

# 라우터를 활용한 네트워크 보안설정

2005. 5.

인프라보호단 / 보안관리팀

## 목 차

I . 라우터를 활용한 네트워크 보안.....	1
1. 라우터 자체 보안 .....	1
2. 라우터를 활용한 네트워크 보안.....	35
<별첨 #1> 라우터 보안 체크하기 .....	45

## 그림 목차

[그림 1] ipconfig 실행화면.....	2
[그림 2] 라우터의 접근 방법.....	3
[그림 3] 라우터에 설치된 인터페이스 목록.....	10
[그림 4] access-group 설정 예.....	11
[그림 5] extended access-list 설정 예.....	12
[그림 6] 설정파일 조회.....	15
[그림 7] access-list 룰을 삭제하는 과정.....	16
[그림 8] 설정파일 조회.....	17
[그림 9] access-list 조회.....	17
[그림 10] line 명령어.....	18
[그림 11] 원격 접근 제어 설정.....	19
[그림 12] 리스너 자체 off 설정.....	19
[그림 13] SNMP 설정.....	21
[그림 14] SNMP 설정 해제.....	22
[그림 15] small-servers 서비스 중지.....	23
[그림 16] finger 서비스 중단.....	23
[그림 17] http 서비스 중단.....	24
[그림 18] 서비스 중단 설정.....	24
[그림 19] 인터페이스 모드에서 서비스 중단 설정 예.....	25

[그림 20]	사용하지 않는 인터페이스 다운.....	27
[그림 21]	다운된 인터페이스 재가동.....	27
[그림 22]	암호화가 설정되지 않은 config .....	28
[그림 23]	암호화 명령어 실행.....	29
[그림 24]	암호화가 적용된 예.....	29
[그림 25]	exec-timeout 설정.....	30
[그림 26]	buffered 로깅 설정.....	31
[그림 27]	show logging 실행 화면.....	31
[그림 28]	clear logging 화면.....	31
[그림 29]	syslog logging 설정.....	32
[그림 30]	현재 시간 조회.....	33
[그림 31]	시간 및 timezone 설정.....	33
[그림 32]	타임서버와 시간 동기화.....	33
[그림 33]	비정상 ip 대역 필터링.....	36
[그림 34]	악성 포트를 필터링 한 예.....	37
[그림 35]	icmp 패킷 필터링 예.....	38
[그림 36]	통합된 access-list 설정.....	38
[그림 37]	access-group 에 적용한 예.....	39
[그림 38]	access-list 설정.....	40
[그림 39]	access-group 설정.....	40
[그림 40]	Null 0 인터페이스.....	41
[그림 41]	Null 라우팅 설정.....	41
[그림 42]	blackhole 필터링 설정 해제.....	42
[그림 43]	URPF 설정.....	43
[그림 44]	CEF 가 enable 되어 있지 않을 경우.....	43
[그림 45]	URPF 설정.....	43
[그림 46]	리스너 자체 off 설정.....	47

## I. 라우터를 활용한 네트워크 보안 설정

라우터는 일반 PC방이나 기업 등에서 자주 사용되고 있지만 운영의 특성상 IT 관련 종사자에게도 익숙하게 접하기는 쉽지 않은 것이 사실이다. 그러나 최근의 공격 경향이 PC나 서버에만 머무르지 않고 라우터나 스위치 등 네트워크 장비를 직접 대상으로 삼는 경우가 증가하고 있는데, 만약 이러한 공격으로 인하여 네트워크 장비에 장애가 발생할 경우에는 이하의 시스템 전체가 직접적인 영향을 받게 되므로 그 피해는 견줄 수 없이 커질 것이다.

또 한 가지 경향으로는 공격의 양상이 단순히 한 시스템에만 머무르지 않고 웜(worm)이나 봇넷(botnet)과 같이 대단위의 트래픽이나 짧은 시간에 많은 패킷을 유발하여 네트워크에 직접적이고 심각한 장애를 유발하는 경우가 많이 발생하고 있으며 이 추세는 앞으로도 더욱 가속화 될 것으로 보인다. 굳이 지난 1.25 대란을 언급하지 않더라도 이러한 경우 문제의 원인을 찾고 대처하기 위해서는 각 개별 시스템 수준에서 처리하기에는 한계가 있으며 네트워크 수준에서 대처하여야 한다. 따라서 각 기관에서 라우터를 운영하고 있다면 라우터에 대한 관리와 라우터 등 네트워크 장비를 이용하여 보안을 강화할 수 있는 방안에 대하여 고민하여야 한다. 실제로 라우터(router)와 스위치의 기능은 원하는 목적지를 찾아 패킷을 포워딩 또는 스위칭해 주는 것이지만, 모든 트래픽이 이 장비를 통과하는 만큼 네트워크 장비에서 제공하는 접근 통제 등 여러 보안 기능을 조금만 활용해도 굳이 고가의 상용 솔루션을 구입하지 않고도 상용 솔루션 수준의 기능이나 심지어는 그 이상의 기능을 이용하여 네트워크 보안을 상당 부분 강화할 수 있는 것이 사실이다. 따라서 라우터로 대표되는 네트워크 장비 자체에 대한 보안 설정 방법과 아울러 네트워크 장비를 통한 네트워크 보안 구성 방도에 대해 알아본다.

### 1. 라우터 자체 보안

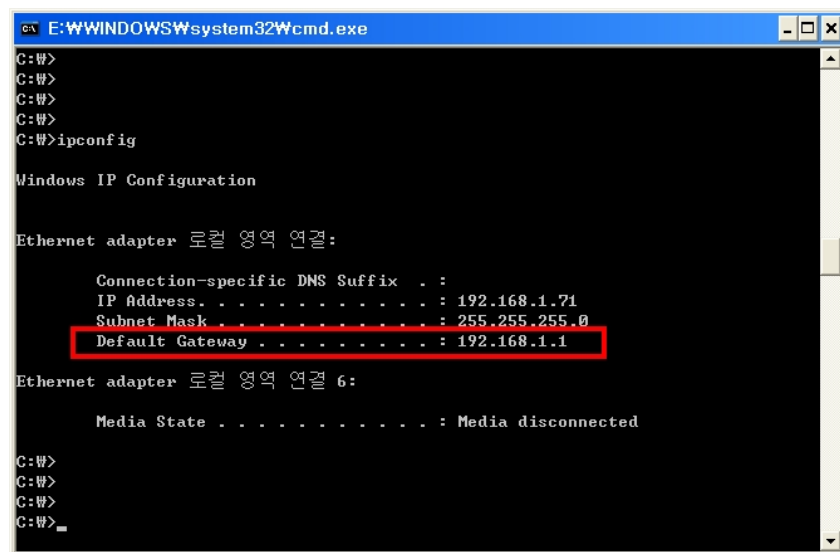
라우터 자체의 보안은 일반 시스템 보안과 크게 다를 바는 없다. 다만 명령어 형식과 방법에만 차이가 있을 뿐 보안의 원리는 동일하게 적용된다. 이를테면 암호 보안이나 불필요한 서비스에 대한 정책, 허가된 사용자만 접근할 수 있도록 엄격한 접근 통제 등은 시스템이나 네트워크 장비에 관계없이 공통적인 정책이 될 수 있을 것이다.

#### STEP 1. 라우터 암호 설정하기

어떠한 장비든 장비와 직접 연결된 콘솔이나 원격에서 네트워크를 통해 로그인

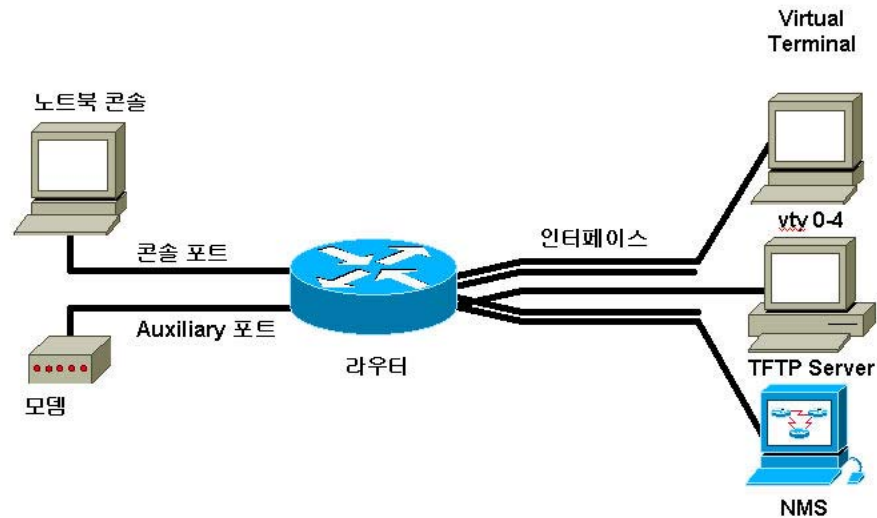
가능한 경우 암호 설정은 가장 중요하면서도 기본이 되는 보안 설정 단계이다. 그러나 실제로 라우터를 사용하고 있는 PC방이나 중소 규모의 업체에서는 보안의 첫 단계라 할 수 있는 암호조차 제대로 설정하지 않고 사용하는 경우가 대부분이다. 이는 대부분의 영세한 업체는 별도로 라우터를 관리할 수 있는 인력이 부족하여 설치 이후 전혀 관리를 하지 못하고 있으며 라우터를 설치하고 관리해 주는 업체의 직원들도 보안 관념이 부족하여 단지 관리상의 편리함 때문에 로그인 암호를 설정하지 않거나 상호등 쉽게 추측이 가능한 기본 암호를 일괄적으로 설정하여 사용하기 때문이다. 이렇듯 암호에 대한 보안을 고려하지 않는 것은 문은 있으나 잠금 기능을 사용하지 않거나 문을 열어 둔 것과 같을 만큼 매우 위험한 것임에도 불구하고 이 중요성을 간과하곤 한다.

실제로 자신이 속해있는 기관에서 라우터를 사용한다면 혹 쉬운 암호를 사용하고 있지는 않은지 각자 확인해 보기 바란다. 시작->실행에서 **cmd**나 **command**를 입력 후 DOS 창에서 아래와 같이 "**ipconfig**"를 실행하면 ip에 대한 정보가 나오는데, 이때 Default Gateway로 등록된 것이 라우터 일 것이다. 이 ip로 telnet 접속을 해 보면 암호를 묻는 창이 나오는데, 여기에 쉽게 추측이 가능한 문자열을 입력해 보아 확인하면 된다.



[그림 1] ipconfig 실행화면

아래는 라우터에 접근 가능한 방법과 각각의 모드에서 라우터의 암호를 설정하는 방법을 보여주고 있다. 물론 암호는 cisco 나 router, admin 또는 상호명 등 일반적으로 추측하기 쉬운 암호를 사용하지 않도록 하고, 관리자 중 퇴사자나 부서이동 등이 있을 경우에는 수시로 암호를 변경하여 암호 관리를 철저히 하여야 할 것이다.



[그림 2] 라우터의 접근 방법

어떠한 방법으로 접근하든 라우터에 로그인하기 위해서는 username 없이 초기 암호를 입력하여 로그인해야 하는데 이때 프롬프트는 Router> 와 같이 되며 이때의 모드를 'User exec 모드'라고 한다. 이후 **enable** 또는 **en** 명령어를 실행하여 다시 암호를 입력하면 프롬프트가 Router#와 같이 되며 이때의 모드를 '**Privileged EXEC 모드**' 또는 '**enable 모드**'라 한다. 여기에서 초기에 User exec 모드로 들어가기 위해 입력하는 암호는 일반 사용자, Privileged EXEC 모드 또는 enable 모드는 일종의 root 또는 관리자라고 생각하면 된다. 아래는 이 때의 로그인 과정을 보여주고 있다.

```

Password: xxxxxxx
Router>enable
Password: xxxxxx
Router#

```

<참고> 라우터 사용 모드

<b>User EXEC 모드</b>	한정된 명령어만 사용이 가능하며 주로 라우터의 간단한 상태등을 조회할 수 있다. 프롬프트는 Router> 와 같이 보이게 된다.
<b>Privileged EXEC 모드</b>	재부팅이나 라우팅등 라우터에서의 모든 명령어에 대한 수행이 가능하며 프롬프트는 Router# 와 같이 보이게 된다.
<b>Global Configuration 모드</b>	Privileged EXEC 모드에서 라우터 전반적인 설정을 변경하고자 할 때의 모드로서 Router(config)# 와 같이 보이게 된다. 만약 특정 인터페이스나 특정 라우팅등을 변경하고자 할 때에는 아래의 Other Configuration 모드가 사용된다.
<b>Other Configuration 모드</b>	좀 더 복잡하고 세부적인 설정을 하는 메뉴로서 Router(config - mode)#와 같이 보이게 된다. 설정이 끝난 후에는 exit 나 Ctrl+Z를 입력하면 된다.

#### <참고> 일반적인 라우터 접근 방법

##### 가. Console Password (노트북을 이용한 Console 접속 시 사용)

먼저 초기에 라우터를 셋팅하거나 이후에 작업을 할 경우 대부분 노트북등을 라우터에 연결하여 직접 콘솔에서 작업하는 경우가 많다. 이는 원격으로 작업시 만약의 경우 연결이 끊길 수도 있기 때문이다. 따라서 라우터의 설정을 변경하거나 재부팅 등을 한다면 아무리 숙련된 관리자라 하더라도 원격에서 하지 말고 콘솔에서 작업 하는 것이 좋다. 설정을 변경하려면 User exec 모드에서는 불가능하며 반드시 Privileged EXEC 모드로 들어가야 한다. 따라서 로그인후 enable를 실행하여 Privileged EXEC 모드로 들어가도록 한다. 이후 설정을 변경하기 위해 "conf t"를 실행하여 Global Configuration 모드로 들어간 후 콘솔을 지정하여 암호를 재설정하면 된다. 이때의 설정 방법은 아래와 같다. 여기에서 xxxxx는 각자 콘솔에서 노트북으로 연결하였을 때의 User EXEC 모드로 로그인할 때의 암호를 뜻한다.

```

C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password xxxxx
Router(config-line)#^Z
Router#_

```

##### 나. Terminal(Virtual) Password (telnet등 원격 접속 시 사용)

콘솔에서 초기 셋팅이나 설정 변경등을 한 후 정기적으로 모니터링을 하고자 할 때에는 매번 콘솔에서 작업하려면 번거로우므로 이때는 원격으로 로그인하여 작업하는 경우가 많다. 주로 telnet 이나 ssh를 이용하여 접속하는데, 이때 입력하여야 하는 암호를 Terminal password 또는 Virtual password 라고 한다. 실제로 많이 사용되며 대부분의 비정상적인

로그인 역시 이를 통해 이루어지므로 이 암호는 특히 신경 써서 설정하여야 한다. 반드시 추측하기 어렵고, 자주 변경하도록 하는 것이 좋다.

설정을 변경하려면 User EXEC 모드에서는 불가능하며 반드시 Privileged EXEC 모드로 들어가야 한다. 따라서 로그인후 enable를 실행하여 Privileged EXEC 모드로 들어가도록 한다. 이후 설정을 변경하기 위해 "conf t"를 실행하여 Global Configuration 모드로 들어간 후 vty(virtual terminal) line을 0부터 4까지 지정하여 암호를 재설정하면 된다. 여기에서 0부터 4까지 지정할 경우 동시에 5번의 접속이 가능하며 이때의 설정 방법은 아래와 같다.

여기에서 xxxxx 는 원격으로 User EXEC 모드로 로그인할 때의 암호를 뜻한다.

실제 적용이 되었는지 telnet 으로 접속하여 아래와 같이 확인해 보기 바란다.

```
# telnet router.abc.com
```

```
Trying 192.168.0.1...
```

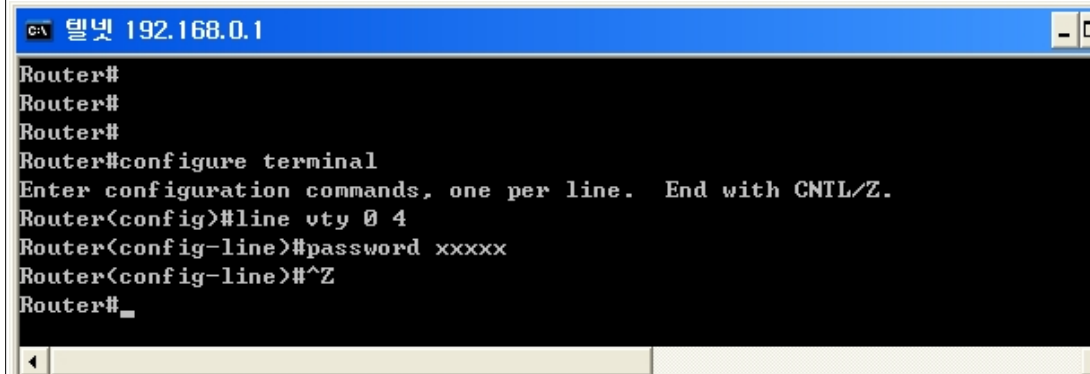
```
Connected to 192.168.0.1 (192.168.0.1).
```

```
Escape character is '^['.
```

```
User Access Verification
```

```
Password:xxxxx <-- 방금 설정한 암호
```

```
Router>
```



```
c:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password xxxxx
Router(config-line)#^Z
Router#_
```

다. Enable Password 및 Enable Secret (enable 모드로 접근시 사용)

User EXEC 모드에서 더 많은 명령어를 실행하거나 설정을 변경하기 위해 Privileged EXEC 모드로 접근하기 위해서는 enable 명령어를 실행하여 암호를 입력 후 로그인하여야 하여야 한다. 이때의 암호는 아래와 같이 enable password 또는 enable secret를 이용할 수 있는데, 각각은 지정한 암호가 평문으로 저장되는지 아니면 암호화되어 저장되는지의 여부에 차이가 있다. 즉, enable password로 지정시에는 지정한 암호가 평문으로 저장되고 enable secret 로 지정시에는 암호화되어 저장된다.

- enable password



C:\ 텔넷 192.168.0.1

```

Router#
Router#
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password xxxxxx
Router(config)#^Z
Router#_

```

- enable secret

C:\ 텔넷 192.168.0.1

```

Router#
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret xxxxxx
Router(config)#^Z
Router#

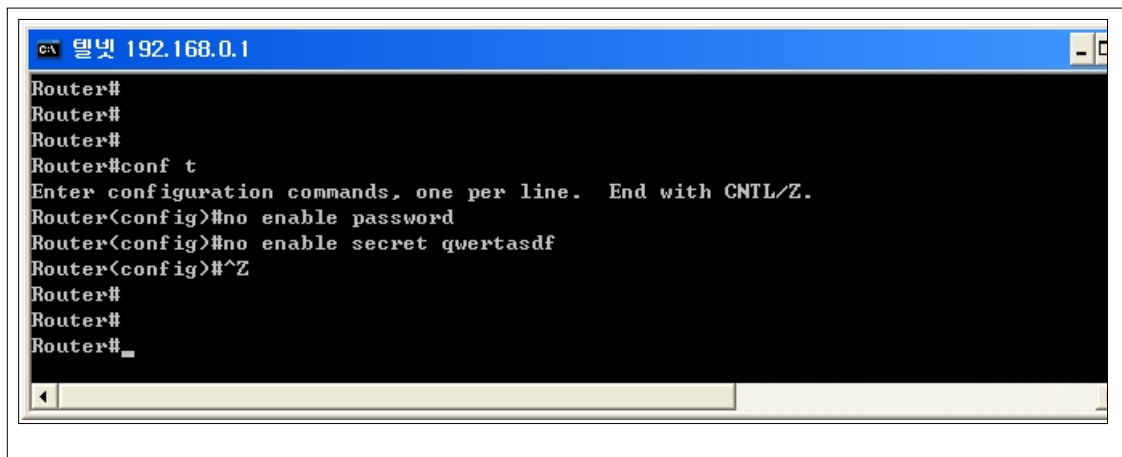
Building configuration...

