

## Skype 相關知識入門

Skype 由於採用 P2P 架構 (Peer to Peer)，通話品質出奇的好，讓人大感不可思議，擺脫一般人「網路電話品質很糟」的印象。加上通話免費，也因此短時間內迅速在全球吸引了 5 億多的用戶。兩台安裝 Skype 的電腦，就可以透過接到電腦的耳機和麥克風交談，只要是電腦之間對打就是免費，因此很多人用於取代國際電話。如果打到一般的電話號碼，還是需要付費，不過卻也相對便宜。

採用 P2P 架構的優點在於，透過 Skype 交談時電腦是直接連線，不需經過任何伺服器中介處理通話資料。因此 Skype 和傳統電信業比起來營運成本大幅降低，不似傳統電信業者必須採購與維護昂貴交換設備。

## Skype 主要功能



### 超清晰音質

Skype 的語音通話效果比您所見到的所有同類產品都要好，甚至比傳統的電話語音有更好的適應性。用專業術語來說，傳統的電話您只能聽到介於 300Hz 到 3000Hz 頻率的語音。Skype 可以聽到所有頻率的語音，從最低沈的到最尖銳的。



### 全球都能通用的免費電話

Skype 提供了全球搜索目錄，您可以根據不同的查詢條件查詢您認識的、或者不認識的朋友，並且，可以馬上開始進行暢通無阻的語音通話，讓您的溝通更無障礙，效率更高。



### 保密電話，通話加密

Skype 在語音發送之前進行加密，在接收到的時候進行解密，不會在中途被竊聽。採用的加密演算法與美國政府用來保護機密資料安全的演算法相同。使用了 256 位加密，這種加密方法共有  $1.1 \times 10^{77}$  種可能的 Key，可以動態的將每個呼叫和即時消息加密。Skype 採用 1536 和 2048 位 RSA 來生成對稱 AES 密鑰。用戶的公共密鑰 (public keys) 在用戶登錄的時候在 Skype 伺服器進行驗證。



### 穿透防火牆

Skype 運用 Skype 通訊軟體的輔助，可以與所有防火牆、NAT 和路由器一起使用，且無需進行任何配置！在您使用其他同類產品不能正常連接的時候，Skype 通常可

以，例如語音通話、文件傳輸等。



## 撥打固定電話

Skype 可以使用 Skype Out 實現 PC to Phone 的功能，價格低廉而且音效很好，屬於 VOIP。如果你有國際信用卡可以到 Skype 網站[購買 SkypeOut 點數](#)，打國際長途，價格約每分鐘 0.17 元（打到不同國家資費略有不同，[詳細資費點此查看](#)）。

## Skype 主要功能解說

本文主要從技術角度簡要闡述 Skype 為什麼優於傳統的 VoIP、IM 軟體，包括 P2P 技術、穿透防火牆、安全加密、簡易的操作與強大的功能、節省網路資源、跨平臺幾個方面。

### 一、採用領先的 P2P 的技術

目前比較流行的 IM 軟體基本都採用集中式的 Client-Server 模式，即需要通過大量的伺服器資源進行資訊集中存儲、通訊協調等。P2P 的技術相當於將每個用戶端都作爲了伺服器資源，從而在整個網路中發揮作用。

非集中式 P2P 網路在一些方面優於傳統的 Client-Server 模式的網路。這種網路可以無限的擴展，並且不會因爲擴展而導致搜索時間的延長和費用的增加。它利用終端用戶機器的處理能力和網路帶寬，非集中式網路的處理能力本身與此成正向比例，即每增加一個節點，P2P 網路的處理能力和帶寬都相應增加。所以，這種利用節點資源的 P2P 網路技術事實上可以完全取消原先集中式網路所需的費用。

P2P 技術在穿透防火牆和 NAT（網路位址轉換）方面也具有優勢。傳統的集中式網路也可以穿透防火牆和 NAT，但是通常會因此增加非常昂貴的費用，用戶越多費用會成比例的增加。所以，提供這樣服務的服務商通常只能給每個用戶提供非常少的伺服器資源，大大降低了語音通話的質量。Skype 實現了將網路資源分散（即不是利用集中式

的伺服器資源，而是利用各個節點的網路資源)。使得語音呼叫的接通率、語音質量在很大程度上甚至超過傳統的電話網絡。

從搜索方面來講，Skype 所採用的技術可稱為第三代 P2P 網路技術。P2P 技術最早被一些文件共用應用廣泛使用，例如非常有名的 Napster 和 KaZaA，最近比較流行的有 BT 等，國內比較有名的 P2P 軟體有 POCO、OP 等。在此類應用中，用戶可以共用、並搜索下載文件。這些文件共用使用的 P2P 網路技術也可以進行資源分散 (decentralizing)，但是文件共用 P2P 技術所使用的網路本質上是分段的，即當您進行搜索的時候，並不能搜索到網路中的所有節點。為了實現高質量低成本的語音呼叫，必須有第三代 P2P 網路技術來實現。Skype 採用了全球搜索目錄 (GI)，GI 代表了另一種意義上的可擴展網路技術。全球搜索目錄使用多層的網路結構，這種結構利用超節點 (Supernodes) 來實現網路中的每個節點可以獲取所有其他可利用節點的資源，並將這些節點資源動態組合，來參與流量分配、路徑選擇、處理需要較大帶寬的任務等，並保證最小的延時。

