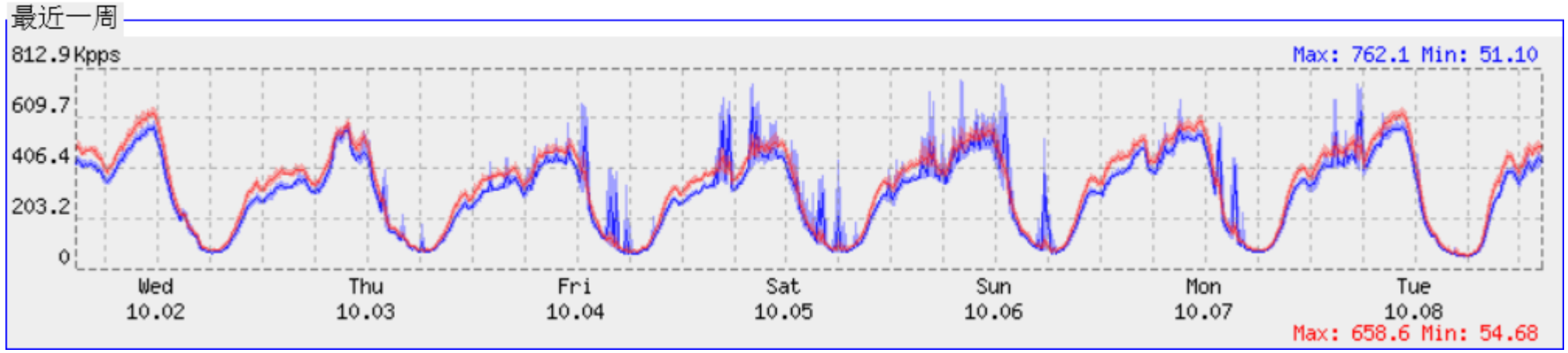
清华大学校园网基本情况

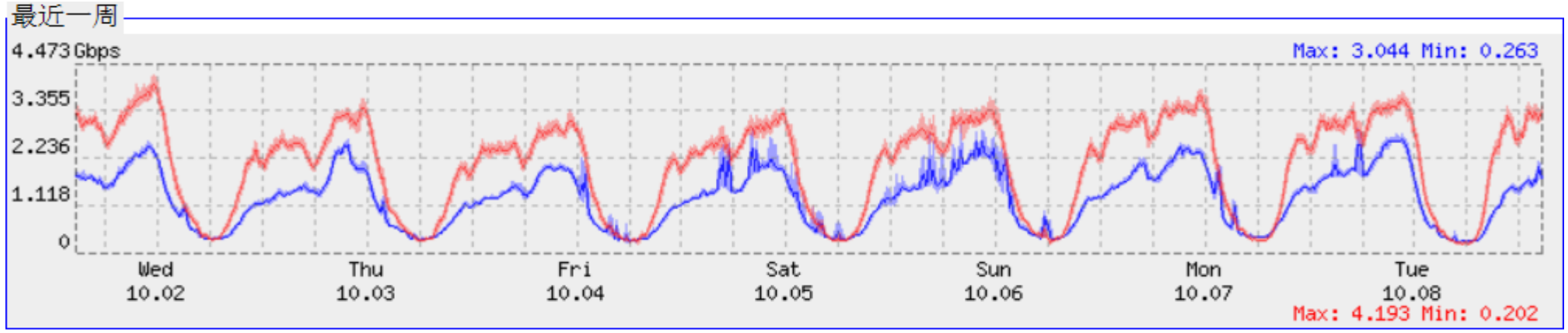
- 校园网**1994**年始建，目前校园网骨干万兆互联，开通到**cernet**万兆链路，到中国电信**1Gb**链路，同时开通**ipv6**万兆上联，校园覆盖**2260**颗无线**AP**。
- 校园网规模：**6**万**5**千信息点，**3**千**500**台交换机
- 校园网用户：**15**万用户，**6**万**5**千活动用户
- 高峰在线数：**4.2**万个**IP**地址在线

