以多重式 IP 分配管理政策實現可追蹤封閉式企業網路安全防禦縱深之研究

魏子文[1]、吳宗禮[2]、王順吉[3]、江清泉[3]、孟興漢[3]、孫秉良[4]
國防部通信電子資訊參謀次長室軟體發展中心[1]
私立中國科技大學資訊傳播/工程系[2]
國防大學中正理工學院資訊科學系[3]
經國管理暨健康學院資訊科技系[4]
zwwei@ccit.edu.tw

摘要

為有效嚇阻網路攻擊者(Attacker)、確保網路安全(尤其是封閉型企業或官方網路),本文提出並具體實作了一種集權式的網際網路位址(Internet Protocol Address)資源分配管理策略,以便利追蹤與確認攻擊來源。此法採用階層式 IP 位址配置規則,結合了使用單位地理位置、實體電路配置等特性、再搭配複式的網路存取過濾規則,形成多重性防護、拉長防禦縱深,來提高 IP 網路基礎建設的防護強固力。本策略同時改善了防衛者(Defender)網路路由與網路封包傳遞的效能。綜合以上效能,當攻擊事件發生時,管理者可以迅速的追蹤與確認攻擊來源,面對網路上常見的各類攻擊方法,足以採取適當、精準的防護回應,以達成強化網路安全防護的目標。

關鍵詞:網路安全、封閉型網路、分散式阻斷服務攻擊、網路基礎建設防護、防禦縱深、可追蹤 IP 配置架構、存取過濾

一、動機簡介

現行網際網路的開放式環境,對於執行攻擊來源追蹤仍有許多限制[1]、也造成攻擊者可以輕易的隱匿身份於網際空間,恣意進行各種網路攻擊行為。

從網路攻防戰的角度來看,網際網路空間就如同是個開放性的戰場,攻防雙方在此戰場上各自運用所能掌控的資源進行對抗[2];能確實管理並妥善運用這些網路資源的一方,就能在對抗中掌握戰場主控權並進一步取得勝利。防衛者面對層出不窮的網路攻擊事件,傳統的安全服務如保密性、完整性與可用性(Security Services : Confidentiality, Integrity, and Availability)一般屬於輔助性質的工具,主要作用止於外在地強化或填補資訊基礎建設(Information Infrastructure)安全架構的縫隙,而我們認為一個本體即強固的基礎建設安全架構卻是有效保護整體資訊應用環境安全的根本。

以處理資訊安全事件為例,最有效的作為是找出問題發生的原因,當面對網路入侵攻擊行為時,若能先識別真實的攻擊來源不僅可以幫助資源的管理者瞭解問題所在、修正或防堵防護漏洞,強勢嚇阻潛藏的攻擊者,使其難以遁形、減低其攻擊企圖,甚至可以進一步採取反制作為;這種考慮在屬於封閉型的企業或官方網路防護中更顯可行與重要。

本文針對於在企業封閉式網路的環境中,提出集權式的網際網路協定位址資源分配管理策略,採階層性的 IP 位址配置規則,再結合使用單位地理位置、實體電路配置等特性、並搭配多層次的網路存取過濾規則,來實現具可追蹤特性的 IP 網路基礎建設。實作結果的經驗顯示此策略除了可改善防衛者網路路由與網路封包傳遞的效能外,特別在有攻擊事件發生時,管理者可以迅速的追蹤與確認攻擊來源,面對現今網路上常見的各類攻擊方法,足以採取適當、精準的防護回應,以達成強化網路安全防護的目標。而本研究的實驗過程與結果也可提供網路安全研究者相當的參考。本論文的實驗均在國防大學中正理工學院資訊系的 iSAR (information Security Analysis and Research)實驗室完成,詳如下列各節說明。

二、攻擊源追蹤技術探討

由於網路封包中的來源位址可以輕易的被偽造,現今各種探討追蹤攻擊來源的技術文獻多不採信來源封包中的 IP 位址，而著重於掌握被追蹤封包所經過的節點路徑，這些回溯機制，大致上分類為主動式(Proactive)和被動式(Reactive)兩種[3]，分別說明如下：

(一) 主動式追蹤(Proactive)

~~請~~主動式追蹤回溯機制的概念為在封包傳送過程中，當封包經過每個轉送的路由節點的同時，產生一些回溯時所需要的資訊。主要的應用有下列兩種方式：

1. 封包標記法(Packet marking)：

~~在~~封包由來源端傳送到目的地端的路徑中，經由許多路由器轉送到下一個路由器,路由器在轉送封包時,將自己的身份資訊如IP位址等，記錄於封包之中，因此我們在回溯時，便可依據封包上的紀錄，往回找到攻擊源。

2. 訊息通知法(Messaging)：

封包在經過路由器時，路由器就傳送一個網路控制訊息協定(Internet Control Message Protocol, ICMP)封包給目的位址，如此目的位址便可將路由器所傳送來的 ICMP 封包收集起來，透過這些 ICMP 封包可提供正確的回溯資訊。

(二) 被動式追蹤(Reactive)

被動式回溯(Reactive tracing)的運作機制概念是當發現遭受攻擊時，才開始進行追蹤，方法簡要說明如下：

1. 逐站追蹤法(Hop-by-hop tracing)：

逐站追蹤法回溯方式為當偵測到攻擊封包時，藉著登入在上游的路由器並監視封包的流向，若攻擊事件持續發生,則再經由監測的結果登入到更上游的路由器，如此遞迴的進行，直到找到攻擊者的來源位址為止。此法的限制為當節點站數量愈多時，處理回溯程序也變的複雜，效能也因此受到影響。

2. 使用重疊網路追蹤法(Hop-by-hop tracing with an overlay network)：

這個方法是為了改進前述逐站追蹤法的效能問題。為了簡化回溯過程，本方法提出建立一個覆蓋型的網路，即是把所有邊緣路由器(Edge routers)和一個特別稱為追蹤路由器(Tracing router)的路由器,以 IP 通道(Tunnel)的方式連在一起，這樣追蹤路由器便能把封包再繞送(Re-route)至應該到達的其它的邊緣路由器,如此便能增加回溯的效能。

3. IP 安全(IPSec)認證機制法：

類似逐站追蹤法，但當入侵偵測系統偵測到攻擊時，則利用網路金鑰交換協定(Internet Key Exchange, IKE)在受攻擊目標~~和~~與鄰近的路由器間，建立 IPSec 安全關係(IPSec Security Associations, SAs)，因此要回溯到上一個路由器時只需要檢查IPSec標頭裡的相對應的路由來源位址即可，如此遞迴的進行，直到找到攻擊來源。

