I315139

（此處由本局於收文時黏貼條碼）

761773

# 發明專利說明書

公告本

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：95118494

※申請日期：95 年 05 月 24 日

※IPC 分類：H04L 12/26 (2006.01)
H04L 12/24 (2006.01)
G06F 9/44 (2006.01)

## 一、發明名稱：

(中) 網路監視裝置、網路監視方法、網路系統及網路監視方法及網路通訊方法

(英)

## 二、申請人：(共 2 人)

1.姓　名：(中) 日立製作所股份有限公司
(英) HITACHI, LTD.
代表人：(中) 1.古川一夫
(英)
地　址：(中) 日本國東京都千代田區丸之內一丁目六番六號
(英) 6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
國籍：(中英) 日本　JAPAN

2.姓　名：(中) 日立信息控制系統有限公司
(英) HITACHI INFORMATION & CONTROL SOLUTIONS, LTD.
代表人：(中) 1.臼井敏雄
(英) 1.USUI, TOSHIO
地　址：(中) 日本國茨城縣日立市大甕町五丁目二番一號
(英) 5-2-1, Omika-cho, Hitachi-shi, Ibaraki-ken, 319-1293 Japan
國籍：(中英) 日本　JAPAN

## 三、發明人：(共 5 人)

1.姓　名：(中) 吉川秀之
(英) YOSHIKAWA, HIDEYUKI
國　籍：(中) 日本
(英) JAPAN

2.姓　名：(中) 足達芳昭
(英) ADACHI, YOSHIAKI
國　籍：(中) 日本
(英) JAPAN

(S)

3.姓　名：（中）外岡秀樹
（英）TONOOKA, HIDEKI
國　籍：（中）日本
（英）JAPAN

4.姓　名：（中）鴨志田弘司
（英）KAMOSHIDA, KOJI
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）武富浩二
（英）TAKEDOMI, KOJI
國　籍：（中）日本
（英）JAPAN

## 四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　；2005/06/20；2005-178697 ☑有主張優先權

3.姓　名：（中）外岡秀樹
（英）TONOOKA, HIDEKI
國　籍：（中）日本
（英）JAPAN

4.姓　名：（中）鴨志田弘司
（英）KAMOSHIDA, KOJI
國　籍：（中）日本
（英）JAPAN

5.姓　名：（中）武富浩二
（英）TAKEDOMI, KOJI
國　籍：（中）日本
（英）JAPAN

## 四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　；2005/06/20；2005-178697 ☑有主張優先權

(1)

## 九、發明說明

【發明所屬之技術領域】

本發明係有關於網路監視裝置、網路監視方法、網路系統及網路監視方法及網路通訊方法。

【先前技術】

爲了保護公司內 LAN 等受到保護的網路，限制對網路之連接的所謂網路監視裝置已爲公知。此種技術，例如日本特開 2003-303118 號公報中已有記載。

〔專利文獻 1〕日本特開 2003-303118 號公報

【發明內容】

〔發明所欲解決之課題〕

此種檢疫網路中，尤其是從外部攜入的電腦等，往受保護之網路的連接被許可之前，會確認該當電腦的作業系統或病毒偵測軟體是否有被更新，若未更新，則必須要供給該當電腦之作業系統或病毒偵測軟體的版本升級軟體。

因此，考慮利用認證交換器(switch)。亦即，在將從外部攜入的電腦連接至公司內 LAN 等受保護之網路之際，支援檢疫網路機能的交換式集線器會將被該電腦所連接的埠，連接至由和受保護之網路式呈虛擬性切離之虛擬 LAN(VLAN)所構成之檢疫網路。然後，一旦在檢疫網路上，作業系統(OS)或病毒偵測軟體的更新完成，則交換式集線器會變更 VLAN 的設定，使得將被該當電腦所連接的埠

變成隸屬於受保護之網路側。

可是在此同時，在受保護之網路中，從終端所連接的交換式集線器，至檢疫伺服器所連接之交換式集線器爲止，該路徑上所有的交換式集線器都必須要支援檢疫網路機能。

又，還可考慮利用認證 DHCP 方式。亦即，當從外部攜入的電腦要使用 DHCP 來取得 IP 位址之際，DHCP 伺服器會將檢疫網路用的 IP 位址和預設閘道 IP 位址，發配給該當電腦。由於檢疫網路用的 IP 位址係和受保護之網路在 IP 位址體系上互異，因此該當電腦式無法和受保護之網路內的裝置通訊。該當電腦係一旦在檢疫網路上完成了 OS 或病毒偵測軟體的更新，便再次被發配可和受保護之網路連接之 IP 位址和預設閘道 IP 位址，變成可和受保護之網路內之裝置通訊。

又，雖然只要式受保護之網路爲使用 DHCP 的環境就可適用，但在固定分配 IP 位址之網路環境中是無法適用，又，即使是使用 DHCP 的環境中，對於固定分配 IP 位址的裝置也沒有效果。

甚至，還有考慮到利用個人防火牆。亦即，和受保護之網路連接之電腦上，事前安裝好具有防火牆機能之軟體。當該當電腦試圖連接至受保護之網路之際，個人防火牆會限制通訊，使其只能和保存有 OS 或病毒偵測軟體之更新程式的檢疫伺服器通訊。一旦更新結束，則個人防火牆的限制就解除，而變成可和受保護之網路內之裝置通訊。

(3)

可是在此同時，具有連接至受保護之網路之可能性的電腦上必須事前安裝個人防火牆之軟體，對沒有安裝這些軟體的裝置是沒有效果的。

本發明的目的，係爲了解決上記至少 1 個問題點，並提供可圖像之網路監視裝置、網路監視方法、網路系統及網路監視方法及網路通訊方法。

〔用以解決課題之手段〕

爲了達成上記目的，本發明中是構成爲，以收訊部接收訊框；當該收訊，是從檢疫對象節點所送來之訊框時，不妨礙檢疫對象節點和儲存檢疫資訊之節點的通訊，且以不含有關於其他節點之網路位址和比前述網路高層中的相應之位址的組合之方式進行演算處理，從送訊部發送訊框。

具體而言，係使用具備：接收乙太網路上之乙太訊框的訊框收訊處理部；和發送乙太訊框的訊框送訊處理部；和積存著連接至檢疫網路之裝置的相關資訊的連接可否資訊表；和根據收到之乙太訊框和連接可否資訊表來判斷 ARP 訊框送訊的連接可否判斷處理部；和依照來自連接可否判斷處理部的指示來發送 ARP 訊框的 ARP 回應訊框生成部；和記憶著檢疫所必須之軟體的 OS/病毒偵測軟體之更新資料保存部的連接著乙太網路之廣播網域的監視裝置，隨應於來自檢疫對象裝置的 ARP 要求而發送 ARP 回應，藉此而實現檢疫網路。

〔發明效果〕

若依據本發明，則對於從外部攜入的電腦等之節點，在被許可往網路之節點的通訊以前，可使電腦的作業系統或病毒偵測軟體等維持在適切的版本。

【實施方式】

以下使用圖面來說明本發明的實施例。圖 1 係本發明之檢疫網路方式的實施例 1。本構成例中，由乙太網路所致之 1 個廣播網域所成的網路 104 上，連接有監視裝置 100、數台裝置 101a～101b、檢疫對象裝置 103。本實施例中，保持著 OS/病毒偵測軟體之更新資料的檢疫伺服器是由監視裝置 100 來兼任。

圖 2 係本實施例中的監視裝置 100 之構成，是由：連接至網路 104 的訊框收訊處理部 201、訊框送訊處理部 202、OS/病毒偵測軟體之更新資料保存部 203、連接可否判斷處理部 204、連接可否資訊表 205、ARP 回應訊框生成部 206 所成。此外，ARP (Address Resolution Protocol)，係在 TCP/IP 協定中，用來從 IP 位址求出 MAC 位址所須之協定。具體而言，是將自己的乙太網路位址和自己的 IP 位址、以及通訊目的地之 IP 位址這 3 者的組合，當成 ARP 要求，對 LAN 上進行廣播。由於 LAN 上的各節點係會監視著 ARP 詢問的廣播，因此只要自己的 IP 位址有被指定，便在封包中裝入自己的 MAC 位址作爲 ARP 回應而回送回應。藉由此 ARP 要求，和 ARP 回應，就可從 IP 位

址獲得 MAC 位址。此外，所謂的 MAC 位址，係在網際網路上用來進行訊框收送訊所需之實體性的位址；是以全世界上不會具有相同實體位址的方式，而分配著全部互異之固有的位址。又，IP 位址，係在使用 TCP/IP 協定的網路等，對每台伺服器或客戶端、路由器等之節點所分配的固有之位址，是爲了指定通訊目的地機器所使用。

圖 8 係圖示了連接可否資訊表 205 的構成。本表係由連接網路 104 的各台裝置之相關的 MAC 位址 MAC、IP 位址 811、狀態 812 的組合所構成。關於狀態 812 是記爲連接許可的裝置間的通訊，監視裝置 100 係一切不加以干涉。關於狀態 812 是記爲檢疫對象的裝置，監視裝置 100 會進行處理使得該當裝置只能和監視裝置 100 之間通訊。本表中沒有記錄項目的裝置係爲不許可連接的裝置。檢疫對象裝置 103 係爲從外部攜入的電腦，且雖然是被許可和網路的連接，但是仍需要更新 OS/病毒偵測軟體者。檢疫對象裝置 103 係爲了要和其他裝置通訊，而以廣播來發送出 ARP 要求訊框。

