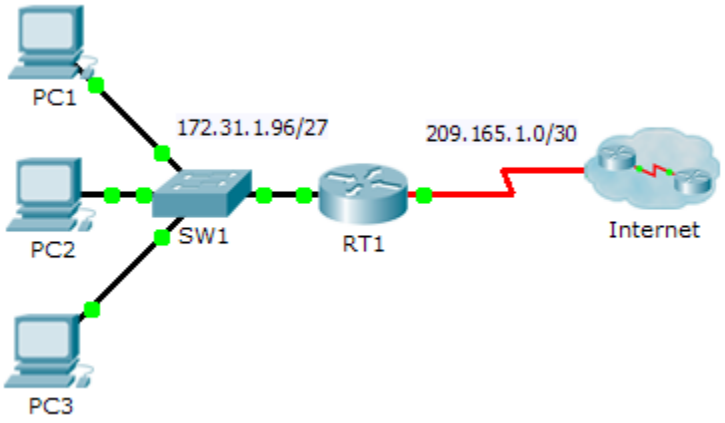
# Packet Tracer - 設定延伸 ACL - 場景 3

## 拓樸




## 位址分配表

| 裝置 | 介面 | IP 位址 | 子網路遮罩 | 預設閘道 |
|---|---|---|---|---|
| RT1 | G0/0 | 172.31.1.126 | 255.255.255.224 | N/A |
| | S0/0/0 | 209.165.1.2 | 255.255.255.252 | N/A |
| PC1 | NIC | 172.31.1.101 | 255.255.255.224 | 172.31.1.126 |
| PC2 | NIC | 172.31.1.102 | 255.255.255.224 | 172.31.1.126 |
| PC3 | NIC | 172.31.1.103 | 255.255.255.224 | 172.31.1.126 |
| Server1 | NIC | 64.101.255.254 | | |
| Server2 | NIC | 64.103.255.254 | | |

## 目標

**第 1 部分：設定延伸命名 ACL。**

**第 2 部分：套用並檢驗延伸 ACL**

## 背景/場景

在此場景中，LAN 中的特定裝置允許存取網際網路上的伺服器上的各種服務。

# 第 1 部分: 設定延伸命名 ACL

使用一個命名 ACL 來實作以下政策：

- 阻止從 **PC1** 對 **Server1** 和 **Server2** 進行 HTTP 和 HTTPS 存取。伺服器位於雲端，你僅知道其 IP 位址。
- 阻止從 **PC2** 對 **Server1** 和 **Server2** 進行 FTP 存取。

- 阻止從 **PC3** 對 **Server1** 和 **Server2** 進行 ICMP 存取。

**注意：**因為評分目的，你必須按以下步驟中指定的順序設定這些敘述。

### 第 1 步: 拒絕 PC1 存取 Server1 和 Server2 上的 HTTP 和 HTTPS 服務。

a. 新增一個延伸 IP 存取清單命名 ACL，用於拒絕 **PC1** 存取 **Server1** 和 **Server2** 的 HTTP 和 HTTPS 服務。因為無法直接觀察網際網路上伺服器的子網，所以需要建立四條規則。

那個命令可以用於啟動命名 ACL？

b. 記錄用於拒絕從 **PC1** 對 **Server1** 進行存取的敘述，只針對 HTTP（連接埠 80）。

c. 記錄用於拒絕從 **PC1** 對 **Server1** 進行存取的敘述，只針對 HTTPS（連接埠 443）。

d. 記錄用於拒絕從 **PC1** 對 **Server2** 進行存取的敘述，只針對 HTTP。

e. 記錄用於拒絕從 **PC1** 對 **Server2** 進行存取的敘述，只針對 HTTPS。

### 第 2 步: 拒絕 PC2 存取 Server1 和 Server2 上的 FTP 服務。

a. 記錄用於拒絕從 **PC2** 對 **Server1** 進行存取的敘述，只針對 FTP（只有連接埠 21）。

b. 記錄用於拒絕從 **PC2** 對 **Server2** 進行存取的敘述，只針對 FTP（只有連接埠 21）。

### 第 3 步: 拒絕 PC3 對 Server1 和 Server2 執行 ping 操作。

a. 記錄用於拒絕從 **PC3** 對 **Server1** 進行 ICMP 存取的敘述。

b. 記錄用於拒絕從 **PC3** 對 **Server2** 進行 ICMP 存取的敘述。

### 第 4 步: 允許其他所有 IP 流量。

預設情況下，存取清單會拒絕不匹配清單中的所有規則的流量。那個命令允許所有其他流量？

## 第 2 部分: 套用和檢驗延伸 ACL

要過濾來自 172.31.1.96/27 網路及其目的地是遠端網路的流量，其 ACL 的正確放置，取決於流量與 **RT1** 的關係。

### 第 1 步: 將 ACL 套用到正確的介面和正確的方向上。

a. 你需要那些命令來將 ACL 套用於正確的介面和正確的方向上？

### 第 2 步: 測試每台 PC 的存取。

a. 使用 **PC1** 的 Web 瀏覽器並同時使用 HTTP 和 HTTPS 協定存取 **Server1** 和 **Server2** 的網站。

b. 使用 **PC1** 存取 **Server1** 和 **Server2** 的 FTP。用戶名和密碼是“**cisco**”。

c. 從 **PC1** 對 **Server1** 和 **Server2** 執行 ping 操作。

d. 對 **PC2** 和 **PC3** 重複第 2a 步到第 2c 步以檢驗存取清單是否正確執行。