

行政院及所屬各機關出國報告  
(出國類別：會議)

參加 2017 年

「歐洲網路資訊中心第 75 次會議  
(The Réseaux IP Européens Network  
Coordination Center, RIPE75)」  
會議報告

出國日期：2017 年 10 月 20 至 10 月 27 日

派赴國家：阿拉伯聯合大公國 杜拜

出國人員：

國家通訊傳播委員會

基礎設施事務處 柯技正勝民

平臺事業管理處 施技士智韋

報告日期：2017 年 12 月 29 日

# 目錄

壹、 前言.....	1
貳、 RIPE75 簡介與現況 .....	3
參、 RIPE75 2017 年會議 .....	5
一、    IPV6 最新訊息(含 IP 位址政策) IP ADDRESS POLICY .....	7
二、    物聯網 (IOT) 解碼物聯網生態系統.....	20
三、    網際網路互連 法國網際網路狀況：數據互連市場演變與轉換到 IPv6 .....	26
肆、 心得與感想.....	45

# 壹、 前言

網路為人類生活與社會帶來各種不同面向的影響，由網路所衍生的相關議題也隨著科技的演進變得愈來愈複雜且多元。當中包含接近使用權、網路資訊安全、內容產製與傳播、數位經濟與環境、資訊基礎建設等等。

IPv6 網際網路協定對於實現物聯網(IoT)、智能城市和機器對機器(M2M)通信的概念至關重要。這個協定將以其高安全性和大容量特性來滿足不斷增長的內部帶寬/速度需求，克服全球 IPv4 地址資源不足所帶來的挑戰。透過阿拉伯聯合大公國的電信管理局 (Telecommunications Regulatory Authority, TRA) 分享阿聯酋如何利用 IPv6 技術轉型成數據經濟化和智慧城市。

智慧行動裝置大量整合雲端應用服務，使得原有 IPv4 資源無法支應，Network Address Translation 無法滿足行動點對點通訊需求，因此 IPv6 地址大於當前可用的 IPv4 地址，藉以達成未來各項數位經濟、人工智慧(AI)及高科技的生活運。

國家通訊傳播委員會 (NCC) 為掌握歐洲地區網路資訊中心的物聯網(IoT)發展、IPv6 轉換情況、IP 地址政策、域名系統 (DNS) 及網路互連等發展及管理議題，派員參加 2017 年在阿拉伯聯合大公國杜拜召開的 RIPE75 會議，與來自 54 國共計 713 人(會議現場 483 人及線上會議 230 人)，所含三大議題就各項 IPv6、IP 地址政策、DNS 及物聯網 IoT 等議題進行交流。本次會議中分享的國家，包含亞太地區、歐美、非洲及地主國阿聯酋等，除學者專家經驗分享，了解業界最新發展和最佳做法，進行必要的管理和技術協調，以維持歐非區域內互聯網營運，另就各國應用角度提出見解，也從更寬闊觀點，回答來自不同國家與會者的疑問，基於物聯網的本質，提出超越國界的前瞻性看法，有助於激發全球性物聯網發展及管理。此行所帶回諸如科技法律訂定、數位人權保障、數位經濟發展及跨國數據管轄等相關議題最新資料，將有助於未來網際網路治理政策與相關法令之擬定。



國家通訊傳播委員會一行 2 人赴阿拉伯聯合大公國-杜拜參加 2017-RIPE75



Newcomers' Introduction Talk 會場與 RIPE 主席 Hans Petter Holen 先生  
合影

## 貳、 RIPE75 簡介與現況

為區域互聯網 NGO-總部設在荷蘭（阿姆斯特丹），是全球 5 大洲註冊管理機構之一（RIR ），另有 RIR 服務區域包括 ARIN(美洲)，LACNIC(拉丁美洲)，AFRINIC(非洲)，APNIC(亞太地區)等。RIPE 是由廣泛的 IP 網絡感興趣的各方開放的協作論壇，互聯網(IoT)的技術發展以及結構化，管理或管理的方式。它自 1989 年以來一直存在。RIPE 社區是任何個人或組織的統稱，無論是否為 RIPE NCC 成員，都可以參與 RIPE 。



本屆 2017 年歐洲網路資訊中心第 75 次會議參與人員來自世界各地的互聯網服務提供商，網絡運營商和其他利害關係方，透過專家經驗分享，了解業界最新發展和最佳做法，進行必要的管理和技術協調，以維持歐非區域內互聯網營運。為期 5 日會議活動主要探討下列議題：

- 互聯網號碼資源的政策和程序的討論
- IoT,IPv6,DNS 當前的技術引發各項政策及管理問題
- 互聯網社群開發同行網絡開發

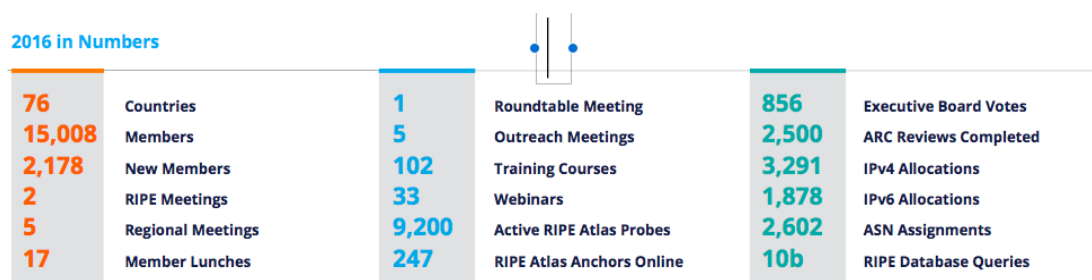
透過以下 4 個工作小組進行開放式討論

- 1.學術合作項目（RACI）
- 2.工作小組（Working Group）
- 3.任務小組（Task Forces）

#### 4. 協作論壇 (RIPE NCC)

作為歐洲，中東和中亞部分地區的區域互聯網註冊管理機構 (RIR)，RIPE NCC 向成員提供互聯網號碼資源，如 IPv4 和 IPv6 地址空間以及自治系統號 (ASN)。它還提供與互聯網技術協調有關的其他服務。是一個開放，透明，中立和公正的組織，其主要運作方式為社區主導由下而上自治組織。工作項目如下：

- 一、負責發放歐洲及中東地區之"IP 位址"、"AS 號碼"、".arpa"網域註冊，以及維護 IP 之 Whois 查詢系統。
- 二、向 RIPE NCC 申請 IP 對象限於該組織之會員，申請時並須簽訂契約，RIPE NCC 會員僅包含一般用戶及 LIR(Local Internet Registry)。與 APNIC 不同，RIPE NCC 並不承認 NIR(National Internet Registry，如 TWNIC、JPNIC、CNNIC 等)，亦即一個國家可以有多個代理發放 IP 組織。
- 三、向 RIPE NCC 申請的 IP 可以自己再發給別人，不限 LIR。但是發給別人的 IP 需要提供建立 Whois 的正確資料。
- 四、RIPE NCC 發 IP 的政策(如一次發多少、每年繳多少年費、如何轉賣、IP 轉移的程序等)由 RIPE 的 ADDRESS POLICY WG 討論提案，在 RIPE NCC General Meeting 會議上投票表決，通過即成為正式政策。政策投票人資格，多數只須事先網站註冊即可，不必是 RIPE NCC 的會員。



2016 RIPE NCC 工作項目及會員數

本次會議地點阿拉伯聯合大公國杜拜是歐洲外唯一 RIPE NCC 辦事處，2017 年網路服務指標全球列第 9 名，並設定 2021 年網路服務指標目標-全球網路服務指標第 1 名。而 5 天 25 堂專業課題其中有三大焦點內容如下：

- (一) IP 地址及 AS 政策
- (二) 目前 IPv6 當前技術所引發各項政策及管理問題
- (三) 互聯網技術、社群及網路等如何成功管理及執行 IPV6 部署

## 參、 2017 歐洲網路資訊中心第 75 次會議



時間：2017 年 10 月 22 日(日)至 26 日(四)。


地點：阿拉伯聯合大公國杜拜捷運世貿中心站旁康萊德飯店 (Conrad hotel)。

行程：

日期	行程
10 月 21 日(六)	由桃園國際機場出發，抵達阿聯酋杜拜國際機場。
10 月 22 日(日)	會場辦理報到手續並參加會議。
10 月 23 日(一)	參加會議
10 月 24 日(二)	參加會議
10 月 25 日(三)	參加會議
10 月 26 日(四)	參加會議
10 月 27 日(五)	由阿聯酋杜拜國際機場，返抵桃園國際機場。

## 會議議程：10月22日(日)至10月26日(四)相關議程



	Sunday 22 October	Monday 23 October	Tuesday 24 October	Wednesday 25 October	Thursday 26 October			
09:00	Tutorial	Plenary	Address Policy	Routing	NRO/RIR Reports			
09:30						Tutorial	MAT	Cooperation
10:00						Tutorial		
10:30	Coffee Break		Coffee Break	Coffee Break	Coffee Break			
11:00	Coffee Break		Connect	Open Source	Closing Plenary			
11:30	Plenary					Address Policy	Anti-Abuse	
12:00	Newcomers' Introduction							
12:30	Lunch		Lunch	Lunch	Lunch			
13:00	Lunch		Lunch	Lunch	Lunch			
13:30	Lunch		Lunch	Lunch	Lunch			
14:00	Opening Plenary	Plenary	IoT	Database	DNS			
14:30						Plenary		
15:00						Plenary		
15:30	Coffee Break		Coffee Break	Coffee Break				
16:00	Plenary	Plenary	RIPE NCC Services	IPv6				
16:30					Plenary			
17:00					Plenary			
17:30								
18:00	BCOP Task Force	Workshop	RIPE NCC General Meeting	Workshop				
18:30	BoF	Workshop			Workshop			
19:00								
19:30								
20:00	RIPE 75 Welcome Event	Networking at Cielo Sky Lounge	DIY Social	RIPE 75 Dinner				
	Meet the RIPE NCC Executive Board							
	RIPE 75 Welcome Reception							

Main Room: level 2
Side Room: level 2
Tutorial Room: level 4



會議主題：

## 1、IPV6 最新訊息(含 IP 位址政策) (IP Address Policy)

### (一) IP 位置發放

國際 IPv4/IPv6 網路位址相關政策是由管理網路資源(如 IP address, AS number, DNS 等)的註冊機構 (Internet Registry)以會員共識決的方式制定。目前管理網路資源是採階層式架構，最高層為主管機關為 ICANN (Internet Corporation for Assigned Names and Numbers)負責 IP 位址分發、指定協定編號、domain name 管理與 root server 管理等 (ICANN IP 管理為 Internet Assigned Numbers Authority (IANA))，底下則由各州所組成的 RIR (Regional Internet Registry)，包括 AfriNIC、APNIC、ARIN、LACNIC、及 RIPE NCC 等。



本次 RIPE75 會議，同往例均有成立專屬 IP 位址政策工作小組，相關議題如下：

一、行政事務：由 NCC 政策發展官員馬可·施密特 (Marco Schmidt) 主講，介紹了歐洲地區和全球政策世界的情況，並看看其他四個地區在同時間最新情勢件，而開講前首先是概述工作團隊一如以往地做了那些豐功偉業，並同步發送每月份郵件列表清單中，及其他四個地區正在討論哪些建議政策及關於政策主題的相關數據等。

二、分配政策：互聯網服務提供商（ISP）和其他組織分配和分配全球唯一 IPv6 地址的註冊管理機構政策是經由 AfriNIC、APNIC、ARIN、LACNIC、及 RIPE NCC 社區協定的共同討論而形成的。且 IPv6 地址空間是一種公共資源，地址空間管理涉及平衡等一系列有時相互競爭的目標。

	APNIC	RIPE
IPv4	禁止在最後/ 8 中轉移 IPv4 地址塊” (Last Call)	專用的 IXP IPv4 池 採用 32 位 ASN 分配的 PI /無轉換成 PA <ul style="list-style-type: none"> <li>•~2500 PI 分配轉換為 PA</li> <li>•~500 個 NOT-SET 賦值轉換為 PI / PA</li> <li>•~200 作業已被刪除</li> <li>•~1500 份作業仍在進行中</li> </ul> 分配 PI - 沒有設置 - 早期註冊 <ul style="list-style-type: none"> <li>•添加到定義</li> <li>- LEGACY</li> </ul>
IPv6	NIR	PI 分配不能被進一步分配到其他組織”。

三、何謂 IPv6 網際網路協定：2016 年底全球 RIR 已將 IPv4 發放完畢，代表即將資源耗盡且智慧行動裝置大量整合雲端應用服務，使得 IPv4 資源無法完全支應，另有網際網路協定第 6 版，設計目的是取代 IPv4 等。

(一)IPv6 優點：

IPv6 的位址格式則採用 128 位元長度，其位址能提供 2 的 128 次方個。它所能提供的 IP 位址，遠遠超過 IPv4 的數量。IPv6 與 IPv4 不能進行相互操作(IPv6 does not interoperate with IPv4)。

移除未使用或不必要的欄位以簡化標頭長度(Simplify IP headers to remove unused or unnecessary fields)：降低 router 轉送 IP 封包的處理時間。固定標頭長度，使晶片設計師和軟體工程師更容易研發(Fixed length headers to make it easier for chip designers and software engineers)。

整合 IPsec 安全協定(IPsec is integrated)：IPv6 已整合網際網路安全

協定 (Internet Protocol Security, IPsec), 傳輸資料可執行加密及身份驗證, 增加 IPv6 安全性的保證。IPv6 刪除廣播機制(No more broadcast)。

(二)如何取得 IPv6 網路位址：

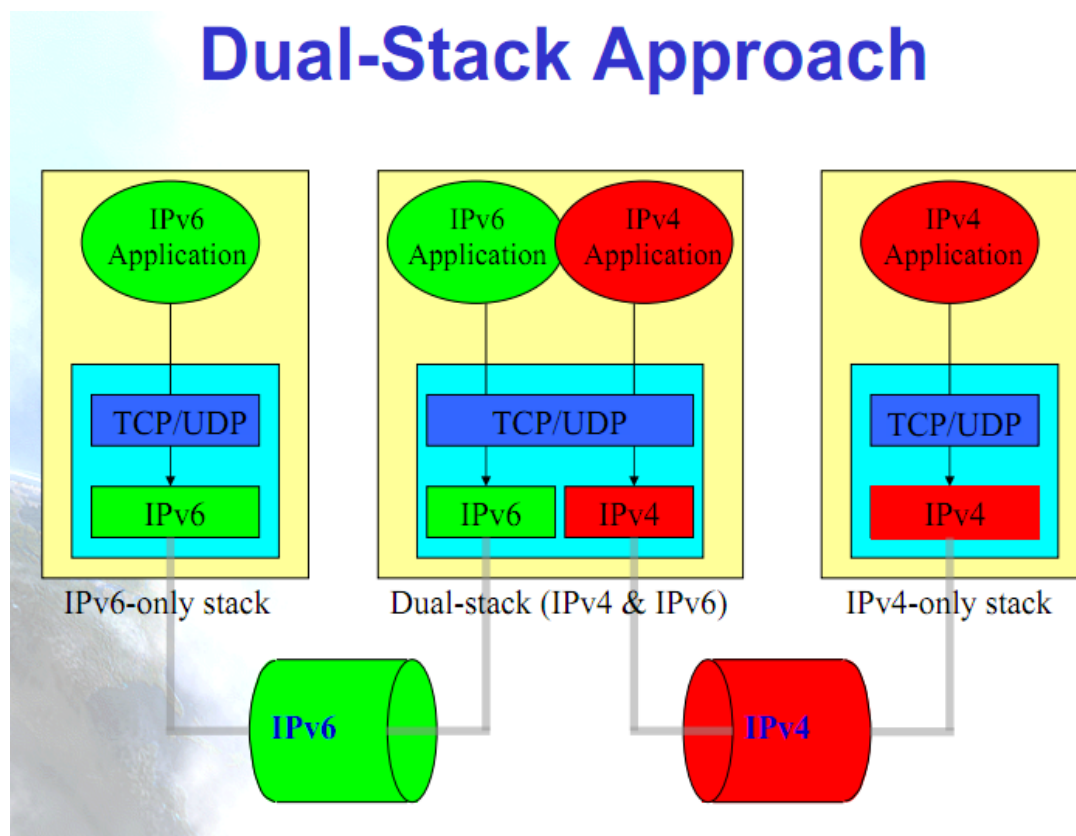
1. 一般商業或個人用戶, 可向所屬的網際網路服務供應商 (Internet Service Provider, ISP) 申請。
2. 國內網際網路服務供應商若要取得 IPv6 網路位址者, 可向財團法人台灣網路資訊中心。

