OSI第二层网络架构安全要素 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/271/2021_2022_OSI_E7_AC_AC_E4_BA_8C_E5_c101_271539.htm 许多安全管理员多关注网络层和应用层的安全问题，经常会忽略Layer2网络架构（数据链路层），同时这也是网络安全和可靠性方面最容易被人忽视的一个方面。在本文中，我会向你展示如何修正交换机配置以及架构方面最常见的错误。虽然我使用Cisco来作为我的例子，但是同样的策略和所讨论的教训一样适用于其他厂商。这些安全手续对任何数据网络来说都是必须的，特别是在使用IP电话的时候。 启用SSh，禁止Telnet 对于一台Cisco设备来说，最明显需要设置的就是口令和启用加密了。如果你让它保持空白的话，你的交换机就等于是在敞开大门，任何人都可以查看并攻击你的VLAN设置。如果你有多台交换机，以及多位系统管理员时，最好使用AAA认证模式，并使用一个本地用户数据库，集中的TACACS，或者RADIUS服务器来管理所有的交换机和系统管理员。使用TACACS 可能是更正确的选择，因为它可以记录下所有的事件，以便你有一个历史记录，可以记录下所有做出的修改，以及是谁在你的交换机和路由器架构中做出了修改。不过要记住，最重要的事情是，不惜任何代价禁止Telnet，并持续的对所有交换机部署SSH.即便你的交换机上并没有一个启用加密的软件镜像，所有的当前镜像也依然可以让你SSH进交换机。为每一个系统管理员都建立一个独一无二的用户名以及口令。然后，你应当启用SSH，并干掉Telnet. 在Cisco Native IOS上启用SSH，禁止Telnet 命令 描述 username admin1 privilege 15 password 0

Admin-Password 建立一个叫做admin1的系统管理员，每一个管理都必须重复。 aaa new-model 使用一个本地数据库，设置为AAA模式 aaa authentication login default local aaa authorization exec default local aaa authorization network default local aaa session-id common ip domain name MyDomain.com 建立一个用于认证的名字 crypto key generate rsa 建立数字证书。使用至少768位的Diffie-Hellman关键字 line vty 0 4 进入vty配置 transport input ssh 仅仅允许SSH登录 在 Cisco Catalyst OS上启用SSH，禁止Telnet 命令 描述 set crypto key rsa 1024 生成一个1024位的RSA key set ip permit 10.0.10.0 255.255.255.0 ssh 明确仅允许指定IP范围内的地址SSH set ip enable 要注意，对Cisco Native IOS交换机来说，Native IOS命令同样可以工作在Cisco IOS路由器上。无法使用SSH可能会导致口令被窃，并让攻击者获得对交换架构完全的控制权。 锁闭VTP及SNMP的安全 这听起来很难令人相信，但是在我当顾问的日子里，我看到过大量的网络根本不曾在他们的Cisco交换机中配置VTP域口令。如果你把它以默认值丢在那里的话，那么你就相当于拱手交出了国门的钥匙，并将你的整个交换机架构公布在了网页上，任何人都可以看到它。在“ configt ”的全局配置模式中使用下述命令，或者在较老的Cisco软件镜像中使用“ vlandata ”的VLAN数据库模式，来锁闭你的VTP配置。务必确认使用你自己的字符串以及IP地址，来取代示例中的相关参数。 在 Cisco Native IOS上配置VTP 命令 描述 vtp domain My-VTP-name 设置VTP名字 vtp password My-VTP-password 设置VTP口令 vtp pruning 打开VTP修剪 在Cisco Catalyst OS上配置VTP 命令 描述 set vtp domain My-VTP-name 设置VTP名字

set vtp passwd My-VTP-password 设置VTP口令 set vtp pruning enable 打开VTP修剪 你同样也应当设置你的SNMP（SNMP版本3更合适）秘密，这些是有效的口令。检查此文档，以获取对Cisco SNMP管理的完全指南。下面是个示例，用于演示如何使用正确的口令，在“ config t ”的全局配置模式下，配置一个SNMP只读及读写的服务器。 为Cisco Native IOS配置SNMP 命令 描述 snmp-server community MY-Read-Only-string ro 50 对来自ACL 50的SNMP请求设置只读字串 snmp-server community MY-Read-Write-string rw 51 对来自ACL 51的SNMP请求设置读写字串 access-list 50 permit IP-address-ro 建立只读SNMP服务器ACL。允许多于一个。 access-list 51 permit IP-address-rw 建立读写 为Cisco Catalyst OS配置SNMP 命令 描述 set snmp community read-only read-only-string 设置只读字串 set snmp community read-write read-write-string 设置读写字串 set snmp community read-write-all rwo-string 设置全部读写字串 如果你根本不打算使用SNMP，你应当在Native IOS之中，在全局配置模式下，使用“ no snmp-server ”命令将其彻底关闭。这样你就可以跳过前述的所有SNMP命令，直接阅读下文。 基础端口锁闭 交换机应当像安全领域中的其他事物一样，使用那种最低权限的理念。设置一个交换机的最好方法就是在部署时先关闭所有的端口，然后再一一打开自己需要的端口。除此以外，你应当将每一个端口都放入一个不曾使用的，无处可去，没有默认网关的VLAN之中。你可以建立一个名为“ unused（不曾使用）”的VLAN，并使用一个指定的数字，比如333，然后将所有的端口都放入这个VLAN之中。在下面的例子里，我们将使用

一台基于传统CIscoIOS的48口交换机。 