**I. Giới thiệu**:

**STANDARD ACCESS LIST**

- Một trong những công cụ rất quan trọng trong Cisco Router được dùng trong lĩnh vực security là Access List. Đây là một tính năng giúp bạn có thể cấu hình trực tiếp trên Router để tạo ra một danh sách các địa chỉ mà bạn có thể cho phép hay ngăn cản việc truy cập vào một địa chỉ nào đó.

- Access List có 2 loại là **Standard Access List** và **Extended Access List**.

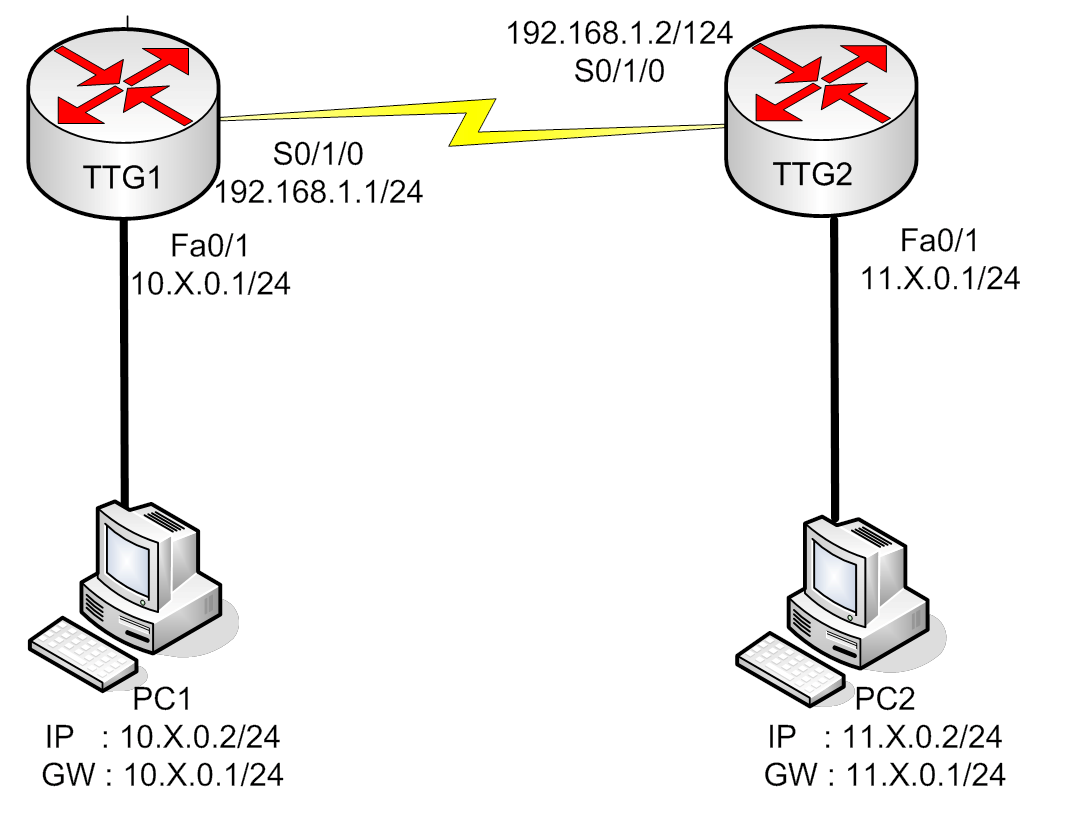
+ **Standard Access List**: đậy là loại danh sách truy cập mà khi cho phép hay

ngăn cản việc truy cập,Router chỉ kiểm tra một yếu tố duy nhất là địa chỉ nguồn(Source Address)

+ **Extended Access List**: đây là loại danh sách truy cập mở rộng hơn so với loại Standard,các yếu tố về địa chỉ nguồn, địa chỉ đích,giao thức,port..sẽ được kiểm tra trước khi Router cho phép việc truy nhập hay ngăn cản.

