國立交通大學

理學院科技與數位學習學程

碩士論文

簡易 ARP 欺騙攻擊偵測與防禦系統之實作

Simple system of detecting and defending the ARP spoofing

研 究 生：蕭瑛旗

指導教授：蔡文能　教授

中 華 民 國　九 十 九　年 六 月

簡易 ARP 欺騙攻擊防禦偵測系統之實作

Simple system of detecting and defending the ARP spoofing

研 究 生：蕭瑛旗　　Student：Ying-Chi Hsiao

指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國 立 交 通 大 學

理學院科技與數位學習學程

碩 士 論 文

A Thesis

Submitted to Degree Program of E-Learning

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Degree Program of E-Learning

June 2010

Hsinchu, Taiwan, Republic of China

中華民國九十九年六月

簡易 ARP 欺騙攻擊防禦偵測系統之實作

學生：蕭瑛旗　　指導教授：蔡文能

國立交通大學理學院科技與數位學習學程

摘　要

網路傳輸過程中常用到的位址解析協定(Address Resolution Protocol，ARP)以便從網路位址(IP address)查出實體位址(physical address; MAC address)，用於製作要傳送的封包(packet)。然則 ARP 存在著驗證不嚴謹的漏洞，駭客(hacker)開始開發 ARP 欺騙(ARP Spoofing)為基礎的攻擊程式。攻擊程式可以在交換式乙太網路上實現網路監聽，也可以阻斷網路連線而造成阻斷服務攻擊(DoS)。這些程式不但在網路上容易取得，而且操作容易，嚴重威脅區網上使用者的資訊安全，更是網路管理者要煩惱的一大問題。

本論文提出一個可以抵抗 ARP 欺騙攻擊的方法並實作出可用在區網中管理 IP 之使用的系統。本系統透過偵測主機的 ARP Table 收集區域網路中所有的電腦主機 IP、MAC 對應關係，並建立資料庫。憑藉著資料庫中正確的 IP 與 MAC 對應關係，以 ARP 欺騙的手法來修正被 ARP 欺騙攻擊的主機的 ARPTable 表，讓被欺騙攻擊的之主機在傳送封包時，能將封包傳送到正確的主機位址，避免傳輸資料被監聽或電腦主機被阻斷上網。

關鍵字：位址解析協定、實體位址、驗證、駭客、ARP 欺騙、網路監聽、阻斷服務攻擊

Simple system of detecting and defending the ARP spoofing

Students：Ying-Chi Hsiao　　Advisor：Wen-Nung Tsai

Degree Program of E-Learning
College of Science
National Chiao Tung University

ABSTRACT

Address Resolution Protocol (ARP) is a protocol used by hosts to map network address (IP address) into physical address (MAC address) when preparing the Ether frame for network transmission. Because of the protocol flaws, it is difficult to verify the sender of an arp packet. The hackers have begun developing the attack tools based on ARP spoofing. Some attacking tools are used to do network sniffing. Some tools are used to block the communication and thus results in a Denial of Service (DoS). What is worse, it is very easy to find and download these attacking tools from the Internet. Users with bad intention might use these tools to annoy the network admisistrator.

In this thesis, we proposed a method to resist ARP attack and implementd it as a web-based system. The system can be used in a local area network. The system examines the ARP table, collects the map of IP and MAC and then creates the database. With the database, the system can check the sender address of an ARP packet. It will send a correct ARP packet to fix the problem when it finds a wrong ARP reply packet with wrong mapping of IP and MAC. As a result, the system can defend the hosts in the LAN so that the sniffing and the Denial of Service (DoS) attack won't harm the computer hosts in the LAN.

Keywords：ARP、MAC address、Authentication、Hacker、Spoofing、network sniffing、DoS attack

誌　謝

首先誠摯的感謝指導教授蔡文能教授，教授細心的教導使我得以一窺領域的深奧，不時的討論並指點我正確的方向，使我在這些年中獲益匪淺。老師對學問的嚴謹更是我輩學習的典範。

感謝建德學長以過來人的身份給我指導與鼓勵，且總能在我迷惘時為我解惑，也感謝興能、真神、丁榮、茂南同學的幫忙，恭喜我們順利走過這兩年。

老婆在背後的默默支持更是我前進的動力，沒有老婆的體諒、包容，相信這兩年的研究所生涯會倍加辛苦；有老婆的支持，我才可以無後顧之憂地完成學業。

目　　錄

表目錄

圖目錄

第一章 緒論

寬頻網路的普及與網路應用層面的推陳出新，人們漸漸習慣使用電腦網路來決解生活上的問題：上網購物、信用卡消費、網路銀行轉帳、網路社交活動……等。人們愈來愈依賴電腦網路的便利，我們的個人隱私資料常常透過網路傳輸，資料的保全也因此變得愈來愈重要。駭客常常利用電腦網路存在的漏洞，對網路上資料的傳輸透過駭客軟體實施監聽的動作；透過監聽網路上傳輸的資料，便可以獲取他人隱私資料：帳號密碼、信用卡卡號被側錄竊取，網站上的個人資料遭盜用，這些事件時有所聞。

由於資安設備功能的進步，大多數區網外部的攻擊被有效的阻隔，也因此網路網攻擊型態也因而改變；網路安全問題由區網外部轉移到區網內部。在大部份的機關團體所使用的網路拓撲結構以多階層的星狀拓撲(樹狀拓撲)為主，使用 UTP 雙絞線串接乙太網路交換器(Ethernet Switch)與電腦節點，也因此改善了早期以集線器(Hub)連結個人電腦時，網路廣播封包容易被竊聽的問題。

但是因為網路傳輸過程中常用到的位址解析協定(Address Resolution Protocol，ARP)存在著驗證不嚴謹的漏洞，駭客開始開發 ARP 欺騙(ARP Spoofing)為基礎的攻擊程式。攻擊程式可以在交換式乙太網路上實現網路監聽，也可以造成 DoS 攻擊阻斷網路連線上網。這些程式容易操作且在網路上容易取得，嚴重威脅區網上使用者的資訊安全，更是網路管理者要煩惱一大問題。

1.1 研究動機

在早期的乙太網路使用一般匯流排(bus)的網路拓撲搭(topology)與集線器(hub)連串連網路上的電腦，電腦之間的訊息傳送，基本上是以廣播(broadcast)方式來傳送；因此網路上的裝置傳送的封包，都被網路上其它的裝置所接收。接收到封包後，會把該封包的訊框(Frame)的目地端 MAC 位址與本機的 MAC 位址做比對，如果一樣的話，此封包則會被本機所接受；如果比對結果不一樣，則會將此封包丟棄不理。在這種網路拓撲環境下，只要想辦法讓網路卡去比對 MAC 位址的結果都相符，就可以竊聽(sniff)到傳送到網路卡的的封包。

使用集線器造成網路竊聽非常容易，所以現在的乙太網路環境都以交換器(switch)來取代集線器。封包會在第一次傳送時廣播，等傳送封包後，就會在交換器上建立的 port 和 MAC 位址的對照表，之後有其它封包要透過此交換器傳送到

相同的電腦時,就不會再使用廣播方式去傳輸資料,而是按照交換器的 port 和 MAC 位址對照表，直接將封包傳送到目的主機所使用的 port。所以在交換器為主的乙太網路下，除了廣播封包外，電腦就只能接收到傳給自己本身的封包；傳統的封包監聽技術已不可行。ARP 欺騙((Address Resolution Protocol Spoofing)技術的出現是一個令網站者很頭痛的問題，除了在交換式的乙太網路上可以監聽封包外，還可以形成阻斷式攻擊(Denial of Service; DoS) 癱瘓網路上的電腦甚至是整個網路。

在學校的區域網路(LAN)中，常常遭受病毒的攻擊，病毒更透過 USB 隨身碟或網頁掛馬的方式在校園網路中傳播；或有心人事為了讓自己使用網路上大部份的頻寬，使用了駭客工具軟體，阻斷別人上網；更有在校園網路中使用監聽程式來窺探他人穩私。在以 ARP 欺騙為基礎的駭客工具中，甚至有宣稱可以拿來做網路管理之用途；如果在學校區域網路中，有太多人拿這些隨手可得的駭客工具，行地下管理員之實，那整個學校網路就會亂無法紀。

1.2 研究目的

ARP 欺騙(ARP Spoofing)的原理是應用一個人工編造的 ARP 封包來改變電腦或區域網路設備中的 ARP 快取表(ARP Table)，影響電腦要與其他電腦傳輸路徑。如果編造的 ARP 封包所包含的來源端與目的端的 IP 與 MAC 對應關係是錯誤的，封包傳送路徑也因為被操控，容易被拿來做阻斷攻擊或網路竊聽；但如果編造的 ARP 封包裡面所包含的來源端與目的端的 IP 與 MAC 對應關係是正確的，則可以確保網路中封包傳送路徑的正確性。

試想如果以 ARP 欺騙技術試做一個網路管理工具，並應用相關技術來有效管理校園網路，不但可以將原本是區域網路的漏洞轉化為管理校園網路的一項利器，減輕管理者的工作負擔，還可以讓無法負擔價格昂貴的網路管理設備之學校節省開銷，使用極少的成本，達到網路管理的最大效益。

1.3 研究方法與範圍

本研究設定在國小校園網路，以 ARP 欺騙攻擊軟體為研究對象；另因小學經費普遍不足，故本研究捨棄使用功能強大的網路硬體設備，只在 Open source 的 FreeBSD 作業系統上，使用 C 語言搭配 libpcap 及 libnet 函式庫來開發程式，利用 ARP 欺騙技術反制常見的 ARP 欺騙的駭客程式，並實做成一個 ARP 欺騙攻擊防禦與偵測系統。最後在作者本身服務的小學校園網路內實驗，並測試改進其成效

至一定的水準：至少維持校園網路可以正常運作，並可找出使用 ARP 欺騙攻擊的電腦主機。

1.4 論文架構

本論文共分六章節，第一章為研究動機與目的。第二章介紹相關背景知識包含 IP 與 MAC 位址、ARP 協定、ARP 欺騙技術、封包的擷取與發送。第三章探討與本研究相關的期刊論文與研究，分成以 TCP/IP 程式實驗來運用網路封包擷取與封包偽造發送，及在交換式乙太區域網路環境下，封包如何監聽，並說明可行的 ARP 欺騙攻擊解決方法。在第四章中將闡述本論文反制 ARP 欺騙的構想與程式設計流程。第五章中將展示本論文實作之 ARP 欺騙防禦與偵測系統及其在實驗環境中之實測結果，期本論文所提方法可行。第六章為結論及未來研究方向。

第二章 背景知識

國際標準組織(International Standards Organization,簡稱 ISO)[1]在 1984 提出開放式系統互連參考模式(Open System Interconnection Reference Model，簡稱 OSI 模型)。在 OSI 模型中，提供一個有彈性的概念性架構，協調各種網路系統之間通訊。TCP/IP[1]起源於 1973 年，由文頓·格雷·瑟夫（Vinton Gray Cerf）與羅伯特·埃利奧特·卡恩（Robert Elliot Kahn）所定義出來，1984 年由美國國防部將 TCP/IP 定為所有計算機網路的標準。由於 TCP/IP 通訊協定在 Internet 上廣泛的被應用，並成為商業使用的主要架構，使得 OSI 模型只是一個理想架構，從未被完全實現出來。我們把 OSI 七層模式與 TCP/IP 通訊協定組的四層做對照比較(見圖 2-1)，其原理與概念相當。

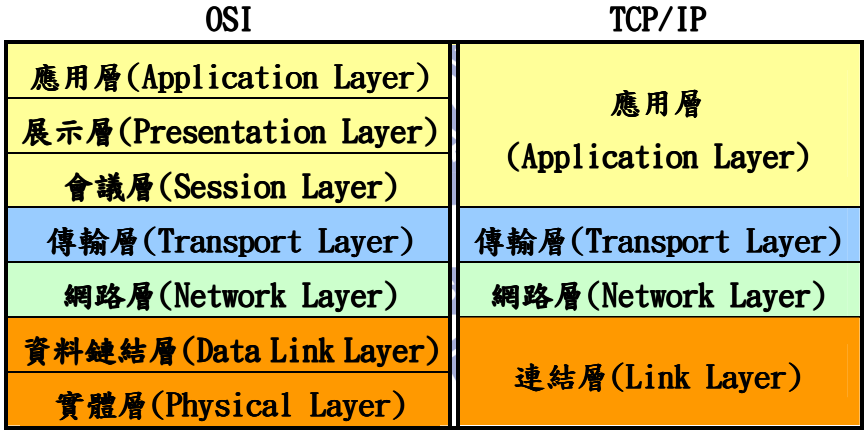


圖 2 - 1 OSI 與 TCP/IP 分層對照

2.1 MAC 與 IP 位址

兩台電腦之間訊息的傳遞，中間可能經過多個中繼站，而電腦與中繼站或中繼站與中繼站之間訊息的傳送，通常只有用到 OSI 網路分層模型的下面三層(如圖 2-2)。而其中所用到的位址，只有實體位址(physical address)與邏輯位址(logical address)，在乙太網路中，實體位址就是 MAC 位址，而邏輯位址就是 IP 位址。

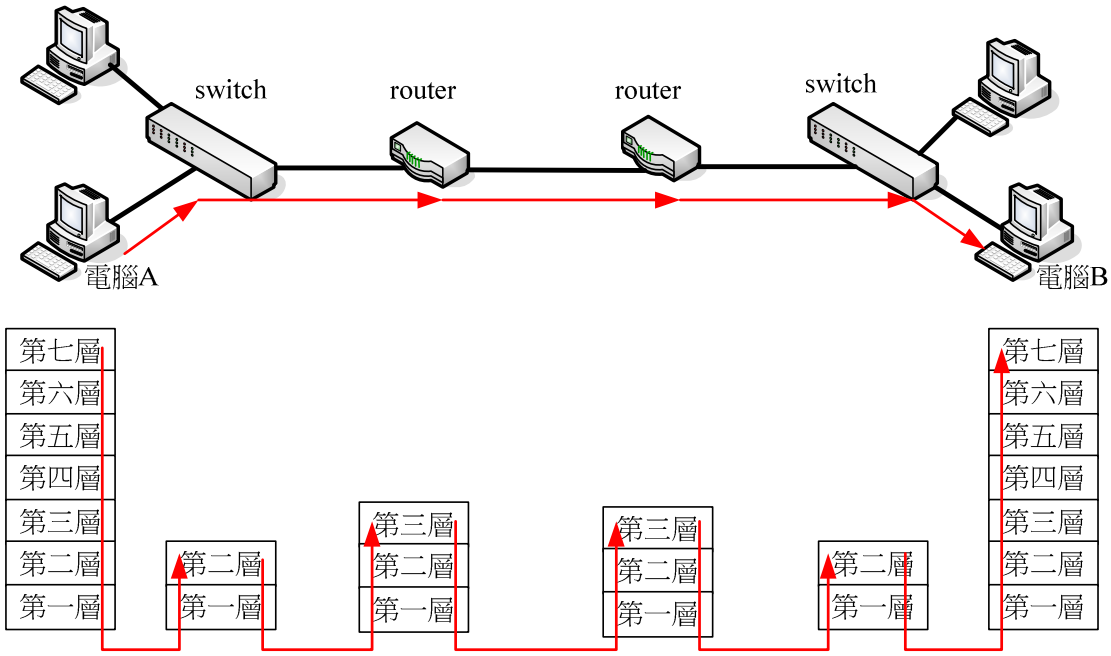


圖 2 - 2 電腦通訊使用 OSI 模型的層級

2.1.1 MAC 位址

OSI 模型中資料鏈結層的實體位址，也就是在乙太網路中 MAC 位址，是在區域網路中一個節點(如：電腦或路由器)的位址，其的長度是 48 位元，一般表示為 12 個 16 進位制的數，每 2 個數之間用冒號區隔；前 24 位元由 IEEE 分配予網路硬體製造商，後 24 位元則是由造製商自行分配，例如：00:25:D3:7D:66:13 這個 MAC 位址，前 24 位元 00:25:D3 為 IEEE 所配給的，後 24 位元 7D:66:13 代表製造商網路產品系列號。MAC 位址在製造時寫在網路設備硬體內部，而且製造商所生產的網路設備 MAC 位址不會重覆，也就是說每個乙太網路設備都配給一個世界上唯一的 MAC 位址。

2.1.2 IP 位址

MAC 位址用於區域網路中不適用於網際網路，所以在 OSI 的網路層中定義網路路由與定址，讓資料可以在網路間傳遞，其所依賴的是 IP 位址；在網際網路中使用 IP 位址來為網路上的主機做定址，所以封包裡面記錄會著封包傳送的來源與目的地，所以在網際網路上 IP 具有獨特性(unique)，資料傳輸才能夠正確的傳送與接收。在目前常用的 IP(IPv4)位址其長度為 32 位元，通常分成四組 8 位元，每一組以十進位數字來表式，每個數值介於 0 到 255 之間，各組數值間用小數點來分隔，例如：163.30.0.1。

2.1.3 網路傳輸模式

網路傳輸模式分下列三種模式：

- 單點傳播模式(unicast)：這是交換式乙太網路上最常見到的傳輸模式，此種方式是直接將資料封包傳送到網路上的某台主機。ARP 回應封包就是使用單點傳播模式。
- 群組廣播模式(multicast)：此種傳播方式是同一時間將封包傳送到網路上的某些主機。
- 廣播模式(broadcast)：此種傳播方式是同一時間將封包傳送到網路上的每一台電腦。ARP 詢問封包的傳播方式就是使用廣播模式。

2.2 ARP 通訊協定

在 TCP/IP 協定架構中提到，網路上每一個節點使用邏輯位址，讓彼此之間傳輸資料辨認身分用。封包實際的傳輸還是要透過網路介面卡來接收與傳送，而網路介面卡看不懂 IP 位址，只看得懂網路實體位址，也就是說實體位址是一個區域性位址，在區域網路的傳輸中用來辨認身分用的；在乙太網路上封包傳遞前會加上網路訊框(Ethernet Frame)，封包在傳送時，訊框中記錄著傳送目的地的實體位址，這樣子封包才能透過實體層傳輸，經由網路介面卡來傳收與傳送。所以上層網路應用程式只要知道封包所要傳送目的地的 IP 位，再透過機制將 IP 位址對應為 MAC 位址，有了實體位址，資料封包就可以正確的與目的端電腦做點對點的通訊；這個機制就是 ARP(Address Resolution Protocol)協定。

2.2.1 ARP 的詢問封包與回應封包

當區域網路上的電腦節點要與在同一個區域網路上的另一台電腦節點通訊時，需要知道對方的實體位址，因此在區域網路上廣播一個 ARP 的詢問封包(query packet)，封包中記錄著廣播這封包的電腦節點之實體位址、IP 與要詢問實體位址的電腦節點的 IP 位址。

這個區域網路上的每個電腦節點都會收到這個 ARP 詢問封包，而電腦節點的 IP 位址如果與 ARP 詢問封包所問的 IP 位址一樣，就會回應一個 ARP 的回應封包(response packet)。這個回應封包裡面就會包含傳送者(被詢問者)的 IP 位址、實體位址與接收者(詢問者)的 IP 位址與實體位址。這個封包是以單點傳播的方式直接傳送給詢問者，裡面就會有詢問者所要的實體位址。

ARP 的詢問與回應的概念，可以由圖 2-3 與圖 2-4 說明。圖中有兩個區域網路，

其中區域網路一中當電腦 B 要傳送資料封包給電腦 A 時，因為電腦 B 只知道電腦 A 的 IP 位址(192.168.1.1)但不知道它的 MAC 位址，於是電腦 B 就廣播一個 ARP 詢問封包，詢問區域網路一上的所有電腦 IP 位址為 192.168.1.1 的 MAC 位址是多少，而這個封包也會含有電腦 B 的 IP 位址與 MAC 位址。電腦 C、電腦 D 與路由器接收到這個廣播封包，因為 IP 位址不是自己的 IP 位址，所以會直接丟棄此封包；而電腦 A 接收到這個 ARP 詢問封包，知道是在詢問自己的 MAC 位址，因此回送一個 ARP 回應封包給電腦 B，這個封包上包含了電腦 A 的 MAC(00:10:2E:34:11:11)位址，這樣子電腦 B 就能準確的傳送資料封包給電腦 A 了。