```

라. 라우터 암호 저장방식

type 0 : 평문으로 저장되는 방식  
type 5 : 단방향의 md5 hash로서 역함수가 존재하지 않는 암호화 방식으로 저장되는 방식  
type 7 : 암호화되지 저장되지만 역함수가 존재하여 암호화된 암호를 통해 원래의 암호를 알 수 있는 방식,

여기에서 "enable password" 는 type 0 의 평문으로 저장되며 "enable secret" 는 역함수가 존재하지 않는 암호화된 형태로 저장되는 것이다. 물론 라우터에서 제공하는 명령어중 “service password-encryption” 을 실행하면 enable password와 같이 평문으로 저장된 암호를 암호화 하지만 이는 type 7 로서 역함수가 존재하여 암호화된 암호를 통해 원래의 암호를 알 수 있다는 한계가 있다. 따라서 먼저 "no enable password"를 실행하여 enable password를 disable 하고 대신 "enable secret" 를 사용할 것을 권장한다. enable password는 enable secret가 없을 때 적용되며 만약, enable password 와 enable secret 가 함께 설정되어 있을 경우에는 enable secret 가 적용된다. 또한 IOS type7의 암호화된 암호를 복호화 하는 즉 암호화된 암호를 해석하는 공개 프로그램이나 상용 프로그램들도 많이 공개되어 있어 인터넷에서 쉽게 다운로드 받을 수 있으므로 혹 암호화된 암호가 유출되었다면 반드시 암호를 변경하도록 하여야 한다.



```
터넷 192.168.0.1
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no enable password
Router(config)#no enable secret qwertasdf
Router(config)#^Z
Router#
Router#
Router#_
```

## STEP 2. access-list 를 이용한 접근제어 설정하기

일반적으로 unix 계열의 경우 tcp wrapper나 리눅스의 경우 iptables와 같은 방화벽을 이용하여 패킷 필터링 기능을 이용하고 있다. 이를 통해 허용된 유저 또는 허용된 패킷만 접근할 수 있도록 설정할 수 있는데, 라우터에서는 access-list 라는 것을 이용하여 특정 패킷을 허용하거나 차단하도록 설정할 수 있다. access-list는 라우터에서 여러 목적으로 사용되며 특히 패킷 필터링시에는 매우 유용하게 사용되므로 사용방법을 반드시 알고 있어야 한다. 라우터에서의 access-list 는 라우터 보안의 기본이라 할 만큼 중요한 역할을 하므로 작동 방식에 대해 정확하게 이해하고, 활용할 수 있도록 충분히 연습을 하여야 한다. 또한 굳이 라우터를 사용하지 않더라도 다른 보안 장비나 프로그램에서도 유사하거나 동일한 형식을 사용하므로 사용 방법을 익혀 두는 것이 좋다.

access-list란 용어 자체에서 설명하듯이 라우터 자체를 향하거나 라우터를 통과하는 패킷에 대한 접근을 제어할 수 있는 명령어로서 크게 **standard access-list**와 **extended access-list**로 나눌 수 있다. standard access-list는 패킷의 소스 ip만으로 패킷을 허용하거나 차단할 수 있으며 반면에 extended access-list는 용어가 의미하듯이 패킷의 소스 ip 뿐만 아니라 목적지 ip, 포트(port), 프로토콜(protocol) 등으로 차단할 수 있어 좀 더 확장된 기능을 이용할 수 있다. 이때 access-list 는 주로 선언되는 번호를 기준으로 분류하는데 1부터 99까지는 standard access-list에서 사용하고 100부터 199까지는 extended access-list에서 사용된다. 즉 선언된 access-list를 해석할 때 access-list 번호를 보고 standard access-list인지 extended access-list인지 확인하면 된다.



## access-list 이용방법

### 가. access-list 룰 설정

- 어떤 패킷에 대해 허용하고 거부할 것인지에 대한 룰 설정
- 소스 ip만으로 필터링한다면 standard access-list를 이용,  
포트와 프로토콜 등 다양한 인자로 필터링한다면 extended access-list를 이용
- access-list 는 중복 설정이 되지 않으므로 만약 기존 번호로 access-list가 설정되어 있었다면 추가할 경우 원하지 않는 결과가 초래될 수 있어 오작동을 하게 되므로 만약 기존에 정의하려는 번호로 access-list가 있었다면 먼저 해당 룰을 삭제한 후 새롭게 설정하여야 함

### 나. 적용할 인터페이스 지정

- 외부의 serial interface 에 적용할 것인지 내부의 ethernet 인터페이스에 적용할 것인지 정함
- 해당 인터페이스에서 어떤 룰을 적용할 것인지는 access-group 110과 같이 access-group 뒤에 룰의 번호를 지정
- 패킷이 인터페이스로 들어오는 패킷인지 나가는 패킷인지에 따라 in과 out을 정의

### 다. 설정내용 확인

- 정상적으로 설정되었는지 확인



## access-list 룰 설정하기

### 가. standard access-list

```
C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 5
Router(config)#access-list 5 permit host 192.168.1.70
Router(config)#access-list 5 permit host 192.168.1.71
Router(config)#access-list 5 deny any
Router(config)#
Router(config)#^Z
Router#sh access-list 5
Standard IP access list 5
    permit 192.168.1.71
    permit 192.168.1.70
    deny any
Router#
Router#
Router#_
```

access-list를 설정한다는 것은 설정을 변경하는 것이므로 enable 모드에서 "conf t"를 입력하여 global configuration 모드로 변경하도록 하여야 한다. 이후 standard access-list 5번을 사용하기 위해 먼저 access-list 5번이 설정되어 있는지 모르니 no access-list 5를 실행하여 access-list 5번을 삭제하였다. 그리고 이제 access-list 5번에 대한 룰을 정의하면 된다. 여기서 먼저 standard access-list의 룰 형식에 대해 알아보면 다음과 같이 표현하면 된다.

```
access-list ACL번호 {permit 또는 deny} {소스주소 wildcard 또는 any}
```

여기에서 ACL 번호는 standard이므로 1부터 99번까지 가능한데, 이 번호는 선후차의 개념이 없으며 단지 각 룰을 구별하기 위한 번호일 뿐이므로 번호 자체에 별다른 의미는 없다. 즉, ACL 번호가 1번이라고 해서 10번에 비해 우선하거나 덜 우선하지는 않는다는 것이다. 그리고 permit으로 허용할 것인지 아니면 deny로 거부할 것인지 지정하며, 이후에 허용하거나 거부할 소스 ip 주소를 명시하면 된다. 소스 주소를 명시할 경우 ip 대역을 명시할 때는 ip 주소와 함께 wildcard mask를 이용하거나 모든 ip에 대해 룰을 지정할 경우 any를 쓰면 된다. 만약 단일한 ip 주소를 뜻할 때는 host라는 옵션을 주면된다.

이렇게면 위의 그림에서 첫 번째 실행 예를 보면, "access-list 5 permit host 192.168.1.70"이라고 하였는데, 이는 소스 ip 주소가 192.168.1.70인 패킷을 허용하겠다는 룰이다. 단일한 ip이므로 ip 주소 앞에 host를 추가하였다. 만약 ip 대역이라면 "access-list 5 permit 192.168.1.0 0.0.0.255"와 같이 하여야 할 것이다. 이는 소스 ip 대역이 192.168.1.x인 패킷을 허용하겠다는 룰로서 원래 이를 뜻하는 netmask는

255.255.255.0이지만 access-list에서는 이의 반대되는 개념으로 wildcard mask라는 것을 사용하여 0.0.0.255가 된다. 이 wildcard mask 값은 255.255.255.255에서 원래의 netmask를 빼면 쉽게 계산된다.

그 다음 줄은 ACL 번호가 5로 동일하므로 같은 룰이 계속되는 것을 알 수 있으며 소스 ip 주소가 192.168.1.71인 패킷도 허용하는 것을 알 수 있다. 그 다음줄 역시 ACL 번호가 동일하므로 같은 룰이지만 permit이 아닌 deny로서 패킷을 거부하는 것을 알 수 있으며 any라고 하였으므로 모든 패킷을 거부한다는 의미이다. access-list에서는 룰의 순서가 매우 중요하므로 어떤 룰을 먼저 설정하고 어떤 룰을 뒤에 설정하는가에 따라 그 결과는 많이 달라질 수 있기 때문에 룰 설정시 주의하여야 한다.

이렇게 하면 위 5번 룰의 경우 먼저 소스 ip 가 192.168.1.70 이거나 192.168.1.71 인 패킷은 허용하지만 외의 패킷은 모두 거부한다는 의미가 되는 것이다. 만약 access-list 5 deny any가 제일 먼저 나온다면 모든 패킷을 거부하므로 뒤에서 192.168.1.70 이나 192.168.1.71을 허용하여도 역시 거부되는 것이다.

설정이 완료된 후에는 exit를 입력하거나 Ctrl 키를 누른 상태에서 z 키를 입력하면 config 모드에서 빠져 나오게 된다. 설정을 한 후에는 애초에 의도한 대로 룰이 설정되었는지 확인하기 위해 show access-list 5 또는 sh access-list 5 로 확인해 보면 된다. 여기에서 5는 확인하고자 하는 access-list 번호이다. 만약 5를 입력하지 않고 show access-list 만 실행하면 설정되어 있는 모든 access-list를 보여주게 된다.

이렇게 해서 access-list 에 대한 룰 설정이 완료되었다. 다음에는 해당 룰을 어떤 인터페이스에 적용할 것인지 정할 차례이다.

access-list 를 인터페이스에 지정하려면 해당 인터페이스 모드로 들어간 후 "ip access-group 적용할acl번호 in 또는 out" 과 같이 실행하면 된다. 만약 in 이나 out 을 별도로 지정하지 않으면 기본적으로 out 이 된다. 그런데 여기에서 두 가지 고민을 하게 된다. 그것은 바로 어떤 인터페이스에 access-group을 지정할 것인지와 해당 인터페이스에서 in을 하여야 하는지 out을 하여야 하는지 이다. 먼저 라우터의 인터페이스는 크게 serial 인터페이스와 ethernet 인터페이스로 나눌 수 있는데, serial 은 외부 네트워크와 연동하는 부분이고 ethernet 인터페이스는 내부 네트워크와 연동하는 부분이다. 즉, 내부에서 라우터를 게이트웨이로 사용한다면 게이트웨이 ip 주소가 라우터의 ethernet 인터페이스의 ip 주소일 것이다. 이렇게 생각하면 해당 인터페이스에서 in을 하여야 하는지 out을 하여야 하는지도 자연스럽게 이해가 될 수 있다. 정리를 하면 아래와 같다.

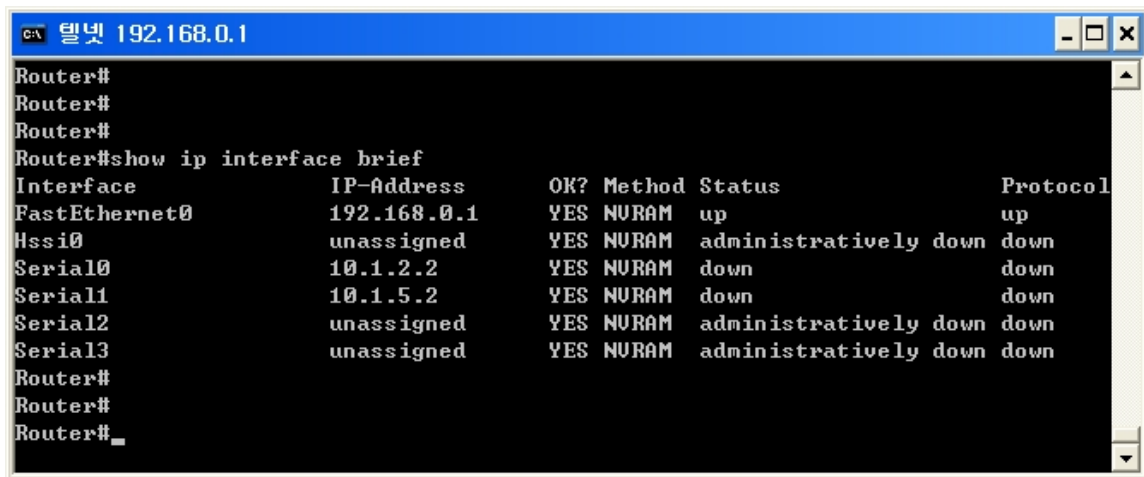
[내부에서 외부로 나가는(outgoing) 트래픽을 제어할 경우]

- ethernet 인터페이스에서는 out 이 되고,
- serial 인터페이스에서는 in 이 된다.

[외부에서 내부로 들어오는(incoming) 트래픽을 제어할 경우]

- serial 인터페이스에서는 out 이 되고,
- ethernet 인터페이스에서는 in 이 된다.

access-list에서 in 과 out 은 매우 중요한 개념이다. 이제 실제 인터페이스에 설정해 보도록 한다. 먼저 자신의 라우터 장비에서 어떤 인터페이스가 있는지 확인하여야 하는데, 이는 아래와 같이 "show ip interface brief" 나 줄여서 "sh ip int b"를 실행해도 된다. 아래 그림의 경우 이더넷 인터페이스는 FastEthernet0가 1개 있고 시리얼 인터페이스로 Hssi0 이라는 인터페이스와 Serial0부터 Serial3 까지 있는데, 이더넷 인터페이스는 FastEthernet0으로, 시리얼 인터페이스는 Serial0 으로 한다고 가정해본다.



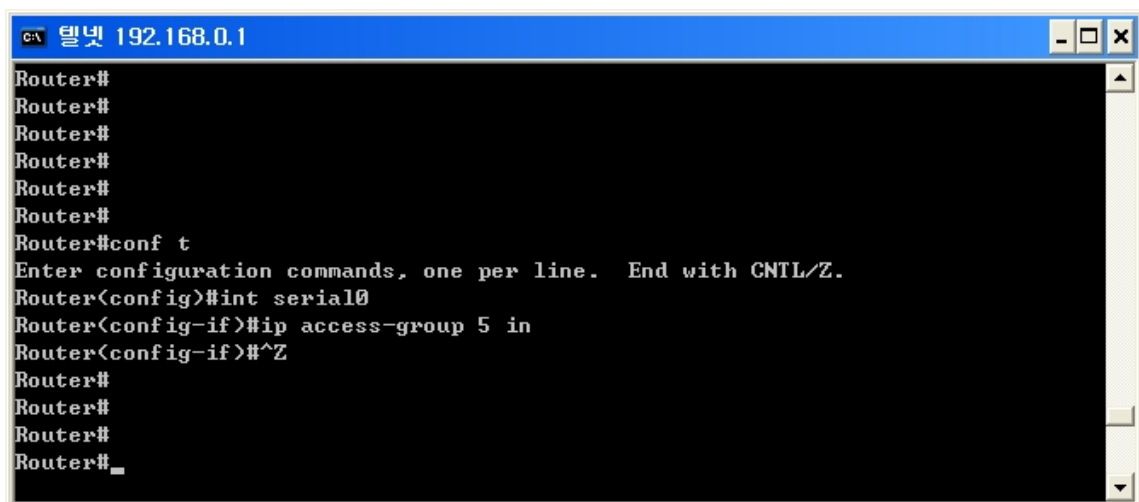
```

Router#
Router#
Router#
Router#show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
FastEthernet0            192.168.0.1     YES NURAM    up            up
Hssi0                     unassigned      YES NURAM    administratively down down
Serial0                   10.1.2.2        YES NURAM    down          down
Serial1                   10.1.5.2        YES NURAM    down          down
Serial2                   unassigned      YES NURAM    administratively down down
Serial3                   unassigned      YES NURAM    administratively down down
Router#
Router#
Router#_

```

[그림 3] 라우터에 설치된 인터페이스 목록

만약 시리얼 인터페이스를 통해 외부에서 내부로 들어오는 트래픽을 필터링하고자 할 경우에는 앞에서 살펴본 바와 같이 시리얼 인터페이스와 이더넷 인터페이스에서 각각 설정 가능하지만 여기에서는 시리얼 인터페이스에서 필터링 설정하려고 한다면 아래와 같이 먼저 serial0 인터페이스 모드로 들어간 후 해당 인터페이스 모드에서 "ip access-group 5 in" 을 실행하면 된다. 이 명령어를 입력한 후 엔터를 치면 실행과 동시에 해당 인터페이스에서 192.168.1.70과 71을 소스로 한 패킷 이외의 패킷은 모두 차단될 것이다.



```

Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int serial0
Router(config-if)#ip access-group 5 in
Router(config-if)#^Z
Router#
Router#
Router#
Router#_

```

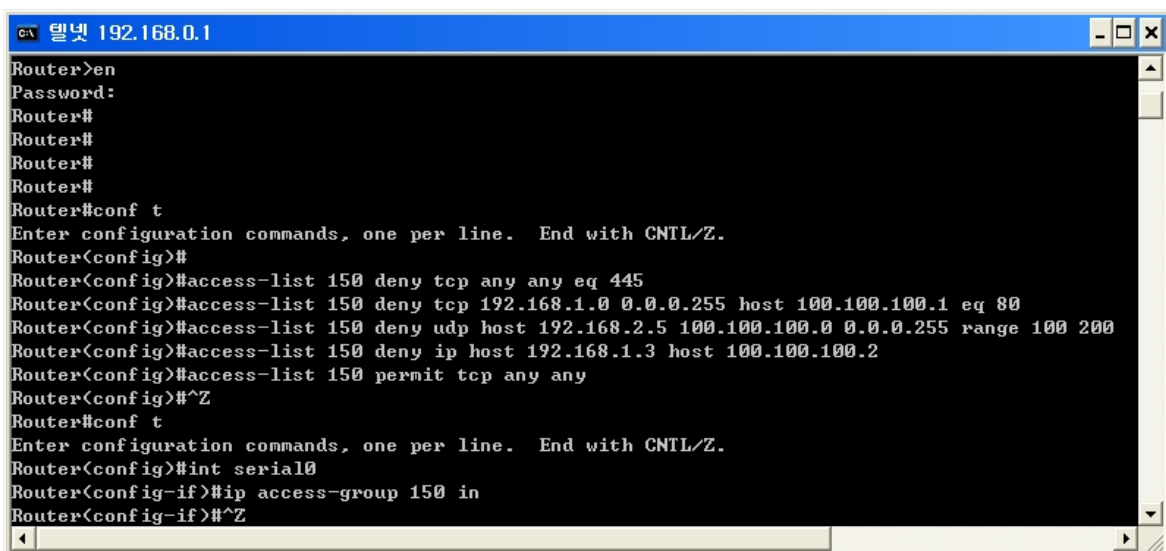
[그림 4] access-group 설정 예

#### 나. extended access-list

다음은 소스 ip 만을 가지고 필터링하는 standard access-list가 아니라 소스ip를 포함하여 목적지 ip, 소스 포트, 목적지 포트, 프로토콜 등으로 필터링 설정할 수 있는 extended access-list를 알아보도록 한다. standard access-list를 이해했다면 extended access-list도 크게 다를 것은 없는데, extended access-list에서 사용할 수 있는 번호는 100부터 199번까지이며 사용 형식은 다음과 같다.

```
access-list acl번호 {permit 또는 deny} 프로토콜 소스 소스-wildcard 목적지 목적지-wildcard
```

여기에서 ACL번호는 standard와 같이 각각의 룰을 구별하기 위한 번호일 뿐이며 번호 자체에 큰 의미가 없다는 점을 주의하기 바란다. 즉 101번과 102번은 단순히 룰을 구별하기 위한 번호일 뿐이며 선후차의 개념과는 관계가 없다는 것이다. 그리고 permit으로 이하의 트래픽을 허용할 것인지 아니면 deny로 이하의 트래픽을 거부할 것인지 지정하며 이후에 프로토콜 및 소스 ip 정보, 목적지 ip 정보를 지정하면 된다. 프로토콜 부분에는 ip 나 tcp, udp, icmp가 올 수 있으며 ip를 지정하면 포트번호를 지정하지 않고 소스 및 목적지 ip만 지정하면 되고, tcp나 udp를 지정하면 해당 포트 번호를 지정하면 된다. 그리고 icmp는 포트번호라는 것이 없이 대신 icmp type과 code가 있으므로 이를 지정하면 된다. 그리고 wildcard mask는 standard access-list에서 언급한 바와 같이 255.255.255.255에서 netmask를 뺀 값으로 지정하면 된다.



```
터넷 192.168.0.1
Router>en
Password:
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router<config>#
Router<config>#access-list 150 deny tcp any any eq 445
Router<config>#access-list 150 deny tcp 192.168.1.0 0.0.0.255 host 100.100.100.1 eq 80
Router<config>#access-list 150 deny udp host 192.168.2.5 100.100.100.0 0.0.0.255 range 100 200
Router<config>#access-list 150 deny ip host 192.168.1.3 host 100.100.100.2
Router<config>#access-list 150 permit tcp any any
Router<config>#^Z
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router<config>#int serial0
Router<config-if>#ip access-group 150 in
Router<config-if>#^Z
```

[그림 5] extended access-list 설정 예

위의 예를 통해 extended access-list를 살펴보도록 하자.

먼저 access-list를 설정한다는 것은 설정을 변경하는 것이므로 enable모드에서

"conf t"를 입력하여 global configuration모드로 변경하도록 한다. 이후 extended access-list 150번을 사용하기 위해 먼저 access-list 150 번을 정의하였다. 물론 기존에 access-list 150번이 설정되어 있다면 no access-list 150을 먼저 실행하여 해당 룰을 삭제 후 새롭게 정의하여야 할 것이다.

먼저 첫 번째의 "access-list 150 deny tcp any any eq 445"를 살펴보도록 하자. 150번을 정의후 deny로 하였으므로 뒤에 언급된 트래픽을 거부한다는 의미가 될 것이다. 프로토콜에서는 tcp 로 하였고 다음에는 소스ip 와 목적지 ip 가 나올 부분인데, 각각 모두의 의미인 any 가 언급되었으므로 소스와 목적지와 관계없다는 의미이며 목적지 포트 부분에 eq 445 로 되었으므로 목적지 포트가 445번인 tcp 패킷은 모두 필터링한다는 의미이다.

