[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04L 29/02

[12] 发明专利申请公开说明书

[21] 申请号 200410063870.X

[43] 公开日 2005 年 7 月 27 日

[11] 公开号 CN 1645794A

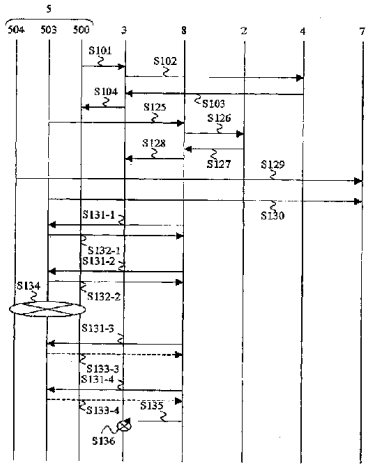
[22] 申请日 2004.7.13
[21] 申请号 200410063870.X
[30] 优先权
[32] 2004.1.19 [33] JP [31] 2004-010011
[71] 申请人 日立通讯技术株式会社
地址 日本东京
[72] 发明人 吉本哲郎 泷广真利 横山卓
[74] 专利代理机构 永新专利商标代理有限公司
代理人 胡建新

权利要求书 3 页 说明书 11 页 附图 10 页

[54] 发明名称 访问用户管理系统、访问用户管理装置

[57] 摘要

本发明涉及访问用户管理系统、访问用户管理装置。提供一种新的 web 认证方式，消除用户的再认证不方便。设置如下服务器，来替代认证用 web 服务器，该服务器具有：认证用户的功能；通过对用户定期进行再认证请求或发送连接确认包、接收其回信，来确认用户的连接状态的功能；和对访问服务器设定策略路由的功能；在终端中，替代 web 浏览器，而通过与上述服务器通信，在启动时进行认证，使响应再认证请求或连接确认包的客户机工作，来保持连接状态。另外，通过在认证用 web 服务器的位置上，设置具有认证用户的功能的服务器，在终端中替代 web 浏览器，而与上述服务器通信，在启动时进行认证，之后也定期地进行认证，使客户机工作，由此来保持连接状态。



ISSN1008-4274

1、一种访问用户管理方法，在利用访问服务器、监视服务器、及认证服务器将用户终端连接到网络上时对访问用户进行管理，所述访问服务器接收来自所述用户终端的访问请求后将所述用户终端连接到网络上，所述监视服务器监视所述用户到网络的连接状态，所述认证服务器进行向所述访问服务器发送了访问请求的用户终端的认证，该访问用户管理方法的特征在于：

通过所述访问服务器，接收来自所述用户终端的访问请求；

在所述访问请求是来自未被认证的用户终端的访问请求的情况下，设定该访问服务器的路径控制条件，以便将来自所述用户终端的发送包传送到所述认证服务器；

在所述访问请求是来自已被认证的用户终端的访问请求的情况下，设定所述访问服务器的路径控制条件，以便将来自所述用户终端的发送包连接到网络上；

由所述监视服务器监视所述已被认证的用户终端对网络的访问状态；

对来自如下用户终端的发送包、即所述监视的结果被判断为未访问网络的用户终端的发送包，设定所述访问服务器的路径控制条件，以便传送到所述认证服务器。

2、根据权利要求 1 所述的访问用户管理方法，其特征在于：

所述监视服务器与所述认证服务器是相同的服务器。

3、根据权利要求 1 所述的访问用户管理方法，其特征在于：

通过所述监视服务器，向所述用户终端发送生存确认包或用户认证请求包，

在一定时间以上没有来自该用户终端的响应的情况下，判断为所述用户终端未访问网络。

4、根据权利要求3所述的访问用户管理方法，其特征在于：

所述用户终端在后台执行对所述生存确认请求包或用户认证请求包的响应。

5、一种访问用户管理装置，其特征在于，具有：接收来自用户终端的访问请求后将所述用户终端连接到网络上的访问服务器、监视所述用户到网络的连接状态的监视服务器、及进行向所述访问服务器发送了访问请求的用户终端的认证的认证服务器；

所述访问服务器具有：对包进行发送接收的单元、对已从用户终端发送的包实施预定的路径控制的单元、及根据已接收的变更请求来变更该路径控制条件的单元；

所述监视服务器具有：对包进行发送接收的单元、辨别接收包的发送方是未被认证的用户终端还是已被认证的用户终端的单元、生成向已被认证的用户终端发送的生存确认包或再认证请求包的单元、及生成向所述访问服务器发送的路径控制条件的变更请求包的单元；

在一定时间以上没有对所述生存确认请求包或再认证请求包的响应的情况下，向所述访问服务器发送所述路径控制条件的变更请求包；

设定所述访问服务器的路径控制条件，以便向所述认证服务器传送来自该一定时间以上没有响应的用户终端的发送包。

6、根据权利要求5所述的访问用户管理装置，其特征在于：

在所述监视服务器中，安装存在获知软件（presence awareness software）。

7、根据权利要求6所述的访问用户管理装置，其特征在于：

所述存在获知软件是IM（Instant Messaging）。

8、根据权利要求5所述的访问用户管理装置，其特征在于：

在所述监视服务器，安装邮件服务器软件。

9、一种应用程序服务器，连接到向因特网传送接收包的访问服务器上，其特征在于，具有：

对包进行发送接收的单元；

辨别接收包的发送方是未被认证的用户终端还是已被认证的用户终端的单元；

生成向所述已被认证的用户终端发送的生存确认包或再认证请求包的单元；

对发送给该用户终端的生存确认包或再认证请求包发送后所经过的时间进行计数的计数器；及

生成向所述访问服务器发送的路径控制条件的变更请求包的单元；

在预定时间内没有对所述生存确认包或再认证请求包的响应的情况下，向所述访问服务器发送所述路径控制条件的变更请求包。

10、根据权利要求 9 所述的应用程序服务器，其特征在于：

安装了邮件服务器软件。

11、根据权利要求 9 所述的应用程序服务器，其特征在于：

安装了 IM（Instant Messaging）功能。

访问用户管理系统、访问用户管理装置

技术领域

本发明涉及一种宽带因特网连接中的访问用户的管理。

背景技术

在确保网络通信的安全上，用户认证技术是非常重要的技术。现在，在宽带因特网连接中的访问用户的认证及状态管理中，广泛使用 PPPoE（Point-to-Point Protocol Over Ethernet：基于以太网的点到点协议）（Ethernet 是注册商标）。PPPoE 是将在拔号连接中使用的 PPP 用于 Ethernet 上的技术，可根据认证协议，用第二层级（layer 2 level）进行用户认证，另外，可通过定期地请求用户再认证、或使用 LCP Echo 包（packet）来监视用户的连接状态。

另外，还有使用所谓 IEEE802.1x 通信规格的认证方法。这是执行第二层（layer 2）下的端口单位的认证的方法，现在多用于本地的无线连接的认证上。可根据认证协议，用第二层级进行用户认证，还可通过定期地请求用户再认证，来监视用户的连接状态。

上述两种认证方法可以是第二层下的用户管理，但也可以使作为一般加入最近的路由器中的功能的策略路由（policy routing）功能和基于 World-Wide-Web（万维网）（Web）的应用层级下的认证组合，来认证访问用户。这是如下的用户认证方法：使用策略路由功能来事先设定通过第三层级（layer 3 level）与访问用户直接连接的装置、即访问服务器（路由器），以使得用户的连接最初只能访问特定的 Web 服务器，在用户连接之后，从 Web 浏览器进行认证，从 Web 服务器设定并修改访问服务器，以便仅对被认证了的用户的 IP 地址进行普通路由。

