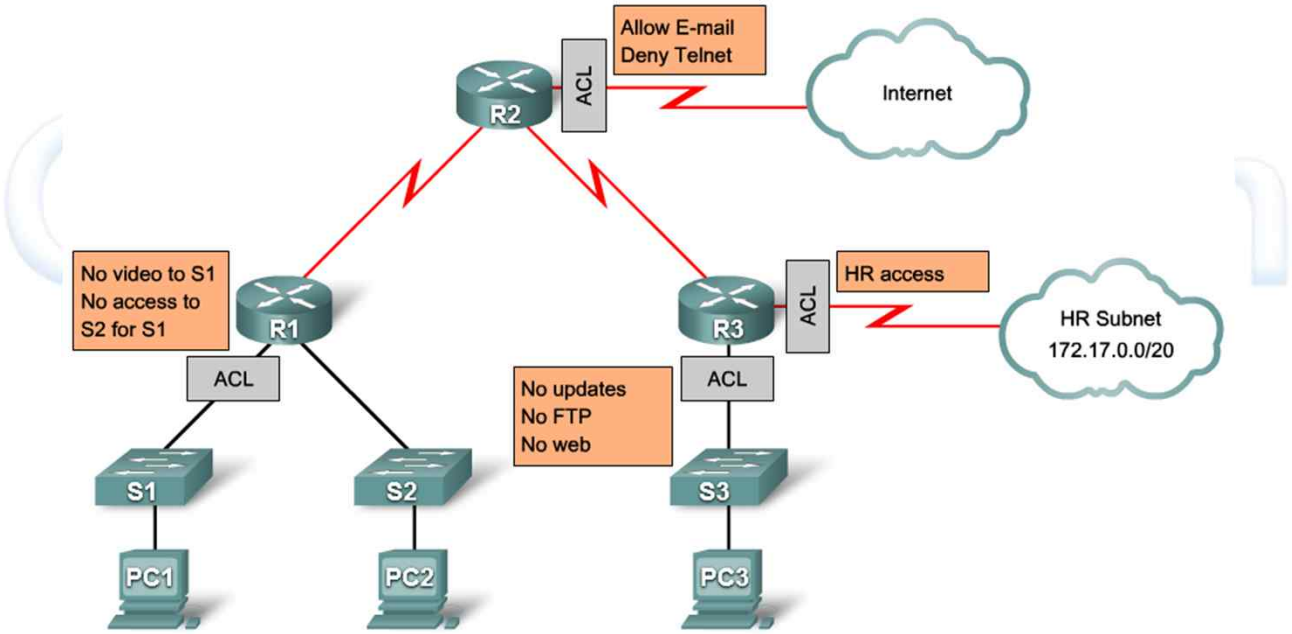
Access List and Their Applications

ACL(Access Control List) 개요

Why Use Access Lists ?

