[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/24
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 200410016195.5

[43] 公开日 2004 年 12 月 29 日

[11] 公开号 CN 1558606A

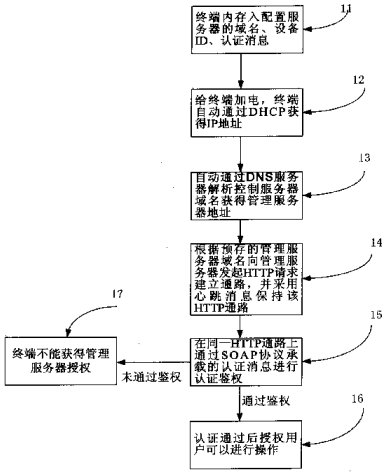
[22] 申请日 2004.2.10
[21] 申请号 200410016195.5
[71] 申请人 UT 斯达康通讯有限公司
地址 310012 浙江省杭州市杭州文一路 129 号益乐工业园 2－3 号楼
[72] 发明人 李 朋 王宏晔

[74] 专利代理机构 上海翼胜专利事务所
代理人 翟 羽
权利要求书 5 页 说明书 13 页 附图 4 页

[54] 发明名称 网络终端自动配置方法

[57] 摘要

一种网络终端自动配置方法，包括以下步骤：a. 预先在终端设备内存入管理服务器的域名、终端设备 ID、认证消息等信息；b. 给终端加电，终端自动获取 IP 地址；c. 根据预存的管理服务器域名向管理服务器发起 HTTP 请求；d. 建立连接后，终端定期发送心跳消息保持终端与管理服务器之间的 HTTP 连接；e. 在同一 HTTP 通路上通过 SOAP 协议承载的认证消息进行认证鉴权；f. 当认证通过后，授权用户可以进行配置文件的自动下载，软件版本的自动升级等工作。 这种方法可使网络终端设备加电、联网后无需配置即可使用。



ISSN1008-4274

知识产权出版社出版

1、一种网络终端自动配置方法，其特征在于主要包括以下步骤：A.在终端设备内存入管理服务器的域名、终端设备 ID、认证密钥；B.给终端加电联网后，终端自动获取 IP 地址；C.根据预存的管理服务器域名向管理服务器发起 HTTP 请求；D. 建立连接后，在同一 HTTP 通路上通过 SOAP 协议承载的认证消息进行认证鉴权；E.当认证通过后，授权用户可以进行配置文件的自动下载。

2、根据权利要求 1 所述的网络终端自动配置方法，其特征在于步骤 f 所述的配置文件的自动下载还包括以下步骤：g.终端设备在这一连接上通过认证后，向管理服务器申请配置文件；h.管理服务器根据终端设备的类型和服务模式返回相应的配置文件地址；i.终端可以通过访问这一地址取回相应的配置文件。

3、根据权利要求 1 所述的网络终端自动配置方法，其特征在于步骤 e 所述的配置文件的自动下载还可以由管理服务器通过命令下发要求终端更新其配置文件。

4、根据权利要求 1 所述的网络终端自动配置方法，其特征在于还包括以下软件版本的自动升级步骤：j.终端首先将现有的软件版本信息、硬件版本等发送到管理服务器；k.管理服务器根据硬件版本、服务模式向终端返回最新的软件版本信息；l.终端进行版本比

较，如果需要更新，即向管理服务器请求新版本地址，管理服务器返回相应的新版本的地址，再由终端通过 HTTP 访问这一地址，取回相应的新版本。

5、根据权利要求 1 所述的网络终端自动配置方法，其特征在于在用户终端通过认证后，可由终端自动发起软件升级请求或由管理服务器下发命令要求终端发起升级。

6、根据权利要求 1 所述的网络终端自动配置方法，其特征在于管理服务器通过步骤 d 建立的同一条 HTTP 通路可以向终端下发命令，接受终端的事件或告警上报。

7、根据权利要求 6 所述的网络终端自动配置方法，其特征在于采用 GENA 作为事件上报协议，采用订阅鉴权机制保证消息只发向授权的管理服务器。

8、根据权利要求 1 所述的网络终端自动配置方法，其特征在于终端设备 ID 是统一定义的，通过这一 ID 管理服务器可以分析出终端设备的类型，终端设备供应商，和标识终端设备唯一性的地址符。

9、根据权利要求 1 至 8 中任一权利要求所述的网络终端自动配置方法，其特征在于配置文件以 XML 的形式存储和传送。

10、根据权利要求 1 至 8 中任一权利要求所述的网络终端自动配置方法，其特征在于采用 SSL 对 HTTP 进行加密。

11、根据权利要求 1 至 8 中任一权利要求所述的网络终端自动配置方法，其特征在于采用分级采集、委托管理的架构，各类终端首先汇集到一级管理服务器，一级管理服务器进行事件收集、配置下发、控制代理等功能，可根据网络状况，灵活配置管理服务器层次。

