CISCODHCPSnooping技术思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_CISCODHCPS_c101_644331.htm 1.介绍 DHCP Snooping技术是DHCP安全特性，通过建立和维护DHCP Snooping绑定表过滤不可信任的DHCP信息，这些信息是指来自不信任区域的DHCP信息。DHCP Snooping绑定表包含不信任区域的用户MAC地址、IP地址、租用期、VLAN-ID 接口等信息. 当交换机开启了DHCP-Snooping后，会对DHCP报文进行侦听，并可以从接收到的DHCP Request或DHCP Ack报文中提取并记录IP地址和MAC地址信息。另外，DHCP-Snooping允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发DHCP Offer报文，而不信任端口会将接收到的DHCP Offer报文丢弃。这样，可以完成交换机对假冒DHCP Server的屏蔽作用，确保客户端从合法的DHCP Server获取IP地址。 作用：1 1.dhcp-snooping的主要作用就是隔绝非法的dhcp server，通过配置非信任端口。 2.建立和维护一张dhcp-snooping的绑定表,这张表一是通过dhcp ack包中的ip和mac地址生成的,二是可以手工指定。这张表是后续DAI（dynamic arp inspect）和IP Source Guard 基础。这两种类似的技术，是通过这张表来判定ip或者mac地址是否合法，来限制用户连接到网络的.来源：www.examda.com 2.配置 switch（config）#ip dhcp snooping switch（config）#ip dhcp snooping vlan 10 switch（config-if）#ip dhcp snooping limit rate 10 /*dhcp包的转发速率，超过就接口就shutdown，默认不限制 switch（config-if）#ip dhcp snooping trust /*这样这个端口就变成了信任端口，信任端口可以正常

接收并转发DHCP Offer报文，不记录ip和mac地址的绑定，默认是非信任端口" switch#ip dhcp snooping binding 0009.3452.3ea4 vlan 7 192.168.10.5 interface gi1/0/10 /*这样可以静态ip和mac一个绑定. switch（config）#ip dhcp snooping database tftp://10.1.1.1/dhcp_table /*因为掉电后，这张绑定表就消失了，所以要选择一个保存的地方，ftp，tftp，flash皆可。本例中的dhcp_table是文件名，而不是文件夹，同时文件名要手工创建一个。 编辑特别推荐: Cisco交换机DHCPSnooping功能 Cisco认证知识:Switch命令大全 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