圖 3 中圖示了 ARP 要求訊框。當檢疫對象裝置 103 發送出 ARP 要求訊框時，送訊來源 MAC 位址 301 中放入了檢疫對象裝置 103 的 MAC 位址，送訊來源 IP 位址 302 中放入了檢疫對象裝置 103 的 IP 位址。目的端 MAC 位址 303 中則放入 0。目的端 IP 位址中則放入了檢疫對象裝置 103 所欲通訊之對方裝置的 IP 位址。

圖 4 中圖示了，監視裝置 100 內的連接可否判斷處理

部 204 之處理流程。處理 401 中判斷已收到之訊框的協定種別，若爲 ARP 以外則結束處理。處理 402 中判定已收到之 ARP 的種別，若爲 ARP 回應則結束處理。處理 403 中，判斷已收到之 ARP 要求的送訊來源 MAC 位址是否有在連接可否資訊表 205 中被登錄成連接許可裝置。若已有登錄則結束處理。處理 404 中，判斷是否有正在使用已收到之 ARP 要求的送訊來源 IP 位址的連接許可裝置。若無則實施處理 405，若有則實施處理 406。處理 405 中藉由將不正當裝置排除用 ARP 回應 a 予以廣播發送，例如，可防止從裝置 101a 對檢疫對象裝置 103 之通訊。處理 406 中係將不正當裝置排除用 ARP 回應 b 予以廣播發送。這是爲了應付當檢疫對象裝置 103 正在使用其他裝置所被發配之 IP 位址時的情況。亦即，檢疫對象裝置 103 雖然會因爲發送 ARP 要求而導致該當 IP 位址收的通訊目的端被改寫成檢疫對象裝置 103 收，但藉由發送不正當裝置排除用 ARP 回應 b，就可將該當 IP 位址收的通訊，修正成原本的裝置收。處理 407 係將不正當裝置排除用 ARP 回應 c 送出給檢疫對象裝置 103 收，以使檢疫對象裝置 103 將作爲通訊對方而發送過 ARP 要求之裝置的 MAC 位址，覆寫成監視裝置 100 的 MAC 位址，藉此以使來自檢疫對象裝置的通訊，被轉向成監視裝置 100 收。

圖 5 中圖示了不正當裝置排除用 ARP 回應 a。送訊來源 MAC 位址 501 中係放入了監視裝置 100 的 MAC 位址，送訊來源 IP 位址 502 中係放入了檢疫對象裝置的 IP 位址

(7)

，收訊端 MAC 位址 503 中係放入了檢疫對象裝置的 MAC 位址，收訊端 IP 位址 504 中係放入了檢疫對象裝置的 IP 位址。

圖 6 中圖示了不正當裝置排除用 ARP 回應 b。送訊來源 MAC 位址 601 中係放入了通訊對方的 MAC 位址，送訊來源 IP 位址 602 中係放入了通訊對方的 IP 位址，收訊端 MAC 位址 603 中係放入了檢疫對象裝置的 MAC 位址，收訊端 IP 位址 604 中係放入了檢疫對象裝置的 IP 位址。

圖 7 中圖示了不正當裝置排除用 ARP 回應 b。送訊來源 MAC 位址 701 中係放入了監視裝置 100 的 MAC 位址，送訊來源 IP 位址 702 中係放入了通訊對方的 IP 位址，收訊端 MAC 位址 703 中係放入了檢疫對象裝置的 MAC 位址，收訊端 IP 位址 704 中係放入了檢疫對象裝置的 IP 位址。

此處，檢疫對象裝置 103 和監視裝置 100 以外的裝置、例如裝置 101a 進行通訊時的動作，依照圖 4 所示的流程和圖 15 所示的流程來詳細說明。此處係假設，檢疫對象裝置 103 係持有和其他裝置不重複的 IP 位址。在和裝置 101a 開始通訊之前，檢疫對象裝置 103 係將 ARP 要求 1501 予以廣播發送。此時，圖 3 所示之通訊對方的 IP 位址 304 中係設定了裝置 101a 的 IP 位址。

對該 ARP 要求，裝置 101a 會回送 ARP 回應 1502。又，ARP 要求 1501 係因爲廣播發送，所以監視裝置 100 也會接收。監視裝置 100 係依照如圖 4 所示的流程而進行

對該訊框的處理。亦即，處理 401 係因爲是 ARP 所以進入處理 402，處理 402 係因爲是要求所以進入處理 403，處理 403 中，由於檢疫對象裝置 103 之 MAC 位址，係在連接可否資訊表 205 上被登錄成檢疫對象，因此進入處理 404。

處理 404 中，由於檢疫對象裝置 103 之 IP 位址係沒有正在被其他裝置使用，因此進入處理 405。處理 405 中，監視裝置 100 係將圖 15 之 1503 中所示之不正當裝置排除用 ARP 回應 a 予以廣播發送。藉此，連接著網路 104 的裝置係將監視裝置 100 之 MAC 位址當成檢疫對象裝置 103 之 MAC 位址而加以記憶，因此往檢疫對象裝置 103 收的通訊是變成不可能進行。

然後，依照圖 4 的流程，監視裝置 100 係於處理 407 中將圖 15 之 1504 中所示的不正當裝置排除用 ARP 回應 c，送出給檢疫對象裝置 103 收。藉此，由於檢疫對象裝置 103 係將監視裝置 100 的 MAC 位址當成裝置 101a 的 MAC 位址而加以記憶，因此往裝置 101a 收的通訊是變成不可能進行。

然後，檢疫對象裝置 103 在嘗試和監視裝置 100 通訊時的動作，依照圖 4 所示的流程和圖 16 所示的流程來詳細說明。至處理 405 爲止的動作係和上記說明過的動作沒有不同。接下來的處理 407 中，監視裝置 100 雖然係將圖 16 之 1604 中所示之不正當裝置排除用 ARP 回應 c 送出給檢疫對象裝置 103 收，但此時，檢疫對象裝置 103 係將監

視裝置 100 的 MAC 位址當成監視裝置 100 的 MAC 位址而加以記憶。換言之，由於檢疫對象裝置 103 係記憶著正確的監視裝置 100 之 IP 位址和 MAC 位址的組合，因此變成可對監視裝置 100 進行通訊。藉此，檢疫對象裝置 103 係變成可將監視裝置 100 所擁有的 OS/病毒偵測軟體之更新資料傳送至自裝置，而可實施 OS/病毒偵測軟體的更新。在確認了本更新已經完成後，便將連接可否資訊表 205 上的檢疫對象裝置 103 的狀態，從檢疫對象改寫成連接許可。藉此，以後檢疫對象裝置 103 也能夠和裝置 101a～101b 同等地進行通訊。

以下，說明實施例 2。

圖 9 係本發明之實施例 2 的構成。本實施例中，和實施例 1 不同，監視裝置 100 係內部不具有 OS/病毒偵測軟體之更新資料保存部 203，取而代之的是設置了保持這些資料的檢疫伺服器 102。檢疫伺服器 102 的用途，是隨著來自檢疫對象裝置 103 的要求，而將 OS/病毒偵測軟體之更新資料傳送至檢疫對象裝置 103。

圖 10 中圖示了實施例 2 的監視裝置 100 內的連接可否判斷處理部 204 之處理流程。此外，此處僅記述和圖 4 不同的部份。處理 401～處理 403 爲止都和圖 4 相同。處理 403 之後的處理 1001 中，判定已收到之 ARP 要求的送訊來源 MAC 位址是否有在連接可否資訊表 205 中被登錄成檢疫對象。若未被登錄，則進入圖 4 的處理 404。若有登錄，則進入處理 1002。處理 1002 中，判定已收到之

ARP 要求的收訊端 IP 位址是否爲檢疫伺服器 102。若爲檢疫伺服器 102 以外，則進入圖 4 的處理 404。若爲檢疫伺服器 102 收則執行處理 405。處理 405 中藉由將不正當裝置排除用 ARP 回應 a 予以廣播發送，例如，可防止從裝置 101a 對檢疫對象裝置 103 之通訊。只不過，如此一來從檢疫伺服器 102 往檢疫對象裝置 103 的通訊也變成不可能，因此接著於處理 1003 中會將檢疫裝置位址修復用 ARP 回應，送出給檢疫伺服器 102 收。

圖 11 中圖示了檢疫裝置位址修復用 ARP 回應。送訊來源 MAC 位址 1101 中係設定了檢疫對象裝置 103 的 MAC 位址，送訊來源 IP 位址 1102 中係設定了檢疫對象裝置 103 的 IP 位址，收訊端 MAC 位址 1103 中係設定了修復對方的 MAC 位址，收訊端 IP 位址 1104 中係設定了修復對方的 IP 位址，並發送給修復對方收。

此處，檢疫對象裝置 103 在嘗試和檢疫伺服器 102 通訊時的動作，依照圖 10 所示的流程和圖 17 所示的流程來詳細說明。此處係假設，檢疫對象裝置 103 係持有和其他裝置不重複的 IP 位址。

在和檢疫伺服器 102 開始通訊之前，檢疫對象裝置 103 係將 ARP 要求 1701 予以廣播發送。此時，圖 3 的 ARP 要求訊框的通訊對方之 IP 位址 304 中，係設定了檢疫伺服器 102 的 IP 位址。因應該 ARP 要求，檢疫伺服器 102 係發送出 ARP 回應 1702。又，由於 ARP 要求 1701 係爲廣播發送，因此監視裝置 100 也會接收之，並依照圖 10

