(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년09월24일
(11) 등록번호 10-2024182
(24) 등록일자 2019년09월17일

(51) 국제특허분류(Int. Cl.)
G06F 9/54 (2018.01)
(21) 출원번호 10-2014-7013290
(22) 출원일자(국제) 2012년11월15일
심사청구일자 2017년11월10일
(85) 번역문제출일자 2014년05월16일
(65) 공개번호 10-2014-0091704
(43) 공개일자 2014년07월22일
(86) 국제출원번호 PCT/EP2012/072694
(87) 국제공개번호 WO 2013/072404
국제공개일자 2013년05월23일
(30) 우선권주장
11447027.1 2011년11월18일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US20060225075 A1
(뒷면에 계속)
전체 청구항 수 : 총 12 항

(73) 특허권자
톰슨 라이센싱
프랑스 35510 세숑-세비네 씨에스 17616 애비뉴 데 샹 블랑 975
(72) 발명자
반 드 폴, 디르크
벨기에 2650 에데겜 프린스 부데비인라안 47 테크니컬러 딜리버리 테크놀로지스 벨기에
괴메레, 패트릭
벨기에 2650 에데겜 프린스 부데비인라안 47 테크니컬러 딜리버리 테크놀로지스 벨기에
용케르, 커트
벨기에 2650 에데겜 프린스 부데비인라안 47 테크니컬러 딜리버리 테크놀로지스 벨기에
(74) 대리인
양영준, 백만기

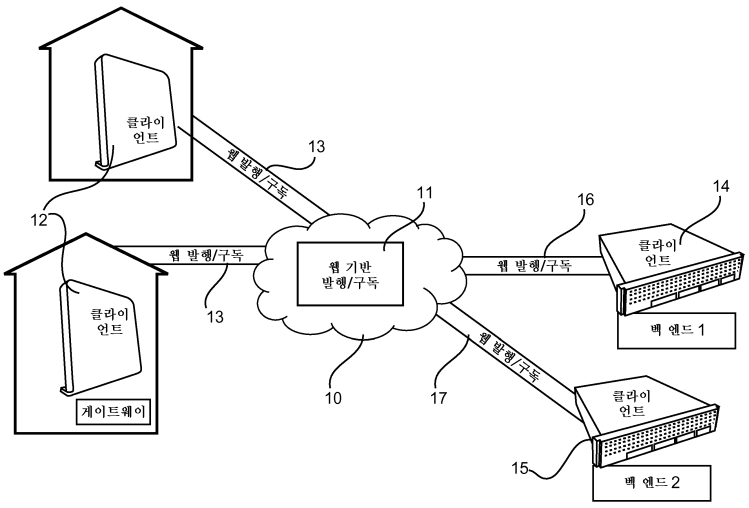
심사관 : 임재우

(54) 발명의 명칭 **엔드-유저 디바이스들의 원격 관리를 위한 발행/구독 브로커를 포함하는 시스템 및 각각의 엔드-유저 디바이스**

(57) 요 약

광대역 접속을 통해 서비스 제공자 네트워크(10)와 연결된 다수의 엔드-유저 디바이스(12), 다수의 엔드-유저 디바이스(12)와 통신하도록 구성된 발행/구독 브로커(11) 및 서비스 제공자 네트워크(10)와 연결된 적어도 하나의 제1 백-엔드 엔티티(14, 15)를 포함하는 시스템이다. 제1 백-엔드 엔티티는 발행/구독 브로커에 접속하기 위한 제1 클라이언트 소프트웨어 애플리케이션을 포함하고 엔드-유저 디바이스들의 디바이스 관리를 위해 제어 데이터 채널을 통해 제어 데이터를 발행한다. 엔드-유저 디바이스들은 발행/구독 브로커에 접속하고, 제어 데이터 채널을 구독하고, 제어 데이터를 수신하고, 제어 데이터의 지시에 따라 디바이스 데이터 및 액션 데이터를 발행하기 위한, 제2 클라이언트 소프트웨어 애플리케이션을 포함한다. 백엔드 엔티티 인증은 특히 제어 데이터 서명을 사용하여 확인된다.

대 표 도 - 도2



(56) 선행기술조사문헌
KR1020070093281 A
KR1020060133696 A
KR100423836 B1*
KR1020110003894 A*
US07650347 B2*
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

광대역 접속을 통해 서비스 제공자 네트워크(10)와 연결된 다수의 엔드-유저 디바이스(12)를 포함하는 시스템으로서,

상기 시스템은 상기 다수의 엔드-유저 디바이스(12)와 통신하도록 구성된 발행/구독 브로커(publish/subscribe broker)(11), 및 상기 서비스 제공자 네트워크(10)와 연결된 적어도 제1 백엔드 엔티티(14, 15)를 더 포함하고, 상기 제1 백엔드 엔티티(14, 15)는, 상기 발행/구독 브로커(11)에 접속하고, 상기 엔드-유저 디바이스들(12)의 디바이스 관리를 위해 제어 데이터 채널을 통해 제어 데이터를 발행하기 위한 제1 클라이언트 소프트웨어 애플리케이션을 포함하고,

상기 엔드-유저 디바이스들(12)은, 상기 제어 데이터 채널을 구독하며 상기 제어 데이터를 수신하기 위해 상기 발행/구독 브로커(11)에 접속하고, 상기 제어 데이터에 의해 지시된 대로 디바이스 데이터 및 액션 데이터를 발행하기 위한 제2 클라이언트 소프트웨어 애플리케이션을 포함하고,

각각의 엔드-유저 디바이스(12)는, 그 디바이스 관리를 위한 실행 명령들을 수신하기 위해 적어도 하나의 제어 데이터 채널을 구독하고, 각각의 엔드-유저 디바이스(12)는 디바이스 데이터 채널을 통해서는 상기 디바이스 데이터를 발행하며 액션 데이터 채널을 통해서는 액션 데이터를 발행하는, 시스템.

청구항 2

제1항에 있어서,

상기 제2 클라이언트 소프트웨어 애플리케이션은 각각의 엔드-유저 디바이스의 스타트업(startup) 시에 각각의 엔드-유저 디바이스(12) 상에서 시작되고, 사전 구성된 URL(uniform resource locator)을 사용함으로써 상기 엔드-유저 디바이스에 대하여 상기 발행/구독 브로커(11)에 대한 접속을 설정하는, 시스템.

청구항 3

제1항 또는 제2항에 있어서,

상기 서비스 제공자 네트워크(10)는 인터넷 서비스들을 제공하기 위한 네트워크 서비스 제공자 네트워크이고, 상기 엔드-유저 디바이스들(12)의 디바이스 관리를 제공하는, 시스템.

청구항 4

제3항에 있어서,

상기 발행/구독 브로커(11)는, 상기 네트워크 서비스 제공자 네트워크를 운영하는 네트워크 서비스 제공자에 의해 제공되는, 시스템.

청구항 5

제1항 또는 제2항에 있어서,

상기 발행/구독 브로커(11)는 인터넷 서비스 제공자에 의해 제공되는, 시스템.

청구항 6

삭제

청구항 7

제1항 또는 제2항에 있어서,

상기 발행/구독 브로커(11)에 접속하기 위한 제3 클라이언트 소프트웨어 애플리케이션을 포함하는 제2 백엔드

엔티티(14)를 포함하고, 상기 제2 백엔드 엔티티(14)는, 상기 다수의 엔드-유저 디바이스(12)의 인벤토리를 유지하기 위해 상기 엔드-유저 디바이스들(12)의 디바이스 데이터, 제어 데이터 및 액션 데이터를 구독하고, 상기 엔드-유저 디바이스들(12)에 대한 제어 데이터를 발행하지는 않는, 시스템.

청구항 8

제7항에 있어서,

상기 제2 백엔드 엔티티(14)는, 상기 엔드-유저 디바이스들(12)의 제조업자 또는 벤더에 의해 제공되는 서버인, 시스템.

청구항 9

제4항에 있어서,

상기 제1 백엔드 엔티티(15)는, 상기 네트워크 서비스 제공자에 의해 제공되는 서버인, 시스템.

청구항 10

제1항 또는 제2항에 있어서,

상기 엔드-유저 디바이스의 관리는, 새로운 펌웨어 또는 미들웨어 버전으로 업그레이드하는 것, 소프트웨어 애플리케이션을 설치, 업데이트 또는 제거(uninstalling)하는 것, 프로그램 또는 스크립트 파일을 실행하는 것, 상기 엔드-유저 디바이스(12)의 구성 또는 상태 데이터에 대한 구조화된 쿼리(structured query)를 실행하는 것, 또는 상기 엔드-유저 디바이스들(12)을 리셋 또는 리부팅하는 것을 포함하는, 시스템.

청구항 11

제1항 또는 제2항에 있어서,

상기 엔드-유저 디바이스들은 제어 데이터 서명을 통해 백엔드 엔티티 인증을 확인하는, 시스템.

청구항 12

제1항 또는 제2항에 따른 시스템과 함께 동작하도록 구성된 엔드-유저 디바이스(12).

청구항 13

제12항에 있어서,

상기 엔드-유저 디바이스(12)는 레지덴셜 게이트웨이, 셋톱 박스, 스마트 폰 또는 셀 폰, 태블릿 PC, 스마트 TV, 또는 임의의 다른 네트워크나 인터넷에 접속된 기기인, 엔드-유저 디바이스(12).

