目 录

1 ARP攻击防御

1.1 ARP防止IP报文攻击配置命令

1.1.1 arp resolving-route enable

arp resolving-route enable 命令用来开启 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。

【命令】

arp resolving-route enable

undo arp resolving-route enable

【缺省情况】

ARP 黑洞路由功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

开启 ARP 黑洞路由功能。

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

【相关命令】

- **arp resolving-route probe-count**
- **arp resolving-route probe-interval**

1.1.2 arp resolving-route probe-count

arp resolving-route probe-count 命令用来配置发送 ARP 请求报文的次数。

undo arp resolving-route probe-count 命令用来恢复缺省情况。

【命令】

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

【缺省情况】

发送 ARP 请求报文的次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

count：发送 ARP 请求报文的次数，取值范围为 1～25。

【举例】

配置发送 ARP 请求报文的次数为 5 次。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-count 5
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-interval**

1.1.3 arp resolving-route probe-interval

arp resolving-route probe-interval 命令用来配置发送 ARP 请求报文的时间间隔。

undo arp resolving-route probe-interval 命令用来恢复缺省情况。

【命令】

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

【缺省情况】

发送 ARP 请求报文的时间间隔是 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：发送 ARP 请求报文的时间间隔，取值范围为 1～5，单位为秒。

【举例】

配置发送 ARP 请求报文的时间间隔为 3 秒。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-count**

1.1.4 arp source-suppression enable

arp source-suppression enable 命令用来开启 ARP 源地址抑制功能。

undo arp source-suppression enable 命令用来关闭 ARP 源地址抑制功能。

【命令】

arp source-suppression enable

undo arp source-suppression enable

【缺省情况】

ARP 源地址抑制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

开启 ARP 源地址抑制功能。

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

【相关命令】

- **display arp source-suppression**

1.1.5 arp source-suppression limit

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。

【命令】

arp source-suppression limit *limit-value*

undo arp source-suppression limit

【缺省情况】

ARP 源抑制的阈值为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

limit-value：ARP 源抑制的阈值，即设备在 5 秒间隔内可以处理的源 IP 相同，但目的 IP 地址不能解析的 IP 报文的最大数目，取值范围为 2～1024。

【使用指导】

如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

【举例】

配置 ARP 源抑制的阈值为 100。

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

【相关命令】

- **display arp source-suppression**

1.1.6 display arp source-suppression

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

【命令】

display arp source-suppression

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【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
```

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

字段	描述
ARP source suppression is enabled	ARP源抑制功能处于开启状态
Current suppression limit	设备在5秒时间间隔内可以接收到的源IP相同，但目的IP地址不能解析的IP报文的最大数目

1.2 源MAC地址固定的ARP攻击检测配置命令

1.2.1 arp source-mac

arp source-mac 命令用来开启源 MAC 地址固定的 ARP 攻击检测功能，并选择检查模式。

undo arp source-mac 命令用来关闭源 MAC 地址固定的 ARP 攻击检测功能。

【命令】

```
arp source-mac { filter | monitor }
undo arp source-mac [ filter | monitor ]
```

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filter：配置检查方式为过滤模式。

monitor：配置检查方式为监控模式。

【使用指导】

建议在网关设备上开启本功能。

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。当开启了 ARP 日志信息功能（配置 **arp check log enable** 命令），且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。关于 ARP 日志信息功能的详细描述，请参见“网络互通配置指导”中的“ARP”。

如果 **undo arp source-mac** 命令中未指定检查模式，则关闭任意检查模式的源 MAC 地址固定的 ARP 攻击检测功能。

【举例】

开启源 MAC 地址固定的 ARP 攻击检测功能，并选择 **filter** 检查模式。

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

1.2.2 arp source-mac aging-time

arp 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 source-mac aging-time 命令用来恢复缺省情况。

【命令】

arp source-mac aging-time *time*

undo arp source-mac aging-time

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【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。

【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 source-mac aging-time 60
```