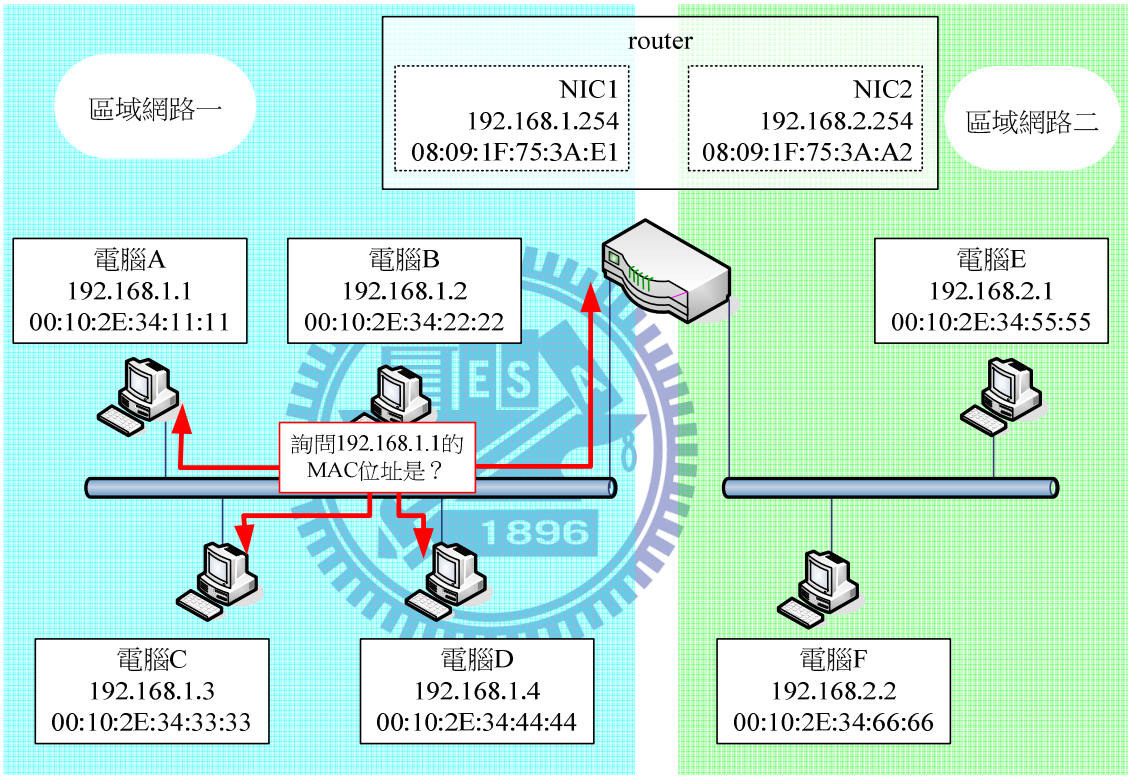


圖 2 - 3 電腦 B 廣播 ARP 詢問封包

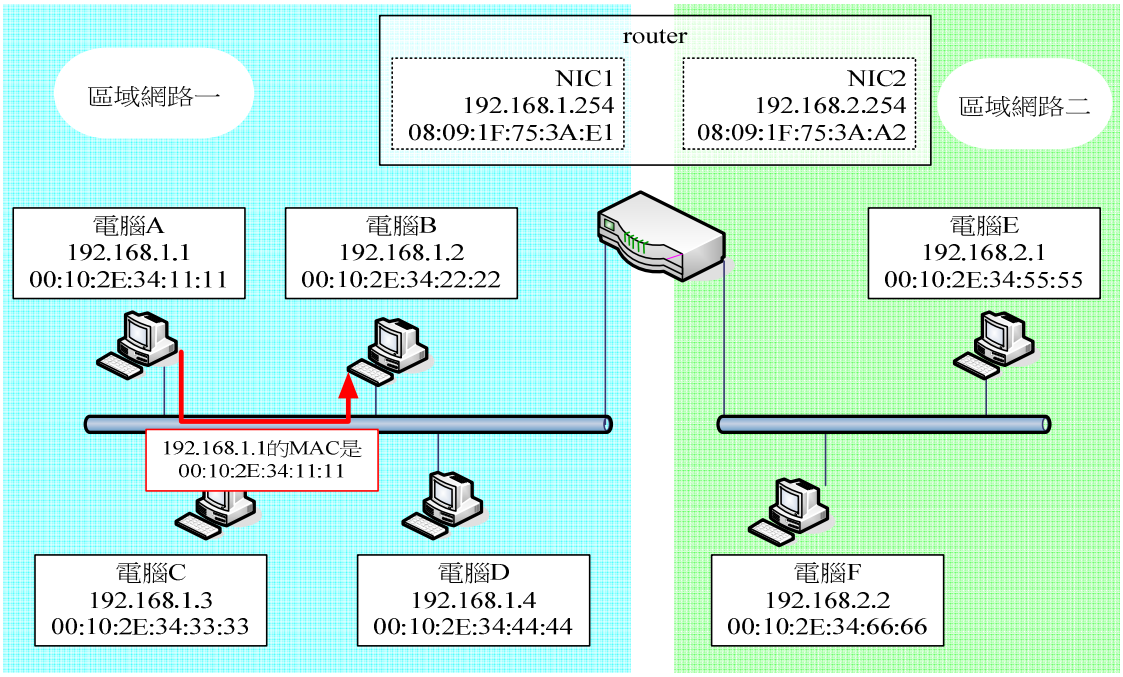


圖 2 - 4 電腦 A 送回 ARP 回應封包給電腦 B

2.2.2 ARP Table

由於網路上傳遞一個檔案，往往要把它切割成多個資料封包來傳送，如果傳送每個封包前都要廣播 ARP 詢問封包一次，傳遞速度必會拖慢。由於網路上主機的 IP 位址與 MAC 位址變動的頻率不大，短時間內詢問的結果通常得到的答案都一樣，所以作業系統會建立 ARP 的快取(Cache)來儲存區域網路中電腦的 IP 位址與 MAC 位址的對應表(ARP Table)，這樣就不用每次要傳資料前，都要做一次 ARP 詢問封包的廣播，而且先從 ARP Table 中找看看是否有要找的 IP 對應的 MAC 位址記錄，有就直接傳送資料封包給目的端的主機，如果找不到記錄，才廣播 ARP 詢問封包。

圖 2-3，當電腦 B 收電腦 A 的 ARP 回應封包時，會就電腦 A 的 IP 位址與 MAC 位址暫存在 ARP Table 中。除此之外，圖 2-4，當電腦 B 廣播 ARP 詢問封包時，因為此 ARP 詢問封包中含有電腦 B 的 IP 位址與 MAC 位址，所以接收到這個封包的所有電腦，也都會在自己的 ARP Table 中儲存一筆電腦 B 的 IP 位址與 MAC 位址的對應資料。

主機 IP 位址與 MAC 位址的對應有可能改變，所以 ARP Table 裡的資料有可能會無法即時的變更資料，必需等到 IP 位址與 MAC 位址對應變更的這台主機廣播 ARP 詢問封包或獲得它 ARP 回應封包時，或人工設定，才會更新資料。ARP Table 裡每一筆紀錄稱為一個 entry，ARP entry 的型態(type)有下列兩種：

1、動態(Dynamic) entry：這類型的 entry 具有彈性，接收到 ARP 封包時就會記錄起來，甚至覆蓋原來的紀錄；每一個 entry 存活一段的時間後，會自動刪除。

2、靜態(Static) entry：這類型的 entry 不會因為 ARP 封包而變更其紀錄，存活時間無限制，除非主機重新開機，或資料被人工重新設定。可以借由 arp －s 的指令將靜態 entry 加入 ARP Table 中(見圖 2-5)。

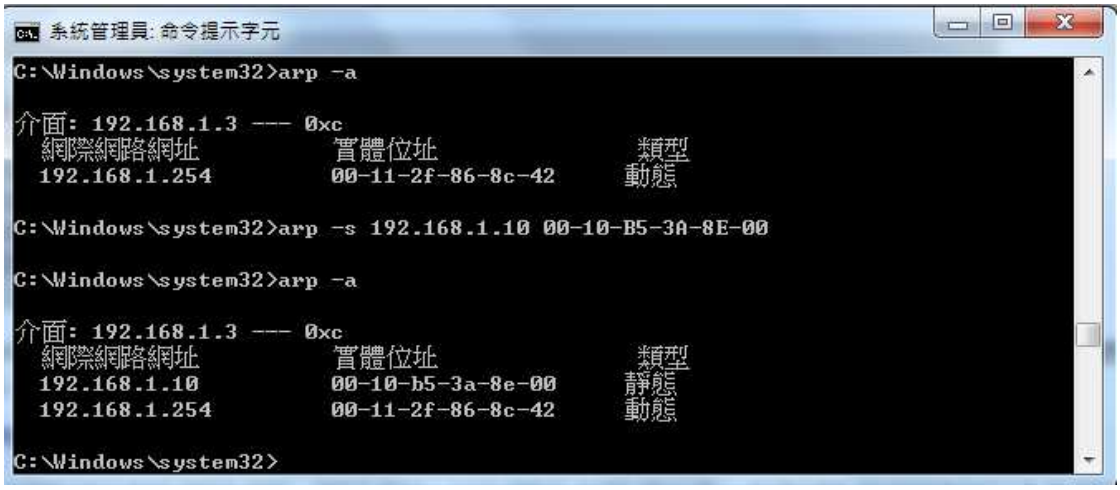


圖 2 － 5 以 ARP 指令查看 ARP Table 與增加一筆靜態 ARP entry

2.2.3 ARP 封包結構

ARP 為了能在不同的網路類型中負起位址解析的工作，因此封包的每個欄位長度會因網路類型的不同而有所不同，所以 ARP 封包並沒有一個固定的大小，但是所有的 ARP 封包架構都很大同小異。圖 2-6 是乙太網路 IPv4 的 ARP 封包的封包格式及欄位定義，封包的大小為 224 位元(28 Bytes 位元組)。

Internet Protocol (IPv4) over Ethernet ARP packet		
Bit Offset	0 – 7	8 – 15
0-15	Hardware type (HTYPE)	
16-31	Protocol type (PTYPE)	
32-47	Hardware address length (HLEN)	Protocol address length (PLEN)
48-63	Operation (OPER)	
64-79	Sender hardware address (SHA)	
80-95		
96-111		
112-127	Sender protocol address (SPA)	
128-143		
144-159	Target hardware address (THA)	
160-175		
176-191		
192-207	Target protocol address (TPA)	
208-223		

圖 2 － 6 ARP 封包結構
資料參考 WIKIPEDIA

ARP 封包結構有九個欄位，各欄位的說明如下：

- **Hardware type(硬體類型)：**
  這個欄位大小為 16 位元，定義執行 ARP 通訊協定的網路類型，以 16 進制數值記錄。例如：乙太網路的數值為 0X0001。
- **Protocol type(通訊協定類型)：**
  這個欄位大小 16 位元，定義 ARP 解析的通訊協定類型，以 16 進制數值記錄。例如：IPv4 通訊協定的數值為 0X0800。
- **Hardware address length(硬體位址長度)：**
  這個欄位大小為 8 位元，定義實體位址的長度，以 16 進制數值記錄，單位是位元組。例如：乙太網路的實體位址長度為 0x06 位元組。
- **Protocol address length(通訊協定位址長度)：**
  這個欄位大小為 8 位元，定義邏輯位址的長度，以 16 進制數值記錄，單位是位元組。例如：乙太網路的 IPv4 位址長度為 0X04 位元組。
- **Operation(操作)：**
  這個欄位大小為 16 位元，定義 ARP 封包的型態，以 16 進制數值表示，ARP 詢問封包為 0X0001，ARP 的回應封包為 0X0002。
- **Sender hardware address(發送者的硬體位址)：**
  這個欄位大小不固定，定義傳送者的實體位址。如果使用乙太網路，則本欄大小為 48 位元。
- **Sender protocol address(發送者的通訊協定位址)：**
  這個欄位大小不固定，定義發送者的邏輯位址。如果是 IPv4 通訊協定，則本欄大小為 32 位元。
- **Target hardware address(目標的硬體位址)：**
  這個欄位大小不固定，定義接收者的實體位址。如果使用乙太網路，則本欄大小為 48 位元；如果是 ARP 詢問封包，這個欄位的值為 00:00:00:00:00:00。
- **Target protocol address(目標的通訊協定位址)：**
  這個欄位大小不固定，定義接收者的邏輯位址。如果是 IPv4 通訊協定，則本欄大小為 32 位元。

2.2.4 訊框格式與 ARP 封裝

在資料鏈結層裡資料傳輸的來源與目的都以訊框為依據，下圖 2-7 為乙太網路訊框的結構。ARP 封包要傳送前必須被封裝在資料鏈結層的訊框裡，如此才能傳送到想傳送的實體位址。這裡對特別提的如果訊框的資料欄位封裝的是乙太網路 ARP 的封包，這時類別的欄位數值為 16 進制的 0X0806；而如果是 ARP 詢問封包，

目的位址為 FF:FF:FF:FF:FF:FF，如此則可以在區域網路中以廣播的方式傳送，與前面所提的 ARP 詢問封包的目標實體位址(00:00:00:00:00:00)不同。

前導碼	目的位址 DST MAC	來源位址 SRC MAC	類別 0X806	資料 ARP 封包資料	檢查碼
8 位元組	6 位元組	6 位元組	2 位元組	46-1500 位元組	4 位元組

圖 2 - 7 乙太網路的訊框格式

2.3 封包偽造

在前面所提到的訊框是在乙太網路上傳遞封包的重要依據，訊框裡面的目的位址決定封包傳送到哪一台主機上。當目標位址為 FF:FF:FF:FF:FF:FF 時，則封包會傳遞到區域網路上的每一台主機，如果目標位址是 01:02:03:04:05:06，則封包會傳送到 MAC 位址為 01:02:03:04:05:06 這台主機，並且被這台主機的網卡接收。而 ARP 封包格式裡面含有發送者的 MAC 位址與 IP 位址，以及接收者的 MAC 位址與 IP 位址。當接收到 ARP 封包時，ARP Table 會記錄發送端的 MAC 位址與 IP 位址。

圖 2-8 是使用封包擷取軟體，擷取網路上 ARP 封包後，分析 ARP 封包裡面的資訊。我們可以很清楚看到擷取下來的訊框的部份裡面包含來源端(Src)為 00:50:56:f5:50:f4，而接收端(Dst)為 00:0c:29:20:53:11，類別為 806(ARP)；而在 ARP 封包的部份，發送端的 MAC 位址為 00:50:56:f5:50:f4、IP 位址為 192.168.137.2，而目標端的 MAC 位址為 00:0c:29:20:53:11、IP 位址為 192.168.137.128。

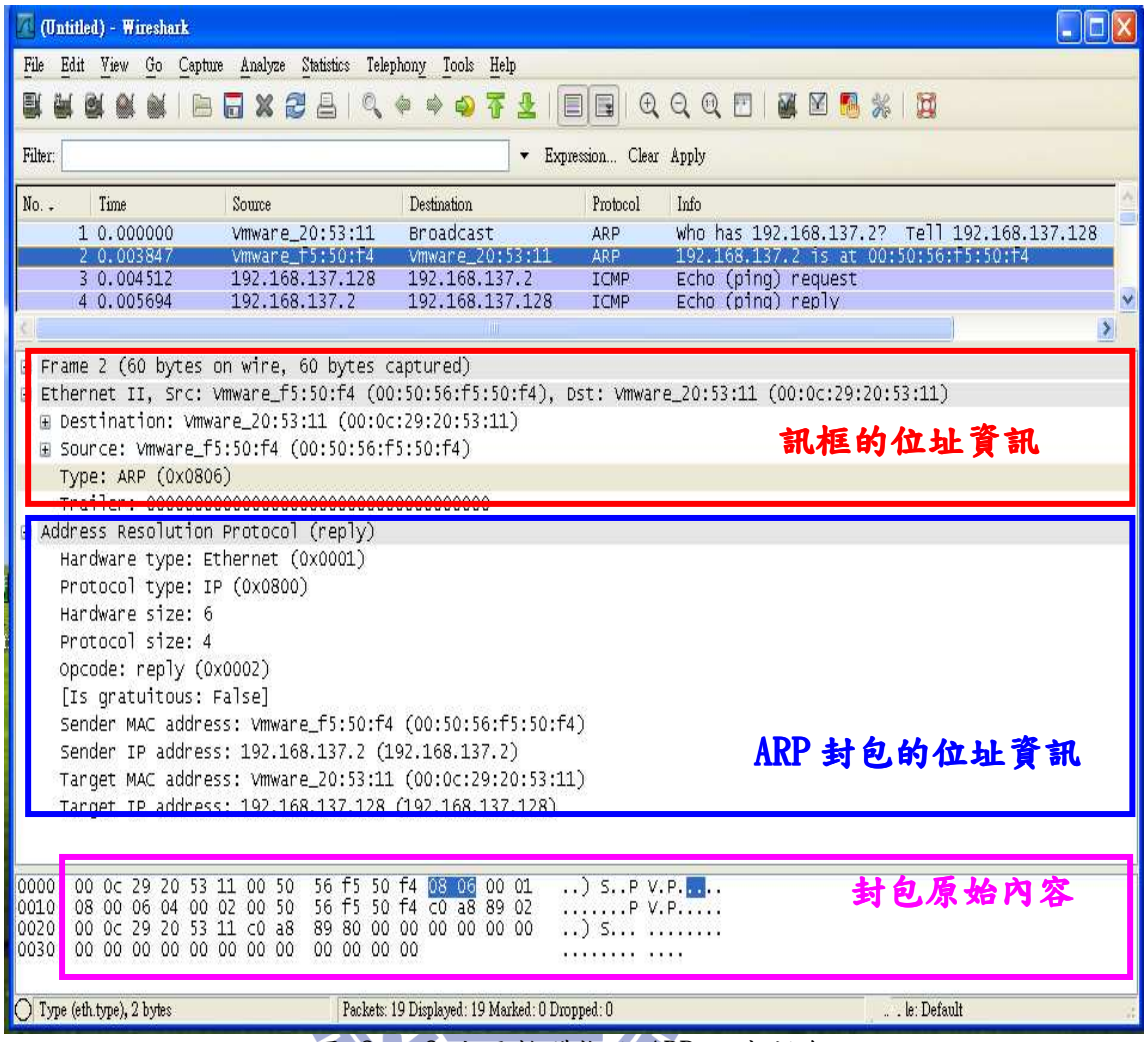


圖 2 - 8 使用軟體擷取 ARP 回應封包

封包偽造是駭客攻擊常用的手法，當駭客偽造訊框裡面的目的位址時，封包就會傳送到偽造的位置。如果 ARP 封包裡面的發送者 MAC 位址與 IP 位址被偽造，再透過偽造訊框的目的位址，就可以使用 ARP 欺騙攻擊區網上的電腦主機了。

2.4 ARP 欺騙攻擊

ARP 欺騙攻擊(ARP Spoofing)最主要是因為 ARP 封包存在著安全上的漏洞所造成，以下就針對 ARP 漏洞與本篇所要研究的中間人攻擊與阻斷攻擊來做說明。

2.4.1 ARP 漏洞

由上述 ARP 封包變更 ARP TABLE 紀錄與 ARP 封包結構我們可以明顯看出 ARP 的運作過程缺少了認證機制，接收到 ARP 詢問封包便把發送者的 IP 位址與 MAC 位址對應關係存到 ARP TABLE 中；如果接收到不是自己本發出的詢問封包而傳送回

來的 ARP 回應封包，也會將其 IP 位址與 MAC 位址的對應關係記錄到 ARP TABLE 中；如果我們偽造 ARP 封包中的 IP 位址與 MAC 位址的對應資料，並將此封包傳送到目標主機，該主機只能依接收到的封包裡的 IP 位址與 MAC 位址而紀錄到 ARP TABLE 中；如果 IP 位址與 MAC 位址的對應關係是錯誤的，就形成 ARP 欺騙攻擊了。以下說明 ARP 欺騙所形成的攻擊型態。

2.4.2 中間人攻擊

所謂中間人攻擊(Man in the middle，簡稱 MITM)就是在網路上通訊傳輸的兩台主機中間偷偷加上一個節點，如此這兩台主機所有的通訊傳輸資料都必需經由這個節點來傳送，而駭客便可以在這個節點上使用監聽軟體來竊聽兩台主機之通訊內容，進一步獲取機密資料。

主機 A 和主機 B 在區域網路中通訊(如圖 2-9)，主機 C 分別傳送偽造的 ARP 封包給主機 A 與主機 B，更改 ARP TABLE 裡面彼此的 IP 位址都對應到主機 C 的 MAC 位址，如此主機 A 要傳送資料給主機 B 時，會傳送到 MAC 位址為 01:e5:33:54:19:0C，而這個位址就是主機 C，同理主機 B 要傳給主機 A 時，也會傳給主機 C，主機 C 就成為中間人(如圖 2-10)，並可進行竊聽了。

