

# 網路頻寬管理器

## 產品功能與效能評比

測試計畫主持人：林盈達

主測者：魏煥雲

測試助理：姜景娟、柳奕仲

網際網路快速地商業化後，許多企業需要存取 Internet 資源或被 Internet 成員存取。這些動作除了應被防火牆保護不受破壞外，狹小的 Internet 專線資源亦有管理的需求。目前國內的 Internet 專線昂貴，例如 T1 一個月需要 20 幾萬元，國際專線更貴得不在話下，因此在有限的專線頻寬內做最有效的管理早已是個趨勢。在此，我們將檢視各家廠商的網路頻寬管理器（Bandwidth Management Device），比較各家的功能（Functionality）、管理介面（Management）、準確性（Accuracy）、公平性（Fairness）、穩定度（Stableness）、穩固性（Robustness）、頻寬共享狀況（Bandwidth Borrowing）、延遲測試、VoIP（Voice over IP）品質測試等，以提供網管人員選購時的參考。

## 1. 市場需求與主要技術

- 市場需求

企業利用 Internet 各項服務可以節省很多成本，增加便利性。例如分公司間資料的流通、外勤人員利用 Internet 存取公司資源等。因為這些流量的重要性不一，狹小卻又昂貴的頻寬往往無法為公司有效地利用。例如企業的 ERP (Enterprise Resource Planning) 軟體、與顧客交易的電子商務連線的流量，可能被不重要的 FTP 佔據頻寬。企業因而使用頻寬管理器來訂立許多策略（policy），例如每部門或某項應用可分到多少頻寬，以謀求企業的最大利益；甚至同一大樓的多家分公司共租一條專線時也有切割頻寬的需求。policy 的訂立通常透過設定封包分類器（packet classifier）來分群（哪些 packet 符合此策略？），再設定各群的頻寬參數（符合此群者應得到多少頻寬？）。

- 傳統技術：排隊

頻寬管理器最直覺的想法，就是讓不重要的 packet 排隊，重要的快速通過，其中又

分為「優先式 (priority-based)」與「頻寬控制式 (rate-based)」。前者透過訂立各群的優先次序來讓重要的 packet 優先通過，適用於少量、極端重要、交談式的資料流，但卻無法保證某群組的頻寬上下限（這就好比說若大家都有 VIP 卡，那其實就沒有人是 VIP 了）；後者透過訂立各群的頻寬上下限，並由封包排程演算法 (packet scheduling algorithm) 來決定下一個要轉送的 packet 由哪一群挑出，讓送過多的送端們排隊，並讓某些應用享有最低保證的頻寬。

排隊的方法在處理 UDP 與 TCP 資料流時會有不同的效果：

- UDP 送端的流速通常並不會視網路擁塞狀況而調整，除非 application 有流速控制。
- TCP 送端除具備「保證資料送達 (reliability)」外，還具備「自動調節流速 (congestion control)」的功能。前者是在 data packet 成功送達後透過收端回應 ack packet 來確認收到（沒收到某 packet 的 ack 則會重傳該封包）並觸發送出新的 packet；後者會因線路品質 (packet loss) 和連線遠近 (round-trip time) 來調整流速。雖然 TCP 會自動調整流速，但是會造成極大量的封包在頻寬管理器排隊。

對頻寬管理器而言，最理想的狀況應該是主動地控制送端的流速，讓送端送出剛好的量以避免排隊，減低排隊的空間與延遲；次理想的狀況才是完全利用排隊來被動地控制送端的流速，因此許多產品皆對 TCP 連線作控制。

- 針對 TCP 設計的作法：

由於 TCP 連線可以透過對控制回程的 ack 來主動控制送端，因此許多廠商可做到保證各「群」中各「TCP 連線」的頻寬，主要方法有二：透過「更改 TCP window size」與「強迫封包遺失 (packet drop)」。前者透過縮小 window size 直接影響送端送出的量，本次測試的 IPolicer、PacketShaper、WiseWAN、QoSWorks、GuardianPro 屬於此類；後者透過送端偵測 packet loss 間接縮小 window size，本次測試的 FloodGate 屬於此類。

本次測試的對象大部分有混合 priority-based 及 rate-based 的方案，然而我們的測試偏重於 rate-based 方面的設定，著重於其對「由 LAN 流向 WAN」的「TCP 連線」(TCP 占 90% Internet 流量) 的控制力，檢視各產品在設定各種頻寬上下限後，能否能真正落實。UDP 方面我們採用 VoIP 的測試來作代表。

## 2. 測試對象

在篩選產品的過程中，我們首先查詢各家廠商的網頁，找尋哪些產品具有頻寬管理的功能，再由網路通訊雜誌社出面對各廠商發出邀請，並附上我們的測試計畫書。邀請到的廠商與其資訊列於表一。由於各廠商借測的機器等級有差別，因此我們作的測試以低頻寬的連線

設定為主，降低硬體的因素以測出各家控制頻寬「能力」的差別。

Vendor/ Model	背景	代理商	頻寬控制能力(廠商宣稱)	S/W version	作業系統，平台	Hardware						Price (未稅，無service)
						Boot from	CPU	RAM	Interface	Fail Over	Log to	
NetGuard's Guardian Pro	原產於以色列	新脈	10Mbps	5.02	NT, Software	Our P!!! 700MHz NT 4.0 Server with 256M SDRAM, 2 Intel 100M NICs installed						15 萬
CheckPoint's FloodGate	原產於以色列	精誠	無限制，建議為 45 Mbps	4.1	NT, Software	High Availability Module						13 萬 (25人)~80 萬(無限)
NetReality's Wise Wan 200/500	原產於以色列	漢康	5Mbps	4.0	Proprietary, Hardware	Flash 32M	P 133	32M	V.35 (10Mbps for logging)	Y	Another NT server	48 萬
Acute's IPolicer/ Broadweb's BandKeeper 100-CR2202	台灣，由威播掌軟體，普邦掌硬體	普邦	100 Mbps	1.6.4	Embedded NT, Hardware	Flash 32M	P!!! 600	128M	10/100Mbps	N	Another NT server	30 萬
Packeteer's PacketShaper 4500	原產於美國，佔有率世界第一	旭昇	45 Mbps	4.1.2	Embedded Linux, Hardware	Flash	P!!! 600	128M	10/100Mbps	Y	Embedded Hard Disk	80 萬
Sitara's QoSWorks QWX-10000	原產於美國	聚碩	100 Mbps	1.8	Embedded FreeBSD, Hardware	Hard Disk	P!!! 600	192M	10/100Mbps	Y	Embedded Hard Disk	150 萬

註：受邀單位另外包括 Lucent 的 Access Point、Allot 的 NetEnforcer (此二家經詳閱測試計畫書並評估後，決定不參加) 與 Cisco 的 Cisco Assure (一開始即不參加)。Fail Over 定義為斷電是否可 bypass traffic。

表一、產品資訊與軟硬體平台表

待測物若看得懂越高層的協定運作，網管人員越可以簡單地設定群組的成員。例如 FTP 協定中有所謂的 passive mode，在 FTP-Cmd (port 21) 連線中協議將傳資料的 port 由原來的 FTP-data (port 20) 動態地調成另一個 port，若待測物不認得 FTP-Cmd 中在溝通的事，就沒有辦法控制到後來真正在傳資料的連線了。表二整理了各廠商支援的協定、網路協定層級以及可管理到流量的協定 (非僅辨識公司內部使用的協定)。由於分公司間可能會有 LAN 的 protocol 在互傳，亦有管理 IPX、NetBios 的需求。詳細比較結果請參閱 4.1 節。

Vendor/ Model	Layer awareness	Built-in protocols		Application Aware	ICMP	IPX	NetBios	# of other protocols
		TCP	UDP					
NetGuard's Guardian Pro	4	60	35	N	Y	N	N	15
CheckPoint's FloodGate	7	60	35	URL/MIME-aware	Y	N	N	
NetReality's Wise Wan 200/500	7	109	79	URL/MIME-aware	Y	Y	Y	Above 250
Acute's IPolicer/ Broadweb's BandKeeper 100-CR2202	4	12	Cannot control	N	Y	N	N	可人工新增 service
Packeteer's PacketShaper 4500	7	Above 200 (layer 2 ~7)		URL-aware	Y	Y	Y	Above 200
Sitara's QoSWorks QWX-10000	4	靠人工填入 port #		N	N	N	Y	靠人工填入 port #

註：此表為廠商宣稱可控管到的協定，非僅可辨識到的協定，且此部分並未逐一驗證。

表二、協定支援比較表

在功能方面(表三)，所有待測物皆可以控制「群組(class)」頻寬的上下限(Max/Min)，

除 Netguard Guardian Pro 以外都還可以做到保證「群組中的連線 (connections in a class)」頻寬下限 (min)。這兩種設定大都可進一步設定「群組之間 (inter-class)」或「群組內保證頻寬連線之間 (intra-class)」的互借頻寬，使得 class 間可利用其他 class 剩餘沒用的頻寬。詳細比較結果請參閱 4.1 節。

Vendor/ Model	Packet Classifier		Schedule Control (policy active time interval)	Direction (In/Out)	UDP traffic control	WAN Link Speed Setup	Bandwidth Borrowing 互借頻寬		Per-Class Bandwidth Control		
	Src/Dst IP/Port, mask, Prot. ID	Host list					Inter-class (class 間)	Intra-class (class 內保證頻寬連線間)	Max	Min	Guarantee connections in the class (Min)
NetGuard's Guardian Pro	Y	Y	Per-rule	Y	Y	Y	Y	無保證連線頻寬功能	Y	Y	N
CheckPoint's FloodGate	Y	Y	Per-rule	Y	Y	Y	Y	Y	Y	Y	Y
NetReality's WiseWan 200/500	Y	Y	Per-rule	Y	Y	Y	Y	Y	Y	Y	Y
Acute's IPolicer/ Broadweb's BandKeeper 100-CR2202 100-CR2202	Y	Y	Per-rule	Y	N	N	N	N	Y	Only support exactly the same (註二)	Y
Packeteer's PacketShaper 4500	Y	Y	Per-device (CLI*)	Y	Y	Y	Y	Y	Y	Y	Y
Sitara's QoSWorks QWX-10000	Y	N	Per-device	Y	Y	Y	Y	Auto	Y	Y	Y

