

Defeat Public DNS

Water

2011-09-08

SACC2011

**In a CDN' d world,
OpenDNS is the enemy!**

——国外网友

2009年12月4日

Google推出了免费的DNS服务,
并称使用Google的DNS可以加速
用户的访问速度,提升上网安全性,
且没有烦人的重定向问题

.....

大批的G粉与非G粉将
LocalDNS设成了4个8



SACC2011

随后，陆续有使用4个8的童鞋 发现网站访问速度极慢



8.8.8.8

坑爹呢，哥在TC!

nslookup www.abc.com
American IP address

90周年期间，opendns
用户反映网站打开缓慢



SACC2011

一些运营商使用了双线或者多层级DNS，也导致用户分配错误

The screenshot displays a web browser window titled "http://rpc.networkbench.com - 基调监测中心 - SeaMonkey". The browser shows a table of monitoring data for a specific IP and target. Below the table, there is a section for network performance indicators. A terminal window is open in the foreground, showing a command prompt where a user has run a command to check the logs for a specific IP address. The terminal output shows a query from a client with IP 58.240.56.26 to the target IP 210.51.29.30.

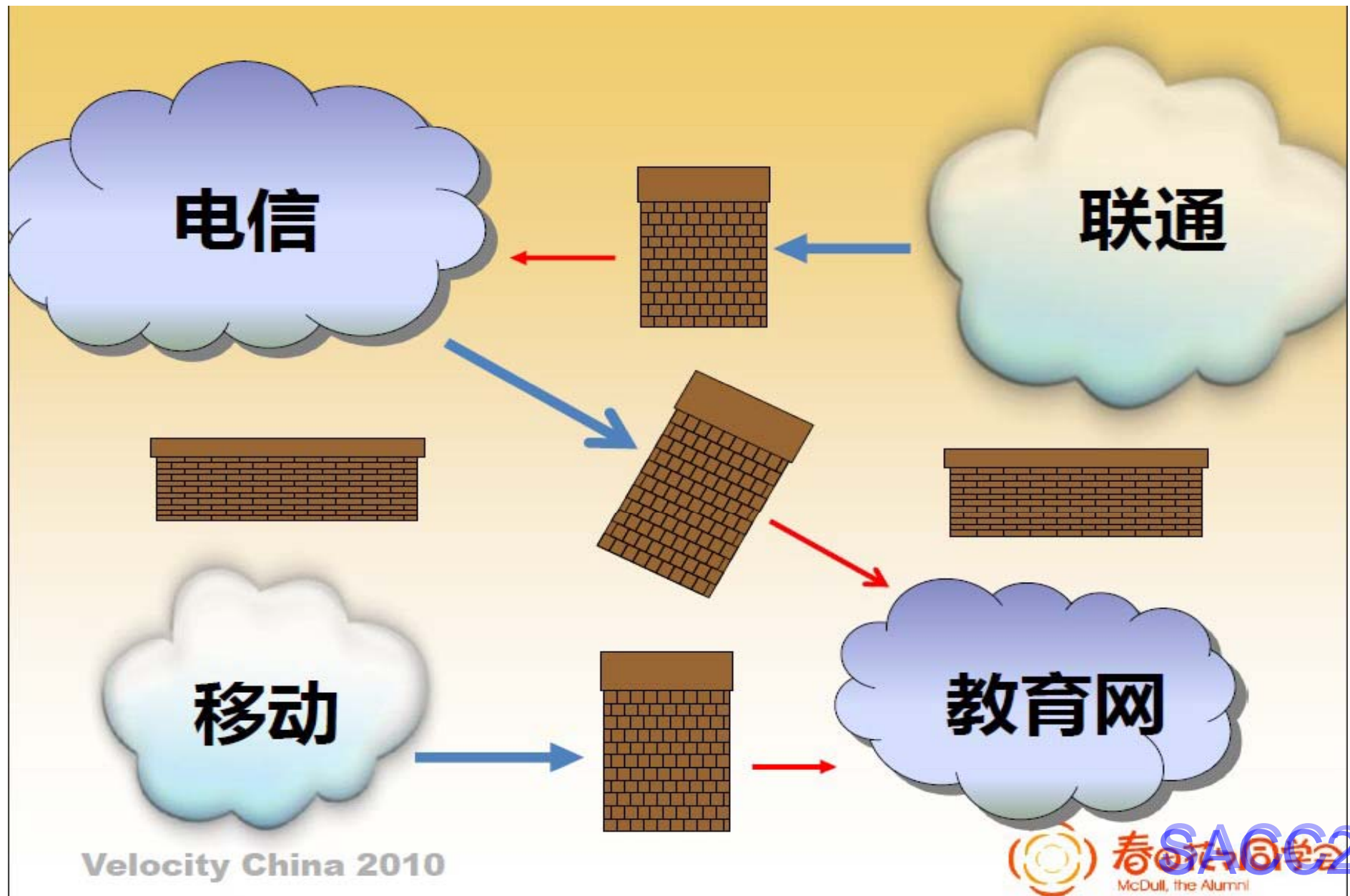
监测数据(2011年08月17日 10:58:24)	
监测时间	2011年08月17日 10:58:24
监测点IP	122.195.72.248 (常州市, 中国联通)
DNS服务器	58.241.84.5
连接方式	LastMile
操作系统	Windows XP sp3
浏览器	Internet Explorer 8
当前任务CPU使用率	3%
当前任务内存使用率	0%
平均CPU使用率	0%
平均内存使用率	0%
平均下载速度	--

