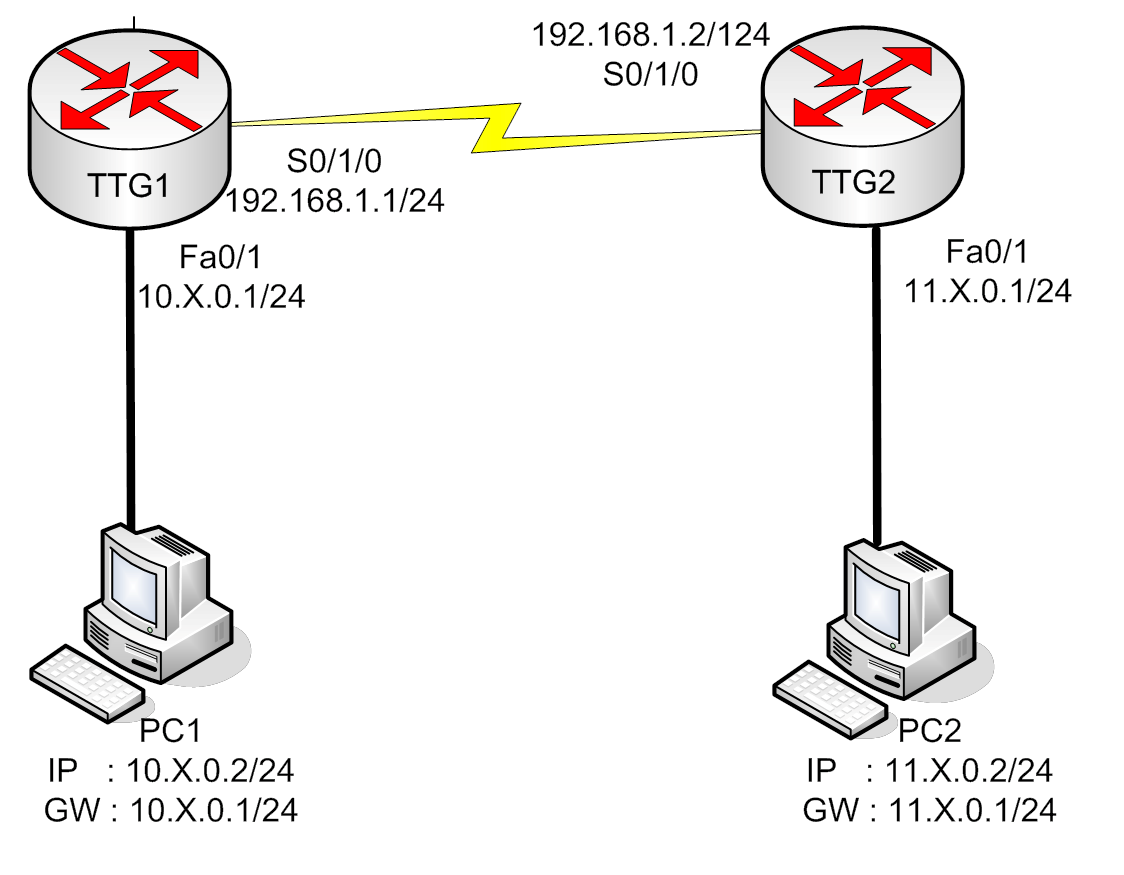
**EXTENDED ACCESS LIST**

**I. Giới thiệu :**

-Ở bài trước bạn đã thực hiện việc cấu hình Standard Access List, bài Lab này bạn sẽ tiếp tục tìm hiểu sâu hơn về Extended Access List. Đây là mở rộng của Standard Access List, trong quá trình kiểm tra, Router sẽ kiểm tra các yếu tố về địa chỉ nguồn, đích,giao thức và port…



**II. Mô tả bài lab và đồ hình :**

- **Mục đích của bài Lab**:Bạn thực hiện cấu hình **Extended Access List** sao cho **PC1**

không thể **Telnet** vào **Router TTG2** nhưng vẫn có thể **duyệt web** qua **Router TTG2**

- Bạn thực hiện việc cấu hình cho Router và Host như đồ hình trên:

**III. Cấu hình router :**

PC1:

IP Address:10.X.0.2

Subnet mask:255.255.255.0

Gateway:10.X.0.1

*PC2:*

IP Address:11.X.0.2

Subnet mask:255.255.255.0

Gateway:11.X.0.1

*Router TTG1:* Router> enable Router#configure terminal Router(config)#hostname TTG1

