行政院國家科學委員會專題研究計畫　成果報告

子計畫三：NBEN 中區網路安全建置與回復規劃

計畫類別：整合型計畫
計畫編號：NSC92-2219-E-009-002-
執行期間：92 年 05 月 01 日至 93 年 04 月 30 日
執行單位：國立交通大學資訊工程學系

計畫主持人：謝續平
共同主持人：曾黎明，孫宏民
計畫參與人員：協同主持人:王晉良 教授，顏嵩銘 教授，陳奕明 副教授，周立德副教授； 協同研究人員:楊明豪,賴守全

報告類型：完整報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 6 月 8 日

行政院國家科學委員會補助專題研究計畫☑ 成 果 報 告 □期中進度報告

國家寬頻實驗網路(NBEN)網路安全建置與實驗計畫

子計畫三：NBEN 中區網路安全中心建置與回復中心規劃

計畫類別：□ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC　92－2219－E－009－002
執行期間：　92 年 05 月 01 日至 92 年 04 月 30 日

計畫主持人：　謝續平　教授
共同主持人：　曾黎明　教授，孫宏明　副教授
協同主持人：　王晉良　教授，顏嵩銘　教授，陳奕明　副教授，周立德副教授
協同研究人員：楊明豪，賴守全

成果報告類型(依經費核定清單規定繳交)：□精簡報告　☑完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學資訊工程學系暨研究所
國立中央大學資訊工程學系暨研究所
國立清華大學資訊工程學系暨研究所
中　華　民　國　93　年　6　月　7　日

摘要

隨著網際網路(Internet) 技術的迅速發展，電腦主機透過網際網路連結在一起，資訊的傳遞越來越依賴網路，以求得最高之處理效率；但是伴隨著網路的大量使用而產生的網路安全問題也日趨嚴重。網路通訊應用於資訊安全領域也是必然的趨勢。以網際網路連結資訊網路，能獲得更迅速、更有效的通訊。

以往的網際網路技術發展，只求能夠成功的進行資料傳輸的工作，當時有關網路安全方面的問題還未受到如此的重視。但是隨著網際網路的日漸龐大與複雜，今日的網路入侵攻擊事件時有所聞，任何人稍不留心都有可能遭受入侵攻擊，尤其是分散式阻絕服務攻擊(Distributed Denial of Service, DDoS)更是難以預防的。本子計畫目的，在研究網路攻擊行為，分析入侵偵測相關技術，並建立一個分散式阻絕服務攻擊的測試平台，能偵測攻擊，並回復攻擊前狀態之機制。我們成功的建立了一套封閉式的分散式阻絕服務攻擊測試平台，並在其上發展了一套網路式入侵預防偵測系統(Network-based Intrusion prevention system, NIPS)。

關鍵詞：網際網路、網路入侵、分散式阻絕服務攻擊

Abstract

As the development of the Internet, the propagation of the information and the communication is much more boundless, make our life more convenient. But it also has its drawback; for example, a person who has a mind to do something in bad intension can cause damage to the Internet or steal something useful from the Internet. It happens all the time presently. These dangers maybe arise from the faults of the architecture of the Internet, communication protocol, or routing protocol in itself, or the software implementation bug and the administrator's carelessness. It, therefore, facilitates the attackers' action. As the protocol, TCP/IP, maybe suffer from the DDOS attack when it implements the three-way handshaking at the moment of constructing the connection, many other protocols and the network and computers themselves are suffered from many kinds of DDoS threat. Our research topics focused on attacking behaviors on the internet, technologies and analysis of intrusion detection, and constructing a DDoS test-bed which can detect the DDoS attack and recover the victim's status. We developed a closed test-bed environment and a network-based intrusion prevention system (NIPS).

Keywords: internet, intrusion, Distributed Denial of Service (DDoS)

目錄

中文摘要 I

英文摘要 II

一、前言 1

二、研究目的 1

三、文獻探討 2

四、研究方法 3

五、攻擊手法 7

六、防禦措施… 12

七、結果與討論 19

參考文獻 20

計畫成果自評 21

前言

由於大環境的劇烈變化，現在人們不需要是電腦專家也能成為駭客，因為網際網路上有數萬個以入侵為目的的網站，提供許多簡單易用的程式與指令檔，任何人只要將它們下載，然後用滑鼠按一按就可以四處入侵別人的系統。由於這些入侵工具到處都有，幾乎已經氾濫到唾手可得的地步，因而也導致各種入侵事件層出不窮，如同野火燎原般一發不可收拾。

眾多駭客中第一批廣為世人熟知推崇的包括 Steve Wozniak、Bill Gates 與 Linus Trovalds，目前多項電腦科技都是拜他們所賜而得以蓬勃發展。他們這些早期的駭客對於科技非常狂熱，熱衷於鑽研各種技術的運作原理，矢志將程式推展發揮到淋漓盡致，並超越原來的限制。在那個時代，「駭客」這個字眼沒有任何負面意義，與今日世人的印象大不相同，可惜由於時代的變遷，原本單純以好奇與勇於接受挑戰為出發點的駭客倫理至今已蕩然無存。

早期駭客的目標與今日駭客的目標大異其趣，新世代駭客的動機似乎不再是過往的好奇心或對知識的渴望而已，而是已經變質成受到貪婪、權力、報復或其他不良企圖所驅策，將入侵當作一種遊戲或運動，並利用網際網路上俯拾即是的工具遂行其目的。

研究目的

由於阻絕服務攻擊影響網路安全事件最受人矚目之一，相關的研究持續在研發新的技術。拒絕服務攻擊根據其攻擊的手法和目的不同，有兩種不同的存在形式：一種是以消耗目標主機的可用資源為目的，使目標伺服器忙於應付大量的非法的，無用的連接請求，占用了伺服器所有的資源，造成伺服器對正常的請求無法再做出及時回應，從而形成事實上的服務中斷。這也是最常見的拒絕服務攻擊形式。這種攻擊主要利用的是網路協定或者是系統的一些特點和漏洞進行攻擊，主要的攻擊方法有 Land、Teardrop、SYN Flood、UDP Flood、ICMP Flood、Smurf 等等，針對這些漏洞的攻擊，目前在網路上都有大量成熟現成的工具可以利用，比較常見和有效的有 Trinoo、TFN、Stacheldraht、TFN2K 等；另一種拒絕服務攻擊是以消耗伺服器連線的有效頻寬為目的，比如伺服器的出口為 100M 的頻寬線路，攻擊者通過發送大量的有用或無用封包，將整條網路頻寬全部占用，從而使合法用戶請求無法通過網路到達伺服器，伺服器對部分合法請求的回應也無法返回用戶，造成服務中斷。對於這種攻擊，可以說非常難以區分和防範，它本來就是利用網路發展過程中不可避免的資源缺乏造成的矛盾進行攻擊，大量的合法請求只要湧向一個資源有限的網路系統，就可能造成服務故障，很難說這樣的行為是攻擊行為還是正常的要求。因為網路上所有的連線主機都牽動阻絕服務攻擊成功與否，分散阻絕服務攻擊讓抵禦駭客攻擊已經不是少數人才需要關注的問題。因此本計畫特別針對阻絕服務攻擊實驗，了解網路面臨衝擊與抵抗阻絕服務攻擊技術可用性。

文獻探討

DDoS 攻擊的特性是由一個或多個攻擊者(Attackers)發動攻擊，操縱許多被植入後門程式的受控者(Zombies)，發出以亂數產生或是造假的來源 IP (source IP) 的大量封包來攻擊少數的受害者(victims)，使受害者的網路連線擁塞而無法提供服務。

國際上許多的網路安全專家觀察到了 DDoS 攻擊的這些特性，也設計了許多種不同的解決方式，其中包含防堵攻擊的封包、Ingress filtering、Link testing、Logging、Pushback、ICMP Traceback、PPM(Probabilistic Packet Marking)及 DPM(Deterministic Packet Marking)… 等等方法，以下就各種防止、偵測 DDoS Attack 的方法作簡略的介紹，並且比較各種方法在真實網路上的可行性。

1. Ingress Filtering

此法是針對 Router 上對封包往外傳送的來源位址做設限，使得原本不該由某些 interface 經過的封包作過濾。Ingress Filter 的功能在較新的 router 都包含有此功能了，所以此法在實際上的實行沒有問題。此法在網路流量小而且單純的 edge router 上可以開啟，因為在 edge router 上只負責少數網域的封包，可以很清楚很快速的作檢查。但要是在流量大又負責數個網域轉傳的 router 上，此法很明顯的會讓 router 的 performance 降下來。雖然此法不會造成其他不必要的網路流量，但卻會造成效能下降，更重要的是會影響到幾個需要用到 source IP spoof 技巧才能完成的服務[1]，例如：Mobile IP。

2. Link Testing

從最接近受害者的 router 開始，一個一個的檢查所有上游的連線，直到找到其中的一個連線包含攻擊的封包。用這個方法一直往上游找，直到找到攻擊來源為止。這個方法有兩個延伸，分別為 input debugging 和 controlled flooding。這個方法的假設前題為在找到真正的攻擊者之前，這個攻擊還要持續在進行中，否則這個方法將不可能會成功。

3. Logging

[2][3]提出在重要的 router 上面記錄封包的資訊，在事後使用 data mining 的方式來得知封包經過哪些主機。雖然這個方法可以在事後判斷出攻擊者的所在，但是它所需要的資源與設備非常的龐大，而且幾乎沒有機構使用它。

