I248737

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：92106497
※ 申請日期：92 3 24　　※IPC 分類：H04L 12/02

壹、發明名稱：（中文/英文）

無線存取點之方法、裝置及程式產品

METHODS, APPARATUS AND PROGRAM PRODUCTS FOR WIRELESS ACCESS POINTS

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）
美商萬國商業機器公司
INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）
傑拉德　羅森賽
GERALD ROSENTHAL

住居所或營業所地址：（中文/英文）
美國紐約州阿蒙市新果園路
NEW ORCHARD ROAD, ARMONK, NEW YORK 10504, U. S. A.

國　籍：（中文/英文）
美國　　U.S.A.

參、發明人：（共 6 人）

姓　名：（中文/英文）
1.大衛　卡羅　查仁納
DAVID CARROLL CHALLENER
2.大衛　羅伯特　莎福特
DAVID ROBERT SAFFORD
3.黎德特　彼得　凡　多恩
EENDERT PETER VAN DOORN

4.蓋利　M.　坎普

GARRY M. KUMP

5.法蘭西斯　E.　諾爾　二世

FRANCIS E. NOEL, JR.

6.道格拉斯　L.　斯查勒斯

DOUGLAS L. SCHALES

住居所地址：（中文/英文）

1.美國北卡州羅林市獵人山路 713 號

713 HUNTING RIDGE RD., RALEIGH, NC 27613, U. S. A.

2.美國紐約州布萊斯特市印地安山莊路 41 號

41 INDIAN HILL ROAD, BREWSTER, NY 10509, U. S. A.

3.美國紐約州凡哈拉市席達街 21 號

21 CEDAR STREET, VALHALLA, NY 10595, U. S. A.

4.美國北卡州艾沛斯市戴爾大道 2402 號

2402 DIAL DRIVE, APEX, NC 27523, U. S. A.

5.美國北卡州達拉謨市史瓦瑟摩路 4021 號

4021 SWARTHMORE ROAD, DURHAM, NC 27707, U. S. A.

6.美國紐約州米奇斯寇市郵政信箱 41 號

PO BOX 41, MT. KISCO, NY 10549, U. S. A.

國　籍：（中文/英文）

1.、2.、4.、5.、6.均美國　　U.S.A.

3.荷蘭　　THE NETHERLANDS

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑本案申請前已向下列國家（地區）申請專利：

1.美國；2002 年 03 月 27 日；10/107,794

2.美國；2002 年 07 月 30 日；10/209,568

3.美國；2002 年 07 月 30 日；10/208,281

4.美國；2002 年 07 月 30 日；10/208,277

5.專利合作條約；2002 年 11 月 20 日；PCT/US02/33648

☑ 主張國際優先權(專利法第二十四條)：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.美國；2002 年 03 月 27 日；10/107,794

2.美國；2002 年 07 月 30 日；10/209,568

3.美國；2002 年 07 月 30 日；10/208,281

4.美國；2002 年 07 月 30 日；10/208,277

5.專利合作條約；2002 年 11 月 20 日；PCT/US02/33648

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記】

1.

2.

3.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

技術領域

下述專利說明要求吾人須具備有關網路資料通信及該等通信網路中所用交換機及路由器之知識。具體言之，本專利說明要求吾人須熟悉ISO模型之網路架構(該網路架構將網路運作劃分為若干層)。一基於ISO模型之典型架構係自層1(有時亦標識為L1")向上延伸並穿過層2、3、4等直至層7，其中層1為信號傳輸用之實體路徑或媒體，而最後該層7則為在一鏈結至網路之電腦系統中執行的應用程式設計層。在本文中，L1、L2等係表示此類網路架構中之對應層。本發明內容亦要求吾人須基本瞭解該等網路通信中所用之位元串(亦稱作封包及訊框)。

先前技術

802.11標準係由電氣與電子工程師協會(IEEE)針對24億赫帶寬空間內無線區域網路所制訂的一系統規格。吾人可將802.11標準認作一種將電腦與其他電子裝置相互連接並且以高速度連接網際網路的方法，而無需繁瑣之佈線，基本上與一種無線電話鏈結至其基地台之快迅版本相同。藉由802.11標準，電子裝置可在約300英尺之距離內以每秒11百萬位元之速度相互通話，該速度快於某些公司辦公室用有線網路。

採用802.11標準之裝置(其逐漸以Wi-Fi之名稱為吾人所知曉)具有較低廉之價格。吾人僅需花費約$500即可購得一網路存取點，且該網路存取點可在其範圍內協調所有按802.11

標準配置之裝置之通信，並提供一通往網際網路及/或任一內部網路(鏈結至該存取點所)之鏈路。可使一膝上型電腦或其他裝置插入網路之介面卡價值為$100至$200。某些個人通信裝置則無需使用一額外介面卡即可實現802.11通信。目前，電腦供應商所售無線802.11標準網路卡及存取點供不應求。人們希望輕鬆連接網路且發現使用802.11-標準產品可達成該目的。該等網路之較正式之名稱為特定無線網路，而在某些狀況下則稱作行動式特定網路或MANET。

