“有关 IP 的网络安全那些事儿”

@高春辉 • 2016.7

DRoP: DNS-based Router Positioning

Bradley Huffaker, Marina Fomenkov, kc claffy

DDec: DNS Decoding

Ken Keys, Bradley Huffaker

DHS site vist
June 18, 2014

Homeland Security

IP 库是什么？

定义

互联网基于 IP 地址，每个 IP 理论上都有其物理位置以及各种标签，为查询计，我们需要这样一类数据库。

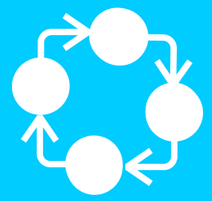
IP 库是什么？

用途

用户信息获取

广告精准定向投放

流量行为分析



CDN / DNS / VPN
节点就近就快调度

IP 库有多少种？

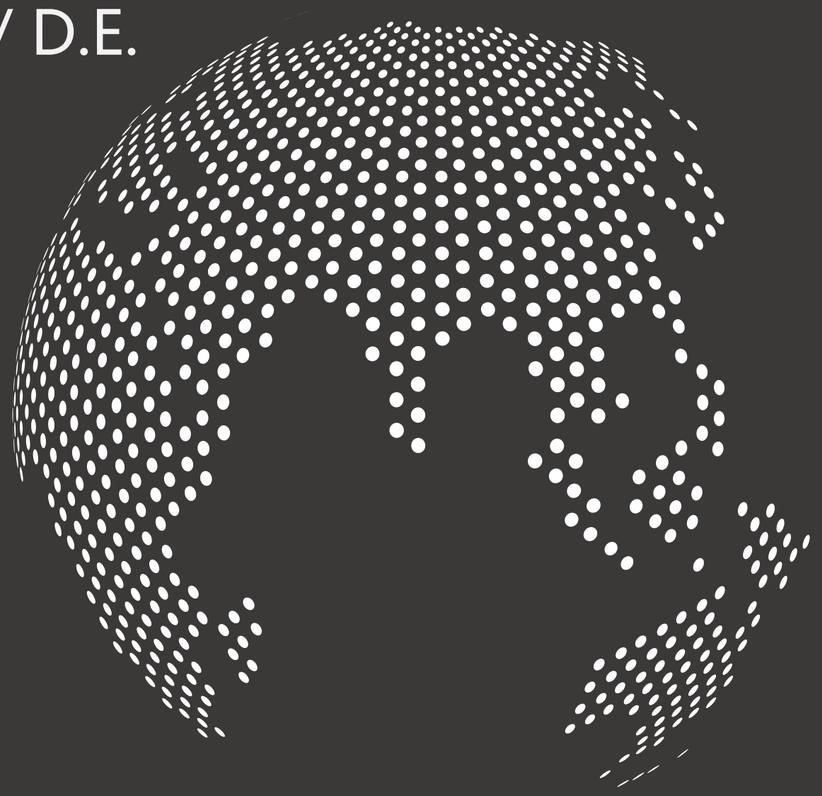
不同于 WHOIS 数据，IP 库没有所谓的官方数据，理论上也不可能有。按精度区别，可分为城市级数据库或者区县级以及街级数据库。以城市级为主流。

国外

- MaxMind / IP2Location / D.E. / 其它

国内

- 纯真
- 新浪、淘宝、腾讯、百度
- 中国互联网广告行业 IP 库
- IPIP.NET



为什么要单独维护一个，而不是用其它版本呢？

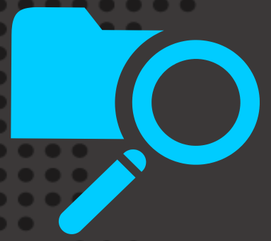
起源于 ECSHOP 时代和对 CDN 方面的困惑

数据积累初步启动于 2013年 10 月

2014 年 3 月正式发布第一个免费版，2014 年 5 月开始运营付费版本。

接近 200 家商业客户（截至 2015年底）

2016 年 7 月，客户数量 230+

1
准确性问题

以 WHOIS、多个 IP 库投票为基础来维护的话，很 LOW，不直接，非常不准确。

2
规范性问题

1、描述不规范，一会北京，一会北京市，如何破？

2、一会电信通、一会鹏博士、到底哪个为准？

3
及时性问题

IP 数据去掉非公网 IP，大概有 36 亿个需要维护。

全球相关机房上万个，相关公司上十万个。

变动是正常的，工作量超大，你跟得上否？

4
持续性问题

既有专业性问题，又有精力投入问题，兼职工作如何能破？

“ipip.net 版本 ”

“我们会严格的对 IP 数据进行审核与标注”

“我们对 **准确度** 的要求高于 **精准度** 的要求”

请仔细思考 准确度 和 精准度 的区别!

如何维护 IP 库？

首先是一个技术活

即使你想自己拼装一个库的话，至少你要会去抓取和解析拼装其它人的库。

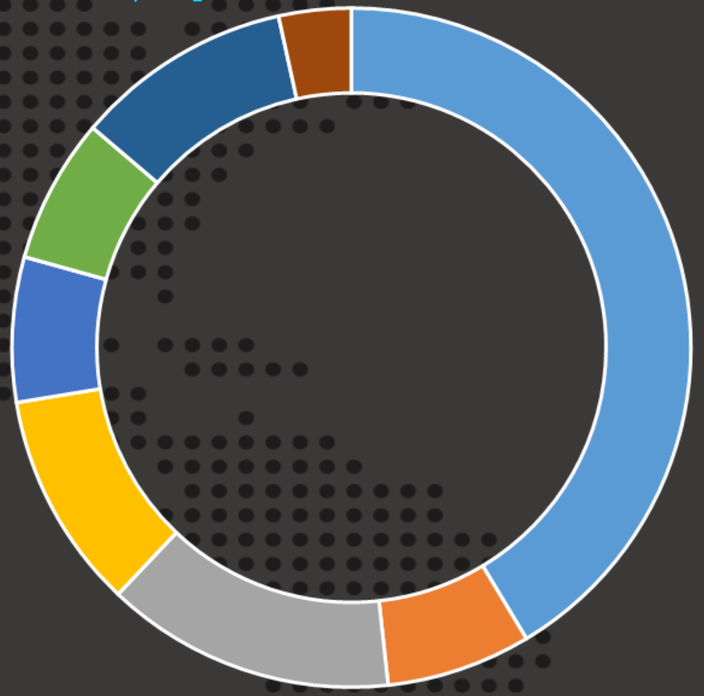
从完全自行维护的角度，你需要懂 IP 地址的基础知识，你需要懂网络工程师的一些知识（BGP、ASN、CIDR），还有语言和地理知识、省市区域这些难关。

长期是一个力气活

好吧，现在是 IPV4，未来是 IPV6……

“重点介绍 ipip.net 版本”

我们如何维护 IP 库？



包括但不限于：

1. 我们在全球的 330+ 个监测点，不断增加中；
2. 自有或者其它可信任的数据来源；
3. 全球 WHOIS / BGP / ASN / RADB 数据；
4. 全球 Internet Exchange Point 数据；
5. 自行维护的全球 rDNS 以及骨干网路由 IP 数据库；
6. 运营商、客户、合作伙伴的反馈数据；
7. 网友提交纠错的数据；
8. 其它方式。

我们通过总结的一些方法通过程序或人工方式进行 IP 数据的收集分析与审核入库

你需要知道的事情

IPV4 全部接近 **43 亿个 IP**。
实际上可以用于外网访问的在 36 亿左右。
BGP/AS 数据接近 **78000 条**，
实际投入使用的有 **55000 条**。
每天都有新的 AS 号和 IP 通过申请。
全球与此相关的公司应该有 **200000+ 家**公司以上。
全球提供 IP 数据库的公司总体不到 **100 家**。

