HCIE-Security 备考指南

ARP 安全配置(S5700 交换机)

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security ARP 安全配置(S5700 交换机)需要掌握的知识点

- 掌握 DHCP Snooping 原理及配置

ARP 安全概述

ARP 攻击是网络中最常见同时影响比较大的攻击方式，作为交换机的 S5700 在离攻击源最近的位置，从设备级安全的角度提供 ARP 的防攻击方法。

在现今的网络中，Ethernet 是最常用的接入手段，而 ARP 协议作为 Ethernet 网络上的开放协议，由于本身过于简单和开放，没有任何的安全手段，为恶意用户的攻击提供了可能。

ARP 攻击类型

ARP 的攻击方式多种多样。

- 按照攻击对象可以分为针对主机的攻击和针对设备的攻击。
- 按照攻击触发源可以分为来自病毒的攻击或者来自非法软件的人为攻击。
- 按照攻击影响可以分为：
  - 地址欺骗型的攻击

    地址欺骗攻击主要包括：

    - 用错误的主机 MAC 地址刷新网关的 ARP 缓存，导致主机无法上线。
    - 向主机发送错误的 ARP 应答，使主机得到错误的网关地址，导致主机无法上线。
  - DOS（Denial of Service）攻击
    - 从空间方面，攻击主要利用设备 ARP 缓存的有限性，通过发送大量伪造的 ARP 请求、应答报文，造成设备的 ARP 缓存溢出，从而无法缓存正常的 ARP 表项，进而阻碍正常转发。
    - 从时间方面，攻击主要利用设备计算能力的有限性，通过发送大量伪造的 ARP 请求、应答报文或其他能够触发设备 ARP 处理的报文（比如攻击者利用工具扫描本网段主机或者跨网段进行扫描时，设备在发送回应报文前，会查找 ARP 表项，如果目的 IP 地址对应的 MAC 地址不存在，会导致设备的 ARP 模块向上层软件发送 ARP Miss 消息，要求上层软件发送 ARP 请求报文

以获得目的端的 MAC 地址，大量的扫描报文会导致大量的 ARP Miss 消息。），造成设备的计算资源长期忙于 ARP 报文处理，影响其他业务的处理，进而阻碍正常转发。

欺骗攻击的防范措施往往只能针对非法用户，仿造合法用户报文造成的大量的 DOS 攻击是当前影响比较大的攻击方式。

ARP 攻击影响

如果是主机遭受 ARP 攻击，该主机无法上线，网关信息被篡改或者被窃取。

如果接入交换机遭受 ARP 攻击，可能导致局域网内多用户甚至大量用户无法上线。

如果路由器遭受 ARP 攻击，由于路由器一般下接多个交换机，结果是更多的用户无法上线。

ARP 防攻击策略

从造成的影响看，防攻击越靠近攻击源进行防范，代价越小，效果越佳。

- 对于主机的防攻击，由于造成的影响比较小，可以通过在主机上安装守护程序的方法来解决，如果守护程序发现网关 MAC 地址被欺骗就清除本机 ARP 缓存，并重发 ARP 请求。
- 对于路由器的防攻击，目前双向绑定、主动防御等大部分的 ARP 防攻击的技术都可以在路由器上实施 ARP 防攻击。但是由于路由器是整个局域网的出口，而 ARP 攻击是以整个局域网为目标，当 ARP 攻击包已经达到路由器的时候，影响已经造成。所以由路由器来承担防御 ARP 攻击的任务并不能很好的解决问题。
- 对于交换机的防攻击，由于任何 ARP 包，都必须经由交换机转发，才能达到被攻击目标，只要交换机不接受非法的 ARP 报文，非法报文的攻击就不可能产生。

双向绑定等防 ARP 攻击方法可以防范非法用户的上线，属于防欺骗攻击的范畴，相关的措施一般在攻击发生前进行，但是伪造合法用户的 DOS 攻击往往会造成大量用户下线，影响范围更大。而且在攻击发生后才能发现，所以在大部分的网络中会默认使能限速或者 CAR 等用于预防此类攻击的产生。如果攻击仍然产生，根据具体的情况，可以通过网络监控等方式发现后通过指定目标限速、隔离等方法来解决。

作为交换机的 S5700 可以起到良好的 ARP 防攻击的作用。

S5700 的 ARP 防攻击定位

层次化网络安全分为业务级安全、网络级安全和设备级安全。业务级安全依赖于业务本身的安全机制、无阻塞可靠网络的建设；网络级的安全依赖于网络流量区分隔离，配合客户终端和安全控制服务器，精细监控；设备级安全依赖于基本的设备高可靠性。在 ARP 防攻击领域，S5700 聚焦于设备级的网络安全。

S5700 支持的 ARP 安全特性

S5700 支持的 ARP 安全特性包括 ARP 报文速率抑制、ARP 报文源抑制、ARP Miss 消息速率抑制、ARP Miss 消息源抑制等防 ARP 泛洪攻击的功能，以及防止 ARP 地址欺骗、防止 ARP 中间人攻击、防止 ARP 网关冲突等防 ARP 欺骗攻击的功能。。

防 ARP 泛洪和欺骗攻击功能

为了避免 ARP 攻击行为造成的各种危害，ARP 安全特性针对泛洪和欺骗攻击提供了多种解决方案，具体如表 1 所示：

表 1 ARP 安全针对泛洪和欺骗攻击的解决方案

攻击类型	防攻击功能	功能说明	部署设备
ARP 泛洪	ARP 报文速率抑制	通过 ARP 报文速率抑制功能，可以防止设备因处理大量 ARP 报文，导致 CPU 负荷过重而无法处理其他业务。	建议在网关设备上部署本功能 **说明：** 当接入设备上部署了 MFF 功能时，为了避免 MFF 模块处理过多的过路 ARP 报文（即 ARP 报文的目的 IP 地址不是该报文接收接口的 IP 地址）导致 CPU 负荷过重，则可以在接入设备上部署针对全局、VLAN 和接口的 ARP 报文速率抑制功能。
	ARP 报文源抑制	配置 ARP 报文源抑制功能后，可以使设备在一段时间内，如果收到某一源 IP 地址或者源 MAC 的 ARP 报文数目超过设定阈值，则不处理超出阈值部分的 ARP 请求报文，防止设备处理某个源 IP 地址、MAC 地址发送的大量 ARP 报文，造成设备 CPU 资源的浪费。	建议在网关设备上部署本功能
	ARP Miss 消息速率抑制	通过 ARP Miss 消息速率抑制功能，可以防止设备因收到大量目的 IP 不能解析的 IP 报文，触发大量 ARP Miss 消息，导	建议在网关设备上部署本功能

