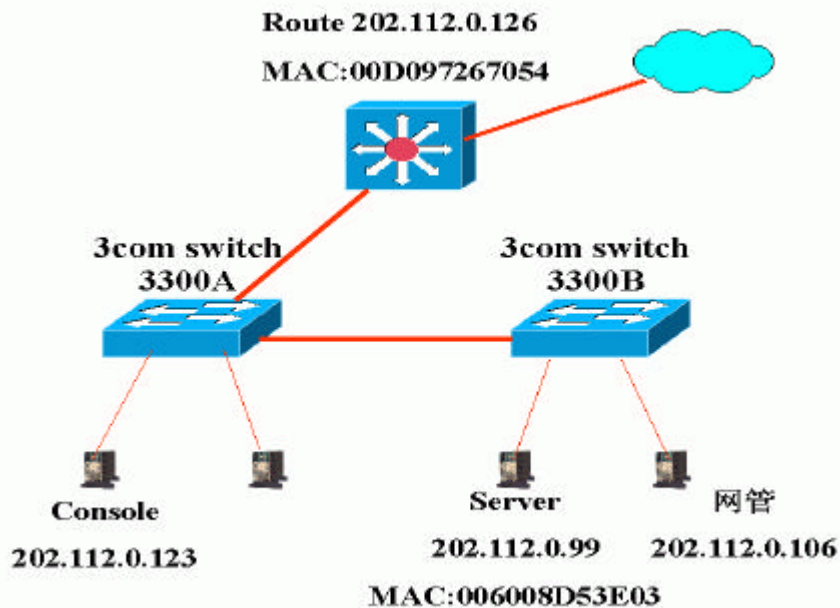


如何利用协议分析仪发现网络攻击型病毒
——FLUKE OptiView 网络综合协议分析应用实例
安恒公司 李瑞文

近期，应北京某高校的邀请，我们对该校的校园网络进行了系统的测试。在测试过程中碰巧遇到网络控制中心某网段出现故障，我们利用 FLUKE OptiView 网络综合协议分析仪及时的帮助发现并排除了故障，具体过程如下：

故障网段拓扑：

运行控制中心网络结构为两台 3com switch3300 以 10Mbps 速率级连，为便于区分我们下面以 3300A/3300B 命名，其中 3300A 级连到中心路由器上。某台重要的网管服务器（IP202.112.0.106）及众多服务器连接于 3300B 上，控制中心的控制平台（Console202.112.0.123）都连接于 3300A 上。



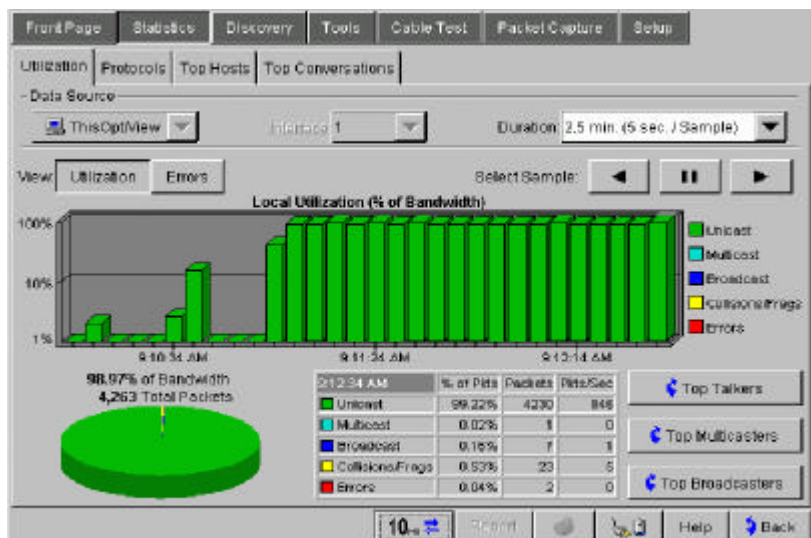
故障现象：

Console 访问网管服务器和其他所有设备的速度极慢，PING 其它设备几乎都没有回应。如果将 3300B 脱离 3300A，则上述现象全部消失，恢复连接后现象又重复出现。

