行政院及所屬各機關出國報告

（出國類別：其它－國際會議）

出席「亞太國際學術網路年會 APRICOT 2006 會議」報告

服務機關：教育部（電算中心）

姓名職稱：李長樹 組長

派赴國家：澳洲

出國期間：95 年 2 月 28 日 至 3 月 3 日

報告日期：95 年 6 月 2 日

系統識別號：C09501242
行政院及所屬各機關出國報告提要
頁數：49
含附件：是

報告名稱：

亞太國際學術網路 2006 年年會（APRICOT 2006 Conference）

主辦機關：

教育部

聯絡人／電話：

黃茂全／23566375

出國人員／電話：

李長樹　教育部　電算中心　組長 ／ 87329084

出國類別：其它
出國地點：澳洲
出國期間：民國 95 年 2 月 28 日 - 民國 95 年 3 月 3 日
報告日期：民國 95 年 6 月 2 日
分類號／目：I8／資訊科學
關鍵詞：APRICOT2006

內容摘要：

APRICOT 是 Asia-Pacific Region Internet Conference of Technology 的縮寫，是亞太區域重要的網際網路會議之一，每年春季在亞太地區各國輪流舉行。此會議提供亞太地區國家相互了解網路環境與進行網際網路社群交流之平台；促進亞太地區國家網路合作；同時提供世界各國參與亞太地區網際網路活動之入口。亞太地區各個國家之網際網路社群均相當重視此一會議，各國網際網路社群無不爭取此一會議回國主辦。主辦之國家除可以促進本國網際網路活動及對外交流外，對於提升國家網際網路形象，及促進對外交流也有相當大之助益。

每次會議均邀請世界各國網際網路先進與業者分享他們寶貴的經驗，世界各國人士也會依據不同角度提供亞太地區網路發展與合作建議；並討論過去一年重要的網際網路相關議題，探討未來一年新興的技術及應用。今年的 APRICOT 會議主題有 Peering Track、SPAM、Routing and Operations、Security、IPv6 等主題。Peering Track 主題討論世界各地網際網路互聯現況及 Peering 的運作趨勢；SPAM 主題討論目前 SPAM 之威脅及相關防範之最新技術； Routing and Operations 主題探討各種骨幹路由運作技術與趨勢，包含高速頻寬對路由運作之挑戰及 BGP 實務運作經驗交流等；Security 主題則是因應網路應用探討相關網路安全與防範； IPv6 主題是延續近年來 IPv6 實作與應用的討論，提供各國對 IPv6 環境建置之經驗交流，並於會場舉辦 IPv6 Summit。

本文電子檔已上傳至出國報告資訊網

目　次

出席「亞太國際學術網路年會 APRICOT 2006 會議」心得報告

一、 會議基本資料

會議名稱：亞太國際學術網路年會 APRICOT 2006 會議

時間：95 年 3 月 1 日 至 95 年 3 月 2 日

地點：澳洲

參加國家人員：亞太地區各國網際網路相關組織及人士

二、 會議目的

APRICOT（Asia-Pacific Region Internet Conference of Technology）會議是由 APNIC（Asia Pacific Network Information Center）所贊助發起，第一屆的會議於 1996 年在新加坡召開，爾後定期每年二或三月於亞太地區各國爭取主辦，會議中的主題以網路實作應用技術爲主，網路發展趨勢與策略方向爲輔；同時也有亞太區域特有的網路相關運作議題。APRICOT 會議近年來每次與會人數均達六百人以上、參與的國家含括亞太區域三十多個國家，是亞太區域最大的網際網路會議，與會人員含括各國 ISP 網路相關技術人員與主管、跨國的網路設備與電路供應商、網路相關的管理及策略制定組織、及少部分政府與學界人士等。APRICOT 的最主要目的是希望藉由會議中對議題的討論，讓亞太地區的網際網路相關人員做經驗分享、交流，並藉此互相學習、溝通，促進亞太國家的網路交流與技術，間接引導各國政府與民間發展與制定網路相關策略。

2002 年 9 月 APRICOT Executive Committee 與 APIA Board 協議將

APRICOT 與 APIA 相關活動作密切的結合，2003 年起 APIA（Asia & Pacific Internet Association）成爲 APRICOT 的法定支援運作單位，APRICOT 便成爲 APIA 最主要的活動，APIA 則負責 APRICOT 未來的運作與成長。每年舉辦 APRICOT 的同時也一併舉辦亞太區域網際網路相關會議，如：APNIC（Asia Pacific Network Information Center）年會、APNG（Asia Pacific Networking Group）會議等等。

國內出席參與 APRICOT 會議的單位除了教育部外還有：財團法人台灣網路資訊中心（TWNIC）、中華電信股份有限公司（HiNet）等等，代表出席的都是各單位主要技術人員、主管或策略制定者。我國代表出席者也透過 APRICOT 會議與亞太地區各國做技術合作交流、討論，並可藉此會議期間參與 APNIC 舉辦的活動並給予建議，促進我國與亞太地區網際網路合作與發展。

三、 APRICOT 2006 Conference 會議資訊

APRICOT 2006 是由 WAIA（Western Australian Internet Association）所主辦的，目前已是亞太區域網際網路研討會中最具歷史及規模的會議。除可透過此會議觀摩、學習亞太區域各國 Internet 之發展經驗及技術外，此會議並希望可以透過此一會議讓亞太區域國家能夠同步提昇網際網路技術與經驗。

本次為 APRICOT 第 11 次之會議，於 3 月 1 日至 3 月 2 日在澳洲伯斯會議暨展覽中心（Perth Convention and Exhibition Centre）舉行。今年有來自 30 多個國家，超過 600 人與會。本次研討會的主題除了近年來亞太地區持續積極發展的 IPv6 應用技術外，還有 Peering Track、SPAM、Routing and Operations、Security 等主題。Peering Track 主題介紹澳洲 Peering 的現況，並探討各 ISP 互連時之網路維運中心之溝通與問題解決機制，並藉此機會討論亞太地區各國網際網路交換中心之發展現況與發展限制。SPAM 主題則討論網際網路廣告信最新防範技術及 Botnet 行為模式及防制技術。Routing and Operations 主題內包含了 IPv6 與 IPv4 共同運作的相關路由與運作問題；BGP（Border Gateway Protocol）收斂的相關議題；及 Peer-to-peer 這類流量對骨幹網路運作造成的衝擊等等。Security 主題則討論網際網路維運者，在處理跨網路領域問題時的溝通協調機制等。

相關資訊已在網站上公佈：http://www.2006.apricot.net/ 或 http://www.apricot.net/。

四、 會議過程（**Program Schedule**）及內容

（一）議程：詳細資料請參考附錄

Wednesday, 1 March

09:00 ~ 10:30 Opening Plenary Session

11:00 ~ 12:30 Concurrent Sessions (Peering Track、SPAM、Addressing & Renumbering、Routing/Operations、APNIC Database SIG、APNIC IPv6 SIG)

14:00 ~ 15:30 Concurrent Sessions (Peering Track、SPAM、Access、Routing/Operations、APNIC NIR SIG、APNIC Routing SIG)

16:00 ~ 17:30 Concurrent Sessions (Peering Track、SPAM、Wireless Network、Routing/Operations、APNIC Routing SIG、)

Thursday, 2 March

09:00 ~ 10:30 Concurrent Sessions (DNS、IAB IPv6 Multihoming Panel、Network Analysis Tools、Routing/Operations、APNIC Policy SIG)

11:00 ~ 12:30 Concurrent Sessions (VoIP、IAB IPv6 Multihoming Panel、Routing/Operations、Security、APNIC Policy SIG)

14:00 ~ 15:30 Concurrent Sessions (Content Track、Routing/Operations、Security、APNIC IX SIG、IPv6 Summit 2006)

16:00 ~ 17:30 Concurrent Sessions (Content Track、Routing/Operations、Security、APNIC DNS Operation SIG、APNIC IX SIG、IPv6 Summit 2006)

（二）大會專題座談會（Plenary Panel）：分別提出網際網路路由安全之增進方法；及分析探討網際網路的整合（Convergence）趨勢。

網際網路路由安全之增進方法由 BBN 的 Dr. Stephen T. Kent 教授提出，網際網路路由交換安全方法主要著重於自治區（Autonomous System）之間的路由交換，因爲自治區內的路由環境是由一個公司或組織可以掌控的環境，但是自治區之間的路由交換就需要參與路由交換雙方互相信任及協調後才能達成，所以自治區之間的路由交換就需要再加入一些認證查核機制，以確保該自治區交換給另一自治區的路由是經過認可的、是可以交換這些特定的路由資訊的。Dr. Stephen 提出了一種 PKI 設計可以達到上述的路由安全交換目的，這個設計利用了 RFC 3779 中定義的擴充認證方式表達 IP 區塊及 Autonomous System Number，並且同時比較現行管理這些資源的單位（如：RIRs，LIRs/NIRs，及 ISPs）中的組織架構，這個方式不需要依賴新的認證欄位，也不像傳統的 PKI 需要發送憑證給資源使用者，而是透過查證 ROAs（Route Origination Authorizations）來達到目的。

分析探討網際網路的整合（Convergence）趨勢問題的是 APNIC 的資深研究科學家 Geoff Huston，Convergence 一直是資訊通訊產業中一直備受討論的話題，最近因爲聲音、影像及資料傳輸的整合，讓人們又不斷地討論 IP 將是這 3 類傳輸的整合服務提供者。Convergence 就是利用一個網路平台提供多樣化的服務需求，Convergence 便可以使成本支出降低、增加網路價值、增強服務需求控制、並有極高的邊際效應。在這個趨勢分析演講與討論中，Geoff Huston 利用收集數年的資料，證實這些想要整合網際網路服務的業者目前都是虧損連連，真正能夠讓網路環境發揮效益從中獲益的公

司，都是儘可能單純化網路環境讓網路負載保持最低，憑藉單純網路環境創造出的單一特殊化附加價值才是效益最大的。

（三）研討會內容分爲 12 個主題

1. 網際網路互聯（Peering Track）
2. 垃圾郵件議題（SPAM）
3. 網際網路位址及重分配（Addressing & Renumbering）
4. 接取網路議題（Access）
5. 無線網路議題（Wireless Networks）
6. 網域名稱主機議題（DNS）
7. 網路電話議題（VoIP）
8. 第六代網際網路協定相關議題（IPv6）
9. 網路分析工具（Network Analysis Tools）
10. 網路內容（Content Track）
11. 網路路由及運作議題（Routing/Operations）
12. 網路安全議題（Security）

依各項分類分別說明如下：

1. 網際網路互聯（Peering Track），分成 3 個部份：
   - 回顧過去亞洲網際網路互連的歷史，及澳洲網際網路互連發展的過程，希望能夠藉由這些演進歷程，預測亞太地區網際網路互連發展的方向，並協助亞太地區網際網路互連順利演進。
   - 利用最近網際網路互連社群及網際網路互連的相關研究，探討網際網路內容業者（ICP）的互連型態與觀點；一般網際網路服務提供者（ISP）互連評估模式之合理性；並希望藉此討論機會促成亞太地區更多網際網路互連與合作。
   - 網際網路互連模擬運作探討，這個部份利用網際網路互連模擬軟體

讓與會者及講者進行高度互動，藉此模擬讓每一個與會者有機會更深刻了解網際網路互連的運作及問題。

2. 垃圾郵件議題（Spam），分成 3 個部份：
   - 說明 Botnet（一種被遙控的電腦網路）的運作、目的、危險性、及如何防範等問題，目前所知很多亞洲區域國家的電腦系統因爲管理及保護不善，大量被搖控供做多種不當用途，希望藉此一議題的討論及說明，讓與會各界重視此一問題，並能藉此促進跨國合作防範此類之事件。
   - 開放討論防治 SPAM 黑名單之相關策略，藉此討論讓網際網路服務提供者能彼此交流防治 SPAM 的經驗。
   - 探討現在及未來的 SPAM 過濾工具及技術，包含非自我學習型（特徵法、黑名單法、流量分析法等）及自我學習型（向量分析計算、向量模式、樣態學習法等）的 2 種工具，藉此讓與會人士更熟析這些工具的優缺點。
3. 網際網路位址及重分配（Addressing & Renumbering）：
   - 分析探討 IPv4 不足使用的現況及後續影響，並分析網路位址用盡後對產業界的可能影響。
   - 討論如何有效利用 IPv4 有限的位址達到最有效率使用的目的，另外探討因應 IPv4 位置不足狀況，如何設計規劃網路環境之問題。
4. 接取網路議題（Access）：
   - 討論 Metro Ethernet 的發展趨勢與優缺點；DSL 類的接取網路應用經驗交流；及語音、影像、資料傳輸在接取網路環境中面對的挑戰與解決方法等。
5. 無線網路議題（Wireless Networks）：
   - 討論無線網路建置與發展的關鍵技術，並針對 ISP 提供的無線網路環境與行動電話網路結合運用的相關議題。

6. 網域名稱主機議題（DNS）：

- DNS 爲網際網路各項應用的基本服務，DNS 的存在與正常運作將對人們使用網際網路有著很重要的意義，故此議題討論 DNS 運作安全的問題，及最佳的 DNS Anycast 的建置服務環境等。

7. 網路電話議題（VoIP）：

- 說明 SIP-IX 建構的技術與應用功能；利用 VoIP 建立 ISP 之間的溝通熱線，以利及時解決網路問題；另有紐西蘭人士說明建構 VoIP 之經驗，並提供紐西蘭建構 VoIP 環境的優劣分析。

8. 第六代網際網路協定相關議題（IPv6）：

- 延續近幾年來的 IPv6 技術探討，內容包含日本 IPv6 發展現況說明；日本 IPv6 網路交換中心之運作概況；韓國的 IPv6 DNS 建置經驗；最重要的是希望與會人士分享彼此的 IPv6 環境建置經驗。

9. 網路分析工具（Network Analysis Tools）：

- 分享利用 Shell Script 及 Perl 自行製作網路管理工具之經驗。

10. 網路內容（Content Track）：

- 澳洲的網際網路內容過濾經驗分享，透過國家政策引導澳洲訂定網路內容分級標示，以便於網路內容過濾之施行。
- 內容交換器及應用最佳化技術設計適當資料中心之經驗交流。

11. 網路路由及運作議題（Routing/Operations）：

- Peer-to-peer（P2P）服務控制技術探討，分別提出 2 種作法因應 P2P 流量的挑戰，第一種方式爲：深入封包檢查後，利用收費及控制流量機制導引網路頻寬公平使用。另一種方式爲：P2P 快取，引導 P2P 流量優先由自治區內部取得資源，以避免聯外頻寬的耗費。
- 分享網路路由交換之研究成果，以便於路由資料之監控與掌握。

12. 網路安全議題（Security）：

- 提出 ISP 網路安全管理之日常工作內容，並藉此說明 ISP 處理網路

安全議題時的重點任務，並希望藉此交流機會提升 ISP 處理資訊安全問題時能更得心應手。

（四）實際應用展示會內容（Demo Exhibition）：新的網路技術產品與相關實作展示。主要參展單位包含 Juniper、Cisco、Alcatel、Packet Design 等本次會議主要贊助的設備製造商及網路服務廠商等，內容包括各家廠商新型設備與技術，網路流量分析管理軟體展示，網路相關服務展示說明等等。

