國防科技學術合作協調小組研究計畫成果報告

路由類通訊協定的弱點分析

計畫編號：NSC 90-CS –7-009 -002

執行期間： 90 年 01 月 01 日至 90 年 12 月 31 日

計畫主持人：謝續平 教授暨系主任

共同主持人：

執行單位：交通大學資訊工程系所

中華民國 90 年 12 月 日

目　次

提　要

關鍵詞： 路由器 ， 網路安全

由於提供更方便及快速的傳遞資訊 ， 網際網路在近幾年來風行全世界 ， 許多電腦也連結在網際網路上以使用者個方便的媒介 ， 但伴隨而來的問題卻是連結在網際網路上的所有電腦主機共同面對的網際網路安全性 。

在現今的網路結構下 ， 通訊雙方欲透過網路進行交流 ， 多半是利用封包交換 (Packet Switching) 的方式 ， 而路由器 (Router) 正是實際負責傳送封包的網路元件 。 針對路由器所提供的服務，正確性與安全性是不可缺的 。 路由器的安全性與正確性導致路由器之間的溝通與路由器下的網路有很多安全上的問題。

有鑑於此，本計畫擬從網路上負責傳送封包的路由器著手，對於路由類網路通訊協定的相關規範與資料加以蒐集、整理並分析其弱點，並研究目前主流的路由器的設計。本計劃能夠提供完整的資料，以為今後改良或設計新的路由類網路安全協定之重要參考；此外，本計畫之研究成果，也將能為補強或發展路由器提供一份研究報告。雙管齊下，強化網路對抗網路攻擊之能力，降低網路攻擊的發生概率，進而減少因網路攻擊而造成的種種損失。

第一章　簡介

1.1　緒論

隨著網際網路的大力風行，企業與政府機關也都紛紛透過網際網路提供便捷的服務與網際網路的整合已成趨勢，愈來愈多的應用系統將在這個網路上被執行，然而網路上駭客橫行，網路安全是急待克服的難題。

在現今的網路結構下，通訊雙方欲透過網路進行交流，多半是利用封包交換的方式，而路由器正是實際負責傳送封包的網路元件。駭客欲對目標主機發起攻擊，也必須透過這樣的管道，才能將發起攻擊所必備的資訊傳到目標主機，除此之外，路由器本身也可能遭受網路攻擊。一旦路由器遭攻擊，則封包將因無法正確傳送(Routing)而導至網路大亂、出入某子網路(Subnet)的封包遭攔截而造成此子網路被孤立、流經路由器的封包遭駭客竊視，甚至網路可能因路由器損毀而癱瘓，影響甚鉅。

有鑑於此，本計畫除了將對路由類通訊協定之相關資料進行蒐集、整理與弱點分析之外，也將蒐集主要 Router 的設計弱點與組態弱點，期能藉由本計畫之研究成果，對於路由類通訊協定與主要的 Router 提供有系統的統整報告，方便今後相關研究進行查閱，並讓相關之技術發展能擁有更多方面的考量。

1.2　報告編排

本報告將針對計畫的研究成果做一個說明，範圍包含十三個路由類通信協定詳述和路由類通信協定相關之漏洞分析，並針對 Cisco ， Lucent ， 3Com ， Extreme Network ， Xylan Network 暨 Cabletron 路由器作弱點分析與提供弱點的解決方法。主要成果分兩大部分：

（一）十三個通信協定詳述，漏洞分析與解決方法。

（二）六種路由器攻擊案例，弱點分析與解決方法。

第二章 路由器通信協定詳述與漏洞分析 ： 分為通信協定詳述，參考資料， 以及有可能存在的漏洞三方面來探討十三個路由器通信協定並分析各種有可能存在的弱點與解決方法，此達到說明十三個路由器通信協定漏洞的效果。路由類通信協定所存在的漏洞可歸納成兩大原因：

1. 當通信協定的某些欄位被偽造，而剛好那個通信協定對那些欄位沒有做檢查

的動作，則此通信協定若在實作上剛好用到那些欄位，便會造成一個可能存在的漏洞。

2. 當設定通信協定時，沒有把安全機制設好，而在實作造成可能存在的漏洞。

第三章 路由器漏洞分析 ： 對於六種路由器已被發現的弱點依照路由器廠商分為

- Cisco 路由器
- Lucent 路由器
- 3Com 路由器
- Extreme Network 路由器
- Xylan Network 路由器
- Cabletron 路由器

共 6 類 ， 並對於各種路由器已被發現的弱點依照弱點類別再分為 ：

1. Denial of Service (阻斷式攻擊)

   此為一般 router or switch 最常發生的弱點，只要是系統實作缺失，或者軟體某部分有問題，都很容易最直接產生這項問題，因為此項問題並不牽涉到高深的入侵技巧，攻擊者只需找出有問題的程式或硬體部分，對該部分做影響即可牽動整個系統。

   此次收集到的 DOS 弱點，共有下列幾項方式達到對該設備 DOS 的作用：

   1. 直接使該設備 crash。
   2. 使該系統重新開機(重新開機期間將導致無法正常服務)。
   3. 使該系統某運作進入無限迴圈。
   4. 僅使某項服務停止運作。
   5. 使得流量轉向某些介面卡，使其承受更大流量導致無法正常運行。

   注意到路由器上的 DOS 攻擊僅只有第五項是因流量造成，而其他幾乎皆是使該機器停擺或 reboot 導致無法正常服務。

2. Can Access Restricted resource(非法存取)

   此項弱點可能導致某些較低權限的使用者可以使用非經允許的資源，譬如像是可以使用到非經授權的服務，或執行某些不該執行的檔案，或不用經認證就可以瀏覽某些檔案或目錄。

3. View or modify configuration(偷閱或更改系統設定)

   此項問題也與上述弱點類似 ， 也是在非經授權下 ， 可以觀看或更改

某些系統設定，這將可以觀看到他人的資料或者藉由更改系統設定而達到其他攻擊目的。資訊外洩或系統設定被更動將會是比 DOS 攻擊影響更為嚴重，因為 DOS 攻擊頂多造成無法服務，但是資訊外洩或被更動，系統管理者將很難去發現系統被做了什麼手腳或資訊外洩造成的影響有多大，而且恐怕經過了一段時間才會發現自己的系統曾經被人偷看或更動。

4. Flaw of the Implementation/specification（實作或規格上的缺失）
某些規格上的設計缺失，或者系統實作時的漏洞，導致某些安全上的漏洞，譬如像是 Cisco CVCO-4k Remote Username and Password Retrieval 漏洞，該認證系統的密碼竟使用簡單的代換密碼 (substitution cipher)，這將很容易被簡單的破譯工具破解密碼，而 Cisco Catalyst 2900 VLAN 漏洞，是規格上的缺失，兩不同 VLAN 之間原本不該有 frame 互相流通，但是規格上的失誤導致產生了此項問題。這形成了不太安全的環境，這將無法達到原本設定的目標。

5. Lost Access Control (Access Control 失效)
Access Control 失效，分為兩項：
   1. 該設備無法經由設定好的 rule 來過濾封包或過濾連線。這將導致無法過濾掉惡意的使用者來源。
   2. 該設備的管理系統的認證措施失效，導致任何人可以不需認證即可控管該機器。這更是一項危險的漏洞，任何人不需打密碼即可使用該機器上的進階服務。

在受到影響的系統，弱點詳述，解決方法以及參考資料的分類欄位中對每一種路由器弱點做詳細的說明與整理，使整份報告成為更容易閱讀的文件。

以下為 Cisco 路由器已發現的弱點列表：

1. Denial of Service (阻斷式攻擊)
   - Cisco Discovery 通信協定漏洞
   - Cisco 675 Web Admin 漏洞
   - Cisco 7xx Series Router DoS 漏洞
   - Cisco Catalyst Memory Leak 漏洞
   - Cisco Catalyst SSH Protocol mismatch DOS
   - Cisco Catalyst Supervisor Remote Reload
   - Cisco Content Service Switch Long Name DOS
   - Cisco IOS HTTP Request ?/ 漏洞
   - Cisco IOS Remote Router Crash 漏洞

- Cisco IOS Software Telnet Option Handling 漏洞
- Cisco IOS Syslog Crash
- Cisco IOS-700 Router Password Buffer Overflow
- Cisco 7xx Password Buffer Overflow 漏洞
- Cisco TAC+ DOS 漏洞
- Cisco IOS HTTP %% 漏洞

2. Can Access Restricted resource(非法存取)
   - Cisco Catalyst 3500XL Remote Arbitrary Command Execution 漏洞
   - Cisco Content Switch Directory Structure File Reading 漏洞
   - Cisco Router Online Help 漏洞

3. View or modify configuration(偷閱或更改系統設定)
   - Cisco Aironet Web Administration Access 漏洞
   - Cisco IOS ILMI SNMP Community String 漏洞
   - Cisco PIX Passive Mode FTP Internal Address Disclosure 漏洞

4. Flaw of the Implementation or specification (實作或規格上的缺失)
   - Cisco Catalyst 2900 VLAN 漏洞
   - Cisco Web Cache Control Protocol Router 漏洞
   - Cisco IOS TCP Initial Sequence Number 漏洞
   - Cisco CVCO-4k Remote Username and Password Retrieval 漏洞

5. Lost Access Control (Access Control 失效)
   - Cisco Catalyst Enable Password Bypass 漏洞
   - Cisco Gigabit Switch Router ACL Bypass 漏洞
   - Cisco IOS CHAP Authentication 漏洞
   - Cisco IOS Extended Access List Failure 漏洞
   - Cisco IOS Software Input Access List Leakage with NAT
   - Cisco IOS Established Access Keyword 漏洞

以下為 Lucent 路由器已發現的弱點列表：

1. Denial of Service (阻斷式攻擊)
   - Ascend Max UDP Port 漏洞
   - Lucent Postmaster DOS 漏洞

2. Flaw of the Implementation or specification (實作或規格上的缺失)
   - 可預測的 Initial TCP Sequence Number 漏洞

3. Can Acess Restricted Resource (非法存取)

- Lucent Orinoco 封閉網路非授權存取漏洞
- Lucent RADIUS Buffer Overflow 漏洞

以下為 3Com 路由器已發現的弱點列表：

1. Denial of Service (阻斷式攻擊)

- 3com Office Connect DSL 路由器漏洞
- 3com Home Connect 纜線書籍路由器漏洞

2. Can Access Restricted resource (非法存取)

- 3com SwitchesBackdoor 漏洞
- 3Com AirConnect 無線閘門非存取漏洞

3. View or modify configuration (偷閱或更改系統設定)

- 3com HiPer Arc Community Name 漏洞

4. Flaw of the Implementation or specification (實作或規格上的缺失)

- 3com Corebuilder & Superstack II LAN Switch 漏洞
- 3COM SuperStack II 交換機 1001 的預設帳號和密碼漏洞

5. Lost Access Control (Access Control 失效)

- 3com Total Control Filter Bypass 漏洞

以下為 Extreme 路由器已發現的弱點列表：

1. Denial of Service (阻斷式攻擊)

- Extreme Network 嵌入系網頁伺服器漏洞

以下為 Xylan-OmniSwitch 路由器已發現的弱點列表：

1. Flaw of the Implementation or specification (實作或規格上的缺失)

- Xylan-OmniSwitch ftp 漏洞
- Xylan-OnmiSwitch-login 漏洞

以下為 Cabletron 路由器已發現的弱點列表：

1. Denial of Service (阻斷式攻擊)

- Cabletron Smart Switch Router ARP Flood DOS 漏洞

2. Flaw of the Implementation or specification (實作或規格上的缺失)

- Cabletron Spectrum Enterprise Manager 5.0 漏洞

第二章　路由類通信協定詳述與漏洞分析

2.1. BGP

2.1.1. 通信協定詳述

Border Gateway Protocol Version 4〈BGP-4〉，這是目前 internet 上最常使用的 exterior routing protocol。BGP 主要是距離-向量〈distance-vector〉演算法為主的 protocol。

BGP 使用 TCP ,和 port 179 作為其通訊協定，當 BGP 開始運作，BGP 端點便互相交換彼此的 routing tables，如果這些 routing tables 很大的話，就只交換有改變的資訊，這樣使得 BGP 協定更有效率。

BGP 繞境資訊的最小單位是 BGP path。另外 BGP 雖然是一個 distance-vector 協定，但是和大部分的 RIP 不同，BGP 不但計算到每個目的地的花費，並且還會持續紀錄使用的路徑，並且會週期性的告訴每個相鄰的機器到每個目的地可能的花費，以及正在使用的路徑。

由於外部繞境協定〈EGPs〉必須考慮到繞境政策的問題，譬如某個 AS 不想負責轉送某些 AS 來的封包，這些都可以在 BGP 裡面由手動的方式來進行設定。這些設定並雖不屬於 BGP 協定的一部分，但是 BGP 都有支援這個功能〈可以在 configuration 裡〉，因此我們稱 BGP 為一種『policy-based routing protocol』。BGP 不但有讓 AS 挑選不同路徑的能力，也不必像傳統的 EGP protocol ，倚賴中央集權控制的路徑仲裁機構。也就是不需要所謂的 core gateway 也可以交換和選擇路徑。

2.1.2. 參考資料

- RFC 1105: Border Gateway Protocol〈BGP〉, Obseleted by RFC 1163
- RFC 1163: Border Gateway Protocol〈BGP〉, Obseletes RFC 1105, Obseleted by RFC 1267
- RFC 1164: Application of the Border Gateway Protocol in the Internet, Obsoleted by RFC 1268
- RFC 1265: BGP protocol analysis

- RFC 1266: Experience with the BGP protocol
- RFC 1267: Border Gateway Protocol 3 (BGP-3), Obseletes RFC 1163
- RFC 1268: Application of the Border Gateway Protocol in the Internet, Obseletes RFC 1164, Obseleted by RFC 1655
- RFC 1269: Definitions of managed objects for the Border Gateway Protocol
- RFC 1364: BGP OSPF Interaction, Obsoleted by RFC 1403, Also RFC 1247, RFC 1267
- RFC 1397: Default Route Advertisement In BGP2 And BGP3 Versions Of The Border Gateway Protocol
- RFC 1403: BGP OSPF Interaction, Obsoletes RFC 1364
- RFC 1654: A Border Gateway Protocol 4 (BGP-4), Obsoleted by RFC 1771
- RFC 1655: Application of the Border Gateway Protocol in the Internet, Obsoletes RFC 1268, Obsoleted by RFC 1772
- RFC 1656: BGP-4 Protocol Document Roadmap an Implementation Experience, Obsoleted by 1773
- RFC 1657: Definitions of Managed Objects for the Fourth version of the Border Gateway Protocol (BGP-4) using SMIv2
- RFC 1745: BGP4/IDRP for IP---OSPF Interaction
- RFC 1771: A Border Gateway Protocol 4 (BGP-4), Obsoletes RFC 1654
- RFC 1772: Application of the Border Gateway Protocol in the Internet, Obsoletes RFC 1655
- RFC 1773: BGP-4 Protocol Document Roadmap and Implementation Experience, Obsoletes RFC 1656
- RFC 1774: BGP-4 Protocol Analysis
- RFC 1863: A BGP/IDRP Route Server alternative to a full mesh routing
- RFC 1965: Autonomous System Confederations for BGP, Obsoleted by RFC 3065
- RFC 1966: BGP Route Reflection An alternative to full mesh IBGP, Updated by RFC 2796
- RFC 1997: BGP Communities Attribute
- RFC 1998: An Application of the BGP Community Attribute in Multi-home Routing
- RFC 2042: Registering New BGP Attribute Types
- RFC 2796: BGP Route Reflection - An Alternative to Full Mesh IBGP, Updates RFC 1966
- RFC 3065: Autonomous System Confederations for BGP, Obsoletes RFC 1965

- http://www.ieng.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm
- http://cio.cisco.com/univercd/data/doc/cintrnet/ito/55143.htm
- http://www.freesoft.org/CIE/Topics/88.htm

2.1.3. 可能存在的漏洞

BGP 本身不保證它是一個非常安全的通信協定，從 Transport 和 Network 階層的角度來看 BGP 封包純粹只是一個資料的封包，而 BGP4+（Border Gateway Protocol version 4 plus）只是一個支援 IPv6 的 BGP，如此以來 BGP 並沒辦法保證它沒有安全方面的漏洞。

入侵者是一個存在有攻擊網路能力的人，他會修改，重播，製造或移除任何網路所傳輸的封包。在一個使用 BGP 的網路裡，有可能存在幾種入侵者如下：

* Subverted BGP speakers： 違反 BGP 通信協定或不適當地提出網路資源權的一台主機。
* Unauthorized BGP speakers： 非經授權執行 BGP 通信協定並跟經授權的 BGP 主機成功建立 BGP 連接的一台主機。
* Masquerading BGP speakers：偽造靜授權的 BGP 主機之身分的一台主機。
* Subverted links：一個違反 BGP 通信協定的主機所製造的連接。

BGP 存有三種基本漏洞如下：

1. 沒有一個能在 BGP 點對點的通訊中保護資料和資料來源之正直的機制。
2. 沒有一個能確認一個 AS 可發布 NLRI 資訊之權利的機制。
3. 沒有一個能確認 AS 所發布的 AS 路徑的機制。

BGP 提供四種 message types，如：OPEN，KEEP ALIVE，NOTIFICATION 及 UPDATE，各種有各種的漏洞與風險，下列詳細討論各種 message 的漏洞與危險。

1. BGP OPEN message

在一個 established 狀態中，若收到一個新 OPEN message，主機會把目前正在溝通的 BGP session 立即關掉，解放所有資源與移除所有相關的路徑。偽造這種訊息能停斷路由器的運作。

2. BGP KEEPALIVE message

在一個 openstate 狀態中， 收到一個新 KEEPALIVE message ， 造成連接失敗，偽造這種訊息能讓兩段無法建立連接 。

3. BGP NOTIFICATION message

收到 NOTIFICATION message 造成 BGP 連接被關掉而解放資源及移除相關的路徑，偽造這種訊息能停斷路由器的運作。

4. BGP UPDATE message

BGP Update message 攜帶路由的資訊。偽造這種 message 能中斷路由器的運作 .接下詳細討論 BGP UPDATE message 所攜帶的路由資訊的漏洞：

4.1. Unfeasible Routes Length

修改 length(封包長度) 欄位 ， 讓訊息無法正確被切割 ， 導致錯誤 。 路由器會送一份 NOTIFICATION 訊息給對方 ， 然後關掉目前的連接 。

4.2. Withdrawn Routes

偽造這個欄位能讓一個非 BGP 主機消除已經存在的合法路徑 。 重發出前封包的 withdrawal 訊息也會讓重建的路徑被消除掉。一個 BGP 主機使用 Withdrawn routes 欄位 ， 能發布錯誤的 withdraw feasible 路徑 ， 不過一個 BGP 主機本來就有權利發布路徑的資訊 ， 它可以 withdraw 之前所發布的路徑 ， 一個 BGP receiver 主機只能跟相關的 BGP sender 主機交換 withdraw 路徑的訊息 ， 所以 BGP-BGP 架構不會有這個漏洞 。

4.3. Total Path Attributes Length

一個多變序列長度的 Path Attribute 每次會出現在一個 BGP Update 訊息 ， Path Attribute 是由 Attribute type ， Attribute length 與 Attribute value 三個變數所組成的 。 因此 Path attributes 存有對這三個變數的漏洞 。 修改 Attribute Length 導致 UPDATE 訊息沒有正確的被切割 ， 而修改 Attribute value 或 Attribute Flags 也會引起兩個欄位之間的值彼此不合， 使 UPDATE 訊息沒有正確的被切割 。 一個切錯的 UPDATE 訊息導致 BGP 主機發布一個 NOTIFICATION 訊息 ， 關掉現有的連接 ， 要是一個真正的 BGP 主機才能夠隨時關掉連接 。 當封包來源是從一個非 BGP 主機 ， 這些漏洞帶來很大問題 ， 如果封包是從一個 BGP 主機發出來的這些漏洞不會有什麼影響的 。BGP 共有 7 個 Attribute value 如： Origin (type code 1) ， AS_Path (type code2) ， Next_HOP(type code 3) ， Multi_Exit_Disc(type code 4) ， Local_Pref(type code 5) ， Atomic_Aggregate(type code 6) 下列詳細討論各種 message 的漏洞與危

險：

4.3.1. ORIGIN

此欄位指出路由資訊是從 IGP 或 EGP 得知的 ， 比如路徑是被用在於 inter-AS multicast routing 的話 ， 於是此欄位會指出 INCOMPLETE 的值 。 Origin 欄位不是用來做 routing decision ， 所以不管是一個 BGP 或 非 BGP 連接 ， Origin 欄位不會帶來安全漏洞的問題 。

4.3.2. AS_PATH

一個 BGP 或 非 BGP 有可能發布對於相關 NLRI(Network Layer Reachability Information) 不準確的 AS_PATH, 導致 sub-optimal 路徑〈 sub-optimal 路徑是一個沒有符合預期策略的路徑或者一個不能幫封包做發送的路徑 〉。 因為 Sub-optimal 路徑沒有辦法做封包發送 ， 封包變得不能到達目的地 ， 如果很多封包無法到達目的地 ， 一些路由器及中轉網路會被指導錯誤的封包淹沒 。

RFC 說明 BGP 主機發布公告給它鄰居之前要預謀自己的 AS 當 AS_PATH . 即使 BGP 主機要預謀自己的 AS 當 AS_PATH ， 製造贋造 AS_PATH 的 BGP 主機不能收到跟 NRLI 相關的封包 ， 因此用這種方式可防止一台 BGP 主機偽造 AS_PATH 。

判斷 AS_PATH 是否一個 BGP 漏洞是要看 BGP 主機有沒有檢查 AS_PATH 正值的功能 〈查看第一個 AS 是否它的鄰居〉。 如果 BGP 主機可以把 AS_PATH 傳開給它的鄰居但是不用把自己的 AS 放在 AS_PATH 的第一欄的話 ， 那就沒辦法檢測到偽造得 AS_PATH 。

4.3.3. NEXT_HOP

NEXT_HOP 欄位限定 UPDATE 訊息裡面的 NEXT_HOP 的邊界路由器之 IP Address 。 如果接受器是一個外部鄰居 ， 那接受器與 NEXT_HOP 的位址必要是共同一個 subnet 。 顯然如果有一個非 BGP 主機更改這個欄位 ， 兩個 AS 的連接會被中斷 。.

4.3.4. MULTI_EXIT_DISC

MULTI_EXIT_DISC 欄位是被用在 AS 之間被傳送的 UPDATE 訊息 。 從一個 AS 之間收到的 MULTI_EXIT_DISC 可以傳播在一個 AS 裡面 ， 但不可以傳播給其他 ， 因此這欄位只被用在製造一個 AS 內部的 。 修改此欄位 ， 不管是 BGP 主機或 非 BGP 主機 ， 都會影響到路由裡面的 AS 變得 sub-optimal ， 但影響該在有限的範圍內。

4.3.5. LOCAL_PREF

LOCAL_PREF 欄位得包含於所有內部機器的訊息裡面及不包括外部機器的訊息．因此修改 LOCAL_PREF 會影響到在 AS 內部的路由過程．注意，在 BGP RFC 裡並沒有一個必要條件以 LOCAL_PREF 在一個 AS 內部的 BGP 主機之間一定要一致的．因為 BGP 主機是自由的挑選 LOCAL_PREF 隨著它想要的，所以修改此欄位反而是對一個非 BGP 主機的漏洞。

4.3.6. ATOMIC_AGGREGATE

ATOMIC_AGGREGATE 欄位指示一個 AS 已經收到一個更多或更少特殊路由到 NLRI 與設置合計的路由。此路由不能被減少因為比較具體的 Prefix 不一定會跟隨列在單子上的 AS 路徑，因此收到一個有 ATOMIC_AGGREGATE 的路由的 BGP 主機會被限制做更具體的 NLRI。移除 ATOMIC_AGGREGATE 就會移出掉限制規定，有可能造成預期更具體的 NLRI 封包被傳送錯。當沒有集成的時候，增加 ATOMIC_AGGREGATE 會有一點影響，深於限制減少集合 (un-aggregated) 的 NLRI 由讓它更具體，不管是一個 BGP 主機或非 BGP 主機此漏洞都會存在。

4.3.7. AGGREGATOR

此欄位有可能被一個 BGP 主機包括的，而那 BGP 主機已經算好由其他集合的路由之 UPDATE 訊息裡所描繪的路由。AGGREGATOR 欄位含有最後合計器之路由的 AS number 與 IP address，它沒有被用在製造 routing decision 的過程，所以此欄位不會有漏洞的。

4.4. Network Layer Reachability Information (NLRI)

修改或偽造此欄偽，不管來源是從一個非 BGP 主機或 BGP 主機會帶來網路路由之總斷，淹沒路由的路由器，資料遺失〈已公佈的路由無法傳送資料給已公佈的網路〉，資料被傳送到一個 sub-optimal 路由，等等。

2.2. EGP

2.2.1. 通信協定詳述

Routing protocol 大致可分為兩大類 ， Interior Gateway Protocols (IGPs) ， 以及 exterior gateway protocols (EGPs) 。 其中 IGPs 有 RIP ， HELLO 和 Interior Gateway Routing Protocol (IGRP)等 ， EGPs 則有 EGP ， BGP 等 。 IGPs 通常是在 AS 內部使用，而 EGPs 是在 AS 之間的繞送演算法 。

IGRP 事由 CISCO 公司發展 ， 使用在較大型 ， 網路拓樸較複雜 ， 並且各網路區段的 bandwidth 和 delay characteristics 各不相同的網路中 。 RIP ， 通常使用在 Berkeley-derived UNIX 系統中 ， 許多小型 ， 網路拓樸不那麼複雜的網路都使用 RIP 。 HELLO 是一個很早期使用的網路繞送協定 ， 早期 National Science Foundation (NSF) backbone network 是使用 HELLO 。

EGP 算是最早期的 Exterior gateway protocol ， DDN (Defense Data Network) 和 NSFnet (National Science Foundation Network)都是使用 EGP ， BGP 則改良了 EGP 的一些問題 。

EGP 可以使相鄰的 gateways ， 互相傳遞訊息 ， 已便知道是否存在繞送路徑 ， 尤其使用在 autonomous systems 之間 。 EGP 有下列機制： acquire neighbors (鄰居探詢) ， monitor neighbor reachability (監督鄰居狀態) ， exchange net-reachability information (交換相鄰 gateway 的 routing 資訊) EGP 週期性的發出 Hello/I-Heard-You (I-H-U)訊息 ， 藉此來跟鄰機交換資訊及要求回應 。

EGP 運作時的三大 Procedure：
EGP 在運作時有主要的三大 Procedure：neighbor acquisition ， neighbor reachability ， network reachability 。

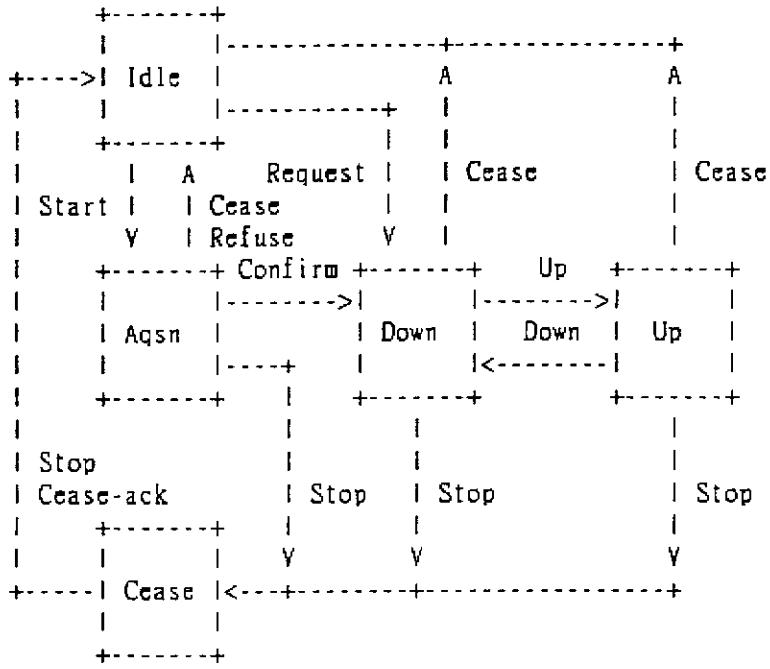
1. *neighbor acquisition：*
主要用來確認 Gateway 之間是否同意要使用 EGP 來作為傳遞訊息之用。

2. *neighbor reachability：*
確認鄰近的 Gateway 是否正常運作或者已經停擺了。

3. network reachability：

確認在鄰近Gateway之下的網路是否正常運作 ， 在進行這個Procedure之前要先確認 neighbor reachability 是成功的 ， 同時這個Procedure所需的時間會比neighbor reachability花上更多的時間 。

EGP 運作時的Finite State Daigram：



Idle State (0)

在這個State中 ， Gateway沒有被指定給其他的neighbor或protocol activity來做一些處理 。只有當它接收到一個Request訊息或是一個Start event時 ， 才會有反應（意即 ， 若接收到其他的訊息就忽略不理） ， 若收到Start event則會跳至Acquisition State ， 同時發出一個Request訊息 ； 若收到Request則會跳至Down State ， 同時發出一個確認的回應訊息 。

Acquisition State (1)

在這個State中 ， gateway會將從Idle State送來的Start訊息加以翻譯 ， 所得的結果有三種：

1. Refuse
2. Confirm

3. Stop event

當收到的Start 訊息為Refuse時 ， 將會跳回至Idle State。當收到的Start 訊息為Confirm時 ， 代表Gateway同意用EGP這個protocol來作為訊息傳遞之用 ， 如此將會如同在Idle State收到Request一樣跳回至Down State 。

當收到的Start 訊息為Stop event時 ， 將會跳回至Cease State 。

Down State (2)

在這個State中，不管是從Idle State接收到Request或是從Acquisition State 因為Confirm訊息跳至Down State，Gateway會開始處理neighbor-reachablility protocol(procedure)，當這個procedure開始時，會先將neighbor Gateways都假設為「down」(沒有運作)，然後一一發出訊息去確認他們是否有運作。

Up State (3)

在這個State中，Gateway會將neighbor Gateways都假定為「up」(正常運作)，同時開始處理各式各樣的process、routing等，除此之外，還會每隔一段時間就發出訊息，用來確認neighbor Gateways是否還在運作，如果發現neighbor Gateways沒有正常運作，則會回到Down State。

Cease State (4)

會來到Cease State是因為收到Stop event，在這個State中，Gateway會每隔一段時間就發出Cease command，並且當接收到Cease-ack response或另一個Stop event之後回到Idle State。這樣的設計是用來確保具有較高優先權的neighbor Gateways可以接收Cease command以回到Idle State並停止EGP運作。

2.2.2. 參考資料

- RFC 0827 : Exterior Gateway Protocol (EGP), Updated by RFC 0904
- RFC 0888 : "STUB" Exterior Gateway Protocol, Updated by RFC 0904
- RFC 0904 : Exterior Gateway Protocol formal specification, Updates RFC 0827, RFC 0888
- http://www.cisco.com/univercd/cc/td/doc/product/software/ssr83/rpc_r/53992.htm