测试与分析：

根据上述故障现象，我们初步判断问题可能同 3300B 及其所连接的设备有关。

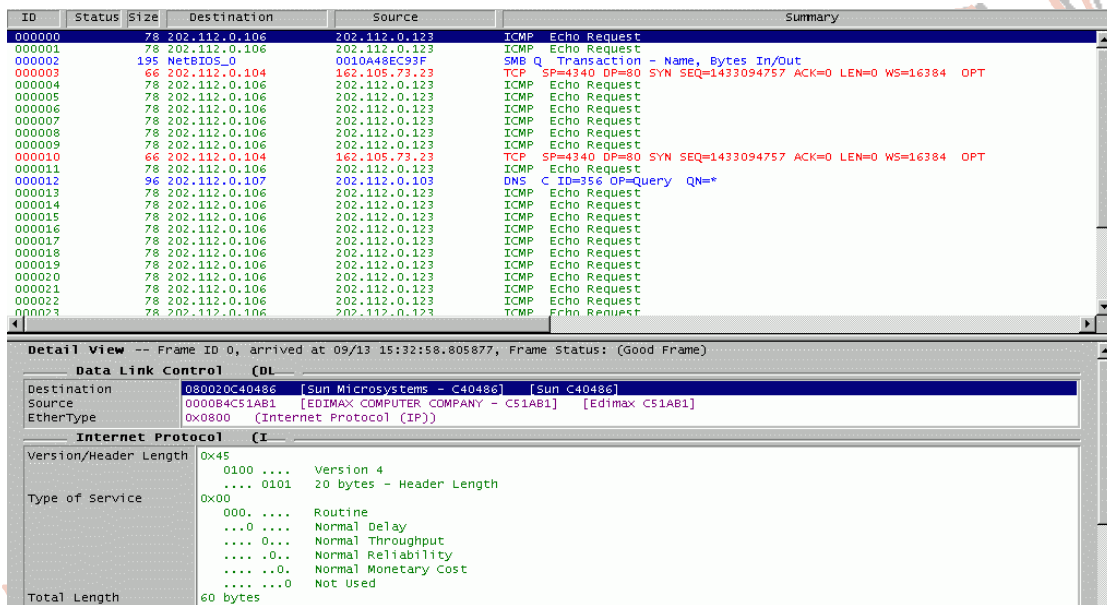
为了进一步判断故障是由硬件造成还是由于带宽阻塞造成，我们将一 10M 的 HUB 串在了 3300A 和 3300B 之间，然后将测试仪 OptiView 接入 HUB，这样就可以通过仪器来监测两个交换机之间的流量。



当仪器一接入 HUB，流量指示灯立刻显示网络的带宽利用率达到了 100%（图一），但没有报告任何帧错误，也没发现过多碰撞。为了确定这一现象不是由串入的 HUB 同交换机协商的速率不匹配造成的。我们分别用测试仪 FLUKE OneTouch 测试 3300A 和 3300B 互连的两个端口，结果 3300A 端口为 10Mbps，3300B 为 10/100Mbps 自适应，结合刚刚流量信息并未发现任何错误帧和冲突，我们可以判断 HUB 的连接状态是正确的。

由此看来，故障可能是由网络拥塞造成的。那么为什么会有如此高的流量？是什么应用导致如此高的流量？是谁造成的这样高的流量？这一连串的问题都是我们迫切需要的知道的。为了得到准确的答案，我们又进行了下述测试：

1. 将连接 3300B 到 HUB 的跳线去掉，利用 OptiView 中的协议分析功能捕捉从 3300A 过来的流量并进行解码分析，见下图：



通过对捕捉到的大量数据帧分析，我们发现大部分帧都是从 202.112.0.123 到网管服务器 202.112.0.206 的 ICMP Request 帧。而这是因为 Console202.112.0.123 为了配合我们的测试在一直不停的 PING 网管服务器 202.112.0.206 造成的，由于此时断掉了同 3300B 的连接，所以只有请求而无应答。还有两帧来自 162.105.73.23 到 202.112.0.104 TCP SYN（同步请求帧），其它帧的数量很少，并不存在异常流量。此时的带宽利用率为 3% 左右。

2. 恢复 3300B 到 HUB 的条线，将连接 3300A 到 HUB 的跳线去掉，利用 OptiView 中的协议分析功能捕捉从 3300B 过来的流量并进行解码分析，如下图：

