VoIP 網路電話發展及安全簡介

提要

一、VoIP 的技術原理，是以 IP 網路取代傳統語音網路，來傳送語音。因此，IP 網路可能出現的安全問題，也會威脅到 VoIP，像是病毒、惡意程式攻擊、被他人竊聽等問題。

二、美國國防部於戰術通訊建置安全的 VoIP 網路電話系統，係為在 IP 網路上將所有通訊流量(數據、語音及視訊等)集中有效運用，為符合資訊確保政策之要求，訂定網路電話安全技術設置準則，作為各單位建置準則。

三、未來國軍規劃運用 VoIP 時，應以「資訊安全」為首要考量，本文提出(一)系統整體規劃，策頒安全規範；(二)隔離語音及數據傳輸的網路；(三)保護 VoIP 設備的重要位址及埠；(四)語音封包及控制訊號的加密；(五)結合無線行動、有線網路安全防護等安全部署建議，以作為國軍參考。

前言

VoIP(Voice over Internet Protocol)網路電話係指透過網際網路(Internet)所提供之語音服務，由於網際網路具有全球相連之特性，以及易於整合語音、數據及視訊進行處理與傳輸之優勢，故較傳統公眾電話服務更符合整合性(Convergence)、全球化(Globalization)、即時性(Immediacy)及移動性(Mobility)之通訊市場主流趨勢。

根據 2005 年通訊雜誌[1]引述，Gartner於 2004 年 10 月以「當企業要採取VoIP服務之前會考慮什麼？」為前提，對北美及西歐大型企業所做的一項調查發現，安全問題是僅次於價格下跌，其受重視程度遠超過通話品質及應用服務之要求。

企業在運用 VoIP 網路電話時，如何兼顧安全與成本，以共創雙贏局面，成為重要議題。以安全為首重之國軍網路環境，對於建置 VoIP 網路電話系統更須審慎規劃，應由安全政策訂定、申請審核管制、安全稽核至定期檢討，以確保國軍網路安全。

本文分別從 VoIP 網路電話技術與發展、安全威脅與弱點及安全需求範圍與實現等，探討 VoIP 網路電話安全，並以美國國防部(Department of Defense,DoD)為例，簡介其網路電話安全技術設置準則，最後提出國軍安全部署建議，作為未來國軍運用參考。

---

[1] 北電(Nortel)，「打造滴水不漏的企業 VoIP 安全環境」，通訊雜誌，第 126 期，2005 年 3 月。

網路電話技術與發展

以點對點(Peer To Peer, P2P)為技術的知名網路電話 Skype，在與國內入口網站 PChome 合作下，進軍網路電話市場，共同提供即時通訊語音服務給國內用戶，其免費、簡單安裝使用的特性，在短時間內獲得廣大用戶下載採用，開啟國內 VoIP 網路電話市場，而電信總局於 2006 年通過開放網路電話號碼 070 之政策法令，使公眾電話網路(Public Switched Telephone Network,PSTN)與網路電話可雙向互通，更掀起一場語音服務市場大戰。以下就其技術與發展作一簡介：

一、VoIP 網路電話

VoIP 網路電話是將語音訊號轉換成數據資料封包後，在 IP 網路(IP Network)傳送的語音服務，意即透過開放性的網際網路，傳送語音的電信應用服務。利用網際網路不僅做到即時提供語音服務，更可連接至世界各地，讓使用者可以不需再透過傳統的 PSTN 進行遠距離電話交談。

二、VoIP 組成元件

(一)IP 網路

VoIP 是以 IP 網路取代傳統線路交換網路來傳送語音，IP 網路為 VoIP 基礎元件。

(二)呼叫處理器/控制器(Call processor/controllers)

屬系統軟體型式，如軟體式交換器、呼叫管理員或閘道管理員，其功能包含啟動及監控呼叫訊號、維護撥號作業、執行電話號碼轉換及控制每通連線之頻寬使用。

(三)媒體/訊號閘道器(Media/signaling gateways)

