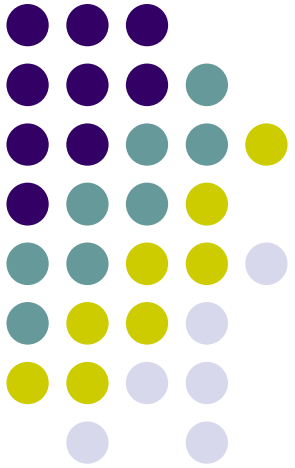
實驗22 NetSim－Cisco存取規則清單

實驗目的：

- 明瞭Cisco安全管理法則
- 建立ACLs－Standard、Extended



背景資料

- Access List（存取規則清單）或Access Control List(ACL)是網路安全中的一項必要功能，當網路規模還很小時，常會使用密碼來允許使用者得到設備的權限，但如果網路規模愈來愈大時，網路管理者會開始面臨到存取上的管理問題，而Access List就是用來解決大中型網路上存取關係問題的方式。
- 當Access List功能啟動之後，如果有個封包進入路由器時，路由器所扮演的不再只是轉送的角色而已，而是要經過Access List的測試，才可以轉送出去，假若無法通過Access List中的存取規則，該封包就會被丟棄（drop）。

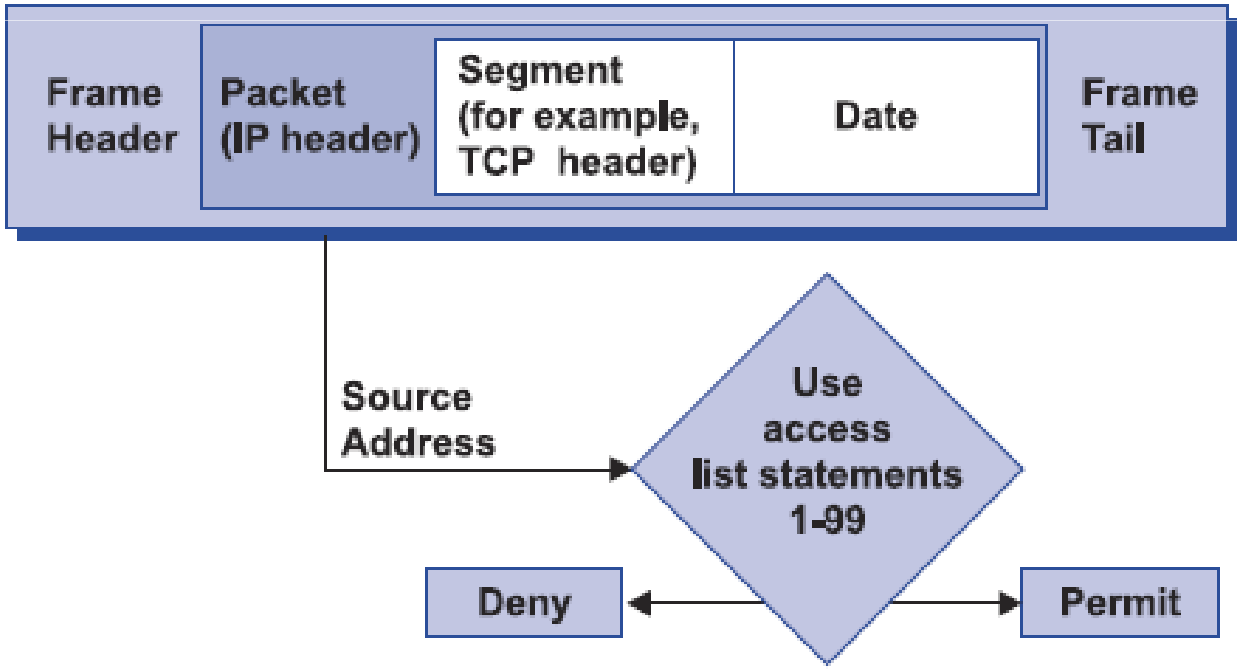
IP存取列表

- IP網路環境中，我們使用IP存取列表有分成IP標準的存取列表（IP Standard Access Lists）及IP延伸的存取列表（IP extended Access Lists），範圍如下表所示。

