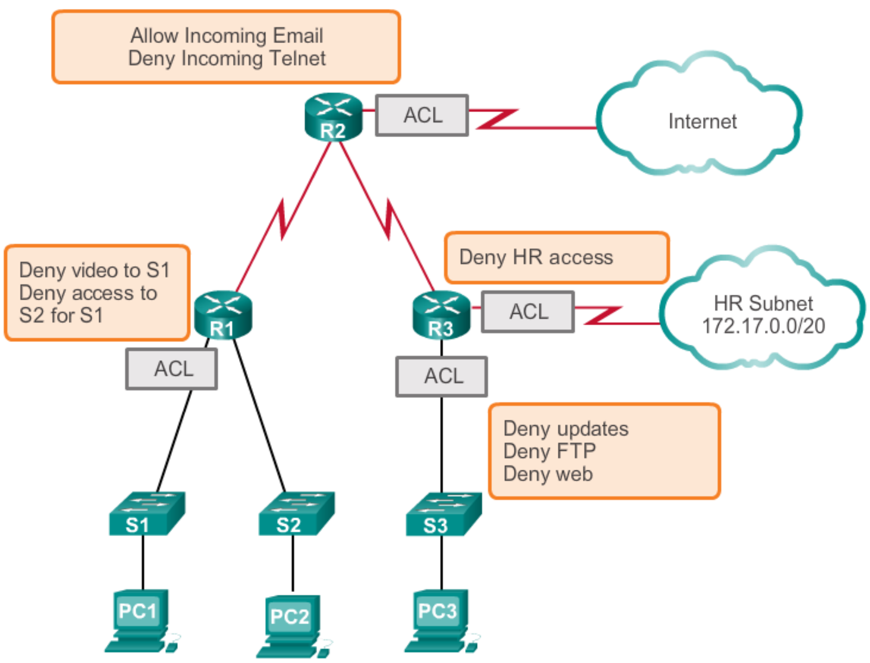
Firewall
存取控制列表

什麼是 ACL？(1/2)

- ACL (Access Control List)
  - 限制網路流量以提高網路效能
  - 提供流量控制
  - 提供基本的網路存取安全性
  - 根據流量類型過濾流量
  - 遮蔽主機以允許或拒絕對網路服務的存取
- 預設情況下，路由器並未設定 ACL；因此，路由器不會預設過濾流量
- 當 ACL 套用於介面時，路由器會在網路封包透過介面時執行另一項評估所有網路封包的任務，以確定是否可以轉發封包

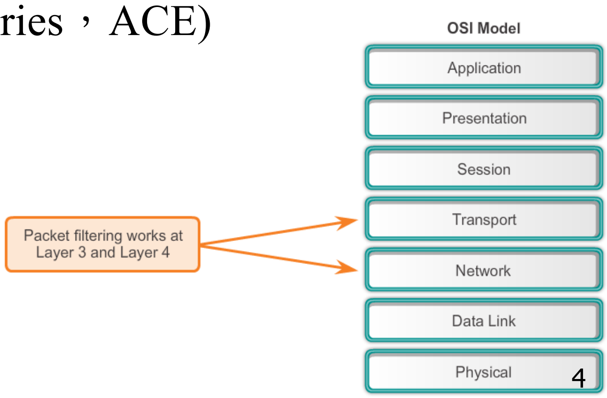
什麼是 ACL？(2/2)

What Is an ACL?



