

이 글은 2001년4월경에 작성된 것입니다. 따라서 현재의 상황과 다른 것이 있을 수 있으며,
교정을 보지 않아 오류가 있을 수 있음을 미리 알려드립니다. 다른 사람들에게 도움이 될
수도 있을 것 같아 제 홈페이지 <http://www.whchang.com>에 등록을 합니다.

Feb 15, 2002

장우현 whchang@whchang.com

WHOIS와 Looking Glass

인터넷의 IP address 혹은 라우팅과 관계된 정보를 얻으려면 WHOIS와 Looking Glass를 잘 이용해야 합니다.

WHOIS는 원래 단어가 의미하듯이 인명정보를 제공해 주는 서비스로 TCP well-known port 43으로 서비스를 제공합니다.

```
$ grep whois /etc/services
whois          43/tcp        nicname
```

그러나 WHOIS는 인명정보를 제공하는 용도로도 쓰이지만, 실질적으로는 다양한 용도로 쓰이고 있습니다. 대표적인 예가 인터넷에서 domain name에 대한 등록 정보를 제공하는 서비스, IP address의 할당정보 서비스, 그리고 어떠한 AS번호를 가지고 라우팅 정보가 전달되는가에 대한 서비스 등의 목적으로 이용되고 있습니다.

Looking Glass는 BGP 라우팅정보와 ping, traceroute 등의 기능을 제공해 주는 서비스를 의미하는 것으로, 그 Looking glass를 이용하여 다양하게 네트워크의 상태나 라우팅 정보 등을 파악할 수 있습니다. Looking Glass는 주요 ISP들마다 개별적으로 서비스되므로 그러한 것들의 목록을 정리해 두면 Looking Glass를 제공하는 ISP 네트워크의 관점에서 라우팅 정보나 네트워크 상태를 파악할 수 있어 매우 큰 도움을 얻을 수 있습니다.

WHOIS 서버

이 글에서 다룰 WHOIS 서버들은 IP address에 대한 정보를 제공한 것, AS번호에 대한 정보를 제공하는 것, BGP 라우팅 정보를 제공하는 것, 그리고 domain name에 대한 정보를 제공하는 것으로 한정하여 설명을 하도록 하겠습니다. 이러한 정보를 제공하는 WHOIS 서버 목록은 다음과 같습니다.

- whois.krnic.net
- whois.apnic.net
- whois.arin.net
- whois.ra.net

WHOIS.KRNIC.NET 은 국내에 할당되는 AS번호, IP address, ISP 연락처, domain name 등에 대한 정보를 제공하는 WHOIS 서버입니다.

KRNIC은 .kr 의 하위 domain name을 신청을 받아 등록을 해주는 기능과, 하위 domain name에 대한 DNS 서버 목록을 유지하는 역할을 담당하고 있습니다. 그리고 IP address를 APNIC으로부터 큰 규모단위(block 단위)로 전달받아 그것을 국내 ISP들에게 할당하는 역할도 함께 하고 있습니다. 또한 BGP 라우팅 운영에 필요한 AS번호도 IP address와 같은 방법으로 APNIC으로부터 일정 영역을

전달받아 국내의 기업에 할당하고 있습니다. 따라서 KRNIC은 이러한 정보들을 다른 사람들이 참조할 수 있도록 KRNIC이 운영하고 있는 WHOIS 서버에 등록을 해 서비스를 제공하고 있습니다. 따라서 국내 인터넷과 관계된 정보를 얻을 때 KRNIC의 WHOIS 서버인 `whois.krnic.net`을 참조하면 많은 도움을 얻을 수 있습니다.

그러나 한 가지 유의할 것은, KRNIC에 등록된 정보들은 100% 신뢰할 수 없다는 것을 알고 있어야 합니다. 그 이유는 관련 정보과 관계된 ISP 혹은 기업, 개인들이 관련 정보가 현재의 실제 상태와 동일하게 유지될 수 있도록 KRNIC에 통보하여 갱신을 요청해야 하나 그렇게 하는 곳들이 많지 않기 때문입니다.

신뢰도가 높은 정보는 domain name이 어느 기업의 것이고, 어느 IP address가 어느 ISP에 의해서 서비스되며, 어느 AS번호가 어느 기관에 할당되었는가에 대한 것들입니다. 반면에 KRNIC WHOIS 서버는 물론 세계에 있는 대부분의 WHOIS 서버들에서 신뢰도가 가장 낮은 정보는 인명정보입니다. 그 이유는 담당자가 일정한 시간이 지나면 변경되는 경우가 많은데 그 정보에 대한 갱신 요청을 거의 하지 않기 때문입니다. 따라서 어떤 IP address로부터 포트스캐닝(port scanning)과 같은 보안침해시도 같은 것이 발생했을 때 그 IP address와 관계된 담당자를 알아내어 연락을 시도할 때 담당자 정보가 갱신되어 있지 않아 연락이 되지 않는 경우가 많습니다. 일반 기업은 물론이고 ISP들도 그런 경우가 많습니다. 따라서 KRNIC WHOIS 서버에 있는 정보를 참고할 때 다른 정보들과 교차점검(cross check)하여 볼 필요가 있습니다.

[주의] 국내의 ISP나 어떤 기업이 사용하는 IP address라도 할지라도 그것에 대한 IP address 정보를 WHOIS.KRNIC.NET에 조회해도 결과가 없는 경우가 있습니다. 그 이유는 각 NIC의 WHOIS 서버는 대개 자신이 직접 할당한 IP address에 대한 정보만을 제공해주기 때문입니다. 대표적으로 국내의 몇몇 ISP는 KRNIC에서 IP address를 할당받지 않고 APNIC에서 직접 할당을 받는데 그 IP address에 대한 정보는 KRNIC에서 조회되지 않습니다. 아래의 예는 데이콤 보라넷에서 이용하는 61.32.0.0/13에 대한 정보를 KRNIC에서 조회했으나 결과가 없고 APNIC에서 조회했을 때 관련정보가 나오는 예입니다.

```
[whchang@home /tmp]$ whois 61.32.0.0@whois.krnic.net
[whois.krnic.net]
```

Korea Internet Information Service V1.0 (created by KRNIC, 1999.6)

query: 61.32.0.0

* 한글 기관명에 대한 whois 조회는 웹(<http://whois.nic.or.kr>)에서 하시기 바랍니다.

조회하신 해당 IP주소는 국내(KRNIC)에 배정된 주소가 아닙니다.

<http://www.apnic.net> (APNIC) 또는 <http://www.arin.net> (ARIN)에서 조회해 주십시오.
(UNIX: `whois -h whois.apnic.net [IP주소]` 또는 `whois -h whois.arin.net [IP주소]`)

* 참고로 전세계 IP주소 배당 절차는 <http://www.nic.or.kr> - "IP주소할당절차"에서 보실 수 있으며, 국내에 배정된 IP주소는 한국인터넷정보센터(KRNIC)가 KRNIC회원

ISP기관(www.nic.or.kr - "국내인터넷서비스제공기관목록" 참조)에게 다시 배정-
할당관리하며 회원 ISP기관은 IP주소를 고객(End-User)에게 할당하고 할당내역을
한국인터넷정보센터에게 통보해 줍니다. 그 통보된 내역으로 Whois 서비스를 제공
하는 것입니다.

- 한국인터넷정보센터 (Korea Network Information Center)
hostmaster@nic.or.kr

```
[whchang@home /tmp]$ whois 61.32.0.0@whois.apnic.net  
[whois3.apnic.net]
```

% Rights restricted by copyright. See <http://www.apnic.net/db/dbcopyright.html>

```
inetnum: 61.32.0.0 - 61.43.255.255  
netname: BORANET-1  
descr: DACOM Corp.  
descr: Facility-based Telecommunication Service Provider  
descr: providing Internet leased-line, on-line service, BLL etc.  
country: KR  
admin-c: DB50-AP  
tech-c: DB50-AP  
mnt-by: APNIC-HM  
mnt-lower: MAINT-KR-DACOM  
changed: hostmaster@apnic.net 20000918  
source: APNIC  
  
role: DACOM BORANET  
address: DACOM Bldg., 706-1, Yoeksam-dong, Kangnam-ku, Seoul  
phone: +82-2-6220-7755  
fax-no: +82-2-6220-0312  
e-mail: ipadm@nic.bora.net  
admin-c: SK91-AP  
tech-c: TH45-AP  
tech-c: CJS3-AP  
tech-c: PHS1-AP  
tech-c: WSH3-AP  
tech-c: HEK1-AP  
nic-hdl: DB50-AP  
remarks: IP address administrator group of NIC team, DACOM Corp.  
notify: ipadm@nic.bora.net  
mnt-by: MAINT-KR-DACOM  
changed: ipadm@nic.bora.net 20001106  
source: APNIC
```

WHOIS.APNIC.NET 은 아태지역에 할당되는 AS번호, IP address 등에 대한 정보를 제공하는 WHOIS 서버입니다. KRNIC은 국내에 할당되는 IP address를 APNIC에서 큰 단위로 받아 국내 ISP나 기업에 재할당하므로, 국내에 할당된 IP address에 대한 정보도 APNIC의 WHOIS서버에서 조회가 가능합니다. 그러나 KRNIC에서 제공하는 정보만큼 상세하지 않고 관련정보가 갱신되어 있지 않은 경우가 있습니다. 아래의 예는 210.124.0.0에 대한 정보를 WHOIS.APNIC.NET과 WHOIS.KRNIC.NET에서 조회한 경우입니다. KRNIC의 WHOIS 서버에서 제공하는

것이 보다 많고 정확합니다.

```
[whchang@home /tmp]$ whois 210.124.0.0@whois.apnic.net  
[whois3.apnic.net]
```

% Rights restricted by copyright.