存取規則清單	範圍
IP標準存取列表	1~99
IP延伸存取列表	100~199

標準的IP存取列表

- 標準的IP存取列表如圖示，只有比對封包的來源位址，然後進行允許(permit)或拒絕(deny)的限制動作。

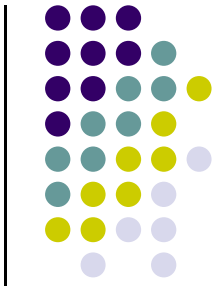


標準的IP存取列表

- 標準的IP存取列表的語法，如下所示：

  access-list access-list-number {permit|deny} source [wildcard mask]
- access-list是主要的指令，而後面的參數說明如下：
  - access-list-number：存取列表的號碼，標準的IP存取列表號碼是1~99。
  - permit|deny：指定這條規則是[允許|拒絕]。
  - source：要使用這條規則的來源IP位址。
  - wildcard mask：通配遮罩，0是進行檢查，1是不檢查。

通配遮罩 (wildcard mask)



- 範例一：source：192.192.73.120
  - Wildcard mask：0.0.0.0，代表每個位元都必需符合，此規則只針對192.192.73.120。
- 範例二：source：192.192.73.0
  - Wildcard mask：0.0.0.255，代表後面的256個位置會符合規則，也就是192.192.73.0~192.192.73.255都符合。

標準的IP存取列表

- 在訪問列表的最後有一條隱含聲明：**deny any**，即使並沒有設定，所以每一條正確的訪問列表都至少應該有一條允許語句。

通配遮罩

- 通配遮罩用來設定個別的主機、網路區塊、或特定範圍的一個網路或多個網路，和子網路遮罩不同的是它並不需要連續的0再接上連續的1，其中0是進行檢查，1是不檢查，例如0.0.0.19(00010011)，表示不檢查最後第5,2,1位元，不過除非是考試需要否則一般並不會如此設定，底下用一些實用範例來說明通配遮罩的設定。

通配遮罩

- 個別的主機
  - 標準存取列表
    - Access-list 1 permit 192.168.1.1 0.0.0.0
    - Access-list 1 permit 192.168.1.1(標準存取列表預設值 0.0.0.0)
    - Access-list 1 permit **host** 192.168.1.1
  - 延伸存取列表
    - Access-list 101 permit ip 192.168.1.1 0.0.0.0 any
    - Access-list 101 permit ip host 192.168.1.1 any

通配遮罩

- 全部子網路：

  Wildcard mask = 255.255.255.255 – subnet mask

  範例一：子網路192.168.1.0 subnet mask 255.255.255.0

  255.255.255.255

  - subnet mask 255.255.255. 0

  Wildcard mask 0. 0. 0. 255

  答案：Access-list 1 permit 192.168.1.1 0.0.0.255

通配遮罩

範例二：子網路192.168.1.0 subnet mask 255.255.255.224

255.255.255.255

- subnet mask 255.255.255.224

Wildcard mask 0. 0. 0. 31

答案：Access-list 1 permit 192.168.1.0 0.0.0.31

範例三：子網路172.16.1.0 subnet mask 255.255.192.0

255.255.255.255

- subnet mask 255.255.192. 0

Wildcard mask 0. 0. 63.255

答案：Access-list 1 permit 172.16.1.0 0.0.63.255

通配遮罩

範例四：子網路192.168.1.0 subnet mask 255.255.255.240

255.255.255.255

- subnet mask 255.255.255.240

Wildcard mask 0. 0. 0. 15

答案：Access-list 1 permit 192.168.1.0 0.0.0.15

通配遮罩

- 特定範圍：

  範例一：網路範圍192.168.16.0 – 192.168.31.255

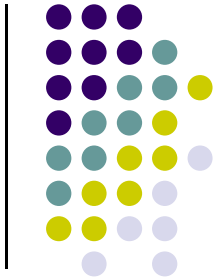
  192.168. 31.255

  - subnet mask 192.168. 16. 0

  Wildcard mask 0. 0. 15. 255

  答案：Access-list 1 permit 192.168.16.0 0.0.15.255

通配遮罩



範例二：網路範圍192.168.16.32 – 192.168.31.63

192.168. 31. 63

- subnet mask 192.168. 16. 32

Wildcard mask 0. 0. 15. 31

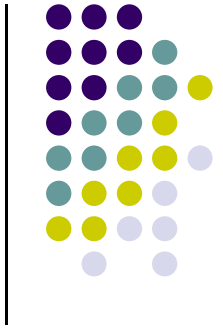
答案：Access-list 1 permit 192.168.16.32 0.0.15.31