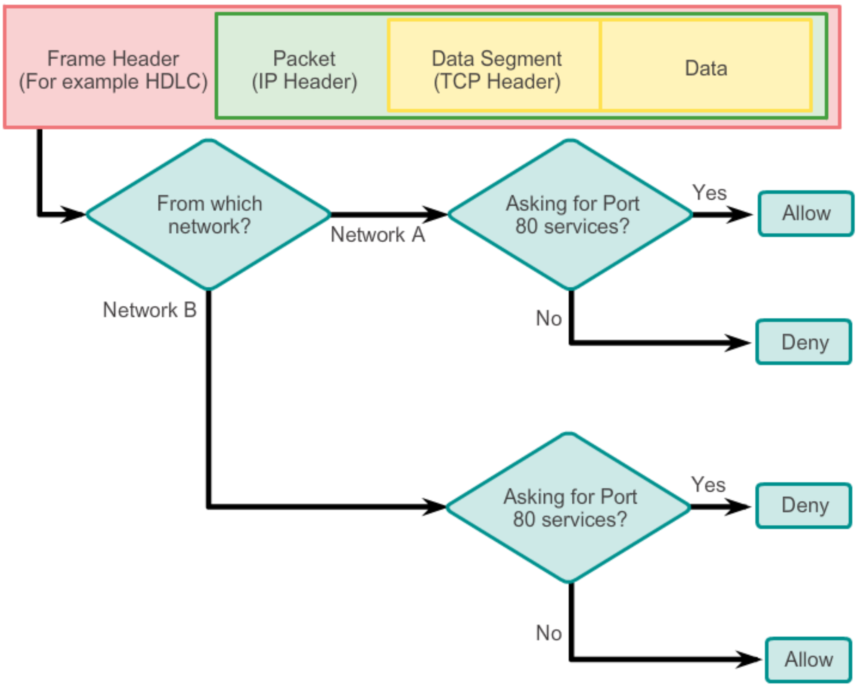
封包過濾（Packet Filtering）(1/2)

- 封包過濾透過分析傳入和傳出的封包並根據給定的條件傳遞或丟棄封包，從而控制網路存取，例如來源IP位址、目的IP位址和封包內傳輸的協定
- 當路由器根據過濾規則轉發或拒絕封包時，它便充當了一種封包過濾器
- ACL是一系列 permit 或 deny 語句組成的順序列表，稱為存取控制條目(Access Control Entries，ACE)

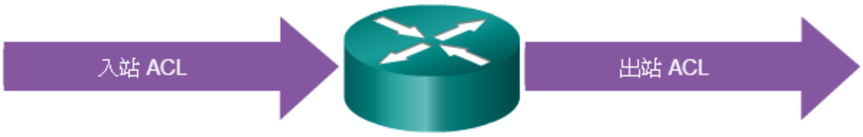


封包過濾（Packet Filtering）(2/2)

Packet Filtering Example

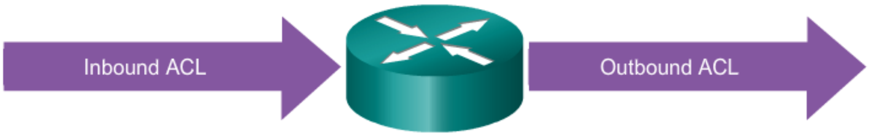


ACL工作原理



在資料封包被路由到出站介面之前，入站 ACL 過濾流入特定介面的資料封包。

在資料封包被路由之後，出站 ACL 過濾流入任意入站介面的資料封包。

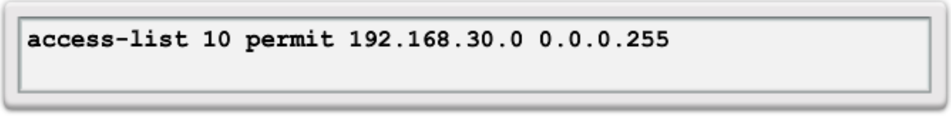


An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

An outbound ACL filters packets after being routed, regardless of the inbound interface.

思科 IPv4 ACL 類型

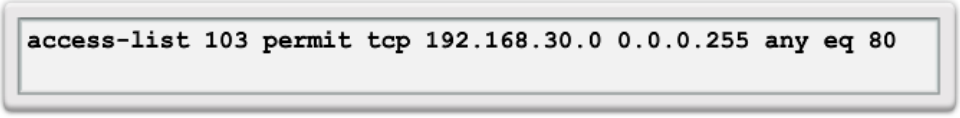
- 有兩種類型的Cisco IP ACL
  - 標準ACL



```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

  - 延伸ACL

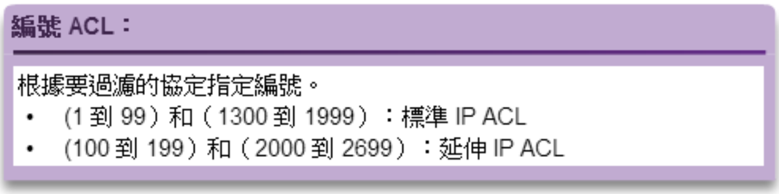


```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/Protocol number (example: IP, ICMP, UDP, TCP, etc.)

