



(12) 发明专利

(10) 授权公告号 CN 101218805 B

(45) 授权公告日 2012. 04. 25

(21) 申请号 200680024916. 4

(22) 申请日 2006. 06. 02

(30) 优先权数据

102005033211. 0 2005. 07. 13 DE

(85) PCT申请进入国家阶段日

2008. 01. 08

(86) PCT申请的申请数据

PCT/EP2006/062879 2006. 06. 02

(87) PCT申请的公布数据

W02007/006611 EN 2007. 01. 18

(73) 专利权人 汤姆森许可贸易公司

地址 法国布洛涅-比朗库尔

(72) 发明人 英戈·许特尔 迈克尔·韦伯

(74) 专利代理机构 中科专利商标代理有限责任公司 11021

代理人 戎志敏

(51) Int. Cl.

H04L 29/08 (2006. 01)

(56) 对比文件

US 2002078161 A1, 2002. 06. 20, 全文.

US 2005108331 A1, 2005. 05. 19, 全文.

EP 1469654 A, 2004. 10. 20, 全文.

US 2005122934 A1, 2005. 06. 09, 全文.

审查员 王瑞

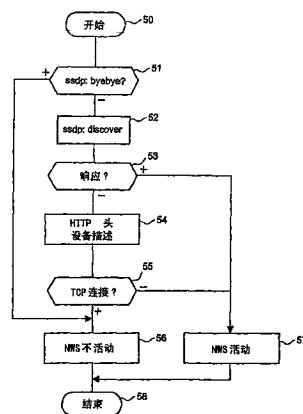
权利要求书 1 页 说明书 5 页 附图 3 页

(54) 发明名称

在分布式站点网络中设备活动检测的方法，
以及执行该方法的网络站点

(57) 摘要

本发明涉及本地数据传输网络、尤其是家庭网络技术领域。在诸如此类的网路中，网络站点登录与网络连接。一旦断开连接，离开网络的网络站点以合适的方式注销。在用户仅通过拔出网络电缆而将网络站点从网络中断开的情况下，物理上不可以传输注销消息。现在本发明考虑到如何可靠地识别不活动的网络站点的问题，也考虑到仅通过拔出网网络插头而断开网络站点的情况。本发明通过有规律地向网络中的站点传输搜索请求解决了该问题。如果一个网络站点保持不应答搜索请求 (53)，那么另外地尝试对例如所述网络站点的设备描述或控制请求的 HTTP 访问 (54)。只有在该访问 / 控制请求也失败的时候，才标识该网络站点不活动 (56)。在 UPnP 网络的情况下，使用不受保护的 SSDP 协议做出搜索请求，从而对搜索请求任何响应的缺乏不会客观可靠地指示网络站点已经注销。通过发生在差错保护基础上的 HTTP 访问的方式来确认没有响应搜索请求的站点是不活动的推测。



1. 一种用于检测分布式站点网络中网络站点的活动的方法,其中通过不受保护的传输协议,由对网络站点的搜索请求来检查一个网络站点的活动,至少一个安全传输协议可用于数据访问和 / 或控制网络站点,其特征在于:如果所寻址的网络站点不对搜索请求做出响应,则通过安全传输协议附加地做出对该网络站点的数据访问和 / 或控制请求,以及当通过安全传输协议用信号通知数据访问和 / 或控制请求已经失败的事实时,确认所寻址的网络站点不活动。

2. 如权利要求 1 所述的方法,其中,经由网络站点的网络服务器,访问与网络站点相关的信息。

3. 如权利要求 2 所述的方法,其中,所述信息包括 XML 文件形式的设备描述和服务描述。

4. 如权利要求 3 所述的方法,其中,利用针对所述网络站点的设备描述或服务描述来做出对 XML 文件的 HTTP 访问。

5. 如前述权利要求之一所述的方法,其中,差错保护数据传输协议用于数据访问。

6. 如权利要求 5 所述的方法,其中对应于超文本传输协议的 HTTP 协议用作差错保护数据传输协议。

7. 如权利要求 6 所述的方法,其中,通过 HTTP 头访问或 HTTP 获取访问进行数据访问,和 / 或通过 HTTP 邮递访问发送控制请求。

8. 如权利要求 1 至 4 之一所述的方法,其中,对应于简单服务发现协议的 SSDP 协议用于搜索请求。

9. 如权利要求 1 至 4 之一所述的方法,其中,分布式站点的网络是基于通用即插即用 UPnP 的网络。

10. 一种用于检测分布式站点网络中网络站点的活动的设备,包括:用于检查一个网络站点的活动的装置,用于检查的所述装置通过不受保护的传输协议来执行对网络站点的搜索请求,其中至少一个安全传输协议可用于数据访问和 / 或控制网络站点,其特征在于,所述设备还包括:

如果所寻址的网络站点不对搜索请求做出响应,则通过安全传输协议附加地做出对该网络站点的数据访问和 / 或控制请求的装置,以及

当通过安全传输协议用信号通知数据访问和 / 或控制请求已经失败的事实时,确认所寻址的网络站点不活动的装置。

11. 如权利要求 10 所述的设备,其中,对应于超文本传输协议的 HTTP 协议用作差错保护数据传输协议。

12. 如权利要求 13 所述的设备,其中,通过 HTTP 头访问进行数据访问,和 / 或通过 HTTP 邮递访问发送控制请求。

13. 如权利要求 10 到 12 之一所述的设备,其中,对应于简单服务发现协议的 SSDP 协议用于所述搜索请求。

14. 如权利要求 10 到 12 之一所述的设备,其中,分布式站点的网络是基于通用即插即用 UPnP 的网络。

在分布式站点网络中设备活动检测的方法,以及执行该方法的网络站点

技术领域

[0001] 本发明涉及局域网的技术领域,尤其是家庭网络。

背景技术

[0002] 各种家庭网络标准可用于家庭领域中设备的网络互联。由微软领导的公司协会,尤其是计算机行业的公司,已经开始倡导基于现有因特网协议(IP)上的网络控制软件的规范。该网络系统以缩写 UPnP(通用即插即用)而知名。该 UPnP 系统基于一系列标准化网络协议和数据格式,并用于控制来自不同制造商的设备(包括计算机行业的典型设备(例如 PC,路由器、打印机和扫描机),家庭娱乐电子设备,以及大型家用电器和建筑管理系统领域的家庭设备)。在有或没有“驻地网关”中央监控的情况下,通过基于 IP 的网络来将这些设备联网。在这种情况下,网络系统是即插即用系统的形式,即在没有同用户进行任何交互的情况下配置网络。与控制点相对应的控制点设备能在网络中自主地找到设备。支持 IP 通信的所有类型的介质可以用作物理传输媒介,即例如以太网、火线和无线传输系统(例如蓝牙和无线局域网等)。使用标准化技术,例如 IP、UDP(对应于用户数据报协议)、多播、TCP(对应于传输控制协议)、HTTP(对应于超文本传输协议)、XML(对应于扩展标记语言)、SOAP(对应于简单对象访问协议)和 SSDP(简单服务发现协议)。

[0003] UPnP 规范描述了如何设置基于 UPnP 标准的设备,以及如何监控这些设备。该规范的基本思想之一是可以过标准的网络浏览器操作任何 UPnP 设备。为了达到这个目的,每个 UPnP 设备具有存储用于设备操作的 HTML 页面(所谓的呈现页面)的网络服务器。

[0004] 在 UPnP 网络系统中,执行确认过程,其中,网络中的新站点必须登录,以及断开的站点必须从网络中注销。这通过根据 SSDP 协议的特定消息来完成。UPnP 标准向各个网络站点提供有规律地通知它们的活动(activity)。这通过 SSDP 消息,更具体地,“ssdp:alive”来完成,网络站点必须至少每 1800 秒发送一次该消息。这和半小时的最少会话持续时间相对应。

