



上



上网行为管理系统巡检作业指导书

2013 年 11 月

一、作业准备

序号	所需资源	名称	备注
1	工具软件	无	
2	资料文档	上网管理系统维护手册	

二、巡检记录

项目名称	业务范围	巡检内容	备注
系统状态	硬件部分	系统 CUP、硬盘、内存使用率情况	
		会话连接数	
		WAN 实时流量	
	软件部分	许可情况	
		HA 集群状态检查	
系统日志检查	软件部分	系统日志检查	

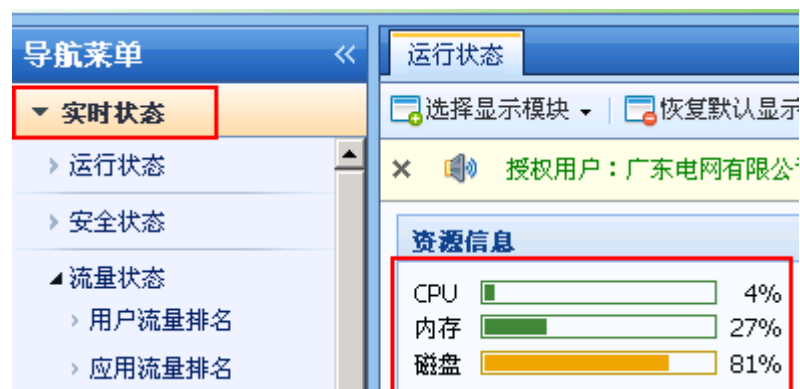
流量排名	软件部分	组流量排名	
		用户流量排名	
		应用流量排名	
		Ip 流量排名	

