99年5月14日修正本

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：095100167

※ 申請日期：2006/1/3　　※IPC 分類：H04L 12/18 (2006.01)

一、發明名稱：（中文/英文）

控制一頭端系統與複數個客戶端系統間之通訊之方法

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

伊達圖亞瑟士貝威公司

代表人：（中文/英文）艾倫 費亞佛

住居所或營業所地址：（中文/英文）

荷蘭 霍夫德普 吉彼特街 42 號

國　籍：（中文/英文）

三、發明人：（共 2 人）

姓　名：（中文/英文）

鮑加，艾伯-珍

杜普羅依，杰可

國　籍：（中文/英文）

荷蘭

美國

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：

歐洲專利公約(EPC)、申請日：2005/2/14、申請號：05101087.4

☐ 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。

九、發明說明：

【發明所屬之技術領域】

本發明關於一種透過包含複數個多播路由器系統與接收器之一網路控制一頭端系統與一些客戶端系統間之一通訊之方法，

各多播路由器系統配置以發送傳送自該頭端且向接收器提出至個別多播群組之多播訊息，該接收器允許接受提出至該接收器係一成員之任何多播群組之一客戶端系統訊息，其中，對各接收器來說，僅一最近之多播路由器系統配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，

該方法包含：

維護鏈接該些客戶端系統之各已註冊者至複數個用戶群組之一相關者用戶群組資訊，及分派已註冊客戶端系統至至少一多播群組，使得關於一特定用戶群組之所有客戶端系統於一共同多播群組中，該頭端中之一伺服器配置利用提出至一多播群組之訊息以多播用戶群組訊息至客戶端系統，各用戶群組訊息意欲用於一用戶群組中之所有客戶端系統。

本發明亦關於一種用以透過包含複數個多播路由器系統與接收器之一網路控制一頭端系統與一些客戶端系統間之通訊之系統，各多播路由器系統配置以發送傳送自該頭端且向允許接受提出至該接收器係一成員之任何多播群組之一客戶端系統

訊息之接收器提出至個別多播群組之多播訊息，其中，對各接收器來說，該多播路由器系統中僅一最接近者配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，該系統包含一資料庫，用以維護鏈接該些客戶端系統之各已註冊者至複數個用戶群組之一相關者之用戶群組資訊，

其中該系統配置以分派已註冊客戶端系統至至少一多播群組，使得關於一特定用戶群組之所有客戶端系統於一共用多播群組中，一伺服器，於配置以提出至一多播群組之訊息多播用戶群組訊息至客戶端系統之頭端中，各用戶群組訊息意欲用於一用戶群組中之所有客戶端系統。

本發明亦關於一種要求自透過包含複數個多播路由器系統與接收器一網路與一些其他客戶端系統通訊之頭端系統傳遞群組訊息至一第一客戶端系統之方法，各多播路由器系統配置以發送傳送自該頭端且向允許接受提出至該接收器係一成員之任何多播群組之一客戶端系統訊息之接收器提出至個別多播群組之多播訊息，其中，對各接收器來說，該多播路由器系統中僅一最接近者配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，該頭端系統包含一註冊系統，用以維護連接該些客戶端系統之各已註冊者至複數個群組之一相關者之群組資訊，及分派多播位址至該客戶端系統，使得關於一特定群組之所有客戶端系統具有一共同多播位址，

及一伺服器，配置以具有一多播位址之訊息多播該群組訊息至至少一該客戶端系統，各群組訊息意欲用於一群組中之所有客戶端系統。

本發明亦關於一種用以要求自透過包含複數個多播路由器系統及接收器之一網路與一些其他客戶端系統通訊之一頭端系統傳遞群組訊息至一第一客戶端系統之系統，各多播路由器系統配置以發送傳送自該頭端且向允許接受提供至該接收器係一成員之任何多播群組之一客戶端系統訊息之接收器提供至個別多播系統群組之多播訊息，其中，對各接收器來說，該多播路由器系統之僅一最接近者配置以直接發送提供至該接收器係一成員之多播群組之一訊息副本至該接收器，該頭端系統包含一註冊系統，用以維護鏈接該些客戶端系統之各已註冊者至複數個群組之一相關者之群組資訊，及分派多播位址至該客戶端系統，使得關於一特定群組之所有客戶端系統具有一共用多播位址，及一伺服器，配置以具有一多播位址之訊息多播該群組訊息至至少一該客戶端系統，各群組訊息意欲用於一群組中之所有客戶端系統。

本發明亦關於一種電腦程式。

【先前技術】

根據該前言之方法之一範例已知於 WO 01/91465 中。此公開案描述一種用以一安全方式廣播數位媒體內容至遠端使用者之

普通群組，而就實際使用或存取該數位媒體內容之那些遠端使用者而論仍維護明確性之想要程度之方法。一遠端使用者裝置與一廣播頭端透過至少一頻道通訊。最好藉由加密該內容提供該內容之安全特徵，使得僅可能供已授權之使用者存取該媒體內容。該存取資訊最好透過一 ECM(控制訊息)加以散佈，其更好允許該遠端使用者裝置建立該正確金鑰。最好，該遠端使用者裝置僅可於若該遠端使用者裝置亦自該廣播器頭端接收一 EMM(或應得權利訊息)時該產生金鑰。該 EMM 可以一廣播或多播一次傳送至複數個不同遠端使用者裝置，使得一群遠端使用者裝置立刻接收該資訊。根據一特別預定計畫或其他型態之付費結構與/或根據該群遠端使用者裝置之成員之網路位址，可為一群遠端使用者裝置指定一特別 EMM。

使用該群遠端使用者裝置之成員之網路位址之一方法之一問題係並不非常有效提供關於該網路拓樸之資訊。此亦只於該頭端處來源之一樹之不同分支處之遠端使用者裝置可結束於一群組中，其接著於靠近該頭端系統之多播路由器系統提供該群組訊息之副本至數個鄰接多播路由器系統時導致一大量網路流量。

【發明內容】

本發明之一目標係提供定義於前言中之型態之方法與系統，其允許更有效使用該網路之頻寬。

此目標係藉由根據本發明之控制通訊之方法加以達成，其特徵在於藉由獲得唯一為一第一客戶端系統辨識最接近一接收器之最近多播路由器系統之資訊，及指派該第一客戶端系統至包含具有相同最近多播路由器系統之至少另一客戶端系統之一用戶群組。

由於該多播路由器系統之僅一最近者配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，提出至該多播群組織訊息經由最短路徑由另一多播路由器系統發送至該最近多播路由器系統。由於關於一特定用戶群組之所有客戶端系統接於一共同多播群組中，該訊息數量可保持相當低。由於該第一客戶端系統指派至包含具有相同最近多播路由器系統之至少另一客戶端系統之一用戶群組，該多播訊息僅透過該「最後一段」傳送至該個別客戶端系統，無論為單播(即二訊息)或使用於該資料鏈階層提供之多播功能。

於一較佳實施例中，該獲得唯一辨識該最近多播路由器系統之資訊之步驟包含自該第一客戶端系統接收一註冊要求訊息、包含對為該第一客戶端系統最接近該接收器之最近多播路由器系統係唯一之一網路位址。