校园网出口流量

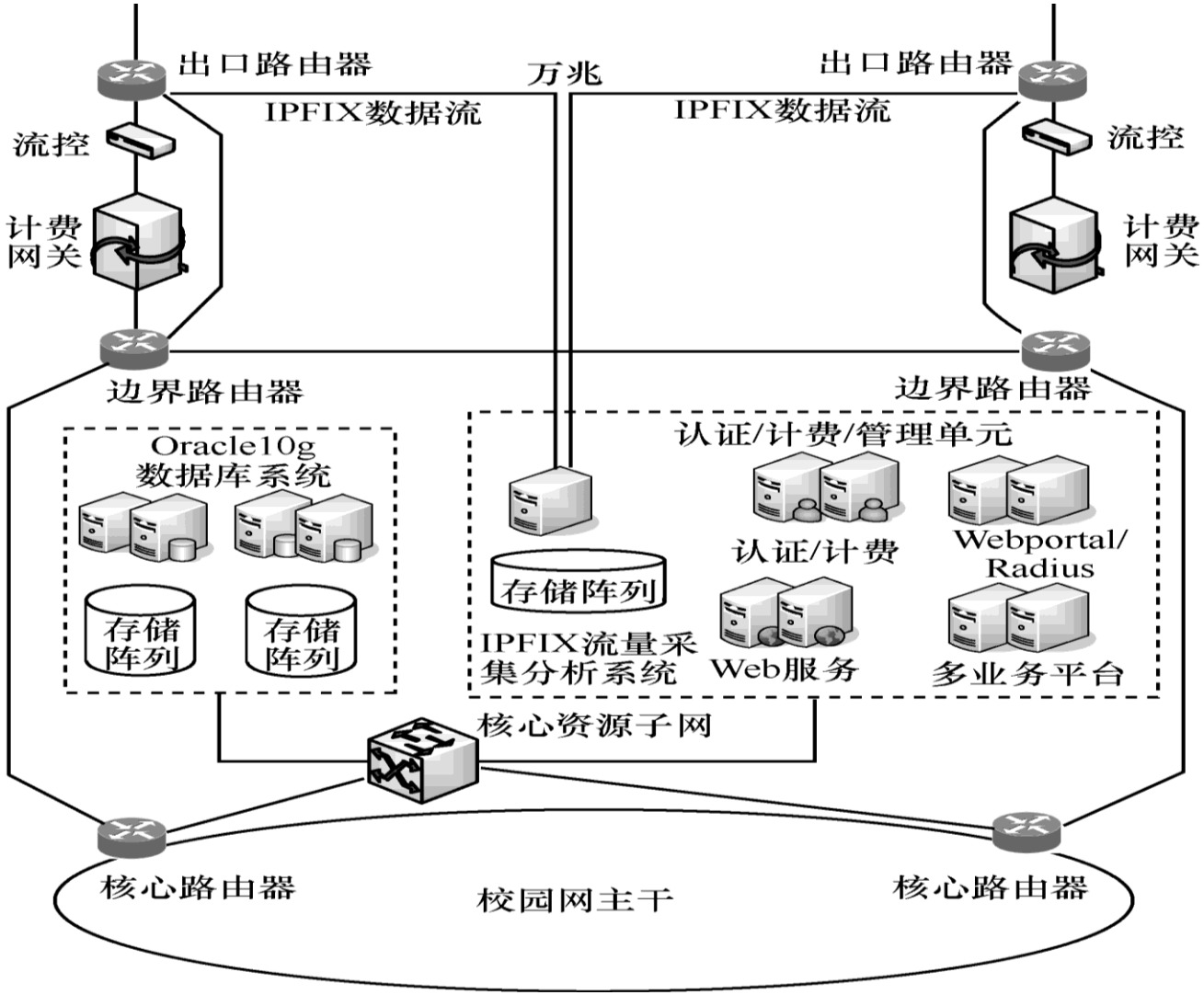
- 分组流量统计



- 比特流量统计

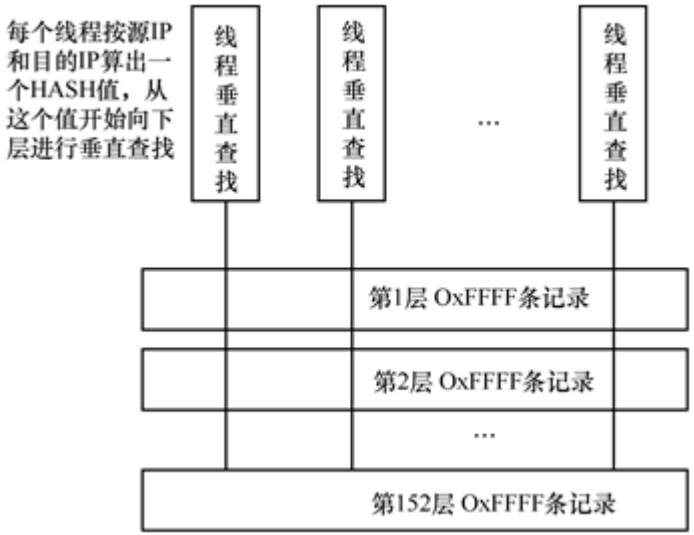


基于IPFIX的网络流量日志系统



系统设计

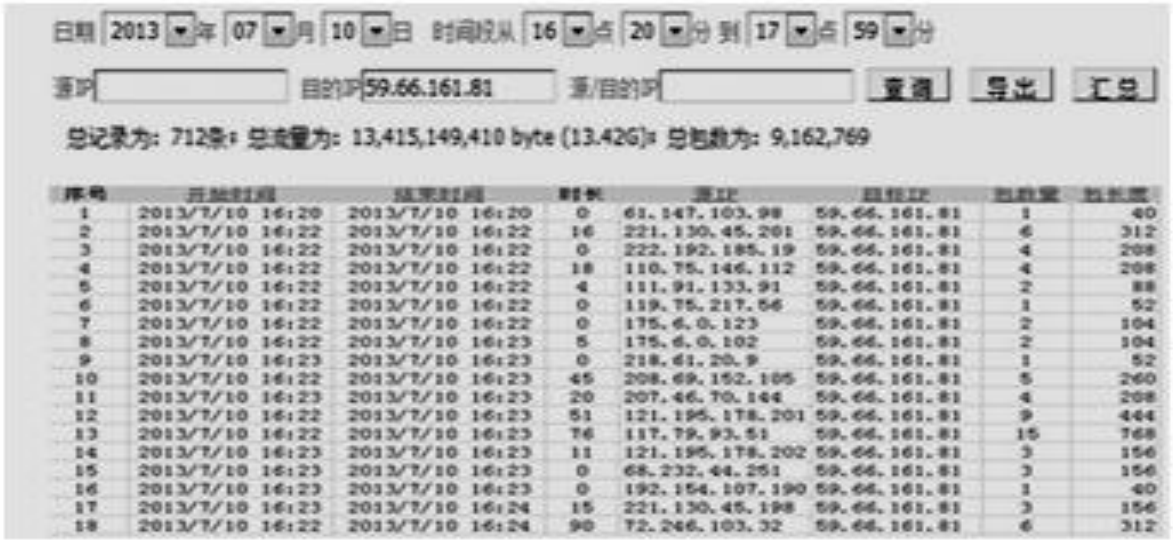
- 一种多层结构的**HASH**算法结构



- 设计每分钟**1kw**条**ipfix**流记录的内存空间，格式为源地址、目标地址、写入时间、更新时间、包数和字节数。
- 每一层表容量设计为**16**位（可存储**65536**条记录），**16*4k=65536**，**1kw/65536=152**层
- 每**10**秒钟检测一次缓存表中每条记录的更新时间，大于**1**分钟即写入**sqlite**文本数据库，同时清空该位置

