 最近，要求做端口安全的case越来越多。这里指的端口安全主要是通过绑定客户端MAC来限制端口接入的访问，vlan间的ACL不在今天的范围。 通过几天的实际调试，借鉴了前辈的经验，同时总结自己的调试心得，总结如下： 1、Cisco29系列交换机可以做基于2层的端口安全，即mac地址与端口进行绑定。 2、 Cisco3550以上交换机均可做基于2层和3层的端口安全，即mac地址与端口绑定以及mac地址与ip地址绑定。 3、以cisco3550交换机为例 做mac地址与端口绑定的可以实现两种应用： a、设定一端口只接受第一次连接该端口的计算机mac地址，当该端口第一次获得某计算机mac地址后，其他计算机接入到此端口所发送的数据包则认为非法，做丢弃处理。 b、设定一端口只接受某一特定计算机mac地址，其他计算机均无法接入到此端口。 4、破解方法：网上前辈所讲的破解方法有很多，主要是通过更改新接入计算机网卡的mac地址来实现，但本人认为，此方法实际应用中基本没有什么作用，原因很简单，如果不是网管，其他一般人员平时根本不可能去注意合法计算机的mac地址，一般情况也无法进入合法计算机去获得mac地址，除非其本身就是该局域网的用户。 