监测数据(2011年08月17日 10:58:25.127)	
目标IP	210.51.29.30 (上海市, 中国联通)
HTTP Server	nginx
HTTP Via	

网络性能指标	
总下载时间	
总下载字节数	
速度(KB/s)	
首屏时间	
网络层时间	
DNS时间	
建立连接时间	
SSL握手时间	
重定向时间	

```
[root@localhost log]# tail -f gather.log |grep qwertyuiop
17-Aug-2011 10:58:25.127 queries: info: client 58.240.56.26#56909: query: qwertyuiop.gather.sdo.com IN A -EDC
```

大量用户跨运营商访问



据不完全统计：

Public DNS resolver服务器数量超过**7000**台

超过**5W**的国内用户使用国际Public DNS

超过**21W**的国内用户因为DNS混搭混指问题, 导致跨运营商访问

如何把这些用户分配到正确的节点呢？

Google DNS神马的最讨厌了,偶要把4个8指回国内！



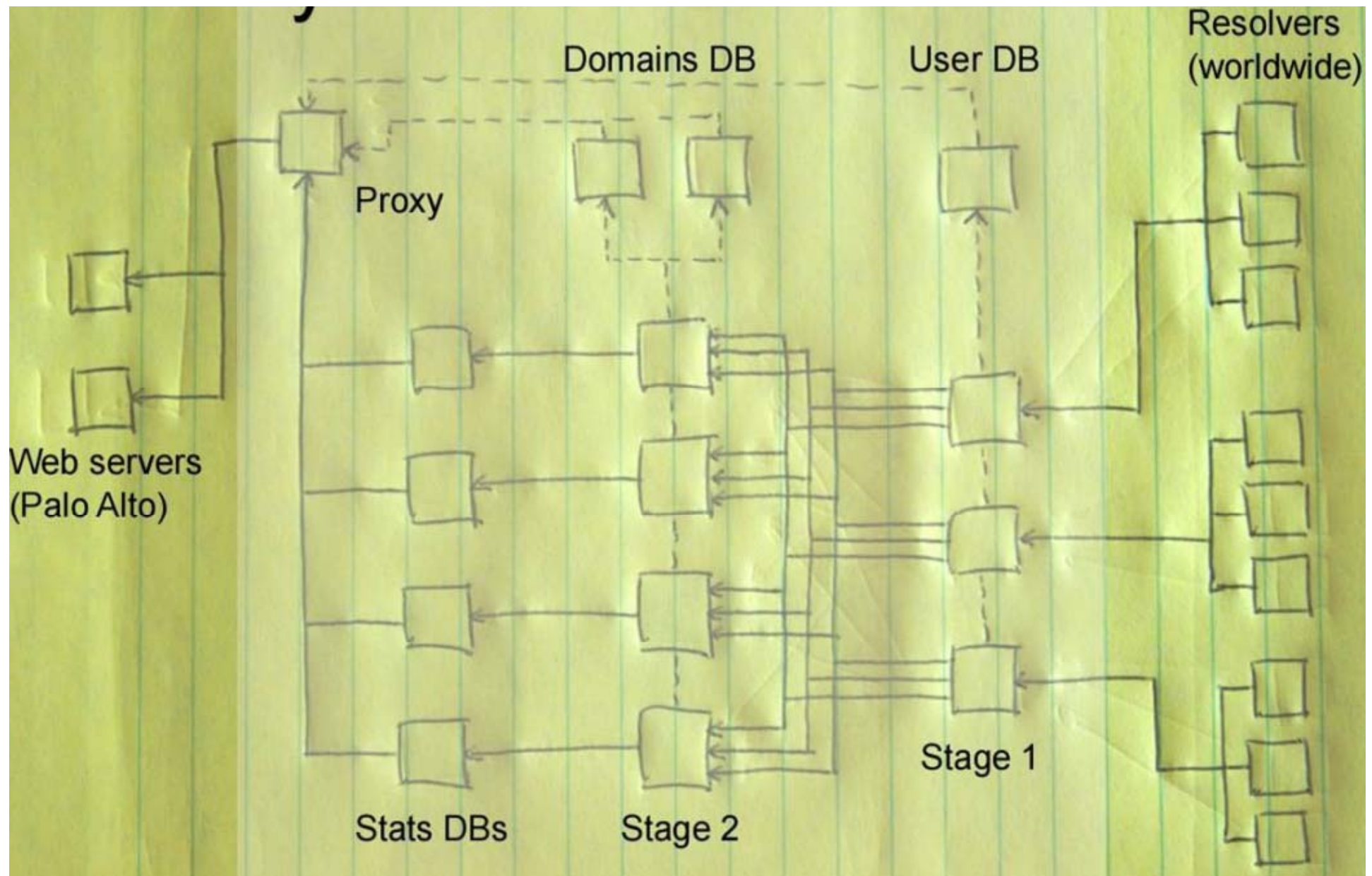
SACC2011

When a DNS resolver queries an authoritative nameserver for a CDN's IP address, **the nameserver returns an address which is closest (in network distance) to the *resolver*, not the user.**

.....

<http://code.google.com/speed/public-dns/faq.html#cdn>

SACG2011



OpenDNS architecture

SACC2011

按照resolver与用户区域的对应关系，将resolver划分到该区域，便能修正一些publicdns的用户

```
view "china" {  
    match-clients { 64.233.182.81; 64.233.182.82; };
```

.....

```
view "japan" {  
    match-clients { 64.233.182.83; };
```

.....

```
view "korea" {  
    match-clients { 64.233.182.0/24; };
```

.....