對於每時每地皆依賴於通信之世界而言，以適度之價格提供此等無線速度具有深遠之寓意。Wi-Fi目前正迅速蔓延：大學生在其公寓及餐廳中建立網路，三藩市某些地區之居民亦在建構覆蓋其社區之802.11網路，Starbucks Corp., United Airlines Inc.、Holiday Inn及其它公司則在其商店、機場候機廳及賓館內安裝802.11網路，藉以滿足其顧客保持網路連接之需求。據Synergy Research Group報導，在2000年度，使用無線區域網路之人數增加了150%。據位於亞利桑那州Scottsdale市的市場研究公司Cahners In-Stat Group預測，到2006年，商務領域之無線資料使用者數量將從目前的660萬增長至超過3900萬。助長此趨勢之事實在於：中小企業職員中近四分之一為流動職員，其至少有20%之時間係在辦公室之外度過。因此，無線電子郵件乃該等職員之首要需求，此乃為何具有始終保持電子郵件連接功能之行動式電腦產品持續熱銷之原因。2002年初，有人曾估計每天有25,000至50,000人安裝並使用802.11網路。

該無線網路之發展趨勢勢必蔓延至家庭網路市場。其中一主要原因在於價格：存取點(用於連接無線網路之設備)及網路介面卡(即NIC，其構成PC與存取點間之鏈結)之價格正在降低。此低廉之價格吸引了購物者之目光，此乃為何2001年最後一季度家庭市場增長20%之原因所在。

802.11之後繼技術已初現端倪，其中之一為超寬帶無線電技術或UWB，其使用一種低功率寬頻譜技術高速傳送資料。UWB將來或許會比802.11快十倍，然而其亦存在某些本文所述相同之弱點。另一技術係將射頻功能直接包含於執行其他功能(例如系統中央處理器及網路處理器)之晶片上。

然而，該技術亦存在問題，且造成了一種實際上左右兩難之窘境，資訊技術管理者與使用者再次面臨使用方便性與安全性要求之矛盾。目前，無線方式存在兩個主要問題，且吾人預期該等問題將來亦會繼續存在。一項問題係：在無線技術實施時，常常無任何類型之安全性。另一問題係：當消費者開始最新型安全選項時，該等選項完全無效。據Gartner Dataquest稱，在所有使用電腦網路之公司中，約30%具有某一類型之無線網路，該等無線網路或為正式之網路，或為偷竊網路。此外，若隔壁之公司或飲食店具有一無線網路，則該公司可能會遇到麻煩。

無線網路之如此開放，實際上已促成了一新型之電腦技術專家奧林匹克運動：路過式入侵。此種運動係查看參與者能夠找到多少潛在之目標，其僅需使用一膝上型電腦、一無線PC卡及若干軟體。「路過式入侵」已於技術刊物及

技術網站中受到廣泛之討論，且確係經常發生之狀況。無聊之青少年或電腦技術癡迷者之新嗜好係在膝上型電腦上安裝一天線及GPS，四處搜尋無線存取點。儘管其中大部分人並非蓄意對網路實施密碼攻擊，同時竭力約束自己不去存取網路及其中所包含之任一檔案，但是並非所有人均如此禮貌行事。

「路過式入侵」中所用一頗受歡迎之工具－NetStumbler可告知吾人存取點之名稱、是否加密及眾多其他資訊位元。對於管理者而言，NetStumbler亦為一極佳之工具，管理者可藉此識別已連接至組織內之偷竊、非授權存取點。一使用者曾駕車沿矽谷101公路高速行使，其間，其探測出二十個存取點。而另一使用者曾駕車緩慢駛過倫敦金融區，其僅藉由一空Pringles牌油煎馬鈴薯片金屬罐製成之天線即在三十分鐘內發現近六十個存取點。Kismet為一Linux用無線網路監視程式，其包括眾多與NetStumbler相同之功能。AirSnort則為一基於Linux之工具，其用於恢復加密密鑰。上述及眾多其他之工具可在網際網路中免費隨意獲得。

儘管該等組織仍須保持警惕，以保證其主網際網路閘道器之安全性，但是公司之周界正以無線之方式擴展。究竟有多少使用者藉由一VPN或其他遠端存取之手段存取至內部網路？該等使用者中究竟有多少使用者具有家庭無線網路？其安全否？若不安全，無論主網際網路閘道器如何安全，該內部網路亦易受到攻擊。在802.11與UWB採取安全措施且經證實安全無誤之前，機敏的網路管理者會始終對此

感到憂慮，尤其是員工未經存取授權，即自行從電腦便利供應商店購買無線存取點，並將其帶回工作場所，連接至其雇主之內部網並通電使用之狀況。

應特別注意的是，現有存取節點或存取點一般皆工作於層2，毫不知曉層3之定址狀況，而其所連接之邊緣路由器則完全知曉層3之定址狀況。伴隨技術之進步，存取點已包含愈來愈多之功能。舉例而言，最初，存取點僅係簡單之佈線中樞器，例如IBM 8228，其係一完全無動力之產品。無論是無線或有線，當今之存取點通常皆為層2交換機，其完全知曉層2、或媒體存取控制(MAC)、及與其相連接之裝置之位址。

將來，隨著低成本網路處理器(關於該等網路處理器，另有單獨之文字說明)之出現，該等存取點將完全知曉層3，尤其知曉與其相連接之終端站之IP位址。當然，邊緣路由器目前已知曉直接與其相連接之終端裝置之IP位址。目前，所有邊緣節點及某些存取節點已具有藉由網路連接至一網路管理控制台(其使用一稱作簡單網路管理協定(SNMP)之訊息通訊協定)之功能。將來，所有存取節點均將具備此種功能。

發明內容

本發明之一目的係：使網路管理者或管理程式能夠識別一偷竊或非授權存取點之存在，藉此幫助提高網路之安全性。本發明之另一目的係達成非授權存取點之地理位置之判定。本發明尚有另外一目的：使網路管理者或管理程式

能夠控制偷竊或非授權存取點之活動。本發明之另一目的係：使網路管理者或管理程式能夠對偷竊或非授權存取點實施自動化之控制，藉此幫助提高網路之可管理性。本發明之另一目的係：使網路管理者或管理程式能夠控制偷竊或非授權存取點與網路間資料交換活動之結算及記帳，進而幫助提高網路之財務安全性。

