IDC\_流量分析系统后台详解

IDC流量分析系统后台主要通过libpcap提供的API工作。主要流程为以下几步：

1. 注册alarm信号处理程序，用于每5分钟计算汇总数据并发给服务端入库
2. 启动alarm信号处理线程
3. 启动alarm定时，时间为300秒
4. 网卡信息获取
5. 针对每个网卡信息(IP)启动工作线程
6. 根据相应网卡信息设置libpcap抓取规则
7. 启动libpcap抓包，并将抓到的包排入处理队列
8. 当队列达到10000个元素，启动数据包处理线程
9. 分析数据包，判断源地址与目的地址是否与本地网络重合，然后选取相应ip作为key存入相应hashtable
10. 每5分钟接收到alarm信号后，加锁互斥数据包处理线程，汇总计算数据，并通过socket返给服务端，然后清空5分钟数据

流程图如下：



流程详解：

1. 程序启动，初始化相关变量，主要包括key双向链表初始化，hashtable初始化等
2. 注册信号处理线程，主要用于阻塞alarm信号，以实现每5分钟数据汇总的定时效果
3. 启动信号处理线程，阻塞直到接收到信号。
4. 获取网卡信息，根据网卡上的IP为单位启动工作线程。
5. 根据网卡IP设置与子网掩码设置相应匹配规则。
6. 启动pcap抓包
7. 将抓到的数据包排入待处理队列，当队列达到1000个元素，启动数据包处理线程。
8. 加锁互斥，处理数据包。
9. 根据数据包的源地址与目标地址，取相应IP作为key，将数据包信息存入hashtable。
10. 信号处理程序接收到信号后，加锁互斥。
11. 将原key双向链表与原数据存储hashtable重定向到新的内存空间，
12. 处理上5分钟数据，根据流量排序，取前20名。
13. 通过socket将分析完数据发给服务器端。
14. 服务器端接收数据后将数据入库，供前台使用。
15. 信号处理线程清理数据，重新阻塞。