行政院所屬各機關因公出國人員出國報告書

（出國類別：實習）

赴美國實習

【Terabit Switch Router（TSR）網路技術與應用】

出國報告書

服務機關：中華電信股份有限公司
出國人：職稱：助理工程師
姓名：邱文華

出國地點：美國
出國期間：自 92 年 10 月 27 日至 11 月 09 日
報告日期：93 年 02 月 04 日

系統識別號:C09204127

公 務 出 國 報 告 提 要

頁數: 53　含附件: 否

報告名稱:

實習「Terabit Switch Router(TSR)網路技術與運用」

主辦機關:

中華電信股份有限公司

聯絡人／電話:

柯志勇／2344-4094

出國人員:

邱文華　中華電信股份有限公司　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 10 月 27 日 -民國 92 年 11 月 09 日

報告日期: 民國 92 年 02 月 04 日

分類號/目: G0／綜合（各類工程）　／

關鍵詞:　SLA,QOS

內容摘要: 奉派赴美國 Cisco System 公司實習「TSR (Terabit Switch Router)網路技術與應用」，含行程前後共十四天。實習目的在了解高速路由器 TSR 在寬頻核心網路之發展技術與應用，以及 Cisco System 公司路由器之最新產品及其使用之相關技術。 IP 網路是利用路由器彼此相互連接而成的網路，實施應用上，網際網路就是成千上萬個 IP 子網路藉由路由器互相連結的國際性網路。在 IP 網路中，路由器不僅負責對 IP 封包的轉發，還要透過對等的路由通信協定與其他路由器進行溝通，以確定 IP 網路的路由選擇結果以及當 IP 網路上有路由器增減時能自動維護相關的路由表，瞭解相互之間彼此的位址。隨著網際網路規模的快速延伸，路由器已成爲相當重要的網路設備之一，不僅路由器連接時所需使用的路由通信協定非常重要，其對於 IP 網路的安定性及頻寬的需求亦成爲網際網路的關鍵技術。本實習報告首先針對 IP 網路路由器產品，作一簡單概要之描述，接著報告其在實際應用上的狀況，特別是管理方面之引用，包括 SLA、QOS、先進的路由協定安全性等，尤其是 Cisco System 公司所研發使用之 QoS Policy Manager。能確實掌握 IP 網路的通信品質，提供更有保障的服務水準，達成不同客戶不同需求的滿意程度。 IP 的技術隨著市場的需求快速發展，不僅功能增加，容量的提供，網路的管理，品質的保證，也成爲電信業者投資的考慮因素。感謝 Cisco

System 思科系統公司提供新技術及應用的相關資訊。不僅網際網路上的應用，未來可朝 IP 化交換機及 IP 化用戶專用機方面發展。帶給使用者更新更優質的通信環境。本出國報告僅就個人淺見提出說明，尚祈先進前輩不吝指正。以下就管理及品質方面提供兩點建議作爲參考：一、IP 網路的環境，銜接客戶端所需設備關係通信路徑之整體品質，宜有相關規格加以規範，避免造成彼此之間 interworking 的障礙與困擾，影響通信品質，甚至於對本公司造成負面的效果。二、SLA (Service Level Agreement)機制的建立配合網路管理的功能，更有彈性，確實依不同客戶的需求提供不同等級的服務，以創造更高的營收，再搭配 QoS (Quality of Service)、CoS(Class of Service)、ToS(Type of Service)等考核方式，確保點對點的通信品質。

目　　錄

壹、摘要

職奉派赴美國 Cisco System 公司實習「TSR (Terabit Switch Router)網路技術與應用」，含行程前後共十四天。實習目的在了解高速路由器 TSR 在寬頻核心網路之發展技術與應用，以及 Cisco System 公司路由器之最新產品及其使用之相關技術。

IP 網路是利用路由器彼此相互連接而成的網路，實施應用上，網際網路就是成千上萬個 IP 子網路藉由路由器互相連結的國際性網路。在 IP 網路中，路由器不僅負責對 IP 封包的轉發，還要透過對等的路由通信協定與其他路由器進行溝通，以確定 IP 網路的路由選擇結果以及當 IP 網路上有路由器增減時能自動維護相關的路由表，瞭解相互之間彼此的位址。隨著網際網路規模的快速延伸，路由器已成為相當重要的網路設備之一，不僅路由器連接時所需使用的路由通信協定非常重要，其對於 IP 網路的安定性及頻寬的需求亦成為網際網路的關鍵技術。

網路 IP 技術的演進，網際網路訊務之激增，加上客戶對頻寬的需求日益增加，新世代的電信網路正加速往 IP 化與寬頻化之標準發展，IP 寬頻核心網路將是下一代電信網路的主流。本公司營運之固網、行動及數據業務均居國內電信市場之龍頭地位，相對的競爭壓力也是最大。本公司現有之 PSTN 長途網路已 Migrate 至 PTSS Class 4 IP 寬頻交換設備，目前亦積極引進 PTSS Class 5 現場試用建設計畫，作為評估未來網路 IP 化之基礎，實有必要吸取 IP 寬頻網路最新相關技術及應用，祈能提昇網路服務品質，滿足消費者需求，鞏固電信市場競爭優勢。

本實習報告首先針對 IP 網路路由器產品，作一簡單概要之描述，接著報告其在實際應用上的狀況，特別是管理方面之引用，包括 SLA、QOS、先進的路由協定安全性等，尤其是 Cisco System 公司所研發使用之 QoS Policy Manager。能確實掌握 IP 網路的通信品質，提供更有保障的服務水準，達成不同客戶不同需求的滿意程度。

貳、行程及實習內容紀要

本案之行程及實習內容如下所述：

十月二十七日~七月二十七日：去程，由台北搭機經紐約前往舊金山 Cisco System 公司訓練中心

十月二十八日~十月三十一日：實習：

- Cisco Terabit Switch Router (TSR) product update
- Demo & Tour of Cisco System Company
- IP Network Requirements

十一月一日~十一月二日：由舊金山搭機前往紐約假日整理資料

十一月三日~十一月七日：實習：

- IP-based Broadband Content Practice
- IP Network Operation & Maintenance

十一月八日~十一月九日：返程，由紐約搭機返回台北

參、實習報告

一、思科公司新一代路由器（趨勢）

1、全方位高等級路由器策略

& 核心路由器的兩種處理方式：

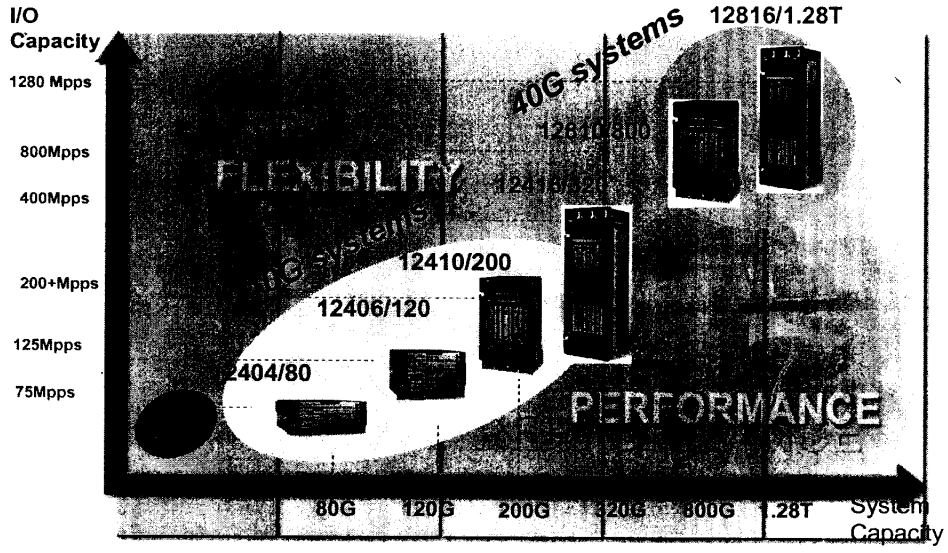
12800 系列用於保障業者之投資

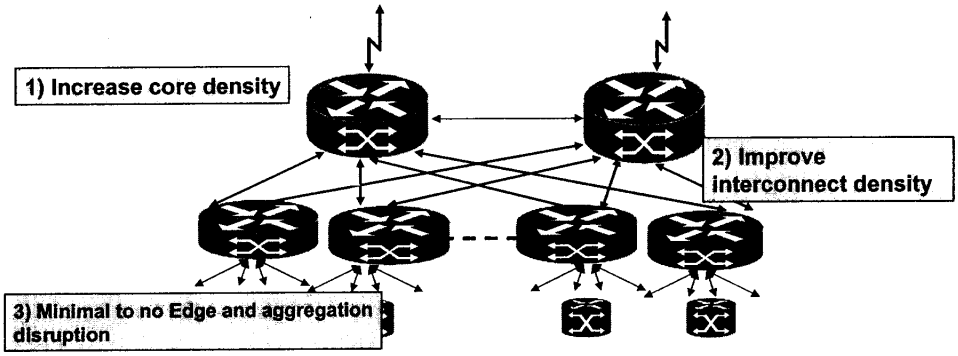
HFR 專為網路業者設計的高度可調規模之全新路由系統

& 邊緣路由器的處理方式：

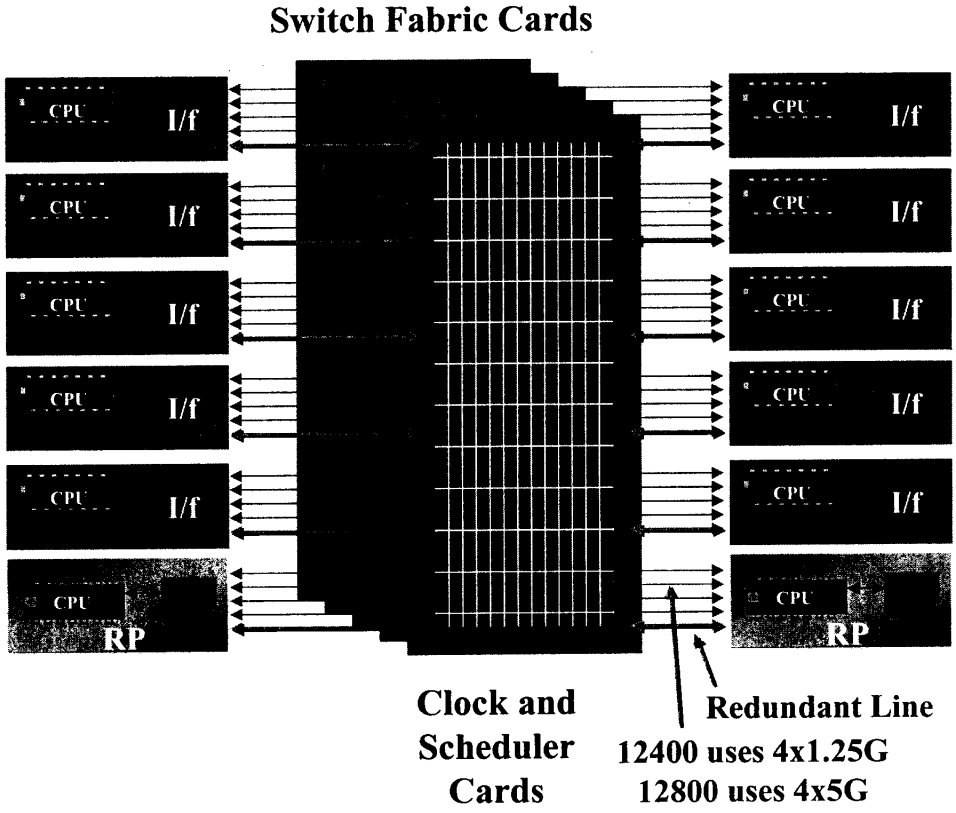
12000 系列支援 VPA 之 10G 及 2.5G 用戶卡片

IP 網路是利用路由器互連起來的網路，網際網路(Internet)就是成千上萬個 IP 子網路藉由路由器互聯的國際性網路，是以路由器為基礎的網路，形成了以路由器為節點的「網際網」。在 IP 網路中，路由器不僅負責對 IP 封包的轉發，還要藉由路由通信協定負責與別的路由器進行聯絡，共同確定 IP 網路的路由選擇和維護路由表。隨著網際網路規模的快速發展，路由器隨之成為最重要的網路設備，路由器連接所使用的路由通信協定已成為網際網路的關鍵技術。由於對
IP 數量的需求日益增加，不僅使用中的 IPv4 有不敷使用的感覺，致有 IPv6 的發展，高速大容量之路由器也漸次開發，並且商用化。





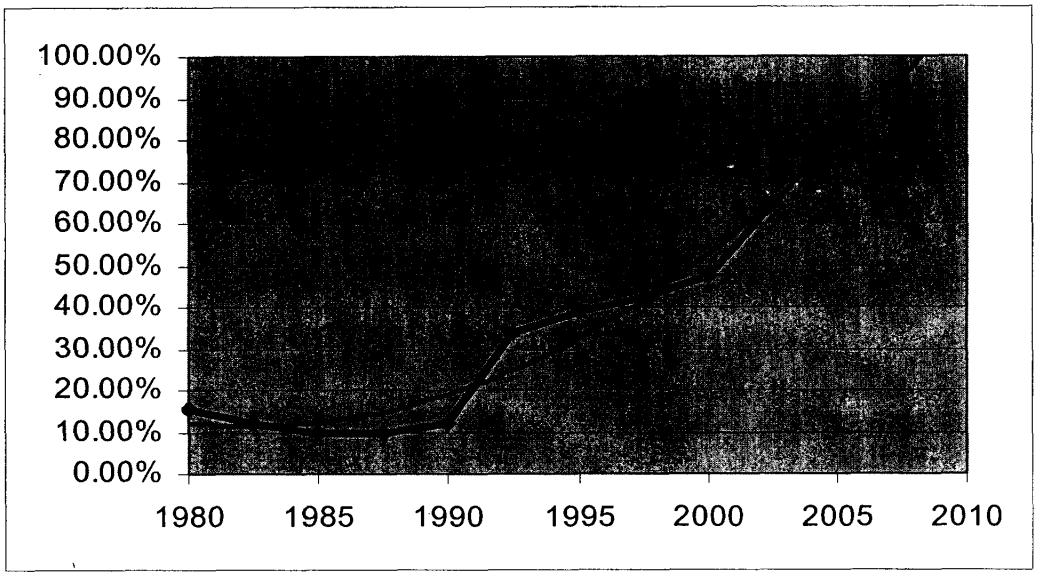
高速可規劃之 IP 架構為增加核心路由器的容量、改進相互連結的容量及朝無需邊緣路由器及因需彙集我造成的損失。以營收為考量將 POP 結構設計成可調整比例大小的架構，使得每一插槽可達 40Gbps，並且有更多空餘的插槽可供使用。利用既有的 12410/12416 機架，支援所有的用戶卡片。



二、IPv6 基本概念

1、基本概念回顧

是否真的需要較大的位址空間呢？（一）網際網路的使用者由 2002 年的五十三億到 2004 年預估的九十四億。（二）PDA、Pen-Tablet 及 Notepad 等使用者 2004 年約二千萬。（三）行動電話已有一億用戶。（四）到 2008 年預估約有一億輛運輸工具，外加在飛機上使用網際網路。（五）上億的家庭及工業使用類似的裝置。下圖可顯示 IP 位址需求的歷史。



1981 - IPv4 protocol published

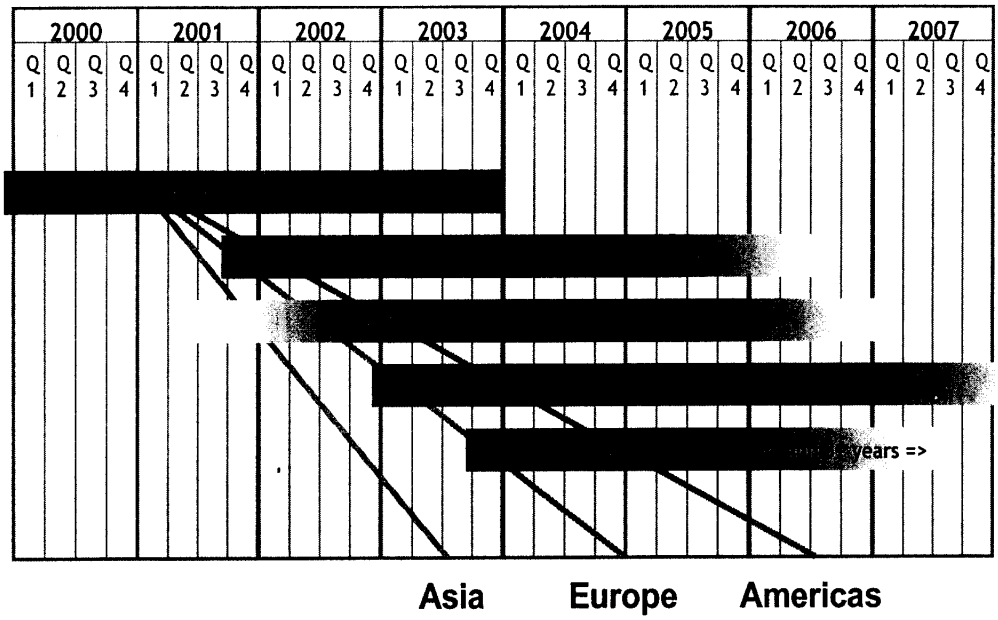
1985 ~ 1/16 of total space

1990 ~ 1/8 of total space

1995 ~ 1/3 of total space

2000 ~ 1/2 of total space

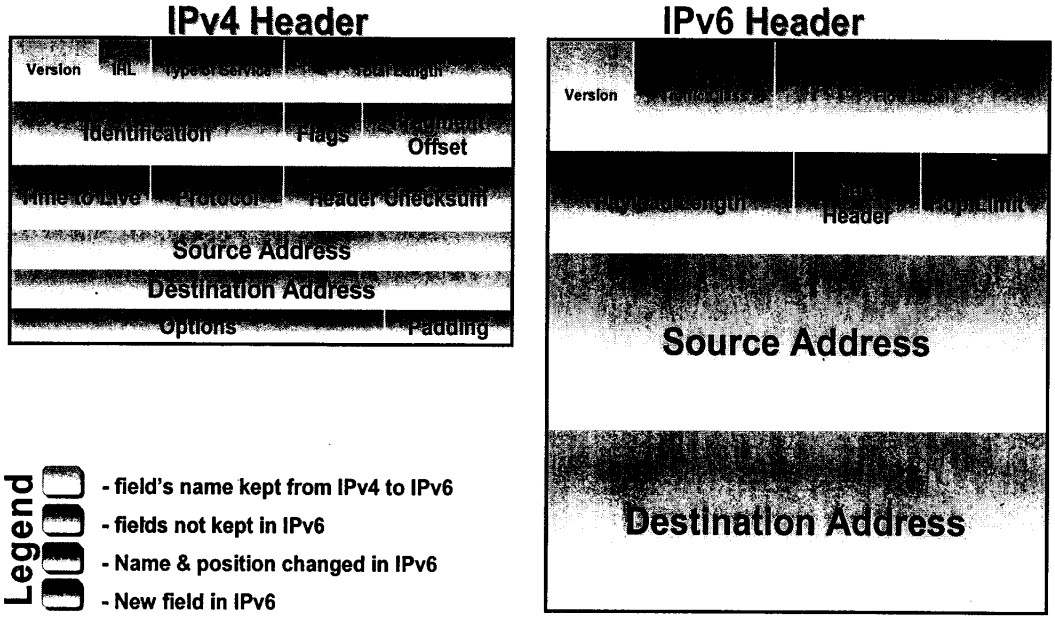
2002.5 ~ 2/3 of total space



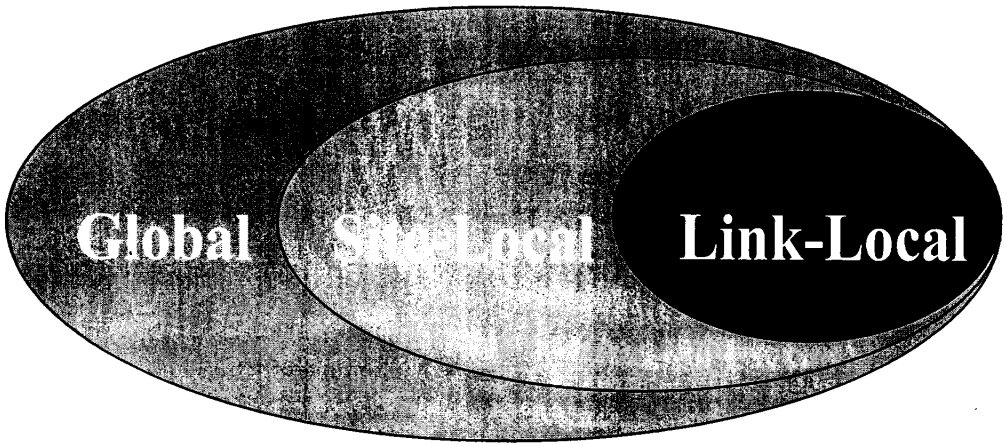
本表可顯示 IPv6 需求的時間線。

IPv4 與 IPv6 在 IP 各項服務的不同解決方法：位址範圍

IP Service	*IPv4 Solution*	*IPv6 Solution*
Addressing Range	32-bit, Network Address Translation	128-bit, Multiple Scopes
Autoconfiguration	DHCP	Serverless, Reconfiguration, DHCP
Security	IPSec	IPSec Mandated, works End-to-End
Mobility	Mobile IP	Mobile IP with Direct Routing
Quality-of-Service	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service
IP Multicast	IGMP/PIM/Multicast BGP	MLD/PIM/Multicast BGP,Scope Identifier



