102年7月10日修　正替換頁

第 94142831 號專利申請案 102 年 02 月 20 日修正

公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：94142831

※ 申請日期：2005 年 12 月 05 日　　※IPC 分類：G06F 15/16 (2006.01)
H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

安全供應一客戶端裝置的方法、系統及電腦儲存媒體

METHOD, SYSTEM, AND COMPUTER STORAGE MEDIUM FOR SECURELY PROVISIONING A CLIENT DEVICE

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 2 人）

姓　名：（中文/英文）

1.崔凱文 C/CHOE, CALVIN C.

2.卡馬士維偉克 P/KAMATH, VIVEK P.

國　籍：（中文/英文）

1.美國/USA

2.美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

美國；2004 年 12 月 8 日；11/007,122

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本發明揭露一種在一動態配置處理過程中（dynamic configuration process）藉由驗證一客戶端而安全供應該客戶端的機制。本發明結合安全及動態配置為一整合方案，而非依賴配置後驗證（post-configuration authentication）方案。任何嘗試存取一網路的客戶端裝置可自與該網路有關之一配置伺服器請求驗證資訊，但該伺服器將不遵照該請求直到該客戶端已成功地驗證自我為被授權接收該網路之配置資訊的一裝置。該配置伺服器可提供允許該客戶端繼續進行該驗證處理但拒絕該客戶端完全存取該網路的暫時配置資訊。一旦驗證成功，該伺服器可給予該客戶端新的非暫時配置資訊或可將已給予之資訊狀態從暫時的改變為給予更完全存取之狀態。

六、英文發明摘要：

Disclosed is a mechanism for securely provisioning a client by authenticating that client during a dynamic configuration process. Rather than relying on post-configuration authentication schemes, the present invention combines security and dynamic configuration into a unified scheme. Any client device attempting to access a network may request configuration information from a configuration server associated with that network, but the server does not comply with the request until the client has successfully authenticated itself as a device authorized to receive configuration information for the network. The configuration server may provide the client with temporary configuration information that allows the client to proceed with the authentication process but that denies the client full access to the network. Upon successful authentication, the server may give the client new, non-temporary configuration information or may change the status of the information already given from temporary to a status giving fuller access.

七、指定代表圖：

(一)、本案指定代表圖為：第 1 圖。

(二)、本代表圖之元件代表符號簡單說明：

100 網路

102 裝置

104 安全配置伺服器

106 配置客戶端

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本發明一般與電腦通信有關，更特言之其係與遠端供應一客戶端裝置有關。

【先前技術】

過去一旦配置一電腦的工作環境，該配置鮮少或從不改變。然而在今日動態計算環境中，可能經常需要改變一電腦之配置。當例如一行動電腦自一無線網路移至另一者時，其可改變其網路位址為與該新網路相容者。再者，當一電腦暫時加入一特定無線網路時，管理及安全政策可要求該電腦改變其配置為該特定群組之一或多個可接受者。在一第三範例中，某些電腦於每次透過一網路服務提供者（ISP）存取網際網路時存取至少改變其網路位址之配置。

已開發協定以支援各種配置態樣。舉一例來說，DHCP－動態主機配置協定－在其他網路配置資訊中提供一 IP（網際網路協定）位址予一請求電腦。DHCP 使用一客戶端－伺服器模型，其中需要一 IP 位址之一客戶端電腦請求其中一 DHCP 伺服器。該 DHCP 伺服器－某些情況中由一 ISP 所提供－控制一群 IP 位址。一旦接收該客戶端之請求，該 DHCP 伺服器執行三種位址分配模式其中之一。在“自動分配”模式中，該 DHCP 伺服器自該群 IP 中選擇一未使用 IP 位址並永久將其指派至該請求客戶端。在“手動分配”模式中，一網路管理員選擇該位址。動態配置最有利的

莫過於在“動態分配”模式中，該 DHCP 伺服器指派一目前未使用的 IP 位址至該客戶端，但此動態位址僅於該 DHCP 伺服器所設定之一有限期間中有效或於該客戶端明確放棄其對該位址之使用前有效。不論使用何種分配方法，該 DHCP 伺服器藉由告知該客戶端其被分配之位址以及在動態分配情形中的指派期間而回應該客戶端的請求。若該 DHCP 伺服器無法提供一 IP 位址（或許是因為該群中所有 IP 位址目前均在使用中），則該 DHCP 伺服器告知該客戶端此一事實，而該客戶端必須等待稍後存取該網路。

在任何動態電腦系統中，應求取配置之簡易性與安全考量間的平衡。許多機構對該機構之內部（意即私密的）工作建立一動態網路，而若一未授權電腦被允許動態地自我配置並加入該網路將可危害該機構。包括 DHCP 的實用動態協定在安全領域中是脆弱的。由於重度依賴配置後處理（如加密金鑰式驗證機制）以保護其網路，某些配置伺服器不慎允許惡意客戶端進入。雖然該配置後處理方案如廣告所言而運作以限制惡意客戶端之存取或可能的損害，但仍有一惡意者甚至於被強制送交其可能無法通過之一配置後保護方案前便造成損害。

【發明內容】

如前所述，本發明提供藉由在一動態配置處理中驗證一客戶端以安全地供應該客戶端的一機制。本發明結合安全及動態配置成為一整合方案，而非依賴配置後處理方案。

任何嘗試存取一網路的客戶端裝置可向一配置伺服器請求與該網路有關之配置資訊，但該伺服器並不順從該請求，直到該客戶端成功地驗證自我為被授權接收該網路之配置資訊的一裝置為止。在一實施例中，該配置伺服器可提供該客戶端暫時的配置資訊及一暫時的網路位址而使該客戶端可進行該驗證處理，但拒絕該客戶端完整地存取該網路。一旦驗證成功，該伺服器可給予該客戶端新的非暫時性配置資訊，或可將已賦予為暫時的資訊狀態改變為賦予完全存取之一狀態。

在一實施例中，本發明使用一既有配置協定如 DHCP 而無須改變該協定。用於該驗證處理之訊息被攜帶於既有配置訊息中，例如於 DHCP 訊息之選項欄位中。

在另一實施例中，本發明應用既有安全協定至一動態配置環境中。例如可不修改地使用可延伸驗證協定（EAP）作為本發明之許多安全任務的一驗證架構。

結合前兩段之實施例，EAP 訊息可被攜帶於 DHCP 訊息之選項欄位中。當一客戶端請求配置資訊時，其將一 EAP 功能選項包括於其 DHCP 訊息中。EAP 被持續（pursued）直到該客戶端已驗證自我於該 DHCP 伺服器（且於某些方案中該伺服器已驗證自我於該客戶端）。於該情況中該 DHCP 伺服器可藉由提供該請求配置資訊而回應該初始請求。

作為一安全動態供應機制之部分，一配置伺服器可應用對其伺服之網路所設置的政策。舉例來說，所提供之配

置資訊可受到期間或範圍之限制。

【實施方式】

移至該圖示，其中相似的參照編號係指相似的項目，而本發明被說明為被實施於一適合計算環境中。本說明乃基於本發明之實施例且於此處未明確描述之替代實施例方面不應被視為對本發明之限制。

在以下描述中，係參照一或多個計算裝置之動作及操作表示而描述本發明之周圍環境，除非有其他指示。因此，將了解有時係指由電腦執行之此動作及操作包括該計算裝置之處理單元對表示一結構化形式之資料的電子信號的控制。此控制將該資料轉換或維持於該計算裝置之記憶體系統的位置上，其以習知技藝人士所熟知的一方式重配置或除此之外轉換該裝置之操作。維持該資料所在的資料結構為具有該資料格式所定義之特定屬性的記憶體實體位置。然而，雖然前文已描述本發明，但其並非限制性的，而習知技藝人士將瞭解下文所描述之各種動作及操作亦可被實施於硬體中。

可使用第 1 圖表示本發明之各種態樣的一概觀。將參照其他圖示而於其後更詳細地加以說明。第 1 圖中說明一安全網路 100。此處，安全僅表示該網路 100 不對未授權使用者開放。安全係由一組配置參數所實行：已位於該網路 100 中的裝置 102 具有適當的配置參數因而可自由地彼此通信。一外部裝置如該配置客戶端 106 並不具有一組適

當的配置參數因而無法與這些裝置 102 通信。由於該配置客戶端 106 想要加入該網路 100，其透過“防護”該網路 100 之安全配置伺服器 104 尋求許可。作為該網路 100 之一閘道，任何外部裝置可自由地與該安全配置伺服器 104 通信。