12、一种网络终端自动配置方法，其特征在于主要包括以下步骤：a.在终端设备内存入管理服务器的域名、终端设备 ID、认证密钥；b.给终端加电联网后，终端自动获取 IP 地址；c.根据预存的管理服务器域名向管理服务器发起 HTTP 请求；d.建立连接后，终端定期发送心跳消息保持终端与管理服务器之间的HTTP连接；e.在同一 HTTP 通路上通过 SOAP 协议承载的认证消息进行认证鉴权；f.当认证通过后，授权用户可以进行配置文件的自动下载。

13、根据权利要求 12 所述的网络终端自动配置方法，其特征在于步骤 f 所述的配置文件的自动下载还包括以下步骤：g.终端设备在这一连接上通过认证后，向管理服务器申请配置文件；h.管理服务器根据终端设备的类型和服务模式返回相应的配置文件地址；i.终端可以通过访问这一地址取回相应的配置文件。

14、根据权利要求 12 所述的网络终端自动配置方法，其特征在于步骤 e 所述的配置文件的自动下载还可以由管理服务器通过命令

下发要求终端更新其配置文件。

15、根据权利要求 12 所述的网络终端自动配置方法，其特征在于还包括以下软件版本的自动升级步骤：j.终端首先将现有的软件版本信息、硬件版本等发送到管理服务器；k.管理服务器根据硬件版本、服务模式向终端返回最新的软件版本信息；l.终端进行版本比较，如果需要更新，即向管理服务器请求新版本地址，管理服务器返回相应的新版本的地址，再由终端通过 HTTP 访问这一地址，取回相应的新版本。

16、根据权利要求 12 所述的网络终端自动配置方法，其特征在于在用户终端通过认证后，可由终端自动发起软件升级请求或由管理服务器下发命令要求终端发起升级。

17、根据权利要求 12 所述的网络终端自动配置方法，其特征在于管理服务器通过步骤 d 建立的同一条 HTTP 通路可以向终端下发命令，接受终端的事件或告警上报。

18、根据权利要求 17 所述的网络终端自动配置方法，其特征在于采用 GENA 作为事件上报协议，采用订阅鉴权机制保证消息只发向授权的管理服务器。

19、根据权利要求 12 所述的网络终端自动配置方法，其特征在于终端设备 ID 是统一定义的，通过这一 ID 管理服务器可以分析出

终端设备的类型，终端设备供应商，和标识终端设备唯一性的地址符。

20、根据权利要求 12 至 19 中任一权利要求所述的网络终端自动配置方法，其特征在于配置文件以 XML 的形式存储和传送。

21、根据权利要求 12 至 19 中任一权利要求所述的网络终端自动配置方法，其特征在于采用 SSL 对 HTTP 进行加密。

22、根据权利要求 12 至 19 中任一权利要求所述的网络终端自动配置方法，其特征在于采用分级采集、委托管理的架构，各类终端首先汇集到一级管理服务器，一级管理服务器进行事件收集、配置下发、控制代理等功能，可根据网络状况，灵活配置管理服务器层次。

网络终端自动配置方法

技术领域

本发明涉及通信领域，特别是有关一种网络终端的自动配置方法。

背景技术

近年来逐渐浮出水面的 NGN（Next Generation Network）网络将完全不同于传统网络，智能节点已经移至网络边缘，将来会有大量的智能终端部署在用户的家中。任何新业务的推出都必然要求终端的更新和升级。管理、升级、配置必将变为运营商选择方案，降低运营成本的核心问题。

目前用 SNMP 管理终端设备的方式已越来越难以解决日益复杂的网络终端设备。SNMP 是简单网络管理协议的缩写，它是由 Internet 工程任务组织(Internet Engineering Task Force)(IETF)的研究小组为了解决 Internet 上的路由器管理问题而提出的，提供了一

种从网络上的终端设备中收集网络管理信息的方法，也为终端设备向网络管理中心报告问题和错误提供了一种方法。这种采用 SNMP 方案进行配置的网络终端的配置方案，无法穿越防火墙，亦不可完成终端的自动配置。

因为 Internet 地址资源正在迅速被耗尽，大多数的家庭网络都使用网络地址转换（NAT）技术建立了一个网关。NAT 是 Internet 工程任务组（IETF）制订的一种标准，它允许私有网络中的多台 PC 或终端设备共享一个全球唯一的公共地址（所使用私有地址的范围为 10.0.x.x、192.168.x.x 和 172.x.x.x。）作为对 IP 地址短缺的一种临时补救措施，NAT 可以很好地完成很多工作：例如 Windows XP 的 Internet 连接共享就使用 NAT，正如 DSL 和线缆调制解调器很多网关设备等所做的一样。