上述目的乃本發明之方法、裝置及程式產品所欲達成之目的，其可監視存取點(藉由該存取點可與一網路交換資料)、識別非授權存取點、並控制某些藉由該存取點之活動。

實施方式

在下文中，將參照附圖(附圖展示本發明之一較佳具體實施例)對本發明予以更為詳盡之說明。然而，在下文之說明開始之前，吾人應瞭解：熟悉此項技術者可修改本文所述之發明，並仍能達成本發明之良好效果。因此，吾人應將下文之說明理解為一針對熟悉此項技術者之廣義性、介紹性說明，而非對本發明具有限定意義之說明。

如上文所述，伴隨802.11標準之推廣應用而出現一問題：他人可在負責管理網路資訊技術(IT)之組織毫無察覺之狀況下，很容易地建立一存取至網路之無線存取點。此成為一問題，乃因該等存取點可能(且通常)會被錯誤組態，使得世人皆可隨意存取該網路及其中所包含之資料。

當已設立該等存取點時，藉由查詢網路難以確定該等存取點之存在或其組態方式。此等情形可因所佈署之特定類型存取點及網路複雜度而有所不同，在下文中將對此予以

更詳盡之說明。現行的簡單存取點解決方案為：在一行動式電腦裝置(例如一筆記型電腦或個人數位助理(PDA))中使用Net Stumbler(或類似之軟體)，藉由信號強度之量測確定使用者正在接近或遠離一存取點之時間，爾後，藉由人工參閱一索引確定該存取點是否為一非授權之"竊賊"。此一解決方案需要一人定期普查整個設施，藉以找出非授權存取點。

本發明提供多種方法，其無需派遣一使用者實施漫遊巡查即可快速定位非授權存取點。

現在請具體參見附圖。圖1展示一網路10，其具有一伺服器電腦系統11、複數個經授權之存取點12(其可為無線或有線連接)及複數個工作站電腦系統14。每一工作站電腦系統14皆耦合至該網路，此種耦合或藉由一無線連接或一有線連接，或兩種方式之並用。根據設施之大小及範圍，所管理之網路可具有不同之系統類型及不同之連接類型。該工作站可以為筆記型電腦系統、個人數位助理系統、高階功能電話機、桌上型電腦、袖珍直立型系統、或其他能夠藉由存取點存取網路10之裝置。

可藉由一經授權之無線存取點15來存取網路10而在圖式之網路中，該存取乃藉由一非授權或偷竊之無線存取點16而達成。該偷竊存取點16可能係由一個人或團體在資訊技術管理方毫不知曉或未許可之狀況下而設立。依據本發明之某些目的，偷竊存取點16之偵測及定位為吾人所欲達成之一目標。

依據本發明，該等工作站14中至少一(若非複數個或甚至全部)工作站14配備有一用於連接至網路10之無線連接或射頻連接之設備。該工作站或該等工作站亦安裝有監視軟體，例如Net Stumbler，其能夠偵測並收集可與該系統通信之所有無線存取點之相關資訊。此外，依據本發明，該(該等)系統亦安裝有報告軟體，其能夠將監視程式所收集之資訊傳送回網路10，並傳送至伺服器電腦系統11。圖2示意性地展示了軟體之功能，該軟體依據下文中所述本發明之特點安裝於一工作站14中。

若吾人欲使用最小數量之監視及報告系統，則其數量可減小至一數學上所謂之稠密集，換言之，即一系統之集合，其因與可能存在一偷竊存取點之所有點皆夠近而致使至少一系統可偵測出該偷竊存取點。對於一較小之建築物或區域而言，一系統即可提供該稠密集。對於較大之區域，採用圖1所示之複數個系統較佳。

本發明考慮：所收集之存取點(該等存取點被一工作站偵測)資訊將包括關於信號強度之資訊。本發明亦考慮：監視軟體可定期執行(區別於連續執行)。因此，該軟體可於正常之工作時間內每小時執行一次或每天執行一次，藉以避免對工作站之其他用途施加過大之負荷。在執行監視軟體時，需暫時將網路介面卡(NIC)或無線介面設定為一不同模態，藉以收集資訊；爾後重設該介面，藉以繼續正常之運行。該操作可在夠短之時間內完成，從而使大多數(若非全部)使用者毫無察覺。監視亦可包括對所感測之存取點之活動實

施一起始核對，以便信號強度之量測值可得到正確校準。

若使用一工作站實施監視，可提供兩個資料點：是否存在一偷竊存取點及該偷竊存取點之信號強度。下文將對使用多個監視站之潛在優點予以說明。

當實施監視且收集資訊時，該等資訊將藉由網路報告至伺服器11。吾人可對所傳輸之資訊加密或予以保護，使其免遭不當之存取。伺服器系統安裝有軟體，該軟體可接收所報告之資訊，維護一經授權之存取點列表，並比較所報告之資訊與該表。該伺服器系統可藉此識別任一偷竊或非授權存取點(例如圖1中之存取點16)，只要其進入其中一監視工作站所屬通信範圍內。該伺服器系統亦可儲存關於所報告信號強度之資訊。

藉由分析所報告之存取點(例如圖1所示之存取點15及16)之信號強度，IT負責組織可知曉每一工作站14之位置或能夠確定其位置(若該工作站為行動式工作站)。藉由該資訊及所報告之偷竊存取點之偵測信號強度，吾人可確定一偷竊存取點之位置。圖3示意性地展示了依據於本發明之某些特點安裝於伺服器系統11中之軟體之功能。