需要的知识（一）

网络知识

了解全球的网络情况；

了解全球的运营商情况；

了解全球的数据中心分布情况；

光缆、建设、链接与分布情况；

Internet Exchange Point。

需要的知识（二）

地理知识与语言知识

洲级与国家知识
城市知识
各种语言的网站
各种代码、缩写、区号、时区、变更
等等，比你想象的要多一点点。

需要的知识（三）

网络测量知识

时延测量
网络知识
BGP 知识
安全知识

需要的能力（一）

DevOps

PHP、GO、C
服务器维护能力
全球 330+ 台云主机，80 台独立主机
还有专门用于收集和处理数据的独立主机
不断强化数据采集和挖掘的能力
自动化处理数据，人工确认和标注数据

```
Tasks: 714 total,   2 running, 712 sleeping,   0 stopped,   0 zombie
Cpu0  : 13.3%us,  4.7%sy,  0.0%ni, 77.1%id,  3.4%wa,  0.0%hi,  1.5%si,  0.0%st
Cpu1  : 20.9%us, 19.2%sy,  0.0%ni, 56.7%id,  3.2%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  :  9.3%us,  3.1%sy,  0.0%ni, 87.5%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  : 19.9%us, 15.5%sy,  0.0%ni, 64.6%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu4  :  8.7%us,  2.4%sy,  0.0%ni, 88.8%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu5  :  9.7%us,  2.4%sy,  0.0%ni, 87.9%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu6  :  8.5%us,  1.8%sy,  0.0%ni, 89.7%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu7  :  8.9%us,  1.3%sy,  0.0%ni, 89.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu8  :  8.5%us,  1.5%sy,  0.0%ni, 90.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu9  :  8.4%us,  0.4%sy,  0.0%ni, 91.2%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu10 :  8.5%us,  1.1%sy,  0.0%ni, 90.4%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu11 :  8.4%us,  0.5%sy,  0.0%ni, 91.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu12 :  8.4%us,  0.8%sy,  0.0%ni, 90.8%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu13 :  8.7%us,  0.7%sy,  0.0%ni, 90.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu14 :  8.3%us,  0.7%sy,  0.0%ni, 90.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu15 :  8.3%us,  0.2%sy,  0.0%ni, 91.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu16 :  8.3%us,  0.6%sy,  0.0%ni, 91.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu17 :  8.3%us,  0.2%sy,  0.0%ni, 91.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu18 :  8.3%us,  0.7%sy,  0.0%ni, 90.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu19 :  8.3%us,  0.2%sy,  0.0%ni, 91.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu20 :  9.8%us,  3.5%sy,  0.0%ni, 86.4%id,  0.4%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu21 :  8.9%us,  1.4%sy,  0.0%ni, 89.4%id,  0.2%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu22 :  8.6%us,  0.9%sy,  0.0%ni, 90.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu23 :  9.8%us,  3.7%sy,  0.0%ni, 86.5%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu24 :  9.3%us,  1.0%sy,  0.0%ni, 89.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu25 : 10.6%us,  4.3%sy,  0.0%ni, 85.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu26 :  8.5%us,  0.9%sy,  0.0%ni, 90.6%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu27 :  9.0%us,  1.1%sy,  0.0%ni, 89.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu28 :  8.3%us,  0.6%sy,  0.0%ni, 91.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu29 :  8.5%us,  0.6%sy,  0.0%ni, 91.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu30 :  8.4%us,  0.7%sy,  0.0%ni, 90.8%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu31 :  9.1%us,  2.5%sy,  0.0%ni, 88.4%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu32 :  8.4%us,  0.6%sy,  0.0%ni, 91.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu33 :  8.5%us,  0.7%sy,  0.0%ni, 90.8%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu34 :  8.4%us,  0.6%sy,  0.0%ni, 91.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu35 :  8.5%us,  0.5%sy,  0.0%ni, 91.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu36 :  8.5%us,  0.6%sy,  0.0%ni, 90.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu37 :  9.1%us,  1.1%sy,  0.0%ni, 89.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu38 :  8.4%us,  0.6%sy,  0.0%ni, 90.9%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu39 :  9.6%us,  1.7%sy,  0.0%ni, 88.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:  198297336k total, 195092092k used,  3205244k free,    28492k buffers
Swap:  1048572k total,   310940k used,   737632k free, 71061028k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6788 root      20   0 11.6g 8.6g 1364 S 95.6  4.6  11142:08 ./tip tip.cfg
 7919 root      20   0 23.0g  21g 1384 R 95.6 11.3  15779:16 ./drop drop.cfg
```