但问题是:NAT希望所有的网络应用程序都以一种标准方式(即在数据包头中使用 IP 地址）进行通信，有些网络程序预计到 NAT 的存在。他们使用了 NAT 无法转换的嵌入式 IP 地址，如 Windows XP 中标准安装的聊天软件 Windows Messenger。Windows Messenger 虽然具有 IP 电话及视频聊天功能，但这种功能无法经由使用 NAT 的宽带路由器使用。这是由于在使用此项功能时，Windows Messenger 在数据部分也嵌入了 IP 地址的缘故。在 NAT 功能中，虽然位于 IP

数据包头部的收信方及发信方的IP地址可以更换，但数据内的地址无法更换，因此前后不统一，无法进行通信。

综上所述，目前的网络终端管理主要存在以下几大问题：不能够传越防火墙及NAT转化，对终端设备要求高。不能够自动发现管理服务器。不能够实现对大量的终端设备，复杂拓扑结构的统一管理。

针对以上问题，目前分别推出了一些解决方案，如可以透过NAT的NAT穿越技术；为跨平台系统而开发的SOAP（Simple Object Access Protocol）简单对象访问协议，这是一种在分散或分布式的环境中交换信息的简单的协议；XML（Extensible Markup Language）是作为HTML的新一代版本而开始用于各种用途的表述语言；HTTP的扩展协议GENA（General event Notification Architecture）等，但是目前还没有形成完整的解决方案。

发明内容

本发明的目的在于提供一种网络终端自动配置方法，以克服上述现有技术的不足，解决NGN网络中终端的自动配置、管理、软件升级问题。使得网络终端设备加电，联网后无需配置即可使用。

为实现上述目的，本发明提供一种网络终端自动配置方法，包

括以下步骤：A.在终端设备出售给客户以前，在终端设备内存入管理服务器的域名、终端设备ID、认证密钥等信息；B.在终端卖给用户后，用户给终端加电，终端获取IP地址；C.根据预存的管理服务器域名向管理服务器发起HTTP请求；D. 建立连接后，在同一HTTP通路上通过SOAP协议承载的认证消息进行认证鉴权；E.当认证通过后，授权用户可以进行配置文件的自动下载，软件版本的自动升级等工作。

所述的网络终端自动配置方法，包括以下步骤：g.终端设备在这一连接上通过认证后，向管理服务器申请配置文件；h.管理服务器根据终端设备的类型和服务模式返回相应的配置文件地址；i.终端可以通过访问这一地址取回相应的配置文件。

进一步的，所述的配置文件的自动下载还可以由管理服务器可以通过命令下发要求终端更新其配置文件。

步骤f所述的软件版本的自动升级还包括以下步骤：j.终端首先将现有的软件版本信息，硬件版本等发送到管理服务器，k.管理服务器根据硬件版本，服务模式向终端返回最新的软件版本信息；l.终端进行版本比较，如果需要更新，向管理服务器请求新版本地址，管理服务器返回相应的新版本的地址，终端通过HTTP访问这一地址，取回相应的新版本。

进一步的，也可由终端自动发起软件升级请求或由管理服务器下发命令要求终端发起升级。

此外，本发明的网络终端自动配置方法采用 GENA 作为事件上报协议，采用订阅鉴权机制保证消息只发向授权的管理服务器。终端设备 ID 是统一定义的，通过这一 ID 管理服务器可以分析出终端设备的类型，终端设备供应商，和标识终端设备唯一性的地址符。其配置文件以 XML 的形式存储和传送。管理服务器制定了心跳消息，定时发送以监测终端设备的运行状态。管理服务器采用分级采集、委托管理的架构，各类终端首先汇集到一级管理服务器，一级管理服务器进行事件收集、配置下发、控制代理等功能，可根据网络状况，灵活配置管理服务器层次。

本发明的另一目的在于提供一种能够穿透防火墙的网络终端自动配置方法。一些防火墙会定时检查 NAT，对没有流量的 NAT 条目进行清除从而拆除 HTTP 通路。本发明通过终端定时发送心跳消息刷新 NAT，防止被防火墙删除而断开 HTTP 通路的方式穿越防火墙与管理服务器通信。

为实现上述目的，本发明提供一种网络终端自动配置方法，包括以下步骤：a.在终端设备内存入管理服务器的域名、终端设备 ID、认证密钥；b.给终端加电联网后，终端自动获取 IP 地址；c.根据预