图 10 是一般的访问服务器的硬件结构图。31 是 CPU，用于按照用户管理或根据情况，用软件处理路由等复杂的处理。32 是 CPU 31 使用的存储器，在其上存储作为访问服务器所需要的软件或数据。在存储器 32 上至少存在连接信息管理部 321、外部管理服务器协同部 322 和包传送部设定部 323 等。其中，连接信息管理部 321 对终端的连接信息进行保持；外部管理服务器协同部 322 接收来自外部的连接信息更新请求，向连接信息管理部 321 及包传送部设定部 323 输出状态变更指示；包传送部设定部 323 根据连接信息管理部 321 和外部管理服务器协同部 322 的指示，对包传送部的信息进行更新等。33 是包传送部。包传送也可通过 CPU 31 的软件处理来执行，但多数情况下具有独立的包传送部，可比用 CPU 31 更高速地执行。包传送部还存在完全按硬件逻辑构筑的处理器的情况，还存在使用称为网络处理器的在包传送中特化的特殊的 MPU 的情况。包传送部 331 高速地进行通常的包传送。策略路由部 332 具有如下功能：对具有特定图形的包，重写包传送部 331 的传送结果，并根据策略来变更包传送的目的地。重写包传送部 331 及策略路由部 332 根据包传送部 33 的结构，若为由硬件实现的情况，则也存在由软件实现的情况。NIF 34 是实际上与网络物理连接的位置。此前所述的各模块通过总线 35 连接。35 也可以不是总线而是开关。

用图 2 及图 3 说明组合了策略路由与 Web 认证的方法。图 2 是系统示意图。终端 5 经访问服务器 3 连接于因特网 7 上。访问服务器 3 与 DHCP 服务器 4 和 Web 服务器 1 相连。Web 服务器 1 与认证服务器 2 连接。在终端 5 的下方，示出了在终端 5 上工作的软件结构。在终端 5 上 OS 500 工作，在 OS 500 上 Web 浏览器 501 和其他的网络应用程序 502 工作。

图 3 是组合了策略路由和 Web 认证的认证方法的序列图。一旦终端启动，则终端上的 OS 通过 DHCP 取得 IP 地址（S101）。接收到

DHCP 请求的访问服务器通过 DHCP 中继，将请求传送到 DHCP 服务器（S102）。DHCP 服务器对终端分配 IP 地址，将结果返回到访问服务器（S103）。访问服务器将 IP 地址传送到终端（S104），终端 5 变成可进行 IP 通信的状态。

分配给终端 5 的 IP 地址在该时刻由访问服务器 3 设定策略路由，不能对因特网自由地访问。来自应用程序 502 的因特网访问 S105 和来自 Web 浏览器的因特网访问 S106 都失败。图 3 所示的×标记意味着各步骤 S105、S106 两者都不可实现。在该时刻，终端 5 可访问的仅是 Web 服务器 1。终端访问 Web 服务器 1，并通过输入用户名和密码来请求认证（S107）。接收了认证请求的 Web 服务器将认证请求传送到认证服务器 2（S108）。接收了来自认证服务器的认可（S109）的 Web 服务器对访问服务器 3 进行设定，以便对终端 5 的 IP 地址避开策略路由的设定（S110）。这样，终端 5 可进行因特网访问，来自 Web 浏览器的因特网访问 S111 和来自其他应用程序的因特网访问 S112 都成功。

在用图 2 及图 3 的说明中，为了简单，将访问服务器 3 和 Web 服务器 1、认证服务器 2、DHCP 服务器 4 表示为不同的服务器，但若在功能上等效，则各服务器也可通过任意组合缩减。另外，作为 IP 地址分配的实例，给出了 DHCP，但 IP 地址的分配方法可以使用任意的方法。例如，若 IP 协议是 IPv6，则也可使用 RA（Router Advertisement：路由器争议）。另外，在 S106 和 S107，Web 浏览器指明访问 Web 服务器 1，但也可通过使用 Web 服务器的重定向（redirect）功能，使 S106-S107 成为连续的序列。

【专利文献 1】：日本特开 2003-224577

【非专利文献 1】：RFC2516:Method for Transmitting PPP Over Ethernet （PPPoE） IEEE 802.1X-2001:IEEE Standards for Local and Metropolitan Area Networks:Port-Based Network Access

Control

PPPoE 具有向包赋予 PPP 标题（head）及 PPPoE 标题所导致的通信效率恶化，或不可使用以太网原来具有的多点传送（multicast）功能等限制。另外，PPPoE 是第二层级的通信协议，所以通过第三层级与访问用户直接连接的访问服务器必须具有 PPPoE 功能，这样，存在访问服务器的成本变高的问题。

IEEE802.1x 没有通信效率或多点传送功能的限制，但与 PPPoE 同样是第二层级的通信标准，所以在访问服务器中必须安装对应于 IEEE802.1x 的功能，这样存在访问服务器的成本变高的问题。

在组合了策略路由和 Web 认证的用户认证方法中，不存在监视用户的连接状态的单元。用户在访问因特网时，若从 ISP（Interner Service Provider：因特网服务提供商）侧看，则意味着对用户分配特定的网络资源（例如，通过 DHCP 路径对用户分配的 IP 地址等）。因而，在现行的 Web 认证方法中，不判定分配了网络资源的用户当前是否未连接于现有的因特网上。但是，以 IPv4 地址为代表，网络资源是有限的，所以不能仍对未连接的用户分配资源。因此，现在的方法是：以通过访问服务器 1 监视访问数据包的导通，在超时的情况下，认为用户变为不通，再次将用户的 IP 地址仅连接于 Web 服务器，如上进行重新设定，在用户再次使 Web 浏览器工作时，请求再认证。

用图 3 来说明超时（time out）时访问服务器的再认证请求工作。在图 3 中，S113 表示超时期间。由 S113 表示的期间，在不是来自终端 5 的 IP 访问时，访问服务器 3 在 S114 对终端 5 的 IP 地址重新设定策略路由。之后，来自终端 5 的应用程序的因特网访问 S115 失败。因此，用户通过 Web 浏览器重新访问 Web 服务器 1，在 S116～S119 中再次重复与 S107～S110 一样的认证工作。通过用户的再认证，用户侧可再次进行来自终端 5 的因特网访问 S120。这若从用户

方面看，则增加了不必要的负担。尤其是，在用户只使用除 Web 浏览器以外的应用程序时，仅为了认证就必须使全部 Web 浏览器再次工作，明显阻碍了宽带下一般经常连接的便利性。

发明内容

因此，本发明的目的在于提供一种新的 Web 认证方法、及可提供该认证方法的 Web 认证装置，可解决在现有 Web 认证方式中，不能把握用户连接状态的课题，以及由用户反复再认证程序的手续复杂等 2 个课题。

现有组合了策略路由和 Web 认证的认证方法的问题在于，使用不能独立工作的 Web 浏览器作为终端方的认证框架。

为了实现上述目的，本发明的访问用户管理方法，在利用访问服务器、监视服务器、及认证服务器将用户终端连接到网络上时对访问用户进行管理，所述访问服务器接收来自所述用户终端的访问请求后将所述用户终端连接到网络上，所述监视服务器监视所述用户到网络的连接状态，所述认证服务器进行向所述访问服务器发送了访问请求的用户终端的认证，该访问用户管理方法的特征在于：通过所述访问服务器，接收来自所述用户终端的访问请求；在所述访问请求是来自未被认证的用户终端的访问请求的情况下，设定该访问服务器的路径控制条件，以便将来自所述用户终端的发送包传送到所述认证服务器；在所述访问请求是来自已被认证的用户终端的访问请求的情况下，设定所述访问服务器的路径控制条件，以便将来自所述用户终端的发送包连接到网络上；由所述监视服务器监视所述已被认证的用户终端对网络的访问状态；对来自如下用户终端的发送包、即所述监视的结果被判断为未访问网络的用户终端的发送包，设定所述访问服务器的路径控制条件，以便传送到所述认证服务器。

另外，本发明的访问用户管理装置，其特征在于，具有：接收

来自用户终端的访问请求后将所述用户终端连接到网络上的访问服务器、监视所述用户到网络的连接状态的监视服务器、及进行向所述访问服务器发送了访问请求的用户终端的认证的认证服务器；所述访问服务器具有：对包进行发送接收的单元、对已从用户终端发送的包实施预定的路径控制的单元、及根据已接收的变更请求来变更该路径控制条件的单元；所述监视服务器具有：对包进行发送接收的单元、辨别接收包的发送方是未被认证的用户终端还是已被认证的用户终端的单元、生成向已被认证的用户终端发送的生存确认包或再认证请求包的单元、及生成向所述访问服务器发送的路径控制条件的变更请求包的单元；在一定时间以上没有对所述生存确认请求包或再认证请求包的响应的情况下，向所述访问服务器发送所述路径控制条件的变更请求包；设定所述访问服务器的路径控制条件，以便向所述认证服务器传送来自该一定时间以上没有响应的用户终端的发送包。

