設定常用的 IP ACL

目錄

簡介

本檔案介紹常用IP存取控制清單(ACL)的組態範例，這些清單會篩選IP封包。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 對 IP 定址有基礎認識

請參閱[新使用者的 IP 定址和子網路劃分以瞭解其他資訊 。](#)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IP存取控制清單根據以下條件篩選封包：

- 來源位址
- 目的地位址
- 封包類型
- 以上項目的任意組合

為了過濾網路流量，ACL 會控制是否在路由器介面上轉送或封鎖路由的封包。您的路由器會檢查每個封包，以根據您在 ACL 中指定的標準來決定轉送或捨棄封包。ACL 標準包括：

- 流量的來源位址
- 流量的目的地位址
- 上層通訊協定

完成以下步驟即可建構如本文件所示範例的 ACL：

1. 建立 ACL。
2. 將 ACL 套用至介面。

IP ACL 是套用至 IP 封包之 permit 和 deny 條件的循序集合。路由器會根據 ACL 中的條件來逐一測試封包。

第一個符項目會判斷 Cisco IOS® 軟體要接受或拒絕封包。因為Cisco IOS軟體會在第一個相符專案出現後停止條件測試，所以條件的順序非常重要。如果沒有相符的條件，路由器就會基於隱含的 deny all 子句而拒絕封包。

以下是可以在 Cisco IOS 軟體中設定的 IP ACL 範例：

- 標準型 ACL
- 延伸型 ACL
- 動態（鎖鑰型） ACL
- IP 命名型 ACL
- 自反型 ACL
- 使用時間範圍的時間型 ACL
- 備註型 IP ACL 項目
- 內容型 ACL
- 驗證代理
- 增強型 ACL
- 分散式時間型 ACL

本文件將討論一些常用的標準型和延伸型 ACL。請參閱設定 IP 存取清單，以取得更多有關 Cisco IOS 軟體支援之不同類型 ACL 以及如何設定和編輯 ACL 的資訊。

標準型ACL的命令語法格式為**access-list access-list-number {permit|deny} {host|source source-wildcard|any}**。

標準型 ACL 會將 IP 封包的來源位址與 ACL 中設定的位址進行比較，以便控制流量。

延伸型 ACL 會將 IP 封包的來源和目的地位址與 ACL 中設定的位址進行比較，以便控制流量。您也可以將延伸型 ACL 設定得更精細，並設定為依照標準過濾流量，例如：

- 通訊協定
- 連接埠號碼
- 區別服務代碼點 (DSCP) 值
- 優先順序值
- 同步序號 (SYN) 位元的狀態

延伸型 ACL 的命令語法格式為：

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

網際網路控制訊息通訊協定 (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

傳輸控制通訊協定 (TCP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[established] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

使用者資料包通訊協定 (UDP)

