

# 對等式（P2P）網絡架構

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 介紹.....	3
II. 管理方面的考慮.....	4
趨勢與影響.....	4
管治與法規.....	4
III. 保安方面的考慮.....	6
P2P 網絡架構的分類.....	6
保安的威脅.....	6
機構與終端用戶的最佳作業實務.....	8
IV. 結論.....	10

## 摘要

在一個對等式（Peer-to-peer, P2P）網絡架構當中，每部電腦都是同時扮演著用戶端與伺服器端的角色。雖然對等式網絡架構在某期間內的執行效率，以及容錯能力都比傳統主從式架構模組多了許多優點，但它同時也帶來了許多額外附加的風險與威脅。用戶與 IT 管理員都必須從惡意程式碼的傳播、合法內容的下載、以及對等式軟件的弱點當中，透析並了解它們的風險所在，以及應該執行保安防禦措施，以保護任何敏感資料的潛在外洩危機與可能的保安風險。在公司內部的網絡使用上，系統管理員必須保證所有對等式的傳輸都能夠確實遵守公司內的保安政策。此外，他們應該有限度地開啟防火牆的埠以供這類型的傳輸所專用。對每個終端用戶或家庭用戶來說，能夠避免那些由對等式網絡架構所散播的病毒之預防措施也是必須的。

## I. 介紹

對等式 (P2P) 架構代替傳統主從式架構網絡模式，是一個非傳統形式的網絡模組。P2P 網絡在每台電腦上都使用了一個分散式的模組，可參照等級相同的點之內容，且以他們自身伺服器的功能強度作為分級標準，來分別扮演客戶端的角色。每個點都同時扮演著一個客戶端與一個伺服器端的角色<sup>1</sup>。換言之，這些點不但可以自發送出要求給其他的點，同時亦能對網絡上其他點的要求作出回應。傳統的主從式架構只能讓客戶端每次送出要求給一個伺服器，然後就只能等待伺服器的回覆。

在主從式架構底下，伺服器的效能將會在客戶端對其提出的要求增加時開始遞減。然而，當點的數目被逐漸增加並放置到網絡上時，P2P 網絡的執行效能卻反而能得到實際上的改善。當它們之間在進行溝通時，這些點也可以將自己分配到臨時的對等式傳輸模組的群組中，以互相合作與共享頻寬，來完成許多即時的工作（例如檔案共享）。每個點都能同時作上傳與下載，且在這類型的運作程序中，新的點隨時都可以在舊的點離開時加入這個群組。用戶也察覺不到這種不斷重組的群組成員架構。

另一個 P2P 網絡架構的特徵就是容忍錯誤功能。當其中一個點離開或者取消連線時，P2P 的應用程式將可以用其他點作為替補來繼續傳輸下去。舉例來說，在一個 BitTorrent 的系統中，任何客戶端在下載某些檔案時，同時也能夠扮演伺服器的角色。當一個客戶端在眾多的點中找到一個沒有回應者時，它就會去搜尋其他的點，來繼續下載舊的點所擁有的部份檔案，並完成所有的下載程序。當主從式架構的伺服器故障時，所有的傳輸與溝通活動就會立即停止。相較於主從式架構，P2P 網絡架構擁有更高的容忍錯誤能力。

---

<sup>1</sup> <http://www.intel.com/technology/magazine/systems/it02012.pdf>

## II. 管理方面的考慮

### 趨勢與影響

最先開始公開源碼的系統，如 1999 年的 Napster，改變了檔案共享的方法。傳統主從式架構的檔案分享與任務分派所使用的協定類似檔案傳送規約 (FTP)，已可由一個新的選擇—P2P 網絡架構來補充。在那時，Napster 是被用來分享大量的音樂檔案。但 Napster 也因為與唱片業界的法律訴訟而在 2001 年中停止運作<sup>2</sup>。

不過，Napster 的停業並沒有就此中止了 P2P 應用程式的增長。已有數個 P2P 系統工具在過去的幾年間陸續出現，如 Gnutella, KaZaA, WinMX 以及 BitTorrent 等軟件。從分析 P2P 網絡在 2007 年的傳輸活動，BitTorrent 仍然是最受歡迎的檔案分享協定，總計共佔了 50%—75% 的 P2P 傳輸量與大約 40% 的網絡傳輸量<sup>3</sup>。

