行政院及所屬各機關出國報告

(出國類別：實習)

「實習下一代網際網路新技術」報告

服務機關：中華電信股份有限公司

數據通信分公司

出國人：職稱　　姓名

助理工程師　朱永正

出國地點：美國

出國期間：92年09月28日 至 92年10月11日

報告日期：92年12月09日

系統識別號:C09203532

公 務 出 國 報 告 提 要

頁數: 42　含附件: 否

報告名稱:

實習下一代網際網路新技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

朱永正　中華電信數據通信分公司　網際網路處　助理工程師

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 09 月 28 日 -民國 92 年 10 月 11 日

報告日期: 民國 92 年 12 月 09 日

分類號/目: H6／電信　／

關鍵詞:　IPv6, MPLS, QoS

內容摘要: 下一代網際網路新技術不論是在軟體或是硬體方面已有較大的變革，許多以前無法在現有運作網路上啓動的應用技術已漸漸被使用，例如在網路中實際啓動Multicast機制或QoS（Quality of Service）機制等，然後搭配這些服務應用在思考未來的使用規模與發展趨勢也發展了新的網路技術，如IPv6（IP Protocol Version 6）協定或MPLS（Multi-protocol Label Switching），迄今標準達成熟之餘逐漸地成爲大型網路中必須啓用的新技術。爲因應未來網際網路頻寬及服務的需求，我們需要及早參考國外所發展及進行中的寬頻網際網路新技術及使用中設備的極限功能與該設備廠商正在進行的Roadmap已因應多元化的網際網路服務。本報告書共分四個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元則敘述下一代網際網路新技術，以闡述現今 QoS、IPv6、以及MPLS技術爲主。第四單元則爲實習心得與結論。

本文電子檔已上傳至出國報告資訊網

摘要

下一代網際網路新技術不論是在軟體或是硬體方面已有較大的變革，許多以前無法在現有運作網路上啟動的應用技術已漸漸被使用，例如在網路中實際啟動 Multicast 機制或 QoS（Quality of Service）機制等，然後搭配這些服務應用在思考未來的使用規模與發展趨勢也發展了新的網路技術，如 IPv6（IP Protocol Version 6）協定或 MPLS（Multi-protocol Label Switching），迄今標準達成熟之餘逐漸地成為大型網路中必須啟用的新技術。為因應未來網際網路頻寬及服務的需求，我們需要及早參考國外所發展及進行中的寬頻網際網路新技術及使用中設備的極限功能與該設備廠商正在進行的 Roadmap 已因應多元化的網際網路服務。

本報告書共分四個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元則敘述下一代網際網路新技術，以闡述現今 QoS、IPv6、以及 MPLS 技術為主。第四單元則為實習心得與結論。

目次：

壹、實習目的

目前網際網路在傳輸技術及硬體設備蓬勃發展的推波助瀾下新的技術與標準儼然成熟，骨幹頻寬也達到了10 Gbps的傳輸基本單位，因此產生了新的應用與加值服務。不論是學術研究網路抑或是商用服務網路已經開始導入了新的網路技術，如：QoS機制、IPv6協定與MPLS等並且更新設備為下一代網際網路的發生而準備。因為下一代網際網路所帶動的產業升級也成為國家或公司在世界舞台上的一項競爭力指標。如何保有既存網路之優勢及提早妥善運用新的網際網路寬頻技術以提供更多元化的寬頻網路服務將是身為ISP業界龍頭的HiNet必須時刻思考與實行的議題。因此本次職奉派出國實習，主要在於學習下一代網際網路新技術，明瞭現今 QoS機制、IPv6協定與MPLS的 最新技術，並對現有 HiNet所使用的網路設備與原廠製造商-Cisco、Juniper等討論了解其設備未來發展的藍圖與重要的技術項目，希望未來在規劃新的網路服務與更新設備時能學以致用並提供最佳的解決方案。

貳、 實習行程及實習課程

職奉派至美國實習『下一代網際網路新技術』，實習時間自民國九十二年九月二十八日至九十二年十月十一日為期十四天。本次實習課程計有：

Cisco公司 ：MPLS、IPv6、MAN、QoS（5天）

Juniper公司 ：MPLS TE、MPLS VPN、IPv6、QoS（4天）

參、 下一代網際網路新技術

3.1 QoS機制

Qos-Quality of Service 這名詞在 Internet 上並不是一個陌生的名詞，而構成 QoS 的幾個 Performance 量測因子則分別有 Delay、Jitter、Loss 及 Throughput 等。對於目前一般 Internet 上的使用者而言，較敏感及在乎的項目應為 Delay 及 Loss 兩項因素。因為使用者使用的應用程式暫時仍侷限於 Real-time 及 Non-real-time 兩種類別。例如 Voice over IP、線上遊戲、多媒體影音內容等類的應用程式需要的是即時性的網路環境，而如 Browsing Web、FTP、Telnet 等類的應用程式需要的是封包傳送正確性高的網路環境。與現今的 Internet 所提供的 Best effort 傳輸相較，Internet QoS 的實現將使 Internet 上更多的 Value-Added 服務存取有別於過去一是同仁的方式，服務的提供是基於一個 Managed IP 網路上，所以產生的效果及功能將更加顯著。所以 Internet QoS 事實上是一種 Internet 上資源配置與管理的一項議題。

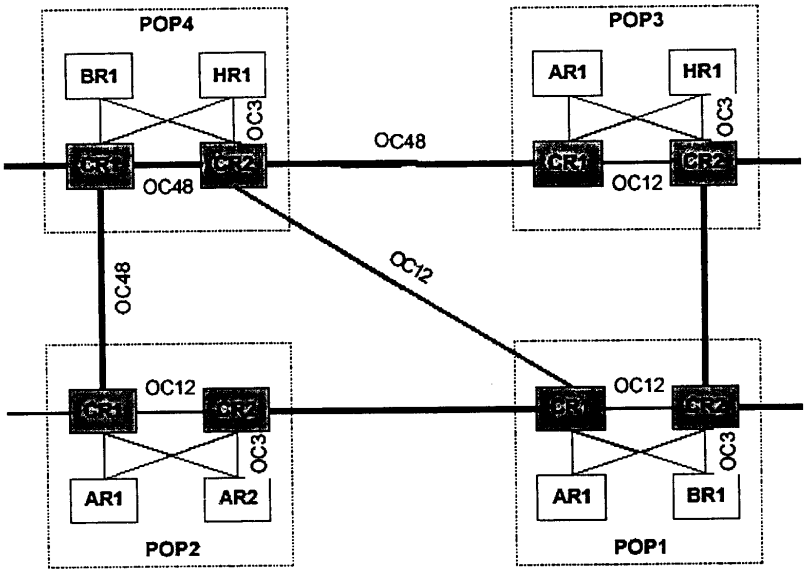
在 IETF 制定的 RFC 規範文件，QoS 分為兩種 model：Integrated Serivces（Intserv）以及 Differentiated Services（Diffserv）。Intserv 是一種 end-to-end 的 model，針對每一項 IP Flow 對於網路資源如連線頻寬、路由器或交換器內轉送的 Buffer 空間等作一預約保留動作，以確保服務啟動期間品質有保證。而 Diffserv 則是將 Internet 訊務切割分成幾個等級，整個網路區間（Network Domain）中好像 Aggregating 成幾個虛擬的管線（Pipe）一樣，而各管線間對於封包傳輸的優先權上就根據所劃分的等級而有所不同。綜觀 QoS 的機制，Intserv 是屬於一種微觀式的 QoS 機制，而 Diffserv 則是屬於一種巨觀式的 QoS 機制。

過去傳統的網路並無 QoS 觀念，而要談及 QoS 的問題常常以所謂頻寬不足來闡釋，然後以擴充頻寬的方式試圖解決。對於以往的應用程式型態而言，如此 best effort 的網路架構似乎沒有發生太多問題，即便今天頻寬費用大幅降低，仍然有許多人是以大的 Pipe 頻寬在思維，認為 overprovision bandwidth 的方式就可避免複雜的 QoS 機制。過去所謂的網路 QoS 最成功的當屬 ATM 網路，ATM 的訊務分為 CBR、rt-VBR、nrt-VBR、ABR、UBR 等各類等級，但 ATM 真正的設計是屬於 Telecom Carrier 使用的網路型態，Internet 在過去訊務未達今日需求的規模時，IP over ATM，ATM over SONET 的 Cell-based 傳輸方式，在將近 20%的 overhead 下，因為有傳輸品質保障故仍可作為 Internet 高速骨幹網路使用。

隨著網路使用趨勢的變化，光纖通訊技術的進步，頻寬需求以 Gigabits 計算甚而至 Terabits，ATM 在高速網路上遭遇到了 SAR（Segmentation and Reassembly）的瓶頸，而一般網路設備亦必須面臨 Electrical-Optical，Optical-Electrical 的轉換瓶頸，故 ATM 網路已逐步退至接取端網路使用，IP over Optical Network（All Optical Network）成為現今高速骨幹網路的架構。IP over Optical Network 的傳輸過程中省略了 overhead，而原先在傳輸層所依賴的 QoS 機制，如今必須依賴網路層（IP）、傳輸層（TCP/UDP）甚至於更上層的應用層的屬性及機制來達成。現今 Internet 架構如下圖所示：

