

关于 8 月 29 日校园网出口速度减慢的说明

8 月 29 日早晨 9 点左右，网络信息技术中心发现校园网出口访问出现异常，校内主机到校园网四个出口的延时出现明显跃升现象，导致访问校外网站出现大面积故障。

经排查，学校出口网关设备持续接收到来自校内的碎片包，导致相关设备 CPU 接近满载状态，进而影响到整个校园网出口的链路通信质量。



图 1 出口网关设备的实时 CPU 负载图

经紧急处理，当日 11 点左右校园网出口基本恢复正常。

校园网出口监控

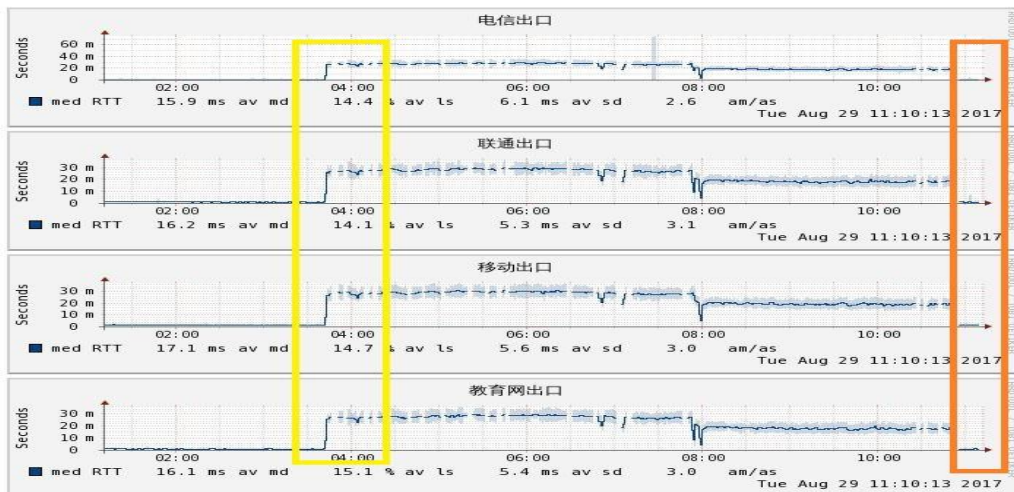


图 2 校园网出口监控显示 11 点左右恢复正常

经数据分析，信息源在某教学楼 9 层实验室内（IP 是 10.108.*.*）。该 IP 持续性地向外网 218.7.*.* 发送长度 109 字节的 UDP 数据包，大量碎片数据包造成了

网关设备的 CPU 超载。

No.	Time	Source	Destination	Protocol	Length	Info
33	0.014549	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
37	0.014626	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
41	0.014639	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
44	0.014653	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
49	0.014686	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
51	0.014700	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
57	0.014726	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
62	0.014743	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
67	0.014756	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
78	0.014769	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
90	0.014787	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
95	0.014800	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
104	0.014813	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
109	0.014828	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
115	0.014840	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
124	0.014866	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
128	0.014879	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
134	0.014892	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
139	0.014905	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
144	0.014918	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
149	0.014931	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
153	0.014950	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
229	0.015168	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
234	0.015187	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
237	0.015206	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
239	0.015219	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
240	0.015232	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
247	0.015250	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
252	0.015263	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
256	0.015276	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999
260	0.015289	10.108.1.2	218.7.219.90	UDP	109	source port: 3266 Destination port: 9999

图 3 网关设备的后台抓包数据

事后该实验室相关人员告知，该 IP 为年代较为久远的服务器设备，平常疏于管理，才导致了此次事件的发生。在此，中心特向全校用户做出如下安全建议：

(1) 安装使用正版操作系统和正版办公软件，中心已于 2017 年 4 月正式上线运行了正版化平台网站 <http://ca.bit.edu.cn>，校内师生用户可采用单点登录方式下载正版 Windows 和 Office 软件。

(2) 安装杀毒软件，且保持病毒库实时更新。

(3) 安全上网，不访问来路不明的网站，对于邮箱内未识别身份的发件人的邮件不轻易点击下载，防止中毒被黑成为“肉鸡”用户。

网络信息技术中心
2017.09.05