



(12) 发明专利申请

(10) 申请公布号 CN 103281286 A

(43) 申请公布日 2013. 09. 04

(21) 申请号 201210385522. 9

(22) 申请日 2012. 10. 11

(30) 优先权数据

2011-227926 2011. 10. 17 JP

(71) 申请人 佳能株式会社

地址 日本东京都大田区下丸子 3-30-2

(72) 发明人 丹治雅道

(74) 专利代理机构 北京怡丰知识产权代理有限公司

11293

代理人 迟军 李艳丽

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 29/12 (2006. 01)

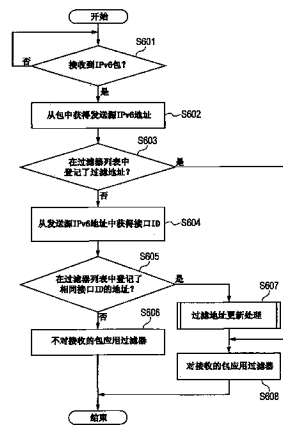
权利要求书2页 说明书10页 附图9页

(54) 发明名称

经网络与外部设备通信的信息处理装置及其信息处理方法

(57) 摘要

本发明提供经网络与外部设备通信的信息处理装置及其信息处理方法。本发明的目的是更加合适地过滤来自所述外部设备的包。该目的通过以下步骤来实现：从所述包中获得所述外部设备的地址信息；判断所述外部设备的所述地址信息是否已被登记为过滤信息；在判断出所述地址信息没被登记的情况下，从所述外部设备的所述地址信息中提取所述外部设备的设备识别信息；判断具有与所提取的设备识别信息相同的设备识别信息的地址信息是否已被登记为所述过滤信息；以及在判断出具有所述相同的设备识别信息的地址信息已被登记时，将所述外部设备的地址信息登记为所述过滤信息。



1. 一种经由网络与外部设备通信的信息处理装置,该信息处理装置包括:

登记单元,其被构造为将 IP 地址登记为过滤信息;

接收单元,其被构造为从所述外部设备接收包;

获得单元,其被构造为从所接收到的包中获得发送源 IP 地址;

提取单元,其被构造为判断由所述获得单元获得的所述发送源 IP 地址是否已被登记为所述过滤信息,并在判断出所述发送源 IP 地址没被登记为所述过滤信息的情况下,从所述发送源 IP 地址中提取接口 ID;以及

添加单元,其被构造为判断具有与由所述提取单元提取的接口 ID 相同的接口 ID 的 IP 地址是否已被登记为所述过滤信息,并在判断出所述具有所述相同的接口 ID 的 IP 地址已被登记的情况下,将所述发送源 IP 地址添加作为所述过滤信息。

2. 根据权利要求 1 所述的信息处理装置,其中,

所述信息处理装置可通信地连接到管理被分配给所述外部设备的 IP 地址的 DNS 服务器,

所述信息处理装置还包括地址信息获得单元,该地址信息获得单元被配置为通过基于所述外部设备的 IP 地址在所述 DNS 服务器处进行询问,来获得与所述外部设备的 IP 地址不同的、所述外部设备的其他 IP 地址,并且

在判断具有所述接口 ID 的 IP 地址已被登记为所述过滤信息、并且进一步判断出所述地址信息获得单元获得了所述其他 IP 地址的情况下,所述添加单元将所述其他 IP 地址添加作为所述过滤信息。

3. 根据权利要求 1 所述的信息处理装置,该信息处理装置还包括:

删除单元,其被构造为在判断出具有所述接口 ID 的 IP 地址已被登记为所述过滤信息的情况下,并且进一步在将用于确认存在的确认包发送至具有所述接口 ID 的 IP 地址、在一定时间段内等待对所述确认包的响应包、并判断出在所述一定时间段内未接收到所述响应包的情况下,从所述过滤信息中删除具有所述接口 ID 的 IP 地址。

4. 根据权利要求 1 所述的信息处理装置,其中,

在 IP 地址中还包括用于识别装置连接到的通信线路的前缀编号,并且,

所述信息处理装置还包括改变单元,该改变单元被构造为在判断出具有所述接口 ID 的 IP 地址已被登记为所述过滤信息的情况下,并且在进一步判断出具有与具有所述接口 ID 的 IP 地址的前缀编号相同的前缀编号的 IP 地址已被登记为所述过滤信息的情况下,将被判断为已被登记的 IP 地址的前缀编号改变为所述外部设备的 IP 地址的前缀编号。

5. 根据权利要求 1 所述的信息处理装置,其中,

在 IP 地址中还包括用于识别装置连接到的通信线路的前缀编号,

所述信息处理装置还包括生成单元,该生成单元被构造为在判断出与具有所述接口 ID 的 IP 地址具有相同的前缀编号的 IP 地址已被登记为所述过滤信息的情况下,生成候选地址,在该候选地址中,被判断为已被登记的 IP 地址的前缀编号已被改变为所述外部设备的 IP 地址的前缀编号,并且,

在判断出具有所述接口 ID 的 IP 地址已被登记为所述过滤信息的情况下,并且进一步在将用于确认存在的确认包发送至所述候选地址、在一定时间段内等待对所述确认包的响应包、并判断出在所述一定时间段内接收到所述响应包的情况下,所述添加单元将所述候

选地址添加作为所述过滤信息。

6. 根据权利要求 5 所述的信息处理装置,该信息处理装置还包括:

删除单元,其被构造为在将用于确认存在的确认包发送至被所述生成单元判断为已被登记的 IP 地址、在一定时间段内等待对所述确认包的响应包、并判断出在所述一定时间段内未接收到所述响应包的情况下,从所述过滤信息中删除被所述生成单元判断为已被登记的所述 IP 地址。

7. 根据权利要求 1 所述的信息处理装置,其中,所述外部设备的 IP 地址包括 IPv6 无状态地址。

8. 一种经由网络与外部设备通信的信息处理装置的信息处理方法,该信息处理方法包括以下步骤:

将 IP 地址登记为过滤信息;

从所述外部设备接收包;

从所接收到的包中获得发送源 IP 地址;

判断所获得的发送源 IP 地址是否已被登记为所述过滤信息,并在判断出所获得的发送源 IP 地址没被登记为所述过滤信息的情况下,从所述发送源 IP 地址中提取接口 ID;以及

判断具有与所提取的接口 ID 相同的接口 ID 的 IP 地址是否已被登记为所述过滤信息,并在判断出具有所述相同的接口 ID 的 IP 地址已被登记时,将所述发送源 IP 地址添加作为所述过滤信息。

经网络与外部设备通信的信息处理装置及其信息处理方法

技术领域

[0001] 本发明涉及过滤从网络接收的包的信息处理装置。

背景技术

[0002] 近年来,由于诸如 WWW(万维网)等的互联网的普及,诸如来自可疑外部设备的远程访问、攻击及包窃听等的网络安全的脆弱性引发忧虑。作为此种问题的对策,具有过滤 IP(互联网协议)地址的功能(即过滤功能)的网络设备已变得普遍。这里,在过滤功能中,已预先将外部设备的地址登记在网络设备的过滤器列表中,以使得用户能够拒绝来自任意地址的访问,或仅允许来自任意地址的访问。这样,通过切断与具有未知地址的外部设备的连接,网络设备确保了安全性。

[0003] 然而,在 IPv6(互联网协议第 6 版)中,一个设备能够保持多个地址。结果,在网络设备中,如果用户希望通过使用过滤功能来过滤 IPv6 地址,则用户需要在过滤器列表中登记作为目标的外部设备保持的全部 IPv6 地址。

[0004] 在用户将多个 IPv6 地址手动登记在过滤器列表中的情况下,用户工作负荷重。此外,当手动登记多个地址时,存在发生不完全登记及错误登记等的情况,由此存在所需地址被从过滤目标中排除的忧虑。结果,出现了如下的网络安全的脆弱性的问题,即信息处理装置被从未指定的外部设备不合希望地访问。

[0005] 在日本专利申请特开 2008-154009 号公报中提出的方法中,当用户把确定地址登记在过滤器列表中时,网络设备在 DNS(域名系统)服务器处进行询问,从而自动获得由具有所登记的确定地址的外部设备保持的全部地址。