4. Pushback

Pushback[6] 把所有的 traffic 分成三種類型，分別為 Good Traffic, Bad Traffic 與 Poor Traffic。當一個 router 開始丟棄 (drop) 封包的時候，代表這個 link 開始壅塞，此時就在丟棄的封包中檢查是否有攻擊的封包包含在內。當發現有可疑的封包時就找出他的上一層是由哪一部 router 送出來的，由 router 送一個控制的訊息給那一台 router 去控制這個攻擊連線的流量。但若是 router 無法精確地辨斷各個流量，其他正常的流量也很可能被影響到，這就是作者所提的 poor traffic。

5. ICMP Traceback

當攻擊發生的時候，受害者可以藉由 router 的幫忙，將封包的資訊放入一個特定格式的 ICMP 封包內，藉由 router 間的傳送，可以找出原本發出該攻擊封包的來源。但由於 ICMP 封包在網路上的功能特殊，所以通常在一個網域受到攻擊時，ICMP 封包就會被隔絕，而只要在這個路徑上有一個 router 無法參與，這個方法就會失敗(除非用更複雜的 key distribution 架構去解決它)。

6. PPM

Router 在一個固定的機率 ρ 下，把自己的 IP Address 分段放入 IP Header 中的 ID 這個欄位。這個方法把 16 bit 的 ID 欄位分成三個部份，分別為 3 bit 的 offset，8 bit 為 start 和 end 欄位，和 5 bit 的 distance 欄位。如果 router 決定在這個 packet 上面記下自己的 IP Address，它便把 distance 設為零。若這個封包的 distance 已經為零，則代表這個封包已經被 mark 過了，router 就把它的 IP Address 寫進去 end 這個欄位。而每個這個封包經過一個 router，每個 router 就幫他在 distance 這個欄位加一。

7. DPM

在封包要出所有的 edge router 的時候，都由 edge router 在 incoming interface 上面，把該 interface 的 IP Address 附在封包的 ID + Unused Bit (共 17 bit) 上面。因為只有 17 bit 的長度不夠放總長 32 bit 的 IP Address，所以將會由 router 以亂數的方式將 IP Address 的某一個部份放上。當封包到達 victim 端時，若這個攻擊連線所送的封包數足夠時，victim 端就有很大的機會重組出攻擊者的真正來源。此法包含了 Packet Marking 這種方法的特性，只需要在每個 interface 上面加上標記 IP Address 的功能即可，不需要其他的網路流量，也不需要其他的網路設備與管理。但也保有了 Packet Marking 的弱點，需要使用到 ID 這個欄位，使得 IP 封包的 fragment 功能產生不能正常運作的缺點[4]，雖然有人對此法作改進[5]，但仍無法避免這個狀況發生。另外，此法也無法在攻擊封包數非常小的情形上運作。

結論：DDoS 攻擊所造成的代價是非常大的，所以學者專家也非常致力於 DDoS 的防禦與阻絕。但常常還是需要考慮到現實面的問題，包含網路設備的能力，所需要附加阻絕 DDoS 攻擊的成本。真實的網路是由數個大的 ISP 所組成，而在各 ISP 之間的配合及實行上，是否會因為有少數的 router 沒有附加這些功能而讓這些方法有所缺陷。而開啟了這些防制 DDoS 的功能是否會造成目前所使用的網路協定無法正常運行，更是 ISP 與用戶更加關注的重點。

研究方法

本計畫是在一內部 Giga 級網路 testbed 上，以四台 PC 模擬 Router，另外六台 PC 來模擬 attacker 和 victim。實驗網路架構如下：

實驗網路架構

設備:

6 Host node:

CPU: Intel Pentium III 733MHz

RAM:128MB

Nics:Intel PILA8460M 10/100 pro family

4 Router node:

CPU:AMD Authon XP1800+

RAM:128MB

Nics: Intel Pro/1000XT Server Adapter, Intel PILA8460M 10/100 pro family

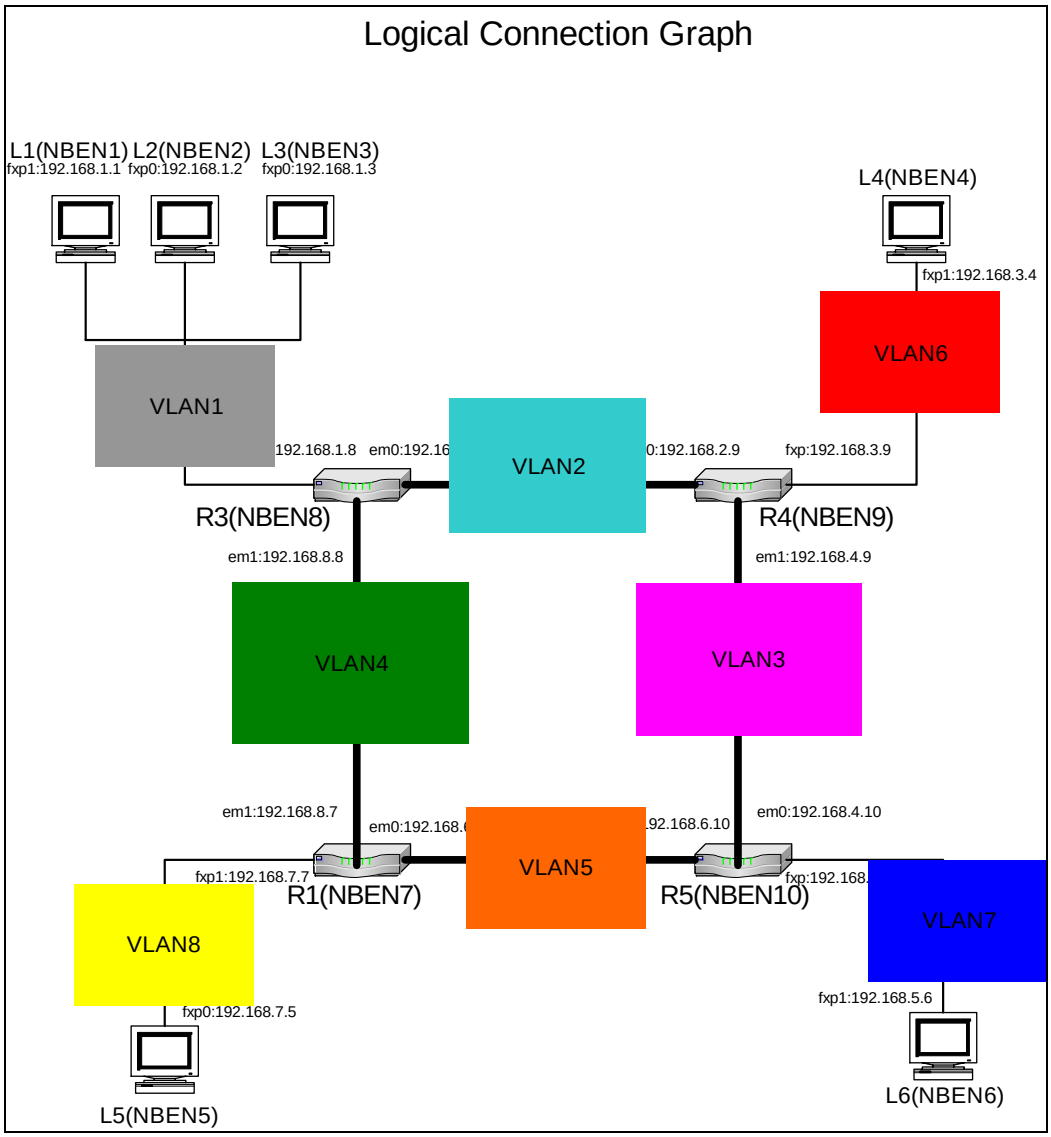
VLAN:

3Com Gigabit Switch 4900

圖三： 機櫃，GigaSwitch 等裝置設備及線路配置

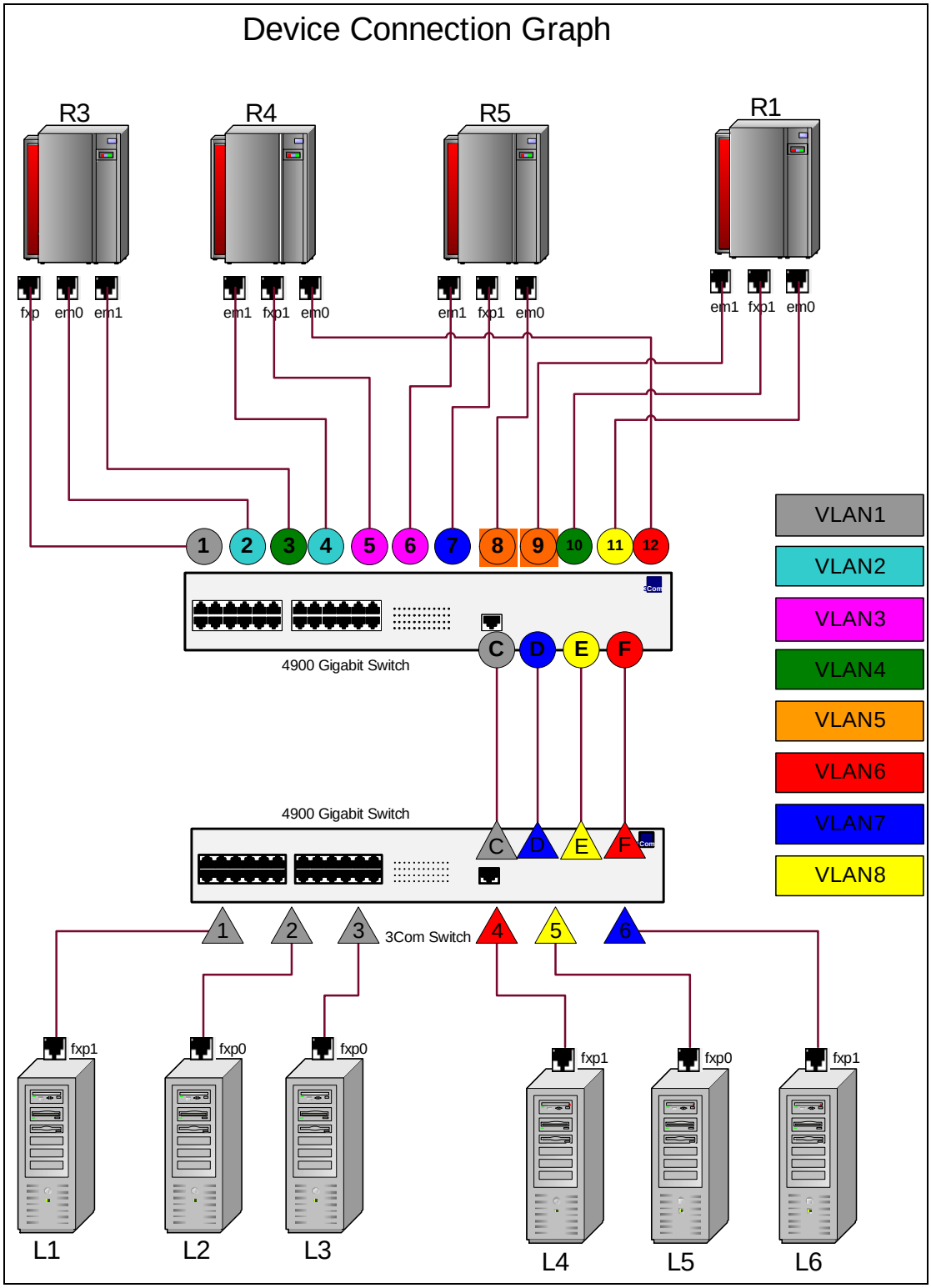
底下是我們所配置的實驗網路的架構圖，在這個架構圖中，VLAN2,VLAN3,VLAN4，VLAN5，是用來模擬 router 之間交換訊息的線路，理論上，這些線路的速度，皆可達 1Gbps，而 VLAN1,VLAN6,VLAN7,VLAN8，則各個模擬 4 個獨立的 Network，且其線路的速度也皆可達

100Mbps，若欲在上實驗者，可利用 BSD 上一些限流的機制，如 Dummy net 等，來完成並達到實驗所需的要求。



圖四：實驗網路的邏輯架構圖

底下為我們運用於實際機器配置時的示意圖，圖中的 L，R 分別代表置於左右機櫃的機器，圖中各個顏色，分別代表不同 VLAN 的配置，而圓形、三角形分別為 Switch 上面的 ethernet port，數字即為 port number。



圖五： 裝置架構設定圖

接著了解這些 device 的配置方式，底下我們將解釋闡明如何設定此系統步驟

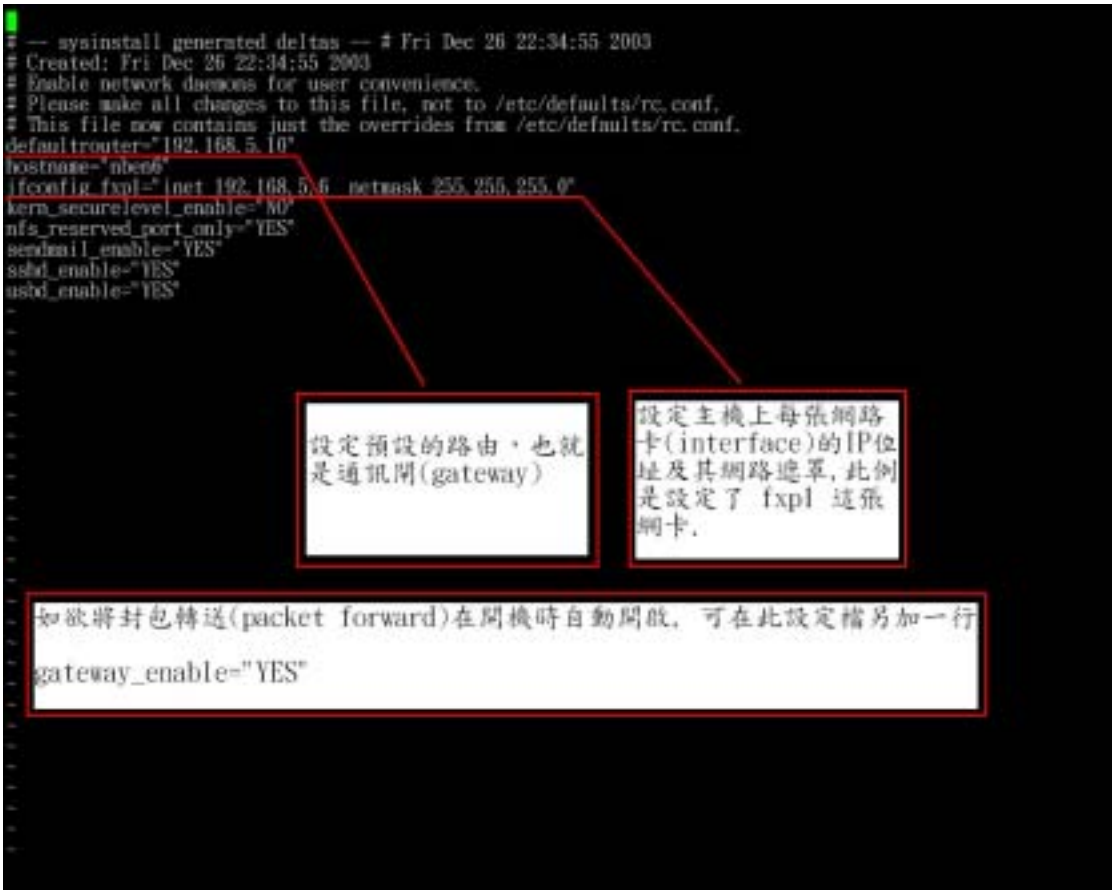
1．設定各 interface 的 ip(參考邏輯架構圖中的顯示)

```
> ifconfig fxp1 192.168.5.6 netmask 255.255.255.0
>
```

2．對於 router 設定 ipforwarding=1

```
> sysctl net.inet.ip.forwarding=1
>
```

３．對 rc.conf 修改開機自動設定的選項，如圖所示



攻擊手法

DoS 的攻擊方式有很多種，最基本的 DoS 攻擊就是利用合理的服務請求來佔用過多的服務資源，從而使合法用戶無法得到服務的回應。

DDoS 攻擊手段是在傳統的 DoS 攻擊基礎之上產生的一類攻擊方式。單一的 DoS 攻擊一般是採用一對一方式的，當攻擊目標 CPU 速度慢、記憶體小或者網路頻寬小等等各項性能指標不高它的效果是明顯的。隨著電腦與網路技術的發展，電腦的處理能力迅速增長，記憶體大大增加，同時也出現了 Giga 級的網路，這使得 DoS 攻擊的困難程度加大了－目標對惡意攻擊包的"消化能力"加強了不少，例如你的攻擊軟體每秒鐘可以發送 3,000 個攻擊包，但我的主機與網路帶寬每秒鐘可以處理 10,000 個攻擊包，這樣一來攻擊就不會產生什麼效果。

這時侯分散式的拒絕服務攻擊手段（DDoS）就應運而生了。你理解了 DoS 攻擊的話，它的原理就很簡單。如果說電腦與網路的處理能力加大了 10 倍，用一台攻擊機來攻擊不再

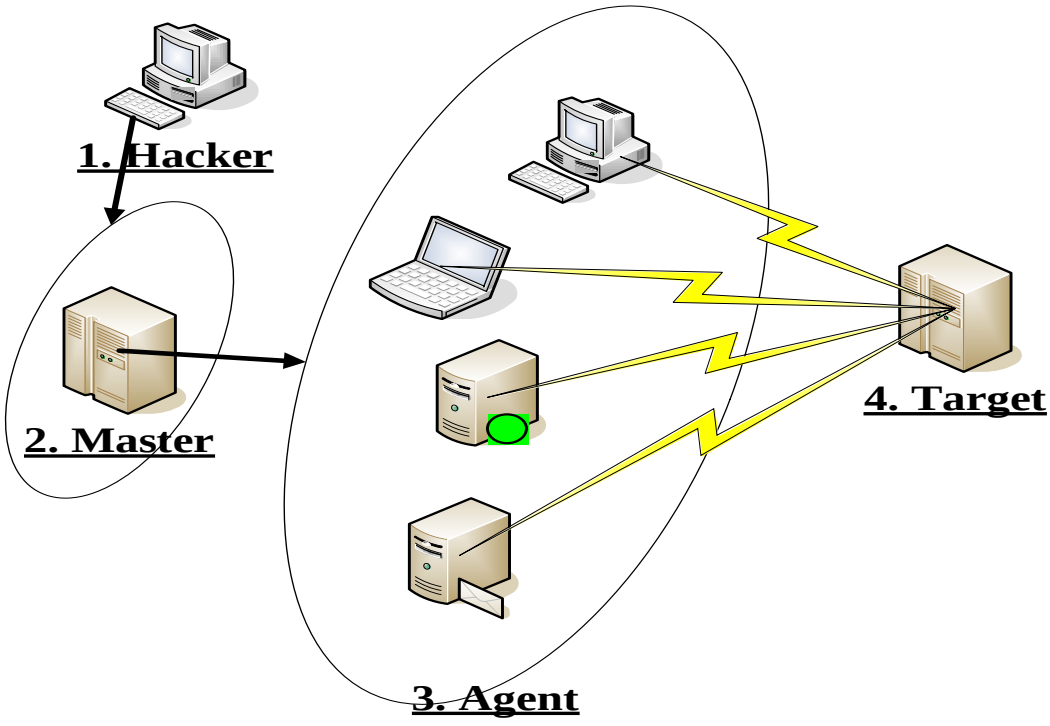
能起作用的話，攻擊者使用 10 台攻擊機同時攻擊呢？用 100 台呢？DDoS 就是利用更多的傀儡機來發起進攻，以比從前更大的規模來進攻受害者。

