

“

看着难，做着更难 —— IP 库背后的故事

”



@高春辉 · 2017.5

DRoP: DNS-based Router Positioning

Bradley Huffaker, Marina Fomenkov, kc claffy

DDec: DNS Decoding

Ken Keys, Bradley Huffaker



DHS site visit
June 18, 2014



DHS site visit
June 18, 2014



Homeland Security



最常会被问到的几个问题？

- 1、做IP库还不简单？抓公开的 WHOIS 信息或者找几个库做投票就够了啊。
- 2、IP库应该做到每个IP都可以具体到一个很明确的位置才对，你们为什么做不到？
- 3、你们数据里的经纬度为什么不是这个IP的经纬度？
- 4、IP库应该是大公司做的更好，或者是运营商自己最清楚啊。为什么是你们做这个？

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，为查询计，我们需要这样一个数据库。

IP 库是什么?



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

用途

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 /
- Digital Element / db-ip.com

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



如何验证 IP 库？

最快速的办法：



查询 8.8.8.8 的标注是否为 GOOGLE

原因：因为 8.8.8.0/24 和 8.8.4.0/24 两组 IP 使用了 ANYCAST 技术，这两组 IP 在全球部署有多组服务器，根据网络情况为网友提供就近服务，所以无法标注到具体地区，具体 ANYCAST 技术详情请自行搜索。

[IP 数据库分享计划](#)

IPIP.net数据

您输入的IP: 8.8.8.8

GOOGLE GOOGLE

其它参考数据

来自淘宝的数据	来自腾讯的数据	来自新浪的数据
国家: 美国 地区: 省份: 城市: 运营商:	美国 未知	国家: 美国 省份: 加利福尼亚 城市: Mountain View 运营商: IP段: 8.8.8.0 - 8.8.8.255
中国互联网广告行业IP库	纯真IP库数据	MaxMind GeoLite2
北美洲 美国 美国 美国	美国 加利福尼亚州圣克拉拉县山景市谷歌公司DNS服务器	美国 加利福尼亚州 芒廷维尤

为什么要单独维护一个，而不是用其它版本呢？





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

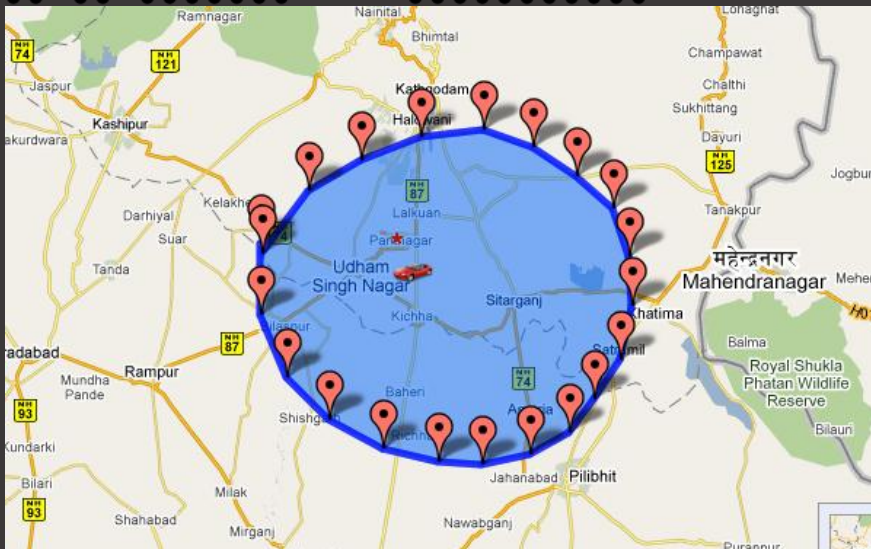
IP 数据去掉非公网 IP，大概有 36 亿个需要维护。全球相关机房上万个，相关公司上十万个。变动是正常的，工作量超大，你跟得上否？



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。

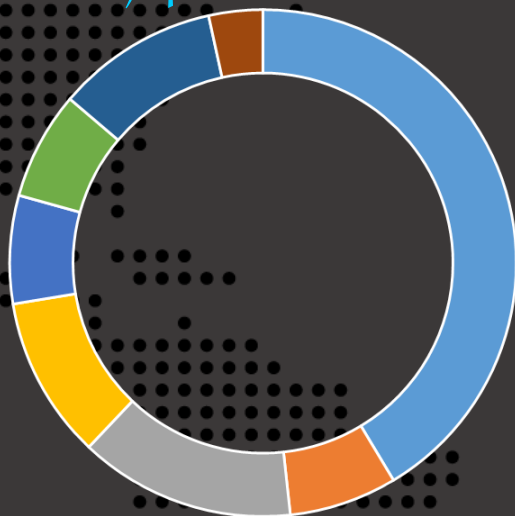
长期是一个力气活

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 300+ 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 **82000+ 条**，
实际投入使用的有 **58000+ 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 300+ 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 (2017.5)



原始文本数据文件
提交 50000+ 次
共 600000+ 行



IPIP.NET 网站代码
10000+ 行。



命令行与客户端代码
25000+ 行



BGP 不重复数据量
10000+ 万行。



手工整理的
HOST 定义文件
15000+ 行



生成一次全球 ASN
相关数据文件的时
间, 2 小时。*

* BGP 涉及文本数据量, 32GB, TRACEROUTE 涉及文本数据量, 300GB。

* 主体运行在荷兰阿姆斯特丹和北京的服务器上

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
2016071300	344778	2016-07-13 00:43:18
当前 IP 数据库版本	数据库条目数	数据库最后更新时间
2017051213	601948	2017-05-12 13:13:53

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→

12.216.20.0-12.216.20.255,12.216.105.0-12.216.105.255,12.230.56.0-12.230.57.255,45.40.0.0-45.40.0.255,45.40.1.0-45.40.1.255,45.40.2.0-45.40.2.255,45.40.3.0-45.40.3.255,45.40.4.0-45.40.4.255,45.40.5.0-45.40.5.255,45.40.10.0-45.40.10.255,45.40.14.0-45.40.14.255,45.40.15.0-45.40.15.255,104.192.156.0-104.192.157.255,104.192.159.0-104.192.159.255↓

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, 4154
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 | 七牛云 Qiniu IT大咖说 知识分享平台

AS11992 - CENTENNIAL-PR - Centennial de Puerto Rico,PR | 波多黎各 => AS7018 - ATT-INTERNET4

AS12061 - 24HOURFITNESS - 24 Hour Fitness USA, Inc.,US | 美国 => AS23005 - SWITCH-COMMUNICATIONS - SWITCH COMMUNICATIONS

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 | LIMELIGHT

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 MONACO

AS12488 - KRYSTAL Krystal Solutions LLP,GR | 英国 梅德斯通 => AS24958 - TBSH The Bunker Secure Hosting Limited

AS12501 - NORRNOD An Internet Exchange point and ISP in Umea, Sweden,SE | 瑞典 于默奥 => AS2119 - TELENOR-NEXT

