Doc Code: **TR.PROV**
Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (11-08)
Approved for use through 05/31/2015. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1 Remove

Given Name	Middle Name	Family Name	City	State	Country i
Patrick		Kuo	Yilan County		TW

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Title of Invention	A METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME
Attorney Docket Number (if applicable)	6121.001.PPA

Correspondence Address

Direct all correspondence to (select one):

◉ The address corresponding to Customer Number	○ Firm or Individual Name
Customer Number	11336

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

◉ No.

○ Yes, the name of the U.S. Government agency and the Government contract number are:

Doc Code: **TR.PROV**
Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (11-08)
Approved for use through 05/31/2015. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Entity Status

Applicant claims small entity status under 37 CFR 1.27

- (•) Yes, applicant qualifies for small entity status under 37 CFR 1.27
- ( ) No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Min-Lee Teng/			Date (YYYY-MM-DD)	2013-04-15
First Name	Min-Lee	Last Name	Teng	Registration Number (If appropriate)	65623

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or paten. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, t o a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

A METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME

【Field of Invention】

本發明是有關一種建立點對點連線的系統與方法，尤指一種辨識連網設備以建立點對點連線的系統與方法。

【Descriptions of Prior Art】

隨著科技進步與網際網路的普及，使用者可以預先於欲監視的場所架設網路攝影機，並經由網際網路在世界各地監看網路攝影機的影像，且當緊急情況發生時，使用者亦可利用與網際網路連線的警報系統通知當地的應變中心採取緊急措施以避免緊急情況失控。雖然網際網路在打擊犯罪以及保全證據上具有絕佳的利用價值，但習用的網路攝影機需要搭配網路配線，若欲將保全設施應用於一般住宅內，即必須安裝複雜的網路配線以將網路攝影機配置於居家的各個角落。針對上述缺失，目前市場一般採用無線區域網路將各個網路攝影機連線，由於不需要實體的網路線，故免除了複雜的安裝工序。但無線區域網路並非毫無缺點，因為無線傳輸是以電磁波作為資料傳輸的媒介，而在室內電磁波會受到牆壁與樓上及樓下之間的空間阻隔，導致無線傳輸的使用區域受到限制。

由於不具有實體網路線以及無線區域網路的缺失，電力線傳輸(Power Line Communication)被視為未來提供寬頻

網路接取的最後一哩(Last Mile)解決方案中最具競爭力的技術之一。電力線傳輸，顧名思義是指利用住宅中既有的電力線傳輸高速率的資料、語音與視訊多媒體服務的一種通訊技術，該技術的工作原理是是利用 4MHz 至 21MHz 或 2MHz 至 30MHz 頻帶範圍傳輸信號，在傳送端利用正交分頻多工(OFDM)技術將通訊信號加以編碼與調變，然後在電力線上進行資料傳輸，在接收端首先經過電力線耦合器及高頻濾波將調變信號濾出，並經解碼與解調變之後，就可得到原來通訊信號。因為不需再佈網路線且訊號強度不受室內障礙物的阻隔而影響，故能夠省下高昂的架設費用且無收不到訊號的可能。與電力線傳輸相關的專利案可參閱美國公開專利第 US2005/0047379 號以及美國公開專利第 US2004/0186908 號。

雖然電力線傳輸能夠充分利用電力線，但為連線配置於不同位置的網路攝影機，電力線傳輸可搭配點對點技術(point-to-point)來實現透過網際網路監控家中的影像的目的。請參閱中國台灣公開專利第 M382669 號所揭示的一種網路影像監視及設備控制系統，該系統包含有一攝影裝置、一電力線網路橋接器、一第一路由器、一第二路由器、一點對點伺服器與一監控裝置。該攝影裝置攝錄影像後將該影像壓縮成數位影像訊號，並將該數位影像訊號傳送到電力線網路橋接器，再經由該第一路由器連接至網際網路。當攝影裝置連接至網際網路後自動連接至點對點伺服器，該點對點伺服器會對連接攝影裝置的第一路由器打洞

(hole punching)，而當監控裝置連接至網際網路後也自動連接至點對點伺服器，該點對點伺服器會對連接監控裝置的第二路由器打洞(hole punching)，經過打洞程序後，該攝影裝置即可建立與監控裝置的直接連線，亦即，該攝影裝置不需經過點對點伺服器即可將影像訊號傳送至監控裝置。

雖然上述前案所提出的系統能夠透過電力線將攝影裝置和監控裝置連線，但該系統的點對點連線機制僅能應用於同服務提供者所營運的點對點伺服器，或具有相同軟體的連網設備上，因此，在網路設備以及連網設備的擴充性以及相容性上即受到極大的限制。為克服上述缺失，先前技術提出一種點對點網物聯網連線平台，該平台具有一管理伺服器、複數個點對點伺服器，以及複數個具備應用介面程式(Application Programming Interface, API)的近端設備與連網設備，其中，該管理伺服器與該些點對點伺服器透過網際網路建立連線，且該應用介面程式(API)能適用於各種不同的作業系統。在實際的運作模式中，該連網設備內建有一組識別代碼(ID)，並於開機後自動與該管理伺服器連線並登錄該連網設備的資訊於該管理伺服器中，該近端設備輸入該連網設備的識別代碼(ID)，即可向該管理伺服器請求與該連網設備連線的點對點伺服器的位址，該近端設備依據該位址連線該點對點伺服器，由於該連網設備與該近端設備具備可相容的應用介面程式(API)，該點對點伺服器得以順利的建立該連網設備與該近端設備的連線。

雖然前述系統解決網路設備擴充後的連線問題，但由

於各個該連網設備各自有一組識別代碼(ID)，當配置的連網設備數量增加時，識別代碼(ID)的組數與複雜度隨之增加，例如超過 10 位數字或英文的組合。當使用者欲選擇一連網設備進行監控，即必須在該近端設備輸入對應該連網設備的識別代碼(ID)，即使該近端設備為一智慧型手機，位數過多的識別代碼(ID)亦造成手動輸入過程過於繁複而無法快速的建立近端設備與連網設備之間的連線。

SUMMARY

本發明的主要目的，在於解決識別代碼的位數過多而無法快速建立終端設備與連網設備之間的連線的缺失。

為達上述目的，本發明提供一種辨識連網設備以建立點對點連線的系統，該系統包括有至少一網路伺服器、至少一連網設備與至少一終端設備。該網路伺服器包含有一連網設備列表；該連網設備內建有一識別代碼以及一對應該識別代碼且設置於該連網設備上的連線條碼，該連網設備透過網際網路連線至該網路伺服器以登錄該識別代碼於該連網設備列表中；該終端設備包含有一影像截取模組，該終端設備以該影像截取模組截取該連網設備的連線條碼以產生一對應該連線條碼的連線請求訊號，該連線請求訊號透過網際網路傳輸至該網路伺服器；其中，該網路伺服器自該連網設備列表讀取該連線請求訊號所對應的連網設備以向該連網設備通知該終端設備欲與其連線，使該連網

設備與該終端設備之間建立一通訊通道，藉此該連網設備與該終端設備經由該通訊通道進行點對點連線。

透過前述的系統，本發明提出一種辨識連網設備以建立點對點連線的方法，該方法包括以下步驟：A.透過網際網路將至少一連網設備連線至一網路伺服器；B.登錄該連網設備所內建的一識別代碼於該網路伺服器的一連網設備列表中，並設置一對應該識別代碼的連線條碼於該連網設備上；C.透過一終端設備的一影像截取單元截取該連線條碼以產生一對應該連線條碼的連線請求訊號，並將該連線請求訊號透過網際網路傳輸至該網路伺服器；D.自該連網設備列表讀取該連線請求訊號所對應的連網設備，使該網路伺服器向該連網設備通知該終端設備欲與其連線，再令該連網設備與該終端設備之間建立一通訊通道，藉此該連網設備與該終端設備經由該通訊通道進行點對點連線。

於本發明第一種實施態樣中，其中步驟 C 更包括以下子步驟：子步驟 1：以該終端設備的一條碼解讀模組解讀該連線條碼影像為該識別代碼；子步驟 2：令該連線請求訊號包含有該識別代碼。

於本發明第二種實施態樣中，為避免該識別代碼在傳送的過程中遭到攔截而被不肖人士所利用，步驟 C 更包括以下子步驟：子步驟 1：令該連線請求訊號包含有該連線條碼影像；子步驟 2：透過網際網路將該連線請求訊號傳輸至該網際網路伺服器。且搭配第二種實施態樣的步驟 C，步驟 D 更包括以下子步驟：子步驟 1：接收該連線請求訊號；

子步驟 2：以該網路伺服器的一條碼解讀模組解讀該連線請求訊號為該識別代碼。

更進一步地，為避免他人無故取得該終端設備而可輕易的由該終端設備監控該連網設備，接續該步驟 D 更包括下述的步驟：E.自該終端設備輸入一安全密碼；F.判斷該安全密碼是否相同於該連網設備的一預設安全密碼，若否，則跳回步驟 E，若是，則允許該終端設備登入該連網設備。

於本發明另一實施例中，該網路伺服器執行打洞技術以建立該連網設備與該終端設備之間的通訊通道。

於本發明另一實施例中，該網際網路是選擇自乙太網路(Ethernet)、區域網路(LAN)、廣域網路(WAN)和虛擬私有網路(VPN)所組成的群組中的任何一種。

於本發明另一實施例中，該連線條碼更對應該預設安全密碼，該影像截取模組截取該連網設備的連線條碼後產生一連線條碼影像。

於本發明另一實施例中，該終端設備包含有一將該連線條碼影像解讀為該識別代碼與該預設安全密碼的條碼解讀模組，而該連線請求訊號包含有該識別代碼與該預設安全密碼。

於本發明另一實施例中，該連線請求訊號包含有該連線條碼影像，而該網路伺服器包含有一將該連線條碼影像解讀為該識別代碼與該預設安全密碼的條碼解讀模組。

於本發明另一實施例中，該連線條碼是為一快速回應碼或一一維條碼。

藉由上述的技術方案，本發明與習知技術相較具有如下所述的優點：

一、可快速的建立行動裝置與連網設備的連線。不同於習知技術以手動的方式逐字輸入該識別代碼，本案在該連網設備上設置有對應該識別代碼的連線條碼，並利用行動裝置既有的影像截取模組截取該連線條碼，且該連線條碼經解讀為該識別代碼，進而該網路伺服器以該識別代碼快速建立該連網設備與該終端設備之間的點對點連線。

【圖式簡單說明】

圖 1，是本發明第一種實施態樣的架構示意圖

圖 2，是本發明第二種實施態樣的架構示意圖

圖 3，是本發明的傳送打洞連線訊息示意圖

圖 4，是本發明的建立點對點連線示意圖

圖 5，是本發明的建立點對點連線 terminal equipment 示意圖

圖 6，illustrates that a terminal equipment can be any device such as a remote control

圖 7，illustrates that a portable hard drive can be used for sharing information for all the connected devices

Detail Descriptions of Embodiments

Embodiment 1:

本案為一種辨識連網設備以建立點對點連線的系統，以下將配合圖式說明本案的技術。

請參閱『圖 1』至『圖 2』，是本案的辨識連網設備以建立點對點連線的系統的架構示意圖，如圖所示，為方便說明本案技術內容，於本實施例中，本案的系統包含有一網路伺服器 10、一第一連網設備 20、一第二連網設備 21 與一終端設備 30，該終端設備 30 可為手機、平板電腦、筆記型電腦等具備有攝像頭的可攜式電子設備，而該第一與第二連網設備可為一網路攝影機、一網路監視鏡頭或一網路監視器，但並不用以限定本發明。於本實施例中，該終端設備 30 是為一手機，而該第一與第二連網設備 20、21 則分別為一網路攝影機。

該第一連網設備 20 與該第二連網設備 21 分別內建有一識別代碼 A 與 B，且該第一、第二連網設備 20、21 透過網際網路連線至該網路伺服器 10，其中，網路網路可為乙太網路(Ethernet)以及無線網路所建置的網際網路(Internet)、區域網路(LAN)、廣域網路(WAN)或虛擬私有網路(VPN)。可替代地，若該第一、第二連網設備 20、21 為設置於住宅內的網路攝影機，則該第一、第二連網設備 20、21 亦可藉由一路由器、一電力線網路橋接器與一電力線連接至網路伺服器 10，亦即，該第一、第二連網設備 20、21 可透過電力線傳輸的方式連接至網路伺服器 10，由於電力線傳輸並非本案的技術重點，且已可見於習知技術，故並不多加贅述。

該第一、第二連網設備 20、21 透過網際網路連線至該

網路伺服器 10，並且登錄各自的識別代碼 A、B 與其網路位址於該網路伺服器 10 的一連網設備列表之中。本案的技術重點在於該第一、第二連網設備 20、21 設置有一第一連線條碼 201 與一第二連線條碼 211，該第一與第二連線條碼 201、211 是分別儲存有該一第一、第二識別代碼 A、B 的資訊，而與本案實施例中，為了可儲存該第一、第二識別代碼 A、B 的複雜資訊，該第一與第二連線條碼 201、211 是為一二維代碼，例如一快速反應碼(QR code)，然該第一與第二連線條碼 201、211 亦不限定為一快速反應碼(QR code)，一維條碼亦是可行的實施方式。

