(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 101166173 B
(45)授权公告日 2012.03.28

(21)申请号 200610113937.5

(22)申请日 2006.10.20

(73)专利权人 北京直真节点技术开发有限公司
地址 100080 北京市海淀区北四环西路 9 号银谷大厦 1506 室

(72)发明人 金建林 袁隽 郭卫增 杨朝令

(74)专利代理机构 北京海虹嘉诚知识产权代理有限公司 11129
代理人 吴小灿

(51)Int.Cl.
H04L 29/00(2006.01)
H04L 9/00(2006.01)
H04L 9/32(2006.01)

(56)对比文件
WO 2005/064882 A2,2005.07.14, 全文.
CN 1627683 A,2005.06.15, 全文.
CN 1725687 A,2006.01.25, 全文.
李宏涛等. 目录服务与统一身份认证的设计与实现. 甘肃科技 21 12.2005,21(12),65,42.
杜娟等. 多系统用户单点登陆系统解决方案. 科技资讯 25.2006,(25),201-202.
杨帆等. 企业级单点登陆系统模型的设计与实现. 微电子学与计算机 22 6.2005,22(6),217-220.

审查员 王桂霞

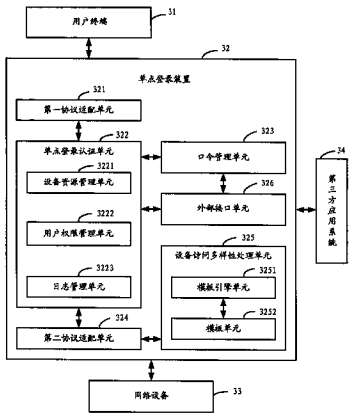
权利要求书 2 页 说明书 10 页 附图 3 页

(54)发明名称

一种单点登录系统、装置及方法

(57)摘要

本发明公开了一种单点登录系统及方法，用于解决现有技术在用户终端访问网络设备时，难以实现直接面向设备的单点登录的问题。本发明所述系统包括：用户终端，用于向单点登录装置发送访问请求，其中含有要访问的网络设备标识以及虚拟用户身份信息；单点登录装置，用于保存每个虚拟用户可以访问的网络设备的信息，当收到访问请求时，如果确定允许该虚拟用户访问所请求的网络设备，则与该用户终端可以访问的网络设备建立连接；网络设备，用于与所述单点登录装置建立连接。本发明还提供了一种单点登录方法。本发明方案用于实现用户终端在访问网络设备时的单点登录，提高工作效率及网络设备访问的安全性。



CN 101166173 B

1. 一种直接面向设备的单点登录系统，其特征在于，该系统包括：至少一个用户终端、单点登录装置以及至少一个向用户终端提供服务的网络设备，其中，

用户终端，处于 Internet 网络范围内，用于向单点登录装置发送访问请求，其中含有要访问的网络设备标识以及虚拟用户身份信息；

单点登录装置，用于保存每个虚拟用户可以访问的网络设备的信息，当收到访问请求时，如果确定允许该虚拟用户访问所请求的网络设备，则与该用户终端可以访问的网络设备建立连接；

所述单点登录装置包括第一协议适配单元、单点登录认证单元和第二协议适配单元，所述第一协议适配单元接收所述用户终端的访问请求，并进行协议适配；所述第二协议适配单元在获取到所述网络设备访问的格式控制信息后，发起对网络设备的访问请求，在建立与网络设备的通信连接后，返回通信连接的标识信息给单点登录认证单元；单点登录认证单元在接收到第二协议适配单元的访问请求成功响应后，建立第二协议适配单元和第一协议适配单元的访问连接数据通信信道，同时返回访问请求成功响应给用户终端；

网络设备，位于单独的业务网中，用于与所述单点登录装置建立连接。

2. 根据权利要求 1 所述的系统，其特征在于，所述的虚拟用户为可以访问单点登录装置的用户，所述虚拟用户身份信息包括虚拟用户标识和口令，每个虚拟用户可以访问网络设备的信息包括：

虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系、虚拟用户标识和虚拟用户口令的对应关系以及网络设备标识与网络设备口令之间的对应关系；

则所述单点登录装置包括：

口令管理单元，用于存储所述虚拟用户口令及网络设备口令；

所述单点登录认证单元，用于保存所述虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系；收到访问请求后，从口令管理单元中获取访问请求虚拟用户标识对应的虚拟用户口令，如果确定访问请求中的虚拟用户口令与获得的虚拟用户口令一致，以及根据所述映射关系确定该用户终端所请求的是允许访问的设备，则从所述口令管理单元中获取该虚拟用户可以访问的网络设备标识对应的口令，通过该口令与所述网络设备建立连接。

3. 如权利要求 2 所述的系统，其特征在于，所述单点登录认证单元还包括：日志管理单元，用于记录所述用户终端的登录信息，和 / 或外部访问网络设备的会话，和 / 或命令，和 / 或命令执行结果的日志信息。

4. 如权利要求 1 至 3 任意一项所述的系统，其特征在于，

所述的第一协议适配单元，用于接收到所述用户终端的访问请求后，将用户终端提交的访问信息发送给所述单点登录认证单元，所述的访问信息包括用户终端要访问的网络设备标识以及虚拟用户身份信息；

所述的第二协议适配单元，用于在单点登录认证单元通过对所述用户终端的认证后，接收单点登录认证单元的请求，从所述单点登录认证单元中的设备资源管理单元获取相应的网络设备信息，并根据该信息与所述网络设备建立连接，并返回通信连接的标识信息给单点登录认证单元；

所述的单点登录认证单元，根据所述通信连接的标识信息建立第二协议适配单元和第

一协议适配单元的数据通信信道，并返回访问请求成功响应消息给所述用户终端；

所述用户终端通过所述数据通信信道与所述网络设备进行数据交互。

5. 如权利要求 4 所述的系统，其特征在于，所述单点登录装置还包括：

设备访问多样性处理单元，用于根据不同的网络设备类型，定义不同的模板，根据网络设备类型信息，通过模板引擎解释相应的模板，得到所述网络设备的访问格式控制信息，并将该信息发送给所述第二协议适配单元；