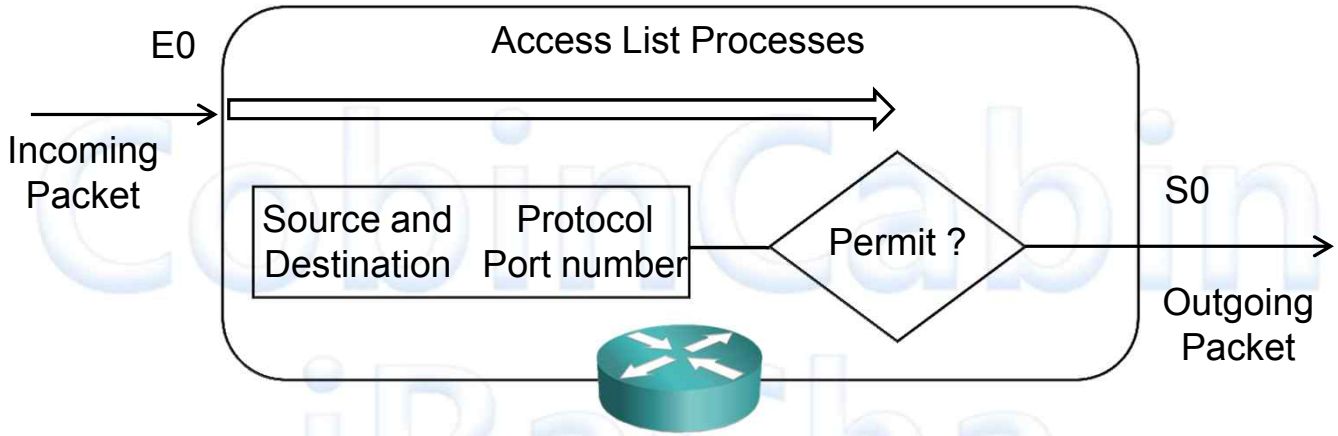


- ACL(Access Control List)
  - Interface로 들어오고 나가는 패킷을 분석해서 정해진 규칙에 따라 패킷을 전송하거나 차단함으로써 네트워크 접근을 제어
  - Packet을 식별해서 필터링, 분류, 그리고 변환해주는 작업을 수행
  - 사용자의 네트워크에 보안성을 제공

Access List and Their Applications

ACL(Access Control List) 종류

Types of Access Lists



- Numbered Access List
  - Filter list 조합을 숫자로 구분
  - Entry를 추가하거나 지울 수 없다
- Named Access List
  - Filter list 조합을 이름으로 구분
  - Entry를 추가하거나 지울 수 있다.