為了能夠解讀該第一與第二連線條碼 201、211，本案揭示了兩種實施態樣。請參閱『圖 1』，在第一種實施態樣當中，該終端設備 30 包含有一供使用者操作的應用介面程式(API)與一影像截取模組 301，該影像截取模組 301 較佳的為一攝像頭，若使用者決定建立該第一連網設備 20 與該終端設備 30 的連線，則操作該應用介面程式(API)以令該影像截取模組 301 將設置於該第一連網設備 20 的第一連線條碼 201 的影像截取下來而產生一連線條碼影像，再藉由該終端設備 30 內部的一條碼解讀模組 302，將該連線條碼影像解讀為該第一識別代碼 A，緊接著，該終端設備 30 相應的產生一包含有該第一識別代碼 A 的連線請求訊號 303，該應用介面程式(API)透過該終端設備 30 所具備的無線網路，將該連線請求訊號 303 傳輸至該網路伺服器 10。

然而，考量到經過解碼後的第一識別代碼 A 有可能在無

線網路傳輸的過程中遭到攔截而被不肖人士所利用，本案亦揭示了第二種實施態樣。請參閱『圖 2』，在第二種實施態樣當中，該終端設備 30 包含有供使用者操作的應用介面程式(API)與一影像截取模組 301，若使用者決定建立該第一連網設備 20 與該終端設備 30 的連線，則操作該應用介面程式(API)以令該影像截取模組 301 截取該第一連線條碼 201 而產生一連線條碼影像，與第一種實施態樣不同的地方在於，第二種實施態樣的連線條碼影像並未在該終端設備 30 解讀，因此，該終端設備 30 所產生的該連線請求訊號 303 包含有該連線條碼影像。該應用介面程式(API)透過該終端設備 30 所具備的無線網路，將該連線請求訊號 303 傳輸至該網路伺服器 10。

由於該第一連線條碼 201 可為一快速反應碼(QR code)，因此，在第二種實施態樣中，該快速反應碼(QR code)可保有原來的影像格式而夾帶於該連線請求訊號 303，並透過無線網路傳輸至該網路伺服器 10，如此一來，因為他人需多一道解讀該快速反應碼(QR code)的程序，故本案系統的安全度能夠藉此提高。相應地，為了解讀該請求連線訊號 303 所包含的第一連線條碼 201，該網路伺服器 10 內部設置有該條碼解讀模組 101 以將該第一連線條碼 201 解讀為該第一識別代碼 A。

請復參閱『圖 3』，是本案的辨識連網設備以建立點對點連線的系統的傳送打洞連線訊息示意圖，如圖所示，當該網路伺服器 10 接收到該請求連線訊號 303，該請求連線訊號

303所包含的連線條碼影像不管是在終端設備30進行解讀或是在該網路伺服器 10 進行解讀，該請求連線訊號 303 都能夠經過分析而產生該第一識別代碼 A，如此，該網路伺服器 10 即可根據該第一識別代碼 A 於該連網設備列表中搜尋該第一識別代碼 A 所對應的連網設備的網路位址，於本實施例中，該第一識別代碼 A 即為該第一連網設備所內建的識別代碼，因此，該網路伺服器 10 接收到該請求連線訊號 303 後，即會藉由對應該第一識別代碼 A 的網路位址，向該第一連網設備 20 通知該終端設備 30 欲與該其連線的訊息，透過一習知的打洞技術(hole punching)，該網路伺服器 10 分別與該第一連網設備 20 與該終端設備傳輸一打洞連線訊息 401、402，此時，如『圖 4』所示，該第一連網設備 20 與該終端設備 30 建立一直接的通訊通道 50，藉此，該第一連網設備 20 與該終端設備 30 經由該通訊通道而可進行點對點連線。

更進一步，該第一連網設備 20 包含有一可供使用者設定的預設安全密碼，若使用者欲以該終端設備 30 登入該第一連網設備 20，則使用者於該終端設備 30 輸入一組安全密碼，該應用介面程式(API)再透過網際網路將該安全密碼傳送至該第一連網設備 20，當輸入的安全密碼與該預設安全密碼相同時，該終端設備 30 才取得授權而得以與該第一連網設備 20 進行資料交換。

且為了能夠省略手動輸入該預設安全密碼的過程，該第一連線條碼 201 除了對應該識別代碼外，亦可對應該預設安全密碼，如此一來，當該影像截取模組 301 截取該第一連網

設備 20 的第一連線條碼 201 以產生該連線條碼影像後，即可經由該條碼解讀模組 101、302 將該連線條碼影像解讀為該識別代碼與該預設安全密碼，使得該終端設備 30 與第一連網設備 20 建立點對點連線時，得以同時被授權而與該第一連網設備 20 進行資料交換。

於另一實施態樣中，該終端設備 30 的應用介面程式(API)得以將該第一連網設備 20 的識別代碼與預設安全密碼編譯為對應該識別代碼與預設安全密碼的連線條碼並儲存，以做為下次與該第一連網設備 20 建立點對點連接及資料交換所使用。但除上述的實施態樣外，該應用介面程式(API)亦可將該第一連網設備 20 的識別代碼與預設安全密碼編譯為對應該識別代碼與預設安全密碼的連線條碼後，透過無線網路將該連線條碼分享至另一終端設備，以令該另一終端設備得以對該第一連網設備 20 進行點對點連線及資料交換。

請復參閱『圖 5』，是本發明的連網設備與終端設備之間建立點對點連線流程示意圖，如圖所示，首先，使用者透過網際網路將至少一連網設備連線至一網路伺服器(步驟 S1)，該網路伺服器將該連網設備所內建的一識別代碼與一網路位址登錄於一連網設備列表之中，且設置一對應該識別代碼的連線條碼於該連網設備(步驟 S2)上，緊接著，使用者以一終端設備的影像截取單元截取該連線條碼以產生一對應該連線條碼的連線請求訊號，並將該請求連線訊號以該終端設備所具備的無線網路傳輸至該網路伺服器(步驟 S3)，該網路伺服器接收到該請求連線訊號後，自該連網設備列表尋找該

請求連線訊號所對應的連網設備，而向該連網設備通知該終端設備欲與其連線的訊息，透過打洞技術(hole punching)於該連網設備與該終端設備之間建立一通訊通道，藉此該連網設備與該終端設備經由該通訊通道進行點對點連線(步驟S4)。

In one embodiment，該終端設備 30 是為一手機，而該第一與第二連網設備 20、21 之任一也可為 a storage equipment, such as a portable hard drive, a portable solid state disk, a redundant disk array, etc.

Embodiment 2:

本案為一種辨識連網設備以建立點對點連線的系統，以下將配合圖式說明本案的技術。

請參閱『圖 1』至『圖 2』，是本案的辨識連網設備以建立點對點連線的系統的架構示意圖，如圖所示，為方便說明本案技術內容，於本實施例中，本案的系統包含有一網路伺服器 10、一第一連網設備 20、一第二連網設備 21 與一終端設備 30，該終端設備 30 可為 a storage device，such as a portable hard drive, a portable solid state disk, a remote control, a power extension cord 等不具備有攝像頭的電子設備。該第一與第二連網設備可為一 mobile phone, a PAD, a

notebook、一網路攝影機、一網路監視鏡頭或一網路監視器，但並不用以限定本發明。於本實施例中，該終端設備 30 是為一可攜式磁碟(a portable hard drive)，(Please note that 該終端設備 30 is now referring to a portable hard drive instead of a mobile phone and 影像截取模組 301 in Fig. 1 should be removed, for the descriptions in Embodiment 2)，而該第一與第二連網設備 20、21 則分別為一網路攝影機，其中 a proxy mobile phone (Not shown in Fig. 1) has a 影像截取模組將設置於該第一連網設備 20 的第一連線條碼 201 的影像截取下來而產生一連線條碼影像再將其傳送至該終端設備 30，再藉由該終端設備 30 內部的一條碼解讀模組 302，將該連線條碼影像解讀為該第一識別代碼 A。其中 the proxy mobile phone can transfer information to the terminal equipment through many ways such as wireless or wired lines. 另一實施方式為 the proxy mobile phone has a 影像截取模組將設置於該第一連網設備 20 的第一連線條碼 201 的影像截取下來而產生一連線條碼影像，再藉由 the proxy mobile phone 內部的一條碼解讀模組，將該連線條碼影像解讀為該第一識別代碼 A，再將該第一識別代碼 A 傳送至該終端設備 30。更有另一實施方式為連線條碼影像並未在該終端設備 30，也並未在 the mobile phone 中解讀，因此，該終端設備 30 所產生的該連線請求訊號 303 包含有該連線條碼影像。該應用介面程式(API)透過該終端設備 30 所具備的無線網路，將該連線請求訊號 303 傳輸至該網路伺服器 10。

更進一步，該第一連網設備 20 包含有一可供使用者設定的預設安全密碼，若使用者欲以該終端設備 30 登入該第一連網設備 20，則使用者於 the proxy mobile phone 輸入一組安全密碼，再將其傳送至該終端設備 30，該終端設備 30 之應用介面程式(API)再透過網際網路將該安全密碼傳送至該第一連網設備 20，當輸入的安全密碼與該預設安全密碼相同時，該終端設備 30 才取得授權而得以與該第一連網設備 20 進行資料交換。

且為了能夠省略手動輸入該預設安全密碼的過程，該第一連線條碼 201 除了對應該識別代碼外，亦可對應該預設安全密碼。當 the proxy mobile phone 影像截取模組截取該第一連網設備 20 的第一連線條碼 201 以產生該連線條碼影像後，該連線條碼影像即可經由一條碼解讀模組將該連線條碼影像解讀為該識別代碼與該預設安全密碼，使得該終端設備 30 與第一連網設備 20 建立點對點連線時，得以同時被授權而與該第一連網設備 20 進行資料交換。其中該連線條碼影像解讀可由該終端設備 30 來解讀，也可由 the proxy mobile phone 中來解讀，或是該終端設備 30 所產生的該連線請求訊號 303 包含有該連線條碼影像並傳輸至該網路伺服器 10，並由該網路伺服器 10 來解讀。

Other descriptions are the same as in Embodiment 1 described above. In this Embodiment 2, a proxy device, such as a mobile phone, is used to generate an image of a pattern, such

as a one dimensional Bar Code or a QR code, for inputting identification information for a terminal equipment, so that the terminal equipment, which has no image sensing capability or inputting capability for inputting a series of words, characters, symbols or digits by a user, can establish a p2P connection with other terminal equipments.

Please note that the proxy device such as a mobile phone can input identification information for a terminal equipment through an input device such as a keyboard, touch screen, etc. In other words, it is not necessary for the proxy device to have image sensing capability.

As shown in Fig. 6, the terminal equipment can be any device such as a remote control or a power control device such as a power extension code, a lamp, a water supply and etc., which has no imaging sensing or inputting capability for inputting identification information to establish a p2P connection with other terminal equipments. Likewise, the proxy device can be any device, such as a camera, a notebook, a PAD, etc., which has imaging sensing or inputting capability for inputting identification information in order to allow the terminal equipment to establish a p2P connection with other terminal equipments. Furthermore, the proxy device can transfer information to the terminal equipment through many

ways such as wireless or wired lines.

As shown in Fig. 7, the portable hard drive can be used for sharing information for all the connected devices, such as a mobile phone, an IP camera, a notebook, etc., by establishing P2P connections between the portable hard drive and all the connected devices.

