交换机安全设置六大原则总结 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/234/2021_2022__E4_BA_A4_E6_8D_A2_E6_9C_BA_E5_c101_234056.htm 如何过滤用户通讯，保障安全有效的数据转发？如何阻挡非法用户，保障网络安全应用？如何进行安全网管，及时发现网络非法用户、非法行为及远程网管信息的安全性呢？ 这里我们总结了6 条近期交换机市场上一些流行的安全设置功能，希望对大家有所帮助。 L2-L4 层过滤 现在的新型交换机大都可以通过建立规则的方式来实现各种过滤需求。规则设置有两种模式，一种是MAC模式，可根据用户需要依据源MAC或目的MAC有效实现数据的隔离，另一种是IP模式，可以通过源IP、目的IP、协议、源应用端口及目的应用端口过滤数据封包；建立好的规则必须附加到相应的接收或传送端口上，则当交换机此端口接收或转发数据时，根据过滤规则来过滤封包，决定是转发还是丢弃。另外，交换机通过硬件“ 逻辑与非门 ”对过滤规则进行逻辑运算，实现过滤规则确定，完全不影响数据转发速率。 802.1X 基于端口的访问控制 为了阻止非法用户对局域网的接入，保障网络的安全性，基于端口的访问控制协议802.1X无论在有线LAN或WLAN中都得到了广泛应用。例如华硕最新的 GigaX2024/2048等新一代交换机产品不仅仅支持802.1X 的Local、RADIUS 验证方式，而且支持802.1X 的Dynamic VLAN 的接入，即在VLAN和802.1X 的基础上，持有某用户账号的用户无论在网络内的何处接入，都会超越原有802.1Q 下基于端口VLAN 的限制，始终接入与此账号指定的VLAN组内，这一功能不仅为网络内的移动用户对资源的

应用提供了灵活便利，同时又保障了网络资源应用的安全性；另外， GigaX2024/2048 交换机还支持802.1X的Guest VLAN功能，即在802.1X的应用中，如果端口指定了Guest VLAN项，此端口下的接入用户如果认证失败或根本无用户账号的话，会成为Guest VLAN 组的成员，可以享用此组内的相应网络资源，这一种功能同样可为网络应用的某一些群体开放最低限度的资源，并为整个网络提供了一个最外围的接入安全。流量控制（traffic control） 交换机的流量控制可以预防因为广播数据包、组播数据包及因目的地址错误的单播数据包数据流量过大造成交换机带宽的异常负荷，并可提高系统的整体效能，保持网络安全稳定的运行。 SNMP v3 及SSH 安全网管SNMP v3 提出全新的体系结构，将各版本的SNMP 标准集中到一起，进而加强网管安全性。SNMP v3 建议的安全模型是基于用户的安全模型，即USM.USM对网管消息进行加密和认证是基于用户进行的，具体地说就是用什么协议和密钥进行加密和认证均由用户名称（userNmae）权威引擎标识符（EngineID）来决定（推荐加密协议CBCDES，认证协议HMAC-MD5-96 和HMAC-SHA-96），通过认证、加密和时限提供数据完整性、数据源认证、数据保密和消息时限服务，从而有效防止非授权用户对管理信息的修改、伪装和窃听。 至于通过Telnet 的远程网络管理，由于Telnet 服务有一个致命的弱点它以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令，受到攻击，但采用SSH进行通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听，便于网管人员进行远程的安全网络管理。 Syslog 和Watchdog 交换机的Syslog 日志功能可以将系统错误、系统

配置、状态变化、状态定期报告、系统退出等用户设定的期望信息传送给日志服务器，网管人员依据这些信息掌握设备的运行状况，及早发现问题，及时进行配置设定和排障，保障网络安全稳定地运行。 Watchdog 通过设定一个计时器，如果设定的时间间隔内计时器没有重启，则生成一个内在CPU重启指令，使设备重新启动，这一功能可使交换机在紧急故障或意外情况下时可智能自动重启，保障网络的运行。 双映像文件 一些最新的交换机， 像A S U SGigaX2024/2048还具备双映像文件。这一功能保护设备在异常情况下（固件升级失败等）仍然可正常启动运行。文件系统分majoy和 mirror两部分进行保存，如果一个文件系统损害或中断，另外一个文件系统会将其重写，如果两个文件系统都损害，则设备会清除两个文件系统并重写为出厂时默认设置，确保系统安全启动运行。 其实，近期出现的一些交换机产品在安全设计上大都下足了功夫层层设防、节节过滤，想尽一切办法将可能存在的不安全因素最大程度地排除在外。广大企业用户如果能够充分利用这些网络安全设置功能，进行合理的组合搭配，则可以最大限度地防范网络上日益泛滥的各种攻击和侵害，愿您的企业网络自此也能更加稳固安全。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com