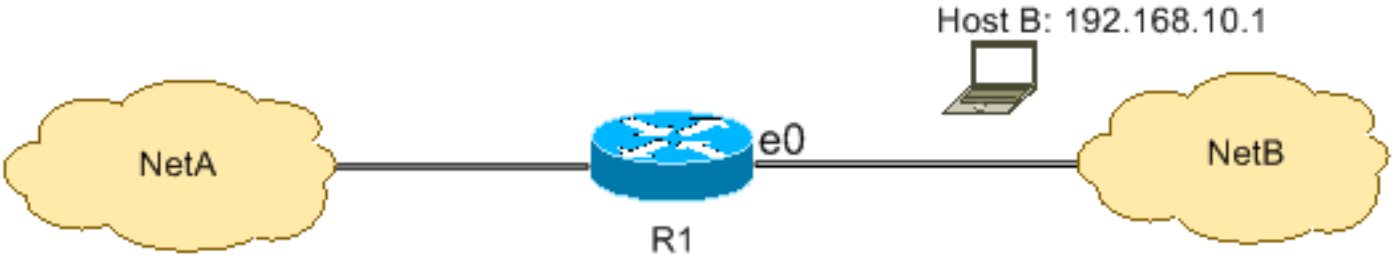
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name][fragments]
```

設定

這些組態範例使用的是最常見的 IP ACL。

允許特定主機存取網路

下圖顯示特定主機獲得存取網路的許可權。來源為主機 B 且目的地為 NetA 的所有流量允許通過，而來源為 NetB 且目的地為 NetA 的所有其他流量則遭到拒絕。



R1 表上的輸出顯示了網路如何對主機授予存取權限。此輸出顯示：

- 此組態僅允許 IP 位址為 192.168.10.1 的主機通過 R1 的乙太網路 0 介面。
- 此主機擁有對 NetA 的 IP 服務存取權限。
- NetB 中的任何其他主機都無法存取 NetA。
- ACL 中未設定 deny 陳述式。

預設情況下，每個 ACL 的結尾都有一個隱含的 deny all 子句。任何未明確允許的內容均會遭到拒絕。

R1

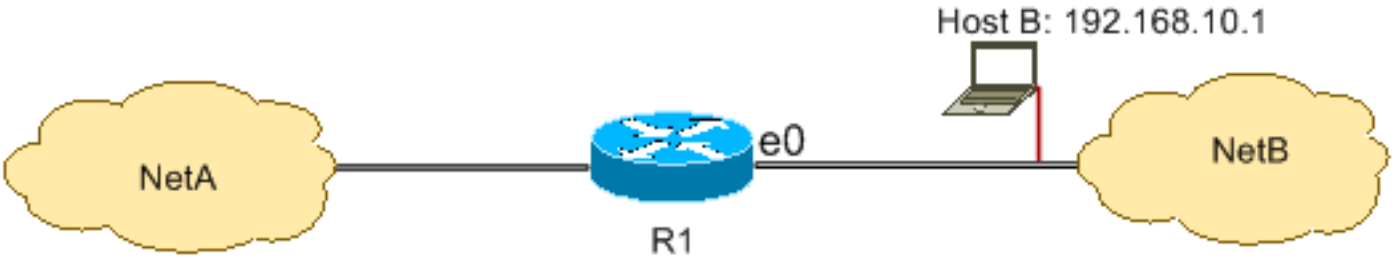
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

註:ACL會過濾從NetB到NetA的IP封包，但來源為主機B的封包除外。仍會允許來源為主機B到NetA的封包。

附註：ACL **access-list 1 permit 192.168.10.1 0.0.0.0 是設定相同規則的另一種方式。**

拒絕特定主機存取網路

下圖顯示，來源為主機 B 且目的地為 NetA 的流量會遭到拒絕，但是從 NetB 到 NetA 的所有其他流量都允許通過。



此組態會拒絕來自主機 192.168.10.1/32 的所有封包通過 R1 的乙太網路 0，但允許所有其他封包通過。因為每個 ACL 都有一個隱含的 deny all 子句，您必須使用命令 **access list 1 permit any 來明確允許所有其他封包。**

R1

```
hostname R1
```

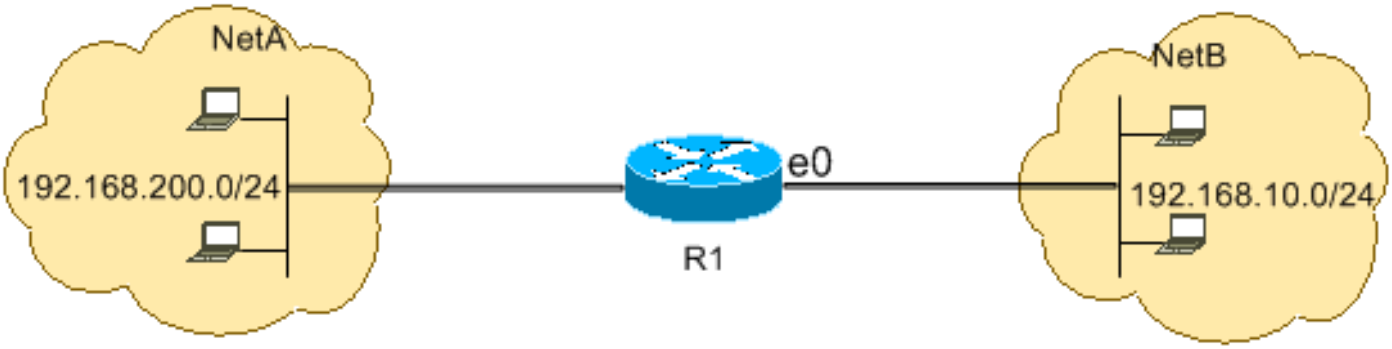
```
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