4. 流量樣本比較法：

這個方法透過數學模式計算進、出路由器之間的封包流量樣本，再加以比對，以找出可能的攻擊來源方向，進而確定發動攻擊的來源地。

綜合以上說明可知，一般來說若要實現 IP 可追蹤與回溯機制,無法避免需要網路上所有實體路由設備共同合作,並在大部份路由器能支援的情形下，才能達到路徑回溯的效果。很明顯的，這種大量設備間的合作並不容易且效能因素影響甚大。

而本研究強調回歸網路安全的基本面，從強化基礎建設本身的架構強固性著手,將可追蹤封閉式網路IP架構植基於對偽造來源封包的限制性,透過逐層的存取過濾機制,巨幅壓縮攻擊封包所能偽造的來源位址空間至過濾機制所容許的範圍之內。接著，我們採信來源封包所記錄的IP位址，並配合階層式的IP配置策略,即可建立可~~快~~迅速回溯其來源位址的機制。

三、多重式可追蹤 IP 架構設計與實驗網路概述

習慣上我們常將是否與網際網路 (Internet) 連結來區別開放式與封閉式網路的類型[4]，但從網路的應用目的與使用範圍來看，封閉式網路通常有其任務的專屬性(Dedicated Network)，使用對象也有針對性，不似開放式網路屬於通用型~~網路~~，對使用者的身份限制條件也較少。

(一)封閉式網路的特性與優勢

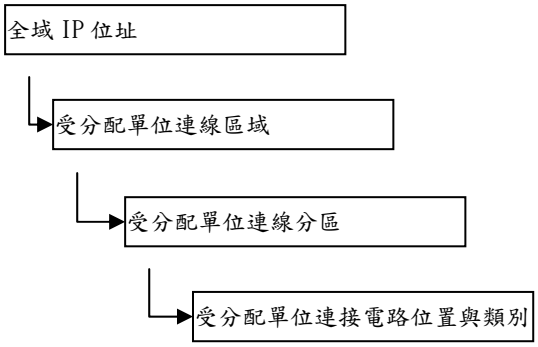
通常封閉式網路所有者對網路資源有絕對的掌握權,在安全與網路管理策略上多採用集權式管理架構,由單一最高管理權責單位由上而下律定,有利於階層式 IP 管理架購的佈建與利用,乃至進一步有助於可追蹤網路機制的實現,來落實執行企業組織的安全政策。;相對下,開放式網路則由個別所屬的不同管理權責單位掌握再相互協調構連,彼此間較無相依性,其比較說明詳見附表一。

(二)階層式 IP 位址空間配置

現行網際網路近似平面式的 IP 位址空間配置法,必須透過註冊的程序或其它應用服務的協助(如 Whois, Domain Name Service 網域名稱服務),才能間接迂迴地正確解析所查詢的 IP 位址在網路上的位置、使用單位與其真實的地理所在位置。相反的,若採用已結合地理位置資訊的階層式 IP 配置管理策略則可以解決這個限制,使 IP 資源的管理者與使用者,能以直觀的規則快速而正確地標示出此 IP 的實體地理位置。這概念與網域名稱服務以類別、屬性來建立網域名稱的階層結構相類似。

不同於 Internet 中已定型的 IP 分配習慣,在個別封閉式網路中,若企業組織對網路的資源擁有絕對的控制權,在規劃配置與指定 IP 資源時,配合上層連接電路服務的供應者與網路交換中心,使 IP 位址空間能以階層式的規則配置,建立樹狀的分配結構,將更有利於網路管理者整合縱向資訊(如 IP 位址、電路資訊、地理位址資訊等)。

在規劃配置 IP 資源時,可依據以下程序來決定使用單位受分配的位址:



以本文所使用實驗室網路的環境設定為例,全域使用的 IP 位址空間為 172.16.0.0/12,將此位址空間依據受分配組織所在的地理位置,向下區分為北、西、南、東四個不同的區域層級,並將全域使用的 IP 位址空間平均配置予每個區域,然後在每個區域中,再細分為多個分區,每個受指定的末端用戶的 IP 位址空間,均由其地理位置相符的分區所配置,建立出階層式 IP 位址空間配置規則,如圖 1。

IP 位址結合地理區域與階層式配置策略的益處有:

(1)藉由階層式的 IP 位址配置規則,管理者在瞭解資源配置規則後,可快速、直覺的判斷所欲查詢的 IP 位址,其所在的網際空間與實際的地理空間位置,減少必須透過 Whois、DNS 等其它輔助查詢機制的機會。

(2)隨著網路的擴展,路由紀錄數量的快速成長也成為所有網路管理人員必須克服的問題之一。透過樹狀結構的 IP 配置程序,可有效聚合路由記錄,簡化路由器繞徑表(Routing Table)管理負載,同時提升網路封包交換傳輸效益。

(3)當攻擊事件發生時,快速鑑別真實的攻擊來源與攻擊方法,是首要的防護要領之一,階層式的 IP 位址設計,可縮小範圍利於追蹤可疑的攻擊來源,可有效防堵如病毒、阻斷服務等癱瘓網路的攻擊模式。

(三)網路入口封包過濾

由於缺乏適當的驗證與保護措施,偽造來源 IP已經成為攻擊者隱匿真實位址的慣用搭配手法之一。要防範這類攻擊~~手法~~,最有效的做法就是在每一個路由器介面上,設定入口封包過濾檢查(Network Ingress Filter)機制[5]。

圖 2 為本實驗入口封包過濾程序圖解,攻擊者位於 172.16.10.0/24 區段,在區域路由器上的過濾檢查規則為

```
IF    封包來源位址屬於 172.16.0.0/16
  THEN  傳送這個封包到適當目的地
  ELSE  拒絕封包進入
```

當入口過濾規則套用在愈接近攻擊者的路由節點上,過濾的效果愈好,攻擊者能偽冒的 IP 位址空間也愈小。

儘管使用流量過濾機制可大幅降低偽冒來源位址封包流入受害端網路的數量,它仍無法杜絕攻擊者假造其它過濾許可範圍內封包表頭的來源位址;但依然可確保當這類攻擊真正發生時,網路管理者必能在已公佈的已知表頭區段中,確認出攻擊者真正的來源位址,且很快的追查出攻擊源。

在封閉式網路環境中由於集權式的管理作法,過濾的機制更能落實到末端節點,當所有的網路設備都能導入入口封包過濾機制後,追蹤攻擊者

來源也將變的更為容易，即使攻擊者利用多個跳板意圖使受害端難以追查真實的攻擊源，但只要能在安全機制或電腦鑑識找出 IP 連線記錄，對辨認真實的攻擊源仍有相當大的助益。

