

發明專利說明書

(本申請書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

識別代理 IP 位址的方法及裝置

【技術領域】

本發明涉及網際網路技術領域，尤其涉及一種識別代理 IP 位址的方法及裝置。

【先前技術】

目前，網際網路上存在一種廣泛的應用，即，IP 位址與地理位置互查技術，該技術廣泛應用於網際網路各個領域，尤其是風險控制領域，作為一個強風險因數而被使用。也即是說，該互查技術在風險控制領域的方案所應用的原理是：檢測一個用戶是否短時間內在不同的地理位置登錄，如果是，則可以認為是一個高風險操作。這個判斷是基於用戶的 IP 是真實 IP 才成立的。但代理伺服器技術打破了這一應用的前提。也就是說一個北京的使用者完全可以透過杭州的代理伺服器，則伺服器看到的用戶 IP 位址則為杭州代理伺服器的位址，本發明主要就是識別這種情況，區分出使用者是否使用代理伺服器。也即是說，檢查一個 IP 位址是位於一個地理位置處的終端的真實 IP 位址，還是一個代理伺服器的 IP 位址，例如一個 VPN 代理伺服器的 IP 位址。

本問題一直在網際網路領域中被討論，本領域也有針對該類問題的一些解決方案，但是這些解決方案主要還是集中在兩個方向：1、代理伺服器庫的收集，有基於爬蟲從網際網路上抓取的，還有基於主動掃描的代理伺服器收集。2、基於反向探測，反向掃描目前網際網路上的所有主機，判斷知名的代理埠是否開放。第一種思路下的方案，代理伺服器庫的收集，針對基於爬蟲從網際網路上抓取的方式，有很多代理伺服器是未在網際網路上公佈的，或者是駭客控制的一些肉機，此資訊非常的不完全。第二種思路下的方案，基於反向探測，原理就是反向掃描所有的 IP，判斷一些常用的代理埠是否開放。但是網際網路上活躍主機量非常巨大，而且代理伺服器的服務埠不固定，故此方案掃描週期非常長。

因此，目前需要一種能夠快速準確地識別 IP 位址是否為代理 IP 位址的方法。

【發明內容】

本發明的主要目的在於提供一種識別 IP 位址的方法，以解決現有技術存在的上述問題，其中：

本發明提供一種識別代理 IP 位址的方法，其特徵在於，包括：確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時；確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時；判斷第一網路延時與第二網路延時之比是否大於閾

值；如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。

本發明的另一方面提供了一種識別代理 IP 位址的裝置，其特徵在於，包括：第一確定模組，用於確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時；第二確定模組，用於確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時；判斷模組，用於判斷第一網路延時與第二網路延時之比是否大於閾值；識別模組，用於如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。

與現有技術相比，根據本發明的技術方案，透過確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時與伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址，從而能夠快速準確地識別代理 IP 位址。

【圖式簡單說明】

此處所說明的圖式用來提供對本發明的進一步理解，構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在圖式中：

圖 1 是本發明實施例的一種識別代理 IP 位址的方法

的流程圖；

圖 2 是本發明實施例的識別代理 IP 位址的方法中確定第一網路延時的流程圖；

圖 3 是本發明實施例的識別代理 IP 位址的方法中確定第一網路延時的流程圖；

圖 4a 是本發明實施例的終端透過網路直接連接伺服器的示意圖；

圖 4b 是本發明實施例的終端透過網路經由代理間接地連接伺服器的示意圖；以及

圖 5 是本發明實施例的一種識別代理 IP 位址的裝置的結構方塊圖。

【實施方式】

本發明的主要思想在於，透過確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時，並且確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時，從而判斷第一網路延時與第二網路延時之比是否大於閾值，如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的圖式對本發明技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本發明一部分實施例，而不是全部的實施例。基於本發明中的

實施例，本領域普通技術人員在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

根據本發明的實施例，提供了一種識別代理 IP 位址的方法。

參考圖 1，圖 1 是本發明實施例的一種識別代理 IP 位址的方法的流程圖，如圖 1 所示，在步驟 S101 處，確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時。

具體而言，為了識別一個 IP 位址是否為代理 IP 位址，首先需要獲取伺服器與以該 IP 位址作為自己的用戶 IP 位址而試圖與伺服器建立 TCP 連接的那個真實終端之間的第一網路延時。

下面我們參考圖 2 來詳細地描述可以如何獲取該第一網路延時的一種方法實施例的流程圖。

為了更清楚地理解該第一網路延時的含義，我們首先介紹一下終端與伺服器為了建立 TCP 連接而進行三次握手的過程。所謂三次握手（Three-way Handshake），是指建立一個 TCP 連接時，需要用戶端和伺服器總共發送 3 個封包（packet）。三次握手的目的是連接伺服器指定埠，建立 TCP 連接。第一次握手：終端發送一個帶 SYN（同步序列編號 Synchronize Sequence Numbers）標誌的 TCP 封包到伺服器，這是三次握手過程中的封包 1，在本發明中稱為 SYN 封包。第二次握手：伺服器端回應終端，發送一個 SYN-ACK 封包給終端，這是三次握手中的

