

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/28 (2006.01)

H04B 7/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 03148376.3

[45] 授权公告日 2006年6月14日

[11] 授权公告号 CN 1259788C

[22] 申请日 2003.6.30 [21] 申请号 03148376.3

[30] 优先权

[32] 2002.7.1 [33] JP [31] 192508/2002

[71] 专利权人 美禄可股份有限公司

地址 日本爱知县

[72] 发明人 石彻白敬

审查员 何怀燕

[74] 专利代理机构 北京东方亿思知识产权代理有
限责任公司

代理人 陆锦华

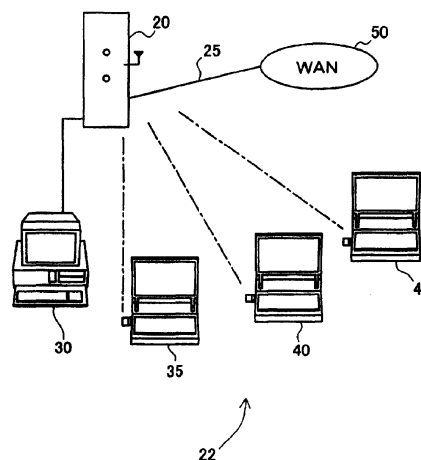
权利要求书2页 说明书9页 附图9页

[54] 发明名称

无线局域网装置

[57] 摘要

一种无线局域网装置，所述局域网装置(20)的管理员在局域网装置中分别为发送源终端的MAC地址或IP地址及发送目的地终端的IP地址设定通讯中可使用的协议。当协议是通讯中可使用的协议时，局域网装置发送数据，当协议是不可使用的协议时，就不发送数据。从而提供了一种内部具有控制通讯功能的局域网装置。



- 1、一种连接多个客户端并构筑局域网的局域网装置，具有：
通讯接收部分，接收来自所述客户端的、向所述局域网其他客户端
5 或其他网络进行通讯的请求；
注册部分，注册所述局域网客户端中规定的客户端的指定客户端；
判断部分，判断所述通讯请求是否为向所述指定客户端的通讯的请求；以及
限制部分，通过所述判断部分，当判断为向指定客户端的通讯时，
10 通过限制所述通讯的协议来限制所述通讯，当判断为不是向指定客户端的通信请求时，不进行通信的限制。
- 2、如权利要求 1 所述局域网装置，其中，
所述注册部分，通过其 IP 地址注册所述指定客户端；
所述判断部分，通过存储在所述通讯请求中的 IP 地址进行所述判
15 断。
- 3、如权利要求 1 所述局域网装置，具有：
判别部分，判别进行所述通讯请求的客户端；以及
所述限制部分，根据所述判别部分发出的判别结果，改变所述协议的
限制内容。
- 20 4、如权利要求 3 所述局域网装置，其中，所述判别部分通过搭载
在所述客户端的网络机器的 MAC 地址来判别所述客户端。
- 5、如权利要求 3 所述的局域网装置，其中，所述判别部分通过所
述客户端的 IP 地址来判别所述客户端。
- 6、如权利要求 3 所述局域网装置，其中，所述限制部分是 WAN
25 限制部分，其当所述通讯请求为向所述其他网络的通讯的请求时，通
过限制所述通讯的协议来限制所述通讯。
- 7、如权利要求 6 所述局域网装置，其中，所述 WAN 限制部分根
据所述判别部分发出的判别结果来改变所述协议的限制内容。

8、如权利要求 1 所述局域网装置，其中，所述协议的限制是通过限定可通讯的协议来进行的。

9、一种总括连接了多个客户端的局域网的方法，其特征在于，接收来自所述客户端的、向所述局域网其他客户端或其他网络进行
5 通讯的请求；

注册所述局域网客户端中规定的客户端的指定客户端；

判断所述通讯请求是否为向所述指定客户端的通讯的请求；以及

通过所述判断，当判断为向指定客户端的通讯时，通过限制所述通讯的协议来限制所述通讯，当判断为不是向指定客户端的通信请求
10 时，不进行通信的限制。

无线局域网装置

5 技术领域

本发明涉及连接多个客户端的局域网装置。

背景技术

以往，在像互联网那样以经常连接为前提的网络中，准备有这样的
10 环境：在公司、大学等的设施内构筑内部网络(intranet)等局域网络
(LAN)，并经路由器或网关，将其经常连接在互联网等的广域网
(WAN)上。在这样的局域网中，可以预先特别指定连入局域网的客
户端(计算机或使用者)。与此相对，近年来，在狭小范围的公共区
域内，提供一种使没有特别指定的客户端连接高速局域网的服务(即
15 热点(注册商标)服务)。就是说，可以在店铺内等构筑局域网，并
让顾客自由连接，可以连接外部的互联网等。最近，随着无线局域网
的普及，不必再用电缆将计算机一个一个连接到互联网上，而可以享受
这种服务。

这种热点服务(hotspot service)，如果是小规模，可以很容易地
20 通过用于无线局域网的路由器来构筑。我们知道，无线局域网装置，
通常可连接几台到十几台客户端，而且，还可以通过有线方式连接若
干台计算机。因此，可以有这样的使用方法：即，在咖啡店、美容院
等小规模店铺内安装无线局域网装置，并且将有线方式连接的计算机
用作控制局域网的管理服务器，而将无线方式连接向店内使用者开
25 放。