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 MediaServicePlus

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 C

AS13100 - TELECITYGROUP INTERNATIONAL LIMITED,IE | 爱尔兰 => AS15830 - TELECITY-LON TELECITYGROUP INTERNATIONAL

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 Corporation

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 Co

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 不列颠哥伦比亚

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'],  
1824          'cph' => ['丹麦', '德累斯顿机场', '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'],
```

日本东京

www.linode.com

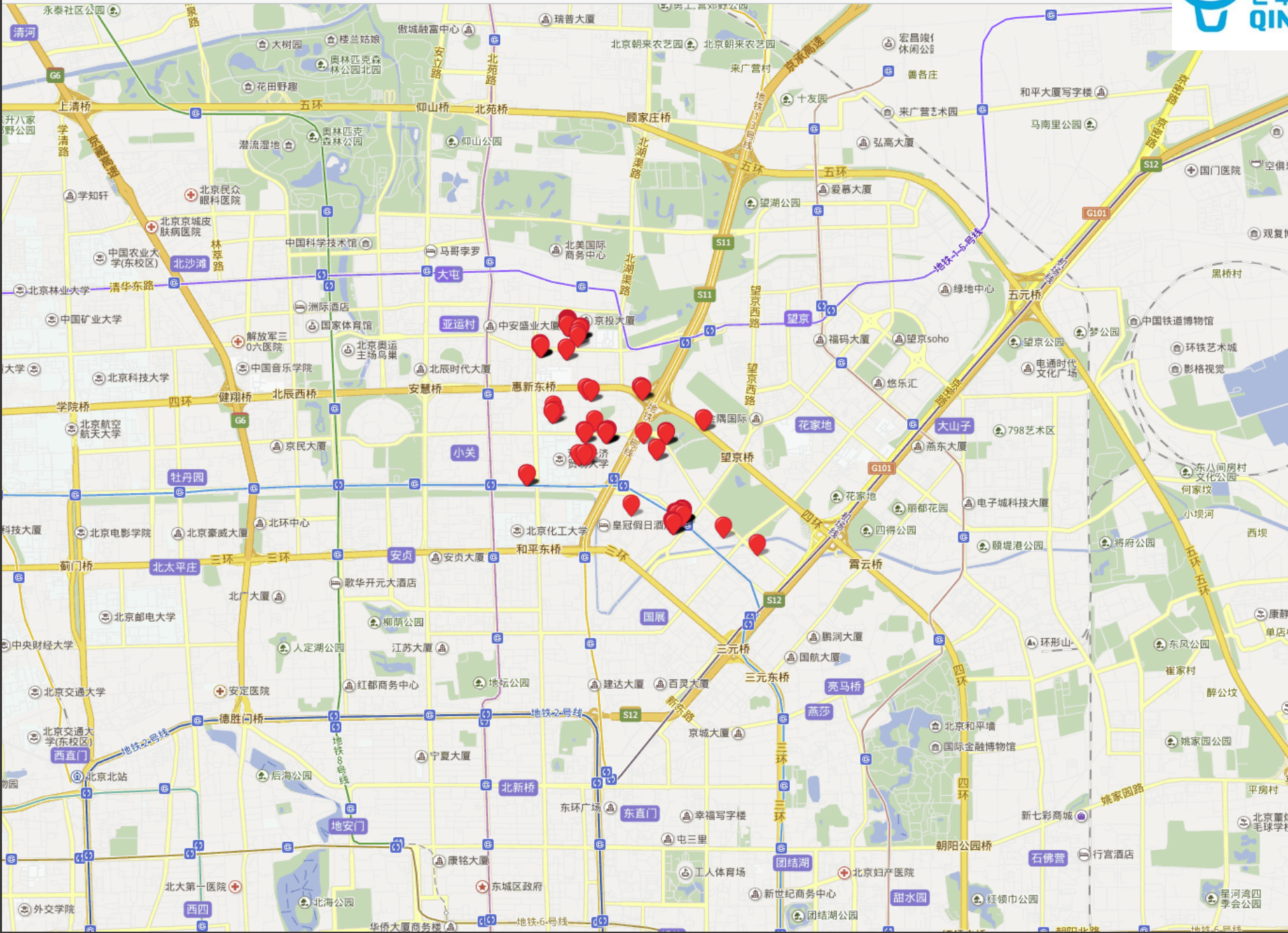
查看

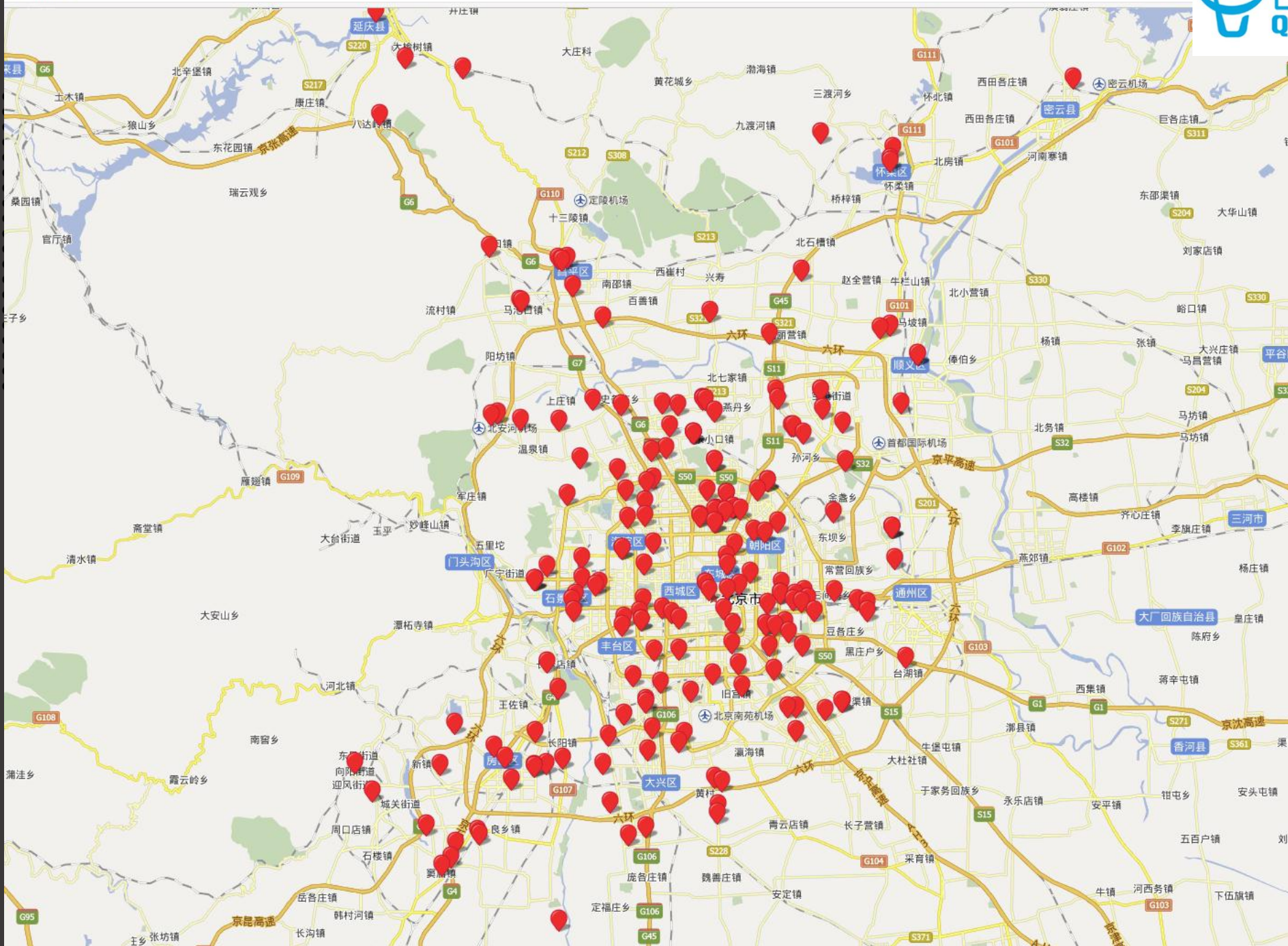


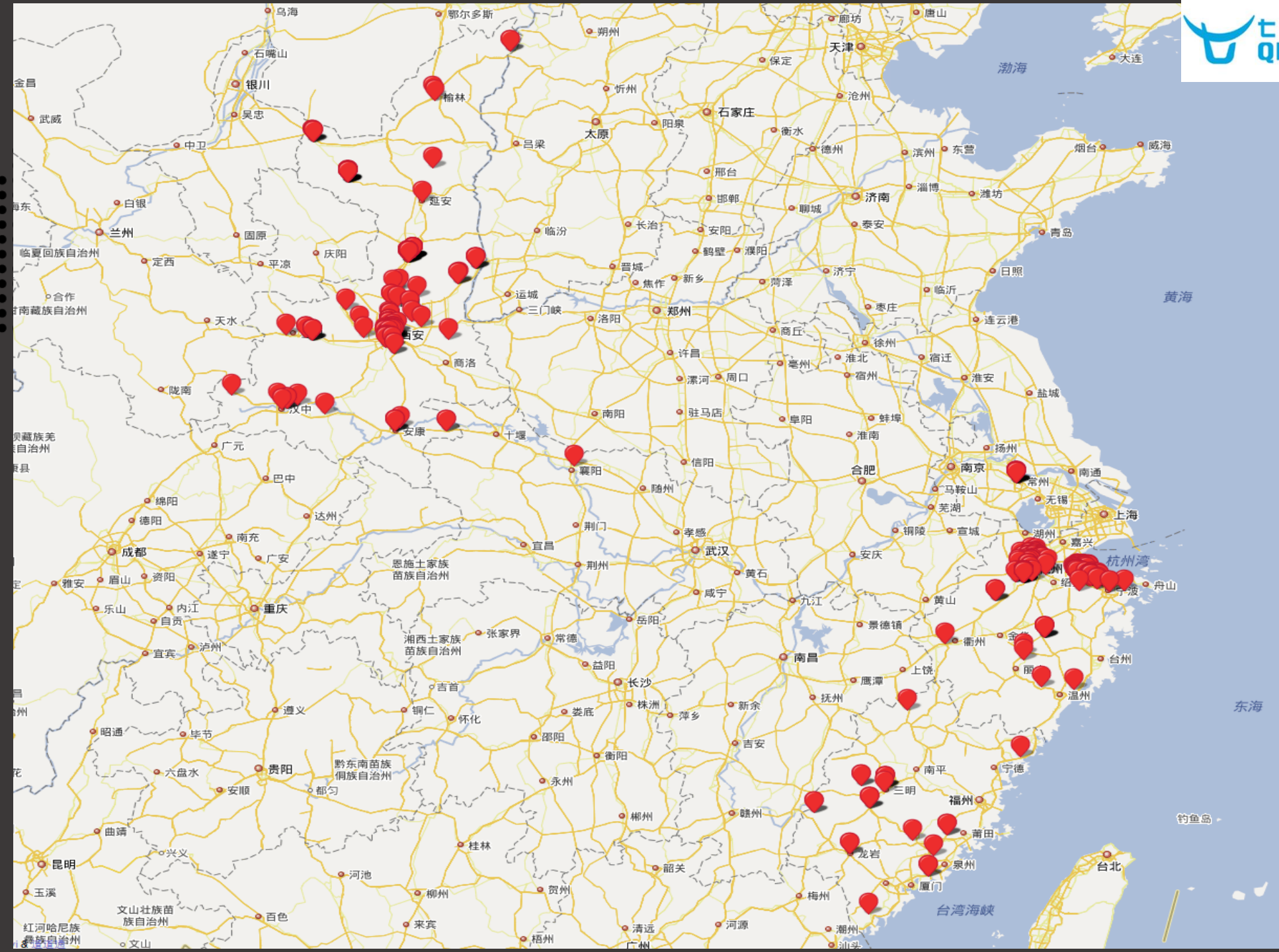
目标 IP: 72.14.180.202