- 全部：

Access-list 1 permit any

Access-list 1 permit 0.0.0.0 255.255.255.255

啟動Access List



- 設定好存取列表的規則後，我們必需在指定的介面上啟動列表才算完成設定。啟動的語法如下所示：

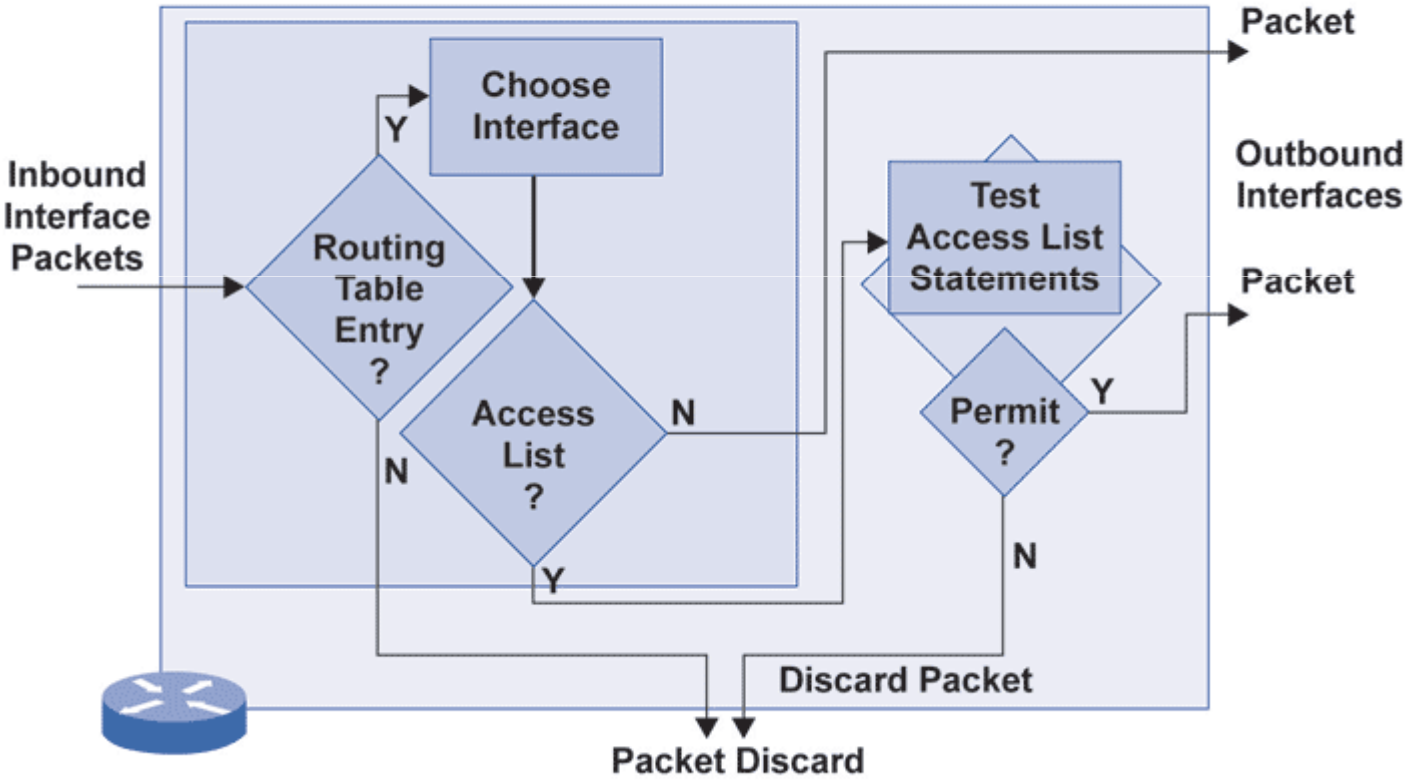
  ip access-group access-list-number {in | out}

  - ip access-group是主要指令，其後面的參數說明如下：
    - access-list-number：是已設定好的存取列表編號。
    - in/out：in是進入介面，out是從介面輸出，預設是out。