000026	64	202.112.0.33	202.112.0.106	ICMP	Echo Request
000027	99	202.112.36.241	202.112.0.106	SNMP	ao (Get)
000028	64	202.112.0.35	202.112.0.106	ICMP	Echo Request
000029	64	202.112.0.36	202.112.0.106	ICMP	Echo Request
000030	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000031	99	202.112.36.241	202.112.0.106	SNMP	ao (Get)
000032	99	202.112.36.241	202.112.0.106	SNMP	ao (Get)
000033	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000034	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000035	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000036	64	202.112.0.56	202.112.0.106	ICMP	Echo Request
000037	64	202.112.0.70	202.112.0.106	ICMP	Echo Request
000038	64	202.112.3.65	202.112.0.106	ICMP	Echo Request
000039	64	202.112.4.65	202.112.0.106	ICMP	Echo Request
000040	64	202.38.99.36	202.112.0.106	ICMP	Echo Request
000041	64	202.112.0.34	202.112.0.106	ICMP	Echo Request
000042	64	202.112.0.33	202.112.0.106	ICMP	Echo Request
000043	64	202.112.0.35	202.112.0.106	ICMP	Echo Request
000044	64	202.112.0.36	202.112.0.106	ICMP	Echo Request
000045	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000046	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000047	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000048	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000049	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000050	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000051	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000052	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000053	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000054	64	BROADCAST	202.112.0.99	ARP	Q PA=202.112.0.126
000055	90	202.112.0.35	202.112.0.107	DNS	C ID=20920 OP=Query QN=13.103.81.209.in-addr.arpa.
000056	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000057	99	202.112.4.254	202.112.0.106	SNMP	ao (Get)
000058	81	202.112.0.34	202.112.0.100	DNS	C ID=54115 OP=Query QN=hotpop.net.edu.cn.
000059	64	BROADCAST	127.180.139.131	ARP	Q PA=202.112.0.126
000060	64	166.111.91.1	202.112.0.106	ICMP	Echo Request
000061	64	166.111.91.1	202.112.0.106	ICMP	Echo Request
000062	64	166.111.0.210	202.112.0.106	ICMP	Echo Request
000063	92	202.102.224.68	202.112.0.103	DNS	C ID=88 OP=Query QN=131.139.180.127.IN-ADDR.ARPA.
000064	64	166.111.0.209	202.112.0.106	ICMP	Echo Request
000065	64	166.111.0.206	202.112.0.106	ICMP	Echo Request
000066	64	166.111.0.205	202.112.0.106	ICMP	Echo Request
000067	64	166.111.0.202	202.112.0.106	ICMP	Echo Request
000068	64	166.111.0.201	202.112.0.106	ICMP	Echo Request
000069	64	202.112.36.241	202.112.0.106	ICMP	Echo Request
000070	64	202.112.53.113	202.112.0.106	ICMP	Echo Request
000071	64	202.112.63.243	202.112.0.106	ICMP	Echo Request
000072	64	202.112.63.243	202.112.0.106	ICMP	Echo Request
000073	64	202.112.38.210	202.112.0.106	ICMP	Echo Request

我们发现大部分帧 (84%) 都是从网管服务器 202.112.0.206 发出的到不同设备的 ICMP Request 帧和 SNMP GET 帧。经网络管理员核实, 这些目的地址都是合法的网络设备, 因为网管需要不停的轮询各个网络设备, 所以这些帧的存在是合理的。同时还发现有从 202.112.0.99 发出的 ARP 广播包解析默认网关 202.112.0.126 的 MAC, 如图:

Address Resolution Protocol (A)			
Hardware Type	1	(Ethernet)	
Protocol Type	0x0800	(IP)	
Hardware Addr Length	6	bytes	
Protocol Addr Length	4	bytes	
Operation	1	(Request)	
Sender Ethernet Addr	006008053E03	[3COM CORPORATION - D53E03]	[3com D53E03]
Sender IP Address	202.112.0.99		
Target Ethernet Addr	000000000000	[No Vendor Name. - 000000]	[000000000000]
Target IP Address	202.112.0.126		

ARP 占到了总帧数的 5%。此时测得的带宽利用率也仅为 2% 左右。

这样看来 3300B 也不存在明显问题, 那么为什么恢复两个交换机的连接后就会出现拥塞呢? 为此我们又进行第三步测试:

3. 将两台交换机都连接到 HUB, 同时将测试仪 OptiView 接入 HUB。这样就可以通过仪器捕捉二者之间的流量, 如图:

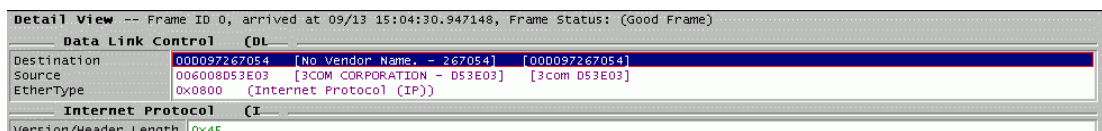
ID	Status	Size	Destination	Source	Summary
000000	64	193.13.70.249	41.205.231.13	TCP	SP=63550 DP=25276 SYN SEQ=1025939142 ACK=0 LEN=0 WS=65535
000001	64	193.13.70.249	61.135.245.134	TCP	SP=62583 DP=25277 SYN SEQ=1816711684 ACK=0 LEN=0 WS=65535
000002	64	193.13.70.249	99.117.54.168	TCP	SP=13623 DP=25278 SYN SEQ=2001231675 ACK=0 LEN=0 WS=65535
000003	64	193.13.70.249	27.153.114.118	TCP	SP=6127 DP=25279 SYN SEQ=1690381900 ACK=0 LEN=0 WS=65535
000004	64	193.13.70.249	255.132.168.41	TCP	SP=40335 DP=25280 SYN SEQ=647192118 ACK=0 LEN=0 WS=65535
000005	64	193.13.70.249	207.205.252.12	TCP	SP=12529 DP=25281 SYN SEQ=374810258 ACK=0 LEN=0 WS=65535
000006	64	193.13.70.249	104.104.150.203	TCP	SP=9676 DP=25282 SYN SEQ=1070534771 ACK=0 LEN=0 WS=65535
000007	64	193.13.70.249	107.3.174.135	TCP	SP=32464 DP=25283 SYN SEQ=165000669 ACK=0 LEN=0 WS=65535
000008	64	193.13.70.249	5.0.73.4	TCP	SP=44017 DP=25284 SYN SEQ=1945961773 ACK=0 LEN=0 WS=65535
000009	64	193.13.70.249	215.128.99.166	TCP	SP=22623 DP=25285 SYN SEQ=1043274674 ACK=0 LEN=0 WS=65535
000010	64	193.13.70.249	161.80.68.9	TCP	SP=15066 DP=25286 SYN SEQ=1490751956 ACK=0 LEN=0 WS=65535
000011	64	193.13.70.249	149.166.72.1	TCP	SP=37366 DP=25287 SYN SEQ=15510920 ACK=0 LEN=0 WS=65535
000012	64	193.13.70.249	75.199.133.80	TCP	SP=64719 DP=25288 SYN SEQ=1016883796 ACK=0 LEN=0 WS=65535
000013	64	193.13.70.249	76.192.130.35	TCP	SP=53989 DP=25289 SYN SEQ=1452019401 ACK=0 LEN=0 WS=65535
000014	64	193.13.70.249	142.89.123.48	TCP	SP=27839 DP=25290 SYN SEQ=1586381369 ACK=0 LEN=0 WS=65535
000015	64	193.13.70.249	78.153.14.227	TCP	SP=30294 DP=25291 SYN SEQ=1000183012 ACK=0 LEN=0 WS=65535
000016	64	193.13.70.249	234.76.108.53	TCP	SP=38898 DP=25292 SYN SEQ=1669101445 ACK=0 LEN=0 WS=65535
000017	64	193.13.70.249	219.193.217.39	TCP	SP=20827 DP=25293 SYN SEQ=1524791115 ACK=0 LEN=0 WS=65535
000018	64	193.13.70.249	194.65.20.81	TCP	SP=45200 DP=25294 SYN SEQ=2130712193 ACK=0 LEN=0 WS=65535
000019	64	193.13.70.249	27.79.186.105	TCP	SP=44232 DP=25295 SYN SEQ=91209565 ACK=0 LEN=0 WS=65535
000020	64	193.13.70.249	41.30.49.19	TCP	SP=46494 DP=25296 SYN SEQ=178872680 ACK=0 LEN=0 WS=65535
000021	64	193.13.70.249	126.144.205.89	TCP	SP=55974 DP=25297 SYN SEQ=882289537 ACK=0 LEN=0 WS=65535
000022	64	193.13.70.249	210.2.204.149	TCP	SP=43232 DP=25298 SYN SEQ=1995329766 ACK=0 LEN=0 WS=65535
000023	64	193.13.70.249	201.112.103.228	TCP	SP=49165 DP=25299 SYN SEQ=678709627 ACK=0 LEN=0 WS=65535