存的管理服务器域名向管理服务器发起 HTTP 请求；d.建立连接后，终端定期发送心跳消息保持终端与管理服务器之间的HTTP连接；e.在同一HTTP通路上通过SOAP协议承载的认证消息进行认证鉴权；f.当认证通过后，授权用户可以进行配置文件的自动下载。

本方案的部署灵活，与网络的实际环境相耦合，更具灵活性。可穿越防火墙，有完善的安全加密机制。采用自动发现管理服务器模式，可智能搜寻管理服务器。动态更新配置，在城域网环境发生变化时，无需终端进行人工改动。可进行远程访问终端设备，动态通报故障给管理服务器，这种访问和通报可进行安全限制。解决了NGN网络中各类智能终端的自动配置、管理和软件自动升级问题。克服了现有技术在实际网络拓扑中遇到的问题。主要优点有以下几点：

1. 采用 HTTP 作为协议的承载，利用 XML 描述协议的具体内容，这样的方案可以克服现有 SNMP 方案中无法穿越防火墙的问题，并减少了管理包的流量，简单易于实现，减轻终端的运行负荷。
2. 通过预先存入终端管理服务器的域名，解决了终端设备分散部署时自动发现管理服务器的难题。终端设备启动时首先通过 DHCP 获得地址，然后自动通过 DNS 服务器解析管理服

务器域名获得管理服务器地址。

3. 终端设备向管理服务器发起 HTTP 请求，建立 HTTP 通路后，终端定时发送心跳消息刷新 NAT，以防止被防火墙删除而断开 HTTP 通路，这一方式可以穿越防火墙与管理服务器通信，解除了对管理服务器部署上的限制，使得管理服务器部署更加灵活。连接管理服务器过程有鉴权机制，可以防止恶意攻击。

4. 所有配置文件以 XML 的形式存储和传送，易于扩展，使得协议与平台无关，易于跨平台的操作。

5. 采用 SOAP 作为远程管理协议，同样具备跨平台的优势。终端部分只需很少的资源即可运行，在终端的远程控制能力和相应的管理负荷之间取得相应的平衡。具有可靠的安全机制保证通信的可靠性和防攻击。

6. 采用 GENA 作为事件上报协议。终端部分只需很少的资源即可运行。采用订阅鉴权机制保证消息只发向授权的管理服务器。

7. 针对终端管理的实际问题（数量巨大，拓扑复杂等），采用分级采集、委托管理的架构，各类终端首先汇集到一级管理服务器，一级管理服务器进行事件收集、配置下发、控制代

理等功能。可根据网络状况，灵活配置管理服务器层次。

以下结合附图与实施例对本发明作进一步的说明。

附图说明

图 1 为一种参考拓扑结构的示意图。

图 2 为本发明的网络终端自动配置流程图。

图 3 为本发明的配置文件下载及软件更新流程图。

图 4 为本发明分层次配置管理服务器的示意图。

具体实施方式

有关本发明的详细说明及技术内容，现就结合附图说明如下：

首先参阅图 1，图 1 揭示了一种参考拓扑结构，从中我们可以发现，网络环境的多种多样，终端的配置也非常复杂。这就要求终端配置方案可以适应上述环境，包括穿越防火墙、自动配置、故障的自动上报等。在 NGN 网络中随着网络架构的演进，网络的智能节点广泛地分布于网络的边缘，任何增值业务没有终端的配合几乎都无法实施。所以现在的终端已不再是简单的傻终端了，终端的智能化改变了网络管理结构，终端的配置也必然更加复杂。但是，所有终端用户希望能够加电即可使用，希望是零配置。为了迎接这一

挑战，本发明提供了一种在网络环境中对终端设备的自动配置、软件的自动升级、远端控制的方案，解决了现实中 NGN 网络终端的部署和管理难题。

请参阅图 2，这是本发明的网络终端自动配置流程图。一个根据本发明的实施例在图 2 中表现为如下步骤：在步骤 11 中，终端设备在出售给客户以前，在终端设备内存入管理服务器的域名、终端设备 ID、认证 key 等信息。值得注意的是终端设备 ID 是统一定义的，通过这一 ID 管理服务器可以分析出终端设备的类型，终端设备供应商，和标识终端设备唯一性的地址符。通过这一 ID 管理服务器可以分析出终端设备的类型、终端设备供应商和标识终端设备唯一性的地址符。终端卖给用户后，在步骤 12 中，当用户给终端加电，终端自动通过 DHCP 获得 IP 地址，DHCP 提供了一种动态指定 IP 地址和配置参数的机制。这主要用于大型网络环境和配置比较困难的地方。DHCP 服务器自动为客户机指定 IP 地址，它的配置参数使得网络上的计算机通信变得方便而容易实现了,在 DHCP 请求失败时或另外一些实施例中，终端设备可以自动使用预先配置的 IP 地址。紧接着进行步骤 13，自动通过 DNS 服务器解析管理服务器域名获得管理服务器地址，DNS 服务器也叫域名服务器，它可以解析域名来获取该域名相对应的地址，这一步由网络自动完成。接下来