於接收該配置客戶端 106 對加入該網路 100 之請求而於提供該配置客戶端 106 一組適當配置參數之前，該安全配置伺服器 104 強制該配置客戶端 106 驗證自我，意即證明其為被授權加入該網路 100 的一裝置。

該配置客戶端 106 繼續向該安全配置伺服器 104 證明其識別。該驗證程序之詳細範例與第 3a 至 3c、4a、4b 及 5 圖有關。在某些網路中，該安全配置伺服器亦向該請求配置客戶端證明其識別。此雙向或*相互*驗證藉由防止一惡意裝置模仿該網路之安全配置伺服器而強化這些網路之安全性。

若該驗證程序成功完成，則該安全配置伺服器 104 瞭解該配置客戶端 106 被授權加入該網路 100。該安全配置伺服器 104 隨後提供一組適當配置參數予該配置客戶端 106，而該配置客戶端 106 使用該些參數以加入該網路 100 並自由地與已位於該網路 100 中的其他裝置 102 通信。

最後，該配置客戶端 106 離開該網路 100。此可為該配置管理員 106 之判斷或可為向其提供之該組配置參數到期。在任一情況中，該些配置參數不再有效，而不論該配置客戶端 106 何時希望重新加入該網路 100，其重複前述處理。

第1圖之方案係刻意加以簡化以聚焦於本發明之相關態樣。第1圖之安全配置伺服器104於某網路中可實際地為協同一分離安全伺服器運作之一配置伺服器。再者，該安全配置伺服器104（不論其描述為何）實際上不可位於該網路100中。位於該網路100中的一轉接代理程式可傳送配置及驗證訊息至位於遠端的一安全配置伺服器。轉接代理程式消除了在每個安全網路部分中具有一安全配置伺服器的需要。

該配置客戶端106及第1圖之安全配置伺服器104可為任何結構。第2圖為一方塊圖，其一般地說明支援本發明之一示範電腦系統。第2圖之電腦系統僅為一適用環境的一範例且無意對本發明之使用範圍或功能暗示任何限制。該客戶端106及該安全配置伺服器104均不應被認為具有任何關於第2圖中說明之任何一元件或其結合的依賴或需求。可伴隨其他一般目的或特殊目的計算環境或配置而操作本發明。適合伴隨本發明所使用之著名電腦系統、環境及配置的範例包括但不限於個人電腦、伺服器、手持或筆記型裝置、多處理器系統、微處理器式系統、機上盒、可程式消費型電子、網路個人電腦、微電腦、大型電腦及包括任何上述系統或裝置的分散計算環境。在其最基本配置中，該客戶端106及該安全配置伺服器104典型地包括至少一處理單元200及記憶體202。該記憶體202可為依電性（如RAM）、非依電性（如ROM或快閃記憶體）、或兩者之某種組合。此最基本配置於第2圖中由底線204加

以說明。該客戶端106及該安全配置伺服器104可具有額外特徵及功能。舉例來說，其可包括額外儲存（可移除及不可移除）包括但不限於磁碟、光碟及磁帶。此額外儲存於第2圖中由可移除儲存206及不可移除儲存208加以說明。電腦儲存媒體包括以任何儲存如電腦可讀取指令、資料結構、程式模組或其他資料之資訊的方法或技術所實施之依電性及非依電性、可移除及不可移除媒體。記憶體208、可移除儲存206及不可移除儲存208均為電腦儲存媒體之範例。電腦儲存媒體包括但不限於，隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電子抹除式唯讀記憶體（EEPROM）、快閃記憶體、其他記憶體技術、CDROM、數位多媒體光碟、其他光儲存、磁匣、磁帶、磁碟儲存、其他磁儲存裝置以及可用於儲存所需資訊且可被該客戶端106或該安全配置伺服器104存取之任何其他媒體。任何此電腦儲存媒體可為該客戶端106或該安全配置伺服器104之部分。該客戶端106及該安全配置伺服器104亦可含有通信通道210以允許其與其他裝置—包括一網路100上的裝置—通信。通信通道210為通信媒體之範例。通信媒體典型地包含電腦可讀取指令、資料結構、程式模組或位於一模組化資料信號如一載波或其他傳輸機制中的其他資料且包括任何資訊傳遞媒體。不受限地舉例來說，通信媒體可包括光媒體、有線媒體如有線網路及直接連線以及無線媒體如音頻、無線電頻率、紅外線以及其他無線媒體。此處所使用之“電腦可讀取媒體”一詞同時包括儲存媒體及

通信媒體。該客戶端 106 及該安全配置伺服器 104 亦可具有輸入裝置 212 如觸控感應顯示螢幕、一硬體鍵盤、一滑鼠、一語音輸入裝置等等。輸出裝置 214 包括該裝置本身如觸控感應顯示螢幕、喇叭及一印表機以及驅動這些裝置的演算模組（通常稱為“配接卡”）。所有這些裝置均為習知記憶人士所熟知而無須於此處詳加討論。該客戶端 106 及該安全配置伺服器 104 各具有一電源供應 216。

深入第 1 圖之概觀，第 3a 至 3c 圖提供依據本發明之示範安全配置方案的細節。為了說明之目的，這些圖形之邏輯流程圖包括可能無法用於一特定環境之選擇及變化。特言之，該圖中的步驟表示邏輯任務且不必然一對一地對應個別訊息。一特定實施例之更特定細節包括訊息交換及訊息格式將於第 4a、4b 及 5 圖中加以討論。

第 3a 圖之邏輯起始於步驟 300，於該步驟中該配置客戶端 106 向該安全配置伺服器 104 請求能使用該網路 100 的一組有效配置參數。該安全配置伺服器 104 於步驟 302 中請求該配置客戶端 106 自我識別而非立刻遵守該請求。在某些實施例中（特別參見第 4a 圖之步驟 400），該配置客戶端 106 不等待該安全配置伺服器 104 請求驗證；反之該配置客戶端 106 在其初始配置請求之同時進行該驗證處理。

該配置客戶端 106 於某些網路配置中需要使用一組有效配置參數以繼續與該安全配置伺服器 104 通信。此為一快取-22 之部分。基於安全理由，該安全配置伺服器 104

不願提供有效配置資訊予該配置客戶端 106 直到該客戶端 106 已驗證自我為被授權接收此資訊之一裝置。步驟 304 及 306 表示對於本發明之某實施例得脫離此困境的一種方式。在步驟 304 中，該安全配置伺服器 104 提供一組有效的配置參數予該配置客戶端 106 因而該客戶端可繼續該驗證處理。然而，該被提供的配置資訊雖為有效的，但僅為“暫時的”且僅能用於驗證過程中。舉例來說，該配置資訊可包括標示該位址之使用者未完全驗證的一 IP 位址。在步驟 306 中，該配置客戶端 106 接收該暫時配置資訊且將其用於該剩餘驗證過程中。在某些情況中，該暫時配置資訊防止該配置客戶端與該網路中該安全配置伺服器之外的任何裝置通信。將該配置客戶端 106 稱為位於“隔離區”中。

在步驟 308 中，該配置客戶端 106 及該安全配置伺服器 104 繼續進行該驗證處理。許多此驗證處理為習知技藝人士所熟知，且其任一者均可用於此處。在某些實施例中，於該配置客戶端 106 及該安全配置伺服器 104 之間協調該待使用之特定驗證程序。如前文關於第 1 圖所述，該驗證程序可為相互的，其中該配置客戶端 106 及該安全配置伺服器 104 各自對彼此加以驗證。

若該驗證處理失敗，必然拒絕該配置客戶端 106 存取該網路 100。若該配置客戶端 106 於步驟 306 中收到暫時配置資訊，由於該資訊之使用是有限的，故該網路 100 仍為安全的。若該驗證程序成功，則於第 3b 圖之步驟 310

中該安全配置伺服器 104 應用可存在於該網路 100 中的任一政策以決定如何提供該請求的配置資訊。這些政策可為例如限制該配置資訊的使用期間或範圍（例如該資訊僅於一小時之“租約”中有效）。

若有可能，則於步驟 312 中該安全配置伺服器 104 提供該請求的配置資訊予該配置客戶端 106，該資訊並伴隨政策於步驟 310 中所設置之任何使用限制。當然若該網路 100 已耗盡滿足該請求所需之資源（例如所有可分配的 IP 位址均已被使用），則即使該驗證程序成功，該配置處理仍會失敗。在某些實施例中，於繼續進行該驗證處理之前將檢查資源可用性，而該安全配置伺服器 104 可據以拒絕該配置請求而非開始步驟 302 中的驗證程序。然而，由於其提供秘密資訊（該網路資源偏低）予並未被授權之配置客戶端 106，其可能使用該資訊而損害該網路 100。