上圖為 IPv4 與 IPv6 Header 的比較。IPv6 位址模式為位址均被指派到介面，由 IPv4 改變而來期望每一個位址有多重介面。位址的範疇由當地鍊路到當地區域再到全球整體。如下所示：



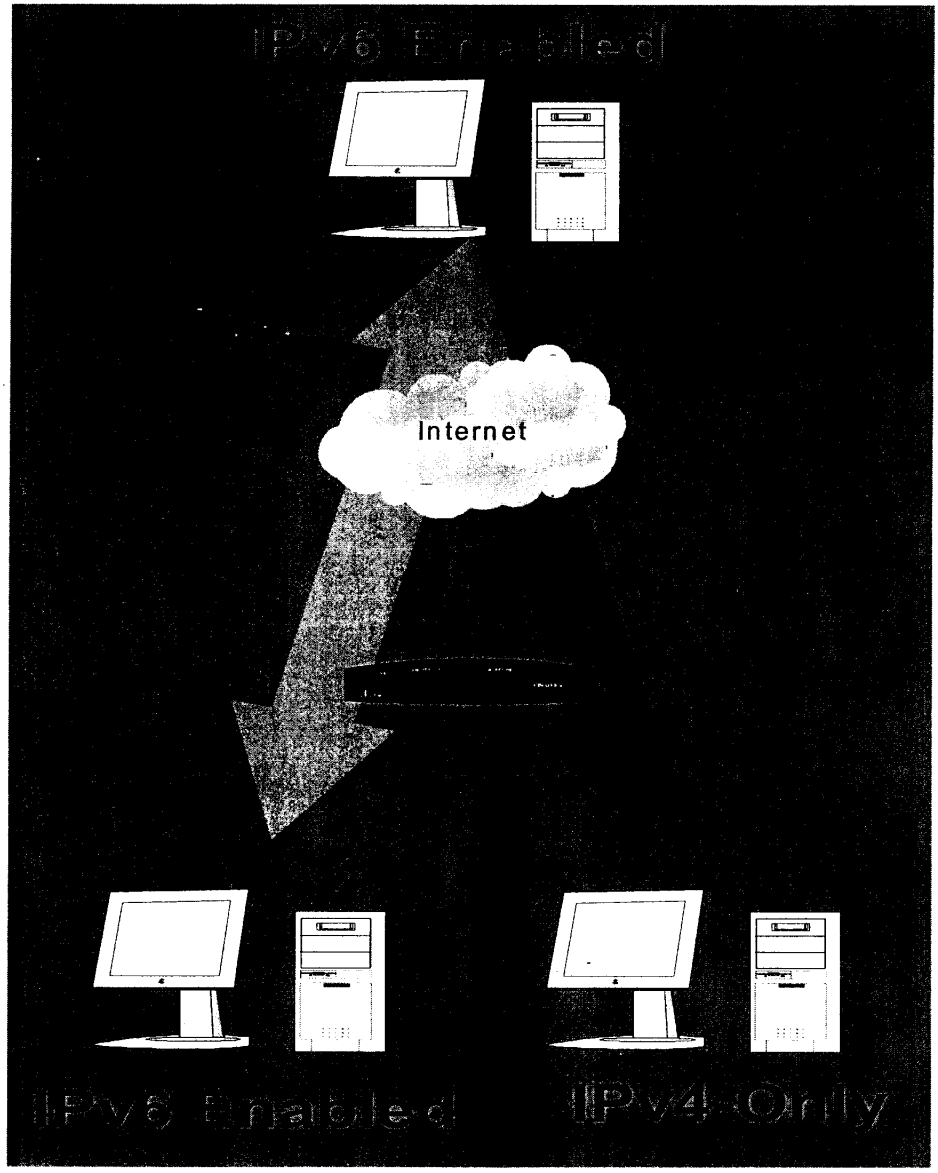
且所有的位址都有其有效性及時效性。

2. IPv4 與 IPv6 間之傳送及共存

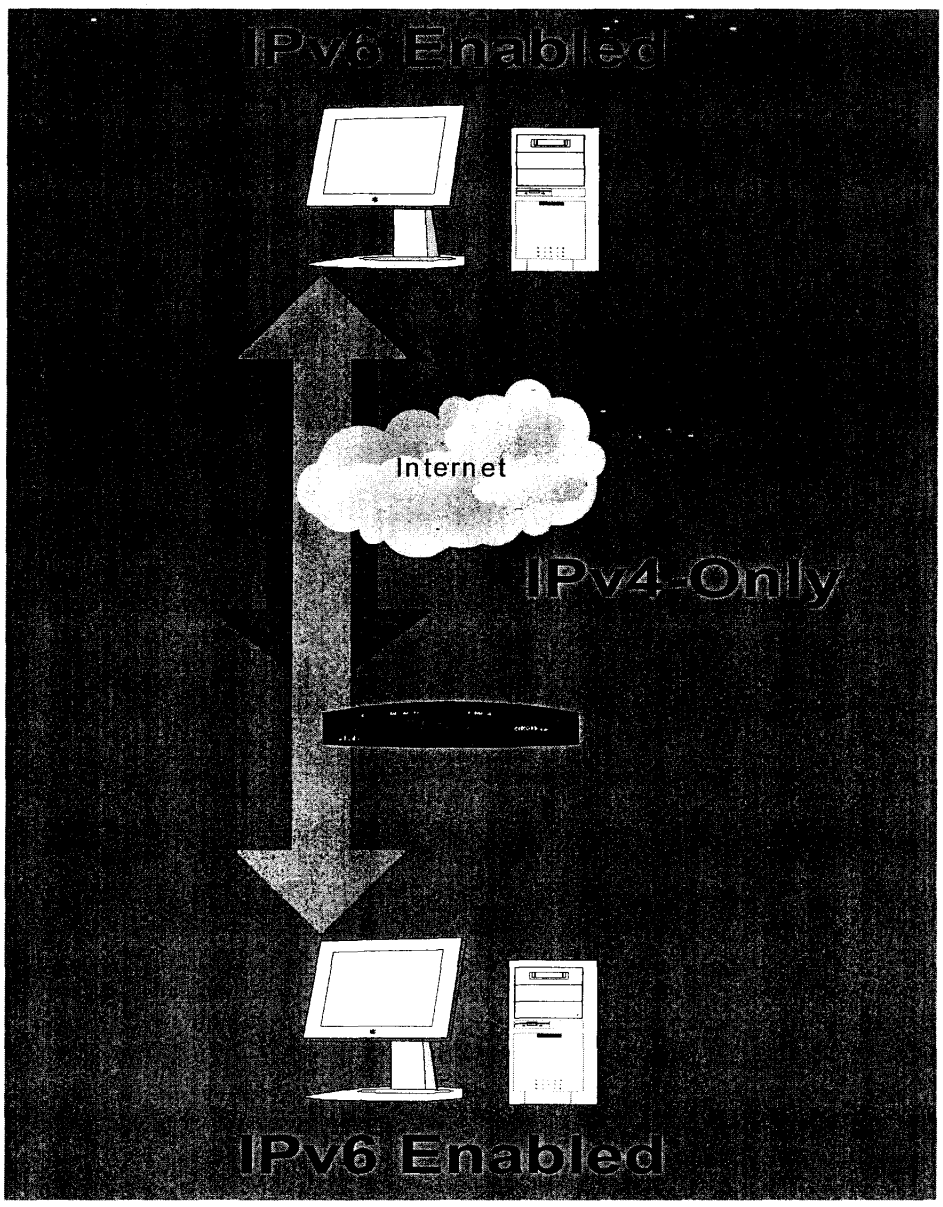
廣範得技術早已被用於識別及使用，基本上有三種不同的分類：(一) 雙重堆疊技術：允許 IPv4 與 IPv6 在同一設備及網路上共存。

(二) 隧道技術：當主機、路由器或區域昇級時避免順序的依賴性。

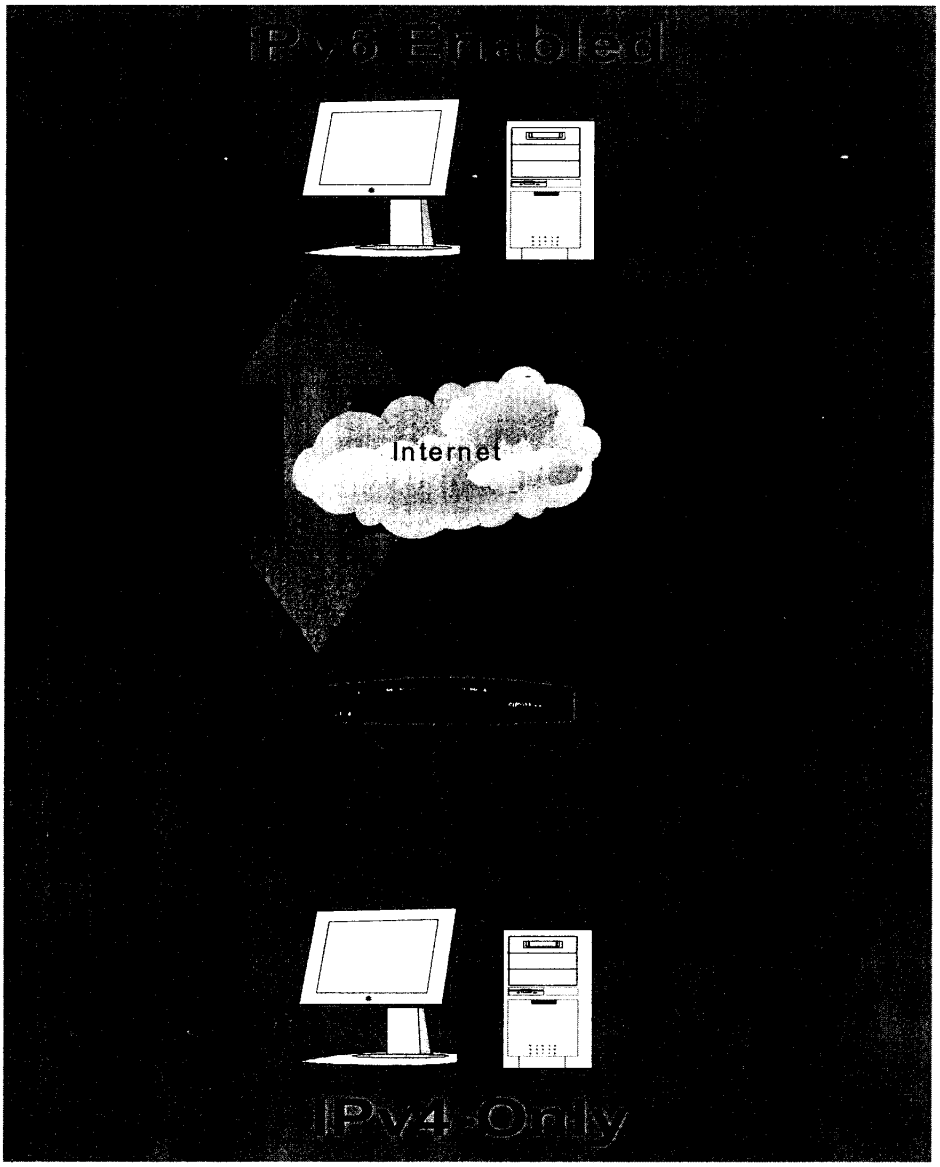
(三) 翻譯技術：允許僅具 IPv6 的設備單向的與僅具 IPv4 的設備通訊。



此乃初級的工具，允許持續的“正常的”與僅具 IPv4 的節點運作。位址的選擇規則一般趨向於 IPv6。也允許 DSTM 變化的暫時使用 IPv4 的緩衝器。惟當系統加入 IPv6 時，不可江 IPv4 刪除。



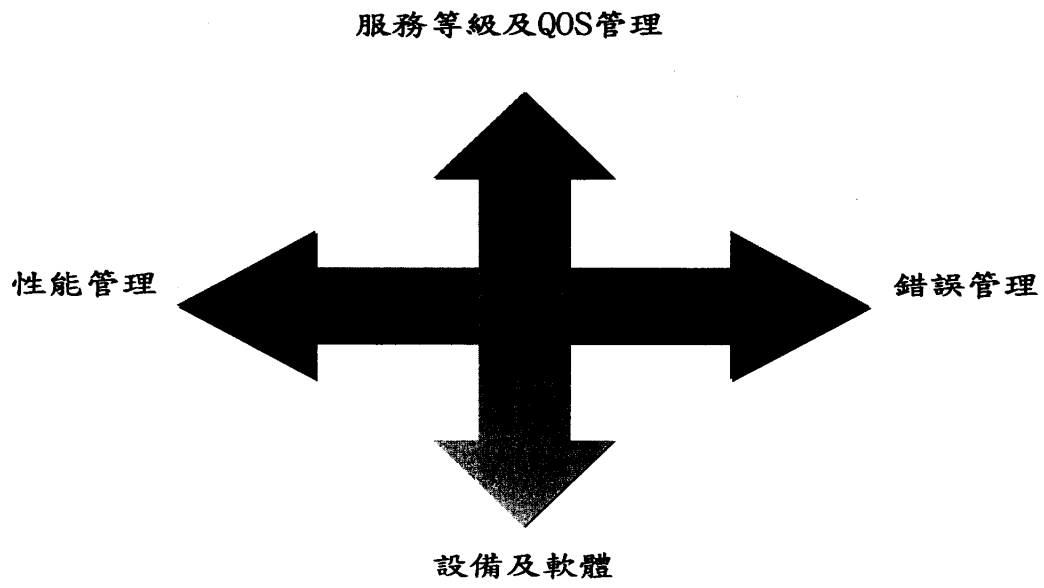
節點視 IPv4 的網路為一個邏輯上的鏈路層。有時可被用來與雙堆疊方式連接。



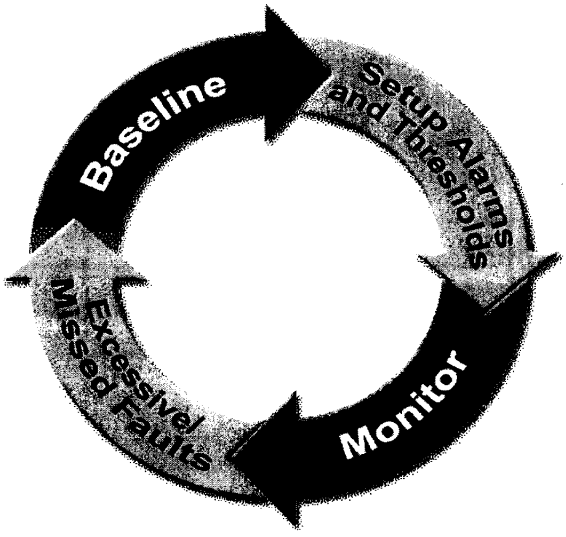
允許有些元件分別只有 IPv6 和 IPv4 的狀況。且對於規模這一項特性需特別注意。相同的情形也發生在 IPv4 對 IPv4 的翻譯上。