CR: Core 路由器　　BR: Boarder Router

AR: Access Router　　HR: Host Router

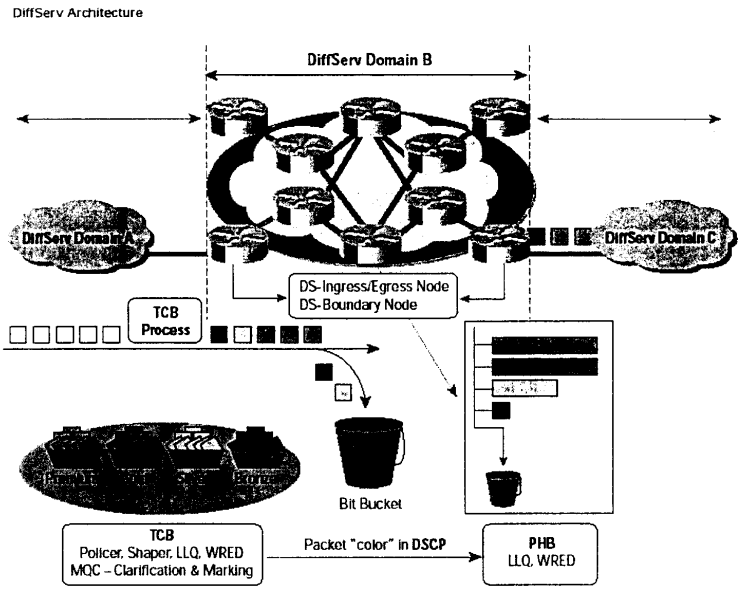


事實上針對 QoS 在 Internet 架構中扮演的角色，考慮現在與未來的 Internet 網路中完整的 QoS 架構則應包含有 Diffserv、Traffic Engineering、Traffic Directing 以及 Load Balancing 等，所考慮到的是整體 Internet 網路由下而上各層的整合架構，詳細說明如下表所列：

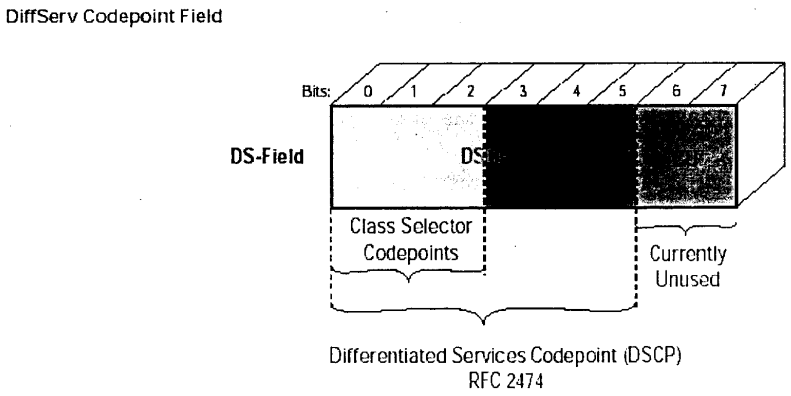
Location	QoS scheme	Mechanisms	Purpose of the QoS scheme
Application Layer	Traffic directing and load balancing	URL redirecting, load balancing	Direct traffic away from congesting part of a network or server
Transport/ Network Layer	Diffserv	Classification, policing, shaping, marking, class-based queueing and scheduling, Random Early Detection (RED)	Provide differentiated services for different classes of traffic, especially during network congestion
Network Layer	Traffic engineering	MPLS, constraint-based routing, LSP path signaling, and enhanced link state IGPs	Avoid congestion in the network
	Fast reroute	Local repair	Avoid packet loss during link and/or router failure

而這裡我們要探討的是以 Diffserv 為主的內容，此項技術在各大網路

中已開始建置提供用戶端不同等級之服務。以整個 Internet 結構來看，如下圖所示，



其主要目的就是要提供 Scalability 的 QoS 機制，將 Traffic 分成簡單的幾個 group 對應至 RFC2474 所定義之 Diffserv Codepoint Field（DSCP），如下圖所示，



如此一來網路設備上僅須執行幾個簡單的 classification 動作，並且不用保持如 Intserv 所需的 per flow soft-state 狀態，網路設備的 QoS 效

能將大幅提升。而 Diffserv 的架構中一般有分三種等級的 Service：Best-effort、Assured、Premium。

Best-effort 即為傳統的網路傳輸模式，而新定義的 Assured Service、Premium Service 將於下列章節中說明。另外，接下來的章節中對於 IP 網路中 Diffserv 機制加以討論的主要內容分別有 Traffic differentiation 與 Prioritization，亦即 Assured Service 及 Premium Service，並且將討論在這些 Diffserv-QoS 的機制中所實行的 Resource Management（congestion control）、Resource Negotiation（admission control）以及 Service Level Agreement（SLA）。

在進行討論 Assured Service 及 Premium Service 前對於 Diffserv 使用的專有名詞部分，依據 RFC2597、RFC2598 節錄如下：

Flow：

A stream of packets with the same source IP address, source port number, destination IP address, destination port number and protocol ID.

Classification：

The process of sorting packets based on the content of packet headers according to defined rules.

Behavior Aggregate (BA) Classification：

The process of sorting packets based only on the contents of the DS field.

Multi-Field (MF) Classification：

The process of classifying packets based on the content of multiple fields such as source address, destination address, TOS byte, protocol ID, source port number, and destination port number.

Service Level Agreement (SLA)：

A service contract between a customer and a service provider that specifies the forwarding service a customer should receive. A

customer may be a user organization or another provider domain (upstream domain).

Traffic Profile：

A description of the properties of a traffic stream such as rate and burst size.

Precedence Field：

The three leftmost bits in the TOS octet of an IPv4 header. Note that in Diffserv, these three bits may or may not used to denote the precedence of the IP packet.

TOS Field：

bits 3-6 in the TOS octet of IPv4 header.

Differentiated Services field (DS field)：

the TOS octet of an IPv4 header, or the traffic class octet of an IPv6 header, is renamed the differentiated services field by Diffserv. It is the field where service classes are encoded

Per-Hop-Behavior (PHB)：

The externally observable forwarding treatment of a class of packets at a Diffserv-compliant node.

Admission Control：

The decision process of whether to accept a request for resources (link bandwidth plus buffer space).

Marking：

The process of setting the DS fields of packets.

Policing：

The process of handling out of profile traffic, e.g., discarding excess packets.

Shaping：

The process of delaying packets within traffic stream to cause it to

conform to some defined traffic profile.

Scheduling：

The process of deciding which packet to send first in a system of multiple queues.

Queue Management：

Controlling the length of packet queues by dropping packets when necessary or appropriate.

（1）Assured Service

Assured Service所提供的是一種相對性質的QoS，較適用於non-real-time的應用程式例如Telnet、Web Browsing等。網路品質的等級類似ATM 的non-rt-VBR。依據RFC2597- Assured Forwarding PHB Group的定義，Assured Service可進一步區分為金（Gold）及銀（Silver）等級。而目前使用者與ISP協定的SLA中的Assured Service也大約分成這兩類等級，若再加上Best-effort劃分為Bronze等級則 構成所謂的「Olympic Model」－金、銀、銅牌等級。

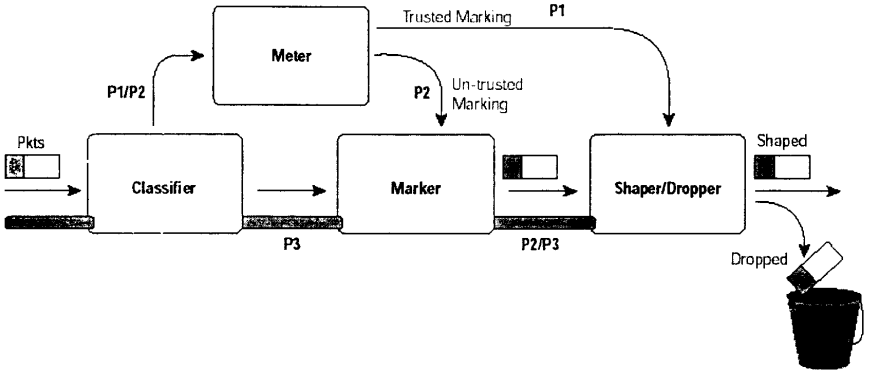
（2）Premium Service

Premium Service所提供的是一種屬於絕對性質的QoS，適用於real-time的應用程式例如Voice over IP、Streaming、Network control等。網路品質的等級類似ATM 的CBR。而在ISP方面，對於此類服務等級相當於提供給使用者一條虛擬專線電路，像是「公車專用道」一般。Premium Service的服務等級則是依據RFC2598- An Expedited Forwarding PHB的定義內容，提供給使用者的網路環境具固定的封包延遲以及具peak bit rate之約定頻寬等特性，對於網路Resource Allocation 上Premium Service具有最高的優先順序，屬於「鑽石」等級。