Data Link Control (DL)			
Destination	000097267054	[No Vendor Name. - 267054]	[000097267054]
Source	006008053E03	[3COM CORPORATION - D53E03]	[3com D53E03]
EtherType	0x0800	(Internet Protocol (IP))	
Internet Protocol (I)			
Version/Header Length	0x45		
	0100	Version 4	
 0101	20 bytes - Header Length	
Type of Service	0x00		
	000.	Routine	
 0000	Normal Relay	

仔细观察所捕捉到的帧, 问题出现了: 所有帧都是 TCP SYN (同步请求帧), 并且目的

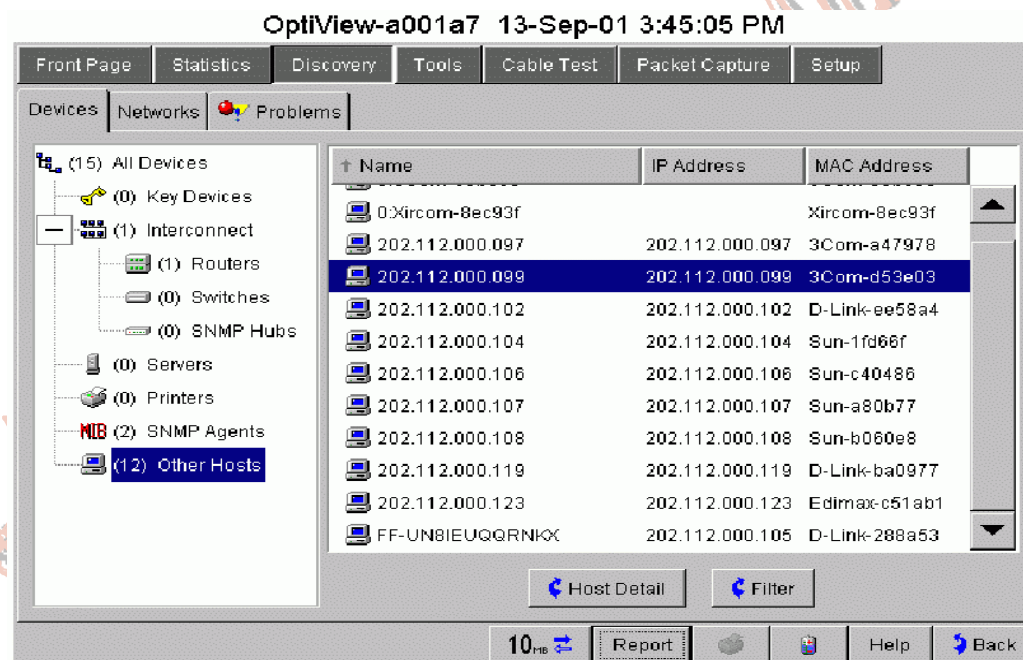
地址都是同一个——193.13.70.249，而源地址“天南地北”哪的都有（经网管核实均非本网地址），更奇怪的是这些来自不同 IP 地址的 TCP 流量发到 193.13.70.249 的 TCP 端口号却是从低到高非常有序的递增。是“病毒”，直觉告诉我们这是网络病毒在捣鬼。

为了证实这一判断，我们进一步进行解码分析发现，所有流量在数据链路层的封装完全相同，也就是说，所有帧的源地址（SA）都相同，所有帧的目的地址（DA）也都是相同的，如下图：



目的地址经查证确认为路由器 202.112.0.126，源地址为 MAC: 006008D53E03（3com 网卡地址）。那么这源地址是谁呢？

通过测试仪 OptiView 的网管功能，我们发现了它，见下图：



屏幕上清楚的显示出这块网卡所绑定的 IP 为 202.112.0.99，网卡地址为 3com-d53e03。

经过一番查找，终于我们在服务器架上找到了 IP 为 202.112.0.99 的设备。当我们把它的网线拔掉时，网络恢复了正常。

结论：

由于该服务器感染了具有攻击性的网络病毒，服务器通过伪装 IP 地址针对某一网络设备所有 TCP 端口发出大量流量以实现对该服务器的攻击。如此大的攻击性流量几乎占用了全部网络带宽，造成了网络拥塞。而当路由连接中断时由于链路中断，该服务器只是发出极少的 ARP 进行地址解析寻找默认网关，所以测试 2 并未能发现，可见此“病毒”的狡诈。