\*CLI : Command Line Interface

註二：僅能控制「連線頻寬」剛好為多少

表三、頻寬設定功能比較表

在管理介面方面 (表四)，比較重要的是以一個主控台到底可以管幾台機器。對於 PacketShaper 與 QoSWorks 我們只能使用瀏覽器連上後對其管理，而其他皆可控制多台機器。

Vendor/ Model	Type	Management Console	OS		Monitor/Statistics	Alert
NetGuard's Guardian Pro	GUI Win32 Application	Global devices	Win NT/2000		Line Statistics Report Response Time Report Protocol Distribution Report	Log (日誌)
CheckPoint's FloodGate	GUI Win32 Application	Global devices	Win NT/2000		Line Statistics Report Response Time Report Protocol Distribution Report	N
NetReality's WiseWan 200/500	GUI Java Application	Global devices	Win NT/Solaris		Line Statistics Report Port Report Response Time Report Protocol Distribution Report VoIP Report Top Ten Talkers/Listeners Top Ten Protocols/Applications	SNMP trap
Acute's IPolicer/ Broadweb's BandKeeper 100-CR2202	Web Browser (Java Applet)	Global devices	Web Server Another NT Server	Web Client IE 5.0	Line Statistics Report Top Ten Report Top Ten Talkers/Listeners Top Ten Protocols	Email trap
Packeteer's PacketShaper 4500	Web Browser (HTML)	Single Device	Web Server Embedded Web Server	Web Client Any	Utilization Network Efficiency Top Ten Classes Top Ten/Twenty Talkers/Listeners Per-class Bandwidth Usage Response Time Report	SNMP trap
Sitara's QoSWorks	Web Browser	Single device	Web Server	Web Client	Per-class Bandwidth Usage	SNMP trap

QWX-10000	(HTML)		Embedded Web Server	Any	Link statistics Top classes per link Top Applications Protocol Distribution Traffic by address
-----------	--------	--	---------------------	-----	--

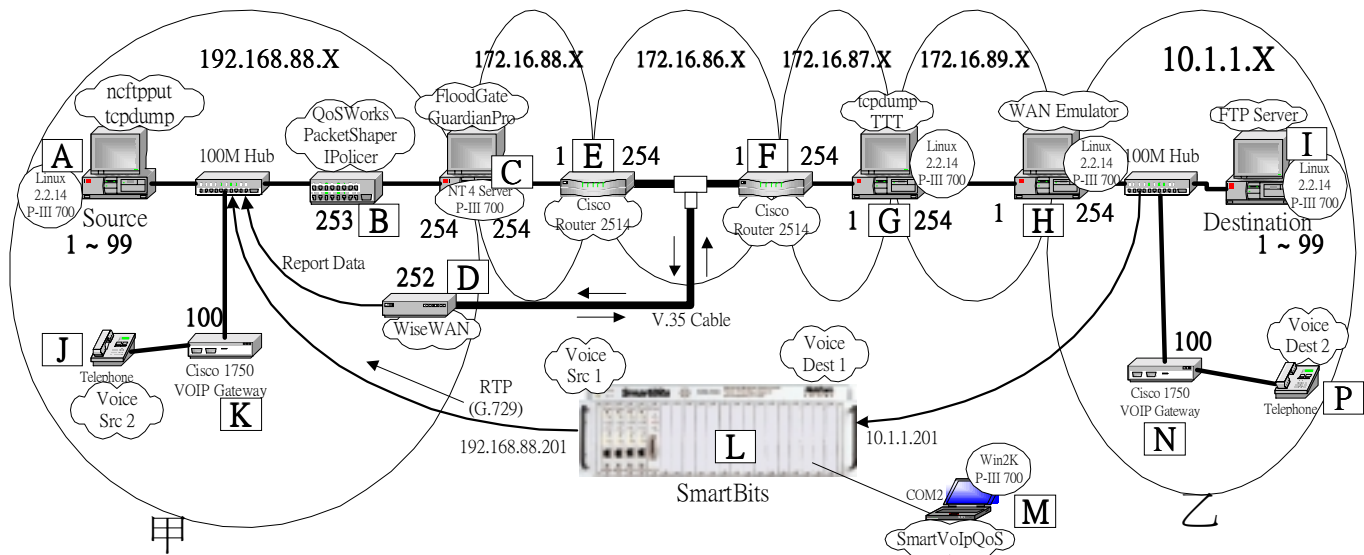
表四、管理介面與流量統計比較表

### 3. 測試平台與方法

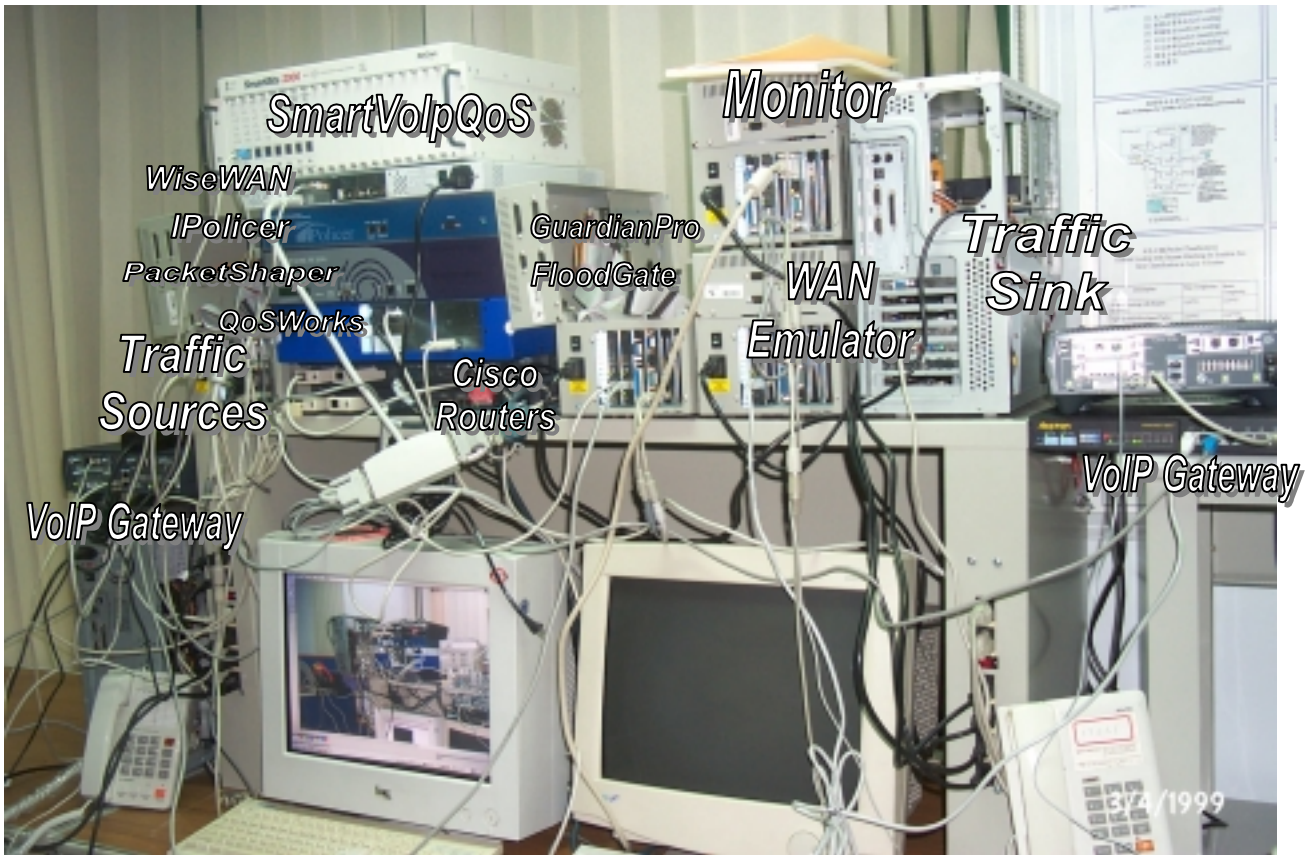
本單位測試分工如下：測試計畫主持人規劃主要測試大項與方向；主測者規劃測試細節、撰寫程式、學習使用機器、架設測試平台、實際測試、效能面圖形繪製、文章撰寫；測試助理負責聯絡廠商、學習使用機器、初步測試、整理功能面表格。在歸納整理過各廠商大部分的功能後，決定測試細項與方法，並撰寫測試工具來測試。測試平台細節與測試方法的細節是本節的重點，其重要性關係到測得的數據，網管人員若欲參考此文件結果請務必細讀本章，以免對結果認知有誤。

#### 3.1 測試平台 (Testbed)

如圖一所示，測試時資料流由甲→乙，中間的 Cisco Router 是專為 WiseWAN 而裝的(因其介面為 V.35 的專線上)，為公平起見，所有測試皆在此平台上(同一時間僅一待測物啟動)。Cisco Router 間的連線 clock rate 設為 2Mbps。圖二展示了測試平台照片。