1.2.3 arp source-mac exclude-mac

arp source-mac exclude-mac 命令用来配置保护 MAC 地址。当配置了保护 MAC 地址之后，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 source-mac exclude-mac 命令用来取消配置的保护 MAC 地址。

【命令】

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

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

【缺省情况】

未配置任何保护 MAC 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【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 的取值为 10。

【使用指导】

如果 **undo** 命令中未指定 MAC 地址，则取消所有已配置的保护 MAC 地址。

【举例】

配置源 MAC 地址固定的 ARP 攻击检查的保护 MAC 地址为 001e-1200-0213。

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

1.2.4 arp source-mac threshold

arp source-mac threshold 命令用来配置源 MAC 地址固定的 ARP 报文攻击检测阈值，当在固定的时间（5 秒）内收到源 MAC 地址固定的 ARP 报文超过该阈值则认为存在 ARP 报文攻击。

undo arp source-mac threshold 命令用来恢复缺省情况。

【命令】

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

【缺省情况】

源 MAC 地址固定的 ARP 报文攻击检测阈值为 30。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold-value：固定时间内源 MAC 地址固定的 ARP 报文攻击检测的阈值，单位为报文个数，取值范围为 1～5000。

【举例】

配置源 MAC 地址固定的 ARP 报文攻击检测阈值为 30 个。

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

1.2.5 display arp source-mac

display arp 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。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【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，*interface-type interface-number* 表示指定接口的类型和编号。

【举例】

显示接口 GigabitEthernet1/0/1 检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface               Aging-time
23f3-1122-3344      4094     GE1/0/1                 10
```

表1-2 display arp 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
Aging-time	ARP防攻击策略表项老化剩余时间，单位为秒

1.3 ARP报文源MAC地址一致性检查配置命令

1.3.1 arp valid-check enable

arp valid-check enable 命令用来开启 ARP 报文源 MAC 地址一致性检查功能。

undo arp valid-check enable 命令用来关闭 ARP 报文源 MAC 地址一致性检查功能。

【命令】

arp valid-check enable

undo arp valid-check enable

【缺省情况】

ARP 报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备。

开启 ARP 报文源 MAC 地址一致性检查功能后，设备会对接收的 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。

【举例】

开启 ARP 报文源 MAC 地址一致性检查功能。

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

1.4 ARP主动确认配置命令

1.4.1 arp active-ack enable

arp active-ack enable 命令用来开启 ARP 主动确认功能。

undo arp active-ack enable 命令用来关闭 ARP 主动确认功能。

【命令】

arp active-ack [**strict**] **enable**

undo arp active-ack [**strict**] **enable**

【缺省情况】

ARP 主动确认功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

strict：ARP 主动确认功能的严格模式。

【使用指导】

ARP 的主动确认功能主要应用于网关设备，防止攻击者仿冒用户欺骗网关设备。通过 **strict** 参数开启或关闭主动确认的严格模式。开启严格模式后，ARP 主动确认功能执行更严格的检查，新建 ARP 表项前，需要本设备先对其 IP 地址发起 ARP 解析，解析成功后才能触发正常的主动确认流程，在主动确认流程成功后，才允许设备学习该表项。

【举例】

开启 ARP 主动确认功能。

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

1.5 授权ARP配置命令

1.5.1 arp authorized enable

arp authorized enable 命令用来开启接口下的授权 ARP 功能。

undo arp authorized enable 命令用来关闭接口下的授权 ARP 功能。

【命令】

arp authorized enable

undo arp authorized enable

【缺省情况】

接口下的授权 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

开启 Vlan-interface200 接口下授权 ARP 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] arp authorized enable
```

1.6 ARP Detection配置命令

1.6.1 arp detection enable

arp detection enable 命令用来开启 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。

【命令】

arp detection enable

undo arp detection enable

【缺省情况】

ARP Detection 功能处于关闭状态，即不进行用户合法性检查。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 2 下开启 ARP Detection 功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection rule**