綜上所述，本案主要是在該連網設備設置有對應該識別代碼的連線條碼，該終端設備透過內建的影像截取模組或是一外部裝置之影像截取模組以截取該連線條碼,而於該終端設備，該外部裝置或於該網路伺服器解讀該連線條碼為該識別條碼，藉此，本案可建立該終端設備與該連網設備的點對點連線，而可達到快速建立連線的目的。因此本發明極具進步性及符合申請發明專利的要件，以上已將本發明做一詳細說明，惟以上所述者，僅爲本發明的一較佳實施例而已，當不能限定本發明實施的範圍。即凡依本發明申請範圍所作的均等變化與修飾等，皆應仍屬本發明的專利涵蓋範圍內。

. CLAIMS

What is claimed is:

1. 一種辨識連網設備以建立點對點連線的系統，其特徵在於包括有：

至少一網路伺服器，該網路伺服器包含有一連網設備列表；

至少一連網設備，該連網設備內建有一識別代碼以及一對應該識別代碼且設置於該連網設備上的連線條碼，該連網設備透過網際網路連線至該網路伺服器以登錄該識別代碼於該連網設備列表中；

至少一終端設備，該終端設備包含有一影像截取模組，該終端設備以該影像截取模組截取該連網設備的連線條碼以產生一對應該連線條碼的連線請求訊號，該連線請求訊號透過網際網路傳輸至該網路伺服器；

其中，該網路伺服器自該連網設備列表尋找該連線請求訊號所對應的連網設備以向該連網設備通知該終端設備欲與其連線，使該連網設備與該終端設備之間建立一通訊通道，藉此該連網設備與該終端設備經由該通訊通道進行點對點連線。

2. 如權利要求第 1 項所述的系統，其特徵在於該影像截取模組截取該連網設備的連線條碼後產生一連線條碼影像。

3. 如權利要求第 2 項所述的系統，其特徵在於該終端設備包含有一將該連線條碼影像解讀為該識別代碼的條碼解讀模組，而該連線請求訊號包含有該識別代碼。

4. 如權利要求第 2 項所述的系統，其特徵在於該連線請求訊號包含有該連線條碼影像，而該網路伺服器包含有一將該連線條碼影像解讀為該識別代碼的條碼解讀模組。
5. 如權利要求第 1 項所述的系統，其特徵在於該網路伺服器執行打洞技術以建立該連網設備與該終端設備之間的通訊通道。
6. 如權利要求第 1 項所述的系統，其特徵在於該網際網路是選擇自乙太網路(Ethernet)、區域網路(LAN)、廣域網路(WAN)和虛擬私有網路(VPN)所組成的群組中的任何一種。
7. 如權利要求第 1 項所述的系統，其特徵在於該連網設備包含有一可供使用者設定的預設安全密碼，該終端設備輸入該預設安全密碼以登入該連網設備。
8. 如權利要求第 7 項所述的系統，其特徵在於該連線條碼更對應該預設安全密碼，該影像截取模組截取該連網設備的連線條碼後產生一連線條碼影像。
9. 如權利要求第 8 項所述的系統，其特徵在於該終端設備包含有一將該連線條碼影像解讀為該識別代碼與該預設安全密碼的條碼解讀模組，而該連線請求訊號包含有該識別代碼與該預設安全密碼。
10. 如權利要求第 8 項所述的系統，其特徵在於該連線請求訊號包含有該連線條碼影像，而該網路伺服器包含有一將該連線條碼影像解讀為該識別代碼與該預設安全密碼的條碼解讀模組。
11. 如權利要求第 1 至 10 項任一項所述的系統，其特徵在

於該連線條碼是為一快速回應碼(QR code)。

12.如權利要求第 1 至 10 項任一項所述的系統，其特徵在於該連線條碼是為一一維條碼。

13.一種辨識連網設備以建立點對點連線的方法，其特徵在於該方法包括以下步驟：

A.透過網際網路將至少一連網設備連線至一網路伺服器；

B.登錄該連網設備所內建的一識別代碼於該網路伺服器的一連網設備列表中，並設置一對應該識別代碼的連線條碼於該連網設備上；

C.透過一終端設備的一影像截取單元截取該連線條碼以產生一對應該連線條碼的連線請求訊號，並將該連線請求訊號透過網際網路傳輸至該網路伺服器；

D.自該連網設備列表尋找該連線請求訊號所對應的連網設備，使該網路伺服器向該連網設備通知該終端設備欲與其連線，再令該連網設備與該終端設備之間建立一通訊通道，藉此該連網設備與該終端設備經由該通訊通道進行點對點連線。

14.如權利要求第 13 項所述的方法，其特徵在於步驟 C 更包括以下子步驟：

子步驟 1：以該終端設備的一條碼解讀模組解讀該連線條碼影像為該識別代碼；

子步驟 2：令該連線請求訊號包含有該識別代碼。

15.如權利要求第 13 項所述的方法，其特徵在於步驟 C 更包括以下子步驟：

子步驟 1：令該連線請求訊號包含有該連線條碼影像；

子步驟 2：透過網際網路將該連線請求訊號傳輸至該網際網路伺服器。

16.如權利要求第 15 項所述的方法，其特徵在於步驟 D 更包括以下子步驟：

子步驟 1：接收該連線請求訊號；

子步驟 2：以該網路伺服器的一條碼解讀模組解讀該連線請求訊號為該識別代碼。

17.如權利要求第 13 項所述的方法，其特徵在於步驟 D 之後更包括下述的步驟：

E.自該終端設備輸入一安全密碼；

F.判斷該安全密碼是否相同於該連網設備的一預設安全密碼，若否，則跳回步驟 E，若是，則允許該終端設備登入該連網設備。

18.如權利要求第 13 項所述的方法，其特徵在於該網路伺服器執行打洞技術以建立該連網設備與該終端設備之間的通訊通道。

19.如權利要求第 13 項所述的方法，其特徵在於該網際網路是選擇自乙太網路(Ethernet)、區域網路(LAN)、廣域網路(WAN)和虛擬私有網路(VPN)所組成的群組中的任何一種。

20.如權利要求第 13 至 19 項任一項所述的方法，其特徵在於該連線條碼是為一快速回應碼。

21.如權利要求第 13 至 19 項任一項所述的方法，其特徵在

於該連線條碼是為一一維條碼。

ABSTRACT

一種辨識連網設備以建立點對點連線的系統與方法，該系統包含有網路伺服器、複數個連網設備與終端設備。該方法包括有：透過網際網路將連網設備連線至網路伺服器；登錄連網設備的識別代碼於網路伺服器的連網設備列表中，並設置對應識別代碼的連線條碼於連網設備上；透過終端設備的影像截取單元截取連線條碼以產生連線請求訊號，並將連線請求訊號透過網際網路傳輸至網路伺服器；自連網設備列表尋找對應的連網設備，使網路伺服器向連網設備通知終端設備欲與其連線，再令連網設備與終端設備之間建立通訊通道以進行點對點連線。