2.2.3. 可能存在的漏洞

此通信協定有可能收到兩種攻擊如:第三者DoS 攻擊與Man in the middle 攻擊。為了防止收到這兩種攻擊 ， 以下提供一些防護機制：

1. *Unsolicited Updates*
如果一個網路被分享給鄰居，EGP implementation 應該要發送一個unsolicited update 訊息當封包來源是那個共用網路。

2. *Abort timer*
EGP implementation 應該要支援 abort timer ， 遇到 Idle 狀態可以自動發 Start 事件重開通信協定的機器。當 Stop 事件被啟動，Abort timer 不應該被啟動。

3. *Idle 狀態中收到 Cease 指令*
當 EGP 機器進入 Idle 狀態而收到 Cease 指令 ， 那台機器應該要反應一個 Cease-ack。

4. *Hello Polling 模式*
EGP implementation 應該都要支援 active 和 passive polling 模式 。

5. *Neighbor Acquisition 訊息*
以上述 Hello 與 Poll 的間隔應該只能夠出現在Request 和 Confirm 訊息， 應此對於Request 或 Confirm 訊息，EGP neighbor Acquistion 訊息的長度是 14 bytes ， 對於 Refuse ， Cease 或 Cease-ack 訊息 ， 它是10 bytes。Implementations 不應該對於 Refuse ， Cease 或 Cease-ack 訊息送此訊息 14 bytes 的長度 。

6. *Sequence Numbers*
收到的Response 或 Indication 封包隨著 sequence number 不等於 S，那些封包應該要被丟棄。正好 Poll 指令被送出去之後 sequence number S 必須被增加，其他時短不要增加 sequence number S。

7. *Indirect Neighbors*
EGP implementation 應該要支援 indirect neighbor。

8. *Polling Intervals*

Hello 指令和 Poll retransmission 的隔間應該要可以設定的但是必須限定它的 最少值。Impelmentation 給 Hello 和 Poll 指令反應的隔間應該也要可以設定的但是必須限定它的最少值。

9. *Network Reachability*

Implementation 必要預設不提供外部 routers list ， 只提供可以從內部路由器到達目的地的 router list ， 而這些路徑應該要包含於 Update Response / Indication 封包裡面 ， 不過 implementation 可以選定提供設定選項可有權利提供一些外部 routers list 。在此 Implementation 不該包含從外部獨自系統所學來的外部 ， 也不該把相關路徑的封包回送給從那邊學到那路徑的外部獨自系統 。

2.3. EIGRP

2.3.1. 通信協定詳述

Enhanced Interior Gateway Routing Protocol〈EIGRP〉 有四個基本的元件：

a．鄰近的發現/復原〈Neighbor Discovery/Recovery〉
b．可靠傳輸協定〈Reliable Transport Protocol〉
c．DUAL 有限狀態機器〈DUAL Finite State Machine〉
d．獨立協定的模組〈Protocol Dependent Modules〉

鄰近的發現/復原〈Neighbor Discovery/Recovery〉是路由器使用來動態得知在相連網路上其他的路由器的過程 。 當身旁的路由器變的不可到達或是無效的 ， 路由器必須要發覺到 。 這一個過程可以藉由定期送出一個小的打招呼封包而達到 。 當這個打招呼封包被接受 ， 路由器就可以確定鄰近的是否存在著而且正常運作著 。 一但上述被確定 ， 鄰近的路由器就可以互換路由的資訊 。

可靠傳輸協定〈Reliable Transport Protocol〉是為了擔保 ， 有順序地傳達 EIGRP 封包給所有鄰近的路由器而負責 。 他可以混合支援 multicast 或是 unicast 封包的傳送 。 有些 EIGRP 必須可靠的傳輸 ， 而有些不必 。 由於效率因素 ，所以可靠也只有在需要時才被提供 。 例如：在一個多重存取擁有 multicast 相容的網路中 ， 像是乙太網路 ， 不必要個別傳送 Hollo 的封包給所有鄰近的路由器 。 因此 EIGRP 傳送單一個 multicast Hollo 封包 ， 封包中含有指示通知接收者不必回應此封包，而其他型態的封包 ， 像是更新〈Updates〉要求回應 ， 這也是被包含於封包中 。 可靠傳輸有一個規定就是快速傳送 multicast 封包 ， 當有未回應封包等候處理時 。 這可以幫助 ，在多變速率的連線下 ， 確認聚合的時間仍然必較慢 。

DUAL 有限狀態機器〈DUAL Finite State Machine〉使得決定所有路由計算的過程成為一體 。 追蹤所有被鄰近路由器通知的路由器。距離的資訊 ， 為大家所知的 metric ， 被 DUAL 使用來選擇有效率的自由迴路途徑 。DUAL 選擇路由後 ， 被嵌入路由表列中 ， 這個表列是以適當的繼承者為基礎 。 繼承者是一個鄰近的路由器 ， 這個路由器被使用作封包的轉交 ， 至少有一個路徑可以到達目的地 。 當沒有適當的繼承者時而且有鄰近的路由器可以到達目的地 ， 因此就會發生重新計算 。 這也就是一個新的繼承者將會被確定/產生， 總共花費計算路由的時間會影響聚合時間 。 即使重新計算

並不是密集的處理 ， 但試者避免重新計算當沒有需要的時候 。 當一個地誌發生改變時 ， DUAL 對所有繼承者作測試.如果有適當的繼承者 ， 他將依序使用他發現的任一個 ， 一避免不需要的重新計算 。

獨立協定的模組〈Protocol Dependent Modules〉是為了 network layer protocol-specific requirements 而負責 。 例如：IP-EIGRP 模組就是負責傳送接收 EIGRP 封包 ， 但 EIGRP 封包被包裝在 IP 中 。 IP-EIGRP 負責剖析 EIGRP 和告知 DUAL 新被接收的資料 。 IP-EIGRP 要求 DUAL 作路由的決定和哪一個儲存於 IP 路由列表中 。 IP-EIGRP 負責藉由其他的 IP 路由協定重新分散路由 。

EIGRP 是 IGRP 的增強版本，同距離的向量技術用於 IGRP 也用於 EIGRP ，和基礎距離資訊仍然沒改變 。 聚合的特性和協定有效的操作已經很明顯的改善 。 對改良過的架構 ， 保留已存在在 IGRP 的研究 。

聚合的技術〈convergence technology〉以 SRI 國際組織主導的研究為基礎 。分散更新演算法〈Distributed Update Algorithm〈DUAL〉〉是一套被使用在每一個情況下遍佈於路由〈route〉的計算的一套演算法 。 為了在同一個時間的同步 ， 這也就允許所有的路由器忙於位置的改變 。 沒有受位置改變的路由器並不會忙於重新計算 。 用 DUAL 的方法的聚合時間會與任何其他存在路由的協定相競爭 。 EIGRP 已經被延伸到 network layer protocol independent ，因此允許 DUAL 支援其他的協定套裝 。

Enhanced IGRP New Feature ：

1. Fast Convergence
   因為每個 Router 會紀錄其鄰近 Router 的 Routing Table ， 藉此使 Routing Path 比較 Optimize。(使用 Diffusing Update Algorithm:DUAL)可以讓 Information 的聚集(converge)跟所有現行的 routing protocol 一樣快。
2. Variable Length Subnet Mask
   可以處理 Subnet 之中各個不同 mask 設定。
3. Partial Bounded Updates
   只有當 Route cost 有所改變的時候 ， 才去 Update Routing table 的內容。這個 Feature 能夠使 IGRP packet 的 bandwidth required 達到 Optmize。
4. 支援 multiple network-layer
   能夠支援好幾種 network 類型：例如 IP ， Apple Talk ， Novell IPX 等等。

5. Less CPU usage than IGRP

因為 Full update packets 在被接收的時候並不需要作任何的 process。

Enhanced IGRP New technology：

1. Neighbor discovery/recovery

會自動去找尋自己是否有新的 Neighbor ， 或者對 Neighbor 作 recovery 的動作。

2. Dynamically learn new neighbors

自動去學習加入新的 neighbor 之後的動作 ， 這是 protocol independent 的。

3. Reliable Transport Protocol (RTP)

4. Guaranteed ordered delivery of IGRP packets

使 IGRP packet 的傳送是 ordered 的。

5. Dual finite state machine

6. Protocol-dependent modules

獨立協定的模組 ， 比如說如果 IP 之中包含 IGRP 的 packets 則需要用此功能 。

2.3.2. 參考資料

- RFC 1371: Choosing a Common IGP for the IP Internet
- http://www.cisco.com/warp/public/103/5.html
- http://www.ieng.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

2.4. HSRP

2.4.1. 通信協定詳述

傳統專線的容錯一般都是透過額外的 ISDN。平時利用專線對外連接，當專線斷線時，則啟動 ISDN 來作連結。但是卻受限於 ISDN 的撥接線路品質，而且此種方式無法同時利用專線和 ISDN 對外連接。所以 Cisco 發展出 HSRP(Hot Standby Router Protocol)，讓專線也可以作為專線的備援，同時又可以利用這兩條專線同時對外連接。在 Cisco Router IOS 10.0 以上開始支援 HSRP。透過一組 Router 的協同作業，讓這一組 Router 共用一個 IP Address 的方式，讓區域網路中的用戶，可以在備援 Router 啟動時也不須重新設定 gateway。HSRP Router 每 3 秒鐘發出一個 hello 訊息，來偵測線路是否正常；也因此可以在最短的時間內，讓區域網路對外的連接重新建立。

透過 MHSRP(Multi-HSRP)，可以讓 HSRP Router 做到線路的共享。讓 Standby 的線路也可以成為 Active 線路，使兩條專線同時讓區域網路的用戶連接上 Internet，增加區域網路對外連接的速度。

HSRP 不只可以做 IP 網路的備援，Novell 的 IPX 和 Apple 的 Apple Talk 都可以做到備援。依照 HSRP 設定出的一群 routers，有著不同的先後優先次序。一般來說預設為 100，數值越大 priority 就越大。因此設定一個 default active router 就是把 priority 值設的比其他 router 的還大。

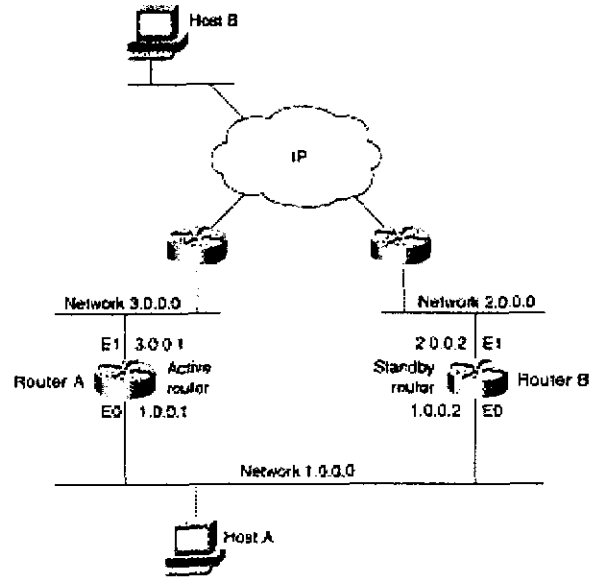
一群 HSRP 的 routers 藉由交換彼此優先次序來輪番工作。也就是說只要 Active router 在一段時間內沒送出 Hello 訊息，Standby router 就會接替 Active router 的工作，並且把封包轉送的工作告知給在網路上所有主機。設定為 HSRP 的 routers 彼此交換三種不同的訊息：

1. Hello 傳送 "hello" 的訊息(包括 HSRP priority 及 state information)到其他 HSRP routers 手中。一般來說，每三秒鐘 HSRP router 送出一個 Hello 的訊息。
2. Coup 當 Standby Router 負擔起 Active Router 的工作，他會送出一個 coup 的訊息。
3. Resign 當 Active Router 正打算要關機或有其他 router 透過 hello 說他有著比 Active Rounter 更高的 priority 時，便送出這樣的訊息。

在任何時間，設定為 HSRP 的 routers 有著以下不同的狀態：

1. Active　　此 router 正執行封包轉送的工作。
2. Standby　　假如 Active router 掛了，此 router 將負擔起封包轉送的工作。
3. Speaking and listening　此 router 正在接收並且接受 hello 訊息。
4. Listening　　此 router 正接收 hello 訊息。

下圖表示 IP 網路拓撲裡兩個設定為 HSRP 的 Router。



所有在網路上的主機設定(1.0.0.3)這個虛擬路由的 IP 為預設之路由。以下為 Router A 的設定：

```
hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 preempt
standby 1 priority 110
standby 1 authentication denmark
standby 1 timers 5 15
!
interface ethernet 1
ip address 3.0.0.1 255.0.0.0
!
router eigrp 1
```

```
network 1.0.0.0
network 3.0.0.0
```

以下為 Router B 的設定:

```
hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 preempt
standby 1 authentication denmark
standby 1 timers 5 15
!
interface ethernet 1
ip address 2.0.0.2 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
```

Standby IP 界面設定的指令提供 HSRP 並且建立虛擬路由器的 IP 位址為 1.0.0.3 。 A Router 及 B Router 都包含這個指令， 如此一來兩個 Router 共享同個虛擬 IP。

假如不指定一個 group number， 那麼預設的 group 會是 0 ; 假如 group 1 為一 Hot Standby group 。 在這 group 必須至少有一個 router 設定 IP 為虛擬路由器的 IP 位址；對其他 Router 來說 ， 這是可自由選擇的 。當它的 priority 比其它設定為 HSRP 的 Router 還高時 ， Standby Router 優先取得設定 interface 指令並允許成為 Active Router 。

Router 們的設定也包含這樣一個指令 ， 如此一來每一個 router 都可成為其它 router 的 Standby Router 。 因此如果不透過 standby preempt command 去設定 ，它就不能成為 Active Router 。

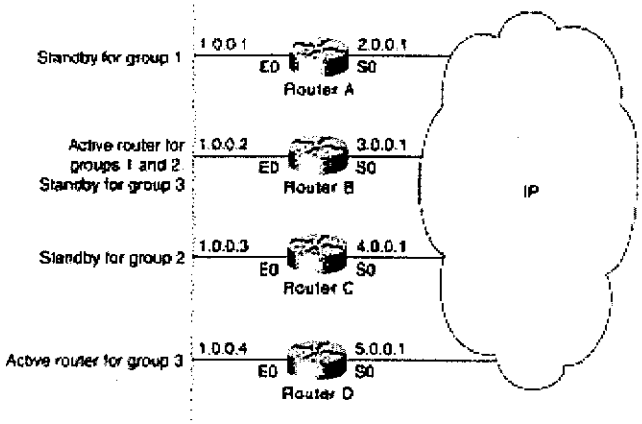
Standby authentication interface configuration 指令建立一未加密的 8 character 認證字串 ， 結合在每一個 multicast HSRP 訊息上 。 這樣的指

令是可自由選擇的。假如使用它，在這group每個設定為HSRP的routeru，也必須使用同樣個字串，如此一來在這group的router就能確認HSRP訊息的來源了。

Standby timers interface configuration指令設定 hello 訊息的間格（稱為hello time）為 5 sec並且設router等待成為 Active Router 的時間(稱為hold time)為 8 sec。

假如你想修改預設值的話，你必須設定每個router的 hello time 及 hold time。注意的是在任何Ethernet或FDDI LAN。可有 255 Hot Standby group；在Token Ring LAN，則不能超過3個。

Multigroup HSRP (MHSRP) 允許單一router介面屬於超過一個 Hot Standby group。MHSRP需要Cisco IOS Software Release 10.3 或更新的版本（支援結合Ethernet interface及multiple unicast MAC addresses的特殊硬體）。這些都是AGS及AGS+ routers並且任何屬於Cisco 7000 series，如此一來允許你設定AGS，AGS+，or Cisco 7000 series router介面成為更多Hot Standby group的備用router，如圖示，以下為hot standby groups的例子：



在圖中，Router A 的Ethernet interface 0屬於group1；Router B 的Ethernet interface 0屬於group 1，2，3；Router C的Ethernet interface 0屬於group2；Router D的Ethernet interface 0屬於group3。

當你建立group時，這這個例子中，group 1也許支援工程部門，group 2也許支援製造部門，group 3也許支援金融部門。Router B被設為

groups 1 ， 2 的 Active Router ， Router D 為 group 3 。 萬一 Router D 掛了 ， Router B 將負起封包轉送的工作並起維護在金融部門的使用者存取其它 subnets 的能力 。 以下為 Router B 的設定：

```
hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.5
standby authentication sclara
!
interface serial 0
ip address 2.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
```

以下為 Router B 的設定(必須是 AGS ， AGS+ ， Cisco 7000 series router):

```
hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0 0.0
standby 1 ip 1.0.0.5
standby 1 priority 110
standby 1 preempt
standby 1 authentication sclara
standby 2 ip 1.0.0.6
standby 2 priority 110
standby 2 preempt
standby 2 authentication mtview
standby 3 ip 1.0.0.7
standby 3 preempt
standby 3 authentication svale
!
interface serial 0
ip address 3.0.0.1 255.0.0.0
```

```
!
router eigrp 1
network 1.0.0.0
network 3.0.0.0
```

以下為 Router C 的設定：

```
hostname RouterC
!
interface ethernet 0
ip address 1.0.0.3 255.0 0.0
standby 2 ip 1.0.0.6
standby 2 authentication mtview
!
interface serial 0
ip address 4.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 4.0.0.0
```

以下為 Router D 的設定:

```
hostname RouterD
!
interface ethernet 0
ip address 1.0.0.4 255.0 0.0
standby 3 ip 1.0.0.7
standby 1 priority 110
standby 1 preempt
standby 3 authentication svale
!
interface serial 0
ip address 4.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 5.0.0.0
```

The format of the data portion of the UDP datagram is：

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	Op Code	State	Hellotime
Holdtime	Priority	Group	Reserved
Authentication Data			
Authentication Data			
Virtual IP Address			

Op Code：

描述 type of this packet

0 - Hello：表示 router 正在 running 而且可以當作 active or standby router

1 - Coup：表示一個 router 想要變成 active router

2 - Resign：表示 router 不想再當作 active router

State：

State 顯示目前的傳送 message 的狀態

0 - Initial

1 - Learn

2 - Listen

4 - Speak

8 - Standby

16 - Active

Hellotime：

包含著 hello message 間大約所需的時間 ， given in seconds。

Holdtime：

代表目前 hello message 有效的時間 ， given in seconds。

Priority：

用以選擇要當 active 或 standby 的 router，一樣就比 IP address。

Group：
This field identifies the standby group。

Authentication Data:
8 character reused password。Default value is
0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00

Virtual IP Address：
The virtual IP address used by this group。

2.4.2. 參考資料

- RFC 2281: Cisco Hot Standby Router Protocol
- http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2022.htm

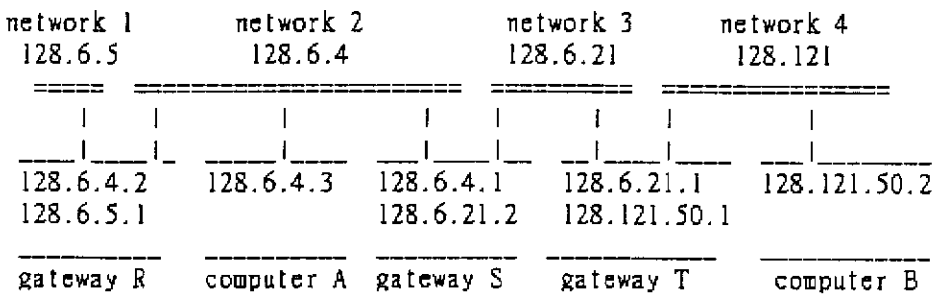
2.4.3. 可能存在的漏洞

HSRP 沒提供安全機制 ， 它的 Authentication 欄位只能對錯誤設定做防護 。 此通信協定有可能被內部 LAN 的入侵者破壞 ， 從而造成 DoS 攻擊或封包的漏洞 。 但是外部 LAN 的入侵者很難要破壞它 ， 原因是路由器通常不會對目的地是 multicast （224.0.0.2） 的封包幫忙做封包傳送。

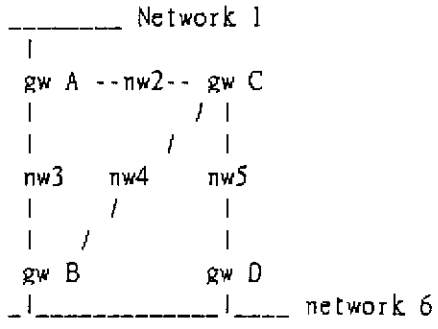
2.5. IGRP

2.5.1. 通信協定詳述

假設有以下這一個網路架構：



在網路 Intital 的時候，Gateway S 知道自己連接了 Network 2 和 Network 3，其資訊 Gateway S 並不知道，但是他會經由 Gateway R 和 Gateway T 所傳來的資訊來 Update 自己的 Routing table。會從 Gateway R 學到如何把 packet route 到 Network 1 去，也會從 Gateway T 學習到如何連接到 Network 4 去，和 Gateway S 一樣，Gateway R 會學到如果要把東西送到 Network 2，3，4，必須要把 packet 丟給 Gateway S 來作；Gateway T 則是學會經由 Gateway S 把 packet 送到 Network 1 的 Routing Path。



則在 A 的 Routing Table 之中，有三條 Path 能夠由 Network 1 到 Network 6：

1. 直接連到 Gw B
2. 經過 Gw C 連到 Gw B
3. 經由 Gw C 連到 Gw D

Composite Metirc 的計算

$$[(K1 / Be) * (K2 * Dc)] r$$

r ：fractional reliability
Dc：Composite Delay
Be：Effective Bandwidth，Unloaded bandwidth * (1 - channel occupancy)
K1, K2：Constant

Composite Delay Dc 的計算

$$Dc = Ds + Dcir + Dt$$

Ds ：switching Delay
Dcir ：Circuit Delay(Propagation Delay with 1 bit)
Dt ：Transmission delay(no-load Delay for a 1500 bit message)

Routing Table 例子：

	interface	next gateway	metric
network 1	nw 1	none	directly connected
network 2	NW 2	none	directly connected
network 3	NW 3	none	directly connected
network 4	NW 2	C	1270
	NW 3	B	1180
network 5	NW 2	C	1270
	NW 3	B	2130
network 6	NW 2	C	2040
	NW 3	B	1180

IGRP 是 Cisco 內部所使用的 Routing Protocol ， 主要的功能 ， 要讓需多

台 Gateway 共同達到 Routing 的功能，主要想要達到的目標如下：

1. 不管是在多大，多複雜的網域裡面工作，都能夠順利的達成 Routing 的工作，而不會產生 Routing Loop 的情形。
2. 在 Routing 資訊，也就是 Network Topology 交換的速度上面，擁有很快的 Respones Time。
3. 很低的 Overhead，也就是說，IGRP 在做 Router 之間的必要資訊傳遞所需要的 Bandwidth 相當少。
4. 會把封包用幾條平行的 Routing Path 來送，而每一條 Path 都各有優點。
5. 會自動計算以及處理每一 Path 的 Error rate 以及 Traffic。
6. 對單一個 set 之中的 Information，IGRP 可以依據服務的不同設定很多種不同的標頭 headle。

而現在已經 Implement 的 IGRP handle Routing for TCP/IP 已經可以 handle 各種不同的 Protocol 了。

IGRP 有點類似一些比較舊的 Protocol ， 像是 Xerox's Routing Information Protocol ， Berkeley's RIP ， 或者是 Dave Mills' Hello 和這一些比較舊的 Protocol 不同的是 ， IGRP 都是使用在大而複雜的網路上面 。

IGRP 使用了 Distance Vector Protocol ， 而每一台 Router 會和自己鄰近的 Router 交換資訊，而所交換的路由資訊包括了整個網路的效能資訊，而 IGRP 會協調所有的 Router 一起來 Optimize 整個網路上面的 Route 速度，而每個 Router 或者是 gateway 只需要解決自己那一部份的網路問題就可以了，當然，他們收到的路由資訊也只是關於他們自己所包含的那一部份網路的資訊，藉著收到這些資訊來 Optimize Network 。

IGRP Routing 作法

IGRP 用於 gateway，主要功用是用來連接幾個不同的網路 。 其 Routing 的基本方法並不困難 ， 假設網路是 packet-based 的 Network technology ， 那麼 Gateway 在接到一個 packet 的時候，會去看看這個 packet 的目的地到底是在那裡，如果是自己能夠直接連過去的位置，那麼就會把這個 packet 直接 forward 到目的地去 ， 反之 ， 如果不是 Router 自己能直接連接過去的目的地 ， 那麼他就會把這個 packet forward 到其他比自己更接近 packet 目的地的 Router，讓這些 Router 繼續傳下去。

而 Router 所用到的這種 Routing 方法，必須要配合 Routing Table 使用，

Routing Table 的形式如下所示：

network	gateway	interface
128.6.4	none	ethernet 0
128.6.5	none	ethernet 1
128.6.21	128.6.4.1	ethernet 0
128.121	128.6.5.4	ethernet 1
10	128.6.5.4	ethernet 1

在 IGRP 的 Protocol 之中，因為是動態的 Routing，所以 Router 必須動態的更新自己的 Routing Table 才可以 。 而 IGRP maintion Routing Table 的方式，是透過 Gateway 之間的資訊交換而達成的，每個 Gateway 會從自己鄰近的 Gateway 取得所需要的 Routing 資訊 ， 而由全部的 Routing Information 之中選擇有最好 Performance 的一個，來當作以後 Routing 的依據，而每一條 path 所必須紀錄的資料，包括了下一站是那一個 Gateway，所需要使用的 Network Interface，以及計算出來，要 Route 到目的地所需要的『長度』結果(metric information)，而每台 Gateway 會把自己收到所有 path 中的 metric information 拿來作比對，而最後選擇一條出來使用。但是通常 IGRP 為了要分散網路上面的 Traffic，會讓 Router 紀錄不只一條的 path，送 packet 時，就分成好幾條 path 送出去，而達到降低 Network Load 的目的，但是有一個前提，就是這幾條 Path 都差不多一樣好才可以。這種方法將可以讓全部的 packet 都能在比較好，Load 比較的網路上傳送，而擁有比較好的效能 。

IGRP Path 所使用的 Metric Information 如下：

1) 這條 Path 在網路上面的延遲時間(The Topological delay Time) ， 計算方法：

Delay = Delay from packet + Interface Topological Delay

2) 這條 Path 之中 Bandwidth 最低一段所擁有的 Bandwidth (The bandwidth of the nerrowest bandwidth segment of the path) ， 計算方法：

Bandwidth = Max(bandwidth from packet , interface bandwidth)

3) Path 自己站有的 Channel 數目(The channel occupancy of the path)，計算方法：

Channel Occupancy = Max(Channel Occupancy from packet , Interface Channel Occupancy)

4) 這一條 Path 的可靠度，可信任度 (The reliability of the path)，計算方法：

Reliability = min(Reliability from packet , Interface Reliability)

以下兩個項目並不在 Composite metric 的計算公式之中，但是也存在於 Routing Table 之中，作為 Path 的一個項目：

1) 跳站數目(hop count)： Packet 到 Destination 的經過 Router 數目。

2) MTU:如果不算 Fragmentation ， 而可以經此 path 傳送的最大封包大小。計算方法：

MTU = min(MTU from packet, interface MTU)

第一個項目是 Delay Time ， 這是假設網路在沒有 Load 的情況之下 ， 從 Gateway 自己到 Destination 所要經過的時間 。當然 ， 如果在網路上面有 Load 的情況下 ， Delay Time 一定會有所增加，但是這會在第三項的 Channel occupancy 來討論; 第二項是 Nerrowest Bandwidth，儲存的是在整條 path 之中，最慢一段的 bits per second; 第三項儲存現在這一條 path 正在使用的 Bandwidth; 第四項則是儲存這條 path 傳送時所可能產生的 Error rate。而以上四個項目，最後會合起來一起計算出一個單一的值 (Composite metric value)，而 Gateway 就靠這個 Composite metric 來決定這個 path 到底要不要使用。而計算 Composite metric 的公式如下：

[(K1 / Be) + (K2 * Dc)] r

K1，K2 ：常數
Be ：Path Bandwidth * (1 - Channel Occupancy)
Dc ：Topological Delay Time

r　　：Reliability

而計算出來的 Composite metric 如果最低的話，那麼就會是最好的 Path，當然，如上面所說，Router 也可能會使用好幾個路徑來送 Data。K1 和 K2 這兩個常數的數目，和傳輸封包的目的有關，不同 Service 的封包對於 Delay 和 Bandwidth 的要求各不相同，如果像是 Interactive Traffic 的封包，只要有一點點的 Delay 就會被看出來，所以對於 Delay 會比較重　視，而如果是 File Transfer 這種 Service，那麼對頻寬的重視程度一定　相對較高。

2.5.2. 參考資料

- RFC 1371 : Choosing a Common IGP for the IP Internet
- http://www.cisco.com/warp/public/103/5.html
- http://www.ieng.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

2.6. GRE

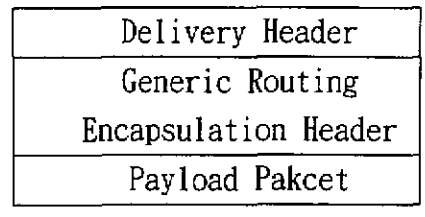
2.6.1. 通信協定詳述

RFC 裡已經有很多文件(例如 RFC1234, RFC1226, RFC1241, RFC1479..) 在介紹如何把一個 protocol 封裝在另一個 protocol 裡作 transporting IP 的工作，而 RFC2784 - GRE(Generic Routing Encapsulation)，就是定義一個普遍的封裝 protocol，提供一個較概括，簡單，普通的機制，把目前封裝問題的 size 從 O(n^2)降到更易於處理的 size。

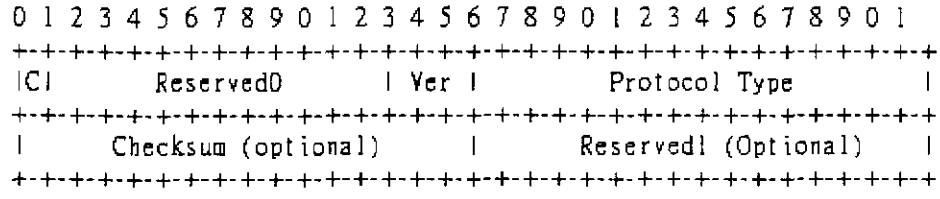
在有關 tunnel 的問題裡，我們通常稱一個欲被 tunnel 的封包叫 payload packet，而經由 GRE encapsulation 之後，發送的協定叫 delivery protocol。RFC2783 為 GRE 版本 0，PPTP(RFC2637)為 GRE 版本 1。

運作流程圖：

payload packet → add GRE header → add delivery header → forward → remove delivery header → remove GRE header → payload packet go on forward



圖一:GRE encapsulated pakcet



圖二: GRE Header 的 form(RFC2783)

Checksum Present (bit 0)
設成 1 的時候，表 Checksum 和 Reservel 欄位有使用並包念有效的資訊，注意相容的實作“必須”實作這部份。