本發明考慮：所說明之操作可藉由下列方式得以改良：於一擬監視區域內各處設置若干無線存取點且不具體連接至網路。該等虛存取點可提供關於相對信號強度之補充資訊，並可幫助吾人定位略遠離經授權存取點之非授權存取點。此外，監視站(其未用作工作站)亦可同樣分佈於一擬監視之區域，藉以專門監視略遠離固定或行動式工作站之正

常分佈區域之區域。吾人可選擇性地收集關於監視站及存取點之資訊，藉以提供分析用之附加資料點。亦可監視及報告關於其他用戶端之該等資訊，且伺服器系統可使用該等資訊對監視系統及偷竊及經授權之存取點實施定位或不實施定位。

藉由工作站與伺服器系統之相互配合，本發明可達成下列一方法：監視可與一網路交換資料之存取點，識別一非授權存取點，並確定已識別之非授權存取點之位置。在實施該方法前，吾人須裝備複數個電腦裝置，藉以偵測可存取至該裝置之存取點並向一伺服器電腦系統報告所偵測之存取點之身份。監視包括：藉由預定之規律時間間隔或隨機之非規律時間間隔之監視方式，間歇地並定期地確定存取點之可用性。非授權存取點之識別方式為，比較所監視存取點之身份與一經授權存取點之資料庫。同時，可藉由比較複數個電腦裝置(該等電腦裝置皆報告偵測出一所識別之非授權存取點)之位置，確定該已識別之非授權存取點之位置。

至此，關於存取點之資訊基本上係以被動之形式得到。然而，當吾人欲重新組態一存取點(如下文所述)時，卻會造成難以被動獲取該等資訊。雖然以被動方式所獲取之資訊可包含一存取點之MAC位址、信號強度及至少某組態資料，但未包含建立存取點控制所必需的IP位址。

本發明考慮一步驟序列，藉由該步驟序列可進一步識別一已識別為偷竊存取點之存取點。一傾聽方戶端可繼續監

視經由該存取點之通信量，監視封包流，藉此或確定一連接至該存取點之用戶端之IP位址或監視等待一DHCP之出現。藉由此種方式收集之資訊提供至伺服器，藉以提供足夠之資訊，使該伺服器可判定該存取點是否實際上處於一企業內部網路中。若該存取點處於該企業內部網路中，則伺服器向一已連接之用戶端發出一資訊，指示該用戶端使用主動方式來確定該存取點之IP位址。該操作藉由一查詢技術得以實現，該技術可將一特殊ICMP封包傳送至指向MAC位址之存取點，並廣播至子網路。該存取點將以其IP位址作出回覆，於是該IP位址即傳送至伺服器。

適於本發明所述功能之軟體可採用電腦可讀媒體(例如圖7所示之磁碟)之形式分發給使用者，該等電腦可讀媒體可載有下列功能之軟體：當吾人在一工作站系統或一伺服器系統中執行該軟體時，其可使系統依據安裝該軟體之系統類型執行圖2及圖3所示之序列。

圖4所示為一依據本發明之其他特點之實例性存取點，其中該存取點一般用20表示。存取點20係網路10中之一節點，其藉由一有線連接或介面21連接至某些其他元件，亦可藉由無線連接或介面22連接至其他元件。該存取點20內儲存有一連接能力表24。該表可儲存於一位於兩層介面21、22之間之網路處理器內。

業內諮詢人士業已將網路處理器(本文亦稱之為NP)定義為一能夠執行下列一或多項功能之可程式規劃型積體電路：

封包分類－依據已知特徵(例如位址或協定)識別一封包；

封包修改－修改該封包，使其符合IP、ATM或其他協定(例如，更新IP標頭中之生存時間欄)；

佇列/策略管理－反映封包佇列、出佇列及特定應用中之封包排程之設計策略；及

封包轉遞－經由一交換機結構發送及接收資料，並將封包轉遞或路由至適當之位址。

儘管此一定義係早期NP之基本特點之精確說明，但是目前NP之全部潛在功能及優點尚待吾人達成。藉由硬體執行先前軟體所處理之網路連接工作，網路處理器可增大帶寬且解決存在於廣大應用範圍內之等待時間問題。此外，NP可藉由架構之設計(例如平行分散式處理及管線處理設計)達成速度之提高。此等功能可實現高效率之搜索引擎，提高通量並快速執行複雜之事務。

網路處理器有望成為網路之基本建構組塊，如同CPU之於PC。一NP所提供之典型功能為：即時處理、安全性、儲存及轉遞、交換機構造之連接能力、及IP封包處理及學習功能。NP係針對ISO層2至層5，其設計旨在最佳化網路特有之工作。

處理器模型NP結合了多種一般用途型處理器及專用邏輯。目前供應商傾向於此種設計來提供多種可擴充且具彈性之解決方案，以及時且具成本效率的方式適應變化。處理器模型NP允許在整合的較低層級採用分散式處理，藉以達成更大之通量、彈性及控制。其可程式規劃性可允許吾

人無需採用新ASIC設計即可輕鬆改用新協定及技術。倘若採用處理器模型NP，可縮減非可償還之設計成本且縮短上市時間，網路設備賣主可從中獲益非淺。

依據傳統之網路運作方式，網路10內之節點維護連接能力表，該等連接能力表包含可與之建立通信之其他節點之位址。依據維護該等表之節點之不同特徵，該等表可稱作路由選擇表或可信鄰域表。依據所偵測連接能力之廣播廣告來定期重新整理該等表。本發明係利用該等路由選擇表或可信鄰域表及一智慧型節點之能力實施上述之處理。