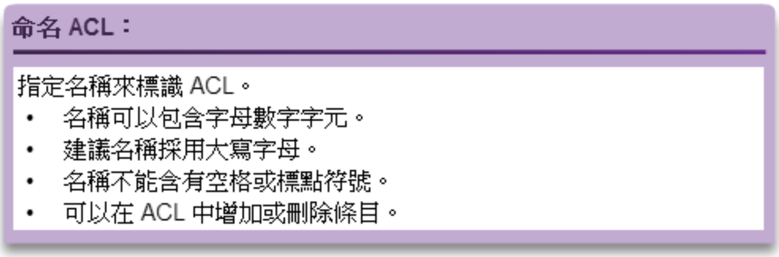
編號ACL和命名ACL



編號 ACL：

根據要過濾的協定指定編號。

- (1 到 99）和（1300 到 1999）：標準 IP ACL
- (100 到 199）和（2000 到 2699）：延伸 IP ACL



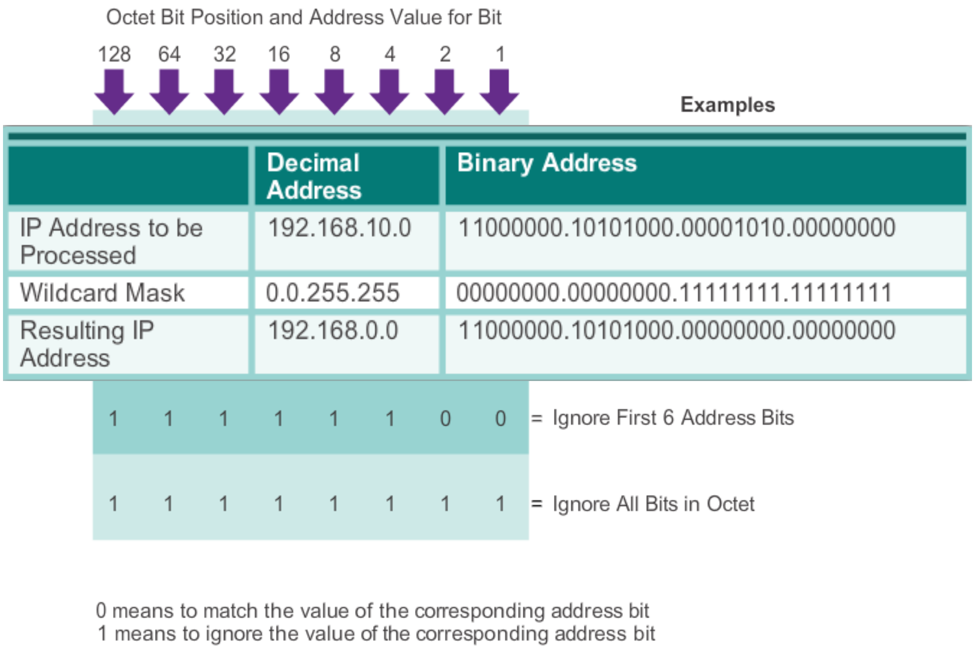
命名 ACL：

指定名稱來標識 ACL。

- 名稱可以包含字母數字字元。
- 建議名稱採用大寫字母。
- 名稱不能含有空格或標點符號。
- 可以在 ACL 中增加或刪除條目。

介紹ACL萬用遮罩

Wildcard Masking



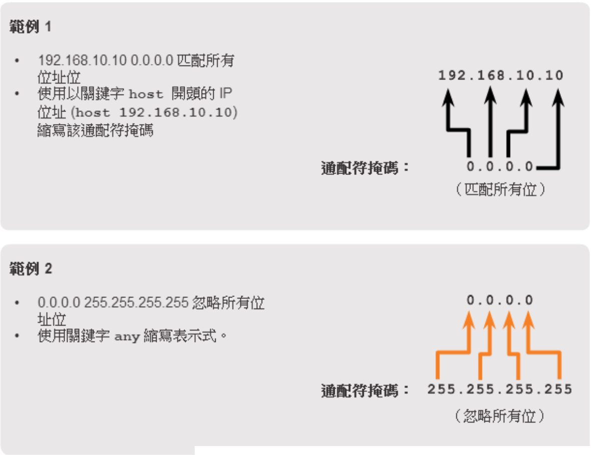
Octet Bit Position and Address Value for Bit
128 64 32 16 8 4 2 1
Examples

	Decimal Address	Binary Address
IP Address to be Processed	192.168.10.0	11000000.10101000.00001010.00000000
Wildcard Mask	0.0.255.255	00000000.00000000.11111111.11111111
Resulting IP Address	192.168.0.0	11000000.10101000.00000000.00000000

1 1 1 1 1 1 0 0 = Ignore First 6 Address Bits