- Standard Access List
  - Source Address를 검사한다
  - 검사결과에 따라 전체 Protocol Suite에 대한 Packet 출력을 허용하거나 거부한다
- Extended Access List
  - Source Address와 Destination Address를 모두 검사한다
  - 특정 Protocol, Port번호, 다른 매개변수를 검사하여 유연하게 제어가 가능하다

Access List and Their Applications

ACL(Access Control List) 종류

How to Identify Access Lists

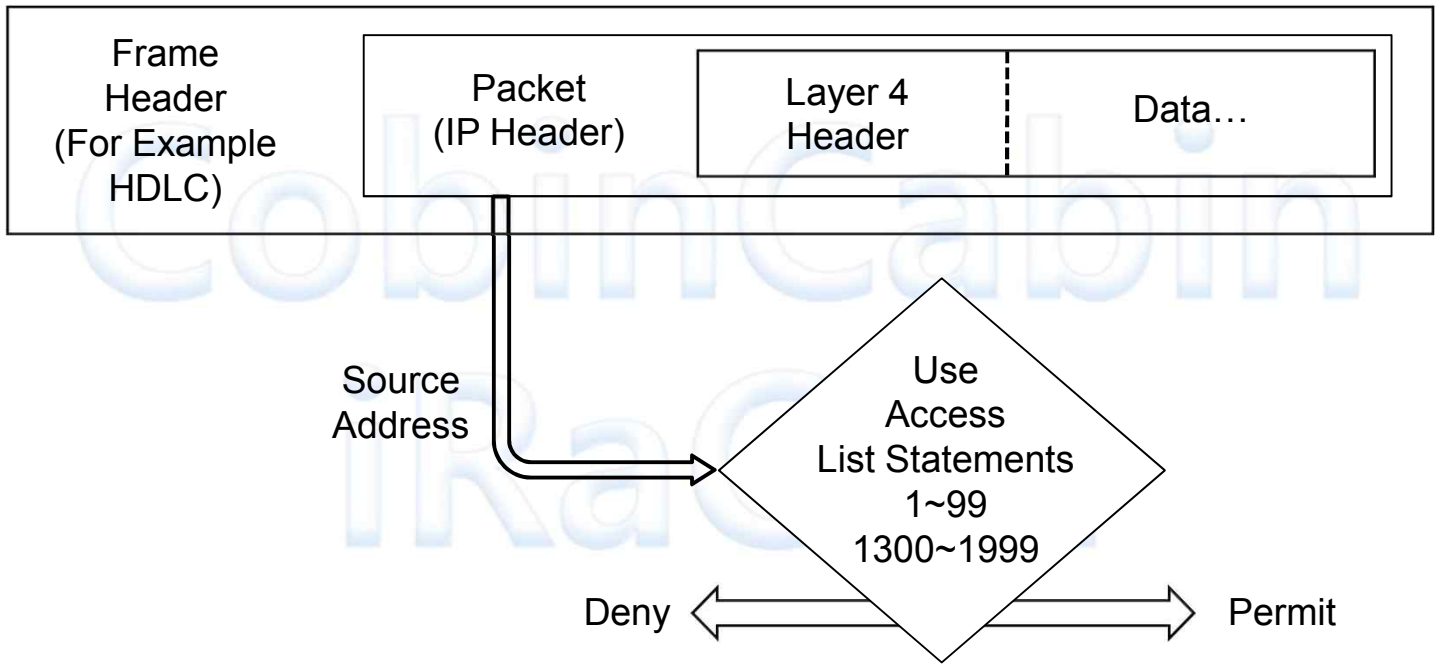
Access List Type	Number Range/Identifier
Standard	1~99, 1300~1999
Extended	100~199, 2000~2699
Named	Name

