

10 ARP 安全配置

10.1 ARP 安全简介

介绍ARP安全的定义和作用。

定义

ARP (Address Resolution Protocol) 安全是针对ARP攻击的一种安全特性，它通过一系列对ARP表项学习和ARP报文处理的限制、检查等措施来保证网络设备的安全性。ARP安全特性不仅能够防范针对ARP协议的攻击，还可以防范网段扫描攻击等基于ARP协议的攻击。

目的

ARP协议有简单、易用的优点，但是也因为其没有任何安全机制，容易被攻击者利用。在网络中，常见的ARP攻击方式主要包括：

- ARP泛洪攻击，也叫拒绝服务攻击DoS (Denial of Service)，主要存在这样两种场景：
 - 设备处理ARP报文和维护ARP表项都需要消耗系统资源，同时为了满足ARP表项查询效率的要求，一般设备都会对ARP表项规模有规格限制。攻击者就利用这一点，通过伪造大量源IP地址变化的ARP报文，使得设备ARP表资源被无效的ARP条目耗尽，合法用户的ARP报文不能继续生成ARP条目，导致正常通信中断。
 - 攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标IP地址不能解析的IP报文，导致设备触发大量ARP Miss消息，生成并下发大量临时ARP表项，并广播大量ARP请求报文以对目标IP地址进行解析，从而造成CPU (Central Processing Unit) 负荷过重。
- ARP欺骗攻击，是指攻击者通过发送伪造的ARP报文，恶意修改设备或网络内其他用户主机的ARP表项，造成用户或网络的报文通信异常。

ARP攻击行为存在以下危害：

- 会造成网络连接不稳定，引发用户通信中断。
- 利用ARP欺骗截取用户报文，进而非法获取游戏、网银、文件服务等系统的帐号和口令，造成被攻击者重大利益损失。

为了避免上述ARP攻击行为造成的各种危害，ARP安全特性针对不同的攻击类型提供了多种解决方案，具体如[表10-1](#)和[表10-2](#)所示：

表 10-1 ARP 安全针对泛洪攻击的解决方案

防攻击功能	功能说明	部署设备
ARP报文限速	通过ARP报文限速功能，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
ARP Miss消息限速	通过ARP Miss消息限速功能，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
免费ARP报文主动丢弃	使能免费ARP报文主动丢弃功能后，设备直接丢弃免费ARP报文，可以防止设备因处理大量免费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
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
禁止接口学习ARP表项	通过禁止指定的接口学习ARP表项，可以防止该接口下所接入的用户主机发起ARP攻击使整个设备的ARP表资源都被耗尽。	建议在网关设备上部署本功能

表 10-2 ARP 安全针对欺骗攻击的解决方案

防攻击功能	功能说明	部署设备
ARP表项固化	<p>使能ARP表项固化功能后，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。</p> <p>设备提供三种ARP表项固化模式：fixed-all模式、fixed-mac模式和send-ack模式。</p>	建议在网关设备上部署本功能
动态ARP检测	<p>使能动态ARP检测DAI（Dynamic ARP Inspection）功能后，当设备收到ARP报文时，将此ARP报文的源IP、源MAC（Media Access Control）、收到ARP报文的接口及VLAN（Virtual Local Area Network）信息和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，否则认为是攻击，丢弃该ARP报文。</p> <p>本功能仅适用于DHCP Snooping（Dynamic Host Configuration Protocol Snooping）场景。</p>	建议在接入设备上部署本功能
免费ARP报文主动丢弃	<p>使能免费ARP报文主动丢弃功能后，设备直接丢弃免费ARP报文，可以防止设备因收到大量伪造的免费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。</p>	建议在网关设备上部署本功能
ARP报文内MAC地址一致性检查	<p>通过ARP报文内MAC地址一致性检查功能，可以防止以太网数据帧首部中的源、目的MAC地址和ARP报文数据区中的源、目的MAC地址不一致的ARP欺骗攻击。</p>	建议在网关设备上部署本功能
ARP表项严格学习	<p>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。</p>	建议在网关设备上部署本功能

受益

- 可以有效降低用户为保证网络正常运行和网络信息安全而产生的维护成本。
- 可以为用户提供更安全的网络环境和更稳定的网络服务。

10.2 ARP 安全原理描述

介绍ARP安全的实现原理。

10.2.1 ARP 报文限速

如果设备对收到的大量ARP报文全部进行处理，可能导致CPU负荷过重而无法处理其他业务。因此，在处理之前，设备需要对ARP报文进行限速，以保护CPU资源。

设备提供了如下几类针对ARP报文的限速功能：

- 根据源MAC地址或源IP地址进行ARP报文限速
当设备检测到某一个用户在短时间内发送大量的ARP报文，可以针对该用户配置基于源MAC地址或源IP地址的ARP报文限速。在1秒时间内，如果该用户的ARP报文数目超过设定阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文。
 - 根据源MAC地址进行ARP报文限速：如果指定MAC地址，则针对指定源MAC地址的ARP报文根据限速值进行限速；如果不指定MAC地址，则针对每一个源MAC地址的ARP报文根据限速值进行限速。
 - 根据源IP地址进行ARP报文限速：如果指定IP地址，则针对指定源IP地址的ARP报文根据限速值进行限速；如果不指定IP地址，则针对每一个源IP地址的ARP报文根据限速值进行限速。
- 根据目的IP地址进行ARP报文限速
当设备需要处理大量目的IP地址相同的ARP报文时，可以配置基于目的IP地址的ARP报文限速。设备会对上送CPU的ARP报文根据目的IP地址进行统计，如果在1秒内收到的同一个目的IP地址的ARP报文超过设定阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文。
- 针对全局、VLAN和接口的ARP报文限速
设备支持在全局、VLAN和接口下配置ARP报文的限速值，当同时在全局、VLAN和接口下配置ARP报文的限速值时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

说明

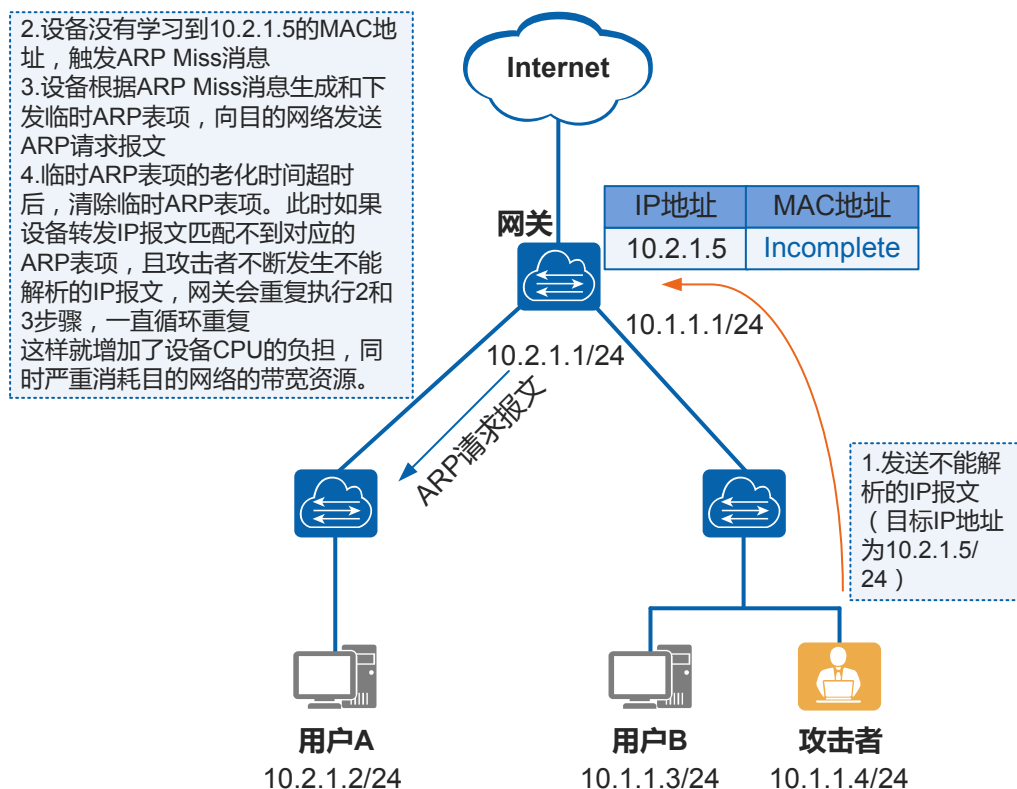
CE6870EI和CE6875EI不支持在接口视图下配ARP报文限速。

- 针对全局的ARP报文限速：在设备出现ARP攻击时，限制全局处理的ARP报文数量。
- 针对VLAN的ARP报文限速：在某个VLAN内的所有接口出现ARP攻击时，限制处理收到的该VLAN内的ARP报文数量，配置本功能可以保证不影响其他VLAN内所有接口的ARP学习。
- 针对接口的ARP报文限速：在某个接口出现ARP攻击时，限制处理该接口收到的ARP报文数量，配置本功能可以保证不影响其他接口的ARP学习。

10.2.2 ARP Miss 消息限速

如果网络中有用户向设备发送大量目标IP地址不能解析的IP报文（即路由表中存在该IP报文的IP地址对应的路由表项，但设备上没有该路由表项中下一跳对应的ARP表项），将导致设备触发大量的ARP Miss消息。这种触发ARP Miss消息的IP报文（即ARP Miss报文）会被上送到CPU进行处理，设备会根据ARP Miss消息生成和下发大量临时ARP表项并向目的网络发送大量ARP请求报文，这样就增加了设备CPU的负担，同时严重消耗目的网络的带宽资源。如图10-1所示，攻击者向网关发送目的地址为10.2.1.5/24且不能解析的IP报文。

图 10-1 ARP Miss 攻击



为了避免这种IP报文攻击所带来的危害，设备提供了如下几类针对ARP Miss消息的限速功能：

- 根据源IP地址进行ARP Miss消息限速
当设备检测到某一源IP地址的IP报文在1秒内触发的ARP Miss消息数量超过了ARP Miss消息限速值，就认为此源IP地址存在攻击。
如果指定了IP地址，则针对指定源IP地址的ARP Miss消息根据限速值进行限速；如果不指定IP地址，则针对每一个IP地址的ARP Miss消息根据限速值进行限速。
- 针对全局、VLAN和接口的ARP Miss消息限速
当同时在全局、VLAN或接口下配置ARP Miss消息限速时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。
 - 针对全局的ARP Miss消息限速：在设备出现目标IP地址不能解析的IP报文攻击时，限制全局处理的ARP Miss消息数量。

- 针对VLAN的ARP Miss消息限速：在某个VLAN内的所有接口出现目标IP地址不能解析的IP报文攻击时，限制处理该VLAN内报文触发的ARP Miss消息数量，配置本功能可以保证不影响其他VLAN内所有接口的IP报文转发。
- 针对接口的ARP Miss消息限速：在某个接口出现目标IP地址不能解析的IP报文攻击时，限制处理该接口收到的报文触发的ARP Miss消息数量，配置本功能可以保证不影响其他接口的IP报文转发。
- 通过设定临时ARP表项的老化时间控制ARP Miss消息的触发频率
当IP报文触发ARP Miss消息时，设备会根据ARP Miss消息生成临时ARP表项，并且向目的网段发送ARP请求报文。
 - 在临时ARP表项老化时间范围内：
 - 设备收到ARP应答报文前，匹配临时ARP表项的IP报文将被丢弃并且不会触发ARP Miss消息。
 - 设备收到ARP应答报文后，则生成正确的ARP表项来替换临时ARP表项。
 - 当老化时间超时后，设备会清除临时ARP表项。此时如果设备转发IP报文匹配不到对应的ARP表项，则会重新触发ARP Miss消息并生成临时ARP表项，如此循环重复。