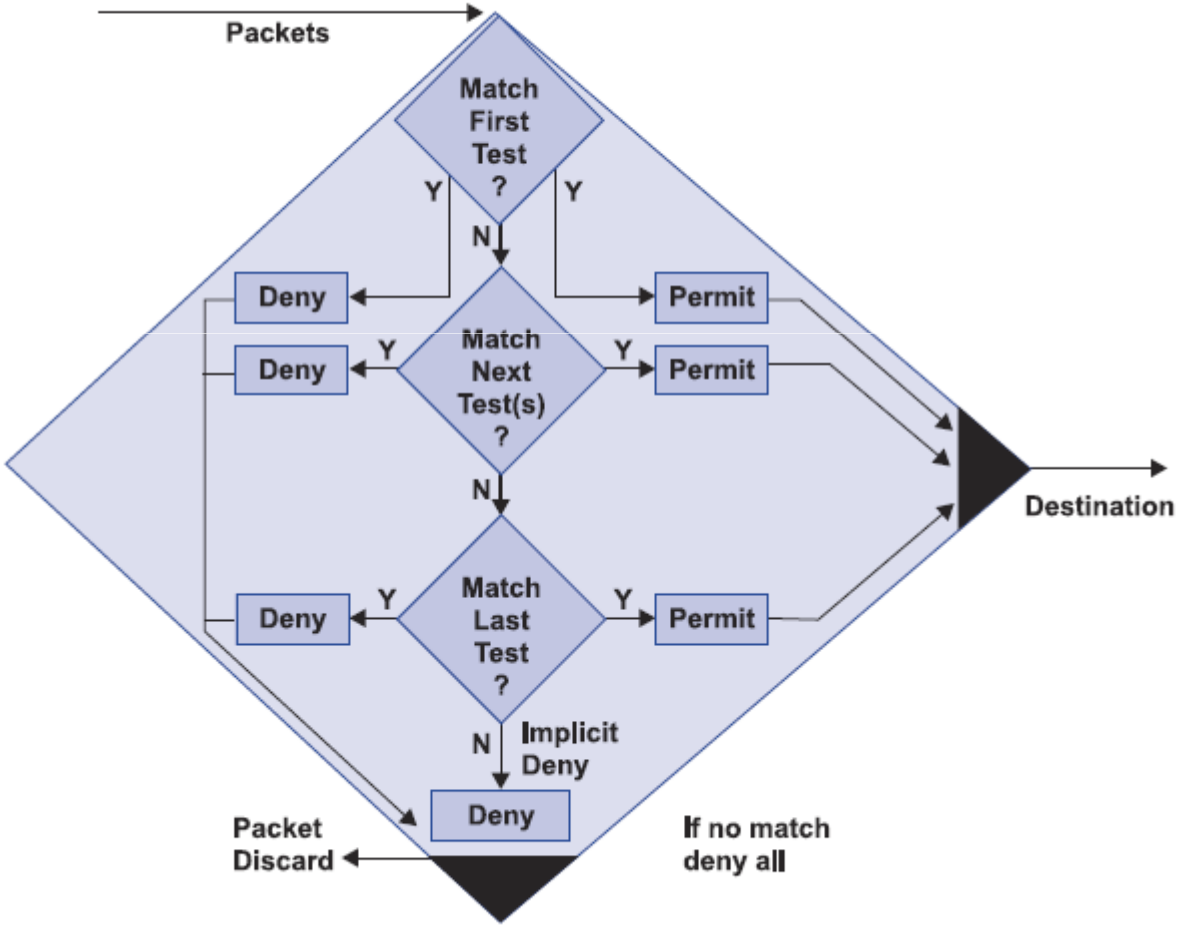
路由器有ACL的封包處理流程

- 路由器待處理的封包數量眾多，所以增加ACL會增加路由器的負擔，有時會建議使用專用防火牆來過濾封包。

路由器有ACL的封包處理流程



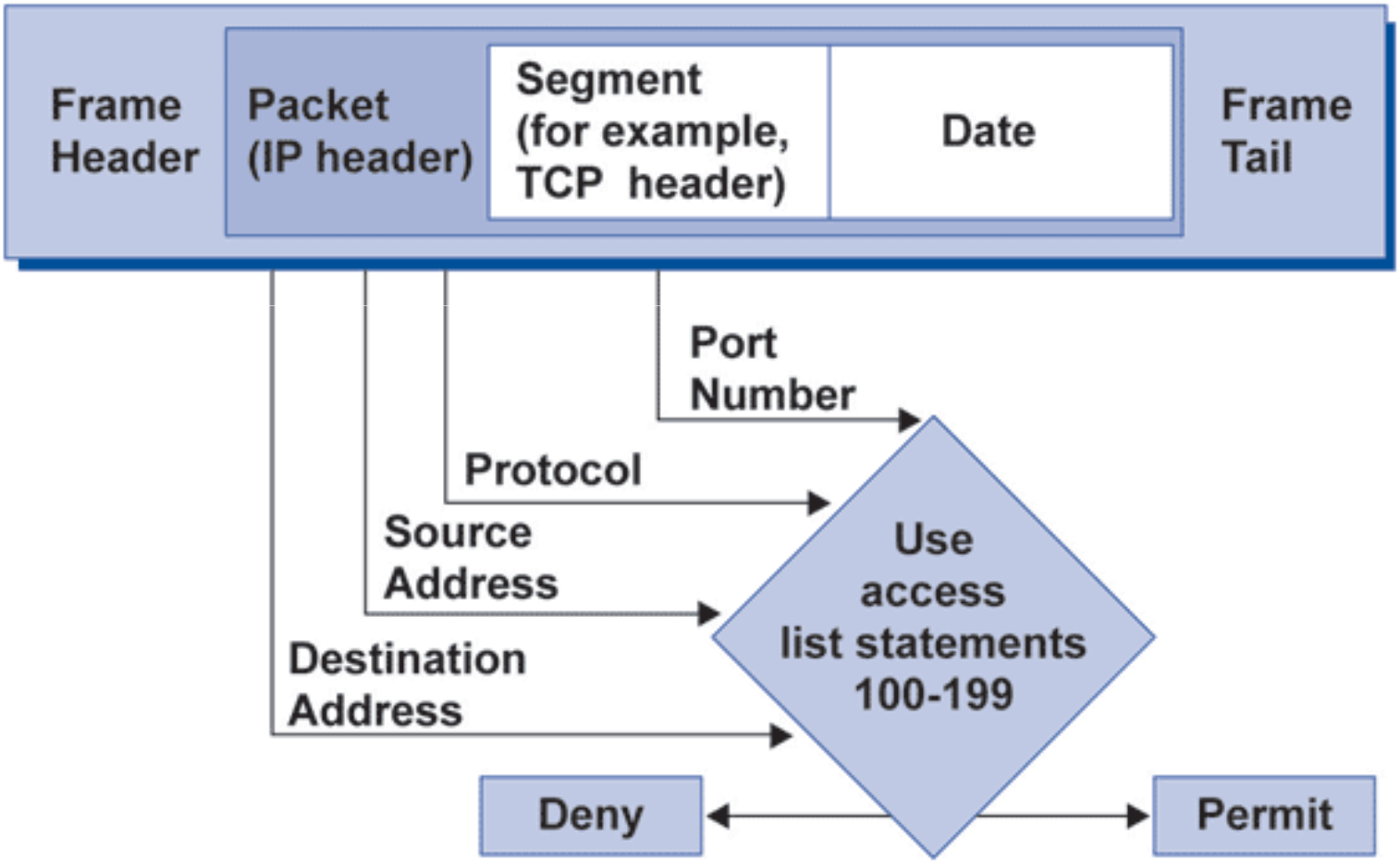
路由器有ACL的封包處理流程



延伸的IP存取列表

- IP延伸存取列表，顧名思義，就是IP標準存取列表的進階版本。IP延伸存取列表如圖示，可以使用較多的控制參數，比對封包的來源位址、目的位址、埠號和協定，然後進行允許(permit)或拒絕(deny)的限制動作。

延伸的IP存取列表

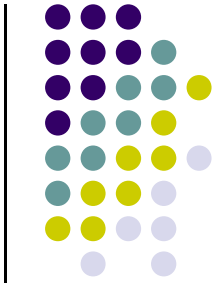

Frame Header
Packet (IP header)
Segment (for example, TCP header)
Date
Frame Tail
Port Number
Protocol
Source Address
Destination Address
Use access list statements 100-199
Deny
Permit

延伸的IP存取列表

- 延伸的IP存取列表的語法如下所示：

  access-list access-list-number {permit | deny} protocol source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [log]

延伸的IP存取列表



- 其中access-list是主要的指令，而後面的參數說明如下：
  - access-list-number：存取列表的號碼，延伸的IP存取列表號碼是100~199。
  - permit|deny：指定這條規則是[允許|拒絕]。
  - protocol：可以使用的協定，有tcp、udp、IP、ICMP、IGRP、EIGRP、OSPF等。
  - source source-wildcard：來源位址的IP。source-wildcard是用來辨識來源IP位址是否符合我們想要制定的規則，當source-wildcard為1時忽略不檢查，若為0則是需要檢查，用法和標準存取列表相同，而any是代表任何來源的IP封包，也就是0.0.0.0 255.255.255.255。
  - destination destination-wildcard：目的位址的IP，和source source-wildcard的用法一樣。
  - operator port：協定指定的選項。
  - log：記錄有關封包進入存取列表的資訊。