二、巡检步骤

1. 系统状态检查

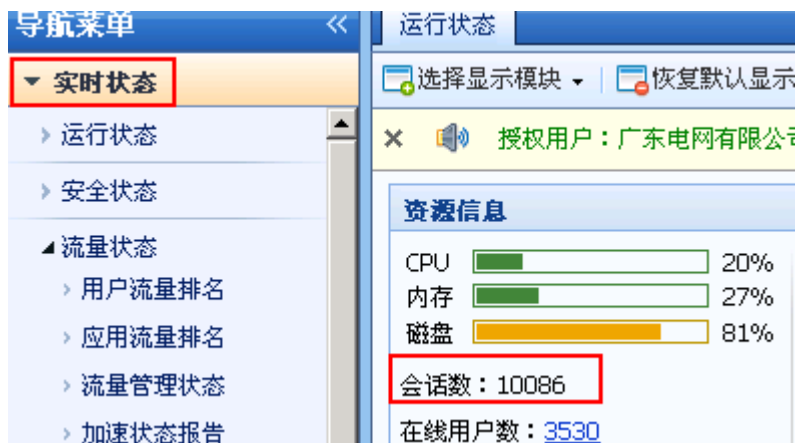
1.1 系统 CUP、硬盘、内存使用率情况

登陆网上管理系统，在实时状态中能看见当前CPU、内存、磁盘使用情况。



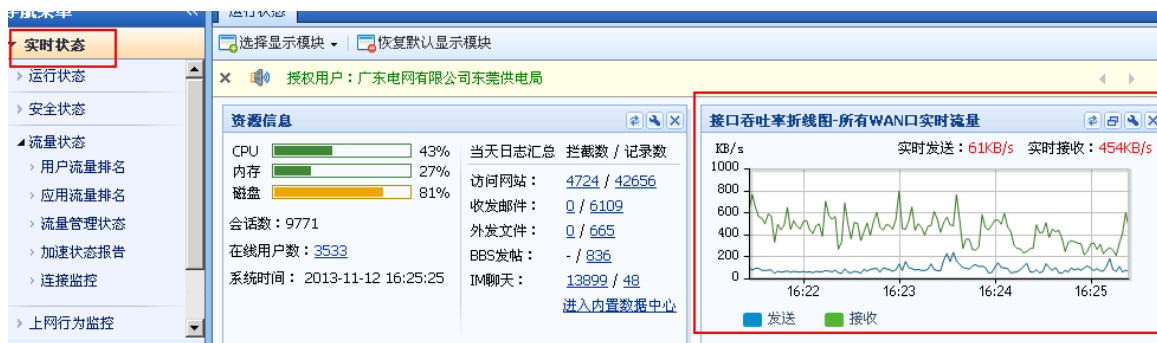
1.2 会话连接数

登陆网上管理系统，在实时状态中能看见当前会话连接数。



1.3 WAN 实时流量

登陆网上管理系统，在实时状态中能看见当前WAN实时流量。



1.4 许可证状态

登陆网上管理系统，在系统配置—序列号能看见许可信息。



1.5 HA 集群状态检查

登录上网管理系统，在网络配置中---双机维护—能看见与对端通信正常。



2. 系统日志分析

2.1 系统日志检查

登陆网上管理系统，在系统诊断中，系统日志里能看见日志信息。

导航菜单

实时状态

对象定义

用户与策略管理

流量管理

上网加速

安全防护

防火墙

网络配置

系统配置

系统诊断

系统日志

抓包工具

命令控制台

Bypass与拦截定位

重启操作

系统日志

日志选项设置

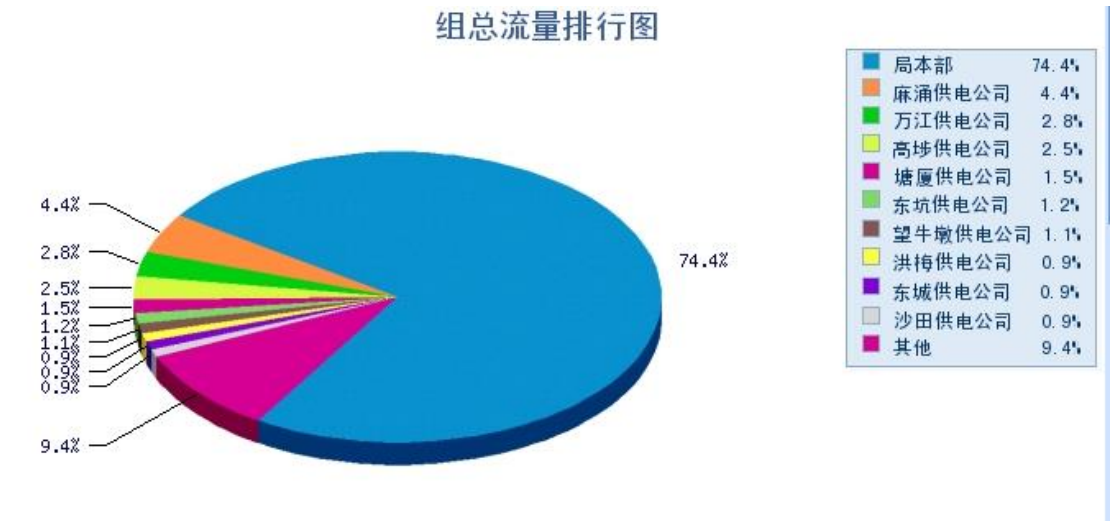
选择日期：20130916

序号	来源	类型	时间	详细信息
1	访问日志系统	信息	17:10:50	update ac User table ok.
2	访问日志系统	信息	17:10:49	update ac Group table ok.
3	双机热备	信息	16:29:56	[cluster]本端目前状态为【主机】，对端【备机】工作正常！向备机同步系统时间[2013-09-16 :
4	邮件代理	信息	16:10:47	Read Crc form contchkprivate ok: 1448942861, 3420019107, 1841528731
5	访问日志系统	信息	16:10:46	update ac User table ok.
6	访问日志系统	信息	16:10:45	update ac Group table ok.
7	网络准入系统	信息	16:10:44	没有启用准入规则
8	网络准入系统	信息	16:10:44	echo
9	应用审计	信息	16:10:44	i0:main.cpp:697 min_logtime = 600
10	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:663 访问控制组配置更新
11	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:646 访问控制用户配置更新
12	访问日志系统	信息	15:31:18	Read log days: 330
13	访问日志系统	信息	15:31:18	aclog used space : 362030936 kb, 362030936 kb
14	访问日志系统	信息	15:30:57	Calcualte attach file size for 15:27
15	访问日志系统	信息	15:30:57	exec sql success.sql:update AttachInfo set file_size = 38576128 where table_name =
16	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/actrace/20130916, the size is 38576128
17	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/ips/20130916, the size is 0
18	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
19	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/delaysnd/20130916, the size is 0
20	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
21	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/ass3log/20130916, the size is 0

3. 流量排名

3.1 组流量排名

访问控制组流量排行榜：以dg. gpgc. local组的流量占比重较大



3.2 用户流 70 唐栗林 女 15193213727

15193217627

3.3 26 任如平 女 15891968874 15891967627

3.4 34 吴丹 女 15385445250 15385447627

3.5 27 蒋燚 男 15271136614 15271137627

3.6 2 陈金花 女 13175999707 13175997627

3.7 41 廖秋 女 15190369192 15190367627

3.8 43 林俊荣 女 13672268233 13672267627

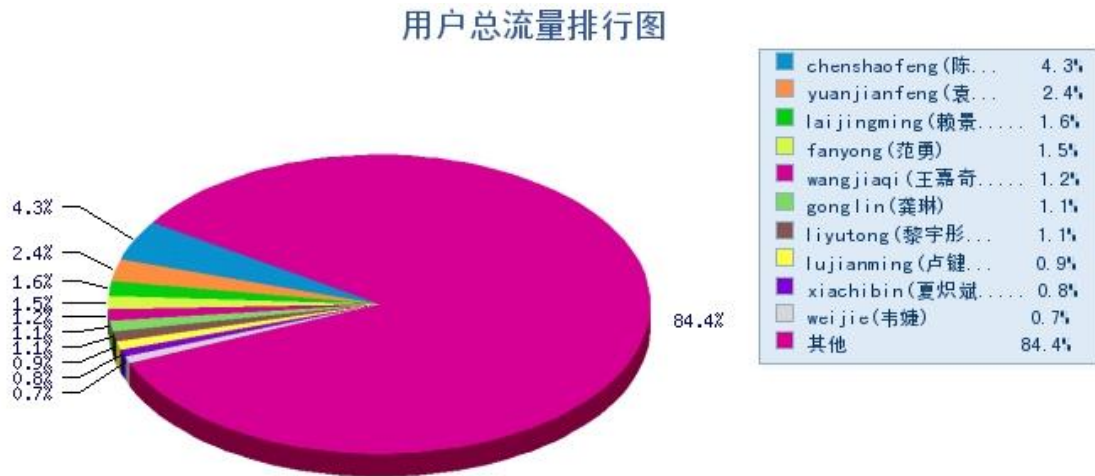
3.9

3.10 3 陈国伟 男 15187720817

3.11 31 宋秀红 女 17571381198

3.12 82 谢卫鹏 男 13228473943

3.13 量排行榜：

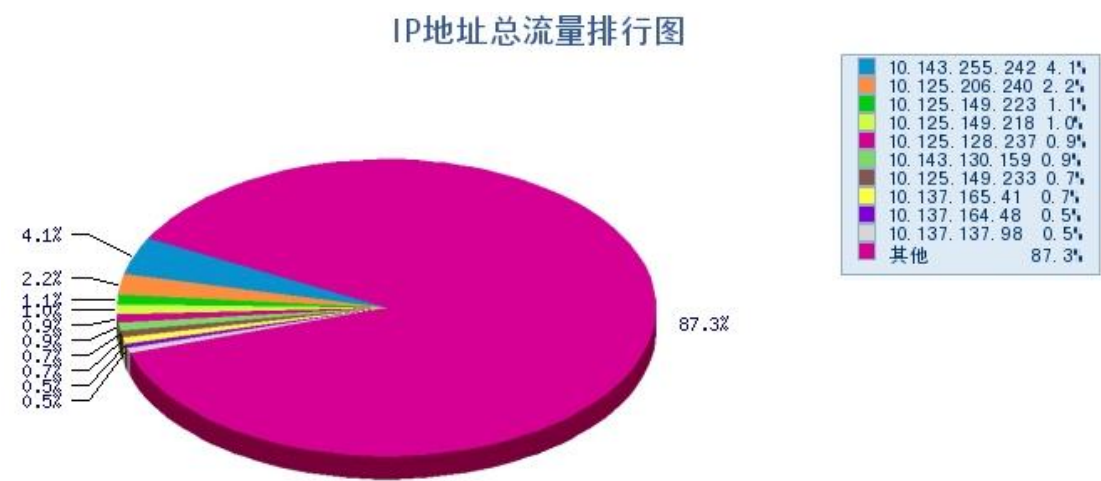


3.14 应用流量排行

应用流量排行：以访问网站的流量比重较大



3.15 IP 流量排行：



4、作业中异常现象及主要对策

序号	异常现象	处理对策	注意事项
1	上网行为管理系统的硬件出现故障	采取主备双机热备的部署模式，当其中一台出现故障时，另一台自动接替工作，保证业务不中断运行；联系原厂更换设备。	
2	主备无法切换	检查主备配置是否更改过，更换主备之间的心跳线	
3	上网行为管理系统略配置意外丢失	通过上网行为管理系统还原备份配置文件，恢复正常工作；	
4	上网行为管理系统端口故障	若是上网行为管理系统端口物理损坏，更换网络接口卡，若端口物理状态正常，处于 down 状态，检查对端设备端口状态，或尝试更换新的光纤线。	

