(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103718510 B
(45)授权公告日 2018.01.30

(21)申请号 201280031897.3
(22)申请日 2012.06.27
(65)同一申请的已公布的文献号
申请公布号 CN 103718510 A
(43)申请公布日 2014.04.09
(30)优先权数据
11447015.6 2011.06.29 EP
(85)PCT国际申请进入国家阶段日
2013.12.27
(86)PCT国际申请的申请数据
PCT/EP2012/062415 2012.06.27
(87)PCT国际申请的公布数据
WO2013/000936 EN 2013.01.03
(73)专利权人 汤姆逊许可公司
地址 法国伊西莱穆利诺
(72)发明人 D.范德波尔
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 吕晓章
(51)Int.Cl.
H04L 12/24(2006.01)
H04L 12/26(2006.01)
G06F 9/445(2006.01)
H04L 29/12(2006.01)
H04L 29/08(2006.01)
H04L 29/06(2006.01)
(56)对比文件
US 2007214262 A1,2007.09.13,
CN 101765072 A,2010.06.30,
US 2009182907 A1,2009.07.16,
WO 03107629 A3,2004.03.18,
US 2011060822 A1,2011.03.10,
审查员 刘珊珊

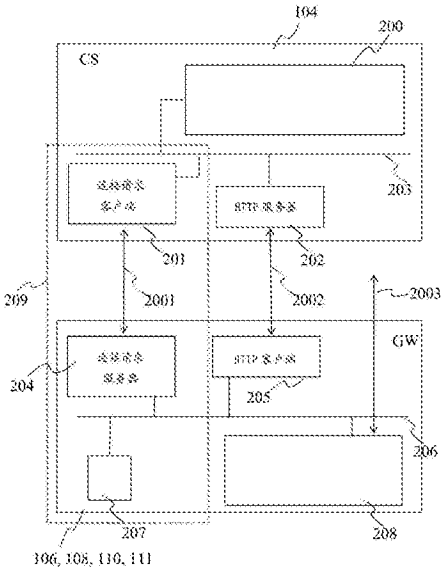
权利要求书2页 说明书7页 附图2页

(54)发明名称

设备间通信的方法和实现该方法的设备

(57)摘要

本发明涉及设备的远程管理领域，以及用于实现该方法的设备。具体地说，本发明涉及用于远程可管理设备的生命线连接，该生命线连接可用于重新建立远程配置管理服务器和远程可管理设备之间已经丢失的通信。



CN 103718510 B

1.一种在数字通信网络(105)中相互连接的远程配置设备(104)与远程可配置设备(106、108、110、111)之间、经由所述远程配置设备(104)与所述远程可配置设备(106、108、110、111)的远程管理连接(2002)进行通信的方法,包括:当所述远程配置设备已经确定所述远程管理连接丢失时,

-所述远程配置设备将救援消息传输到所述远程配置设备已知的所述远程可配置设备的地址以及所述远程可配置设备的预定端口号,所述远程可配置设备在预定端口号上监听救援消息,所述救援消息允许所述远程可配置设备重新配置自身,并且允许所述远程可配置设备向所述远程配置设备传输请求以重新建立与所述远程配置设备的远程管理连接,所述救援消息至少包括所述远程配置设备的地址,

-所述远程配置设备接收重新建立所述远程管理连接的请求,所述请求是所述远程可配置设备使用被包括在所述救援消息中的信息的结果,以及

-所述远程配置设备重新建立所丢失的与远程可配置设备的远程管理连接。

2.如权利要求1所述的方法,其中,所述救援消息还包括连接请求证书。

3.如权利要求1或2所述的方法,其中,所述救援消息还包括要由所述远程可配置设备执行的命令。

4.如权利要求3所述的方法,其中,所述命令是用于下载新固件的命令。

5.一种在数字通信网络(105)中相互连接的远程可配置设备(106、108、110、111)和远程配置设备(104)之间、经由所述远程配置设备(104)与所述远程可配置设备(106、108、110、111)的远程管理连接(2002)进行通信的方法,其中,所述方法包括:当所述远程配置设备已经确定所述远程管理连接丢失时,