[0006] 也就是说,在日本专利申请特开 2008-154009 号公报中,由于网络设备把从 DNS 服务器获得的地址自动登记在过滤器列表中,因此,实现了不发生不完全登记及错误登记等的过滤,而不会对用户施加工作负荷。

[0007] 这里,应当指出,IPv6 地址包括诸如值可能周期性改变的无状态地址等的地址。

[0008] 在任何情况下,无状态地址均由前缀编号及接口 ID(通常,是通过预定计算方法由网络设备自身的 MAC(媒体访问控制)地址生成的数值)组成,其中,所述前缀编号是从路由器周期性分发的,所述接口 ID 是网络上唯一的并且由网络设备自身生成。这里,无状态地址具有有效期,并且,该有效期依赖于路由器的设置内容。当有效期到期时,由路由器分发新的前缀编号,并且生成由新前缀编号以及设备自身的接口 ID 组成的新无状态地址。

发明内容

[0009] 本发明是针对经由网络与外部设备通信的信息处理装置。这里,所述信息处理装置的特征在于包括:登记单元,其被构造为将 IP(互联网协议)地址登记为过滤信息;接收单元,其被构造为从所述外部设备接收包;获得单元,其被构造为从所接收到的包中获得发送源 IP 地址;提取单元,其被构造为判断由所述获得单元获得的所述发送源 IP 地址是否已被登记为所述过滤信息,并在判断出所述发送源 IP 地址没被登记为所述过滤信息的情况

下,从所述发送源 IP 地址中提取接口 ID;以及添加单元,其被构造为判断具有与由所述提取单元提取的所述接口 ID 相同的接口 ID 的 IP 地址是否已被登记为所述过滤信息,并在判断出具有所述相同的接口 ID 的 IP 地址已被登记的情况下,将所述发送源 IP 地址添加作为所述过滤信息。

[0010] 根据本发明,能够更加合适地过滤来自外部设备的包。

[0011] 通过以下参照附图对示例性实施例的描述,本发明的其他特征将变得清楚。

附图说明

[0012] 图 1 是例示数字多功能机的硬件构成的示例的框图。

[0013] 图 2 是例示数字多功能机的处理单元的示例的框图。

[0014] 图 3 是例示系统结构的示例的图。

[0015] 图 4 是例示过滤地址的示例的图。

[0016] 图 5 是例示 IP 地址与主机名称相互关联的信息的示例的图。

[0017] 图 6 是表示过滤地址自动更新处理的示例的流程图。

[0018] 图 7 是表示过滤地址更新处理的示例的流程图。

[0019] 图 8 是表示过滤地址更新处理的示例的流程图。

[0020] 图 9 是表示过滤地址更新处理的示例的流程图。

[0021] 图 10 是表示过滤地址更新处理的示例的流程图。

具体实施方式

[0022] 在下文中,将参照附图来详细描述本发明的优选实施例。另外,应当指出,实施例并不限定本发明,并且在本发明的问题解决手段中,并非实施例中描述的全部配置及构成都总是必需的。

[0023] < 第一实施例 >

[0024] 图 1 是例示根据本发明的第一实施例的数字多功能机的硬件构成的示例的框图。

[0025] 作为信息处理装置(计算机)的示例的打印机控制器 100 控制打印机 120。

[0026] 在打印机控制器 100 中,CPU(中央处理单元)101 执行数字多功能机的软件程序,从而控制整个数字多功能机。也就是说,当 CPU 101 根据存储在 ROM(只读存储器)102 及 HDD(硬盘驱动器)108 等中的程序的过程来执行处理时,实现数字多功能机的功能以及后述流程图中的处理。另外,可以通过专用硬件,来实现数字多功能机的功能以及后述流程图中的处理的部分或全部。

[0027] ROM 102 中存储数字多功能机的引导程序及固定参数等。RAM(随机存取存储器)103 中存储当 CPU 101 控制数字多功能机时要使用的临时数据等。HDD 108 中存储诸如打印数据等的各种数据。

[0028] 定时器 109 管理在定时器处理中经过的时间等。打印机 I/F(接口)控制单元 104 控制与打印机 120 之间的数据发送及接收(数据通信)等。NVRAM(非易失性随机存取存储器)105 中存储数字多功能机的各种设置值。

[0029] 屏板控制单元 106 控制操作屏板 111。这样,在屏板控制单元 106 的控制下,在操作屏板 111 上显示各种信息并输入来自用户的各种指令。网络 I/F 控制单元 107 控制与经

由诸如 LAN(局域网)112 等的网络而连接的外部设备的数据发送及接收。

[0030] 在总线 110 上,以可通信的方式连接了 CPU 101、ROM 102、RAM103、HDD 108、定时器 109、打印机 I/F 控制单元 104、NVRAM 105、屏板控制单元 106 及网络 I/F 控制单元 107。另外,总线 110 是系统总线,经由该系统总线发送和接收来自 CPU 101 的控制信号以及各单元间的数据信号等。

[0031] 图 2 是例示数字多功能机的处理单元(模块)的构成的示例的框图。具体而言,用户 I/F 单元 201 接受用于登记执行过滤的地址(地址信息)的用户操作。通过过滤地址登记单元 202,把从用户 I/F 单元 201 输入的地址存储(登记)在过滤地址存储单元 204 中。另外,已存储在过滤地址存储单元 204 中的地址将被任意地称为过滤地址(过滤信息的一个示例)。这里,过滤地址存储单元 204 被配设于 ROM 102、HDD 108 或 NVRAM 105 上。

[0032] 此外,当地址被登记时,过滤地址登记单元 202 将登记的地址发送至地址扩展控制单元 203,以判断保持登记的地址的外部设备是否还保持其他地址。然后,从过滤地址登记单元 202 接收到地址的地址扩展控制单元 203 通过使用网络包发送/接收单元 206,从管理外部设备的管理设备等获得保持接收地址的外部设备的其他地址。此外,网络包发送/接收单元 206 控制与外部设备的数据通信。

[0033] 这里,在地址已被登记在过滤地址存储单元 204 中的情况下,每次当网络包发送/接收单元 206 从外部设备接收到包(网络包)时,网络包发送/接收单元 206 将外部设备的地址发送至网络过滤器控制单元 205。

[0034] 当地址被接收时,网络过滤器控制单元 205 通过参照过滤地址存储单元 204,来确认是否存在与接收的地址相对应的过滤地址。然后,当相应的过滤地址被找到时,网络过滤器控制单元 205 对发送了连接请求的外部设备执行预先设置的处理。

[0035] 图 3 是例示根据本实施例的系统结构的示例的图。也就是说,例示的系统被构造为包括网络设备 300、外部设备 301、外部设备 302、DNS 服务器 303 及路由器 304 等。

[0036] 网络设备 300 是包括打印机控制器 100、操作屏板 111 及打印机 120 的数字多功能机的示例。此外,网络设备 300 具有过滤功能,并被构造为能够对外部设备(301、302)执行过滤设置。

[0037] 外部设备 301 及外部设备 302 分别从不同的子网,经由路由器 304 来执行与网络设备 300 的通信。在本实施例中,假定在外部设备 301 中,保持了两个地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”作为 IPv6 地址(IPv6 无状态地址)。此外,假定在外部设备 302 中,保持了两个地址“fee0:1::204:4ff:fe40:2”及“fee0:2::204:4ff:fe40:2”作为 IPv6 地址。

[0038] 另外,外部设备 301 及外部设备 302 各自还至少保持链接本地地址作为 IPv6 地址。然而,因为在超出诸如路由器 304 等的中继装置的通信中不被使用,所以省略了链接本地地址的显示。

[0039] DNS 服务器 303 解析网络中的设备的 IP 地址及主机名称。

[0040] 另外,虽然本实施例是针对在不同于网络设备 300 的子网上存在外部设备 301、外部设备 302 及 DNS 服务器 303 的示例,但是本发明不局限于该网络结构。例如,在与网络设备 300 相同的子网上或与网络设备 300 不同的子网上,可以分别存在外部设备 301、外部设备 302 及 DNS 服务器 303。

[0041] 图 4 是例示在网络设备 300 的过滤地址存储单元 204 中登记的过滤地址（过滤地址信息 401）的示例的图。

[0042] 这里，假定在过滤地址信息 401 中，已登记了外部设备 301 中保持的地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”。此外，假定在过滤地址信息 401 中，已登记了外部设备 302 中保持的地址“fee0:1::204:4ff:fe40:2”及“fee0:2::204:4ff:fe40:2”。