P2P 的技術並不僅是被使用在多媒體檔案的分享上。舉例說，在生物資訊學的研究社群中，P2P 有一個名為「Chinook」<sup>4</sup>的服務，已經被開發用來促進技術分析資料的交流。

這種技術也被使用在其它的領域中，例如以 IP 為基礎的網絡電話—Skype<sup>5</sup>；以及網絡電視如 PPLive<sup>6</sup>。Skype 讓人們以一般電話或影音電話的方式來聊天。當它被推出時，每個 Skype 的用戶端都扮演著其中一個點的角色，為了要以一般電話或影音電話的方式來聊天，而去建立與整理出一份有著可接達節點 (Peer)<sup>7</sup>的表格。PPLive 則是用來分享即時的電視內容，每個點的用戶都能夠經由其他點的用戶分享、下載與重新分配這些內容<sup>8</sup>。

### 管治與法規

在美國，已有一定數量的政客提高了可能因 P2P 網絡技術所帶來全國性的安全威脅之影響力。政府的機密資料很有可能因為公務員在使用 P2P 工具分享軟件的同時，不小心被洩漏給他國政府、恐怖份子，或者是其他組織型的犯罪者；而這也提醒了我們一個方向，即「*new laws and rules should be enacted to protect personal information held by federal*

<sup>2</sup> <http://www.oecd.org/dataoecd/55/57/32927686.pdf>

<sup>3</sup> <http://torrentfreak.com/bittorrent-dominates-internet-traffic-070901/>

<sup>4</sup> <http://smweb.bcgsc.bc.ca/chinook>

<sup>5</sup> <http://www.skype.com/products/explained.html>

<sup>6</sup> <http://www.pplive.com/en/about.html>

<sup>7</sup> <http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf>

<sup>8</sup> <http://eeweb.poly.edu/faculty/yongliu/docs/pplive.pdf>

*agencies and other organisations*」，這表示聯邦機構以及其他相關組織應盡速通過新的法律與規章來保障個人資料。雖然此項提案並沒有對 P2P 網絡架構造成整體的限制，但已經嘗試爭取：「*a balance that protects sensitive government, personal and corporate information and copyright laws*<sup>9</sup>」，即在保護政府敏感資料、個人與公司資訊，及著作權法律等方面爭取平衡。

P2P 網絡架構本身只是一種技術，和檔案內容與知識產權的爭論性問題是沒有任何關係的。然而，香港已經出現了反對非法 P2P 活動的判例。於 2005 年，一名香港居民透過互聯網使用 Bittorrent 軟件來以對等式傳輸分享檔案程式，並且製作出其它能夠下載檔案的載點給別的網絡用戶，而涉及非法上傳並損害相關版權條例的判決<sup>10</sup>。

---

<sup>9</sup> [http://www.news.com/Congress-P2P-networks-harm-national-security/2100-1029\\_3-6198585.html](http://www.news.com/Congress-P2P-networks-harm-national-security/2100-1029_3-6198585.html)

<sup>10</sup> [http://www.customs.gov.hk/eng/new\\_release\\_20070518\\_bt\\_e.html](http://www.customs.gov.hk/eng/new_release_20070518_bt_e.html)

### III. 保安方面的考慮

#### P2P 網絡架構的分類

P2P 網絡架構大致上可以被分為兩類 — 「純對等式網絡」(Pure P2P network) 以及「混合式對等式網絡」(Hybrid P2P network)。在純對等式網絡中，所有參予分享的點都是平等的，且每個點都同時扮演著客戶端與伺服器端的角色。系統並不需要依賴中央伺服器去幫忙控制、協調、以及管理所有點之間的資料交換<sup>11</sup>。Gnutella<sup>12</sup>與 Freenet<sup>13</sup>就是純對等式網絡的兩個例子。

在混合式對等式網絡中，則必須存在一個中央伺服器，來確實做到管理的工作，以促進 P2P 的服務。舉例說，在使用 Napster 軟件時，伺服器就能幫助一個點的用戶去「*search for particular files and initiate a direct transfer between the clients*」<sup>14</sup>，即搜尋受歡迎的檔案，並且創造出與客戶端之間正確的傳輸路徑。真正的檔案透過許多點的用戶被分散在網絡各處時，通常只會有一個目錄檔案被保存在伺服器上。另一個例子就是 BitTorrent (BT)，它擁有一個名為 Tracker 的中央伺服器，幫助協調 BT 點之間的溝通以求完成下載。