[0005] 当设备离开网络时,它们应该也发送“ssdp:byebye”类型的注销消息。当注销消息发出时,控制点设备可以利用该消息快速地确认 UPnP 设备已经离开网络。此外,控制点设备也可以在所定义的重复间隔之后利用任何活动确认消息的缺乏来识别相应的网络站点已经切换至不活动状态。实际上,当切断所述设备时,它们可以发送 ssdp:byebye 消息,这样,原则上这些设备不再在网络中(即使所述设备仍与该网络连接)。然而,如果所述设备通过拔出电缆的方式与网络断开,那么出于物理原因而不再可能发送已经提及的注销消息。然而,由于要观察的最小时间段是相当长的半个小时,所以对于用户来说,这可能有不可预料反应。尤其是如果用户希望使用已经有一段时间被切换到不再活跃的设备,但活动确认消息在最大可允许时间段内还没有消失,那么理想地,网络不响应。这是因为,一旦访问了想象中存在的设备,就会发现该设备不再活跃,并且该确认消息就会突然从用户菜单中消失,这就会困扰用户。

发明内容

[0006] 本发明的目的是在未识别的设备注销消息出现时,提供更用户友好的响应。

[0007] 根据本发明的解决方案是基于控制点设备有规律地以短时间间隔将搜索请求发送至网络站点。根据 UPnP 规范,这是可允许的,并且对于这种搜索请求没有最小时间间隔。例如,这样可以每 5、10 或 15 秒发送搜索请求。所寻址网络站点必须对这种搜索请求做出响应。如果各个设备没有响应,那么控制点设备可以发现那些设备离开了网络。

[0008] 然而,在该上下文中,必须记住搜索请求和关联响应都是作为 UDP 分组发送的,也就是说,不保证分组也将实际到达被访地址。UDP 是不受保护的数据传输协议。尤其是当各个设备通过无线链路同网络进行通信时,这是个问题。无可否认地,该问题可以通过以下方法解决:其中,对搜索请求的单个响应的缺失不会造成设备不活动的假设,只有在两个或更多响应缺失时才会做出该假设。然而,这有以下缺点:要花更长的时间来识别设备是否实际上从网络注销。

[0009] 为了解决该附加问题,本发明提供:在对搜索请求的响应缺失的情况下,另外地使用差错保护传输协议来检查该设备是否仍然活跃。SSDP 协议和根据 UPnP 规范关于设备识别的整个章节不可否认地不支持该措施,但能够在 UPnP 规范内以简单的方式检查设备的存在。根据该规范,每个 UPnP 设备具有网络服务器,通过该网络服务器可以访问与该设备相关的信息。例如,该信息包括所谓的设备描述和服务描述。这两者都是 XML 文件。通过 HTTP 协议专有地访问这些文件。由于 HTTP 协议基于 TCP 协议,所以 HTTP 协议是差错保护协议。因为当设备登录时,将 URL(对应于 UPnP 设备的设备描述的统一资源定位符)传输至所有的网络站点,所以在任何情况下控制点设备均知道 URL。因此,控制点设备可以在已经描述的对搜索请求的响应缺失的情况下,利用对设备描述或某个其它现有文件的 HTTP 访问来确定该设备在网络中是否还活跃。可选地,也可以将控制请求发送至要控制的设备,并且这也是通过 HTTP 进行发送。如果可以建立 HTTP 链路,那么该设备仍然是活跃的,但如果不再可以建立 HTTP 链路,那么就从网络中移除该设备。

[0010] 因此,这克服了上述用户不友好的响应。

[0011] 通过在从属权利要求中所描述的措施,可以有根据本发明的方法和根据本发明的装置的有利发展和改进。

[0012] 如果使用 HTTP 头访问(HTTP head access)进行数据访问,那么其所具有的优势在于只需要转移最少数量的数据。当通过发送控制请求来执行活动检测时,使用 HTTP 邮递访问(HTTP post access)是有利的。在这种情况下,对于控制请求来说,不改变被寻址设备的状态也是有利的。

附图说明

[0013] 在下面的描述中,将详细描述本发明的示例性实施例,并附图说明,其中:

[0014] 图 1 示出了具有两个网络连接切换单元的网络示例的结构;

[0015] 图 2 示出了根据本发明用于网络站点的软件协议的概观;

[0016] 图 3 示出了在 UPnP/AV 结构 0.8.3 的基础上两个网络站点之间用于 AV 数据传输的轮廓图;