VoIP 閘道器的功能在於呼叫初始、偵測、語音類比/數位轉換及語音封包產生等，包含媒體閘道器、訊號閘道器及媒體閘道控制器等三種閘道器型態。

(四)電話用戶終端(Subscriber terminals)

IP 網路電話的終端用戶設備，分為硬體及軟體設備，前者有網路電話閘道器(GW)、網路電話盒(Analog Telephone Adapter,ATA)、網路電話機(IP phone/Video phone)及有線/無線電話(Wi-Fi phone)等，後者有軟體電話(Soft phone)。

三、網路電話與傳統電話比較

以下表列 VoIP 網路電話與傳統電話之差異，如表一。

表一 傳統電話與網路電話比較

	傳統電話	網路電話
形式	利用線路交換(Circuit switch)技術將兩點通話路徑建立，透過編碼方式，撥不同號碼即可建立不同通話路徑	利用網路封包交換(Packet switching)網路技術將語音壓縮成封包，透過TCP/IP 傳輸,使得語音與數據均可在同一線路上傳送
使用線路	佔用專線直到通完話	不佔用專線
品質	保證服務品質(QoS)	沒有保證服務品質(QoS)
延遲	低	不一定
頻寬	雙向固定 64K	不一定
成本	視距離及通話時間計算	低
傳輸	語音	數據、語音、視訊等多媒體資料

(資料來源：本研究整理)

四、VoIP 標準通訊協定

語音傳送特性和數據資料不同，前者要求語音品質和即時性，後者則要求正確性。然 TCP/IP 網路特性是重視正確性，忽略即時性，倘若要達到 VoIP，必須提出一套標準方法和協定，來提高語音傳送的品質和即時性。

VoIP 標準通訊協定，包含 H.323、MGCP(Media Gateway Control Protocol)及 SIP(Session Initiation Protocol)等，相關比較如表二。

表二 VoIP 標準通訊協定比較

通訊協定	H.323	SIP	MGCP
訂定單位	ITU-T	IETF	IETF
訂定時間	1996 年	1999 年	1999 年
複雜性	高	高	適中
定義範圍	完全	有限	部分
擴充性	好	好	未定
與 PSTN 的作業互通性	是	稍微	是
SS7 相容性	好	差	好
成本	適中	適中	適中
訊息大小	小	大	適中
與路由器的分割方式	不相似	相似	不相似
運用彈性度	低	高	低
支援多媒體	好	差	差

註：SS7 : Signaling System 7，係取代早期Plain Old Telephone Service (POTS)所用的信號系統，可傳送多樣的信號，以提供更多的服務。

(資料來源：本研究整理)

網路電話安全威脅與弱點

VoIP 網路系統所需安全與一個封閉式的線路交換網路是截然不同的，其所

需安全包括語音封包安全及 IP 網路安全，前者著重於語音應用安全，後者則著重於網路系統安全，以下就網路電話之安全威脅與弱點作一說明：

一、安全威脅

為使 VoIP 用戶確實掌握可能存在的安全威脅，2005 年百來家全球知名 VoIP 製造廠商成立 VoIP 安全聯盟(Voice over IP Security Alliance,VoIPSA)，並提出 VoIP 安全威脅分類書(VoIP Security Threat Taxonomy)，劃分社工威脅(Social Threats)、竊聽(Eavesdropping)、攔截與修改(Interception and Modification)、系統服務濫用(Services Abuse)、網際網路服務阻斷(Intentional Interruption of Service)及其他服務阻斷等六大類安全威脅。

該報告將具備性騷擾、勒索語音內容及垃圾語音(Spam over Internet Telephony,SPIT)等歸納在社工威脅類別；竊聽類別包括通話模式追蹤與封包流量擷取等；至於當前眾所皆知的通話劫持、身分冒用，抑或採用通話轉址技術的 Pharming 等安全問題，歸類於攔截與修改類別；所謂網際網路服務阻斷，則泛指不同目標或採用不同手法的各種 DoS 或 DDoS(Distributed DoS)攻擊；至於其他類別，則專指電力或系統耗盡的 DoS 攻擊。