延伸的IP存取列表

- access-list 101 permit tcp 192.168.1.16 0.0.0.15 any eq telnet
- access-list 102 permit ip 192.168.2.0 0.0.0.15 any
- access-list 101 deny tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
- access-list 101 deny tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
- access-list 101 permit ip any any

實驗方法

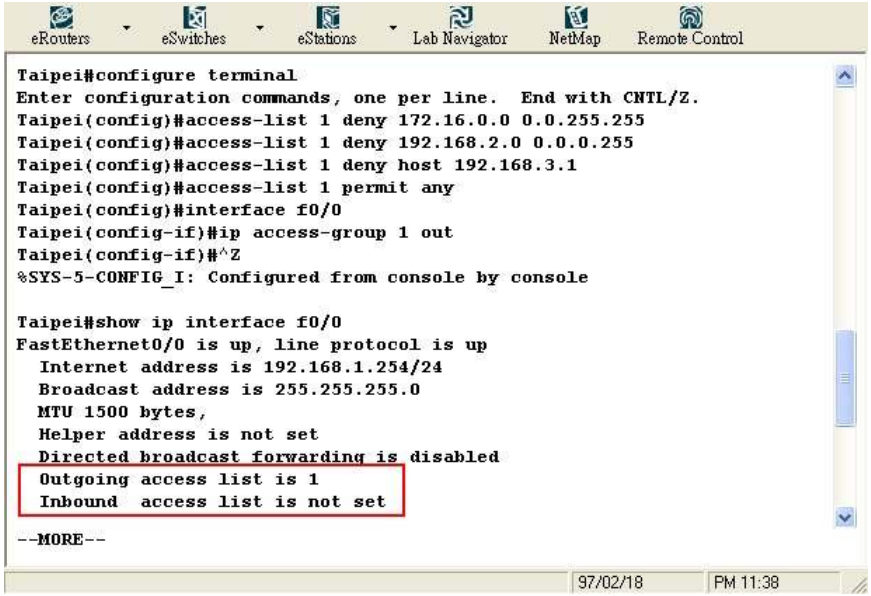
- 實驗要求：不允許172.16.0.0/16, 192.168.2/0, 192.168.3.1連線至PC1。

首先建立存取列表

- (config)#access-list 1 deny 172.16.0.0 0.0.255.255
- (config)#access-list 1 deny 192.168.2.0 0.0.0.255
- (config)#access-list 1 deny host 192.168.3.1
- (config)#**access-list 1 permit any**

標準存取列表

- 啟動這條規則，並可用『show ip interface f0/0』來驗證，過程如下所示：
  - (config)#interface f0/0
  - (config-if)#ip access-group 1 out



延伸存取列表

- 實驗要求：新竹(Router 2)只允許由高雄(Router 3)來telnet。
- 路由器要使用telnet命令來被遠端虛擬終端控制的話，其路由器需在vty上設有密碼，本實驗要求新竹(Router 2)可被telnet，相關命令請參考實驗十六。