圖一：測試平台實體連接圖



圖二：測試平台照片

## 3.2 測試工具（Benchmarking Tools）

在熟悉過所有產品後，我們發現並沒有多少合適的測試工具來表現出產品的差異性，於是開始自行撰寫測試程式。所使用的工具列舉如下（安裝位置標於圖一）：

- 流量產生器（Traffic Generator）：由於 Smartbits 不具 TCP 堆疊，僅可發出 TCP 封包，故使用多個同時在背景執行的 ncftpput（安裝於圖一的 A）產生多個 connection，封包大小皆為 1500 bytes，以較嚴格的狀況檢驗頻寬控制的準確度（大封包較難控制）。
- 即時流量監控器（Real time Monitor）：使用 ttt，安裝於 G。
- 封包擷取器（Packet Sniffer）：使用 tcpdump 記錄封包表頭到 RAM 磁碟中安裝於 A、H。
- 資料分析（Data Analyzer）：自行撰寫 awk script 來分析封包擷取器之結果。
- VoIP 效能測試：使用 SmartBits 上的 SmartVoIPQoS（安裝於 M）軟體。
- 廣域網路特性產生器（WAN Emulator）：可產生 WAN 上 delay 與 loss 的現象，由自行撰寫的 Linux Kernel Virtual Device Driver，利用精細度為 1ms 的 timer interrupt 來決定延遲每一個進入的 packet 多久。此外亦可設定「週期性/隨機性封包遺失率（periodic/random loss rate）」來模擬 Internet 上的封包遺失。此軟體安裝於 H。



## 3.3 測試方法 (Methodology)

測試的方向分爲兩類：功能面 (Functionality) 與效能面 (Performance)，分別詳述於後。

### 3.3.1 功能面 (Functionality)

功能面分爲「安裝簡易度」、「管理的簡易度」、「協定支援度」與「功能的完整性」。前二者檢視產品是否簡單易用；後二者著重在對應有的功能比較。此方面測試由三人分別替各產品打分數後取平均。

### 3.3.2 效能面 (Performance)

本測試計畫分爲三子測試計畫：

- A. 基本效能測試：彰顯各待測物「設定」與「實際測得」的差異性。
- B. 穩固性測試：彰顯各待測物在各種 Internet 實際狀況的穩固性或相容性。
- C. 進階功能測試：彰顯各待測物在特殊功能設定下的效能。

#### A. 基本效能測試 (Basic Test)

綜觀各待測儀器的功能，除了可以控制「群組 (class)」頻寬以外，還可以控制「群組中的連線 (connections in a class)」頻寬 (除 GuardianPro 以外)。簡單舉例來說，假設一公司各部門在待測物中各別被設定成一 class，待測儀不但可控制各部門使用的頻寬上限，亦可控制某部門中各連線頻寬至少都有多少以上。

議題	說明	比較標準 (解釋詳見內文)	簡而言之
準確性	測試 5 次各 class 「實際量測到」與「給定」的頻寬是否相符。	normalized goodput (註 1)，5 次取平均	越接近 1 越好
「準確性」之穩定度	比較「準確性測試」之中 5 次的差異性，彰顯是否每次測試的數據差距不大。	同上，但取 5 次之 CoV (註 2)	越接近 0 越好
公平性	各 class 中 connection 之間頻寬使用之公平性。	CoV of goodputs among 4 connections in each class，5 次取平均	越接近 0 越好
「公平性」之穩定度	每項測試作 5 次後，比較其差異性。也就是看看是否每次測試的數據是否差距不大。	同上，但取 5 次之標準差	越接近 0 越好
重傳率	各 class 中封包重傳率。	重傳數/送出數	越接近 0 越好

註 1：Goodput 爲『有效輸出』(bytes\_sent/time)，意即因封包遺失導致 TCP 重傳者不計入有效輸出。

註 2：CoV 爲 Coefficient of Variation，意即 standard deviation (標準差) 除以 mean (平均數)。

表五、基本效能測試

- 準確性及其穩定度：  
意義如表五所示。(若以測試結果為例，圖三 A1 各點皆為跑五次的平均，然而這五次中可能有高有低，因此在圖三 B1 中以 CoV 彰顯這五次之間各群組的變異性。)
- 公平性及其穩定度：  
在公平性方面要檢視的是，各群組中的四個連線是否公平地使用頻寬。「公平」是什麼意思呢？我們定義為 Class 內各連線（4 條）Goodput 間的 CoV。(若以測試結果為例，圖四 A1 中各點為五次 CoV 的平均；然而每點的五次中可能有高有低，因此我們在圖四 B1 中計算了這五次 CoV 之間的標準差來判斷「公平性的穩定度」。)
- 重傳率：  
重傳率高有二種可能性：(1)待測物對待 TCP 連線是以「強迫封包遺失(drop)」以致使 TCP 縮小 window 減低流速。(2)待測物 buffer 不足導致溢滿(overflow)。重傳會耗損企業內部的頻寬。

**待測物設定**：設定對外專線之頻寬為 T1 (1.544Mbps，其中 IPolicer 無此設定)，分為 5 種 class：20、40、128、256、1100kbps，每個 Class 設定『保證』每個 connection 都有該 Class 的 1/4 頻寬（註：NetGuard 無 per-connection 的設定）。這些設定都是「固定式」的，沒有「互借頻寬」的設定，以彰顯其準確度。

**測試方法**：由 A→I 灌入 20 個 FTP 資料流，並由 tcpdump 收集資料，250 秒後 kill 掉所有的 nctfpput，取其中 30~230 秒資料作分析；分析完後等待 200 秒，重複以上過程共 5 次。

## B. 穩固性測試 (Robustness Test)

Internet 中有很多的變化，造就出不同連線可能有不同的路徑，因此各連線會有不同的遠近、連線品質；在企業內部網路也可能有不同的作業系統，由於許多待測物對 TCP 資料流的 ACK 封包做更改，是否能相容於所有的作業系統則是一個考量。表六詳列了各測試參數與方法。

議題	說明	比較標準
連線距離不同	<p><b>待測物設定</b>：測試參數同 Basic Test。</p> <p><b>測試方法</b>：於 WAN emulator 中讓每個 class 中之 4 連線「來回時間 (round-trip time)」各為 10ms、50ms、100ms 與 150ms 後，作與 Basic Test 一樣的分析。</p>	同 Basic Test



封包遺失率 不同時	測試單一 TCP 連線在不同的 Internet 封包遺失率下效能的改變。 <b>待測物設定</b> ：設定某 connection 頻寬固定為 200kbps。 <b>測試方法</b> ：於 WAN emulator 中設定 periodic loss rate (每多少個遺失一個) 為 0.5%、1%、2%、4%、8%。	Normalized Goodput
送端作業系 統不同時	不同的 TCP 實作會在 Internet 有 delay 和 packet loss 時表現出來。 <b>待測物設定</b> ：設定某 connection 頻寬固定為 80kbps。 <b>測試方法</b> ：WAN emulator 設定 round-trip time 為 50ms，periodic loss rate 為 1%。測試單一 TCP 連線，送端分別為 Linux 2.2.14、Windows 2000、FreeBSD 4.0、Solaris 8 時，待測物是否可一視同仁 (收端固定為 Linux 2.2.14)。	TCP 連線在各 OS 下「送出 byte 與時間」 圖是否重疊

表六、穩固性測試

## C. 進階效能測試 (Advanced Test)

此測試包含「頻寬互借測試」與「VoIP」測試。前者可讓某 class 用不完設定的頻寬時，將剩餘的頻寬借給其他 class 使用；VoIP 測試透過 SmartBits 與 VoIP Gateway 方式來測試通話品質。詳細測試方法與待測物設定詳見表七。

議題	說明	比較標準
頻寬互借測 試	<p><b>群組間頻寬互借 (Inter-class Bandwidth Borrowing)：</b> <b>待測物設定</b>：總頻寬 (T1) 均分為 2 class，且可借用到全部。 <b>測試方法</b>：一個 class 一個 connection，依序啟動與結束。</p> <p><b>群組內保證頻寬連線互借 (Intra-class Bandwidth Borrowing)：</b> <b>待測物設定</b>：總頻寬 (T1) 為一 class，保證頻寬連線為 class 一半，且連線可用滿整個 class。 <b>測試方法</b>：一個 class 兩個 connection，依序啟動與結束。</p>	以 ttt 觀測各 連線頻寬與 總頻寬
VoIP 測試	<p>設定保證給 VoIP 群組的人某頻寬，沒通電話時頻寬可轉讓給其他群組，測試在流量滿載的情況下，啟動 VoIP 時的聲音品質。 <b>待測物設定</b>：待測物設定保證 30kbps 給 Voice，沒有 Voice 時背景 FTP 流量得佔用其頻寬。本測試之專線總頻寬有兩種設定：1.544Mbps 與 125kbps。</p> <p><b>透過 Smartbits (使用 SmartVoIPQoS)：</b> <b>測試方法</b>：由 SmartVoIPQoS 軟體控制 Smartbits，使其透過一埠產生 VoIP Traffic (RTP 格式，G.729 Codec，50 frame/s，frame size=74 byte，頻寬為 30kbps 左右)，另一埠收集資料並計算每個封包的 end-to-end 延遲、封包遺失率 (packet loss rate)、延遲差異性 (delay jitter)，並將這些參數轉換成一公認的聲音品質標準認定值 PSQM (Perceptual Speech Quality Measurement)，以對通話品質做最終的判斷。</p>	PSQM、 jitter、delay、 loss

	<p><b>透過 VoIP Gateway (Cisco 1750) :</b></p> <p><b>測試方法</b>：測試員手持甲乙兩方電話，在流量滿載的情況下由甲方撥打 VoIP 電話至乙方 (JK→NP)，並以正常講話速度唸數字 1~10 來判斷聲音的品質。VoIP Gateway 設定為靜音時依然 sample 聲音，因此即使不講話，流量依然為 30kbps 左右。此測試的結果比較主觀。</p>	以耳朵聆聽
--	---	-------

表七、進階效能測試

## 4. 測試結果

### 4.1 功能面 (Functionality Test Result)

#### A. 安裝簡易度

由表一、表四可概略瞭解安裝時的簡易性。內含 Web Server 者 (PacketShaper 與 QoSWorks) 安裝起來是格外容易；FloodGate、WiseWAN 軟體安裝起來到也還算好裝，除了 WiseWAN 的 Server Manager (使用 Sybase 資料庫) 安裝相當耗時間、空間；IPolicer 管理介面用的 Web Server 要裝在另一台 NT Server，手續稍嫌複雜；Guardian Pro 產品由於當時與廠商溝通時得知其必得與防火牆和 NAT 一起使用 (在 policy 訂立時要讓所有的 packet 通過，與 router 間得作轉址的動作)，中英文手冊、設定程式的中文化選單、中文化的 Help 等敘述不清楚，較不容易安裝。不過報告初稿付梓後廠商澄清頻寬管理器可單獨運作 (未經驗證)。