(三)IPv4 與 IPv6 過渡及共存方式(如架構圖)：

網路環境要從 IPv4 轉換到 IPv6, 因網路設備需要非常長的一段時間才能完全汰換, 故如網路環境不能短期從 IPv4 轉成 IPv6, 轉換過渡及共存方式有三種, Dual Stack、Tunnels 及 Translation, 分例如下：

1. Dual Stack (IPv4/IPv6 雙協定堆疊)：係為網路上之網路裝置同時支援 IPv4 和 IPv6 協定。

網路環境裝置換成支援 Dual Stack 之裝置即可, 但增加網路環境的複雜度, 網路裝置的效能會因此被兩種協定瓜分因資料傳

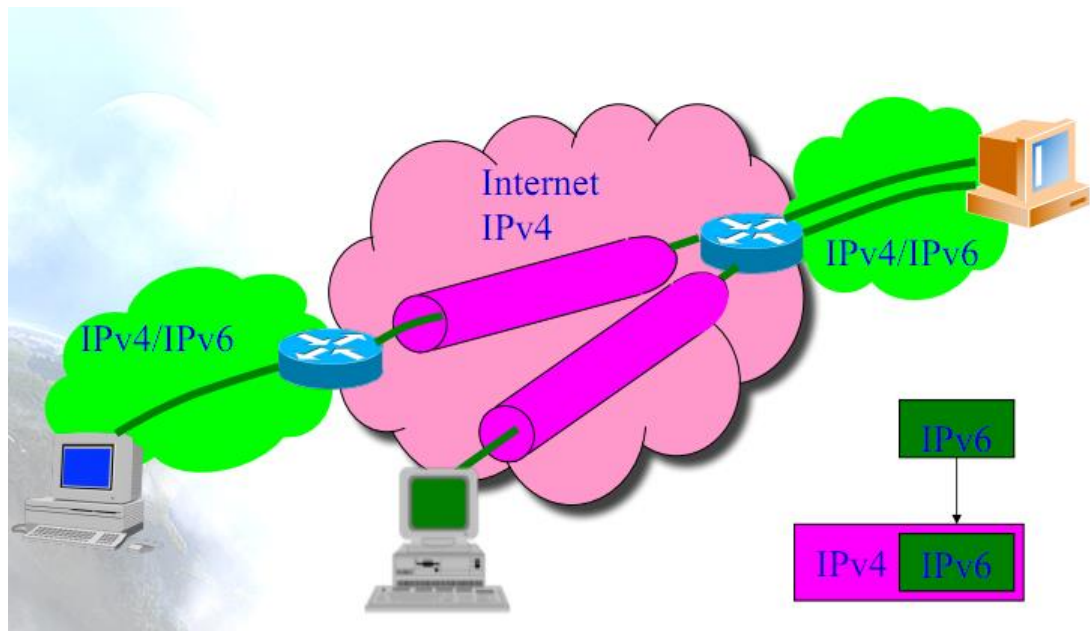


輸路徑有純 IPv4 或 IPv6 之網路節點，網路裝置必須同時消耗 1 個 IPv4 及 IPv6 位址。

## 2. Tunnel (隧道):

Tunnel 是以透過 IPv4 網路建立虛擬的網路隧道，來傳輸 IPv6 封包，IPv6 封包在進入隧道端點前，會包裝成 IPv4 封包，再藉由 IPv4 網路傳輸到另一個隧道端點，抵達後就轉換回原有的 IPv6 封包。其缺點為封裝 IPv6 封包及解封裝 IPv6 封包之步驟進行時，會對網路裝置增加額外的運算負擔。

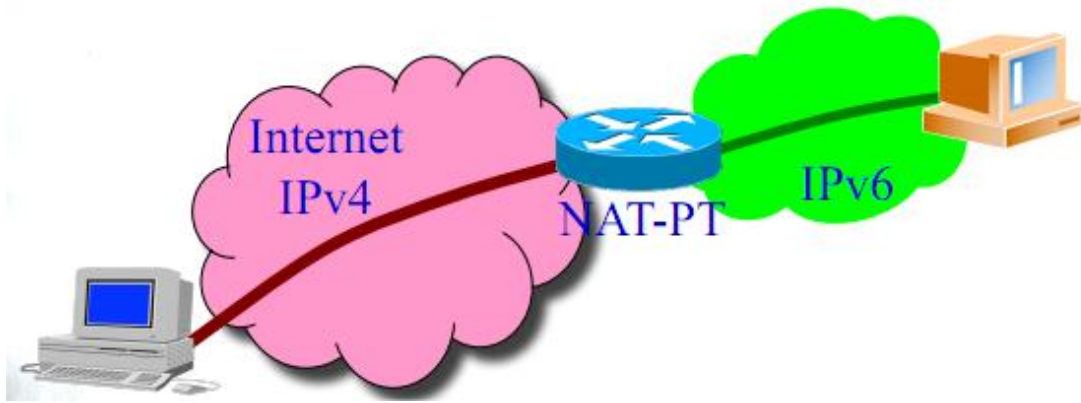
IPv4/IPv6 Dual Stack 架構圖



IPv4/IPv6 Tunnel 架構圖

## 3. Translation(轉譯):

因 IPv4 與 IPv6 封包格式完全不同，所以不能互相連線，若以 NAT-PT(Network Address Translator - Protocol Translator)充當兩者間的翻譯後，就能夠讓 IPv4 與 IPv6 網路位址互相轉換格式。NAT-PT 會建置在 IPv4 與 IPv6 的交界節點上，讓 IPv4 與 IPv6 互相連線，不用改變現有網路環境，但需在 IPv4 與 IPv6 的交界節點上建置 NAT-PT。



IPv4/IPv6 Translation 架構圖

#### (四)IPv6 特性：

IPv6 地址空間是一種公共資源，必須謹慎管理，以符合互聯網的長遠利益。地址空間管理涉及平衡一系列有時相互競爭的目標。

##### 1. 唯一性(only)

每個地址空間的分配和 / 或分配必須保證在全球範圍內的獨特性。這是確保互聯網上每個公共主機都能被唯一標識的絕對要求。

##### 2. 註冊(Registers)

互聯網地址空間必須在互聯網社區的成員可以查詢的數據庫中註冊。確保每個互聯網地址的獨特性以及為從所有 RIR 和 IR 到最終用戶的各級互聯網故障排除提供參考信息是必要的。註冊的目標應該在合理的隱私考慮和適用法律的範圍內應用。

##### 3. 最佳路由聚合效率

地址空間應盡可能按照網絡基礎設施的拓撲結構分層分佈。這對於允許 ISP 的路由信息的聚合以及限制 Internet 路由表的擴展是必要的。

IPv6 地址規劃方案影響全網路由聚合能力。IPv4 地址缺乏層次結構，地址分配和管理缺乏統一規劃，導致網絡路由效率低下。IPv6 地址規劃標榜路由效率最佳化：地址空間分成 3 層，使路由資訊匯總變得更精簡，不僅可縮短主機回應時間並將流量負載分散節省頻寬的首要任務在於減少網絡地址碎片，增強

路由聚合能力，降低路由器等設備的 CPU、內存等消耗，提高網絡路由效率。

IPv6 地址分配方案影響地址的有效管理。當前對已分配的 IP 地址，我國尚缺乏有效的管理手段。通過科學規劃 IPv6 地址方案，有利於提高我國在互聯網收到攻擊時的網絡溯源能力，保障網絡安全性和可信任性。

#### 4. 公平

與使用公共地址空間有關的所有政策和做法應當公平，公平地適用於互聯網社區所有現有和潛在的成員，不論其位置，國籍，規模或任何其他因素。

#### 5. 小結

IPv6 自動註記資料種類及標記有助於服務品質管控動態主機自動配置及表頭可擴充性，縱使 IPv6 有這麼多優點，智慧行動裝置大量整合雲端應用服務，內容為王的世代，網路的管理及各利害關係人的改善變得相對重要，例如資料管轄權，地址是否要實名管理之類的等等。

#### (五) IPv6 PI地址空間政策



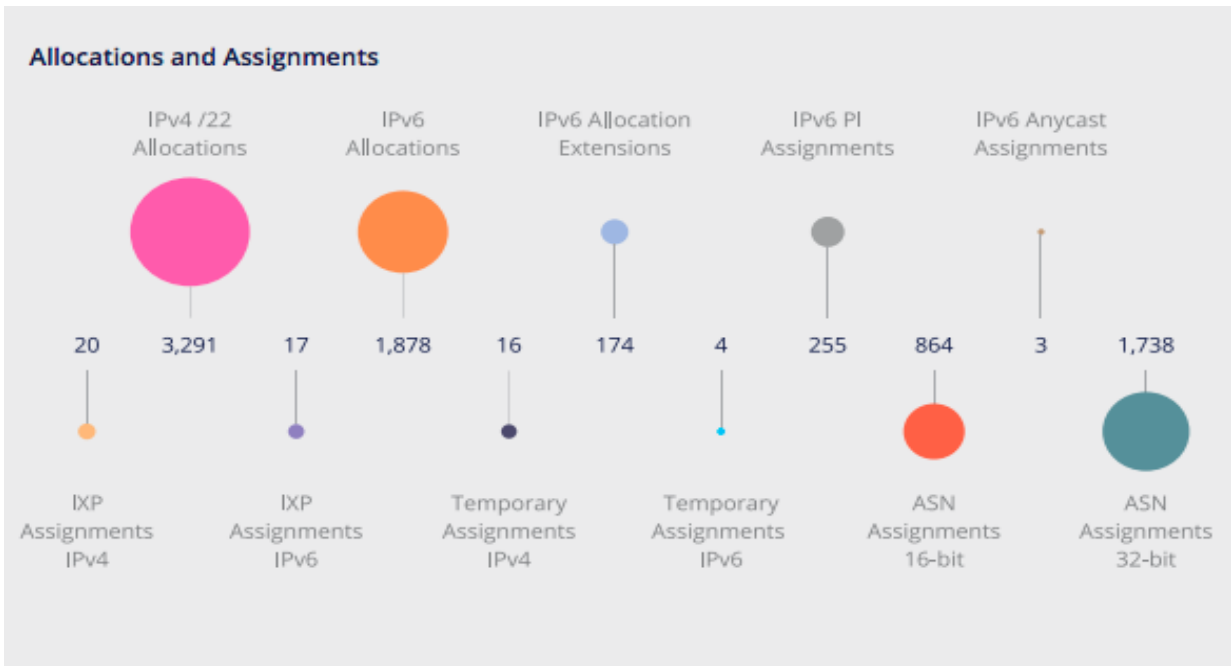
RIPE NCC根據“IPv6地址分配和分配策略”分配IPv6提供商無關(PI)前綴。小於a / 32的IPv6 PI分配取自2001:678: / 29: 路由決策是網路運營商的責任。

## 1. 分配及分派政策 ( **Allocations and Assignments** )

	分配	註冊
RIPE	<ol style="list-style-type: none"> <li>當持有 IPv6 地址分配的組織進行 IPv6 地址分配時，必須將這些分配註冊到相應的 RIR 數據庫中。</li> <li>這些註冊既可以作為單獨的作業，也可以插入一個狀態值為“AGGREGATED-BY-LIR”的對象，其中作業大小屬性包含對最終用戶作出的各個作業的大小。當超過 1/48 被分配給組織，它必須在數據庫中註冊為一個狀態為“ASSIGNED”的獨立對象。</li> <li>在進行審計或提出後續分配請求時，LIR 必須能夠以 RIR 的方式顯示統計數據，該統計數據顯示所有對象的狀態為“AGGREGATED-BY-LIR”能夠計算和驗證實際的 HD 比率。</li> </ol>	<ol style="list-style-type: none"> <li>當持有 IPv6 地址分配的組織進行 IPv6 地址分配時，必須將這些分配註冊到相應的 RIR 數據庫中。</li> <li>這些註冊既可以作為單獨的作業，也可以插入一個狀態值為“AGGREGATED-BY-LIR”的對象，其中作業大小屬性包含對最終用戶作出的各個作業的大小。當超過 1/48 被分配給組織，它必須在數據庫中註冊為一個狀態為“ASSIGNED”的獨立對象。</li> <li>在進行審計或提出後續分配請求時，LIR 必須能夠以 RIR 的方式顯示統計數據，該統計數據顯示所有對象的狀態為“AGGREGATED-BY-LIR”能夠計算和驗證實際的 HD 比率。</li> <li>當 RIR / NIR 將 IPv6 地址空間委派給組織時，它也委派管理與分配的 IPv6 地址空間相對應的反向查找區域的責任。每個組織都應妥善管理其反向查找區域。在進行地址分配時，組織必須根據請求委託給受讓組織，負責管理與分配的地址相對應的反向查找區域。</li> <li>持有一個或多個 IPv6 分配的 LIR 能夠請求將這些分配中的</li> </ol>

		<p>每一個擴展到 1/2，而無需提供進一步的文檔。</p> <p>6. RIPE NCC 應該與 LIR 現有的分配連續分配新的地址空間，並避免在本政策部分下分配不連續的空間。</p> <p>7. 任播 TLD 和 0/1 層 ENUM 名稱服務器適用的組織是 TLD 管理者，如國際電聯指定的 IANA 根區數據庫和 ENUM 管理員所記錄。該組織每個 TLD 可以接收最多四個/ 48 個前綴，每個 ENUM 可以接收四個/ 48 個前綴。如 BCP126 /<a href="#">RFC 4786</a> 中所述，這些前綴必須僅用於為所述的 TLD / ENUM 選播權威 DNS 服務器的唯一目的。</p> <p>8. 權威 TLD 或 ENUM Tier 0/1 DNS 查詢服務的分配受 RIPE 文檔 “<a href="#">RIPE NCC 服務區域內提供商獨立資源持有者的契約要求</a>” 中描述的策略的約束。</p> <p>9. Anycasting 任務在 RIPE 數據庫中以 “ASSIGNED ANYCAST” 狀態註冊，如果不再用於提供權威 TLD 或 ENUM Tier 0/1 DNS 查找服務的基礎設施，則必須將其返回給 RIPE NCC。</p>
--	--	--