第 2 個封包，這個封包同時帶 ACK 標誌和 SYN 標誌。因此它表示對剛才用戶端 SYN 封包的回應；同時又標誌 SYN 給用戶端，詢問用戶端是否準備好進行資料通信。第三次握手：終端必須再次回應伺服器一個 ACK 封包（即是三次握手的確認封包），這是封包段 3，表示終端準備好進行資料通信。透過三次握手，TCP 連接建立。本發明利用了終端與伺服器之間建立 TCP 連接的這個三次握手過程，從而可以獲得伺服器發送 SYN-ACK 封包與接收到終端回覆的 ACK 封包之間的第一網路延時。下面，描述如何獲取第一網路延時的具體步驟。

伺服器接收來自以該 IP 地址為用戶 IP 地址的所述終端的 SYN 封包，該終端請求建立 TCP 連接。伺服器接收到該 SYN 封包之後，向所述終端發送 SYN-ACK 封包。因此，如圖 2 所示，在步驟 201 處，伺服器記錄向所述終端發送 SYN-ACK 封包的時刻，例如可以將該時刻定義為第一時刻。

然後伺服器接收到來自該終端的 ACK 封包，因此，在步驟 202 處，伺服器記錄接收到來自所述終端的 ACK 封包的時刻，例如可以將該時刻定義為第二時刻。

最後，在步驟 203 處，將向所述終端發送 SYN-ACK 封包的時刻與接收到來自所述終端的 ACK 封包的時刻之間的時間差確定為第一網路延時。也即是說，將第二時刻與第一時刻的時間差確定為第一網路延時。

透過上述方法步驟，就可以獲知伺服器與該終端之間

的第一網路延時。

返回圖 1，在確定了第一網路延時之後，接下來在步驟 102 處，確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時。

該第二網路延時的獲取是基於如下原理。

服務端可以記錄使用者 IP 位址為 ip1，服務端可以構建多個（例如 255 個）生存時間（ttl）分別為 1 至 255、且目標 IP 為 ip1 的一系列探測封包。根據 TCP/IP 協定，這一系列探測封包每經過一條路由器，則 ttl 將會減 1，當封包 ttl 被減為 0 且還沒到達目標位址時，此時路由器報錯，發送一個 ICMP（網際網路控制訊息協定）差錯封包給發送方，從而可以知道最後一個 ICMP 差錯封包即為該 IP 位址的上一跳路由器發送的。因此，利用該這一系列探測封包，可以分析出用戶上一級路由的位址和網路延時。

下面我們參考圖 3 來詳細地描述可以如何獲取該第二網路延時的一種方法實施例的流程圖。

如上所述，伺服器構建並發送具有遞增生存時間、目標位址為所述使用者 IP 地址的一系列探測封包。如上所述，例如可以構建並發送 255 個遞增生存時間為 1-255、目標 IP 為上述使用者 IP 位址的一系列探測封包。從而如圖 3 所示，在步驟 301 處，可以記錄一系列探測封包中的每個探測封包的發送時刻。

接下來，基於該一系列探測封包獲取所述 IP 位址的

上一跳路由器向伺服器發送的 ICMP 差錯封包。如上所述，例如，當這一系列探測封包中生存時間為 1 的探測封包到達為第一個路由器時，由於還沒有到達所述 IP 位址，所以產生並發送第一個 ICMP 差錯封包，並被伺服器接收，記錄第一個差錯封包接收時刻；如此類推，例如當這一系列探測封包中生存時間為 n 的封包到達為第 n 個路由器時，由於還沒有到達所述 IP 位址，所以產生並發送第 n 個 ICMP 差錯封包，並被伺服器接收，記錄第 n 個差錯封包接收時刻；當這一系列探測封包中生存時間為 $n+1$ 的封包到達為所述 IP 位址，所以不產生 ICMP 差錯封包。從而伺服器知曉該第 n 個路由器為該 IP 地址的上一跳路由器，從而將該第 n 個差錯封包接收時刻記錄為接收到所述 IP 位址的上一跳路由器向伺服器發送的 ICMP 差錯封包的時刻。也即是說，在步驟 302 處，記錄接收到所述 IP 位址的上一跳路由器向伺服器發送的 ICMP 差錯封包的時刻，例如，將該時刻定義為第四時刻。

