如何保证交换机端口安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E4_BF_9D_E8_c101_461768.htm 网络管理员面临的一个日渐严峻的挑战是决定哪些人可以访问单位内部的网络，哪些人不可以。如果公司需要演示某个外来客户的产品,将以太网电缆从公司内部一台计算机上拔下来，插到的客户电脑上。这样一来，他计算机内部的蠕虫、病毒什么的对你的局域网就是一个极大威胁了。今天我们看一下怎样通过配置交换机端口来解决类似的安全问题。 从基本原理上讲，Port Security(端口安全)特性记住的是连接到交换机端口的以太网MAC地址即网卡号，并只允许某个MAC地址通过本端口通信。如果任何其它MAC地址试图通过此端口通信，端口安全特性会阻止它。使用端口安全特性可以防止某些设备访问网络，并增强安全性。 配置端口安全是相对比较简单的。最简单的形式，就是Port Security需要指向一个已经启用的端口并输入Port Security接口模式命令。 Switch)# config t Switch(config)# int fa0/18 Switch(config-if)# switchport port-security aging Port-security aging commands mac-address Secure mac address maximum Max secure addresses violation Security violation mode Switch(config-if)# switchport port-security Switch(config-if)#^Z 在此我们通过输入最基本的命令来配置端口安全，接授了只允许一个MAC地址的默认设置，这就决定了只有第一个设备的MAC地址可以与这个端口通信；如果另一MAC地址试图通过此端口通信，交换机会关闭此端口。下面谈一下如何可以改变此设置。 当然应该根据实际情况来配

置端口安全。此例中，实际上用户还可以配置其它的端口安全命令： switchport port-security maximum {允许的最多MAC地址数量}:可以使用这个选项允许多个MAC地址。例如，如果用户有一个12端口的集线器连接到交换机的此端口，就需要12个MAC：switchport port-security maximum 12 /允许此端口通过的最大MAC地址数目为12。 switchport port-security violation {shutdown | restrict | protect}:此命令告诉交换机当端口上MAC地址数超过了最大数量之后交换机应该怎么做。默认是关闭端口。我们可以选择使用restrict来警告网络管理员，也可以选择protect来允许通过安全端口通信并丢弃来自其它MAC地址的数据包。 switchport port-security mac-address {MAC 地址}:使用此选项来手动定义允许使用此端口的MAC地址而不是由端口动态地定义MAC地址。 当然，你可以在一系列端口上配置端口安全。下面举一个例子： Switch)# config t Switch(config)# int range fastEthernet 0/1 - 24 Switch(config-if)# switchport port-security 然而，如果在一个UPLINK端口上输入此命令，用户必须十分小心使用此选项，因为它指向不只一个设备，第二个设备一旦发送一个数据包，整个端口就会关闭，这样可就麻烦了。 一旦你配置了端口安全而此端口上的以太网设备又发出了数据，交换机会记录下MAC地址而且通过使用这个地址来保障端口安全。要查看交换机上端口安全状态，可以使用show port security address 和show port-security interface命令。举例说明如下： Switch# show port-security address Switch# show port-security interface fa0/18 Port Security : Enabled Port Status : Secure-up Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging :

Disabled Maximum MAC Addresses : 1 Total MAC Addresses : 1 Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Last Source Address : 0004.00d5.285d Security Violation Count : 0 Switch#