See <http://www.apnic.net/db/dbcopyright.html>

```
inetnum: 210.124.0.0 - 210.124.255.255  
netname: BORANET  
descr: DACOM CO.  
descr: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku  
descr: Seoul Korea  
descr: 140-013  
country: KR  
admin-c: SJ1-AP  
tech-c: SL11-AP  
remarks: ISP in Korea  
changed: hostmast@rs.krnic.net 980707  
source: APNIC
```

```
person: Sanggyu Jang  
address: DACOM CO.  
address: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku  
address: Seoul Korea  
phone: +82 2 220 5202  
fax-no: +82 2 220 0751  
country: KR  
e-mail: mgr@bora.net  
nic-hdl: SJ1-AP  
mnt-by: MAINT-NULL  
changed: hostmast@rs.krnic.net 19980702  
source: APNIC
```

```
person: Sangjo Lee  
address: DACOM CO.  
address: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku  
address: Seoul Korea  
phone: +82 2 220 5206  
fax-no: +82 2 220 0751  
country: KR  
e-mail: ip@bora.net  
nic-hdl: SL11-AP  
mnt-by: MAINT-NULL  
changed: hostmast@rs.krnic.net 19980702  
source: APNIC
```

```
[whchang@home /tmp]$ whois 210.124.0.0@whois.krnic.net  
[whois.krnic.net]
```

Korea Internet Information Service V1.0 (created by KRNIC, 1999.6)

query: 210.124.0.0

* 한글 기관명에 대한 whois 조회는 웹(<http://whois.nic.or.kr>)에서
하시기 바랍니다.

조회하신 해당 IP주소는 아래의 가입기관에 할당된 블럭입니다.

ENGLISH

IP Address : 210.124.0.0-210.124.1.255
Connect ISP Name : BORANET
Connect Date : 19961110
Registration Date : 20000601
Network Name : BORANETUSERSERIAL

[Organization Information]

Organization ID : ORG91351
Name : DACOM
State : SEOUL
Address : 706-1 Yeoksam-dong Kangnam-gu
Zip Code : 135-610

[Admin Contact Information]

Name : Taeseon Ha
Org Name : DACOM
State : SEOUL
Address : 706-1 Yeoksam-dong Kangnam-gu
Zip Code : 135-610
Phone : +82-2-6220-7755
Fax : +82-2-6220-0312
E-Mail : ipadm@bora.net

[Technical Contact Information]

Name : Taeseon Ha
Org Name : DACOM
Address : 706-1 Yeoksam-dong Kangnam-gu
Zip Code : 135-610
Phone : +82-2-6220-7755
Fax : +82-2-6220-0312
E-Mail : ipadm@bora.net

KOREAN

IP 주소 : 210.124.0.0-210.124.1.255
연결 ISP명 : BORANET
ISP 연결날짜 : 19961110
할당내역 등록일 : 20000601
네트워크 이름 : BORANETUSERSERIAL

[IP 사용 기관 정보]

기관고유번호 : ORG91351
기관명 : 데이콤
시도명 : 서울
주소 : 강남구 역삼동 706-1

WHOIS.ARIN.NET 은 북남미지역에 할당되는 AS번호, IP address 등에 대한 정보를 제공하는 WHOIS 서버입니다. 그리고 대륙별 혹은 국가별 NIC이 없던 시절에 할당된 IP address에 대한 정보도 갖고 있는데, 시간이 많이 경과하여 그런 정보들의 세부 정보가 정확하지 않은 경우가 많습니다. 또한 ARIN은 커다란 IP address 영역을 대륙 혹은 지역별 NIC에 할당하는 역할도 하고 있어 각 IP address 영역이 어떤 NIC에 할당되었는지에 대한 정보도 갖고 있습니다. 따라서 그런 정보들을 근거로 하여 지역별 NIC의 WHOIS 서버에 접근하여 정보를 조회하면 정확한 정보를 얻을 수 있습니다.

아래는 203.248.0.0에 대한 정보를 조회한 것입니다. 결과를 보면 이 영역이 APNIC에 할당되었다는 것을 알 수 있습니다. 그리고 APNIC에서 정보를 조회해 보면 203.248.0.0/17이 INET (현재는 PSINet KR)에 할당되었고 203.248.128.0/17은 데이콤 보라넷에 할당되었다는 것을 알 수 있습니다. 더 상세한 정보는 KRNIC WHOIS 서버에서 조회할 수 있습니다.

```
[whchang@home /tmp]$ whois 203.248.0.0@whois.arin.net
[whois.arin.net]
```

Asia Pacific Network Information Center (APNIC2)

These addresses have been further assigned to Asia-Pacific users.
Contact information can be found in the APNIC database,
at WHOIS.APNIC.NET or <http://www.apnic.net/>
Please do not send spam complaints to APNIC.

Netname: APNIC-CIDR-BLK

Netblock: 202.0.0.0 - 203.255.255.255

Maintainer: AP

Coordinator:

Administrator, System (SA90-ARIN) sysadm@APNIC.NET
+61-7-3367-0490

Domain System inverse mapping provided by:

SVC00.APNIC.NET	202.12.28.131
NS.APNIC.NET	203.37.255.97
NS.TELSTRA.NET	203.50.0.137
NS.RIPE.NET	193.0.0.193

Regional Internet Registry for the Asia-Pacific Region.

*** Use whois -h whois.apnic.net <object> ***
*** or see <http://www.apnic.net/db/> for database assistance ***

Record last updated on 18-Jun-1999.

Database last updated on 19-Jan-2001 07:40:06 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related

Information and whois.nic.mil for NIPRNET Information.

```
[whchang@home /tmp]$ whois 203.248.0.0@whois.apnic.net  
[whois3.apnic.net]
```

% Rights restricted by copyright. See <http://www.apnic.net/db/dbcopyright.html>

```
inetnum: 203.248.0.0 - 203.248.127.255  
netname: INET  
descr: Inet INC.  
descr: Inet Bldg., 738-37, Yoksam-dong, Kangnam-gu, Seoul  
descr: 135-080  
country: KR  
admin-c: JR1-AP  
tech-c: SL91-AP  
mnt-by: MNT-KRNIC-AP  
changed: hostmaster@nic.or.kr 20000122  
source: APNIC
```

```
person: Jaejun Ryu  
address: Inet INC.  
address: Inet Bldg., 738-37, Yoksam-dong, Kangnam-gu, Seoul  
address: 135-080  
phone: +82 2 531 7931  
fax-no: +82 2 555 8127  
country: KR  
e-mail: mgr@nuri.net  
nic-hdl: JR1-AP  
mnt-by: MAINT-NULL  
changed: hostmast@rs.krnic.net 19980702  
source: APNIC
```

```
person: Soojeong LEE  
address: Inet INC.  
address: Inet Bldg., 738-37, Yoksam-dong, Kangnam-gu, Seoul  
address: 135-080  
phone: +82-2-531-7932  
fax-no: +82-2-555-8127  
country: KR  
e-mail: ip@nuri.net  
nic-hdl: SL91-AP  
mnt-by: MAINT-NULL  
changed: hostmaster@apnic.net 19990103  
source: APNIC
```

```
[whchang@home /tmp]$ whois 203.248.128.0@whois.apnic.net  
[whois3.apnic.net]
```

% Rights restricted by copyright. See <http://www.apnic.net/db/dbcopyright.html>

```
inetnum: 203.248.128.0 - 203.248.255.255  
netname: BORANET  
descr: DACOM CO.
```

descr: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku
descr: Seoul Korea
descr: 140-013
country: KR
admin-c: SJ1-AP
tech-c: SL11-AP
remarks: ISP in Korea
changed: hostmast@rs.krnic.net 980707
source: APNIC

person: Sanggyu Jang
address: DACOM CO.
address: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku
address: Seoul Korea
phone: +82 2 220 5202
fax-no: +82 2 220 0751
country: KR
e-mail: mgr@bora.net
nic-hdl: SJ1-AP
mnt-by: MAINT-NULL
changed: hostmast@rs.krnic.net 19980702
source: APNIC

person: Sangjo Lee
address: DACOM CO.
address: Sungji Bldg. 40-712 3-Ga Hangnag-Ro Yongsan-Ku
address: Seoul Korea
phone: +82 2 220 5206
fax-no: +82 2 220 0751
country: KR
e-mail: ip@bora.net
nic-hdl: SL11-AP
mnt-by: MAINT-NULL
changed: hostmast@rs.krnic.net 19980702
source: APNIC

WHOIS.RA.NET 은 인터넷 라우팅을 담당하는 사람이라면 꼭 알아야 할 WHOIS 서버 중의 하나입니다. WHOIS.RA.NET에는 인터넷 라우팅 정보에서 볼 수 있는 IP Network address 정보, AS번호 정보가 등록되어 있습니다. IP Network address 정보는 BGP 라우팅정보에서 볼 수 있는 영역단위(블록단위)로 등록이 되어 있으며, 그 IP Network address 정보가 어떤 AS번호에서 사용되고 있는가에 대한 정보도 제공합니다. WHOIS.RA.NET에서 제공되는 정보를 잘 이해하기 위해서는 BGP 라우팅을 알아야 합니다만 해당 address가 어떤 AS번호에서 이용되고 있는가에 대한 정보만으로도 우리들은 많은 도움을 얻을 수 있습니다. 그리고 WHOIS.RA.NET의 정보와 Looking-glass를 통해 얻을 수 있는 정보를 조합하면 보다 정확한 정보를 얻을 수 있습니다. 그러나 주의할 것은 어떤 NIC의 서버나 제공되는 정보들이 모두 정확하지는 않다는 것입니다.