网行为管理系统巡检作业指导书

2013 年 11 月

一、作业准备

序号	所需资源	名称	备注
1	工具软件	无	
2	资料文档	上网管理系统维护手册	

二、巡检记录

项目名称	业务范围	巡检内容	备注
系统状态	硬件部分	系统 CUP、硬盘、内存使用率情况	
		会话连接数	
		WAN 实时流量	
	软件部分	许可情况	
		HA 集群状态检查	
系统日志检查	软件部分	系统日志检查	

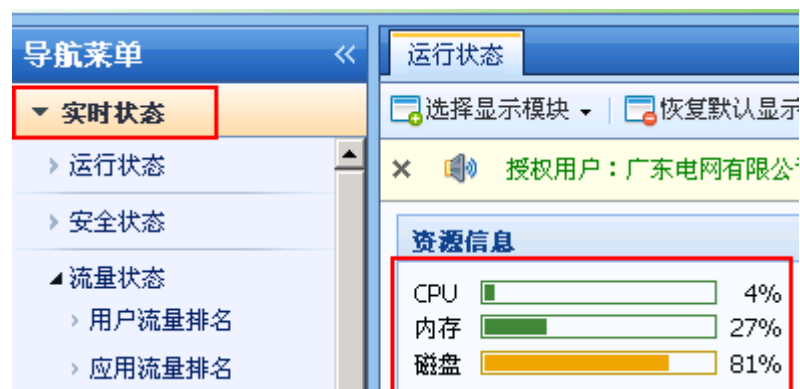
流量排名	软件部分	组流量排名	
		用户流量排名	
		应用流量排名	
		Ip 流量排名	