附註：陳述式的順序對於 ACL 的運作至關重要。如果項目的順序顛倒（如以下命令所示），第一行就會比對每個封包的來源位址。因此，ACL 就無法阻擋主機 192.168.10.1/32 存取 NetA。

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

允許存取連續範圍的 IP 位址

下圖顯示，NetB 中網路位址為 192.168.10.0/24 的所有主機都可以存取 NetA 中的網路 192.168.200.0/24。



此組態會允許 IP 標頭中來源位址在網路 192.168.10.0/24 內、目的地為只在網路 192.168.200.0/24 內的 IP 封包存取 NetA。此 ACL 結尾有隱含的 deny all 子句，因此會拒絕所有其他流量經由 R1 的乙太網路 0 傳入。

R1

```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

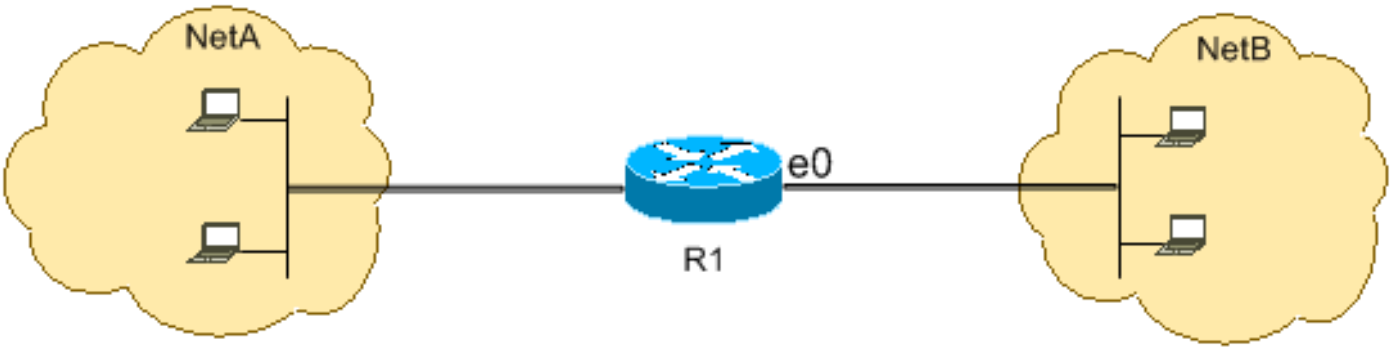
附註：在命令**access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255**中，「0.0.0.255」是網路192.168.10.0（遮罩為255.255.255.0）的反向遮罩。ACL會使用反向遮罩來瞭解網路位址中有多少位元需要比相符。在上表中，ACL 會允許來源位址在 192.168.10.0/24 網路中、目的地位址在 192.168.200.0/24 網路之所有主機的封包。

請參閱設定 IP 存取清單的遮罩區段，以取得更多有關網路位址遮罩的資訊，並瞭解如何計算 ACL 所需的反向遮罩。

