目 录

1 ARP攻击防御配置命令

1.1 ARP防止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 命令用来使能 ARP 黑洞路由功能。**undo arp resolving-route enable** 命令用来关闭 ARP 黑洞路由功能。

缺省情况下，ARP 黑洞路由功能处于关闭状态。

【举例】

使能 ARP 黑洞路由功能。

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

1.1.2 arp source-suppression enable

【命令】

arp source-suppression enable

undo arp source-suppression enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp source-suppression enable 命令用来使能 ARP 源地址抑制功能。**undo arp source-suppression enable** 命令用来恢复缺省情况。

缺省情况下，关闭 ARP 源地址抑制功能。

相关配置可参考命令 **display arp source-suppression**。

【举例】

使能 ARP 源地址抑制功能。

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

1.1.3 arp source-suppression limit

【命令】

arp source-suppression limit *limit-value*

undo arp source-suppression limit

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

limit-value：ARP 源抑制的阈值，取值范围为 2～1024。

【描述】

arp source-suppression limit 命令用来配置 ARP 源抑制的阈值。**undo arp source-suppression limit** 命令用来恢复缺省情况。

缺省情况下，ARP 源抑制的阈值为 10。

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 秒内的 ARP 请求报文的流量超过设置的阈值），对于由此 IP 地址发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理，从而避免了恶意攻击所造成的危害。

相关配置可参考命令 **display arp source-suppression**。

【举例】

配置 ARP 源抑制的阈值为 100。

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

1.1.4 display arp source-suppression

【命令】

display arp source-suppression [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display arp source-suppression 命令用来显示当前 ARP 源抑制的配置信息。

【举例】

显示当前 ARP 源抑制的配置信息。

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
 Current cache length: 16
```

表1-1 display arp source-suppression 显示信息描述表

字段	描述
ARP source suppression is enabled	ARP 源地址抑制功能处于使能状态
Current suppression limit	设备在 5 秒时间间隔内可以接收到的同源 IP，且目的 IP 地址不能解析的 IP 报文的最大数目
Current cache length	目前记录源抑制信息的缓存的长度

1.2 ARP报文限速配置命令

1.2.1 arp rate-limit (system view)

【命令】

集中式设备：

arp rate-limit { **disable** | **rate** *pps* **drop** }

undo arp rate-limit

分布式设备：

arp rate-limit { **disable** | **rate** *pps* **drop** } [**slot** *slot-number*]

undo arp rate-limit [**slot** *slot-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

disable：不进行限速。

rate *pps*：ARP 限速速率，单位为包每秒（pps）。取值范围为 5～8192。

drop：丢弃超出限速部分的报文。

slot *slot-number*：指定单板所在的槽位号。

【描述】

arp rate-limit 命令用来开启 ARP 报文限速功能，可以配置全局 ARP 报文限速速率，配置对超速 ARP 报文的处理，或者配置取消 ARP 报文限速。**undo arp rate-limit** 命令用来恢复缺省情况。

缺省情况下，开启 ARP 报文限速功能。

【举例】

配置 ARP 报文限速为 50pps，超过限速部分的报文丢弃。

```
<Sysname> system-view
[Sysname] arp rate-limit rate 50 drop
```

1.3 ARP报文源MAC地址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 地址一致性检查功能。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** 命令用来恢复缺省情况。

缺省情况下，关闭 ARP 报文源 MAC 地址一致性检查功能。

【举例】

使能 ARP 报文源 MAC 地址一致性检查功能。

```
<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。

【举例】

使能 ARP 主动确认功能。

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

1.5 授权ARP配置命令

说明

本特性目前仅支持三层以太网接口。

1.5.1 arp authorized enable

【命令】

arp authorized enable

undo arp authorized enable

【视图】

三层以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

arp authorized enable 命令用来使能接口下的授权 ARP 功能。**undo arp authorized enable** 命令用来恢复缺省情况。

缺省情况下，接口下未使能授权 ARP 功能。

使能接口下的授权 ARP 功能后，会启动接口下授权 ARP 表项的老化探测功能，并禁止该接口学习动态 ARP 表项；关闭接口下的授权 ARP 功能后，会关闭该接口下授权 ARP 表项的老化探测功能，并允许该接口学习动态 ARP 表项。