앞에서 설명한 NIC들의 WHOIS 서버는 NIC이 운영하나 WHOIS.RA.NET 서버는 NIC에서 운영하지 않습니다. WHOIS.RA.NET은 Merit에서 운영을 하며, WHOIS.RA.NET의 운영목적은 BGP 라우팅과 관계된 정보를 제공하기 위해서입니다.

다. WHOIS.RA.NET에 등록된 정보들은 실제 미국내 중요 인터넷교환점(IX 혹은 NAP)에서 운영되고 있는 ROUTE SERVER의 운영정보에 반영되는 것들입니다.

WHOIS.RA.NET을 이용해 다양한 방법으로 활용할 수 있습니다만, 여기에서는 어떤 IP address가 어느 ISP에 의해 서비스 되는지를 알아내는 것을 설명해 보도록 하겠습니다.

가령 192.132.247.0에 포함된 IP address에서 내 서버에 불법적인 접근을 시도했다고 가정해 보시기 바랍니다. 그 경우 192.132.247.0가 어디에 있는 것인지부터 확인해야 합니다. 192.132.247.0에 대한 정보를 whois.krnic.net, whois.apnic.net에 조회를 하면 등록되어 있지 않다는 결과를 받게 되며, whois.arin.net에 조회를 하면 192.132.247.0는 충남대에 할당이 된 것이며, 연락처가 Steve Jones이고, 해당 정보는 1992년에 마지막으로 수정되었다는 것을 보게 됩니다.

```
[whchang@home whchang]$ whois 192.132.247.0@whois.arin.net
[whois.arin.net]
ChungNam National University (NET-CNU-NET1)
  220 Kung-Dong, Youseong-Ku, Taejeon 305-764, KOREA

Netname: CNU-NET1
Netblock: 192.132.247.0 - 192.132.247.255

Coordinator:
  Jones, Steve (SJ104-ARIN) sjones@CORTECH.COM
  303-657-8020

Record last updated on 29-Jan-1992.
Database last updated on 19-Jan-2001 19:30:25 EDT.
```

The ARIN Registration Services Host contains ONLY Internet Network Information: Networks, ASN's, and related POC's. Please use the whois server at rs.internic.net for DOMAIN related Information and whois.nic.mil for NIPRNET Information.

위 정보는 192.132.247.0이 충남대에 할당되었다는 것을 제외하고 나머지는 모두 부정확한 정보입니다. 이런 경우 대개 이런 기업/학교 (여기에서는 충남대)에게 인터넷서비스를 제공해 주는 ISP에게 연락을 할 수 밖에 없습니다. 이럴 때 WHOIS.RA.NET을 활용할 수 있습니다. WHOIS.RA.NET에 IP Network address에 대해 정보를 조회하는 방법은 NIC의 WHOIS 서버에게 조회하는 방법과 동일합니다.

```
[whchang@network ~]$ whois 192.132.247.0@whois.ra.net
[whois.radb.net]
route: 192.132.247.0/24
descr: contact noc@bora.net if necessary
origin: AS3786
mnt-by: MAINT-AS3786
changed: ysjeon7@bora.net 20000410
source: RADB
```

```
route:      192.132.247.0/24
descr:      KORnet operation Center
origin:     AS4766
mnt-by:     MAINT-AS4766
changed:    jyoungk@streamwk.kix.net 20000415
source:     RADB
```

```
route:      192.132.247.0/24
descr:      KORnet operation Center(Korea Telecom)
origin:     AS4766
mnt-by:     ASN-KOREA-TELECOM
changed:    jyoungk@streamwk.kix.net 20000414
source:     CW
```

192.132.247.0에 대한 조회결과가 3개가 나왔습니다. 각각을 route object라고 말하며, 여기에서는 3개의 route object가 출력되었습니다. 그 이유는 **192.132.247.0**에 대한 정보를 여러 곳에서 등록하는 경우(이 예에서는 데이콤 보라넷과 한국통신 코넷에서 등록함)도 있고, 등록하는 방법을 잘 몰라 중복해서 등록하는 경우(이 예에서는 코넷에서 CW에만 등록하면 되는데 RADB에도 등록했음), 혹은 필요없는 것을 지우지 않아서 발생하는 경우도 있습니다.

Route object에서 주의 깊게 보아야 할 부분은 route: 필드와 origin: 필드입니다. 즉 어떤 IP network address가 어떤 ISP에 의해서 서비스되는가는 origin: 필드를 보면 됩니다. **192.132.247.0**에 대해서는 origin이 AS3786과 AS4766으로 나타나며 AS3786은 데이콤 보라넷의 AS번호, AS4766은 한국통신 코넷의 AS번호입니다. 실제로, 뒤에 설명할 Looking-glass를 활용하면 **192.132.247.0**가 보라넷에 접속되어 있는지 코넷에 접속되어 서비스되고 있는지 보다 정확히 확인할 수 있습니다. 확인 결과 **192.132.247.0**는 보라넷과 코넷에 모두 접속이 되어 있습니다 (2001/1/20 기준).

그리고 각 ISP의 연락처는 maint-by: 필드에 나타난 것을 WHOIS.RA.NET에서 다시 검색하면 알아낼 수 있습니다. 아래는 MAINT-AS3786, MAINT-AS4766, ASN-KOREA-TELECOM 모두에 대해 조회한 결과입니다.

```
[whchang@network ~]$ whois MAINT-AS3786@whois.ra.net
[whois.radb.net]
mntner:     MAINT-AS3786
descr:      Maintainer for AS 3786
admin-c:    Raejoon Jung
admin-c:    Jin-seob Park
admin-c:    Youngseo Jeon
upd-to:     peering@bora.net
upd-to:     ipeng@bora.net
auth:       CRYPT-PW BZCdKw4N6cKOs
mnt-by:     MAINT-AS3786
changed:    ysjeon7@bora.net 20000701
source:     RADB
```

```
[whchang@network ~]$ whois MAINT-AS4766@whois.ra.net
[whois.radb.net]
```

mntner: MAINT-AS4766
descr: Maintainer for AS 4766
KORNET NOC Powered By Korea Telecom.
Seoul Korea
admin-c: Kwangsuk Cho
tech-c: Won Kang
tech-c: Junyoung Kwon
upd-to: noc@kornet.net
mnt-nfy: noc@kornet.net
auth: MAIL-FROM kscho@streamwk.kix.net
auth: MAIL-FROM pioneer@streamwk.kix.net
auth: MAIL-FROM jyoungk@streamwk.kix.net
auth: MAIL-FROM hongji@streamwk.kix.net
auth: MAIL-FROM chiyh@soback.kornet.net
remarks: KOREA Telecom IP Sevice Division
notify: nets@soback.kornet.net
mnt-by: MAINT-AS4766
changed: db-admin@radb.net 20010102
source: RADB

[whchang@network ~]\$ **whois ASN-KOREA-TELECOM@whois.ra.net**
[whois.radb.net]

mntner: ASN-KOREA-TELECOM
descr: AS4766/KOREA-TELECOM
admin-c: Kwangsuk Cho
tech-c: Junyoung Kwon
upd-to: kscho@streamwk.kix.net
mnt-nfy: nets@soback.kornet.net
auth: MAIL-FROM kscho@streamwk.kix.net
auth: MAIL-FROM jyoungk@streamwk.kix.net
auth: MAIL-FROM pioneer@streamwk.kix.net
auth: MAIL-FROM hongji@streamwk.kix.net
auth: MAIL-FROM chiyh@soback.kornet.net
notify: nets@soback.kornet.net
mnt-by: ASN-KOREA-TELECOM
changed: kscho@streamwk.kix.net 20010102
source: CW

Looking-glass

Looking-glass라는 것은 인터넷의 라우팅정보나 네트워크상태를 정보를 제공하는 서버를 말합니다. 우리들은 그것을 웹브라우저를 이용해 접속해 이용할 수도 있고 telnet 을 이용해 접속해 이용할 수도 있습니다. Looking-glass를 설명하는 이유는 인터넷의 라우팅 정보 혹은 네트워크상태를 ping, traceroute, whois server 그리고 이들과 Looking-glass를 이용하면 보다 정확하게 파악하고 이해할 수 있기 때문입니다.

Looking-glass는 일반적으로 다음과 같은 것들을 기본적으로 제공하는데 필자가 주로 이용하는 것은 bgp, ping, trace 입니다.

- bgp
- dampened-paths
- ping
- trace

그러나, 일반적인 Looking-glass는 위와 같은 것들을 일반적으로 제공하지만, traceroute (혹은 trace), ping 중 어느 1가지 기능만을 제공하는 서버들도 있습니다. 이것들은 보통 traceroute 서버, ping 서버라고 하는데 필자는 이런 것들도 Looking-glass의 범주에 넣고 이곳에서 설명을 하려고 합니다. 그 이유는 그런 서버들도 내 입장이 아니라, 그 서버가 위치한 곳의 입장에서 내가 있는 곳까지의 네트워크상태나 다른 목적지까지의 네트워크 상태 및 기타 정보를 제공하는 동일한 역할을 하기 때문입니다. 다만 ping 서버, traceroute 서버에서는 bgp 라우팅 정보를 확인할 수 없습니다.

Looking-glass 서버를 이용하려면 우선 Looking-glass 서버가 어디에 있는지 알아야 합니다. Looking-glass 서버에 대한 URL을 알아내는 방법은 웹검색엔진 등에서 검색을 하는 방법도 있지만, Looking-glass 서버들의 목록을 정리해 놓은 서버를 알아두면 편리합니다. 그 목록에는 대부분 국가별/ISP별로 정리가 되어 있습니다. 필자가 원하는 그러한 목록을 가진 서버에 대한 URL을 다음의 순서와 같습니다.