所述第二协议适配单元根据所述网络设备的访问格式控制信息，发起对所述网络设备的访问请求。

6. 如权利要求 5 所述的系统，其特征在于，所述单点登录装置还包括：

外部接口单元，用于向第三方应用系统提供接口；

所述的第三方应用系统通过所述外部接口单元与所述设备资源管理单元和 / 或所述口令管理单元进行数据共享。

7. 一种直接面向设备的单点登录的方法，其特征在于，该方法包括以下步骤：

A、在单点登录装置中建立虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系；

B、当单点登录装置收到用户终端的访问请求后，根据所述映射关系，判断用户终端是否具有访问相关网络设备的权限，如果具有，建立所述用户终端可以与要访问的网络设备进行数据交互的数据通信信道；所述用户终端处于 Internet 网络范围内，所述网络设备位于单独的业务网中；

所述单点登录装置包括第一协议适配单元、单点登录认证单元和第二协议适配单元，所述第一协议适配单元用于接收所述用户终端的访问请求，并进行协议适配，所述第二协议适配单元在获取到所述网络设备访问的格式控制信息后，发起对网络设备的访问请求，在建立与网络设备的通信连接后，返回通信连接的标识信息给单点登录认证单元；单点登录认证单元在接收到第二协议适配单元的访问请求成功响应后，建立第二协议适配单元和第一协议适配单元的访问连接数据通信信道，同时返回访问请求成功响应给用户终端。

8. 如权利要求 7 所述的方法，其特征在于，步骤 B 所述的用户终端访问所述网络设备的过程中，该步骤进一步包括：

单点登录装置记录所述用户终端的登录信息，所述登录信息包括所述用户终端的登录请求信息及对相应网络设备的操作信息。

9. 如权利要求 7 所述的方法，其特征在于，在执行步骤 B 之后，该方法进一步包括：所述用户终端通过所述单点登录装置与所述网络设备进行通信；在通信过程中，所述单点登录装置对所述用户终端和所述网络设备的协议进行协议适配。

10. 如权利要求 9 所述的方法，其特征在于，该方法进一步包括：

预先根据不同的网络设备类型，定义不同的模板，并设置模板引擎；

所述用户终端通过所述单点登录装置与所述网络设备进行通信的步骤包括：所述模板引擎是根据网络设备类型信息，解释相应的模板，获得网络设备的访问格式控制信息，并利用访问格式控制信息访问相应的网络设备。

一种单点登录系统、装置及方法

技术领域

[0001] 本发明涉及通信网络技术领域，尤其涉及一种单点登录系统及方法。

背景技术

[0002] 电信运营业务需要大量的网络设备硬件和软件来支撑，这些设备硬件和软件通常分别由多个不同的生产厂家提供，分布在不同的地理位置，登录方式各异，每个设备都有自身的用户和权限管理功能，大量的登录用户名和口令分布存储在这些设备之中。

[0003] 随着电信运营商的用户数量和业务种类的不断增多，网络规模不断扩大，设备种类和数量也越来越多。

[0004] 由于网络设备数量爆炸式膨胀，但维护人员的数量有限，维护人员需要同时维护多台设备，在日常工作中需要登录不同的设备进行配置、测试和相关操作，维护人员就需要记住大量设备的口令，给维护工作增加了额外的难度。

[0005] 并且，由于厂商的维护人员和运营商不同部门的维护人员，都同时具备对网络设备的操作权限，设备操作口令繁多，可是当前却缺乏系统的、有效的口令管理，最终导致设备口令丢失、窃取时有发生，口令安全隐患突出；另外，在用户访问设备的过程中，如果缺乏有效的设备访问日志记录，造成系统无法追踪用户对设备的操作，导致系统无法察觉用户的非法操作，从而使系统陷入了不可预计的危险中。

[0006] 传统的设备访问，如图 1 所示，针对每一台设备，用户都要进行登录、身份验证、建立连接这样的过程，这就要求用户必须记住每台设备的登录名称和口令，在电信运营企业，特别是存在大量网络设备需要管理的环境中，如果都采用这样的登录方式，不仅繁琐费时，而且需要用户记录下大量的设备口令，必然存在安全方面的隐患，一旦口令丢失，或者造成信息泄漏，或者无法正常登录系统，都会影响到正常的管理工作。

[0007] 基于 RADIUS 的设备访问，如图 2 所示，RADIUS 是一种分布的客户 / 服务器系统，可以实现安全网络，拒绝未经验证的访问。

[0008] 当一个用户试图登录并验证到一个使用了 RADIUS 的访问服务器时，会产生以下步骤：

[0009] 输入用户名和密码；

[0010] 用户名和加密的密码经过要访问的设备发送到网络中的 RADIUS 服务器，该服务器对该用户进行认证；

[0011] 该用户通过了认证 (ACCEPT)，或者，该用户没有被认证 (REJECT)，允许重新输入用户名和密码，或者，拒绝访问相应设备。

[0012] 连接参数，包括主机、IP 地址、访问列表和用户超时。

[0013] RADIUS 是目前最常用的认证计费协议之一，它简单安全，易于管理，扩展性好，所以得到广泛应用。但是由于协议本身的缺陷，比如基于 UDP 的传输、简单的丢包机制、没有关于重传的规定和集中式计费服务，都使得它不太适应当前网络的发展，需要进一步改进。

[0014] 传统意义的单点登录 (SSO，Single Sign On)，常用于企业、政府内部应用系统的

访问控制，如果企业中有很多应用系统，每个系统都有相应的登录认证方式，用户进入相应的系统都要输入相应系统的登录信息，非常繁琐不便。

[0015] 同时，在传统的单点登录系统中，部署 Web 应用也面临双重的安全挑战。首先，必须保证只有合法的用户才能访问相应的 Web 应用资源。其次，实施安全保护措施时应尽量避免增加用户的负担。随着业务系统的增加，每个用户需要记住多个口令，访问不同的 Web 应用系统采用不同的口令。这虽然能够保证用户对 Web 资源的合法访问，但增加了用户的负担。一方面，为了方便记忆，用户会采用简单的口令或将口令记录下来，这大大降低了应用系统的安全性；另一方面，用户每访问一个 Web 应用资源都需要登录一次，这又大大降低了工作效率。

[0016] 传统的单点登录技术是面向应用而生，不论是普通的系统应用还是 Web 应用，传统的单点登录设计都难以实现直接面向设备的单点登录。

[0017] 但是，在电信网管系统中，设备作为最基本的网元之一，很多最重要和最基本的系统信息都是来自于设备，因此发明建立一个面向设备的单点登录系统与装置 (SASS，Single Access & Security Service)，对于设备访问需要实现单点、接入和安全三个功能就显得格外关键。