需要的能力（二）

学习能力

这个事情，没有教程和文章告诉你如何做。

只有自行钻研一条路。

维护的难点？

网络情况非常复杂：

1、卫星上网 / 省级出口；

2、VPN / NAT / MOBILE；

3、ANYCAST / BACKBONE；

4、BGP/路由器数据出错或伪造；

5、运营商的内网黑盒子；

6、就是不想告诉你。

IPIP.NET 数据分享（2016.7）

原始文本数据文件
提交 30000+ 次
共 344000+ 行

IPIP.NET 网站代码
9000+ 行。

命令行与客户端代码
20000+ 行

BGP 不重复数据量
10000+ 万行。

HOST/RDNS 定义文件
10000+ 行

生成一次全球 ASN 相关数据文件的时间，
2 小时。*

当前 IP 数据库版本	数据库条目数	数据库最后更新时间
20151202	223052	2015-12-02 01:15:15

当前 IP 数据库版本	数据库条目数	数据库最后更新时间
20151212	224717	2015-12-12 02:10:11

当前 IP 数据库版本	数据库条目数	数据库最后更新时间
2016071300	344778	2016-07-13 00:43:18

518418	223.250.200.0	223.250.200.255	中国	上海	上海	浦东新区	310115	14.4
518419	223.250.201.0	223.250.201.255	中国	上海	上海	浦东新区	310115	11.9
518420	223.250.202.0	223.250.202.255	中国	上海	上海	浦东新区	310115	12.6
518421	223.250.203.0	223.250.203.255	中国	上海	上海	浦东新区	310115	14.1
518422	223.250.204.0	223.250.204.255	中国	上海	上海	浦东新区	310115	12.8
518423	223.250.205.0	223.250.205.255	中国	上海	上海	浦东新区	310115	11.7
518424	223.250.206.0	223.250.206.255	中国	上海	上海	浦东新区	310115	4.2
518425	223.250.207.0	223.250.207.255	中国	上海	上海	浦东新区	310115	11.8
518426	223.251.32.0	223.251.32.255	中国	上海	上海	浦东新区	310115	4.5
518427	223.251.33.0	223.251.33.255	中国	上海	上海	浦东新区	310115	4.1
518428	223.251.36.0	223.251.36.255	中国	上海	上海	浦东新区	310115	3.9
518429	223.251.37.0	223.251.37.255	中国	上海	上海	浦东新区	310115	7.5
518430	223.251.38.0	223.251.38.255	中国	上海	上海	浦东新区	310115	4.5
518431	223.251.39.0	223.251.39.255	中国	上海	上海	浦东新区	310115	4.8
518432	223.251.40.0	223.251.40.255	中国	上海	上海	浦东新区	310115	2.4
518433	223.251.41.0	223.251.41.255	中国	上海	上海	浦东新区	310115	3
518434	223.251.43.0	223.251.43.255	中国	上海	上海	浦东新区	310115	66
518435	223.251.44.0	223.251.44.255	中国	上海	上海	浦东新区	310115	2
518436	223.251.45.0	223.251.45.255	中国	上海	上海	浦东新区	310115	0.3
518437	223.251.66.0	223.251.66.255	中国	上海	上海	浦东新区	310115	10.3
518438	223.255.156.0	223.255.156.255	中国	香港	香港	油尖旺区	810018	8.4
518439	223.255.172.0	223.255.172.255	中国	香港	香港	油尖旺区	810018	9

```
[root@i-1rhsjmn5 ~]# php /home/codebase/loveapp/dpt/toolbox/asn.php --check=4 --as=AS133905

ASN: EASYINTERNETCOMPANY-AS-AP Network Infrastructure,HK

==================================AS133905================================
43.228.124.0 - 43.228.124.255          中国香港        中国香港
  Tracert 43.228.124.1 from 59.188.242.204:
        1  IP:  59.188.242.129 host:                                59.188.242.129 AS:                                AS17444 Time: 7.9       area: 中国香港
        2  IP:  113.10.230.233 host:                                113.10.230.233 AS:                                AS17444 Time: 7.9       area: 中国香港
        3  IP:  113.10.229.105 host:             irb9.10g-tc2.wpc.nwtgigalink.com AS:                                AS17444 Time: 7.9       area: 中国香港
        4  IP:  113.10.229.130 host:              ae2.10g-pp2.wpc.nwtgigalink.com AS:                                AS17444 Time: 7.9       area: 中国香港
        5  IP:  202.40.160.207 host:                           telin9-RGE.hkix.net AS:                                        Time: 7.9       area: 中国香港
        6  IP:            * host:                                             * AS:                                      * Time: * area:
        7  IP:   43.228.124.1 host:                               43.228.124.1 AS:                               AS133905 Time: 43.9      area: 中国香港

43.228.125.0 - 43.228.125.255          中国香港        中国香港
  Tracert 43.228.125.1 from 59.188.242.204:
        1  IP:  59.188.242.129 host:                                59.188.242.129 AS:                                AS17444 Time: 11.8      area: 中国香港
        2  IP:  113.10.230.233 host:                                113.10.230.233 AS:                                AS17444 Time: 7.7       area: 中国香港
        3  IP:  113.10.229.105 host:             irb9.10g-tc2.wpc.nwtgigalink.com AS:                                AS17444 Time: 7.7       area: 中国香港
        4  IP:  113.10.229.130 host:              ae2.10g-pp2.wpc.nwtgigalink.com AS:                                AS17444 Time: 7.6       area: 中国香港
        5  IP:  202.40.160.207 host:                           telin9-RGE.hkix.net AS:                                        Time: 7.6       area: 中国香港
        6  IP:            * host:                                             * AS:                                      * Time: * area:
        7  IP:   43.228.125.1 host:                               43.228.125.1 AS:                               AS133905 Time: 42.5      area: 中国香港


==================================={UPSTREAM}=================================
   AS56308 | TELIN-NET-SG TELEKOMUNIKASI INDONESIA INTERNATIONAL, PTE.LTD,SG | 新加坡

IP Number TotalCount: 512
IP Number TotalCount: 2C

====================================={BGP}====================================
AS地区范围：中国 香港

    43.228.124.0 - 43.228.124.255                                  中国香港                                  中国香港
    43.228.125.0 - 43.228.125.255                                  中国香港                                  中国香港

============================== BGP AS INFO V4 ==============================
   AS56308 | TELEKOMUNIKASI INDONESIA INTERNATIONAL, PTE.LTD | TELIN-NET-SG TELEKOMUNIKASI INDONESIA INTERNATIONAL, PTE.LTD,SG | 新加坡
  AS133380 |         Pacificnet Hosting Ltd | PACHOST-AS Pacificnet Hosting Ltd,HK | 中国 香港

============================== BGP AS PEER V4 ==============================
   AS56308 | TELEKOMUNIKASI INDONESIA INTERNATIONAL, PTE.LTD | TELIN-NET-SG TELEKOMUNIKASI INDONESIA INTERNATIONAL, PTE.LTD,SG | 新加坡
  AS133380 |         Pacificnet Hosting Ltd | PACHOST-AS Pacificnet Hosting Ltd,HK | 中国 香港


====================================END=====================================
```

```
),
'AS4811' => array(
    array('中国', '上海', '电信'),
),
'AS4812' => array(
    array('中国', '上海', '电信'),
),
'AS4813' => array(
    array('中国', '广东', '电信'),
),
'AS4815' => array(
    array('中国', '上海', '电信'),
),
'AS4816' => array(
    array('中国', '广东', '广州', '电信'),
),
'AS4818' => array(
    array('马来西亚'),
),
'AS4819' => array(
    array('澳大利亚'),
),
'AS4820' => array(
    array('澳大利亚'),
),
'AS4821' => array(
    array('印度尼西亚'),
),
'AS4822' => array(
    array('澳大利亚'),
),
```