所示的流程，進行對該訊框的處理。只不過，由於處理401～處理 402 係和實施例 1 的處理相同，因此省略其說明。

接著在處理 403 中，由於檢疫對象裝置 103 之 MAC 位址，係在連接可否資訊表 205 上沒有被登錄成連接許可，因此進入處理 1001。處理 1001 中，由於檢疫對象裝置 103 之 MAC 位址，係在連接可否資訊表 205 上被登錄成檢疫對象，因此進入處理 1002。處理 1002 中，由於已收到之 ARP 要求的收訊端 IP 位址係爲檢疫伺服器 102，因此進入處理 405。處理 405 中，監視裝置 100 係將不正當裝置排除用 ARP 回應 a 1703 予以廣播發送。藉此，連接著網路 104 的裝置係將監視裝置 100 之 MAC 位址當成檢疫對象裝置 103 之 MAC 位址而加以記憶，因此往檢疫對象裝置 103 收的通訊是變成不可能進行。接著在處理 1003 中，監視裝置 100 係將檢疫裝置位址修復用 ARP 回應 1704，發送給檢疫伺服器 102 收。此時，收訊端 MAC 位址 1103 中係設定了檢疫伺服器 102 的 MAC 位址，收訊端 IP 位址 1104 中係設定了檢疫伺服器 102 的 IP 位址。藉此，由於檢疫伺服器 102 係將正確的 MAC 位址當成檢疫對象裝置 103 的 MAC 位址而加以記憶，因此，檢疫伺服器 102 和檢疫對象裝置 103 間的通訊是成爲可能。因此，檢疫對象裝置 103 係變成可將檢疫伺服器 102 所擁有的 OS/病毒偵測軟體之更新資料傳送至自裝置，而可實施 OS/病毒偵測軟體的更新。其後的動作係和實施例 1 相同。

以下，說明實施例 3。

圖 12 係本發明之實施例 3 的構成。本實施例中，和實施例 2 不同，檢疫伺服器 102 係透過路由器 106 而連接在其他網路 105 上。路由器 106 係具有，對通過其的 IP 封包，藉由條件而加以過濾之機能。過濾機能本身是先前以來就存在的一般性技術。

圖 13 中係圖示了路由器 106 的過濾設定表之例子。過濾設定表 1301，係由：作爲條件的送訊來源 IP 位址 1302 及收訊端 IP 位址 1303，和對滿足該條件之 IP 封包的行動 1304 所成。本實施例中，是對從網路 104 通過路由器 106 而往其他網路 105 的 IP 封包，適用本過濾。其設定值，在送訊來源 IP 位址中係設定了檢疫對象裝置 103 的 IP 位址。當檢疫對象裝置有複數台時，係如檢疫對象裝置 103a～103c 這樣作成複數的項目。收訊端 IP 位址 1104 中係設定成檢疫伺服器 102 以外而當作條件。行動則設定爲丟棄。

又，本實施例中，作爲檢疫對象裝置的預設閘道，係設定爲路由器 106 的網路 104 側 IP 位址。

圖 14 中圖示了實施例 3 的監視裝置 100 內的連接可否判斷處理部 204 之處理流程。此外，此處僅記述和圖 10 不同的部份。處理 401～處理 1001 爲止都和圖 10 相同。處理 1001 之後，處理 1402 中，判定已收到之 ARP 要求的收訊端 IP 位址是否爲路由器 106。若爲路由器 106 以外，則進入圖 4 的處理 404。若爲路由器 106 收則執行處理

405。處理 405 中藉由將不正當裝置排除用 ARP 回應予以廣播發送，例如，可防止從裝置 101a 對檢疫對象裝置 103 之通訊。只不過，如此一來從路由器 106 往檢疫對象裝置 103 的通訊也變成不可能，因此接著於處理 1403 中會將檢疫裝置位址修復用 ARP 回應，送出給路由器 106 收。

此處，檢疫對象裝置 103 在嘗試和檢疫伺服器 102 通訊時的動作，依照圖 14 所示的流程和圖 18 所示的流程來詳細說明。此處係假設，檢疫對象裝置 103 係持有和其他裝置不重複的 IP 位址。在和檢疫伺服器 102 開始通訊之前，檢疫對象裝置 103 係將 ARP 要求 1801 予以廣播發送。此時，圖 3 的 ARP 要求訊框的通訊對方之 IP 位址 304 中，係設定了路由器 106 的 IP 位址作爲檢疫對象裝置之預設閘道。因應該 ARP 要求，路由器 106 係發送出 ARP 回應 1802。又，由於 ARP 要求 1801 係爲廣播發送，因此監視裝置 100 也會接收之，並依照圖 14 所示的流程，進行對該訊框的處理。只不過，由於處理 401～處理 1001 係和實施例 2 的處理相同，因此省略其說明。接著在處理 1402 中，由於已收到之 ARP 要求的收訊端 IP 位址係爲路由器 106，因此進入處理 405。

處理 405 中，監視裝置 100 係將所示之不正當裝置排除用 ARP 回應 a 1803 予以廣播發送。藉此，連接著網路 104 的裝置係將監視裝置 100 之 MAC 位址當成檢疫對象裝置 103 之 MAC 位址而加以記憶，因此往檢疫對象裝置 103 收的通訊是變成不可能進行。接著在處理 1403 中，監視

裝置 100 係將檢疫裝置位址修復用 ARP 回應 1804，發送給路由器 106 收。此時，收訊端 MAC 位址 1103 中係設定了路由器 106 的 MAC 位址，收訊端 IP 位址 1104 中係設定了路由器 106 的 IP 位址。藉此，由於路由器 106 係將正確的 MAC 位址當成檢疫對象裝置 103 的 MAC 位址而加以記憶，因此，路由器 106 和檢疫對象裝置 103 間的通訊是成爲可能。從檢疫對象裝置 103 往檢疫伺服器 102 收的 IP 封包在通過路由器 106 之際，會和過濾設定表 1301 進行比較。此例中，由於送訊來源 IP 位址爲檢疫對象裝置 103、收訊端 IP 位址爲檢疫伺服器，因此 IP 封包係會通過路由器 106，而可送往其他網路 105，進而到達檢疫伺服器 102。因此，檢疫對象裝置 103 係變成可將檢疫伺服器 102 所擁有的 OS/病毒偵測軟體之更新資料傳送至自裝置，而可實施 OS/病毒偵測軟體的更新。其後的動作係和實施例 2 相同。

接著，詳細說明當檢疫對象裝置 103 和連接著其他網路 105 的檢疫伺服器 102 以外之裝置進行通訊時的動作。此情況下也是和前述檢疫對象裝置 103 和檢疫伺服器 102 間的通訊同樣地，因爲網路 104 內的檢疫對象裝置 103 的通訊對方係爲路由器 106，所以即使假設收訊端爲檢疫伺服器 102 以外的裝置，監視裝置 100 仍許可檢疫對象裝置 103 和路由器 106 間的通訊。可是，在和路由器 106 的過濾表 1301 的比較當中，由於收訊端 IP 位址爲檢疫伺服器 102 以外，因此 IP 封包會被丟棄。因此，檢疫對象裝置

103 和連接著其他網路 105 之檢疫伺服器 102 以外的裝置的通訊是不可能進行。

若依據本實施例，則不需要支援檢疫網路機能的專用交換式集線器，又，即使使用一般的重複集線器(repeater hub)也能夠成檢疫網路，因此不需要變更既存之網路的硬體構成。又，由於無論在 DHCP 環境中或是固定 IP 位址環境中都是同樣地動作，因此不需要變更既存網路環境。甚至，也不需要對所有的終端安裝個人防火牆等專用軟體，可更簡便地實現檢疫網路。

【圖式簡單說明】

〔圖 1〕實施例 1 的系統全體構成圖。

〔圖 2〕監視裝置的構成圖。

〔圖 3〕ARP 要求訊框的說明圖。

〔圖 4〕實施例 1 之監視裝置的動作的流程圖。

〔圖 5〕爲了使往檢疫對象裝置的通訊變成不可能而由監視裝置所發送之 ARP 回應 1。

〔圖 6〕爲了使往檢疫對象裝置的通訊變成不可能而由監視裝置所發送之 ARP 回應 2。

〔圖 7〕爲了使來自檢疫對象裝置的通訊變成不可能而由監視裝置所發送之 ARP 回應。

〔圖 8〕連接可否資訊表的構成。

〔圖 9〕實施例 2 的系統構成圖。

〔圖 10〕實施例 2 之監視裝置的動作的流程圖。

〔圖 11〕對一部份的裝置，爲了使前往檢疫對象裝置的通訊變成可能，而由監視裝置所發送之 ARP 回應。

〔圖 12〕實施例 3 的系統構成圖。

〔圖 13〕路由器的過濾設定表。

〔圖 14〕實施例 3 之監視裝置的動作的流程圖。

〔圖 15〕實施例 1 中當檢疫對象裝置嘗試和監視裝置以外的裝置進行通訊時的流程。

〔圖 16〕實施例 1 中當檢疫對象裝置是和監視裝置進行通訊時的流程。

〔圖 17〕實施例 2 中當檢疫對象裝置是和檢疫伺服器進行通訊時的流程。

〔圖 18〕實施例 3 中當檢疫對象裝置是經由路由器而和檢疫伺服器進行通訊時的流程。

【主要元件符號說明】

100：監視裝置、102：檢疫伺服器、103：檢疫對象裝置、104：監視裝置或檢疫對象裝置所連接之網路、105：透過路由器的其他網路、106：路由器、201：訊框收訊處理部、202：訊框送訊處理部、203：OS/防毒軟體的更新資料保存部、204：連接可否判斷處理部、205：連接可否資訊表、206：ARP 回應訊框生成部。

## 五、中文發明摘要

發明之名稱：網路監視裝置、網路監視方法、網路系統及網路監視方法及網路通訊方法

〔課題〕

先前，爲了實現檢疫網路，必須要導入具有支援該機能的專用交換式集線器等硬體，或者，將網路全體設成DHCP環境、導入專用的DHCP伺服器，或者，對預想會連接至LAN的所有裝置都安裝專用的個人防火牆程式等。