四、實驗驗證與分析

(一)實驗環境介紹

為具體驗證本文所提出的 IP 位址分配管理政策對網路安全防護的效益，我們建置了一套封閉網路的模擬架構，透過實作常見的網路攻擊行為—分散式阻斷服務攻擊(Distributed Denial of Service Attack, DDoS)，驗證在不同的 IP 與路由管理分配政策下，對有效達成網路安全防護的影響程度。

實驗網路架構設計依照網路防護徑線，概分為三個網路區塊：來源網路(Source Network)、中繼網路(Intermediate Network)與受攻擊網路(Victim Network)，如圖 3 所示。每個網路間均設置封包的監測點，以蒐集在不同管理政策下封包流量的變化。平台設備計使用八部路由器(Router)、三部交換器(Switch)及十三部個人電腦，其中四部做為攻擊主機(命名為 Attack_E, Attack_S, Attack_W 與 Attack_N)，四部監測主機分別擔任各網路區塊間封包流量監測，名稱與其功能如下說明：

Monitor_A：監測進、出來源網路與中繼網路間封包。

Monitor_B：監測進、出中繼網路與受攻擊網路的封包。

Monitor_C：監測進、出 Victim_A 的封包。

Monitor_D：監測進、出 Victim_B 的封包。

實驗網路區域路由器間的路由協定採用開放式最短繞徑協定(Open Shortest Path First protocol, OSPF)，將圖 3 所示之實驗配置進一步描述為網路層邏輯架構與設備參數配置後則為圖 4。此外，為使實驗網路較接近企業組織環境，我們分別在各階段的區域路由設備中加入靜態路由紀錄，以模擬各區域路由器以下所界接的路由資訊。

研究中我們進行兩階段的實驗測試，分別以不同位置與不同數量的攻擊主機組合而成，共進行了 27 組實驗以觀察攻防效果，詳如表 2 說明。實驗一模擬現行網際網路IP配置實況，在未設置任何過濾保護的環境下，利用阻斷服務偽冒來源IP的攻擊手法，我們觀測與記錄由攻擊端送出的封包數量(P_{Send})和到達受害者端封包的數量($P_{Received}$) 與各路由器CPU資源使用率的變化。我們以實驗一所蒐集到的封包數量做為第二階段實驗中比較的基準值。

其中：

$P_{Send} = SUM(P_{attack\_W}, P_{attack\_S}, P_{attack\_E})$

$P_{Received} = P_{Victim}$

在實驗二中，IP位址的分配依照第三節所介紹的配置規則，依階層化的方式重新配發，並分別驗測在區域路由器與末端路由器上加入實現入口封包過濾機制後，攻擊封包實際可到達受害端網路的成功率($P_{success} = P_{Recived} / P_{Send}$)與各路由器CPU資源使用率的變化。

表 3、4、5 分別為實驗中各監測點封包數量統計，圖 5、6、7 分別為各階段三部攻擊主機的測試中，處理器資源的使用變化。

本論文所有實驗均使用使用 TFN2K[6]做為攻擊測試的工具，攻擊過程中均採用偽造的來源 IP，偽造的 IP 位址範圍為 172.0.0.0/8。

(二)效益分析

在單一攻擊主機狀態的個別測試中，攻擊主機Attack_W、Attack_E所送出的攻擊封包實際到達受害端的比率$P_{Success}$，約分別為總攻擊封包數的 2.55%與 2.47%，其中攻擊主機Attack_S在雙傳送路徑的助益下，成功率提高為 4.58%（如圖 8）

實驗二中，當入口過濾條件僅套用於區域路由器的測試中，只有原來攻擊封包總量的 0.32%左右能送達受害端，也就是說過濾效果$P_{Efficiency}$為 99.68%（圖 9）；當入口過濾規則延伸套用至末端路由器時，其過濾效果則高達 99.99%（見圖 10）。

(三)路由器處理效能分析

在此我們僅分析在同時有三部攻擊主機的情況下，處理器資源使用率的變化(如圖 11)。

以實驗一為比對樣本，不論攻擊主機數量的

多寡，在實驗二第一階段中，將入口過濾條件加入區域路由器上時，攻擊端所連接的區域路由器 CPU 使用率由實驗一趨於滿載 99%的情況下，降低為平均 94%左右；對受害端網路所連接的區域路由器 North 與末端路由器 Taipei，其 CPU 使用率更分別由實驗一的 64%與 6%降低至 20%與 2%，降低了近三分之一的 CPU 使用率。入口過濾設定進一步的套用在攻擊端所連接的末端路由器後，區域路由器的 CPU 使用率更進一步降低至 5%的平均值，這數值已經相當接近區域路由器在無攻擊負載時，我們所觀察的 4%的基本使用率；同時 North 與 Taipei 路由器的使用率，都幾乎與平時一般負載無異。

從以上結果分析得知，我們驗證在良好的 IP 資源配置基礎上，搭配簡單的存取過濾規則就可以有效的防止常見的阻斷服務攻擊手法，同時也提供資源管理者快速而準確的攻擊來源判斷的條件，當攻擊者無法輕易隱匿於網路空間時，網路防護的安全機制會變得更有成效，入侵者發動攻擊的企圖也會相對被嚇阻與削弱。

五、結論

在 1994 年，網際網路架構委員會(Internet Architecture Board, IAB)所發佈的一篇名為 Security in the Internet Architecture(RFC 1636)[7]的文件報告中指出，網際網路環境需要更多更好的安全機制，其關鍵在加強網路基礎建設的安全性。

網際網路上要回溯攻擊來源，直接從受害者端網路上的防火牆、入侵偵測系統或遭攻擊系統上記錄的攻擊封包來源 IP 位址判別，參考價值不高，主因是來源 IP 位址能輕易的被偽冒。即使採用現行已提出的各種複雜的主、被動回溯追蹤技術，在實務執行上也是困難重重，最主要的原因還是受制於網際網路上分散式的網路管理權責與鬆散的安全政策。

本研究中，我們著眼於封閉式企業網路架構上的優勢，提出適用於封閉式網路可追蹤 IP 分配管理架構，搭配多重機制以實現 IP 位址回溯的功能。經由實驗的驗證，一個規劃與管理良善的網路基礎建設，拉長了防禦縱深，並可以對所偵測到攻擊封包來源 IP 的可信度有相當的信心。藉由本論文完成實驗所產生的經驗與心得，我們確信對強化未來此類型網路管理與安全維護的作業，將有具體而實際的幫助；甚至對開放型網路的安全防護，只要採取適當的設定與管理，也能有相當的參考價值。

六、誌謝

本文實驗過程得以順利進行，特別要感謝經國技術學院資訊科技系簡承光先生不吝提供路由設備，並協助相關網路管理技術咨詢與許多寶貴的實務經驗，使實驗得以順利完成，致上最誠摯的謝意。

七、參考文獻

[1] Burch Hal, and Cheswick Bill, Tracing Anonymous Packets to Their Approximate Source, USENIX LISA, 2000.

