원격 관리를 허용한다.

[0010] 이러한 취지로, 본 발명은 원격 관리 접속을 통해 디지털 통신 네트워크에서 상호 접속된 원격 설정 장치(remote configuration device)와 원격 설정가능 장치(remote configurable device) 간의 통신 방법으로서, 원격 설정 장치에서, 원격 관리 접속이 손실된 것으로 결정되면, 원격 관리 접속 이외의 접속(2001)을 통해 원격 설정가능 장치의 어드레스 및 원격 설정가능 장치의 미리 결정된 포트 번호로 원격 설정가능 장치에 의한 손실된 원격 관리 접속의 재확립을 허용하는 적어도 하나의 커맨드(command) 및 정보를 포함하는 메시지를 송신하는 단계; 및 원격 관리 접속의 재확립에 대한 요청을 수신하는 단계를 포함하고, 요청은 적어도 하나의 커맨드의 원격 관리 장치에 의한 적용 및 메시지 내에 포함된 정보의 원격 설정가능 장치에 의한 사용의 결과인 방법을 제안한다.

[0011] 본 발명은 또한 원격 관리 접속을 통해 디지털 통신 네트워크에서 상호 접속된 원격 설정가능 장치와 원격 설정 장치 간의 통신 방법으로서, 원격 설정가능 장치에서, 원격 관리 접속이 손실된 것으로 결정되면, 원격 관리 접속 이외의 접속을 통해 미리 결정된 포트 번호 상에서 원격 설정가능 장치에 의한 손실된 원격 관리 접속의 재확립을 허용하는 적어도 하나의 커맨드 및 정보를 포함하는 메시지를 수신하는 단계; 적어도 하나의 커맨드를 적용하는 단계; 손실된 원격 관리 접속의 재확립에 대한 요청을 원격 설정 장치로 송신하는 단계를 포함하고, 요청은 적어도 하나의 커맨드의 적용 및 메시지 내에 포함된 정보의 사용의 결과인 방법을 제안한다.

[0012] 변형 실시예에 따르면, 미리 결정된 포트 번호는 원격 관리 접속이 손실될 때 원격 설정가능 장치로 하여금 원격 설정 장치와의 원격 관리 접속을 재확립하게 하도록 하는 메시지를 원격 설정가능 장치가 청취하는 포트 번호이다.

[0013] 변형 실시예에 따르면, 정보는 손실된 원격 관리 접속을 재확립하는데 사용되는 접속 요청 크리덴셜을 포함한다.

[0014] 변형 실시예에 따르면, 정보는 손실된 원격 관리 접속이 재확립되는 원격 설정 장치의 어드레스를 포함한다.

[0015] 본 발명은 또한 원격 관리 접속 이외의 접속을 통해 장치의 미리 결정된 포트 번호 상에서 장치에 의한 손실된 원격 관리 접속의 재확립을 허용하는 적어도 하나의 커맨드 및 정보를 포함하는 메시지를 수신하는 접속 요청 서버; 및 원격 설정 장치로 손실된 원격 관리 접속의 재확립에 대한 요청을 송신하는 클라이언트 모듈을 포함하

고, 요청은 적어도 하나의 커맨드의 장치에 의한 적용 및 메시지 내에 포함된 정보의 장치에 의한 사용의 결과인 장치를 포함한다.

[0016] 장치의 변형 실시예에 따르면, 접속 요청 서버 및 클라이언트 모듈은 장치의 다른 모듈과 독립적으로 기능한다.

도면의 간단한 설명

[0017] 본 발명의 더 많은 이점은 본 발명의 특정한 비제한적 실시예의 설명을 통해 나타날 것이다. 실시예는 다음의 도면을 참조하여 설명한다.

도 1은 본 발명이 구현되는 예시적인 네트워크 인프라스트럭쳐를 나타내는 도면.

도 2는 본 발명을 구현하는 도 1의 장치(104 및 106/108/110/111)에 추가된 추가적인 모듈(201 및 204)을 나타내는 도면.