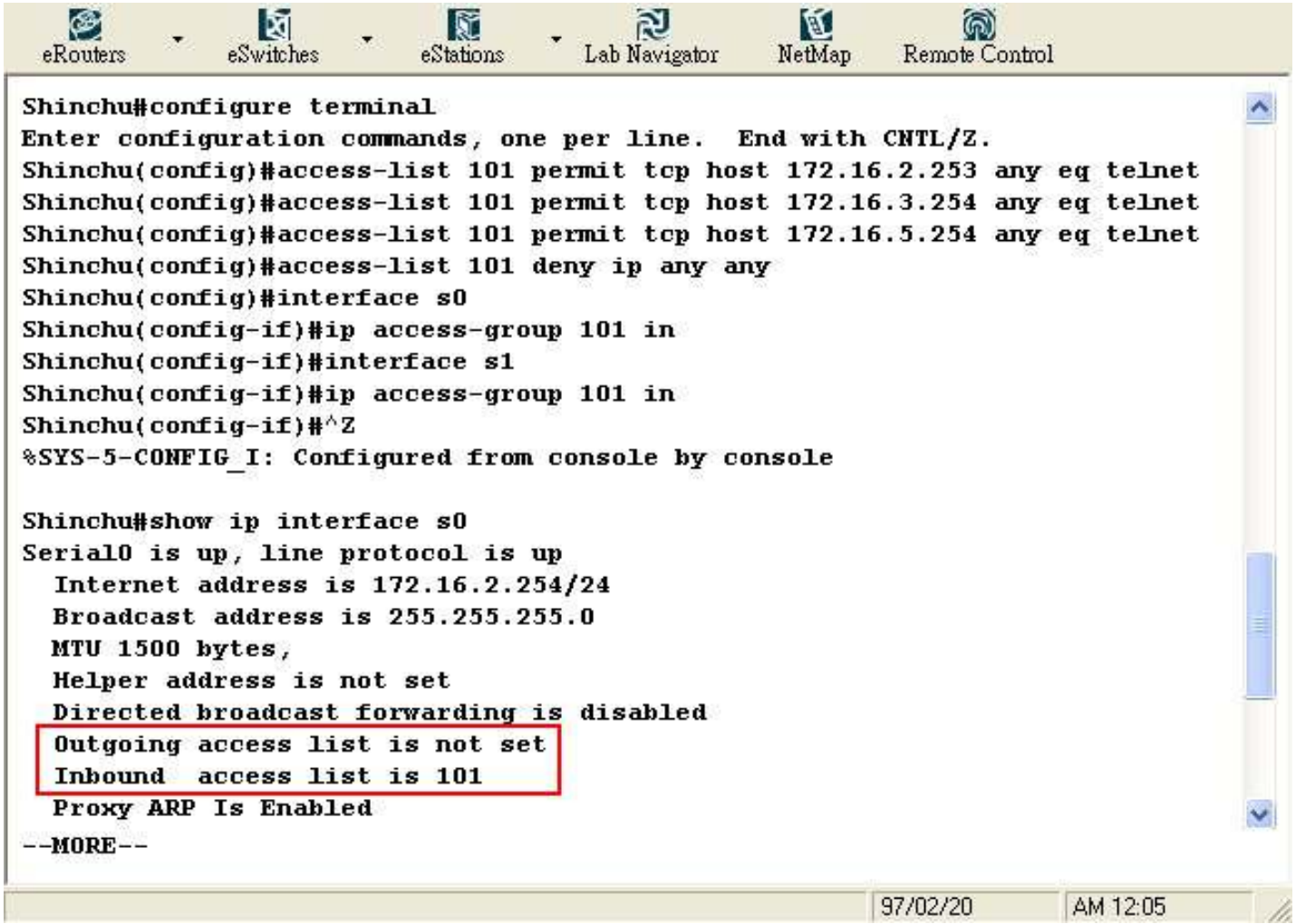
首先建立存取列表

- (config)#access-list 101 permit tcp host 172.16.2.253 any eq telnet
- (config)#access-list 101 permit tcp host 172.16.3.254 any eq telnet
- (config)#access-list 101 permit tcp host 172.16.5.253 any eq telnet
- (config)#access-list 101 deny tcp any any eq telnet
- (config)#**access-list 101 permit ip any any**

延伸存取列表

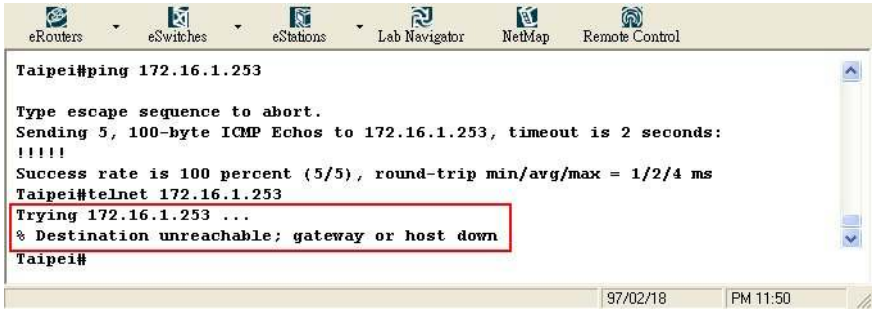
- 啟動這條規則，並可用『show ip interface f0/0』來驗證，過程如下所示：
  - (config)#interface s0
  - (config-if)#ip access-group 101 in
  - (config-if)#interface s1
  - (config-if)#ip access-group 101 in