TTG1(config)#interface s0/1/0

TTG1(config-if)#ip address 192.168.1.1 255.255.255.0

TTG1(config-if)#no shutdown TTG1(config-if)#exit TTG1(config)#interface fa0/1

TTG1(config-if)#ip address 10.X.0.1 255.255.255.0

TTG1(config-if)#no shutdown

*Router TTG2 :*

Router> enable Router#configure terminal Router(config)#hostname TTG2

TTG2(config)#interface s0/1/0

TTG2(config-if)#ip address 192.168.1.2 255.255.255.0

TTG2(config-if)#no shutdown

TTG2(config-if)#exit

TTG2(config)#interface fa0/1

TTG2(config-if)#ip address 11.X.0.1 255.255.255.0

TTG2(config-if)#no shutdown

-Cấu hình định tuyến cho 2 router bằng OSPF

**Router TTG1 :**

TTG1(config)#router ospf 1

TTG1(config-router)#network 10.X.0.0 0.255.255.255 area 0

TTG1(config-router)#network 192.168.1.0 0.0.0.255 area 0

TTG1(config-router)#exit

**Router TTG2 :**

TTG1(config)#router ospf 1

TTG1(config-router)#network 11.X.0.0 0.255.255.255 area 0

TTG1(config-router)#network 192.168.1.0 0.0.0.255 area 0

TTG1(config-router)#exit

- Bạn thực hiện lệnh Ping để kiểm tra quá trình định tuyến.Sau khi chắc chắn rằng quá trình định

tuyến đã thành công.

- Tại **Router TTG2** bạn thực hiện câu lệnh:

TTG2(config)#**ip http server** *//Câu lệnh này dùng để giả một http server trên Router//*

- Tạo username và password dùng để chứng thực cho Web Server

TTG2(config)#username TTG2 password cisco

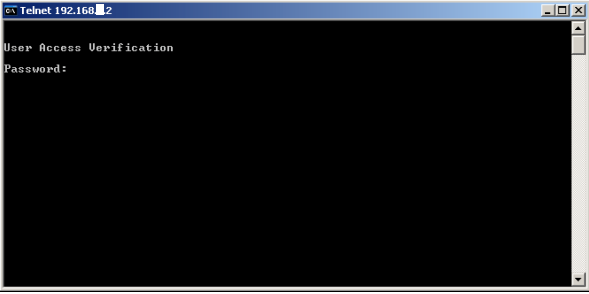
- Lúc này Router sẽ đóng vai trò như một Web Server

- Sau khi quá trìnhđ ịnh tuyến đã thành công,b ạn thực hiện các bước Telnet và duyệt Web từ

**PC1** vào **Router TTG2**.

**- Chú ý** :để thành công việc **Telnet** bạn phải **Login** cho đường **line vty** và **đặt mật khẩu**

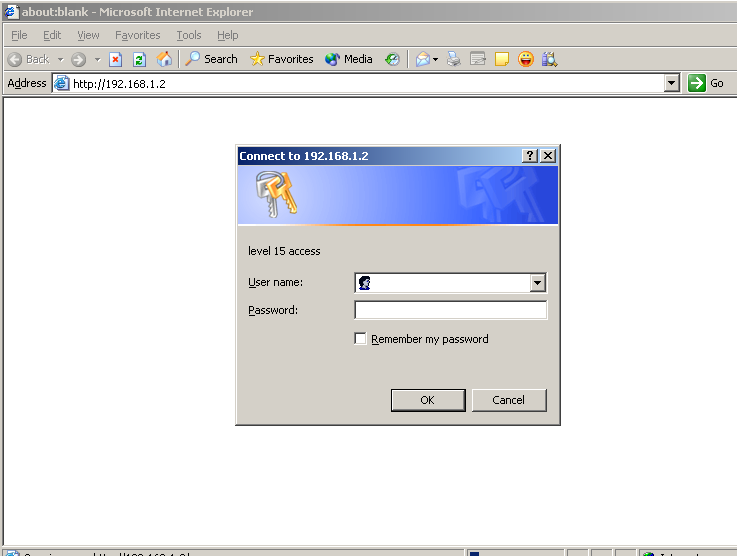
cho đường này(ở đây là **Cisco**) TTG2(config)#line vty 0 4



TTG2(config-line)#login TTG2(config-line)#password **cisco Telnet :**

**Duyệt web :**

- Bạn nhập vào User Name và Password



**User name: TTG2**

**Password : cisco**

- Các bước trên đã thành công,bạn thực hiện việc cấu hình Access list

TTG2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. TTG2(config)#access-list 101 deny tcp 11.X.0.2 0.0.0.0 192.168.1.2 0.0.0.0 eq telnet TTG2(config)#interface s0/1/0

TTG2(config-if)#ip access-group 101 in

- Bạn thực hiện lại việc Telnet như trên,bạn nhận thấy quá trình Telnet không thành công nhưng bước duyệt Web của bạn cũng không thành công.