但是，实现这样的热点服务时，如何实现网络安全就成了问题。在
通常的内部网络等中，连接的客户端是固定的，使用者名字等由管理
员进行识别。在连接网络的机器中，虽然被标注硬的MAC地址这种唯

一的符号，但是，如果使用这个 MAC 地址，则可以识别连入局域网的机器，也可以通过确认 MAC 地址，较容易地进行对预先特别指定的服务允许或不允许。然而，由于热点服务中连接的客户端是不特别指定的，因此通过注册这种 MAC 地址注册的管理是不实际的。虽说如此，
5 但是，若允许客户端无限制地连接，就可以对管理用服务器内的数据进行存取，从而，有时会成为导致一些问题的原因。

针对这样的问题，可以考虑将管理服务器放在与用于热点服务的局域网不同的网络上，或是在管理服务器连接 RAM 的地方设置 VLAN 开关或防火墙，但此时都需要设置新机器，这与欲提供简便而小规模的热
10 点服务的目的是相违背的。

发明内容

本发明的目的是提供一种局域网装置，从而解决上述问题，同时，满足向局域网装置的简便连接和确保网络安全这两个要求。

15 至少解决一部分上述问题的本发明的装置，是连接多个客户端并构筑局域网的局域网装置，其特征在于，具有：

通讯接收部分，接收来自所述客户端的、向所述局域网其他客户端或其他网络进行通讯的请求；

注册部分，注册所述局域网客户端中规定的客户端的指定客户端；

20 判断部分，判断所述通讯请求是否为向所述指定客户端的通讯的请求；以及

限制部分，通过所述判断部分，当判断为向指定客户端的通讯时，通过限制所述通讯的协议来限制所述通讯，当判断为不是向指定客户端的通信请求时，不进行通信的限制。

25 此外，与本装置对应的方法的发明，是总括连接多个客户端的局域网的方法，其特征在于，

接收来自所述客户端的、向所述局域网其他客户端或其他网络进行通讯的请求；

注册所述局域网客户端中规定的客户端的指定客户端；

判断所述通讯请求是否为向所述指定客户端的通讯的请求；

通过所述判断，当判断为向指定客户端的通讯时，通过限制所述通讯的协议来限制所述通讯，当判断为不是向指定客户端的通信请求时，不进行通信的限制。

- 5 根据这种局域网装置及方法，可以限制从构成局域网的终端向规定的终端的存取（access）。此外，若根据请求通讯的终端改变协议的限制内容，就可以进行各种存取限制。还有，即使根据被请求通讯的终端来改变协议的限制内容，也可以进行各种存取限制。

附图说明

- 10 图 1 是热点系统 22 的说明图。
图 2 是管理服务器 30 的内部结构说明图。
图 3 是局域网装置 20 的内部结构说明图。
图 4 是经营者数据库 75 的说明图。
图 5 是第一实施例中的发送数据库 85 的说明图。
15 图 6 是第一实施例中的局域网装置 20 的处理流程图。
图 7 是第二实施例中的发送数据库 85 的说明图。
图 8 是第二实施例中的局域网装置 20 的处理流程图。
图 9 是第三实施例中的发送数据库 85 的说明图。
图 10 是第三实施例中的局域网装置 20 的处理流程图。

20 具体实施方式

（第一实施例）

（1）结构

- 以下，参照附图说明本发明的实施方式。图 1 是提供所述热点服务的系统（以下称为热点服务系统 22）的整体结构图。所谓热点服务，
25 就是提供从通过局域网装置 20 构成的局域网连入 WAN 50 的环境这样的服务。热点服务系统 22 由局域网装置 20、管理服务器 30、经营者客户端 35 和一般客户端 40 构成。管理服务器 30 是用于管理热点服务系统 22 的终端。经营者客户端是提供热点服务系统 22 的咖啡店、美容院等的经营者的终端，经营者自身在利用热点服务系统连入 WAN 50 时

使用。一般客户端是利用热点服务系统 22 的使用者的终端。管理服务器 30、经营者客户端 35 和一般客户端 40 统称为热点终端。热点终端均属于同一物理段。

局域网装置 20 通过 ADSL 回路 25 连接提供者，并经提供者连入
5 WAN 50。热点终端可以通过有线或无线方式连接局域网装置 20，并通过局域网装置 20 连入 WAN 50。此外，也可以通过局域网装置 20 与其他热点终端相互通讯。其中，通讯协议使用 TCP/IP，即在网络层使用 IP 协议，在传输层使用 TCP 协议。还有，管理服务器 30 和经营者客户端 35 的私人 IP 地址是固定的，而一般客户端的私人 IP 地址是由局
10 域网装置 20 动态分配。热点终端与 WAN 50 通讯时，局域网装置 20 将私人 IP 地址变换为全局 IP 地址进行通讯。

接下来，根据图 2 说明管理服务器 30 的内部结构。管理服务器 30 具有，通过局域网装置 20 控制与 WAN 50 的数据交换的网络接口（NT-I/F）70、进行处理的 CPU 80、存储处理程序及固定数据的 ROM
15 90、作为工作区的 RAM 100、管理时间的计时器 110、向监视器 165 进行显示的显示电路 130、将文本数据作为数据库存储的硬盘（HD）120、以及用作键盘 150 或鼠标 160 接口的输入接口（I/F）140 等。