拒絕 Telnet 流量（TCP，連接埠 23）

為了滿足更高的資安標準，您可以停用公用網路對您私人網路的Telnet存取許可權。下圖顯示從

NetB（公用）到 NetA（私人）的 Telnet 流量如何遭到拒絕（但允許 NetA 對 NetB 發起和建立 Telnet 作業階段），而允許所有其他 IP 流量。



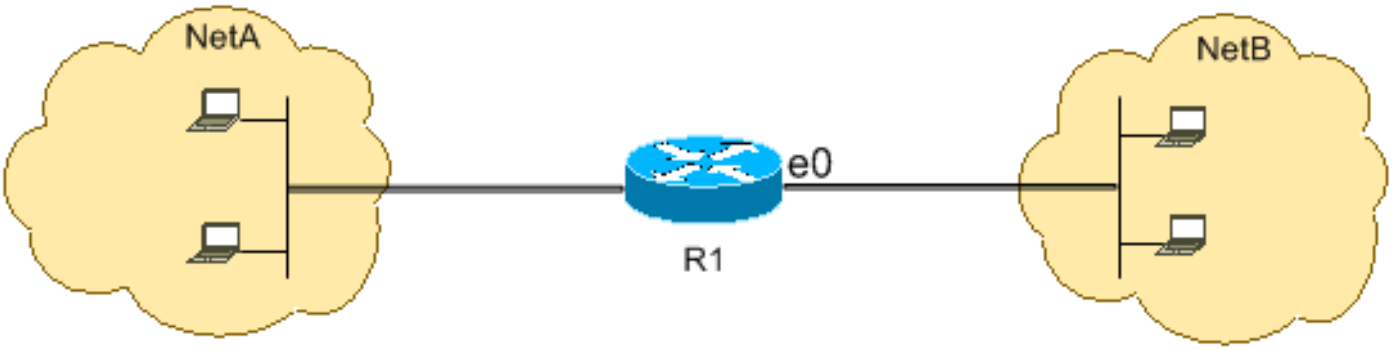
Telnet會使用TCP，連線埠23。此組態顯示，所有目的地為NetA連線埠23的所有TCP流量都會遭到封鎖，但允許所有其他IP流量通過。

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

僅允許內部網路發起 TCP 作業階段

下圖顯示，來源為 NetA 且目的地為 NetB 的 TCP 流量會允許通過，但來源為 NetB 且目的地為 NetA 的 TCP 流量會遭到拒絕。



在此範例中，ACL 的用途如下：

- 允許 NetA 中的主機向 NetB 中的主機發起和建立 TCP 作業階段。
- 拒絕 NetB 中的主機向 NetA 中的主機發起和建立 TCP 作業階段。

此組態會允許資料包透過 R1 的介面乙太網路 0 傳入，但資料包必須符合以下條件：

- 已確認(ACK)或重設(RST)位元集（表示已建立TCP作業階段）
- 目的地連接埠值大於 1023

R1

```
hostname R1
```

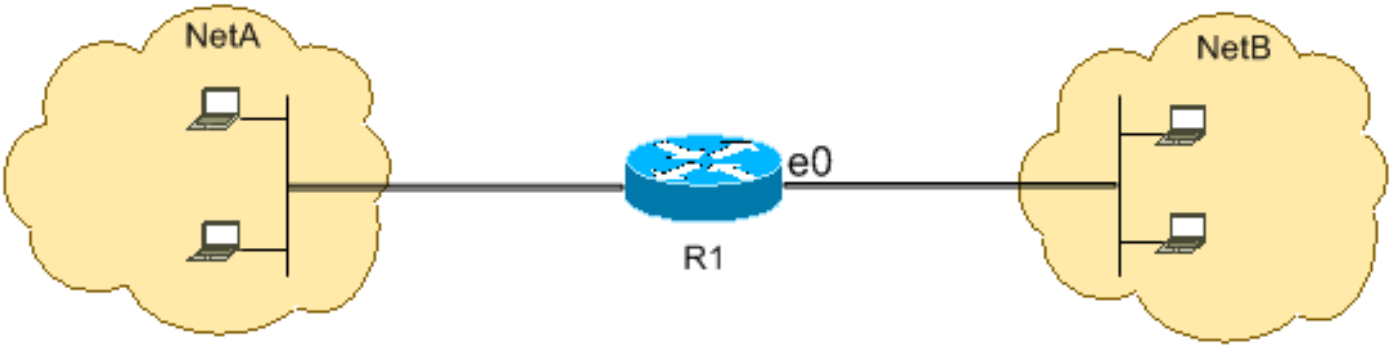
```
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