Reserve 0 (bits 1-12)
當一個封包 bits 1-5 任一不為 0 時，接收者“必須”丟棄這個封包，除非接收者實作 RFC1701。Bits 6-12 被保留在未來使用，這些 bits“必須”被發送者設為 0 且被接收者忽略。

Version Number (bits 13-15)
此欄位必須設值為 0。

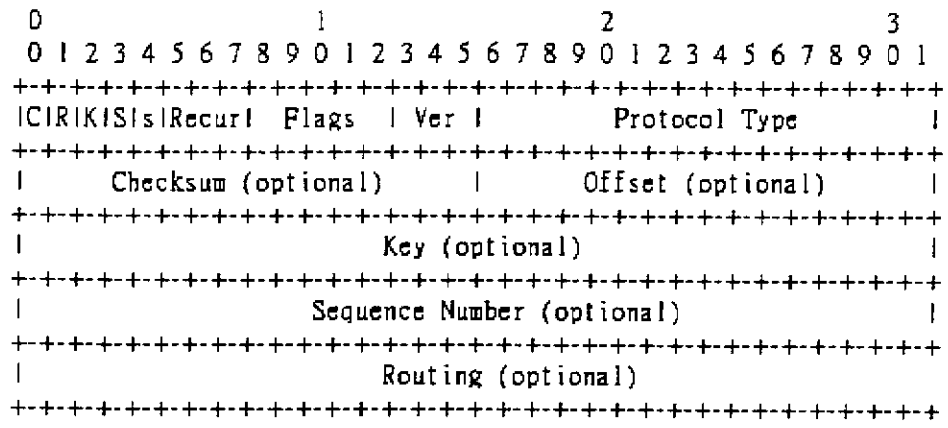
Protocol Type (2 octets)
此欄位包含 payload packet 的協定種類資訊。協定種類在 RFC1700 定義為 ETHER TYPE 和在[ETYPES]。實作時如接收到一個封包，協定種類不在 RFC1700 的 listing 或[ETYPES]必須被丟棄。

Checksum (2 octets)
包含所有在 GRE 表頭和 payload 封包 16 bit words 的 ip (1 補數) checksum 總合。在 checksum present bit 設成 1 時才用。

Reservel (2 octets)
包留作未來使用。在 checksum present bit 設成 1 時才用。

IPv4 (as a Payload)
當 IPv4 封包作為 GRE payload 時，協定種類必須設為 0x800。

RFC2784 GRE 主要是從 RFC1702 和 RFC1701 而來，當 GRE packets 在 IPv4 上封裝時，RFC1700 會被使用到。而 RFC1701 的實作在 RFC2748 則有些相容性問題的探討，如 Routing Present、Key Present、Sequence Number Present、Strict Source Route bits 已經過時了。



圖三: GRE Header 的 form(RFC1701)

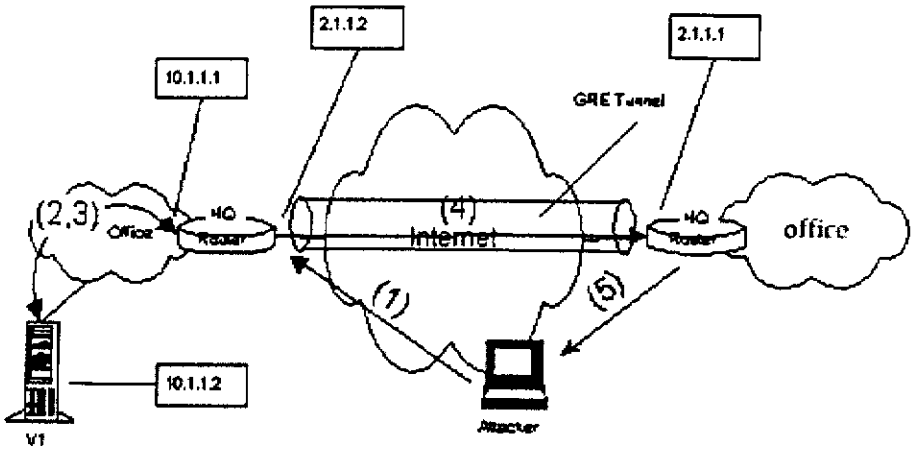
2.6.2. 參考資料

- RFC 1701: Generic Routing Encapsulation (GRE)
- RFC 1702: Generic Routing Encapsulation over IPv4 networks
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE

2.6.3. 可能存在的漏洞

GRE 網路的安全機制應該會跟普通 IPv4 網路的安全機制相似，因為使用 GRE 傳送封包的機制是類似使用 IPv4 傳送封包的現有機制。Route filtering 可以不用變，但是 packet filtering 需要 firewall 察看 GRE packet 的內容。

GRE Header 可以隨意地攜帶 Key 和 Sequence Number。 當 Sequence number 欄位有被使用，入侵者有可能把反覆無常的 sequence number 引入封包及進行 DoS 攻擊。為了防護這些攻擊，一定要用 IPsec 來防護 GRE header 和 tunneled payload. 我們應該使用 ESP 和 AH 的兩者之中來保護 GRE header，ESP 可以保護 IP payload 內的 GRE header 而 AH 可以保護整個封包除了鑑定易變的欄位。 攻擊案例如下：



1. 首先我們送一個 GRE 封包給受害者路由器（Tunnel 來源介面的 IP 地址）。封包裡面包含 IP header，Router 的來源地址（受害者 HQ 路由器所設定的目的地 Tunnel），因爲沒有限定 flag 所以 GRE header 填空白（32 Bits 的 0）。Payload 封包，含有受害者機器的 IP 地址和你的來源地址。在此要確定你沒有在一個 NAT 系統或防火牆後面。
2. 如果以上步驟一切順利而受害者的路由器有受到你所發給它的上述封包，受害者的路由器將檢查封包裡的來源地址並發現此封包是從 HQ 路由器來的。因爲一切滿足檢查的條件，受害者的路由器將把封包解開，之後根據 Payload 裡面的路由資訊再把封包送給受害者的機器或後端的路由器處理。
3. 受害者機器收到 Payload 封包之後，它將認爲那是一個正常的封包，並含有我們的 IP 地址爲送封包者的地址。假設那個封包是一個 ICMP echo request（ping），它將送 ICMP echo reply 出去給我們。
4. 受害者的路由器收到此封包之後，使用 GRE 把 Payload 送給它的 HQ 路由器。
5. 雖然 HQ 路由器有阻止外來的封包，但是 HQ 路由器可以跟網際網路溝通，它並可以建立連結。所以 HQ 路由器將 reply 的封包送給我們。
6. 我們的主機將收到從不同來源的完整封包，那就是受害者機器的回應。

2.7. NARP

2.7.1. 通信協定詳述

NARP 〈NBMA Address Resolution Protocol〉 使得 node 與 node 在 Non Broadcast Multi-Access link layer 〈NBMA〉 network 之間 ， 能夠進行通訊 。 原先 IP 架構上的 ARP 〈address resolution protocol〉 協定 ， 必須在同一個 segment 網路上〈同一個 subnetwork〉才可以運作 ， 對於 NBMA 網路就無法有效的解決 address resolution 問題，而 NARP 並不侷限在同一 subnet 底下 。

所謂的 NBMA 〈Non Broadcast Multi Access〉網路是指那些沒辦法做廣播〈Broadcast〉 的網路 ， 像 Frame Relay ， X.25 ATM 網路等皆是 NBMA 網路 ， Connectionless 的 NBMA 網路, ex: SMDS ， Connection-oriented 的 NBMA 網路, ex: ATM ， Non-Brodcast network, ex: X.25 〈不支援 broadcast 的網路〉 。

先判斷目的地位址是否在同一個 network ， 若是， 就用 ARP 即可 ， 如果不在同一 network ， 則送出 request 到 "NBMA ARP Server" 〈NAS〉. 一個 NAS 的運作類似 router ， 當收到 request 時 ， 先判斷自己是否 "server" 目的地的 address ， 如果有 ， 就 reply 資訊回去 ， 如果沒有 ， 就類似 router 的運作方法 ， 將封包繼續往下一個 NAS 送 ， 當沒有 next-hop 且沒有找到對應的 address ， 就傳回一個負的值 ， 若找到 ， 則送 address 回來 ， 途中所經的 NAS 皆可將其 address cache 下來 ， 以便下次還有 request 時可以直接使用 。

設定方法分成兩個部分:

終端機:

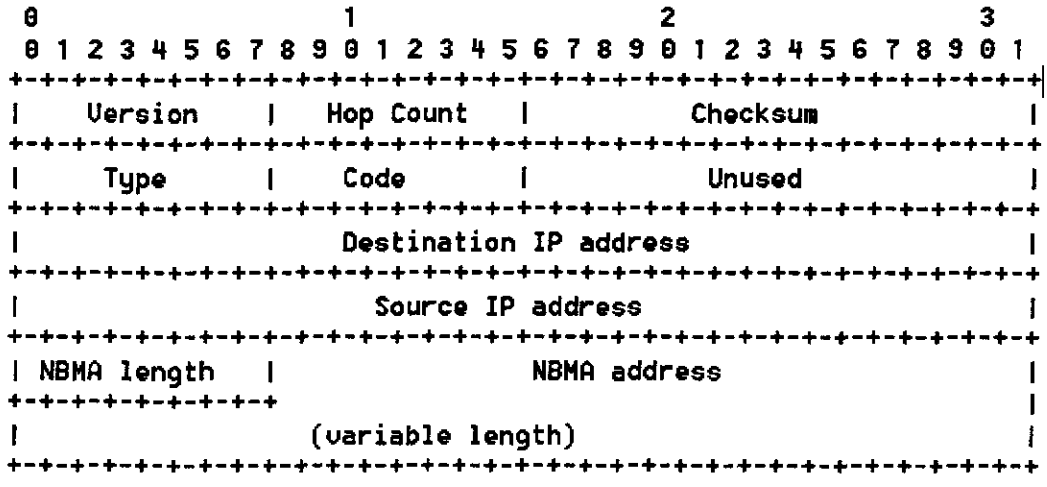
1. 設定一個或多個 NAS 的 IP
2. 必須能接收來自 NAS 的 reachability information

NAS:

1. 要包含正在 serving 的終端機 IP addresses
2. 必須能跟相連接的 NAS 交換 reachability information

3. 也可以跟鄰近的 router 交換 reachability information
4. 若一個終端機連接多個 NBMA network, 則 NAS 也要送 reachability information 到此台終端機

NARP 的封包格式



Request 的格式:

- Version: 目前只有到 version 1
- Hop Count: 封包可傳送的最多 hop 數
- Checksum: 用 IP 的 checksum 方法對整個 NARP 封包做運算
- Type: 1 是 request
- Code: 2 是 request for Authoritative Information, 1 用在 request 時
- Destination IP address: 目的地 IP address
- Source IP address: 自己的 IP address
- NBMA length: NBMA address 的 bit 數
- NBMA address: 用 0 補到接近 32 bits

Reply 的格式:

- Version: 目前只有到 version 1
- Hop Count: 封包可傳送的最多 hop 數
- Checksum: 用 IP 的 checksum 方法對整個 NARP 封包做運算

- Type: 2 是 reply
- Code: positive, Non-authoritative Reply 是 1,
  Positive Authoritative Reply 是 2,
  Negative, Non-authoritative Reply 是 3
  Negative, Authoritative reply 是 4
- NBMA length, address: 若是 negative reply 則不使用者兩個 field 其餘跟 Request 的格式一樣

NAS 若收到 authoritative 的 request 不會用 cached information 當作 reply 送回去, 只有在收到 non-authoritative request 時才會用 cached information 當 reply, 但若 NAS 的 load 過高, 也可以經由設定, 使 NAS 針對 authoritative request 產生 non-authoritative reply 回去, 這樣的設定可以用在 cache 常 update 的情況下

NARP 的運作跟 ATMARP 的運作很接近, 兩者的差異:
- NARP 有 hop-count 來避免 infinite loop
- NARP request 和 reply 多了 authoritative 和 non-authoritative 的資訊

2.7.2. 參考資料

- RFC 1735: NBMA Address Resolution Protocol (NARP)
- http://www.networksorcery.com/enp/protocol/narp.htm

2.8. NHRP

2.8.1. 通信協定詳述

NHRP 是 NBMA (Non Broadcast Multi Access) next Hop Resolution Protocol 的縮寫 ， NHRP 能夠被一個 source station (主機或 router) 用來連接 NBMA (Non Broadcast Multi Access) 的子網決定下一個 NBMA' s hop 的 internetworking 層位址和 NBMA 子網的位址向一個目的地位址 。 如果目的地連接在 NBMA 子網上 ， 則 NBMA 下一個 hop 是那台目的地本身。 否則， NBMA 下一個 hop 是最靠近到這一台目的地之 NBMA 子網的排出發送程式 。 NHRP 在 NBMA 子網上旨在於用於一個 multiprotocol internetworking 環境。

NHRP 是 IETF 所提出，以讓 NBMA 網路中屬於某一 LIS (Logical IP Subnet) 的 NHC (Next Hop Client) 可以得知屬於另一 LIS 的終端設備之 NBMA 網址的通訊規格。如此一來各不同 LIS 的終端設備之間就可以建立 Short-Cut Path 來相互通訊；而不需要透過 Router 傳遞資料。

2.8.2. 參考資料

- RFC 2332: NBMA Next Hop Resolution Protocol (NHRP)
- RFC 2333: NHRP Protocol Applicability Statement
- RFC 2335: Distributed NHRP Service Using SCSP
- RFC 2336: Classical IP to NHRP Transition
- RFC 2520: NHRP with Mobile NHCs
- RFC 2603: ILMI-Based Server Discovery for NHRP
- RFC 2677: Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)
- RFC 2735: NHRP Support for Virtual Private Networks
- http://www.ietf.cnri.reston.va.us/ids.by.wg/ion.html
- http://www.cs.ubc.ca/nest/dsg/tevia_files/techreport/node15.html

2.8.3. 可能存在的漏洞

有一些 MIB 管理物件擁有 read-write 或 read-create 的 MAX-ACCESS ，

而這些物件有可能在一些網路環境中易受攻擊 。 對於一個非安全的環境中放 SET 操作的支援能夠有對網路操作帶來不好的影響 。

應該利用認證機制來鑑別 source package 及對 NHRP payload 提供資料完整性 。 MIB 沒含有任何管理的物件構成或暴露例如對 NHRP 鑑別或者資料的完整性所需要的安全資訊 。

下面的項是有可能使安全受危害並且，沒增加到這個 MIB 。 被指示當「configurable」是那些需要值的 。 被指示當「read-only」 是那些提供資訊的 。 雖然 NHRP 通信協定 ，需要或者擁有這個資訊 ，如果在 MIB 裡暴露了這個資訊將在 NHRP 被使用的整個 NBMA 領域受危害 。 因此 ， MIB 省略了這些項 ：

1. (可設定的) enable/disable security。
2. (可設定的) SPI (security parameter index)。
3. (可設定的) 演算法 (預設 HMAC-MD5-128 hash 演算法)。
4. (可設定的) lifetime 值 (秒)。
5. (唯讀) key。
6. (唯讀) 擁有上述權限的使用者目錄。

如當整個系統的安全取決於恰當地選擇鑰匙和算法的正確的執行 ， 選擇強壯的鑰匙是滿重要的 ， 而這些防護是由 hop by hop 基礎上完成 。 收到的資料能夠僅僅被信任像一個人信任橫越的路徑中的所有實體那樣那麼許多 。 一系列信任是被建立在 NHRP 消息的路徑中的 NHRP 實體之間 。 如果損害 NHRP 實體中的安全 ， 則損害整個 NHRP 領域中的安全 。

資料完整性覆蓋這整個 NHRP 有效載荷 ， 保證訊息沒被修改並且也鑑別這個來源。如果沒使用鑑別擴展或者安全損害 ， 則 NHRP 實體對二者容易哄騙攻擊，活躍攻擊和被動的攻擊 。

目前沒有機制要把訊息譯成密碼 。 這認為將用一個網路標準的第 3 階層來加密或解密 。 則建議用網路之間標準鑰匙管理協定來議訂鄰居之間的鑰匙 。 使用清楚課文傳導鑰匙 ， 如果使用其他談判方法, 將完全損害安全 。

任何 NHS (Next Hop Server) 有可能受到 DOS (Denial of Service) 攻擊變得CPU 過載 。 惡棍主機能夠把要求和註冊的封包送到第一個 NHS' hop 。 如果沒使用鑑別選項 ， 這些註冊封包會沿著傳送路線被傳送並需要在每一個 NHS 作處理 。 如果使用鑑別選項 ， 則第一個 NHS 僅有可能受

到 DOS (Denial of Service) 攻擊 (將未經證實的封包繼續下落而非促進) 。 如果損害任何主機的安全 (用來與一個 NHS 通訊的鑰匙被認識) ， 一個惡棍主機能夠對其鑰匙損害的主機的第一個 NHS' hop 派遣 NHRP 封包 ， 那些封包如同在未經證實的封包情況下沿著規定傳送路線的路徑向前將 。 然而 ， 此攻擊需要那惡棍主機跟作為妥協主機擁有相同的第一個 NHS' hop 。

最後 ， 應該注意的是 DOS 攻擊 ， 將規定傳送路線的 routers 使處理 NHRP 封包的資源膨脹 ， 而在 NHRP 封包的 Destination 欄位含有相同的目的地也是另外容許的攻擊方法 。

2.9. OSPF

2.9.1. 通信協定詳述

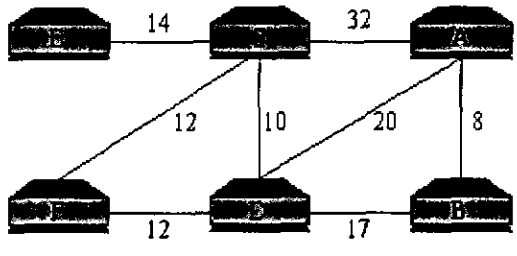
OSPF 是RIP 的最新替代品，用於內部閘道協定（IGPs），屬於連結狀態協定（link-state），階層式(hierarchical)的網路架構，是由 Internet Engineering Task Force(IETF)所發展且採用 Dijkstra' s Algorithm 和 Autonomous System 等方法使 routing 更加有效率，並加入認證的功能，有效防止修改 routing packet。

OSPF 彼此互相傳送資訊給對方，等收集了足夠的資訊，建立自己的 Network map(意指 Routing Table)，進而得知 packet 應往那走才到的了目的地。OSPF 協定是一種所謂的『連結動態協定』(link-state protocol)。Link 是指向外連結的介面，State 是指 Router 介面的特性及其相鄰 Router 間的關係一其中最重要的是，兩 Router 間的距離。相對於另一重要的 Routing Protocol RIP，OSPF 具有較大的彈性，它直接使用 IP 而不透過 UDP 或 TCP，也就是說，在 IP Header 中有一欄位可讓 OSPF 使用的值，可適用於較大型的網路，但相對的其運算也比較複雜。

OSPF 主要就是要得知與四周相鄰 Router 間的資訊，其中最重要的是 Router 與 Router 之間的距離，而兩 Router 間的距離我們通常使用 Metric 來表示，而 Metric 的定義如下所示：

$$\text{Metric} = 10^8 / \text{Bandwidth in bps}$$

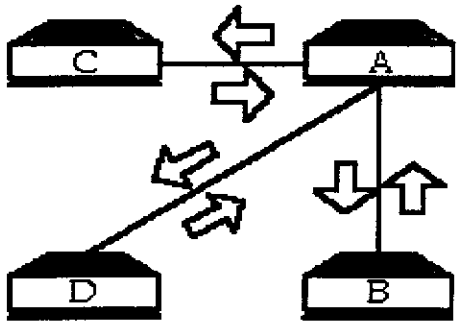
意指當兩 Router 間的頻寬愈大時，Metric 會愈小，也就是可以視為距離愈短的意思。例如：10M bps 的乙太網路其 Metric 為 $10^8/10^7 = 10$，而 T1 為 $10^8/(1.544 * 10^6) \sim 64$。(圖二)



圖一、OSPF 圖例

OSPF 主要的運作模式可分為四個步驟來說明：

一、每個 Router 會送一個招呼封包（hello packet ）給周邊的 Router，告知自己的存在，並接受其他相鄰 Router 傳來的招呼封包。(圖二)



圖二、Router 互相傳送 hello packet

二、每個 Router 收集到相鄰 Router 的資訊後，會將其 Link State 的資訊組合成 LSA 資訊散播給其他的 Router 。如圖一所示，A 收集到 B、C 和 D 的資訊後，組合成表一所示的 LSA 資訊。

表一、LSA Infomation

相鄰 Router	Metric
B	8
C	32
D	20

當每個 Router 收到 LSA 資訊時，會將它存作 Link State Database 且都必需再把此 LSA 資訊再傳送給其相鄰的 Router，逐一散播，此動作稱 Flooding。

三、當在此網路區域散播 LSA 的動作完成後，每個 Router 都具有其他 Router 的資訊，此時每個 Router 應都有 Link State Database，如表二所示：

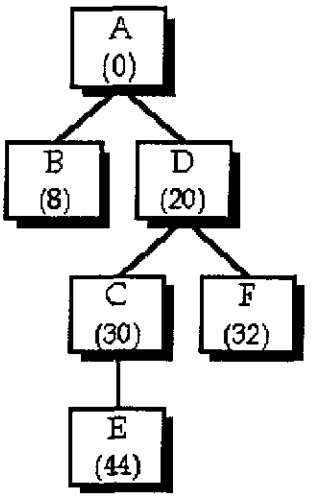
表二、Link State Database

A		B		C		D		E		F	
B	8	A	8	A	32	B	17	C	14	C	12
C	32	D	17	D	10	C	10	D	12		
D	20			E	14	F	12				

每一 Router 再利用此 Database 的資訊來算出最短路徑，而 OSPF 所使用的演算法是 Dijkstra's Algorithm(在參考文件中)。

四、經由 Dijkstra's Algorithm 可將所有的資訊建立成一棵 Shortest Path

Tree(圖三)，再利用此 Tree 建立自己的 Routing Table(如表三)，當 Router 收到 packet 時就可以依此 Routing Table 來決定要轉送到那一個 Router 上，而當其中如有 Router 發生錯誤時，因收不到對方的 hello packet，就會更新自己的 LSA 資訊，而其他 Router 也因收到 LSA 資訊而更新自己的 LSA Database，所以 OSPF 依然可以運作。

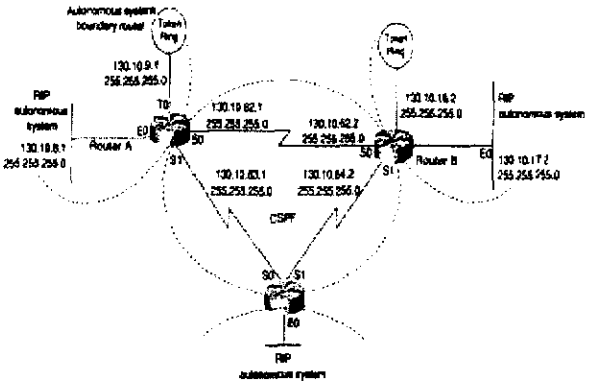


圖三、Shortest Path Tree for Router A

表三、Router A 的 Routing Table

Destination	Metric	Next Hop
B	8	B
C	30	D
D	20	D
E	44	D
F	32	D

在 OSPF 的協定中，它必須跟每一個 Router 作資訊交換，但當在大型的網路中，所要交換的資料量會讓整個 LSA Database 變的太大，計算 shortest path 上需花上許多時間，且 LSA 資訊交換會使 traffic load 變大，所以就有所謂的『階層式』(hierarchical) 的網路架構。根據區域性將之劃分成幾個區域 (Area) 在同一個區域內可以 OSPF 協定來交換 routing 訊息。這每一個區域都可稱之為自主系統 (Autonomous System, AS)(圖四)，每一個 AS 都可以有自己的 routing protocol，而兩不同 AS 間可以使用 OSPF 協定，這樣可以減少大量的 LSA 資訊和計算時間。如圖四所示，中間是採用 OSPF protocol 而其他 AS 則以 RIP 來作溝通。



圖四、RIP network with OSPF at the center

另外，一個 AS 跟另一個 AS 要作溝通時，通常會採用所謂『摘要』（summarization）的方式來交換，例如：Lan A 和 Lan B 中間由 R1 Router 連接，而 R1 Router 不需告訴負責 Lan A 的 Router 關於 Lan B 的 Routing information，而只需告知所有往 Lan B 的 packet 都往 R1 送即可，反之對 Lan B 亦 然。

2.9.2. 參考資料

- RFC 1131 : OSPF Specification, Obsoleted by RFC 1247
- RFC 1245：OSPF Protocol Analysis, Also RFC 1247, RFC 1246
- RFC 1246：Experience with the OSPF Protocol, Also RFC 1247, RFC 1245
- RFC 1247 : OSPF Version 2, Obsoletes RFC 1131, Obsoleted by RFC 1583, Also RFC 1246, RFC 1245
- RFC 1248 : OSPF Version 2 Management Information Base, Obsoleted by RFC 1252
- RFC 1252 : OSPF Version 2 Management Information Base, Obsoletes RFC 1248, Obsoleted by RFC 1253, Also RFC 1247, RFC 1245
- RFC 1253 : OSPF Version 2 Management Information Base, Obsoletes RFC 1252, Obsoleted by RFC 1850, Also RFC 1247, RFC 1245, RFC 1246
- RFC 1354 : IP Forwarding Table MIB, Obseleted by RFC 2096
- RFC 1583 : OSPF Version 2, Obseletes RFC 1247, Obseleted by RFC 2178
- RFC 1586 : Guideliness for Running OSPF Over Frame Relay Network
- RFC 1587：The OSP NSSA Option
- RFC 1765：OSPF Database Overflow
- RFC 1793：Extending OSPF to Support Demand Cirsuits
- RFC 1850：OSPFv2 的 MIB (Management Information Base)
- RFC 2096：IP Forwarding Table MIB, Obseletes RFC 1354

- RFC 2178 : OSPF Version 2, Obseletes RFC 1583, Obseleted by RFC 2328
- RFC 2328 : OSPF Version 2, Obseletes RFC 2178, Also STD 0054
- RFC 2329 : OSPF Standardization Report
- RFC 2370 : OSPF Opaque LSA Option, Also RFC 2328
- RFC 2740 : OSPF for IPv6
- STD 0054 : OSPF Version 2 , Also RFC 2328
- http://www.ietf.org/html.charters/ospf-charter.html
- http://cat.ice.ntnu.edu.tw/tcpip/main.htm
- http://carnap.ss.uci.edu/java/dijkstra/DijkstraText.html
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs001.htm

2.9.3. 可能存在的漏洞

OSPF 基本上它的架構已算非常完整，會發生問題通常會在 OS 及 Application 的 Implementation 上，如 routed、gated 及 zebra 等軟體。另外就是人為的疏失，若 Router 本身沒有使用 Authentication 的機制就會讓有心人士將 Routing packet 截取下來，並送出假的 Routing information。 解決方法是將所有的軟體進行 Patch，更新到最新版本，儘量減少人為疏失，使用現有分析工具來查看設定是否有錯。

2.10. RIP

2.10.1. 通信協定詳述

RIP 源於全錄(Xerox)公司的 XNS 網路系統，正式定義文件發表於 1981 年，並在 1982 年與 BSD Unix 及 TCP/IP 相結合。許多廠商也將 RIP 移植至他們的網路產品中，例如 Mac 的 AppleTalk 協定的 RTMP 即修改自 RIP，Novell、3Com 的產品則直接引用全錄公司(Xerox)標準的 RIP，Banyan、Ungermann-Bass 等廠商則是對 RIP 作小幅的修正以滿足各自產品的需求 。

RIP 是屬於一種選徑協定(Routing Protocol)，選徑協定主要是使用在路由器(Router)之間的協定，使路由器能自動地學習其他路由器的選徑表格(Routing Table)，並進而更新自己的選徑表格，使網路的管理較容易。在一個自主性系統(Autonomous System)內，所使用的選徑資訊協定稱內部閘道器協定(Interior Gateway Protocol，簡稱 IGP)，而自主性系統與自主性系統間的協定就稱為外部閘道器協定(Exterior Gateway Protocol，簡稱 EGP)。RIP 就是屬於內部閘道器協定的一種。用來實現它的程式叫做 routed。

RIP 服務基本上維護了一份動態選徑表格(dynamic routing table)，其中登錄了每一目標主機的相對距離、及下個最近的路由器(router)，距離代表其間的路由器數目。典型的選徑表格舉例如下：

目標 (destination)	下一站 (next hop)	距離 (distance)	計時器 (timers)	旗號 (flags)
網路 A	選徑器 2	5	t1,t2,t3	x,y
網路 B	選徑器 1	2	t1,t2,t3	x,y
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
網路 X	選徑器 2	4	t1,t2,t3	x,y

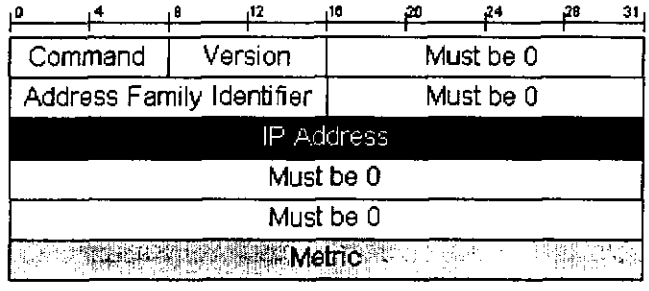
RIP 是以傳統的最短距離演算法提供詢問者一最佳的遞送路徑，由於 RIP 是路由器間對談時使用的協定(Protocol), 且是以廣播(Broadcast)的方式來傳送，每 30 秒便傳送一次本身全部的選徑表格(Routing Table)，所以較佔網路頻寬。當路由器收到別的路由器所傳送的 RIP 資料，便會將這些的選徑表格資料的 Hop 數加一，同時將其加入本身的選徑表格，若是同一個目的地址

有二個 Routing 的路徑時，會將 Hop 數少的路徑留下，而拋棄 Hop 數多的路徑。

當網路拓撲(Topology)發生變動時，例如路由器偵測到另一個路由器發生當機、或是在網路上出現新的路由器時， RIP 會將新的變動訊息廣播(broadcast)至所有支援 RIP 的路由器。

參與動態選徑(dynamic routing)的主機間以 RIP 封包(packet)交換資訊，RIP 利用 UDP 的埠 520 收發封包，此封包的固定表頭長 32 位元，其後可接至多 25 筆

RIP (Routing Information Protocol) Packet



相同格式的訊息，其中的訊息內含該網路的選徑資訊，每個封包皆有固定作用，在其命令(Command)欄描述。

RIP 的封包命令(packet command)如下：

命令碼	描述
1	要求(Request)選徑表資訊
2	回應(Response)選徑表資訊
3	追蹤開啓(Traceon)(此命令已宣布停用)
4	追蹤關閉(Traceoff)(此命令已宣布停用)
5	Sun Microsystems 保留命令