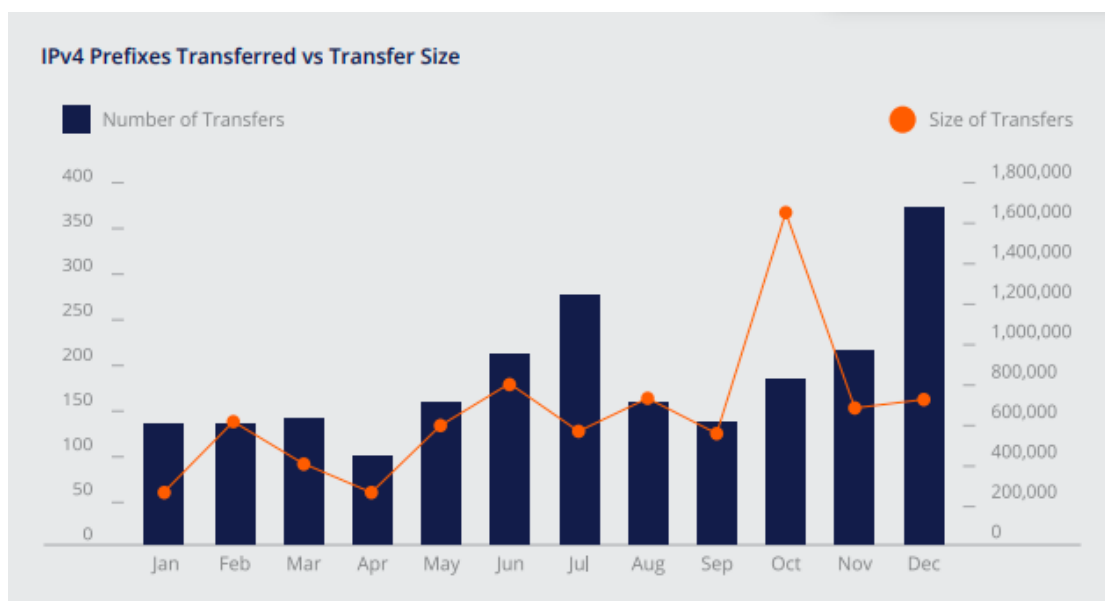
IPv4 及 IPv6分配及分派圖

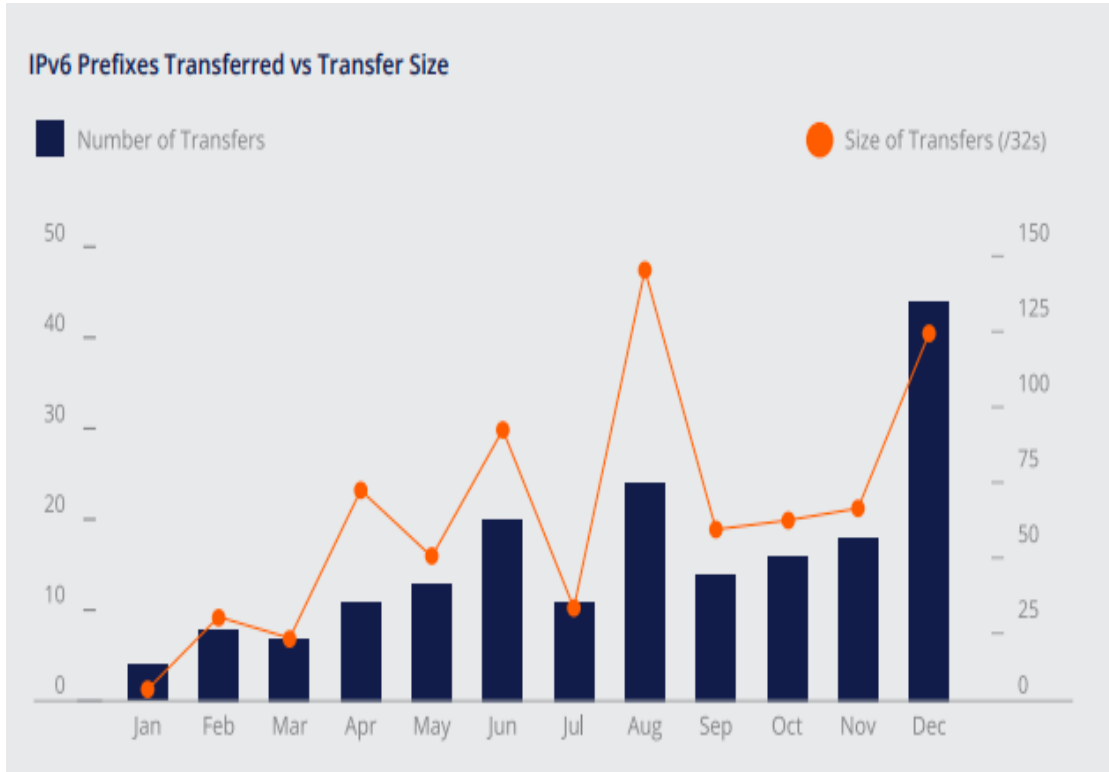
截至 2016 年底，共有 11237 個 LIRs 進行 IPv6 分配，相當於 RIPE NCC 成員的 74.8%，而 2015 年底為 75.4%。

2016 年的自主系統編號（ASN）分配比 2015 年高出 2.3%。自 2009 年以來，RIPE NCC 默認分配了 32 位（或 4 字節）ASN。為鼓勵了採用新格式。2016 年，RIPE NCC 服務區域中 ASN 佔 66.8%。190 個 IPv6 傳輸。其中，170 個屬分配（714 / 32s），20 個屬分派（20 / 48s）。

在 2016 年，RIPE NCC 處理了 418 個 ASN 轉賬。

註：本部分統計資料中不包括因合併或收購等公司結構變化而產生的轉移。



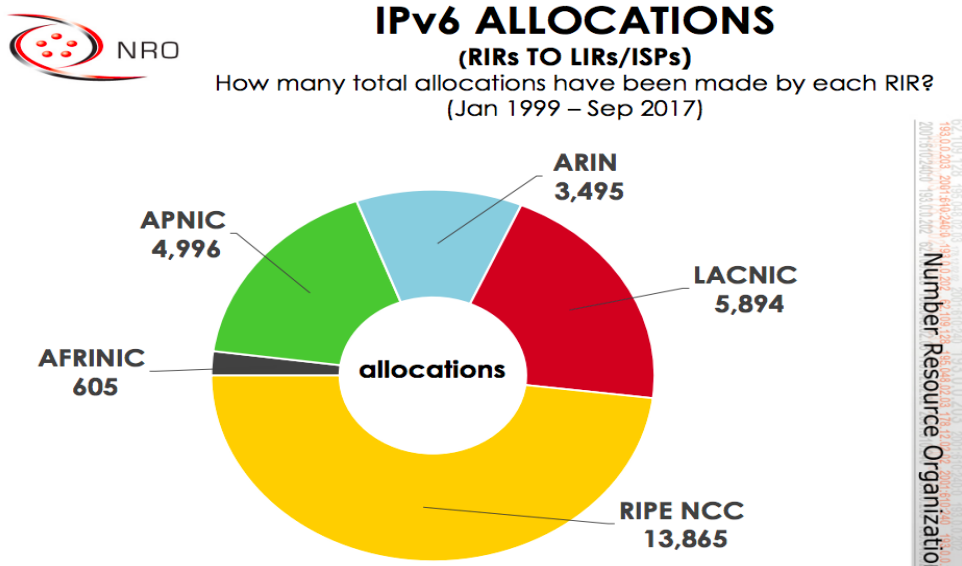


## 2. 國際 IPv4 網路位址移轉（歐亞比較）

政策	RIPE	APNIC
IPv4 販售	非會員公司及個人可申請，可販售，但仍需 RIPE 審查核可。	可販售但僅限 APNIC 成員
同意 IPv4 轉移	同意，但不認同未授權的移轉	不承認位址空間的出售或未授權移轉，並將此類移轉視為無效的行為。APNIC 要求進行此類移轉的組織交回位址空間予適當的註冊管理機構。5 年內不能轉移，甚至不能主動整併
IPv4 位址移轉接收者相關規定	限定 RIPE 會員 須經 RIPE 依政策進行 評估確認需求後，方能 接收被移轉的 IPv4 位址。	限定 APNIC 會員 接收端必須負責有效 使用所掌握的 IPv4 位址資源，包括所有移轉 過去的位址。 移轉網段移轉的最小單位為 /24，且必須是由

		APNIC 所管理並配置或發放予 APNIC 會員 RIR
註冊審核	AFRINIC 另 Whois 數據庫反停止政策、互聯網號碼資源審查、軟著陸政策則等議題仍後續研議發展中。 AFRINIC 另 Whois 數據庫反停止政策、互聯網號碼資源審查、軟著陸政策則等議題仍後續研議發展中。拉丁美洲、東亞、東南亞、南亞及大洋洲等 IPv4 仍然有大約三分之一的可用，有關 ASN 及 RIR 的移轉仍在區域持續發展中，且正致力於推動 IPv4 的移轉及 IPv6 的教育訓練，另 IPv6 址今年 1 至 10 月從 50%成長至 56%，未來仍透過組織運作，加強全球合作。	即將用罄，已加強 IPv4 及 IPv6 的介接教育訓練中。
號碼爭端解決		
使用 (Whois) 數據庫和隱私問題		
提供執法單位必要訊息		

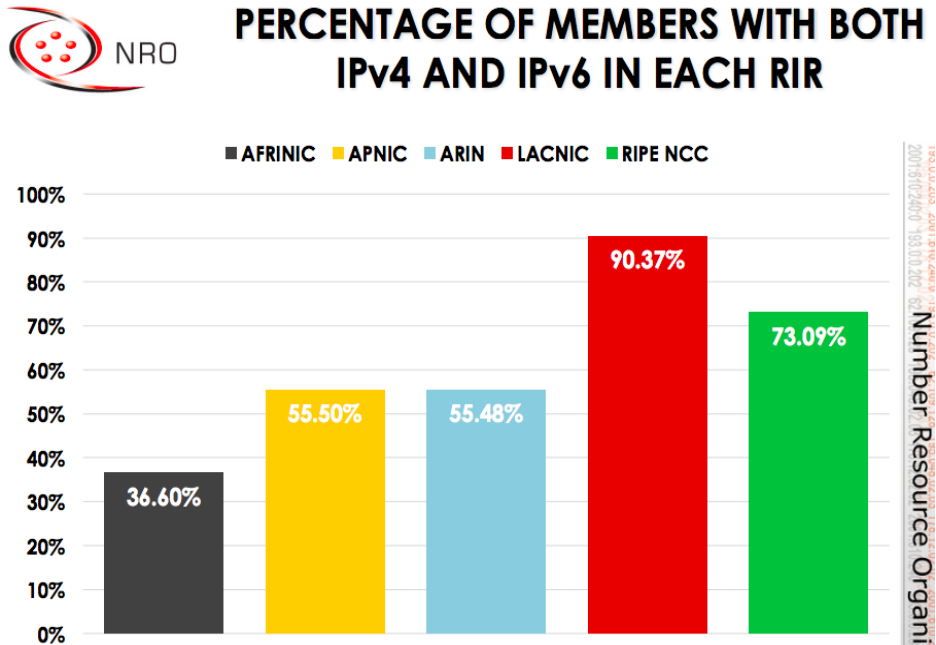
IP 資訊的公開是治理的方法之一，基於 IP 位址為公共資源的特性，以及減少資訊取得成本、減緩資訊不對稱的情形，建議宜評估 IPv4 位址移轉歷程資訊公開的必要性及公開方式。公開方式可以參考 WHOIS 資料庫作法，或在目前 TWNIC 網 站中「IP 位址代理發放單位取消代理發放權公告」的頁面增加 IPv4 位址移轉的來源端、接收端等等的歷程資料。



RIPE NCC IPv6 ISP 及終端用戶分配情況

### 3.RIR 間轉移

2016 年，RIPE NCC 處理了 126 個 IPv4 RIR 間轉移，共有 1753344 個 IP 地址。其中，77 是 PA 分配（1,055,488 個 IP 地址），45 個是傳統資源（691,456 個 IP 地址），四個是 PI 分配（6,400 個 IP 地址）。



在 126 次轉移中，有 14 次來自 APNIC，RIPE NCC 有 100 次，ARIN 來自 RIPE NCC；三名從 RIPE NCC 到 APNIC，九名從 RIPE NCC 到 ARIN。2016 年沒有 RIR 間 IPv6 或 ASN 轉移。

### 4.DNS 是否該命名

這個目標在 IPv6 尋址中特別重要，其中總地址池的大小對內部和外部路由 DNS 是否該命名由講師 Sandoche Balakrichenan 主講，講者先從一些術語先定義，如身分(Identity)：可定義和可識別、不需要獨特，不需要遵循任何特定的“命名公約”。

識別碼(Identifier)：識別物理或虛擬對象的獨特方式。應該跟著特定命名約定；位址(Addressing)：識別範圍內的物理或虛擬對象的唯一方式通訊、需要遵循特定的“命名約定”（例如郵政地址，IPv4/IPv6，MAC 地址）；

命名服務(Naming Service)：將唯一識別碼對應到其相應的唯一服務/資訊，次說明網際網路的域名(DN)識別碼配置是屬於階層式的，識別碼的命名約定是由命名機構 IETF 所定；為因應物聯網發展，使事物在物聯網中可識別，於是講者提出 EUI-48 and EUI-64 的命名約定，域名識別碼配置包含國家碼、公司碼、產品身分及序號等由 96 位元所組成，另提出為物聯網命名服務要求：包含

必須可擴展、必須為舊的和新的命名約定工作、應適用於階層和平面識別碼等條件，有別於網際網路的域名命名服務是由 IETF 所定，而物聯網的命名服務需由不同的標準組織訂定，講者提出的觀念尚須審慎評估可行性及國際趨勢，再決定我國應採取之態度。

AFRINIC 另 Whois 數據庫反停止政策、互聯網號碼資源審查、軟著陸政策則等議題仍後續研議發展中。AFRINIC 另 Whois 數據庫反停止政策、互聯網號碼資源審查、軟著陸政策則等議題仍後續研議發展中。LACNIC 東亞、東南亞、南亞及大洋洲等 IPv4 仍然有大約三分之一的可用，有關 ASN 及 RIR 的移轉仍在區域持續發展中，且正致力於推動 IPv4 的移轉及 IPv6 的教育訓練，另 IPv6 今年 1 至 10 月從 50%成長至至 56%，未來仍透過組織運作，加強全球合作。

互聯網號碼分配機構（IANA）已將最後的五/八塊 IPv4 地址空間分配給五個地區互聯網註冊管理機構（RIRs），根據成熟的 436 號“全球剩餘 IPv4 地址空間分配政策”（）這意味著 IANA 免費的 IPv4 地址空間池已經耗盡。

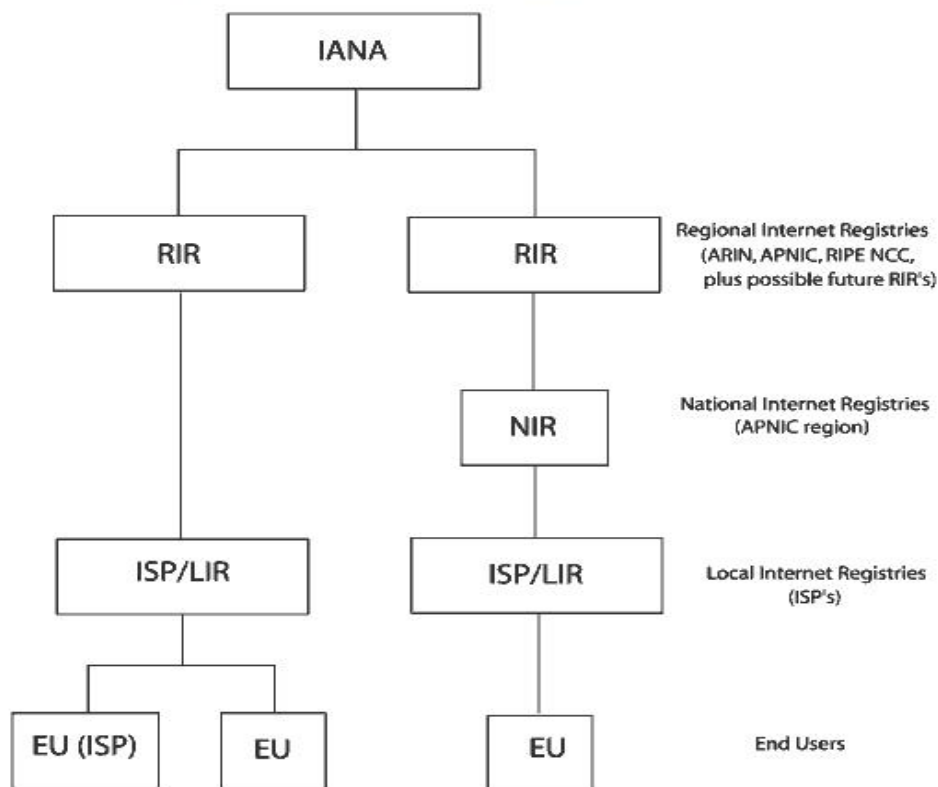
五個地區互聯網註冊管理機構（RIR）在健全的治理框架內運作，確保其公司結構的有效性，流程的透明度以及對成員和社區的問責制。根據法律要求和地區政策，這些框架在五個 RIR 中有所不同，但都是透明可訪問和公開記錄的。它提持有者或會員的 IPv4 歷史位址空間持有者；組織間的合併、收購及接管。