的步骤 14 中，终端发现管理服务器后向管理服务器发起 HTTP 请求，请求的具体的内容利用 XML 来描述，为了防止建立连接后防火墙在没有流量的情况下将这条 NAT 条目清除从而拆除 HTTP 通路。终端定时发送心跳消息以使系统能够监测终端设备的运行状态，并使得管理服务器可以通过这条 HTTP 长连接实时访问内网终端，解决了穿越 NAT 管理内网设备的问题。步骤 15 利用控制消息和控制承载相分离的原则，采用同一 HTTP 连接进行双向的 SOAP 消息传递，并通过 SOAP 协议承载的认证消息进行认证鉴权，当认证通过后，步骤 16 中授权用户可以进行配置文件的自动下载，软件版本的自动升级等工作。反之，如果未能通过鉴权，则进入步骤 17，管理服务器断开连接，拒绝进一步的操作请求。这就是本发明针对网络的实际情况，在安全上采用挑战应答机制进行鉴权，增强了网络配置的安全性。

由于本发明是采用终端设备向管理服务器发起 HTTP 请求并进行双向的 SOAP 消息传递，从而完成自动配置的任务。为了防止防火墙在没有流量的情况下将这条 NAT 条目清除从而拆除 HTTP 通路以及更好地对终端的状态进行动态监测，本发明的自动配置方案制定了心跳消息，终端定时发送以使系统能够监测终端设备的运行状态，并使得管理服务器可以通过这条 HTTP 长连接实时访问内网终

端，解决了穿越 NAT 管理内网设备的问题。这种方法对网络终端的部署没有限制，可以穿越 NAT 和防火墙，支持管理服务器和终端的双向访问。本发明采用控制消息和控制承载相分离的原则，采用同一 HTTP 连接进行双向的 SOAP 消息传递。因而本发明具有更好的跨平台性和可扩展性。

请参阅图 3，这是本发明的配置文件下载及软件更新流程图。上面提到当认证通过后，授权用户可以进行配置文件的自动下载，软件版本的自动升级等操作。其中，配置文件的下载由以下步骤组成：步骤 21 中终端设备在上面提到的连接上通过认证后，向管理服务器申请配置文件。步骤 22 中管理服务器根据终端设备的类型和服务模式返回相应的配置文件地址，这个地址一般是 URL 地址，如果配置文件是以其他方式存放的，那么这个地址也可以是终端可以找到的相应地址。步骤 23 中，终端通过访问这一地址取回相应的配置文件，从而完成配置文件的下载。这是一种终端设备主动申请配置文件下载的模式，同样管理服务器可以通过命令下发，要求终端更新其配置文件。

终端的软件升级也是一个困扰运营商和用户的问题，本发明也解决了这一问题。同上，在用户终端通过认证后，可由终端自动发起软件升级请求或由管理服务器下发命令要求终端发起升级。在步

骤 31 中，终端首先将现有的软件版本信息，硬件版本等发送到管理服务器。在步骤 32 中，管理服务器根据硬件版本，服务模式向终端返回最新的软件版本信息。终端进行版本比较，如果需要更新，则在步骤 33 中向管理服务器请求新版本地址，管理服务器返回相应的新版本的 URL 地址，终端通过 HTTP 访问这一地址，取回相应的新版本。 反之，如果不需要更新，则进入步骤 34 终端不发送请求。

管理服务器还可以通过上面建立的同一条 HTTP 通路向终端下发命令，接受终端的事件或告警上报。采用 GENA 作为事件上报协议，终端部分只需很少的资源即可运行，并采用订阅鉴权机制保证消息只发向授权的管理服务器。为了增强管理通路的安全性，本发明提供一个安全的可选项，即采用 SSL 对 HTTP 进行加密，而不用改变上层消息语义。

请参阅图 4，这是本发明分层次配置管理服务器的示意图。根据本发明的网络终端自动配置方法，可以进行分级采集、委托管理的架构，各类终端首先汇集到一级管理服务器，一级管理服务器进行事件收集、配置下发、控制代理等功能。这样就可以根据网络的复杂程度以及终端设备和管理服务器之间的适配状况，灵活配置管理服务器层次。管理服务器向上级管理服务器可以提供其他网管协议接口，如：SNMP、CORBA 等．即可完成网关协议的转化。

图 4 中描述的是一个具有二层服务管理器的网络结构，当然这仅是一个示例而已，根据需要也可以具有三层或更多层结构，管理服务器之间也可以相互联通或分别担负不同的任务。