1 1 1 1 1 1 1 1 = Ignore All Bits in Octet

0 means to match the value of the corresponding address bit
1 means to ignore the value of the corresponding address bit

萬用遮罩關鍵字

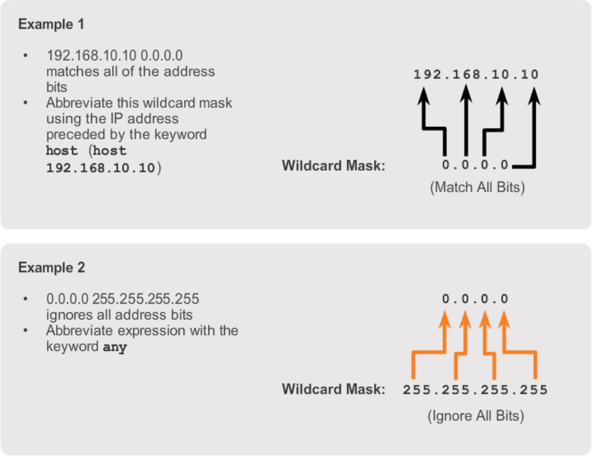


範例 1

- 192.168.10.10 0.0.0.0 匹配所有位址位
- 使用以關鍵字 host 開頭的 IP 位址 (host 192.168.10.10) 縮寫該通配符掩碼

範例 2

- 0.0.0.0 255.255.255.255 忽略所有位址位
- 使用關鍵字 any 縮寫表示式。



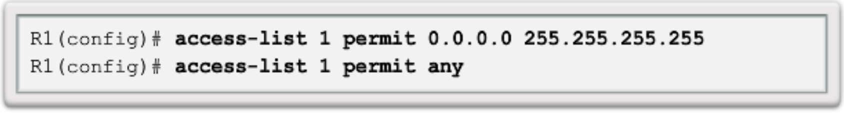
Example 1

- 192.168.10.10 0.0.0.0 matches all of the address bits
- Abbreviate this wildcard mask using the IP address preceded by the keyword host (host 192.168.10.10)

Example 2

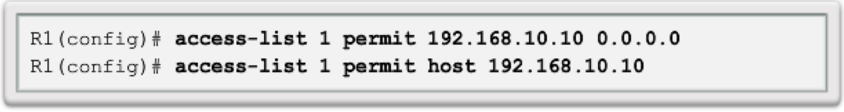
- 0.0.0.0 255.255.255.255 ignores all address bits
- Abbreviate expression with the keyword any