두 번째는 역시 150번이므로 같은 룰이 계속되는 것을 알 수 있다. 역시 tcp이며 소스 ip 부분에 192.168.1.0 0.0.0.255 라고 되어 있는데, 0.0.0.255 는 wildcard mask 이므로 이를 netmask로 변경하면 255.255.255.0 이 되므로 소스 ip 는 192.168.1.0/255.255.255.0 이라는 의미가 될 것이다. 즉, 192.168.1.1 192.168.1.255 까지를 뜻하는 것이다.

다음으로 목적지 ip 부분에는 host 100.100.100.1이므로 단일한 ip인 100.100.100.1 이라는 의미가 된다. eq80은 목적지 포트가 80 이라는 의미이므로 이 룰의 의미는 소스 ip가 192.168.1.0/255.255.255.0인 곳에서 목적지 ip가 100.100.100.1로 향하는 80/tcp 패킷을 필터링한다는 의미이다.

세 번째 룰은 udp이면서 소스 ip가 host이므로 단일한 ip인 192.168.2.5이라는 의미이고, 목적지 ip는 100.100.100.0 0.0.0.255이므로 역시 wildcard mask를 netmask로 변경하면 255.255.255.0 이므로 100.100.100.0/255.255.255.0 이 될 것이다. 다음에 목적지 포트 부분에 range라는 부분이 처음 소개되었는데, eq 가 단일한 하나의 포트를 뜻하는 반면에 range는 포트의 범위를 지정할 수 있도록 하는 옵션이다. range를 사용할 때는 "range 시작포트번호 끝포트번호" 와 같이 지정하면 되는데, 따라서 위의 경우 100번부터 200번까지의 포트를 뜻하는 것이다. 세 번째 룰의 의미를 정리하면 소스 ip가 192.168.2.5 이고 목적지 ip가 100.100.100.0/255.255.255.0 이면서 목적지 포트가 100번에서 200번 사이인 udp 패킷을 필터링한다는 의미가 된다.

네 번째 룰은 tcp나 udp가 아니라 ip로 지정되었는데 이는 뒤에 올 정보가 포트가 아니라 ip 라는 것을 알 수 있다. ip 부분에 host 라고 언급되었으므로 단일한 ip 라는 것을 알 수 있으며 따라서 이 룰의 의미는 소스 ip가 192.168.1.3이고, 목적지



ip가 100.100.100.2인 모든 트래픽을 거부한다는 의미이다.

마지막으로 다섯 번째 룰에서는 permit 이므로 패킷을 허용한다는 의미이며 프로토콜은 tcp, 소스 주소와 목적지 주소가 any 이므로 tcp 와 관련된 모든 패킷은 허용한다는 의미가 된다.

앞에서는 언급하지 않았지만 access-list와 관련하여 꼭 알아야 할 사항이 한 가지 있다. 이는 별도로 언급하지 않을 경우에는 해당 룰의 제일 마지막에는 항상 “deny any any”가 추가된다는 것이다. 즉, 별도로 거부하는 룰을 지정하지 않아도 항상 마지막에는 모든 패킷을 거부한다는 의미이므로 위와 같은 경우 앞에서 거부한 몇몇 트래픽을 제외한 모든 tcp는 허용하며 이외의 패킷 즉 udp나 icmp 등은 모두 거부한다는 의미가 된다. 따라서 3번째에 udp를 거부하는 룰은 어차피 default로 tcp를 제외한 모든 패킷은 거부되므로 사실상 의미가 없는 것이다. 특별히 지정한 패킷 이외의 패킷을 허용하려면 "access-list 150 permit ip any any"가 되어야 할 것이다. 여기에서 ip는 tcp나 udp, icmp 등 모든 프로토콜을 포함한 의미이다.

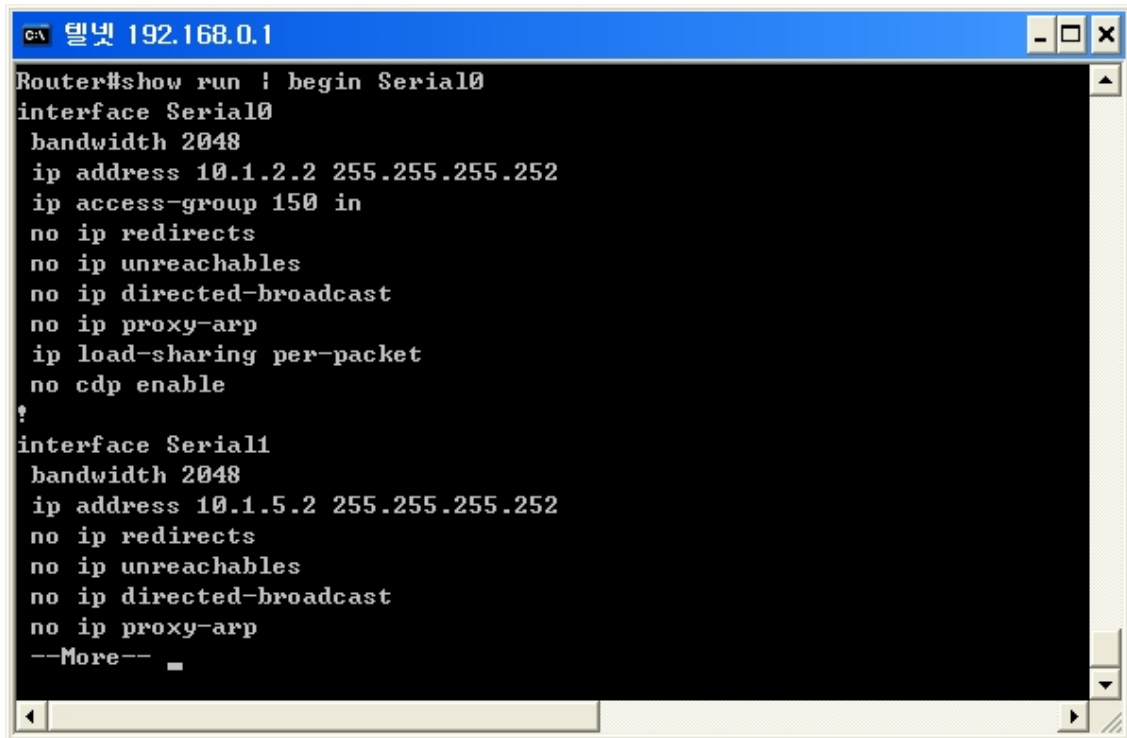
단순히 룰만 지정했다고 해서 바로 적용이 되는 것은 아니다. 룰 지정이 끝난 후에는 해당 룰을 어떤 인터페이스에 대해 in 또는 out으로 할 것인지를 지정하여야 하므로 Ctrl 키를 누른 상태에서 z를 입력하여 config 모드를 빠져 나온 후 serial 0 인터페이스에 지정하기 위해 int serial0을 실행한 후 150번 룰에 대한 access-group을 지정하였다. serial 인터페이스에서 in 으로 하였으므로 외부에서 내부로 들어오는 패킷에 대한 제어임을 알 수 있다. 만약 이더넷 인터페이스에서 지정하였다면 out을 명시하면 같은 의미가 될 것이다.

여기에서 또 하나 주의해야 할 것이 있다. 앞에서는 standard access-list의 예를 들면서 serial 0 인터페이스에 in을 지정한 바 있는데, extended access-list에서도 serial 0 인터페이스에 in을 지정하였다. 한 인터페이스에서는 in 이나 out 이 각각 1번만 사용될 수 있으므로 만약 중복 설정하였을 경우에는 기존의 access-group 이 사라진다는 것이다. 따라서 이러한 경우에는 두개의 룰을 합쳐 하나의 룰로 만들도록 하여야 한다. 아니라면 비슷한 효과를 낼 수 있도록 이더넷 인터페이스에서 out으로 정의하면 될 것이다.

즉, 하나의 인터페이스에는 각각 in 1개, out 1개 이렇게 최대 2개의 룰을 지정할 수 있는 것이다.

아래는 access-group을 설정한 후 현재의 설정 파일의 내용을 살펴보기 위해 show running-config를 실행한 예이다. 명령어 입력시 | begin Serial0 부분을 추가한 이유는 많은 설정 파일 부분에서 Serial0과 관련된 부분을 바로 확인하기 위해 Serial0으로 시작하는 부분부터 출력하라는 의미이다. Serial0과 관련된 룰을 보면 앞에서

언급한 바와 같이 access-group이 150 - 한개만 지정되어 있는 것을 알 수 있다. 이는 in을 중복 지정하면서 기존의 5번 룰이 사라졌기 때문이다.



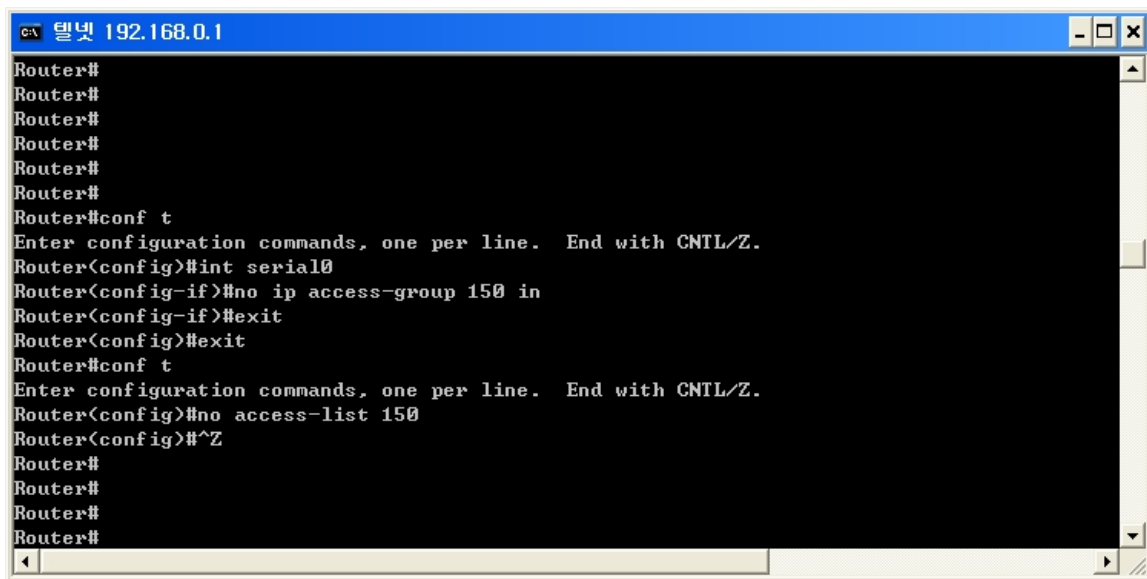
```
Router#show run ! begin Serial0
interface Serial0
  bandwidth 2048
  ip address 10.1.2.2 255.255.255.252
  ip access-group 150 in
  no ip redirects
  no ip unreachable
  no ip directed-broadcast
  no ip proxy-arp
  ip load-sharing per-packet
  no cdp enable
!
interface Serial1
  bandwidth 2048
  ip address 10.1.5.2 255.255.255.252
  no ip redirects
  no ip unreachable
  no ip directed-broadcast
  no ip proxy-arp
--More--
```

[그림 6] 설정파일 조회

#### 다. 룰 설정 변경하기

지금까지는 기존의 룰이 없는 상태에서 룰을 생성하는 방법에 대해 알아보았는데, 다음으로 살펴볼 기존의 access-list를 설정하여 적용한 후 룰을 변경, 삭제하고자 할 때의 방법에 대해 알아보도록 하겠다. 실제로 라우터를 운영하다보면 각종 정책의 변경에 따라 access-list 룰을 수정해야 할 일이 생기곤 하는데, 이 역시 룰을 설정할 때만큼이나 중요하므로 주의하여야 한다. 특히 access-list 룰을 수정하는 것은 처음에 설정하는 것보다 더 복잡하고 어려우므로 주의하여야 한다.

다시 한번 절차에 대해 확인해 보자. access-list를 설정하려면 먼저 global config 모드에서 access-list 룰을 정의한 후 해당 인터페이스 모드로 들어가서 access-group을 이용하여 access-list를 인터페이스에 적용하면 된다. access-list를 삭제 또는 해제하려면 이의 반대 순서로 진행하면 된다. 먼저 해당 인터페이스 모드로 들어가서 삭제 또는 해제의 의미인 no를 이용하여 access-group을 삭제한 후 역시 global config 모드에서 no를 이용하여 access-list를 삭제하면 되는 것이다.



```
Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int serial0
Router(config-if)#no ip access-group 150 in
Router(config-if)#exit
Router(config)#exit
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 150
Router(config)#^Z
Router#
Router#
Router#
Router#
```

[그림 7] access-list 룰을 삭제하는 과정

위의 그림은 기존에 설정했던 access-list를 삭제하는 과정을 보여주고 있는데, 앞에서 언급한 절차대로 하고 있는 것을 알 수 있다.

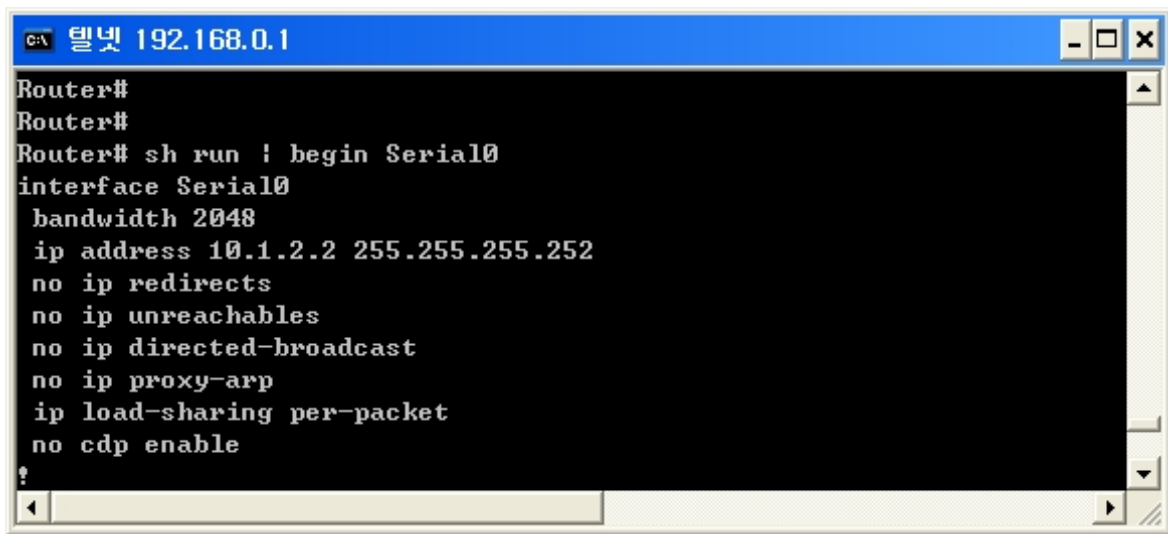
먼저 serial0 인터페이스로 들어가서 설정시 “ip access-group 150 in”을 실행했으므로 no를 붙여서 그대로 실행하여 serial0 인터페이스에 설정되어 있는 access-group을 해제하였다. 이제 access-list 룰 150은 해당 인터페이스에서 해제되었으므로 아무런 의미가 없게 되었고, serial 0 인터페이스에서는 어떠한 필터링 룰도 적용되지 않은 상태가 되었다.

이번에는 Ctrl 키를 누른 상태에서 z를 입력하지 않고 대신 exit를 2번 입력하여 원래의 enable 모드로 들어왔다. 다음으로는 access-list를 삭제할 차례이다. 이를 위해 conf t를 입력후 global config 모드에서 “no access-list 150”을 실행하여 access-list 150과 관련된 룰을 모두 삭제하였다. access-list에서 또 하나 주의할 점이 있는데, access-list의 룰이 여러 줄 있을 경우 특정한 줄만 삭제하거나 변경할 수는 없으며 해당 번호의 모든 룰을 삭제한 후 다시 처음부터 다시 생성하여야 한다는 것이다.

따라서 위와 같이 no access-list 150을 실행하면 150번의 룰 모두가 삭제하며 만약 특정한 하나의 룰만 삭제하려고 no access-list 150 deny tcp any any eq 445와 같이 실행해도 해당 룰만 삭제되는 것이 아니라 150번의 모든 룰이 삭제된다.

이렇게 해서 access-list 설정이 깨끗하게 초기화되었다. 다음 단계로 넘어가기 전에 실제로 원하는 대로 초기화 되었는지 확인해 보도록 하자.

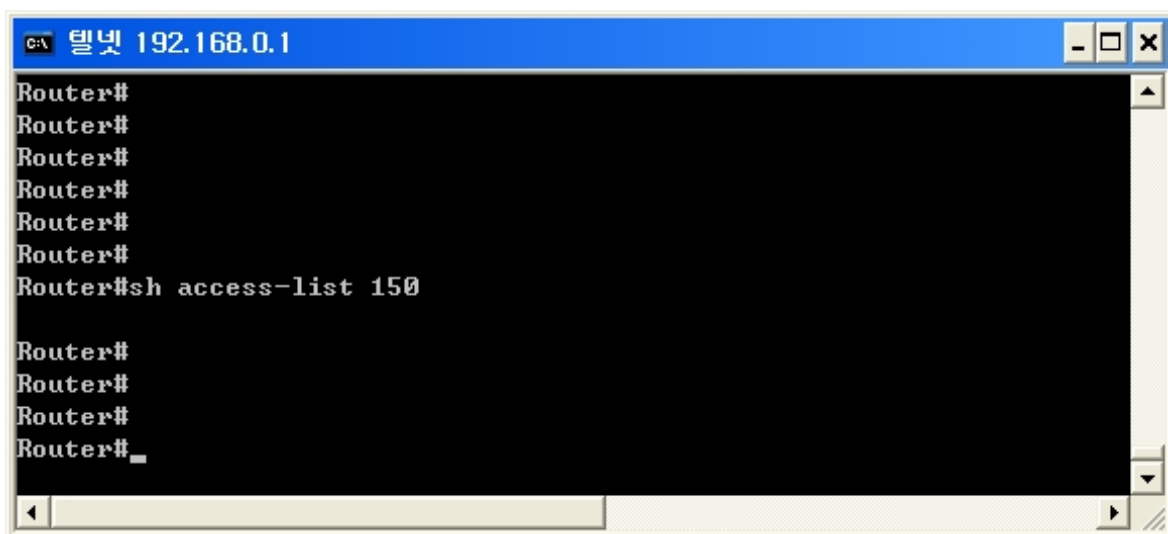
먼저 설정 파일을 살펴보니 아래와 같이 Serial0 인터페이스에 access-group이 없는 것을 알 수 있다.



```
C:\> 텔넷 192.168.0.1
Router#
Router#
Router# sh run | begin Serial0
interface Serial0
  bandwidth 2048
  ip address 10.1.2.2 255.255.255.252
  no ip redirects
  no ip unreachable
  no ip directed-broadcast
  no ip proxy-arp
  ip load-sharing per-packet
  no cdp enable
?
```

[그림 8] 설정파일 조회

그리고 access-list 150번을 조회하자 역시 아무런 룰이 없이 깨끗한 것을 알 수 있다.



```
C:\> 텔넷 192.168.0.1
Router#
Router#
Router#
Router#
Router#
Router#
Router# sh access-list 150

Router#
Router#
Router#
Router#
```

[그림 9] access-list 조회

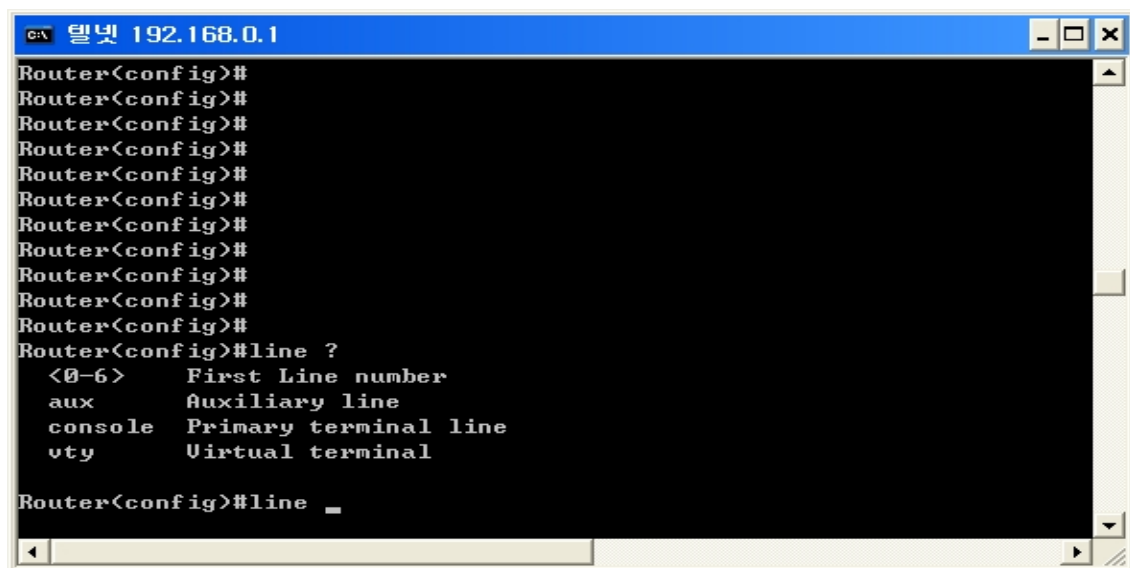
이렇게 모든 설정이 초기화된 것을 확인하였으니 변경할 정보로 새롭게 access-list 를 적용하면 된다. 이는 룰을 설정할 때와 동일한 방법으로 설정하면 된다.