步驟 314 注意若該配置客戶端 106 於步驟 304 中被提供暫時配置資訊，則於某些實施例中，該安全配置伺服器 104 可選擇僅改變該資訊之狀態為非暫時性的，而非傳送新的一組配置參數。兩者狀況之效果是相同的。

若驗證完成且擁有該非暫時配置資訊，該配置管理員 106 此刻將為該網路 100 中的一裝置，且於第 3c 圖之步驟 316 中可與該其他裝置 102 通信（受制於加諸該提供的配置資訊上的任何政策限制）。此持續直到步驟 318 中該配置客戶端 106 選擇放棄該提供的配置資訊或該資訊上的一租約到期為止。在後者情況中，該安全配置伺服器 104 將該

提供的配置資訊標記為無效的。在任一情形中，該客戶端106離開該網路100且若其希望繼續通信，便重複該安全配置處理（步驟320）。

伴隨第3a至3c圖之討論被保持一高層級以說明本發明之應用的範圍（雖然其最終將由該申請專利範圍而非由此說明書中的任何說明所定義）。為了進一步該討論，第4a及4b圖表示本發明之一特定實施例。

雖然一般而言任一方可起始該安全配置處理，但在第4a圖之步驟400中該配置客戶端106藉由傳送一DHCP發現訊息至該安全配置伺服器104而起始該處理。此DHCP訊息含有該配置客戶端106對配置資訊之請求。該DHCP發現訊息之選項欄位中帶有該配置客戶端106準備使用EAP以驗證自我的一通知。此DHCP及EAP兩協定均為習知技藝人士所熟知，因而其細節無須於此贅述。此兩協定各自被定義於該網路工程任務小組（Internet Engineering Task Force）之評論請求（Requests for Comments）2131及3748中，其全文將藉由參照而包含於此說明書中。

由於該安全配置伺服器104將不會提供配置資訊予一未驗證客戶端，其於步驟402中回應一DHCP提供訊息，該訊息之選項欄位中包含請求該配置客戶端106之識別的一EAP訊息。該配置客戶端106於步驟404中藉由傳送含有其識別之一EAP訊息加以回應。重申該EAP訊息被包含於一DHCP訊息之選項欄位中。

EAP允許該配置客戶端106及該安全配置伺服器104

協調以及使用數種驗證機制之任一者。在步驟406及408中，該雙方繼續處理該EAP之細節以及其已選擇之驗證資訊。在某些實施例中，對本發明之目的而言無須以任何方式改變EAP，且習知技藝中已知的EAP細節亦可於此處加以使用。在步驟406及408中，如同第4a圖之前述步驟，EAP訊息被攜帶於DHCP訊息之選項欄位中。

若該驗證程序繼續進行至一成功結果，則該安全配置伺服器104接收該配置客戶端106之驗證，而於第4b圖之步驟410中傳送一DHCP ACK訊息之選項欄位中攜帶的一EAP成功訊息。該DHCP訊息亦包括該請求的配置資訊。

當該配置客戶端106已完成其與該網路100之作業時，其藉由於步驟412中傳送一DHCP釋放訊息而放棄該配置資訊。

第5圖為一DHCP訊息500之一示範資料結構圖，於其選項欄位502中含有一EAP訊息504。該EAP訊息之核心為其資料欄位506。藉由結合一已知配置協定DHCP與一已知驗證架構協定EAP，本發明之實施例對該配置處理提供安全性而無須對於任一協定的任何改變。

依據可應用本發明之原理的許多可能實施例，應瞭解關於該圖示而於此處描述之實施例僅為說明之用而不應被視為限制本發明之範圍。該些習知技藝人士將瞭解某些實施細節如配置及驗證協定係由特定情況所決定。雖然以軟體模組或元件之形式描述本發明之環境，但某些處理可同樣地由硬體元件所執行。因此，此處描述之本發明已考慮

所有此實施例可落於以下申請專利範圍及均等物的範圍中。

【圖式簡單說明】

雖然附加申請專利範圍詳細提出本發明之特徵，但可由以下詳細描述結合伴隨圖示而最佳地了解本發明及其目的與優點，其中：

第 1 圖為一方塊圖，其說明一客戶端嘗試加入由一安全配置伺服器所"防護"的一網路；

第 2 圖為一般地說明支援本發明之一示範計算裝置的一圖示；

第 3a 至 3c 圖為共同說明一客戶端及一安全配置伺服器之間的一示範交換的一邏輯流程圖；

第 4a 及 4b 圖共同為一通信流程圖，其說明 DHCP 及 EAP 訊息如何可被用於實施一安全配置方案；及

第 5 圖為一 DHCP 訊息之選項欄位中攜帶之一 EAP 訊息的一資料結構圖。

【元件代表符號簡單說明】

100 網路

102 裝置

104 安全配置伺服器

106 配置客戶端

200 處理單元

202 記憶體

204 底線

206 可移除儲存

208 不可移除儲存

210 通信通道

212 輸入裝置

214 輸出裝置

216 電源供應

300, 302, 304, 306, 308, 310, 312, 314, 316, 318, 320,

400, 402, 404, 406, 408, 410, 412 步驟

500 DHCP 訊息

502 選項

504 EAP 訊息

十、申請專利範圍：

1. 一種在一客戶端/伺服器計算環境中安全地提供一網路位址予一客戶端計算裝置之方法，該方法包含以下步驟：

請求步驟，其係用以由該客戶端計算裝置請求一網路位址，該請求步驟包含指出該客戶端計算裝置能夠嘗試來自我驗證至一伺服器計算裝置；

接收步驟，其係用以由該伺服器計算裝置接收該客戶端對一網路位址之請求；

給予步驟，其係用以由該伺服器計算裝置給予以提供該客戶端計算裝置一網路位址，該給予步驟包含請求該客戶端計算裝置自我驗證至該伺服器計算裝置；

接收給予的步驟，其係用以經由該客戶端計算裝置接收針對一網路位址之該伺服器計算裝置的給予；

嘗試驗證步驟，其係用以嘗試驗證該客戶端計算裝置至該伺服器計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址，則執行以下步驟：

識別步驟，其係用以由該伺服器計算裝置識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置的一網路位址；

指派步驟，其係用以由該伺服器計算裝置指派該識別的網路位址至該客戶端計算裝置；

提供步驟，其係用以由該伺服器計算裝置提供該指派的網路位址予該客戶端計算裝置；及

接收所指派網路位址的步驟，其係用以由該客戶端計算裝置接收該所指派的網路位址。

2. 如申請專利範圍第1項所述之方法，其中該指派的網路位址為一網際網路協定（IP）位址。

3. 如申請專利範圍第1項所述之方法，其中該請求步驟包含使用動態主機配置協定（DHCP）。

4. 如申請專利範圍第1項所述之方法，其中嘗試驗證步驟包含使用可延伸驗證協定（EAP）。

5. 如申請專利範圍第1項所述之方法，其中請求步驟包含使用DHCP，而其中嘗試驗證步驟包含使用EAP，而其中EAP訊息被攜帶於一DHCP選項欄位中。

6. 如申請專利範圍第1項所述之方法，其中嘗試驗證步驟係由該該客戶端計算裝置所起始。

7. 如申請專利範圍第 1 項所述之方法，其中該嘗試驗證步驟係由該伺服器計算裝置所起始。

8. 如申請專利範圍第 1 項所述之方法，其中於該客戶端/伺服器計算環境中即使該客戶端計算裝置未被驗證為被允許接收一網路位址，其仍將執行識別一網路位址。

9. 如申請專利範圍第 1 項所述之方法，其更包含以下步驟：

使用步驟，其係用以由該客戶端計算裝置於嘗試驗證之過程中使用一暫時網路位址。

10. 如申請專利範圍第 9 項所述之方法，其中該暫時網路位址係由該伺服器計算裝置指派至該客戶端計算裝置以供一限制性使用。

11. 如申請專利範圍第 9 項所述之方法，其中於該客戶端/伺服器計算環境中若該客戶端計算裝置被驗證為被允許接收一網路位址，則該所指派的網路位址係與該暫時網路位址相同。

12. 一種具有電腦可執行指令以供於一客戶端/伺服器計算環境中執行一方法的電腦儲存媒體，而該方法係用以安

全地對一客戶端計算裝置提供一網路位址，該方法包含以下步驟：

請求步驟，其係用以由該客戶端計算裝置請求一網路位址；

接收步驟，其係用以由一伺服器計算裝置接收該客戶端對一網路位址之請求；

嘗試驗證客戶端計算裝置步驟，其係用以嘗試驗證該客戶端計算裝置至該伺服器計算裝置；

嘗試驗證伺服器計算裝置步驟，其係用以嘗試驗證該伺服器計算裝置至該客戶端計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址，且若該伺服器計算裝置被驗證為被允許於該客戶端/伺服器計算環境中提供一網路位址，則執行以下步驟：