一般ISP在其網路設備上提供Assured Service以及Premium Service所需執行的機制有下列程序：

（1）在Ingress端進行Multi-field Classification（MF）

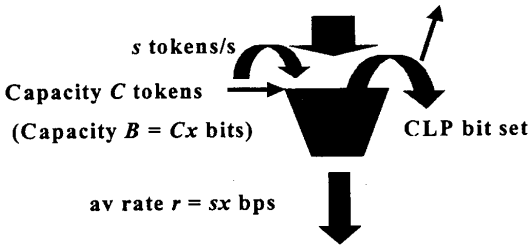
Ingress端指的是ISP網域內的Edge路由器，Edge路由器介接使用者的網路設備，並且執行複雜的classification規則來對使用者送出的封包進行分類。一般分類的方式是根據介接的介面、Source IP Address、Destination IP Address、Source Port、Destination Port、Protocol等封包標頭內的值作區分。封包分類後，隨即根據SLA設定之Profile開始進行Policing、Marking、Shaping以及Scheduling，其中也含Queue Management的動作。如下圖所示：



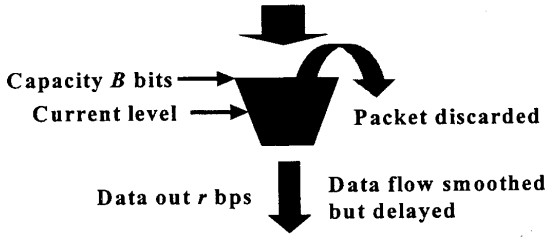
（2）Policing、Marking、Shaping

Policing的實行在Assured Service上一般是以Token Bucket演算法來遂行SLA所定的內容，其中允許的Burst訊務量就是Bucket深度。而在Premium Service上則是以Leaky Bucket為主，兩者演算法，允許Burst Traffic的容量各不同。T時間內Token Bucket允許Burst大小=$(C+sT)$ x bits；Leaky Bucket允許Burst大小=$(B+rT)$ bits。兩種Bucket Model如下圖所示：

Leaky Bucket



Token Bucket



而Marking的工作則是將ISP所預執行的等級定義與Classification後的結果對應，然後將DSCP寫入至封包中，參見下表。

	DSCP	Queue
Premium Service	111000	Priority Queue（PQ）
Assured Service	10x000	Assured Queue（AQ）
Best-effort	00x000	Default Queue（DQ）

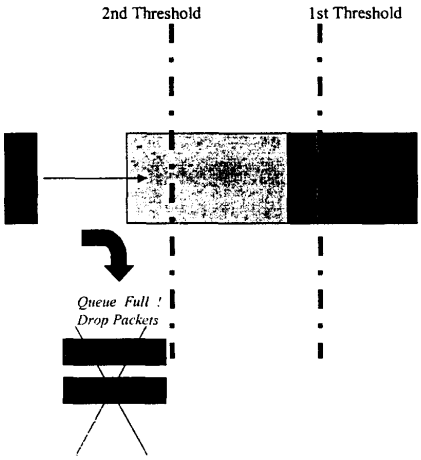
x：表示drop preference 1: high preference 0: Low preference

當封包經過Policing及Marking之後會依據Marking的結果送至各個

Output Queue（PQ、AQ、DQ），各個Output Queue送出的output rate也不相同，因此達到Traffic Shaping的效果。

（3）Edge端與Core端的Queue Management及Packet Scheduling

不管是在Edge端與Core端的網路設備，當封包進入Queue使Queue滿載（input rate > output rate）或是Queue長度設定太小的情況下，則必須使用Queue Management機制來進行drop封包的動作。一種經驗證有效的封包drop演算法為Random Early Detection（RED）。RED依據DSCP及Queue的平均長度狀況採用random方式來drop封包，如此做法可避免Queue的overflow與tail-drop（所有陸續到達的封包不得其門而入一律drop）現象。而目前普遍實行的是另一種進階方式的RED—RED with in and out（RIO）。RIO就像是在介面的input方向與output方向分別各執行一套 RED演算法一般。當Queue的平均長度低於第一界限（1st threshold）時，並不會有任何封包被drop而當Queue長度介於第一界限與第二界限（2nd threshold）之間時，則進入Queue內的封包將會被random的選擇drop；而超過第二界限時，所有封包則一律drop，如下圖所示，並且封包drop的機率與Queue的長度是一種線性關係。另外，對於Premium Service而言，Priority Queue中並不實行RED/RIO，因為希望的是PQ中的封包是全部送出的，故PQ的output rate必須大於input rate。



當封包依序進入要傳遞的「輸送帶」－Queue 之後，就必須考慮各種 Queue 所應佔有的傳送時間。從前 Queue 執行的是 Round-robin 模式，而現在因為各種 Queue 各有其 Priority，所以執行 Weight Fair Queueing（WFQ），以 weight 按 Priority 將系統傳送封包的時間依比例劃分。所以一般以 WFQ 而言，weight：PQ > AQ（GQ>SQ）> DQ，系統管理者再依據實際 Traffic 狀況對系統參數加以調整。但值得注意的是，任何一種 Queue（PQ 或是 AQ）不當地佔據過多的 weight 或未經計算規劃都易影響系統的執行效率或導致封包遺失的可能，不可不小心並隨時監看與調整所設定的系統狀態是否符合預期。

當 ISP 與使用者簽訂 SLA 之後，ISP 就必須針對用戶的條件去設定網路上系統與設備的一些參數以符合 SLA 中的需求。而進行如上述所提之 PQ、AQ（GQ、SQ）、DQ 等 Queue 長度，AQ（GQ、SQ）、DQ 等的 RIO 參數，還有 WFQ 中各個 Queue 的 weight 參數等的設定動作（Resource Provisioning）。

對於 Diffserv，Edge 路由器執行 MF，要符合 SLA，在 classification、policing、shaping 上可以直接依據 profile 執行，但是對於 Queue Length、RIO、Scheduling 的設定則必須在執行一段時間後蒐集到相關數據，分析其訊務特徵，具備訊務的特徵值之後再進行設定。通常是利用 SNMP 或是 COPS 來更動網路設備的設定參數，並且在一段時間的 QoS 監控後，得依據 Internet 的訊務變化及 SLA 作調整。但是上述的動作對於 Core 路由器而言，執行上有相當的困難，因為 Core 路由器執行的是 BA，看到的是 DSCP，所以無法分辨進出 Core 路由器的訊務變化來自何方。Queue Length、RIO 參數的設定必須就整體網路考量，無法就單一使用者的 SLA 考量。有找到某一篇論文的公式可以作為參考：

pf：provisioning factor used as the output rate of the queue, determined by the corresponding class and maybe by the domain policy as well.

For example, *pf* can be set to

2.0 for PQ

1.5 for AQ

1.2 for DQ.

r(q)：inflated output rate of the three queues

Percentage of link capacity of queue q = r(q) / [r(PQ) + r(AQ) + r(DQ)],

where q is either PQ or AQ or DQ

Diffserv 提供的是一種可在 Internet 上實行的 QoS 並且具備 scalable 的架構。與 Intserv 不同的是 Diffserv 提供了 coarse-grain 的 end-to-end QOS。目前的路由器或交換器都已支援 Diffserv，所以網路人員在規劃網路時已經可以考慮如何導入 Diffserv 架構使整體網路效率提昇，而非僅只有 best-effort 的 dump design（or you think it's an excellent design）。Diffserv 架構再配合 MPLS-traffic engineering 的實行則整個網路的 QoS 機制會更加完整及健全（robust）。

3.2 新一代網際網路協定－IPv6

現行所使用的 IP 協定為 IP version 4 (簡稱為 IPv4)，開發至今已逾數十年，蓬勃發展之後如何解決現有面臨的問題及因應未來更多樣化的的網路需求，遂成為要維持 IP 網路發展的最重要課題。新一代網際網路的世界不僅是人人上網，各種家電及休閒影音娛樂設備等都會連上 Internet（All IP Network）。如此多采多姿的網際網路資訊世界，將導致現今使用之網際網路通信協定-32 位元的 IP 網路定址方式加速面臨位址即將耗盡的問題。此外，未來的網路應用服務對於各種服務品質的要求亦不斷的提高，舉凡網路安全、行動數據、頻寬保障、及服務分級等，傳統 IPv4 所定的相關協定已漸無法滿足未來網際網路需求，新一代之 IP(Internet Protocol)協定(簡稱 IPv6)遂被提出來解決此一問題。

網際網路起源於 1968 年開始研究的 ARPANET，當時的研究者們為了給 ARPANET 建立一個標準的網路通信協議而開發了 IP 協議。開發者當時認為 ARPANET 的網路數量不會超過數十個，因此他們將 IP 協議的位址長度設定為 32 位元，其中前 8 個位元用以標識網路，其餘 24 個位元用以標識主機。然而隨著 ARPANET 日益膨脹，

IP 協議開發者意識到原先設想的標識網路的方式已經無法滿足實際需求，相對的因應技術也隨之誕生，其中包括「非分類之領域間路徑選擇」（Classless InterDomain Routing，CIDR）及「網路位址轉譯」（Network Address Translation, NAT）等技術，說明如下：