五、 會議心得

（一）APRICOT 是非官方式的會議活動，而 APRICOT 會議最重要目的之一就是希望透過非正式官方的交流互動，屏除國家的界限促進亞太地區的網際網路現況交流，促使各國均衡發展網際網路環境，間接促成亞太地區網際網路合作及互連等等。亞太地區的網際網路發展因各國經濟狀況不同而有不同的發展，藉由此次會議觀察發現：日本、韓國、澳洲、新加坡及我國是亞太地區網際網路發展較爲領先且自由的國家，中國近年來急起直追上述 5 個國家，不論在軟體技術的研發、硬體設備發展等方面都已經逼近這 5 國，甚至在部分領域的實作與技術已超越這所有亞太地區國家，但是中國的網路自由度仍是遠遠落後的，因此也限制了中國網際網路的創造與發展，我國在網路自由度的優勢是中國在短期內無法超越的，我國應該妥善利用此一優勢，正面看待我國任何網際網路上的創新與創意，並適當鼓勵國人進行網路創作與創新應用。

（二）網路互連（Peering）是網際網路運作的關鍵活動之一，透過 ISP 的網路互連才能達到今天的網際網路規模與環境，APRICOT 議程訂定時特別考量網路互連的重要性，因此連續幾年 Peering 都是 APRICOT 會議中的主要議程之一，也因爲亞太地區國家之間大多數以海相隔，Peering 的成本遠高於歐美國家，也提高了亞太地區各國網際網路互連與合作的門檻，APRICOT 有鑑於此每年均提供相關問題討論議程，並安排相當多的時間供各國網際網路業者組織互相交流與瞭解困難。國內的網際網路環境發展趨於成熟，國內組織與業者間的 Peering 運作約與歐美國家之模式相當，但是跨國的 Peering 礙於海纜成本過高，如何克服此一門檻？我國仍有相當大的努力空間。

（三）IPv6 發展近幾年來在亞太及歐洲地區進展最快也較重視，但是一直缺乏適當的推廣應用環境是相當大的致命傷，這次會議中美國的 Comcast 公司在規劃該公司有線電視系統網路化需求時，發現 IPv4 的定址根本無法符合需求，只能轉用 IPv6 的定址方式，同時也因爲此一需求已達到經濟規模，硬體設備廠商也願意投資開發相關軟硬體供 Comcast 使用。國內開始大力推動 IPv6 應用發展也已超過 4 年，但是因爲缺乏類似 Comcast 這類的需求，導致實際應用需求仍非常低。

（四）SPAM 的問題困擾各網際網路業者與組織已經接近 10 年，最近更因爲網路遠端控制攻擊（Botnet）、網路釣魚（Phishing）等嚴重的資訊安全問題均透過 SPAM 方式滲透至各個組織、業者、與個人電腦造成各界嚴重損害，所以目前 SPAM 的防治工作亦爲資訊安全重點工作之一，資訊安全工作亦需要評估納入 SPAM 防制，以避免 SPAM 之滲透危害資訊安全。

六、 對於未來國內的網路發展建議事項

IPv6 此一網路定址技術已經制訂完成約 12 年了，但是截至目前爲止因爲 IPv4 網路位置使用因緊縮控制得宜，及 NAT 等相關技術發展之故，仍未到達先前預期的 IPv4 位址大量不足的地步，而這次會議中 Comcast 說明因應未來該公司有線電視系統網路化需求時，大幅調整了原有之有線電視系統使之網路化，但因爲用戶數過多之影響，該公司的網路位址需求突然因此而暴增，IPv4 已無法滿足該公司的需求，將因此朝向使用 IPv6 來做所有用戶的網路定址，此一事件正說明了 IPv6 不一定得取代原有 IPv4 的環境，IPv6 可以用於一些特殊環境與需求中。目前國內 IPv6 相關計畫的主要方向是將 IPv6 視爲 IPv4 的取代者，而非優先將 IPv6 應用於特定之環境與需求，國內此一推動方向恐無法將 IPv6 應用於適當的場所，間接也壓縮了國內 IPv6 技術發展，若能重點式朝向配合特殊需求及特定應用面推展 IPv6，可能可以促進國內 IPv6 應用發展並提升國內 IPv6 相關技術。

資訊安全問題是近年來深深困擾各個資訊環境與組織的最重要問題之一，國內的網際網路應用發展約與歐美國家同步，國內網路發展歷程中的最初也最重要的莫過於各級學校資訊化相關措施，國內資訊安全的推動目前也是選擇教育體系優先進行推動，一般來說教育體系的教師與職員接收資訊化程度相當高、執行能力優良、訊息傳達管道通暢，學齡兒童及青少年的吸收能力也最強。目前教育體系上網人口約佔國內總人口 20%，若能提供適當協助予教育體系優先執行資訊安全推動工作，讓所有國民從小建立資訊安全觀念，讓教育體系全面實施資訊安全工作，對全國資訊安全推動將有莫大的助益，將來更可以將資訊安全落實到各個層面。

七、 研討會的相關資料

研討會的相關詳細資料於下列網頁中

http://www.apricot2006.net/index.php/fuseaction/home.program

八、 附錄

會議議程與內容相關資料：

ABOUT APRICOT

- Background and Mission of APRICOT
- Structure of APRICOT

Background and Mission of APRICOT

Throughout Asia and the Pacific Rim, Internet service providers, backbone and regional networks, web hosting facilities, firewalls, and Intranets are being created, deployed, and installed at a staggering pace. The technicians, managers, entrepeneurs and decision-makers responsible are under tremendous pressure to master the skills necessary to build and operate these increasingly complex systems.

The mission of the Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) is to provide a forum for those key Internet builders in the region to learn from their peers and other leaders in the Internet community from around the world.

Held annually, the ten day long summit consists of seminars, workshops, tutorials, conference sessions, birds-of-a-feather (BOFs), and other forums all with the goal of spreading and sharing the knowledge required to operate the Internet within the Asia Pacific region.

In an attempt to ease the travel burden on attendees, APRICOT is held in conjunction with one of the Asia Pacific Network Information Center's (APNIC) two annual meetings, the winter Asia Pacific Networking Group (APNG) meeting, and meetings of other Asia Pacific Internet organisations.

Wherever possible, APRICOT also attempts to derive synergy by having the meetings close to or back-to-back with other Internet events such as Asia Internet World, ICANN etc.

- **APRICOT's** mission is to develop and advance the skills and understanding necessary to grow a robust Internet infrastructure in the Asia-Pacific region. APRICOT is about bringing the world's top Internet experts together with those who can most benefit from their knowledge.
- **APRICOT** attendees are the key builders of Asia's Internet. Many of the world's best Internet engineers attend APRICOT either to teach, present or do their own human networking.
- **APRICOT** provides its sponsors the chance to participate in a quality, content-rich event with excellent opportunities to target their products and services at the decision-makers in the Asia Pacific Internet community.
- **APRICOT's** primary goal is to provide a vehicle for the transfer of technology and techniques to the Asia and Pacific Rim region. As such, our attendance fees are set below those of the more promotionally orientated conferences and in fact are set to match the fees found at many similar Internet Operator Group meetings.
- **APRICOT** is an activity supported by various Asia Pacific Internet organisations as well as numerous individuals who give freely of their time and talent, and is not a commercial profit making venture. Any surplus funds are rolled over to keep attendance fees low at the next APRICOT event and support outreach activities in the less developed areas of the Asia and Pacific region.

APRICOT and APIA

In September 2002, the APRICOT Executive Committee and the APIA Board agreed that APIA and APRICOT should work more closely together. And as from March 2003, APIA became the legal entity supporting the APRICOT conference effort. APRICOT is now APIA's main activity, with the board working with the APRICOT Advisory Committee (formerly the Exco) to ensure the future development and growth of APRICOT.

The revised organisation has the APIA Board responsible for the legal entity which supports APRICOT, with the APRICOT Advisory Committee replacing the function of the Executive Committee, and the APRICOT Management Committee taking on the day to day role of working with the local host on the APRICOT conference organisation and programme. The APIA Board has delegated the APRICOT Secretariat responsibility to PIKOM as from 1st September 2003.

HOST ORGANISATION

Western Australian Internet Association

The Western Australian Internet Association (Inc.) (WAIA) is an organisation that was formed in 1995 to represent the Internet community in Western Australia. At the time of formation, pending regulation and uncertainty meant that collaboration between different businesses in the Internet industry was a necessity.

Since then, WAIA has helped the industry to continue to grow in WA. Leading many vital debates and helping to set policy at different levels, WAIA has been instrumental in providing an innovative range of services to association members.

WAIA's purpose
The Western Australian Internet Association was initially formed to be an authoritative body to represent the Internet community during the formation of new laws surrounding the medium. Today, its purpose is to provide support to all suppliers and users of online services in WA and to assist in the growth of the Internet industry generally.

From the WAIA constitution:
- To support, encourage and advise of the development and use of on-line services and related innovations.
- To establish links with similar organisations.
- To support and protect the status, reputation and interests of IAPs.
- To decide all questions of professional practice and conduct by IAPs.
- To support, encourage and advise on the establishment of similar organisations in other States.
- To assist the expansion of Internet usage within Western Australia and to promote informed discussion in all matters affecting the Internet, as the Association sees fit.

WAIA run the Western Australian Internet eXchange, the largest Internet Exchange in Australia.

VENUE

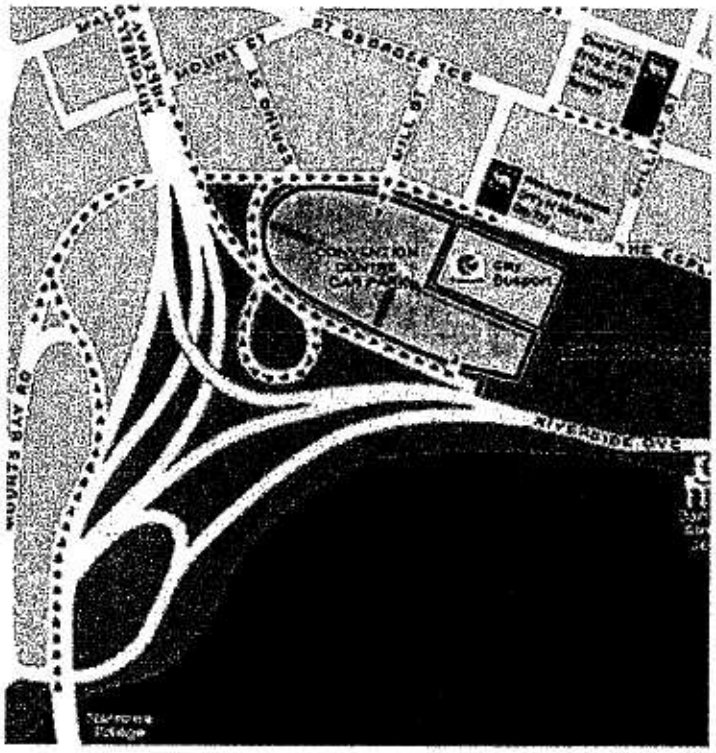
Perth Convention and Exhibition Centre (PCEC)

PERTH CONVENTION EXHIBITION CENTRE
WESTERN AUSTRALIA

The Perth Convention and Exhibition Centre, located in the heart of Perth's central business district, can cater for up to 5,000 delegates. The state-of-the-art, three-level venue is Western Australia's only purpose-built convention, exhibition and meeting venue. The PCEC is within walking distance of most major hotels, and a range of public transport options are available. The 300-metre long, floor-to-ceiling glass foyer, across all three levels, features expansive pre-function and foyer areas providing panoramic city and Swan River views.

The venue is easily accessible by car and public transport, being well positioned close to train & bus routes and is located on the Bus Port site on Mounts Bay Road, the venue also offers parking onsite, directly beneath the venue.

How to get there - please refer to the map below:



Driving from the North along Mitchell Freeway: Take the off ramp clearly marked - Convention Centre Parking. This is located adjacent to the Riverside Drive off ramp. Once on the ramp you can choose to follow the signs directly to the Centre's car park entrance or take the right hand loop to Mounts Bay Road. Continue along Mounts Bay Road to the Wilson car park located in the Hilton (open 7 days) or further along in Westralia Square Building (open Mon to Fri only) opposite the Centre.

Driving from the South along Kwinana Freeway: Take the off ramp that feeds onto Mounts Bay Road. On Mounts Bay Road keep to the left hand lane if you wish to use the Wilson car park located in Parmelia Hilton (open 7 days) or the Westralia Square Building (open Mon to Fri only) opposite the Centre. Keep to the right hand lane on Mounts Bay Road if you wish to use the Centre car park.If you intend entering the city from any other direction study the location map below to determine the most suitable way to access parking.

Parking

Perth Convention Exhibition Centre Parking Station: The Perth City Council (PCC) operates the 1,500 bay car parking station underneath the Perth Centre.

For further information and customer inquiries, phone (08) 9464 2844 or email info_city@cityofperth.wa.gov.au

Alternative Parking Options

- **Wilson Parking** Stations located at:
  The Westralia Square Building - (opposite the Perth Centre, entry on Mounts Bay Road) offering 450 bays (open only Mon - Fri).
- **Central Park** - (entry at 152-158 St Georges Terrace) offering 450 bays (open 7 days a week).
- **Parmelia Hilton** - 56 Mounts Bay Rd (open 7 days a week).