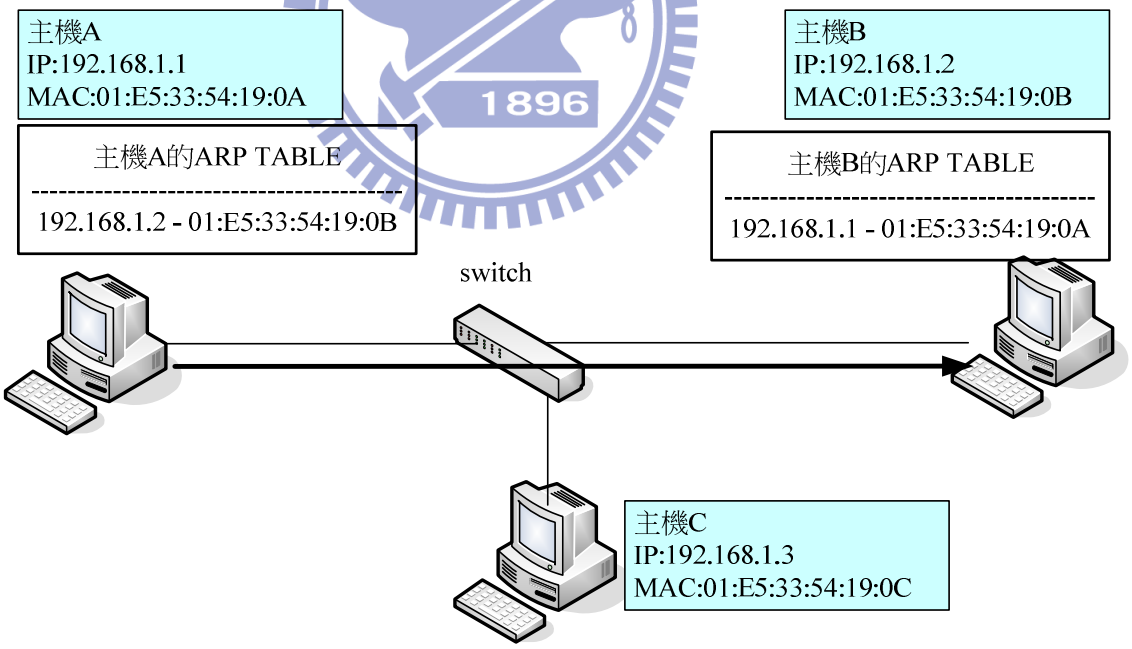


圖 2 - 9 主機 A 正常狀況下傳封包給主機 B

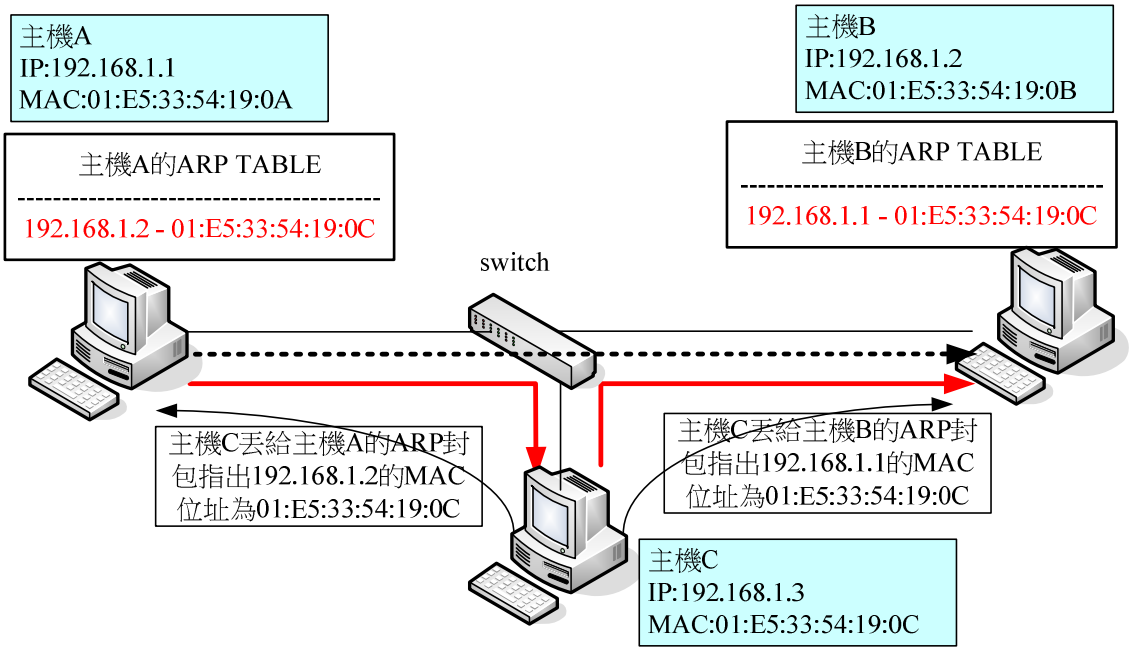


圖 2 - 10 主機 C 以 ARP 欺騙所造成的中間人攻擊

網路上可以輕易下載到的中間人攻擊軟體 Cain & Abel，提供了和善的視窗操作介面，可以很容易的被操作使用，只要指定要竊聽的對象，軟體就會同時欺騙傳輸中的兩台主機，讓自己成為中間人，如此軟體就會幫你在區域網路上收集有用的資訊，例如使用者的帳號與密碼。

2.4.3 阻斷服務攻擊

阻斷服務攻擊(Denial of Service，簡稱 DoS)是針對某一台主機或網路設備進行攻擊，使其無法再正常提供服務。而以 ARP 欺騙為基礎的阻斷服務是攻擊者發出偽造的 ARP 封包，讓區域網路內的主機或網路設備的 ARP TABLE 擁有錯誤的 IP 位址與 MAC 位址，所以在傳送資料時，無法傳送到正確的主機，便達成阻斷服務攻擊了。

如圖 2-11 所示，攻擊者以偽造的 ARP 封包發送給主機 A 和主機 B，並在它們的 ARP TABLE 裡留下錯誤的 IP 位址與 MAC 位址對應紀錄，主機 A 要傳送封包給主機 B 時，會將封包傳給 MAC 位址為 01:E5:33:54:19:BB 的主機 B，而在區域網路上並沒有這個 MAC 位址，所以主機 A 傳送的封包無法正確的送達主機 B。同樣的道理，主機 B 也無法傳封包給主機 A，所以主機 A 與主機 B 之間就無法通訊連線了。

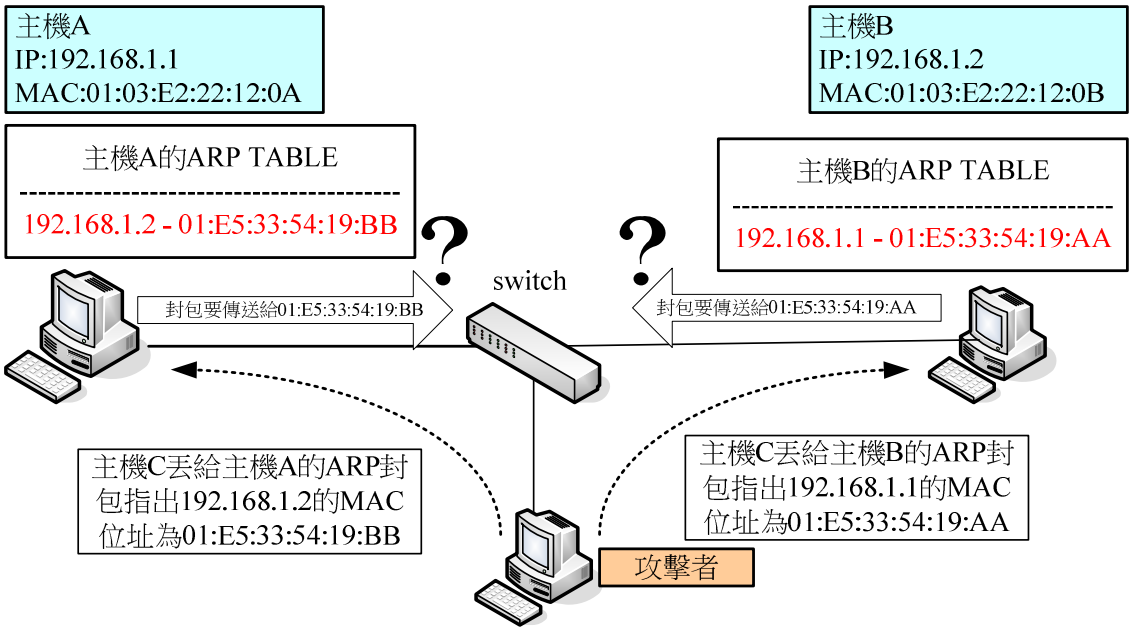


圖 2 - 11 阻斷服務攻擊

在網路上可以很容易搜尋到以 ARP 欺騙為基礎的阻斷服務攻擊軟體，最有名的是 NetCut 這一套軟體。攻擊者使用這一套軟體，可以清楚知道區域網路中有哪幾台電腦上線，並可以指定哪幾台電腦不能上網。有網管使用這一套軟體來管理網路，但是如果一般使用者也拿這一套軟體來限制某些電腦無法正常上網，這時就會造成網路秩序大亂。

第三章 相關研究

ARP 欺騙技術已經行之多年了，也有很多人研究如何修復 ARP 這個先天性的漏洞，也有人利用 ARP 欺騙技術來管理網路。本章在一開始介紹以 ARP 欺騙為基礎的網路管理，利用 ARP 欺騙對非法連上網的的主機做阻斷性攻擊，讓它無法連線上網；Zouheir 對網路監聽做研究**錯誤！找不到參照來源。**，歸納出一個可以偵測出網路卡進入任意模式狀態；劉修仁則是在使用者端利用 ARP 封包的數量來判斷出 ARP 封包的正確性；楊文龍則是利用網路設備的相關網路位址資訊來偵測網路上 ARP 欺騙攻擊的源頭；最後說明 CISCO 對 ARP 欺騙的防禦機制。

3.1 ARP 欺騙為基礎的網路管理

曾憲民在非法連網自動偵測與資源效能監控機制[7]這篇論文裡巧妙的利用 ARP 欺騙原理來做區網的連線管理。在區域網路中有使用者不小心使用到別人的 IP 位址時，就會造成 IP 衝突，造成別人無法正常連上網路；利用管理系統，可以呈現區網上的使用者使用 IP 的情形，並對非法取得 IP 的主進進行封鎖，以達成網路管理的最終目的。

3.1.1 使用者連網管理

在區域網路上設立一台伺服器，提供區域網路上的主機申請連線上網用；使用者向伺服器登記使用網路，並填寫申請者及主機的基本資料及 MAC 位址，管理者透過網頁介面審查申請者所填寫的基本資料，如果確定無誤就配發一個 IP 給申請者，申請者便可以完成申請上網的登記正常使用網路(如圖 3-1)。

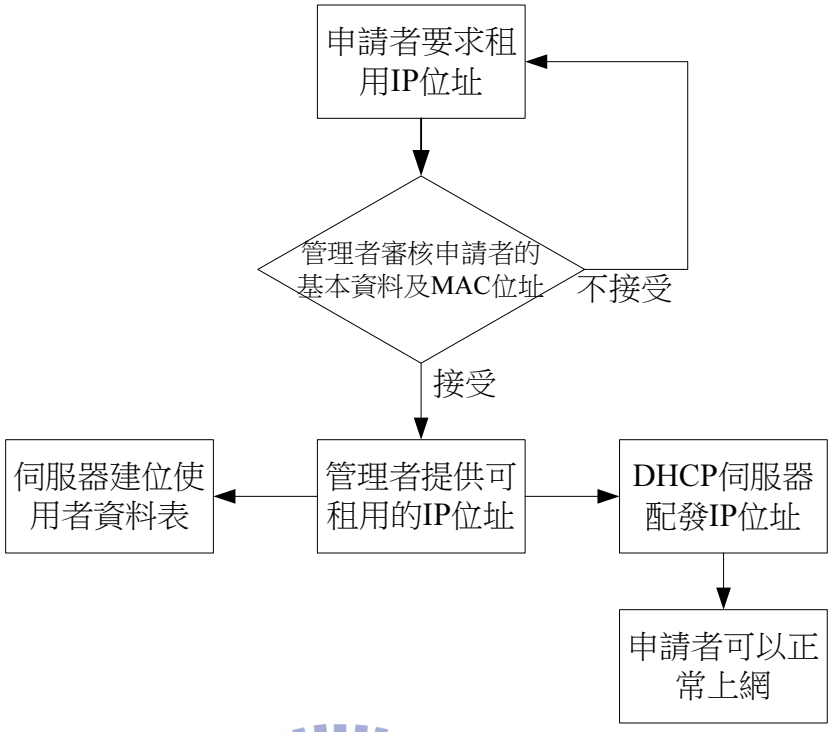


圖 3－1 使用者申請上網之流程

透過此機制，伺服器上的資料庫便可以方便的記錄合法的 IP 位址與 MAC 位址的對應關係。管理者可以在網路介面上查詢使用者的基本資料方便聯絡；也可以任意更改使用者的 IP 位址，以利後續上網管控；更可以管理使用者正常上網的權限，讓管理者可以限制使用者上網時間或甚至禁止使用者上網。

3.1.2 非法連網的偵測

如圖 3-2，首先要先利用 nmap 軟體偵測區域網路上有哪幾台主機，再利用 ARP 軟體具得 ARP TABLE 裡面 IP 位址與 MAC 位址的對應關係，即時建立網路使用者清冊，並與資料庫裡合法使用者登記的 MAC 位址和配發 IP 做比對；先比對 MAC 位址是否正確，再比對 IP 是否正確，如果都正確則增加其使用次數紀錄；如果其中一項不成功，則將其判定為不合法的連接 IP 位址或 MAC 位址，並記錄至資料庫中，以利後續追蹤管制。

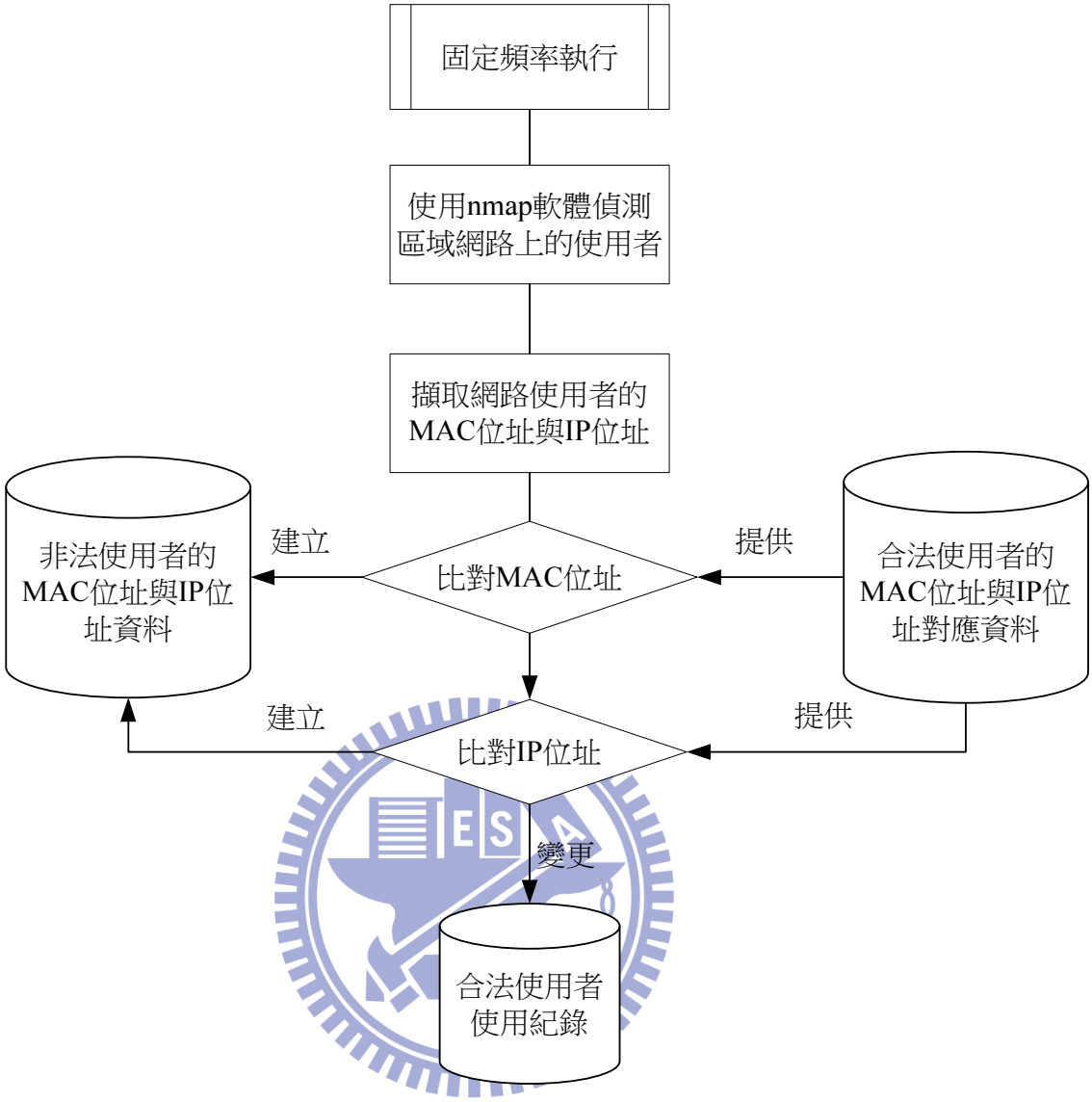


圖 3 - 2 非法使用者偵測的流程

3.1.3 非法連網的封鎖

伺服器建立非法使用者資料庫後，便會使用 ARP 欺騙方式或管理者在網管理的交換器裡面做設定阻絕非法使用者的連網作業。ARP 期騙方式是透過 arpupdate 這一個程式來達成，欺騙的方式可分為兩種：第一種方式，伺服器以 arpupdate 廣播偽造 ARP 詢問封包，此 ARP 詢問封包的來源 IP 位址與非法使用者的 IP 相同，非法使用者接收到此封包後，便會出現 IP 位址衝突錯誤，以致無法正常上網；第二種方式，伺服器以 arpupdate 偽造 ARP 回應封包，此封包的來源 IP 位址為閘道(Gateway)的 IP 位址，而來源 MAC 位址與非法使用者的 MAC 位址相同，將此封包傳送到非法使用者，更改其 ARP TABLE，非法使用者就無法與閘道器通訊，而無法正常上網。

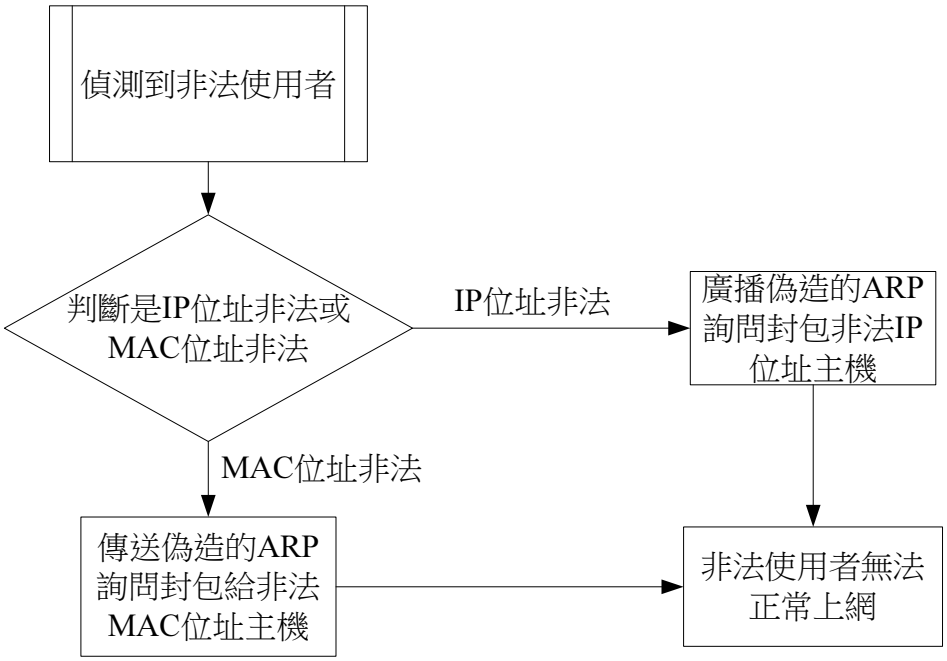


圖 3 - 3 封鎖非法使用者流程圖

3.2 偵測 ARP 欺騙攻擊主機之研究

ARP 欺騙偵測是本論文中最終系統實作的核心，下以針對幾個偵測的技術做分析探討。一開始探討偵測網路監聽之研究，利用其對網路卡任意模式的提出有效的偵測方法；再來介紹透過分析 ARP 封包數量，來判斷 ARP 回應封包的正當性；最後介紹使用 SNMP 技術來偵測網路中 ARP 欺騙。

3.2.1 偵測網路監聽之研究

在乙太網路上封包傳送到目的端主機的網路卡時，目的端系統會做網路卡卡號(MAC)與訊框的「目的端硬體位址」做比對；在正常模式下，訊框的「目的端硬體位址」與本身 MAC 位址相符或訊框的「目的端硬體位址」為 FF:FF:FF:FF:FF:FF(也就是廣播封包)時，此封包才會被網路卡所接收。不過還有一種情況封包也會被網路卡所接收，就是當網路卡調成任意模式(Promiscuous Mode)時。一般監聽軟體(sniffer)就是將網路卡調成任意模式來接收所有傳送來的封包，從中獲取有用的訊息資料。

跟據上面所述的特徵是用來判斷網路上主機是否正在監聽的關鍵，Zouheir 等人於是提出了偵測網路卡是否處於任意模式的方法[8]。由於網路卡調成任意模式，封包便不會被過濾而進入系統的核心。假設偽造一個 ARP 封包，它傳送的目

標端的位址不是廣播位址的任一個錯誤位址(如：00:00:00:00:00:01)，而且將這個封包廣播到區域網路上的每一台主機，如果有主機網路上的主機回應，那這些主機的網路卡正處於任意模式。

表 3-1 是 Zouheir 等人運用偽造的 ARP 詢問封包裡面訊框目標端的 MAC 位址並廣播到網路上，測試五種作業系統網路卡處於正常模式與任意模式下，ARP 封包回應的情況。其中 Br 是正常的廣播，測試每一個作業系統是否正常回應；M1 是測試網路卡是否接受群播；而 B47 可以檢查五種作業系統是否處於任意模式。利用此研究的結果，便可以設計一個偵測封包，來偵測網路上是否有人在竊聽。

		Windows XP		Windows Me/9x		Windows 2k/NT		Linux 2.4.x		FreeBSD 5.0	
		Norm.	Prom.	Norm.	Prom.	Norm.	Prom.	Norm.	Prom.	Norm.	Prom.
FF:FF:FF:FF:FF:FF	Br	O	O	O	O	O	O	O	O	O	O
FF:FF:FF:FF:FF:FE	B47	--	X	--	X	--	X	--	X	--	X
FF:FF:00:00:00:00	B16	--	X	--	X	X	X	--	X	--	X
FF:00:00:00:00:00	B8	--	--	--	X	--	--	--	X	--	X
01:00:00:00:00:00	Gr	--	--	--	--	--	--	--	X	--	X
01:00:5E:00:00:00	M0	--	--	--	--	--	--	--	X	--	X
01:00:5E:00:00:01	M1	O	O	O	O	O	O	O	O	O	O
01:00:5E:00:00:02	M2	--	--	--	--	--	--	--	X	--	X
01:00:5E:00:00:03	M3	--	--	--	--	--	--	--	X	--	X
O:Legal response , X:Illegal response , --:No response											

表 3 - 1 Promiscuos mode detection results

資料來源：*Malicious Sniffing Systems Detection Platform* [8]