識別步驟，其係用以由該伺服器計算裝置識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置的一網路位址；

指派步驟，其係用以由該伺服器計算裝置指派該識別的網路位址至該客戶端計算裝置；

提供步驟，其係用以由該伺服器計算裝置提供該指派的網路位址予該客戶端計算裝置；及

接收所指派網路位址的步驟，其係用以由該客戶端計算裝置接收該所指派的網路位址。

13.一種在一客戶端/伺服器計算環境中使一伺服器計算裝置安全地對一客戶端計算裝置提供一網路位址的方法，該方法包含：

接收步驟，其係用以接收該客戶端對一網路位址之請求；

嘗試驗證客戶端計算裝置步驟，其係用以嘗試驗證該客戶端計算裝置至該伺服器計算裝置；

嘗試驗證伺服器計算裝置步驟，其係用以嘗試驗證該伺服器計算裝置至該客戶端計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址，且若該伺服器計算裝置被驗證為被允許於該客戶端/伺服器計算環境中提供一網路位址，則執行以下步驟：

識別步驟，其係用以識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置的一網路位址；

指派步驟，其係用以指派該識別的網路位址至該客戶端計算裝置；及

提供步驟，其係用以提供該所指派的網路位址予該客戶端計算裝置。

14.如申請專利範圍第13項所述之方法，其中該指派的網

路位址為一 IP 位址。

15. 如申請專利範圍第 13 項所述之方法，其中嘗試驗證步驟包含使用 EAP。

16. 如申請專利範圍第 15 項所述之方法，其中 EAP 訊息被攜帶於 DHCP 選項欄位中。

17. 如申請專利範圍第 13 項所述之方法，其中嘗試驗證步驟係由該伺服器計算裝置所起始。

18. 如申請專利範圍第 13 項所述之方法，其中於該客戶端/伺服器計算環境中即使該客戶端計算裝置未被驗證為被允許接收一網路位址，其仍將執行識別一網路位址。

19. 如申請專利範圍第 13 項所述之方法，其更包含以下步驟：

指派暫時網路位址的步驟，其係用以指派一暫時網路位址至該戶端裝置以供於嘗試驗證過程中使用。

20. 如申請專利範圍第 19 項所述之方法，其中於該客戶端/伺服器計算環境中若該客戶端計算裝置被識別為被允許接收一網路位址，則該所指派的網路位址係與該暫時

網路位址相同。

21.一種具有電腦可執行指令以供於一客戶端/伺服器計算環境中執行一方法的電腦儲存媒體，而該方法係用以安全地對一客戶端計算裝置提供一網路位址，該方法包含以下步驟：

接收步驟，其係用以接收一客戶端對一網路位址之請求，該請求步驟包含指出該客戶端計算裝置能夠嘗試來自我驗證至一伺服器計算裝置；

給予步驟，其係用以給予以提供該客戶端計算裝置一網路位址，該給予步驟包含請求該客戶端計算裝置自我驗證至該伺服器計算裝置；

嘗試驗證步驟，其係用以嘗試驗證該客戶端計算裝置至該伺服器計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址，則執行以下步驟：

識別步驟，其係用以識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置的一網路位址；

指派步驟，其係用以指派該識別的網路位址至該客戶端計算裝置；及

提供步驟，其係用以提供該所指派的網路位

址予該客戶端計算裝置。

22.一種在一客戶端/伺服器計算環境中使一客戶端計算裝置保護一網路位址之方法，該方法包含以下步驟：

請求步驟，其係用以請求一網路位址，該請求步驟包含指出該客戶端計算裝置能夠嘗試來自我驗證至一伺服器計算裝置；

接收步驟，其係用以由該客戶端計算裝置接收來自該伺服器計算裝置之針對一網路位址的一給予，該給予包含該客戶端計算裝置自我驗證至該伺服器計算裝置的一請求；

嘗試驗證步驟，其係用以嘗試驗證該客戶端計算裝置至一伺服器計算裝置；及

若於該客戶端/伺服器計算環境中該客戶端計算裝置被驗證為被允許接收一網路位址，則接收一指派的網路位址。

23.如申請專利範圍第22項所述之方法，其中該所指派的網路位址係為一IP位址。

24.如申請專利範圍第22項所述之方法，其中請求步驟包含使用DHCP。

25. 如申請專利範圍第 22 項所述之方法，其中嘗試驗證步驟包含使用 EAP。

26. 如申請專利範圍第 22 項所述之方法，其中請求步驟包含使用 DHCP，而嘗試驗證步驟包含使用 EAP，而其中 EAP 訊息係被攜帶於 DHCP 選項欄位中。

27. 如申請專利範圍第 22 項所述之方法，其中嘗試驗證步驟係由該客戶端計算裝置所起始。

28. 如申請專利範圍第 22 項所述之方法，其更包含以下步驟：

使用步驟，其係用以由該客戶端裝置於該嘗試驗證過程中使用一暫時網路位址。

29. 如申請專利範圍第 28 項所述之方法，其中於該客戶端/伺服器計算環境中若該客戶端計算裝置被驗證為被允許接收一網路位址，則該所指派的網路位址係與該暫時網路位址相同。

30. 一種具有電腦可執行指令以供於一客戶端/伺服器計算環境中執行一方法的電腦儲存媒體，該方法係用以安全地對一客戶端計算裝置提供一網路位址，該方法包含以

下步驟：

請求步驟，其係用以請求一網路位址；

嘗試驗證客戶端計算裝置步驟，其係用以嘗試驗證該客戶端計算裝置至一伺服器計算裝置；

嘗試驗證伺服器計算裝置步驟，其係用以嘗試驗證該伺服器計算裝置至該客戶端計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址，且若該伺服器計算裝置被驗證為被允許於該客戶端/伺服器計算環境中提供一網路位址，則接收一指派的網路位址。

31.一種在一客戶端/伺服器計算環境中安全地提供一網路位址予一客戶端計算裝置之系統，該系統包含：

客戶端計算裝置，其係配置以用於請求一網路位址、用以嘗試驗證該客戶端計算裝置至一伺服器計算裝置、用以嘗試驗證該伺服器計算裝置至該客戶端計算裝置、及若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址時且若該伺服器計算裝置被驗證為被允許於該客戶端/伺服器計算環境中提供一網路位址時，用於接收一指派的網路位址；及

伺服器計算裝置，其係配置以用於接收該客戶端對一網路位址之請求、用以嘗試驗證該客戶端計算裝

置至該伺服器計算裝置、用以嘗試驗證該伺服器計算裝置至該客戶端計算裝置、及若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一網路位址時且若該伺服器計算裝置被驗證為被允許於該客戶端/伺服器計算環境中提供一網路位址時，用於識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置之一網路位址、用以指派該識別的網路位址至該客戶端計算裝置、及用以提供該所指派的網路位址予該客戶端計算裝置。

32. 如申請專利範圍第 31 項所述之系統，其中該所指派的網路位址係為一 IP 位址。

33. 一種具有電腦可執行指令以提供一系統於一客戶端/伺服器計算環境中安全地提供一 IP 位址予一客戶端計算裝置的電腦儲存媒體，其中該系統包含：

客戶端計算裝置，其係配置以用於：

傳送一 DHCPDISCOVER 訊息，請求能夠提供一 IP 位址之一伺服器的識別，該 DHCPDISCOVER 訊息包含一第一 DHCP 選項部分，該第一 DHCP 選項部分包含一 EAP 功能訊息，其指出該客戶端計算裝置能夠嘗試自我驗證至一伺服器計算裝置；

自該伺服器計算裝置接收給予來提供一 IP 位址

的一第一 DHCPOFFER 訊息，該第一 DHCPOFFER 訊息包含一第二 DHCP 選項部分，該第二 DHCP 選項部分包含一 EAP 識別請求訊息，其用於請求該客戶端計算裝置之識別；

傳送一 DHCPREQUEST 訊息，請求一 IP 位址，該 DHCPREQUEST 訊息包含一第三 DHCP 選項部分，該第三 DHCP 選項部分包含一含有該客戶端之識別的 EAP 識別回應訊息；

自該伺服器計算裝置接收給予來提供一 IP 位址的一第二 DHCPOFFER 訊息，該第二 DHCPOFFER 訊息包含一第四 DHCP 選項部分，該第四 DHCP 選項部分包含一 EAP 請求訊息，其用於請求該客戶端自我驗證至該伺服器計算裝置；