Public Transport

Please click on the following link for Public Transport information www.pcecwa.com.au/attendingEvent.cfm

Disabled Access

The Perth Centre has been designed with lift and ramp facilities to all areas for easy and efficient access. Please click on the following link for Disabled Access information www.pcecwa.com.au/attendingEvent.cfm

PROGRAM

Workshops	22 - 26 February 2006
Tutorials	27 - 28 February 2006
Conference	1 - 2 March 2006
APNIC Member Meeting	3 March 2006

Fees & On-line Registration

Date Session details

Wednesday 22 Feb - Sunday 26 Feb — **Workshops**

[L2 / Room 2] **IPv6 Deployment**
Lindqvist, Palet, Upadhaya, Fujii

[L2 / Room 3] **ISP Routing**
Beldona, Jiandani, Alvaran

[L2 / Room 6] **DNS & DNSSEC**
Manning, Ihren, Lewis

[L2 / Room 7] **ISP and NSP Network Security**
Shrestha, Holloway, Trevidi

[L2 / Room 8] **BGP Multihoming**
NG, Rahim, Lim, Smith

Monday 27 Feb — **Full day Tutorials**

[L2 / Room 1] Maximising Your **IP Address Potential**
APNIC

[L2 / Room 4] Integrated **IS-IS** Primer and Infrastructure Routing
Seo Boon NG & Lim Fung (Cisco)

[L2 / Room 5] **MPLS** Deployment Best Practices
Mukhtiar Shaikh, Muhammad Sagheer, Syed Nawaz, Jeff Apcar, Monique Morrow (CISCO)

[L2 / Room 7] **Juniper** Advanced Routing
Damien Holloway (Juniper)

Half day Tutorials

	09:00 - 12:30	14:00 - 17:30
[L2 / Room 2]	**Zebra/Quagga** Routing Suite Anura Abayaratne	**IPv6** Transition and Deployment Salman Asadullah (Cisco)
[L2 / Room 3]	Introduction to **WiMax** and Broadband Access technologies Mohammad Farhad, Richard Pruss	Delivering **Triple Play Services** Over Metro Broadband Network Lim Wong & Richard Pruss (Cisco)
[L2 / Room 6]	**Security in Mobile and Wireless Networks** Ray Hunt (University of Canterbury)	Using **EAP Authentication with RADIUS** and Configuration of Linux Authentication Server Hugh Irvine & Dhruba Bandari

Tuesday 28 Feb — **Full day Tutorials**

[L2 / Room 1] APNIC: Practical introduction to **IPv6**
Jordi Palet Martinez (ConsulinTel)

[L2 / Room 2] **VoIP - Asterisk and SIP** Implementation, Theory, Monitoring and Traffic Engineering
Jonny Martin (CityLink), Ruwen Silva (LinkaCom), Habib Madani (Cisco), Syed Khurram (Cisco)

[L2 / Room 3] **BGP Deployment**, Best Current Practices and Troubleshooting Techniques for Service Providers
Philip Smith (Cisco)

[L2 / Room 7] **Juniper Advanced Routing**
Damien Holloway (Juniper)

Half day Tutorials

	09:00 - 12:30	14:00 - 17:30
[L2 / Room 4]	Best Practice for Security Patch and Vulnerability Management Neal Gemassmer (Patchlink)	Introducing Layer3 VPNs in MPLS Networks Ariff Premji (Juniper)
[L2 / Room 5]	ISP Network Security - Survey of Security Threats and Attack Classification Danny McPherson (ArborNetworks)	Large Scale Denial of Service (DOS) Attack Mitigation Paul Quinn (Cisco)
[L2 / Room 6]	Traffic Engineering in MPLS Networks Harpreet Singh (VSNL)	Netflow, Flow Tools and Flow Analysis Gaurab Raj Upadhaya (PCH)

19:00 for 19:30 - 21:30

APRICOT Opening Reception

Full Day

[L2 / Room 8] APIA & ISOC-AU Joint Forum

Wednesday 1 March

APRICOT 2006 Conference

9:00 - 10:30
APRICOT Plenary:

[Auditorium]
Steve Kent (BBN)
A PKI to Support Improved Internet Routing Security

Geoff Huston (APNIC)
Convergence?

	11:00 - 12:30	14:00 - 15:30	16:00 - 17:30	18:00 - 19:00
[L2 / Room 1-2]	APNIC IPv6 SIG • Highlight: Deprecation of ip6.int	APNIC Routing SIG • Highlight: Routing security	APNIC Routing SIG • Highlight: Real-world use of route analytics technology	
[L2 / Room 3]	APNIC Database SIG • Highlight: Whois data privacy issues in Japan	APNIC NIR SIG • Highlight: NIR updates	APNIC fee structure • Open session to discuss APNIC fee structure	APOPS and ICONS BoF
[L2 / Room 4]	Peering Track • Barry Greene (Cisco): A Historical perspective • Stephen Baxter (Pipe Networks): An Australian Historical Perspective • Mike Hughes (LINX): Best Current Practices in Peer NOC-to-NOC Communications	Peering Track • Brokaw Price (Yahoo): Peering from a Content Provider perspective • William B Norton (Equinix): The Folly of Peering Ratios? • Sylvie LaPerriere (TeleGlobe): International Peering Dynamics	Peering Track • Bill Norton (Equinix) The New Peering Simulation Game v4 • Fumio Terashima (Japan Telecom) Softbank group international IP Peering	Peering Reception
[L2 / Room 5]	SPAM • Dave Crocker (Brandenburg Internetworking): DKIM and email authentication update • Kwan Hee	SPAM • Suresh Ramasubramanian (Outblaze Limited), Richard Cox (Spamhaus.org), Matthew Sullivan (SORBS), Mark Reynolds (Reynolds.Net.Au):	SPAM • Ray Hunt (University of Canterbury): Tightening the Net: A Review of Current and Next Generation Spam Filtering Tools	

	(Kevin) Hong (KISA/KRCERT-CC): "BOTNET Activity & Mitigation"	An open discussion on antispam blocklists, from an operator perspective.	• John Haydon (Australian Communications and Media Authority): Technical initiatives to combat spam	
[L2 / Room 6]	**Addressing & Renumbering**	**Access**	**Wireless Networks**	
	• Geoff Huston: IPv4 Address Exhaustion • Akinori MAEMURA, Masataka MAWATARI, Kiyoteru ISHIHARA: IP Addressing design	• Truman Boyes (Juniper): Broadband Access Networks and Triple Play • Greg Bader (iiNet): DSL deployment lessons learnt • S Khandekar (Alcatel): Design considerations for delivery of Triple Play Services over Access Networks. • Yogesh Jiandani (Cisco): Metro Ethernet	• Dhruba Raj Bhandar (Final Quadrant Solutions): Large hotel wireless network deployment • Matt Kolon (Juniper): Mobile and Wireless Technologies for Service Providers • Richard St Clair (Internet Users Society of Niue): Internet and Wifi Development on a Remote Island	
[Ballroom 1]	**Routing/Operations**	**Routing/Operations**	**Routing/Operations**	**NSP-SEC BOF**
	• Alain Duran (Comcast): IPv6 Deployment in Comcast • Khalid Raza (Cisco): IPv6 IGP/BGP Routing	• Jeff Doyle (Juniper): Transitioning to IPv6: Issues & Mechanisms • Toerless Eckert (Cisco): Multicast v6	• Pradosh Mohapatra: Advanced BGP Convergence Technics • Ariga Seiji (NTT Communications): IPv4&IPv6 Network implementation and operations • Sachin Natu (Redback): Fast Reroute for Triple Play	• Facilitator: Danny McPherson (Arbor)

19:00 for 19:30 - 21:30

APNIC Social Event

Thursday 2 March

APRICOT 2006 Conference

	9:00 - 10:30	11:00 - 12:30	14:00 - 15:30	16:00 - 17:30	18:00 - 19:00
[L2 / Room 1-2]	**APNIC Policy SIG** • Highlight: 4-byte AS numbers	**APNIC Policy SIG**	**APNIC IX SIG** • Highlight: IXP panel discussion	**APNIC IX SIG** • Highlight: Exchange point operational experiences	**PGP Key Signing BoF**
[L2 / Room 3]	**DNS** • Edmon Chung (Afilias): DNSSEC implementation and issues • Bill Woodcock (PCH): DNS Anycast Service Provision Best Practices • Stephane Bortzmeyer: The CODEV-NIC DNS registry software	**VoIP** • Gene Lew: A technical and functional description of the SIP-IX framework that NeuStar is deploying. • Gaurab Raj Upadhaya: "INOC-DBA (Inter-NOC Dial-by-ASN) hotline phone system • Jonny Martin: Current VoIP activities in NZ -		**APNIC DNS operations SIG** • Highlight: improvements and roadmap for registry to DNS production systems	

both constructive and destructive.

[L2 / Room 4]	**IAB IPv6 Multihoming Panel** • **Moderator: David Meyer (IANA)** **Speakers: David Meyer, Lixia Zhang, Kurt Erik Lindqvist** This BOF is designed to be an interactive session covering the IETF's approach to IPv6 multihoming. The BOF outlines the current state of the art, and the IAB is hoping to get feedback on your IPv6 deployments.	**IPv6 Summit 2006** **IPv6 Technical Issues** Download IPv6 Summit Slides • **Chair: Toshi Hosaka (JPNIC)** • **Kato Jun'ya, (NTT): IPv6 Multi-Prefix Services** • **Toshi Hosaka, (JPNIC): IPv6 Metrics** • **Seunghoon Lee, (KRNIC): IPv6 DNS development and deployment in Korea** • **Tomohiro Fujisaki, (NTT): Clear and Present Danger' of IPv6 - IPv6/IPv4 fallback and DNS queries.**	**IPv6 Summit 2006** **IPv6 Activities** • **Chair: Fukushima, (MRI)** • **Fukushima, (MRI): IPv6 Deployment Status in Japan** • **Shuji Inaba (General Manager of Planning and General Affair Department Internet Multifeed Co.): IPv6 in JPNAP** • **Kosuke Ito (IRI Ubitech): Experiences from /43 trails**
[L2 / Room 5]	**Network Analysis Tools** • **Hugh Irvine: A RADIUS server written in Perl** • **Anjali Gajendragadkar: Building custom scripts to manage large scale Campus WAN.** • **Vishal Sharma: A Survey of Recent Advances in Network Planning/TE Tools**	**Content Track** • **Masaru Akai (SoftbankBB Corp): SoftbankBB's Broadband Contents** • **Peter Coroneos (Internet Industry Association, Australia): Content Filtering: a technical legal analysis of Australia's online content.**	**Content Track** • **Kelvin TEOH and HO Hock Jin (National University of Singapore): Art and Science of Building NUS Data Centres** • **Zeeshan Naseh (Cisco Data Center Networking Practice): Content Switching and Application Optimization Technologies and Design Approaches within Data Centers**
[Ballroom 1]	**Routing/Operations** • **Kireeti Kompella (Juniper): Pros and Cons of going unnumbered** • **Teruyuki Hasegawa (KDDI R&D Labs) & Lior Gendel (Cisco): Service Control Technologies for peer-to-peer traffic in next generation**	**Routing/Operations** • **Arman Maghbouleh (Caridant): Peering Planning Cooperation without Revealing Confidential Information** • **Stefano Previdi (Cisco): IPFRR**	**Routing/Operations** • **Olaf Maennel (University of Adelaide): Modelling Inter-Domain Routing** • **Matt Kolon (Juniper): Opportunities for SPs with Enterprise MPLS** • **Jeffrey**	**Routing/Operations** • **Andrew G. Malis (Tellabs): Using Multi-Layer Routing to Provision Services across the MPLS/GMPLS Domain Boundaries** • **Stephan Millet (Telstra): Internet routing**

		networks		Sugimoto (Nortel): Multi-Segment PWs: "A small step for PWs, a giant step for Metro Convergence?"	table analysis • Jian Feng Xu (China Telecom): Metro scalability and Availibility
	[Ballroom 2]	**Security**	**Security**		**Security**
			• Barry Raveendran Greene: Guest: PCH - INOC Phone Demonstration.	• Peter Schoenmaker (NTT Verio): A Day in the Security Life of a Security Professional.	• Vishal Sharma: Case Study - Network Infrastructure in Cellular Data Networks: An Initial Investigation • Slides: download

19:00 for 19:30 - 20:30

APRICOT Closing Event

Friday 3 March

APRICOT 2006 Conference 9:00 - 17:30

APNIC Member Meeting

19:00 for 19:30 - 21:30

APNIC 21 informal closing dinner

PROGRAM

Workshops

**All workshops run for 5 days (22 - 26 Feb 2005).
Full 5-day attendance is required.**

ISP Routing
Instructors: Srinath Beldona (Cisco), Yogesh Jiandani (Cisco), Amante Alvaren (APNIC)

BGP Multihoming
Instructors: Vincent Ng, Abdul Rahim, Lim Fung (all Cisco)

IPv6 Deployment
Instructors: Kurtis Lindqvist (Netnod), Jordi Palet Martinez (Consulintel), Gaurab Raj Upadhaya (PCH), Miwa Fujii (APNIC)

DNS & DNSSEC
Instructors: Bill Manning (EP.net), Johan Ihren (Autonomica), Ed Lewis (Neustar)

ISP and NSP Network Security
Instructors: Vicky Shrestha (World Link), Damien Halloway (Juniper), Kunjal Trivedi (Cisco)

Tutorials

Monday 27 February

Juniper Advanced Routing
Instructors: Damien Holloway (Juniper)
Level: Intermediate

Best Practice Guidelines for Deploying MPLS
Instructors: Mukhtiar Shaikh, Muhammad Sagheer, Syed Nawaz, Jeff Apcar,
Level: Intermediate

Introduction to WiMax and Broadband Access technologies
Instructors: Mohammad Farhad
Level: Intermediate

Delivering Triple Play Services Over Metro Broadband Network
Instructors: Lim Wong, Richard Pruss (Cisco)
Level: Intermediate

Security in Mobile and Wireless Networks
Instructors: Ray Hunt (University of Canterbury, NZ)
Level: Intermediate

Using EAP Authentication with RADIUS and Configuration of Linux Auth
Instructors: Hugh Irvine, Dhruba Raj Bhandari
Level: Intermediate

Integrated IS-IS Primer and Infrastructure Routing
Instructors: Seo Boon Ng, Lim Fung
Level: Intermediate

Zebra/Quagga Routing Suite
Instructors: Anura Abayaratne (iee.org)
Level: Advanced

IPv6 Transition and Deployment
Instructors: Salman Asadullah
Level: Intermediate

Maximising Your IP Address Potential
Instructors: APNIC staff

Tuesday 28 February

Introducing Layer3 VPNs in MPLS Networks
Instructors: Ariff Premji
Level: Intermediate

Integrated IS-IS Primer and Infrastructure Routing
Instructors: Seo Boon Ng, Lim Fung
Level: Intermediate

Traffic Engineering in MPLS Networks
Instructors: Harpreet Singh
Level: Advanced

Netflow, Flow Tools and Flow Analysis
Instructors: Gaurab Upadhaya
Level: Intermediate

BGP Deployment, Best Current Practices and Troubleshooting Techniqu
Instructors: Philip Smith (Cisco)
Level: Introductory

VoIP - Asterisk and SIP Implementation, Theory, Monitoring and Traffic F
Instructors: Jonny Martin, Ruwan Silva, Habib Madani, Syed Khurram
Level: Intermediate

ISP Network Security - Survey of Security Threats and Attack Classificati
Instructors: Danny McPherson, Ray Hunt
Level: Intermediate

Large Scale Denial of Service (DOS) Attack Mitigation

Instructors: Paul Quinn and Darrel Lewis
Level: Intermediate

Best Practice for Security Patch and Vulnerability Management
Instructors: Neal Gemassmer
Level: Introductory

Juniper Advanced Routing
Instructors: Damien Holloway (Juniper)
Level: Intermediate

APNIC: Practical Introduction to IPv6
Instructors: Jordi Palet Martinez, Tomohiro Fujisaki (NTT), Amante Alvaran (

PROGRAM

PLEASE NOTE: All workshops run for 5 days (22 - 26 Feb 2005). Full 5-day attendance is required.