发明内容

[0018] 本发明提供一种直接面向设备的单点登录系统、装置及方法，用以解决现有技术在用户访问设备时，难以实现直接面向设备的单点登录的问题。

[0019] 本发明系统包括：至少一个用户终端、单点登录装置以及至少一个向用户终端提供服务的网络设备，其中，

[0020] 用户终端，处于 Internet 网络范围内，用于向单点登录装置发送访问请求，其中含有要访问的网络设备标识以及虚拟用户身份信息；

[0021] 单点登录装置，用于保存每个虚拟用户可以访问的网络设备的信息，当收到访问请求时，如果确定允许该虚拟用户访问所请求的网络设备，则与该用户终端可以访问的网络设备建立连接；

[0022] 所述单点登录装置包括第一协议适配单元、单点登录认证单元和第二协议适配单元，所述第一协议适配单元接收所述用户终端的访问请求，并进行协议适配；所述第二协议适配单元在获取到所述网络设备访问的格式控制信息后，发起对网络设备的访问请求，在建立与网络设备的通信连接后，返回通信连接的标识信息给单点登录认证单元；单点登录认证单元在接收到第二协议适配单元的访问请求成功响应后，建立第二协议适配单元和第一协议适配单元的访问连接数据通信信道，同时返回访问请求成功响应给用户终端；

[0023] 网络设备，位于单独的业务网中，用于与所述单点登录装置建立连接。

[0024] 所述的虚拟用户为可以访问单点登录装置的用户，所述虚拟用户身份信息包括虚拟用户标识和口令，每个虚拟用户可以访问网络设备的信息包括：

[0025] 虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系、虚拟用户标识和虚拟用户口令的对应关系以及网络设备标识与网络设备口令之间的对应关系；

[0026] 则所述单点登录装置包括：

[0027] 口令管理单元，用于存储所述虚拟用户口令及网络设备口令；

[0028] 所述单点登录认证单元，用于保存所述虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系；收到访问请求后，从口令管理单元中获取访问请求虚拟用户标识对应的虚拟用户口令，如果确定访问请求中的虚拟用户口令与获得的虚拟用户口令一致，以及根据所述映射关系确定该用户终端所请求的是允许访问的设备，则从所述口令管理单元中获取该虚拟用户可以访问的网络设备标识对应的口令，通过该口令与所述网络设备建立连接。

[0029] 所述单点登录认证单元还包括：

[0030] 日志管理单元，用于记录所述用户终端的登录信息，和/或外部访问网络设备的会话，和/或命令，和/或命令执行结果的日志信息。

[0031] 所述的第一协议适配单元，用于接收到所述用户终端的访问请求后，将用户终端提交的访问信息发送给所述单点登录认证单元，所述的访问信息包括用户终端要访问的网络设备标识以及虚拟用户身份信息；

[0032] 所述的第二协议适配单元，用于在单点登录认证单元通过对所述用户终端的认证后，接收单点登录认证单元的请求，从所述单点登录认证单元中的设备资源管理单元获取相应的网络设备信息，并根据该信息与所述网络设备建立连接，并返回通信连接的标识信息给单点登录认证单元；

[0033] 所述的单点登录认证单元，根据所述通信连接的标识信息建立第二协议适配单元和第一协议适配单元的数据通信信道，并返回访问请求成功响应消息给所述用户终端；

[0034] 所述用户终端通过所述数据通信信道与所述网络设备进行数据交互。

[0035] 所述单点登录装置还包括：

[0036] 设备访问多样性处理单元，用于根据不同的网络设备类型，定义不同的模板，根据网络设备类型信息，通过模板引擎解释相应的模板，得到所述网络设备的访问格式控制信息，并将该信息发送给所述第二协议适配单元；

[0037] 所述第二协议适配单元根据所述网络设备的访问格式控制信息，发起对所述网络设备的访问请求。

[0038] 所述单点登录装置还包括：

[0039] 外部接口单元，用于向第三方应用系统提供接口；

[0040] 所述的第三方应用系统通过所述外部接口单元与所述设备资源管理单元和/或所述口令管理单元进行数据共享。

[0041] 本发明方法包括以下步骤：

[0042] A、在单点登录装置中建立虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系；

[0043] B、当单点登录装置收到用户终端的访问请求后，根据所述映射关系，判断用户终端是否具有访问相关网络设备的权限，如果具有，建立所述用户终端可以与要访问的网络设备进行数据交互的数据通信信道；所述用户终端处于 Internet 网络范围内，所述网络设备位于单独的业务网中；

[0044] 所述单点登录装置包括第一协议适配单元、单点登录认证单元和第二协议适配单元，所述第一协议适配单元用于接收所述用户终端的访问请求，并进行协议适配，所述第二协议适配单元在获取到所述网络设备访问的格式控制信息后，发起对网络设备的访问请

求，在建立与网络设备的通信连接后，返回通信连接的标识信息给单点登录认证单元；单点登录认证单元在接收到第二协议适配单元的访问请求成功响应后，建立第二协议适配单元和第一协议适配单元的访问连接数据通信信道，同时返回访问请求成功响应给用户终端。

[0045] 步骤 B 所述的用户终端访问所述网络设备的过程中，该步骤进一步包括：

[0046] 单点登录装置记录所述用户终端的登录信息，所述登录信息包括所述用户终端的登录请求信息及对相应网络设备的操作信息。

[0047] 在执行步骤 B 之后，该方法进一步包括：所述用户终端通过所述单点登录装置与所述网络设备进行通信；在通信过程中，所述单点登录装置对所述用户终端和所述网络设备的协议进行协议适配。

[0048] 该方法进一步包括：

[0049] 预先根据不同的网络设备类型，定义不同的模板，并设置模板引擎；

[0050] 所述用户终端通过所述单点登录装置与所述网络设备进行通信的步骤包括：所述模板引擎是根据网络设备类型信息，解释相应的模板，获得网络设备的访问格式控制信息；并利用访问格式控制信息访问相应的网络设备。

[0051] 本发明方案通过建立虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系，用户终端只要发起一个网络设备的连接请求，之后的复杂连接步骤皆由系统自动地控制和完成，而不用再次手动的输入网络设备的口令，从而起到单点登录及口令保密的作用；