2.10.2. 參考資料

- RFC 1058 : Routing Information Protocol , Updated by RFC 1388, RFC 1723
- RFC 1387 : RIP Version 2 Protocol Analysis, Obsoleted by RFC 1721
- RFC 1388 : RIP Version 2 Carrying Additional Information, Obsoleted by RFC 1723, Updates RFC 1058
- RFC 1389 : RIP Version 2 MIB Extensions, Obsoleted by RFC 1724
- RFC 1581 : Protocol Analysis for Extensions to RIP to Support Demand Circuits
- RFC 1582 : Extensions to RIP to Support Demand Circuits
- RFC 1721 : RIP Version 2 Protocol Analysis, Obseletes RFC 1387
- RFC 1722 : RIP Version 2 Protocol Applicability Statement, Also STD0057
- RFC 1723 : RIP Version 2 - Carrying Additional Information, Obsoletes RFC 1388, Obseleted by RFC 2453, Updates RFC 1058, Also STD 0056
- RFC 1724 : RIP Version 2 MIB Extension, Obsoletes RFC 1389
- RFC 1923 : RIPv1 Applicability Statement for Historic Status
- RFC 2082 : RIP-2 MD5 Authentication
- RFC 2091 : Triggered Extensions to RIP to Support Demand Circuits
- RFC 2092 : Protocol Analysis for Triggered RIP
- RFC 2453 : RIP Version 2, Obsoletes RFC 1723, Also STD 0056
- STD 0056 : RIP Version 2, Obsoletes RFC 1723, Also RFC 2453
- STD 0057 : RIP Version 2 Protocol Applicability Statement, Also RFC 1722
- http://www.ieng.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm
- http://www.ietf.org/html.charters/rip-charter.html

2.10.3. 可能存在的漏洞

RIPv1 擁有一些問題如下 :

1. RIPv1 不能用可變長度的切割子網路 。 在可變長度的切割子網路上它將一貫地誤譯 prefix 的長度 。
2. 所有 CIDR supernet 都必須分開及公佈為個體 自然班的公告 。

3. 甚至當跑 RIPv1 的時網路透過固定的方法是自己唯一的子網路 ， 如果網路的其餘部分有可變的切割子網路則人們必須精心地確信 RIPv1 不毀壞 mask 資訊當這些資訊傳送給跑 RIPv1 的子網路 當跑 RIPv1 。
4. 網際網路不久將利用出現以 RIPv1 之位址為 Class A 部分網路 。 使用 RIPv1 的網路也許不能到達一 分段的單一 Class A 的所有地點 。

安全功能不包含於 RIPv1 裡面 。 RIPv2 含有一個機制可鑑別發送路由資訊的發送器 。 有擔憂路由基礎弱點而有必要跑像 RIP 協定一樣的地點應該使用 RIPv2 。
RIPv2 的鑑別方式如下 ：

因為鑑別是每訊息的功能 ， 而在訊息 header 中只有可用的兩個八位組的欄位 ， 任何合理的鑑別設計將需要多於兩個八位組 ， 所以 RIPv2 的鑑別設計將使用整個 RIP 協定入口的空間 。 如果訊息中的第一個 (和僅僅第一個) 入口的 Address Family Identifier 是 0xFFFF ， 則其餘部分的入口含有這個鑑別 。 意思是有可能至多 24 個 RIP 入口在其餘訊息中 。 如果鑑別不處於使用中 ， 則訊息中的入口不應該有 0xFFFF 的 Address Family Identifier 。 目前 ， 唯一的鑑別類型是簡單密碼並是第 2 類型的 。 這些剩下 16 個八位組含有清楚的文字密碼 。 如果密碼是在 16 個八位組下 ， 它必須先從左邊證明正確然後又移之後將左邊以零 (0x00) 填滿 。

如果路由器沒被設成鑑別 RIPv2 訊息 ， 那時 RIPv1 訊息和未被批准的 RIPv2 訊息會被接受 ， 反而已被批准的 RIPv2 訊息會被放棄 。 如果路由器有被設成鑑別 RIPv2 訊息 ， 那時 RIPv1 訊息和已被批准的 RIPv2 訊息會被接受 ， 未被批准的訊息和鑑別失敗的 RIPv2 訊息會被放棄 。為最安全的考量 ， 當鑑別處於使用時應該忽視 RIPv1 的訊息 。

2.11. RIPng

2.11.1. 通信協定詳述

路由資訊協定(Routing Information Protocol)係一個廣被使用的內部閘道器協定，它原本是定義於 1988 年而相關文件則記錄於 RFC1058。IPv6 所支援的 RIP 稱為 RIPng，而相關文件記錄於 RFC 2080[6-1]。

RIP 是一個遠方向量演算法架構的協定，它的歷史可以追溯到 ARPAnet 的早期。RIP 是為中等大小的網路而設計，它具有以下的一些限制：

- 被網路限制其最長路徑(或網路的直徑)為 15 個跳躍。
- 協定需要依賴一個名為「算至無限(counting to infinity)」的程序來解決特定的形勢，例如路由迴路。這個程序在解決之前先會假設擁有大量的網路頻寬。
- 協定需要依賴固定的計量去比較其他的路由器，而忽略即時性的參數，如遲延、可靠性或負載。

RIPng 是一個允許路由器交換在 IPv6 架構網路計算路由資訊的協定。每一個執行 RIPng 的路由器會假定擁有路由表(Routing Table)，它當中登記了每一個可以到達的 IPv6 目的地。而記錄中包含的資料如下：

- IPv6 目的地的字首
- 一個可以指出將封包資料從路由器到達目的地總成本的計量
- 到達目的地的路徑中下一個路由器的 IPv6 位址，此稱下一跳躍(Next Hop)
- 一個用以指示有關於路由器資訊最近是否有被修改的路由改變旗標(Route Change Flag)
- 各種的計時器，例如 30 秒計時器會觸發傳送路由表資訊到鄰近路由器

RIPng 是一個使用者資料封包協定(User Datagram Protocol，UDP)架構的協定，它在 UDP Port 521 上發送與接收封包。RIPng 封包(圖 6-1)包括三個欄位：命令(Command，要求或回覆)、版本(Version，1)，與路由表登記(Route Table Entry，RTE)。每一個路由表登記(圖 6-2)包括了 IPv6 字首(IPv6 Prefix)、路由標籤(Route Tag，用以從外部路由中區分內部路由)、字首長

度欄位(Prefix Length，用以決定字首中有意義的位元數目)，與計量(Metric，用以定義現在對目的地的計量)。

RIPng 也為封包提供最接近的下一跳躍的 IPv6 位址的功能。這個下一跳躍是由一個特別的 RTE、下一跳躍路由表登記所定義(圖 6-3)。字首欄位指出下一跳躍的 IPv6 位址；路由標籤與字首長度會被設定為 0，而被接收方所忽略。

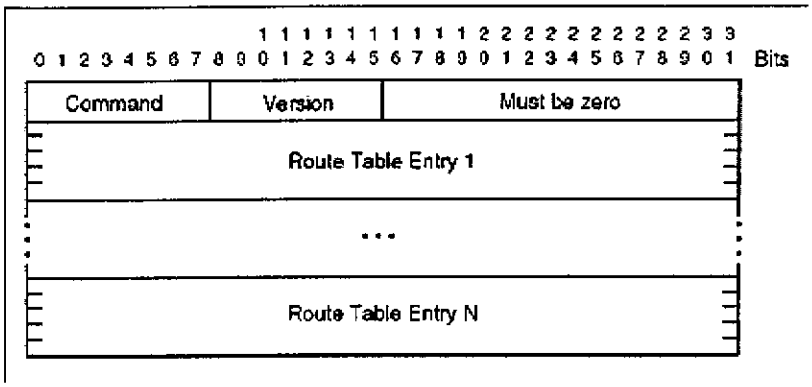


圖 6-1 RIPng 封包格式

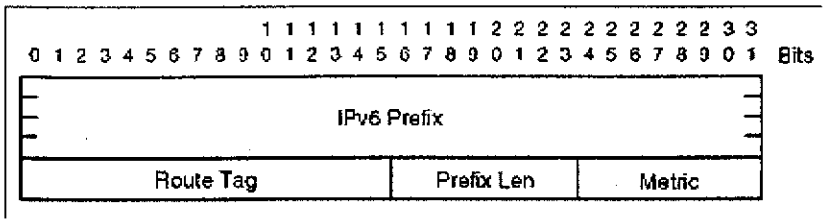


圖 6-2 路由表登記格式

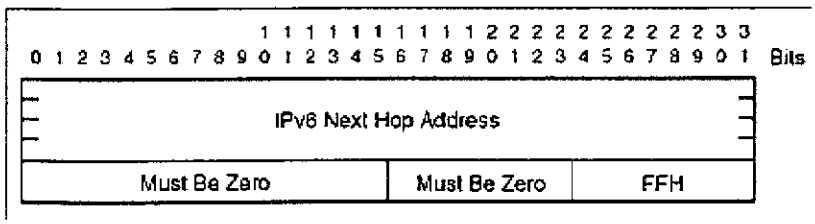


圖 6-3 下一跳躍 RTE 格式

第一版的 RIPng 支援兩個命令：要求(Request)與回覆(Response)。一個要求是用于要求所有或部份的路由表。通常，要求會以多重播送從 RIPng 埠(port 521)所發送，如果資訊只有被一個路由器所要求，那麼要求會直接由其他的埠傳送給路由器，而不是 RIPng 的埠。而回覆又分為三種：回覆特定查詢、定期更新、與因為路由改變而引發的更新。有關於要求與回覆封包的明確詳細資料已記錄於 RFC 2080 中。

2.11.2. 參考資料

- RFC 2080 : RIPng for IPv6
- RFC 2081 : RIPng Protocol Applicability Statement

2.12. RSVP

2.12.1. 通信協定詳述

RSVP (Reservation Protocol) 主要是用來提供網際網路上點對點的即時品質服務。一個 Real-time 的應用程式可以利用 RSVP 要求相關 router 保留資源（頻寬）以利其傳送 Real-time 資料。如此一來，我們才能在這些資訊的取得上，有較高的品質。例如我們要看一段影片，如果老是斷斷續續，又很不清楚，那麼勞心效果、興致都大打折扣。但如果有 RSVP 的幫助，router 可以提供特別的資源讓這些資訊優先通過，那麼我們就可以很順利的看到這一段影片。

RSVP 是用來建立網路上的資源保留。當一個用戶端的應用程式要以特殊的品質服務傳送資料流的時候，他可以利用 RSVP 向資料所經過的 router 要求一個特殊路徑來傳送這些資料。RSVP 利用參數與這些 router 交涉。如果這項資源保留的管道允許被建立，那麼 RSVP 也承擔起維持 router 和用戶端狀態確保傳輸品質的責任。

每一個點對於是否有能力保留資源，以及往後如何建立保留制度、履行保留機制，都需要經過一些局部性的考量步驟。Policy control 決定使用者是否有權力去產生保留機制。在未來，保留機制的驗證、存取控制以及記錄都會被實做在 control policy 中。Admission control 是負責記錄該點 (router) 的系統資源，並解決定是否有足夠的力量提供這項品質服務。可以參見圖一。

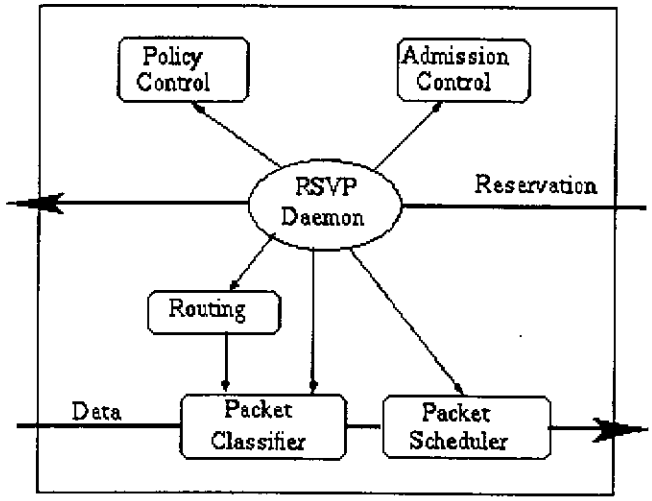


Figure 1

RSVP daemon 會檢查這兩個 control 程序。如果失敗，則 RSVP 會告知要求此服務的應用程式。如果成功，RSVP 的 daemon 就會在 packet classifier 和 packet scheduler 中設好參數以取得這項服務。Packet classifier 決定每個 packet 的服務品質等級，而 packet scheduler 則是負責排列封包傳送的順序，好讓每個資料流都能達到這項服務品質。RSVP daemon 也會和 router 上的 routing process 溝通決定他要使用的路線。

保留的機制被實做成兩種 RSVP 的訊息：PATH 和 RESV。PATH 訊息每隔一段時間就會從 sender 送向 multicast address。一個 PATH 的訊息包含了資料流的一些性質，如：資料格式、來源地址、來源 port，同時也有傳遞一些網路上交通的特性。這些由 PATH 帶來的訊息可以讓接收端找到一條反向回 sender 的路徑，同時也能決定什麼樣的資源需要保留下來提供特殊服務。當然，接收端要在 multicast group 裡面，這樣才能接收到這項 PATH 訊息。

另外一個訊息 RESV 是由接收端所產生的。而且其中包含 flow spec 和 filter spec。Filter spec 定義資料流中的哪一個 packet 要用來當作 packet classifier，而 flow spec 用在 packet scheduler，其中內容是根據服務而定。RESV 依照送來 PATH 的反向路徑，在許多相關的 node 上，對所有通過要求的 sender，建立起保留資源的機制。

建立在 router 上的 RSVP 資源保留機制是一種軟性狀態。RSVP daemon 必須每隔一段時間就送出更新的訊息，這樣才可以保持這項資源保留的機制。如果在一段時間內，更新的訊息沒有送給 router，那麼資源保留的機制將會被破壞。利用這種軟性狀態的方法，使得 RSVP 可以很容易對經常變動的服務成員以及不同的繞路路徑加以掌控。

雖然這項服務是由使用者，也就是接收端來發出要求。但是每一個接收端卻不需要對資料流過路徑上的所有 node 都發送此一訊息。所謂資料流過的路徑，就是指 sender 到 receiver 之間的路徑。接收端送出的要求訊息會往 sender 的方向走，因為要通知資料流經過的 router 提供資源保留的服務。但是如果這個要求訊息到達某個 node，該 node 上也有被要求要提供資源保留的服務，且資料流的來源是同一個 sender 的話，那麼這個要求訊息將會被合併，而不需要繼續往 sender 的方向通知所有 node。圖二有顯示出資源保留的要求訊息是如何合併，最後在網路上產生類似一個 tree 的廣播架構。

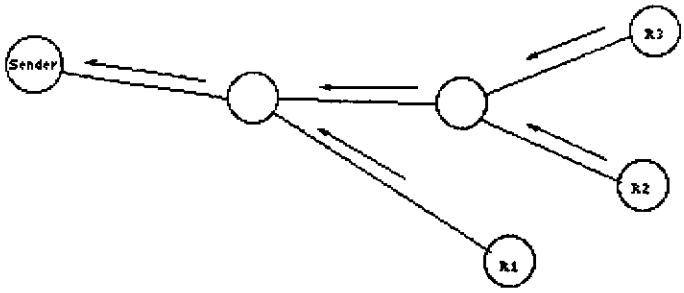


Figure 2

這項合併的方式帶給 RSVP 很大的彈性。就算有很多的使用者發出訊息要加入廣播行列也不會增加網路太多的負擔。就是因為這樣的方式，使得 RSVP 在很多人加入接收廣播的情況下，協定上的平均負擔反而會下降。

實際上，這項保留資源機制並不去做資料的傳輸以及提供所要求的服務品質。但是有了這些資源，RSVP 就可以保證資料的傳送不會間斷。
雖然 RSVP 是放在七層協定架構中 IP 的頂端，但是他並不是一個繞路的協定，而是一個資網路控制的協定。再說明確一些，RSVP 是依靠繞路的協定去找尋要送出服務要求的 node。RSVP 也會和 unicast、multicast 的協定合作。當 RSVP 所管理的路徑有所改變時，負責繞路的模組會通知 RSVP 路徑改變情形，因此 RSVP 就能夠迅速的在新的路徑上，調整出適當的資源保留機制。

傳送資源保留機制的參數並不屬於 RSVP 的工作，而是屬於要求 QoS 的 control device。RSVP 所扮演的角色是把這些參數發出去。因為不同的應用程式會有不同的 QoS control device，所以 RSVP 將這些可能為不同格式的參數看作是一個不明確的資料。把這些資料分給適當的 router，再由 router 上的控制模組去解讀這些參數是什麼意思。這樣的設計可以簡化 RSVP 的複雜度，也使得 RSVP 更有彈性，能夠適應往後新的網路科技或應用程式。

RSVP 的一些性質：

a. RSVP 的保留機制是單向的

RSVP 會分辨到底這裡是 sender 還是 receiver。但是很多情況中，一個主機可以是接收端同時也可以當作發送端。不過 RSVP 只會為某一方向做資源保留的機制。

b. RSVP 提供 multicast 和 unicast，而且可以根據參與成員和繞路狀況作調整

RSVP 同時為了 multicast 和 unicast 設計。因為保留機制的要求是發自接收端，而且資源保留狀態是有彈性的，所以 RSVP 對於參與成員和繞路的改變很好處理。一個主機可以利用 IGMP 去餐加一個廣播團體，而 RSVP 只要根據前面所述的方法，就可以輕鬆的將這台主機加入資源保留機制的行列，而不會花去大量多餘的網路負擔。

c. RSVP 是以接收端為導向，且可以處理很多不同種的接收端

在許多性質不同的廣播團體中，接收端擁有不同的能力和品質要求。而以接收端為導向設計的 RSVP，就必須能夠處理這樣的情況。接收端根據自己的需要，選擇品質等級。而發送端會將不同品質等級分成不同的 RSVP 流。接收端就可以自由參加一個或多個 RSVP。這樣的設計可以使接收端有更大的彈性，獲得自己需要的品質等級。

d. RSVP 有良好的相容性

RSVP 已經可以跑在 Ipv4 和 Ipv6 上面。他提供了不明確的流程控制和政策控制，為的是能夠方便適應新的科技。他在沒有支援的區域提出了明確的運算功能。

RSVP 溝通的是接收端的應用程式和網際網路中的 router。因此相信許多應用程式的設計者比較關心 RSVP 的介面為何？就目前而言，ISI 和 Sun Microsystems 已經提出了一套 RSVP client library 叫做 RAPI 供程式設計員使用。重要的幾個函數如下：

a. rapi_session() 產生並初始化一個 session 並傳回一個 handle。
b. rapi_sender() 被發送端應用程式呼叫指定資料參數。
c. rapi_reserve() 這是對資源保留機制做改變的函數。
d. rapi_release() 要求 RSVP daemon 拆除資源保留機制。

2.12.2. 參考資料

- RFC 2205 : Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification , Updated by RFC 2750

- RFC 2206 : RSVP Management Information Base using SMIv2
- RFC 2207 : RSVP Extensions for IPSEC Data Flows
- RFC 2208 : RSVP Version 1 Applicability Statement Some Guideline on Deployment
- RFC 2209 : RSVP Version 1 Message Processing Rules
- RFC 2210 : The Use of RSVP with IETF Integrated Services
- RFC 2750 : RSVP Extensions for Policy Control, Updates RFC 2205
- http://www.isi.edu/div7/rsvp/overview.html

2.12.3. 可能存在的漏洞

RSVP 提起下面的安全問題：

1. 訊息的完整性和節點的鑑別

破壞或者哄騙的要求能導引由未經認證主機引起服務的偷竊行為或者導引由把網路資源鎖起來產生的 DOS (Denial Of Service) 攻擊 。 RSVP 為了避免如此攻擊 ， 則有一個 hop by hop 鑑別的機制 ， 使用一個加密的 hash function 。 此機制是由可以在任何 RSVP 訊息中出現的 INTEGRITY 物件支援 。

這些物件使用一個 cryptographic digest 技術 ， 採取 RSVP 鄰居所分享的祕密 。 RSVP 完整性機制的普遍使用將為一些 router 需要長久尋找的 key management 和分發的基礎的能力 。 直到那個基礎變可用的, 將要求手動 key management 確保 RSVP 訊息的完整性 。

2. 使用者確證

策略控制將取決於負責每一個預定要求的用戶的正確鑑別 。 因此策略資料可能包括密碼保護的用戶憑證 。 憑證詳細規劃是一個將來的研究方向 。

甚至沒有全部可驗證的用戶憑證 ， 也許可能透過建立一系列信任在許多情況中提供實際的用戶鑑別 ， 使用之前所描述的 hop by hop 完整性 。

前二個的安全問題是 RSVP 的操作相關的問題。這第三個安全問題是對於安全資料流的資源保留問題。尤其是，把 IPSEC 用於資料流為 RSVP 提出一個問題：如果運輸層和更高層的 header 加密，則不能用 RSVP's 的普遍 port 數字來定義 session 或發送器。

為了解決這個問題，定義了一個 RSVP 擴展將 IPSEC SPI 作為相當於普遍的 Port。

2.13. VRRP

2.13.1. 通信協定詳述

VRRP 路由器 是一個 有跑 Virtual Router Redundancy Protocol 的 路由器 。 它可能)參與一或更多的虛擬路由器 。

虛擬路由器是由在一個分享的 LAN 上充當預設路由器的 VRRP 所管理的一個抽象物體 。 它含有一個 Virtual Router Identifier (VRID) 和一套聯繫普通 LAN 的 IP 位址 。 一個 VRRP 路由器有可能備用一或更多的虛擬路由器 。 IP 位址所有者是擁有作為真實界面位址的虛擬路由器的 IP 位址 。

Virtual Router Redundancy Protocol (VRRP) 是被設計用來除去單一點的失敗所存在靜態預設傳送路線的環境 。 VRRP 路由器 規定一個選舉協定 ， 動態地在 LAN 上對 VRRP 路由器之一為一個虛擬路由器分發責任 。 VRRP 路由器控制 IP 位址與虛擬路由器聯繫的叫作 master ， 他把封包轉送到這些 IP 位址去 。 選舉過程提供動態失敗在傳遞責任中應該 master 變得不能用 。 那時任何在 LAN 上的虛擬路由器的 IP 位址能夠被末端主機應用當第一個 hop 路由器 。 使用 VRRP 所獲得的優點是一個更高效力的預設路徑 ， 而不需要在每一台末端對動態 routing 或 discovery 協定作設定 。

一個簡單模型的 master 選舉在一套多餘路由器中是對每一台路由器在聚集任何路由器當 master 之後使用同等優先選擇來處理 。 然而 ， 很有可能有許多環境在一套多餘路由器中具有不同優先選擇 (或者優先選擇的範圍) 。 例如 ， 此優先選擇可能基於途徑聯結的費用或速度 ， 路由器的表現或可靠性 ， 或者其他策略的考量 。 那些協定應該以直覺模式承認這個相關路徑優先選擇的表現 ， 與對目前可用的最優惠的路由器保證 master 收斂性 。

VRRP 指定一個選舉協定提供虛擬路由器功能 。 所有訊息協使用 IP 多重播送資料電報執行 ， 因此那協定可作出多存取 LAN 技術支援 IP 多重播送 。 每一個 VRRP 虛擬路由器有一個 MAC 位址給它 。 虛擬路由器是由它的 Virtual Router Identifier (VRID) 和一套 IP 位址定義 。 VRRP 路由器可以結合一個虛擬路由器跟它的真實位址 ， 也可以用附加虛擬路由器的 mappings 和虛擬路由器的優先構成。

為了使網路流量減到最少 ， 每一個虛擬路由器的 master 僅僅送週期性的 VRRP 廣告訊息 。 備用路由器不能試圖先取得 master 除非它有更高的優先 。 此消除服務的破壞除非有更多路徑變可用的 。 這也可以禁止所有先取得權限的試圖 。 唯一的例外是 VRRP 路由器總是將成為與它擁有位址的任何虛擬路由器的 master 。 如果 master 那時變不可拿到最高的優先 ， 備用路由器將在短短的耽擱時間後變成 master ， 在最小服務中斷間提供虛擬路由器責任的控制 。

VRRP 封包是被送為囊中的 IP 封包 。 他們被送到歸因於 VRRP 的 IPv4 多重播送位址 。

IP 欄位詳述 ：

1. Source 位址是寄這個封包的 IP 位址 。
2. Destination 位址是多重播送 IP 位址 IANA 所分給 VRRP (如 ： 224.0.0.18) 。 這是聯結本地範圍的多重播送位址 。 路由器不應該發送含有這類目的地而不管它的存活時間的資料電報 。
3. TTL ， 必須把存活時間設成 255 。 如果一個 VRRP 路由器有收到存活時間不等於 255 的封包必須放棄這個封包 。
4. Protocol Number ， IANA 所分給 VRRP 是 112 (小數) 。

VRRP 欄位詳述 ：

1. Version 欄位 ， 指定這個封包的 VRRP 版本 。
2. Type 欄位 ， 指定這個 VRRP 封包的類型 。
3. Virtual Router Identifier (VRID) 欄位 ， 識別此虛擬路由器將這封包報告狀況給它 。
4. Priority 欄位 ，指定送 VRRP 路由器的優先給虛擬路由器。 更高的值等於更高的優先 。
5. Count IP Address 欄位 ， 是在這個 VRRP 廣告中含有的 IP 位址的數目。
6. Authentication Type 欄位 ，確定利用鑑別方法 。 鑑別類型在一個實虛擬路由器基礎方面是唯一的。 這個鑑別類型欄位是 8 bit unsigned 整數。 不鑑別類型不清楚或不符合本地所設的鑑別方法的封包必須被丟掉 。鑑別方法目前所定義的是 ：

    0 沒有鑑別

    1 簡單文字密碼

    2 IP 鑑別 Header

7. Advertisement Interval 欄位 ，表示廣告訊息之間的時間間隔 ， 預設 1 秒 。 這欄位是用作故障查找路由器的錯誤設定 。
8. Checksum 欄未 ， 用來探查 VRRP 訊息中的資料貪污腐化 。 Checksum 是採用 16 bit one' s complement 之整個從 Version 欄位的 VRRP 訊息的 one' s complement 。
9. 一或更多的 IP 位址 ， 包括位址的數目在 "Count IP Addrs " 欄位中規定的。 這些欄位是用作故障查找路由器的錯誤設定 。
10. Authentication string ，目前僅僅利用簡單 text 鑑別 ， 與簡單 text 鑑別類似在 OSPF 中規定的 。

2.13.2. 參考資料

- RFC 2338 : Virtual Router Redundancy Protocol
- RFC 2787 : Definitions of Managed Objects for the Virtual Router Redundancy Protocol

2.13.3. 可能存在的漏洞

不倚賴於任何鑑別類型 ， VRRP 含有避免從另一遠程網路注射 VRRP 封包的一個機制（設存活時間 = 255 ， 檢查收據）。 此限制易受本地攻擊。

在此所討論的安全措施僅僅提供各種種類的鑑別 。 祕密對於 VRRP 的正確操作是不必要的 ， 另外沒有任何資訊在 VRRP 訊息中是需要從其他 LAN 上的節點保密的 。

1. 沒有鑑別

使用這種鑑別的意思是將 VRRP 交流沒有被鑑別 。 此類鑑別只應該用於擁有最小限度的安全危險與少機會有錯誤設定的環境上 (如: 在 LAN 上的兩個 VRRP 路由器) 。

2. 簡單文字密碼

使用這種鑑別的意思是將 VRRP 交流由一個簡單清楚的文字密碼作鑑別 。 這類鑑別對於避免在 LAN 上的路由器不小心設錯是很有用的 。 這避免一些路由器非故意的後援其他路由器 。 一個新路由器在跟其他路由器執行 VRRP

前一定要先把密碼設好 。 當惡意者能夠由竊聽 LAN 上的 VRRP 封包學習它的密碼這類鑑別不防護敵對攻擊 。 與 TTL 核對結合的簡單文字鑑別使一個 VRRP 包難從另一個 LAN 送以破壞 VRRP 操作 。

建議使用這種類型的鑑別當有最小限度危險的節點在 LAN 上積極地破壞 VRRP 操作 。 如果使用這種類型的鑑別 ， 用戶應該會察覺到此鑑別經常送清楚文字密碼 ， 因此 ， 不應該是與任何安全重要密碼相同 。

3. IP 鑑別 Header

使用這種鑑別的意思是 VRRP 交流由 IP 鑑別 Header [AUTH] 所定義的機製作鑑別 ， 使用 HMAC - MD5 - 96 在 ESP 和 AH 之內 。這提供與設定錯誤 ， replay 攻擊 ， 和封包修正相對的強壯保護 。

建議使用這種類型的鑑別當有管理限制控制的節點在 LAN 上 。 當這種類型的鑑別確實保護 VRRP 的操作, 有其他類型的攻擊可能在分享聯結中使用 (如 ： 生產偽造的 ARP replies) 從 VRRP 那裡獨立而不保護 。

雖然為 VRRP 作保可防止未被批准的機器參加選舉協定 ， 但是它不使網路上的主機避免被欺騙 。 例如 ， gratuitious ARP reply 從所主旨的虛擬路由器的 IP 位址有可能把流量指向一個未被批准的機器 。 同樣地 ， 借助於鍛造的 ICMP redirect 訊息個體連接有可能被轉移 。

第三章　路由器漏洞分析

將各個主流路由器已被發現的弱點依照路由器廠商分為六大類來說明，主要分為 Cisco 路由器 ， Lucent 路由器 ， 3Com 路由器 ， Xylan 路由器 ， Network Extreme 路由器 和 Cabletron 路由器 。 這六種路由器的弱點通常是經由修補程式或更改路由器上的設定來補強系統 。 由於路由器的漏洞是很少被公開 ， 故將目前已發現的漏洞和解決方法分析完之後整理成一分完整的報告 。

3.1　Cisco 路由器

Denial of Service (阻斷式攻擊)

3.1.1. Cisco Discovery 通信協定漏洞

弱點名稱	Cisco Discovery 通信協定漏洞
受影響系統	- Cisco 1005 IOS 11.1.x - Cisco 1603 IOS 11.2, 11.3.11b - Cisco 2503 IOS 12.0.19 - Cisco 2600 IOS 12.1.? - Catalyst 2940XL IOS 12.0(5.1)XP
弱點詳述	Cisco Discovery 通信協定是一個第二層通信協定 。 一台 Cisco 機器在定期的時間內會從它的介面送出更新訊息通知它的鄰居的機器 。 由於他是一個第二層通信協定，所以此封包沒有被轉送 。 此封包是透過多重播送 01:00:0C:CC:CC:CC 地址送出去 。 當 Cisco 機器收到從其他機器送給它的一個 CDP frame，它會複製 CDP frame 的內容至資料結構裡面，使管理者可以用 'show cdp neighbors' 指令觀察從別的機器送來的 CDP 訊息，裡面的資訊包括機器身分，功能，平台及送封包者的通訊埠身分。CDP frames 也包含了保留計時值，讓鄰居機器可以判斷送來的 CDP 訊息要被保留多久，保留計時值最大值為 255 秒 (4 分鐘 15 秒) 。