當然，「安裝簡易度」也許算不上是產品嚴重的優缺點 (尤其 Guardian Pro 是為了防火牆的安全性)，反正你買的時候廠商會教你那倒也還好，像我們自己 K 說明書是太強求了些。

#### B. 管理簡易度

表三、表四透露出些許管理的簡易度。大部分功能其實是大同小異，名字不同而已。不過我們一致認為 QoSWorks 的管理設計最人性化，但是 PacketShaper 也毫不遜色，尤其在 Traffic Discovery 上更勝一籌。PacketShaper 可自動察覺網段上的流量並新增好 policy，待管理者填上頻寬管理的各項參數 (如表三所示) 後即可，其他產品都得在手動設定完 policy 後監看流量是否有控制到；WiseWAN 與 IPolicer 設定 policy 的方式類似，其中 WiseWAN 是「非跨平台的 Java Application」，IPolicer 是「非跨平台的 Java Applet」(需 IE 5.0)，但是 IPolicer 無法設定讓群組間頻寬互借，而 WiseWAN 可以「自動」互借頻寬；FloodGate 除了要人工

計算各 Class 的 Weight 以外管理起來也算是方便；Guardian Pro 由於程式中文化翻譯不清，算是比較難設定的，不過熟能生巧，習慣後發現其是唯一可利用 Windows 拖放功能來設定的。

## C. 協定支援度

表三整理了各廠商協定支援的情況。如第二節所述，認識到第 7 層的協定會增加管理的簡易度與能力；在協定數量上 WiseWAN 和 PacketShaper 簡直在比多，相信備而不用的居多；其他至少可透過設定 port 來認識到一定數目的協定；FloodGate 與 NetGuard 其實也支援很多，只是沒前兩者誇張；IPolicer 與 QoSWorks 內建好的協定數很少，多得由自己查表設定。然而 IPolicer 雖可認出 UDP 類的協定，但卻無法控制其頻寬，加上其不能設定「專線總頻寬」與「頻寬互借」，推測可能 IPolicer 完全靠「針對 TCP 設計的作法」運作（如第一節所述），沒有 Packet Scheduler 在後以「排隊法」來處理。

## D. 功能完整度

表二整理了各待測物的功能。在 schedule 方面我們認為 per-rule 的控制較有意義（例如公司在下班後某些 policy 可取消，但像 VoIP 的 policy 一直 active 會比較好）；IPolicer 缺乏群組頻寬互借功能，IPolicer 在 Intra-class 方面僅能控制「連線頻寬」剛好為多少，算是有保證到 class 內各連線的品質，但是無法利用 class 內剩餘頻寬，另外，無法控制 UDP 類的頻寬、不能設定「專線總頻寬」，功能完整度尚待努力。NetGuard 無法設定 class 內各連線頻寬，但其實有自動對每一連線作控制（更改 TCP window size），推估是為減低在 Guardian Pro 排隊的長度。

## E. 特別功能

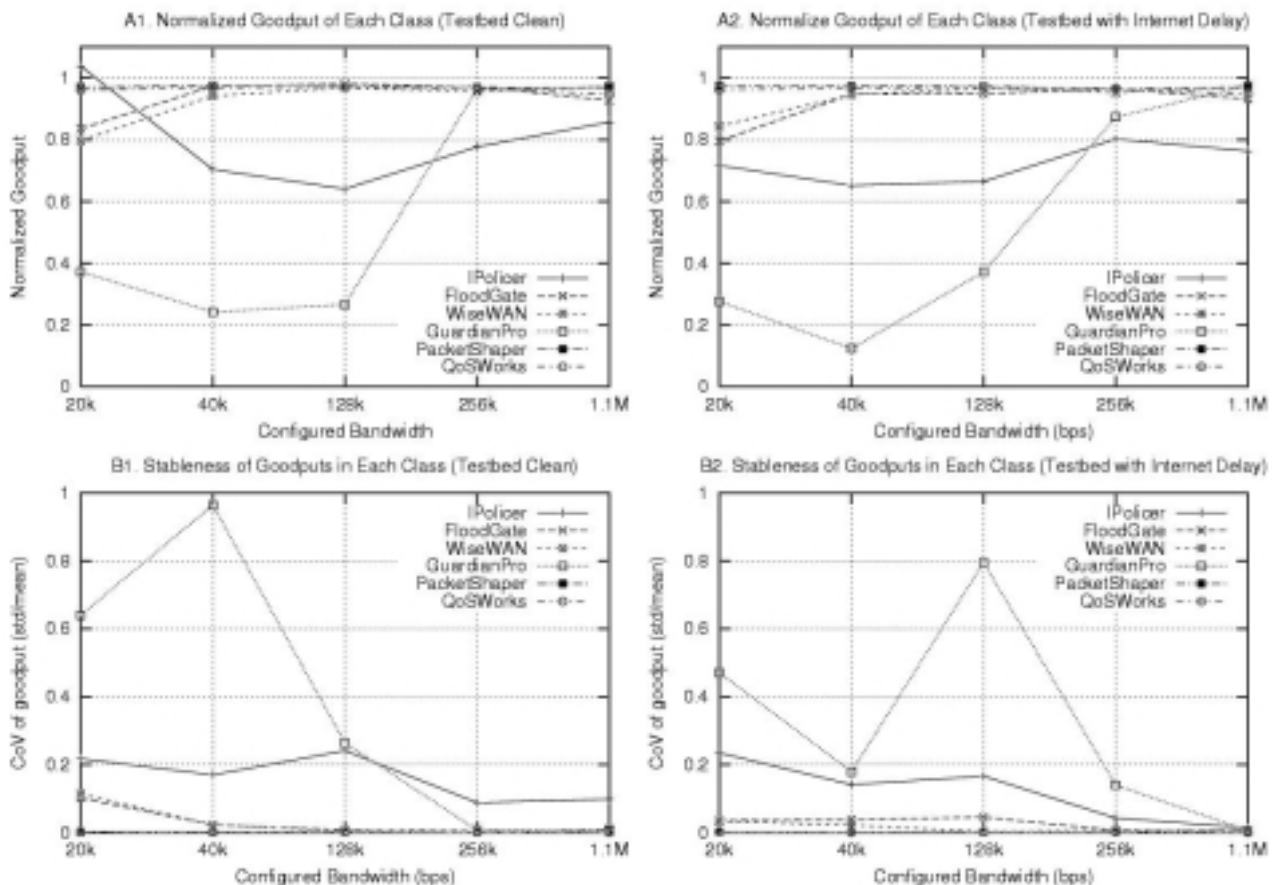
PacketShaper 可以利用 Traffic Discovery 來自動新增 policy，讓我們覺得很方便；WiseWAN 直接放在 WAN link 上作控制，具廠商所述可以偵測 ISP 給定的頻寬（使用者可確定與簽約時是否相符），而且由於 frame relay 的特性（所有 traffic 都可由 PVC 偵測到），錯綜複雜的 lease-line（各分公司間的網狀連結虛擬電路）僅需安裝一台就可搞定。這一點對很多公司的實體網路狀況很實用，很可惜我們沒有這樣的環境作測試。QoSWorks 對 VoIP 著力頗深，為此特別有控制 TCP 連線封包大小、Voice queue depth、max delay 設定，以讓 Voice 封包較順利地通過，在 VoIP 的測試中可以略知一二。另外 QoSWorks 內建 Web Cache，若企業不想另外設 Proxy Server 來節省頻寬，QoSWorks 是個選擇（此功能並沒有測試）。另外 FloodGate 與 Guardian Pro 皆為整合性的方案，支援防火牆、VPN、NAT，若一併選購可能可以節省管理成本。

## 4.2 效能面 (Performance Test Results)

### A. 基本效能測試 (Basic Test)

- 「準確性」與「準確性的穩定度」

圖三 (A1 為準確性, B1 為其穩定度, A2 與 B2 在穩固性測試中探討) 的測試結果告訴我們可以分出三組: PacketShaper、QoSWorks 表現最為準確、穩定; WiseWAN 與 FloodGate 在低頻寬的 class 稍微遜色; IPolicer 與 GuardianPro 在此測試中則較為遜色。值得注意的是 IPolicer 幾乎五次之中, 會有幾次有幾個 connection 建不起來的狀況, 所以該 connection 沒有傳送資料, 因此頻寬浪費掉、穩定度不佳 (註: 測試人員每台都測很多個「五次」, 確定確有此現象才將其中的一個「五次」納入分析)。