二、安全弱點

以下介紹現有常見的 VoIP 安全弱點：

(一)Sniffing

竊取呼叫(Stealing call)，意即偽裝成合法使用者行使呼叫命令或透過對用戶 ADSL、纜線網路進行封包攔截，甚至直接入侵語音閘道的方式進行服務竊取，如盜打電話的話費詐欺(Toll Fraud)。

(二)阻斷服務(DoS)攻擊

以下表列 VoIP 網路電話之阻斷服務攻擊種類，如表三。

表三 DoS 攻擊種類表

攻擊名稱	說　　明
ICMP flood	湧入高傳輸率的 ICMP 封包
Teardrop	未經適當處理之重疊的 IP fragment
Land	封包之來源與目的 IP 位址相同
Ping to Death	湧入高傳輸率的 Ping 封包
IP spoof SYN flood	高傳輸率的 TCP SYN 同步封包

註：ICMP : Internet Control Message Protocol 網路控制訊息協定

(資料來源：摘譯於美國國防部[3])

(三)呼叫重新導向(Traffic Flow Redirection)

針對語音流量，有心人士將原本屬於某位接收者的呼叫，被重新導向至其它人。

(四)竊聽

VoIP 語音資訊的通訊協定是開放的，即使是一小段的媒體流都可以被重放出來而不需要前後資訊的關聯。

(五)語音信箱炸彈(V-bombing)

攻擊手法類似垃圾郵件以量取勝的攻擊方式，以單一的 VoIP 語音信箱為攻擊目標，同時間以暴增的巨量語音郵件來癱瘓語音留言服務，亦稱為垃圾語音(SPIT)。

(六)網址嫁接(Pharming)

使 VoIP 用戶不知情狀況下，被莫明其妙地轉接到不明的 IP 位址，不僅因而通話費用大漲，甚至有可能被駭客胡亂地以電話下單或購買股票。

(七)殭屍網路(Zombie)

透過後門、木馬程式的入侵與植入，完全取得用戶電腦的主控權，並藉其 VoIP 電話簿清單濫打網路電話，如此一傳十、十傳百，駭客便可輕鬆建立龐大 SPIT Zombie 網路。

網路電話安全需求範圍及實現

2004 年Bebbie G. and Sophia S.[2] 深入剖析VoIP安全需求範圍，以瞭解如何實現VoIP安全目標，以下作一說明：

一、安全需求範圍

VoIP 安全需求範圍分為設定(Configuration)、數據流(Data Streams) 、呼叫控制(Call Control)及語音流(Voice Streams)等四項，分述如下：

(一)設定：VoIP 設備啟動時，藉由設定伺服器來執行設定動作。

(二)數據流：VoIP 設備啟動後，開始有數據流量，數據流是獨立於呼叫控制及語音流。

(三)呼叫控制：當設備偵測到拿起電話機聽筒(off-hook)訊號或來電訊息時，以呼叫管理伺服器啟動呼叫控制處理。

(四)語音流：一旦呼叫完成，兩個用戶端設備間即可傳送語音流。

二、安全實現

[2] Debbie Greenstreet, Sophia Scoggins (2004) “Building Residential VoIP Gateways: A Tutorial Part Four : VoIP Security Implementation”, VoIP Business Unit, Texas Instrument Incorporated.