由於大多數IP服務的公認連線埠使用的值小於1023，因此ACL 102會拒絕目的地連線埠小於1023或未設定ACK/RST位元的任何資料包。因此，NetB的主機發起TCP連線並傳送第一個連線包(未設定同步/啟動封包(SYN/RST)位元)至小於1023的連線埠號碼時，就會遭到拒絕，且TCP作業階段會失敗。從 NetA 發起且目的地為 NetB 的 TCP 作業階段會獲得允許，因為它們已針對傳回封包設定 ACK/RST 位元，而且使用的連接埠值大於 1023。

請參閱 RFC 1700 以取得完整的連接埠清單。

拒絕 FTP 流量（TCP，連接埠 21）

下圖顯示，來源為 NetB 且目的地為 NetA 的 FTP（TCP，連接埠 21）和 FTP 資料（連接埠 20）流量會遭到拒絕，但所有其他 IP 流量會允許通過。



FTP使用連線埠21和連線埠20。目的地為連線埠21和連線埠20的TCP流量會遭到拒絕，但所有其他流量會明確地允許通過。

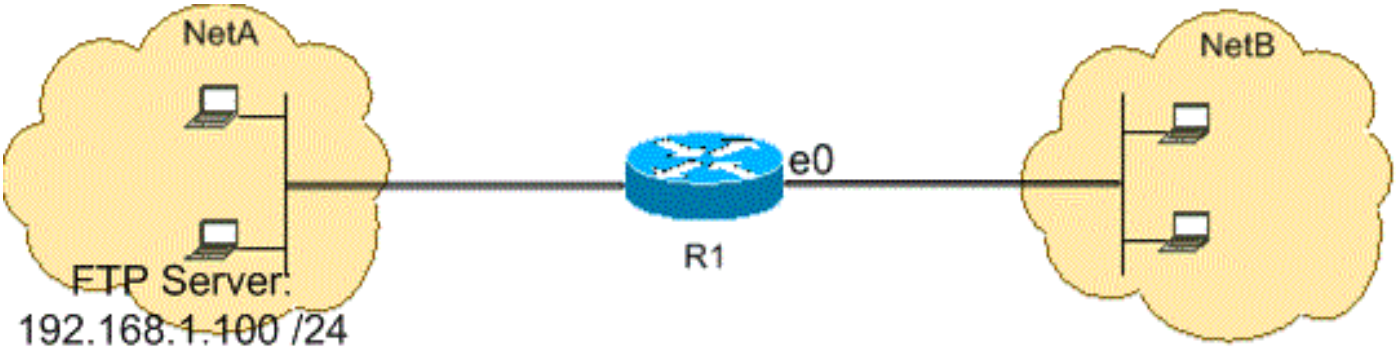
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

允許 FTP 流量（主動式 FTP）

FTP 可以在兩種不同模式下運作，分別是主動和被動。

FTP 在主動模式下運作時，FTP 伺服器會將連接埠 21 用來進行控制，並將連接埠 20 用於資料。FTP 伺服器 (192.168.1.100) 位於 NetA 中。下圖顯示，來源為 NetB 且目的地為 FTP 伺服器 (192.168.1.100) 的 FTP（TCP，連接埠 21）和 FTP 資料（連接埠 20）流量會允許通過，但所有其他 IP 流量會遭到拒絕。