-所述远程可配置设备接收在所述远程配置设备已知的所述远程可配置设备的地址上以及在所述远程可配置设备的预定端口号上的救援消息,所述远程可配置设备在预定端口号上监听救援消息,所述救援消息允许所述远程可配置设备重新配置自身,并且允许所述远程可配置设备向所述远程配置设备传输请求以重新建立与所述远程配置设备的远程管理连接,所述救援消息至少包括所述远程配置设备的地址,以及

-所述远程可配置设备传输重新建立所述远程管理连接的请求,所述请求是使用被包括在所述救援消息中的信息的结果。

6.如权利要求5所述的方法,其中,所述救援消息还包括连接请求证书。

7.如权利要求5或6所述的方法,其中,所述救援消息还包括要由所述远程可配置设备执行的命令。

8.如权利要求7所述的方法,其中,所述命令是用于下载新固件的命令。

9.一种远程可配置设备(106、108、110、111),所述远程可配置设备在数字通信网络中、经由远程配置设备(104)与所述远程可配置设备的远程管理连接(2002)、与所述远程配置设备(104)相互连接,其中,所述远程可配置设备包括:

-连接请求服务器(204),用于接收在所述远程配置设备已知的所述远程可配置设备的地址上以及在所述远程可配置设备的预定端口号上的救援消息,所述连接请求服务器在预定端口号上监听救援消息,所述救援消息允许所述远程可配置设备重新配置自身,并且允许所述远程可配置设备向所述远程配置设备传输请求以重新建立与所述远程配置设备的所述远程管理连接,所述救援消息至少包括所述远程配置设备的地址;以及

-客户端模块(205),用于传输重新建立所述远程管理连接的请求,所述请求是所述远程配置设备使用被包括在所述救援消息中的信息的结果。

10.如权利要求9所述的远程可配置设备,其中,连接请求服务器和客户端模块独立于该远程可配置设备的其他模块工作。

设备间通信的方法和实现该方法的设备

技术领域

[0001] 本发明涉及设备的远程管理、以及用于实现该方法的设备的领域。尤其地，本发明涉及一种可以在远程可管理的设备和远程管理服务器之间的远程管理通信已经丢失时使用的设备的远程管理的生命线连接(life-line connection)。

背景技术

[0002] 随着家庭中服务订购设备的出现，例如所谓的三网合一网关(triple-play gateway)(VoIP电话(互联网协议语音)、互联网、IP电视)，对于服务运营商来说，就会出现如何管理这些服务订购设备以便正确地配置它们能够以令人满意的方式使用/接收由这些服务运营商提出的服务的问题。尤其是，服务运营商可能经常需要安装额外的软件、升级固件或配置家庭网关中由运营商提供的已有的软件或硬件，以提供新的服务，或改善现有的服务。

[0003] 解决方案包括将这些服务订购设备连接到专用配置设备或ACS(自动配置服务器)，例如根据CPE或服务订购设备的远程配置的TR-069规范，ACS负责自动分发所需的软件给服务订购设备。一些设备，如网关和路由器、用于视听接收的机顶盒、IP语音(VoIP)电话机和网络附加存储(NAS)，都支持TR-069。

[0004] 然而，当ACS和CPE设备之间的通信明确丢失时，现有的解决方案将会失效，例如在TR-069的情形中，CPE设备负责建立与自动配置服务器(ACS)的管理会话。ACS可以在任何时候通过所谓的“连接请求”触发CPE建立管理会话。此允许远程管理、包括附加的安全措施(如，验证)的相对复杂的手段，可以确保远程管理的安全性。虽然TR-069被设计成健壮的协议，但仍存在ACS不能成功触发CPE与之建立远程管理连接的情况。这种失败的原因包括：TLS(传输层安全)证书过期而导致CPE不再信任ACS，因此拒绝建立与ACS的管理连接；CPE的配置问题，例如：CPE已经丢失ACS URL(统一资源定位器)，或CPE具有错误的ACS认证证书；由于CPE在很长一段时间内都处于断电状态，网络拓扑变化未能通信给CPE设备；或者甚至是自愿的终端用户干预，例如出于获得对CPE设备的控制权的原因通过黑客行为禁用远程管理。这种远程管理连接的丢失对服务运营商构成大问题，因为远程管理连接用于监视、诊断、配置管理或甚至固件更新。不再可管理的设备无法再接收：使用服务(如QoS(服务质量)、安全或防火墙服务、IPTV(互联网协议电视))所需的配置更新；新的服务，如添加VoIP和配置电话号码；任何报告的问题(如，连接不好、较差的服务质量)的诊断或故障排除；以及解决小问题或引入新的设备功能的自动固件升级。一旦CPE已经失去ACS的正确位置(地址)或已经失去有效的认证信息，该CPE就被视为相对于该ACS“丢失”，因为CPE无法成功建立到该服务器的管理连接。在这种情况下，服务运营商和订购设备之间的通信明确丢失，只能通过运营商手动干预恢复，通过指示用户或通过派工程师到用户所在地。