3.2.2 以封包數量作 ARP 欺騙之研究

電腦主機要發送封包時，會以 ARP Table 中記錄的 IP 位址所對應的 MAC 位址來做為封包的目的地，而 ARP Table 中紀錄的異動主要是受制於兩種情況：第一種是電腦主機收到 ARP 詢問封包時，會讀取該封包中發送端的 MAC 位址與 IP 位址，並記錄在 ARP Table 中；第二種是電腦主機收到 ARP 回應封包時，讀取該封包中發送端的 MAC 位址與 IP 位址，並記錄到 ARP Table 中。在劉修仁的論文[9]中提到以 ARP 封包發送與接收的數量來判斷是否為 ARP 欺騙。

電腦主機無法判斷 ARP 詢問封包是否正常的 ARP 詢問封包，因為網路上任何主機要與本機連線，均會發出 ARP 詢問封包。所以設法讓本機收到 ARP 詢問封包後直接發送 ARP 回應封包，而不去變更 ARP Table 中的紀錄。如址作法便可確認 ARP TALBE 紀錄是來自於 ARP 回應封包。而 ARP 回應封包的正確性是可以被檢驗的。在 ARP 運作的流程中，我們可以清楚的知道獲得 ARP 回應封包前，電腦本機應該

至少要發送一個以上的 ARP 詢問封包，用此機制，即可用來檢驗 ARP 回應封包是否為偽造的。

因此針對一個 IP 位址而言，由本機發送 ARP 詢問封包與本機接收的 ARP 回應封包的數量應該符合表 3-2 中的公式(1)，也就是說本機所接收的 ARP 回應封包不得大於對此 IP 所發送的 ARP 詢問封包的次數。如此可以檢查某一個 IP 是否發生 ARP 欺騙。知道某個 IP 發生 ARP 欺騙後，再把 MAC 位址納入考量，當主機獲得的 ARP 回應封包中某個 IP 位址與 MAC 位址的組合的次數不得大於對某個 IP 發出的詢問封包數，我們使用表 3-2 中的公式(2)來判斷 MAC 位址的正確性。

名稱	判別公式
公式(1)	**Count (ARP reply from the IP) ≦ Count (ARP request for the IP)**
公式(2)	**Count (ARP reply from the IP+MAC) ≦ Count (ARP request for the IP)**

表 3 - 2 ARP 欺騙判別公式

劉修仁依上述兩個公式在三種情況下實驗：

●情況一：連線中的 ARP 欺騙

網路上最常用的 ARP 欺騙工具為了確保監聽的有效性，會不斷的要監聽的主機發送偽造的 ARP 回應封包，以確保被監聽的主機的 ARP Table 裡的紀錄不會被刪除。電腦 A 與電腦 B 在網路上傳訊，電腦 C 使用監聽軟體分別對電腦 A 電腦 B 發送偽造的 ARP 回應封包。使用公式(1)(2)來檢驗：

公式(1) Count (ARP reply from the IP) ≦ Count (ARP request for the IP)			
電腦主機	詢問封包	接收的回應封包	是否遭受 ARP 欺騙
電腦 A	1 個	n 個(n>1)	是
電腦 B	1 個	n 個(n>1)	是

公式(2) Count (ARP reply from the IP+MAC) ≦ Count (ARP request for the IP)				
電腦主機	詢問封包	接收的回應封包	接收的回應封包	偽造的 MAC 位址
電腦 A	1 個	MAC2 位址 1 個	MAC3 位址 n 個 (n>1)	MAC3 位址
電腦 B	1 個	MAC1 位址 1 個	MAC3 位址 n 個 (n>1)	MAC3 位址

表 3 - 3 以公式(1)(2)來判斷情況一之 ARP 欺騙

●情況二：連線前的 ARP 欺騙

電腦 C 在電腦 A 與電腦 B 尚未連線前，已經發送出偽造的 ARP 回應封包，修

改電腦 A 與電腦 B 的 ARP Table。電腦 A 與電腦 B 若要傳輸資料，這時會傳送給電腦 C，形成封包監聽。使用公式(1)(2)來判斷：

公式(1) Count (ARP reply from the IP) ≦ Count (ARP request for the IP)			
電腦主機	詢問封包	接收的回應封包	是否遭受 ARP 欺騙
電腦 A	0 個	n 個(n>0)	是
電腦 B	0 個	n 個(n>0)	是

公式(2) Count (ARP reply from the IP+MAC) ≦ Count (ARP request for the IP)				
電腦主機	詢問封包	接收的回應封包	接收的回應封包	偽造的 MAC 位址
電腦 A	0 個	MAC2 位址 0 個	MAC3 位址 n 個 (n>0)	MAC3 位址
電腦 B	0 個	MAC1 位址 0 個	MAC3 位址 n 個 (n>0)	MAC3 位址

表 3 - 4 以公式(1)(2)來判斷情況二之 ARP 欺騙

使用公式(1)(2)來判斷，可以得知 ARP 欺騙以及偽造的 ARP 回應封包，但是無法得知正確的 MAC 位址。

●情況三：連線初始時的 ARP 欺騙

當電腦 C 欲監聽電腦 A、電腦 B 的通訊內容，一開始先在網路上等待電腦 A 與電腦 B 的 ARP 詢問封包，當電腦 A 欲與電腦 B 連線而廣播一個 ARP 詢問封包，電腦 C 收到此封包後，隨即對電腦 A 與電腦 B 各送出一個 ARP 回應封包。

公式(1) Count (ARP reply from the IP) ≦ Count (ARP request for the IP)			
電腦主機	詢問封包	接收的回應封包	是否遭受 ARP 欺騙
電腦 A	1 個	2 個(2>1)	是
電腦 B	0 個	1 個(1>0)	是

公式(2) Count (ARP reply from the IP+MAC) ≦ Count (ARP request for the IP)				
電腦主機	詢問封包	接收的回應封包	接收的回應封包	偽造的 MAC 位址
電腦 A	1 個	MAC2 位址 1 個	MAC3 位址 1 個	無法判斷
電腦 B	0 個	MAC1 位址 0 個	MAC3 位址 1 個 (1>0)	MAC3 位址

表 3 - 5 以公式(1)(2)來判斷情況三之 ARP 欺騙

使用此種偵測方式必需在使用者端安裝此偵測程式，才可以有效判斷出非法 ARP 封包，但是網路管理員無法有效的控制使用者安裝程式，而且此程式只有偵測

非法 ARP 封包，並沒有防禦 ARP 封包的機制。

3.2.3 基於 SNMP 之 ARP 攻擊偵測研究

楊文龍在提出一個基於 SNMP 網管協定的 ARP 攻擊偵測機制[10]：在區域網路透過收集路由器、DHCP 伺服器及交換器之位址組態資訊，用來偵測區域網路中使用 ARP 欺騙技術的中間人攻擊與阻斷服務攻擊的所在交換器之埠號，並以 SNMP 呼叫交換器上對攻擊者所在埠進行封鎖，以阻止其繼續攻擊。底下就 DHCP 伺服器、路由器及交換器所收集的資料來做說明：

1、DHCP 伺服器：DHCP 伺服器的 log 檔中每一筆配發 IP 紀錄包含配發的 IP、申請者的網路卡卡號(MAC)。透過 log 檔可以知道主機是否正常取得 IP 位址，如果正常取得 IP 位址後卻無法上網，都可以用來判斷是否遭受 DoS 攻擊。

2、路由器：路由器的 ARP TABLE 記錄著短期內與網路上有通訊過的主機其 IP 位址與 MAC 位址的對應關係。如果表格中兩筆以上的資料有著想同的 MAC 位址，則可以知道該 MAC 位址被用於 ARP 欺騙攻擊。

3、交換器：交換器的運作效能比集線器好的原因在於交換器會記錄每一埠底下有哪些 MAC 位址，而這此紀錄記錄在交換器的交換表(Switching Table)中。如果知道哪一個 MAC 位址有問題，可以依此表找出所對應的埠號，並拔除網路線，可以有效隔離攻擊的源頭。

表格類型 \ 位址資訊	MAC 位址	IP 位址	交換器埠號
DHCP 之 log 檔	✔	✔	
路由器之 ARP TABLE	✔	✔	
交換器之交換表	✔		✔

表 3 - 6 DHCP、路由器、交換器所收集之位址資訊

當 DHCP 的 log 檔中 IP 位址與 MAC 位址的記錄和路由器的 ARP Table 中的同一個 IP 位址和 MAC 位址對應不同時則可以知道 ARP Table 中的 MAC 位址為 ARP 欺騙的 MAC 位址，因此可以找出中間人攻擊。利用週期性的獲得路由器，並找出前後之間相同 IP 位址，但 MAC 位址不同的紀錄，再透過 DHCP 中的 log 檔來判斷是否有 ARP 欺騙攻擊。圖 3-4 為 ARP 欺騙之偵測流程，步驟說明如下：

1、使用 SNMP 到路由器取得 ARP Table，收集目前路由器上所看到的 IP 位址與 MAC 位址的對應關係。

2、檢查 ARP Table 中同網段是否有不同 IP 位址對應相同 MAC 位址，並將其所對應的 IP 位址列出來。

3、排除手動加入 MAC 位址名單，例口路由器本身的 MAC 位址會對應到多個 IP 位址。

4、向 DHCP 伺服器取回 log 檔中有效租約的 IP 位址與 MAC 位址對應表。Log 檔中會記錄攻擊者與被攻擊者的 IP 位址與 MAC 位址，所以用來佐證步驟 2 重覆的 MAC 位址所對應的真正 IP 位址，並找出攻擊者的 IP 位址與 MAC 位址。

5、知道攻擊者的 MAC 位址後，使用 SNMP 取得交換器的交換表，比對後取得攻擊者的 MAC 位址所在的埠號。

6、知道攻擊者所在之交換器及對應的埠號，即可以 SNMP 至交換器進行斷網措施。

7、清除路由器上的 ART Table Cache，以維持 ARP Table 資料的即時性與正確性。

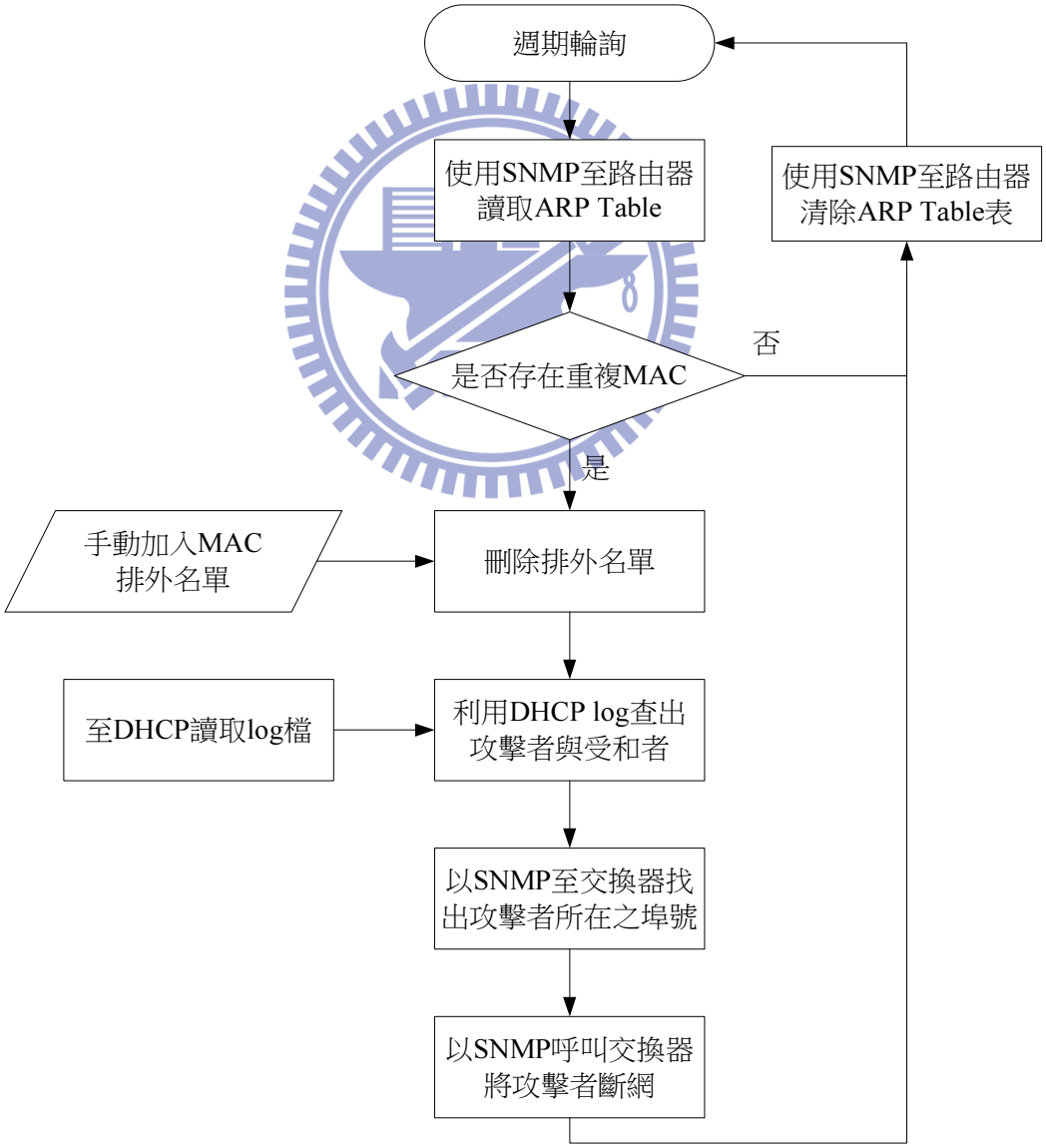


圖 3 - 4 ARP 攻擊偵測流程圖

此種偵測方式可以偵測出 ARP 欺騙，但是偵測系統所仰賴的網路設備必需支援 SNMP 協定，而支援 SNMP 協定的交換器一定比一般交換器貴。且其資料庫上的 MAC 位址與 IP 位址對應關係是透過路由器的 ARP Table 以及 DHCP 的 log 檔而來，如果利用此收集 MAC 位址與 IP 位址對應關係，所收集到的資料正確性便可提升。

3.3 CISCO 對 ARP 欺騙的防禦

CISCO 是網路設備安全防禦技術最有名的公司，其技術走在世界潮流的前端；該公司在面對 ARP 期騙，使用了一些應該策略，如 Port Security 與 Dynamic ARP Inspection。

3.3.1 Port Security

CISCO 交換器上的 Port Security 機制[11][12][13]簡單來說就是讓限定的 MAC 位址在交換器上傳輸，透過設定每個埠 (port)上可以學到的 MAC 位址數量有一個上限，如果超過這個上限時，交換器就會關閉該埠或發出訊號通知網管；如果該埠連接的主機不會短期內不會更動 MAC 位址，更可以設定綁 MAC 位址。這些功能用來防範每個埠連接的電腦主機受到 ARP 欺騙攻擊。

發生 ARP 攻擊是某一埠連接的電腦主機發送會發送大量的偽造 ARP 封包，如果這個 ARP 封包的目標 MAC 位址不在交換器的埠號與 MAC 位址設定資料中，則封包會直接被丟棄；但如這個 ARP 封包的來源 MAC 位址與設定的不同，這時交換器啟動防範機制，然後進行下列三種處理方式：

1、直接將該埠關閉。

2、直接丟棄偽造的 ARP 封包，不發出訊息通知網管。

3、直接丟棄偽造的 ARP 封包，並發出訊息通知網管。

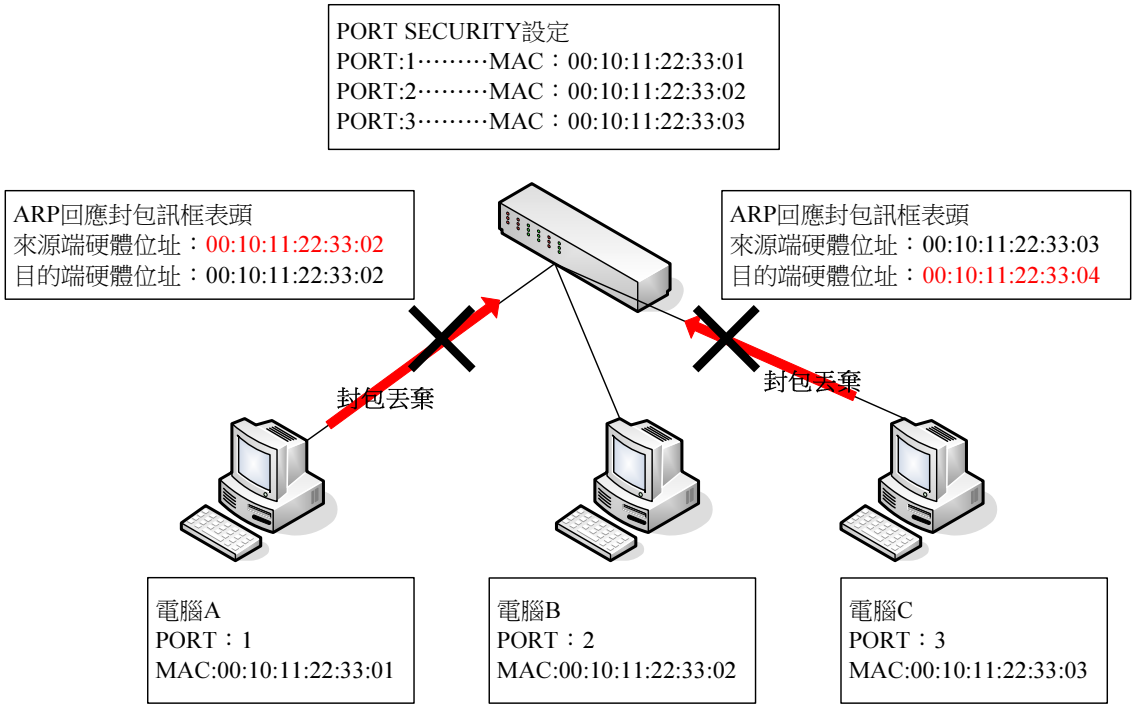


圖 3- 5 PORT SECURITY 防禦方式

由圖 3-5 可以知道，Port Security 可以用來檢驗訊框裡的來源位址與目標位址，如果不符合 Port Secruity 所設定的交換表，則會被丟棄，必要時此交換器會將該埠斷線。但是此種方法只能確保封包的訊框不被偽造，可以有效防止 MAC 洪流攻擊，但對於封包訊框正常的 ARP 欺騙則無任何作用。

3.3.2 Dynamic ARP Inspection

動態 ARP 檢驗(Dynamic ARP Inspection，簡稱 DAI)[11][14][15]是由 CISCO 公司所開放的，其原理是利用 DHCP 服務上面所記錄的 IP 位址、MAC 位址及所使用的交換機的 PORT 號來檢驗交換器上所接收到的 ARP 封包的正當性，如果 ARP 封包上所登記的 IP 位址與 MAC 位址與 CISCO 機器上面所記錄的資料符合時，封包就會繼續傳送到目的端主機；如果不符合時，此 ARP 封包會被視為非法的，就會丟棄封包並記錄在系統上，必要時系統會關閉該 ARP 封包所使用的 PORT，使該 PORT 號上的主機無法再繼續連線。

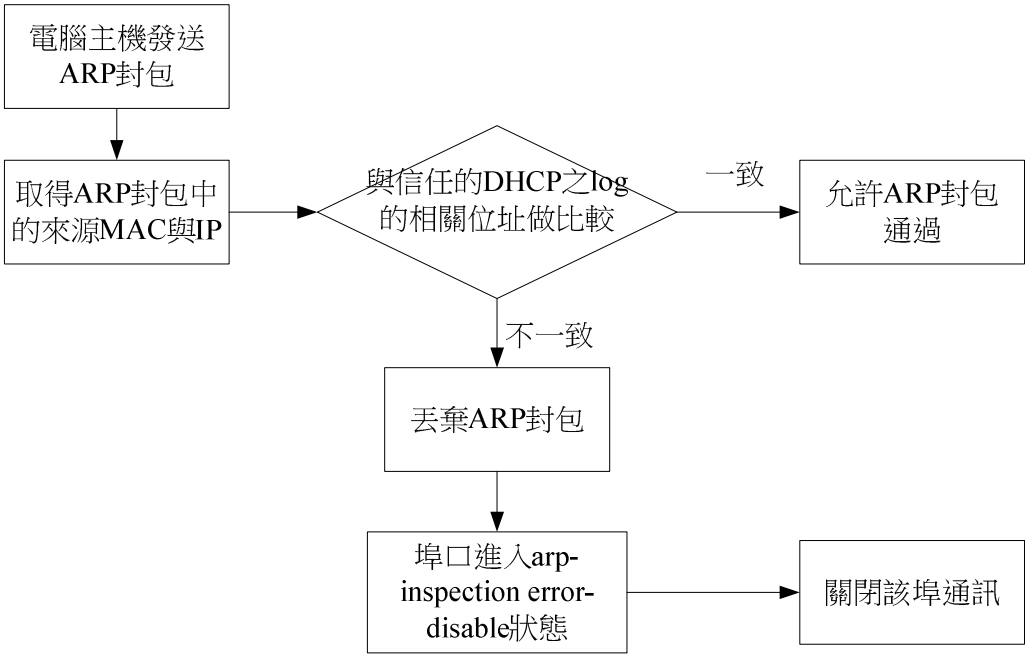


圖 3- 6 ADI 工作流程圖

CISCO 公司研發的 ADI 機制是目前防禦 ARP 欺騙的好用的作法，可是目前中信局中所賣的 CISCO 交換器支援 ADI 機制的設備一台 24 埠的要接近 3 萬[16]，如果要全校建置，需要一筆龐大經費，而這經費不是一般小學可以輕易付擔的。