二、巡检步骤

2. 系统状态检查

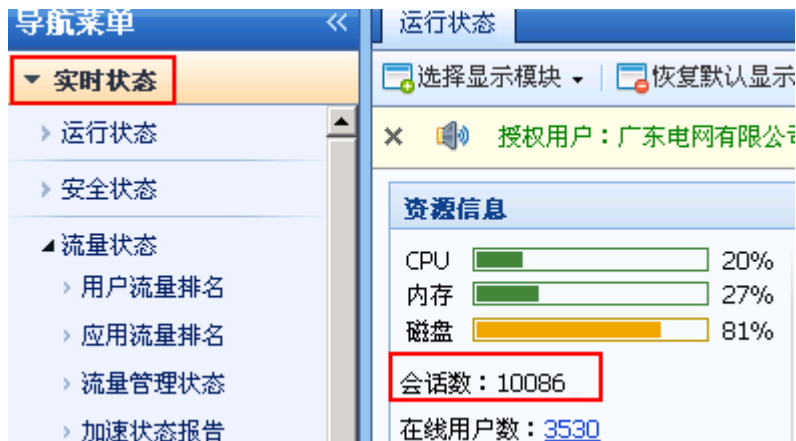
3.16 系统 CUP、硬盘、内存使用率情况

登陆网上管理系统，在实时状态中能看见当前CPU、内存、磁盘使用情况。



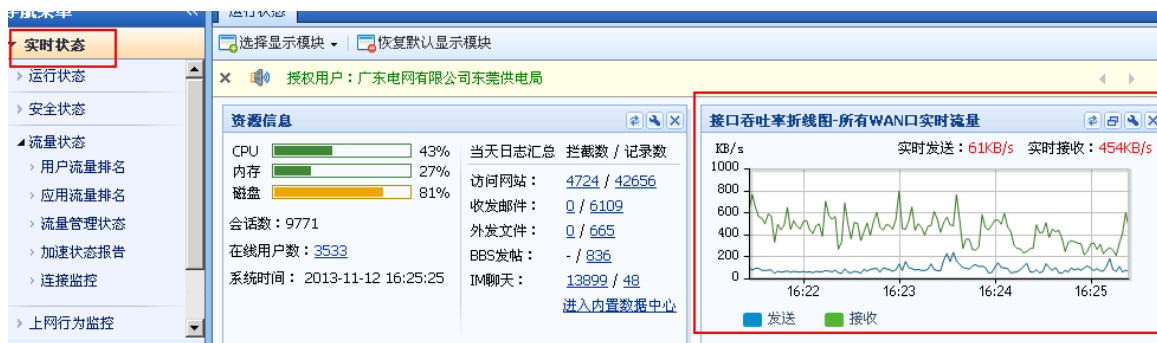
3.17 会话连接数

登陆网上管理系统，在实时状态中能看见当前会话连接数。



3.18 WAN 实时流量

登陆网上管理系统，在实时状态中能看见当前WAN实时流量。



3.19 许可证状态

登陆网上管理系统，在系统配置—序列号能看见许可信息。



3.20 HA 集群状态检查

登录上网管理系统，在网络配置中---双机维护—能看见与对端通信正常。



4. 系统日志分析

4.1 系统日志检查

登陆网上管理系统，在系统诊断中，系统日志里能看见日志信息。

导航菜单

实时状态

对象定义

用户与策略管理

流量管理

上网加速

安全防护

防火墙

网络配置

系统配置

系统诊断

系统日志

抓包工具

命令控制台

Bypass与拦截定位

重启操作

系统日志

日志选项设置

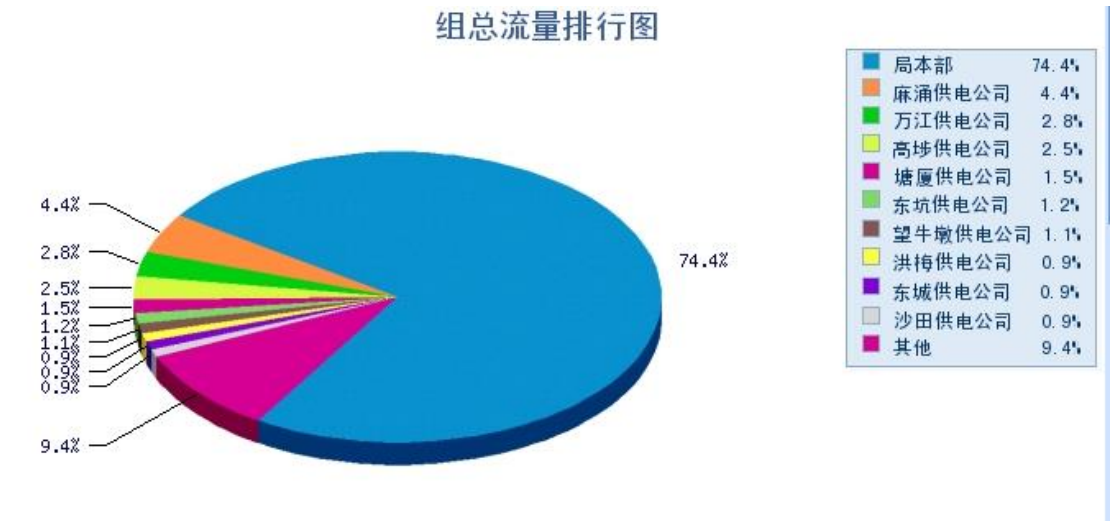
选择日期：20130916

序号	来源	类型	时间	详细信息
1	访问日志系统	信息	17:10:50	update ac User table ok.
2	访问日志系统	信息	17:10:49	update ac Group table ok.
3	双机热备	信息	16:29:56	[cluster]本端目前状态为【主机】，对端【备机】工作正常！向备机同步系统时间[2013-09-16 :
4	邮件代理	信息	16:10:47	Read Crc form contchkprivate ok: 1448942861, 3420019107, 1841528731
5	访问日志系统	信息	16:10:46	update ac User table ok.
6	访问日志系统	信息	16:10:45	update ac Group table ok.
7	网络准入系统	信息	16:10:44	没有启用准入规则
8	网络准入系统	信息	16:10:44	echo
9	应用审计	信息	16:10:44	i0:main.cpp:697 min_logtime = 600
10	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:663 访问控制组配置更新
11	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:646 访问控制用户配置更新
12	访问日志系统	信息	15:31:18	Read log days: 330
13	访问日志系统	信息	15:31:18	aclog used space : 362030936 kb, 362030936 kb
14	访问日志系统	信息	15:30:57	Calcualte attach file size for 15:27
15	访问日志系统	信息	15:30:57	exec sql success.sql:update AttachInfo set file_size = 38576128 where table_name =
16	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/actrace/20130916, the size is 38576128
17	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/ips/20130916, the size is 0
18	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
19	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/delaysnd/20130916, the size is 0
20	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
21	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/conn3log/20130916, the size is 0

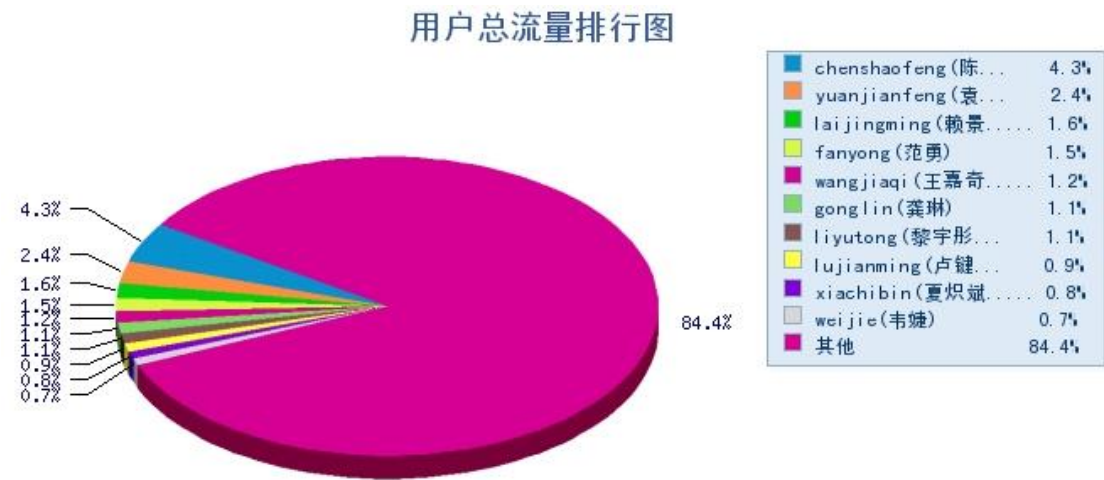
5. 流量排名

5.1 组流量排名

访问控制组流量排行榜：以dg. gpgc. local组的流量占比重较大



5.2 用户流量排行榜：

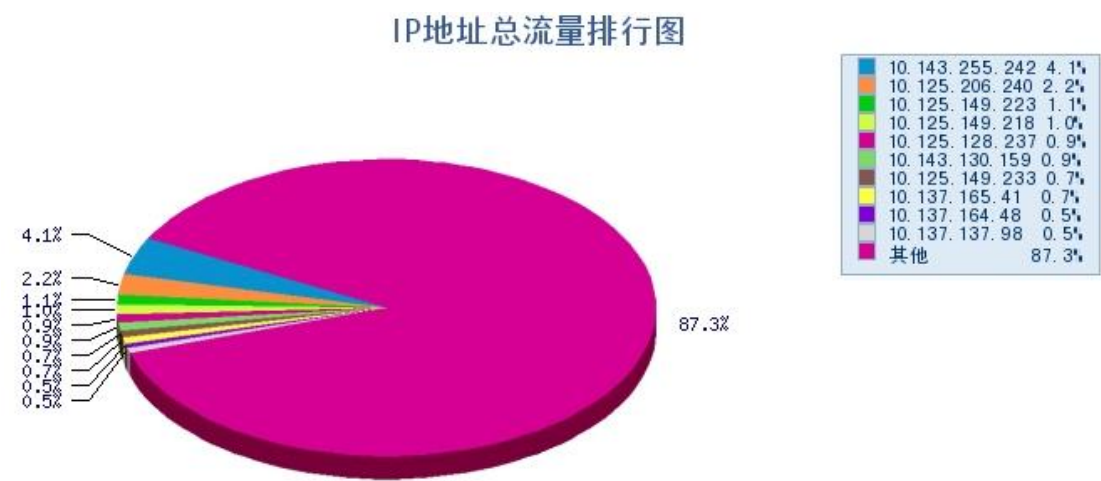


5.3 应用流量排行

应用流量排行：以访问网站的流量比重较大



5.4 IP 流量排行：



4、作业中异常现象及主要对策

序号	异常现象	处理对策	注意事项
1	上网行为管理系统的硬件出现故障	采取主备双机热备的部署模式，当其中一台出现故障时，另一台自动接替工作，保证业务不中断运行；联系原厂更换设备。	
2	主备无法切换	检查主备配置是否更改过，更换主备之间的心跳线	
3	上网行为管理系统略配置意外丢失	通过上网行为管理系统还原备份配置文件，恢复正常工作；	
4	上网行为管理系统端口故障	若是上网行为管理系统端口物理损坏，更换网络接口卡，若端口物理状态正常，处于 down 状态，检查对端设备端口状态，或尝试更换新的光纤线。	

