財團法人台灣網路資訊中心因公出國人員報告書

98年 4月 28日

報告人 姓名	高境輿 楊禎葆	服務單位 及職稱	TWNIC 技術組工程師
出國期間	98.3.22-98.3.29	出國地點	美國舊金山
出國事由	參與 IETF 第 74 屆舊金山會議		
報告書內容應包含： 一、出國目的 二、考察、訪問過程 三、考察、訪問心得 四、建議意見 五、其他相關事項或資料			
授權聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人：　　（簽章）		

附註

一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

一、出國目的

第七十四屆 IETF 會議於九十八年三月二十二日至九十八年三月二十七日在美國舊金山舉行。此次會議爲期六天，而中心參加之主要目的參與及了解各技術發展 WG 的趨勢及討論方向，包含 DNS、IDN、IPv6..等方向，本次會期 EAI WG 並無議程，與會期間並與 CNNIC 討論 EAI 測試評估 DRAFT 之撰寫及其 KEYWORD BoF 相關事項交換意見。

二、考察、訪問過程

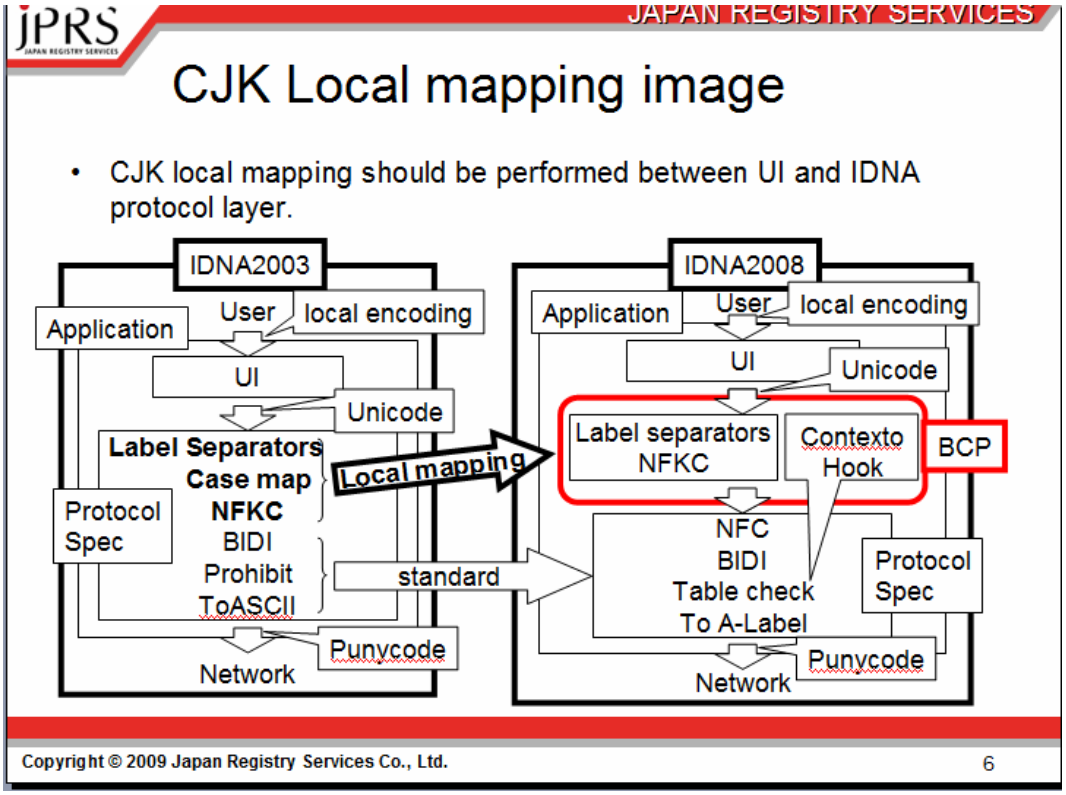
此次會議雖期程共六天，於會期間均於會場飯店參與各 WG

三、考察、訪問心得

以下爲幾個本會期之觀察及說明,供參考:

於 IDNA 的 WG,經與日本 YONEYA 會前討論, 本次會期 CJKT 提供了自身語言版本的 IDNAbis guild line, 針對句號在 CJKT 中的應用，及針對不同的輸入法(繁體中文、簡體中文，日文，韓文 中各種不同的輸入法) 在全形及半形的情況下,所產的句點,將其列出並以 Unicode 列出寫入 Draft,這個會前會即是在確認大家對 Draft 內容,會議上的報告有無其他意見,而溝通已在過去的 Mailing list 上討論過,YONEYA 表示對於 CJKT 來說 LOCAL MAPPING 的重要性,對於 IDNA2008 取消 LOCAL MAPPING 的作法,他強調會造成許多問題,他所提出的問題點包含: Normalization of string(Full width 及 helf width 在使用上的表現)與 Label Separators(分隔符號的使用)及 Quasi Ideographic marks(同形異義)..等,對於 cn 應有影響,但經過討論確認目前.tw 在這三種影響狀況都不存在,而經在場與會人員(CNNIC 人員缺席)的 TWNIC (Abel, Markkao) , JPRS (YONE, FUJIWARE), NIDA (Peter, Kim Do-Won),皆同意由 YONE 在 IDNAbis 會議上報告。之後在 WG 上 YONEYA 也將此狀況提出說明,之後現場討論 IDNA2003v2 及 IDNA2008 之可行性及未來發展方向,會後經與會者共同決議以 IDNA2008 爲發展的目標,但會考慮類似 local mapping 機制,但因爲 idna2008 原設計爲 NON-MAPPING PROTOCOL,但目前顯然已有所修正,後續將持續觀察發展。

下圖,說明 IDNA2003 至 IDNA2008 中所調整的地方及對 CJKT 的影響



在DNSOP WG上討論的主題依然與上次會期一樣是DNSSEC,不過明顯與上此會期之氣氛不同,上次會期與會者多對於DNSSEC的必要性及其安全性表示懷疑,甚至有OPEN MIC時間一連超過40分鐘,大家輪番表達不應朝DNSSEC的方向發展的意見,而這次則是已經開始針對”如何具體實現DNSSEC”爲方向開始討論,這表示,在將來標準齊備及各方面的問題大致解決後,DNSSEC應該是會全面實施的!在WG上針對DNSSEC Key Rollovers的TIMEING及DNS64的議題均有討論。在DNSSEC 64 的 Draft，它指出了目前 DNSSEC 在 IPv4/IPv6 轉換過程中的不足，因爲不足，故存在許多問題或不同的意見。由於本篇目前僅止於初稿狀況。問題存在於 IPv6/IPv4 NAT 在轉換時的對應，其結構會形成 IPv6::IPv4 之對應，由 NAT64 來進行 mapping 對照，可是 DNS 記錄中並沒有這個格式的類別 (TYPE)，而且這個格式來進入 IPv4 網路路要去除 IPv6，或回來時要變成 IPv6，所以在 DNSSEC中要考慮到這些問題的話就有許多記錄要產生，且整個架構的模式目前尚未定案，會議上持不同意見的人各有不同的看法，因時間問題，故最後主席裁示把問題留到 mailing list 上討論，以便大家陳述不同的意見。

DNSOP 有一篇新的 Draft 是關於 DNSSEC key rollover 的,因爲 DNSSEC 中, Key Rollover 時期長將會造成 Zone file 需要兩個 ZSK (Zone Sign Key) ,一個新的、一個舊的。主要因爲 DNS 中的 Cache 因素造成此,而如此的情況,將大量增加 TLD (ccTLD) 等 Zone File Generator 的速度,在這樣的情況下非常不利 DNSSEC 的推展,尤其是愈大的 TLD (ccTLD) 影響就愈大,因爲所花費的時間是成幾何成長的,若是再依一般加密長度的擴展,由 1024bits 成長至 2048bits, 則時間更將無限加長,在這種情況下 (Key Rollover, key size 2048bit),更加不利 DNSSEC 的推展,以目前已知重要的 TLD (com , org…), 皆不在近期內考慮佈建 DNSSEC, 因爲他們 Domain Name 的數量太多,而且用戶分布太廣,在現實上將會等大家都做了他們才會