- <http://www.traceroute.org/>
- <http://www.above.net/html/traceroute.html>
- <http://labcerro.addr.com/BW/>
- <http://neptune.dti.ad.jp/>

특히 <http://www.traceroute.org/>는 traceroute 서버와 looking-glass 서버, route 서버에 대한 목록도 함께 제공하고 있습니다. 따라서 기억해 두면 좋습니다.

국내의 Looking-glass 서버

국내의 Looking-glass 서버는 현재(2001년1월 기준) 많지 않은 상태입니다. 필자는 그 이유를 Looking-glass 서버에 대한 인식 부족도 하나의 원인이지만,

더 큰 이유는 인터넷서비스를 제공하는 사업자(ISP)가 자기 네트워크의 상태를 보여주길 꺼려하기 때문이라고 생각을 하고 있습니다. Looking-glass를 통해 네트워크의 중요정보는 보여 주지 않는다고 하더라도 네트워크의 상태를 제3자가 어느 정도 파악을 할 수 있기 때문에 자기 네트워크의 상태에 대해 자신이 없는 ISP는 Looking-glass를 제공하려고 하지 않습니다. 그러나 다행스럽게도 국내 ISP에서 큰 축을 이루고 있는 한국통신 및 데이콤은 Looking-glass 서버를 제공하고 있습니다. 2000년말까지만 교육전산망(KREN)에서도 Looking-glass 서버를 제공했습니다만, 현재 제공되지 않고 있습니다.

- 한국통신 KORNET Looking-glass (<http://kix.net/looking-glass/>)
- 데이콤 BORANet Looking-glass (<http://looking-glass.bora.net/>)

해외의 Looking-glass 서버

Looking-glass의 서버를 이용할 때 자주 이용하게 되는 서버는 일반적으로 중요 ISP의 것이거나, 다른 ISP들과 연결이 많이 되어 있는 기업의 것입니다. 따라서 중요 ISP의 Looking-glass나 IX에 있는 Looking-glass 서버를 알아두면 좋습니다. 그리고 주요 국가별로 1개씩은 기억해 두는 것이 좋습니다. 기억해 둘만한 것들은 다음과 같은 것들이 있습니다.

- Abovenet (<http://lg.above.net/>)
미국 및 전세계 주요 NAP에 있는 정보를 볼 수 있음.
- Intermedia DIGEX (<http://nitrous.digex.net/>)
미국내 중요 NAP에 있는 정보를 제공. 국내 많은 네트워크들이 이용하고 있음.
- Oregon Exchange (<telnet://route-views.oregon-ix.net>)
- CERFNet (<telnet://route-server.cerf.net>)
- Genuity AS1 Route Monitor (<telnet://ner-routes.bbnplanet.net>)
- Exodus Communications (<telnet://route-server.exodus.net>)
Exodus사에서 제공하는 것으로 미국내 정보를 볼 수 있음.
- Exodus Communications (<telnet://route-server-eu.exodus.net>)
Exodus사에서 제공하는 것으로 유럽지역의 정보를 볼 수 있음.
- Global Crossing (<telnet://route-server.gblx.net>)
- EBONE (<http://www.ebone.net/looking-glass/>)
유럽의 네트워크에 대한 정보를 파악할 수 있음.
- Dream Train Internet (<http://neptune.dti.ad.jp/ixp2-lg.html>)
일본의 네트워크에 대한 정보를 파악할 수 있음.

Looking-glass를 활용하는 방법

Looking-glass는 다음과 같은 때 활용할 수 있습니다.

- 되돌아 오는 경로(return path)를 파악할 때
- 경로의 상태(delay, error 등)를 파악할 때
- 특정한 IP address에 대한 경로가 차단되어 있는지 확인할 때
- 최적경로(best path)가 어떤 것이 선택되는지 파악할 때

- 자신의 네트워크 정보가 Looking-glass 서버를 제공하는 사업자까지 전달되는지 확인할 때
- 어떤 네트워크정보가 BGP에 의해 차단되어 있는지 파악할 때 (dampened-paths)

되돌아 오는 경로 파악

traceroute를 설명할 때 traceroute는 목적지까지 가는 경로에 대한 정보를 제공할 뿐이지, 되돌아 오는 경로에 대한 정보를 제공하지 않는다고 설명했었습니다. 특히 인터넷에서 여러 ISP들을 거쳐가야만 하는 목적지인 경우 그런 확률은 더욱 높습니다. 한가지 예를 들어 설명해 보도록 하겠습니다.

Source address와 destination address가 아래와 같은 경우

```
Source address 210.207.9.166 (anyaba9-s10-1-2-c.rt.bora.net)
Destination address 203.181.71.196 (neptune.dti.ad.jp)
```

Source에서 destination 까지 traceroute를 해보면 나오는 결과는 다음과 같습니다.

```
router#trace neptune.dti.ad.jp

Type escape sequence to abort.
Tracing the route to neptune.dti.ad.jp (203.181.71.196)

 0 210.207.9.166 [M] 0 msec 0 msec 0 msec
 1 anyaba9-s10-1-2.rt.bora.net (210.207.9.165) 8 msec 8 msec 4 msec
 2 anybbb185-fe6-0-0.rt.bora.net (210.120.193.4) 8 msec 4 msec 4 msec
 3 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 8 msec 4 msec 8 msec
 4 ysng12bb1-pos8-0.rt.bora.net (210.120.192.113) 4 msec 4 msec 4 msec
 5 210.120.192.4 8 msec 4 msec 8 msec
 6 158.205.226.57 60 msec 60 msec 60 msec
 7 FastEthernet9-1-0.tok2.idc.ad.jp (158.205.224.185) 64 msec 60 msec 60 msec
 8 POS1-1.tokgl.idc.ad.jp (158.205.224.237) 60 msec 64 msec 60 msec
 9 POS1-0-0.otml.idc.ad.jp (158.205.224.78) 60 msec 64 msec 60 msec
10 DTI-main.DTI.idc.ad.jp (158.205.227.10) 144 msec 148 msec 148 msec
11 core1.otemachi.dti.ad.jp (203.181.69.1) 164 msec 168 msec 168 msec
12 atm-otemachi-gate-1.akasaka.dti.ad.jp (202.216.225.221) 152 msec 156 msec 148 msec
13 plan.akasaka.dti.ad.jp (210.170.128.27) 152 msec 148 msec 152 msec
14 neptune.dti.ad.jp (203.181.71.196) 148 msec 148 msec 152 msec
router#
```

우리는 결과에서 데이콤 보라넷을 경유한 후 일본의 IDC를 경유하고 다음에 DTI의 네트워크를 경유하여 목적지인 neptune.dti.ad.jp까지 도달하는 것을 볼 수 있습니다. 그런데 한 가지 의문을 가질 수 있는 것은 RTT입니다. 일반적으로 국내와 일본간에 통신을 할 때 가는 경로와 되돌아 오는 경로가 동일할 경우 delay(RTT)는 100msec 이내입니다. 그러나 위 결과에서는 150msec입니다. 만약 DTI 네트워크에서 발생하는 지연 때문이라고 생각할 수 있습니다만 우리는 그것 즉, 되돌아 오는 경로를 확인해 보아야 할 필요가 있습니다.

되돌아 오는 경로를 파악하기 위해서는 목적지(Destination address)가 있는 네트워크에 Looking-glass가 있어야 합니다. 만약 Looking-glass가 그곳에 없다면 목적지 이전의 ISP (위에서는 일본의 IDC)의 Looking-glass에서 확인을

간접적으로 할 수 있습니다만 정확하지는 않습니다. 위의 예에서도 실제 확인을 해보면 DTI에서 source로 되돌아 오는 경로와 IDC에서 source로 되돌아 오는 경로는 틀립니다. 따라서 위 예에서는 반드시 DTI에 있는 looking-glass를 이용해야 되돌아오는 경로를 정확히 파악할 수 있습니다. 만약 DTI에 looking-glass가 없다면 DTI에 전화를 걸어 되돌아 오는 경로를 파악할 수 밖에 없습니다.

그러나 다행스럽게도 DTI에서는 Looking-glass를 제공하므로 그것을 이용하면 됩니다. DTI의 looking-glass 서버의 URL은

<http://neptune.dti.ad.jp/ixp2-lg.html>

입니다. 그곳에서 Query는 trace, address는 source인 210.207.9.166로 지정을 하고 Submit 버튼을 누릅니다. 그러면 잠시 후 결과와 나오는데 그 결과는 아래와 같습니다. 한가지 주의할 점은 아래 결과가 지금 글을 쓰고 있는 현재 시점(2001-1-27)과 독자가 보는 시점에 서로 다를 수 있다는 것이며, 그 이유는 DTI의 BGP 라우팅 정책에 의해 210.207.9.166로 오는 최적경로(best path)가 변경될 수 있기 때문입니다.

DTI Looking Glass Results

Query: trace

Addr: 210.207.9.166

traceroute 210.207.9.166

Type escape sequence to abort.