小結：

本次會議有提供法國相關的市場現況資料包含 IX 或在 IPv6 轉換及國家數據互連(Data Interconnection)Peering 經驗 Paid peering 情況或可對台灣網際網路互連之研究有所突破，另外該國 IPv6 的轉換一些推動經驗，如對使用者宣導或協調利害關係人改善等方式，可提供我國未來推動 IPv6 之參考。

## 5. IPv6 地址空間分配 (IPv6 Working Group)

IPv6地址空間的管理責任按照如下所示的分層結構進行全球分配。



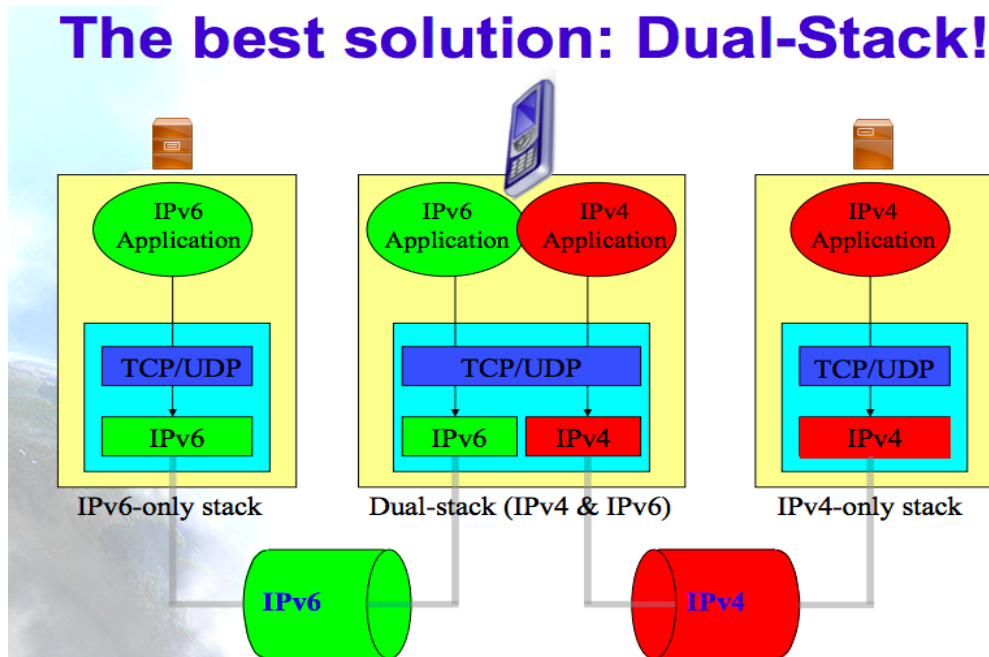
整體架構重點如下：

- 一、採階層式架構- IP 位址分發、指定協定編號、domain name 管理與 root server 管理。
- 二、RIPE 不承認 NIR，RIPE 申請 IP 的對象限該組織會員，申請時並須簽訂契約，會員僅一般用戶及 LIR(Local Internet Registry)，亦即一個國家可以有多个代理發放 IP 組織，APNIC 為獨家代理。
- 三、IPv6 地址空間是一種公共資源，不應視為個人財產，而地址空間管理涉及平衡，要如何達到 IPv6 全面普及？RIPE 將地址空間 policy 分成分配、移轉、註冊 3 大區塊及數據互連(Data Interconnection)來討論。

國際 IPv4 網路位址回收政策

- 一、督促業者保持 IPv4 位址的高使用率，維持正確的 whois 資料庫，並確實讓取得的 IPv4 位址在 BGP routing table 上也大都能看的到，避免產生被回收的疑慮。
- 二、由於回收的難度高，不建議以回收政策為解決 IPv4 枯竭問題的主要策略。但可以在 IPv4 位址枯竭後(IANA final /8 後)，卻急需 IPv4 位址

時， 檢討並執行現有之 IPv4 位址回收政策，並將回收之位址以移轉 (transfer policy)方式，釋放給需要 IPv4 位址的單位。



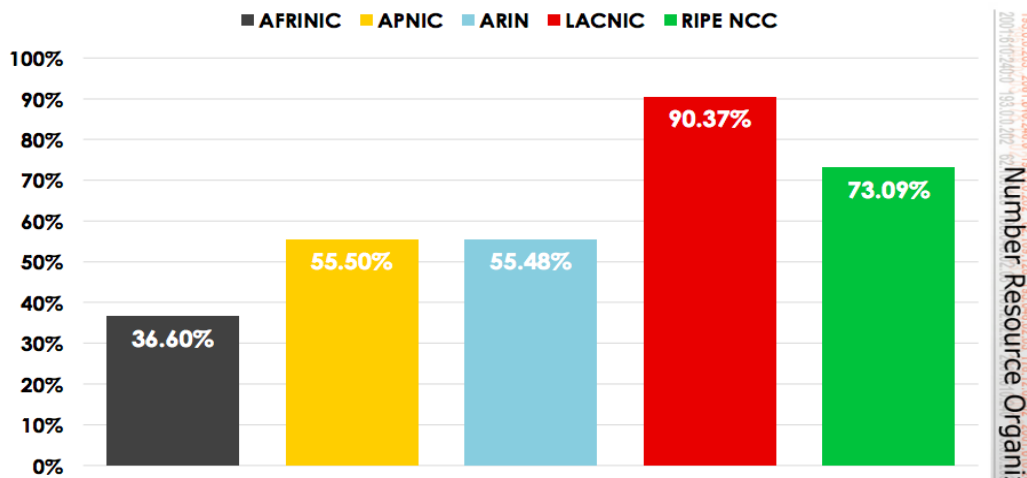
IPv6 地址分配及網路部署雙軌並行：

網路在 IPv6 的原始設計中，處理大數據領域有兩件事情基本相當。其一為知識產權本身在 20 世紀 80 年代和 90 年代取得如此成功因素之一，就是它可以處理不同的數據包大小和碎片。其二是我們運用 IP 而不是 DECNET 全部原因可能是因為它碎片處理剛剛更有彈性。

我們在 IPv6 中發現一些變化。首先是將分段控制字段移出來成為可選的。其次“不分片”位被卡住，路由器不能運行。所以在 IPv4 中，總有一個數據包前進模式，如果它不能被推到下一階，路由器是相當有能力碎片包並發送它，只要他們的片段有設置本功能。在 IPv6 中，它開始看來像一個 3G GP 網路圖，當這個數據包遇到不能前進路由器時，它必須丟棄該數據包，但是在它必須成為一個太大的 ICMP 數據包，並且“太大”訊息不會傳遞給它。而來源是取決於發生了什麼訊息。IPv6 可以發送片段訊息，現在沒有幾次需要從網路中發送一個數據包。而對於所有的民間運轉 MPLS 是一件好事，因為 MPLS 是個單向隧道，你不能保證一旦在路徑中找到問題，你就有答案，因為它肯定不會是標籤路徑後，您的標籤路由器上可能沒有完整的路由。想一下 IPv6 是要求做什麼，且試著知道你能做什麼，答案可能是不能的。很多時候，您需要從網路中間發送一個數據包，而對於所有民間運行 MPLS，因 MPLS 是一個單向隧道，你不能保證一旦在路徑中找到問題，你就有希望倒退，因為它肯定是不是標籤路徑向後，您的標籤路由器上可能沒有完整的路由。



## PERCENTAGE OF MEMBERS WITH BOTH IPv4 AND IPv6 IN EACH RIR



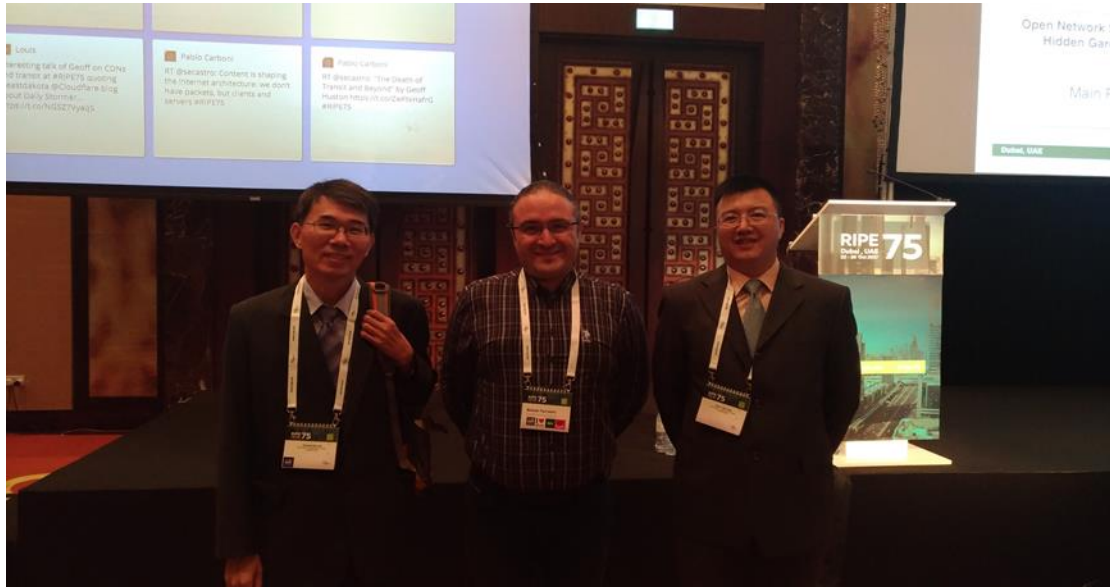
發送方收到該 ICMP 消息時會發生什麼？這是一個非常好的問題，因為它是發件人，而不是路由器。因此，如果該片段第一個前導部分已含一個 TCP 控制域，那麼發送方將要將該審核發送回相關 TCP 控制域。而且我們現在發明了一個 TCP 之前不存在的新 TCP 信號，它被稱為 Nack，因為該訊息是隱含的，我沒有發送，你必須重新發送一個不同的訊息。因此，在 TCP 中絕對不會將其分解，主要用意是將訊息傳遞給控件者且是重新發送一個新的 TCP 訊息大小。對於 UDP 是一個數據報，有個小細節東西沒有做？是我已經忘記了已經發訊息了，這是個問題。因此，將它實現在存儲某種每個主機轉發路徑中，若是一個修訂的 MSS，我需要重新使用這個 MMS 和片段，若要再次發送該數據包。有些操作系統根本不做任何事情，為什麼他們會得到訊息？原因在對於那些運行 Anycast 的人來說，誰在運行 Anycast？而且為什麼任何 IP 網絡中返迴路徑不一定與轉發路徑相同。若您的 Anycast 部署密集，則返迴路徑上最接近路由器的 Anycast 實例可能不是發送大數據包的 Anycast 實例。

因此，對部署進行維護以及正在運轉時，真正需要適用 IPv6 的 ICMP 訊息將會轉移至 Anycast Cloud 錯誤實例。屆時運轉停止了且不能調整，因錯誤實例已經收到相關訊息且沒有解決掉這個問題。對於那些運轉 TCP 和 Anycast 的情境中，若真是沒辦法解決這個問題，它變得難以置信的複雜思維。對於那些在 IPv6 上運行 Anycast 情境的使用人。

至於路徑中的 IPv6 碎片擴展頭，有關 IPv6 於數據變化時間長短的爭論，是如果你有可變地址連接或變量等，超高速交換設備沒有時間處理標題，因為它必須解釋標題，而不是看到一個修復大小的契合偏差。所以我們今天開始做真正廉價且適宜的產品，當插入接收端頭時，傳輸控制域移動到數據包端中未知和可變偏移量。如果只有 30 個指令周期，即使在世界上所有的 Intel DPDK 中，您可能不會在可用於處理數據包周期內找到傳輸頭。我們發現，有大量的設



備，當它看到一個接收端頭的 IPv6 數據包，但只有一個接收端時，它會降低處理效能。所以，碎片看起來很糟糕，由於 ICMP PTB 處理，藉由 DNS 由於接收端頭處理所引起的反向信令，來解決這個難題。



會中有提個很好的例子：一個權威名稱流覽器，它只適用在 IPv6，而不能在 IPv4 中存在，且只提供 IPv6 境域中。所以當我要求 Google 通過 IPv4 向我的權威名稱流覽器詢問有關我的特殊域名問題時，Google 無法處理，因為總共大於 1,500 個八位字節，超過 IPv4 工作範圍，且發現 UDP 緩衝區大小，Google 回送給我們才可加以處理 4096 所發送任何你想要的數據包。DNS 顯然希望碎片正常工作，這正在發生，緩衝區大小表示我們可以控制這一點，但您知道在 IPv6 中並沒有太好的效果。尾隨的碎片總是遇到防火牆和過濾器的問題，因此整個不匹配的問題將成為一場噩夢且不易處理。在 DNS 中，如果真的被卡住移動到 TCP 時，只有當收到一個截斷的回應時，靜默的 drop 不會被切斷，所以這種魔法問題的靜默丟棄屬性不會導致 DNS 使用 TCP，因此在這種情況下，TCP 並不希望得到這不好的結果。但只要你還有 IPv4 存在就不是什麼大問題，大家都沒有動力去解決它，甚至發現 Google 並無立即修復它，因為這問題不可能讓用戶來抱怨。

當大型流覽器發送大數據包時的接收器丟棄率大約在 30%到 40%之間，但是向流覽器傳送大數據包，是最通常不過的事。流覽器無論是 DNS 或網絡，負責傳送大數據量，我會對此感到好奇，我認為可以做相反的事情，可以傳送真正的大 IPV6 數據包回到目的地，想看看會發生什麼情境!就像 Google 廣告一樣簡單，因為我使用這個廣告平臺來測量大型的互聯網的各種方法和一個你得到的答案，DNS 答案可以在 IPv6 中分散，所以 URL 及 TCP 對話。所以我們在做的第