[0043] 另外，上述登记处理可以由用户整体手动执行，或者通过诸如日本专利申请 2008-154009 号公报中公开的手段自动执行。在任何情况下，由于外部设备 301 及外部设备 302 中保持的全部地址均被恰当地登记，因此，网络设备 300 处于能够恰当控制来自这些外部设备的访问的状态。

[0044] 例如，当从外部设备 301 试图对网络设备 300 访问时，首先，网络包发送 / 接收单元 206 接收相关访问的包（访问包），并且从访问包中获得发送源的地址。在本实施例中，假定能够获得地址“fee0:1::203:3ff:fe30:1”作为发送源的地址。然后，网络包发送 / 接收单元 206 将发送源的地址发送至网络过滤器控制单元 205。

[0045] 随后，网络过滤器控制单元 205 通过参照过滤地址存储单元 204，来确认是否存在与接收的发送源地址相对应的过滤地址。在本实施例中，如图 4 所示，由于地址“fee0:1::203:3ff:fe30:1”已被登记作为过滤地址，因此网络过滤器控制单元 205 对相关访问包执行预先设置的处理。

[0046] 图 5 是例示其中网络设备 300、外部设备 301 及外部设备 302 等的 IP 地址及主机名称相互关联的信息（设置文件信息 501）的示例的图。

[0047] DNS 服务器 303 在每次收到从诸如网络设备 300 等的客户端发送的请求（DNS 请求）时，参照设置文件信息 501，执行名称解析等，然后向客户端返回响应。此外，通过各设备的动态更新功能 {DDNS（动态 DNS 功能）} 等，来及时更新设置文件信息 501。例如，当各设备的地址被更新时，更新设置文件信息 501。

[0048] 这里，在图 3 中所示的结构中，假定外部设备 301 的 IPv6 地址有一次被改变。也就是说，假定传统的地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”分别被改变为“1234:1::203:3ff:fe30:1”及“1234:2::203:3ff:fe30:1”。

[0049] 之所以导致上述改变，是因为在路由器 304 中，要管理的前缀编号（“fee0:1”及“fee0:2”）的有效期到期。这样，路由器 304 将新的前缀编号（“1234:1”及“1234:2”）发送至外部设备 301 所在的网络。另外，前缀编号是使得能够识别设备（外部设备 301 等）连接到的通信线路（网络等）的通信线路识别信息的示例。

[0050] 图 6 是表示当作为过滤目标的外部设备（以下将以外部设备 301 为例）的地址改变时、要在网络设备 300 中执行的过滤地址自动更新处理的示例的流程图。这里，应当指出，关于该流程图的程序以及执行程序所需的数据，已被存储在 ROM 102 及 HDD 108 等中，并且由 CPU 101 读取到 RAM 103 上并执行。

[0051] 首先，网络包发送 / 接收单元 206 判断是否从外部设备接收到包（S601）。此时，当网络包发送 / 接收单元 206 判断接收到包时，处理进入到 S602。另一方面，当判断未接收到包时，处理再次进入到 S601。换句话说，网络设备 300 等待网络包发送 / 接收单元 206 从外部设备接收网络包。在本实施例中，假定网络设备 300 从地址改变后的外部设备 301，

接收到发送源具有新 IPv6 地址“1234:1::203:3ff:fe30:1”的包。

[0052] 在 S602 中,网络包发送 / 接收单元 206 从接收的包中获得发送源的地址 (S602)。在本实施例中,获得地址“1234:1::203:3ff:fe30:1”。然后,网络包发送 / 接收单元 206 将发送源的地址,发送至网络过滤器控制单元 205。

[0053] 随后,网络过滤器控制单元 205 通过参照过滤地址存储单元 204 (即过滤器列表),来判断是否存在与接收的发送源的地址相对应的过滤地址 (S603)。此时,当网络过滤器控制单元 205 判断存在过滤地址时,处理进入到 S608。另一方面,当判断不存在过滤地址时,处理进入到 S604。

[0054] 在 S604 中,网络过滤器控制单元 205 获得发送源的地址的接口 ID (即从发送源的地址提取接口 ID)。另外,接口 ID 是使得能够识别设备 (外部设备 301 等) 的设备识别信息的示例,并对应于例如发送源的地址的定义的低位部分。

[0055] 随后,网络过滤器控制单元 205 判断在过滤地址存储单元 204 中是否存在具有获得的接口 ID 的过滤地址 (S605)。此时,当网络过滤器控制单元 205 判断存在过滤地址时,处理进入到 S607。另一方面,当判断不存在过滤地址时,处理进入到 S606。

[0056] 在 S606 中,网络过滤器控制单元 205 结束该流程图的处理,而不对从外部设备 301 接收的包 (访问包) 执行预先设置的处理 (即不应用过滤器)。

[0057] 在 S607 中,执行后述的过滤地址更新处理 (子程序)。另外,例如,在过滤地址更新处理中登记发送源的地址。

[0058] 这里,在本实施例中,在过滤地址存储单元 204 中不存在与发送源的地址“1234:1::203:3ff:fe30:1”相同的过滤地址。然而,在过滤地址存储单元 204 中,已登记了与地址“1234:1::203:3ff:fe30:1”相同的接口 ID 的地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”。因此,执行过滤地址更新处理。

[0059] 在 S608 中,网络过滤器控制单元 205 对访问包执行预先设置的处理 (即应用过滤器),然后该流程图的处理结束。

[0060] 图 7 是表示过滤地址更新处理的示例的流程图。这里,应当指出,关于该流程图的程序以及执行程序所需的数据已被存储在 ROM 102 及 HDD 108 等中,并且由 CPU 101 读取到 RAM 103 上并执行。

[0061] 首先,地址扩展控制单元 203 通过使用网络包发送 / 接收单元 206 在 DNS 服务器 303 处进行询问,从而获得保持发送源的地址的外部设备的主机名称 (S701)。在本实施例中,地址扩展控制单元 203 在 DNS 服务器 303 处询问地址“1234:1::203:3ff:fe30:1”的主机名称。然后,DNS 服务器 303 通过参照设置文件信息 501 的内容,将相应的主机名称“dev1”返回至网络设备 300。另外,应当指出,如上所述已由外部设备 301 的地址的改变,而更新了设置文件信息 501。

[0062] 随后,地址扩展控制单元 203 在 DNS 服务器 303 处询问主机名称“dev1”的 IPv6 地址,从而获得主机名称“dev1”的全部 IPv6 地址 (S702)。另外,应当指出,S701 至 S702 中的处理是如下的地址信息获得处理的示例,即基于外部设备 (外部设备 301 等) 的地址信息,在管理设备 (DNS 服务器 303 等) 处进行询问,从而获得与外部设备的上述地址信息不同的该外部设备的其他地址信息。

[0063] 在本实施例中,作为与主机名称“dev1”相对应的 IPv6 地址,获得地址

“1234:1::203:3ff:fe30:1”及“1234:2::203:3ff:fe30:1”。然后,地址扩展控制单元 203 将主机名称“dev1”的全部 IPv6 地址发送至过滤地址登记单元 202。

[0064] 随后,过滤地址登记单元 202 更新过滤地址存储单元 204 的内容 (S703)。也就是说,将地址“1234:1::203:3ff:fe30:1”及“1234:1::203:3ff:fe30:1”,登记在过滤地址存储单元 204 中。这里,从已经登记的过滤地址中,删除地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”。然后,过滤地址登记单元 202 结束该流程图的处理。

[0065] 正如所描述的,根据本实施例,即使在作为过滤目标的外部设备的无状态地址改变的情况下,该改变也能被网络设备检测到,由此能够将过滤器列表的内容更新为最新地址。

[0066] 因此,网络设备能够连续执行合适的过滤,而不会产生不能执行过滤的时间。此外,在这方面,由于用户不需要手动改变设置的内容,因此,能够大幅减轻用户的工作负荷。

[0067] < 第二实施例 >

[0068] 在本实施例中,将描述与第一实施例中不同的过滤地址更新处理。具体而言,将描述不使用 DNS 服务器 303 的过滤地址更新处理。另外,在本实施例中,与第一实施例中相同的构成及配置分别用与相同的附图标记和符号来表示,并且将适当省略其描述。