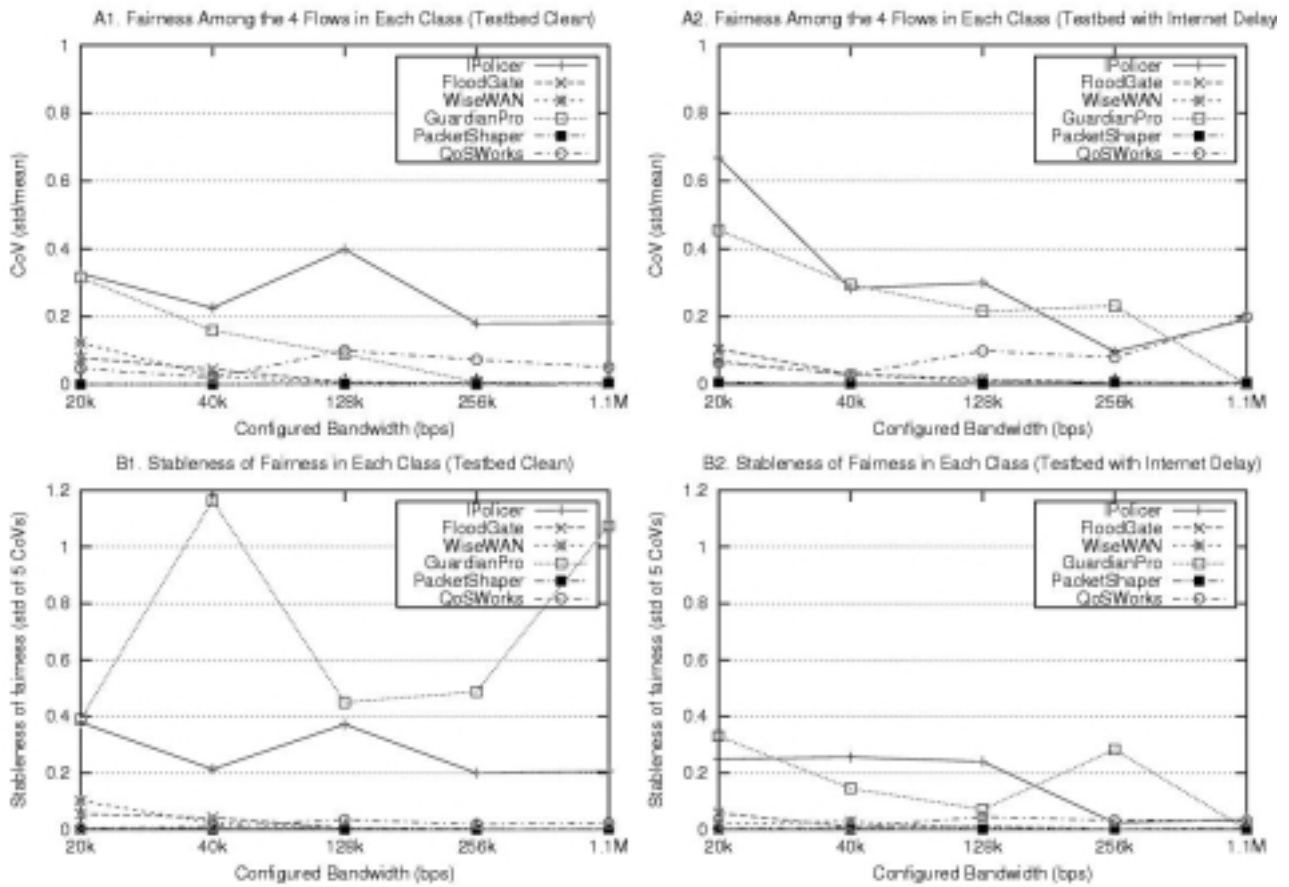


圖三、準確性及其穩定度測試結果 (A1、B1: No Internet Delay, A2、B2: With Internet Delay)

- 「公平性」與「公平性的穩定度」

圖四 (A1 為公平性, B1 為其穩定度, A2 與 B2 在穩固性測試中探討) 的測試結果可以讓我們分出兩群: PacketShaper、FloodGate、WiseWAN、QoSWorks 公平性較佳、

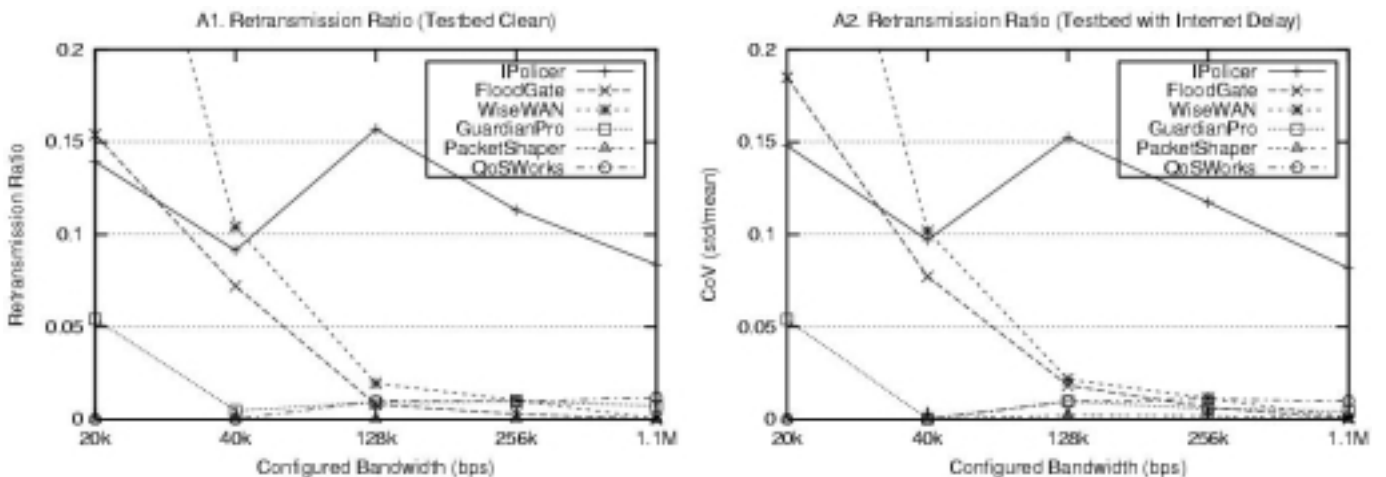
較穩定；IPolicer 與 GuardianPro 則較為遜色。



圖四、公平性及其穩定度測試結果 (A1、B1 : No Internet Delay, A2、B2: With Internet Delay)

- **重傳率**：各 class 中封包重傳率。

於圖五 (A1) 中可見在小頻寬 (20~40kbps) 的群組中除 Packeteer、QoSWorks 外皆有可察覺的封包遺失率，尤其是 WiseWAN、IPolicer 與 FloodGate。FloodGate 的技術正是利用「強迫封包遺失」來控制，WiseWAN 有可能是在 Cisco router 端就發生 packet loss 了，導致 WiseWAN 在其後也無法控制；IPolicer 的結果若以其宣稱的技術來說是較不容易理解的。



圖五、重傳率測試結果（A1：No Internet Delay，A2: With Internet Delay）

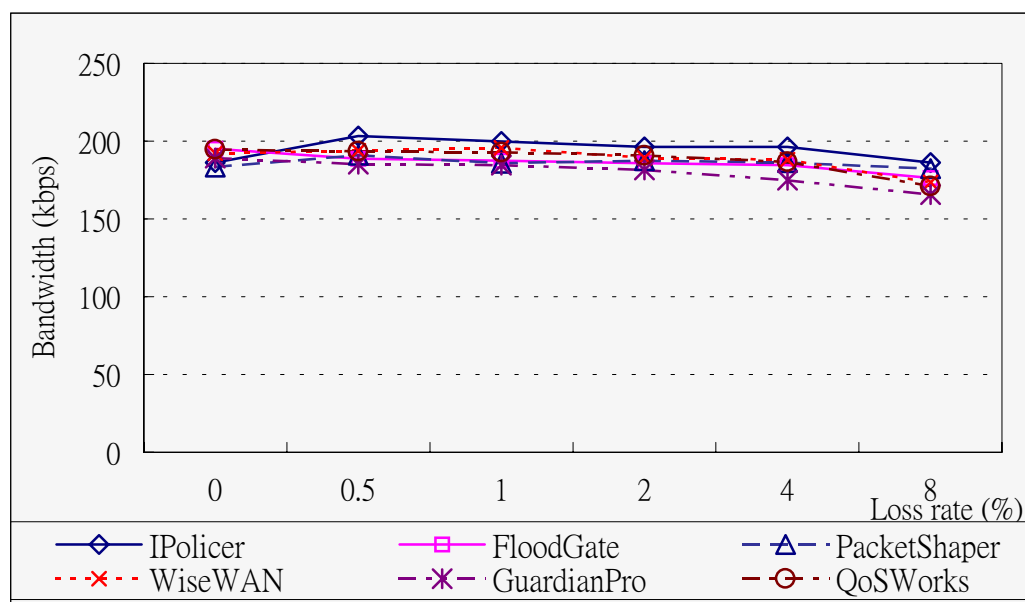
## B. 穩固性測試（Robustness Test）

### B-1. 連線遠近不同時

為方便與 Basic Test 比較，本測試項結果與 Basic Test 並列。圖二(A2)(B2)、圖三(A2)(B2)、圖四(A2)分別展示了在不同 Internet 延遲下 Basic Test 各項的結果。從中得知大部分結果並無和 Basic Test 有太大差別。IPolicer 似乎在有 Internet Delay 時會較不公平；Guardian Pro 沒有控制群組內各連線頻寬的能力，表現較差的穩定度，甚至在公平性上有 Internet Delay 時還比較公平。QoSWorks 則在高頻寬的設定（1.1Mbps）下會因連線遠近不同而有不公平的表現。