[0052] 本发明装置部署在用户终端和网络设备之间，通过协议适配，可以将用户终端和网络设备完全隔离，以保证网络设备的访问安全性；

[0053] 本发明装置通过日志统计管理可详细地记录用户终端每次登录网络设备的活动资料，使维护人员及系统管理员取得各种日志档案以作备份和检查；

[0054] 本发明装置通过针对不同的网络设备类型定义不同的模板，通过模板引擎解释执行相应的模板，获取网络设备的访问格式控制信息，屏蔽网络设备访问的多样性，为用户终端提供统一的设备访问方式；

[0055] 本发明装置还提供了第三方接口，使第三方系统可以通过该接口与本发明装置进行数据共享。

附图说明

[0056] 图 1 为现有技术中传统的设备访问方式示意图；

[0057] 图 2 为现有技术中基于 RADIUS 的设备访问方式示意图；

[0058] 图 3 为实现本发明系统的结构示意图；

[0059] 图 4 为实现本发明方法的流程示意图。

具体实施方式

[0060] 本发明方案的核心思想为：通过建立虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系，使用户终端只要通过一次登录认证，就可以登录相关网络设备，从而避免了在登录其他网络设备时进行再次登录的麻烦；通过协议适配，使外部任意位置的用户对网络设备的访问请求从协议层上终结在单点登录装置，对网络设备的访问从单点

登录装置发起，起到了协议层隔离的作用。另外，通过实行虚拟用户口令和该虚拟用户可以访问的网络设备口令的统一管理，以及对口令的加密处理也可以提高设备访问的安全性；对不同的网络设备定义不同的模板，在访问网络设备时，通过设备类型信息，利用专有的模板引擎读取相应的模板，并解释执行该模板，实现设备访问多样性的自动化。

[0061] 所述的虚拟用户为用户终端访问单点登录装置时设置的用户，即该虚拟用户是该单点登录装置的用户；

[0062] 而所述的虚拟用户可以访问的网络设备标识为能够访问网络设备的用户标识，即该虚拟用户可以访问的网络设备标识是所述网络设备的用户标识；

[0063] 所述的虚拟用户标识与该虚拟用户可以访问的网络设备标识是一对多的关系，即一个单点登录装置的虚拟用户标识可以对应多个虚拟用户可以访问的网络设备标识，也就是说一个具有访问所述单点登录装置权限的用户终端可以通过所述单点登录装置访问不同的网络设备。

[0064] 参照图 3，实现本发明所述的单点登录系统包括：用户终端 31、单点登录装置 32、网络设备 33 和第三方应用系统 34。

[0065] 用户终端 31，用于向单点登录装置 32 发送访问请求，其中含有要访问的网络设备 34 的标识以及虚拟用户身份信息；在收到单点登录装置 32 的登录通知后，访问自身对应的网络设备 33；

[0066] 所述的虚拟用户为可以访问单点登录装置 32 的用户；

[0067] 所述虚拟用户身份信息包括虚拟用户标识和口令；

[0068] 单点登录装置 32，用于保存用户终端 31 可以访问的网络设备 33 的信息，当收到所述用户终端 31 发送的访问请求时，判断是否允许该用户终端 31 访问所请求的网络设备 33，如果允许，与该用户终端 31 可以访问的网络设备 33 建立连接，并向该用户终端 31 发送登录通知；

[0069] 网络设备 33，与所述单点登录装置 32 建立连接，所述用户终端 31 通过所述单点登录装置 32 所建立的数据通道与所述网络设备 33 进行数据的交互。

[0070] 所述的用户终端 31 可以访问的网络设备 33 的信息包括：虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系、虚拟用户标识和虚拟用户口令的对应关系以及网络设备标识与设备口令之间的对应关系。

[0071] 总体来讲，所述的用户终端 31 向所述单点登录装置 32 发起登录请求，单点登录装置 32 根据虚拟用户标识和虚拟用户口令的对应关系对用户终端 31 提供的虚拟用户身份信息进行鉴权，鉴权成功意味着该用户终端 31 具有访问该单点登录装置 32 的权限，则单点登录装置 32 根据自身存储的虚拟用户标识和该虚拟用户可以访问的网络设备标识之间的映射关系，在用户终端 31 请求访问网络设备 33 时，判断用户终端 31 是否有请求访问的网络设备 33 的权限，是则所述单点登录装置 32 根据自身存储的网络设备 33 的访问信息，包括网络设备的名称、IP 地址和网络设备类型等信息，和网络设备 33 的用户信息，包括网络设备 33 的用户标识和口令之间的对应关系，登录到网络设备 33，其中的口令是经过加密处理的，那么用户终端 31 就可以通过单点登录装置 32 访问网络设备 33，在整个用户终端 31 请求访问网络设备 33 的过程中，单点登录装置 32 记录下用户终端 31 的登录信息，包括请求登录信息和相关操作信息。

[0072] 进一步，所述的单点登录装置 32 包括：第一协议适配单元 321、单点登录认证单元 322、口令管理单元 323、第二协议适配单元 324、设备访问多样性处理单元 325 及外部接口单元 326；

[0073] 所述单点登录认证单元 322 包括：设备资源管理单元 3221、用户权限管理单元 3222 和日志管理单元 3223；

[0074] 所述的设备访问多样性处理单元 325 包括：模板引擎单元 3251 和模板单元 3252。

[0075] 所述的第一协议适配单元 321 接收所述用户终端 31 的访问请求，并进行协议适配，提取用户终端 31 的访问信息，包括网络设备 33 的标识，访问单点登录装置 32 的用户和密码信息，并将该信息提交给单点登录认证单元 322 进行用户认证和权限控制；其中所述的单点登录装置 32 的用户为虚拟用户，所述单点登录认证单元 322，保存有所述虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系，在用户提出访问本系统的请求时，从口令管理单元 323 中获取访问请求虚拟用户标识对应的虚拟用户口令，并判断访问请求中的虚拟用户口令与获得的虚拟用户口令是否一致，如果不一致，则返回认证失败响应结果通过第一协议适配单元 321 返回给用户终端 31；如果一致，则说明该用户终端 31 具有访问所述单点登录装置 32 的权限，根据所述映射关系，继续根据单点登录装置的权限管理规则对用户终端 31 和要访问的网络设备 33 以及网络设备 33 的用户的关系进行权限鉴别，鉴权失败，则返回鉴权失败响应结果通过第一协议适配单元 321 返回给用户终端 31；如果鉴权成功，则从所述口令管理单元 323 中获取该虚拟用户可以访问的网络设备 33 的标识对应的口令信息，并从设备资源管理单元 3221 中获得网络设备访问信息，包括网络设备的名称、IP 地址和网络设备类型等信息，并向第二协议适配单元 324 发送访问网络设备 33 的请求，并将所述网络设备访问信息和用户信息发送给第二协议适配单元 324。其中，在各单元的处理过程中，日志管理单元 3223 进行日志记录；