[0005] 2003年12月23日的文献WO 03/107133 A2《Secure Remote Management Appliance》(SMRA)描述了到网络服务现有连接的丢失以及通过另一个接口重新建立到网络服务的连接。但试图通过另一个、附加的网络接口联系网络管理站仍然不会使得SMRA在

发生前面描述的问题之一的情形中(见上文:“这种失败的原因包括”)联系上网络管理站,因为网络接口的改变不会消除这些失败的原因。

[0006] 2009年9月10日的文件US 2011/060822 A1《Apparatus and method for managing communications》描述了一种通过请求邻近网关代其建立管理连接来管理WAN连接丢失的网关。这并不能使网关能够在发生前面描述的问题之一的情形中恢复WAN连接,因为失败的网关无法建立替代的管理连接,例如,在无法提供合适的证书的情形中。此外,这种解决方案要求失败的网关能够与相邻的网关通信,这在网络拓扑发生变化时可能是不可能的。

[0007] 因此,有必要对部署在运营商的消费者家中的运营商的服务订购设备的远程配置管理进行优化,以支持为从服务运营商的角度来看被认为是“丢失的”的设备重新建立远程管理连接,并避免设备的昂贵的物理替换或每个顾客干预的需要。

发明内容

[0008] 本发明的目的是缓解现有技术的至少一些不便。

[0009] 更准确地说,本发明允许对服务运营商的服务订购设备或CPE的远程管理进行优化。

[0010] 为了达到这样的效果,本发明提出一种在经由远程管理连接在数字通信网络中相互连接的远程配置设备和远程可配置设备之间通信的方法,该方法包括在远程配置设备的以下步骤:

[0011] 如果确定远程管理连接丢失,那么

[0012] -通过除远程管理连接之外的连接(2001)将包括信息和允许通过远程可配置设备重新建立丢失的远程管理连接的至少一个命令的消息传输到远程可配置设备的地址和远程可配置设备的预定端口号;

[0013] -接收重新建立远程管理连接的请求,该请求是远程可配置设备使用被包括在消息中的信息和远程管理设备应用至少一个命令的结果。

[0014] 本发明还提出一种在经由远程管理连接在数字通信网络中相互连接的远程可配置设备和远程配置设备之间通信的方法,该方法包括在远程可配置设备的以下步骤:

[0015] 如果确定远程管理连接丢失,那么

[0016] -通过除远程管理连接之外的连接在预定的端口号上接收包括信息和允许远程可配置设备重新建立丢失的远程管理连接的至少一个命令的消息;

[0017] -应用所述至少一个命令;