該實施例使用該接收器為一客戶端系統接受多播訊息必須於具有最近多播路由器系統之最多網路暫存器中之事實。因此，其將具有該最近多播路由器系統之身分之消息或具有獲得此

消息之功能。此消息於遠離由該最近多播路由器系統所形成之網路節點之網路中之節點處更難獲得。

本發明之一較佳實施例包含自包含該第一客戶端系統之一識別之第一客戶端系統接收一註冊要求訊息，及驗證該第一客戶端系統式否已授權以接收意欲用於該用戶群組中所有客戶端系統之訊息，其中若已授權，該第一客戶端系統僅指派至該用戶群組。

由於來自該第一客戶端系統之註冊要求訊息包含該第一客戶端之一識別，其可透過一代理主機傳送。

一較佳變化包含接收包含一數位簽名之一註冊要求訊息、使用該識別取出該客戶端系統之一公用鑰、及使用該公用鑰驗證該簽名之確實性。

因此，提供偵測來自假裝該第一客戶端系統之欺詐客戶端系統之要求之一機構。

一較佳實施例包含自該第一客戶端系統接收一註冊要求訊息、包含對配置以為該第一客戶端系統接收多播訊息之一接收器係唯一之一網路位址、及於指派該第一客戶端系統至該用戶群組後傳回一註冊回應訊息至對該接收器係唯一之網路位址，該註冊回應訊息包含該第一客戶端系統已指派之用戶群組之至少該共用多播系統之一多播網路位址。

由於該註冊回應訊息傳送至該接收器之唯一網路位址，即單

播，該接收器還不需要配置以接受於該多播位址下之訊息。該註冊回應訊息包含該多播網路位址。此允許該接受器接受於該位址下之訊息之後續配置，與/或發送於該多播網路位址下傳送之群組訊息至該接收器之一或多個多播路由器系統之配置。一較佳變化包含接收包含驗證資料之一註冊要求訊息及形成包含至少部分該驗證資料之資料典型之一註冊回應訊息。

此避免「中間人」攻擊以哄騙該第一客戶端系統接受來自另一來源而非該頭端中之伺服器之訊息。此於該群組訊息傳送至具有允許解密已加密訊息與/或已擾亂內容之一功能之客戶端系統之所有情況中特別有用。於此實施例中，嘗試傳送該客戶端系統群組訊息以習得由該客戶端系統所儲存之秘密金鑰係受阻撓。

一較佳實施例包含自該第一客戶端系統接收一註冊要求訊息、包含對配置以為該第一客戶端系統接受一多播訊息之一接收器係唯一之一網路位址、於指派該第一客戶端系統至該用戶群組後傳回一註冊回應訊息至對該接收器係唯一之網路位址，該註冊回應訊息包含至少一金鑰對之至少一金鑰，及其後傳送提出至該共用多播群組且以該金鑰對之另一金鑰加密之至少一群組訊息。

因此，允許該第一客戶端系統接收已加密群組訊息，例如以該用戶群組共用之一金鑰加密。由於該註冊回應訊息傳回對該接

收器係唯一之網路位址，該金鑰資訊不由其他接收器或客戶端加以接收。尤其，不可能藉由加入該多播群組獲得該金鑰。

其中該網路係一封包切換網路且最好使用該網際網路通訊協定之一較佳實施例包含以具有一負載與一標頭之單一封包自該伺服器傳送群組訊息，其中各封包負載係分別加密。

因此，該頭端與為相同用戶群組中之客戶端系統接受封包之各該接收器間之鏈接係以密碼加以保護。

一較佳實施例包含指派該第一客戶端系統至僅包含具有相同最近多播路由器系統之其他客戶端系統之一用戶群組。

因此，該頭端中之伺服器僅需傳送作為一多播訊息之各用戶群組訊息一次以到達該用戶群組之所有成員。

一較佳實施例包含於決定該多播路由器系統之一不同者是否為允許為該第一客戶端系統接受多播訊息之一接收器變為該最近多播路由器系統後自該用戶群組移除該第一客戶端系統。此實施例允許該第一客戶端系統於其使用期期間透過不同接受器接收群組訊息。於此同時，維護來自該頭端之通訊效率。

根據另一態樣，根據本發明用以透過包含複數個多播路由器系統與接收器之一網路控制一頭端系統與一些客戶端系統間之通訊之系統之特徵在於該系統配置以獲得唯一為一客戶端系統識別最接近一接收器之最近多播路由器系統之資訊，及

指派該第一客戶端系統至包含具有相同最近多播路由器系統

之至少另一客戶端系統之一用戶群組。

最好，該系統配置以執行根據本發明之一方法。

根據本發明之另一態樣，要求自透過包含複數個多播路由器系統與接收器之一網路與一些其他客戶端系統通訊之頭端系統）傳遞群組訊息至一第一客戶端系統之方法之特徵在於獲得唯一為該第一客戶端系統識別最接近一接收器之一最近多播路由器系統之資訊，及傳送一註冊要求訊息至包含該已獲得資訊之註冊系統，以允許該註冊系統指派該第一客戶端系統至包含具有相同最近多播路由器系統之至少另一客戶端系統之一用戶群組。

因此，執行該方法之系統與該頭端合作以增加群組訊息傳送至該客戶端系統之效率。

於一較佳實施例中，該唯一識別該最近多播路由器系統之資訊係對該多播路由器系統唯一且藉由根據一網路通訊協定交換訊息所獲得之一網路位址。

因此，使用可用機構以習得該最近多播路由器系統之身分。此使得該方法容易實施。其不需要修改用於多播之網路通訊協定，但僅修改該頭端與該接收器與/或客戶端系統。

一較佳實施例包含接收包含該分派至該第一客戶端系統已被指派之用戶群組之共用多播位址之一註冊回應訊息，及

傳送通知該最近多播路由器系統該共用多播位址之一訊息。

因此確保配置以為該第一客戶端系統接受該用戶群組訊息之接收器實際接收實質所有該用戶群組訊息。

於一實施例中，其中該接收器包含一介面至其中包含該第一客戶端系統之至少一裝置，該方法包含透過該介面自該第一客戶端系統接收代表一用戶識別之至少資訊及傳送一註冊要求訊息至另包含該用戶識別之註冊系統。

因此，該方法允許該接收器為改變身分之客戶端系統作為一代理主機。此具有此客戶端系統可傳送至其他網路位置之優點。

於一較佳實施例中，其中該第一客戶端系統包含於為該第一客戶端系統具有一介面至該接收器之一裝置中，該方法包含

透過該藉面自該接收器接收唯一識別一最接近該接收器之最近多播路由器系統之資訊及透過至用以發送至該註冊系統之接收器之介面傳回該註冊要求訊息。

此實施利益具有允許該客戶端系統用以於該網路中不同位置處結合不同接收器之優點。另外，該註冊要求訊息因此由該客戶端系統加以形成，允許使用一相當簡單之接收器。

於一較佳變化中，其中該第一客戶端系統包含於一安全裝置之一防竄改環境中，最好係一電腦卡，其中該第一客戶端系統配置以儲存一秘密金鑰，該註冊要求訊息係至少由該第一客戶端系統所簽署。

