NBL 實驗室訪問報告

林盈達、陳一瑋、陳世揚

摘要

為了進一步了解國外測試實驗室的定位，以及市場領導廠商產品線發展及對測試的重視程度，NBL 一行三人（主任、網安與無線之專案經理）於九月拜訪了美國十個單位，包含三個實驗室（UNH/IOL, ICSA, Veritest），三個測試設備廠商（Azimuth, IXIA, Spirent）及四個網路設備廠商（Fortinet, Cisco, Juniper, Alcatel）。除了與 ICSA 協議在台灣合辦研討會、與 Veritest 同意研究在台合作的方式，成為 IXIA 全球支援的七個實驗室之一，以及 Fortinet 加入 NBL 近期將成立之 Security Consortium 等合作，我們將此行討論過的議題及心得整理於本文，一般性議題如產品化資源是否充足、測試實驗室的定位及與大廠的關係等，網安議題如為何 ICSA 很難取得、在多合一的趨勢下 best-of-breed 與 in-house 作法的差異、Switch IC 的生態是否也會重現於 security IC 等，無線區域網路議題如 Wi-Fi 會增加哪些測試、MAC 與 PHY 沒有 conformance 的情況、整合各種測試工具的需求與困難等。

1. 訪問對象、目的與結論

我們一行三人從波士頓開始，拜訪 UNH/IOL 的 director 及 WLAN 的 manager，以及 Azimuth 的 VP 及 PQA manager，然後飛到賓州的 Harrisburg 拜訪 ICSA 的 VP、technology program manager 及 sales manager，之後轉往舊金山，拜訪 Fortinet 的 CEO/Founder 及多名 director，Cisco 的 test lab manager，Juniper 的 test technologies director 及多名 manager，再飛往洛杉磯拜訪 IXIA 的 VP 及多名 director 及 manager，Veritest 的 VP 及 director，Alcatel 的 Sr. director 及 manager，最後是 Spirent 的三個產品線的 director 或 manager。近年來我們每一兩年都會進行類似的拜訪，綜合的觀感是大部分的測試實驗室都很偏僻，離主要都市也都一兩個小時，但只要有價值並且持續演進，都可以找到生存之道，而大部分的公司則是群聚於幾個點，如 San Jose，洛杉磯附近的 Calabasas 及 Irvine，波士頓的 Cambridge，德州 Austin，北卡的 Research Triangle Park 等。大部分的美國公司或實驗室也都較 open，願意討論及表達看法，所以整個產業環境的進展腳步也會較快。

測試實驗室

拜訪 UNH/IOL（full-time: 23 人，partime: 100 人）主要是 renew 雙方的合作關係，透過去年的合作 MOU，NBL 派人去 UNH/IOL 受訓，建立 Conformance

及 Interoperability 測試的能力，後來雖討論過在台灣合辦 ADSL2+ Plugfest 插拔大會的可能性,但 UNH/IOL 在 survey 過 DSLAM 廠商及 DSL Forum 後因成員意願不高而作罷，NBL 則與電通所自行籌畫將於今年 12 月 6 - 10 日舉行之亞太區第一次的 ADSL2+插拔大會，雙方之後的合作將定位於人員互訪與技術交流。另外由於 UNH/IOL 尚未有 security 方面的 consortium,目前他們也在考慮是否要將目前散佈於不同 consortium 的 security 測試集中成立一個 consortium。

相較於 UNH/IOL 的 open，ICSA（full-time: 35 人）顯然較為封閉，只公開測試項目（criteria）而沒有測試步驟（procedure），也有許多世界各地實驗室希望與 ICSA 合作成為一個 branch 的要求，但都被回絕，原因是 Intellectual Property、crediability、quick update on criteria 三個考量，如果 NBL 進行 ICSA pre-test，ICSA 也不會提供額外協助但樂觀其成。對於為何 ICSA 難以通過，回答是因為許多廠商對自己程式及標準文件的掌握度不夠，往往無法解決 ICSA criteria 所列之問題。為了增加台灣廠商對 ICSA 的了解以及送測產品的數量，ICSA 同意與 NBL 在台灣合辦研討會，說明測試內容與流程，預計於明年第一季。我們也參觀了 ICSA 的 lab，主要分 network security 及 content security 兩區，但五點多就都下班了，我們也很驚訝他們並未取得 ISO17025，但已排入其 roadmap。