[0018] -将重新建立丢失的远程管理连接的请求传输到远程配置设备,该请求是使用被包括在消息中的信息和应用至少一个命令的结果。

[0019] 根据一个变型实施例,预定端口号是远程可配置设备在其上监听允许远程可配置设备在远程管理连接丢失时重新建立与远程配置设备的远程管理连接的消息的端口号。

[0020] 根据一个变型实施例,该信息包括将被用于重新建立丢失的远程管理连接的连接请求证书。

[0021] 根据一个变型实施例,该信息包括将重新建立与之的远程管理连接的远程配置设备的地址。

[0022] 本发明还包括一种设备，包括：

[0023] -连接请求服务器，用于通过除远程管理连接之外的连接在设备的预定端口号上接收包括信息和允许设备重新建立丢失的远程管理连接的至少一个命令的消息；

[0024] -客户端模块，用于将重新建立丢失的远程管理连接的请求传输到远程配置设备，该请求是该设备使用被包括在消息中的信息和该设备应用所述至少一个命令的结果。

[0025] 根据该设备的一个变型实施例，连接请求服务器和客户端模块独立于该设备的其他模块工作。

附图说明

[0026] 通过描述本发明的具体的、非限制的实施例，本发明的更多优点将显现。将参照以下附图描述这些实施例：

[0027] 图1示出了本发明实现于其中的示例性网络架构；

[0028] 图2示出了添加到实现本发明的图1的设备104和106/108/110/111上的附加模块201和204。

具体实施方式

[0029] 图1示出了本发明实现于其中的示例性网络架构。

[0030] 该网络架构包括：

[0031] -一组运营商服务器100-103，例如，Web服务器100、视频点播(VoD)服务器101、宽带广播服务器102和VoIP服务器103；

[0032] -配置服务器(CS)104；

[0033] -网关(GW)设备106，CPE；

[0034] -接入网络105，例如，因特网或专用网络；接入网络互连运营商服务器100-103(经由连接1000)、配置服务器104(经由连接1001)和网关106(经由连接1002)；

[0035] -本地网络107，将家庭网络上的设备相互连接，并经由网关106将它们连接到接入网络105(经由连接1004、1005和1006)，并连接到连接至接入网络105的其他设备(100-103、104)；

[0036] -个人计算机(PC)108，CPE；

[0037] -电视机109；

[0038] -机顶盒(STB)110，CPE；以及

[0039] -无线PC111，CPE。

[0040] 网关106是由运营商提供为订购者提供三网合一服务的设备。网关106 允许订购者：

[0041] -经由IPTV机顶盒110和电视机109通过逻辑连接2002访问分别由运营商的宽带广播服务器101、102提供的VoD电视和IP广播服务；

[0042] -经由PC108和111访问因特网，经由逻辑连接2003访问由Web服务器100提供的服务；以及

[0043] -访问无线DECT电话机(DECT=数字增强无绳通信)，设备未显示)上的IP电话服务，经由逻辑连接2003由VoIP服务器103提供的服务。

[0044] 连续线1000，1001和1001是物理连接。虚线2001-2003是逻辑连接。虚线2001示出了根据本发明的逻辑生命线连接。虚线2002示出了配置服务器104和网关CPE设备106之间的逻辑远程管理连接。虚线2003示出了一个或多个服务提供商服务器100-103和网关106之间的逻辑连接。虽然虚线被描绘为具有在网关106处的中心点，但应该理解的是，这些虚线也可以将CPE设108、110和111中的任何一个或几个连接到提供商服务服务器100-103和配置服务器104。

[0045] 当提供商想发送配置或软件更新到一个或多个CPE设备(106、108、110、111)时，它使用远程管理连接2002在没有人工干预的情况下(即，在订购者所在地的干预不要求运营商的技术服务)指示可以自动更新或重新配置所选择的(多个)CPE设备的配置服务器104。具体地，配置服务器104使用远程管理连接2002可以修改配置服务器的地址，因为其被存储在网关106中(例如，如果附加的配置服务器由于订购者数量的增加是必要的，或者在重新分配IP地址的情形中；即在网络拓扑变化影响(多个)配置服务器地址的情形中)。然而，当一个或多个订购者的CPE设备从网络105或107断开，或者如果它们断电时，地址更新无法传播到这些设备。然后，它们中的一些对配置服务器的配置管理来说可能不再是可到达的(即，远程管理连接2002被说成是“丢失的”)，这可能导致相关CPE设备的不正确行为。根据另一种情景，通过远程管理连接2002在配置管理会话期间分发到CPE的软件更新可能导致CPE操作系统在重新启动时崩溃，在这种情况下，相关CPE明确是乱序的，无法再通过用于配置管理的配置服务器到达，订购者无法再访问订购的服务，包括例如电话服务。根据又一情景，订购者家庭网络中的一个或多个CPE设备由于配置服务器送出的错误配置变得不可通过配置服务器管理(记住，CPE设备必须建立管理连接；如果建立管理连接所需的数据是错误 的，那么CPE设备无法建立远程管理连接2002)。根据另一情景，TLS(传输层安全)的安全证书已经到期，CPE设备不再信任配置服务器，CPE设备因此拒绝建立管理会话。所有这些情景和其他未讨论的情景都由于它们导致远程配置连接2002的丢失而使得CPE设备对于配置管理来说无法到达。