ISP Routing
Instructors: Srinath Beldona and Yogesh Jiandani (Cisco), Amante Alvaran (APNIC)

Class Size: 28
Download slides here - 11M tar.gz

Attendees must bring a laptop computer

Who should attend: This is a technical workshop, made up of lectures and hands-on lab work. Open to technical staff who are now or soon will be building or operating a wide area TCP/IP base Internet Service Provider (ISP) network or Internet eXchange Point (IXP), likely with international and/or multi-provider connectivity.

Pre-requisites: Cisco IOS Fundamentals; user level UNIX and maybe some system administration; some use of network design, preferably TCP/IP-based.

What you will learn:

- Techniques for design, set-up, and operation of a metropolitan, regional, or national ISP backbone network. This includes advanced OSPF, BGP4, and policy based routing configurations.

- IOS Essentials every ISP should be doing. The hidden secrets that all key NSPs have been using for years, but not telling anyone (i.e. competitive advantage).

- Techniques for the design, set-up, and operation of Internet Exchange Points.

- Techniques for multiple connections to the Internet (multihoming), including connections to IXPs and ISPs.

- Techniques to achieve optimal performance and configuration from a Cisco backbone router. This includes routing scalability, network design, and configuration tips.

Technologies Covered: OSPF and OSPF areas, iBGP, eBGP, BGP Scaling, BGP Policies, Route Reflectors, BGP Best Practices, BGP Configuration Essentials, Policy Routing, IXP Design.

[Top]

BGP Multihoming
Instructors: Vincent Ng, Abdul Rahim, Lim Fung (all Cisco)

Class Size: 28
Download slides here - 15M tar.gz

Attendees must bring a laptop computer

Who should attend: This is a technical workshop, made up of lectures and hands-on lab work. Open to technical staff who are operating a wide area TCP/IP base Internet Service Provider (ISP) network or Internet eXchange Point (IXP), likely with international and/or multi-provider connectivity.

Pre-requisites: Cisco IOS Fundamentals; user level UNIX and maybe some system administration; some use of network design, preferably TCP/IP-based; knowledge of OSPF and of BGP. Ideally all attendees will have in the past completed the APRICOT Routing Workshop.

What you will learn:

- Techniques for design, set-up, and operation of a metropolitan, regional, or national ISP backbone network. This includes advanced BGP4 and complex network configurations.

- Techniques for the design, set-up, and operation of Internet Exchange Points.

- Techniques for multiple connections to the Internet (multihoming), including connections to IXPs, other ISPs and to Internet Transit providers.

- Techniques to achieve optimal performance and configuration from a Cisco backbone router. This includes routing scalability, network design, and configuration tips.

Technologies Covered: Refresher on OSPF and iBGP; eBGP, BGP Scaling, BGP Multihoming Techniques, BGP Transit, BGP Best Practices, BGP Communities, Advanced IXP Design.

[Top]

IPv6 Deployment
Instructors: Kurtis Lindqvist (Netnod), Jordi Palet Martinez (Consulintel), Gaurab Raj Upadhaya (PCH), Miwa Fujii (APNIC)
Slides: download

Class Size: maximum 28

Attendees with laptops are desirable.

Intended Audience: Engineers and operational staffs at ISPs and large networks including academic networks who are planning to use IPv6 either as research or into production networks. Anyone who wants to learn how IPv6 works in practice can also attend.

Pre-Requisites: Good knowledge of IPv4 addressing, network operations as well as knowledge of DNS, Routing with both IGP and BGP. It is important that students have good prior knowledge of operations in IPv4 in order for them to attend this workshop.

Topics Covered:

The workshop will be a a combination of theory and lab. The lab will constitute about 60% of the total course. The course will cover

History of IPv6
- What where the problems to be solved?
- Which where the proposed solutions
- Why was IPv6 chosen?

IPv6 Design and addressing
- What's an IPv6 address?
- Packet formats
- Comparison between IPv4 and IPv6 packets
- Address allocation

Transition from IPv4 to IPv6
- Applications
- Dual-stack
- Various transition technologies
- Teredo
- 6to4
- SIIT
- ISATAP
- 6over4
- etc

IPv6 Neighbour discovery
IPv6 Stateless auto-configuration
Mobile IPv6
Address selection
IPv6 and DNS
- Things to think about
- How to configure

Applications
- What applications are there?
- How do I port my application to support IPv6?
- IPv6 POSIX API

Is IPv6 any good?
- Does it solve today's problems?
- What does the future for IPv6 looks like?

Configuring IPv6 on your machines
- Static addresses
- Prefix advertisement
- Auto-configuration
- DNS-server (bind) and zones
- Configuring postfix for mail
- Configuring Apache for IPv6

- RIP
- OSPFv3
- ISIS
- BGP and BGP Multihoming
- Filtering
- Configuring IPv6 on your router
- Configuring OSPFv3

- Configuring BGP
- Configuring filtering
- APNIC policies with regards to IPv6 Allocation.
- Global IPv6 scenario
- Migration strategies and case studies

[Top]

DNS & DNSSEC
Instructors: Bill Manning (EP.net), Johan Ihren (Autonomica), Ed Lewis (Neustar)

Class Size: maximum 28

Attendees with laptops are desirable.

Intended audience: This course is suited for systems staff, network administrators, DNS administrators, and other staff with responsibility for design and operations of network services (almost all of which depend on DNS). Anyone else who wants a better understanding of how DNS actually works is welcome too. ccTLD administrators are most welcome.

Pre-Requisites: Basic user level Unix, knowledge of TCP/IP addressing and reasonable idea about how the Internet naming scheme works.

What you will Learn:

A complete and compact introduction to DNS. All of "classic DNS" is covered. Most of standard DNS issues are both theoretically discussed and, through lab exercises, worked with in practice.

Excerpt of topics covered: historic overview, database structure, record types, zones and domains, DNS message structure, recursion, authoritative servers, resolvers, caching, delegation, glue records, the ice floe model vs. the tree hierarchy model, reverse delegation, master vs slave, primary master and hidden master, zone transfers, notify, access control, logging, implementations, design alternatives and aspects.

As time permits, more complex scenarios (including firewalls, "split-DNS", forwarding, etc), TSIG (Transaction Signatures), rndc (remote control of BIND9 nameservers), EDNS(0) (Extended DNS), DNSSEC (securing DNS data through the addition of digital signatures), views, etc. The lab exercises are performed in a BIND9 environment.

The later part of the course covers emerging topics such as secure dynamic update of DNS data. Furthermore DHCP for address space management is covered, including all the details of interection between DHCP and DNS in environments utilizing dynamic update. This course also treat the DNS aspects of IPv6 and DNS issues with migration to a mixed IPv4/IPv6 Internet. Finally international domain names are discussed in some detail.

All topics are fully covered with both lectures and hands-on exercises.

[Top]

ISP and NSP Network Security
Instructors: Vicky Shrestha (World Link), Damien Halloway (Juniper), Kunjal Trivedi (Cisco)

Class Size: maximum 28

Attendees with laptops are desirable.

Intended audience: Network Operations and security staff at ISPs and Network Service Providers. People who are trying to learn ropes of establishing a functioning security system in their network core and edges. Any one else with interest in Security topics.

Pre -Requisites: This is an advanced course. Good familiarity with UNIX command line and system administration jobs. Knowledge of Layer 3 protocols, and command line of popular routers. Basic knowledge of security concepts is an added advantage.

What do you Learn:

The ISP / NSP Security Workshop focuses on following components to provide comprehensive understanding and hands-on experience allowing you to gain valuable experience in network security best common practices, tools and techniques.

- Network infrastructure security
- Security services

For network infrastructure security, best common practice for protecting infrastructure including IP addressing, baseline building, securing IGP and BGP routing protocols and router filtering techniques are covered in detail. Controlling access to the routers, collecting network telemetry information and control plane protection techniques are discussed.

A six step methodology for detecting and mitigating DDoS attacks on the infrastructure provides hands-on understanding on how to deal with such attacks. Anti-spoofing measures to combat IP spoofing attacks and Remotely Triggered Blackhole (RTBH) filtering to protect against infrastructure

attacks hands-on practice provides easy to deploy tools on the SP networks.

The security services address designing, deploying and managing L3 Virtual Private Networks. A balanced discussion covering security of L3VPN provides good basis of evaluating the level of security for the business needs. Finally, a discussion of how managed security services such as IP VPN prepares SP networks for provisioning other security services.

PROGRAM

Juniper Advanced Routing (2 days)
Instructors: Damien Holloway (Juniper)
Level: Intermediate

- JUNOS philosophy and features,
- the Juniper router family,
- typical placement of various routers in networks.
- Introduction to JUNOS CLI and exercises
- Routing policies, filters and routing protocols - OSPF and BGP - configuration exercises
- MPLS and VPN configuration
- Demonstrating High Availability features - fast reroute, graceful restart etc.
- guidance on network design principles for high availability.
- high level overview of network security issues and techniques for DDoS mitigation and security mechanisms such as IDS, Firewalls.

[Top]

Best Practice Guidelines for Deploying MPLS (1 day)
Instructors: Monique Morrow (Cisco), Jeff Apcar (Cisco), Muhammad Sagheer (Cisco)
Level: Intermediate
Slides: download

MPLS core related technologies: Layer 2 and Layer 2 VPNs; multicast, OAM, Security, IPv6; GMPLS; interworking scenarios and future direction of MPLS technology.
The tutorial focus will be in providing practical implementation guidelines with case study example.

[Top]

Introduction to WiMax and Broadband Access technologies (1/2 day)
Instructors: Mohammad Farhad, Richard Pruss
Level: Intermediate
Slides: download

The IEEE 802.16/WiMax (Worldwide Interoperability for Microwave Access) standard defines the air interface for fixed point-to-multipoint broadband wireless access networks. It is a wireless alternative to Digital Subscriber Line (DSL). An amendment, being drafted, adds mobility support. A lot of works are also going on in many standards bodies and many edge of service provider network deployments on session and policy control. This tutorial provides a detailed introduction to WiMax and covers the ground of access privileges, resource usage control, QoS, accounting and service and application mediation. Standards status and update for Cable, DSL Forum, mobile/ 3GPP, ITU, TISPAN and some hopes for convergence. It also discusses some deployment cases to show how it looks like in practice.

[Top]

Delivering Triple Play Services Over Metro Broadband Network (1/2 day)
Instructors: Lim Wong, Richard Pruss (Cisco)
Level: Intermediate
Slides: download

Metro broadband networks are capable of delivering a variety of services to the end customers but why are so many carriers having issues offering triple play services?
This tutorial will discuss the architectural options for delivering high quality video, voice, and Internet services to the home; and how video and voice can be integrated into existing data network. What last mile technology, security and Quality of Service mechanism are needed to offer these services?
Topics include:
- Triple play network architecture
- Last mile access options - PONs, xDSL, Metro Ethernet, WiMAX, Cable
- IP video essentials
- Multicast video (IPTV) network design
- Video on Demand network design
- Security and Quality of service requirements

[Top]

Security in Mobile and Wireless Networks (1/2 day)
Instructors: Ray Hunt (University of Canterbury, NZ)
Level: Intermediate
Slides: download

This tutorial will address a range of technical and performance issues central to the deployment and operation of secure Wireless LANs (IEEE802.11a, b, g) and UMTS / CDMA2000 3G networks appropriate for both the enterprise and for wireless and mobile network operators. It will examine security in the mobile network architecture including important topics such as cryptographic tools, devices and equipment, mobility, authentication and security standards, security testing and evaluation, performance and quality of service as well as a range of WLAN/3G interoperability and standards issues. It will discuss the new IEEE802.11i (WPA2) security standard including new products and performance issues and examine how this will interwork with 3G Networks. Further, it will discuss the results of performance tests on various security architectures and configurations in order to provide useful guidelines for configuration and operation in practice.

Demonstration of basic stumbling, attack and sniffing tools will also be included.

[Top]

Using EAP Authentication with RADIUS and Configuration of Linux Authentication Server (1/2 day)
Instructors: Hugh Irvine, Dhruba Raj Bhandari
Level: Intermediate

The RADIUS protocol is widely used for AAA (authentication, authorisation and accounting. EAP (extensible authentication protocol) is now extensively used for both wireless and wired networks, and there is a bewildering array of EAP flavours to choose from. This tutorial will demonstrate and explain the configuration and operation of a number of EAP versions.

The practical demonstration will involve:
- General overview of wireless authentication
- Configure Apache as an portel page server
- Mysql as an database server for user and accounting info
- Free Radius as an authentication server.

[Top]

BGP Deployment, Best Current Practices and Troubleshooting Techniques for Service Providers (1 day)
Instructors: Philip Smith (Cisco)
Level: Introductory

This tutorial introduces service providers to BGP, including IBGP, eBGP and common attributes. It will then introduce some more advanced features of BGP, and look at the various scaling techniques available, when to use BGP instead of an IGP, and examine policy options available through the use of local preference, MED and communities. This tutorial introduces service providers to some of the features available in BGP to aid multihoming to the Internet. After an explanation of multihoming and the principles being followed in this tutorial, several examples involving different scenarios will be given. Configuration techniques for modifying inbound and outbound traffic flows are covered, as are some examples on how to use BGP communities in inter-AS relationships. The tutorial finishes by covering some common multihoming security issues.

The tutorial discusses the best current practices for ISPs, including how to configure external peering sessions and how to deploy BGP across ISP backbones as well as examining common problems ISPs have when deploying BGP within their network. It looks at problems with peer establishment, missing routes, inconsistent route selection, and convergence issues. It also looks at real world examples of common errors which are made when deploying BGP, both as IBGP and eBGP, in service provider networks.

[Top]

Zebra/Quagga Routing Suite (1/2 day)
Instructors: Anura Abeyaratne (MTT Network, Sri Lanka)
Level: Advanced
Slides: download

Overview:
- Installation
- Basic commands
- Starting BGP
- BGP router
- BGP network
- BGP Peer
- BGP Peer Group
- BGP Address Family
- Autonomous System
- BGP Communities Attribute
- BGP Extended Communities Attribute
- Displaying BGP Routes
- VTY shell
- Filtering

[Top]

Maximising Your IP Address Potential (1 day)
Instructors: APNIC staff
Slides: download

This tutorial consists of four different modules. Each module is self-contained so you can pick and choose which modules you are interested in. The modules are described below.

1. Infrastructure development, education and APNIC
This module will explain what APNIC is, who makes up the APNIC community, and what services and activities APNIC provides. The module will also examine APNIC's role in Internet development as well as the role of training and the future of the Internet.

2. Creating policies that work for you
This module provides an overview of APNIC policy, explains policy changes made in the past, and how you can participate in the policy development in the future. The module also provides an explanation of how to apply for IP addresses by selecting the appropriate APNIC policy for you. Finally, the module explains how to propose a new policy if current policies do not meet the needs of the Internet community.

3. Efficient address space management
This module will provide you with an overview of the Internet resource management system, how to use the functions in MyAPNIC, and how to query and update the APNIC Whois Database.

4. Managing your "old" address space
If you have IP addresses that were allocated to you in the early days of the Internet, this module should be of interest. This module will define what historical addresses are, where they come from, and what recent changes may now have an impact on the way your historical address space is registered.