做。本篇 Draft 還提到了在緊急情況下需要進行 key rollover (Emergency Rollover),但如何進行並沒有沒確的說明,只有陳述在緊急情況下,必需即時進行更新,在更新後應馬上要準備一個新的緊急備用 key. 何謂 DNSSEC 的緊急情況,

[DNSSEC Operational Practices] 的草案則介紹了許多在 DNSSEC 上實作的問題或想法,像 KSK (Key Sign Key) 到底要用多久,如果一年會不會太短,用十年如何 ? 因爲 KSK 的更換工程從 ICANN 到 TLD,到最後的 Zone File,影響層面相當大,但是不做 ZSK/KSK的更新,其實引起的問題更大,也就失去了當初 DNSSEC 標準建立的用意了。另外,文件也提到了,改變 key rollover 演算(間時點,週期,長度等)是必要的,而不能僅固定在一種情況。

draft-bagnulo-behavedns64 個人覺得是一個很重要的 Draft, 主要因應日後 IPv4:IPv6 異質網路的 DNS 查詢應該如何實作,及可能會有什麼問題,目前 IETF 或一些 IPv6 專家普遍公認, Dual Stack/Native/Tunnel Broker 不能解決 IPv4 過渡到 IPv6 的問題,因爲 IPv6 沒有足夠誘因。

在 SIP 相關的 WG 上,比較特別的是針對 RFC4244 此篇的狀況加以討論,因爲此篇 RFC 有不少的問題點,所以在 4244bis 討論得相當熱烈,另外提到 SIP Secure Call ID 衍生的問題解決部份則是討論將以 update RFC3261,並不再使用“localid@host”當產生 call ID 的值時,另外不將 host 的資訊放在 call id 中,並將文中的 ABNF 也換掉,另外也討論到針對 SESSION ID 的必要性及實現方式,不過許多人在 OPEN MIC 時針對增加 SESSION ID 這個欄位是持反對意見的,在 SIP 的討論中常可聽到對於 B2BUA 角色有不少意見,在 SECURITY 方面則有一篇 PRESENTATION” Relay Attacks by Raphael Coeffic”針對 draft-state-sip-relay-attack-00 這篇 draft,在兩天的 sipWG 上有一個小花絮就是對 SIP 之父 Jon Peterson 頒獎,WG 頒發紅酒一瓶,第二天 WG 上又頒一瓶,主席的說法是”因爲昨天頒獎沒拍照,所以今天再頒一次獎” 。

在 IPv6 的相關 WG 中,在 V6 ROUTE 上,Ralph Droms 在『Default Router and Prefix Advertisement Options for DHCPv6』，以『DHCP as a routing protocol』爲主題，說明 Service Provider 網路中，Edge 端的 Provider Router 設備經常使用 DHCP。DHCPv4 會將設定送 DHCPv4 Client，在 IPv6，DHCPv6 的原理同 DHCPv4，但 IPv6 主機需以 ICMPv6 的 Neighbor Discovery，先取得 Default Route 和 Prefix 後再經 DHCPv6 協定取得 IPv6 位址及組態。本篇提到設計兩種格式的 DHCP Option，一爲 Default Router Option，含 Address of the interface for a default router、Source link-layer address for the interface 和 Router lifetime 三個參數。另一種爲 Prefix Information Option，裡面包含 Prefix、Prefix length、Valid lifetime 和 Preferred lifetime 四個參數，Client 首先在 DHCPv6 的 Solicit 或是 Request 的訊息夾帶使用 Option Request Option 裡面包含 Prefix Information

Option Code 和 Default Router Option Code，Server 經由 Advertise 或是 Reply 的訊息回傳 Client 索取的相關參數，那麼擁有 DHCPv6 Client 的主機由可以如同 DHCPv4 一樣，獲取完整的設定。