[0069] 图 8 是表示根据本实施例的过滤地址更新处理的示例的流程图。这里,应当指出,关于该流程图的程序以及执行程序所需的数据已被存储在 ROM 102 及 HDD 108 等中,并且由 CPU 101 读取到 RAM 103 上并执行。

[0070] 另外,如同第一实施例一样,在图 6 的 S607 中调用过滤地址更新处理。

[0071] 首先,网络过滤器控制单元 205 经由过滤地址登记单元 202,将发送源的地址登记至过滤地址存储单元 204 (S801)。在本实施例中,将地址“1234:1::203:3ff:fe30:1”新登记在过滤地址存储单元 204 中。然后,将与地址“1234:1::203:3ff:fe30:1”相同的接口 ID 的地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”发送至地址扩展控制单元 203。

[0072] 然后,地址扩展控制单元 203 通过使用网络包发送 / 接收单元 206,将存在确认包发送至地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1” (S802)。这里,存在确认包是如下的包,其用于利用外部设备来确认相关地址是否仍然被该地址的外部设备使用,即相关地址是否仍然存在。例如,存在确认包是针对相关地址的 ICMPv6 (IPv6 的互联网控制消息协议) 的相邻要求 (Neighbor Solicitation) 包。

[0073] 然后,地址扩展控制单元 203 在预定时间段内,等待接收响应于存在确认包而发送的存在响应包 (即在一定时间段内等待存在响应包)。随后,地址扩展控制单元 203 判断是否接收到存在响应包 (S803)。

[0074] 此时,当判断在预定时间 (即一定时间段) 内接收到存在响应包时,地址扩展控制单元 203 结束该流程图的处理,而不执行更新过滤地址存储单元 204 的处理。在这种情况下,例如,地址“1234:1::203:3ff:fe30:1”作为结果是被新添加至外部设备 301 的 IPv6 地址。

[0075] 另一方面,当判断在预定时间段 (即一定时间段) 内未接收到存在响应包时,地址扩展控制单元 203 判断相关地址已经不被使用,并且处理进入到 S804。另外,存在响应包是针对存在确认包的包,并且是例如 ICMPv6 的相邻广告 (Neighbor Advertisement) 包。

[0076] 在 S804 中,地址扩展控制单元 203 经由过滤地址登记单元 202,从过滤地址存储单元 204 中删除被判断为不存在的地址,并且该流程图的处理结束。

[0077] 正如所描述的,根据本实施例,即使在不存在 DNS 服务器的网络环境下,网络设备也能够自动检测到作为过滤目标的外部设备的无状态地址的改变。因此,能够将过滤器列表的内容更新为最新的地址。

[0078] < 第三实施例 >

[0079] 在本实施例中,在第一实施例的过滤地址更新处理中进一步判断在过滤地址存储单元 204 中是否存在可能已被改变的其他过滤地址。然后,当判断相关地址存在时,该地址也被更新。另外,在本实施例中,与第一实施例中相同的构成及配置分别用与相同的附图标记和符号来表示,并且将适当省略其描述。

[0080] 图 9 是表示根据本实施例的过滤地址更新处理的示例的流程图。这里,应当指出,关于该流程图的程序以及执行程序所需的数据已被存储在 ROM 102 及 HDD 108 等中,并且由 CPU 101 读取到 RAM 103 上和执行。

[0081] 另外,如同第一实施例一样,在图 6 的 S607 中调用过滤地址更新处理。

[0082] 首先,地址扩展控制单元 203 通过使用网络包发送 / 接收单元 206 在 DNS 服务器 303 处进行询问,从而获得保持发送源的地址的外部设备的主机名称 (S901)。在本实施例中,地址扩展控制单元 203 在 DNS 服务器 303 处询问地址“1234:1::203:3ff:fe30:1”的主机名称。然后,DNS 服务器 303 通过参照设置文件信息 501 的内容,将相应的主机名称“dev1”返回至网络设备 300。

[0083] 随后,地址扩展控制单元 203 通过使用网络包发送 / 接收单元 206,在 DNS 服务器 303 处询问主机名称“dev1”的 IPv6 地址,从而获得主机名称“dev1”的全部 IPv6 地址 (S902)。在本实施例中,作为与主机名称“dev1”相对应的 IPv6 地址,获得地址“1234:1::203:3ff:fe30:1”及“1234:2::203:3ff:fe30:1”。然后,地址扩展控制单元 203 将主机名称“dev1”的全部 IPv6 地址发送至过滤地址登记单元 202。

[0084] 随后,过滤地址登记单元 202 更新过滤地址存储单元 204 的内容 (S903)。也就是说,过滤地址登记单元 202 在登记于过滤地址存储单元 204 中的过滤地址当中,将地址“fee0:1::203:3ff:fe30:1”重写为地址“1234:1::203:3ff:fe30:1”。此外,过滤地址登记单元 202 将地址“fee0:2::203:3ff:fe30:1”重写为地址“1234:2::203:3ff:fe30:1”。

[0085] 随后,过滤地址登记单元 202 判断在过滤地址存储单元 204 中,是否存在具有与过滤地址 (即重写前的过滤地址) 相同的前缀编号的过滤地址 (S904)。此时,当判断相关过滤地址存在时,处理进入到 S905。另一方面,当判断不存在相关过滤地址时,过滤地址登记单元 202 结束该流程图的处理。

[0086] 在本实施例中,存在具有与地址“fee0:1::203:3ff:fe30:1”相同的前缀编号“fee0:1”的过滤地址“fee0:1::204:4ff:fe40:2”。此外,存在具有与地址“fee0:2::203:3ff:fe30:1”相同的前缀编号“fee0:2”的过滤地址“fee0:2::204:4ff:fe40:2”。

[0087] 这里,能够判断具有相同前缀编号的外部设备的地址已同样地被改变。

[0088] 因此,在 S905 中,当判断在过滤地址存储单元中存在具有与重写前的过滤地址相同的前缀编号的过滤地址时,过滤地址登记单元 202 用与在 S903 中更新的过滤地

址相同的前缀编号来更新相关的过滤地址。也就是说,过滤地址登记单元 202 将地址“fee0:1::204:4ff:fe40:2”重写为地址“1234:1::204:4ff:fe40:2”。此外,过滤地址登记单元 202 将地址“fee0:2::204:4ff:fe40:2”重写为地址“1234:2::204:4ff:fe40:2”。然后,过滤地址登记单元 202 结束该流程图的处理。

[0089] 正如所描述的,根据本实施例,当发送访问包的发送源的地址被更新时,搜索地址可能已被改变的其他过滤地址,并且还更新关于搜索的过滤地址的信息。

[0090] 根据上述结构,当之后从具有相关地址的外部设备接收到访问包时,能够迅速执行预先设置的过滤处理。

[0091] < 第四实施例 >

[0092] 在本实施例中,在第二实施例的过滤地址更新处理中进一步判断在过滤地址存储单元 204 中是否存在可能已被改变的其他过滤地址。然后,当判断存在相关地址时,该地址也被更新。另外,在本实施例中,与第一及第二实施例中相同的构成及配置分别用相同的附图标记和符号来表示,并且将适当省略其描述。

[0093] 图 10 是表示根据本实施例的过滤地址更新处理的示例的流程图。这里,应当指出,关于该流程图的程序以及执行程序所需的数据已被存储在 ROM 102 及 HDD 108 等中,并且由 CPU 101 读取到 RAM 103 上并执行。

[0094] 另外,如同第一实施例一样,在图 6 的 S607 中调用过滤地址更新处理。

[0095] 首先,网络过滤器控制单元 205 经由过滤地址登记单元 202,将发送源的地址登记至过滤地址存储单元 204(S1001)。在本实施例中,将地址“1234:1::203:3ff:fe30:1”新登记在过滤地址存储单元 204 中。然后,将与地址“1234:1::203:3ff:fe30:1”相同的接口 ID 的地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”,发送至地址扩展控制单元 203。

[0096] 然后,地址扩展控制单元 203 通过使用网络包发送 / 接收单元 206,将存在确认包发送至地址“fee0:1::203:3ff:fe30:1”及“fee0:2::203:3ff:fe30:1”(S1002)。例如,存在确认包是针对相关地址的 ICMPv6 的相邻要求包。然后,地址扩展控制单元 203 在预定时间段内,等待接收响应于存在确认包而发送的存在响应包。