表 1 ARP 安全针对泛洪和欺骗攻击的解决方案

攻击类型	防攻击功能	功能说明	部署设备
		致 CPU 负荷过重而无法处理其他业务。	
	ARP Miss 消息源抑制	配置 ARP Miss 消息源抑制功能后，如果一个源 IP 地址在一定时间内不断触发 ARP Miss 消息，而且其触发速率超过了设定的阈值，设备则认为此 IP 地址在进行攻击。对于前 16 个攻击源，设备将下发 ACL 规则，在后续的一段时间内把这个地址发出的 IP 报文丢弃；对于之后的攻击源，设备使用设定的阈值对 IP 报文进行抑制。这可以防止设备因收到某个源 IP 发送的大量目的 IP 不能解析的 IP 报文，触发大量 ARP Miss 消息，导致 CPU 负荷过重而无法处理其他业务。	建议在网关设备上部署本功能
	ARP 表项严格学习	使能 ARP 表项严格学习功能后，只有本设备主动发送的 ARP 请求报文的应答报文才能触发本设备学习 ARP，其他设备主动向本设备发送的 ARP 报文不能触发本设备学习 ARP。这可以防止设备收到大量 ARP 攻击报文时，ARP 表被无效的 ARP 条目占满。	建议在网关设备上部署本功能
	ARP 表项限制	使能 ARP 表项限制功能后，设备接口只能学习到设定的最大动态 ARP 表项数目。这可以防止当一个接口所接入的某一台用户主机发起 ARP 攻击时整个设备的 ARP 表资源都被耗尽。	建议在网关设备上部署本功能
ARP 欺骗	防止 ARP 地址欺骗	配置防止 ARP 地址欺骗后，设备在第一次学习到 ARP 之后，不再允许用户更新此 ARP 表项或只能更新此 ARP 表项的部分信息，或者通过发送 ARP 请求报文的方式进行确认，以防止攻击者伪造 ARP 报文修改正常用户的 ARP 表项内容。 设备提供三种模式防御 ARP 地址欺骗攻击：fixed-all 模式、fixed-mac 模式和 send-ack 模式。	建议在网关设备上部署本功能
	防止 ARP 中间人攻击	配置防止 ARP 中间人攻击功能后，当设备收到 ARP 报文时，将此 ARP 报文的源 IP、源 MAC、收到 ARP 报文的接口及 VLAN 信息和 DHCP Snooping 绑定表的信息进行比较，如果信息匹配，则认为是合法用户，允许此用户的 ARP 报文通过，	建议在接入设备上部署本功能 **说明：** 当网关设备上部署了 DHCP 触发 ARP 学习功能时，则需要在网关设备上部署本功能。

表 1 ARP 安全针对泛洪和欺骗攻击的解决方案			
攻击类型	**防攻击功能**	**功能说明**	**部署设备**
		否则认为是攻击，丢弃该 ARP 报文。 本功能仅适用于 DHCP Snooping 场景。	
	防止 ARP 网关冲突	配置防止 ARP 网关冲突功能后，可以防止用户仿冒网关发送 ARP 报文，非法修改网络内其他用户的 ARP 表项。	建议在网关设备上部署本功能
	发送免费 ARP 报文	使能发送免费 ARP 报文功能后，设备作为网关，主动向用户发送以自己 IP 地址为目标 IP 地址的 ARP 请求报文，定时更新用户 ARP 表项的网关 MAC 地址，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。	建议在网关设备上部署本功能
	ARP 报文源 MAC 地址检查	配置 ARP 报文源 MAC 地址检查功能后，设备会对源 MAC 地址不合法的报文进行过滤。	建议在网关设备或接入设备上部署本功能
	ARP 表项严格学习	使能 ARP 表项严格学习功能后，只有本设备主动发送的 ARP 请求报文的应答报文才能触发本设备学习 ARP，其他设备主动向本设备发送的 ARP 报文不能触发本设备学习 ARP。这可以防止设备因收到伪造的 ARP 报文，错误地更新 ARP 表项，导致合法用户的通信流量发生中断。	建议在网关设备上部署本功能
	DHCP 触发 ARP 学习	使能 DHCP 触发 ARP 学习功能后，设备根据收到的 DHCP ACK 报文直接生成 ARP 表项。当 DHCP 用户数目很大时，可以避免大规模 ARP 表项的学习和老化对设备性能和网络环境形成的冲击。 此时设备上还可同时配置防止 ARP 中间人攻击功能，防止 DHCP 用户的 ARP 表项被伪造的 ARP 报文恶意修改。	建议在网关设备上部署本功能

配置防 ARP DOS 攻击

大量 ARP 攻击报文会造成 MAC 地址表项溢出或者 CPU 资源占用过高，S5700 可以针对不同的报文类型进行丢弃、限速等操作防范 ARP DOS 攻击。

建立配置任务

建立配置任务主要介绍了防 ARP DOS 攻击的应用场景、前置条件和数据准备，为后期的配置提供整体背景和相关准备。

应用环境

产生 ARP DOS 攻击的报文包括 ARP 请求应答报文、ARP Miss 报文、免费 ARP 报文，表 1 分析了不同报文类型的产生过程、子场景和 S5700 对应的处理措施，提供了不同的解决方法，增强网络抗击 ARP DOS 攻击的能力。

表 1 ARP 防 DoS 攻击的场景和处理方法

报文类型	攻击产生场景	S5700 的处理方法
ARP 请求应答报文	• 攻击者发送大量的 ARP 请求应答报文，造成 S5700 设备 CPU 资源占用过高和 ARP 表项溢出。	整体的思路是抑制此类报文，具体措施包括： • 基于源 MAC 地址、源 IP 地址对 ARP 报文进行限速。 • 在全局、VLAN 下或者接口下进行 ARP 限速。