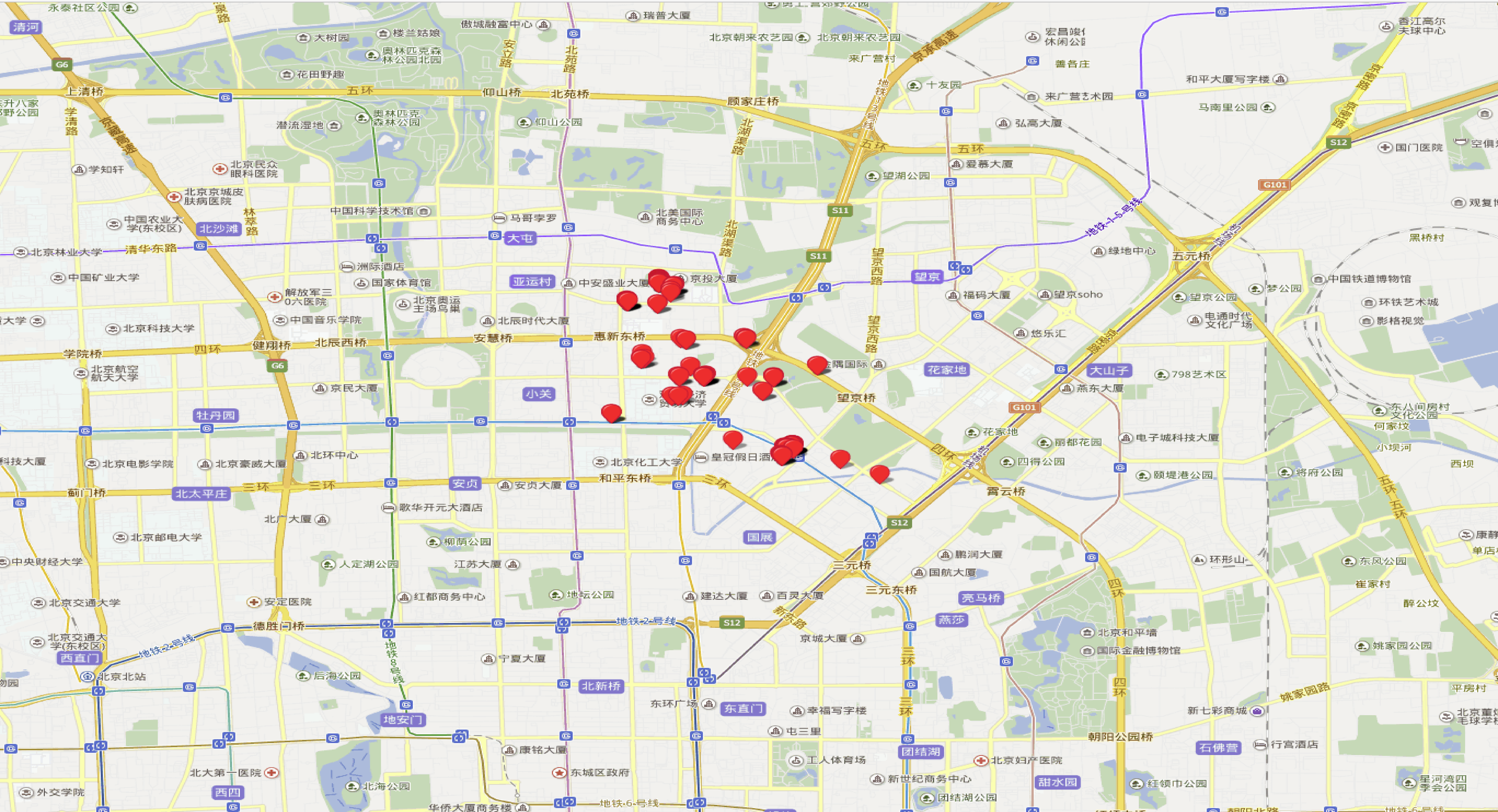
```
50284 393791→ 173.241.83.0-173.241.83.255,173.241.92.0-173.241.92.255↲
50285 393795→ 63.144.152.0-63.144.152.255↲
50286 393796→ 104.128.32.0-104.128.32.255↲
50287 393797→ 192.149.72.0-192.149.72.255↲
50288 393800→ 38.94.173.0-38.94.173.255↲
50289 393804→ 199.96.149.0-199.96.149.255↲
50290 393807→ 104.247.160.0-104.247.191.255↲
50291 393809→
      12.216.20.0-12.216.20.255,12.216.105.0-12.216.105.255,12.230.56.0-12.230.57.255,45.40.0.0-45.40.
      0.255,45.40.1.0-45.40.1.255,45.40.2.0-45.40.2.255,45.40.3.0-45.40.3.255,45.40.4.0-45.40.4.255,45.
      40.5.0-45.40.5.255,45.40.10.0-45.40.10.255,45.40.14.0-45.40.14.255,45.40.15.0-45.40.15.255,104.1
      92.156.0-104.192.157.255,104.192.159.0-104.192.159.255↲
50292 393810→ 208.103.7.0-208.103.7.255↲
50293 393812→ 192.88.186.0-192.88.186.255↲
50294 393814→ 209.194.255.0-209.194.255.255↲
50295 393817→ 192.109.104.0-192.109.104.255↲
50296 393818→ 64.96.160.0-64.96.191.255↲
50297 393834→ 63.157.124.0-63.157.124.255↲
50298 393839→ 208.89.244.0-208.89.244.255,208.89.244.0-208.89.245.255,208.89.244.0-208.89.247.255↲
50299 393841→ 45.42.32.0-45.42.33.255↲
50300 393845→ 192.69.86.0-192.69.87.255↲
50301 393846→ 192.101.9.0-192.101.9.255↲
50302 393848→ 199.26.169.0-199.26.169.255↲
50303 393849→ 192.122.150.0-192.122.150.255↲
50304 393857→ 38.29.144.0-38.29.151.255,38.29.152.0-38.29.155.255↲
50305 393858→ 192.122.201.0-192.122.201.255↲
50306 393861→ 167.201.224.0-167.201.227.255,167.201.240.0-167.201.243.255↲
50307 393869→ 129.19.176.0-129.19.191.255,204.132.32.0-204.132.47.255↲
50308 393875→ 152.37.128.0-152.37.255.255↲
```

```
1100 3212→    3303,6939,13237,31042→    5603,12644,24747,25017,25034,28682,31042,31060,33929,41543,42560,42613,43061,43
1101 3213→    174,2914,3356,5413,5459,5580,6939,13237,19151,24482,30844,36236→8916,42689,59817↲
1102 3215→    5511,8218,39180→288,1708,2129,3259,3295,3298,8218,8255,8362,8528,8891,8921,9089,9159,12601,12910,12980,
1103 3216→    251,701,702,1267,1273,2603,2914,3267,3303,3320,3356,3549,3741,4589,5459,5580,5769,6453,6667,6762,6939,8
1104 3217→    20485,39293→↲
1105 3218→    3267,8492,24482,39792→    5386,34849,49554↲
1106 3219→    31581→    ↲
1107 3220→    1257,1880,6939,24482→    ↲
1108 3221→    2603,3267,20965→2586,62024↲
1109 3222→    3292→    ↲
1110 3223→    1299,2914,3267,4589,4739,5580,6079,6762,6939,7385,7922,8121,8365,8492,10026,11666,13030,13237,13618,152
1111 3224→    1653→    ↲
1112 3225→    1299,6762,6939,15412,15802,19151,24482,30844,36236,39386,41811→ 25122,47519,47589,60992,199869↲
1113 3226→    1299,31133→ 34983,38959,47418,49557,52217,196685↲
1114 3228→    8612→    ↲
1115 3233→    2614,12310→ ↲
1116 3238→    174,3549,6939,24482,36351,39792→31644,41878,47605↲
1117 3239→    12389,35400→3203,8324,28970,31470,34246,47733,47787,48043,48527,49483,58231↲
1118 3242→    1267→    8660↲
1119 3243→    8426,8657→    6773,9118,25253,28672,28998,31497,39088,41159↲
1120 3244→    6939,21229→ ↲
1121 3245→    6939,8866,8928,9070,57344→    42909,48053,197997↲
1122 3249→    1299,3267,6667,39792→    3332,8240,16014,21147,28955,34729,35106,35407,39211,39632,42012,42016,42300,439
1123 3252→    174,3267,3333,6939,8365,8492,10026,13237,24482,30844,39792,48526→    12593,12654,12963,25521,29107,29275
1124 3253→    3216→    20619,39073,41928,42276,47740,49675,51316,59495,198544,202239↲
1125 3254→    3255,13249→ 8788,35442,48649,196825↲
1126 3255→    251,3257,3267,3303,3333,5413,6939,8359,8365,8492,9002,10026,13030,13237,19151,24482,28917,29076,29439,3
1127 3257→    174,209,701,852,1239,1273,1299,2497,2516,2828,2914,3320,3356,3491,3549,4436,4589,4637,4826,6453,6461,70
1128 3259→    3215,15557→ ↲
```