[0017] 图 4 示出了根据本发明的网络站点的重要软件组件 ;以及

[0018] 图 5 示出了可以通过其检查网络站点活动的程序的流程图。

具体实施方式

[0019] 图 1 示出了具有五个网络站点 12-16 和两个网络连接切换单元 10、11 的家庭网络的示例。网络连接切换单元 10、11 和网络站点 12 到 15 之间的总线连接是基于以太网技术（特别是 100 Base/TX 以太网）的。根据 IEEE802. 11b, 不使用电线（例如通过无线 LAN），将网络站点 16 与网络连接切换单元 10 相连接。两个网络连接切换单元 10 和 11 之间的连接也是基于以太网技术的。针对每个网络连接切换单元 10、11 示出四个网络连接点（也称为端口）。该图没有示出在各个网络站点中的以太网接口、或网络连接切换单元中的以太网接口。

[0020] 已经在引言中提到的以太网总线系统的 100 Base/TX 变体被用作网络中数据传输的传输系统。虽然可以使用不同的变体作为其它应用中的传输系统，但是对所选择的应用来说，认为该变体是合适的。例如，所谓的 1000 Base/T 或 1000 Base/SX 或 1000 Base/LX 是可用于更高的数据率。在这种情况下，最后两个变体是基于光学玻璃纤维技术的。图 1 中所示出的网络是基于 UPnP 的，即各个网络站点都是根据 UPnP 标准而设计的。

[0021] 由于传输帧可能丢失，所以以太网总线系统不为更高的协议层提供受到保护的链路。这不适于大量的用户数据传输，因此经常通过更高协议层来保护该传输。对于 UPnP 网络系统，将 IP 协议（对应于用于数据通信的 OSI 层模型的网络层层级处的因特网协议）设置为下一更高协议层级。仅通过建立在数据链路层上的 TCP 协议来实现该数据链路层。对于不再是以以太网标准的组成部分的两个协议层级来说存在特定的标准，对于本发明的公开，应当参考该标准。

[0022] 各个网络站点需要升级的协议栈用于使用 UPnP 网络的通信。该协议栈在图 2 中示出。在最低的层级设置两个以太网协议层级：以太网 PHY 和以太网 MAC。前面提到的协议层级 IP 位于这两个层级之上。然后也将 UDP 协议设置在传输层层级上，并用于与设备标识（设备发现）相关联的所有消息的传输。HTTP 协议的特定版本位于 UDP 协议之上。这是 HTTPMU 协议（基于 UDP 的 HTTP 多播）。经由较低的 UDP 和 IP 协议层级，继续传递诸如此类的 HTTP 消息，并在按比例的基础上进行寻址。

[0023] SSDP 协议也设置在 HTTPMU 协议层级之上。除了 UDP 协议之外，也使用 TCP 协议，该 TCP 协议意欲用于所有其他 UPnP 消息传输（尤其是针对设备和服务描述的）、用于设备控制、以及用于事件信令。HTTP 协议位于 TCP 协议之上，位于 HTTP 协议之上的 SOAP 协议处于 SSDP 协议层级，SOAP 协议先前被称为简单对象访问协议。可以使用 SOAP 协议来执行针对其它设备的与远程程序呼叫（PRC）相对应的功能呼叫。此外，也可以实现 GENA 协议（对应于一般事件通知结构），该协议允许在其它站点中登记事件消息。

[0024] 可以在 UPnP 规范中找到 UPnP 网络系统中使用的完整的协议结构（可以通过 www.upnp.org 获得）。

[0025] 在 UPnP 标准化的过程中，也制定出用于网络用户站点之间的 AV 数据（音频/视频数据）传输的规范，并在 2002 年六月完成。该规范的确切标题是：UPnP-AV-Architecture：0. 83, 日期 2002 年 6 月 12 日。在该规范中定义了 3 种不同类型的设备用于 AV 数据的传输。

第一,所谓的媒体服务器,即选作 AV 数据源的设备。第二,存在媒介再现器设备类型,该类型表示用作 AV 数据的数据接收器的设备。第三,也将控制点设备提供作为特定设备类型,并在下文中称作控制点设备。通常地,例如,将用于 AV 设备的通用远程控制器用作控制点设备。然而,可选地,个人计算机也可以在网络中执行该任务,或具有遥控器的 TV 也可适于用作控制设备。