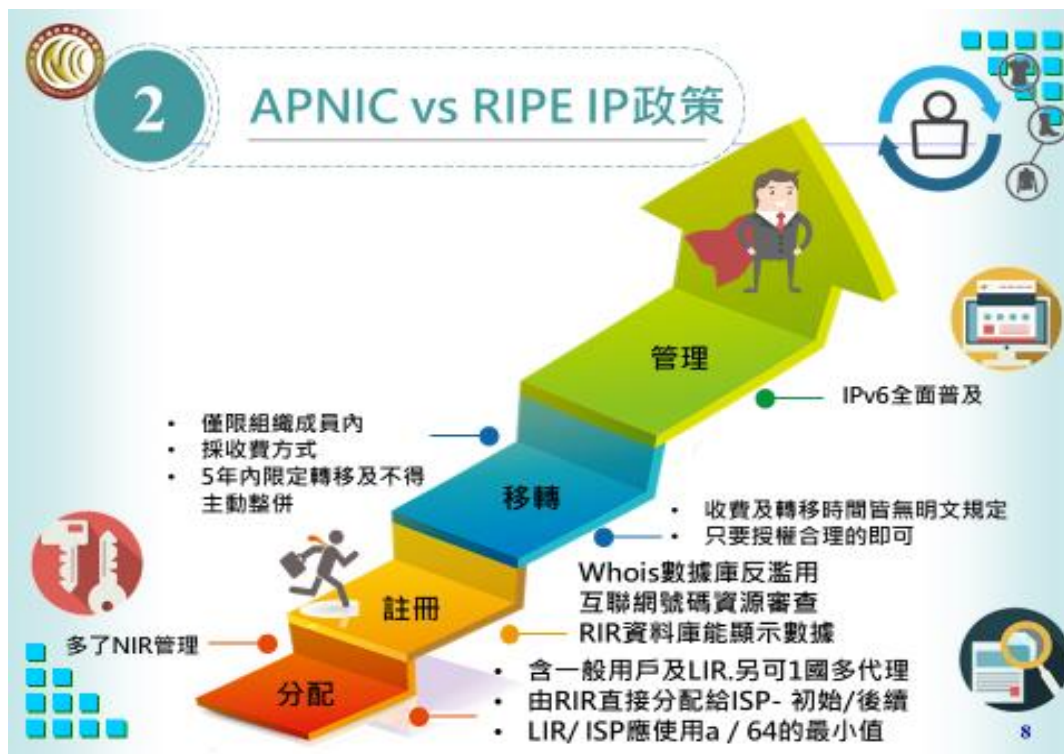
一件事是發回零碎 IPv6。因為我使用這個廣告平臺來測量大量的各種互聯網方式，一起做一個 get，DNS 的答案可以在 IPv6 中分片，我會用 DNS 做一個小技巧，以確保我了解發生了什麼。而對於 DNS 來說，因為我對這個流覽器名稱的查詢的響應進行了彌補，並使其分散。如果 DNS 解析器成功接收到分散的 IPv6 資源，您將只會查詢目標名稱。所以，我做了這個 1080 萬次，我覺得夠了，但在這一點上，你看到足夠的互聯網是代表性的，失敗率為 108 萬，400 萬，38 %。哪個解決方案，10,000 人參加，三點半到三點六五分顯示我們有問題，所以列出所有這些都將是一個乏味和漫長的時間。

另一個問題是 AS 的網絡，谷歌在 Sprint 某處是從斯洛文尼亞的 SNET，這些與您的 DNS 解析器無法接收分散的 IPv6，無論什麼原因，它根本沒有得到，那就是 DNS，這意味著沒有人會認真的通過 DNS 在 IPv6 上運算大數據包，因為它不起作用。TCP 呢？同樣的方法是設置一個流覽器並修改數據包處理程序，以便它們在得到你之前總是將 TCP 數據包分解。所以用運算它，發現在 IPv6 和 434,000 中運行了 190 萬個不同的端點，當嘗試發送分片 TCP 時，它失敗率為 22%。如果是 ISP，而正在運行的服務的失敗率為 22%，這算比較糟糕的了，有很多人在討論分散 TCP 的問題，分散的 IPv6 問題在各階層做 IPv6，這是很有趣的事，且世界各地都有。

目前發現有兩個問題：整個分散和防火牆的問題。但這第二個問題是，中級或甚至便宜的切換裝置希望看到傳輸分組，並且當存在接收端頭時它們不能放棄分組。所以有很多網絡設備，只有看到擴展頭。但現在樂觀是拉入 ICMP PTB 訊息，且只是分散了一切，並沒有等到彼此的發送包太大，只是把它分解，這並不考慮 ICMP PTB 已知訊息的問題。

如果正在運作 IPv6 唯一的互聯網，唯一可以假設的是它們不運作 DNS，因為它不能一起工作，特別是 DNSSEC，因為如果真的善用 IPv6 協定資源，而且我們必將 DNS 和 DNSSEC 安全性納入，那麼今天組合就不會對大家有所助益。

## 6. APNIC 與 RIPE IP 地址政策之比較



## 完善的網路治理及推動 IPV6 之建議

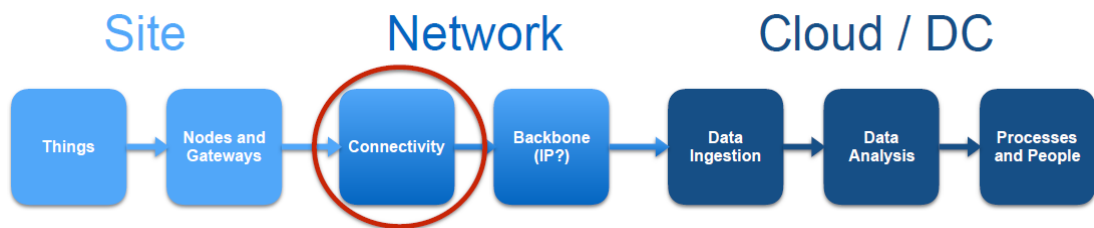


## 2、物聯網 (IoT)

### (一)解碼物聯網生態系統(Decoding the IoT Ecosystem)

RIPE NCC 的 Jad El Chal 講述，從物聯網的生態系統，來說明未來物聯網的挑戰。展望 2020 年，物件連接到網路的數量，根據 Cisco 的預測，大約為 500 億個，使得物聯網的重要性，不可言喻；物聯網的使用案例與機會，大致可包含智慧水錶及瓦斯表、公共路燈、智慧建築、智慧停車、資產追蹤、智慧農業，即洩漏檢測及灌溉、水位與洪水管理、故障管理、安全服務，即煙霧探測器、智慧能源和快速需求響應、垃圾管理及交通管理等。整個物聯網的生態系統，以其資料流 (Data Flow) 來區分，可分為物件端 (Site)、網路端 (Network) 及雲端或資料中心端 (Cloud/DC) 三部分，茲將各端的挑戰說明如下：

- 1、物件端 (Site)：因其包括物件 (Thing) 及節點 (Nodes) 與閘道器 (Gateways)，所以其未來相關挑戰的因素可能有：運作技術、物件被感測後以類比或數位輸出、感測器由 IoT 節點或電源供電、使用 MQTT, CoAP 等編碼、很多物件被連接到 IOT 節點、及很多節點被連接到 IOT 閘道器。
- 2、網路端 (Network)：包含連接 (Connectivity) 及骨幹 (Backbone)，其未來相關挑戰的因素可能有：大規模運送數據的挑戰、對源設備的電池/電源的影響、低功率廣域網路 (LPWA) 作為 IoT 啟動器、目前可能建置情境：Sigfox、LoRaWAN、NB-IoT, LTE-M, 5G、WiFi + 3/4G 等。
- 3、雲端或資料中心端 (Cloud/DC)：包含數據攝入 (Data Ingestion)、數據分析 (Data Analysis) 及過程和人 (Processes and People)，其未來相關挑戰的因素可能有：IoT 大數據應用、雲軟體提供商的許多解決方案、人類介面來了解數據和與其互動、基於收到的輸入的自動進程、機器學習、人工智慧等。

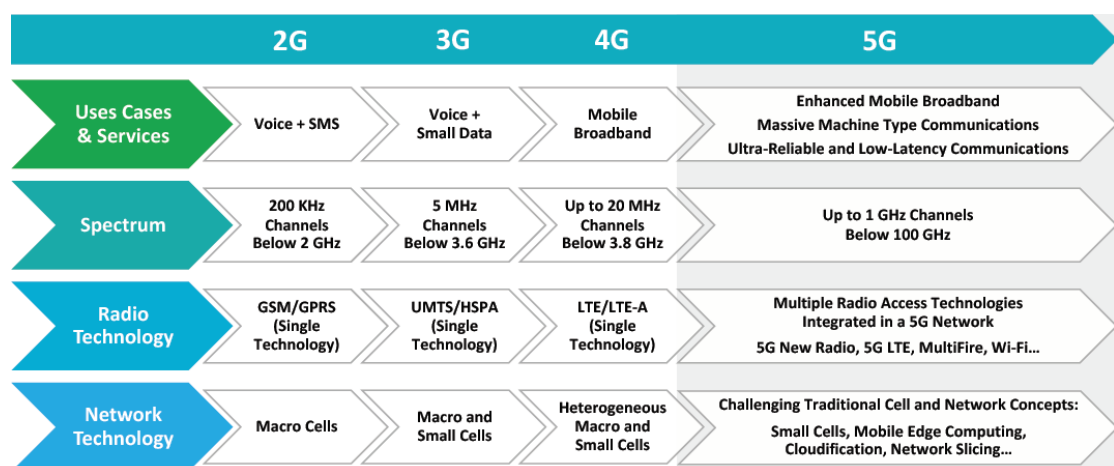


## IoT Enabler

物聯網的生態系統圖示如上，在整個物聯網的生態系統裡，其最重要的部分是網路端，因為它就像是承先啟後的角色，我們也可將之稱作啟動器（Enabler），其作為物聯網生態系統的資料連接，在通訊領域，連接即是所謂之接取（Access）與傳輸網路，就物聯網傳輸關技技術，目前物聯網發展仍在持續進行中，尚無統一的標準，主要可分為區域型網路、低功率廣域網路及電信級物聯網等三類：

- （1）區域型網路：技術標準發展成熟、適合短距離傳輸，但無法確保QoS及缺乏整合的技術標準，此類技術代表為WiFi、ZigBee及Bluetooth。
- （2）低功率廣域網路：低功耗、網路建置成本低且可提供長距離傳輸，但無法確保QoS及缺乏整合的技術標準，此類技術代表為LoRa、SIGFOX。
- （3）電信級物聯網：統一的標準、綿密的網路涵蓋及提供全臺漫遊，但網路建置成本高，此類技術代表為LTE-M、NB-IoT。

另外物聯網之傳輸技術與現在尚在發展中的5G標準也息息相關，以下就先談談5G，5G是什麼，可以從以下的圖瞭解：



通訊技術標準的演進，係從 2G 開始，未來即將進入 5G 的時代，最早的 2G 時代，最主要提供語音及簡訊的服務，3G 時代是提供語音及少

量之數據服務，到了 4G 其主要的服務即為行動寬頻服務，至於未來的 5G 則是更高頻寬行動寬頻、大量機器型態通訊、及極可靠與低延遲通訊的服務，另從頻譜、射頻技術及網路技術面向觀之，我們發現 5G 有相當之優勢存在，包含大於 1G 的頻寬、多無線接取技術之整合、及小型基地台與行動邊緣計算等特性。所以 5G 在物聯網生態系統的網路端：

(1) 就是超連接的願景：

①其為預先存在的技術（2/3 / 4G，WiFi 等）的混合，以獲得更高的覆蓋範圍和可用性。

②作為 M2M 和物聯網的推動者，關鍵的區別在於更大的連接性。

③可能包括一種新的無線電技術，以實現低功耗，低吞吐量的現場設備。

(2) 下一代無線接取技術：

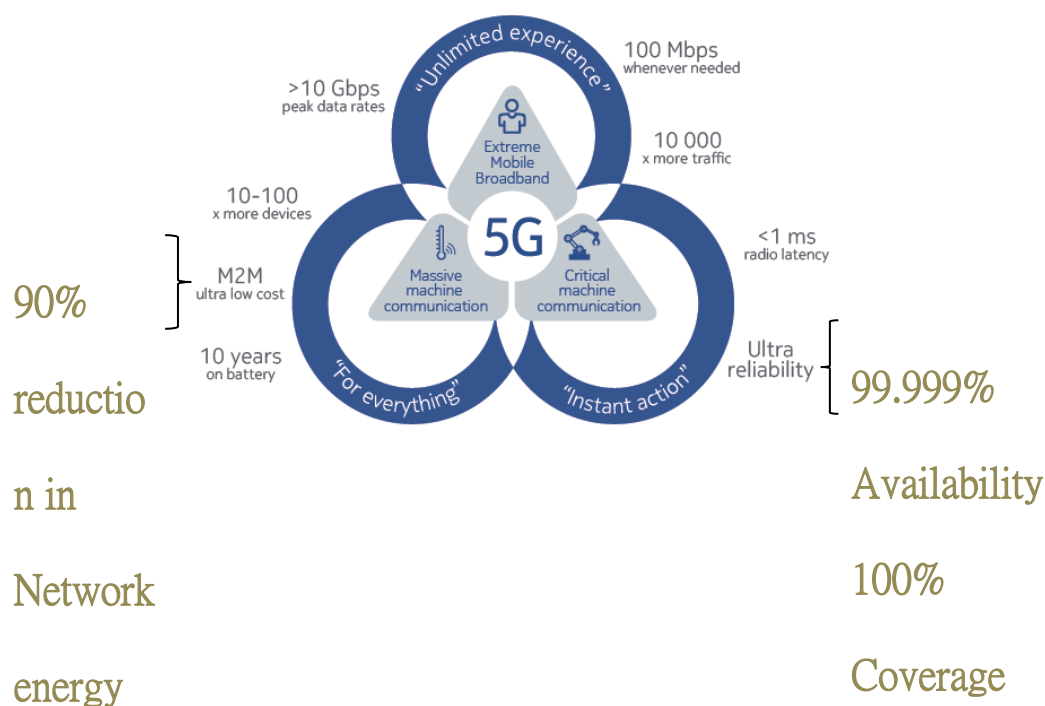
①更多的是傳統的生成定義的觀點

②確定數據速率和延遲的具體目標

③更容易確定技術是否是 5G。超連接的示意圖如下：



對於未來 5G 技術的要求，則包含如下：



對於物聯網的發展，除了上述物件端、網路端及雲端與資料中心端可能有的挑戰外，對於近來越來越受重視的資安亦不容小覷，以物聯網服務框架（如下圖）來看，包含資料管理、裝置管理及連接性管理都與資安脫離不了關係，物聯網的安全挑戰可歸納以下：

- (1) 網路上有更多設備
- (2) 供應商缺少安全更新和修補之措施
- (3) 弱點或無加密/數據保護
- (4) 設備運行帶有漏洞的舊服務
- (5) 許多物聯網設備缺乏計算能力
- (6) 安全設計不是某些供應商關心的問題
- (7) 懶惰的消費者
- (8) 未記錄的硬編碼密碼。

另外物聯網安全衝擊包含：

- (1) 設備成為物聯網殭屍網路的一部分
- (2) 設備被磚或毀壞
- (3) 健康相關的影響（連接的醫療設備）

- (4) 妥協的隱私
- (5) 數據盜竊
- (6) 全面的網路妥協
- (7) 進階持續性威脅 (Advanced Persistent Threat, APT)：針對特定組織所作的複雜且多方位的網路攻擊。