範例 1：



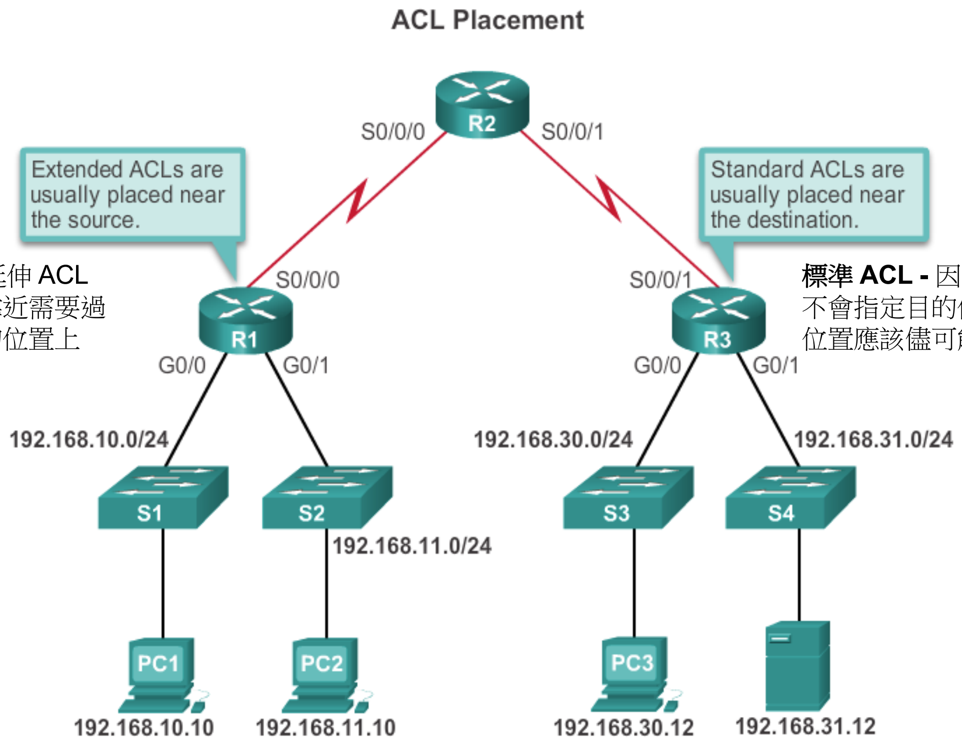
```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 permit any
```

範例 2：



```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit host 192.168.10.10
```

ACL的放置位置(1/3)



ACL Placement

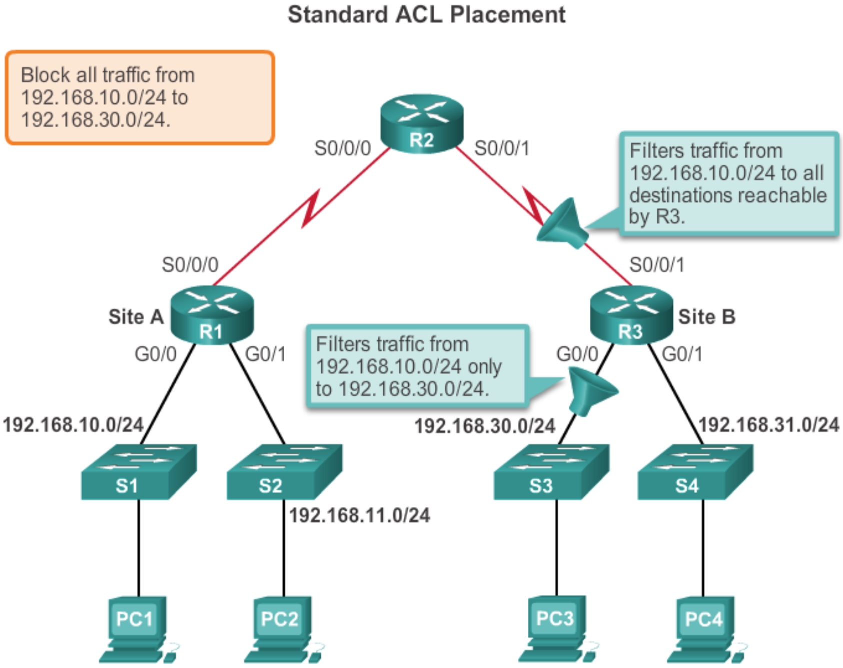
Extended ACLs are usually placed near the source.