(1)「非分類之領域間路徑選擇」（Classless InterDomain Routing，CIDR）：此技術是節省傳統 IP 分類(Classical)位址配發的一個措施。CIDR 的原理是打破原本 IP 制式化的分類 ClassA、B、C 等，節省因 IP 切割所造成的損失。例如，假設某個企業網路有 1,000 個主機，那麼可為該使用者分配 8 個連續的「類別 C 位址」，例如：192.56.0.0 至 192.56.3.0，並將子網路遮罩設定為 255.255.252.0，即位址的前 22 位元標識網路，其餘的 10 位元標識主機。儘管使用 CIDR 技術可以保護類別 A 或 B 位址免遭無謂的消耗，但是依然無法從根本上解決 IPv4 面臨的位址耗盡問題。

(2) 網路位址轉譯（Network Address Translation，NAT）：它是一種將「私用 IP 位址 (Private IP)」轉譯成可以在 Internet 上使用的「公共 IP 位址 (Public IP)」的機制。NAT 技術使得企業不必再為無法得到足夠的合法 IP 位址而發愁了，它們只要為內部網路主機分配 Private IP 位址，然後在內部網路與 Internet 介接點設置支援 NAT 的路由器，此路由器僅需具備由少量 Public IP 位址組成的 IP 位址池，就可以解決大量內部主機連線 Internet 的需求了。由於目前要想得到一個類別 A 或類別 B 位址十分困難，因此許多企業紛紛採用 NAT 的機制。然而，NAT 也有其無法克服的弊端。首先，NAT 會使網路傳輸效能降低，其次 NAT 必須對所有來往 Internet 的 IP 資料進行位址轉譯，但是大多數 NAT 無法完整保留 IP 表頭的訊息，這個缺陷將導致某些必須將位址信息嵌在 IP 數據報負載中的

Security)及 QoS(end-to-end quality of service)等機制的失敗。

IPv6 是 IETF 為了滿足現今的需求而發展出來的，IPv6 保留了 IPv4 成功之處，所以 IPv6 的原則與 IPv4 是相類似的，IPv6 所做的修正與新增部分敘述如下：

(1) IPv4 表頭格式

IP 表頭(IP Header)包括版本、表頭長度、服務型態、封包長度、識別號碼、旗號、區段位移、存活時間、協定、表頭檢查碼、起始位址、目的位址等，接著才是 IP 資料。IPv4 表頭各欄位，參考下圖所示，其定義說明如下：

- 版本 (Version)：標示 IP 的版本。
- 表頭長度 (IP Header Length)：IP Header 包含固定部份和選項部份。一般只有固定部份時，其長度為 20 bytes，選項部份則長度不固定。
- 服務型態 (Type of Service)：標示此封包所期望的服務品質。
- 封包長度 (Total Length)：標示整個 IP 封包的長度、包括表頭(Header)及負載(Payload)，其數值以 byte 為單位。
- 識別 (Identification)： 標示封包編號（Sequence Number）。
- 旗號 (Flag)：用來標示封包的切割與組合。
- 區段位移 (Fragment Offset)：標示此區段在原來的封包中的起始位置。
- 存活時間 (Time to Live)：標示封包所能允許經過的節點數。
- 協定 (Protocol)：標示上一層協定的種類。
- 表頭檢查碼 (Header Checksum)：標示表頭之錯誤檢查碼。
- 來源位址 (Source Adress)：標示 IP 資料的來源位址。
- 目的位址 (Destination Address)：標示 IP 資料目的位址。

- 選項 (Option)：IP 有不同的選項。
- 封包組合及拆解 (Padding)：此欄位用以填塞 IP 表頭為 32 位元的整數倍。

(2) IPv6 表頭格式

IPv6 基本表頭長度是 IPv4 基本表頭長度的兩倍（40 Bytes），它卻含有較少資料欄位。IPv6 基本表頭格式，如下圖所示，其中大部分的空間都分配給兩個欄位，即來源位址(Source Address) 欄位與目的位址(Destination Address) 欄位，這兩個欄位各佔 16 個位元組（128 bits），是 IPv4 相對欄位長度的四倍。除此之外，IPv6 基本表頭還有另外五個欄位。版本欄位說明這個協定是第六版；訊務等級 (Traffic Class)欄位及資料流標記 (Flow Label)欄位用途皆為服務品質控制用；負載長度(Payload Length) 欄位則標示資料的長度，但並不計算表頭的長度；下一表頭 (Next Header)欄位；跳躍點限制(Hop Limit) 欄位相當於 IPv4 的 Time-to-Live 欄位。

相關欄位的增減及修訂說明如下：

首先，取消以下 6 個在 IPv4 之欄位：

- 表頭長度(Header Length)：由於 IPv6 係採固定表頭長度，故不再需要。
- 服務型態(Type of Service)：此欄位改名為 Traffic Class，但對應相同的服務機制。
- 識別 (Identification)：由於 IPv6 只支援端點對端點(end-to-end) 分割，故不再需要這些欄位。
- 旗號(Flags)：同上。
- 區段位移(Fragment Offset)：同上。
- 表頭檢查碼(Header Checksum)：靠著媒介存取(Media Access)

控制程序中的檢查總和，不需要再重複檢查，如此可以減少表頭處理的負擔。

其次，有三個欄位重新定義：

- 長度(Length)：由於 IPv6 表頭長度固定，IPv4 的「封包長度」欄位由 IPv6 的「封包負載長度 (Payload Length)」所取代。
- 協定 (Protocol Type)：「協定」欄位重新命名成「下一表頭 (Next Header)」，用以反映 IP 封包新的封裝架構。此外，除了原先的 UDP 協定和 TCP 協定型式外，亦可增加延伸表頭(Extension Header)。
- 存活時間 (Time To Live)：此欄位變更成「跳躍點限制 (Hop Limit)」，以跳躍節點數取代時間為單位，防止封包在網路上行成迴圈。

最後，增加二個新的欄位，用以支援即時(Real Time)訊務之需求：

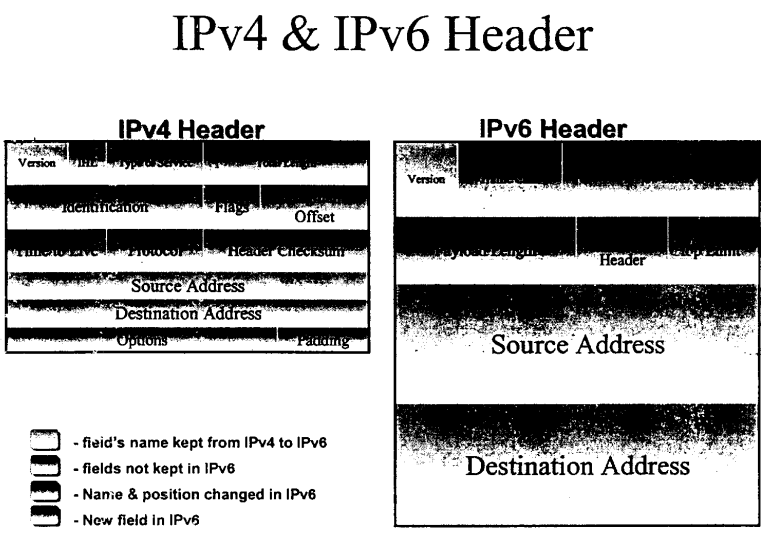
- 訊務等級 (Traffic Class)。
- 資料流標記 (Flow Label)。

雖然表頭的整體長度是增加的，欄位的數目卻相對減少了。此外，選項機制(Option)是完全地被修正，選項欄位是由延伸表頭（Extention Header）來取代且置放於 IPv6 表頭和轉送層(Transport Layer) PDU 之間，目前已經定義下列的延伸表頭。

- Hop-by-Hop 延伸表頭：定義需要 Hop-by-Hop 處理的特別選項。
- 目的選項表頭(Destination Option Header)：包含由封包最後目的地處理的透通資訊。
- 路由表頭(Routing Header)：提供延伸路由選擇，其功能與 IPv4 來源路由選項功能相同。
- 區段表頭(Fragment Header)：包含端點與端點分割與重組資訊，

幾乎與 IPv4 區段控制參數是相同的。

- 認證表頭(Authentication Header)：提供封包整合與認證。
- 封裝安全負載(Encapsulating Security Payload)：提供安全保密功能。