〔解決手段〕

本發明中，則在乙太網路之廣播網域中設置監視裝置，該監視裝置，會監視著來自檢疫對象裝置的ARP要求，隨應該要求而回送ARP回應，以實現僅許可和特定裝置之通訊的檢疫網路。

〔效果〕

將監視裝置連接至乙太網路的各廣播網域，就可實現監視裝置。

## 六、英文發明摘要

發明之名稱：

(1)

## 十、申請專利範圍

1.一種網路監視裝置，其特徵爲，具有：接收訊框的收訊處理部；和發送訊框的送訊處理部；和當接收到從檢疫對象節點所發送過來的訊框時，以不妨礙對檢疫對象節點之檢疫相關資訊之通訊的方式，且不含有關於其他節點之網路位址和比前述網路高層中的相應之位址的組合的方式，來發送訊框的處理部。

2.如申請專利範圍第 1 項之網路監視裝置，其中，具有記憶檢疫對象節點之位址的可否資訊表；藉由將前述訊框的位址和前述可否資訊表的記憶內容進行比較，以特定出成爲檢疫對象的節點。

3.如申請專利範圍第 1 項之網路監視裝置，其中，前述檢疫資訊係儲存在檢疫伺服器中。

4.如申請專利範圍第 3 項之網路監視裝置，其中，發送出訊框，其係含有前述檢疫伺服器之網路位址和比前述網路高層中的相應之位址的組合。

5.如申請專利範圍第 4 項之網路監視裝置，其中，當接收到要求含有網路位址和比前述網路高層中的相應之位址的組合之資訊的訊框時，進行前述訊框的發送處理。

6.如申請專利範圍第 5 項之網路監視裝置，其中，發送出資訊，其係含有自裝置之網路位址和比前述網路高層中的前述檢疫對象節點所相應之位址的組合。

7.如申請專利範圍第 5 項之網路監視裝置，其中，發送出資訊，其係含有自裝置之網路位址和比前述網路高層

中的通訊對方節點所相應之位址的組合。

8.如申請專利範圍第 3 項之網路監視裝置，其中，前述檢疫伺服器係被設置在其他網路中，且和前述檢疫伺服器，透過具有 IP 封包之過濾機能的路由器而連接。

9.如申請專利範圍第 1 項之網路監視裝置，其中，從保存 OS 或病毒偵測軟體之更新資料的保存部，往前述檢疫對象節點發送前述更新資料。

10.一種網路監視裝置，其特徵爲，具有：接收訊框的收訊處理部；和發送訊框的送訊處理部；和當接收到從檢疫對象節點所發送過來的訊框時，將檢疫對象節點所特定之節點上的網路位址或比前述網路更高層中的位址之至少一方，當成不相應於該節點的位址而發送訊框的處理部。

11.一種網路系統，其特徵爲，一旦訊框從檢疫對象節點被發送，則從監視節點，以不妨礙前述檢疫對象節點和儲存檢疫相關資訊之節點的通訊的方式，且不含有關於其他節點之網路位址和比前述網路高層中的相應之位址的組合之方式，來發送訊框。

12.一種網路監視方法，其特徵爲，以收訊部接收訊框；當該收訊，是從檢疫對象節點所送來之訊框時，以不妨礙對檢疫對象節點之檢疫相關資訊之通訊的方式，且以不含有關於其他節點之網路位址和比前述網路高層中的相應之位址的組合之方式進行演算處理，從送訊部發送訊框。

(3)

13.一種網路通訊方法，其特徵爲，一旦訊框從檢疫對象節點被發送，則從監視節點，以不妨礙前述檢疫對象節點和儲存檢疫相關資訊之節點的通訊的方式，且不含有關於其他節點之網路位址和比前述網路高層中的相應之位址的組合之方式，來發送訊框。

圖1

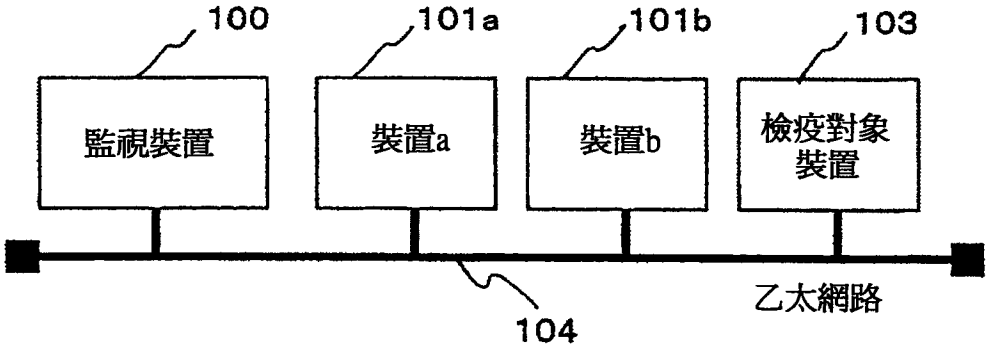

100
101a
101b
103
監視裝置
裝置a
裝置b
檢疫對象裝置
乙太網路
104

圖2

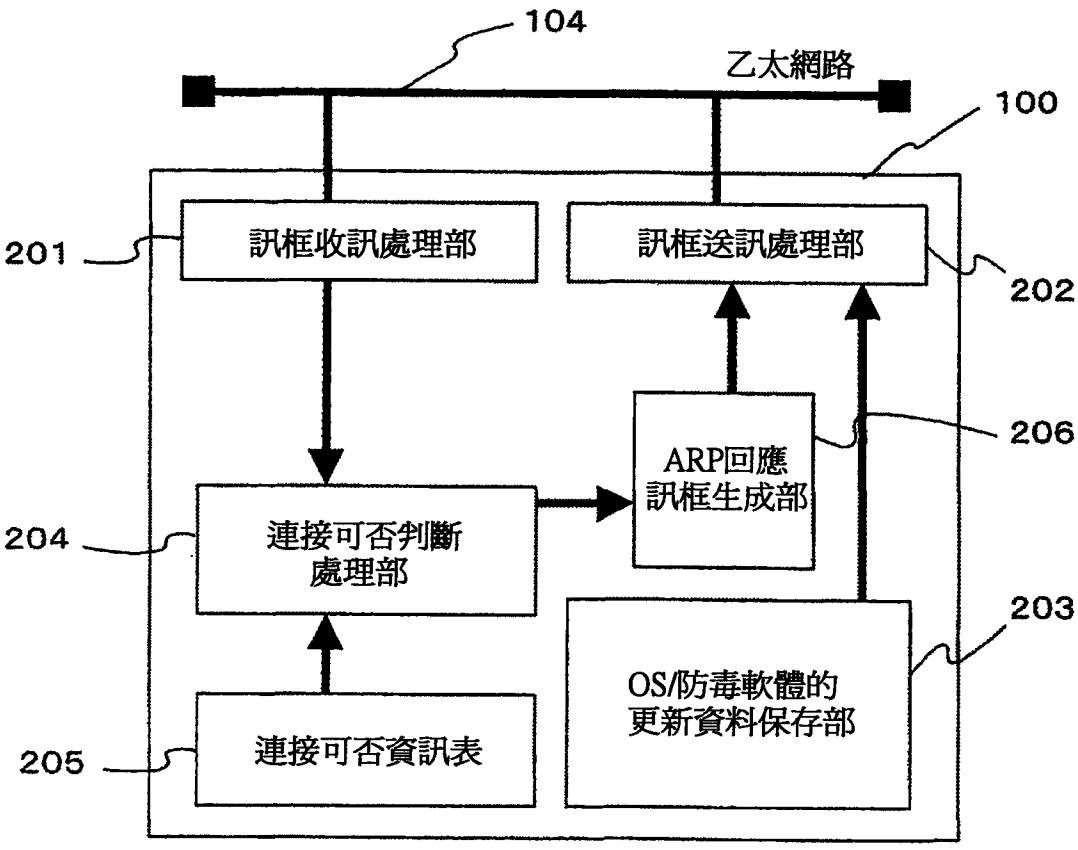
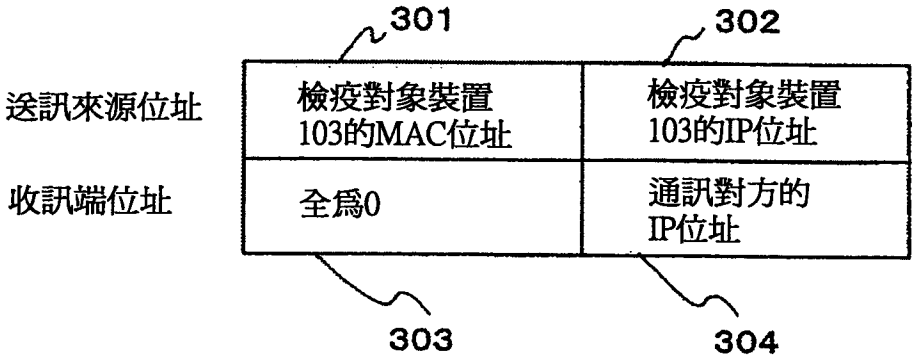
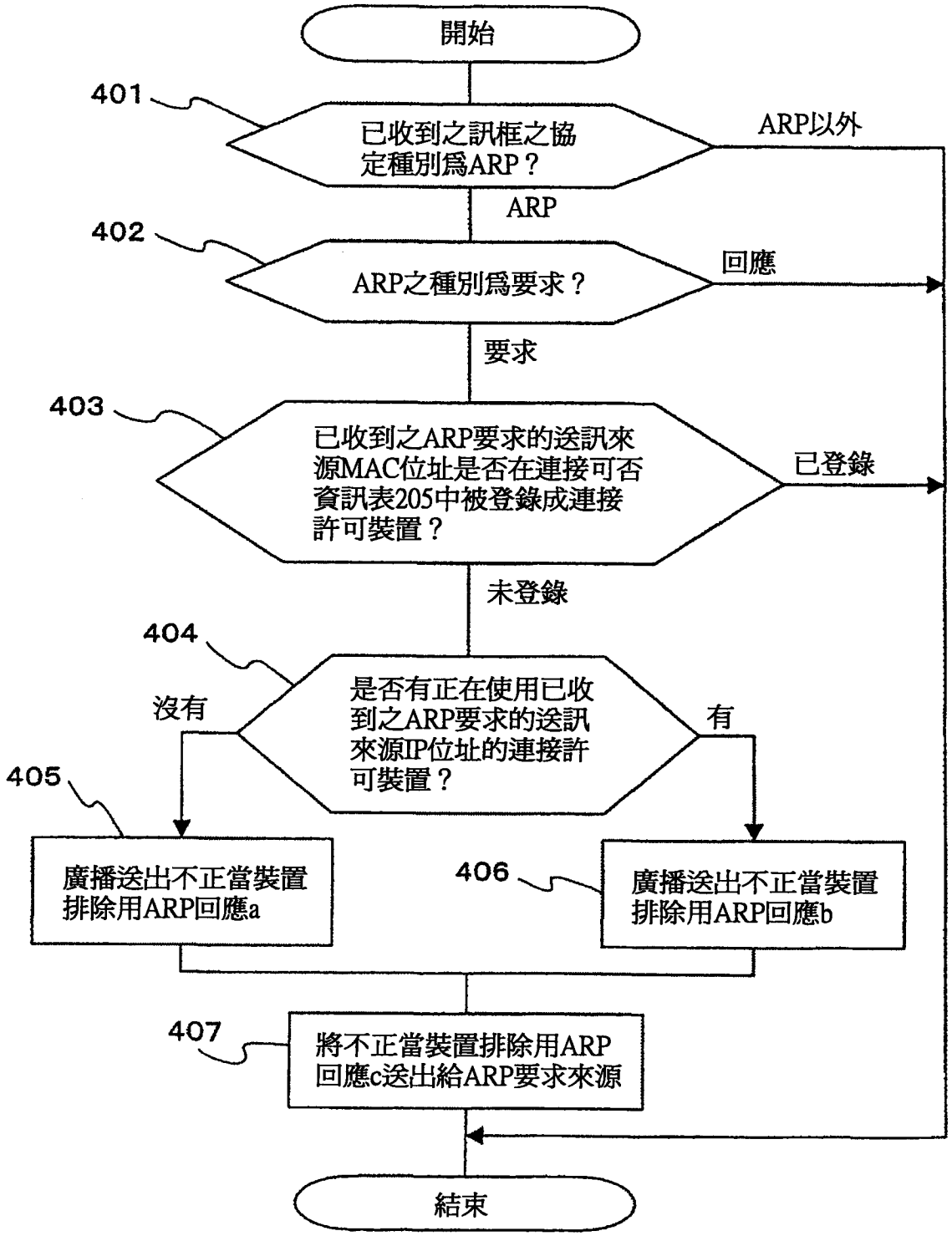

