如何进行IP和MAC地址绑定，以防范ARP欺骗

ARP　樊凡　2019-10-30 发表

问题描述

如何进行IP和MAC地址绑定，以防范ARP欺骗

解决方法

1. 如何进行IP和MAC地址绑定，以防范ARP欺骗?

用路由器做地址转换，上网频繁掉线，此时将PC机的网卡禁用一下或将PC机重启一下又可以上网了，并且不能上网时ping PC机的网关不通。这种情况一般来说,都是中了ARP欺骗病毒，可以通过以下方法进行防范。

方法一：在路由器上静态绑定PC机的IP地址和MAC地址，在PC机上绑定路由器内网口的IP地址和MAC地址。

步骤如下：

(1) 在路由器上绑定PC机的IP地址和MAC地址，格式如下：

[H3C]arp static 192.168.1.2 00e1-7778-9876

注意：需要对该网段内的每一个IP都绑定MAC，没有使用的IP地址也需要绑定，可以任意指定其绑定的MAC地址，推荐使用0000-0000-0123等特殊MAC。

(2) 在PC机上绑定路由器内网口的IP地址和MAC地址，命令格式如下：

arp –s 192.168.1.1 00-0f-e2-21-a0-01

方法二：让路由器定时发送免费ARP报文，刷新PC机的ARP表项

进入路由器相应的内网接口，配置如下命令：

[H3C-Ethernet1/0]arp send-gratuitous-arp 1

方法三：ARP固化

可以在全局视图和接口视图下配置ARP固化功能，使动态ARP转化为固定ARP，有效防范ARP攻击。

固化ARP有三种方式：

(1) 全局视图下配置动态ARP固化

[H3C] arp fixup

(2) 接口视图下配置动态ARP固化

[H3C] interface ethernet 1/0/0

[H3C-Ethernet1/0/0] arp fixup

(3) 配置指定固化ARP表项的功能

[H3C] arp fixed 10.1.0.1 00-11-22

【提示】

1) PC机重启后，静态配置的arp表项会丢失，需要重新配置，可以在PC机上制作一个.bat的批处理文件，放到启动项中。

2) arp send-gratuitous-arp 并非所有产品均支持，请查询网站上的配置手册和命令手册，确认您所使用的产品是否支持该功能。

3) ARP固化并非所有产品均支持，请确认您所使用的产品是否支持该功能。

方法四：授权arp方式（要求局域网中的PC动态获取IP）

启动DHCP服务。

[H3C] dhcp enable

#配置DHCP地址池

[H3C] dhcp server ip-pool 0

[H3C-dhcp-pool-0] network 192.168.1.0 mask 255.255.255.0

[H3C-dhcp-pool-0]gateway-list 192.168.1.1

针对DHCP全局地址池使能授权ARP。

[H3C-dhcp-pool-0] synchronize arp

[H3C-dhcp-pool-0] quit

禁止动态ARP学习，配置授权ARP表项的老化时间为120秒。

[H3C] interface ethernet 1/0/0 /*内网接口*/

[H3C-Ethernet1/0/0]ip add 192.168.1.1 24

[H3C-Ethernet1/0/0] arp security

[H3C-Ethernet1/0/0] arp security time-out 120

[H3C-Ethernet1/0/0] quit

方法五：IPS方式

打开IPS功能

[H3C] ips enable

创建并配置IPS检测策略

[H3C] ips policy 1

[H3C-ips-policy-1] defend-attack arp-reverse-query

在存在arp攻击的接口上应用攻击检测策略

[H3C] interface ethernet 1/0/0
[H3C-Ethernet1/0/0] ips policy 1 inbound

2. 什么是自然网段ARP，如何理解?

