(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 1905495 B
(45)授权公告日 2011.12.21

(21)申请号 200610094656.X

(22)申请日 2006.06.20

(30)优先权数据
2005-178697 2005.06.20 JP

(73)专利权人 株式会社日立制作所
地址 日本东京
专利权人 日立信息控制系统有限公司

(72)发明人 吉川秀之 足达芳昭 外冈秀树 鸭志田弘司 武富浩二

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 曲瑞

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 12/28(2006.01)

(56)对比文件
CN 1457178 A,2003.11.19, 全文.
US 2005/0131997 A1,2005.06.16, 全文.
JP 特开2003-303118 A,2003.10.24, 全文.

审查员 白雪慧

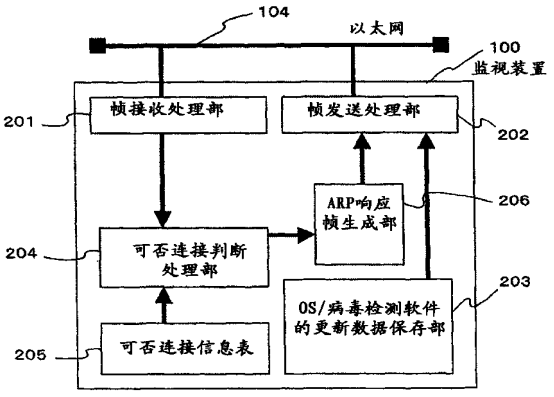
权利要求书 2 页 说明书 7 页 附图 13 页

(54)发明名称

网络监视装置、网络监视方法、网络系统和网络通信方法

(57)摘要

本发明公开了一种网络监视装置、网络监视方法、网络系统和网络通信方法，所克服的技术问题是：以前，为了实现隔离网络，必须引入具有与其对应的功能的专用交换式集线器等硬件，或者必须使网络整体为DHCP环境，并引入专用的DHCP服务器，或者必须向所有预计与LAN连接的装置安装专用的个人防火墙程序。本发明实现了一种隔离网络，在以太网的广播域中设置监视装置，该监视装置通过监视来自隔离对象装置的ARP请求并相应返回ARP响应，仅允许与特定的装置进行通信。本发明可以实现与以太网的各广播域连接的监视装置。



CN 1905495 B

1. 一种用于局域网的网络监视装置，其特征在于，具有：

当从接收部接收到的帧是从隔离对象节点发送的 ARP 请求帧时，根据物理地址比较隔离对象节点是否是预先允许的节点的装置，

当隔离对象节点不是预先允许的节点时，以下述方式进行运算处理并从发送部发送帧的装置：不包含其它节点的、在用于帧的接收和发送的网络中使用的网络地址与对应于上述网络地址的物理地址的组合，以便不妨碍上述隔离对象节点与存储与隔离有关的信息的、作为上述网络监视装置或隔离服务器的节点之间的通信。

2. 根据权利要求 1 所述的网络监视装置，其特征在于，通过将上述接收部接收的帧的地址与用于存储隔离对象节点的地址的可否信息表的存储内容相比较，来确定作为隔离对象的节点。

3. 根据权利要求 1 所述的网络监视装置，其特征在于：上述进行运算处理并从发送部发送帧的装置发送包含上述隔离服务器的网络地址与对应于上述网络地址的物理地址的组合的帧。

4. 根据权利要求 1 所述的网络监视装置，其特征在于：上述进行运算处理并从发送部发送帧的装置发送的帧包括包含自身装置的物理地址和与上述隔离对象节点相应的网络地址的组合的信息。

5. 根据权利要求 1 所述的网络监视装置，其特征在于：上述进行运算处理并从发送部发送帧的装置发送的帧包括包含自身装置的物理地址和与通信对方节点相应的网络地址的组合的信息。

6. 根据权利要求 1 所述的网络监视装置，其特征在于：上述隔离服务器被设置在其它网络中，并且上述网络监视装置经由具有 IP 分组的过滤功能的路由器与上述隔离服务器相连接。

7. 根据权利要求 1 所述的网络监视装置，其特征在于：上述网络监视装置向上述隔离对象节点发送操作系统或病毒检测软件的更新数据。

8. 一种用于局域网的网络监视方法，其特征在于，具有：

当接收到从隔离对象节点发送的 ARP 请求帧时，根据物理地址比较隔离对象节点是否是预先允许的节点的步骤，

当隔离对象节点不是预先允许的节点时，将隔离对象节点所确定的节点的、在用于帧的接收和发送的网络中使用的网络地址或对应于上述网络地址的物理地址中的至少一个作为不相应于该节点的地址来发送帧，以便不妨碍上述隔离对象节点与存储与隔离有关的信息的、作为上述网络监视装置或隔离服务器的节点之间的通信的步骤。

9. 一种用于局域网的网络系统，包括隔离对象节点、监视节点、存储与隔离有关的信息的节点以及其它节点，其中：

在从隔离对象节点发送了 ARP 请求帧后，根据物理地址比较隔离对象节点是否是预先允许的节点，并且当隔离对象节点不是预先允许的节点时，从监视节点以下述方式发送帧：不包含其它节点的、在用于帧的接收和发送的网络中使用的网络地址与对应于上述网络地址的物理地址的组合，以便不妨碍上述隔离对象节点与存储与隔离有关的信息的、作为上述监视节点或隔离服务器的节点之间的通信。

10. 一种用于局域网的网络监视方法，其中：

由接收部接收帧，当所接收的是从隔离对象节点发送的 ARP 请求帧时，根据物理地址比较隔离对象节点是否是预先允许的节点的步骤，

当隔离对象节点不是预先允许的节点时，以下述方式进行运算处理并从发送部发送帧的步骤：不包含其它节点的、在用于帧的接收和发送的网络中使用的网络地址与对应于上述网络地址的物理地址的组合，以便不妨碍上述隔离对象节点与存储与隔离有关的信息的、作为监视网络的装置或隔离服务器的节点之间的通信。

11. 一种用于局域网的网络通信方法，其中：

在从隔离对象节点发送了 ARP 请求帧后，由监视节点根据物理地址比较隔离对象节点是否是预先允许的节点，并且当隔离对象节点不是预先允许的节点时，从上述监视节点以下述方式发送帧：不包含其它节点的、在用于帧的接收和发送的网络中使用的网络地址与对应于上述网络地址的物理地址的组合，以便不妨碍上述隔离对象节点与存储与隔离有关的信息的、作为上述监视节点或隔离服务器的节点之间的通信。

网络监视装置、网络监视方法、网络系统和网络通信方法

技术领域

[0001] 本发明涉及一种网络监视装置、网络监视方法、网络系统和网络通信方法。

背景技术

[0002] 为了保护企业内部 LAN 等受保护网络而限制向网络连接的所谓网络监视装置是已知的。例如在特开 2003-303118 号公报中记载了这种技术。

[0003] 【专利文献 1】特开 2003-303118 号公报

发明内容

[0004] 这种隔离网络特别是在允许从外部带入的计算机等连接到受保护网络之前，确认该计算机的操作系统和病毒检测软件是否被更新，在未被更新的情况下，必须提供该计算机的操作系统和病毒检测软件的版本更新软件。

[0005] 为此，考虑使用认证交换机。即，在将从外部带入的计算机连接到企业内部 LAN 等受保护网络时，支持隔离网络功能的交换式集线器将连接有该计算机的端口连接到由与受保护网络虚拟断开的虚拟 LAN(VLAN) 构成的隔离网络。然后，在隔离网络上操作系统 (OS) 和病毒检测软件的更新完成后，交换式集线器变更 VLAN 的设定，以使连接有该计算机的端口属于受保护网络侧。

[0006] 然而，在受保护网络中，从终端所连接的交换式集线器到隔离服务器所连接的交换式集线器的路径上的所有交换式集线器都必须支持隔离网络功能。

[0007] 此外，考虑利用认证 DHCP 方式。即，当从外部带入的计算机利用 DHCP 获得 IP 地址时，DHCP 服务器向该计算机分配隔离网络用的 IP 地址和默认网关 IP 地址。由于隔离网络用的 IP 地址与受保护网络的 IP 地址体系不同，因而该计算机无法与受保护网络内的装置进行通信。该计算机在隔离网络上完成了 OS 和病毒检测软件的更新后，被再次分配可连接于受保护网络的 IP 地址和默认网关 IP 地址，从而可以与受保护网络内的装置进行通信。

[0008] 此外，受保护网络可以应用于利用 DHCP 的环境下，但无法应用于固定分配 IP 地址的网络环境下，并且，即使是在利用 DHCP 的环境下，对固定分配了 IP 地址的装置也是无效的。