透過一 EAP 交談（session），嘗試驗證該客戶端計算裝置至該伺服器計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一 IP 位址時，接著接收一指派的 IP 位址；及

伺服器計算裝置，其係配置以用於：

接收該 DHCPDISCOVER 訊息；

傳送該第一 DHCPOFFER 訊息；

接收該 DHCPREQUEST 訊息；

傳送該第二 DHCPOFFER 訊息；

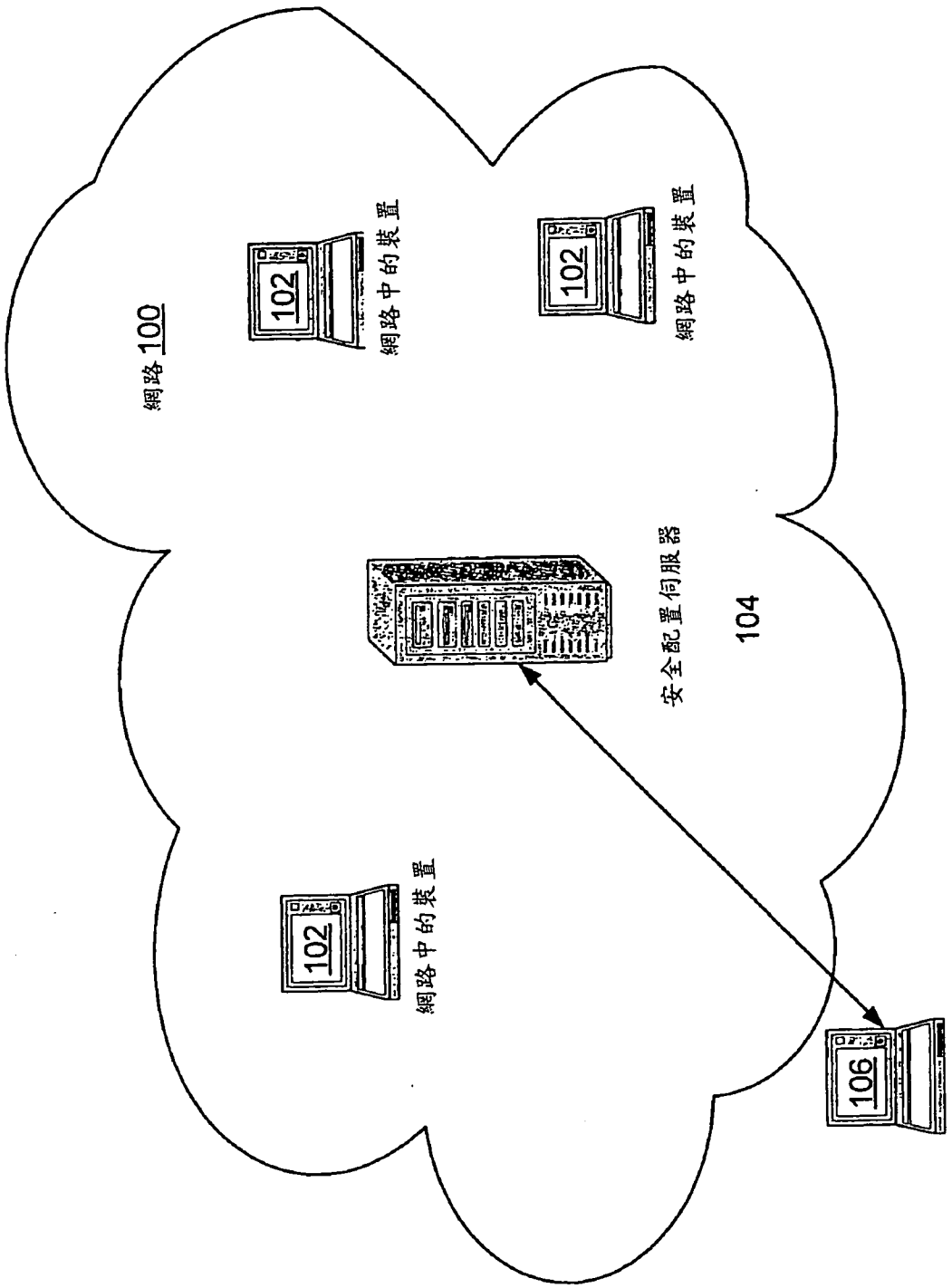
透過一 EAP 交談，嘗試驗證該客戶端計算裝置至該伺服器計算裝置；及

若該客戶端計算裝置被驗證為被允許於該客戶端/伺服器計算環境中接收一 IP 位址時，用於：

識別適合該客戶端/伺服器計算環境且目前並未被指派至一計算裝置之一 IP 位址；