系统运行情况

- 实例



日期 2013 年 07 月 10 日 时间段从 16 点 20 分 到 17 点 59 分

源IP 目的IP 59.66.161.81 源/目的IP 查询 导出 汇总

总记录为: 712条; 总流量为: 13,415,149,410 byte (13.42G); 总包数为: 9,162,769

序号	开始时间	结束时间	时长	源IP	目的IP	包数量	包长度
1	2013/7/10 16:20	2013/7/10 16:20	0	61.147.103.98	59.66.161.81	1	40
2	2013/7/10 16:22	2013/7/10 16:22	16	221.130.45.201	59.66.161.81	6	312
3	2013/7/10 16:22	2013/7/10 16:22	0	222.192.185.19	59.66.161.81	4	208
4	2013/7/10 16:22	2013/7/10 16:22	18	110.75.146.112	59.66.161.81	4	208
5	2013/7/10 16:22	2013/7/10 16:22	4	111.91.133.91	59.66.161.81	2	88
6	2013/7/10 16:22	2013/7/10 16:22	0	119.75.217.56	59.66.161.81	1	52
7	2013/7/10 16:22	2013/7/10 16:22	0	175.6.0.123	59.66.161.81	2	104
8	2013/7/10 16:22	2013/7/10 16:23	5	175.6.0.102	59.66.161.81	2	104
9	2013/7/10 16:23	2013/7/10 16:23	0	218.61.20.9	59.66.161.81	1	52
10	2013/7/10 16:22	2013/7/10 16:23	45	208.69.152.105	59.66.161.81	5	260
11	2013/7/10 16:23	2013/7/10 16:23	20	207.46.70.144	59.66.161.81	4	208
12	2013/7/10 16:22	2013/7/10 16:23	51	121.195.178.201	59.66.161.81	9	444
13	2013/7/10 16:22	2013/7/10 16:23	76	117.79.93.51	59.66.161.81	15	768
14	2013/7/10 16:23	2013/7/10 16:23	11	121.195.178.202	59.66.161.81	3	156
15	2013/7/10 16:23	2013/7/10 16:23	0	68.232.44.251	59.66.161.81	3	156
16	2013/7/10 16:23	2013/7/10 16:23	0	192.154.107.190	59.66.161.81	1	40
17	2013/7/10 16:23	2013/7/10 16:24	15	221.130.45.198	59.66.161.81	3	156
18	2013/7/10 16:22	2013/7/10 16:24	90	72.246.103.32	59.66.161.81	6	312

图 5　某用户的流量日志截图

- 采集分析**PC SERVER为IBM X3650M4 2*6核cpu**，后端挂载**Netapp存储**
- 目前每分钟**sqlitedb文件为30MB**左右，每天**45G**。

