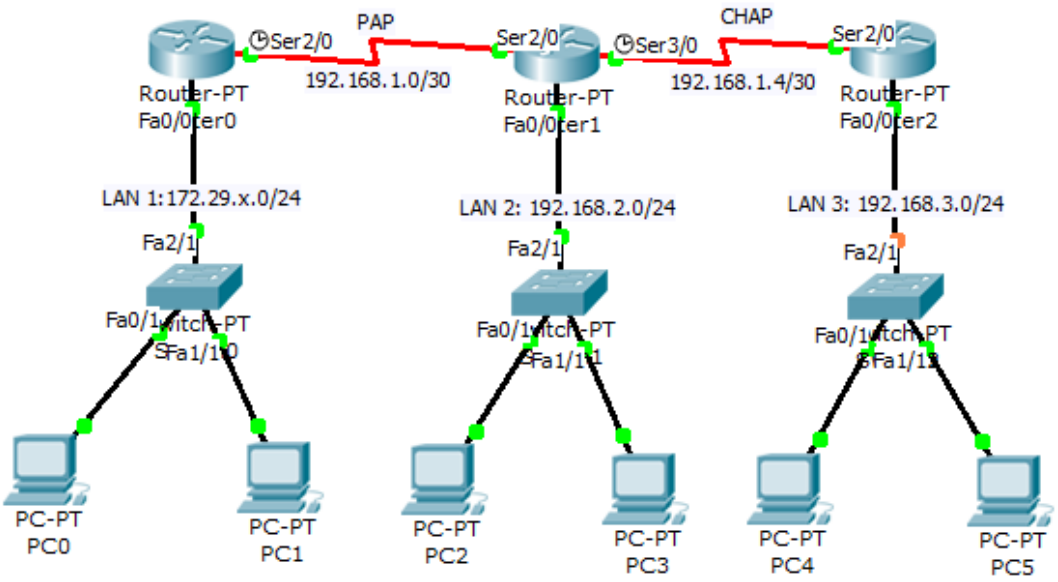
Access List

Cisco cung cấp một bộ lọc khác mạnh trong các routers của mình, đó là access-list.

Khi một gói tin đến router nó sẽ được lọc qua access0list, nếu thoả bộ lọc mới được phép cho qua, nếu không sẽ bị huỷ.

Access list có thể chia thành hai dạng: access list theo số và access list theo tên.

1. Mô hình thực hiện:



2. Access-list dạng số

Access list dạng số có 2 dạng:

- Standard: chỉ lọc địa chỉ nguồn
- Extended: lọc được cả địa chỉ nguồn và địa chỉ đích.

a. Access-list dạng standard

Cú pháp:

access-list *access-list-number* {**deny**|**permit**} *source* [*source-wildcard*]

Áp dụng 1:

Ví dụ ta có yêu cầu: *Cấm các máy tính ở mạng LAN của R0 (172.29.X.0/29) truy xuất đến mạng LAN của R2(192.168.3.0/24)*

```
R2>
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ac
R2(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
R2(config)#access-list
```

Copy Paste

Ta thấy access list dạng standard có dải <1-99>

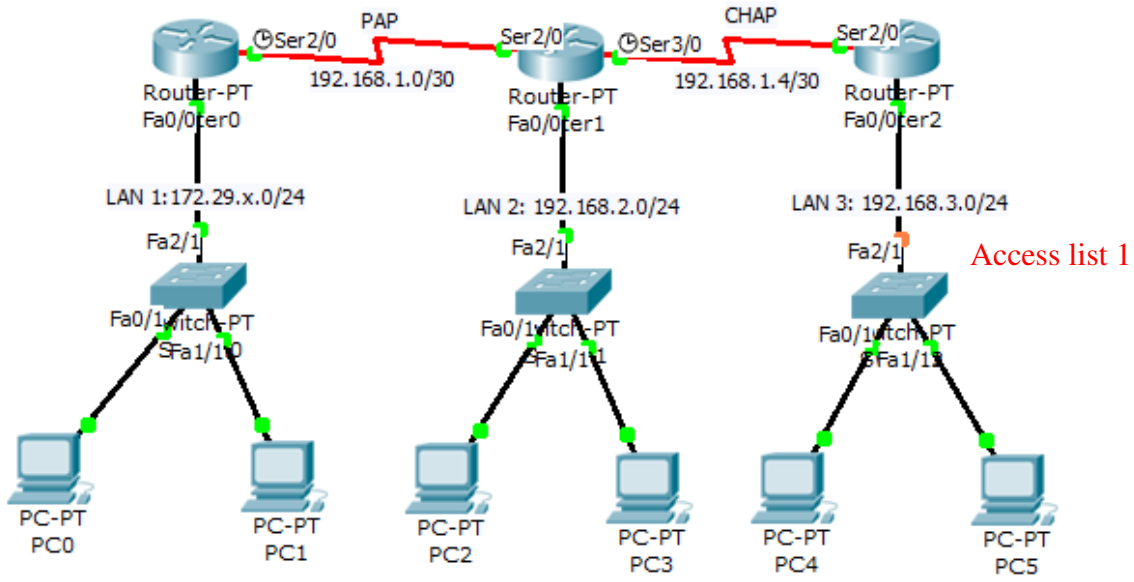
Ta sẽ sử dụng số 1:

```
R2(config)#access-list 1 deny 172.29.1.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
```