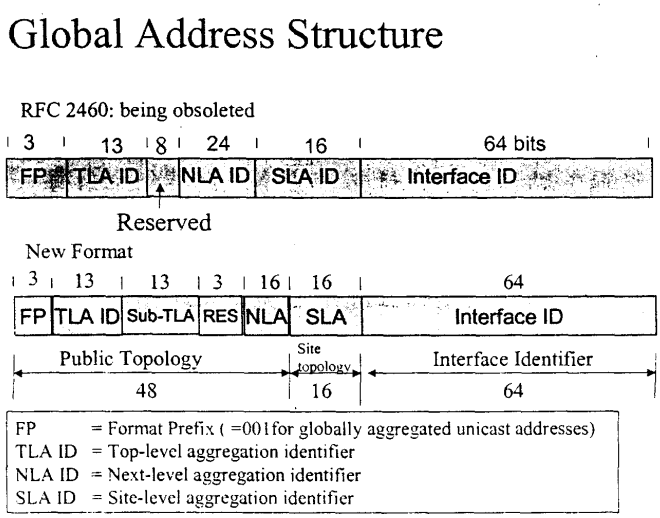
IPv4 與 IPv6 表頭格式

IPv6 的位址長度為 128 位元，表示方式是將 16 個位元畫分成一個區塊，每一區塊的數值以 16 進位格式表示，各區塊間再以「：」區隔，例如：3FFE:3600:0000:2F00:02AA:00FF:FE31:5A9C；透過移除各區塊中連續前置的「零」，可簡化 IPv6 位址的表示法，如上例可簡化為：3FFE:3600:**0**:2F00:2AA:FF:FE31:5A9C 或是透過移除中置連續為「零」的 16 位元區塊，可進一步簡化 IPv6 位址的表示法，如上例可簡化為：3FFE:3600::2F00:2AA:FF:FE31:5A9C。

- IPv6 位址分級架構

IPv6 則為點對點通信設計了一種具有分級結構的位址，這種位址

被稱為可聚合全球單點播送位址（Aggregatable Global Unicast Address），其分級結構劃分如下圖所示。包括起始 3 個位元的「位址類型」，13 個位元的「Top-Level Aggregator Identification (TLA ID)」、13 個位元的「Sub-TLA Identification (Sub-TLA ID)」、16 個位元的「Next-Level Aggregator Identification (NLA ID)」、16 個位元的「Site-Level Aggregator Identification (SLA ID)」、64 個位元的「Interface ID」。TLA 是與長途服務供應商和電話公司相互連接的公共網路接入點，它從國際 Internet 註冊機構如 IANA 處獲得位址。NLA 通常是大型 ISP，它從 TLA 處申請獲得位址，並為 SLA 分配位址。SLA 也可稱為用戶（Subscriber），它可以是一個機構或一個小型 ISP。SLA 負責為屬於它的訂戶分配位址。SLA 通常為其訂戶分配由連續位址組成的位址塊，以便這些機構可以建立自己的位址分級結構以識別不同的子網。分級結構的最底級是網路主機。



IPv6 位址分級架構

IPv6 的位址定義了三種類型：單一播送(Unicast)位址、任一播送(Anycast)位址、及多點播送(Multicast)位址。

(1) 單一播送位址：一對一的介面識別位址，當封包要傳送到單一播送的位址上時，此即表示封包將傳送到此單一播送位址所代表的單一介面上，由目的地位址標示接收端的主機或路由器，而封包會沿著最短路徑路由到目的位址。。

(2) 任一播送位址：一對任一介面的識別位址，當封包要傳送到一個任一播送位址時，即表示傳送到以此位址作為識別之多個介面中的一個。這是一種 IPv6 所提供的新位址。任一播送提供一個位址指給多個介面，通常是不同的網路主機。其目的地位址是一組共享單一位址的網路主機。其封包會沿著最短路由推進到那一組有此位址的網路主機，然後再將封包傳送給群組中的最近的一台網路主機，其最短路由根據距離衡量的路由協定決定。

(3) 多點播送位址：一對多的介面識別位址，當封包要傳送到一個多點播送位址時，即表示傳送到以這組位址作為識別之所有介面。多點播送的目的地位址是一群網路主機，且可能散布在不同的地區。透過多點播送，其封包會被傳送到群組中的每一成員。值得注意的是 IPv6 因為已去除 Broadcast 機制，所以多點播送機制在 IPv6 協定中相當重要而且應用的更廣泛。

依據此 IPv6 協定的設計，可歸納下列七項特性：

(1) 較大的位址空間

IPv4 使用 32 個位元定址，定址能力為 2^{32}，這樣的定址能力在 20 年前目的只是提供學校或研究單位用途來說，十分充裕，但面對現今與未來，家用與商用電腦甚至於一般設備皆使用網際網路的情況來說，網際網路位址明顯不足，因此 IPv6 使用 128 個位元加以定址

網際網路節點，定址空間高達 2^{128}（32 bits 擴充為 128 bits），預估地球上的每個人可分到一百萬個 IP 位址，所以未來從 PDA 到手機，甚至 CD 隨身聽、手錶等電子商品都將會有一個獨一無二的 IP 位址，可以透過網路取得更新資訊或進行遠端遙控等。

(2) 整合認證及安全的機制

IPv4 原為提供學校研究單位之用，使用者單純且環境也較為封閉，所以 IPv4 在設計之初並未考慮安全性問題，資料在網路上並未使用安全機制傳送，因而在早期的 Internet 時常發生企業或機構網路遭到攻擊、機密數據被竊取等網路安全事件。相較於 20 年前，現今的網際網路極為普遍，同時伴隨著大量具安全需求資訊之交換，安全性成為任何一種網路的技術都必須面對的問題，雖然 IPv4 可以透過網際網路安全協定(IP Security，IPSec)提供安全保護，但架設及管理上都是額外的負擔，有鑑於此，IPv6 協定設計時已考量網路安全功能，希望提供內嵌式的點對點安全保護能力，以提供未來網際網路一個更安全的資料交換方式。IPv6 係利用 Next Header 中的 Authentication Header 及 Encrypted Security Payload Header 對傳輸的資料進行認證及加密，故未來使用者將不需透過額外的設備或軟體就可以達到網路安全的功效。

(3)較佳的路由效率及最佳化

IPv6 將位址空間使用階層式的方式劃分為 Top Level Aggregator Identifier、Next Level Aggregator Identifier、Site Level Aggregator Identifier 三層，各層負責授權 IP 網段給其下層的機構，此種管理方式使得交換的路由資訊可以經由彙整變得非常精簡。此外，IPv6 亦支援 anycast 的功能，藉由從路由器的路由表中挑選出一台最佳(最短距離或最小花費等)的主機，從而縮短回應時間並將流量負載分散及節

省頻寬。

(4) 服務品質的保證

IPv6 的表頭中，保留了 Flow Label 的欄位，可和 Multiple Protocol Label Switch (MPLS)的技術相配合，不同的資料流對應到不同的 Flow Label，可做為服務品質控制的依據。網際網路在早期僅提供資料交換之用，對於資料傳送品質的要求以正確性為第一優先，然而隨著多媒體，網際網路電信服務等在網際網路上遞送，IP 封包提供服務品質的特性成為其一大考驗，IPv6 在表頭加入兩項參數，包括資料流種類(Traffic Class)與資料流標記(Flow Label)將有助於服務品質控制機制的設計。

(5) 自動設定及行動性的功能

早期電腦無移動性的考量，然而隨著電腦技術的日新月異，手提式電腦，手持式設備幾乎隨手可得，人們對於網際網路支援行動功能的需求日益殷切。因此 IPv6 也在設計上加入支援行動 IP 的機制，以利未來支援行動網際網路。

而支援行動 IP 機制中的另一項重要特性即藉由網路芳鄰找尋(Neighbor Discovery)與自動定址(Auto-configuration)機制來簡化使用者 IP 位址的設定。IPv6 網路上的主機可自動取得 IP 不需透過手動設定。而利用 Extension Header 的 Destinetion Header 與 Routing Header，將使行動通訊中之路由機制獲得最佳化，解決了三角路由(triagle route)的問題。

自動定址(Auto-configuration)機制包括全狀態自動配置（Stateful Auto-configuration）及無狀態自動配置（Stateless Auto-configuration）。

- 全狀態自動配置：在 IPv4 中，動態主機配置協議（Dynamic Host Configuration Protocol，DHCP）實現了主機 IP 位址及其相關配置

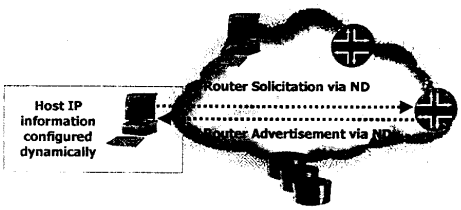
的自動設置。一個 DHCP 服務器擁有一個 IP 位址池(IP Pool)，主機由 DHCP 伺服器賦予 IP 位址並獲得有關的配置信息（例如：Gateway 及 DNS 位址），由此達到自動設置主機 IP 位址的目的。IPv6 繼承了 IPv4 的這種自動配置服務，並將其稱為全狀態自動配置（Stateful Auto-configuration）。