上



上网行为管理系统巡检作业指导书

2013 年 11 月

一、作业准备

序号	所需资源	名称	备注
1	工具软件	无	
2	资料文档	上网管理系统维护手册	

二、巡检记录

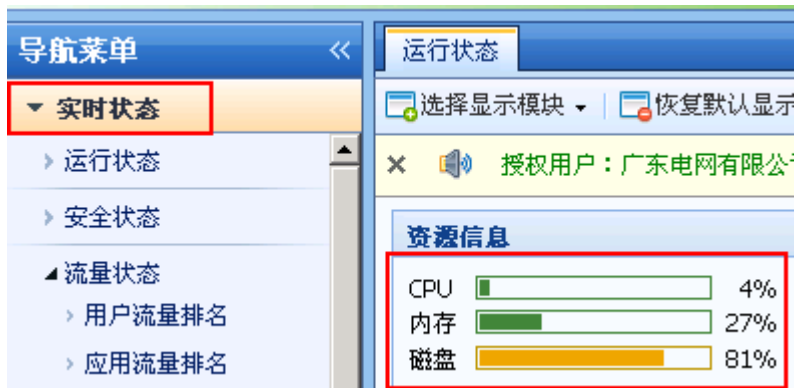
项目名称	业务范围	巡检内容	备注
系统状态	硬件部分	系统 CUP、硬盘、内存使用率情况	
		会话连接数	
		WAN 实时流量	
	软件部分	许可情况	
		HA 集群状态检查	
系统日志检查	软件部分	系统日志检查	
流量排名	软件部分	组流量排名	
		用户流量排名	
		应用流量排名	
		Ip 流量排名	