- Standard ACL (1~99)은 IP Packet의 Source Address를 검색
- Extended ACL (100~199)은 Source & Destination Address와 Port 그리고, Protocol을 검색
  - Protocol : IP, ICMP, UDP, TCP등
- Standard List (1300~1999) : Expanded Range
- Extended IP List (2000~2699) : Expanded Range
- Named ACL은 Standard와 Extended 이름으로 선언하여 각 조건을 검사한다

Access List and Their Applications

ACL(Access Control List) 종류

Testing Packets with Standard Access Lists



Access List and Their Applications

ACL(Access Control List) 동작

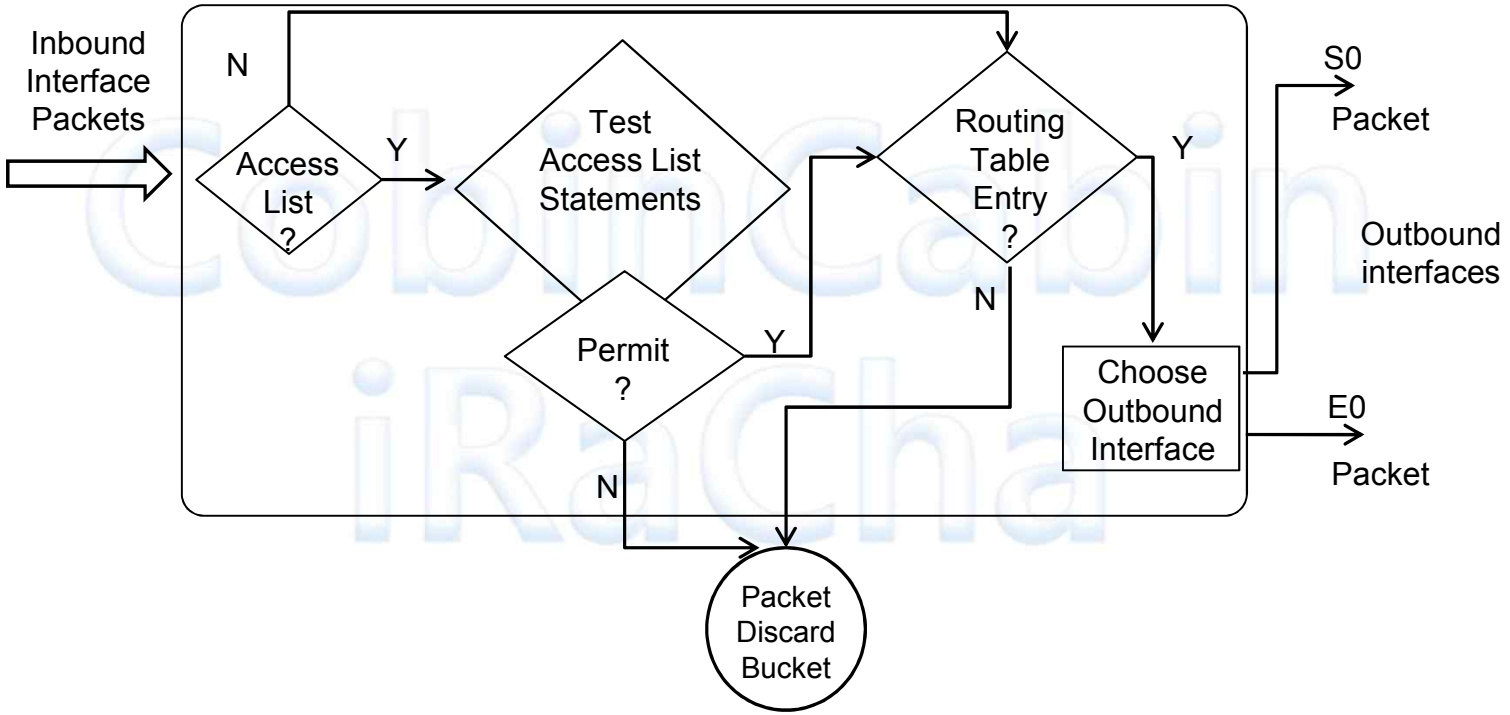
ACL Operation

- IP Address, Port & Protocol정보를 검사하여 동작을 결정한다.
- ACL 명령은 한 번에 한 명령씩 위에서 부터 순차적으로 처리된다.
  - Packet header가 ACL명령과 일치하면, 나머지 부분 검사 생략
  - Packet header가 ACL 명령과 일치하지 않으면, 다음 명령에 의해서 검사 된다.
  - Packet header가 모든 ACL명령과 일치 하지 않으면, 거부 명령으로 자동 차단