발명의 설명

기 술 분 야

[0001] 본 발명은 엔드-유저 디바이스들(end-user devices)의 분야에 관한 것으로, 특히 서비스 제공자 네트워크와 광대역 접속을 통해 운영하는 고객 구내 장비(customer premises equipment: CPE) 디바이스들과 같은, 인터넷에 접속되어 원격으로 관리되는 엔드-유저 디바이스에 관한 것이다.

배 경 기 술

[0002] 고객 구내 장비(CPE) 디바이스들은 예를 들어 레지덴셜 게이트웨이, 라우터, 스위치, 텔레폰, 셋톱-박스, 등이다. 고객의 홈에서의 디바이스들을 인터넷 또는 임의의 다른 광역 네트워크(wide area network: WAN)에 접속하기 위해 레지덴셜 게이트웨이들이 요즘 널리 사용되고 있다. 레지덴셜 게이트웨이들은 예를 들어 구리 선을 통해 높은 데이터 레이트 전송을 가능하게 하는 DSL(digital subscriber line) 기술을 사용하거나 광대역 전송 시스템들, 예를 들어 FTTH(fiber-to-the-home) 및 FTTP(fiber-to-the premises)를 사용한다.

[0003] 네트워크 서비스 제공자들(Network service providers: NSP), 또한 몇몇 인터넷 서비스 제공자들(Internet service providers: ISP)은, 예를 들어 광대역 인터넷 액세스 또는 IPTV와 같은 그들의 서비스의 일부로서 사용

하는, 수백만 개에 이르는 많은 양의 CPE 디바이스를 관리해야 한다. CPE 디바이스들의 원격 관리는 중앙 설정 서버(central configuration server: CCS)를 이용하여 달성될 수 있는데, 이 중앙 설정 서버는 CPE 디바이스들에게 환경 설정들(configuration settings)을 제공하고 특정한 애플리케이션 레이어 프로토콜(application layer protocol)을 사용하여 진단 정보(diagnostics information)를 추출하기 위해 개별의 CPE 디바이스들과 상호작용한다.

[0004] CPE 원격 관리 통신 프로토콜의 널리 사용되는 예는 CWMP(CPE WAN management protocol)로 알려져 있는데, CWMP는 광대역 포럼(Broadband Forum)에 의해 개발되고, 기술 리포트 번호 069에 의해 정의되고, 또한 보편적으로 TR-069로 일컬어진다. 이 CWMP는 CPE 디바이스들 및 자동 설정 서버(auto configuration server: ACS) 간의 통신 프로토콜을 제공함으로써, CPE 디바이스들의 원격 관리를 위한 애플리케이션 레이어 프로토콜을 정의한다.

[0005] 도 1에서, CPE 디바이스들에 광대역 서비스들을 제공하는 이런 종류의 광역 네트워크가 개략적으로 도시된다: 다수의 레지덴셜 게이트웨이(2) 및 셋-톱 박스(3)에 광대역 접속(5)[예를 들어 DSL/케이블/섬유들(fibers) 등]을 통해 인터넷 서비스들을 제공하기 위해, 네트워크 서비스 제공자 네트워크(1)는 마련된다. 또한, 레지덴셜 게이트웨이들(2) 및 셋-톱 박스들(3)을 원격으로 관리하기 위해 NSP 네트워크(1)는 ACS(4)를 포함한다. TR-069 프로토콜을 사용함으로써, ACS(4)는 예를 들어 자동 설정 및 동적 서비스 프로비저닝(dynamic service provisioning), 소프트웨어/펌웨어 이미지 관리, 상태(status) 및 성능 모니터링(monitoring), 그리고 레지덴셜 게이트웨이들(2) 및 셋-톱 박스들(3)에 대한 진단을 할 수 있다.

[0006] CWMP, 또한 예를 들어 OMA 디바이스 관리(OMA Device Management)나 웹 서비스 기반 프로토콜들(web service based protocols)과 같은 다른 포로토콜들도, "전통적인" 클라이언트/서버(client/server) 및 요청/응답(request/response) 모델을 포함한다. 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol: HTTP) 클라이언트로서 행동하는 디바이스는 하나 또는 HTTP 서버들의 클러스터(cluster)에 접속하고 HTTP 요청을 전송하고, 서버 또는 클러스터는 HTTP 응답에 응답한다. CWMP는 웹(HTML) 페이지들을 제공하는 월드 와이드 웹(World Wide Web)과 동일한 원칙들(principles)을 상응하게 적용한다.

[0007] 최근에, http://www.w3.org/TR/html5/를 보면, 다가오는 HTML5 표준의 범위에 진화가 있었고, W3C가 기여한 "http://tools.ietf.org/html/draft-ietf-hybi-thewebsocketprotocol-17"의 정의 하에 있는 새로운 웹 소켓들 프로토콜(web sockets protocol)이 있다. 웹 소켓들은 전 이중(full deplex), 웹 소켓 클라이언트 및 서버 간의 양방향(bidirectional) 통신을 지원하는데, 클라이언트들에 데이터를 전송하는 서버에 대한 중간(intermediate) 비표준의 메커니즘들(mechanisms)이 있음에도 불구하고, 전통적인 요청/응답 모델을 넘어서고, 예들은 http://svn.cometd.com/trunk/bayeux/bayeux.html, http long poll 등의 코멧(comet)을 포함한다.

[0008] 로직(logic) 및 HTTP 요청/응답 모델과 관련된 모든 관리를 포함하는 완전히 중앙집중된 서버(centralized server)는 다수의 중요한 제약 및 문제가 있다:

[0009] - 수백만 개의 디바이스가 (요청들을 전송하는) 서버 및 헬프데스크들(helpdesks)에 주기적으로 접속하고 다른 엔티티들(entities)이 (모니터링, 진단 등의) 다수의 애플리케이션에 대한 서버를 통과할 필요가 있으면, 확장성(Scalability)은 중앙집중된 서버 모델에서의 문제점(challenge)이 된다.

[0010] - ACS 또는 다른 백엔드(backend) 애플리케이션으로부터 특정 디바이스로의 가능한 한 빠른 통신은 문제가 있다. 예를 들어, TR-069는 접속 요청 메커니즘(connection request mechanism)을 정의하는데, 이 메커니즘에서 ACS는 HTTP 요청을 CPE로 전송하고, 전형적으로 HTTP 다이제스트 인증(HTTP digest authentication)을 사용하여 인증하고, 그 이후에 CPE 디바이스가 HTTP 요청들을 전송하는 ACS에 접속한다.

[0011] - 많은 수의 CPE 디바이스의 호출(interrogation)은 중앙 서버가 각각에 접촉하고, 데이터를 수집하고 서버 측에서 이런 수집된 데이터를 분석하기 위해 요청/응답 반복들(iterations)을 개별적으로 통과할 것을 필요로 한다.

[0012] - 모든 로직은 하나의 장소에 중앙집중되어 있고, 하나의 장소의 예로서 ACS 서버는 이하를 의미한다:

[0013] ○ ACS 서버는 잠재적으로 느린 네트워크 접속을 거쳐 디바이스들에 명령들(commands)을 발행할 필요가 있다.

[0014] ○ ACS 서버는 CPE 디바이스로부터 (성공/실패 및 가능한 한 요청된 데이터의) 응답을 기다리고, 이 결과를 분석하고 이에 기초하여 취해야 할 다음 단계를 결정한다.

[0015] ○ 각 개별의 CPE 디바이스에 대해, 매우 많은 수의 CPE 디바이스에 대해 일반적으로 공통되는, 이 로직을 수행한다.

[0016] US 2010/0235433 A1은 다양한 유저 구내에서 게이트웨이 디바이스들을 갖는 광역 네트워크를 통해 통신하는 서비스 관리 시스템을 설명하는데, 이는 게이트웨이 디바이스들에 관련된 가입자들의 서비스 구독들에 기반을 둔 게이트웨이 디바이스에 의해 애플리케이션 서비스들의 제공(delivery) 및/또는 기능들(features)을 원격으로 관리한다. 구독 관리자(subscription manager)는 활성화할 수 있는 애플리케이션 서비스들 및 기능들을 식별하는 WAN을 통해, 각각의 게이트웨이 디바이스에 정보를 제공한다. 구독 관리자에 의해 제어되는 서비스 관리자(service manager)는 게이트웨이 디바이스들에서 애플리케이션 서비스들에 대한 서비스 기능성(functionality)을 구현하는 로직에, 서비스 특정한 설정 데이터를 분배하고, 게이트웨이 디바이스들로부터의 요청들에 반응한다.

[0017] 기술 보고서 SSC/1998/022, 스위스, 로잔, Jean-Philippe Martin-Flatin에 의한 간행물인 "Push vs. Pull in WEB-Based Network Management"는 네트워크 관리 애플리케이션 디자인들을 설명한다. 첫 번째인, 풀(pull) 모델은 요청/응답 패러다임(paradigm)에 기반을 두고 있다. 두 번째인, 푸시(push) 모델은 발행/구독 패러다임에 의존하는데, 이 패러다임은 관리자들이 관리 스테이션 상의 CPU 시간뿐만 아니라 네트워크 대역폭을 보존하도록 한다. 세 번째 모델은, 위 두 개의 모델이 공존하는, 붕괴된 네트워크 관리 플랫폼의 개념을 소개한다.