二、巡检步骤

3. 系统状态检查

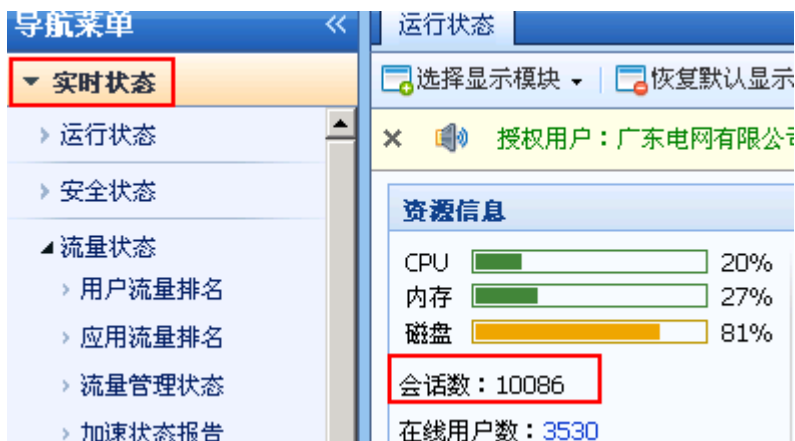
5.5 系统 CUP、硬盘、内存使用率情况

登陆网上管理系统，在实时状态中能看见当前CPU、内存、磁盘使用情况。



5.6 会话连接数

登陆网上管理系统，在实时状态中能看见当前会话连接数。



5.7 WAN 实时流量

登陆网上管理系统，在实时状态中能看见当前WAN实时流量。



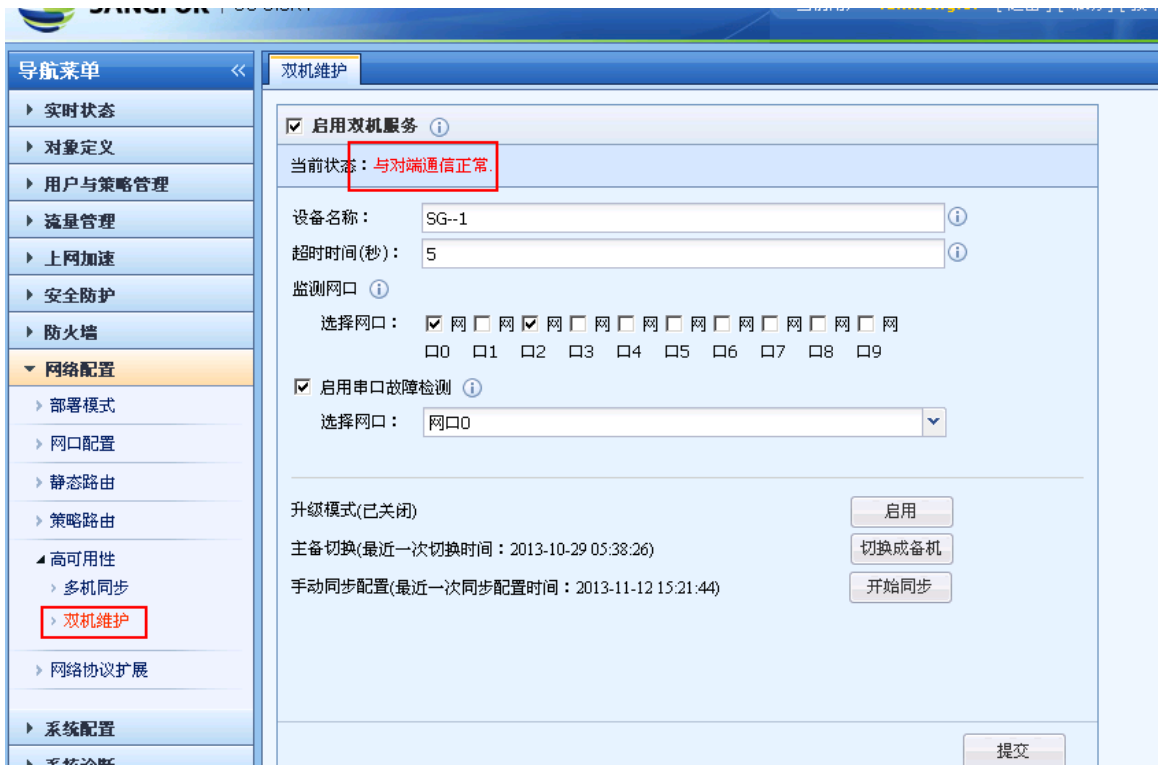
5.8 许可证状态

登陆网上管理系统，在系统配置—序列号能看见许可信息。



5.9 HA 集群状态检查

登陆上网管理系统，在网络配置中---双机维护—能看见与对端通信正常。



6. 系统日志分析

6.1 系统日志检查

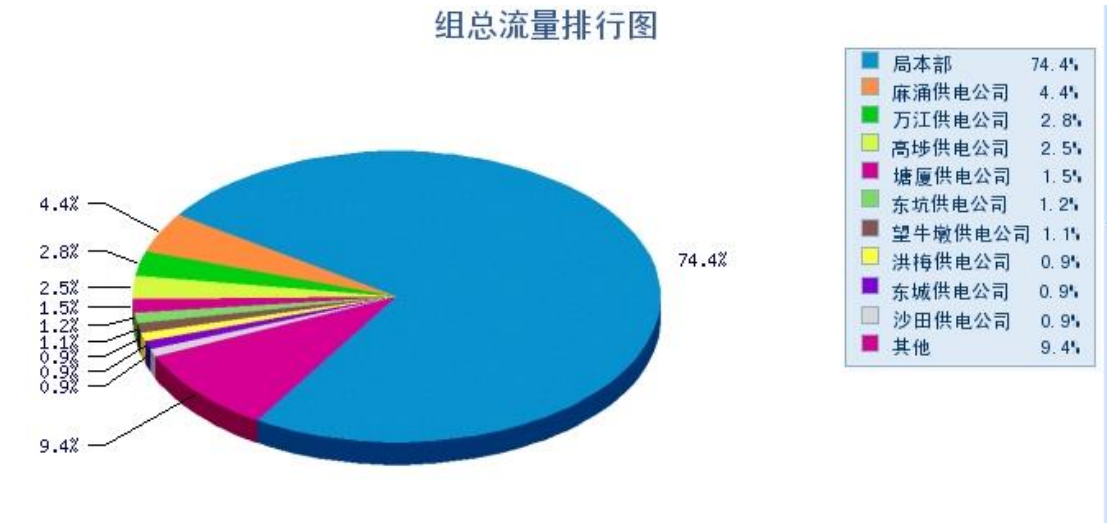
登陆网上管理系统，在系统诊断中，系统日志里能看见日志信息。

序号	来源	类型	时间	详细信息
1	访问日志系统	信息	17:10:50	update ac User table ok.
2	访问日志系统	信息	17:10:49	update ac Group table ok.
3	双机热备	信息	16:29:56	[cluster]本端目前状态为【主机】，对端【备机】工作正常！向备机同步系统时间[2013-09-16 .
4	邮件代理	信息	16:10:47	Read Crc form contchprivate ok: 1448942861, 3420019107, 1841528731
5	访问日志系统	信息	16:10:46	update ac User table ok.
6	访问日志系统	信息	16:10:45	update ac Group table ok.
7	网络准入系统	信息	16:10:44	没有启用准入规则
8	网络准入系统	信息	16:10:44	echo
9	应用审计	信息	16:10:44	i0:main.cpp:697 min_logtime = 600
10	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:663 访问控制组配置更新
11	WEB认证系统	信息	16:10:44	i0:loadconf.cpp:646 访问控制用户配置更新
12	访问日志系统	信息	15:31:18	Read log days: 330
13	访问日志系统	信息	15:31:18	aclog used space : 362030936 kb, 362030936 kb
14	访问日志系统	信息	15:30:57	Calcalte attach file size for 15:27
15	访问日志系统	信息	15:30:57	exec sql success.sql:update AttachInfo set file_size = 38576128 where table_name =
16	访问日志系统	信息	15:30:57	Calcalte attach file size of /aclog/actrace/20130916, the size is 38576128
17	访问日志系统	信息	15:30:57	Calcalte attach file size of /aclog/ips/20130916, the size is 0
18	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
19	访问日志系统	信息	15:30:57	Calcalte attach file size of /aclog/mailproxy/delaysnd/20130916, the size is 0
20	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
21	访问日志系统	信息	15:30:57	Calcalte attach file size of /aclog/mailproxy/asn3log/20130916, the size is 0