Tracing the route to anyaba9-s10-1-2-c.rt.bora.net (210.207.9.166)

```
1 above-dti.nrt.above.net (208.185.175.169) [AS 6461] 0 msec 0 msec 0 msec
2 seal-nrt2-stml.seal.above.net (208.185.175.85) [AS 6461] 100 msec 84 msec 84 msec
3 core3-core1-oc48.seal.above.net (208.185.175.182) [AS 6461] 84 msec 84 msec 88 msec
4 sjc2-seal-oc48-2.sjc2.above.net (208.184.102.177) [AS 6461] 100 msec 100 msec 104 msec
5 paol-sjc2-oc48-2.paol.above.net (208.185.175.162) [AS 6461] 100 msec 104 msec 100 msec
6 core1-core2-oc48.paol.above.net (208.185.175.141) [AS 6461] 104 msec 100 msec 104 msec
7 abovenet.paix.bora.net (209.133.31.36) [AS 6461] 100 msec 104 msec 104 msec
8 p4.bora.net (203.255.234.44) [AS 3786] 100 msec 100 msec 104 msec
9 gw1.bora.net (203.255.234.181) [AS 3786] 268 msec 268 msec 268 msec
10 ysng12bb1-ge2-0.rt.bora.net (210.120.192.131) [AS 3786] 244 msec
    ysng12bb1-ge3-0.rt.bora.net (210.120.192.1) [AS 3786] 248 msec 244 msec
11 anyg12bb1-pos8-0.rt.bora.net (210.120.192.114) [AS 3786] 248 msec
    anyg12bb2-pos8-0.rt.bora.net (210.120.192.118) [AS 3786] 248 msec
    anyg12bb1-pos8-0.rt.bora.net (210.120.192.114) [AS 3786] 244 msec
12 anybbb185-p1.rt.bora.net (210.120.193.137) [AS 3786] 248 msec 272 msec
    anybbb185-ge1-0-0.rt.bora.net (210.120.193.147) [AS 3786] 360 msec
13 anyaba9.rt.bora.net (210.120.193.9) [AS 3786] 248 msec 248 msec 248 msec
14 anyaba9-s10-1-2-c.rt.bora.net (210.207.9.166) [AS 3786] 252 msec * 252 msec
```

결과를 보면 DTI에서는 source 210.207.9.166로 올 때 미국의 Abovenet을 거쳐 데이콤 보라넷을 경유해 오는 것을 알 수 있습니다. 국내와 미국간 delay(RTT)는 120msec에서 200msec 사이이며, 일본과 미국간도 마찬가지로입니

다. 위 결과를 보고 결론 지을 수 있는 것은 Source 210.207.9.166에서 Destination 203.181.71.196간에는 비대칭(Asymmetric Routing) 형태로 경로가 구성되며, source로 되돌아 올 때 미국을 경유하므로 delay(RTT)가 100msec 이상이 발생한다는 것입니다. 또한 한가지 더 확정적으로 유추할 수 있는 것은 IDC에서 source 210.207.9.166로 올 때 미국을 경유하지 않는다는 사실입니다. 그 이유는 source 210.207.9.166에서 IDC에 있는 임의의 목적지 POS1-1.tokg1.idc.ad.jp (158.205.224.237)에 대해 RTT가 60msec 이며, 미국을 경유한다면 100msec 이하의 delay (RTT)는 발생할 수 없기 때문입니다.

비대칭 형태로 경로가 설정되는 또 다른 예는 아래와 같습니다. Source에서는 destination으로 갈 때 데이콤 보라넷을 경유, 한국통신 코넷을 경유합니다. Destination에서 source로 되돌아올 때는 데이콤 보라넷을 경유하지 않습니다.

```
Source address      210.182.173.129
Destination address 168.126.3.3(soback.kornet21.net)
```

아래 결과는 Source에서 destination으로 traceroute를 한 결과입니다.

```
router#tr
Protocol [ip]:
Target IP address: soback.kornet21.net
Source address: 210.182.173.129
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to soback.kornet21.net (168.126.3.3)

 0  1 anyaba9-s10-1-2.rt.bora.net (210.207.9.165)  4 msec 8 msec 8 msec
 1  2 anybbb185-fe6-0-0.rt.bora.net (210.120.193.4)  4 msec 8 msec 8 msec
 2  3 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135)  4 msec 4 msec 8 msec
 3  4 ysng12bb1-pos8-0.rt.bora.net (210.120.192.113)  8 msec 4 msec 8 msec
 4  5 ysng12kix4-ge5-0.rt.bora.net (210.120.248.23)  4 msec 4 msec 8 msec
 5  6 128.134.40.137 276 msec 268 msec 264 msec
 6  7 sv1-ge6.kornet.net (211.217.32.201) 252 msec 260 msec 260 msec
 7  8 soback.kornet21.net (168.126.3.3) 244 msec * 260 msec
router#
```

아래 결과는 Destination 이 있는 네트워크의 Looking-glass 서버인

<http://streamwk.kix.net/looking-glass/>

에서 traceroute를 한 결과입니다.

```
KORNET Looking Glass Results
Query: trace
Addr: 210.182.173.129
```

```
Type escape sequence to abort.
Tracing the route to 210.182.173.129
```

```
 1 hh-c2-ge1.kornet.net (211.192.46.2) [AS 170] 0 msec
    hh-c2-ge2.kornet.net (211.192.46.132) [AS 170] 0 msec
    hh-c2-ge1.kornet.net (211.192.46.2) [AS 170] 0 msec
 2 youngdong1-center2-2500M.kornet.net (168.126.109.6) [AS 170] 0 msec
    211.196.155.6 [AS 110] 4 msec
    youngdong1-center2-2500M.kornet.net (168.126.109.6) [AS 170] 0 msec
 3 168.126.0.41 [AS 140] 0 msec 0 msec 0 msec
 4 210.182.173.190 [AS 10054] 4 msec 4 msec 4 msec
 5 210.182.173.129 [AS 10054] 200 msec * 432 msec
```

경로의 상태 (delay, error 등) 를 파악할 때

source 210.182.173.129에서 soback.kornet.net으로 가는 경로가 보라넷을 거쳐 코넷으로 가고 코넷에서는 직접 되돌아 오는 것을 위에서 보았습니다. 그런데 보라넷에서 경유되는 지점들까지의 delay (RTT)는 10msec 이내로 양호한데 코넷에서 경유되는 지점들까지의 delay(RTT)가 100msec 이상으로 상대적으로 매우 높은 것을 볼 수 있습니다. 이때 일반인들이 코넷에 문제가 있다고 쉽게 결론을 짓는데 그것은 틀린 결론입니다. 그 결론이 틀리다는 것은 코넷 looking-glass에서 source 210.182.173.129로 traceroute를 했을 때 코넷과 source 210.182.173.129가 있는 네트워크를 연결하는 지점 (210.182.173.190)까지의 delay(RTT)가 4msec 으로 양호하기 때문입니다. 현재까지의 정보로 결론 지을 수 있는 것은 source와 한국통신 코넷간, source와 데이콤 보라넷간에는 상태가 양호하다는 사실입니다. 따라서 조금 더 살펴 보아야 할 사항은 한국통신 코넷과 데이콤 보라넷 사이의 상태입니다.

```
router#tr
Protocol [ip]:
Target IP address: soback.kornet21.net
Source address: 210.182.173.129
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to soback.kornet21.net (168.126.3.3)

 1 anyaba9-s10-1-2.rt.bora.net (210.207.9.165) 4 msec 8 msec 8 msec
 2 anybbb185-fe6-0-0.rt.bora.net (210.120.193.4) 4 msec 8 msec 8 msec
 3 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 4 msec 4 msec 8 msec
 4 ysng12bb1-pos8-0.rt.bora.net (210.120.192.113) 8 msec 4 msec 8 msec
 5 ysng12kix4-ge5-0.rt.bora.net (210.120.248.23) 4 msec 4 msec 8 msec
 6 128.134.40.137 276 msec 268 msec 264 msec
 7 sv1-ge6.kornet.net (211.217.32.201) 252 msec 260 msec 260 msec
 8 soback.kornet21.net (168.126.3.3) 244 msec * 260 msec
router#
```

KORNET Looking Glass Results

Query: trace

Addr: 210.182.173.129

Type escape sequence to abort.

Tracing the route to 210.182.173.129

```
 1 hh-c2-ge1.kornet.net (211.192.46.2) [AS 170] 0 msec
    hh-c2-ge2.kornet.net (211.192.46.132) [AS 170] 0 msec
    hh-c2-ge1.kornet.net (211.192.46.2) [AS 170] 0 msec
 2 youngdong1-center2-2500M.kornet.net (168.126.109.6) [AS 170] 0 msec
    211.196.155.6 [AS 110] 4 msec
    youngdong1-center2-2500M.kornet.net (168.126.109.6) [AS 170] 0 msec
 3 168.126.0.41 [AS 140] 0 msec 0 msec 0 msec
 4 210.182.173.190 [AS 10054] 4 msec 4 msec 4 msec
 5 210.182.173.129 [AS 10054] 200 msec * 432 msec
```

한국통신 코넷과 데이콤 보라넷간의 상태를 파악할 수 있는 방법은 두 ISP에 있는 Looking-glass를 활용하여 상대 ISP에 있는 시스템을 대상으로 ping 혹은 traceroute를 해 보는 것입니다. 아래 결과는 한국통신 코넷에서 데이콤 보라넷에 있는 웹서버 www.bora.net에 대해 traceroute를 해 본 것입니다.

KORNET Looking Glass Results

Query: trace

Addr: www.bora.net

Translating "www.bora.net"...domain server (168.126.63.1) [OK]

Type escape sequence to abort.