[0097] 随后,地址扩展控制单元 203 判断是否接收到存在响应包(S1003)。这里,存在响应包是例如 ICMPv6 的相邻广告包。

[0098] 此时,当地址扩展控制单元 203 判断在预定时间段内接收到存在响应包时,处理进入到 S1005。在这种情况下,例如,地址“1234:1::203:3ff:fe30:1”作为结果是被新添加至外部设备的 IPv6 地址。另一方面,当地址扩展控制单元 203 判断在预定时间段内未接收到存在响应包时,即当判断相关地址已经不被使用时,处理进入到 S1004。

[0099] 在 S1004 中,地址扩展控制单元 203 经由过滤地址登记单元 202,从过滤地址存储单元 204 中删除被判断为不存在的地址。

[0100] 随后,过滤地址登记单元 202 判断在过滤地址存储单元 204 中,是否存在具有与过滤地址(即重写前的过滤地址)相同的前缀编号的过滤地址(S1005)。此时,当过滤地址登记单元 202 判断存在相关过滤地址时,处理进入到 S1006。另一方面,当判断不存在相关过滤地址时,过滤地址登记单元结束该流程图的处理。

[0101] 在本实施例中,存在具有与地址“fee0:1::203:3ff:fe30:1”相同的

前缀编号“fee0:1”的过滤地址“fee0:1::204:4ff:fe40:2”。此外,存在具有与地址“fee0:2::203:3ff:fe30:1”相同的前缀编号“fee0:2”的过滤地址“fee0:2::204:4ff:fe40:2”。

[0102] 这里,能够判断具有相同前缀编号的外部设备的地址已同样地被改变。

[0103] 因此,当具有相同前缀编号的过滤地址存在时,地址扩展控制单元 203 也对相关过滤地址执行存在确认。

[0104] 随后,地址扩展控制单元 203 生成被视为地址“fee0:1::204:4ff:fe40:2”及“fee0:2::204:4ff:fe40:2”的改变之后的候选地址(改变候选地址)的地址(S1006)。通过将地址的前缀编号替换为在 S1001 中登记的发送源的地址的前缀编号,来生成候选地址(候选地址信息的示例)。也就是说,在本实施例中,作为结果,生成地址“1234:1::204:4ff:fe40:2”及“1234:2::204:4ff:fe40:2”作为候选地址。

[0105] 随后,地址扩展控制单元 203 通过使用网络包发送/接收单元 206,将存在确认包发送至候选地址(S 1007)。然后,地址扩展控制单元 203 在预定时间段内,等待接收响应于存在确认包而发送的存在响应包。随后,地址扩展控制单元 203 判断是否接收到存在响应包(S1008)。此时,当地址扩展控制单元 203 判断在预定时间段内接收到存在响应包时,处理进入到 S1009。另一方面,当判断在预定时间段内未接收到存在响应包时,地址扩展控制单元结束该流程图的处理。

[0106] 在 S1009 中,网络过滤器控制单元 205 经由过滤地址登记单元 202,将候选地址登记至过滤地址存储单元 204。此外,过滤地址登记单元 202 把过滤地址存储单元 204 中登记的现有地址,发送至地址扩展控制单元 203。在本实施例中,地址“fee0:1::204:4ff:fe40:2”及“fee0:2::204:4ff:fe40:2”被发送。

[0107] 随后,地址扩展控制单元 203 通过使用网络包发送/接收单元 206,将存在确认包发送至现有地址(S1010)。然后,地址扩展控制单元 203 在预定时间段内,等待接收响应于存在确认包而发送的存在响应包。

[0108] 随后,地址扩展控制单元 203 判断是否接收到存在响应包(S1011)。此时,当判断在预定时间段内接收到存在响应包时,地址扩展控制单元 203 不执行关于更新过滤地址存储单元 204 的处理,并结束该流程图的处理,而保留登记的现有地址。另一方面,当地址扩展控制单元 203 判断在预定时间段内未接收到存在响应包时,即当判断相关地址已经不被使用时,处理进入到 S1012。

[0109] 在 S1012 中,地址扩展控制单元 203 经由过滤地址登记单元 202,从过滤地址存储单元 204 中删除现有地址。

[0110] 正如所描述的,根据本实施例,即使在不存在 DNS 服务器的网络环境下,当访问包的发送源的地址被更新时,也检测可能已被改变的其他过滤地址。此外,对该地址执行存在确认。

[0111] 根据上述结构,当之后从具有相关地址的外部设备接收到访问包时,能够迅速执行预先设置的过滤处理。

[0112] <其他实施例>

[0113] 在图 6 中,可以将对在 S601 中接收的访问包执行预先设置的处理的定时设置在执行过滤地址更新处理的定时之前。在这种情况下,能够避免如下情形,即避免由于过滤地

址更新处理花费时间,而使得访问包的发送源必须在长的时间段内等待响应。

[0114] 此外,本发明也通过执行以下处理来实现。也就是说,将用于实现上述实施例的功能的软件(程序),经由网络或者各类存储介质供给至系统或装置,然后,该系统或该装置的计算机(或者CPU或MPU)读取并执行所述程序。

[0115] 根据上述实施例的结构,能够更加合适地过滤从外部设备发送的包。

[0116] 还可以由读出并执行记录在存储设备上的程序来执行上述实施例的功能的系统或装置的计算机(或者诸如CPU或MPU等的设备),来实现本发明的各方面;并且可以利用由通过例如读出并执行记录在存储设备上的程序来执行上述实施例的功能的系统或装置的计算机来执行各步骤的方法,来实现本发明的各方面。为此,例如经由网络或从充当存储设备的各种类型的记录介质(例如,计算机可读介质)将程序提供给计算机。

[0117] 虽然参照示例性实施例对本发明进行了描述,但是应当理解,本发明不局限于所公开的示例性实施例。应当对所附权利要求的范围给予最宽的解释,以使所述范围涵盖所有的此类变型例以及等同结构和功能。