[0046] 因此，当CPE设备已经变得相对于ACS不可管理时，即当远程管理连接2002丢失时，本发明增加允许恢复CPE设备的正确运行的生命线连接2001。在图2中，生命线连接2001将配置服务器104连接到网关106。根据一个变型实施例，生命线连接2001连接到不是CS104的另一设备(未示出)。这允许例如从特别设备中“故障排除”网关106。

[0047] 图2示出了添加到实现本发明的设备104和106的附加模块201、204和207。这些模块在图2中用虚线框209表示。在配置服务器(“CS”或“ACS”)侧，将连接请求客户端201添加到配置服务器104。在CPE侧(106、108、110或111)，添加连接请求服务器203和持久存储空间207。CS104中的连接请求客户端201与CPE中的连接请求服务器通过连接2001进行通信。服务提供商经由连接2003将其服务提供给任何CPE设备。

[0048] 在配置管理会话期间，CPE设备(106、108、110或111)中的HTTP客户端205经由远程管理连接2002与在CS104中的HTTP服务器202通信。根据一个特定实施例，HTTP服务器202和HTTP客户端204通过连接2002根据TR-069协议进行通信。模块200和208分别是配置服务器104和网关106正常工作所需的模块。这些模块包括例如CPU(中央处理单元)、存储器、防火墙、NAT(网络地址转换)模块等。这些模块经由内部通信部件(例如分别用于配置服务器104的内部总线203和用于设备106、108、110或111的内部总线206)相互通信。

[0049] 连接2001构成到设备106、108、110和111的生命线连接，允许在由于前面针对图1描述的非穷尽的通信失败的情景而丢失远程管理通信链路2003时恢复远程管理通信链路2003。

[0050] 设备106、108、110或111的连接请求服务器(CRS)204的作用是充当服务器和监听在预定的端口号(例如TCP端口7547)上传入的连接请求，即HTTP GET请求。此端口在下文中称作“生命线连接端口”。CRS进一步认证发出带有一组CPE配置的证书(例如，出厂默认用户名和密码)的请求的实体。根据本发明的一个变型实施例，CPE设置有可选机制，如允许防范恶意 使用的机制。一个示例性保护机制是连接请求抑制，允许限制随时间推移接受的请求的数量，以保护CPE不受拒绝服务攻击，其中CPE在它同时服务许多请求时将变得不可用。

[0051] 设备106、108、110或111的HTTP客户端205的作用是充当可能在已经经由DNS(域名系统)查询一个或多个DNS服务器(未示出)解析配置服务器的URL(统一资源定位符)以获得配置服务器104的IP地址之后通过远程配置连接2002与配置服务器104通信的HTTP客户端。在发生多个事件之后——例如：每当CRS204通过生命线连接2001接收到连接请求，CRS都将此类事件通知给HTTP客户端；在设备106、108、110或111启动之后，或者当设备106、108、110或111的设备配置变化时，都将此变化通知给订购的CS104——建立到CS104的连接。根据一个变型实施例，触发建立到CS104的连接的事件列表包括TR-069通知RPC(远程过程调用)事件。设备106、108、110或111的HTTP客户端205进一步验证CS104提供的证书签名和多个本地存储的证书中的任何一个(例如，本地存储在永久性存储器107中)以信任该CS104，HTTP客户端205应用从CS104接收到的命令，该命令包括例如存储在永久性存储器207中的修改设备106、108、110或111的特定配置参数的“SetParameterValues”，或“Reboot”。

[0052] 设备106、108、110或111的永久性存储器207的作用是：

[0053] • 包括CS URL(例如：http://cs.provider.com)；

[0054] • 包括连接请求证书(用户名和密码)；

[0055] • 包括可重复使用来验证CS提供商证书签名的一个或多个本地存储的证书；

[0056] • 包括设备106、108、110或111制造商的公共密钥，用于验证固件映像和其他制造商所提供的数据的真实性；以及

[0057] • 包括设备106、108、110或111的CPE设备配置。

[0058] 例如，CS104的连接请求客户端(CRC)201是HTTP客户端，其可以在特定的时间点发起连接请求和认证到设备106、108、110或111，并触发远程可配置设备建立管理会话。