此提供一額外保護，以確保該第一客戶端事實上關聯於一有效

用戶。

一較佳實施例包含為該第一客戶端系統取出對該接收器係唯一之一網路位址，及包含對該接收器係唯一之網路位址於該註冊要求訊息中。

此實施例允許秘密資訊傳回至該第一客戶端系統，以響應該註冊要求訊息，而無其他接收器接受該訊息。

根據本發明之另一態樣，一種用以要求自一頭端系統傳遞群組訊息至一第一客戶端系統之系統配置以實行根據本發明之要求自一頭端系統傳遞群組訊息至一第一客戶端系統之一方法。

根據另一態樣，本發明提供一種配置當執行於一電腦上時根據本發明實行一方法之電腦程式。

【實施方式】

於第一圖中，一第一頭端系統包含一 CA 系統 1、一用戶管理系統(SMS)2、一預先加密系統 3 及一隨選視訊(VOD)系統 4。一第二頭端系統包含相同 CA 系統 1 與 SMS 2，以及一擾亂系統 5 與廣播伺服器 6。該廣播伺服器 6 配置以透過於第一圖中以元件符號 7 所表示之網際網路廣播內容資料，例如視訊、音訊或文字資料。於另一實施例中，該內容資料經由一衛星、電纜或地球網路或一組合作為一數位視訊廣播(DVB)服務加以廣播。亦可想像其中藉由此手段自該 VOD 系統 4（為一伺服器）傳送該內容資料之一變化。

該內容資料以 MPEG-2 格式傳送。於由 VOD 伺服器 4 之需求或廣播伺服器 6 之廣播供應之事件中，作成亦稱為一元件之至少一基本流。這些可包含一或多個視訊資料流、音訊資料流、電視文字廣播資料流等等。至少該視訊與音訊資料具有一相同時間基礎。該基本流資料攜帶於一俗稱為封包化基本流(PES)封包中。一 PES 流由皆包含由來自單一基本流之資料組成之負載及皆包含相同流識別之PES封包與包含於該PES封包之標頭中之一碼組成。

該 PES 封包接著由 MPEG-2 傳輸流(TS)封包加以攜帶。一 PES 封包可透過多個 MPEG-2 TS 封包加以散佈。該內容資料係於一快速變化控制字(CW)下於該 PES 封包層或於該運輸流層加以擾亂。CW 以應得權利控制訊息(ECM)透過網際網路 7 加以提供。於該範例中，其攜帶於一分離 MPEG-2 運輸流中，以傳輸自該 VOD 伺服器 4 與廣播伺服器 6 之流多路傳輸。該 ECM 中之 CW 以一產品金鑰加密，其以比該 CW 較低之一比率加以變化。賦予解密一特別服務資格之接收器群組以應得權利管理訊息(EMM)之方式提供有該產品金鑰。這些 EMM 係群組訊息之範例，意欲用於複數個用戶之訊息。

於第一圖之範例中，群組訊息由多播網路通訊協定(IP)數據電報中之 CA 系統 1 透過網際網路 7 傳送。

舉一範例，顯示五個接收器系統，各包含五個整合接收器解碼

器(IRD)8-12 其中之一。該 IRD 8-12 可實施為具有一網路卡或數據機之一個人電腦系統、用以傳送一視訊與音訊信號至一電視之一俗稱機上盒、具有一網路卡或數據機之一數位電視、具有多媒體功能之一行動電話聽筒等等。

一接收器系統之一詳細範例以一 IRD 裝置 13 之形式顯示於第二圖中。該 IRD 裝置 13 包含一處理器 14，具有對(易失性)主記憶體 15 之存取權及通訊一系統匯流排 16 上之控制指令與資料。允許該處理器 14 參與要求 EMM 之傳遞之一過程之一電腦程式儲存於唯讀記憶體(ROM)17 中，與/或可透過提供存取一儲存媒體 19 之一控制器 18 存取該處理器 14，例如一硬碟單元或光碟媒體讀取器。此一儲存媒體 19 亦可用以將該碼載入該 ROM 17，以提供該 IRD 裝置 13 具有如業界中所知之所需功能。

於所示範例中，該接收器系統亦包含一 CA 模組 20，透過一介面 21 與該 IRD 裝置 13 通訊，最好遵從該共用介面標準。該 CA 模組 20 接著配置以透過一電腦卡介面 23 與一存取符記合作，於此情況中係一電腦卡 22。

於此範例中，該電腦卡 22 提供有一主處理器 24、記憶體 25 與一密碼共處理器 26。該電腦卡 22 儲存對應至維護於該 SMS 2 中之用戶資料。於一實施例中，其係一多片段電腦卡，配置以處理內容資料，提供內容資料作為部分隨選視訊用戶，部分隨

選視訊用戶分離自某些用戶，提供那些用戶作為廣播服務的部分用戶。

該CA模組20具有用以自該IRD裝置13接收指令之一介面模組27及用以與該電腦卡22交換資料與/或指令之一電腦卡介面模組27。其另包含一處理器29、ROM 30及RAM 31，用以執行提供存取已擾亂內容資料之一過程之不同步驟。

該IRD裝置13包含一網路介面裝置32，最好係一乙太網路卡。其他實施例可包含一數據機、用以通訊一外部xDSL數據機之一無線介面裝置等等。欲簡化下列說明，假設該網路介面裝置32係一乙太網路卡。

該網路介面裝置32透過以軟體實施之一網路堆疊傳送IP數據電報。以已擾亂MPEG-2 TS封包之形式之負載傳送至一過濾及解擾亂模組33。此模組33過濾出屬於該IRD裝置13已指示協調之一服務之已接收多路傳輸封包。ECM與EMM傳送至該CA模組20。該CA模組20提供具有該(已加密)ECM與EMM之電腦卡22。該電腦卡22自儲存於記憶體25中之EMM取出產品金鑰。該產品金鑰用以解密傳回該過濾與解擾亂模組33之CW。於另一實施例(未顯示)中，該IRD本身包含至少一電腦卡介面，使得不需要該CA模組20。

該網路介面裝置32由軟體加強，允許該IRD裝置13實施各種網路通訊協定。該組合允許該IRD裝置13接受提出至一多播

群組之 IP 數據電報。也就是允許該 IRD 裝置 13 接受包含攜帶一 IP 多播位址之一標頭之 IP 數據電報。此位址可由第一部分識別，指派給多播位址之一特別位址字首。該 IRD 裝置 13 使用網際網路群組管理通訊協定 IGMP 結合該多播群組。

回到第一圖，顯示第一、第二與第三 IRD 8-10 包含為一區域網路(LAN)34 中之節點之架構形式。一第一多播路由器 35 運作以接受具有指派給任何該第一、第二與第三 IRD 8-10 係一成員之群組之多播 IP 位址之 IP 數據電報。其轉譯該 IP 多播位址至一鏈接層多播位址，於此情況中為乙太網路多播位址。該 IGMP 允許該第一、第二與第三 IRD 報告其多播群組成員身分至最接近之第一多播路由器 35。

明白顯示第二、第三與第四多播路由器 36-38。應了解僅非常概要性顯示之第一與第二網路片段 39、40 將包含更多此類多播路由器。第五與第六路由器 41、42 並不允許多播。一第四多播路由器 38 係最接近第四與第五 IRD 之多播路由器。該第四多播路由器 38 轉換提出至由該第四與第五 IRD 11、12 所結合之群組之多播 IP 數據電報至具有攜帶該目標位址欄位中之第四與第五 IRD 11、12 之個別單播位址之一標頭之 IP 數據電報。