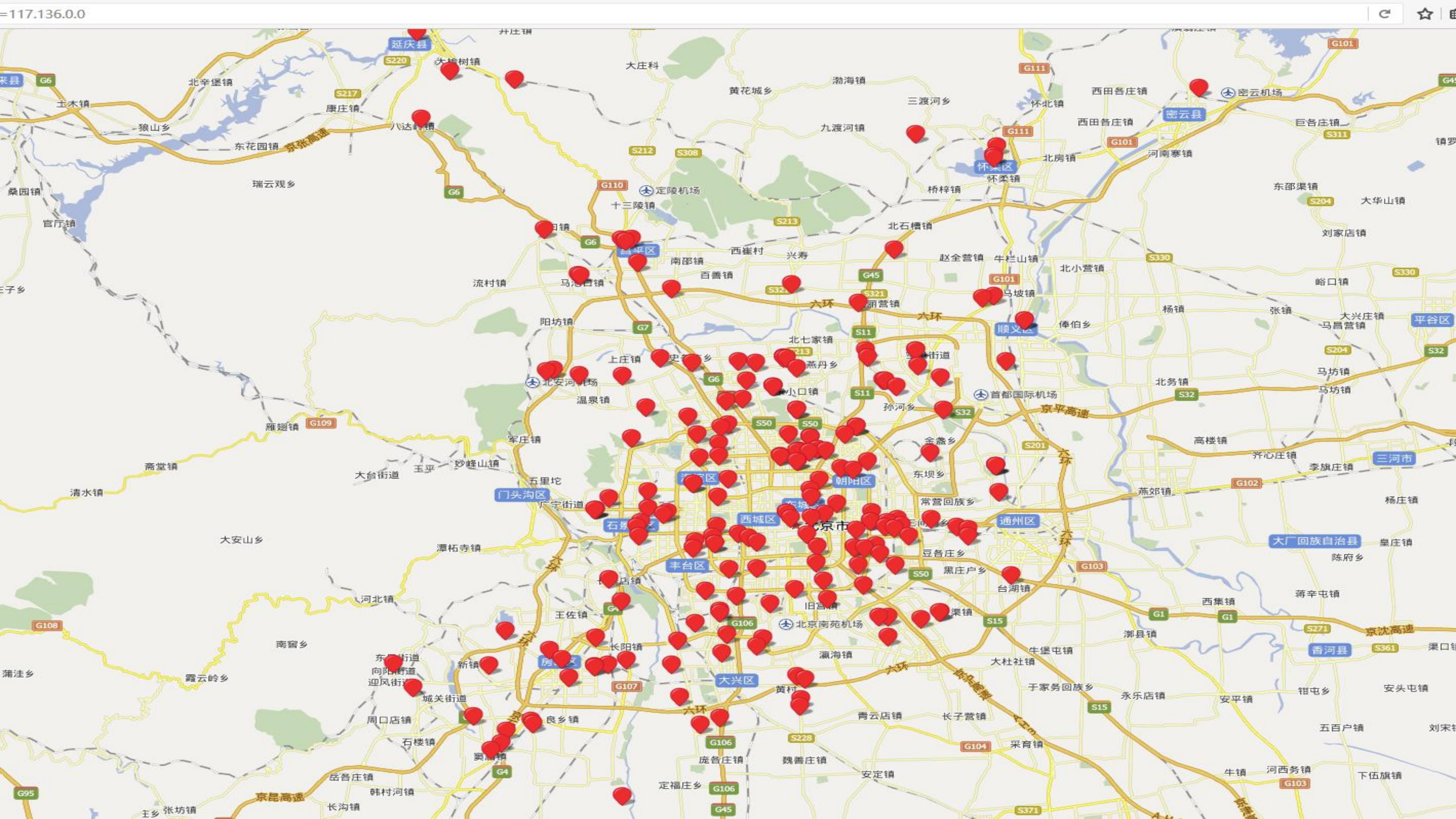
AS11984 - NETWALK - NetWalk,US | 美国 => AS40715 - DATACENTER-BZ - DataCenter.BZ, LLC,US | 美国 哥伦布
AS11992 - CENTENNIAL-PR - Centennial de Puerto Rico,PR | 波多黎各 => AS7018 - ATT-INTERNET4 - AT&T Services,
AS12061 - 24HOURFITNESS - 24 Hour Fitness USA, Inc.,US | 美国 => AS23005 - SWITCH-COMMUNICATIONS - SWITCH Comm
AS12110 - AS-INTER - Internex Inc.,US | 美国 => AS16724 - WOW-DATACENTER-NET - WideOpenWest Finance LLC,US |
AS12120 - AAO-AIO - Amphenol Corp,US | 美国 => AS11351 - RR-NYSREGION-ASN-01 - Time Warner Cable Internet LLC
AS12136 - N?cleo de Inf. e Coord. do Ponto BR - NIC.BR,BR | 巴西 => AS8763 - DENIC-AS DENIC eG,DE | 德国
AS12340 - TZM-NET Wispone S.R.L.,IT | 意大利 => AS15830 - TELECITY-LON TELECITYGROUP INTERNATIONAL LIMITED,GB
AS12361 - PANAFONET-AS VODAFONE-PANAFON HELLENIC TELECOMMUNICATIONS COMPANY SA,GR | 希腊 => AS3209 - VODANET
AS12411 - LLNW-GCC Limelight Networks, INC.,BH | 巴林 => AS22822 - LLNW - Limelight Networks, Inc.,US | LIMEL
AS12433 - ORBTALK Orbtalk Limited,GB | 英国 => AS25577 - C4L-AS Connexions4London Ltd,GB | 英国 伦敦
AS12463 - ASN-SBM S.A. des Bains de Mer et du Cercle des Etrangers a Monaco,FR | 法国 => AS6758 - AS6758 MONA
AS12488 - KRYSTAL Krystal Solutions LLP,GR | 英国 梅德斯通 => AS24958 - TBSH The Bunker Secure Hosting Limite
AS12501 - NORRNOD An Internet Exchange point and ISP in Umea, Sweden,SE | 瑞典 于默奥 => AS2119 - TELENOR-NEX
AS12539 - PENKI Penki Kontinentai, Ltd.,LT | 立陶宛 => AS12578 - APOLLO-AS LATTELEKOM-APOLLO,LV | 拉脱维亚
AS12556 - internet-solutions-ke,KE | 肯尼亚 => AS3741 - IS,ZA | 南非
AS12608 - MAXHOSTING-AS MediaServicePlus Ltd.,RU | 俄罗斯 => AS50113 - SUPERSERVERSDATACENTER MediaServicePlu
AS12818 - BIZANGA-AS Cloudmark Labs,FR | 法国 => AS15421 - Internap European Autonomous System,GB | 法国 巴黎
AS12833 - GIGAPIX GigaPix - Portuguese Internet eXchange,PT | 葡萄牙 里斯本 => AS1930 - RCCN Fundacao para a
AS13100 - TELECITYGROUP INTERNATIONAL LIMITED,IE | 爱尔兰 => AS15830 - TELECITY-LON TELECITYGROUP INTERNATIONA
AS13301 - UNITEDCOLO-AS United Gameserver GmbH,DE | 德国 科堡 => AS24961 - MYLOC-AS myLoc managed IT AG,DE |
AS13362 - PCWORLD - PCWorld.com,US | 美国 => AS14743 - INTERNAP-BLOCK-4 - Internap Network Services Corporati
AS13383 - INFORMATIONBUILDERS - Information Builders,US | 美国 => AS13789 - INTERNAP-BLK3 - Internap Network
AS13478 - TESSAPORT-AS - Tessaport Inc.,US | 美国 => AS14742 - INTERNAP-BLOCK-4 - Internap Network Services C
AS13559 - LOVULLOASN - LoVullo Associates, Inc.,US | 美国 => AS11351 - RR-NYSREGION-ASN-01 - Time Warner Cable
AS13578 - MDASSOCIATES-MAIN - MDAssociates, Inc.,US | 美国 => AS36086 - TELX-LEGACY - Telx,US | 美国 亚特兰大
AS13718 - SOLUSLP - SOLUS ALTERNATIVE ASSET MANAGEMENT LP,US | 美国 => AS13789 - INTERNAP-BLK3 - Internap Netw
AS13764 - KPU-CA-AS-1 - Kwantlen Polytechnic University,CA | 加拿大 => AS271 - BCNET-AS - BCnet,CA | 加拿大
AS13870 - AAML-ASN - Aureus Asset Management, LLC,US | 美国 => AS21755 - RBS-BOSTON - Sidera Networks LLC US
AS13912 - COMMTOUCH-INC - Commtouch Inc.,US | 美国 => AS12182 - INTERNAP-2BLK - Internap Network Services Corp

```
1804     /* http://www.cogentco.com/en/network/looking-glass */
1805     public static function parseByCOGENTCOCOM($host, $area)
1806     {
1807         $datas = array(
1808             'vie' => ['奥地利', '维也纳'],
1809             'anr' => ['比利时', '安特卫普'],
1810             'bru' => ['比利时', '布鲁塞尔'],
1811             'sof' => ['保加利亚', '索非亚'],
1812             'hkv' => ['保加利亚', '哈斯科沃'],
1813             'bsl' => ['瑞士', '巴塞尔'],
1814             'zrh' => ['瑞士', '苏黎世'],
1815             'prg' => ['捷克', '布拉格'],
1816             'ber' => ['德国', '柏林'],
1817             'bre' => ['德国', '不来梅'],
1818             'dus' => ['德国', '杜塞尔多夫'],
1819             'fra' => ['德国', '法兰克福'],
1820             'ham' => ['德国', '汉堡'],
1821             'muc' => ['德国', '慕尼黑'],
1822             'nue' => ['德国', '纽伦堡'],
1823             'drs' => ['德国', '德累斯顿'], //
    http://zh.wikipedia.org/wiki/%E5%BE%B7%E7%B4%AF%E6%96%AF%E9%A1%BF%E6%9C%BA%E5%9C%BA
                                  德累斯顿机场
1824             'cph' => ['丹麦', '哈根'],
1825             'tll' => ['爱沙尼亚', '塔林'],
1826             'agp' => ['西班牙', '马拉加'], // Malaga
1827             'bcn' => ['西班牙', '巴塞罗那'],
1828             'bio' => ['西班牙', '毕尔巴鄂'],
1829             'grx' => ['西班牙', '格拉纳达'],
1830             'mad' => ['西班牙', '马德里'],
1831             'mjv' => ['西班牙', '穆尔西亚'], // Murcia
1832             'ovd' => ['西班牙', '卡斯特里利翁'], // Asturias Airport
1833             'vlc' => ['西班牙', '瓦伦西亚'],
```