那么如何取得这个
resolver与用户区域
的对应关系呢？



Google公布了解析器IP，不同解析器负责不同区域的用户解析

(现如今Google较少维护这个Iplist)

Where are your servers currently located?

Google Public DNS servers are available worldwide.

Here are the subnets from which Google Public DNS sends requests to authoritative nameservers, and their associated IATA airport codes:

64.233.162.0/24 gru
64.233.168.0/24 iad
66.102.12.0/24 grq
72.14.202.0/24 tpe
72.14.212.0/24 dls
74.125.112.0/24 chs
74.125.114.0/24 chs
74.125.126.0/24 dls
74.125.152.0/24 tpe
74.125.154.0/24 dls
74.125.156.0/24 atl
74.125.158.0/24 atl
74.125.38.0/24 fra
74.125.42.0/24 ber
74.125.44.0/24 atl
74.125.46.0/24 atl
74.125.52.0/24 dls
74.125.64.0/24 atl
74.125.66.0/24 atl
74.125.76.0/24 grq
74.125.78.0/24 grq
74.125.86.0/24 bud
74.125.90.0/24 mrn
74.125.92.0/24 mrn
74.125.94.0/24 cbf
208.117.247.0/24 pao
209.85.142.0/24 dub
209.85.174.0/24 kul
209.85.224.0/24 cbf
209.85.226.0/24 bru
209.85.228.0/24 bru

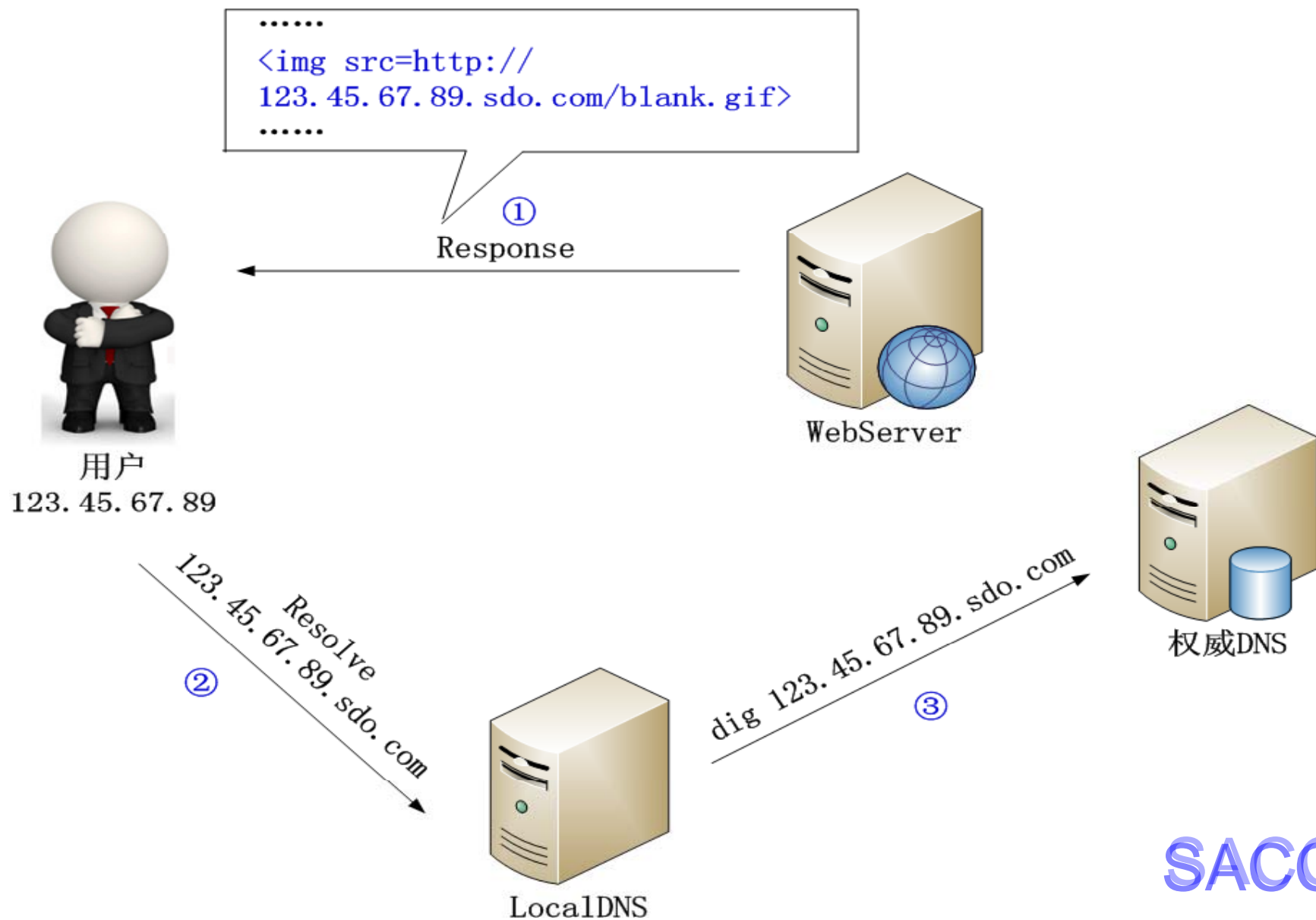
```
SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
queries: info: client 64.233.182.81#42083: query: 116.205.84.57-login.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#63690: query: 183.4.74.175-login.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#53480: query: 114.86.19.61-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#50002: query: 113.134.107.209-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#47147: query: 116.231.111.134-ecard.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#62257: query: dl.gather.sdo.com IN
queries: info: client 64.233.182.81#54217: query: 58.209.101.253-cas.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#54345: query: 113.250.38.246-cas.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#44822: query: 60.190.163.58-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#64868: query: 113.1.218.133-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#62159: query: 123.129.42.199-ecard.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#62318: query: 114.217.226.238-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#49556: query: 114.88.116.182-login.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#64998: query: 183.62.141.46-cas.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#49561: query: 202.134.92.10-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#46273: query: 61.219.80.241-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#42143: query: 114.139.26.177-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#47954: query: 113.111.125.122-cas.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#42801: query: 122.159.19.171-cas.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#43931: query: 218.1.68.98-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#48136: query: dl.gather.sdo.com IN
queries: info: client 64.233.182.81#50829: query: 219.137.115.40-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#59783: query: 219.131.129.170-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#48371: query: 117.63.107.172-dplogin.sdo.com.gather.sdo.com IN
queries: info: client 64.233.182.81#60932: query: 210.22.93.126-dplogin.sdo.com.gather.sdo.com IN
```