还有，硬盘 120 是以固定式硬盘进行了说明，但也可以使用拆装式硬盘，还可以同时使用拆装式存储装置（例如 CD-ROM、CD-R、CD-
20 RW、DVD-ROM、DVD-RAM、软盘等）。并且，在本实施例中，管理服务器 30 的处理程序被存储在 ROM 90 内，但也可以先存储在硬盘 120 中，启动时在 RAM 100 上展开并运行。或者，也可以从所述拆装式存储媒体读取。甚至，还可以通过局域网装置 20 从其它终端读取并运行。同样地，也可以采取如下的结构形式，即，不必将所有必要的
25 数据存储存储在硬盘 120 上，可以在通过局域网装置 20 而连接的其他终端上分散存储、更新和管理庞大的数据。还有，经营者客户端、一般客户端的内部结构也与管理服务器 30 大致相同。

图 3 是局域网装置 20 的内部结构说明图。局域网装置 20 由控制器 95、存储器 105 和输入输出部分 65 构成。存储器 105 中存储着本实施

例中使用的两个数据库。即，经营者数据库 75 和发送数据库 85。在这些数据库中进行数据的注册或删除时，需要热点系统 22 的管理员的密码。而且，这些数据库的管理（数据的注册、删除等）只能由管理服务器 30 进行。

- 5 经营者数据库 75 的一个例子如图 4 所示。经营者数据库 75 是注册了管理服务器 30 和经营者客户端 35 的 MAC 地址及局域网内部的 IP 地址，即私人 IP 地址的数据库。

10 发送数据库 85 如图 5 所示。发送数据库 85 是注册了一般客户端可用于通讯的协议的数据库。因为对于一个协议，热点系统 22 的热点终端使用预先规定的端口，所以在发送数据库 85 中，将协议和端口号配对存储。还有，这以下所说的协议指的是在 TCP/IP 协议中应用层的协议。

15 图 3 的输入输出部分 65 由主管与 WAN 50 的输入输出的 WAN 部分 45、主管无线通讯的输入输出的无线部分 55 及主管有线通讯的输入输出的有线部分 60 构成。无线部分 55 或有线部分 60，主管与热点系统 22 的热点终端的输入输出。控制器 95 总括局域网内部的动态。

(2) 处理

20 即根据图 6 说明第一实施例中局域网装置 20 的处理，其中，局域网装置 20 限制由热点终端向管理服务器 30 和经营者客户端 35 进行通讯的协议。当通过无线部分 55 或有线部分 60 接收到数据（步骤 S15）时，局域网装置 20 用存储在所接收数据头部的、发送源的 MAC 地址，检索经营者数据库 75 的 MAC 地址段（步骤 S20）。若该 MAC 地址存在（步骤 S25），则接收到的数据是来自管理服务器 30 或经营者客户端 35 的通讯。所以，对通讯协议不做任何限制，将接收数据向作为发送目的地所指定终端的地址发送（步骤 S30）。当发送的数据是要求返回数据的返回请求数据时（例如互联网中的 URL），会应对返回请求数据而发回返回数据（用于显示符合所述例中 URL 的网页），所以，此时接收返回数据（步骤 S32）。并且，向发出返回请求数据的管理服务器或经营者客户端的地址发送返回数据（步骤 S32）。

若经营者数据库 75 中不存在所述 MAC 地址（步骤 S25），则接收到的数据是来自一般客户端 40 的通讯。所以接下来，通过存储在接收数据的头部的、发送目的地的 IP 地址，检索经营者数据库 75 中的 IP 地址段（步骤 S35）。若该 IP 地址不存在（步骤 S40），则接收数据是

5 发送至 WAN 50 或热点服务系统 22 的一般客户端 40 的数据。所以，对通讯协议不做任何限制，将接收数据向作为发送目的地所指定终端的地址发送（步骤 S30）。当发送的数据是返回请求数据时，接收返回数据，并向发出返回请求数据的一般客户端 40 的地址发送返回数据（步骤 S32）。

10 当该 IP 地址存在时（步骤 S40），接收数据就是向管理服务器 30 或经营者客户端的 35 的通讯。因此，由于限制了协议，通过存储在接收数据头部的端口号，检索发送数据库 85 的端口号段（步骤 S45）。当端口号不存在时（步骤 S50），由于通过该协议的通讯被禁止，因此，不发送所接收数据而结束。当端口号存在时（步骤 S50），向作为

15 发送目的地所指定终端的地址发送接收数据（步骤 S30）。当发送的数据是返回请求数据时，就接收返回数据，并向发出返回请求数据的一般客户端 40 的地址发送返回数据（步骤 S32）。

根据以上说明的实施例，在使用局域网装置 20 的系统中，不用设置其他路由器或防火墙等机器，就可以限制一般客户端 40 对管理服务器

20 30 或经营者客户端 35 的访问。

（第二实施例）

第二实施例是，根据一般客户端 40 的类型改变协议的限制内容的热点服务系统 22 的例子。热点服务系统 22 的管理员将一般客户端 40

25 分为高级客户端和次级客户端的两种类型。协议的限制没有严格设定的为高级客户端，而严格设定的为次级客户端。例如，支付了较多热点系统 22 的使用费时，设为高级客户端，或者是诚信的使用者也设为高级客户端。于是，将被搭载在高级客户端的网络机器的 MAC 地址存储在局域网装置 20 内存储器 105 上的高级数据库 115 中。对于所述存