[0009] 另外，考虑使用个人防火墙。即，预先在将要与受保护网络连接的计算机中安装具有防火墙功能的软件。当该计算机连接于受保护网络时，个人防火墙限制通信，从而只能与保存有 OS 和病毒检测软件的更新程序的隔离服务器进行通信。在完成更新后，个人防火墙的限制被解除，从而可以与受保护网络内的装置进行通信。

[0010] 然而，必须预先在可能与受保护网络连接的计算机中安装个人防火墙软件，因而对没有安装该软件的装置是无效的。

[0011] 本发明的目的是解决上述问题中的至少一个，提供一种可视网络监视装置、网络监视方法、网络系统和网络监视方法以及网络通信方法。

[0012] 为了实现上述目的，本发明由接收部接收帧，当所接收的是从隔离对象节点发送

的帧时，以下述方式进行运算处理并从发送部发送帧：不包含其它节点的网络地址与比上述网络更高的层中的相应地址的组合，以便不妨碍隔离对象节点与保存隔离信息的节点之间的通信。

[0013] 具体地说，实现了一种隔离网络，其使用与以太网的广播域连接的监视装置，根据来自隔离对象装置的 ARP 请求来发送 ARP 响应，所述隔离网络包括：帧接收处理部，用于接收以太网上的以太帧；帧发送处理部，用于发送以太帧；可否连接信息表，用于蓄积与连接于隔离网络的装置有关的信息；可否连接判断处理部，用于根据所接收的以太帧和可否连接信息表来判断 ARP 帧发送；ARP 响应帧生成部，用于按照来自可否连接判断处理部的指示发送 ARP 帧；和 OS/ 病毒检测软件的更新数据保存部，用于存储隔离所必需的软件。

[0014] 根据本发明，在允许从外部带入的计算机等节点向网络节点的通信之前，使计算机的操作系统和病毒检测软件等保持为适当的版本。

附图说明

[0015] 【图 1】实施例 1 的系统整体结构图。

[0016] 【图 2】监视装置的结构图。

[0017] 【图 3】ARP 请求帧的说明图。

[0018] 【图 4】表示实施例 1 的监视装置的操作的流程图。

[0019] 【图 5】为了不允许向隔离对象装置的通信而由监视装置发送的 ARP 响应 1。

[0020] 【图 6】为了不允许向隔离对象装置的通信而由监视装置发送的 ARP 响应 2。

[0021] 【图 7】为了不允许来自隔离对象装置的通信而由监视装置发送的 ARP 响应。

[0022] 【图 8】可否连接信息表的结构。

[0023] 【图 9】实施例 2 的系统结构图。

[0024] 【图 10】表示实施例 2 的监视装置的操作的流程图。

[0025] 【图 11】为了可以进行向隔离对象装置的通信而由监视装置向一部分装置发送的 ARP 响应。

[0026] 【图 12】实施例 3 的系统结构图。

[0027] 【图 13】路由器的过滤设定表。

[0028] 【图 14】表示实施例 3 的监视装置的操作的流程图。

[0029] 【图 15】在实施例 1 中隔离对象装置尝试与监视装置以外的装置进行通信的情况下的图。

[0030] 【图 16】在实施例 1 中隔离对象装置与监视装置进行通信的情况下的图。

[0031] 【图 17】在实施例 2 中隔离对象装置与隔离服务器进行通信的情况下的图。

[0032] 【图 18】在实施例 3 中隔离对象装置经由路由器与隔离服务器进行通信的情况下的图。

具体实施方式

[0033] 下面，利用附图来说明本发明的实施例。图 1 是本发明的隔离网络方式的实施例 1。在本结构示例中，监视装置 100、若干装置 101a ～ 101b 和隔离对象装置 103 与由以太网的一个广播域构成的网络 104 连接。在本实施例中，监视装置 100 兼用于保存 OS/ 病毒检

测软件的更新数据的隔离服务器。

[0034] 图 2 是本实施例中的监视装置 100 的结构，包括连接于网络 104 的帧接收处理部 201、帧发送处理部 202、OS/ 病毒检测软件的更新数据保存部 203、可否连接判断处理部 204、可否连接信息表 205、ARP 响应帧生成部 206。ARP（地址解析协议，Address Resolution Protocol）是 TCP/IP 协议中用于从 IP 地址求得 MAC 地址的协议。具体地说，作为 ARP 请求，向 LAN 上广播自己的以太网地址和自己的 IP 地址以及通信目标的 IP 地址这三者的组。LAN 上的各节点监视 ARP 询问的广播，因此如果自己的 IP 地址被指定，则作为 ARP 响应，在分组中加入自己的 MAC 地址并返回响应。通过该 ARP 请求和 ARP 响应，从 IP 地址获得 MAC 地址。MAC 地址是用于在以太网中执行帧的收发的物理地址，并且被分配全部不同的固有地址，以便在世界范围内不具有相同的物理地址。此外，IP 地址是在使用 TCP/IP 协议的网络等中向服务器和客户机、路由器等各个节点分配的固有地址，用于指定通信目标设备。

[0035] 图 8 示出可否连接信息表 205 的结构。该表由与连接于网络 104 的各个装置相关的 MAC 地址 810、IP 地址 811、状态 812 的组构成。对于状态 812 为允许连接的装置间的通信，监视装置 100 不做任何干涉。对于状态 812 为隔离对象的装置，监视装置 100 执行处理，以使该装置只能与监视装置 100 之间进行通信。在该表中没有表目的装置是不允许连接的装置。隔离对象装置 103 虽然被允许利用从外部带入的计算机与网络连接，但必须进行 OS/ 病毒检测软件的更新。隔离对象装置 103 为了与其它装置进行通信，以广播方式发送 ARP 请求帧。

[0036] 图 3 中示出 ARP 请求帧。当隔离对象装置 103 发送 ARP 请求帧时，在发送源 MAC 地址 301 中加入隔离对象装置 103 的 MAC 地址，在发送源 IP 地址 302 中加入隔离对象装置 103 的 IP 地址。在目的地 MAC 地址 303 中加入 0。在目的地 IP 地址中加入隔离对象装置 103 将与之进行通信的对方装置的 IP 地址。

[0037] 图 4 中示出监视装置 100 内的可否连接判断处理部 204 的处理流程。在处理 401 中，判断所接收的帧的协议类型，如果是 ARP 以外的协议，则结束处理。在处理 402 中，判断所接收的 ARP 的类型，如果是 ARP 响应，则结束处理。在处理 403 中，判断所接收的 ARP 请求的发送源 MAC 地址是否作为允许连接装置被登记在可否连接信息表 205 中。如果已经登记，则结束处理。在处理 404 中，判断是否有正在使用所接收的 ARP 请求的发送源 IP 地址的允许连接装置。如果没有，则执行处理 405，如果有，则执行处理 406。在处理 405 中，广播发送非法装置排除用 ARP 响应 a，以防止例如从装置 101a 向隔离对象装置 103 的通信。在处理 406 中，广播发送非法装置排除用 ARP 响应 b。该处理对应的情形是，隔离对象装置 103 正在使用已经分配给其它装置的 IP 地址。即，隔离对象装置 103 通过发送 ARP 请求，将发向该 IP 地址的通信的目的地改写成隔离对象装置 103，但通过发送非法装置排除用 ARP 响应 b，将发向该 IP 地址的通信修改成发向原来的装置。处理 407 向隔离对象装置 103 发送非法装置排除用 ARP 响应 c，从而隔离对象装置 103 用监视装置 100 的 MAC 地址来盖写作为通信对方发送了 ARP 请求的装置的 MAC 地址，从而使来自隔离对象装置的通信发给监视装置 100。

[0038] 图 5 中示出非法装置排除用 ARP 响应 a。在发送源 MAC 地址 501 中加入监视装置 100 的 MAC 地址，在发送源 IP 地址 502 中加入隔离对象装置的 IP 地址，在目的地 MAC 地址 503 中加入隔离对象装置的 MAC 地址，在目的地 IP 地址 504 中加入隔离对象装置的 IP 地

址。

[0039] 图 6 中示出非法装置排除用 ARP 响应 b。在发送源 MAC 地址 601 中加入通信对方的 MAC 地址，在发送源 IP 地址 602 中加入通信对方的 IP 地址，在目的地 MAC 地址 603 中加入隔离对象装置的 MAC 地址，在目的地 IP 地址 604 中加入隔离对象装置的 IP 地址。

[0040] 图 7 中示出非法装置排除用 ARP 响应 b。在发送源 MAC 地址 701 中加入监视装置 100 的 MAC 地址，在发送源 IP 地址 702 中加入通信对方的 IP 地址，在目的地 MAC 地址 703 中加入隔离对象装置的 MAC 地址，在目的地 IP 地址 704 中加入隔离对象装置的 IP 地址。