就绪

ssh2: AES-256 25, 9

SACC2011

获取用户与LDNS的对应关系



PHP代码：

<?

```
$ip = $_SERVER["REMOTE_ADDR"];
```

```
echo "<img
```

```
src=http://$ip.cdn.sdo.com/blank_$ip.jpg>";
```

```
echo "<br>";
```

```
echo "<img
```

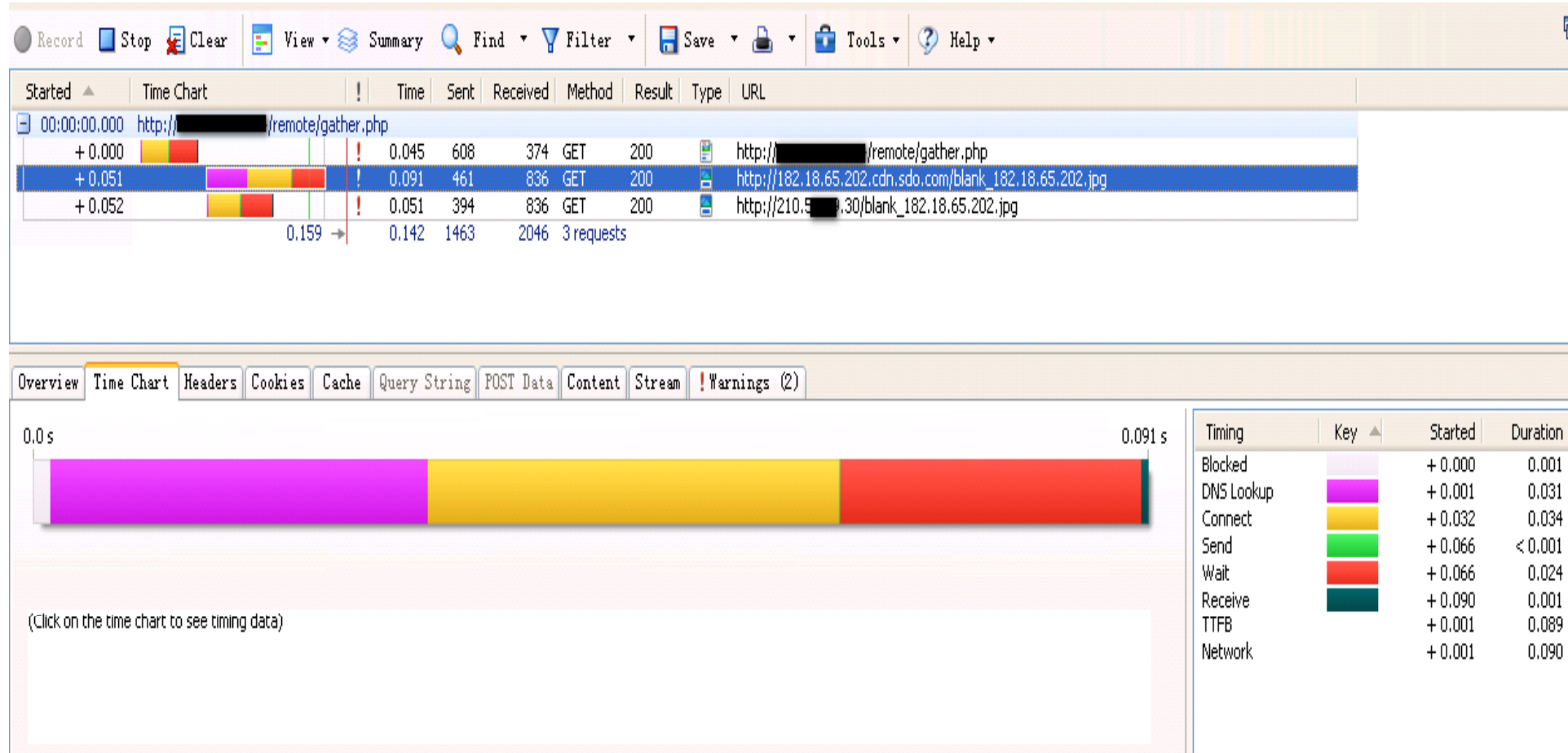
```
src=http://123.45.67.89/blank_$ip.jpg>";
```

```
?>
```

```
queries: info: client 202.101.173.146#26335: query: 115.199.226.149-login.sdo.com.gather.sdo.com IN A -P
queries: info: client 61.140.11.160#20134: query: 125.89.187.148-dplogin.sdo.com.gather.sdo.com IN A -
queries: info: client 202.101.173.146#28989: query: 115.199.226.149-login.sdo.com.gather.sdo.com IN A -P
queries: info: client 219.146.2.34#51968: query: 113.124.52.41-login.sdo.com.gather.sdo.com IN A -EDC
queries: info: client 220.167.29.230#17713: query: 125.70.133.184-ecard.sdo.com.gather.sdo.com IN A -
queries: info: client 182.151.191.100#63278: query: 125.70.133.184-ecard.sdo.com.gather.sdo.com IN A -EL
queries: info: client 202.101.173.130#18572: query: 115.199.226.149-login.sdo.com.gather.sdo.com IN A -P
```

