



## [12] 发明专利申请公开说明书

[21] 申请号 200310120197.4

[43] 公开日 2005 年 6 月 15 日

[11] 公开号 CN 1627705A

[22] 申请日 2003.12.9

[74] 专利代理机构 北京市柳沈律师事务所

[21] 申请号 200310120197.4

代理人 吕晓章 马 莹

[71] 申请人 趋势株式会社

地址 日本东京都

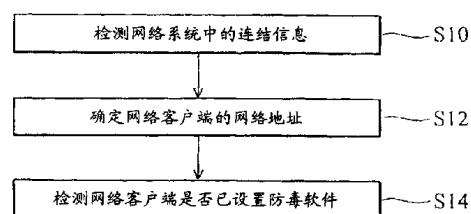
[72] 发明人 周存胜

权利要求书 2 页 说明书 8 页 附图 4 页

[54] 发明名称 强制设置防毒软件的方法、网络系统及存储媒体

**[57] 摘要**

一种强制设置防毒软件的方法，其适用于具有防毒软件检测单元、网络服务器(DHCP Server)以及网络客户端的网络系统中。首先，防毒软件检测单元检测网络系统中，由网络客户端与网络服务器所发出的连结信息。接着，防毒软件检测单元根据连结信息，确定网络客户端的网络地址。最后，防毒软件检测单元根据网络地址，检测网络客户端是否已设置防毒软件。当网络客户端未设置防毒软件时即强制网络客户端设置防毒软件。



1. 一种强制设置防毒软件的方法，其适用于一网络系统，上述网络系统  
5 具有一防毒软件检测单元、一网络服务器以及一网络客户端，其中，上述网  
络客户端是连结至上述网络系统的一计算机设备。包括下列步骤：

上述防毒软件检测单元检测上述网络系统中的多个连结信息，上述连结  
信息是由上述网络客户端与上述网络服务器所发出；

10 上述防毒软件检测单元根据上述连结信息，确定上述网络客户端的一网  
络地址；

上述防毒软件检测单元根据上述网络地址，检测上述网络客户端是否已  
设置防毒软件；以及

当上述网络客户端未设置防毒软件时，强制上述网络客户端设置防毒软  
件。

15 2. 如权利要求 1 所述的强制设置防毒软件的方法，其中，上述检测上述  
连结信息的步骤尚包括下列步骤：

上述防毒软件检测单元检测上述网络系统中的一连结显示，上述连结显  
示是由上述网络客户端所发出，用以询问上述网络服务器以连结至上述网络  
系统；以及

20 上述防毒软件检测单元检测上述网络系统中的一连结显示回复，上述连  
结显示回复是由上述网络服务器所发出，并包含上述网络地址，用以响应上  
述连结显示。

3. 如权利要求 2 所述的强制设置防毒软件的方法，其中，上述连结显示  
以及上述连结显示回复均是以广播方式发送至上述网络系统中。

25 4. 如权利要求 1 所述的强制设置防毒软件的方法，其中，上述防毒软件  
检测单元是置于连结在上述网络系统的一计算机设备中，或为连结于上述网  
络系统的一计算机设备。

30 5. 如权利要求 1 所述的强制设置防毒软件的方法，其中，上述网络系统  
是采用动态主机模块协议，以及上述网络服务器是为动态主机模块协议的网  
络服务器。

6. 一种存储媒体，用以存储一计算机程序，上述计算机程序用以加载至

一计算机系统中并且使得上述计算机系统执行如权利要求 1 至 5 中任一个所述的强制设置防毒软件的方法。

7. 一种强制设置防毒软件的网络系统，包括：

一网络系统，上述网络系统包括一网络服务器以及一网络客户端，上述  
5 网络服务器以及上述网络客户端用以发出多个连结信息至上述网络系统中，  
其中，上述网络客户端是连结至上述网络系统的一计算机设备；以及  
一防毒软件检测单元，其耦接于上述网络系统，用以检测上述连结信息，  
根据上述连结信息确定上述网络客户端的一网络地址，以及根据上述网络地  
址检测上述网络客户端是否已设置防毒软件，当上述网络客户端未设置防毒  
10 软件时，即强制上述网络客户端设置防毒软件。