第一圖中之各 IRD 8-12 與一電腦卡(未顯示)形成介面，例如該電腦卡 22，或更精確的說與如包含於該電腦卡 22 之一部分

之一客戶端系統之一實施方式形成介面。下列範例假設該客戶端系統可用以允許該 IRD 裝置 13 自該 VOD 伺服器 4 取出內容資料。

於第三圖中所示之一實施例中，該 IRD 裝置 13 執行要求 EMM 之傳遞之一方法，即群組訊息，允許解密攜帶用以解擾亂一已要求 VOD 服務之已加密 CW 之 ECM。

於一第一步驟 43 中，該 IRD 裝置 13 傳送出一訊息，以獲得最近多播路由器之 IP 位址。該最近多播路由器係於該多播路由器 35-38 中之多播路由器，其於傳送一多播訊息至該 IRD 裝置 13 時繞過所有其他多播路由器。若該 IRD 裝置 13 對應至該第一、第二與第三 IRD 8-10 其中之一，其為該第一多播路由器 35。若該 IRD 裝置 13 對應至第一圖中之第四與第五 IRD 11、12 其中之一，其為該第四多播路由器 38。何路由器係該最近路由器可根據路由器系統用以找到至一特定目的地之最短鏈接之路由通訊協定。該第一步驟 43 亦可包含聆聽來自該最近多播路由器系統之定期傳送通告訊息。

於另一實施例中，該第一步驟 43 由其中該 IRD 裝置 13 自儲存於該儲存媒體 19 上之配置資訊取出最進多播路由器系統之網路位址之一步驟加以取代。此配置可由一使用者於設定該 IRD 裝置 13 時輸入。

於一後續步驟 44 中，該 IRD 裝置 13 取出最近多播路由器之

IP 位址。應注意此 IP 位址係指派至該路由器之一介面之 IP 位址，即其對該路由器係唯一。雖然該步驟 44 一般於該第一步驟 43 之後，該步驟 44 亦可包含取出一 ICMP 重新導向訊息。此將發生於若先選擇之多播路由器事實上並非由該路由器所實施之路由通訊協定所決定之最近路由器時。

該 CA 系統 1 至派要求一服務之各客戶端系統至複數個用戶群組其中之一。為此目的，其獲該 SMS 2 維護鏈接客戶端系統之各已註冊者至其指派者之用戶群組資訊。於此同時，分派已註冊客戶端系統至至少一多播群組，各多播群組對應至一多播 IP 位址。於自關聯一客戶端系統之一特定 IRD 裝置 13 接收要求傳遞 EMM 之一訊息之後，該 CA 系統分派該客戶端系統至至少一多播群組，使得關聯於該客戶端系統係一成員之用戶群組之所有客戶端系統具有共用之至少一已分派多播群組。

意欲用於該用戶群組之所有成員之 EMM 係以對應至該共用多播群組之多播 IP 位址於多播 IP 數據電報中多播。這些攜帶 EMM 之數據電報由包含於該 CA 系統中之一伺服器加以多播。於另一實施例中，ECM 亦以相同方式多播。

欲確保網際網路 7 之有效使用，來自該 IRD 裝置 13 之註冊要求訊息包含內含於步驟 44 中之 IP 位址。該 CA 系統 1 指派該第一客戶端系統至包含已報告最近多播路由器之相同 IP 位址之至少另一客戶端系統之一用戶群組。最好，該 CA 系統確保

指派一要求客戶端系統之用戶群組僅含有具有一共用最近多播路由器之客戶端系統。

該 CA 系統 1 將最好於決定是否不同多播路由器系統為允許為該客戶端系統接受多播訊息之一接收器變成最近多播路由器系統之後重新指派該客戶端系統至一不同用戶群組，因此自其先前指派之群組移除該客戶端系統。此係一有利之特徵，由於如上所述般該客戶端系統將部份實施於該電腦卡 22 之一部分上。由於該電腦卡 22 係可攜帶、防竄改、存取符記，其可用以結合該五個 IRD 8-12 之不同者。

藉由實施上述之方法，該第一、第二與第三 IRD 35-37 接受多播 IP 數位電報之客戶端群組指派至一第一用戶群組。該第四與第五 IRD 11、12 接受攜帶群組訊息之多播 IP 數據電報之客戶端系統指派至一不同用戶群組。因此，一多播 IP 數據電報為該第一用戶群組由該 CA 系統 1 與該第一多播路由器 35 間之各路由系統傳送一次。一多播 IP 數據電報為該第二用戶群組傳送一次，直到其到達該第四多播路由器 38 為止。接著僅該二分離副本傳送至該第四與第五 IRD 11、12。這些副本「隧道」個別傳過上述非允許多播之第五與第六路由器 41、42。若使用該第一至第三 IRD 8-10 其中之一之任何客戶端系統指派至相同於第四與第五 IRD 11、12 所使用者，接著於更上游處作成分離副本。因此，此分派客戶端系統至用戶群組之特別

方法節省頻寬。

回到第三圖，該 IRD 裝置 13 最好自該電腦卡 22 獲得一隨機號碼(步驟 45)。該隨機號碼作為驗證資料，如將於稍後解釋般。該電腦卡 22 或該 IRD 裝置保留代表該隨機號碼之資訊於記憶體中以供稍後驗證。該 IRD 裝置包含該隨機號碼於其建立之註冊要求訊息中，將其加入於步驟 44 中所接收之 IP 位址。

該 IRD 裝置 13 後續(步驟 46)或同時獲得如儲存於該電腦卡 22 之一部分上之一用戶識別。此資料透過該 CA 模組 20 接收。該註冊要求訊息包含允許該用戶之身分建立之用戶識別或資訊。該因此所建立之註冊要求訊息首先傳送至該電腦卡 22(步驟 47)。該電腦卡 22 配置以儲存一秘密金鑰，其用以數位簽名與/或加密該註冊要求訊息。於此狀態中，該 IRD 裝置 13 自該電腦卡 22 將其收回(步驟 48)。

後續(步驟 49)該註冊要求訊息傳送至該 CA 系統 1。該註冊要求訊息透過 IP 使用 UDP 傳送。

欲避免該 IRD 裝置 13「擱置」，其開始一計數器(步驟 50)。其預期於一時間間隔 Δt 中自該 CA 系統 1 接收一註冊回應訊息。若否，重複步驟 49，該時間間隔設定為隨機增加值 Δt。

處理繼續如第五圖中所示。另一替代步驟顯示於第三圖中，其替代者顯示於第四圖中，將首先加以解釋。於此替代方法中，該要求傳遞 EMM 之方法由該電腦卡 22 實行，而非該 IRD 裝置

13。為此目的，該電腦卡 22 執行儲存於記憶體 25 中之指令。於一實施例中，這些指令採取透過網際網路 7 經由該 IRD 裝置 13 下載之一應用程式之形式。