储，需要管理员的密码，并只能由管理服务器 30 进行。而且，高级客户端和次级客户端的可使用的协议几乎是不同的。

第二实施例中发送数据库 85 的一个例子如图 7 所示。高级协议是高级客户端对管理服务器 30 或经营者客户端 35 通讯时可使用的协议。

- 5 高级端口号是高级协议的通讯中所使用的、预先规定的端口号。此外，次级协议是次级客户端对管理服务器 30 或经营者客户端 35 通讯时可使用的协议。次级端口号是次级协议的通讯中所使用的、预先规定的端口号。

10 图 8 是在第二实施例中的局域网装置 20 的处理流程图。在图 6 的判断处理（步骤 S55）后，发送目的地是管理服务器 30 或经营者客户端 35 时（图 6 之③），首先判断发送接收数据的一般客户端 40 是高级客户端还是次级客户端。为此，用存储在接收数据头部的发送源终端的 MAC 地址，检索高级数据库 115（步骤 S60）。

15 当 MAC 地址存在于高级数据库 115 中时，即发送源终端是高级客户端时（步骤 S65），用存储在接收数据头部的端口号，检索发送数据库 85 的高级端口号段（步骤 S70）。当该端口号不存在时（步骤 S75），通过该协议的通讯被禁止，因此，不发送所接收数据而结束。当端口号存在时（步骤 S75），就向作为发送目的地所指定终端的地址发送所接收数据（步骤 S80）。发送数据是返回请求数据时，接收返回数据，并向发出返回请求数据的高级客户端的地址发送返回数据（步

20 骤 S82）。

当高级数据库 115 中不存在 MAC 地址时，即发送源终端是次级客户端时（步骤 S65），用存储在接收数据头部的端口号，检索发送数据库 85 的次级端口号段（步骤 S85）。当该端口号不存在时（步骤

25 S90），该协议的通讯被禁止，因此，不发送所接收数据而结束。当端口号存在时（步骤 S90），向作为发送目的地所指定终端的地址发送接收数据（步骤 S80）。所发送数据是返回请求数据时，就接收返回数据，并向发出返回请求数据的次级客户端的地址发送返回数据（步骤 S82）。

根据以上说明的第二实施例，不仅可发挥与第一实施例相同的作用效果，而且还可以对一般客户端 40 进行分类，并对它们分别指定各自可使用的协议，从而，可以对管理服务器 30 或经营者客户端 35 分阶段地设定网络安全。

5

（第三实施例）

在第三实施例中，不仅对管理服务器 30 或经营者客户端 35，还限制向 WAN 50 的通讯。第三实施例的发送数据库 85 如图 9 所示。高级 WAN 协议是高级客户端对 WAN 50 通讯时可使用的协议。高级 WAN 10 端口号是高级 WAN 协议的通讯中所使用的、预先规定的端口号。而且，次级 WAN 协议是次级客户端对 WAN 50 通讯时可使用的协议。次级 WAN 端口号是次级 WAN 协议的通讯中所使用的预先规定的端口号。

图 10 是在第三实施例中的局域网装置 20 的处理流程图。在图 6 的 15 判断处理（步骤 S55）后，当发送目的地既不是管理服务器 30 也不是经营者客户端 35 时（图 6 之②），判断发送目的地的 IP 地址是否为私人 IP 地址，即是否为热点终端的 IP 地址（步骤 S100）。当是私人 IP 地址（步骤 S100）时，不限制任何协议，将接收数据向作为发送目的地所指定终端的地址发送（步骤 S105）。当发送数据是返回请求数据 20 时，就接收返回数据，并向发出返回请求数据的一般客户端 40 的地址发送返回数据（步骤 S107）。当不是私人 IP 地址时（步骤 S100），进行在第二实施例中进行的高级、次级发送处理（步骤 S95）。还有，在这时的高级、次级发送处理中而检索发送数据库时，若是高级客户端就检索高级 WAN 端口号，是次级客户端就检索次级 WAN 端口号。

25 根据以上说明的第三实施例，不仅可以发挥与第一实施例、第二实施例相同的作用效果，而且，还可以限制向 WAN 50 的通讯。

以上，尽管阐述了本发明的实施方式，但本发明并不局限于所述的实施方式，在不脱离本发明特征的范围，可以采用其他各种各样的实施方式。例如，由热点终端向管理服务器 30 或经营者客户端 35 进行

通讯时，可以区分管理服务器 30 或经营者客户端 35，能够以各自不同的协议进行通讯。这对在管理服务器 30 和经营者客户端 35 上想要进行不同设定时是很有效的。

- 此外，也可以限制由一般客户端 40 向一般客户端 40 的通讯协议。
- 5 这对想要限制一般客户端 40 间的访问时也是很有效的。而且，实施例中协议的分类为两类，但可不必那样，对应热点终端也可以分为任何几类。

- 还有，在第二实施例、第三实施例中，在高级数据库中存储了高级客户端，但这并不是必需的，也可以在次级数据库中存储次级客户端，
- 10 可将热点终端分为更加详细的等级。