Tracing the route to www.bora.net (164.124.107.17)

```
 1 hh-k4-ge2.kornet.net (211.192.46.144) [AS 170] 0 msec
    hh-k4-ge1.kornet.net (211.192.46.14) [AS 170] 0 msec
    hh-k4-ge2.kornet.net (211.192.46.144) [AS 170] 0 msec
 2 128.134.40.74 [AS 110] 4 msec 0 msec 0 msec
 3 kidcg5-ge6-0.rt.bora.net (210.92.194.41) [AS 3786] 0 msec 4 msec 0 msec
 4 idcg12bb1-ge8-0.rt.bora.net (210.92.194.213) [AS 3786] 164 msec 236 msec 168 msec
 5 ysnng12bb2-pos9-0.rt.bora.net (210.120.192.197) [AS 3786] 228 msec 164 msec 224 msec
 6 ysnbbb245-ge4-0-0.rt.bora.net (210.120.248.152) [AS 3786] 228 msec
    ysnbbb241-p1.rt.bora.net (210.120.248.151) [AS 3786] 212 msec
    ysnbbb245-ge4-0-0.rt.bora.net (210.120.248.152) [AS 3786] 212 msec
 7 ysnaba4.rt.bora.net (210.120.246.4) [AS 3786] 220 msec
    ysnaba4-fe4-1-0.rt.bora.net (210.120.246.24) [AS 3786] 172 msec
    ysnaba4.rt.bora.net (210.120.246.4) [AS 3786] 232 msec
 8 203.248.246.85 [AS 3786] 232 msec 196 msec 220 msec
 9 www.bora.net (164.124.107.17) [AS 3786] 224 msec * *
```

결과를 보면 idcg12bb1-ge8-0.rt.bora.net (210.92.194.213) 에서 갑자기 delay (RTT)가 증가하는 것을 볼 수 있는데 이 결과만을 보고 idcg12bb1-ge8-0.rt.bora.net (210.92.194.213)에 문제가 있다고 판단을 하면 안됩니다. 위 결과는 코넷 Looking-glass 입장에서의 delay(RTT) 이므로 되돌아오는 경로(traceroute에서는 볼 수 없음)에서 delay(RTT) 때문에 위와 같은 결과가 나올 수 있습니다. 즉 kidcg5-ge6-0.rt.bora.net (210.92.194.41)에서 코넷 looking-glass로 되돌아가는 경로와 idcg12bb1-ge8-0.rt.bora.net (210.92.194.213)에서 코넷 looking-

glass로 되돌아가는 경로가 틀릴 수 있기 때문입니다 (현재 시점(2001-1-27)에 실제로 되돌아가는 경로가 틀립니다). 따라서 위 정보만으로 결론을 내릴 수 있는 것은 한국통신 코넷과 데이콤 보라넷간에 연결된 많은 회선중에 어딘가에 병목현상(bottleneck)이 있다는 것뿐입니다. 그러나 128.134.40.74와 kidcg5-ge6-0.rt.bora.net (210.92.194.41) 사이의 병목은 아니라는 것은 짐작할 수 있습니다.

이제 마지막으로 보라넷의 Looking-glass에서 코넷에 있는 서버 soback.kornet21.net 에 traceroute를 시도해 원인을 추측해 볼 차례입니다. Traceroute 결과는 아래와 같습니다.

BORANET Looking Glass Results

Query: trace

Addr: soback.kornet21.net

Type escape sequence to abort.

Tracing the route to soback.kornet21.net (168.126.3.3)

```
1 ysnbbb245-fe5-1-0.rt.bora.net (210.120.246.18) 0 msec
  ysnbbb245-fe5-0-0.rt.bora.net (210.120.246.13) 0 msec
  ysnbbb241-fe1-0-0.rt.bora.net (210.120.246.17) 4 msec
2 ysng12bb2-ge4-0.rt.bora.net (210.120.248.150) 0 msec 0 msec 0 msec
3 ysng12kix4-ge5-0.rt.bora.net (210.120.248.23) 0 msec
  ysng12kix4-ge3-0.rt.bora.net (210.120.192.85) 4 msec
  ysng12kix4-ge5-0.rt.bora.net (210.120.248.23) 0 msec
4 128.134.40.197 [AS 4766] 284 msec 260 msec 248 msec
5 sv1-ge1.kornet.net (211.192.46.71) [AS 4766] 252 msec
  sv2-ge5.kornet.net (211.217.32.72) [AS 4766] 256 msec
  sv1-ge1.kornet.net (211.192.46.71) [AS 4766] 276 msec
6 soback.kornet21.net (168.126.3.3) [AS 4766] 284 msec * 288 msec
```

위 결과를 보면 보라넷과 코넷을 연결하는 구간 128.134.40.197에서 갑자기 delay가 증가합니다. 위 결과와 앞에서 얻은 결과들을 종합하여 다음과 같은 결론을 내릴 수 있습니다.

- 한국통신 코넷 내부와 데이콤 보라넷 내부에서는 병목구간이 없다고 가정한다. 대개 사업자 내부에서 병목현상이 발생하는 경우는 매우 적다.
- 그리고 한국통신 코넷과 데이콤 보라넷을 연결하는 구간에 여러 개의 회선이 있다.
- 그런데 traceroute 결과 나타나는 2개의 회선(128.134.40.74과 128.134.40.197) 중에서 128.134.40.74에는 병목현상이 없다는 것을 코넷에서 www.bora.net으로 traceroute 했을 때 알았다. 따라서 128.134.40.197와 관계된 회선에 병목 현상이 있을 가능성이 높다.

위와 같은 결론을 내리고 데이콤 보라넷에서 라우팅과 관계된 사람과 통화를 하여 위 결론이 맞다는 것을 확인하였습니다.

특정한 IP address에 대한 경로가 차단되어 있는지 확인할 때

전세계적으로 스팸메일을 증계하는 메일서버에 대해서는 ISP들이 그 메일서버에 대한 경로를 차단하는 것이 일반적입니다. 그리고 그러한 경로 차단은 ISP간에 협력을 통해 조직적으로 이루어지고 있으며, 그 중심역할을 담당하는 것이 MAPS

(mail abuse prevention system)입니다. MAPS는 스팸메일을 발송하거나 중계하는 메일서버들을 등록해 관리하고 있으며, ISP들은 그 정보를 참조하여 스팸 메일을 발송하는 메일계정, 메일 서버들에 대한 서비스를 차단하고 있습니다.

[참고] MAPS에 대한 정보는

<http://mail-abuse.org/>

에서 얻을 수 있습니다. 스팸메일 중계서버와 관계된 내용은

<http://mail-abuse.org/rbl+/>

에서 얻을 수 있습니다.

국내에서는 데이콤 보라넷에서 스팸메일 중계서버에 대해 서비스를 차단하고 있는데, 그 이유는 다음과 같습니다.

- 첫번째, 스팸메일 중계서버에 대해 서비스를 차단하는 것이 일반화되어 가고 있고, ISP가 그런 중심적인 역할을 하여야 하기 때문입니다.
- 두번째, ISP가 관리하는 IP address 영역에 포함되는 고객의 스팸메일 중계서버로 인해 스팸메일이 많이 발송될 경우 해당 ISP가 다른 ISP로부터 비난을 받기 때문입니다.
- 세번째, 스팸메일 중계서버는 다른 ISP에서 서비스가 차단될 수 있는데 그런 서버가 다른 ISP에 의해서 차단되기 이전에 해당 ISP가 먼저 서비스 차단을 하여, 스팸메일 중계기능을 차단하도록 압력을 주기 위해서 입니다.
- 네번째, 다른 ISP에 의해서 고객의 서버에 대한 서비스가 차단될 경우 그것을 해제하게끔 하는 것이 매우 번거롭기 때문에, 해당 ISP 자신이 먼저 그 서버에 대한 서비스 차단을 하여 다른 ISP에 의해 차단되는 것을 방지하고, 스팸메일 중계기능이 차단될 경우 서비스 차단조치를 즉시 해제해 주기 위해서 입니다.

스팸메일 중계서버에 대한 서비스 차단조치는 메일서비스만 차단하는 것이 아니라 일반적으로 모든 통신서비스를 이용할 수 없게 하며, 그 방법은 다양하겠지만 일반적으로 ip route null0 (cisco IOS 기준) 를 이용합니다. 따라서 스팸메일 중계로 인해 어떤 ISP에 의해 통신이 차단되는 서버는 그 ISP를 경유한 통신서비스가 이루어지지 않습니다. 이런 경우 그것을 확인하는 방법은 그 ISP의 담당자에게 전화를 걸어서 확인하거나 아니면 그 ISP 네트워크에 있는 Looking-glass에서 trace를 이용해 확인하는 방법이 있습니다. 데이콤 보라넷에 의해 차단된 스팸중계 메일서버는 다음과 같이 확인할 수 있습니다.

데이콤 보라넷의 Looking-glass에 접속을 한 후 Query는 trace, address는 통신이 되지 않는 서버의 IP address를 입력한 후 Submit 버튼을 누릅니다. 일례로 아래 첫번째 결과는 통신이 차단된 211.171.255.25에 대해서 trace를 한 것이며, 그 결과를 보면 보라넷의 어떠한 조치에 의해 목적지까지 정상적으로 도달하지 못하고 특정한 곳에서 Loop현상이 발생하는 것을 볼 수 있습니다. 그러나 아래 두번째 결과는 통신이 차단되지 않은 211.171.255.26에 대해서 trace를 한 것인데 목적지까지 정상적으로 도달하는 것을 볼 수 있습니다.

http://looking-glass.bora.net/

Query: trace

Addr: 211.171.255.25

Type escape sequence to abort.