발명의 내용

[0018] 시스템은 광대역 접속을 통해 서비스 제공자 네트워크와 연결된 다수의 엔드-유저 디바이스, 상기 다수의 엔드-유저 디바이스와 통신하도록 구성된 발행/구독 브로커 및 상기 서비스 제공자 네트워크와 연결된 적어도 하나의 제1 백-엔드 엔티티를 포함한다. 상기 제1 백-엔드 엔티티는 상기 발행/구독 브로커에 접속하기 위한 제1 클라이언트 소프트웨어 애플리케이션을 포함하고 상기 엔드-유저 디바이스들의 디바이스 관리를 위해 제어 데이터 채널을 통해 제어 데이터를 발행한다. 상기 엔드-유저 디바이스들 각각은 상기 발행/구독 브로커에 접속하고, 상기 제어 데이터 채널을 구독하고, 상기 제어 데이터를 수신하고, 상기 제어 데이터에 의해 지시된 대로 디바이스 데이터 및 액션 데이터를 발행하기 위한, 제2 클라이언트 소프트웨어 애플리케이션을 포함한다. 상기 백엔드 엔티티 인증은 특히 제어 데이터 서명을 사용하여 확인된다.

[0019] 바람직한 실시예에서, 상기 서비스 제공자 네트워크는 인터넷 서비스들을 제공하는 네트워크(예를 들어 네트워크 서비스 제공자 네트워크)이고, 상기 엔드-유저 디바이스들의 상기 디바이스 관리를 제공하고, 상기 발행/구독 브로커는 상기 네트워크 서비스 제공자 네트워크를 운영하는 상기 서비스 제공자에 의해서도 제공받는다. 각각의 엔드-유저 디바이스는 그 디바이스 관리를 위한 관리 명령들을 수신하기 위해 특히 적어도 하나의 제어 데이터 채널을 구독하고, 각각의 엔드-유저 디바이스는 디바이스 데이터 채널을 통해 그 디바이스 데이터를 발행하고 액션 데이터 채널을 통해 액션 데이터를 발행한다.

[0020] 본 발명의 다른 측면에서, 상기 시스템은 상기 발행/구독 브로커에 접속하기 위한 제3 클라이언트 소프트웨어 애플리케이션을 갖는 제2 백엔드 엔티티를 포함하는데, 상기 제2 백엔드 엔티티는 상기 다수의 엔드-유저 디바이스의 인벤토리를 유지하기 위해 상기 엔드-유저 디바이스들의 디바이스 데이터, 제어 데이터 및 액션 데이터를 구독하지만, 상기 엔드-유저 디바이스들을 위해 제어 데이터를 발행하지 않는다. 상기 제2 백-엔드 엔티티는 예를 들어 상기 엔드-유저 디바이스들의 제조업자에 의해 제공되는 서버이고, 상기 제1 백-엔드 엔티티는 상기 네트워크 서비스 제공자에 의해 제공되는 서버이다.

[0021] 상기 디바이스 관리는 특히 새로운 펌웨어 또는 미들웨어 버전으로 업그레이드, 설치, 소프트웨어 애플리케이션의 업데이트 또는 제거, 프로그램 또는 스크립트 파일의 실행, 상기 엔드-유저 디바이스 설정 상의 또는 상태 데이터 상의 구조화된 쿼리, 상기 엔드-유저 디바이스가 발행할 필요가 있는 데이터에 관한 정책의 제공, 또는 상기 엔드-유저 디바이스들의 리세팅 또는 리부팅을 포함한다.

[0022] 상기 시스템을 운영하도록 구성된 엔드-유저 디바이스들은 특히 CPE 디바이스들, 예를 들어 레지덴셜 게이트웨이, 셋-톱 박스, 스마트 폰, 셀 폰, 태블릿 PC, 스마트 TV 및 원격으로 관리되는 다른 네트워크에 또는 인터넷에 접속된 기기이다.

도면의 간단한 설명

[0023] 본 발명의 바람직한 실시예들은 이하에서 예로서 개략적 도면들을 참조하여 더욱 상세히 설명된다.

도 1은 CPE 디바이스들 및 인터넷 서비스들을 제공하기 위한 네트워크 서비스들 제공자 네트워크를 포함하는 종래 기술에 따른 광역 네트워크를 도시하는 도면.

도 2는 다수의 엔드-유저 디바이스, 발행/구독 브로커, 및 두 개의 백-엔드 엔티티를 포함하는 본 발명에 따른 시스템을 도시하는 도면.

도 3은 도 2의 시스템의 바람직한 실시예를 도시하는 도면.

도 4는 도 2 및 도 3에서 도시된 백엔드 엔티티의 실행 액션을 수행하는 방법을 도시하는 도면.

도 5는 도 3에 도시된 시스템의 예시적인 운영을 설명하는 방법을 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0024] 이하의 설명에서, 광대역 접속을 통해 서비스 제공자 네트워크와 연결된 다수의 엔드-유저 디바이스를 포함하는 시스템이 설명된다. 설명의 목적으로, 바람직한 실시예들의 철저한 이해를 위해, 많은 구체적인 세부사항들이 기재된다. 그러나, 이러한 구체적인 세부사항들 없이 본 발명이 실시될 수 있다는 것은 당해 기술분야의 통상의 기술자에게 명백할 것이다.

[0025] 엔드-유저 디바이스들은 특히 CPE 디바이스들, 예를 들어 레지덴셜 게이트웨이, 라우터, 스위치, 텔레폰, 셋톱-박스, 및 임의의 다른 네트워크 또는 인터넷에 접속된 기기이고, 이는 각각이 마이크로프로세서, 운영 체제와 애플리케이션들이 저장되어 있는 비-휘발성 메모리(non-volatile memory), 및 CPE 디바이스의 운영을 위한 휘발성 메모리(volatile memory)를 포함한다. CPE 디바이스의 운영 체제는 예를 들어 리눅스 운영 체제 및 디바이스 실행 환경을 나타내는 CPE 디바이스-특화 미들웨어(CPE device-specific middleware)이다. 디바이스 실행 환경은 예를 들어 DSL 모뎀 기능, 게이트웨이 및 스위칭 기능, FXS 기능, VoIP 기능성 및 Wi-Fi 운영을 제공하는 소프트웨어 구성요소들을 포함한다.

[0026] 도 2에 도시된 바람직한 실시예에서, 본 발명에 따른 시스템은, 각각 광대역 접속(13)을 통해 서비스 제공자 네트워크(10), 특히 네트워크 서비스 제공자(NSP) 네트워크와 연결된 다수의 CPE 디바이스(12), 및 다수의 CPE 디바이스(12)와 통신하도록 구성된 발행/구독 브로커(11)를 포함한다. 시스템은 광대역 접속(16)을 통해 서비스 제공자 네트워크와 연결된 적어도 하나의 제1 백-엔드 엔티티(14)를 더 포함하고, CPE 디바이스들(12)의 원격 CPE 디바이스 관리를 위해 백-엔드 엔티티(14)는 발행/구독 브로커(11)에 접속하기 위한 클라이언트 소프트웨어 애플리케이션을 포함한다. 발행/구독 브로커(11)는 예를 들어 NSP 네트워크(10)의 일부이거나 인터넷 서비스 제공자에 의해 제공받을 수 있고, CPE 디바이스들(12)의 원격 CPE 디바이스 관리를 위해 특히 CPE 디바이스들(12)에 대한 통신 및 제어 서비스들을 관리한다. 발행/구독 브로커(11)는 NSP 네트워크(10) 또는 인터넷 서비스 제공자 네트워크 외부의 데이터센터에 위치한 클라우드 플랫폼 상에 호스팅될(hosted) 수도 있다. CPE 디바이스(12)는 발행/구독 브로커(11)에 접속하기 위한 클라이언트 소프트웨어 애플리케이션도 포함하고, 따라서 발행/구독 브로커(11) 및 백-엔드 엔티티(14)의 "관리 아래" 있는 디바이스이다. CPE 디바이스들(12)은 하나 또는 여러 특정한 토픽들(topics), 예를 들어 하나 또는 여러 제어 채널들을 구독하고, 하나 또는 여러 특정한 토픽들, 예를 들어 데이터 채널들 상의 데이터를 발행한다.

[0027] 또한, CPE 디바이스들(12)의 CPE 디바이스 관리를 제공하고 지원하기 위해, 광대역 접속(17)을 통해 발행/구독 브로커(11)와 접속된 어떤 추가적인 백-엔드 엔티티(15)는 발행/구독 브로커(11)에 접속하기 위한 클라이언트 소프트웨어 애플리케이션을 포함한다. 특정한 애플리케이션 또는 용도(use-case)에 따라, 백-엔드 엔티티들(14 및/또는 15)은 특정한 토픽들, 예를 들어 제어 채널들 상의 제어 데이터를 발행하고, 특정한 토픽들, 예를 들어 데이터 채널들을 구독한다.