表 1 ARP 防 DoS 攻击的场景和处理方法		
报文类型	**攻击产生场景**	**S5700 的处理方法**
		• 限制接口能够学习到的最大动态 ARP 表项数目，抑制攻击端口接收的 ARP 请求应答报文更新 ARP 表项。
ARP Miss 报文	攻击者使用大量的找不到目的 MAC 地址扫描 IP 报文攻击 S5700，造成 S5700 产生大量的 ARP Miss 报文，生成 ARP 临时表项。	S5700 针对该类攻击的处理方法包括： • 基于源 MAC 地址、源 IP 地址对 ARP Miss 报文进行限速。 • 基于不同的视图进行 ARP Miss 限速。
免费 ARP 报文	免费 ARP 是用于帮助作为网关的 S5700 及时向 VLAN 内的主机更新 MAC 地址信息，防止对主机网关 MAC 地址的恶意篡改。 但是，如果攻击者伪造大量的免费 ARP 报文可能造成 S5700 设备 CPU 资源占用过高	S5700 针对该类攻击的处理方法是当判断出该类攻击后，配置 S5700 丢弃免费 ARP 报文。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 防 DoS 攻击功能之前，需要准备以下数据。

序号	数据
1	ARP 请求应答报文的源抑制地址、限速值
2	（可选）ARP 报文限速丢弃告警阈值
3	ARP Miss 报文的源抑制地址、限速值
4	（可选）ARP Miss 消息限速丢弃告警阈值

配置 ARP 报文的源 MAC 地址抑制

背景信息

说明：

仅 S5700HI 和 S5710EI 支持基于源 MAC 地址的 ARP 抑制。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp speed-limit source-mac maximum** *maximum*，配置基于源 MAC 地址的 ARP 报文源抑制速率。
3. 执行命令 **arp speed-limit source-mac** [*mac_addr*] **maximum** *maximum*，配置指定 MAC 地址用户的 ARP 报文源抑制速率。

   对指定了 MAC 地址的用户，ARP 报文源抑制速率为步骤 3 中配置的 *maximum* 值；其它 MAC 地址的 ARP 报文源抑制速率为步骤 2 中配置的 *maximum* 值。

   缺省情况下，所有 MAC 地址的 ARP 报文源抑制速率为 0pps，即不对 ARP 报文进行源抑制。

配置 ARP 报文源 IP 地址抑制

背景信息

考虑到某些特定的用户有特别的需求，在对 ARP 报文进行源 IP 地址抑制时，可以针对该用户的 IP 地址配置不同于其他 IP 地址的 ARP 报文抑制速率。

说明：

S5700LI、S5710LI 和 S5700S-LI 不支持基于源 IP 地址的 ARP 抑制。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp speed-limit source-ip maximum** *maximum*，配置 ARP 报文源 IP 地址抑制速率。
3. 执行命令 **arp speed-limit source-ip** *ip-address* **maximum** *maximum*，配置指定 **source-ip** 用户的 ARP 报文源 IP 地址抑制速率。

   对指定了 source-ip 的用户，ARP 报文源 IP 地址抑制速率为步骤 3 中配置的 *maximum* 值；其它 IP 地址的 ARP 报文源抑制速率为步骤 2 中配置的 *maximum* 值。

   缺省情况下，设备对每一个源 IP 地址的 ARP 报文抑制速率为 0，即不进行 ARP 报文源抑制。

配置 ARP Miss 消息源抑制

背景信息

考虑到某些特定的用户有特别的需求，对于该用户的 IP 地址可以配置不同于其他 IP 地址的 ARP Miss 抑制速率。

说明：

S5700LI、S5710LI、S5700S-LI 不支持基于源 IP 地址的 ARP Miss 报文抑制功能。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp-miss speed-limit source-ip maximum** *maximum*，配置 ARP Miss 消息源抑制速率。
3. （可选）执行命令 **arp-miss speed-limit source-ip** [*ip-address* [**mask** *mask*]] **maximum** *maximum* [**none-block** | **block timer** *timer*]，配置指定 **source-ip** 用户的 ARP Miss 源抑制速率。

   完成上述配置后，对指定了 source-ip 的用户，ARP Miss 源抑制速率为步骤 3 中配置的 *maximum* 值；其它 IP 地址的 ARP Miss 源抑制速率为步骤 2 中配置的 *maximum* 值。

   如果将速率配置为 0，则表示不作 ARP Miss 源抑制。缺省情况下，ARP Miss 消息的源抑制功能已经使能，设备最多允许同一个源 IP 地址每秒触发 500 个 ARP Miss 消息。

   如果该端口指定 IP 地址的 ARP Miss 达到速率后 S5700 会下发一条 ACL 丢弃触发 ARP Miss 的 IP 报文，5 秒的老化时间后撤销该 ACL。

配置临时 ARP 表项的老化时间

通过设置临时 ARP 表项的老化超时时间，可以控制 ARP Miss 消息向上层软件发送的频率，从而减小对系统的攻击。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

3. 执行命令 **arp-fake expire-time** *expire-time*，配置临时 ARP 表项的老化时间。

   缺省情况下，临时 ARP 表项的老化时间是 1 秒。

后续处理

临时 ARP 表项的老化时间配置成功后，在老化时间内，相同的 ARP Miss 信息只发送一次。老化时间超时后，临时 ARP 表项被清除，设备转发时如果匹配不到对应的 ARP 表项，重新生成 ARP Miss 消息进行上报，设备再次生成临时 ARP 表项发送给设备。直到设备生成正确的 ARP 表项替换掉临时 ARP 表项。

配置 ARP Miss 消息速率抑制

背景信息

如果全局、VLAN 或接口在一定时间内不断上报 ARP Miss 消息，使得设备由于忙于发送广播 ARP 请求而性能下降。ARP Miss 消息的抑制功能是对上报的 ARP Miss 消息进行统计，并将超过限速值的 ARP Miss 消息丢弃的过程。

说明：

S5700LI、S5700S-LI、S5710LI 不支持 ARP Miss 报文的速率抑制功能。

操作步骤

- 系统视图下配置 ARP Miss 消息速率抑制功能

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp-miss anti-attack rate-limit enable**，全局使能 ARP Miss 消息速率抑制功能。

     缺省情况下，全局未使能 ARP Miss 消息速率抑制功能。

  3. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在系统视图下配置 ARP Miss 消息的限速时间和限速值。

     配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。

4. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，全局使能 ARP Miss 消息限速丢弃告警功能。

   缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。

5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在系统视图下配置 ARP Miss 消息限速丢弃告警阈值。

   缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

- VLAN 视图下配置 ARP Miss 消息速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
3. 执行命令 **arp-miss anti-attack rate-limit enable**，在 VLAN 视图下使能 ARP Miss 消息速率抑制功能。

   缺省情况下，VLAN 视图下未使能 ARP Miss 消息速率抑制功能。

4. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在 VLAN 视图下配置 ARP Miss 消息的限速时间和限速值。

   配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。

5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，在 VLAN 视图下使能 ARP Miss 消息限速丢弃告警功能。

   缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。

6. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在 VLAN 视图下配置 ARP Miss 消息限速丢弃告警阈值。

   缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

- 接口视图下配置 ARP Miss 消息速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

3. 执行命令 **arp-miss anti-attack rate-limit enable**，在接口视图下使能 ARP Miss 消息速率抑制功能。

   缺省情况下，接口视图下未使能 ARP Miss 消息速率抑制功能。

4. 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，在接口视图下配置 ARP Miss 消息的限速时间和限速值。

   配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。

5. （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，在接口视图下使能 ARP Miss 消息限速丢弃告警功能。

   缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。

6. （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，在接口视图下配置 ARP Miss 消息限速丢弃告警阈值。

   缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

配置 ARP 报文速率抑制

背景信息

说明：

S5700LI、S5710LI 和 S5700S-LI 不支持 ARP 报文速率抑制。

操作步骤

- 系统视图下配置 ARP 报文速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp anti-attack rate-limit enable**，全局使能 ARP 报文速率抑制功能。

   缺省情况下，全局未使能 ARP 报文速率抑制功能。

3. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在系统视图下配置 ARP 报文的限速时间和限速值。

配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。

4. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，全局使能 ARP 报文限速丢弃告警功能。

   缺省情况下，未使能 ARP 报文限速丢弃告警功能。

5. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在系统视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

- VLAN 视图下配置 ARP 报文速率抑制功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
3. 执行命令 **arp anti-attack rate-limit enable**，在 VLAN 视图下使能 ARP 报文速率抑制功能。

   缺省情况下，VLAN 视图下未使能 ARP 报文速率抑制功能。

4. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在 VLAN 视图下配置 ARP 报文的限速时间和限速值。

   配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。

5. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，在 VLAN 视图下使能 ARP 报文限速丢弃告警功能。

   缺省情况下，未使能 ARP 报文限速丢弃告警功能。

6. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在 VLAN 视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

- 接口视图下配置 ARP 报文速率抑制功能

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **arp anti-attack rate-limit enable**，在接口视图下使能 ARP 报文速率抑制功能。

   缺省情况下，接口视图下未使能 ARP 报文速率抑制功能。

4. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*] [**block timer** *timer*]，在接口视图下配置 ARP 报文的限速时间、限速值以及丢弃超过 ARP 报文限速值端口下所有 ARP 报文的功能。

   缺省情况下，接口下 ARP 报文的限速时间是 1 秒，在 1 秒内最多允许 100 个 ARP 报文通过，且未配置丢弃超过 ARP 报文限速值端口下所有 ARP 报文的功能。

   说明：

   该命令只对上送 cpu 的 ARP 报文做抑制，对芯片转发的报文不会产生影响。

5. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，在接口视图下使能 ARP 报文限速丢弃告警功能。

   缺省情况下，未使能 ARP 报文限速丢弃告警功能。

6. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在接口视图下配置 ARP 报文限速丢弃告警阈值。

   缺省情况下，ARP 报文限速丢弃告警阈值为 100。

配置基于接口的 ARP 表项限制

背景信息

为了防止攻击者占用大量 ARP 表项资源，造成 S5700 学习不到合法用户的 ARP 表项，可以配置接口能够学习到的最大动态 ARP 表项数目。

操作步骤

- 配置接口的 ARP 表项限制

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

3. 在非 VLANIF 接口下，执行命令 **arp-limit vlan** *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*，在 VLANIF 接口视图下，执行命令 **arp-limit maximum** *maximum* 配置基于接口的 ARP 表项限制。

   当在非 VLANIF 接口下配置时，必须指定 vlan *vlan-id1*。

配置防 ARP 欺骗攻击

ARP 表项攻击、网关攻击、中间人攻击是 ARP 欺骗攻击的主要应用场景，S5700 针对这三个场景可以进行针对性的防攻击。

- **建立配置任务**

  建立配置任务主要介绍了防 ARP 欺骗攻击的应用场景、前置条件和数据准备，为后期的配置提供整体背景和相关准备。

- **配置严格学习 ARP 表项**
- **配置防止 ARP 地址欺骗**
- **配置防止 ARP 网关冲突**
- **配置防止 ARP 中间人攻击**
- **配置 ARP 报文源 MAC 地址检查功能**
- **配置发送 ARP 免费报文**