**II. Mô tả bài lab và đồ hình :**

- Bài Lab này giúp bạn thực hiện việc cấu hình **Standard Access Lis**t cho Cisco Router với mục đích ngăn không cho host truy cập đến router TTG2, ( X là số thứ tự của nhóm do giảng viên phân )



**III. Cấu hình router :**

*- 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

*- PC1:*

IP Address:10.X.0.2

Subnet mask:255.255.255.0

Gate way : 10.X.0.1

*- PC2:*

IP Address:11.X.0.2

Subnet mask:255.255.255.0

Gate way : 11.X.0.1

- Bạn thực hiện việc định tuyến cho các Router như sau(**Dùng giao thức RIP**): TTG1(config)#router rip

TTG1(config-router)#version 2

TTG1(config-router)#network 192.168.1.0

TTG1(config-router)#network 10.0.0.0

TTG2(config)#router rip

TTG1(config-router)#version 2

TTG2(config-router)#network 192.168.1.0

TTG2(config-router)#network 11.0.0.0

- Bạn thực hiện kiểm tra quá trình định tuyến: TTG2#ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

TTG2#ping 11.X.0.1

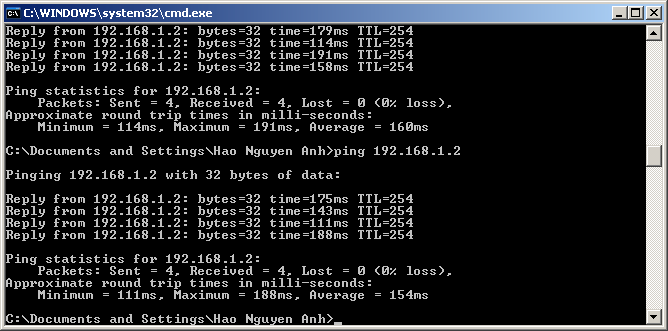
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.0.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

TTG2#ping 11.X.0.2



Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/40 ms

- Sau quá trình định tuyến,kiểm tra chắc chắn rằng mạng đã được thông,bạn thực hiện việc tạo

Access List Standard để ngăn không cho PC1 ping vào TTG2.

- Bạn thực hiện tạo **Access List** trên **Router TTG2** như sau:

TTG2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. TTG2(config)#access-list 1 deny 11.X.0.2 0.0.0.0

*//từ chối sự truy nhập của địa chỉ 11.0.0.2//*

- Lúc này bạn thực hiện lệnh Ping từ Host1 đến TTG2

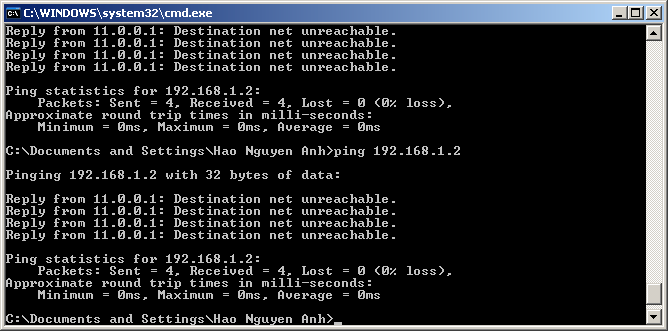
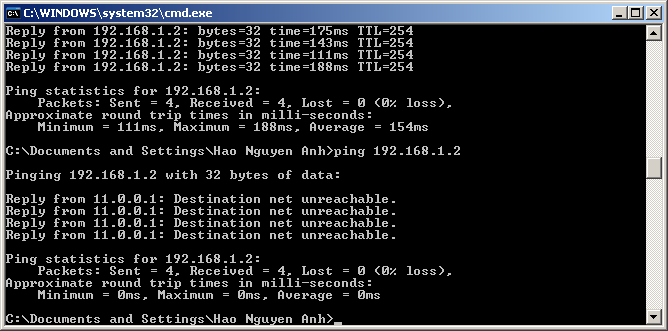
- Bạn thấy lệnh Ping thực hiện vẫn thành công, lý do là bạn chưa mở chế độ Access list trên interface s0/1/0 của router TTG2