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







互动一下

LAX



互动一下

AMS

互动一下

STO



互动一下

NRT

细分数据之：中国区县数据库



价值与用途



中国的**地市级**精度，有 **300** 多个；

中国的**区县级**精度，有 **3000** 多个；

中国的**互联网用户**在 **8 亿**左右，你说哪个更合适？

我们目前的中国区县数据库基本上可以覆盖一半左右的中国 IP 段。1.92亿 vs 3.88亿

1.13.176.0→1.13.176.255→	中国→	吉林→	长春→	绿园区→	220106→	7.1→125.25582→	43.88045↓
1.13.177.0→1.13.177.255→	中国→	吉林→	长春→	朝阳区→	220104→	4→125.2883→	43.83339↓
1.13.178.0→1.13.178.255→	中国→	吉林→	长春→	绿园区→	220106→	10.6→125.25582→	43.88045↓
1.13.179.0→1.13.179.255→	中国→	吉林→	长春→	绿园区→	220106→	3.9→125.25582→	43.88045↓
1.13.180.0→1.13.180.255→	中国→	吉林→	长春→	绿园区→	220106→	1044.9→125.25582→	43.88045↓
1.13.181.0→1.13.181.255→	中国→	吉林→	长春→	绿园区→	220106→	9.5→125.25582→	43.88045↓
1.13.182.0→1.13.182.255→	中国→	吉林→	长春→	绿园区→	220106→	8.5→125.25582→	43.88045↓