  通过配置发送免费 ARP 报文，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

- **配置 DHCP 触发 ARP 学习**
- **配置端口隔离后 ARP 报文转发功能**
- **检查配置结果**

建立配置任务

建立配置任务主要介绍了防 ARP 欺骗攻击的应用场景、前置条件和数据准备，为后期的配置提供整体背景和相关准备。

应用环境

如表 1 所示，S5700 针对不同 ARP 欺骗攻击的场景，提供了不同的解决方法，增强网络抗击 ARP 欺骗攻击的能力。

表 1 ARP 防欺骗攻击的场景和处理方法

场景名称	场景产生过程	S5700 的处理方法
ARP 表项自我保护	ARP 欺骗攻击一般都是通过修改 ARP 表项来完成的。	增强 ARP 表项的自我保护功能，S5700 提供了如下的处理方法： • 严格地址学习：S5700 只学习自己发送的 ARP 请求报文的应答报文 • 防地址欺骗：通过固定 ARP 表项的 MAC 地址、接口、VLAN 等信息，或者确认机制，保证 ARP 表项的相对稳定。 • DHCP 触发 ARP 学习：当 DHCP 服务器给用户分配 IP 地址时，S5700 回应用户 DHCP ACK 报文成功后，会取用户的 MAC 地址，生成该 IP 地址对应的 ARP 表项。这样可以省掉 S5700 学习用户主机 ARP 的过程,避免攻击者通过 ARP 报文对 ARP 表项的攻击。
网关冲突	攻击者仿冒网关地址，发送 ARP 报文头的源 IP 地址是网关地址的 ARP 报文，从而使主机修改网关的 MAC 地址为攻击者的 MAC 地址，需要发送给原来网关的报文就发送给攻击者了。	配置作为网关的 S5700 丢弃 ARP 报文头的源 IP 地址是自己 IP 地址的 ARP 报文。 但是这种防攻击策略只能适用于所有主机的 ARP 报文必须通过网关转发的场景。
防中间人攻击	中间人攻击会同时修改主机和网关的信息。 • 修改主机上的网关信息：攻击者仿冒网关地址，发送 ARP 报文头的源 IP 地址是网关地址的 ARP 报文，使主机修改网关的 MAC 地址为攻击者的 MAC 地址 • 修改网关上的主机信息：攻击者仿冒主机地址，发送 ARP 报文头的源 IP 地址是主机地址的 ARP 报文，使网关修改主机的 MAC 地址为攻击者的 MAC 地址	在 S5700 上配置绑定表，将 ARP 报文与绑定表进行对比，不符合的丢弃该报文。目前 S5700 只支持 DHCP Snooping 的绑定表。 但是这种防攻击策略只能适用于所有主机的 ARP 报文必须通过网关转发的场景。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 防欺骗攻击功能之前，需要准备以下数据。

序号	数据
1	ARP 地址防欺骗的方式
2	防中间人攻击中与 DHCP Snooping 绑定表匹配检查方式
3	（可选）ARP 报文检查不匹配丢弃报文告警阈值

配置严格学习 ARP 表项

背景信息

严格学习 ARP 表项指的是 S5700 只学习自己发送的 ARP 请求报文的应答报文。

说明：

S5700SI 和 S5700EI 上 ARP 严格学习功能默认处于使能状态，如果用户需要向设备发送 ARP 报文，触发设备进行 ARP 学习，则必须在设备上去使能 ARP 严格学习功能。

操作步骤

- 配置全局严格学习 ARP 表项

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp learning strict**，配置严格学习 ARP 表项。

     缺省情况下，S5700SI 和 S5700EI 上 ARP 严格学习功能处于使能状态，S5700HI、S5700LI、S5700S-LI、S5710LI 和 S5710EI 上 ARP 严格学习功能处于关闭状态。

- 配置 VLANIF 接口严格学习 ARP 表项功能

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *interface-number*，进入 VLANIF 接口视图。
  3. 执行命令 **arp learning strict** { **force-enable** | **force-disable** | **trust** }，配置 VLANIF 接口的 ARP 严格学习功能。

     - **force-enable** 表示使能 VLANIF 接口的 ARP 严格学习功能。

- **force-disable** 表示去使能 VLANIF 接口的 ARP 严格学习功能。
- **trust** 表示 VLANIF 接口的 ARP 严格学习功能与全局配置保持一致。

缺省情况下，VLANIF 接口的 ARP 严格学习功能和全局配置保持一致。

配置防止 ARP 地址欺骗

背景信息

说明：

S5700LI、S5710LI 和 S5700S-LI 不支持 ARP 地址防欺骗功能。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，使能 ARP 地址防欺骗功能。

   只能同时使能一种 ARP 地址防欺骗方式。如果原来使能了某一种方式，则新配置的方式将覆盖原来配置的方式。

   缺省情况下，S5700 未使能 ARP 地址防欺骗功能。

配置防止 ARP 网关冲突

背景信息

如果有攻击者仿冒网关，在局域网内部发送源 IP 地址是网关 IP 地址的 ARP 报文，会导致局域网内其他用户主机的 ARP 表记录错误的网关地址映射关系。这样其他用户主机就会把发往网关的流量均发送给了攻击者，攻击者可轻易窃听到他们发送的数据内容，并且最终会造成这些用户主机无法访问网络。

为了防范攻击者仿冒网关，当用户主机直接接入网关时，可以在网关设备上配置防止 ARP 网关冲突功能。当设备收到的 ARP 报文存在下列情况之一：

- ARP 报文的源 IP 地址与报文入接口对应的 VLANIF 接口的 IP 地址相同
- ARP 报文的源 IP 地址是入接口的虚拟 IP 地址，但 ARP 报文源 MAC 地址不是 VRRP 虚 MAC

设备就认为该 ARP 报文是与网关地址冲突的 ARP 报文，设备将生成 ARP 防攻击表项，并在后续一段时间内丢弃该接口收到的同 VLAN 以及同源 MAC 地址的 ARP 报文，这样就可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp anti-attack gateway-duplicate enable**，使能 ARP 网关冲突防攻击功能。

   ARP 网关冲突防攻击功能使能后，系统生成 ARP 防攻击表项，在后续一段时间内对收到具有相同源 MAC 地址的报文直接丢弃，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

配置防止 ARP 中间人攻击

背景信息

防止 ARP 中间人攻击，可以配置 ARP 报文检查功能，对接口或 VLAN 下收到的 ARP 报文和绑定表进行匹配检查，当报文的检查项和绑定表中的特征项一致时，转发该报文，否则丢弃报文。

同时可以配置告警功能，当丢弃的报文数超过限制的阈值时，发出告警信息。

说明：

本功能仅适用于 DHCP Snooping 场景。设备使能 DHCP Snooping 功能后，当 DHCP 用户上线时，设备会自动生成 DHCP Snooping 绑定表；对于静态配置 IP 地址的用户，设备不会生成 DHCP Snooping 绑定表，所以需要手动添加静态绑定表。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。或者执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
3. 执行命令 **arp anti-attack check user-bind enable**，使能 ARP 报文检查功能。

   缺省情况下，接口或 VLAN 未使能对 ARP 报文的检查功能。

4. 接口视图下执行命令 arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **vlan** }*，或者 VLAN 视图下执行命令 arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **interface** }*，配置 ARP 报文检查方式。

   缺省情况下，对 IP 地址、MAC 地址、VLAN 和接口都进行检查。对检查项不匹配绑定表的报文做丢弃处理。

   说明：

   IP 地址包括 IPv4 地址和 IPv6 地址，即配置 ARP 报文检查方式为 IP 地址时，S5700 将对 ARP 报文的 IPv4 地址和 IPv6 地址都进行绑定表匹配检查。

   指定 ARP 报文绑定表匹配检查项对配置了静态绑定表的用户不起作用，即设备仍然按照静态绑定表的内容对 ARP 报文进行绑定表匹配检查。

   当同时在 VLAN 和加入该 VLAN 的接口下配置 ARP 报文检查功能，设备会先按照接口下配置的检查方式对 ARP 报文进行绑定表匹配检查，如果 ARP 报文检查通过，设备再根据 VLAN 下配置的检查方式进行检查。