	內部資料結構使用遠端機器身分當關鍵值，當某些 IOS 版本收到兩個同樣而很長的機器身分的時候，它會錯誤認為那兩個封包是兩個不同的封包而將兩個封包各存到不同的地方。 當一個網路端被大量機器身分而從不同地方的 CDP frame 淹沒的時候，各種 IOS 會有不同的反應如下 ： + 收到 3 至 5 個 frame 之後機器會自動重開 + 收到千數 frame 之後 IOS 會完全暫停服務 + 一直把 CDP 鄰居的資訊存到機器的記憶體塞滿為止 當記憶體被塞滿之後，機器沒辦法執行其他需要用到記憶體的服務如： telnet session 和動態路由器更新。 若管理者想使用機器上的 console 執行 'debug cdp packets' 的指令，所有被測試的介面會立即當機。
解決方法	有兩種解決方法，第一種是使用以下指令把機器上的 CDP 功能關掉 ： Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# no cdp run 也可以使用以下指令關掉特定介面的 CDP 功能： Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# interface Ethernet0 Router(config-if)# no cdp enable 第二種解決方法是更新機器的系統版本，以下是解決此問題的系統版本 ： Cisco IOS 12.2(3.6)B Cisco IOS 12.2(4.1)S Cisco IOS 12.2(3.6)PB Cisco IOS 12.2(3.6)T

	Cisco IOS 12.1(10.1) Cisco IOS 12.2(3.6)
攻擊工具	cisco_CDP.pl
參考資料	http://www.cisco.com/warp/public/707/cdp_issue.shtml http://www.securiteam.com/securitynews/6K00J1F2UI.html

3.1.2. Cisco 7xx Series Router DoS 漏洞

弱點名稱	Cisco 7xx Series Router DoS 漏洞
受影響系統	- Cisco Router 770.0 - Cisco Router 760.0 - Cisco Router 750.0
弱點詳述	在 port 23 開啟大約 98 個連線將會導致 Cisco760 系列路由器重開機，如果一直使用這個步驟將會是一種 DOS 攻擊。
解決方法	Cisco 對所有客戶提供免費升級軟體來解決 CSCdm03231。
攻擊工具	cisco_760series.c cisoc_760series.pl
參考資料	http://www.cisco.com CVE-1999-0415 http://www.securityfocus.com/bid/1211

3.1.3. Cisco 675 Web Admin 漏洞

弱點名稱	Cisco 675 Web Admin 漏洞
受影響系統	- Cisco DSL Router 677.0 + Cisco CBOS 2.3 + Cisco CBOS 2.2 - Cisco DSL Router 675.0 + Cisco CBOS 2.3 + Cisco CBOS 2.2
弱點詳述	Cisco 675DSL Router 是一個相當普及及廣為使用的 DSL 路由器，主要使用在電話總機房的 SOHO 客戶端。 在 Cisco 675 DSL 路由器中存在著一項弱點，可能使該 router 遭受 DOS 攻擊，除非重新啟動才能回復到正常狀況。 如果 Cisco 675 DSL 路由器有打開 Web 管理介面，遠端攻擊者可以用 telnet 連到此台路由器，並發出一個簡單卻有問題的 HTTP GET 需求，一旦利用 telnet 連到 Web 管理介面並發出 GET ? \n \n，不但將使這個 telnet session 斷掉，此路由器也會當掉。 以下的 Cisco 路由器系列都有此述弱點： 673, 675e, 676, and 678
解決方法	目前解決辦法可以將 Web 管理介面關掉，用以下步驟可以關掉： commands: cbos# set web disabled cbos# write cbos# reboot Cisco 已經發佈此項弱點參考，可以參考 cisco 釋出的建議事項來察看詳情。 並且暫時在 2000 12-11 釋出官方 patch，以及其他在 CBOS 作業系統的漏洞。
攻擊工具	cisco_675_DSL.pl
參考資料	http://www.cisco.com

3.1.4. Cisco Catalyst Memory Leak 漏洞

弱點名稱	Cisco Catalyst Memory Leak 漏洞
受影響系統	- Cisco Catalyst 4000 5.5(1), Cisco Catalyst 4000 5.5 - Cisco Catalyst 4000 5.4(3), Cisco Catalyst 4000 5.4(2), Cisco Catalyst 4000 5.4(1) - Cisco Catalyst 4000 5.4 - Cisco Catalyst 4000 5.2(7), Cisco Catalyst 4000 5.2(6), Cisco Catalyst 4000 5.2(5) - Cisco Catalyst 4000 5.2(4), Cisco Catalyst 4000 5.2(2), Cisco Catalyst 4000 5.2(1a) - Cisco Catalyst 4000 5.2(1), Cisco Catalyst 4000 5.2 - Cisco Catalyst 4000 5.1(2a), Cisco Catalyst 4000 5.1(1a), Cisco Catalyst 4000 5.1(1) - Cisco Catalyst 4000 5.1, Cisco Catalyst 4000 4.5(9), Cisco Catalyst 4000 4.5(8) - Cisco Catalyst 4000 4.5(7), Cisco Catalyst 4000 4.5(6), Cisco Catalyst 4000 4.5(5) - Cisco Catalyst 4000 4.5(4), Cisco Catalyst 4000 4.5(3), Cisco Catalyst 4000 4.5(2) - Cisco Catalyst 5000 5.5(4), Cisco Catalyst 5000 5.5(3), Cisco Catalyst 5000 5.5(2) - Cisco Catalyst 5000 5.5(1) - Cisco Catalyst 5000 5.4.1, Cisco Catalyst 5000 5.4(4), Cisco Catalyst 5000 5.4(2) - Cisco Catalyst 5000 5.4(1), Cisco Catalyst 5000 5.2(4), Cisco Catalyst 5000 5.2(3) - Cisco Catalyst 5000 5.2(2), Cisco Catalyst 5000 5.2(1), Cisco Catalyst 5000 5.2 - Cisco Catalyst 5000 5.1(2a), Cisco Catalyst 5000 5.1(1), Cisco Catalyst 5000 5.1 - Cisco Catalyst 5000 4.5(9), Cisco Catalyst 5000 4.5(8), Cisco Catalyst 5000 4.5(7) - Cisco Catalyst 5000 4.5(6), Cisco Catalyst 5000 4.5(5), Cisco Catalyst 5000 4.5(4) - Cisco Catalyst 5000 4.5(3), Cisco Catalyst 5000 4.5(2),

	Cisco Catalyst 6000 5.5(4a) - Cisco Catalyst 6000 5.5(4), Cisco Catalyst 6000 5.5(3), Cisco Catalyst 6000 5.5(2) - Cisco Catalyst 6000 5.5(1), Cisco Catalyst 6000 5.5, Cisco Catalyst 6000 5.4(4) - Cisco Catalyst 6000 5.4(3), Cisco Catalyst 6000 5.4(2), Cisco Catalyst 6000 5.4(1) - Cisco Catalyst 6000 5.4 - Cisco Catalyst 6000 5.3(6)CSX, Cisco Catalyst 6000 5.3(5a)CSX, Cisco Catalyst 6000 5.3(5)CSX - Cisco Catalyst 6000 5.3(4)CSX, Cisco Catalyst 6000 5.3(3)CSX, Cisco Catalyst 6000 5.3(2)CSX - Cisco Catalyst 6000 5.3(1a)CSX, Cisco Catalyst 6000 5.3(1)CSX
弱點詳述	Cisco Catalyst 是 LAN 上的高速 switch。內建在 Catalyst 韌體上，用來遠端管理的 telnet server 有記憶體耗盡的弱點，可能會造成阻斷式攻擊，每次當 telnet 服務啟動時，將使用記憶體資源但是之後並不會被釋放，所以，可以利用連續多次對該 Catalyst 的 telnet server 連線，造成該機記憶體耗損，導致無法繼續運作。 這將導致 Catalyst 上的服務 DOS，直到該機器重新啟動。
攻擊工具	cisco_memory_leak_telnet.c
解決方法	為了解決這個問題請裝修補版本如下： Cisco Catalyst 4000 4.5(9), Cisco Catalyst 4000 4.5(8), Cisco Catalyst 4000 4.5(7), Cisco Catalyst 4000 4.5(6), Cisco Catalyst 4000 4.5(5), Cisco Catalyst 4000 4.5(4), Cisco Catalyst 4000 4.5(3), Cisco Catalyst 4000 4.5(2): 請使用 Cisco upgrade Catalyst Release 4.5(10) Cisco Catalyst 4000 5.5(1), Cisco Catalyst 4000 5.5, Cisco Catalyst 4000 5.4(3), Cisco Catalyst 4000 5.4(2), Cisco Catalyst 4000 5.4(1), Cisco Catalyst 4000 5.4,

	Cisco Catalyst 4000 5.2(7), Cisco Catalyst 4000 5.2(6), Cisco Catalyst 4000 5.2(5), Cisco Catalyst 4000 5.2(4), Cisco Catalyst 4000 5.2(2), Cisco Catalyst 4000 5.2(1a), Cisco Catalyst 4000 5.2(1), Cisco Catalyst 4000 5.2, Cisco Catalyst 4000 5.1(2a), Cisco Catalyst 4000 5.1(1a), Cisco Catalyst 4000 5.1(1), Cisco Catalyst 4000 5.1, Cisco Catalyst 5000 5.5(4), Cisco Catalyst 5000 5.5(3), Cisco Catalyst 5000 5.5(2), Cisco Catalyst 5000 5.5(1), Cisco Catalyst 5000 5.4(4), Cisco Catalyst 5000 5.4(2), Cisco Catalyst 5000 5.4(1) , Cisco Catalyst 5000 5.2(4), Cisco Catalyst 5000 5.2(3) , Cisco Catalyst 5000 5.2(2), Cisco Catalyst 5000 5.2(1), Cisco Catalyst 5000 5.2, Cisco Catalyst 5000 5.1(2a), Cisco Catalyst 5000 5.1(1), Cisco Catalyst 5000 5.1(1), Cisco Catalyst 5000 5.1, Cisco Catalyst 6000 5.5(4a), Cisco Catalyst 6000 5.5(4), Cisco Catalyst 6000 5.5(3), Cisco Catalyst 6000 5.5(2), Cisco Catalyst 6000 5.5(1), Cisco Catalyst 6000 5.5, Cisco Catalyst 6000 5.4(4), Cisco Catalyst 6000 5.4(3), Cisco Catalyst 6000 5.4(2), Cisco Catalyst 6000 5.4(1), Cisco Catalyst 6000 5.4, Cisco Catalyst 6000 5.3(6)CSX, Cisco Catalyst 6000 5.3(5a)CSX, Cisco Catalyst 6000 5.3(5)CSX, Cisco Catalyst 6000 5.3(4)CSX, Cisco Catalyst 6000 5.3(3)CSX, Cisco Catalyst 6000 5.3(2)CSX, Cisco Catalyst 6000 5.3(1a)CSX, Cisco Catalyst 6000 5.3(1)CSX : 請使用 Cisco upgrade Catalyst Release 5.5(4b) Cisco Catalyst 5000 4.5(9), Cisco Catalyst 5000 4.5(8), Cisco Catalyst 5000 4.5(7), Cisco Catalyst 5000 4.5(6), Cisco Catalyst 5000 4.5(5), Cisco Catalyst 5000 4.5(4),

	Cisco Catalyst 5000 4.5(3), Cisco Catalyst 5000 4.5(2), : 請使用 Cisco upgrade Catalyst Release 4.5(10)
參考資料	CVE-2001-0041 http://www.securityfocus.com/bid/2072

3.1.5. Cisco Catalyst SSH Protocol mismatch DOS

弱點名稱	Cisco Catalyst SSH Protocol mismatch DOS
受影響系統	- Cisco Catalyst 4000 6.1(1b) - Cisco Catalyst 4000 6.1(1a) - Cisco Catalyst 4000 6.1(1) - Cisco Catalyst 5000 6.1(1b) - Cisco Catalyst 5000 6.1(1a) - Cisco Catalyst 5000 6.1(1) - Cisco Catalyst 6000 6.1(1b) - Cisco Catalyst 6000 6.1(1a) - Cisco Catalyst 6000 6.1(1)
弱點詳述	Catalyst 是一系列 LAN 上使用的高速 switch 裝置。 軟體版本為 6.1(1), 6.1(1a) 和 6.1(1b)的 Catalyst 4000, 5000, 與 6000，都支援 SSH 和 3-DES 加密，但是有一個弱點可能導致他遭受 DOS 攻擊。 如果連上一個有此弱點的 Catalyst 的 SSH 服務，且發生了 protocol mismatch error，將導致此台機器重新啟動，這是因為 supervisor engine 錯誤，無法處理錯誤。結果是導致裝置重新啟動，無法傳遞封包，無法正常運作。 以下是這些有漏洞的 image 檔。 cat4000-k9.6-1-1.bin cat5000-sup3cvk9.6-1-1a.bin cat5000-sup3k9.6-1-1.bin cat5000-supgk9.6-1-1.bin cat6000-sup2cvk9.6-1-1b.bin cat6000-sup2k9.6-1-1b.bin cat6000-supcvk9.6-1-1b.bin cat6000-supk9.6-1-1b.bin SSH 服務預設是關閉的，需要由管理者手動將他打開，這個漏洞只有發生當 SSH 服務是打開的。
解決方法	Catalyst software release 6.1(1c)已經修正此項漏洞。

參考資料	CVE-2001-0080 http://www.securityfocus.com/bid/2117

3.1.6. Cisco Catalyst Supervisor Remote Reload

弱點名稱	Cisco Catalyst Supervisor Remote Reload
受影響系統	- Cisco Catalyst 12xx supervisor software 4.29 - Cisco Catalyst 29xx supervisor software 2.1.502 - Cisco Catalyst 29xx supervisor software 2.1.501 - Cisco Catalyst 29xx supervisor software 2.1.5 - Cisco Catalyst 29xx supervisor software 1.0 - Cisco Catalyst 5xxx supervisor software 2.1.502 - Cisco Catalyst 5xxx supervisor software 2.1.501 - Cisco Catalyst 5xxx supervisor software 2.1.5 - Cisco Catalyst 5xxx supervisor software 1.0
弱點詳述	遠端的攻擊者可由 port 7161 讓此台有漏洞 switch 的 supervisor module reload，當 supervisor reload 的時候，該 switch 將無法轉送 packet，此時攻擊者便可以使得連在此 switch 的機器遭受 DOS 攻擊。雖然此台 switch 將會自動回復，但是重複此項攻擊將會無限制的使得此機器 DOS。
解決方法	Catalyst 29xx 及 Catalyst 5xxx switches，此項漏洞有 Cisco 漏洞 ID 為 CSCdi74333，此項漏洞出現在所有 supervisor software，從 2.1(5)，包括 spot fix releases 2.1(501)和 2.1(502)，此項漏洞已經在 2.1(6)和後面的版本修正了，包括所有 2.2 ,2.3 ,2.4。還有所有的 3.x 4.x 及後面的版本。而 catalyst 1200，此項漏洞 ID 為 CSCdj71684，此漏洞發生在 4.29，而在 4.30 和後面的版本獲得修正。 不要 assign IP 給受到此問題的 Cisco Catalyst switches，或者關掉這個遠端管理的服務，或者使用 firewal 檔掉不受信任的 ip，保護只有授權過的 ip 才能連道 tcp port 7161。
參考資料	CVE-1999-0430 http://www.securiteam.com/securitynews/5IP010A3RC.html

3.1.7. Cisco Content Service Switch Long Name DOS

弱點名稱	Cisco Content Service Switch Long Name DOS
受影響系統	- Cisco WebNS 4.0 - Cisco WebNS 3.0
弱點詳述	Cisco Content Services (CSS) 是設計用來對使用 Cisco Web Network Services (Web NS)提供強化 e-commerce web service、Web Content delivery，CSS switch 是 Cisco 公司發佈的。 這個問題是『CSS 允許一個 local user 對一個合法的 user 停止服務。』 問題出在處理 local user 對 input 的處理。使用者必須先取得該 switch 的命令列介面才能使用這項攻擊，但不需要用到 administrator 的權力。當用一個 non-privileged 的帳號，使用者可以在該 switch 的本地端執行命令，並使用一個檔名作為參數，當該指定檔名是 filename buffer 的 size 上限時，這台 switch 便會 reboot，然後開始做 system check 動作。 這項漏洞使得惡意的使用者可以連上該 switch 並取得較高的權限，或者執行命令導致正常使用者無法正常使用。此項漏洞影響 CSS switch 11050, 11150, 11800。
解決方法	Upgrades available: Cisco WebNS 4.0: Cisco upgrade WebNS 4.0.1 http://www.cisco.com/public/sw-center/sw-web.shtml Cisco WebNS 3.0: Cisco upgrade WebNS 3.1.0 http://www.cisco.com/public/sw-center/sw-web.shtml
參考資料	http://www.securityfocus.com/bid/2330

3.1.8. Cisco IOS HTTP Request『?/』漏洞

弱點名稱	Cisco IOS HTTP Request『?/』漏洞
受影響系統	- Cisco IOS 12.1XP, Cisco IOS 12.1XL - Cisco IOS 12.1XJ, Cisco IOS 12.1XI - Cisco IOS 12.1XH, Cisco IOS 12.1XG - Cisco IOS 12.1XF, Cisco IOS 12.1XE - Cisco IOS 12.1XD, Cisco IOS 12.1XC - Cisco IOS 12.1XB, Cisco IOS 12.1XA - Cisco IOS 12.1T, Cisco IOS 12.1EC - Cisco IOS 12.1DC, Cisco IOS 12.1DB - Cisco IOS 12.1DA, Cisco IOS 12.1AA - Cisco IOS 12.0XJ, Cisco IOS 12.0XH - Cisco IOS 12.0XE, Cisco IOS 12.0XA - Cisco IOS 12.0W5, Cisco IOS 12.0T
弱點詳述	如果一個 URL 的 request 內含有『?/』，該台跑 IOS 的 Cisco 機器可能會受到 DOS 攻擊。如果 URL 包含一個『?/』並且 enable password ，這台機器將會進入一個無限迴圈，接著這台 router 將會在 watchdog timer 過時然後接著 reload 後的兩分鐘內當機，在某些狀況下，該機器將不會 reload，且需要重新開機才能回到正常運作的狀態。 這個問題只會發生在沒有 enable password 或 password 被知悉或容易被猜中的 password，只有 Cisco 1003, 1004 1005 系列有這些問題，要測試自己的機器是否有問題，可以 log 進該台機器，然後打 show version，如果出現 Internetwork Operating System Software 或 IOS (tm)，表示該台機器便是裝 IOS，然後下列為型號搭配有問題的 IOS，包括有 ： * Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series. * Most recent versions of the LS1010 ATM switch.

	* The Catalyst 6000 if it is running IOS. * The Catalyst 2900XL LAN switch only if it is running IOS. * The Cisco DistributedDirector.
攻擊工具	Cisco_ioshttp.pl
解決方法	除了升級外，下列有幾項可以降低這項問題的傷害： *選擇及設定較難猜的密碼。 *關掉 http server 設定的功能。 *如果仍要打開 http server 管理的功能，並且不打算 patch 的話，可以利用 access list 來限制只有某些機器可以連上來管理，例如可以用下列命令來只允許 10.1.2.3 的機器連上： access-list 1 permit 10.1.2.3 ip http access-class 1 *如果該 access list 1 已經被使用了，可以再次選取 0-99 中其他數字，這些動作可以作為 access control。 另外一種方法也是利用限制的功能，在連往有問題的 HTTP server 的路徑上，設下 access control list，可以在有問題的 router 的網路卡上設下 access list 或可以在路徑上的其他 router 上設下限制，來避免這項問題。
參考資料	http://xforce.iss.net/static/5412.php

3.1.9. Cisco IOS Remote Router Crash 漏洞

弱點名稱	Cisco IOS Remote Router Crash 漏洞
受影響系統	- Classic Cisco IOS 9.1 之後 因為 IOS 9.1 版之後的數量很多所以在此沒有把所有受影響的版本列出來，但是以下提供一個方法讓您能夠檢查機器是否有受到此漏洞的影響： 1. 登入機器 2. 執行 show version 指令 Classic Cisco IOS 軟體會回應一個 "IOS" 或是 "Internetnetwork Operating System Software" 的字串，而版本是大於等於 9.1。其他不受此漏洞影響的 Cisco 機器不會有這種回應或是根本沒有 show version 的指令 。 以下是不受到此漏洞影響的 Cisco 產品： - 7xx 撥接路由器 (750, 760, 與 770 系列) . - Catalyst LAN 交換機 (除了 Catalyst 2900XL 之外) . - IGX 或 BPX 之 WAN 交換機產品 in the IGX or BPX lines . - AXIS shelf . - LS1010 或 LS2020 ATM 交換機 . - 任何 host-based 軟體 . - Cisco PIX 防火牆 . - Cisco LocalDirector . - Cisco Cache Engine .
弱點詳述	攻擊者透過 console 或 非同步 serial 連接，Telnet 連接，UNIX "r" 指令連接，LAT 連接，MOP 連接，X.29 連接，V.120 連接以及其他連接方式有可能攻擊這個漏洞 。 如果攻擊者知道 Cisco IOS 軟體的錯誤細節，他可以使該台 router 當機或者重新啟動，且不會留下 log。因為此項問題關鍵在於內部資料結構，另外其他對系統操作的細微影響，都有可能演變成某種漏洞。但是這些都需要相當的系統知識與網路工程等的專業背景，還有必須對 cisco 軟體有相當的瞭解。

解決方法	請更新系統，自從以下版本開始，之後的 IOS 不會受到此漏洞的影響： • 11.3(1), 11.3(1)ED, 11.3(1)T • 11.2(10), 11.2(9)P, 11.2(9)XA, 11.2(10)BC, 11.2(8)SA3 • 11.1(15)CA, 11.1(16), 11.1(16)IA, 11.1(16)AA, 11.1(17)CC, 11.1(17)CT • 11.0(20.3)
參考資料	http://www.cisco.com/warp/public/770/ioslogin-pub.shtml

3.1.10. Cisco IOS Software Telnet Option Handling 漏洞

弱點名稱	Cisco IOS Software Telnet Option Handling 漏洞
受影響系統	- Cisco Access Server AS5800 - Cisco Access Server AS5300 - Cisco Access Server AS5200 - Cisco AccessPath VS-3 - Cisco AccessPath TS-3 - Cisco AccessPath LS-3 - Cisco Cable Router ubr7200 - Cisco IOS 12.0.7 - Cisco IOS 12.0.6 - Cisco IOS 12.0.5 - Cisco IOS 12.0.4T, Cisco IOS 12.0.4S - Cisco IOS 12.0.4 - Cisco IOS 12.0.3T2 - Cisco IOS 12.0.2XG - Cisco IOS 12.0.2XF - Cisco IOS 12.0.2XD - Cisco IOS 12.0.2XC - Cisco IOS 12.0.2 - Cisco IOS 11.3AA - Cisco Router 7500.0 - Cisco Router 7200.0 - Cisco Router 7100.0 - Cisco Router 3660.0 - Cisco System Controller SC3640 - Cisco Voice Gateway AS5800
弱點詳述	某些版本的Cisco IOS在Telnet Environment handling code (option #36) 有問題，特別在某些選項(ENVIRON)再通過 Cisco IOS telnet Daemon 的時候，會導致IOS reload，而讓機器重新啟動，如果重複這個動作將導致DOS(denial of service)
解決方法	Cisco IOS 12.1 版之後沒有受到此漏洞的影響，有授權的使用

	者可以到 Cisco 的網站免費下載升級版。 以下是此漏洞的防禦方法整理給讀者參考： • 使用 “access-group” 控制那一些 IP 和使用者可以使用 vty 連接 。 • 關掉 Telnet 服務而使用 SSH 服務連接。設定路由器的時候，在 "line vty 0 4" 後面加 "transport input ssh"，將路由器只允許 SSH 連接，但是要在 Cisco 7200 , 7500 和 12000 系列上而使用 Cisco IOS 12.0S，12.1S，和 12.1T 版才有提供 SSH 連接的功能。 • 移除 “line” 指令，將關掉虛擬 console 的功能讓攻擊者沒有辦法從遠端登入。 現在有許多 Security scanner 或 tool 都可以檢測出這個漏洞 。
參考資料	CVE-2000-0268 http://www.cisco.com/warp/public/707/iostelnetopt-pub.shtml

3.1.11. Cisco IOS Syslog Crash

弱點名稱	Cisco IOS Syslog Crash
受影響系統	- Cisco IOS 12.0.2XD - Cisco IOS 12.0.2XC - Cisco IOS 12.0.1XE - Cisco IOS 12.0.1XB - Cisco IOS 12.0.1XA3 - Cisco IOS 12.0.1W - Cisco IOS 12.0T - Cisco IOS 12.0S - Cisco IOS 12.0DB - Cisco IOS 12.0 - Cisco IOS 11.3DB - Cisco IOS 11.3AA
弱點詳述	如果在跑 classic IOS 的 Cisco 裝置，對 syslog port 514 送出一個 UDP 封包，系統可能會當機，重新啟動，如果是當機的話可能需要手動來重新啟動，最特別的是 Nmap 已知會導致這個問題。 有執行 Classic Cisco IOS 軟體的 Cisco 產品如下: - Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx, ubr9xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx, AS53xx, AS58xx, 64xx, 70xx, 72xx (including the ubr72xx), 75xx, and 12xxx series. - Most recent versions of the LS1010 ATM switch. - Some versions of the Catalyst 2900XL LAN switch. - The Cisco DitributedDirector.
攻擊工具	Cisco_IOSsyslog.pl
解決方法	可以用拒絕對在 Cisco 機器上 syslog port (514) 的存取來避免此項問題。 這可以用 access list 或用附近的機器來過濾來達到這個方法。 可以在 Cisco Advisory 上找到更細節的資料。
參考資料	http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

3.1.12. Cisco IOS-700 Router Password Buffer Overflow

弱點名稱	Cisco IOS-700 Router Password Buffer Overflow
受影響系統	- Cisco IOS/700 4.1.2 - Cisco IOS/700 4.1.1 - Cisco IOS/700 4.1
弱點詳述	這項問題可以讓攻擊者對 7xx 系列 router 重新啟動。這將使得合法使用這在這段重新啟動期間無法正常運作。也可能造成 "call flapping" 導致 router 關機或重新啟動。 如果過長字串裡面的特定地方有某些資料的話，將會讓攻擊者獲得該台 router 的完全控制權，或讓他無限期的當機。達到此項結果的方式目前不明，成功控制該台機器的攻擊者可能是重新設定該台 router 或更改了他的某項功能。 在密碼輸入的 data buffer 因為邊界檢查沒做好可能使得輸入的密碼超過 buffer size，而覆寫掉 buffer 後面的記憶體內容，當系統試著去使用這份不正確的資料時，將有不可預期的結果發生，如果這份資料是隨意選取到，這個非預期的結果就會偵測是錯誤，像是對不合法的記憶體作存取。這是會導致當機。 但是有可能小心的設計一個字串，使得不會讓系統偵測到錯誤，卻可導致系統變成攻擊者希望的狀況。但 Cisco 工程師卻沒發現這種字串。
解決方法	可以用 filters 或 firewall 或周圍的 router 來對 telnet 來作過濾的動作，限制對 7xx router 作 telnet 的動作。只允許某台可以管理的機器去管理。可以用下列動作來設定 filter： 1. source = not trusted-ip-address 2. destination = 7xx- 3. address:23 block
參考資料	http://www.networkice.com/Advice/Intrusions/2000903/default.htm

3.1.13. Cisco 7xx Password Buffer Overflow 漏洞

弱點名稱	Cisco 7xx Password Buffer Overflow 漏洞
受影響系統	- Cisco 7xx routers with IOS/700 software version 4.1(1), 4.1(2), or 4.1 interim releases earlier than 4.1(2.1)
弱點詳述	在密碼輸入的 data buffer 因為邊界檢查沒做好可能使得輸入的密碼超過 buffer size，而覆寫掉 buffer 後面的記憶體內容，當系統試著去使用這份不正確的資料時，將有不可預期的結果發生，如果這份資料是隨意選取到，這個非預期的結果就會偵測是錯誤，像是對不合法的記憶體作存取。這是會導致當機。 但是有可能小心的設計一個字串，使得不會讓系統偵測到錯誤，卻可導致系統變成攻擊者希望的狀況。
解決方法	可以用 filters 或 firewall 或周圍的 router 來對 telnet 來作過濾的動作，限制對 7xx router 作 telnet 的動作。只允許某台可以管理的機器去管理。 可以用下列動作來設定 filter。 set ip filter tcp in source = not trusted-ip-address destination = 7xx- address:23 block
參考資料	http://www.cisco.com/warp/public/770/pwbuf-pub.shtml

3.1.14. Cisco TAC+ DOS 漏洞

弱點名稱	Cisco TAC+ DOS 漏洞
受影響系統	- Cisco tac_plus 4.0.3alpha - Cisco tac_plus 4.0.2alpha
弱點詳述	在 Tacacs+ server 的實作上有 small buffer overrun，Tacas+ server 是 Cisco 發佈的，當 buffer overrun 後似乎不算各 exploit ，相關弱點是如果有攻擊者讓該 tac_plus server 去 malloc 一塊大的記憶體位址，可能會造成 DOS。 當 Tacacs+ protocol 的分析公布在 Bugtraq 時指出，clients (包含 IOS)都受到上述問題影響。但 Cisco 宣稱 IOS clients 將會 reject 掉封包，並且回報錯誤，不會有更深入的問題。攻擊 client 需要計算到 TCP sequence ，所以很難達到。 最早的問題，buffer overflow，起因在於 tac_plus server 為進入的封包分配記憶體，他只會在 primary read 讀取到在 header 長度，分配 header 裡指出的記憶體，將 header 拷貝到分配好的記憶體中，然後再讀出，拷貝剩下的 buffer 到裡面。Buffer overrun 發生的原因是，當 header 的 length 欄位加入到 header 長度時，檢查整數溢位發生錯誤。這導致了 11 bytes 溢位 第二個是因為 length field sanity checking 的問題，可以對 body length 送出任意大的數，不管多長，server 或 client 將會 malloc，這將導致分配超過記憶體總數，而發生 DOS。
解決方法	請至下列網址下載新版本，F4.0.4 alpha，或 patch 系統： http://www.stanford.edu/~bbense/tac_plus/
參考資料	http://www.securityfocus.com/bid/1294