[0059] CS104中的HTTP服务器202的作用除了其他的之外还包括提供HTTP服务器和提供CS的证书签名给设备106、108、110或111。

[0060] 在图2中，设备106、108、110或111被作为示例性的CPE设备。然而，本发明不限于使用这些类型的设备实现，而可以使用任何类型的CPE来实现。

[0061] 当远程配置连接2002丢失时，CS104的CRS204被配置为在生命线连接端口上进行监听。根据一个特定实施例，该机制由看门狗机制实现，其中实现本发明的设备的其他模块之一定期发送保持活跃信号给CRS204。如果在看门狗定时器到期之后还未接收到保持活跃信号，那么自动启动CRS的监听进程。根据另一个实施例，监听进程始终是有效的。第一实施例允许例如降低实现本发明的设备的功耗，因为监听进程(和实现监听进程所需的模块)不必在所有时间保持通电。

[0062] 服务运营商通常知道CPE的IP地址。生命线连接端口号是例如TR-069的IANA(国际因特网地址分配委员会)固定的默认端口号(TCP端口7547),或者是服务提供商和CPE设备制造商之间同意的端口号。当CPE(例如,GW106)在生命线连接端口上接收到传入的HTTP GET连接请求消息(即,救援消息)时,CPE的CRS(例如,GW106的CRS204)验证该救援消息。为了允许CPE重新建立丢失的与远程配置设备的远程管理连接,救援消息包括救援信息和救援命令。典型的救援信息是:设备实体,例如包括制造商ID、产品类别、序列号;这是为了确保救援命令只被其预定要用于的CPE设备考虑;或有效的ACS URL地址等。典型的救援命令包括:

[0063] -还原到出厂默认值(撤消可能导致丢失与CS的远程管理连接的任何用户配置或其他配置更改);

[0064] -使用在救援信息中提供的新的CS URL;

[0065] -将CS证书(用户名,密码)设置为在救援信息中提供的证书;

[0066] -禁用CS证书检查,以在任何情况下信任CS;或

[0067] -打开任何其他的管理接口,如用户接口、Telnet会话,以允许服务提供商连接和管理设备,例如,排除故障和纠正配置问题。可选地,为了提高安全性和防范通过生命线连接2001恶意传输救援信息命令,救援消息中的信息包括通过救援消息命令计算得到的哈希值,使用CPE制造商的私钥对其签名,从而使CPE设备可以检查救援命令没有被未授权的实体的改变。

[0068] 如果救援消息被CPE正确认证,那么CPE执行救援命令,例如下载新的固件。应用救援命令之后,CPE被正确地重新配置,并且CPE将重新建立远程管理连接的请求传输给CS。该请求可能基于在救援消息中提供的信息(即,使用提供的新的ACS URL,或换言之,远程配置设备的地址),并且可能包括在救援消息中提供的信息中提供的信息的至少一部分(即,使用提供的认 证有效的新的连接请求证书);因此,请求是远程可配置设备使用在救援消息中提供的信息和所述远程管理设备应用被包括在救援消息中的救援命令的结果。

[0069] 根据一个变型实施例,CPE设备通过生命线连接2001将表示已经考虑命令的确认消息发送到CS来确认已经考虑救援命令。该变型具有在CPE准备建立远程管理会话时将确切时刻发信号给配置服务器的优点。

[0070] 根据一个变型实施例,救援消息包括将由CPE执行的若干个救援命令。

[0071] 根据一个变型实施例,CS通过生命线连接2001传输若干个救援消息,以应用若干个救援命令。可选地,每个后续的救援消息都只在接收到前面提到的确认CPE考虑了之前传输的救援消息的确认信息之后被传输。

[0072] 根据又一变型实施例,CPE在已经考虑救援消息之后,验证它是否能够联系上CS,并通过生命线连接2001往回报告该验证。

[0073] 根据一个变型实施例,实现本发明所必需的组件(连接请求服务器204和客户端模块205)以自治的方式工作,即独立于远程可配置设备的其他模块。在这种情况下,即使实现本发明的设备已经“崩溃”,即无响应,该设备也可以经由生命线连接2001返回允许例如下载较好的配置或纠正的固件版本到处于不可操作和不可管理状态的设备的可操作状态。