5. （可选）接口视图下执行命令 arp anti-attack check user-bind alarm enable，使能 ARP 报文检查丢弃报文告警功能。

   缺省情况下，接口未使能丢弃 ARP 报文告警功能。

   注意：

   请不要在 VLAN 和接口下同时配置 arp anti-attack check user-bind enable，否则将导致 ARP 报文检查丢弃报文告警功能失效。

6. （可选）接口视图下执行命令 arp anti-attack check user-bind alarm threshold *threshold*，配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

   缺省情况下，ARP 报文不匹配绑定表而丢弃的告警阈值为 100。

配置 ARP 报文源 MAC 地址检查功能

背景信息

ARP 报文进入 S5700 后，系统会首先自动对 ARP 报文的有效性进行检查，包括但不限于：

- 报文长度检查
- 以太头的源 MAC 合法性检查
- ARP 请求、回应类型检查
- 硬件地址长度检查
- 协议地址长度检查
- ARP 帧格式是否为以太类型检查

这些检查是用来判断是否与协议一致，过滤无效报文。其中 ARP 头源 MAC 和以太头源 MAC 地址不匹配的 ARP 报文是协议允许的 ARP 报文，但是在现网应用中，该类报文很可能是攻击报文，配置了 **arp anti-attack packet-check sender-mac** 命令后，系统会检查 ARP 头源 MAC 和以太头源 MAC 地址是否匹配，如果不匹配，则丢弃该报文，可以防止此类报文的攻击产生。

ARP 头源 MAC 和以太头源 MAC 地址不一致的 ARP 报文在协议里面定义的是有效报文，但是在实际的组网中这种报文很多情况下都是攻击报文。S5700 提供了命令行控制是否进行该类报文的检查，如果满足条件就删除该报文，配置灵活。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **arp anti-attack packet-check sender-mac**，启动对 ARP 头源 MAC 和以太头源 MAC 地址不匹配的 ARP 报文的检查功能，如果不匹配，丢弃该报文。

配置发送 ARP 免费报文

通过配置发送免费 ARP 报文，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

背景信息

该报文使用网关的 IP 地址作为目标地址发送 ARP 请求，定时更新用户 ARP 表项的网关 MAC 地址，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

当 S5700 作为网关时，可以在全局或 VLANIF 接口下发送免费 ARP 报文。当全局和 VLANIF 接口下都使能发送免费 ARP 功能时，VLANIF 接口下的配置优先生效。

说明：

S5700LI、S5710LI 和 S5700S-LI 不支持免费 ARP 报文功能。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. （可选）执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
3. 执行命令 **arp gratuitous-arp send enable**，使能发送免费 ARP 报文的功能。

   缺省情况下，发送免费 ARP 报文的功能未使能。
4. （可选）执行命令 **arp gratuitous-arp send interval** *interval-time*，配置发送免费 ARP 报文的时间间隔。

   缺省情况下，系统发送免费 ARP 报文的时间间隔为 60 秒。

配置 DHCP 触发 ARP 学习

背景信息

配置 DHCP 触发 ARP 学习，当 DHCP 服务器给用户分配 IP 地址，S5700 回应用户 DHCP ACK 报文成功后，会取用户的 MAC 地址，生成该 IP 地址对应的 ARP 表项。这样可以省掉设备学习用户主机 ARP 的过程。

说明：

S5700LI、S5710LI 和 S5700S-LI 不支持 DHCP 触发 ARP 学习功能。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface vlanif** *interface-number*，进入 Vlanif 接口视图。
3. 执行命令 **arp learning dhcp-trigger**，配置 S5700 根据 Vlanif 接口上收到的 DHCP ACK 报文生成 ARP 表项。

   缺省情况下，S5700 收到 DHCP ACK 报文不生成 ARP 表项。当有流量通过时，才触发学习 ARP。

   说明：

- 本命令生效的前提是使能 DHCP Snooping 功能。
- 在 VRRP 和 DHCP Relay 组合场景下，VRRP 主备设备上都不能再配置 DHCP Snooping 功能和 **arp learning dhcp-trigger** 命令。

配置端口隔离后 ARP 报文转发功能

背景信息

S5700 开启基于 DHCP Snooping 的 ARP 安全功能，上行连接的设备启动 VLAN 内 ARP 代理功能，下挂用户 PC，各用户 PC 通过用户侧端口上线。如果用户上线的端口配置了端口隔离，则隔离用户间的 ARP 请求报文因端口隔离而丢弃，相互之间无法正常通信。此时，通过配置端口隔离后 ARP 报文转发功能，将 ARP 请求报文转发到信任端口。由于信任端口上方配置了 VLAN 内 ARP 代理功能，隔离的用户可以通过 VLAN 内代理实现相互通信。

操作步骤

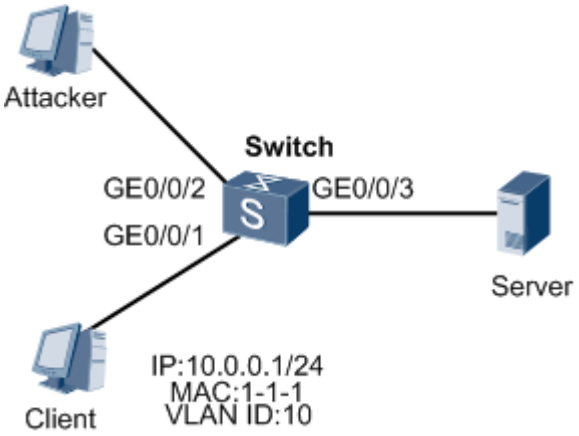
- 执行命令 **system-view**，进入系统视图。
- 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
- 执行命令 **dhcp snooping arp security enable**，开启基于 DHCP Snooping 的 ARP 安全功能。
- 执行命令 **dhcp snooping arp security isolate-forwarding-trust**，开启在入接口与出接口端口隔离时将报文向信任端口转发功能。