自然网段的ARP的命令是在系统视图下执行naturemask-arp enable（默认是不使能的）；在学习ARP表项时，若发现ARP报文的源IP地址和入接口IP地址不在同一网段后，则使用自然网段进行判断。

假设Vlan-interface1000接口的IP地址为3.3.3.2/24，收到一个源IP地址为3.4.4.3的ARP报文，由于两个IP地址不在同一网段，Vlan-interface1000接口无法处理这个报文。如果使能支持自然网段的ARP请求功能，则通过自然网段进行判断，由于Vlan-interface1000接口的IP地址为A类地址，因此默认掩码应该为8位，于是两个IP地址就在同一个网段，Vlan-interface1000接口就可以学习源IP地址为3.4.4.3的ARP表项了。

3. 什么是免费ARP，如何理解?

免费ARP报文是一种特殊的ARP报文，该报文中携带的发送者IP地址和目标IP地址都是本机IP地址，发送者MAC地址是本机MAC地址，目标MAC地址是广播地址。

(1) 设备通过对外发送免费ARP报文，实现以下功能：

l 确定其它设备的IP地址是否与本机IP地址冲突。

l 设备改变了接口MAC 地址，通过发送免费ARP报文通知其他设备更新ARP表项。

l 命令行打开gratuitous-arp-sending enable（默认此功能关闭）后，设备收到非同一网段的ARP请求时发送免费ARP。

(2) 设备通过学习免费ARP报文，命令行为gratuitous-arp-learning enable（默认此功能打开），实现以下功能：对于收到的免费ARP 报文，如果ARP 表中没有与此报文对应的ARP表项，就将免费ARP报文中携带的信息添加到本地动态ARP映射表中。

4. 什么是ARP 源抑制，如何理解?

如果网络中有主机通过向设备发送大量目标IP地址不能解析的IP报文来攻击设备，则会造成下面的危害：

(1) 设备向目的网段产生大量ARP请求报文，加重设备的负载。

(2) 设备会不断解析目标IP地址，增加了CPU 的负担。

为避免这种大量目标IP不能解析的IP报文攻击所带来的危害，设备提供了ARP源抑制功能，命令行为arp source-suppression enable（默认此功能关闭），当开启该功能后，如果网络中某主机向设备某端口连续发送目标IP地址不能解析的IP报文，当每5秒内对该目的IP 解析的ARP 的流量超过设置的阈值，系统就会丢弃由此端口进入的与发送者IP 地址相同的报文，直至5秒后再处理，从而避免了恶意攻击所造成的危害。

5. 什么是ARP 黑洞路由，如何理解?

所谓ARP黑洞路由，是设备防IP报文攻击一种功能；在进行IP报文转发过程中，设备需要依靠ARP解析下一跳IP地址的MAC地址。如果地址解析成功，报文可以直接通过硬件转发芯片直接转发出去，而不需要再由软件处理；如果地址解析不成功，需要由软件进行解析处理。这样，如果接收到大量下一跳IP地址循环变化并且该IP地址不可达的IP报文，由于下一跳IP地址解析不成功，平台会一直发ARP请求报文试图解析不可达的目的IP，大量的ARP请求导致CPU负荷过重，就造成了IP报文对设备的攻击。

可以通过配置ARP黑洞路由，即防IP报文攻击功能来预防这种可能存在的攻击情况，命令行为arp resolving-route enable，在防IP报文攻击功能启用后，一旦接收到下一跳地址不可达的IP 报文（即ARP解析失败的IP报文），设备立即产生一个黑洞路由，黑洞路由表项可以在隐藏模式下通过命令_display arp dummy进行查看，使硬件转发芯片在一段时间内将去往该地址的报文直接丢弃。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则由硬件进行转发，否则仍然下发黑洞路由。这种方式能够有效的防止IP报文的攻击，减轻CPU的负担。

6. 什么是代理ARP，如何理解?

