

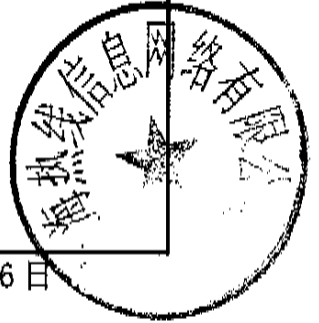
故障分析报告

HLWB/F/JL/D/0/WL-007-2009

主题	20110126 海量机房故障分析报告		
日期	2011-01-26	历时	125 分钟 ; 180 分钟
故障处理经过	<p>10: 15 机房监控报警, 发现核心交换机有告警。</p> <p>10: 20 工程师接到通知, 进行远端处理。流量监控图中发现海量机房核心交换机入站流量异常, 初步判定可能是遭到攻击所致, 经进一步排查确定为一台下联 Cisco2950 中 218.1.72.0 段受流量攻击。由于此时攻击流量较大影响到同交换机下其他网段正常通信。</p> <p>10: 40 对该网段数据流进行抓包分析, 确认为 IP 地址 218.1.72.48 受流量攻击攻击。</p> <p>11: 30 随即在本端核心交换机 6509 上启动流量清洗应急方案, 将攻击流量引入网络黑洞, 初步消除对其他业务影响。尽管在核心交换机上进行流量清洗将流量截至在核心层, 但无法阻止大量攻击流量进入上联链路占据一定量的出口带宽, 造成了部分网段有丢包和访问迟缓的现象</p> <p>12: 20 由于对流量进行了清洗攻击流量收不到攻击目标的响应, 攻击逐步停止, 部分网段逐步开始恢复。</p> <p>14: 30 监控发现有新的流量异常情况, 再次影响此核心交换机下联的网络。</p> <p>14: 50 通过再次抓包分析, 发现新的攻击情况, 此时攻击方式转为小包攻击, 造成了上联接路的入站队列被占满, 机房内用户有一部分发生了访问迟缓和丢包现象, 再次采用流量清洗方法消除攻击影响。</p> <p>15: 30 但是由于小包攻击的流量并不大, 不过会占满上联接路的入站队列, 造成在本端清洗流量的方法收效甚微, 于是联系上联链路对端单位在核心做流量清洗, 清除流量。</p> <p>17: 30 攻击流量消除, 受攻击影响的业务全部恢复。</p>		
原因分析	<p>本次故障起初由于是大流量攻击 218.1.72.48 造成上联链路阻塞, 同交换机下的用户影响最大, 其他用户有丢包延迟等影响, 其后发生小包攻击造成上联接口的入站队列塞满, 用户访问有丢包和延迟等情况发生</p>		



整改及建议	提升判障能力，跟踪“先抢通，后分析”原则，尽快恢复业务。 增加双上联冗余，增强网络安全。
-------	---



部门：维护操作中心 徐伟强

2011年1月26日