目 录

1 ARP攻击防御

1.1 ARP防IP报文攻击配置命令

1.1.1 arp resolving-route enable

【命令】

arp resolving-route enable

undo arp resolving-route enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp resolving-route enable 命令用来启用 ARP 防 IP 报文攻击功能。**undo arp resolving-route enable** 命令用来关闭 ARP 防 IP 报文攻击功能。

默认情况下关闭 ARP 防 IP 报文攻击功能。

【举例】

启用 ARP 防 IP 报文攻击功能。

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

1.2 源MAC地址固定的ARP攻击检测配置命令

1.2.1 arp anti-attack source-mac

【命令】

arp anti-attack source-mac { **filter** | **monitor** }

undo arp anti-attack source-mac [**filter** | **monitor**]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

filter：检测到攻击后，打印告警信息，同时对该源 MAC 地址对应的 ARP 报文进行过滤。

monitor：检测到攻击后，只打印告警信息，不对该源 MAC 地址对应的 ARP 报文进行过滤。

【描述】

arp anti-attack source-mac 命令用来使能源 MAC 地址固定 ARP 攻击检测功能，并选择检查模式。**undo arp anti-attack source-mac** 命令用来恢复缺省情况。

缺省情况下，源 MAC 固定 ARP 攻击检测功能处于关闭状态。

使能源 MAC 固定 ARP 攻击检测之后，该特性会对上送 CPU 的 ARP 报文按照源 MAC 和 VLAN 进行统计。当在一定时间（5 秒）内收到某固定源 MAC 地址的 ARP 报文超过设定的阈值，不同模式的处理方式存在差异：在 **filter** 模式下会打印告警信息并对该源 MAC 地址对应的 ARP 报文进行过滤；在 **monitor** 模式下只进行告警，不过滤 ARP 报文。

需要注意的是，如果 **undo** 命令中没有指定检查模式，则关闭任意检查模式的源 MAC 固定 ARP 攻击检测功能。

【举例】

使能源 MAC 固定 ARP 攻击检测功能，并选择 **filter** 检查模式。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac filter
```

1.2.2 arp anti-attack source-mac aging-time

【命令】

arp anti-attack source-mac aging-time *time*

undo arp anti-attack source-mac aging-time

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

time：源 MAC 地址固定的 ARP 攻击检测表项的老化时间，取值范围为 60～6000，单位为秒。

【描述】

arp anti-attack source-mac aging-time 命令用来配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。**undo arp anti-attack source-mac aging-time** 命令用来恢复缺省情况。

缺省情况下，源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒，即 5 分钟。

【举例】

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

1.2.3 arp anti-attack source-mac exclude-mac

【命令】

arp anti-attack source-mac exclude-mac *mac-address*&<1-n>

undo arp anti-attack source-mac exclude-mac [*mac-address*&<1-n>]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

mac-address&<1-n>：MAC 地址列表。其中，*mac-address* 表示配置的保护 MAC 地址，格式为 H-H-H。&<1-n>表示每次最多可以配置的保护 MAC 地址个数。n 的取值范围 1～10。

【描述】

arp anti-attack source-mac exclude-mac 命令用来配置保护 MAC。当配置了保护 MAC 之后，即使该 ARP 报文中的 MAC 地址存在攻击也不会被检测过滤。**undo arp anti-attack source-mac exclude-mac** 命令用来取消配置的保护 MAC。

缺省情况下，没有配置任何保护 MAC。

需要注意的是，如果 **undo** 命令中没有指定 MAC 地址，则取消所有配置的保护 MAC。

【举例】

配置源 MAC 固定攻击检查的保护 MAC 地址为 2-2-2。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

1.2.4 arp anti-attack source-mac threshold

【命令】

arp anti-attack source-mac threshold *threshold-value*

undo arp anti-attack source-mac threshold

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

threshold-value：固定时间内源 MAC 固定 ARP 报文攻击检测的阈值，单位为报文个数。取值范围 10～100，缺省值 50。

【描述】

arp anti-attack source-mac threshold 命令用来配置源 MAC 固定 ARP 报文攻击检测阈值，当在固定的时间（5 秒）内收到源 MAC 固定的 ARP 报文超过该阈值则认为存在攻击。**undo arp anti-attack source-mac threshold** 命令用来恢复缺省阈值。

【举例】

配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac threshold 30
```