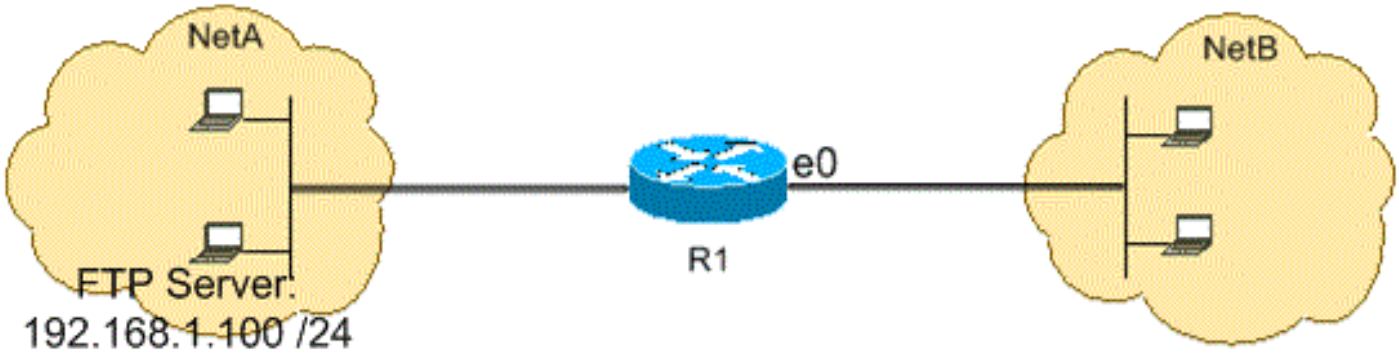
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

允許 FTP 流量（被動式 FTP）

FTP 可以在兩種不同模式下運作，分別是主動和被動。

FTP 在被動模式下運作時，FTP 伺服器會將連接埠 21 用來進行控制，並將大於或等於 1024 的動態連接埠用於資料。FTP 伺服器 (192.168.1.100) 位於 NetA 中。下圖顯示，來源為 NetB 且目的地為 FTP 伺服器 (192.168.1.100) 的 FTP（TCP，連接埠 21）和 FTP 資料（連接埠大於或等於 1024）流量會允許通過，但所有其他 IP 流量會遭到拒絕。



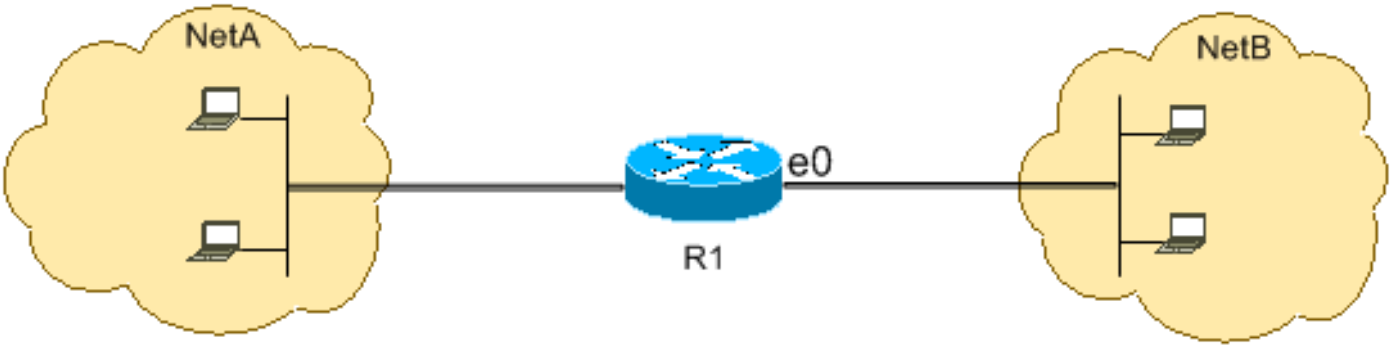
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
```

```
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

允許 Ping (ICMP)

