某大学城防病毒案例

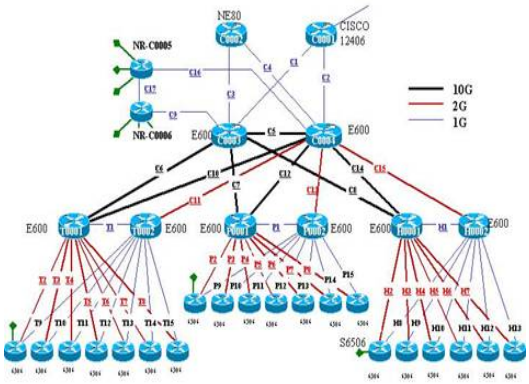
齐楠 2006-02-09 发表

某大学城防病毒案例

问题描述：

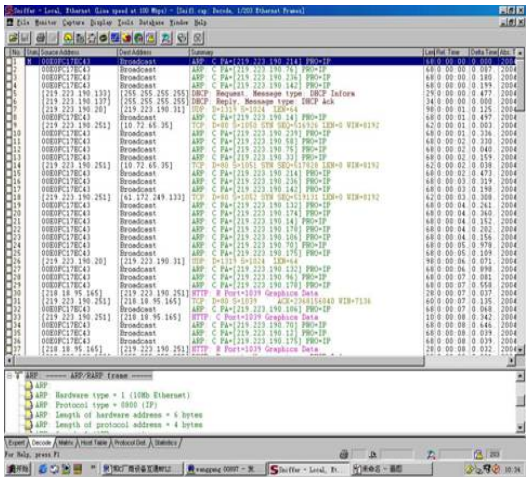
某大规模教育园区网络中，采用两台万兆交换机FORCE 10作为网络核心，三个分校区各采用两台FORCE 10作为校区核心，而采用我司的S6506共22台做为三级汇聚层交换机，并接入800多台接入交换机S3026E，接园区一万多个信息点，承载整个校园INTERNET业务。

设备拓扑图如下：



发生问题时，客户反馈S6506 出现 VLAN内不停的有ARP扫描（就是6506的VLAN INTERFACE不停的发本VLAN内每个IP地址的ARP REQUEST解析报文），网络速度很慢。

现场抓包记录如下：



在接入层交换机S3026E上的电脑上网发现网络速度缓慢,且S3026的cpu占用率也较高

处理过程：

通过使用抓包软件分析发现网络内有大量的ARP解析报文,从而导致网络速度缓慢,怀疑可能是网内有多台电脑感染病毒造成。

解决方案：

在上网PC机上安装天等防火墙个人版，通过看防火墙的攻击日志可以得知攻击是从219.223.180.155和219.223.169.54 这两台电脑来的,（由于是下班时间，可能网内还有其它电脑也感染）。所以在S6506上做:

acl number 110

rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 49 deny tcp destination-port eq 445
rule 50 deny udp destination-port eq 445
int g 1/0/1
qos
packet-filter inbound ip-group 110 not-carefo
以阻止病毒攻击。

由于是下班时间，所以无法得知这两台电脑的更详细的信息。如果没有防火墙个人版或者没有明确的病毒信息，可以添加如下列表测试：
rule 30 deny tcp destination-port eq 3127
rule 31 deny tcp destination-port eq 1025
rule 32 deny tcp destination-port eq 5554
rule 33 deny tcp destination-port eq 9996
rule 34 deny tcp destination-port eq 1068
rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 37 deny tcp destination-port eq 137
rule 38 deny udp destination-port eq netbios-ns
rule 39 deny tcp destination-port eq 138
rule 40 deny udp destination-port eq netbios-dgm
rule 41 deny tcp destination-port eq 139
rule 42 deny udp destination-port eq netbios-ssn
rule 43 deny tcp destination-port eq 593
rule 44 deny tcp destination-port eq 4444
rule 45 deny tcp destination-port eq 5800
rule 46 deny tcp destination-port eq 5900
rule 48 deny tcp destination-port eq 8998
rule 49 deny tcp destination-port eq 445
rule 50 deny udp destination-port eq 445
rule 51 deny udp destination-port eq 1434

结论：
对染毒电脑进行杀毒并对所有电脑加装微软的漏洞补丁，并安装防病毒软件，已彻底清除病毒对网络的影响。