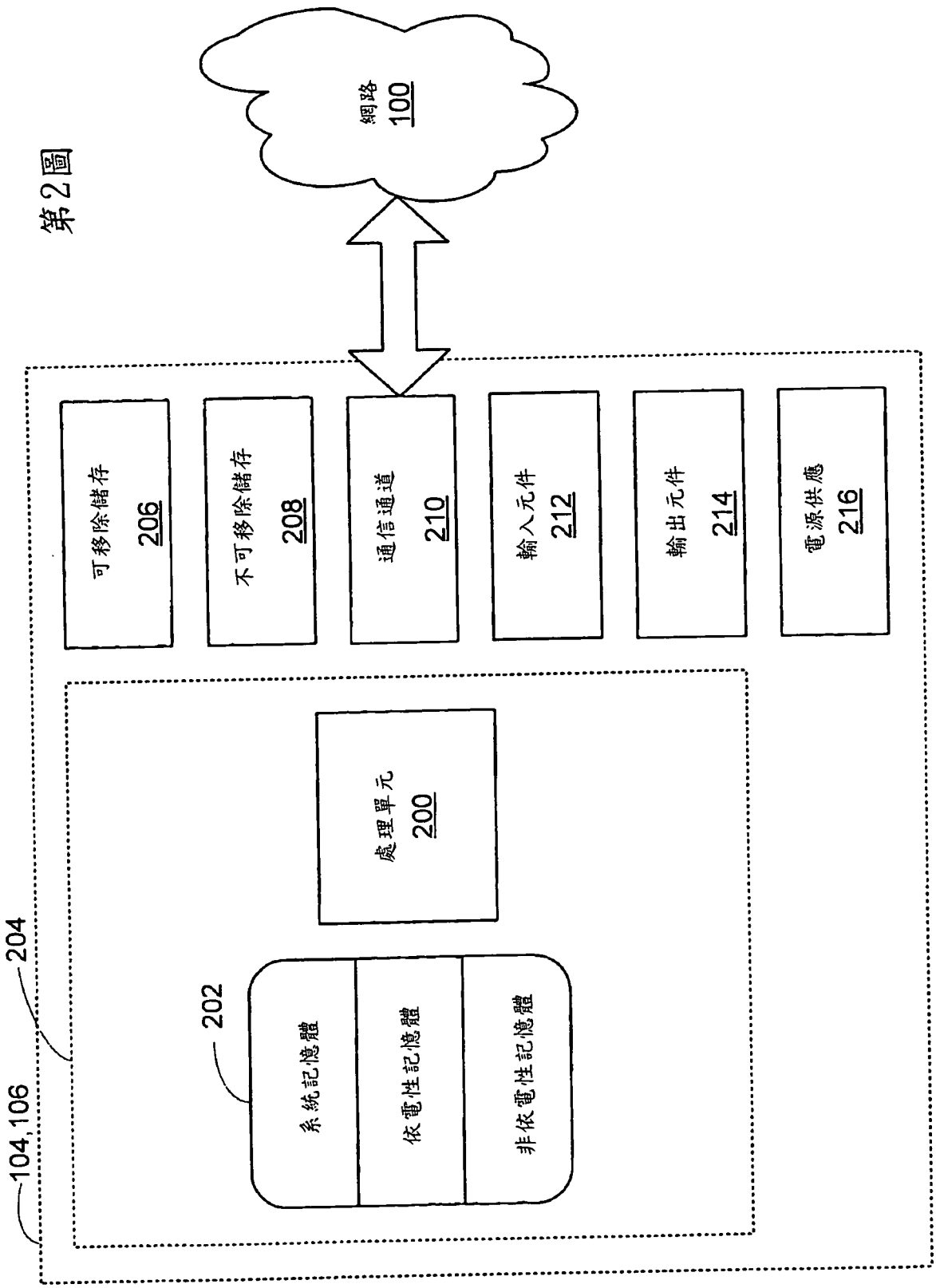
指派該識別的 IP 位址至該客戶端計算裝置；及

提供該指派的 IP 位址予該客戶端計算裝置。

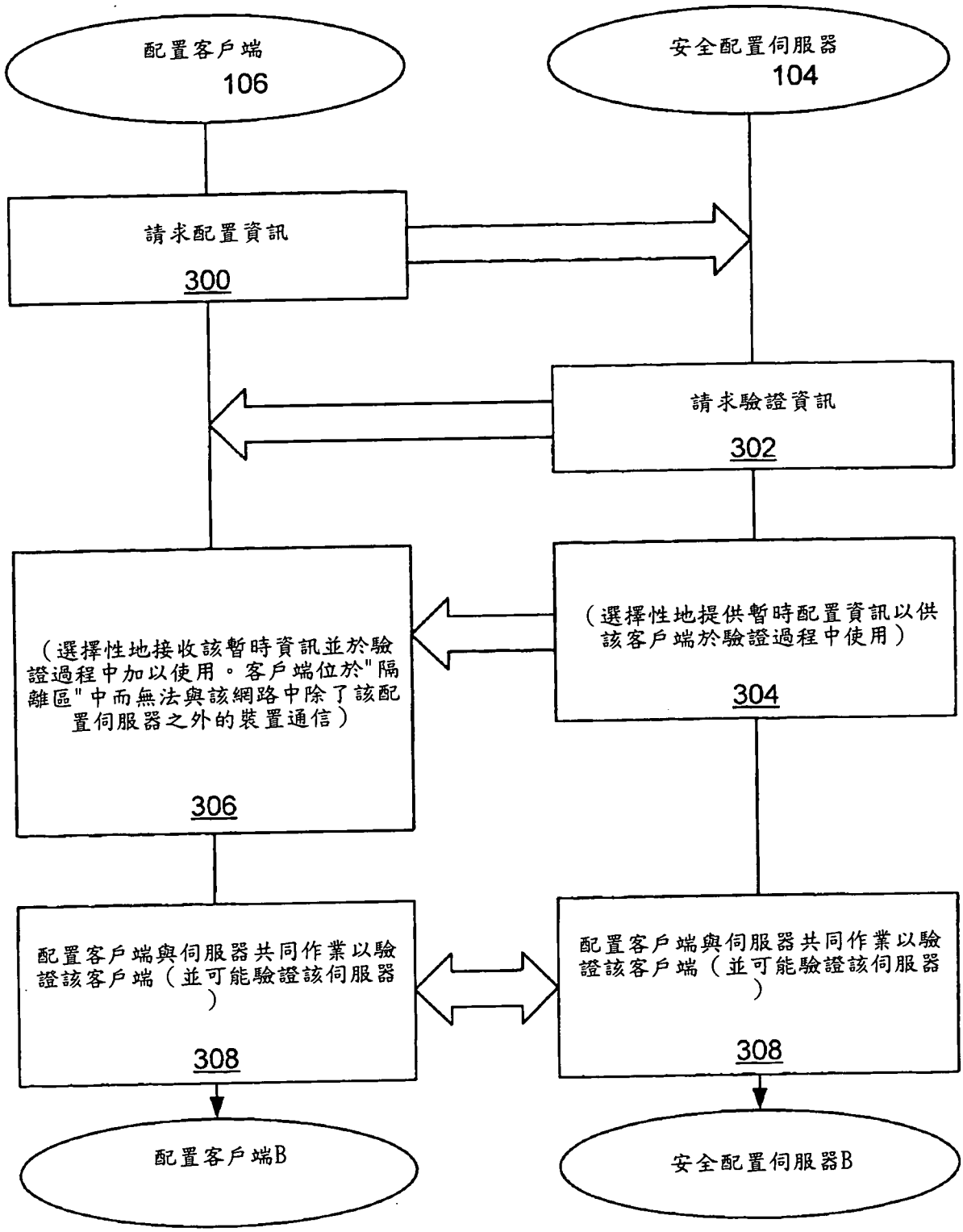

網路 100
102
網路中的裝置
102
網路中的裝置
安全配置伺服器
104
102
網路中的裝置
106
配置客戶端

第1圖

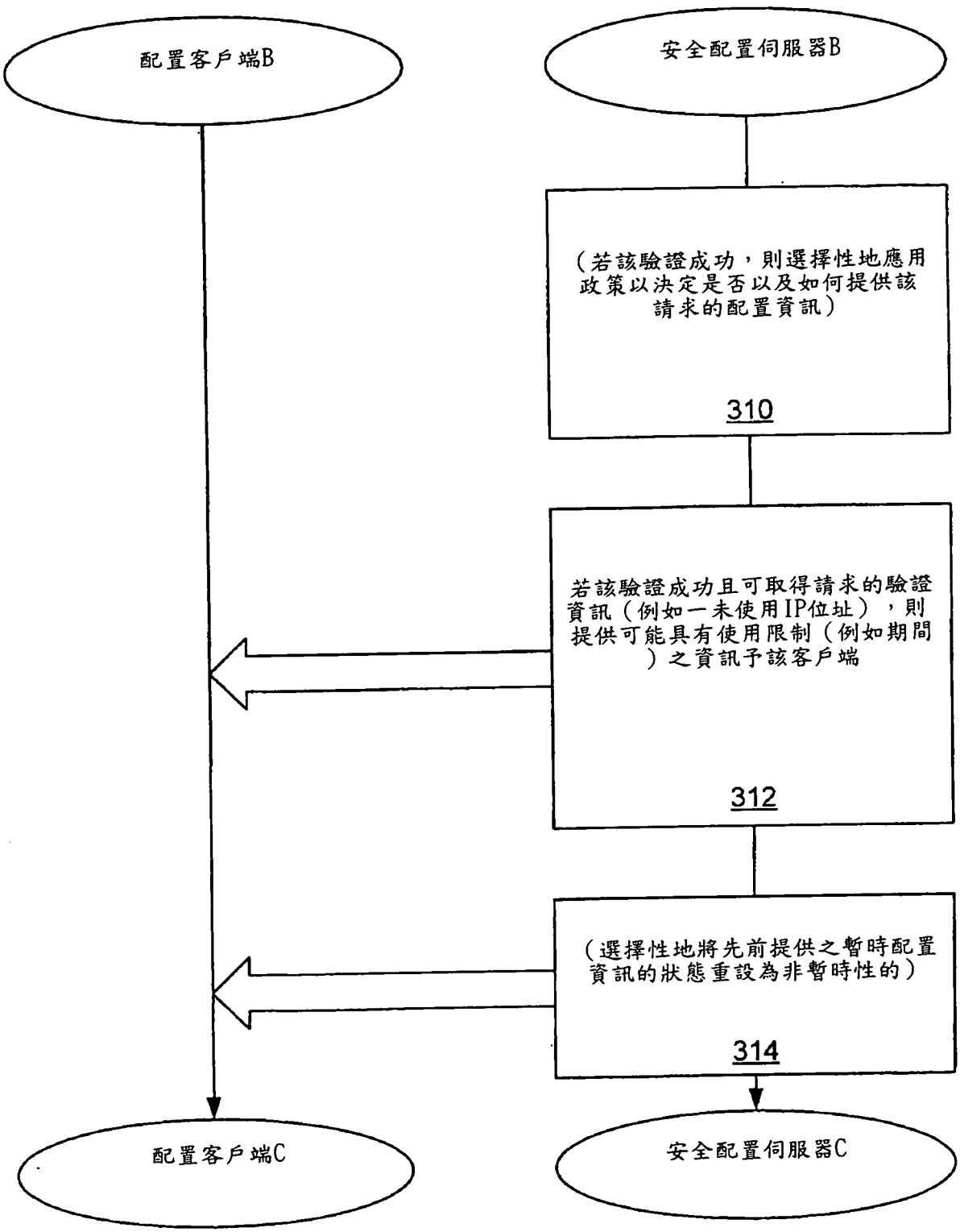
第2圖


網路
100
可移除儲存
206
不可移除儲存
208
通信通道
210
輸入元件
212
輸出元件
214
電源供應
216
處理單元
200
204
202
系統記憶體
依電性記憶體
非依電性記憶體
104,106