### STEP 3. 라우터 원격 접근 제한을 통한 보안강화 하기

암호를 아무리 어렵게 설정하였다 하더라도 관리자중에 퇴사자나 부서 이동자가 있을 수 있고 또는 관리의 부주의 등으로 암호가 유출될 수도 있다. 또한 이 뿐만 아니라 a부터 zzzzz까지 무작위로 대입하는 brute force 프로그램을 이용하여 일일

이 암호를 입력해 보는 방법으로도 암호를 알 수 있으므로 단순히 암호를 추측하기 어렵게 설정하는 것만으로는 확실한 대안이 될 수 없으며 암호를 설정한 후에는 허용된 ip 외에는 telnet이나 ssh를 통해 라우터에 원격접속을 할 수 없도록 제한하는 것이 좋다. 실제로 라우터의 관리를 위해서는 라우터를 직접적으로 관리하는 특정한 유저만 접근이 가능하면 되므로, 특정 ip에서만 접근 가능하도록 설정하면 될 것이다. 이를 위해서는 앞에서 살펴보았던 access-list를 활용하면 되는데, 먼저 접근을 허용할 ip를 정의한 후 나머지는 거부하도록 access-list를 정의하도록 한다. 단순히 ip 주소에 대한 허용·거부 설정이므로 standard access-list를 이용하는 것이 편할 것이다.

이를 위해 아래와 같이 라우터로의 원격 접근을 허용할 ip로 192.168.0.71과 192.168.2.4에 대해서는 허용한 후 나머지는 모두 거부하도록 설정하였다. 다음에는 access-group을 설정할 차례인데, 라우터에 대한 직접적인 접근을 제어하려면 각각의 인터페이스에 각각의 access-group을 in, out을 지정하여 설정하여야 할 것이다. 만약 인터페이스가 몇 개 없다면 관계없지만 여러 개라면 여간 번거로운 것이 아닐 수 없다. 이를 위해서 라우터의 디바이스(device)에 대한 직접적인 접근은 별도의 설정 방법을 제공하고 있다. 먼저 config 모드로 들어간 후 line 명령어를 입력한다. line은 terminal line의 의미로 원격으로 접속하게 되면 라우터에 별도의 터미널 라인을 이용하게 된다. line 입력 후에는 아래와 같이 aux나 console, vty 등이 올 수 있는데, aux는 모뎀라인, console은 콘솔, vty는 telnet 등 접속시 가상 터미널을 뜻하므로 여기에서는 line vty를 선택하고 이후에 동시접속을 허용할 터미널을 지정하면 된다. 통상적으로 0부터 4까지 지정하면 된다.



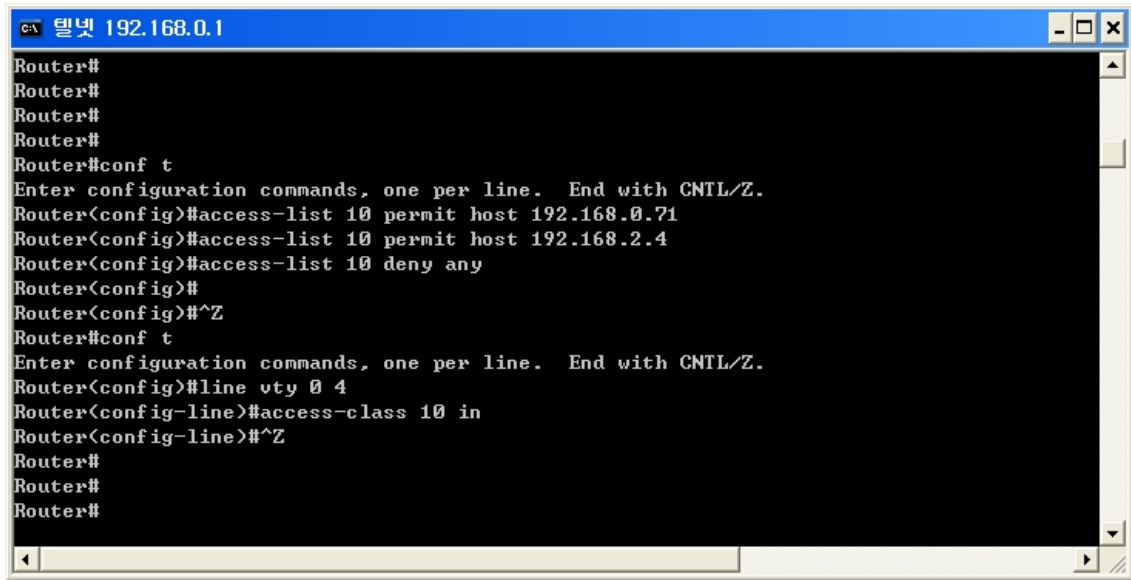
```

C:\ 텔넷 192.168.0.1
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#line ?
<0-6>      First Line number
aux        Auxiliary line
console    Primary terminal line
vty        Virtual terminal
Router(config)#line _

```

[그림 10] line 명령어

access-list를 설정할 가상 터미널을 설정한 후에는 access-group과 동일한 방식으로, 그러나 access-group 대신 access-class라고 지정하도록 한다. 이렇게 해서 설정이 끝났는데 라우터는 설정을 적용함과 동시에 바로 적용되므로 만약 192.168.0.71이나 192.168.2.4에서 접속하지 않았다면 이 룰에 따라 바로 접속이 끊기게 되므로 주의하여야 한다.



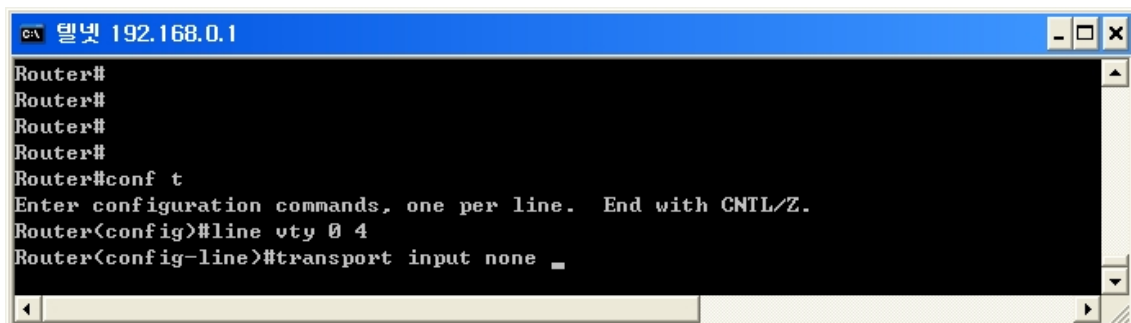
```

C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 permit host 192.168.0.71
Router(config)#access-list 10 permit host 192.168.2.4
Router(config)#access-list 10 deny any
Router(config)#
Router(config)#^Z
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
Router(config-line)#^Z
Router#
Router#
Router#

```

[그림 11] 원격 접근 제어 설정

이렇게 해서 라우터에 원격 접근할 수 있는 ip 대역을 제한 설정하여 특정한 ip 외에는 라우터에 telnet이나 ssh 등을 통해 직접 접근하는 것은 불가능하다. 그러나 이 보다 더 좋은 방법은 만약 원격 접속 자체를 사용하지 않고 콘솔(console)에서만 작업한다면 라우터의 telnet listener 자체를 다운시켜 외부에서의 접속 자체를 차단하는 것도 좋다. 아래는 telnet listener 자체를 disable하는 설정을 보여주고 있다.



```

C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#transport input none

```

[그림 12] 리스너 자체 off 설정

위와 같이 설정한 후에는 추가적으로 아래의 두 명령어도 실행할 수 있는데 여기에

서 "no exec" 란 지정된 해당 모드에서는 어떠한 명령어도 실행하지 않도록 하는 설정이며, "exec-timeout 0 1"은 아무런 키 입력 없이 0분 1초가 지나면 자동으로 접속을 종료한다는 의미이다. 즉, 현실적으로 사용할 수 없도록 한다는 의미가 된다.

```
Router(config-line)# no exec
Router(config-line)# exec-timeout 0 1
```

#### STEP 4. 라우터 SNMP 접근 제한하기

SNMP(Simple Network Management Protocol)는 그 이름이 뜻하는 바와 같이 단순한 네트워크 관리를 위한 목적으로 주로 서버나 네트워크 장비에서 SNMP를 설정한 후 mrtg 프로그램을 이용하여 트래픽 관리 등을 위해 사용되고 있다. 그러나 트래픽 정보뿐만 아니라 전체 네트워크의 구성이나 MAC 주소, IP주소, IOS 버전등 소프트웨어 정보 및 각종 하드웨어 정보까지 제공하는 등 관리자 입장에서는 매우 중요한 정보를 제공하므로 이의 보안에 신경을 쓰도록 하여야 한다. 더군다나 SNMP에 대한 읽기 권한뿐 아니라 쓰기 권한까지 있을 경우에는 config 파일을 열람하거나 직접 네트워크 설정을 변경할 수도 있다.

SNMP는 버전별로 v1과 v2c가 주로 사용되고 있지만 두 버전은 거의 유사하며 최근의 v3에서는 인증을 위해 암호화가 제공되고 있다.

SNMP와 관련해서는 다음의 두 가지를 주의하면 된다.

##### 가. community 문자열(string)

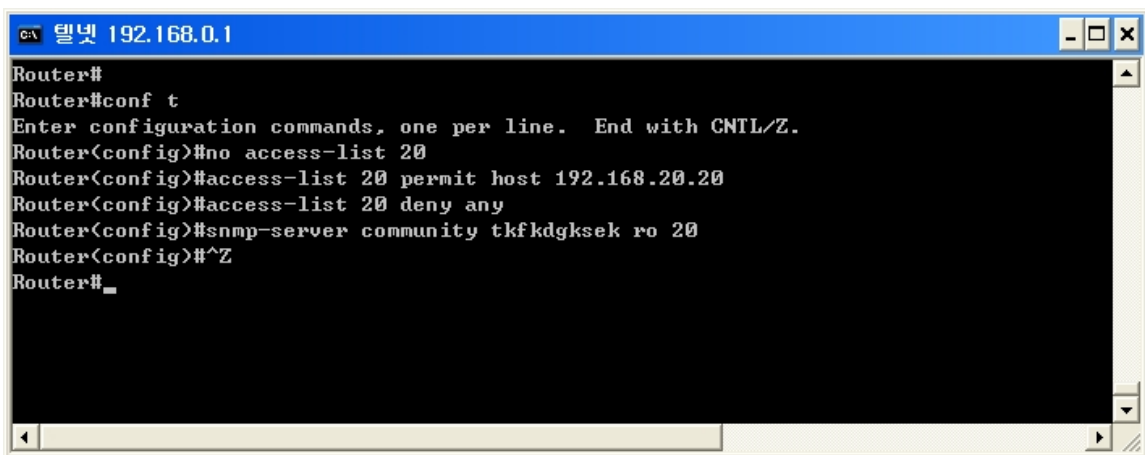
SNMP에서 community 문자열(string)은 SNMPd(데몬)와 클라이언트가 데이터를 교환하기 전에 인증하는 일종의 암호로서 초기값으로 public 또는 private로 설정되어 있다. 이는 비단 라우터뿐만 아니라 대부분의 서버에서도 public으로 되어 있는데, 이를 그대로 사용하는 것은 암호를 사용하지 않는 계정을 사용하는 것 이상 위험하다. 그럼에도 불구하고 대부분의 시스템, 네트워크 관리자들이 기본적인 문자열인 public을 그대로 사용하거나 다른 문자열로 변경을 해도 상호나 monitor, router, mrtg 등 사회공학적으로 추측할 수 있는 문자열을 사용하고 있어 문제가 되고 있다. community 문자열(string)은 뒤에서 설명할 "service password-encryption" 라는 명령어로도 암호화되지 않으므로 반드시 기존의 public 대신 누구나 추측하기 어렵고 의미가 없는 문자열로 변경하도록 하여야 한다. 그리고 SNMP에서는 RO(Read Only)와 RW(Read Write) 모드를 제공하는데, 대부분 RO모드를 사용하지만 일부 관리자들은 SNMP를 이용한 쉬운 관리를 위해 RW(Read Write) community 문자열

을 사용하는 경우도 있는데, 이러한 경우 보안 설정을 확실하게 하지 않을 경우 SNMP를 이용하여 설정을 수정할 수 있는 등 심각한 보안문제를 유발할 수 있으니 가급적 사용을 자제하되 부득이 사용하여야 한다면 각별히 주의하여야 한다.

#### 나. 암호화 여부

SNMP(v1, v2c)에서 클라이언트와 데몬간의 get\_request(요청)와 get\_response(응답) 과정은 암호화가 아닌 평문으로 전송되므로 전기적인 도청인 스니핑(sniffing)이 가능하다. 따라서 아무리 community 문자열을 어렵게 수정하였다 하더라도 중간 네트워크에서 스니핑을 하면 community 문자열을 알 수 있으므로 라우터에서 access-list를 이용하여 SNMP에 대한 접근을 엄격히 제한하여야 한다.

이렇듯 SNMP에서의 두 가지 문제를 해결하기 위해 라우터에서 설정을 해 본다.



```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 20
Router(config)#access-list 20 permit host 192.168.20.20
Router(config)#access-list 20 deny any
Router(config)#snmp-server community tkfkdgksek ro 20
Router(config)#^Z
Router#_
```

[그림 13] SNMP 설정

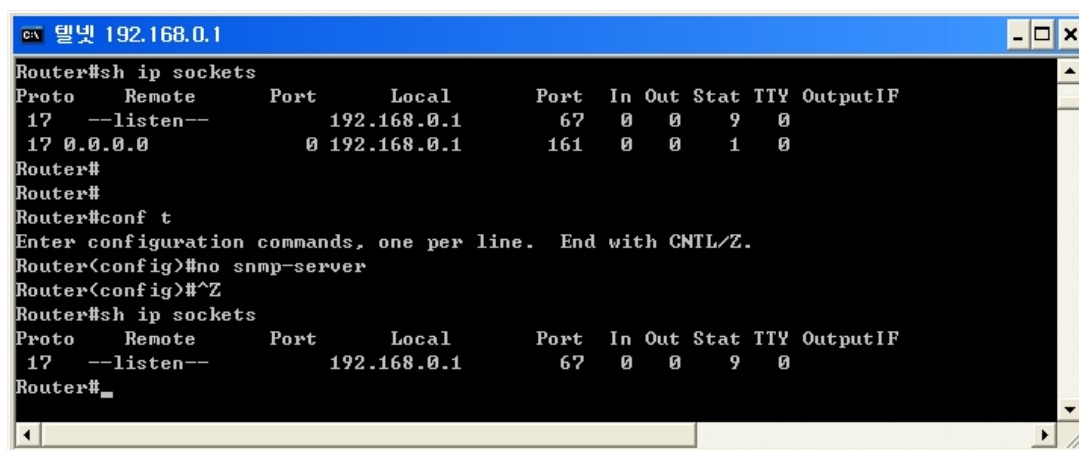
먼저 config 모드로 접속한 후 라우터의 SNMP에 접근할 ip를 제한 설정하기 위해 access-list를 정의하도록 한다. SNMP로의 접근을 허용할 ip는 mrtg와 같은 프로그램이 설치되어 있는 모니터링 서버 정도가 될 것인데, 소스 ip로 접근 제한을 하므로 standard access-list를 이용하면 될 것이다. 따라서 먼저 이 용도로 access-list를 20번으로 하기로 하였다. 혹, 기존에 access-list 20번이 있을지 모르므로 먼저 no access-list 20 으로 해당 룰을 삭제하도록 한다. 그리고 access-list 20번 룰을 설정하면 되는데, 먼저 모니터링 프로그램이 설치되어 있는 해당 ip에 대해 permit을 한 후 나머지는 모두 거부하도록 설정하면 된다. 앞서서도 언급한 바와 같이 access-list에서는 별도로 지정하지 않으면 기본적으로 deny any이므로 “access-list 20 deny any”는 언급하지 않아도 될 것이다.



access-list 설정이 끝난 후에는 SNMP 설정을 할 차례이다.

위와 같이 “SNMP-server community 커뮤니티이름 ro access-list번호” 와 같은 형식으로 하면 된다. 위와 같은 경우 community 문자열이 tkfkdgksek라는 것으로 설정되었고 ro은 Read Only의 의미로 SNMP 에 대해 읽기전용이라는 의미이다. 즉, 읽기전용이기 때문에 SNMP를 통해 설정을 변경하거나 하는 것을 불가능하게 된다. 그리고 ro 뒤의 20은 access-list 번호를 뜻하므로 SNMP 서버에 대해 access-list 20번에서 허용한 192.168.20.20 에서만 접근이 가능하다는 의미가 되는 것이다.

만약 SNMP 자체를 사용하지 않는다면 당연히 SNMP 자체를 off 하는 것이 좋다. 이는 아래와 같이 config 모드로 들어간 후 no SNMP-server를 실행하면 된다.



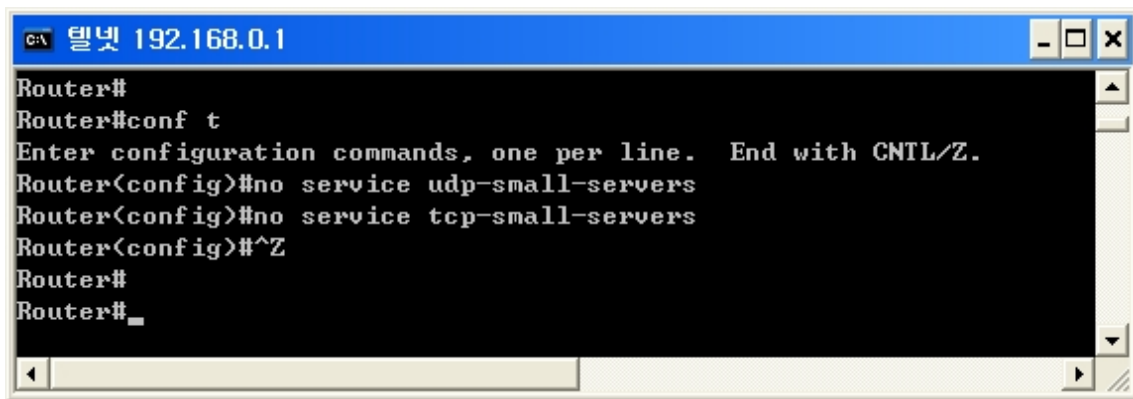
```
Router#sh ip sockets
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 --listen-- 192.168.0.1 67 0 0 9 0
17 0.0.0.0 0 192.168.0.1 161 0 0 1 0
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no snmp-server
Router(config)#^Z
Router#sh ip sockets
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 --listen-- 192.168.0.1 67 0 0 9 0
Router#
```

[그림 14] SNMP 설정 해제

위 그림에서는 먼저 sh ip sockets를 실행하면 라우터에서 리스(listen)하고 있는 udp 서비스를 보여주는데, SNMP가 설정되어 있는 경우에는 위와 같이 port 에 161번이 listen하고 있는 것을 알 수 있다. 그러나 이후에 no SNMP-server를 실행하여 SNMP를 off 한 상태에서는 161번이 없는 것을 알 수 있다.