3.1.15. Cisco IOS HTTP %% 漏洞

弱點名稱	Cisco IOS HTTP %% 漏洞
受影響系統	- Cisco IOS 12.0.7, Cisco IOS 12.0.6, Cisco IOS 12.0.5 - Cisco IOS 12.0.4T, Cisco IOS 12.0.4S, Cisco IOS 12.0.4 - Cisco IOS 12.0.3T2 - Cisco IOS 12.0.2XG, Cisco IOS 12.0.2XF, Cisco IOS 12.0.2XD. Cisco IOS 12.0.2XC - Cisco IOS 12.0.2 - Cisco IOS 12.0.1XE, Cisco IOS 12.0.1XB, Cisco IOS 12.0.1XA3, Cisco IOS 12.0.1W - Cisco IOS 12.0T, Cisco IOS 12.0S, Cisco IOS 12.0DB - Cisco IOS 12.0(9)S, Cisco IOS 12.0(8), Cisco IOS 12.0(7)T, Cisco IOS 12.0(5)T1 - Cisco IOS 12.0 - Cisco IOS 11.3.1T, Cisco IOS 11.3.1ED, Cisco IOS 11.3.1, Cisco IOS 11.3T - Cisco IOS 11.3 - Cisco IOS 11.2.9XA, Cisco IOS 11.2.9P, Cisco IOS 11.2.8P - Cisco IOS 11.2.8 - Cisco IOS 11.2.4F1, Cisco IOS 11.2.10BC - Cisco IOS 11.2.10 - Cisco IOS 11.2P, Cisco IOS 11.2(17), Cisco IOS 11.2, Cisco IOS 11.1
弱點詳述	受到影響的 router，如果該 router 的 IOS 中設定中，設定了讓一台 web server 運作，譬如像下列 IOS 命令 ip http server 但是如果該機器收到一個 request http://<router-ip>/%% 此時就會導致此台 router 當掉，甚至有些機器會自動重新開機，導致需要重送一些封包。
攻擊工具	cisco_ioshttp2.pl
解決方法	此項問題已經有 patch。在 IOS 上關掉該 web service，加上

	ACL’s 使得只有特定的機器可以連到該 port。可以在 IOS 下打入： no ip http server 並且 save 來關掉此 web service.
參考資料	CVE-2000-0380

Can Access Restricted Resource（非法存取）

3.1.16. Cisco Catalyst 3500XL Remote Arbitrary Command Execution 漏洞

弱點名稱	Cisco Catalyst 3500XL Remote Arbitrary Command Execution 漏洞
受影響系統	- Cisco Catalyst 3500 XL
弱點詳述	Cisco Catalyst 3500 XL 是一個 LAN 上使用的高速 switch 裝置。 但是有一個漏洞，在 webserver 的設定介面上，可以使得任意使用者執行命令。一個包含/exec ＋已知的檔名 的 http request 可以顯示該檔的內容。 更甚者，這個漏洞甚至允許使用者執行任意 code。 這個漏洞可以完全取得該台機器的使用權限。 Example: http://target/exec/show/config/cr This URL will disclose the user password configuration file.
解決方法	關掉 Web Configuration 。 目前 Cisco 還沒有推出修補版本。
參考資料	CVE-2000-0945 http://xforce.iss.net/static/5415.php http://www.securityfocus.com/archive/1/141471

3.1.17. Cisco Content Switch Directory Structure File Reading 漏洞

弱點名稱	Cisco Content Switch Directory Structure File Reading 漏洞
受影響系統	- Cisco WebNS 4.0.1 - Cisco WebNS 4.0 - Cisco WebNS 3.1 - Cisco WebNS 3.0
弱點詳述	Cisco Content Services (CSS) 是設計用來對使用 Cisco Web Network Services (Web NS)提供強化 e-commerce web service、Web Content delivery，CSS switch 是 Cisco 公司所發佈的。 WebNS software 可能導致 local user 取得受保護的資源。CSS switch 允許使用者獲取該 switch 上某些功能，可以藉由加強 access control 來避免某些人讀取或更動 switch 上的設定。因為對 input 上的處理，使得某使用者有可能經由執行某個不存在的檔名，獲取到檔案目錄結構，一旦檔案目錄結構獲悉，就有可能讀取到該目錄下的檔案。 這項弱點使得惡意的使用者可以得知目錄結構，且可以讀取檔案。
參考資料	CVE-2001-0020 http://www.securityfocus.com/bid/2331 http://www.safermag.com/html/safer34/alerts/64.html

3.1.18. Cisco Router Online Help 漏洞

弱點名稱	Cisco Router Online Help 漏洞
受影響系統	- Cisco IOS 9.14 - Cisco IOS 12.0.7, Cisco IOS 12.0.6, Cisco IOS 12.0.5 - Cisco IOS 12.0.4T, Cisco IOS 12.0.4S, Cisco IOS 12.0.4 - Cisco IOS 12.0.3T2 - Cisco IOS 12.0.2XG, Cisco IOS 12.0.2XF, Cisco IOS 12.0.2XD, Cisco IOS 12.0.2XC - Cisco IOS 12.0.2 - Cisco IOS 12.0.1XE, Cisco IOS 12.0.1XB, Cisco IOS 12.0.1XA3, Cisco IOS 12.0.1W - Cisco IOS 12.0T, Cisco IOS 12.0S, Cisco IOS 12.0DB - Cisco IOS 12.0(9)S, Cisco IOS 12.0(8), Cisco IOS 12.0(7)T, Cisco IOS 12.0(5)T1 - Cisco IOS 12.0 - Cisco IOS 11.2.9XA, Cisco IOS 11.2.9P - Cisco IOS 11.2.8SA5, Cisco IOS 11.2.8SA3, Cisco IOS 11.2.8SA1, Cisco IOS 11.2.8P - Cisco IOS 11.2.8 - Cisco IOS 11.2.4F1 - Cisco IOS 11.2.10BC, Cisco IOS 11.2.10 - Cisco IOS 11.2P, Cisco IOS 11.2(17), Cisco IOS 11.2 - Cisco IOS 11.1.17CT, Cisco IOS 11.1.17CC, Cisco IOS 11.1.16IA, Cisco IOS 11.1.16AA - Cisco IOS 11.1.16, Cisco IOS 11.1.15CA, Cisco IOS 11.1.13IA, Cisco IOS 11.1.13CA - Cisco IOS 11.1.13AA, Cisco IOS 11.1.13 - Cisco IOS 11.1 - Cisco Router 7500.0, Cisco Router 7200.0, Cisco Router 4000.0 - Cisco Router 3600.0, Cisco Router 2600.0, Cisco Router 2500.0
弱點詳述	某些 IOS multiple Cisco router 在他們的 online help 系統上，有資訊外流的危險。基本上，這個問題可以讓在該台機器

	只有低權限的使用者，可以使用這個 help system。但是這個功能只開放給有' enabled ' user。Access list 這項資訊還是需由其他項目找出，該 help system 本身並沒有列出這些項目(使用 show 命令)。
解決方法	-將 default 權限的 access lines 設定為 0 (預設為 1) -使用"privilege exec"，指定 level 0 的 user 只能執行某些命令。
參考資料	CAN-2000-0345 http://www.securityfocus.com/bid/1161 http://www.safermag.com/html/safer25/alerts/60.html

View or Modify Configuration (偷閱或更改系統設定)

3.1.19. Cisco Aironet Web Administration Access 漏洞

弱點名稱	Cisco Aironet Web Administration Access 漏洞
受影響系統	- Cisco Aironet Firmware 8.24 - Cisco Aironet Firmware 7.0.x - Cisco Aironet Firmware 8.07
弱點詳述	Aironet Wireless Bridges 是 Cisco 的產品，提供無線與有線部分的連接。 此漏洞是出現在韌體上，遠端使用者將有可能調整或察看設定，就算該機器的 Web 管理介面是關掉的。且不管是從無線或有線網路端。 因此惡意的使用者將可從遠端察看設定或調整此機器的設定。
解決方法	Updates available: Cisco Aironet Firmware 8.24: Cisco upgrade Cisco Aironet Firmware 8.55 ftp://ftp.cisco.com/pub/wireless/aironet Cisco Aironet Firmware 7.0.x: Cisco upgrade Cisco Aironet Firmware 8.55 ftp://ftp.cisco.com/pub/wireless/aironet Cisco Aironet Firmware 8.07: Cisco upgrade Cisco Aironet Firmware 8.55 ftp://ftp.cisco.com/pub/wireless/aironet
參考資料	CVE-2001-0455 http://www.securityfocus.com/bid/2461 http://www.safermag.com/html/safer35/alerts/33.html

3.1.20. Cisco IOS ILMI SNMP Community String 漏洞

弱點名稱	Cisco IOS ILMI SNMP Community String 漏洞
受影響系統	- Cisco IOS 12.0XV, Cisco IOS 12.0XS, Cisco IOS 12.0XR, Cisco IOS 12.0XQ - Cisco IOS 12.0XM, Cisco IOS 12.0XL, Cisco IOS 12.0XK, Cisco IOS 12.0XJ - Cisco IOS 12.0XI, Cisco IOS 12.0XH, Cisco IOS 12.0XG, Cisco IOS 12.0XF - Cisco IOS 12.0XE, Cisco IOS 12.0XD, Cisco IOS 12.0XC, Cisco IOS 12.0XB - Cisco IOS 12.0XA, Cisco IOS 12.0WT, Cisco IOS 12.0W5, Cisco IOS 12.0T - Cisco IOS 12.0SX, Cisco IOS 12.0ST, Cisco IOS 12.0SL, Cisco IOS 12.0SC - Cisco IOS 12.0S, Cisco IOS 12.0DC, Cisco IOS 12.0DB, Cisco IOS 12.0DA - Cisco IOS 12.0 - Cisco IOS 11.3WA4, Cisco IOS 11.3T - Cisco IOS 11.3NA, Cisco IOS 11.3MA - Cisco IOS 11.3DB, Cisco IOS 11.3DA - Cisco IOS 11.3AA, Cisco IOS 11.3(2)XA - Cisco IOS 11.3, Cisco IOS 11.2WA3 - Cisco IOS 11.2SA, Cisco IOS 11.2P - Cisco IOS 11.2GS, Cisco IOS 11.2BC - Cisco IOS 11.2(9)XA, Cisco IOS 11.2(4)XA - Cisco IOS 11.1IA, Cisco IOS 11.1CT - Cisco IOS 11.1CC, Cisco IOS 11.1CA - Cisco IOS 11.1AA, Cisco IOS 11.1 - Cisco IOS 11.0
弱點詳述	IOS 是 Cisco 公司針對 Cisco 網路裝置設計的作業系統。 問題發生在版本 IOS 11.x 和 12.0 可能使得沒有經過授權就可以修改某些設定參數。 ILMI SNMP Community 字串允許對 MIB-II community group 的

	system object 做存取的動作。就算更動了這些設定參數，也不會影響機器的正常運作。這類的攻擊可能導致社交工程攻擊(social engineering attack)。 惡意的遠端使用者可以更動MIB-II Community object設定。將系統更名，改變系統的location name，或改變系統的聯絡資訊。這項問題只影響某些機器而已。
解決方法	修補版本如下： Cisco IOS 11.0: Cisco Upgrade IOS 11.0(22a) Cisco IOS 11.1CT: Cisco Upgrade IOS 12.0(11)ST2 Cisco IOS 11.1CC: Cisco Upgrade IOS 11.1(36)CC1 Cisco IOS 11.1CA: Cisco Upgrade IOS 11.1(36)CA1 Cisco IOS 11.1AA: Cisco Upgrade IOS 12.1(7) Cisco IOS 11.1: Cisco Upgrade IOS 11.1(24a) Cisco IOS 11.2WA3: Cisco Upgrade IOS 12.0(10)W(18b) Cisco Upgrade IOS 12.0(13)W5(19b) Cisco IOS 11.2SA: Cisco Upgrade IOS 12.0(5)WC Cisco IOS 11.2P: Cisco Upgrade IOS 11.2(25a)P Cisco IOS 11.2GS: Cisco Upgrade IOS 12.0(15)S1 Cisco IOS 11.2BC: Cisco Upgrade IOS 12.1(7) Cisco IOS 11.2(9)XA: Cisco Upgrade IOS 11.2(9)XA1 Cisco IOS 11.2(4)XA: Cisco Upgrade IOS 11.2(25a)P Cisco IOS 11.3WA4: Cisco Upgrade IOS 12.0(10)W(18b) Cisco Upgrade IOS 12.0(13)W5(19b) Cisco IOS 11.3T: Cisco Upgrade IOS 11.3(11b)T1 Cisco IOS 11.3NA: Cisco Upgrade IOS 12.1(7) Cisco IOS 11.3MA: Cisco Upgrade IOS 11.3(1)MA8 Cisco IOS 11.3DB: Cisco Upgrade IOS 12.1(4)DB1 Cisco IOS 11.3DA: Cisco Upgrade IOS 12.1(5)DA1 Cisco IOS 11.3AA: Cisco Upgrade IOS 11.3(11a)AA Cisco IOS 11.3(2)XA: Cisco Upgrade IOS 11.3(11b)T1 Cisco IOS 11.3: Cisco Upgrade IOS 11.3(11b) Cisco IOS 12.0XV: Cisco Upgrade IOS 12.1(5)T5 Cisco IOS 12.0XS: Cisco Upgrade IOS 12.1(5c)E8 Cisco IOS 12.0XR: Cisco Upgrade IOS 12.1(5)T5 Cisco IOS 12.0XQ: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XM: Cisco Upgrade IOS 12.1(7)

	Cisco IOS 12.0XL: Cisco Upgrade IOS 12.1(5)T5 Cisco IOS 12.0XK: Cisco Upgrade IOS 12.0(7)XK4 Cisco IOS 12.0XJ: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XI: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XH: Cisco Upgrade IOS 12.0(4)XH5 Cisco IOS 12.0XG: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XF: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XE: Cisco Upgrade IOS 12.0(4)XH5 Cisco Upgrade IOS 12.1(5c)E8 Cisco IOS 12.0XD: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XC: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XB: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0XA: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0WT: Cisco Upgrade IOS 12.0(13)WT6(1) Cisco IOS 12.0W5: Cisco Upgrade IOS 12.0(10)W5(18f) Cisco Upgrade IOS 12.0(10)W5(18) Cisco Upgrade IOS 12.0(13)W5(19) Cisco Upgrade IOS 12.0(13)W5(19c) Cisco Upgrade IOS 12.0(10)W5(18e) Cisco IOS 12.0T: Cisco Upgrade IOS 12.1(7) Cisco IOS 12.0SX: Cisco Upgrade IOS 12.1(5c)E8 Cisco IOS 12.0ST and Cisco IOS 12.0SL: Cisco Upgrade IOS 12.0(14)SL1 Cisco Upgrade IOS 12.1(5c)E8 Cisco IOS 12.0SC: Cisco Upgrade IOS 12.0(15)SC1 Cisco IOS 12.0S: Cisco Upgrade IOS 12.0(15)SC1 Cisco IOS 12.0DC: Cisco Upgrade IOS 12.1(4)DC2 Cisco IOS 12.0DB: Cisco Upgrade IOS 12.1(4)DC2 Cisco IOS 12.0DA and Cisco IOS 12.0: Cisco Upgrade IOS 12.0(8) Cisco Upgrade IOS 12.0(16)
參考資料	CAN-2001-0711 http://www.securityfocus.com/bid/2427 http://www.safermag.com/html/safer35/alerts/54.html

3.1.21. Cisco PIX Passive Mode FTP Internal Address Disclosure 漏洞

弱點名稱	Cisco PIX Passive Mode FTP Internal Address Disclosure 漏洞
受影響系統	- Cisco PIX Firewall 5.0(3) - Cisco PIX Firewall 4.2(5) - Cisco PIX Firewall 4.2(4)
弱點詳述	Cisco PIX 是 Cisco 公司的 firewall 產品。 可能發生的狀況是：可以藉由連到 PIX，更動 PIX 的設定來隱藏內部 ftp server 的 IP address，藉由在『一次的 ftp session 送出數次的 PASV』，IP address 最後還是會被發現。目前這個問題還不知道會造成什麼影響。
解決方法	上述漏洞主要是因為 "fixup protocol ftp [protnum]" 指令 。請輸入 "no fixup protocol ftp" ，將把 PIX 上的 fixup FTP protocol 的功能關掉 。"fixup protocol ftp 21" 指令是一個 Cisco Secure PIX Firewall 的預設值 。 上述的做法將會強迫 client 端使用 FTP passive 模式，而不提供 inbound FTP 服務。 關掉 "fixup protocol ftp 21" 功能將影響 Outbond FTP 不能夠正常運作，不過 passive FTP 正確運作 。 Cisco PIX Firewal 5.1(1) 版沒有受到此漏洞的影響。
參考資料	http://www.netsys.com/firewalls/firewalls-2000-03/msg00472.html

Flaw of the Implementation or specification（實作或規格上的缺失）

3.1.22. Cisco Catalyst 2900 VLAN 漏洞

弱點名稱	Cisco Catalyst 2900 VLAN 漏洞
受影響系統	- Cisco Catalyst WS-C2924M-XL - Cisco IOS 11.2.8SA5
弱點詳述	這是 802.1q 規格的設計缺陷，當應用在 Cisco Catalyst switches 的 VLAN 上。 VLAN 技術常用來在現有實體 Switch 的 LAN 網路中再建立虛擬的 LAN（VLAN），每個 Switch 的 port 可以再分配給一個 VLAN，在 Cisco Catalyst 中，VLAN 是實作在 OSI 的第二層，所以 VLAN 的資訊是可以通過任何 layer 3 的設備（譬如路由器）。除了上述以外，VLANs 除了使用在單一 switch 外，也可以使用在串接（trunk）起來的 switch 上，為了維持 VLAN 在此 trunk 架構上的必要資訊，ethernet frame 會被 trunking protocol 包起來，而 Cisco 使用自己的獨有 trunking protocol ，但是他們仍繼續支援新的 802.1q 標準，而我們是使用 802.1q 的 trunking 來測試。 基本上，802.1q 在 ethernet frame 上增加了一個 tag，來表示 frame 屬哪個 VLAN ，因此當框架在 switches 間傳遞時，接到的 switch 將可以正確的將此 frame 傳到正確的 VLAN 裡，在 Cisco 802.1q 的實作上，是用 4 bytes 的長度以及"0x 80 00 0n nn"的格式，其中 nnn 是 VLAN 的辨識子，tag 直接插入 ethernet frame 的 source MAC address 之後，例如一個屬於 VLAN4 的 ethernet frame 進入 switch 將有以下 tag "80 00 00 04" 。802.1q frame 在 switch trunk 間遊歷，然後等到達目標 switch port 才被剝掉這個 tag。 在我們的測試中，我們使用 Sniffer Pro v2 來產生具修正過 VLAN identifiers 的 802.1q frame，試著去取得數各 VLAN 之間的 frame。 我們發現在特定的情況下，是可以在其中一個 VLAN 中注入 frame 然後讓他 hop 到另外一個 VLAN 裡，這是一個蠻嚴重的考

	量，如果這個 VLAN 有 security 上的考量的話。這個問題 Cisco 也注意到，我們認為這有各問題可能出在 802.1q 規格上而不是出在這個 VLAN 的實作上。 與其他 ports 分開的那個 trunk port，必須指派給一個 VLAN 區域，如果某些 switch 上的 non-trunk ports 與 trunk port 共同使用某個 VLAN，那有可能導致用一個修改過的 802.1q 框架注入這些 non-trunk ports，然後使得這些框架跨到其他的 switch 上的 VLAN。 例如，VLAN1 用 switch 1 上的 ports 1-12 ，VLAN2 用 switch1 上 的 ports 13-23，然後用 port 24 來作為 trunk port，與 switch 2 串接起來，再來用 switch 2 上的 1-12 再用來作為 VLAN 1 使用 ，13-23 用來給 VLAN2 來使用，然後同樣用 port24 與 switch 1 串接。機器 1 安裝在 switch 1 的 port 1 ，機器 2 安裝在 switch2 的 port 13。 我們可以用下列格式發出 802.1q 框架 Source MAC =Machine 1 Destination MAC = Machine 2 VLAN ID = VLAN 2 ... 這個框架從機器 1 發出，然後會到達機器 2。 這個會造成下列問題： 1. 攻擊者可以藉由這個問題進入其他 VLAN。 2. 可以進入另外一個串接的 switch。 3. 攻擊者可以知道目標機器的 MAC address。
解決方法	如果要採用較高的安全策略，就不要使用這個 VLAN 機制。因為 VLAN 雖然可以是一個切割網路區段的方式，可以減低廣播和碰撞，但是並不是用來作為網路安全的工具。 如果非要使用 VLAN 機制，要確定 trunking ports 要使用唯一的 VLAN 號碼。
參考資料	CAN-1999-1129 http://www.securityfocus.com/bid/615 http://www.safermag.com/html/safer17/alerts/46.html

3.1.23. Cisco IOS TCP Initial Sequence Number 漏洞

弱點名稱	Cisco IOS TCP Initial Sequence Number 漏洞
受影響系統	- Cisco 路由器 800, 1000, 1005, 1400, 1600, 1700, 2500, 2600, 3600, MC3810, 4000, 4500, 4700, 6200, 6400 NRP, 6400 NSP 系列 - ubr900 and ubr920 universal 寬頻路由器 - Catalyst 2900 ATM, 2900XL, 2948g, 3500XL, 4232, 4840g, 5000 RSFC 交換機系列 - Access 伺服器 5200, 5300, 5800 系列 - Catalyst 6000 MSM, 6000 Hybrid Mode, 6000 Native Mode, 6000 Supervisor Module, Catalyst ATM Blade - Cisco 路由器 RSM, 7000, 7010, 7100, 7200, ubr7200, 7500, 10000 ESR, and 12000 GSR 系列 - DistributedDirector - Catalyst 8510CSR, 8510MSR, 8540CSR, 8540MSR 交換機系列
弱點詳述	為了達到資料傳送的可靠性，Transmission Control Protocol (TCP) 使用一連串數字叫作 TCP Sequence numbers，讓對方主機在受到資料的時候將會判斷資料的順序，使用此方法對方也可以通知送封包者，那一些封包已被對方收到。 TCP sequence numbers 是一個 32-bit 整數一直由 0 至 4,294,967,295 循環．兩個終端的主機一開始會互相交換 Initial Sequence Number (ISN)，ISN 使用隨機的方式取得。交換成功之後才開始從那個 ISN 送資料，之後 Sequence Number 一直加以至送完為止。為了避免封包重的時候組發生複製或遺失的狀況，每個主機擁有一個 window，Squence Number 接近的範圍，近來的封包要落在 window 裡面才能被收到。當送來的封包有正確的來源 IP 和目的地 IP，正確的來源通信埠和目的地通信埠，與正確的 Sequence Number 的時候，接收端將接受此封包。 此方法理論上是一個非常好的保護方法，但是為了保護

	不友善的使用 ， 它不應該讓攻擊者有可能猜想在溝通中的 Sequence Number 。 若當初 ISN 沒有使用隨機過程來選擇或是若在雙方溝通之間增加 Sequence Number 的時候使用非隨機過程，那時攻擊者有可能偽造溝通中的 sequence number ， 導致攻擊者可以竊聽或是強制在溝通中的連結 。 為了避免這種攻擊方法 ISN 必須使用隨機過程送出來的 。 某些 Cisco 機器在產生 ISN 的過程不夠隨機，所以有可能被不友善的人攻擊到 。
解決方法	更新您的 IOS ， 由於更新版有很多種 ， 請直接到 Cisco 網站查詢與下載： http://www.cisco.com/
參考資料	CVE-2001-0288 http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml

3.1.24. Cisco Web Cache Control Protocol Router 漏洞

弱點名稱	Cisco Web Cache Control Protocol Router 漏洞
受影響系統	- Cisco IOS 11.2(P) - Cisco IOS 11.2(10)P - Cisco IOS 11.1(14)CA - Cisco IOS 11.1 - Cisco IOS 11.1CC
弱點詳述	Cisco Cache Engine 產品對使用 HTTP 瀏覽網頁時，提供一個 transparent caching 的機制。Cache Engine 使用 Cisco 專屬的 Web Cache Control Protocol (WCCP)來與設定好的 Cisco router 溝通，且形成一個 Cache service 服務提供者，這台 router 會將 HTTP traffic 轉到 Cache Engine 去。 雖然這些過程預設並不是打開的，而且使用者需要特別設定才打開 WCCP，但是 WCCP 本身並沒有認證機制。任何經過設定後，支援 Cache Engines 的 router 將會視每一個送出合法的 WCCP hello 封包的主機為一個 cache engine，且會將 HTTP 轉向該主機，這有可能使得惡意的使用者將 Web traffic 轉向而經過這樣的 router，雖然這各惡意使用者並沒有實際經過或設定要經過該 router。 這個攻擊可以使用 access lists 來避免 WCCP traffic 從非信任的主機到達這台 router，Cisco 在以後的版本將會使用 hash-based 的認證機制來改善 WCCP 的這項缺失。
解決方法	WCCP 是跑在 UDP port 2048。可以在有跑 WCCP 的 router 藉由檔掉非經過授權，目標是 port2048 的 UDP traffic。這可以防止攻擊者送 WCCP traffic 到該 router ，並轉送正確的 traffic。較為恰當的是擋掉所有目標是 port 2048，像是所有這台 router 會聽到的廣播封包或 multicast 封包。可以在該台跑 WCCP 的 router 上，經由設定 inbound access list 或用 access list 或其他過濾機制。
參考資料	CAN-1999-1175

	http://www.ciac.org/ciac/bulletins/i-054.shtml http://bugtraq.inet-one.com/dir.1998-05/msg00143.html http://www.codetalker.com/advisories/misc/cisco980513.html http://cert.uni-stuttgart.de/archive/win-sec-ssc/1998/05/msg00007.html http://www.cisco.com/warp/public/770/wccpauth-pub.shtml

3.1.25. Cisco CVCO-4k Remote Username and Password Retrieval 漏洞

弱點名稱	Cisco CVCO-4k Remote Username and Password Retrieval 漏洞
受影響系統	- Cisco Virtual Central Office 4000 (VCO/4K) 5.1.3 或更早的版本
弱點詳述	這台機型上的 SNMP 管理介面上面的使用者與密碼是用簡單的 substitution cipher 來加密的，很容易就被破解，若被破解密碼，攻擊者將會取得許多有效的使用者名稱與密碼，若取得較高得權限將導致系統安全。
解決方法	如果不需要 SNMP，就將此項服務關掉，若需要此項服務，請務必設定較為難猜的密碼。 請升級到： Cisco Virtual Central Office 4000 (VCO/4K) 5.1.4
攻擊工具	cisco_CVCO_4k.pl
參考資料	CAN-2000-0955 http://www.nipc.gov/cybernotes/2000/cyberissue2000-22.pdf http://www.securityfocus.com/bid/1885 http://xforce.iss.net/static/5425.php

Lost Access Control (Access Control 失效)

3.1.26. Cisco Catalyst Enable Password Bypass 漏洞

弱點名稱	Cisco Catalyst Enable Password Bypass 漏洞
受影響系統	- Cisco Catalyst 4000 5.4.1 - Cisco Catalyst 5000 5.4.1 - Cisco Catalyst 5500 5.4.1 - Cisco Catalyst 6000 5.4.1 - Cisco Catalyst 6500 5.4.1
弱點詳述	在某些版本的 Cisco Catalyst，一個已經可以 access 該裝置的使用者可以提升目前的權限到 'enable mode' 而不必打密碼。一旦 enable mode 取得，此用者可以進入 configuration mode 並且交付沒經過授權的設定或改變。 這個漏洞可以由 local 端或遠端 telnet 達成。
解決方法	請至 cisco 網站升級新版本。嚴格限制 telnet 連接也會防禦對此漏洞的攻擊 。 請參考以下步驟限制 telnet 連接： set ip permit <address> <mask> telnet set ip permit enable 此指令將拒絕所有沒有在 permit 裡面的連接地址。
攻擊工具	請使用 telnet client 程式進行上述攻擊方法
參考資料	CVE-2000-0267 http://www.securiteam.com/securitynews/5VQ0B000GO.html http://www.safermag.com/html/safer24/advisories/09.html http://www.cisco.com/warp/public/707/catos-enable-bypass-pub.shtml http://www.ciac.org/ciac/bulletins/k-034.shtml

3.1.27. Cisco Gigabit Switch Router ACL Bypass 漏洞

弱點名稱	Cisco Gigabit Switch Router ACL Bypass 漏洞
受影響系統	- Cisco Gigabit Switch Router 12016 - Cisco Gigabit Switch Router 12012 - Cisco Gigabit Switch Router 12008 - Cisco IOS 12.1 , Cisco IOS 12.0.7 , Cisco IOS 12.0.6 - - Cisco IOS 12.0.5 - Cisco IOS 12.0.4 - Cisco IOS 12.0.3 - Cisco IOS 12.0.2 - Cisco IOS 12.0.1 - Cisco IOS 12.0 - Cisco IOS 11.3.1 - Cisco IOS 11.3 - Cisco IOS 11.2.8 - Cisco IOS 11.2.10 - Cisco IOS 11.2P - Cisco IOS 11.2
弱點詳述	Cisco Gigabit Switch Routers (GSRs)，與設定過的 Fast Ethernet/Gigabit Ethernet 網路卡一起使用，將會根據 ACLs 規則來轉遞流量，這次的弱點可能就因為 ACLs 限制不了而產生的漏洞。攻擊者可能可以藉由利用某個 target GSR interface 來讓其停止轉遞封包，導致 DOS，然後剩下的 ACLs 就為了最佳化就必須出現在受影響的網路介面上，這項弱點僅存在於當 Fast Ethernet/Gigabit Ethernet network interface cards 與 Gigabit Switch Routers 一起使用，即此為受影響的介面。 GSRs 上所有高于 11.2 的 IOS 都確定有此問題。
解決方法	請升級您的 IOS 到下列版本： * CISCO IOS 11.2(19)GS0.2 * CISCO IOS 12.0(8.0.2)S * CISCO IOS 12.0(7)S1 * CISCO IOS 12.0(7.4)S * CISCO IOS 12.0(8.3)SC

	* CISCO IOS 12.0(7)SC
參考資料	CVE-2000-0700 http://www.safermag.com/html/safer28/advisories/85.html http://www.securityfocus.com/bid/1541 http://www.nipc.gov/cybernotes/2000/cyberissue2000-16.pdf

3.1.28. Cisco IOS CHAP Authentication 漏洞

弱點名稱	Cisco IOS CHAP Authentication 漏洞
受影響系統	- Cisco IOS 9.1 - Cisco IOS 11.2P - Cisco IOS 11.2 - Cisco IOS 11.1 - Cisco IOS 11.0 - Cisco IOS 10.3 - Cisco IOS/700 4.1
弱點詳述	這份資料出於Cisco advisory，"classic" cisco IOS 軟體版本(使用在Cisco non-switch 產品的軟體，及AGS/AGS+/CGS/MGS, CS-500 產品編號大於或等於1000，但是不包含Catalyst switches 或7xx 9xx 系列router，在PPP CHAP 認證上有個嚴重的安全上的漏洞。這項漏洞可使得有技術與知識的攻擊者可以避掉CHAP 認證，其他PPP 認證方法則不受影響。 相關的弱點存在於Cisco IOS/700 軟體(the software used on 7xx routers). 一個經驗老到的程式設計師可以建起一個unauthorized PPP connection 到一個受影響的系統上，因為受CHAP 認證，可以由下列專業知識取得某些權力。 - 瞭解這項問題的細節。 - 對PPP/CHAP implementation source code 有修改的能力。 - 知悉欲攻擊網路的設定。 用簡單的沒有變更過，或適當的PPP/CHAP 實作無法利用此項弱點，攻擊者必須修改過軟體才有辦法利用此項弱點。
解決方法	將IOS 軟體更新為不受影響的版本。 IOS/700 可以藉由下列設定防止 -避免router 對任何連進來的連線做認證，也許可以改變ISDN switch 設定，或relying on callerID 及使用 callerid set , callidreceive set 命令。 -Router 要避免接受『認證自己的calls』，可以使用ppp secret

	client 命令來設定 CHAP secret，可選一個隨機的" garbage" 值。 - 對 router 兩端設定不同的 CHAP secret，這可以使用 ppp secret clent 還有 ppp secret host 命令，注意這個方式無法在 7xx 系列上使用，因為這類 classic Cisco IOS 並不支援非對稱的 CHAP secret。 上述任一項作法可以解決此問題。
參考資料	CVE-1999-0160 http://www.cisco.com/warp/public/770/chapvuln-pub.shtml http://www.ciac.org/ciac/bulletins/i-002a.shtml