SACG2011

Tip：对同一资源的两次访问，测量DNS解析时间



<http://yahoo.github.com/boomerang/doc/howtos/howto-8.html>

SACG2011

对于无法提供内容的CDN服务提供商，可以使用如下方法：

```
proxy_intercept_errors on;
```

```
location /favicon.ico {  
    proxy_pass http://backend;  
    error_page 404 = @gather;  
}
```

```
location @gather {  
    rewrite ^  
    http://$remote_addr.sdo.com/favicon.ico;  
    expires -1;  
}
```

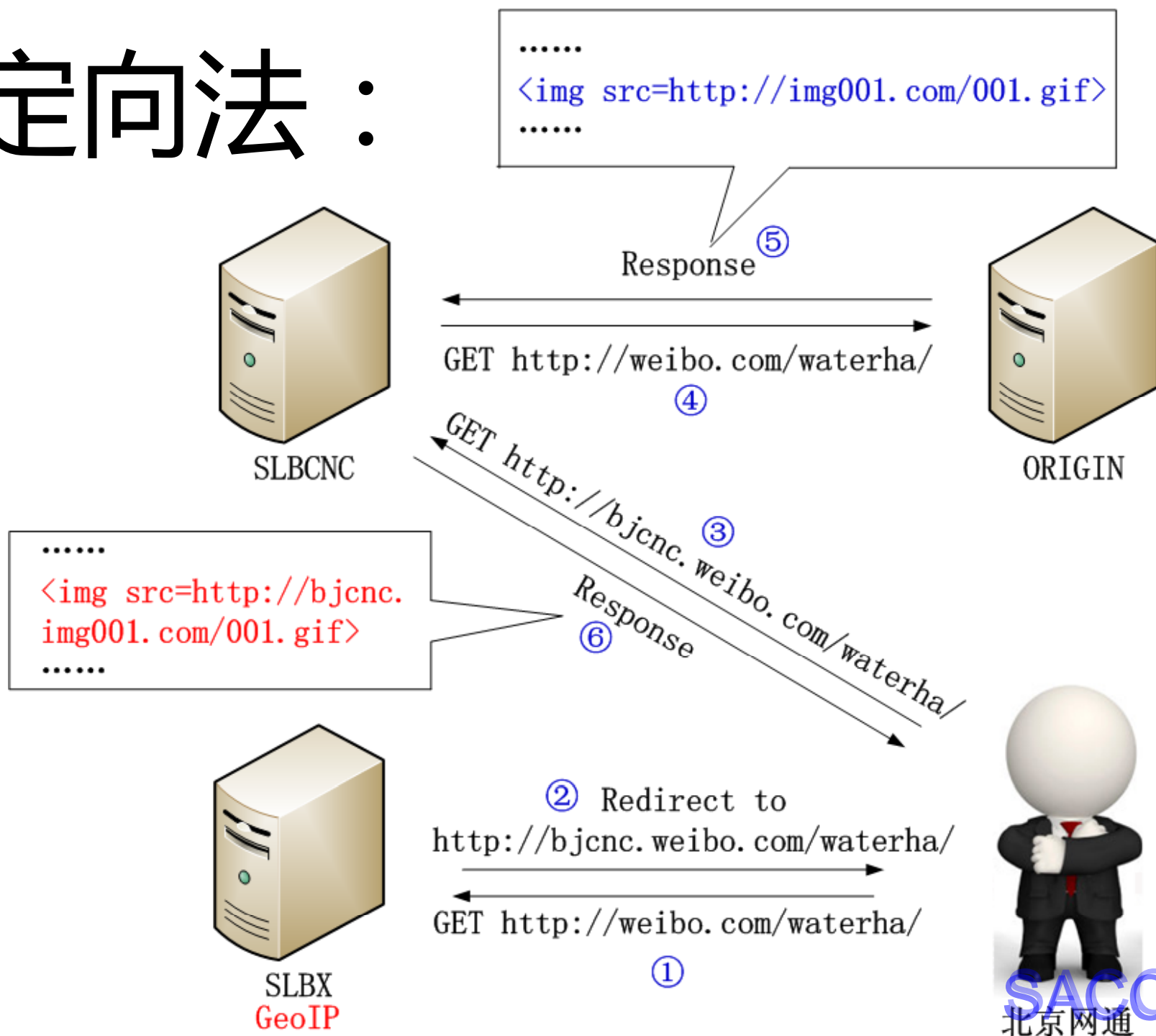

多区域用户共用resolver node 时无法区分用户来源



如何区分共用resolver用户？
国内publicdns用户的归宿？
如何分配双线运营商用户？



重定向法：



1. 通过前面提到的方法将存在共用情况的resolver解析到一台调度服务器上
2. 用户向调度服务器发起请求
3. 调度服务器根据用户来源，返回一个重定向



SLBX
GeoIP

② Redirect to
<http://bjcnc.weibo.com/waterha/>
←
GET <http://weibo.com/waterha/>