以此為背景，本文中所述之本發明之特徵在於：中心位置網路管理控制台可採用SNMP或更複雜之技術，定期或隨機查詢無線存取節點或無線邊緣節點。此種查詢之目的係：確定層3之路由選擇表中最新加入者，並監視最新進入者及其通信量流程有無異常之活動(例如：拒絕伺服器存取)。另外，若查詢係針對層2之裝置，則可信鄰域表中之最新進入者會受到查詢且其通信量受到監視(如上所述)。

若欲即刻採取措施，則可藉由SNMP及其它技術，立即設置層2或層3之過濾表(視需要)，藉以拒絕網路存取。若吾人欲捕捉該入侵者，則可使用上述之信號強度技術確定該偷竊存取點之位置。若欲拖住該入侵者，吾人可在層2或層3設置過濾表，藉以將該偷竊存取點之交換通信量路由至一安全伺服器，該伺服器可程式規劃為一系列之指令碼，藉以給予入侵者以正在存取該網路之感覺。

依據管理程式及存取點之功能，吾人在許多情形下可識

別出一已識別之偷竊存取點之製造商。若已識別出其製造商，吾人便可從一適當建構之列表來存取該存取點之預設組態及密碼。若已獲得預設密碼且假定在網路中建構該存取點者尚未安裝其他替代裝置，管理系統軟體可存取該存取點之安全特徵，且除重新組態路由選擇表及可信鄰域表外，亦可重新組態該存取點。具體言之，吾人可將該存取點變為一經認可、非偷竊之存取點並施予常規之網路管理控制。該等管理控制可包括財務控制(例如收取存取費)及安全性控制(例如設立系統管理方已確定之密碼)。

因此，本發明之重要特徵包括查詢邊緣路由器中路由選擇表或存取點中可信鄰域表之能力，即：以隨機或既定之方式查詢上述各表，藉以確定是否存在新進入者；監視該等新進入者之通信量流程，藉以確定其與網路之間是否存在問題(例如拒絕服務)；藉由路由選擇表及可信鄰域表過濾入侵者之通信量，並藉由或在表中輸入適當之內容而將其關閉，或將其通信量流程路由至一安全伺服器，以起始一事件序列，旨在捕捉該入侵者。上述之步驟展示於圖5中。

此外，依據本發明之其他目的，若重新組態該存取點，則會將該存取點之身份加入至費用分配之埠暫存器內，且會累積該埠身份之使用費及存取費。相關之步驟展示於在圖6中。

需再次說明的是，如上文中所述，用於執行上述步驟之程式(須在一系統(例如，伺服器11)中運行)可藉由寫入適當之電腦可讀媒體(例如圖7所示之磁碟)進行散分發。

圖式及說明書已對本發明之一較佳具體實施例予以說明；其雖然使用了特定之術語，但是此種說明所用術語僅具有一般性及描述性之意義，而非限定之目的。

圖式簡單說明

上文已提及本發明之部分目的，在實施方式之說明內容中，隨著結合附圖之更詳盡之說明，吾人亦會獲悉本發明之其他目的。圖式中：

圖1為一網路之示意圖，其安裝於一設施內且包括工作站電腦系統及一伺服器電腦系統，且在該網路上附裝有一非授權存取點；

圖2、圖3、圖5及圖6為圖1所示網路中步驟實施之簡化流程圖；

圖4為一無線存取點之示意圖，該無線存取點可用於圖1所示網路並包含一網路處理器；及

圖7為一電腦可讀媒體之視圖，其載有一程式，當在圖1所示之一適當系統中執行該程式時，其可實施圖2、圖3、圖5及圖6所示之步驟。

圖式代表符號說明

10	網路
11	伺服器電腦系統
12	經授權之存取點
14	工作站電腦系統
15	經授權之無線存取點
16	偷竊或非授權之無線存取點

20	存取點
21	有線連接或介面
22	無線連接或介面
24	連接能力表

伍、中文發明摘要：

本發明揭示一種用於監視可與一網路交換資料之無線存取點、識別一非授權存取點、並以多種方式回應所監視之資料流程的方法、裝置及程式產品，其中回應方式包括：確定已識別之非授權存取點之位置，實施過濾，並控制存取服務之結算。

陸、英文發明摘要：

Methods, apparatus and program products which monitor wireless access points through which data can be exchanged with a network, identify an unauthorized access point, and respond to monitored data flow in a variety of manners including determining the location of the identified unauthorized access point, establishing filtering, and controlling accounting for access services.