三、SLA 服務等級管理

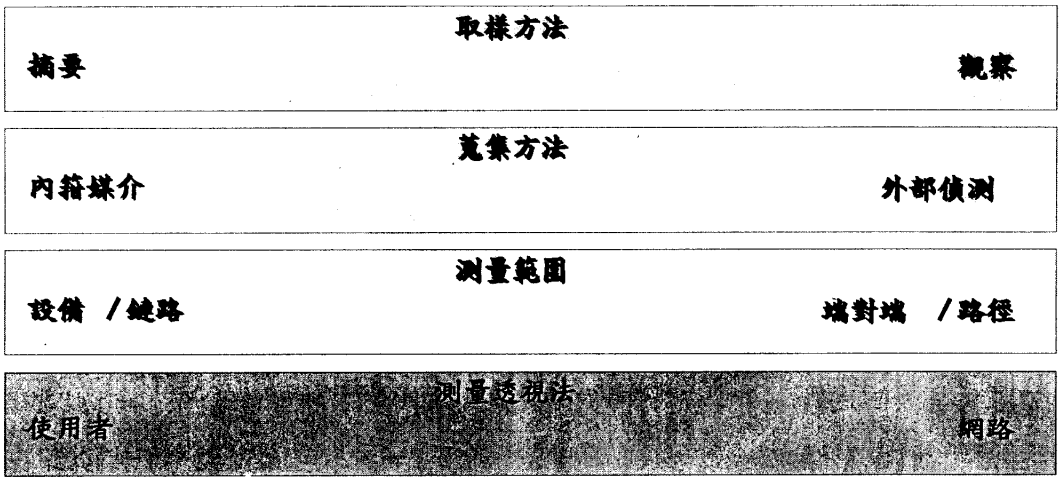
1. 管理範疇：



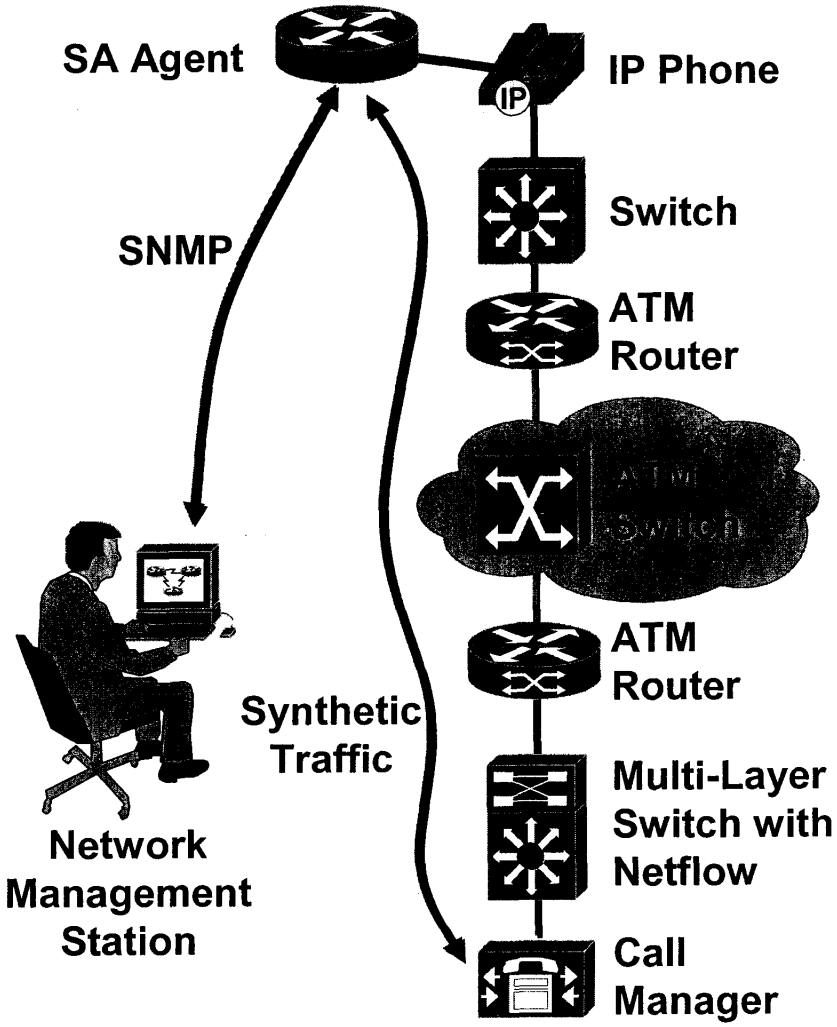
性能管理是指量測網路並允許使用者決定是否適當地提供服務給客戶。測量的適切性是跟據和客戶所簽訂的契約來決定，那就是 Service Level Agreement（SLAs）。而使管理發生效果的步驟則如下圖所示。網路的基準線、設定告警臨界值、監視、作必要的調整（被忽略的錯誤）。



2. 測量的策略分為取樣方法、蒐集方法、測量範圍及測量透視法等四種。分別詳述如下：



3. 取樣方法—摘要：

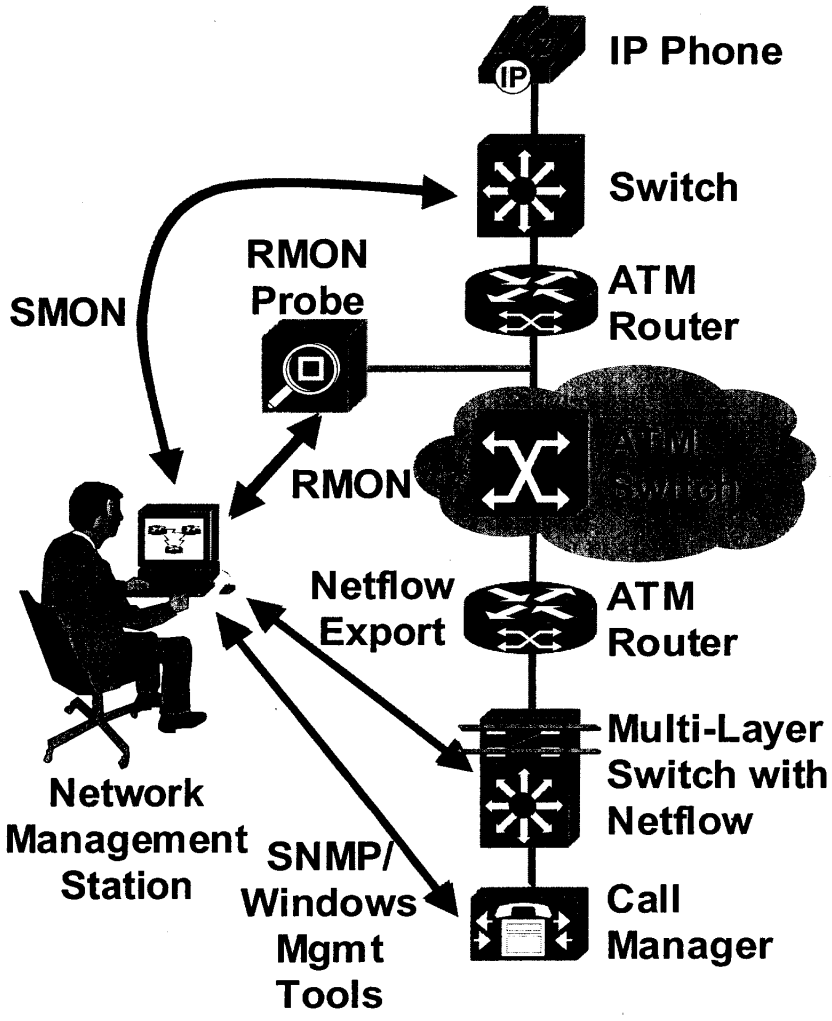


定義：網路的訊務為了量測網路性能特質的目的而精確地產生。

優點：位於網路上的任何兩點間且在連續的基礎上藉由訊務的分類建立在 IP 先後的標籤上並可控制地量測其性能。

缺點：只能約略地得到存活著的性能。

4. 取樣方法—觀察：

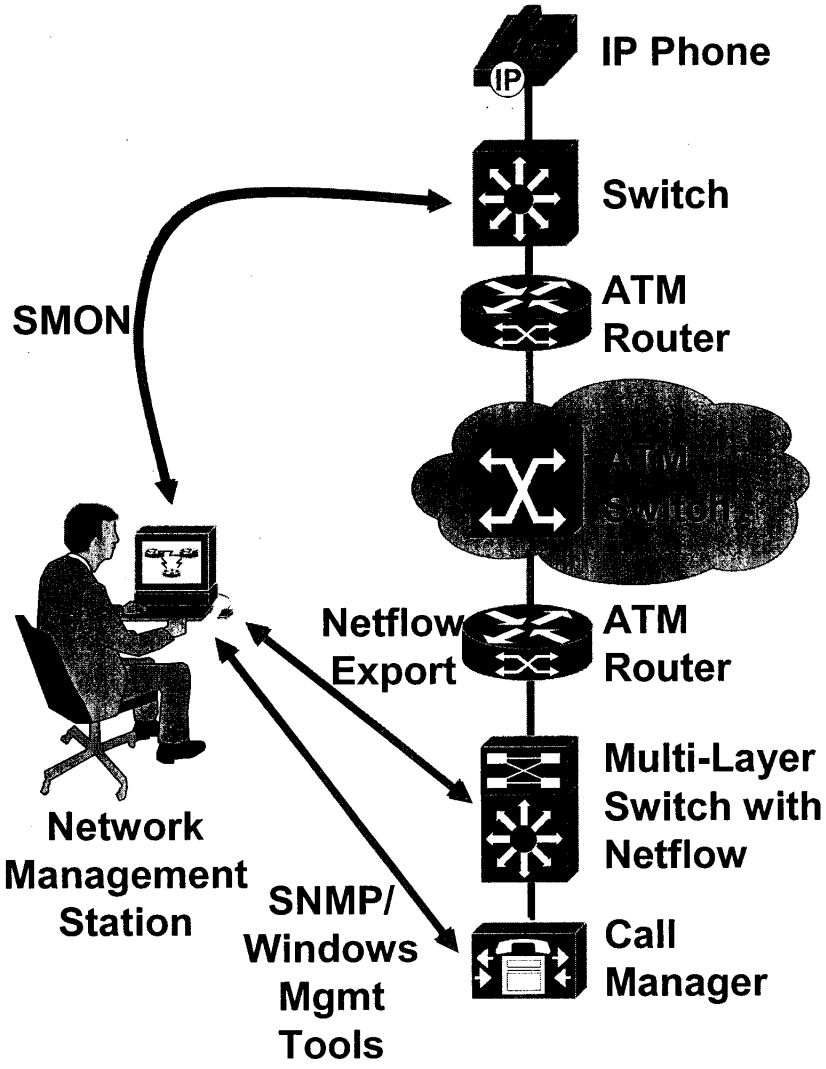


定義：真正端點使用者之網路訊務，藉由特定時間應用的訊務流量以量測其性能。

優點：在指定的鏈路上經確地得到存活著的應用訊務。

缺點：測量上的限制。既成的訊務型態有可能不會全部呈現在網路上。且既成的訊務模式也有可能不會反映在新的或未來的應用上。

5. 蒐集方法—內箝媒介：

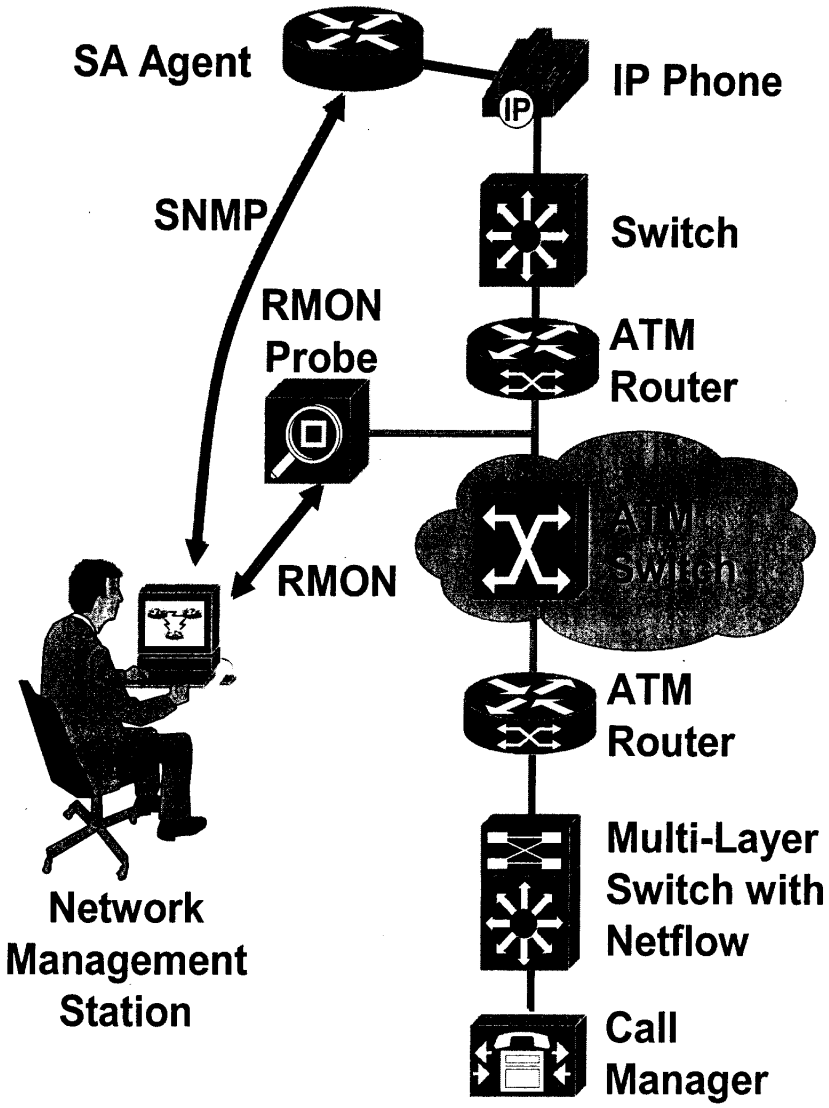


定義：蒐集網路統計資料的機制大都整合在網路通信設備（路由器、交換器）本身。

優點：按照網路架構聚集那些無法在外部觀察到的矩陣資料。

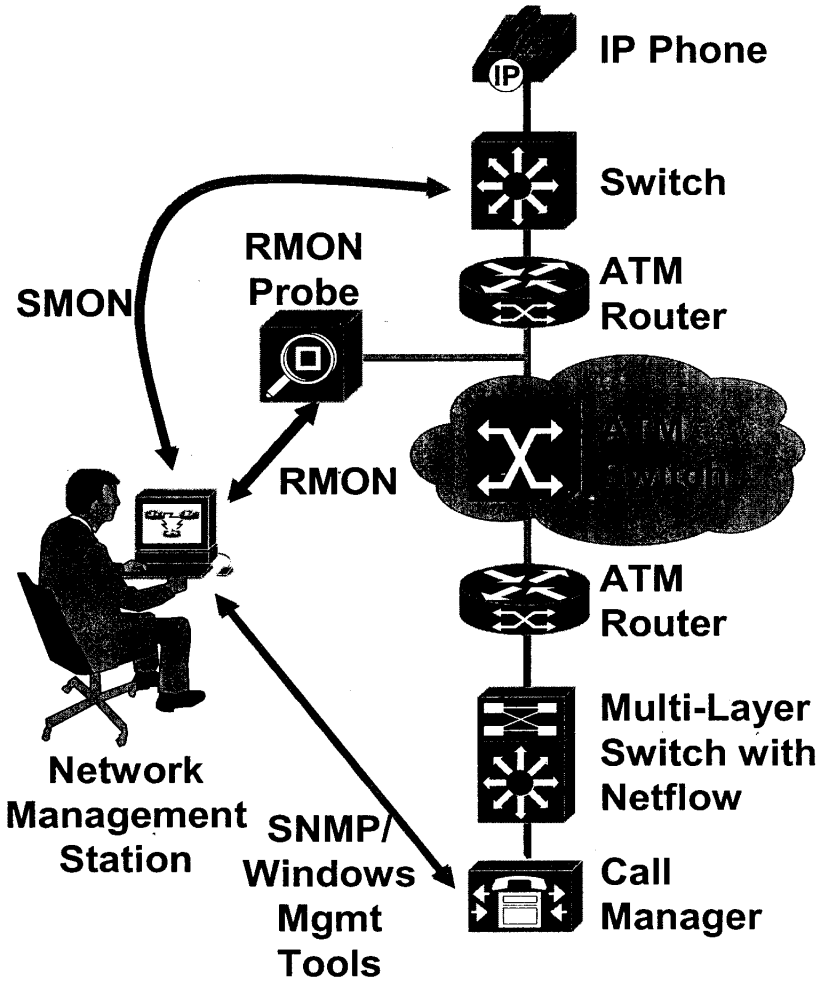
缺點：性能監視牽涉設備的性能等級。

6. 蒐集方法—外部偵測：



定義：由獨立的設備提供特別統計，用以蒐集性能統計資料。
優點：性能的有效性由獨立的設備執行，並且傳送網路的訊務。
缺點：有較多數的硬體設備需要管理，觀察統計囿於應用點數量的限制。

