IT 관리자가 알아야 할 보안 키포인트

네트워크의 미래를 제시하는 세미나 **NetFocus 2003** :
IT 관리자를 위한 네트워크 보안 방법론

on the NET
Network Intelligence for Leading Networkers

㈜오늘과내일 / 과장
홍 석 범
antihong@tt.co.kr

발표 순서

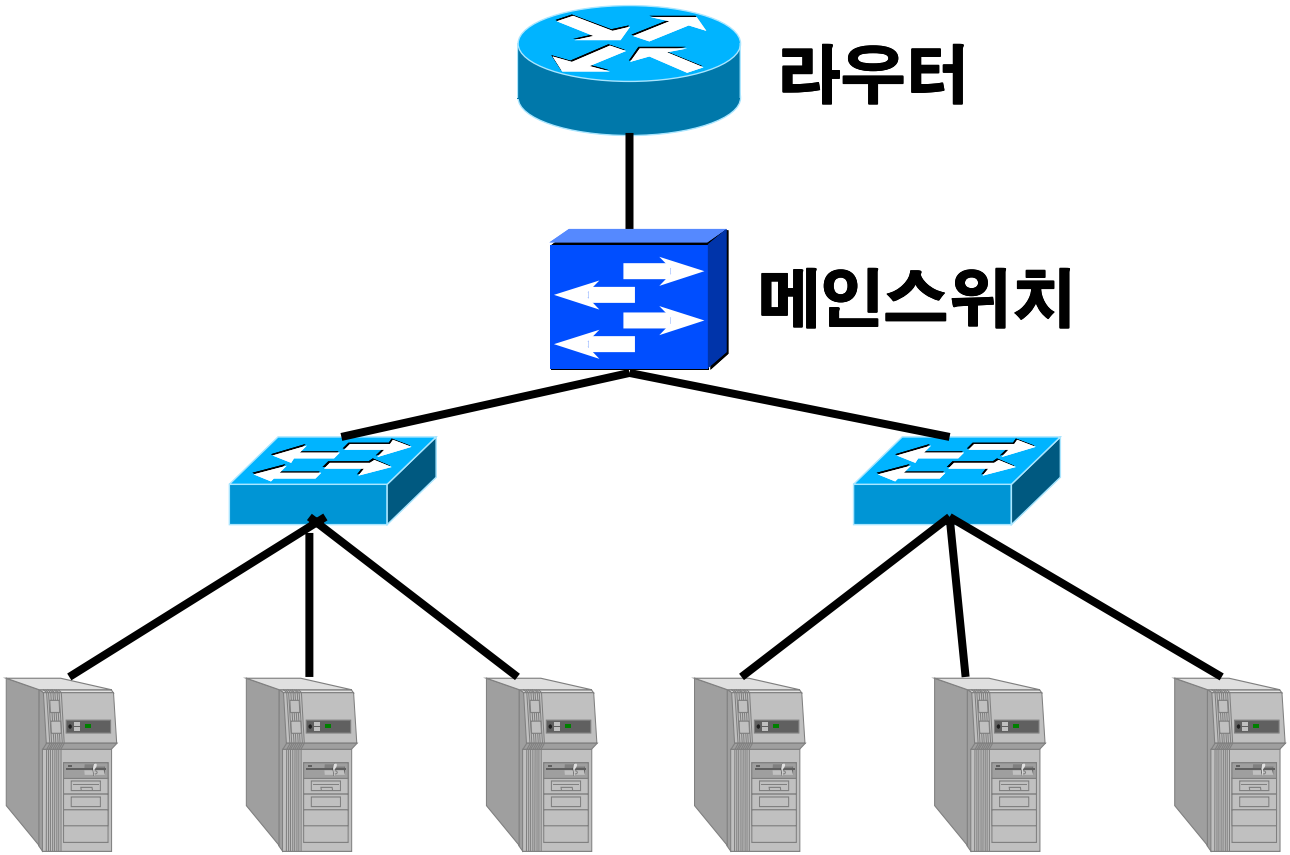
1. 스니핑등 네트워크 기반 공격의 이해
   기본전제 : 네트워크는 원래(!) 취약하다.

2. 라우터 , 스위치 보안

3. 서버보안
   -. 메일 서버 보안
   -. DNS 서버 보안
   -. 웹서버, ftp 서버 보안

4. 사무실에서의 보안
   -. 공유차단
   -. 사설 네트워크 구현
   -. p2p 프로그램 차단

네트워크 구성의 전형



네트워크 기반 공격의 이해 **(1)**

-. LAN 구간의 통신 : ARP의 Broadcast가 선행.

Windows의 경우 IP 충돌을 검사하기 위해 부팅시 arp 를 broadcast

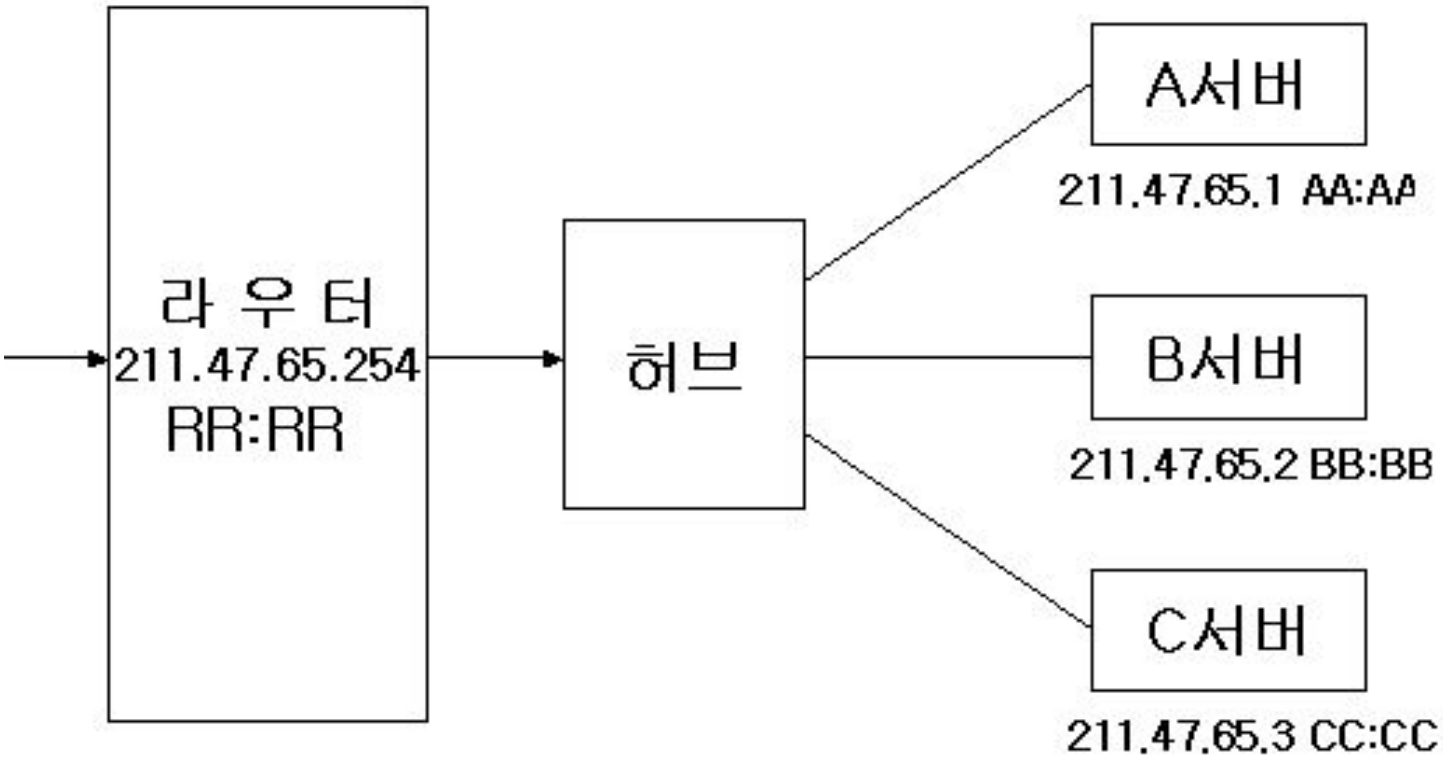
-. ARP(Address Resolution Protocol)

IP --> MAC(Media Access Control)

-.로컬구간에서 TCP 접속시

ARP 교환후 3 Way-Handshake 시작.
(tcpdump or windump로 확인)
Windump : http://windump.polito.it/

ARP 작동방식


라 우 터
211.47.65.254
RR:RR
허브
A서버
211.47.65.1 AA:AA
B서버
211.47.65.2 BB:BB
C서버
211.47.65.3 CC:CC