[Top]

Introducing Layer3 VPNs in MPLS Networks (1/2 day)
Instructors: Ariff Premji (Juniper)
Level: Intermediate
Slides: download

Workshop for customers who do not have L3VPNs and would like to migrate to a MPLS VPN architecture. The workshop would cover the migration procedure from any non-Juniper environment to a Juniper environment. Hands-on material will be included in this tutorial.

[Top]

Integrated IS-IS Primer and Infrastructure Routing (1 day)
Instructors: Seo Boon Ng, Lim Fung
Level: Intermediate
Slides: download

Integrated IS-IS is an IGP that is popular with large service providers. The objectives of this tutorial is to allow attendees who have not been using ISIS, to evaluate if IS-IS is more suited in their environment. For attendees who are using IS-IS, this session would emphasis the optimal ways to deploy ISIS in ISP environment. This includes pointers on tuning IS-IS for fast convergence. The tutorial comprises hands-on and theory sections. The theory session includes designs and case studies which are specific to service provider networks. Participants should have baseline knowledge of either IS-IS/OSPF/BGP.
Introduction to IS-IS
- IS-IS Protocol Overview
- CLNS Addressing
- IS-IS Protocol Concept
- IS-IS Database concept
- Difference between IS-IS and OSPF
- IS-IS SP deployment best practise (IS-IS working with BGP)
- IS-IS MD5 authentication
- IS-IS security Using IS-IS to hide the core network

Lab session
- IS-IS case study and lab setup
- Lab on IS-IS and Routing security (Hiding the core network)
- Basic ISIS Troubleshooting technique

[Top]

Traffic Engineering in MPLS Networks (1/2 day)
Instructors: Harpreet Singh
Level: Advanced

This presentation talks about the conventional problems in IP networks, different techniques in MPLS traffic engineering and the limitations and capabilities of MPLS traffic engineering. The presentation starts with RSVP signaling, various approaches to Fast reroute, and traffic protection. The presentation also touches on the multivendor aspects of traffic engineering in Juniper and Cisco routers and the different implementation flavours

[Top]

Netflow, Flow Tools and Flow Analysis (1/2 day)
Instructors: Gaurab Upadhaya
Level: Intermediate

Netflow has been increasingly used as a tool to gather information about traffic flows in IP networks. Flow analysis has the ability to tell administrators what kind of traffic is flowing in the network based on traffic types. As has been observed in the past, netflow can be used to detect attacks and troubleshoot networks. goals - Enable participant to enable flows on their routers, collect flow data and display flow data in RRDTool generated graphs. Pre-requisites - Basic knowledge about routers, Unix based systems, and IP address and ports.

[Top]

VoIP - Asterisk and SIP Implementation, Theory, Monitoring and Traffic Engineering (1 day)
Instructors: Jonny Martin, Ruwan Silva, Habib Madani, Syed Khurram
Level: Intermediate
Slides: download, download2, download3

This tutorial aims to get a few more people up and running with their own VoIP systems and to provide additional information to those who already are up and running. Implementation of an Asterisk - the Open Source PBX - based VoIP system will be covered from the initial build through to a fully

functioning system.

The theory and operation of the Session Initiation Protocol (SIP) will be covered. This will include the theory of operation and architecture of SIP and exploration of Open Source implementations with particular emphasis on Asterisk and SIP Express Router (SER).

Finally VOIP Network traffic trend analysis through SIP, SIP-T, ISUP, MGCP, Trunk protocol counters will be covered. This provides an innovative way to monitor VoIP networks and traffic flows which can help in identifying capacity, malfunction and mis-configuration issues. Industry wide the switches need to have this information available for doing trend analysis. BTS provides ways export the data to a file, which can then be pulled off the switch in pseudo-real time manner for trend analysis purposes.

[Top]

ISP Network Security - Survey of Security Threats and Attack Classification (1/2 day)
Instructors: Danny McPherson, Ray Hunt
Level: Intermediate
Slides: download, download2

Information on ISP security survey results recently published includes many things that can be done to raise the bar in ISP network, lots of open source tools and techniques. This tutorial will include an introduction to commercial tools as well.

Internet architectures are built upon a pair of protocols designed over 25 years ago and to which virtually no consideration was given to security. Although the IPv6 networking family has been designed to address this issue, the majority of existing network infrastructure is subject to substantial threats. This tutorial examines the current security risks resulting from using TCP/IP by network providers and ISPs and how these threats related to traffic carried by these providers on behalf of their customers can have such devastating effects. This tutorial classifies the type of attacks possible focusing particularly on both wireless local and wide area networks.
These threats are largely centered on IP sniffing, IP spoofing, TCP hijacking, Buffer Overflow, Blended and Distributed Denial of Service attacks. Although firewalls have been designed to provide protection for many services, it is now recognised that they can be broken and new firewall and IDS technology is necessary to complete the TCP/IP security framework.

This tutorial will examine and classify the risks and threats in TCP/IP networks today addressing the limitations of firewalls as well as the use of Intrusion Detection and Prevention architectures.

[Top]

Large Scale Denial of Service Attack Mitigation (1/2 day)
Instructors: Paul Quinn, Darrel Lewis (Cisco)
Level: Intermediate
Slides: download

Denial of service attacks are a fact of life for service providers today and effective attack mitigation is key for maintaining availability and exercising control.
This session will begin with an overview and characterization of attacks. We will then review attack detection techniques before turning to the core of the tutorial: mitigation. We will cover a wide-range of network-centric tools available to operators, as well as advanced mitigation architectures. The session will conclude with some deployment guidelines and a discussion of the future of denial of service attacks.
Following this tutorial attendees will have a thorough understanding of best practices for attack mitigation and be able to determine the most effective mitigation deployment models for their network.

[Top]

Best Practice for Security Patch and Vulnerability Management (1/2 day)
Instructors: Neal Gemassmer
Level: Introductory

Organisations that invest in complex and expensive network systems could find these systems become rendered useless if something as simple as patching is not managed effectively. Hackers continue to use worms, viruses, spyware and malware to exploit known vulnerabilities on unpatched systems, resulting in costly network downtime and considerable administrative resource and expense to repair.
Moreover, as the trend continues in enterprise networking for the convergence of voice, video and data onto a single network, the implications of downtime due to a compromised network become more far-reaching. Unpatched critical applications such as telephony are now vulnerable to malicious attack, with potentially disastrous consequences for an organisation's data. This is in addition to having a negative affect on the productivity of staff.
Patching is, of course, only one element of an overall security program. However, it does make a pivotal contribution to reducing the myriad of vulnerabilities and their resulting exploits. It also helps to resolve issues arising from spyware and malware. By establishing the correct procedures and process for patch management, companies can ensure they are less likely to fall victim to network attacks.
This presentation will discuss best practices approach to patch and vulnerability management and why it's critical for businesses to adopt an effective network security program in order to best protect their networks against emerging security threats.

[Top]

IPv6 Transition and Deployment (1/2 day)
Instructors: Salman Asadullah
Level: Intermediate

IPv6 Network Design and Operation
- IPv6 Merits and Motivations
- IPv6 Addressing Planning and Assignment
- IPv6 and DNS
- IPv6 and Network Management

- IPv6 Routing Protocols

Enterprise Deployment
- Campus
- WAN
- S2S VPN
- Remote Access

Service Provider Deployment
- Core
- Access

IPv6 Services
- Multicast
- QoS
- Security
- Mobility

[Top]

APNIC: Practical introduction to IPv6 (1 day)
Instructors: Jordi Palet Martinez, Tomohiro Fujisaki (NTT), Amante Alvaran (APNIC)
Slides: download

The IPv6 tutorial will offer a practical introduction to the basics of IPv6. Participants will learn how to activate IPv6 on PCs, and be given practical instruction on:

* Installing IPv6 on different platforms (XP/W2003, Linux, BSD)
* Basic stateless/stateful configuration, including privacy setup
* Transition mechanisms
* Examples of applications
* Basic configuration of routers
* IPv6 policies and procedures

During the tutorial, attendees will also learn how to accomplish some
Basic monitoring and troubleshooting of the IPv6 network.

The tutorial is targeted at engineers and network administrators from both ISPs and SOHO/Enterprise networks. Participants should already have a basic knowledge of IPv4.

Note: Considering the hands-on approach of this tutorial, it is highly recommended that participants bring their own laptops, so they can practice the lessons learned during the tutorial. It is assumed that most participants will be using Windows XP, so most of the training will be done on this operating system. However, instructions for other operating systems will be provided as part of the tutorial materials.

PROGRAM

When: Wednesday 1 March 2006 9:00 - 10:30
Where: [Auditorium]
APRICOT Plenary Keynote Address: A PKI to Support Improved Internet Routing Security
Steve Kent (BBN)
Slides: download 15MB pdf

Several proposals have but put forth for improving the security of routing in the public Internet, e.g., S-BGP, soBGP, and SPV. The ultimate goal of these proposals is to enable ISPs to verify the legitimacy of route advertisements received via BGP UPDATEs. A first step toward this goal is enabling an ISP to verify that an Autonomous System (AS) is authorized to originate routes to specified blocks of IP addresses.

This presentation describes a PKI designed to support these goals, through the issuance of X.509 digital certificates to resource holders. It makes use of the certificate extension defined in RFC 3779, to represent address space and AS number allocations. The PKI parallels the existing organizational structure by which these resources are managed (RIRs, LIRs/NIRs, and ISPs), hence no new "trusted" entities are introduced. Unlike a conventional PKI, this one does not issue certificates to identify resource holders, but rather enables Route Origination Authorizations (ROAs) to be verified as having been digitally signed by the resource holder, whoever that may be. A repository system for distribution of the PKI data, and ROAs is also described.

About the Speaker

- **Dr. Stephen T. Kent**
  Vice President & Chief Scientist - Information Security BBN Technologies

  In his role as Chief Scientist, Dr. Kent oversees information security activities within BBN Technologies, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of network security systems and served as principal investigator on a number of network security R&D projects for over 25 years.

  Over the last two decades, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, public-key certification authority systems, PKI models, and key recovery (key escrow) systems. His most recent work focuses on security for Internet routing, voice over IP, and high assurance cryptographic modules.

  The author of two book chapters and numerous technical papers on network security, Dr. Kent has served as a referee, panelist, session chair and keynote speaker for security conferences around the world. Since 1977 he has lectured on the topic of network security on behalf of government agencies, universities, and private companies throughout the United States, Europe, Australia, Africa and the Far East. Dr. Kent received the B.S. degree in mathematics from Loyola University of New Orleans, and the S.M., E.E., and Ph.D. degrees in computer science from the Massachusetts Institute of Technology. He is a Fellow of the ACM and a member of the Internet Society and Sigma Xi.

[Top]

When: Wednesday 1 March 2006 9:00 - 10:30
Where: [Auditorium]
APRICOT Plenary Keynote Address: Convergence?
Geoff Huston (APNIC)
Slides: download

One of the more persistent themes of the communications industry is that of "convergence". The term has had a long and rich history, and in its most recent incarnation convergence is being associated with the delivery of voice, video and data services. IP is, of course, heavily implicated here as the foundation technology of a new generation of converged service providers. Is convergence truly a major force in today's industry, and what other pressures are shaping the future structure of our industry? It appears that convergence is not delivering on its promises, and while the industry is undergoing yet another transformation, this has less to do with convergence and much more to do with deregulation, fragmentation and associated pressures for role specialization within the industry. What is the future of the traditional monolithic carrier in tomorrow's unconverged world?

About the Speaker

- **Geoff Huston**
  Senior Research Scientist at APNIC.

  He was largely responsible for Australia's first Internet service, the Australian Academic and Research Network. He then served a 10 year term in Telstra, in various technical roles, finishing as the Chief Internet Scientist for the company. He has been a member of the Internet Architecture Board, and currently chairs a couple of working groups in the IETF.

[Top]

When: Wednesday 1 March 2006 11:00-12:30
Where: [L2 / Room 4]
Session: Peering Track
Speakers: Barry Greene (Cisco), Stephen Baxter (PIPE Networks), Mike Hughes (LINX)
Slides: download, download2, download3

At APRICOT2004 and APRICOT 2006 we highlighted the operations and peering challenges facing ISPs building into and within Asia, sharing the collective experiences of the Peering Coordinators in the room. In this session we will focus on evolution - in order to continue forward it is sometime useful to reflect on the past.

A Historical perspective
As one of the early Internet architects intimately involved with peering in Asia, Mr Greene will share a historical perspective on some of the first peering sessions in Asia. He will share his view on questions such as: What was the Asia Internet like before regional peering? What was the motivation for dedicating expensive (oceanic) transport for the first peering sessions between parts of Asia? Who were the players involved in setting up peering? (telcos with ISP subsidiaries? ISPs purchasing transport on the open market? Engineers or Business Development staff?) What was the nature of the cooperation required?

An Australian Historical Perspective
Peering issues have often been heated when focused on recently privatised incumbents and the peering inclinations of Tier 1 ISPs (those who have access to the entire country routing table solely through peering relationships). Australia is no different and has taken broad strides towards the privatization of the incumbent (Telstra). Mr. Baxter, as an early participant in the Australian peering ecosystem, will share with us the evolution of peering in Australia, focusing on the rise of the so-called "Gang of Four" Tier 1 ISPs, the regulatory initiatives from the ACCC to deal with grievances, and the current peering ecosystem in Australia.

Best Current Practices in Peer NOC-to-NOC Communications
Over the years we have seen a wide variety of operations support and escalation communications issues that can and should quickly be repaired. The speaker has spent the last few years working with the Peering Community to document and share the best practices in Network Operations Center communications. This is particularly important when NOCs are spread across cultural and language boundaries.

[Top]

When: Wednesday 1 March 2006 14:00-15:30
Where: [L2 / Room 4]
Session: Peering Track
Speakers: Brokaw Price (Yahoo!), William B. Norton (Equinix), Sylvie LaPerriere (TeleGlobe)
Slides: download

This talk is based on recent research with the peering coordinator community and highlights the strongest arguments for and against using peering ratios to discriminate peering candidates. The audience will decide which side of the argument is stronger by a show of hands at the end of the talk.

Peering from a Content Provider perspective
Yahoo! is one of the world's most popular destinations in part because of its intense focus on end-user experience. To that end Yahoo! has built its own peering infrastructure and expanded into parts of Asia. Mr. Price has established hundreds of peering sessions to date and will share his experiences building into and throughout Asia from a Content Provider perspective.

The Folly of Peering Ratios?
Peering is often established with mindset that the two parties are "peers"; that theis networks are of similar reach and scale. Peering "Ratios" are among the potentially many peering metrics for selecting peering candidates. For example, one ISP might stipulate that peering is acceptable if your ratio does not exceed 2:1 outbound to inbound. Since content providers send large volumes of content in response to a relatively small request packet, this metric makes it very difficult for content providers to qualify. This issue becomes more critical as content providers expand into more high bandwidth applications like high definition video streaming and emerging time-delayed large scale content distribution.