1.13.183.0→1.13.183.255→	中国→	吉林→	长春→	绿园区→	220106→	2.7→125.25582→	43.88045↓
1.13.184.0→1.13.184.255→	中国→	吉林→	长春→	绿园区→	220106→	6.9→125.25582→	43.88045↓
1.13.185.0→1.13.185.255→	中国→	吉林→	长春→	绿园区→	220106→	8.4→125.25582→	43.88045↓
1.13.186.0→1.13.186.255→	中国→	吉林→	长春→	绿园区→	220106→	7.2→125.25582→	43.88045↓
1.13.187.0→1.13.187.255→	中国→	吉林→	长春→	绿园区→	220106→	6.3→125.25582→	43.88045↓
1.13.188.0→1.13.188.255→	中国→	吉林→	长春→	绿园区→	220106→	7.3→125.25582→	43.88045↓
1.13.189.0→1.13.189.255→	中国→	吉林→	长春→	绿园区→	220106→	9.1→125.25582→	43.88045↓
1.13.190.0→1.13.190.255→	中国→	吉林→	长春→	绿园区→	220106→	3.4→125.25582→	43.88045↓
1.13.191.0→1.13.191.255→	中国→	吉林→	长春→	绿园区→	220106→	5.7→125.25582→	43.88045↓
1.13.192.0→1.13.192.255→	中国→	辽宁→	大连→	金州区→	210213→	19.3→121.71893→	39.1004↓