7. 流量排名

7.1 组流量排名

访问控制组流量排行榜：以dg. gpgc. local组的流量占比重较大



7.2 用户流 70 唐栗林 女 15193213727

15193217627

7.3 26 任如平 女 15891968874 15891967627

7.4 34 吴丹 女 15385445250 15385447627

7.5 27 蒋燦 男 15271136614 15271137627

7.6 2 陈金花 女 13175999707 13175997627

7.7 41 廖秋 女 15190369192 15190367627

7.8 43 林俊荣 女 13672268233 13672267627

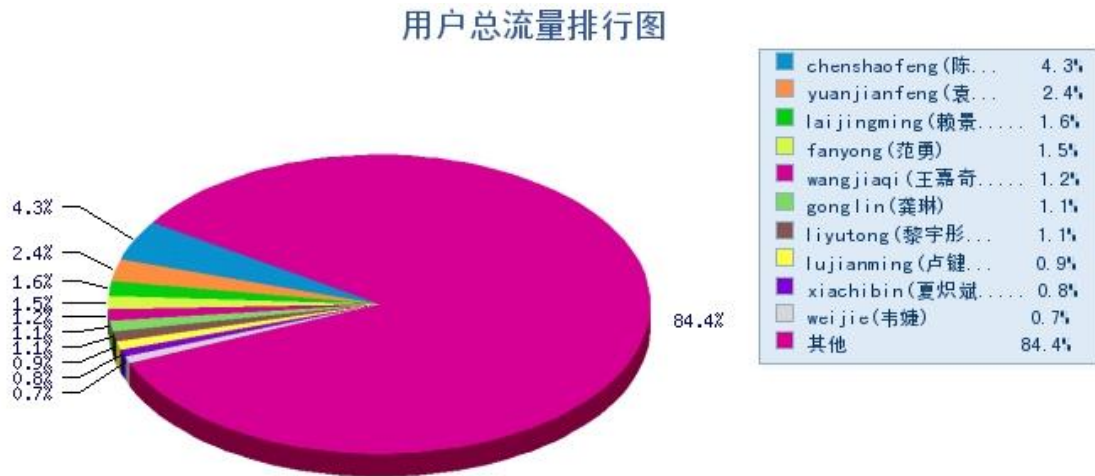
7.9

7.10 3 陈国伟 男 15187720817

7.11 31 宋秀红 女 17571381198

7.12 82 谢卫鹏 男 13228473943

7.13 量排行榜：

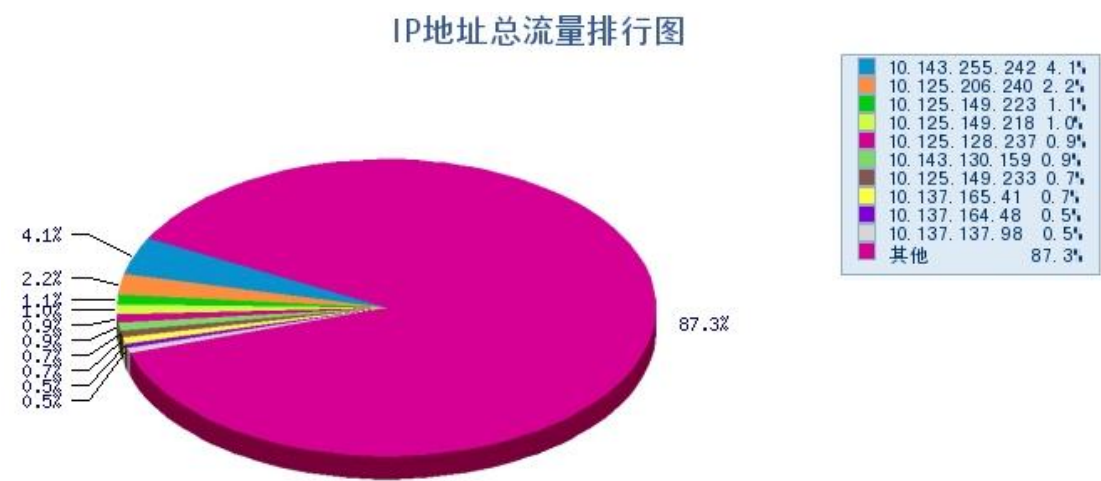


7.14 应用流量排行

应用流量排行：以访问网站的流量比重较大



7.15 IP 流量排行：



4、作业中异常现象及主要对策

序号	异常现象	处理对策	注意事项
1	上网行为管理系统的硬件出现故障	采取主备双机热备的部署模式，当其中一台出现故障时，另一台自动接替工作，保证业务不中断运行；联系原厂更换设备。	
2	主备无法切换	检查主备配置是否更改过，更换主备之间的心跳线	
3	上网行为管理系统略配置意外丢失	通过上网行为管理系统还原备份配置文件，恢复正常工作；	
4	上网行为管理系统端口故障	若是上网行为管理系统端口物理损坏，更换网络接口卡，若端口物理状态正常，处于 down 状态，检查对端设备端口状态，或尝试更换新的光纤线。	

网行为管理系统巡检作业指导书

2013 年 11 月

一、作业准备

序号	所需资源	名称	备注
1	工具软件	无	
2	资料文档	上网管理系统维护手册	

二、巡检记录

项目名称	业务范围	巡检内容	备注
系统状态	硬件部分	系统 CUP、硬盘、内存使用率情况	
		会话连接数	
		WAN 实时流量	
	软件部分	许可情况	
		HA 集群状态检查	
系统日志检查	软件部分	系统日志检查	

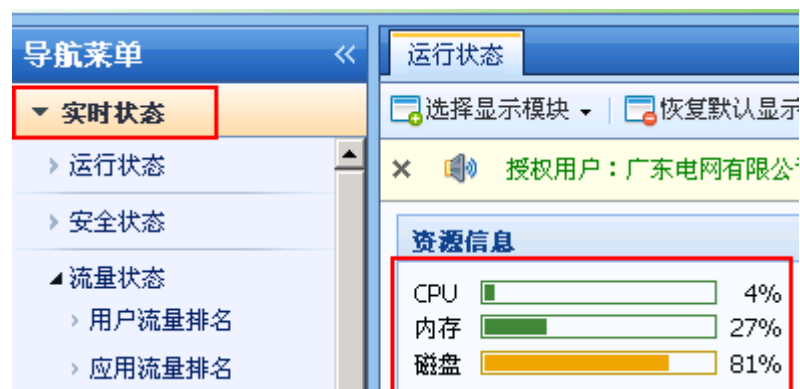
流量排名	软件部分	组流量排名	
		用户流量排名	
		应用流量排名	
		Ip 流量排名	

