(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201208302 A1
(43)公開日： 中華民國 101 (2012) 年 02 月 16 日

(21)申請案號：100115196 (22)申請日： 中華民國 100 (2011) 年 04 月 29 日
(51)Int. Cl.： *H04L12/46 (2006.01)*
(30)優先權：2010/04/30 美國 61/329,860
2010/08/30 美國 61/378,171
(71)申請人：麥可 牛頓 (英國) NEWTON, MICHAEL (GB)
英國
(72)發明人：牛頓 麥可 NEWTON, MICHAEL (GB)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：25 項 圖式數：11 共 60 頁

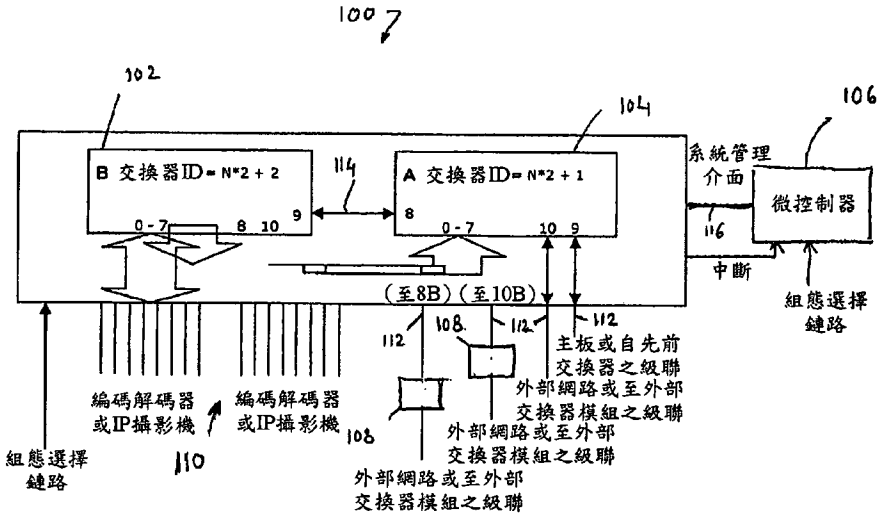
(54)名稱

網際網路協定封閉電路系統及方法

AN IP-CLOSED CIRCUIT SYSTEM AND METHOD

(57)摘要

本發明係關於一種用於產生並操作資料來源及監測台之安全網路且用於提供自公用網路對該等資料來源及監測台之受控存取的交換模組。



100：交換模組

102：交換器

104：交換器

106：微控制器/微控制器晶片

108：Gb 乙太網路實體連接器/裝置(PHY)

110：10/100 Mb 乙太網路埠

112：Gb 乙太網路埠

114：連接

116：串列管理介面(SMI)匯流排

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201208302 A1
(43)公開日： 中華民國 101 (2012) 年 02 月 16 日

(21)申請案號：100115196 (22)申請日： 中華民國 100 (2011) 年 04 月 29 日
(51)Int. Cl.： *H04L12/46 (2006.01)*
(30)優先權：2010/04/30 美國 61/329,860
2010/08/30 美國 61/378,171
(71)申請人：麥可 牛頓 (英國) NEWTON, MICHAEL (GB)
英國
(72)發明人：牛頓 麥可 NEWTON, MICHAEL (GB)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：25 項 圖式數：11 共 60 頁

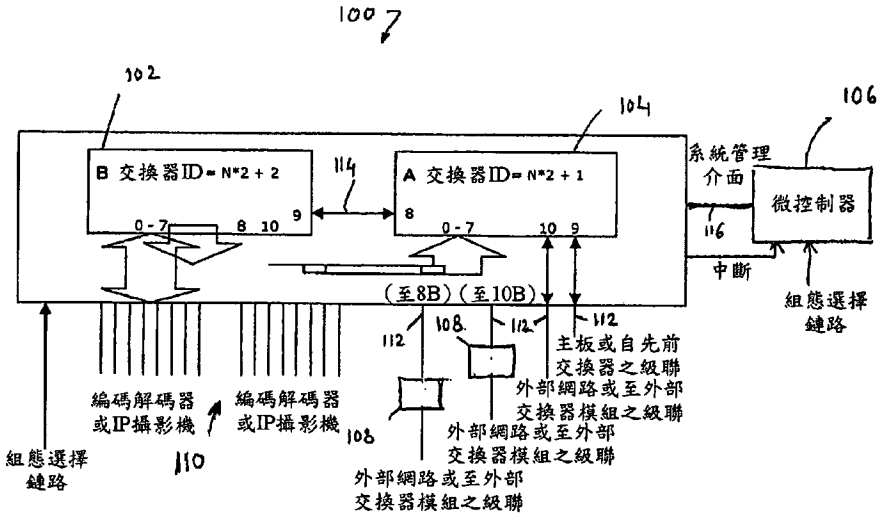
(54)名稱

網際網路協定封閉電路系統及方法

AN IP-CLOSED CIRCUIT SYSTEM AND METHOD

(57)摘要

本發明係關於一種用於產生並操作資料來源及監測台之安全網路且用於提供自公用網路對該等資料來源及監測台之受控存取的交換模組。



100：交換模組

102：交換器

104：交換器

106：微控制器/微控制器晶片

108：Gb 乙太網路實體連接器/裝置(PHY)

110：10/100 Mb 乙太網路埠

112：Gb 乙太網路埠

114：連接

116：串列管理介面(SMI)匯流排

六、發明說明：

【發明所屬之技術領域】

本發明係關於網際網路協定(IP)網路，且更特定言之，係關於封閉電路IP視訊(video-over-IP)網路。

本申請案主張2010年8月30日申請之美國臨時申請案第61/378,171號以及2010年4月30日申請之美國臨時申請案第61/329,860號的優先權，該等申請案之揭示內容以全文引用的方式併入本文中。

【先前技術】

閉路電視(CCTV)通常基於以下事實進行工作：可經由點對點類比連接來部署習知類比視訊攝影機以達成安全性及監視之目的，從而形成所部署攝影機之封閉且安全之網路。然而，可使用IP攝影機來促進經由TCP/IP網路之視訊傳輸。使用TCP/IP網路可促進高解析度傳輸，藉此改良所傳輸影像之品質，且可提供在寬廣地理區域上部署攝影機之能力。TCP/IP網路亦可用以產生與其他具備IP能力之端點裝置互連的封閉電路(CC)系統。此等裝置之實例包括：門禁讀卡器，其可准許在各種入口處進入一建築物；及警報器，其可監測特定狀況(例如，存在氣體之狀況)且向經由TCP/IP網路而連接之接收台發出警示。在以下論述中，為了便於論述，參考CCTV系統。然而，應理解，TCP/IP及IP-CC系統不限於TV系統，且可經組態為包括各種端點裝置(例如，門禁讀卡器、警報器等)。

然而，使用TCP/IP網路可對CCTV之管理及操作造成挑

戰，因為所傳輸之視訊資料可容易地被已知IP駭客技術攔截。駭客行為之可能性使CCTV-IP網路變得不安全。在部署於TCP/IP網路上時，對多個裝置(諸如，視訊伺服器及IP攝影機，其將被用作CCTV監視系統/視訊監測系統之部分)之識別及組態亦可為困難的。此係因為某些方法要求安裝者經由理解出現於動態主機組態協定(DHCP)伺服器上的裝置之媒體存取控制(MAC)位址來手動地逐一識別連接於網路上之該等裝置中之每一者。DHCP伺服器將接著分配一IP位址給該裝置，或者必須手動地分配IP位址。只有在對裝置之該識別及IP位址之分配之後，才可定位及控制該裝置。

此外，一IP佈線端點(在該IP佈線端點處，一攝影機可連接至一電纜)可能位於一受保護區外部。受保護區可為對於入侵者而言可能難以獲得存取權之區域，其使入侵者難以篡改攝影機。然而，在受保護區外部(例如，在建築物後面一定距離處之房屋)，入侵者可獲得對IP佈線端點之存取權且可安裝一不同之未授權裝置。該未授權裝置可將假視訊資料發送至TCP/IP網路中之一監測台，從而使網路易受攻擊。又，由於常常將系統之元件安裝至難以維護之位置(諸如，屋頂/高大建築物或CCTV攝影機柱上)，因此若可在不需要雇用平台/車載升降台(cherry picker)來存取該等裝置的情況下識別該等裝置並進行IP組態，則對於安裝者而言可為有利的。

一些方法(例如，DHCP選項82)可將IP位址分配給諸如IP

攝影機之裝置，且可經組態以使得一個埠與一個所分配之IP位址相關聯。因此，透過使用DHCP選項82，藉由准許對應於所分配IP位址之僅一子集的裝置之間的通信，可產生一安全網路。然而，依據DHCP選項82，組態每一埠至僅單一IP位址可為累贅的。此外，在准許兩個裝置之間的通信之前，DHCP選項82不提供IP位址授權。因此，除了使用DHCP選項82之外，亦必須實施授權IP位址及由此提供一安全網路之步驟。根據此等方法來操作一安全網路造成又一問題。舉例而言，網路中之一裝置並非可由其自身之識別符(諸如，媒體存取控制(MAC)位址)唯一地識別。若未授權裝置替代了連接至網路之經授權裝置，則該未授權裝置將簡單地使用分配給該經授權裝置之IP位址，且由此對於其他網路組件而言將看起來像是經授權的。

另外，使用此等方法來組態一安全網路可要求一特定IP位址分配方法，該特定IP位址分配方法可能與該網路所使用之其他分配方法並不相容。最後，對於大量埠而言，組態一網路交換器之埠以存取IP位址及相關聯之識別符以便基於該等識別符來路由接收到之資料訊框可為累贅的。

【發明內容】

在各種實施例中，本發明之特徵在於以一點對點方式連接至一或多個控制系統之裝置的一封閉IP網路，從而產生此等裝置之一安全網路。如本文中所使用，「封閉」意謂僅經組態為包括於該IP網路中之裝置可彼此交換資料。

本發明藉由產生一點對點隨插即用組態而解決了難以在

TCP/IP網路上組態多個裝置及攝影機(歸因於其位置)的問題。此部分地藉由以下方式而實現：將裝置(例如，攝影機)分配至網路埠且自動地將IP位址指派給該等裝置；及允許待部署為CCTV監視系統之部分的裝置以一確定性方式自動地配對，其中各別伺服器/記錄裝置不受安裝者或使用者之任何介入。確定性且裝置特定之資料管理可使得能夠確保TCP/IP網路之安全。

詳言之，具有預先分配之網路埠的交換模組可被建置至控制設備中。此等交換器可標記接收到之資料訊框，藉此允許將第3層交換器能力整合至應用程式中。接著，該應用程式可自動地將裝置或「端點」分配至該交換器之埠，且將一連接至一埠之裝置與該控制設備相關聯。此可得以實現而不需要進行在有可能將有關裝置連接至控制/記錄設備之前找到該裝置之以手動方式或DHCP方式分配之IP位址的冗長且充斥著缺陷之程序。如本文中所使用，「標記」意謂藉由將特定資訊添加至一資料訊框或將此資訊自一資料訊框移除而修改該資料訊框。

藉由使用埠、裝置/端點及控制設備之間的該關聯性，該等裝置與該控制設備可安全地彼此通信，從而產生裝置之一獨特拓樸，其可為在另一TCP/IP網路內之一安全網路。如本文中所使用，一安全網路指示該端點或連接至一埠之裝置為安全的，亦即，一埠與連接至該埠之裝置之間的關聯性不可更改。結果，形成一封閉IP TV網路，在該封閉IP TV網路中該等裝置(例如，攝影機)與該控制設備之

間可存在一實質上獨佔之關係。由此產生之封閉IP TV網路可立即開始串流傳輸並記錄視訊資料。

一交換模組可因此藉由提供嵌入式IP網路視訊記錄(NVR)而產生一針對標準解析度資料/視訊及高解析度資料/視訊兩者之完全基於IP之解決方案。可使用零組態網路連接(零組態(Zeroconf))或多播網域名稱系統(mDNS)來自動地發現IP攝影機。零組態為自動地產生一可使用IP網路而無操作者手動介入或特殊組態伺服器的一組技術。mDNS致能電腦主機名稱之自動解析及散佈。此外，該交換模組可提供整合之第2/3層交換器解決方案，從而致能按輸入連接器之確定性個別攝影機識別。

因此，可組態一點對點IP網路而不需要大量努力。組態IP攝影機可實質上為透明的，亦即，可能實質上並不需要具體瞭解該攝影機之IP位址或其他IP相關資訊。此組態可允許多型態串流傳輸及進階事件處置(例如，多模式)。舉例而言，作為一較高應用層，此組態提供順暢NetVu連接環境。可使用一預設防火牆設定來將該等IP攝影機實質上隔離於IP視訊存取，且額外之防火牆設置選項可允許深入整合至一用戶端之網路，同時維持高安全性等級。因此，該交換模組可提供一實質上安全且穩健之IP解決方案而不要求實質IP專業知識。