8. 如权利要求 7 所述的强制设置防毒软件的网络系统，其中，上述防毒  
软件检测单元检测上述连结信息是检测上述网络系统中的一连结显示以及一  
连结显示回复，上述连结显示是由上述网络客户端以广播方式发送至上述网  
络系统中，用以询问上述网络服务器以连结至上述网络系统，上述连结显示  
15 回复是由上述网络服务器以广播方式发送至上述网络系统中，并包含上述网  
络地址，用以响应上述连结显示。

9. 如权利要求 7 所述的强制设置防毒软件的网络系统，其中，上述防毒  
软件检测单元是置于连结在上述网络系统的一计算机设备中，或为连结于上  
述网络的一计算机设备。

20 10. 如权利要求 7 所述的强制设置防毒软件的网络系统，其中，上述网络  
系统是采用动态主机模块协议，以及上述网络服务器是动态主机模块协议的  
网络服务器。

## 强制设置防毒软件的方法、网络系统及存储媒体

### 5 技术领域

发明涉及一种设置防毒软件的方法，特别涉及一种强制设置防毒软件的方法。

### 技术背景

10 由于因特网 (Internet) 技术的进步，使得网络的使用日益普及，而网络普及化导致网络使用环境日趋复杂。一企业内部网络 (Intranet) 的使用者，往往以各种方式与外部网络或计算机设备进行连结，而外部网络或计算机设备也可能与企业内部网络进行连结。例如，某企业内部网络的使用者连结外部网络以下载 (download) 数据或者某企业进行会议时，由其它公司人员自行  
15 携带计算机设备，如笔记型计算机 (Notebook) 等，连结至企业内部网络进行简报。

换言之，企业内部网络的使用者及使用状态无法严格控管，而在计算机病毒 (computer virus) 盛行的情形下，往往造成企业内部网络被计算机病毒感染，进而降低企业生产力，造成企业重大损失。因此，近来许多企业于架构企业内部网络时，已将防毒软件 (anti-virus software) 视为标准配备，也就是强制所有企业内部网络的使用者或者欲连结至企业内部网络的计算机设备，均必须先设置 (install) 防毒软件，利用防毒软件以避免企业内部网络被计算机病毒感染。

前述强制性的防毒软件设置政策可以公告方式进行，要求所有企业内部  
25 网络的使用者，必须设置防毒软件于个人的计算机设备中，此方式执行的效力并不大，况且有些使用者认为防毒软件的执行会影响其原有计算机设备的执行效能，或者防毒软件与某些驱动程序不兼容等，因此不愿配合防毒软件设置政策，无法达到强制执行的效果。另外，也可以在企业内部网络的使用者登录 (logon) 企业内部网络网域 (domain) 时，要求设置防毒软件于个人的计算机设备中，此方式虽稍具强制性，但若无配合其它检测方法，在使用者使  
30 用期间无法监测其使用情形，也无法达到预期的强制效果。

再者，企业可利用检测工具，如检测程序 (probe program) 等，定期检测连结于企业内部网络的所有计算机设备，若发现某些连结于企业内部网络的计算机设备尚未设置防毒软件时，便强制加装于其上。此方式虽具有强制性的效果，但并不适用于网络架构庞大的企业中，因为在企业内部网络的使用者人数众多的情形下，执行检测工具往往耗时费力，亦造成网络资源的浪费，而且检测工具的管理及执行机制可能又是网络管理的另一难题。

以往，防毒软件强制性设置被认为仅牵涉企业内部的执行力，也就是防毒软件无需考虑强制执行的问题，但由于近来许多企业于架构企业内部网络时，已将防毒软件视为标准配备，因此防毒软件同时具有强制性设置的执行力，亦成为目前发展的趋势。然而，现行的防毒软件并无法达到强制性设置的要求。

### 发明内容

有鉴于此，本发明的目的就在于利用企业内部网络普遍采用的动态主机模块协议 (Dynamic Host Configuration Protocol, DHCP) 进行连结时所发出的连结信息 (message)，获得欲连结至企业内部网络的计算机设备的网络地址，再根据此网络地址对欲连结至企业内部网络的计算机设备进行防毒软件检测及强制性设置。