1.13.193.0→1.13.193.255→	中国→	辽宁→	大连→	金州区→	210213→	23.8→121.71893→	39.1004↓
1.13.194.0→1.13.194.255→	中国→	辽宁→	大连→	金州区→	210213→	4.3→121.71893→	39.1004↓
1.13.195.0→1.13.195.255→	中国→	辽宁→	大连→	金州区→	210213→	19.4→121.71893→	39.1004↓
1.13.196.0→1.13.196.255→	中国→	辽宁→	大连→	金州区→	210213→	22.9→121.71893→	39.1004↓
1.13.197.0→1.13.197.255→	中国→	辽宁→	大连→	金州区→	210213→	21.4→121.71893→	39.1004↓
1.13.198.0→1.13.198.255→	中国→	辽宁→	大连→	金州区→	210213→	31.6→121.71893→	39.1004↓
1.13.199.0→1.13.199.255→	中国→	辽宁→	大连→	金州区→	210213→	22.9→121.71893→	39.1004↓
1.13.200.0→1.13.200.255→	中国→	辽宁→	大连→	金州区→	210213→	19→121.71893→	39.1004↓
1.13.201.0→1.13.201.255→	中国→	辽宁→	大连→	金州区→	210213→	2.9→121.71893→	39.1004↓
1.13.202.0→1.13.202.255→	中国→	辽宁→	大连→	金州区→	210213→	10.9→121.71893→	39.1004↓