然後在步驟 303 處，將一系列探測封包中與所述 ICMP 差錯封包相對應的那個探測封包的發送時刻記錄為第三時刻。具體而言，可以查找到與該 ICMP 差錯封包相應的探測封包，從而知曉該相應的那個探測封包的發送時刻，並將該探測封包的發送時刻定義為第三時刻。

然後，在步驟 304 處，將接收到來自所述 IP 位址的上一跳路由器的 ICMP 差錯封包的時刻與所述一系列探測封包中的、與該 ICMP 差錯封包相對應的那個探測封包的

發送時刻之間的時間差確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時。

也即是說，將第四時刻與第三時刻的時間差確定為第二網路延時。

下面，返回圖 1，在確定了第一網路延時和第二網路延時之後，在步驟 103 處，判斷第一網路延時與第二網路延時之比是否大於閾值。

正常情況下，如果終端沒有採用代理 IP 位址而在網路上利用終端的使用者 IP 位址直接連接伺服器的情況下，終端和服務端之間的第一網路延時 $T1$ 和的該使用者 IP 位址（終端 IP 位址）的上一跳路由器 $R1$ 與伺服器之間的第二網路延時 $T2$ 數值近似。從而 $T1$ 與 $T2$ 之比近似為 1。

但是如果使用者使用任何一種代理伺服器，則伺服器一端所探測到的所謂“用戶 IP 位址”的都是代理伺服器的代理 IP 位址。從而確定的第二網路延時是伺服器與該所謂的“用戶 IP 位址”（實際上為代理伺服器的代理 IP 位址）的上一跳路由器之間的網路延時 $T2'$ 。 $T2'$ 和 $T1$ 之間的差異較大，從而 $T1$ 與 $T2'$ 之比通常大於一個閾值，例如，將該閾值設置為 2。應該理解，可以根據實際需要設置適當的閾值。

在步驟 104 處，如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。

也即是說，如果第一網路延時與第二網路延時之比大

於閾值，則由於二者差異較大，所以可以判斷該 IP 位址應該不是終端的 IP 位址，終端使用了代理伺服器的代理 IP 位址接入該伺服器，因此將所述 IP 位址識別為代理 IP 位址。可選地，在本發明中，代理伺服器可以是 VPN 代理伺服器，所述代理 IP 位址可以是 VPN 代理 IP 位址。

在步驟 105 處，如果第一網路延時與第二網路延時之比小於等於閾值，則將所述 IP 位址識別為非代理 IP 位址。

也即是說，如果第一網路延時與第二網路延時之比小於等於閾值，則由於二者差異不大，所以可以判斷該 IP 位址應該是終端的 IP 位址，終端沒有使用代理 IP 位址接入該伺服器，因此將所述 IP 位址識別為非代理 IP 位址。

為了更清楚地描述本發明實施例的技術方案，下面將參考圖 4a 和圖 4b 進行更詳細的說明。

例如，如圖 4a 所示，例如位於某地 A 的終端使用者（第一終端）發出 SYN 封包，該 SYN 封包例如經由該終端使用者的例如社區接入路由器 R1，然後經過例如某地 A 的骨幹網出口——路由器 R2，經過例如某地 B 的骨幹網出口——路由器 R3，最後到達伺服器，被伺服器接收到該 SYN 封包。也即是說，伺服器接收到來自以第一 IP 位址為用戶 IP 位址試圖與伺服器建立 TCP 連接的第一終端的 SYN 封包。伺服器向該第一終端發送 SYN-ACK 封包，並記錄下向第一終端發送 SYN-ACK 封包的第一時刻 Time1。接下來，伺服器接收到來自該第一終端的 ACK 封

包，伺服器記錄下接收到來自該第一終端的 ACK 封包的第二時刻 Time2 。從而確定第一網路延時為 $T1 = \text{Time2} - \text{Time1}$ 。從圖 4a 可以看出，網路延時 $T1$ 包含了伺服器與路由器 R3 之間的延時、路由器 R3 與 R2 之間的延時、路由器 R2 與 R1 之間的延時、路由器 R1 與第一終端之間的延時。

另外，伺服器例如可以構建並發送 255 個生存時間 ttl 為 1-255、目標 IP 位址為該第一 IP 位址的一系列探測封包，從而伺服器可以記錄下這一系列探測封包中每個探測封包的發送時刻；並且如上所述，伺服器還可以記錄接收到該第一 IP 位址（第一終端的 IP 位址）的上一跳路由器發送的 ICMP 差錯封包的第四時刻 Time4 。並且，基於該 ICMP 差錯封包，還可以找到其相應的探測封包，從而知曉該相應的那個探測封包的發送時刻，也即是說，例如將一系列探測封包中與所述 ICMP 差錯封包相對應的那個探測封包的發送時刻定義為第三時刻 Time3 。從而確定第二網路延時為 $T2 = \text{Time4} - \text{Time3}$ 。從圖 4a 可以看出，網路延時 $T2$ 包含了伺服器與路由器 R3 之間的延時、路由器 R3 與 R2 之間的延時、路由器 R2 與 R1 之間的延時。也即是說 $T1$ 與 $T2$ 之間的差別僅僅是路由器與第一終端之間的延時，差別較小。