此外，攝錄一體機(ICR)可提供用於標準解析度及百萬像素之圖片、視訊及其他資料的完全IP基礎架構。一分散式IP/ICR架構可減小中央網路風險，同時提供強大之多螢

幕、多串流解碼器及高解析度顯示器。該架構可為一完全整合之集中式視訊管理系統(VMS)。

攝錄一體機(ICR)通常包括一企業級伺服器、本地儲存裝置及媒體，例如可使用基於乙太網路之ATA(AoE)技術而完全獨立於攝影機之IP狀態之固態磁碟機(SDD)或硬碟機(HDD)。由於多個攝影機可儲存所記錄之資料且可提供對此資料之存取，因此可實質上消除單一故障點，且高昂之網路基礎架構安裝及維護成本以及對網路之高可靠性要求可得以減小。此外，ICR可促進隨選檢視及管理、互補備份儲存，且可使用高解析度多媒體介面(HDMI)將視訊資料傳輸至高解析度檢視工作站。

ICR之多層儲存架構可提供與儲存媒體成比例之多個解析度及儲存選項。此可允許有效地平衡儲存要求與儲存成本。一嵌入於攝影機內之企業級伺服器可提供對警報處置、整合及中繼資料處理之支援，且充當一視訊管理工具。可使用組態指令碼靈活地將ICR與供暖通風與空氣調節(HVAC)系統及/或建築管理相整合。

本發明之特徵在於以一新穎且獨特之方式部署乙太網路訊框標記，該方式將第3層交換器能力整合至視訊伺服器應用程式中，該視訊伺服器應用程式自身允許裝置以安全方式確定性地發現彼此且自動地被分配至內建交換器內之埠。因此，可產生裝置之一獨特拓樸，其成為另一TCP/IP網路內之一完全安全之網路。

因此，在一態樣中，本發明係關於一交換模組，該交換

模組包括：一第一埠群組及一第二埠群組；及一控制單元，其用於組態每一埠群組中之該等埠。該第一埠群組包括至少一埠。該第一埠群組中之每一埠經組態以用於與一資料來源連接，且修改由該所連接之資料來源傳輸的一資料訊框。此藉由將經指派給該埠之一唯一埠號包括在該資料訊框中而實現。若經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯，則該埠將該經修改之資料訊框路由至該目的地埠。該第二埠群組亦包括至少一埠。該第二埠群組中之每一埠經組態以用於與一監測台連接，且用於接收由該第一埠群組中之該等埠中之一者修改的一資料訊框。該控制單元將一唯一埠號指派給該第一埠群組及該第二埠群組中之每一埠。其亦將一路由表指派給該第一埠群組中之每一埠。該路由表包括至少一來源埠號，及與該表中之每一來源埠號相關聯的至少一目的地埠號。

在各種實施例中，該交換模組之該資料來源包括一IP攝影機或一類比攝影機，及一編碼解碼器。該資料來源可為一編碼器，且一連接至該編碼器之裝置可為一IP攝影機、一類比攝影機，或一SDI攝影機。該資料來源亦可為一門禁讀卡器或一警報器。該監測台可包括用於檢視經由所連接之該埠而接收到之資料訊框的構件，及/或用於儲存經由所連接之埠而接收到之資料訊框的構件。在一些實施例中，該交換模組進一步包括一第三埠群組，該第三埠群組包括至少一埠。該第三埠群組中之每一埠可經組態以用於

與計算裝置之一私人網路連接。該控制單元可經組態以用於將一唯一埠號指派給該第三埠群組中之每一埠。該控制單元亦可致能該第三群組中之埠之間的資料訊框之通信、該第三埠群組中之一埠與該第一或第二埠群組中之一埠之間的資料訊框之通信，以及該第三群組中之一埠與該控制單元之間的資料訊框之通信。

在一些實施例中，該交換模組進一步包括一第四埠群組，該第四埠群組包括至少一埠。該第四埠群組中之每一埠可經組態以用於與計算裝置之一公用網路連接。該控制單元可經組態以用於將一唯一埠號指派給該第四埠群組中之每一埠。該控制單元亦可致能該第四埠群組中之埠之間的資料訊框之通信，及該第四群組中之一埠與該控制單元之間的資料訊框之通信。然而，該控制單元可阻止該第四埠群組中之一埠與該第一或第二埠群組中之一埠之間的資料訊框之通信。

在另一態樣中，本發明係關於一視訊裝置，該視訊裝置包括一攝影機、一儲存單元及一伺服器。該儲存單元與該攝影機通信以用於儲存由該攝影機記錄之資料訊框。該伺服器控制該攝影機及該儲存單元，且提供對所儲存之該等資料訊框的存取及傳輸。

在各種實施例中，該視訊裝置可進一步包括一埠單元，該埠單元經組態以用於接收一唯一埠號。該埠單元可藉由將該唯一埠號包括在一資料訊框中來修改由該攝影機傳輸之該資料訊框。額外地或替代性地，該視訊裝置可進一步

包括一交換模組。該交換模組可包括：一第一埠群組及一第二埠群組；及一控制單元，其用於組態每一埠群組中之該等埠。該第一埠群組包括至少一埠。該第一埠群組中之每一埠經組態以用於與一資料來源連接，且其修改由該所連接之資料來源傳輸的一資料訊框。此藉由將經指派給該埠之一唯一埠號包括在該資料訊框中而實現。若經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯，則該埠將該經修改之資料訊框路由至該目的地埠。該第二埠群組亦包括至少一埠。該第二埠群組中之每一埠經組態以用於與一監測台連接，且用於接收由該第一埠群組中之該等埠中之一者修改的一資料訊框。該控制單元將一唯一埠號指派給該第一埠群組及該第二埠群組中之每一埠。其亦將一路由表指派給該第一埠群組中之每一埠。該路由表包括至少一來源埠號，及與該表中之每一來源埠號相關聯的至少一目的地埠號。該攝影機使用該第一埠群組中之一個埠而連接至該交換模組。

在一些實施例中，該視訊裝置之該伺服器可藉由使用所連接之任何攝影機經由該埠來接收控制資訊。回應於接收到之該控制資訊，該伺服器可控制該控制單元。該視訊裝置之該第一埠群組亦可包括至少一輔助埠。一資料來源可連接至該等輔助埠中之一者。該資料來源可為一視訊攝影機。

在另一態樣中，本發明係關於一種用於操作一IP網路之方法。該網路可包括一交換模組，該交換模組包括：一第

一埠群組，其包括至少一埠；一第二埠群組，其包括至少一埠；及一控制單元。該方法包括：自該控制單元將一唯一埠號指派給該第一埠群組及該第二埠群組中之每一埠；及自該控制單元為該第一埠群組中之每一埠指派一路由表，該路由表包括至少一來源埠號及與該至少一來源埠號相關聯之至少一目的地埠號。該方法亦包括：將一資料來源連接至該第一埠群組中之該至少一埠；對由該資料來源傳輸之一資料訊框進行授權；及修改該經授權之資料訊框。若經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯，則該經修改之資料訊框可為到該目的地埠的。該方法進一步包括：將一監測台連接至該第二埠群組中之該至少一埠；及在該監測台處接收由該第一埠群組中之至少一埠修改的一資料訊框。

在各種實施例中，在該方法中對一資料訊框進行授權包括將該資料訊框中之一裝置來源號與該唯一埠號進行比較。該方法可進一步包括以下步驟：阻止一未授權資料訊框之傳輸；及將接收該未授權資料訊框之該埠之該唯一埠號傳達至該控制單元以用於阻塞經由該埠之存取。該第一埠群組中之一埠的唯一埠號可包括連接至該埠之資料來源的一裝置來源號。該第二埠群組中之一埠的唯一埠號可包括連接至該埠之監測台的一裝置來源號。

在一些實施例中，該操作一IP網路之方法亦包括：在該第一群組中之一埠處儲存與連接至該埠之該資料來源相關聯的一安全參數。該安全參數可為與該所連接裝置相關聯

之一唯一識別符，及/或由該埠或交換器基於該唯一識別符或該所連接裝置之另一性質而產生的一密鑰。該密鑰可隨機產生，且亦可用以對該等資料訊框進行加密。該唯一識別符亦可為在一特定時段期間所接收及/或傳輸之資料訊框的數目。該方法亦包括在該資料來源處儲存一相應安全參數，該安全參數可為該唯一識別符、密鑰，或如上文所描述之該等相應計數。

該方法進一步包括接收該相應參數並將其與儲存於該埠處之該安全參數相比較以判定該埠處是否存在一未授權裝置。最後，該方法包括：若該比較失敗(亦即，經判定存在一未授權埠)，則在一預定時段內停用該埠以阻止自該未授權裝置進行之資料傳輸。當經判定存在一未授權埠時，亦可藉由發送一諸如一電子郵件或警報之警示來向管理員報告一違規行為(violation)。該報告亦可包括在偵測到一來路不明的裝置之存在的該埠處接收到的非受信任資料訊框。

參考以下描述、隨附圖式及申請專利範圍，此等及其他目標連同本文中所揭示之本發明之優點及特徵將變得顯而易見。此外，應理解，本文中所描述之各種實施例之特徵並非互相排斥，而是可以各種組合及排列之形式存在。

【實施方式】

在諸圖中，相同參考字元貫穿不同視圖大體上指代相同部件。又，該等圖式不必按比例描繪，而是重點大體上在於說明本發明之原理。在以下描述中，參看以下圖式描述

本發明之各種實施例。

圖1及圖2中所展示之例示性系統包括：一交換模組100，其包含一對交換器102、104(例如，Marvell 88E6097交換器)；及根據需要之附屬組件，包括一設置微控制器106及Gb乙太網路實體連接器/裝置(PHY)108。僅出於說明之目的而使用交換器88E6097，且應理解，可對接收到之資料訊框加標記的任何交換器皆在本發明之範疇內。此模組提供16個10/100 Mb乙太網路埠110，及四個Gb乙太網路埠112。該等10/100 Mb埠110可具有嵌入式PHY，且Gb埠112可能要求使用外部PHY裝置。該等兩個交換器裝置藉由使用無PHY裝置之Gb埠的直接串列器/解串器(serdes)連接114來互連。

該交換器可包括許多可組態特徵，可經由內部暫存器來程式化該等特徵。可由一微控制器晶片106經由一雙線串列管理介面(SMI)匯流排116載入該等交換器之開機組態，但可經由使用可經路由至每一裝置之埠9中的特殊乙太網路控制訊框來查詢及更新設定。此埠可連接至視訊伺服器之主板中央處理單元(CPU)，以直接用於第一模組之第一交換器。如圖3中所說明，其展示了兩個模組302、304之組態300，控制訊框亦可被間接地經由中間交換器路由以用於第一模組之第二交換器以及用於任何級聯模組之兩個交換器。

如圖3中所展示，一個別SMI匯流排316可用於交換模組302、304中之每一者，從而允許微控制器306使用一較快

速之暫存器存取協定。此可要求該等裝置兩者之交換器ID值由開機ID鏈路設定為零。微控制器306可隨後在該組態程序期間指派該等操作交換器ID。可藉由通用輸入輸出(GPIO)線上之組態選擇鏈路來將模組ID號N設定至微控制器中；接著可使用值2×N+1及2×N+2來設定交換器ID。可不啟用交換器裝置之外部乙太網路埠直至該組態程序已完成，因此在網路上可能看不到交換器ID零。

一中斷線318可自該等交換器晶片中之每一者連接至微控制器；有可能由來自主板CPU之控制訊框觸發該中斷。此可用以請求微控制器自交換器讀回暫存器值，以使得其可記錄下可能已遠端地作出之組態改變。視情況而定，一網路位址轉譯(NAT)路由器單元或一狀態封包檢查防火牆(SPI)單元可包括於交換器模組內。

如圖3中所展示，一交換器晶片可在其埠連接之間路由乙太網路訊框。當在一輸入埠處接收到一訊框(進入)時，可應用若干規則(亦即，訊框路由規則)以根據交換器之暫存器設定來判定該訊框可能被輸出至何處(離開)。為了應用訊框路由規則，交換器模組通常在每一乙太網路訊框內插入額外資料欄位(已知為標記)。視埠進入及離開規則而定，可在該等訊框之進入及離開之時自動地插入及移除此等標記，或可在訊框位於晶片外部時將該等標記應用於該等訊框以便支援多個交換器晶片之互連。亦可在組態了埠之後(亦即，如上文所描述，在已為埠指派了唯一編號之後)使用標記，以將特定MAC位址限制於特定埠。此可藉

由確定性埠指派而提供MAC級存取控制清單(ACL)操作，而不要求大量的操作者具體知識。

一典型乙太網路訊框格式為如下：

6個位元組	目的地位址
6個位元組	來源位址
2個位元組	乙太網路類型
n個位元組	有效負載資料

當一乙太網路資料訊框由一交換器晶片接收到時，其可藉由插入如下所示之標記資料來修改訊框格式：

6個位元組	目的地位址
6個位元組	來源位址
2個位元組	標記類型旗標/來源晶片ID/來源埠號
2個位元組	優先權/VLAN ID
2個位元組	乙太網路類型
n個位元組	有效負載資料