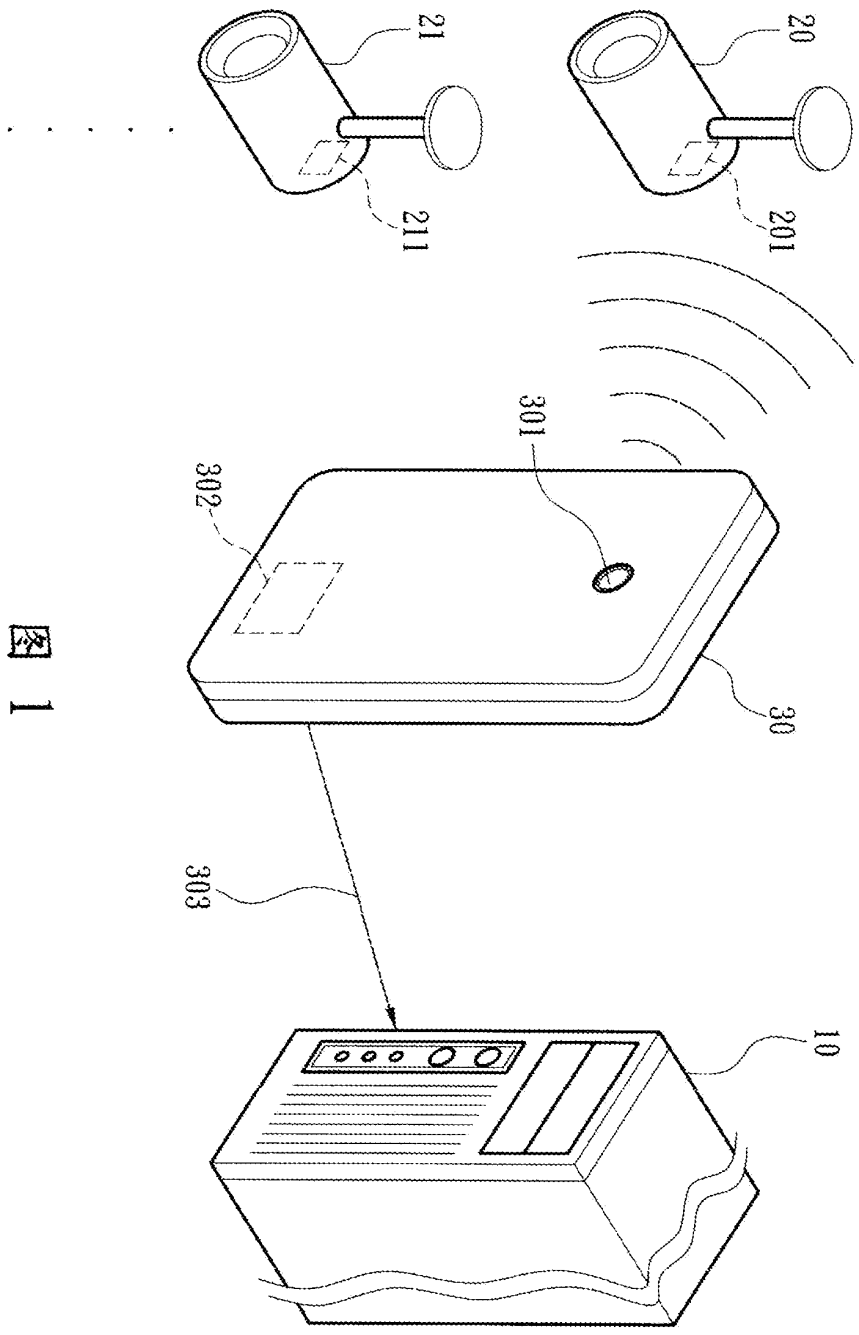


图 1

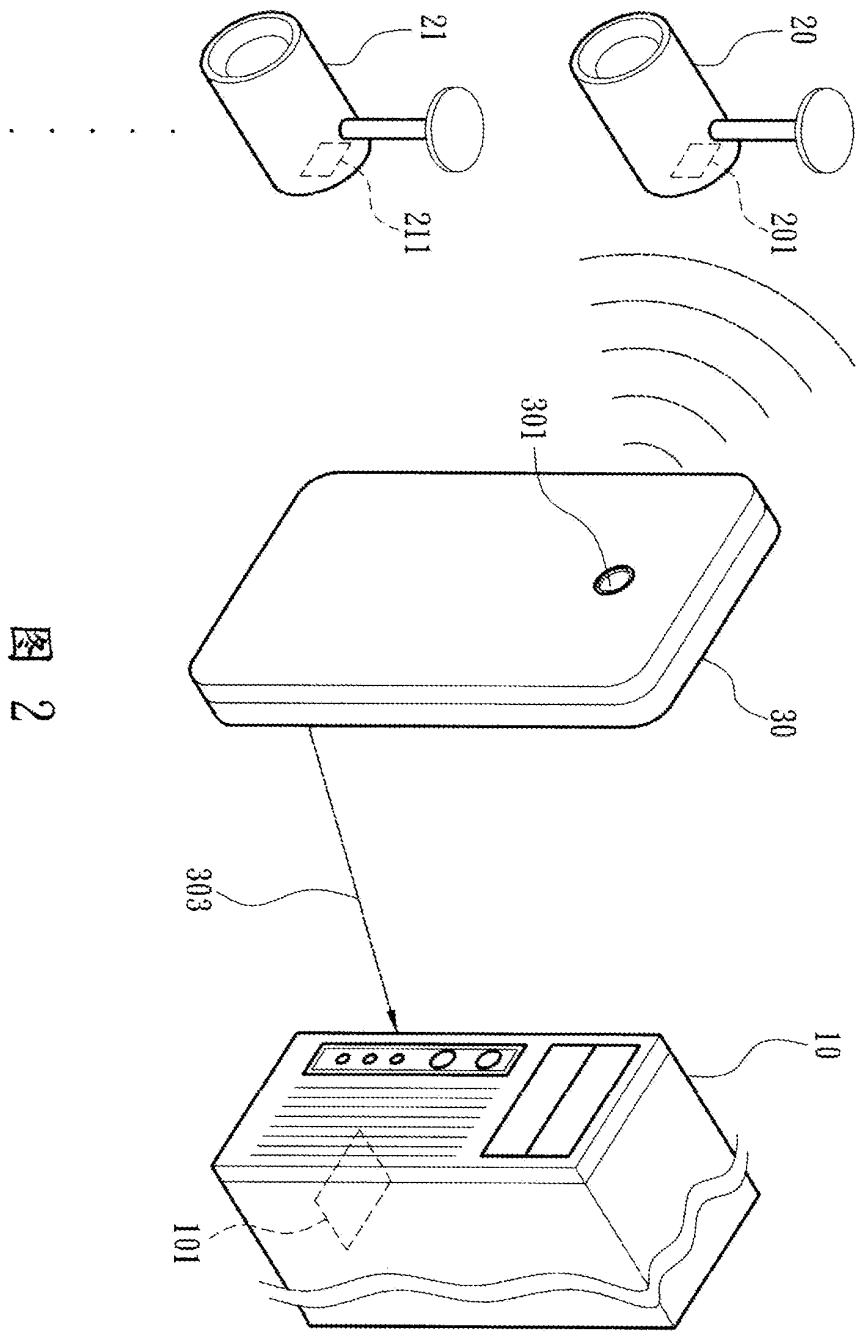


圖 2

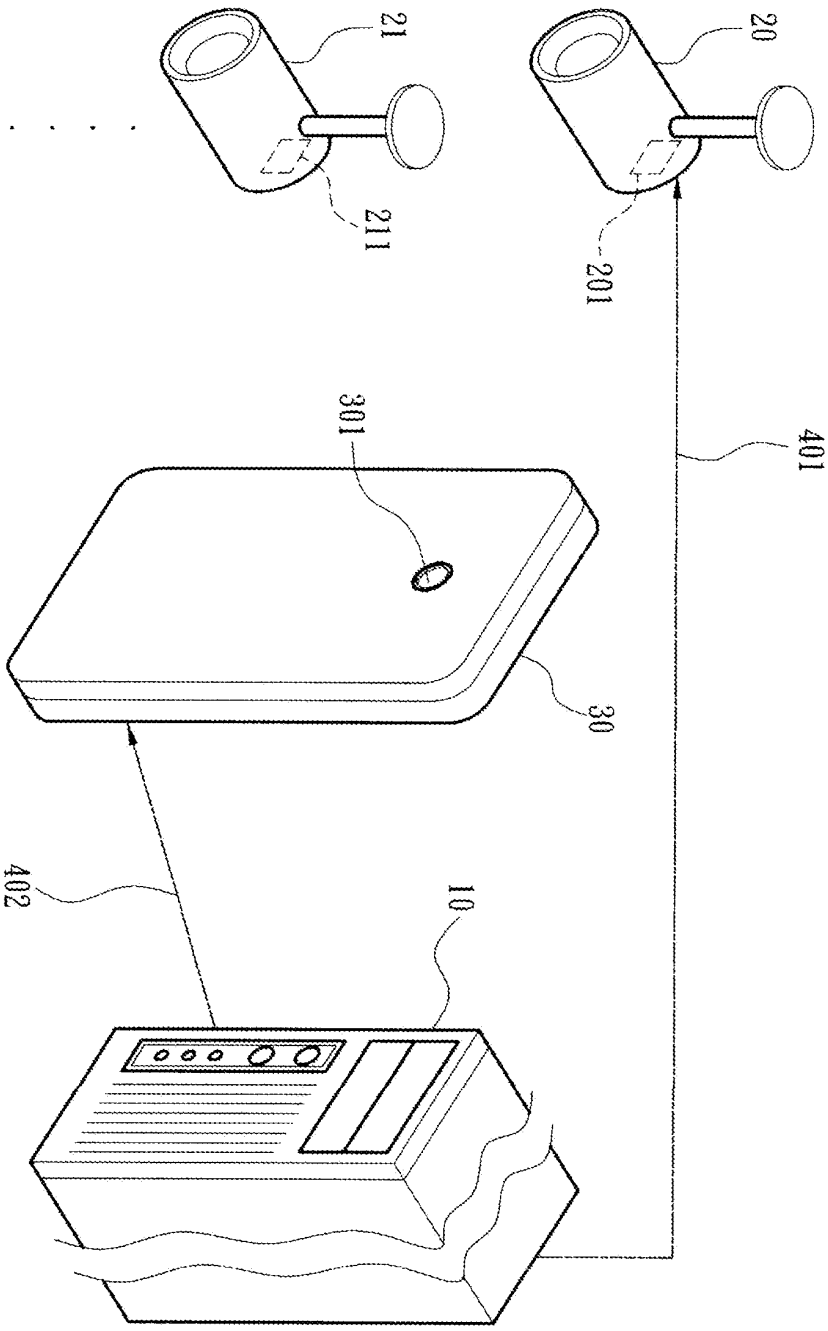


圖 3

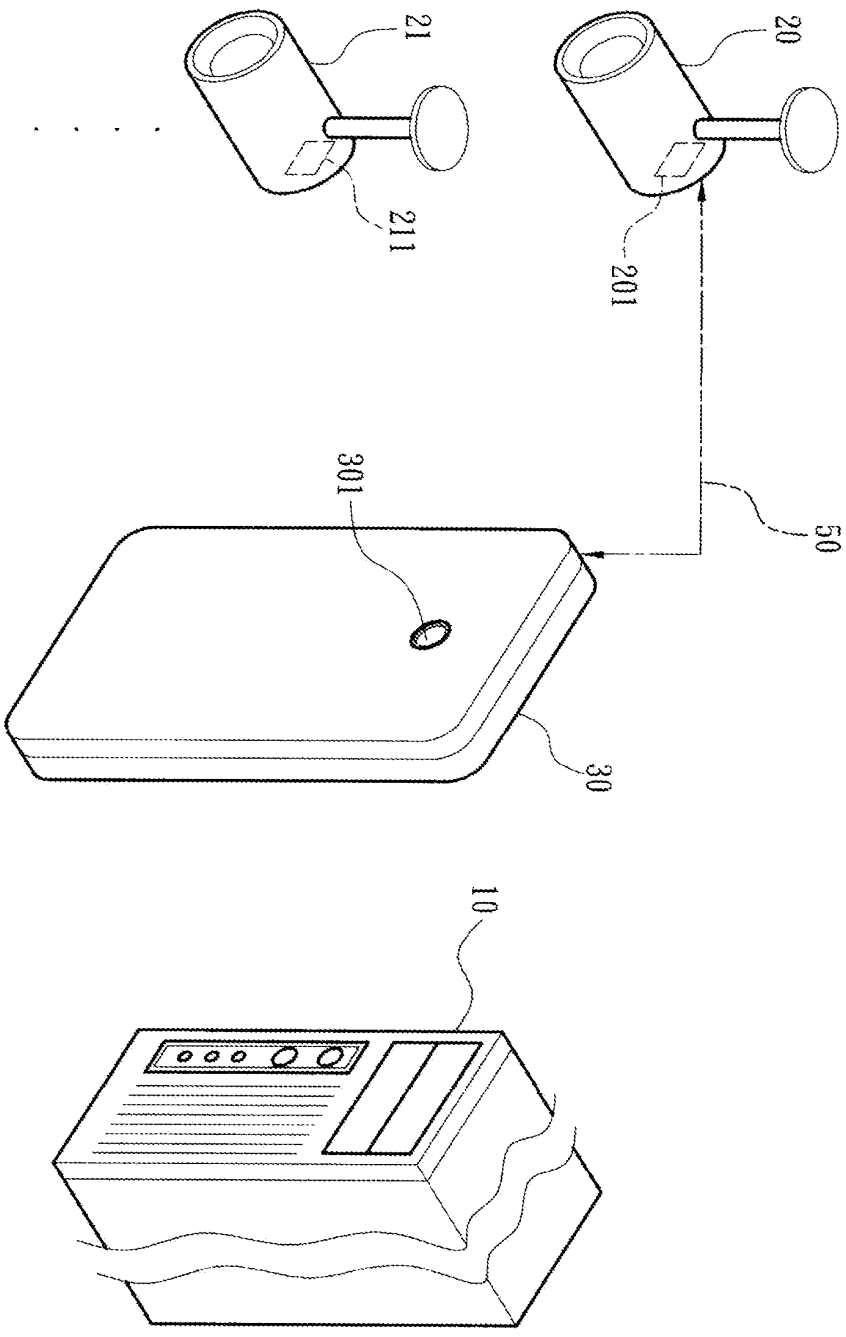


圖 4

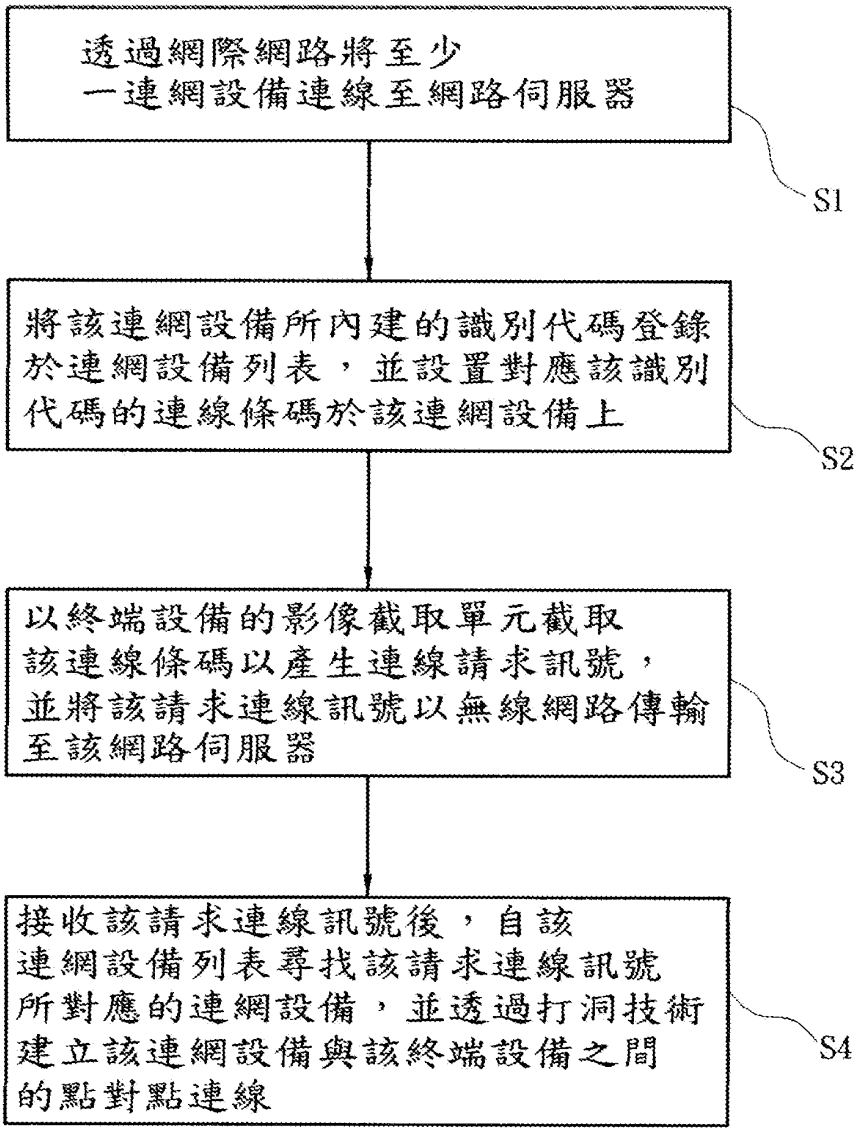

透過網際網路將至少
一連網設備連線至網路伺服器
S1
將該連網設備所內建的識別代碼登錄
於連網設備列表，並設置對應該識別
代碼的連線條碼於該連網設備上
S2
以終端設備的影像截取單元截取
該連線條碼以產生連線請求訊號，
並將該請求連線訊號以無線網路傳輸
至該網路伺服器
S3
接收該請求連線訊號後，自該
連網設備列表尋找該請求連線訊號
所對應的連網設備，並透過打洞技術
建立該連網設備與該終端設備之間
的點對點連線
S4

图 5

Smart Control:

- Smart IR Remote controller
- Smart Strip for power saving

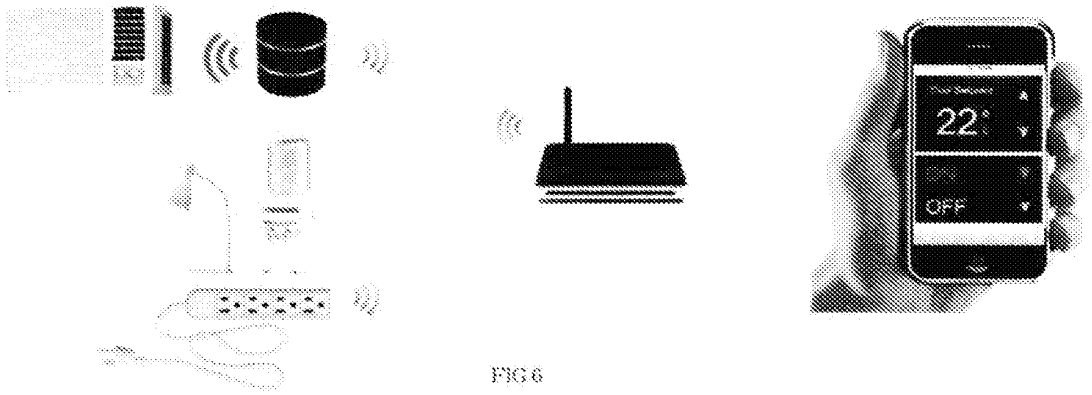


FIG 6

Smart Personal Cloud:

- Personal Cloud for smart phone
- Always connected

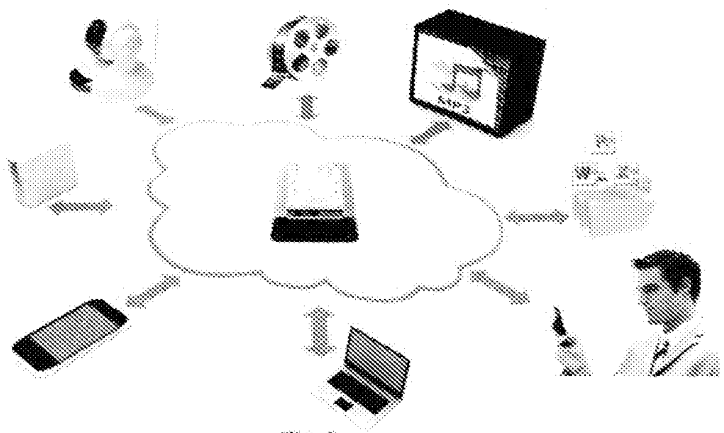


FIG. 7

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	A METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME
First Named Inventor/Applicant Name:	Patrick Kuo
Filer:	Min-Lee Teng
Attorney Docket Number:	6121.001.PPA