123.113.10.0



永泰社区公园
清河
G6
上清桥
大树园
楼兰姑娘
奥林匹克森林公园北园
花田野趣
傲城融富中心
瑞普大厦
北京朝来农艺园
来广营村
京承高速
宏昌竣佳休闲公园
善各庄
香江高尔夫球中心
五环
仰山桥
北苑桥
顾家庄桥
十友园
来广营艺术园
和平大厦写字楼
马南里公园
潜流湿地
奥林匹克森林公园
仰山公园
北湖渠路
弘高大厦
S12
国门医院
学知轩
北京民众眼科医院
北京京城皮肤病医院
爱慕大厦
望湖公园
G101
观复
中国农业大学(东校区)
北沙滩
林萃路
中国科学技术馆
马哥孛罗
北美国际商务中心
S11
大屯
清华东路
北京林业大学
洲际酒店
地铁15号线
绿地中心
五元桥
黑桥村
中国矿业大学
解放军三0六医院
国家体育馆
亚运村
中安盛业大厦
京投大厦
北京奥运主场鸟巢
望京
福码大厦
望京soho
望京公园
梦公园
中国铁道博物馆
环铁艺术城
电通时代文化广场
影格视觉
中国音乐学院
北辰时代大厦
北京科技大学
悠乐汇
学院桥
四环
健翔桥
北辰西桥
安慧桥
惠新东桥
花家地
大山子
798艺术区
北京航空航天大学
京民大厦
小关
望京桥
燕东大厦
G101
东八间房村文化公园
何家坟
牡丹园
北环中心
花家地
丽都花园
电子城科技大厦
小坝河
北京电影学院
北京豪威大厦
北京化工大学
皇冠假日酒店
四得公园
颐堤港公园
将府公园
西坝
蓟门桥
北太平庄
三环
安贞
安贞大厦
和平东桥
霄云桥
歌华开元大酒店
北广大厦
国展
北京邮电大学
柳荫公园
鹏润大厦
康静
人定湖公园
江苏大厦
三元桥
国航大厦
环形山
东风公园
单店
中央财经大学
北京交通大学
安定医院
红都商务中心
地坛公园
建达大厦
百灵大厦
三元东桥
亮马桥
崔家村
醉公坟
德胜门桥
地铁2号线
S12
新东路
燕莎
北京和平墙
国际金融博物馆
姚家园公园
北京交通大学(东校区)
西直门
宁夏大厦
京城大厦
北京北站
后海公园
地铁8号线
北新桥
东直门
东环广场
幸福写字楼
姚家园路
平房村
新七彩商城
地安门
屯三里
朝阳公园桥
石佛营
行宫酒店
康铭大厦
工人体育场
团结湖
北京妇产医院
北大第一医院
东城区政府
西四
新世纪商务中心
甜水园
红领巾公园
星河湾四季会公园
外交学院
北海公园
地铁6号线
华侨大厦商务楼
团结湖公园



=117.136.0.0
延庆县
北京市
昌平区
怀柔区
密云县
顺义区
平谷区
海淀区
朝阳区
东城区
西城区
石景山区
丰台区
门头沟区
通州区
大兴区
房山区
三河市
大厂回族自治县
香河县
定陵机场
首都国际机场
北京南苑机场
北安河机场
密云机场
六环
京平高速
京沈高速
京昆高速
京张高速
十三陵镇
南邵镇
百善镇
流村镇
阳坊镇
上庄镇
温泉镇
北七家镇
燕丹乡
小口镇
孙河乡
金盏乡
东坝乡
常营回族乡
豆各庄乡
黑庄户乡
台湖镇
旧宫镇
瀛海镇
黄村
青云店镇
长子营镇
采育镇
魏善庄镇
庞各庄镇
定福庄乡
安定镇
长阳镇
良乡镇
城关街道
周口店镇
石楼镇
窦店镇
韩村河镇
岳各庄镇
长沟镇
张坊镇
王佐镇
潭柘寺镇
军庄镇
妙峰山镇
大台街道
清水镇
斋堂镇
雁翅镇
大安山乡
南窖乡
霞云岭乡
蒲洼乡
河北镇
五里坨
广宁街道
新镇
向阳街道
迎风街道
北石槽镇
赵全营镇
牛栏山镇
北小营镇
马坡镇
杨镇
张镇
大兴庄镇
马昌营镇
俸伯乡
北务镇
马坊镇
高楼镇
齐心庄镇
李旗庄镇
燕郊镇
杨庄镇
皇庄镇
陈府乡
蒋辛屯镇
西集镇
漷县镇
牛堡屯镇
大杜社镇
于家务回族乡
永乐店镇
安平镇
钳屯乡
安头屯镇
五百户镇
河西务镇
牛镇
下伍旗镇
怀北镇
北房镇
桥梓镇
三渡河乡
九渡河镇
渤海镇
黄花城乡
大庄科
西田各庄镇
河南寨镇
巨各庄镇
东邵渠镇
大华山镇
刘家店镇
峪口镇
大榆树镇
八达岭镇
康庄镇
狼山乡
东花园镇
北辛堡镇
土木镇
桑园镇
官厅镇
瑞云观乡
西崔村
兴寿
G6
G7
G45
G101
G102
G103
G104
G106
G107
G108
G109
G110
G111
G1
G4
G95
S11
S15
S32
S50
S201
S204
S212
S213
S217
S220
S228
S271
S308
S311
S321
S330
S361
S371


BGP 安全

BGP 方面的网络安全问题

AS2146,AS3266,AS7512,AS9380,AS9804,AS10123,AS17440,AS18644,AS24142,AS24196,AS37217,AS37962,AS49597,AS52478,AS52523,AS55830,AS56119,AS131472,AS131788,AS197329,AS200002,AS200439,AS201288,AS203406,AS203496
AS24155,AS63849