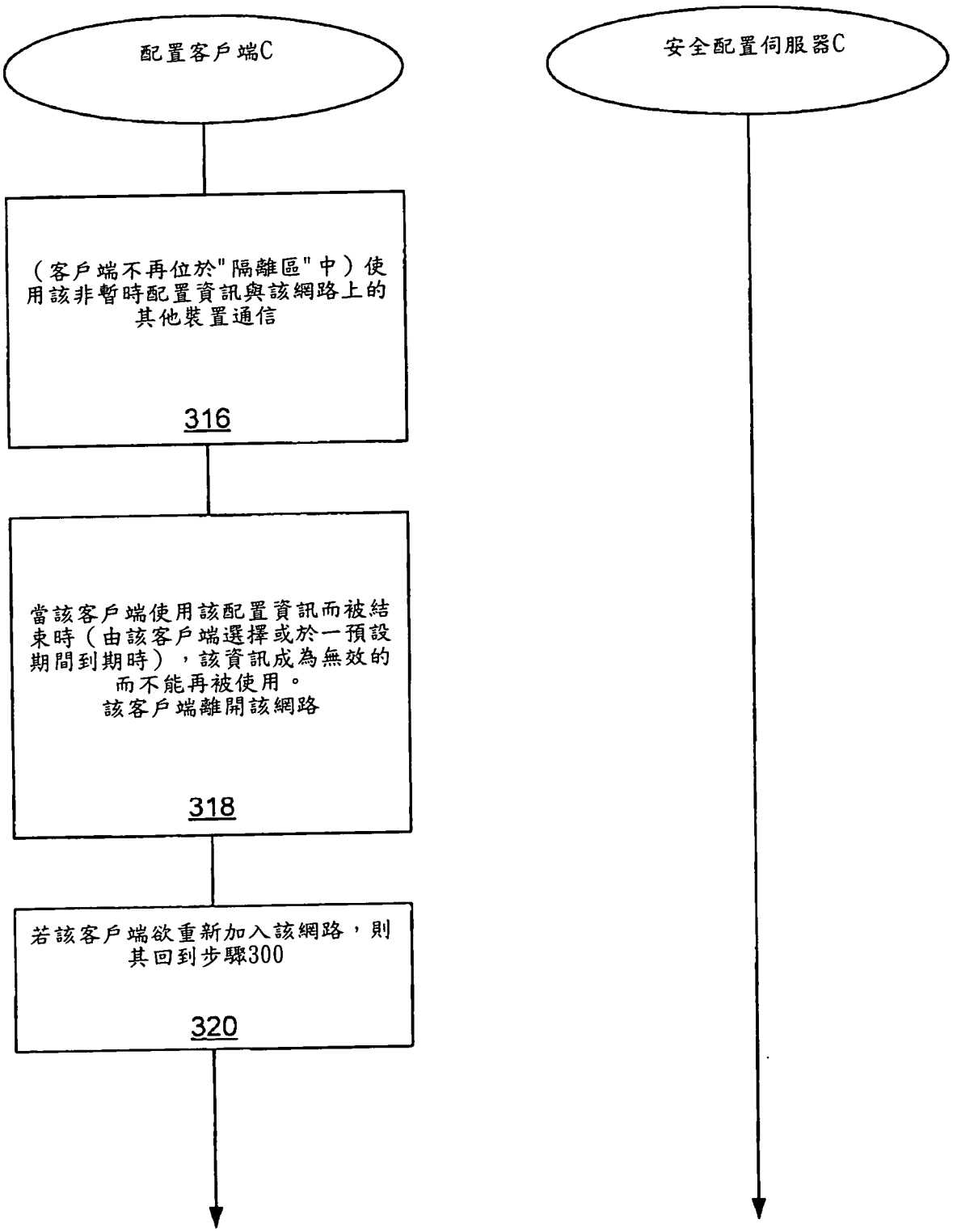
第3a圖


配置客戶端
106
安全配置伺服器
104
請求配置資訊
300
請求驗證資訊
302
（選擇性地接收該暫時資訊並於驗證過程中加以使用。客戶端位於"隔離區"中而無法與該網路中除了該配置伺服器之外的裝置通信）
306
（選擇性地提供暫時配置資訊以供該客戶端於驗證過程中使用）
304
配置客戶端與伺服器共同作業以驗證該客戶端（並可能驗證該伺服器）
308
配置客戶端與伺服器共同作業以驗證該客戶端（並可能驗證該伺服器）
308
配置客戶端B
安全配置伺服器B

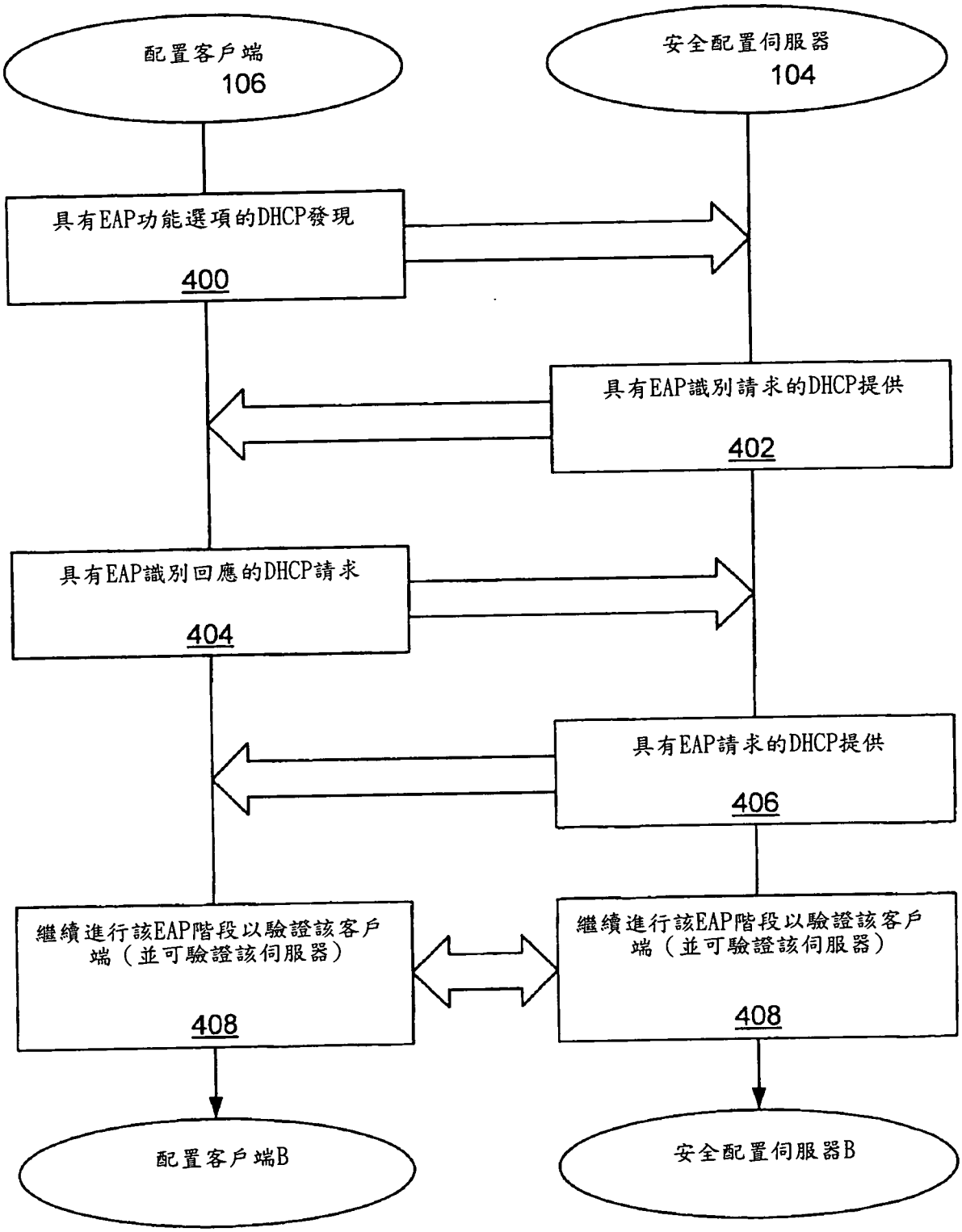
第3b圖


配置客戶端B
安全配置伺服器B
（若該驗證成功，則選擇性地應用政策以決定是否以及如何提供該請求的配置資訊）
310
若該驗證成功且可取得請求的驗證資訊（例如一未使用IP位址），則提供可能具有使用限制（例如期間）之資訊予該客戶端
312
（選擇性地將先前提供之暫時配置資訊的狀態重設為非暫時性的）
314
配置客戶端C
安全配置伺服器C