Access List and Their Applications

ACL(Access Control List) 동작

Inbound ACL Operation

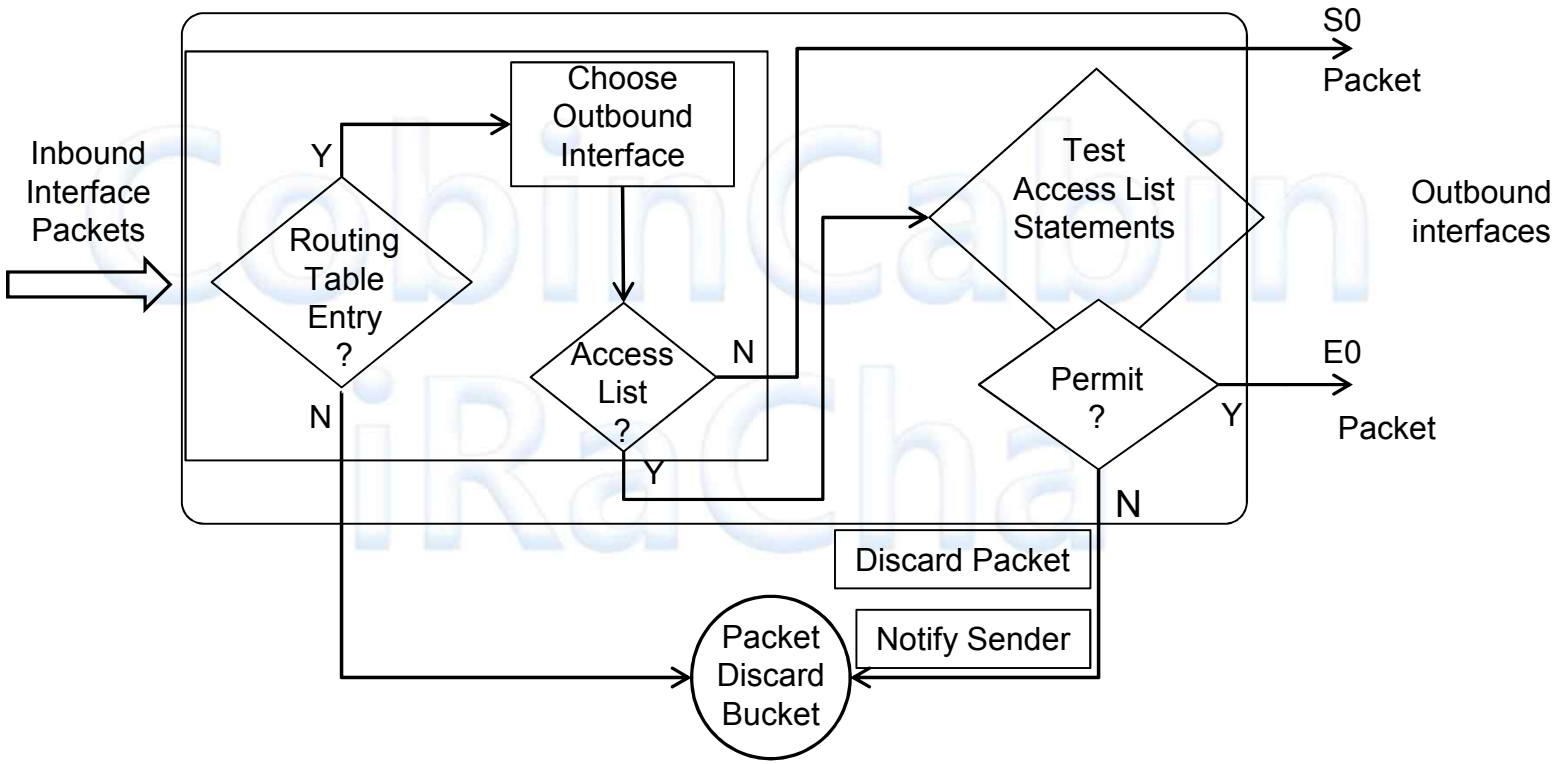


- Access List에 매치되지 않는 모든 Packet은 암시적으로 거부된다

Access List and Their Applications

ACL(Access Control List) 동작

Outbound ACL Operation

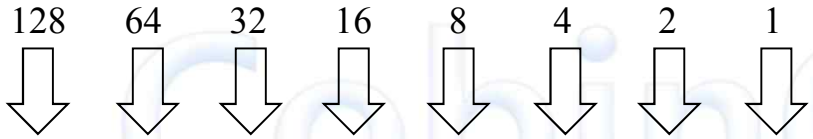


- Access List에 매치되지 않는 모든 Packet은 암시적으로 거부된다

Access List and Their Applications

ACL(Access Control List) 동작

Wildcard Bits : How to Check the Corresponding Address Bits



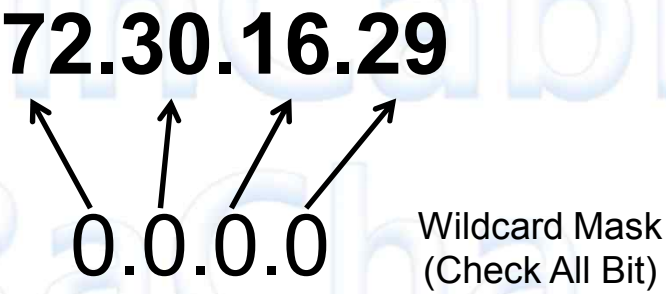
0	0	0	0	0	0	0	0	Check All Address Bits (Match All)
0	0	1	1	1	1	1	1	Ignore Last 6 Address Bits
0	0	0	0	1	1	1	1	Ignore Last 4 Address Bits
1	1	1	1	1	1	0	0	Check Last 2 Address Bits
1	1	1	1	1	1	1	1	Do Not Check Address (Ignore Bits in Octet)