Veritest(full-time: 400 人於全球 11 個 lab)是我們不熟悉也是第一次接觸，它是附屬在從事 IT outsourcing solutions 的 LionBridge 之下，LionBridge 的核心業務為 application development 與 maintenance 及 localization/translation，systems/app/product testing 為附帶業務，前者之客戶為 enterprises，後者之客戶為 vendors，而散佈於全球的 11 個 lab 也可以支援其核心業務，11 個 lab 分工從事 ISP MS windows、S/W app、S/W desktop SAN/NAS、Network 等之測試，其中與網路相關的是在北卡 Raleigh 由 ZDlab(30 人)併購進來。幫 Microsoft、AT&T wireless、Palm、Alcatel、 Novell、CMM 等執行 certification program 是 Veritest 主要的業務，而幫其他設備廠進行 benchmarking (performance 及 feature comparison)則是次要業務。NBL 將與 Veritest 在 Raleigh 的 lab 討論合作模式，尋找互補的空間。

測試設備廠

網路測試設備產業目前由 Spirent、Agilent 及 IXIA 三家主導，Spirent 最初著力於 switch 測試，目前產品線最廣，延伸至以 Avalanche 為主的 app 層測試、以 Abacus 為主的 VoIP 測試、及各種 GPRS/3G 測試，Agilent 著力於 router 及實體層之測試，但也以 VQT 進入 VoIP 及以 Network Tester 進入 app 層測試，IXIA 以較低價格切入市場最大的 switch 測試，並以收購 Chariot、ANVL 及 CST 進入 app 層、conformance 及 VoIP 測試。

Azimuth 是一家新公司，其產品 W-Platform 以調整 attenuation 提供目前其他設備無法進行的 WLAN mobility 及 roaming 測試，對於新的應用如 streaming

及 VoIP，以及 public WLAN、雙網環境（GSM 及 Wi-Fi）之測試有幫助，我們的拜訪主要是了解 Wi-Fi 增加這些測試項目的進展、W-Platform 的測試軟體發展的 roadmap、以及對 NBL support 的程度，據 Azimuth VP 表示，Netgear/ D-Link/ Linksys 將會要求供應商進行這些測試，而其軟體發展 roadmap 看起來也很完整迅速，也將持續提供支援 NBL。

IXIA 與 Spirent 都位於洛杉磯郊區的 Calabasas，相對於 Spirent，IXIA 在台灣的 marketing 活動少很多，我們的拜訪主要是希望 IXIA 能給予 NBL 更多的設備支援，經過一段的報告與討論後，IXIA 決定將 NBL 放在他們全球支援的 lab program 中，過去他們 support 50 個 lab，現在只 support 7 個有技術深度及代表性的 lab，NBL 是亞太地區的唯一。IXIA 近期推出許多以 Ix 為名的測試工具，包括 Ixload、IxVPN、IxChariot、IxAccess、IxANVL、IxExplorer、IxVoice 等。

Spirent 的 Avalanche、Abacus 及 GPRS/3G 測試設備的開發都在 San Jose，產品經理也特別到 Calabasas 總部與我們討論，了解我們在 Avalanche 及 Abacus 的使用經驗的新需求，因為資源有限，NBL 並不會投入 GPRS/3G 之測試。

網路設備廠商

此行所拜訪的四家廠商，有兩家是網安產品領導廠商（Juniper/Netscreen 及 Fortinet），兩家網通大廠（Cisco 及 Alcatel），前兩家系出同門，Fortinet 的 founder 也是 Netscreen 的 co-founder，都是以 ASIC 技術分別解決 network security 及 content security，兩家也都是 all-in-one 產品的代表，但主要的歧異在於 Juniper/Netscreen 認為在 AV 等 content security 的技術應使用市場上的 BoB(best of breed)，而不是自己發展，Fortinet 則是使用 in-house 自有技術，兩者到底誰好，似乎只能透過評比測試及市場考驗來判斷。Cisco 是網路產業的老大不用詳述，Alcatel 雖然在 datacom 的版圖還不夠大，但在 carrier 級的通訊包括寬頻、光纖網路、行動等都是第一，現正結合在 carrier 市場的優勢進入 non-carrier 市場，特別是在 switch、VoIP、WLAN、Security 等。