第四章 偵測防禦系統設計

在第三章中提到 ARP 欺騙的偵測方式與 arpupdate 駭客程式的特性，本章就利用這個特性設計一套偵測防禦系統，系統分成偵測分析模組、防禦模組、警示模組與管理模組，管理模組可以設定其它三個模組，而偵測分析模組則示持續監聽分析網路上經過本主機的 ARP 封包，將有問題的網路位址資料傳送到警示模組與防禦模組，警示模組再將相關資料主動傳給網路管理者，而防禦模組則是將有問題的網路位址以封包重製方式，將正確的網路位址資料傳送給受欺騙的電腦主機，如圖 4-1 所示。

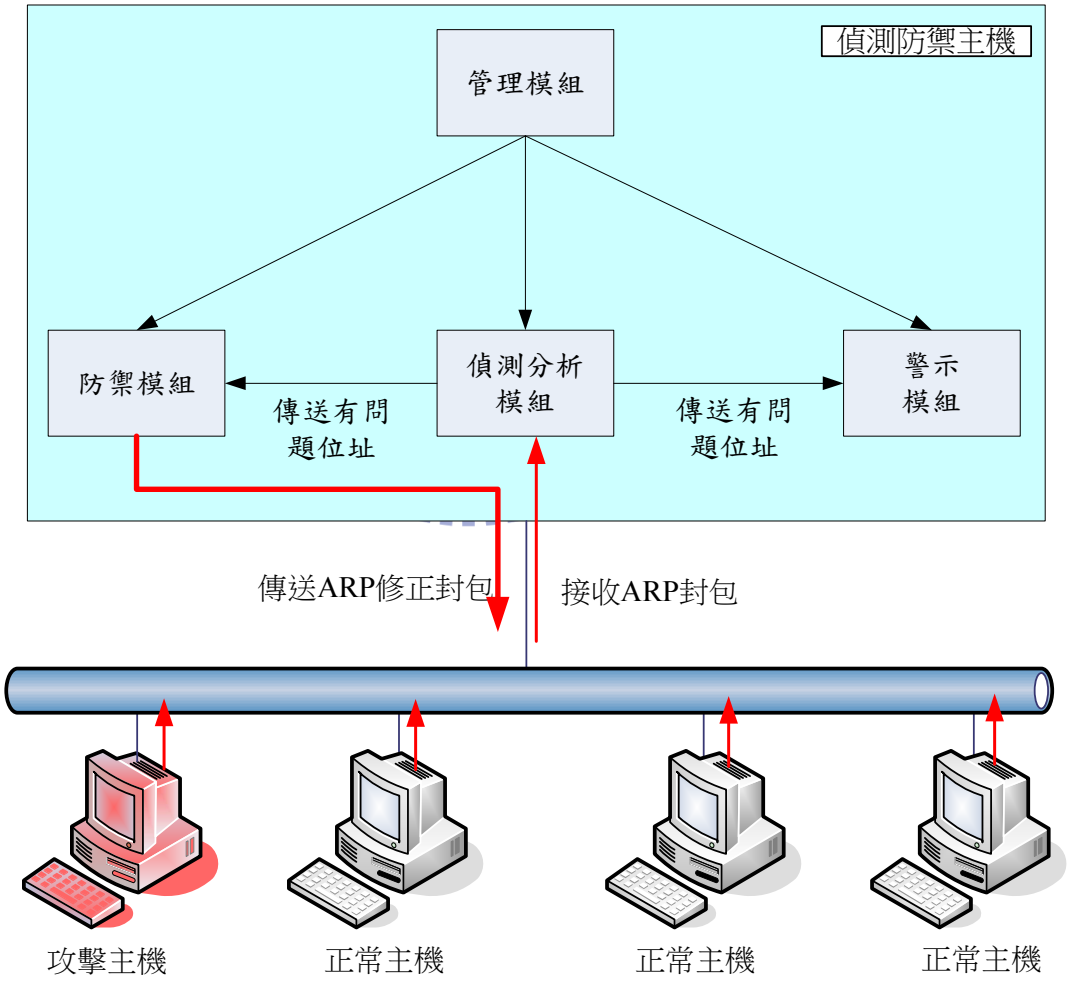


圖 4 - 1 偵測防禦系統架構圖

4.1 偵測分析模組

偵測分析模組是本系統的核心，此模組是透過網路監聽的方式，擷取本系統主機所接收到的 ARP 封包，並將封包裡面的位址資料存入資料庫中。在監聽的同時，系統會與資料庫的資料比對 ARP 封包的正確性，如果分析出來有問題的網路位址，則將此網路位址資料傳送給警示模組。圖 4-2 為偵測分析模組的運作架構圖。

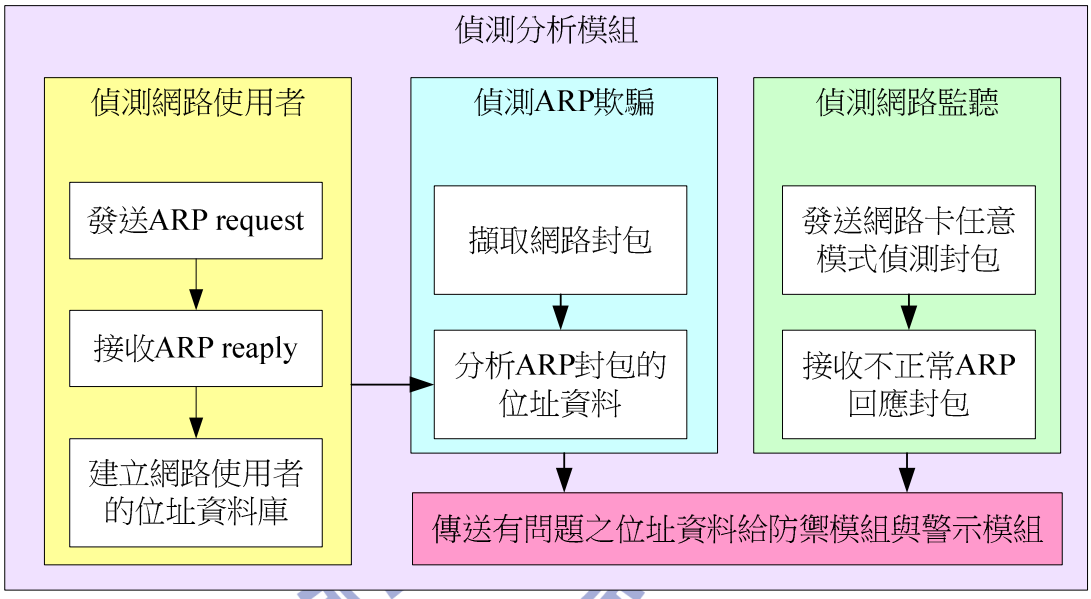


圖 4 - 2 偵測分析模組運作架構圖

4.1.1 網路監聽偵測

在 Zouheir 對網路監聽研究[8]中，利用偽造的 ARP 詢問封包，傳送到網路上的每一台主機，觀察網路卡在正常模式與任意模式時的回應該形，然後作成統計表。在其統計表中，當封包的訊框設定為 FF:FF:FF:FF:FF:FE 時，在五種作業系統中，可以完全偵測出主機網路卡處於任意模式。

利用 Zouher 對網路監聽的研究，本論文實作一個網路主機網路卡任意模式的偵測程式。在網路上連續詢問區域網路上所有的 IP，而使用偽造 ARP 詢問封包的訊框目標位址使用 FF:FF:FF:FF:FF:FE，傳送到網路上所有的電腦主機，然後接收回應的 ARP 回應封包，並將回應封包的主機位址取出寫入資料庫，如圖 4-3 所示。偽造封包程式偽造一個 ARP 詢問封包，此封包格式如圖 4-3

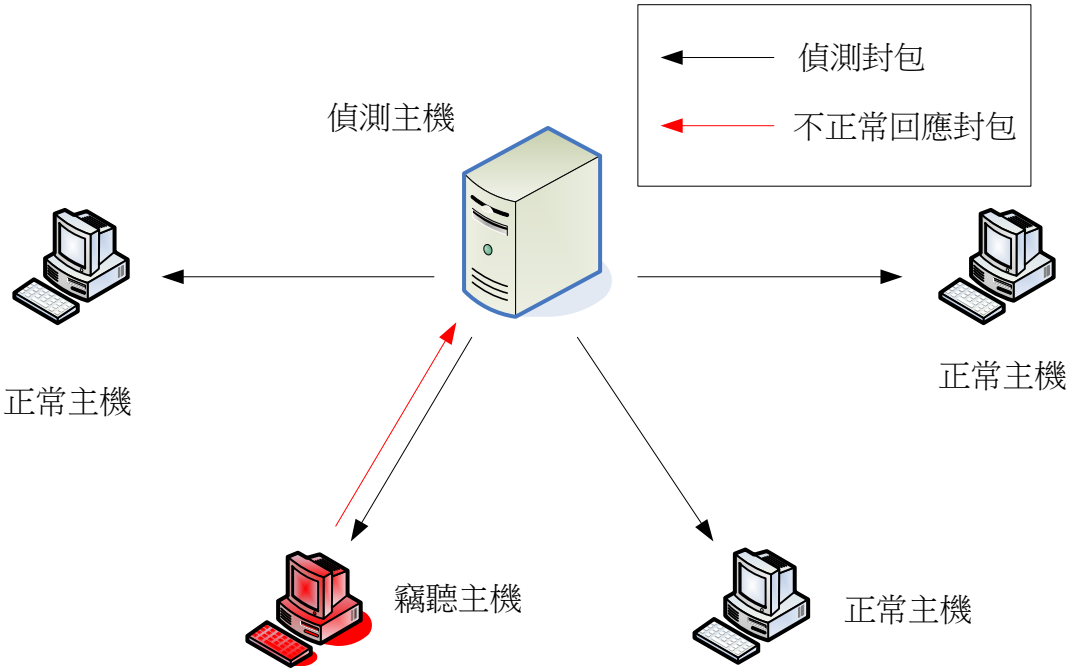


圖 4 - 3 偵測竊聽主機示意圖

DST MAC：FF:FF:FF:FF:FF:FE	
SRC MAC：偵測系統主機之MAC位	
TYPE：0806	
HTYPE：1	PTYPE：0800
HLEN：6 PLEN：4	OPER：1
SHA：偵測系統主機之MAC位址	
SPA：偵測系統主機之IP位址	
THA：00:00:00:00:00:00	
TPA：測試目標之IP位址	

圖 4 - 4 偵測網路卡任意模式之 ARP 封包

當偵測封包訊框的目標位址未存在於交換器的交換表中時，交換器就會先廣播封包到所有的埠口，而因為訊框的目標位址一直不在區域網路上，所以沒有 ARP 封包會以此訊框來源位址(FF:FF:FF:FF:FF:FE)來做回應，此 MAC 位址就不會留紀錄在交換器的交換表中，所以每次傳送此偵測封包時，都會以廣播的的方式傳送到區域網路上的每一台電腦主機。

由於 ARP 詢問封包一次只能詢問一個 IP 位址所對應的 MAC 位址，所以每次偵測時，必需連續廣播多個 ARP 詢問封包，詢問的 IP 位址為區域網路上所有的 IP(如 192.168.0.0/24)，如此竊聽主機便會接收到屬於自己 IP 位址的詢問封包，且會回應一個 ARP 回應封包給偵測主機，如此便可以由回應的 ARP 詢問封包知道竊聽主機的位址資訊。

4.1.2 建立網路使用者資料庫

網路使用者資料庫建置是非常重要的基本工作，偵測分析模組在網路上分析所接收到的 ARP 封包時，分析封包的 MAC 位址與 IP 位址，需要網路上主機的 MAC 位址與 IP 位址的正確對應關係，偵測分析模組其中一個功能便可達成。

偵測分析模組利用 ARP 詢問封包對區域網路廣播，再收集 ARP 回應封包來建立使用者的 IP 位址與 MAC 位址的對應關係，並寫入資料庫。每次必需連續廣播多個 ARP 詢問封包，詢問的 IP 位址為區域網路上所有的 IP(如 192.168.0.0/24)，只要電腦主機有上線，必會回應 ARP 回應封包給偵測主機。利用此方法，除了可以建立網路電腦 MAC 位址與 IP 位址對應關係外，也可以即時知道有哪幾台主機正在線上。

圖 4-5 是偵測主機廣播 ARP 詢問封包給區域網路上所有的電腦主機，圖 4-6 是區域網路上連線的電腦主機傳回 ARP 回應封包給偵測主機，偵測主機的 ARP Table 中便有即時連線的電腦主機資料，再把 ARP Table 的紀錄寫入資料庫，當偵測分析模組正在執行偵測 ARP 欺騙攻擊時，就可以利用此位址資料和擷取到的 ARP 封包位址做比對。

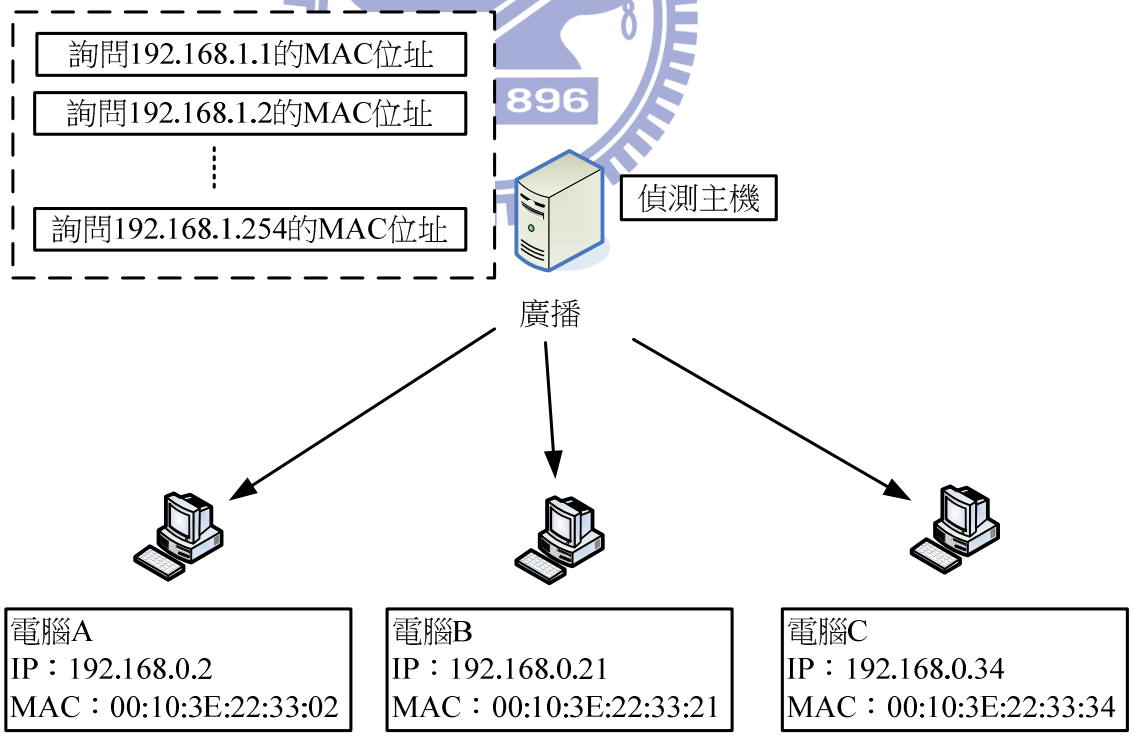


圖 4 - 5 偵測主機廣播 ARP 詢問封包

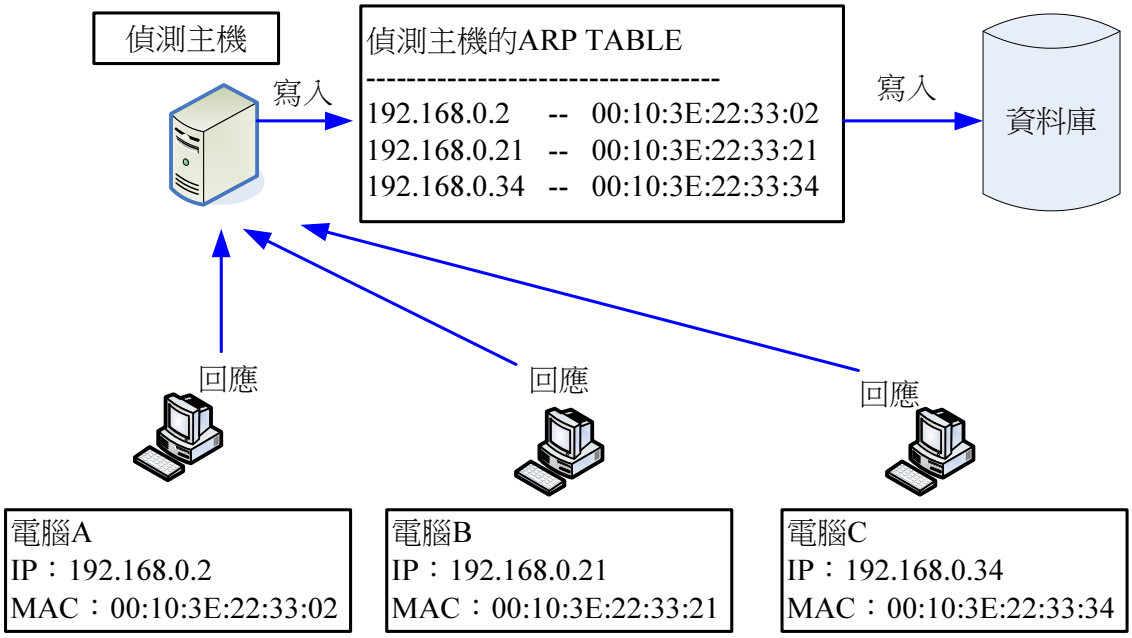


圖 4 - 6 網路主機傳送 ARP 回應封包給偵測主機

4.1.3 偵測 ARP 欺騙攻擊

偵測主機在區域網路上持續監聽擷取傳送來的 ARP 封包，偵測分析模組便開始分析 ARP 封包內容，取出封包中訊框的來源 MAC 位址、目的 MAC 位址和 ARP 封包中的傳送者 MAC 位址、IP 位址與目標 MAC 位址、IP 位址，再與資料庫中 MAC 位址與 IP 位址的對應資料做比對。比對後發現有問題的位址，便將錯誤的位址資料傳送給警示模組，而傳送者的位址資訊是改變 ARP Table 的重要關鍵，所以傳送者的位址資訊如果有誤，便直接傳給防禦模組。

如圖 4-7，位址比對時，首先比對 ARP 封包的傳送者 MAC 位址、IP 位址的對應關係與資料庫中的位址對應紀錄是否相同，如果有誤便將位址資訊傳送給防禦模組；再來判斷 ARP 封包的格式，如果是 ARP 詢問封包，訊框的目的 MAC 位址是 FF:FF:FF:FF:FF:FF，如果是一般的 MAC 位址，那表示這個 MAC 位址有問題，而在 ARP 封包格式中的目標 MAC 位址應該是 00:00:00:00:00:00，如果是一般的 MAC 位址，那表示這個 MAC 位址有問題；如果是 ARP 回應封包，則 ARP 封包格式中目標 MAC 位址與 IP 位址的對應關係與資料庫中的位址資料要相符，且訊框的目的 MAC 位址要與 ARP 封包格式中的目標 MAC 位址一致、訊框的來源位址與 ARP 封包格式中的傳送者 MAC 位址要一樣；如果發現位址資料有問題，便將錯誤的位址資料傳送給警示模組。