如圖1及圖4中所展示，在單一模組交換器組態中，來源晶片ID可由晶片之組態鏈路來設定，且來源埠號可為訊框進入於之實體埠之編號。可為交換器埠110、112中之每一者設定優先權及虛擬區域網路ID(VLAN ID或VID)值。此等值可用以設定來自特定埠之訊務的優先權，且用以限制訊框之路由以使特定埠之間的訊務與其他埠之間的訊框相互之間保持私密。標記類型旗標可用以表示標記格式上之特殊變化(如下文所描述)。

如圖3及圖5中所展示，在多個模組交換器組態中，用於晶片互連之該等埠可經組態成一「散佈式交換器架構」模式。在此模式中，在一訊框離開時可不將標記資料自該訊

框移除，且可假定該標記資料在訊框進入時已存在。來源晶片ID及來源埠號欄位可接著識別一訊框自外部網路首次進入該系統時所在之實體晶片及埠，且優先權及VLAN ID值可提供對在整個擴展交換器網路中操控該訊框之控制。在一實施例中，其中一來源晶片ID可為5位元之欄位且為了特殊目的而保留值0x00及0x1F，可互連最多30個晶片。

如下文所展示，當一CPU可直接連接至交換器時，可使用一擴展標記格式。

6個位元組	目的地位址
6個位元組	來源位址
2個位元組	使用者選定之標記規格符(tag specifier)值
2個位元組	保留-始終為零
2個位元組	標記類型旗標/來源晶片ID/來源埠號
2個位元組	優先權/VLAN ID
2個位元組	乙太網路類型
n個位元組	有效負載資料

標記規格符值欄位可用以指示該訊框是否含有一標記或是否為一普通乙太網路訊框。在正常(亦即，未加標記)訊框中，在乙太網路類型欄位中通常僅使用特定值(例如，0x800=IPv4訊框，0x0806=位址解析協定(ARP)訊框，0x88A2=基於乙太網路之進階科技附件(ATA)(AoE)訊框)。交換器可經程式化以辨別一特殊值作為以下情形之指示：包括標記資料且實際的乙太網路類型欄位在8個位元組之其他資料之後。一特殊值之一實例可為0xAD01，其通常不作為任何正常乙太網路訊框之乙太網路類型出現。

當一交換器埠經組態以辨別一標記規格符值時，加標記

之乙太網路訊框及正常乙太網路訊框兩者皆可按任何序列進入。若位元組13至14具有一特殊標記規格符值，則位元組17至20可經解譯為標記資訊；否則，可將訊框視為未加標記，且可根據晶片/埠之編號及該埠之預設優先權/VLAN ID設定來自動地插入標記資料。

此組態允許CPU起始訊框，可藉由以不同VID值對不同訊框加標記來將訊框操控至特定出口埠。可使用入口埠之預設規則來操控普通訊框(亦即，未加標記之訊框)。該等預設規則可由CPU提供。此外，離開交換器至CPU之該等訊框內的來源晶片/埠ID欄位可允許CPU識別每個訊框之原始實體埠。詳言之，來自經由每一交換器晶片之埠0至7而連接之編碼解碼器或IP攝影機的資料訊框可與實體連接相關聯，而無需專門瞭解每一編碼解碼器/IP攝影機之乙太網路來源位址或IP位址。

CPU亦可使用標記類型旗標位元之特殊設定，如下所示：(a)設定11b，亦即，前向散佈式交換器架構(DSA)標記，其可暗示來自/至CPU之正常資料訊框，或自一交換器晶片至另一交換器晶片之正常資料訊框；(b) 00b，亦即，至CPU DSA標記，其可暗示可由CPU接收之控制/管理訊框；(c) 01b，亦即，來自CPU DSA標記，其可暗示由CPU發送之控制/管理訊框；及(d) 10b，亦即，至嗅探器 DSA標記，其可暗示訊框至一指定監測器埠之鏡像。

該等至/來自CPU DSA標記格式可用以將暫存器讀取/寫入命令發送至交換器晶片且自交換器晶片接收狀態資訊。

在來自CPU格式中，來源晶片ID欄位可用作一目的地晶片ID，從而允許CPU將命令發送至擴展交換器組態內之任何晶片。由於安全性原因，交換器晶片僅可接受經由一特定實體埠(例如，經由埠9抑或埠10)進入之命令訊框，該特定實體埠係在開機時藉由微控制器程式化而選定。在一些實施例中，埠9為一用於與CPU互連之較佳埠，且可經組態為交換器模組之一控制埠。

一用於所有訊框之典型預設路由演算法如下所示：(a)在每一訊框進入時，可將MAC來源位址(SA)與實體埠號一起儲存於交換器之位址轉譯單元(ATU)中。此可為一雜湊查找表，其可容納多達8192個輸入項。假定將經由同一實體埠來接收具有一給定SA之所有訊框。若在一特定時間段(例如，5分鐘)內不重新使用ATU內之輸入項，則該等輸入項將老化；(b)為了決定一單播乙太網路訊框之出口埠，可檢查ATU以查找一匹配MAC目的地位址(DA)之輸入項。若找到一輸入項，則此可給出自此MAC位址接收到之訊框先前進入於的埠號；此埠可接著用於該訊框之離開。若未找到任何輸入項，則無法知曉哪一埠將通向所需目的地，且該訊框可自所有埠(除了其最初進入時所在之埠)離開；(c)廣播乙太網路訊框可自所有埠(除了其最初進入時所在之埠)離開；及(d)視ATU內之特殊輸入項而定，多播乙太網路訊框離開至一或多個埠。然而，不同於單播訊框(其中，ATU可自動地藉由檢查經過之訊框的SA而得知其輸入項)，可能必須自微控制器及/或CPU手動地載入針對多播

位址之輸入項。

該預設路由演算法可由暫存器設定修改，該等暫存器設定基於實體埠號而組態虛擬區域網路(VLAN)。在未使用基於埠之VLAN設置的情況下，進入任一埠之訊框可經由任一其他埠離開。當使用基於埠之VLAN設置時，對於每一入口埠，通常存在所允許之出口埠的個別清單。進入/離開規則不需要為對稱的，例如，有可能組態一允許訊框自埠0流至埠1但不允許自埠1流至埠0之VLAN。

除了ATU路由之外，亦可操作基於埠之VLAN路由。因此，廣播訊框之出口可限於視入口埠而非所有埠而定的埠之選擇。單播/多播訊框之出口可由ATU中之輸入項來判定，但可能根據VLAN規則而阻塞特定埠(亦即，訊框不可自一被阻塞埠離開)。

可在使用「散佈式交換器架構」方法直接互連之多個交換器晶片上操作基於埠之VLAN。此處，當訊框在晶片之間通過時，可在標記資訊內保存每一訊框之原始來源裝置及埠之編號，且可參考原始晶片/埠之ID值來進行每一晶片內之路由。舉例而言，若一訊框進入至晶片1之埠2，則基於埠之VLAN規則可能將其出口限制為彼晶片之僅埠7及埠8。若埠8連接至晶片2，則可能限制該訊框僅在第二晶片之埠5及埠6處離開。但若一訊框最初進入至晶片1之埠3，且類似地經由晶片1之埠8而轉遞至晶片2，則彼訊框可能被限制為僅經由第二晶片之埠7離開。

基於埠之VLAN可提供將一網路複雜地分割成若干個虛

擬LAN，其中可在每一VLAN群組內保持訊務私密。然而，此等VLAN不允許逐訊框地改變用於個別訊框之群組。可進一步藉由對訊框加VLAN ID標記而修改預設訊框路由及訊框之基於埠之路由。當一正常乙太網路訊框首次進入多晶片交換器系統時，可藉由插入如上文所描述之標記資料來對其進行修改。此包括一VLAN ID(VID)值，可針對每一晶片之每一埠個別地設置該VID值。在一實施例中，可准許4094個不同VID值。若一訊框經由一CPU-交換器直接連接埠而進入交換器中，則CPU可對該訊框預先加標記，從而允許視所要訊框目的地而定逐訊框地設定VID。

當訊框在按「散佈式交換器架構」模式連接之交換器晶片之間轉送時，可保存來自原始入口埠之標記資料，由此，訊框中之原始VID值可保持不被修改直至訊框最後離開至一正常網路埠為止。在每一交換器晶片內，可存在與每一可能VID值相關聯之埠號的清單。一經標記有一特定VID之訊框僅可經由針對彼VID列出之埠而離開。

除了基於埠之VLAN規則及訊框之正常ATU路由之外，基於VID之VLAN規則亦可操作。舉例而言，由CPU起始之訊框及晶片1之入口埠9可由基於埠之VLAN規則限制為僅經由晶片1之埠0至埠7或晶片2之埠8或埠10而離開。VID規則可進一步指定：僅VID=1訊框可經由晶片1之埠0至埠7而離開，僅VID=2訊框可經由晶片2之埠8而離開，且僅VID=3訊框可經由晶片2之埠10而離開。對於非廣播訊

框，正常ATU規則亦可適用，其使得可根據特定MAC目的地位址來篩選VID=1訊框之出口，亦即，VID=1之任何特定訊框僅可自晶片1之埠0至埠7中之一具有ATU中之匹配MAC位址的埠離開。一IP攝影機亦可經組態以使得其可指定/改變正傳輸之訊框的VID。

在圖4中所展示的根據本發明之一系統之一實施例中，一用於視訊記錄器/伺服器之模組400可包括兩個交換器402、404。該模組可經組態以為16個編碼解碼器或IP攝影機110提供連接。至公用乙太網路之連接412，及至私人視訊網路或級聯至擴展交換器模組的兩個連接414、416。在開機時，預設交換器設定(其可由微控制器設定)假定埠8B及埠10B之連接將至一外部私人視訊網路。在CPU啟動及網路組態程序期間，可將命令發送至交換器以偵測是否事實上此等埠中之任一者正用作級聯以連接至一或多個額外交換器，且因此，可修訂該等交換器設定。

在圖4中所展示之模組400中，可產生五個單獨網路區，如下所示：外部公用網路、外部私人視訊網路、IP攝影機/編碼解碼器連接、主板連接，及內部交換器間連接。可使用基於埠之VLAN規則及對乙太網路訊框之VID標記來強制執行此等網路區之間的訊務之正確路由。舉例而言，來自編碼解碼器/IP攝影機之訊框通常最初未加標記；可在該等訊框進入交換器模組時使用VID=1對此等訊框加標記。可將來自公用網路之訊框始終視為未加標記，且可在其進入交換器模組時使用VID=2來加標記。亦可將來自私人視

訊網路之訊框視為未加標記，且可在其進入交換器模組時使用VID=3來加標記。來自主板之訊框可為未加標記的或是預先加標記的。可使用VID=4來對任何未加標記之訊框(例如，來自啟動載入程式碼之訊框)加標記。可使用VID=5對來自一應用程式之預先加標記之訊框加標記。經過交換器間連接之訊框可保留其在首次進入模組中時接收到之VID值。

訊框可接著以如下所示之方式離開：VID=1之訊框(亦即，來自編碼解碼器/IP攝影機之訊框)可離開至編碼解碼器/IP攝影機、私人網路或主板CPU。VID=2之訊框(亦即，來自公用網路之訊框)可被允許離開至公用網路或主板CPU。VID=3之訊框(亦即，來自私人網路之訊框)可離開至編碼解碼器/IP攝影機、私人網路或主板CPU。VID=4之訊框(亦即，來自主板CPU之訊框)可被允許離開至公用網路或主板CPU。此等訊框可包括待由一公用網路上之電腦檢視的視訊資料。VID=5之訊框(亦即，來自主板CPU之訊框)可離開至編碼解碼器/IP攝影機或私人網路。此等訊框可包括控制資訊(例如，搖攝、縮放等)。注意，可藉由每一交換器之位址資料庫內的已知位址(如上文所述)將單播訊框操控至正確之目的地埠。VID/埠VLAN路由規則可進一步限制用於未知位址及用於廣播/多播訊務之可能路由。