高速廣泛連接的網路給大家帶來了方便，也為 DDoS 攻擊創造了極為有利的條件。在低速網路時代時，駭客佔領攻擊用的傀儡機時，總是會優先考慮離目標網路距離近的機器，因為經過路由器的 hop 數少，效果好。而現在電信骨幹節點之間的連接都是以 G 為級別的，大城市之間更可以達到數 G 以上的連接，這使得攻擊可以從更遠的地方或者其他城市發起，攻擊者的傀儡機位置可以在分佈在更大的範圍，選擇起來更靈活了。

被 DDoS 攻擊時的現象

- 被攻擊主機上有大量等待的 TCP 連接
- 網路中充斥著大量的無用的資料封包，來源位址為假造
- 製造高流量無用資料，造成網路擁塞，使受害主機無法正常和外界通訊
- 利用受害主機提供的服務或傳輸協定上的缺陷，反復高速的發出特定的服務請求，使受害主機無法及時處理所有正常請求
- 嚴重時會造成系統當機

攻擊運行原理



圖一： DDoS 攻擊原理架構

如圖，一個比較完善的 DDoS 攻擊體系分成四大部分，先來看一下最重要的第 2 和第 3 部分：它們分別用做控制和實際發起攻擊。請注意控制機與攻擊機的區別，對第 4 部分的受害者來說，DDoS 的實際攻擊包是從第 3 部分攻擊機上發出的，第 2 部分的控制機只發佈

命令而不參與實際的攻擊。對第 2 和第 3 部分電腦，駭客有控制權或者是部分的控制權，並把相應的 DDoS 程式上傳到這些平臺上，這些程式與正常的程式一樣運行並等待來自駭客的指令，通常它還會利用各種手段隱藏自己不被別人發現。在平時，這些機器並沒有什麼異常，只是一旦駭客連接到它們進行控制，並發出指令的時候，攻擊機就成為害人者去發起攻擊了。

駭客是如何組織一次 DDoS 攻擊的？

這裏用“ 組織 ”這個詞，是因為 DDoS 並不像入侵一台主機那樣簡單。一般來說，駭客進行 DDoS 攻擊時會經過這樣的步驟：

1．搜集瞭解目標的情況
下列情況是駭客非常關心的情報：

- 被攻擊目標主機數目、位址情況
- 目標主機的配置、性能
- 目標的頻寬

對於 DDoS 攻擊者來說，攻擊網際網路上的某個站點，如 http://www.mytarget.com，有一個重點就是確定到底有多少台主機在支援這個站點，一個大的網站可能有很多台主機利用負載均衡技術提供同一個網站的 www 服務。所以事先搜集情報對 DDoS 攻擊者來說是非常重要的，這關係到使用多少台傀儡機才能達到效果的問題。簡單地考慮一下，在相同的條件下，攻擊同一站點的 2 台主機需要 2 台攻擊機的話，攻擊 5 台主機可能就需要 5 台以上的攻擊機。反正不管你有多少台主機我都用儘量多的攻擊機來攻就是了，攻擊機超過了時效果更好。

但在實際過程中，有很多駭客並不進行情報的搜集而直接進行 DDoS 的攻擊，這時候攻擊的盲目性就很大了，效果如何也要靠運氣。

2．佔領攻擊機
駭客最感興趣的是有下列情況的主機：

- 網路狀態好的主機
- 性能好的主機
- 安全管理水準差的主機

這一部分實際上是使用了另一大類的攻擊手段：利用型攻擊。這是和 DDoS 並列的攻擊方式。簡單地說，就是佔領和控制被攻擊的主機。取得最高的管理許可權，或者至少得到一個有許可權完成 DDoS 攻擊任務的帳號。對於一個 DDoS 攻擊者來說，準備好一定數量的攻擊機是一個必要的條件，下面說一下他是如何攻擊並佔領它們的。

首先，駭客做的工作一般是掃描，隨機地或者是有針對性地利用掃描器去發現網際網路上那些有漏洞的機器，像程式的溢出漏洞、cgi、Unicode、ftp、資料庫漏洞.....，都

是駭客希望看到的掃描結果。隨後就是嘗試入侵了。

總之駭客現在佔領了一台攻擊機了！然後除了上面說過留後門擦腳印這些基本工作之外，他會把 DDoS 攻擊用的程式上載過去，一般是利用 ftp。在攻擊機上，會有一個 DDoS 的攻擊程式，駭客就是利用它來向受害目標發送惡意攻擊封包。

3．實際攻擊

經過前 2 個階段的精心準備之後，駭客就開始瞄準目標準備攻擊。前面的準備做得好的話，實際攻擊過程反而是比較簡單的。就像圖示裡的那樣，駭客登入到做為控制臺的傀儡機，向所有的攻擊機發出命令。這時候埋伏在攻擊機中的 DDoS 攻擊程式就會回應控制臺的命令，一起向受害主機以高速度發送大量的封包，導致它當機或是無法回應正常的請求。駭客一般會以遠遠超出受害方處理能力的速度進行攻擊。

老到的攻擊者一邊攻擊，還會用各種手段來監視攻擊的效果，在需要的時候進行一些調整。簡單些就是開個視窗不斷地 ping 目標主機，在能接到回應的時候就再加大一些流量或是再命令更多的傀儡機來加入攻擊。

在攻擊程式的準備上，大都是改良或小部分修改網路已知的攻擊程式。這些程式大多透過使用大量的資料流、不規則的封包大小、蓄意的協定違反，阻礙主要設備等方式，使網路無法正常的運作。如針對受害者主機、應用緩衝器氾濫及其他技術而導致封包超過頻寬。

我們攻擊的程式大概可以分成下面幾類:

(1)利用流量暴增式的攻擊：

- 例如：smurf 攻擊：直接對網路進行廣播，造成網路很快地充滿垃圾封包而中斷。smurf 會不斷地將小量偽造的 icmp 要求封包送給任意 IP 位址，或是 IP 廣播位址（IP broadcast address），然後廣播位址會傳回大量的 icmp 回應封包給目標主機。這種 smurf 的攻擊方式除了攻擊特定目標主機，也能在網路上塞滿 icmp 的要求封包與回應封包而造成網路中斷，所以常被稱為 smurf 倍增型攻擊。
  程式範例：smurf

- icmp 攻擊：將大量『偽造來源位址』的 icmp 要求封包送給目標主機，目標主機會回應等量的 icmp 回應封包而造成目標主機無法負荷而當機。
  程式範例： inetddos

(2)利用 TCP/IP 通訊協定漏洞進行攻擊：

- SYN Flood 攻擊：駭客只對目標主機發送一連串的 SYN 封包，每個封包都要求目標主機系統回應一個 SYN-ACK 封包，然後目標主機系統在回應 SYN-ACK 封包後會等待對方送出 ACK 封包。由於駭客並不產生任何 ACK 封包給目標主機，因此目標主機的系統佇列裡面會暫存大量的 SYN-ACK 封包，這些封包必須等到收到對方的 ACK

封包或是超過逾時時間之後才會被移除。如此目標主機系統會因為充滿了 SYN-ACK 封包而造成無法再處理其他使用者的服務與要求。

程式範例： dos

- Stream2 攻擊:

和 SYN-Flooding 類似，不過他是發送巨量的 SYN-ACK 去干擾正常連線。

- Arp spoofing 攻擊：

arpspoof 使用 ARP（位址解析協定）作為打開受害者之門的契機。首先，攻擊者使用 arpspoof 工具將偽造的 ARP 資訊封包向外發送給目標系統。這個偽造的資訊封包告訴目標預設閘道已經被更改成攻擊者給定的位址，這通常是攻擊者自己的 IP 位址。要發送偽造的資訊封包並使它起作用，攻擊者必須在同一個子網域中。這意味著攻擊者和目標通常共用一個公共預設閘道(一個攻擊者知道的閘道)。一旦目標接受了 ARP 表中的更改，每次目標向外發送資訊流，它就會把資訊流發送給偽裝成閘道的攻擊者。攻擊者將資訊封包轉發給它的原始目的地，但保留了它包含的資訊。這樣，閘道把資訊封包轉發給正確的最終目的地，而受到危害的用戶並不知道發生了什麼事。