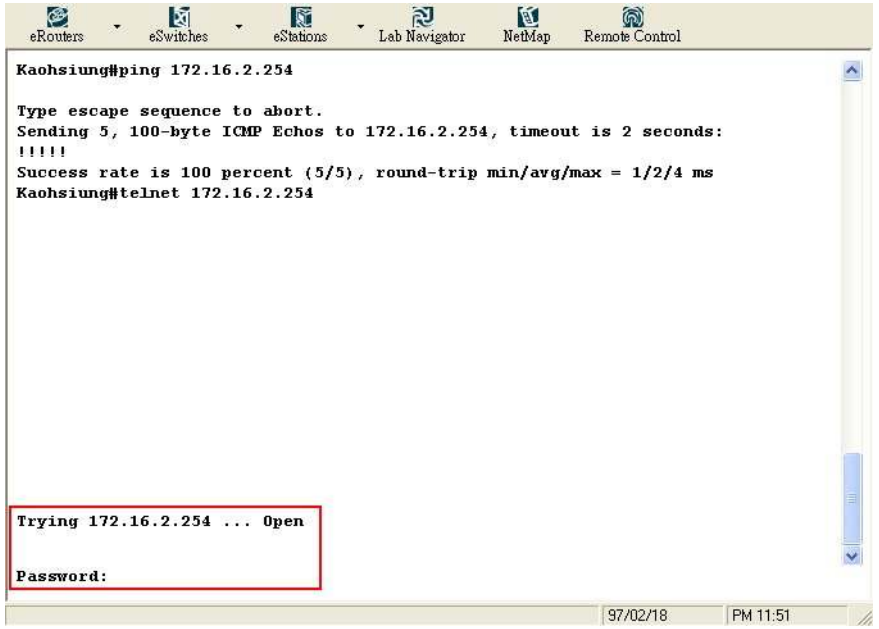
延伸存取列表


eRouters
eSwitches
eStations
Lab Navigator
NetMap
Remote Control
Shinchu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Shinchu(config)#access-list 101 permit tcp host 172.16.2.253 any eq telnet
Shinchu(config)#access-list 101 permit tcp host 172.16.3.254 any eq telnet
Shinchu(config)#access-list 101 permit tcp host 172.16.5.254 any eq telnet
Shinchu(config)#access-list 101 deny ip any any
Shinchu(config)#interface s0
Shinchu(config-if)#ip access-group 101 in
Shinchu(config-if)#interface s1
Shinchu(config-if)#ip access-group 101 in
Shinchu(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Shinchu#show ip interface s0
Serial0 is up, line protocol is up
Internet address is 172.16.2.254/24
Broadcast address is 255.255.255.0
MTU 1500 bytes,
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 101
Proxy ARP Is Enabled
--MORE--
97/02/20
AM 12:05

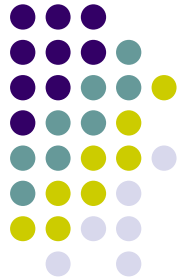
延伸存取列表

- 接下來分別使用台北(Router 1)和高雄(Router 3)對新竹(Router 2) telnet來驗證。





延伸存取列表



- 實驗要求：高雄(Router 3)不允許PING。

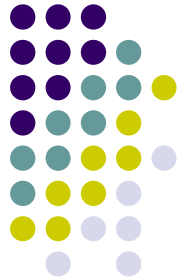
首先建立存取列表

- (config)#access-list 101 deny icmp any any
- (config)#**access-list 101 permit ip any any**

接下來，啟動這條規則，過程如下所示：

- (config-if)#interface s0
- (config-if)#ip access-group 101 in
- (config-if)#interface s1
- (config-if)#ip access-group 101 in
- (config-if)#interface s2
- (config-if)#ip access-group 101 in
- (config-if)#interface f0/0
- (config-if)#ip access-group 101 in

名稱式存取清單



- 名稱式存取清單不是另外種類存取清單，僅是一種產生標準與延伸式存取清單的方法，名稱式存取清單可用名稱來產生，讓我們以較有意義的方式來參考，這存取清單沒有任何新的或不同的意義，命令如下：

  ip access-list {extended |logging | standard} ***access-list-name***

- 啟動名稱式存取清單的語法如下所示：

  ip access-group ***access-list-name*** {in | out}

學習評量

1. 說明建立存取列表的目的。
2. 說明標準存取列表的範圍。
3. 說明伸存取列表的範圍。
4. any所代表的位址為何？
5. 說明哪個指令是指啟動存取列表？
6. 說明何謂Source-wildcard？該如何計算？
7. 說明存取列表和防火牆是否相同？
8. 說明TCP和UDP常用的port號為何？
9. 說明標準存取列表和延伸存取列表的差異性。
10. 在延伸存取列表的實驗中，新竹(Router 2)只允許由高雄(Router 3)來telnet，除實驗範例外有沒有其它的指定方式？