在以下之表中展示典型開機設定。應理解，表中所描述之設定僅為說明性的，且埠之其他設定在本發明之範疇

內。

埠0A至7A(用於至編碼解碼器或IP攝影機的連接)	
	正常網路入口模式，在內部使用VID=1、SID=1、PID=埠號對訊框加標記。
	正常網路出口模式，將內部標記自訊框移除。
	基於埠之VLAN路由規則，允許進入訊框離開埠0A至7A(前往其他編碼解碼器/IP攝影機)、埠8A(前往其他交換器晶片)及埠9A(前往主板CPU)。埠10A出口為阻塞的(訊框無法前往公用網路)。
埠8A(級聯至交換器B)	
	DSA標記入口模式；所有訊框含有自交換器B傳遞之標記資訊。
	DSA標記出口模式；所有訊框含有傳遞至交換器B之標記資訊。
	允許進入之訊框基於上文詳細描述之VLAN路由規則在根據VID之埠處離開。
埠9A(用於至主板CPU的連接)	
	乙太網路類型DSA標記入口模式；含有擴展標記資訊之訊框保持其現有VID/SID/PID值，在內部使用VID=4、SID=1、PID=9對尚不含有標記資訊之訊框加標記。此允許CPU用其他VID值注入用於交換器暫存器之讀取/寫入的預先加標記之控制訊框，及預先加標記之正常資料訊框。
	針對所有訊框之乙太網路類型DSA標記出口模式，使用來自內部標記之資訊來產生擴展標記。此允許CPU看到所有接收到之訊框的VID/SID/PID。
	允許進入之訊框基於上文詳細描述之VLAN路由規則在根據VID之埠處離開。
埠10A(用於至外部公用網路的連接)	
	正常網路入口模式，在內部使用VID=3、SID=1、PID=10對訊框加標記。
	正常網路出口模式，將內部標記自訊框移除。
	基於埠之VLAN路由規則，允許進入訊框離開埠8A(前往其他交換器晶片)及埠9A(前往主板CPU)。埠0A至7A出口為阻塞的(訊框無法前往編碼解碼器/IP攝影機)。
埠0B至7B(用於至編碼解碼器或IP攝影機的連接)	
	正常網路入口模式，在內部使用VID=1、SID=2、PID=埠號對訊框加標記。
	正常網路出口模式，將內部標記自訊框移除。
	基於埠之VLAN路由規則，允許進入訊框離開埠0B至7B(前往其他編碼解碼器/IP攝影機)、9B(前往其他交換器晶片)、8B及10B(前往私人視訊網路)。
埠8B及10B(用於至外部私人視訊網路的連接，但允許偵測至其他交換器模組之級聯)	
	乙太網路類型DSA標記入口模式；含有擴展標記資訊之訊框保持其現有VID/SID/PID值，在內部使用VID=3、SID=2、PID=埠號對尚不含有標記資訊之訊框加標記。

	針對控制訊框之乙太網路類型DSA標記出口模式，使用來自內部標記之資訊來產生擴展標記。針對所有其他訊框之正常網路出口模式，捨棄內部標記資訊。
	允許進入之訊框基於上文詳細描述之VLAN路由規則在根據VID之埠處離開。
埠9B(自交換器A級聯)	
	DSA標記入口模式；所有訊框含有自交換器A傳遞之標記資訊。
	DSA標記出口模式；所有訊框含有傳遞至交換器A之標記資訊。
	允許進入之訊框基於上文詳細描述之VLAN路由規則在根據VID之埠處離開。

一啟動作業系統中之乙太網路驅動程式碼(例如，啟動載入程式碼)可經修改以移除(且捨棄)來自傳入訊框之任何擴展標記資訊，該資訊如由乙太網路類型欄位之位置中的0xAD01值來指示。在此位置處之任何其他值的情況下，可將訊框不改變地傳遞至TCP/IP堆疊。此交換器組態可允許主板與公用網路連接之間的自由資料傳送，而啟動作業系統不需要知曉交換器模組之存在。不需要對交換器進行任何動態組態來允許正常啟動操作，亦即，DHCP/ARP/TCP等可在無除了如上文所描述之低層級乙太網路驅動程式中之單一改變以外的其他程式碼修改的情況下操作。注意，具有此修改之Redboot亦可在一直接連接至公用網路之主板上(亦即，在不存在交換器模組時)正確地操作。

根據上文所描述之組態，訊框不能自埠10A傳遞至埠0A至7A，且反之亦然，此被基於埠之VLAN路由規則禁止。訊框可經由交換器間鏈路自埠10A傳遞至交換器B，但基於VID之VLAN路由規則可接著阻止其離開至埠0B至7B或私人網路埠。注意，此亦可在基於埠之路由中實現，其中來源埠ID將保留在訊框中，且接著交換器B之入口埠將應

用埠10A之規則。因此，在公用網路與私人視訊網路之間自動地強制執行一完全防火牆，即使在啟動作業系統之控制下操作時及在無任何特定交換器模組監督軟體處於作用中時亦如此。結果，由公用網路上之攻擊者進行的訊框標頭詐騙方法不可提供對私人視訊網路上之裝置的存取。

然而，可自由地允許埠0A至7A中之任一者與埠0B至7B中之任一者之間的訊務(經由埠8A至9B交換器間鏈路)，且亦可自由地允許此等埠中之任一者與私人網路連接埠8B及10B之間的訊務。當IP攝影機(而非編碼解碼卡)連接至埠0A至7A、0B至7B中之任一者時，此組態允許其甚至在主板應用程式啟動之前亦可正常地操作。舉例而言，即使主視訊伺服器不在作用中，亦可自一連接於私人視訊網路上之解碼器單元來瀏覽IP攝影機。

當一端點/裝置(例如，具有一編碼解碼器之IP攝影機或類比視訊攝影機)連接至一埠時，將一與該裝置相關聯之唯一識別符(諸如，該裝置之MAC位址)記錄在該埠中。一旦記錄了每一埠之裝置識別符，系統即「鎖定」，亦即，所記錄之識別符隨後僅可由一經授權應用程式改變。在鎖定之時，該等裝置/端點變為安全端點或受信任端點。在正常操作期間，該埠僅在與一所連接裝置相關聯之唯一識別符匹配該埠中所儲存之識別符的情況下接收並路由來自該裝置之資料訊框。在識別符失配之情況下，該埠及/或交換器偵測到一不同之未授權裝置連接至該埠，且該埠忽略接收到之資料訊框。因此，該封閉網路亦變得安全，因

入口埠確保了經由該網路而路由之資料訊框係接收自一安全或受信任端點。

在一些實施例中，可能有必要提供對一些裝置/端點之受限存取，而並非在公用網路與私人視訊網路之間形成一完全防火牆。在彼情形下，關鍵在於偵測到對連接至一埠之裝置的任何篡改，以便確保私人網路僅接收經授權資料。即使在授予一端點/裝置之存取權被限制的情況下，亦存在冒充與該裝置相關聯之唯一識別符(例如，MAC位址、IP位址等)的風險。若裝置之唯一識別符被冒充，則其將與交換器/埠中之所記錄之識別符相匹配。因此，該交換器/埠將不會偵測到該未授權之裝置。

為了實質上消除或減輕識別符冒充之風險，實施主動式監測方案以確保僅安全裝置連接至交換器。在一實施例中，在鎖定之時，由交換器產生一對應於受信任端點之唯一密鑰，且將其儲存於該交換器中及該受信任端點處。額外地或替代性地，將該密鑰儲存於一IP主機(例如，主電腦或另一受信任端點，甚至未授予對其的有限存取權)處。藉由使用MD5雜湊對裝置之MAC位址進行加密來產生該唯一密鑰，且其可隨機地產生。除了裝置之唯一識別符以外，亦可使用其他加密方法及/或裝置參數來產生該唯一密鑰。該唯一密鑰經組態以使得實質上不可自公用網路存取該唯一密鑰，即使該公用網路可具有對產生該密鑰所針對之安全端點的受限存取權。

在鎖定之時，編譯關於所有已知、允許且連接之IP位址

的聲明(manifesto)。藉由使用該聲明，定期及/或按隨機時間間隔輪詢該等安全端點，以請求其各別唯一密鑰。即使一連接至一埠之來路不明的裝置冒充唯一識別符，其亦不可具有在鎖定時由交換器供應之正確唯一密鑰。因此，若由一端點傳輸之密鑰不匹配交換器中及/或IP主機處所儲存之密鑰，則可判定該端點為來路不明的。

在一些實施例中，該裝置可在所傳輸之資料訊框之標頭中包括該唯一密鑰。為了限制網路訊務負載，該唯一密鑰可包括在僅一些而非全部資料訊框中。與上文類似地，若標頭中之唯一密鑰不匹配交換器中所儲存之密鑰，或若在預期之時未接收到密鑰，則可將發送該資料訊框之裝置識別為未授權的。在其他實施例中，該密鑰可用以對由一受信任端點/裝置傳輸之資料訊框進行加密。若一未授權裝置發送資料訊框至一埠，則不會使用提供給經授權裝置之唯一密鑰來對彼等資料訊框進行加密，且因此，交換器及/或埠將辨別出接收到之資料訊框並非由一經授權來源傳輸。

在一實施例中，藉由組態一安全端點以監測網路訊務以偵測另一裝置是否正進行詐騙(亦即，將該端點之唯一識別符傳輸至交換器)來實現主動式監測。在彼情況下，受信任端點可發送一警示信號至交換器。

一安全端點亦可儲存進入及離開該端點之資料訊框的計數。定期地及/或按隨機時間間隔，交換器可向端點輪詢所儲存之計數，且將接收到之值與交換器所保留之各別計

數相比較。若一未授權裝置成功地將資料訊框傳輸至交換器，則交換器處之計數值將不匹配自受信任端點接收到之計數值，由此告知該交換器在計數值發生不匹配之埠處存在未授權裝置。

根據上文所描述之各種實施例，在一特定埠處存在一未授權裝置的情況可由交換器偵測到。然而，交換器可能不能夠定位惡意裝置，從而無法阻止其發送資料。為了阻止來自來路不明的裝置之其他干擾，交換器可將偵測到惡意裝置之埠與公用網路及/或私人網路隔離開。交換器亦可將該埠完全隔離歷時一特定持續時間，在一預定時間間隔之後重新檢查該埠之狀態及其對輪詢之回應，且重新建立其連接。該埠及/或交換器亦可在偵測到一未授權埠時產生一系統事件(例如，電子郵件、警報等)，從而警示系統管理員採取可能必要之進一步動作以保護網路。

應用程式中之乙太網路驅動程式碼可經修改以將任何擴展標記資訊自傳入訊框移除。然而，可維持對應於乙太網路來源位址之交換器ID(SID)/埠ID(PID)值的快取區。VID值可用以將訊框經由若干虛擬乙太網路介面頻道而路由至TCP/IP堆疊。TCP/IP堆疊之上層可接收正常網路訊框，然而根據VID值，該等訊框看似已經過了多個介面。

若來自TCP/IP堆疊之傳出訊框係源自虛擬乙太網路第零號頻道，則可將其作為正常網路訊框傳輸。對於其他虛擬頻道，可傳輸插入有含有適當VID值之擴展標記資訊的訊框。可藉由自一交換器驅動應用程式直接呼叫乙太網路驅

動程式來產生交換器控制訊框，且此等訊框通常繞過TCP/IP堆疊。

現有應用程式之網路程式碼可在無關於主板與公用網路之間的訊務之修改的情況下操作。該應用程式不需要任何交換器感知(switch-awareness)來實現DHCP/ARP/TCP等之正常操作。應用程式組建亦可在直接連接至公用網路之主板上(亦即，在不存在交換器模組之情況下)正常地操作。

交換器感知應用程式碼可藉由檢查SID/PID/SA值之乙太網路驅動程式快取區以查看正接收之傳入訊框是否具有標記來檢查交換器模組之存在。若不存在傳入訊框(介面連接似乎為可操作的，但不接收訊務)，則可發送控制訊框以判定是否存在來自交換器之回應。若在不存在交換器之情況下將此等訊框傳輸至一公用網路，則該等訊框可不影響此網路。訊框中之0xAD01標誌(亦即，標記規格符值)可能僅對於特殊組態之交換器具有意義。所有其他設備(即使含有一交換器晶片)可忽略該等控制訊框。

當已確認存在一第一乙太網路交換器模組時，可發送出控制訊框以偵測可能經由埠8B及10B級聯連接而連接之第二模組及隨後模組的存在。若偵測到額外交換器，則可修訂路由規則，且可重新組態此等埠之出口模式以使用針對所有訊框之乙太網路類型DSA標記。接著，可將源自CPU之VID/SID/PID值保存在經定址至經由第二/隨後交換器模組而到達之目的地埠的訊框上。

可使用所需VID值來自動地對自CPU發送至編碼解碼

器/IP攝影機(或，發送至經由私人視訊網路而附接之任何裝置(例如，在公用網路上必須不可存取之AoE驅動程式))之正常網路訊務加標記，以允許藉由經由適當虛擬乙太網路介面頻道傳輸來將其路由至交換器模組之必要埠。在TCP/IP堆疊中，此係由IP位址路由表以與使用多個實體乙太網路介面時完全相同之方式來尋找。在AoE驅動程式中，此僅要求添加介面「eth2」作為一額外介面，可在該介面處搜尋AoE驅動程式。交換器感知應用程式碼可藉由查詢乙太網路驅動程式快取區以獲得SID/PID/SA值來找到實體地附接至交換器埠0A至7A及0B至7B之編碼解碼器/IP攝影機。接著可藉由搜尋ARP快取區或是使用RARP協定來容易地將SA轉換成編碼解碼器/攝影機IP位址。