[2] Dorothy E. Denning, Information Warfare and Security, Addison Wesley, 1998..

[3] Tatsuya Baba and Shigeyuki Matsuda, Tracing network attacks to their sources, IEEE Internet Computing, Vol.6, No.2, pp.20–26, 2002.

[4] M. Bishop and L. Heberlein, An Isolated Network for Research, Proceedings of the Nineteenth National Information Systems Security Conference, pp. 349-360, Oct., 1996.

[5] P. Ferguson, and D. Senie, Network Ingress Filtering:Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, May, 2000.

[6] http://mixter.void.ru/

[7] R. Braden, D. Clark, S. Crocker, and C. Huitema, Report of IAB Workshop on Security in the Internet Architecture, RFC 1636, June, 1994.

表 1 封閉式與開放式網路架構比較

封閉式網路與開放式網路比較表		
比較項目	封閉式網路	開放式網路
連接網際網路	無	有
使用者身份	有限制性	通用性
網路服務	有限制性	通用性
實體電路	專屬電路	共用電路
IP資源	私有IP，可律定內部配置策略	由上游ISP或NIC分發
安全政策	集權式安全政策	分散式，由領域自行律定
路由資訊管控	可有效聚合路由資訊，並掌握路由記錄有效性。	無法簡化路由，無效路由依賴路由協定消除。

表 2 實驗驗測流路

實驗驗測流路					
實驗項次	IP 分配策略	入口過濾規則	攻擊主機數量與組成*		實驗編號
實驗一	IP 資源仿現行網際網路分配	路由器無入口過濾規則	1	E	Lab 1.1
				S	Lab 1.2
				W	Lab 1.3
			2	S,E	Lab 1.4
				W,E	Lab 1.5
				W,S	Lab 1.6
			3	W,S,E	Lab 1.7
					Lab 1.8
					Lab 1.9
實驗二	階層式 IP 資源 分配策略	區域路由器加入入口過濾規則	1	E	Lab 2-1.1
				S	Lab 2-1.2
				W	Lab 2-1.3
			2	S,E	Lab 2-1.4
				W,E	Lab 2-1.5
				W,S	Lab 2-1.6
			3	W,S,E	Lab 2-1.7
					Lab 2-1.8
					Lab 2-1.9
		末端路由器加入入口過濾規則	1	E	Lab 2-2.1
				S	Lab 2-2.2
				W	Lab 2-2.3
			2	S,E	Lab 2-2.4
				W,E	Lab 2-2.5
				W,S	Lab 2-2.6
			3	W,S,E	Lab 2-2.7
					Lab 2-2.8
					Lab 2-2.9
*** W,S,E 分別代表為攻擊主機 Attack_W, Attack_S, Attack_E**					

表 3 實驗一各監測點封包數量統計

實驗項次	Attack_N	Attack_W	Attack_S	Attack_E	Monitor_A	Monitor_B	Monitor_C
1.1	handler	0	0	10355453	264549	264549	264549
1.2	handler	0	10628864	0	489425	487139	487063
1.3	handler	10689201	0	0	263941	263941	263941
1.4	handler	0	10692788	10576034	490311	488255	487586
1.5	handler	10776964	0	10589517	487700	486868	486566
1.6	handler	10108630	10040002	0	465510	462792	462709
1.7	handler	10660807	11480086	11577183	494898	490338	489268
1.8	handler	10548401	10881597	10711220	491457	490313	490245
1.9	handler	10805349	10655421	10739862	492792	489719	489248

表 4 實驗二第一子項目各監測點封包數量統計

實驗項次	Attack_N	Attack_W	Attack_S	Attack_E	Monitor_A	Monitor_B	Monitor_C
2-1.1	handler	0	0	10123819	34017	34017	34017
2-1.2	handler	0	10086326	0	30999	30999	30999
2-1.3	handler	10293011	0	0	34451	34451	34451
2-1.4	handler	0	9833483	10184518	65732	65732	65732
2-1.5	handler	10712450	0	10413934	63112	63112	63112
2-1.6	handler	10153701	10222007	0	65566	65566	65566
2-1.7	handler	10167674	9994436	10030274	99715	99715	99715
2-1.8	handler	10388738	10001907	9968438	98631	98631	98631
2-1.9	handler	10155035	9855251	10128064	99336	99336	99336

表 5 實驗二第二子項目各監測點封包數量統計

實驗項次	Attack_N	Attack_W	Attack_S	Attack_E	Monitor_A	Monitor_B	Monitor_C
2-2.1	handler	0	0	10820948	1119	1119	1119
2-2.2	handler	0	9892999	0	1047	1047	1047
2-2.3	handler	10079800	0	0	967	967	967
2-2.4	handler	0	10038899	10109403	2215	2215	2215
2-2.5	handler	10063179	0	10362115	2135	2135	2135
2-2.6	handler	10006322	9979056	0	2176	2176	2176
2-2.7	handler	10325183	10251973	10538036	3385	3385	3385
2-2.8	handler	10158608	10140510	10444946	3426	3426	3426
2-2.9	handler	10347388	10420414	10391513	3466	3466	3466