[0076] 第二协议适配单元 324，将网络设备类型信息发送给设备访问多样性处理单元 325，设备访问多样性处理单元 325 接收网络设备类型信息，根据该信息从模板单元 3252 中查询获取相应的模板，然后由模板引擎单元 3251 对所述相应的模板配置进行解释，获得网络设备访问的格式控制信息，并将该信息返回给第二协议适配单元 324；

[0077] 第二协议适配单元 324 在获取到所述网络设备访问的格式控制信息后，发起对网络设备 33 的访问请求，在建立与网络设备 33 的通信连接后，返回通信连接的标识信息给单点登录认证单元 322；

[0078] 单点登录认证单元 322 在接收到第二协议适配单元 324 的访问请求成功响应后，建立第二协议适配单元 324 和第一协议适配单元 321 的访问连接数据通信信道，同时返回访问请求成功响应给用户终端 31；

[0079] 用户终端 31 通过建立的访问连接数据通信信道直接与网络设备 33 进行命令操作和数据交互，在交互过程中，通过日志管理单元 3223 记录会话和操作过程日志信息。

[0080] 用户终端 31 访问结束后，拆除访问连接数据通信信道。

[0081] 另外，单点登录装置 32 维护一套网络设备资源信息，和网络设备访问的用户及口令信息，在电信运营支撑管理体系中，存在第三方的网络资源管理系统或第三方的访问设备，即本实施例中所述第三方应用系统 34，因此网络设备资源信息和 / 或网络设备用户及口令信息需要共享，单点登录装置 32 通过外部接口单元 326 使设备资源管理单元 3221 和

/ 或口令管理单元 323 与第三方应用系统 34 进行数据共享。

[0082] 其中，所述的映射关系是通过在数据库里建立二维表，将所述虚拟用户标识和该虚拟用户可以访问的网络设备标识进行映射，减少用户记录太多的账户和密码，同时又可以使得虚拟用户的口令和网络设备的口令实现统一的维护和管理；

[0083] 所述的登录信息包括用户终端的登录请求信息以及对网络设备进行的操作信息。

[0084] 所述设备资源管理单元 3221，用于存储所述系统的网络设备标识以及可以访问该网络设备的用户标识，包括所述单点登录装置 32 管理的所有网络设备以及访问这些网络设备的信息，即所述单点登录装置 32 都管理了哪些网络设备，都有哪些用户可以登录这些设备。

[0085] 所述用户权限管理单元 3222，在用户终端 31 提出登录所述单点登录装置 32 的请求时，该请求包括虚拟用户的标识和口令，从所述口令管理单元 323 中获取访问请求虚拟用户标识对应的虚拟用户口令，并判断访问请求中的虚拟用户口令与所述用户终端 31 提出请求时提供的虚拟用户口令是否一致，如果一致，所述用户终端 31 具有登录单点登录装置 32 的权限，则本单元再根据所述用户终端 31 提出的网络设备 33 的访问请求，该请求中包括网络设备 33 的标识，本单元再根据所述设备资源管理单元 3221 的网络设备 33 的标识和可以访问该网络设备 33 的用户标识对应的所述虚拟用户标识，以及该虚拟用户可以访问的网络设备标识之间的映射关系，判断该用户终端 31 所请求的是否是允许访问的网络设备 33，如果是，从所述口令管理单元 323 中获取该虚拟用户可以访问的网络设备 33 的标识对应的口令，通过该口令与所述网络设备 33 建立连接；

[0086] 其中，所述用户权限管理单元 3222 对所述用户权限的管理方法可以为：

[0087] 将所述系统中的网络设备进行分类，定义不同类型网络设备的登录权限；

[0088] 定义可以访问所述不同类型网络设备的不同角色，即每个角色定义为可对不同类型设备设备进行登录的权限；

[0089] 定制不同用户的角色，即同一个用户可以同时拥有多个角色，而该用户的权限等于该多个角色所拥有的权限之和。

[0090] 例如运营商目前拥有五台设备分别是 1、2、3、4、5，分属两个部门甲、乙，甲部门管理设备 1、2 和 3，乙部门管理设备 4 和 5。甲部门的人员是张三、乙部门的人员是李四，两个部门都由同一个经理管理。那么根据上面的分析，要定义两个角色，即甲和乙。角色甲拥有对设备 1、2 和 3 的访问权限，角色乙拥有对设 4 和 5 的访问权限。而用户只能通过归属到角色才能拥有权限，因此用户张三拥有角色甲的权限，李四拥有角色乙的权限，假设部门来了新员工，只要把对应的角色分配给他就可以了。对于经理而言，他可以同时拥有两个角色甲和乙的权限。这样定义的好处在于，无论是新添加用户还是新添加设备，都不用分别设置用户和设备的对应关系，降低了工作量和出错的几率。

[0091] 那么用户终端通过虚拟用户访问所述单点登录装置 32 时，根据与用户信息的对应关系，可以具有不同角色的权限，即可以访问不同类型的网络设备。

[0092] 日志管理单元 3223，用于记录所述用户终端 31 的登录信息，该登录信息包括用户终端 31 的登录请求信息及对网络设备 33 的操作信息；

[0093] 即日志管理单元 3223 详细地记录用户终端 31 每次的登录活动资料，如登录的时间、用户名称，同时也记录用户终端 31 与网络设备 33 连线和互动的活动信息，如登录网络

设备 33 的时间、虚拟用户标识、网络设备标识和曾使用的操作指令。此外，日志管理单元 3223 还提供介面给维护人员及系统管理员取得各种日志档案以作备份和检查，使系统管理员可通过浏览器追踪用户终端 31 的登录和与网络设备 33 进行连接的活动。

[0094] 口令管理单元 323，用于存储所述虚拟用户口令及所述虚拟用户可以访问的网络设备 33 的标识对应的口令，并对所述口令进行加密处理；

[0095] 该口令管理单元 323 可以单独设置在一台服务器上，而且只具有与单点登录认证单元特定的接口，不支持其他访问接口，因此安全性高。

[0096] 电信运维人员处于 Internet 网络范围内，网络设备位于单独的业务网络中，为了网络设备的安全，在网络规划和部署中，是禁止 Internet 网络中的请求直接访问业务网络中的网络设备的。