拾壹、圖式：

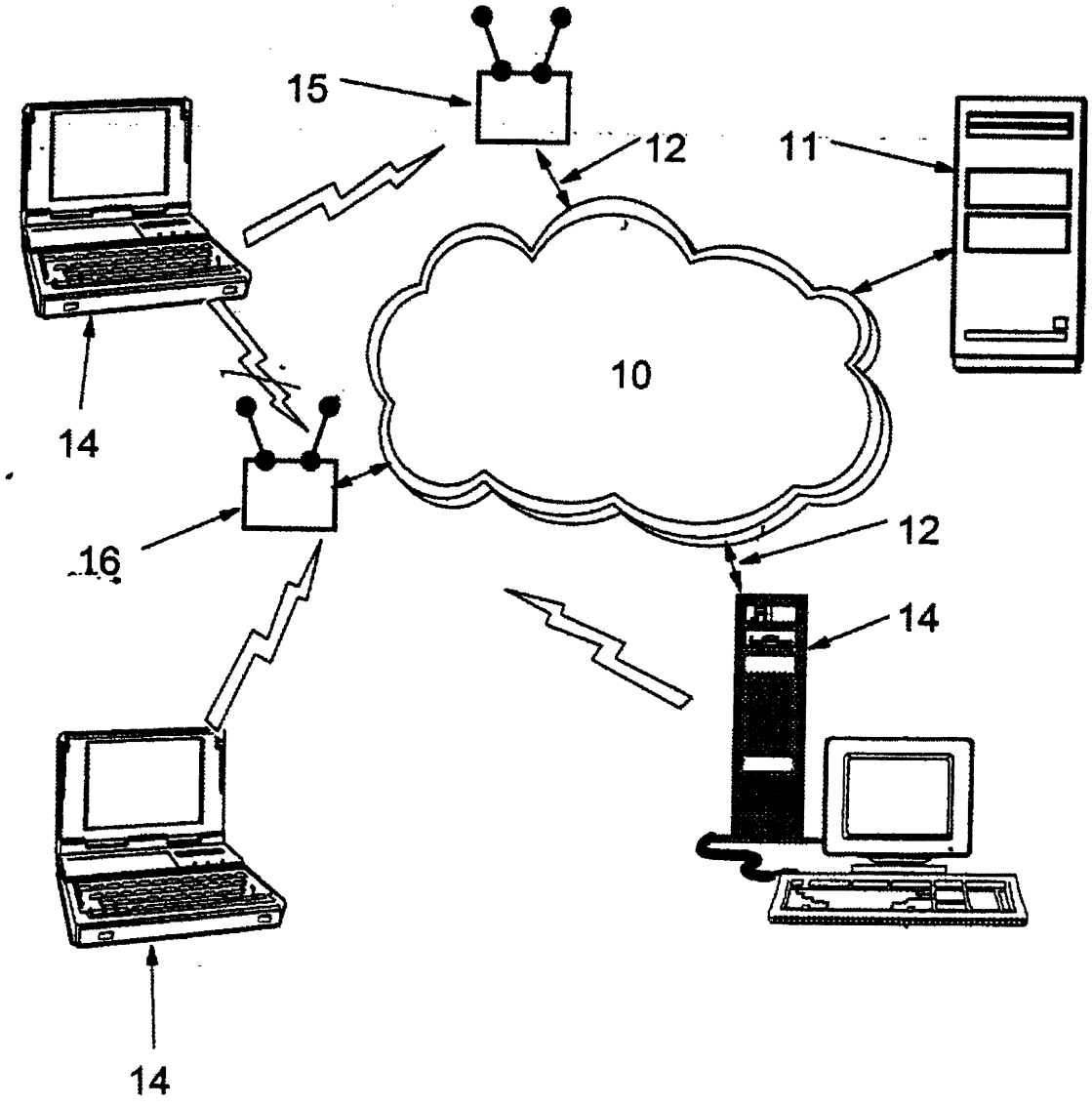

圖　1

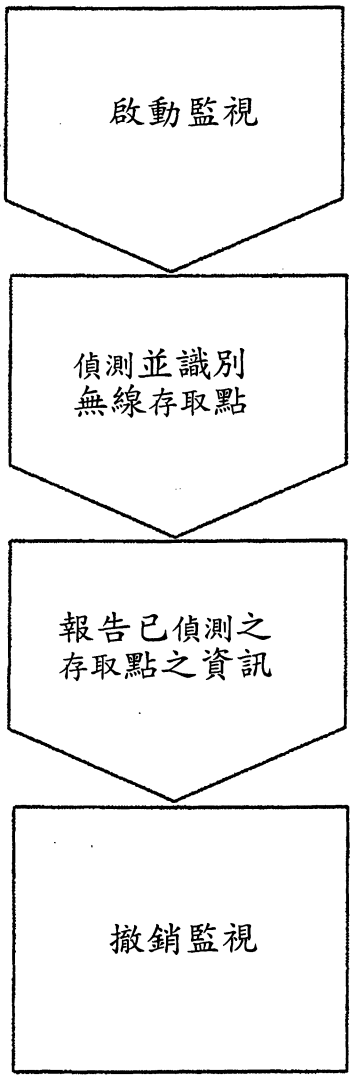

圖　2

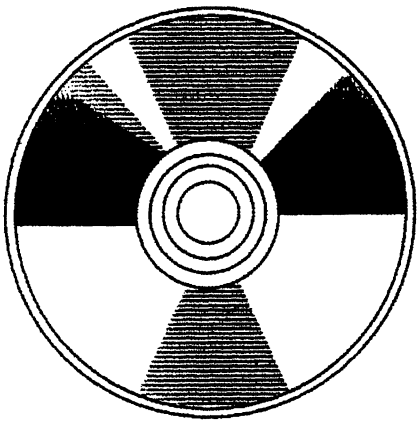

圖　7

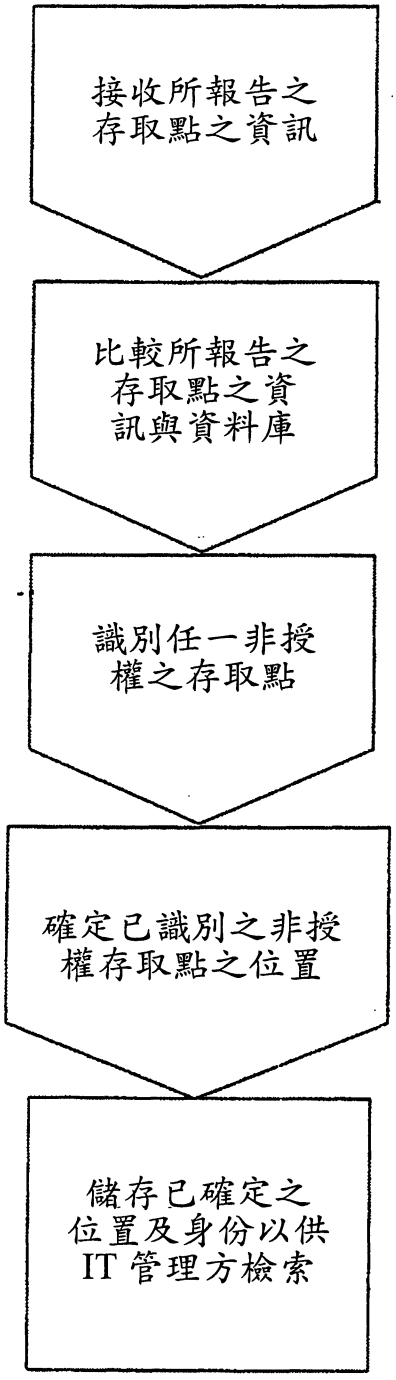
接收所報告之
存取點之資訊
比較所報告之
存取點之資
訊與資料庫
識別任一非授
權之存取點
確定已識別之非授
權存取點之位置
儲存已確定之