如果轉送未完成，實施攻擊的機器就會變成資訊封包交彙點，進而把攻擊的目標網路斷線。若轉送成功的話，攻擊者就可以讀取由目標以明文方式發出的任何資訊，例如 Web 頁面或電子郵件內容。

(3)反彈式攻擊：

- DrDoS（反射式分布拒絕服務攻擊）

這是 DDoS 攻擊的變形，它與 DDoS 的不同之處就是 DrDoS 不需要在實際攻擊之前占領大量的傀儡機。這種攻擊也是在偽造封包來源位址的情況下進行的，從這一點上說與 Smurf 攻擊一樣，而 DrDoS 是可以在廣域網路上進行的。其名稱中的"r"意為反射，就是這種攻擊行為最大的特點。駭客同樣利用特殊的發送封包工具，首先把偽造來源位址的 SYN 連接請求封包發送到那些被欺騙的主機上，根據 TCP 三次握手的規則，這些主機會向來源 IP 發出 SYN+ACK 或 RST 封包來回應這個請求。同 Smurf 攻擊一樣，駭客所發送的請求封包的來源 IP 位址是被害者的位址，這樣受欺騙的主機就都會把回應發到受害者處，造成該主機忙於處理這些回應而被拒絕服務攻擊。

程式範例：DrDOS v2.0

- DNS Flooding attack

DNS 拒絕服務攻擊原理同 DrDoS 攻擊相同，只是在這裡被欺騙利用的不是一般的主機，而是 DNS 伺服器。駭客透過向多個 DNS 伺服器發送大量的偽造的查詢請求，查詢請求封包中的源 IP 地址為被攻擊主機的 IP 地址，DNS 伺服器將大量的查詢結果發送給被攻擊主機，使被攻擊主機所在的網路壅塞或不再對外提供服務。

程式範例：dnsflood

實驗心得：

其實在整個實驗的過程中，我們發現攻擊最重要的手法有下列幾種：

(1)利用頻寬去消耗對方；

可以利用製作大型封包，或一直發送大量封包，造成網路擁塞，達成 DOS 目的。但此種攻擊模式是利用大量頻寬，所以當對方採用 limit Rate 策略，可能就無法達成攻擊效果。

(2)利用協定上的弱點去攻擊：

通常是利用反彈，或是查詢及反應等等，一直幫對方製造查詢的封包，導致小流量匯集起來攻擊目標，算是一種不錯的攻擊方式。不過這一類的方式可以被網管人員關閉這項功能去制止，不過像 TCP SYN handshaking 當然是無法防止。

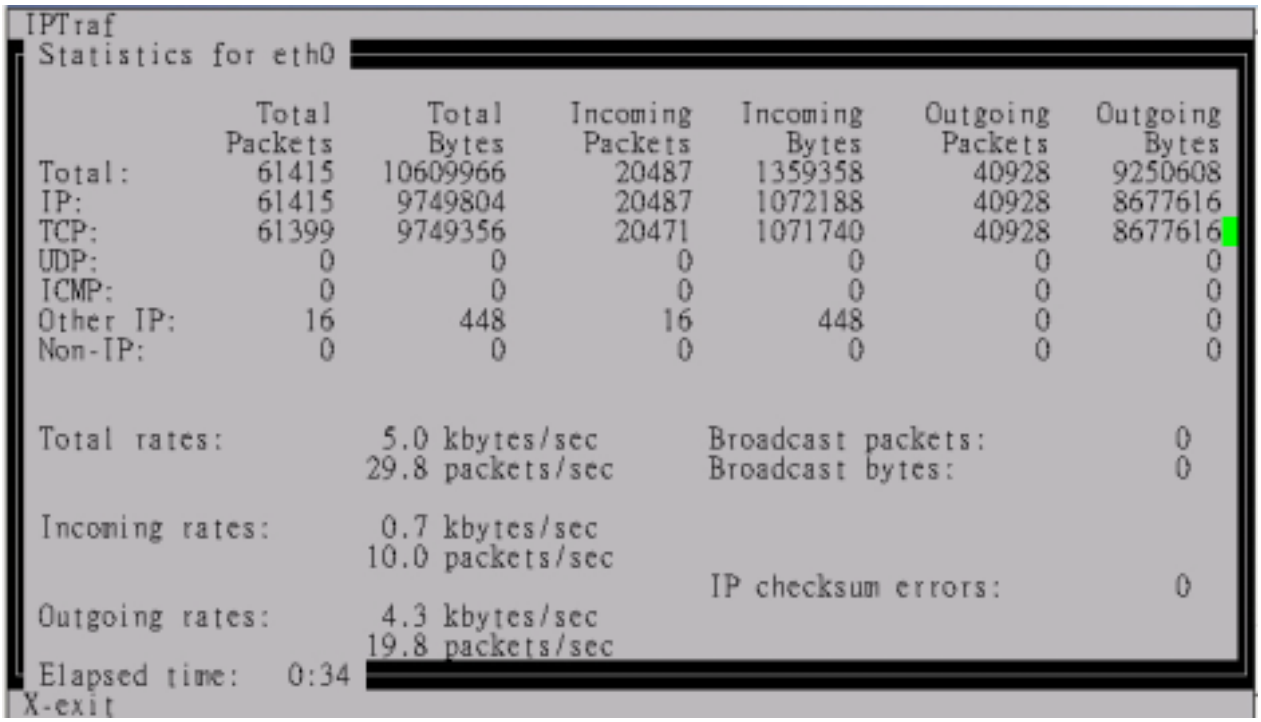
(3)利用封包數目去消耗對方：

因為我們可以一直製造封包數目龐大，但封包很小的攻擊模式，由於此種方式會使網路不致於壅塞，比較不會被察覺。小封包也能使發送速度變快，而目標會因為一直處理封包而耗損 CPU resource，而且通常在網路協定上，有很多 Protocol 連線數目都有上限，會因為這類攻擊長達致上限，造成 DOS 攻擊成功。

防禦措施

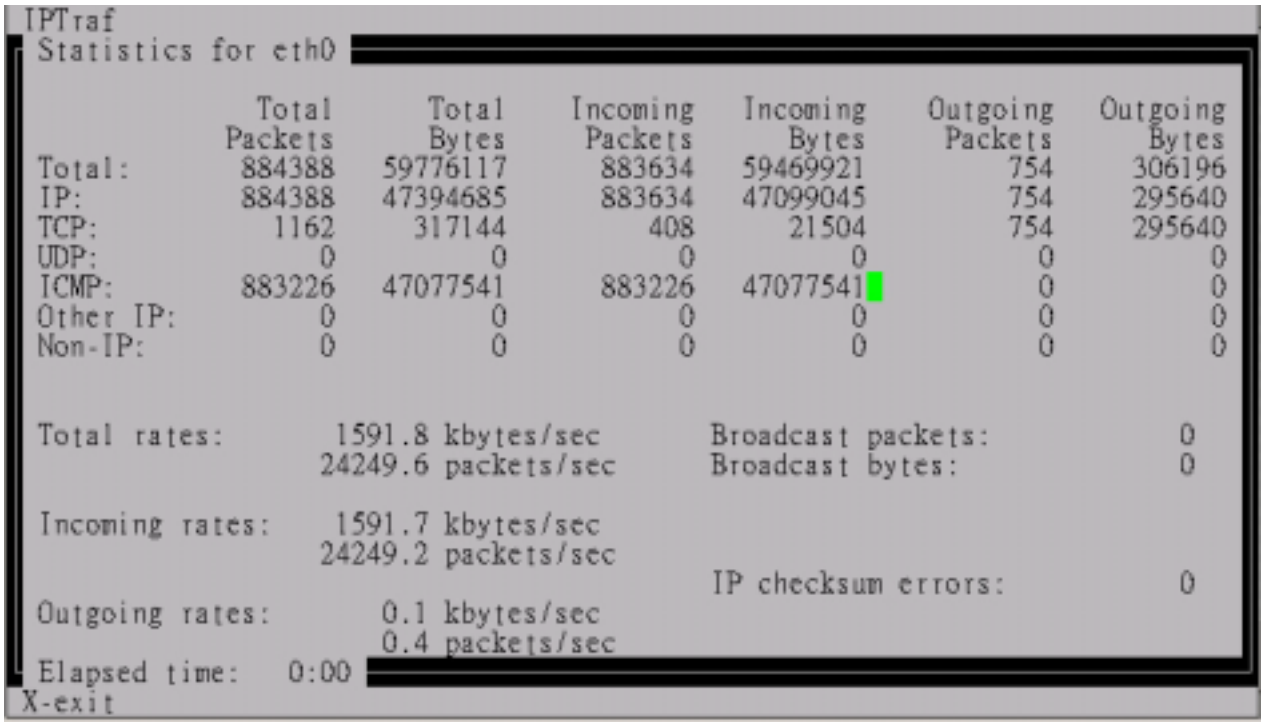
阻絕服務攻擊的問題最困難的就是辨識正常封包和攻擊封包。目前最常見的偵測系統就是針對已知的攻擊手法已規則紀錄之，當流經的封包比對之後，符合已知手法者，即判定為攻擊，因此辨識的規則明確性相當重要。另外一種就是建立異常流量的 Threshold，藉由事先的定義了解異常流量的發生。因為 Threshold 依據跟所在網路會有很大的差異性，使得辨識的準確性有很大的調整空間。實驗中希望藉由阻絕服務攻擊偵測系統了解攻擊手法與偵測方式，明白阻絕服務攻擊偵測在安全建置中扮演重大的角色。