視情況而定，交換器感知應用程式碼可尋求將自公用網路段接收到之一些ARP訊框鏡射至私人網路段上，且反之亦然。通常，對私人網路上之裝置的IP分配使用零組態協定，且公用網路上之分配通常使用DHCP伺服器，以使得不會存在位址衝突。然而，在一些情況下，零組態協定亦可用於公用網路上，從而產生位址衝突之可能性。

若零組態位址範圍之ARP訊框在公用網路至私人網路之間鏡射(且反之亦然)，則可避免衝突，因為該等網路段兩者皆可具有對已使用之位址的可見性。ARP訊框為可被允許在公用網路段與私人網路段之間傳遞之僅有的訊框類型。注意，此鏡射可能並非在交換器模組內自動地完成，而是藉由在主板CPU處接收且自主板CPU重新傳輸而完

成。此可促進阻止ARP訊框經由公用網路段及私人網路段在兩個視訊伺服器之間繞圈(亦即，在兩個伺服器之間反覆地來回傳輸)。若一傳入ARP被辨識為等同於先前在一短時間間隔內傳輸之一ARP，則可不重新傳輸該ARP。

除了通常使用零組態方法而非DHCP來指派IP位址之外，編碼解碼器及IP攝影機軟體可在無修改之情況下操作。就此等模組而言，其可經由一普通乙太網路而連接。只要交換器模組為開機的，編碼解碼器/IP攝影機軟體即可正常地操作，即使主板不在作用中或正執行啟動作業系統亦如此。然而，在此模式中，網路可作為對於公用網路而言隱藏不見之私人網路來操作，亦即，在兩個網路段之間可無任何資料傳送。

一用於交換器埠0A至7B之出口模式的替代性設定可提供編碼解碼器/IP攝影機之高度安全操作模式。此等埠可經設定以使用針對所有訊框之乙太網路類型DSA標記出口模式，其中使用來自內部標記之資訊來產生擴展標記。此可要求編碼解碼器/IP攝影機之乙太網路驅動程式碼為標記感知的(tag-aware)，以使得其可在將訊框傳遞至TCP/IP堆疊之前檢查並移除擴展標記，從而在驅動程式中快取SID/PID/SA資訊。所快取之資訊可允許裝置獲得對起始所接收之命令之實體連接(亦即，埠)的瞭解，尤其用以提供相比於自任一其他連接之存取而言更高層級的自主板CPU(SID=1，PID=9)之存取。舉例而言，連接至埠0A至7B中之一者的IP攝影機可能僅允許來自直接連接至交換器之一

視訊伺服器之主板的組態命令，而僅允許連接至私人視訊網路之其他視訊伺服器或解碼器單元出於檢視影像之目的而進行連接。僅可在編碼解碼器/IP攝影機已被識別為支援此操作之情況下使用該高安全模式。

現參看圖5描述雙模組系統。此系統可提供用於32個編碼解碼器或IP攝影機之多個連接502、用於公用乙太網路之兩個連接504、506，及用於私人視訊網路或用於級聯至擴展交換器模組之三個連接508。針對第一模組之開機設定可類似於針對如上文所述之具有兩個交換器之單一模組的彼等設定。針對第二模組之設定為類似的，但一重要差別在於埠9A之預設VID值可為5(亦即，私人網路訊務)而非4(亦即，公用網路訊務)。此設置可由模組微控制器基於模組ID而自動地管理。

亦可如上文針對單一模組所描述地操作主板軟體。交換器模組之開機設定可允許啟動作業系統經由交換器模組零上之第一公用網路連接而與公用網路段上之裝置進行通信。私人網路段上之所有裝置可互相通信，而Redboot不要求對交換器模組之任何特殊感知或Redboot不必執行任何特殊設置動作。Redboot可不與私人視訊網路進行通信，且公用網路段與私人網路段之間可不存在訊務。

當主應用程式碼啟動時，其可藉由偵測正接收之傳入訊框是否具有標記且藉由將控制命令發送至交換器來檢查第一交換器模組之存在。一旦已偵測到第一模組，即可傳遞控制命令以偵測第二模組。可接著修改交換器之互相通信

之埠的入口/出口模式，以提供完全散佈式交換器架構操作模式，其中在按任何方向穿過鏈路之所有訊框上保存標記資訊。此程序可接著在必要時重複以偵測任何其他級聯之交換器。

散佈式交換器架構設計可允許針對單一視訊伺服器連結多達30個交換器模組，從而提供多達240個埠來連接IP攝影機/編碼解碼器。可使用不同SID值來設定所有交換器，以致能正確的實體埠對標記資訊對應性。交換器模組可以一鏈結方式級聯在一起，而不要求任何其他外部傻瓜式交換器/集線器單元。每一模組可具有兩個可用連接，該等連接可用作私人網路連接或作為至其他交換器模組之級聯。在圖6至圖8中展示幾個實例組態。

圖6中所說明之實施例包括排列成一線性鏈之三個模組602、604、606。其具有3個公用網路連接、4個私人網路連接，及多達48個編碼解碼器/IP攝影機。來自第一組8個攝影機之資料可由主板經由單一交換器來接收，來自第二組8個攝影機之資料可由主板經由兩個交換器來接收，且來自第三組8個攝影機之資料可由主板經由三個交換器來接收。

藉由使用一純線性鏈，訊框須穿過之交換器的最大數目隨著攝影機計數而直接增加。注意，模組編號可為根據攝影機的升序的，或為任何其他次序。視訊伺服器之內部模組可為模組零，因為模組0之預設開機組態通常為不同的。然而，若所有模組經給定唯一編號，則可按任何次序

來將其他模組之模組ID設定為任何值。

圖7中所展示之另一實施例具有五個模組702、704、706、708、710，其形成一分支鏈。其可提供5個公用網路連接、6個私人網路連接，及多達80個編碼解碼器/IP攝影機。在此組態中，自任一攝影機傳輸至主板之資料可無須穿過6個以上之交換器(亦即，三個模組)。藉由使用分支鏈，訊框須穿過之交換器的最大數目隨著攝影機計數而對數地增加。

如圖8中所展示，可以一星形互連組態來連接使用的額外傻瓜式交換器/集線器單元(例如，現成網路交換器)。圖8中所展示之實施例使用七個智慧型視訊交換器模組802、804、806、810、812、814、816，及具有至少七個埠之傻瓜式網路Gb乙太網路交換器820。此系統可提供多達112個IP攝影機/編碼解碼器，七個公用網路連接，及十三個私人視訊網路連接。在此系統中，乙太網路訊框可無須穿過五個以上交換器(模組中之四個交換器，及傻瓜式網路交換器)。然而，傻瓜式交換器之備用埠不可用作額外之私人或公用網路埠。將該傻瓜式交換器視為級聯連接之部分，且穿過其之所有訊務可含有使用0xAD01標記標誌的VID/SID/PID標記資訊。

圖9說明兩個視訊伺服器902、904之間的一可能互連，該等視訊伺服器中之每一者使用多個交換器模組。如圖9中所展示，多個視訊伺服器系統可使用其公用及/或私人網路連接而互連。必須隔離其級聯連接。單一視訊伺服器

可被認為包括一主系統單元，該主系統單元具有內建交換器模組以及連結於一級聯網路中的可選的額外交換器模組。在一個伺服器之網路內，模組ID號必須均為唯一的，但在不同伺服器間不需要為唯一的(事實上，每一伺服器可具有至少一個別模組零)。

在該等交換器模組中之每一者上，所展示之四個連接(自左至右)為私人/級聯輸出910、私人/級聯輸出912、公用網路914、主板/級聯輸入916。兩個伺服器一起連接在公用網路及私人網路兩者上。然而，注意，在每一側上僅存在單一互連以用於阻止網路迴圈。該等伺服器之間的私人網路鏈路與一內部級聯連接之不同之處在於：來自伺服器1之傳出埠在私人網路模式而非級聯輸出模式中操作；而伺服器2之傳入埠為另一私人網路埠而非級聯輸入埠。

每一視訊伺服器內所連接之IP攝影機/編碼解碼器可被認為由特定伺服器所擁有。僅伺服器1可具有對來自伺服器1 IP攝影機之訊務上的VID/SID/PID標記的可見性(且因此，對此等IP攝影機之實體連接性的立即瞭解)；同樣地，僅伺服器2可具有對其IP攝影機之訊務標記的可見性。然而，所有此等IP攝影機/編碼解碼器亦可作為私人視訊網路上之正常網路裝置而可見。因此，伺服器2有可能進行一訪客連接以檢視伺服器1之攝影機中的任一者，而不必經由伺服器1主板CPU路由全部資料。一例示性資料流可為：[伺服器1 IP攝影機]->私人網路->[伺服器2顯示器編碼解碼器]。

亦可經由公用網路來進行訪客連接，但在此狀況下，防火牆操作意謂著須經由主板CPU路由所有資料。舉例而言，伺服器1可經由公用網路來請求來自伺服器2之攝影機資料，但可能必須在兩個CPU之間建立連接，且資料可如下流動：[伺服器2 IP攝影機]->[伺服器2主板]->公用網路->[伺服器1主板]->[伺服器1顯示器編碼解碼器]。由此，一般而言，對於本地相關的視訊伺服器之間的連接而言，可能使用私人視訊網路較佳，而僅在存取遠端或無關伺服器時使用公用網路。

如圖10中所展示，對於進階防火牆應用程式，NAT路由器單元可包括於交換器單元內。此可致能在公用網路段、私人網路段及內部網路段之間智慧地隧道傳輸選定訊務。NAT路由器1002可包括一快速網路處理器裝置，該快速網路處理器裝置能夠接收訊框、檢查L2(乙太網路標頭)/L3(IP標頭)/L4(TCP標頭)協定層處的訊框資料、應用用於接受/拒絕/修改訊框的規則，且接著重新傳輸該等訊框。該NAT路由器1002可位於第一交換器模組1004之埠10A與公用網路連接1006之間。亦可使用一SPI單元來替代NAT路由器，或除了NAT路由器之外，亦可使用一SPI單元。

在公用網路與交換器模組之間移動之所有訊框可能必須穿過NAT路由器1002。其可檢查並視情況修改MAC位址、IP位址及TCP埠號資訊。針對在埠10A處自公用網路進入交換器模組之訊框的標準路由規則僅允許在埠9A上離開至

主板CPU。然而，當已偵測到NAT路由器1002之存在時，可更新此等規則以允許對進入之訊框進行VLAN標記。接著可根據VID值將該等訊框導引至主板CPU、編碼解碼器/IP攝影機，或是外部私人視訊網路。類似地，源自編碼解碼器/IP攝影機及私人視訊網路之訊框通常僅可離開埠9A，但特殊VID值可允許其在埠10A處離開以經由NAT路由器1002而轉送至公用網路。對NAT路由器之偵測及動態組態可由發送特殊控制訊框之主板CPU來執行。此亦可允許在運作中更新該等NAT路由規則。

圖11示意性地展示根據本發明之IP攝影機1100。該IP攝影機1100包括一儲存單元1102、一伺服器1104，及一交換模組1106。攝影機1100之一端子1110連接至交換模組1106之埠0A，且亦連接至儲存單元1102。可在端子1110上遞送由攝影機1100記錄之視訊資料，且可將其儲存於儲存單元1102中，且亦可經由交換模組1106將該等視訊資料路由至一安全網路中之其他目的地。其他攝影機(IP或類比)可連接至交換模組1106之埠1A至7A及埠0B至7B。

已描述了本發明之特定實施例，對於一般熟習此項技術者而言將顯而易見，可在不脫離本發明之精神及範疇的情況下使用併有本文中所揭示之概念的其他實施例。因此，將在各方面將所描述之實施例視為僅說明性的而非限制性的。

【圖式簡單說明】

圖1示意性地展示一包含兩個交換器之交換模組；

圖2示意性地展示包括於一交換模組中之一交換器，及其在該交換模組外部之連接；

圖3示意性地說明包括於一交換模組中之兩個交換器之間的連接；

圖4示意性地展示一交換模組及其外部連接；

圖5示意性地展示兩個交換模組之組態；

圖6示意性地展示連接成一鏈之三個交換模組的組態；

圖7示意性地展示以一分支型樣連接之五個交換模組的組態；

圖8示意性地展示星形連接之交換模組，其使用傻瓜式網路交換器；

圖9示意性地說明兩個視訊伺服器之組態；

圖10示意性地展示一交換模組及一網路位址轉譯(NAT)路由器之組態；及

圖11示意性地展示根據本發明之一IP攝影機。

【主要元件符號說明】

100	交換模組
102、104	交換器
106	微控制器/微控制器晶片
108	Gb乙太網路實體連接器/裝置(PHY)
110	10/100 Mb乙太網路埠
112	Gb乙太網路埠
114	連接

116	串列管理介面(SMI)匯流排
300	組態
302、304	交換模組
306	微控制器
316	SMI匯流排
318	中斷線
400	模組
402、404	交換器
412、414、416	連接
502、504、506、508	連接
602、604、606	模組
702、704、706、708、710	模組
802、804、806、810、812、814、816	智慧型視訊交換器模組
820	傻瓜式網路Gb乙太網路交換器
902、904	視訊伺服器
910	私人/級聯輸出
912	私人/級聯輸出
914	公用網路
916	主板/級聯輸入
1002	NAT路由器

1004	第一交換器模組
1006	公用網路連接
1100	IP攝影機
1102	儲存單元
1104	伺服器
1106	交換模組
1110	端子

201208302

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：100115196

※ 申請日：100、4、29　　※IPC 分類：H04L 12/46 (2006.01)

一、發明名稱：（中文/英文）

網際網路協定封閉電路系統及方法

AN IP-CLOSED CIRCUIT SYSTEM AND METHOD

二、中文發明摘要：

本發明係關於一種用於產生並操作資料來源及監測台之安全網路且用於提供自公用網路對該等資料來源及監測台之受控存取的交換模組。

三、英文發明摘要：

The invention relates to a switching module for creating and operating secure networks of data sources and monitoring stations, and for providing controlled access to the data sources and monitoring stations from public networks.