[0028] 백-엔드 엔티티들(14 및 15)은 상이한 기술들, 예를 들어 상이한 소프트웨어 프로그래밍 언어로 구현될 수 있고, 동일한 서버 또는 상이한 서버들 및 장소들, 예를 들어 인터넷 접속되는 세계의 어느 장소라도 위치할 수 있다. 다른 디바이스들과 유사하게, 그들은 발행/구독 브로커(11)를 통해 인터넷으로 통신한다. 본 발명은 특히 어떤 장소에 상주하는(residing) 하나, 두 개 또는 어떤 수의 백-엔드 엔티티를 지원한다.

[0029] 발행/구독 시스템에서, 발행자들은 중간 메시지 브로커인 발행/구독 브로커(11)에 메시지를 발송(post)하고, 구독자는 그 브로커에 구독들을 등록하고, 브로커는 발행된 메시지들의 포워딩(forwarding) 및 필터링(filtering)을 수행한다. 가능한 한 효율적인 방법으로 발행자들로부터 구독자들로 메시지들을 라우팅하기(route) 위해, 브로커는 일반적으로 저장 및 포워딩 기능을 수행하는 것에 최적화되어 있다. 메시지 브로커의 예는 http://en.wikipedia.org/wiki/message_broker에서 설명된다. 발행/구독 메커니즘은 느슨하게 연결된(loosely

coupled) 엔티티들 간의 일-대-일, 일-대-다, 및 다-대-다 통신을 가능하게 한다. 본 발명의 맥락에서 느슨하게 연결된 것은 엔티티들이 서로의 존재 및 위치에 대해 알 필요가 없다는 것을 의미한다. 브로커는 각각의 클라이언트인, CPE 디바이스 또는 백엔드 엔티티를 인증하고, 일정한 채널들 상에 메시지들이 발행됨에 따라 어느 백엔드 엔티티가 어느 메시지들을 구독하고 수신하는지에 관한 인증 제약들을 부과할 것이다.

[0030] 발행/구독 메커니즘은 예를 들어 OMG(object management group)가 제공하는 데이터 분배 서비스(data distribution service: DDS)에 의해서도 사용되는데, OMG는 확장가능한(scalable) 실-시간의 높은 성능 및 발행자들과 구독자들 간의 상호동작이 가능한(inter-operable) 데이터 확장들을 할 수 있게 한다. 다른 예는 IBM에 의해 발행되어 공개된 프로토콜 규격인, MQTT(Message Queue Telemetry Transport) 프로토콜이다. 본 발명은 하나의 특정한 발행/구독 기술에 의존하지 않는다.

[0031] 발행/구독 브로커(11)를 사용함으로써, 발행/구독 브로커(11)에 접속하기 위한 클라이언트 소프트웨어 애플리케이션을 각각 포함하는 여러 또는 심지어 어떤 수의 백엔드 엔티티(14, 15)는 CPE 디바이스(12)의 관리에 사용될 수 있다. 이 솔루션은 TR-069 CWMP 또는 OMA DM 프로토콜들과 같은 현재 기준 표준들(reference standards)보다 특히 더 확장가능하고 더 비용 효율이 높다. 발행/구독 브로커(11)는, 예를 들어 웹 애플리케이션들에 실-시간 양방향의 기능성을 빠르고, 쉽고, 안전하게 추가한 단순 호스팅된(hosted) API인 Pusher(http://pusher.com), Beaconpush(http://beaconpush.com), PubNub(http://www.pubnub.com), MQTT 브로커 또는 극대규모(Ultra large scale)의 DDS(http://www.omg.org/news/meetings/GOV-WS/pr/rte-pres/ultra-large-scale-dds.pdf)와 유사한 서비스를 사용할 수 있다.

[0032] 시스템은 다음과 같이 운영한다:

[0033] 1. 제1 단계에서, 각각의 CPE 디바이스(12)는 웹 기반의 발행/구독 인프라스트럭처인 발행/구독 브로커(11)에 접속한다(웹 기반은 브로커가 인터넷을 통해 도달가능하다는 것을 의미함):

[0034] a. (선)구성된 URL(uniform resource locator)을 사용함으로써, CPE 디바이스(12)가 스타트업(startup)할 때 각각의 CPE 디바이스(12) 상에서 실행되는 클라이언트 소프트웨어 애플리케이션은, 예를 들어 TCP인, 발행/구독 프로토콜을 통해, 발행/구독 브로커(11)에 접속을 설정한다. 클라이언트 소프트웨어 애플리케이션은 인증하고 발행/구독 브로커가 클라이언트 아이덴티티(identity)를 확인하도록 하는 TLS(Transport Layer Security) 인증서를 제공해야 할 수 있다.

[0035] b. CPE 디바이스(12)는 선구성된 채널/토픽(예를 들어 디바이스 데이터 채널) 상의 그 디바이스 데이터를 발행할 수 있다.

[0036] i. 디바이스 데이터는 특히 시리얼 넘버(serial number), 하드웨어 버전, 소프트웨어 버전, 현재 공용 (인터넷) IP 주소, 등등을 포함한다.

[0037] ii. 어떤 백엔드 엔티티(14, 15)는 디바이스 데이터를 구독할 수 있고, 이는 예를 들어 CPE 디바이스와 함께 접속되는 그들의 디바이스 데이터를 함께 저장하는 백엔드 디바이스 인벤토리 애플리케이션을 포함하는 백엔드 엔티티이다.

[0038] iii. 특정한 이벤트들이 발생할 때, 예를 들어 스타트업 할 때, 또는 소프트웨어 버전 또는 IP 주소의 어떤 변화가 있을 때, 각각의 CPE 디바이스(12)에 의해 디바이스 데이터는 주기적으로 발행될 수 있다.

[0039] c. CPE 디바이스들(12)은 하나 이상의 제어 채널 또는 토픽을 더 구독할 수 있다.

[0040] i. CPE 디바이스들이 구독하는 채널들/토픽들은 선구성되어, 이전에 수신된 제어 데이터에 의해 결정되거나 다른 기준(criteria)에 의해 결정된다.

[0041] 1. 채널 구독은, 가능하게는 특정한 지역 내의 또는 특정의 서비스들에 구독되는 특정한 NSP의 가입자들을 제어 데이터가 대상으로 할 수 있도록, 지역의 NSP 마다, 구독자 그룹마다 일 수 있다.

[0042] 2. 채널 구독은 시간에 따라 변할 수 있고, 예를 들어 주어진 CPE 제품 (하드웨어 버전) 및 소프트웨어 버전을 갖는 NSP 가입자들은 업그레이드를 지시하는 제어 데이터에 대한 특정한 채널/토픽을 구독할 수 있다. 예를 들어 이 채널 상에 발행된 제어 데이터가 CPE 디바이스들(12)을 새로운 펌웨어/소프트웨어 버전으로 대량으로 업그레이드하도록, 레지덴셜 게이트웨이 또는 셋-톱 박스 디바이스들은 <NSP-HW-SW> 채널을 구독할 수 있다. 업그레이드 이후에, 각각의 CPE 디바이스(12)는 새로운 업그레이드 제어 데이터를 듣는(listening) <NSP-HW-SW2> 채널을 구독할 수 있다.

[0043] 3. 선택적인 채널/토픽 구독들을 사용하여, 발행된 데이터가 특정한 CPE 디바이스들(12)의 세트를 대상으로 하도록, CPE 디바이스들(12)의 큰 세트는 특정한 원격 관리 애플리케이션들로 분할될(partitioned) 수 있다.

[0044] ii. 설정가능한 정책을 기반으로 한 특정한 채널/토픽을 구독하기 위해 발행/구독 브로커는 CPE 디바이스들(12)을 거절할 수 있다.

[0045] 2. 백엔드 엔티티(14 및/또는 15)는 특정한 제어 채널 또는 토픽 상에 컨트롤 데이터를 발행한다:

[0046] a. 하나 이상의 백엔드 엔티티(14, 15)는 특정한 제어 채널/토픽 상에 제어 데이터를 발행할 수 있다. 전통적인 중앙집중된 CWMP 서버들과 달리, 발행/구독 메커니즘은 느슨하게 연결된 일-대-일, 일-대-다, 및 다-대-다 통신을 가능하게 한다. 분리된 백엔드 엔티티들(14, 15)을 가짐으로써, 예를 들어 확장성을 우회하여, 중앙의 병목현상들(bottlenecks)이 필요하지 않을 수 있다.

[0047] b. 제어 데이터가 발행될 수 있도록, 각각의 백엔드 엔티티(14, 15)는 웹 발행/구독 인프라스트럭처인 발행/구독 브로커(11)를 인증할 필요가 있을 수 있다.

[0048] c. 제어 데이터는 예를 들어 이하의 상이한 데이터 필드들(fields)을 포함하지만, 그에 제한되지 않는다:

[0049] i. CPE 디바이스들을 대상으로 설정: 제어 액션을 적용할 필요가 있는 구독 중인 CPE 디바이스들의 선택적인 제한. 이 제한은 CPE 디바이스 특징들(예를 들어 HW/SW 버전, IP 주소 범위, 시리얼 넘버 범위 등) 또는 구독자 특징들[예를 들어 ppp 자격증(credentials), VoIP 텔레폰 번호 (범위), 액티브 서비스들 등]의 세트 형태로 표현될 수 있다.