실시간 ARP 작동예

```
#
# tcpdump -e arp
ning on eth0
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.150 tell 211.47.67.2
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.181 tell 211.47.67.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.224 tell 211.47.67.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.205 tell 211.47.67.2
1 52:54:5:f0:e7:f8 Broadcast arp 60: arp who-has 211.47.67.187 tell 211.47.67
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.65.250 tell 211.47.65.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.106 tell 211.47.67.2
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 0:50:8b:9a:2e:a8 0:50:8b:9a:2a:1 arp 60: arp who-has 211.47.65.192 tell 211
1 0:50:8b:9a:2a:1 0:50:8b:9a:2e:a8 arp 60: arp reply 211.47.65.192 is-at 0:50
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.67 tell 211.47.67.25
1 0:0:0:0:31:70 Broadcast arp 60: arp who-has 211.47.64.64 tell 211.47.64.71
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.150 tell 211.47.67.2
1 52:54:5:f0:e7:f8 Broadcast arp 60: arp who-has 211.47.67.187 tell 211.47.67
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.65.250 tell 211.47.65.2
1 0:0:f0:51:4:1e Broadcast arp 60: arp who-has 211.47.67.112 tell 211.47.67.1
1 0:0:f0:51:4:1e Broadcast arp 60: arp who-has 211.47.67.119 tell 211.47.67.1
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.65.224 tell 211.47.65.2
1 52:54:5:f0:e7:f8 Broadcast arp 60: arp who-has 211.47.67.187 tell 211.47.67
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.205 tell 211.47.67.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.106 tell 211.47.67.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.224 tell 211.47.67.2
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 52:54:5:f0:e7:f8 Broadcast arp 60: arp who-has 211.47.67.187 tell 211.47.67
1 0:d0:b7:88:ea:4a Broadcast arp 60: arp who-has 211.47.65.206 tell 211.47.65
1 0:a0:4b:9:c6:72 Broadcast arp 60: arp who-has 211.47.64.254 tell 211.47.64.
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.65.250 tell 211.47.65.2
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.106 tell 211.47.67.2
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.67.150 tell 211.47.67.2
1 0:e0:7d:7f:31:90 Broadcast arp 60: arp who-has 211.47.64.168 tell 211.47.64
1 0:50:8b:9a:2e:a8 Broadcast arp 60: arp who-has 211.47.65.143 tell 211.47.65
1 0:2:fc:8:c4:a0 Broadcast arp 60: arp who-has 211.47.65.224 tell 211.47.65.2
```

Arp 작동방식

arp who-has 192.168.1.192 tell 192.168.1.1

→ 192.168.1.1이 192.168.1.192의 MAC 주소를 알기 위해 브로드캐스트 질의

arp reply 192.168.1.192 0:50:8b:9a:2e:a8

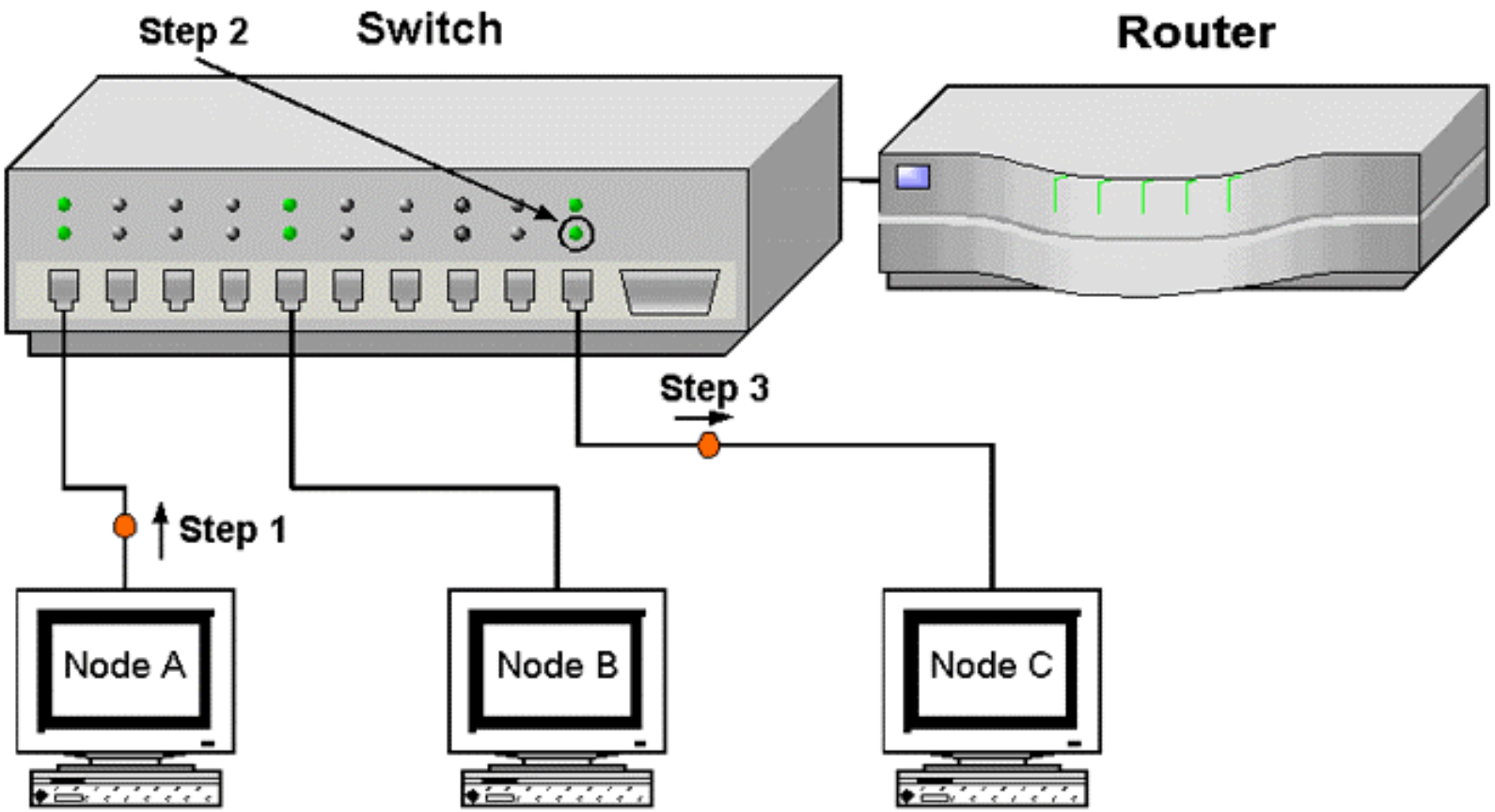
→ 192.168.1.192 의 MAC 주소가 (0:50:8b:9a:2e:a8)임을 응답함

-. arp cache

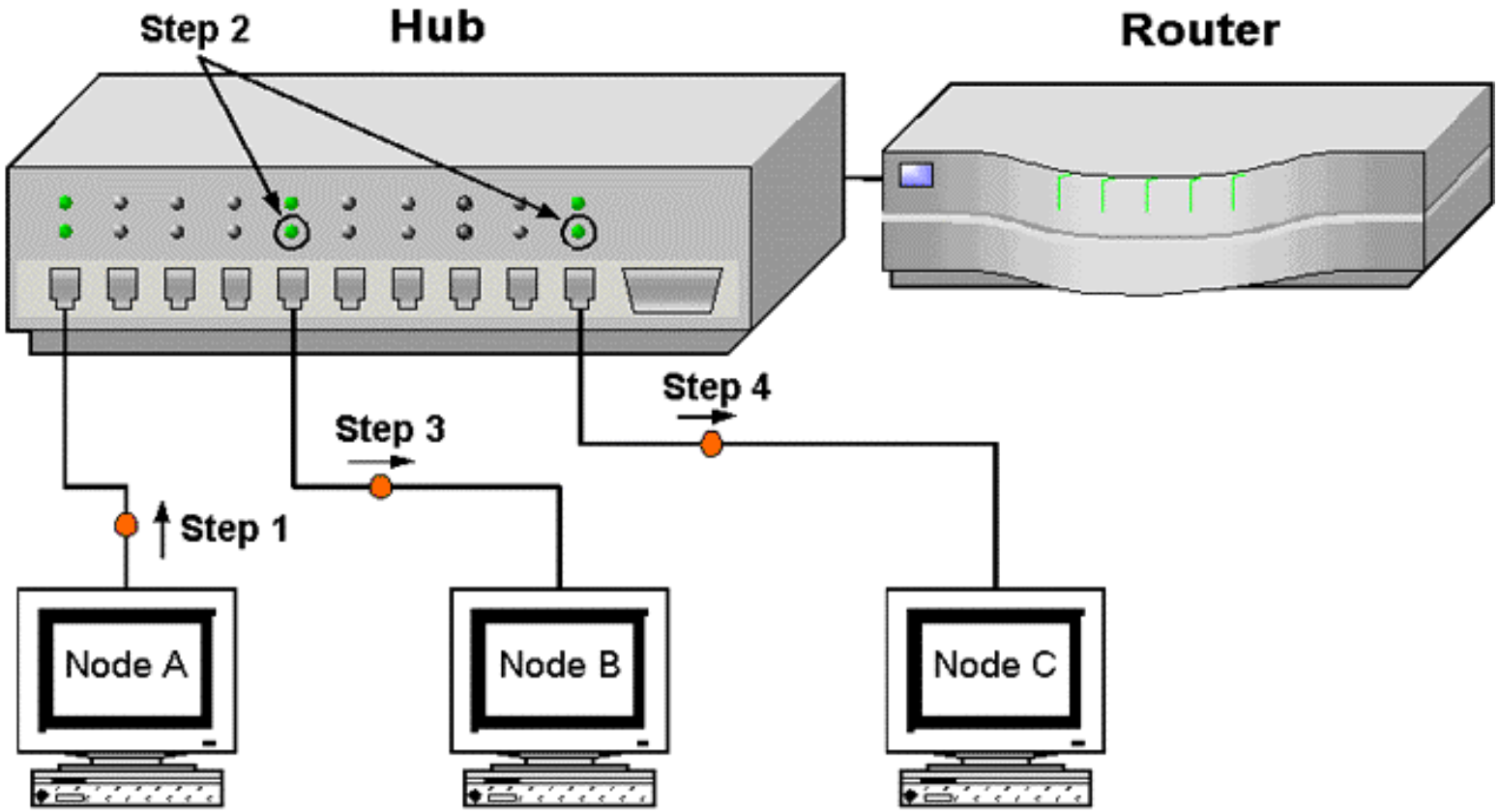
arp cache timeout: 서버:60s, 라우터4h

```
[root@test1 ~]# arp -a
? (211.47.65.15) at 00:50:8B:9A:2E:A8 [ether] on eth0
? (211.47.65.254) at 00:02:FC:08:C4:A0 [ether] on eth0
ns5.tt.co.kr (211.47.65.75) at 00:50:8B:9A:2C:AF [ether] on eth0
? (211.47.65.51) at 00:50:8B:9A:37:9A [ether] on eth0
[root@test1 ~]#
```