International Peering Dynamics
One of the most important challenges a Peering Coordinator faces is determining the locations where peering strategically makes sense across and within Asia. How does one assemble the business case and business plan for peering regionally and then within particular countries? What are the gotchas, hidden underlying assumptions, and challenges to overcome? What should we as a Peering Community do to foster more interconnections? Ms. LaPerriere will share her tenure of International Peering experiences with the group, helping to lay the groundwork for the group to build more peering in Asia.

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [L2 / Room 4]
Session: Peering Reception - The New Peering Simulation Game v4
Facilitator: William B. Norton (Equinix)

Bring your wireless-enabled laptop computers to interact with this new Interactive Peering Simulation!

The Peering Simulation Game has been re-engineered so the players and the audience members fire up their java-enabled browsers and participate interactively with the newest incarnation of the Peering Simulation Game.

Four players from the audience will bring up their laptops and play the role of Peering Coordinator, building out their networks, managing their transit commits, building into Internet Exchanges (if it makes financial sense) and negotiating "paid" peering. As the ISPs build out, and the peerings are established, all laptops are updated in real time.

The audience plays the role of The Market, helping decide which players get bonus customers and traffic, which ones suffer equipment failures, etc.

There is of course a twist or two in the game. First, the players now make their moves at the same tme, and all player and audience screens are updated in real time. Second, the audience has complete information - they can see the relative strengths of the players, as well as the players future rolls, but the players have only a limited view into the other players negotiating position. Third, the ISPs can steal each others customers! They can offer a lower price to sway the customers. ISPs can apply "Customer Care" to protect their customers from being stolen, which can be countered by applying "Taint" to help encourage a customer to leave a "bad" ISP. These peering and competitve dynamics mimic the real world coopetition that ISPs face every day. In the five years of evolution of this game, we have seen that the negotiations carried out in the game are strikingly similar to peering negotations in the real world.

This is a not a presentation ! Aside from the 5-10 minute introduction to "What is Peering? and How do we play the Peering Simulation Game?", the players and audience members (along with the facilitator) will provide the content and discussion. This is a highly interactive and audience involved participation game that helps teach how peering really works.

[Top]

When: Wednesday 1 March 2006 11:00-12:30
Where: [L2 / Room 5]
Session: SPAM
Speakers: Dave Crocker (Brandenburg Internetworking), Kwan Hee (Kevin) Hong (KISA/KRCERT-CC)
Slides: download

BOTNET Activity & Mitigation
The main topic will be how BOTNET works, purpose of BOTNET, dangerous of BOTNET, how to mitigate BOTNET, how we should cooperate it. Too many Asian Region system has been compromised then function as Zombie PC and being abused to several ways.

[Top]

When: Wednesday 1 March 2006 14:00-15:30
Where: [L2 / Room 5]
Session: SPAM
Speakers: Suresh Ramasubramanian (Outblaze Limited), Richard Cox (Spamhaus.org), Matthew Sullivan (SORBS), Mark Reynolds (Reynolds.Net.Au)

An open discussion on antispam blocklists, from an operator perspective.
An open discussion on antispam blocklists, from an operator perspective. The topics covered deal with blocklist listing policies, cooperation and notification strategies between ISPs and blocklists, and how ISPs can deal with listings of their IP spece in various blocklists. Each presenter will be allowed 20 minutes of speaking time, with a 30 minute open mike session on blocklists to follow.

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [L2 / Room 5]
Session: SPAM
Speakers: Ray Hunt (University of Canterbury), John Haydon (Australian Communications and Media Authority)
Slides: **download**

Tightening the Net: A Review of Current and Next Generation Spam Filtering Tools
This paper provides an overview of current and future spam filtering approaches. It then examines the problems spam introduces, including discussing what constitutes spam and how it can be measured. The paper then focuses on discussing automated, non-interactive filters, which cover a broad range from open source to commercial implementations leading on to new ideas proposed by research papers in this area. These filtering techniques can be based upon non-machine learning (heuristics, signatures, blacklisting, hash-based, traffic analysis, etc) or upon machine learning techniques (Bayesian, spare binary polynomial hashing, support vector machine, Markov models, pattern discovery etc). The paper thus aims to review existing techniques and discuss the new research ideas being published which are likely to lead to solutions in the future.
Finally a case study involving the PreciseMail Anti-Spam System is evaluated to investigate the effectiveness of implementing modern machine learning techniques such as Bayesian filtering.

Technical initatives to combat spam
ACMA is involved in a number of technical initatives aimed at reducing spam within Australia.
The benefits of these initiatives is that the information gained from them can be used to address the spam problem within Australia but can also be used by other jurisdictions to combat spam."

[Top]

When: Wednesday 1 March 2006 11:00-12:30
Where: [L2 / Room 6]
Session: Addressing & Renumbering
Speakers: Geoff Huston, Akinori MAEMURA, Masataka MAWATARI, Kiyoteru ISHIHARA, Champika Wijayatunga
Slides: download

IPv4 Address Exhaustion
The exhaustion of the IPv4 address space has been a long-anticipated event, with initial predictions being made in 1990 that predicted exhaustion by 1995. Obviously IPv4 has managed to not only survive but thrive well beyond that date, and more than one quarter of the entire IPv4 address

space remains in the as-yet-unallocated free address pool. This presentation will report on a statistical analysis of the recent trends in IPv4 address consumption, and report on the trend analysis in terms of address exhaustion. The presentation will also look at some of the implications of address exhaustion in terms of likely industry response to this situation.

IP Addressing design
IP Addressing design is one of the most basic one among variety of component of design, however it is not easy at all in practice.
This presentation will discuss about various practical cases of IP addressing which requires various consideration in day-to-day operations like following:
- IPv4 addressing
- Key points for very efficient use of IP address block
- IPv6 addressing:
- Initial design and operational consideration
- Diffrence between IPv4 and IPv6
This will include the latest discussion in JANOG17 conference on January 19 & 20.

Internet Resource Management - Past lessons and current policies in the Asia Pacific
This presentation will take a look at history to give us an understanding of the importance of internet resource management and the role of industry in self-regulation. It will explain key terminology when talking about the RIRs and will examine important aspects of the IPv4 and IPv6 policy framework.

[Top]

When: Wednesday 1 March 2006 14:00-15:30
Where: [L2 / Room 6]
Session: Access
Speakers: Truman Boyes (Juniper), Greg Bader (iiNet), S Khandekar (Alcatel), Yogesh Jiandani (Cisco)
Slides: download, download2, download3

Broadband Access Networks and Triple Play
This presentation will cover current Triple Play delivery techniques (DHCP/PPPoE/multiple VC), Broadband and Ethernet Architecture, and Broadband service resiliency (HA elements, MPLS-TE, QoS).

DSL deployment lessons learnt
A look at the business case, deployment methodology, and lessons learnt by iiNET during it's ADSL2 rollout in Australia's unbundled local loop environment.

Design considerations for delivery of Triple Play Services over Access Networks
Mr. Khandekar is the co-author of the DSLForum technical contribution (DSL2006.269.00) that describes an MPLS enabled Ethernet aggregation network for delivery of triple play services. In his talk, he will discuss design considerations and operational challenges for delivery of Triple Play Services over Ethernet based access networks that are increasingly Ethernet based.
Mr. Khandekar will also discuss the role of technologies such as VPLS, MPLS, DHCP and IP multicast as presented in the DSLForum contribution and how these technologies can be leveraged to improve the scalability, OAM, resiliency and restoration of large scale triple play networks.

Metro Ethernet
Service Providers are also looking to capitalize on the ""broadband"" opportunity, providing high-speed services to apartment blocks, multi-tenanted business centers and hotels. This is also revolutionising the Enterprise and SMB market where the access mechanism is a commonly understood technology - Ethernet.
This technology is easy to deploy, own and upgrade and will help in deployment of newer and faster services.
The UNI and NNI are both the same media Ethernet which makes this technology cost effective and simple to deploy. It can also be deployed over existing telephone cables (EtherDSL).
Ethernet economics, speed and the cost-effectiveness, simplicity, ease of use and familiarity are seen as a big plus and a new approach to metropolitan networking. Metropolitan Area Networks enabling broadband access are becoming more viable to deliver services that offer more bandwidth.

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [L2 / Room 6]
Session: Wireless Networks
Speakers: Dhruba Raj Bhandar (Final Quadrant Solutions), Matt Kolon (Juniper), Richard St Clair (Internet Users Society of Niue)
Slides: download

Large hotel wireless network deployment
This presentation gives a look at the how a large wireless network was deployed in the Soaltee Crowne Plaza Kathmandu. Architecture, tools, authentication, and limitations and lessons learnt will be covered.

Mobile and Wireless Technologies for Service Providers
As mobility becomes the 4th leg in many providers ""voice, data, and video"" strategies, many IP network engineers and architects are struggling to understand the relationship between mobility/wireless networks and IP-based infrastructure. This conference session will introduce participants to IP- and MPLS-based solutions to the data needs of mobile networks, from basic 2G GPRS networks to faster 3G networks and beyond. The role of IP access networks for WiFi and WiMax deployments will also be explored. By the conclusion, participants will understand the place and importance of IP and MPLS to the modern converged mobile network operator, and the potential for outsourcing and co-operation between mobile

and wireline operators that this relationship exposes.

Internet and Wifi Development on a Remote Island
An overview of developing a wifi nation on a South Pacific Island Nation, this presentations takes you through various aspects of what can run simply and effectively in hostile tropical environments. After some years of trial and error, the video presentation is the product of being able to find that happy combination of hardware, software, location, colocation and some luck to top it all off. Question and discussion session at the conclusion.

[Top]

When: Wednesday 1 March 2006 18:00-19:00
Where: [Ballroom 1]
Session: NSP-SEC BoF
Speakers:
NSP-SEC Overview - Danny McPherson (Arbor)
NSP-SEC-JP: Peers Working Together to Battle Attacks to the Internet - Taka Mizuguci (NTT)
Internet Motion Sensor Update - Danny McPherson (Arbor)
Slides: download

Security incidents are a daily event for Internet Service Providers. Attacks on an ISP's customers, attacks from an ISP's customer, worms, BOTNETs, and attacks on the ISP's infrastructure are now one of many "security" NOC tickets through out the day. This increase in the volume and intensity of attacks has forced ISP's to spend constrained resources to mitigate the effects of these attacks on their operations and services. This investment has helped minimize the effects of the attacks, but it has not helped stop them at the source. Stopping attacks at their source requires rapid and effective inter-ISP cooperation. Hence, these ISP Security BOFs are also used as a face-to-face syncup meeting for the NSP-SEC forum.

Additional information can be found here: https://puck.nether.net/mailman/listinfo/nsp-security

If you would like to contribute to the BOF, please send email to danny [at] arbor.net

[Top]

When: Thursday 2 March 2006 9:00-10:30
Where: [L2 / Room 3]
Session: DNS
Speakers: Edmon Chung (Afilias), Bill Woodcock (PCH), Stephane Bortzmeyer
Slides: download, download2, download3, download4

DNSSEC Implementation and Issues
In the fall of 2006, Afilias provided the technical services to PIR (Public Interest Registry) for a DNSSEC testbed for .org. Afilias implemented then-current RFCs in the testbed in order to gain experience with the technology and observe operational issues for Top Level Domain (TLD) Registries. Afilias discovered that technical issues were not serious impediments to deployment. The more serious barriers were social ones. The lack of a protocol for trust anchor key management meant intractable problems for publication. Furthermore, promoting interest in the technology turned out to be even more difficult than anticipated.

DNS Anycast Service Provision Best Practices
Anycast is now the de-facto standard for carrier-grade DNS service provision. Although anycast provides great benefits in stability and performance, there are also potential pitfalls in its implementation. In this talk, Bill Woodcock, who has built three of the largest DNS service provision networks in the world, will discuss best practices for anycast network design and implementation.

The CODEV-NIC DNS registry software
Every DNS registry must manage a database of names currently registered and produce a DNS zone file (as well as whois output) from it. To do so, most registries use a custom, locally written program.
For the smallest and poorest registries, like it is common in the South, this can be too difficult: that is why many TLDs do not have a real information system, and, for instance, cannot host a whois server.
CODEV-NIC attempts to be a solution for these TLD. Not only it is free software, but it is also multi-policy (every TLD has different registration rules).
CODEV-NIC has been developed by three registries acting in common, "".ci"" (Ivory Coast), "".mg"" (Madagascar) and "".fr"" (France).
The talk will present CODEV-NIC, the requirments it had (specially the need to be multi-policy), the technical choices and the way it was developed by three teams working in three different countries.

[Top]

When: Thursday 2 March 2006 11:00-12:30
Where: [L2 / Room 3]
Session: VoIP
Speakers: Gene Lew, Gaurab Raj Upadhaya, Jonny Martin
Slides: download, download2, download3

A technical and functional description of the SIP-IX framework that NeuStar is deploying.

INOC-DBA (Inter-NOC Dial-by-ASN)
INOC-DBA (Inter-NOC Dial-by-ASN) hotline phone system connects the network operations centers of network operators around the world in a closed VOIP system. The INOC-DBA hotline system has been in production use since October, 2002, and undergoes continuous development and refinement. Recent developments have included cryptographic authentication, a self-provisioning web interface for participant organizations, as well as inter-operability tests SIP devices and software PBXes.
This presentation will also present statistics as well as data on quality of calls.

Current VoIP activities in NZ
This presentation will cover current VoIP activities in NZ - both constructive and destructive. Telecommunications and VoIP regulation, current operators and experience, legal aspects and technical details will be investigated. A status report of the InternetNZ run ENUM trial will also be provided. Lastly and perhaps most importantly, the impact open source VoIP solutions are having on the voice landscape will be analysed."

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [L2 / Room 5]
Session: SoftbankBB's Broadband Contents
Speakers: Masaru Akai (SoftbankBB)
Slides: download

Softbank BB is a successful venture ADSL carrier who holds the most number of ADSL users in Japan with their brand-new full IP network. They have been really active in providing contents over their network.

In this session their contents services are introduced.

+ BBTV Broadband Service
+ BBTV VoD Service
+ Broadcasting of the games of Softbank Hawks Pro baseball Team:

About the Speaker

- **Masaru AKAI**
  Softbank BB Corp. Japan

  After having gained experience as a domestic integrator, Masaru has been involved with domestic/ global IT industry since joining PSINet Japan in 2004. Learned server facility & surroundings, IPv6, and BGP operating. Joined Softbank BB Corp. in 2004 as a server engineer and have focused on broadband content.

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [L2 / Room 5]
Session: Myths and Realities: How the government regulates what Australians see on the internet
Speakers: Peter Coroneos (Internet Industry Association of Australia)
Slides: download

Myths and Realities: How the government regulates what Australians see on the internet
(A legal analysis for non lawyers of Australia's online content regulatory regime)

In 1999, the internet industry in Australia, when first presented with the prospect of mandatory filtering of internet content to protect children, responded by develop three industry codes of practice. These were registered by the national regulator, the Australian Broadcasting Authority (ABA), and only after passing a strict adequacy test in relation to community safeguards.