拜訪 Fortinet 及 Juniper/Netscreen 主要是想了解他們對網安產業的看法以及對內容安全如 AV、IDP、SSL VPN 的測試方法，Fortinet 舉 IDC 的預測說明 UTM（unified threat management，即 content security）的產值將於 2008 年超過傳統 FW/VPN 所代表的 network security，他們也認為 AV、IDP 等問題可以 in-house 用 ASIC 技術解決，不需用現有 BoB，另外，獨立的網路晶片廠商，如 network processor 及 security ASIC 的晶片商，空間將不若 PC 晶片組廠商，因為除了少量多樣的因素外，軟硬體整合的困難度較高使產品效能無法進入高階市場。Juniper/Netscreen 則在 AV 方面相信 BoB，他們對 IDP 及 AV 以外插 module 方式整合，同時因 Juniper 的影響，著力更多在 connectivity 上，如 multicast、IPv6、BGP、MPLS、GPRS、ADSL 等的支援。對於測試，我們也討論了很多 AV、IDP、SSL VPN 的測試方法與重點，IDP 的測試是最棘手的，因為不像 AV 有公認的組織維持 signatures，所以很難有公正客觀的評比結果，而 SSL VPN 的測試重點應

是好不好用、用戶端是否要額外安裝以及管理功能，而不是在效能的評比。

在 Cisco test lab 的討論主要在於 Cisco 所有產品線將強制執行的 Security Function Baseline(SFB)要求，以及對產品或系統進行這些測試所需的工具與方法，目前並沒有標準的工具或方法，故亟待開發。

由於 Alcatel 以 carrier 市場的經驗切入 non-carrier 市場，故強調產品的 manageability、availability 及 security，也特別在意自家產品在 price vs. feature rating 的圖中的位置，如果無法在 price 或 feature rating 上佔據利基位置就不會進入該市場，另外 Alcatel 並不直接進入網安市場，而是與 gateway 廠商合作進行 Switch-gateway 的聯防，並轉而開發更接近 carrier 等級的 security 管理機制。Alcatel test lab 的 director 將 PQA 人員的每週績效排名表直接貼在 lab 入口，雖然不太人道但效果不錯。

與 UNH-IOL 合影

與 Azimuth 合影

與 ICSA 合影

與 Fortinet 合影

與 Cisco 合影

與 Juniper/Netscreen 合影

與 IXIA 合影

與 Veritest 合影

與 Alcatel 合影

與 Spirent 合影

2. 一般性議題

接著我們將此行重要議題的看法，整理並分類為一般性、網安及無線區域網路，我們的答案也許仍有爭議性，但應具有參考價值。

游擊戰 vs 正規戰？

一個產品線的開發與維護，至少需要七種角色的人：(1)PM，(2)RD（分增加 spec 及解 bug），(3)PQA（分功能及系統），(4)marketing，(5)presales，(6)sales，(7)postsales(tech support)，如果 PM 的規格是抄來的或聽來的，而不是 presales 及 postsales 收集來的，如果同一個 RD 因為解 bug 而無法應付新增 spec，如果 PQA 也要去做 tech support，如果 presales 也要兼做 sales 或 postsales，那都代表投入的資源不足，無法進行正規作戰，這對習慣於經營 ODM 而不是自有品牌 OBM，以及 retail 而不是 SI 通路的廠商而言，可能是常態的游擊戰，這對於使用 turn-key solution，大量 ODM 給客戶，透過 retail 通路去賣的經營模式應該是沒有問題，但對於整合與累積自我 IP，經營自我品牌，透過 SI 通路去賣的模式就不行了，當然打正規戰燒錢的速度會很快，管銷費用比較高，也要有較高的 gross margin 才能支撐，但如果不這樣做只能在低階產品及低階行銷模式辛苦生存。技術開發可以靠天才，但產品開發與行銷要靠人力，相對而言，國內廠商對同一件事投入的資源是小於國外 leading 廠商（不一定是大廠）。測試實驗室也是如此，與國外許多 lab 相比，NBL 的資源太少，如何突破這個瓶頸也是我們的議題。

Test lab 的定位與價值？

UNH/IOL 及 ETSI 是以技術磨合為定位，兩者都非常 open，ETSI 僅以互通插拔大會為主，而 UNH/IOL 除了插拔大會還提供了常態性的測試環境與測試服務，故更有價值，這些價值是由大廠資助的 23 名 full-time、100 名 part-time 人員經歷 16 年累積創造出來的，是無法複製的。