[0041] 这里，根据图 4 中所示的流程和图 15 中所示的图，来详细说明隔离对象装置 103 与监视装置 100 以外的装置、例如装置 101a 进行通信情况下的操作。这里，隔离对象装置 103 具有不与其它装置重复的 IP 地址。在开始与装置 101a 进行通信之前，隔离对象装置 103 广播发送 ARP 请求 1501。此时，装置 101a 的 IP 地址被设定成图 3 中所示的通信对方的 IP 地址 304。

[0042] 针对 ARP 请求，装置 101a 返回 ARP 响应 1502。此外，ARP 请求 1501 由于是广播发送，因而监视装置 100 也接收到。监视装置 100 根据图 4 所示的流程对该帧进行处理。即，处理 401 由于是 ARP 而进入处理 402，处理 402 由于是请求而进入处理 403，在处理 403 中，由于隔离对象装置 103 的 MAC 地址作为隔离对象被登记在可否连接信息表 205 中，因而进入处理 404。

[0043] 在处理 404 中，由于隔离对象装置 103 的 IP 地址未在其它装置中使用，因而进入处理 405。在处理 405 中，监视装置 100 广播发送图 15 的 1503 所示的非法装置排除用 ARP 响应 a。由此，由于连接于网络 104 的装置将监视装置 100 的 MAC 地址存储作为隔离对象装置 103 的 MAC 地址，因而不可进行向隔离对象装置 103 的通信。

[0044] 接着，根据图 4 的流程，监视装置 100 在处理 407 中向隔离对象装置 103 发送图 15 的 1504 所示的非法装置排除用 ARP 响应 c。由此，由于隔离对象装置 103 将监视装置 100 的 MAC 地址存储作为装置 101a 的 MAC 地址，因而不可进行向装置 101a 的通信。

[0045] 接下来，根据图 4 所示的流程和图 16 所示的图，来详细说明隔离对象装置 103 尝试与监视装置 100 进行通信的情况下的操作。到处理 405 为止的操作与上述操作没有差别。在后续的处理 407 中，监视装置 100 向隔离对象装置 103 发送图 16 的 1604 所示的非法装置排除用 ARP 响应 c，但在这种情况下，隔离对象装置 103 将监视装置 100 的 MAC 地址存储作为监视装置 100 的 MAC 地址。即，由于隔离对象装置 103 正确地存储了监视装置 100 的 IP 地址和 MAC 地址的组合，从而可以进行向监视装置 100 的通信。由此，隔离对象装置 103 可以向自身装置传送监视装置 100 所具有的 OS/ 病毒检测软件的更新数据，从而可以实施 OS/ 病毒检测软件的更新。在确认该更新结束后，将可否连接信息表 205 上的隔离对象装置 103 的状态从隔离对象改写为允许连接。这样，此后隔离对象装置 103 也可以与装置 101a ～ 101b 同等地进行通信。

[0046] 下面，对实施例 2 进行说明。

[0047] 图 9 是本发明的实施例 2 的结构。本实施例不同于实施例 1，监视装置 100 在内部没有 OS/ 病毒检测软件的更新数据保存部 203，而是设置了用于保存这些数据的隔离服务器 102。隔离服务器 102 的作用是根据来自隔离对象装置 103 的请求，将 OS/ 病毒检测软件的更新数据传送到隔离对象装置 103。

[0048] 图 10 中示出实施例 2 的情况下监视装置 100 内的可否连接判断处理部 204 的处理流程。在此仅描述与图 4 不同的部分。处理 401 ～处理 403 与图 4 相同。在处理 403 之后，在处理 1001 中，判断所接收的 ARP 请求的发送源 MAC 地址是否作为隔离对象被登记在可否连接信息表 205 中。如果未登记，则进入图 4 的处理 404。在已经登记的情况下，进入处理 1002。在处理 1002 中，判断所接收的 ARP 请求的目的地 IP 地址是否为隔离服务器 102。如果不是隔离服务器 102，则进入图 4 的处理 404。如果是隔离服务器 102，则执行处理 405。在处理 405 中，广播发送非法装置排除用 ARP 响应 a，以防止例如从装置 101a 向隔离对象装置 103 的通信。但是，由于这样也无法进行从隔离服务器 102 向隔离对象装置 103 的通信，因而在后续的处理 1003 中，向隔离服务器 102 发送隔离装置地址修复用 ARP 响应。

[0049] 图 11 中示出隔离装置地址修复用 ARP 响应。将隔离对象装置 103 的 MAC 地址设定成发送源 MAC 地址 1101，将隔离对象装置 103 的 IP 地址设定成发送源 IP 地址 1102，将修复对方的 MAC 地址设定成目的地 MAC 地址 1103，将修复对方的 IP 地址设定成目的地 IP 地址 1104，并发送给修复对方。

[0050] 这里，根据图 10 所示的流程和图 17 所示的图，来详细说明隔离对象装置 103 尝试与隔离服务器 102 进行通信的情况下的操作。在这里，隔离对象装置 103 具有不与其它装置重复的 IP 地址。

[0051] 在开始与隔离服务器 102 进行通信之前，隔离对象装置 103 广播发送 ARP 请求 1701。此时，将隔离服务器 102 的 IP 地址设定成图 3 的 ARP 请求帧的通信对方的 IP 地址 304。根据该 ARP 请求，隔离服务器 102 发送 ARP 响应 1702。此外，ARP 请求 1701 由于是广播发送，因而监视装置也接收到，并根据图 10 所示的流程来对该帧进行处理。但是，处理 401 ～处理 402 由于与实施例 1 的处理相同而省略其说明。

[0052] 在后续的处理 403 中，由于隔离对象装置 103 的 MAC 地址不是作为允许连接被登记在可否连接信息表 205 中，因而进入处理 1001。在处理 1001 中，由于隔离对象装置 103 的 MAC 地址作为隔离对象被登记在可否连接信息表 205 中，因而进入处理 1002。在处理 1002 中，由于所接收的 ARP 请求的目的地 IP 地址为隔离服务器 102，因而进入处理 405。在处理 405 中，监视装置 100 广播发送非法装置排除用 ARP 响应 a 1703。由此，由于连接于网络 104 的装置将监视装置 100 的 MAC 地址存储作为隔离对象装置 103 的 MAC 地址，因而不能进行向隔离对象装置 103 的通信。在后续的处理 1003 中，监视装置 100 向隔离服务器 102 发送隔离装置地址修复用 ARP 响应 1704。此时，将隔离服务器 102 的 MAC 地址设定成目的地 MAC 地址 1103，将隔离服务器 102 的 IP 地址设定成目的地 IP 地址 1104。由此，由于隔离服务器 102 将正确的 MAC 地址存储作为隔离对象装置 103 的 MAC 地址，因而隔离服务器 102 与隔离对象装置 103 之间可以通信。因此，隔离对象装置 103 可以向自身装置传送隔离服务器 102 所具有的 OS/ 病毒检测软件的更新数据，从而可以实施 OS/ 病毒检测软件的更新。这之后的操作与实施例 1 相同。

[0053] 下面，对实施例 3 进行说明。

[0054] 图 12 是本发明实施例 3 的结构。本实施例不同于实施例 2，隔离服务器 102 经由路由器 106 与其它网络 105 连接。路由器 106 具有根据条件对通过它的 IP 分组进行过滤的功能。过滤功能本身是现已存在的一般技术。

[0055] 图 13 中示出路由器 106 的过滤设定表的例子。过滤设定表 1301 由作为条件的发

送源 IP 地址 1302 和目的地 IP 地址 1303 以及针对满足该条件的 IP 分组的动作 1304 构成。在本实施例中，针对从网络 104 向着其它网络 105 通过路由器 106 的 IP 分组应用本过滤器。其设定值是将隔离对象装置 103 的 IP 地址设定成发送源 IP 地址。在隔离对象装置为多个的情况下，象隔离对象装置 103a ～ 103c 那样，生成多个表目。以不是隔离服务器 102 为条件，设定为目的地 IP 地址。动作设定为废弃。

[0056] 此外，在本实施例中，将路由器 106 的网络 104 侧 IP 地址设定作为隔离对象装置的默认网关。

[0057] 图 14 中示出实施例 3 的监视装置 100 内的可否连接判断处理部 204 的处理流程。在此仅描述与图 10 不同的部分。处理 401 ～处理 1001 与图 10 相同。在处理 1001 之后，在处理 1402 中，判断所接收的 ARP 请求的目的地 IP 地址是否为路由器 106。如果不是路由器 106，则进入图 4 的处理 404。如果是路由器 106，则执行处理 405。在处理 405 中，广播发送非法装置排除用 ARP 响应，以防止例如从装置 101a 向隔离对象装置 103 的通信。但是，由于这样也无法进行从路由器 106 向隔离对象装置 103 的通信，因而在后续的处理 1403 中，向路由器 106 发送隔离装置地址修复用 ARP 响应。