### STEP 5. 불필요한 서비스 중단하기

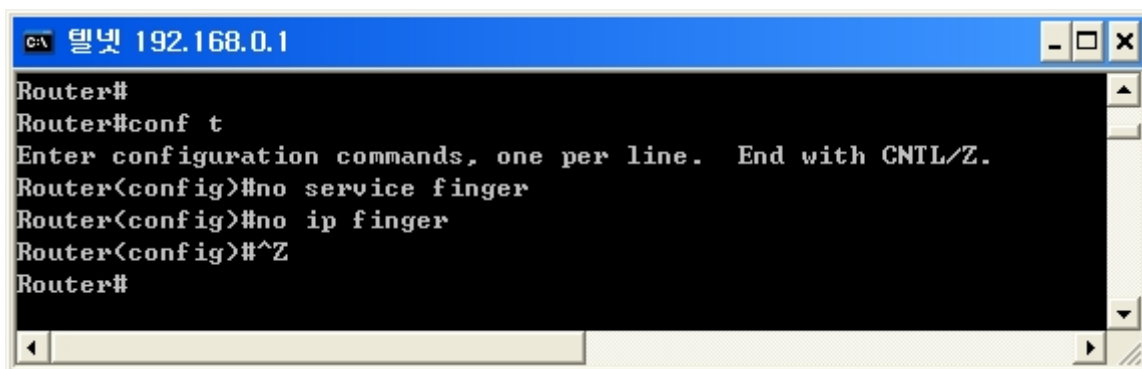
서버 시스템과 마찬가지로 네트워크 장비 역시 처음에 설치를 하거나 IOS 등을 업그레йд 한 후에는 사용하지 않거나 보안상 불필요한 서비스나 기능이 너무 많이 활성화되어 있는 경우가 많다. 따라서 불필요한 서비스는 반드시 끄도록 하는 것이 권장된다. 물론 정상적인 서비스까지 disable하여 서비스에 문제를 유발하지 않도록 주의해야 하겠지만 아래에서 설명하는 내용은 기본적으로 비활성화 하여도 서비스에 무방한 것들이다.



```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no service udp-small-servers
Router(config)#no service tcp-small-servers
Router(config)#^Z
Router#
Router#_
```

[그림 15] small-servers 서비스 중지

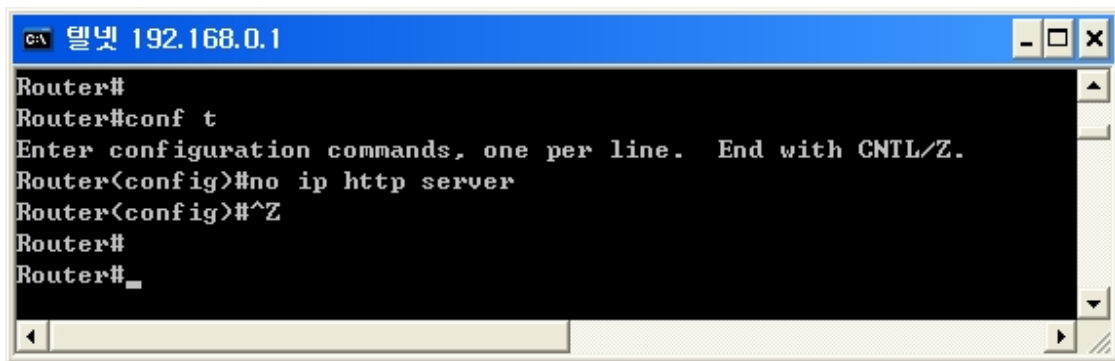
라우터에는 small-servers라는 서비스가 있는데, 이는 예전에 DoS로 악용되기도 한 echo나 discard, daytime 등 일반적으로 20번 이하의 포트를 사용하는 서비스들이다. 이러한 종류의 서비스들은 실제로 거의 사용되지 않으므로 라우터에서 중단하는 것이 좋다. 위 명령어는 각각 udp와 tcp기반의 small-servers 서비스를 중지하는 예를 보여주고 있다.



```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no service finger
Router(config)#no ip finger
Router(config)#^Z
Router#
```

[그림 16] finger 서비스 중단

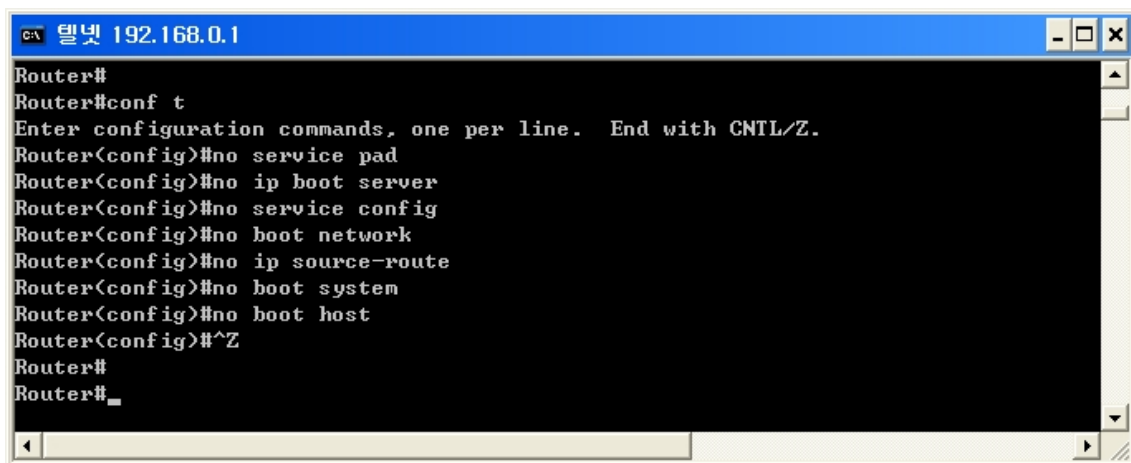
다음으로는 finger 서비스를 중지하는 명령어이다. 위 두 명령어는 각각 구 버전, 신 버전의 IOS에서 작동 방법인데, 만약 finger가 허용되었다면 외부에서 라우터에 로그인 해 있는 유저의 ip 주소 등 개인 정보를 알 수 있게 되므로 반드시 서비스를 중지하도록 한다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip http server
Router(config)#^Z
Router#
Router#
```

[그림 17] http 서비스 중단

다음으로는 http 서비스를 중단하는 예이다. 만약 라우터에 http 서비스가 설정되어 있다면 웹을 통해 라우터의 설정을 조회하거나 변경할 수 있는데, 이는 보안상 문제가 될 뿐만 아니라 라우터의 http server 자체가 취약성을 가지고 있으므로 이 때문에 네트워크 장애를 유발할 수도 있다. 따라서 위와 같이 반드시 http 서버를 중지하도록 하는 것이 좋다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no service pad
Router(config)#no ip bootp server
Router(config)#no service config
Router(config)#no boot network
Router(config)#no ip source-route
Router(config)#no boot system
Router(config)#no boot host
Router(config)#^Z
Router#
Router#
```

[그림 18] 서비스 중단 설정

다음으로는 서비스를 한꺼번에 중지하는 예이다. 먼저 “no service pad” 는 x.25 프로토콜을 사용할 때 필요하므로 일반적인 경우에는 중지하도록 한다. 다음으로 “no ip bootp server” 는 라우터가 bootp 서버로 작동할 때 필요한 서비스인데, 부팅 시 bootp 는 거의 사용되지 않으므로 역시 중지하도록 한다.

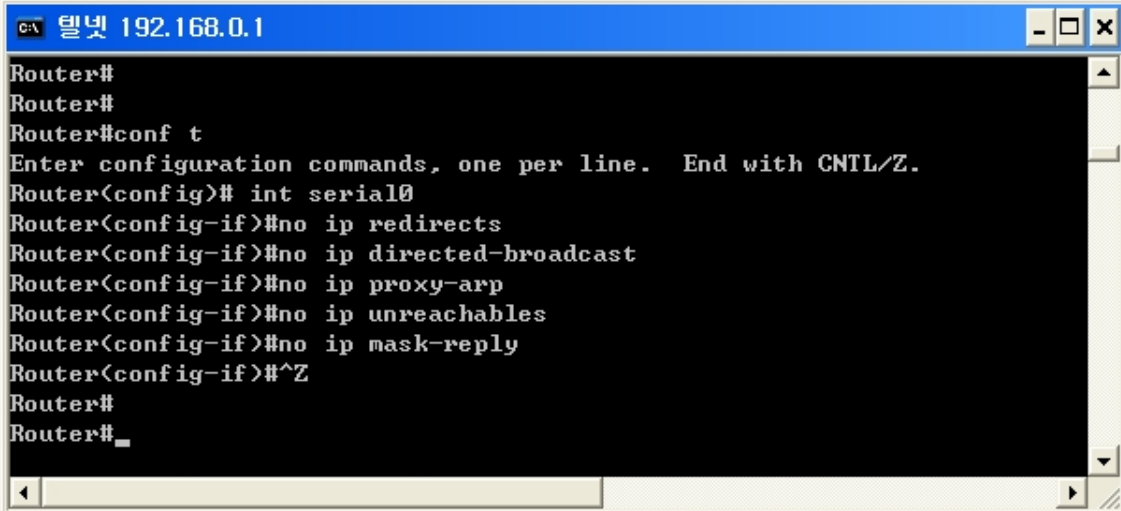
“no service config”, “no boot network”, “no boot system”, “no boot host” 등은 부팅 시 네트워크를 통해 config 파일을 읽어오는 설정인데, 거의 사용되지 않고 불필요한 서비스이므로 역시 중지하도록 한다.

다음으로 “no ip source-route” 는 ip spoofing 을 차단하기 위해 설정하는데, source-route 란 패킷이 전송되는 경로를 각각의 시스템이나 네트워크에 설정되어

있는 라우팅 경로를 통하지 않고 패킷의 발송자가 설정 할 수 있는 기능인데, 악용될 소지가 있으므로 역시 중지하지 않는 것이 좋다.

지금까지는 global configuration 모드에서 설정하였는데, 이를 통해 라우터 전반적인 설정에 영향을 미치게 된다. 이 설정 후에는 라우터에 있는 각각의 인터페이스별로 세부적인 설정을 할 차례인데, 이는 해당 인터페이스 모드로 들어가서 설정하므로 해당 인터페이스에만 영향을 주게 된다. 현재 라우터에 꼽혀 있는 인터페이스는 "show ip interface brief (또는 sh ip int b)"를 입력하면 알 수 있다. 상태(status)가 up으로 되어 활성화되어 있는 인터페이스뿐만 아니라 만약을 위해 지금 당장 사용하지 않더라도 함께 설정하는 것이 좋다.

아래는 serial0 인터페이스에 설정하는 예를 보여주고 있다.



```
터미널 192.168.0.1
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# int serial0
Router(config-if)#no ip redirects
Router(config-if)#no ip directed-broadcast
Router(config-if)#no ip proxy-arp
Router(config-if)#no ip unreachable
Router(config-if)#no ip mask-reply
Router(config-if)#^Z
Router#
Router#_
```

[그림 19] 인터페이스 모드에서 서비스 중단 설정 예

앞에서는 설정을 하기 위해 conf t를 실행하여 config 모드로 들어간 후 바로 명령어를 입력하였지만 특정 인터페이스에 적용을 하기 위해서는 적용을 하고자 하는 해당 인터페이스 모드로 들어가야 한다. 위의 경우 serial0을 선택하였다.

먼저 "no ip redirects" 는 라우터의 인터페이스로 icmp redirect 패킷이 들어오는 것을 차단하기 위한 설정인데, 만약 라우터로부터 icmp redirect 패킷이 나가는 것을 차단하려면 각 인터페이스에서 access-list를 이용하여 icmp redirect를 필터링하여야 한다. icmp redirect 는 최적의 경로를 알려주는 용도로 사용되지만 실제로 대부분의 환경에서는 불필요하며 설정되어 있다면 라우팅 테이블을 변경하는 등의 방법으로 악용될 가능성이 있으므로 서비스를 중지하는 것이 좋다.

다음으로 살펴볼 “no ip directed-broadcast” 는 매우 중요한 설정이다. 만약 라우터에 directed-broadcast 설정이 되어 있다면 외부에서 브로드캐스트 주소로 ping 과 같은 특정한 패킷을 발송할 경우 해당 패킷이 브로드캐스트 주소를 통해 내부의 모든 주소로 그대로 전달되게 된다. 이를테면 만약 내부에서 C Class를 사용하고 있다면 123.123.123.255 주소로 ping을 보냈다면 123.123.123.1부터 123.123.123.254까지 255개의 시스템에 그대로 전달된다는 것이다. 이는 일면 편리하게 사용될 수도 있는 기능이지만 DoS 나 DDoS 공격으로 악용될 가능성이 매우 높기 때문에 반드시 사용하지 않도록 하여야 한다.

최근의 버전에서는 대부분 기본값으로 no 로 설정되어 있다.

다음으로, proxy-arp는 게이트웨이를 가지고 있지 않은 네트워크의 호스트들에게 arp 서비스를 제공하는 역할을 하는데, 실제 거의 사용되지 않고 악용될 소지가 있으므로 역시 중지하도록 한다. no ip unreachable는 공격자에 의한 스캔에 대응하기 위한 것인데, 일부 스캐닝 기법들 중에는 스캔시 되돌아오는 icmp unreachable 메시지를 이용하여 스캔하고자 하는 호스트 또는 특정 포트의 open 여부를 결정하게 된다. 따라서 해당 인터페이스에 no ip unreachable를 실행하여 이를 차단 설정하면 스캔시 소요되는 시간도 길어지게 되어 결국 스캔 공격을 지연시키거나 차단하는 효과가 있다. 특히 Null 인터페이스에는 반드시 이 설정을 하도록 한다.

다음의 no ip mask-reply는 인터페이스를 통해 netmask를 요청하는 icmp 패킷을 발송했을 때 이에 응답하지 않도록 하는 설정이다. 만약 응답할 경우 내부 네트워크의 netmask 정보 등을 유출할 수도 있으므로 굳이 허용할 필요가 없다.

위와 같이 설정한 후에 “sh ip int serial0”과 같이 실행하면 아래와 같이 보이게 된다. 변경 전과 변경 후에 어떻게 바뀌었는지 살펴보기 바란다.

변경전)

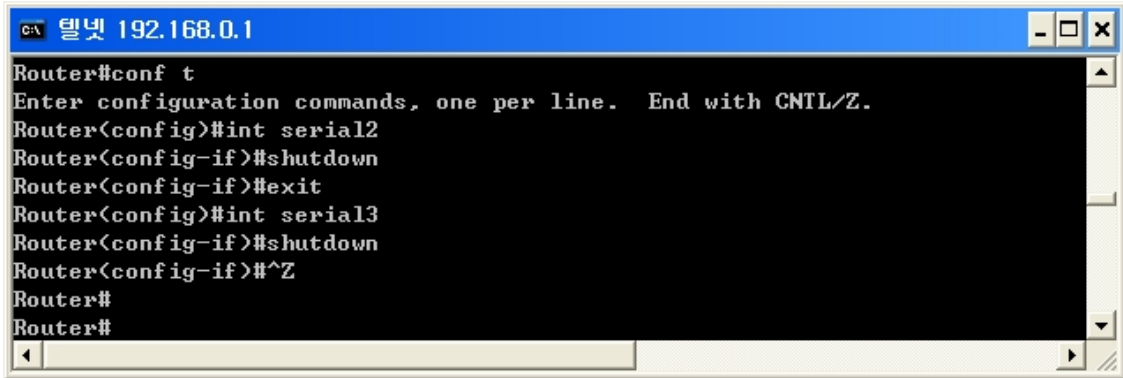
```
Directed broadcast forwarding is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
```

변경후)

```
Directed broadcast forwarding is disabled
ICMP redirects are never sent
ICMP unreachable are never sent
ICMP mask replies are never sent
```

마지막으로 다시 한번 “sh ip int b” 를 실행하여 현재 라우터에 설정되어 있는 인

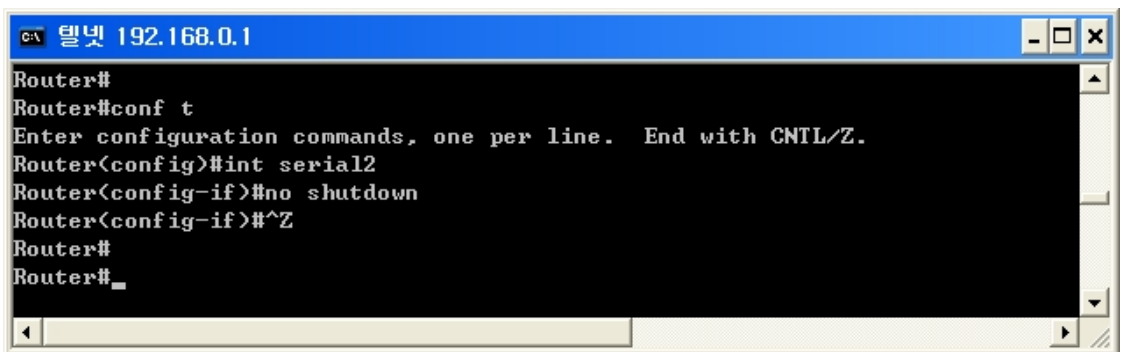
터페이스를 살펴보기 바란다. 사용하지 않는 인터페이스는 다음과 같이 반드시 shutdown 하도록 한다.



```
C:\ 텔넷 192.168.0.1
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int serial2
Router(config-if)#shutdown
Router(config-if)#exit
Router(config)#int serial3
Router(config-if)#shutdown
Router(config-if)#^Z
Router#
Router#
```

[그림 20] 사용하지 않는 인터페이스 다운

만약 다운된 인터페이스를 재가동하려면 해당 인터페이스 모드에서 no를 붙여서 no shutdown을 실행하면 된다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int serial2
Router(config-if)#no shutdown
Router(config-if)#^Z
Router#
Router#
```

[그림 21] 다운된 인터페이스 재가동

불필요한 서비스나 인터페이스에 대한 중지를 한 후에는 꼭 필요한 서비스만 오픈되어 있는지 확인하기 위해 실제 포트 스캔을 해 보는 것도 좋은 방법이다. nmap 등과 같은 포트 스캔 프로그램을 이용하여 스캔해 보면 된다.

```
# nmap -sT -p 1-65535 192.168.0.1 // tcp 포트 스캔
# nmap -sU -p 1-65535 192.168.0.1 //udp 포트 스캔
```

## STEP 6. 암호화 설정하기

라우터 설정을 변경한 후에는 애초에 의도한 대로 설정되었는지 확인하기 위해 설정 파일을 살펴보는 습관을 들이는 것이 좋다. 라우터의 설정 파일은 크게 두 가지

로 나눌 수 있는데, ROM에 설정되어 있어 라우터 부팅시에 적용이 되는 startup-config와 RAM에 설정되어 있어 설정할 때마다 바로 적용이 되어 부팅이 되면 사라지는 running-config가 그것이다. 물론 설정을 변경하면 별도로 물을 저장하는 명령어를 실행하지 않는 한 이 명령어는 running-config에만 적용이 되므로 sh running-config 또는 간단히 sh run을 실행하여 RAM에 저장되어 있는 설정 파일을 살펴보아야 한다.

그런데 설정 파일을 살펴보면 앞에서 설정한 내용 중 암호가 그대로 보이는 경우가 있다. 만약 config 파일이 유출되었을 경우에는 암호를 그대로 보여주게 되므로 보안상 문제가 될 수 있으므로 설정 파일에서 암호를 암호화하는 것이 좋다. 아래는 현재의 설정 파일을 보기 위해 sh run을 실행한 결과인데, 제일 아래에 enable password 부분이 12345로 그대로 보이는 것을 확인할 수 있다.

```

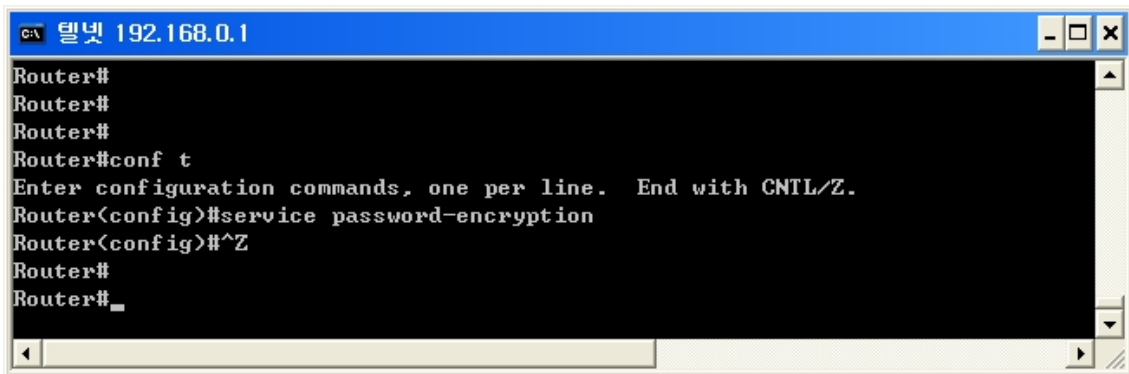
Router#
Router#
Router#
Router#
Router#
Router#sh run
Building configuration...