Filed as Small Entity

Provisional Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Provisional Application Filing Fee	2005	1	130	130
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**130**

Electronic Acknowledgement Receipt	
EFS ID:	15525251
Application Number:	61812262
International Application Number:	
Confirmation Number:	9399
Title of Invention:	A METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME
First Named Inventor/Applicant Name:	Patrick Kuo
Customer Number:	11336
Filer:	Min-Lee Teng
Filer Authorized By:	
Attorney Docket Number:	6121.001.PPA
Receipt Date:	16-APR-2013
Filing Date:	
Time Stamp:	04:56:27
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$130
RAM confirmation Number	8252
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Provisional Cover Sheet (SB16)	6121_001US_PPA_Cover_Sheet.pdf	2071565 998e2a54d2f9e58db16bb5664a9b2edecef95cfc	no	3
Warnings:					
Information:					
2	Specification - Not in English	6121_001US_Specification.pdf	1804867 d04729a390a1ac0838c02fe1f3091b5361172430	no	29
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29867 9291e181d2286f67fdc161abb3c5f66cd243d28b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3906299		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
61/812,262	04/16/2013	Patrick Kuo	6121.001.PPA

CONFIRMATION NO. 9399

11336
Min-Lee Teng
Litron Patent and Trademark Office
7F-2, No. 79, Sec.2, Roosevelt Rd.
Taipei, 106
TAIWAN

IMPROPER PROVISIONAL LETTER

OC00000061471270

Date Mailed: 05/31/2013

Letter re Non-English Language Application Papers in a Provisional Application

The above-identified provisional application was filed in a language other than English. An English-language translation of a non-English provisional application and a statement that the translation is accurate must be filed in the provisional application. See 37 CFR 1.78(a)(5)(iv). Applicants are strongly encouraged to file the English-language translation of the provisional application and the statement that the translation is accurate in the provisional application before a nonprovisional application claiming the benefit of the provisional application is filed, or, alternatively, when making a claim for the benefit of the provisional application in a nonprovisional application. If, however, an English translation and a statement that the translation is accurate have not been filed in the above-identified provisional application when a nonprovisional application is filed claiming the benefit of the filing date of the provisional application, the Office should mail a Notice requiring an English translation and the statement to be filed in the provisional application and a confirmation to be filed in the nonprovisional application.

In the event that the Office schedules a nonprovisional application that claims the benefit of a provisional application filed in a language other than English for publication without issuing a Notice requiring the applicant to file an English translation of the non-English provisional application, the applicant should file the English translation of the non-English provisional application and a statement that the translation is accurate as soon as possible in the provisional application.

/laguirre/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
61/812,262	04/16/2013		130	6121.001.PPA		

CONFIRMATION NO. 9399

FILING RECEIPT

11336
Min-Lee Teng
Litron Patent and Trademark Office
7F-2, No. 79, Sec.2, Roosevelt Rd.
Taipei, 106
TAIWAN

Date Mailed: 05/31/2013

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Patrick Kuo, Yilan County, TAIWAN;

Applicant(s)

Patrick Kuo, Yilan County, TAIWAN;

Power of Attorney:
Min-Lee Teng--65623

If Required, Foreign Filing License Granted: 05/23/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/812,262**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent

in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Min-Lee Teng
Litron Patent and Trademark Office
7F-2, No. 79, Sec.2, Roosevelt Rd.
Taipei, 106
TAIWAN

Courtesy Reminder for
Application Serial No: 61/812,262

Attorney Docket No: 6121.001.PPA
Customer Number: 11336
Date of Electronic Notification: 05/31/2013

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

miketeng@litronip.com
miketeng@litron-intl.com
janiceshih@litron-intl.com

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. :	61/812,262	Confirmation No. :	9399
First Applicant:	Patrick KUO	Filed :	16-APRIL-2013
Docket No. :	6121.001.PPA	Customer No. :	11336

Incoming Letter to Submit English Translation of the Specification

Dear Sir:

Applicants hereby submit an English translation of the specification of the provisional application, **61/812,262**, and state that the translation is accurate.

Respectfully Submitted,

Date: Jun. 27, 2016

/Min-Lee Teng/
Min-Lee Teng
Reg. No. 65,623

7F-2, No. 79, Sec. 2, Roosevelt Rd.
Taipei, Taiwan
Tel: +886-2-2362-7180
Email: miketeng@litron-intl.com

SYSTEM AND METHOD OF IDENTIFYING NETWORKED DEVICE FOR ESTABLISHING A P2P CONNECTION

I. Field of the Invention

The present invention relates to establishing a network connection and, in particular, to establishing a P2P (Point to Point) connection.

II. Description of the Prior Art

With the advancement of technology and popularity of the network, the user can set up a network video camera to monitor places around the world via the Internet. When an emergency occurs, the user can take advantage of the alarm systems connected to the Internet to notify local Response Center to take urgent measures to put the emergency situation in control. Although the Internet has great use value in fighting against the crime and preservation of evidence, but the conventional network cameras need to match the complex wiring for connecting the cameras. If you want to install a security surveillance system in home, you must install complex wiring to configure cameras in every corner of the home. In response to these shortcomings, the market generally use wireless LAN to connect each webcam, because the wireless network does not require wired lines, which eliminates the complex installation process. But the wireless LAN also has some disadvantages, because the wireless transmission is based on electromagnetic waves which can be blocked by the walls and the spaces between upstairs and downstairs.

Power Line Communication becomes a promising method as a solution to the last mile of the broadband communication, because it does not have the above-mentioned disadvantages in wireline and wireless network. Power line transmission, by definition, refers to sinal transmission utilizing the existing power lines in home with a high-speed transmission rate of data, voice, video and multimedia services.

The Power Line Communication uses the frequency bands in 4MHz to 21MHz or 2MHz to 30MHz to transmit signals. It uses orthogonal Frequency division multiplexing (OFDM) techniques for signal coding and modulation at the transmitting end, and then the modulated signal will be transmitted in power line. At the receiving end, the receiver coupled to the power line will decode and demodulate the OFDM signal so as to recover back to the original signal, which can save a huge amount of cost, because the power line signal is not blocked by all of the barriers in home. And the power transmission line technique can be found in the relevant patent applications such as US2005/ 0047379 and US2004 / 0,186,908.

The power line transmission can use P2P connection to connect different cameras at different locations as well. Please refer to the China Taiwan Patent Publication No. M382669, which disclosed a network video surveillance equipment and control system, which includes camera, a powerline network bridge, a first router and a second router, a P2P connection server and a monitoring device. After the camera captures the images and compresses the images into digital video signals and transmits the video signals to the powerline network bridge, and then connect to the Internet via the first router.

When the camera device is connected to the Internet, it will automatically connect to the P2P server, the server would perform a hole-punching technique in the second router connected to the monitoring device, and the monitoring device can be directly connected to camera device

via the Internet without going through the P2P server. Although the system using the power line to connect the camera device and the surveillance device, it will be limited to the P2P serves of a single service; therefore, the scalability and the comparability are very much limited.

To overcome the above-mentioned issue, the prior art discloses a platform for connectivity of Things through point to point network, wherein the platform has a management server, a plurality of proximal equipment and networked devices having a plurality of application program interfaces, wherein the management server and the linking server establish a P2P connection through the Internet, and the application programming interface (API) can be applied to a variety of different operating systems.

In the actual mode of operation, each of the networked devices has an identification code (ID) and automatically connects to the management server and registers the identification code (ID) of the networked device in the management server, the terminal device can make a request to the management server to provide addressing information of a linking sever for connecting to the networked device by inputting the identification code (ID) of the networked device for establishing a P2P connection between the networked device and the terminal device through an identical application programming interface (API).

While the foregoing system solves the connection problems when the number of network equipment increases, however, the number of identification codes and the complexity of the connecting process will increase as well, especially when the identification code is more than 10

digits or English characters or a combination thereof. When the users want to select a networked device to monitor some activities, the identification code of the networked device must be inputted to the proximal end equipment. Even if the proximal end equipment is a smart phone, it is complicated and cumbersome to input such a lengthy identification code (ID) to establish a connection.

SUMMARY

One object of the present invention is to solve the slow process of establishing connections between the terminal devices and networked devices, which is caused by excessive number of digits or characters in the identification codes.

To achieve the above object, the present invention discloses a system to identify networked devices for establishing P2P connections, wherein the system comprises at least one network server, at least one networked device and at least one terminal device, wherein the server has a list of networked devices; the networked device has an identification code and a barcode corresponding to the identification code, the networked device registers its identification code to a list of networked devices in a server through Internet;

The terminal device includes an image capture unit which captures the barcode of the networked device for generating a connection request signal corresponding to the barcode,

The connection request signal is transmitted through the Internet to the network server, wherein the network server identifies the networked device from the list of networked devices corresponding to the connection request signal and notifies the networked device that the terminal device is requesting to make a connection therewith, so that a communication channel can be established between the networked device and the terminal device, whereby a P2P connection can be established via the communication channel.

According to the system described above, the present invention provides a method to identify networked device for establishing a P2P connection, wherein the method comprises the steps of: (a) connecting at least one networked device to a network server through the Internet; (b) registering the identification code of the networked device to the list of networked devices of the server and setting up a barcode corresponding to the identification code on the networked device; (c) capturing the barcode of the networked device by an image capture unit of the terminal device to capture the barcode to produce a connection request signal corresponding to the barcode; (d) identifying, by the network server, the networked device from the list of networked devices corresponding to the connection request signal and notify the networked device that the terminal device is requesting to make a connection therewith, so that a communication channel can be established between the networked device and the terminal device, whereby a P2P connection can be established via the communication channel.

In one embodiment of the method described above, the step (c) further comprises the sub-steps of: (c1) interpreting the barcode image to an identification code; (c2) embedding the identification code in the connection request signal.

In one embodiment of the method described above, in order to avoid the interception of the identification code by unauthorized individuals, step (c) further comprises the sub-steps of (c1) embedding the connection barcode image in the connection request signal; (c2) transmitting the connection request signal to the server through the Internet, wherein step (d) further comprises the sub-steps: (d1) receiving the connection request signal; (d2) interpret the barcode image to an identification code by an image interpreting unit of the server.

Furthermore, in order to avoid unauthorized use of the terminal device to monitor by the networked devices, the step (d) further comprises the following steps: (e) input a security code through the terminal device; (f) determine whether the security password is the same as a default security password in the networked device, if not, then back to step (e), and if so, allow the terminal device to log on to the networked device.

In another embodiment in accordance with the present invention, the network server to perform holes punching to establish a communication channel between a terminal device and a networked device. In another embodiment of the present invention, the Internet is based on Ethernet

(Ethernet), local area network (LAN), wide area network (WAN) and virtual private network (VPN) group consisting of any kind.

In another embodiment of the present invention, connection barcode image should be matched with the default password, and the image capture unit captures the barcode of the networked device to produce a connection request signal corresponding to the barcode.

In another embodiment of the present invention, the terminal includes an image interpreting unit to interpret the barcode image into an identification code and a default password, and the connection request signal carries the identification code and the default password.
In another embodiment of the present invention, the connection request signal carries the connection barcode image, and the server includes an image interpreting unit to interpret the barcode image into the identification code and the default password.

In another embodiment of the present invention, the connection barcode is a QR code or one-dimensional barcode. With the above technical solution, the present invention has the following advantages: It can quickly establish connections between mobile devices and networked devices. Unlike prior art to manually enter the identification code word by word, the image capture unit of a mobile phone captures the barcode image of the networked device, the barcode image is then converted into the identification code so as to allow the server to establish a P2P connection between the networked device and the terminal device.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing aspects and many of the accompanying advantages of this invention will become more readily appreciated as the same becomes better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

Fig.1 illustrates a schematic of a system to identify a networked device for establishing a P2P connection according to one embodiment of the present invention;

Fig.2 illustrates a schematic of a system to identify a networked device for establishing a P2P connection according to one embodiment of the present invention;

Fig.3 illustrates a schematic of transmission hole-punching messages to establish a P2P connection;

Fig.4 depicts a schematic of a P2P connection;

Fig.5 depicts a flowchart of establishing a P2P connection; and

Fig.6 illustrates that a terminal equipment can be any device such as a remote control;

Fig.7 illustrates that a portable hard drive can be used for sharing information for all the connected devices.

Detail Descriptions of Embodiments

Embodiment 1:

The present invention provides a system to identify a networked device for establishing a P2P connection. The technology of the present invention are described as follows along with the drawings.