位置及身份以供
IT 管理方檢索

圖 3

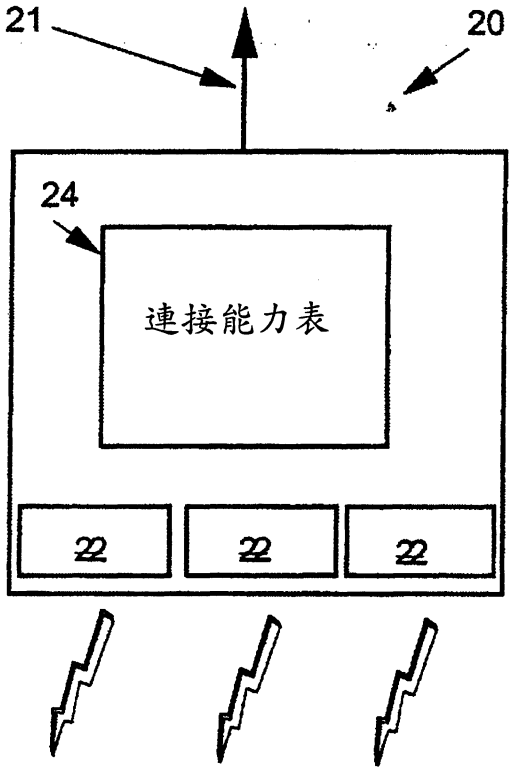
21
20
24
連接能力表
22
22
22

圖 4

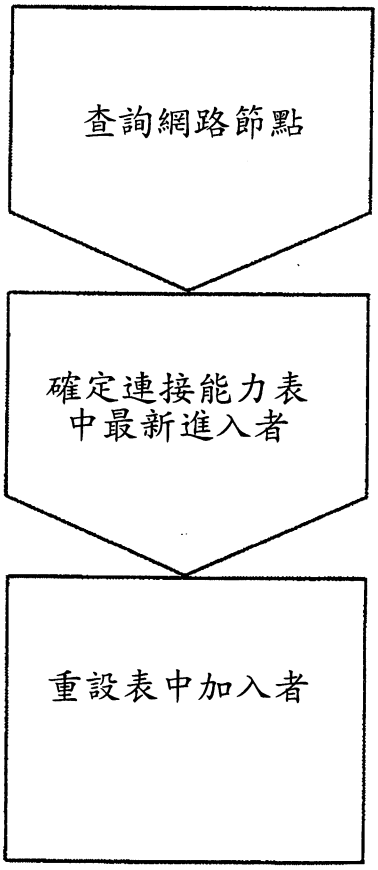
查詢網路節點
確定連接能力表中最新進入者
重設表中加入者

圖　5

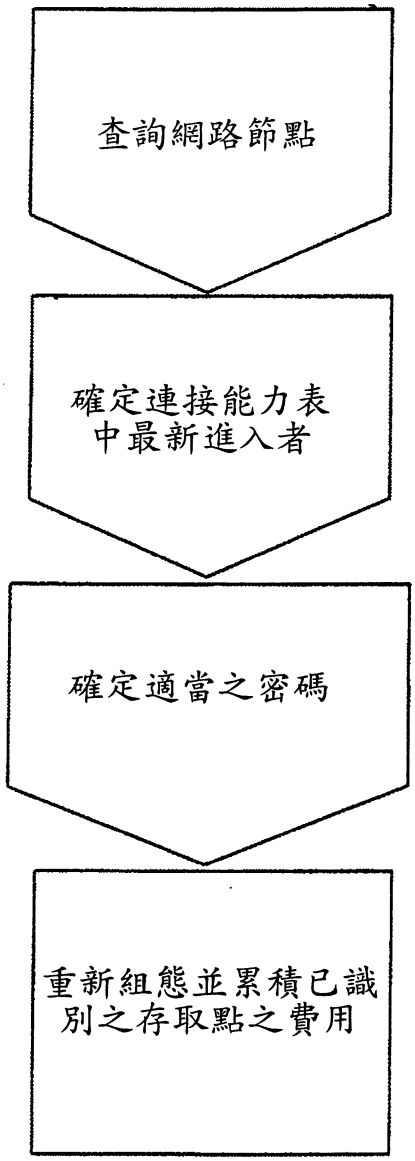
查詢網路節點
確定連接能力表中最新進入者
確定適當之密碼
重新組態並累積已識別之存取點之費用