為因應 DDoS 攻擊的特性，並即時有效地獲知是否有攻擊發生，我們同時採用多種方式，在攻擊目標主機、路由器、及 switch 上分別來監控網路流量的變化。在攻擊目標主機上，我們採用 iptraf 這支程式來監控該主機上的流量。一般正常使用，或是遭受攻擊前，網路流量多在數 K 到數百 Kbytes 之間，如下圖二所示。



圖二、iptraf 執行畫面(正常使用，攻擊前畫面)

在遭受攻擊後(這裡是執行一支 smurf 程式來進行攻擊)，網路流量會瞬間飆升到數萬個封包，幾 Mbytes 的資料量，如下圖三所示。



圖三、iptraf 執行畫面(執行一支 smurf 進行攻擊)

在路由器上，我們採用 MRTG (Multi Router Traffic Grapher) 來進行資料分析。MRTG 是透過 SNMP (Simple Network Management Protcol)來監視並記錄網路傳輸流量，並將這些資訊以含有 PNG 格式圖形的 Web 方式顯示給使用者觀察流量負載，關於 MRTG 的詳細的資訊可以至官方網站(http://people.ee.ethz.ch/~oetiker/webtools/mrtg)中取得。使用方式如下：

1．先到要觀察的 host 上執行 snmpd

2．建立 mrtg.cfg 檔案

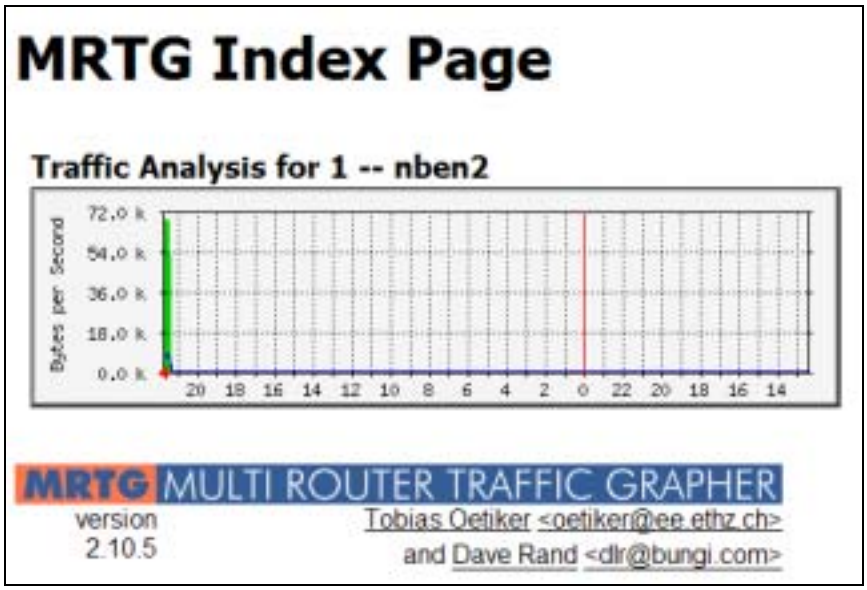
```
# cfgmaker public@主機 IP 位址或是主機名稱 > mrtg.cfg
   編輯 mrtg.cfg 內容如下

### Global Config Options
#  for UNIX
    WorkDir: /var/www/html/mrtg ← 統計資料存放目錄
```

3．執行 /usr/bin/mrtg /etc/mrtg/mrtg.cfg

4．執行 indexmaker /etc/mrtg/mrtg.cfg > /var/www/html/mrtg/index.html 這行指令以產生 index.html 檔案。

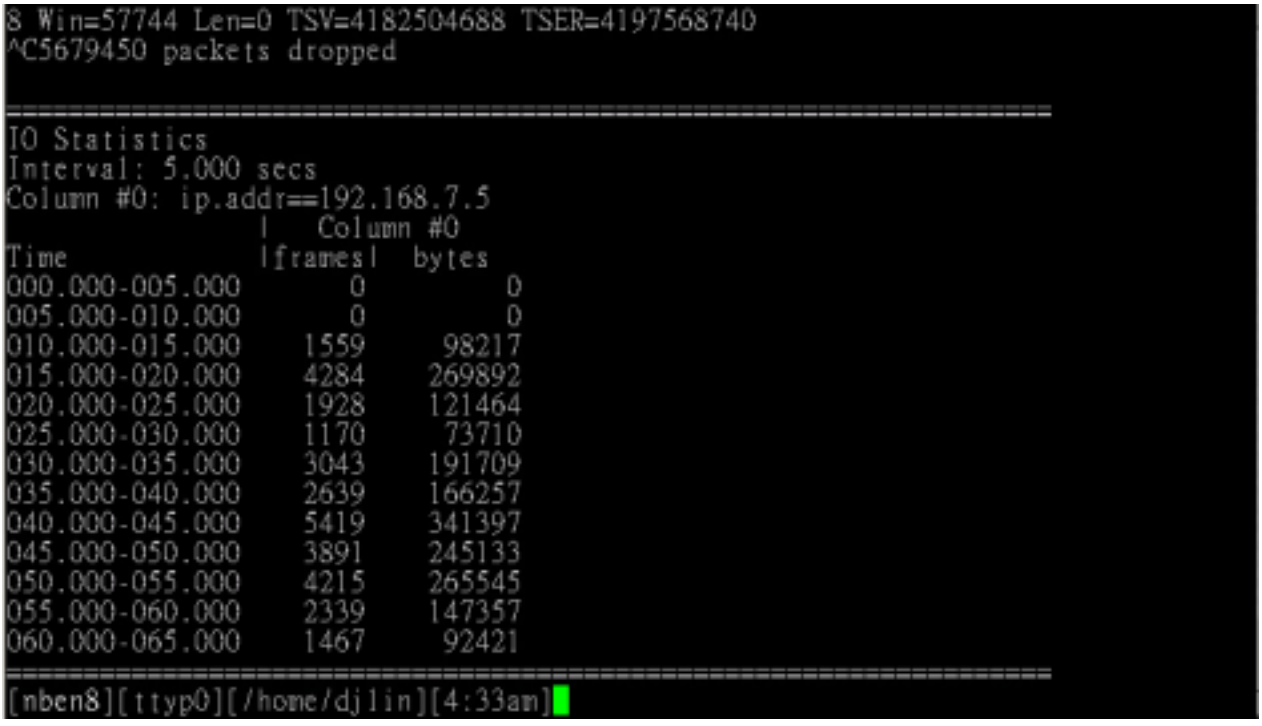
5．檢視產生的網頁，如下圖



圖四、 MRTG 流量統計 Web 畫面一覽

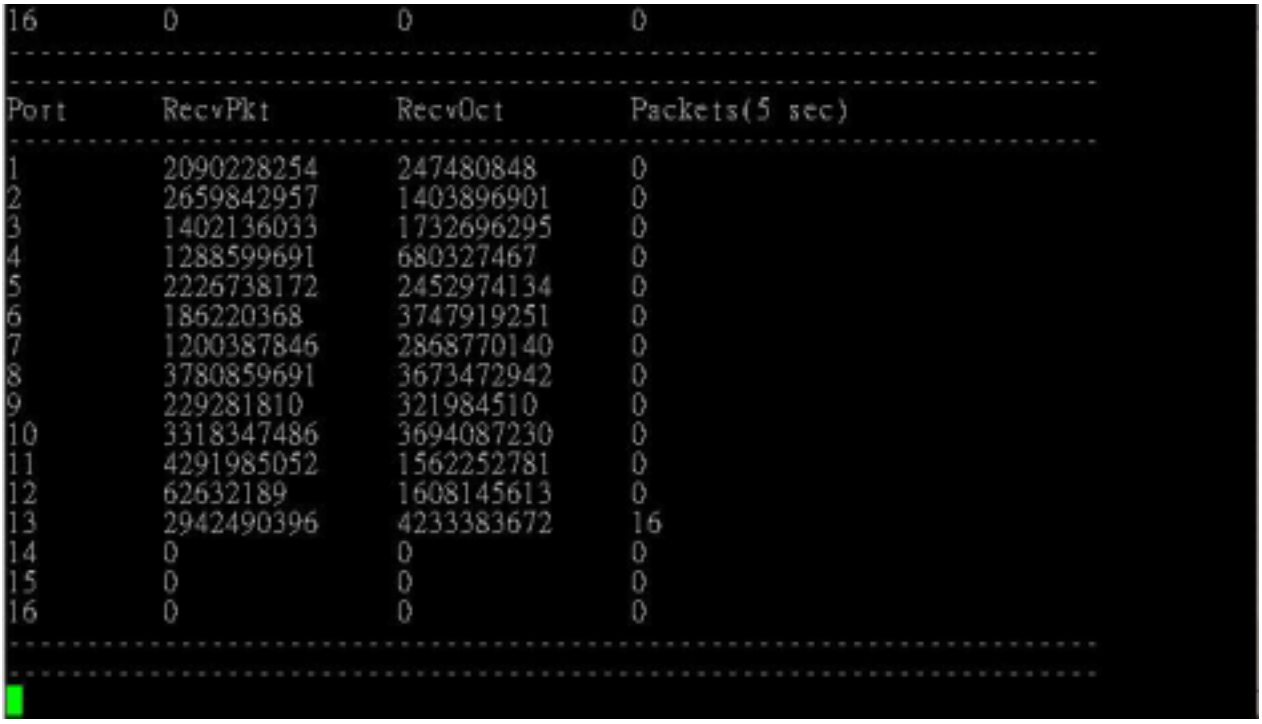
因為 MRTG 需要較長的更新時間，比較適合用於長時間的統計資料。為了監控即時的流量，另外使用了一套工具程式 ethereal(可在 http://www.ethereal.com/取得程式及相關說明資料)。利用 tethereal(ethereal 的文字模式版)，可以監控網路各通訊協定、封包資料、監聽不同網路卡介面、統計時間區段內的封包數/大小等等方便的資訊。使用畫面如下圖五、圖六。