当判断设备受到攻击时，可以增大临时ARP表项的老化时间，减小设备ARP Miss消息的触发频率，从而减小攻击对设备的影响。

10.2.3 免费 ARP 报文主动丢弃

免费ARP报文是一种特殊的ARP报文，该报文中携带的源IP地址和目的IP地址都是本机IP地址，源MAC地址是本机MAC地址，目的MAC地址是广播地址。当有新的用户主机接入网络时，该用户主机会以广播的方式发送免费ARP报文，来确认广播域中是否有其他设备与自己的IP地址冲突；当用户主机改变了硬件地址时，为了能够在其他所有用户主机的ARP表项老化之前通告其硬件地址已经发生改变，该用户主机也会发送免费ARP报文。

由于发送免费ARP报文的用户主机并不需要经过身份验证，任何一个用户主机都可以发送免费ARP报文，这样就引入了两个问题：

- 如果网络中出现大量的免费ARP报文，设备会因为处理这些报文而导致CPU负荷过重，从而不能正常处理合法的ARP报文。
- 如果设备处理的免费ARP报文是攻击者伪造的，会造成设备错误地更新ARP表项，导致合法用户的通信流量发生中断。

参考以上问题描述，在确认攻击来自免费ARP报文之后，可以在网关设备上使能免费ARP报文主动丢弃功能，使网关设备直接丢弃免费ARP报文。

须知

当有主机更新了硬件地址并重新接入网络（如主机关机后更换了接口卡并重新启动，或双机热备份系统中主用设备发生故障，备用设备接管）时，如果设备开启了免费ARP报文主动丢弃功能，可能会导致其他网络设备因无法正常更新相应的ARP表项而无法与该主机建立正常通信。

10.2.4 ARP 表项严格学习

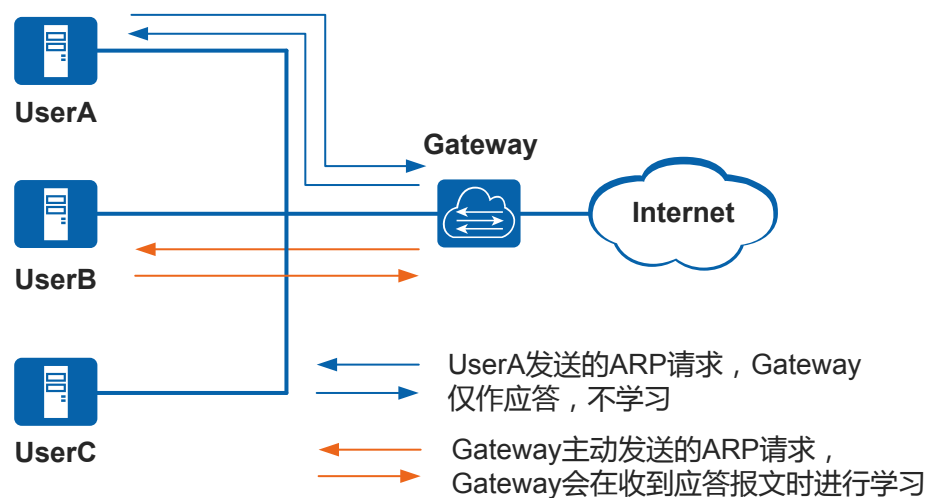
如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成下面的危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，进而导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备的ARP表项，导致用户无法正常通信。

为避免上述危害，可以在网关设备上部署ARP表项严格学习功能。

ARP表项严格学习是指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，这样可以拒绝大部分的ARP报文攻击。

图 10-2 ARP 表项严格学习



如图10-2所示。通常情况下，当UserA向Gateway发送ARP请求报文后，Gateway会向UserA回应ARP应答报文，并且添加或更新UserA对应的ARP表项。当Gateway配置ARP表项严格学习功能以后：

- 对于Gateway收到UserA发送来的ARP请求报文，Gateway不添加也不更新UserA对应的ARP表项。如果该请求报文请求的是Gateway的MAC地址，那么Gateway会向UserA回应ARP应答报文。
- 如果Gateway向UserB发送ARP请求报文，待收到与该请求对应的ARP应答报文后，Gateway会添加或更新UserB对应的ARP表项。

10.2.5 ARP 表项限制

ARP表项限制功能应用在网关设备上，可以限制设备的某个接口学习动态ARP表项的数目。默认状态下，接口可以学习的动态ARP表项数目规格与全局的ARP表项规格保持一致。当部署完ARP表项限制功能后，如果指定接口下的动态ARP表项达到了允许学习的最大数目，将不再允许该接口继续学习动态ARP表项，以保证当一个接口所接入的某一用户主机发起ARP攻击时不会导致整个设备的ARP表资源都被耗尽。

10.2.6 禁止接口学习 ARP 表项

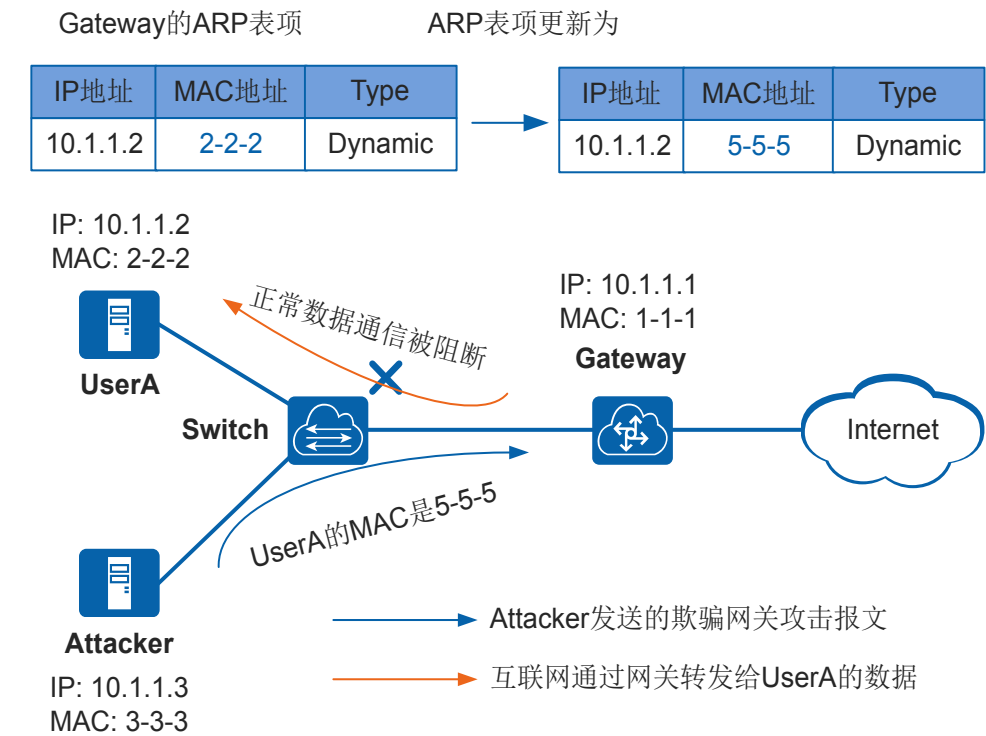
当某接口下学习了大量动态ARP表项时，出于安全考虑可以配置禁止该接口的动态ARP表项学习功能，以防止该接口下所接入的用户主机发起ARP攻击使整个设备的ARP表资源都被耗尽。

禁止接口学习ARP表项功能和ARP表项严格学习功能配合起来使用，可以使设备对接口下动态ARP的学习进行更加细致的控制。

10.2.7 ARP 表项固化

如图10-3所示，Attacker仿冒UserA向Gateway发送伪造的ARP报文，导致Gateway的ARP表中记录了错误的UserA地址映射关系，造成UserA接收不到正常的数据报文。

图 10-3 欺骗网关攻击示意图



为了防御这种欺骗网关攻击，可以在网关设备上部署ARP表项固化功能。网关设备在第一次学习到ARP以后，不再允许用户更新此ARP表项或只能允许更新此ARP表项的部分信息，或者通过发送单播ARP请求报文的方式对更新ARP条目的报文进行合法性确认。

设备提供的三种ARP表项固化模式，如表10-3所示。

表 10-3 ARP 表项固化模式介绍

固化模式	功能
fixed-all模式	如果设备收到的ARP报文中的MAC地址、接口或VLAN信息和ARP表中的信息不匹配，则直接丢弃该ARP报文。此模式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
fixed-mac模式	如果设备收到的ARP报文中的MAC地址与ARP表中对应条目的MAC地址不匹配，则直接丢弃该ARP报文；如果匹配，但是收到报文的接口或VLAN信息与ARP表中对应条目不匹配，则可以更新对应ARP条目中的接口和VLAN信息。此模式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。
send-ack模式	<p>如果设备收到的ARP报文A涉及ARP表项MAC地址、接口或VLAN信息的修改，设备不会立即更新ARP表项，而是先向待更新的ARP表项现有MAC地址对应的用户发送一个单播的ARP请求报文进行确认。</p> <ul style="list-style-type: none"> 如果在随后的3秒内设备收到ARP应答报文B，且当前ARP条目中的IP地址、MAC地址、接口和VLAN信息与ARP应答报文B的一致，则认为ARP报文A为攻击报文，不更新该ARP条目。 如果在随后的3秒内设备未收到ARP应答报文，或者收到ARP应答报文B与当前ARP条目中的IP地址、MAC地址、接口和VLAN信息不一致，设备会再向刚才收到的ARP报文A对应的源MAC发送一个单播ARP请求报文。 <ul style="list-style-type: none"> 如果在随后的3秒内收到ARP应答报文C，且ARP报文A与ARP应答报文C的源IP地址、源MAC地址、接口和VLAN信息一致，则认为现有ARP条目已经无效且ARP报文A是可以更新该ARP条目的合法报文，并根据ARP报文A来更新该ARP条目。 如果在随后的3秒内未收到ARP应答报文，或者ARP报文A与收到的ARP应答报文C的源IP地址、源MAC地址、接口和VLAN信息不一致，则认为ARP报文A为攻击报文，设备会忽略收到的ARP报文A，ARP条目不会更新。 <p>此模式适用于用户的MAC地址和接入位置均频繁变动的场景。</p>

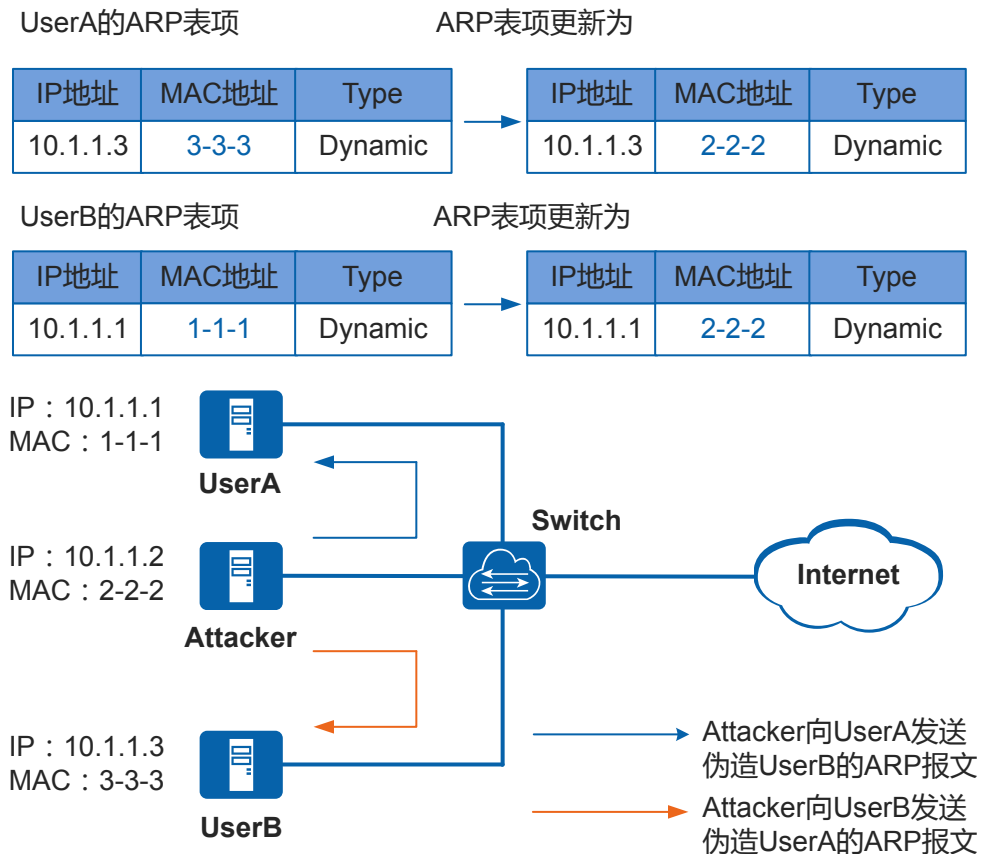
10.2.8 动态 ARP 检测

网络中针对ARP的攻击层出不穷，中间人攻击是常见的ARP欺骗攻击方式之一。

中间人攻击（Man-in-the-middle attack）是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为与对方直接对话，但事实上整个会话都被攻击者完全控制。在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容。