104
乙太網路
100
201
訊框收訊處理部
訊框送訊處理部
202
206
ARP回應訊框生成部
204
連接可否判斷處理部
203
OS/防毒軟體的更新資料保存部
205
連接可否資訊表

圖3

ARP要求訊框

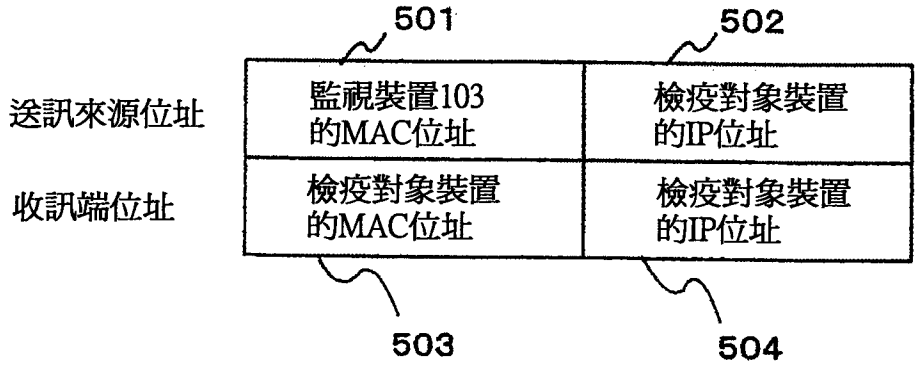

301
302
送訊來源位址
檢疫對象裝置
103的MAC位址
檢疫對象裝置
103的IP位址
收訊端位址
全爲0
通訊對方的
IP位址
303
304

# 圖4


開始
401
已收到之訊框之協定種別爲ARP？
ARP以外
ARP
402
ARP之種別爲要求？
回應
要求
403
已收到之ARP要求的送訊來源MAC位址是否在連接可否資訊表205中被登錄成連接許可裝置？
已登錄
未登錄
404
是否有正在使用已收到之ARP要求的送訊來源IP位址的連接許可裝置？
沒有
有
405
廣播送出不正當裝置排除用ARP回應a
406
廣播送出不正當裝置排除用ARP回應b
407
將不正當裝置排除用ARP回應c送出給ARP要求來源
結束