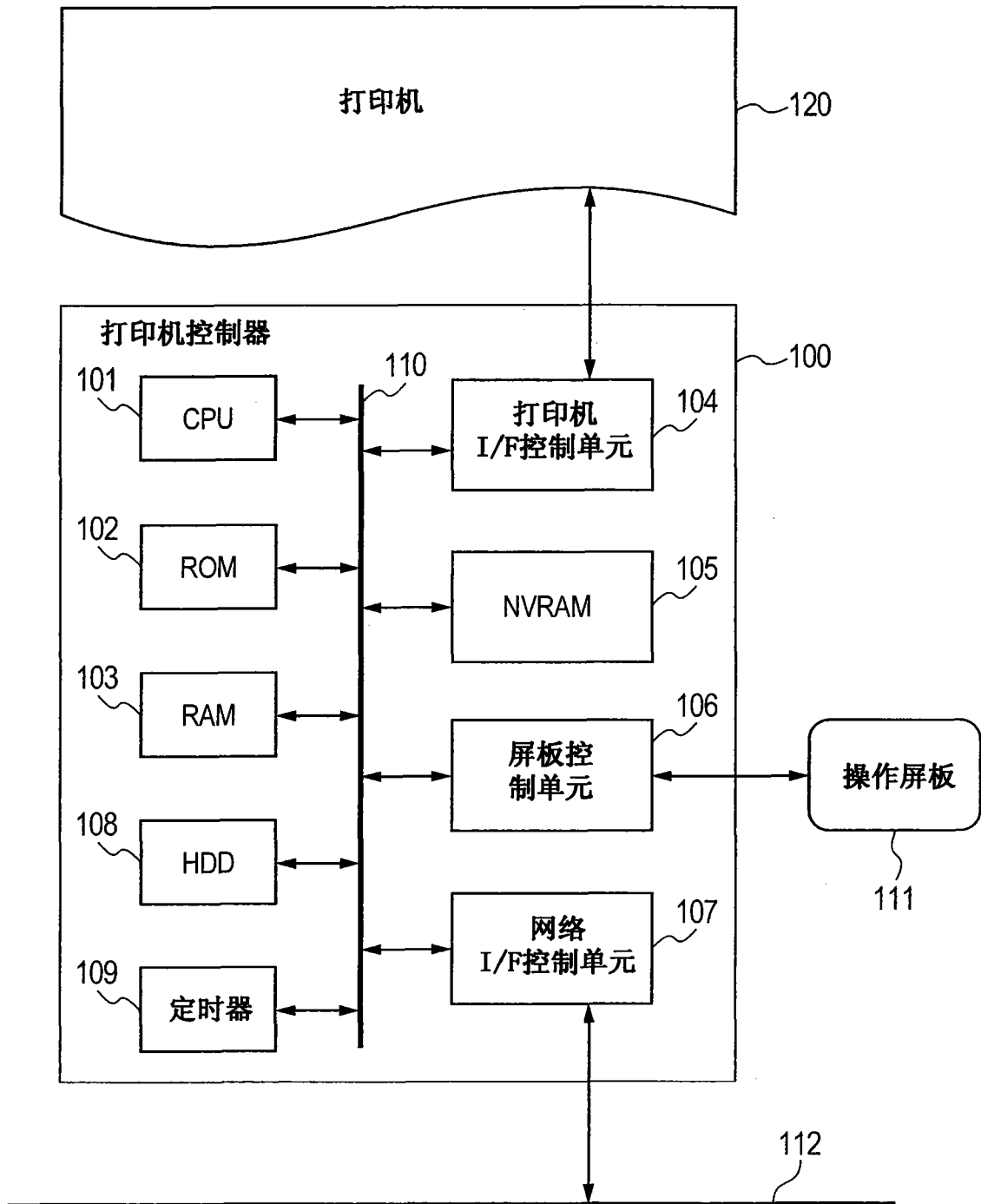


图 1

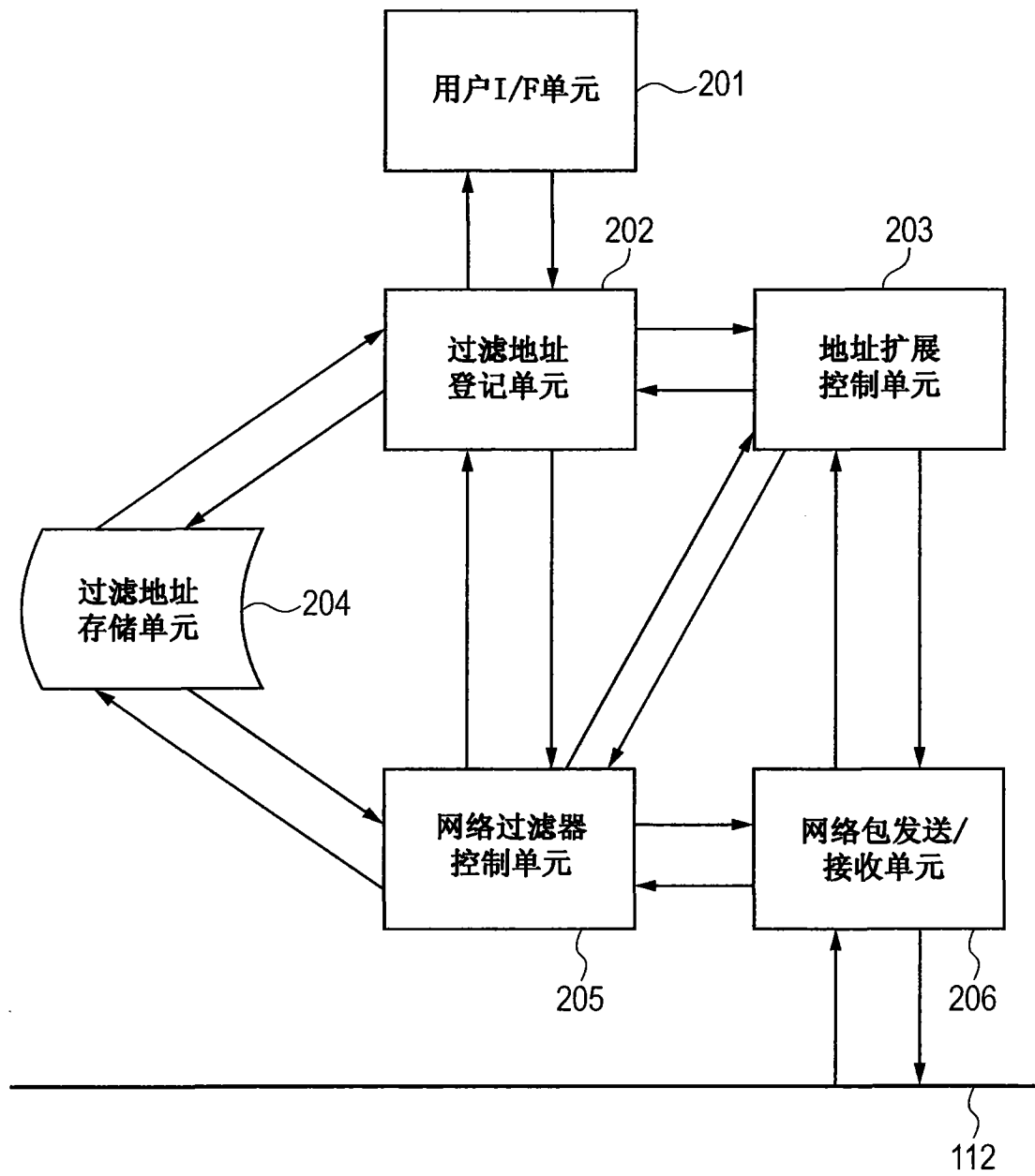


图 2

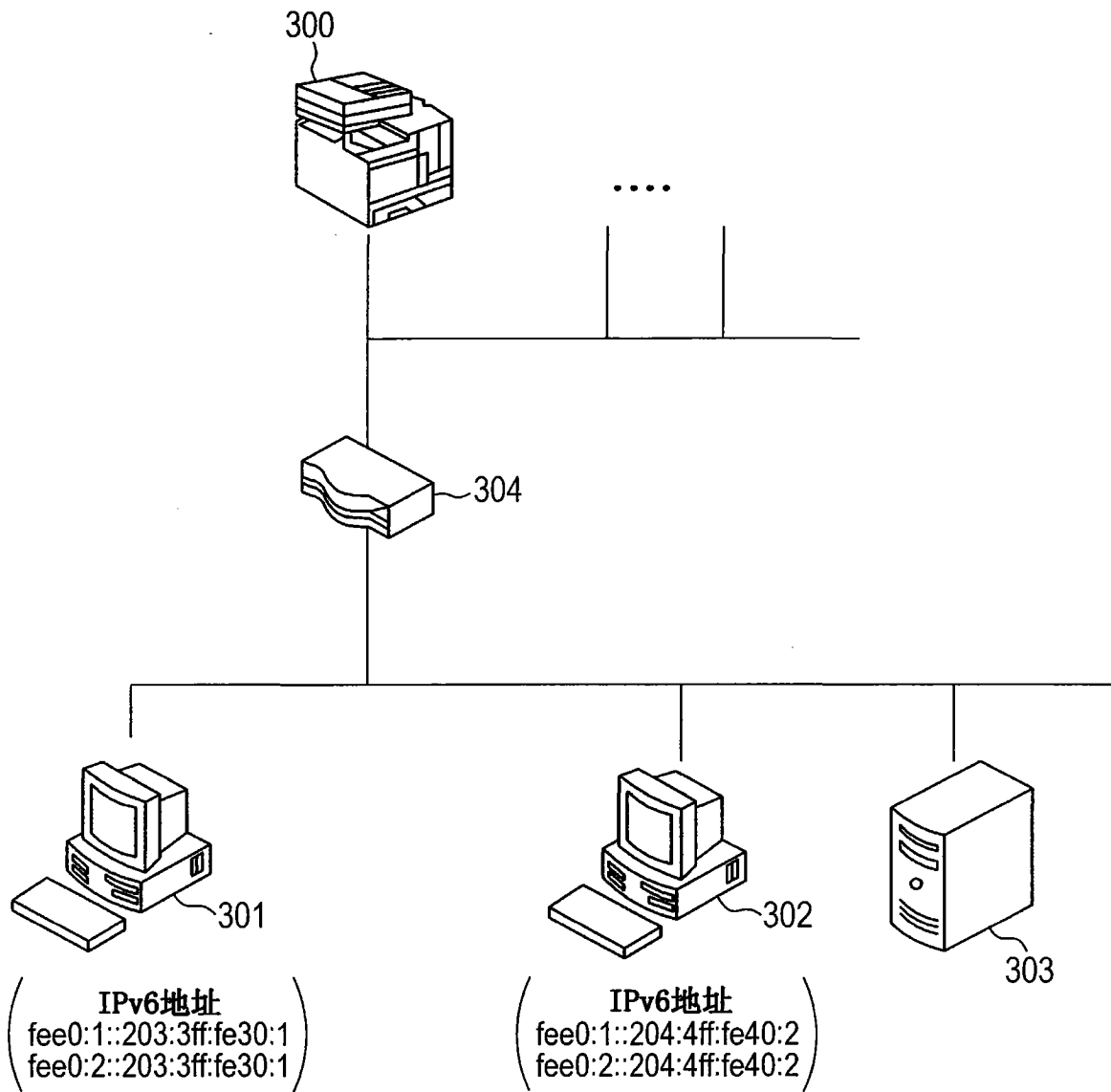


图 3

401

过滤地址
fee0:1::203:3ff:fe30:1
fee0:2::203:3ff:fe30:1
fee0:1::204:4ff:fe40:2
fee0:2::204:4ff:fe40:2