如图10-4所示，是中间人攻击的一个场景。攻击者主动向UserA发送伪造UserB的ARP报文，导致UserA的ARP表中记录了错误的UserB地址映射关系，攻击者可以轻易获取到UserA原本要发往UserB的数据；同样，攻击者也可以轻易获取到UserB原本要发往UserA的数据。这样，UserA与UserB间的信息安全无法得到保障。

图 10-4 中间人攻击



为了防御中间人攻击，可以在 Switch 上部署动态 ARP 检测 DAI（Dynamic ARP Inspection）功能。

动态 ARP 检测是利用绑定表来防御中间人攻击的。当设备收到 ARP 报文时，将此 ARP 报文对应的源 IP、源 MAC、VLAN 以及接口信息和绑定表的信息进行比较，如果信息匹配，说明发送该 ARP 报文的用户是合法用户，允许此用户的 ARP 报文通过，否则就认为是攻击，丢弃该 ARP 报文。

说明

CE5880EI、CE6881、CE6881K、CE6820、CE6863、CE6863K、CE6881E 和 CE6880EI 不支持此功能。

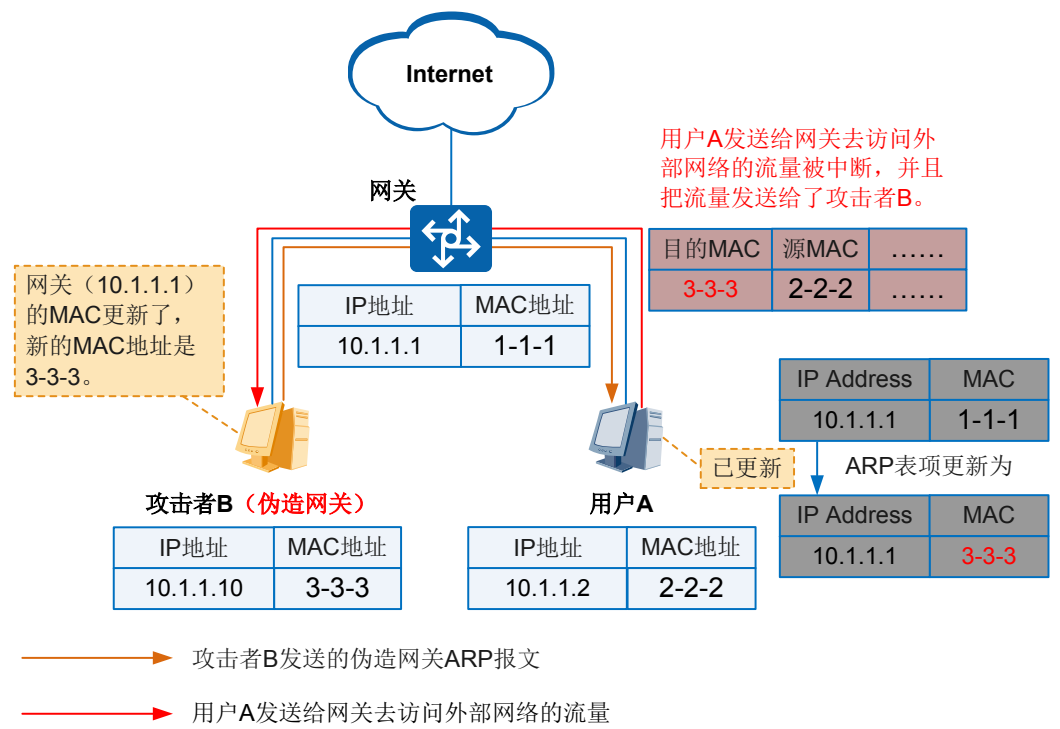
动态 ARP 检测功能仅适用于 DHCP Snooping 场景。设备使能 DHCP Snooping 功能后，当 DHCP 用户上线时，设备会自动生成 DHCP Snooping 绑定表；对于静态配置 IP 地址的用户，设备不会生成 DHCP Snooping 绑定表，所以需要手动添加静态绑定表。关于 DHCP Snooping 的详细介绍，请参见 [DHCP Snooping 的基本原理](#) 中的描述。

当 Switch 上部署动态 ARP 检测功能后，如果攻击者连接到 Switch 并试图发送伪造的 ARP 报文，Switch 会根据绑定表检测到这种攻击行为，对该 ARP 报文进行丢弃处理。

10.2.9 ARP 防网关冲突

如图 10-5 所示，攻击者 B 将伪造网关的 ARP 报文发送给用户 A，使用户 A 误以为攻击者即为网关。用户 A 的 ARP 表中会记录错误的网关地址映射关系，使得用户 A 跟网关的正常数据通信中断。

图 10-5 ARP 网关冲突



为了防范攻击者仿冒网关, 当用户主机直接接入网关时, 可以在网关设备上使能ARP防网关冲突攻击功能。当同时满足如下条件:

- 收到报文的接口是VLANIF接口或VBDIF接口
- 收到的报文的源IP地址与报文入接口的IP地址相同
- 收到的报文的以太网报文头的源MAC以及ARP报文内的源MAC都与接口MAC不同
- 收到的报文源MAC地址不是VRRP虚MAC

说明

一个VRRP备份组, 被当作一个共享局域网内主机的缺省网关, 即虚拟交换机。一个虚拟交换机拥有一个VRRP虚MAC, VRRP虚MAC根据虚拟交换机ID生成, 格式为: 00-00-5E-00-01-{VRID}(VRRP)。当虚拟交换机回应ARP请求时, 使用的是VRRP虚MAC地址, 而不是接口的真实MAC地址。

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 (虚MAC场景不生成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或者同BD的同源MAC地址的报文, 这样可以防止与网关地址冲突的ARP报文在VLAN内或者BD内广播。

10.2.10 ARP 报文内 MAC 地址一致性检查

ARP报文内MAC地址一致性检查功能主要应用于网关设备上, 可以防御以太网数据帧首部中的源/目的MAC地址和ARP报文中的源/目的MAC地址不同的ARP攻击。

部署本功能后, 网关设备在进行ARP学习前将对ARP报文进行检查。如果以太网数据帧首部中的源/目的MAC地址和ARP报文中的源/目的MAC地址不同, 则认为是攻击报文, 将其丢弃; 否则, 继续进行ARP学习。

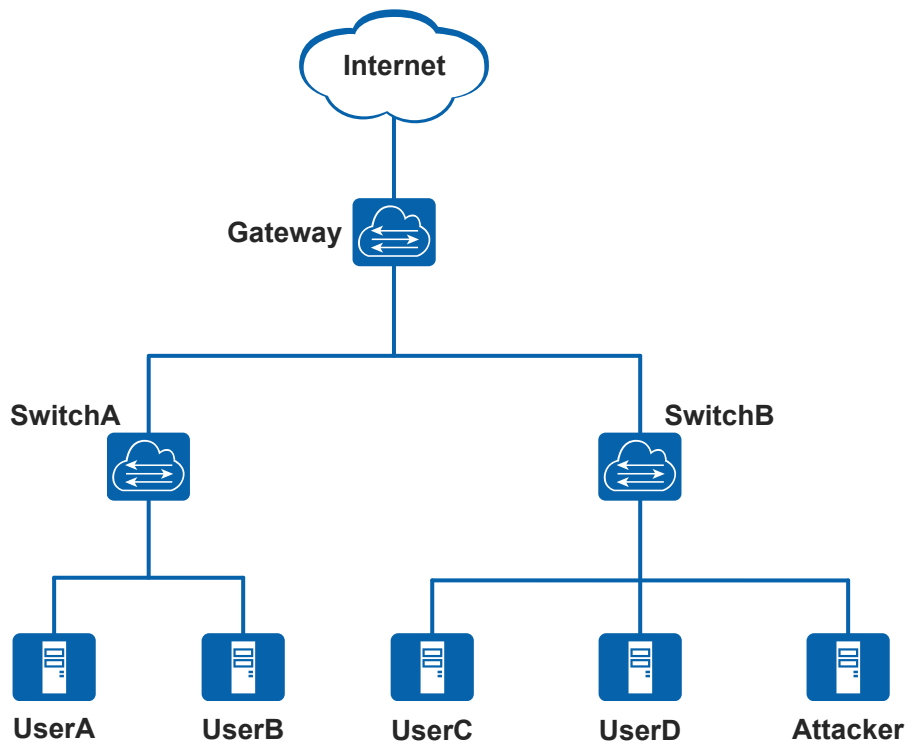
10.3 ARP 安全应用场景

介绍ARP安全的应用场景。

10.3.1 防 ARP 泛洪攻击

如图10-6所示，局域网中用户通过SwitchA和SwitchB接入连接到Gateway访问Internet。当网络中出现过多的ARP报文时，会导致网关设备CPU负载加重，影响设备正常处理用户的其它业务。另一方面，网络中过多的ARP报文会占用大量的网络带宽，引起网络堵塞，从而影响整个网络通信的正常运行。

图 10-6 防 ARP 泛洪攻击组网



为了避免上述危害，可以在网关设备上部署防ARP泛洪攻击功能，包括ARP报文限速功能、ARP Miss消息限速功能、免费ARP报文主动丢弃功能、ARP表项严格学习功能以及ARP表项限制功能。

- 部署**ARP报文限速**功能后，Gateway会对收到的ARP报文进行数量统计，如果在一定时间内，ARP报文的数量超出了配置的阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文，这样可以防止设备因处理大量ARP报文造成CPU负荷过重。
- 部署**ARP Miss消息限速**功能后，Gateway会对ARP Miss消息进行数量统计，如果在一定时间内，ARP Miss消息的数量超出了配置的阈值（ARP Miss消息限速值），则超出部分的ARP Miss消息将被忽略，且Gateway会丢弃触发ARP Miss消息的IP报文，这样可以防止Gateway因处理大量目标IP地址不能解析的IP报文造成CPU负荷过重。

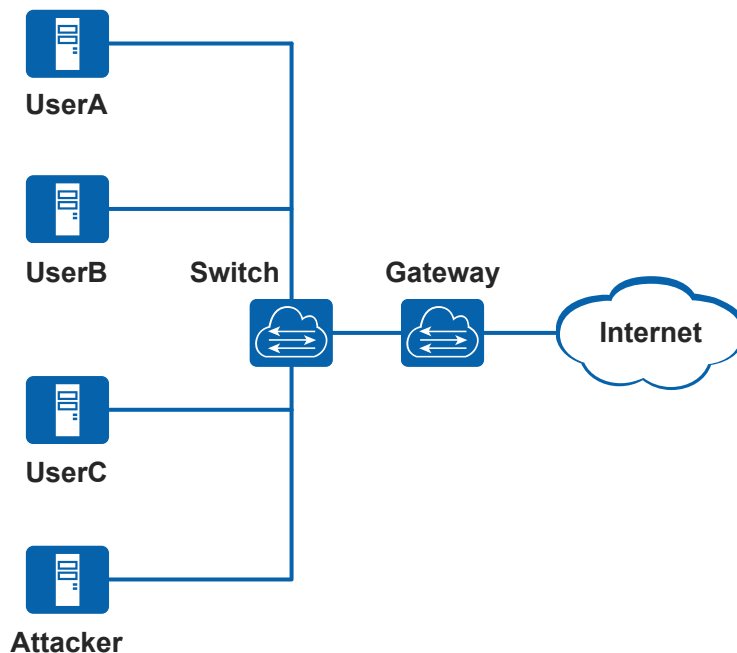
- 部署**免费ARP报文主动丢弃**功能后，Gateway直接丢弃免费ARP报文，这样可以降低CPU的负担。
- 部署**ARP表项严格学习**功能后，Gateway仅仅学习自己发送的ARP请求报文的应答报文，并不学习其它设备主动向Gateway发送的ARP报文，这样可以防止Gateway因学习大量ARP报文而导致ARP表项资源被无效的ARP条目耗尽。
- 部署**ARP表项限制**功能后，Gateway会对各个接口学习动态ARP表项的数目进行限制。当指定接口下的动态ARP表项达到允许学习的最大数目后，将不允许新增动态ARP表项，这样可以防止一个接口所接入的某一用户主机发起ARP攻击而导致整个设备的ARP表资源都被耗尽。