另外一種定位是 certification lab，ICSA、NSS、Wi-Fi、Cable Lab、Veritest 等都是這樣的定位，它們都是做 quality assurance testing，並以發 logo（Veritest 是幫別人做）為其價值所在，但也都有大廠間接（ICSA）或直接（Wi-Fi）的支持，如果無法取得國際大廠的支持，所發的 logo 的價值也會降低，這些支持，不只是資金，還包括技術的 co-work 合作，去定義與新增測試要求。Wi-Fi 及 ICSA lab 的價值，不是 lab 本身而是背後支持的國際大廠。

還有另外一群以marketing tool為定位的test lab，包括Tolly Group、Miercom 及一部份的Veritest，通常它們都是與雜誌合作進行評比開始，累積信用後再開始賣信用為出錢廠商進行 3rd party測試報告，做為行銷工具，通常為了替委託廠商

測出較有利之結果，必須「慎選」測試項目與方法，雖然結果是reproducible，但評比項目或方法往往不夠完整客觀，故行銷效果有時會被打折扣。

除了以技術磨合、certification 或 marketing tool 定位外，NBL 可以有什麼選擇？應該是 engineering reference，儘量找出產品在功能、效能、符合、互通、評比方面的詳細缺點，作為工程改進之參考，這是目前 NBL 的定位與價值，但是這件事卻是辛苦的，因為要告訴委測廠商一些原本他們不知道的問題，不同的人用不同的方式測本來就可發現不一樣的問題，如果這件事可以做的很好，將來結合大廠的支持或許有機會可發 certification。另外一個可行的定位是 outsourced testing，但必須是高階的工作，因為低階的 outsourcing 會跑去印度，高階指的是高階功能的 test case design 及 automation。

3. 網安議題

內容過濾防火牆 vs. 封包過濾防火牆

網路的世界裡，安全性議題一直是非常重要的一環，因為在網路上有太多的”有害物質”會對一般使用者或企業的經營者造成傷害，例如駭客攻擊、色情網頁、病毒、蠕蟲、垃圾郵件，甚至是即時訊息(IM; Instant Message)及 P2P 共享軟體，都是可能會造成企業經營重大損失的因素之一，對於傳統以”封包過濾(Packet Filtering)”技術為主的防火牆而言，能夠抑制這些威脅的效果非常有限，必需仰賴更新的防火牆技術 -”內容過濾(Content Filtering)”來達到有效的嚇阻。[註: 本文所說的防火牆，若沒特別註明，都是指 appliance，即硬體式防火牆]

傳統防火牆主要是根據封包的 five tuple (i.e. source/destination IP address, source/destination port number, transport layer protocol)來決定要對此封包作什麼樣的動作 (e.g. block or permit)，可稱之為靜態封包過濾，進一步有廠商研發出”封包狀態檢測(SPI; Stateful Packet Inspection)”技術，除了根據 five tuple 作過濾之外，還會根據”協定(i.e. TCP/UDP)的行為、狀態”或是”連線的行為、狀態”來處理封包，亦可稱為動態封包過濾，不論是靜態還是動態，都是對”封包”檢測，而不是”內容”，所謂的內容即是指應用層(application layer)的資料，可以是一個封包或是由多個封包重組過後的資料，例如:一個網頁、一個檔案、一封郵件、或是一則訊息，”內容”裡含有”特徵值”，內容過濾防火牆主要便是依據此特徵值來決定是否要阻擋該內容，可稱之為靜態內容過濾，跟封包過濾技術一樣，相對應的就是動態內容過濾，根據 application protocol (e.g. HTTP, DNS)的行為來決定該是否要將其阻擋，市面上的內容過濾防火牆裡所具備的功能大致上有: 入侵偵測與阻擋(IDP)、網頁過濾(Web Filtering)、防毒(Anti-Virus)、防垃圾信(Anti-Spam)、以及 IM&P2P management。

著名的市場分析組織 - IDC(International Data Corporation)，最近在

Security Appliance 這個領域裡,新增了一個 category 叫作 UTM(Unified Threat Management),定義為同時含有傳統防火牆、IDP、以及 Anti-Virus 這三大類功能的硬體平台,代表著這類產品目前已經在 Security Appliance 市場中占有一席之地,在 2004 年 9 月份公佈的一些報告中提到了以下幾個重要的市場現象:

(1) UTM 在 2003 年有超過 US$100 million 的 revenue,相較於 2002 年成長了 160%,是在 Security Appliance 裡成長最多的一個 category。