为达成上述目的，本发明提供一种强制设置防毒软件的方法，其适用于采用动态主机模块协议的网络系统中，此网络系统具有防毒软件检测单元、网络服务器 (DHCP server) 以及网络客户端 (client)。在一实施例中，此网络服务器是动态主机模块协议的网络服务器 (DHCP server)，此网络客户端是欲连结至此网络系统的计算机设备，如桌上型计算机 (desktop computer)、笔记型计算机或个人数字助理 (Personal Digital Assistant, PDA) 等。防毒软件检测单元可能是计算机程序或执行模块，置于连结于网络系统的任一计算机设备中，或者可设计为连结于网络系统的独立的计算机设备。

首先，防毒软件检测单元检测网络系统中的连结信息，连结信息是网络客户端与网络服务器所发出。连结信息是网络客户端欲连结至网络服务器所在的网络系统时，根据动态主机模块协议，网络客户端与网络服务器所发送的信息。连结信息会以广播 (broadcast) 方式发送至网络系统中，因此防毒软件检测单元可检测到由网络客户端或网络服务器所发出的连结信息。

根据动态主机模块协议，网络客户端欲与网络系统进行连结时，会先发出一连结显示(DHCP Discover)，用以询问网络系统中的网络服务器是否可连结至该网络系统。而网络服务器在接收到连结显示后，便发出一连结显示回复(DHCP Offer)并赋予一网络地址(IP address)至网络系统中。网络客户端由网络系统接收连结显示回复及网络地址后，便发出一连结要求(DHCP Request)，要求以所接收的网络地址进行连结。最后，网络服务器接受网络客户端的连结要求并发出一连结要求确认(DHCP Acknowledgment)，确认网络客户端可进行连结。

因此，防毒软件检测单元检测网络系统中的连结信息可细分为下列步骤。  
10 防毒软件检测单元检测网络系统中的连结显示，连结显示是由网络客户端所发出，用以询问网络服务器以连结至网络系统。防毒软件检测单元再检测网络系统中的连结显示回复，连结显示回复是由网络服务器所发出，并包含网络地址，用以响应连结显示。

接着，防毒软件检测单元根据连结信息，即连结显示及连结显示回复，  
15 确定网络客户端的网络地址。然后，防毒软件检测单元根据网络地址，检测网络客户端是否已设置防毒软件。其后，当网络客户端未设置防毒软件时，可强制网络客户端设置防毒软件。

由上可知，本发明所提出的方法，防毒软件检测单元可以外挂(plug in)  
一计算机设备于网络系统来达成，或者以一计算机程序或执行模块放置于连  
20 结于网络系统的计算机设备中来达成，无需增加网络系统的负担，亦无需在所有连结于网络系统的计算机设备中安装特定检测程序。应用于网络架构庞大、使用者连结频繁或者跨国企业网络中，尤其可见其特出的效果。

此外，本发明提出一种存储媒体，用以存储一计算机程序，上述计算机程序用以加载至一计算机系统中并且使得上述计算机系统执行如前所述的方法步骤。  
25

再者，本发明提出一种强制建置防毒软件的装置，其适用于具有网络服务器以及网络客户端的网络系统，包括连结信息检测模块、网络地址确定模块以及防毒软件检测模块。在一实施例中，网络系统是采用动态主机模块协议，网络服务器(DHCP Server)是动态主机模块协议的网络服务器，网络客户端是连结至网络系统的计算机设备，如个人计算机(personal computer)、笔记型计算机、个人数字助理或其它可连结网络系统的计算机设备。而强制建  
30

置防毒软件的装置可置于连结在网络系统的计算机设备中，或者可以是一独立连结于网络系统的计算机设备。

连结信息检测模块用以检测网络系统中的连结信息，连结信息是由网络客户端与网络服务器所发出。连结信息检测模块包括连结显示检测模块、连结显示回复检测模块。连结显示检测模块用以检测网络系统中的连结显示，连结显示是由网络客户端所发出，用以询问网络服务器以连结至网络系统。连结显示回复检测模块用以检测网络系统中的连结显示回复，连结显示回复是由网络服务器发出，并包含网络地址，用以响应连结显示。网络地址确定模块用以根据连结信息，确定网络客户端的网络地址。防毒软件检测模块用以根据网络地址，检测网络客户端是否已建置防毒软件，当网络客户端未建置防毒软件时，可强制网络客户端建置防毒软件。