7. 測量範圍—設備鏈路：

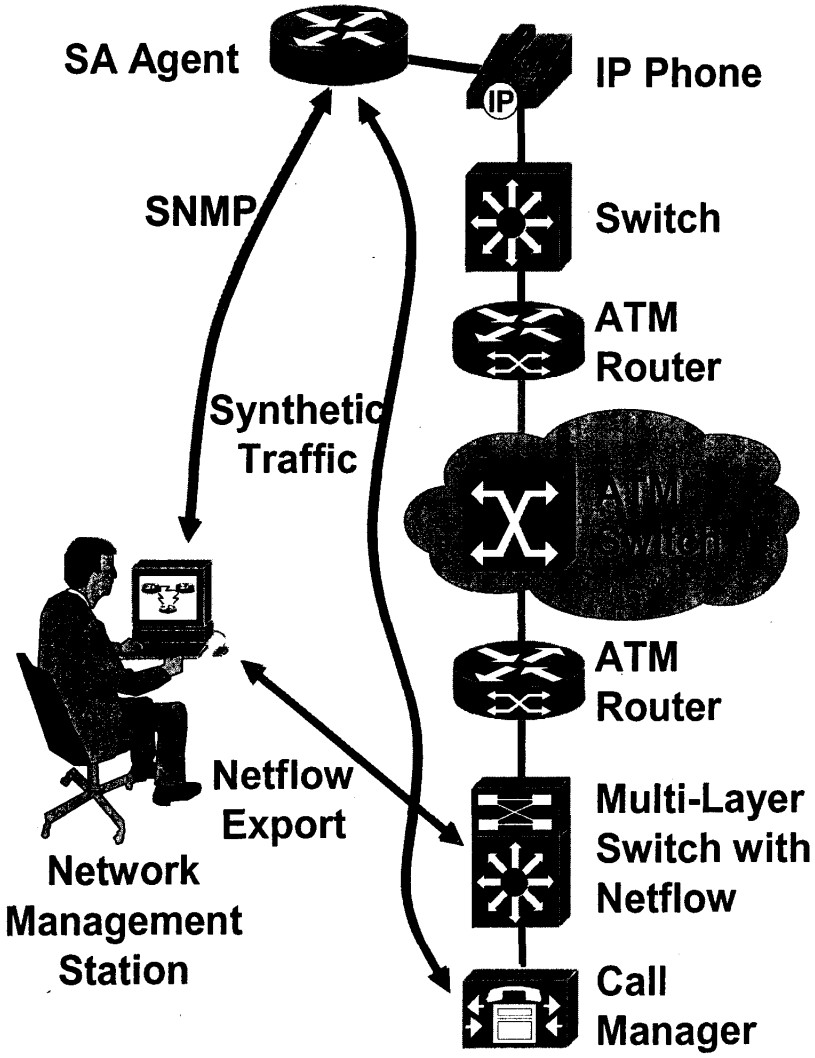


定義：性能測量乃基於特定設備的分析或設備介面，以及典型的以利用率為基礎。

優點：針對網路鏈路的臨界點做詳細的應用性能監視。

缺點：當全域（整個）網路性能問題存在時，如何選擇設備或練鏈路來評估。

8. 測量範圍—端對端：

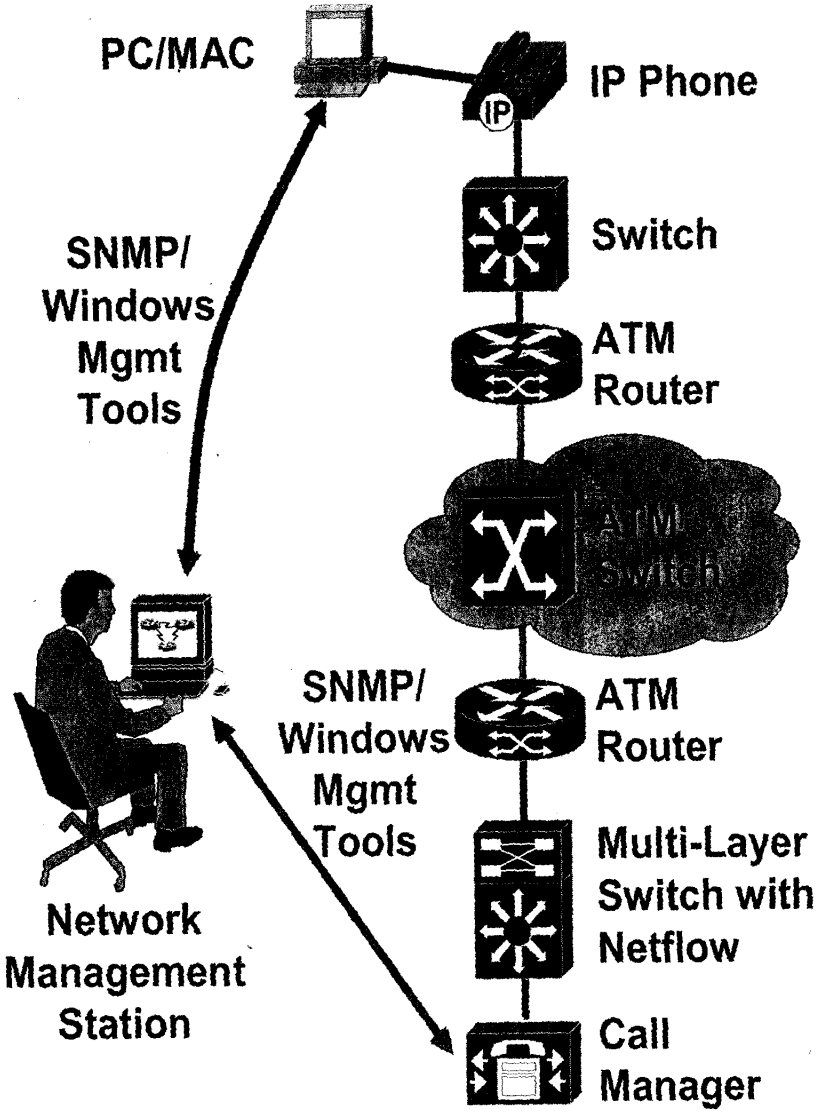


定義：性能量測乃基於兩個或兩個以上更多網路接取反應時間的分析以及點型的基於延遲。

優點：【1】啟始點性能維修【2】能反應端點使用者的性能。

缺點：必需具備相關於端對端路徑的先導知識。

9. 測量透視法—使用者：

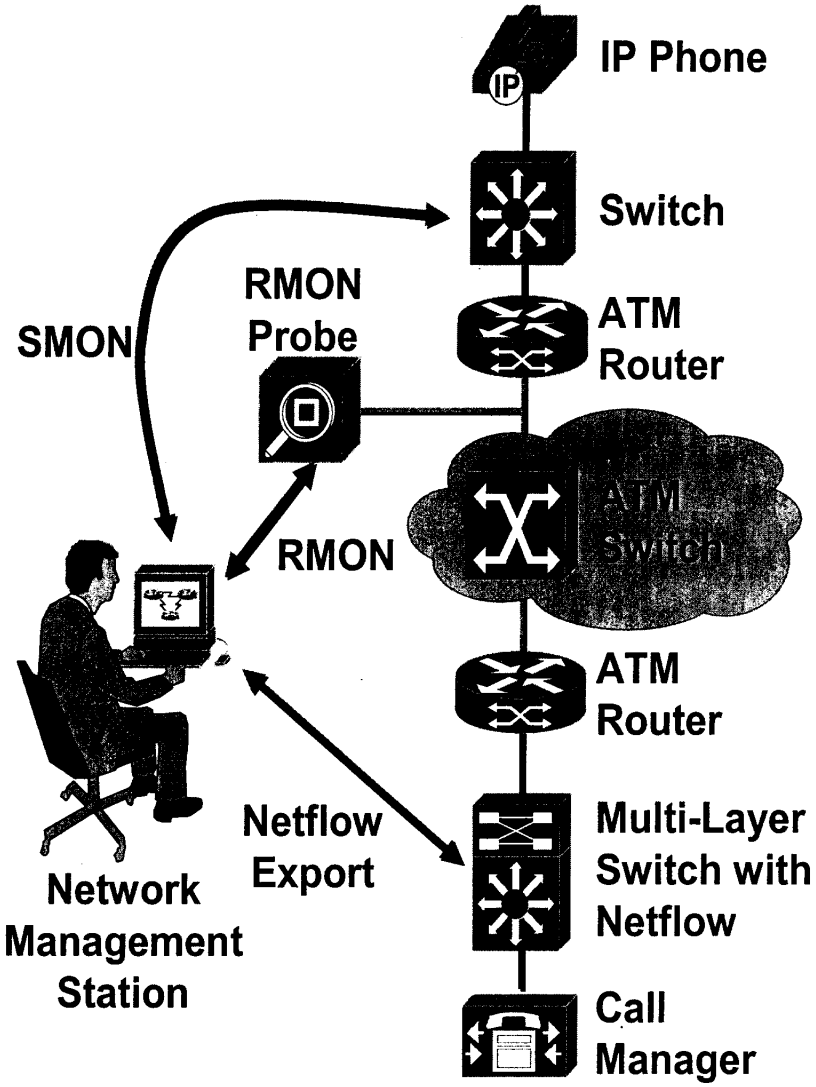


定義：量測乃基於在端點使用者工作者站性能統計的測量。

優點：精確地量測端點使用者的經驗。

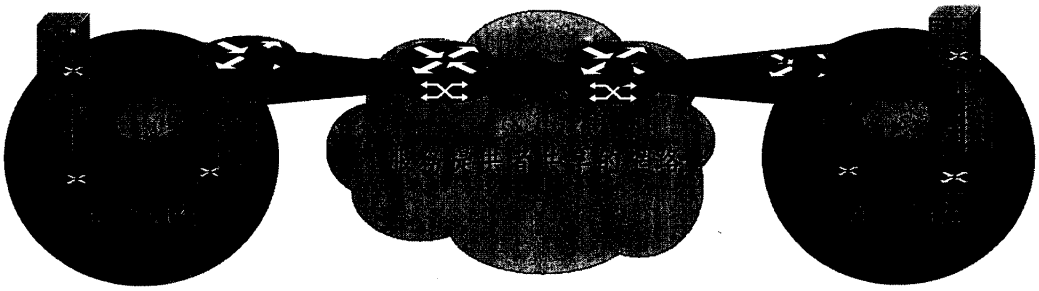
缺點：刻度及分配議題不會干預到桌上型電腦設備。

10. 測量透視法—網路：



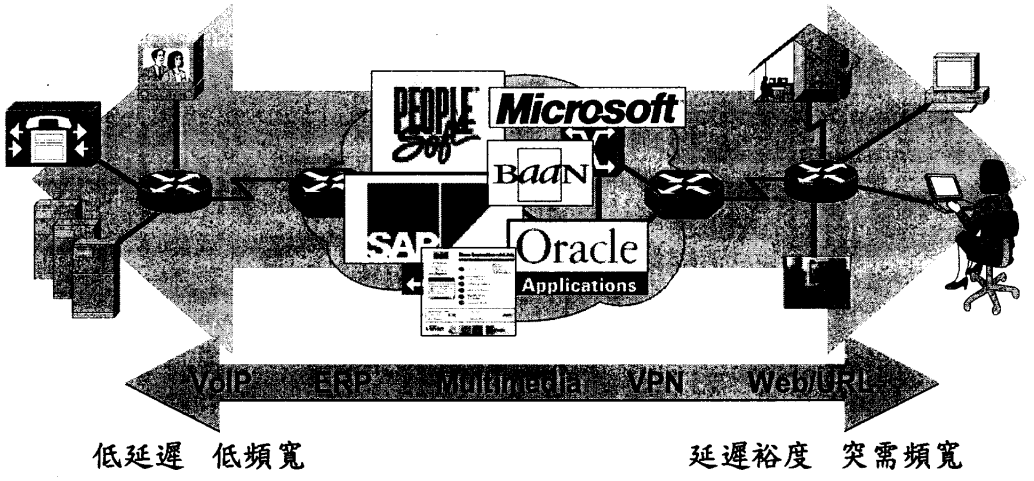
定義：量測乃基於網路設備內部性能統計的測量。
優點：易於應用不會干預到桌上型電腦設備。
缺點：對於端點使用者經驗的瞭解並非十分完美。

11. 服務等級管理：Service Level Agreements（SLAs）服務等級契約逐漸成為服務遞送的整合部份。



如上圖所示：商業客戶均賴以作為任務臨界應用及程序之處理。SLA 是業者提供不同服務的角石。那麼，何謂 SLA 呢？SLA（Service Level Agreement）是客戶與服務提供者之間的契約（Contract）中將服務品質（Quality of Service）予以正式化的記載。那麼，什麼又是 SLC 呢？SLC（Service Level Contract）詳細記載服務提供者與端點客戶間契約的連續性及效能。SLC 包含多個 SLA，且違反任何一個 SLA，就是違反 SLC。由此觀之，SLA 應該是容易理解、標準化、容易量測及產出報告表及對服務提供者而言是有價格上的差異。對同一群組的使用者，有著相同的 SLA，並非為每一位使用者量身訂作。

在多重服務網路裡的服務等級管理：每一種應用均有它自己的性能限制，網路必需與這些限制吻合。

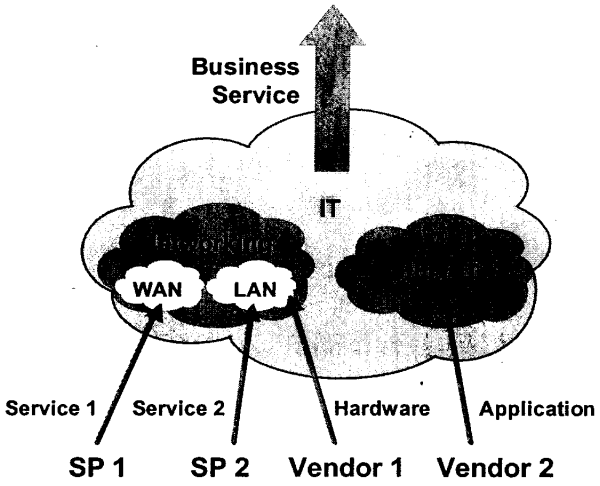


12. 服務等級管理受到訊務管理以及端對端限制的挑戰。

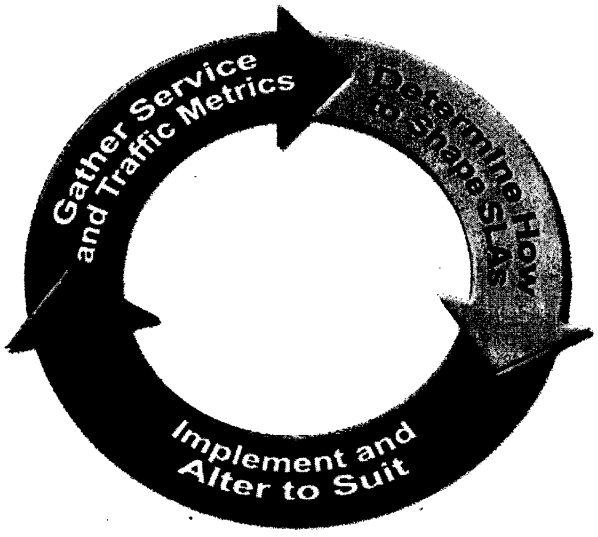
Traffic Management

Plus

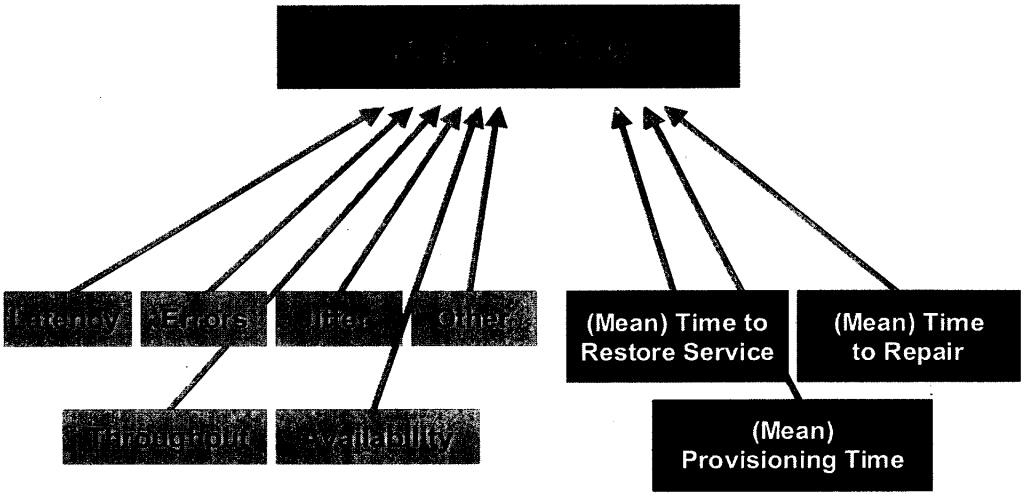
End-to-End abstraction



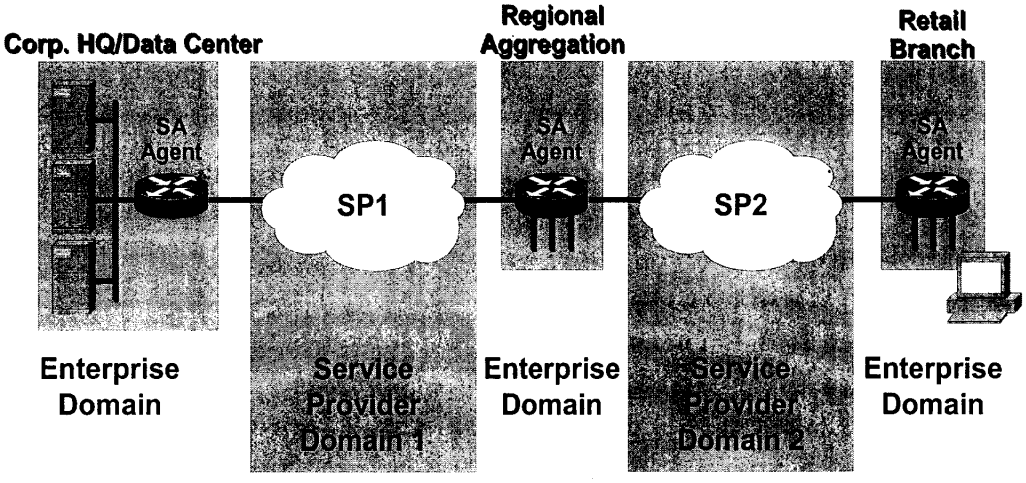
量測：現在訊務及服務矩陣。
定義：不同的策略及多種服務、不同的界限、服務元件。
運用：相交的界線、組織、技術。



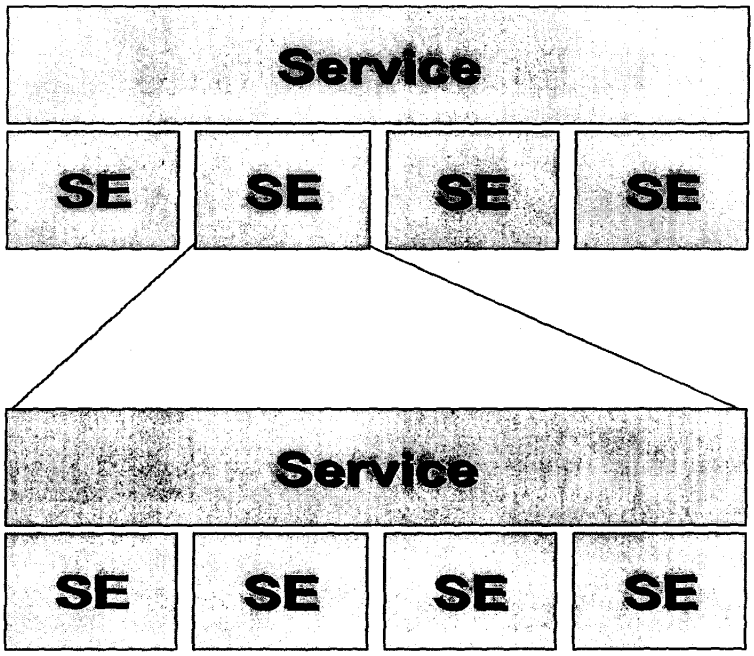
13. 定義不同的策略及服務



14. 固有的服務包括延遲、錯誤、不穩定、產出及可用性。選擇性服務則包括恢復服務的平均時間、平均修護時間及平均調度時間。這些均和服務品質的等級有關。



15. 網路硬體、工作站硬體、應用軟體等等。均為實體上不同的界線。



網路、路徑、鏈路、防火牆、應用程式、伺服器均是 QoS 的服務元件。至於實際運用上 SLA 所稱的元件則有可用性、封包遺失、網路延遲、網路不穩定性等等。分別敘述如下：

16. 可用性（Availability）：

可用性是一個矩陣，用於決定工作及當機的時間。可以用數學式表示

Availability=(Uptime)/(Total Time)

A=(MTBF)/(MTBF+MTTR)