스위치 및 허브의 차이(스위치)



스위치 및 허브의 차이(허브)



스위치/허브에서의 arp

Dummy 환경

(1) arp 요청
(2) arp 응답
(3) tcp 3 way handshake
(4) 데이터 교환 모두 broadcast

Switch 환경

(1) arp 요청만이 broadcast
(2) arp 응답
(3) tcp 3 way handshake
(4) 데이터 교환 모두 unicast 로 작동

스위치환경에서 다른 IP가 보이는 경우

(1) 미러링(span) 포트인 경우

(2) 스위치가 어떤 포트로 패킷을 포워딩 해줘야 할 지 모르는 경우

(3) 스위치의 각 포트별 IP:MAC 정보 메모리가 Full 일 경우

(4) 기본적으로 모든 스위치는 완전히 모든 패킷을 정확히 필터링 하지 않음. 특히 스위치가 busy 할 경우.

Sniffing

가능한 이유

(1) Plain text 전송

(2) broadcast

Dummy허브대신 스위치 사용?

Arp 위조를 이용한 스니퍼 프로그램

http://www.arp-sk.org/

http://monkey.org/~dugsong/dsniff/

http://www.securiteam.com/tools/5ZP0D1F2KQ.html

Gratuitous Arp

gratuitous_arp -i eth0 192.168.1.3 00D0B788E08F 192.168.1.255 ffffffffffff

ARP 를 이용한 sniffing

Switch Jam(MAC Flooding)

위조된 MAC을 지속적으로 발생시켜 스위치의 ARP 테이블을 Flood 시킨다.

→ dsniff 의 경우 분당 155,000개 MAC 정보 발생

ARP Redirect

자신이 마치 Gateway 인 것처럼 위조된 MAC 을 Broadcast하여 모든 트래픽이 통과하게 한다.

ARP Spoofing

양 서버사이에서 스니핑하고자 하는 서버인 것처럼 MAC을 위조하여 트래픽을 포워딩한다.

MAC Duplicating

스니핑하고자 하는 서버의 MAC주소와 같은 MAC 주소를 설정하는 방법.

Sniffing 에 대한 대처 방법

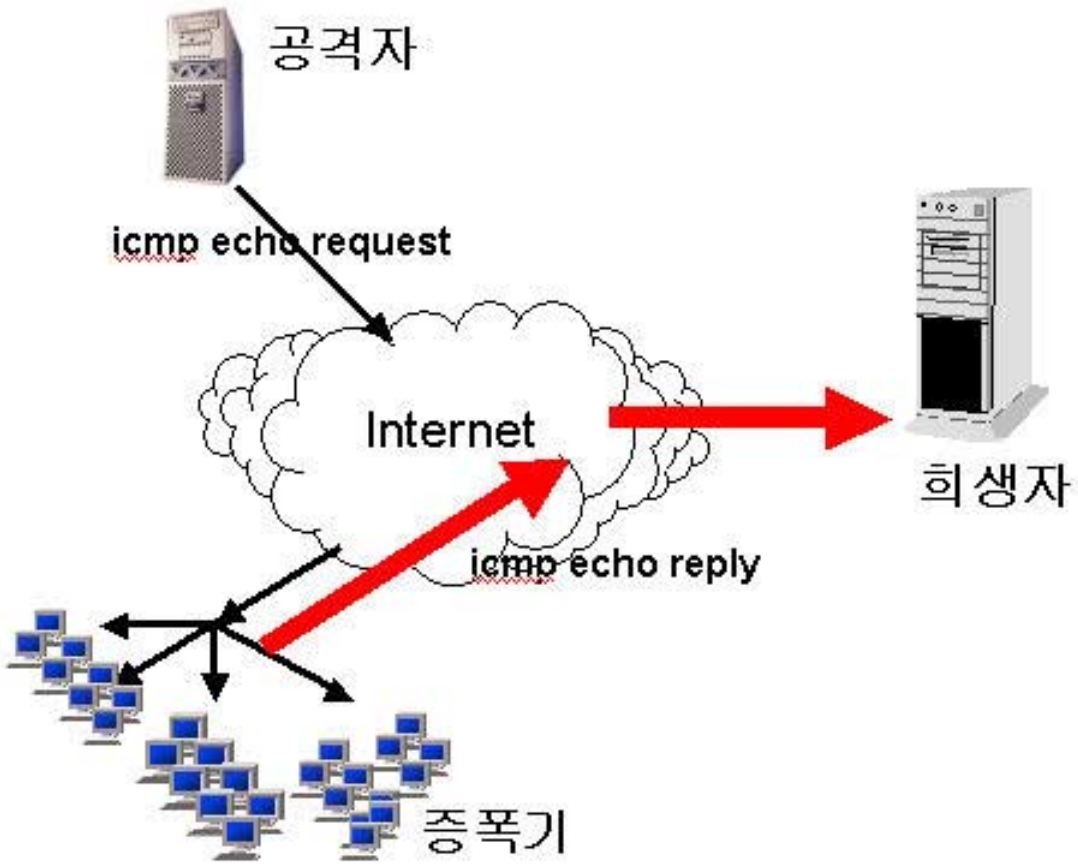
(1) IP Flitering
각각의 스위치 포트에서 오가는 트래픽을 필터링

(2) Port security
각각의 포트에 물리적인 MAC 주소를 정적(Static)으로 설정

(3) 라우터 등에서 static 설정
Router# **conf t**
Router(conf)# **arp 1.1.1.1 00d0.b789.d700**

(4) 암호화 전송 프로토콜 사용

icmp 기반의 DDoS 공격



icmp 기반의 DDoS 공격

-. 외부에서의 broadcast 요청에 응답하는 경우

```
# ping 202.102.233.255
PING 202.102.233.255 (202.102.233.255) from 211.0.0.1 : 56(84) bytes of data.
64 bytes from 202.102.233.207: icmp_seq=0 ttl=126 time=3345.4 ms
64 bytes from 202.102.233.194: icmp_seq=0 ttl=126 time=3542.7 ms (DUP!)
64 bytes from 202.102.233.193: icmp_seq=0 ttl=126 time=3738.8 ms (DUP!)
64 bytes from 202.102.233.214: icmp_seq=0 ttl=126 time=4053.1 ms (DUP!)
64 bytes from 202.102.233.207: icmp_seq=1 ttl=126 time=3316.3 ms
64 bytes from 202.102.233.194: icmp_seq=1 ttl=126 time=3541.0 ms (DUP!)
```

-. 열려있는 IP 대역 : http://www.netscan.org/

-. 공격자가 되지 않기 위해

-- egress filtering

-. 희생자가 되지 않기 위해

-- icmp echo reply 에 대한 rate-limit(QoS)

icmp 기반의 DDoS 공격

-.증폭기(amplifier)로 악용되지 않기 위해

(1) no ip directed-broadcast

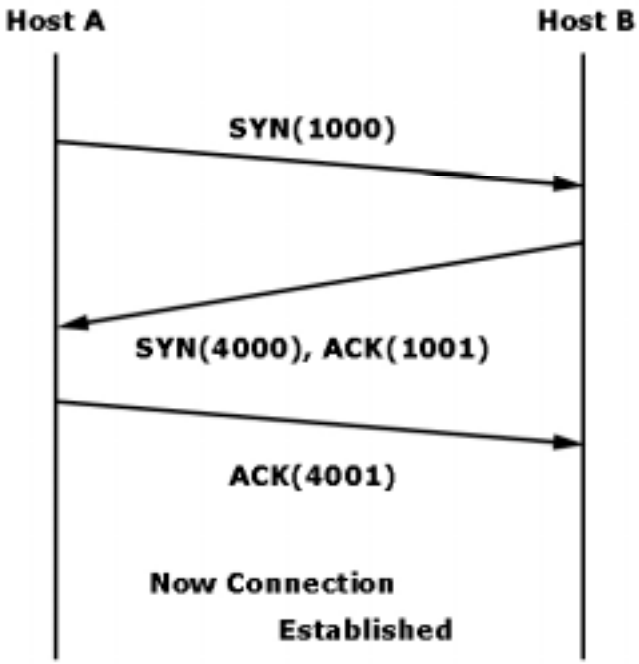
Router(config)# **interface serial 2/0**
Router(config-if)# **no ip directed-broadcast**

(2) access-list

Router(config)# **access-list 110 deny ip any host 14.2.6.255**
Router(config)# **access-list 110 deny ip any host 14.2.6.0**
Router(config)# **interface interface serial 2/0**
Router(config-if)# **ip access-group 110 in**

TCP 기반의 DoS 공격

-.SYN_Flooding Attack



3 way handshake

TCP 기반의 DoS 공격

-.**SYN_Flooding Attack** 에 대한 대비방법

1. 시스템의 백로그큐(Backlog Queue) 크기를 늘려준다.