Please refer to Fig. 1 to Fig. 2, which illustrates a schematic of a system to identify a networked device for establishing a P2P connection, wherein the system includes a network server 10, a first networked device 20, a second networked device 21 and a terminal device 30, wherein the terminal device 30 can be portable electronic devices such as mobile phones, tablet computers, notebook computers equipped with cameras, but not limit to; and the first and second networked device can be a webcam, a network surveillance camera or a network monitor, but not limit to.

In this embodiment, the terminal device 30 is a cell phone, and each of the first and second networked devices 20, 21 is a webcam. The first networked devices 20 and 21 have a built-in identification code A and B respectively, and the first, second networked devices 20, 21 connect to the network server 10 through the Internet, wherein the Internet can be based on Ethernet, wireless networks, local area network (LAN), wide area network (WAN) or virtual private network (VPN).

Alternatively, if the first, second networked device 20, 21 is a network camera installed in a house, the first and second networked device can use a power line to connect to a network server 10 through a router and a bridge to bridge the power line to the router. That is, the first and second networked devices 20, 21 can be connected to network server 10 through the power line. As the power line transmission technology is not the focus of current invention and is well known in the art, it is not described herein further. The first and second networked devices 20, 21 connect to the network server 10 through the Internet, and register identification codes A, B and their network

addresses respectively in a list of networked devices of the network server 10.

One key focus of the present invention is that the first and second networked device 20, 21 is respectively equipped with a first connection barcode 201 and a second connection barcode 211, the first and second connection bar 201, 211 are respectively stored with information of the first and the second identification codes A, B. Each of the first and second connection barcodes 201 211 is a two-dimensional code such as a quick response code (QR code), however, it is not limited to that and it can be in other form such as a one-dimensional barcode.

In order to interpret the first and second connection barcode 201, 211, two embodiments are disclosed as follows. Please refer to Fig.1, in one embodiment, the terminal device 30 includes an application program interface (API) and an image capture unit 301 preferably a camera. If the user decides to connect the terminal device 30 to the first networked device 20, she/he can operate the application program interface (API) to enable the image capture unit 301 to capture the image of the connection barcode 201 on the first networked device 20 to produce a connection barcode image, and then convert the captured barcode image to a first identification code A by an interpretation unit 302, then the terminal device 30 generates a first connection request signal 303 comprising the identification code A, and the application programming interface (API) transfers the connection request signal 303 to the network server 10 through a wireless device of the terminal device 30.

However, after taking into consideration that the decoded first identification code can be intercepted by unauthorized individuals during transmission in the wireless network, a second embodiment of the present invention is also disclosed. Please refer to Fig.2, in one embodiment, the terminal device 30 includes an application program interface (API) and an image capture unit 301. If a user decides to connect the terminal device 30 to the first networked device 20, she/he can operate the application program interface (API) to enable the image capture unit 301 to capture the first connection bar 201 to produce a connection barcode image, however, in this embodiment, the connection barcode image will not be interpreted in the terminal device 30, therefore, the terminal device 30 sends a connection request signal 303 containing the connection barcode image instead of the identification code of the first networked device 20. The application programming interface (API) transfers the connection request signal 303 to the network server 10 through a wireless device of the terminal device 30.

As the first connection barcode 201 can be a QR code, the QR code can be kept in its original form and carried in the connection request signal 303 and transmitted to the network server 10 through a wireless network. Thus, the security can be enhanced as an extra interpretation procedure of the QR code is necessary for those unauthorized individuals. Accordingly, in order to interpret the first connection bar 201 carried in the connection request signal 303, the network server 10 is equipped with a barcode interpretation unit 101 for converting the first connection barcode 201 to the first identification code A.

Please refer to Fig. 3 which illustrates a schematic of transmitting messages for punching holes to establish a P2P connection. As shown in Fig. 3, when the network server 10 receives the connection request signal 303, the first identification code A can be obtained by analyzing the connection request signal 303 no matter if the interpretation of the barcode image is done in the terminal device 30 or in the network server 10,

As a result, the network server 10 can search for the network address of the networked device in the list of the networked devices corresponding to the first identification code, in this embodiment, the first identification code is just the same as the built-in identification code of the first networked device,

Therefore, when the network server 10 receives the connection request signal 303, it will notify the first networked device 20 that the terminal device 30 is making a request to connect therewith, according to the network address of the networked device corresponding to the first identification code. Through hole-punching technique, which is well known in the field, the server 10 respectively transmits hole-punching messages 401, 402 to the first networked device 20 and the terminal device 30 respectively. At this time, as shown in Fig. 4, a direct communication passage 50 is established between the first networked device 20 and the terminal device 30; and a P2P connection is then established between the first networked device 20 and the terminal device 30 via the direct communication passage 50.

Furthermore, the first networked device 20 has a default security password which can be set by a user. If a user tries to use the terminal device 30 to log on the first networked device 20, the user inputs to the terminal device 30 a security password and the application programming interface (API) then send the security password to the first networked device 20 through the internet. Only when the input security password matches the default security code, will the terminal equipment 30 be authorized to connect to the first networked devices 20 to exchange data.

In order to avoid manually entering the default security password, the first connection barcode 201 can carry the identification code as well as the security password. By doing so, when the image capture unit 301 captures the first barcode of the first networked device 20 to produce a first connection barcode image, the barcode image interpretation units 101, 302 convert the first connection barcode image into the identification code and the security password. When the terminal device 30 is connected to the networked devices 20, it will be authorized to exchange data with the networked devices 20 at the same time.

In another embodiment, the application programming interface (API) of the terminal device 30 can convert the identification code and default security password into a connection barcode, which can be stored for establishing a P2P connection with the first networked device 20 to exchange data, next time.

In one embodiment, after the terminal device 30 converts the identification code and default security password into a connection barcode, the terminal device 30 can transmit the connection barcode to other terminal devices to enable them to establish a P2P connection with the first networked devices 20 to exchange data as well.

Please refer to Fig. 5 which depicts a flowchart of establishing a P2P connection between the terminal devices and networked devices. As shown Fig. 5, firstly, connect at least one networked device to a server over the Internet (step S1). Then, the server registers an identification code and a network address of the networked device in a list of networked devices, and sets up a connection barcode corresponding to the identification code on the networked device (step S2), and

Then, the terminal device 30 captures the connection barcode to produce a connection request signal 303 and transfers the connection request signal 303 to the network server 10 through a wireless device of the terminal device 30 (step S3), the network server 10 receives the connection request signal and searches for the networked device in the list of the networked devices according to the connection request signal, and notify the first networked device 20 that the terminal device 30 is making a request to connect therewith. Through hole-punching technique, a communication channel between the networked device and the terminal device is established for establishing a P2P connection between the networked device and the terminal device (step S4).

In one embodiment, the terminal device 30 is a cell phone, and the first and second networked devices 20, 21 can be storage equipment, such as portable hard drive, portable solid state disk, redundant disk array, etc.

Embodiment 2:

The embodiment 2 of present invention provides a system to identify a networked device for establishing P2P connection. The technology of the present invention are described as follows along with the drawings.

Please refer to Fig. 1 to Fig. 2, which illustrates a schematic of a system to identify a networked device for establishing a P2Pconnection, wherein the system includes a network server 10, a first networked device 20, a second networked device 21 and a terminal device 30, the terminal device 30 can be a storage device such as a portable hard drive, a portable solid state disk, a remote control, a power extension cord, which does not have a camera or lens to capture images.

The first and second networked device can be a mobile phone, a PAD, a notebook, a webcam, a network surveillance camera or one network monitor, but not limit to. In this embodiment, a terminal device 30 is a portable hard drive，(Please note that terminal device 30 is now referring to a portable hard drive instead of a mobile phone and the image capture unit 301 in Fig. 1 should be removed, for the descriptions in Embodiment 2)，and the first and second networked devices 20, 21 respectively a webcam, wherein a proxy mobile phone (Not shown in Fig. 1) has an image capture unit to capture the barcode image of the first networked device 20 to produce a connection

barcode and transmits to the terminal device 30, and an interpreting unit 302 of the terminal device 30 converts the connection barcode into the first identification code A, wherein the proxy mobile phone can transfer information to the terminal equipment through many ways such as wireless or wired lines.

In another embodiment, the proxy mobile phone has a video capture unit to capture the barcode image of the first networked device 20 to produce a connection barcode image; and an interpreting unit to convert the connection barcode into the first identification code A and transmit the first identification code A to the terminal device 30.

In another embodiment the connection code image is not interpreted in the terminal device 30 and the mobile phone, therefore, the terminal device 30 embeds the connection code image in the connection request signal 303 which is transmitted to the network server 10 through a wireless network via an application programming interface (API) of the terminal device 30.

Furthermore, the first networked device 20 includes a default security password which can be set by a user, if a user tries to use the terminal device 30 to log on the first networked device 20, the user inputs a security password to the proxy mobile phone and the proxy mobile phone transmits a security password to the terminal device 30. The application programming interface (API) of the terminal device 30 then sends the security code to the first networked device 20 through the internet; only when the input security password matches the default security code, will the terminal equipment 30

obtain the authorization to connect to the first networked devices 20 to exchange data. In order to avoid manually entering the default security password, the first connection barcode 201 can carry the identification code as well as the security password.

When the proxy mobile phone video interception unit captures first connection bar 201 of the first networked device 20 to generate a connection barcode image, an image interpretation unit converts the connection barcode image into the identification code with the default security code, so that a P2P connection can be established between the terminal device 30 and the first networked device 20, and at the same time the terminal device 30 is authorized to exchange data with the first networked device 20, wherein the connection barcode image can be interpreted by an interpreting unit in the terminal device 30, the proxy mobile phone. Alternatively, the terminal device 30 sends the connection request signal 303 to the server 10 in which the connection barcode image can be interpreted.

Other descriptions are the same as in Embodiment 1 described above. In this Embodiment 2, a proxy device, such as a mobile phone, is used to generate an image of a pattern, such as a one dimensional Barcode or a QR code, for inputting identification information for a terminal equipment, so that the terminal equipment, which has no image sensing capability or inputting capability for inputting a series of words, characters, symbols or digits by a user, can establish a P2P connection with other terminal equipment.
Please note that the proxy device such as a mobile phone can input identification information for terminal equipment through an input device

such as a keyboard, touch screen, etc. In other words, it is not necessary for the proxy device to have image sensing capability.

As shown in Fig. 6, the terminal equipment can be any device such as a remote control or a power control device such as a power extension code, a lamp, a water supply and etc., which has no imaging sensing or inputting capability for inputting identification information to establish a p2P connection with other terminal equipment. Likewise, the proxy device can be any device, such as a camera, a notebook, a PAD, etc., which has imaging sensing or inputting capability for inputting identification information in order to allow the terminal equipment to establish a p2P connection with other terminal equipment. Furthermore, the proxy device can transfer information to the terminal equipment through many ways such as wireless or wired lines.

As shown in Fig. 7, the portable hard drive can be used for sharing information for all the connected devices, such as a mobile phone, an IP camera, a notebook, etc., by establishing P2P connections between the portable hard drive and all the connected devices.

In summary, a connection barcode is attached to a networked device corresponding to an identification code of the networked device, the connection barcode can be scanned by an image capture unit, in the terminal device or an external device, to capture the connection barcode, and the captured connection barcode image can be interpreted in the terminal device, the external device or on the network server to obtain the identification code of the networked device, whereby a P2P connection can be established between the terminal device and the networked device quickly.

The present invention is therefore nonobvious and meets the requirements to apply for a patent, the above embodiments are just preferred embodiments, and should not limit the scope of the present invention. Any modifications and alterations made according to the claims are all within the protection of this invention.

CLAIMS

What is claimed is:

1. A system to identify a networked device for establishing a P2P connection, the system comprising:

at least one network server having a list of networked devices;

at least one networked device, wherein the networked device has an identification code and a connection barcode corresponding to the identification code being attached on the networked device, wherein the networked device registers the identification code into the list of networked devices by connecting to the network server through the Internet;

at least one terminal device, wherein the terminal device comprises an image capturing module, wherein the terminal device generates a connection request signal when the connection barcode is captured to the terminal device by the image capturing module; and the terminal device transmits the connection request signal to the network server through the Internet, wherein the network server identifies the networked device in the list of the networked devices according to the connection request signal so as to establish a P2P connection between the terminal device and the networked device.

2. The system according to claim 1, wherein a barcode image of the connection barcode is generated after the image capturing module captures the connection barcode.

3. The system according to claim 2, wherein the terminal device includes a barcode image interpretation unit to convert the captured barcode image

into the identification code, wherein the connection request signal comprises the identification code.

4. The system according to claim 2, wherein the connection request signal comprises the captured barcode image and the network server includes a barcode image interpretation unit to convert the captured barcode image into the identification code.

5. The system according to claim 1, wherein the network server establishes a communication channel between the terminal device and the networked device through a hole-punching technique, for establishing the P2P connection.

6. The system according to claim 1, wherein the Internet is selected from a group that is formed by at least one of the following: Ethernet, LAN, Broadcast network and VPN.

7. The system according to claim 1, wherein the networked device includes a default security password and the terminal device enters the default security password to log on the networked devices.