該 IRD 裝置 13 導向使用上述結合第三圖之步驟 43 之方法獲得最近多播路由器系統之 IP 位址。該電腦卡 22 透過至該 CA 模組 20 之介面 23 接收該已獲得 IP 位址(步驟 51)。於該所示實施例中，其亦接收該 IRD 裝置 13 之單播 IP 位址。其接著產生一隨機號碼(步驟 52)與一註冊要求訊息之本體(步驟 53)。此包含最近多播路由器之已接收 IP 位址與該隨機號碼，以及一用戶識別。其另包含於步驟 51 中所接收之單播 IP 位址或該 IRD 裝置 13。於一實施例中，該用戶識別由代表該電腦卡續號之資料加以形成。於一實施例中，該訊息本體包含內含於該訊息本體中之資訊之一或多個項目之一拼湊。所選擇之拼湊函數設計以確保不可能自藉由加以應用所產生之拼湊值之一分析導出該輸入值，且無二不同值導向相同拼湊值。

簽名該訊息本體(步驟 54)。於一實施例(未顯示)中，其加以加密。接著，該註冊要求訊息傳送至該 IRD 裝置 13(步驟 55)。於一實施例中，自該 IRD 裝置 13 中之記憶體取出該 CA 系統 1 之 IP 位址。於另一實施例中，該電腦卡 22 通知該 IRD 裝置 13 該伺服器 1 之 IP 位址。該 IRD 裝置產生攜帶該註冊要求訊息之一 IP 數據電報，並包含該 CA 系統 1 之單播 IP 位址於其

標頭中。

於在此所討論之範例中，該 CA 系統 1 接收該註冊要求訊息。若該訊息以已加密形式接收，加以解密。該註冊要求訊息中之用戶識別接收且參照至該 SMS 2。因此，驗證該訊息源自之客戶端系統是否授權接收意欲用於即將指派至之用戶群組中之所有客戶端系統之 EMM。僅若此授權存在時，該客戶端系統指派至該用戶群組。若該訊息已簽名，使用對應至把持於該電腦卡 22 中之一私用鑰之一公用鑰驗證該簽名。該用戶識別最好用以取出用以驗證該簽名之確實性之適當公用鑰。

包含於該註冊要求訊息中之雜湊值自該註冊要求訊息之內容重新產生，並與和該註冊要求訊息一起傳送之雜湊值相比較。該 CA 系統 1 另取出配置以為傳送該註冊要求訊息之客戶端系統接受多播訊息之 IRD 裝置 13 之唯一(即單播)IP 位址。

假設其授權接收該已要求 EMM，指派該要求客戶端至為該已要求服務接收 EMM 之一用戶群組。選擇包含指示相同最近多播路由器位址於其註冊要求訊息中之至少另一客戶端系統之一用戶群組。

藉由由該 CA 系統 1 所產生之一註冊回應訊息，允許該客戶端系統接收該 EMM。該註冊回應訊息包含內涵於該註冊要求訊息中之隨機號碼，或唯一根據該隨機號碼之資訊。該註冊回應訊息另包含至少一金鑰對之至少一金鑰。最好，其包含一金鑰或

三金鑰對之各者。一金鑰對用以單播訊息至一客戶端系統。一金鑰對用以加密提出至一用戶群組之群組訊息。一金鑰用以加密提出至橫跨超過一用戶群組之客戶端系統之族群之廣播訊息。該註冊回應訊息亦包含該要求客戶端系統已指派至此之用戶群組之至少共用多播群組織多播位址。於某些實施例中，其另包含一多播位址，用以提出複數個用戶群組之所有成員。於一較佳實施例中，該註冊回應訊息根據包含於該註冊回應訊息之剩餘者中之某些或所有資料包含一雜湊值。於該所示實施例中，其包含一數位簽名。

回到第五圖，該 IRD 裝置 13 接收該註冊回應訊息(步驟 56)。添附至此之簽名使用該 CA 系統 1 之一公用鑰加以驗證(步驟 57)。對保留於步驟 45 或 52 之副本檢查該隨機號碼(步驟 58)。後續取出可應用至該客戶端系統已指派至此之用戶群組之共用多播群組之多播位址(步驟 59)。

觸發該 IRD 裝置 13 以最近多播路由器啟始註冊。尤其，其根據該網際網路群組管理通訊協定傳送一訊息，通知最近多播路由器系統於步驟 59 中所接收之多播位址。因此，該 IRD 裝置 13 結合該多播群組。其允許接收包含該多播位址於該標頭之目的地位址欄位中之 IP 數據電報。這些 IP 數據電報之至少其中之一包含以一金鑰對之一金鑰加密之一負載。解密該負載之對應金鑰係自該註冊回應訊息取出，且儲存於該電腦卡 22 之

記憶體中。附帶一提，於使用對稱加密處，該金鑰對之金鑰將相同。

本發明並非限制於上述實施例，其可於所附申請專利範圍之範疇中加以變化。舉例來說，可結合該註冊要求訊息與/或註冊回應訊息中之雜湊值與簽名，其中該簽名係該雜湊值之一密碼。

【圖式簡單說明】

本發明參照附圖更詳細加以解釋，其中：

第一圖顯示為上方定義以允許用戶接收已加密內容資料之方法之應用形成一網路架構之架構圖，

第二圖顯示形成包含為一條件式存取模組與電腦卡之形式之一接收器/解碼器與一客戶端系統之一接收器系統之架構圖，

第三圖係關於要求一客戶端系統註冊之一方法之一第一變化之一流程圖，

第四圖係關於要求一客戶端系統註冊之一方法之一第二變化之一流程圖，及

第五圖係示範於接受一註冊回應訊息後實行之數個步驟之一流程圖。

【主要元件符號說明】

1 CA 系統

2 用戶管理系統(SMS)

3 預先加密系統

4 隨選視訊(VOD)系統

5 擾亂系統

6 廣播伺服器

7 網際網路

8 整合接收器編碼器(IRD)

9 整合接收器編碼器(IRD)

10 整合接收器編碼器(IRD)

11 整合接收器編碼器(IRD)

12 整合接收器編碼器(IRD)

13 IRD 裝置

14 處理器

15 (易失性)主記憶體

16 系統匯流排

17 唯讀記憶體(ROM)

18 控制器

19 儲存媒體

20 CA 模組

21 介面

22 電腦卡

23 電腦卡介面

24 主處理器

25 記憶體

26 密碼共處理器

27 介面模組

29 處理器

30 ROM

31 RAM

32 網路介面裝置

33 解擾亂模組

34 區域網路(LAN)

35 第一多播路由器

36 第三多播路由器

37 多播路由器

38 第四多播路由器

39 第一網路片段

40 第二網路片段

41 第五路由器

42 第六路由器

43 票選最近多播路由器

44 接收 IP 位址

45 獲得隨機碼

46 獲得電腦卡資訊

47 傳送至電腦卡

48 接收自電腦卡

49 傳送至頭端

50 重設計時器

51 接收 IP 位址

52 產生隨機碼

53 產生訊息本體

54 簽署訊息

55 傳送至 STB 以供發送

56 接收回應訊息

57 檢查簽名

58 檢查隨機碼

59 取出多播位址

60 以多播路由器起始註冊

五、中文發明摘要：

一種透過一網路(7)控制一頭端系統(1-6)與一些客戶端系統(13,22)間之通訊之方法，

其中，對各接收器來說，該網路中僅一最近之多播路由器系統(35-38)配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，其包含：