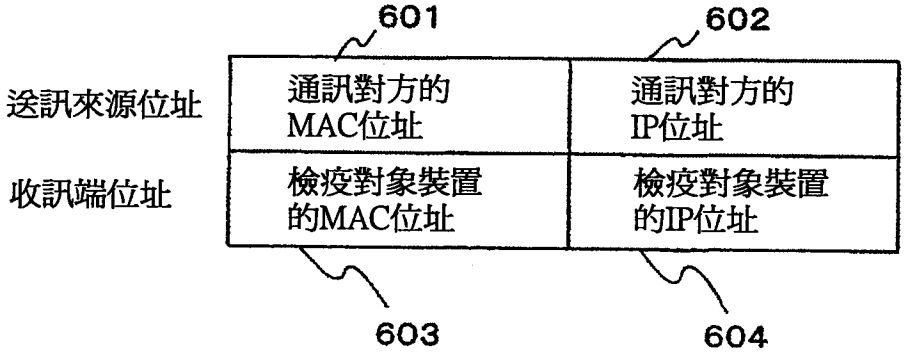
# 圖5

不正當裝置排除用ARP回應a



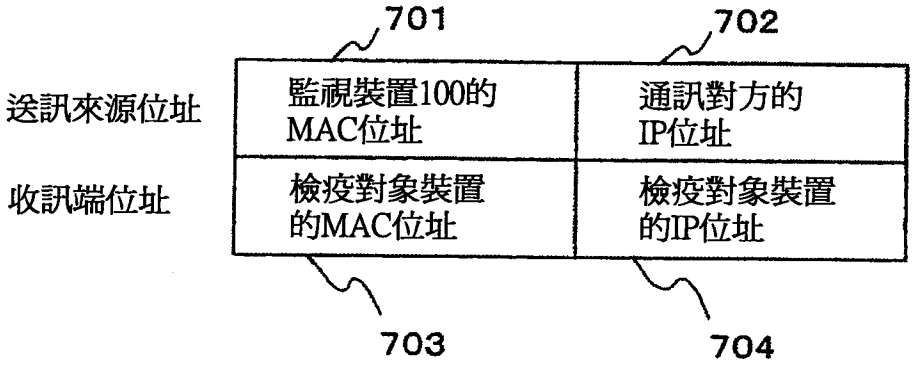

# 圖6

不正當裝置排除用ARP回應b




# 圖7

不正當裝置排除用ARP回應c



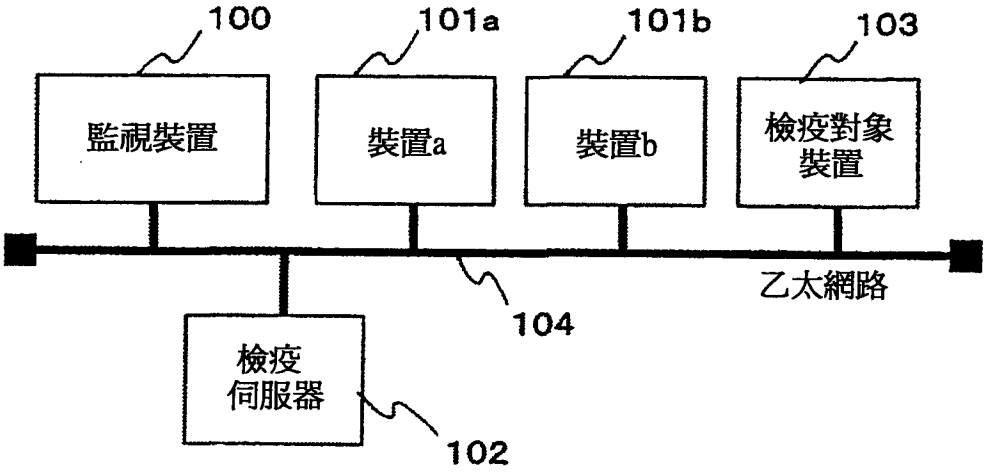
# 圖8

連接可否資訊表205的構成

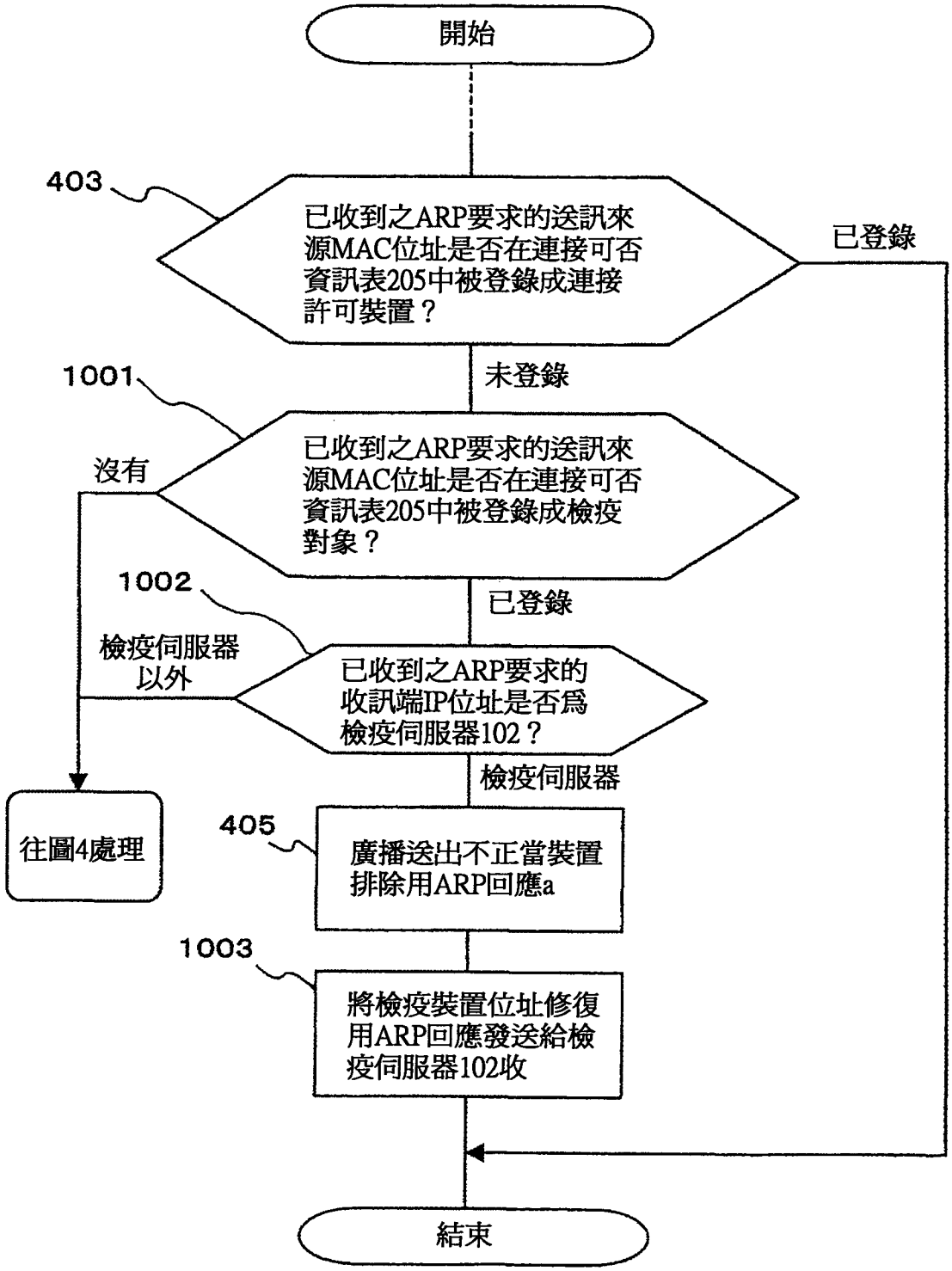
| | MAC位址 | IP位址 | 狀態 |
|---|---|---|---|
| 裝置101a | MAC801 | IP804 | 連接許可 |
| 裝置101b | MAC802 | IP805 | 連接許可 |
| 檢疫對象裝置103 | MAC803 | IP806 | 檢疫對象 |

810 811 812

# 圖9

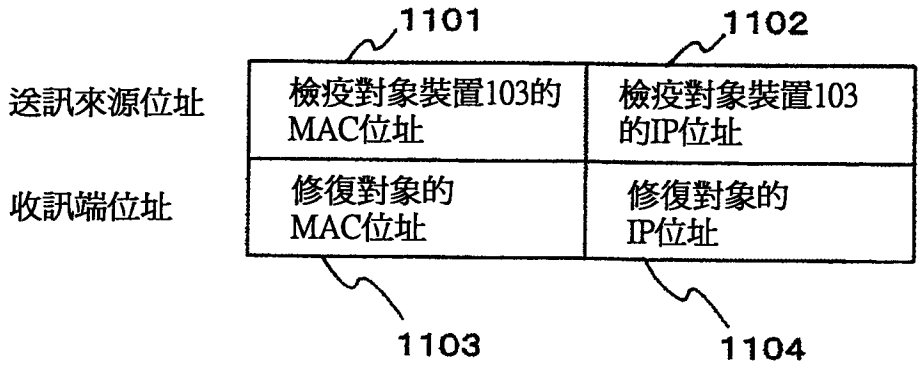


# 圖10

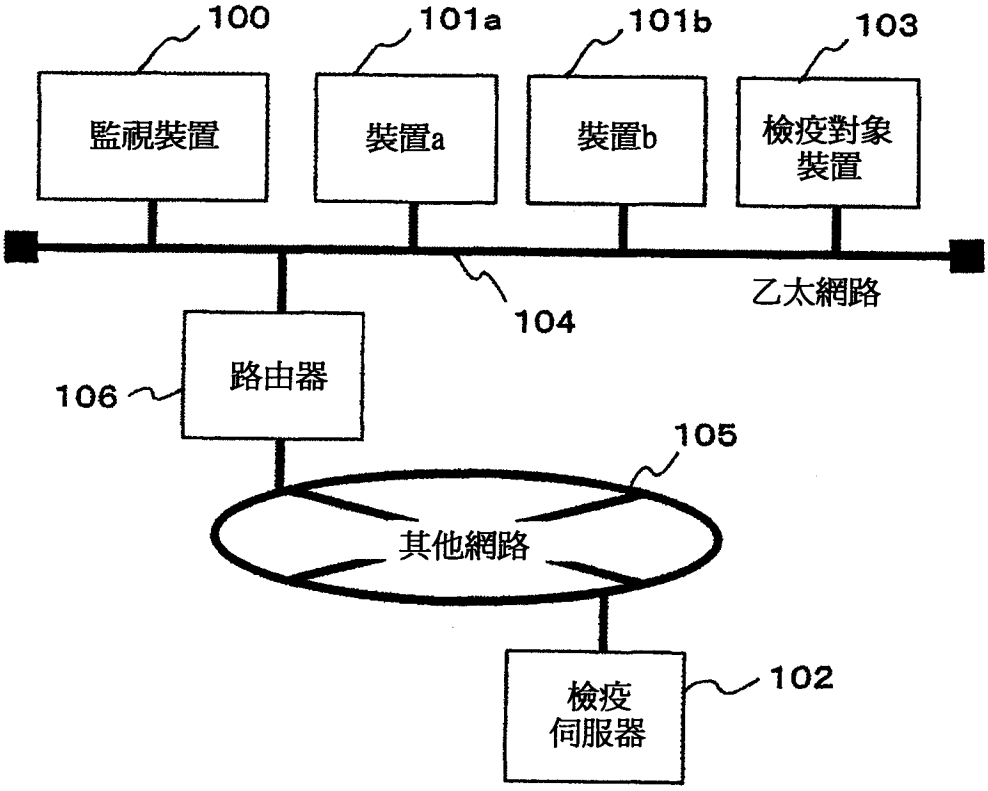

開始
403
已收到之ARP要求的送訊來源MAC位址是否在連接可否資訊表205中被登錄成連接許可裝置？
已登錄
未登錄
1001
已收到之ARP要求的送訊來源MAC位址是否在連接可否資訊表205中被登錄成檢疫對象？
沒有
已登錄
1002
檢疫伺服器以外
已收到之ARP要求的收訊端IP位址是否爲檢疫伺服器102？
檢疫伺服器
往圖4處理
405
廣播送出不正當裝置排除用ARP回應a
1003
將檢疫裝置位址修復用ARP回應發送給檢疫伺服器102收
結束