因此，在本发明中，其特征在于，配置如下服务器，来替代现有的认证用 Web 服务器，该服务器具有确认用户的连接状态的功能，以及根据确认的用户的连接状态来向访问服务器发送策略路由的策略变更请求或解除当前策略的请求的功能，另外，若在终端侧安装可与该服务器通信的客户机功能，并确认切断用户的连接，则访问服务器不允许用户对因特网自由的访问。

在终端开始因特网访问时，使用所述客户机功能替代 Web 浏览器，进行最初的认证。安装在终端上的客户机功能必须可对来自所述服务器的连接确认请求进行后台响应。这样，用户不反复再认证工作，就能使终端保持连接状态。

上述的服务器和客户机可以是用户管理专用装置，也可以是在已经存在的、具有相同功能的应用程序的服务器中附加了访问服务器设定功能的装置。作为已经存在的应用程序的实例，是以 Instant

Messenger（IM）为代表的、对因特网上特定或不特定的用户公开用户的终端使用状态的存在获知软件（presence awareness software），或邮件服务器（MTA）和邮件客户机（MUA）等。

作为服务器，也可在一台服务器上安装现有认证用服务器具有的认证功能、和策略路由的策略变更请求的发送功能。或者，也可组合存在获知服务器和现有的认证用服务器来使用。

服务器也可将再认证请求发送给终端，来替代所述连接确认请求。但是，此时安装在终端上的客户机必须具备可对来自服务器的再认证请求进行后台响应的功能。终端经由安装的客户机功能，定期地连接于服务器，并执行再认证工作。

本发明具有以下效果：

根据本发明，不设置处理 PPPoE 或 IEEE802.1x 的特殊的访问服务器，可适当地管理用户的连接状态，对用户适当地分配 IP 地址等资源。

附图说明

图 1 是第一发明的序列图。

图 2 是组合了策略路由和 Web 认证的方式的系统示意图。

图 3 是组合了策略路由和 Web 认证的方式的序列图。

图 4 是第一发明的系统示意图。

图 5 是在第一发明中使用的 IM 服务器的功能框图。

图 6 是第二发明的系统示意图。

图 7 是第二发明的序列图。

图 8 是在第二发明中使用的定期认证客户机的功能框图。

图 9 是认证客户机工作的终端的示意图。

图 10 是路由器的框图。

具体实施方式

（实施例 1）

在本实例中，说明使用 IM 作为可取得与用户终端的网络连接状态有关的信息的应用程序的情况。下面，用图 1、图 5 及图 7 来详细说明。图 4 是本发明的系统示意图。与图 2 比较，设置附带访问服务器设定功能的 IM 服务器 8 来替代认证用 Web 服务器 1，在终端 5 上，IM 客户机 503 替代 Web 浏览器来工作，包含 Web 浏览器的其他因特网应用程序 504 工作。

图 1 是本发明的序列图。首先，一旦终端启动，则与图 3 完全相同，OS 500 取得 IP 地址（S101～S104）。接着，从 IM 客户机 503 向 IM 服务器 8 发送使用了用户名和密码的认证请求（S125）。通常 IM 客户机在 OS 启动的时刻自动启动，在 OS 取得 IP 地址的时刻向服务器自动发送认证请求。接收到认证请求的 IM 服务器 8 将认证确认用的认证包发送到认证服务器 2（S126）。若数据库中登录的用户名和密码一致，则认证服务器 2 向 IM 服务器 8 发送可认证的认可包（S127）。在用户名和密码不一致时，认证服务器 2 向 IM 服务器 8 发送不可认证的否认包。

若 IM 服务器 8 接收来自认证服务器 2 的认可包，则向访问服务器 3 发送策略路由的解除请求包、或策略路由中使用的路径控制策略的变更请求包（S128）。这样，对发送端的地址是终端 5 的地址的包，解除或变更访问服务器 3 设定的路径控制的设定条件，经由应用程序 504 向因特网 7 上的任意对象发送从终端 5 发送的包(S129)。另外，IM 客户机 503 也可访问因特网 7 上的其他 IM 服务器(S130)。

认证成功后，IM 服务器 8 定期地将认证确认或生存确认发送到 IM 客户机 503（S131）。相反，IM 客户机返送回认证请求或生存通知（S132）。这样，IM 服务器 8 确认终端 5 正在通信继续中。这样，用户在终端工作期间，不进行再认证的工作，就可进行因特网访问。

这里，考虑在 S134 时刻终端 5 已停止的情况。IM 服务器定期地连续发送认证确认或生存确认，但因终端停止，故不回复响应

（S133）。在这连续一定次数的情况下，IM 服务器判断为终端不通，对访问服务器3进行针对终端5的IP地址的策略路由的设定(S135)。在访问服务器的设定结束的时刻S136，可释放对终端 5 的因特网资源，再次提供给其他的终端使用。

图 5 是本发明中 IM 服务器 8 的功能框图。终端接口部 801 接收来自终端 5 的认证请求、至其他用户的消息等各种通信后，分别分配给适当的功能块，还中转从 IM 服务器 8 内的各功能块至终端 5 的通信。认证部 802 接收来自终端 5 的认证，在认证服务器 2 中进行认证确认，其结果判断用户可否访问。另外，在本发明中，也对访问服务器设定部 805 通知判断结果。终端管理部 803 通过定期地对终端 5 发送认证确认请求或生存确认请求，接收其响应，或者定期地接收来自终端 5 的再认证请求或生存确认，来管理终端 5 的状态。另外，在本发明中，还向访问服务器设定部 805 通知管理状态。其他 IM 功能部 804 实现终端 5 与其他用户的消息通信等、与本发明无关的功能。访问服务器设定部 805 在本发明中是特征功能块，对访问服务器进行针对终端 5 的 IP 地址的策略路由等的设定。

这次为了说明，将访问服务器 3 和 IM 服务器 8、认证服务器 2、DHCP 服务器 4 表示为不同的服务器，但与现有实例相同，若在功能性上等效，则各服务器也可任意组合来缩减。尤其是，访问服务器 3 和 IM 服务器 8 的组合，在想进行端口单位的设定时是有效的。另外，在访问服务器中设置代理（Proxy）服务器功能，用于在 IM 服务器与终端之间代理通信，这样在想进行端口单位的设定时也是有效的。另外，作为 IP 地址分配的实例，给出了 DHCP，但 IP 地址的分配方式也可是任何方式。

（实施例 2）

用图来说明使用 Web 认证时的第二发明的实施例图。在本实施例中，与实施例 1 不同之处在于，作为与认证服务器相连接的应用

服务器，可使用与现有实例相同的 Web 服务器 1。图 6 是本发明的系统示意图。与图 2 比较，在终端 5 上，定期认证客户机 505505 替代 Web 浏览器来工作，包含 Web 浏览器的其他的因特网应用程序 506 来工作。

图 7 是本发明的序列图。首先，终端一旦启动，则与图 3 完全相同，OS 500 取得 IP 地址（S101～S104）。接着，定期从认证客户机 503 向认证用 Web 服务器 1 发送使用了用户名和密码的认证请求（S141）。该工作通过如下设定来实现：在 OS 启动的时刻，自动启动定期认证客户机，在 OS 取得 IP 地址的时刻，定期认证客户机向服务器自动发出认证请求。接收认证请求的认证用 Web 服务器 1 对认证服务器 2 进行认证确认（S142），接收来自认证服务器的认可 S143，对访问服务器进行策略路由的附带期限的解除设定（S144）。这样，终端上的应用程序 506 可对与因特网 7 上任意的对象进行访问（S145）。认证成功后，定期认证客户机定期地将认证信息发送到认证用 Web 服务器 1（S147）。接收该信息的认证用 Web 服务器 1 对访问服务器设定策略路由解除的期限延长（S148）。这样，用户在终端工作期间，不进行再认证的工作，就可进行因特网访问。

