解决IP地址冲突的完美方法 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_A7_A3_E5_86_B3IP_E5_9C_c101_142436.htm 使用的方法是采用DHCP方式为用户分配IP，然后限定这些用户只能使用动态IP的方式，如果改成静态IP的方式则不能连接上网络；也就是使用了DHCP SNOOPING功能。 例子： version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption service compress-config ! hostname C4-2_4506 ! enable password xxxxxxx! clock timezone GMT 8 ip subnet-zero no ip domain-lookup ! ip dhcp snooping vlan 180-181 // 对哪些VLAN 进行限制 ip dhcp snooping ip arp inspection vlan 180-181 ip arp inspection validate src-mac dst-mac ip errdisable recovery cause udld errdisable recovery cause bpduguard errdisable recovery cause security-violation errdisable recovery cause channel-misconfig errdisable recovery cause pagp-flap errdisable recovery cause dtp-flap errdisable recovery cause link-flap errdisable recovery cause l2ptguard errdisable recovery cause psecure-violation errdisable recovery cause gbic-invalid errdisable recovery cause dhcp-rate-limit errdisable recovery cause unicast-flood errdisable recovery cause vmps errdisable recovery cause arp-inspection errdisable recovery interval 30 spanning-tree extend system-id ! ! interface GigabitEthernet2/1 // 对该端口接入的用户进行限制，可以下联交换机 ip arp inspection limit rate 100 arp timeout 2 ip dhcp snooping limit rate 100 ! interface GigabitEthernet2/2 ip arp inspection limit rate 100 arp timeout 2 ip dhcp snooping limit rate

100 ! interface GigabitEthernet2/3 ip arp inspection limit rate 100 arp timeout 2 ip dhcp snooping limit rate 100 ! interface GigabitEthernet2/4 ip arp inspection limit rate 100 arp timeout 2 ip dhcp snooping limit rate 100 --More-- 简单介绍一下这个解决方案的来历: 我是某个高校的网络管理员（假假的），我校所有学生宿舍区、教学区都使用了CISCO的设备接入了网络（有 8台 CISCO6509 , 2台CISCO 7613 ，30多台的CISCO 4506 , 二百多台的各系列的CISCO2950 ，学生入网数目 > 10000 ），与其他人的问题一样，我们的最大问题就IP地址冲突的问题，以前我们的解决办法是在2950上把IP与端口绑定，但是，在2004年的时候，我们又购买了一大批的CISCO2950T-48-SI ，而这些设备不支持二层的ACL，所以上述的方法失效了。就这个问题，我们和网络集成商、思科的技术人员讨论了许久的以求解决方案，虽然他们好几个都是什么CCIE的，但就是没有什么好的方案。直到在04年底我参加了思科在北京的用户大会，与思科总部的一个鬼佬CCIE讨论，他给出了上诉的解决方案。回来后立即实施，效果非常理想。 IP Source Guard Similar to DHCP snooping, this feature is enabled on a DHCP snooping untrusted Layer 2 port. Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN Access Control List (PACL) is installed on the port. This process restricts the client IP traffic to those source IP addresses configured in the binding. any IP traffic with a source IP address other than that in the IP source

binding will be filtered out. This filtering limits a hosts ability to attack the network by claiming neighbor hosts IP address. 