[0058] 这里，按照图 14 所示的流程和图 18 所示的图，来详细说明隔离对象装置 103 尝试与隔离服务器 102 进行通信的情况下的操作。这里，隔离对象装置 103 具有不与其它装置重复的 IP 地址。在开始与隔离服务器 102 进行通信之前，隔离对象装置 103 广播发送 ARP 请求 1801。此时，被设定作为隔离对象装置的默认网关的路由器 106 的 IP 地址被设定成图 3 的 ARP 请求帧的通信对方的 IP 地址 304。根据该 ARP 请求，路由器 106 发送 ARP 响应 1802。此外，ARP 请求由于是广播发送，因而监视装置 100 也接收到，并按照图 14 所示的流程对该帧进行处理。但是，由于处理 401 ～ 1001 与实施例 2 的处理相同，因而省略其说明。在后续的处理 1402 中，由于所接收的 ARP 请求的目的地 IP 地址为路由器 106，因而进入处理 405。

[0059] 在处理 405 中，监视装置 100 广播发送非法装置排除用 ARP 响应 a 1803。由此，由于连接于网络 104 的装置将监视装置 100 的 MAC 地址存储作为隔离对象装置 103 的 MAC 地址，因而不能进行向隔离对象装置 103 的通信。在后续的处理 1403 中，监视装置 100 向路由器 106 发送隔离装置地址修复用 ARP 响应 1804。此时，将路由器 106 的 MAC 地址设定成目的地 MAC 地址 1103，将路由器 106 的 IP 地址设定成目的地 IP 地址 1104。由此，由于路由器 106 将正确的 MAC 地址存储作为隔离对象装置 103 的 MAC 地址，因而可以进行路由器 106 与隔离对象装置 103 之间的通信。当从隔离对象装置 103 发向隔离服务器 102 的 IP 分组通过路由器 106 时，将其与过滤设定表 1301 进行比较。在该例子中，由于发送源 IP 地址是隔离对象装置 103、目的地 IP 地址是隔离服务器，因而 IP 分组可以通过路由器 106、进入其它网络 105、进而到达隔离服务器 102。因此，隔离对象装置 103 可以向自身装置传送隔离服务器 102 所具有的 OS/ 病毒检测软件的更新数据，从而可以实施 OS/ 病毒检测软件的更新。这之后的操作与实施例 2 相同。

[0060] 接下来，对隔离对象装置 103 与连接于其它网络 105 的隔离服务器 102 以外的装置进行通信的情况下的操作进行详细说明。在这种情况下，与上述隔离对象装置 103 和隔离服务器 102 之间的通信相同，由于网络 104 内的隔离对象装置 103 的通信对方是路由器 106，因而即使目的地是隔离服务器 102 以外的装置，监视装置 100 也允许隔离对象装置 102

与路由器 106 之间的通信。然而，在与路由器 106 的过滤表 1301 的比较中，由于目的地 IP 地址不是隔离服务器 102，因而 IP 分组被放弃。因此，不允许隔离对象装置 103 与连接于其它网络 105 的隔离服务器 102 以外的装置进行通信。

[0061] 根据本实施例，不需要支持隔离网络功能的专用交换式集线器，此外，由于可以使用一般的中继器集线器来构成隔离网络，因而没有必要改变现有网络的硬件结构。此外，由于在 DHCP 环境下和固定 IP 地址环境下都可以同样地操作，因而不必改变现有的网络环境。而且，也不需要向所有终端安装个人防火墙等专用软件，从而可以更简便地实现隔离网络。

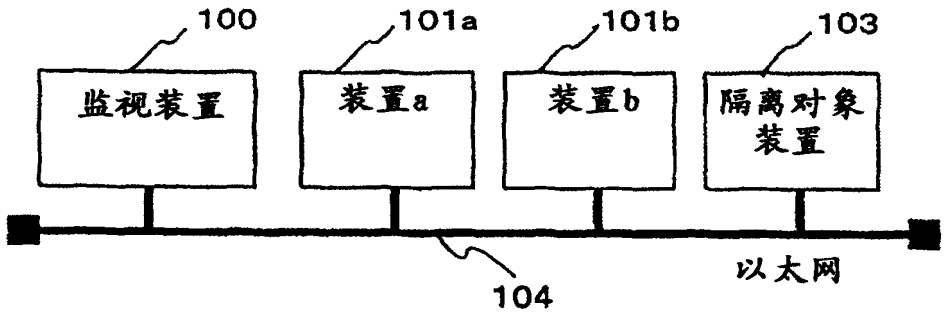

100
101a
101b
103
监视装置
装置a
装置b
隔离对象装置
以太网
104

图1

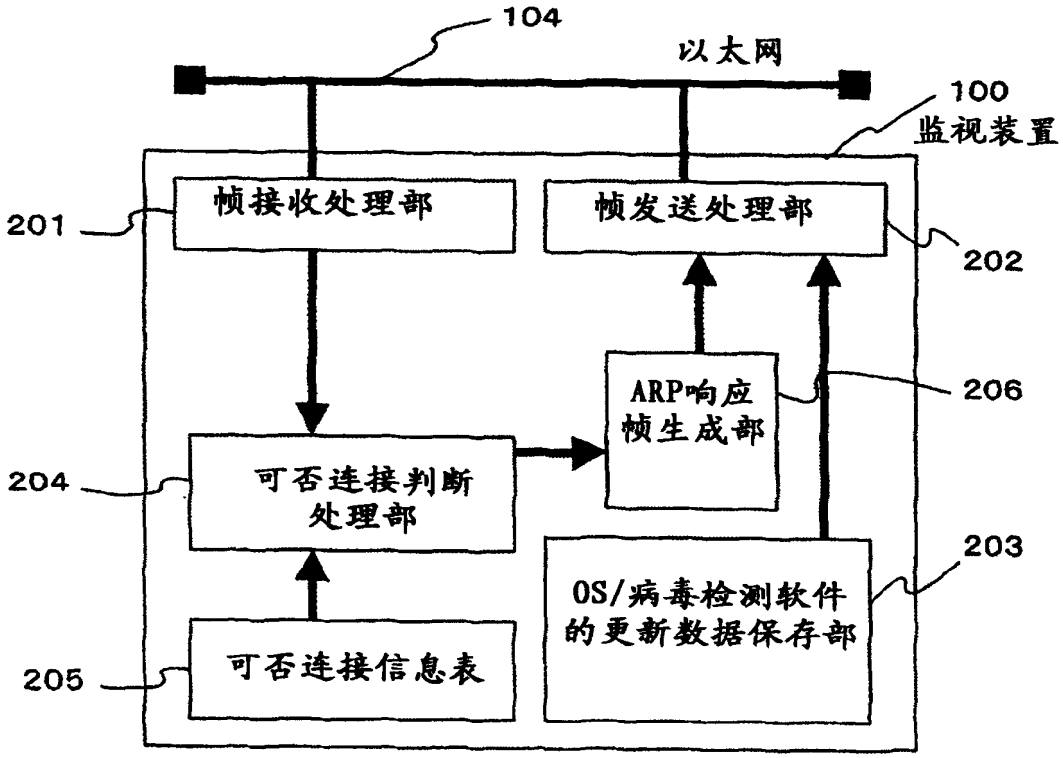

104
以太网
100
监视装置
201
帧接收处理部
帧发送处理部
202
ARP响应帧生成部
206
204
可否连接判断处理部
203
OS/病毒检测软件的更新数据保存部
205
可否连接信息表

图2

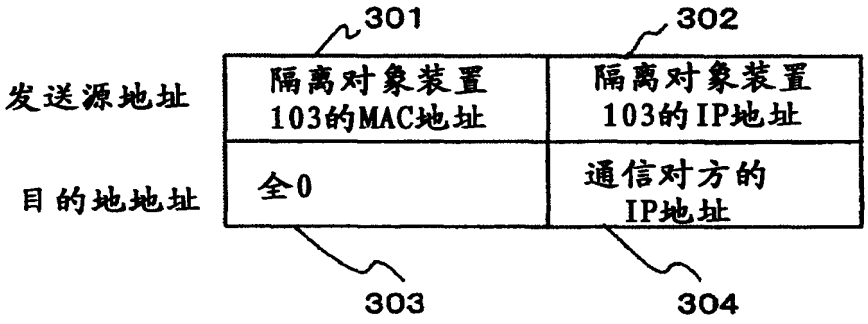

ARP请求帧
301
302
发送源地址
隔离对象装置
103的MAC地址
隔离对象装置
103的IP地址
目的地地址
全0
通信对方的
IP地址
303
304