配置防止 ARP 中间人攻击示例

组网需求

如图 1 所示，Switch 的 GE0/0/1 和 GE0/0/2 接口连接了两个用户。Switch 的接口 GE0/0/1、GE0/0/2 和 GE0/0/3 都属于 VLAN10。假设 GE0/0/3 接口连接的用户是一个攻击者。为了防止 ARP 中间人攻击，要求在 Switch 上配置 ARP 报文检查功能，只有接收到的 ARP 报文信息和绑定表中的内容一致才会被转发，否则报文将被丢弃。同时使能丢弃报文告警功能。

图 1 配置防止 ARP 中间人攻击组网图



配置思路

采用如下的思路配置防止 ARP 中间人攻击：

1. 使能 ARP 报文检查功能。
2. 使能丢弃报文告警功能。
3. 配置 DHCP Snooping 功能，使 ARP 报文检查功能生效。
4. 配置静态绑定表。

数据准备

为完成此配置举例，需要准备以下数据：

- 使能报文检查的接口：GE0/0/1、GE0/0/2。
- DHCP Snooping 信任接口：GE0/0/3。
- ARP 报文检查丢弃告警阈值：80。
- 静态绑定表绑定 Client 的的 IP 地址：10.0.0.1/24，MAC 地址：1-1-1，VLAN ID：10。

操作步骤

1. 创建 VLAN，将接口加入到 VLAN 中

   # 创建 VLAN10，并将接口 GE0/0/1、GE0/0/2、GE0/0/3 加入 VLAN10 中。

```
<Quidway> system-view
[Quidway] vlan batch 10
```

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type access
[Quidway-GigabitEthernet0/0/1] port default vlan 10
[Quidway-GigabitEthernet0/0/1] quit
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type access
[Quidway-GigabitEthernet0/0/2] port default vlan 10
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Quidway-GigabitEthernet0/0/3] quit
```

2. 配置 ARP 报文检查功能

在连接 Client 的 GE1/0/1 接口使能 ARP 报文检查功能。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
```

在连接 Attacker 的 GE0/0/2 接口使能 ARP 报文检查功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind enable
```

3. 配置报文丢弃告警功能

在连接 Client 的 GE0/0/1 接口配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

```
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[Quidway-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm threshold 80
[Quidway-GigabitEthernet0/0/1] quit
```

在连接 Attacker 的 GE0/0/2 接口配置 ARP 报文不匹配绑定表而丢弃的告警阈值。

```
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind alarm enable
```

```
[Quidway-GigabitEthernet0/0/2] arp anti-attack check user-bind alarm threshold 80
[Quidway-GigabitEthernet0/0/2] quit
```

4. 配置 DHCP Snooping 功能

全局使能 DHCP Snooping 功能。

```
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

在 VLAN10 内使能 DHCP Snooping 功能。

```
[Quidway] vlan 10
[Quidway-vlan10] dhcp snooping enable
[Quidway-vlan10] quit
```

配置接口 GE0/0/3 为 DHCP Snooping 信任接口。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/3] quit
```

5. 配置静态绑定表项

配置 Client 为静态绑定表项。

```
[Quidway] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface
gigabitethernet 0/0/1 vlan 10
```

6. 验证配置结果

执行 **display arp anti-attack configuration check user-bind interface** 命令可以查看接口下 ARP 报文检查配置信息。

```
<Quidway> display arp anti-attack configuration check user-bind interface
gigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
```

```
 arp anti-attack check user-bind alarm threshold 80
<Quidway> display arp anti-attack configuration check user-bind interface
gigabitethernet 0/0/2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
```

配置文件

```
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface GigabitEthernet 0/0/1
vlan 10
#
vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 80
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
```

```
#
return
```

配置 ARP 安全功能示例

组网需求

如图 1 所示，Switch 通过 GE0/0/3 接口连接一台服务器，通过 GE0/0/1 和 GE0/0/2 接口连接 VLAN10 和 VLAN20 下的四个用户。网络中存在的 ARP 威胁是：

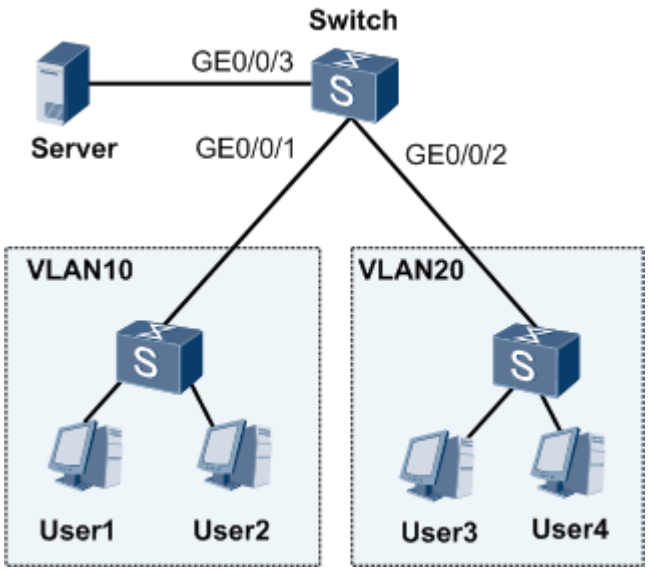
- 服务器可能会发出一些目的 IP 地址不可达的报文，而且这种报文相对其他普通用户的报文要多。
- 用户 User1 中病毒后，会发出大量 ARP 攻击报文，部分 ARP 报文的源 IP 地址在本网段内不停变化，部分 ARP 报文的源 IP 地址和网关 IP 地址相同。
- 用户 User3 构造大量源 IP 地址固定的 ARP 报文对网络进行攻击。
- 用户 User4 发送大量目的 IP 不可达的 IP 报文对网络进行攻击。

要求在 Switch 配置 ARP 的安全功能，能够防止以上的攻击。对 Server，需要配置其 ARP Miss 源抑制的速率比其他用户大。

说明：

以 S5700HI 为例。

图 1 配置 ARP 安全功能组网图



配置思路

采用如下思路配置 ARP 的安全功能：

1. 配置严格学习 ARP 表项。
2. 配置基于接口的 ARP 表项限制。
3. 配置防止 ARP 地址欺骗攻击。
4. 配置防止 ARP 网关冲突攻击。
5. 配置 ARP 报文源抑制。
6. 配置 ARP Miss 源抑制。
7. 配置对潜在的攻击行为写日志和发送告警。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 ARP 表项限制：20 个。
- 防止 User1 发起的 ARP 地址欺骗攻击方式为 **fixed-mac**。
- 服务器 IP 地址：2.2.2.2/24。
- 发出大量 ARP 报文的 User4 的地址：2.2.4.2/24。
- ARP 报文速率源抑制阈值：User4 为 10pps，其他用户为 15pps。
- ARP Miss 源抑制阈值：普通用户为 20pps，对 Server 为 50pps。
- 对潜在的攻击行为写日志和发送告警的时间间隔为 300 秒。

操作步骤

1. 配置严格学习 ARP 表项

