安全技巧提高交换机端口的安全性 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/0/2021_2022__E5_AE_89_E5_85_A8_E6_8A_80_E5_c99_486.htm 导读:企业网络安全涉及到方方面面。从交换机来说，首选需要保证交换机端口的安全。在不少企业中，员工可以随意的使用集线器等工具将一个上网端口增至多个，或者说使用自己的笔记本电脑连接到企业的网路中。类似的情况都会给企业的网络安全带来不利的影响。在这篇文章中，笔者就跟大家谈谈，交换机端口的常见安全威胁及应对措施。 一、常见安全威胁 在企业中，威胁交换机端口的行为比较多，总结一下有如下几种情况。 一是未经授权的用户主机随意连接到企业的网络中。如员工从自己家里拿来一台电脑，可以在不经管理员同意的情况下，拔下某台主机的网线，插在自己带来的电脑上。然后连入到企业的网路中。这会带来很大的安全隐患。如员工带来的电脑可能本身就带有病毒。从而使得病毒通过企业内部网络进行传播。或者非法复制企业内部的资料等等。 二是未经批准采用集线器等设备。有些员工为了增加网络终端的数量，会在未经授权的情况下，将集线器、交换机等设备插入到办公室的网络接口上。如此的话，会导致这个网络接口对应的交换机接口流量增加，从而导致网络性能的下降。在企业网络日常管理中，这也是经常遇到的一种危险的行为。 在日常工作中，笔者发现不少网络管理员对于交换机端口的安全性不怎么重视。这是他们网络安全管理中的一个盲区。他们对此有一个错误的认识。以为交换机锁在机房里，不会出大问题。或者说，只是将网络安全的重点放在防火墙等软件上，而忽

略了交换机端口等硬件的安全。这是非常致命的。 二、主要的应对措施 从以上的分析中可以看出，企业现在交换机端口的安全环境非常的薄弱。在这种情况下，该如何来加强端口的安全性呢？如何才能够阻止非授权用户的主机联入到交换机的端口上呢？如何才能够防止未经授权的用户将集线器、交换机等设备插入到办公室的网络接口上呢？对此笔者有如下几个建议。 一是从意识上要加以重视。笔者认为，首先各位网络管理员从意识上要对此加以重视。特别是要消除轻硬件、重软件这个错误的误区。在实际工作中，要建立一套合理的安全规划。如对于交换机的端口，要制定一套合理的安全策略，包括是否要对接入交换机端口的MAC地址与主机数量进行限制等等。安全策略制定完之后，再进行严格的配置。如此的话，就走完了交换机端口安全的第一步。根据交换机的工作原理，在系统中会有一个转发过滤数据库，会保存MAC地址等相关的信息。而通过交换机的端口安全策略，可以确保只有授权的用户才能够接入到交换机特定的端口中。为此只要网络管理员有这个心，其实完全有能力来保障交换机的端口安全。 二是从技术角度来提高端口的安全性。如比较常用的一种手段是某个特定的交换机端口只能够连接某台特定的主机。如现在用户从家里拿来了一台笔记本电脑。将自己原先公司的网线接入到这台笔记本电脑中，会发现无法连入到企业的网络中。这时因为两台电脑的MAC地址不同而造成的。因为在交换机的这个端口中，有一个限制条件。只有特定的IP地址才可以通过其这个端口连入到网络中。如果主机变更了，还需要让其允许连接这个端口的话，那么就需要重新调整交换机的MAC地址设置。这种手段的好处就是

可以控制，只有授权的主机才能够连接到交换机特定的端口中。未经授权的用户无法进行连接。而缺陷就是配置的工作量会比较大。在期初的时候，需要为每个交换机的端口进行配置。如果后续主机有调整或者网卡有更换的话(如最近打雷损坏的网卡特别多)，那么需要重新配置。这就会导致后续工作量的增加。如果需要进行这个MAC地址限制的话，可以通过使用命令switchport port security mac-address来进行配置。使用这个命令后，可以将单个MAC地址分配到交换机的每个端口中。正如上面所说的，要执行这个限制的话，工作量会比较大。 三是对可以介接入的设备进行限制。出于客户端性能的考虑，我们往往需要限制某个交换机端口可以连接的最多的主机数量。如我们可以将这个参数设置为1，那么就只允许一台主机连接到交换机的端口中。如此的话，就可以避免用户私自使用集线器或者交换机等设备拉增加端口的数量。不过这种策略跟上面的 MAC地址策略还是有一定的区别。MAC地址安全策略的话，也只有一台主机可以连接到端口上。不过还必须是MAC地址匹配的主机才能够进行连接。而现在这个数量的限制策略，没有MAC地址匹配的要求。也就是说，更换一台主机后，仍然可以正常连接到交换机的端口上。这个限制措施显然比上面这个措施要宽松不少。不过工作量上也会减少不少。要实现这个策略的话，可以通过命令swichport-security maximun来实现。如故将这个参数设置为1，那么就只允许一台主机连接到交换机的端口之上。这就可以变相的限制介入交换机或者集线器等设备。不过这里需要注意的是，如果用户违反了这种情况，那么交换机的端口就会被关闭掉。也就是说，一台主机都连接不到这个端口上。

在实际工作中，这可能会殃及无辜。所以需要特别的注意。四是使用sticky参数来简化管理。在实际工作中，sticky参数是一个很好用的参数。可以大大的简化MAC地址的配置。如企业现在网络部署完毕后，运行以下switch-port port-security mac-addres sticky命令。那么交换机各个端口就会自动记住当前所连接的主机的MAC地址。如此的话，在后续工作中，如果更换了主机的话，只要其MAC地址与原有主机不匹配的话，交换机就会拒绝这台主机的连接请求。这个参数主要提供静态MAC地址的安全。管理员不需要再网络中输入每个端口的MAC地址。从而可以简化端口配置的工作。不过如果后续主机有调整，或者新增主机的话，仍然需要进行手工的配置。不过此时的配置往往是小范围的，工作量还可以接受。 最后需要注意的是，如果在交换机的端口中同时连接PC主机与电话机的时候，需要将Maximun参数设置为2。因为对于交换机端口来说，电话机与PC机一样，都是属于同类型的设备。如果将参数设置为1，那么就会出现问题。在电话机等设备集成的方案中设置端口安全策略时，需要特别注意这一点。很多网络管理员在实际工作中，会在这个地方载跟斗。 可见，要实现交换机的端口安全难度也不是很大，主要是网络管理员需要有这方面的观念。然后使用交换机的端口安全特性，就可以保障交换机的端口安全。以上介绍的几种方法，各有各的特点。在可操作性上与安全性上各有不同。网络管理员需要根据自己公司网络的规模、对于安全性的要求等各个方面的因素来选择采用的方案。总之，在网络安全逐渐成为管理员心头大患的今天，交换机的端口安全必须引起大家的关注。 编辑特别推荐: #0000ff>中小企业防范 “ 网页式社交工程

”恶意攻击 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