- Wildcard mask bit 0은 대응 bit값을 검사하라는 것을 의미한다
- Wildcard mask bit 1은 대응 bit값을 검사하지 말고 무시하라는 것을 의미한다

Access List and Their Applications

ACL(Access Control List) 동작

Wildcard Bits to Match a Specific IP Host Address

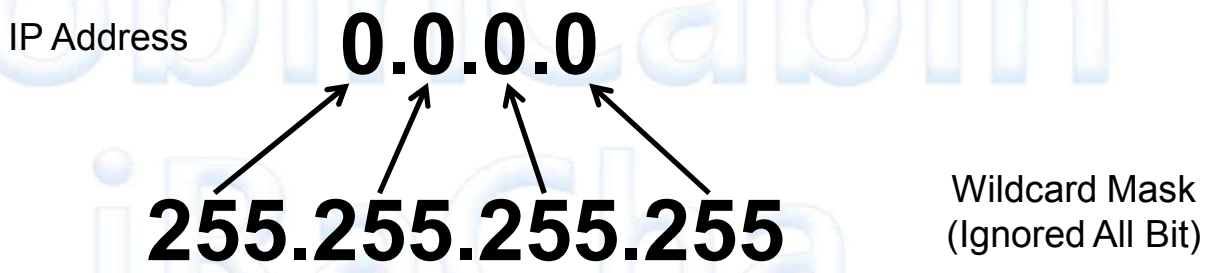


- 모든 Address Bit 검사 (모두 일치)
  - 1개의 IP Host Address만 검사
- 172.30.16.29 0.0.0.0은 모든 Address를 검사해서 매치되는 주소 지정
  - 172.30.16.29 IP host 지정
- 하나의 IP를 지정하기 위해 host 사용
  - 172.30.16.29 0.0.0.0를 host 172.20.16.29로 사용할 수도 있다

Access List and Their Applications

ACL(Access Control List) 동작

Wildcard Bits to Match Any IP Address



- 모든 Address Bit 무시 (Match Any)
  - 모든 IP Address
- 모든 Address를 받아들이려면 IP Address는 0.0.0.0을 입력하고 Wildcard mask는 255.255.255.255를 지정한다
- 관리자는 모든 주소를 지정할 목적으로 0.0.0.0 255.255.255.255를 명시하는 대신 any라는 문자를 사용할 수 있다

Access List and Their Applications

ACL(Access Control List) 동작

Wildcard Bit to Match IP Subnets

- 172.30.16.0/24에서 172.30.31.0/24까지의 IP Subnet 검사하기
  - Address and wildcard mask : 172.30.16.0 0.0.15.255

Access List and Their Applications

ACL(Access Control List) 설정

Standard IP Access List Configuration

```
Router(config)#access-list access-list-number {permit | deny} source [mask]
```

- Access-list-number : Entry가 속할 list 번호 설정. 1~99, 1300~1999사이의 번호가 들어간다
- permit | deny | remark는 해당 Entry에 매치되면 취할 Action을 정의
- Source는 송신지 IP Address를 정의한다
- mask는 Wildcard mask를 사용하여 Address 필드의 어느 비트들이 일치되어야 하는지 설정한다
- Interface에서 no ip access-list *access-list-number*명령을 사용하여 적용된 Access-list를 제거한다

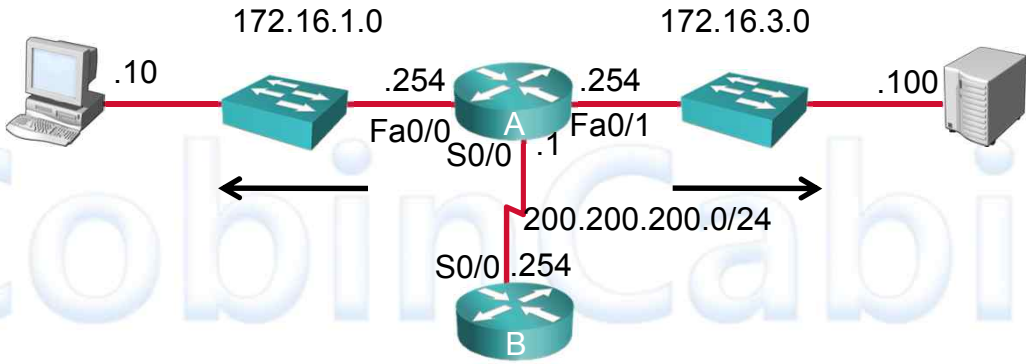
```
Router(config-if)#ip access-group access-list-number  {in | out}
```