Ý nghĩa:

- Cấm các máy thuộc đường mạng 172.29.1.0/24
- Cho phép các máy còn lại

Áp dụng access-list này vào cổng Fa0/0 của R2, hướng out




```
R2(config)#int f0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

Ta không đặt access-list tại R0 và R1, vì đây là Access-list chỉ lọc theo địa chỉ nguồn; nếu đặt tại R0 toàn mạng LAN1: 172.29.X.0/24 sẽ không thể đi ra ngoài. Trong khi đó ta chỉ cần mạng LAN1 đến mạng LAN3.

Với lý do tương tự ta sẽ không đặt access này tại R1

Vị trí thích hợp nhất là đặt tại R2, cấm các gói tin này ra khỏi (out) cổng fa0/0

Thử nghiệm:

- Ping từ PC0, PC1 đến PC4, PC5 sẽ không thành công
- Ping từ PC1 đến PC2, PC3 vẫn thực hiện được.

b. Access list dạng extended

Áp dụng 2:

Dùng extended access-list cấm PC1 đến mạng LAN2.

Dùng Access-list dạng extended có thể lọc cả địc chỉ đích và nguồn, do đó có thể đặt càng gần nguồn càng tốt, để tránh các gói tin không mong muốn được phép đi ra ngoài, chiếm băng thông đường truyền.

➔ Ta sẽ đặt access-list này tại cổng fa0/0 của R0

```
R0(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
R0(config)#access-list
```

Access-list extended có thể sử dụng <100-199>

Ta dùng số 150 trong ví dụ này:

```
R0(config)#access-list 150 deny ip 172.29.1.3 0.0.0.0 192.168.3.0 0.0.0.255
R0(config)#access-list 150 permit ip any any
R0(config)#
```

Tham số: 172.29.1.3 0.0.0.0: địa chỉ PC nguồn

Tham số: 192.168.3.0 0.0.0.255: địa chỉ mạng LAN 3 (192.168.3.0/24)(địa chỉ đích)

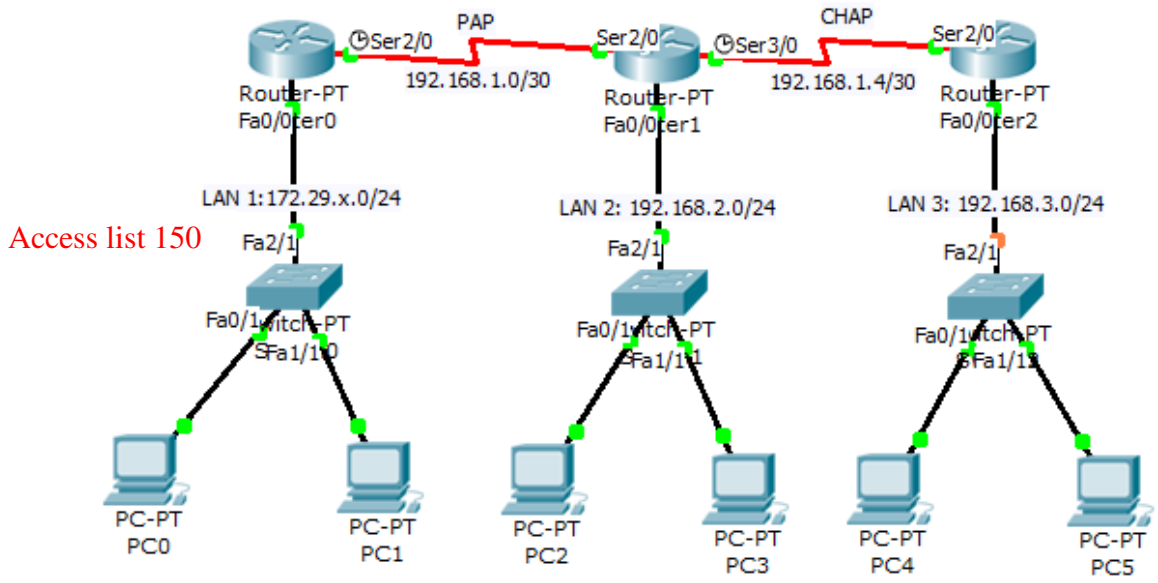
Với địa chỉ 172.29.1.3 0.0.0.0 ta có thể viết gọn bằng 1 từ khoá **"host"** được định nghĩa sẵn.

Ví dụ: *Xây dựng 1 access-list khác có tính năng tương tự.*