Current configuration:
!
version 12.0
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router
!
logging buffered 16000 debugging
enable password 12345
!

```

[그림 22] 암호화가 설정되지 않은 config

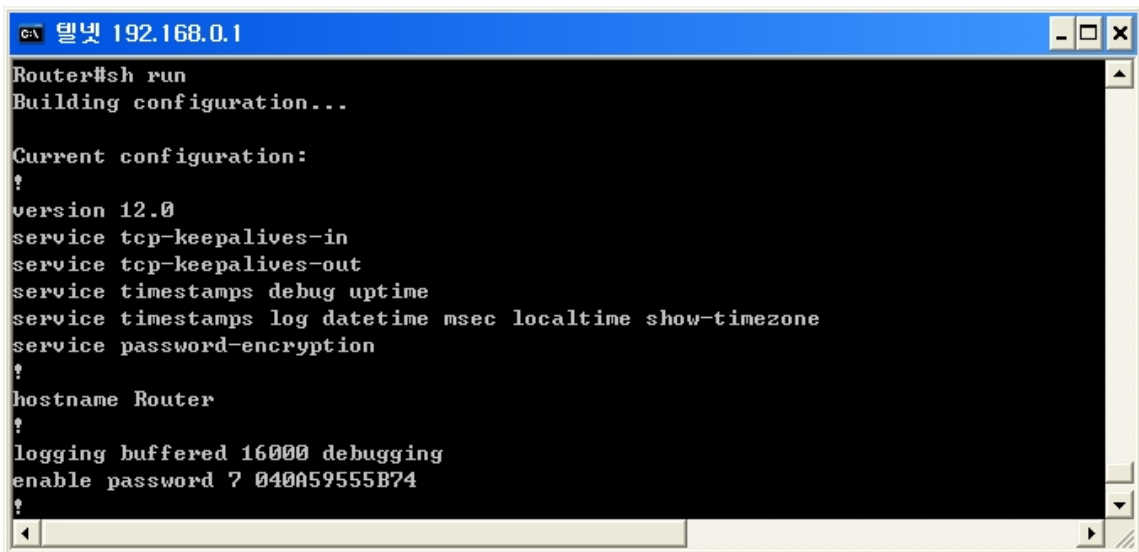
따라서 평문으로 저장되어 있는 암호를 암호화 하고자 할 때 사용할 수 있는 명령어로는 “service password-encryption”이 있는데, 이 명령어를 실행하면 일부 암호를 암호화하게 된다. 아래는 이 명령어를 실행한 예이다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#service password-encryption
Router(config)#^Z
Router#
Router#
```

[그림 23] 암호화 명령어 실행

위와 같이 암호화 명령어를 실행한 후 다시 sh run을 실행하여 현재의 설정을 살펴보니 아래와 같이 12345 대신 암호화된 정보로 보이는 것을 확인할 수 있다. 그러나 암호화가 되기는 하였지만 강력한 암호화 기법은 아니어서 복호화 할 수 있으므로 주의하기 바란다.



```
C:\ 텔넷 192.168.0.1
Router#sh run
Building configuration...

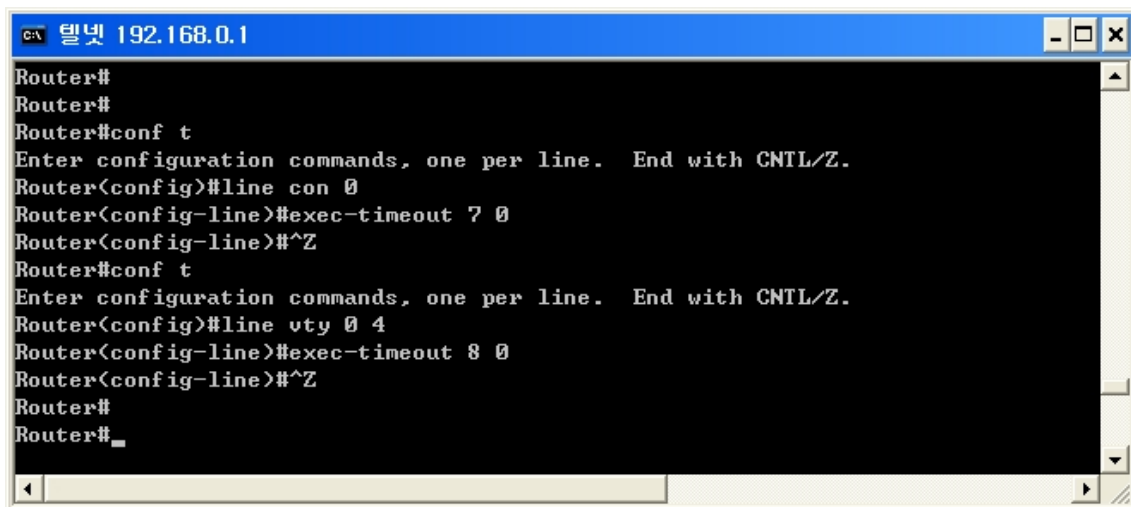
Current configuration:
?
version 12.0
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
service password-encryption
?
hostname Router
?
logging buffered 16000 debugging
enable password ? 040A5955B74
?
```

[그림 24] 암호화가 적용된 예

#### STEP 7. exec-timeout 설정을 통한 로그인시간 제어하기

라우터에 로그인 한 후 일정 시간동안 아무런 명령어를 입력하지 않으면 자동으로 접속을 종료하거나 로그아웃이 되도록 설정하는 것이 좋다. 이는 실수로 로그 아웃을 하지 않고 자리를 뜨는 경우에 대비하기 위한 설정인데, 이 설정을 위해서는 각 각의 디바이스 모드에서 “exec-timeout 분 초” 설정을 하면 된다.





```
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line con 0
Router(config-line)#exec-timeout 7 0
Router(config-line)#^Z
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 8 0
Router(config-line)#^Z
Router#
Router#_
```

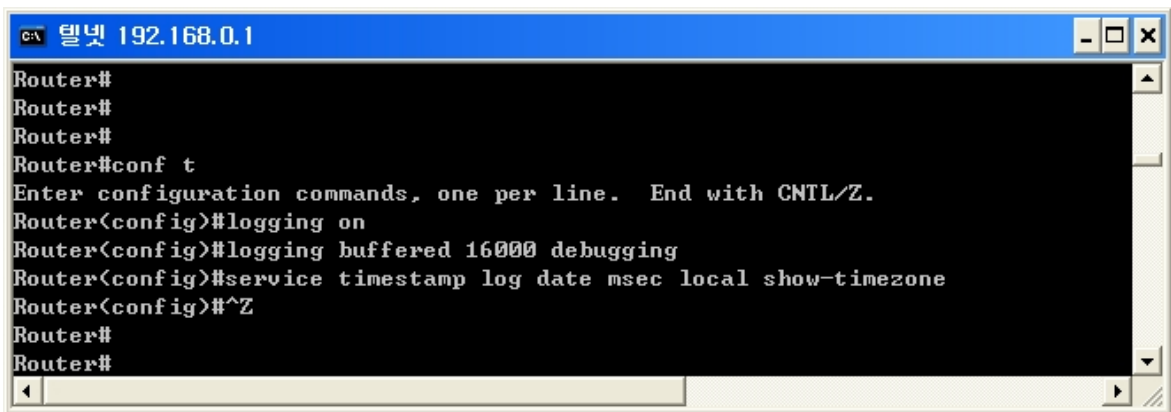
[그림 25] exec-timeout 설정

위는 먼저 console 모드에서 접근하였을 때 7분 0 초 동안 아무런 키 입력이 없으면 자동으로 로그 아웃 하도록 한 설정이며, 두 번째는 virtual terminal을 통해 즉 telnet 이나 ssh를 통해 접근하였을 때 8분 0초 동안 아무런 키 입력이 없으면 자동으로 로그아웃 되도록 한 설정이다.

## STEP 8. 로깅(logging)을 통한 로그관리 설정하기

서버든 라우터와 같은 네트워크 장비든 관계없이 로그는 매우 중요한 의미를 가진다. 시스템에서 자체적으로 제공하는 로그를 통해 다양한 현상이나 장애등을 인지할 수 있으며 access-list와 같은 특정한 룰에 매칭되었을 경우 로그를 남길 수 있도록 함으로써 모니터링의 용도로도 중요한 역할을 하게 된다. 그러나 대부분 라우터에서 로그를 남기는 설정을 하지 않고 사용하는데, 관리상의 목적으로 또는 보안상의 목적으로도 반드시 설정할 것을 권장한다. 라우터에서 제공되는 로깅 기법은 여러 가지가 있는데, 이 중에서 buffered logging과 syslog logging 방법이 가장 많이 사용되고 있으므로 이 방법에 대해 각각 알아본다.

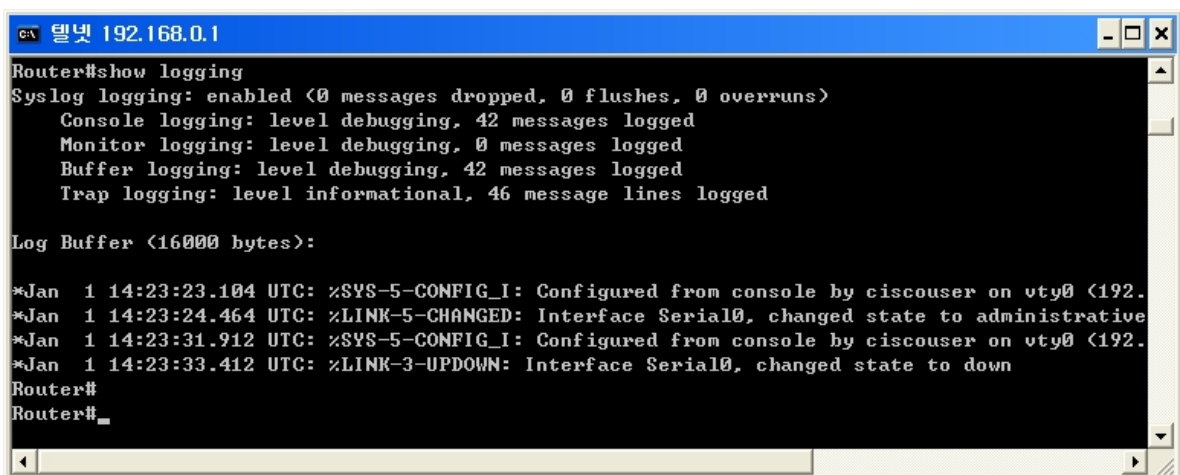
먼저 buffered 로깅은 라우터의 buffer(RAM)에 로그를 남기도록 하는 방법으로 가장 많이 사용되는 방법이다. 이를 위해서는 먼저 logging on을 실행하여 로깅을 남기도록 설정한 후 얼마만큼의 버퍼를 할당할 것인지 그리고 로깅 수준은 어느 정도로 할 것인지 설정하도록 한다. 아래 그림에서는 16K 정도를 할당하였고 로깅 수준은 debugging으로 설정하여 상세한 로그가 남도록 하였다. 다음으로는 로그에 남길 때 timestamp를 지정하여 관리자가 지정한 형식으로 시간 정보를 남기도록 설정하였다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging on
Router(config)#logging buffered 16000 debugging
Router(config)#service timestamp log date msec local show-timezone
Router(config)#^Z
Router#
Router#
```

[그림 26] buffered 로깅 설정

이후 show logging을 실행해 보면 아래와 같이 생성되는 로그 정보를 확인할 수 있다.



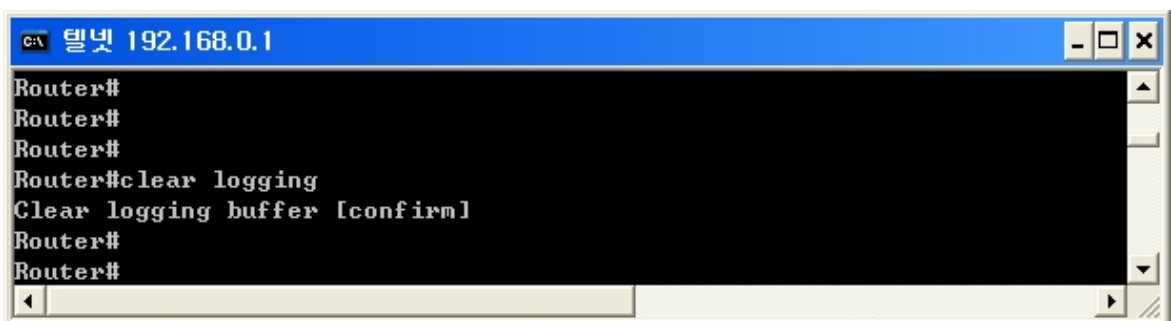
```
C:\ 텔넷 192.168.0.1
Router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 42 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 42 messages logged
  Trap logging: level informational, 46 message lines logged

Log Buffer (16000 bytes):

*Jan  1 14:23:23.104 UTC: %SYS-5-CONFIG_I: Configured from console by ciscouser on vty0 (192.
*Jan  1 14:23:24.464 UTC: %LINK-5-CHANGED: Interface Serial0, changed state to administrative
*Jan  1 14:23:31.912 UTC: %SYS-5-CONFIG_I: Configured from console by ciscouser on vty0 (192.
*Jan  1 14:23:33.412 UTC: %LINK-3-UPDOWN: Interface Serial0, changed state to down
Router#
Router#
```

[그림 27] show logging 실행 화면

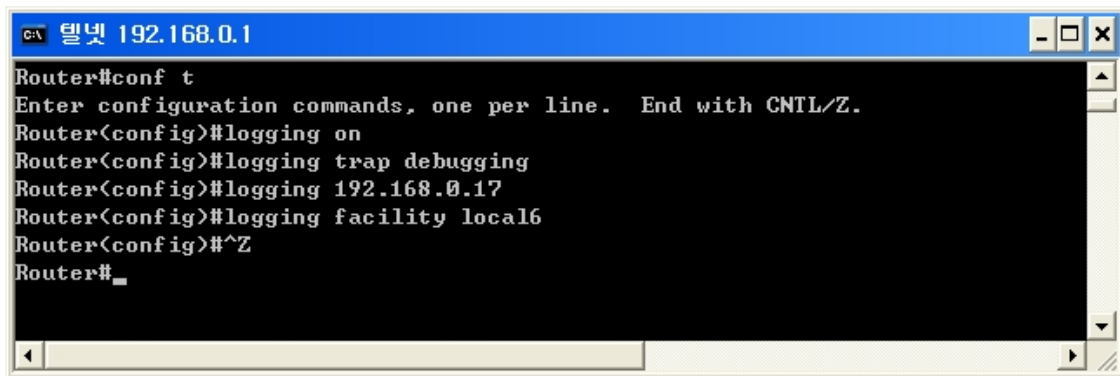
이후 logging 정보를 삭제하려면 아래와 같이 clear 하면 된다.



```
C:\ 텔넷 192.168.0.1
Router#
Router#
Router#
Router#clear logging
Clear logging buffer [confirm]
Router#
Router#
```

[그림 28] clear logging 화면

buffered logging도 좋지만 매번 라우터에 로그인해서 확인해 보아야 한다는 번거로움이 있고 로그에 남길 수 있는 용량에 한계가 있어 이의 대안으로 syslog 로깅을 실행할 수 있다. syslog 로깅이란 로그를 라우터에 남기지 않고 514/udp를 통해 원격지의 호스트에 전달하는 것으로 원격지의 호스트는 통상적으로 리눅스 등 유닉스 호스트가 사용된다.



```
C:\ 텔넷 192.168.0.1
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging on
Router(config)#logging trap debugging
Router(config)#logging 192.168.0.17
Router(config)#logging facility local6
Router(config)#^Z
Router#
```

[그림 29] syslog logging 설정

위는 syslog 로깅을 남기는 설정인데, 먼저 앞에서와 같이 logging 기능을 켜고 로그의 수준을 debugging 으로 설정하였다. 그리고 제일 중요한 설정으로 로그를 남길 원격지 호스트의 ip를 지정하도록 한다. 위의 경우 로그를 남길 주소로 192.168.0.17 로 설정하였다.

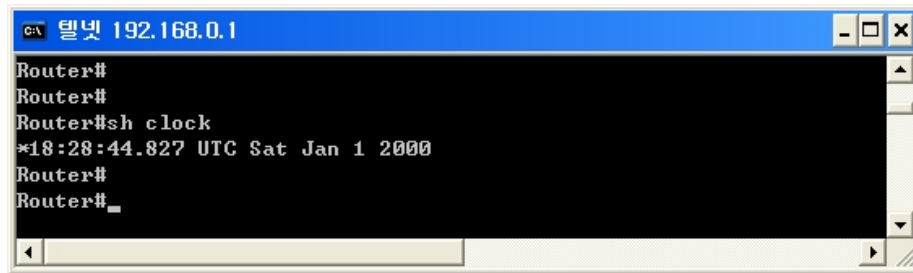
마지막으로 라우터에서 로그를 보내는 syslog facility 를 local6 으로 설정하였으므로 리눅스 서버에서 syslog 설정 파일인 /etc/syslog.conf 에서도 다음과 같이 설정한 후 syslogd 프로세스를 재가동하면 라우터의 로그가 해당 호스트의 /var/log/router 파일에 저장되게 된다.

```
local6.* /var/log/router
```

이후 /etc/logrotate.conf 파일에 아래와 같이 설정해 두면 /var/log/router 의 내용이 매일 자동으로 순환(rotation)되면서 7일이 지난 로그는 자동으로 삭제될 것이다.

```
/var/log/router {
    daily
    rotate 7
}
```

로그를 남길 때는 로그에 남은 시간이 중요한 단서가 된다. 따라서 라우터의 시간을 정확하게 맞추는 것이 매우 중요하게 된다. 먼저 현재 라우터에 설정되어 있는 시간을 보려면 "show clock"을 실행하면 된다.

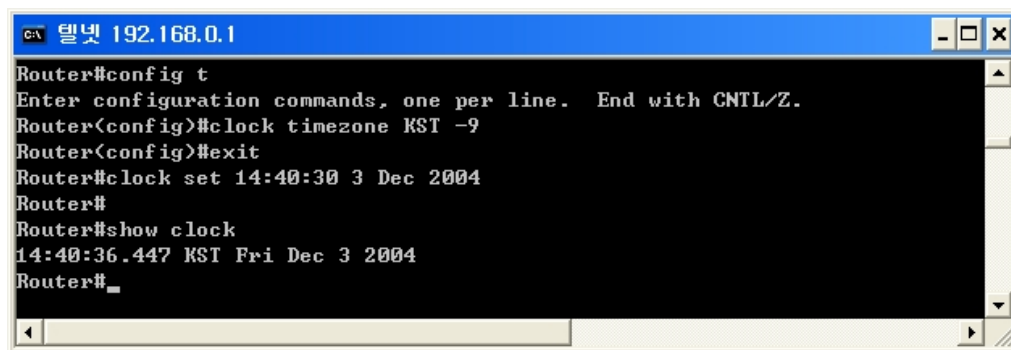


```

C:\ 텔넷 192.168.0.1
Router#
Router#
Router#sh clock
*18:28:44.827 UTC Sat Jan 1 2000
Router#
Router#
  
```

[그림 30] 현재 시간 조회

위의 경우 시간이 잘못 되어 있으므로 현재의 시간으로 수동 설정해 보도록 하자. 먼저 timezone을 맞추도록 하자. 한국의 경우 KST 설정하면 되고, 이후에 수작업으로 현재의 시간을 입력해 보도록 하자. 현재의 시간 형식은 "clock set hh:mm:ss 날 짜 월 년도" 인데, 아래의 경우 2004년 12월 3일 오후 2시 40분으로 지정한 예이다.

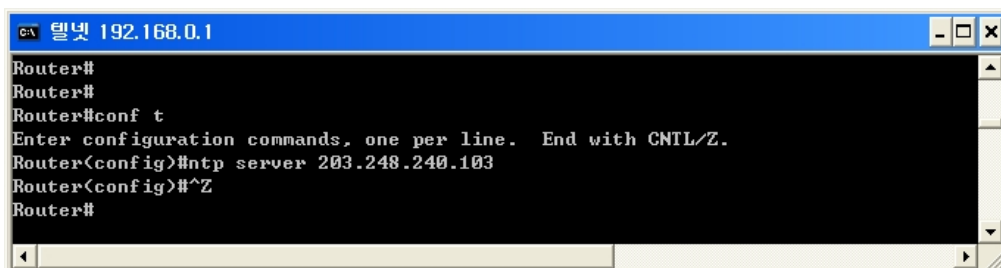


```

C:\ 텔넷 192.168.0.1
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#clock timezone KST -9
Router(config)#exit
Router#clock set 14:40:30 3 Dec 2004
Router#
Router#show clock
14:40:36.447 KST Fri Dec 3 2004
Router#
  
```

[그림 31] 시간 및 timezone 설정

시간 설정을 한 후에 일정 시간이 지나면 다시 시간이 정확하지 않게 작동하는 경우가 있으므로 정기적으로 시간을 재설정해 주는 것이 좋은데, 이를 위해서는 time 서버에 접속하여 시간을 동기화 하도록 설정하는 것이 좋다. 아래의 경우 203.248.240.103(time.bora.net) 에 접속하여 시간을 동기화하게 된다.