[0050] ii. 액션: CPE 디바이스들(12)에 의해 수행될 액션. 액션들의 예는 이하에서 포함되지만, 그에 제한되지 않는다:

[0051] 1. 펌웨어 업그레이드

[0052] 2. 애플리케이션 설치/업데이트/제거

[0053] 3. 프로그램 또는 스크립트 파일을 실행

[0054] 4. 발행: 디바이스 또는 데이터 채널 또는 토픽 상의 CPE 디바이스 데이터 또는 고정된 데이터를 무조건적으로 발행

[0055] 5. 쿼리(query): CPE 설정 데이터 또는 상태 데이터 상의 구조화된 쿼리를 제공(쿼리는 결과들을 가질 때만, CPE 디바이스에 의해 발행될 것임)

[0056] 6. 리부팅(reboot)

[0057] iii. URL: 파일을 지칭하는 선택적 URL. 이는 특정한 액션들(예를 들어 펌웨어 업그레이드)에 대해서만 적용할 수 있고, URL은 액션으로서 실행을 위해 다운로딩하고 적용할 펌웨어 이미지를 가리키고, URL은 다운로딩하고 실행할 소프트웨어 프로그램 또는 스크립트 파일을 가리킨다.

[0058] iv. 데이터 채널: 액션의 결과를 발행하는 곳의 채널/토픽 이름. 예를 들어, JSON(JavaScript Object Notation) 인코딩된(encoded) 데이터를 갖는 이 URL에 대한 HTTP POST와 같은, 전통적인 http 요청/응답 웹 서비스들을 사용하는, 액션의 결과 데이터를 발행하는 곳에 대한 URL이 선택적으로 될 수 있다.

[0059] v. 기준에 관련된 타이밍(Timing): 선택적인 타이밍 제약들의 예가 이하에서 포함되지만, 그에 제한되지 않는다:

[0060] 1. 반복적으로 수행하는 액션들 간의 간격(예를 들어 모니터링의 이유들로 스크립트의 주기적인 실행에 대한 간격), 0의 값은 액션이 한번뿐이고 비-반복적이라는 것을 나타낸다.

[0061] 2. 액션을 수행하기 전의 상대적인 딜레이(예를 들어 고정된 또는 랜덤 범위의 딜레이)

[0062] 3. 액션을 수행하는 절대적 시간 범위(예를 들어 동일한 날의 오전 2시 및 오전 4시 사이)

[0063] vi. 보안 서명(Security signature): 가능한 다수의 백엔드 엔티티(14 및 15)에 관한 분배된 접근에서 필요한 보안의 레벨을 제공하기 위해, 메시지의 서명은, 본 발명의 키 요소(key element)이다. 백엔드 엔티티 디지털 인증서(예를 들어 X.509)에 대한 허용된 기능성을 포함하는 확장 필드들(extension fields)을 추가하고 그 자신의 인증서에 서명함으로써, 중앙 관리자(central authority)는 백엔드 엔티티들에 일정한 관리 기능성을 수행하는 권한을 수여할 것이다. 클라이언트 디바이스들은 중앙 관리자들 그 자신의 인증서의 공개 키(public key)를 포함하고, 각각 수신된 메시지에 대해 메시지에 서명한 인증서가 적절한 관리 권한을 가지는지 및 중앙 관리자에 의해 서명되었는지를 확인한다.

[0064] 3. 발행/구독 브로커(11)를 구독하고 어떤 백엔드 엔티티들(14, 15)로부터 제어 데이터를 수신하는 각각의 CPE 디바이스(12)는 요청된 액션을 수행한다:

[0065] a. 제1 단계는 제어 데이터의 원점(origin), 진정성(authenticity) 및 완전성(integrity)을 확인한다:

[0066] i. 제어 데이터는 제어 데이터 메시지를 통해 해시(hash)로 암호화된 비대칭 키(예를 들어 서명)를 포함할 수 있다.

[0067] ii. (백엔드 엔티티에 대응하는) 메시지에 서명하는데 사용되는 인증 개인 키는 그 확장 필드들 내의 적절한 관리 권한들을 포함하고, CPE 디바이스들(12) 상에 저장된 중앙 관리자의 사전-프로비저닝된(pre-provisioned) 공개 키를 사용하여 확인된다.

[0068] b. 제2 단계는 CPE 디바이스(12)가 실제로 액션을 수행해야 하는지를 평가하기 위한 선택적인 목표 CPE 디바이스 제약들을 확인하는 것이다. CPE 디바이스(12)가 목표 제약들에 충족될(covered) 수 없다면, 추가 액션 없이 제어 데이터 메시지는 폐기된다.

[0069] c. 액션은 선택적 제어 데이터 필드들의 일부가 중요한지 아닌지를 결정한다. CPE 디바이스(12)는 예를 들어 이하에서 타이밍 제한들을 고려하는 액션을 수행하지만, 이에 제한되지 않는다:

[0070] 1. 펌웨어 업그레이드: URL(URL은 schema로서 사용될 프로토콜을 포함함)위치에서 펌웨어 이미지를 다운로딩하고, 디바이스를 리부팅한 다음 펌웨어를 급송/적용한다(flash/apply).

[0071] 2. 애플리케이션 설치/업데이트/제거: 디바이스 상의 특정한 애플리케이션을 설치 또는 제거하기 위해, 예를 들어 file:// schema의 URL에 의해 식별되는 애플리케이션 바이너리(application binary)를 다운로딩한다.

[0072] 3. 프로그램 또는 스크립트 파일을 실행: URL 위치에서 프로그램 또는 스크립트 파일을 다운로딩하고, 프로그램 또는 스크립트 파일을 실행한다.

[0073] 4. 발행: 디바이스 데이터 채널 또는 토픽 상의 CPE 디바이스 데이터 또는 고정된 데이터를 무조건적으로 발행한다.

[0074] 5. 쿼리: CPE 디바이스 설정 상의 구조화된 쿼리 또는 CPE 디바이스들(12)의 상태 데이터(쿼리가 결과들을 가질 때만, CPE 디바이스들에 의해 발행될 것임).

[0075] 6. 리부팅: CPE 디바이스들(12)의 웜(warm) 리세팅(reset) 또는 리스타팅(restart).

[0076] 4. CPE 디바이스들(12)은 액션 데이터 채널 또는 토픽 상의 액션의 결과들을 발행할 수 있다:

[0077] a. 데이터는 예를 들어 이하에서 특정한 액션에 의존하지만, 이에 제한되지 않는다:

[0078] 1. 펌웨어 업그레이드: 결과 데이터는 실패 장애 코드(failure fault code)일 수 있다. 성공의 경우, 디바이스는 디바이스 데이터를 재발행할 수 있다(단계 1.b 참조).

[0079] 2. 애플리케이션 설치/업데이트/제거: 결과 데이터는 성공 또는 실패 표시들(indications)일 수 있다.

[0080] 3. 프로그램 또는 스크립트 파일을 실행: 결과 데이터는 프로그램 또는 스크립트 실행의 결과의 어떤 데이터일 수 있다. 그것은 예를 들어 모니터링 데이터, 진단 결과 코드들, 특정한 쿼리들의 결과들, 집계된 데이터 등일 수 있다.

[0081] 4. 발행: CPE 디바이스 데이터 또는 고정된 데이터

[0082] 5. 쿼리: 쿼리는 결과를 가지거나 가지지 못할 수 있고, 결과 데이터는 실제 쿼리에 의존하고,

이는 예를 들어 CPE 설정 데이터 및/또는 상태 데이터(예를 들어 광대역 포럼 TR-181i2 데이터 모델과 같은 표준 게이트웨이 데이터 모델을 참조하는 데이터)에 대하여 수행될 수 있다.

[0083] 6. 리부팅: 존재하지 않는 결과 데이터, 예를 들어 리부팅 이후에, CPE는 그 디바이스 데이터를 재발행할 수 있다.

[0084] b. 데이터를 발행하기 위한 데이터 채널 또는 토픽은 액션을 유발하는 초기 제어 데이터에 의해 결정된다:

[0085] i. 데이터 채널 또는 토픽은 각각의 액션에 대해 상이할 수 있고, 이것은 완전히 제어 데이터를 관리하는 백엔드 관리자에 의해 결정된다.

[0086] ii. 하나 이상의 백엔드 엔티티(14, 15)는 액션 데이터 채널들 또는 토픽들에 관심을 가질 수 있거나 구독할 수 있다.

[0087] 5. CPE 디바이스들(12)이 수행할 새로운 액션을 구독하는 제어 채널 또는 토픽 상에서, CPE 디바이스들(12)은 새로운 제어 데이터를 수신할 수 있다.

[0088] 도 3에, 본 시스템의 더 상세한 실시예가 도시되어 있다. 이 시스템은 다수의 CPE 디바이스(12 및 18)를 포함하는데, 각각이 광대역 접속(13)을 통해 서비스 제공자 네트워크(10) 및 인터넷과 접속되어 있다. 시스템은 서비스 제공자 네트워크(10)(예를 들어 NSP 네트워크) 내에 또는 인터넷에서의 소정의 장소에 위치할 수 있는 발행/구독 브로커(11)를 더 포함한다. 시스템은 수백만 개의 CPE 디바이스(12)를 포함할 수 있고, CPE 디바이스들(12)의 CPE 디바이스 관리를 위해 각각은 발행/구독 브로커(11)와 접속하기 위한 클라이언트 소프트웨어가 있다. CPE 디바이스들(12)의 각각은 제어 데이터를 수신하는 발행/구독 브로커(11)의 하나 이상의 제어 채널(들)을 구독하고, CPE 디바이스들(12)의 각각은 데이터 채널(예를 들어 디바이스 데이터 채널 및 액션 데이터 채널) 상에 데이터를 발행하고, 이를 통해 CPE 디바이스들(12)은 디바이스 데이터(예를 들어 하드웨어 및 소프트웨어 데이터, IP-주소 등)를 전송할 수 있다.