又再者，本发明提出一种强制建置防毒软件的网络系统，包括网络系统以及防毒软件检测单元。

网络系统是采用动态主机模块协议，包括网络服务器以及网络客户端，网络服务器以及网络客户端用以发出连结信息至网络系统中。网络服务器是为动态主机模块协议的网络服务器。网络客户端是为连结至网络系统的计算机设备。防毒软件检测单元是置于连结在网络系统的计算机设备中，或者为一连结于网络的独立的计算机设备。

防毒软件检测单元用以检测连结信息，根据上述连结信息确定网络客户端的网络地址，以及根据网络地址检测网络客户端是否已建置防毒软件，当网络客户端未建置防毒软件时，可强制网络客户端建置防毒软件。

根据动态主机模块协议，网络客户端与网络服务器在进行连结时会发出连结显示、连结显示回复、连结要求以及连结要求确认。连结显示是由网络客户端所发出用以询问网络服务器以连结至网络系统。连结显示回复是由网络服务器发出，并包含网络地址，用以响应连结显示。连结要求是由网络客户端所发出用以响应连结显示回复。连结要求确认是由网络服务器所发出用以响应连结要求。防毒软件检测单元检测连结信息只需要检测网络系统中的连结显示以及连结显示回复。连结显示以及连结显示回复是以广播方式发送至网络系统中，因此防毒软件检测单元可由网络上加以检测得到。

- 图 1 是显示本发明所揭示的方法的执行流程图。  
图 2 是显示本发明所揭示的方法的局部流程图。  
图 3 是显示本发明所揭示的存储媒体的示意图。  
图 4 是显示本发明所揭示的装置的功能方块图。  
5 图 5 是显示本发明所揭示的网络系统的示意图。

#### 附图符号说明

30 - 存储媒体； 32 - 强制设置防毒软件的计算机程序； 320 - 检测网络系统中连结信息的程序逻辑； 322 - 确定网络客户端网络地址的程序逻辑； 324 - 检测网络客户端是否已设置防毒软件的程序逻辑； 40 - 连结信息检测模块；  
10 400 - 连结显示检测模块； 402 - 连结显示回复检测模块； 42 - 网络地址确定模块； 44 - 防毒软件检测模块； 50 - 网络系统； 52 - 防毒软件检测单元； 54 - 网络服务器； 56 - 欲进行连结的网络客户端； 58 - 其它计算机设备。

#### 具体实施方式

15 请参照图 1，图 1 是显示本发明所揭示的方法的执行流程图。一种强制设置防毒软件的方法，其适用于采用动态主机模块协议的网络系统中，此网络系统具有防毒软件检测单元、网络服务器以及网络客户端。此网络服务器是为动态主机模块协议的网络服务器，此网络客户端是为欲连结至此网络系统的计算机设备。防毒软件检测单元可能是计算机程序或执行模块，置于连  
20 结于网络系统的任一计算机设备中，或者为连结于网络系统的独立的计算机设备。

首先，防毒软件检测单元检测网络系统中的连结信息(步骤 S10)，连结信息是由网络客户端与网络服务器所发出。连结信息是根据动态主机模块协议，网络客户端与网络服务器进行连结时的信息。连结信息会以广播方式发送至网络系统中，因此防毒软件检测单元可检测到由网络客户端或网络服务器所发出的连结信息。  
25

接着，防毒软件检测单元根据连结信息，确定网络客户端的网络地址(步骤 S12)。然后，防毒软件检测单元根据网络地址，检测网络客户端是否已设置防毒软件(步骤 S14)。其后，当网络客户端未设置防毒软件时，强制网络  
30 客户端设置防毒软件。