### B-2. 封包遺失率不同時

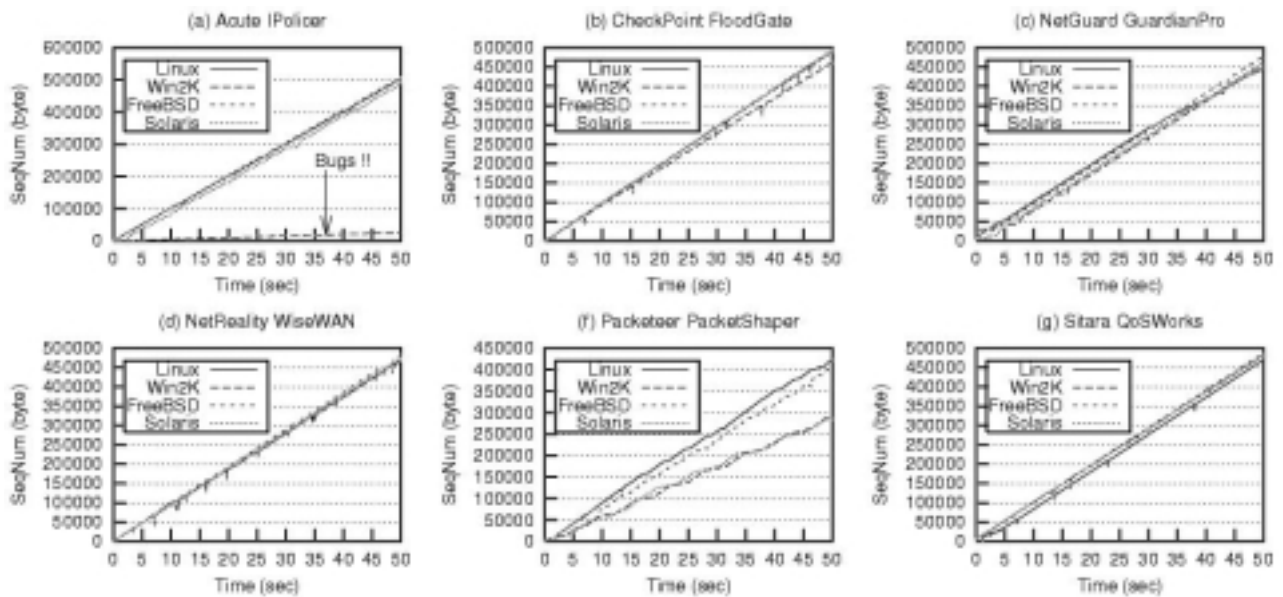
單一 TCP flow 在封包遺失時應會調慢流速以因應網路擁塞。圖六展示了各待測物在 200kbps 下不同 Internet 封包遺失率時的效能（200 秒內的平均 goodput）。幾乎每一待測物都很平順地因 packet loss rate 遞增而降低 goodput。



圖六、穩固性測試：各種封包遺失率下頻寬使用率（重傳不計）

## B-3. 送端作業系統不同時

在此相容性測試（見圖七，X 軸為時間，Y 軸為送出的 byte 數，斜率即為頻寬）中可以看到，在 80kbps、50ms 的 delay、1% 的 periodic loss rate 下，PacketShaper 會因送端作業系統不同而有差別待遇；IPolicer 在由 Windows 2000 傳給 Linux 2.2.14 時會有嚴重的 bug。測試人員利用 tcpdump 得知，TCP ack 的表頭長度經過 IPolicer 後會算錯，導致於不能正確的觸發送端送出資料；其他產品大致上皆可對不同 OS 的 TCP 送端一視同仁。



圖七、穩固性測試：送端作業系統不同時

## C. 進階效能測試 (Advanced Test)

### C-1. 頻寬互借測試

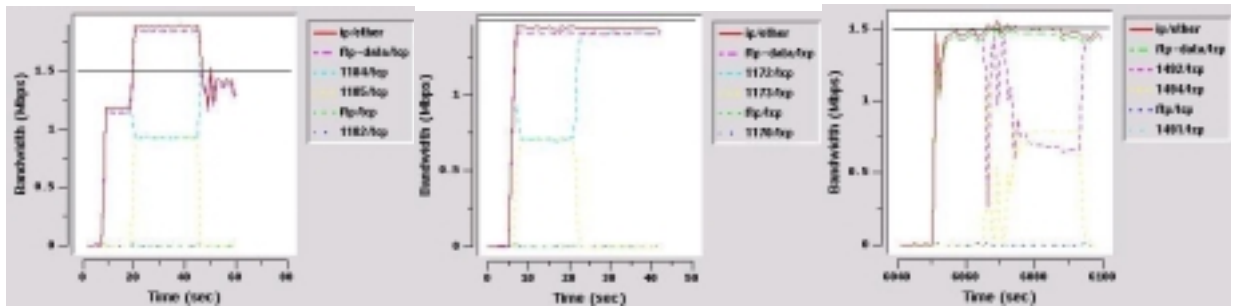
本測試結果以 ttt 觀測到的畫面來展示。每張圖我們只關心三條線的消長情況：總頻寬線 (ip/ether 頻寬線)、連線一的頻寬線 (xxxx/tcp)、連線二的頻寬線 (yyyy/tcp)。測試人員並在頻寬上界 (1.544Mbps) 處畫上線以方便觀察。

#### ● 群組間頻寬互借 (Inter-Class Bandwidth Borrowing)

圖八是「群組間」頻寬互借測試結果，IPolicer 並無此設定，因此我們將其兩個 class 上限設為總頻寬 (1.544Mbps)，然而由於 Cisco Router 的 clock rate 設為 2Mbps (因為無 T1 的 clock rate)，因此 IPolicer 超用頻寬；在其中一 connection 離去後，頻寬收斂到 1.5Mbps，但



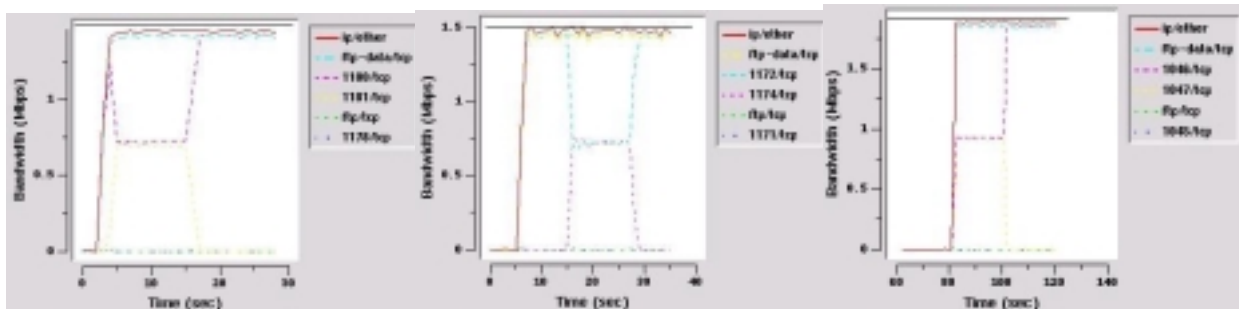
頻寬線稍微不穩定。WiseWAN 可設定為群組間「自動」互借頻寬，另四者皆有「群組間」頻寬互借設定，其中 GuardianPro 在第二個 connection 起來時 Class 間均分頻寬的情況很混沌，不過至少可用滿全部 1.5Mbps；FloodGate、PacketShaper、QoSWorks 則表現優異。



(a) Acute/Broadweb IPolicer

(b) CheckPoing FloodGate

(c) NetGuard GuardianPro



(d) Packeteer PacketShaper

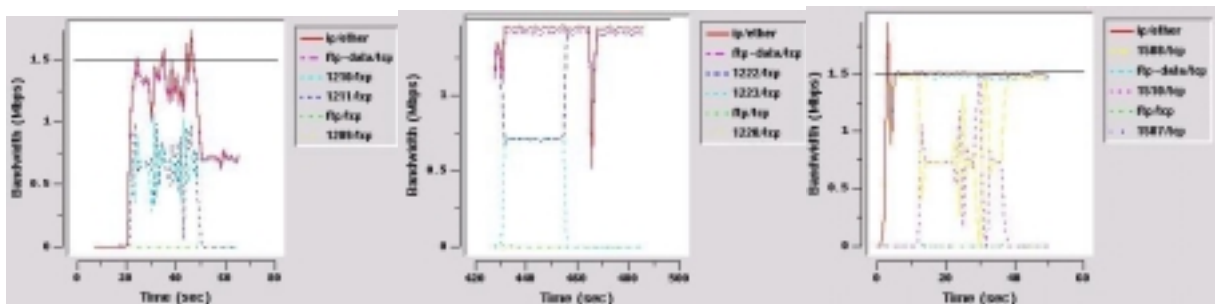
(e) Sitara QoSWorks

(f) NetReality WiseWAN

圖八、頻寬互借測試：群組間互借

● 群組內「保證頻寬的連線間」頻寬互借 (Intra-Class Bandwidth Borrowing)

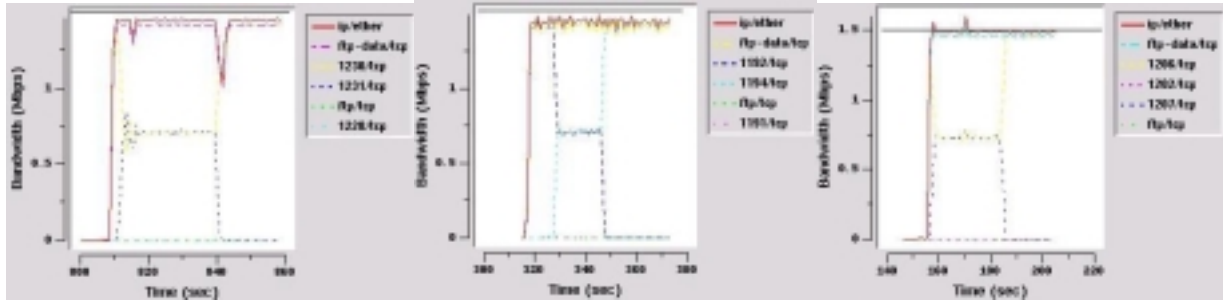
圖九是群組內「保證頻寬的連線間」頻寬互借測試結果，其中 IPolicer 無法設定互借，所以在一 connection 離去後另一 connection 無法用滿整個群組的頻寬。GuardianPro 在頻寬均分時雖有混沌的情況，總頻寬仍能用滿。其他四者結果大致相同，除 PacketShaper 與 FloodGate 總頻寬有點缺口，並沒有重大的差別。