발명을 실시하기 위한 구체적인 내용

[0018] 도 1은 본 발명이 구현되는 예시적인 네트워크 인프라스트럭쳐를 나타낸다.

[0019] 네트워크 인프라스트럭쳐는,

[0020] - 제공자 서버의 세트(100-103), 예를 들어, 웹 서버(100), VoD(Video On Demand) 서버(101), 광대역 방송 서버(102), 및 VoIP 서버(103);

[0021] - 설정 서버(CS:configuration server)(104);

[0022] - 게이트웨이(GW:gateway) 장치(106), CPE;

[0023] - 액세스 네트워크(105), 예를 들어, 인터넷 또는 전용 네트워크; 액세스 네트워크는 (접속(1000)을 통해) 제공자 서버(100-103), (접속(1001)을 통해) 설정 서버(104) 및 (접속(1002)을 통해) 게이트웨이(106)를 상호 접속한다.

[0024] - 홈 네트워크 상의 장치를 상호 접속하고 게이트웨이(106)를 통해 장치를 (접속(1004, 1005, 1006)을 통해) 액세스 네트워크(105) 및 액세스 네트워크(105)에 접속된 다른 장치(100-103, 104)에 접속하는 로컬 네트워크(107);

[0025] - 퍼스널 컴퓨터(PC:personal computer)(108), CPE;

[0026] - 텔레비전 세트(109);

[0027] - 셋탑박스(STB:Set Top Box)(110), CPE; 및

[0028] - 무선 PC(111), CPE

[0029] 를 포함한다.

[0030] 게이트웨이(106)는, 가입자에게 트리플 플레이 서비스를 제공하기 위하여 오퍼레이터에 의해 제공되는 장치이다. 게이트웨이(106)는 가입자가

[0031] - IPTV 셋탑 박스(110) 및 TV 세트(109)를 통해 논리적 접속(2002)을 통해 오퍼레이터의 광대역 방송 서버(101, 102)에 의해 각각 제공되는 VoD 텔레비전 및 IP 방송 서비스를 액세스하고;

[0032] - PC(108 및 111)를 통해 인터넷을, 논리적 접속(2003)을 통해 웹 서버(100)에 의해 제공되는 서비스를 액세스하고;

[0033] - 무선 DECT(Digital Enhanced Cordless Telecommunications)(장치는 도시되지 않음) 전화 세트 상의 IP 전화 서비스, 논리적 접속(2003)을 통해 VoIP 서버(103)에 의해 제공되는 서비스를 액세스하도록 한다.

[0034] 연속 라인(1000, 1001, 1001)은 물리적 접속이다. 점선(2001-2003)은 논리적 접속이다. 점선(2001)은 본 발명에 따른 논리적 라이프라인(lifeline) 접속을 나타낸다. 점선(2002)은 설정 서버(104)와 게이트웨이 CPE 장치(106) 간의 논리적 원격 관리 접속을 나타낸다. 점선(2003)은 하나 이상의 서비스 제공자 서버(100-103)와 게이트웨이(106) 간의 논리적 접속을 나타낸다. 점선은 게이트웨이(106)에서 중심점을 갖는 것으로 도시되지만, 이들 점선은 제공자 서비스 서버(100-103) 및 설정 서버(104)에 CPE 장치(108, 110 및 111) 중의

임의의 것을 접속할 수 있는 것으로 해석되어야 한다.