[0089] 시스템은 또한 발행/구독 브로커(11)와 접속되는 제1 및 제2 백엔드 엔티티들(14, 15)을 더 포함한다. 바람직한 실시예에서, 어느 CPE 디바이스들(12)이 설치되었고 현재 활성화되었는지를 인지하도록, 백엔드 엔티티들(14, 15)은 모두 CPE 디바이스들(12)의 데이터 채널을 구독한다. 다른 예의 실시예에서, 백엔드 엔티티(14)만이 디바이스 데이터를 구독하고, 이는 예로서 백엔드 엔티티(14)가 모든 CPE 디바이스들(12)의 인벤토리를 유지하고 CPE 디바이스들(12)의 가장 필수적인 정보(예를 들어 하드웨어 및 소프트웨어 데이터, 언제 CPE 디바이스들(12)이 데이터를 발행했는지, 어떤 제어 액션을 CPE 디바이스들(12)이 수행했는지, 등등의 정보)를 저장하기 때문이다. 백엔드 엔티티(15)는 제어 데이터 채널 및 액션 데이터 채널을 통해 발행/구독 브로커(11)와 연결된다. 제어 데이터 채널을 통해, 백엔드 엔티티(15)는 CPE 디바이스들(12)에 URL을 포함하는 실행 액션을 전송하고, URL은 CPE 디바이스들(12)에 의해 실행되는 백엔드 스크립트를 가리킨다.

[0090] 백엔드 엔티티(15)로부터 제어 데이터 및 CPE 디바이스들(12)로부터 디바이스 및 액션 데이터를 수신하기 위해, 발행/구독 브로커(11)에 의해 제공된 대로, 백엔드 엔티티(14)는 제어 데이터 채널, 디바이스 데이터 채널 및 액션 데이터 채널을 구독한다.

[0091] 두 개 또는 다수의 백엔드 엔티티가, 그들의 로직 또는 필요성에 따라, 채널들/토픽들 및 메시지들의 전부 또는 일부를 구독할 수 있는 방법의 예들이 설명된다. 특정한 지역 등에서, 특정한 NSP에서의 디바이스들로부터 메시지를 오직 발행하기 위한 또는 수신하기 위한 특정한 백엔드 엔티티는 특정한 채널 부분을 구독할 수 있다. 백엔드 엔티티들은 또한 시스템에 동적으로 추가되거나 모든 다른 기능성을 온전히 유지한 채로 제거될 수 있다.

[0092] 상술한 예들에서, CPE 디바이스들(12)은 발행/구독 브로커(11)에 의해 제공된 대로 특히 제어 데이터 채널을 구독할 수 있고, 발행/구독 브로커(11)에 디바이스 데이터 채널 및 액션 데이터 채널을 통해 디바이스 및 액션 데이터를 발행할 수 있다. 따라서, CPE 디바이스들(12)은 백엔드 엔티티(15)에 의해 제공된 대로 제어 데이터 채널을 통해 어떤 액션 데이터를 수신하고, 제어 데이터에 의해 지시된 대로, 프로그램 또는 스크립트를 다운로딩하고, 그것을 실행한다. 프로그램 또는 스크립트의 실행 이후에, CPE 디바이스들(12)은 액션 데이터 채널 상의 액션 데이터로서 결과를 발행하는데, 이 정보는 발행/구독 브로커(11)에 의해 제1 및 제2 백엔드 엔티티들(14, 15)로 포워딩된다. 백엔드 엔티티(15)는 예를 들어 CPE 디바이스들(12)의 액션들의 진행을 추적하는 제어 데이터를 사용하는 네트워크 서비스 제공자의 서버이고, 백엔드 엔티티(14)는 예를 들어 CPE 디바이스들(12)의 운영

을 추적하는 액션을 완료하는 CPE 디바이스(12)의 정보를 저장하는 CPE 디바이스(12)의 벤더의 서버이다.

[0093] CPE 디바이스(18)는 발행/구독 브로커(11)에 디바이스 데이터 채널을 통해 디바이스 데이터만을 발행하는데, 이는 CPE 디바이스(18)는 상이한 네트워크 서비스 제공자에 속하고 백엔드 엔티티(15)에 의해 제어되지 않기 때문이다. CPE 디바이스들(12)은 특히 동일한 네트워크 서비스 제공자에 의해 제공되고/제공되거나 NSP 네트워크의 일부이다.

[0094] 제1 백엔드 디바이스(15)의 실행 액션을 통해, 예를 들어 새로운 소프트웨어 애플리케이션은 CPE 디바이스들(12) 상에 설치될 수 있거나 펌웨어 업데이트는 CPE 디바이스들(12)에 대해 수행될 수 있다. 백엔드 엔티티(15)의 실행 액션을 수행하는 방법은 도 4에서 도식적으로 설명되는데, 이는 백엔드 엔티티(15) 및 CPE 디바이스들(12) 간의 데이터 플로우를 도시한다. 백엔드 엔티티(15)는 예를 들어 URL을 포함하는 실행 액션을 전송함으로써[단계(20)], 발행/구독 브로커(11)에 제어 데이터 채널을 통해 CPE 디바이스들(12)에 대한 제어 데이터를 발행하는데, 발행/구독 브로커(11)는 제어 데이터를 CPE 디바이스들(12)로 포워딩한다. 실행 액션은 예를 들어 다음 종류의 JSON 메시지이다:

[0095] {"ctrl":{"action":"exec","key":"45335435".,"url":https://username:password@tchbackend.com/files/sdghsdg.lua,"data":"dsdghf321", "target":"*"}, "signature": "<base64encoded signature over ctrl data>"}. JSON은 메시지를 직렬화하는(serializing) 하나의 예에 불과하고, 다른 예들은 XML(Extensible Markup Language), ASN.1, Comma Separated Values 등을 포함하지만 그에 제한되지 않는다.

[0096] 다음 단계(21)에서, CPE 디바이스들(12)은 JSON 파일에서 가리키고 URL에 위치한 스크립트 파일을 다운로딩한다. 스크립트 파일은 예를 들어 Lua 스크립트 파일이다. CPE 디바이스들(12)은 스크립트 파일에 포함된 제어 데이터 서명 및 그것이 신뢰할 수 있는 백엔드 개인 키에 의해 서명되었는지를 확인한다. 확인을 위해, 기본 또는 다이제스트(digest) 식별, 예를 들어 유저이름(username) 및 암호(password)는 HTTP Get 명령을 사용함으로써 URL: https:// tchbackend.com/files/sdghsdg.lua로부터 https를 통해 요청된다.

[0097] 유효한 개인키 및 서명의 경우에서, CPE 디바이스(12)는 이러한 스크립트를 실행한다[단계(22)]. 스크립트는 예를 들어 설정을 변경하고, 상태 및 통계를 체크하고, 통계를 검색하고, 경보 임계값들(thresholds)에 대해 그들을 집계하거나 체크하는 등의, 어떤 조건적 또는 무조건적 상호작용을 수행한다. 스크립트 결과들은 예를 들어 성공, 상세한 장애 코드를 포함하는 실패 표시, 상태/통계, 특정한 쿼리 결과가 되거나 포함할 수 있고, 발행/구독 브로커(11)에 액션 데이터 채널 상의 액션 데이터로 발행되고, 발행/구독 브로커(11)는 백엔드 엔티티(15)에 결과들을 포워딩한다[단계(23)].

[0098] 도 3에 대하여 설명된 시스템의 예시적인 운영은 도 5에 관하여 이하에서 설명된다. 제1 CPE 디바이스(12)인 클라이언트1은 발행된 구독 브로커(11)에 디바이스 데이터를 발행한다[단계(30)]. 발행/구독 브로커(11)는 제1 및 제2 백-엔드 엔티티들(14, 15)인, 백엔드1 및 백엔드2에 디바이스1 데이터를 포워딩한다[단계(31, 32)]. 단계(33)에서, 제2 CPE 디바이스(12)인 클라이언트2는 발행/구독 브로커(11)에 그 디바이스 데이터를 발행하고, 발행/구독 브로커(11)는 백엔드1 및 백엔드2 서버들(14, 15)에 디바이스2 데이터를 상응하게 포워딩한다[단계(34, 35)]. 또한, CPE 디바이스(16)인 클라이언트3은 발행/구독 브로커(11)에 그 디바이스 데이터를 포워딩하고, 발행/구독 브로커(11)는 백엔드1 및 백엔드2 엔티티들(14, 15)에 이러한 디바이스 데이터를 포워딩한다[단계(36-38)]. 백엔드 엔티티(15)는 특히 네트워크 서비스 제공자의 서버이고, 백엔드 엔티티(14)는 CPE 디바이스(12)의 벤더의 서버이다. 단계(39)에서, 디바이스 데이터 디바이스1 내지 디바이스3은 서버들(14, 15)에 의해 로그인 된다.