[0097] 实际的运维过程中，运维人员直接对设备进行操作，管理和维护是不可避免的，协议适配单元对网络访问协议进行适配和转换，把来自于 Internet 的访问请求在数据内容上不变，在协议处理上进行适配；网络通信和数据交换中，单点登录装置对于 Internet 网络的请求是服务器，为 Internet 的访问请求提供服务，对于网络设备是客户端，发起对网络设备的访问请求，发送操作命令并获取执行结果和数据。Internet 网对网络设备的访问请求由单点登录装置中的协议适配单元实现内部的转换和适配，通过面向网络设备的业务网服务的客户端应用转发请求到网络设备业务网，从而实现公网用户请求对业务网设备的操作、管理和维护。

[0098] 单点登录装置中，在面向 Internet 侧的服务器应用和面向业务网的客户端应用之间通过内部数据通信管道建立数据信道，数据信道的建立、监视和维护由单点登录装置根据业务需求和控制策略进行管理，因此在单点登录装置通过协议适配解决实际需求的同时，还实现了对数据内容的过滤、监视和日志记录，并可以提供安全机制对信道建立进行控制。

[0099] 单点登录装置支持的协议适配不仅包括对等协议的适配，还支持非对等访问协议的适配。例如公网到单点登录装置和单点登录装置到业务网之间都是 telnet；或者公网到单点登录装置之间是 telnet，单点登录装置到业务网之间是 SSH。

[0100] 外部接口单元 326，向第三方系统提供软件接口，实现与第三方资源系统或者安全管理系统的数据共享。

[0101] 即外部接口单元 326 是给第三方系统提供的软件接口，可以使其他厂家的网络资源管理系统或者安全口令管理系统 34 与单点登录装置 32 进行网络设备资源数据或者网络设备安全口令数据的共享。如果用户并无第三方的软件，可以不安装这个单元。

[0102] 设备访问多样性处理单元 325，对不同的网络设备定义不同的模板，在访问网络设备时，所述的模板引擎单元 3251 从设备资源管理单元 3221 获取要访问的网络设备的类型信息，并根据该信息找到相应的模板，并解释执行该模板，实现设备访问多样性的自动化；其中所述的模板单元 3252 存储了根据各种设备类型定义的各种模板。

[0103] 设备访问的多样性发生在单点登录装置和业务网之间的访问过程中，由于网络设备以及业务系统的供应厂商的不同，虽然在设备和业务系统访问的协议标准和规范方面是相同的，但是由于实现方式、手段、技术和习惯的不同，造成了设备访问上的多样性，比如两个不同厂商生产的路由器都提供 telnet 的访问，但是在数据格式上却不相同，对于运维人

员，就必须面对这种差异，操作不同的路由器的时候就要按照不同厂商提供的访问方式进行操作。

[0104] 单点登录装置的设备访问多样性处理单元解决设备访问多样性的技术方案是通过模板，不同设备的访问方式是不同的，但是对于同一类型的设备或者业务系统，访问的方式一定是相同的，并且访问的操作控制格式是固定的，可以模板化的。对于不同的设备类型，按照模板规则定义不同的模板对象。

[0105] 设备访问多样性处理单元通过模板定义工具，对不同的设备类型定义访问模板。在单点登录装置访问业务网的时候，专有的模板引擎模块读取对应的模板，并解释执行该模板，自动化解决设备访问差异化问题。

[0106] 那么综合起来说明本发明系统的工作过程为：

[0107] 用户终端 31 在通过单点登录装置 32 访问网络设备 33 时，首先通过第一协议适配单元 321 将网络设备 33 的设备信息和虚拟用户信息发送给单点登录认证单元 322，单点登录认证单元 322 对用户访问该单点登录装置 32 的权限进行判断，所述单点登录认证单元 322 中的用户权限管理单元 3222，根据口令管理单元 323 中存储的虚拟用户口令信息判断该用户是否具有登录单点登录装置 32 的权限，如果不具有权限，则通过第一协议适配单元 321 返回失败响应消息给用户终端 31，如果具有权限，则根据所述用户权限管理单元 3222 中的虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系判断所述用户终端 31 是否具有访问所述网络设备 33 的权限，如果不具有权限，则通过第一协议适配单元 321 返回失败响应消息给用户终端 31，如果具有这样的权限，则从设备资源管理单元 3221 中获取网络设备 33 的相关信息，其中包括网络设备 33 的设备类型信息，以及口令管理单元 323 的所述虚拟用户口令及所述虚拟用户可以访问的网络设备 33 的标识对应的口令信息，将该信息发送给第二协议适配单元 324，第二协议适配单元 324 将网络设备 33 的设备类型信息发送给设备访问多样性处理单元 325，设备访问多样性处理单元 325 根据所述设备类型信息查找相应的模板，模板引擎单元 3251 对该模板进行解释执行，获取网络设备 33 的访问格式控制信息，并将该信息发送给第二协议适配单元 324，第二协议适配单元 324 根据该信息以及网络设备 33 的相关信息和网络设备 33 的用户信息与所述网络设备 33 建立连接，并返回通信连接的标识信息给单点登录认证单元 322，单点登录认证单元 322 建立第一协议适配单元 321 和第二协议适配单元 324 的访问连接通信信道，并返回访问请求成功响应消息给用户终端 31，那么所述用户终端 31 就可以通过单点登录装置 32 所建立的访问连接通信信道与网络设备 33 进行数据交互。

[0108] 在数据传输过程中，经过协议适配单元的协议适配，使公网任意位置的用户终端 31 对网络设备 33 的访问请求从协议层上终结在单点登录装置 32，从单点登录装置 32 发起对网络设备 33 的访问请求，保证了网络设备 33 的访问安全性，与此同时，日志管理单元 3223 记录所述用户终端 31 的登录信息，和 / 或外部访问网络设备 33 的会话，和 / 或命令，和 / 或命令执行结果的日志信息；另外，当有第三方应用系统 34 请求与单点登录装置 32 进行数据共享时，该系统可以是外部的资源系统，也可以是外部的安全系统，可以通过外部接口单元 326 与单点登录装置 32 相连接，通过所述的设备资源管理单元 3221 和 / 或口令管理单元 323 与所述的第三方应用系统 34 进行数据的共享。