图 4

501

net	IN	A	192.168.0.120
net	IN	AAAA	ffe:2::201:1ff:fe10:1
net	IN	AAAA	ffe:2::201:1ff:fe10:1
dev1	IN	A	192.168.100.80
dev1	IN	AAAA	fee0:1::203:3ff:fe30:1
dev1	IN	AAAA	fee0:2::203:3ff:fe30:1
dev2	IN	A	192.168.100.90
dev2	IN	AAAA	fee0:1::204:4ff:fe40:2
dev2	IN	AAAA	fee0:2::204:4ff:fe40:2
dev3	IN	A	192.168.0.70
dev3	IN	AAAA	ffe:2::201:1ff:fe10:5
dev3	IN	AAAA	ffe:2::201:1ff:fe10:5

图 5

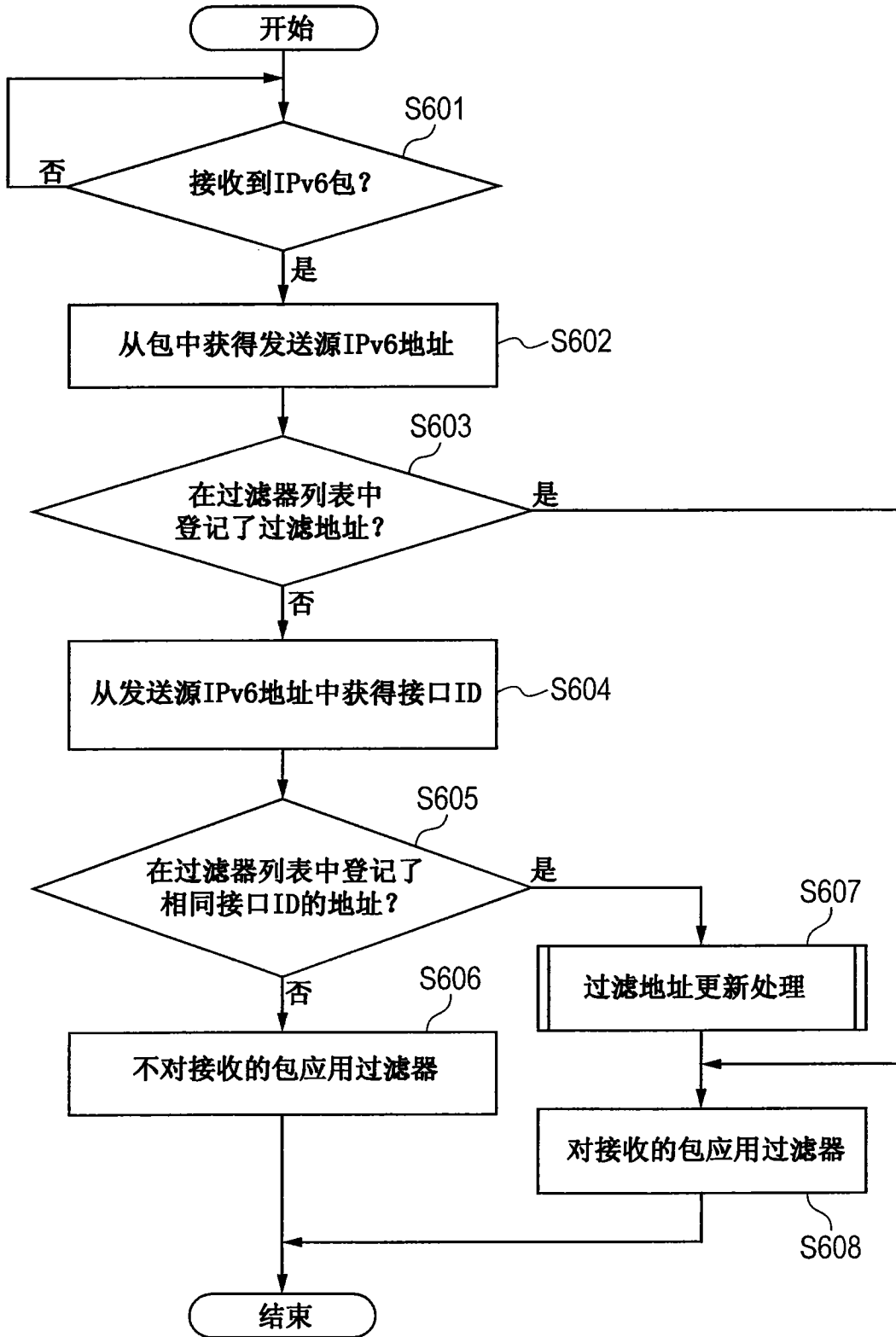


图 6

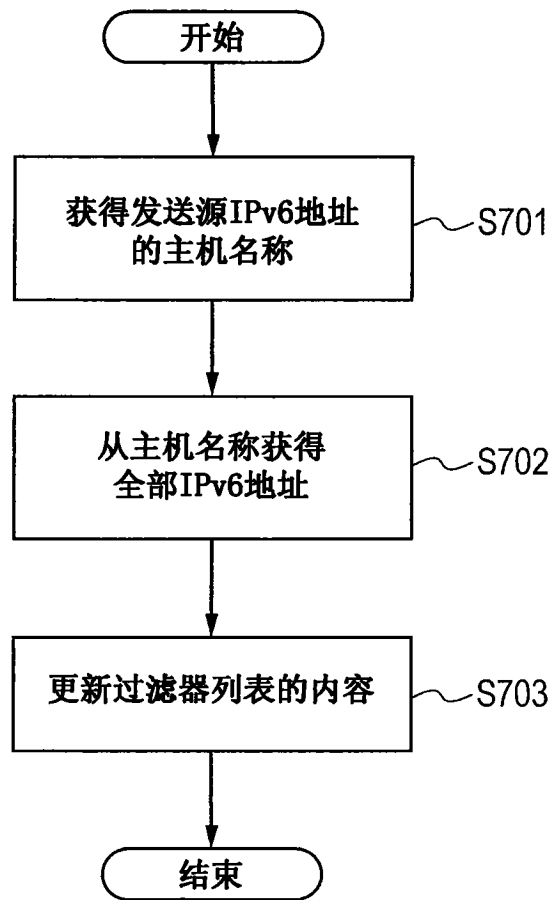


图 7

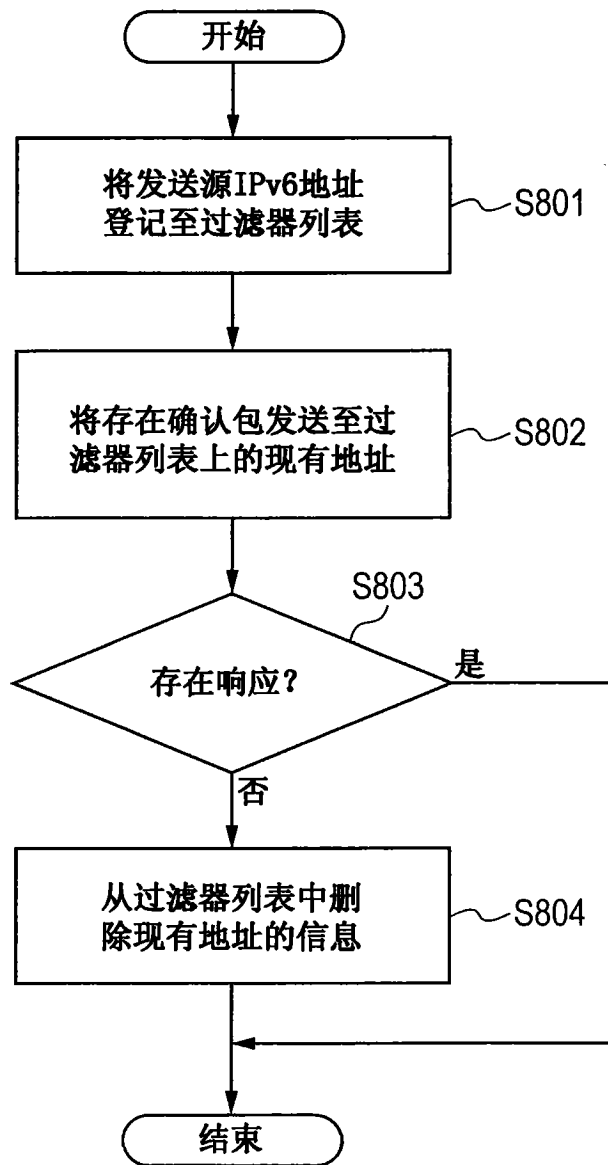


图 8

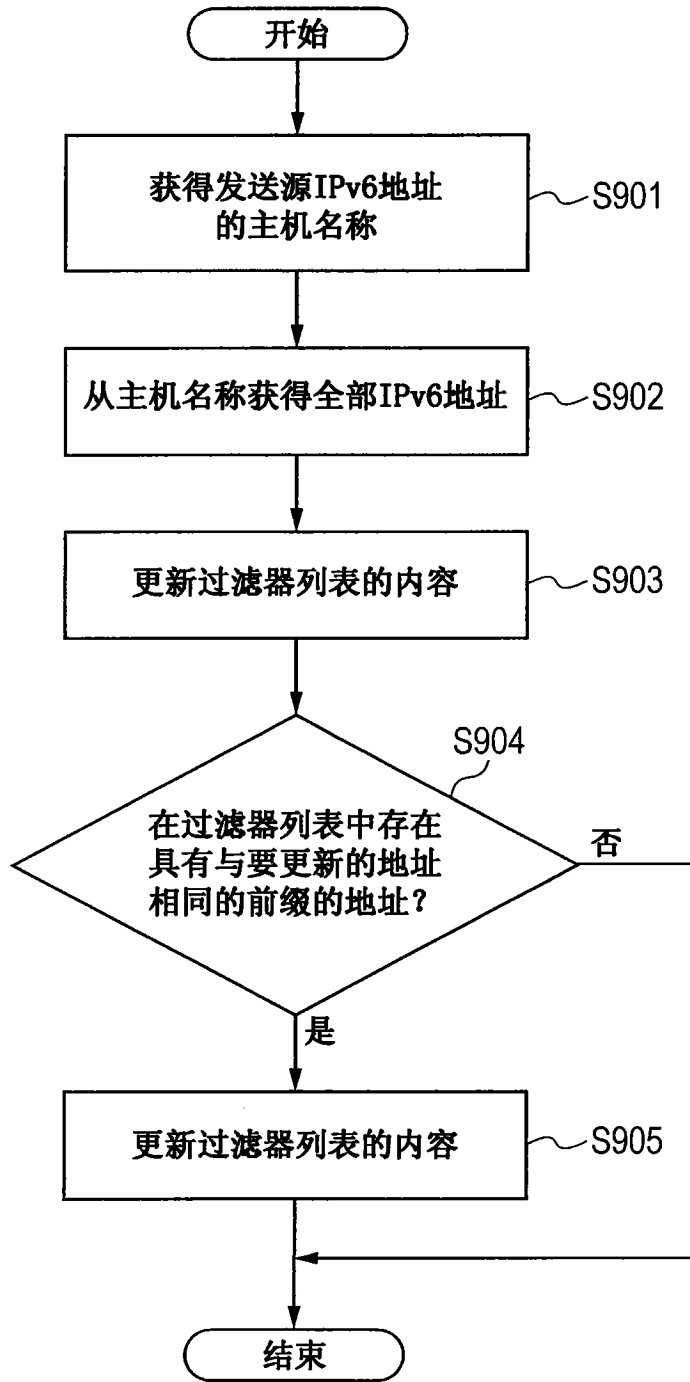


图 9

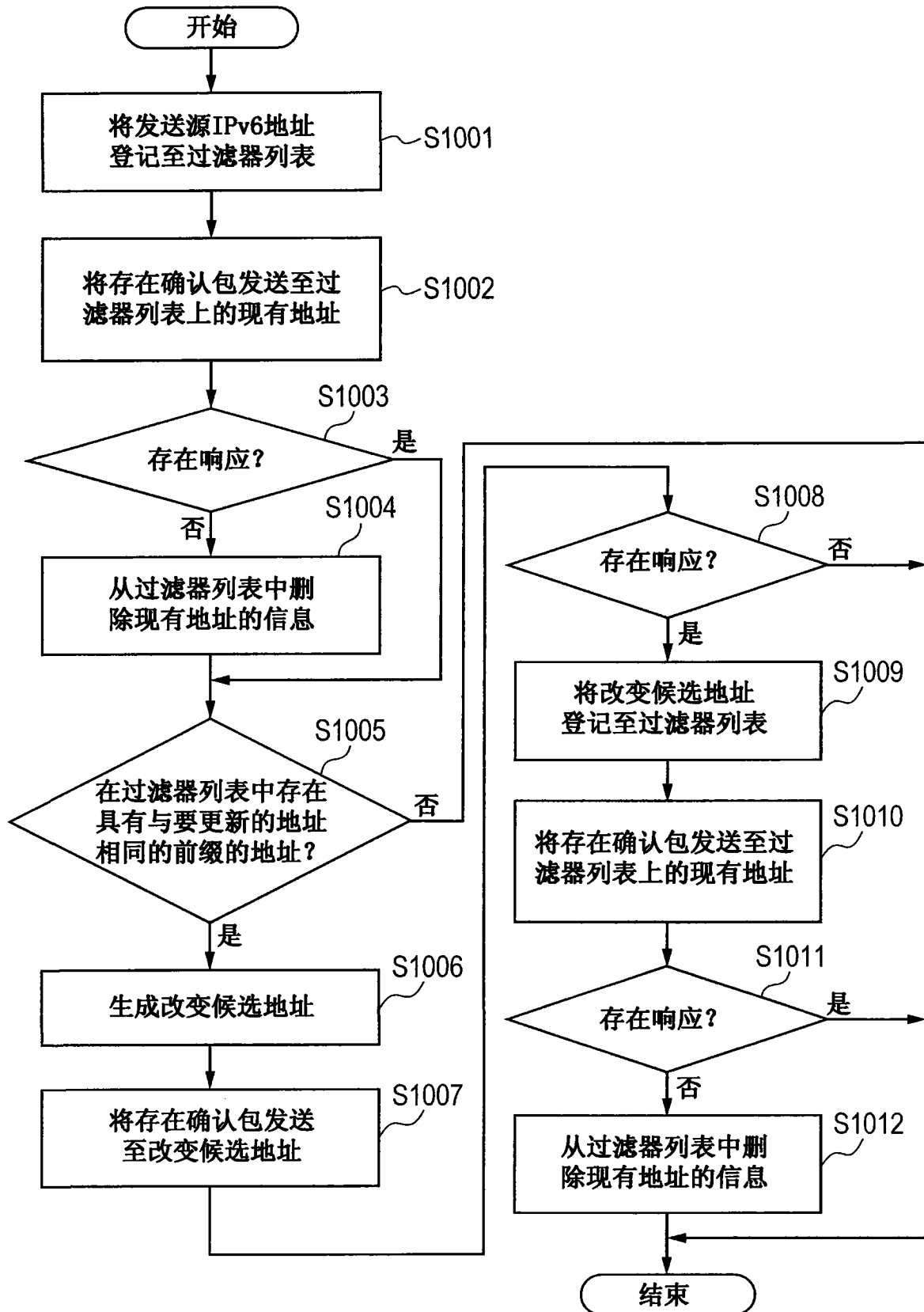


图 10