2. 리눅스계열 : syncookies

   Windows 계열 : 레지스트리 변경

3. 라우터나 파이어월의 방어 솔루션을 이용한다.

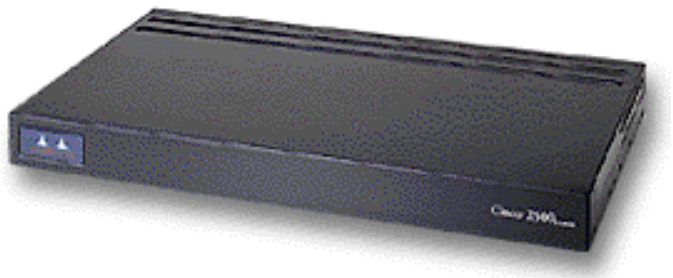
tcp intercept (실제 적용시 주의)

- -. Intercept mode
- -. watch mode

라우터 보안

-. 라우터 자체 보안
-. 라우터를 통한 네트워크 보안

1. 라우터에 password 설정하기
2. telnet 접근 제한하기
3. SNMP 설정하기
4. 불필요한 서비스 disable
5. 패킷 필터링
6. 네트워크 모니터링



라우터에 **password** 설정하기

Console Password (Console 접속 시 사용)

```
Router#configure terminal
Router(configure)#line console 0
Router(configure-line)#password router
```

Terminal Password (Telnet 접속 시 사용)

```
Router#configure terminal
Router(config)#line vty 0 4
Router(config-line)#password router
```

Enable Password

```
Router#configure terminal
Router(config)enable password 12345
```

Enable Secret

```
Router#configure terminal
Router(config)enable secret 12345
```

라우터에 **password** 설정하기

typ 0 : cleartext
typ 5 : one way md5 hash – nonreversible
typ 7 : reversible

Hash function　　Reverse function
Cisco ----------→ 02050D480809 ----------→ Cisco

telnet 접근제한(1/2)

Access-list 를 이용한 접근제어

```
access-list 10 permit host 211.1.2.3
access-list 10 permit host 211.1.2.4
access-list 10 deny any
line vty 0 4
access-class 10 in
exec-timeout 5 0
password 7 09581B031200032F064G173W2E25
login local
```

* access-class 대신 각각의 인터페이스에 access-list 이용도 가능

telnet 접근제한(2/2)

-. 라우터의 telnet listener를 disable

```
line vty 0 4
   transport input none
```

-. console에 암호 설정

```
line con 0
   login local                 // console로 접근 시 암호설정
   exec-timeout 2 0            // 2분 동안 키 입력 없을 시 종료
                               // 0은 무제한
```

CatOS 기반 스위치 접근 제한

-. telnet 접근 제어

Switch>(enable)**set ip permit enable**

Switch>(enable)**set ip permit 211.1.1.1 telnet**

-. Snmp 접근 제어

Switch>(enable)**set ip permit 211.1.1.1 snmp**

-. 모든 service를 허용

Switch>(enable)**set ip permit 211.1.1.1 all**

SNMP 설정

1. Default community string 변경
   예: Public → x27swf3
2. SNMP 접근 통제(udp/161)

   snmp-server community x27swf3 ro 11

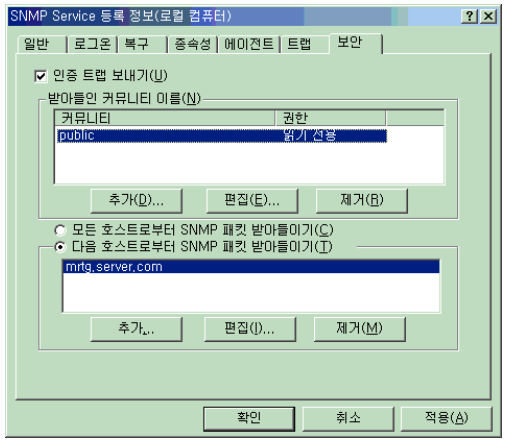
   snmp-server contact antihong@tt.co.kr

   access-list 11 permit host 211.1.2.5

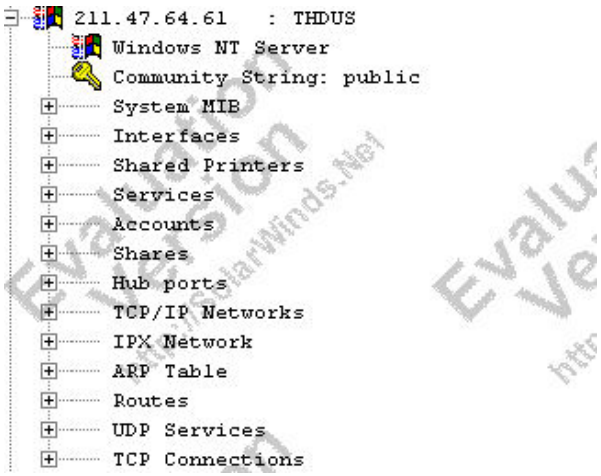
   access-list 11 deny any
3. 사용하지 않는다면 SNMP를 disable 한다.

   no snmp-server
4. 암호화가 지원되는 **v3** 지원 여부 **(mrtg** 지원 **X)**

SNMP 제어 설정



Windows 계열 SNMP 설정



SNMP를 통해 얻을 수 있는 정보

com2sec mynetwork 211.0.0.1 x27swf3

*NIX 계열 snmpd.conf 파일

Snmp brute force 공격

불필요한 서비스 disable

conf t
(config)# **no service udp-small-servers**
(config)# **no service tcp-small-servers**
(config)# **no service finger**
(config)# **no service pad** → x.25 프로토콜에서 사용
(config)# **no ip bootp server**
→ 이 라우터를 통해 부팅가능(네트워크부팅)
(config)# **no ip http server**
(config)# **no tftp-server**
(config)# **no ip source-route**
→ ip spoofing 을 막기 위해 source-route disable
(config)# **no c에 run**

set cdp disable → CatOS 경우

불필요한 서비스 disable

Interface에 설정.

(config)# **int serial0**
(config-if)# **no ip redirects**
(config-if)# **no ip directed-broadcast**
(config-if)# **no ip proxy-arp**

← 양 LAN 세그먼트를 연결해 주는 브리지로 사용시에만 필요

(config-if)# **no ip unreachables**

사용하지 않는 **interface** 는 반드시 **shutdown!!**

(config)# **interface eth0/3**
(config-if)# **shutdown**

Ingress filtering

interface Serial0
ip access-group 101 **in**

access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.0.2.0 0.0.0.255 any
access-list 101 deny ip 169.254.0.0 0.0.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny udp any any eq 1433
access-list 101 deny ip 211.1.1.0 0.0.0.255 any
access-list 101 deny ip 211.1.2.0 0.0.0.255 any
access-list 101 permit ip any any

라우터 내부로 **inbound** 되는 패킷의 소스 **IP** 를 체크해 필터링

최근의 **IP** 할당 내역**:** **http://www.iana.org/assignments/ipv4-address-space**

egress filtering

```
interface Serial0
  ip access-group 110 out

access-list 110 permit ip 211.1.1.0 0.0.0.255 any
access-list 110 permit ip 211.1.2.0 0.0.0.255 any
access-list 110 deny   ip any any log
```

*** log : 매칭되는 패킷을 로그에 남김**
*** log-input : 인터페이스 정보도 함께 남김(increase some CPU load)**

SLOT 5:*May 17 20:06:46: %SEC-6-IPACCESSLOGDP: list 110 denied icmp 10.1.1.2 (GigabitEthernet0) -> 61.182.3.158 (0/0), 2 packets

라우터 외부로 **outgoing** 되는 패킷의 소스 **IP**를 체크해 필터링

Black Hole Filtering

형식)

interface Null0
no ip unreachables
!
ip route <dest to drop> <mask> Null0

예)
interface Null0
no ip unreachables
!
ip route 211.1.1.1 255.255.255.255 Null0

해당 패킷은 라우터 내부로 들어올 수는 있지만 나갈 수는 없다.
→ **ACL**에 비해 맞은 **cpu** 부하율

Switch Filtering

CatOS> (enable) set port security 3/1 enable
CatOS> (enable) set port security 3/1 enable 01-02-03-04-05-06
CatOS> (enable) set port security 3/21 enable age 10 maximum 5
violation shutdown

로그 : 2003 May 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:
Port 3/21 shutdown due to no space

CatOS> (enable) set cam static filter 00-02-03-04-05-06 1
소스나 목적지에 특정한 **MAC** 주소를 포함한 트래픽을 필터링

CatOS> (enable) set port broadcast <mod/port> 0.01%
특정 포트의 **broadcast** 양을 제한하여 **broadcast storm** 을 방지

IP accounting

IP Accounting : 특정 회선 트래픽의 소스,목적지 **IP,**패킷수, 바이트등을 보여줌
performance impact 주의!!!