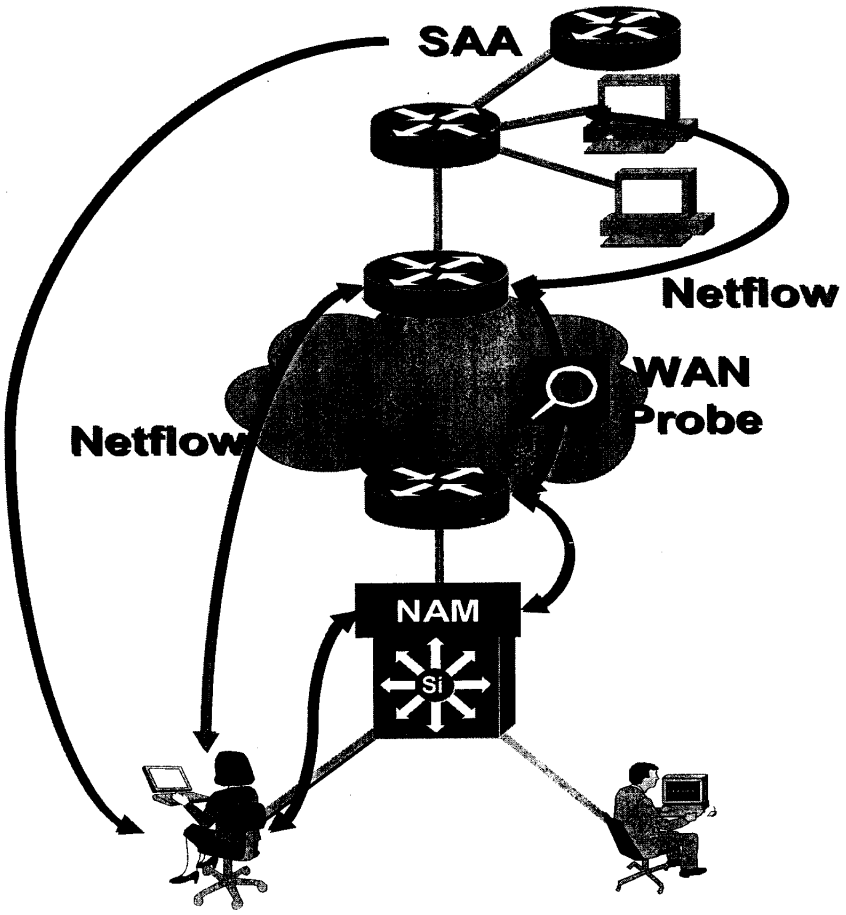
MTBF：Mean Time Before Failure

MTTR：Mean Time To Restore

有些時候，從使用者的觀點來看，路由器是可用的，但是訊務偵測器卻不可用。

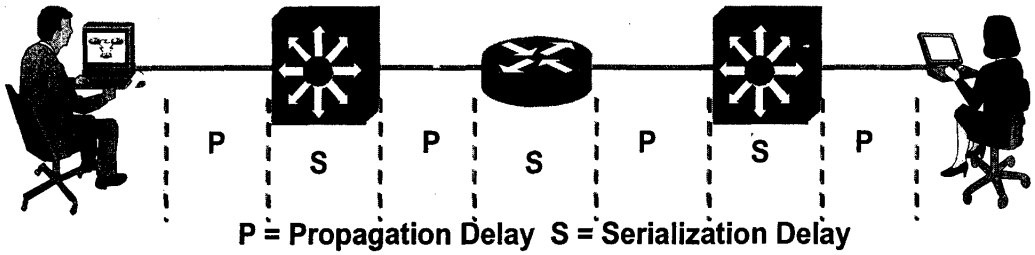
量測的方法有 ICMP ping、Echo Protocol、Application Probe

17. 封包遺失（Packet Loss）：



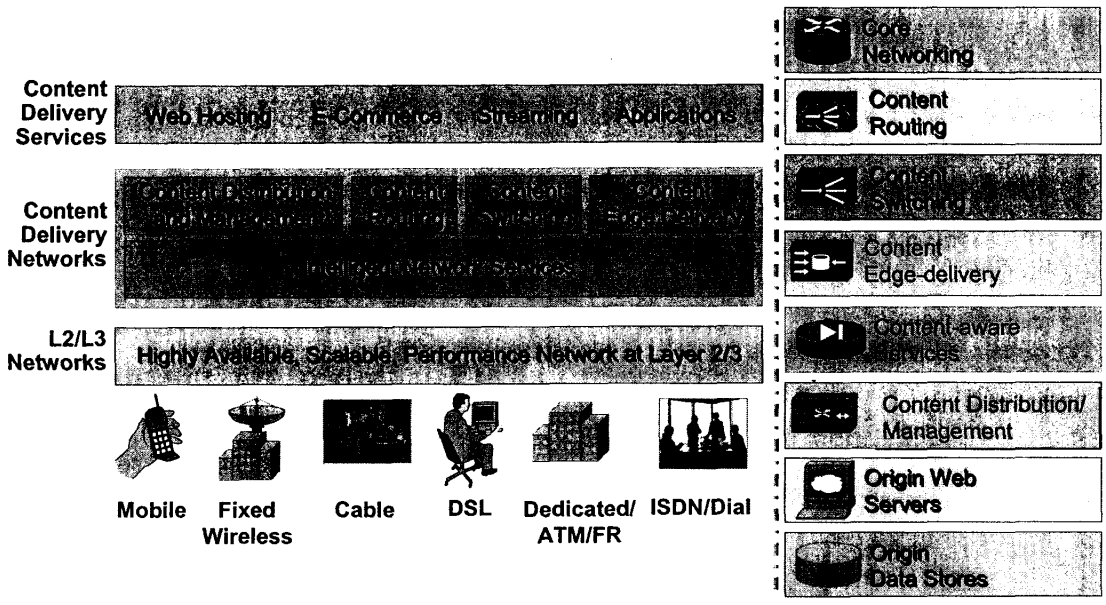
封包的計算在於來源路由器的出端介面及目的地端設備的入端介面。比較困難的工作在於必需蒐集大量的資料及經過廣域網路鏈路的更正資料。量測的方法是利用 SA 媒介（SA Agent）；它包括一個控制協定。在那裡傳送器（sender）和反應器（responder）取得一致，並計算有多少封包將會被傳送。

18. 網路延遲（Network Delay）：



網路延遲是計算封包從一個端點到另一個端點旅行所需花費的時間。
Network Delay = Propagation Delay + Serialization Delay
傳播延遲（Propagation Delay）是指一個電子脈衝從一個端點到另一個端點經過物理媒體所需花費的總時間。連續延遲（Serialization Delay）是指跳躍經過網路中間設備所造成；包括在中間設備內部的排列、處理、交換時間。
量測的方法有【1】網路時令協定 Network Time Protocol【2】ICMP ping 的來回時間 ICMP ping with round-trip time【3】Cisco ping MIB【4】SAA（Service Assurance Agent）及其應用 SAA and Applications (IPM)。

19. 實例：內容傳遞網路的服務元件

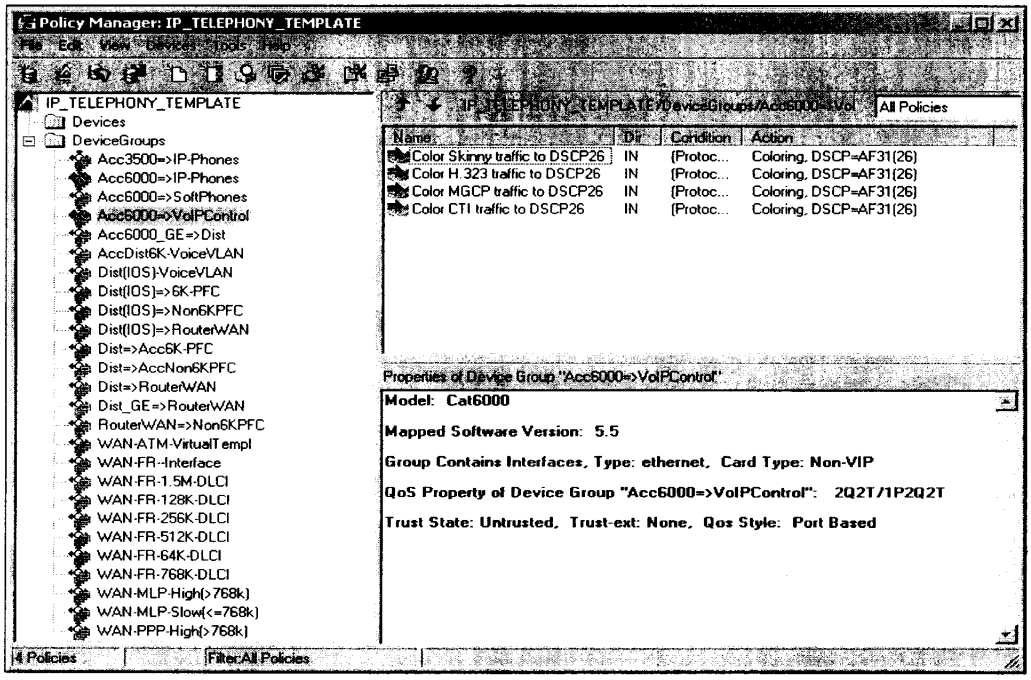


四、QOS 服務品質管理

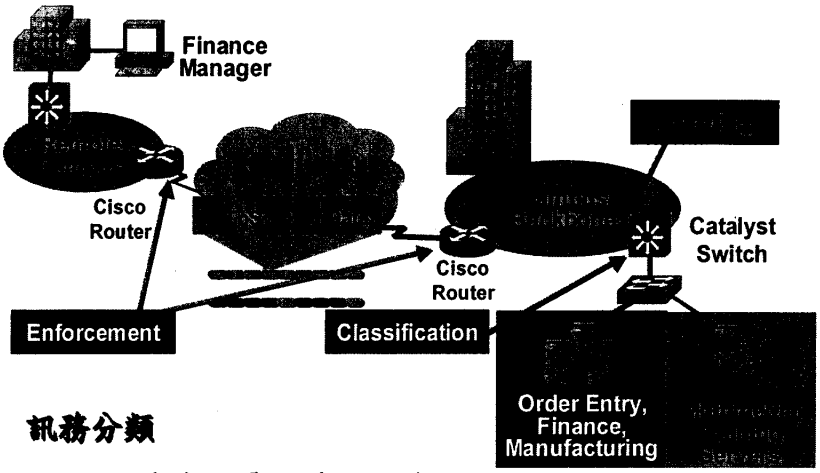
> The problem we are trying to solve is to give "better" service to some at the expense of giving worse service to to others — QoS fantasies to the contrary, it's a zero sum game
>
> - Van Jacobson

換言之 QOS 管理是管理不正當的部份。思科系統公司提供一種策略的管理，稱為 Policy Management。它是一種集中式多設備的管理，共同使用〝角色（roles）〞或設備群的觀念，將指定的策略適用於多個設備上。規則是以策略指導為基礎，自動化地將高等級策略定義轉換為特定設備所用的語法，以簡化網路的應用。QPM（QOS Policy Management）併入思科系統公司的測試結果，建議對於 IP 電話網路採用預先定義的樣板，這些樣板是可以為使用者量身訂做的。

Cisco QoS Policy Manager



1. 策略為基礎的端對端 QOS，乃是透過訊務的分類，提供前後一貫的差別服務，以強化 QOS 的機制。

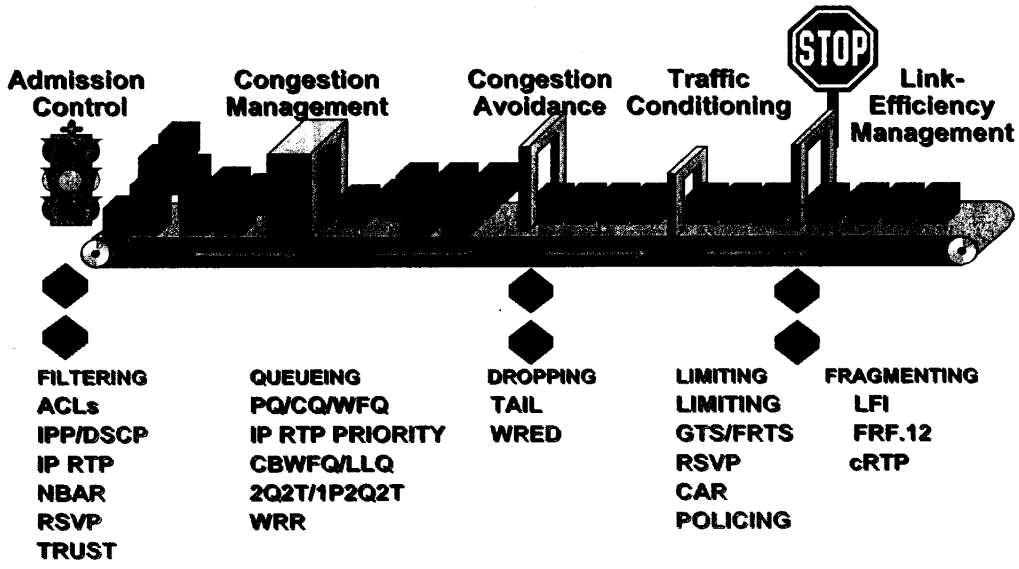


訊務分類

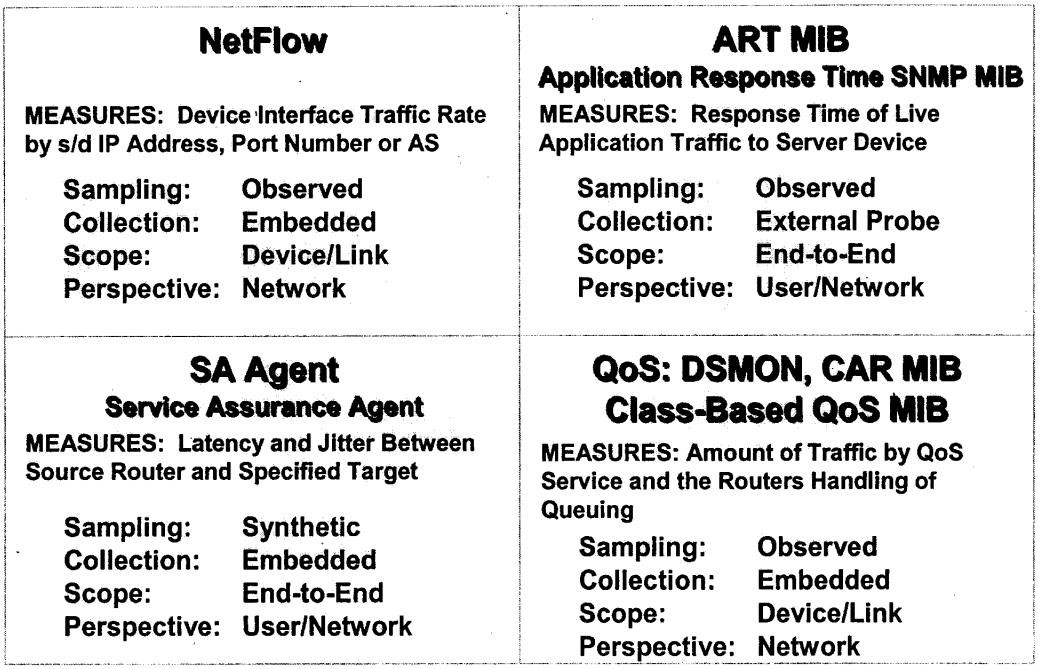
前後一貫的差別服務

QoS 強化機制

QOS 的特徵可用以支援允許控制的過濾、、擁塞管理時的排列、避免擁塞時的丟棄動作、訊務條件式的限制及鏈路效能管理的片段等功能。



2. QOS 的分類：



測量技術包括

【1】網路流量 Net Flow

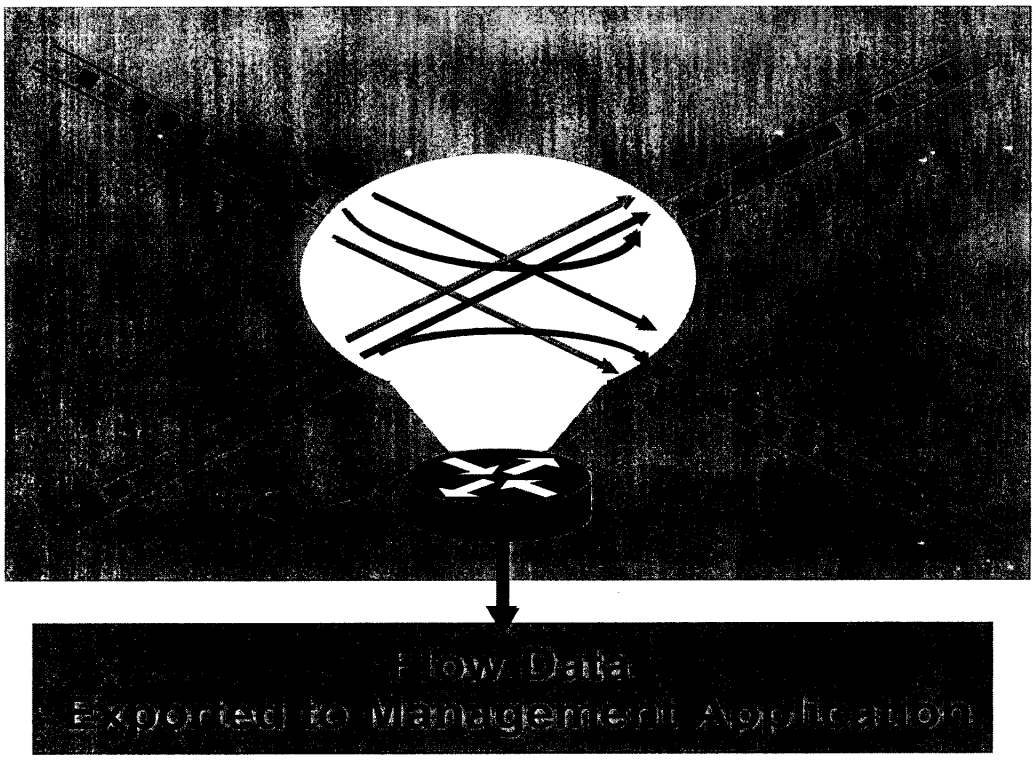
【2】服務保證媒介 Service Assurance Agent

【3】應用反應時間 ART MIB Application Response Time SNMP MIB

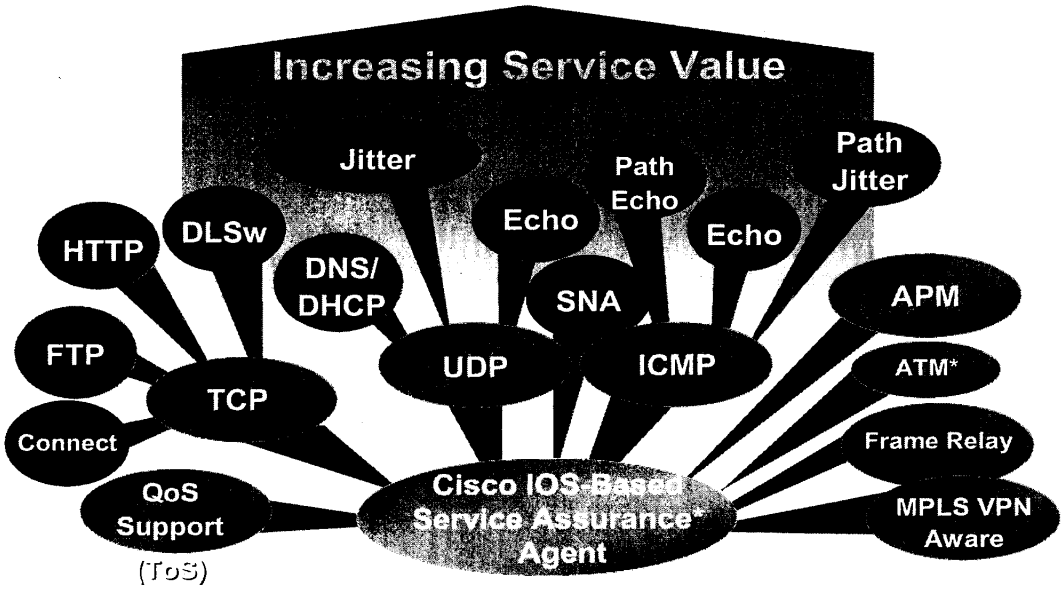
【4】QoS：DSMON、CAR MIB、Class-Based QoS MIB。