這兩種 P2P 網絡的分別在於，混合式對等式網絡利用一個中心伺服器去執行一些行政功能，而純對等式網絡就沒有此種中心伺服器<sup>15</sup>。相較於混合式對等式網絡的結構，純對等式網絡構造較為簡單，且擁有較大的錯誤容忍力。另一方面，混合式對等式網絡消耗的網絡資源較少，且比純對等式網絡有著更高的擴展性。

#### 保安的威脅

P2P 網絡將每個用戶都當作具有相同地位的點來處理。在檔案共享工具，如 BT 中每個點的用戶都是被分散開來提供服務，上傳檔案給其他的點來完成下載。這是一個開放式的管道，從外來電腦上擷取資料，並放置儲存在個別用戶電腦上的。

它的潛在保安弱點包括：

---

<sup>11</sup> <http://www.intel.com/technology/magazine/systems/it02012.pdf>

<sup>12</sup> <http://www.gnutella.com/>

<sup>13</sup> <http://freenetproject.org/>

<sup>14</sup> <http://opennap.sourceforge.net/>

<sup>15</sup> <http://www.iu.hio.no/~frodes/rm/trond.pdf>

### 1. 傳輸控制規約 (TCP) 埠的問題與爭議：

通常，P2P 相關的應用程式為了得到更順暢的運作，都會要求防火牆開放一定數量的埠。舉例說，BitTorrent 會要求開放編號 6881-6889 的 TCP 埠（在版本 3.2 之前）。自版本 3.2 開始甚至在稍新的版本中，其所要求使用的 TCP 埠已經進一步的擴展到編號 6881-6999<sup>16</sup>。每個在防火牆中開放的埠，都可能等同於是給攻擊者一條潛在的路徑，並用以對網絡進行攻擊。所以，為了允許 P2P 網絡運作得更流暢而開放大量的埠，並不是一個正確的方法。

### 2. 像病毒的惡意程式碼傳播：

當利用 P2P 網絡架構來幫助檔案的傳輸與分享時，惡意程式碼同樣的也能夠經由這條管道來散佈給其他所有點的用戶。舉例說，在 2000 年時，就發現了一隻名為 VBS.Gnutella 的蠕蟲程式，它可以在 Gnutella 檔案共享網絡中對自身的程式加以製作與共享<sup>17</sup>。

特洛伊木馬也同時在 P2P 網絡上被發現，其中一個例子就是 W32/Inject-H。它控制了一個 IRC 的後門，且可利用 P2P 網絡來自我散佈。特洛伊木馬會在用戶的視窗電腦上開啟後門，讓遠端遙控的入侵者能夠接達與控制這部電腦<sup>18</sup>。理論上，儲存在受到感染的電腦內的敏感和個人的資料，是很有可能透過 P2P 網絡而被複製存放到其它電腦上。

### 3. 下載所帶來的風險：

當透過使用 P2P 軟件去下載一個檔案時，我們不可能會知道這個檔案的創建者，以及這檔案的可信性。此外，當病毒或者惡意程式碼與檔案相結合時，把這可能含有非法內容的檔案下載到公司電腦的人，就有可能使自己處於犯法和/或民事訴訟的危機。

另外，當透過使用 P2P 軟件去下載一個檔案時，我們不可能會知道哪個點在哪個時間會連接，以及這個點究竟是否可信等。不可信的檔案來源往往便會引起並造成其它保安的威脅。

### 4. P2P 軟件的弱點：

如同其它的軟件，P2P 軟件一樣有保安漏洞。當某個點同時作為用戶端與伺服器

---

<sup>16</sup> <http://www.dessent.net/btfaq/#ports>

<sup>17</sup> [http://www.symantec.com/security\\_response/writeup.jsp?docid=2000-121813-5230-99](http://www.symantec.com/security_response/writeup.jsp?docid=2000-121813-5230-99)

<sup>18</sup> <http://www.sophos.com/security/analyses/w32injecth.html>

端時，它就會時常收到來自其他點的要求，若此伺服器的 P2P 軟件又有很多保安漏洞，就很有可能把相關的保安漏洞置於用戶的電腦內。入侵者便可以利用這一點來散佈病毒、入侵電腦，甚至是發動拒絕服務的攻擊等。在 2003 年，有一個關於 P2P 軟件 Kazaa Media Desktop 的程式錯誤就被報導與記述出來；它會造成拒絕服務的攻擊，或者是允許遠端遙控的攻擊者利用惡意程式碼進行破壞<sup>19</sup>。