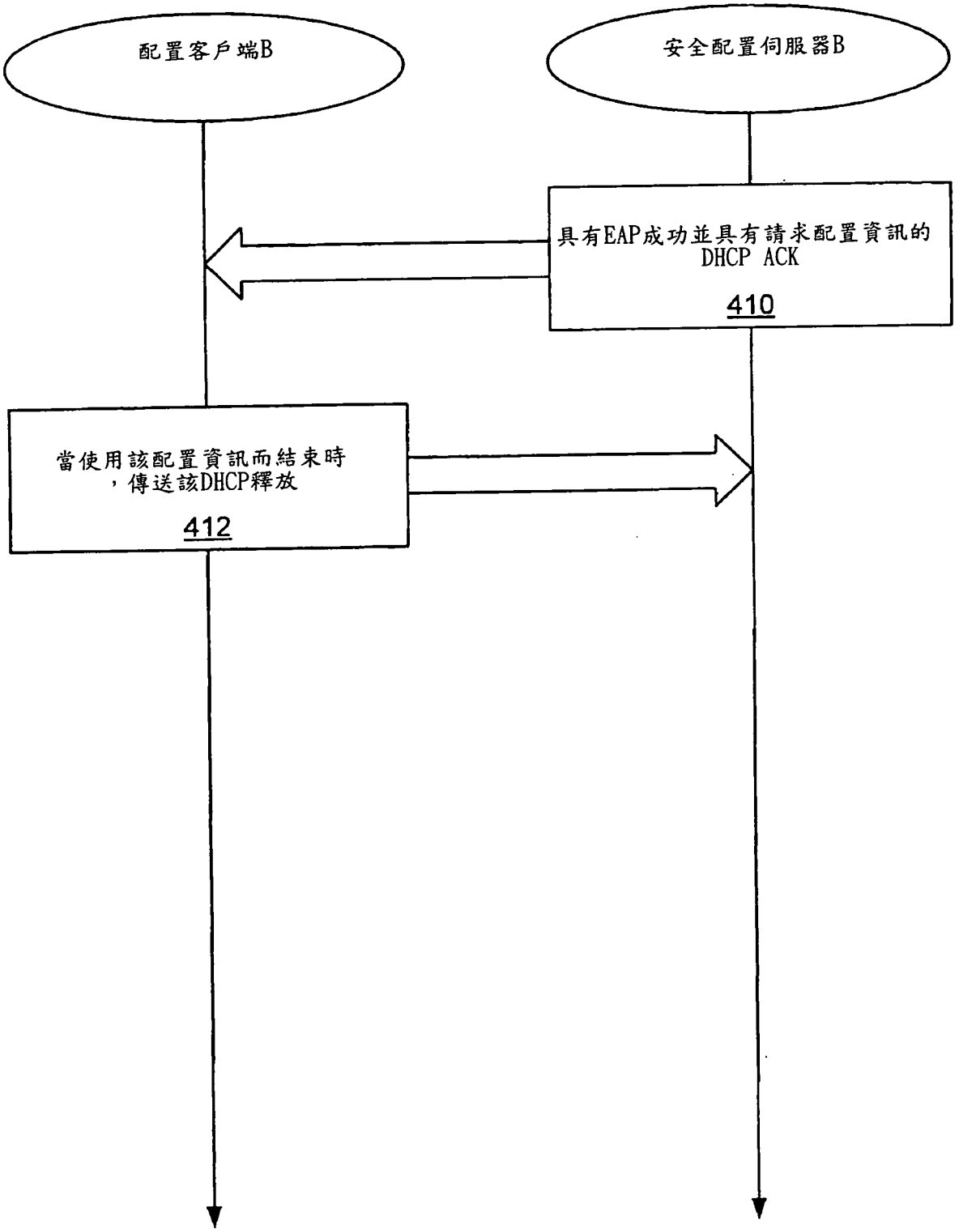
第3c圖


配置客戶端C
安全配置伺服器C
（客戶端不再位於"隔離區"中）使用該非暫時配置資訊與該網路上的其他裝置通信
316
當該客戶端使用該配置資訊而被結束時（由該客戶端選擇或於一預設期間到期時），該資訊成為無效的而不能再被使用。
該客戶端離開該網路
318
若該客戶端欲重新加入該網路，則其回到步驟300
320

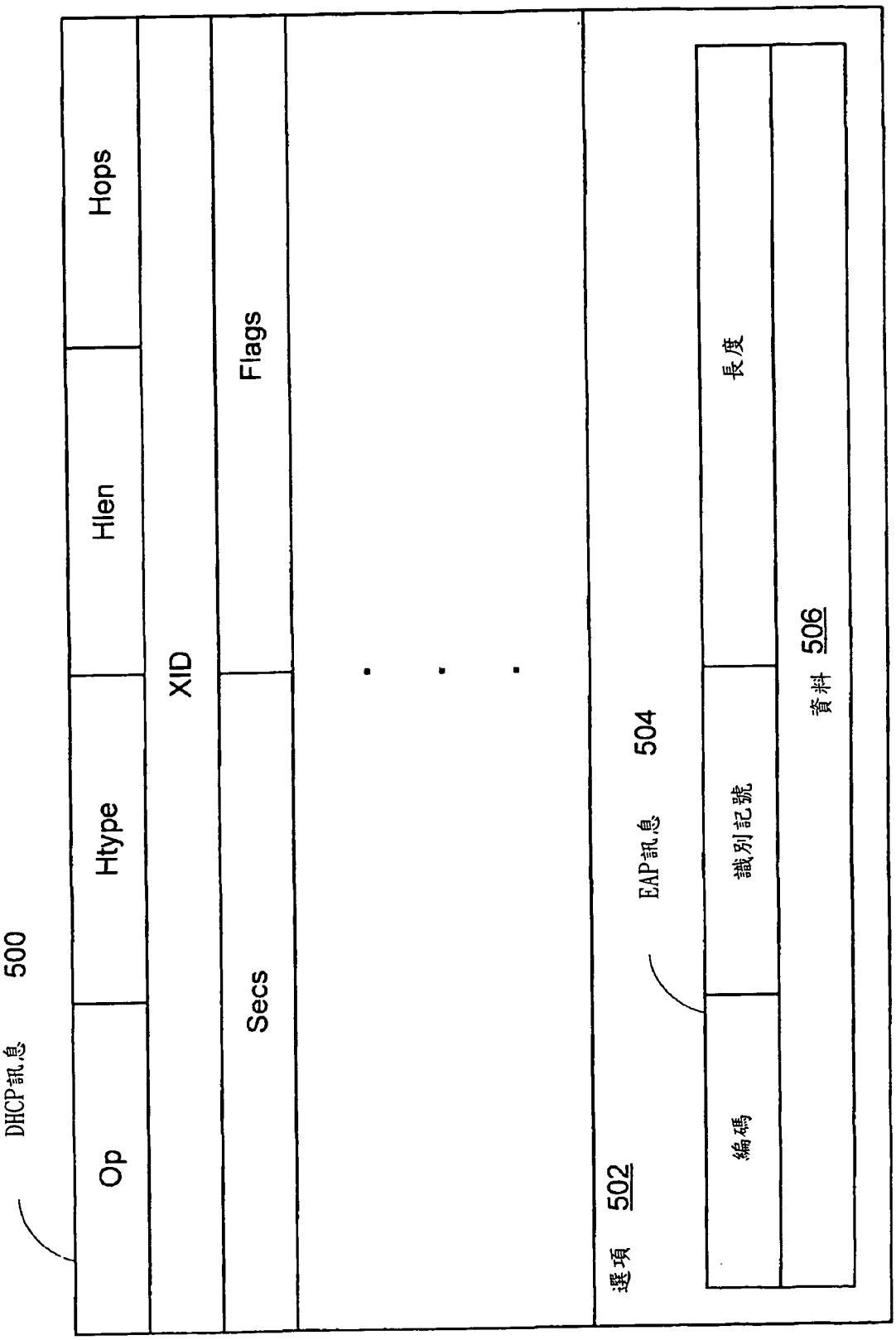
第4a圖


配置客戶端
106
安全配置伺服器
104
具有EAP功能選項的DHCP發現
400
具有EAP識別請求的DHCP提供
402
具有EAP識別回應的DHCP請求
404
具有EAP請求的DHCP提供
406
繼續進行該EAP階段以驗證該客戶端（並可驗證該伺服器）
408
繼續進行該EAP階段以驗證該客戶端（並可驗證該伺服器）
408
配置客戶端B
安全配置伺服器B

第4b圖


配置客戶端B
安全配置伺服器B
具有EAP成功並具有請求配置資訊的DHCP ACK
410
當使用該配置資訊而結束時，傳送該DHCP釋放
412

第5圖


DHCP訊息 500
Op
Htype
Hlen
Hops
XID
Secs
Flags
選項 502
EAP訊息 504
編碼
識別記號
長度
資料 506