從圖中可以看出，由於第一 IP 位址為第一終端的真實位址，所以確定得到的 $T1$ 與 $T2$ 的數值相近，從而 $T1$ 與 $T2$ 之比沒有大於閾值，從而可以確定該第一 IP 位

址不是代理 IP 位址。透過本發明的技術方案，可以看出，識別結果與實際結果相符。

同樣，如圖 4b 所示，如果第一終端以代理接入一伺服器，則位於某地 A 的終端使用者（第一終端）發出 SYN 封包，該 SYN 封包經由該終端使用者的例如社區接入路由器 R1，然後經過例如某地 A 的骨幹網出口——路由器 R2，經過例如某地 B 的骨幹網出口——路由器 R3，經過代理，經由該代理的例如社區接入路由器 R4，再經過例如某地 C 的骨幹網出口——路由器 R5，經過例如某地 D 的骨幹網出口——路由器 R6，最終到達伺服器，被伺服器接收到該 SYN 封包。也即是說，伺服器接收到以第二 IP 位址（代理 IP 位址）為使用者 IP 位址試圖與伺服器建立 TCP 連接的第一終端的 SYN 封包，伺服器向該第一終端發送 SYN-ACK 封包，並記錄下向第一終端發送 SYN-ACK 封包的第一時刻 $Time1'$ 。接下來，伺服器接收到來自該第一終端的 ACK 封包，伺服器記錄下接收到來自該第一終端的 ACK 封包的第二時刻 $Time2'$ 。從而確定第一網路延時為 $T1' = Time2' - Time1'$ 。從圖 4b 可以看出，由於使用了代理，網路延時 $T1'$ 包含了伺服器與路由器 R6 之間的延時、路由器 R6 與 R5 之間的延時、路由器 R5 與 R4 之間的延時、路由器 R4 與代理之間的延時、代理與路由器 R3 之間的延時、路由器 R3 與 R2 之間的延時、路由器 R2 與 R1 之間的延時、路由器 R1 與第一終端之間的延時。

另外，伺服器例如可以構建並發送 255 個生存時間 ttl 為 1-255、目標 IP 位址為該第二 IP 位址的一系列探測封包，從而伺服器可以記錄下發送這一系列探測封包中每個探測封包的發送時刻；並且如上所述，伺服器還可以記錄接收到該第二 IP 位址（代理伺服器而非第二終端的 IP 位址）的上一跳路由器發送的 ICMP 差錯封包的第四時刻 Time4'。並且，基於該 ICMP 差錯封包，還可以找到其相應的探測封包，從而知曉該相應的那個探測封包的發送時刻，也即是說，例如將一系列探測封包中與所述 ICMP 差錯封包相對應的那個探測封包的發送時刻定義為第三時刻 Time3'。從而確定第二網路延時為 $T2' = \text{Time4}' - \text{Time3}'$ 。從圖 4b 可以看出，由於使用了代理，所以第二 IP 位址（代理 IP 位址）的上一跳路由器不再是路由器 R1 而是變成了路由器 R4，因此網路延時 T2' 包含了伺服器與路由器 R6 之間的延時、路由器 R6 與 R5 之間的延時、路由器 R5 與 R4 之間的延時。也即是說 T1' 與 T2' 之間的差別是路由器 R4 與代理之間的延時、代理與路由器 R3 之間的延時、路由器 R3 與 R2 之間的延時、路由器 R2 與 R1 之間的延時、路由器 R1 與第一終端之間的延時，差別很大。

從圖 4b 中可以看出，由於第二 IP 位址不是第一終端的真真實位址，第一網路延時 T1' 遠大於 T2'。從而 T1' 與 T2' 之比大於閾值，從而可以確定該第二 IP 位址是代理 IP 位址而非第一終端的 IP 位址。透過本發明的技術方案，可以看出，識別結果與實際結果相符。

上面透過圖 1 至圖 4b 描述了根據本發明實施例的識別代理 IP 位址的方法。

本發明還提供了一種識別代理 IP 位址的裝置。

圖 5 示意性地示出了根據本發明一個實施例的識別代理 IP 位址的裝置的結構方塊圖。根據本發明的一個實施例，該裝置 500 可以包括：第一確定模組 501、第二確定模組 502、判斷模組 503 以及識別模組 504。

根據本發明的實施例，第一確定模組 501 可以用於確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時。