## (二)DNS 為何應作為物聯網命名服務 (Why DNS should be the naming service for IoT?)

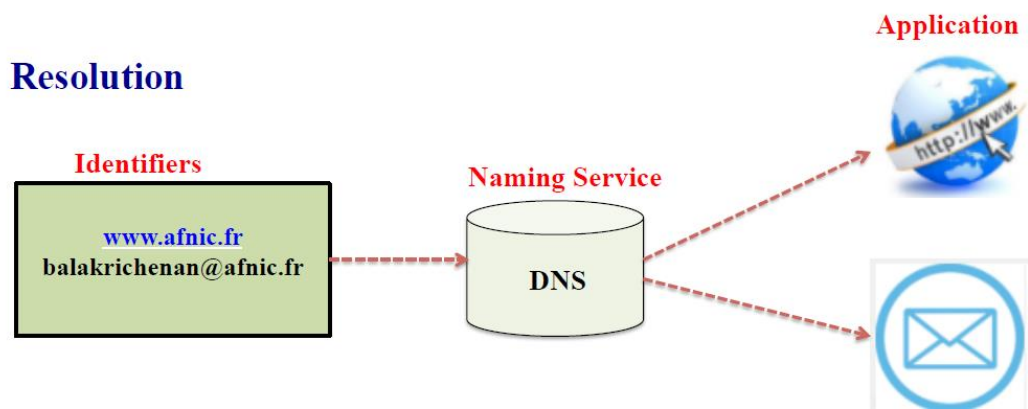
由講師 Sandoche Balakrichenan 主講，本議題之重點為事物在物聯網中之可識別，講者先從一些術語先定義如下：

- (1) 身分(Identity)：可定義和可識別、不需要獨特，不需要遵循任何特定的“命名公約”。
- (2) 識別碼(Identifier)：識別物理或虛擬對象的獨特方式。應該跟著特定命名約定。
- (3) 位址(Addressing)：識別範圍內的物理或虛擬對象的唯一方式通訊、需要遵循特定的“命名約定”（例如郵政地址，IPv4/IPv6，MAC 地址）。
- (4) 命名服務(Naming Service)：將唯一識別碼對應到其相應的唯一服務/資訊。

在網際網路的域名 (Domain Name) 識別碼配置是屬於階層式的，識別碼的命名約定是由命名機構 IETF 所定；為因應物聯網發展，使事物在物聯網中可識別，於是講者提出 EUI-48 and EUI-64 的命名約定，域名識別碼配置包含國家碼、公司碼、產品身分及序號等由 96 位元所組成，另提出為物聯網命名服務要求：包含必須可擴展、必須為舊的和新的命名約定工作、應適用於階層和平面識別碼等條件，有別於網際網路的域名命名服務是由 IETF 所定，而物聯網的命名服務需由不同的標準組織訂定。對於物聯網的命名服務，必須先從網際網路的命名服務談起，次再說明物件的命名服務，整體之說明，將以下圖示表示：



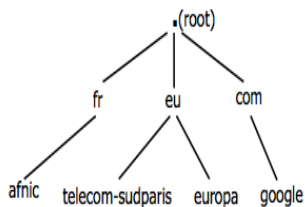
1、網際網路序言：



2、域名配置：

## 配置

**Provisioning  
Naming  
(Hierarchical)  
Authority**



**Naming convention for the  
Identifiers**

**IETF**

**- Domain**

**names, URI**

3、IoT-消費行業配置：

**EPC Provisioning (Hierarchical)**



**Naming Authority**

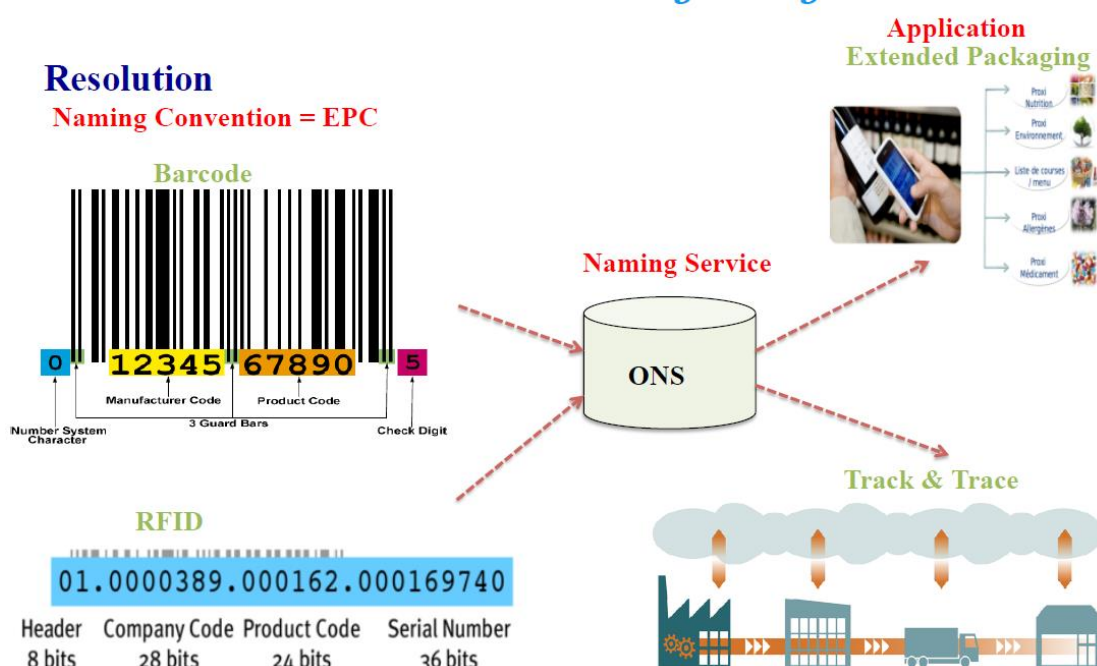
GS1 Prefix (Country Code)

Company Code

Product ID

Serial number

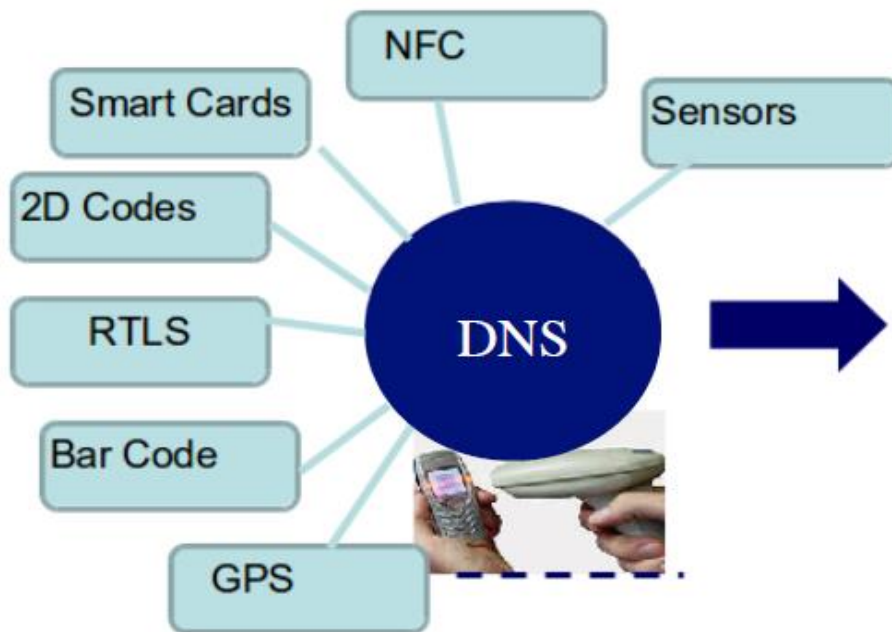
#### 4、IoT-消費行業使用 DNS：



#### 5、不同標準組織的命名服務

- (1) Domain names (IETF) - DNS
- (2) Electronic Product Code (GS1) - ONS which uses DNS
- (3) Object Identifier (ISO, ITU-T) - ORS which uses DNS
- (4) Digital Object Identifier (ISO) - For initial resolution uses DNS

6、願景：未來物件若有個別識別碼，並以相關的介面讀取技術如近場通訊（NFC）、智慧卡（Smart Cards）、二維碼、條碼等等進行辨識後，即可以物聯網命名服務轉換為域名，透過資料攫取、運算和通訊能力的開發，讓物件提供各類應用服務，同時合乎安全和隱私要求。



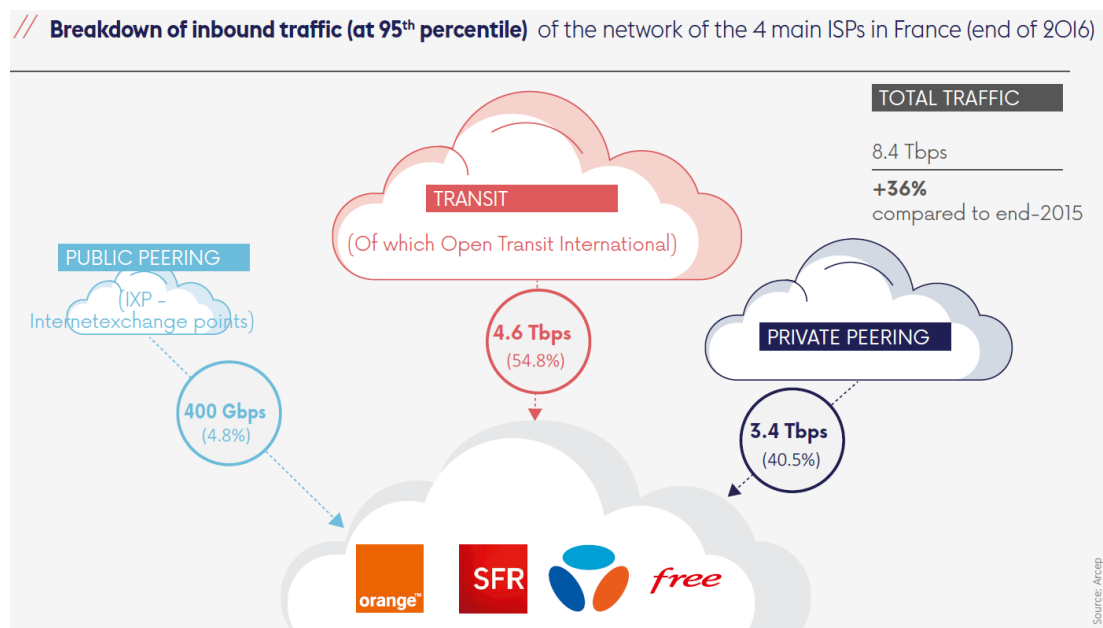
### 3、網際網路互連

#### (一)法國網際網路狀況：數據互連市場演變與轉換到 IPv6 (State of the Internet in France:Data Interconnection Market Evolution and Transition to IPv6)

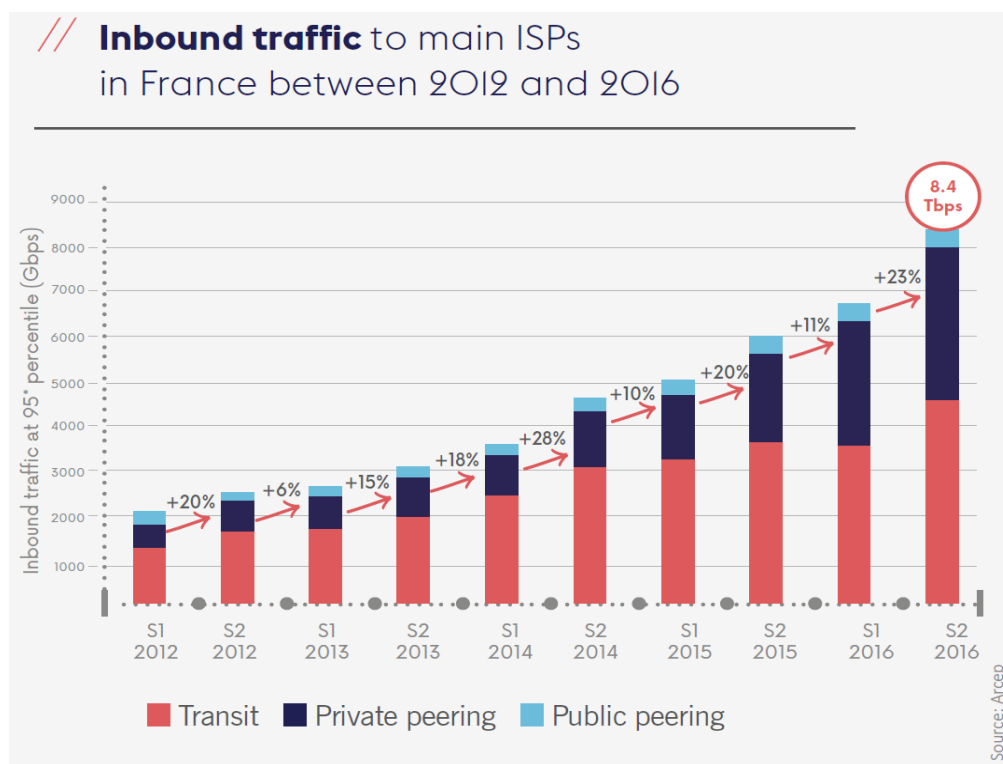
本主題由 Samih Souissi 主講，議題重點在監測互連市場演變，必要時迅速因應，講者講述其國家數據互連(Data Interconnection)市場現況及 IPv6 轉換情況，數據互連市場，講者認為是一個可以產生緊張的市場，其意涵是因

- (1) 偶爾的緊張關係，需要提高警戒
- (2) 不同意互連模式的行為者之間的緊張關係
- (3) 垂直整合或付費對等警戒
- (4) 但放棄硬性規定/法律。

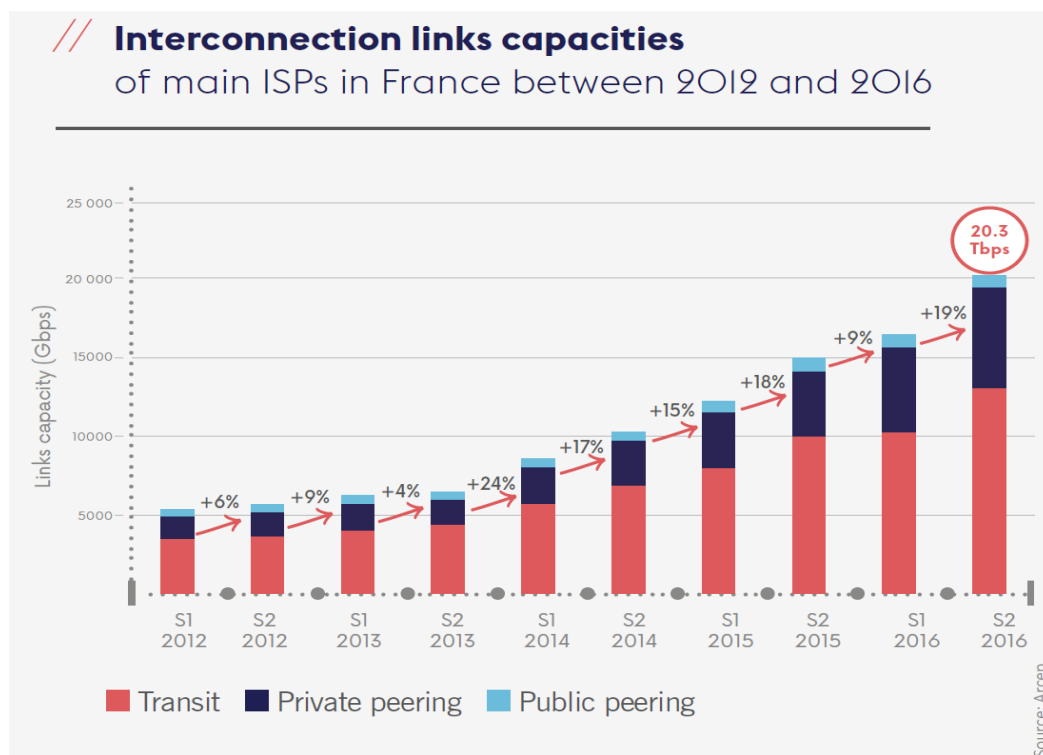
該國為何要監測數據互連市場，起因於該國 Cogent 公司向競爭管理局抱怨 Orange 公司關於數據互連之不公平，因此該國電子通訊與郵政管理局 (Arcep, Autorité de régulation des communications électroniques et des postes) 開始數據收集活動，自 2012 年起至 2016 年底，收集數據和持續分析，從 4 家主要的網際網路服務提供者之 Inbound traffic 分析，如下圖，主要發現，總訊務量為 8.4Tbps，其中雙方互連訊務量為 3.4Tbps、轉訊訊務量為 4.6Tbps，公共互連訊務量僅占 400Gbps。