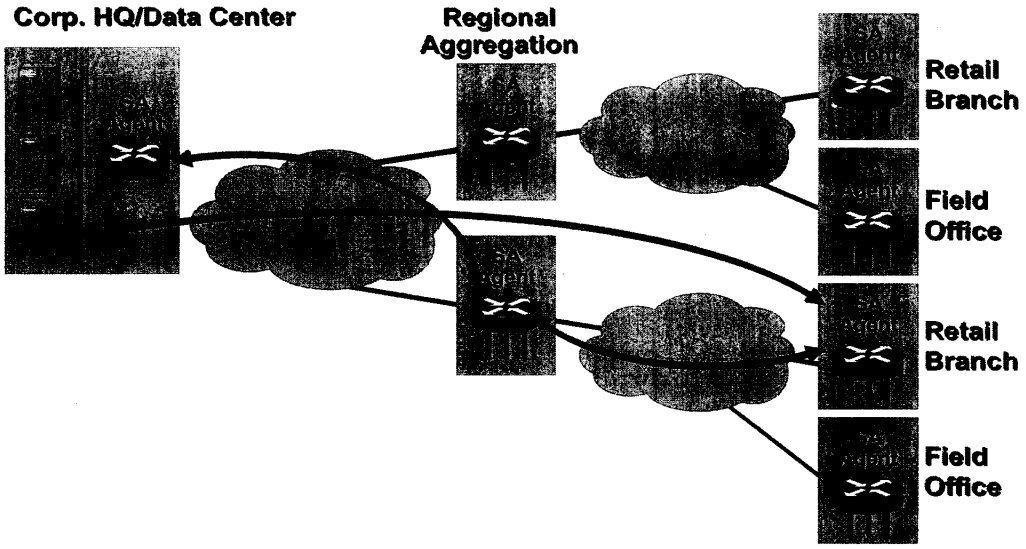
3. 網路流量：

網路流量是以下列七個主要項目定義之：1.來源位址 2.目的地位址 3.來源埠 4.目的地埠 5.第三層協定 6.ToS byte 7.輸入介面。它只有單向性，以每一輸入介面為基礎來發生效用，且能被規劃為隨選性或連續性。量測是在邊緣路由器而非在核心路由器。在帳務上的應用為發端、受端的資訊。在監視的應用上著眼於端對端更多的密集資料。


Flow Data
Exported to Management Application

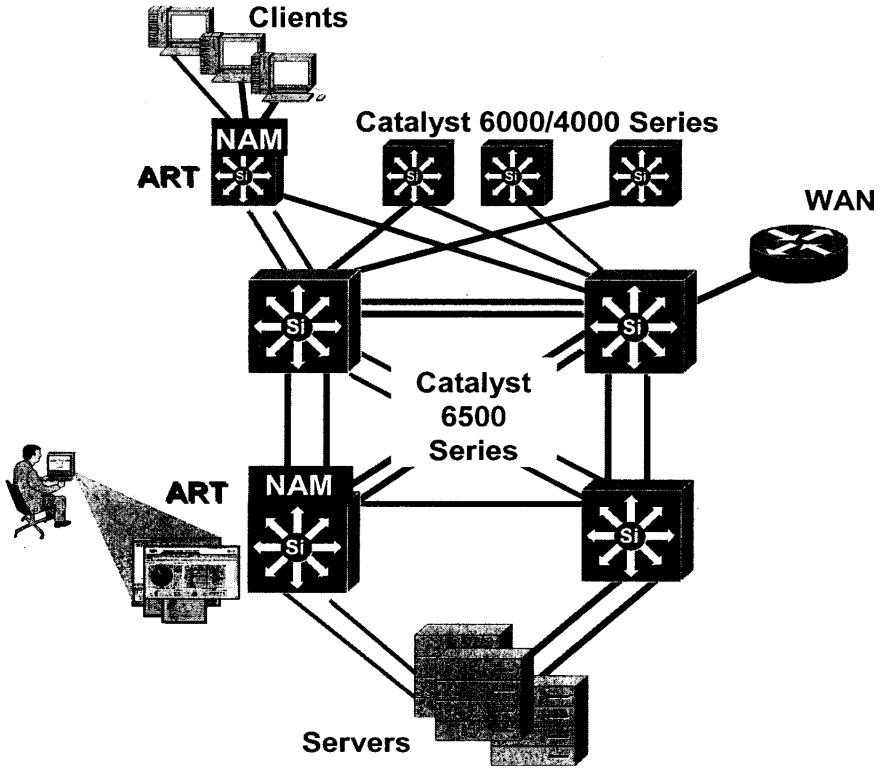
4. 服務保證媒介：


Increasing Service Value
Jitter
Path Echo
Path Jitter
Echo
Echo
HTTP
DLSw
DNS/ DHCP
SNA
APM
FTP
UDP
ICMP
ATM*
TCP
Connect
Frame Relay
QoS Support
(ToS)
Cisco IOS-Based Service Assurance Agent
MPLS VPN Aware

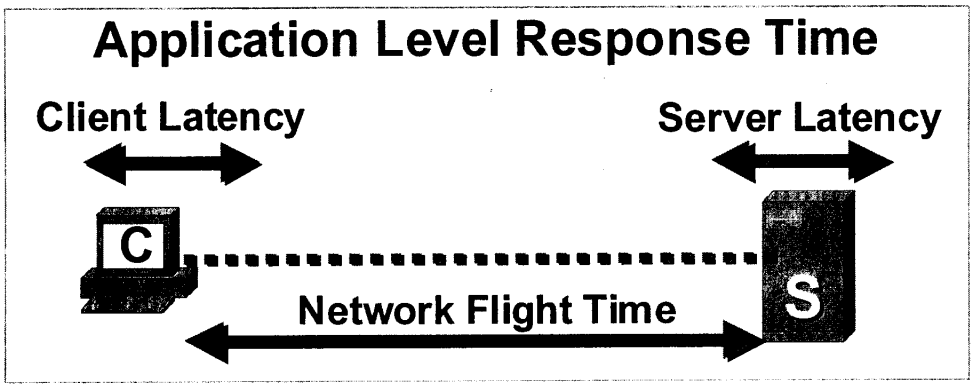


今日的SA隨著服務價值的增加而有不同的測量項目及對象。針對不同的協定可量測綜合的訊務，支援IP領先地位的QoS，且可量測延遲、不穩定及可用性，更具有決定性的方法論。

5. 應用反應時間：



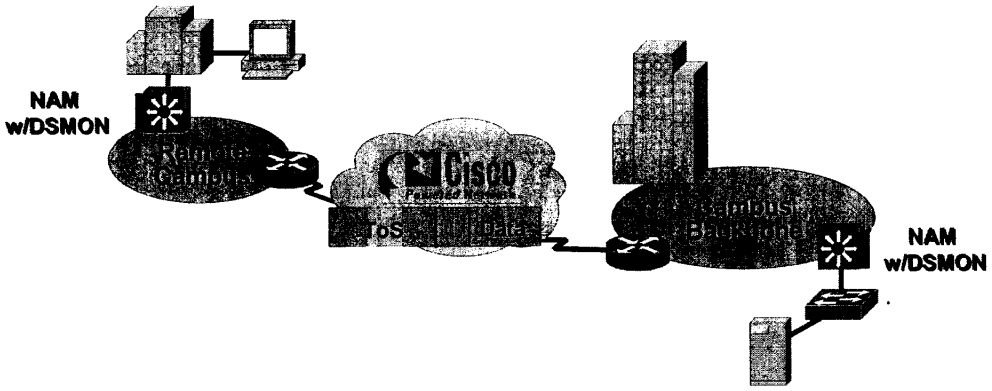
就內箝之 RMON 媒介而言，網路分析模組（NAM Network Analysis Modules）是針對臨界鏈路及高速骨幹網路設計。ART 監視選擇地安裝在 NAM 內。監視應用之工具用於量測應用效能及反應時間。



ART MIB 之功能性僅於 TCP 1.0，基於眾所皆知的目的地埠，可支援 25 種以上之協定。

6. DSMON：

不同的服務分別監視不同的 MIB。每一 DS 點碼（DSCP DS Code Point）值可被前向設備給予不同的處理。DSMON 能結合不同的 DSCP 以決定網路訊務。這項資料能被加以分析，便於調整 DSCP 的分配及設定 QoS 策略。當違反 QoS 策略時，DSMON 亦能顯示其可看性。



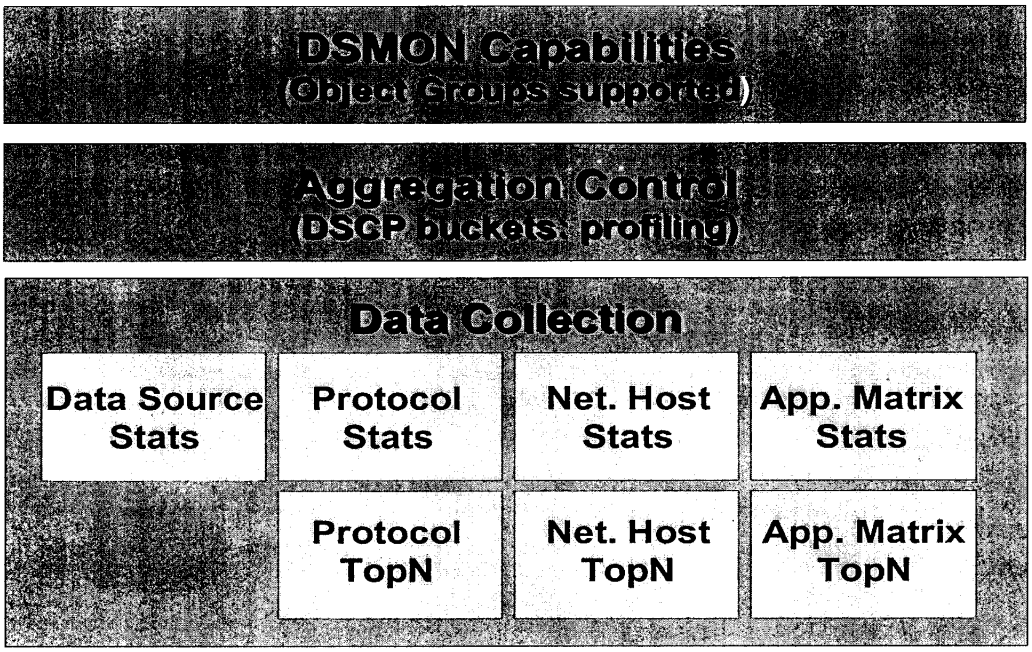
當使用 DSCP 時以 QoS 為基礎市有用的。使用 DSMON 能監視下列情況：

◆以 Diff Serv 分類項的訊務百分比➔有效規劃各種假設遺 QoS 的分配。

◆分類項的協定➔偵測標示不正確或未經授權的訊務。

◆分類項內協定的訊務量➔藉主機及對話有效規劃細節部分。

7. DSMON MIB 功能架構圖



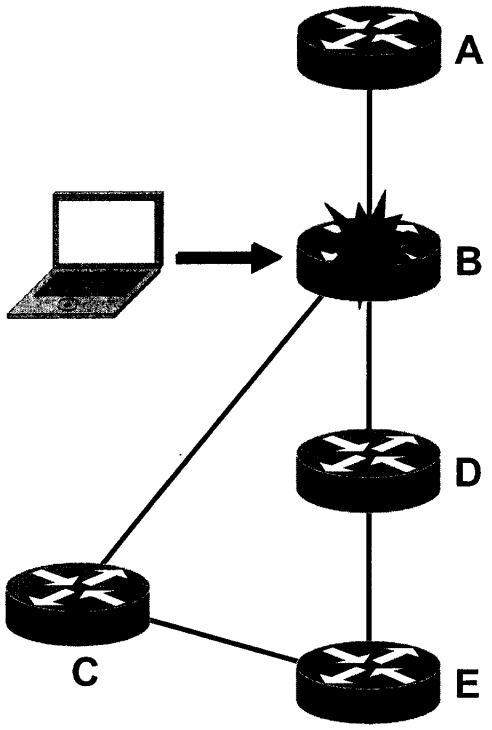
五、先進路由協定之安全性

必須事先知道的幾個基本概念(一)路由之基本概念，包含路徑之選擇及過濾。（二）BGP、EIGP、OSPF 及 IS-IS 之基本概念。(三）內部網路連結及網際網路之基本概念。(四）公共進鑰匙密碼使用法之基本概念。

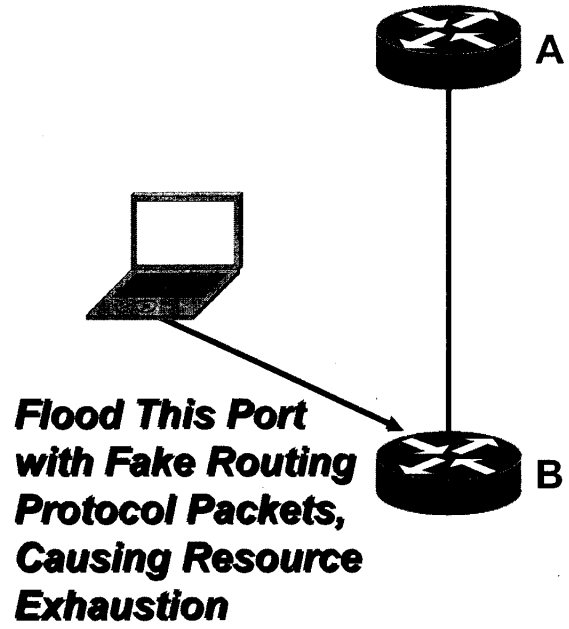
防禦攻擊之路由方式
路由器之保護
端對端之保護
網路邊緣器之過濾
BGP 之黑白名單

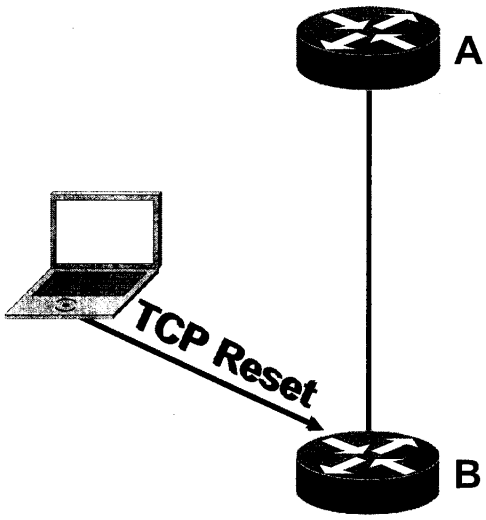
1. 中斷端對端：

路由協定描述端對端間之關係、資料傳遞之方法及其他相關語義。防禦協定遭受攻擊能透過拒絕服務中斷網路之使用性。抵禦及遭受攻擊時可能造成由 A 到 E 的訊務被丟棄不被傳遞。



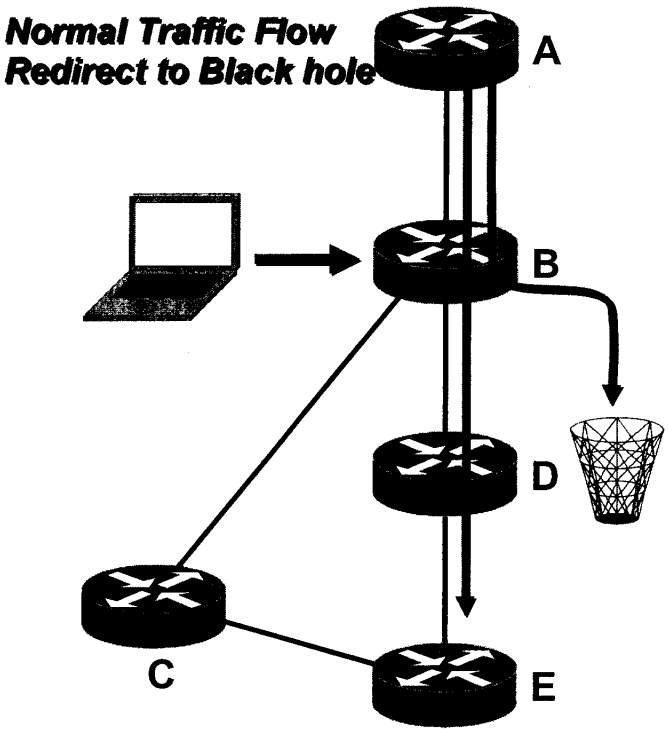
中斷端對端間之關係，一般而言和在臨界地點找出一個路由器的位址有關。找到該路由器之後改以正常 DOS 方式攻擊該路由器。透過 DOS 方式之攻擊必須有能力對那些遭受攻擊的路由器送出封包。



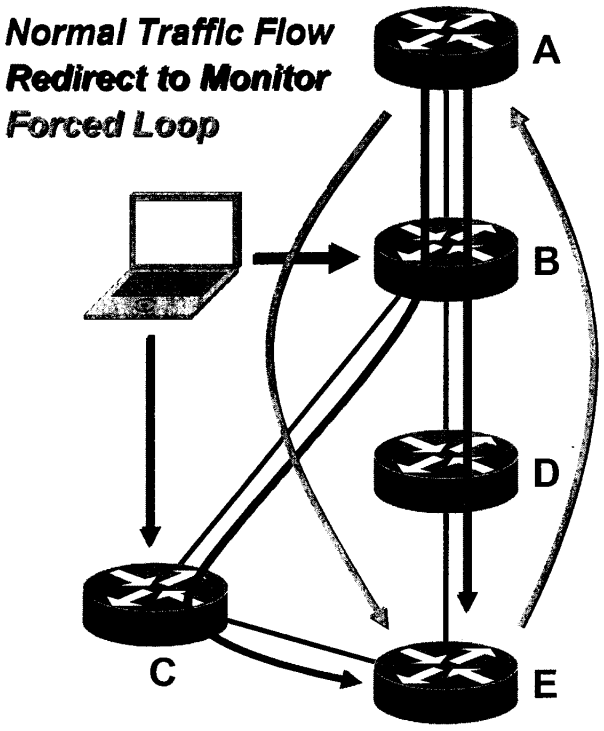


另一種更狡猾的攻擊如圖（p8）所示，是透過畸形封包或顯示設備已被攻擊等方式，迫使端對端的活動失敗，亦即以假的路由協定封包，造成 A 與 B 間之資源不足。如圖（p9）所示，是對 A 送出 TCP 重置信號使 A 與 B 之間的活動失敗。