[0035] 제공자가 설정 또는 소프트웨어 업데이트를 CPE 장치(106, 108, 110, 111) 중의 하나 이상에 보내기를 원할 때, 제공자는 설정 서버(104)에게 수동 개입 없이(즉, 가입자의 지역에서 오퍼레이터의 기술적 서비스가 개입되는 것을 요구하지 않고) 원격 관리 접속(2002)을 이용하여 선택된 CPE 장치(들)를 자동으로 업데이트하거나 재설정하도록 지시한다. 특히, (예를 들어, 증가된 수의 가입자 때문에 추가의 설정 서버가 필요하거나, IP 어드레스의 재분배의 경우에, 즉, 설정 서버 어드레스(들)에 영향을 주는 네트워크 토폴로지 변화의 경우에) 원격 관리 접속(2002)을 이용하여, 설정 서버(104)는 게이트웨이(106)에 저장된 설정 서버의 어드레스를 변경할 수 있다. 그러나, 하나 이상의 가입자의 CPE 장치가 네트워크(105 또는 107)로부터 접속해제될 때 또는 파워 다운되는 경우, 어드레스 업데이트는 이들 장치로 전파될 수 없다. 그 후, 이들 장치의 일부에는 설정 서버에 의한 설정 관리가 도달할 수 없어(즉, 원격 관리 접속(2002)이 "손실"되어) 관련 CPE 장치의 부정확한 거동을 초래할 수 있다. 다른 시나리오에 따르면, 원격 관리 접속(2002)을 통한 설정 관리 세션 동안 CPE로 배포된 소프트웨어 업데이트는 리부팅시 CPE 오퍼레이팅 시스템 크래쉬(crash)를 초래할 수 있고, 이 경우, 관련된 CPE는 확실히 고장나게 되고 설정 관리에 대하여 설정 서버에 의해 도달될 수 없고, 가입자는 더이상 예를 들어 전화 서비스를 포함하는 가입된 서비스를 액세스할 수 없다. 또다른 시나리오에 따르면, 설정 서버에 의해 전송된 잘못된 설정 때문에 가입자의 홈 네트워크 내의 하나 이상의 CPE 장치가 설정 서버에 의해 관리될 수 없게 된다(CPE 장치는 관리 접속을 확립해야 하고, 관리 접속을 셋업하는데 필요한 데이터가 잘못되면, 원격 관리 접속(2002)은 CPE 장치에 의해 셋업될 수 없음을 기억한다). 다른 시나리오에 따르면, TLS(Transport Layer Security) 보안 인증서가 만료되어 CPE 장치가 더이상 설정 서버를 신뢰할 수 없고, 따라서, CPE 장치는 관리 세션 확립을 거절한다. 이들의 모든 시나리오 및 논의되지 않은 다른 시나리오는 이들이 원격 설정 접속(2002)의 손실을 초래하기 때문에 CPE 장치가 설정 관리에 대해 도달될 수 없게 한다.

[0036] 그러므로, 본 발명은 CPE 장치가 ACS에 대하여 관리될 수 없을 때, 즉, 원격 관리 접속(2002)이 손실되었을 때, CPE 장치의 정확한 기능을 복원하도록 하는 라이프라인 접속(2001)을 추가한다. 도 2에서, 라이프라인 접속(2001)은 설정 서버(104)를 게이트웨이(106)에 접속한다. 변형 실시예에 따르면, 라이프라인 접속(2001)은 CS(104)와 다른 장치(미도시)에 접속된다. 이것은 예를 들어 애드혹 장치로부터 게이트웨이(106)를 "트러블슈팅(troubleshoot)"하도록 한다.

[0037] 도 2는 본 발명을 구현하는 장치(104 및 106)에 추가된 추가의 모듈(201, 204, 207)을 나타낸다. 이 모듈은 점선 박스(209)에 의해 도 2에 표시된다. 설정 서버("CS" 또는 "ACS") 측 상에서, 접속 요청 클라이언트(201)가 설정 서버(104)에 추가된다. CPE 측(106, 108, 110 또는 111) 상에서, 접속 요청 서버(204) 및 영구적(persistent) 스토리지 공간(207)이 추가된다. CS(104) 내의 접속 요청 클라이언트(201)는 접속(2001)을 통해 CPE 내의 접속 요청 서버와 통신한다. 서비스 제공자는 자신의 서비스를 접속(2003)을 통해 CPE 장치 중의 임의의 것에 제공한다.