1.2.5 display arp anti-attack source-mac

【命令】

display arp anti-attack source-mac [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface *interface-type interface-number*：显示指定接口检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【描述】

display arp anti-attack source-mac 命令用来显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

在集中式设备上，如果不指定接口，则显示所有接口检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【举例】

显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp anti-attack source-mac
Source-MAC          VLAN ID          Interface            Aging-time
23f3-1122-3344      4094             GE0/0                10
23f3-1122-3355      4094             GE0/1                30
23f3-1122-33ff      4094             GE0/2                25
23f3-1122-33ad      4094             GE0/3                30
23f3-1122-33ce      4094             GE0/4                2
```

表1-1 display arp anti-attack source-mac 命令显示信息描述表

字段	描述
Source-MAC	检测到攻击的源MAC地址
VLAN ID	检测到攻击的VLAN ID
Interface	攻击来源的接口索引
Aging-time	ARP防攻击策略表项老化剩余时间

1.3 ARP报文源MAC一致性检查配置命令

1.3.1 arp anti-attack valid-ack enable

【命令】

arp anti-attack valid-check enable

undo arp anti-attack valid-check enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp anti-attack valid-check enable 命令用来在网关设备上使能 ARP 报文源 MAC 一致性检查功能。网关使能此功能时，会对接收的 ARP 报文进行检查，如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则丢弃该报文。**undo arp anti-attack valid-check enable** 命令用来关闭 ARP 报文源 MAC 一致性检查功能。

缺省情况下，关闭 ARP 源 MAC 一致性检查功能。

【举例】

使能 ARP 源 MAC 一致性检查功能。

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

1.4 ARP主动确认配置命令

1.4.1 arp anti-attack active-ack enable

【命令】

arp anti-attack active-ack enable

undo arp anti-attack active-ack enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp anti-attack active-ack enable 命令用来使能 ARP 主动确认功能。**undo arp anti-attack active-ack enable** 命令用来恢复缺省情况。

缺省情况下，关闭 ARP 主动确认功能。

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

ARP 主动确认功能包括两部分：新建 ARP 表项前的主动确认、修改已有 ARP 表项前的主动确认。

- 新建 ARP 表项前的主动确认：当收到 ARP 报文触发新建动态 ARP 表项时，设备根据收到的 ARP 报文的源 IP 地址发送一个广播 ARP 请求报文，如果在随后的 3 秒内收到对应的 ARP 应答报文，则新建 ARP 表项。否则忽略之前收到 ARP 攻击报文，不新建 ARP 表项。
- 修改已有 ARP 表项前的主动确认：当收到的 ARP 报文中的源 MAC 地址和对应 ARP 表项中的不同时，首先判断 ARP 表项刷新时间是否超过 1 分钟，如果没有超过 1 分钟，则不更新 ARP 表项。否则向 ARP 表项对应的源发送一个单播请求，如果在随后的 5 秒内收到对应的应答报文，则忽略之前收到的 ARP 攻击报文；如果没有收到对应的应答报文，则向之前收到的 ARP 报文对应的源发送一个单播请求，如果在随后的 5 秒内收到了对应的应答报文，则根据该 ARP 报文更新 ARP 表项，否则 ARP 表项不会被修改。

【举例】

使能 ARP 主动确认功能。

```
<Sysname> system-view
[Sysname] arp anti-attack active-ack enable
```

1.5 ARP Detection配置命令

1.5.1 arp detection enable

【命令】

arp detection enable

undo arp detection enable

【视图】

VLAN 视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp detection enable 命令用来使能 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。**undo arp detection enable** 命令用来关闭 ARP Detection 功能。

缺省情况下，关闭 ARP Detection 功能。

【举例】

使能 ARP Detection 功能。

```
<Sysname> system-view
```

```
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

1.5.2 arp detection mode

【命令】

arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

undo arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dhcp-snooping：基于 DHCP Snooping 安全表项的检查模式，此模式主要针对仿冒用户的攻击。

dot1x：基于 802.1X 安全表项的检查模式，此模式主要针对仿冒用户的攻击。

static-bind：基于 IP 和 MAC 静态绑定表项的检查模式，此模式主要针对仿冒网关的攻击。

【描述】

arp detection mode 命令用来配置 ARP Detection 检查模式。**undo arp detection mode** 命令用来取消指定的 ARP Detection 检查模式。