202.97.64.0 查询

IPIP.NET

AS	IP	INFO
AS49597	202.97.64.0/19	ENDAV-AS , BG

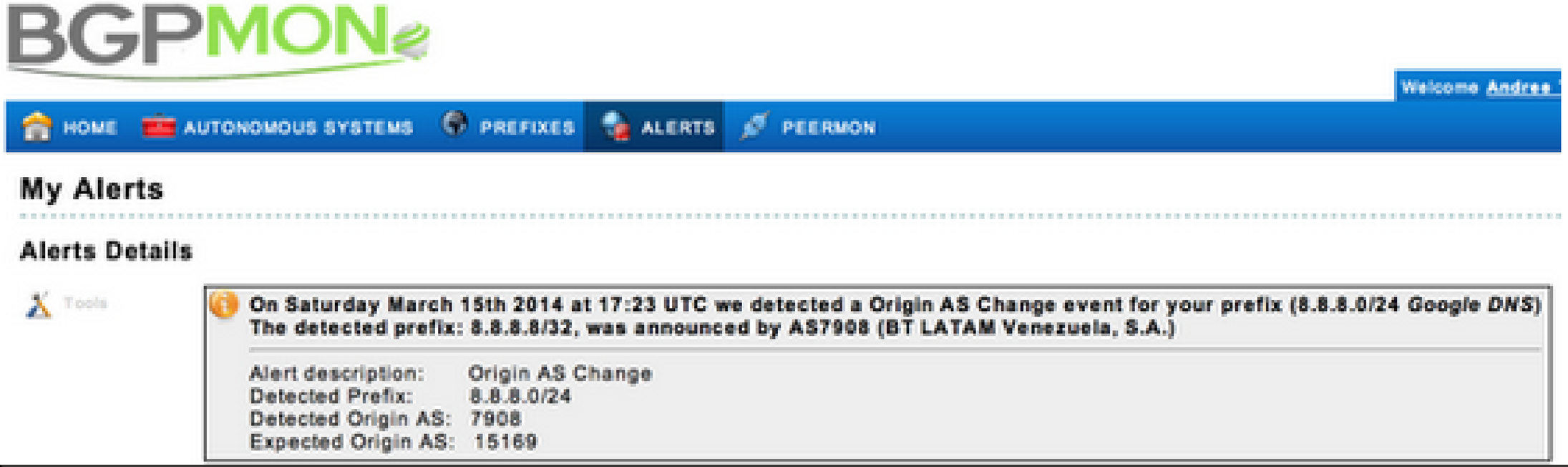
宫一鸣cn

2014-9-1 14:49 来自 微博 weibo.com

观测到黑客在互联网骨干bgp注入广播未启用网段，然后用来发垃圾邮件，发完垃圾邮件后bgp路由撤回，系统下线；由于这些网段根本没有正式启用，不在任何黑名单上，所以用来成功逃避垃圾邮件的黑名单机反制。有些佩服这个小思路。

Google DNS 8.8.8.8/32 was hijacked for ~22min yesterday, affecting networks in Brazil & Venezuela #bgp #hijack #dns pic.twitter.com/wlBuui8dwO

Reply Retweet Favorite More



BGPMON 今年监控数据：

07/2016 : 481

06/2016 : 1671

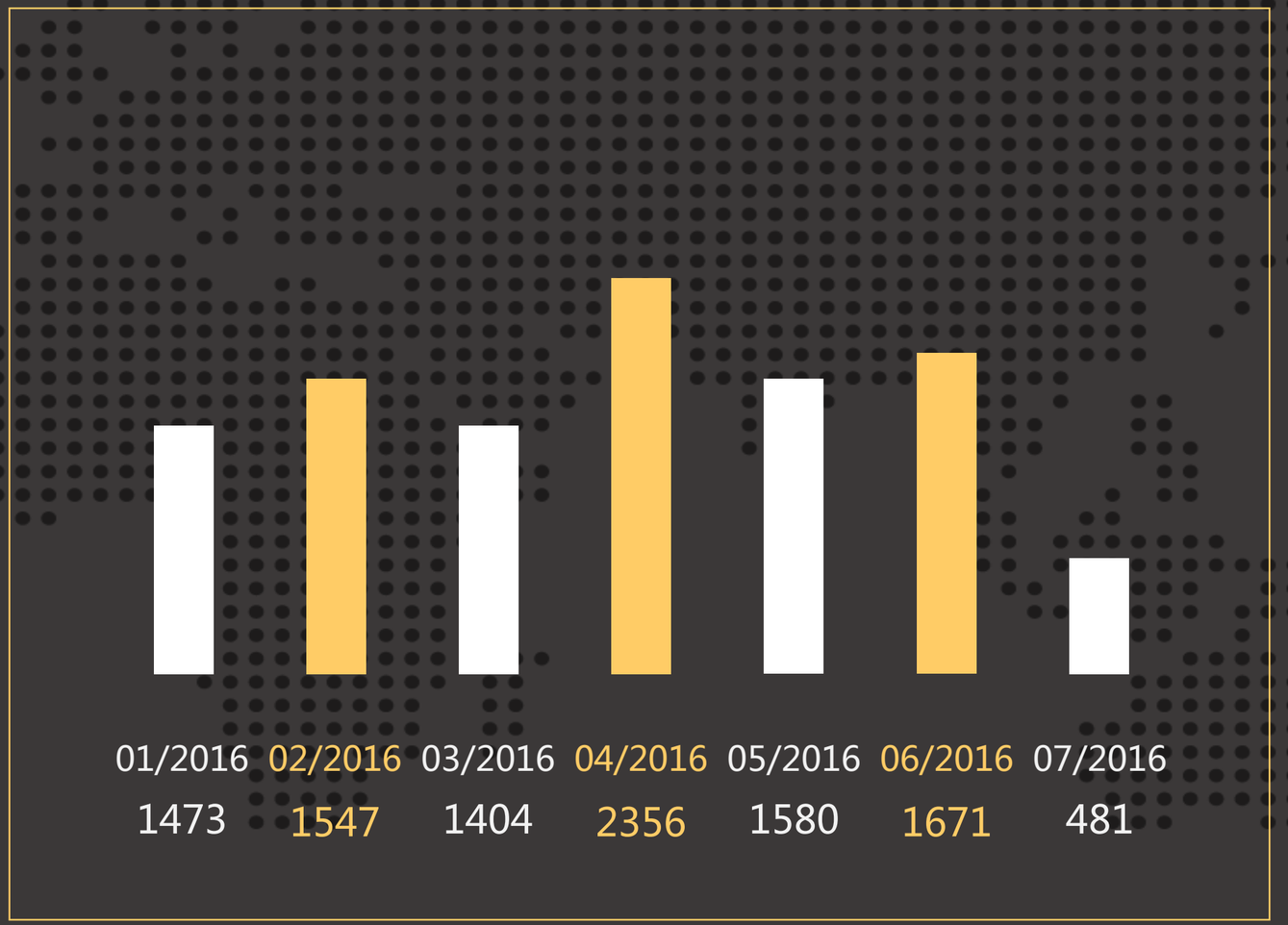
05/2016 : 1580

04/2016 : 2356

03/2016 : 1404

02/2016 : 1547

01/2016 : 1473



宫一鸣cn

2015-5-28 09:56 来自 微博 weibo.com

国内的巨头公司和国外的巨头公司"整体"网络水平差距应该是明显存在的。侧面印证下：阿里招聘 网页链接 搜索bgp和mpls,命中全0，对应amazon招聘 网页链接 命中188和40 搞技术的自傲很正常，不过保持清醒还是必要的，别把自己都给忽悠了（sorry拿阿里举例了，国内都一样）

收藏 | 32 | 10 | 6

希望与各公司共同探讨 BGP 安全

IDC IP 列表数据

价值与用途

黑来的主机用起来不够方便，自有主机才是王道。

用途？

1、流量控制（含防 DDOS）

丢弃低价值流量

2、流量识别

搜索引擎与各种爬虫

广告作弊

电商羊毛党

金融与支付风控

IDC IP 列表的制作

1、WHOIS 数据，通过注册信息来判断该拥有者的情况；
2、BGP 数据，通过 AS 信息判断该 AS 所有者的情况；
3、DNS 数据，我们采集了全球各类型网站域名进行解析，再并且对 IP 进行聚合处理；
4、自有的端口扫描与协议检测的数据；
5、基于以上数据，我们再根据 traceroute 的数据进行严格推测；
6、基于合作伙伴以及网友的反馈。