```

C:\ 텔넷 192.168.0.1
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 203.248.240.103
Router(config)#^Z
Router#
  
```

[그림 32] 타임서버와 시간 동기화

## STEP 9. 설정 파일 백업하기

마지막으로 살펴볼 부분은 아무리 강조해도 지나치지 않은 백업(backup) 이다. 꼭 해킹에 대비하기 위해서라기보다는 어떤 문제가 발생할지 모르기 때문에 백업은 필수라고 할 수 있다. 이를테면 설정을 변경한 후에 변경한 설정이 문제가 있어 원래의 설정으로 되돌리려고 할 때도 있을 수 있는데 설정이 변경될 때마다 백업을 받아 두면 작업에 대한 히스토리가 될 수도 있을 것이다.

설정 파일을 백업하려면 고전적인 방법인 tftp 나 좀 더 진보된 방식인 ftp를 이용할 수 있고 설정 파일을 직접 copy & paste 로 백업해 두어도 된다. 라우터의 설정 파일이 길어야 A4 분량으로 몇장 되지 않기 때문이다. 어떤 방법을 이용하든 중요한 것은 설정 파일 백업은 반드시 하여야 하는 필수 조건이라는 것이다.

## 2. 라우터를 활용한 네트워크 보안

앞에서는 라우터 자체의 보안을 강화할 수 있는 방안에 대해 알아보았다면 지금부터는 라우터를 통해 네트워크의 보안을 강화할 수 있는 방안에 대해 알아보도록 하자. 특히나 모든 트래픽이 라우터를 통하여 들어오고 나가기 때문에 라우터에서의 트래픽 제어는 매우 효율적이고 그만큼 중요하다 할 수 있겠다. 물론 라우터의 본래 기능은 패킷을 라우팅 테이블에 따라 포워딩하는 것이지만 자체적으로 제공하는 각종 보안기능과 모니터링 기능을 활용하면 보안 제품 이상의 솔루션이 될 수 있을 것이다. 특히나 사내에서 라우터를 이용한다면 사내 트래픽을 모니터링하거나 사내 방화벽의 용도로도 적합할 것이다.

### STEP 1. ingress filtering 설정하기

ingress 필터링은 앞에서 살펴보았던 standard 또는 extended access-list를 활용하여 라우터 내부로 즉 사내 네트워크로 유입되는 패킷의 소스 ip 나 목적지 포트등을 체크하여 허용하거나 거부하도록 필터링하는 것을 뜻한다.

먼저 공통적으로 필터링하여야 할 소스ip 는 인터넷상에서 사용되지 않는 ip 대역이다. 대부분의 공격이 실제 존재하지 않는 위조된 ip 주소를 소스로 하여 진행되므로 이 ip 대역만 차단해도 일정정도의 비정상 패킷을 사전에 차단하는 효과가 있다.

현재 ip 할당 및 미 할당 내역은 아래의 url에서 참고할 수 있다.

<http://www.iana.org/assignments/ipv4-address-space>

위 정보를 참고로 외부에서 유입되는 것을 차단하여야 할 네트워크 주소 목록은 아래와 같다.

0.0.0.0/32  
127.0.0.0/8  
10.0.0.0/8  
172.16.0.0/12  
192.168.0.0/16  
224.0.0.0/4  
240.0.0.0/5  
255.255.255.255/32

여기에서 /32 나 /8 과 같은 형식은 CIDR 라고 하는데, /8 은 A class(255.0.0.0)

/16 은 B class(255.255.0.0), /24 는 C class(255.255.255.0), /32 는 단일한 호스트 255.255.255.255 라고 생각하면 된다. 위 정보를 참고로 access-list를 작성해 보도록 하자. 물론 단순히 특정 소스 ip 및 ip 대역을 차단하는 것이므로 standard access-list를 활용해도 되지만 이후에 1434/udp 등 악성 포트도 차단하는 룰을 함께 사용할 것이므로 extended access-list 로 작성해 보도록 하자.

```

터미널 192.168.0.1
Router#
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 102
Router(config)#access-list 102 deny ip host 0.0.0.0 any
Router(config)#access-list 102 deny ip 127.0.0.0 0.255.255.255 any
Router(config)#access-list 102 deny ip 10.0.0.0 0.255.255.255 any
Router(config)#access-list 102 deny ip 172.16.0.0 0.15.255.255 any
Router(config)#access-list 102 deny ip 192.0.2.0 0.0.0.255 any
Router(config)#access-list 102 deny ip 169.254.0.0 0.0.255.255 any
Router(config)#access-list 102 deny ip 192.168.0.0 0.0.255.255 any
Router(config)#access-list 102 deny ip 240.0.0.0 15.255.255.255 any
Router(config)#access-list 102 permit ip any any
Router(config)#^Z
Router#

```

[그림 33] 비정상 ip 대역 필터링

위 룰에서 단일한 ip 는 host 로, ip 대역은 255.255.255.255에서 netmask를 뺀 wildcard mask 로 하였고 목적지 ip 대역은 라우터 내부로 향하는 모든 트래픽에 적용되므로 모두 any 가 된다.

다음으로는 잘 사용하지 않거나 보안에 취약한 악성 포트를 필터링할 차례이다. 이를테면 지난 1.25 대란의 주범이었던 MS-SQL 웹에서 사용했던 1434/udp 가 대표적인 예가 될 것이다. 이외 udp/tcp 135~138 까지는 정상적인 서비스로는 거의 사용되지 않으면서도 웹 바이러스등이 스캔을 할 때 많이 사용하는 포트이므로 가능한대로 필터링하는 것이 좋다. 만약 외부에서 네트워크 드라이브를 이용한 공유를 허용하지 않도록 한다면 139/tcp 와 445/tcp 도 함께 필터링하는 것이 좋다. 이외의 다른 포트 목록은 각자 설정하기 바람

아래는 비정상 포트를 목적지로 한 패킷을 필터링 한 예를 보여주고 있는데 각자의 환경에 따라 다를 수 있으므로 단지 참고로만 하기 바란다.

```

c:\ 멀넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 103 deny tcp any any range 1 chargen
Router(config)#access-list 103 deny udp any any eq tftp
Router(config)#access-list 103 deny tcp any any eq finger
Router(config)#access-list 103 deny udp any any eq sunrpc
Router(config)#access-list 103 deny udp any any range 135 138
Router(config)#access-list 103 deny tcp any any range 135 138
Router(config)#access-list 103 deny tcp any any range exec 518
Router(config)#access-list 103 deny tcp any any range 6000 6099
Router(config)#access-list 103 deny tcp any any range 12345 12346
Router(config)#access-list 103 deny tcp any any range 54320 54321
Router(config)#access-list 103 deny tcp any any eq 6669
Router(config)#access-list 103 deny tcp any any eq 2222
Router(config)#access-list 103 deny tcp any any eq 7000
Router(config)#access-list 103 deny tcp any any eq 161
Router(config)#access-list 103 permit udp host 192.168.0.71 host 211.219.171.144 eq 161
Router(config)#access-list 103 deny udp any any eq 161
Router(config)#access-list 103 deny udp any any eq 1434
Router(config)#access-list 103 permit ip any any
Router(config)#
Router(config)#^Z
Router#
```

[그림 34] 악성 포트를 필터링 한 예

일단 앞의 룰과 중복되지 않도록 이 룰은 103번으로 설정하였는데, 이후에 앞의 룰과 하나의 룰도 합치면 된다. 먼저 103번 룰에서는 deny를 먼저 설정한 후 마지막에 이외의 패킷은 모두 허용하는 룰을 작성하였다. 소스와 목적지 부분은 any를 하였으므로 소스와 목적지 ip 에 관계없이 목적지 포트와만 관련된 것을 알 수 있다. 앞에서 언급한 바와 같이 단일한 포트를 뜻할 때는 “eq 포트번호” 와 같이 하면 되고 포트범위를 뜻할 때는 “range 시작번호 끝번호” 형식으로 하면 된다.

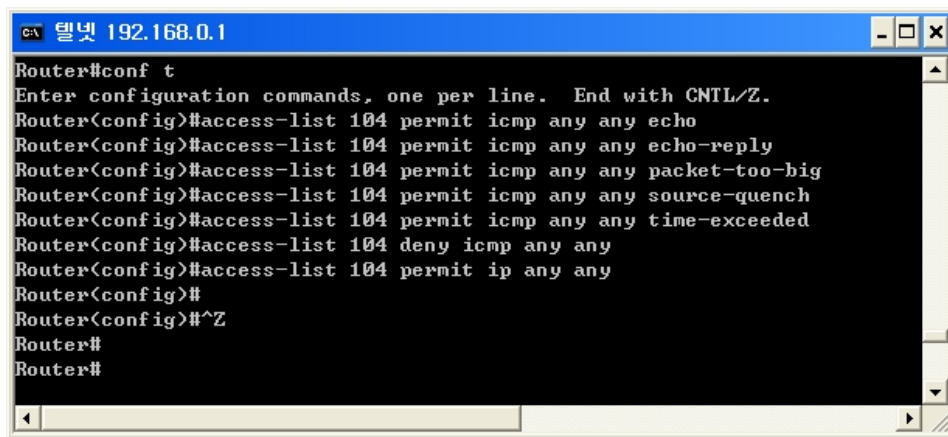
이 중에서 아래에서 3번째 룰인 “access-list 103 deny udp any any eq 161” 을 보면 소스나 목적지에 관계없이 라우터를 통과하는 161/udp 트래픽을 모두 차단한 것을 알 수 있는데, 만약 특정한 ip에서 라우터 내부의 특정한 ip 에 대해서는 허용하고자 할 경우 차단하는 룰 앞에 위와 같이 허용하는 룰을 추가해 주면된다. 위와 같은 경우 161/udp 와 관련된 트래픽 중 소스가 192.168.0.71 이고 목적지가 211.219.171.144 로 향하는 패킷은 허용하되 다른 161/udp 트래픽은 거부한다는 의미가 된다.

지금까지는 ip 및 tcp 나 udp 등의 필터링에 대해 알아보았는데, 추가적으로, icmp 에 대해 필터링을 어떻게 할 것인지 고민해 보아야 한다. icmp 는 tcp 나 udp 와 달리 포트번호로 서로 구분하지 않고 icmp type 과 code 라는 것으로 구분한다. 라우터에서는 반드시 허용해 주어야 할 몇 가지 타입과 코드를 제외하고는 필터링 하는 것이 좋다.

icmp type 과 code 목록에 대해서는 아래 url을 참고하면 된다.

<http://www.iana.org/assignments/icmp-parameters>

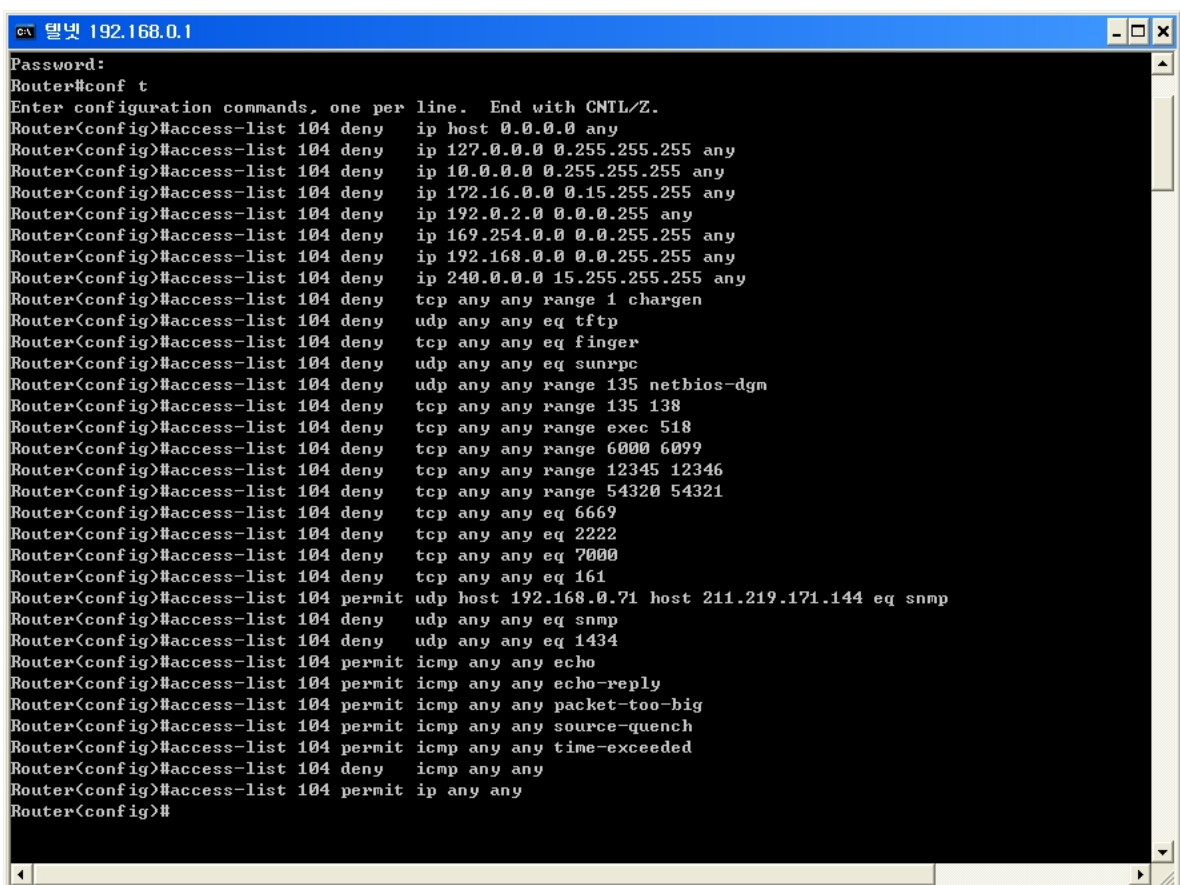




```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 104 permit icmp any any echo
Router(config)#access-list 104 permit icmp any any echo-reply
Router(config)#access-list 104 permit icmp any any packet-too-big
Router(config)#access-list 104 permit icmp any any source-quench
Router(config)#access-list 104 permit icmp any any time-exceeded
Router(config)#access-list 104 deny icmp any any
Router(config)#access-list 104 permit ip any any
Router(config)#
Router(config)#^Z
Router#
Router#
```

[그림 35] icmp 패킷 필터링 예

이제 앞에서 살펴본 3개의 룰인 access-list 102, 103, 104 번 룰을 합칠 차례이다. access-list 번호만 같게 설정하여 하나로 통합하면 아래와 같이 보이게 될 것이다.

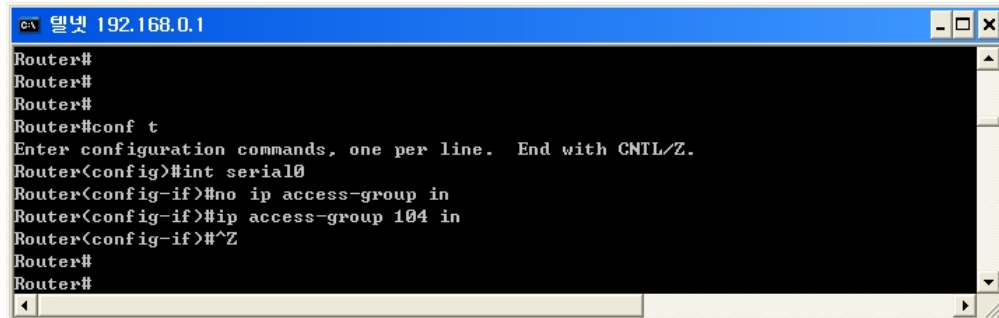


```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 104 deny ip host 0.0.0.0 any
Router(config)#access-list 104 deny ip 127.0.0.0 0.255.255.255 any
Router(config)#access-list 104 deny ip 10.0.0.0 0.255.255.255 any
Router(config)#access-list 104 deny ip 172.16.0.0 0.15.255.255 any
Router(config)#access-list 104 deny ip 192.0.2.0 0.0.0.255 any
Router(config)#access-list 104 deny ip 169.254.0.0 0.0.255.255 any
Router(config)#access-list 104 deny ip 192.168.0.0 0.0.255.255 any
Router(config)#access-list 104 deny ip 240.0.0.0 15.255.255.255 any
Router(config)#access-list 104 deny tcp any any range 1 chargen
Router(config)#access-list 104 deny udp any any eq tftp
Router(config)#access-list 104 deny tcp any any eq finger
Router(config)#access-list 104 deny udp any any eq sunrpc
Router(config)#access-list 104 deny udp any any range 135 netbios-dgm
Router(config)#access-list 104 deny tcp any any range 135 138
Router(config)#access-list 104 deny tcp any any range exec 518
Router(config)#access-list 104 deny tcp any any range 6000 6099
Router(config)#access-list 104 deny tcp any any range 12345 12346
Router(config)#access-list 104 deny tcp any any range 54320 54321
Router(config)#access-list 104 deny tcp any any eq 6669
Router(config)#access-list 104 deny tcp any any eq 2222
Router(config)#access-list 104 deny tcp any any eq 7000
Router(config)#access-list 104 deny tcp any any eq 161
Router(config)#access-list 104 permit udp host 192.168.0.71 host 211.219.171.144 eq snmp
Router(config)#access-list 104 deny udp any any eq snmp
Router(config)#access-list 104 deny udp any any eq 1434
Router(config)#access-list 104 permit icmp any any echo
Router(config)#access-list 104 permit icmp any any echo-reply
Router(config)#access-list 104 permit icmp any any packet-too-big
Router(config)#access-list 104 permit icmp any any source-quench
Router(config)#access-list 104 permit icmp any any time-exceeded
Router(config)#access-list 104 deny icmp any any
Router(config)#access-list 104 permit ip any any
Router(config)#
```

[그림 36] 통합된 access-list 설정

앞에서는 각각의 룰을 따로 작성하였지만 실제로는 위와 같이 한꺼번에 작성하면 된다. 특히 "permit ip any any" 는 마지막에 한번만 들어가야 한다는 점을 주의하

기 바란다. access-list 설정이 끝난 후에는 access-group을 이용하여 룰을 해당 인터페이스에 지정하면 된다.



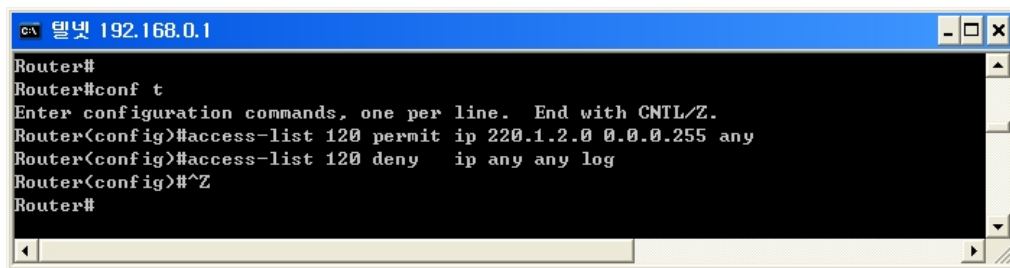
```
터미널 192.168.0.1
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int serial0
Router(config-if)#no ip access-group in
Router(config-if)#ip access-group 104 in
Router(config-if)#^Z
Router#
Router#
```

[그림 37] access-group 에 적용한 예

위 그림에서는 serial0 인터페이스에 access-group을 설정하였는데, 하나의 인터페이스에서는 in 이나 out 이 각각 1개씩만 언급될 수 있으므로 적용을 하기 전에 no ip access-group in 으로 in 과 관련된 기존의 access-group을 삭제하였다. 그리고 access-group을 적용하였는데, 여기에서 104 는 앞에서 설정한 access-list의 번호를 뜻한다. 라우터의 외부에서 내부로 들어오는 패킷에 대한 제어이므로 serial 인터페이스에서 in 으로 설정하였으며 만약 이더넷 인터페이스에서 설정하려면 out 으로 하여야 할 것이다.

## STEP 2. egress filtering 설정하기

다음으로는 ingress filtering 과 반대의 개념인 egress filtering 에 대해 알아보도록 한다. 앞에서 살펴보았던 ingress filtering 이 라우터 외부에서 라우터 내부로 들어오려는 패킷의 소스ip 나 목적지 포트등을 살펴보고 필터링 한 것이라면 지금부터 살펴볼 egress filtering 이란 반대로 내부에서 라우터 외부로 나가는 패킷의 소스 ip 를 체크하여 필터링하는 것이다. 만약 라우터 내부에서 220.1.2.0/24 의 C class 대역을 사용한다면 라우터를 통과하여 외부로 나가는 트래픽의 소스 ip 는 반드시 이 대역인 것이 정상이며 이외의 패킷은 모두 위조된 패킷일 것이다. 따라서 라우터를 통해 나가는 패킷의 소스 ip중 사용중인 ip 대역을 소스로 한 패킷은 허용하고 나머지는 거부하도록 access-list를 설정하면 내부 네트워크에서 소스 ip를 위조하여 외부로 나가는 트래픽을 차단할 수 있을 것이다.

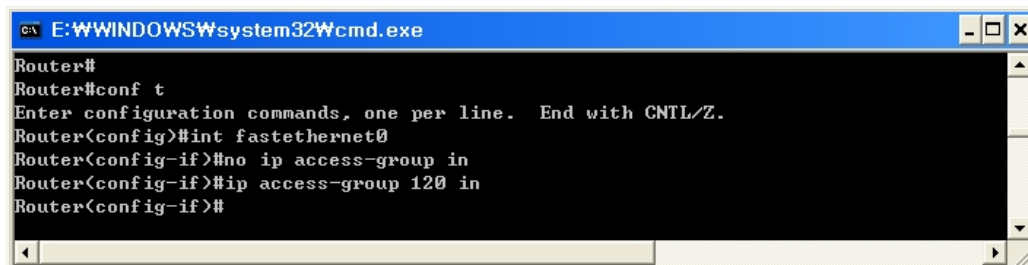


```
c:\ 텔넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 120 permit ip 220.1.2.0 0.0.0.255 any
Router(config)#access-list 120 deny ip any any log
Router(config)#^Z
Router#
```

[그림 38] access-list 설정

위는 내부 네트워크에서 220.1.2.0/24 즉 C class 대역을 사용한다고 가정하고 access-list를 설정한 예이다. 이 룰은 소스 ip 가 220.1.2.0/255.255.255.0 인 패킷은 허용하고 이외의 패킷은 모두 거부한다는 의미가 된다. 거부시 마지막에 log 가 추가되었는데, 이를 통해 이 룰에 매칭된 패킷 즉, 위조된 패킷이 보일 경우에는 로그에 남게 된다.

access-list 설정을 한 후에는 access-group을 이용하여 해당 인터페이스에 룰을 적용할 차례이다. 라우터 내부에서 외부로 나가는 패킷에 대한 제어이므로 이더넷 인터페이스에 적용하면 in 이 되고, 시리얼 인터페이스에 적용하면 out 이 될 것이다. 아래는 이더넷 인터페이스에 in 으로 설정한 예이다. 여기에서 in 이라고 해서 외부에서 내부로 들어오는 패킷에 대한 제어가 아니라는 것을 주의하기 바란다.