無狀態自動配置：除了全狀態自動配置，IPv6 還採用了一種被稱為無狀態自動配置（Stateless Auto-configuration）的自動配置服務，如下圖所示。在無狀態自動配置過程中，主機首先啟動 IPv6 協定，產生一個 Link-local IPv6 位址（IEEE 已經將網卡 MAC 位址由 48 位改為 EUI-64 格式，即將主機採用的網卡的 MAC 位址（48 bits）中間加入 0xFFFE 成為 64 bits。接著主機向該位址發出一個被稱為芳鄰找尋（Neighbor Discovery）的請求，以驗證位址的唯一性。如果請求沒有得到回應，則表明主機自我設置的鏈接本地單點播送位址是唯一的。否則，主機將使用一個隨機產生的介面 ID 組成一個新的鏈接本地單點播送位址。然後，以該位址為來源位址，主機向本地鏈接中所有路由器多點播送一個被稱為路由器請求（Router Solicitation）的配置信息請求，路由器以一個包含一個可聚合全球單點播送位址和其它相關配置信息的路由器公告回應該請求。主機用它從路由器得到的全局位址首碼加上自己的 Interface ID，自動配置 IPv6 位址，然後就可以與 Internet 中的其它主機通信了。使用無狀態自動配置，無需手動干預就能夠改變網路中所有主機的 IP 位址。例如，當企業更換了連接 Internet 的 ISP 時，將從新 ISP 處得到一個新的可聚合全球位址首碼。ISP 把這個位址首碼從它的路由器上傳送到企業路由器上。由於企業路由器將周期性地向本地鏈接中的所有主機多點播送

路由器公告，因此企業網路中所有主機都將通過路由器公告收到新的位址首碼，此後它們就會自動產生新的 IP 位址並覆蓋舊的 IP 位址。對於網管人員而言，在 Re-numbering IP 位址時有很大的方便性與效率。

Stateless Auto-configuration

- 主機啟動IPv6協定
- 主機送出Router Solicitation或是路由器送出Router Advertisement
- 主機獲取IPv6 Prefix



IPv6 Stateless Auto-configuration

(6) 封包表頭處理更有效率

IPv6 簡化原先 IPv4 的表頭設計，雖然 IP 位址從原來的 32 位元加長四倍成為 128 位元，但表頭長度僅成長兩倍且固定長度，因為 IPv6 將「可選擇性擴充部分」與「IP 切割」的功能刪除成為固定檔頭長度。除此之外亦同時刪除檢查碼(Checksum)並盡可能將每個欄位對齊在位元組上，這樣固定長度與對齊的設計讓表頭簡化許多，在處理封包表頭時將更有有效率。

(7) 可擴充性

刪除了原先 IPv4 可選擇性擴充部分，IPv6 設計以「下一表頭(Next

Header)」的方式來增加表頭的可擴充性。使用者可以透過「下一表頭(Next Header)」的方式自行在表頭中指示下一個表頭的內容以利網路端或是接收端完成特定的工作，其為 IPv6 可擴充性設計的實施範例，這樣的設計讓 IPv6 檔頭具更高的擴充性。

目前各國皆已相繼投入 IPv6 技術之研發與推動。亞太地區以日本與韓國為首，陸續投入大筆經費，並在政府資金挹注下逐見成效，日本更有數家 ISP 已於 2001 年中開始提供跨國之 IPv6 商用服務，中國大陸亦急起直追。在歐洲方面，歐盟委員會已正式呼籲歐洲各國政府及工業界傾全力支持 IPv6，更於歐盟行政系統下成立 IPv6 工作小組 (EC IPv6 Task Force)，為歐洲地區勾勒出 IPv6 整體之發展藍圖。近年來 IPv6 發展已由學術界的研究，邁入許多國家之科技發展重要政策階段。IPv6 在國內也有許多突破性的發展，本公司已於 2001 年 7 月提供 HiNet IPv6 試用服務，另外 TANet 及國家寬頻實驗網路 (NBEN)亦分別著手建置 IPv6 相關學術及研究網路，而新的「TWAREN 網路」的規劃亦包含 IPv6 的建置。

日本可說是投入 IPv6 最積極的國家，目前是世界上申請取得 IPv6 位址最多的國家。這應該都得歸功於日本政府於西元 2000 年成立 IPv6 Council，由首相發佈全力推動 IPv6 之政策，明訂西元 2005 年日本將達成網路由 IPv4 轉換成 IPv6 的目標，且大筆投入 80 億日圓之發展經費。此舉大大的促成日本 IPv6 產業全面性的起飛，除 NTT 與 Hitachi 自行研發 IPv6 路由器外，亦有許多 ISP 免費提供客戶試用，其中 NTT Communications 及 IIJ 兩家更率先推出商用 IPv6 服務。

除了採用 IPv6-over-IPv4 Tunnel 方式外，NTT Communications 及 IIJ 亦提供 Native IPv6 連線，另外也提供 IPv4-IPv6 translator，使 IPv4 主機可與 IPv6 主機連繫。至於服務對象，目前仍限於專線用戶，IPv6

ADSL 上網亦即將推出。至於在應用服務方面，仍著重在 WWW、DNS、FTP 及 TELNET 等基本項目，NTT 曾於 IPv6 Forum 會議中展示其 TV conference 及 Music Distribution with IPSec 等功能，非常吸引人。日本已於西元 1999 年八月在位於東京的 KDDI Otemachi 建立 IPv6 網路交換中心 NSPIXP6，目前已有超過二十五家 ISPs 與它互連，是世界最大的 IPv6 IX 之一。

在韓國方面，韓國亦十分關注 IPv6 之發展，不但成立測試平台(6Bone-KR)及 Korea IPv6 Forum 以促進 IPv6 之發展，並且建置 6NGIX IPv6 網路交換中心，目前是僅次於日本之第二大取得 IPv6 位址配置單位的國家，已有數家 ISP 提供試用服務。另外，許多全球性之 IPv6 研究計劃在進行，致力於轉移機制及應用軟體之研發，同時提供測試平台並制定推廣策略。其國家策略亦參考日本，預計在 2006 至 2010 年間，IPv6 網路規模會逐漸超越 IPv4 網路，2011 年後完成網路全面 IPv6 化之建置。

韓國約在 1994 年開始了他們 IPv6 實驗網路的測試工作。初期的發展，正如同台灣現在的 IPv6 進程一樣，是緩慢的在進行，一直到 2001 年左右，整個 IPv6 環境開始有了重大的發展。大約是在 2000 年起開始受到 ISP 業者的重視，在 KRNIC 及各大 ISP 業者的努力之下，從 2000 年 9 月迄今不到兩年的時間裡，他們的 IPv6 商用網段由 2 組劇增到 13 組，也由於各大 ISP 的相繼推展，更進而帶動了韓國下一代 IPv6 產業的起飛，像是 LG 與日本 Hitachi 結盟發展大型骨幹網路設備、Opicom 自創周邊的網路閘道器、i2Soft 發展的 IPv6 網路軟體等等。

中國大陸的情況最受矚目，一般認為 IPv6 與中國大陸的網路網路發展有密切關係，有云：「中國因 IPv6 而起，IPv6 因中國而生」。

中國大陸對 IP 位址的需求隨上網人口(目前僅次於美國，居世界第二)急遽發展與日俱增，為發展 IPv6 最具潛力之地區。中國大陸自 1998 年即開始發展及推動 IPv6，目前有許多進行中的大型軟硬體研究及網路建置計劃，除於 2001 年與日本簽訂官方層級之 IPv6 合作備忘錄外，每年舉辦數次大型 IPv6 國際研討會，皆吸引大批國內外廠商參與。

中國大陸在學術方面，其最大之教育研究網路 CERNET 已逐步建置全國性之 IPv6 網路，設立測試平台進行 IPv6 研究發展，目前並已申請一個 IPv6 位址區段。IPv6 在中國大陸的發展，是由政府單位所支持，將持續推展與國際間的合作、推廣更多的試用網路、並發展更多本土化 IPv6 的產品。

相對地在網際網路發達的美國就有不同的發展境遇。美國在 IPv6 的推展上較不積極，最重要的原因是美國並未面臨 IPv4 位址不足的問題，但是美國的網路設備廠商已經生產 IPv6 的產品了，軟體業者也已將新的作業系統提供 IPv6 功能，但是網路服務業者仍只是停留在試用階段，他們所持的理由大多是尚未有客戶提出此需求，也即尚未見到商機所在，但是各家網路服務業者都相信，他們都具備能夠立即啟動這項服務的能力。不過值得注意的是國防部今年宣佈其未來的網路設備採購必須將 IPv6 列入採購規格而能源部及國防部的網路新計劃 ESnet (research institute under the US Department of Energy) 及 DREN (experimental network of DoD)也都將 IPv6 協定列為標準。

歐洲因為是無線通信及 3G 發展之重鎮，很早即投入 IPv6 之發展。重要之活動為成立 Euro6IX 計劃，該計劃是一整合歐洲重要電信業者、ISP、設備廠商及學研界所合作推動的為期三年的計劃。希望建置橫跨全歐洲並與世界各重要 IPv6 網路交換中心連接之 Native

IPv6 網路，惟尚未有真正商用運轉之服務。

另外歐盟委員會(EU Commission)已正式建議各國政府及工業界儘早投入 IPv6，2001 年更成立 IPv6 工作小組(IPv6 Task Force)，為歐洲地區規畫 2005 前整體 IPv6 發展藍圖。目前歐洲地區 IPv6 相關的跨國研究計劃共有 31 個，參與國家達 37 國，投入研究的單位超過 100 個，總金額達 1.56 億歐元(其中 0.85 億直接由歐盟委員會撥付)。2002 年所宣佈的「eEurope2005」亦將 IPv6 的推動列為重點。