[0038] 설정 관리 세션 동안, CPE 장치(106, 108, 110 또는 111) 내의 HTTP 클라이언트(205)는 원격 관리 접속(2002)을 통해 CS(104) 내의 HTTP 서버(202)와 통신한다. 특정한 실시예에 따르면, HTTP 서버(202) 및 HTTP 클라이언트(205)는 TR-069 프로토콜에 따라 이 접속(2002)을 통해 통신한다. 모듈(200 및 208)은 각각 설정 서버(104) 및 게이트웨이(106)의 정상 기능에 필요한 모듈이다. 이들 모듈은 예를 들어, CPU(Central Processing Unit), 메모리, 방화벽, NAT(Network Address Translation) 모듈 등을 포함한다. 모듈은 각각 설정 서버(104)에 대한 내부 버스(203) 및 장치(106, 108, 110 또는 111)에 대한 내부 버스(206) 등의 내부 통신 수단을 통해 서로 통신한다.

[0039] 접속(2001)은 도 1에서 상술한 비배타적인 통신 실패 시나리오 때문에 손실될 때 원격 관리 통신 링크(2002)를 복원하도록 하는 장치(106, 108, 110 및 111)로의 라이프라인 접속을 구성한다.

[0040] 장치(106, 108, 110 또는 111)의 접속 요청 서버(CRS:Connection Request Server)(204)의 역할은, 서버로서 동작하고 미리 결정된 포트 번호, 예를 들어, TCP 포트 7547 상에서 입력 접속 요청, 즉, HTTP GET 요청을 청취하는 것이다. 이하에서, 이 포트는 "라이프라인 접속 포트"라 한다. CRS는 또한 CPE 설정 크리덴셜 세트, 예를 들어, 공장 디폴트 사용자 이름 및 패스워드를 갖는 요청을 발행하는 엔티티를 인증한다. 본 발명의 변형 실시예에 따르면, 악의적 사용에 대하여 보호할 수 있도록 하는 것 등의 선택적 메카니즘이 CPE에 제공된다. 예시적인 보호 메카니즘은 CPE를 서비스 공격의 거부에 대하여(against) 보호하기 위하여 시간에 걸쳐 수락되는 요청의 수를 제한하도록 하는 접속 요청 스로틀(connection request throttling)이고, 여기서, CPE는 동시에 많은 요청을 서비스할 때 이용불가능하다.

[0041] 장치(106, 108, 110 또는 111)의 HTTP 클라이언트(205)의 역할은 설정 서버(104)의 IP 어드레스를 얻기 위하여 하나 이상의 DNS(Domain Name System) 서버(미도시)로의 DNS 쿼리를 통해 설정 서버의 URL(Unified Resource Locator)를 해결한 후에 원격 설정 접속(2002)을 통해 가능하게는 설정 서버(104)와 통신하는 HTTP 클라이언트로서 동작하는 것이다. CS(104)로의 접속은, 다수의 이벤트 발생시, 예를 들어, CRS가 이러한 이벤트를 HTTP 클라이언트에게 알리는 라이프라인 접속(2001)을 통해 접속 요청이 CRS(204)에 의해 수신될 때마다, 장치(106, 108, 110 또는 111)의 스타트업시, 또는 장치(106, 108, 110 또는 111)의 장치 설정이 변하고 이러한 변화를 가입된 CS(104)에 통지할 때, 확립된다. 변형 실시예에 따르면, CS(104)로의 접속의 확립을 트리거하는 이벤트의 리스트는 TR-069 인폼(Inform) RPC(Remote Procedure Call) 이벤트를 포함한다. 장치(106, 108, 110 또는 111)의 HTTP 클라이언트(205)는 또한 CS(104)를 신뢰하기 위하여 (예를 들어, 영구적 스토리지(207)에 국부적으로 저장된) 다수의 로컬 저장 인증서 중의 임의의 하나로 CS(104)에 의해 제공된 인증서 서명을 유효성 검사하고 HTTP 클라이언트(205)는 CS(104)로부터 수신된 커맨드를 적용하고, 커맨드는 예를 들어 영구적 스토리지(207)에 저장된 장치(106, 108, 110 또는 111)의 특정 설정 파라미터를 변경하는 "SetParameterValues" 또는 "리부팅"을 포함한다.