[0026] 控制点设备与另外两个 UPnP 设备进行通信,这两个设备可以用作所期望数据链路的数据源和数据接收器。控制点设备将针对 AV 链路的两个设备进行初始化和配置,从而也可以将所期望的数据流应用其中。这样,典型地,控制点设备的任务是在两个网络用户之间建立 AV 链路,有可能改变这两个设备的设置,并且一旦传输了所期望的 AV 数据流来再次覆盖链路,即在 AV 链路中请求两个设备删除表征该链路的数据。

[0027] 图 3 示出了 AV 链路所需要的网络站点的基本细目表。媒体服务器设备包含或访问 AV 数据流,例如在本地存储或从外界接收该 AV 数据流。媒体服务器设备访问 AV 数据,并能够经由网络将相关联的 AV 数据流传输至另一个网络站点。在这种情况下,使用适于在网络中使用的传输介质的传送协议来传输 AV 数据流。针对每个可能的资源,在内容目录服务中明确定义由媒体服务器支持的数据传输格式。典型地,可以将媒体服务器设备类型与下列设备之一相关联:数字录影机、CD/DVD 播放器、照相机、可携式摄像机、PC、机顶盒、卫星接收器、盒式录音机等。通常地,,根据媒体服务器中的 UPnP 标准来执行用于内容目录的模块,以选择特定的 AV 内容。此外,也存在被称作连接管理器的模块,并且通过该模块,控制点设备与媒体再现器进行通信,同时建立链路。

[0028] 媒体再现器设备接收从媒体服务器处传输的 AV 数据流,并将其作为视频信息或音频信息输出。同样,当建立链路时,媒体再现器设备也包含用于与控制点设备进行通信的连接管理器模块的实现。在媒体再现器设备中实现模块再现控制。该模块接收命令,用于调整再现特征(例如音量、音调、图片清晰度、对比度、亮度、颜色等),并实现该命令。在家庭网络中,应该将媒体再现器设备类型分配到作为设备示例所提及的电视、立体声放大器和 MP3 播放器。取决于所实现的传输格式,媒体服务器或媒体再现器也具有 AV 传送服务,用于控制数据传输和再现(例如播放、停止和快进等)。控制点设备协调媒体服务器和媒体再现器之间的数据传输。该控制点设备也通常用于实现操作者的控制命令,并将控制命令传送至 AV 链路上合适的设备。具体地,这种示例包括命令:播放、停止、暂停、快进和快速返回。正如引言中所提到的,设计控制点设备用于找到和控制标准 UPnP 设备。这将在下文中详细地描述。首先,将参照图 4 解释 UPnP 设备的标准软件组件。参考号 35 表示协议栈,包括协议层级以太网、IP 和 TCP。参考号 31 与根据 UPnP 设备描述存储 UPnP 设备描述的软件组件相对应。参考号 32 表示与 UPnP 事件相对应的管理事件消息的软件组件。UPnP 设备的一个标准组件也是网络服务器 33。参考号 34 表示 UPnP 发现单元。正如更详细地所描述的,这允许 UPnP 控制点设备识别网络中的其它设备。在这些块上,UPnP 应用程序也由参考号 30 来表示。所有这些单元是 UPnP 设备中的标准组件,并在 UPnP 规范中详细地描述。

[0029] UPnP 发现单元用于允许 UPnP 设备在网络中被发现 - 因为一旦发现这些 UPnP 设备才能控制它们。原理上,该单元操作如下:

[0030] 设备发送“发现消息”作为所谓的多播 UDP 分组。已经提到的 HTTPPMU 协议用于该目的。原理上,多播数据分组的不同之处是将它们传输到网络中的所有设备。各个网络

站点可以登记它们特定的地址以用于接收这样的多播分组。原理上,存在两种类型的发现消息:

[0031] 1. 所谓的广告消息。一旦设备连接至网络,它应该发送广告消息。根据 SSDP 协议,这是“ssdp:alive”消息。该消息通知网络中的其它设备:该设备现在在网络中是活跃的。然而,一旦该设备在网络中使它自己为其它设备所知,它应该有规律地发送这些广告消息。该控制点设备可以利用广告消息的缺乏来识别该设备已经从网络中移出。针对广告消息的重复传输的最大会话持续时间是 1800 秒,即半个小时。