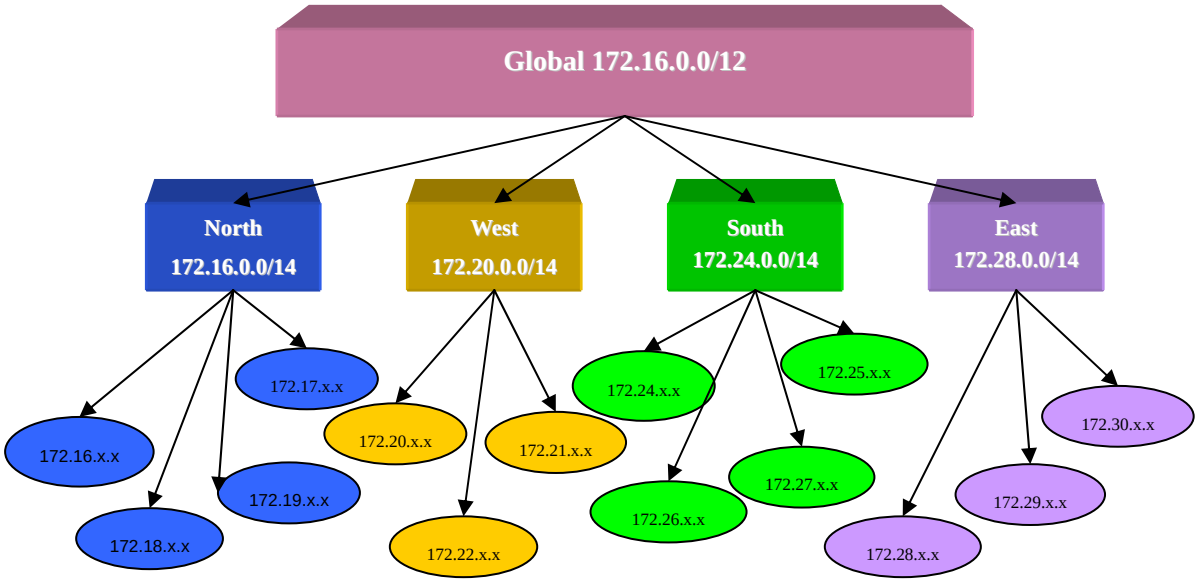


圖 1 實驗室階層式 IP 配置架構圖

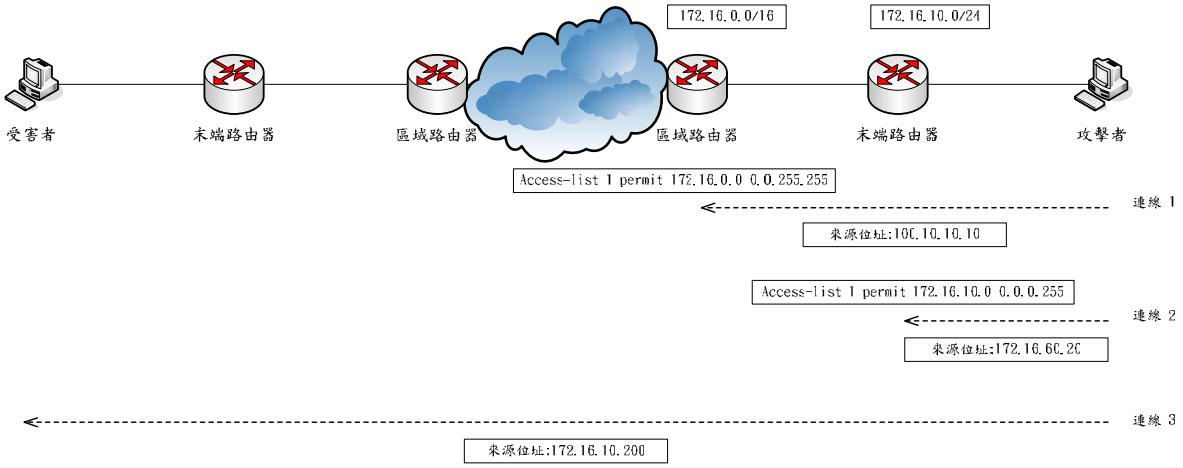


圖 2 入口封包過濾程序

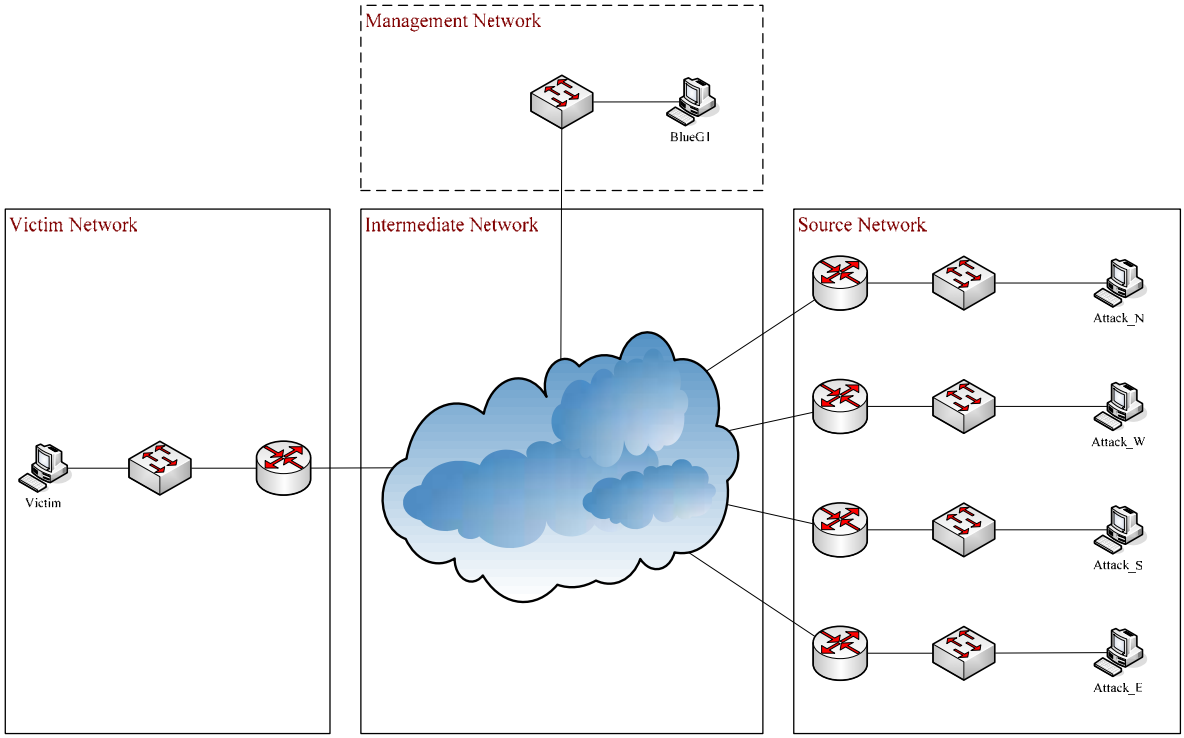


圖 3 實驗雛型網路模組示意圖

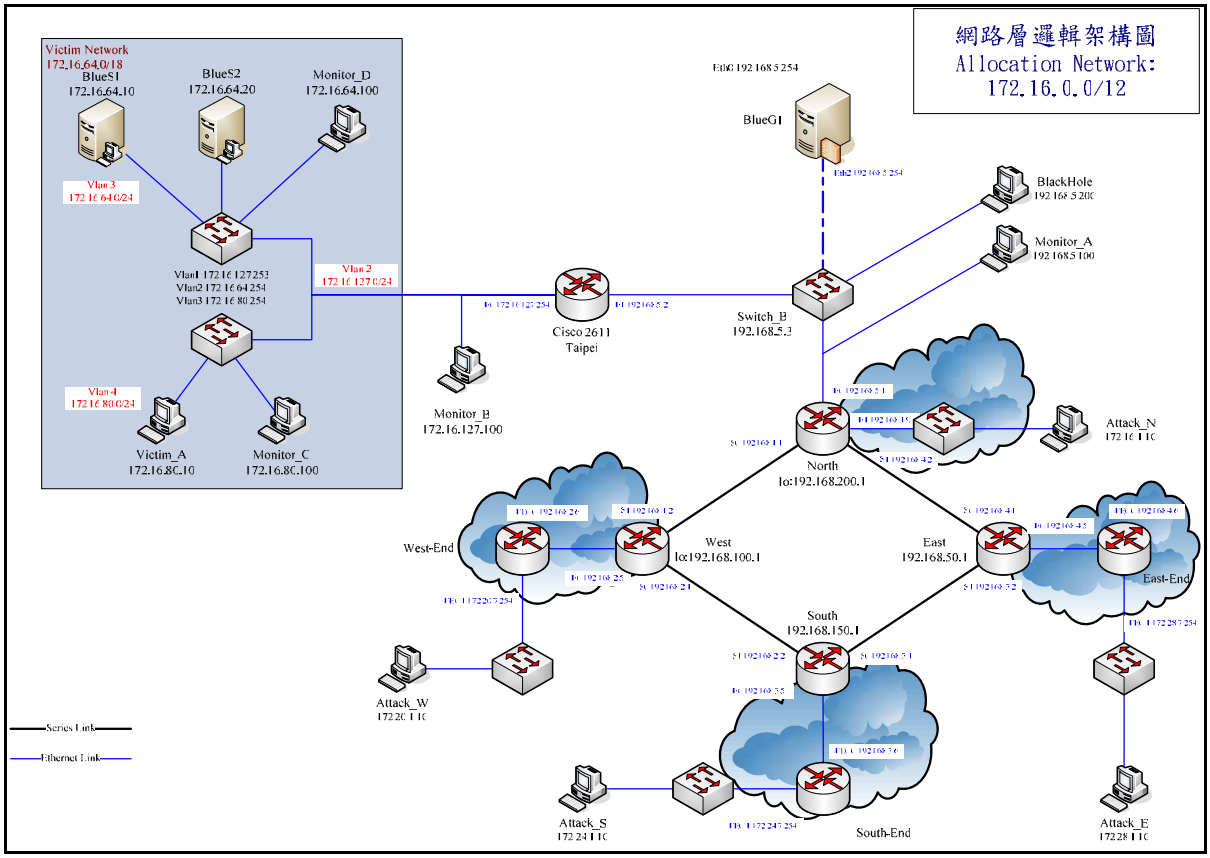