[0042] 장치(106, 108, 110 또는 111)의 영구적 스토리지(207)의 역할은,

[0043] · CS URL(예를 들어, http://cs.provider.com)를 포함하고,

[0044] · 접속 요청 크리덴셜(사용자 이름 및 패스워드)을 포함하고,

[0045] · CS 제공자 인증서 서명을 유효성 검사하기 위하여 재사용될 수 있는 하나 이상의 로컬 저장 인증서를 포함하고,

[0046] · 펌웨어 이미지 및 다른 제조자 제공 데이터의 신뢰성(authenticity)을 유효성 검사하는데 사용되는 장치(106, 108, 110 또는 111) 제조자의 공개키를 포함하고,

[0047] · 장치(106, 108, 110 또는 111) CPE 장치 설정을 포함한다.

[0048] CS(104)의 접속 요청 클라이언트(CRC:Connection Request Client)(201)는, 예를 들어 특정 시점에 장치(106, 108, 110 또는 111)에 대한 접속 요청 및 인증을 개시하고 원격 설정가능 장치에 의해 관리 세션의 확립을 트리거할 수 있는 HTTP 클라이언트이다.

[0049] CS(104) 내의 HTTP 서버(202)의 역할은 그 중에서도 HTTP 서버를 제공하고 CS의 인증서 서명을 장치(106, 108, 110 또는 111)에 제공하는 것이다.

[0050] 도 2에서, 장치(106, 108, 110 또는 111)는 예시적인 CPE 장치로 간주된다. 그러나, 본 발명은 이러한 타입의 장치에서의 구현에 제한되지 않고, 임의의 타입의 CPE에서 구현될 수 있다.

[0051] 원격 설정 접속(2002)이 손실되면, CPE 장치(106, 108, 110 또는 111)의 CRS(204)는 라이프라인 접속 포트 상에서 청취하도록 구성된다. 특정한 실시예에 따르면, 이러한 메카니즘은 감시(watchdog) 메카니즘에 의해 구현되고, 여기서 본 발명을 구현하는 장치의 다른 모듈 중의 하나는 킵 얼라이브 신호(keep alive signal)를 CRS(204)로 규칙적으로 전송한다. 감시 타이머의 만료 후에 킵 얼라이브 신호가 수신되지 않으면, CRS의 청취 프로세스가 자동으로 시작된다. 다른 실시예에 따르면, 청취 프로세스는 항상 액티브이다. 제1 실시예는 예를 들어 청취 프로세스(및 청취 프로세스를 구현하는데 필요한 모듈)가 계속 파워 온 상태로 유지될 필요는 없기 때문에 본 발명을 구현하는 장치의 전력 소비를 줄일 수 있다.

[0052] CPE의 IP 어드레스는 일반적으로 서비스 오퍼레이터에 의해 알려져 있다. 라이프라인 접속 포트 번호는 예를 들어 TR-069(TCP 포트 7547)에 대한 IANA(Internet Assigned Numbers Authority)에 의해 고정된 디폴트 포트 번호이거나 서비스 제공자와 CPE 장치 제조자 사이에 동의된다. CPE(예를 들어, GW(106))가 라이프라인 접속 포트 상에서 입력 HTTP GET 접속 요청 메시지(즉, 레스큐(rescue) 메시지)를 수신하면, CPE의 CRS(예를 들어, GW(106)의 CRS(204))는 레스큐 메시지를 확인한다. CPE가 원격 설정 장치와 손실된 원격 관리 접속을 재확립하게 하도록 하기 위하여, 레스큐 메시지는 레스큐 정보 및 레스큐 커맨드를 포함한다. 일반적인 레스큐 정보는 예를 들어 제조자 ID, 제품 클래스, 일련 번호를 포함하는 장치 엔티티이고, 이것은 레스큐 커맨드가 단지 예정된 CPE 장치, 유효 ACS URL 등에 의해 고려되는 것을 보장하는 것이다. 일반적인 레스큐 커맨드는,

