**1. Cấu hình Standard ACLs**

**Router(config)#access-list access-list-number [deny|permit] remark source [source-wildcard] [log]**

Các tham số:

- Access-list-number: số hiệu của  access list. Với Standard ACLs, access-list-number có thể nằm trong dải 1- 99 và 1300- 1999ad

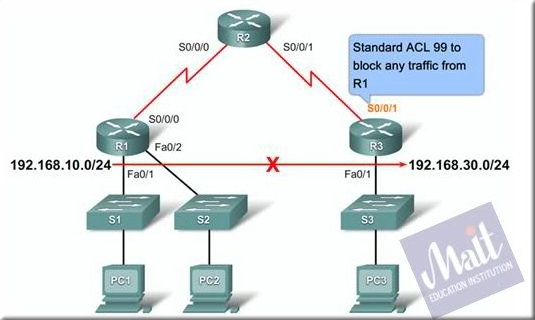
- Deny| permit: nếu gói tin thỏa mãn các điều kiện trong access-list thì gói tin sẽ bị hủy hay cho phép qua tùy thuộc vào tham số này

- Remark : chú thích cho access-list

- Source: chỉ đích danh địa chỉ nguồn gói tin được gửi đi

- Source-wildcard: phần thuộc tính source-wildcard của source xác định số bit trong địa chỉ nguồn cần phải giống khi so sánh với địa chỉ nguồn đã các định trong access-list

**Ví dụ1: Xây dựng access-list 99 chặn tất cả gói tin từ mạng 192.168.10.0/24 sang địa chỉ mạng 192.168.30.0/24**



R3(config)#access-list 99 deny 192.168.10.0 0.0.0.255

R3(config)#access-list 99 permit any

R3(config)#interface s0/0/1

R3(config-if)#ip access-group 99 in

Sau khi làm hãy ping thử từ PC1 sang PC3 -> Thành công hay không?

**Hãy lưu mô hình này lại để lúc sau thực hành ví dụ 3.**

**2. Cấu hình Extended ACLs:**

**Router(config)#access-list access-list-number [permit | deny] [protocol] [source specification] [destination specification]  [protocol qualification][logging]**

Các tham số:

- Access-list-number: số hiệu của access-list. Với Extended ACLs, access-list-number có thể nằm trong dải 100-199(dành cho IP ACLs) 2000-2699

- Permit | deny: gói tin thỏa mãn tất cả các điều kiện của ACL thì sẽ được cho qua hay hủy phụ thuộc vào tham số này

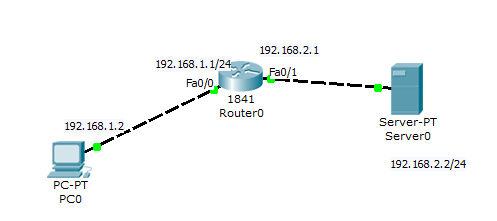
- Protocol :giao thức truyền gói tin : IP, ICMP, TCP hay UDP.

- Source specification : là một hay một dải địa chỉ nguồn + địa chỉ cổng nguồn

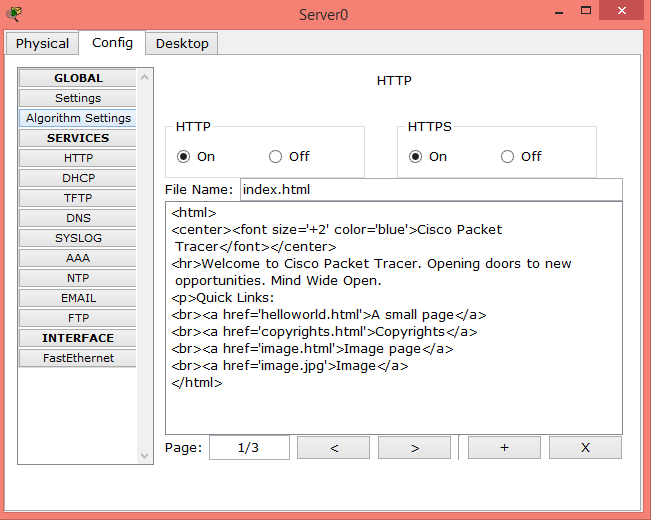
- Destination specification: là một hay một dải địa chỉ đích + địa chỉ cổng đích

- Logging : phần mở rộng, cho phép router xuất ra file log khi một access list nào đó thỏa mãn.

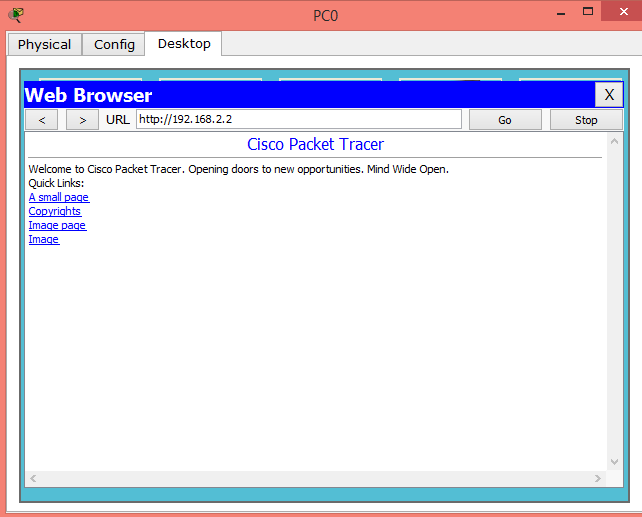
Ví dụ 2: Cấm truy cập web từ PC0 về Server0



Trên con Server0 bật HTTP, HTTPS



Từ PC0 truy cập vào web server



Áp chính sách cấm không cho PC0 truy cập vào Web server

Router(config)#access-list 104 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 80

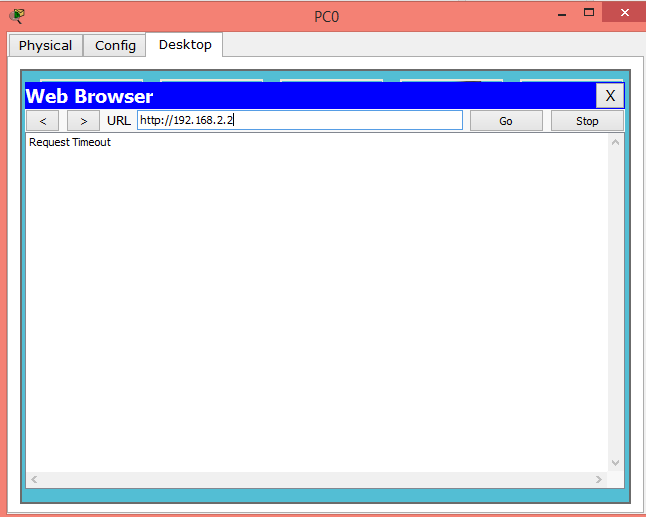
Router(config)#access-list 104 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 443

Router(config)#int f0/1

Router(config-if)#ip access-group 104 out

Router#show access-lists

Kết quả là: không truy cập được



Bài 3: Hãy cấm truy cập vào web



R3(config)#access-list 103 deny tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 equal 80

R3(config)#access-list 103 deny tcp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 equal 443

R3(config)#interface f0/2

R3(config-if)#ip access-group 103 in