下圖顯示，來源為 NetA 且目的地為 NetB 的 ICMP 會允許通過，但來自 NetB 且目的地為 NetA 的 ping 會遭到拒絕。



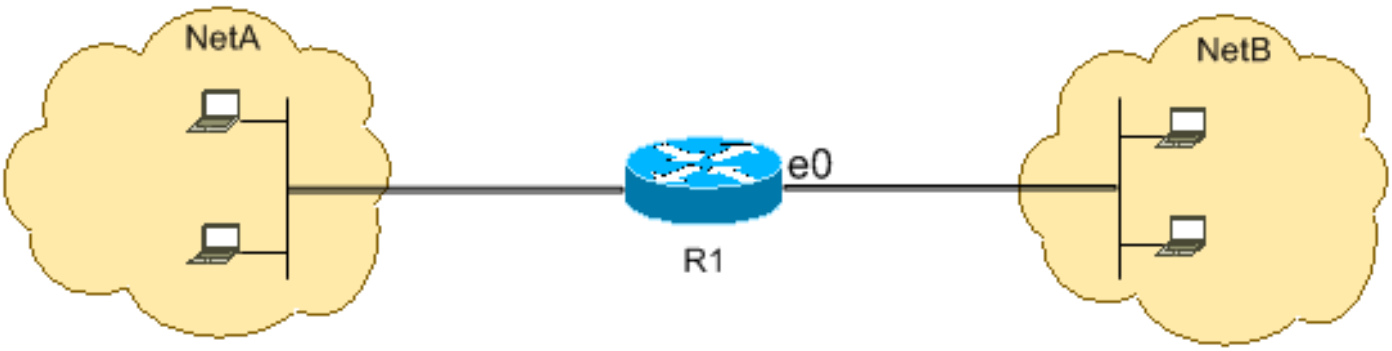
此組態僅允許回應（ping 回覆）封包透過乙太網路 0 介面從 NetB 傳入 NetA 。但是，當 ping 來源是 NetB 且目的地為 NetA 時，此組態會封鎖所有回應請求 ICMP 封包。因此，NetA 中的主機可以 ping NetB 中的主機，但 NetB 中的主機無法 ping NetA 中的主機。

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

允許 HTTP、Telnet、郵件、POP3、FTP

下圖顯示，只有 HTTP、Telnet、簡易郵件傳送通訊協定 (SMTP)、POP3 和 FTP 流量會允許通過，來源為 NetB 且目的地為 NetA 的其餘流量則遭到拒絕。



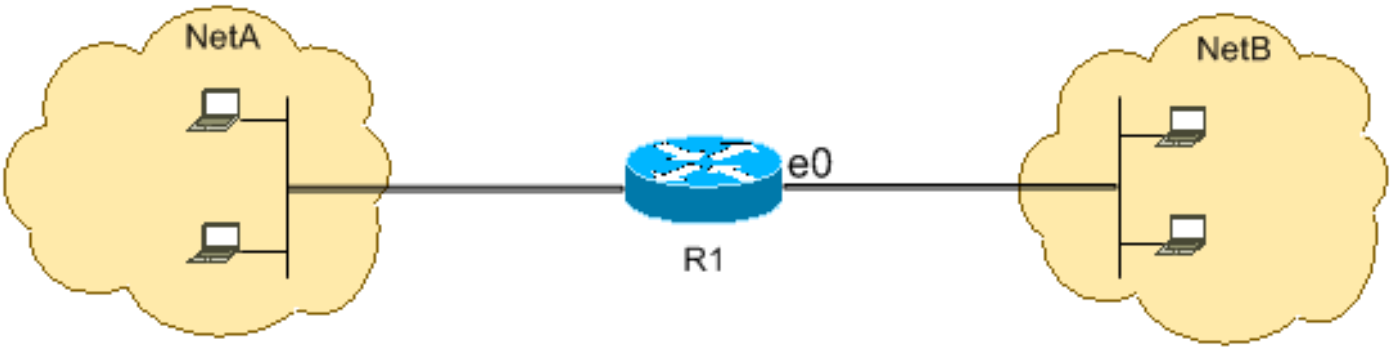
此組態允許目的地連接埠值與 WWW（連接埠 80）、Telnet（連接埠 23）、SMTP（連接埠 25）、POP3（連接埠 110）、FTP（連接埠 21）或 FTP 資料（連接埠 20）相符的 TCP 流量通過。 請注意，ACL 結尾的隱含 deny all 子句會拒絕所有其他與 permit 子句不相符的流量。