[0053] - 가능하게는 (CS와의 원격 관리 접속의 손실을 초래하는 임의의 사용자 설정 또는 다른 설정 변화를 하지 않도록(undo)) 공장 디폴트로 복귀하거나;

[0054] - 레스큐 정보 내에 제공되는 새로운 CS URL를 사용하거나;

[0055] - CS 크리덴셜(사용자이름, 패스워드)을 레스큐 정보에 제공되는 크리덴셜로 설정하거나;

[0056] - CS 인증서 체킹을 디스에이블하여 CS를 어떻게든지 신뢰하거나;

[0057] - 사용자 인터페이스, 텔넷(Telnet) 세션 등의 임의의 다른 관리 인터페이스를 개방하여 예를 들어 설정 문제를 트러블슈팅하고 정정하기 위하여 서비스 제공자가 장치를 접속 및 관리하도록 하는 것을 포함한다. 선택적으로, 보안을 증가시키고 라이프라인 접속(2001)을 통한 레스큐 메시지 커맨드의 악의적 전송에 대하여 보호하기 위하여, 레스큐 메시지 내의 정보는 CPE 제조자의 개인키로 서명된 레스큐 메시지 커맨드를 통해 산출된 해쉬(hash) 값을 포함하여, CPE 장치는 인증되지 않은 엔티티에 의해 레스큐 커맨드가 변경되지 않았다는 것을 체크할 수 있다.

[0058] 레스큐 메시지가 CPE에 의해 정확하게 인증되면, CPE는 레스큐 커맨드, 예를 들어, 새로운 펌웨어의 다운로드를 실행한다. 레스큐 커맨드의 적용(application) 후에, CPE는 정확하게 재설정되고 CPE는 원격 관리 접속을 재확립하라는 요청을 CS로 전송한다. 이 요청은 가능하게는 레스큐 메시지 내에 제공되는 정보(즉, 제공된 새로운 ACS URL 또는, 다시 말해, 원격 설정 장치의 어드레스의 사용)에 기초하고 가능하게는 레스큐 메시지 내에 제공되는 정보에 제공된 정보의 적어도 일부(즉, 인증을 위해 유효한 제공된 새로운 접속 요청 크리덴셜의 사용)를 포함하고; 따라서, 요청은 레스큐 메시지에 포함되는 레스큐 커맨드의 상기 원격 관리 장치에 의한 적용 및 레스큐 메시지 내에 제공되는 정보의 원격 설정가능 장치에 의한 사용의 결과이다.

[0059] 변형 실시예에 따르면, CPE 장치는 라이프라인 접속(2001)을 통해 커맨드가 고려되었다는 것을 지시하는 확인 메시지를 CS로 전송함으로써 레스큐 커맨드가 고려되었다는 것을 확인한다. 이 변형은 CPE가 원격 관리 세션을 확립할 준비가 되어 있을 때 설정 서버로 정확한 순간을 시그널링하는 이점을 갖는다.

[0060] 변형 실시예에 따르면, 레스큐 메시지는 CPE에 의해 실행되는 몇 개의 레스큐 커맨드를 포함한다.

[0061] 변형 실시예에 따르면, 몇 개의 레스큐 커맨드를 적용하기 위하여 CS는 라이프라인 접속(2001)을 통해 몇 개의 레스큐 메시지를 전송한다. 선택적으로, 각각의 후속 레스큐 메시지는 이전에 전송된 레스큐 메시지의 CPE에 의한 고려를 확인응답(acknowledge)하는 상술한 확인 메시지를 수신한 후에만 전송된다.