(a) Acute/Broadweb IPolicer

(b) CheckPoing FloodGate

(c) NetGuard GuardianPro



(d) Packeteer PacketShaper      (e) Sitara QoSWorks      (f) NetReality WiseWAN

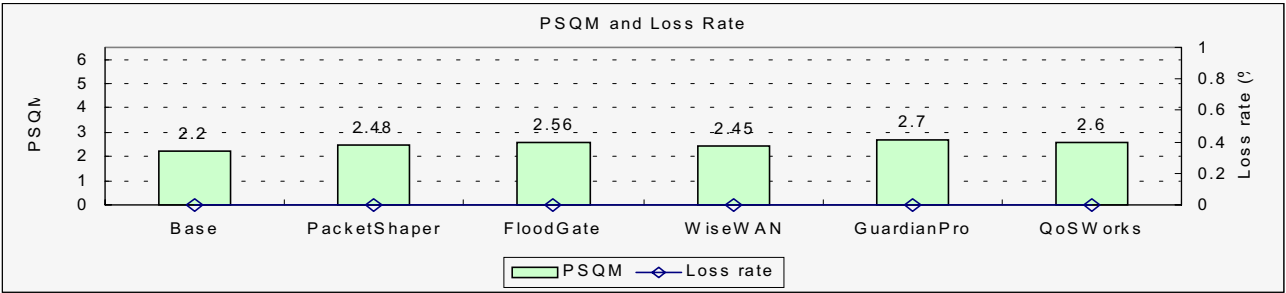
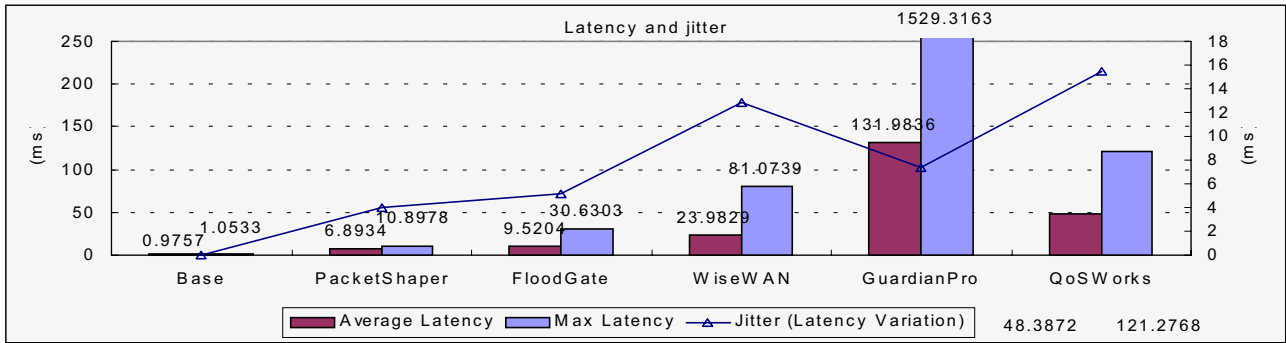
圖九、頻寬互借測試：群組內保證頻寬連線間互借

### C-3. VoIP 通話品質測試

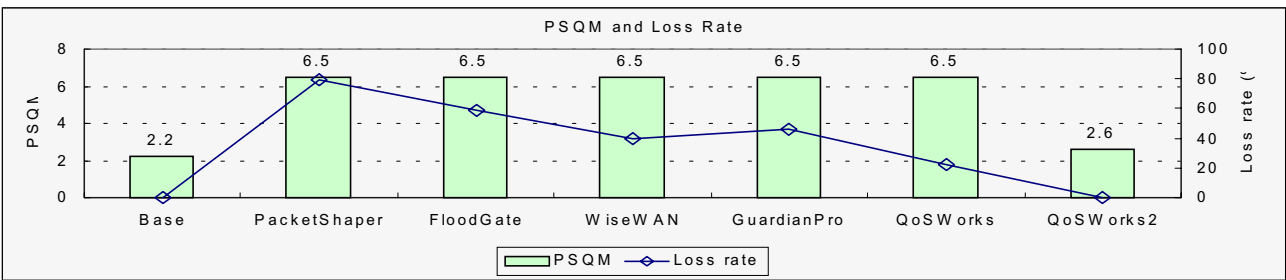
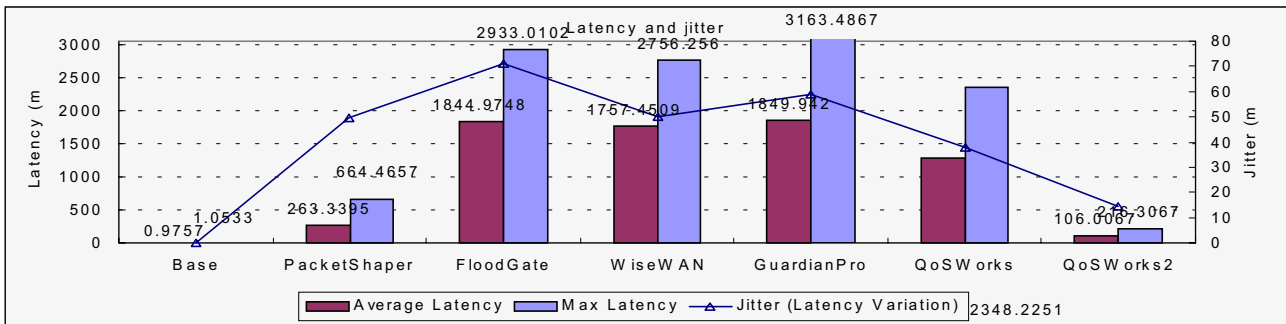
在此測試中由於 IPolicer 借測版本尚不支援 UDP 頻寬控制，因此不加入測試。

#### ● Smartbits 測試結果

由圖十(a)可得知在高頻寬下，雖在 latency 與 jitter 方面各廠商互有消長，但以通話品質 (PSQM) 為考量的話並沒有太大差別；以 VoIP Gateway (見表八(a)) 做主觀的評比亦有相同的結論，足見在高頻寬下 G.729 的頻寬尚可輕易控制；但是在低頻寬的專線下，除了 Packeteer 可勉強聽得懂在講什麼外，都辨認不出聲音。不過 QoSWorks 經過其 Packet Size Optimization(縮小 FTP 連線的 packet size)後效果達到最佳(由圖十(b)與表八(b)的 QoSWorks2 數據)，顯見其在 Voice traffic 控制的用心。然而縮小其他資料流的 packet size 會造成較大的 overhead (同樣的貨物量用幾台小車搬運的 overhead 比用一台大車搬運時還要大)，此點則需要企業自己取捨了。



(a) 專線頻寬 (Cisco Router 間) 為 T1 (1.544Mbps) 時



(b) 專線頻寬 (Cisco Router 間) 為 125kbps 時

註：Base 為在 Testbed 只有 Voice Traffic、無待測物下測得的數據，因 G.729 Codec 為失真壓縮，因此雖 jitter、loss 都極小，PSQM 至少會 2.2。

圖十、SmartBits VoIP 測試結果

## ● VoIP Gateway 測試結果

	撥通時間	延遲時間 (人耳估計)	通話品質
Baseline (僅 voice)	約 0.2 秒	極小 (< 0.1 秒)	極佳
Baseline (FTP 背景)	無法撥通		
IPolicer	無法測試 (借測版本無法控制 UDP 頻寬)		
FloodGate	約 0.5 秒	極小 (< 0.1 秒)	極佳
Guardian Pro	約 0.5 秒	極小 (< 0.1 秒)	極佳
WiseWAN	約 0.5 秒	極小 (< 0.1 秒)	極佳
PacketShaper	約 0.5 秒	極小 (< 0.1 秒)	極佳
QoSWorks	約 1 秒	極小 (< 0.1 秒)	極佳

(a) 專線頻寬 (Cisco Router 間) 為 T1 (1.544Mbps) 時

	撥通時間	延遲時間 (人耳估計)	通話品質
Baseline (僅 voice)	<1 秒	極小	極佳
Baseline (FTP 背景)	無法撥通		
IPolicer	無法測試 (借測版本無法控制 UDP 頻寬)		
FloodGate	7 秒	約 1 秒	差 (分辨不出)
Guardian Pro	3 秒	1 秒多	極差 (幾乎聽不到)
WiseWAN	7 秒	1 秒半	極差 (幾乎聽不到)
PacketShaper	1 秒	約 1 秒	普通 (偶爾斷音)
QoSWorks	17 秒	約 1 秒	差 (分辨不出)
QoSWorks (optimized)	6 秒	極小 (< 0.2 秒)	極佳

(b) 專線頻寬 (Cisco Router 間) 為 125kbps 時

表八、VoIP Gateway 測試

## 5. 結論

綜觀國外的頻寬管理器測試報告 (如 Tolly Group)，商業「服務」性質味道多很濃厚，除了測試環境單調無聊以外，探討的議題也比較淺顯，甚至只測試極少量的連線數。在本學術研究單位所做的測試，測試環境儘量符合實際狀況 (多連線滿載下測試、加入 Internet 的 delay 與 loss 變因、不同 TCP 實作的變因)，探究的議題鞭辟入裡，並站在一個公正的角度，嚴格地檢視每項產品。當然，每個產品都有其取向，價格的考量亦是不可忽略的因素，希望此次評鑑的結果可讓讀者判斷最適用的產品。

### ● 功能與效能評分表

產品 \ 功能面	安裝簡易度	管理簡易度	協定支援度	功能完整性
IPolicer	★★★	★★★★	★★★	★
FloodGate	★★★★★	★★★★★	★★★★★	★★★★★
GuardianPro	★★	★★★	★★★	★★★
WiseWAN	★★★★★	★★★★★	★★★★★	★★★★★
QoSWorks	★★★★★	★★★★★	★★★	★★★★★
PacketShaper	★★★★★	★★★★★	★★★★★	★★★★★

產品 \ 效能面	Basic Test			Robustness Test			BW Borrow		VoIP Test	
	準確性	公平性	穩定度	連線遠近	封包遺失	送端 OS	群組間	群組內	SmartVoIpQoS	Gateway
IPolicer	★★★	★★★	★★	★★★	★★★★★	★	N/A		N/A	
FloodGate	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★	★★★
GuardianPro	★★★	★★	★	★★★	★★★★★	★★★★★	★★★	★★★	★★	★★
WiseWAN	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★	★★
QoSWorks	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
PacketShaper	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★	★★★★★	★★★★★	★★★★★	★★★★★