1.13.203.0→1.13.203.255→	中国→	辽宁→	大连→	金州区→	210213→	9.7→121.71893→	39.1004↓
1.13.204.0→1.13.204.255→	中国→	辽宁→	大连→	金州区→	210213→	14.4→121.71893→	39.1004↓
1.13.205.0→1.13.205.255→	中国→	辽宁→	大连→	金州区→	210213→	19.5→121.71893→	39.1004↓
1.13.206.0→1.13.206.255→	中国→	辽宁→	大连→	金州区→	210213→	25.8→121.71893→	39.1004↓
1.13.207.0→1.13.207.255→	中国→	辽宁→	大连→	金州区→	210213→	23.7→121.71893→	39.1004↓
1.13.208.0→1.13.208.255→	中国→	辽宁→	大连→	金州区→	210213→	16.8→121.71893→	39.1004↓

细分数据之：基站 IP 段



基站 IP 库？



大家在不使用 WIFI 网络的时候，
使用手机通过运营商提供的网络进行上网的时候，
目前方案应该都是在用户端使用私有IP，
然后对外做 NAT 转换，
这样的情况就导致大家在手机端统一使用一些 IP 段进行访问网站或者 APP。一般我们称这些相对固定的 IP 段为 基站 IP。

问题在哪儿？



国内大部分的省都是以**省级为单位**划分基站对外访问 IP，

也就是说，同样一个出口 IP，

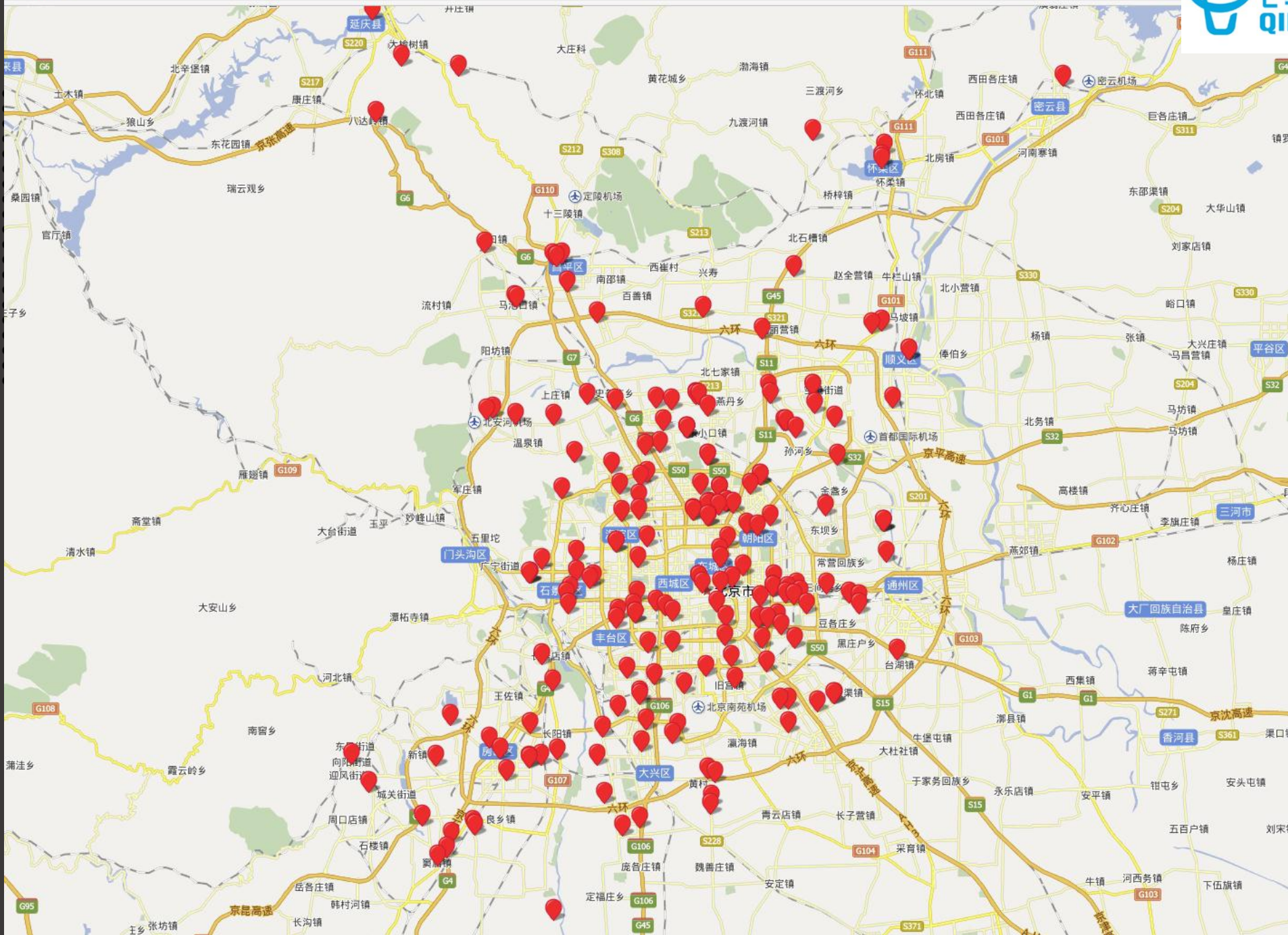
后面的对应用户可能是**跨多个城市**的。

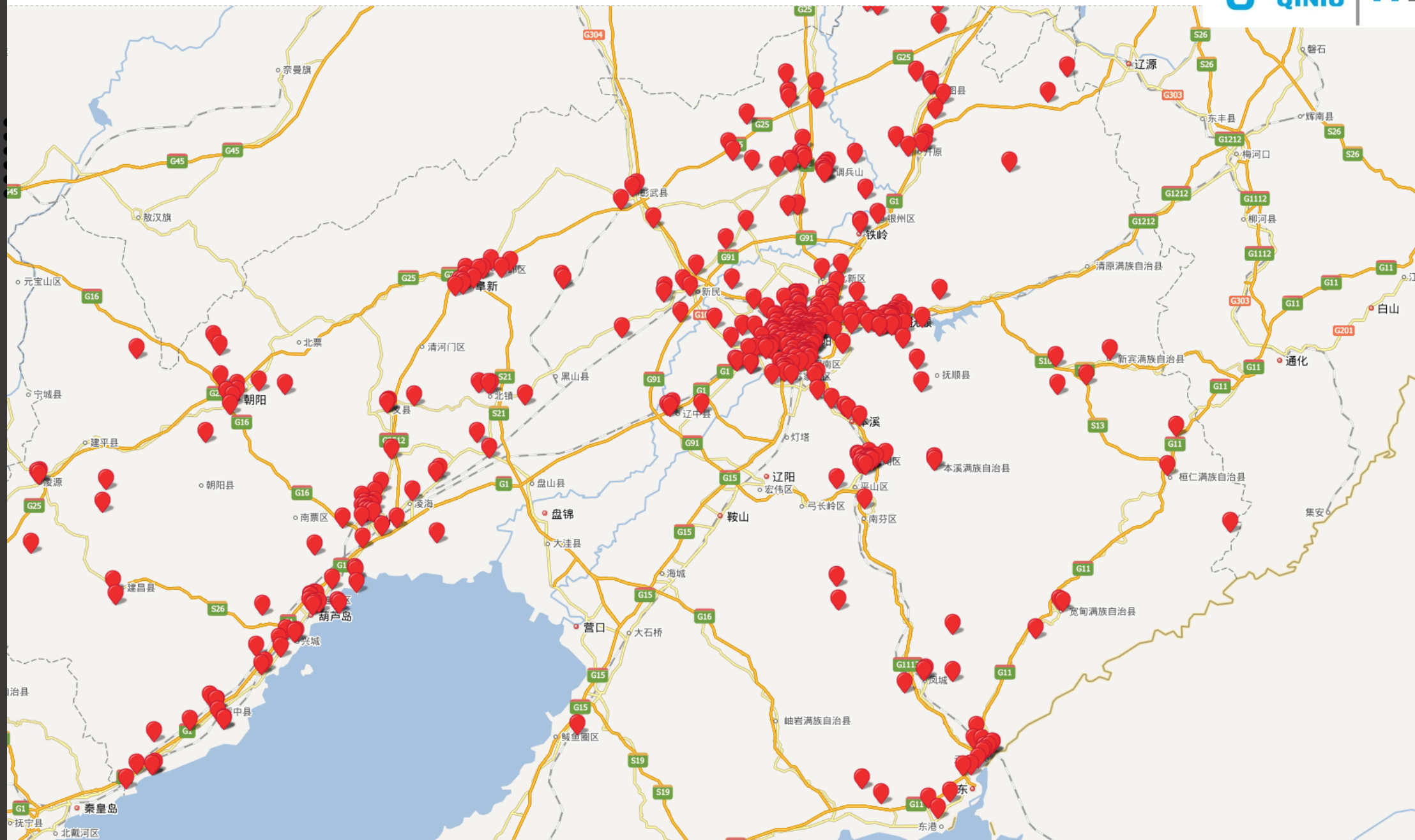
也有一部分省是按照**市一级为单位**划分的，