10.3.2 防 ARP 欺骗攻击

如**图10-7**所示，局域网中UserA、UserB、UserC等用户通过Switch接入连接到Gateway访问Internet。

正常情况下，UserA、UserB、UserC上线之后，通过相互之间交互ARP报文，UserA、UserB、UserC和Gateway上都会创建相应的ARP表项。此时，如果有攻击者通过在广播域内发送伪造的ARP报文，篡改Gateway或者UserA、UserB、UserC上的ARP表项，攻击者可以轻而易举地窃取UserA、UserB、UserC的信息或者阻碍UserA、UserB、UserC正常访问网络。

图 10-7 防 ARP 欺骗攻击组网



为了避免上述危害，可以在网关设备上部署防ARP欺骗攻击功能，包括ARP表项固化功能、免费ARP报文主动丢弃功能、ARP表项严格学习功能等功能。

- 部署**ARP表项固化**功能后，Gateway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，或者通过发送单播ARP请求报文的方式对更新ARP条目的报文进行合法性确认，这样可以防止攻击者伪造ARP报文修改网关上其他用户的ARP表项。

- 部署**免费ARP报文主动丢弃**功能后，Gateway直接丢弃免费ARP报文，这样可以防止伪造的免费ARP报文修改网关上其他用户的ARP表项，导致合法用户的通信流量发生中断。
- 部署**ARP表项严格学习**功能后，Gateway仅仅学习自己向UserA、UserB或UserC发送的ARP请求报文的应答报文，不学习攻击者主动向Gateway发送的ARP报文，并且不允许攻击者主动发送的ARP报文更新Gateway上现有的ARP条目，这样可以防止攻击者冒充其他用户修改网关上对应的ARP表项。

10.4 ARP 安全配置注意事项

介绍配置ARP安全的注意事项。

涉及网元

无需其他网元配合。

License 支持

ARP安全特性属于交换机基础功能，其受基本软件功能License控制。基本软件功能License在设备出厂时已经内置并激活，不需要用户再手动激活。

版本支持

表 10-4 支持本特性的最低软件版本

产品	最低支持版本
CE8860EI	V100R006C00
CE8861EI	V200R005C10
CE8868EI	V200R005C10
CE8850-32CQ-EI	V200R002C50
CE8850-64CQ-EI	V200R005C00
CE7850EI	V100R003C00
CE7855EI	V200R001C00
CE6810EI	V100R003C00
CE6810-48S4Q-LI/CE6810-48S-LI	V100R003C10
CE6810-32T16S4Q-LI/CE6810-24S2Q-LI	V100R005C10
CE6850EI	V100R001C00
CE6850-48S6Q-HI	V100R005C00
CE6850-48T6Q-HI/CE6850U-HI/CE6851HI	V100R005C10

产品	最低支持版本
CE6855HI	V200R001C00
CE6856HI	V200R002C50
CE6857EI	V200R005C10
CE6860EI	V200R002C50
CE6865EI	V200R005C00
CE6870-24S6CQ-EI/CE6870-48S6CQ-EI	V200R001C00
CE6870-48T6CQ-EI	V200R002C50
CE6875EI	V200R003C00
CE6880EI	V200R002C50
CE6881/CE6863	V200R005C20
CE6820	V200R005C20
CE6881K/CE6881E/CE6863K	V200R019C10
CE5810EI	V100R002C00
CE5850EI	V100R001C00
CE5850HI	V100R003C00
CE5855EI	V100R005C10
CE5880EI	V200R005C10

说明

如果需要了解软件版本与交换机具体型号的配套信息，请查看[硬件查询工具](#)。

软件版本演进关系：

- 除CE6881、CE6881E、CE6881K、CE6863、CE6863K、CE6820
V100R001C00 -> V100R002C00 -> V100R003C00 -> V100R003C10 -> V100R005C00 ->
V100R005C10 -> V100R006C00 -> V200R001C00 -> V200R002C50 -> V200R003C00 ->
V200R005C00 -> V200R005C10 -> V200R019C00 -> V200R019C10
- 对于CE6881、CE6881E、CE6881K、CE6863、CE6863K、CE6820
V200R005C20 -> V200R019C10 -> V200R020C00

特性依赖和限制

在交换机上部署ARP安全时，需要注意：

- 一般在用户侧的接口下配置免费ARP报文主动丢弃功能。
- 禁止接口下的动态ARP学习能力，可能会造成转发不通，用户配置时需要注意。
- 禁止ARP学习前，如果接口上已经有动态学习到的ARP表项，系统并不会自动删除这些表项。用户可以根据需要，手动删除或保留这些已经学习到的动态ARP表项。

- 当在VLAN下同时使能DAI和VLAN内协议报文透传功能时，VLAN内协议报文透传功能不生效。
- 对于除CE6870EI和CE6875EI之外的交换机，当在接口下配置ARP限速，同时vlan下配置DAI时，则ARP限速不生效。
- 对于除CE6870EI和CE6875EI之外的交换机，当在跨板LAG下配置ARP限速时，如果LAG下的不同单板上接口发送的ARP报文加起来达到限速值，而单个单板上没达到限速值，则ARP限速不生效。
- 除CE5880EI、CE6870EI、CE6875EI、CE6881、CE6881K、CE6820、CE6863、CE6863K、CE6881E和CE6880EI之外，如果设备同时配置了接口ARP限速和sFlow/NetStream功能，则接口ARP限速不准确。当接口ARP报文很多时，接口上送CPU的ARP报文数为配置的ARP限速值与sFlow/NetStream采样到的ARP报文数之和。
- 当CE6810LI作为Leaf设备时，不能在Leaf设备的接口上配置基于所有接口的ARP报文限速功能。
- 配置了基于所有接口的ARP报文限速功能后，基于端口的ARP本机自动防攻击功能不生效。

10.5 ARP 安全缺省配置

介绍设备的ARP安全缺省配置，实际应用的配置可以基于缺省配置进行修改。

ARP安全的缺省配置如表10-5所示。

表 10-5 ARP 安全缺省配置

参数	缺省值
ARP报文限速（根据源MAC地址）	对每一个源MAC地址的ARP报文速率限制为0，即不根据源MAC地址进行ARP报文限速
ARP报文限速（根据源IP地址）	设备允许1秒内最多只能有30个同一个源IP地址的ARP报文通过
ARP报文限速（根据目的IP地址）	对每一个目的IP地址的ARP报文速率限制为500，即设备在1秒内最多允许同一个目的IP地址的500个ARP报文通过
ARP报文限速（针对全局、VLAN和接口）	<ul style="list-style-type: none"> • 全局：128pps • VLAN和接口：未使能 说明 CE6870EI和CE6875EI不支持在接口视图配置ARP报文限速。
ARP Miss消息限速（根据源IP地址）	允许每秒最多处理同一个源IP地址触发的30个ARP Miss消息
ARP Miss消息限速（针对全局、VLAN和接口）	<ul style="list-style-type: none"> • 全局：在1秒内设备最多允许处理3000个ARP Miss消息 • VLAN和接口：未使能

参数	缺省值
临时ARP表项的老化时间	5秒
免费ARP报文主动丢弃功能	未使能
ARP表项严格学习功能	未使能
基于接口的ARP表项限制	在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制
ARP表项固化功能	未使能
动态ARP检测功能	未使能
ARP报文内MAC地址一致性检查功能	未使能

10.6 配置防 ARP 泛洪攻击

通过配置防ARP泛洪攻击功能，可以避免ARP泛洪攻击带来的ARP表项资源被无效ARP条目耗尽、CPU负荷过重造成用户无法正常通信等危害。

前置任务

在配置防ARP泛洪攻击之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

配置流程

在配置防ARP泛洪攻击任务中，各配置步骤均是并列关系，无严格配置顺序，用户根据需要选择配置即可。

说明

当针对全局、VLAN的ARP报文限速以及根据源MAC地址、源IP地址进行ARP报文限速中的多个限速功能同时配置时，设备对同时满足这些限速条件的ARP报文以其中最小的限速值进行限速。

当针对全局、VLAN的ARP Miss消息限速以及根据源IP地址进行ARP Miss消息限速中的多个限速功能同时配置时，设备对同时满足这些限速条件的ARP Miss消息以其中最小的限速值进行限速。

10.6.1 配置 ARP 报文限速（根据源 MAC 地址）

背景信息

设备处理大量源MAC地址相对固定的ARP报文会造成CPU繁忙，并且如果ARP报文的源IP地址同时不断变化，还会导致设备的ARP表资源被耗尽。

为了避免此问题，可以在网关设备上配置设备根据源MAC地址进行ARP报文限速。设备会对上送CPU的ARP报文根据源MAC地址进行统计，如果在1秒内收到的同一个源MAC地址的ARP报文超过设定阈值（ARP报文限速值），设备则丢弃超出阈值部分的ARP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置根据源MAC地址进行ARP报文限速

- 执行命令**arp anti-attack rate-limit source-mac maximum maximum**，配置根据任意源MAC地址进行ARP报文限速的限速值。
- 执行命令**arp anti-attack rate-limit source-mac mac-address maximum maximum**，配置对指定MAC地址用户的ARP报文进行限速的限速值。

两种配置同时存在的条件下，当ARP报文源MAC地址匹配限速指定的MAC地址时，对该源MAC地址的ARP报文限速值为后一步骤中配置的**maximum**值；否则为前一步骤中配置的**maximum**值。

缺省情况下，设备对每一个源MAC地址的ARP报文速率限制为0，即不根据源MAC地址进行ARP报文限速。

步骤3 执行命令**commit**，提交配置。

----结束

10.6.2 配置 ARP 报文限速（根据源 IP 地址）

背景信息

设备处理大量源IP地址相对固定的ARP报文（例如同一个源IP地址的ARP报文对应的MAC地址或出接口信息不断发生跳变），会造成CPU繁忙，影响到正常业务的处理。

为了避免此问题，可以在网关设备上配置设备根据源IP地址进行ARP报文限速。设备会对上送CPU的ARP报文根据源IP地址进行统计，如果在1秒内收到的同一个源IP地址的ARP报文超过设定阈值（ARP报文限速值），设备则丢弃超出阈值部分的ARP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置根据源IP地址进行ARP报文限速

- 执行命令**arp anti-attack rate-limit source-ip maximum maximum**，配置根据任意源IP地址进行ARP报文限速的限速值。
- 执行命令**arp anti-attack rate-limit source-ip ip-address maximum maximum**，配置对指定IP地址用户的ARP报文进行限速的限速值。

两种配置同时存在的条件下，当ARP报文源IP地址匹配限速指定的IP地址时，对该源IP地址的ARP报文限速值为后一步骤中配置的**maximum**值；否则为前一步骤中配置的**maximum**值。