- 最花時間的事

測試人員花很多時間在(a)將全部機器共存於一套測試平台、(b)找出公平的測試方式與參數設定、(c)撰寫測試程式。其中(a)部分在 NetGuard Guardian Pro 設定上最辛苦，原因是當時與廠商認知有差距，以為其一定得和 firewall 及 NAT 的部分一併設定；在(b)部分要找出合理、公平的參數來測試每台機器需要花很多很多時間在設定、微調各機器，其中 Sitara、IPolicer、WiseWAN 的系統有時候會當機（無法 access 到管理器）；在(c)部分由於沒有專門測試頻寬管理器的軟體套件，因此徒手撰寫許多 awk script 來計算各種數據。

- 最感興趣的事

這次所有待測物都以 Intel 為平台，每台機器拆開來確認硬體規格時，也發現裡面真的不過是台迷你型的 PC（甚至以硬碟來開機），但是價格差異可以到如此大，讓人不禁感到其內含軟體的價值。台灣過去長期在製造業表現亮麗，在現今產業轉型的時候，如何快速切入市場將非常重要。我們對未來增進台灣廠商內嵌式軟體（software in the black box）感到非常有興趣，希望能幫助台灣廠商在下一波資訊市場上依然獨占鰲頭。

我們感謝各廠商支援借測，以及網路通訊雜誌的溝通協調。

## 6. References

- 廠商網站

Acute IPolicer/	普邦： <a href="http://www.acutecomm.com">http://www.acutecomm.com</a>
BroadWeb BandKeeper	威播： <a href="http://www.broadweb.com.tw">http://www.broadweb.com.tw</a>
CheckPoint FloodGate	<a href="http://www.checkpoint.com">http://www.checkpoint.com</a>
NetGuard GuardianPro	<a href="http://www.netguard.com">http://www.netguard.com</a>
NetReality WiseWAN	<a href="http://www.net-reality.com">http://www.net-reality.com</a>
Packeteer PacketShaper	<a href="http://www.packeteer.com">http://www.packeteer.com</a>
Sitara QoSWorks	<a href="http://www.sitaranetwork.com">http://www.sitaranetwork.com</a>
Tolly Group	<a href="http://www.tolly.com">http://www.tolly.com</a>

- 測試工具網站

ncftpput	<a href="http://www.ncftp.com">http://www.ncftp.com</a>
tft	<a href="http://www.csl.sony.co.jp/~kjc">http://www.csl.sony.co.jp/~kjc</a>
SmartVoIPQoS	<a href="http://www.netcomsystems.com">http://www.netcomsystems.com</a>
tcpdump	<a href="http://www-nrg.ee.lbl.gov">http://www-nrg.ee.lbl.gov</a>

## Packeteer PacketShaper 回應

在此次測試中,交通大學所使用的 PacketShaper 軟體版本為 4.1.2 版,機種為 PacketShaper 4500 (可控管到 45MB 頻寬), Packeteer 公司 PacketShaper 頻寬管理器目前最高機種為 PacketShaper 6500 (可控管 100MB 頻寬),最新版本為 5.0,基本上可控管的協定種類及頻寬都比此次測試的機種高階. Packeteer 公司爲了讓企業用戶及 ISP/IDC/ASP/SSP 客戶可依企業不同需求有不同的使用方式,並另有擴充模組 LAN Expansion Module ,可讓您使用在 PacketShaper 2500 以上機種,讓您可輕鬆擴充 PacketShaper 頻寬管理器的網路埠,降低您的購置成本。還可選購 PolicyCenter ,讓您在同一畫面同時控管多台頻寬管理器,並透過 ReportCenter 將所有 PacketShaper 頻寬管理器的報表集中,方便管理及分析工作進行。

- 各種等級價格 Range : \$ 150,000 ~ \$ 1,700,000

## CheckPoint FloodGate 回應

從上次防火牆測試到這次的頻寬管理軟硬體測試中可以發現,林教授帶領的測試團隊不論在測試項目、內容、相關流程各方面都相當用心,超越國外專業測試實驗室的水準;由這

次頻寬管理的測試結果來看，精誠資訊所代理的防火牆產品 Check Point 在本次頻寬管理的測試結果中頗受肯定，其中資料傳輸效能方面，在穩定性、精確度的評價極佳，整體 Check Point 頻寬管理軟體效能已可與一般硬體媲美；更值得一提的是，在「人性化管理介面」的表現亮麗，顯示防火牆大廠 Check Point 在頻寬管理軟體上的功能也相當優異。

- 各種等級價格 Range：\$ 130,200～\$ 824,250

## NetReality WiseWAN 回應

在本次測試結果中，再次證明了 WiseWan 的確是眾多頻寬管理設備中的佼佼者，儘管我們未提供最大型號的平台參與測試，但 WiseWan 201 與其他競爭對手最大型號的設備比較後還是表現不俗。唯在本次的測試環境中，因為測試單位所能提供的環境有限，並未能展現出 WiseWan 在 WAN 線路上的獨特功能(Frame-Relay)以及多部 WiseWan 設備集中管理的能力。WiseWan V4.x 的 WanXplorer Server 中採用了 Sybase 關聯式資料庫需要較長的安裝時間，但在 WiseWan V5.0 中已大幅縮減整體所需的安裝時間。使用關聯式資料庫來存放歷史流量資料可存放較長期的歷史資料以及便於與其他計費或報表系統整合。

WiseWan 不只是一個頻寬管理設備，更是一套網管系統。它可以偵測到廣域網路第二層以上信號，將各條線路狀況呈現於管理介面，更備有告警及郵件通知的功能，是一套不錯的網管系統。

- 各種等級價格 Range：128k～52M 價格 \$ 200,000～\$ 1,320,000

## Sitara QoSWorks 回應

我們很高興網路通訊雜誌，邀請聚碩科技代理的 Sitara Network QoSWorks 參加 QoS 產品測試。Sitara QoSWorks 提供了具備擴充性，簡易管理和備援性的完整企業 Intranet 和 Internet QoS 解決方案。QoSWorks 整合了多種 QoS 的機制，諸如 TCP rate shaping 和 Class Based Queuing(CBQ)、Web Cache 等，提供了絕佳網路 QoS 服務功能。不論是 64 kbps 的低速專線或是 155 Mbps ISP 級的連線頻寬，QoSWorks 都提供了相對應的產品。此外，在此次的測試中，證明了 Sitara QoSWorks 不只是對於一般企業網路應用可提供良好的 QoS 機制，對於 VoIP 品質的控制和加強，更是領先其他同業。QoSWorks 是你企業建立網路 QoS 的好夥伴！

- 各種等級價格 Range：64k～1G 價格 \$ 150,000～\$ 4,500,000



## Acute IPolicer/Broadweb BandKeeper 回應

首先，對於交大測試中心長達一個多月的辛苦測試，本公司給予高度的肯定，也對雜誌社的居中協調、規劃深表感謝。由於內部作業疏失，以致送測機器為公司內部開發測試之舊版對照平台，並非一般正式出貨之機種。因此部分功能無法在此次測試中充分展現(如 Fail Over、Set WAN Speed、UDP Traffic Control、VoIP Traffic Control....)，以致影響本產品之整體表現。雖經協調欲以一般出貨機種重新送測，唯新增的測試時程將影響測試報告正式付梓的時間，因此在本次測試報告中刊載之測試結果仍以舊資料為主，並不代表本公司一般產品之測試，未來讀者可以在本公司網站取得其他測試單位(如 Tolly Group)之測試報告。

## NetGuard Guardian Pro 回應

GuardianPro 的頻寬管理是在 GuardianPro 企業安全整合性的解決方案的其中一個主要功能，其整合解決方案不僅包含了防火牆 Firewall、頻寬管理 QoS、虛擬私人網路 VPN、網路轉址 NAT、即時監控 RPM、使用者認證 Authentication，QoS 頻寬管理功能更可以獨立出來作為選購產品，其安全整合方案不但可以為企業節省大量的管理成本，並且在全中文化及操作便利的 GUI 管理介面等各項優點中，能夠讓您對於企業網路狀況瞭若指掌。

本次測試中，在眾多的頻寬管理產品裡，Netguard GuardianPro 是以「對象」的角度來切入管理，所以在管理上和其他產品思考邏輯稍有不同，但是您如果親身使用會發現其實這種管理模式絕對會是一種最人性化的操作介面！

- 各種等級價格 Range：128K~10M 價錢為 \$ 146,520~ \$ 664,520

## 測試單位補充說明：

本次測試過程所花時間多了將近一個月，從邀請到測試報告定稿總計達 2.5 月，取得機器的過程花費超過一個月，加上現有測試工具無法完全符合需要，因此自行撰寫測試工具，測試初稿完成後邀請廠商至測試中心觀看測試平台以及確認結果。經過過去半年多來幾次產品測試報告後，已經完全能夠掌握測試過程中需要謹慎小心的環節，但仍有意想不到的插曲，將來測試規則應該會訂得更清楚。

本次測試初期，威播科技 (BroadWeb) 曾要求更換第二台機器測試，經測試人員反覆測試後發現測試結果與原機差異不大，因而撰寫測試報告初稿給各廠商審閱；審閱過後威播提出更換成第三台機器重測的要求，經其他廠商反對，以及基於公平原則，雜誌社與本測試單位不考慮在測試報告完整初稿付梓後再更換機器。為此本雜誌社與測試單位深感困擾，也感到歉意，但是公平性的原則我們仍須顧及。

本測試報告所揭露出來的現象皆是可以在原機器上重新產生的，在截稿前也曾邀請各廠商前來確認數據。我們希望本報告會促使各廠商更努力讓產品更好，也作為採購單位的參考，唯未來在選購時請以各廠商新版功能與效能為依據。