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

允許 DNS

下圖顯示，只有網域名稱系統 (DNS) 流量會允許通過，而來源為 NetB 且目的地為 NetA 的其餘流量則遭到拒絕。



此組態允許目的地連線埠值為53的TCP流量。ACL結尾的隱含deny all子句會拒絕所有其他與permit子句不相符的流量。

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

允許路由更新

將傳入 ACL 套用到介面時，請確保不會過濾掉路由更新。請使用以下清單中的相關 ACL 來允許路由通訊協定封包：

輸入以下命令可允許路由資訊通訊協定 (RIP)：

```
access-list 102 permit udp any any eq rip
```

輸入以下命令可允許內部閘道路由通訊協定 (IGRP)：

```
access-list 102 permit igrp any any
```

輸入以下命令可允許增強型 IGRP (EIGRP)：

```
access-list 102 permit eigrp any any
```

輸入以下命令可允許開放最短路徑優先 (OSPF)：

```
access-list 102 permit ospf any any
```

輸入以下命令可允許邊界閘道通訊協定 (BGP)：

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

依照 ACL 為流量偵錯

debug 命令的使用需要分配記憶體和處理能力等系統資源，而且在極端情況下可能會導致負荷過重的系統停滯。請謹慎使用 **debug 命令。**使用ACL可選擇性定義需要檢查的流量，以減少**debug**命令的影響。此類組態不會過濾任何封包。

此組態只會對主機 10.1.1.1 和 172.16.1.1 之間的封包啟用 **debug ip packet 命令。**

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
R1(config)#end
R1#debug ip packet 199 detail IP packet debugging is on (detailed) for access list 199
```

請參閱有關 Debug 命令的重要資訊以瞭解其他有關 debug 命令的資訊。

請參閱瞭解 Ping 和 Traceroute 命令的使用 Debug 命令區段，以瞭解其他有關透過 **debug 命令使用 ACL 的資訊。**

MAC 位址過濾

您可以過濾具有特定 MAC 層站台來源或目的地位址的訊框。系統可以設定任意數量的位址，而且不會減損效能。若要依照 MAC 層位址進行過濾，請在全域組態模式下使用以下命令：

```
Router#config terminal
Router(config)#bridge irb
Router(config)#bridge 1 protocol ieee
Router(config)#bridge 1 route ip
```

將橋接通訊協定套用到您需要透過使用**bridge-group <group number> {input-address-list <ACL number>指令建立的存取清單過濾流量的介面上 | output-address-list <ACL number>}**:

```
Router#config terminal
Router(config-if)#interface fastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#bridge-group 1 input-address-list 700
Router(config-if)#exit
```

建立橋接虛擬介面，並套用指派給實體乙太網路介面的IP位址：

```
Router#config terminal
```

```
Router(config-if)#int bvi1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000
Router(config)#access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

透過此組態，路由器只會允許在存取清單700上設定的MAC位址。使用access list指令**access-list <ACL number> deny <mac address> 000.0000.0000**，拒絕無法存取的MAC位址，然後允許其餘位址（例如aaa.bbb.cccc）。

> **附註**：請在存取清單中為每個 MAC 位址建立一行。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- 設定 IP 存取清單
- 存取清單支援頁面
- IP 路由支援頁面
- IP 路由通訊協定支援頁面
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。