虚拟LAN安全的最佳实践经验 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E8_99_9A_E6_8B_9FLAN_E5_c101_142564.htm 独立的安全调研公司 @stake [9] 最近对 Cisco Catalyst 2950 、 Catalyst 3550 、 Catalyst 4500 和 Catalyst 6500 系列交换机上采用的虚拟 LAN （ VLAN ）技术进行了一次安全检查 [1] 。虽然此次检查没有暴露出严重的安全漏洞，但必须指出的是，如果交换机的配置不正确或不适当，则很有可能引发意外行为或发生安全问题。 去年，思科系统公司一直致力于在若干文档中制定安全网络配置的最佳实践准则，例如《 SAFE 蓝图》 [2] 或《 Catalyst 4500 、 5000 和 6500 系列交换机最佳实践经验》 [3] 。但是，迄今为止，思科还没有提供一本全面介绍与 VLAN 相关的所有最佳实践经验、可方便客户和现场工程师参考的文档。 本文的目的是全面介绍思科工程师多年积累的丰富经验和建议，帮助客户和现场工程师正确地在思科交换机上配置 VLAN 。除此以外，本文还将通过要点说明解释 @stake 测试的主要结果，阐述解决安全问题的方法。 基本安全准则 要想创建安全的交换网，必须先熟悉基本安全准则。需要特别注意的是， SAFE 最佳实践 [2] 中强调的基本准则是设计任何安全交换网的基石。 如果用户不希望任何设备受损，则必须严格控制对该设备的访问。不仅如此，所有网络管理员都应该使用思科平台上提供的所有实用安全工具，包括系统密码的基本配置、 IP 准入过滤器和登陆检查，以及 RADIUS 、 TACACS 、 Kerberos 、 SSH 、 SNMPv3 、 IDS 等更先进的工具（详情参见 [3] ）。 必须使所有基本安全准则得到满足之后，再关注

更先进的安全细节。在下面的章节中，我们将说明与 VLAN 相关的问题。 虚拟 LAN 第二层（ L2 ）交换机指能够将若干端口组成虚拟广播域，且各虚拟广播域之间相互隔离的设备。这些域一般称为虚拟 LAN （ VLAN ）。 VLAN 的概念与网络领域中的其它概念相似，流量由标记或标签标识。标识对第二层设备非常重要，只有标识正确，才能隔离端口并正确转发接收到的流量。正如后面章节中将要介绍的那样，缺乏标识有时是引发安全问题的原因，因而需要避免。 如果设备中的所有分组与相应 VLAN 标记紧密结合，则能够可靠区分不同域的流量。这就是 VLAN 交换体系结构的基本前提。 值得注意的是，在物理链路（有时称为干线）上，思科设备使用的是 ISL 或 802.1Q 等常用的 VLAN 标记技术。与此同时，思科设备使用先进标记技术在内部保留 VLAN 信息，并用于流量转发。 此时，我们可以得出这样的结论：如果从源节点发送出去之后，分组的 VLAN 标识不能被修改，即保持端到端不变，则 VLAN 的可靠性应等价于物理安全性。 关于这个问题，我们还将在下面详细讨论。 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