七、申請專利範圍：

1. 一種交換模組，其包含：

一第一埠群組，其包含至少一埠，其中該第一埠群組中之每一埠經組態以用於與一資料來源連接，藉由將經指派給該埠之一唯一埠號包括在一資料訊框中來修改由該所連接之資料來源傳輸的該資料訊框，且在經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯的情況下將該經修改之資料訊框路由至該目的地埠；

一第二埠群組，其包含至少一埠，其中該第二埠群組中之每一埠經組態以用於與一監測台連接，且接收由該第一埠群組中之至少一埠修改的一資料訊框；及

一控制單元，其用於將一唯一埠號指派給該第一埠群組及該第二埠群組中之每一埠，且將一路由表指派給該第一埠群組中之每一埠，該路由表包括至少一來源埠號及與該至少一來源埠號相關聯之至少一目的地埠號。

2. 如請求項1之交換模組，其中該資料來源包含一IP攝影機。

3. 如請求項1之交換模組，其中該資料來源包含一類比攝影機及一編碼解碼器。

4. 如請求項1之交換模組，其中該資料來源包含一編碼器，其中一連接至該編碼器之裝置可選自一由一IP攝影機、一類比攝影機及一SDI攝影機組成之群組。

5. 如請求項1之交換模組，其中該資料來源可選自一由一

門禁讀卡器及一警報器組成之群組。

6. 如請求項1之交換模組，其中該監測台包含用於檢視經由該所連接之埠而接收到之該等資料訊框的構件。

7. 如請求項1之交換模組，其中該監測台包含用於儲存經由該所連接之埠而接收到之該等資料訊框的構件。

8. 如請求項1之交換模組，其進一步包含一第三埠群組，該第三埠群組包含至少一埠，其中該第三埠群組中之每一埠經組態以用於與計算裝置之一私人網路連接，且該控制單元經組態以用於：

將一唯一埠號指派給該第三埠群組中之每一埠；且

致能該第三群組中之埠之間的資料訊框之通信、該第三埠群組中之一埠與該第一或第二埠群組中之一埠之間的資料訊框之通信，以及該第三群組中之一埠與該控制單元之間的資料訊框之通信。

9. 如請求項1之交換模組，其進一步包含一第四埠群組，該第四埠群組包含至少一埠，其中該第四埠群組中之每一埠經組態以用於與計算裝置之一公用網路連接，且該控制單元經組態以用於：

將一唯一埠號指派給該第四埠群組中之每一埠；

致能該第四埠群組中之埠之間的資料訊框之通信，及該第四群組中之一埠與該控制單元之間的資料訊框之通信；且

阻止該第四埠群組中之一埠與該第一或第二埠群組中之一埠之間的資料訊框之通信。

10. 一種視訊裝置，其包含：

一攝影機；

一儲存單元，其與該攝影機通信以用於儲存由該攝影機記錄之資料訊框；及

一伺服器，其用於控制該攝影機及該儲存單元，且用於存取及傳輸該等所儲存之資料訊框。

11. 如請求項10之視訊裝置，其進一步包含一埠單元，該埠單元經組態以用於：

接收一唯一埠號；且

藉由將該唯一埠號包括在該資料訊框中來修改由該攝影機傳輸之一資料訊框。

12. 如請求項10之視訊裝置，其進一步包含一交換模組，該交換模組包含：

一第一埠群組，其包含至少一埠，其中該第一埠群組中之每一埠經組態以用於與一資料來源連接，藉由將經指派給該埠之一唯一埠號包括在一資料訊框中來修改由該所連接之資料來源傳輸的該資料訊框，且在經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯的情況下將該經修改之資料訊框路由至該目的地埠；

一第二埠群組，其包含至少一埠，其中該第二埠群組中之每一埠經組態以用於與一監測台連接，且接收由該第一埠群組中之至少一埠修改的一資料訊框；及

一控制單元，其用於將一唯一埠號指派給該第一埠群

組及該第二埠群組中之每一埠，且將一路由表指派給該第一埠群組中之每一埠，該路由表包括至少一來源埠號及與該至少一來源埠號相關聯之至少一目的地埠號，

其中，該攝影機使用該第一埠群組中之該至少一埠而連接至該交換模組。

13. 如請求項12之視訊裝置，其中該伺服器藉由使用所連接之任何資料來源經由該至少一埠來接收控制資訊，且回應於所接收之該控制資訊而控制該控制單元。

14. 如請求項13之視訊裝置，其中該第一埠群組包含至少一輔助埠，且至少一資料來源連接至該至少一輔助埠。

15. 如請求項14之視訊裝置，其中該至少一資料來源為一視訊攝影機。

16. 一種用於操作一IP網路之方法，該IP網路包含一交換模組，該交換模組包含：一第一埠群組，其包括至少一埠；一第二埠群組，其包括至少一埠；及一控制單元，該方法包含以下步驟：

自該控制單元將一唯一埠號指派給該第一埠群組及該第二埠群組中之每一埠；

自該控制單元為該第一埠群組中之每一埠指派一路由表，該路由表包括至少一來源埠號及與該至少一來源埠號相關聯之至少一目的地埠號；

將一資料來源連接至該第一埠群組中之該至少一埠；

對由該資料來源傳輸之一資料訊框進行授權；

修改該經授權之資料訊框；

若經指派給一目的地埠之一唯一埠號與經指派給該埠之一路由表中的埠相關聯，則將該經修改之資料訊框路由至該目的地埠；

將一監測台連接至該第二埠群組中之該至少一埠；及

在該監測台處接收由該第一埠群組中之至少一埠修改的一資料訊框。

17. 如請求項16之方法，其中對一資料訊框進行授權包含將該資料訊框中之一裝置來源號與該唯一埠號進行比較。

18. 如請求項16之方法，其進一步包含以下步驟：

阻止一未授權資料訊框之傳輸；及

將接收該未授權資料訊框之該埠之該唯一埠號傳達至該控制單元以用於阻塞經由該埠之存取。

19. 如請求項16之方法，其中該第一埠群組中之該至少一埠的該唯一埠號包含連接至該第一埠群組中之該至少一埠之該資料來源的一裝置來源號，且該第二埠群組中之該至少一埠的該唯一埠號包含連接至該第二埠群組中之該至少一埠之該監測台的一裝置來源號。

20. 如請求項16之方法，其進一步包含以下步驟：

在該第一群組中之一埠處儲存與連接至該埠之該資料來源相關聯的一安全參數；

在該資料來源處儲存一相應安全參數；

自該資料來源接收所儲存之該相應安全參數；

將所接收之該相應安全參數與儲存於該埠處之該安全參數相比較以判定一未授權裝置是否連接至該埠；及

回應於判定一未授權裝置連接至來自一或多個埠群組之該埠，在一預定時段內停用該埠以阻止自該未授權裝置進行之資料傳輸。

21. 如請求項20之方法，其中該安全參數為一隨機產生之密鑰。

22. 如請求項20之方法，其中該安全參數為一對，其包含在一特定時間段期間進入之封包的一數目及離開之封包的一數目。

23. 如請求項20之方法，其進一步包含回應於判定一未授權裝置連接至該埠而報告一違規行為。

24. 如請求項23之方法，其中報告包含發送一警示至一管理員。

25. 如請求項23之方法，其中報告包含發送非受信任資料訊框至一管理員。

八、圖式：

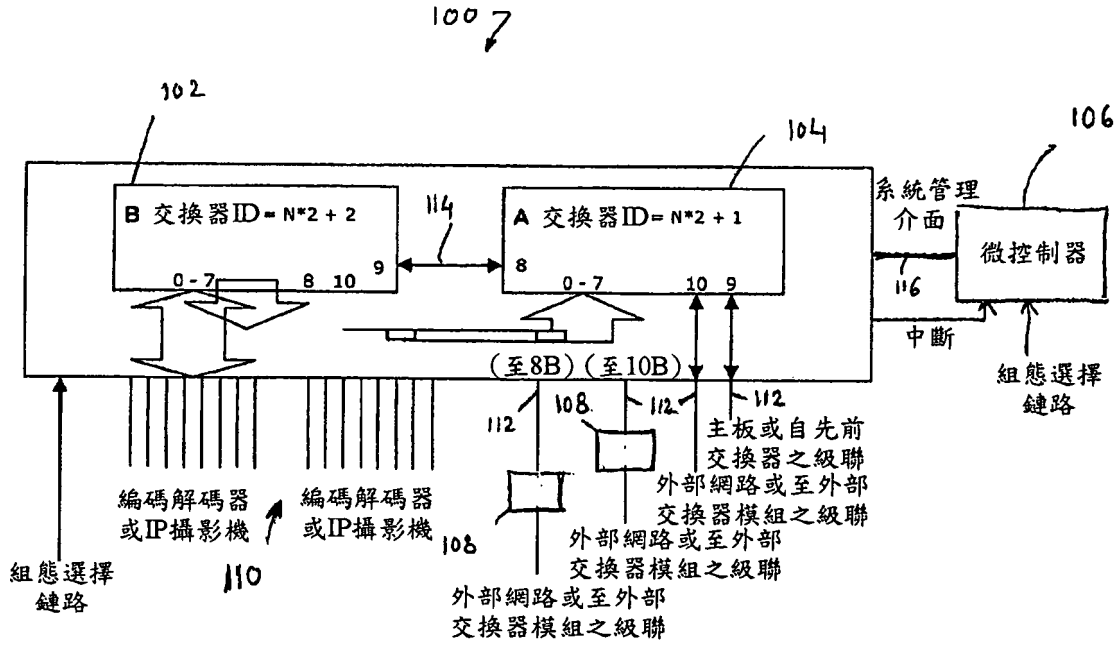

100
102
104
106
B 交換器ID= N*2 + 2
A 交換器ID= N*2 + 1
0 - 7
8 10 9
8
0 - 7
10 9
114
系統管理
介面
116
微控制器
中斷
組態選擇
鏈路
(至8B) (至10B)
112
108
112
112
主板或自先前
交換器之級聯
外部網路或至外部
交換器模組之級聯
編碼解碼器
或IP攝影機
編碼解碼器
或IP攝影機
110
108
外部網路或至外部
交換器模組之級聯
組態選擇
鏈路
外部網路或至外部
交換器模組之級聯

圖1

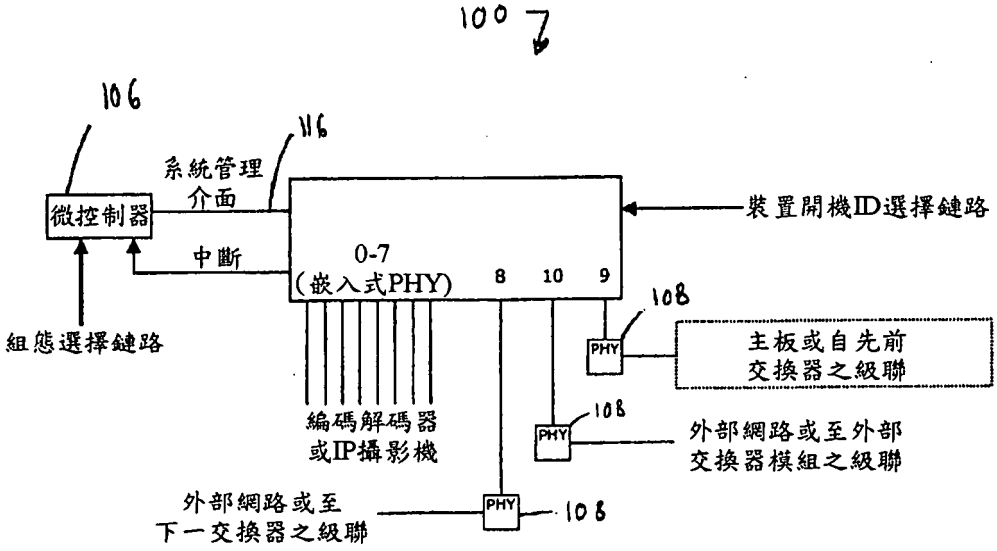

100
106
116
系統管理
介面
微控制器
中斷
組態選擇鏈路
0-7
(嵌入式PHY)
8
10
9
裝置開機ID選擇鏈路
108
PHY
主板或自先前
交換器之級聯
108
PHY
外部網路或至外部
交換器模組之級聯
編碼解碼器
或IP攝影機
外部網路或至
下一交換器之級聯
PHY
108