鑑於 VoIP 網路電話系統可直接連結至內部網路及外部網路，使得 VoIP 網路電話更易在竊聽、盜撥及阻斷服務上受到攻擊，對安全的需求也有著更高的標準，因此，美國商務部國家標準技術局(National Institute of Standards and Technology , NIST)於 2005 年訂定 VoIP 安全標準規範--「VoIP 系統安全考量(NIST SP 800-58)」，說明 VoIP 標準通訊協定之安全標準、安全挑戰及對於安全弱點的潛在對策。然而，如何實現網路電話安全，以下作一說明：

(一)設定安全

用戶端設備須以安全的 ID 密碼方能進入網路設定伺服器，一旦密碼正確後，設定伺服器將回應乙把認證金鑰，用戶端設備藉此金鑰進行認證程序，並在用戶端設備閘道完成認證後，設定伺服器提供乙把加密金鑰，並使用這把金鑰將用戶端設備與設定伺服器之間的所有訊息加以加密。

伺服器應用系統之存取控制可使用加密通訊協定，如 SSL(Session Security Layer)、TLS(Transport Layer Security)及 SHTTP(Secure Hyper Tex Transfer Protocol)，其使用加密演算法為 RC4(Rivest Cipher 4)，金鑰長度為 54 到 128 位元。

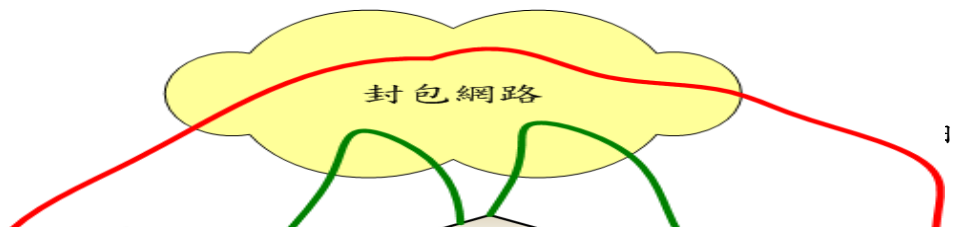
(二)呼叫控制訊號安全

VoIP 用戶端設備包含語音應用(Micro)及數位訊號處理(Digital Signaling Process , DSP)等兩個主要元件(如圖一)，其呼叫處理訊號(如綠線)係依 IETF RFC 3551 即時控制通訊協定(Real-Time Control Protocol , RTCP)，藉於 Micro 及呼叫管理伺服器之間，以呼叫處理通協定(如 SIP、H.323 及 MGCP)來加以溝通通連。

RTCP 可依據 IETF RFC 3771 安全即時傳輸控制通訊協定(Secure RTCP , SRTCP)加以加密，以確保呼叫控制訊號安全。

(三)語音封包安全

語音封包係依據 IETF RFC 3550 即時傳輸通訊協定(Real-time Transport Protocol , RTP)將語音流(如圖一-紅線)打包為封包後，透過 DSP 處理語音加密及密鑰交換，其中語音封包加密由 Micro 或 DSP 執行，可於 IP 層使用 IETF RFC 2401 IPSec 安全協定將封包加以加密或於 UDP 層將 RTP 封包依據 IETF RFC 3771 安全即時傳輸通訊協定(Secure RTP,SRTP)加以加密，而密鑰交換分別以 IETF RFC 2409 網路密鑰交換(Internet Key Exchange,IKE)及 IETF RFC 3830 多媒體網路密鑰(Multimedia Internet Keying,MIKEY)於兩個 Micro 之間加以執行。



圖一 VoIP 網路電話安全架構

(資料來源：翻譯繪製於 Bebbie G. and Sophia S.[2])

(四)阻斷服務攻擊之對抗方式

以下表列 VoIP 網路電話之阻斷服務攻擊之對抗方式，如表四。

表四 DoS 對抗方式

攻擊名稱	對抗方式
ICMP flood	以軟體限制固定時間單位所能接收的封包數量，如果封包數量於設定之時間單位內超過限制，存下紀錄並且丟棄封包。
Teardrop	檢查 IP fragment，如果未經適當地處理即丟棄該封包。
Land	RFC 2267 – 如果位址來自內部，以軟體輸入過濾器(針對外部的網路流量)將不允許封包通過。如果來源位址並非來自內部，軟體輸出過濾器將不允許封包通過。比較封包之來源與目的 IP 位址，若相同，存下紀錄並且丟棄封包。
Ping to Death	限制固定時間單位所能接收的 ping 封包數量，如果封包數量於設定之時間單位內超過限制，存下紀錄並且丟棄封包。
IP spoof SYN flood	RFC 2267 – 如果位址來自內部，以軟體輸入過濾器(針對外部的網路流量)將不允許封包通過。如果來源位址並非來自內部，軟體輸出過濾器將不允許封包通過。