IDC IP 列表的的注意事项

1、不是黑名单，而是灰名单，结合业务数据使用；

中国特色的第三方出口；

各种默认开启浏览器代理，各种奇葩业务；

企业专线与 IDC 运维人员。

2、覆盖度：

精力有限，目前以中国互联网公司需求为优先。

3、数据量：

确认数据：450000+ 个 C 段；

猜测数据：440000+ 个 C 段。

端口扫描与协议检测

端口扫描与协议检测

1、全网 IPV4；

2、35 个常见端口；

3、14 种常见协议；

4、快速部分 2 - 3 天滚动更新，慢速部分 15 – 30 天滚动更新。

5、正在增加端口所属服务的细节描述。

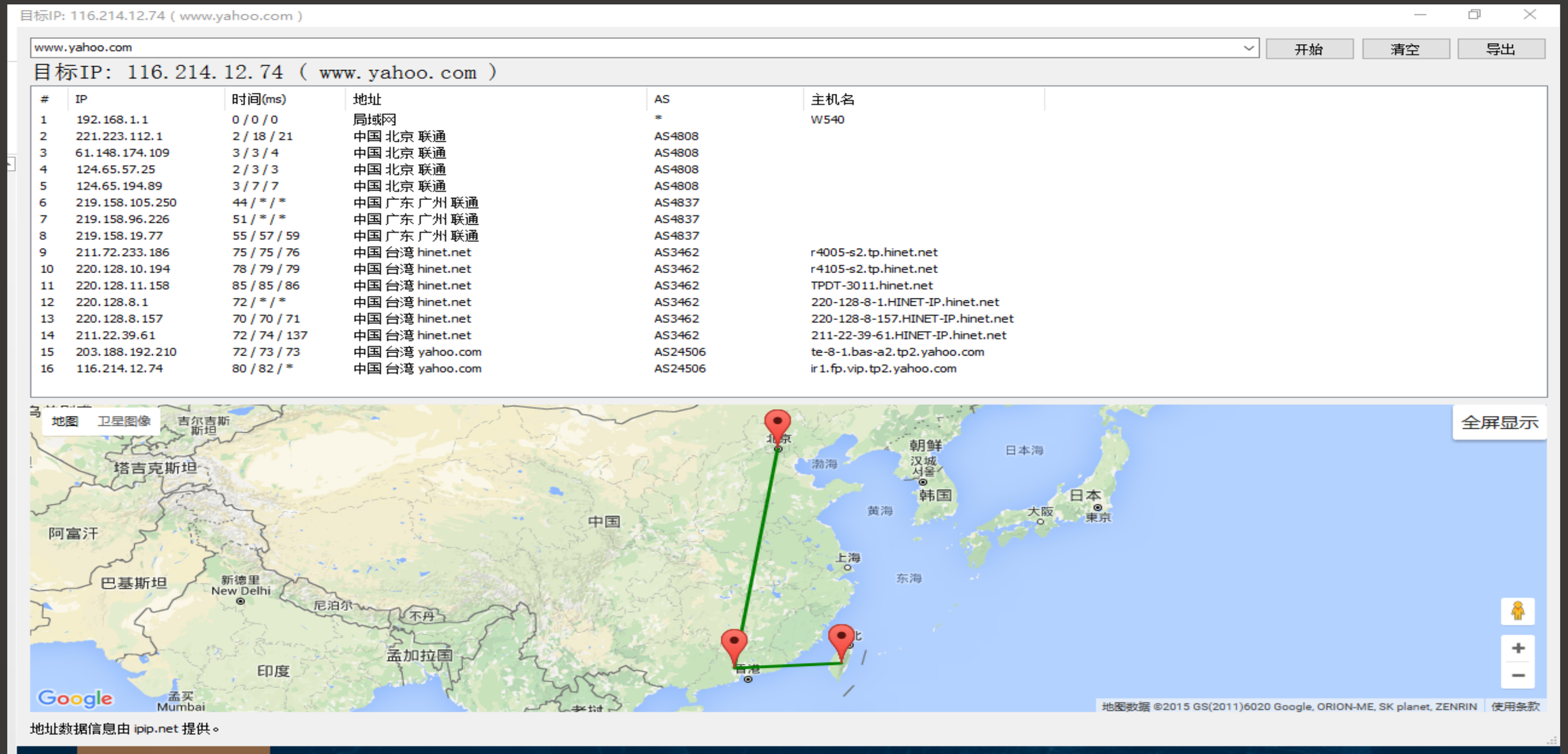
6、即将推出代理服务数据库。

7、未来提供 API 查询。

工具介绍 Best Trace

http://www.ipip.net/download.html

Win & Android & iPhone/iPad & Mac



日本东京 | www.linode.com | 查看

目标 IP：72.14.180.202 监测点赞助商：Linode

跳数	IP	主机名	地区（仅供参考）	AS号（仅供参考）	时间（毫秒）
1	106.187.33.3	106.187.33.3	日本东京	AS2516	0.4 / 0.5 / 0.7
2	124.215.199.125	124.215.199.125	日本东京	AS2516	0.6 / 0.7 / 0.7
3	124.215.194.177	otejbb206.int-gw.kddi.ne.jp	日本东京	AS2516	2 / 2 / 2
4	203.181.100.178	pajbb002.int-gw.kddi.ne.jp	美国帕洛阿尔托	AS2516	119.8 / 119.9 / 119.9
5	124.211.34.130	ix-pa7.kddnet.ad.jp	美国帕洛阿尔托	AS2516	110.8 / 110.8 / 110.9
6	50.97.16.45	xe-0-1-1.bbr01.eq01.pal01.networklayer.com	美国帕洛阿尔托	AS36351*	111 / 110.9 / 110.9
7	173.192.18.242	ae3.bbr02.eq01.sjc02.networklayer.com	美国圣何塞	AS36351*	105 / 105 / 105
8	173.192.18.151	ae0.bbr02.cs01.lax01.networklayer.com	美国加利福尼亚州洛杉矶	AS36351*	112.5 / 112.3 / 112.3
9	173.192.18.166	ae7.bbr01.cs01.lax01.networklayer.com	美国加利福尼亚州洛杉矶	AS36351*	117.5 / 119.2 / 119.2
10	173.192.18.140	ae19.bbr01.eq01.dal03.networklayer.com	美国达拉斯	AS36351*	149.9 / 149.9 / 149.9
11	173.192.18.227	po31.dsr02.dllstx3.networklayer.com	美国达拉斯	AS36351*	142.8 / 142.8 / 142.6
12	70.87.255.70	po32.dsr02.dllstx2.networklayer.com	美国达拉斯	AS21844	161.4 / 161.4 / 161.4
13	70.87.254.78	po2.car01.dllstx2.networklayer.com	美国达拉斯	AS21844	214.4 / 209.2 / 208.9
14	67.18.7.90	router1-dal.linode.com	美国达拉斯	AS21844	161.8 / 162.3 / 161.9
15	72.14.180.202	www-loadbal1.linode.com	美国达拉斯	AS36351*	149.9 / 149.9 / 149.9


地图
卫星图像
全屏显示
俄罗斯
哈萨克斯坦
蒙古
中国
日本
韩国
印度
伊朗
阿富汗
巴基斯坦
沙特阿拉伯
土耳其
缅甸
泰国
越南
菲律宾
马来西亚
印度尼西亚
巴布亚新几内亚
澳大利亚
新西兰
加拿大
美国
墨西哥
古巴
委内瑞拉
哥伦比亚
巴西
秘鲁
玻利维亚
巴拉圭
智利
阿根廷
格陵兰岛
冰岛
英国
爱尔兰
法国
西班牙
葡萄牙
摩洛哥
北太平洋
太平洋
北大西洋
大西洋
印度洋
白令海
鄂霍次克海
日本海
东海
南海
渤海
黄海
墨西哥湾
加勒比海
哈德森湾
Baffin Bay
东西伯利亚海
喀拉海
阿拉伯海
孟加拉湾
珊瑚海
Google
地图数据 ©2016 GS(2011)6020 Google, INEGI
使用条款

联通（广州-洛杉矶）


地图
卫星图像
全屏显示
北京电信（洛杉矶）
Google

北京移动（法兰克福-阿姆斯特丹-伦敦-纽约）


地图
卫星图像
全屏显示
北京铁通（香港-新加坡-洛杉矶）
Google
地图数据 ©2016 GS(2011)6020 Google, INEGI
使用条款


地图
卫星图像
全屏显示
北京教育网（香港-洛杉矶）
Google
地图数据 ©2016 GS(2011)6020 Google, INEGI
使用条款


寻找小伙伴
。。。

2 交流时间