[0099] 다음 단계(40)에서, 백엔드2 서버는 제어 액션을 개시하고, 발행/구독 브로커(11)에 제어 데이터를 발행한다[단계(41)]. 발행/구독 브로커(11)는 클라이언트1 및 클라이언트2 CPE 디바이스들에 이러한 제어 데이터를 포워딩하지만[단계(42, 43)], 그러나 클라이언트3 CPE 디바이스에는 포워딩하지 않는다. 제어 데이터는 또한 발행/구독 브로커(11)에 의해 제어 데이터를 기록하는 백엔드1 서버(14)에 포워딩된다[단계(44, 45)]. 단계(46,47)에서, 제어 데이터는 클라이언트1 및 클라이언트2 CPE 디바이스들에 의해 처리되고 실행된다[단계(46, 47)]. 클라이언트1 디바이스가 액션을 종료할 때, 클라이언트1 디바이스는 발행/구독 브로커(11)에 액션 데이터를 발행하고[단계(48)], 발행/구독 브로커(11)는 백엔드1 및 백엔드2 서버들(14, 15)에 액션 데이터를 포워딩한다[단계(49, 50)]. 클라이언트2 디바이스가 액션을 종료하고 실행할 때, 이는 발행/구독 브로커(11)에 액션 데이터를 발행하고, 발행/구독 브로커(11)는 백엔드1 및 백엔드2 서버들(14, 15)에 액션 데이터를 포워딩한다[단계(51-53)]. 액션 데이터는 백엔드1 및 백엔드2 서버들에 의해 로그인되고[단계(54)], 그 이후에 실행 액션 및 제어는 완료된다[단계(55)].

[0100] 따라서, 도 3에 대해 설명된 시스템은 발행/구독 브로커(11), 다수의 CPE 디바이스(12) 및 하나 또는 여러 백엔드 엔티티(14, 15) 간의 일-대-일, 일-대-다, 및 다-대-다 통신을 가능하게 한다. 백-엔드 엔티티들(14, 15)은, 특히 NSP 네트워크(10)의 네트워크 서비스 제공자, 임의의 인터넷 서비스 제공자, 또는 CPE 디바이스들(12)의 벤더 또는 제조업자에 의해, 제공되고/제공되거나 관리되는 서버이다. 백-엔드 엔티티(15)는 예를 들어 네트워크 서비스 제공자에 의해 제공되는 서버이고, 백-엔드 엔티티(14)는 CPE 디바이스들(12)의 제조업자에 의해 제공되는 서버이다.

[0101] 현재 산업 기준 프로토콜들보다 더 확장가능하고 더 비용 효율이 높은 전반적인 대안 솔루션을 제공하기 위해, 본 발명은 하나의 특정한 발행/구독 기술에만 의존하지 않고 가능한 다수의 백엔드 엔티티에 의해 엔드-유저 디바이스 관리에 대한 발명의 개념들을 추가한다.

[0102] 시스템은 다음의 장점들이 있다: 예를 들어, 통신 오버헤드 및 백-엔드 엔티티가 지원할 수 있는 디바이스들의 수에 대하여, 이 접근은 전통적인 중앙집중된 요청/응답 기반의 관리 접근들보다 더 확장가능하다. 중앙 ACS에 의존하기 위한 백-엔드 엔티티들을 필요로 하지 않는다. 또한, 그것은 어디든 상주할 수 있는 엔드-유저 디바이스들 및 백엔드 엔티티들과 느슨하게 연결된 방식으로 일-대-일, 일-대-다, 및 다-대-다 통신을 지원한다.

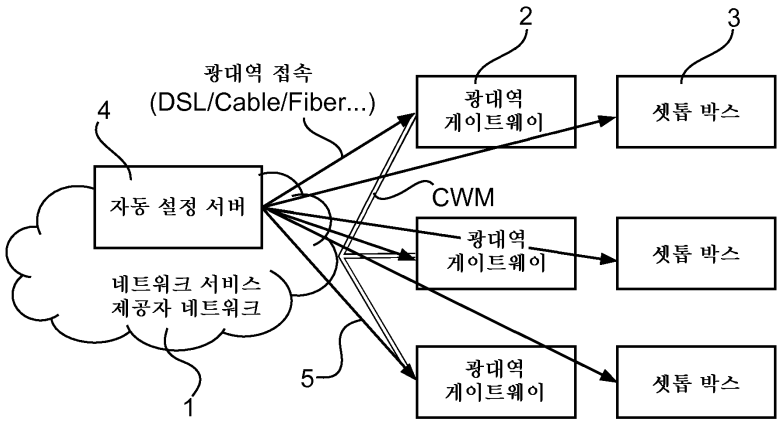
[0103] 시스템은 TR-069와 같은 현존하는 솔루션들과 비교하여 더 빠른 백엔드로부터 디바이스로의 통신도 지원하는데, 이는 언제나 백-엔드 엔티티가 데이터를 전송/발행할 수 있기 때문이고, 이러한 경우에 ACS가 제1 접속 요청을 CPE 디바이스로 전송하고, 그 이후에 CPE 디바이스가 관리 세션을 위해 ACS에 접속한다. 시스템은 디바이스들 그 자체들을 거쳐 많은 수의 CPE 디바이스들에 일반적으로 적용될 백엔드 로직의 분배를 (중앙집중된 TR-069 ACS 로직에 비해) 더 허용하고, 확장성을 상당히 향상시키는데, 이는 중앙 장소로의 값 비싼 통신에 대한 필요성이 제거되기 때문이다(전형적으로, ACS 로직은 디바이스 상의 데이터를 검색하거나 업데이트하고, 결과/성과에 기반을 두어 다음 단계들을 취한다).

[0104] 시스템은 전통적인 중앙 서버(예를 들어 ACS)와 달리, 임의의 수의 백엔드 엔티티를 더 지원하고, 현재 기술의 상태(TR-069, SNMP, OMA-DM)와 비교하여 관리 애플리케이션들의 더 넓은 영역을 지원한다. 그것은 또한 어떤 근본적인 웹 발행/구독 인프라스트럭처를 (중앙집중된 브로커들, 멀티캐스트 기반의 발행/구독) 지원한다. CPE 디바이스들(12)은 특히 그들의 운영에 대한 소규모의 데이터 분배 서비스에 기반을 둔, 미들웨어를 사용할 수 있다. 이 종류의 미들웨어는 발행 구독 메커니즘을 통해 발행/구독 브로커(11)와 작동되도록 쉽게 적용될 수 있다.

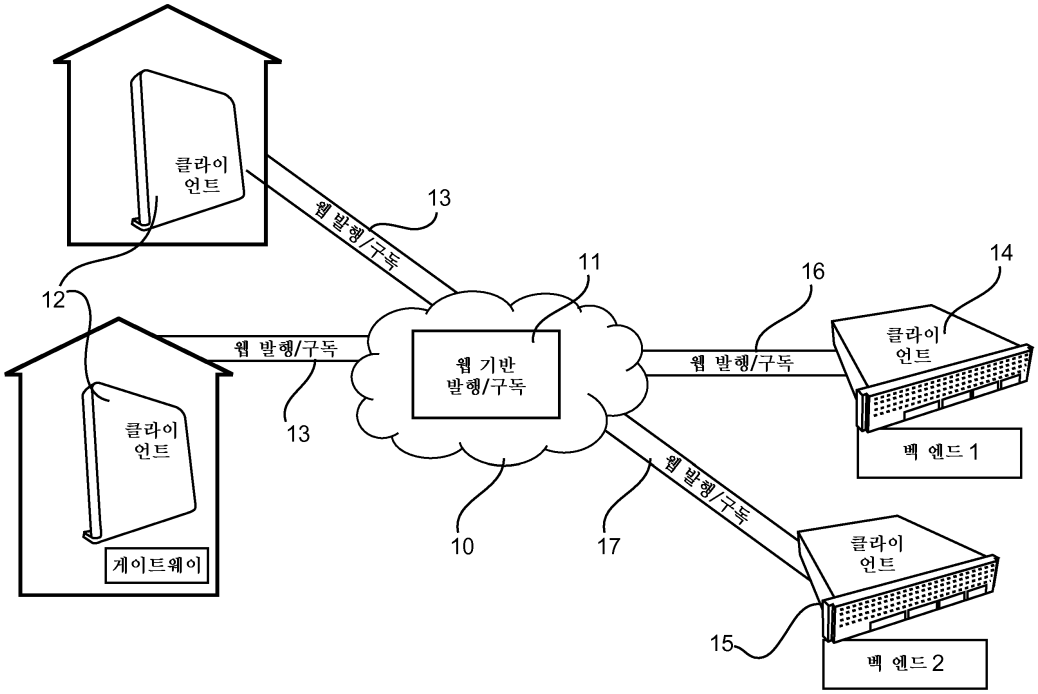
[0105] 또한, 본 발명의 다른 실시예들은, 본 발명의 범위로부터 벗어나지 않고, 당해 기술분야의 통상의 기술자에 의해 활용될 수 있다. 본 발명은 특히 xDSL, DOCSIS 또는 섬유 전송들을 사용하는 광역 네트워크들에 제한되지 않고, 임의의 다른 유무선 광대역 기술(예를 들어 TV 분배 케이블, 임의의 광 전송, 광대역 전력선 통신, WiMax 또는 3G 무선 접속성). 상술된 시스템은 특히 모든 종류의 CPE 디바이스들(예를 들어 레지덴셜 게이트웨이, 라우터, 스위치, 텔레폰 및 셋-톱 박스)과 같은 네트워크로 연결된 엔드-유저 디바이스 및 고객 전자 디바이스(예를 들어 셀 폰 또는 스마트 폰, 태블릿 PC 및 스마트 TV)에 대해 사용될 수 있다. 따라서, 본 발명은 이하에 첨부된 특허청구범위에 있다.