(資料來源：摘譯於美國國防部[3])

網路電話安全技術設置準則

鑑於 VoIP 網路電話技術迅速發展及廣泛運用，美國國防部考量 VoIP 是網路中心戰(Network Centric Warfare , NCW)關鍵性元件之一，它關係到移動性提昇、基礎建設減低、多媒體整合運用及成本降低等問題，為達成有效網路中心戰目標，如何在 IP 網路上將所有通訊流量(數據、語音及視訊等)集中有效運用，於戰術通訊(Tactical Communication)建置安全的 VoIP 網路電話系統將是國防部能否具備此能力之關鍵性步驟。

鑑此，美國國防部防衛資訊系統局(Defense Information System Agency , DISA)訂定「網路電話及VoIP安全技術設置準則(IPT & VoIP STIG)」[3] ，作為各單位建置準則，以符合資訊確保(Information Assurance , IA)政策之要求，依資訊確保弱點管理(Information Assurance Vulnerability Management, IAVM)之弱點可能性定義四級弱點階層碼（Vulnerability Severity Code），訂定「VoIP安全檢查表」，以明確界定VoIP安全設置需求政策項目(如表五)及資訊確保官員（IA

[3] DoD DISA (2006) “IP Telephony & Voice Internet Protocol : Security Technical Implementation Guide”, Version 2,Release 2.

Officers, IAO）職責。

表五 VoIP 安全設置需求政策項目

項次	政　策	說　　明
一	保護VoIP關鍵性伺服器	1.VOIP伺服器的建置是使得語音處理環境得以加密之關鍵點。 2.伺服器應被放置在防火牆保護下之分離的網路區塊中。
二	VoIP設備註冊	VOIP 電話系統於新增電話設備時，呼叫管理伺服器係以自動註冊及下載設定參數方式執行，致使未經授權電話用戶容易進入，應予限制。
三	實體安全	預防未經授權存取 VOIP 設備，應進行人員進出管制，限制存取權限。
四	VoIP系統管理	VoIP 系統管理應以安全方法來管理，包含 VoIP 伺服器之遠端存取管理及 VoIP 防火牆管理。
五	IP軟體電話	安裝於個人電腦，由於作業系統及應用程式存在可能弱點，成為病毒進入媒介。
六	無線VoIP	VoIP 使用無線區域網路來實現（Voice over WLAN, VoWALN），須特別考慮無線安全問題。

七	網路保護及流量管制	網路及所傳輸的數據應被保護，以防禦內部及外部的攻擊，可分從區域網路中 VLAN 對 VLAN 的保護、廣域網路連接及區域網路對廣域網路的保護等執行。
八	呼叫私密性及信賴性	當 VoIP 廣域網路端建立連線後，呼叫私密性可能將遺失；所有防衛交換網路幹線應被加密，以確保 VoIP 終端用戶呼叫的私密性。
九	語音郵件服務	VoIP 語音郵件服務係執行於共通作業系統（如微軟），為避免潛在的弱點風險，應以過濾封包流量或於語音 VLAN 及數據網路間架設防火牆，以防禦阻斷服務攻擊。
十	數據及語音分離 -邏輯位址分離	VoIP元件應被部署在專有的、分離且私有的ip網路，並使用與區域網路不同的位址範圍，來減低語音流量傳輸至電話網路區塊外之機會；當使用dhcp來分配位址時，語音及數據元件應使用不同伺服器。
	數據及語音分離 -使用VLAN之邏輯網路分離	1.語音VLAN：以 802.1Q VLAN標籤方式來分離數據及語音。 2.語音VLAN存取：執行Layer 2 認證存取機制，包含埠安全、以 802.1x執行埠認證及VLAN管理政策伺服器。
十一	系統設定保護	對於電話可顯示設定參數功能者，應以密碼保護，避免提供可能遭受攻擊之資訊。
十二	MGCP安全化	MGCP 協定係介於 MGC 及 MG 間的通訊協定，其所有的呼叫啟動及處理均以明文模式來傳送。建議應以 IPSec 於閘道之間執行加密及認證機制。
十三	VoIP系統管理	應以安全方法來管理，包含 VoIP 伺服器之遠端存取管理及 VoIP 防火牆管理。