这里，考虑终端 5 在 S149 的时刻停止的情况。因终端停止，所以不发送认证信息（151）。在超时期间 S150 的期间连续时，访问服务器判断为终端不通，进行针对终端 5 的 IP 地址的策略路由的设定（S152）。在访问服务器中的设定结束的时刻 S152，释放对终端 5 的因特网资源，可再次提供给其他的终端使用。这里，超时由访问服务器 3 侧设定，但也可由认证用 Web 服务器 1 侧进行超时管理，在超时了的时刻，从认证用 web 服务器 1 对访问服务器 3 设定策略路由。

图 8 是定期认证客户机的功能框图。用户信息管理部 5051 管理用户名或密码等认证所必须的信息。Web 用户访问部 5052 将由用户

信息管理部 5051 管理的信息变换成 http 形式，在启动时和由计时器 5053 通知时，发送到认证用 web 服务器。计时器部 5053 向 web 服务器访问部 5052 通知访问认证用 web 服务器的时间。这次为了说明，将访问服务器 3 和认证用 web 服务器 1、认证服务器 2、DHCP 服务器 4 表示为不同的服务器，但与现有实例相同，若在功能性上等效，则各服务器也可任意组合来缩减。尤其是，想进行端口单位的设定时，组合访问服务器 3 和认证用 web 服务器 1 是有效的。另外，在访问服务器中设置代理服务器功能，用于在认证用 web 服务器和终端之间代理通信，这在想进行端口单位的设定时是有效的。另外，作为 IP 地址分配的实例，给出 DHCP，但 IP 地址分配方式也可是任何方式。

图 9 是定期认证客户机工作的终端示意图。在存储器 50 上，存储着在终端中使用的各种程序（web 浏览器或邮件软件等）506。也分别放置着定期认证客户机 505。CPU 51 实际上执行存储器 50 上的软件。NIF 52 是物理连接于网络上的模块。其他的输入输出装置 53 是键盘或显示器，终端 5 的用户使用这些装置来利用软件。

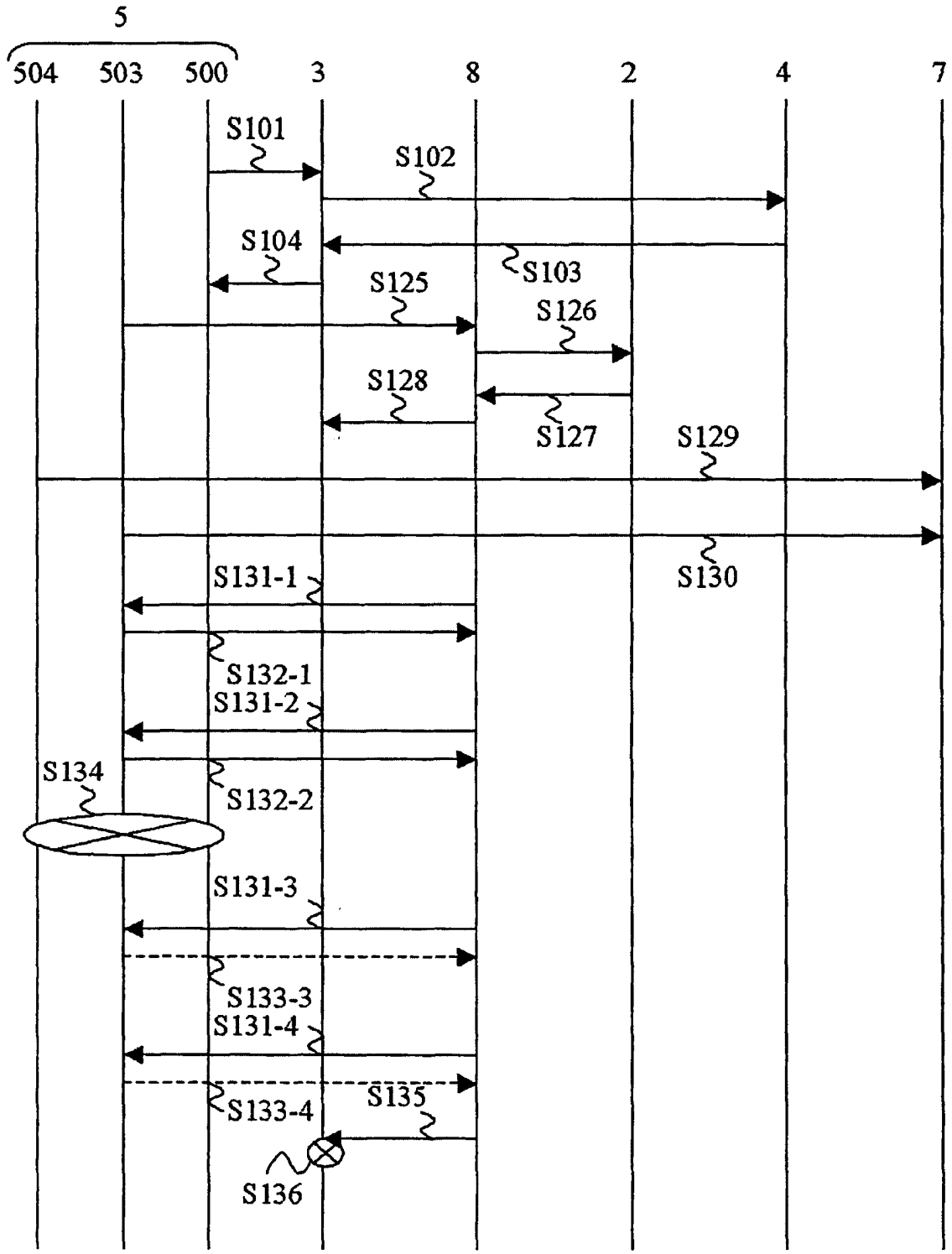

5
504
503
500
3
8
2
4
7
S101
S102
S104
S103
S125
S126
S128
S127
S129
S130
S131-1
S132-1
S131-2
S134
S132-2
S131-3
S133-3
S131-4
S133-4
S135
S136