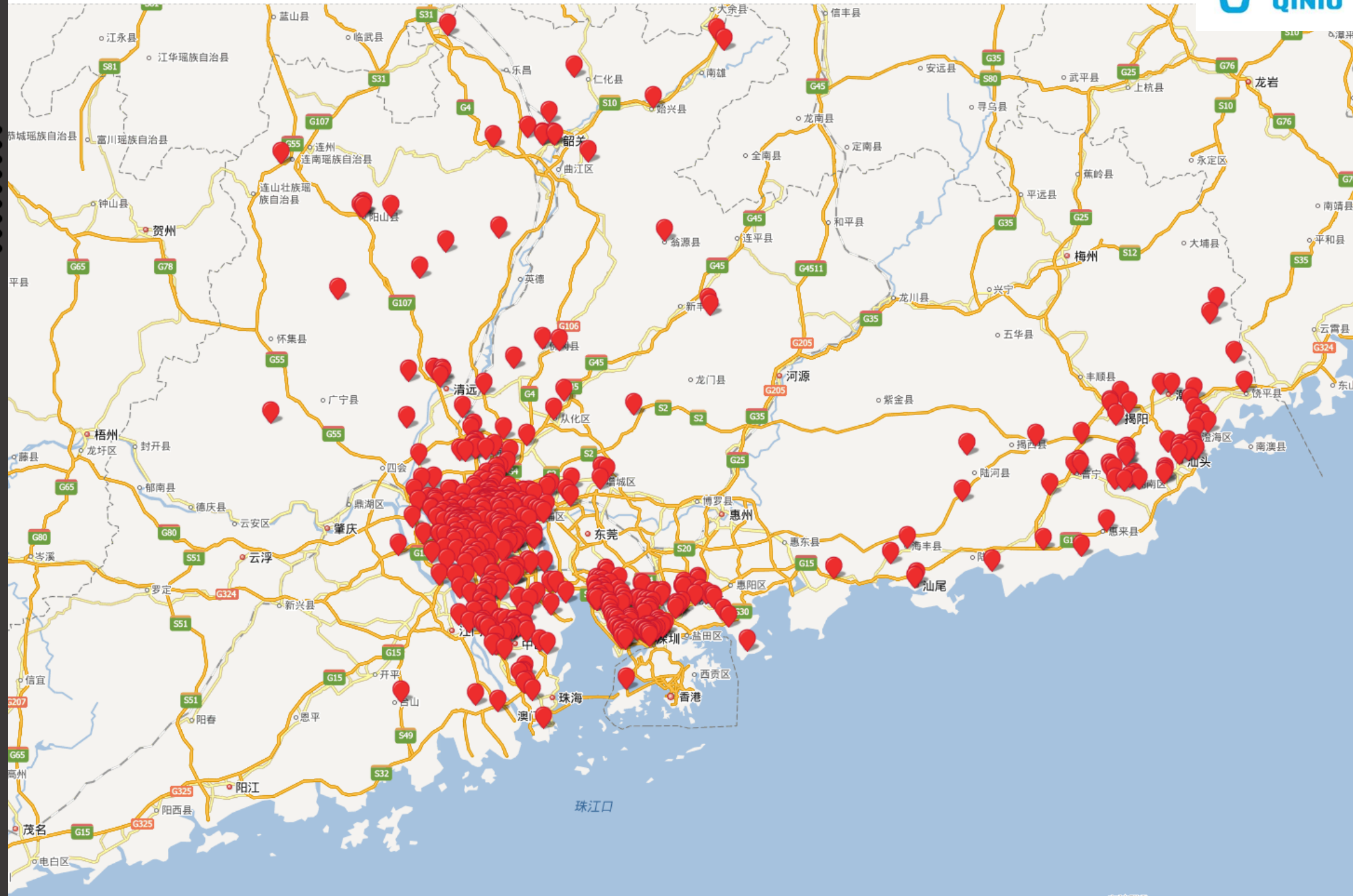
但是**位置偏远**，你估计也不会关心。

还有一部分地区是一段 IP 给两三个城市同时使用，

在我们的数据库依然没法准确到城市。







详细介绍文章请见：
<https://linux.cn/article-8277-1.html>



细分数据之：IDC IP 列表数据



价值与用途

为什么做？

黑来的机器用起来总是不够方便，自有可控主机才是王道。

用途？

1、流量控制（含防 DDOS）

电商秒杀

必要时丢弃低价值流量

2、流量识别

搜索引擎与爬虫

广告作弊

电商羊毛党

金融与支付风控（VPN）



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 的数据进行推测；
- 6、基于合作伙伴以及网友的反馈。

IDC IP 列表的注意事项

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云加速（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，以中国互联网公司需求为优先。

3、**数据量**：

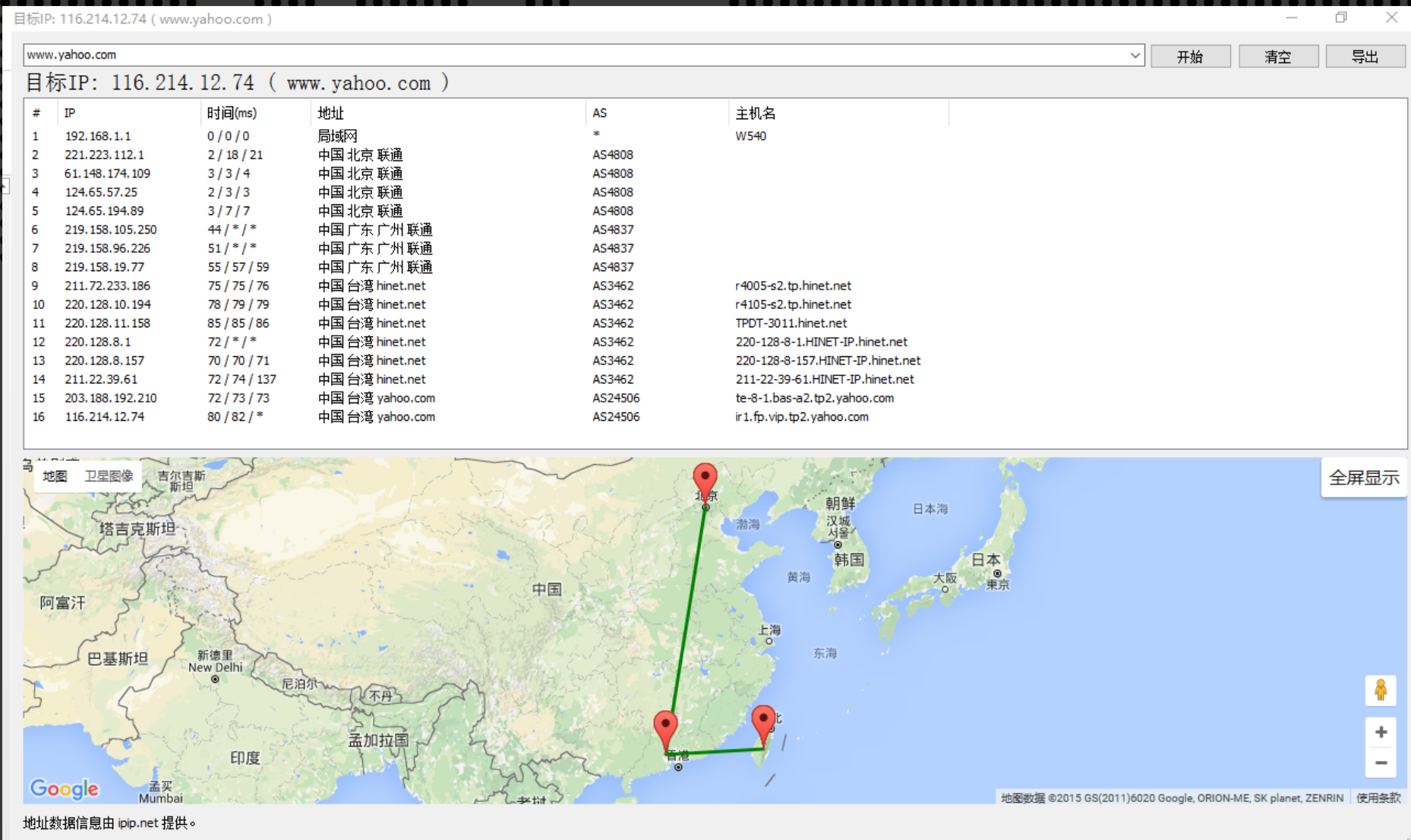
确认数据：610000 个 C 段；

预测数据：200000 个 C 段（两个预测交集部分）。

工具介绍 Best Trace

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

Win & Android & iPhone/iPad & Mac



日本东京