圖 4 網路層邏輯架構圖

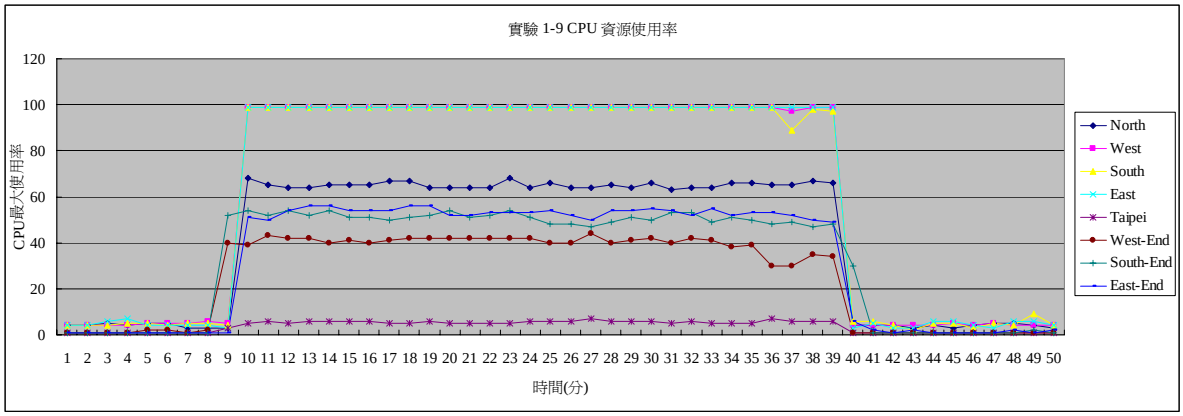


圖 5 實驗 1-9 路由器 CPU 資源使用率

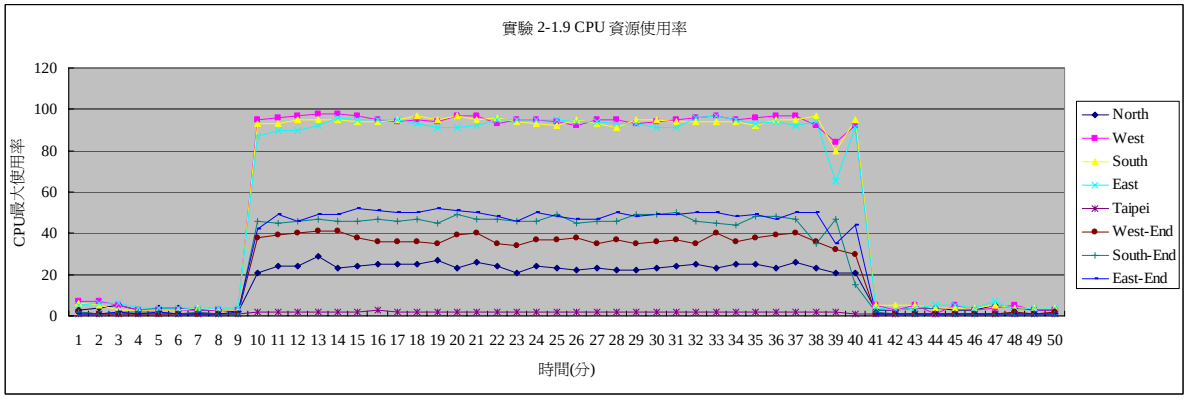


圖 6 實驗 2-1.9 路由器 CPU 資源使用率

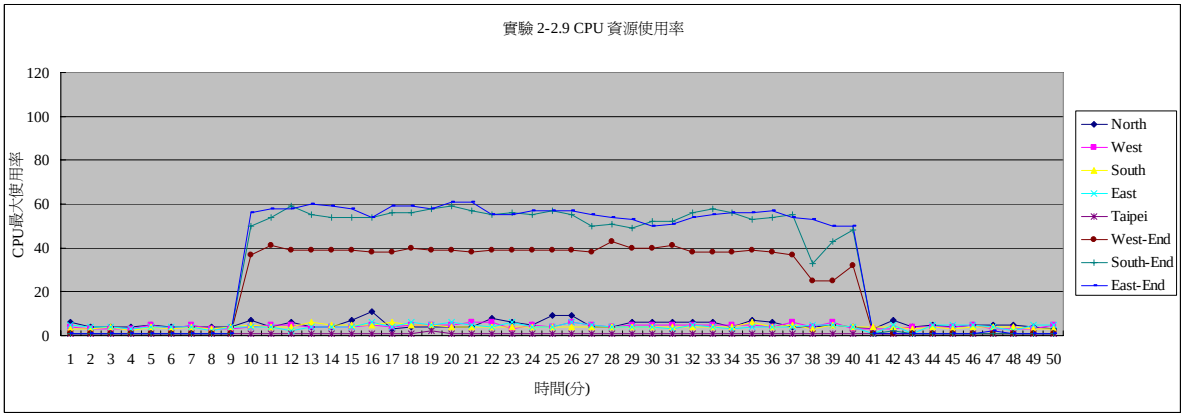