도면

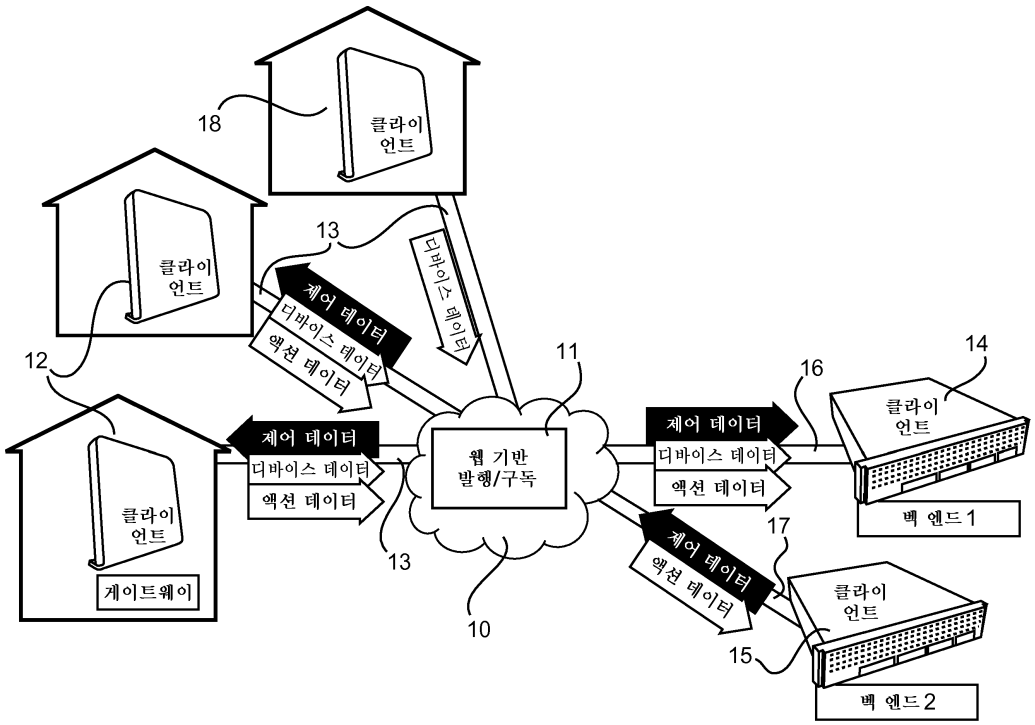
도면1


2
3
광대역 접속
(DSL/Cable/Fiber...)
4
광대역
게이트웨이
셋톱 박스
자동 설정 서버
CWM
광대역
게이트웨이
셋톱 박스
네트워크 서비스
제공자 네트워크
광대역
게이트웨이
셋톱 박스
5
1

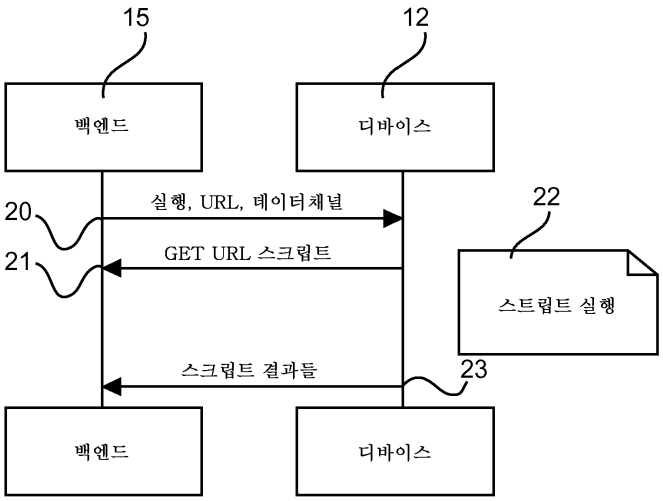
도면2


클라이
언트
웹 발행/구독
13
12
11
16
14
웹 발행/구독
웹 기반
발행/구독
클라이
언트
웹 발행/구독
13
클라이
언트
백 엔드 1
웹 발행/구독
10
17
클라이
언트
게이트웨이
15
백 엔드 2

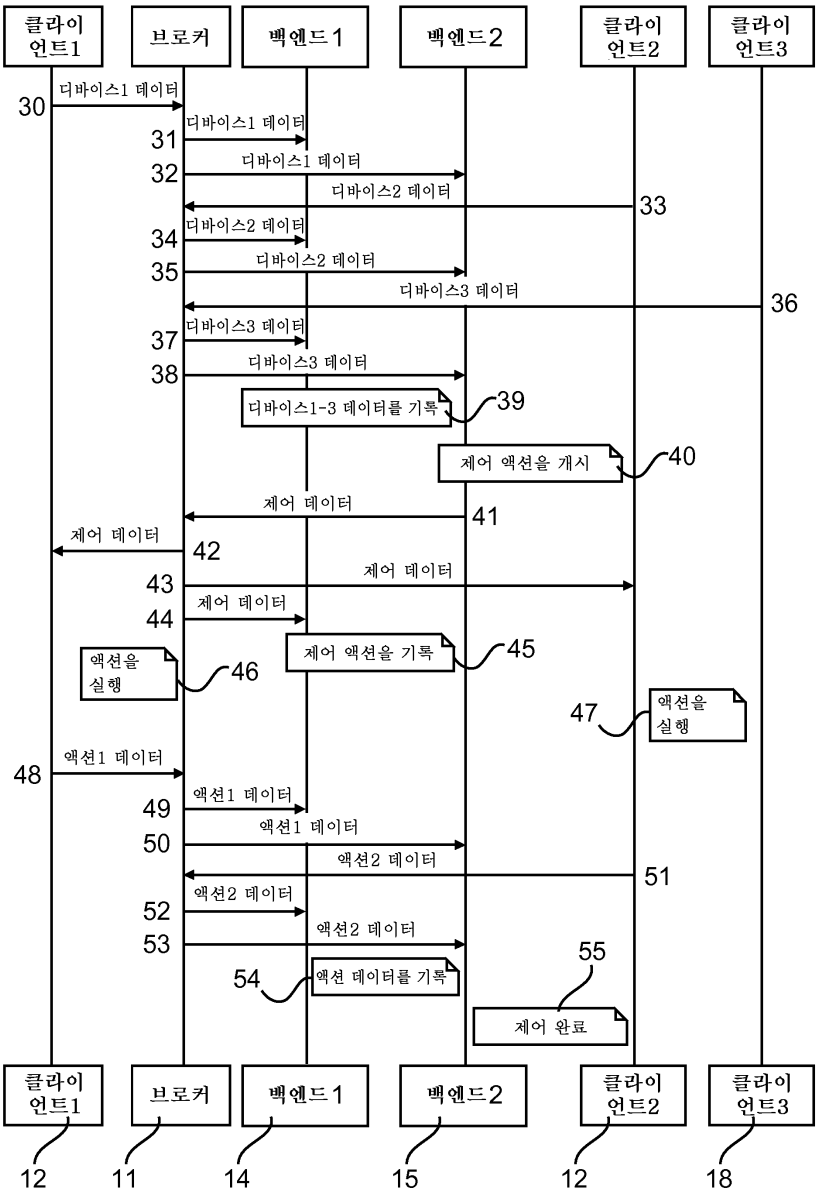
도면3


18
클라이언트
클라이언트
13
디바이스 데이터
제어 데이터
디바이스 데이터
액션 데이터
12
11
14
16
클라이언트
제어 데이터
디바이스 데이터
액션 데이터
웹 기반 발행/구독
제어 데이터
디바이스 데이터
액션 데이터
클라이언트
게이트웨이
13
17
제어 데이터
액션 데이터
클라이언트
10
15
백 엔드 1
백 엔드 2

도면4


15
12
백엔드
디바이스
20
실행, URL, 데이터채널
22
21
GET URL 스크립트
스트립트 실행
스크립트 결과들
23
백엔드
디바이스

도면5


클라이언트1
브로커
백엔드1
백엔드2
클라이언트2
클라이언트3
30
디바이스1 데이터
31
디바이스1 데이터
32
디바이스1 데이터
33
디바이스2 데이터
34
디바이스2 데이터
35
디바이스2 데이터
36
디바이스3 데이터
37
디바이스3 데이터
38
디바이스3 데이터
39
디바이스1-3 데이터를 기록
40
제어 액션을 개시
41
제어 데이터
42
제어 데이터
43
제어 데이터
44
제어 데이터
45
제어 액션을 기록
46
액션을 실행
47
액션을 실행
48
액션1 데이터
49
액션1 데이터
50
액션1 데이터
51
액션2 데이터
52
액션2 데이터
53
액션2 데이터
54
액션 데이터를 기록
55
제어 완료
12
11
14
15
12
18