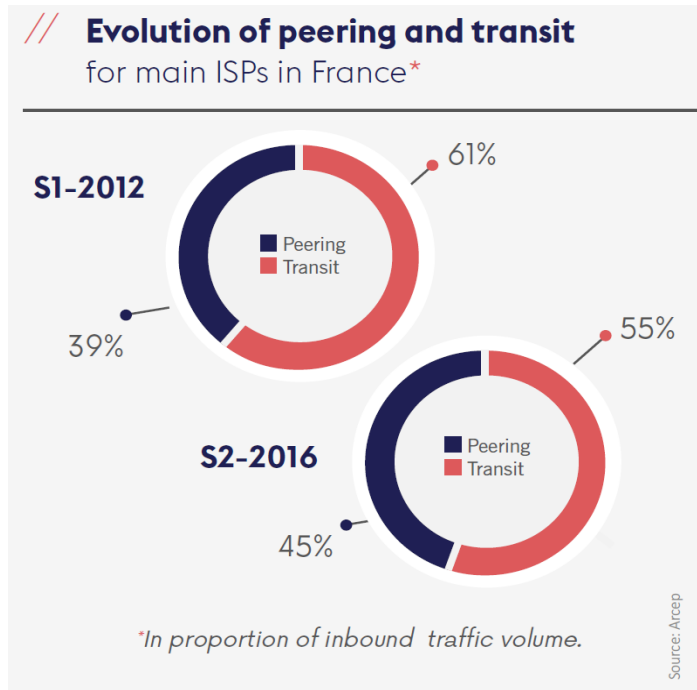
另外對於 4 家主要網際網路服務提供者之 Inbound traffic，自 2012 年迄 2016 年之訊務成長情況，如下圖所示：



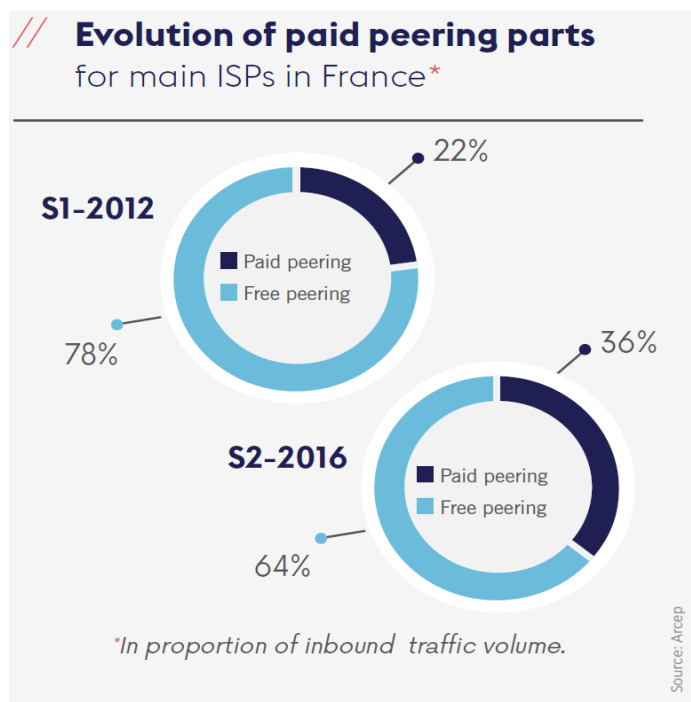
再者，數據互連實體電路容量，自 2012 年迄 2016 年之成長情況如下圖所示：



法國電子通訊與郵政管理局也發現，2012 年至 2016 年，數據互連與轉訊之演變如下，發現互連的比例相較於 2012 年成長 6%：



在數據互連中，付費互連部分之演變，自 2012 年的 22%，上升至 2016 年的 36%，如下：



對於轉訊與互連之成本，法國的電子通訊與郵政管理局也蒐集了下列資訊：

1、 轉訊 (Transit)

(1) 自 2012 穩定下降：between €0.10 plus VAT and several euros plus VAT

(2) 法國 Transit 市場大小：4 million euros per year

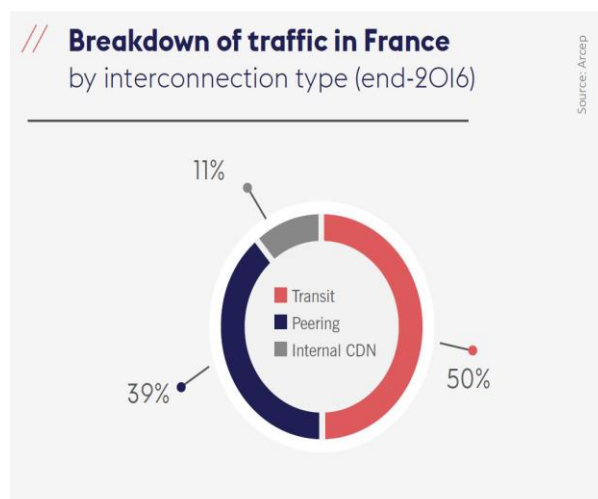
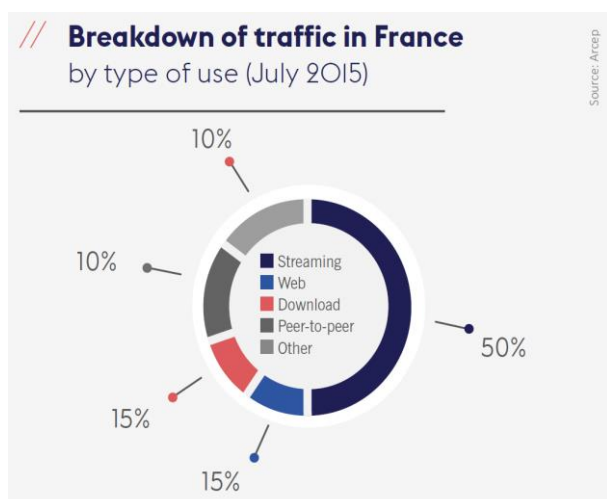
2、 付費互連 (Paid peering)

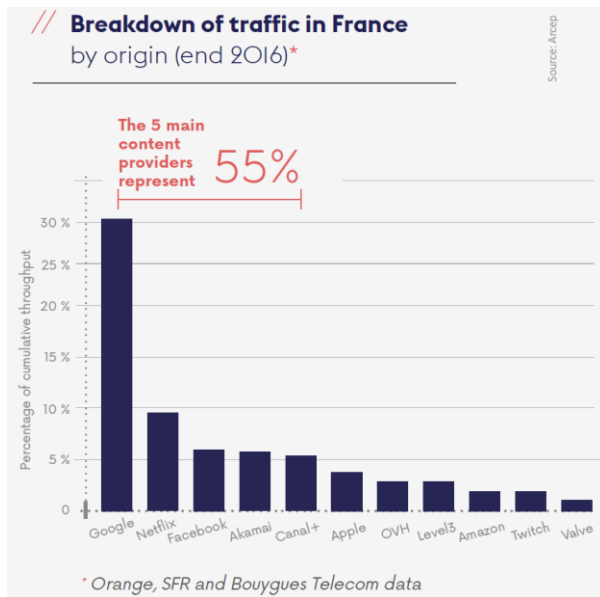
(1) between around €0.25 plus VAT to several euros plus VAT

另外也觀察到法國較小的 ISP 的一些共同屬性：

- 1、 屬於階層 3 營運商等級
- 2、 有多個轉訊提供者
- 3、 與法國主要 IXP 互連
- 4、 較高的轉訊價格

法國電子通訊與郵政管理局也進行新市場趨勢問卷，蒐集資訊並分析訊務使用型態，影音串流服務占 50%、其次網站、下載各占 15%左右；若以互連型態區分，轉訊部分占了 50%，雙方互連占 19%；若以訊務來源分析，大部分訊務來自於 Google、Netflix、Facebook、Akamai 及 Canal+等 5 大內容提供者，約占了 55%。





經過網路互連市場的監測及新市場趨勢問卷，法國電子通訊與郵政管理局做出前瞻性的考慮，即監督不干涉之監理原則，同時亦持續進行相關作為：

- (1) 繼續監測互聯：為了在必要時能夠迅速作出反應。
- (2) 在臨時的基礎上，調查新的市場發展：例如，內部 CDN，本地互連（馬賽，……），過渡到 IPv6 等。
- (3) 升級資訊收集過程：①考慮內部 CDN 流量的增加②整合位址概念 IPv4 或 IPv6。

此外，在鼓勵向 IPv6 轉換的方式，提出了一些看法：

- (1) IPv4 地址短缺及其後果：IPv4 地址短缺、逐漸耗盡可用地址。
- (2) 不可避免的過渡：太多的轉換延遲會導致成本爆炸、在某些服務類別中功能不良等等。
- (3) IPv6 無限制定址和新功能：
  - ①能夠為每個終端或網絡節點分配一個單獨的 IP 地址：可以從互聯網的任何地方直接 accessible。
  - ②簡化某些網絡層功能。
  - ③本地保證更好的交換安全。



法國電子通訊與郵政管理局在 IPv6 宣傳和過渡（轉換）加速中的工作包括：向法國政府報告法國的 IPv6 部署情況，並觀察和學習經驗，觀測台上次更新發現：

（1）2016 年 12 月至 2017 年 3 月法國 IPv6 使用率上升，這主要是由於 2007 年的 Free 和 Orange 在 2016 年進行的遷移舉措，僅限於固定用戶。

（2）CAP 正在向 IPv6 過渡：IPv6 在全球轉型過程中的責任、在 IPv6 部署方面，有 50%（加權平均）、許多中型或小型 CAP 尚未遷移到 IPv6。

（3）為了從這個協議中受益，所有利益相關者必須共同遷移。

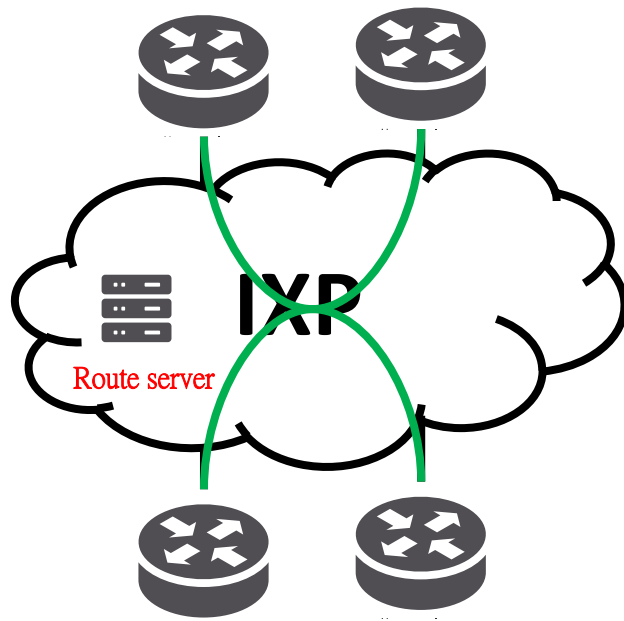
法國電子通訊與郵政管理局在 IPv6 推動的願景，為加強觀測和培育宣傳活動：

（1）加強向 IPv6 觀測站的轉換，2017 年下半年包括從法國 ISP 直接收集的數據和資訊。

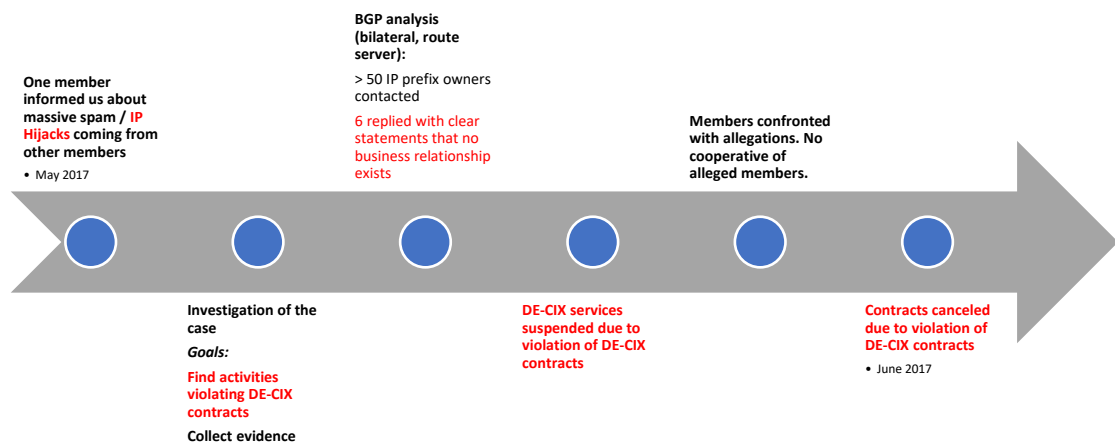
（2）為創建宣傳活動作出貢獻：培養對 IPv6 倡導活動的反思，更好地分享資訊和最佳實踐。

## （二）我們關心 IXP 的數據品質（We Care About Data Quality at IXPs）

本議題重點在於 IX 的管理，IX 是網際網路訊務交換的集中點，其架構如圖所示，就 IXP 的目的，客戶的看法為連接多個 ASN、請求解決免費對等：使訊務交換變得容易。IXP 是垃圾郵件發送者的理想場所：往往沒有很好的過濾 BGP 會話（雙邊+路由服務器）、很容易做壞的 BGP 手法：IP 劫持（例如：未宣布的 IP 空間）、組合的 ASN + IP 劫持（例如，未運行的 ASN）、隱藏上游網絡背後的資源 - 假裝垃圾郵件發送者只是一個無知的/壞的顧客的顧客。垃圾郵件發送者的活動很難察覺：對等意味著學習的路由不會傳播到上游供應商、垃圾郵件發送者公告不會顯示在全球路由表、對於檢測工具（如 RIPE RIS，BGPmon 和 Qrator）它很難（不可能）檢測到 ASN + IP 劫持。



由於有一個會員通知德國 DEC-IX 維運管理單位，其他的會員交換大量的垃圾郵件及 IP 劫持，使得德國 DEC-IX 維運管理單位介入調查，同時也進行邊界閘道路由器分析訊務字綴，最後判定交換大量垃圾郵件的會員，違反合約，同時也將合約解除，在這個案例中，德國 DEC-IX 維運管理單位上了寶貴的一課，也學會了這個艱難的道路。