Tracing the route to 211.171.255.25

```
 1 ysnbbb241-fe5-0-0.rt.bora.net (210.120.246.12) 0 msec
   ysnbbb241-fe1-0-0.rt.bora.net (210.120.246.17) 0 msec
   ysnbbb245-fe5-0-0.rt.bora.net (210.120.246.13) 4 msec
 2 ysng12bb2-ge4-0.rt.bora.net (210.120.248.150) 0 msec 0 msec 0 msec
 3 anyg12bb2-pos8-0.rt.bora.net (210.120.192.118) 4 msec 4 msec 0 msec
 4 210.120.193.158 0 msec 4 msec 0 msec
 5 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 0 msec 0 msec 4 msec
 6 210.120.193.129 0 msec 0 msec 4 msec
 7 203.248.246.5 0 msec 4 msec 0 msec
 8 203.248.246.3 4 msec 4 msec 0 msec
 9 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 4 msec 0 msec 4 msec
10 210.120.193.129 0 msec 0 msec 4 msec
11 203.248.246.5 0 msec 0 msec 4 msec
12 203.248.246.3 0 msec 0 msec 4 msec
13 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 0 msec 0 msec 0 msec
14 210.120.193.129 4 msec 4 msec 0 msec
15 203.248.246.5 4 msec 0 msec 4 msec
16 203.248.246.3 4 msec 4 msec 4 msec
17 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 0 msec 4 msec 4 msec
18 210.120.193.129 0 msec 0 msec 0 msec
19 *
   203.248.246.5 0 msec 0 msec
20 203.248.246.3 4 msec 4 msec 0 msec
21 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 4 msec 4 msec 0 msec
22 210.120.193.129 4 msec 0 msec 4 msec
23 203.248.246.5 0 msec 4 msec 0 msec
24 203.248.246.3 4 msec 0 msec 4 msec
25 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 0 msec 4 msec 0 msec
26 210.120.193.129 0 msec 0 msec 4 msec
27 *
   203.248.246.5 0 msec 4 msec
28 203.248.246.3 0 msec 4 msec 0 msec
29 anyg12bb1-ge2-0.rt.bora.net (210.120.193.135) 4 msec 4 msec 4 msec
30 210.120.193.129 0 msec 4 msec 0 msec
```

http://looking-glass.bora.net/

Query: trace

Addr: 211.171.255.26

Type escape sequence to abort.

Tracing the route to 211.171.255.26

```
 1 ysnbbb245-fe5-0-0.rt.bora.net (210.120.246.13) 0 msec
   ysnbbb245-fe5-1-0.rt.bora.net (210.120.246.18) 0 msec
   ysnbbb241-fe5-0-0.rt.bora.net (210.120.246.12) 4 msec
 2 ysng12bb2-ge4-0.rt.bora.net (210.120.248.150) 0 msec 0 msec 4 msec
 3 idcg12bb1-pos1-0.rt.bora.net (210.120.192.198) 0 msec 0 msec 0 msec
```

```

4 kidcg6-ge8-0.rt.bora.net (210.92.194.238) 0 msec 0 msec 0 msec
5 211.169.248.254 0 msec 0 msec 0 msec
6 211.169.248.194 0 msec 0 msec 4 msec
7 211.171.255.26 0 msec 0 msec 4 msec

```

한가지 유의할 사항은 211.171.255.26가 다른 ISP로 가는 경로가 있다면 데이콤 보라넷에 의해 통신이 차단되어 있다고 하더라도 211.171.255.26는 다른 ISP들을 경유하여 통신을 할 수 있다는 사실입니다. 다만 데이콤 보라넷을 경유한 통신만이 차단될 뿐입니다. 그러나 다른 ISP로 가는 경로가 데이콤 보라넷 이외에 다른 것이 없다면 실질적으로 모든 서비스가 차단됩니다.

최적경로 (best path)가 어떤 것이 선택되는지 파악할 때

(주)한국증권전산 같은 경우에는 한국통신 코넷과 데이콤 보라넷에 모두 연결되어 있으며, 이들로부터 국내 및 해외라우팅 서비스를 동시에 제공받고 있습니다. 이런 상황에서 (주)한국증권전산의 통신회선 이용량이 한국통신 코넷과 연결된 회선에 편중되며, 그 원인이 해외에서 전달되어 오는 트래픽 때문이라고 가정해 봅시다. 이 경우 해외에서 발생된 트래픽이 한국통신 코넷과 데이콤 보라넷중 어느 쪽으로 편중되어 전달되는지 알아볼 필요가 있습니다. 이 경우 그 이유를 해외 ISP에 있는 Looking-glass를 보고 어느 정도 확인할 수 있습니다. 여기에서는 Oregon Exchange의 Looking-glass를 이용해 확인해 보도록 하겠으며, Oregon Exchange Looking-glass를 선택한 이유는 이곳이 다른 Looking-glass들보다 한국통신 코넷과 데이콤 보라넷과 관계되어 최적경로를 선택할 때 중립적인 위치라고 할 수 있기 때문입니다.

Oregon Exchange Looking-glass 서버에 접속하여 정보를 조회하면 아래와 같은 결과를 얻습니다. 결과에서 중요하지 않은 것들은 삭제하였습니다. 그리고 정보 조회 명령어는 "BGP as-path 조회" 부분에서 상세하게 다루며, 여기에서는 간단하게 설명하도록 하겠습니다.

```
route-views.oregon-ix.net>sh ip bgp regexp (3786_|4766_)+9526$
```

```
BGP table version is 13408373, local router ID is 198.32.162.100
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
* 128.134.148.0/24	205.158.2.126				0 2828 209 4766 9526 i
*>	144.228.241.81	6			0 1239 4766 9526 i
* 128.134.149.0/24	205.158.2.126				0 2828 209 4766 9526 i
*>	144.228.241.81	6			0 1239 4766 9526 i
* 128.134.150.0/24	205.158.2.126				0 2828 209 4766 9526 i
*>	144.228.241.81	6			0 1239 4766 9526 i
* 210.108.26.0	205.158.2.126				0 2828 3786 9526 i
*>	144.228.241.81	6			0 1239 4766 9526 i
* 210.108.27.0	205.158.2.126				0 2828 3786 9526 i
*	203.62.248.4				0 1221 3786 9526 i
*	157.22.9.7				0 715 3786 9526 i
*	204.70.4.89				0 3561 4766 9526 i
*	203.62.252.21				0 1221 3786 9526 i

```

*           207. 45. 223. 244           0 6453 4766 9526 i
*>          144. 228. 241. 81           6           0 1239 4766 9526 i
* 210. 108. 137. 0 205. 158. 2. 126     0 2828 3786 9526 i
*           157. 22. 9. 7               0 715 3786 9526 i
*           204. 70. 4. 89               0 3561 4766 9526 i
*           203. 62. 252. 21            0 1221 3786 9526 i
*           207. 45. 223. 244           0 6453 4766 9526 i
*>          144. 228. 241. 81           6           0 1239 4766 9526 i
* 210. 123. 14. 0 193. 140. 0. 1        0 1221 3786 9526 i
*           203. 62. 248. 4             0 1221 3786 9526 i
*           157. 22. 9. 7               0 715 3786 9526 i
*           207. 45. 223. 244           0 6453 4766 9526 i
*>          144. 228. 241. 81           6           0 1239 4766 9526 i
* 211. 169. 225. 0 205. 158. 2. 126     0 2828 3786 9526 i
*           203. 62. 248. 4             0 1221 3786 9526 i
*           157. 22. 9. 7               0 715 3786 9526 i
*           203. 62. 252. 21            0 1221 3786 9526 i
*           207. 45. 223. 244           0 6453 3786 9526 i
*>          144. 228. 241. 81           6           0 1239 4766 9526 i

```

(주)한국증권전산의 BGP AS번호는 9526이며, 한국통신 코넷의 AS번호는 4766, 데이콤 보라넷의 AS번호는 3786입니다. 따라서 Oregon Exchange Looking-glass에서는 다음과 같은 의미로 정보를 조회하였습니다.

- **sh ip bgp regexp**

AS path 정보를 가지고 정보를 조회하겠다는 뜻입니다.

- **(3786_|4766_)+**

AS path 중간에 3786이나 4766이 1번 이상 나타나는 것을 조회하겠다는 뜻입니다. 즉 9526에 포함되 네트워크정보가 3786 혹은 4766을 경유해서 전달된 것을 조회합니다.

- **9526\$**

AS path 가 9526으로 끝이 나는 경우를 조회하겠다는 뜻입니다. 즉, (주)한국증권전산에 포함된 네트워크정보를 조회하게 됩니다.

즉 위 조회명령어는 "(주)한국증권전산에서 발생된 네트워크정보중 한국통신 코넷이나 데이콤 보라넷을 경유해서 전달되는 것들을 보여달라" 라는 뜻입니다.

위 조회결과를 해석하는 방법에 대해 설명하겠습니다. 주의해서 봐야할 Column은 Network, Next-hop, Path, 그리고 Network앞에 표시되는 '*' 및 '>' 입니다. (주)한국증권전산의 AS번호 9526에서 전달되어 오는 Network 정보는

- 128.134.148.0/24
- 128.134.149.0/24
- 128.134.150.0/24
- 210.108.26.0
- 210.108.27.0
- 210.108.137.0

- 210.123.14.0
- 211.169.225.0

들입니다. 128.134.148.0/24에 대한 정보는 2개의 경로가 있으며, 첫번째 것은 Next-hop이 205.158.2.126, AS-path (2828 209 4766 9526) 이며, 두번째 것은 Next-hop이 144.228.241.81, AS-path (1239 4766 9526)입니다. 첫번째 것에 대한 해석은 “네트워크정보 128.134.148.0/24는 AS번호 9526을 가진 기관에서 발생하였으며, AS번호 4766을 가진 기업/ISP, AS번호 209를 가진 기업/ISP, AS번호 2828을 가진 기업/ISP를 차례대로 경유하여 전달되어 왔으며 (AS번호 4개를 경유해 왔으며, 이것을 AS-path 길이가 4라고 표현함), 이 경로가 최적경로로 선택이 될 경우 packet을 Next-hop 205.158.2.126으로 전달한다” 라고 할 수 있습니다. 두번째 것에 대한 해석도 동일하며, 차이는 두번째 것에서는 해당 정보가 AS번호 3개를 경유(AS-path 길이가 3)해 왔다는 사실입니다.

BGP 라우팅 정보를 가지고 최적의 경로를 선택할 때, 특별한 설정이 없는 한 AS-path 길이가 짧은 것이 최적경로로 선택됩니다. 만약 AS-path 길이가 동일하면 Metric 및 위에 표시되지 않은 BGP Router-ID에 의해 선택됩니다. 위 예에서는 128.134.148.0/24에 대해 AS-path 길이가 4보다 작은 3을 가진 Next-hop 144.228.241.81이 최적경로로 선택됩니다. 그리고 최적경로는 ‘*>’ 가 Network 앞에 표시됩니다. 따라서 위 조회결과를 보면 (주)한국증권전산의 모든 네트워크에 대해 Oregon Exchange에서는 최적의 경로를 데이콤 보라넷 (3786)을 경유하는 것보다 한국통신 코넷(4766)을 경유한 것들을 선택하고 있습니다. 따라서 해외에서 (주)한국증권전산으로 전달되어 오는 트래픽이 한국통신 코넷 회선으로 주로 집중되는 현상이 발생하는 것이라고 판단할 수 있습니다. 그리고 이러한 현상은 BGP 라우팅정보를 조절하여 트래픽이 편중되어 전달되어 오는 것을 어느 정도 해소될 수 있습니다. 여기에서 한가지 주의할 점은 Oregon Exchange에서만 라우팅정보를 살펴볼 것이 아니라 다른 중요한 Looking-glass에서도 조회해야 보다 정확한 상황을 파악할 수 있으므로 위 결과만으로 쉽게 결론을 지어서는 안 된다는 사실입니다.

[참고] BGP 라우팅에서 최적경로 선택 방법, 라우팅정보 조절을 통한 트래픽 조절, BGP 라우팅 정보 조회 방법 등에 대해서는 “BGP 라우팅 및 BGP 라우팅에서의 트래픽 조절”에서 상세하게 다루도록 하겠습니다.

자신의 네트워크 정보가 Looking-glass 서버를 제공하는 사업자까지 전달되는지 확인할 때

Looking-glass에서는 network address를 입력해 그것에 대한 결과가 출력되는지 확인할 수 있습니다. 만약 결과가 출력되지 않으면 그 looking-glass 서버까지 그 network address 정보가 전달되지 않는다는 뜻이며, 출력결과가 나올 경우 그 network address 정보가 전달된다는 뜻입니다. 아래는 3곳의 looking-glass에서 210.182.173.128 에 대해 차례대로 조회한 결과입니다.

route-views.oregon-ix.net 에서는 210.182.173.128에 대한 next-hop이 2개 (203.62.248.4 , 203.62.252.21)이며, 최적경로(best)는

203.62.252.21이 선택되었다는 것을 알 수 있습니다. 그것에 대한 AS-path는 1221 3786 10054입니다.

at telnet://route-views.oregon-ix.net