图 3

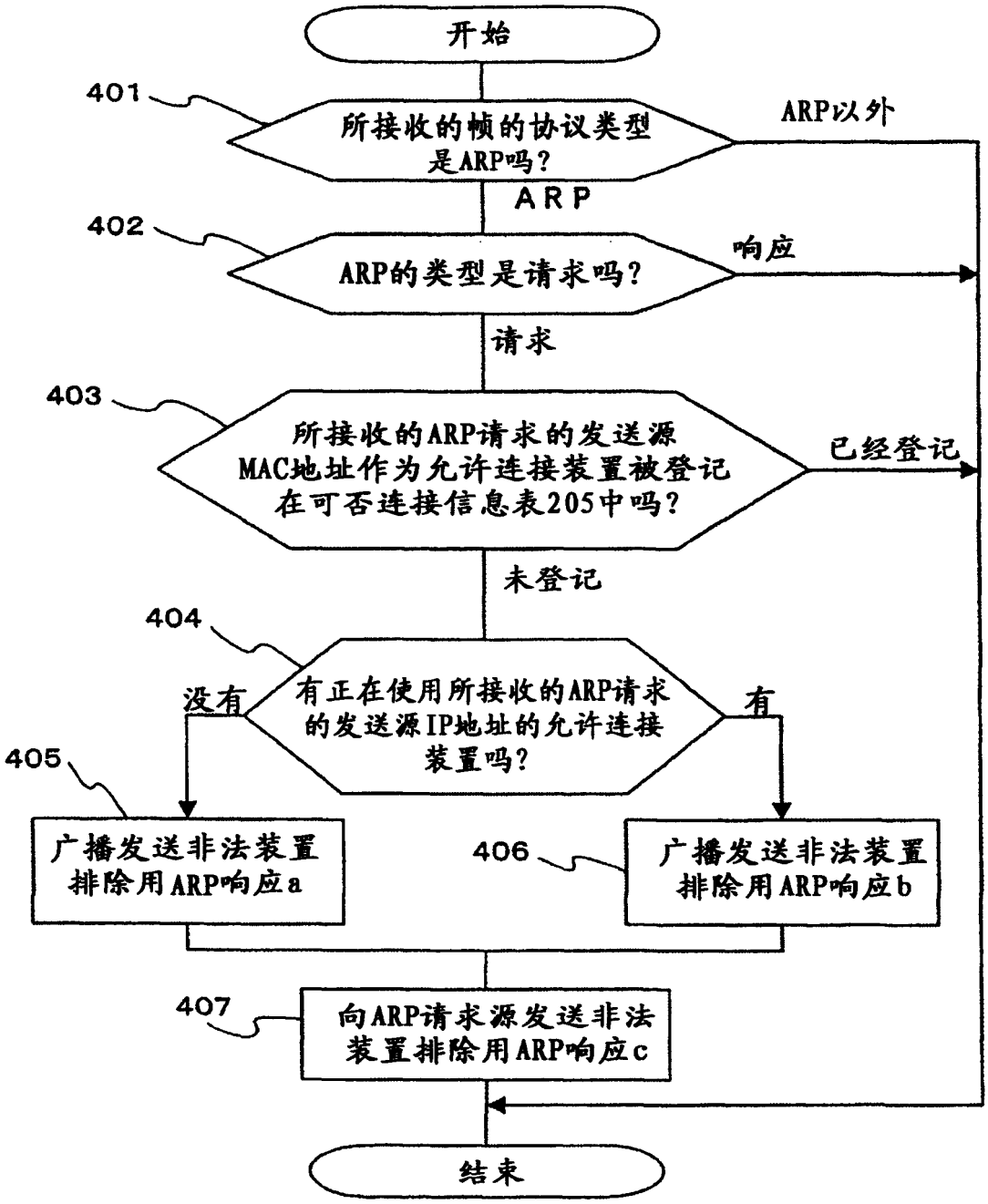

开始
401
所接收的帧的协议类型是ARP吗？
ARP以外
ARP
402
ARP的类型是请求吗？
响应
请求
403
所接收的ARP请求的发送源MAC地址作为允许连接装置被登记在可否连接信息表205中吗？
已经登记
未登记
404
有正在使用所接收的ARP请求的发送源IP地址的允许连接装置吗？
没有
有
405
广播发送非法装置排除用ARP响应a
406
广播发送非法装置排除用ARP响应b
407
向ARP请求源发送非法装置排除用ARP响应c
结束

图4

非法装置排除用ARP响应a

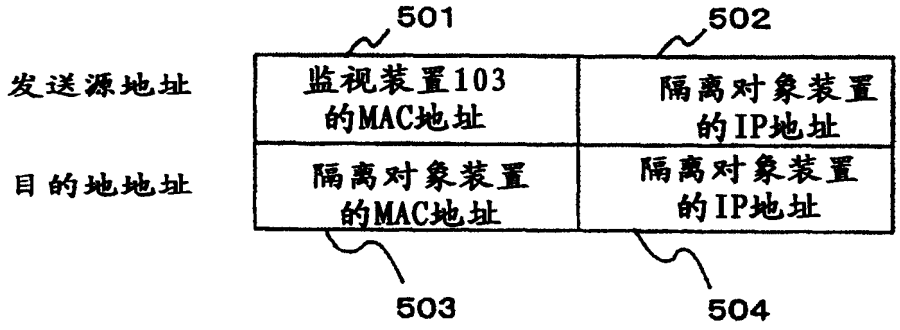


图5

非法装置排除用ARP响应b

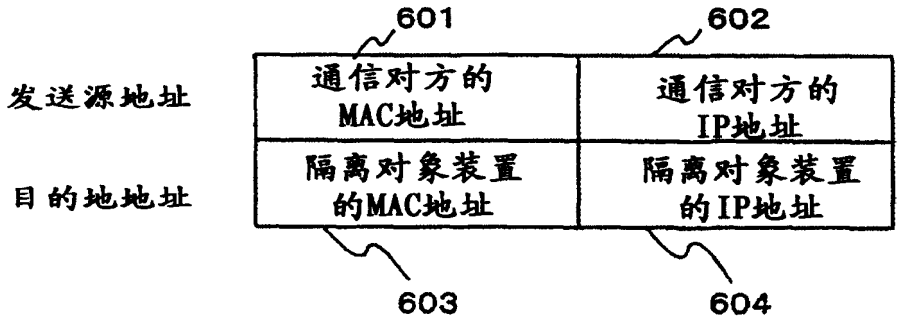


图6

非法装置排除用ARP响应c

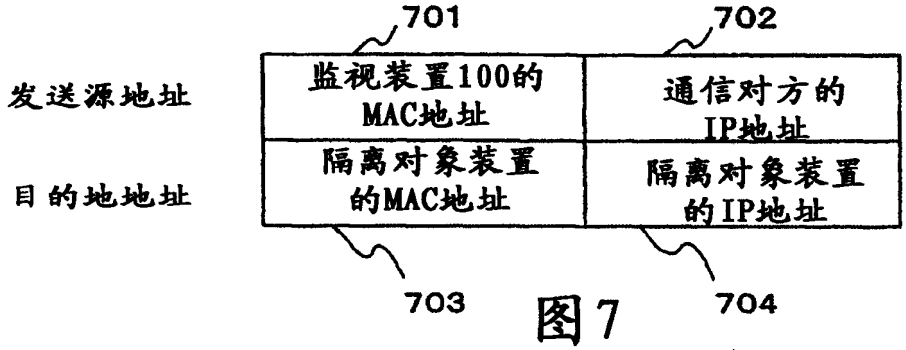


图7

可否连接信息表205的结构

	MAC地址	IP地址	状态
装置101a	MAC801	IP804	允许连接
装置101b	MAC802	IP805	允许连接
隔离对象装置103	MAC803	IP806	隔离对象