```
c:\ E:\WINDOWS\system32\cmd.exe
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fastethernet0
Router(config-if)#no ip access-group in
Router(config-if)#ip access-group 120 in
Router(config-if)#
```

[그림 39] access-group 설정

### STEP 3. Null routing을 활용한 필터링

access-list 와 함께 유용하게 사용할 수 있는 필터링 기법으로는 blackhole 필터링이라는 것이 있다. 이는 access-list 와 비슷한 효과를 내면서도 더욱 간편하게 사용할 수 있는데, 다음과 같은 경우를 생각해 보자. 만약 시스템이나 네트워크를 모니터링 하던 중 특정ip 또는 특정 대역에서 비정상적인 시도가 감지되었을 경우 해당 ip를 차단하기 위해 매번 기존 access-list를 지우고 새롭게 ip를 추가하여 작성하는 것은 여간 번거로운 일이 아닐 수 없다. 이때 사용할 수 있는 것이 바로 black hole 필터링인데, 명령어 자체는 특정한 목적지 ip 또는 ip 대역에 대하여 routing 테이블을

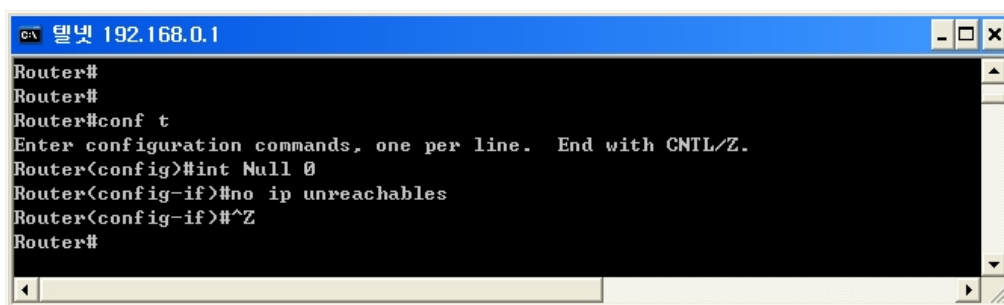
생성하는 방식과 동일하다. 다만, 특정한 ip 또는 ip 대역에 대해서 Null 이라는 가상의 쓰레기 인터페이스로 보내도록 함으로써 패킷의 통신이 되지 않도록 하는 것이다. 이의 사용 형식은 다음과 같다.

```
interface Null0
no ip unreachable

ip route <차단하고자하는목적지ip또는ip대역> <netmask> Null0
```

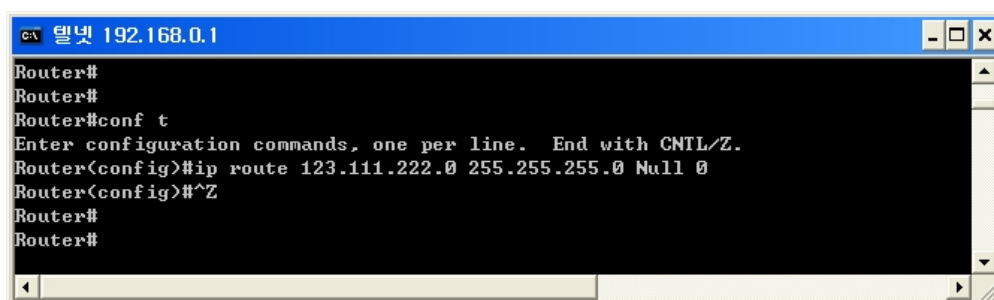
라우터에서는 패킷이 Null 0 인터페이스로 보내어져 패킷이 필터링 될 때마다 패킷의 소스 ip 로 icmp unreachable 이라는 에러 메시지를 발송하게 되는데, 만약 필터링 하는 패킷이 많을 경우에는 라우터에 과부하를 유발할 수 있기 때문에 Null 인터페이스에서 이에 대해 icmp 에러 메시지로 응답하지 않도록 no ip unreachable 설정을 반드시 하도록 한다.

아래의 경우 192.168.3.4 ip 를 차단하는 예를 보여주고 있다. 명령어의 형식은 static routing 이므로 mask를 적용할 때에는 access-list 에서 사용하던대로 wildcard mask 가 아니라 netmask를 그대로 사용하여야 한다는 점을 주의하기 바란다.



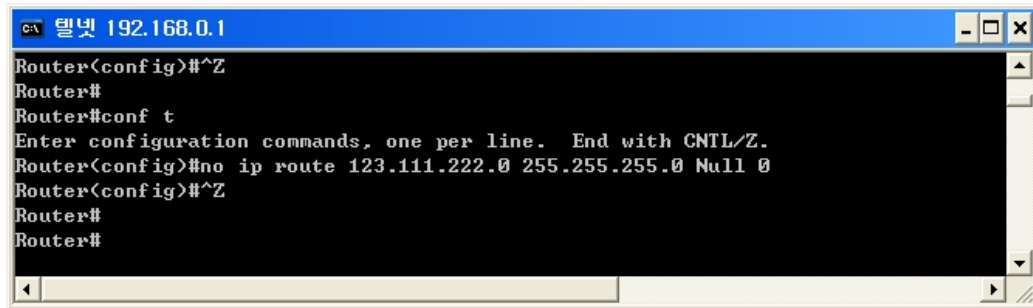
[그림 40] Null 0 인터페이스 생성

위 그림에서는 먼저 Null 0 인터페이스를 생성하고, 이 인터페이스에서 no ip unreachable 설정을 하였다.



[그림 41] Null 라우팅 설정

이후 blackhole 필터링할 ip 또는 ip 대역을 설정하였다. 위의 경우 123.111.222.0/24 대역에 대한 필터링 설정으로 라우터 내부에서는 위 ip 대역으로 접근할 수 없고, 위 ip 대역에서 라우터 내부의 네트워크로 접근할 때 역시 응답을 받을 수 없어 통신을 할 수 없게 된다. 물론 특정 ip 만을 필터링하고자 한다면 255.255.255.255를 이용하면 된다.



[그림 42] blackhole 필터링 설정 해제

물론 앞서 설정한 필터링 설정을 해제하려면 명령어 앞에 no를 붙여서 실행해 주면 된다.

#### STEP 4. Unicast RPF를 이용한 필터링

마지막으로 살펴볼 필터링 기능은 Unicast RPF(Unicast Reverse-Path Forwarding)라는 것으로 이를 이용하면 앞에서 살펴본 access-list 나 blackhole 필터링을 이용하여 일일이 ip 나 ip 대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

Unicast RPF 의 원리는 인터페이스를 통해 들어오는 패킷의 소스 ip 에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다. 즉, URPF 가 enable 된 인터페이스에 1.1.1.1 이라는 소스 ip 를 달고 들어오는 패킷이 있다면 라우팅 테이블을 확인하여 만약 1.1.1.1이라는 목적지로 라우팅 될 때 같은 인터페이스를 통하여 나가는지 확인하여 같다면 정상적인 트래픽으로 간주하여 트래픽을 통과시키고, 다르다면 스푸핑 된 패킷으로 간주하여 필터링하는 것이다. 만약 Unicast RPF를 serial 인터페이스에 설정한다면 라우팅 테이블에 없거나 소스 ip 를 위조하는 형태의 패킷을 필터링할 수 있을 것이고, ethernet 인터페이스에 설정한다면 내부에서 패킷을 위조하여 나가는 패킷을 필터링 할 수 있을 것이다. 즉, serial 인터페이스에 설정할 경우 ingress 필터링의 효과를, ethernet 인터페이스에 설정할 경우 egress 필터링의 효과를 기대할 수 있을 것이다.

```
C:\ 델넷 192.168.0.1
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip cef
Router(config)#int serial0
Router(config-if)#ip verify unicast reverse-path
Router(config-if)#^Z
Router#
```

[그림 43] URPF 설정

Unicast RPF를 사용하려면 먼저 라우터에서 CEF 를 설정하여야 하며 만약 CEF 가 지원하지 않으면 이 기능을 이용할 수 없다. 이후 URPF를 설정할 해당 인터페이스에 설정을 하면 된다.

```
C:\ 델넷 192.168.0.1
Router#
Router#
Router#
Router#sh ip cef
%CEF not running
Prefix          Next Hop      Interface
Router#
```

[그림 44] CEF 가 enable 되어 있지 않을 경우

먼저 CEF 가 enable 되어 있는지 아래와 같이 확인해 보기 바란다. 위와 같은 그림의 경우 CEF 가 enable 되어 있지 않은 것이다.

```
C:\ 델넷 192.168.0.1
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip cef
Router(config)#interface serial0
Router(config-if)#ip verify unicast reverse-path
Router(config-if)#^Z
Router#
```

[그림 45] URPF 설정

위 그림은 먼저 global config 모드에서 ip cef를 실행하여 CEF를 enable 한 후 serial 0 인터페이스에 URPF를 설정하는 예를 보여주고 있다. 위의 경우 serial 인터페이스에 설정하였으므로 외부에서 들어오는 패킷에 대해 Reverse 경로를 체크하게 된다.

만약, 설정 이후 이를 해제하려면 해당 인터페이스 모드에서 "no ip verify unicast

reverse-path“를 입력하면 된다.

지금까지 Unicast RPF 의 장점만을 언급하였지만 그렇다고 해서 반드시 모든 환경에서 적합한 것은 아니다. 특히 라우터에서 두 개 ISP 이상과 연동되어 있다면 이 설정을 하지 말아야 한다. 이를테면 한국통신(KT) 과 하나로(hanaro) 의 E1 회선을 2개 연동하여 사용한다면 경우에 따라 KT 로 나간 접속이 하나로를 통해 들어오거나 반대로 하나로로 나간 접속이 KT를 통해 들어오는 일이 있을 수 있기 때문이다. 이러한 경우 만약 Unicast RPF 가 설정되어 있다면 비정상적인 패킷으로 간주하여 패킷을 차단해 버리게 되기 때문이다.

<참고> CEF(Cisco Express Forwarding)

라우터가 Switching을 하는 방법에는

Process Switching 과 Fast Switching 그리고 CEF(Cisco Express Forwarding) 이 있는데, Process Switching 은 패킷을 전송할 때마다 매번 라우팅 테이블과 Next hop을 확인후 패킷을 전송하는 방식으로 속도가 느리다. 이때 config를 보면 아래와 같이 보이게 된다.

```
no ip cef
```

```
interface serial 0
```

```
no ip route-cache
```

다음으로 Fast Switching 은 패킷이 통과할 때 처음에는 앞에서 설명한 Process Switching 을 하고, 두 번째부터는 이때 저장된 Cache를 이용하여 패킷을 전송하는 방식으로, Process Switching 방식에 비해서 스위칭이 빨라진다. 이때 config를 보면 아래와 같이 보이게 된다.

```
no ip cef
```

```
interface serial 0
```

```
ip route-cache
```

마지막으로 CEF 는 Fast Switching을 더욱 개선한 방식으로 아예 처음부터 라우팅 테이블을 Cache 로 복사해 놓는 방식이다. 이를 통해 패킷이 통과할 때 바로 Cache에서 응답하므로 더욱 속도가 빨라지게 된다. 이때 config를 보면 아래와 같이 보이게 된다.

```
ip cef
```

```
interface serial 0
```

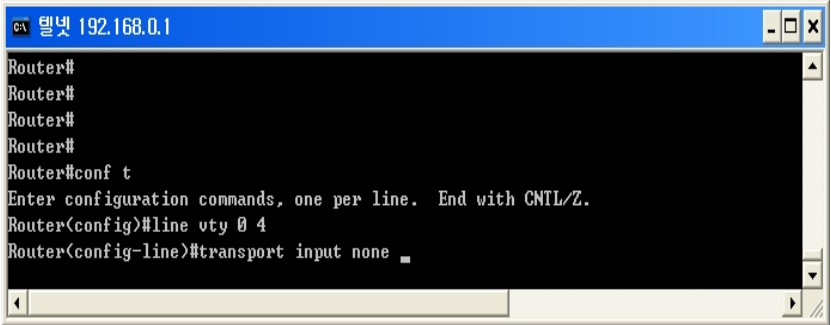
```
ip route-cache
```



## <별첨 #1> 라우터 보안 체크하기

안전한 라우터 설정을 위해서 아래의 항목들은 반드시 설정되어야할 기본적인 보안 설정들에 대해서 정리를 하였다. 해결 방안의 경우 시스코라우터 뿐만 아니라 Alteon Switch 와 Extream Switch 등 널리 쓰이는 스위칭 장비에 대한 커맨드도 수록하였다.

점검항목	설명 및 점검 방법
<p>라우터 접속 시 초기 화면에 비인가자의 라우터 접속에 대하여 라우터 버전 정보 대신 경고를 알리는 메시지가 나타나도록 하여야 한다.</p> <p>※ 점검 방법</p> <p>관리자가 직접 텔넷으로 접근해서 라우터 배너가 노출되어지는 지 확인한다.</p> <p>※ 해결방법</p> <p>배너에 시스템 정보등을 삭제하고 “이곳은 xxx입니다.허가받지 않은 사용자가 접속하여 부당한 사용을 할 경우 법적인 제재를 받을 수 있습니다 ” 라는 식의 경고성 배너를 삽입한다.아래는 각각의 장비별 배너 삽입법 이다</p> <p><b>cisco router</b> banner exec ^C</p> <p><b>Alteon Switch (아래의 위치에 배너 삽입)</b> /cfg/sys/notice /cfg/sys/banner</p> <p><b>Extream Switch</b> config banner</p>	<p>※ 설명</p> <p>라우터 접속 시 초기 화면에 비인가자의 라우터 접속에 대하여 라우터 버전 정보 대신 경고를 알리는 메시지가 나타나도록 하여야 한다.</p> <p>※ 점검 방법</p> <p>관리자가 직접 텔넷으로 접근해서 라우터 배너가 노출되어지는 지 확인한다.</p> <p>※ 해결방법</p> <p>배너에 시스템 정보등을 삭제하고 “이곳은 xxx입니다.허가받지 않은 사용자가 접속하여 부당한 사용을 할 경우 법적인 제재를 받을 수 있습니다 ” 라는 식의 경고성 배너를 삽입한다.아래는 각각의 장비별 배너 삽입법 이다</p> <p><b>cisco router</b> banner exec ^C</p> <p><b>Alteon Switch (아래의 위치에 배너 삽입)</b> /cfg/sys/notice /cfg/sys/banner</p> <p><b>Extream Switch</b> config banner</p>
<p>원격의 사용자가 telnet 로그인이 가능한가?</p>	<p>※ 설명</p> <p>원격의 사용자가 라우터에 telnet 로그인이 가능하지 않도록 해야한다.만약 패스워드가 노출될 경우 치명적인 문제로 발전할수있다.</p> <p>※ 점검 방법</p>

	<p>관리자가 원격에서 라우터에 telnet 로그인 가능한지 확인한다.</p> <p><b>※ 해결방법</b></p> <p><b>cisco router</b> telnet listener 자체를 disable 한다.</p>  <p>[그림 46] 리스너 자체 off 설정</p> <p><b>Alteon Switch</b> /cfg/sys/tnet</p> <p><b>Extream Switch</b> disable telnet</p>
<p>원격의 사용자가 HTTP 로 라우터에 접근이 가능한가?</p>	<p><b>※ 설명</b></p> <p>원격에서 관리를 위해 HTTP 서버를 운영할 수 있지만 보안상 위험하므로 불필요하므로 가능한 제거해야 한다.</p> <p><b>※ 점검 방법</b></p> <p>관리자가 직접 원격에서 라우터 HTTP 서버로 접근 가능한지 확인한다.</p> <p><b>※ 해결방법</b></p> <p><b>cisco router</b> router(config)# no ip http server</p> <p><b>Alteon Switch</b> /cfg/sys/http disable</p> <p><b>Extream Switch</b></p>

	disable web														
보안상 불필요한 서비스가 작동되고 있는가?	<p>※ 설명</p> <p>원격에서 보안상 불필요한 서비스가 열려있다면 라우터의 사용자 정보 및 네트워크 장비에 큰 위험이 될수있으므로 반드시 서비스를 반드시 중지하여야 한다.</p> <p>※ 점검 방법</p> <p>관리자가 직접 원격에서 아래 표의 항목들이 오픈 되었는지 확인한다.</p> <table border="1"> <thead> <tr> <th colspan="2">Telnet을 통한 Tcp 포트 접속시 접속 가능한 Tcp 포트</th> </tr> <tr> <th>Tcp Port number</th> <th>Access Method</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>echo</td> </tr> <tr> <td>9</td> <td>Discard</td> </tr> <tr> <td>23</td> <td>Telnet</td> </tr> <tr> <td>79</td> <td>Finger</td> </tr> <tr> <td>1993</td> <td>SNMP over TCP</td> </tr> </tbody> </table> <p>※ 해결 방법</p> <p><b>cisco router</b></p> <pre>router(config)# no service finger (finger 서비스 제거) router(config)# no ip finger router(config)# no service tftp (tftp 서비스 제거)</pre> <p>※ 확인 방법</p> <p>show configuration 명령으로 확인한다</p> <p><b>Alteon Switch</b></p> <pre>/cfg/slb/filt 10/sport 69 (tftp 서비스 제거) /cfg/slb/filt 10/sport 79 (finger 서비스 제거)</pre> <p>※ 확인 방법</p> <p>/info/dump 명령으로 확인한다.</p>	Telnet을 통한 Tcp 포트 접속시 접속 가능한 Tcp 포트		Tcp Port number	Access Method	7	echo	9	Discard	23	Telnet	79	Finger	1993	SNMP over TCP
Telnet을 통한 Tcp 포트 접속시 접속 가능한 Tcp 포트															
Tcp Port number	Access Method														
7	echo														
9	Discard														
23	Telnet														
79	Finger														
1993	SNMP over TCP														
icmp 서비스가 작동되어 지는가?	<p>※ 설명</p> <p>원격에서 icmp 서비스가 열려있다면 DOS 취약점 이나 라우터의 존재가 외부에 노출 되므로 icmp 서비스는 중지하는것이 좋다.</p>														

	<p>※ 점검 방법</p> <p>관리자가 직접 원격에서 ping 명령어를 이용해서 icmp 사용여부를 확인한다.</p> <p>※ 해결방법</p> <p><b>cisco router</b></p> <pre>Router(config-if)#no ip redirects Router(config-if)#no ip directed-broadcast</pre> <p><b>Alteon Switch</b></p> <p>ip unreachable 기능사용 한다. icmp type code의 하나로 외부에서의 stealth scanning에 사용될수 있으므로 불 필요시 제거한다.</p> <pre>/cfg/slb/filt/adv/icmp commandICMP Message type: 3(destun) : ICMP destination unreachable</pre> <p><b>Extream Switch</b></p> <pre>disable icmp redirects { vlan &lt;name&gt; } switch &gt; disable icmp unreachableables { vlan &lt;name&gt;} (unreachable는 인터넷에서 stealth scanning하는 경우에 사용된다.)</pre>
<p>원격에서 snmp 서비스 유추하기 쉬운지 원격에서 읽기 및 쓰기가 가능한지 확인한다.</p>	<p>※ 설명</p> <p>원격에서 SNMP community string 이 유추하기 쉽다면 네트워크 장비에 대한 설정파일 등이 외부에 노출되게 된다.</p> <p>※ 점검 방법</p> <p>관리자가 직접 원격에서 진단툴을 사용해서 확인해본다.</p> <p>※ 해결방법</p> <p><b>cisco router</b></p> <p>SNMP community string 을 public/private 와 다른 이름으로 설정한다.</p> <pre>Router(config)# snmp-server community \$\$\$\$</pre> <p>access-list를 사용하여 SNMP get-request 및 get-request message 명령은</p>

	<p>특정 ip에서만 사용 가능하도록 설정 하여야 한다.</p> <p>※ 불필요시 SNMP Community Strings 삭제 방법</p> <pre>router &gt; no snmp-server community \$\$\$\$ RO router &gt; no snmp-server community xxxx RW</pre>
	<p><b>Alteon Switch</b></p> <p>네트워크상에 보내어지는 SNMP community string 을 침입자가 trap 메시지를 사용할 수 없도록 방지함.</p> <pre>/cfg/snmp/auth enable</pre> <p>※ 불필요시 SNMP Community Strings 삭제 방법</p> <pre>/cfg/snmp/trap1 ip_address /cfg/snmp/t1comm community_string</pre>
	<p><b>Extream Switch</b></p> <pre>disable snmp access    (snmp 접속을 금지 시킴) disable snmp traps     (snmp trap을 제거함) config snmp community [read-only   read-write] &lt;string&gt; config snmp readonly access-profile [&lt;access-profile&gt;]   none]</pre>