TTG1(config)#interface s0/1/0

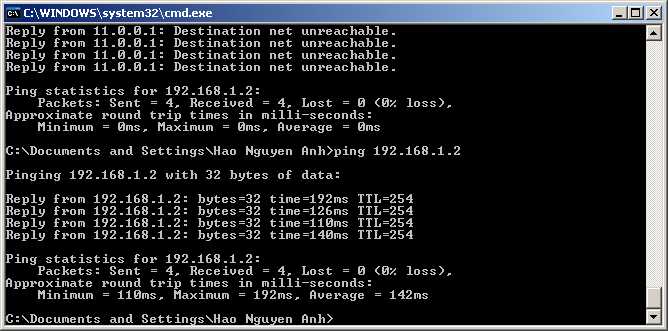
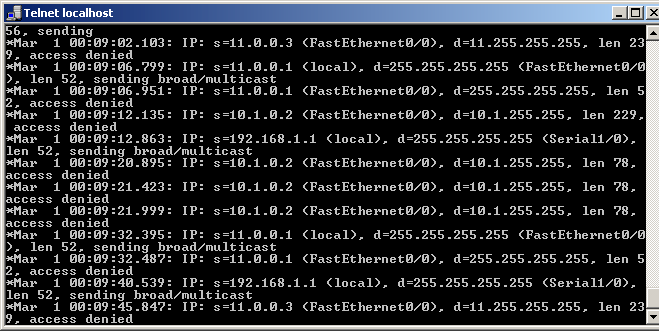
TTG1(config-if)#ip access-group 1 in

- Sau khi apply access list vào interface s0/1/0, ta ping từ PC1 đến TTG2.

- Bây giờ ta đổi địa chỉ của PC thành 11.X.0.3, và thử ping lại 1 lần nữa.



- Bạn thấy lệnh Ping vẫn không thành cộng, lý do là khi không tìm thấy địa chỉ source (địa chỉ lạ) trong danh sách Access list, router sẽ mặc định thực hiện **Deny any,**vì vậy bạn phải thay đổi mặc định này. Sau đây là lệnh **debug ip packet** tại TTG2 khi thực hiện lệnh ping trên.



TTG1(config)#access-list 1 permit any

- Lúc này bạn thực hiện lại lệnh Ping từ PC1 đến TTG2

- Bạn thấy lệnh Ping đã thành công, đến đây bạn đã cấu hình xong Standard Access List.

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

**1. Tạo ACL Standard**

|  |  |
| --- | --- |
| Router(config)#**access-list 10 permit**  **172.16.0.0 0.0.255.255** | Tất cả các gói tin có địa chỉ IP nguồn là  172.16.x.x sẽ được phép truyền tiếp. |
|  | 10 : Chỉ số nằm trong khoảng từ 1 đến 99, hoặc 1300 đến 1999, được sử dụng cho ACL  standard. |
| Router(config)#**access-list 10 deny host**  **172.17.0.1** | Tất cả các gói tin có địa chỉ IP nguồn là  172.17.0.1 sẽ được phép truyền tiếp. |
| Router(config)#**access-list 10 permit any** | Tất cả các gói tin của tất cả các mạng sẽ  được phép truyền tiếp. |

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

|  |  |
| --- | --- |
| Router(config)#**interface fastethernet 0/0** | Chuyển cấu hình vào chế độ interface  fa0/0. |
| Router(config-if)#**ip access-group 10 in** | Câu lệnh này được sử dụng để gán ACL  10 vào interface fa0/0. Những gói tin đi vào router thông qua interface fa0/0 sẽ được kiểm tra. |
| Router(config-if)#**ip access-group 10 out** | Câu lệnh này được sử dụng để gán ACL  10 vào interface fa0/0. Những gói tin đi ra router thông qua interface fa0/0 sẽ được kiểm tra. |
|  | \* Chú ý : Mỗi Interface chỉ được gán 1 chiều in hoặc out |

**3. Kiểm tra ACL**

|  |  |
| --- | --- |
| Router#**show ip interface** | Hiển thị tất cả các ACL được gán vào  interface. |
| Router#**show access-lists** | Hiển thị nội dung của tất cả các ACL trên |

|  |  |
| --- | --- |
|  | router. |
| Router#**show access-list *access-list-***  ***number*** | Hiển thị nội dung của ACL có chỉ số được  chỉ ra trong câu lệnh. |
| Router#**show access-list *name*** | Hiển thị nội dung của ACL có tên được chỉ  ra trong câu lệnh. |

**4. Xóa ACL**

Router(config)#**no access-list 10** Xóa bỏ ACL có chỉ số là 10.