Standard ACLs are usually placed near the destination.

延伸 ACL - 將延伸 ACL 放置在儘可能靠近需要過濾的流量來源的位置上

標準 ACL - 因為標準 ACL 不會指定目的位址，所以其位置應該儘可能靠近目的地

ACL的放置位置(2/3)



Standard ACL Placement

Block all traffic from 192.168.10.0/24 to 192.168.30.0/24.

Filters traffic from 192.168.10.0/24 to all destinations reachable by R3.

Filters traffic from 192.168.10.0/24 only to 192.168.30.0/24.

延伸ACL

Extended ACLs can filter on:

- Source address
- Destination address
- Protocol
- Port numbers

Using Port Numbers

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Using Keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

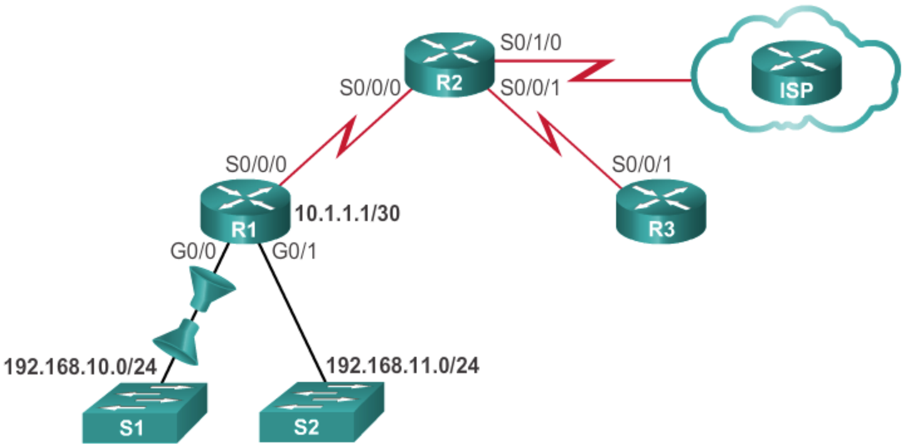
配置延伸ACL

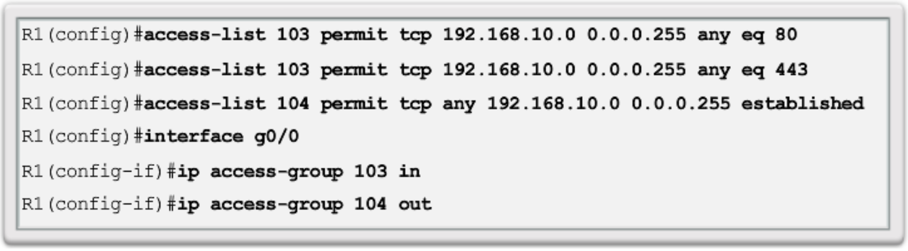
```
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name][established]
```

Parameter	Description
access-list-number	Identifies the access list using a number in the range 100 to 199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Used to enter a remark or comment.
protocol	Name or number of an Internet protocol. Common keywords include **icmp**, **ip**, **tcp**, or **udp**. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword.
source	Number of the network or host from which the packet is being sent.
source-wildcard	Wildcard bits to be applied to source.
destination	Number of the network or host to which the packet is being sent.
destination-wildcard	Wildcard bits to be applied to the destination.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) The decimal number or name of a TCP or UDP port.
established	(Optional) For the TCP protocol only: Indicates an established connection.