[0062] 다른 변형 실시예에 따르면, 레스큐 메시지(들)를 고려한 후에, CPE는 CS에 접촉할 수 있는지를 확인하여 라이프라인 접속(2001)을 통해 이를 다시 보고한다.

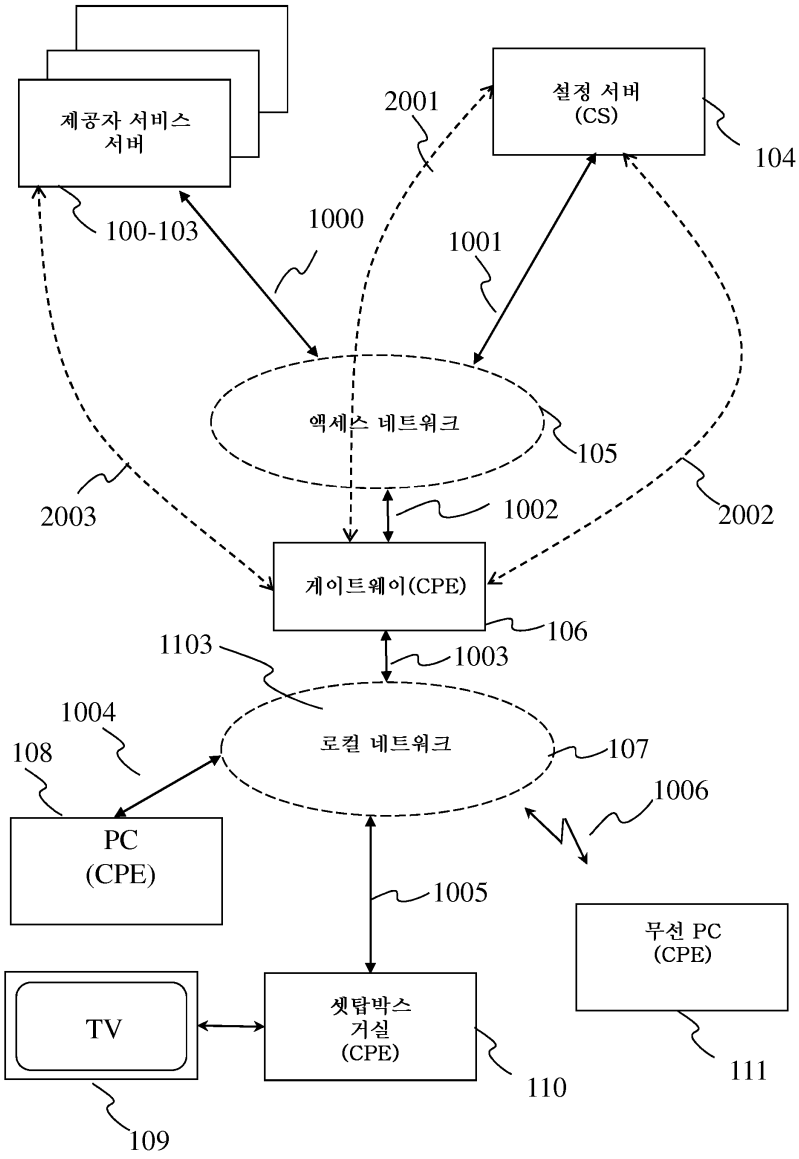
[0063] 변형 실시예에 따르면, 본 발명을 구현하는데 필요한 컴포넌트(접속 요청 서버(204) 및 클라이언트 모듈(205))는 자율적인 방식으로, 즉, 원격 설정가능 장치의 다른 모듈과 독립적으로 기능한다. 이 경우, 본 발명을 구현하는 장치가 "크래쉬"된 경우에도, 즉, 응답을 주지 않는 경우에도, 장치는 라이프라인 접속(2001)을 통해 동작가능한 상태로 복귀하며, 이는 예를 들어 동작가능하지 않고 관리할 수 없는 상태에 있는 장치로 정정된 펌웨어 버전 또는 양호한 설정을 다운로드하도록 한다.