維護鏈接該些客戶端系統之各已註冊者至複數個用戶群組之一相關者用戶群組資訊，及

分派已註冊客戶端系統至至少一多播群組，使得關於一特定用戶群組之所有客戶端系統於一共同多播群組中。獲得唯一為一第一客戶端系統辨識最接近一接收器之最近多播路由器系統之資訊，及

指派該第一客戶端系統至包含具有相同最近多播路由器系統之至少另一客戶端系統之一用戶群組。

六、英文發明摘要：

十、申請專利範圍：

1. 一種透過包含複數個多播路由器系統(35-38)與接收器(8-13)之一網路控制一頭端系統(1-6)與一些客戶端系統(13,22)間之一通訊之方法，各多播路由器系統(35-38)配置以發送傳送自該頭端且向接收器提出至個別多播群組之多播訊息，該接收器允許接受提出至該接收器係一成員之任何多播群組之一客戶端系統訊息，

其中，對各接收器來說，僅一最近之多播路由器系統(35-38)配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，

該方法包含：

維護鏈接該些客戶端系統之各已註冊者至複數個用戶群組之一相關者用戶群組資訊，及

分派已註冊客戶端系統至至少一多播群組，使得關於一特定用戶群組之所有客戶端系統於一共同多播群組中，該頭端中之一伺服器配置利用提出至一多播群組之訊息以多播用戶群組訊息至客戶端系統，各用戶群組訊息意欲用於一用戶群組中之所有客戶端系統，該方法之特徵在於

獲得唯一為一第一客戶端系統辨識最接近一接收器之最近多播路由器系統之資訊，及

指派該第一客戶端系統至包含具有相同最近多播路由器系

統之至少另一客戶端系統之一用戶群組。

2. 如申請專利範圍第 1 項所述之方法，其中該獲得唯一辨識該最近多播路由器系統(35-38)之資訊之步驟包含自該第一客戶端系統接收一註冊要求訊息、包含對為該第一客戶端系統最接近該接收器之最近多播路由器系統係唯一之一網路位址。

3. 如申請專利範圍第 1 項所述之方法，其包含自包含該第一客戶端系統之一識別之第一客戶端系統接收一註冊要求訊息，及

驗證該第一客戶端系統式否已授權以接收意欲用於該用戶群組中所有客戶端系統之訊息，

其中若已授權，該第一客戶端系統僅指派至該用戶群組。

4. 如申請專利範圍第 3 項所述之方法，其包含接收包含一數位簽名之一註冊要求訊息、使用該識別取出該客戶端系統之一公用鑰、及使用該公用鑰驗證該簽名之確實性。

5. 如申請專利範圍第 1 項所述之方法，其包含自該第一客戶端系統接收一註冊要求訊息、包含對配置以為該第一客戶端系統接收多播訊息之一接收器係唯一之一網路位址、及於指派該第一客戶端系統至該用戶群組後傳回一註冊回應訊息至對該接收器係唯一之網路位址，該註冊回應訊息包含該第一客戶端系統已指派之用戶群組之至少該共用多播系統之一

多播網路位址。

6. 如申請專利範圍第 5 項所述之方法，其包含接收包含驗證資料之一註冊要求訊息及形成包含至少部分該驗證資料之資料典型之一註冊回應訊息。

7. 如申請專利範圍第 1 項所述之方法，其包含自該第一客戶端系統接收一註冊要求訊息、包含對配置以為該第一客戶端系統接受一多播訊息之一接收器係唯一之一網路位址、於指派該第一客戶端系統至該用戶群組後傳回一註冊回應訊息至對該接收器係唯一之網路位址，該註冊回應訊息包含至少一金鑰對之至少一金鑰，及其後傳送提出至該共用多播群組且以該金鑰對之另一金鑰加密之至少一群組訊息。

8. 如申請專利範圍第 7 項所述之方法，其中該網路係一封包切換網路，最好使用該網際網路通訊協定，包含以具有一負載與一標頭之單一封包自該伺服器傳送群組訊息，其中各封包負載係分別加密。

9. 如申請專利範圍第 1 項所述之方法，其包含指派該第一客戶端系統至僅包含具有相同最近多播路由器系統之其他客戶端系統之一用戶群組。

10. 如申請專利範圍第 1 項所述之方法，其包含於決定該多播路由器系統(35-38)之一不同者是否為允許為該第一客戶端系統接受多播訊息之一接收器變為該最近多播路由器系統後

自該用戶群組移除該第一客戶端系統。

11. 一種用以透過包含複數個多播路由器系統(35,38)與接收器(8-13)之一網路(7)控制一頭端系統(1-6)與一些客戶端系統(13,22)間之通訊之系統，各多播路由器系統(35,38)配置以發送傳送自該頭端且向允許接受提出至該接收器係一成員之任何多播群組之一客戶端系統訊息之接收器(8-13)提出至個別多播群組之多播訊息，

其中，對各接收器來說，該多播路由器系統(35,38)中僅一最接近者配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器(8-13)，該系統包含

一資料庫(2)，用以維護鏈接該些客戶端系統之各已註冊者至複數個用戶群組之一相關者之用戶群組資訊，其中該系統配置以分派已註冊客戶端系統至至少一多播群組，使得關於一特定用戶群組之所有客戶端系統(13,22)於一共用多播群組中，

一伺服器，於配置以提出至一多播群組之訊息多播用戶群組訊息至客戶端系統(13,22)之頭端中，各用戶群組訊息意欲用於一用戶群組中之所有客戶端系統，該系統之特徵在於該系統配置以獲得唯一為一客戶端系統(13,22)識別最接近一接收器之最近多播路由器系統(35-38)之資訊，及

指派該第一客戶端系統至包含具有相同最近多播路由器系

統之至少另一客戶端系統之一用戶群組。

12. 如申請專利範圍第 11 項所述之系統，其配置以根據如申請專利範圍第 1-10 項中任一項所述執行一方法。

13. 一種要求自透過包含複數個多播路由器系統(35-38)與接收器(8-13)之一網路(7)與一些其他客戶端系統(13,22)通訊之頭端系統(1-6)傳遞群組訊息至一第一客戶端系統之方法，

各多播路由器系統(35-38)配置以發送傳送自該頭端且向允許接受提出至該接收器(8-13)係一成員之任何多播群組之一客戶端系統訊息之接收器(8-13)提出至個別多播群組之多播訊息，

其中，對各接收器來說，該多播路由器系統中僅一最接近者配置以直接發送提出至該接收器係一成員之多播群組之一訊息副本至該接收器，

該頭端系統包含

一註冊系統(1,2)，用以維護連接該些客戶端系統之各已註冊者至複數個群組之一相關者之群組資訊，及分派多播位址至該客戶端系統，使得關於一特定群組之所有客戶端系統具有一共同多播位址，

及

一伺服器(1)，配置以具有一多播位址之訊息多播該群組訊

息至至少一該客戶端系統，各群組訊息意欲用於一群組中之所有客戶端系統，

其特徵在於

獲得唯一為該第一客戶端系統識別最接近一接收器之一最近多播路由器系統之資訊，及傳送一註冊要求訊息至包含該已獲得資訊之註冊系統，以允許該註冊系統指派該第一客戶端系統至包含具有相同最近多播路由器系統之至少另一客戶端系統之一用戶群組。