[0074] 这些变型实施例可以结合起来形成特定的有利实施例。

[0075] 根据一个具体的实施例,本发明完全在硬件中实现,例如,实现为专用组件(例如,

实现为ASIC、FPGA或VLSI)(分别是专用集成电路、现场可编程门阵列和超大规模集成电路),或者实现为集成在设备上的不同的电子元件或以硬件和软件组合的形式。

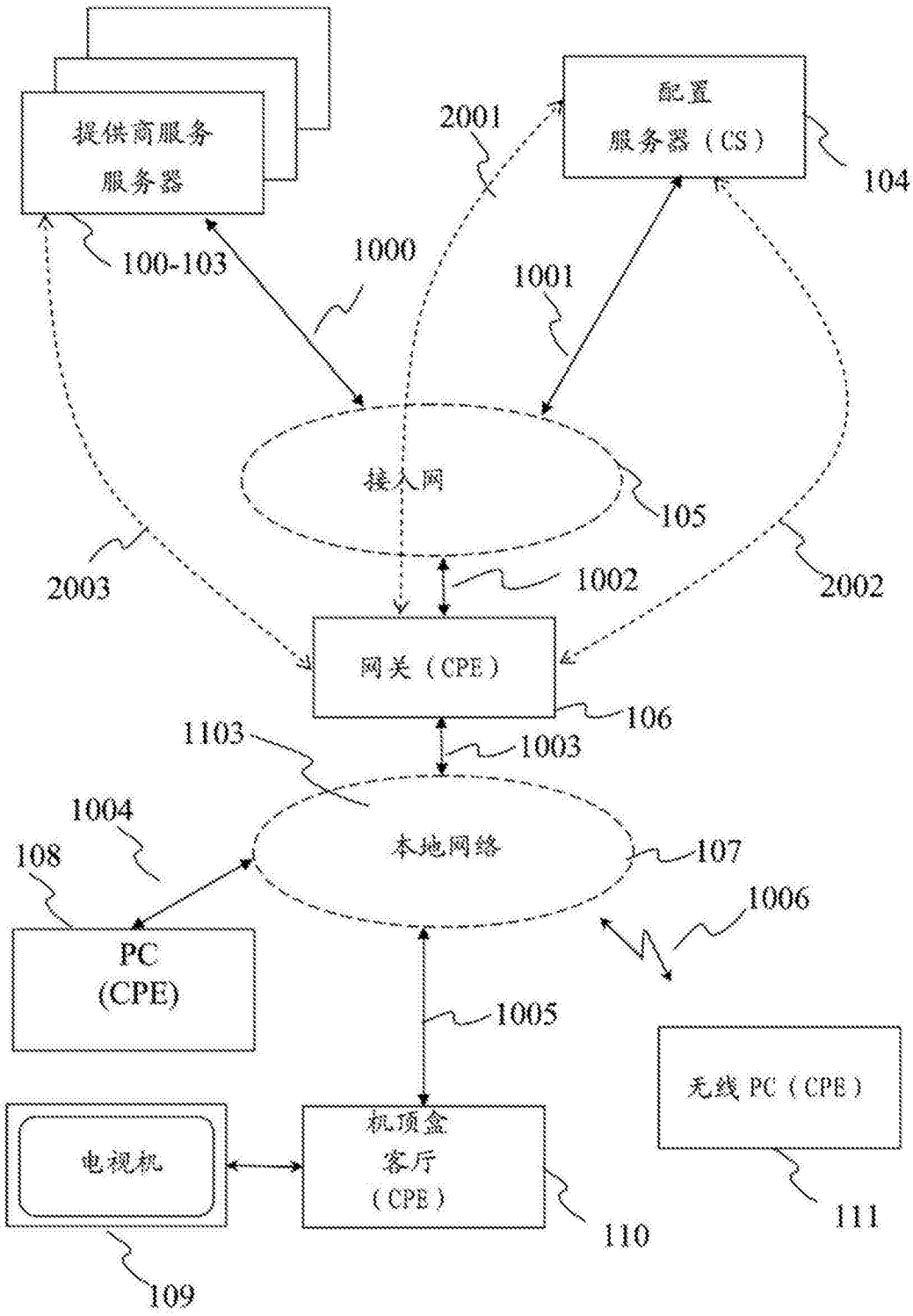

提供商服务
服务器
100-103
2001
配置
服务器（CS）
104
1000
1001
接入网
105
2003
1002
2002
网关（CPE）
106
1103
1003
1004
本地网络
107
108
1006
PC
(CPE)
1005
无线 PC（CPE）
电视机
机顶盒
客厅
（CPE）
110
111
109