810 811 812

图8

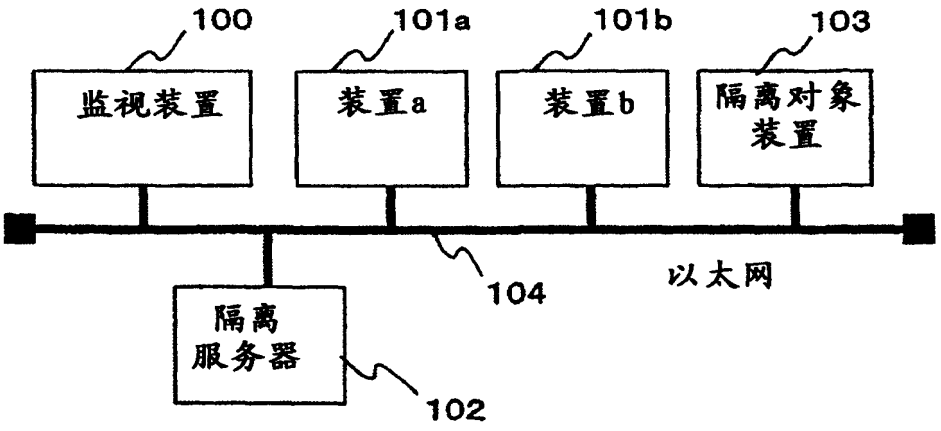


图9

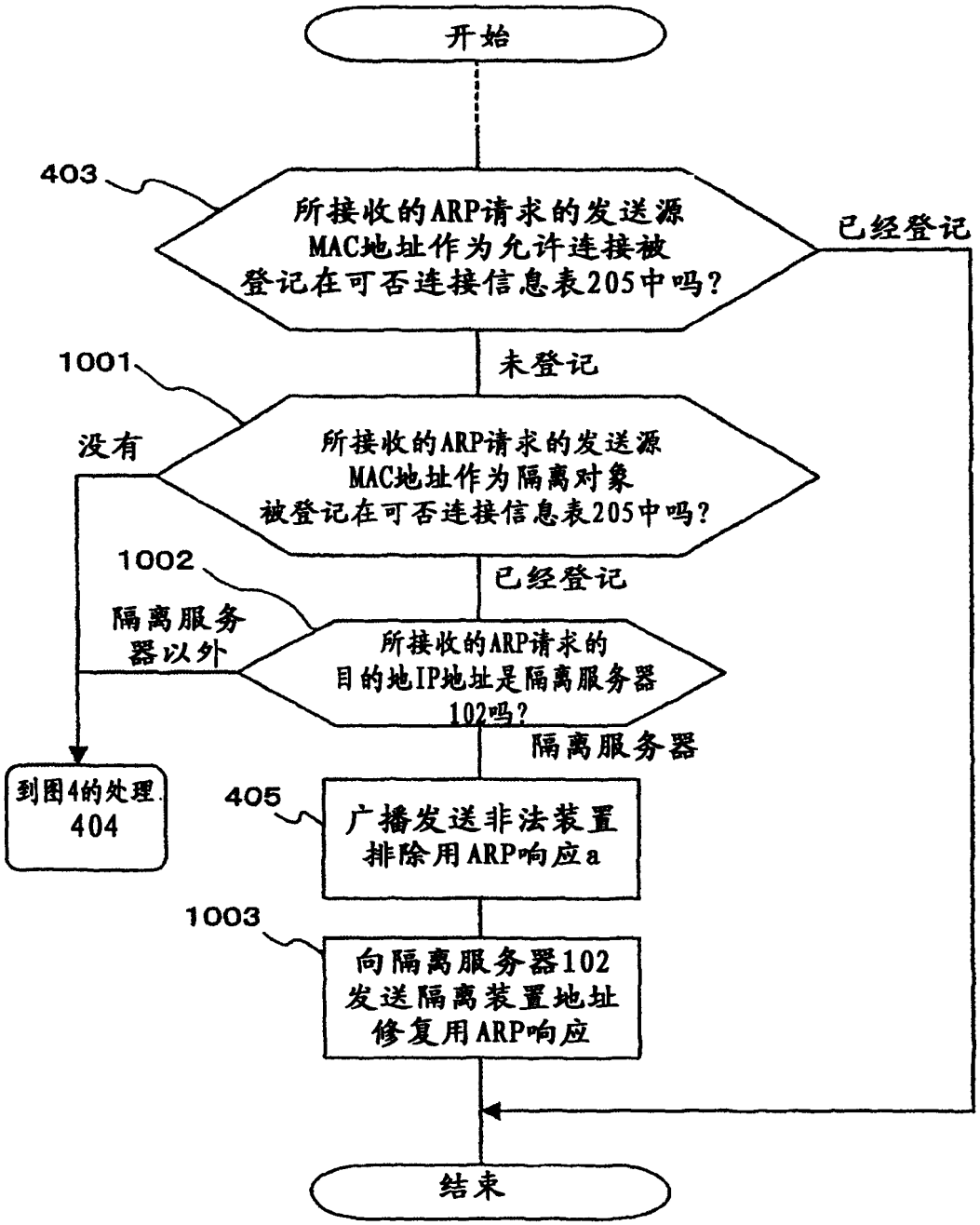

开始
403
所接收的ARP请求的发送源MAC地址作为允许连接被登记在可否连接信息表205中吗?
已经登记
未登记
1001
所接收的ARP请求的发送源MAC地址作为隔离对象被登记在可否连接信息表205中吗?
没有
已经登记
1002
隔离服务器以外
所接收的ARP请求的目的地IP地址是隔离服务器102吗?
隔离服务器
到图4的处理404
405
广播发送非法装置排除用ARP响应a
1003
向隔离服务器102发送隔离装置地址修复用ARP响应
结束

图10

隔离装置地址修复用ARP响应

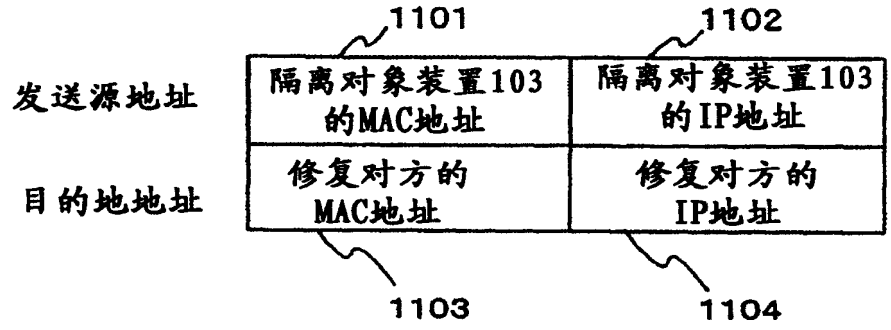


图11

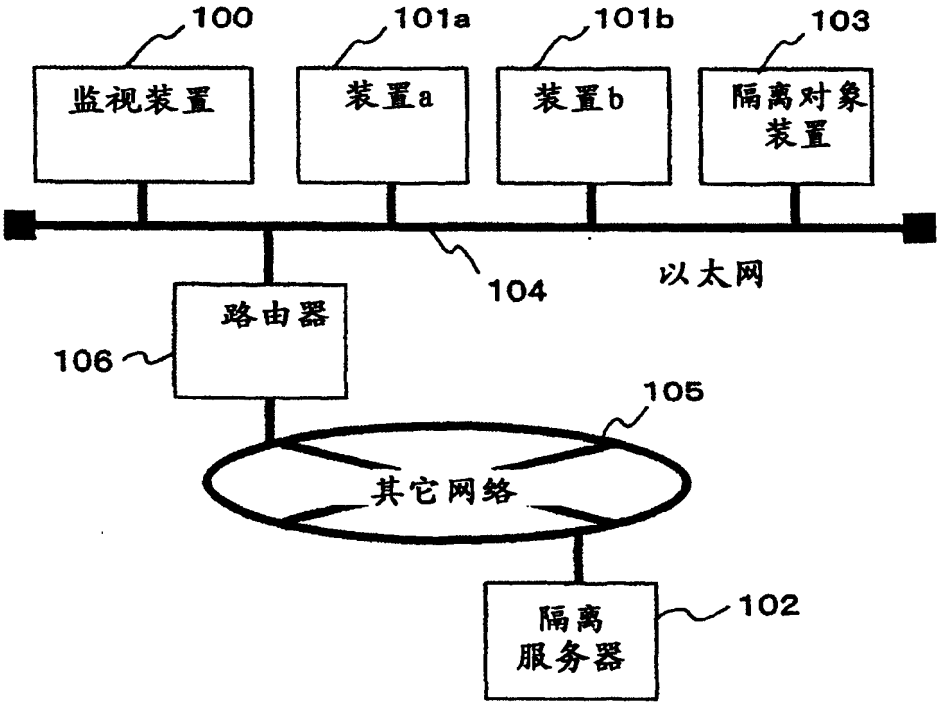


图12

路由器106的过滤设定表

1301

发送源IP地址 (1302)	目的地IP地址 (1303)	动作 (1304)
隔离对象装置103a	隔离服务器以外	废弃
隔离对象装置103b	隔离服务器以外	废弃
隔离对象装置103c	隔离服务器以外	废弃