3.1.29. Cisco IOS Extended Access List Failure 漏洞

弱點名稱	Cisco IOS Extended Access List Failure 漏洞
受影響系統	- Cisco IOS 12.1(4)
弱點詳述	在有些 IOS 12.x 版本，某些在 extended access control lists 中的 rules 將不會被執行，這將使得攻擊者可以藉此進入受影響的 network services 。 目前這個問題的原因尚不清楚。
解決方法	請升級您的系統到下面版本： - Cisco IOS 12.0.7(T) - Cisco IOS 12.1(2)E1
參考資料	http://www.securityfocus.com/bid/1880 http://www.safermag.com/html/safer30/alerts/22.html

3.1.30. Cisco IOS Software Input Access List Leakage with NAT

弱點名稱	Cisco IOS Software Input Access List Leakage with NAT
受影響系統	- Cisco IOS 12.0.2XG, Cisco IOS 12.0.2XF - Cisco IOS 12.0.2XD - Cisco IOS 12.0.2XC - Cisco IOS 12.0.1XE, Cisco IOS 12.0.1XB - Cisco IOS 12.0.1XA3 - Cisco IOS 12.0.1W - Cisco IOS 12.0T - Cisco IOS 12.0S - Cisco IOS 12.0DB - Cisco IOS 12.0
弱點詳述	一堆相關的軟體bugs對NAT，還有某些跑12.0 IOS為基礎版本的Cisco routerinput access list 的處理過程，導致非預期的影響。(包含12.0,12.0S 和12.0T和所有以上版本，但是不包含12.0(4),12(4)S和12.0(4)T，就像其他12.0 releases)，非12.0的release 不受影響。 這將導致input access list filter在某些NAT 設定時漏掉部分封包，這將導致某些安全上疑慮。而沒有NAT設定的機器將不會受此漏洞影響。 個影響有很多，決定於裝置類型，設定，及環境，漏掉的封包可能為偶爾遺失或經常遺失某類型的封包。這個問題發生的設定環境相當複雜，很難去描述，但是基本上這些有問題的設定都受到某種程度的影響。擁有受影響機器的客戶最好確信這些漏洞會影響他們的網路不管何時在他們的12.0 - based 版本的NAT 使用input access lists 。 這個漏洞可以使得某些使用者避開安全過濾機制，像是一些安全政策。某些使用者可以不花特別的功夫，便對這個過濾機制視同無物。不需要任何特別的工具，技巧或知識。在某些設定，攻擊者甚至可以小心的建立起這個環境，來達到這個漏洞。但是需要一些細部的知識及相當老練的技巧。這個問題的情況可能會很頻繁的發生且在某些產品設定持續一陣子。

解決方法	此項問題可以經由更改設定來避免使用 input access list 來解決，拿掉 NAT 的設定。或者使用分開的機器或分開的介面卡來使用 NAT 和 過濾封包的功能。這些更動都牽涉到蠻複雜的安裝或設定，所以要先考量好環境後並確定所受的影響再更動。 最後記得 reload 該台 router 使設定生效。
參考資料	http://www.securiteam.com/exploits/2HUQ9QAQOS.html http://www.codetalker.com/advisories/misc/cisco-990413.html http://cert.uni-stuttgart.de/archive/win-sec-ssc/1999/04/msg00001.html http://www.ciac.org/ciac/bulletins/j-041.shtml http://www.cisco.com/warp/public/770/iosnatacl-pub.shtml

3.1.31. Cisco IOS Established Access Keyword 漏洞

弱點名稱	Cisco IOS Established Access Keyword 漏洞
受影響系統	- Cisco IOS 11.2
弱點詳述	在 Cisco 12000 系列的 Gigabit switch router 上跑某些版本 Cisco IOS 將會導致該機器轉遞非授權過的封包，這是因為在處理 access-list statement 中的 keyword 上發生了錯誤。 這個問題僅影響 cisco gigabit Switch router 上面跑 Cisco IOS release 11.2(14)GS2 到 11.2(15)GS3。此項問題已經在 11.2(15)GS5 和以後的版本修復了。 當某台有問題的 router 執行到下列命令時： access-list 101 permit tcp any any established established keyword 將會被忽略掉，這會導致 GSR 從相關的網路卡轉遞所有的 TCP 封包，而不照原先 accesslist 的中的限制來限制該流量。
解決方法	Upgrade to Cisco IOS release 11.2(15)GS5 or later.
參考資料	CVE-1999-0775 http://www.securiteam.com/exploits/2CVQ2QAQPK.html http://www.cisco.com/warp/public/770/iosgsracl-pub.shtml http://www.safermag.com/html/safer14/advisories/16.html

3.2 Lucent 路由器

Denial of Service (阻斷式攻擊)

3.2.1. Ascend Max UDP Port 漏洞

弱點名稱	Ascend Max UDP Port 漏洞
受影響系統	- Lucent Acsend MAX Router 5.0 - Lucent Acsend MAX Router 4.0 - Lucent Acsend MAX Router 3.0 - Lucent Acsend MAX Router 2.0 - Lucent Acsend MAX Router 1.0 - Lucent Ascend Pipeline Router 6.0 - Lucent Ascend Pipeline Router 5.0 - Lucent Ascend Pipeline Router 4.0 - Lucent Ascend Pipeline Router 3.0 - Lucent Ascend Pipeline Router 2.0 - Lucent Ascend Pipeline Router 1.0 - Lucent Ascend TNT Router 2.0 - Lucent Ascend TNT Router 1.0
弱點詳述	某些 Ascends(Lucent) 路由器軟體的版本會聽 port 9 (UDP Discard)， 而 Ascends 有提供設定工具給 MAX 和 Pipeline 路由器 。因為 MAX 和 Pipeline 路由器透過發布一個特殊格式化的封包給 UDP port 9 設置在本地所安裝的路由器，所以攻擊者有可能把一個類似但是畸形的封包送到相同的 Port ，將讓執行某些軟體版本的 MAX 和 Pipeline 路由器暫停工作。
解決方法	請升級到下列列版本可以舉止此漏洞。 - Lucent Acsend MAX Router 5.0ap48 - Lucent Ascend Pipeline Router 6.0.2 - Lucent Ascend TNT Router 2.0.3
攻擊工具	AscendPort9.pl
參考資料	CVE-1999-0060

	http://www.securityfocus.com/bid/714 http://www.pgp.com/research/covert/advisories/026.asp http://www.insecure.org/sploits/ascend.router.insecurities.html

3.2.2. Lucent Postmaster DOS 漏洞

弱點名稱	Lucent Postmaster DOS 漏洞
受影響系統	- Lucent Portmaster 3.0 - Lucent Portmaster 2.0 - Lucent Portmaster 1.0
弱點詳述	Portmaster 是 Lucent 科技公司的一台路由器，以前叫作 Livingston Ensterprises，是一個阻斷式攻擊的目標。如果遠程進攻者把畸形資料送到 Portmaster 路由器上的 telnet port，服務將停止附應。需要服務的重新開始以獲得正常的狀態。 此漏洞存在於允許遠程進攻者進入 telnet port 的 Livingston Portmaster 2，Portmaster 3 和 Office Router 系列，導引路由器重開機或記憶體載荷高，需要重開機路由器以獲得正常的狀態。使用 direct console 或 console port 進入那台路由器與使用其他 TCP port 不會受到此漏洞的影響。
攻擊工具	PortmasterDOS.pl
解決方法	以下三個方法可以防止此漏洞，此方法可以結合使用： 1 - 升級路由器至 ComOS 3.7（請參考賣主解決方法） 2 - 路由器上應用過濾封包程式（請參考過濾封包的解決方法） 3 - 下 "set telnet 0" 指令關掉 portmaster 的 telnet 存取 過濾封包的解決方法 為了完整防止 portmaster 受到阻斷式攻擊需要設定兩個過濾方法。第一個過濾方法式是限制可存取 Portmaster 的網域（請參考下面的例子），第二個方法是限制可存取 Portmaster 的使用者（請參考下面的例子）。 例子 1：

狀況：

* 只有一個管理電腦：192.168.10.2
* 使用者用 PPP/SLIP 溝通(沒有從 PortMaster 作 rlogin/telnet 的動作)

設定方法：

```
add filter etherscreen
set filter etherscreen 1 permit 192.168.10.2/32
192.168.10.33/32
set filter etherscreen 2 deny 0.0.0.0/0 192.168.10.33/32
set filter etherscreen 3 permit 0.0.0.0/0 0.0.0.0/0
set ether0 ifilter etherscreen
```

例子 2：

狀況：

* 管理電腦：192.168.1.0/24
* Portmaster 跟在這些網域的機器共享路由資訊 192.168.10.0/24
* Portmaster 只處理 PPP/SLIP 連接

設定方法：

```
add filter etherscreen
set filter etherscreen 1 permit 192.168.10.0/24
192.168.10.33/32
set filter etherscreen 2 permit 192.168.1.0/24
192.168.10.33/32
set filter etherscreen 3 deny 0.0.0.0/0 192.168.10.33/32
set filter etherscreen 4 permit 0.0.0.0/0 0.0.0.0/0
```

例子 3:

狀況：

* 管理電腦：192.168.1.0/24
* Portmaster 跟在這些網域的機器共享路由資訊 192.168.10.0/24
* 192.168.1.10 是 shell host 而不直接跟 Portmaster 溝通，但是不允許使用 telnet port 溝通(Telnet port 預設是 23)
* 已經進入的使用者需要可以 telnet 或 rlogin 到其他地方

設定方法：

	add filter etherscreen set filter etherscreen 1 deny 196.168.1.10/32 192.168.10.33/32 tcp dst eq 23 set filter etherscreen 2 permit 192.168.1.0/24 192.168.10.33/32 set filter etherscreen 3 permit 192.168.10.0/24 192.168.10.33/32 set filter etherscreen 4 deny 0.0.0.0/0 192.168.10.33/32 tcp dst eq 23 set filter etherscreen 5 permit 0.0.0.0/0 192.168.10.33/32 tcp established set filter etherscreen 6 deny 0.0.0.0/0 192.168.10.33/32 set filter etherscreen 7 permit 0.0.0.0/0 0.0.0.0/0 上述例子主要是未了達到以下的目的: 1 - 別讓在周圍的機器跟 portmaster 的 telnet port 溝通(但是 Portmaster 還是可以幫周圍的機器作 routing 的動作) 2 - 允許管理者的電腦可以跟 Portmaster 溝通 3 - 允許其他 Portmaster 跟 Portmaster 溝通 4 - 別讓人何人送任何封包給我們的 5 - 允許建立好的連接進入我們 6 - 別讓任何人進入我們 賣主的解決方法 此漏洞被修正在 ComOS 3.7 版本。有受到此漏洞影響的使用者需要立即升級

3.2.3. 可預測的 Initial TCP Sequence Number 漏洞

弱點名稱	可預測的 Initial TCP Sequence Number 漏洞
受影響系統	- Lucent ComOS 3.7
弱點詳述	Lucent Portmaster 經常有 TCP 127 之最初 sequence number ， 這些特性能夠讓遠端攻擊者發起 TCP sequence 的預報攻擊 。 此漏洞在某些情況之下攻擊者有可能送假封包過去。
解決方法	為了避免混亂狀況我們必須預防數據段在一個還在被使用的狀況下被其他連接端使用 ， 即使一個 TCP 碰撞及失去所有被使用過的 sequence number 順序。當產生新的連接 ， 初步 sequence number (Initial Sequence Number) 產生器會選擇一個新的 32 bit 初步 sequence number 。 產生器會在 32 bit clock 之後每 4 微秒把底次序 bit 增加 ， 導致初步 Sequence Number 會在每 4.55 小時內循環一次 。 由於我們假設數據段留在網路的時間不超過 Maximum Segment Lifetime (MSL) 而 MSL 直小於 4.55 小時，所以我們可以假設 ISN 是唯一的。
參考資料	http://www.guardent.com/A0303122001.htm http://www.networkcomputing.com/unixworld/security/001.txt.html

Can Access Restricted Resource（非法存取）

3.2.4. Lucent Orinoco 封閉網路非授權存取漏洞

弱點名稱	Lucent Orinoco 封閉網路非授權存取漏洞
受影響系統	- Lucent Orinoco
弱點詳述	ORiNOCO 是一個 Lucent 無線網路產品，提供無線網路連接的存取方式，它有兩種模式公開模式（會員可以自由加入連結）和封閉模式（限制一些使用者才能夠連結）。 最近發現一個 Oricono 實作上的缺失，讓非授權的使用者取得封閉網路的存取權力。原因是因為 Oricono 網路利用存取控制的時候，一些機器之間所使用的密碼預設使用 WEP 加密方法傳送的，那些密碼是所有主機所使用的共同密碼。最近被發現 WEP 加密方法有一些樓同可以讓攻擊者收到幾個樣本之後推出原文的密碼，所以不友善的使用者有可能執行竊聽程式，取得樣本之後推出原文的共同密碼。
解決方法	請打開其他加密方式的功能，將傳送密碼過程中沒有使用 WEP 加密方式傳送。有關 WEP 的漏洞詳細資料請參考： http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
參考資料	http://www.securityfocus.com/cgi-bin/ vulns-item.pl?section=info&id=2538 http://www.securiteam.com/securitynews/5ZP0I154UG.html http://www.sublimation.org/security/localarchive/ 802.11/lucent-access-point-vuln.txt

3.2.5. Lucent RADIUS Buffer Overflow 漏洞

弱點名稱	Lucent RADIUS Buffer Overflow 漏洞
受影響系統	- Lucent RADIUS 2.1-2
弱點詳述	RADIUS 是一個 client-server 網際網路安全系統，在多使用者網路環境裡面控制 authentication，計帳與存取權限。它主要是被使用於 Internet Service Providers（ISPs）公司來控制存取權限與使用者的 authentication，無線網路 802.11 來控制 MAC 地址的 authentication，大型公司或學術單位來管理大量撥接數據機的聯營。 Lucent RADIUS 實作上有一個 Buffer Overflow 漏洞在它的 authentication 程式裡面。此漏洞的原因是因為不充分的邊界檢查當 authentication 程式分析使用者所輸入的字串。遠端攻擊者有可能把 buffer 填滿之後，在系統上執行任何程式。 如果攻擊者可以控制到 RADIUS 伺服器，攻擊者有可能控制所有落在 RADIUS 管理下的機器，如：收集到各機器的登入密碼和帳號，因為大部分的 radiusd（RADIUS 伺服器程式）使用 super user 權限去執行的。
解決方法	Lucent 公司沒有繼續維護 Lucent RADIUS. Lucent RADIUS 目前是被一名 VA Linux 系統工程師，Simon Horms，維護。所以使用 VA Linux 系統所發的最新修補程式就可以解決此問題了。
參考資料	CAN-2001-0534 http://www.securityfocus.com/bid/2989 http://xforce.iss.net/static/6794.php

3.3 3Com 路由器

Denial of Service (阻斷式攻擊)

3.3.1. 3com Office Connect DSL 路由器漏洞

弱點名稱	3com Office Connect DSL 路由器漏洞
受影響系統	- 3com Office Connect DSL 路由器 812 1.1.7 - 3com Office Connect DSL 路由器 804 1.1.7
弱點詳述	Office Connect 812 是一個 3Com 大量製造的 DSL 路由器，而被很多 DSL 提供者使用。OfficeConnect 812 是一個完整的 ADSL 路由器，具備版面上的 4 埠交換機。 最近發現路由器的韌體有阻斷式攻擊的問題。使用 HTTP 連結送一連串字串給路由器的 HTTP 伺服器程式，有可能讓路由器自動重開，此問題有可能讓遠端攻擊者進行阻斷式攻擊。
解決方法	此問題有兩種解決方法，第一種是過濾路由器之 WAN 介面的 80 埠。另外請升級您的系統，升級版可以從下列網站免費下載： - 3Com OfficeConnect 812 & 840 1.1.9.4 升級版 ftp://ftp.3com.com/pub/officeconnect/ ocradsl/bld_1_1_9_4.zip
攻擊工具	3comAdsl812.c
參考資料	CAN-2001-0740 http://www.securityfocus.com/bid/2721 http://www.safermag.com/html/safer37/dos/13.html

3.3.2. 3com Home Connect 纜線數據機路由器漏洞

弱點名稱	3com Home Connect 纜線數據機路由器漏洞
受影響系統	- 3com Home Connect 3CR29223
弱點詳述	Home Connect 是 3com 的外界纜線數據機路由器 ， 並已經被許多寬頻網路公司使用 。 最近發現纜線數據機路由器有一個漏洞能夠讓遠端使用者進行阻斷式攻擊 。 纜線數據機路由器擁有通訊埠 80/TCP ， 預設提供 HTTP 服務給整個網路使用者 ， 讓網路上的任何使用者可以存取它的 HTTP 服務 。 問題出現當使用者連上此網站並發 100 以上之字串給 HTTP 埠，將路由器在最佳狀況下立刻自動關機。
解決方法	過濾纜線數據機上的 80 通訊埠 ， 讓不友善使用者無法攻擊此漏洞 。 另外由於此產品已停產 ， 建議您通知您的網際網路服務提供者要求更換纜線數據機 。
攻擊工具	3comHomeConnect.pl
參考資料	CAN-2001-0740 http://www.securityfocus.com/bid/2721 http://www.safermag.com/html/safer37/dos/13.html

Can Access Restricted Resource (非法存取)

3.3.3. 3com Switches Backdoor 漏洞

弱點名稱	3com SwitchesBackdoor 漏洞
受影響系統	- Corebuilder 2500/ 3500/ 6000/ 7000 - SuperStack II 2200/ 2700/ 3900/ 9300 - 3Com LANplex 2500 (rev 7.15) with Version 7.0.1-19 - Built 01/17/97 02:41:17 PM - LinkSwitchh
弱點詳述	存在一個無正式文件的存取等級在 3Com 的 LAN Plex / Corebuilder 交換機 。 除了 admin, read 和 write 帳號之外 ， 3Com LAN Plex 7.0.1 和 8.1.1 版持有一個預設 debug 帳號 ， 預設密碼為 synnet 。 Debug 帳號有所有管理者帳號的權限加上別的使用者沒有的移去錯誤指令 ， 導致他在沒有舊密碼的情況之下可以改其他存取密碼 。 另外 Debug 帳號也可以得到置於作業系統之下的殼 。 加上如果把遠端管理的功能打開 (透過 telnet) ， 攻擊者更有可能獲的交換機的控制權限 。
攻擊工具	使用 telnet client 程式進行上述攻擊方法
解決方法	使用 debug/synnet combo 登入交換機而使用 “系統密碼” 指令更改隱含值的設定 ，使 admin 帳號沒辦法更改密碼 。
參考資料	http://spisa.act.uji.es/spi/progs/codigo/exploits/misc/3com.switches.routers.undocumented.backdoors.html

3.3.4. 3com AirConnect 無線閘門非法存取漏洞

弱點名稱	3com AirConnect 無線閘門非法存取漏洞
受影響系統	- 3com AP-4111
弱點詳述	最近發現 AirConnect 無線閘門有非法存取的漏洞，有可能公開機器的 Wired Equivalent Privacy（WEP）鑰匙。使遠端使用者有可能取得無線網路上的存取權力。 使用下列 SNMP 要求，在 Access point 之有線網路上的遠端使用者有可能取得 WEP 鑰匙： 1. IEEE 802.11b MIB: dot11WEPDefaultKeysTable 裡的 dot11WEPDefaultKeyValue 2. Symbol MIB: ap128bWEPKeyTable 裡的 ap128bWepKeyValue 拿到 WEP 鑰匙之後，一個遠端有線網路上的使用者可以取得無線網路上的權力。
解決方法	目前到 2002 年 12 月初 3Com 針對此漏洞還沒有發出修補程式，3Com 預計不久之後發出一個韌體修補程式。
參考資料	http://www.3com.com http://securitytracker.com/alerts/2001/Jun/1001799.html http://www.wispa.org/pipermail/ ism-wireless/2001-June/000664.html

View or Modify Configuration (偷閱或更改系統設定)

3.3.5. 3com HiPer Arc Community Name 漏洞

弱點名稱	3com HiPer Arc Community Name 漏洞
受影響系統	- 3com HiPer Arc 4.1 - 3com HiPer Arc 4.0
弱點詳述	在 3Com HiPer Arc 卡或其他有使用 Pilgrim 程式的卡，有存在一個漏洞讓攻擊者可以從遠端拿到 SNMP 管理者的權限。那些卡有三種權限分為唯讀,讀寫與管理者。SNMP 的 community strings 在三種權限裡是可讀,只要看 usrSnmpCommAccess 表裡面有那些 community string ，加上上述的漏洞就有可能讓惡意者拿道管理者的權限。取得管理者權限之後，攻擊者可以進行其他惡意的行動(如：移動 arp cache)。 所有 HARC 4.0.XX 和 HARC 4.1.YY， YY 小於 59 ， 有受到此漏洞的影響 。 HARC 4.2.XX ， HARC 5.0.XX 及 9/1/99 以後的 HARC 不會有這些問題。
解決方法	為了解決這個問題 ， 3COM 提供 HARC 的最新版本 。 9/1/99 之後的所有 HARC 程式已經解不會受到此漏洞的影響 。 除了升級您的版本還有兩個解決方法可以做 ： 1. 限制固定 IP 的 community string 。 只是一個最基本的安全而 snmp community strings 還是可讀的。 2. 不要打開 ARC 的 snmp 三種權限 ， 但是需要 NMC (Network Management Card) 當 Hiper Arc 的 relay 。 NMC 的 community string 要設為 communitystring@<entitynum> (例如：public@16000 ， 意思是我們要送 SNMP 指令給 Arc slot 16 而 NMC 的 community string 為 public) 。 唯一缺點是因為 NMC 卡使用 486 處理器所以 SNMP 的操作會變慢 。 沒有受到此漏洞的版本如下：

	● 3com HiPer Arc 4.2 ● 3com HiPer Arc 5.0
參考資料	http://xforce.iss.net/alerts/vol-4_num-5.php #3com-hiper-comm-name http://www.networkice.com/Advice/Intrusions/ 2002013/default.htm http://www.securityfocus.com/bid/537

Flaw of the Implementation or specification (實作或規格上的缺失)

3.3.6. 3com Corebuilder & Superstack II LAN Switch 漏洞

弱點名稱	3com Corebuilder & Superstack II LAN Switch 漏洞
受影響系統	- CoreBuilder 2500/6000/3500 - SuperStack II Switch 2200/3900/9300.
弱點詳述	3Com 所發布的安全公告裡面指示 CoreBuilder LAN 交換機和 SuperStack II 交換機的產品擁有安全上的漏洞 。 這個漏洞是一個預設帳號與密碼 ， 本來是 3Com 客戶中心所發的緊急補救方法 ， 讓忘記密碼的管理者還可以登入到那台機器 。 因為那些預設帳號與密碼後來被公開 ， 一些 3Com 交換機的產品含有預設登入帳號的漏洞 。 為了舉止,此問題 ， 請立即使用下面帳號與密碼登入交換機 ，而更改與設帳號的密碼 。 CoreBuilder 6000/2500 - 帳號 : debug 密碼 : synnet CoreBuilder 7000 - 帳號 : tech 密碼 : tech SuperStack II Switch 2200 - 帳號 : debug 密碼 : synnet SuperStack II Switch 2700 - 帳號 : tech 密碼 : tech CoreBuilder 3500 ， SuperStack II Switch 3900 與 9300 也會有上述的帳號與密碼 ， 但是當管理者帳號的密碼被更改的時候 ， 上述帳號的密碼也會隨管理者的密碼更改 。 使用者應該要立即更改 SNMP Community String 從預設值改成私有的設定 。 要這樣做是因為當 MIB 透過 SNMP 讀或寫存取的時候 ， 管理者密碼就可以從特殊的 MIB 變數取得到 。

解決方法	下載新版本 Patch 系統 。
參考資料	CAN-1999-1513 http://www.nta-monitor.com/newrisks/jun98/3com.htm

3.3.7. 3COM SuperStack II 交換機 1001 的預設帳號和密碼漏洞

弱點名稱	3COM SuperStack II 交換機 1001 的預設帳號和密碼漏洞
受影響系統	- 3COM SuperSwitch II 1000
弱點詳述	3COM SuperSwitch II 1000 預設安裝的時候有四種存取等級的帳號與密碼。 預設帳號為： - monitor - manager - security - admin 上述帳號的密碼除了 admin 之外預設跟帳號名稱一樣 ，admin 的密碼預設為空白 。 這些密碼在第一次安裝完之後要馬上更改 ， 避免攻擊者或未被授權的惡意者使用那些帳號更改或存取交換機的參數 。 透過 Telnet port 攻擊者可以使用 VT100 介面管理交換機 。
攻擊工具	使用 telnet client 程式進行上述攻擊方法
解決方法	由 VT100 介面或 SNMP 網管編輯使用者詳述資料 ， 將更改 SuperStackII Switch 1000 的預設密碼 。 每個網管提供它自己的介面讓管理者可以很容易的管理此設備 ， 詳細設定方法請參考 SNMP 網管的相關文件 。
參考資料	http://the.wiretapped.net/security/info/textfiles/underground-periodical/up-6.txt

Lost Access Control (Access Control 失效)

3.3.8. 3com Total Control Filter Bypass 漏洞

弱點名稱	3com Total Control Filter Bypass 漏洞
受影響系統	- 3com Total Control NETServer Card 3.7.24
弱點詳述	Total Control Chassis 系列是一個普通的終端伺服器 ， 當一個人撥一個有提供 X2 的 ISP ， Total Control Chassis 會幫那個人撥給那一台 ISP 。 有回答一個 'host:' 或類似提示的系統而那個系統有執行特殊版本的作業系統是可能有漏洞的系統 。 當一個 port 被設為 "set host prompt" 的時候 ， 雖然特殊 port 有啟動存取過濾程式，但是存取過濾程式會被忽略掉 。 假設存取過濾程式的策略如下 ： > sho filter allowed_hosts 1 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.161/32 tcp dst eq 539 2 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.165/32 tcp dst eq 23 3 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.106/32 tcp dst eq 23 4 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.168/32 tcp dst eq 540 5 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.168/32 tcp dst eq 23 6 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.109/32 tcp dst eq 3030 7 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.109/32 tcp dst eq 3031 8 permit XXX.XXX.XXX.12/24 XXX.XXX.XXX.109/32 tcp dst eq 513 9 deny 0.0.0.0/0 0.0.0.0/0 ip 過濾程式被設為 "set all ifilter allowed_hosts" 撥進來的使用者可以在 "host:" 後面打一個 hostname 兩次 ， 使打開一個 telnet session 到那個 host 如下： > sho ses S19 woodnet.wce.wwu woodnet.wce.wwu. Login In ESTABLISHED 4:30 使用此方法導致 syslogs 裡面出現下面的資訊 ： May 11 08:58:39 XXXXXX remote_access: Packet filter does not exist. User woodnet.wce.wwu.edu access denied 。 雖然 syslogs 裡面指示 access denied 但是實際上並沒有被

	拒絕 。 這些問題在前幾個版本並還沒有被發現，特別是 Total Control™ NETServer Card V.34/ISDN 使用 Frame Relay V3.6.22 才發現有可能受到這個漏洞的影響。
解決方法	下載新版本 patch 系統。
參考資料	CAN-1999-1389 http://www.insecure.org/sploits/ USR.total.control.chassis.html

3.4 Extreme Networks 路由器

Denial of Service (阻斷式攻擊)

3.4.1. Extreme Network 嵌入系網頁伺服器漏洞

弱點名稱	Extreme Network 嵌入系網頁伺服器漏洞
受影響系統	- Allegro RomPager 2.10
弱點詳述	Allegro's RomPager 是一個嵌入系的網頁伺服器，它有提供從網頁上可以管理網路印表機,網路交換機,等等設備的功能。 若有人送給它一個特別地畸形要求，伺服器將會暫停服務，導致其他網路設備及整個網路有可能無法連接。 某些 Extreme Networks 產品會識別自己當 2.10 但是不會受到此漏洞的影響。
解決方法	請升級到 RomPager 2.20 版。受到影響之機器的使用者請跟機器之賣主請教解決方法或至下列網址參考如何解決此問題的文件： http://www.allegrosoft.com 建議使用防火牆來限制網頁伺服器的存取權限。
參考資料	CVE-2000-0470 http://www.securityfocus.com/bid/1290 http://www.safermag.com/html/safer26/dos/26.html

3.5 Xylan Network 路由器

Flaw of the Implementation or specification（實作或規格上的缺失）

3.5.1. Xylan-OmniSwitch ftp 漏洞

弱點名稱	Xylan-OmniSwitch ftp 漏洞
受影響系統	- Xylan OmniSwitch
弱點詳述	一些 Xylan OmniSwitches 允許遠端使用者透過 FTP port 存取那台設備和取得 Flash 記憶體的讀寫權限。因為有一些檔案內容是機密的，如：SNMP community name strings，等等內容，則這些檔案不因該給普通使用者存取權限為避免設備受到攻擊。
攻擊工具	使用 ftp client 程式進行上述攻擊方法
解決方法	限制連接存取的 IP 來源或把 FTP port 關掉。
參考資料	http://packetstorm.decepticons.org/9904-exploits/xylan.omniswitch.txt http://www.netspace.org/cgi-bin/wa?A2=ind9904a&L=bugtraq&F=&S=&P=185 http://www.securiteam.com/exploits/2AUQ3QAQNQ.html

3.5.2. Xylan-OnmiSwitch-login 漏洞

弱點名稱	Xylan-OnmiSwitch-login 漏洞
受影響系統	- Xylan OmniSwitch
弱點詳述	一些 Xylan OmniSwitches 允許遠端使用者透過 telnet port 使用任何帳號和 ctrl 字串的密碼登入交換機 ， 登入之後雖然攻擊者沒辦法下任何指令 ， 但是可以讓別的使用者沒辦法從 telnet port 登入 ， 因為 Xylan OmniSwitches 在同一時間只允許一個人連接 ， 所以造成阻斷式攻擊 。
攻擊工具	請使用 telnet client 程式進行上述攻擊方法
解決方法	限制連接存取的 IP 來源 。
參考資料	http://packetstorm.decepticons.org/9904-exploits/xylan.omniswitch.txt http://www.netspace.org/cgi-bin/wa?A2=ind9904a&L=bugtraq&F=&S=&P=185 http://www.securiteam.com/exploits/2AUQ3QAQNQ.html