第二確定模組 502 可以用於確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時。

判斷模組 503 可以用於判斷第一網路延時與第二網路延時之比是否大於閾值。

識別模組 504 可以用於如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。

此外，識別模組 504 可以用於如果第一網路延時與第二網路延時之比小於或等於閾值，則將所述 IP 位址識別為非代理 IP 位址。

根據本發明的實施例，第一確定模組 501 可以進一步被配置成：將向所述終端發送 SYN-ACK 封包的時刻與接收到來自所述終端的 ACK 封包的時刻之間的時間差確定為第一網路延時。

具體而言，所述第一確定模組 501 可以進一步包括：第一記錄子模組，其可以用於記錄向所述終端發送 SYN-ACK 封包的第一時刻；第二記錄子模組，其可以用於記錄接收到來自所述終端的 ACK 封包的第二時刻；以及第一確定子模組，其可以用於將第二時刻與第一時刻的時間差確定為第一網路延時。

根據本發明的實施例，第二確定模組 502 可以進一步被配置成：將接收到來自所述 IP 位址的上一跳路由器的 ICMP 差錯封包的時刻與一系列探測封包中與所述 ICMP 差錯封包相對應的那個探測封包的發送時刻之間的時間差確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時，其中，所述一系列探測封包具有遞增生存時間，並且其目標位址為所述使用者 IP 位址。

具體而言，所述第二確定模組可以進一步包括：第三記錄子模組，其可以用於記錄所述一系列封包中的每個探測封包的發送時刻；第四記錄子模組，其可以用於記錄接收到來自所述 IP 位址的上一跳路由器的 ICMP 差錯封包的第四時刻；第一定義子模組，用於將一系列探測封包中與所述 ICMP 差錯封包相對應的那個探測封包的發送時刻定義為第三時刻；第二確定子模組，其可以用於將第四時刻與第三時刻的時間差確定為第二網路延時。

由於本實施例的裝置所實現的功能基本相應於前述圖 1 至圖 4b 所示的方法實施例，故本實施例的描述中未詳盡之處，可以參見前述實施例中的相關說明，在此不做贅

述。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀取媒體中的非永久性記憶體，隨機存取記憶體（RAM）和/或非易失性記憶體等形式，如唯讀記憶體（ROM）或快閃記憶體（flash RAM）。記憶體是電腦可讀取媒體的示例。

電腦可讀取媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀取指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體（PRAM）、靜態隨機存取記憶體（SRAM）、動態隨機存取記憶體（DRAM）、其他類型的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電可擦除可程式設計唯讀記憶體（EEPROM）、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體（CD-ROM）、數位多功能光碟（DVD）或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置或任何其他非傳輸媒體，可用於儲存可以被計算設備訪問的資訊。按照本文中的界定，電腦可讀取媒體不包括非暫存電腦可讀取媒體（transitory media），如調變的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且

還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域內的技術人員應明白，本發明的實施例可提供為方法、系統、或電腦程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

以上所述僅為本發明的實施例而已，並不用於限制本發明，對於本領域的技術人員來說，本發明可以有各種更改和變化。凡在本發明的精神和原則之內，所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍的範圍之內。

【符號說明】

500：裝置

501：第一確定模組

502：第二確定模組

503：判斷模組

504：識別模組

R1：路 由 器

R2：路 由 器

R3：路 由 器

R4：路 由 器

R5：路 由 器

R6：路 由 器

※申請案號：103118587

※申請日：103 年 05 月 28 日

※IPC 分類：H04L 12/741 (2013.01)
H04L 12/24 (2006.01)

【發明名稱】(中文/英文)

識別代理 IP 位址的方法及裝置

【中文】

本發明提供一種識別代理 IP 位址的方法和裝置，該方法包括：確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時；確定伺服器與所述 IP 位址的上一跳路由器之間的第二網路延時；判斷第一網路延時與第二網路延時之比是否大於閾值；如果第一網路延時與第二網路延時之比大於閾值，則將所述 IP 位址識別為代理 IP 位址。透過本發明的技術方案，能夠快速準確地識別一個 IP 位址是否為代理 IP 位址。