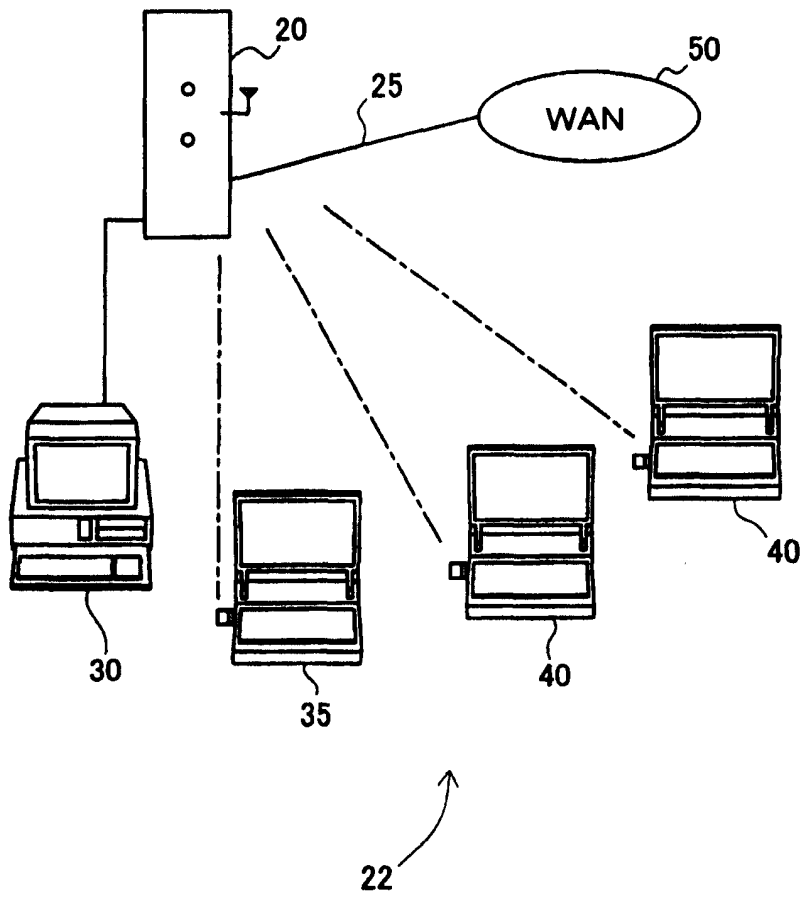


图1

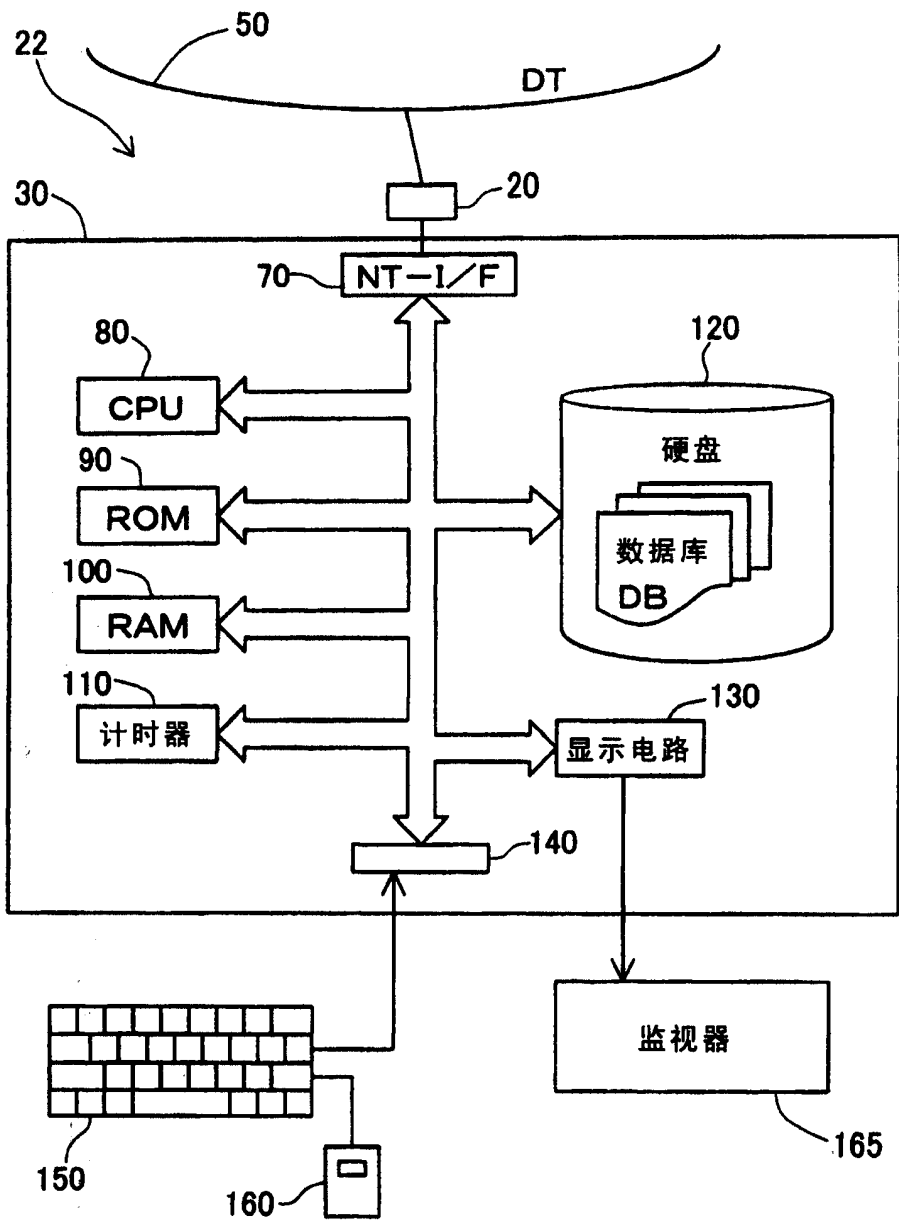


图2