请参照图 2，图 2 是显示本发明所揭示的方法的局部流程图。在步骤 S10

中，防毒软件检测单元检测网络系统中的连结显示(步骤S100)，连结显示是由网络客户端所发出，用以询问网络服务器以连结至网络系统。防毒软件检测单元再检测网络系统中的连结显示回复(步骤S102)，连结显示回复是由网络服务器所发出，并包含网络地址，用以响应连结显示。

5 请参照图3，图3是显示本发明所揭示的存储媒体的示意图。如图所示，一种存储媒体30，用以存储一计算机程序32，计算机程序32用以加载至一计算机系统中并且使得上述计算机系统执行如前所述的方法步骤。计算机程序32主要包括检测网络系统中连结信息的程序逻辑320，确定网络客户端网络地址的程序逻辑322以及检测网络客户端是否已设置防毒软件的程序逻辑  
10 324。

请参照图4，图4是显示本发明所揭示的装置的功能方块图。如图所示，一种强制设置防毒软件的装置，其适用于具有网络服务器以及网络客户端的网络系统，包括连结信息检测模块40、网络地址确定模块42以及防毒软件检测模块44。

15 连结信息检测模块40用以检测网络系统中的连结信息，连结信息是由网络客户端与网络服务器所发出。连结信息检测模块40包括连结显示检测模块400及连结显示回复检测模块402。连结显示检测模块400用以检测网络系统中的连结显示，连结显示是由网络客户端所发出，用以询问网络服务器以连结至网络系统。连结显示回复检测模块402用以检测网络系统中的连结显示回复，连结显示回复是由网络服务器发出，并包含网络地址，用以响应连结显示。网络地址确定模块42用以根据连结信息，确定网络客户端的网络地址。防毒软件检测模块44用以根据网络地址，检测网络客户端是否已设置防毒软件，当网络客户端未设置防毒软件时，即强制网络客户端设置防毒软件。  
20

25 请参照图5，图5是显示本发明所揭示的网络系统的示意图。如图所示，一种强制设置防毒软件的网络系统，包括网络系统50以及防毒软件检测单元52。

30 网络系统是采用动态主机模块协议，包括网络服务器54以及欲进行连结的网络客户端56，网络服务器54以及网络客户端56用以发出连结信息至网络系统50中。网络系统50还可能包括其它计算机设备58。网络服务器54是为动态主机模块协议的网络服务器。网络客户端56是为连结至网络系统50的计算机设备。防毒软件检测单元52是置于连结于网络系统的计算机设

备中，或者可为连结于网络的独立的计算机设备。

防毒软件检测单元 52 用以检测连结信息，根据上述连结信息确定网络客户端 56 的网络地址，以及根据网络地址检测网络客户端 56 是否已设置防毒软件，当网络客户端 56 未设置防毒软件时，即强制网络客户端 56 设置防毒 5 软件。

防毒软件检测单元 52 检测连结信息检测网络系统中的连结显示及连结显示回复。连结显示及连结显示回复均是以广播方式发送至网络系统 50 中。连结显示是由网络客户端 56 所发出用以询问网络服务器 54 以连结至网络系统 50。连结显示回复是由网络服务器 54 发出，并包含网络地址，用以响应 10 连结显示。连结要求是由网络客户端 56 所发出用以响应连结显示回复。连结要求确认是由网络服务器 54 所发出用以响应连结要求。

举例而言，请再参照图 5。采用动态主机模块协议的网络系统 50 中，网络系统 50 具有防毒软件检测单元 52、动态主机模块协议的网络服务器 54、欲进行连结的网络客户端 56 以及其它网络客户端 58。在本实施例中，防毒 15 软件检测单元 52 为连结于网络系统 50 的独立的计算机设备。

当网络客户端 56 欲与网络系统 50 进行连结时，根据动态主机模块协议，网络客户端 56 会先发出一连结显示，用以询问网络系统 50 中的网络服务器 54 是否可连结至网络系统 50。而网络服务器在接收到连结显示后，便发出一连结显示回复与一网络地址至网络系统 50 中。网络客户端 56 由网络系统 50 20 接收连结显示回复及网络地址后，便发出一连结要求，要求以所接收的网络地址进行连结。最后，网络服务器 54 接受网络客户端的连结要求并发出一连结要求确认，确认网络客户端 56 可进行连结。防毒软件检测单元会检测网络系统 50 中的连结显示及连结显示回复。