【英文】

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

圖 式

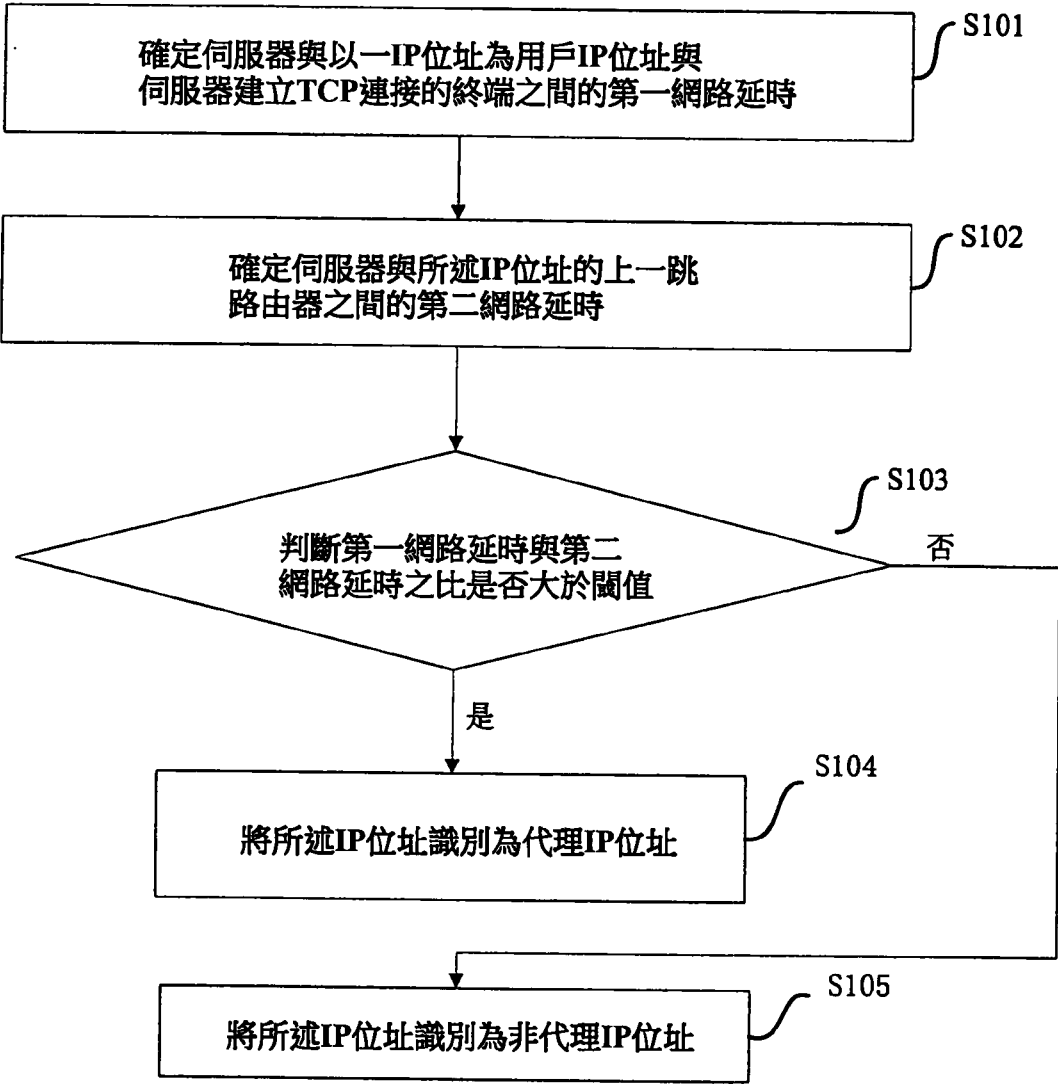


圖 1

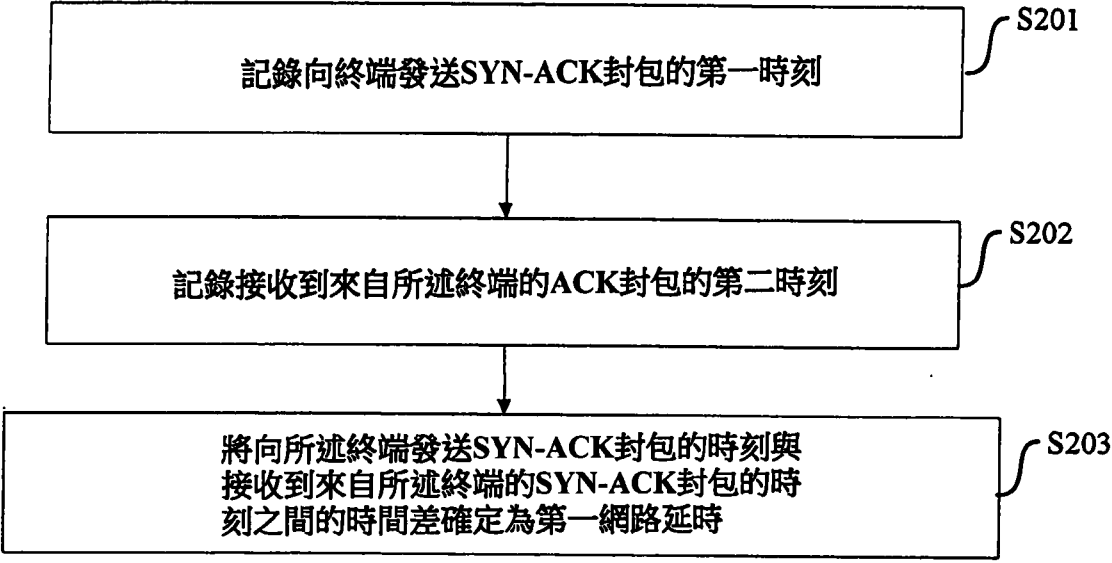


圖 2

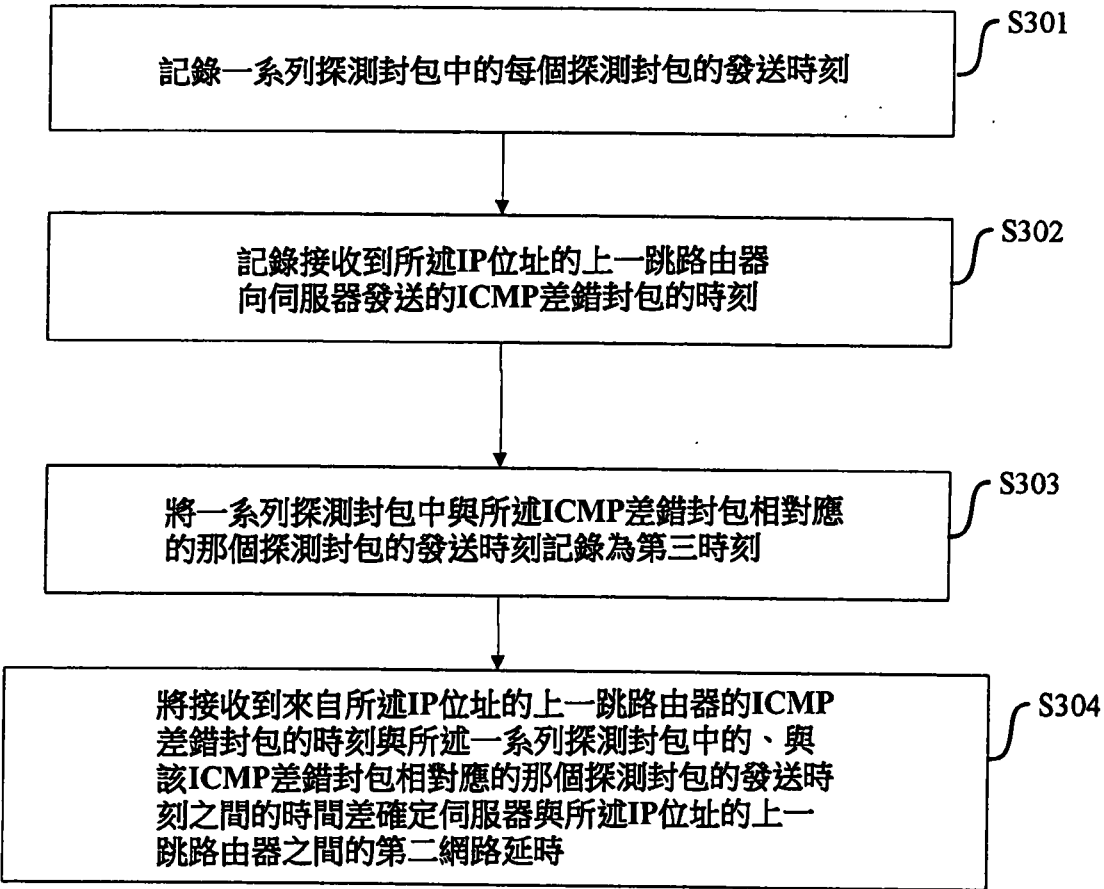


圖 3

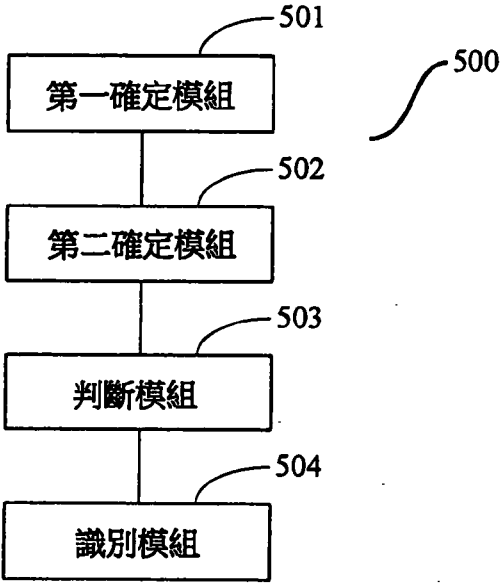


圖 5

申請專利範圍

1. 一種識別代理 IP 位址的方法，其特徵在於，包括：

確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時；

使用在該伺服器所接收到的 IP 位址，確定該伺服器與該 IP 位址的上一跳路由器之間的第二網路延時；

判斷第一網路延時與第二網路延時之比是否大於閾值；

如果第一網路延時與第二網路延時之比大於閾值，則將該 IP 位址識別為代理 IP 位址。

2. 根據申請專利範圍第 1 項的方法，其中，確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時的步驟，進一步包括：