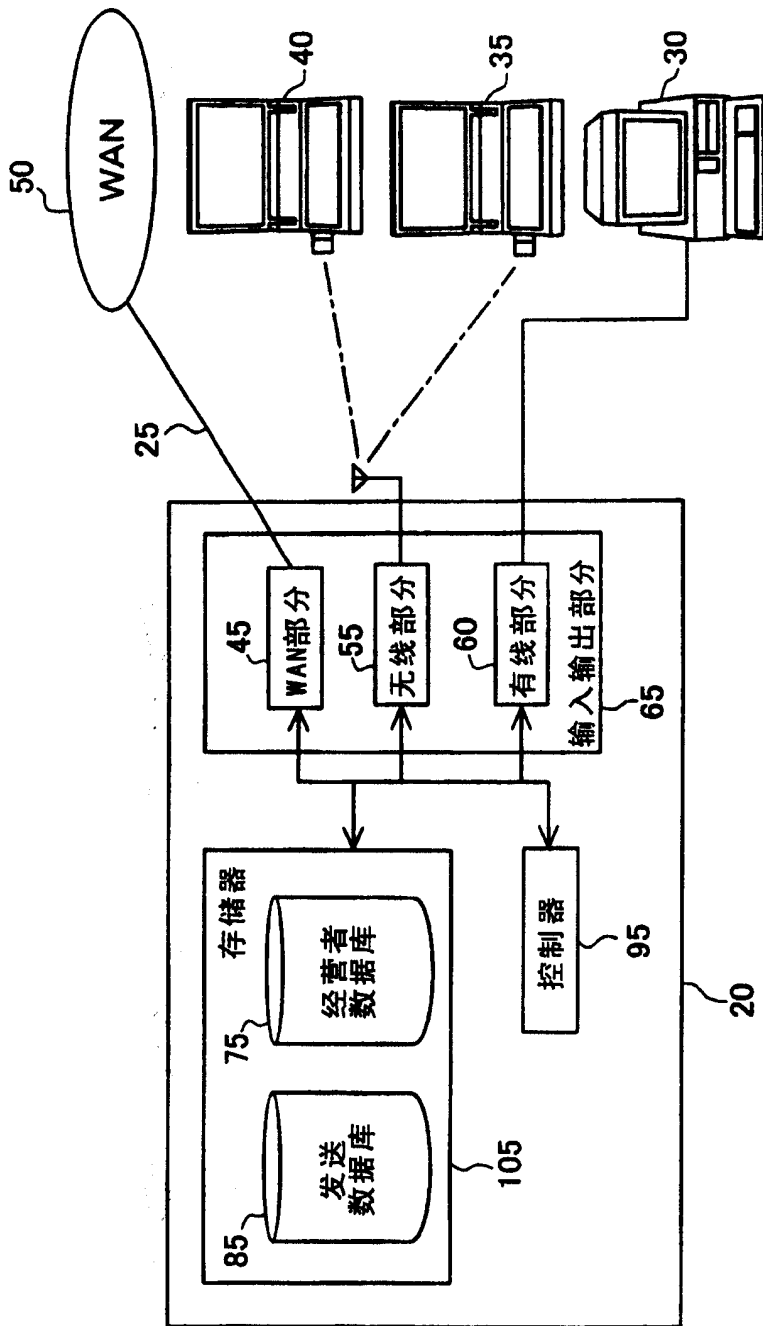


图3

MAC 地址	IP 地址
...	...
000	xxxx
...	...

75

图4

协议	端口号
...	...
xx	00
...	...