對資料傳輸採用智慧路由，保證了語音質量。由於可以利用所有的節點資源，Skype 可以為每個加密的呼叫智慧地搜索最好傳輸途徑。甚至可以並行的打開多個傳輸路徑，動態的及時選擇最佳途徑。這對減少延遲和增強語音質量有非常明顯的效果。

## 二、穿透防火牆

大多數的 Voice-over-IP 應用程式不能穿透防火牆和 NAT (網路位址轉換)。幾乎所有寬帶用戶都處於防火牆和 NAT 之後，所以他們不能用 VoIP 應用程式。Skype 不是一個典型的 VoIP 程式，它運用的是 P2P 技術，幾乎可以在所有的防火牆或者 NAT 之後工作。

大多數此類軟體的進入埠號都是指定的，Skype 沒有指定進入的埠號，而是在安裝程式的時候隨機選擇一個進入埠，如此能增強穿透網路位址轉換（NAT），因為如果有若干個位於 NAT 之後的用戶採用相同的埠的話，則 NAT 會使得語音質量降低。

### 三、安全加密

Skype 採用了端對端的加密方式，保證資訊的安全性。使用了 AES（高級加密標準）加密方法，也稱為 Rijndael，美國政府用同樣的加密方法來保護機密資訊。Skype 使用了 256 位加密，這種加密方法共有  $1.1 \times 10^{77}$  種可能的密鑰，可以動態的將每個呼叫和即時消息加密。Skype 採用 1536 和 2048 位 RSA 來生成對稱 AES 密鑰。用戶的公共密鑰（public keys）在用戶登錄的時候在 Skype 伺服器進行驗證。Skype 在資訊（語音、即時消息、文件）發送之前進行加密，在接收到的時候進行解密，即使在資料傳輸過程中需要經過其他節點進行中轉，也完全沒有可能在中途被竊聽。

Skype 採用了數位元簽名的方式，保證存儲在 P2P 網路中的用戶資料不被篡改。由於 Skype 使用的是 P2P 的技術，用戶資料主要存儲在 P2P 網路中，在用戶進行搜索等操作的時候從公共網路中獲取。如此必須保證存儲在公共網路中的資料是可靠的和沒有被篡改的。Skype 對公共目錄中存儲的和用戶相關的資料都採用了數位簽名，保證了資料無法被篡改。

### 四、使用簡易、功能強大

Skype 具有迄今為止最優質的語音。現在很多 VoIP 和聊天工具都無法和 Skype 相媲美。Skype 與最優秀的聲學科學家聯手創造的獨家擁有版權的軟體，可以傳遞甚至高於固定電話質量的語音。用專業術語來說，傳統的電話您只能聽到介於 300Hz 到 3000Hz 頻率的語音。Skype 可以聽到所有頻率的語音，從最低沈的到最尖銳的。

很高的呼叫成功率。沒有其他任何一個互聯網技術系統可以有和 **Skype** 一樣高的呼叫連通率。

使用簡單。現在 **VoIP** 應用程式配置很困難，不熟悉網路和計算技術的用戶幾乎無法使用。**Skype** 無論在軟體還是硬體方面，用戶都無需做任何收工的設置，通常只要註冊一個賬戶就可以立即登陸，開始語音通話了。

絕對安全的通話方式。如上所述，所有的通訊都是以端對端的模式進行加密的，所以是完全安全的。

多方語音通話。**Skype** 在同類軟體中首先提供了免費的多方語音通話，採用混音的方式，操作簡便、音質良好，且盡可能的節省網路和機器資源。

## 五、最大可能的節省資源

**Skype** 對網路帶寬的要求比同類產品低，**Skype** 在 33.6Kbps 或者以上的 Modem 來撥號上網的情況下也可以使用語音通話。**Skype** 可以根據雙方的連接情況自動選則最佳的編碼方式。語音通話的時候平均佔用帶寬大約是 3-16KB/S，實際佔用帶寬會根據對方的帶寬情況、網路狀況、以及 CPU 性能等有所不同。當空閒的時候大約只需要 0-0.5 k/s 的帶寬，主要是用來更新好友在線資訊。具體的帶寬情況可能會受許多因素的影響。用 **Skype** 進行文件傳輸的時候，如果雙方不能直接連接，則會通過其他用戶的資源來進行中轉。普通的同類軟體在無法直連的時候一般是通過伺服器中轉，**Skype** 不利用伺服器的資源，而是通過網路中的其他用戶機器來進行中轉。爲了不過多佔用做中轉的用戶的資源，將速度限制在了 500K/S 以下。

## 六、跨平臺

目前大多數 IM 軟體都只能在 **Windows** 平臺上運行。即使有單獨開發的針對其他平臺的版本，也往往是功能非常弱，例如只限于文本資訊交換。**Skype** 目前有完全適用

於 Windows 作業系統、Pocket PC、和 Mac OS 和 Linux 作業系統的版本，語音通話、文件交換等資料傳輸都可跨平臺進行。Skype 所採用的底層技術保證了其可以很容易的移植到不同的終端設備上，更加適應終端設備和通訊技術的發展。

GodEngine Technology Inc