將向該終端發送 SYN（同步序列編號）-ACK（確認）封包（packet）的時刻與接收到來自該終端的 ACK 封包的時刻之間的時間差確定為第一網路延時。

3. 根據申請專利範圍第 2 項的方法，其中，進一步包括：

記錄向該終端發送 SYN-ACK 封包的第一時刻；

記錄接收到來自該終端的 ACK 封包的第二時刻；並且

將第二時刻與第一時刻的時間差確定為第一網路延時。

4. 根據申請專利範圍第 1 至 3 項中任一項的方法，其中，確定伺服器與該 IP 位址的上一跳路由器之間的第二網路延時的步驟，進一步包括：

將接收到來自該 IP 位址的上一跳路由器的 ICMP（國際網路控制訊息協定）差錯封包的時刻與一系列探測封包中與該 ICMP 差錯封包相對應的那個探測封包的發送時刻之間的時間差確定伺服器與該 IP 位址的上一跳路由器之間的第二網路延時，其中，該一系列探測封包具有遞增生存時間，並且其目標位址為該使用者 IP 位址。

5. 根據申請專利範圍第 4 項的方法，其中，將接收到來自該 IP 位址的上一跳路由器的 ICMP 差錯封包的時刻與一系列探測封包中與該 ICMP 差錯封包相對應的那個探測封包的發送時刻之間的時間差確定伺服器與該 IP 位址的上一跳路由器之間的第二網路延時的步驟，進一步包括：

記錄該一系列探測封包中的每個探測封包的發送時刻；

記錄接收到來自該 IP 位址的上一跳路由器的 ICMP 差錯封包的第四時刻；

將一系列探測封包中與該 ICMP 差錯封包相對應的那個探測封包的發送時刻定義為第三時刻；

將第四時刻與第三時刻的時間差確定為第二網路延時。

6. 一種識別代理 IP 位址的裝置，其特徵在於，包

括：

第一確定模組，用於確定伺服器與以一 IP 位址為用戶 IP 位址與伺服器建立 TCP 連接的終端之間的第一網路延時；

第二確定模組，用於使用在該伺服器所接收到的 IP 位址，確定該伺服器與該 IP 位址的上一跳路由器之間的第二網路延時；

判斷模組，用於判斷第一網路延時與第二網路延時之比是否大於閾值；

識別模組，用於如果第一網路延時與第二網路延時之比大於閾值，則將該 IP 位址識別為代理 IP 位址。

7. 根據申請專利範圍第 6 項的裝置，其中，該第一確定模組進一步被配置成：

將向該終端發送 SYN（同步序列編號）-ACK（確認）封包的時刻與接收到來自該終端的 ACK 封包的時刻之間的時間差確定為第一網路延時。

8. 根據申請專利範圍第 7 項的裝置，其中，該第一確定模組進一步包括：

第一記錄子模組，用於記錄向該終端發送 SYN-ACK 封包的第一時刻；

第二記錄子模組，用於記錄接收到來自該終端的 ACK 封包的第二時刻；以及

第一確定子模組，用於將第二時刻與第一時刻的時間差確定為第一網路延時。

9. 根據申請專利範圍第 6 至 8 項中任一項的裝置，其中，該第二確定模組進一步被配置成：

將接收到來自該 IP 位址的上一跳路由器的 ICMP（國際網路控制訊息協定）差錯封包的時刻與一系列探測封包中與該 ICMP 差錯封包相對應的那個探測封包的發送時刻之間的時間差確定伺服器與該 IP 位址的上一跳路由器之間的第二網路延時，其中，該一系列探測封包具有遞增生時間，並且其目標位址為該使用者 IP 位址。

10. 根據申請專利範圍第 9 項的裝置，其中，該第二確定模組進一步包括：

第三記錄子模組，用於記錄該一系列探測封包中的每個探測封包的發送時刻；

第四記錄子模組，用於記錄接收到來自該 IP 位址的上一跳路由器的 ICMP 差錯封包的第四時刻；

第一定義子模組，用於將一系列探測封包中與該 ICMP 差錯封包相對應的那個探測封包的發送時刻定義為第三時刻；

第二確定子模組，用於將第四時刻與第三時刻的時間差確定為第二網路延時。