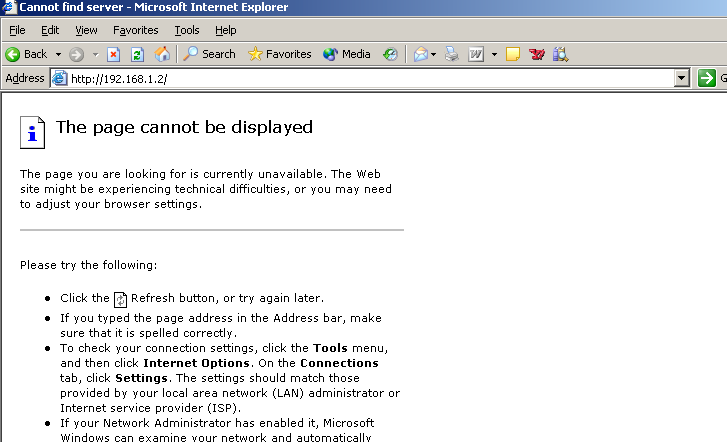
- Theo yêu cầu bạn chỉ ngăn cấm Telnet nhưng cho phép quá trình duyệt Web

**Telnet :**



**Duyệt Web :**

- Để thành công bước duyệt Web,bạn thực hiện câu lệnh thay đổi việc **Deny any mặc**



**định** của Access List.

TTG2(config)#access-list 101 permit ip any any

- Bạn chú ý rằng các câu lệnh trong Access List extended không giống như trong Access

List Standard vì trong Access List Extended,Router sẽ kiểm tra cả địa chỉ nguồn,đích,giao thức

và port..**Permit ip any any** có nghĩa là cho phép tất cả các địa chỉ nguồn và đích khác(không tìm thấy trong danh sách Access List) chạy trên nền giao thức IP đi qua.

Lúc này bạn thực hiện lại quá trình duyệt web

Bạn nhập vào User Name và Password

User name :TTG2

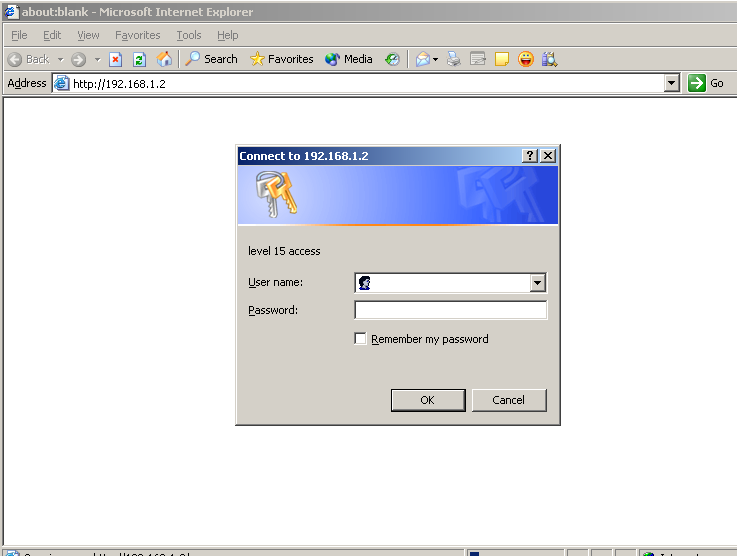
Password : Cisco

-Đến đây bạn đã thành công việc cấu hình cho Extended Access List,bạn đã thực hiện được yêu cầu tạo Access List cho Router với mục đích ngăn cấm việc Telnet vào Router và cho phép quá trình duyệt Web vào Router.Bạn cũng có thể mở rộng thêm đồ hình với nhiều Router để thực tập việc cấu hình Access List cho Router với những yêu cầu bảo mật khác nhau.

**Một số lệnh liên quan đến bài lab :**

**1. Tạo ACL Extended**

Router(config)#**access-list 110 permit**



**tcp 172.16.0.0 0.0.0.255 192.168.100.0**

**0.0.0.255 eq 80**

Các gói tin HTTP có địa chỉ IP nguồn là

172.16.0.x sẽ được cho phép truyền đến

mạng đích là 192.168.100.x

|  |  |
| --- | --- |
|  | 110 : Chỉ số nằm trong khoảng từ 100 đến  199, hoặc từ 2000 đến 2699 sẽ được sử  dụng để tạo ACL extended IP |
| Router(config)#**access-list 110 deny**  **tcp any 192.168.100.7 0.0.0.0 eq 23** | Các gói tin Telnet có địa chỉ IP nguồn sẽ  bị chặn lại nếu chúng truy cập đến đích  là 192.168.100.7 |

**2. Gán ACL extended cho một interface**

|  |  |
| --- | --- |
| Router(config)#**interface fastethernet 0/0** | Chuyển cấu hình vào chế độ interface  fa0/0. |
| Router(config-if)#**ip access-group 110**  **out** | Đồng thời gán ACL 110 vào interface  theo chiều out. Những gói tin đi ra khỏi interface fa0/0 sẽ được kiểm tra. |