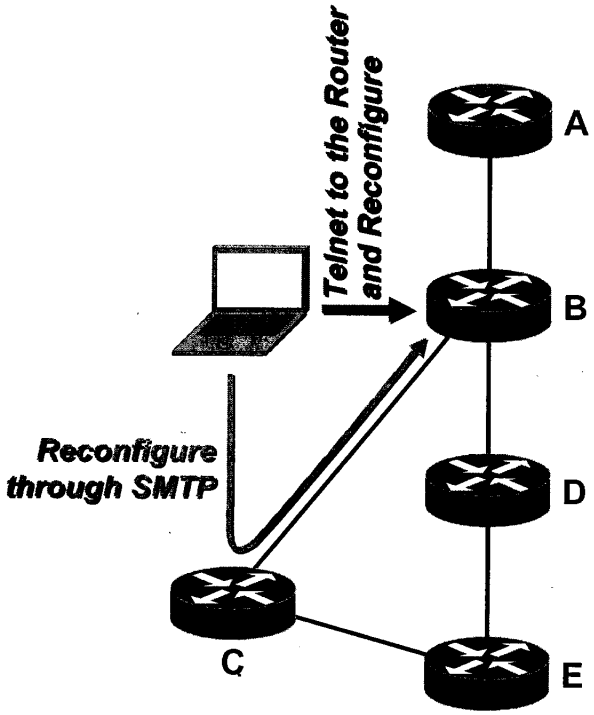
2. 中斷路由：



更狡猾的攻擊牽涉到在協定中攜帶攻擊情報。例如攻擊者很有可能將訊務誤導到一個看不見的黑洞中。

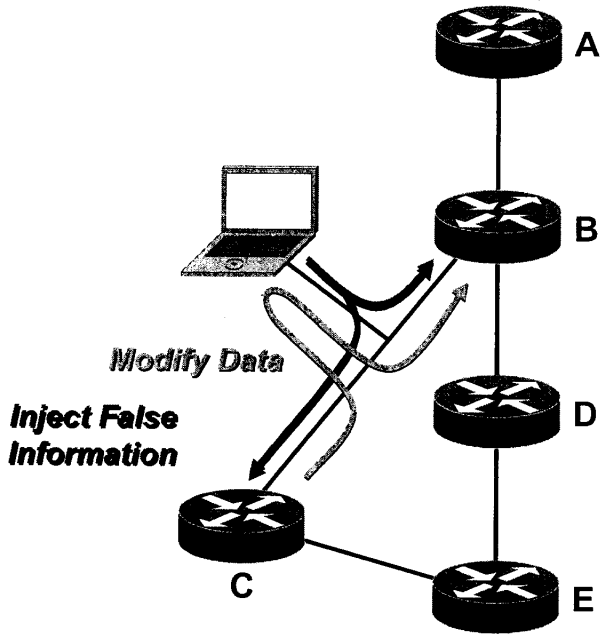


攻擊者有可能沿著監視中的路徑將錯誤的訊務導入，藉此能從資料流中擷取資訊。攻擊者也有可能在系統中強迫將路由形成迴圈，造成網路規模不斷擴張。攻這些林林總總不同型式的協定攻擊方式都必須將路由方式注入網路中。



攻擊者能危及連接在網路中的一個路由器，藉此注入錯誤的路由資訊。這需要能夠處理連接在網路的一個路由器的組態，以擷取得控制權並透過 SNMP 等方式來設定組態。

攻擊者能危及兩個路由器間的鏈路，並且注入錯誤的資料或修改傳送中的資料。注入錯誤的路由資訊包括參與迂迴路由系統。對 IGP 而言，這些需能擷取網路中的兩個路由器間的鏈路，而且有修改的能力或注入路由協定的封包。



總而言之，攻擊者必須能夠（1）找到可資利用之來源封包，傳遞至那些被攻擊的路由器。(2) 透過控制閘口或其他方式，重新修改路由器之組態資料。(3) 附掛在網路上，並模擬成網路範圍內的一部份。因此我們必須保護那些被危及的路由器，路由器間端對端之路徑，從錯誤地注入資訊中取得路由拓樸及垂手可得之情報。

3. 路由器之保護：

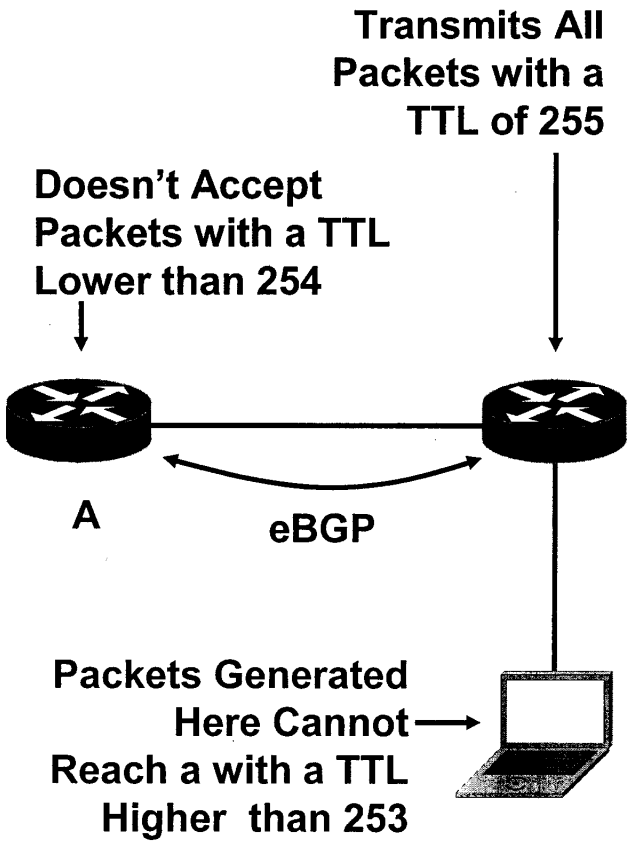
諸多事件中，攻擊者總是想從網路中擷取到一個路由器。因此，必須在網路上的任何一個路由器均有經過安全性考量的組態設定，來拒絕每一個可能被攻擊的機會。

瞭解密碼、權限等級，並且啟用這些機制。使用 SSH 連結到路由器，而不要使用 Telnet 來連結。使用 MD5 增強密碼之安全性或者 TACACS 來認證登入路由器的使用者。在終端機作業線上使用群組接取方式，搭配接取名單之建立，以防止外部人員接取路由器。

4. 端對端之保護：

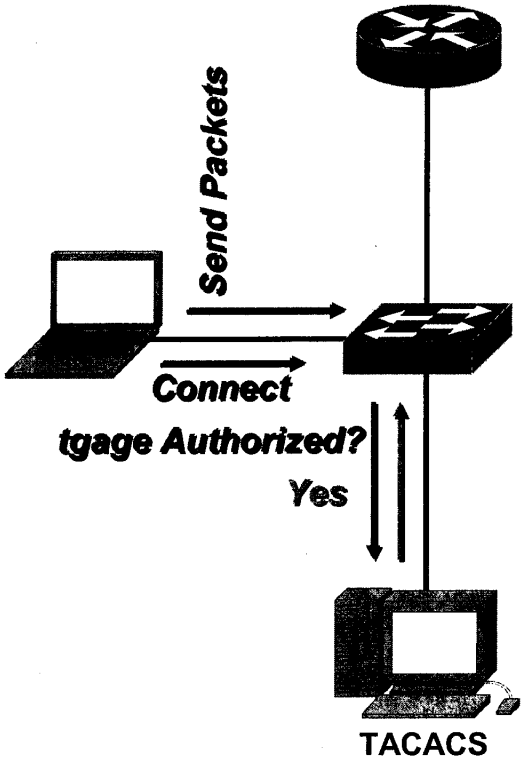
MD5 端對端授權能受到保護以避免畸形封包撕垮端對端連結及未授權的設備傳送路由資訊。但卻不能保護由於伺服器受到拒絕時的路由協定的重置。不正確的路由資訊被已遭受危及的有效設備注入。對於被兩端所傳送資料的授權，OSPF、IS-IS、EIGRP、BGP 均支援 MD5 的分類項目。MD5 在 eBGP 的活動期間必需與其他臨近系統取得協調。RFC1321 描述 MD5，RFC2385 則描述 MD5 和 BGP 的使用。MD5 不需強調到指定路由器封包的處理。它將限制那些路由器到指定路由本身之路由協定封包的處理能力。對於到不具 MD5 的指定路由器封包的處理效能不會產生衝擊。作業的進行使得 IPSec 和所有協定均能工作。

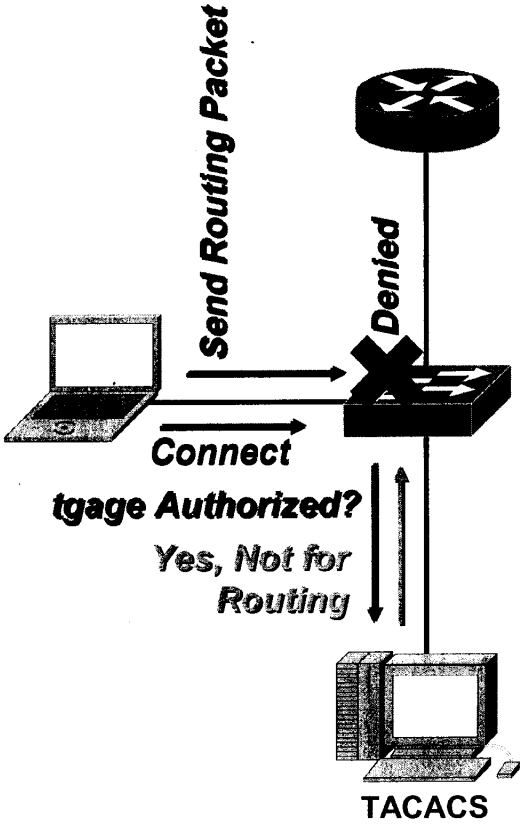
5. BGP TTL Security Hack：



BTSH 是一種機制用以保護 BGP 各端點避免多重跳躍的攻擊。EBGP 的發端被設定成以 255 的 TTL 傳送封包，並且拒絕 TTL 低於 254 或 253 的封包。那些不是連結在 BGP 發端間的設備，不能產生能被任何一端接受的封包。那些被使用的 BTSH 包括 BGP: CSCea29206、OSPF: CSCea59351、EIGRP: CSCea59358、NTP: CSCea59361。

未來的方向是 802.1X 第二層授權能和 TACACS 一齊用於授權連結在網路上的使用者。





一項計劃正與第二層使用者授權的發展下以路由方式緊密結合。如果一個使用者不被允許傳送路由封包進入網

6. 邊緣路由器之過濾：

當與外部網路作端對端連結時，絕對不可使用 IGP，只能用 BGP 方式來連結。因為 BGP 是一種 Policy-based 的協定，它擴充了一些過濾選項，而且 BGP 能去除外部堆疊的濫用。我們的目標是防止來自本地路由表使用路由策略的任何無效路由資訊。如果可能的話，在任何外部 BGP 端對端連結時，使用 MD5 連結。在網路邊緣路由器阻塞所有內部閘道協定（OSPF 及 EIBGP），這將保護避免攻擊者試圖使用路由協定的攻擊。BGP 增強版防止從路由器的廣播通知建立一個 BGP 端對端連結，就好像是源自另一個臨近系統（AS）一樣。

使用臨近系統（AS）路徑過濾器以過濾來自夥伴以及其他端對端路由器的廣告。如果不想接受全路由，那麼僅使用邊緣路由器的過濾機制，作為服務提供者連線之用即可。限制在邊緣上所能接受的路由數目，可防止由於組態誤規劃或攻擊所造成大路由表的傾倒現象。

將每一端對端連結，以及有多少必需廣播通知的路由列入考慮，因為就大部份夥伴端對端連結而言，數目字應該很小。由所有 BGP 各端所收到的路由資訊應予以阻擾，這樣的阻擾能保護避免由於網路的失敗或被當做攻擊的對象而發生經常性的路由攪動。

與其他網路界接的各端點上應過濾出偽造的路由。對於做為專用的端對端連結，應限制在相對應的各端點上。至於網際網路端對端過濾器而言，應過濾出被眾所皆知的偽造位旨空間。並於所有邊緣器對組態及使用單向廣播的反向路徑之前向動作做檢查。

7. 安全導向 BGP：

截至目前為止，我們有各種不同的安全機制，如路由器、端對端關係、過濾從網路外面進來不需要的路由資訊、避免路由的拍擊及過度的路由等等，但是前揭方式無論如何均無法保護路由協定裡所攜帶的資訊。我們一些將會（1）確認一個特定的臨近系統（AS）允許廣播通知其目的地，（2）驗證從實際地學習到路由各端有一通達目的地的有效路由，（3）驗證發訊之臨近系統（AS）可以有相對於任何策略之路由等等的需求。因此 Secure Origin BGP（soBGP）被提議作為 BGP 協定的安全系統。

由於 soBGP 設計上有下列的一些束縛，目前 soBGP 仍在發展階段。

（一）必需是漸增式的運用，亦即必需提供某些安全等級，不需每一臨近系統（AS）都參與。

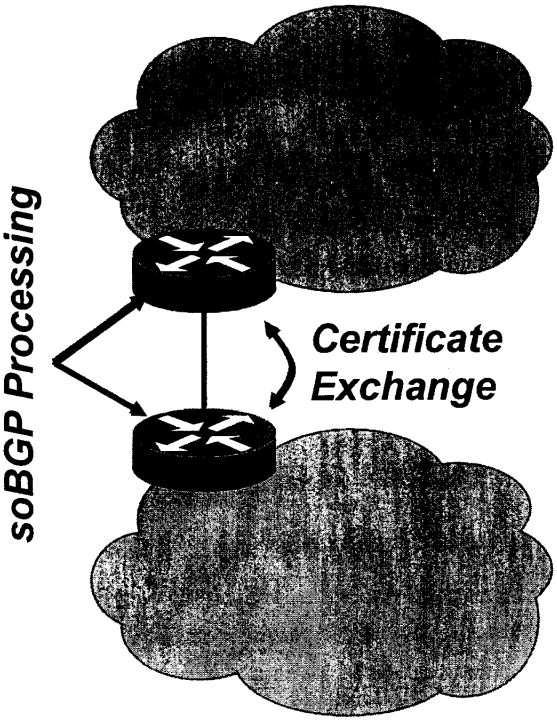
（二）必需具有彈性：使用或關閉密碼的使用；允許操作人員在安全等級、過載及速度收斂之間取得平衡。

（三）必需不依賴迂迴來達成路由的安全。

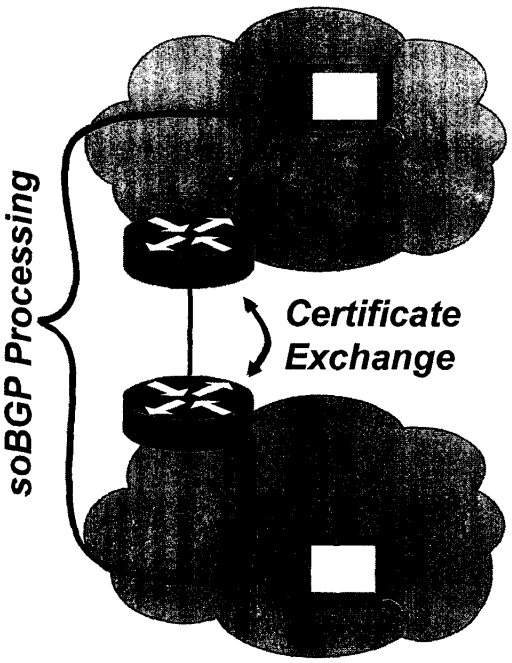
（四）必需不依賴集中式授權。

（五）對現在正在使用中的 BGP 協定所造成的衝擊最少。

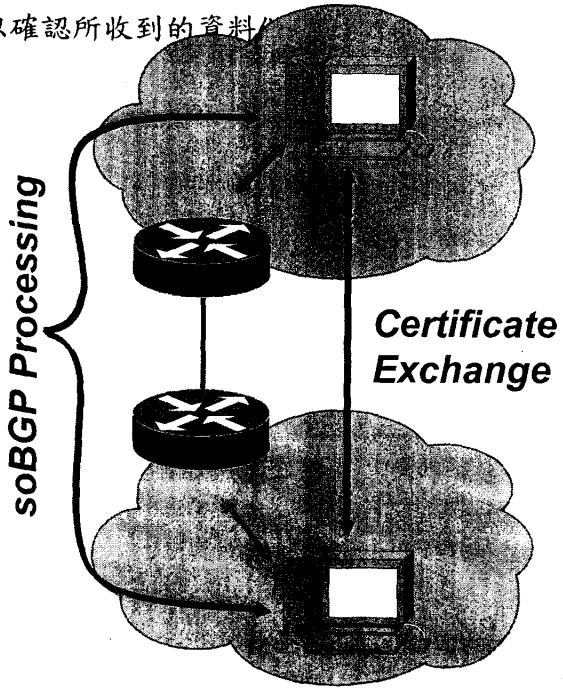
以下僅就 soBGP 的應用作簡單的說明，致於較詳細的束縛實例、授權的確認、確認臨近系統（AS）路徑、認證程序等不再贅述。



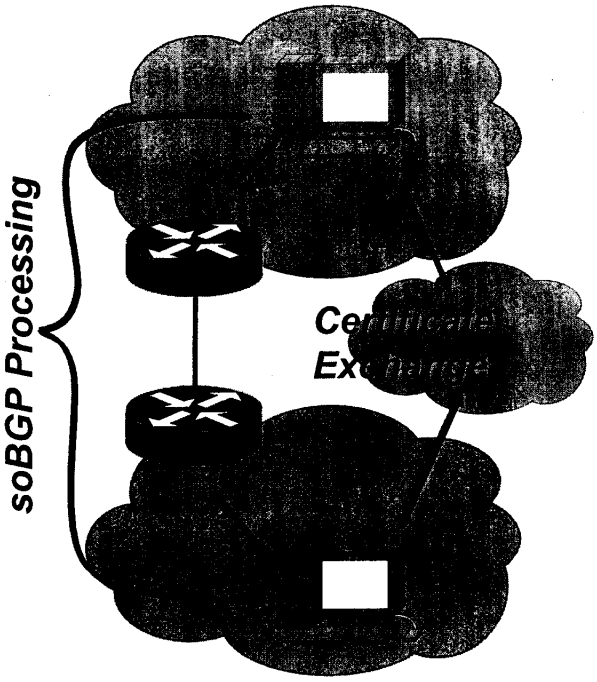
大多數直向應用選項為【1】在所有 eBGP 端點（AS 邊緣器）做交換的認證【2】認證程序及在每一個 eBGP 廣播通知者建立所需的 soBGP 表。每一 eBGP 廣播通知者必需具有執行密碼使用的相關程序以完成認證程序。