[0109] 参照图 4，与本发明所述系统相对应的一种单点登录方法包括以下步骤：

[0110] S401、用户终端向单点登陆装置提出访问网络设备的请求；

[0111] 用户终端在发起访问请求时，提供的信息包括：需要访问的网络设备的标识信息，访问单点登录装置的用户标识及密码信息，所述的单点登录装置的用户相对于网络设备的用户来说为虚拟用户，即所述提交的信息包括虚拟用户标识和密码。

[0112] S402、判断用户终端是否具有访问单点登陆装置的权限；

[0113] 在所述单点登录装置收到用户终端的访问请求后，根据访问请求虚拟用户标识对应的虚拟用户口令，并判断访问请求中的虚拟用户口令与所述用户终端提供的虚拟用户口令是否一致，如果一致，则进行步骤S403，否则拒绝用户终端的访问请求，结束。

[0114] S403、判断用户终端是否具有访问网络设备的权限；

[0115] 单点登录装置根据虚拟用户标识与该虚拟用户可以访问的网络设备标识之间的映射关系，判断用户终端是否具有访问所述网络设备的权限，是则进行步骤S404，否则进行步骤S409，拒绝用户终端的访问请求。

[0116] S404、获取网络设备访问信息和网络设备用户信息；

[0117] 根据所述映射关系获取网络设备访问信息和网络设备用户信息；

[0118] 其中所述的网络设备访问信息包括网络设备的名称、IP地址和网络设备类型等信息。

[0119] S405、根据网络设备访问信息中的网络设备类型信息获取网络设备的访问格式控制信息；

[0120] 通过预先对不同的网络设备定义不同的解析模板，并设置了专有的模板引擎；

[0121] 通过网络设备类型，查找相应的模板，并通过模板引擎读取对应的模板，并解释执行，获取网络设备的访问格式控制信息。

[0122] S406、根据所述网络设备的访问格式控制信息、网络设备访问信息和网络设备用户信息单点登录装置与网络设备建立连接；

[0123] S407、单点登录装置建立访问连接通信信道；

[0124] 单点登录装置与所述的网络设备建立连接后，在单点登录装置内部建立一条访问连接通信信道，该信道建立后，并向用户终端返回访问请求成功响应消息。

[0125] S408、用户终端通过所述访问连接通信信道与所述网络设备进行数据交互；

[0126] 所述的数据交互包括命令的操作等；

[0127] 其中，单点登录装置通过协议适配，使外部任意位置的用户对网络设备的访问请求从协议层上终结在单点登录装置，对网络设备的访问从单点登录装置发起，起到了协议层隔离的作用；

[0128] 在整个用户终端请求访问网络设备的过程中，单点登录装置记录下用户终端的登录信息，包括请求登录网络设备的信息以及对所述网络设备的操作信息，另外，单点登录装置还可以提供介面给维护人员及系统管理员，使他们可以取得各种日志档案，以作备份和检查，系统管理员还可通过浏览器追踪用户终端的登录和连接网络设备的活动。