- List를 적용할 Interface에서 설정한다
- Inbound또는 Outbound시 검사하도록 설정한다
- Default = outbound
- 적용된 Access-list를 제거
  - Interface에서 no ip access-group *access-list-number*명령을 사용하여

Access List and Their Applications

ACL(Access Control List) 설정

Standard IP Access List Example 1



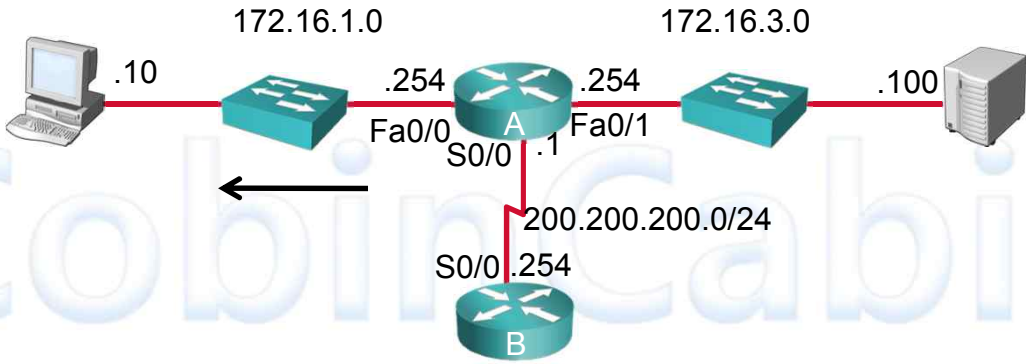
- 외부 접근 차단
- RouterA(config)#access-list 1 permit 172.16.0.0 0.0.255.255
  - implicit deny all – not visible in the list
  - access-list 1 deny 0.0.0.0 255.255.255.255

- RouterA(config)#interface Fa0/0
- RouterA(config-if)#ip access-group 1 out
- RouterA(config)#interface Fa0/1
- RouterA(config-if)#ip access-group 1 out

Access List and Their Applications

ACL(Access Control List) 설정

Standard IP Access List Example 2



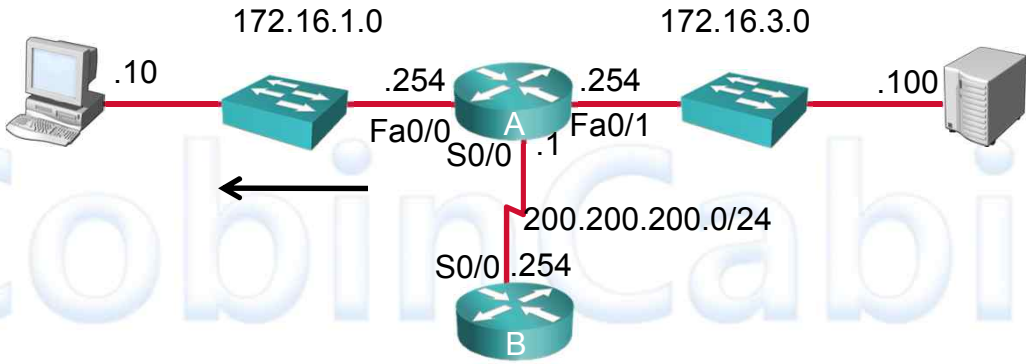
- 호스트 컴퓨터의 서버 접근 차단
- RouterA(config)#access-list 1 deny 172.16.1.10 0.0.0.0
- RouterA(config)#access-list 1 permit 0.0.0.0 255.255.255.255
  - implicit deny all
  - access-list 1 deny 0.0.0.0 255.255.255.255