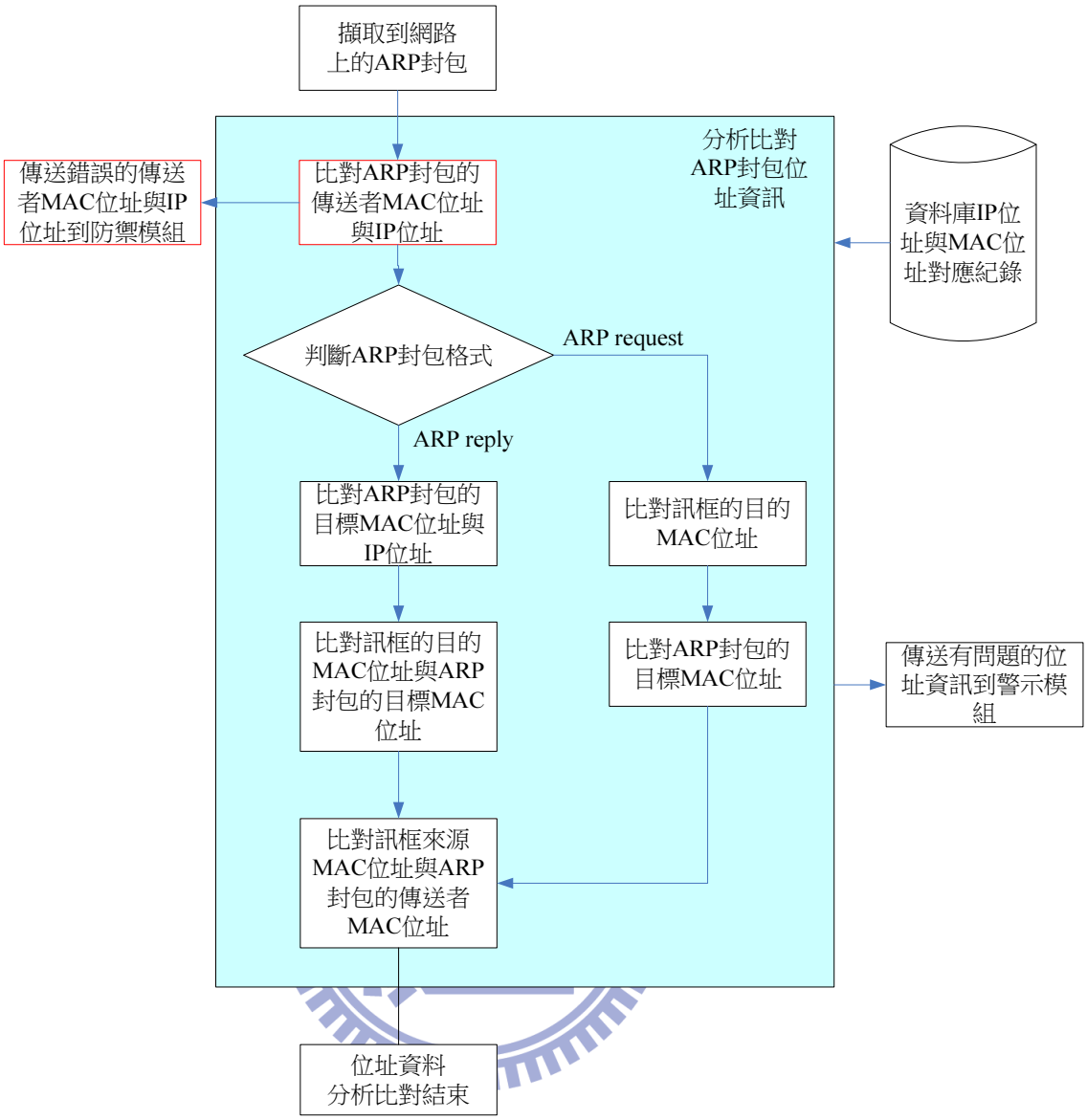


圖 4 - 7 ARP 欺騙攻擊偵測流程圖

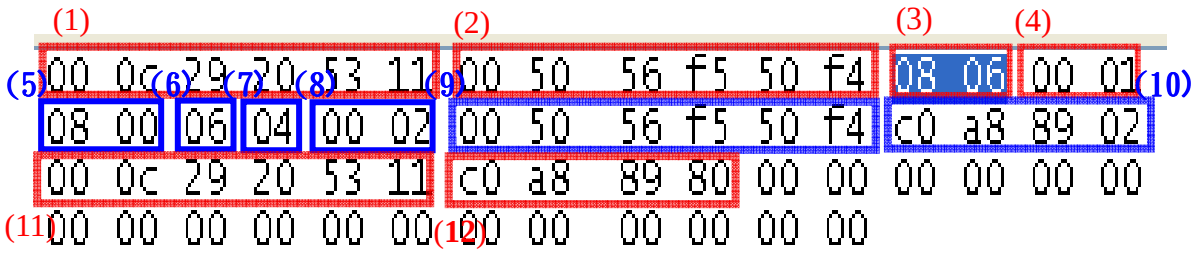
4.2 防禦模組

在當防禦模組接收到偵測模組傳過來有 ARP 欺騙的訊息時，便啟動防禦機制，透過系統封包偽造發送方式去反制 ARP 欺騙封包所帶來的攻擊效應，讓被攻擊者從原本無法上網到可以上網，而不會因為 ARP 攻擊而攤瘓網路。

4.2.1 封包重製

封包擷取程式在網路上擷取封包(圖 2-8)，可以看到封包的原始格式(如圖 4-8)，所以分析其原始格式，我們只要修改其中訊框的目的 MAC 位址(DST MAC)、

來源 MAC 位址(SRC MAC)與 ARP 封包資料中的傳送者 MAC 位址(SHA)、傳送者 IP 位址(SPA)、目標 MAC 位址(THA)、目標 IP 位址(TPA)，再將修改過的 ARP 封包傳送到區域網路上的電腦主機，藉此修正可能已被欺騙之電腦主機的 ARP Table。



DST MAC：(1)		
SRC MAC：(2)		
TYPE：(3)		
HTYPE：(4)	PTYPE：(5)	
HLEN：(6)	PLEN：(7)	OPER：(8)
SHA：(9)		
SPA：(10)		
THA：(11)		
TPA：(12)		

圖 4 - 8 ARP 封包格式分析

圖 4-9 為本系統用來廣播到區域網路上 ARP 封包格式，其中訊框的部份目的 MAC 位址填入 FF:FF:FF:FF:FF:FF，來源 MAC 位址則填上系統主機的 MAC 位址，類型(TYPE)填上 0806；在 ARP 封包部份，在硬體類型(HTYPE)填上 1，通訊協定類型(PTYPE)填上 0800，硬體長度填上 6，通訊協定長度填上 4，操作(OPER)填上 1，傳送者硬體位址填上修正的 MAC 位址，傳送者邏輯位址填上原本 ARP 欺騙封包的傳送者 IP 位址，目標硬體位址填上修正的 MAC 位址，目標邏輯位址填上原本的 IP 位址。此外，被欺騙者的 ARP Table 中 Gateway 的 IP 位址與 MAC 位址對應紀錄亦被更改，故亦針對被欺騙攻擊的電腦主機發送修正位址紀錄的 ARP 回應封包，此時訊框的目標位址則為被攻擊的主機的 MAC 位址，而傳送者的 IP 位址與 MAC 位址則填上 NAT 主機的 IP 位址與 MAC 位址。

DST MAC：FF:FF:FF:FF:FF:FF		
SRC MAC：修正的MAC位址		
TYPE：0806		
HTYPE：1		PTYPE：0800
HLEN：6	PLEN：4	OPER：1
SHA：修正的MAC位址		
SPA：原本的IP位址		
THA：00:00:00:00:00:00		
TPA：原本的IP位址		

DST MAC：修正的MAC位址		
SRC MAC：NAT的MAC位址		
TYPE：0806		
HTYPE：1		PTYPE：0800
HLEN：6	PLEN：4	OPER：2
SHA：NAT的MAC位址		
SPA：NAT的IP位址		
THA：修正的MAC位址		
TPA：原本的IP位址		

圖 4 - 9 修正 ARP Table 紀錄之 ARP 封包

4.2.2 ARP 欺騙攻擊防禦

當接收到偵測分析模組傳送過來有問題的位址資訊時，便從資料庫中的位址資料中取出正確的 MAC 位址與 IP 位址，利用封包重製發送技術，將封包(ARP 封包 1)以廣播方式傳送到區域網路中所有的電腦主機，以更正 ARP Table 的紀錄而不受 ARP 欺騙攻擊，且傳送 ARP 回應封包(ARP 封包 2)給被攻擊者，修正被攻擊者 ARP Table 中 Gateway 的位址紀錄。除修正 ARP Table 外，必要時再對有問題的主機實施 ARP 欺騙攻擊，以阻斷性攻擊的方式對有問題的電腦主機實施斷線處置，使其無法正常上網。

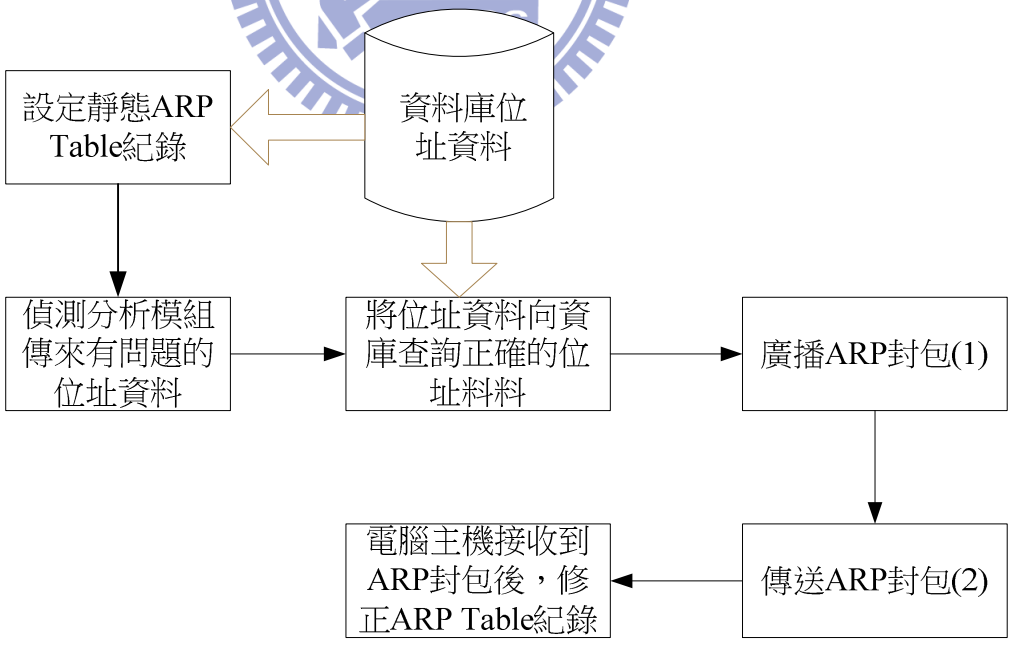


圖 4 - 10 防禦模組運作流程圖

4.3 警示模組

警示模組主要是透過偵測分析模組所分析獲得的資料，將有問題的位址呈現出來。當偵測分析模組監聽網路上封包，將封包的位址資料與資料庫裡面所存在的位址資料做比對，當資料比對後發現不符時，便把有問題的位址資料存入資料庫，並通知管理者。管理者除了被動地透過信件通知外，亦可以主動到網站上獲得這些有問題的位址資料，以便下一步的處理。圖 4-11 為警示模組運作的流程。

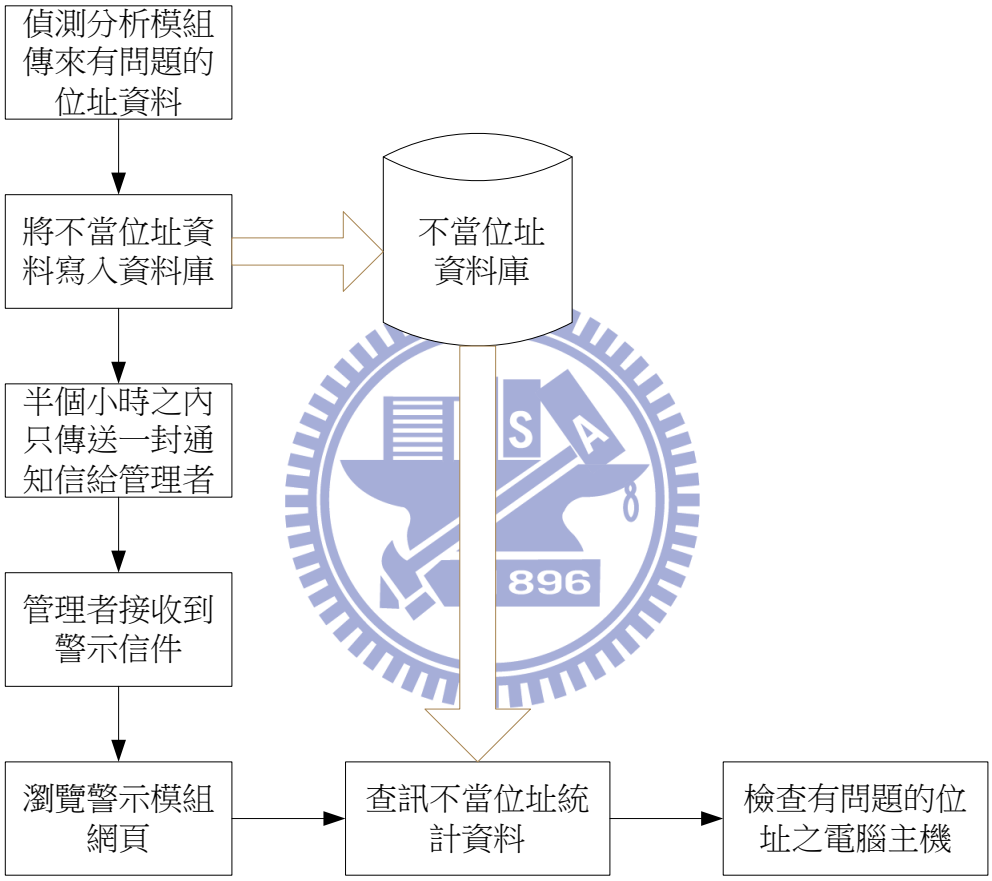


圖 4 - 11 警示模組運作流程圖

4.3.1 不當位址資料匯整

偵測分析模組在分析接收到的 ARP 封包時，將有問題的位址資料傳送到警示模組，警示模組便將此資料存進不當位址資料庫中；因為 ARP Table 裡的紀錄容易被電腦主機修正，所以一般 ARP 欺騙攻擊必需一直傳送偽造的 ARP 封包到被攻擊的電腦主機，所以警示模組在做不當位址資料匯整時，要再統計其次數。

4.3.2 警示方式

警示模組在做不當位址資料匯整時，接收到錯誤的位址資料時，便傳送 E-MAIL 給管理者，這裡傳送 E-MAIL 的頻率設定為半個小時，也就是說半個小時之內如果接收到很多次由偵測分析模組傳過來有問題的位址資料，只有在第一次時會傳送 E-MAIL，第二次以後便不會再傳送，直到半小時後再接收到偵測分析模組傳過來錯誤的位址資料時，才會再傳一封 E-MAIL 給管理者。

E-MAIL 內容中只是告知管理者區域網路中發生 ARP 欺騙攻擊，詳細的有問題位址統計資料，只呈現在警示模組的網頁裡。管理者查詢後，再依匯整的資料做為判斷 ARP 欺騙攻擊主機的依據，檢查該攻擊主機是否執行 ARP 欺騙攻擊。

4.4 管理模組

後端管理模組是用來設定偵測分析模組、防禦模組與警示模組用的，並且加入網路使者的管理，讓此系統可以用來管理網路上不當連線的電腦主機，提升網路管理及防禦功能。

4.4.1 模組設定

管理模組是偵測防禦系統的主宰，用來管理及設定偵測分析模組、防禦模組與警示模組，管理及設定相關說明如下：

1、偵測分析模組：在位址分析方向，全部分析時會分析比對 ARP 封包的傳送者 MAC 位址、IP 位址的對應關係；分析 ARP 詢問封包中訊框的目的 MAC 位址是否為 FF:FF:FF:FF:FF:FF， 分析 ARP 封包格式中的目標 MAC 位址；如果是 ARP 回應封包，則 ARP 封包格式中目標 MAC 位址與 IP 位址，分析訊框的目的 MAC 位址是否與 ARP 封包格式中的目標 MAC 位址一致及訊框的來源位址與 ARP 封包格式中的傳送者 MAC 位址是否一樣。管理模組便可調整要分析的位址資料。

2、防禦模組：在獲得偵測分析模組傳來的錯誤位址資訊時，防禦模組便將正確的位址資料以封包重製方式廣播出去。管理模組可以設定不接廣播方式傳送，而以 Unicast 方式傳送到某台電腦，以減少廣播封包。

3、警示模組：警示模組中需要設定的是管理者 E-MAIL 位址，以及發送警示信間隔的最少時間，預設為半個小時，設定時間可以依當時網路中 ARP 欺騙的頻率來做調整。

4.4.2 網路使用者管理

警示模組中統計有問題的位址資料，可以設定達一定的數量時，便命令防禦模組對有問題的位址實施 ARP 欺騙攻擊，阻斷其正常連網。管理模組中可以看到目前正實施斷網的位址有哪些，經檢查後沒問題，便可以手動將解除斷網恢復正常上網。

如果有新加入的電腦主機，因為在其位址資料未列在資料庫中，故被視為非法的網路使用者，而這些非法的使用者可以設定是否被斷線，預設是設定為斷線狀況，除了一開使為了建位合法使用者資料庫時才會解除斷線狀態。

第五章 系統實作與測試

在本章系統實作與測試中，一開始先對測試環境做簡單的說明，說明網路環境架構與系統軟體版本、硬體規格，再依第四章所規劃設計的系統做實際測試。在偵測網路監聽的實驗中，利用系統偵測出網路中正在執行監聽的電腦之位址，並嘗試阻斷性服務攻擊此監聽電腦、防禦 ARP 欺騙攻擊，以及對網路使用者管理，將測試的結果呈現出來。

5.1 測試環境

此處說明本系統的測試環境，網路環境與系統主機本身的軟體版本與硬體規格大致上依學校現有的網路環境與正在運作的主機做說明，不再變更現在的網路架構，期待測試完後可以直接上線運做。

5.1.1 網路環境

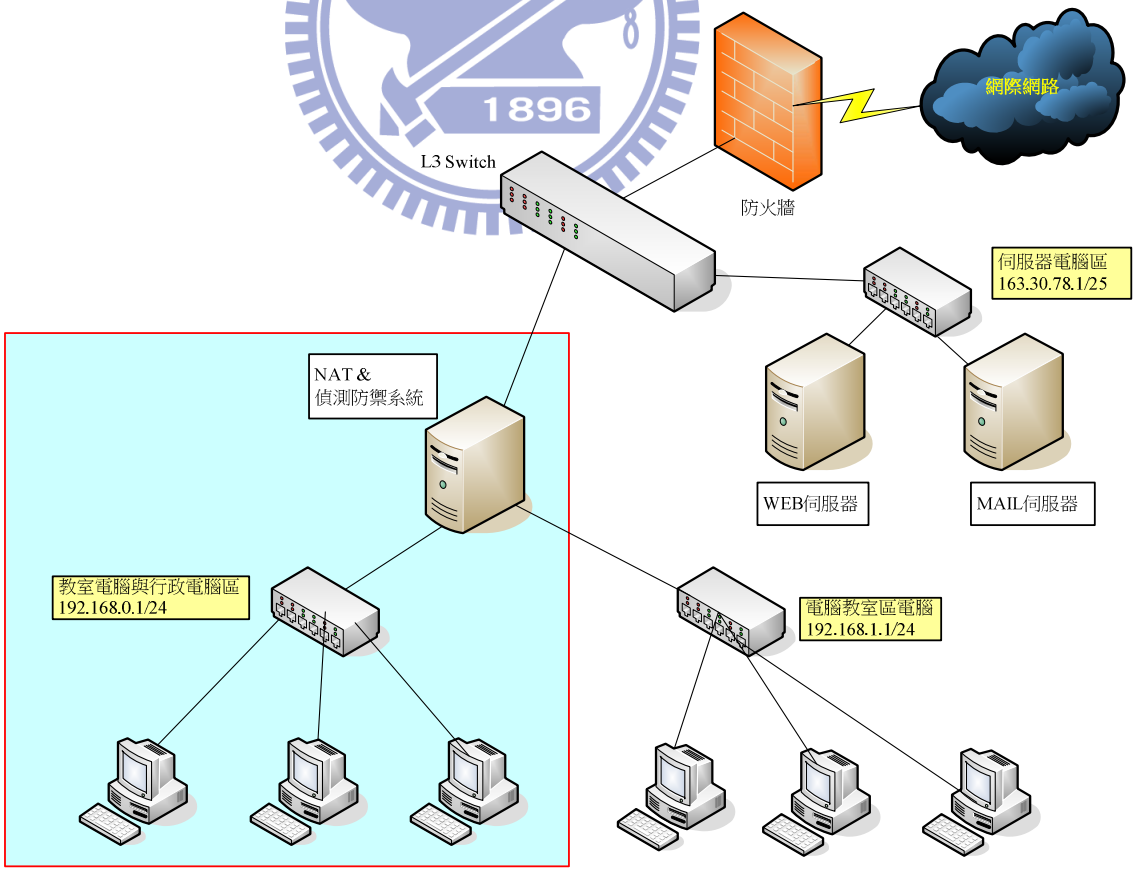


圖 5 - 1 網路測試環境

如圖 5-1 所示，網路測試環境以我服務的國小的網路環境為主，因為電腦教室的電腦有裝還原卡，而且學生操作時間只有 40 分鐘，無法在非上課時間開機使用，故不討論此區段；只以教室電腦與行政電腦網路區段做為試驗環境，這個網路區段的為 192.168.0.1/24，而每台電腦的 IP 設定採固定 IP，如果有發生駭客攻擊，必由此區段發生。

5.1.2 測試環境軟體與硬體架構

本系統使用的程式語言在管理介面上使用 php，在偵測與防禦上則使用 C 語言搭配 Libpcap 和 Libnet 函式庫，其中 Libpcap 是用來擷取程式用，Libnet 是用來發送偽造的 ARP 封包用；攻擊者的電腦主機則採用一般等級的普通電腦，而攻擊軟體則是採用網路上很容易找到的監聽軟體 sniffer 和阻斷攻擊軟體 netcut。硬體規格與軟體版本如表 5-1 所示。

偵測防禦系統		攻擊者	
CPU	Intel Pentium4 2.8 G	CPU	Intel core 2 daul e6600
RAM	1 GB	RAM	1 GB
網路卡	Intel PRO/100	網路卡	Intel PRO/1000
作業系統	FreeBSD 6.4-stable	作業系統	Windows XP SP3
Web	Apache 2.2	監聽軟體	cain＆abel 4.9.35
程式語言	PHP 4.4.9 & C	阻斷攻擊軟體	Netcut 2.8
Mysql	Mysql 4.1.22		

表 5 - 1 硬體規格與軟體版本

5.2 實驗方法與結果

這裡以第四章設計的系統來做實際的測試，測試大致上分成偵測網路監聽、防禦 ARP 欺騙攻擊以及網路使用者管理；攻擊者在網路上針對某台主機實施攻擊，監看系統是否偵測得到該攻擊以及是否能有效防禦攻擊者的攻擊。

5.2.1 偵測網路竊聽

另一種方式是以偽造的 ARP 詢問封包廣播到網路上的每一台電腦，如果網路卡正處於任意模式，則封包會被網路卡所接收，且會回傳 ARP 回應封包，偵測主機接收到回應封包，便可判定傳送此封包的主機就是竊聽者。但是這裡必需要防止系統發送正常的 ARP 詢問封包，所以必需在偵測網路監聽主機時將網路卡的 ARP 功能取消。一旦偵測到竊聽主機後，以 ARP 欺騙方式使阻斷其正常連線。