圖 7 實驗 2-2.9 路由器 CPU 資源使用率

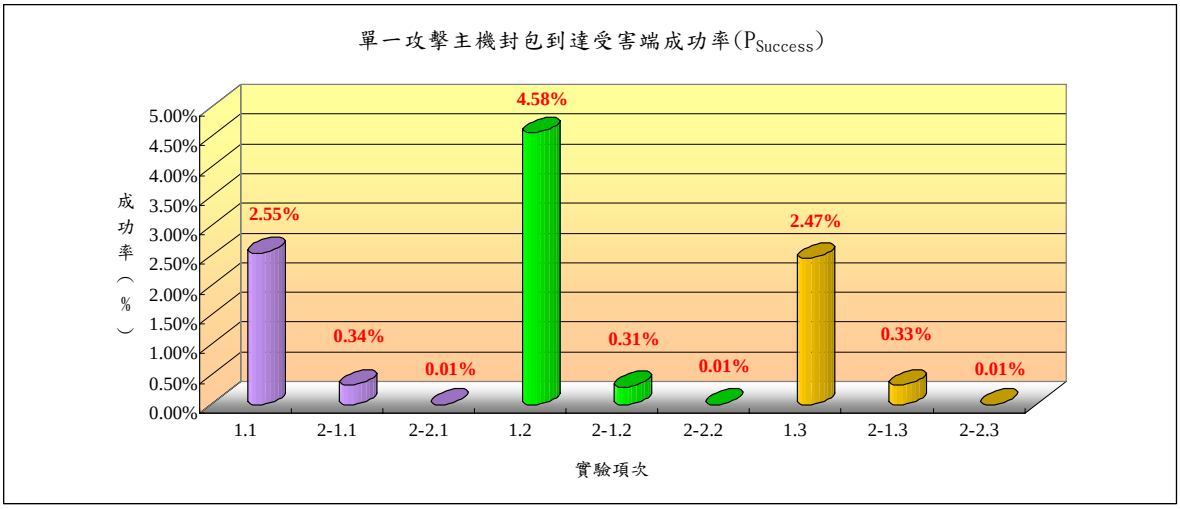


圖 8 單一攻擊主機封包到達受害端成功率

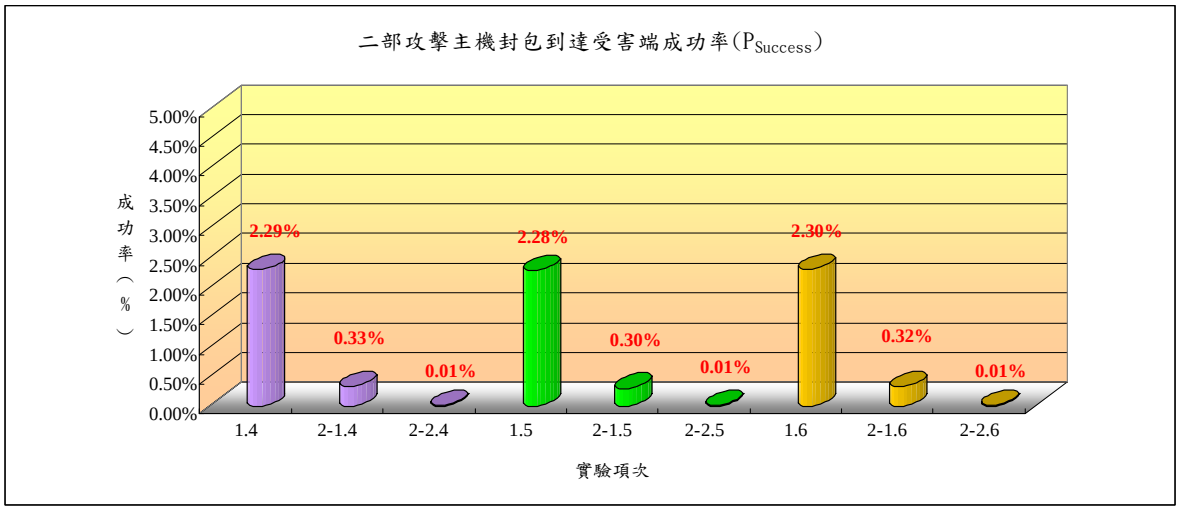


圖 9 二部攻擊主機封包到達受害端成功率

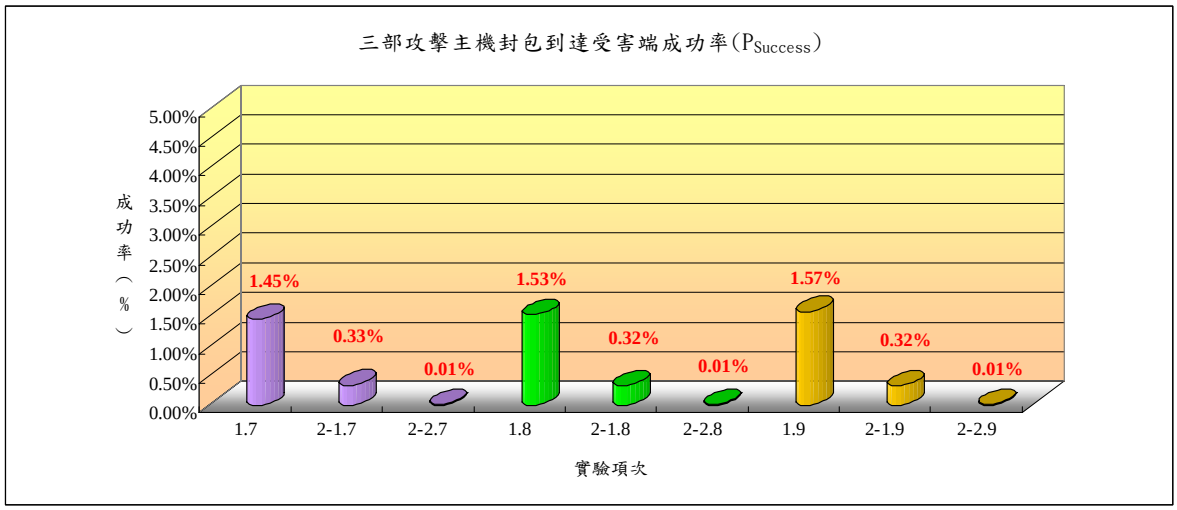