以上所介绍的，仅仅是本发明的较佳实施例而已，不能以此来限定本发明实施的范围，即本技术领域内的一般技术人员根据本发明所作的等同的变化，例如将以上实施例中的各个步骤进行组合变化。以及本领域内技术人员熟知的改进、变化，都应仍属于本发明专利涵盖的范围。

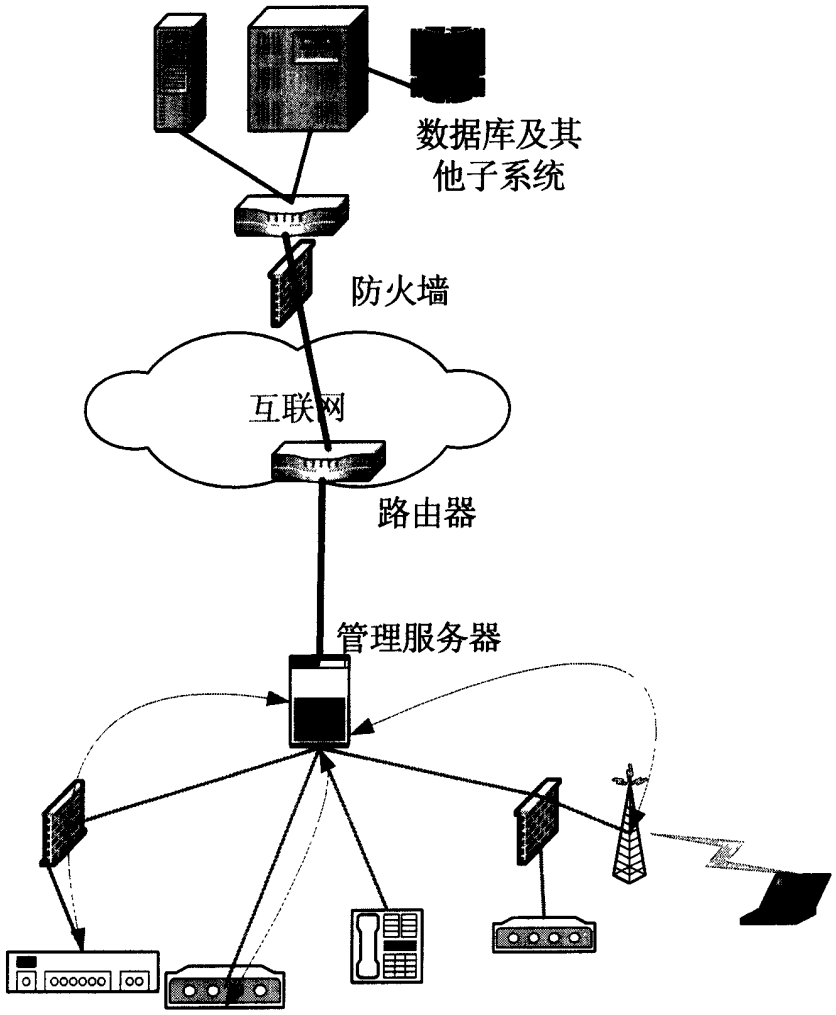


图 1

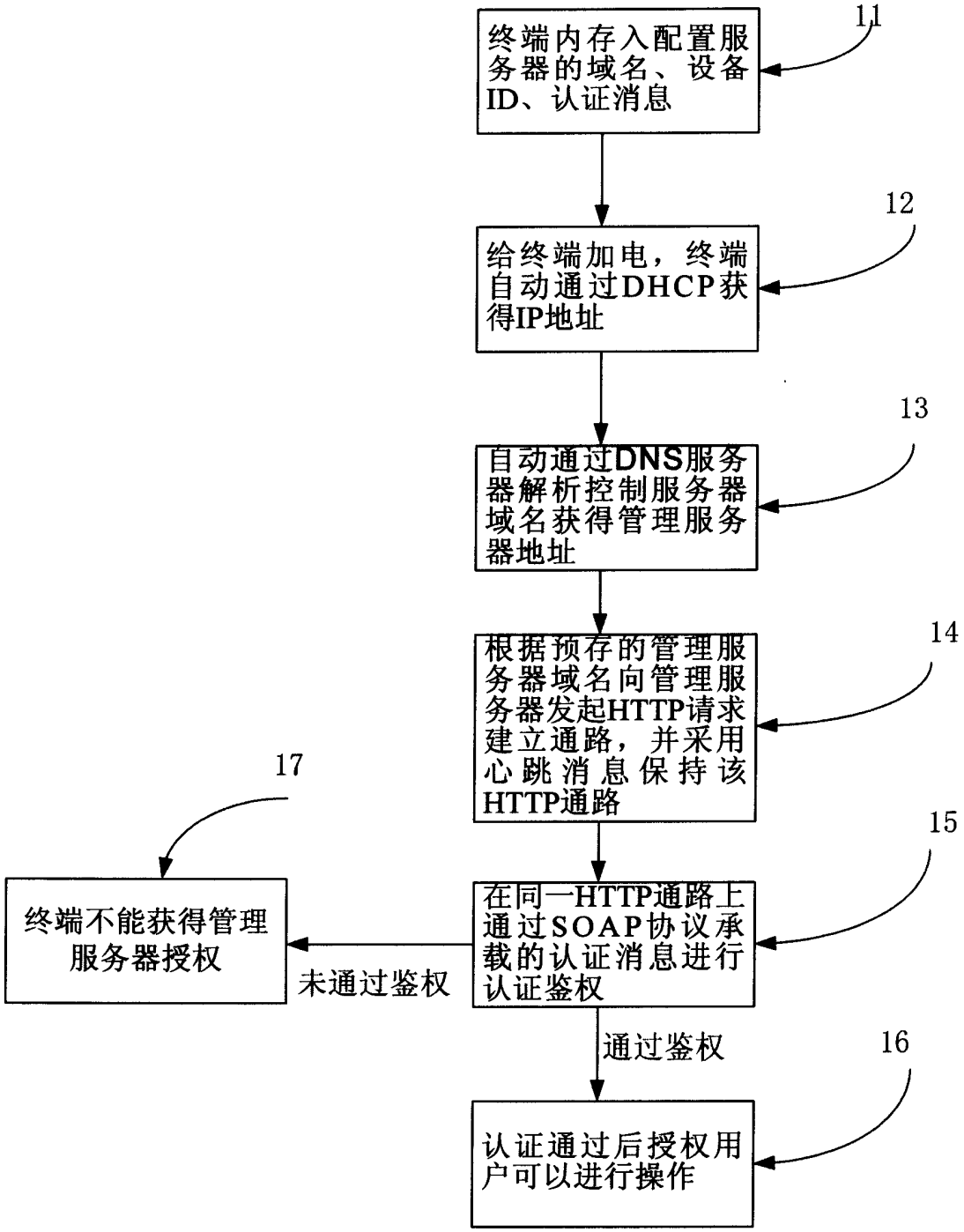

11
终端内存入配置服务器的域名、设备ID、认证消息
12
给终端加电，终端自动通过DHCP获得IP地址
13
自动通过DNS服务器解析控制服务器域名获得管理服务器地址
14
根据预存的管理服务器域名向管理服务器发起HTTP请求建立通路，并采用心跳消息保持该HTTP通路
15
在同一HTTP通路上通过SOAP协议承载的认证消息进行认证鉴权
16
认证通过后授权用户可以进行操作
17
终端不能获得管理服务器授权
未通过鉴权
通过鉴权