图1

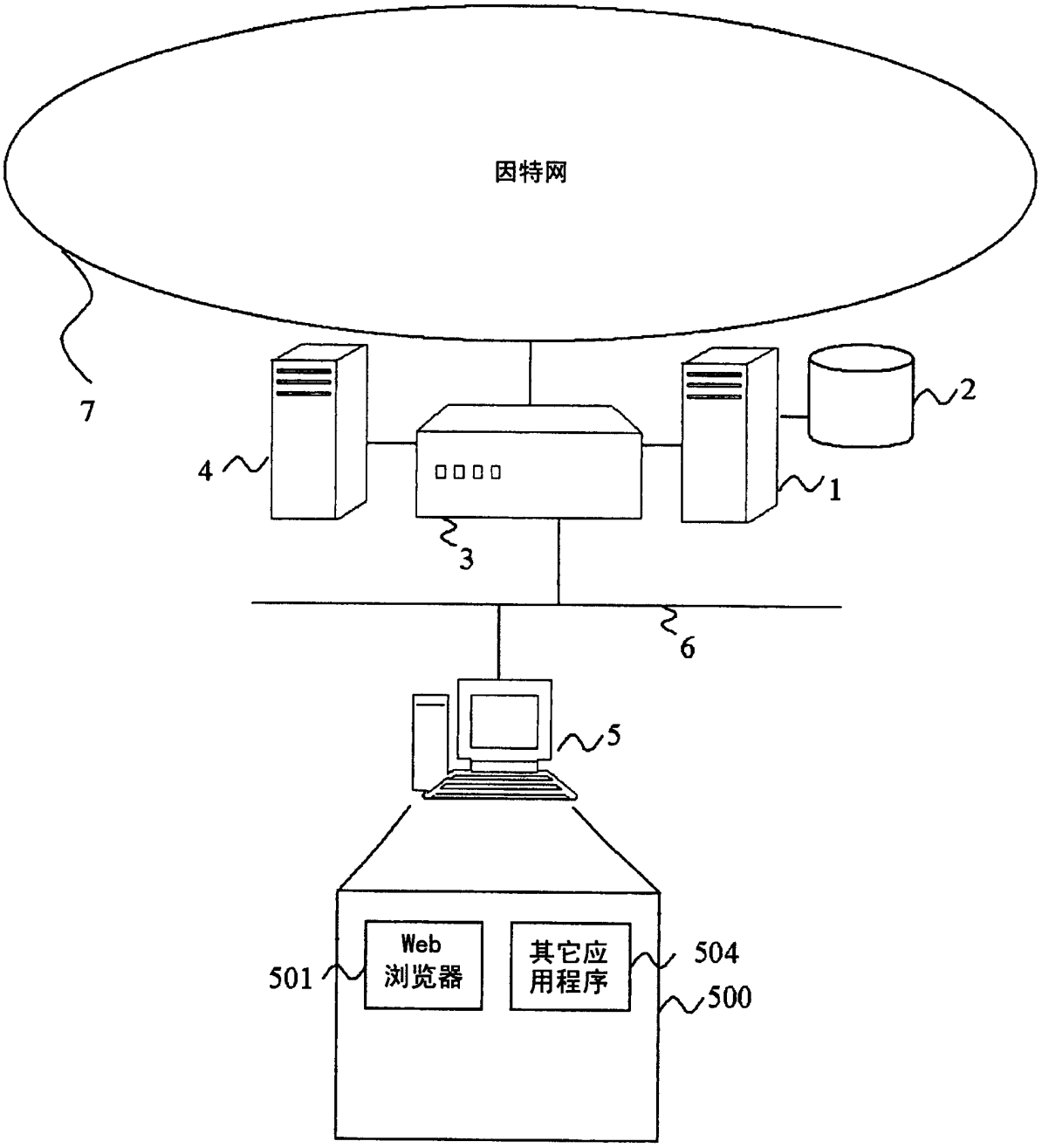


图2

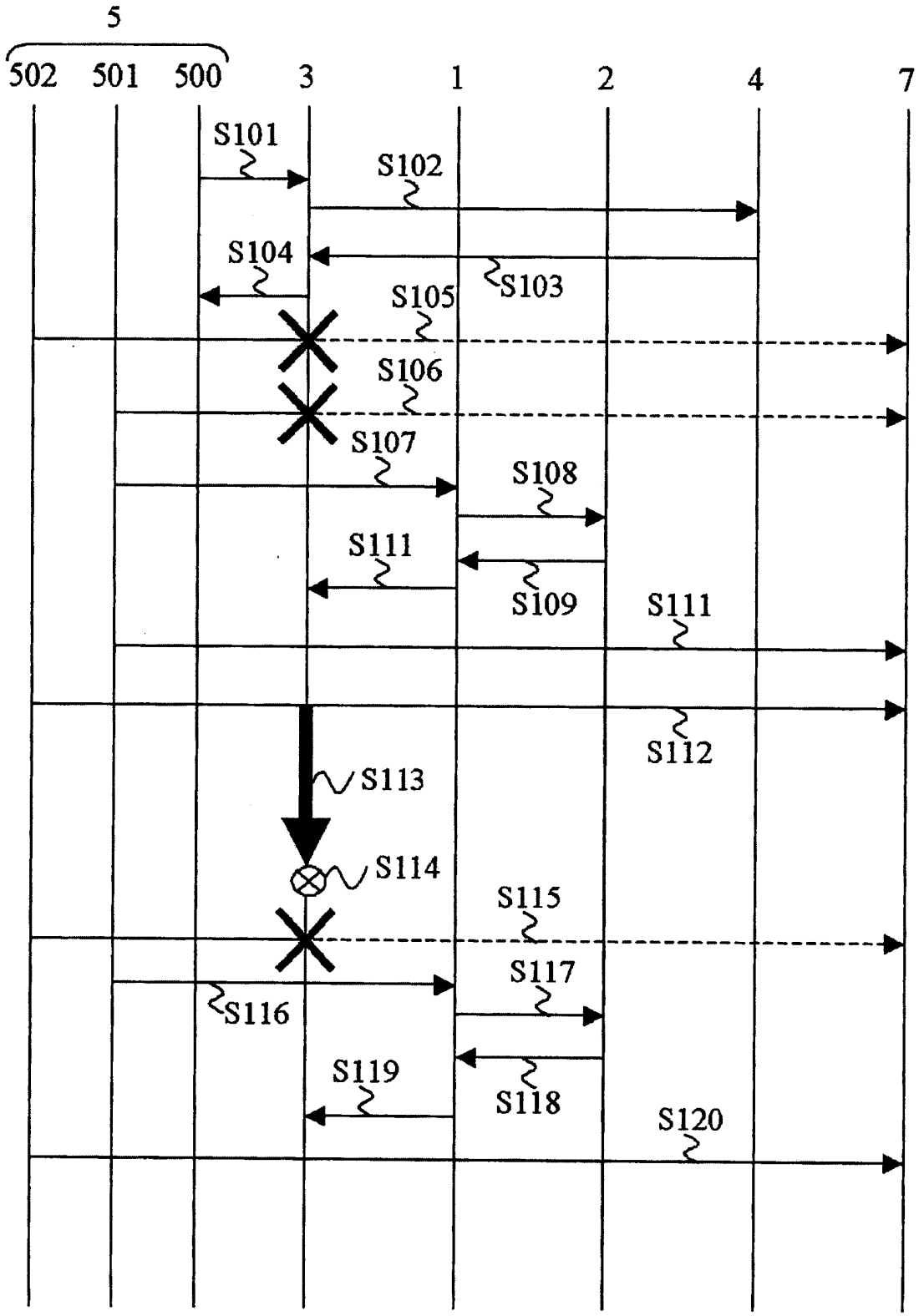

5
502
501
500
3
1
2
4
7
S101
S102
S104
S103
S105
S106
S107
S108
S111
S109
S111
S112
S113
S114
S115
S117
S116
S119
S118
S120

