S3526系列交换机中system-guard命令妙用 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/353/2021_2022_S3526_E7_B3_BB_E5_88_c101_353490.htm 问题描述： 某大学一台S3526下接的用户常常使用BT下载软件。如果在S3526上不开启system-guard命令则容易死机，但是开启这条命令的话有很多用户反映BT软件工作异常。 原因分析： 首先我们看一下system-guard命令原理： system-guard是以太网交换机实现的蠕虫病毒检测功能。交换机通过自动下发ACL方式使染毒主机下线，从而将染毒主机与网络隔离，保证网络其他主机不受感染，在超过一定时间后，交换机将恢复对这个染毒主机地址的正常转发流程。 也就是说这条命令限制了TCP并发连接数，它实时监控每一个进程的并发线程数目，只要超过了系统认为的安全线程数目就开始蔽屏掉部分线程。这是为了防止震荡波这类的蠕虫病毒，但是bt、emule这类的多线程的点对点工具也一起被同等对待了。于是不开启system-guard时，蠕虫病毒将导致设备死机，开启system-guard时导致很多用户BT软件工作异常。 首先掌握一下system-guard命令的配置： 使能system-guard检测功能：system-guard enable 禁止system-guard检测功能：undo system-guard enable 设置当前最大可检测染毒主机的数目： system-guard detect-maxnum number 恢复最大可检测的染毒主机数目至缺省值： undo system-guard detect-maxnum 设置地址学习数目的上限、重复检测次数的上限和隔离时间： system-guard detect-threshold IP-record-threshold record-times-threshold isolate-time 缺省情况下，system-guard地址学习数目的上限（IP-record-threshold）

、重复检测次数的上限（record-times-threshold）、隔离时间（isolate-time）分别为：30、1、3. 例如：在设置了地址学习数目的上限为50、重复检测次数的上限为3、隔离时间为5后，系统如果连续3次检测到来自某源IP的地址每次IP地址学习数目都超过了50，系统就认为受到了攻击，将此源IP检测出来，在5倍的老化周期内不学习来自此源IP的报文中的目的IP地址。 解决方法： 修改system-guard地址学习数目的上限值设为较大值（如50）问题得到解决（具体的参数值需要根据用户数量来确定，用户数量越多，该值应该越大）。 注： 除S3526系列交换机外，S3526E系列交换机也支持system-guard特性。 