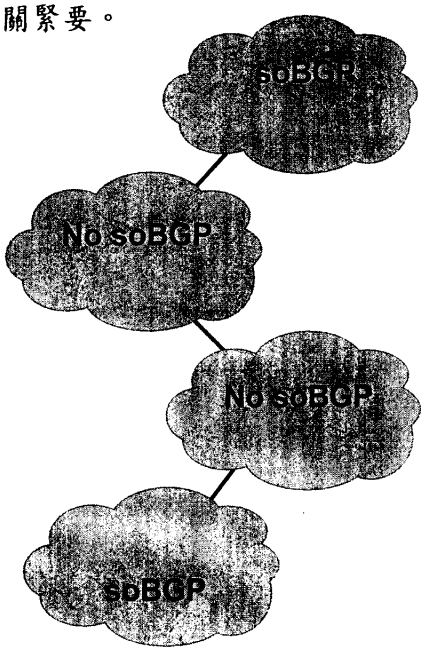
認證也能在 AS 邊緣做交換及穿梭，使用 iBGP 連結到 AS 範圍內的伺服器。這些伺服器履行所有的認證程序及建立所需的資料庫。邊緣路由器以 RADIUS 諮詢這些伺服器，用以確認所收到的資料



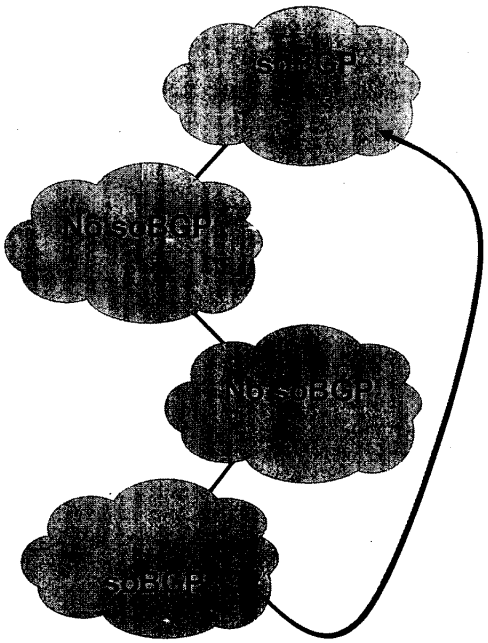
認證也能在每一個 AS 裡的 soBGP 伺服器之間直接使用多點 eBGP 做交換。



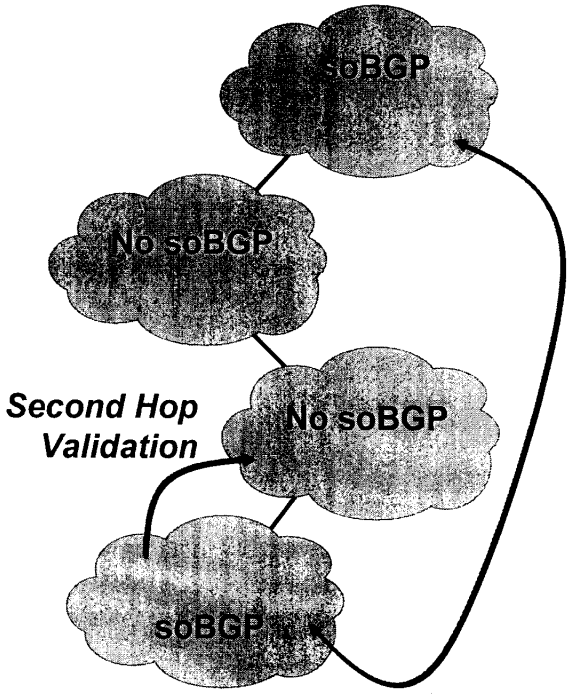
認證也有可能和某些型態的第三方（third party）提供者做交換。認證可能由一個 AS 產生以及被其他的 AS 廣播通知。只要使用相同的驗證程序，認證是如何注入到內部或接收，均無關緊要。



對於任何安全性系統而言，漸增式應用是一大障礙。於一個大的網際工作裡，在那些所有的 AS 執行安全性系統以後，就無法擁有停止的日子。SoBGP 永遠漸增式的應用，但是全部所能提供的安全性是和應用的完整性成比例的。



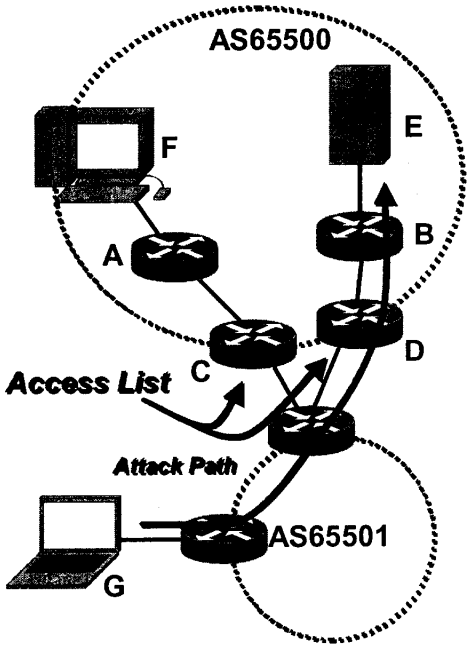
兩個都執行 soBGP 的臨近系統（AS），能直接透過 eBGP 多點連結或一些其他機制交換彼此的認證，他們彼此之間能交叉簽認或對某些信任的第三者予以簽認。



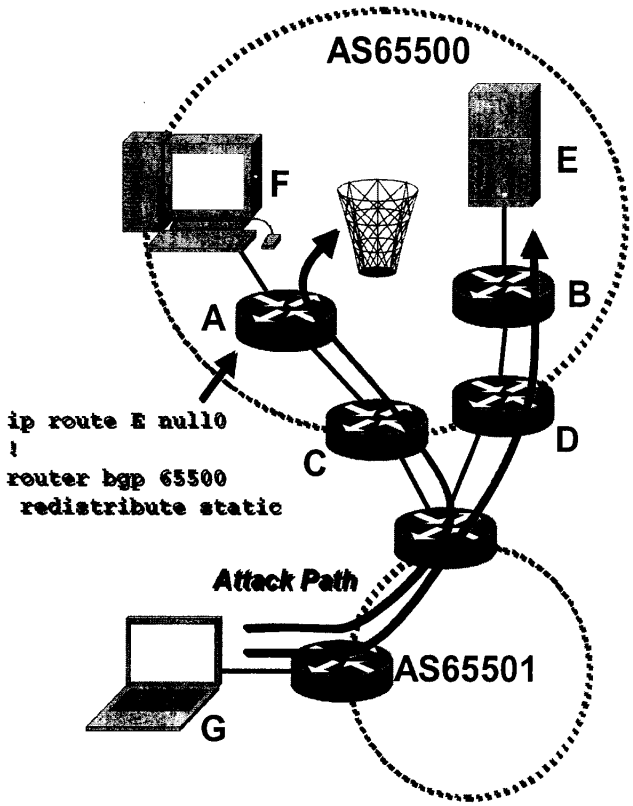
他們可驗證其他每一個認證以及更新這些認證。於 PolicyCerts 裡，藉連結廣播通知的使用，使得在 AS_PATH 裡的每一個方向，也能驗證第二個跳躍節點。當有更多的 AS 參與時，愈多的路徑將被驗證。

對任何使用 **AS_PATH** 方式鑑定資訊的機制而言，『**彙集 aggregation**』是一個問題點。對那些被授權可以發訊的前置內容而言，此一問題能藉限制 AS 到唯一的彙集點加以避免。

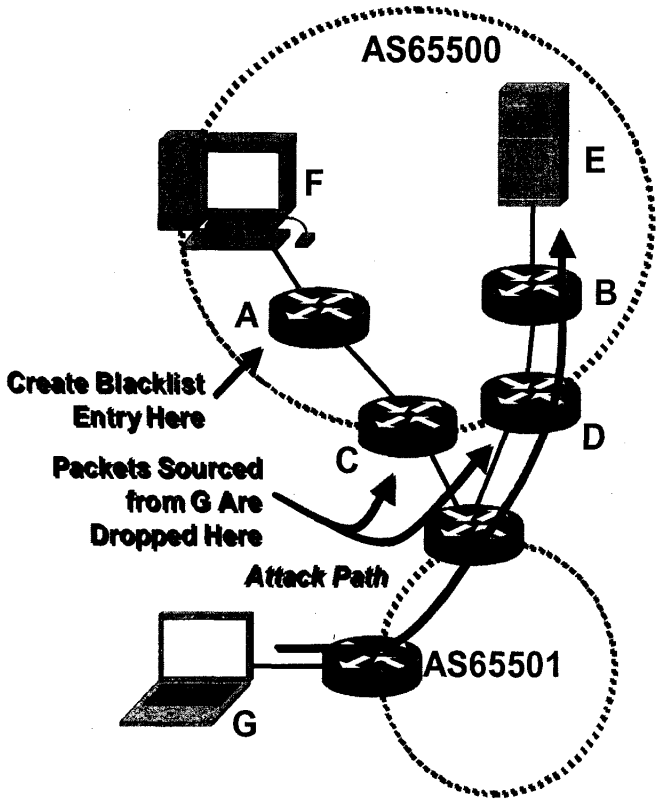
8. BGP 黑名單：



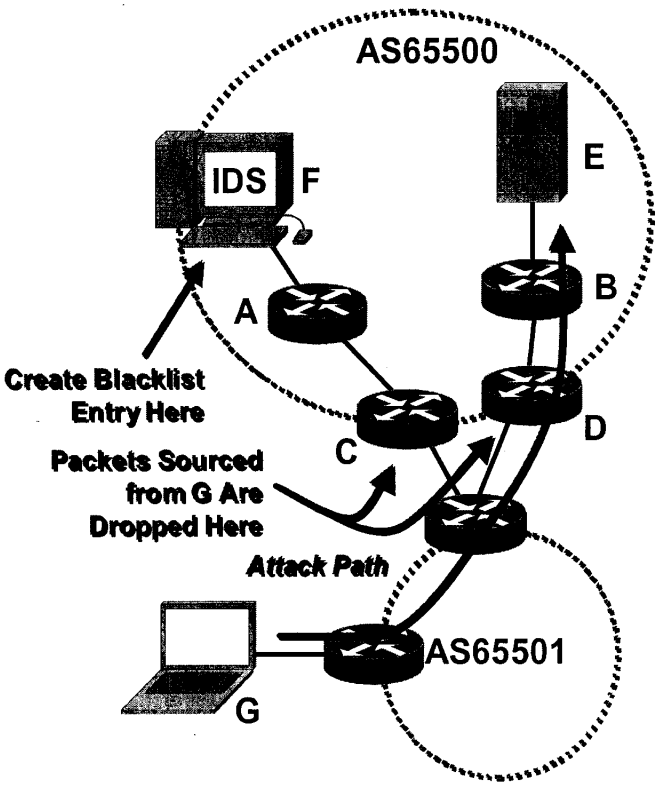
當 G 由外面的 AS 攻擊 E 時，在 AS65500 的系統管理上會有什麼方法可供選擇。在接取名單上阻礙 G 的同時，於 C 及 D 上規劃組態將會制止攻擊。這需要以人工方式在 C 及 D 上作組態規劃，使得某些接取名單上表列者，能適切被規劃，而且不會干擾或移除在邊緣路由器上的其他策略。



我們試著在 A 上規劃一些情況，以阻隔某些訊務。一個主路由設定為 0 或空的時，將能以 E 的位址在 A 上被規劃，且分派進入 BGP。C 和 D 屆時將封包導到 A，並將被丟棄。無論如何，由網路外面來看時，這將使得 E 成為不可達地區。

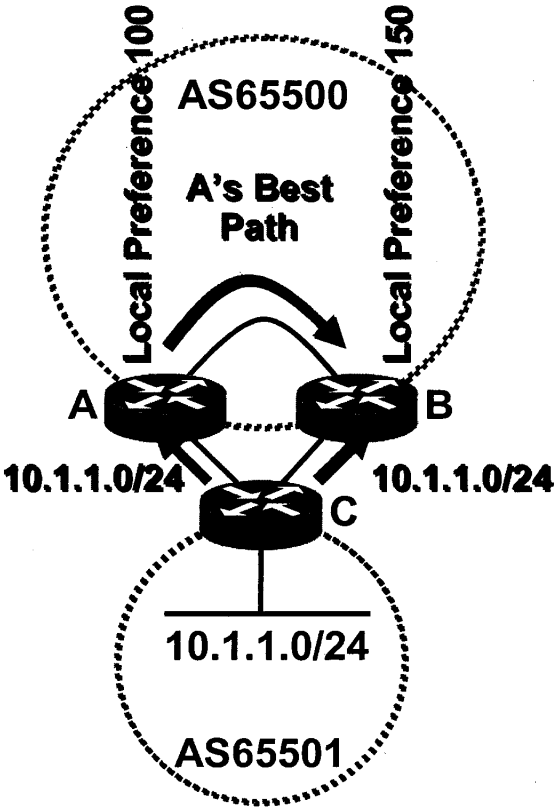


CSCea60907 將允許路由被放置在一個 BGP 社群裡且以 VRF 為基礎的黑名單上。路由可在 A 上被產生出來，而且一整設群附加在後面，如此將造成 C 和 D 將路由放在黑名單上。據此，從 G 而來的訊務，會在 C 和 D 被接收。來源位址被檢查是否違反黑名單，而且封包將被丟棄。

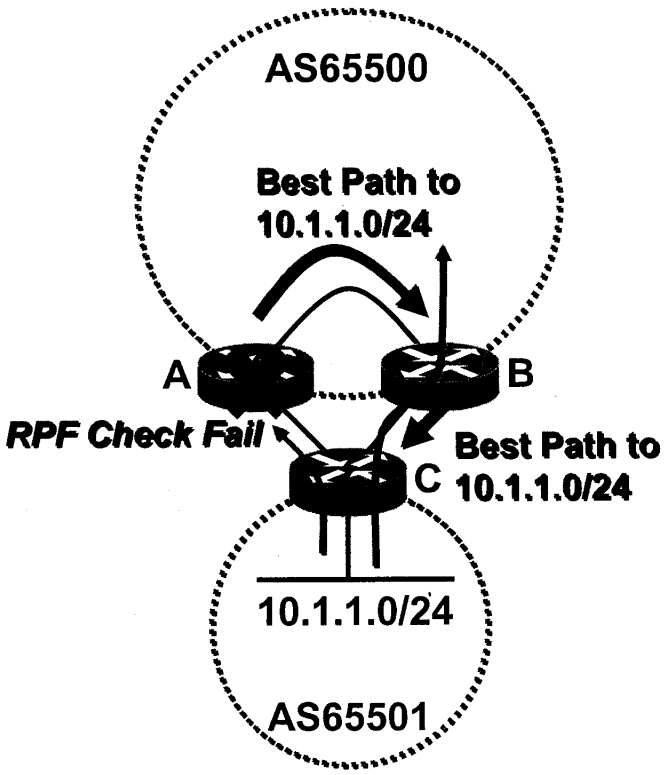


如果與侵入偵測系統結合在一起，功能將會變得更強大。當 IDS 感覺到一攻擊事件正對著網路上的一部主機發出攻擊時，它能注入正確的 BGP 路由，引起來源的封包在網路上的邊緣路由器時就被丟棄。這樣的工作正積極開發中。

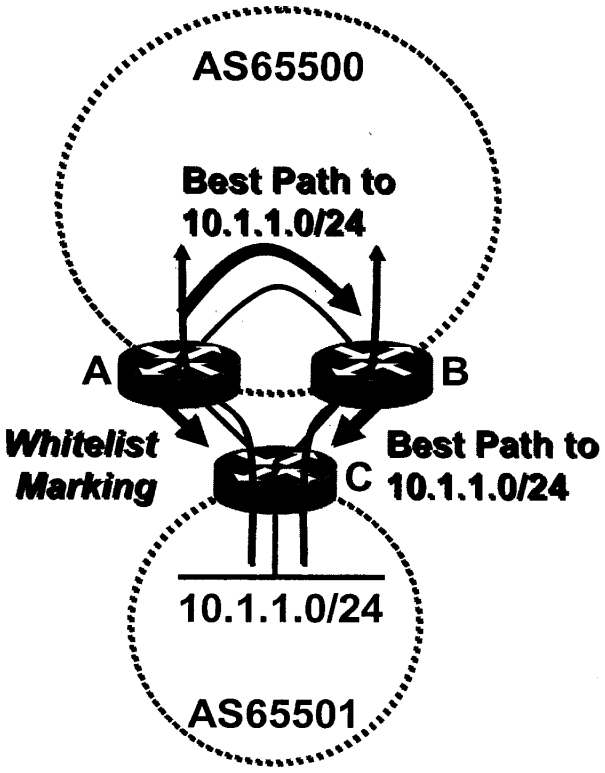
9. BGP 白名單：



CSCea60907 將允許 BGP 路由被放置在一個以設群為基礎的 VRF 白名單上。A 和 B 均學習到 10.1.1.0/24，A 設定本地參考為 100, B 則設定為 150。A 的最佳路由為經由 B。



如果 A 和 B 均啟動 RRF 單向廣播，因為最佳路徑是經由 C，所以由 10.1.1.1 發出的訊務經由 B 是可被接受的。因為 A 的當地路由表顯示訊務將由 B 過來，因此訊務經由 A 將被丟棄。在 A 以人工方式設定其組態權重，將可解決此一問題，但是如使其自動則將會更簡單的解決。



在 AS65500 內的 B 或其他路由器能以白名單社群方式標定為 10.1.1.0/24。當 A 接收到這個廣播通知時，會將 10.1.1.0/24 放置在白名單的 VRF。當封包在 A 作交換時，單向廣播的 RPF 碼檢查白名單的 VRF，因此封包得以向前傳。

肆、結論與建議

IP 的技術隨著市場的需求快速發展，不僅功能增加，容量的提供，網路的管理，品質的保證，也成為電信業者投資的考慮因素。感謝 Cisco System 思科系統公司提供新技術及應用的相關資訊。不僅網際網路上的應用，未來可朝 IP 化交換機及 IP 化用戶專用機方面發展。帶給使用者更新更優質的通信環境。本出國報告僅就個人淺見提出說明，尚祈先進前輩不吝指正。以下就管理及品質方面提供兩點建議作為參考：

一、IP 網路的環境，銜接客戶端所需設備關係通信路徑之整體品質，宜有相關規格加以規範，避免造成彼此之間 interworking 的障礙與困擾，影響通信品質，甚至於對本公司造成負面的效果。

二、SLA (Service Level Agreement)機制的建立配合網路管理的功能，更有彈性，確實依不同客戶的需求提供不同等級的服務，以創造更高的營收，再搭配 QoS (Quality of Service)、CoS(Class of Service)、ToS(Type of Service)等考核方式，確保點對點的通信品質。