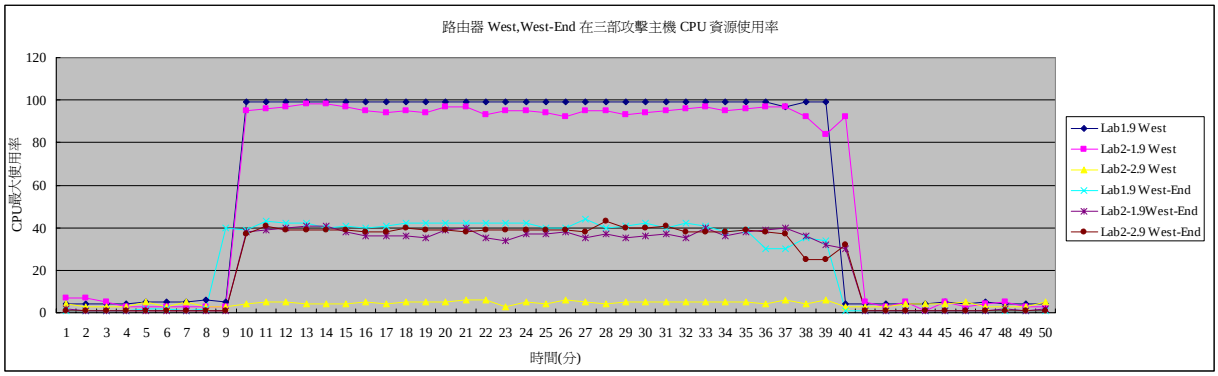
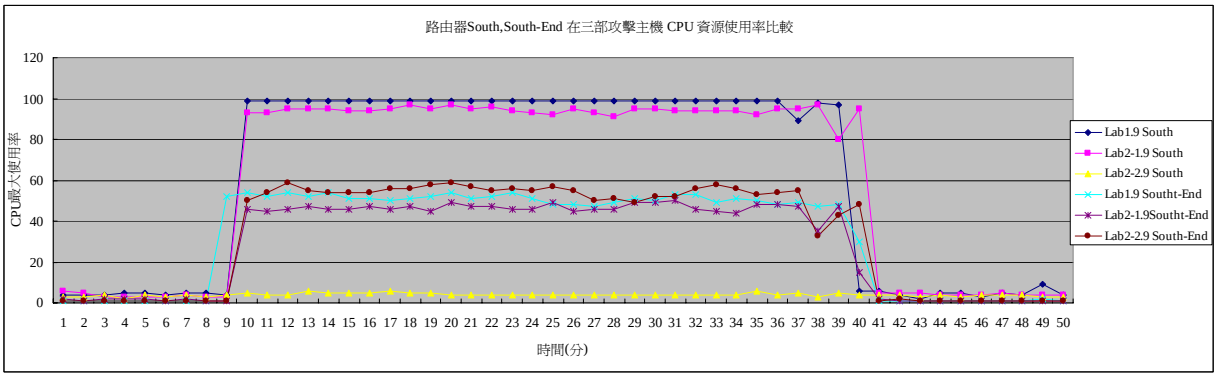
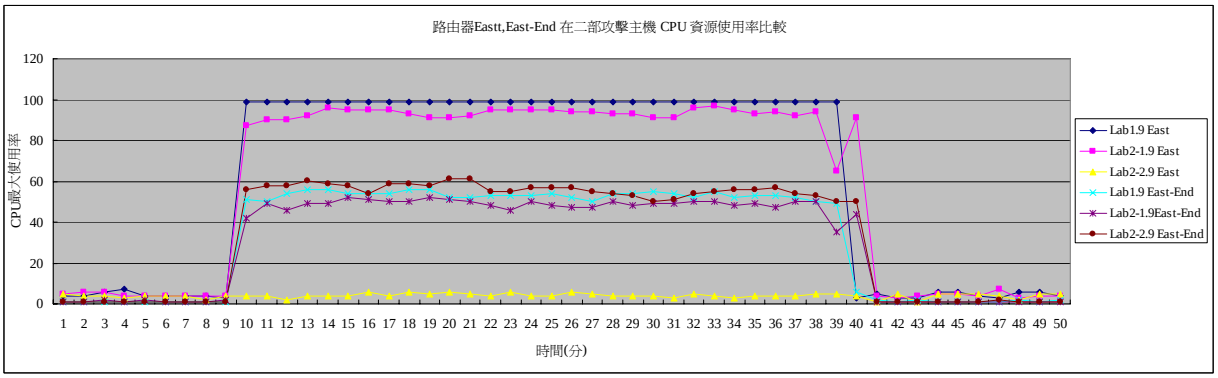


圖 10 三部攻擊主機封包到達受害端成功率







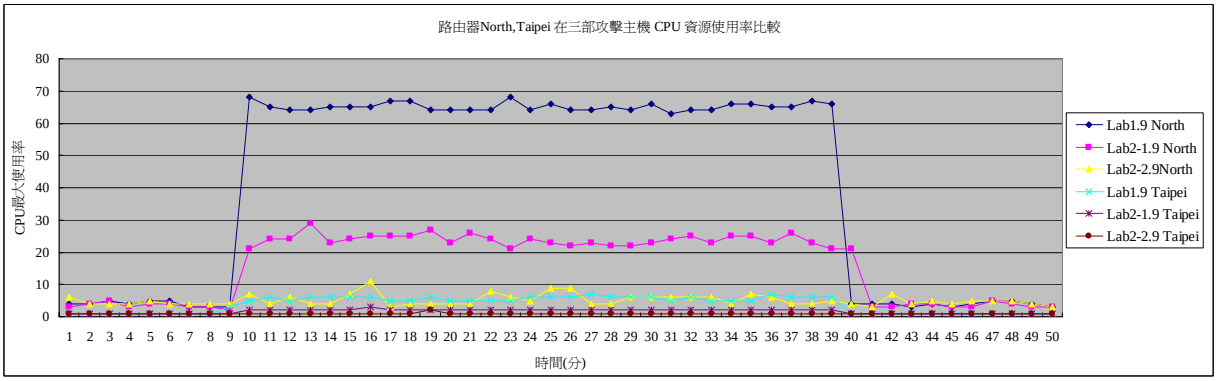


圖 11 三部攻擊主機處理器資源使用率的變化