图13

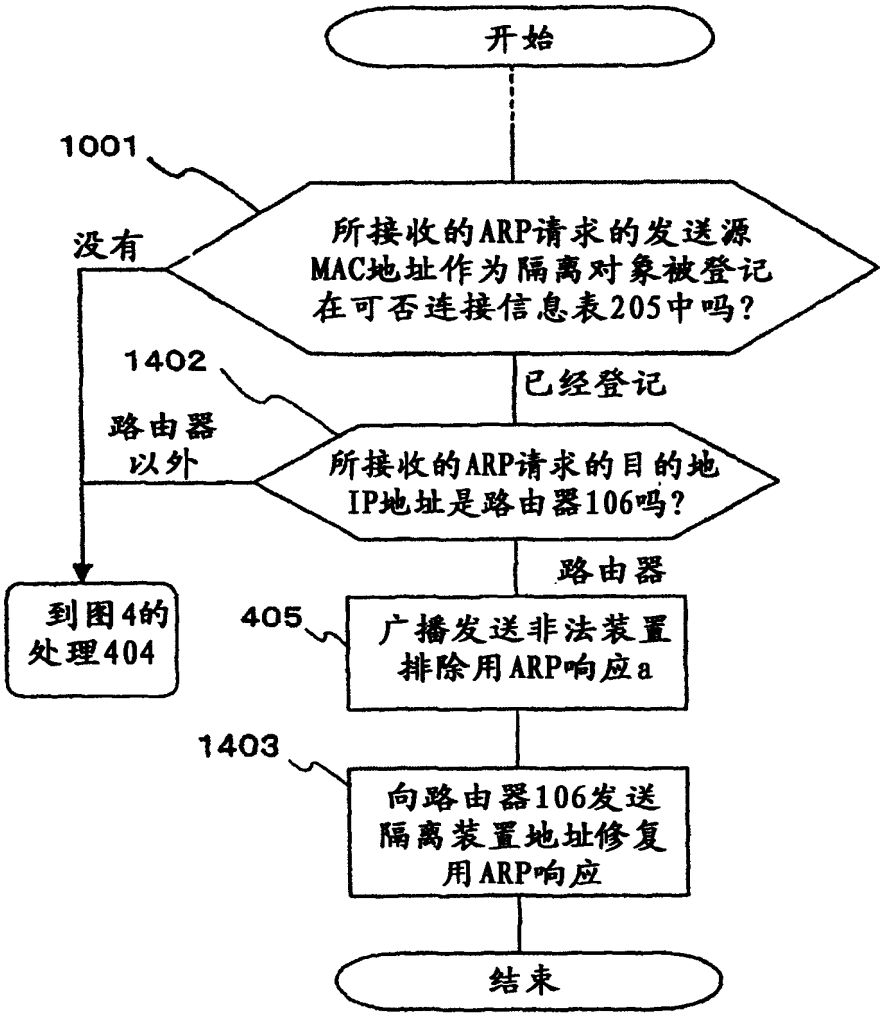

开始
1001
所接收的ARP请求的发送源MAC地址作为隔离对象被登记在可否连接信息表205中吗?
没有
已经登记
1402
路由器以外
所接收的ARP请求的目的地IP地址是路由器106吗?
路由器
到图4的处理404
405
广播发送非法装置排除用ARP响应a
1403
向路由器106发送隔离装置地址修复用ARP响应
结束

图14

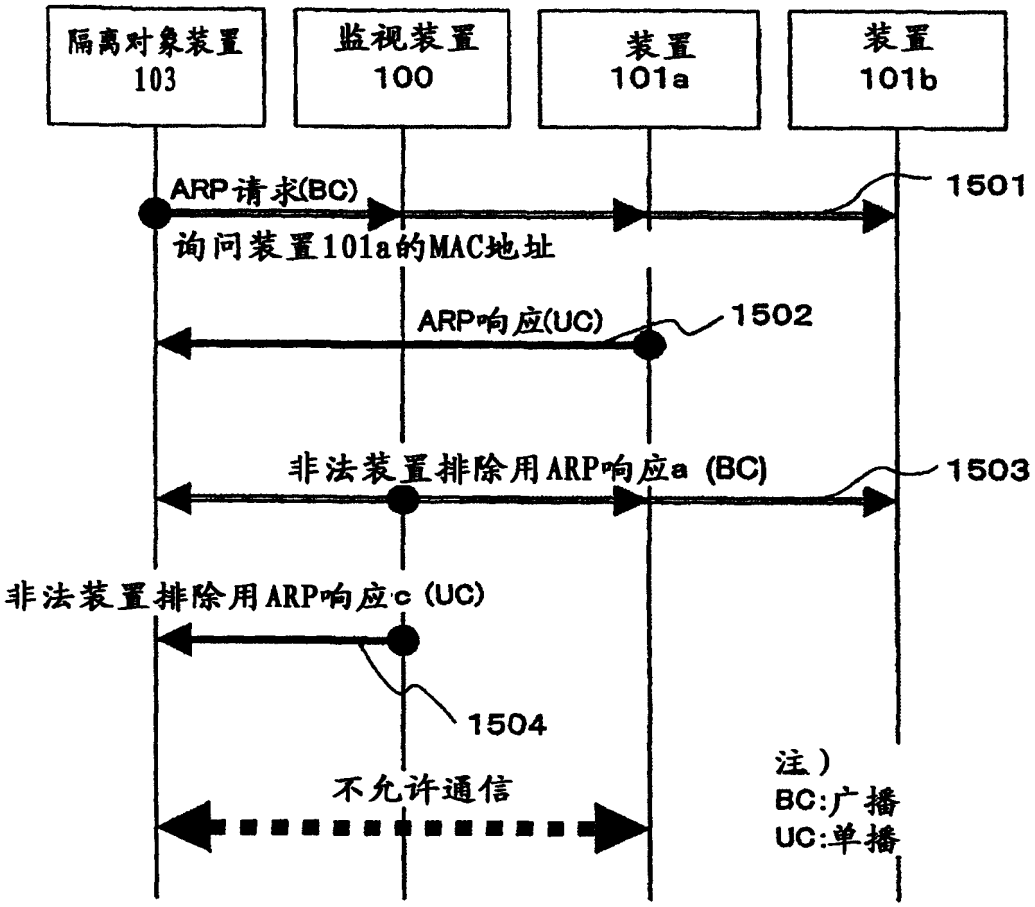

隔离对象装置
103
监视装置
100
装置
101a
装置
101b
ARP请求(BC)
1501
询问装置101a的MAC地址
ARP响应(UC)
1502
非法装置排除用ARP响应a (BC)
1503
非法装置排除用ARP响应c (UC)
1504
不允许通信
注）
BC:广播
UC:单播