在 v6ps WG 上,Tim Chown 之『Rogue IPv6 Router Advertisement Problem Statement』，討論 Router Advertisement 所造成的資安議題，1.網路管理員的網路部署有誤。Ex.Router Lifetime 誤設成零或 Layer 2 VLAN 設定錯誤，讓 Router Advertisement 散佈至其他網段，2.使用者的無意的錯誤設定。3.駭客的蓄意破壞。駭客在區域網路上，讓 rouge 可以達成 Denial of Service 或是 Man in the Middle 的破壞目的,在防範措施方面有 7 點做法:1.IPv6 節點關閉 Stateless Address Autoconfiguration 或是忽略 Router Advertisement 封包，讓 v6 位址和組態使用 menual 的方式設定。2.從 Layers 2 的 Switch 上面防範，Switch 上面開啓『Router Advertisement Snooping』的功能，類似 DHCP Snooping 方式，利用 Layer 2 的機器查驗 Layer 3 以上的封包內容。3.在 Access Control Lists (簡稱 ACL) 的 Switch 上面，防範使用者的 Port 無意或蓄意傳送 RA。4.使用 RFC 3971 中的 Secure Neighbor Discovery (簡稱 SeND)，讓 host 可以驗證來自同網段中 Router 傳送 Router Advertisement 的合法性。5.以 RFC4191 設計 Router Advertisement 所制訂的 router preference option，6.搭配 IEEE 802.1x 的認證機制，僅讓通過認證的 IPv6 節點傳送與接收封包。7.建議使用者架設 IPv6 防火牆，設定 IPv6 Host 只接受在信任名單中的 RA。Rouge Router Advertisement 在 IPv6 資訊安全上是一個很重要的議題，需多加注意。

另外在IPv6 Address Independence (6AI)的BoF上,也經與會者大家的決議,將不以NAT66爲未來發展方向,而維持在NAT64的使用。以下爲幾點討論內容:

1. Symmetric (對稱) NAT Support Extension，以新的 port 爲 NAT 溝通的手段，所有的 Connection 皆會使用到這個 port pool。
2. UPnP-Enabled Symmetric NAT Extension，以即插即用的概念來設計 NAT，所以上線的設備在發起連線時，先向 NAT 取得要用的 ip/port，Client 以此資訊來發送資料，而 Server 端則回應至 NAT，由 NAT 取得內部對應後，導入內部的 Client。
3. Port-Preserving Symmetric NAT Extension，以保護 Port 的方式的 NAT，即是現行的 NAT 模式，在 session 未結束前，NAT 上的這個 port 皆不能再被使用，並自動以這個 port 去對應內部主機。
4. Hairpinning Extension，原路返迴的 NAT，因爲封包在傳送過程中，每次或每個封包的路徑可能有所不同，而此 model 在確保這個路由可以保證去回皆相同，唯有相同的情況，NAT 才能發揮對應的功能及了解連線狀況。
5. Server Load Reduction Extension，以 Server 的角度來思考，直接記錄每個訊息，所有的連線直接以 End to End 的方式來進行。

此外也參加了 YAM(Yet Another Mail)的 BoF,在討論上主要是針對 IETF 的 IESG 的一些現行做法,提出質疑,並對一些主席列出的 mail 相關的 RFC,預計以將這些表列的 RFC 推成爲 STANDARD TRACK 爲目標,另外 HTTPbis 的 BoF 則是針對 HTTP1.1 的改版,進行鋪路,後續也值得加以觀察。

另外也與 CNNIC 與會人員討論 EAI 測試評估 DRAFT 之撰寫之合作部份,另外則針對 CNNIC 預計下次會期要進行 KEYWORD BoF 的相關事項加以討論。

四、建議意見

1. EAI WG 的實作各 NIC 皆未涉及 DSN/POP/IMAP，中心的 test-bed 可考慮此部份之實作。
2. 建議針對 DNSSEC 的佈建宜密切了解 IETF 後續之發展情形。
3. IPv6 於目前 IETF 討論議題中佔相當大的比重，建議相關人員參與 IETF 以深入了解國際間 IPv6 及相關技術之發展趨勢。

五、其他相關事項或資料

有關第**七十四**次 IETF 會議議程及相關會議資料請參考(Agenda/ Session/ Presentations)：

https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=74