(2) 預測到 2008 年,UTM 的 revenue 會有 US$3.45 billion,在 Security Appliance 裡所占的 market share 達到 58%,超過傳統的 Firewall/VPN。

(3) Security Appliance 在 2004 Q2 的 revenue 相較於 2003 Q2,成長了 57%,其中 UTM 在占了整個 marketplace 的 12%,傳統 Firewall/VPN 則從 87%掉到 70%。

從 NBL 的角度來看,台灣的廠商投入在 UTM 設備的研發也確實有增加,只不過感覺上台灣廠商對於這種高階產品的開發似乎還在摸索階段,該投多少的資金、該花多少的人力、技術的開發、產品的測試、行銷的策略,一定都會跟以往較低階的產品有所不同,不過我們相信在 Network/Content Security 領域往這個方向走下去是對的,就像愈來愈多台灣的大廠想要靠 brand name 賺錢,而不是要靠 OEM 或 ODM 的方式賺錢是一樣的道理,唯有向高利潤挑戰,才能突破現狀。

硬體加速的需求

傳統的 Firewall/VPN 產品,在效能上需要特別去加強的就是 VPN 在做加解密(i.e. crypto)時的速度,以 NBL 所測試過的產品而言,ASIC、FPGA、或是 Network Processor,都是曾經看過的解決方法,而在內容過濾防火牆這類產品中,也有需要硬體加速的地方,主要是特徵值比對(signature matching)演算法,這是由於

(1) 搜尋空間變大: 網路流量增加、需要徵值比對的產品功能增多

(2) 特徵值不斷的增加: 攻擊、病毒種類增加

目前所看到的解法是以 ASIC 為主,因其所達到的效能提升最有效益。

在 Switch IC 的生態中,我們可以發現大廠擁有獨門、私有的(proprietary) chip,而較小的廠商便用現成的(off-the-shelf)chip,主因為 Switch 這個領域的技術及市場規模已相當成熟,所以一般廠商用現成的 chip 就足夠與本身系統作整合到穩定的程度且有符合需求的效能表現,但對大廠而言,所面臨到的效能和穩定性需求更加的嚴苛,因此需要自行開發 Switch IC 來加強效能、更緊密地與本身作業系統整合,這樣的生態會不會發生在 Security IC 上呢? 就加、解密方面而言,由於加、解密演算法及其最佳化已經相當固定,不像 Switch 的效能跟架構較有關係,所以網路安全大廠較不需要自行開發 crypto IC,就市場面而言,由於加、解密有一定的需求,crypto IC 的廠商也會樂意開發這類型的 IC,至於特徵值比對就比較不一樣了,IC 廠商可能會因為市場的考量,以致於不去

生產特徵值比對 IC，所以對網安的廠商而言，大廠會自行去開發產特徵值比對 IC 的機率較高，但對小廠而言就比較難像加、解密功能一樣找到適合的加速 IC 了。

網路架構之安全性三層級：點、線、面

在 Host PC 做安全保護措施就是”點”，在 Gateway 上就稱為”線”，而 Gateway 與 Switch 的聯防就稱為”面”，早期的網路安全架構是在 Host PC 安裝防毒軟體，而 Gateway 必須俱備 Firewall(packet filtering)的功能，接下來 MS 也在 Windows 支援 packet filtering，不過並沒有影響到硬體防火牆的市場，然後在 Gateway 上也出現 Anti-Virus 的功能，同樣地也尚未對防毒軟體造成太大的影響，現今除了 Gateway 本身俱備多功能之外，還可以搭配 Layer 2 Switch 作聯防，當 Gateway 發現是哪台機器(i.e. IP address)中毒在狂送封包時，除了將其封包阻擋下來之外，還可通知 Switch，讓 Switch 將那台中毒機器所送出來的封包直接阻擋在其下，不讓中毒的流量在內部網路散播，聯防這項技術最重要的就是如何讓 Gateway 與 Switch 作溝通，我們認為應該利用現有的 protocol(ex. SNMP)來進行聯防，以利全面性的推展。

從上述的演變過程中，我們認為人們對於安全性的要求，無論是在現實生活中還是在網路上都是一樣，能夠愈安全愈好，除非可以保証用了哪一種方法之後可以百分之百杜絕病毒或攻擊的發生，要不然縱使在 Gateway 上已啟動防毒功能，並且與 Switch 聯防，使用者依舊會在 Host PC 上安裝防毒軟體，不怕一萬、只怕萬一。

傳統 Content Filter/Anti-Virus 廠商的未來?