接着，防毒软件检测单元 52 根据连结信息，即连结显示及连结显示回复， 25 确定网络客户端 56 的网络地址。然后，防毒软件检测单元 52 根据网络地址，检测网络客户端 56 是否已设置防毒软件。其后，当网络客户端 56 未设置防毒软件时，强制网络客户端 56 设置防毒软件。

综言之，本发明检测企业内部网络普遍采用的动态主机模块协议进行连结时所发出的连结信息，对欲连结至企业内部网络的计算机设备进行防毒软件检测及强制性设置。而此防毒软件检测单元可设置于网络系统的任一计算机设备中或者以一独立的计算机设备实现，无需增加网络系统额外的负担， 30

---

达到本发明所欲达到的目的。特别地，本发明应用于网络架构庞大，使用者众多的企业网络系统中，在节省网络资源上，具有特出的成效。

虽然本发明已以较佳实施例揭露如上，然其并非用以限定本发明，任何熟习此技艺者，在不脱离本发明的精神和范围内，当可作些许的更动与润饰，

5 因此本发明的保护范围当视后附的申请专利范围所界定者为准。

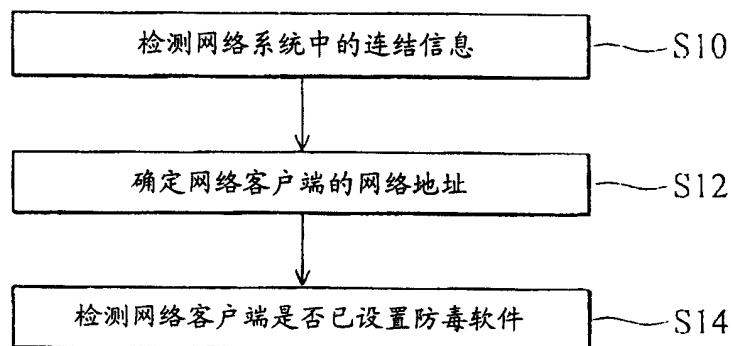


图 1

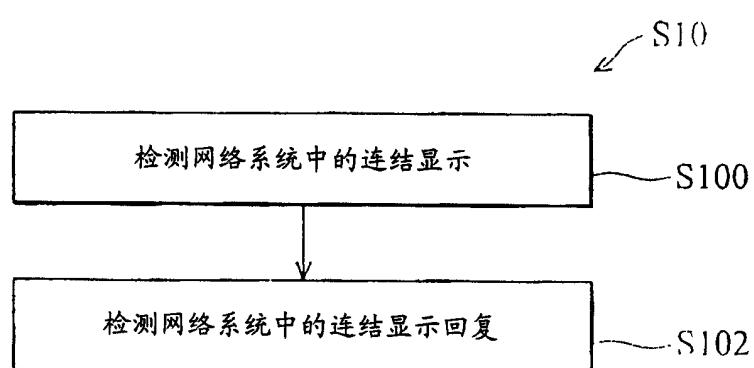


图 2

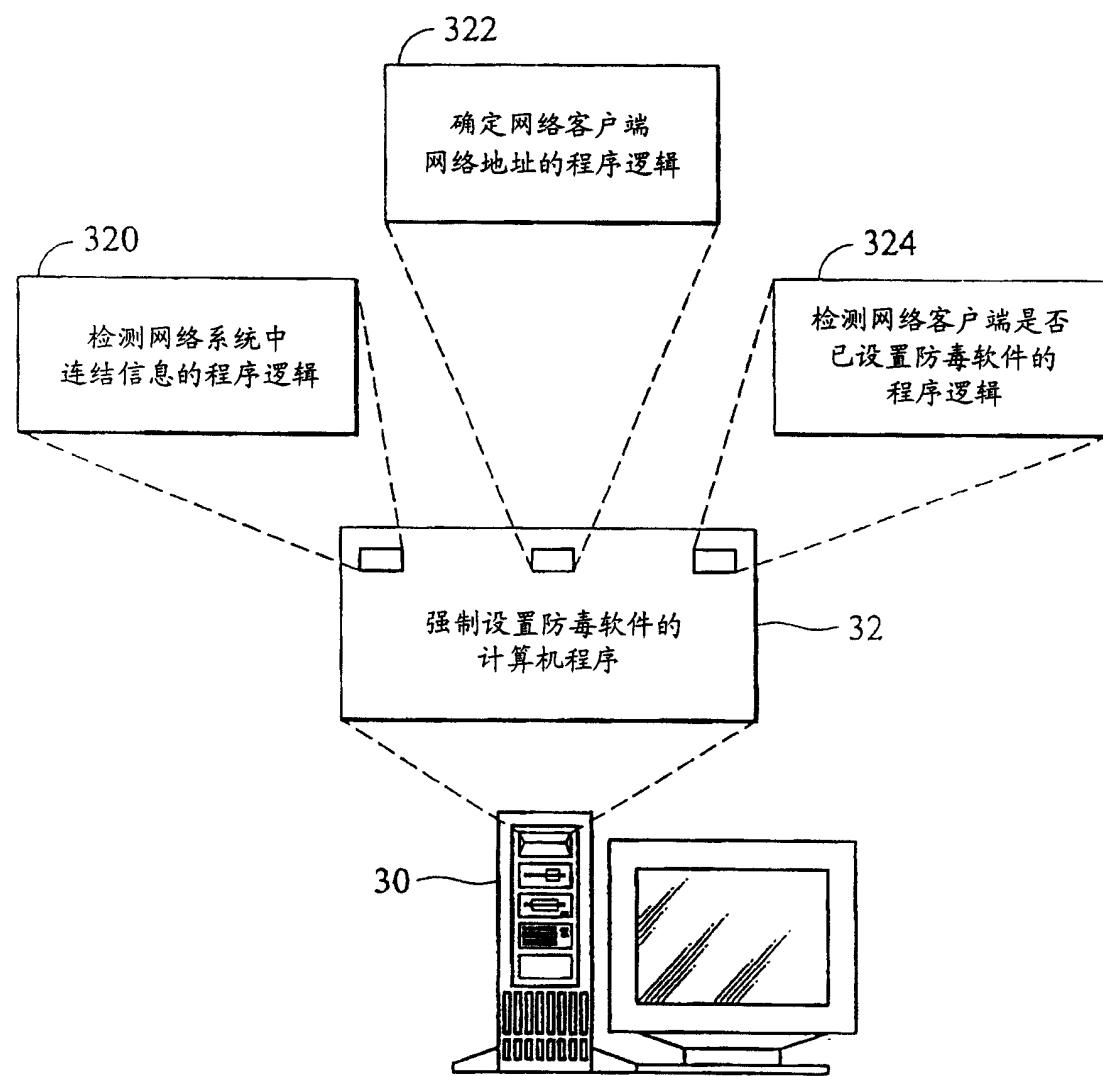


图 3

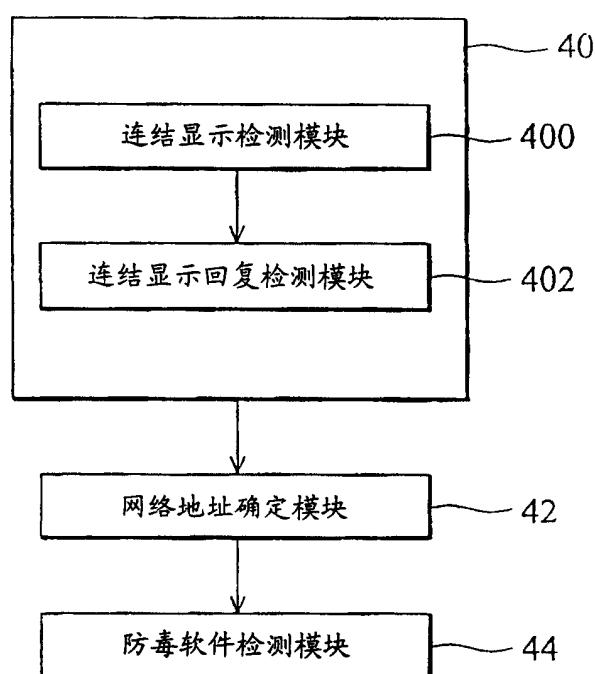


图 4

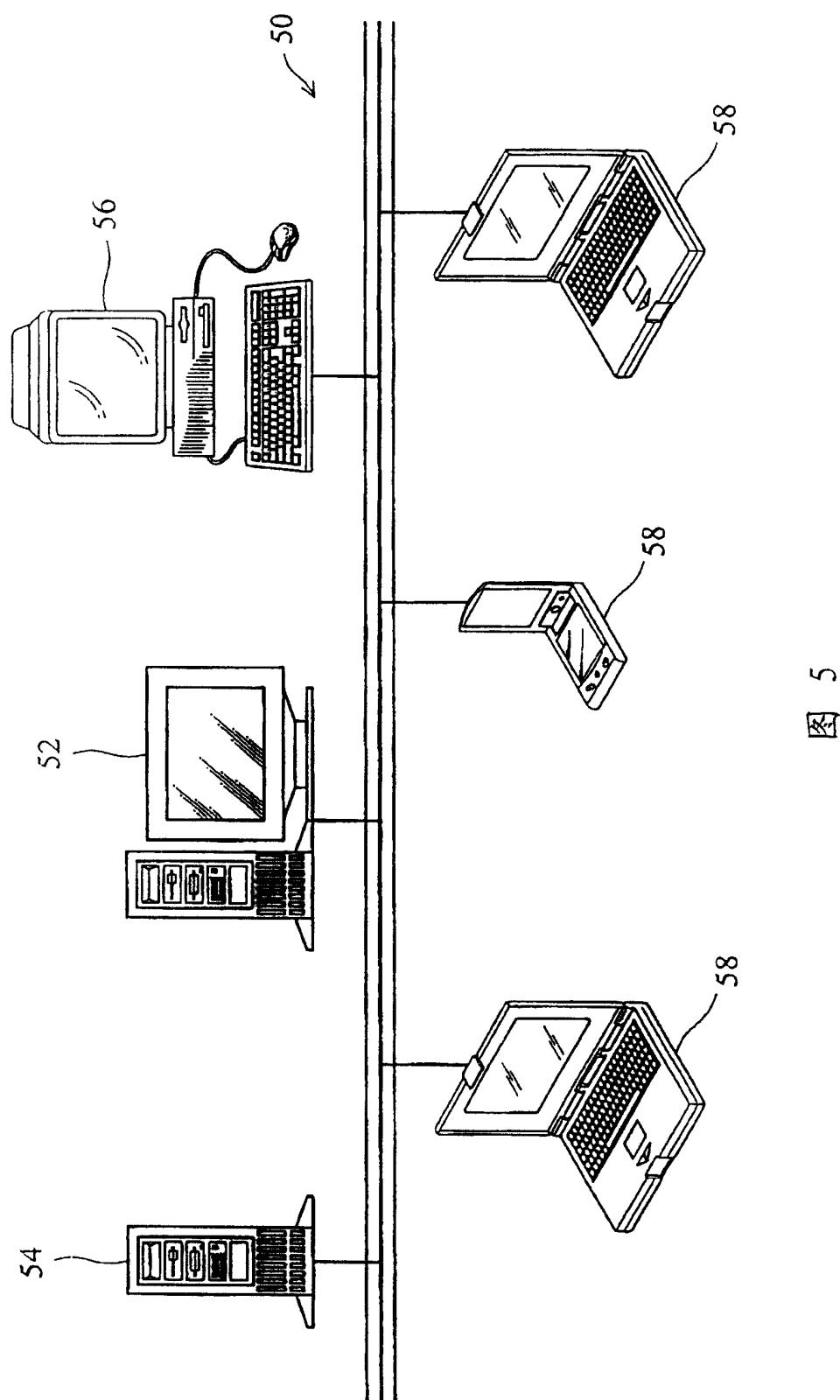


图 5