①

Redirect



北京网通

SACC2011

1. 用户访问重定向后的新地址(新地址被解析到用户最近节点)
2. 节点服务器拿到用户请求并还原，将原始请求转发给源站

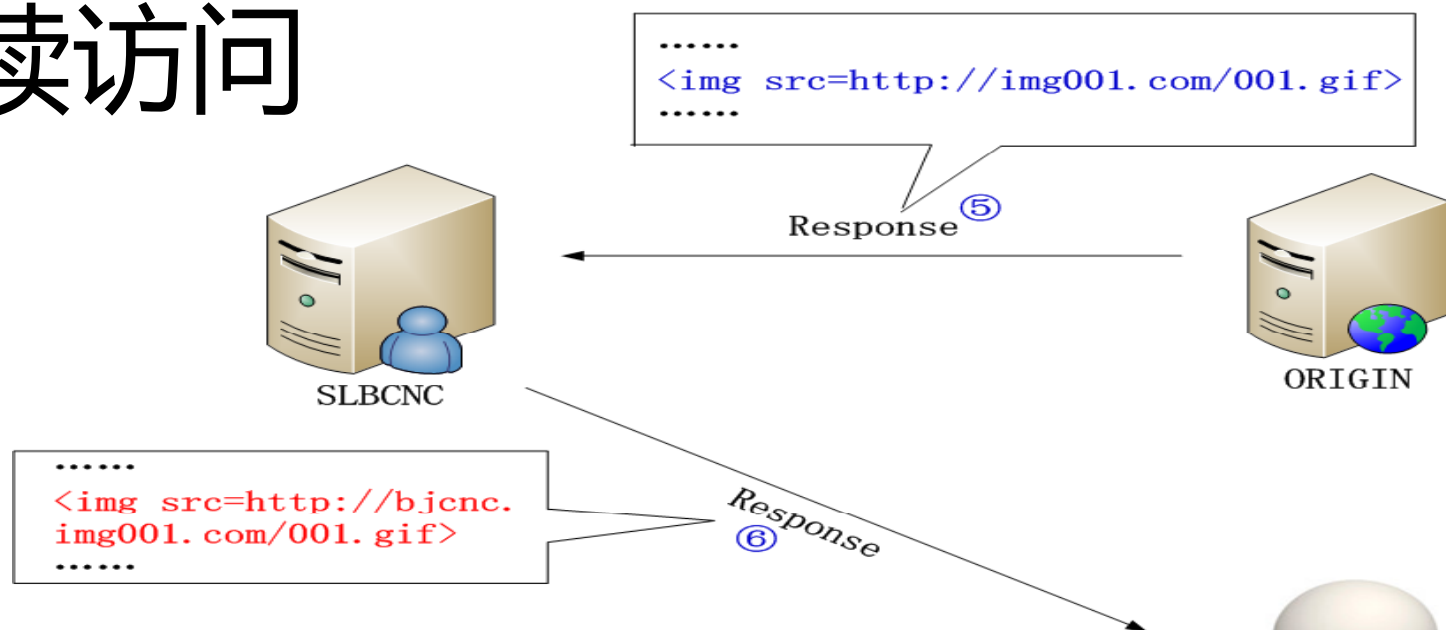


Rewrite



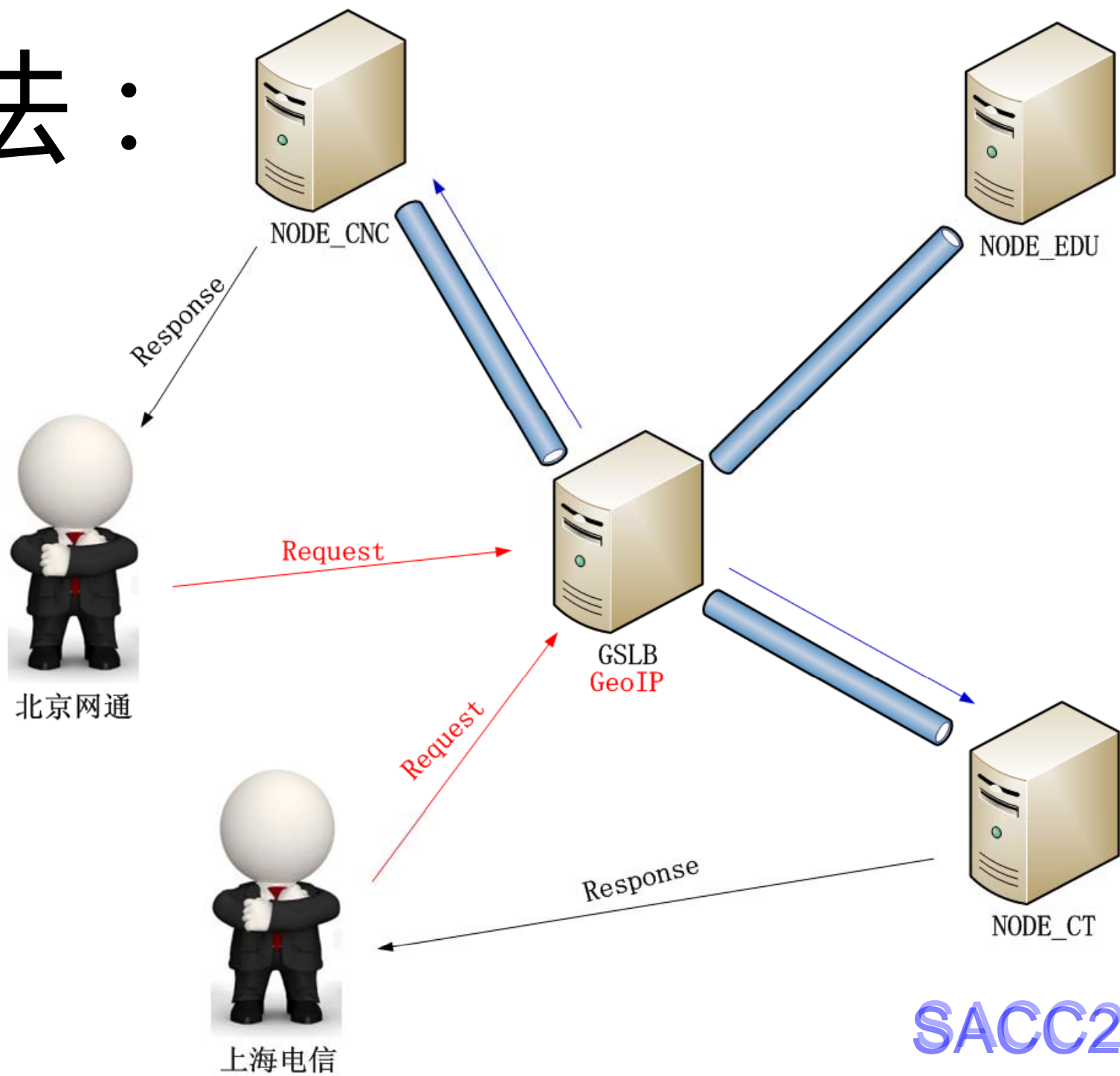
SACC2011

1. 源站返回用户请求给节点服务器
2. 节点服务器拿到源站返回后，扫描其中文本内容的URL链接，并根据自身节点信息进行替换，保证用户的后续访问