ROUTER# **conf t**
ROUTER(config)# **int serial0**
ROUTER(config-if)# **ip accounting**
ROUTER(config-if)# **exit**
ROUTER# **sh ip accounting**

Source	Destination	Packets	Bytes
192.168.65.75	210.145.255.74	1	75
192.168.65.103	66.77.73.150	7	6136
192.168.66.35	210.196.133.2	1	109

참고 : http://cipaf.sourceforge.net/ CIPAF

NetFlow

NetFlow

ROUTER# **conf t**
ROUTER(config)# **ip flow-export version 5 peer-as**
ROUTER(config)# **ip flow-export destination 211.0.0.1 2055**
ROUTER(config)# **int serial0**
ROUTER(config-if)# **ip route-cache flow**
ROUTER(config-if)# **exit**
ROUTER# **sh ip cache flow**

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
--------	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-WWW	716	0.0	9	84	0.1	4.1	2.1
TCP-SMTP	71	0.0	30	996	0.0	8.0	3.2
TCP-other	37	0.0	4	70	0.0	3.0	3.8
UDP-DNS	118	0.0	1	63	0.0	1.2	10.1
UDP-other	68	0.0	1	173	0.0	0.3	10.8
ICMP	5	0.0	1	67	0.0	0.0	11.9
Total:	1015	0.0	9	294	0.2	3.7	3.8

NetFlow

src	dest	pr	src port	des port
203.254.149.28	134.111.200.231	06	0401	0089
203.254.149.28	134.111.200.232	06	0402	0089
203.254.149.28	134.111.200.233	06	0403	0089
203.254.149.28	134.111.200.234	06	0404	0089

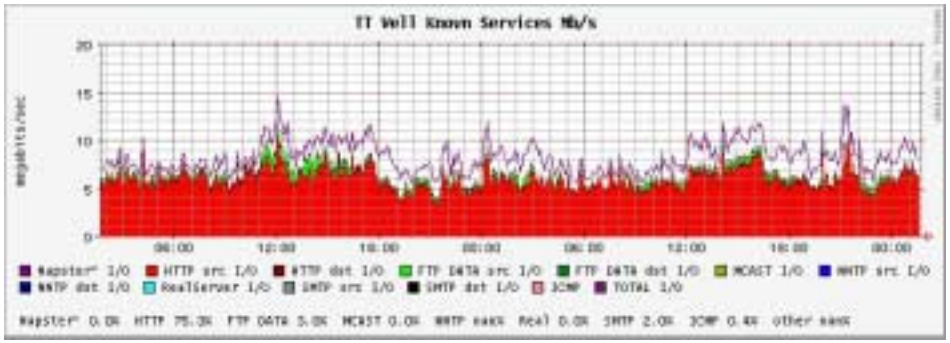
Protocol : 06 = 0*16^1 + 6*16^0 = 6 (**tcp**)

목적지 포트 : 0089 = 16^3*0 + 16^2*0+16^1*8+16^0*9 = 137

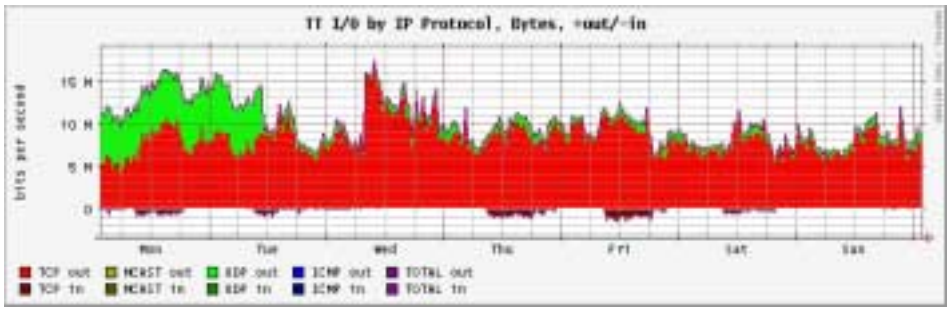
show ip cache flow | include 0089 ← 포트가 137을 포함한 패킷 리스팅

NetFlow 를 이용한 Flowscan

http://moran.kaist.ac.kr/



서비스별 트래픽



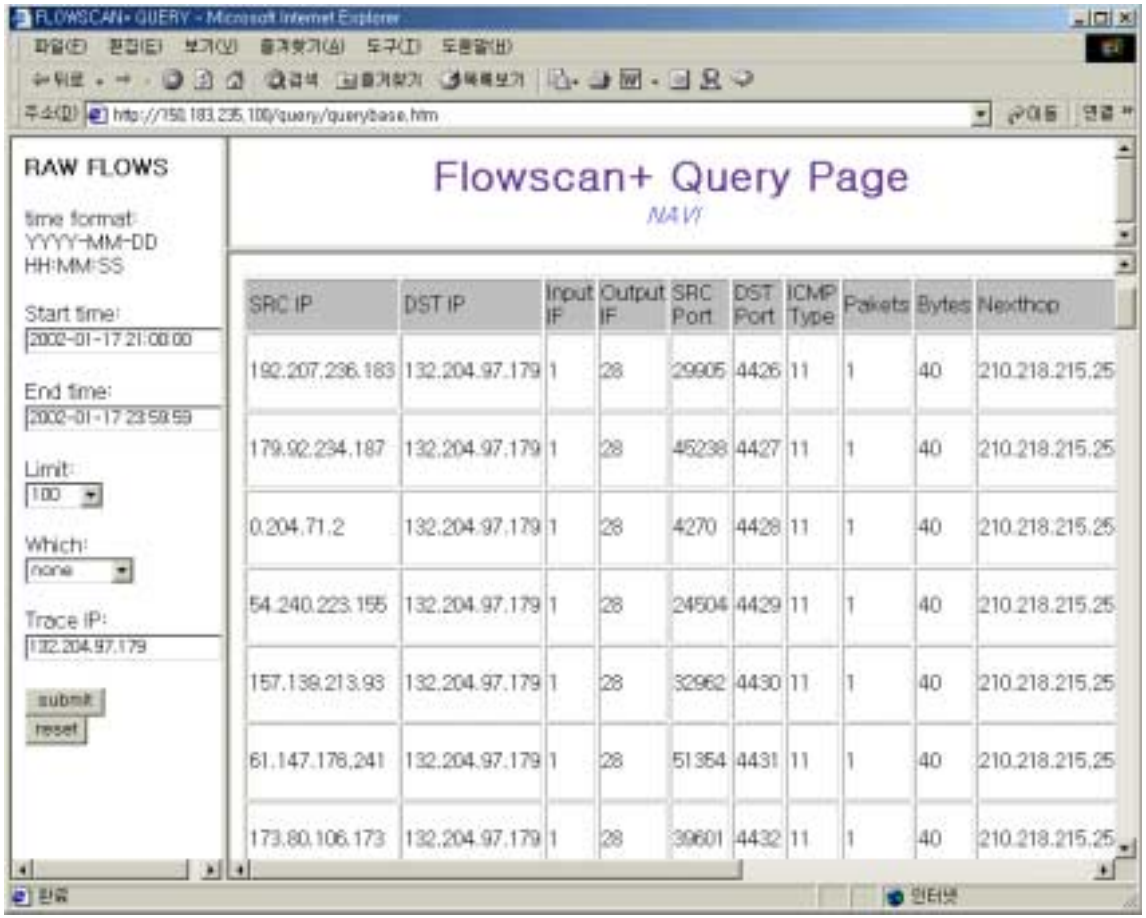
프로토콜별 트래픽

flowscan 을 이용한 문제 추적

```
# flowdumper –s netflow_log_file

2003/04/22 06:25:47 211.47.x.x.27015 -> 213.23.164.95.3364 17 2 317
2003/04/22 06:25:50 211.47.x.x.27015 -> 209.196.48.26.27005 17 1 188
2003/04/22 06:25:55 211.47.x.x.27016 -> 24.175.50.21.1478 17 1 34
2003/04/22 06:25:55 211.47.x.x.27015 -> 68.67.72.151.2213 17 2 68
2003/04/22 06:26:00 211.47.x.x.27015 -> 81.224.104.44.1688 17 2 317
2003/04/22 06:26:02 211.47.x.x.27015 -> 64.81.178.54.27243 17 2 337
2003/04/22 06:26:04 211.47.x.x.27015 -> 24.42.191.135.36549 17 2 317
2003/04/22 06:26:04 211.47.x.x.27015 -> 24.94.62.14.2213 17 1 34
2003/04/22 06:26:07 211.47.x.x.27015 -> 24.226.82.215.1676 17 2 317
2003/04/22 06:26:09 211.47.x.x.27016 -> 80.186.65.119.3299 17 1 34
```

flowscan+ (http://moran.kaist.ac.kr/)



Rate-limit 를 이용한 트래픽 제어(CAR)

** **rate-limit {input | output} bps burst-normal burst-max conform-action action exceed-action action**

burst-normal : 초과 허용 대역폭
burst-max : 초과정책을 적용할 대역폭 한계
conform-action : 한계를 넘지 않을 때 취할 행동으로 단순 패킷 전달(transmit)
exceed-action : 초과시 취할 행동, 패킷 드롭(drop)

통상적으로

burst-normal = (bps/8) * 1.5
burst-normal burst-max = (bps/8) * 2

**** 일반적인 프로토콜별 정상 트래픽 분포**

> TCP : ~90 % (HTTP, FTP and P2P tools)
> UDP : ~10 % (DNS, SNMP, streaming)
> ICMP : <1 %

Rate-limit 를 이용한 트래픽(CAR)적용 예

int serial 0

rate-limit input access-group 150 2000000 250000 250000 conform-action transmit exceed-action drop

rate-limit input access-group 160 512000 8000 8000 conform-action transmit exceed-action drop

rate-limit output access-group 150 2000000 250000 250000 conform-action transmit exceed-action drop

rate-limit output access-group 151 1000000 250000 250000 conform-action transmit exceed-action drop

rate-limit output 19000000 3562500 4750000 conform-action transmit exceed-action drop

access-list 150 permit udp any any

access-list 151 permit ip host 211.0.0.1 any

access-list 160 permit icmp any any echo-reply

효율적인 **Logging** 설정

제공되는 로깅 기법

(1) console logging
(2) Terminal line logging
(3) Buffered logging
(4) snmp trap logging
(5) ACL violation logging
(6) **syslog logging** (best way!!)