缺省情况下，设备允许1秒内最多只能有同一个源IP地址的30个ARP报文通过。

步骤3 执行命令**commit**，提交配置。

----结束

10.6.3 配置 ARP 报文限速（根据目的 IP 地址）

背景信息

如果设备需要处理大量目的IP地址相同的ARP报文，则会造成CPU进程繁忙，影响到正常业务的处理。

为了避免此问题，可以配置设备根据目的IP地址进行ARP报文限速。设备会对上送CPU的ARP报文根据目的IP地址进行统计，如果在1秒内收到的同一个目的IP地址的ARP报文超过设定阈值（ARP报文限速值），设备则丢弃超出阈值部分的ARP报文。

操作步骤

步骤1 执行命令`system-view`，进入系统视图。

步骤2 执行命令`arp anti-attack rate-limit destination-ip maximum maximum`，配置根据目的IP地址进行ARP报文限速的限速值。

缺省情况下，设备对每一个目的IP地址的ARP报文速率限制为500，即设备在1秒内最多允许同一个目的IP地址的500个ARP报文通过。

步骤3 执行命令`commit`，提交配置。

----结束

10.6.4 配置 ARP 报文限速（针对全局、VLAN 和接口）

背景信息

说明

CE6870EI和CE6875EI不支持在接口视图下配置ARP报文限速。

如果设备对收到的大量ARP报文全部进行处理，可能导致CPU负荷过重而无法处理其他业务。因此，在处理之前，设备需要对ARP报文进行限速，以保护CPU资源。

使能ARP报文限速功能后，可以在全局、VLAN或接口下配置ARP报文的限速值。如果每秒收到的ARP报文数目超过ARP报文限速值，设备会丢弃超出限速值的ARP报文。

- 针对全局的ARP报文限速：在设备出现ARP攻击时，限制全局处理的ARP报文数量。
- 针对VLAN的ARP报文限速：在某个VLAN内的所有接口出现ARP攻击时，限制处理收到的该VLAN内的ARP报文数量，配置本功能可以保证不影响其他VLAN内所有接口的ARP学习。
- 针对接口的ARP报文限速：在某个接口出现ARP攻击时，限制处理该接口收到的ARP报文数量，配置本功能可以保证不影响其他接口的ARP学习。

当同时在全局、VLAN和接口下配置ARP报文的限速值时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

说明

在SVF中，不支持在LI Leaf端口上配置基于接口的ARP报文限速功能。

建议在网关设备上进行如下配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**interface interface-type interface-number**，进入接口视图；或执行命令**vlan vlan-id**，进入VLAN视图。

在系统视图下配置ARP报文限速功能无需执行此步骤。

步骤3 执行命令**arp anti-attack rate-limit limit**，配置ARP报文的限速值。

缺省情况下，CE5800系列交换机（除CE5880EI外）对全局的ARP报文速率限制为128pps，即在1秒内设备最多允许128个ARP报文通过，其余设备对全局的ARP报文速率限制为0，即不针对全局进行ARP报文限速；设备对VLAN或接口的ARP报文速率限制为0，即不针对VLAN和接口进行ARP报文限速。

步骤4 执行命令**commit**，提交配置。

----结束

10.6.5 配置 ARP 报文限速（针对所有接口）

背景信息

如果设备对收到的大量ARP报文全部进行处理，可能导致CPU负荷过重而无法处理其他业务。因此，在处理之前，设备需要对ARP报文进行限速，以保护CPU资源。

使能ARP报文限速功能后，可以在系统视图下执行**arp anti-attack rate-limit interface**命令，配置设备上所有接口的ARP报文的限速值。如果某接口每秒收到的ARP报文数目超过ARP报文限速值，设备会丢弃超出限速值的ARP报文。

如果系统视图下配置了**arp anti-attack rate-limit**命令，表示设备上所有接口的ARP报文数量总和的上限为该命令所配置的ARP报文限速值；如果系统视图下配置了**arp anti-attack rate-limit interface**命令，表示所有接口的ARP报文数量的上限均为该命令所配置的ARP报文限速值。

说明

- 当CE6810LI作为Leaf设备时，不支持在Leaf设备的接口上配置基于所有接口的ARP报文限速功能。
- CE6870EI和CE6875EI不支持配置基于所有接口的ARP报文限速功能。
- 配置了基于所有接口的ARP报文限速功能后，基于端口的ARP本机自动机防攻击功能不生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp anti-attack rate-limit interface limit**，配置ARP报文的限速值。

缺省情况下，对所有接口的ARP报文速率限制为0，即不针对所有接口进行ARP报文限速。

步骤3 执行命令**commit**，提交配置。

----结束

10.6.6 配置 ARP Miss 消息限速（根据源 IP 地址）

背景信息

如果网络中有用户向设备发送大量目标IP地址不能解析的IP报文（即路由表中存在该IP报文的源IP对应的路由表项，但设备上没有该路由表项中下一跳对应的ARP表项），将导致设备触发大量的ARP Miss消息。这种触发ARP Miss消息的IP报文会被上送到设备进行处理，设备会根据ARP Miss消息生成和下发大量临时ARP表项并向目的网络发送大量ARP请求报文，这样就增加了设备CPU的负担，同时严重消耗目的网络的带宽资源。

当设备检测到某一源IP地址的IP报文在1秒内触发的ARP Miss消息数量超过了限速值，就认为此源IP地址存在攻击。

管理员可以根据实际网络环境，对ARP Miss消息的限速值进行调整，限制设备在一定时间内只处理指定数目的ARP Miss消息，避免设备的资源浪费在处理ARP Miss消息上，保证用户的其他业务能够正常运行。

建议在网关设备上进行如下配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置根据源IP地址进行ARP Miss消息限速

- 执行命令**arp miss anti-attack rate-limit source-ip maximum *maximum***，配置根据源IP地址进行ARP Miss消息限速的限速值。
- 执行命令**arp miss anti-attack rate-limit source-ip *ip-address* [mask { *mask-length* | *mask* }] maximum *maximum***，配置对指定IP地址用户的ARP Miss消息进行限速的限速值。

两种配置同时存在的条件下，当触发ARP Miss消息的IP报文的源IP地址匹配限速指定的IP地址时，对该源IP地址的IP报文触发的ARP Miss消息限速值为后一步骤中配置的*maximum*值；否则为前一步骤中配置的*maximum*值。

如果将限速值配置为0，则表示不根据源IP地址进行ARP Miss消息限速。缺省情况下，设备允许每秒最多处理同一个源IP地址触发的30个ARP Miss消息。

步骤3 执行命令**commit**，提交配置。

----结束

10.6.7 配置 ARP Miss 消息限速（针对全局、VLAN 和接口）

背景信息

如果网络中有用户向设备发送大量目标IP地址不能解析的IP报文（即路由表中存在该IP报文的源IP对应的路由表项，但设备上没有该路由表项中下一跳对应的ARP表项），将导致设备触发大量的ARP Miss消息。这种触发ARP Miss消息的IP报文会被上送到设备进行处理，设备会根据ARP Miss消息生成和下发大量临时ARP表项并向目的网络发送大量ARP请求报文，这样就增加了设备CPU的负担，同时严重消耗目的网络的带宽资源。

为了避免这种IP报文攻击所带来的危害，建议在网关设备上配置ARP Miss消息限速功能。

- 针对全局的ARP Miss消息限速：在设备出现目标IP地址不能解析的IP报文攻击时，限制全局处理的ARP Miss消息数量。
- 针对VLAN的ARP Miss消息限速：在某个VLAN内的所有接口出现目标IP地址不能解析的IP报文攻击时，限制处理该VLAN内报文触发的ARP Miss消息数量，配置本功能可以保证不影响其他VLAN内所有接口的IP报文转发。
- 针对接口的ARP Miss消息限速：在某个接口出现目标IP地址不能解析的IP报文攻击时，限制处理该接口收到的报文触发的ARP Miss消息数量，配置本功能可以保证不影响其他接口的IP报文转发。

当同时在全局、VLAN或接口下配置ARP Miss消息限速时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**interface interface-type interface-number**，进入二层接口视图，然后执行命令**undo portswitch**，进入三层接口视图；或执行命令**vlan vlan-id**，进入VLAN视图。

说明

在系统视图下配置ARP Miss消息限速功能无需执行此步骤。

步骤3 执行命令**arp miss anti-attack rate-limit limit**，配置ARP Miss消息的限速值。

缺省情况下，针对全局，设备在1秒内最多允许处理3000个ARP Miss消息；针对VLAN或接口，设备在1秒内处理0个ARP Miss消息，即设备上未使能ARP Miss消息限速功能。

步骤4 执行命令**commit**，提交配置。

----结束

10.6.8 配置临时 ARP 表项的老化时间

背景信息

当IP报文触发ARP Miss消息时，设备会根据ARP Miss消息生成临时ARP表项，并且向目的网段发送ARP请求报文。

- 在临时ARP表项老化时间范围内：
 - 设备收到ARP应答报文前，匹配临时ARP表项的IP报文将被丢弃并且不会触发ARP Miss消息。
 - 设备收到ARP应答报文后，则生成正确的ARP表项来替换临时ARP表项。
- 当老化时间超时后，设备会清除临时ARP表项。此时如果设备转发IP报文匹配不到对应的ARP表项，则会重新触发ARP Miss消息并生成临时ARP表项，如此循环重复。

故可以通过配置临时ARP表项的老化时间来控制ARP Miss消息的触发频率。当判断设备受到攻击时，可以调大该时间，减小设备ARP Miss消息的触发频率，从而减小攻击对设备的影响。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface interface-type interface-number**，进入接口视图。

步骤3 （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

步骤4 执行命令**arp fake timeout 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5秒。

步骤5 执行命令**commit**，提交配置。

----结束

10.6.9 配置免费 ARP 报文主动丢弃

背景信息

由于发送免费ARP报文的用户主机并不需要经过身份验证，任何一个用户主机都可以发送免费ARP报文，这样就引入了两个问题：

- 如果网络中出现大量的免费ARP报文，设备会因为处理这些报文而导致CPU负荷过重，从而不能正常处理合法的ARP报文。
- 如果设备处理的免费ARP报文是攻击者伪造的，会造成设备错误地更新ARP表项，导致合法用户的通信流量发生中断。

参考以上问题描述，在确认攻击来自免费ARP报文之后，可以在网关设备上使能免费ARP报文主动丢弃功能，使网关设备直接丢弃免费ARP报文。

丢弃免费ARP报文功能可以在全局和接口下使能。

- 全局使能该功能，则设备的所有接口都丢弃收到的免费ARP报文。
- 接口下使能该功能，则只有该接口丢弃收到的免费ARP报文。

说明

一般在用户侧的接口下配置免费ARP报文主动丢弃功能。


操作步骤

- 全局使能免费ARP报文主动丢弃功能

- a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**arp anti-attack gratuitous-arp drop**，使能免费ARP报文主动丢弃功能。

缺省情况下，未使能免费ARP报文主动丢弃功能。
 - c. 执行命令**commit**，提交配置。
 - 接口使能免费ARP报文主动丢弃功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。
-  **说明**
- 如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } &<1-10>**，批量切换以太网接口的工作模式。
- d. 执行命令**arp anti-attack gratuitous-arp drop**，使能免费ARP报文主动丢弃功能。

缺省情况下，未使能免费ARP报文主动丢弃功能。
- e. 执行命令**commit**，提交配置。

----结束

10.6.10 配置 ARP 表项严格学习

背景信息

如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成如下危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备ARP表项，导致合法用户无法正常通信。

为避免上述危害，可以在网关设备上配置ARP表项严格学习功能。配置该功能后，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，这样，可以拒绝大部分的ARP报文攻击。

ARP表项严格学习功能可在全局和接口视图下进行配置。

- 全局使能该功能，则设备的所有接口均进行ARP表项严格学习。

- 接口视图下使能该功能，则只有该接口进行ARP表项严格学习。

当同时在全局和接口视图下进行配置时，接口下配置的优先级高于全局配置的优先级。

说明

在全局使能ARP表项严格学习功能的前提下：

- 如果在指定接口下执行命令**arp learning strict force-disable**，则该接口将会被强制执行去使能ARP表项严格学习的功能。
- 如果在指定接口下执行命令**arp learning strict trust**时，则该接口的ARP表项严格学习功能和全局的配置保持一致。