```
-----  
route-views.oregon-ix.net>sh ip bgp 210.182.173.128  
BGP routing table entry for 210.182.173.128/26, version 11245544  
Paths: (2 available, best #2)  
  Not advertised to any peer  
    1221 3786 10054  
      203.62.248.4 from 203.62.248.4 (203.62.248.4)  
        Origin IGP, localpref 100, valid, external  
    1221 3786 10054  
      203.62.252.21 from 203.62.252.21 (203.62.252.21)  
        Origin IGP, localpref 100, valid, external, best
```

neptune.dti.ad.jp/ixp2-lg.html 에서는 210.182.173.128에 대한 next-hop이 1개 (203.181.70.236)이며, 최적경로 (best)는 203.181.70.236 이 선택되었다는 것을 알 수 있습니다. 그것에 대한 AS-path는 4694 3786 10054입니다.

at http://neptune.dti.ad.jp/ixp2-lg.html

```
-----  
Query: bgp  
Addr: 210.182.173.128  
  
show ip bgp 210.182.173.128  
BGP routing table entry for 210.182.173.128/26, version 19704750  
Paths: (1 available, best #1)  
  Not advertised to any peer  
    4694 3786 10054  
      203.181.70.236 (metric 1) from 203.181.70.236 (203.181.70.236)  
        Origin IGP, localpref 200, valid, internal, best
```

ner-routes.bbnplanet.net 에서는 210.182.173.128에 대한 정보는 나오지 않고, 210.182.173.128에 대한 supernet 210.182.0.0/16에 대한 정보만 출력이 됩니다. 그리고 210.182.173.128이 AS 10054에서 발생되었다는 정보도 나타나지 않고 있습니다. 즉 이 조회결과는 210.182.173.128에 대한 정보가 ner-routes.bbnplanet.net까지는 전달되지 않았다는 것을 말해 주고 있습니다.

at telnet://ner-routes.bbnplanet.net

```
-----  
ner-routes>sh ip bgp 210.182.173.128  
BGP routing table entry for 210.182.0.0/16, version 0  
Paths: (1 available, best #1)  
  2828 3786  
    4.24.146.14 from 4.0.4.20 (4.24.0.106)  
      Origin IGP, metric 1000, localpref 50, valid, internal, best  
      Community: 1:666  
      Originator : 4.24.0.106, Cluster list: 4.0.4.20
```

그러나 ner-routes.bbnplanet.net에서 210.182.173.128/26에 포함되는

host 210.182.173.129에 대해 접근 가능합니다. 그 이유는 supernet 정보에 따라 데이콤 보라넷(AS 3786)까지 packet이 전달되고, 데이콤 보라넷에서는 210.182.173.128/26에 대한 정보가 있기 때문에 최종적으로 host 210.182.173.129까지 packet이 전달되기 때문입니다.

at telnet://ner-routes.bbnplanet.net

ner-routes>ping 210.182.173.129

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 210.182.173.129, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 212/212/216 ms

ner-routes>trace 210.182.173.129

Type escape sequence to abort.

Tracing the route to 210.182.173.129

```
 1 e0-1-5.burlmal-opsl.bbnplanet.net (4.2.34.162) 4 msec 4 msec 0 msec
 2 s7-0-4.bstnmal-cr7.bbnplanet.net (4.0.3.181) 0 msec 4 msec 0 msec
 3 p5-0.bstnmal-ba2.bbnplanet.net (4.24.4.225) 4 msec 0 msec 0 msec
 4 p7-0.bstnmal-br2.bbnplanet.net (4.24.7.121) 0 msec 4 msec 4 msec
 5 p2-0.bstnmal-br1.bbnplanet.net (4.24.7.113) 0 msec 0 msec 0 msec
 6 p3-0.chcgil2-cr11.bbnplanet.net (4.24.6.85) 24 msec 24 msec 28 msec
 7 so-3-1-0.chcgil2-br1.bbnplanet.net (4.24.6.21) 24 msec 24 msec 24 msec
 8 p6-0.chcgil1-br1.bbnplanet.net (4.24.9.70) 24 msec 24 msec 20 msec
 9 aads-atm-gtei.concentric.net (4.24.146.14) 24 msec 24 msec 24 msec
10 a1-0-0d7.core2.scl-ca.us.xo.com (207.88.0.189) 80 msec 80 msec 84 msec
11 ge9-0.tran1.scl-ca.us.xo.com (64.220.0.49) 80 msec 84 msec 84 msec
12 p0-0.tran1.pal-ca.us.xo.com (64.0.0.2) 84 msec 88 msec 84 msec
13 ge0-0.dist1.pal-ca.us.xo.com (64.220.0.19) 84 msec 84 msec 84 msec
14 ge2-0.access1.pal-ca.us.xo.com (64.220.2.20) 84 msec 84 msec 84 msec
15 207.88.240.102 88 msec 88 msec 84 msec
16 p5.bora.net (203.255.234.55) 84 msec 84 msec 84 msec
17 p4.bora.net (203.255.234.44) 84 msec 84 msec
   203.255.234.197 228 msec
18 ysng12bb2-ge2-0.rt.bora.net (210.120.192.132) 228 msec
   p5.bora.net (203.255.234.55) 84 msec
   ysng12bb2-ge3-0.rt.bora.net (210.120.192.2) 208 msec
19 203.255.234.197 228 msec 228 msec
   p4.bora.net (203.255.234.44) 84 msec
20 ysng12bb2-ge3-0.rt.bora.net (210.120.192.2) 208 msec
   anybbb181-ge1-0-0.rt.bora.net (210.120.193.136) 208 msec 208 msec
21 anyaba9.rt.bora.net (210.120.193.9) 208 msec 208 msec
   anyg12bb2-pos8-0.rt.bora.net (210.120.192.118) 212 msec
22 anybbb181-p1.rt.bora.net (210.120.193.146) 232 msec
   anyaba9-s10-1-2-c.rt.bora.net (210.207.9.166) 212 msec
   anybbb181-ge1-0-0.rt.bora.net (210.120.193.136) 208 msec
ner-routes>
```

at http://looking-glass.bora.net/

Query: bgp

Addr: **210.182.173.128**

```
BGP routing table entry for 210.182.173.128/26, version 643361
Paths: (2 available, best #1, advertised over EBGP)
 10054
   172.30.34.9 (metric 241) from 172.30.2.71 (210.120.193.177)
     Origin IGP, metric 0, localpref 100, valid, internal, best
     Community: 3786:11
     Originator: 210.120.193.177, Cluster list: 0.0.0.20, 0.0.0.3,
0.0.0.10, 0.0.0.30
 10054
   172.30.34.9 (metric 241) from 172.30.2.72 (210.120.193.177)
     Origin IGP, metric 0, localpref 100, valid, internal
     Community: 3786:11
     Originator: 210.120.193.177, Cluster list: 0.0.0.20, 0.0.0.3,
0.0.0.10, 0.0.0.30
```

[참고] looking-glass에서 사용할 수 있는 명령어가 모두 허용되어 있는 경우가 제한되어 있는 경우가 있습니다. 어떤 looking-glass 에서는 'sh ip bgp regexp' 가 지원되는 반면 그렇지 않은 곳도 있으며, 단지 'sh ip bgp net.net.net.net' 만 지원되는 경우도 있습니다.