图1

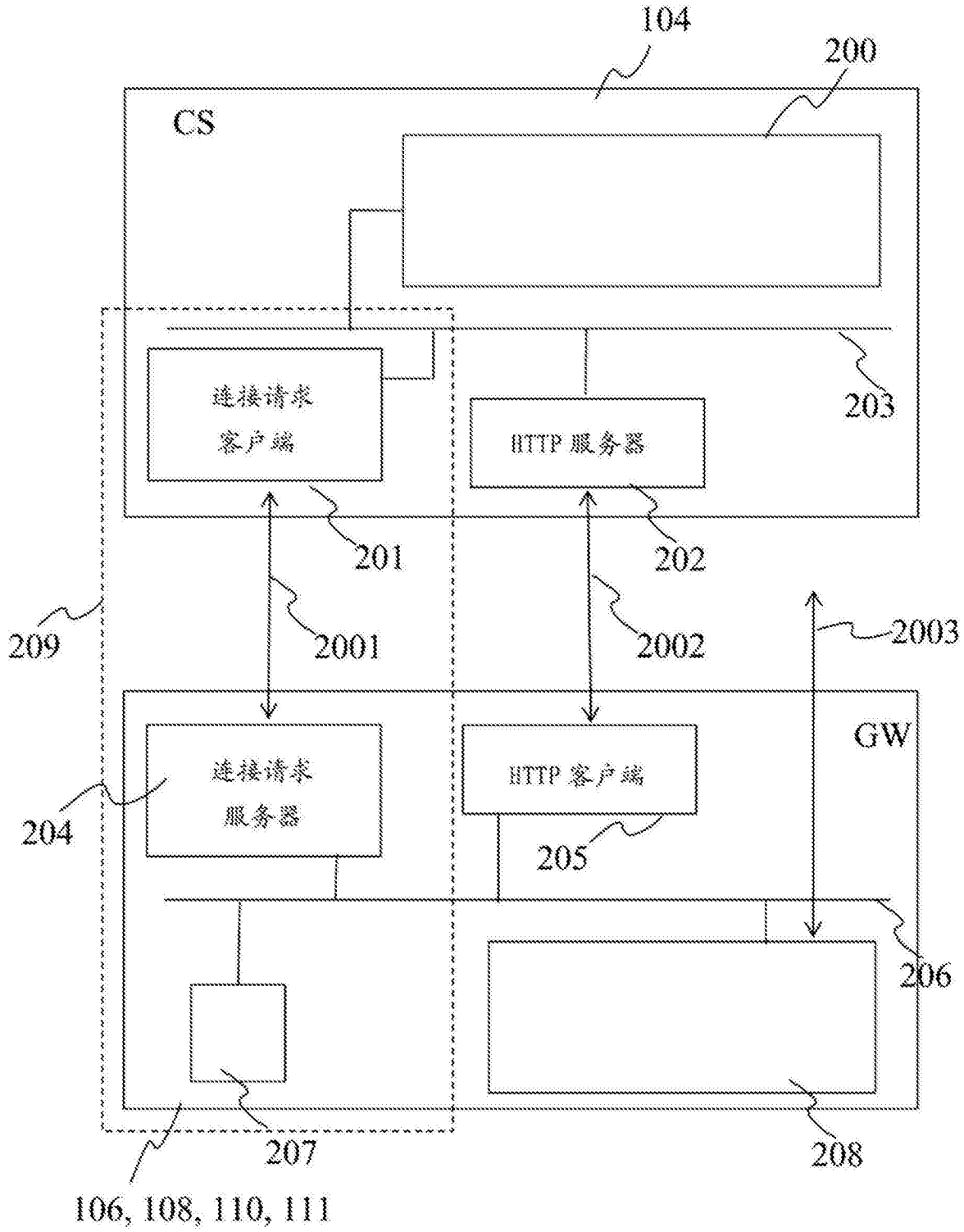

104
200
CS
203
连接请求
客户端
HTTP 服务器
201
202
209
2001
2002
2003
GW
连接请求
服务器
HTTP 客户端
204
205
206
207
208
106, 108, 110, 111

图2