(資料來源：摘譯於美國國防部[3])

國軍網路電話運用及安全部署建議

適逢國軍朝向數位化戰場做戰備整備及檢討新科技引進國軍資訊網路之際，植基於 IP 網路之通資整合平台下，將語音流、數據流及視訊流集中管理，以提昇作戰部隊指管能力、減低電信基礎建設及整合運用多媒體目標，因此，未來運用 VoIP 網路電話系統實屬科技整合趨勢。

然對於屬「實體隔離」之國軍資訊網路環境，運用 VoIP 網路電話系統是否可避免所存在之弱點與威脅等資訊安全問題，實值得國軍深究探討。

以下就國軍使用 VoIP 網路電話之運用策略分析與部署安全建議作一說明：

一、運用策略分析

對於 VoIP 網路電話系統之新科技引進，參考企業管理之策略分析(SWOT)方式，初步探討國軍資訊網路運用 VoIP 網路電話時，面對內部環境之優勢(S)與弱勢(W)及外部環境之機會(O)與威脅(T)，提出因應策略，供國軍參考，如表六：

表六 策略分析表

內部環境 策略 外部環境	S(優勢)	W(弱勢)
	1.各基地通資基礎建設逐年提昇，國軍資訊網路通連性高 2.具備國防研發技術及資訊人員素質高 3.重視資訊戰及 C4ISR	1.傳統電話技術觀念，不易擺脫 2.電話線路老舊維修困難及維護成本居高不下 3.無線網路使用限制
O(機會)	SO(使用機會並利用優勢)	WO(減輕弱勢並利用機會)
1.VoIP 網路電話技術及產品成熟 2.國軍朝向數位化戰場指管及網路集中化目標 3.國軍檢討新科技引進之作法	1.結合資訊戰及數位化需求，策頒國軍 VoIP 網路電話使用作業規定及有效地整體規劃。 2.配合各基地通資基礎建設案，逐步整體規劃運用 VoIP 網路電話，落實教育訓練。	1.精實縮減傳統話務業務，局部逐漸改以 VoIP 網路電話。 2.策頒國軍無線網路安全管制作業規定，納編 VoIP 結合無線網路之安全技術規範。
T(威脅)	ST(使用優勢並減輕威脅)	WT(減輕弱勢並減輕威脅)
1.商用市場技術及產品運用普及，領先國軍。 2.科技技術進步快速，資訊產品週期縮短。	1.結合各資訊戰等專案，進行 VoIP 系統整合運用。 2.納編前瞻技術、科專計畫及學術研究，落實技術及學術奠基。 3.納編國防產學研單位，舉辦國內外技術研討會。	1.檢整老舊線路，改以資訊網路取代。 2.定期參訪美軍基地，掌握科技契機。 3.以 COTS 產品為基，建立衛星工廠，落實軍民通用科技。

(資料來源：本研究整理)