图3

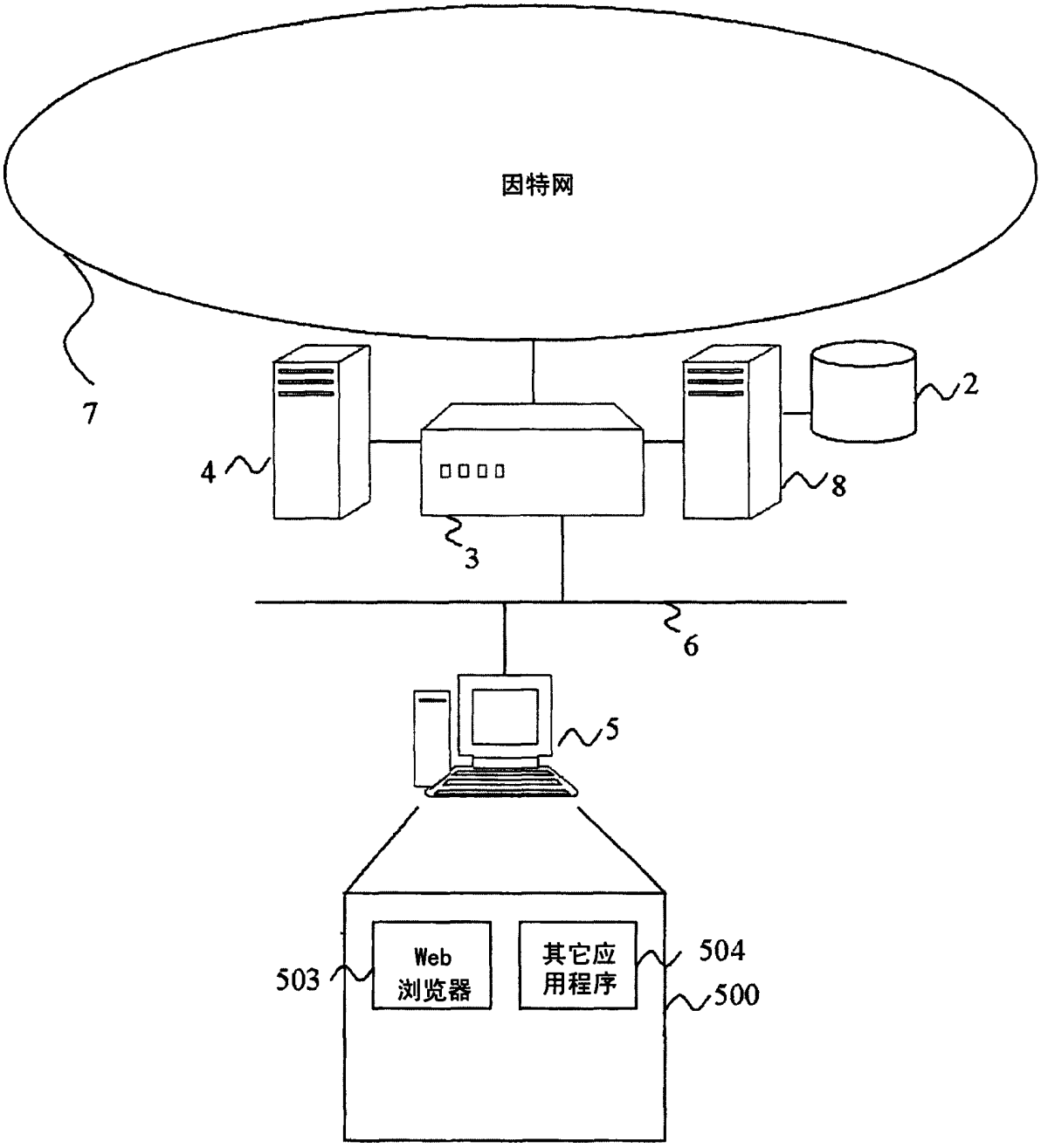


图4

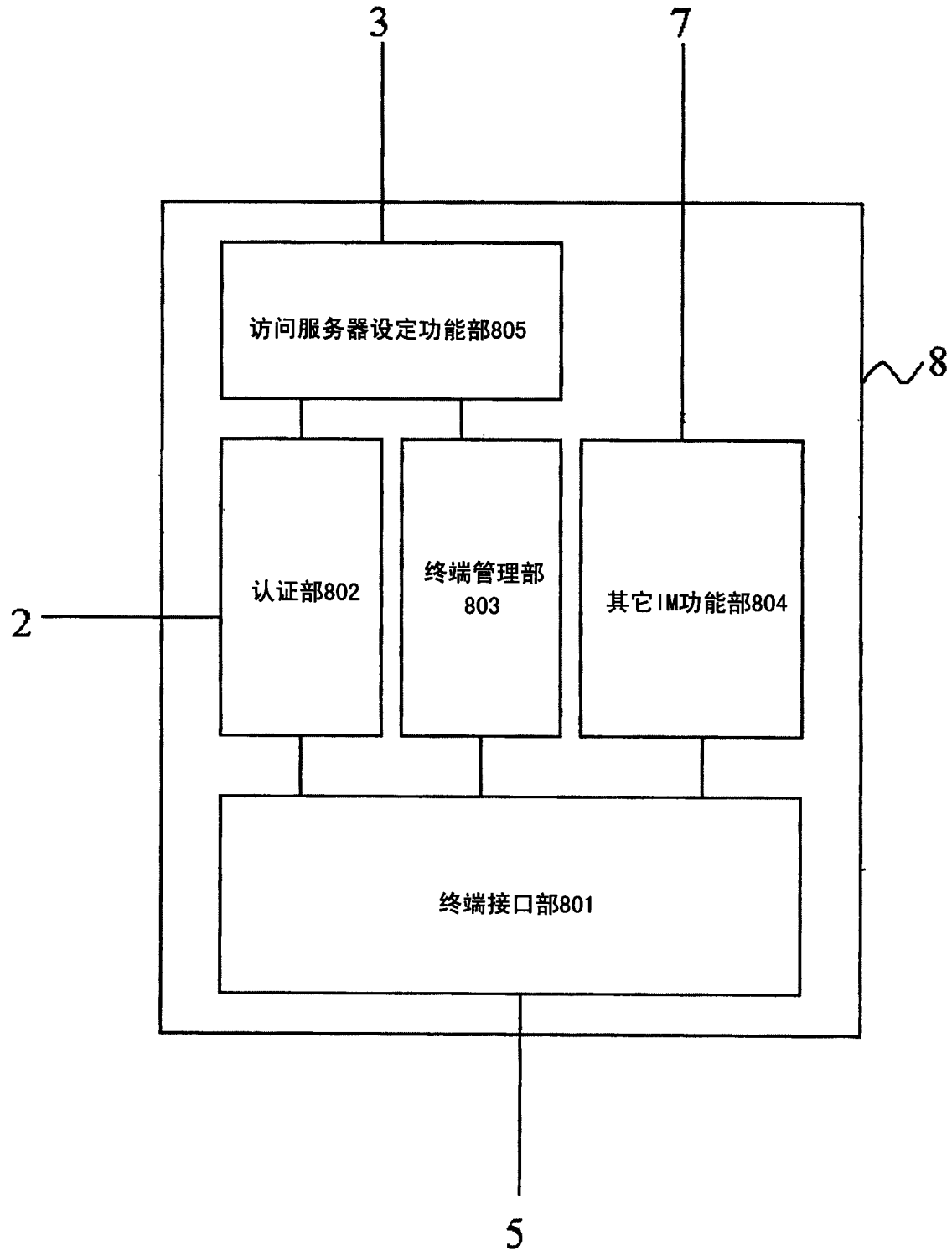

3
7
访问服务器设定功能部805
8
认证部802
终端管理部
803
其它IM功能部804
2
终端接口部801
5

图5

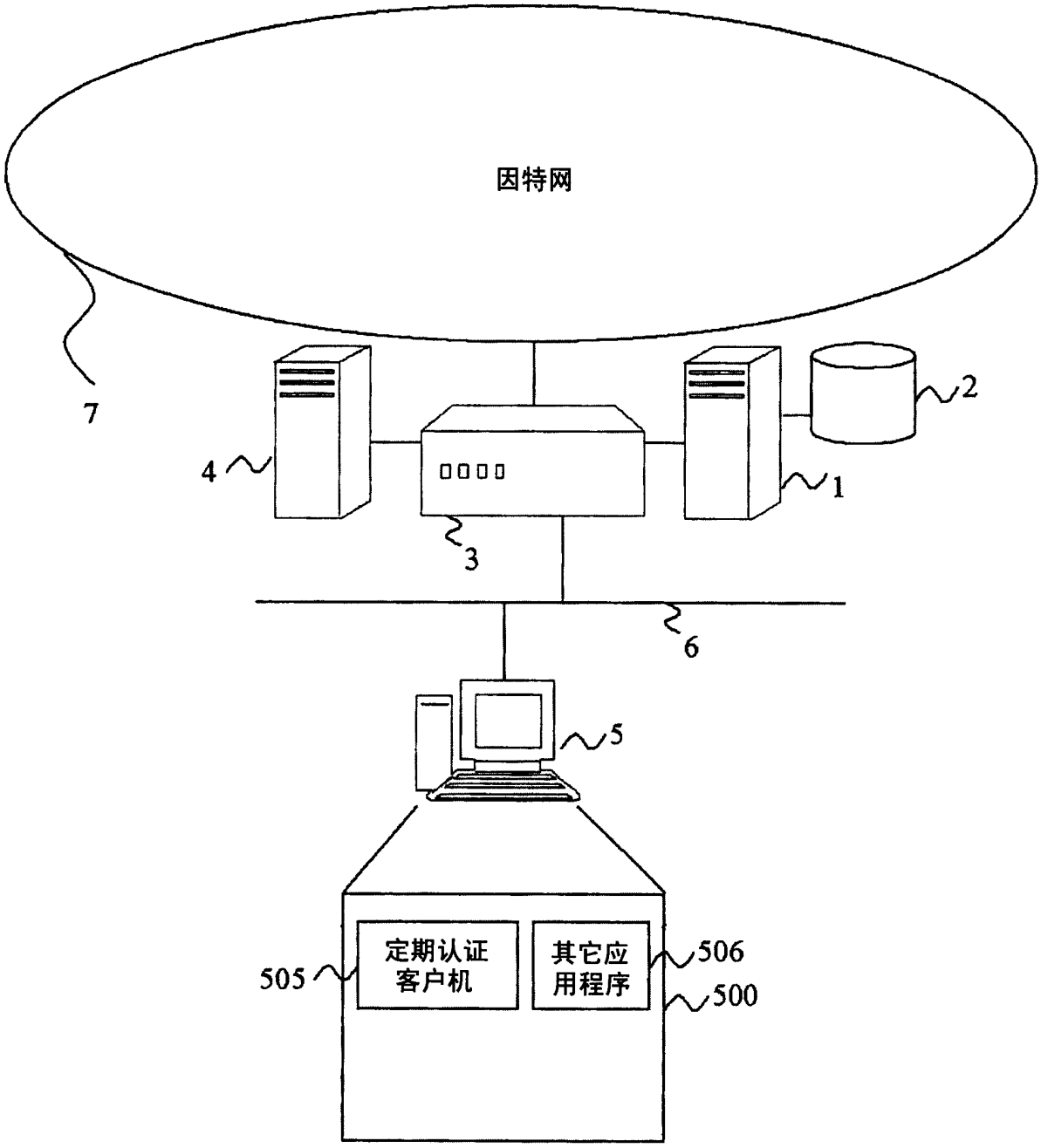


图6