图15

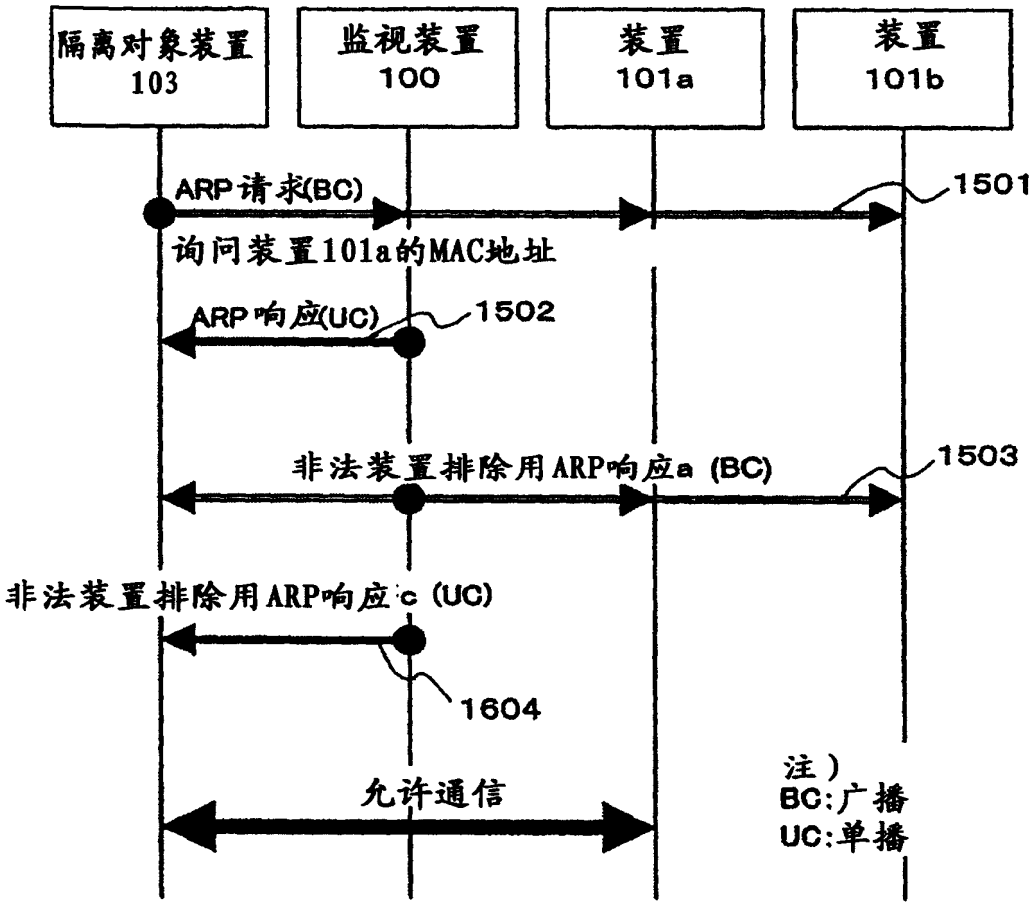

隔离对象装置
103
监视装置
100
装置
101a
装置
101b
ARP请求(BC)
1501
询问装置101a的MAC地址
ARP响应(UC)
1502
非法装置排除用ARP响应a (BC)
1503
非法装置排除用ARP响应c (UC)
1604
允许通信
注）
BC:广播
UC:单播

图16

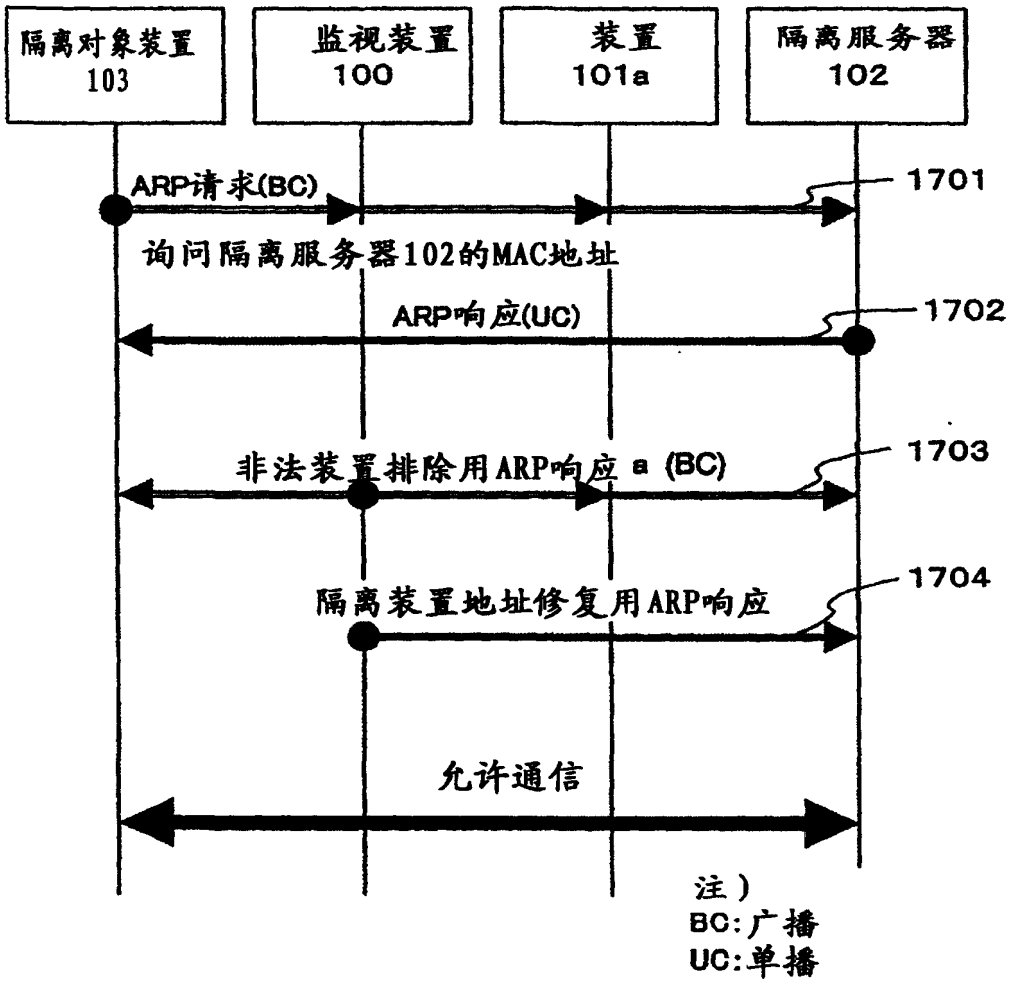

隔离对象装置
103
监视装置
100
装置
101a
隔离服务器
102
ARP请求(BC)
1701
询问隔离服务器102的MAC地址
ARP响应(UC)
1702
非法装置排除用ARP响应 a (BC)
1703
隔离装置地址修复用ARP响应
1704
允许通信
注)
BC:广播
UC:单播

图17

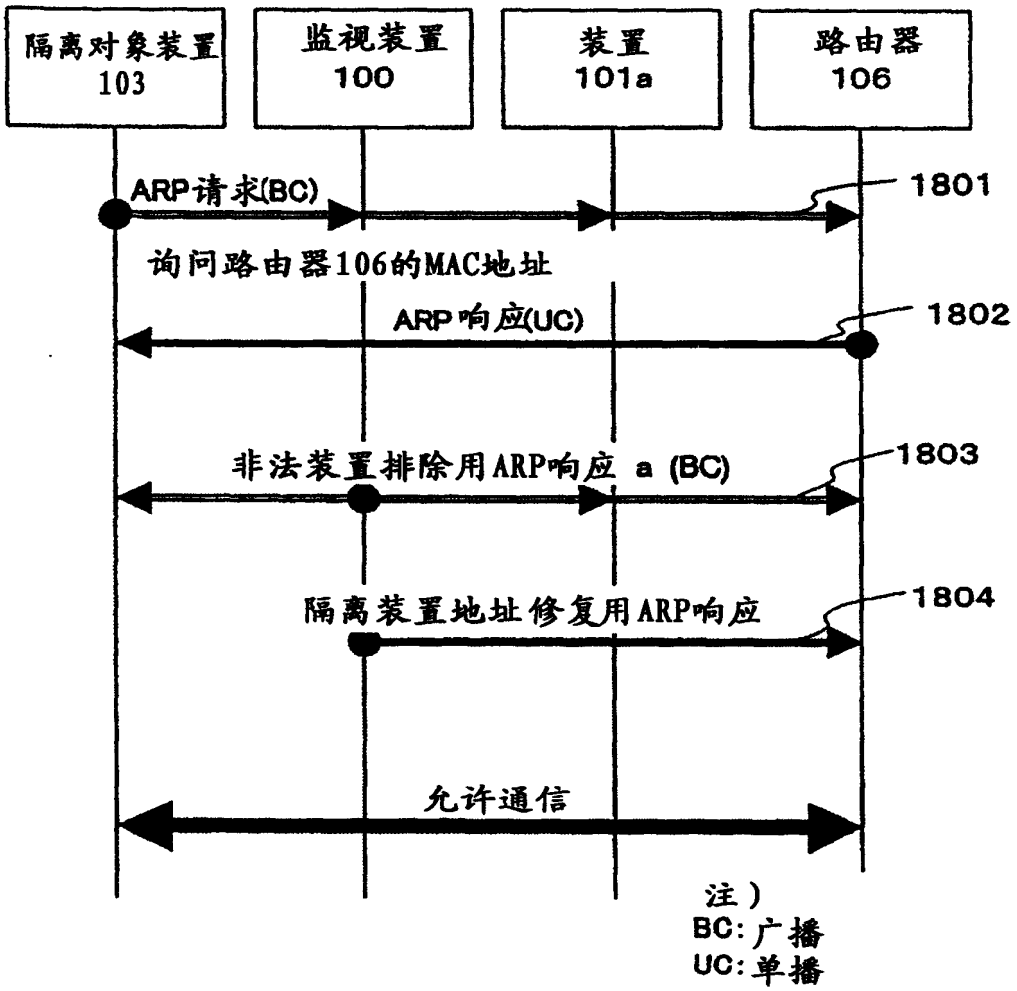

隔离对象装置
103
监视装置
100
装置
101a
路由器
106
ARP请求(BC)
1801
询问路由器106的MAC地址
ARP响应(UC)
1802
非法装置排除用ARP响应 a (BC)
1803
隔离装置地址修复用ARP响应
1804
允许通信
注)
BC:广播
UC:单播

图18