[0032] 2. 搜索消息:为了搜索设备,控制点设备可以发送搜索请求。根据 SSDP 协议,“ssdp:discover”消息用于该目的。接收诸如此类消息的 UPnP 设备必须对该消息做出响应,因而通知发送方它存在。

[0033] 3. 最后,还提到第三种广告消息 - 所谓的注销消息,该消息根据 SSDP 协议被称作“ssdp:byebye”。当从网络中移除设备时,该设备要发送这些消息。实际上,当这些设备以正常方式关闭时,它们可以这样做。只有当通过拔出网络电缆使它们从网络中分离时,因为物理原因才不能发送注销消息。

[0034] 下面将参照图 5 解释在分布式站点网络中用于检测设备活动的根据本发明的方法的一个示例性实施例。

[0035] 图 5 示出了在控制点设备中为了该目的运行的程序的流程图。该程序开始具有参考号 50。参考号 51 标记了检查,其中执行关于 ssdp:byebye 消息是否已经到达要测试的设备的检查。如果是这种情况,那么不需要执行进一步的处理步骤 52 至 55,程序直接跳到步骤 56,其中将所述设备划分为已经从网络中注销。该程序将以程序步骤 58 结束。如果在检查 51 中没有发现所述设备的注销消息,那么在程序步骤 52 之后执行针对所述设备的搜索请求。为了这个目的,控制点设备将 ssdp:discover 消息发送至所述设备。然后,问题 53 检查该搜索请求是否在特定时间段内由所寻址的网络站点所应答。如果是,则在程序步骤 57 中宣布该网络站点为活跃的网络站点。在这种情况下,可以在网络站点表中设置适合的条目。然后该程序再次以程序步骤 58 结束。

[0036] 如果在问题 53 中发现没有接收到对于搜索请求的响应,那么在程序步骤 54 中,利用针对所述网络站点的设备描述来做出对 XML 文件的 HTTP 访问。当该网络站点登录时,通知用于该文件的 URL,从而控制点设备可以仅从关联表中得到该信息。HTTP 头呼叫的示例表示如下:

[0037] 头 /upnp/device_description.xml HTTP/1.1

[0038] 主机:本地 IP 地址站点 3

[0039] 可选地,也可以做出 HTTP 获取呼叫。

[0040] 例如,可以将 UPnP 命令获取状态作为控制请求通过 HTTP 邮递访问发送至网络站点。

[0041] 问题 55 检查是否发送回所期望的文件。如果所述站点不活动,就不可能与之建立任何 TCP 链路。所述网络站点将仅据此来识别 HTTP 访问已经失败。然后在程序步骤 56 中,跟随着针对网络站点的表中条目,以便通知网络站点已经从网络注销或者在网络中不活动的事实。之后,程序又一次在程序步骤 58 中结束。