在目前內容過濾 appliance 市場愈來愈大的情形之下，傳統的 Content Filter/Anti-Virus 廠商是否會有危機? 會不會像當初的 CheckPoint 一樣，打著 solution provider 的招牌卻錯失 appliance 市場良機,之後便漸漸默落了呢? 以下是我們的分析:

對於傳統 Content Filter 廠商而言，這樣的危機的確存在，我們看到一些規模較大的 appliance 廠商,原本是採用傳統 Content Filter 廠商的 solution(e.g. filter engine,URL list),現在已經有了自己的 solution,雖然有些 appliance 還是會以”多選”的方式讓使用者選擇想要用哪一種的 solution，但這只是過渡期的作法，當 appliance 廠商對本身的 solution 有相當的信心之後，就可以隨時將”多選”變成”單選”，對機器的掌控權是 appliance 廠商的一優勢，除此之外，傳統 Content Filter 廠商還得面臨 MicroSoft 的威脅，可以說是前有堵截，後有追兵，處境堪慮。

對於傳統 Anti-Virus 廠商而言，所面臨的挑戰比 Content Filter 要來得小了許

多，主要是因為傳統 Anti-Virus 廠商所提供的 solution 原本就不是給 appliance 使用，而是讓 Host PC 所使用，當使用者在 PC 上已經習慣了 Anti-Virus 的軟體之後，即使在 Gateway 上也啟動了 Anti-Virus 的功能，使用者依舊會安裝軟體的 Anti-Virus 在 PC 上，一方面是習慣性問題，另一方面能讓使用者更安心，不過我們也可以看到目前幾家傳統 Anti-Virus 的大廠 (e.g. TrendMicro, Symantec)也積極地在往 appliance 產品上面發展，可見未來還這兩類型的廠商有一場大戰要打。

BoB(Best of Breed) vs. In-House

在上一個網安議題中，我們提到了目前有幾家傳統 Anti-Virus 的大廠正積極地在往內容過濾 appliance 產品上面發展，有的傳統 Anti-Virus 廠商就乾脆去找 appliance 的大廠合作，這就是所謂的 BoB (Best of Breed)作法(e.g. TrendMicro 與 Juniper)，相反地，原本的 appliance 大廠中若本身就有開發 Anti-Virus，我們稱之為 In-House 作法(e.g. Fortinet)。

在 Anti-Virus 這個領域裡，有兩件事情最重要，一個是 virus signature database 的維護、更新，一個是效能的表現，這兩件事情對 BoB 及 In-House 來說，剛好各有擅長。對 BoB 來說，傳統的 Anti-Virus 廠商一定已經有很好的技術人員來維護 virus signature database，這是需要非常多的人力與時間，長期努力下來的成果的，但對於效能方面來說，這就必須要靠雙方研發內容的共享與整合，這是相當困難的一點; 相反地，對於 In-House 來說，由於整個系統都是自行開發出來，所以對效能的加強可以有最好的效果，但是在於 virus signature database 的維護方面就略遜一籌，這類 database 的維護通常需要相當多的人力投入，並且長時間的研究病毒種類、行為，這樣一有新病毒產生時才能迅速地造出 virus signature，並且寫出解毒程式

Global certification vs. Local certification

網安產品目前功能複雜，在各種不同的做法、技術演變之下，使用者很難去分辨一個產品的好與壞，對於也想往這方面發展的台灣廠商而言，也很需要能夠了解到如何去測試產品、要做到什麼程度才會有競爭力，在國外有一個專門發網安產品 certification 的組織叫作 - ICSA，它訂定出許多的標準，一個產品要拿到 ICSA certification 就必須通過這樣標準的測試，在台灣，總共也才兩、三家大公司有拿到 ICSA certification，除了技術的門檻之外，收費的標準對台灣大部分的廠商來說也是個很大的負擔，ICSA 會在某些領域成立 consortium，讓有做這領域產品的廠商能夠互相交流，其中也包括業界標準、產

品測試、以及產品認証。

由於台灣參與網安產品開發的廠商還算不少，因此我們覺得應該也要有一個在地的 consortium，來討論一些議題，例如: 產品測試、測試工具研發、訓練教材等等，若此 consortium 的活動順利，台灣做網安產品的廠商量持續成長，或許就可以考慮發行 NBL certification，來認証想在台灣販賣的網安產品，這樣無論是對使用者、或是台灣的廠商都會相當有幫助。