Router# config t
(config)# logging trap information
(config)# logging 14.2.9.6
(config)# logging facility local6
(config)# logging source-interface loopback0

/etc/syslog.conf (syslog 서버에서 udp 514 번 open) → udp 514 필터링 주의!!
local6.debug /var/log/routers.log

적용시 주의해야 할 기능

TCP intercept : SYN-Flooding 방어에 효과적.
Performance impact 주의
Unicast RPF(Reverse-Path Forwarding)
: ip spoofing 에 효과적, multi-homed 일 때 적용 주의
NBAR (Network-Based Application Recognition)
: 코드레드,님다등의 Worm에 효과적,Performance impact

Debugging : 패킷 분석,문제해결에 효과적, Performance impact.

Ip accounting/netflow : 대량의 트래픽에서 Performance impact.

SSH : key recovery, CRC32, timing analysis and attacks 등
SSH v1의 취약성에 노출, 최신의 IOS 를 이용.

라우터의 보안사고를 의심시...

show clock detail

show version

show running-config

show startup-config

show reload

show ip route

show ip arp

show users

show logging

show ip interface

show interfaces

show tcp brief all

show ip sockets

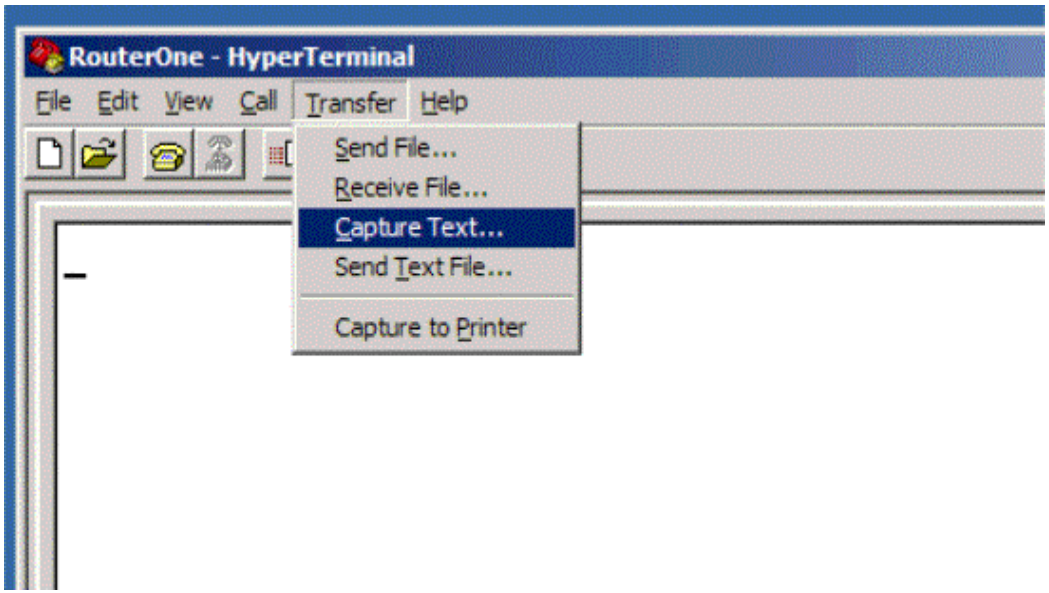
show ip cache flow

show ip cef

show snmp user

show snmp group

show clock detail



메일서버 보안

서버측면 : e-mail server scanner 이용(바이러스 차단)

Inflex(http://pldaniels.com/inflex/) 등.

첨부파일이름/확장자/파일타입/identity등으로 필터링

필터링 시 발송자,관리자에게 메일로 통보

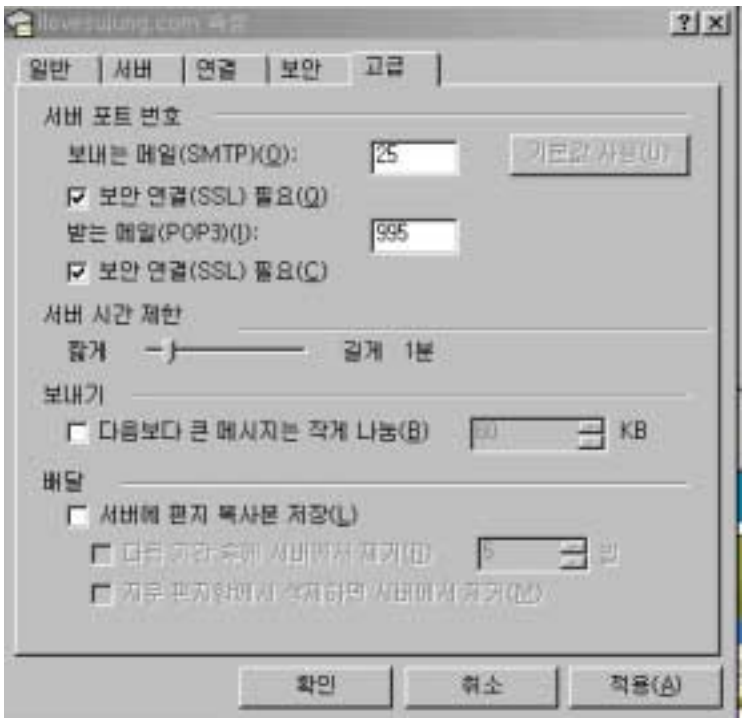
클라이언트 측면 :

pop3 대신 pop3s 이용

smtp대신 smtps 이용

Sslwrap

(http://www.quiltaholic.com/rickk/sslwrap/)

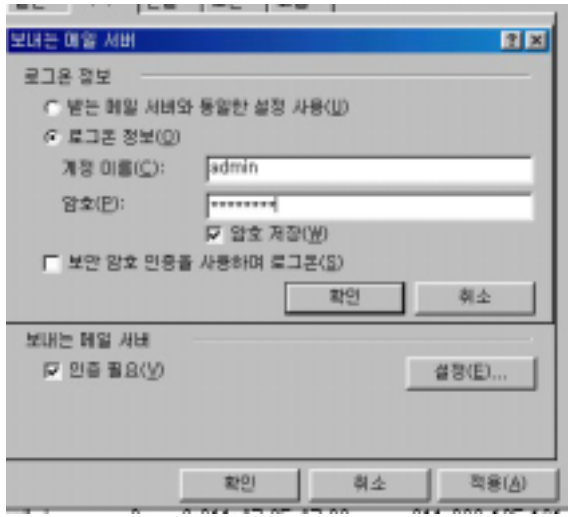


메일서버 보안(relay)

릴레이 허용 방안:

(1) IP 대역을 통한 허용

(2) 사용자 인증을 통한 허용



릴레이 허용 여부 테스트 :

http://www.whchang.com/netprg/is-relay.pl

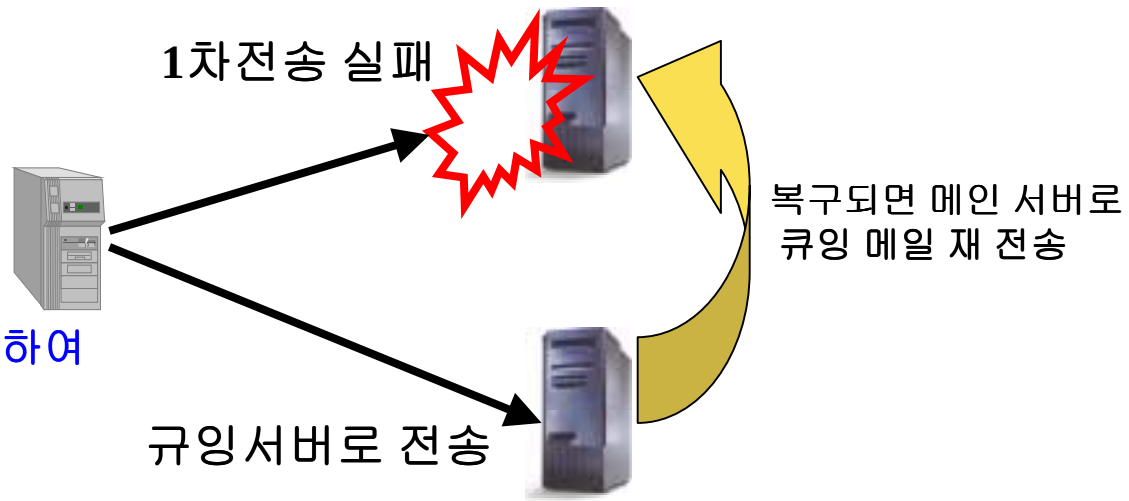
http://www.antispam-ufrj.pads.ufrj.br/test-relay.html

빠른 **relaychecker:** http://david.weekly.org/code/relaycheck.txt

메일서버 보안(큐잉서버 구성)

 # dig @ns1.tt.co.kr tt.co.kr mx

tt.co.kr.	1D IN MX	10 mail-relay.tt.co.kr.
tt.co.kr.	1D IN MX	20 mail-relay2.tt.co.kr.
tt.co.kr.	1D IN MX	30 mail-relay3.tt.co.kr.
tt.co.kr.	1D IN MX	0 www10.tt.co.kr.