【举例】

使能接口下授权 ARP 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp authorized enable
```

1.5.2 arp authorized time-out

【命令】

arp authorized time-out *seconds*

undo arp authorized time-out

【视图】

三层以太网接口视图

【缺省级别】

2：系统级

【参数】

seconds：授权 ARP 表项的老化时间。取值范围为 30～86400，单位为秒。

【描述】

arp authorized time-out 命令用来配置该接口下授权 ARP 表项的老化时间。**undo arp authorized time-out** 命令用来恢复缺省情况。

缺省情况下，授权 ARP 表项的老化时间为 1200 秒。

【举例】

配置授权 ARP 表项的老化时间。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp authorized time-out 120
```

1.6 ARP Detection配置命令

说明

本节所涉及的命令仅在 SAP 板工作在二层模式时支持。

1.6.1 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 命令用来恢复缺省情况。

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
```

1.6.2 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** 命令用来恢复缺省情况。

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 GigabitEthernet1/0/1 为 ARP 信任端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

1.6.3 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，ARP 报文的有效性检查功能处于关闭状态。

【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
```

1.6.4 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
```

1.6.5 display arp detection

【命令】

display arp detection [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【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

1.6.6 display arp detection statistics

【命令】

display arp detection statistics [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【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。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【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
GE1/0/1(U)                40         0          0          78
GE1/0/2(U)                0          0          0          0
GE1/0/3(T)                0          0          0          0
GE1/0/4(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不通过丢弃的报文计数

1.6.7 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
```

1.7 ARP自动扫描、固化配置命令

1.7.1 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 ARP 固化功能，将当前的动态 ARP 表项转换为静态 ARP 表项。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。

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。
- 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 ARP 固化功能。

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

1.7.2 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，该功能可以对接口下指定地址范围内的邻居进行扫描。

需要注意的是：

- 如果用户知道局域网内邻居分配的 IP 地址范围，指定了 ARP 扫描区间，则对该范围内的邻居进行扫描，减少扫描等待的时间。如果指定的扫描区间同时在接口下多个 IP 地址的网段内，则发送的 ARP 请求报文的源 IP 地址选择网段范围较小的接口 IP 地址。
- 如果用户不指定 ARP 扫描区间的起始 IP 地址和终止 IP 地址，则仅对接口下的主 IP 地址网段内的邻居进行扫描。其中，发送的 ARP 请求报文的源 IP 地址就是接口的主 IP 地址。

- 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 GigabitEthernet1/0/1 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan
```

对接口 GigabitEthernet1/0/1 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan 1.1.1.1 to 1.1.1.20
```

1.8 ARP网关保护配置命令

1.8.1 arp filter source

【命令】

arp filter source *ip-address*

undo arp filter source *ip-address*

【视图】

二层以太网接口视图

【缺省级别】

2：系统级

【参数】

ip-address：被保护的网关 IP 地址。

【描述】

arp filter source 命令用来开启 ARP 网关保护功能，配置被保护的网关 IP 地址。**undo arp filter source** 命令用来删除已配置的被保护网关 IP 地址。

缺省情况下，ARP 网关保护功能处于关闭状态。

需要注意的是：

- 每个端口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一端口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 网关保护功能，被保护的网关 IP 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

1.9 ARP过滤保护配置命令

1.9.1 arp filter binding

【命令】

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

【视图】

二层以太网接口视图

【缺省级别】

2：系统级

【参数】

ip-address：允许通过的 ARP 报文的源 IP 地址。

mac-address：允许通过的 ARP 报文的源 MAC 地址。

【描述】

arp filter binding 命令用来开启 ARP 过滤保护功能，限制只有特定源 IP 地址和源 MAC 地址的 ARP 报文才允许通过。**undo arp filter binding** 命令用来删除已配置的被允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。

缺省情况下，ARP 过滤保护功能处于关闭状态。

需要注意的是：

- 每个端口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一端口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 过滤保护功能，允许源 IP 地址为 1.1.1.1、源 MAC 地址为 2-2-2 的 ARP 报文通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 2-2-2
```