而在國內方面，行政院國家資訊通信基本建設推動小組（NICI）成立「IPv6 推動工作小組」，整合產、官、學、研界的資源與力量，積極推動 IPv6 網路建設及產業應用發展計畫。IPv6 推動工作小組輔導工研院與台灣網路資訊中心正式成立「台灣 IPv6 論壇」，致力 IPv6 的推廣服務、技術及應用的開發，同時扮演產業界與政府機關間溝通的橋樑。目前已獲得近 20 家資訊通訊廠商及 ISP 應允加入，包括 HiNet、亞旭、星通、智捷、友訊、智邦、東森寬頻、上元等。此外，行政院已經宣示 IPv6 為我國重要網路建設工作項目，預計 93 年度學術網路骨幹可全面支援 IPv6，94 年度建置完成國內 IPv4 和 IPv6 轉換機制，95 年度完成符合標準的 IPv6 測試驗證中心，96 年度就可完成所有 ISP 及各項網路軟硬體以支援 IPv6。

台灣是亞太地區僅次於日、韓兩國之第三大 IPv6 發展國。而本公司於 2000 年 2 月向 APNIC 申請取得我國第一個 IPv6 商用位址配置，同年 10 月 TWNIC 亦協助 TANet 申請到第二個 IPv6 位址分配，目前 TANet 獲取 IPv6 Address Block 2001：288：：/32 用以籌畫建置學術用途之 IPv6 網路。在網路服務方面，ISP 方面，中華電信最早申請到商用 IPv6 位址，IPv6 Address Block 為 2001：238：：/32，並自 2002 年 7 月起提供試用服務，服務項目包括 IPv6 Native Service、

IPv6 Tunnel Service 及 IPv6 TWIX Service 等三種。

早期我國 IPv6 之發展多屬於研究與學術性質，包括有清華大學 IPv6 路由器研發及各大學相關研究計劃等；大型 IPv6 試驗網路方面則有電信研究所於 1997 年開始 IPv6 測試平台之建置。電信研究所除了建置 IPv6 測試用主機、伺服器及路由器外，亦同時加入國際 IPv6 試驗網路 6Bone，在 1999 年 2 月建置成為我國連接至 6Bone 之主幹匯接站(Backbone Site)，與世界各國十多個骨幹匯接站建置連線，提供我國 IPv6 相關的網路群轉接至國際測試網路之服務（6Bone）。目前電信研究所也已規劃建置 IPv6 標準測試實驗室，以協助未來國內 IPv6 相關技術與產品之驗證測試；而數據分公司則為基礎建設計劃成員除了努力於 IPv6 網路基礎建設之外並有 IPv6 影音子計劃來建設 IPv6 影音服務平台提倡 IPv6 之普遍性。

接觸 IPv6 的人不免都會有一個疑問，究竟 IPv6 是一時的流行趨勢或是一種策略，但是一些著名的公司，像是 Cisco、Nokia、Ericsson、Sony、HP、NEC、NTT、British Telecom、 Matsushita、Microsoft 等廠商都已投入相當的人力及資金，以將 IPv6 的協定整合至他們的產品之中，很顯然的，IPv6 經過長期的發展與驗證，其不只是一時流行的技術，而是一種實際可用的技術。

IPv6 的存在不只是為了它能夠增加可用的 IP 位址範圍，事實上，IPv6 的發展正是針對 IPv4 的一些功能或協定加以改進，例如簡化的 Header 結構、內建式的安全機制等，不過也許 IPv6 最顯著的突破就在於它的 IP Address Auto-configuration 的特性，IPv6 提供移動的裝置能夠迅速取得或轉換 IP 位址，而不需要 Foreign Agent 的機制，Auto-configuration 也代表了即插即用（Plug-and-Play）的網路連線方式，任何電腦、印表機、數位相機、網路電話等需要 IP 的電器，均

能很便利的連上家庭網路免去使用操作手冊的麻煩。

不可諱言的，許多人心中不免還是有個疑問，也就是如何「IPv6」。目前大部分的系統及應用程式大多是構建在 IPv4 網路上，如何找出 IPv6 的關鍵應用程式(Killer Application)，使得 IPv6 網路應用活絡起來是當前一大課題。不過，我們相信驅動全球化 IPv6 的運用及發展將伴隨著行動用戶的日益增加所產生的行動上網需求與寬頻上網服務而日益明顯。另外包含在多媒體串流、語音、影像或網路遊戲等方面的服務模式及規模，都可能成為 IPv6 發展的關鍵。亞洲由於人口眾多，但所擁有的 IPv4 位址資源卻是相對不足。因此，在最近 IPv6 國際會議上，大家一致認為 IPv6 的發展順序一定會是亞太地區最先，再來是歐洲，最後才是美洲。這也就無怪乎人口眾多且科技較發達的日、韓會如此倚重及期待 IPv6 之發展。我國雖暫居亞洲 IPv6 發展之第三位，其實在起跑點上已落後日、韓甚多。台灣值此科技轉型之時，更當好好把握我國多年來在 IT 產業所打下的基礎，繼續發揮以往對產業脈動掌握的高度洞察力與機動性，及早為迎接下一波網際網路產業競爭建立穩固之基礎，才能立於不敗之地，創造另一新的契機。而對於 HiNet 而言，IPv6 何時才興盛是項未知數但當年網際網路也未嘗試如此所以對此我們亦需一步一趨跟緊世界潮流才不致錯失下一代網際網路的盛會。

3.2 MPLS

MPLS 屬於新發展之網路轉送機制，是新一代的 IP 高速骨幹網路交換標準，由 IETF （Internet Engineering Task Force，網際網路工程專案小組）所提出，持續由 Cisco、Juniper、ASCEND、3Com、Nortel 等網路設備大廠所主導。

MPLS 是概念源自於 IP Over ATM 技術，在 Frame Relay

及 ATM Switch 上結合路由功能，封包透過虛擬電路來傳送，只須在 OSI 第二層（資料鏈結層）執行硬體式交換（取代第三層（網路層）軟體式 routing），整合了 IP 選徑作業與第二層標籤交換作業為單一的系統，因此可以解決網際網路上封包經過各層協定封裝的 overhead 問題，使網路封包傳送的延遲時間減短，更適合多媒體訊息的傳送，增加網路傳輸的速度。因此，MPLS 最大技術特色為可以指定封包傳送的先後順序，使用標籤交換式（Label Switching），網路路由器只需要判別標籤，進行轉送處理。簡而言之，MPLS 的基本運作原理是提供每個 IP 封包一個標籤，由此決定封包的路徑以及優先順序，與 MPLS 相容的路由器，會將封包轉送到其路徑前，僅讀取封包標籤，無須讀取每個封包的 IP 位址以及標頭（因此網路速度便會加快），將所傳送的封包置於 Frame Relay、ATM 或 SONET 的傳輸線路上，迅速地將封包傳送至終點的路由器，進而減少封包的延遲。

目前一般大型 Tier 1 ISP 網路（如：AT&T、QWest、Level 3、Worldcom 等）其核心中有三種常見的 MPLS 應用：

（1）訊務工程 (Traffic Engineering)

（2）服務等級（CoS）

（3）虛擬私有網路（VPN）

（1）訊務工程 (Traffic Engineering)

訊務工程允許 ISP 將訊務流移出原先 IGP 所算出的最短路徑，並將其轉送到網路中較不擁擠的路徑。由於業界對網路支援的需求急速增加，加上 IP 應用的重要特性，以及服務供應商市場的競爭越來越激烈，因此 Traffic Engineering 已成為主要的 MPLS 應用。有效的 Traffic Engineering 解決方案，可為網路中所有鏈路提供訊務平衡負載

功能，並將訊務導入網路中，以避免路由器、交換器等個別元件被過度或是低度使用。如此將可提高網路運作效率，並可提供更多效能可預期 (如 VoIP) 的服務。MPLS 非常適合做為大型 ISP 網路的訊務工程基礎，其原因在於 MPLS TE 允許網管人員指定服務供應商網路中的特定 LSP 路徑並且針對每一 LSP 進行統計，將結果輸入網路規劃及分析工具中，以便分析網路瓶頸及骨幹使用率供未來網路擴充規劃之用；而限制性路由 (Constraint based Routing)則 提供許多 sub-optimal 路徑進階功能，因此在建立 LSP 之前，可先確定其符合特定的效能要求。

在 Traffic Engineer 方面需另外考慮到的是故障復原與功能回復。以下針對啟動 MPLS 時對於故障復原與功能回復可運用的不同方法進行分別說明：

（a）具備次要 LSP 的 MPLS：此項支援需倚賴 IGP 收斂（convergence） 功能。LSP 最簡單的重路由方式，就是從頭端（head-end）路由器重送信令，以便建立一條通過整體網路的新路徑，其重路由時間與偵測時間、IGP 重收斂時間，以及信令重送時間等息息相關。此一保護機制可在主要 LSP 故障時，提供一條替代的且以預先重送信令的備用路徑。如此一來，當主要 LSP 故障時，ingress/head-end 可立即將訊務重導至次要 LSP 上，這種方法的優點是，不需要再將信號重新送到新路徑，因為沿著次要路徑中的所有路由器會立即將次要路徑切換到熱備用的狀態。此一方法可縮短將信號從 Ingress 節點重新送至 LSP 所產生的延遲時間，可更快速地將故障復原。