將延伸ACL應用於介面

Applying an ACL to an Interface

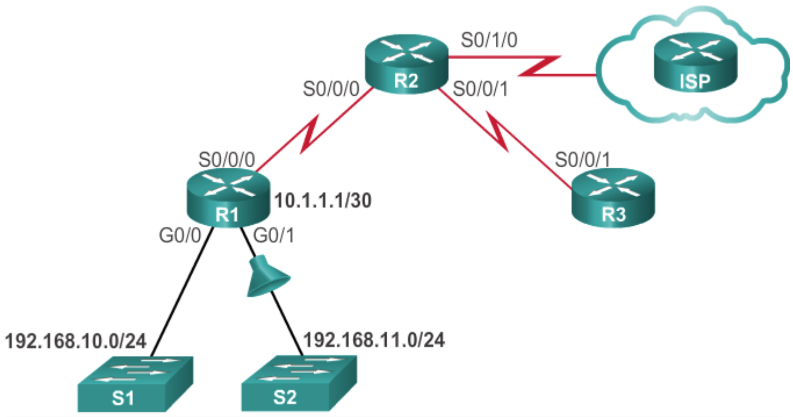


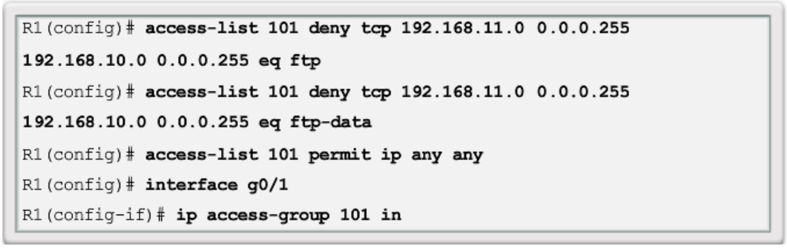


```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

使用延伸ACL過濾流量(1/2)

Extended ACL to Deny FTP

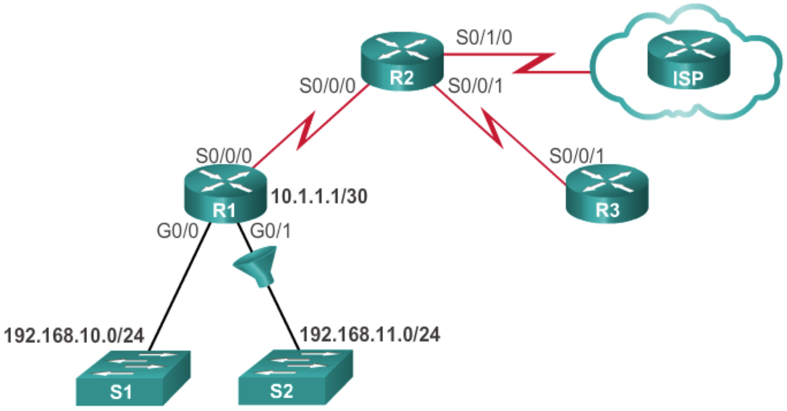


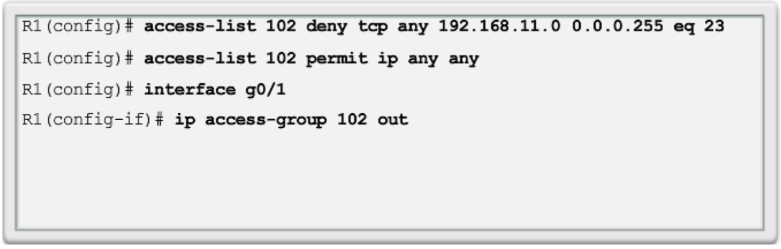