操作步骤

- 配置全局ARP表项严格学习功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**arp learning strict**，配置全局ARP表项严格学习功能。

缺省情况下，未使能ARP表项严格学习功能。

- c. 执行命令**commit**，提交配置。

- 配置接口的ARP表项严格学习功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

- d. 执行命令**arp learning strict { force-enable | force-disable | trust }**，配置接口的ARP表项严格学习功能。

缺省情况下，未使能ARP表项严格学习功能。

- e. 执行命令**commit**，提交配置。

----结束

10.6.11 配置基于接口的 ARP 表项限制

背景信息

为了防止当一个接口所接入的某一用户主机发起ARP攻击时导致整个设备的ARP表资源都被耗尽，可以在指定接口下配置接口能够学习到的最大动态ARP表项数目。当指定接口下的动态ARP表项达到允许学习的最大数目后，将不允许新增动态ARP表项。

建议在网关设备上进行如下配置。

操作步骤

- 配置二层接口的ARP表项限制
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. 执行命令**arp limit vlan vlan-id1 [to vlan-id2] maximum**，配置基于二层接口的ARP表项限制。

缺省情况下，在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制。

- d. 执行命令**commit**，提交配置。
- 配置三层接口的ARP表项限制
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

- d. 执行命令**arp limit maximum**，配置基于三层接口的ARP表项限制。

缺省情况下，在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制。

- e. 执行命令**commit**，提交配置。

----结束

后续处理

当在VBDIF接口上配置了ARP表项限制后，可以在VBDIF接口上配置**arp limit alarm-threshold**命令进一步设置告警阈值，当VBDIF接口学习到的ARP表项达到设置的告警阈值时，设备会发送告警，提醒用户及时介入，删除多余的动态ARP表项。

说明

仅CE5880EI、CE6850HI、CE6850U-HI、CE6851HI、CE6855HI、CE6856HI、CE6857EI、CE6860EI、CE6865EI、CE6870EI、CE6875EI、CE6880EI、CE6881、CE6881K、CE6863、CE6863K、CE6881E、CE7850EI、CE7855EI、CE8850EI、CE8861EI、CE8868EI和CE8860EI设备支持配置**arp limit alarm-threshold**命令。

10.6.12 配置禁止接口学习 ARP 表项

背景信息

当某接口下出现大量动态ARP表项时，出于安全考虑建议在网关设备上配置禁止该接口学习ARP表项的功能，以防止该接口下所接入的用户主机发起ARP攻击使整个设备的ARP表资源都被耗尽。

禁止ARP学习前，如果接口上已经有动态学习到的ARP表项，系统并不会自动删除这些表项。用户可以根据需要，手动删除或保留这些已经学习到的动态ARP表项。

须知

禁止接口下的动态ARP学习能力，可能会造成转发不通，用户配置时需要注意。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface interface-type interface-number**，进入接口视图。

步骤3 （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] }** &<1-10>，批量切换以太网接口的工作模式。

步骤4 执行命令**arp learning disable**，禁止接口学习动态ARP表项。

缺省情况下，接口下的动态ARP表项学习功能处于使能状态。

步骤5 执行命令**commit**，提交配置。

----结束

10.6.13 检查配置结果

操作步骤

- 使用命令**display arp anti-attack { rate-limit | entry-check }**，查看ARP防攻击配置。
- 使用命令**display arp miss anti-attack rate-limit**，查看ARP Miss防攻击配置。
- 使用命令**display arp limit [interface interface-type interface-number] [vlan vlan-id]**，查看接口可以学习到的动态ARP表项数目的最大值。
- 使用命令**display arp learning strict**，查看全局和所有接口上的ARP表项严格学习情况。

----结束

10.7 配置防 ARP 欺骗攻击

通过配置防ARP欺骗攻击功能，可以防止伪造的ARP报文恶意修改设备或网络内其他用户主机的ARP表项，造成网络中的报文转发异常。

前置任务

在配置防ARP欺骗攻击之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

配置流程

在配置防ARP欺骗攻击任务中，各配置步骤均是并列关系，无严格配置顺序，用户根据需要选择配置即可。

10.7.1 配置 ARP 表项固化

背景信息

为了防止ARP地址欺骗攻击，可以在网关设备上配置ARP表项固化功能。三种ARP表项固化模式适用于不同的应用场景，且是互斥关系。

- **fixed-mac**方式：设备收到的ARP报文中的MAC地址与ARP表中对应条目的MAC地址不匹配，则直接丢弃该ARP报文；如果匹配，但是收到报文的接口或VLAN信息与ARP表中对应条目不匹配，则可以更新对应ARP条目中的接口和VLAN信息。此方式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。当用户从不同接口接入设备时，设备上该用户对应的ARP表项中的接口信息可以及时更新。
- **fixed-all**方式：只有当ARP报文对应的MAC地址、接口、VLAN信息和ARP表项中的信息完全匹配时，设备才可以更新ARP表项的其他内容。此方式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
- **send-ack**方式：设备收到一个涉及MAC地址、VLAN、接口修改的ARP报文时，不会立即更新ARP表项，而是先向待更新的ARP表项现有MAC地址对应的用户发送一个单播的ARP请求报文进行确认，根据确认结果再决定是否更新ARP表项中的MAC地址、VLAN和接口信息。此方式适用于用户的MAC地址和接入位置均频繁变动的场景。

可在全局和接口下配置ARP表项固化功能。

- 全局配置该功能后，默认设备上所有接口的ARP表项固化功能均已使能。
- 当全局和接口下同时配置了该功能时，接口下的配置优先生效。

操作步骤

- 全局使能ARP表项固化功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**arp anti-attack entry-check { fixed-mac | fixed-all | send-ack } enable**，配置ARP表项固化功能。

缺省情况下，未配置ARP表项固化功能。

- c. 执行命令**commit**，提交配置。

- 接口使能ARP表项固化功能

- a. 执行命令**system-view**，进入系统视图。
- b. 执行命令**interface interface-type interface-number**，进入接口视图。
- c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } &<1-10>**，批量切换以太网接口的工作模式。

- d. 执行命令**arp anti-attack entry-check { fixed-mac | fixed-all | send-ack } enable**，配置ARP表项固化功能。

缺省情况下，未配置ARP表项固化功能。

- e. 执行命令**commit**，提交配置。

----结束

10.7.2 配置动态 ARP 检测

背景信息

为了防御中间人攻击，避免合法用户的数据被中间人窃取，可以在接入设备上使能动态ARP检测DAI功能。设备会将ARP报文对应的源IP、源MAC、接口和绑定表中的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

说明

- 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。DHCP Snooping的配置，请参见[13 DHCP Snooping配置](#)。静态绑定表的配置，请参见[14.4.1 配置绑定表](#)。
- 当在VLAN下同时使能DAI和VLAN内协议报文透传功能时，VLAN内协议报文透传功能不生效。
- CE5880EI、CE6881、CE6881K、CE6820、CE6863、CE6863K、CE6881E和CE6880EI不支持此功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan *vlan-id***，进入VLAN视图。

步骤3 执行命令**arp anti-attack check user-bind enable**，使能动态ARP检测功能（即对ARP报文进行绑定表匹配检查功能）。

缺省情况下，未使能动态ARP检测功能。

步骤4 （可选）执行命令**arp anti-attack check user-bind check-item { ip-address | mac-address | interface }***，配置对ARP报文进行绑定表匹配检查的检查项。

缺省情况下，对ARP报文的IP地址、MAC地址和接口信息都进行检查。

如果希望仅匹配绑定表某一项或某两项内容的特殊ARP报文也能够通过，则可以配置对ARP报文进行绑定表匹配检查时只检查某一项或某两项内容。

说明

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。

步骤5 执行命令**commit**，提交配置。

----结束

10.7.3 配置 ARP 防网关冲突

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，可以在网关设备上执行本命令使能ARP防网关冲突攻击功能。

如果未配置**check-all**参数，当同时满足如下条件：

- 收到报文的接口是VLANIF接口或VBDIF接口。
- 收到的报文的源IP地址与报文入接口的IP地址相同。
- 收到的报文的以太网报文头的源MAC以及ARP报文内的源MAC都与接口MAC不同。
- 收到的报文源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（虚MAC场景不生成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或

者同BD的同源MAC地址的报文，这样可以防止与网关地址冲突的ARP报文在VLAN内或者BD内广播。

当配置`check-all`参数，如果设备收到ARP报文的源IP地址和本机的IP地址相同，设备就认为该ARP报文是与网关地址冲突的ARP报文。

当配置`check-all`参数后，ARP防网关冲突攻击功能比不配置该参数时更强，此时当检测到网关被仿冒后，网关会产生告警，并立即发送免费ARP报文，使用户主机重新刷新正确的ARP表项。

操作步骤

步骤1 执行命令`system-view`，进入系统视图。

步骤2 执行命令`arp anti-attack gateway-duplicate [check-all] enable`，使能ARP防网关冲突攻击功能。

缺省情况下，未使能ARP防网关冲突攻击功能。

说明

仅CE6850HI、CE6850U-HI、CE6851HI、CE6855HI、CE6856HI、CE6857EI、CE6860EI、CE6865EI、CE6870EI、CE6875EI、CE7850EI、CE7855EI、CE8850EI、CE8861EI、CE8868EI和CE8860EI设备支持配置`check-all`参数。

----结束

后续处理

- 如果使能ARP防网关冲突攻击功能时未配置`check-all`参数，执行命令`display arp anti-attack gateway-duplicate item`查看ARP防网关冲突攻击表项。
- 如果使能ARP防网关冲突攻击功能时配置了`check-all`参数，执行命令`display arp anti-attack gateway-duplicate information`查看ARP防网关冲突攻击表项。

说明

仅CE6850HI、CE6850U-HI、CE6851HI、CE6855HI、CE6856HI、CE6857EI、CE6860EI、CE6865EI、CE6870EI、CE6875EI、CE7850EI、CE7855EI、CE8850EI、CE8861EI、CE8868EI和CE8860EI设备支持此命令。

10.7.4 配置免费 ARP 报文主动丢弃

背景信息

由于发送免费ARP报文的用户主机并不需要经过身份验证，任何一个用户主机都可以发送免费ARP报文，这样就引入了两个问题：

- 如果网络中出现大量的免费ARP报文，设备会因为处理这些报文而导致CPU负荷过重，从而不能正常处理合法的ARP报文。
- 如果设备处理的免费ARP报文是攻击者伪造的，会造成设备错误地更新ARP表项，导致合法用户的通信流量发生中断。

参考以上问题描述，在确认攻击来自免费ARP报文之后，可以在网关设备上使能免费ARP报文主动丢弃功能，使网关设备直接丢弃免费ARP报文。

丢弃免费ARP报文功能可以在全局和接口下使能。

- 全局使能该功能，则设备的所有接口都丢弃收到的免费ARP报文。
- 接口下使能该功能，则只有该接口丢弃收到的免费ARP报文。

说明

一般在用户侧的接口下配置免费ARP报文主动丢弃功能。

操作步骤

- 全局使能免费ARP报文主动丢弃功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**arp anti-attack gratuitous-arp drop**，使能免费ARP报文主动丢弃功能。

缺省情况下，未使能免费ARP报文主动丢弃功能。

- c. 执行命令**commit**，提交配置。
- 接口使能免费ARP报文主动丢弃功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

- d. 执行命令**arp anti-attack gratuitous-arp drop**，使能免费ARP报文主动丢弃功能。

缺省情况下，未使能免费ARP报文主动丢弃功能。

- e. 执行命令**commit**，提交配置。

----结束

10.7.5 配置发送 ARP 免费报文

背景信息

如果有攻击者向其他用户发送仿冒网关的ARP报文，会导致其他用户的ARP表中记录错误的网关地址映射关系，造成其他用户的正常数据不能被网关接收。此时可以在网关设备上配置发送免费ARP报文的功能，用来定期更新合法用户的ARP表项，使得合法用户ARP表项中记录的是正确的网关地址映射关系。

