解决IP地址冲突的方法--DHC OOPING PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022__E8_A7_A3_E5_86_B3IP_E5_9C_c101_284173.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 12.1no service padservice timestamps debug uptimeservice timestamps log uptimeno service password-encryptionservice compress-config!hostname C4-2_4506!enable password xxxxxxx!clock timezone GMT 8ip subnet-zerono ip domain-lookup!ip dhcp snooping vlan 180-181 // 对哪些VLAN 进行限制ip dhcp snoopingip arp inspection vlan 180-181ip arp inspection validate src-mac dst-mac iperrdisable recovery cause udlderrdisable recovery cause bpduguarderrdisable recovery cause security-violationerrdisable recovery cause channel-misconfigerrdisable recovery cause pagp-flaperrdisable recovery cause dtp-flaperrdisable recovery cause link-flaperrdisable recovery cause l2ptguarderrdisable recovery cause psecure-violationerrdisable recovery cause gbic-invaliderrdisable recovery cause dhcp-rate-limiterrdisable recovery cause unicast-flooderrdisable recovery cause vmpserrdisable recovery cause arp-inspectionerrdisable recovery interval 30spanning-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 100arp timeout 2ip dhcp snooping limit rate 100!interface

GigabitEthernet2/2ip arp inspection limit rate 100arp timeout 2ip dhcp snooping limit rate 100!interface GigabitEthernet2/3ip arp inspection limit rate 100arp timeout 2ip dhcp snooping limit rate 100!interface GigabitEthernet2/4ip arp inspection limit rate 100arp timeout 2ip dhcp snooping limit rate 100--More-- 编者注：对不需要明确地址的所有人的时候是一个很好的解决办法。另外，可以查看www.cisco.com的IP Source GuardSimilar 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. 