圖2

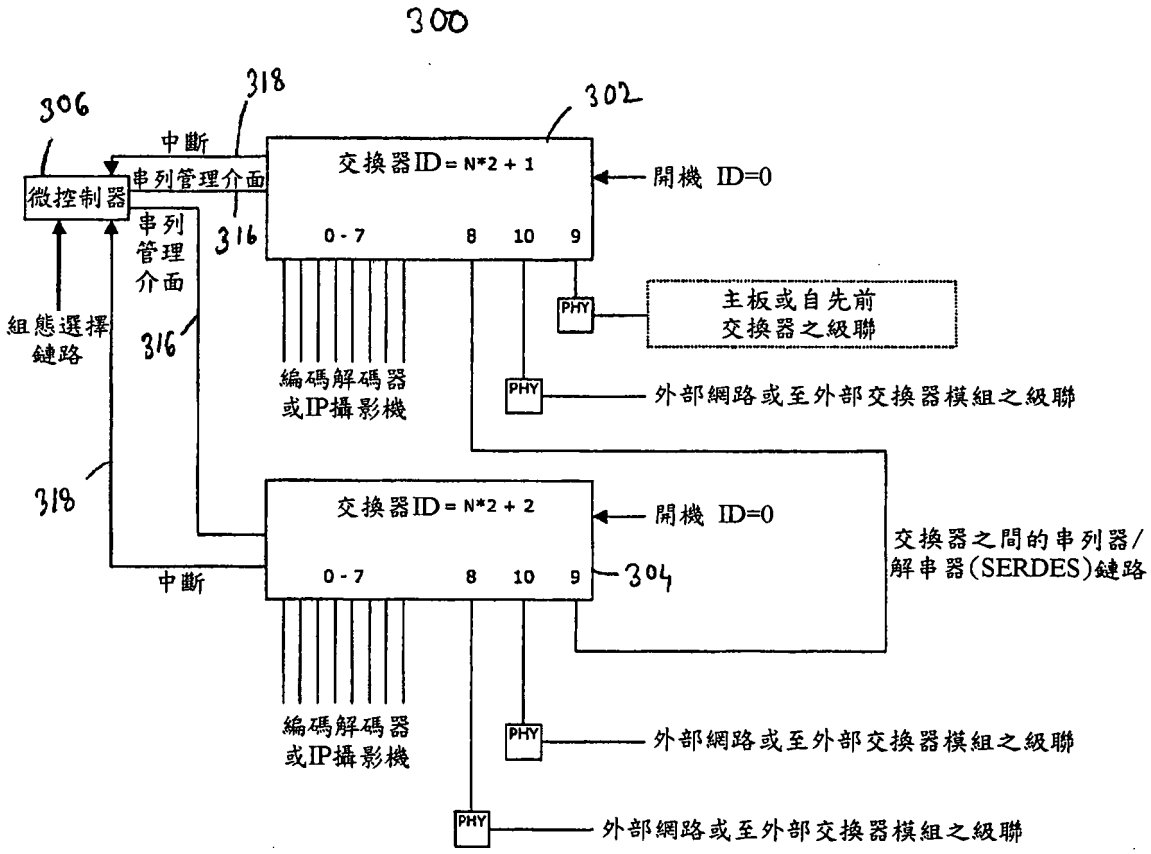

300
306
318
302
中斷
微控制器
串列管理介面
交換器ID = N*2 + 1
開機 ID=0
串列管理介面
316
0 - 7
8
10
9
PHY
主板或自先前交換器之級聯
組態選擇鏈路
316
編碼解碼器或IP攝影機
PHY
外部網路或至外部交換器模組之級聯
318
交換器ID = N*2 + 2
開機 ID=0
交換器之間的串列器/解串器(SERDES)鏈路
中斷
0 - 7
8
10
9
304
編碼解碼器或IP攝影機
PHY
外部網路或至外部交換器模組之級聯
PHY
外部網路或至外部交換器模組之級聯

圖3

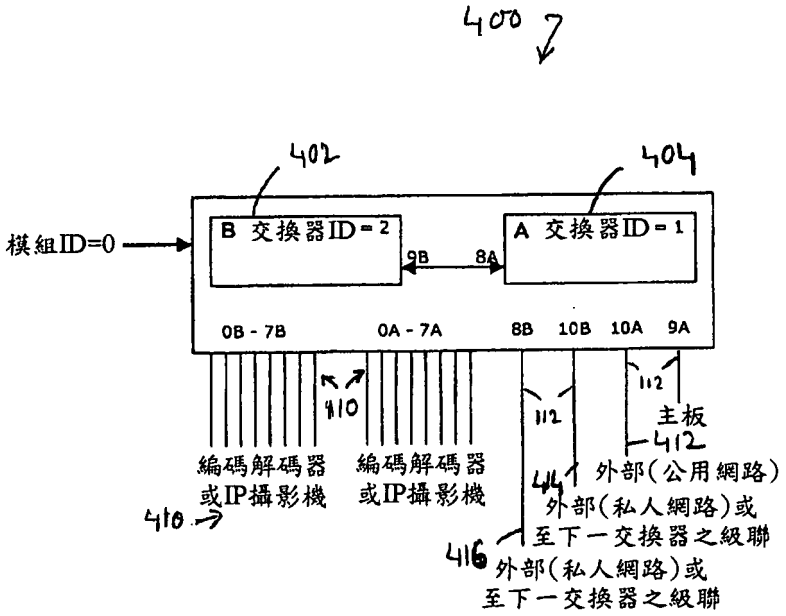

400
402
404
模組ID=0
B 交換器ID = 2
A 交換器ID = 1
9B
8A
0B - 7B
0A - 7A
8B
10B
10A
9A
112
112
112
410
410
主板
412
編碼解碼器
或IP攝影機
編碼解碼器
或IP攝影機
外部(公用網路)
414
外部(私人網路)或
至下一交換器之級聯
416
外部(私人網路)或
至下一交換器之級聯

圖4

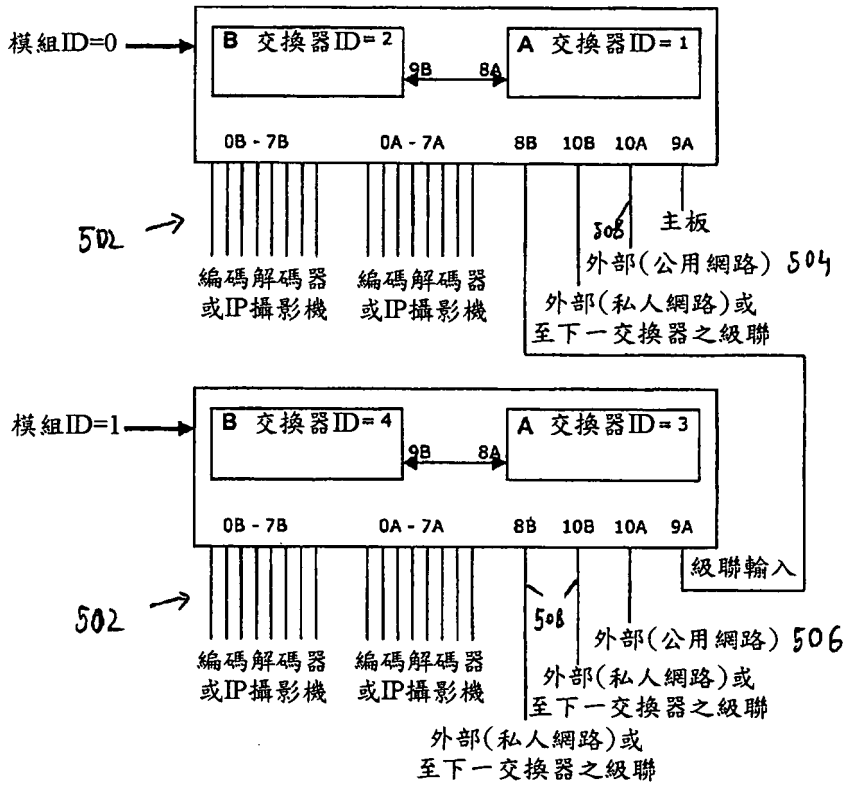

模組ID=0
B 交換器ID=2
A 交換器ID=1
9B
8A
0B - 7B
0A - 7A
8B
10B
10A
9A
502
508
主板
外部(公用網路) 504
編碼解碼器
或IP攝影機
編碼解碼器
或IP攝影機
外部(私人網路)或
至下一交換器之級聯
模組ID=1
B 交換器ID=4
A 交換器ID=3
9B
8A
0B - 7B
0A - 7A
8B
10B
10A
9A
級聯輸入
502
508
外部(公用網路) 506
編碼解碼器
或IP攝影機
編碼解碼器
或IP攝影機
外部(私人網路)或
至下一交換器之級聯
外部(私人網路)或
至下一交換器之級聯

圖5

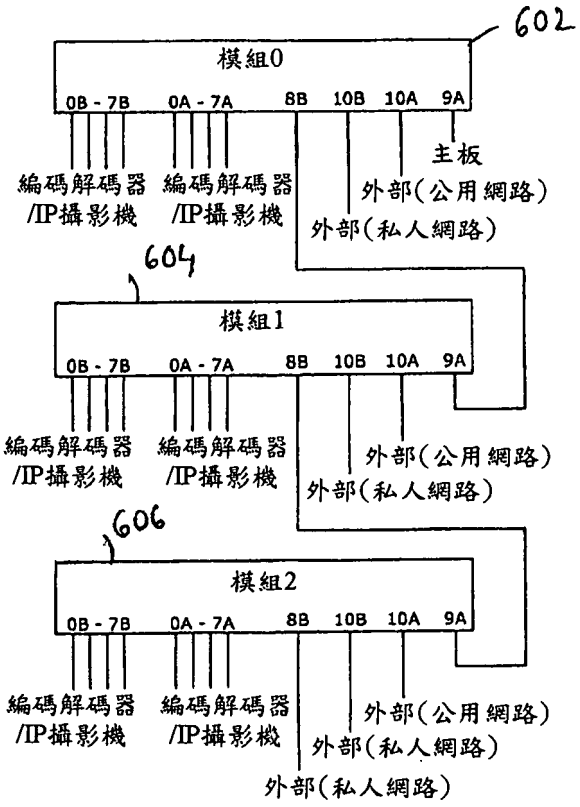

602
模組0
0B - 7B
0A - 7A
8B
10B
10A
9A
主板
編碼解碼器
/IP攝影機
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
604
模組1
0B - 7B
0A - 7A
8B
10B
10A
9A
編碼解碼器
/IP攝影機
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
606
模組2
0B - 7B
0A - 7A
8B
10B
10A
9A
編碼解碼器
/IP攝影機
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
外部(私人網路)