德國 DEC-IX 維運管理單位為了讓客戶在 IX 交換訊務更容易且無垃圾郵件訊務，他們知道可以做得更好，採行了相關措施：

(1) 我們有一個以責備和羞辱來工作的社區：公司名稱改變，但是，ASN 固定許多資訊可用，我們有責任使用它。

(2) 我們關心 IXP 的數據品質：

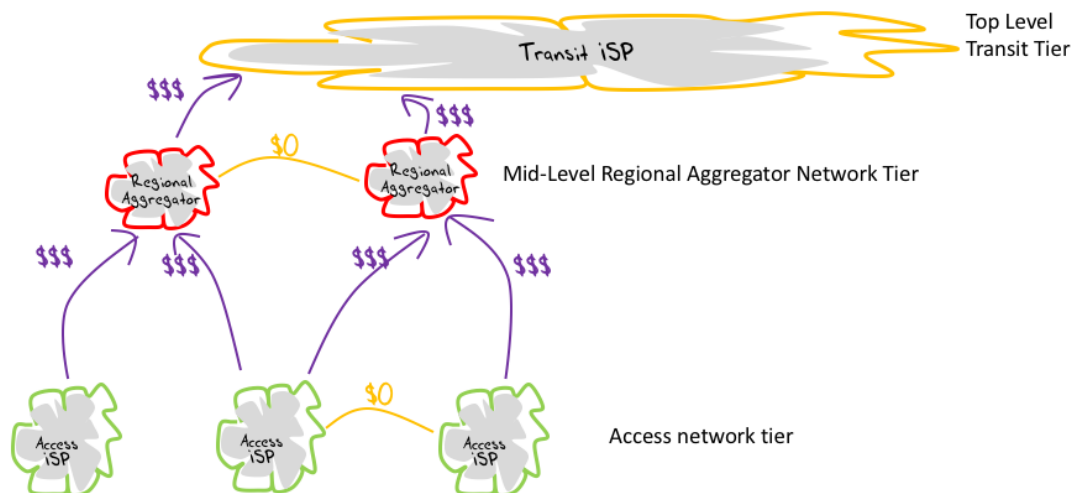
①我們是一家在合同中有明確規定的 IXP 運營商：Layer 2、Layer 3（主要是 BGP）。

②違反這些規定可能會被起訴 - 我們關心關於（BGP）數據質量。

③我們要確保 IXP 是一個穩定可靠的地方交換訊務。

### (三)轉訊之死（The Death of Transit and Beyond）

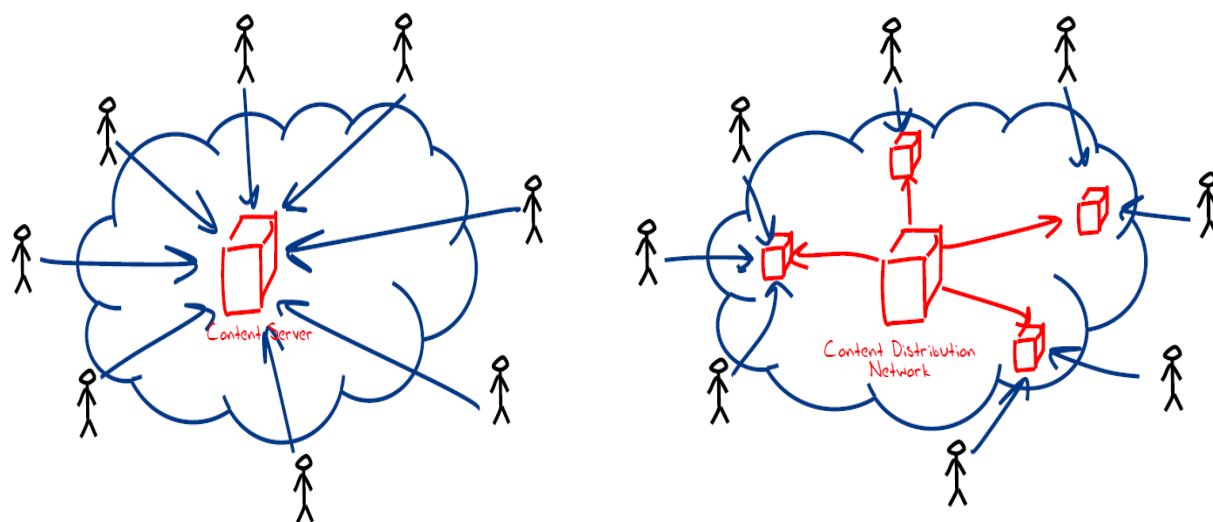
本議題重點在網際網路架構之演變及內容傳遞網路（CDN）之崛起，以及關於這些變化對互聯網公共政策的影響的一些想法。首先，先來看看網際網路角色分割，包含接取網路階層、中階區域彙集網路階層及頂端轉訊階層，在接取網路階層的 ISP 會付費給中階區域彙集網路階層 ISP，請其協助將訊務傳送至目的地，中階區域彙集網路階層 ISP 為了將接取網路階層的 ISP 訊務傳送至目的地，會再付費給頂端轉訊階層的ISP，請其協助將訊務傳送至目的地，因此在網際網路訊務交換是有階層式的，同一階層內的兩個 ISP 是對等的，因此該兩個 ISP 互連是免費的，但不同階層的 ISP，如要交換訊務，低階層 ISP 是必須付費給高階層的 ISP，這是傳統網路訊務交換的架構。



但是進入內容時代，起了一些變化，它打破客戶端和服務器的邊緣：概念上是接取網路服務需求“客戶”、其他客戶無法直接訪問客戶端及客戶連接到服務。這裡的網路的作用是把客戶帶到服務接取點，這裡的假設是有更多的客戶

比服務點。在內容時代，內容與運輸（Carriage）之間，誰應付給誰，有不同說法，一派說法是接取網路有客戶的唯一原因是因為那裡有客戶想要接取的內容服務，因此運輸應該支付內容；另一派說法是網際網路上沒有“端到端”的財務結算模式-這兩個“端”支付介於接取和網路提供商之間的結算。對於一個運輸網路而言，內容只是另一個客戶。因此內容應像其他客戶一樣支付運費。最後，內容人士為了解決這個爭論，藉進行 over the top，並直接與終端用戶建立關係，來消弭此爭論。

傳統客戶想要接取服務，必須連線至內容伺服器進行接取，但因內容伺服器通常放置於遠端，以致客戶存取內容服務受限於距離的嚴酷考驗必須花費較多時間，影響了客戶接取內容得便利性與即時性，例如，如要觀看美國大聯盟資訊，就必須連接至美國的內容伺服器才能存取該資訊；有鑑於此，發展出了內容傳遞網路的概念，亦即在靠近客戶端之處，建置了內容緩存（cache），此舉的目的即是讓客戶他們吃數據！



內容傳遞網路（CDN）的興起，有幾個優點：

- (1) 可讓重複的內容緩存接近大量用戶群體。
- (2) 經由高延遲網路路徑傳遞許多複製服務請求的挑戰，被內容分發系統更新一組本地緩存任務所取代並且經由接取網路服務用戶服務請求。

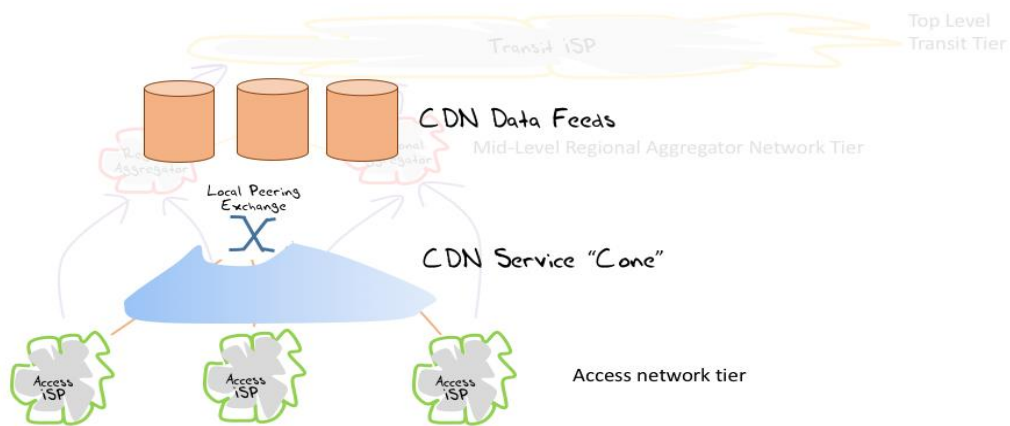
(3) 減少服務延遲，提高服務彈性，讓顧客開心。

CDN 的興起，也讓角色反轉，即服務入口越來越靠近用戶，意味著網路的變化：

(1) 公共網路不再將用戶流量傳送到服務入口經由 ISP 運輸服務。

(2) 相反，私有網路經由 CDN 服務將內容傳送到服務入口。這一轉變對網際網路有著深遠的影響。

今日網際網路架構（如下），我們已經將網路分成客戶端和服務器：Web 服務器、流媒體服務器、郵件服務器及 DNS 服務器。現在，伺服器和服务位於 CDN 掩體中，並進行全球複製，用戶不再接觸到內容，CDN 帶給用戶內容。



轉訊最後會變成如何？如果用戶不再向用戶發送數據封包，如果內容現在經由離散服務錐之 CDN 傳遞給用戶，如果沒有普遍的服務義務，那麼為什麼我們仍然需要轉訊服務提供者？一旦 CDN 緩存放置在接入 ISP 的網路位址轉換

（NAT，Network Address Translation）邊緣的“內部”，然後整個廣域網路就變成邊際活動，對比於內容供給的價值！如果網際網路是（或可能很快將）離散的 CDN 服務‘錐’集合，那麼我們為什麼期待終端用戶支付全球位址計畫或全球命名系統或單一全球網路維修費用。這不只是轉訊的死亡，這是整個網路的重新利用：

(1) 服務提供位於雲端提供商和分散式數據中心內。








(2) 邊緣電腦現在成為數據雲世界的電視機。

(3) 個人和公共數據領域之間的區別正在消失於公司所有的私有數據帝國領

域。網際網路的政策是什麼？如果 CDN 提供網路是專用（private）網路，那就是除最後一公里接取以外，很少剩餘的公共運輸網路，那麼我們真正的“公眾”通信政策是什麼意思？在監管的世界，“內容”是商業，而不是運輸！當我們談論不同的 CDN 作為網際網路的主角時，在今天的網際網路中，我們在政策意義上的意思是：

- (1) 普遍服務義務
- (2) 網路中立
- (3) 接取權
- (4) 市場主導地位

截至 2017 年 9 月全球十大上市公司按其市值排名，如下，可以看出內容真的是王，這五家科技公司都不是電話公司，甚至不是轉訊 ISP，甚至不是一個 ISP！他們都把運輸網路推到了一邊，是為了保持與數十億消費者的直接關係，這些寶貴的消費者關係是基於內容服務，不是運輸（carriage）。

	Company	\$B USD
	Apple	791
	Alphabet	664,
	Microsoft	589
	Amazon	459
	Berkshire Hathaway	451
	Alibaba Group	436
	Tencent	405
	Facebook	399
	Exxon Mobil	348
		347
	Johnson & Johnson	

在數字內容和服務領域的核心，只有少數真正龐大的企業，這仍然是一個競爭壓力的空間。或者，這些占主導地位的在職者是否能夠與使用者，甚至是公共部門建立自己的互動條件？至於這可能聽起來，這不是一個新的情況！在網際

網路的鍍金時代，用戶、彼此、第三方供應商、監管機構和政府，這些演員有足夠的市場影響力來設置他們的自己的規則，憑藉這些突飛猛進的領先地位技術，這些球員能夠積累巨大的財富，對責任更廣泛的公共利益。這是怎麼回事？這不再只是一個關於互聯網內運輸和通訊增量變化的對話。對於我來說，這個談話的基本話題是我們如何能夠在一個迅速積累了對數字服務和內容空間的全面控制的，有活力的私營部門和我們大家都希望的更大社會的需求之間取得可持續的平衡 公平的機會來發展和受益於這個新的數字時代的成果。

## 肆、 心得與感想

### 【IPv6 最新訊息(含 IP 位址政策)】

工業 4.0 (Industrie 4.0) 是德國邁向智慧工廠 (Smart Factory) 的國家級技術戰略目標，對於 IoT 互聯網需求量大增，加上智慧行動裝置大量整合雲端應用服務，IoT 就是 IPv6 殺手級應用，台灣 IoT 產業要跳脫硬體思維轉型開發 AI、智慧城市，IPv6 部署及數據管理將是關鍵。

杜拜現今是全球發展智慧經濟及城市的資優生，小從 M2M 安全性、IPv4 到 v6



相互操作標準擬訂，機器對機器資料保護，機器學習後擬人化的機器人是否需要賦予人權？尚在討論中，而發展智慧城市背後代表大量數據搜集，分析，應用及跨境傳輸，其數據資料管轄，希望跳脫在地管轄原則，以 cyber space 網路架構下進行管轄，但目前仍屬技術測試階段。歐洲國家法院正採用基於接入方式標準，以建立對國外託管內容的管轄權。

杜拜 NOW APP 將市民必備 bankind, school 等 55 項市政業務於 in one pocket

法國相關的市場現況資料包含 IX 或 Paid peering 情況或可對台灣網際網路互連之研究有所突破，另外該國 IPv6 的轉換一些推動經驗，如對使用者宣導或協調利害關係人改善等方式，可提供我國未來推動 IPv6 之參考。

最後做個總結上述介紹，IP 地址是很多國家制定網路政策所關注的重要資源，但重要的技術都在民間團體中，建議應強化與民間增加互動建立技術社群，匯集各路意見領袖，參考歐洲最新管理及技術支援，考量國內 IPv4 基礎設施提升必要的技術教育訓練，加強配套措施誘因及方案鼓勵業者大量投資 IPv6 基礎設施，方能使 IPv6 在台灣全面普及化，使本會透過網路政策擬定達到網路治理目標，促進台灣通傳及各產業轉型。

## 【針對 IoT 主題】

沒有話語權/主導權：IoT 的技術標準，全球正如火如荼的討論，礙於過去我國在 2G、3G 及 4G 發展過程中，非通訊技術研發或通訊標準制定之領先國，因此在參與國際標準組織中，很難發聲，大多遵循國際標準開放我國的行動通信，未來 IoT 發展所涉 Site 及 Network 標準亦只能遵循國際標準組織，才能接軌國際。另外可吸取國際經驗，讓台灣產業先做準備，在全球 IoT 大浪來臨之際，以創新開放的姿態站上引領趨勢的數位浪頭。

推動物聯網服務：對於物聯網服務使用電信號碼 (040 prefix)，國際趨勢未明；或許可考慮使用 IP Address、DNS 方式，將有助於 IPv6 的普及；另外對於 DNS 作為 IoT 命名服務的議題，因提出的觀念尚須審慎評估可行性及國際趨勢，再決定我國應採取之態度。



## 【對於網際網路互連主題】

贊同法國電子通訊與郵政管理局所做出前瞻性的考慮，即監督不干涉之監理原則，付費互連 Paid peering 應由 ISP 雙方商業協商處理。

對於網際網路網路交換中心（IX）公共互連 Public peering 的治理，或許應有突破性之思維，臺灣網際網路交換中心（TWIX）自民國 86 年建置以來，多年來由中華電信公司負責營運管理，不夠中立公正，有球員兼裁判之嫌。比如說，因中華電信公司因是一個網際網路服務提供者且是固網市場主導者，因此會藉調降 Private peering，來限縮接入臺灣網際網路交換中心連接至該公司 HiNet 的 Public peering 頻寬。因此對於 IX 的治理可師法 DEC-IX（1995 創立）、AMS-IX（1994）、LINX（1994）、HKIX（1995），由中立公正角色營運管理。目前 DEC-IX 的峰值訊務量（Peak traffic）已達 5.9+ Tbps 以上。另目前臺灣網路資訊中心（TWNIC）已改隸本會，TWIX 由 TWNIC 負責維運不失為一個好選擇。為何訊務必須在 IX 交換，主要是有效降低互連成本，提升網路運作效率，監控網路流量品質，更有利 IPv6 推行。

因內容是王（Content is King），且內容提供者（Content provider）來勢洶洶，內容之治理政策應如何？首先應先確定內容的權責機關是誰？另外 CDN 的崛起，且其與電信業者之競合也需特別注意，再者是否會衍生互連爭議（如付費問題）也值得重視。