圖五、用 tethereal 監控網路封包狀況(smurf 攻擊中)



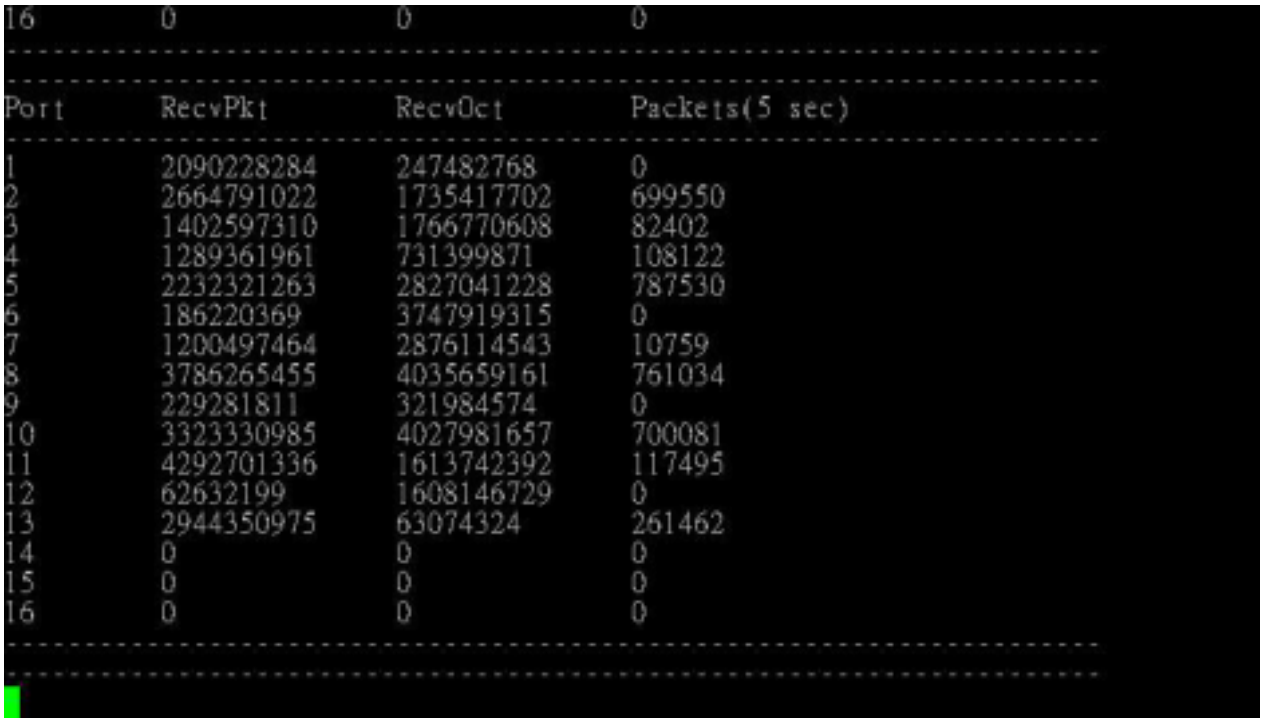
圖六、用 tethereal 監控網路封包狀況(以五秒做時間區段所得的統計資料)

在 switch 上，我們透過自行設計的一個 script，連接到 switch，定期(預設 5 秒)上去讀取每個 switch port 上的流量，並計算該時段之間所流過的封包數和總流量。



Port	RecvPkt	RecvOct	Packets(5 sec)
1	2090228254	247480848	0
2	2659842957	1403896901	0
3	1402136033	1732696295	0
4	1288599691	680327467	0
5	2226738172	2452974134	0
6	186220368	3747919251	0
7	1200387846	2868770140	0
8	3780859691	3673472942	0
9	229281810	321984510	0
10	3318347486	3694087230	0
11	4291985052	1562252781	0
12	62632189	1608145613	0
13	2942490396	4233383672	16
14	0	0	0
15	0	0	0
16	0	0	0

圖七、剛啟動分析 switch port 封包資料的 script 畫面



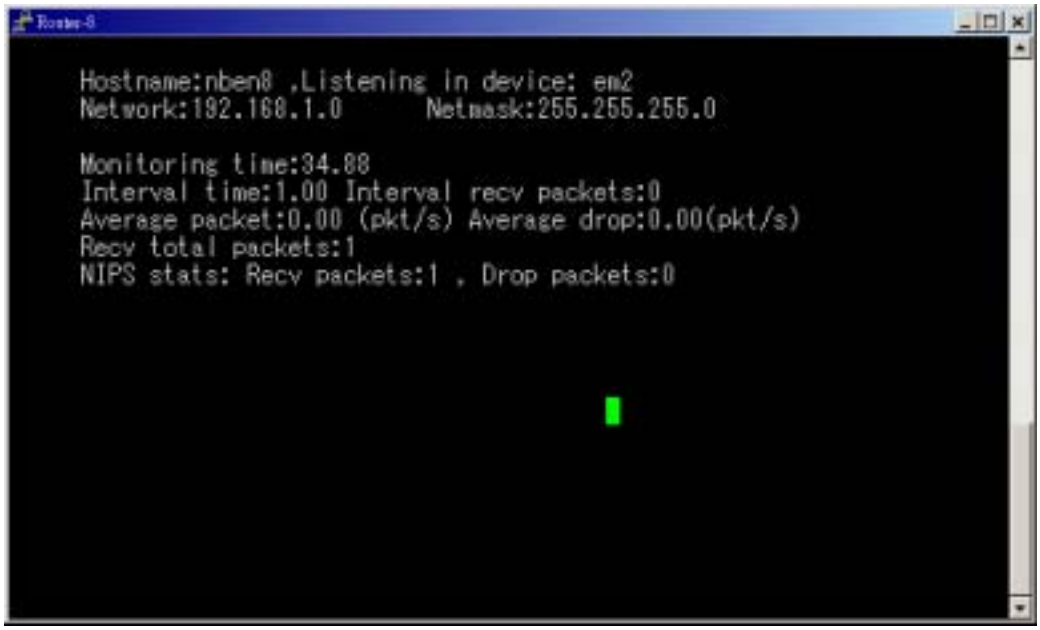
Port	RecvPkt	RecvOct	Packets(5 sec)
1	2090228284	247482768	0
2	2664791022	1735417702	699550
3	1402597310	1766770608	82402
4	1289361961	731399871	108122
5	2232321263	2827041228	787530
6	186220369	3747919315	0
7	1200497464	2876114543	10759
8	3786265455	4035659161	761034
9	229281811	321984574	0
10	3323330985	4027981657	700081
11	4292701336	1613742392	117495
12	62632199	1608146729	0
13	2944350975	63074324	261462
14	0	0	0
15	0	0	0
16	0	0	0

圖八、分析 switch port 封包資料的 script 畫面(使用 smurf 攻擊中)

這裡製作一簡易型之網路式入侵預防偵測系統(Network-based Intrusion prevention system,簡稱 NIPS)，當阻絕服務攻擊發起時，網路流量會有明顯變化，當流量超過 Threshold 之後，受害者端無法承受時，此時網路服務會呈現中斷現象，所以我們必先控制來源端路由器限流。