二、部署安全建議

在「資訊安全」為首要考量下，國軍如何訂定相關的安全規範及管理措施，有效管理 VoIP 網路電話，以確保資訊安全。以下提出幾項安全部署建議，說明如下：

(一)系統整體規劃，策頒安全規範

鑑於國軍資訊網路類分戰情網路、行政網路、學術網路及網際網路等，規劃運用 VoIP 網路電話系統，應從上而下地整體考量各類網路需求，以整合發揮

有限資源及最佳效能；參考美國國防部安全技術設置準則，廣納產官學研界寶貴意見，策頒國軍網路電話安全作業規範。

(二)隔離語音及數據傳輸的網路

所謂隔離並不是指實體上的隔離，而是使所有 IP 網路電話僅能在獨立的虛擬區域網路(Virtual Local Area Network,VLAN)中使用，可隔離病毒與簡單的攻擊；同時，配合 QoS 設定，以提高語音品質。

(三)保護 VoIP 設備的重要位址及埠

對於控制訊號及媒體流等兩類對外的位址(IP address)及埠(Port)加以保護，同時減少需要的埠數，例如使用以 Web 方式為基礎的管理位址，並關閉不需要的服務功能。

(四)語音封包及控制訊號的加密

運用 VoIP 加密式網路電話，如採用安全標準通訊協定 SRTP/SRTCP，從應用伺服器、IP 電話通訊伺服器至 VoIP 用戶端，整體設計語音及控制訊號的加密及密鑰管理機制。

(五)結合無線行動、有線網路安全防護

為實現國軍行動(M)化戰場之目標，參考國軍「010 專案」模式，植基於民用第三代(3G)行動通訊系統之數據服務網路，運用個人式行動 3G PDA 手機及站台式 3G 無線路由器(Wireless Router)，以無線接取 3G 基地台，進入系統業者機房輔以 VPN 流量隔離，透過專線方式介接國軍光纖骨幹網路，在用戶端與入網閘道間，建立傳輸通道安全，在入網閘道端，建立資訊系統安全防護，以確保傳輸及通信安全（如圖二）。