14. 如申請專利範圍第 13 項所述之方法，其中該唯一識別該最近多播路由器系統之資訊係對該多播路由器系統唯一且藉由根據一網路通訊協定交換訊息所獲得之一網路位址。

15. 如申請專利範圍第 13 項所述之方法，其包含接收包含該分派至該第一客戶端系統已被指派之用戶群組之共用多播位址之一註冊回應訊息，及

傳送通知該最近多播路由器系統該共用多播位址之一訊息。

16. 如申請專利範圍第 13 項所述之方法，其中該接收器包含一介面(21)至其中包含該第一客戶端系統之至少一裝置，該方法包含透過該介面自該第一客戶端系統(22)接收代表一用戶識別之至少資訊及

傳送一註冊要求訊息至另包含該用戶識別之註冊系統(1,2)。

17. 如申請專利範圍第 13 項所述之方法，其中該第一客戶端系統包含於為該第一客戶端系統具有一介面(23)至該接收器之一裝置(22)中，該方法包含

透過該藉介面(23)自該接收器接收唯一識別一最接近該接收器(13)之最近多播路由器系統之資訊

及透過至用以發送至該註冊系統(1,2)之接收器(13)之介面傳回該註冊要求訊息。

18. 如申請專利範圍第 16 項所述之方法，其中該第一客戶端系統包含於一安全裝置之一防竄改環境中，最好係一電腦卡，其中該第一客戶端系統配置以儲存一秘密金鑰，且該註冊要求訊息係至少由該第一客戶端系統所簽署。

19. 如申請專利範圍第 13 項所述之方法，其包含為該第一客戶端系統取出對該接收器係唯一之一網路位址，及包含對該接收器係唯一之網路位址於該註冊要求訊息中。

20. 如申請專利範圍第 19 項所述之方法，其包含於對該接收器係唯一之網路位址下接收包含至少一對金鑰之至少一金鑰於一訊息中之一註冊回應訊息，

其後接收提供至該共用多播群組之至少一已加密群組訊息及

使用該適當金鑰對之另一金鑰解密該以加密群組訊息。

21. 如申請專利範圍第 13 項所述之方法，其包含

傳送一註冊要求訊息至包含驗證資料之註冊系統，

接收包含分派至該第一客戶端系統已指配之用戶群組之共用多播位址之一註冊回應訊息及回應資訊，及

驗證包含代表至少部分該驗證資料之資訊之回應資料。

22. 一種用以要求自透過包含複數個多播路由器系統(35-38)及接收器(8-13)之一網路(7)與一些其他客戶端系統通訊之一頭端系統(1-6)傳遞群組訊息至一第一客戶端系統之系統，

各多播路由器系統(35-38)配置以發送傳送自該頭端且向允許接受提供至該接收器係一成員之任何多播群組之一客戶端系統訊息之接收器提供至個別多播系統群組之多播訊息，其中，對各接收器來說，該多播路由器系統(35-38)之僅一最接近者配置以直接發送提供至該接收器係一成員之多播群組之一訊息副本至該接收器，

該頭端系統(1-6)包含

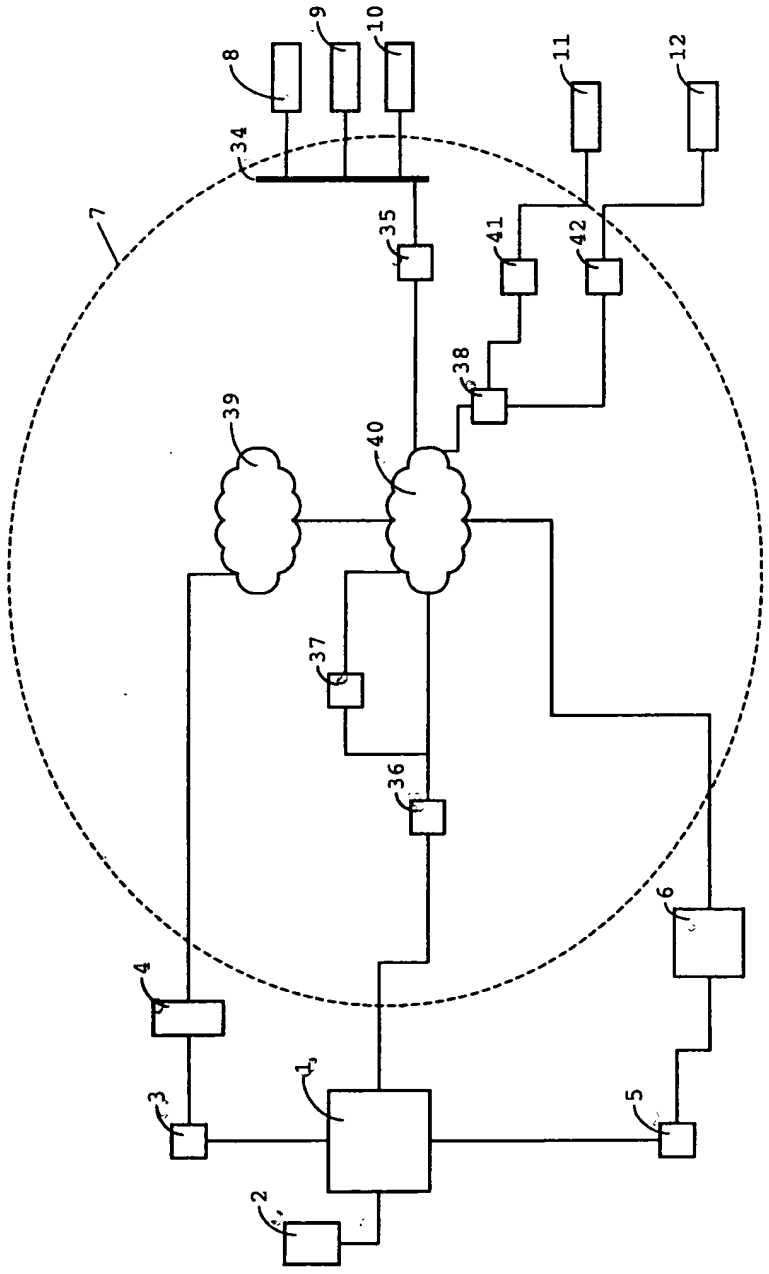
一註冊系統(1,2)，用以維護鏈接該些客戶端系統之各已註冊者至複數個群組之一相關者之群組資訊，及分派多播位址至該客戶端系統，使得關於一特定群組之所有客戶端系統具有一共用多播位址，