二、巡检步骤

4. 系统状态检查

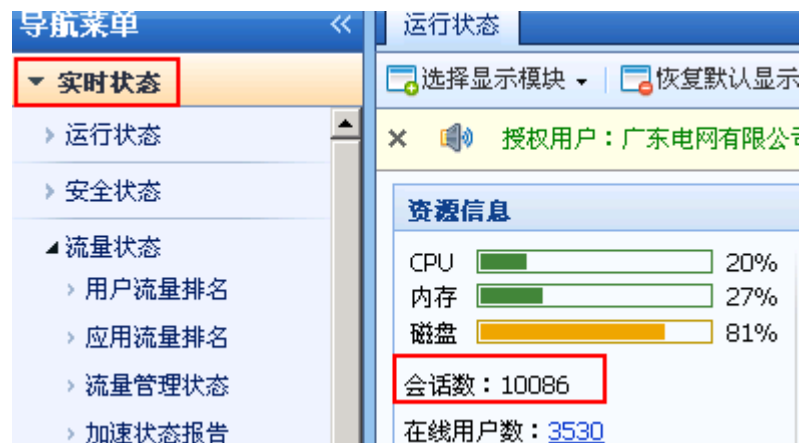
7.16 系统 CUP、硬盘、内存使用率情况

登陆网上管理系统，在实时状态中能看见当前CPU、内存、磁盘使用情况。



7.17 会话连接数

登陆网上管理系统，在实时状态中能看见当前会话连接数。



7.18 WAN 实时流量

登陆网上管理系统，在实时状态中能看见当前WAN实时流量。



7.19 许可证状态

登陆网上管理系统，在系统配置—序列号能看见许可信息。



7.20 HA 集群状态检查

登录上网管理系统，在网络配置中---双机维护—能看见与对端通信正常。



8. 系统日志分析

8.1 系统日志检查

登陆网上管理系统，在系统诊断中，系统日志里能看见日志信息。

导航菜单

实时状态

对象定义

用户与策略管理

流量管理

上网加速

安全防护

防火墙

网络配置

系统配置

系统诊断

系统日志

抓包工具

命令控制台

Bypass与拦截定位

重启操作

系统日志

日志选项设置

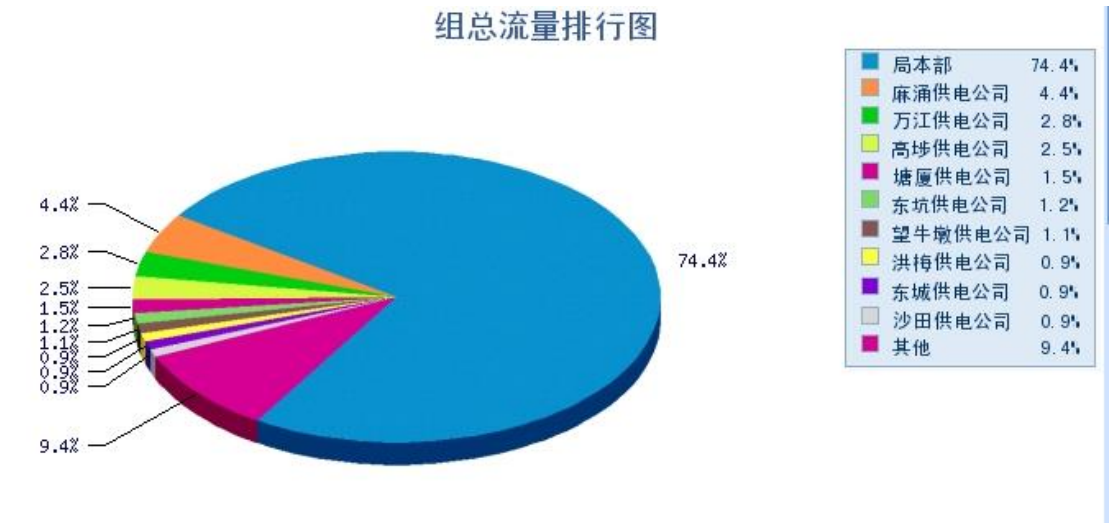
选择日期：20130916

序号	来源	类型	时间	详细信息
1	访问日志系统	信息	17:10:50	update ac User table ok.
2	访问日志系统	信息	17:10:49	update ac Group table ok.
3	双机热备	信息	16:29:56	[cluster]本端目前状态为【主机】，对端【备机】工作正常！向备机同步系统时间[2013-09-16 :
4	邮件代理	信息	16:10:47	Read Crc form contchkprivate ok: 1448942861, 3420019107, 1841528731
5	访问日志系统	信息	16:10:46	update ac User table ok.
6	访问日志系统	信息	16:10:45	update ac Group table ok.
7	网络准入系统	信息	16:10:44	没有启用准入规则
8	网络准入系统	信息	16:10:44	echo
9	应用审计	信息	16:10:44	i0.main.cpp:697 min_logtime = 600
10	WEB认证系统	信息	16:10:44	i0.loadconf.cpp:663 访问控制组配置更新
11	WEB认证系统	信息	16:10:44	i0.loadconf.cpp:646 访问控制用户配置更新
12	访问日志系统	信息	15:31:18	Read log days: 330
13	访问日志系统	信息	15:31:18	aclog used space : 362030936 kb, 362030936 kb
14	访问日志系统	信息	15:30:57	Calcualte attach file size for 15:27
15	访问日志系统	信息	15:30:57	exec sql success.sql:update AttachInfo set file_size = 38576128 where table_name =
16	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/actrace/20130916, the size is 38576128
17	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/ips/20130916, the size is 0
18	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
19	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/delaysnd/20130916, the size is 0
20	访问日志系统	信息	15:30:57	(dp = opendir(dir)) == NULL
21	访问日志系统	信息	15:30:57	Calcualte attach file size of /aclog/mailproxy/ass3log/20130916, the size is 0

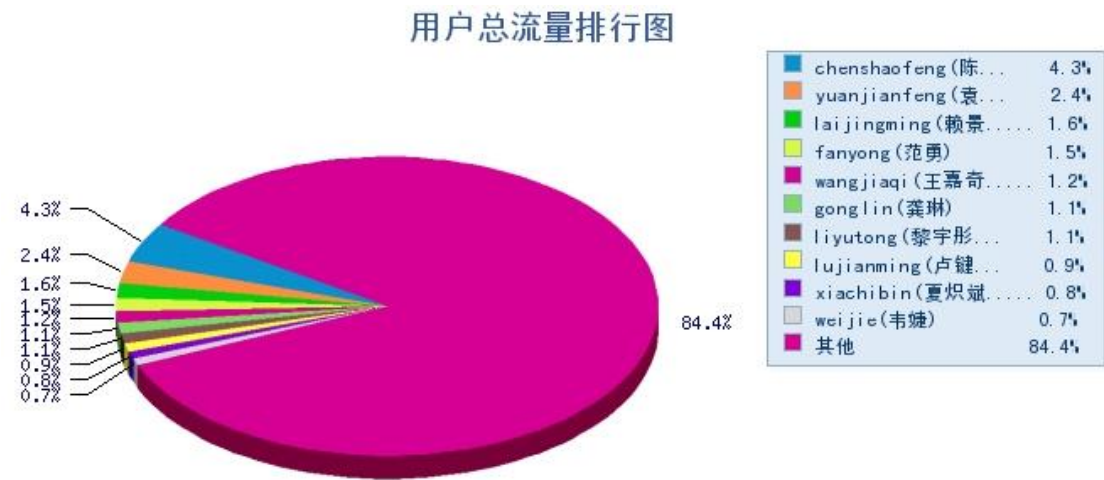
9. 流量排名

9.1 组流量排名

访问控制组流量排行榜：以dg. gpgc. local组的流量占比重较大



9.2 用户流量排行榜：

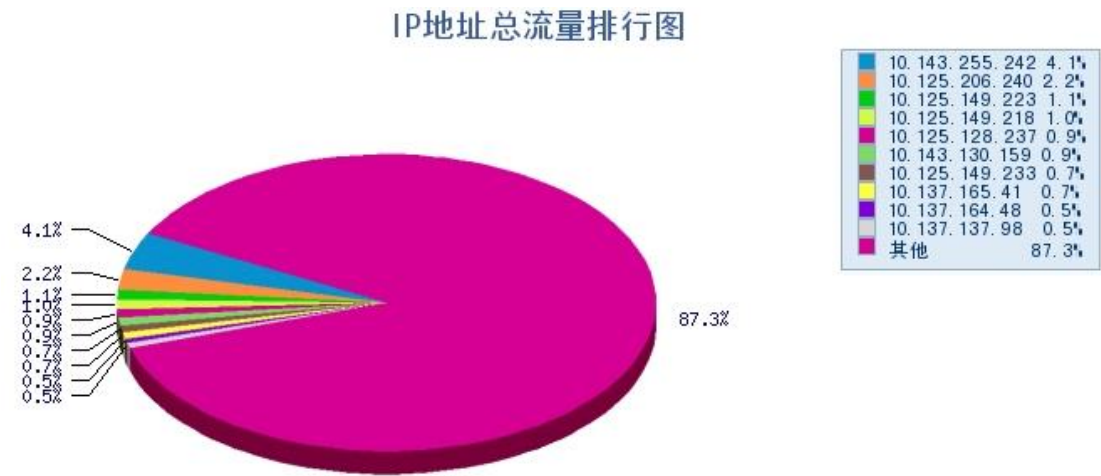


9.3 应用流量排行

应用流量排行：以访问网站的流量比重较大



9.4 IP 流量排行：



4、作业中异常现象及主要对策

序号	异常现象	处理对策	注意事项
1	上网行为管理系统的硬件出现故障	采取主备双机热备的部署模式，当其中一台出现故障时，另一台自动接替工作，保证业务不中断运行；联系原厂更换设备。	
2	主备无法切换	检查主备配置是否更改过，更换主备之间的心跳线	
3	上网行为管理系统略配置意外丢失	通过上网行为管理系统还原备份配置文件，恢复正常工作；	
4	上网行为管理系统端口故障	若是上网行为管理系统端口物理损坏，更换网络接口卡，若端口物理状态正常，处于 down 状态，检查对端设备端口状态，或尝试更换新的光纤线。	