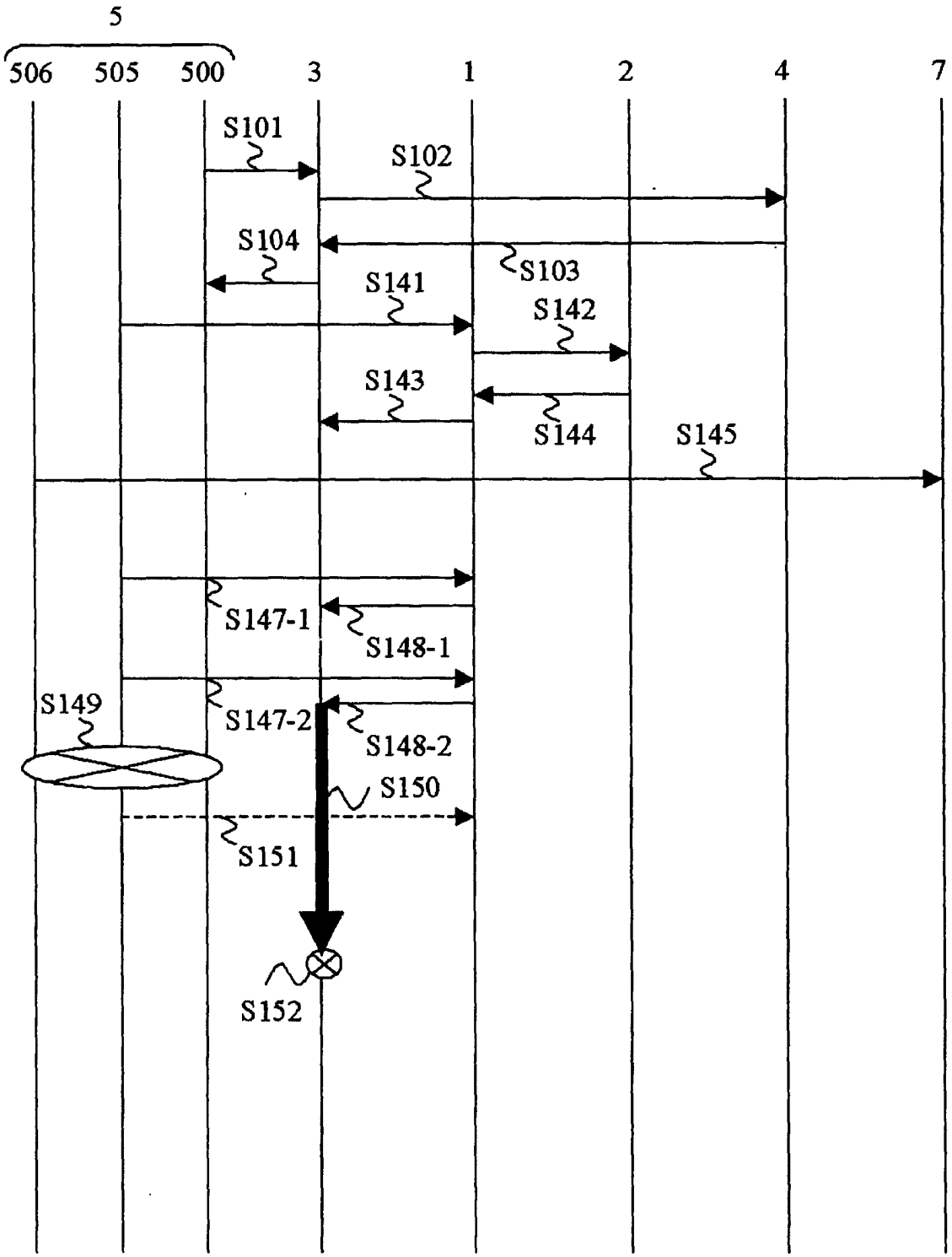

5
506
505
500
3
1
2
4
7
S101
S102
S104
S103
S141
S142
S143
S144
S145
S147-1
S148-1
S149
S147-2
S148-2
S150
S151
S152

图7

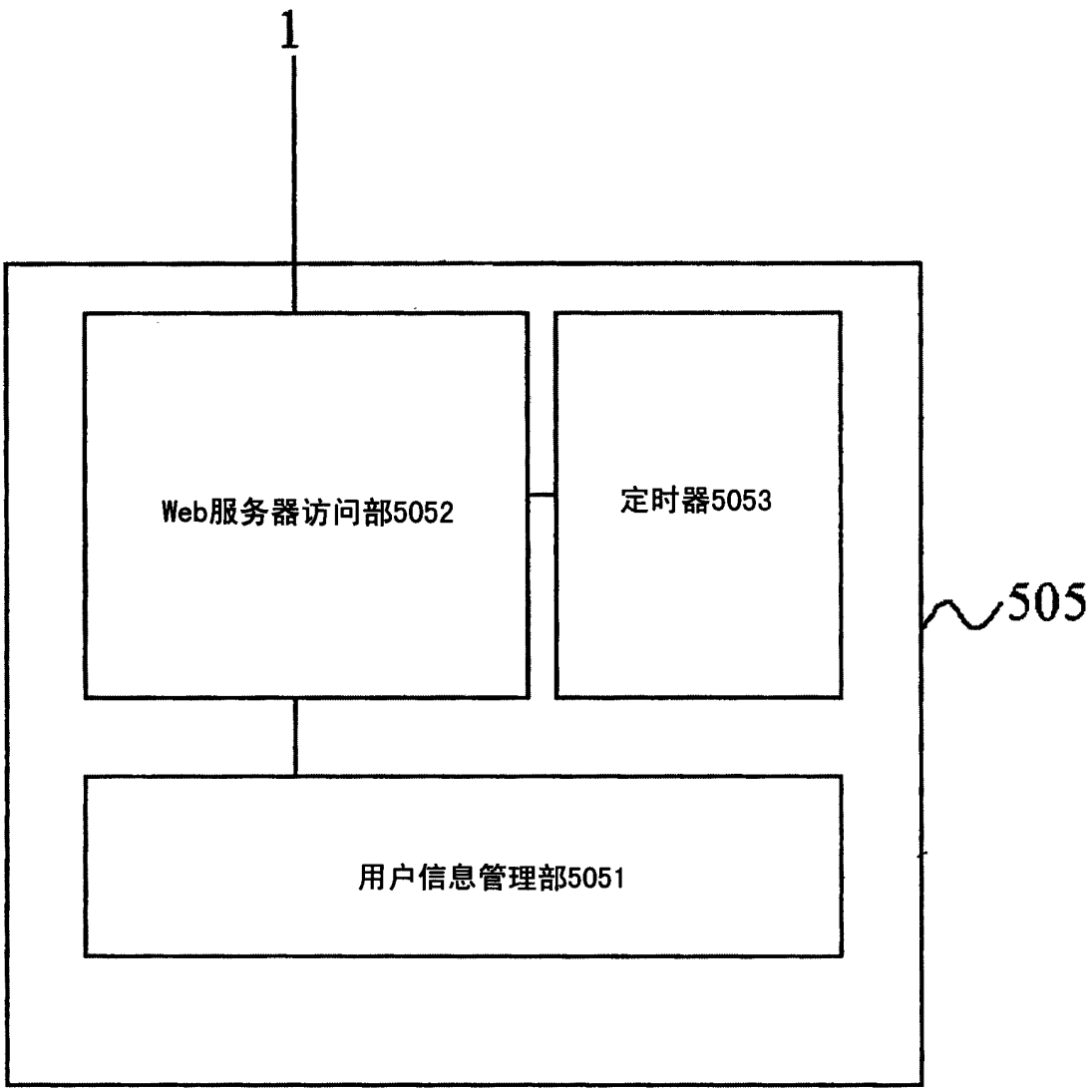


图8

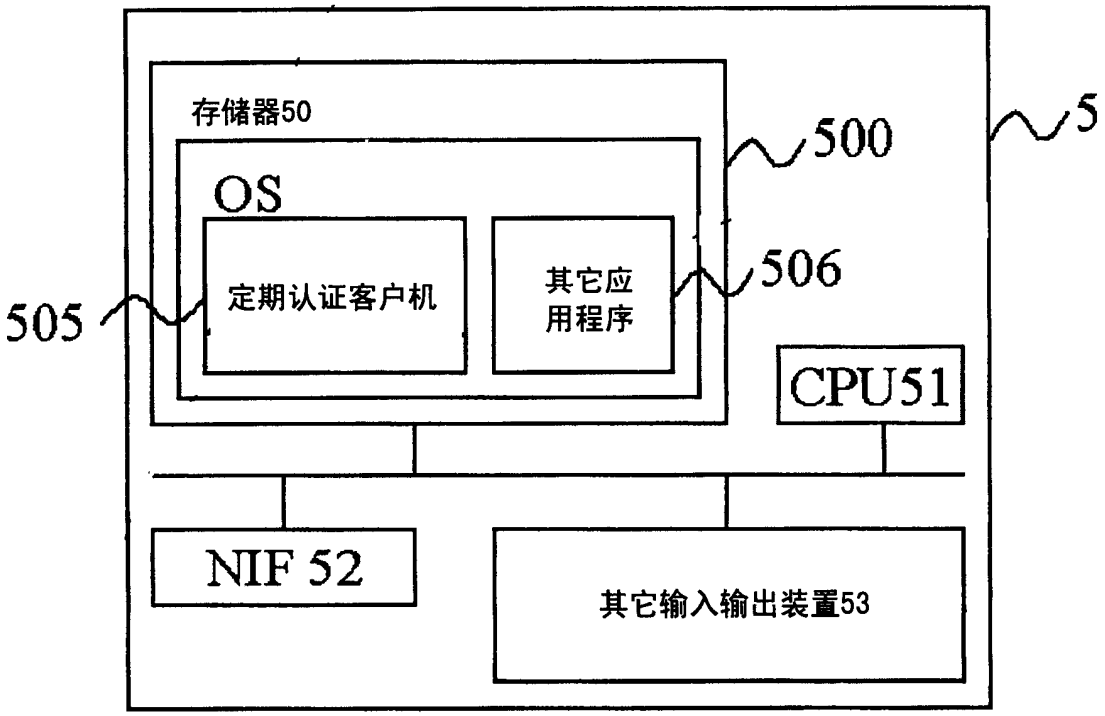