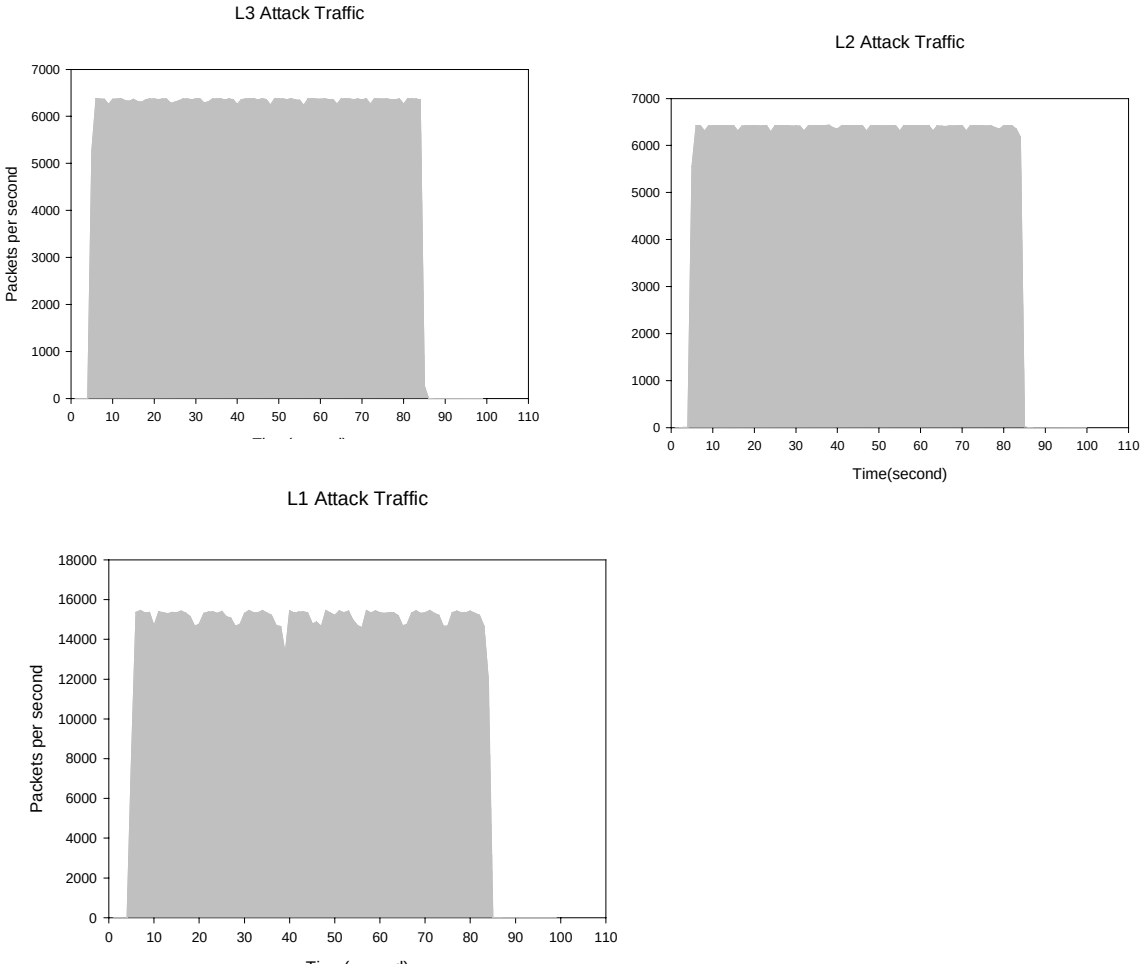
研究步驟如下：

步驟一、 啟動 NIPS 並觀察 NIPS 顯示之流量參數



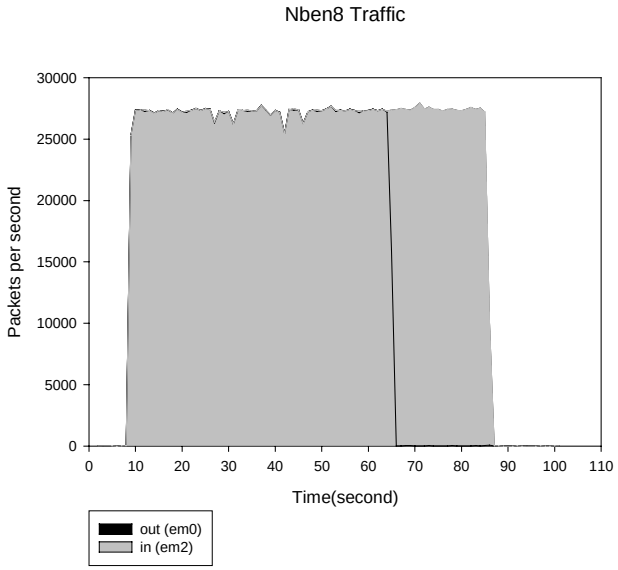
圖九、NIPS 程式執行畫面

步驟二、 關閉 NIPS，以方便觀察統計流量，啟動攻擊者之異常流量手法攻擊

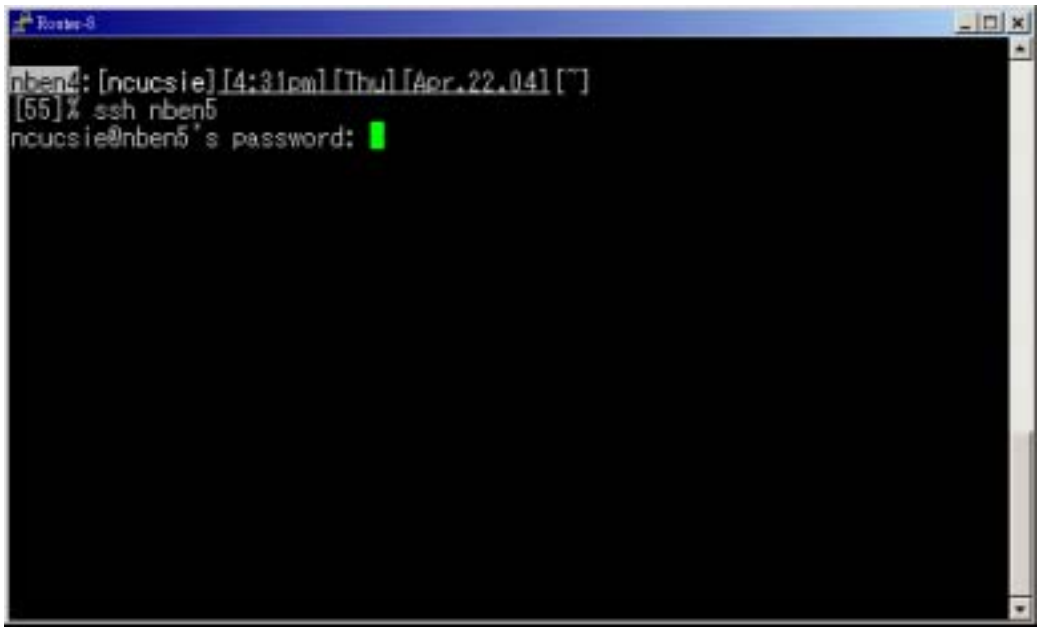


圖十、未執行 NIPS 前，L1~L3 上的網路流量情形

步驟三、 當攻擊之後約六十秒再次啟動 NIPS，觀察 NIPS 顯示之流量參數超過 Threshold 限制流量



步驟四、觀察受害者端電腦是否能夠存活



圖十一、啟動 NIPS 後，解除了 DDoS 攻擊的衝擊，可以提供 ssh 連線

結果與討論

首先說明阻絕服務攻擊對網路影響，接著使用真實的攻擊流量造成網路頻寬的消耗，接著測試軟體模擬防火牆的功能。實驗結果顯示，在軟式路由器建立防守策略是艱困難行，因為攻擊的時候軟式路由器轉送封包本身已經消耗大量的 CPU 和 IO 資源，所以一個輕巧與快速反應的阻絕服務偵測系統是絕對需要的。除此之外，仍然要加強整個網路安全基礎建設，如降低個人網路主機被駭客利用當跳板的可能性，除了不讓異常流量流入網際網路之

外，非自己本身網域 IP 位址應該都要加以嚴格的把關，否則防治阻絕服務攻擊如雪上加霜。

未來工作可以擴展實驗網路架構，增加更複雜的路由節點。這將會使實驗更貼近真實的情況，由於較為龐大的路由機制，更值得去測試 IP Traceback 的技術。此外試圖不以路由器負責統計流量之觀點，改成放置旁邊監測，研發有效且準確的判別攻擊來源之偵測工具，又不會與路由器功能相衝突。一個聯合多類型的阻絕服務防禦系統是將來勢在必行的工作。

參考資料

[1] J. Postel. Internet Protocol. RFC 791, Sept. 1981.
[2] O. Spatscheck and L. Peterson. Defending Against Denial of Service Attacks in Scout. In Proceedings of the 1999 USENIX/ACM Symposium on Operating System Design and Implemetation, pages 59-72, Feb. 1999.
[3] C. Villamizar. Personal Communication, Feb. 2000.
[4] C. Shannon, D. Moore, and K. C. Claffy, “Beyond folklore: observations on fragmented traffic,” IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 709-722, Dec. 2002
[5] A. Belenky and N. Ansari, “Accommodating Fragmentation in Deterministic Packet Marking for IP Traceback,” IEEE GLOBECOM’ 03, December 2003.
[6] John Ioannidis Steven M. Bellovin, “Implementing Pushback: Router-Based Defense Against DDoS Attacks,” in Proceedings of Network and Distributed System Security Symposium, San Diego, California, February 2002.
[7] News About Denial of Services,
http://www.canada.cnet.com/news/0-1007-200-1545348.html
[8] FreeBSD security information，http://www.freebsd.org/security/
[9] Gentoo Linux 安全指南，http://www.gentoo.org/doc/tw/gentoo-security.xml

計畫成果自評

I. 原訂計畫目標：

本子計畫的目標在建立一個分散式阻絕服務攻擊的測試平台，能偵測攻擊，並回復攻擊前狀態之機制。參與此子計畫的交大、清華、中央，則分別進行分散式阻絕服務攻擊平台建立/流量監控技術，DDoS 攻擊程式撰寫與攻擊測試，及 DDoS 攻擊回復技術，針對這類攻擊大流量，攻擊點多的特性，進行技術的研究及系統的實作開發。

II. 研究內容與原計畫相符程度

完全符合。

III. 預期目標達成情況與綜合自評

我們對於分散式阻絕服務攻擊進行測試，本計畫建立一封閉式測試平台可供進行 DDoS 攻擊測試，多種 DDoS 攻擊程式的實作與分析，防禦機制的實作，以及資訊安全訓練教材的撰寫。我們以有限的人力和時間完成了以上的成果，感謝三校參與人員的努力，也謝謝成大的指導。