下圖(圖 5-2)為偵測竊聽的測試環境，電腦 A 與電腦 B 傳輸資料，電腦 C 對電腦 A 與電腦 B 實施 ARP 欺騙，形成中間人攻擊型態，而偵測主機無法擷取到電腦 C 所發送的欺騙封包，所以無法對 ARP 封包作分析，所以才使用上述的方法來偵測竊聽主機。

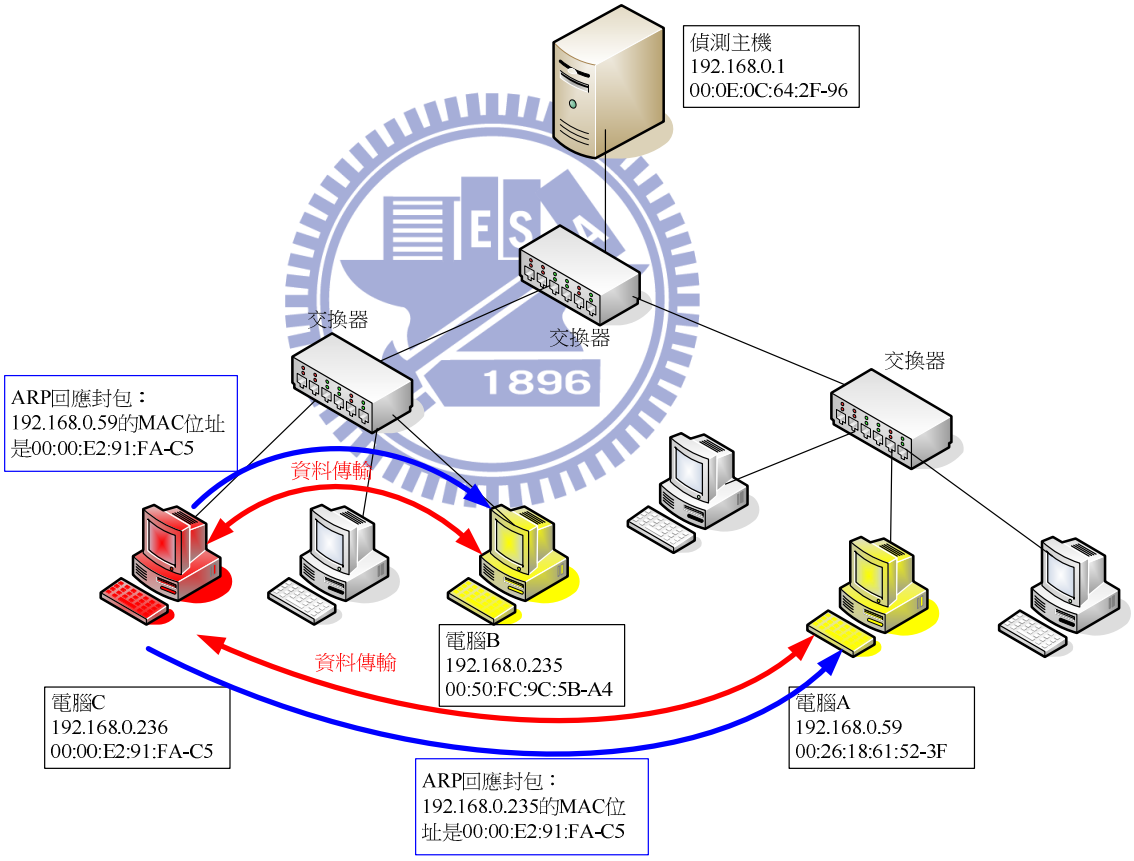


圖 5 - 2 偵測網路竊聽主機測試環境

實驗的方式以操作電腦 B 架設 FTP 伺服器，電腦 A 以 FTP 連線登入電腦 B，而電腦 C 以竊聽軟體監聽電腦 A 與電腦 B 之間的傳輸，比較在未使用本系統時與使用本系統後，偵測系統是否能偵測到處於任意模式的電腦主機，以及在阻斷竊聽主機後，電腦擷取密號密碼的情形。

執行監聽軟體監聽電腦 A 與電腦 B 之間的通訊時，由圖 5-3 可以看到電腦 A 的 ARP Table 中電腦 B 的 IP 位址所對應的 MAC 位址，由 00-50-fc-9c-5b-a4 變為 00-00-e2-91-fa-c5，由圖 5-4 可以看到電腦 B 的 ARP Table 中電腦 B 的 IP 位址所對應的 MAC 位址，由 00-26-18-61-52-3f 變為 00-00-e2-91-fa-c5，這時電腦 C(監聽者)已經成為電腦 A 與電腦 B 資料傳訊的中間人。

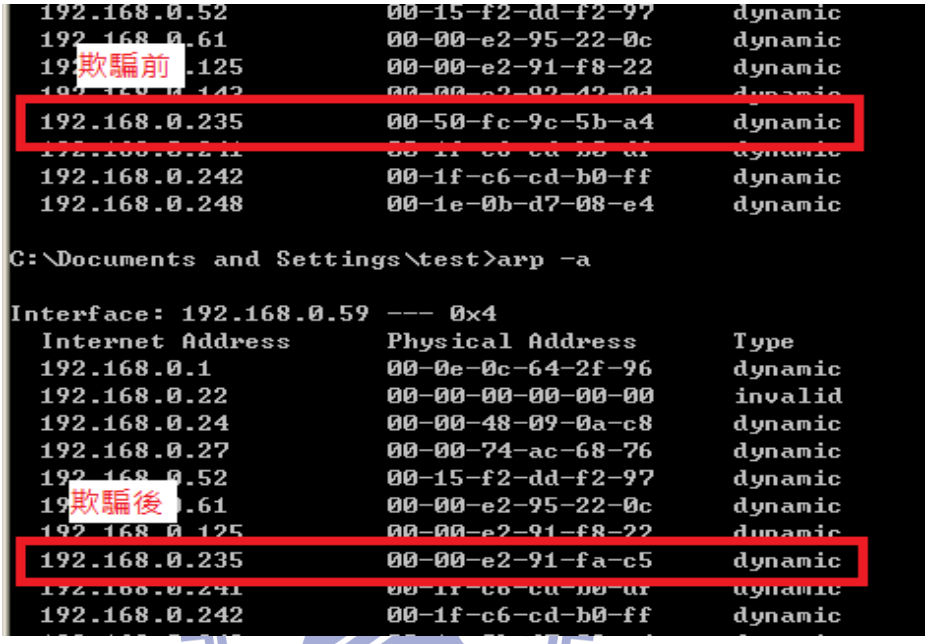


圖 5 - 3 電腦 A 的 ARP Table 紀錄變化情形

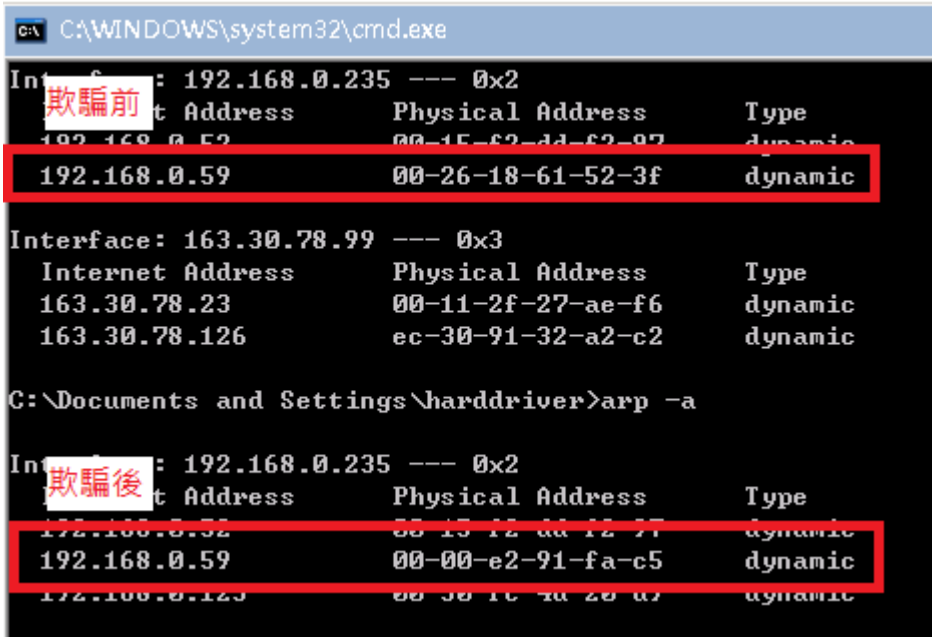


圖 5 - 4 電腦 B 的 ARP Table 紀錄變化情形

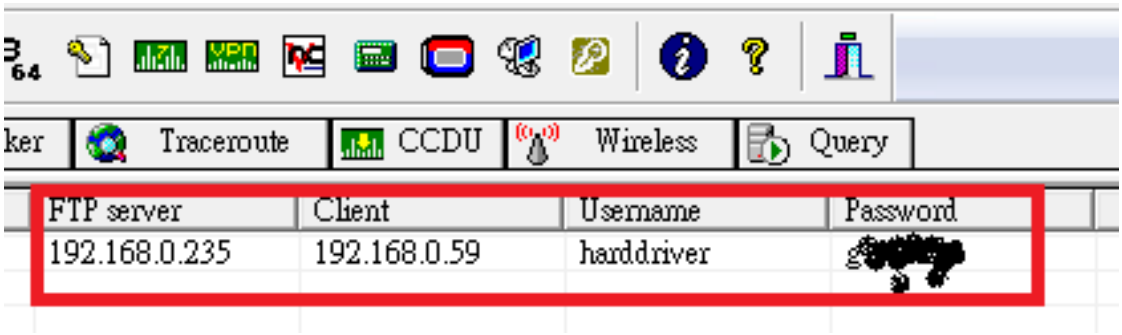


圖 5 - 5 監聽軟體擷取到登入 FTP 的帳號密碼

電腦 A(192.168.0.59)開始使用 FTP 軟體登入到電腦 B(192.168.0.235)，這時候監聽軟體便擷取到電腦 A 輸入的帳號密碼。這時使用本系統的偵測程式偵測到電腦 C(192.168.0.236)正在執行監聽，也就是偵測到電腦 C 的網路卡處於任意模式(如圖 5-6)。利用 ARP 欺騙程式改變電腦 C 的 ARP Table 中的紀錄(如圖 5-7)，這時電腦 C 傳送的任何封包都被傳住 11-22-33-44-55-66 這個不存在的 MAC 位址。

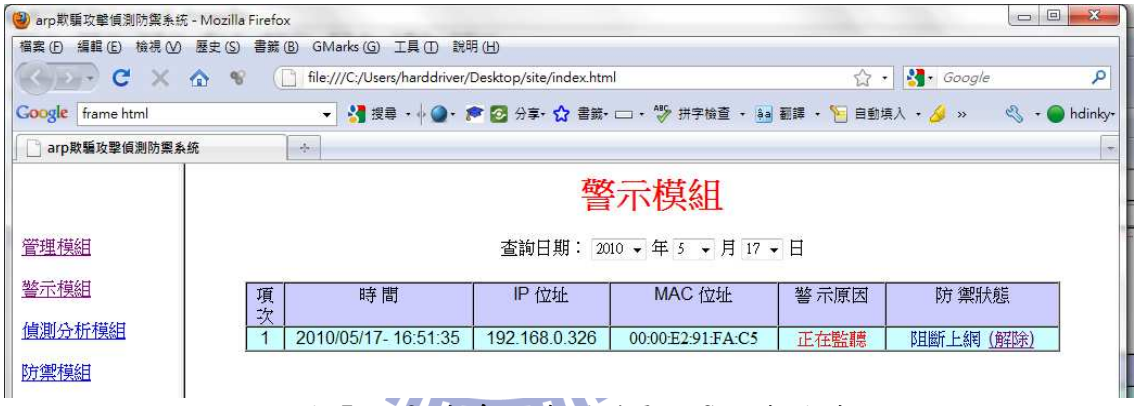


圖 5 - 6 本系統偵測到電腦 C 正在監聽

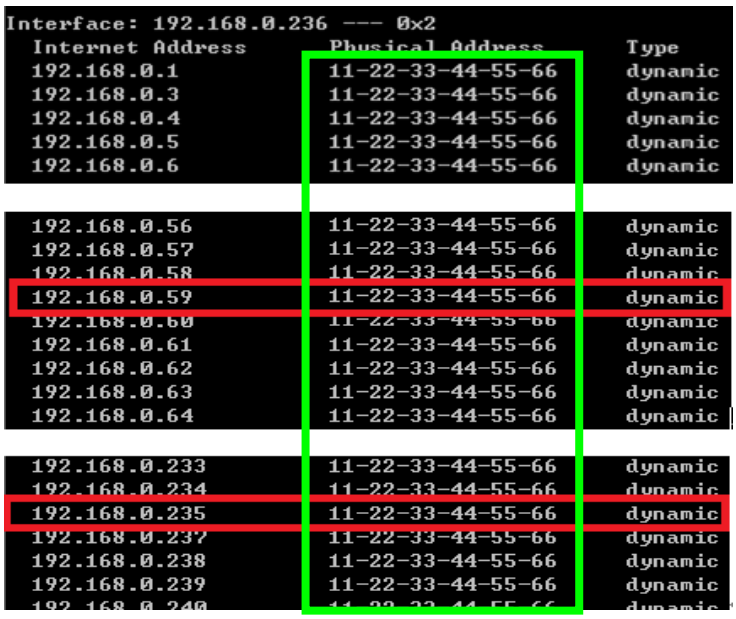


圖 5 - 7 以 ARP 欺騙攻擊阻斷電腦 C 上網

當電腦 C 被阻斷服務時，監聽程式持續持行監聽，電腦 A 再以 FTP 登入電腦 B，這個再觀察監聽軟體上的紀錄，發現監聽軟體還是擷取到了電腦 A 所輸入的帳號與密碼(如圖 5-8)。再次測試電腦 C 的連線上網的狀況，還是無法上網，且無法 ping 到電腦 A 與電腦 B。原因是在 ping 電腦 A 與電腦 B 時，封包傳送的目的位址，是以電腦 C 的 ARP Table 的紀錄為依據；而監聽軟體在成為中間人監聽時，已將電腦 A 與電腦 B 的 MAC 位址記錄在程式的快取中，故就算電腦 C 的 ARP Table 中的所有紀錄全是錯誤的，還是可以執行中間人攻擊。

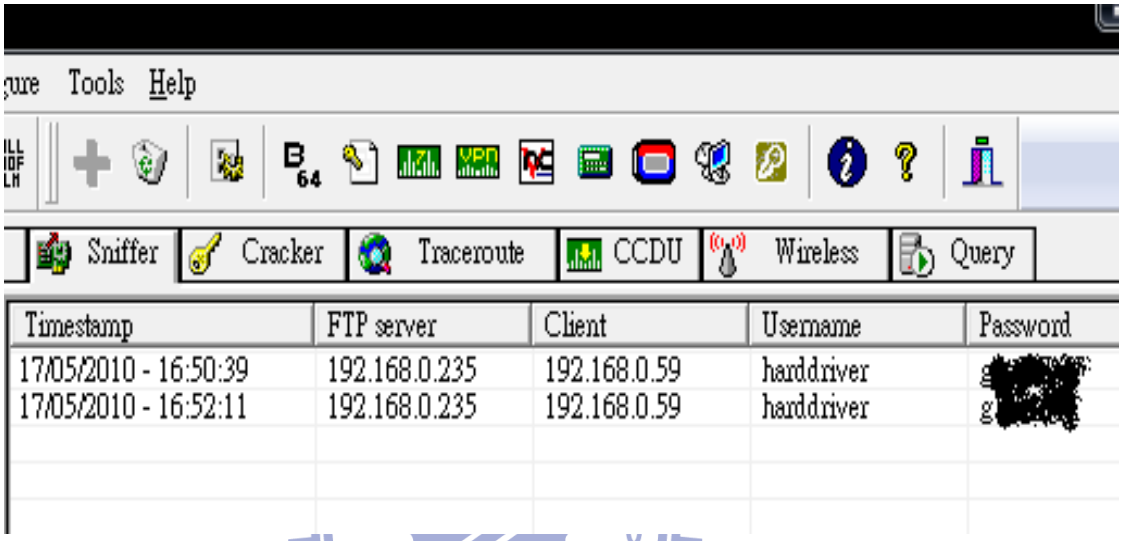


圖 5 - 8 監聽軟體再次擷取到登入 FTP 的帳號密碼

5.2.2 防禦 ARP 欺騙攻擊

網路竊聽是利用 ARP 欺騙所達成的，所以利用系統的偵測分析模組分析傳送者的 MAC 位址與 IP 位址對應，一偵測到錯誤對應，便廣播正確的 IP 位址與 MAC 位址對應關係的 ARP 回應封包給所有的電腦。這種方法只有用在竊聽者竊聽被竊聽者和閘道(Gateway)之間的傳輸，這種竊聽型態比較容易竊聽到有用的資訊，如信用卡卡號、帳號密碼、談話內容……等等。

下圖(圖 5-9)為偵測竊聽型態之一的環境狀態，電腦 C 為了竊聽電腦 A，對 Gateway 與電腦 A 持續傳送錯誤的 ARP 欺騙封包，電腦 A 要和 Gateway 傳送資料，就會把封包往電腦 C 送，而電腦 C 再把封包轉送到 Gateway，反之 Gateway 傳送資料給電腦 A 也會經由電腦 C 來轉送。

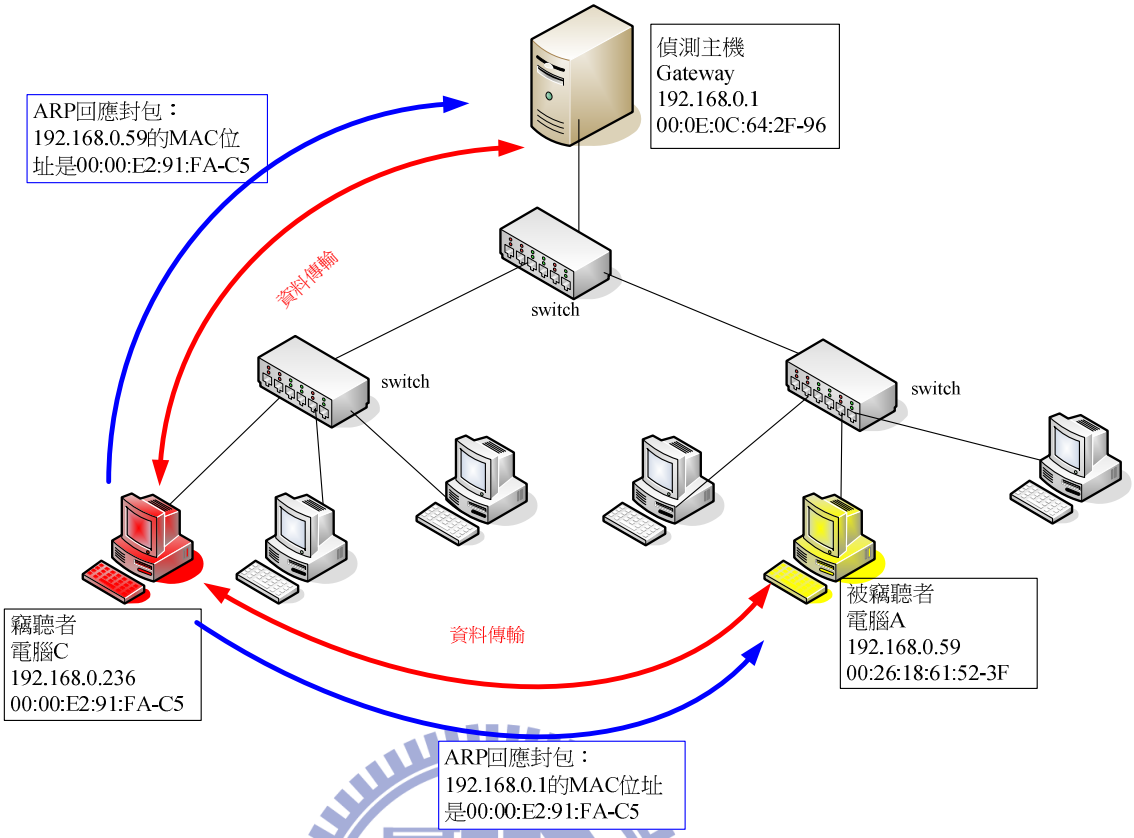


圖 5 - 9 防禦網路竊聽測試環境

實驗的方式以操作電腦 A 進行 telnet 連線 PTT BBS 網站，而電腦 C 以竊聽軟體監聽電腦 A 與 Gateway 之間的傳輸，比較在未使用本系統時與使用本系統後，電腦擷取密號密碼的情形。

使用監聽軟體執行監聽後，以電腦 A 執行 telnet 連線到 PTT BBS 網站，這時電腦 C 的監聽軟體便擷取到 telnet 的連線資料(如圖 5-10)，透過監聽軟體擷取的紀錄可以很清楚看到在電腦 A 連線 PTT BBS 網站時所登入的帳號密碼(如圖 5-11)。