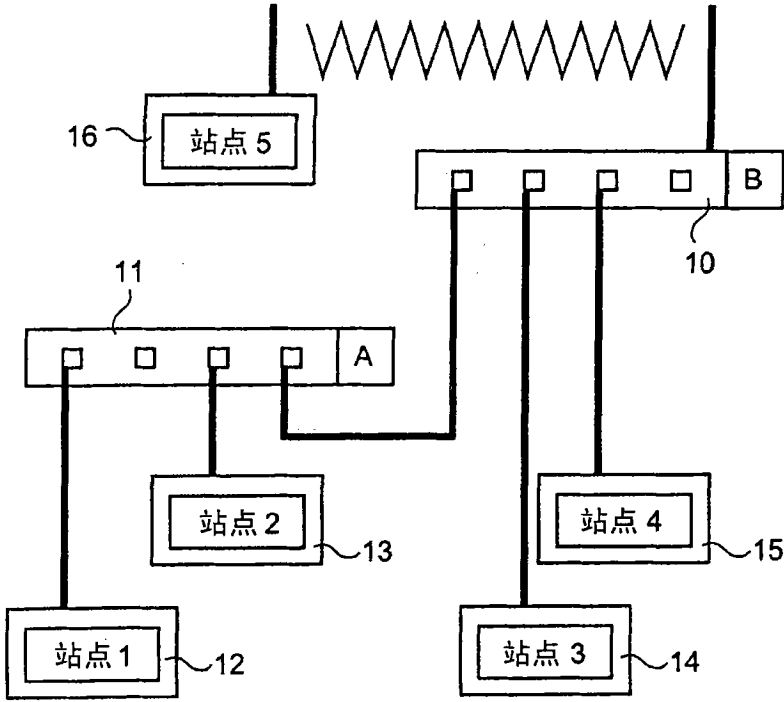


图 1

SSDP		SOAP	GENA
HTTPMU (多播)	HTTPU (单播)	HTTP	HTTP
UDP		TCP	
IP			
以太网 MAC			
以太网 PHY			

图 2

