开启Cisco交换机IPSourceGuard功能Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022__E5_BC_80_E5_90_AFCisc_c101_557841.htm 一、IP地址盗用 IP地址的盗用方法多种多样，其常用方法主要有以下几种： 1、静态修改IP地址 对于任何一个TCP/IP实现来说，IP地址都是其用户配置的必选项。如果用户在配置TCP/IP或修改TCP/IP配置时，使用的不是授权分配的IP地址，就形成了IP地址盗用。由于IP地址是一个逻辑地址，因此无法限制用户对于其主机IP地址的静态修改。 2、成对修改IP-MAC地址 对于静态修改IP地址的问题，现在很多单位都采用IP与MAC绑定技术加以解决。针对绑定技术，IP盗用技术又有了新的发展，即成对修改IP-MAC地址。现在的一些兼容网卡，其MAC地址可以使用网卡配置程序进行修改。如果将一台计算机的 IP地址和MAC地址都改为另外一台合法主机的IP地址和MAC地址，其同样可以接入网络。 另外，对于那些MAC地址不能直接修改的网卡来说，用户还可以采用软件的办法来修改MAC地址，即通过修改底层网络软件达到欺骗上层网络软件的目的。 3、动态修改IP地址 某些攻击程序在网络上收发数据包，可以绕过上层网络软件，动态修改自己的 IP地址（或IP-MAC地址对），以达到IP欺骗。 二、IP Source Guard技术介绍 IP源防护（IP Source Guard，简称IPSG）是一种基于IP/MAC的端口流量过滤技术，它可以防止局域网内的IP地址欺骗攻击。IPSG能够确保第2层网络中终端设备的 IP地址不会被劫持，而且还能确保非授权设备不能通过自己指定IP地址的方式来访问网络或攻击网络导致网络崩溃及瘫痪。 交换机内部有一个IP源绑定

表（IP Source Binding Table）作为每个端口接受到的数据包的检测标准，只有在两种情况下，交换机会转发数据：所接收到的IP包满足IP源绑定表中Port/IP/MAC的对应关系 所接收到的是DHCP数据包 其余数据包将被交换机做丢弃处理。 IP源绑定表可以由用户在交换机上静态添加，或者由交换机从DHCP监听绑定表（DHCP Snooping Binding Table）自动学习获得。 静态配置是一种简单而固定的方式，但灵活性很差，因此Cisco建议用户最好结合DHCP Snooping技术使用IP Source Guard，由DHCP监听绑定表生成IP源绑定表。
以DHCP Snooping技术为前提讲一下IP Source Guard技术的原理。 在这种环境下，连接在交换机上的所有PC都配置为动态获取IP地址，PC作为DHCP客户端通过广播发送DHCP请求，DHCP服务器将含有IP地址信息的DHCP回复通过单播的方式发送给DHCP客户端，交换机从DHCP报文中提取关键信息（包括IP地址，MAC地址，vlan号，端口号，租期等），并把这些信息保存到 DHCP 监听绑定表中。（以上这个过程是由DHCP Snooping完成的） 接下来的由IP Source Guard完成。
交换机根据DHCP监听绑定表的内容自动生成IP源绑定表，然后IOS根据IP源绑定表里面的内容自动在接口加载基于端口的VLAN ACL（PVACL），由该ACL（可以称之为源IP地址过滤器）来过滤所有IP流量。客户端发送的IP数据包中，只有其源IP地址满足源IP绑定表才会被发送，对于具有源IP绑定表之外的其他源IP地址的流量，都将被过滤。 PC没有发送DHCP请求时，其连接的交换机端口默认拒绝除了DHCP请求之外的所有数据包，因此PC使用静态IP是无法连接网络的（除非已经存在绑定好的源IP绑定条目，如静态源IP绑定条

目或者是之前已经生成的动态IP绑定条目还没过期，而且PC还必须插在正确的端口并设置正确的静态IP地址）。 IP源防护只支持第2层端口，其中包括接入（access）端口和干道（trunk）接口。IP源防护的信任端口/非信任端口也就是DHCP监听的信任端口/非信任端口。对于非信任端口存在以下两种级别的IP流量安全过滤： 源IP地址过滤：根据源IP地址对IP流量进行过滤，只有当源IP地址与IP源绑定条目匹配，IP流量才允许通过。当端口创建、 修改、删除新的IP源绑定条目的时候，IP源地址过滤器将发生变化。为了能够反映IP源绑定的变更，端口PACL将被重新修改并重新应用到端口上。默认情况下，如果端口在没有存在IP源绑定条目的情况下启用了IP源防护功能，默认的PACL将拒绝端口的所有流量（实际上是除 DHCP报文以外的所有IP流量）。 源IP和源MAC地址过滤：根据源IP地址和源MAC地址对IP流量进行过滤，只有当源IP地址和源MAC地址都与IP源绑定条目匹配，IP流量才允许通过。当以IP和MAC地址作为过滤的时候，为了确保DHCP协议能够正常的工作，还必须启用DHCP监听选项82。 对于没有选项82的数据，交换机不能确定用于转发DHCP服务器响应的客户端主机端口。相反地，DHCP服务器响应将被丢弃，客户机也不能获得IP地址。 注：交换机使用端口安全（Port Security）来过滤源MAC地址。 当交换机只使用“ IP源地址过滤 ”时，IP源防护功能与端口安全功能是相互独立的关系。端口安全是否开启对于IP源防护功能来说不是必须的。如果同时开启，则两者也只是一种宽松的合作关系，IP源防护防止IP地址欺骗，端口安全防止MAC地址欺骗。而当交换机使用“ 源IP和源MAC地址过滤 ”时，IP源防

护功能与端口安全功能是就变成了一种“集成”关系，更确切的说是端口安全功能被集成到IP源防护功能里，作为IP源防护的一个必须的组成部分。 在这种模式下，端口安全的违规处理（violation）功能将被关闭。对于非法的二层报文，都将只是被简单的丢弃，而不会再执行端口安全的违规处理了。 IP源防护功能不能防止客户端PC的ARP攻击。ARP攻击问题必须由DAI功能来解决。如果要支持IP源防护功能，必须是35系列及以上的交换机。 2960目前不支持该功能。 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