图 2

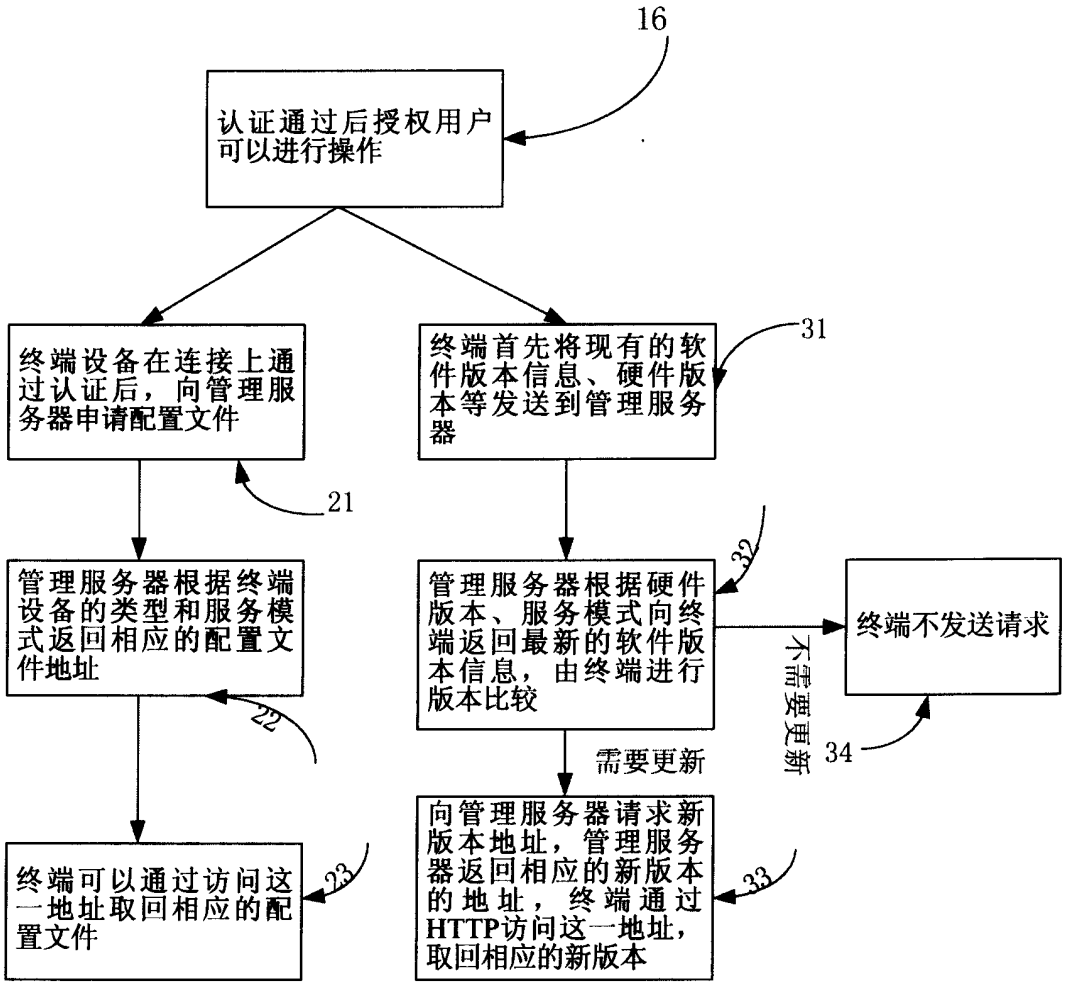

16
认证通过后授权用户可以进行操作
终端设备在连接上通过认证后，向管理服务器申请配置文件
21
管理服务器根据终端设备的类型和服务模式返回相应的配置文件地址
22
终端可以通过访问这一地址取回相应的配置文件
23
终端首先将现有的软件版本信息、硬件版本等发送到管理服务器
31
管理服务器根据硬件版本、服务模式向终端返回最新的软件版本信息，由终端进行版本比较
32
不需要更新
终端不发送请求
34
需要更新
向管理服务器请求新版本地址，管理服务器返回相应的新版本的地址，终端通过HTTP访问这一地址，取回相应的新版本
33

图 3

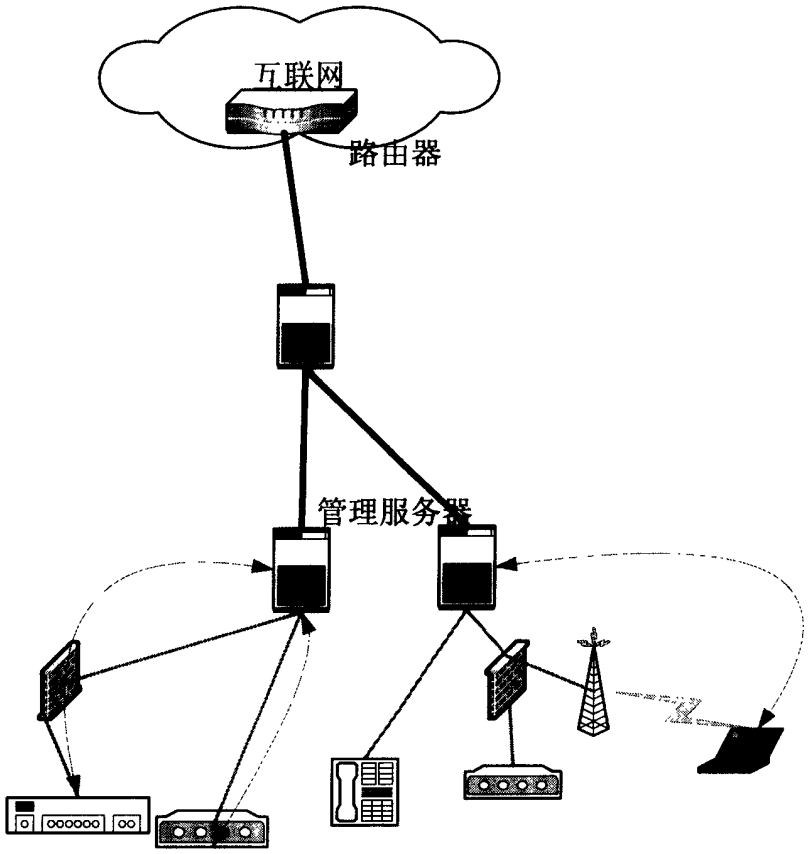


图 4