除了一般的保安風險，如果在公司中的網絡使用 P2P 軟件，不但會多出一些原先不必要的大量網絡傳輸，還會霸佔所有的頻寬，進而造成其它生意上合法可用的程序因而停止。公司員工在商業環境中，使用 P2P 軟件進行下載與上傳所費的效率與時間，都將會影響到員工的生產力以及公司的重要營運等。

### 機構與終端用戶的最佳作業實務

對這些保安威脅而言，執行適當的保安及預防措施，可保護任何敏感資料與保安破壞的潛在漏洞。以下，是當考慮到讓機構與終端用戶使用 P2P 技術時最佳的作業實務。

### 機構的網絡

為了減輕暴露 TCP 埠所帶來的風險，機構應該要反覆檢視他們在日常營運上對 P2P 技術的需求。若 P2P 網絡架構是不需要的，在保安的策略上，就要將網絡上已經確認的那些相關範圍的埠全部阻擋起來。而在相關規則的提示上，公司也應該要告訴所有用戶，在公司內的電腦上不准下載與安裝任何 P2P 的軟件。若 P2P 網絡架構是確定必須使用在公司的營運上，當使用 P2P 軟件時，就應該以逐一檢查與認可的標準來實行。所有用戶都應該要再接受教育，使他們知道關於如何適當使用 P2P 軟件與檔案共享的危險性。再者，P2P 網絡架構根本就不應當被推薦用來分享敏感的，或私人的資訊；因為在 P2P 上的傳輸連結經常都是沒有加密的，所以任何內容都有外洩到他人手上的危險。

此外，所有機構的網絡傳輸活動都應該要以 IDS / IPS（入侵偵測系統 / 入侵防禦系統）來進行監控。只要發現任何未經授權的 P2P 網絡傳輸（例如：當發現網絡的執行突然產生中斷時，對防火牆的設施 / IDS 的歷史紀錄進行檢討），都應該要再進行研究與封鎖。一個清晰的防火牆政策應該能夠定義出欲阻擋的 P2P 應用程式所用相關的埠（如前所描述 Bit-Torrent 使用的那些埠），以便在進出內部網絡時都能夠即時阻絕 P2P 網絡的傳輸活動。

此外，用戶應針對 P2P 技術帶來的攻擊，適當地防禦及保護自己。防毒程式要更新到最新的病毒識別碼、定期為個人電腦作出修補程式管理、及使用適當的個人防火牆設定，

---

<sup>19</sup> <http://ca.com/tw/securityadvisor/vulninfo/Vuln.aspx?ID=7098>

對一個機構的網絡安全是必須的。

### 終端用戶/家庭網絡

相同地，在終端用戶或家庭網絡當中，保安上的控制，如個人防火牆、擁有最新病毒識別碼的防毒程式、最新保安修補程式以及系統管理員所做出的權利限制等，都是必須實行的，以避免潛在的保安破壞與系統誤用。假如不需要分享檔案的話，便應阻擋有關範圍內所有的埠。

這些關於桌上電腦的保安建議對家庭用戶來說也同樣適用。年輕人喜歡透過網絡來分享檔案，但他們也必須接受教育，了解從不可信任或是可疑的來源下載檔案的危險性。假若必須下載 P2P 的檔案，就需要在下載完成後，適當地關閉 P2P 用戶端所用的應用程式。此外，應該永遠不要下載含有兒童色情以及其它非法的內容，包含盜版軟件。

## IV. 結論

當 P2P 網絡為了提升下載的效率及分享檔案和資料而開放了新的渠道時，用戶必須充分意識與明瞭這個技術所帶來的保安威脅。為了避免洩露敏感或個人資料的潛在危機以及其它保安損害，保安措施與適當的防禦都應該要實施。在規劃開放防火牆的埠給員工利用 P2P 軟件來傳輸之前，系統管理員應該保證他們的每一個要求都有遵守公司整體的保安政策；縱使要開放埠給 P2P 網絡使用，也應只是開放必須使用的和有限度的埠。對終端用戶及家庭用戶來說，必須注意避免任何可能透過 P2P 網絡散佈的病毒。