85

图5

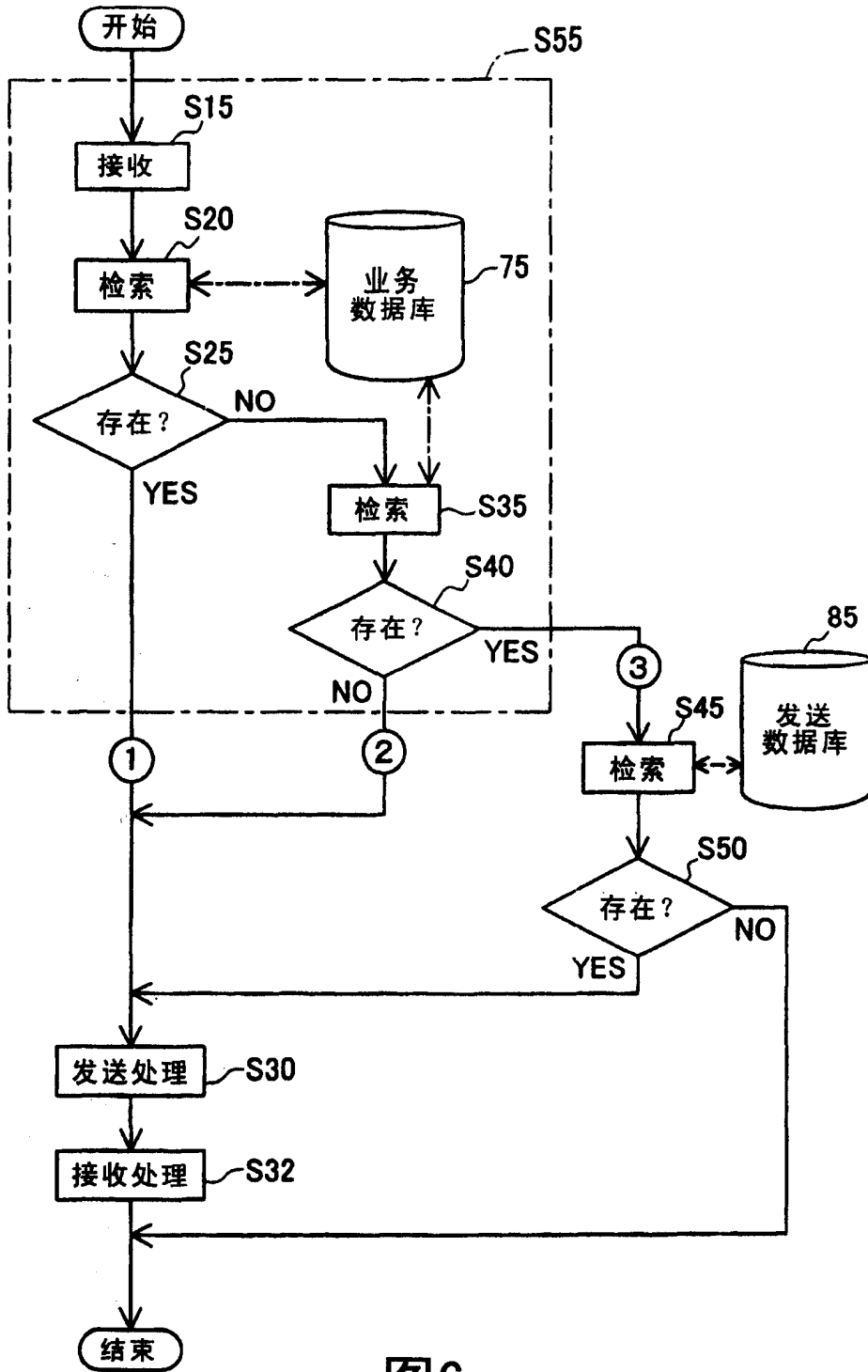


图6

高级协议	高级端口号	次级协议	次级端口号
HTTP	80
SMTP	25		
POP3	110		
...	...		