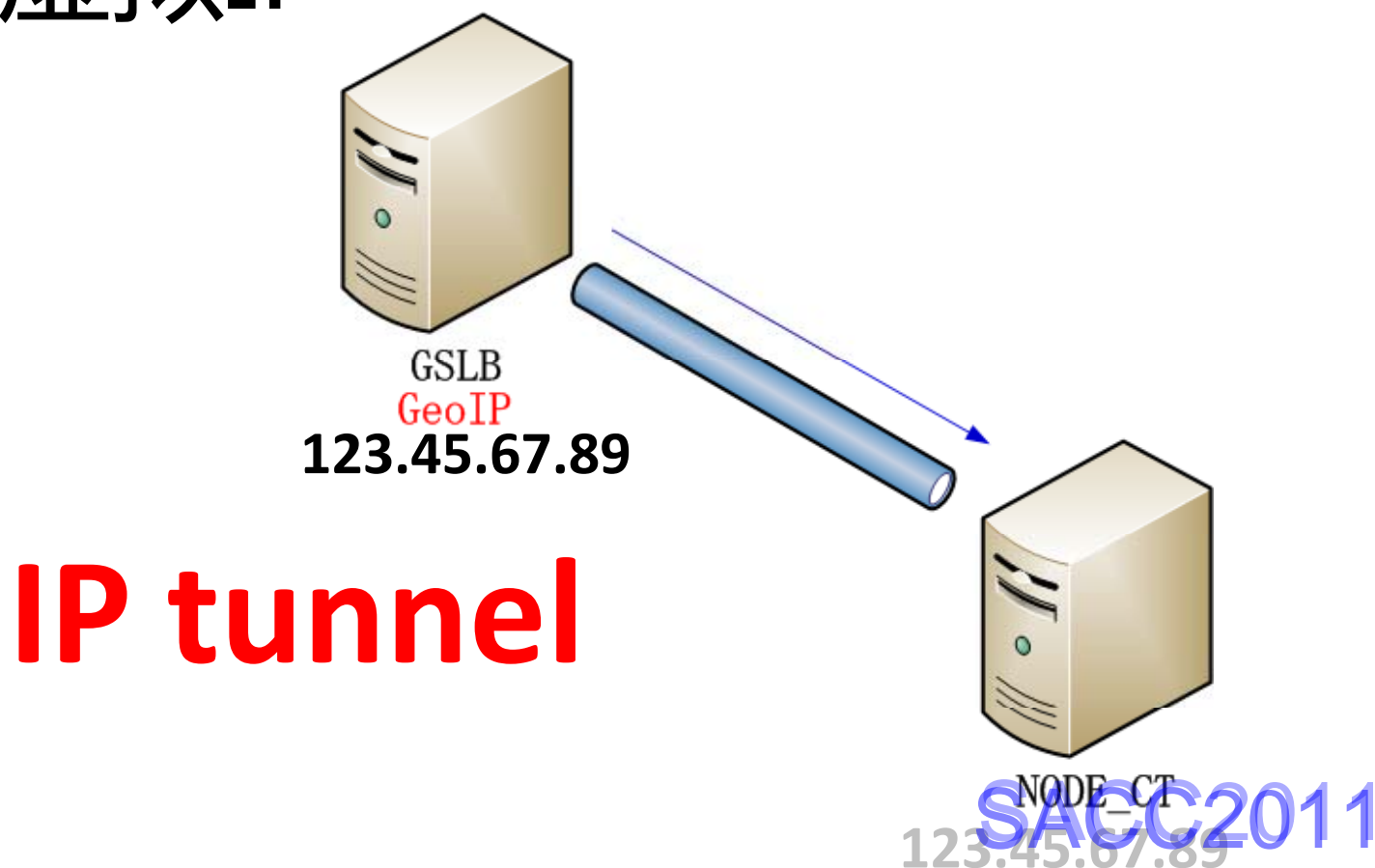


Substitute

调度法：

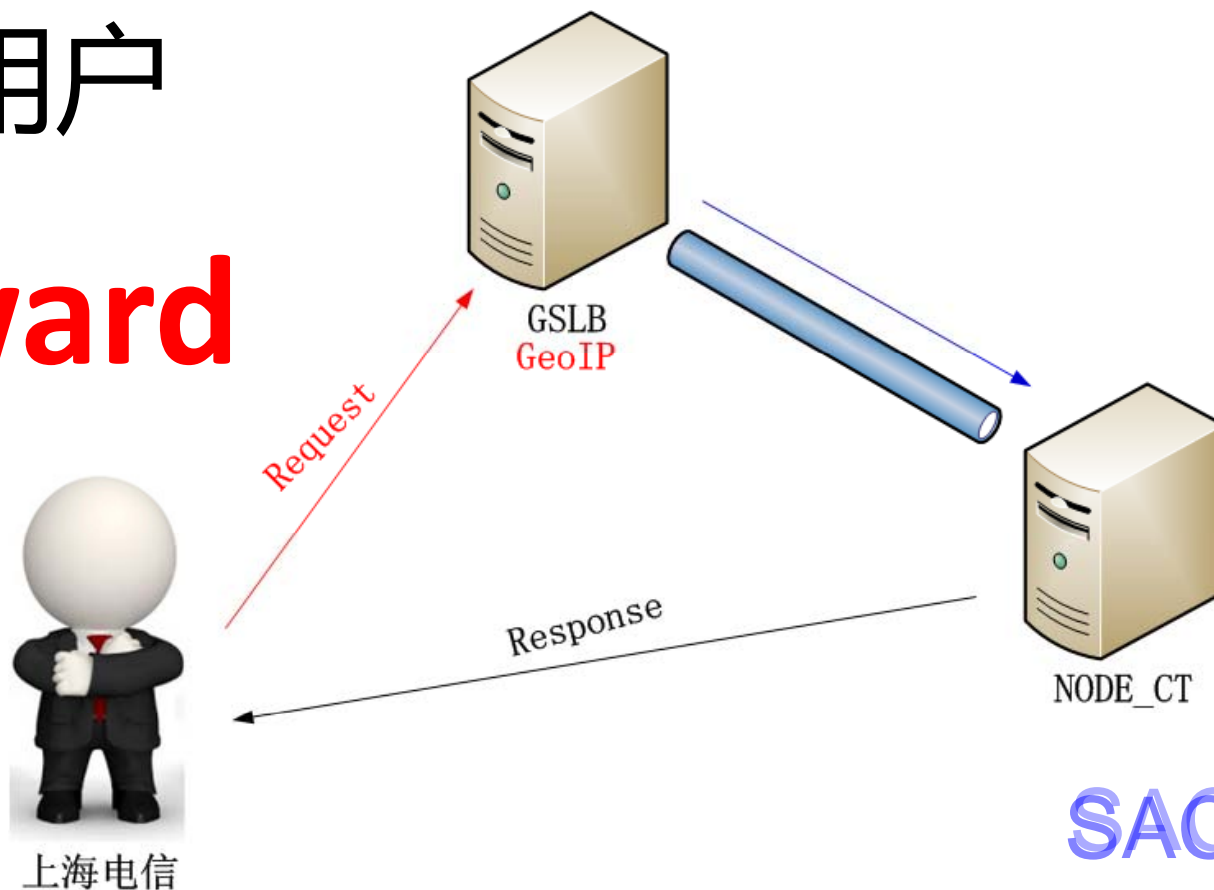


1. 调度服务器与节点服务器间先使用IP隧道打通
2. 节点服务器将调度服务器的IP设置为自己的虚拟IP



1. 用户将请求发送到调度服务器时，调度服务器将用户请求封包并转发给最适合的节点
2. 节点服务器解开封包，直接将请求返回给用户

Forward



SACC2011

回顾：

1. 使用LDNS采集系统收集用户与LDNS对应关系，将resolver分配到对应的区域
2. 将存在用户共用的resolver解析到专门的调度服务器
3. 调度服务器判断用户来源，通过重定向或IP隧道将用户转移到最适合的节点

修正了18.6%的海外用户分配
5.9%的用户访问体验得到提升

盛大网络 云计算主题院

- 云主机
- 云存储
- 云硬盘
- 云监控
- 云分发
- MongoIC

THANK YOU

只要剑法玩得好，剑宗也能胜气宗

<http://weibo.com/waterha/>

SACC2011