圖6

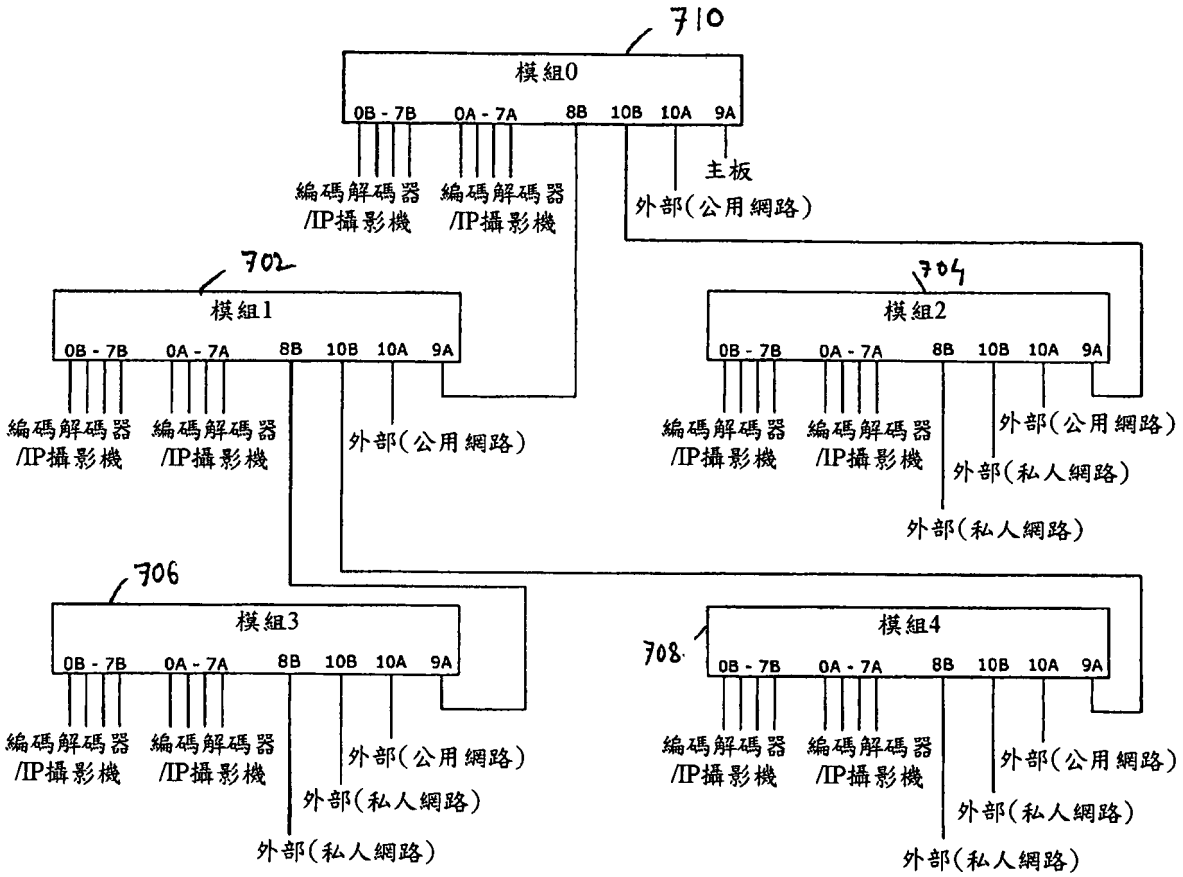

710
模組0
0B - 7B
0A - 7A
8B
10B
10A
9A
編碼解碼器 /IP攝影機
編碼解碼器 /IP攝影機
主板
外部(公用網路)
702
模組1
704
模組2
706
模組3
708
模組4
外部(私人網路)

圖7

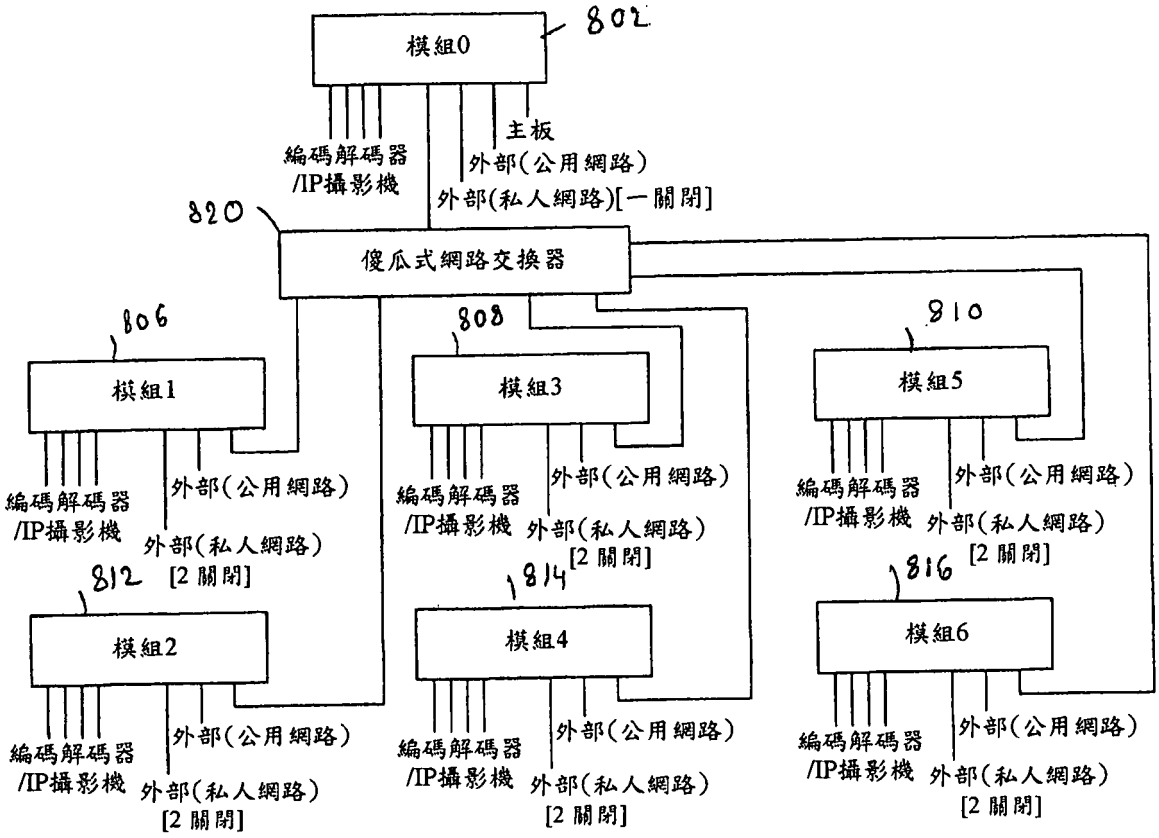

802
模組0
編碼解碼器
/IP攝影機
主板
外部(公用網路)
外部(私人網路)[一關閉]
820
傻瓜式網路交換器
806
模組1
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]
808
模組3
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]
810
模組5
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]
812
模組2
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]
814
模組4
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]
816
模組6
編碼解碼器
/IP攝影機
外部(公用網路)
外部(私人網路)
[2 關閉]

圖8

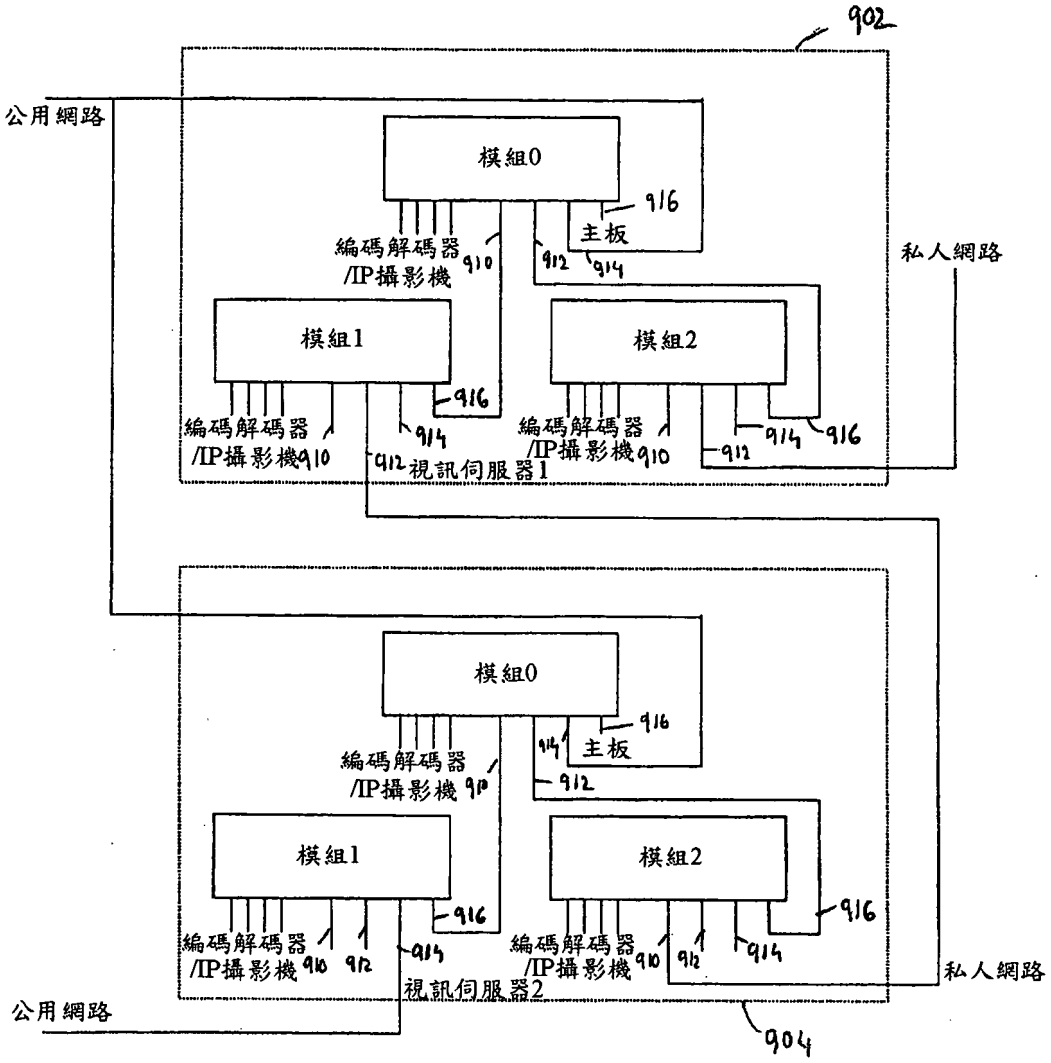

902
公用網路
模組0
916
主板
編碼解碼器
/IP攝影機
910
912
914
私人網路
模組1
模組2
916
編碼解碼器
/IP攝影機910
914
916
912視訊伺服器1
模組0
916
914
主板
編碼解碼器
/IP攝影機
910
912
模組1
模組2
916
916
編碼解碼器
/IP攝影機910
912
914
編碼解碼器
/IP攝影機910
912
914
私人網路
視訊伺服器2
公用網路
904

圖9

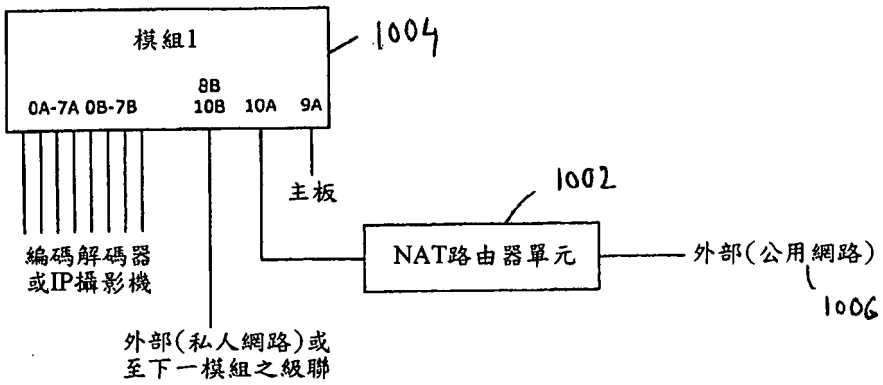

模組1
1004
8B
0A-7A 0B-7B
10B
10A
9A
主板
1002
NAT路由器單元
外部(公用網路)
1006
編碼解碼器
或IP攝影機
外部(私人網路)或
至下一模組之級聯

圖10

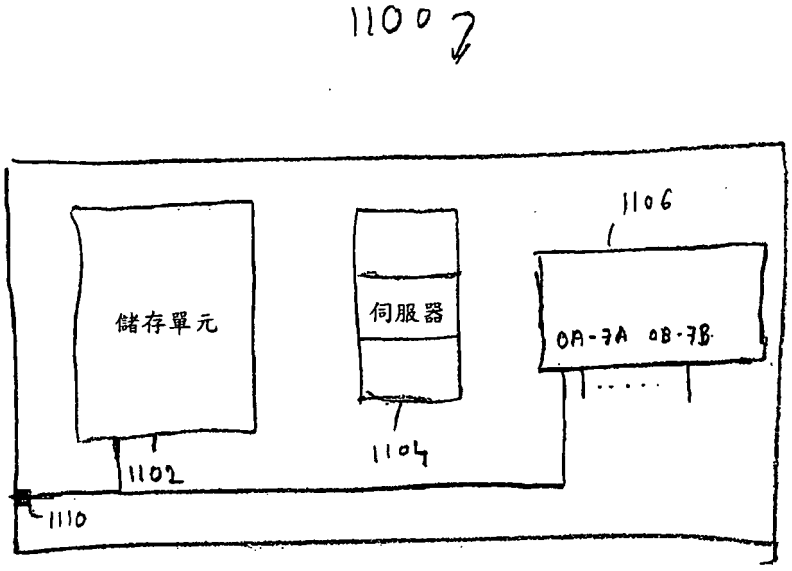


圖11

四、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：

100	交換模組
102、104	交換器
106	微控制器/微控制器晶片
108	Gb乙太網路實體連接器/裝置(PHY)
110	10/100 Mb乙太網路埠
112	Gb乙太網路埠
114	連接
116	串列管理介面(SMI)匯流排

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）