- RouterA(config)#interface Fa0/1
- RouterA(config-if)#ip access-group 1 out

Access List and Their Applications

ACL(Access Control List) 설정

Standard IP Access List Example 3



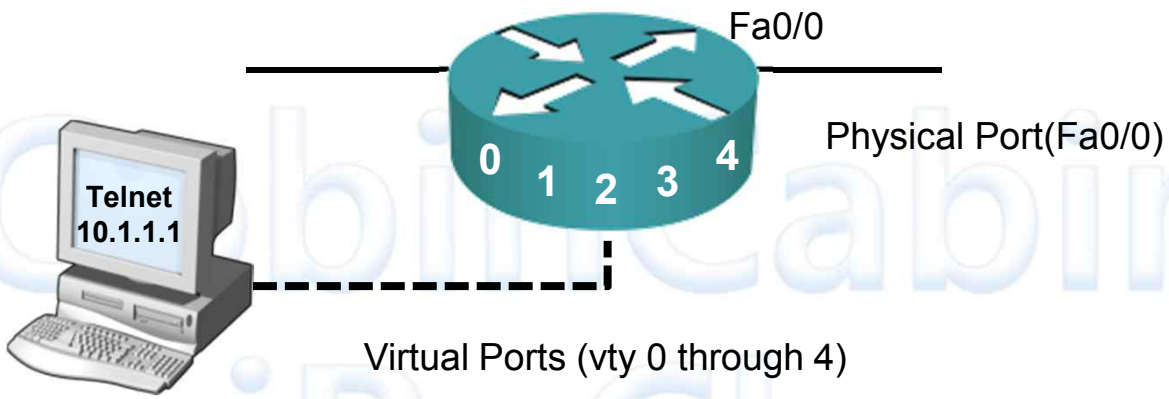
- 172.16.3.0네트워크 차단
- RouterA(config)#access-list 1 deny 172.16.3.0 0.0.0.255
- RouterA(config)#access-list 1 permit any
  - implicit deny all
  - access-list 1 deny 0.0.0.0 255.255.255.255

- RouterA(config)#interface Fa0/0
- RouterA(config-if)#ip access-group 1 out

Access List and Their Applications

ACL(Access Control List) 설정

How to Control vty Access



- VTY 접속 제어
  - VTY는 라우터에 Telnet 접속을 위해 할당된 가상 포트이다
  - Numbered ACL만 VTY에 적용된다

Access List and Their Applications

ACL(Access Control List) 설정

vty Commands

```
Router(config)#line vty {vty# | vty-range}
Router(config)#
```

- 접속 제어할 포트 번호를 활성화 한다

```
Router(config-line)#access-class access-list-number {in | out}
Rotuer(config-line)#
```

- 적용할 Access-list를 적용한다

Access List and Their Applications

ACL(Access Control List) 설정

vty Access Example

```
Router(config)#access-list 12 permit 192.168.1.0 0.0.0.255
(implicit deny all)

Router(config)#line vty 0 4
Router(config-line)#access-class 12 in
Router(config-line)#
```


- Controlling Inbound Access
- 192.168.1.0/24 Subnet에 해당하는 IP Address를 갖는 호스트만 접속을 허용한다

Access List and Their Applications

ACL(Access Control List) 검증

Monitoring Access List Statements

```
Router#show {protocol} access-list {access-list number}

Router#show access-list {access-list number}

Router#show access-lists
Standard IP access list 1
      permit 10.2.2.1
      permit 10.3.3.1
      permit 10.4.4.1
      permit 10.5.5.1
Extended IP access list 101
      permit tcp host 10.22.22.1 any eq telnet
      permit tcp host 10.33.33.1 any eq ftp
      permit tcp host 10.44.44.1 any eq ftp-data
```