Co-regulatory legislation makes the Codes legally enforceable by the ABA and large penalties exist for non compliance. Under the Codes, ISPs must provide for use tools and information to enable customers to better control of content accessible in the homes.

To further promote the empowerment solution, the IIA introduced the Family Friendly ISP scheme in 2003. This scheme has bipartisan political support. It entitles Code-compliant ISPs to display a 'ladybird' seal on their sites, signifying to families their entitlement to the kind of protection and assistance that the Codes mandate.

Importantly, further revisions to the Codes currently in progress extend the basic model to cover content accessible through convergent mobile devices which are now coming into use.

This paper considers the challenges to internet regulation based on the Australian experience and expounds co-regulation framework as an appropriate
policy response.

About the Speaker

- **Peter Coroneos**
  Internet Industry Association of Australia

  Peter Coroneos is Chief Executive of the Internet Industry Association, the national industry body for the Internet in Australia. In addition

to his role as primary industry advocate, political strategist and spokesperson for the IIA, Peter drives the IIA's policy development work and has instigated the formation of specialist taskforces to leverage member expertise in diverse legal, economic and technical areas.

[Top]

When: Thursday 2 March 2006 16:00-17:30
Where: [L2 / Room 5]
Session: Art and Science of Building NUS Data Centres
Speakers: Name Kelvin TEOH, HO Hock Jim (National University of Singapore)
Co-Author: David Liau Tai Wai (National University of Singapore)
Slides: download

The National University of Singapore Data Centre is a 24-hours non-stop high-availability nerve centre for the IT operation and communication backbone for the National University of Singapore. It is purpose-built with advanced temperature and humidity control, fire detection and suppression systems, UPS and standby power generators, access control security system, as well as a diverse routing of communications.

With a nett floor area of 720m2 and a floor loading of 7.5kN/m2, NUS Data Centre hosts a total of more than 200 servers with 61 Terabytes of raw data storage as well as a core communication backbone with 24 Gigabits of aggregated bandwidth. The centre supports a myriad of IT services and applications like Internet, Email, e-Learning, wireless connectivity, video conferencing, student admission, course registration, student feedback, class timetabling, digital library, alumni portal, and many other human resource and financial related applications. Combined with an access controlled media library that is equipped with an independent temperature and humidity control, NUS Data Centre ensures that critical backups are safely secured and retrieved when needed.

NUS Data Centre also provides the University with a globally connected campus via highspeed network connections to the Singapore Government Network (SGNet) and Internet-II networks in Australia, China, Japan and the United Kingdom. Each day, it serves hundreds of thousands of requests and transections from students, staff and visitors from all over the world.

NUS Data Centre...Connecting the Future...

About the Speakers

- **Kelvin TEOH**
  National University of Singapore

  Kelvin Teoh is a Data Centre Specialist and Hock-Jim Ho a Network Engineer, at the Computer Center, National University of Singapore (NUS). As a member of the Data Centre Team, Kelvin is currently managing Data Centre operations. Major projects undertaken includes a full renovation of the NUS Primary Data Centre with minimal downtime, the construction of a new Off-Campus Data Centre, and the design, deployment and operation of a state-of-the-art campus-wide distributed UPS infrastructure (inclusive of remote management and monitoring).

- **HO Hock Jim**
  National University of Singapore

  Hock Jim's role as a member of the Network Infrastructure Team has led to his participation in various engineering and community projects. These includes Inter-School Wireless Roaming, BGP Blackholing, DNS-based Botnet Migitation and Internet Bandwidth Bulk Tender for Schools. He currently oversees the NUS WAN infrastructure, and is a member of NUS Singapore Open Exchange (NUS-SOX) NOC.

- **David Liau Tai Wai**
  National University of Singapore

  IT Professional with more than 10 years of multi-displinary experience in the IT industry.

[Top]

When: Thursday 2 March 2006 16:00-17:30
Where: [L2 / Room 5]
Session: Content Switching and Application Optimization - Technologies and Design Approaches within Data Centers
Speakers: Zeeshan Naseh (Cisco)
Slides: download

Application optimization, high availability, scalability and security are the key requirements for today's Data Center network designs. This session presents several design options when deploying network based application optimization and security services.

The session focuses on the integration of Content Switching (SLB), SSL off load and Firewall technologies within a Data Centers. Deployment examples will be based on the Content Switching Module, SSL Service Module, Firewall Service Modules on the Cisco Catalyst 6500.

The advantages and disadvantages of each design approach and technology will be covered in detail together with some configuration example.

The ideas of secure internal segments and significance application flow will be covered to understand the requirements of the enterprise.

About the Speaker

- **Zeeshan Naseh**
  Cisco Systems

  Zeeshan Naseh, CCIE (#6838), is a Technical Leader in Cisco's World Wide Data Center Networking Practice within Advanced Services. His primary responsibility have been supporting Cisco's major customers, including service providers, wireless service providers, large enterprises, and financial institution. As a design consultant, Zeeshan has focused on Content Switching and Data Center designs. Zeeshan has authored several white papers and design documents that have been published internally within Cisco and on CCO. He is also the author of the upcoming book - "Designing
  Content Switching Solutions". Prior to joining the Cisco Advanced Services team, Zeeshan has worked at US WEST, FORE Systems and Cisco's Cat6500 development team.

[Top]

When: Wednesday 1 March 2006 11:00-12:30
Where: [Ballroom 1]
Session: Routing/Operations: IPv6 Deployment in Comcast
Speakers: Alain Duran (Comcast)
Slides: download

How to manage a network with 100+ million IP addresses in the next few years? When Net10 does not cut it anymore, the sensible answer for Comcast is IPv6. Comcast is one of the first operators to adopt IPv6 as a strategic activity with an aggressive roll-out plan. In its initial phase, this plan focus on the management and operation of Comcast operated devices, like cable modems and set-top boxes. Key architectural choices are made to reduce the complexity of the overall deployment.

About the Speaker

- **Alain Durand**
  Director and IPv6 Architect in Advanced Engineering at Comcast

  Alain has been working on IPv6 since 1994, participated in the INRIA BSD IPv6 implementation in 1995 and was a pioneer on the 6bone in 1996. Alain has authored numerous RFC and Internet Drafts at IETF and co-chaired the NGtrans working group from 1999 to 2002. He now servers as the co-chair of the Softwires working group. Prior to Comcast, Alain was at Sun as the IPv6 architect during the development of Solaris 10.

[Top]

When: Wednesday 1 March 2006 11:00-12:30
Where: [Ballroom 1]
Session: Routing/Operations: IPv6 IGP/BGP Routing
Speakers: Khalid Raza (Cisco)
Slides: download

V6 routing will cover OSPFv3, ISIS enhancements to carry v6 routes and BGP changes. Protocol that is gone through a major rewrite is OSPF, we will look into OSPF how the changes affect the protocol and address the limitation of OSPFv2. We will also look at all the link states and how they are different then v2 plus new LSA types that are specific to V3 only. Presentation will cover ISIS new TLV's added to the protocol for v6. We will also look at MPBGP and how AF v6 works on top of MPBGP.

About the Speaker

- **Khalid Raza**
  Cisco

  Khalid is a Distinguished Engineer at Cisco Systems. As a recognized expert within Cisco and worldwide ISP and NRN community, Khalid has been designing large scale IP networks for over ten years. His expertise includes IP routing protocols (OSPF, ISIS and BGP), MPLS and ISP networks. He represents Cisco in industry panel discussion and technical conferences around the world and discusses technologies and protocols related to large scale ISP and NRN networks.

  Khalid has influenced technology directions and decisions within Cisco and ISP and NRN community worldwide. He has produced technical white papers and co-authored a book called "Large Scale IP Network Solutions". Khalid holds a Bachelor's degree in Electrical

Engineering and a Master's degree in Engineering Management from USA.

[Top]

When: Wednesday 1 March 2006 14:00-15:30
Where: [Ballroom 1]
Session: Routing/Operations: Transitioning to IPv6: Issues & Mechanisms
Speakers: Jeff Doyle (Juniper)
Slides: download

In the past ten years a multitude of IPv6 transition terchnologies have been proposed. This presentation examines what technologiesd are gaining acceptance in the industry and which ones are being abandoned. The application of these technologies and the approaches to transition are also examined.

About the Speaker

- **Jeff Doyle**
  Juniper

  Specializing in IP routing protocols, MPLS, and IPv6, Jeff Doyle has designed or assisted in the design of large-scale IP service provider networks throughout North America, Europe, Japan, Korea, Singapore, and the People's Republic of China. Jeff is the author of CCIE Professional Development: Routing TCP/IP, Volumes I and II; OSPF and IS-IS: Choosing an IGP for Large-Scale Networks; and is an editor and contributing author of Juniper Networks Routers: The Complete Reference. Jeff has presented numerous corporate seminars for Juniper Networks, and has also spoken at NANOG, JANOG, APRICOT, and at IPv6 Forum conferences worldwide.

[Top]

When: Wednesday 1 March 2006 14:00-15:30
Where: [Ballroom 1]
Session: Routing/Operations: Multicast v6
Speakers: Toerless Eckert (Cisco)
Slides: download

"The most important stuff people should know about multicast today (but will have a hard time to figure out just from IETF specs), and some cool new stuff too that's also interesting for IPTV ... bot not everything ;-("

About the Speaker

- **Toerless Eckert**
  Cisco

  Toerless Eckert is technical leader in Ciscos Internet Technologies Division (ITD). Primarily working out of a deployment and architecture role, he is bridging the gap between customers and Cisco engineering for IP multicast both in platform independent software and Cisco product development. His current focus is on advancing the solutions for multicast resilicency, label switching and broadband access.

  First using in IP multicast in 1992 to receive video broadcasts across the globe, he became one of the first customers to EFT test Ciscos IOS IP multicast in 1994 and joined Cisco in 1999.

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: Advanced BGP Convergence Technics
Speakers: Pradosh Mohapatra (Cisco)
Slides: download

A presentation indicating recent advances in BGP protocol. Description of new BGP address families along with the functionality provided by them. New dynamic embedded tools for efficient and very flexible multihoming technics. Tools and recommendations to optimise network end to end convergence for both IPv4/v6 as well as vpnv4/v6 applications.

About the Speaker

- **Pradosh Mohapatra**
  Cisco

  Pradosh Mohapatra is a Technical Leader in the high-end routing group of Cisco Systems, San Jose, CA, where he is involved in the design and implementation of BGP protocol.

  He has more than 8 years of experience in the Networking industry and has worked extensively in IP and MPLS protocols and technologies. He is currently leading the L3VPN development effort in Cisco's high-end router product lines (CRS-1 and Cisco 12000).

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: IPv4/IPv6 Network implementation and operations
Speakers: Ariga Seiji (NTT Communications)
Slides: download

This presentation will introduce what we've done to implement and operate IPv4/IPv6 network in large scale network, for the people who has some experience on designing/operating medium to large scale IPv4 network. This covers, IPv6 characteristics you have to think of when you design large scale IPv6 network, difference between IPv4 and IPv6 which appears when deploying IPv6 into existing IPv4 network with no service interruption, and practical issues on operating IPv6 network.

About the Speaker

- **Seiji Ariga**
  IP Engineer, NTT Communications

  He has been working for NTT Communcations since 2002. He is an IP Engineer operating NTT Communications' Global IP Network (aka 'ntt.net'). NTT Communications has been running IPv4/IPv6 dual stack network globally for more than 4 years. He played a main role in design, implemention and operation of this dual stack network. He started to work on IPv6 since 1997 while he was a student at Keio University as a member of WIDE Project.

[Top]

When: Wednesday 1 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: Fast Reroute for Triple Play
Speakers: Sachin Natu (Redback)
Slides: download

For service providers, applications such as IPTV and VOIP are becoming increasingly important in Next Generation Converged Networks. For successful deployment of such applications, fast repair in case of network or link element failure is becoming a critical piece.

This presentation will focus on different methods and design solutions, which will help in network fast repair. In more details we will look at:
* Use existing routing protocol optimization to perform fast convergence.
* Nexthop Fast Reroute which makes it possible to use MPLS to protect IPTV and VOIP traffic. In this part we will also discuss some new mechanisms which can prevent microloops during subsequent routing convergence.

About the Speaker

- **Sachin Natu**
  Redback

  Sr Product Manager responsible for delivering IPTV and Voice services related product features.

[Top]

When: Thursday 2 March 2006 9:00-10:30

Where: [Ballroom 1]
Session: Routing/Operations: Pros and Cons of going unnumbered
Speakers: Kireeti Kompella (Juniper)
Slides: download

Network administrators typically number (i.e., configure IP addresses on) all directly connected interfaces of an IPv4 router. This talk examines this practice, and assesses its pros and cons, and suggests some alternatives. As this practice is fairly deeply rooted, this talk challenges some of the assumptions and deliberately attempts to stir up thinking on this front. Open discussion is invited.

Topics include: why number? why go unnumbered? when can one go unnumbered? what are some restrictions of going unnumbered? is there a middle ground? what other alternatives exist? what lies beyond going unnumbered?

About the Speaker

- **Kireeti Kompella**
  Juniper

  Kireeti Kompella is a Juniper Fellow at Juniper Networks. His current interests are all aspects of Multi-Protocol Label Switching, including Traffic Engineering, Generalized MPLS, and MPLS applications such as VPNs. Dr. Kompella is active at the IETF where he is a co-chair of the CCAMP Working Group and the author of several Internet Drafts and RFCs in the areas of CCAMP, IS-IS, L2VPN, MPLS, OSPF and TE. He specializes in Layer 2 VPNs, Metro Ethernet and Virtual Private LAN Service. Previously, he worked in the area of filesystems at Network Appliance and SGI; and earlier in the area of security and cryptography.

  Dr. Kompella received his B.S. in Electrical Engineering and M.S. in Computer Science at the Indian Institute of Technology, Kanpur; and his PhD in Computer Science at the University of Southern California.

[Top]

When: Thursday 2 March 2006 9:00-10:30
Where: [Ballroom 1]
Session: Routing/Operations: Service Control Technologies for peer-to-peer traffic in next generation networks
Speakers: Teruyuki Hasegawa (KDDI R&D Labs) & Lior Gendel (Cisco)
Slides: download, download2

"Service Control Technologies Peer-to-peer traffic in next generation networks", Lior Gendel, Oren Raboy, Mallik Tatipamula, Cisco systems; Atsushi Tagami, Teruyuki Hasegawa, Shigehiro Ano, Toru Hasegawa, KDDI labs.

Peer-to-peer (P2P) traffic consumes network resources without creating additional revenue. It is allegedly estimated that 70 percent or more of broadband bandwidth is consumed by downloads of music, games, video, and other content. Consumption will increase as P2P downloads multiply because of increases in subscriber adoption and file sizes.

Identifying P2P applications is complex. Sophisticated P2P protocols can dynamically hop to different ports, making them difficult to detect, monitor, and control. Many existing devices and unsophisticated service control technologies lack the ability to detect changing P2P protocols, hampering a service provider's ability to cope with P2P application traffic.