8. The system according to claim 7, wherein the captured barcode image comprises the default security password, wherein the image capture unit captures the connection barcode to generate a connection barcode image.

9. The system according to claim 8, wherein the terminal device includes a barcode image interpretation unit to convert the captured barcode image

into the identification code and the default security password, wherein the connection request signal comprises the identification code and the default security password.

10. The system according to claim 8, wherein the connection request signal comprises the captured barcode image, wherein the network server includes a barcode image interpretation unit to convert the connection barcode image into the identification code and the default security password.

11. The system according to claims 1 to 10, wherein the barcode image is a quick response code (QR code).

12. The system according to claims 1 to 10, wherein the barcode image is a one dimensional barcode.

13. A method to identify networked device for establishing a P2P connection, the method comprising the steps of:

(a) connecting a networked device to a network server through the Internet;

(b) registering an identification code of the networked device into the list of networked devices of the server, wherein a connection barcode corresponding to the identification code being attached on the networked device;

(c) generating a connection request signal by a terminal device when the connection barcode is captured to the terminal device and transmitting the connection request signal to the network server by the terminal device through the Internet; and

(d) identifying the networked device in the list of the networked devices of the network server according to the connection request signal so as to establish a P2P connection between the terminal device and the networked device.

14. The system according to claim 13, wherein the step (c) further comprises the sub-steps of: (c1) using an image reading module of the terminal device to interpret the captured barcode image to an identification code; (c2) embed the identification code in the connection request signal.

15. The method according to the claim 13, wherein the step (d) further comprises (d1) embedding the captured connection barcode image in the connection request signal; (d2) transmitting the connection request signal to the network server through the Internet.

16. The method according to the claim 15, wherein the step (d) further comprises the sub-steps: (e1) receiving the connection request signal; (e2) interpreting the captured barcode image to an identification code by an image interpreting unit of the server.

17. The method according to the claim 13, wherein the step (e) comprises the steps of: (f) inputting a security code through the terminal device; (g) determining whether the security password is the same as a default security password in the networked device, if not, then back to step (f), and if so, allow the terminal device to log on the networked device.

18. The method according to the claim 13, wherein the communication channel is established between the networked device and the terminal device by using hole-punching technique, for establishing the P2P connection.

19. The system according to claim 13, wherein the Internet is selected from a group that is formed by at least one of the following: Ethernet, LAN, Broadcast network and VPN.

20. The method according to claims 13 to 19, wherein the barcode image is a quick response code (QR code).

21. The method according to claims 13 to 19, wherein the barcode image is a one dimensional barcode.

ABSTRACT

A system and method to identify a networked device for establishing a P2P connection is disclosed, wherein the system comprises a network server, a plurality of networked devices and terminal devices; and the method comprises: connecting at least one networked device to a network server through the Internet; registering the identification code of the networked device to the list of networked devices of the server and dispose a barcode corresponding to the identification code on the networked device; capturing the barcode of the networked device by an image capture unit of the terminal device to intercept the barcode to produce a connection request signal corresponding to the barcode; and obtaining, by the network server, the networked device from the list of networked devices and establish a P2P connection between the terminal device and the networked device.