进一步研究设计

- 对于**IPFIX**全流量日志需求

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2013-09-06 06:49:26.475	0.006	TCP	220.181.156.49:80	->	166.111.132.26:2977	5	443	1
2013-09-06 06:51:04.662	0.000	UDP	205.251.197.168:53	->	166.111.8.28:53578	1	163	1
2013-09-06 06:53:52.358	0.000	UDP	2.60.40.191:39343	->	59.66.96.244:51246	1	131	1
2013-09-06 06:52:00.729	0.002	TCP	115.25.217.12:80	->	166.111.74.232:9162	2	92	1
2013-09-06 06:52:54.206	0.000	UDP	95.76.40.18:30668	->	166.111.180.105:28775	1	145	1
2013-09-06 06:53:55.900	10.392	TCP	58.83.217.209:80	->	59.66.34.54:60514	3	156	1
2013-09-06 06:50:07.850	0.000	UDP	41.82.106.51:22202	->	166.111.132.146:53	1	67	1
2013-09-06 06:51:56.315	0.000	TCP	113.6.248.158:6000	->	166.111.225.28:18186	1	40	1
2013-09-06 06:53:22.249	2.983	UDP	222.78.250.186:49694	->	166.111.89.179:18700	2	116	2
2013-09-06 06:49:52.523	0.000	TCP	216.158.80.246:4445	->	166.111.173.7:135	1	64	1
2013-09-06 06:49:38.985	0.000	UDP	98.243.109.146:13477	->	166.111.94.10:19	1	29	1
2013-09-06 06:50:34.246	3.389	UDP	94.34.171.66:4672	->	59.66.156.79:25943	2	156	1
2013-09-06 06:51:56.180	0.000	TCP	113.6.248.158:6000	->	166.111.208.11:18186	1	40	1
2013-09-06 06:49:24.861	0.000	UDP	88.169.62.249:55388	->	166.111.30.57:53	1	63	1
2013-09-06 06:50:00.224	0.000	UDP	115.151.209.211:16873	->	59.66.56.103:6653	1	30	1
2013-09-06 06:49:34.293	0.000	TCP	60.173.8.248:31448	->	101.5.83.31:18186	1	40	1
2013-09-06 06:49:23.461	0.000	UDP	114.250.7.56:15560	->	166.111.36.192:5625	1	30	1
2013-09-06 06:51:38.484	0.000	UDP	79.117.206.236:12364	->	59.66.82.175:16001	1	131	1
2013-09-06 06:52:40.158	40.172	TCP	171.8.79.45:80	->	59.66.192.22:54279	14	13508	2
2013-09-06 06:49:29.459	0.000	UDP	50.90.168.77:11117	->	59.66.189.141:16001	1	145	1
2013-09-06 06:50:16.884	21.802	TCP	114.112.66.107:80	->	166.111.156.72:58994	4	208	2
2013-09-06 06:51:18.374	0.000	UDP	37.152.153.74:61457	->	59.66.178.17:16001	1	131	1
2013-09-06 06:51:37.996	0.000	UDP	174.48.132.91:15923	->	166.111.94.10:19	1	29	1
2013-09-06 06:52:04.005	2.866	TCP	190.79.203.100:2418	->	166.111.253.127:445	2	96	1
2013-09-06 06:52:28.915	53.156	UDP	111.79.34.73:16001	->	59.66.19.35:51413	0	0	1
2013-09-06 06:49:34.092	0.000	TCP	60.173.8.248:23913	->	101.5.32.34:18186	1	40	1
2013-09-06 06:50:41.470	140.467	TCP	114.112.66.107:80	->	166.111.46.211:57303	8	416	2

- 目前可以将整个出口的**ipfix**流量采集，存储下来，每天**200GB**文件，每**5**分钟**1GB**左右

```
[root@ipfix 07]# ls -hlt
total 216G
-rw-r--r--. 1 nobody nobody  796M Oct  7 23:58 nfcapd.201310072355
-rw-r--r--. 1 nobody nobody  860M Oct  7 23:53 nfcapd.201310072350
-rw-r--r--. 1 nobody nobody  854M Oct  7 23:48 nfcapd.201310072345
-rw-r--r--. 1 nobody nobody  876M Oct  7 23:43 nfcapd.201310072340
-rw-r--r--. 1 nobody nobody  938M Oct  7 23:38 nfcapd.201310072335
-rw-r--r--. 1 nobody nobody  944M Oct  7 23:33 nfcapd.201310072330
-rw-r--r--. 1 nobody nobody  988M Oct  7 23:28 nfcapd.201310072325
-rw-r--r--. 1 nobody nobody 1009M Oct  7 23:23 nfcapd.201310072320
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 23:18 nfcapd.201310072315
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 23:13 nfcapd.201310072310
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 23:08 nfcapd.201310072305
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 23:03 nfcapd.201310072300
-rw-r--r--. 1 nobody nobody  1.3G Oct  7 22:58 nfcapd.201310072255
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:53 nfcapd.201310072250
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:48 nfcapd.201310072245
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:43 nfcapd.201310072240
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 22:38 nfcapd.201310072235
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:33 nfcapd.201310072230
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 22:28 nfcapd.201310072225
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 22:23 nfcapd.201310072220
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:18 nfcapd.201310072215
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:13 nfcapd.201310072210
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 22:08 nfcapd.201310072205
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 22:03 nfcapd.201310072200
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 21:58 nfcapd.201310072155
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 21:53 nfcapd.201310072150
-rw-r--r--. 1 nobody nobody  1.1G Oct  7 21:48 nfcapd.201310072145
-rw-r--r--. 1 nobody nobody  1.2G Oct  7 21:43 nfcapd.201310072140
```

谢谢大家！

清华大学信息化技术中心(原网络中心)
马云龙
myl@tsinghua.edu.cn
13520454132