及

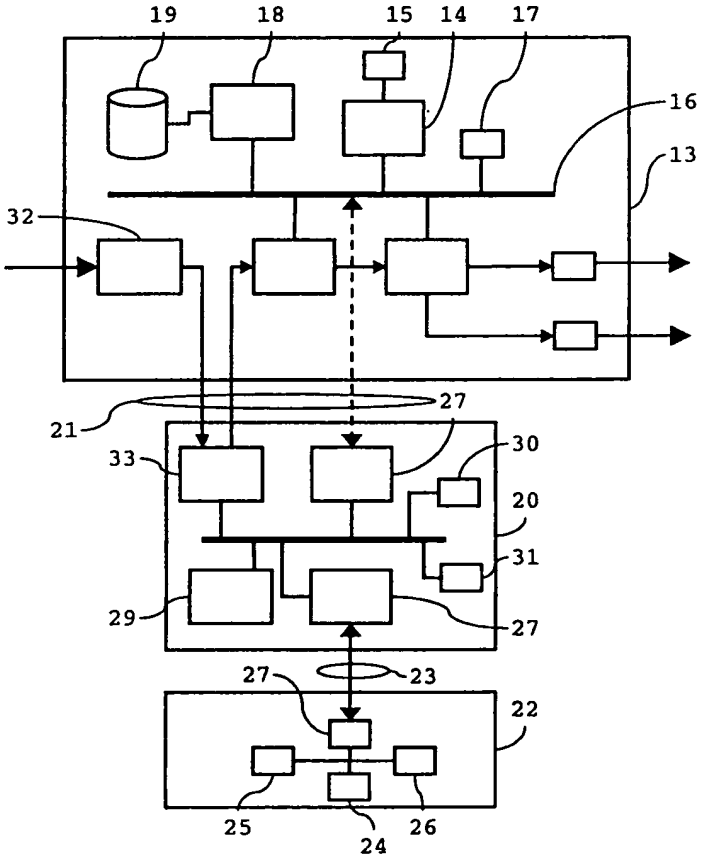
一伺服器(1)，配置以具有一多播位址之訊息多播該群組訊息至至少一該客戶端系統，各群組訊息意欲用於一群組中之

所有客戶端系統，該系統配置以根據申請專利範圍第 13-21 項中任一項實行一方法。

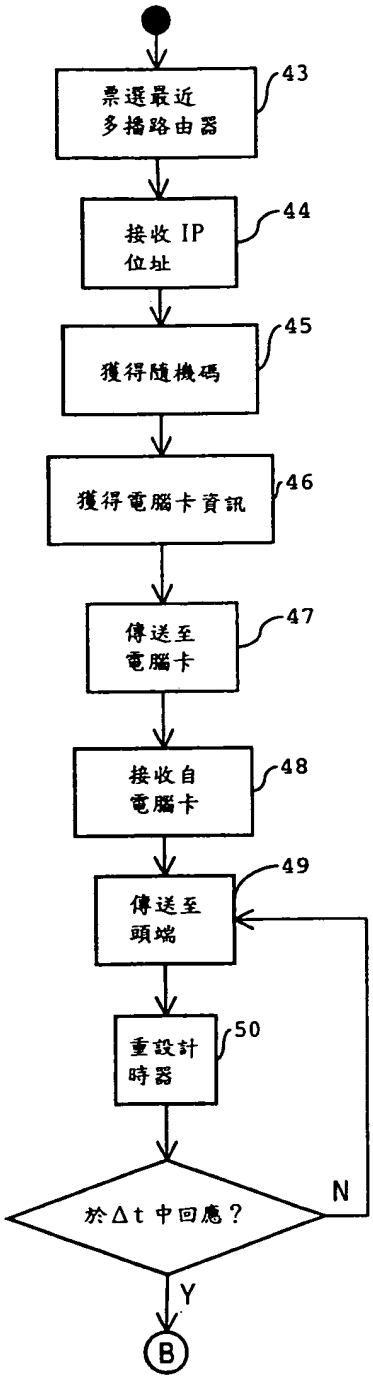
23. 一種配置當執行於一電腦(1;13;20)上時根據申請專利範圍第 1-10 或 13-21 項中任一項實行一方法之電腦程式。



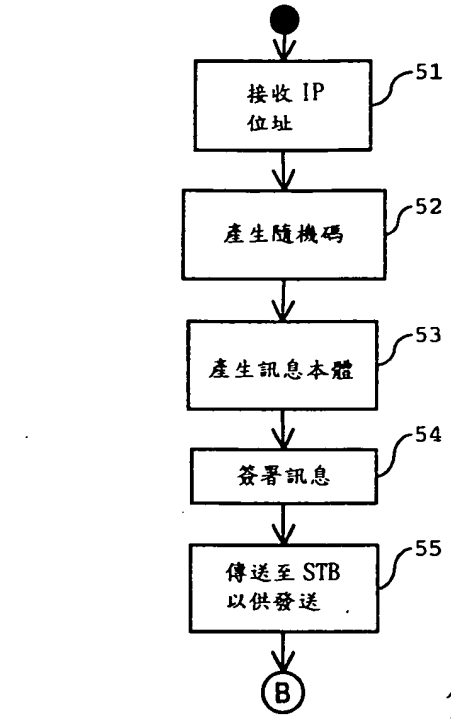
第一圖



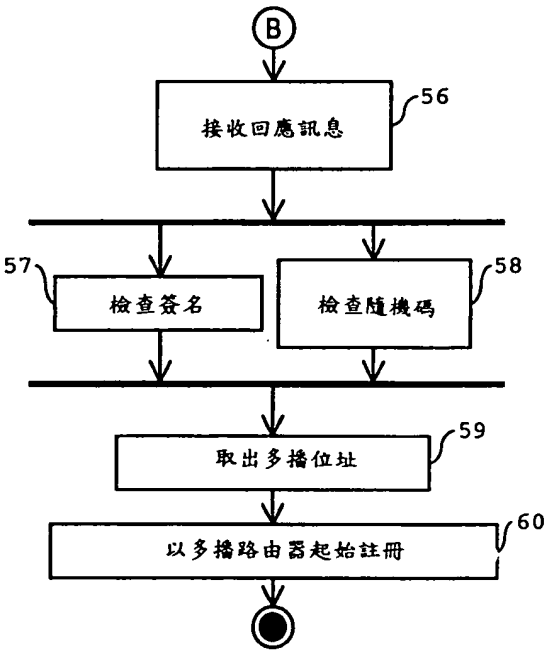
第二圖


43
票選最近多播路由器
44
接收 IP 位址
45
獲得隨機碼
46
獲得電腦卡資訊
47
傳送至電腦卡
48
接收自電腦卡
49
傳送至頭端
50
重設計時器
於Δt中回應？
N
Y
B

第三圖


接收 IP 位址
51
產生隨機碼
52
產生訊息本體
53
簽署訊息
54
傳送至 STB 以供發送
55
B

第四圖


B
接收回應訊息
56
57
檢查簽名
檢查隨機碼
58
取出多播位址
59
以多播路由器起始註冊
60

第五圖

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明:

1 CA 系統

2 用戶管理系統(SMS)

3 預先加密系統

4 隨選視訊(VOD)系統

5 擾亂系統

6 廣播伺服器

7 網際網路

8 整合接收器編碼器(IRD)

9 整合接收器編碼器(IRD)

10 整合接收器編碼器(IRD)

11 整合接收器編碼器(IRD)

12 整合接收器編碼器(IRD)

34 區域網路(LAN)

35 第一多播路由器

36 第三多播路由器

37 多播路由器

38 第四多播路由器

39 第一網路片段

40 第二網路片段

41 第五路由器

42 第六路由器

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：