# 圖11

檢疫裝置位址修復用ARP回應




# 圖12



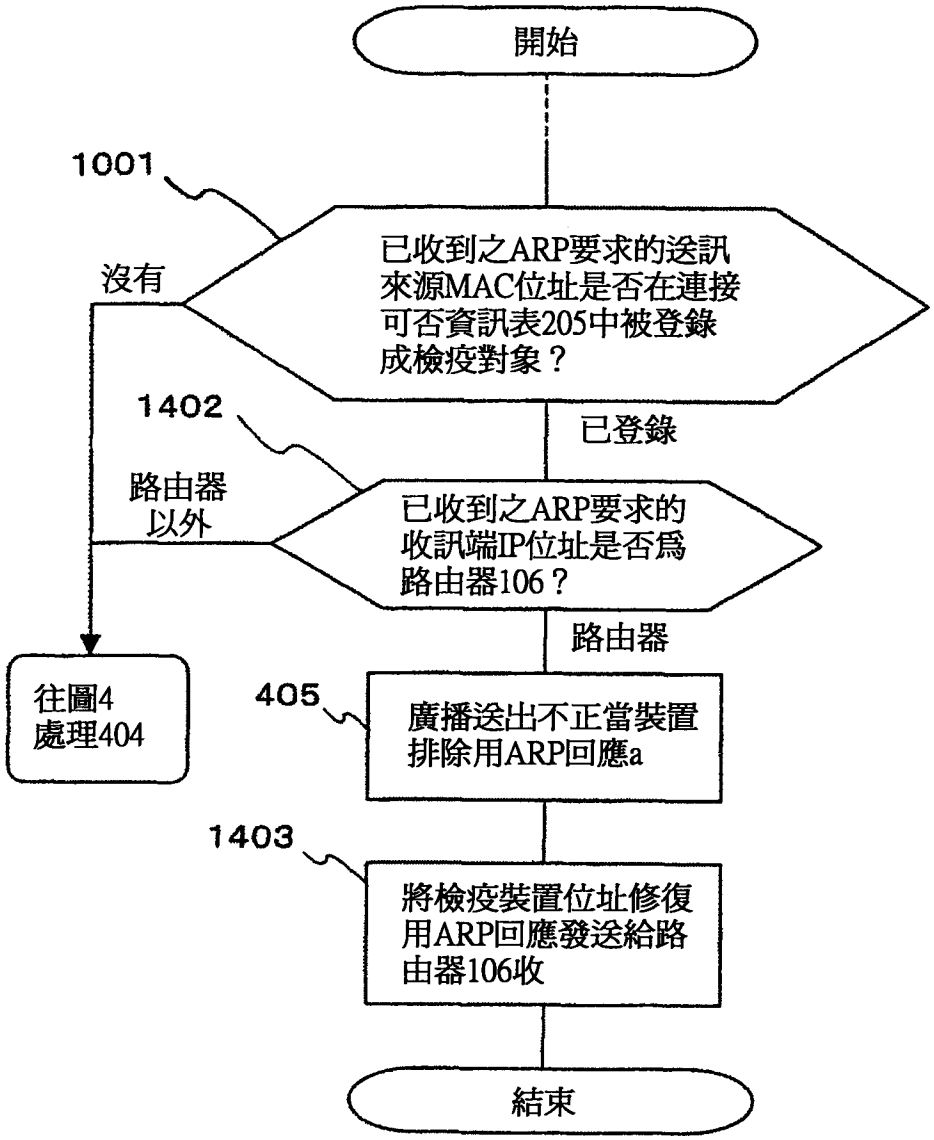
# 圖13

路由器106的過濾設定表

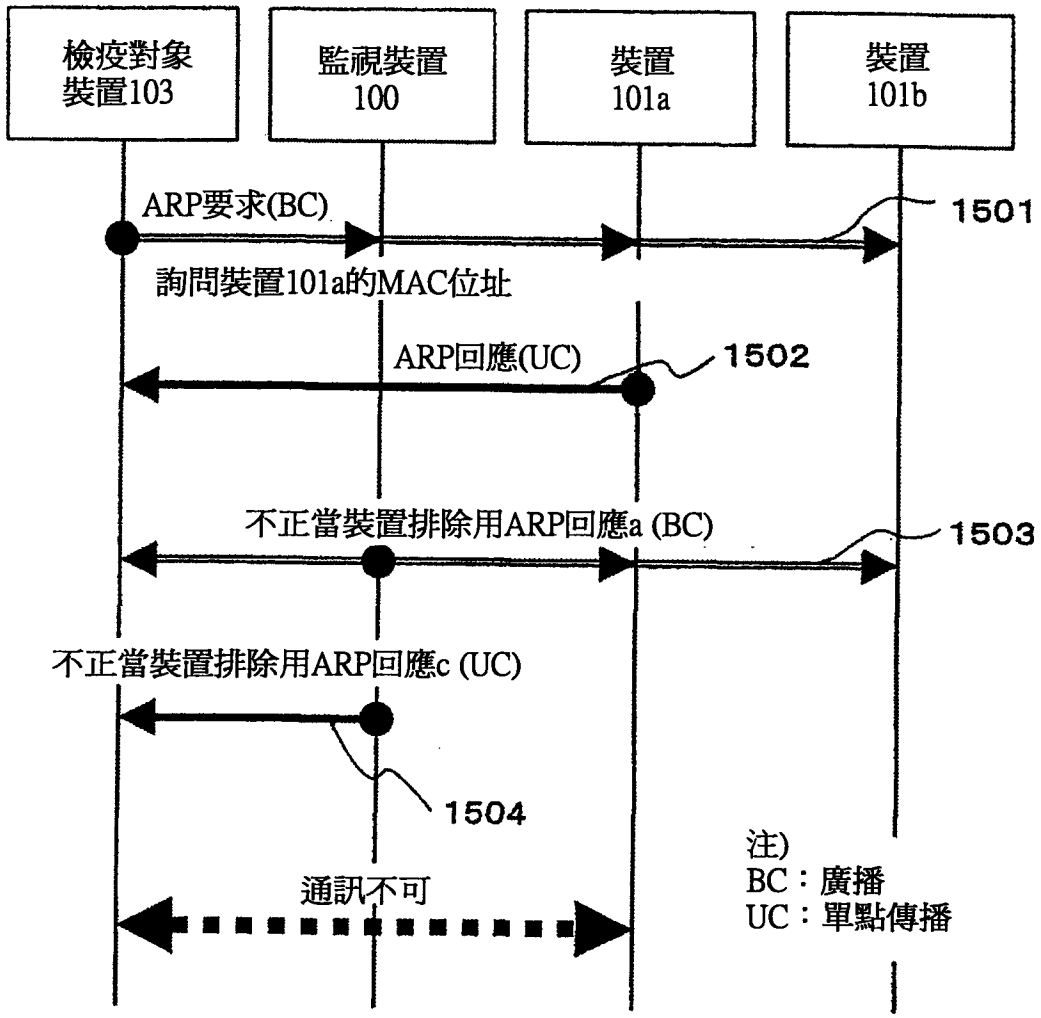
1301

| 送訊來源IP位址 (1302) | 收訊端IP位址 (1303) | 動作 (1304) |
|---|---|---|
| 檢疫對象裝置 103a | 檢疫伺服器以外 | 丟棄 |
| 檢疫對象裝置 103b | 檢疫伺服器以外 | 丟棄 |
| 檢疫對象裝置 103c | 檢疫伺服器以外 | 丟棄 |

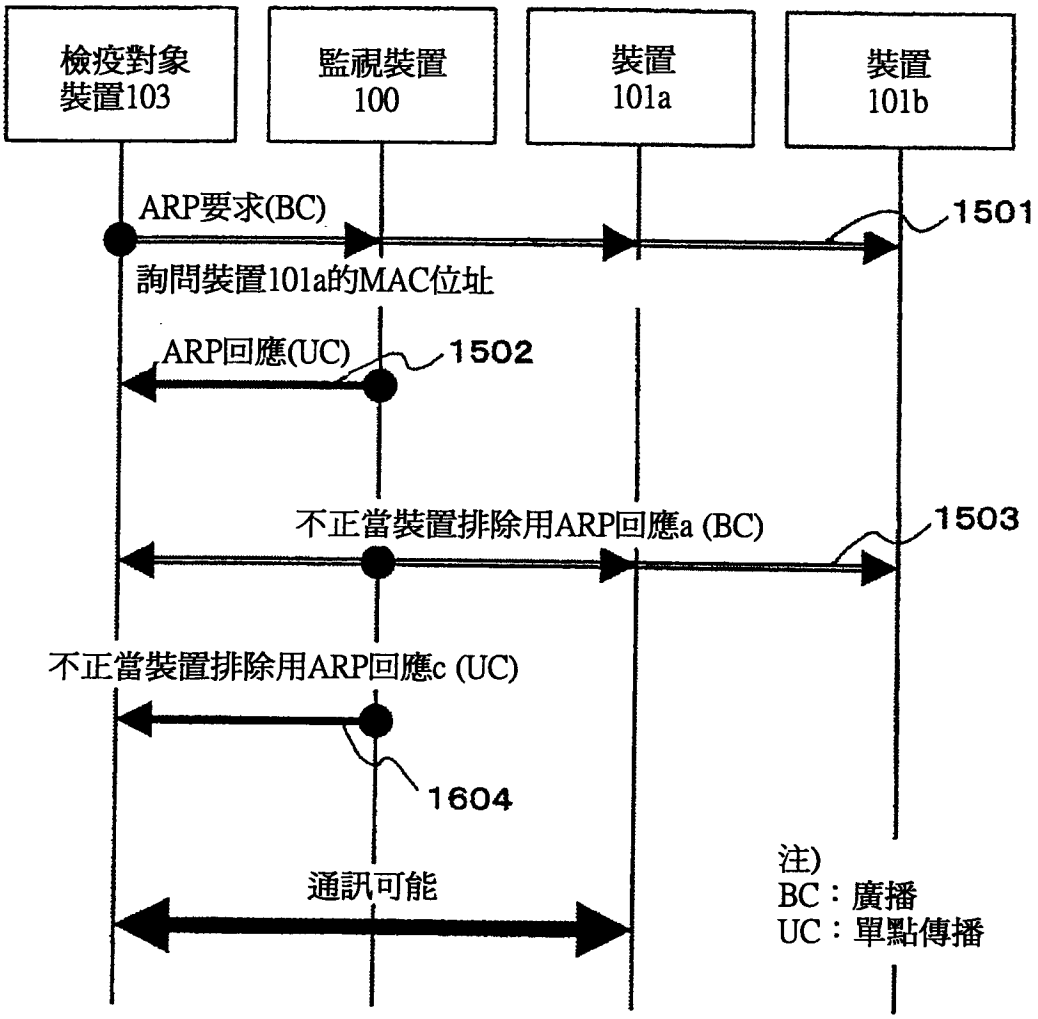
# 圖14


開始
1001
已收到之ARP要求的送訊來源MAC位址是否在連接可否資訊表205中被登錄成檢疫對象？
沒有
已登錄
1402
路由器以外
已收到之ARP要求的收訊端IP位址是否爲路由器106？
路由器
往圖4處理404
405
廣播送出不正當裝置排除用ARP回應a
1403
將檢疫裝置位址修復用ARP回應發送給路由器106收
結束