[0129] S409、结束。

[0130] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

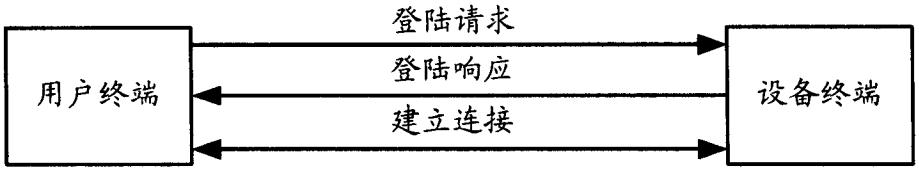


图 1

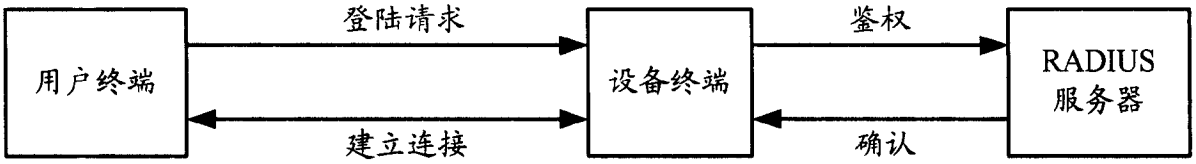


图 2

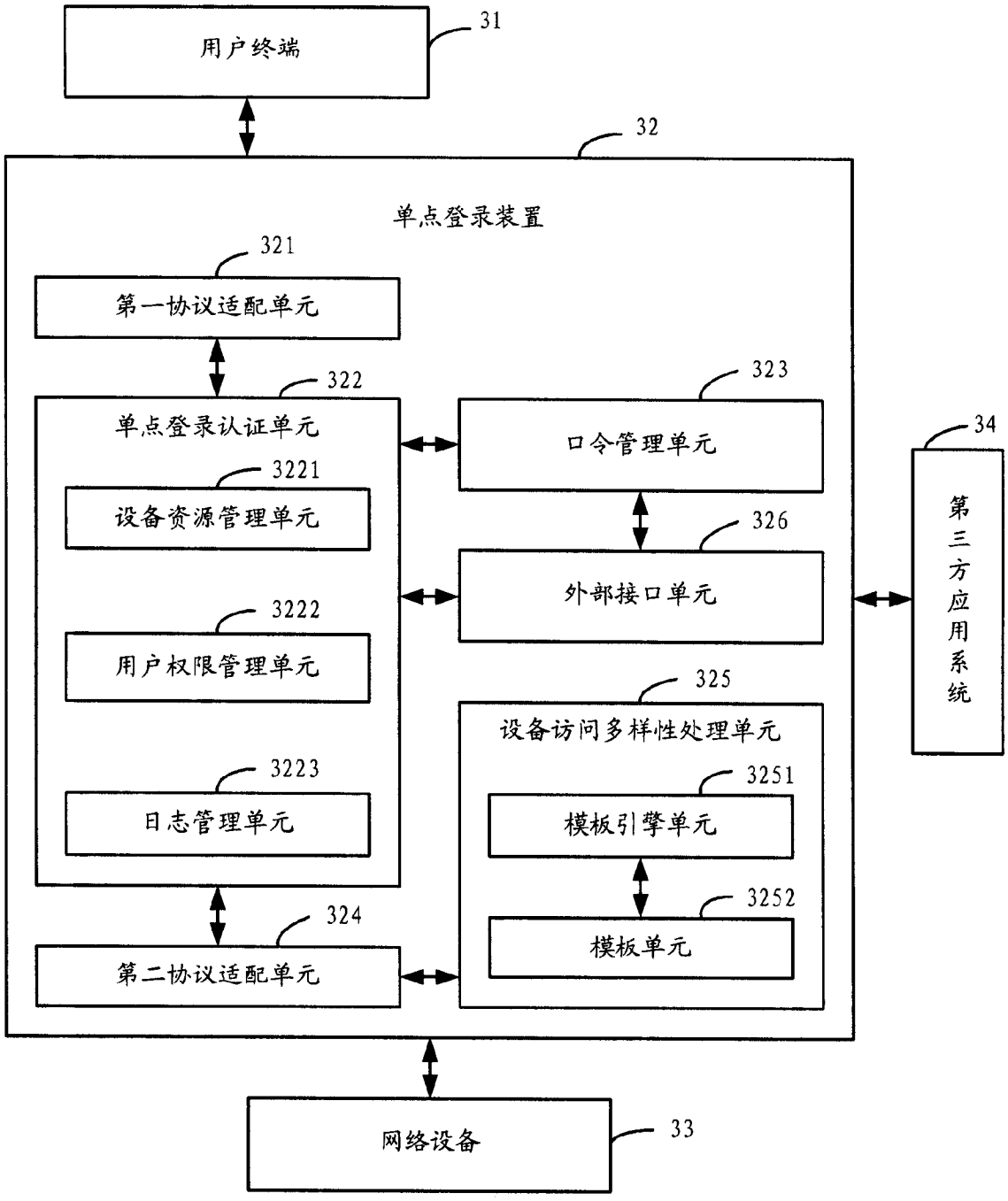

用户终端
31
32
单点登录装置
321
第一协议适配单元
322
单点登录认证单元
3221
设备资源管理单元
3222
用户权限管理单元
3223
日志管理单元
324
第二协议适配单元
323
口令管理单元
326
外部接口单元
325
设备访问多样性处理单元
3251
模板引擎单元
3252
模板单元
34
第三方应用系统
网络设备
33

图 3

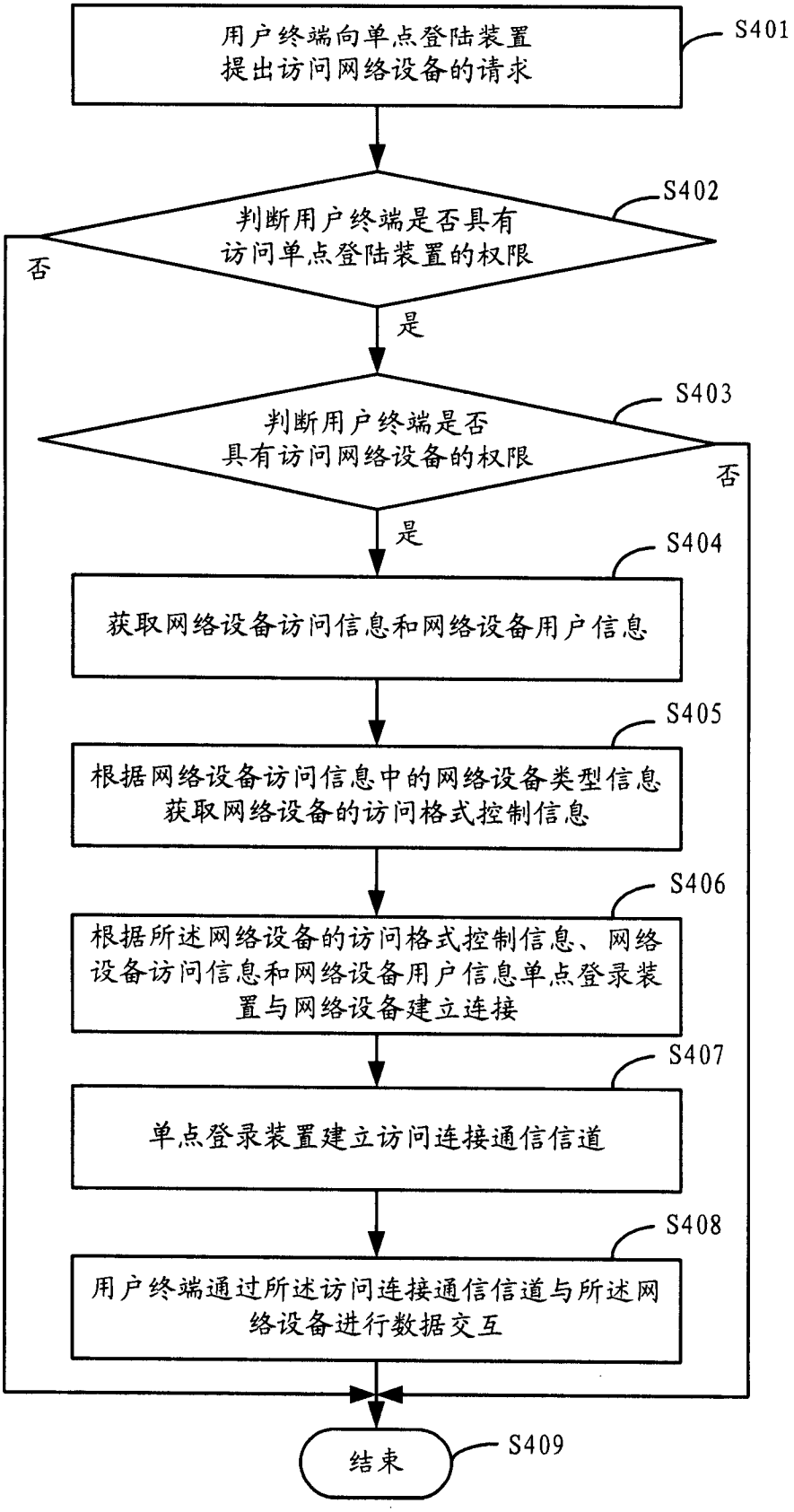

用户终端向单点登陆装置
提出访问网络设备的请求
S401
判断用户终端是否具有
访问单点登陆装置的权限
S402
否
是
判断用户终端是否
具有访问网络设备的权限
S403
否
是
获取网络设备访问信息和网络设备用户信息
S404
根据网络设备访问信息中的网络设备类型信息
获取网络设备的访问格式控制信息
S405
根据所述网络设备的访问格式控制信息、网络
设备访问信息和网络设备用户信息单点登录装
置与网络设备建立连接
S406
单点登录装置建立访问连接通信信道
S407
用户终端通过所述访问连接通信信道与所述网
络设备进行数据交互
S408
结束
S409

图 4