圖　6

柒、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：

10	網路
11	伺服器電腦系統
12	經授權之存取點
14	工作站電腦系統
15	經授權之無線存取點
16	偷竊或非授權之無線存取點

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

修正替換頁
更
94年6月7日

拾、申請專利範圍：

1. 一種用以管理無線存取點之方法，包括下列步驟：

監視存取點，藉由該等存取點可與一網路交換資料，識別一非授權存取點，及

監視經由該已識別之非授權存取點所傳遞之通信量。

2. 根據請求項1之方法，進一步包括確定該已識別之非授權存取點之地理位置之步驟。

3. 根據請求項1或2之方法，進一步包括針對經由該已識別之非授權存取點所傳遞之該受監視之通信量進行通信量過濾之步驟。

4. 根據請求項1或2之方法，進一步包括下列步驟：

回應所識別到的一非授權存取點，確定該非授權存取點之製造商、型號及預設組態密碼，以及

使用該預設密碼對該非授權存取點進行定址，並在存取至該存取點後，將該存取點重新組態為一經授權之存取點。

5. 根據請求項1或2之方法，進一步包括下列步驟：將已識別之網路資源存取費及使用費累積計入該已識別之非授權存取點賬下。

6. 根據請求項1或2之方法，其中識別一非授權存取點之步驟包括：比較該所監視之存取點之身份與一經授權之存取點資料庫。

7. 根據請求項6之方法，其中監視步驟包括：裝備複數個電腦裝置，藉以偵測可存取至該裝置之存取點並向一伺服器

修正替換頁
更 94年6月7日

電腦系統報告所偵測之存取點之身份。

8. 根據請求項6之方法，其中該監視步驟包括：查詢網路節點，確認該等節點所包含之節點識別連接能力表中是否具有最新進入者。

9. 根據請求項7之方法，其中該監視步驟間歇地且定期地實施。

10. 根據請求項9之方法，其中該監視步驟係按預定之規律時間間隔實施。

11. 根據請求項9之方法，其中該監視步驟係按隨機之不規律時間間隔實施。

12. 根據請求項2之方法，其中確定一已識別之非授權存取點之地理位置之步驟包括：對該等複數個電腦裝置之位置進行比較，其中該等複數個電腦裝置皆報告已偵測到該已識別之非授權存取點。

13. 根據請求項3之方法，其中實施通信量過濾之步驟包括：拒絕透過該已識別之非授權存取點來存取網路存取。

14. 一種用以管理無線存取點之裝置，其包括：

一電腦系統；

一網路介面，其連接至該系統且在該系統與一網路之間提供一通信通道；及

一電腦可讀取媒體，其包含以該電腦系統可存取之方式儲存之程式指令，且當該程式指令在該電腦系統中執行時，其可與該電腦系統配合，藉以監視可與一網路交換資料之存取點，幫助識別一非授權存取點，並監視一已識別

修正替換頁
更 96年6月7日

之非授權存取點之通信量。

15. 根據請求項14之裝置，其中該電腦系統係一工作站電腦系統，且其中該程式指令包括：一存取點識別程式，當該程式在該系統中執行時，其可與該系統配合，藉以識別可藉由該介面存取之存取點；及一報告程式，當該程式在該系統中執行時，其可與該識別程式及該系統配合，以藉由該介面向一遠端伺服器電腦系統報告存取點之身份。

16. 根據請求項14之裝置，其中該電腦系統係一伺服器電腦系統，且進一步其中該程式指令包括一節點識別資料庫，當該程式在該系統中執行時，其可與該系統配合，以識別可藉由該介面存取至該系統之非授權存取點。

17. 根據請求項15或16之裝置，進一步包括一地理位置確定程式，當執行該程式時，其可有效獲得一非授權存取點之實體位置。

18. 根據請求項15或16之裝置，其進一步包括一通信量過濾控制程式，當執行該程式時，其可選擇性地對藉由一非授權之節點與該網路交換之通信量施加過濾。

19. 根據請求項15或16之裝置，進一步包括一控制程式，當執行該程式時，可回應所識別到的一非授權存取點，確定該非授權存取點之製造商、型號及預設組態密碼，並使用該預設密碼對該非授權存取點進行定址，且在存取至該存取點後，將該存取點重新組態為一經授權之存取點。

20. 根據請求項15或16之裝置，進一步包括一結算控制程式，當執行該程式時，其可將所識別之網路資源存取費及使用

94.6.7

費累積計入該已識別之非授權存取點賬下。

21. 一種用以管理無線存取點之記錄媒體，包括：

程式指令，其以電腦系統可存取之形式儲存於該媒體內，且當該程式指令在一系統中執行時，其可：

監視可與網路交換資料之存取點，

識別一非授權存取點，及

監視經由該已識別之非授權存取點所傳遞之通信量。

22. 根據請求項21之記錄媒體，其中該程式指令進一步包括用於確定該已識別之非授權存取點之地理位置的指令。

23. 根據請求項21或22之記錄媒體，其中該程式指令進一步包括用於針對經由該已識別之非授權存取點所傳遞之該受監視之通信量進行通信量過濾的指令。

24. 根據請求項21或22之記錄媒體，其中該程式指令進一步包括具有下列功能之指令：回應所識別到的一非授權存取點，確定該非授權存取點之製造商、型號及預設組態密碼，且使用該預設密碼對該非授權存取點進行定址，同時在存取至該存取點後，將該存取點重新組態為一經授權之存取點。

25. 根據請求項21或22之記錄媒體，其中該程式指令進一步包括用於將已識別之網路資源存取費及使用費累積計入該已識別之非授權存取點賬下的指令。

26. 根據請求項21或22之記錄媒體，其中該程式指令進一步包括用於比較該所監視存取點之身份與一經授權存取點資料庫的指令。