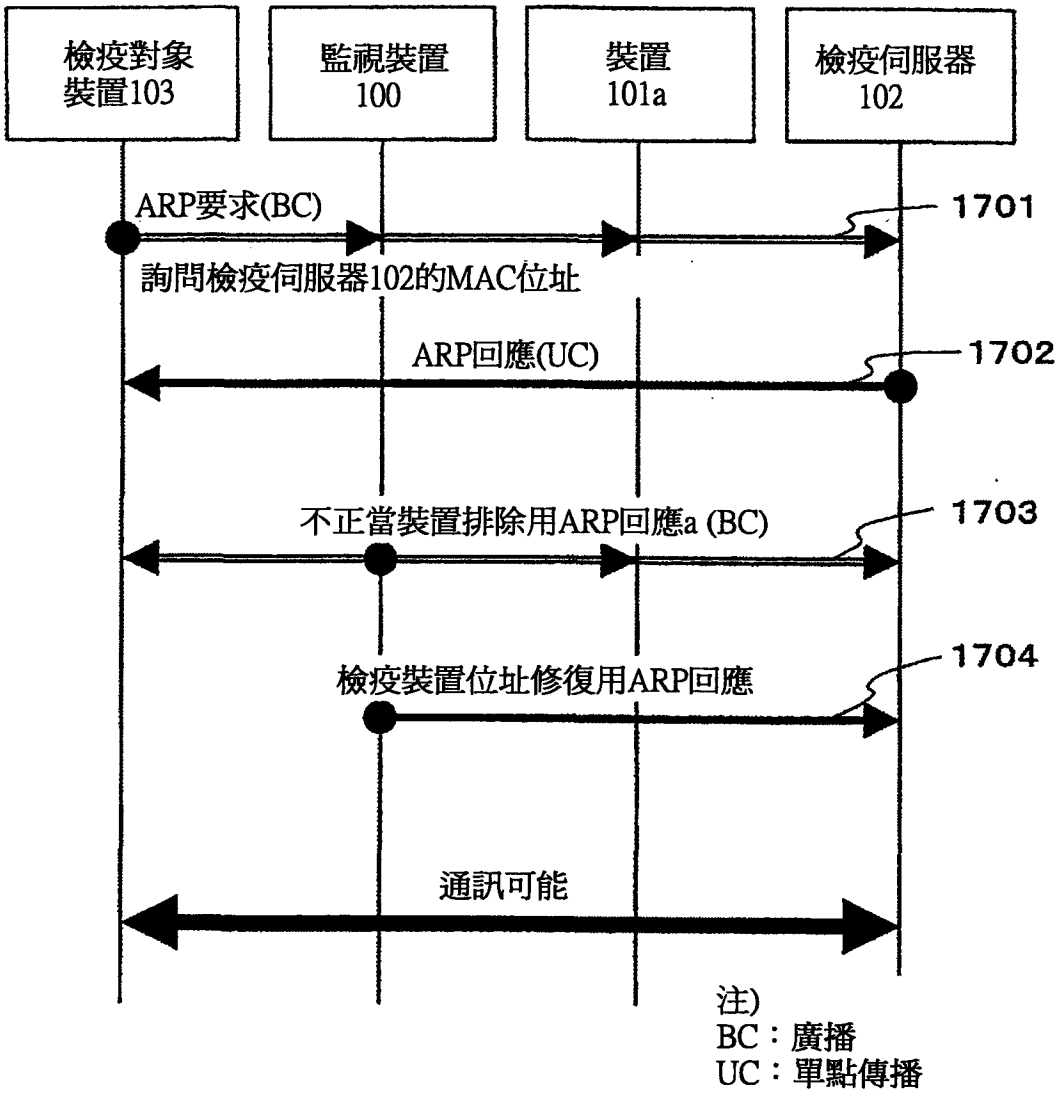
# 圖15


檢疫對象
裝置103
監視裝置
100
裝置
101a
裝置
101b
ARP要求(BC)
1501
詢問裝置101a的MAC位址
ARP回應(UC)
1502
不正當裝置排除用ARP回應a (BC)
1503
不正當裝置排除用ARP回應c (UC)
1504
通訊不可
注)
BC：廣播
UC：單點傳播

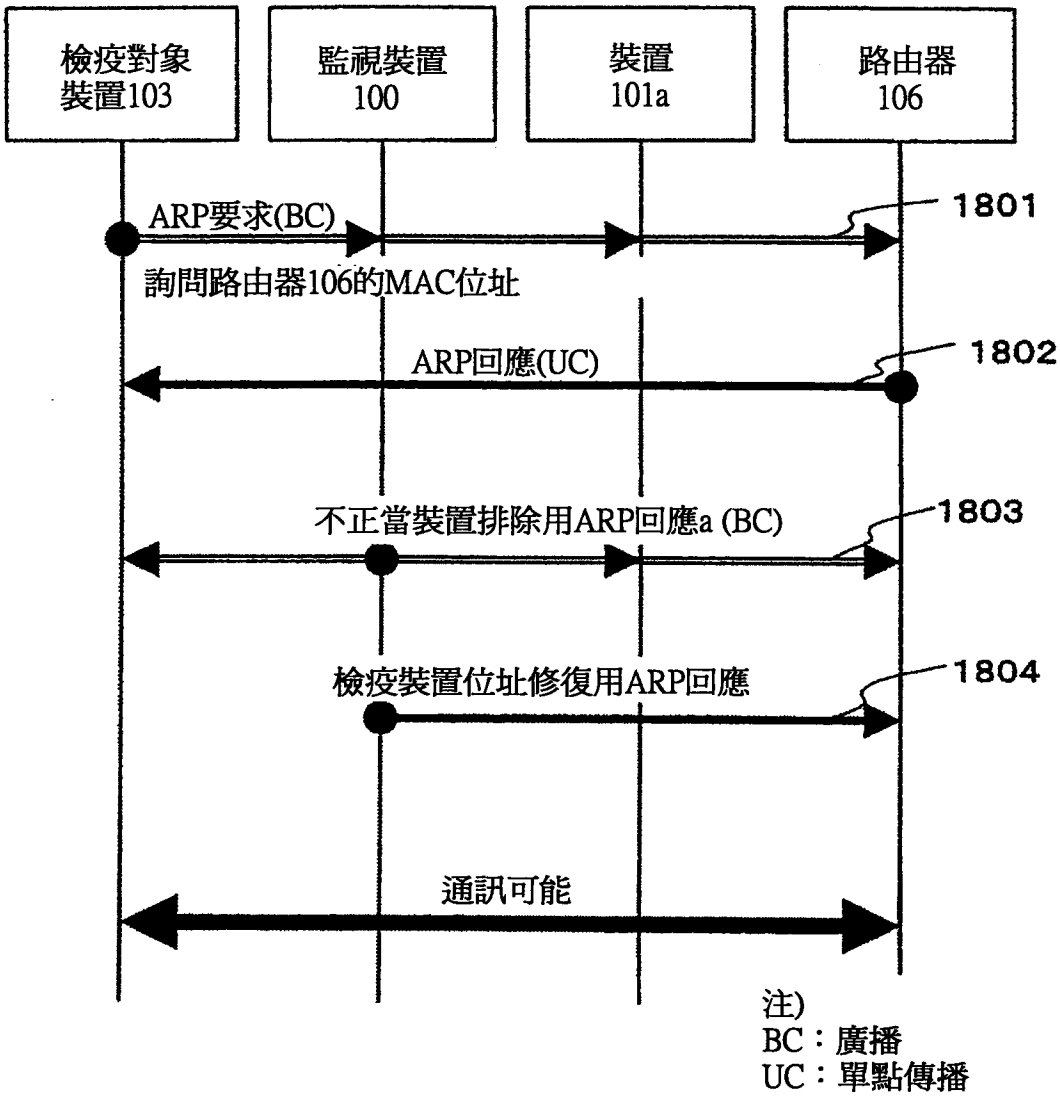
# 圖16


檢疫對象
裝置103
監視裝置
100
裝置
101a
裝置
101b
ARP要求(BC)
1501
詢問裝置101a的MAC位址
ARP回應(UC)
1502
不正當裝置排除用ARP回應a (BC)
1503
不正當裝置排除用ARP回應c (UC)
1604
通訊可能
注)
BC：廣播
UC：單點傳播

# 圖17


檢疫對象
裝置103
監視裝置
100
裝置
101a
檢疫伺服器
102
ARP要求(BC)
1701
詢問檢疫伺服器102的MAC位址
ARP回應(UC)
1702
不正當裝置排除用ARP回應a (BC)
1703
檢疫裝置位址修復用ARP回應
1704
通訊可能
注)
BC：廣播
UC：單點傳播

# 圖18


檢疫對象
裝置103
監視裝置
100
裝置
101a
路由器
106
ARP要求(BC)
1801
詢問路由器106的MAC位址
ARP回應(UC)
1802
不正當裝置排除用ARP回應a (BC)
1803
檢疫裝置位址修復用ARP回應
1804
通訊可能
注)
BC：廣播
UC：單點傳播

七、指定代表圖

（一）、本案指定代表圖為：第（2）圖

（二）、本代表圖之元件代表符號簡單說明：

100：監視裝置
104：乙太網路
201：訊框收訊處理部
202：訊框送訊處理部
203：OS/防毒軟體的更新資料保存部
204：連接可否判斷處理部
205：連接可否資訊表
206：ARP回應訊框生成部

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：