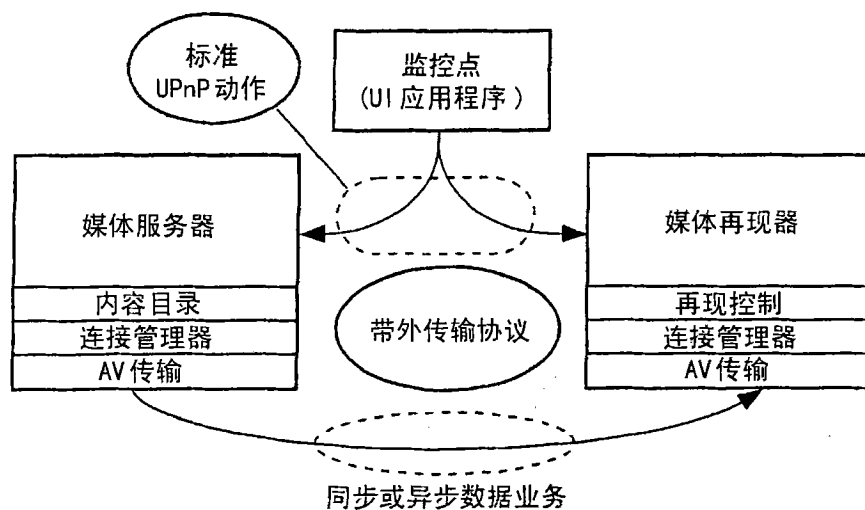


图 3

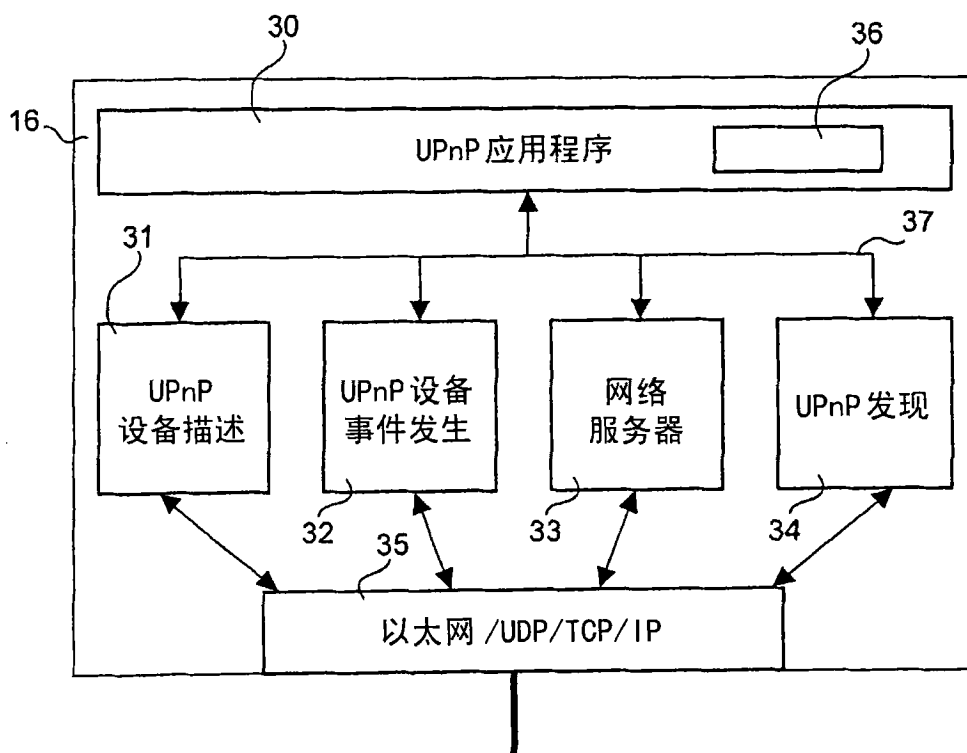


图 4

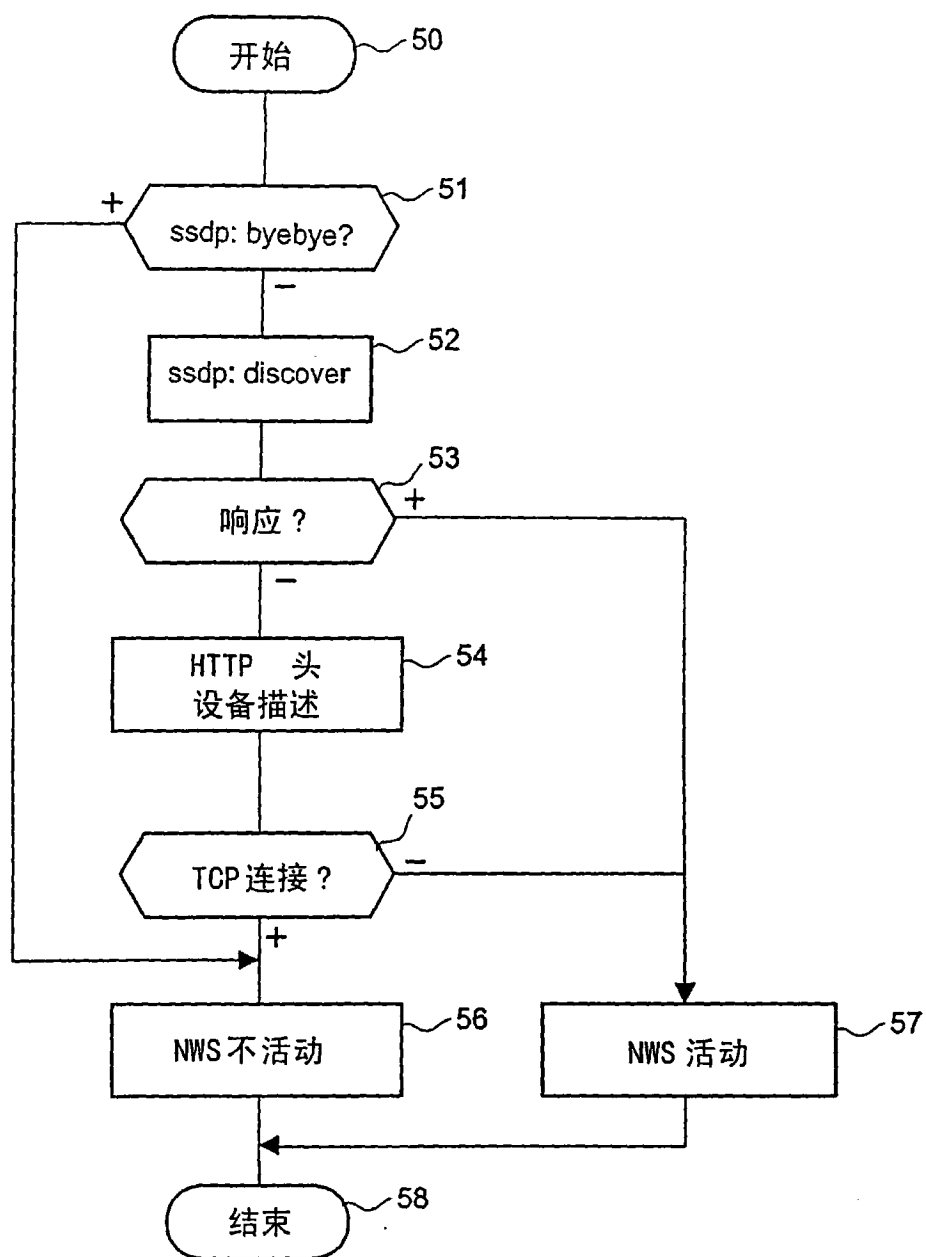


图 5