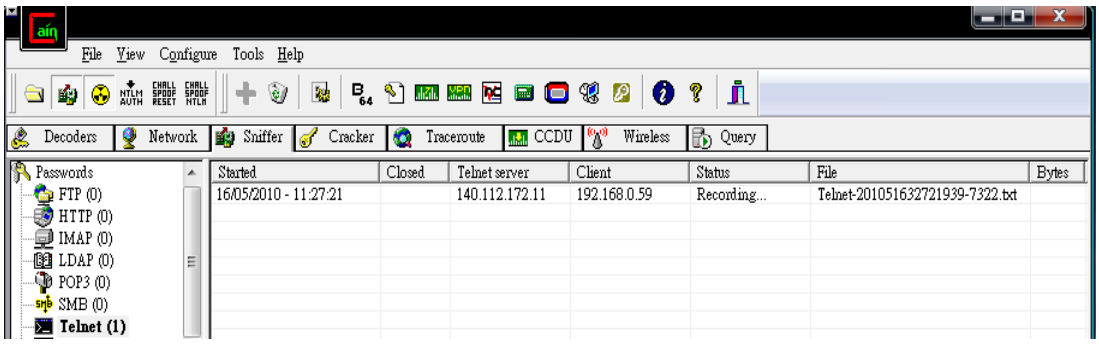


圖 5 - 10 監聽軟體擷取到登入 PTT BBS 的帳號密碼

圖 5 - 11 擷取 Telnet 連線帳號密碼

啟動本系統後，偵測主機的 ARP Table 便以資料庫中合法使用者的 MAC 位址與 IP 位址對應關係登記為靜態 ARP 紀錄後，開始分析接收到的 ARP 封包中傳送傳的 IP 位址與 MAC 位址。不久便分析到有問題的 ARP 封包，此封包傳送者的 IP 為 192.168.0.59，而 MAC 位址為 00-00-e2-91-fa-c5。

圖 5 - 12 本系統偵測到 ARP 欺騙封包

本系統偵測到此有問題封包便廣播 ARP 詢問封包，其傳送者的 IP 為 192.168.0.59，MAC 位址為 00-26-18-61-52-3f 與傳送給電腦 A 一個 ARP 回應封包，修正電腦 A 的 ARP Table 中 Gateway 的位址紀錄。再以 Telnet 登入 PTT BBS 網站

後，再觀看監聽軟體擷取封包情形，發現監聽軟體上看不到擷取的封包資料，證明本系統在防禦 ARP 欺騙攻擊的網路監聽有效。

在阻斷服務攻擊部份，網路上最常看到的 Netcut 軟體，是利用 ARP 欺騙方式，改變欲攻擊的對象的 ARP Table 裡的紀錄，讓被攻擊無法與 Gateway 通訊連線，如此便達到阻斷攻擊。下圖(圖 5-13)就是這次測試的環境示意圖，電腦 C 發送偽造的 ARP 封包給電腦 A，使得電腦 A 的 ARP Table 裡 Gateway 的 MAC 位址是一個錯誤的 MAC 位址，電腦 A 想把封包傳送到 Gateway，但訊框的目標位址是一個錯誤的 MAC 位址，所以封包傳送出去後找不到這個錯誤的 MAC 位址，故無法傳送到 Gateway；如果電腦 C 以相同的手法阻斷 Gateway 與電腦 A 的通訊連線，電腦 A 對外的連線就完全被阻斷了。

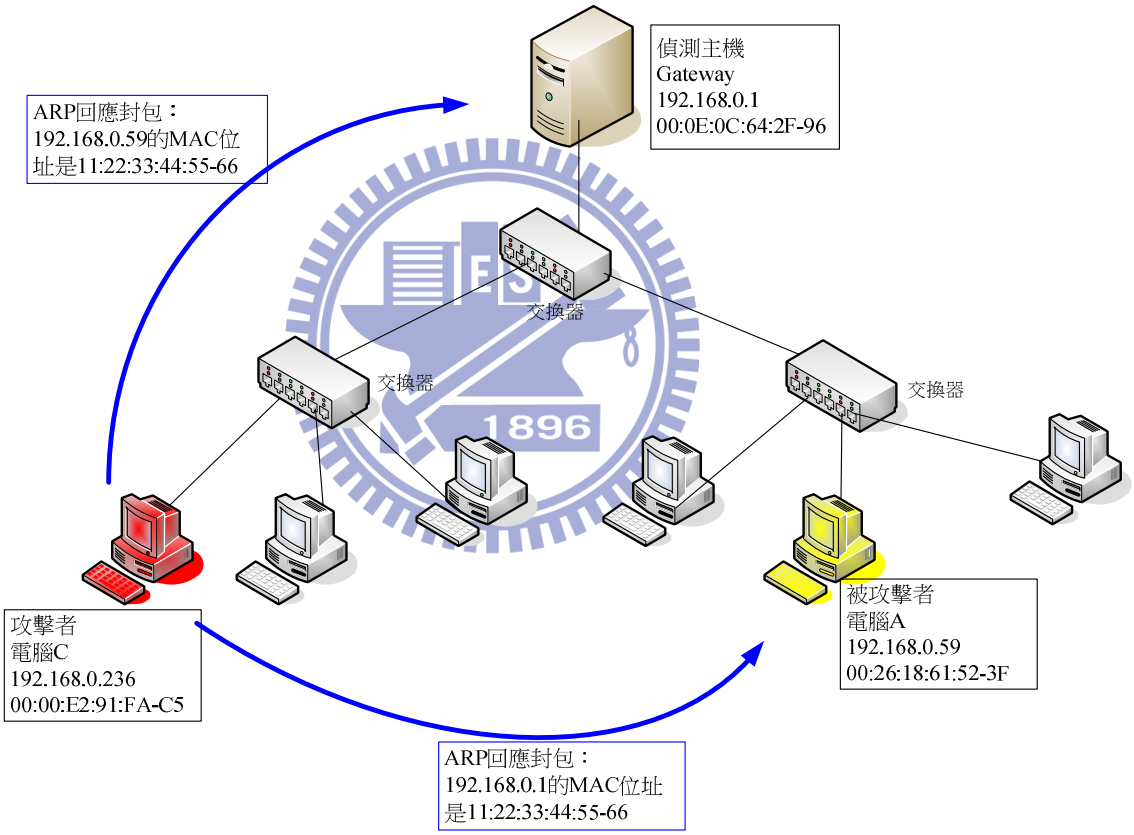


圖 5 - 13 阻斷性攻擊的測試環境

實驗的方式以電腦 A 正常模式下開啟瀏覽器上網，電腦 C 再以 Netcut2.8 軟體對電腦 A 實施阻斷攻擊，使得電腦 A 對外連線受阻，而無法正常正常瀏覽網頁；當偵測分析模組偵測到電腦 A 的 MAC 位址錯誤時，啟動防禦機制，傳送正確的位址資訊封包給電腦 A，再來測試電腦 A 是否能正常瀏覽網頁。

在電腦 C 上以 Netcut 軟體對電腦 A 執行阻斷服務攻擊(如圖 5-14)，此時電腦 A 的 ARP Table 中 Gateway 的 IP 位址與 MAC 位址紀錄已遭電腦 C 欺騙(如圖 5-15)，

在電腦 A 上開啟 IE 瀏覽器上網，發現瀏覽器無法呈現首頁，ping Gateway 的 IP 位址時，都呈現主機關機狀態。

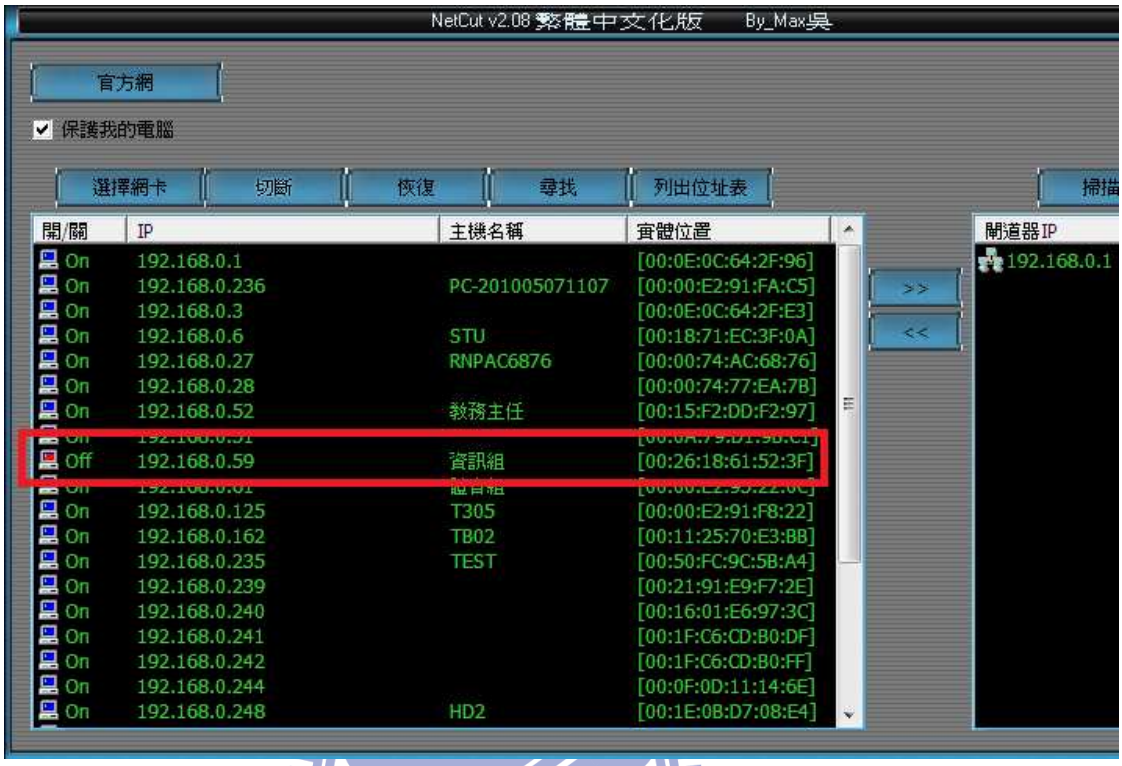


圖 5 - 14 以 Netcut 執行阻斷服務攻擊

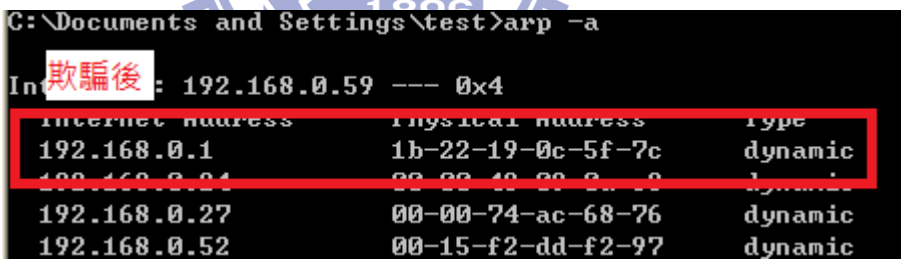


圖 5 - 15 電腦 A 的 ARP Table 中 Gateway 的 MAC 位址被更改

啟動本系統後，防禦模組便將資料庫中合法使用者的 MAC 位址與 IP 位址對應關係在 NAT 的 ARP Table 中登記為靜態 ARP 紀錄，在警示模組上可以看到多筆 ARP 的欺騙封包紀錄(如圖 5-16)，且防禦模組已傳送修正的 ARP 封包。觀察電腦 A 的 ARP Table 中發現 Gateway 的 MAC 位址已被更正，再使用 IE 瀏覽器瀏覽網頁，此時網頁可以正常呈現，ping Gateway 的 IP 位址時，也出現回應的訊息，證明本系統可以解決區域網路中的 ARP 欺騙攻擊事件。

項次	時間	IP 位址	MAC 位址	警示原因	防禦狀態
1	2010/05/18- 16:11:17	192.168.0.59	1E:2A:4F:3D:22:55	MAC錯誤	傳送修正封包
2	2010/05/18- 16:11:47	192.168.0.59	1A:24:5A:F2:45:A1	MAC錯誤	傳送修正封包
3	2010/05/18- 16:12:17	192.168.0.59	3F:1D:77:4A:3F:2B	MAC錯誤	傳送修正封包
4	2010/05/18- 16:12:47	192.168.0.59	0F:A3:F3:2A:DD:34	MAC錯誤	傳送修正封包
5	2010/05/18- 16:13:17	192.168.0.59	F6:55:A3:42:34:E9	MAC錯誤	傳送修正封包
6	2010/05/18- 16:13:47	192.168.0.59	D4:33:F6:BB:23:11	MAC錯誤	傳送修正封包
7	2010/05/18- 16:14:17	192.168.0.59	A3:44:B6:C2:14:61	MAC錯誤	傳送修正封包
8	2010/05/18- 16:14:47	192.168.0.59	0A:32:E3:FF:33:45	MAC錯誤	傳送修正封包
9	2010/05/18- 16:15:17	192.168.0.59	0C:A0:C2:B1:BA:A5	MAC錯誤	傳送修正封包
10	2010/05/18- 16:15:47	192.168.0.59	D3:A0:E2:97:F3:B2	MAC錯誤	傳送修正封包
11	2010/05/18- 16:16:17	192.168.0.59	B2:31:05:7A:60:C5	MAC錯誤	傳送修正封包
12	2010/05/18- 16:16:47	192.168.0.59	70:A1:23:82:BA:F5	MAC錯誤	傳送修正封包
13	2010/05/18- 16:17:17	192.168.0.59	A0:33:7A:32:B6:A1	MAC錯誤	傳送修正封包

圖 5 - 16 警示模組中出現阻斷服務攻擊訊息

5.2.3 網路使用者管理

網路使用者管理是屬於後端管理模式，最主要是利用 ARP 欺騙方式阻斷區域網路上非法的使用者，而判斷非法使用者的方式，是與資料庫裡面合法的 IP 位址與 MAC 位址的對應做比對，如果使用者的 IP 位址與 MAC 位址不在資料庫裡，則使用 ARP 欺騙阻斷該電腦主機無法正常上網。

非法使用者有三種情形，第一種是 IP 位址與 MAC 位址皆不在資料庫中，第二種是 IP 位址或 MAC 位址其中一個不在資料庫中，第三種情形是 IP 位址與 MAC 位址在皆在資料庫中，但位址對應錯誤。第一種情形的實驗方法就是將一台新的電腦連上區域網路，而其 MAC 位址與 IP 位址皆不在資料庫中，再測其是否能正常上網；第二種情況的實驗方法就是將新電腦設成原本就有的 IP 位址，這樣 IP 位址會在資料庫中，但是 MAC 位址不在資料庫中，另一種是將原本的合法使用者電腦的 IP 位址改成另一個不存在資料庫中的 IP 位址；第三種情況是將兩台合法使用者的 IP 位址對調。

在第一種實驗狀態下，在區域網路中接上一台新的電腦，IP 位址設定為 192.168.0.236，而其 MAC 位址為 00:00:E2:91:FA:C5，在使用者管理頁面(如圖 5-18)可以看到此電腦被阻斷，原因是此電腦為不明主機。如果這台電腦是採購的電腦，可以在設定的地上將其設定為合法後，此電腦便可合法使用網路資源，也節省管理者在設定新使用者 IP 位址與 MAC 位址對應的時間。

圖 5 - 17 當 IP 與 MAC 未列於合法使用者資料庫時的使用者管理頁面

在實驗的第二種情況下，將新電腦原本的 IP 位址由 192.168.0.236 改為 192.168.0.10，且將原本 IP 為 192.168.0.52 與 MAC 位址為 00:0C:76:E0:0B:F9 的合法使用者電腦的 IP 改為 192.168.0.236 非法 IP，此時使用者管理頁面(如圖 5-19)的編號 3 便出現 MAC 位址錯誤，與編號 4 出現 IP 位址錯誤，且狀態是被阻斷的。

在實驗的第三種情況，將 IP 位址為 192.168.0.3 與 192.168.0.6 的這兩台電腦的 IP 互換，此時使用者管理介面(如圖 5-19)的編號 1 與編號 2 便出現 IP 與 MAC 對應錯誤的狀態，且電腦狀態是被阻斷的。

圖 5 - 18 當 IP 或 MAC 資料錯誤時的使用者管理頁面

第六章 結論與未來方向

ARP 欺騙攻擊是利用 ARP 運作的過程中對 ARP 封包缺乏認證，也因此啟動對 ARP 欺騙攻擊長期抗戰。而在對抗 ARP 欺騙攻擊中以硬體設備防堵 ARP 欺騙最為直接，而軟體方面最多只能做到偵測與使用者端本身的防禦。

本章就第五章實驗的過程與結果做一個總整理，並針對每個實驗的結果做一個探討，呈述本系統的優缺點，並與第三章相關研究中偵測 ARP 欺騙做一個比較，最後再針對本系統不足的地方提出未來研究的方向，讓本系統能有研究進步的空間。

6.1 討論與結論

本系統的最主要目的是對 ARP 欺騙封包做主動的防禦，而偵測網路攻擊主機的部份只能由 ARP 欺騙封包中的傳送者位址資料來分析。本系統將 Zouheir 等人的研究納入，成為偵測監聽主機的一大利器，此方法可以有效偵測到正在監聽的電腦；利用 ARP 欺騙方式阻斷監聽的電腦，雖然可以有效的讓攻擊者無法正常上網，但是卻無法變更已將位址資料存入監聽軟體快取，所以監聽攻擊怎法被有效防止。

上述的方法是積極的對攻擊者阻斷，得到的效果並不理想；另一種是以消極的方式來防禦被攻擊者，本系統是以 ARP 欺騙方式將原本被攻擊者的 ARP Table 中錯誤的位址對應關係導正，讓被攻擊者在傳輸封包時有正確的依據。在實驗中以中間人攻擊與阻斷服務攻擊對被攻擊者實施攻擊，由於攻擊軟體除了會對被攻擊者欺實施 ARP 欺騙外，也會對 Gateway 做 ARP 欺騙，而本系統則是利用攻擊者對 Gateway 的 ARP 欺騙封包去獲取被攻擊者的位址，並將 Gateway 的正確位址資訊以 ARP 欺騙方式傳送到被攻擊者，讓被攻擊者的 ARP Table 中 Gateway 的 MAC 位址是正確的，如此便可對外正常連線。

而使用者管理在本系統也一個很重要的基礎工作，其目的在建立合法使用者的 IP 位址與 MAC 位址的對應資料庫。當攻擊者的 IP 位址或 MAC 址其中一項不在資料庫中，或是 IP 位址與 MAC 位址在資料庫中，但對應關係錯誤時，本系統都會對此電腦實施阻斷攻擊。這意味者攻擊者無法偽造 IP 位址或 MAC 位址來混淆本系統的封包分析，也就是說當警示模組上面呈現的攻擊主機位址資訊是正確的，此時可以採人工方式檢查此位址的電腦是否被安裝 ARP 欺騙攻擊軟體。

將系統功能與實驗的結果做整理並與劉修仁、楊文龍、CISCO 的偵測防禦系統

做比較，比較表如下：

	本系統	劉修仁	楊文龍	CISCO
建位合法使用者資料庫	可	否	可	可
阻斷非法使用者使用網路	可	否	可(人工)	可
偵測監聽主機	可	可	可	可
偵測阻斷攻擊主機	否	否	可	可
防禦對外網路連線監聽	可(自動)	只防禦使用者端	可(人工)	可(自動)
防禦阻斷對外網路連線	可(自動)	只防禦使用者端	可(人工)	可(自動)
網路環境的SWITCH	一般	一般	需有支援 SNMP	需有支援 DAI
系統環境建置成本	低	低	高	高

表 6 – 1 ARP 偵測防禦系分析比較表

6.2 未來方向

本系統是利用 ARP 欺騙方式來修正被欺騙的電腦之 ARP Table，而在偵測的功能上，只能部份偵測到攻擊主機，且偵測到攻擊主機時，不能完全將其阻斷，所以本系統只是治標不治本。

在參考 ARP 偵測防禦相關文獻時，發現一套寫在網路設備韌體上的作業系統，此系統平台是一個小型的 linux 作業系統名叫 OpenWrt[17]。而本系統中偵測模組與防禦模組是以 C 語言所寫成，所以直接將模組嵌入 OpenWrt 中，並將偵測模組中偵測位址資訊中加入埠號口，便可監視 switch 上每一個埠口的封包，發現封包有問題，但可以直接將此埠口切斷連，達到完全偵測且完全自動防禦的系統架構。

參考文獻

[1] Behrouz A. Forouzan、Sophia Chung Fegan著陳中和、王振傑譯《TCP/IP通訊協定 第三版》麥格羅・希爾， 2006年1月。

[2] D. Plummer, "*Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48-bit Ethernet Address for Transmission on Ethernet Hardware*", RFC 826, 1982.

[3] TCP/IP http://lips.lis.ntu.edu.tw/YTCHIANG/STUDY/others/tcpip/TCPIP.htm

[4] WIKI ARP http://en.wikipedia.org/wiki/Address_Resolution_Protocol

[5] 鳥哥的linux私房菜--簡易的網路基礎概念 http://linux.vbird.org/linux_server/0110network_basic.php

[6] 中間人攻擊 http://firekou.pixnet.net/blog/post/23300253

[7] 曾憲民，<非法連網自動偵測與資源效能監控機制>，碩士論文，東華大學資訊工程研究所，96年5月。

[8] Trabelsi, Z., Rahmani, H., Kaouech, K., Frikha M., "Malicious Sniffing Systems Detection Platform", roceedings of the International Symposium on Applications and the Internet, pages 201-207, 2004.

[9] 劉修仁，<在交換式乙太區域網路中防範封包監聽之研究>，碩士論文，義守大學資訊工程研究所，93年6月。

[10] 楊文龍，<基於SNMP之ARP攻擊偵測研究>，碩士論文，暨南大學資訊管理研究所，97年7月。

[11] CISCO 安全機制 From http://blog.yam.com/magicianlee/article/14018860

[12] Port SECURITY From http://dbmaker.syscom.com.tw/mag/140/tech_01.htm

[13] PORT SECURITY from http://itknowledgeexchange.techtarget.com/network-technologies/introduction-to-port-security-and-the-reasons-to-implement/

[14] DAI from http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_2/security/configuration/guide/n1000v_security_13arpinspect.html

[15] DAI from http://www.ringline.com.tw/epaper/Forum961101.htm

[16] 中信局共同供應契約-資訊設備-電腦周邊設備(契約號：**LP5-970061**)

[17] OpenWRT from http://openwrt.org/