國軍資訊網路及行動網路之VoIP網路電話用戶，藉由轉換閘道器(Trunk GW)介接國軍六碼軍線之交換機(PBX)，以構連雙向之語音(數位及類比)保密通連。

結論

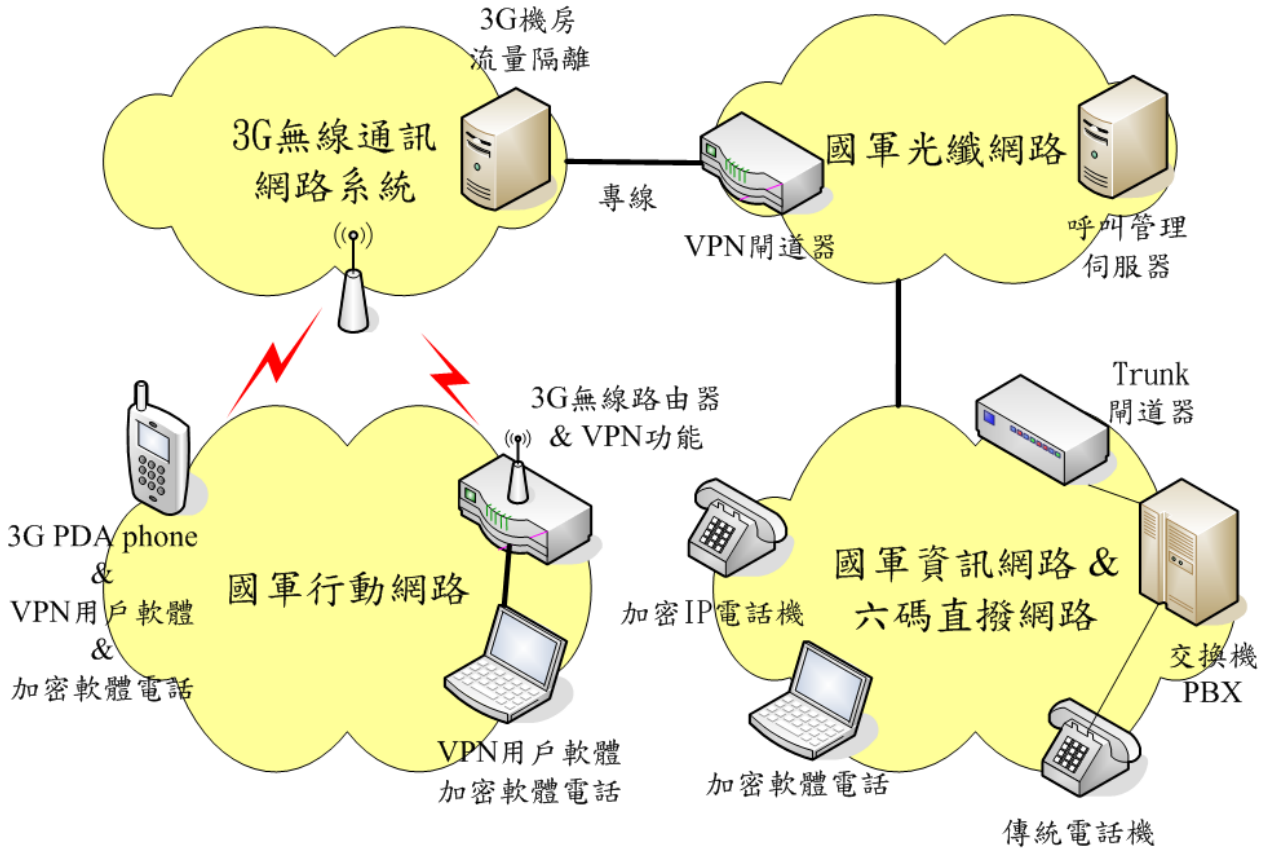
VoIP 之所以能迅速發展，主要在於發展潛力為具備整合且有多元化的應用，未來的應用發展趨勢如下：

一、企業網路應用方面

VoIP 技術導入企業網路，將使得企業內之所有的通訊服務將整合在單一網路。

二、網路應用服務方面

由於公眾電話服務網路與 IP 網路經由 VoIP 而結合，將衍生許多整合網路特性之整合性服務，如 SIP/ENUM，所謂 ENUM 是一種結合電信與網路的服務，使你的電話號碼有多重的電信語音及網際網路功能。



圖二 國軍部署運用示意圖

三、網際網路應用方面

VoIP 在網際網路的應用及 SIP 多媒體應用服務，如即時通訊(Instant Message,IM)、影音信箱(或部落格)、電子郵件、行動秘書、緊急安全電話及呼叫中心等訊息服務等。

四、無線行動通信方面

VoIP 技術與第三代行動通訊系統(3GPP)結合，使其核心網路架構為全 IP 網路。

前瞻未來 VoIP 網路電話系統發展，隨著 VoWLAN(Voice over WLAN)及 VoWiMAX(Voice over WiMAX)技術成熟、安全標準制定及結合第三代行動通訊系統的運用，將提供完整的數據、語音、視訊及多媒體之整合性網路應用服務。國軍能否前瞻地運用新興的 VoIP 技術並確保 VoIP 系統安全，在 IP 網路上將所有通訊流量(數據、語音及視訊等)作有效運用，來達成有效網路中心戰目標，進而確保國軍在數位化戰場之資電優勢，實為刻不容緩的任務。

參考資料

一、VoIPSA “VoIP Security Threat Taxonmy”, Voice over IP Security Alliance (VoIPSA) , 2005.

二、D.Richard Kuhn, Thomas J. Walsh, Steffen Fries “Security Considerations for Voice Over IP Systems”, Special Publication 800-58, National Institute of Standards and Technology(NIST), 2005.

三、DoD DISA “Voice Internet Protocol : Security Checklist”, Version 2,Release 2.2, 2006.