Cisco交换机DHCPSnooping功能 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_Cisco_E4_BA_A4_E6_8D_c101_644862.htm 一、采用DHCP服务的常见问题 架设DHCP服务器可以为客户端自动分配IP地址、掩码、默认网关、DNS服务器等网络参数，简化了 网络配置，提高了管理效率。但在DHCP服务的管理上存在一些问题，常见的有：●DHCP Server的冒充 ●DHCP Server的DOS攻击，如DHCP耗竭攻击 ●某些用户随便指定IP地址，造成IP地址冲突 1、DHCP Server的冒充 由于DHCP服务器和客户端之间没有认证机制，所以如果在网络上随意添加一台DHCP服务器，它就可以为客户端分配IP地址以及其他网络参数。只要让该DHCP服务器分配错误的IP地址和其他网络参数，那就会对网络造成非常大的危害。 2、DHCP Server的拒绝服务攻击 通常DHCP服务器通过检查客户端发送的DHCP请求报文中的CHADDR（也就是Client MAC address）字段来判断客户端的MAC地址。正常情况下该CHADDR字段和发送请求报文的客户端真实的MAC地址是相同的。攻击者可以利用伪造MAC的方式发送DHCP请求，但这种攻击可以使用Cisco 交换机 的端口安全特性来防止。端口安全特性（PortSecurity）可以限制每个端口只使用唯一的MAC地址。但是如果攻击者不修改DHCP请求报文的源 MAC地址，而是修改DHCP报文中的CHADDR字段来实施攻击，那端口安全就不起作用了。由于DHCP服务器认为不同的CHADDR值表示请求来自不同的客户端，所以攻击者可以通过大量发送伪造CHADDR的DHCP请求，导致DHCP服务器上的地址池被耗尽，从而无

法为其他正常用户提供网络地址，这是一种DHCP耗竭攻击。DHCP耗竭攻击可以是纯粹的DOS攻击，也可以与伪造的DHCP服务器配合使用。当正常的DHCP服务器瘫痪时，攻击者就可以建立伪造的DHCP服务器来为局域网中的客户端提供地址，使它们将信息转发给准备截取的恶意计算机。甚至即使DHCP请求报文的源MAC地址和 CHADDR字段都是正确的，但由于DHCP请求报文是广播报文，如果大量发送的话也会耗尽网络带宽，形成另一种拒绝服务攻击。 3、客户端随意指定IP地址 客户端并非一定要使用DHCP服务，它可以通过静态指定的方式来设置IP地址。如果随便指定的话，将会大大提高网络IP地址冲突的可能性。 二、DHCP Snooping技术介绍 DHCP监听（DHCP Snooping）是一种DHCP安全特性。Cisco交换机支持在每个VLAN基础上启用DHCP监听特性。通过这种特性，交换机能够拦截第二层VLAN域内的所有DHCP报文。 DHCP监听将交换机端口划分为两类： ●非信任端口：通常为连接终端设备的端口，如PC，网络打印机等 ●信任端口：连接合法DHCP服务器的端口或者连接汇聚交换机的上行端口 通过开启DHCP监听特性，交换机限制用户端口（非信任端口）只能够发送DHCP请求，丢弃来自用户端口的所有其它DHCP报文，例如DHCPOffer 报文等。而且，并非所有来自用户端口的DHCP请求都被允许通过，交换机还会比较DHCP请求报文的（报文头里的）源MAC地址和（报文内容里的）DHCP客户机的硬件地址（即CHADDR字段），只有这两者相同的请求报文才会被转发，否则将被丢弃。这样就防止了DHCP耗竭攻击。信任端口可以接收所有的DHCP报文。通过只将交换机连

接到合法DHCP服务器的端口设置为信任端口，其他端口设置为非信任端口，就可以防止用户伪造DHCP服务器来攻击网络。DHCP监听特性还可以对端口的DHCP报文进行限速。通过在每个非信任端口下进行限速，将可以阻止合法DHCP请求报文的广播攻击。DHCP 监听还有一个非常重要的作用就是建立一张DHCP监听绑定表（DHCP SnoopingBinding）。一旦一个连接在非信任端口的客户端获得一个合法的DHCPOffer，交换机就会自动在DHCP监听绑定表里添加一个绑定条目，内容包括了该非信任端口的客户端IP地址、MAC地址、端口号、VLAN编号、租期等信息。如：
Switch#show ip dhcp snooping binding MacAddress IpAddress Lease(sec) Type VLAN Interface ------------------ --------------- ---------- ------------- ---- -------------- 00:0F:1F:C5:10:08 192.168.10.131 682463 dhcp-snooping 10 FastEthernet0/1 这张DHCP监听绑定表为进一步部署IP源防护（IPSG）和动态ARP检测（DAI）提供了依据。说明： I.非信任端口只允许客户端的DHCP请求报文通过，这里只是相对于DHCP报文来说的。其他非DHCP报文还是可以正常转发的。这就表示客户端可以以静态指定IP地址的方式通过非信任端口接入网络。由于静态客户端不会发送DHCP报文，所以DHCP监听绑定表里也不会有该静态客户端的记录。信任端口的客户端信息不会被记录到DHCP监听绑定表里。如果有一客户端连接到了一个信任端口，即使它是通过正常的DHCP方式获得IP地址，DHCP监听绑定表里也不有该客户端的记录。如果要求客户端只能以动态获得IP的方式接入网络，则必须借助于IPSG和DAI技术。 II.交换机为了获得高速转发，通常只检查报文

的二层帧头，获得目标MAC地址后直接转发，不会去检查报文的内容。而DHCP监听本质上就是开启交换机对DHCP报文的内容部分的检查，DHCP报文不再只是被检查帧头了。 III. DHCP监听绑定表不仅用于防御DHCP攻击，还为后续的IPSG和DAI技术提供动态数据库支持。 IV.DHCP监听绑定表里的Lease列就是每个客户端对应的DHCP租约时间。当客户端离开网络后，该条目并不会立即消失。当客户端再次接入网络，重新发起DHCP请求以后，相应的条目内容就会被更新。如上面的00F.1FC5.1008这个客户端原本插在Fa0/1端口，现在插在Fa0/3端口，相应的记录在它再次发送DHCP请求并获得地址后会更新为： Switch#show ip dhcp snooping binding or Switch#show ip source binding MacAddress IpAddress Lease(sec) Type VLAN Interface ----------------- ------------- ---------- ------------- ---- --------------- 00:0F:1F:C5:10:08 192.168.10.131 691023 dhcp-snooping 10 FastEthernet0/3 V.当交换机收到一个DHCPDECLINE或DHCPRELEASE广播报文，并且报文头的源MAC地址存在于DHCP监听绑定表的一个条目中。但是报文的实际接收端口与绑定表条目中的端口字段不一致时，该报文将被丢弃。 ●DHCPRELEASE报文：此报文是客户端主动释放IP 地址（如Windows 客户端使用ipconfig/release），当DHCP服务器收到此报文后就可以收回IP地址，分配给其他的客户端了 ●DHCPDECLINE报文：当客户端发现DHCP服务器分配给它的IP地址无法使用（如IP地址发生冲突）时，将发出此报文让DHCP服务器禁止使用这次分配的IP地址。 VI. DHCP监听绑定表中的条目可以手工添加。 VII. DHCP监听绑定表在设备重启后会丢失，需要重新绑定，但可以通过

设置将绑定表保存在flash或者tftp/ftp服务器上，待设备重启后直接读取，而不需要客户端再次进行绑定 VIII. 当前主流的Cisco交换机基本都支持DHCP Snooping功能。 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