缺省情况下，没有配置 ARP Detection 检查模式，认为所有报文都是非法的。

需要注意的是，如果同时配置了三种检查模式，则先进行 IP 和 MAC 静态绑定表项检查，然后进行 DHCP Snooping 安全表项检查，最后进行 802.1X 安全表项检查。

【举例】

配置 ARP Detection 基于 DHCP Snooping 表项和 802.1X 安全表项的检查模式。

```
<Sysname> system-view
[Sysname] arp detection mode dhcp-snooping
[Sysname] arp detection mode dot1x
```

1.5.3 arp detection static-bind

【命令】

arp detection static-bind *ip-address mac-address*

undo arp detection static-bind [*ip-address*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：静态绑定表项的 IP 地址部分。

mac-address：静态绑定表项的 MAC 地址部分，格式为 H-H-H。

【描述】

arp detection static-bind 命令用来配置 IP 和 MAC 的静态绑定表项。**undo arp detection static-bind** 命令用来删除已经配置的 IP 和 MAC 的静态绑定表项。

缺省情况下，没有静态绑定表项。

对于源 IP 存在绑定关系但是 MAC 地址不符的 ARP 报文，设备认为是非法报文进行丢弃处理；对于源 IP 不存在绑定关系和源 IP 存在绑定关系且 MAC 地址相符的 ARP 报文，设备认为是合法报文，通过检查。

需要注意的是，如果 **undo** 命令中没有指定 IP 地址，则删除已经配置的所有 IP 和 MAC 的静态绑定表项。

【举例】

配置 IP 和 MAC 的静态绑定表项。

```
<Sysname> system-view
[Sysname] arp detection static-bind 192.168.1.2 2-1-201
```

1.5.4 arp detection trust

【命令】

arp detection trust

undo arp detection trust

【视图】

二层以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp detection trust 命令用来配置端口为 ARP 信任端口。**undo arp detection trust** 命令用来配置端口为 ARP 非信任端口。

缺省情况下，端口为 ARP 非信任端口。

【举例】

配置二层以太网接口 GigabitEthernet0/1 为 ARP 信任端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet0/1
[Sysname- GigabitEthernet0/1] arp detection trust
```

1.5.5 arp detection validate

【命令】

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dst-mac：检查 ARP 应答报文中的目的 MAC 地址，是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，无效的报文需要被丢弃。

ip：检查 ARP 报文源 IP 和目的 IP 地址，全 0、全 1、或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

src-mac：检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致认为有效，否则丢弃。

【描述】

arp detection validate 命令用来使能对 ARP 报文的目的或源 MAC 地址、IP 地址的有效性检查。使能有效性检查时可以指定某一种检查方式也可以配置成多种检查方式的组合。**undo arp detection validate** 命令用来关闭对 ARP 报文的有效性检查。关闭时可以指定关闭某一种或多种检查，在不指定检查方式时，表示关闭所有有效性检查。

缺省情况不对 ARP 报文的有效性检查。

需要注意的是，如果 **undo** 命令中没有指定检查方式，则关闭已经配置的所有检查方式。

【举例】

使能对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac src-mac ip
```

1.5.6 arp restricted-forwarding enable

【命令】

arp restricted-forwarding enable

undo arp restricted-forwarding enable

【视图】

VLAN 视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp restricted-forwarding enable 命令用来使能 ARP 报文强制转发功能。**undo arp restricted-forwarding enable** 命令用来关闭 ARP 报文强制转发功能。

缺省情况下，ARP 报文强制转发功能处于关闭状态。

【举例】

使能 VLAN 1 的 ARP 报文强制转发功能。

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp restricted-forwarding enable
```

1.5.7 display arp detection

【命令】

display arp detection

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

无

【描述】

display arp detection 命令用来显示使能了 ARP Detection 功能的 VLAN。

相关配置可参考 **arp detection enable**。

【举例】

显示所有使能了 ARP Detection 功能的 VLAN。

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1, 2, 4-5
```