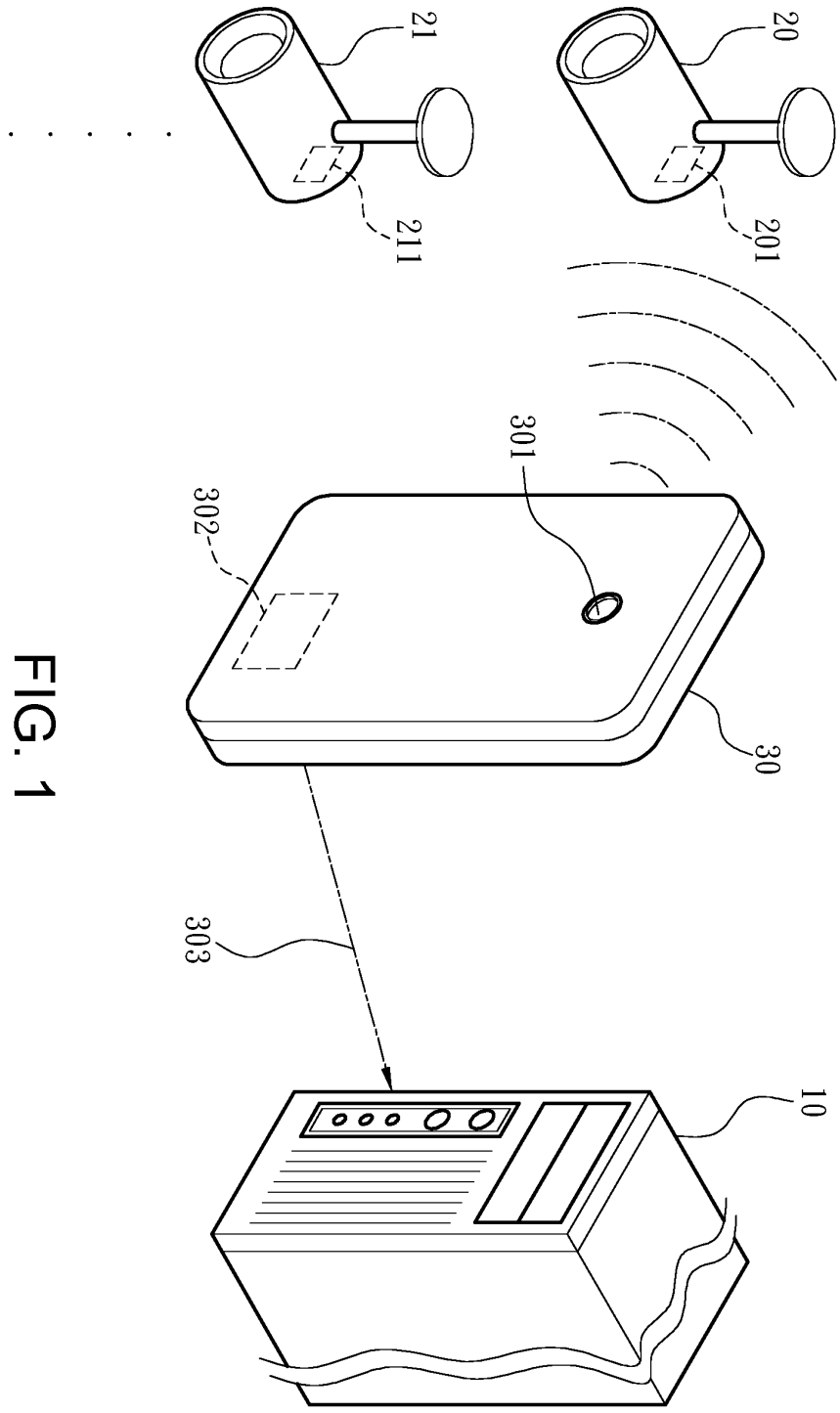


FIG. 1

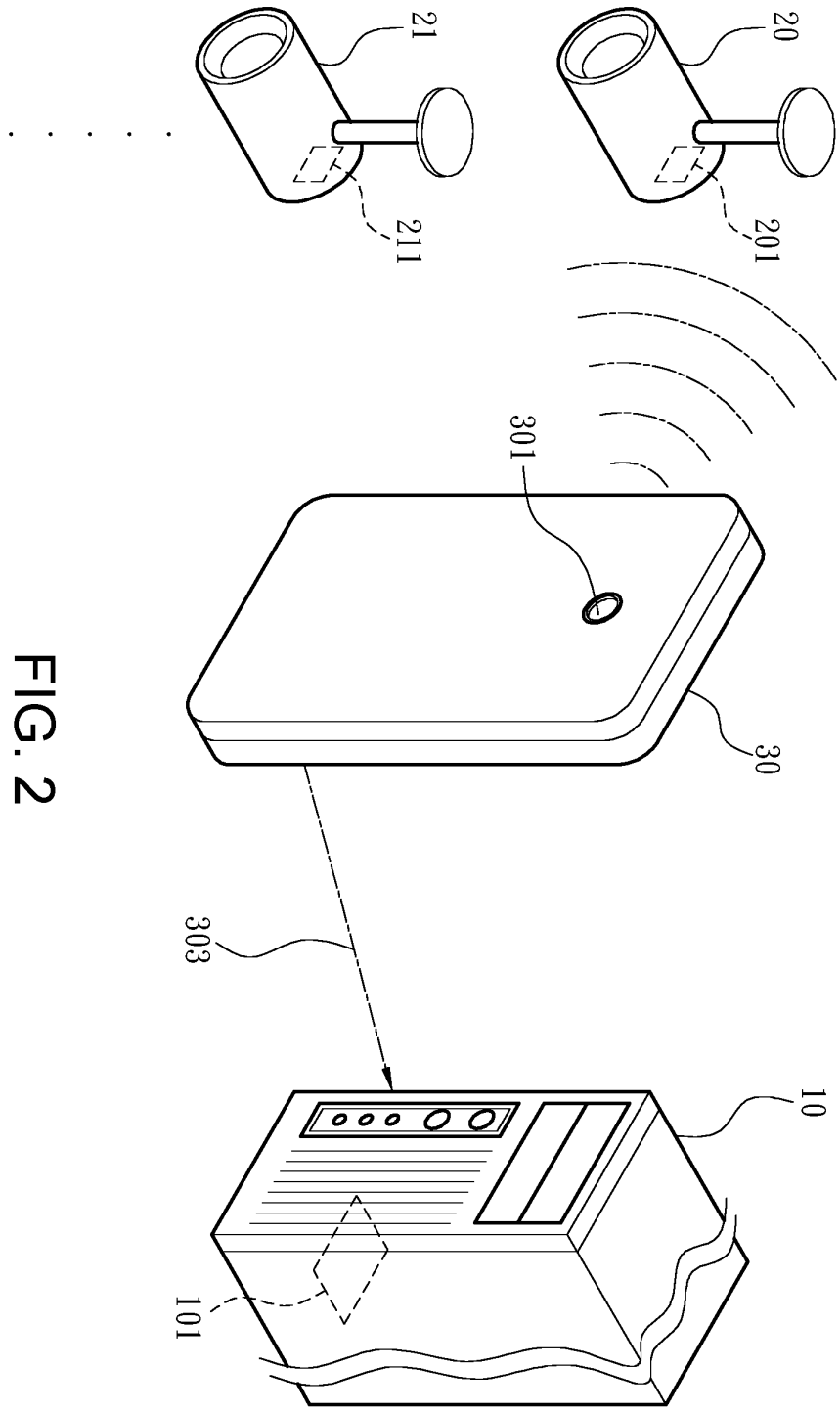


FIG. 2

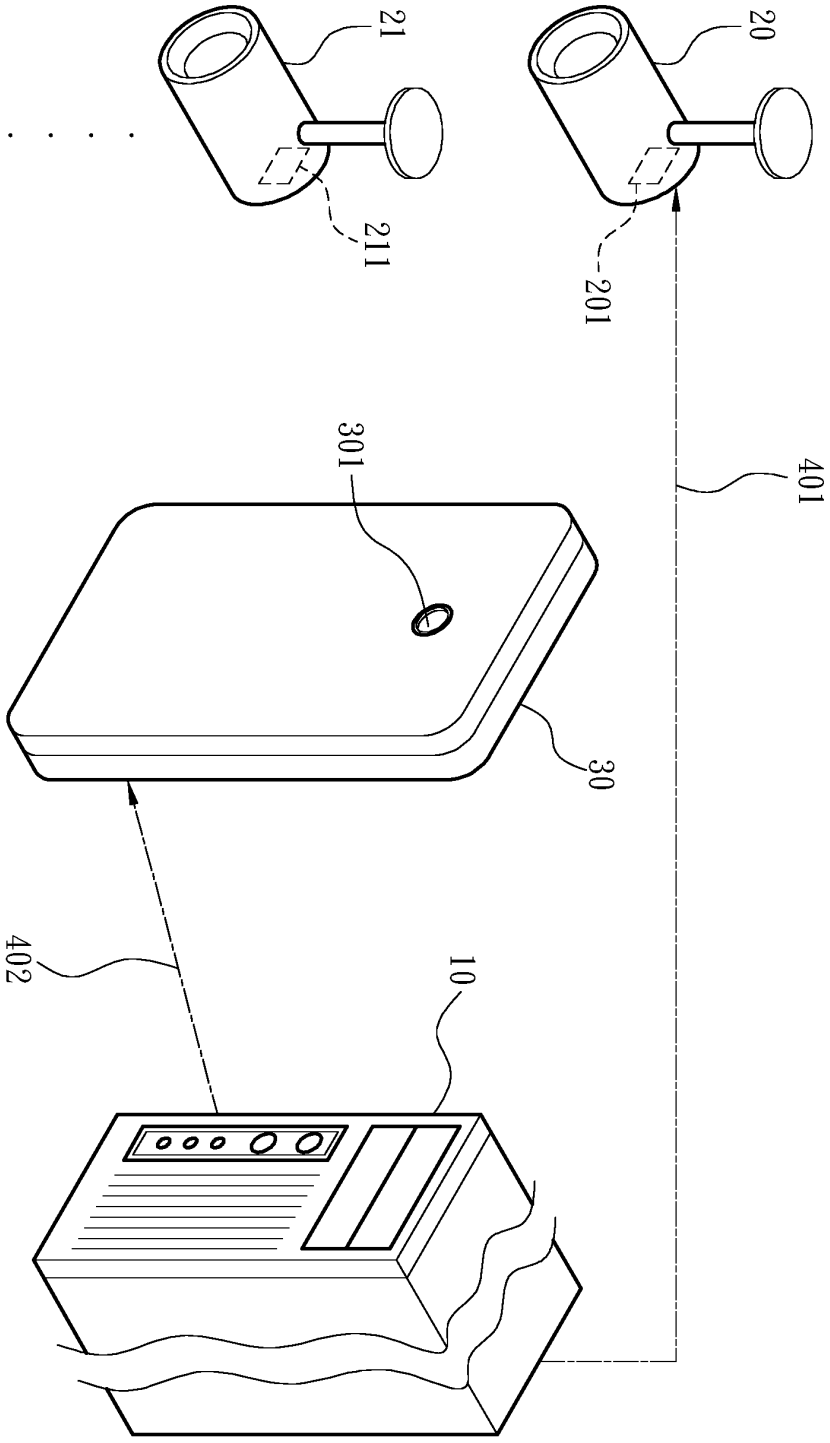


FIG. 3

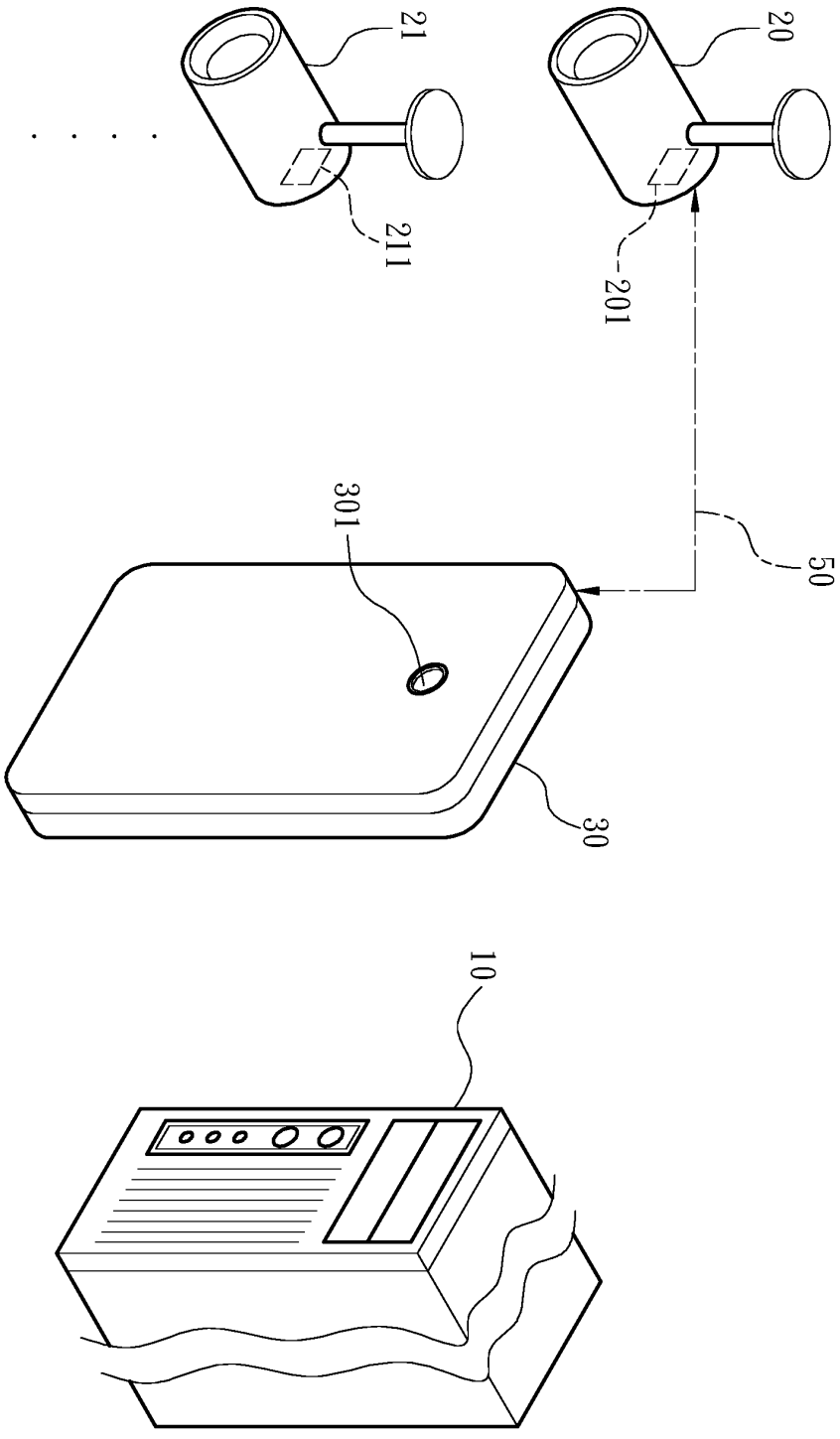


FIG. 4

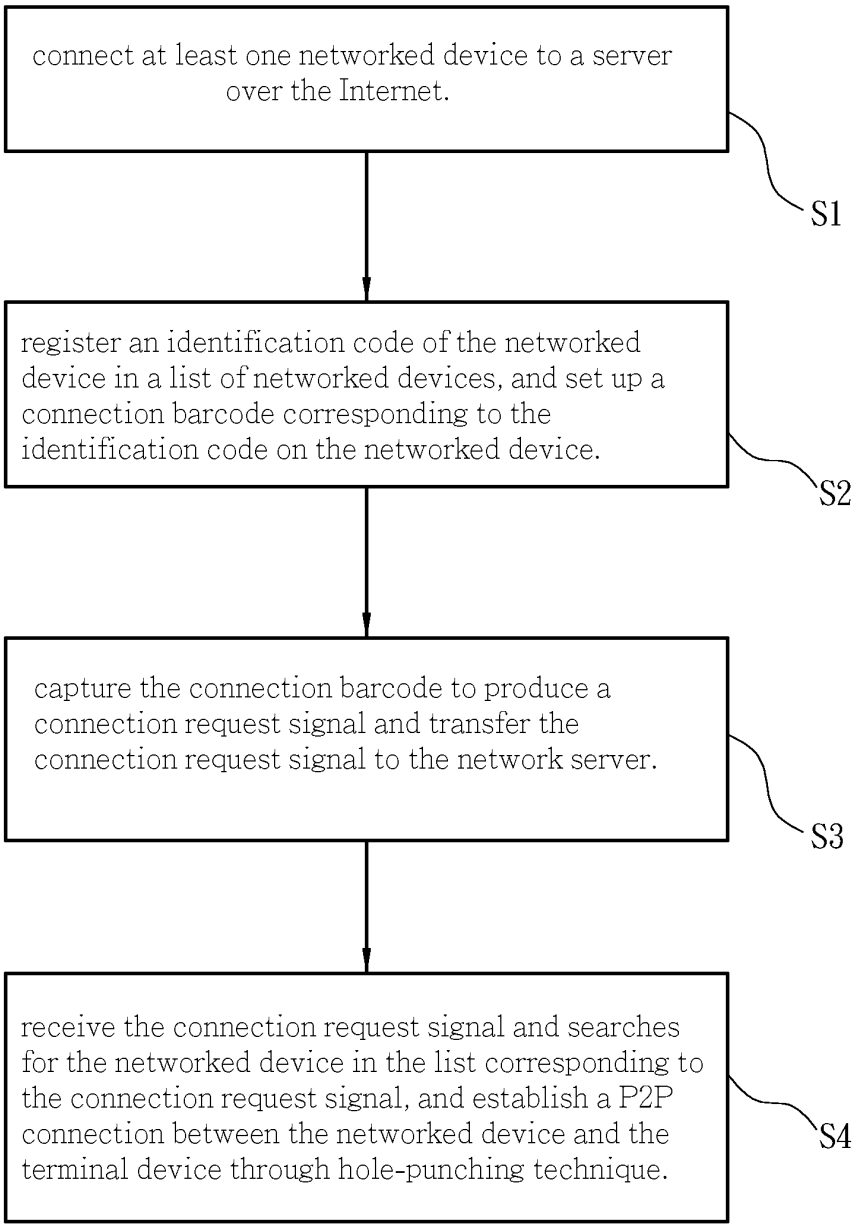

connect at least one networked device to a server over the Internet.
S1
register an identification code of the networked device in a list of networked devices, and set up a connection barcode corresponding to the identification code on the networked device.
S2
capture the connection barcode to produce a connection request signal and transfer the connection request signal to the network server.
S3
receive the connection request signal and searches for the networked device in the list corresponding to the connection request signal, and establish a P2P connection between the networked device and the terminal device through hole-punching technique.
S4

FIG. 5

Smart Control:

- Smart IR Remote controller
- Smart Strip for power saving

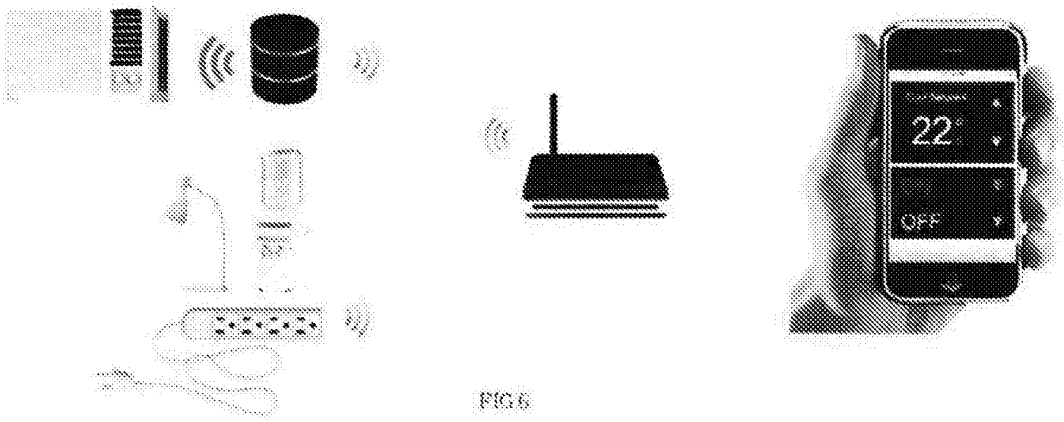


FIG 6

Smart Personal Cloud:

- Personal Cloud for smart phone
- Always connected

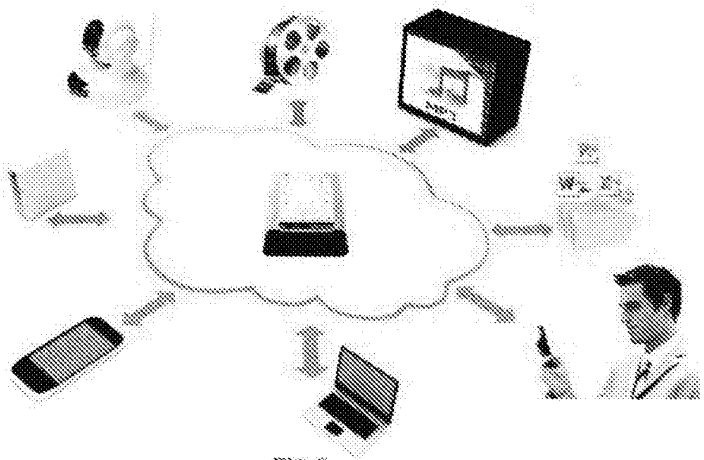


FIG. 7

Electronic Acknowledgement Receipt	
EFS ID:	26175988
Application Number:	61812262
International Application Number:	
Confirmation Number:	9399
Title of Invention:	METHOD OF IDENTIFYING NETWORKING EQUIPMENT FOR ESTABLISHING P2P CONNECTION AND THE SYSTEM USING THE SAME
First Named Inventor/Applicant Name:	Patrick Kuo
Customer Number:	11336
Filer:	Min-Lee Teng
Filer Authorized By:	
Attorney Docket Number:	6121.001.PPA
Receipt Date:	27-JUN-2016
Filing Date:	16-APR-2013
Time Stamp:	03:05:42
Application Type:	Provisional

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	6121_001_PPA_incomg_letter_1.pdf	51472 85567f649788e5ed5f1e755d89c9862b55723e5c	no	1

Warnings:

Information:					
2	Specification	6121_001_PPA_ENGLISH_TRANSLATION_OF_SPEC_1.pdf	1930904 8aa7d111d9f606d9c1e2df5595d876961d1e801c	no	31
Warnings:					
Information:					
			Total Files Size (in bytes):	1982376	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.