85

图7

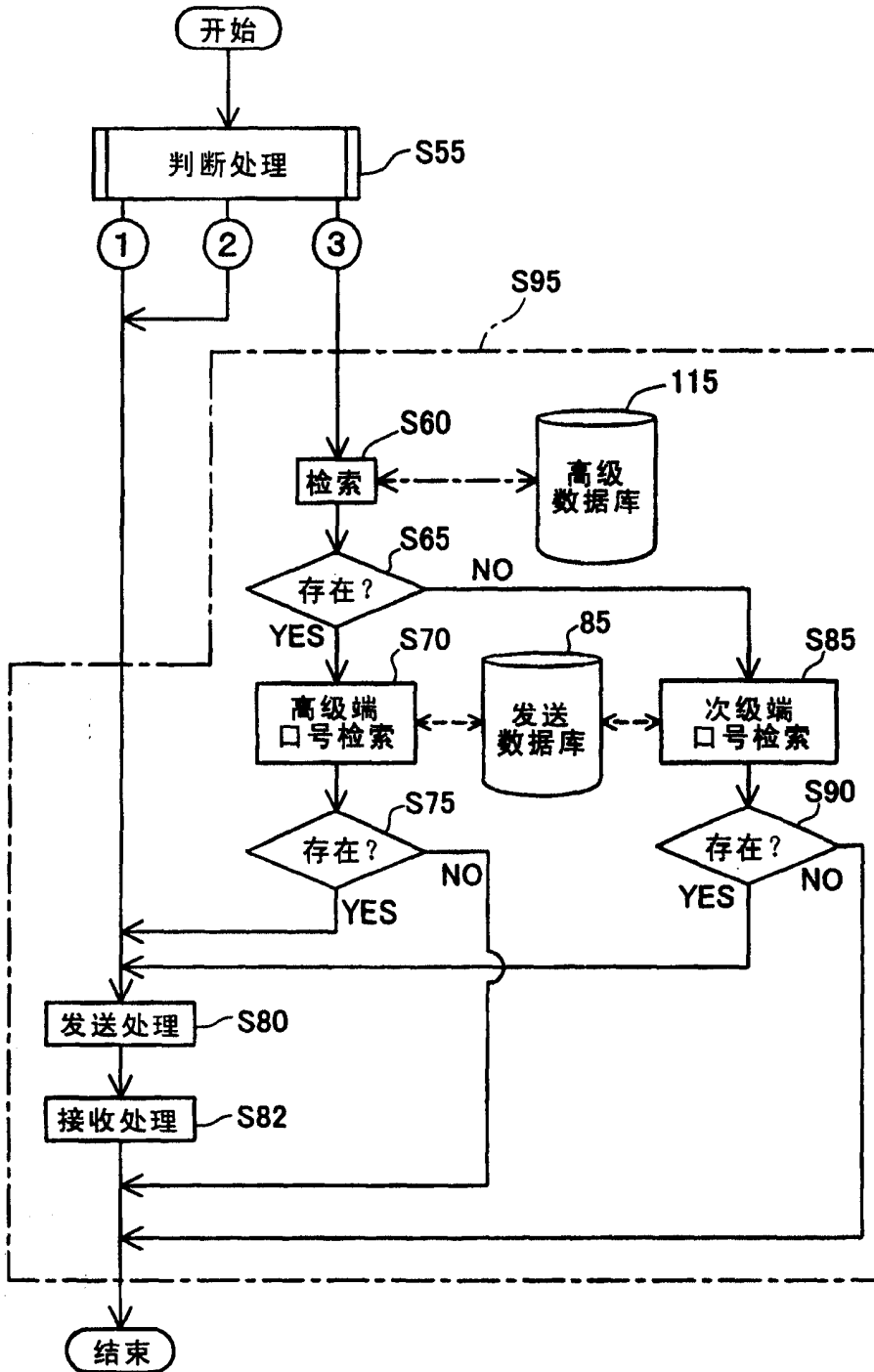


图8

高级协议	高级端口号	高级WAN协议	高级WAN端口号	次级协议	次级端口号	次级WAN协议	次级WAN端口号
HTTP	80	HTTP	80	HTTP	80
SMTP	25	SMTP	25		
POP3	110	POP3	110				
...	...	FTP	21				
					

85

图9

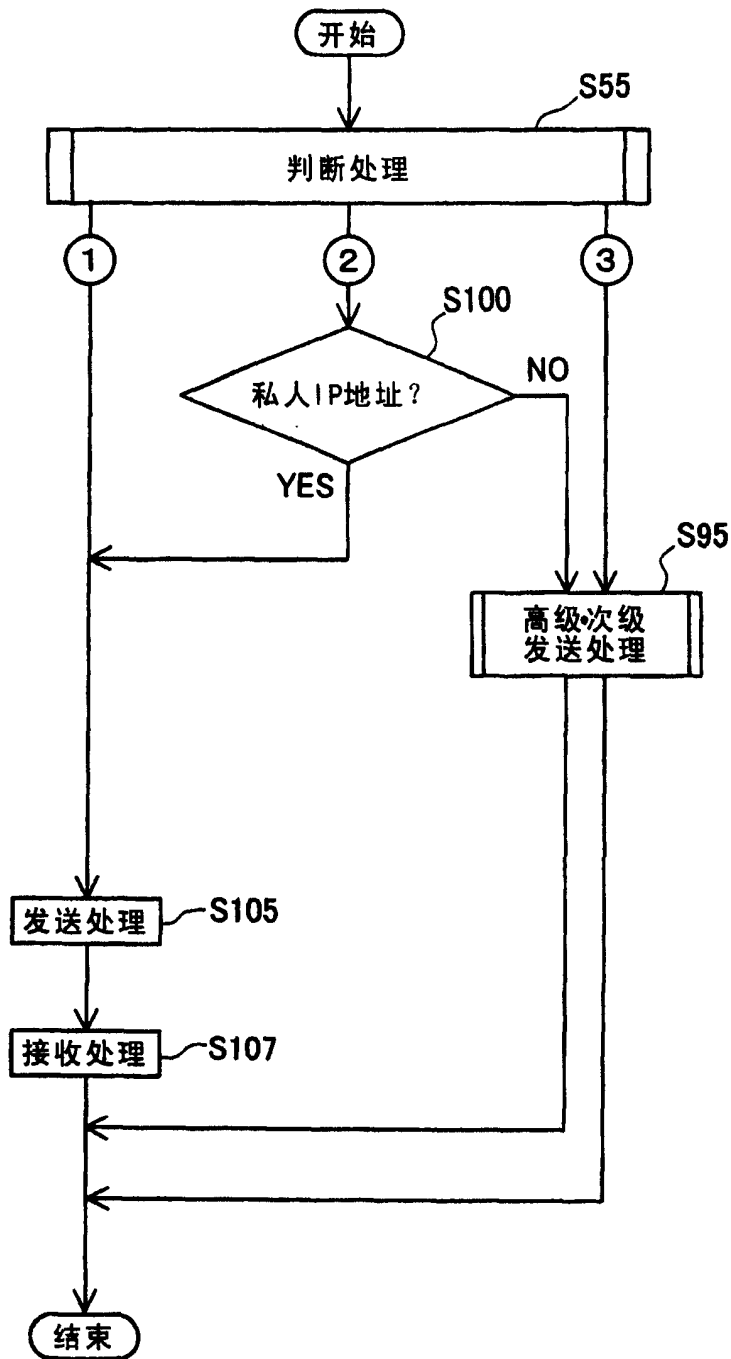


图10