```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp-data
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 101 in
```

使用延伸ACL過濾流量(2/2)

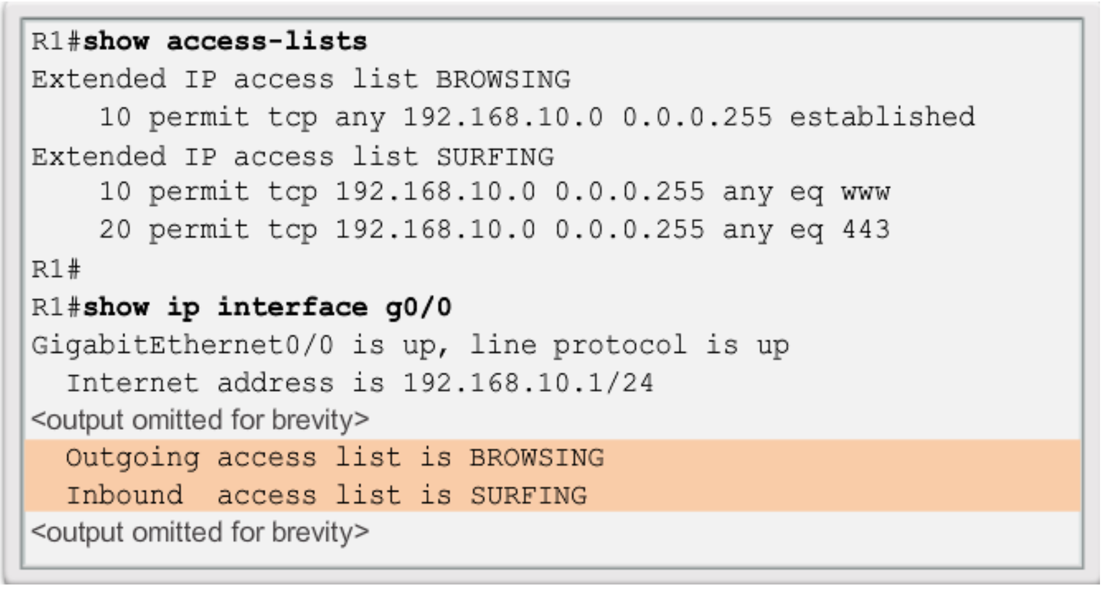
Extended ACL to Deny Telnet





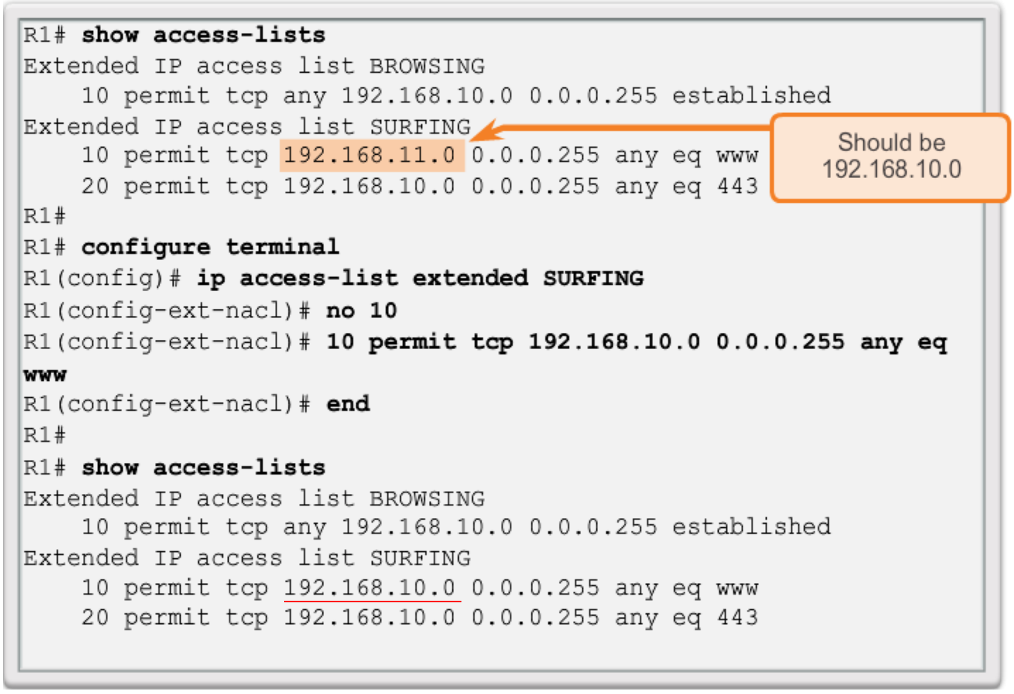
```
R1(config)# access-list 102 deny tcp any 192.168.11.0 0.0.0.255 eq 23
R1(config)# access-list 102 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 102 out
```

檢驗延伸ACL



```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

編輯延伸ACL



```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.11.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq
www
R1(config-ext-nacl)# end
R1#
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

Should be
192.168.10.0