3.6 Cabletron 路由器

Denial of Service (阻斷式攻擊)

3.6.1. Cabletron Smart Switch Router ARP Flood DOS 漏洞

弱點名稱	Cabletron Smart Switch Router ARP Flood DOS 漏洞
受影響系統	- Cabletron Smart Switch Router 8000 firmware 2.x
弱點詳述	Cabletron's Smart Switch Router 是一個第二層和第四層的路由和交換設備 。攻擊者有可能讓路由器暫停處理網路的封包 。 Cabletron 指示隘路會出現在 Smart Switch Router 之 ARP 處理過程。 Smart Switch Router 每一秒鐘只能處理 200 ARP 要求 。 所以只要在初步連接的時候發大於 200 個 IP 之網路封包 ， 攻擊者有可能讓路由器暫停服務因為 ARP 處理器被淹沒 。 很多防火牆的策略會讓 ICMP 過 ， 這表示遠端匿名攻擊者有可能撞 Smart Switch Router 。
攻擊工具	使用 arping 之類的程式進行上述攻擊方法
解決方法	Firmware 3.x 版沒有受到此漏洞的影響 ， 建議升級到最新版免得受到此漏洞的影響 。可以至下面網址下載最新版本 ： http://www.cabletron.com/download/download.cgi?lib=ssr
參考資料	http://packetstorm.decepticons.org/9911-exploits/cabletron.ssr.dos.txt http://www.securiteam.com/exploits/3W5QCR5Q0S.html

Flaw of the Implementation or specification（實作或規格上的缺失）

3.6.2. Cabletron Spectrum Enterprise Manager 5.0 漏洞

弱點名稱	Cabletron Spectrum Enterprise Manager 5.0 漏洞
受影響系統	- Sun Solaris 2.6 - Sun Solaris 2.5.1 - Microsoft Windows NT 4.0SP5 + Microsoft Windows NT 4.0 - Microsoft Windows NT 4.0SP4 + Microsoft Windows NT 4.0 - Microsoft Windows NT 4.0SP3 + Microsoft Windows NT 4.0
弱點詳述	在安裝過程中，Cabletron Spectrum Enterprise Manager 會產生一個樹狀結構目錄 。 這些樹狀包括安裝過程的執行檔 ，而其中一個執行檔需要 root 的權限執行 。 所以會有暫是狀況讓一個不友善的使用者可以取代或修改那些執行檔跟他自己的程式 。 安裝完之後 ， 沒有任何物件會使用 root 的權限被執行 ， 但是執行檔還使用由可寫的權限 ， 這時候不友善的使用者有可能放入木馬或阻斷式攻擊 。
解決方法	建議在安裝過程中產生您的 Spectrum “管理者”與 “操作者” 。 產生完之後 ， 請立即關掉 Spectro SERVER 與檔 Spectrum 管理者重新開機 。接下來請打開使用者編輯程式與毀滅 root 使用者 ， 因為我們已經不需要 root 使用者的存在 。 同樣的方法 ， 在 Windows NT 系統下 ， 請毀滅 SpectroSERVER 資料庫的 Administrator 模式 。 除了上述的方法之外也建議依以下步驟處理： 1. 不要創造或允許登入任何在 Spectrum host 的使用者帳號 ， 請注意是否有打開其他服務 ， 如匿名 FTP ， 因為那些服務准許重疊寫 Spectrum 目錄裡的一些檔案 。 2. 變緊 Spectrum 目錄的讀寫權限 (請參考附件) 。 另外

	我們也可以利用 group 權限提高系統的安全性 ， 用此方法 Spectro GRAPH 使用者還可以擁有 Spectrum 目錄的讀寫權限 。 當設定 Spectrum Enterprise Manager 的時候 ， 創造一個 spectrum group 給 $SPECROOT 目錄和所有分目錄與裡面的檔案 。 打開 $SPECROOT 之 set-gid bit 和所有分目錄讓所有分目錄入口將繼承那個 group ID ， 如 ： spectrum， 等等 (沒有打開 set-gid bit 分目錄入口會是一個執行 process 之 effective group ID) 。 如果你在安裝步驟中有機會作上述動作那是很完美的 。 一個 umask 02 (使用者和群組可以讀寫)也會是一個很好用的辦法 。 當設定 Spectrum 使用者帳號的時候 ， 只要是安裝 Spectrum 的使用者目標 (spectrum) 和那些可以執行 SpectroGRAPH 的使用者就可以設為那台伺服器的 spectrum 群組 ， 讓那些使用者擁有 spectrum 目錄和檔案的存取權限 and those users 。

附件	以下是此漏洞修補 script :
	#! /bin/ksh
	
	# configuration - target user and group:
	typeset target_user=spectrum
	typeset target_group=spectrum
	
	# external commands used by this script:
	find=/usr/bin/find
	xargs=/usr/bin/xargs
	chown=/usr/bin/chown
	chmod=/usr/bin/chmod
	
	if cd ${SPECROOT?}
	then
	  :
	else
	  print -u2 "Could not change to \$SPECROOT directory: ${SPECROOT?}"

	exit 1 fi # set owner and group of directories and non-setuid files: ${find?} . \(-type d -o \(-type f ! -perm -4000 \) \) -print \|${xargs?} ${chown?} ${target_user?}:${target_group?} # turn on set-gid and remove write permission for others on directories: ${find?} . -type d -print \|${xargs?} ${chmod?} g+s,o-w # remove write permission for others on files: ${find?} . -type f -print \|${xargs?} ${chmod?} o-w # remove write permission for group and other on set-uid files: ${find?} . -type f -perm -4000 -print \|${xargs?} ${chmod?} g-w # remove write permission for group on SDPM directory (where processd resides): ${chmod?} g-w SDPM exit 0
參考資料	http://www.securiteam.com/exploits/2BUQERPRFE.html

第四章　Cisco 路由器 1700、2600 系列測試

本計畫除了針對路由類通訊協定及路由器之相關資料進行蒐集、整理與弱點分析之外，也將針對 Cisco 1700 與 2600 路由器系列作弱點測試 。 本計劃的測試環境詳述說明請參考以下文件 。

路由器規格：

機器一

Cisco 1720 with 15360K/5120K bytes of memory

IOS 版本：Version 12.0(3)T3

機器二

Cisco 2621 with 20480K/4096K bytes of memory

IOS 版本：Version 12.0(5)T1

測試弱點(共六項)：

Cisco Router 1700,2600 Vulnerabilities

Target IP :

Vulnerability description	1700 Series	2600 Series	Workaround
Cisco IOS HTTP Server Query Vulnerability	√	√	workaround
Cisco IOS HTTP Server Vulnerability	√	√	workaround
Cisco's "show" command shows too much	√	√	workaround
IOS HTTP Authorization Vulnerability	√	√	workaround
IOS HTTP Authorization Vulnerability(Show Configuration)	√	√	workaround
CDP Denial Of Service	√	√	workaround

Attack! reset

圖：弱點測試介面：

第一項：**Cisco IOS HTTP Server Query Vulnerability**

在此項路由器漏洞中，問題發生在路由器的 Web 服務上，當惡意使用者使用下

列 http request：

http://*router-ip/anytext?/*

此時會要求使用者鍵入 enable password，若通過，則該路由器將會當機 。 此問題僅會使得那些沒有設定 enable password 的機器有危險 。 在本項測試中，1700 與 2600 系列路由器上的 IOS 版本皆會受此問題影響 。 最後必須重新啟動該路由器以恢復正常運作 。

第二項：**Cisco IOS HTTP Server Vulnerability**

此項路由器漏洞中，問題發生在路由器的 Web 服務上，當惡意使用者使用下列 http request：

http://<router-ip>/%%

將會導致路由器當機 。 在本項測試中，1700 與 2600 系列路由器上的 IOS 版本皆會受此問題影響 。 而 1700 系列在本次攻擊下，將進入 rommon 模式，無法僅重新關電源重開，需要重新 reset、boot，重新載入系統才能恢復運作 。 而 2600 必須重新啟動該路由器以恢復正常運作 。

第三項：**Cisco's "show" command shows too much**

此項漏洞導致一個普通使用者，不需鍵入 enable password 進入 enable mode，即可使用 **show access-lists** 指令 獲知目前 access-lists 的內容 。 而且，當一個普通使用者在 Router 命令列下使用『?』來提示命令時候，例如 show？。 雖然沒有顯示可以使用 show access-lists 的權力，但是仍可以使用此參數 。 其他如下列指令：

- sh ip prot
- sh ip ospf dat
- sh ip eigrp top

也將會洩漏出該網路的重要資訊 。 在本次測試的 1700 及 2600 系列及上的 IOS 都發現有此問題 。

第四項：**IOS HTTP Authorization Vulnerability**

本項問題出現在 web 服務上 ， 本項問題將會使得惡意使用者獲取完全控制

router 的權力 。 一個惡意使用者使用下列命令：

http://<device_addres>/level/xx/exec/....

其中 xx 大於 16 即可，如此不用通過認證即可進入 web 管理模式 。 在我們的測試中發現可以察看路由器設定檔，甚至可以使用 erase 刪除在 flash memory 中的系統檔案 。 在本次測試機器中 1700 及 2600 系列皆受到此問題影響 。

第五項：**IOS HTTP Authorization Vulnerability(Show Configuration)**

此項問題同於上述 ， 使用

http://<device_address>/level/xx/exec/show%20conf

即可直接觀看該機器的 configuration 。 在本次測試機器中 1700 及 2600 系列皆受到此問題影響 。

第六項：**CDP Denial Of Service**

對受影響的機器送出大量的 Cisco Discovery Protocol (CDP)封包，將會導致該機器無法運作，在本次測試中，使用攻擊程式經過數分鐘後，被攻擊機器便無法繼續運作，但是經過一段時間後，便可恢復正常 。 根據公告上所述，CDP 屬於 data link 層，所以本攻擊程式無法跨越 router 及 switch，所以攻擊者程式必須放在同一個網路下 。 受測機器 1700 與 2600 在本測試皆受本問題影響。

本次測試，顯示路由器的管理方式非常重要，務必將路由器上不需要的功能及服務關掉，尤其不要使用 web 管理介面或 telnet 管理，如果非要如此重遠端管理，請務必設定好 Access Control 來限制只有某些來源機器擁有管理的權力，否則就完全在 local 端使用 aux port 來管理路由器 。 由於 Access Control 的重要性，本次報告將也使用範例來介紹如何設定基本及進階的 ACL 。

第五章　Cisco 路由器 ACL 設定方式

Cisco IOS 可以使用 Acess lists 控制來處理哪些封包需要丟棄或處理，若要在 Cisco Router 上擁有相當安全的設定，那就必須使用相當多的 Access lists，來限制對 router 上服務的存取，或者來過濾經過這台 router 的封包 。 以下是 Access list 的使用法：

1. 標準語法(**standard access list**)：

access-list *access-list-number* {**deny**|**permit**} *source* [*Source-wildcard*]
access-list number 可以將 access list 分類，可以指定從 1 到 99。

Deny 拒絕符合條件的封包。
Permit 允許符合條件的封包通過。
Source 指該封包的來源。(source-wildcard：可以使用萬用字集)

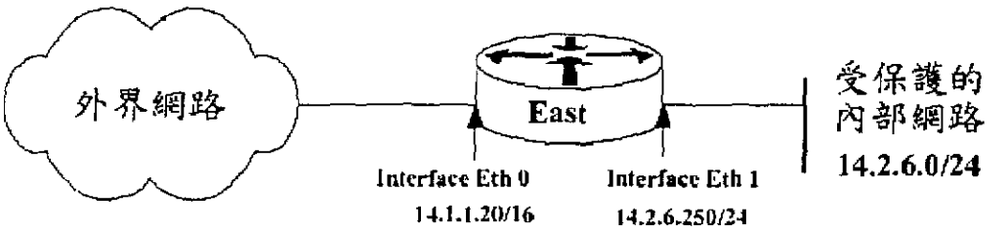
2. 進階語法(**extended IP access list**)：

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard source-qualifiers destination destination-wildcard destination-qualifiers* [**log** | **log-input**]

其中 access-list-number 可以為 100 至 199 。 Protocol 可以為下列關鍵字：eigrp， gre， icmp ， igmp ， igrp ， ip ， ipinip ， nos ， ospf ， tcp or udp 。 *source-qualifiers* 可以對來源位址提供更進一步的資訊篩選。如指定 port 及其他 protocol-specific 的資訊。

路由器安全設定

以下藉由範例來介紹如何使用基本的 Access Control 來保護內部的網路 ，這些都是網路上的路由器所應該必備的基本設定，另外，再加上下一章節所述 ，關閉路由器上不必要的服務 ， 及安全的設定路由器 ， 可以減低被入侵的機會 。



圖一：網路、路由器及介面卡位址。

過濾至 Router 本身的封包

1. 過濾 Remote Login (Telnet) Service:

有時候管理者會使用 Telnet 來連線至 router，來進行管理的工作，這時候必須小心處理 Access list control，以下例子顯示如何使用 ACL 來達到這項目的：

我們在這個例子將只限制 14.2.6.1 和 14.2.6.18 兩部機器來對 router 做 telnet 動作，而其他的位址都不允許。最後也將會 log 下成功與不成功的連線。

```
East(config)# access-list 105 permit host 14.2.6.1 any eq 23 log
East(config)# access-list 105 permit tcp host 14.2.6.18 any eq 23 log
East(config)# access-list 105 deny ip any any log
East(config)# line vty 0 4
East(config-line)# access-class 105 in
East(config-line)# end
```

2. 過濾 SNMP service：

Cisco router 可以打開 SNMP，來藉此啟動一些網管的功能。以下設定方式可以僅允許 14.2.6.6 的機器對這台 router 取得一些 SNMP 資訊。

```
East(config)# access-list 75 permit host 14.2.6.6
East(config)# snmp-server community n3t-manag3m3nt ro 75
```

3. 過濾 OSPF service：

有時候我們需要讓 router 之間彼此交換 routing table 中的資訊，我們也可以對這些 routing protocol 做一些限制，來限制不要從哪些站台獲取到資訊。以下便是一個範例，這台 Router North 將不會對 14.2.9.0 網路來交換 routing 資訊。

```
North(config)# access-list 10 deny 14.2.9.0 0.0.0.255 any
North(config)# access-list 10 permit any
North(config)# router ospf 1
North(config-router)# distribute-list 10 out
North(config-router)# end
```

過濾經過 Router 的封包

有時候我們必須設定一些 Access list 來保護內部網路或抵禦一些外來的攻擊 。 注意，以下個別的例子不能合併為單一的 ACL，因為可能造成某些部分矛盾或錯誤，最後將會介紹如何合併這些 ACL 而達到個別的防護功能 。

1. IP Address Spoof Protection

1.1 Inbound Traffic

以下範例將會不允許位址來自內部的 IP 封包從外面進入（inbound traffic）：

```
East(config)# access-list 100 deny ip 14.2.6.0 0.0.0.255 any log
East(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
East(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
East(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
East(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
East(config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
East(config)# access-list 100 deny ip host 255.255.255.255 any log
East(config)# access-list 100 permit ip any 14.2.6.0 0.0.0.255
East(config)# interface eth0/0
East(config-if)# description "external interface"
```

```
East(config-if)# ip address 14.1.1.20 255.255.0.0
East(config-if)# ip access-group 100 in
East(config-if)# exit
East(config)# interface eth0/1
East(config-if)# description "internal interface"
East(config-if)# ip address 14.2.6.250 255.255.255.0
East(config-if)# end
```

其中，內部配給的 IP 位址是 14.2.6.0，而 local host address 為 127.x.x.x，link-local DHCP default address 為 169.254.0.0，保留的 private IP 位址也被寫在此範例中。最後將這個 ACL 套用在 External interface 上。

1.2 Outbound Traffic

主要是不允許任何 IP source 欄位不是合法的封包流出，例如內部網路 range 為 140.113.33.X，就不該允許 source IP 非這些的封包流出 。 此份 ACL 將套用在 router 的 internal interface。

```
East(config)# no access-list 102
East(config)# access-list 102 permit ip 14.2.6.0 0.0.0.255 any
East(config)# access-list 102 deny ip any any log
East(config)# interface eth 0/1
East(config-if)# description "internal interface"
East(config-if)# ip address 14.2.6.250 255.255.255.0
East(config-if)# ip access-group 102 in
```

另外在 Cisco 路由器上 IOS 12 提供了一個新的機制可以用來防止 IP address spoof，這個機制叫做 IP unicast reverse-path forwarding verification。但是並不適用於所有的網路架構上，必須都使用 Cisco Router 才能擁有此項功能。

2. Exploits Protection：

接下來將介紹使用 ACL 來防止或減低一些著名的攻擊方式。

2.1 TCP SYN Attack

所謂的 SYN Attack 是藉由建立許多不完全的連線到目標，導致

connection queues 滿溢，因此無法處理正常的 TCP 連線，以下是幾種不同的作法：

2.1.1 External Access Blocked

```
East(config)# access-list 106 permit tcp any 14.2.6.0 0.0.0.255 established
East(config)# access-list 106 deny ip any any log
East(config)# interface eth 0/0
East(config-if)# description "external interface"
East(config-if)# ip access-group 106 in
```

此設定可以檔住只有 SYC flag 設定的外來封包，因此只許由路由器內的內部網路建立 TCP 連線，而不允許外界網路建立 TCP 連線。

2.1.2 Limiting External Access with TCP Intercept

```
East(config)# ip tcp intercept list 107
East(config)# access-list 107 permit tcp any 14.2.6.0 0.0.0.255
East(config)# access-list 107 deny ip any any log
East(config)# interface eth 0/0
East(config-if)# description "external interface"
East(config-if)# ip access-group 107 in
```

此設定可以擋住從 unreachable hosts 來的封包，也就是只允許 reachable 的外部主機來建立對內部網路的連線。在 Intercept mode 下，路由器將會先暫時中斷每個 TCP 連線，去檢查建立連線的機器是否存在（是否 reachable），如果是，才允許建立連線。
Cisco IOS 的 Intercept mode 功能是一項防止 TCP SYN 攻擊的機制，使用這項特色可以有效防止這類類似 SYN 這種利用 TCP 連線機制問題的攻擊。

2.2 Land Attack

所謂的 Land Attack 指對路由器送出的 IP 封包中，source 與 Destination 欄位都填相同的 IP 位址;Source port 與 Destination port 都填入相同的 port 號碼，這種攻擊將會導致 Denial of Service，或者降低路由器的效能。下列設定可以防制這類攻擊。

```
East(config)# access-list 100 deny ip host 14.1.1.20 host 14.1.1.20 log
```

```
East(config)# access-list 100 permit ip any any
East(config)# interface eth0/0
East(config-if)# description "external interface to 14.1.0.0/16"
East(config-if)# ip address 14.1.1.20 255.255.255.0
East(config-if)# ip access-group 100 in
East(config-if)# end
East#
```

2.3 Smurf Attack

此類攻擊是指，利用送出大量偽造 source 位址的 ICMP Echo request 封包給某個 subnet broadcast 位址，如此該位址內所有的機器都會對該偽造的 source 位址回覆 Echo reply，如此導致該偽造的機器接收到大量的封包。因此一台位於網路咽喉處的路由器應該擋住所有向內部，但是終點是 broadcast address，以下設定便是擋住 194.168 網域內，所有 destination 是 broadcast address(14.2.6.255 和 14.2.6.0)的封包。

```
East(config)# access-list 110 deny ip any host 14.2.6.255 log
East(config)# access-list 110 deny ip any host 14.2.6.0 log
```

2.4 ICMP Message Types and Traceroute

ICMP 有很多種訊息規格，例如 ping 程式中使用到 ICMP echo 和 echo reply，而其他應用程式或者裝置也都有使用到其他 ICMP 訊息來交換網路上資訊，對於 Inbound 的 ICMP 封包，擋住所有的 Echo 和 redirect 類型，可以使得遠端攻擊者無法藉由此來獲知網路拓樸，也可以防止 Smurf Attack，使用 ICMP redirect 封包，攻擊者可以藉此改變主機的 routing table。而其他的 ICMP 訊息則可以讓他們通過。以下是 inbound ICMP ACL 的範例：

```
East(config)# access-list 100 deny icmp any any echo log
East(config)# access-list 100 deny icmp any any redirect log
East(config)# access-list 100 deny icmp any any mask-request log
East(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
```

對於 Outbound 的 ICMP 封包，Echo ，Parameter Problem，Packet Too Big，還有 Source Quench 這些類型都要放行，而擋住其他類型的封包，Echo 是讓內部使用者可以 ping 外界網路，Parameter Problem 還有 Source Quench

是當 packet 出現某些問題可以作為交換資訊用，Packet Too Big 是給 Path MTU discovery 所使用，這些都是必須要放行的。下列是 Outbound ICMP 封包的 ACL 範例：

```
East(config)# access-list 102 permit icmp any any echo
East(config)# access-list 102 permit icmp any any parameter-problem
East(config)# access-list 102 permit icmp any any packet-too-big
East(config)# access-list 102 permit icmp any any source-quench
East(config)# access-list 102 deny icmp any any log
```

皆下來要處理的是 traceroute 程式，由於此程式也會透露出網路拓樸(藉由 UDP 封包)，所以下列範例示範如何防止惡意攻擊者藉此探查網路拓樸：

```
East(config)# access-list 100 deny udp any any range 33400 34400 log
```

其中 port 33400 至 34400 是常用於 traceroute 的 UDP port 。 而相對的，路由器可以藉由下列設定來允許 outbound traceroute：

```
East(config)# access-list 102 permit udp any any range 33400 34400 log
```

2.5 Distributed Denial Of Service(DDOS)攻擊

事實上沒有完全防制此類攻擊的辦法，只能針對目前網路上流行過的 DDOS 攻擊及其攻擊程式進行防制，但是仍然並不是最有效，且可能對一般合法使用者造成影響。本範例設定將會擋住網路上有名的數種 DDOS 工具的攻擊，但是這是藉由知悉其已知攻擊的 port 來進行防範。因此建議只有確定遭受到 DDOS 攻擊之後再來套用此項 ACL 設定。

```
! the TRINOO DDoS systems
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log
! the Stacheldraht DDoS system
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
! the TrinityV3 system
access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
```

```
! the Subseven DDoS system and some variants
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

而 TFN(Tribe Flood Network) DDOS 攻擊是使用 ICMP echo reply 訊息，所以可能因為 ping 程式的關係，而比較無法擋住，按照上述 ICMP 範例的設定，至少可以擋住一方向的 TFN 攻擊。

以下總和範例雖然不盡能含括上述範例所有的規則，但是也保證了一定的強度，另外此範例允許大部分的 outbound Traffic，而對 Inbound Traffic 做了大量的限制。

```
hostname East
 !
interface Ethernet0
description Outside interface to the 14.1.0.0/16 network
ip address 14.1.1.20 255.255.0.0
ip access-group 100 in
!
interface Ethernet1
description Inside interface to the 14.2.6.0/24 network
ip address 14.2.6.250 255.255.255.0
ip access-group 102 in
!
router ospf 44
network 14.1.0.0 0.0.255.255 area 0
network 14.2.6.0 0.0.0.255 area 1
!
! access-list 75 applies to hosts allowed to gather SNMP info
! from this router
no access-list 75
access-list 75 permit host 14.2.6.6
access-list 75 permit host 14.2.6.18
!
! access-list 100 applies to traffic from external networks
```

```
! to the internal network or to the router
no access-list 100
access-list 100 deny ip 14.2.6.0 0.0.0.255 any log
access-list 100 deny ip host 14.1.1.20 host 14.1.1.20 log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny ip any host 14.2.6.255 log
access-list 100 deny ip any host 14.2.6.0 log
access-list 100 permit tcp any 14.2.6.0 0.0.0.255 established
access-list 100 deny icmp any any echo log
access-list 100 deny icmp any any redirect log
access-list 100 deny icmp any any mask-request log
access-list 100 permit icmp any 14.2.6.0 0.0.0.255
access-list 100 permit ospf 14.1.0.0 0.0.255.255 host 14.1.1.20
access-list 100 deny tcp any any range 6000 6009 log
access-list 100 deny tcp any any eq 6667 log
access-list 100 deny tcp any any range 12345 12346 log
access-list 100 deny tcp any any eq 31337 log
access-list 100 permit tcp any eq 20 14.2.6.0 0.0.0.255 gt 1023


access-list 100 deny udp any any eq 2049 log
access-list 100 deny udp any any eq 31337 log
access-list 100 deny udp any any range 33400 34400 log
access-list 100 permit udp any eq 53 14.2.6.0 0.0.0.255 gt 1023
access-list 100 deny tcp any range 0 65535 any range 0 65535 log
access-list 100 deny udp any range 0 65535 any range 0 65535 log
access-list 100 deny ip any any log
!
! access-list 102 applies to traffic from the internal network
! to external networks or to the router itself
no access-list 102
access-list 102 deny ip host 14.2.6.250 host 14.2.6.250 log
access-list 102 permit icmp 14.2.6.0 0.0.0.255 any echo
access-list 102 permit icmp 14.2.6.0 0.0.0.255 any parameter-problem
access-list 102 permit icmp 14.2.6.0 0.0.0.255 any packet-too-big
```

```
access-list 102 permit icmp 14.2.6.0 0.0.0.255 any source-quench
access-list 102 deny tcp any any range 1 19 log
access-list 102 deny tcp any any eq 43 log
access-list 102 deny tcp any any eq 93 log
access-list 102 deny tcp any any range 135 139 log
access-list 102 deny tcp any any eq 445 log
access-list 102 deny tcp any any range 512 518 log
access-list 102 deny tcp any any eq 540 log
access-list 102 permit tcp 14.2.6.0 0.0.0.255 gt 1023 any lt 1024
access-list 102 permit udp 14.2.6.0 0.0.0.255 gt 1023 any eq 53
access-list 102 permit udp 14.2.6.0 0.0.0.255 any range 33400 34400 log
access-list 102 deny tcp any range 0 65535 any range 0 65535 log
access-list 102 deny udp any range 0 65535 any range 0 65535 log
access-list 102 deny ip any any log
!
! access-list 150 applies to remote access from specific hosts
! (14.2.6.10, 14.2.6.11 and 14.2.6.12) to the router itself
no access-list 150
access-list 150 permit tcp host 14.2.6.10 host 0.0.0.0 eq 23 log
access-list 150 permit tcp host 14.2.6.11 host 0.0.0.0 eq 23 log
access-list 150 permit tcp host 14.2.6.12 host 0.0.0.0 eq 23 log
access-list 150 deny ip any any log
!
snmp-server community n3t-manag3m3nt ro 75
! line vty 0 4
access-class 150 in
password 7 123456789012345678901234
login
transport input telnet
```

第六章　結語

網路安全一直是一門相當重要的課題，而對於網路攻擊的研究是網路安全中相當重要的一環。路由器是公司內部網路與外界網路的溝通橋樑，他負責封包轉送的工作，也可以讓封包傳遞路徑更為有效率，較為高級的機種甚至擁有 VPN，防火牆、等其他更特別的功能。當然，由於路由器處在網路的咽喉處，他的安全性就更加重要，比起花大量時間去研究與攻擊內部網路，惡意攻擊者將會更有興趣直接對路由器下手，造成整個內部網路癱瘓。目前為止，中華民國網路安全危機處理中心 (GSN-CERT/CC) 已經公布了許多針對路由器這類網路硬體設備攻擊的案例，所以不能忽視路由器安全這個重要的環節。

路由器操作基本安全手則：

1. 路由器的放置位置要安全，最好放在上鎖的機櫃裡。
2. 所有對路由器的操作都應該在 Local 端，使用 AUX port 去設定 Router。
3. 只限制某些機器才能做 Telnet 的連線(使用 Access List Control)。
4. 不使用 WEB 介面來操作路由器。
5. 限制從外界網路對路由器做設定。
6. 在 Type 7 Password 下使用"service password encryption"，以避免密碼在直接瀏覽設定檔時就被看到。
7. 在"Privileged EXEC Mode"使用 MD5 Encryption，即" enable secret"命令。
8. AUX 及 console port 上都要使用 EXEC 密碼。
9. 避免在一塊網路介面上的 inbound 及 outbound 上使用 RIP 及 OSPF。
10. 如果使用 Cisco 路由器請把所有介面停用 CDP(Cisco Discovery Protocol)。
11. 盡量少使用 SNMP 及 Web 介面。
12. 如果使用 Cisco 路由器，它提供了另一種系統 Terminal Access Controller Access Control System (TACACS).可加強路由器登入認證時的安全。

下列列出應該盡量避免穿過路由器的服務：

GSN-CERT/CC 所建議應該過濾掉下列的服務		
Service	**Port Type**	**Port Number**
除了外面第二個 DNS 伺服器之 DNS Zone transfers	TCP	53
TFTP daemon	UDP	69
Link	TCP	87
SUN RPC	TCP & UDP	111
BSD UNIX	TCP	512 through 514
LPD	TCP	515
UUCPD	TCP	540
Open Windows	TCP & UDP	2000
NFS	TCP & UDP	2049
X Windows	TCP & UDP	6000+ (to 6255)

總結本研究計畫的結果，對於路由器的安置，提供三方面的建議：

1. 路由器硬體設備

為了提高路由器在硬體設備方面的安全性，機房必須不受電場和磁場的干擾。機房應該要有溫度及濕度控制器，而設置一台不斷電電源供應器為提高路由器的穩定性。如果要防禦阻斷式攻擊及支援更廣大的安全服務，路由器必須設成使用最多記憶體資源。此外，也要設成只有少數人才能夠進出機房。最後，所有跟路由器有連結的設備必有存儲的防護。

2. 路由器作業系統

作業系統是一個非常重要的路由器元件，它會影響到路由器的功能。不

過最新版本的作業系統也不能保證它的可靠性 。 所以使用者必須選出最適合他要求而最新 Stable 版的作業系統當路由器的作業系統 。

3. 路由器設定值

類似其他電腦主機 ， 路由器安裝完的時候會有很多服務預設被打開 。 但是很多服務是不必要打開的，而攻擊者很喜歡使用預設服務的漏洞來攻擊路由器 。 所在此建議把不必要的預設服務關掉，避免受到不友善的攻擊。

參考資料

通信協定相關 RFC ：

- http://www.rfc-editor.org/rfc.html

網路安全相關網站 ：

- http://bugtraq.inet-one.com
- http://carnap.ss.uci.edu
- http://cat.ice.ntnu.edu.tw
- http://cert.uni-stuttgart.de
- http://cio.cisco.com
- http://packetstorm.decepticons.org
- http://spisa.act.uji.es
- http://the.wiretapped.net
- http://www.ciac.org
- http://www.codetalker.com
- http://www.cve.mitre.org
- http://www.freesoft.org
- http://www.guardent.com
- http://www.ieng.com
- http://www.ietf.org
- http://www.insecure.org
- http://www.isi.edu
- http://www.netspace.org
- http://www.netsys.com
- http://www.networkcomputing.com
- http://www.networkice.com
- http://www.nipc.gov
- http://www.nta-monitor.com
- http://www.pgp.com
- http://www.safermag.com
- http://www.securiteam.com
- http://www.securityfocus.com
- http://xforce.iss.net