可在全局或接口下配置发送免费ARP报文功能。

- 全局配置该功能后，则默认设备上所有接口的发送ARP免费报文功能均已使能。
- 当全局和接口下同时配置了该功能时，接口下的配置优先生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 (可选)执行命令**interface interface-type interface-number**，进入接口视图。

说明

在系统视图下配置发送ARP免费报文功能无需执行此步骤。

步骤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，未使能发送免费ARP报文的功能。

步骤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，发送免费ARP报文的时间间隔为60秒。

步骤5 执行命令**commit**，提交配置。

----结束

10.7.6 配置 ARP 报文内 MAC 地址一致性检查

背景信息

ARP报文内MAC地址一致性检查功能主要应用于网关设备上，可以防御以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址不同的ARP攻击。

配置ARP报文内MAC地址一致性检查后，网关设备在进行ARP学习前将对ARP报文进行检查。如果以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址不同，则认为是攻击报文，将其丢弃；否则，继续进行ARP学习。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置ARP报文内MAC地址一致性检查

- 系统视图：

执行命令**arp validate source-mac**，全局使能ARP报文内MAC地址一致性检查功能，即对以太网数据帧首部中的源MAC地址和ARP报文数据区中的源MAC地址进行一致性检查的功能。

缺省情况下，设备不对以太网数据帧首部中的源MAC地址和ARP报文数据区中的源MAC地址进行一致性检查。

- 接口视图：

a. 执行命令**interface interface-type interface-number**，进入接口视图。

说明

只有当需要进入三层接口视图时，才需执行下一步操作。

- b. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

- c. 执行命令**arp validate { source-mac | destination-mac } ***，使能ARP报文内MAC地址一致性检查功能，即设备对以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址进行一致性检查的功能。

缺省情况下，设备不对以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址进行一致性检查。

说明

本命令不支持在VLANIF接口上配置。当VLANIF接口收到ARP报文时，ARP报文内MAC地址一致性检查遵循成员口下的检查规则。

步骤3 执行命令**commit**，提交配置。

----结束

10.7.7 配置 ARP 表项严格学习

背景信息

如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成如下危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备ARP表项，导致合法用户无法正常通信。

为避免上述危害，可以在网关设备上配置ARP表项严格学习功能。配置该功能后，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，这样，可以拒绝大部分的ARP报文攻击。

ARP表项严格学习功能可在全局和接口视图下进行配置。

- 全局使能该功能，则设备的所有接口均进行ARP表项严格学习。
- 接口视图下使能该功能，则只有该接口进行ARP表项严格学习。

当同时在全局和接口视图下进行配置时，接口下配置的优先级高于全局配置的优先级。

说明

在全局使能ARP表项严格学习功能的前提下：

- 如果在指定接口下执行命令**arp learning strict force-disable**，则该接口将会被强制执行去使能ARP表项严格学习的功能。
- 如果在指定接口下执行命令**arp learning strict trust**时，则该接口的ARP表项严格学习功能和全局的配置保持一致。

操作步骤

- 配置全局ARP表项严格学习功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**arp learning strict**，配置全局ARP表项严格学习功能。

缺省情况下，未使能ARP表项严格学习功能。
 - c. 执行命令**commit**，提交配置。
- 配置接口的ARP表项严格学习功能
 - a. 执行命令**system-view**，进入系统视图。
 - b. 执行命令**interface interface-type interface-number**，进入接口视图。
 - c. （对于以太网接口）执行命令**undo portswitch**，配置接口切换到三层模式。

缺省情况下，以太网接口处于二层模式。

使用该命令进行接口的二三层模式切换时，接口下只能存在属性配置信息（例如**shutdown**、**description**配置）或者二三层接口均支持的配置信息（例如**mode lacp**、**lacp system-id**配置），模式切换功能才可以生效。不能有任何切换后的接口模式不支持的配置存在。如果接口上存在不支持的配置，请先将这些配置全部清除，然后再执行**undo portswitch**命令。

说明

如果涉及的以太网接口较多，可以在系统视图下执行命令**undo portswitch batch interface-type { interface-number1 [to interface-number2] } <1-10>**，批量切换以太网接口的工作模式。

- d. 执行命令**arp learning strict { force-enable | force-disable | trust }**，配置接口的ARP表项严格学习功能。

缺省情况下，未使能ARP表项严格学习功能。

- e. 执行命令**commit**，提交配置。

----结束

10.7.8 检查配置结果

操作步骤

- 使用命令**display arp anti-attack { rate-limit | entry-check }**，查看ARP防攻击配置。

- 使用命令**display arp learning strict**，查看全局和所有接口上的ARP表项严格学习情况。

----结束

10.8 维护 ARP 安全

维护ARP安全包括监控ARP运行情况、清除ARP报文统计信息、清除ARP报文丢弃计数以及配置对潜在的ARP攻击行为发送日志和告警。

10.8.1 监控 ARP 安全运行情况

操作步骤

- 执行命令**display arp packet statistics [interface [*interface-type interface-number*]]**，查看ARP处理的报文统计数据。
- 执行命令**display arp anti-attack record**，查看由于ARP报文限速导致丢弃的ARP报文的详细信息。
- 执行命令**display arp miss anti-attack record**，查看由于ARP Miss消息限速导致丢弃的ARP Miss消息的详细信息。

----结束

10.8.2 清除 ARP 安全统计信息

背景信息

须知

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 执行命令**reset arp packet statistics [interface [*interface-type interface-number*]]**，清除ARP报文的统计信息。
- 执行命令**reset arp anti-attack record**，清除由于ARP报文限速导致丢弃的ARP报文的详细信息。
- 执行命令**reset arp miss anti-attack record**，清除由于ARP Miss消息限速导致丢弃的ARP Miss消息的详细信息。
- 执行命令**reset fei fake arp all**，清除临时ARP表项。

----结束

10.8.3 配置对潜在的 ARP 攻击行为发送告警

背景信息

在使能了ARP报文限速或者ARP Miss限速之后，在一定的时间内，如果设备收到的ARP报文或者ARP Miss消息超过了设定的阈值，超出部分的ARP报文或者ARP Miss消息将被丢弃。此时设备认为这是一种潜在的攻击行为，会针对这种攻击行为发送记录ARP日志并向网管系统发送ARP告警，实时记录ARP运行的异常情况。

为了避免网络在遭受ARP攻击时产生海量日志和告警，用户可以配置设备记录ARP日志和发送ARP告警的时间间隔，减少日志和告警的产生数量。

操作步骤

步骤1 执行命令`system-view`，进入系统视图。

步骤2 执行命令`arp anti-attack log-trap-timer time`，配置对潜在的ARP攻击行为记录ARP日志和发送告警的时间间隔。

缺省情况下，设备记录ARP日志和发送ARP告警时间间隔为0，即设备不记录ARP日志和不发送ARP告警信息。

步骤3 执行命令`commit`，提交配置。

----结束

10.9 ARP 安全配置举例

介绍ARP安全配置举例。配置示例中包括组网需求、配置思路、配置过程等。

本节仅列举单特性的配置示例。如果您想了解更多综合场景配置案例、特性典型配置案例、对接案例、替换案例及行业案例，请参考典型配置案例。

10.9.1 配置 ARP 安全综合功能示例

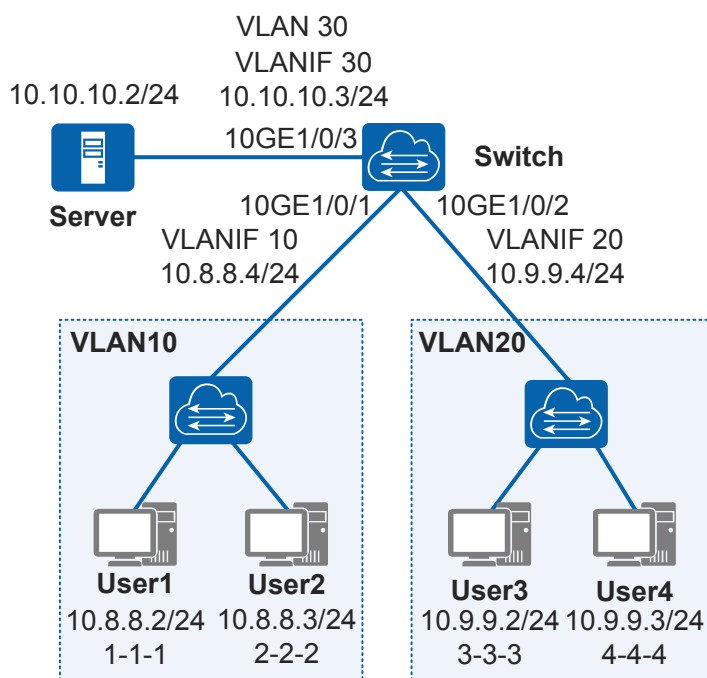
组网需求

如图10-8所示，Switch作为网关通过接口10GE1/0/3连接一台服务器，通过接口10GE1/0/1、10GE1/0/2连接VLAN10和VLAN20下的四个用户。网络中存在以下ARP威胁：

- 攻击者向Switch发送伪造的ARP报文、伪造的免费ARP报文进行ARP欺骗攻击，恶意修改Switch的ARP表项，造成其他用户无法正常接收数据报文。
- 攻击者发出大量目的IP地址不可达的IP报文进行ARP泛洪攻击，造成Switch的CPU负荷过重。
- 用户User1构造大量源IP地址变化MAC地址固定的ARP报文进行ARP泛洪攻击，造成Switch的ARP表资源被耗尽以及CPU进程繁忙，影响到正常业务的处理。
- 用户User3构造大量源IP地址固定的ARP报文进行ARP泛洪攻击，造成Switch的CPU进程繁忙，影响到正常业务的处理。

管理员希望能够防止上述ARP攻击行为，为用户提供更安全的网络环境和更稳定的网络服务。

图 10-8 配置 ARP 安全功能组网图



配置思路

采用如下思路在Switch上进行配置：

1. 配置ARP表项严格学习功能以及ARP表项固化功能，实现防止伪造的ARP报文错误地更新Switch的ARP表项。
2. 配置免费ARP报文主动丢弃功能，实现防止伪造的免费ARP报文错误地更新设备ARP表项。
3. 配置根据源IP地址进行ARP Miss消息限速，实现防止用户侧存在攻击者发出大量目的IP地址不可达的IP报文触发大量ARP Miss消息，形成ARP泛洪攻击。同时需要保证Switch可以正常处理服务器发出的大量此类报文，避免因丢弃服务器发出的大量此类报文而造成网络无法正常通信。
4. 配置基于接口的ARP表项限制以及根据源MAC地址进行ARP限速，实现防止User1发送的大量源IP地址变化MAC地址固定的ARP报文形成的ARP泛洪攻击，避免Switch的ARP表资源被耗尽，并避免CPU进程繁忙。
5. 配置根据源IP地址进行ARP限速，实现防止User3发送的大量源IP地址固定的ARP报文形成的ARP泛洪攻击，避免CPU进程繁忙。

操作步骤

步骤1 创建VLAN，将接口加入到VLAN中，并配置VLANIF接口

创建VLAN10、VLAN20和VLAN30，并将接口10GE1/0/1加入VLAN10中，接口10GE1/0/2加入VLAN20中，接口10GE1/0/3加入VLAN30中。

```
<HUAWEI> system-view
[~HUAWEI] sysname Switch
[*HUAWEI] commit
[~Switch] vlan batch 10 20 30
```

```
[*Switch] interface 10ge 1/0/1
[*Switch-10GE1/0/1] port link-type trunk
[*Switch-10GE1/0/1] port trunk allow-pass vlan 10
[*Switch-10GE1/0/1] quit
[*Switch] interface 10ge 1/0/2
[*Switch-10GE1/0/2] port link-type trunk
[*Switch-10GE1/0/2] port trunk allow-pass vlan 20
[*Switch-10GE1/0/2] quit
[*Switch] interface 10ge 1/0/3
[*Switch-10GE1/0/3] port link-type trunk
[*Switch-10GE1/0/3] port trunk allow-pass vlan 30
[*Switch-10GE1/0/3] quit
```