www.linode.com

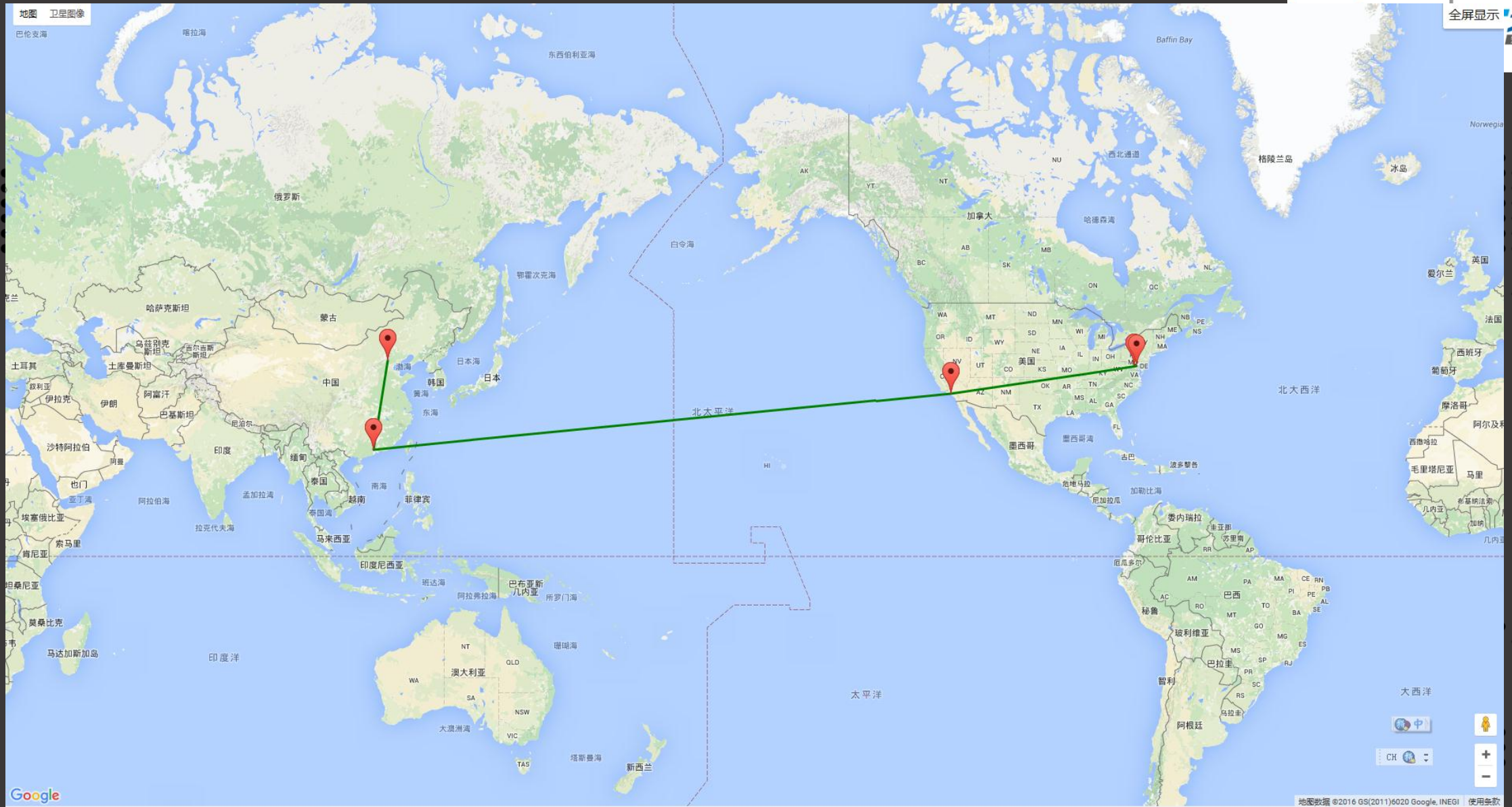
查看



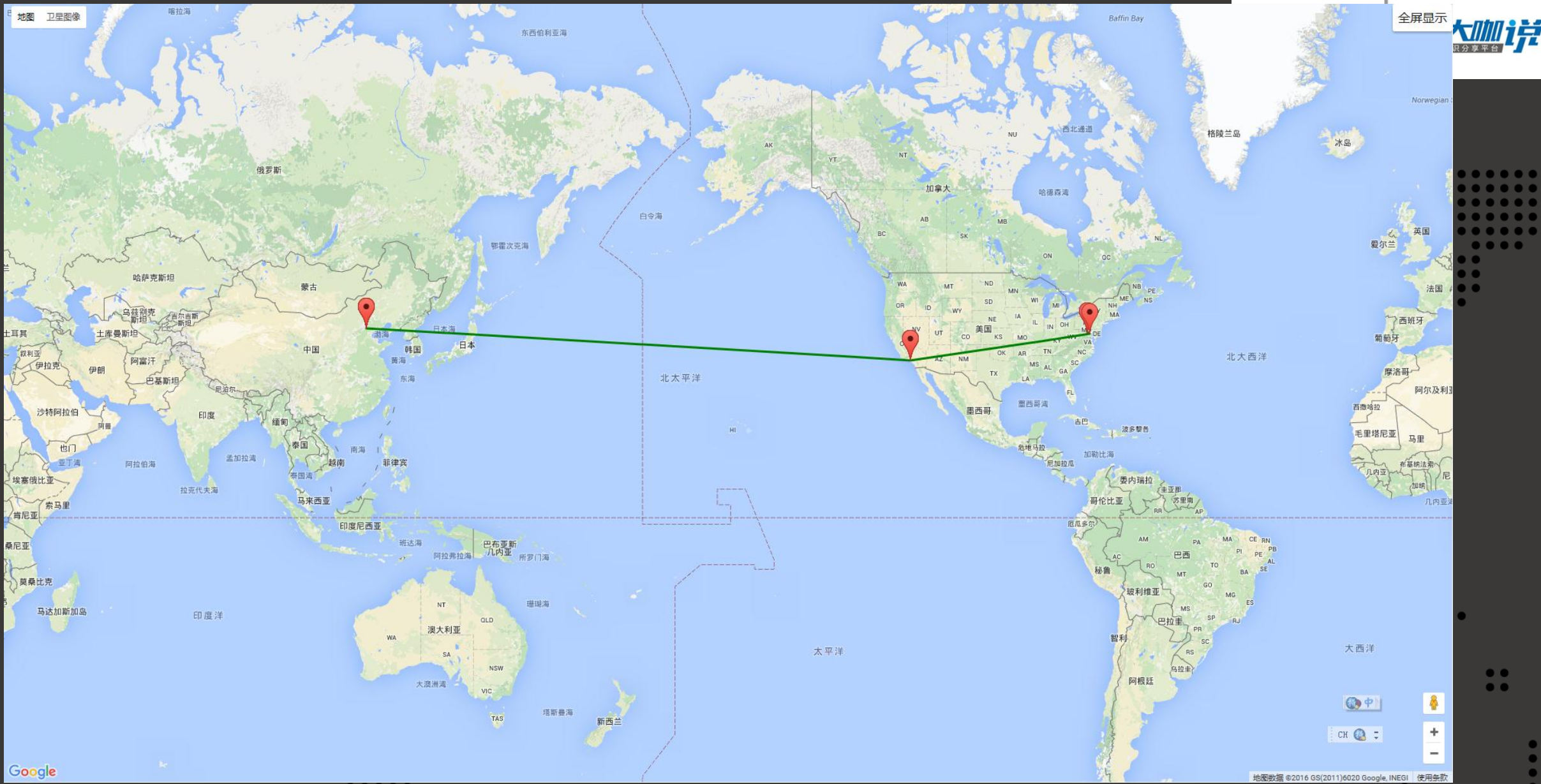
目标 IP: 72.14.180.202

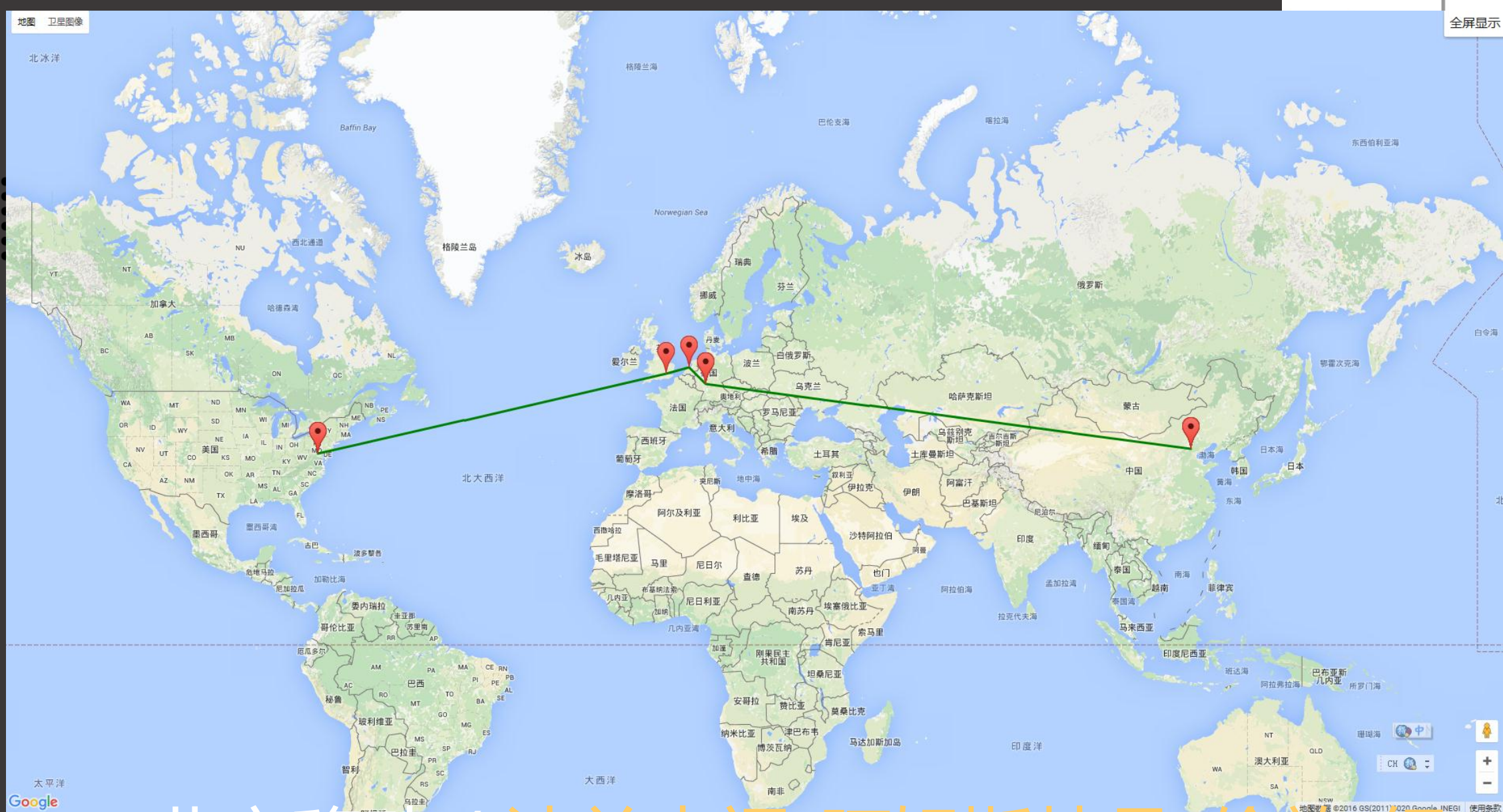
监测点赞助商: Linode

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

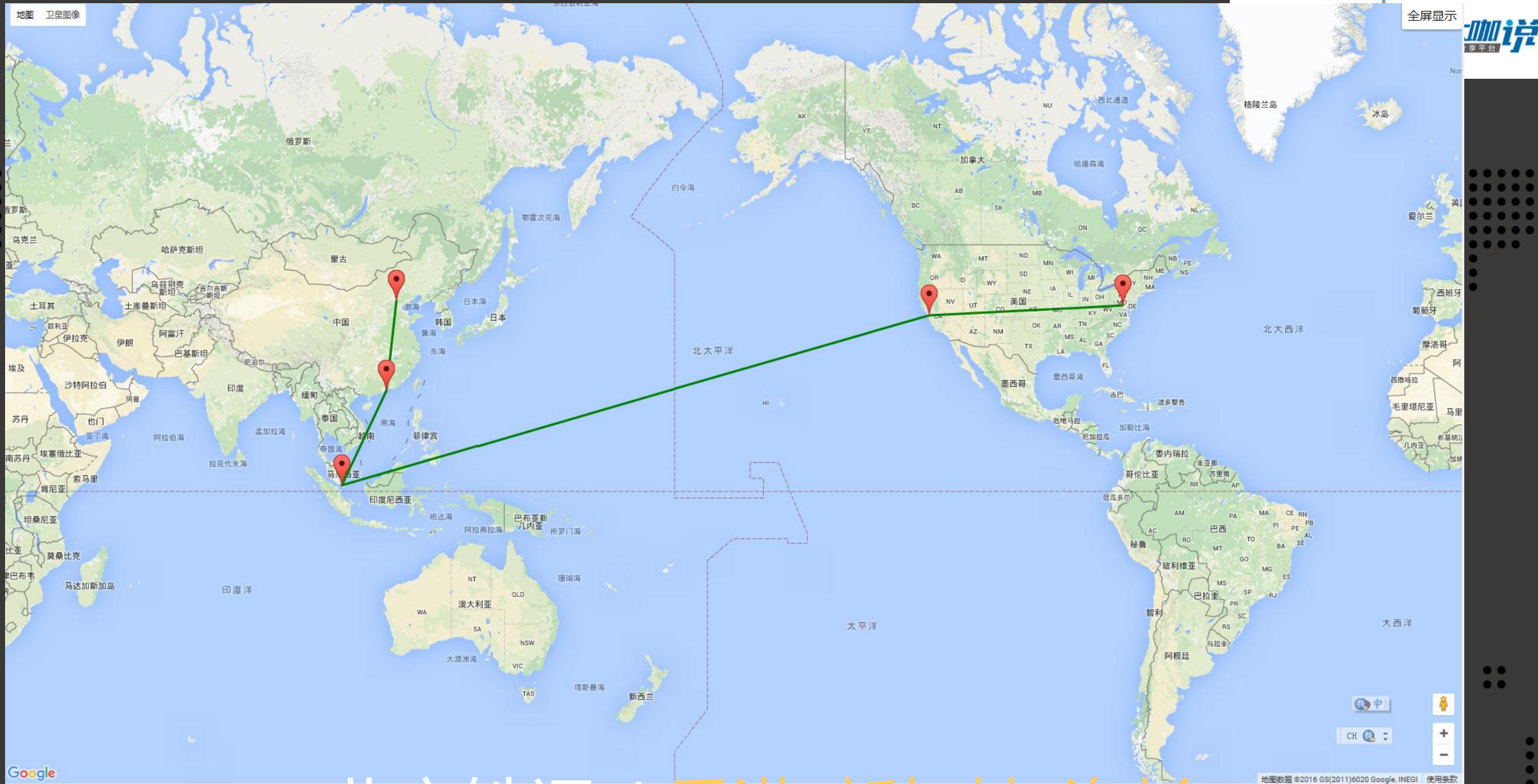


联通（广州-洛杉矶）

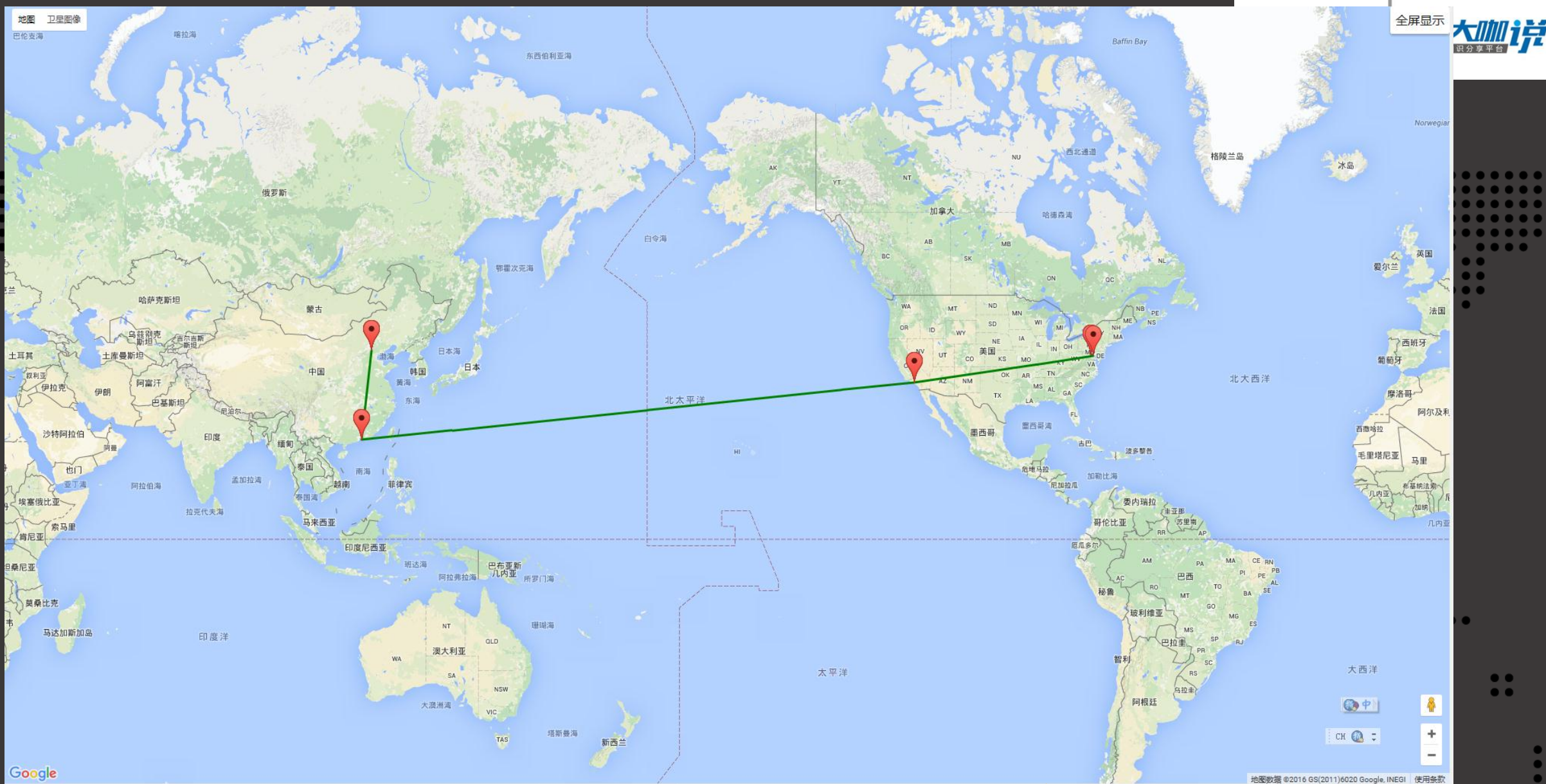




北京移动（法兰克福-阿姆斯特丹-伦敦-纽约）



北京铁通（香港-新加坡-洛杉矶）



北京教育网（香港-洛杉矶）

A wide-angle photograph of the Chicago skyline at dusk or dawn, with the Willis Tower prominently in the center. The sky is a mix of orange, pink, and blue.

去年十月份到现在：美国数据的进展～

原始数据 49058088 条，唯一化后 5017857 条，C 段后 679906 条

识别的结果如下：

只能识别到美国的 138328 条，占 20.3451%；

可以识别到州的 340770 条，占 50.1201%；

可以识别到城市的 200800 条，占 29.5334%。

以上统计数据基于 3 月 10 日的数据。



寻找小伙伴
(网络安全 & IP 数据画像分析方向)