This paper discusses the problems associated with the growing popularity of P2P applications and presents two kinds of service control technologies. First one is deep packet inspection, which enables accounting and controlling traffic with application awareness to attain the bandwidth fairness among subscribers. This approach is effective but needs some consideration about the deepness of inspection not to infringe the privacy of communications. Second one is P2P cache inducing P2P traffic to local destinations, which can mitigate inter-domain traffic. This caching architecture is P2P protocol independent but provides only rough traffic control. We also address the possibility of harmonized service control architecture for next generation network infrastructure.

About the Speakers

- **Teruyuki Hasegawa**
  KDDI R&D Labs

  Teruyuki Hasegawa received the B.E. and M.E. Degrees of electrical engineering from Kyoto University, Japan, in 1991 and 1993, respectively. Since joining KDD (now KDDI) in 1993, he has been working in the field of high speed communication protocol and multicast system.

  He is currently a senior research engineer of IP Communication Quality Lab. in KDDI R&D Laboratories Inc. He received The Meritorious Award on Radio of ARIB in 2003.

- **Lior Gendel**
  Cisco

LIOR GENDEL is Managing Technical Marketing team in Cisco Systems. Prior to joining Cisco he designed and implemented public IP networks. After joining Cisco in 1996 he participated in the design of many private and public IP networks, in particular in Europe. His latest activity in Cisco includes a study of
applications response over large IP networks and architecture of Cisco NG products. He holds a B.Sc. in computer engineering, B.A. computer science and an M.Sc. in computer science from Ben-Gurion University, Israel.

[Top]

When: Thursday 2 March 2006 11:00-12:30
Where: [Ballroom 1]
Session: Routing/Operations: Peering Planning Cooperation without Revealing Confidential Information
Speakers: Arman Maghbouleh (Caridenl)
Slides: download

For most Internet Service Providers the majority of their traffic enters or leaves the network via BGP enabled peerings or upstream provider(s). Not only do these links need to have enough capacity during normal operation, they also need to provide redundant capacity during link failures. For the egress traffic (service provider to remote peer) this can be easily verified by simulating the rerouting under failure, as the topology of the network is completely known. The return traffic (remote peer to service provider) however can not be simulated, as the behavior of the remote network is not known. This creates a gap in the planning process for external peering links.

In this talk we present a simple methodology for creating 'Failover Matrices' that describe the traffic redistribution under peering link failure conditions. the matrices provide a useful mechanism for sharing information and improving the mutual planning process without disclosing any proprietary information. We will describe the principles behind the process as well as walk through a real scenario.

About the Speaker

- **Arman Maghbouleh**
  Caridenl

  Arman Maghbouleh serves as the President of Caridenl Technologies where he works with network operators to develop routing and traffic management solutions. Arman has extensive experience in network design consulting and tools development, including stints at Apple Computer, Fidelity Investments and Advanced Telecommunications Research Laboratories.

[Top]

When: Thursday 2 March 2006 11:00-12:30
Where: [Ballroom 1]
Session: Routing/Operations: IPFRR
Speakers: Stefano Previdi (Cisco)
Slides: download

IP Fast Reroute technologies aim to provide traffic restoration within a few tens of milliseconds. Similar technology has been already developed and deployed using MPLS and now IPFRR delivers the same capability to IP networks or IP+MPLS networks but where RSVP is not deployed. IPFRR also provides protection for multicast traffic. This presentation gives an overview on the current IETF proposals in terms of architecture as well as the Cisco view on these technologies. The presentation covers multiple aspects including:
- IP Fast Reroute Downstream Routes
- IP Fast Reroute Not-Via Addresses
- Micro-loop Avoidance Algorithms (for Fast convergence and FRR technologies)
This session is ideal for anyone who wants to understand the latest developments and techniques in IP routing.

About the Speaker

- **Stefano Previdi**
  Cisco

  Stefano Previdi joined Cisco Systems in March 1996 as Escalation engineer in the Technical Assistance Center for Routing Protocols Technologies. He then moved to a Senior Consulting Engineer position and participated to the architecture definition of MPLS-VPN. He also closely followed the first Cisco implementation of MPLS-VPN as well as the early field deployments.

  In 2001, he moved to engineering as Technical Leader for IS-IS development and implemented a set of Fast convergence features in IOS IS-IS implementation.

  Since 2002, Stefano joined IOS-XR Architecture team and focused on Routing Protocol performance and scalability.

  In parallel with his engineering activity, Stefano is an active member of IETF especially in the IS-IS and Routing Area working groups. He submitted several drafts among which some have been moved to RFC status.

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [Ballroom 1]
Session: Routing/Operations: Modelling Inter-Domain Routing
Speakers: Olaf Maennel (University of Adelaide)
Slides: download

In this talk we discuss a methodology and tool to construct an AS-level model of the Internet topology. The aim of this work is to be able to simulate the inter-domain routing system in such a way that we can predict the results of topology and/or policy changes. With such a tool operators could ask "what-if"-questions, for example: "What impact does a new (or cancelled peering) have on inter-domain traffic flows"? "To which peer/upstream should I connect, given a certain traffic profile"? "What impact has a change in the connectivity of transit networks on my AS"?

To answer such questions we use large-scale simulations. Recent advances in simulation techniques allow us to compute Internet-wide routing models in reasonable time. As input to our simulation, we use BGP routing tables gathered at different vantage points. We start off with a simplified model that matches all observed paths without having to handle the coarser policies applied in the Internet that lead to the observed paths. From there we go on and use heuristics to correlate the information that is available using many observation points and many different prefixes. This gives us insights about how policies might affect routing in the Internet in general and at which granularity policies are actually applied at the AS-level.

While our methodology is still work-in-progress, preliminary results show that we can expect to predict AS paths between two ASs with accuracy above 87%. To improve our methodology we seek feedback from the network community to understand what particular questions our tool should be able to answer.

For more information about how we construct the inter-domain model, please see: http://home.in.tum.de/~muehlbew/thesis.pdf

---

About the Speaker

- **Olaf Maennel**
  University of Adelaide

  Olaf Maennel obtained his Ms degree in computer science from the Saarland University in Germany in May 2002 and? his PhD from the Technical University of Munich in October 2006. He is currently ?a postdoctoral fellow with the University of Adelaide in Australia. His current research ?interest is networking, with a focus on routing, including router testing, understanding convergence issues and topology characteristics.

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [Ballroom 1]
Session: Routing/Operations: Multi-Segment PWs: "A small step for PWs, a giant step for Metro Convergence?"
Speakers: Jeffrey Sugimoto (Nortel)
Slides: download

Pseudowire End to End Emulation (PWE3/PW) is gaining momentum. WAN deployments of PWE3 are currently enabling new Ethernet services and the opportunity to converge ATM, Frame Relay and other legacy services over a common MPLS core. The multi-service attributes of PWs and adaptability to different types of PSN tunnels are giving the technology strong consideration as a candidate to deliver convergence in metro access networks, either as an end to end service or as an aggregation for "new age" solutions: e.g. next generation optical transport, triple play, wireless backhaul.

As PW technology moves from leading edge to mainstream and into the Metropolitan Area Network (MAN) a number of considerations are coming to the forefront:

How can I keep my access network simple while deploying PWs?
How can I segregate my access and core networks?
How can I scale a PW deployment in general?
How can I offer PW between administrative domains, including Inter-provider scenarios?

These requirements drive a need for a new breed of PWs that concatenates several PW segments together to form a Multi-Segment PW (MS-PW). This presentation starts by discussing the new requirements and motivations behind them with a particular focus on the need to provision and connect segments of a MS-PW in an operationally efficient manner. The presentation then discusses the mechanisms that provide solutions to the problem considering the latest IETF work and it concludes with an analysis of possible applications for these building blocks.

About the Speaker

- **Jeffrey Sugimoto**
  Nortel

  Jeff Sugimoto is a senior engineer that manages the L2 VPN services team reporting to the office of the CTO in Nortel's service provider data networks organization. His 12 years at Nortel have included a variety of experiences including several years of engineering, design and architecture, focusing on L2 VPNs over MPLS. Jeff has co-authored several drafts in the IETF and contributions to the MFA related to L2 VPNSs over MPLS, most recently focusing on multi-segment pseudowires. His experience and expertise has enabled Jeff to speak at several large technical conferences, including most recently Carriers World Asia 2006.

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [Ballroom 1]
Session: Routing/Operations: Opportunities for SPs with Enterprise MPLS
Speakers: Matt Kolon (Juniper)
Slides: download

MPLS is no longer a technology just for Service Providers, and enterprise IT managers are beginning to be quite sophisticated consumers of it. Far from being a threat to Providers, this situation opens up a variety of possibilities for interesting hybrid service definitions, using MPLS capabilities in new and technically challenging ways. From enabling a customer's private network, to using inter-AS operations to peer with them at the MPLS NNI, to using carrier's carrier models to transport the MPLS backbone of a geographically disparate organization - there are many chances to offer customers excellent service helping them build a hybrid MPLS network. This presentation discusses the standards and practices you can use to build these networks, and offers practical advice and case studies from providers who have done it.

About the Speaker

- **Matt Kolon**
  Juniper

  Matt Kolon has worked for Juniper Networks since 1999, and is currently Juniper's Mobility Architect in the APAC region. He helps design mobile networks and writes, presents, and teaches about mobility, security, telephony, and the future of IP technologies. Prior to Juniper he was a Senior Member of Technical Staff for Hill Associates, where he trained and consulted for telecommunications providers; prior to that he was an IT consultant in private practice in New York City.

  Matt has presented papers and seminars at networking conferences and trade shows including MPLScon, APRICOT, NANOG, The China VPN Conference, MPLS Forum Japan, and SuperComm. He is a co-author of two books, "IP Telephony" (McGraw-Hill, 1999) and "Juniper Networks Routers: The Complete Reference" (McGraw-Hill, 2002), and since 1994 has published many technical and non-technical articles in industry journals and elsewhere.

[Top]

When: Thursday 2 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: Using Multi-Layer Routing to Provision Services across the MPLS/GMPLS Domain Boundaries
Speakers: Andrew G. Malis (Tellabs)
Slides: download

Network convergence naturally occurs to avoid the need for service specific infrastructures. However, as convergence occurs, the technology selected for the convergence layer (i.e. MPLS, IP, WDM, SDH, ATM) is influenced by the service mix that a carrier expects to carry in that particular portion of the network. This leads to different convergence technologies being chosen in different parts of the network.

The selection of different convergence technologies doesn't change the fact that customers are still going to request services that traverse the entire network. Consequently, control plane mechanisms must support the routing of service requests through a series of regions using dissimilar convergence layers. To facilitate this, the control plane needs to understand the multi-layer structure of the network, and how services requests are routed.

This talk will show how multi-layer routing methods can meet this requirement, and will include a discussion of the information necessary to represent the relationship between the resources in different layer networks.

About the Speaker

- **Andrew G. Malis**
  Tellabs

  Andrew G. Malis holds the position of Chief Technologist at Tellabs, which provides end-to-end service delivery and transport solutions for carriers. He has been active in wide-area data networking and telecommunications for over 30 years, beginning with the ARPANET,

the foundation of today's Internet. He has also held senior engineering positions at Bolt, Beranek, and Newman; Ascom Nexion; Cascade Communications; Ascend Communications; Lucent Technologies; and Vivace Networks, which was purchased by Tellabs. His current responsibilities include Tellabs' product architecture, future product planning, standards participation coordination, and customer consultation.

He is also President and Chairman of the Board of the MFA (MPLS, Frame Relay and ATM) Forum, served as the MPLS Forum's founding Technical Committee Chair, has chaired a number of working groups in the Internet Engineering Task Force (IETF) and the ATM Forum, and is a veteran participant and award recipient in other standards bodies and industry consortia. He has written, edited, and otherwise contributed to many standards documents in these organizations, including 21 IETF RFCs. He also serves on the technical advisory boards of several privately held high-tech companies, and has chaired and spoken at numerous industry conferences. He received his Bachelor of Science degree in Computer Science and Applied Mathematics at Brown University, and his Master of Science degree, also in Computer Science and Applied Mathematics, at Harvard University.

[Top]

When: Thursday 2 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: Internet routing table analysis
Speakers: Stephan Millet (Telstra)
Slides: download

Research into 18 months worth of BGP activity on an Australian ISP Backbone. This research shows a corrolation between the size of the routing table and the BGP updates created as the BGP table size increases. The reseach also investigates ways to minimise the effect of BGP updates on a core network, and attempts to determine what may happen if the BGP table continues to grow at it's current rate.

About the Speaker

- **Stephan Millet**
  Telstra

  Network Engineer for Telstra Internet Direct, with 5 years ISP industry experience in network engineering and routing.

[Top]

When: Thursday 2 March 2006 16:00-17:30
Where: [Ballroom 1]
Session: Routing/Operations: Metro scalability and Availibility
Speakers: Jian Feng Xu (China Telecom)
Slides: download

Today scaling layer 2 metro network is a challenge. Spanning Tree Protocol is not the most suitable means of deploying MAN. The speaker would discuss the problem he face while building MAN. He would also alternative using IP (layer 3) to address some of the issue. He would also share his experiences he encounter. He would quote case study and the direction his organization is moving ahead to achieve their goal of scaling MAN network.

About the Speaker

- **Jian Feng Xu**
  China Telecom

  The speaker has been involved in Internet in China since 1995. He started as a System Intergator supporting China Telecom before moving into the Research Department in China Telecom. The speaker is responsible for the design and building of the ChinaTelecom Next Carrier Network (CN2) backbone which incidentally is the larget IP network in China today. Today, Xu heads the CT research team comprizing of a group of research engineers. He also holds the concurrent role of Chinanet Chief Operation Manager over seeing the smooth running of Chinanet IP network. Xu travel within mainland China to give talks and share his experience of building large scale service provider IP network. He holds a master degree in Communication from Southern China University of Technology.

[Top]

When: Thursday 2 March 2006 11:00-12:30
Where: [Ballroom 2]
Session: Security: Security Operations Centers (SOCs).
Speakers: Barry Raveendran Greene

Guest: PCH - iNOC Phone Demonstration
Slides: download

SPs need tools, procedures, processes and training to survive today world of DOS, WORMs, VIRUSES, PHISHING, and BOTNETS. The presenter will review a SOC Starter Kit using freely available tools and techniques which would help an SP NOC, SOC, or Abuse Desk get an upper hands on today's threats.

[Top]

When: Thursday 2 March 2006 14:00-15:30
Where: [Ballroom 2]
Session: Security: A Day in the Security Life of a SP - NTT USA (Verio).
Speakers: Peter Schoenmaker (NTT America)
Slides: download

ISP Security professionals encounter unique security incidents. Miscreants, extortion, attacks on their infrastructure, law enforcement knocking on their doors, rampant worms, botnets gone wild, and collateral damage that knocks out multiple gig links are all types of incidents that an enterprise security professional will never experience. "A Day in the Security Life of an SP" is a new regular session given by service provider security professionals to help the broader APRICOT operations community learn about their colleagues' work, point out worries and concern in the industry, and recommend actions that the community can take that would make life easer.

[Top]