创建接口VLANIF10、VLANIF20、VLANIF30，配置各VLANIF接口的IP地址。

```
[*Switch] interface vlanif 10
[*Switch-Vlanif10] ip address 10.8.8.4 24
[*Switch-Vlanif10] quit
[*Switch] interface vlanif 20
[*Switch-Vlanif20] ip address 10.9.9.4 24
[*Switch-Vlanif20] quit
[*Switch] interface vlanif 30
[*Switch-Vlanif30] ip address 10.10.10.3 24
[*Switch-Vlanif30] quit
```

步骤2 配置ARP表项严格学习功能

```
[*Switch] arp learning strict
```

步骤3 配置ARP表项固化功能

配置ARP表项固化模式为**fixed-mac**方式。

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

步骤4 配置免费ARP报文主动丢弃功能

```
[*Switch] arp anti-attack gratuitous-arp drop
```

步骤5 配置根据源IP地址进行ARP Miss消息限速

配置对Server（IP地址为10.10.10.2）的ARP Miss消息进行限速，允许Switch每秒最多处理该IP地址触发的40个ARP Miss消息；对于其他用户，允许Switch每秒最多处理同一个源IP地址触发的20个ARP Miss消息。

```
[*Switch] arp miss anti-attack rate-limit source-ip maximum 20
[*Switch] arp miss anti-attack rate-limit source-ip 10.10.10.2 maximum 40
```

步骤6 配置基于接口的ARP表项限制

配置接口10GE1/0/1最多可以学习到20个动态ARP表项。

```
[*Switch] interface 10ge 1/0/1
[*Switch-10GE1/0/1] arp limit vlan 10 20
[*Switch-10GE1/0/1] quit
```

步骤7 配置基于接口的ARP限速

配置接口10GE1/0/1最多允许256个ARP报文通过。

说明

CE6870EI和CE6875EI不支持该功能。

```
[*Switch] interface 10ge 1/0/1
[*Switch-10GE1/0/1] arp anti-attack rate-limit 256
[*Switch-10GE1/0/1] quit
```

步骤8 配置根据源MAC地址进行ARP限速

配置对用户User1（MAC地址为1-1-1）进行ARP报文限速，每秒最多只允许10个该MAC地址的ARP报文通过。

```
[*Switch] arp anti-attack rate-limit source-mac 1-1-1 maximum 10
```

步骤9 配置根据源IP地址进行ARP限速

配置对用户User3（IP地址为10.9.9.2）进行ARP报文限速，每秒最多只允许10个该IP地址的ARP报文通过。

```
[*Switch] arp anti-attack rate-limit source-ip 10.9.9.2 maximum 10
[*Switch] commit
[~Switch] quit
```

步骤10 验证配置结果

执行命令**display arp learning strict**，可以看到全局已经配置ARP表项严格学习功能。

```
<Switch> display arp learning strict
The global arp learning strict state:enable
Interface                LearningStrictState
-----
Total:0      Force-enable:0      Force-disable:0
```

执行命令**display arp limit**，查看接口可以学习到的动态ARP表项数目的最大值。

```
<Switch> display arp limit interface 10ge 1/0/1
Interface          VLAN    Limit    Learnt
-----
10GE1/0/1          10      20       0
Total:1
```

执行命令**display arp anti-attack rate-limit**，查看ARP报文限速的配置情况。

```
<Switch> display arp anti-attack rate-limit
Global ARP packet rate limit (pps)      : --
Suppress Rate of each destination IP (pps): 500

Total number of rate-limit configuration for source IP Address :
1
Source IP          Suppress Rate(pps)
-----
10.9.9.2           10
-----

Total number of rate-limit configuration for MAC Address :
1
Source MAC         Suppress Rate(pps)
-----
0001-0001-0001     10
Other              30
-----
```

执行命令**display arp anti-attack entry-check**，查看ARP表项固化模式的配置情况。

```
<Switch> display arp anti-attack entry-check
Interface    Mode
-----
All          fix-mac
-----
```

执行命令**display arp miss anti-attack rate-limit**，查看ARP Miss消息限速的配置情况。

```
<Switch> display arp miss anti-attack rate-limit
Global ARP miss rate limit (pps)      : 3000

Total number of rate-limit configuration for source IP Address :
1
Source IP      Suppress Rate(pps)
-----
10.10.10.2/32      40
Other              20
-----
```

执行命令**display arp packet statistics**，查看ARP处理的报文统计数据。

```
<Switch> display arp packet statistics
ARP Packets Received
Total:          90402
Learnt Count:   37
Discard For Entry Limit: 146
Discard For Speed Limit: 40529
Discard For Proxy Suppress: 0
Discard For Other: 8367601
ARP Packets Sent
Total:          6447
Request:        6341
Reply:          106
Gratuitous ARP: 0
ARP-Miss Message Received
Total:          12
Discard For Speed Limit: 194
Discard For Other: 238
```

由显示信息可知，Switch上产生了ARP报文和ARP Miss消息丢弃计数，表明ARP安全功能已经生效。

----结束

配置文件

Switch的配置文件（CE6870EI和CE6875EI除外）

```
#
sysname Switch
#
vlan batch 10 20 30
#
arp miss anti-attack rate-limit source-ip maximum 20
arp anti-attack rate-limit source-ip 10.9.9.2 maximum 10
arp miss anti-attack rate-limit source-ip 10.10.10.2 maximum 40
arp anti-attack rate-limit source-mac 0001-0001-0001 maximum 10
arp learning strict
arp anti-attack entry-check fixed-mac enable
arp anti-attack gratuitous-arp drop
#
interface Vlanif10
 ip address 10.8.8.4 255.255.255.0
#
interface Vlanif20
 ip address 10.9.9.4 255.255.255.0
#
interface Vlanif30
 ip address 10.10.10.3 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp limit vlan 10 20
 arp anti-attack rate-limit 256
#
```

```
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 30
#
return
```

Switch的配置文件（CE6870EI和CE6875EI）

```
#
sysname Switch
#
vlan batch 10 20 30
#
arp miss anti-attack rate-limit source-ip maximum 20
arp anti-attack rate-limit source-ip 10.9.9.2 maximum 10
arp miss anti-attack rate-limit source-ip 10.10.10.2 maximum 40
arp anti-attack rate-limit source-mac 0001-0001-0001 maximum 10
arp learning strict
arp anti-attack entry-check fixed-mac enable
arp anti-attack gratuitous-arp drop
#
interface Vlanif10
ip address 10.8.8.4 255.255.255.0
#
interface Vlanif20
ip address 10.9.9.4 255.255.255.0
#
interface Vlanif30
ip address 10.10.10.3 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
arp limit vlan 10 20
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 30
#
return
```

10.9.2 配置防止 ARP 中间人攻击示例

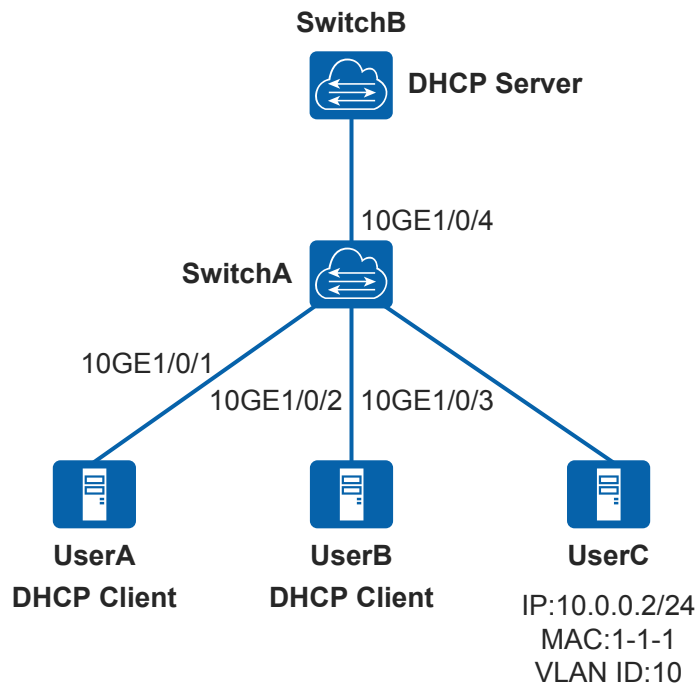
组网需求

如图10-9所示，企业某部门用户通过SwitchA接入Internet。SwitchA下挂的用户，有些采用DHCP方式获取IP地址，有些采用静态配置的IP地址，且所有用户和DHCP Server均位于同一VLAN。如果存在攻击者发起ARP中间人攻击，会造成合法数据的泄漏，因此管理员希望SwitchA能够防止ARP中间人攻击。

说明

CE5880EI、CE6881、CE6881K、CE6820、CE6863、CE6863K、CE6881E和CE6880EI不支持此示例。

图 10-9 配置防止 ARP 中间人攻击组网图



配置思路

采用如下思路在SwitchA上进行配置：

1. 配置DHCP Snooping功能，以便生成动态用户的地址和端口的绑定关系表，并为静态用户配置静态绑定表，用于后续的ARP报文检查。
2. 使能动态ARP检测功能，使SwitchA对收到的ARP报文对应的源IP、源MAC、VLAN以及接口信息进行绑定表匹配检查，过滤非法ARP报文，从而防止ARP中间人攻击。

操作步骤

步骤1 创建VLAN，将接口加入到VLAN中

创建VLAN10，并将接口10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4加入VLAN10中。

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan batch 10
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type access
[*SwitchA-10GE1/0/1] port default vlan 10
[*SwitchA-10GE1/0/1] quit
[*SwitchA] interface 10ge 1/0/2
[*SwitchA-10GE1/0/2] port link-type access
[*SwitchA-10GE1/0/2] port default vlan 10
[*SwitchA-10GE1/0/2] quit
[*SwitchA] interface 10ge 1/0/3
[*SwitchA-10GE1/0/3] port link-type access
[*SwitchA-10GE1/0/3] port default vlan 10
```



```
[*SwitchA-10GE1/0/3] quit
[*SwitchA] interface 10ge 1/0/4
[*SwitchA-10GE1/0/4] port link-type trunk
[*SwitchA-10GE1/0/4] port trunk allow-pass vlan 10
[*SwitchA-10GE1/0/4] quit
```

步骤2 配置DHCP Snooping功能

全局使能DHCP Snooping功能。

```
[*SwitchA] dhcp enable
[*SwitchA] dhcp snooping enable
```

在VLAN10内使能DHCP Snooping功能。

```
[*SwitchA] vlan 10
[*SwitchA-vlan10] dhcp snooping enable
[*SwitchA-vlan10] quit
```

配置接口10GE1/0/4为DHCP Snooping信任接口。

```
[*SwitchA] interface 10ge 1/0/4
[*SwitchA-10GE1/0/4] dhcp snooping trusted
[*SwitchA-10GE1/0/4] quit
```

配置静态绑定表。

```
[*SwitchA] user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface 10ge 1/0/3 vlan 10
[*SwitchA] commit
```

步骤3 在VLAN10内使能动态ARP检测功能

```
[*SwitchA] vlan 10
[*SwitchA-vlan10] arp anti-attack check user-bind enable
[*SwitchA-vlan10] commit
```

步骤4 验证配置结果

执行**display current-configuration**命令，查看DHCP Snooping功能、静态绑定表和动态ARP检测功能的配置情况。具体请参见配置文件。

----结束

配置文件

SwitchA的配置文件：

```
#
sysname SwitchA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface 10GE1/0/3 vlan 10
#
vlan 10
dhcp snooping enable
arp anti-attack check user-bind enable
#
interface 10GE1/0/1
port default vlan 10
#
interface 10GE1/0/2
port default vlan 10
```

```
#
interface 10GE1/0/3
port default vlan 10
#
interface 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 10
dhcp snooping trusted
#
return
```