큐잉서버는 해당 도메인에 대하여
릴레이를 허용하여야 한다.

DNS 보안(문제점)

dig @ns.domain.com domain.com axfr

```
                    10M IN A      61.33.xx.xx
                    10M IN A      210.207.xx.xx
                    10M IN A      61.33.xx.xx
                    1H IN MX      10 mail
battle              1H IN A       61.33.xx.xx
chaos               1H IN A       61.33.xx.xx
conf                1H IN A       61.251.xx.xx
hades               1H IN A       210.207.xx.xx
hak                 20M IN A      61.33.xx.xx
joon                20M IN A      61.33.xx.xx
```

dig @ns.domain.com txt chaos version.bind | grep VERSION

```
VERSION.BIND.          0S CHAOS TXT    "8.1.2-T3B"
```

DNS 보안(recursion)

```
# nslookup zdnet.co.kr. ns.dacom.co.kr
Server:  ns.dacom.co.kr
Address:  164.124.101.2

Non-authoritative answer:
Name:    zdnet.co.kr
Address:  211.111.220.200
```

```
# nslookup zdnet.co.kr. nis.dacom.co.kr
Server:  nis.dacom.co.kr
Address:  164.124.101.31

Name:    zdnet.co.kr
Served by:
- J.ROOT-SERVERS.NET
        192.58.128.30

- K.ROOT-SERVERS.NET
        193.0.14.129

- L.ROOT-SERVERS.NET
        198.32.64.12

- M.ROOT-SERVERS.NET
        202.12.27.33

- I.ROOT-SERVERS.NET
        192.36.148.17
```

DNS 보안(해결안)

```
options {
        directory "/var/named";
        version “no version";
        allow-transfer {localhost; }; // Zone Transfer를 제한한다.
        allow-recursion {192.168.1.0/24; 192.168.3.4; }; // recursion을 제한
};
```

참고 : udp , tcp 53번의 용도

udp 53 : 일반적인 DNS 질의,전송

tcp 53 : (1) Zone transfer 와 같이 많은 용량을 전송시

(2) udp 53 의 메시지 사이즈가 484 byte 초과시 tcp 로 재질의

웹서버 보안

관리자 페이지 재정리

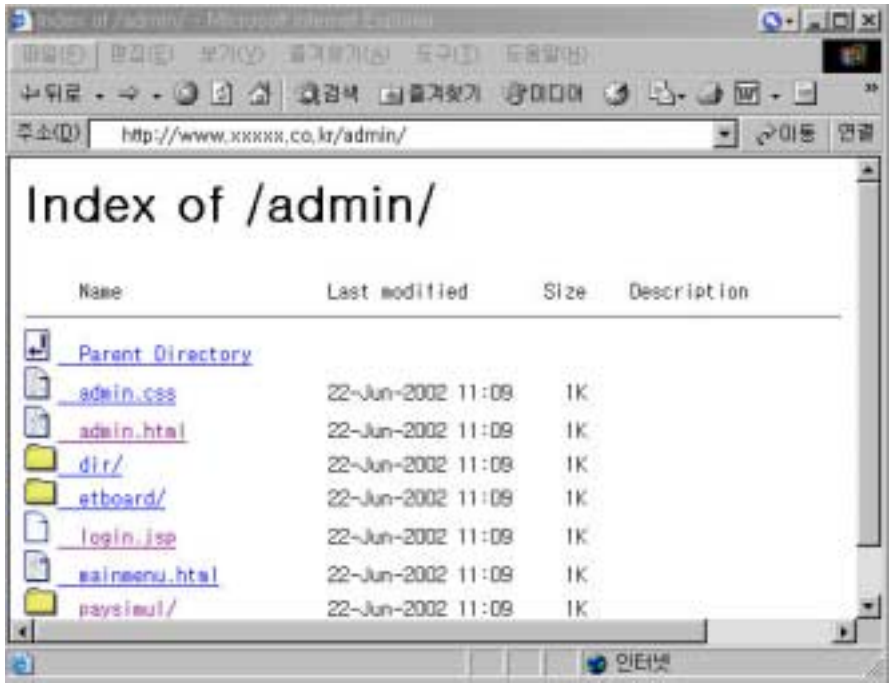
-. id/pw 인증
http://www.xxx.com/admin/
http://admin.xxx.com/

-. 디렉토리 목록 리스팅 주의

-. 관리 사이트는 ip 대역으로 인증

```
<Directory /home/admin/>
        Order deny, allow
        Deny from all
        Allow from 192.168.1
</Directory>
```

-. Non-web file 주의
archive : .tar.gz , .tgz, .zip 등
backup : .bak, .old등
include : .inc 등




```
<Files ~ "\.bak$">
  Order allow,deny
  Deny from all
</Files>
```

→ .bak 에 대한 접근 금지 설정

웹서버 가용성

DNS 기반의 Round-Robin 방식의 문제점

```
www.domain.com.     1M  IN A     211.1.1.1
www.domain.com.     1M  IN A     211.1.1.2
www.domain.com.     1M  IN A     211.1.1.3
```

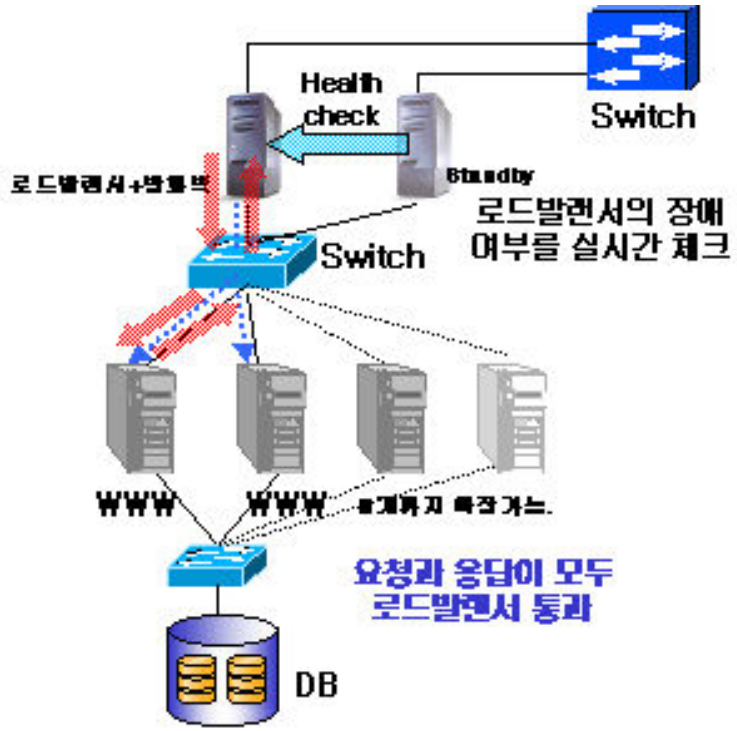
문제점 :

1.서버 다운에 대한 대책 부재

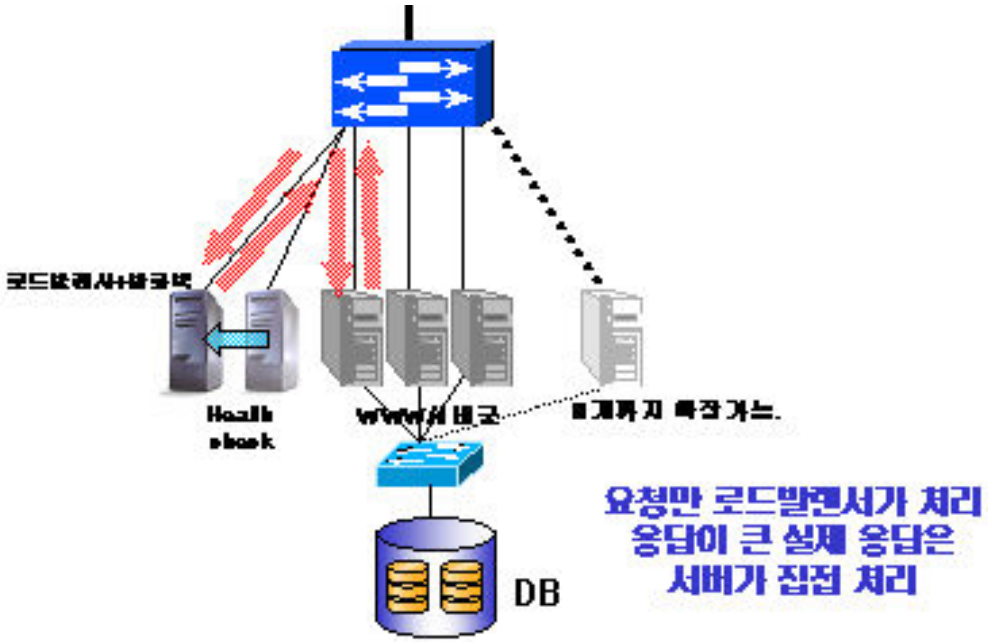
2. 단순 Round Robin 으로 인하여 정확한 부하 분산의 어려움

3. 짧은 Cache Time(TTL) 으로 인한 DNS부하 및 DNS 다운시 접속장애

웹서버 가용성 (로드밸런서 도입)