存储器50
OS
500
5
505
定期认证客户机
其它应
用程序
506
CPU51
NIF 52
其它输入输出装置53

图9

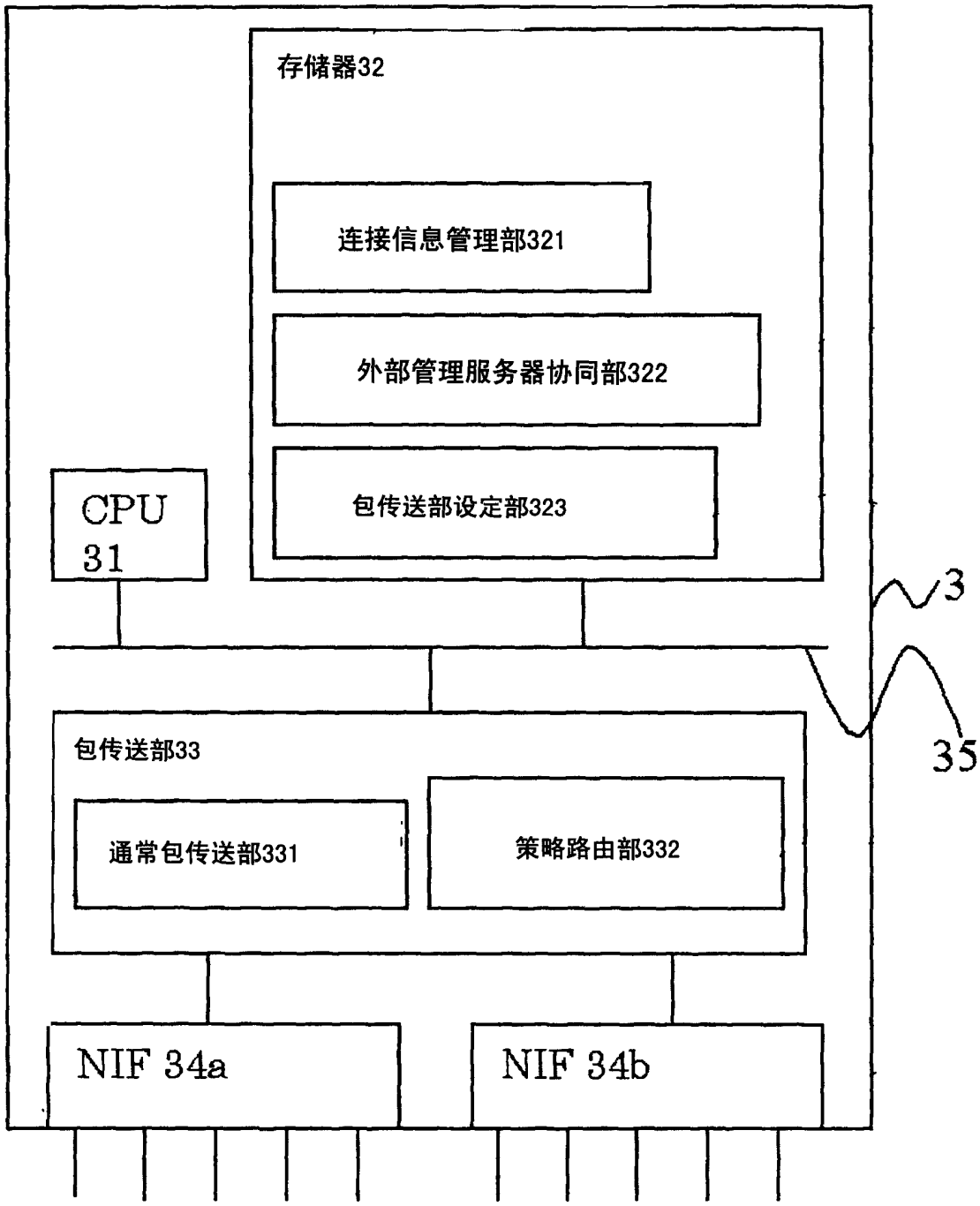

存储器32
连接信息管理部321
外部管理服务器协同部322
包传送部设定部323
CPU
31
3
35
包传送部33
通常包传送部331
策略路由部332
NIF 34a
NIF 34b

图10