```
R0(config)#access-list 160 deny ip host 172.29.1.3 192.168.3.0 0.0.0.255
R0(config)#access-list 160 permit ip any any
R0(config)#
```

Luôn phải có câu lệnh permit ip any any ở cuối.

Nếu không có câu lệnh này ở cuối, mọi gói tin sẽ bị bỏ.



Áp dụng access-list này vào cổng fa0/0 theo chiều in:

```
R0>en
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#int fa0/0
R0(config-if)#ip access-group 150 in
R0(config-if)#
```

Thử nghiệm:

Ping từ PC1 đếng mạng LAN2 không thành công

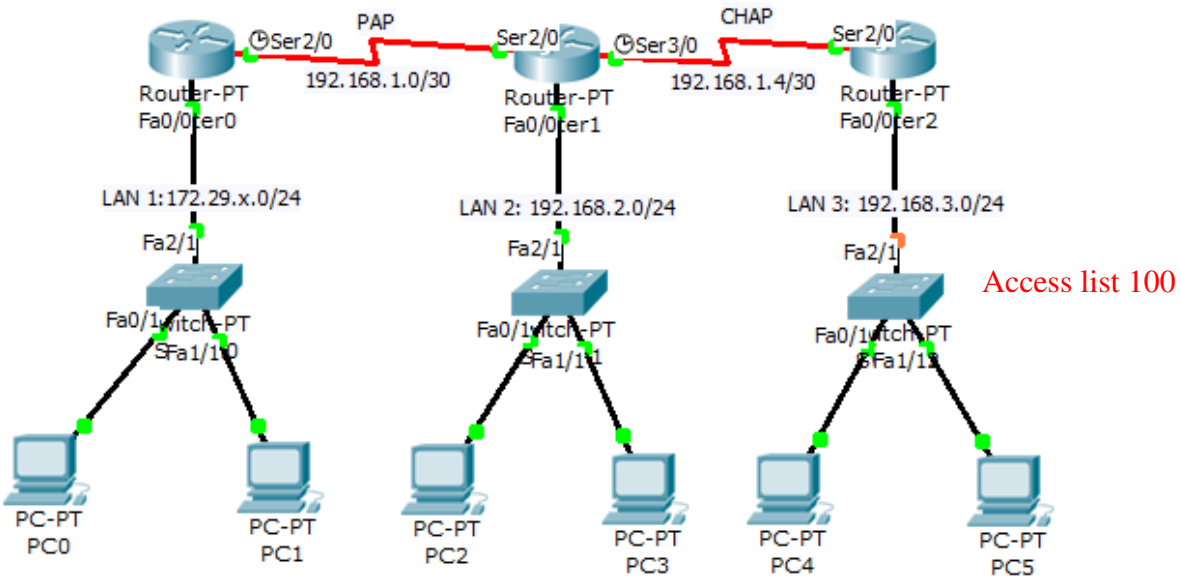
Ping từ PC1 đến địa chỉ 192.168.1.6(R3) thành công.

Ping từ PC0 đến mạng LAN2 thành công.

Áp dụng 3:

Cấm Router PC4 (192.168.3.2/24) connect đến dịch vụ FTP trên PC1.

Ta chặn trên Router 2:



Access list 100

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 100 deny tcp host 192.168.3.2 host 172.29.1.3 eq 21
R2(config)#access-list 100 permit ip any any
R2(config)#
R2(config)#int fa0/0
R2(config-if)#ip access-group 100 in
R2(config-if)#
```

Câu lệnh deny **tcp …… eq 21** có ý nghĩa cấm các traffic đi đến port 21 của dịch vụ TCP.

Vì điều kiện giả lập ta không thể thử nghiệm access-list này.

3. Access-list dạng tên

Áp dụng 4:

Cấm Router1 có ip 192.168.1.5 telnet đến Router2.

Giả sử ta đặt access-list này tại Router2.

Ta tạo 1 list access-list dạng tên:

```
R2(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
R2(config)#ip access-list
```

Có thể dùng từ khoá standard hoặc extended để cho biết loại access-list.

```
R2(config)#ip access-list standard CAM_TELNET
R2(config-std-nacl)#deny host 192.168.1.5
R2(config-std-nacl)#permit any
R2(config-std-nacl)#
```

Access list sẽ được đọc theo thứ tự từ trên xuống.

Xem lại access-list bằng cách dùng lệnh: **show access-list**

Thực nghiệm:

Cấu hình Telnet:

```
R2(config)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#
```

Từ R1 telnet đến R2.

Áp dụng access-lit vào cổng telnet, ta có thể dùng 1 câu lệnh dành riêng: access-class

```
R2(config)#line vty 0 4
R2(config-line)#access-class CAM_TELNET in
R2(config-line)#
```

Lúc này telnet từ R1 đến R2 lúc này không thành công