4. WLAN 的議題與發現

儘管對用戶而言，Wi-Fi 認證已直覺地代表了 WLAN 產品品質的測試，但它其實是互通性測試，不代表包含 WLAN 在內的網通產品所需的完整測試範疇。我們要討論符合性（Conformance）測試、將來會更勝於 Wi-Fi 標準的效能測試、測試設備採用以及跨應用領域測試的困難等。

需要符合性測試嗎？

任何宣稱其產品相容於 IEEE 標準的 WLAN 晶片廠商，因為直接涉及 PHY（Physical）與 MAC（Medium Access Control）的設計，不可能刻意去忽視符合性測試，雖然我們多年來我們已知 Wi-Fi 互通性標準的意義重大，卻沒有見過標準化的符合性測試。然而在產業裡，系統廠商更多，且更無法直接掌握 PHY 與 MAC 是否符合 IEEE 標準，也就難免會忽視符合性測試，而更看重互通的品質優良與否。從這麼多年的結果來看，既然互通性測試已經標準化並且還在翻新，符合性測試僅在於晶片廠商自行設計的方法，顯然符合性並不很要緊。

不過在理念上，如果 WLAN 產品與標準的符合度很好，如此便不必太擔心互通性問題，然而這卻不是一件容易的事情，因為有開發者指出 IEEE 標準仍然有些灰色地帶，而且晶片廠商的某些產品規格可能在不得不偏離標準，而維持著獨特優勢。如果是這樣，這些方案與標準不符合的程度有多少？筆者很難估計，沒有證據顯示晶片廠商的方案是否 IEEE Conformant，畢竟沒有測試標準。直觀而論，以最近幾年某些晶片大廠總是在標準確定之前就推出前導產品，是不可能與標準完全符合的，而其他廠商的後續產品，必然要先重視與大廠互通了。

那麼，晶片廠商有強烈的符合性測試需要嗎？就世界上的測試服務來談，在 NBL 拜訪過的 UNH-IOL 裡，有開發了部分的 WLAN 符合性測試標準。可是，在全球提供 WLAN 符合性測試服務的，幾乎可說是僅此一家實驗室，其 WLAN Consortium 中的十幾個成員，也減少到只有三家晶片廠商，如此看來需求是在降低。另外就測試設備的支援情形來看，Azimuth 是擁有針對 WLAN 產品測試的設備方案，有隔離訊號與 attenuation 的設計，還包括正要推出的 Wi-Fi 自動化，對未來的 Roadmap 卻不著重在符合性，其 VP 告訴我們，儘管他們有開發 MAC 符合性測試的可能，但廠商不會那麼在乎符合性測試。

當晶片廠商一再支持推動互通性測試的 Wi-Fi 組織，答案本來很明白。

在 Wi-Fi 互通性之外

我們還是要問，那麼互通性測試已經足夠了嗎？當然不是，晶片廠商與系統廠商在市場上不斷建立的優勢，除了功能的增加（新標準的支援），還有效能的提昇。效能的觀點在對於產品的評估上從來沒有被忽視過，只是它不會優先於對功能與互通的評估，只要 WLAN 產品的設計趨於成熟，許多廠商都能推出功能不乏的產品，和其他廠商的產品能夠連結順利，那麼效能成了評斷品質優良與否的指標了。Wi-Fi 聯盟會不會考慮某年推出效能測試標準呢？筆者還不得而知，但 Wi-Fi 總是在 IEEE 的標準制定前先推出相關的互通測試標準，例如去年的 WPA（Wi-Fi Protected Access）在今年的 802.11i 之前推出，今年的 WMM（Wi-Fi Multi-Media）在明年的 802.11e 之前推出，只是皆著重在互通性測試。至少在現階段而言，由於功能不斷翻新增加，互通性測試也就可以不斷翻新增加，短期內系統廠商還不會很重視效能，直到效能評估的標準即將制定之時。