```
<Quidway> system-view
[Quidway] arp learning strict
```

3. 配置基于接口的 ARP 表项限制

各个接口的 ARP 表项限制为 20，以 GE0/0/1 为例，其他接口配置步骤相似。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] arp-limit vlan 10 maximum 20
[Quidway-GigabitEthernet0/0/1] quit
```

4. 配置防止 ARP 地址欺骗攻击

配置 ARP 地址欺骗防攻击方式为 fixed-mac 方式，防止 User1 发起的 ARP 地址欺骗攻击。

```
[Quidway] arp anti-attack entry-check fixed-mac enable
```

5. 配置防止 ARP 网关冲突攻击

使能 ARP 网关冲突防攻击功能，防止 User1 发起的伪造网关地址攻击。

```
[Quidway] arp anti-attack gateway-duplicate enable
```

6. 配置 ARP 报文源抑制

配置 User4 发送的 ARP 报文速率抑制阈值为 10pps。为防止所有用户误发过多 ARP 报文，配置系统的 ARP 报文速率抑制阈值为 15pps。

```
[Quidway] arp speed-limit source-ip maximum 15
[Quidway] arp speed-limit source-ip 2.2.4.2 maximum 10
```

7. 配置 ARP Miss 源抑制

配置系统的 ARP Miss 源抑制阈值为 20pps，以防止较大流量目的 IP 地址不可达的 IP 报文的攻击。

```
[Quidway] arp-miss speed-limit source-ip maximum 20
```

配置 Server 的 ARP Miss 源抑制阈值为 50pps，这样既防止 Server 无意发起大流量目的 IP 地址不可达的 IP 报文的攻击；又防止在其发送的目的 IP 地址不可达的 IP 报文速率并非特别大的时候，就阻止了它的网络通信。

```
[Quidway] arp-miss speed-limit source-ip 2.2.2.2 maximum 50
```

8. 配置对潜在的攻击行为写日志和发送告警

```
[Quidway] arp anti-attack log-trap-timer 300
```

9. 验证配置结果

配置完成后，可以使用命令 **display arp learning strict**，查看 ARP 严格学习情况。

```
<Quidway> display arp learning strict
 The global configuration:arp learning strict
 Interface                          LearningStrictState
------------------------------------------------------------

------------------------------------------------------------
 Total:0
 Force-enable:0
 Force-disable:0
```

可以使用命令 **display arp-limit** 查看接口可以学习 ARP 数目的最大值。

```
<Quidway> display arp-limit interface gigabitethernet 0/0/1
 Interface                     LimitNum   VlanID     LearnedNum(Mainboard)
------------------------------------------------------------------------------
 GigabitEthernet0/0/1          20         10         0
------------------------------------------------------------------------------
 Total:1
```

可以使用命令 **display arp anti-attack configuration all** 查看当前 ARP 防攻击配置情况。

```
<Quidway> display arp anti-attack configuration all
ARP anti-attack packet-check function: disable


ARP gateway-duplicate anti-attack function: disabled


ARP anti-attack log-trap-timer: 300 second(s)
(The log and trap timer of speed-limit, default is 0 and means disabled.)


ARP anti-attack entry-check mode:
 Vlanif      Mode
------------------------------------------------------------------------------
```

```
 All         fixed-mac
------------------------------------------------------------------------------


ARP rate-limit configuration:
------------------------------------------------------------------------------
Global configuration:
Interface configuration:
Vlan configuration:
------------------------------------------------------------------------------


ARP miss rate-limit configuration:
------------------------------------------------------------------------------
Global configuration:
Interface configuration:
Vlan configuration:
------------------------------------------------------------------------------


ARP speed-limit for source-MAC configuration:
MAC-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
All                  0
------------------------------------------------------------------------------
The number of configured specified MAC address(es) is 0, spec is 512.


ARP speed-limit for source-IP configuration:
IP-address           suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
2.2.4.2              10
Others               15
------------------------------------------------------------------------------
The number of configured specified IP address(es) is 1, spec is 512.
```

```
ARP miss speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
2.2.2.2/32          50
Others              20
------------------------------------------------------------------------------
The number of configured specified IP address(es) is 1, spec is 512.
```

可以使用命令 **display arp packet statistics** 查看丢弃的 ARP 报文数目和学习到的 ARP 表项。

```
<Quidway> display arp packet statistics
ARP Pkt Received:   sum  154333
ARP-Miss Msg Received:   sum      0
ARP Learnt Count:   sum      8
ARP Pkt Discard For Limit:   sum      5
ARP Pkt Discard For SpeedLimit:   sum    0
ARP Pkt Discard For Proxy Suppress:   sum      0
ARP Pkt Discard For IP Pool Check:   sum      0
ARP Pkt Discard For Other:   sum  151597
ARP-Miss Msg Discard For SpeedLimit:   sum      0
ARP-Miss Msg Discard For Other:   sum      3
ARP Pkt Discard For Gratuitous ARP:   sum      0
ARP Pkt Discard For Destination MAC check:   sum      0
```

配置文件

```
#
 sysname Quidway
#
vlan batch 10 20 30
#
 arp speed-limit source-ip maximum 15
 arp-miss speed-limit source-ip maximum 20
 arp learning strict
 arp anti-attack log-trap-timer 300
```

```
#
 arp anti-attack entry-check fixed-mac enable
 arp anti-attack gateway-duplicate enable
 arp-miss speed-limit source-ip 2.2.2.2 maximum 50
 arp speed-limit source-ip 2.2.4.2 maximum 10
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid tagged vlan 10
 arp-limit vlan 10 maximum 20
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid tagged vlan 20
 arp-limit vlan 20 maximum 20
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
 arp-limit vlan 30 maximum 20
#
return
```

HCIE-Security 模拟面试问题及面试建议

1. 防 ARP DOS 攻击有哪些措施？
2. 防 ARP 欺骗攻击有哪些措施？