表1-2 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	使能了ARP Detection功能的VLAN

1.5.8 display arp detection statistics

【命令】

display arp detection statistics [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface *interface-type interface-number*：显示指定接口的统计信息。*interface-type interface-number* 用来指定接口类型和编号。

【描述】

display arp detection statistics 命令用来显示 ARP Detection 功能报文检查的丢弃计数的统计信息。按端口显示用户合法性检查，报文有效性检查和 ARP 报文上送限速的统计情况，只显示丢弃的情况。不指定端口时，显示所有端口的统计信息。

【举例】

显示 ARP Detection 功能报文检查的丢弃计数的统计信息。

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP         Src-MAC    Dst-MAC    Inspect
GE0/1(U)                  40         0          0          78
GE0/2(U)                  0          0          0          0
GE0/3(T)                  0          0          0          0
GE0/4(U)                  0          0          30         0
```

表1-3 display arp detection statistics 命令显示信息描述表

字段	描述
Interface(State)	ARP报文入接口，State表示该接口的信任状态
IP	ARP报文源和目的IP地址检查不通过丢弃的报文计数
Src-MAC	ARP报文源MAC地址检查不通过丢弃的报文计数
Dst-MAC	ARP报文目的MAC地址检查不通过丢弃的报文计数
Inspect	ARP报文结合用户合法性检查（DHCP Snooping、802.1X、静态绑定）不通过丢弃的报文计数

1.5.9 reset arp detection statistics

【命令】

reset arp detection statistics [**interface** *interface-type interface-number*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

interface *interface-type interface-number*：表示清除指定接口下的统计信息。*interface-type interface-number* 用来指定接口类型和编号。

【描述】

reset arp detection statistics 命令用来清除 ARP Detection 的统计信息。不指定接口时，清除所有的 ARP Detection 统计信息。

【举例】

清除所有的 ARP Detection 统计信息。

```
<Sysname> reset arp detection statistics
```

1.6 ARP自动扫描、固化配置命令

1.6.1 arp fixup

【命令】

arp fixup

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp fixup 命令用来配置 Fixed ARP 功能。Fixed ARP 功能用来固化动态 ARP 表项，将动态 ARP 表项转换为静态 ARP 表项，用于指导报文转发。

需要注意的是：

- 固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。
- 固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。
- 如果用户执行固化前有 D 个动态 ARP 表项，S 个静态 ARP 表项，由于固化过程中存在动态 ARP 表项的老化或者新建动态 ARP 表项的情况，所以固化后的静态 ARP 表项可能为（D＋S＋M－N）个。其中，M 为固化过程中新建的动态 ARP 表项个数，N 为固化过程中老化的动态 ARP 表项个数。
- 通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* [*vpn-instance-name*] 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

【举例】

配置 Fixed ARP 功能。

```
<Sysname> system-view
[Sysname] arp fixup
```

1.6.2 arp scan

【命令】

arp scan [*start-ip-address* **to** *end-ip-address*]

【视图】

三层以太网接口视图/三层以太网子接口视图/VLAN 接口视图

【缺省级别】

2：系统级

【参数】

start-ip-address：ARP 扫描区间的起始 IP 地址。起始 IP 地址必须小于等于终止 IP 地址。

end-ip-address：ARP 扫描区间的终止 IP 地址。终止 IP 地址必须大于等于起始 IP 地址。

【描述】

arp scan 命令用来启动 ARP 自动扫描功能。

需要注意的是：

- 如果用户指定了 ARP 扫描区间，则对该范围内的邻居进行扫描；如果用户不指定 ARP 扫描区间，则对接口下的主 IP 地址网段内的邻居进行扫描。
- ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址（主 IP 地址或手工配置的从 IP 地址）在同一网段。
- 对于已存在 ARP 表项的 IP 地址不进行扫描。
- 扫描操作可能比较耗时，用户可以通过 Ctrl_C 来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

【举例】

对接口 GigabitEthernet0/1 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 0/1
[Sysname-GigabitEthernet0/1] arp scan
```

对接口 GigabitEthernet0/1 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 0/1
[Sysname-GigabitEthernet0/1] arp scan 1.1.1.1 to 1.1.1.20
```