IEEE 確實有要制定 WLAN 的效能評估標準，即 802.11t，但目前還只是剛形成工作小組的階段，離標準的制定應該還有二至三年的時間。該注意效能測試的方法了嗎？正因為標準開始要起草，這是廠商開始去正視的好時機。筆者個人以為，不少台灣的廠商常迫於客戶對 Wi-Fi Logo 需求的壓力，只投入目前 Wi-Fi 測試的項目，不夠深切瞭解到 Wi-Fi 測試標準依然是跟著 IEEE 標準在起舞的，而且在更早就要推出，因為某些晶片廠商在標準制定之前就已經有方案了。如果系統廠商希望不再處在落後追趕的窘境，便要早點開始準備，建立相當的經驗，在選擇與取得新的晶片時才容易得心應手，到時候能夠輕鬆接受晶片廠商根據 802.11t 標準提供的效能數據嗎？廠商自己或委託的測試實驗室要有能力評估。除了 802.11t 以外，還有 802.11r（Fast Roaming）和 802.11s（Mesh Networks），都是 Wi-Fi 將來會重視的標準，早點瞭解早點準備，不該再遲鈍的。

當拜訪 Azimuth 時，他們表示持續地將效能測試放在首要的目標上，其客戶目前也多為晶片廠商，同時也和各家晶片廠商投入 802.11t 的標準制定上。而在 Alcatel，他們告訴筆者對於 Roaming 等效能上的測試是很需要的，卻是他們目前無法進行的測試。目前在台灣的晶片廠商也開始對 NBL 提出效能測試的需求。嚴格說，除了 802.11t 的效能評估標準不是互通性，在多年後的未來裡沒有 Wi-Fi 之外的測試，因為它會不斷改變。其實筆者還認為 Wi-Fi 也會在 802.11t 制定前將互通測試標準延伸至效能測試標準，只要晶片大廠確實支持。

WLAN 的測試工具整合

不像 Spirent 和 IXIA 等已推出了多種對有線媒介裝置的測試設備，Azimuth 只投入專為 WLAN 測試所設計的設備，考慮到 2.4GHz 和 5GHz 無線射頻訊號所

需的媒介，也整合自行開發的 Windows NDIS（Network Device Interface Spec）程式、Wi-Fi 測試指定的 NetIQ Chariot 與常用的 802.11 監視程式：WildPackets AiroPeek。這看起來應該是很不錯的方案，但是身處在 WLAN 廠商先進且多重的測試需求裡，筆者很快就發現這是不夠的。其一，使用 Windows NDIS 程式和 Chariot 產生的 Traffic 還不足以做精確可靠的效能測試，NDIS 程式的能力不足，而 Chariot 實現的應用層協定也不夠真實；其二，WLAN 產品對其它網路介面與系統的整合不斷出現，例如 Router 產品、具備類比輸出介面的 Media Adapter、與支援 SIP 和 RTP 的 VoIP Gateway/ Handset 等，這些產品的應用超越無線媒介而不可能只依賴專為 WLAN 測試所設計的工具。在與 Azimuth 的談話中，他們會繼續對 802.11 系列標準的測試支援，並擴展到 802.16（WiMax）的測試，但是短時間內仍只會專注在這些無線媒介測試的範疇。

Azimuth 承認，例如即將迫切需要的 VoWLAN 測試，把 VoIP Handset 放進平台裡測試對他們而言仍然是難題。然而，其他專業應用領域的測試已經有對應的測試設備，例如要測試 IP 路由與 SIP 交談協定，Spirent 和 IXIA 都已有許多的方案，而語音品質、以至於音視訊品質，Agilent 和 Rohde & Schwarz 也已有相當完整的各式儀器，這些廠商彼此也正在增加對方的一些測試技術。但是這些不同領域測試技術之深入，很可能不是單一家測試設備廠商所能夠涵蓋的，況且就算有機會能有完全整合的設備出現，也可能會是價位過高，因為目前台灣的廠商就已經反應 Azimuth 平台的價位不容易負擔了。筆者設想如果測試實驗室的服務，能夠整合不同領域的專業測試工具，那麼便能創造出價值。

不過在整合設備上會不會有什麼樣的困難呢？當然，因為不同的設備是針對不同的產品去設計的，例如某個 Scenario 需要依序產生一些 Traffic 或需要依序調整媒介的環境，如果是跨越不同測試設備，這些設備彼此要如何協調呢？於是就要開發協調設備的控制程式，這包含一個前提在：這些設備要具備可程式化的 API（Application Programming Interface）。如果各個設備的 API 所倚賴的語言與平台不同，我們又要為各個設備寫個 Wrapper 對應至共通的語言，因此整合工作還是有其複雜之處的，克服這些問題的努力就是價值所在了。