（b）快速重路由（Fast Reroute）：快速重路由（Fast Reroute，尚未完全標準化）透過硬體加速的 LSP 故障復原可大幅縮短故障復原時間

（＜50ms，sub-second）。對於需要 SONET APS 這類快速復原時間，以及 VoIP 這類對延遲敏感的應用而言，Fast Reroute 是絕佳的選擇。

（c）MPLS LSP Link/Node Protection：MPLS LSP Link/Node Protection 是一種硬體式保護設計，以便快速地為多條 LSP 執行訊務重路由。Link Protection 機制也可大幅減少保護 LSP 所需執行的各項設定。不同於 fast reroute 只能提供一對一的 LSP 保護，Link /Node Protection 只需使用一條邏輯繞道（logical bypass）LSP 便可同時保護多條 LSP。因此，Link/Node Protection 可為鏈路或節點提供更穩健的備援支援，並可與其他廠商的設備互通。這些功能使得鏈路保護能夠在 MPLS 網路中支援絕佳的擴充性、備援，以及效能。

（d）LSP Preemption： RSVP-TE 藉由立即移除預先搶佔的 LSP 來支援 LSP preemption 特色，因此在建立 LSP 之前，訊務可能會消失不見。Soft-preemption 是現有 preemption 機制的延伸功能，它會嘗試在移除 preempted LSP 之前為其建立新路徑，如此可避免使用 preempted LSP 的訊務遺失。

（2）服務類型（CoS）

服務業者可使用 MPLS 來推出差異化服務（DiffServ）。DiffServ 模式定義各種可將訊務劃分為不同服務類型的機制。如此將可鼓勵用戶將網際網路當作公眾傳輸媒體，以便使用從傳統的檔案共享應用，一直到語音與視訊等對延遲敏感的各項應用。為滿足客戶要求，ISP 業者不僅需採用訊務工程技術（TE），同時還需使用訊務分類技術來達到完全的 QoS，因為訊務工程技術是一種巨觀（macro）的 QoS，而 DiffServ 則是是一種微觀（micro）的 QoS。有下列兩種方式可用來支援基於 MPLS 的 CoS 功能：

（a）E-LSP：可將通過某一特定 LSP 的訊務流排序（queue），以便根據 MPLS 表頭中之 precedence bits 的設定，在某一 LSR 之對外介面上傳送訊務。

（b）L-LSP：ISP 可在兩個邊緣 LSR 之間配置多條 LSP，而每一 LSP 可利用 Traffic Engineering 技術，來提供不同的效能與頻寬保證。頭端 LSR 可將高優先權訊務加入一條 LSP 中、將中等優先權的訊務加入另一條 LSP、將 best-effort 訊務加入第三條 LSP，並將 less-than-best-effort 的訊務加入第四條 LSP。

（3）虛擬私有網路 (VPN)

ISP 業者如欲為客戶提供實際的 VPN 服務，則需解決資料隱匿性的問題，並且在 VPN 中提供非獨一無二的（non-unique）私有 IP 位址。MPLS 可簡單且有效地解決這些問題，因為它是根據標籤中標示的數值，而非封包表頭的目的地位址，來做出轉送決定。

（a）Layer 3 VPN

Layer 3 VPN 遵循 RFC 2547bis 標準，此一標準定義了可容許網路業者使用 IP 骨幹來提供 VPN 服務的機制。Layer 3 VPN 是由許多共用路由資訊的站台所組成，它使用各項政策來管理網路連結。Layer 3 VPN 的所有站台都是透過網路業者現有的公眾 Internet 骨幹來互相串連的。RFC 2547bis VPN 也稱為 BGP/MPLS VPN，因為 BGP 負責在網路業者之骨幹中分送 VPN 路由資訊，而 MPLS 則負責將 VPN 訊務由骨幹轉送到遠端 VPN 站台。因此，我們可以輕易地在 VPN 中新增站台。MP-BGP 可接管資訊分送的工作，以便將資訊分送給骨幹中所有的相關的 PE，因此遠端站台可立即得知 VPN 已新增站台。因為 VPN 是私有網路，因此可選擇使用公眾或私有位址，如 RFC 1918 所

述。如果客戶選擇使用私有位址來連上公眾網際網路基礎設施，則這些位址很可能會跟其他網路使用者所用的私有位址重複；而MPLS/BGP VPN可有效解決此一問題，它可在來自某一特定站台之每一位址的最前方，加入VPN識別標誌（identifier），因而建立了一個不論在其VPN或在公眾Internet中都是獨一無二的位址。此外，每一VPN分別擁有自己的VPN路由表，其中僅只提供與此VPN有關的路由資訊。

（b）Layer 2 VPN

在路由器中部署Layer 2 VPN的方法，非常類似於使用ATM或Frame Relay等Layer 2技術來部署VPN。不過路由器中的Layer 2 VPN以Layer 2格式將訊務來轉送道路由器中。MPLS負責在網路中傳遞這些訊務，最後到了接收端站台時才將其轉換回Layer 2格式，使用者可傳送與接收端設定各種不同的Layer 2格式。MPLS Layer 2 VPN的安全性和隱匿性，與ATM或Frame Relay VPN所支援的特性非常接近。

在Layer 2 VPN網路中，由客戶的路由器，通常是客戶邊緣（CE）路由器，來執行路由。在Layer 2 VPN中，連上服務供應商網路的CE路由器必須選擇使用合適的線路來傳送訊務；而服務供應商邊緣（PE）路由器在收到訊務後，便將其傳送到連接到接收端站台的PE路由器。PE路由器不需要知道客戶的路由拓樸，只需知道用哪一個通道傳送訊務即可。如欲部署Layer 2 VPN，客戶需設定其路由器以便承載所有Layer 3訊務，而服務供應商只需知道Layer 2 VPN需承載的資料量有多少。網路業者的路由器負責在使用Layer 2 VPN介面的各個客戶站台間傳送訊務。PE路由器所設定的政策將決定所用的VPN拓樸。部署Layer 2 MPLS VPN的好處包括：

- 網路業者可使用同一套 Layer 2 設備來提供 Layer 2 VPN 服務。業者可利用現有的 IP 和 MPLS 骨幹網路來提供 Layer 2 VPN 服務。
- 可設定 PE 路由器，使得它在 Layer 2 協定之外，還可執行各種 Layer 3 協定。
- 希望自行控制其私有網路之管理工作的客戶，可能比較偏好
- Layer 2 VPN 而非 Layer 3 VPN 網路。

（c）Carrier-of-Carrier 和 Interprovider 的 VPN

Carrier-of-Carrier VPN 是一種遵循產業標準的 VPN，可容許大型網路業者為其他的服務供應商提供頻寬批發、訊務傳送服務，並可搭配其他的 IP 和 MPLS VPN 服務來創造更高的營收。使用 Layer 2 VPN 也可達到相似的效果。carrier-of-carriers VPN 都具備下列特性：

- 每一位 interprovider 或 carrier-of-carriers VPN 的客戶必須能夠辨別內部與外部用戶路由的不同。
- 內部用戶路由必須存放在 VPN 服務供應商的 PE 路由器中。
- 只有客戶的路由器，而非 VPN 服務供應商的路由器，才能提供外部用戶路由。

一般而言，VPN 階層中之每一服務供應商都需要在其路由器中建立自己的內部路由，並在 PE 路由器建立其客戶的內部路由。

MPLS 整合 Layer 3 Protocol 的彈性與 Layer 2 Protocol 的 Switching 速度，以提昇整個網路的效能。MPLS 結合了 IP 與 ATM 的優點，可提供更高頻寬及更好的網路品質，即使其仍在制定中，但其趨勢，將成為下一代網路主流，卻是擺在眼前的事實。IETF 目前正在開發 GMPLS(Generalized MPLS)的擴充技術。具體地來說，就是將路由的經路資訊以光信號的波長（λ）來表示，其的後續發展，值得留意。

肆、 實習心得與結論

此次美國之行與目前網際網路及HiNet主要使用的設備供應商-Cisco及Juniper其行銷團隊與R&D團隊會晤並針對下一代網際網路新技術詳加討論。初步可以發現的是在硬體及軟體方面設備供應商目前已能充分支援，哪怕是10G或是40G的產品。但是，我們卻也必需重新思考有充分的"武器"時，我們HiNet面對下一代網際網路的寬頻需求時是否能充分提供服務以滿足使用者？面臨競爭時是否具備多元化的環境因應？還有已投資購買的設備未來如何提高其再利用度的問題？在瞬息變化的網際網路服務市場與競爭激烈的電信環境，唯有能利用最新的技術與開發出新各項新的服務項目才能維持目前中華電信在網際網路的領先地位。因此，隨時準備吸收最新的知識，時時關切新技術的發展情況，或者加入未來可能發生的新技術之研究與測試，適時地引入包裝成為強大的行銷產品，將可讓公司營運成本降低並獲得更高的利潤同時亦使中華電信永遠保持在領先地位。