[0064] 변형 실시예가 결합되어 특정한 유리한 실시예를 형성할 수 있다.

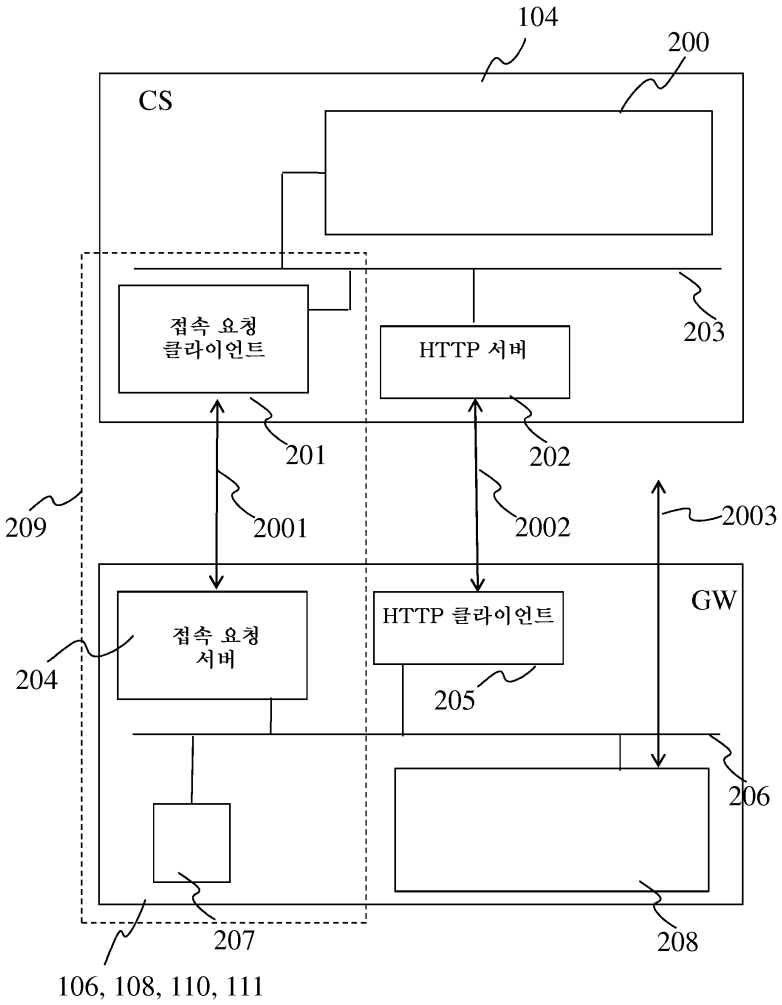
[0065] 특정 실시예에 따르면, 본 발명은 예를 들어 전용 컴포넌트(예를 들어, ASIC(Application Specific Integrated Circuit), FPGA(Field-Programmable Gate Array) 또는 VLSI(Very Large Scale Integration))로서 또는 장치 내에 통합된 개별 전자 컴포넌트로서 하드웨어로 또는 하드웨어 및 소프트웨어의 혼합 형태로 전체적으로 구현된다.

도면

도면1


제공자 서비스
서버
100-103
2001
설정 서버
(CS)
104
1000
1001
액세스 네트워크
105
2003
1002
2002
게이트웨이(CPE)
106
1103
1003
1004
108
로컬 네트워크
107
1006
PC
(CPE)
1005
무선 PC
(CPE)
TV
셋탑박스
거실
(CPE)
110
111
109

도면2


104
200
CS
203
접속 요청
클라이언트
HTTP 서버
201
202
209
2001
2002
2003
GW
접속 요청
서버
HTTP 클라이언트
204
205
206
207
208
106, 108, 110, 111