NAT 방식의 로드발랜서



DR 방식의 로드발랜서

FTP 서버 보안

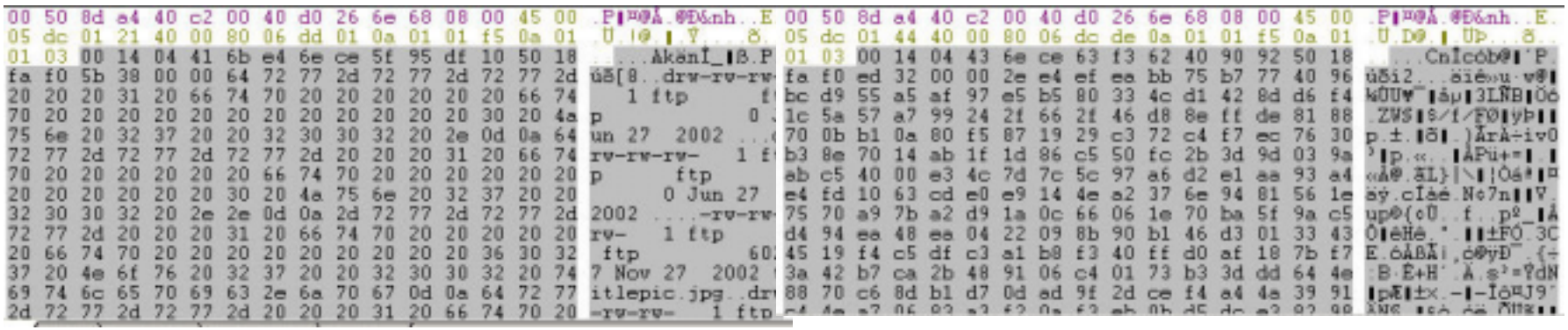
1. 엄격한 접근통제 (anonymous ftp 주의)

   빠른 **anonymous ftpchecker:** http://david.weekly.org/code/ftpcheck.txt

2. SSL 이 지원되는 FTP 이용

   http://www.eftp.org/

   http://www.ipswitch.com



평문전송 예

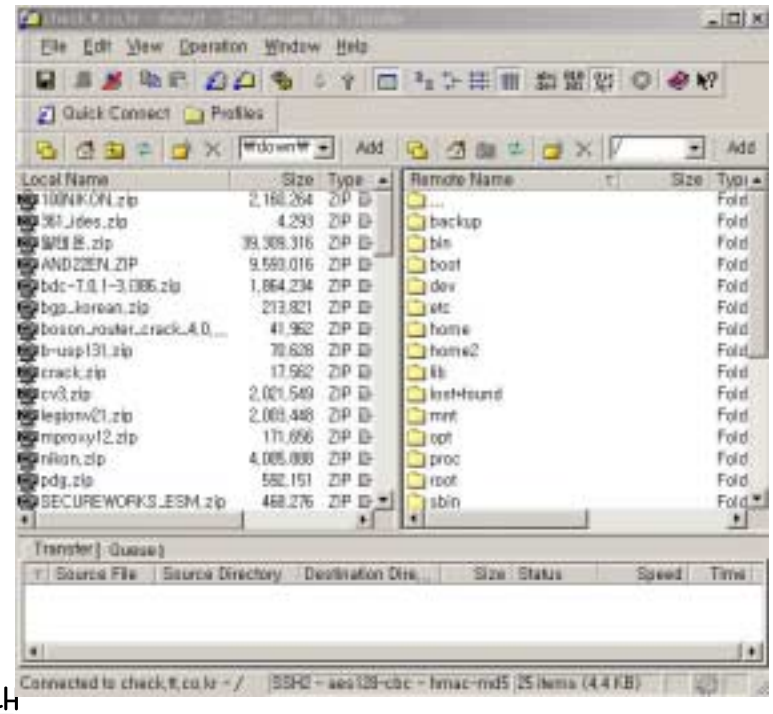
암호화 전송예

FTP 서버 보안

ftp://ftp.ssh.com/pub/ssh/SSHSecureShellClient-3.2.0.exe

-. 유닉스 계열의 경우

-. FTP 대신 SSH 사용



-. SSL/SSH를 지원하는 FTP 프로그램

http://download.zdnet.co.kr/pds/detail_view.html?id=7821

사무실 보안

1. 불필요한 공유 차단

(config)#**access-list 101 deny tcp any any range 135 139**

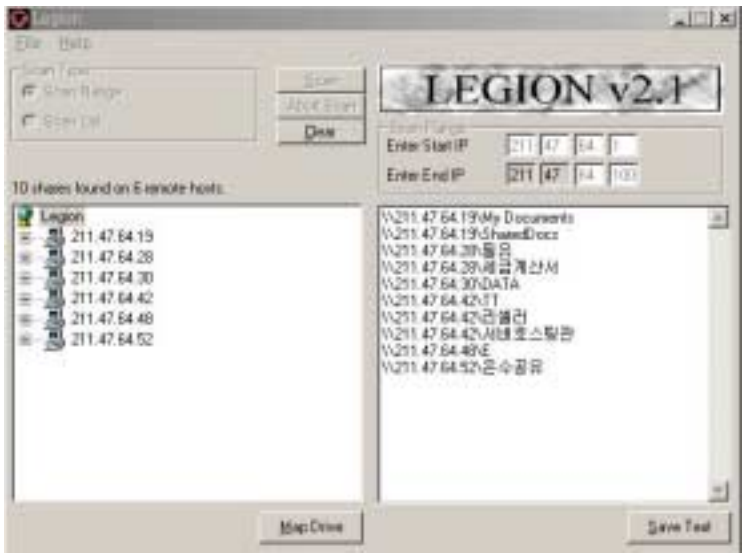
(config)#**access-list 101 deny udp any any range 135 139**

(config)#**access-list 101 deny tcp any any eq 445**

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

(config)#**interface serial0**

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



사무실 보안

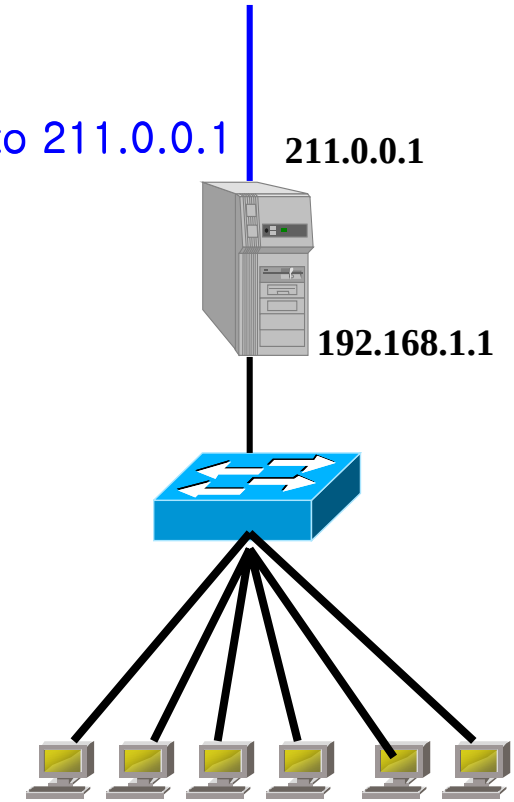
2. 사설 네트워크 구성

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 211.0.0.1

Bridge 방식 파이어월 구축

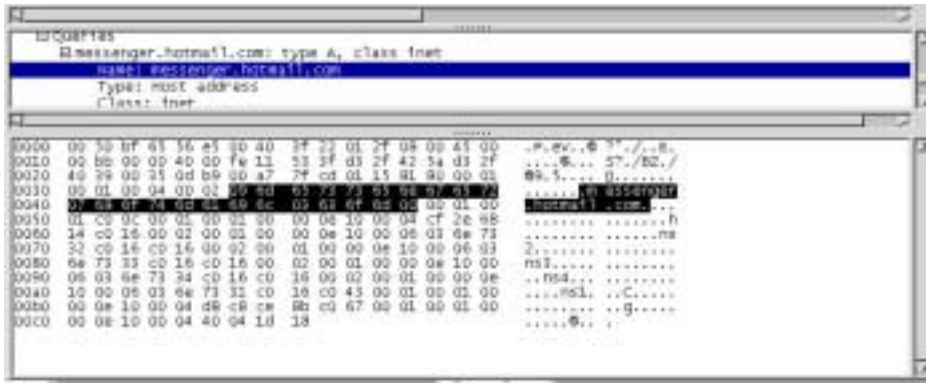
http://bridge.sourceforge.net/



사무실 보안

3. P2P 프로그램 차단방법

(1) 사용하는 포트 차단
msn : 1863
yahoo : 5050
icq : 5190



(2) 사용하는 IP대역(인증서버등) 차단
msn : 64.4.13.0/24
소리바다 : 211.233.14.151

(3) 문자열 차단
analyzer, ethercap 등 패킷 분석 프로그램을 이용한 분석

예) msn 차단예
iptables -A FORWARD -m string -- string "messenger.hotmail.com" -j DROP
예) nate on과 결합된 msn 차단예
iptables -A FORWARD -m string --string "<msn>" -j DROP

감사합니다.

Just because everything is working doesn't mean everything is ok.

질문 : 홍석범(antihong@tt.co.kr)