如果ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理ARP功能的设备就可以回答该请求，这个过程称作代理ARP（Proxy ARP）。

代理ARP分为代理ARP和本地代理ARP。

同一网段内连接到设备的不同接口的主机可以利用设备的代理ARP 功能，命令行为proxy-arp enable（默认此功能关闭），从而通过三层转发实现互通。

为了实现三层互通，在下面三种情况之一需要开启本地代理ARP 功能，命令行为local-proxy-arp enable（默认此功能关闭），

(1) 连接到同一个VLAN 不同二层隔离的端口下的设备要实现三层互通；

(2) 使能Super VLAN 功能后，属于不同Sub VLAN 下的设备要实现三层互通；

(3) 使能Isolate-user-vlan 功能后，属于不同Second VLAN 下的设备要实现三层互通。

7. ARP 的老化时间是如何处理的?

ARP老化时间的主要作用是：防止arp表项在没有使用的情况下一直占用资源。设置老化时间是为了方便用户灵活配置，当系统学习到一个动态ARP表项时，它的老化时间点以当前配置的老化时间计算，然后进行最后一分钟老化。

老化时间配置为30分钟（arp timer aging 30），当表项的老化时间变成18分钟的时候，再配置一遍老化时间为30分钟，为什么表项中的老化时间还是18分钟；而配置老化时间为其它值（如：配置为100分钟的时候），表项中的老化时间才会进行相应的变化?

当配置值没有发生变化时，老化时间不需要处理，所以老化时间仍然按照原值进行老化，当新配置与原配置不一致时，才会对老化时间进行处理；如果新配置的老化时间大于原配置的老化时间，则用新

配置的老话时间减去已经老化掉的时间就为应该显示的老化时间；如果新配置的老化时间小于原配置的老化时间，则用新配置的老话时间减去已经老化掉的时间就为应该显示的老化时间，但是最低老化时间不小于1分钟。

ARP表项老化到最后一分钟老化时间后，发送该表项的ARP请求，如果收到应答则按照新配置的老化时间重新开始老化，如果没有收到ARP应答，则一分钟后删除该表项。

例如：原来的老化时间配置为30分钟，显示的老化时间为12分钟，这时候配置老化时间为100分钟，则设备显示的老化时间应为：100分钟-（30分钟-12分钟）=82分钟；如果新配置老化时间为18分钟，则设备显示的老化时间应为：18分钟-（30分钟-12分钟）=0分钟，但是老化时间不小于1分钟，所以显示的老化时间为1分钟。

8. ARP 表项中VLAN ID、Interface、Aging 关键字为N/A 时的含义

ARP表项中VLAN ID、Interface、Aging字段为N/A的含义：

[H3C]display arp all

Type: S-Static D-Dynamic

IP Address MAC Address VLAN ID Interface Aging Type

2.2.2.2 0002-0002-0002 N/A N/A N/A S

[H3C]

为什么在ARP表项中VLAN ID、Interface、Aging字段为N/A？Type字段中S和D又个表示什么意思？

ARP表项主要有动态和静态之分，设备动态学习到的表项在Type（类型）字段用D表示，为Dynamic的简写，即动态的意思；当手工配置静态的表项在Type字段用S表示，为Static的简写，即静态的意思；而静态表项又分为短静态和长静态，短静态表项是不指定VLAN ID和Interface（出接口）的，这样生成的表项相应的字段就用N/A表示，表示“无”的意思，要注意短静态ARP表项不能直接用于报文转发，当要发送IP数据包时，先发送ARP请求报文，如果收到的响应报文中的源IP地址和源MAC地址与所配置的IP地址和MAC地址相同，则将接收ARP响应报文的接口加入该静态ARP表项中，之后就可以用于IP数据包的转发；若是长静态则需要指定VLAN ID和Interface（出接口）的，长静态ARP表项可以直接转发数据；对于静态ARP表项的Aging字段的值统一使用N/A表示，意思为：不老化。

9. 配置接口允许学习动态ARP表项的最大个数小于现有表项数时，如何处理？

在每个接口上学习到了一定数量的ARP表项，如2000条：

< H3C>display arp all count

Total entry(ies): 2000

现在把接口上的最大学习数配置为1000条：

[H3C-Vlan-interface1000]arp max-learning-num 1000

为什么现有的ARP表项还是2000条？而不是1000条？

< H3C>display arp all count

Total entry(ies): 2000

命令arp max-learning-num number的配置对当前的ARP表项数量不会产生影响，只只对后续的ARP学习有影响，即原有的ARP表项老化以后，则再学习时，则最多只能学到1000条。