1.6.2 arp detection rule

arp detection rule 命令用来配置用户合法性检查规则。

undo arp detection rule 命令用来删除用户合法性检查规则。

【命令】

arp detection rule *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]

undo arp detection rule [*rule-id*]

【缺省情况】

未配置用户合法性检查规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-id：用户合法性规则编号，取值范围为 0～511，数值越小表示该用户合法性规则优先级越高。

deny：丢弃指定范围内的 ARP 报文。

permit：转发指定范围内的 ARP 报文。

ip { *ip-address* [*mask*] | **any** }：指定报文的源 IP 地址范围。

- *ip-address*：表示报文的源 IP 地址，为点分十进制形式。
- *mask*：表示源 IP 地址的掩码，为点分十进制形式。如果未指定该参数，则 *ip-address* 表示主机地址。
- **any**：表示任意源 IP 地址。

mac { *mac-address* [*mask*] | **any** }：指定报文的源 MAC 地址范围。

- *mac-address*：表示报文的源 MAC 地址，格式为 H-H-H。
- *mask*：表示源 MAC 地址的掩码，格式为 H-H-H。如果未指定该参数，则 *mac-address* 表示主机 MAC 地址。
- **any**：表示任意源 MAC 地址。

vlan *vlan-id*：指定规则中匹配的 VLAN，*vlan-id* 的取值范围为 1～4094。如果未指定该参数，则不对报文中的 VLAN 进行匹配检查。

【使用指导】

只有配置了 **arp detection enable** 命令后，通过命令 **arp detection rule** 配置的规则才生效。

使用 **undo arp detection rule** 命令时，如果未指定 *rule-id*，则会删除设备上所有已配置的用户合法性规则。

【举例】

配置用户合法性规则，规则编号为 0，规则内容为转发源地址为 10.1.1.1，掩码为 255.255.0.0，源 MAC 地址为 0001-0203-0405，掩码为 ffff-ffff-0000 的 ARP 报文。并在 VLAN2 中开启用户合法性检查功能。

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

```
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection enable**

1.6.3 arp detection trust

arp detection trust 命令用来配置接口为 ARP 信任接口。

undo arp detection trust 命令用来恢复缺省情况。

【命令】

arp detection trust

undo arp detection trust

【缺省情况】

接口为 ARP 非信任接口。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。

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

1.6.4 arp detection validate

arp detection validate 命令用来开启对 ARP 报文的目的 MAC 地址或源 MAC 地址、IP 地址的有效性检查。

undo arp detection validate 命令用来关闭对 ARP 报文的有效性检查。

【命令】

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

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

【缺省情况】

ARP 报文有效性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【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 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。

【使用指导】

开启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。

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。

【举例】

开启对 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 ip src-mac
```

1.6.5 arp restricted-forwarding enable

arp restricted-forwarding enable 命令用来开启 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。

【命令】

arp restricted-forwarding enable

undo arp restricted-forwarding enable

【缺省情况】

ARP 报文强制转发功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

开启 VLAN 2 的 ARP 报文强制转发功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

1.6.6 display arp detection

display arp detection 命令用来显示配置了 ARP Detection 功能的 VLAN。

【命令】

display arp detection

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示所有配置了 ARP Detection 功能的 VLAN。

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

表1-3 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	配置了ARP Detection功能的VLAN信息，如果不存在配置了ARP Detection功能的VLAN，则显示“ARP detection is not enabled in any VLAN.”

【相关命令】

- **arp detection enable**

1.6.7 display arp detection statistics

display arp detection statistics 命令用来显示 ARP Detection 丢弃报文的统计信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示指定接口的 ARP Detection 丢弃报文的统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则显示所有接口的 ARP Detection 丢弃报文的统计信息。

【使用指导】

按接口显示用户合法性检查和报文有效性检查的统计情况，只显示 ARP Detection 功能报文的丢弃情况。

【举例】

显示 ARP Detection 丢弃报文的统计信息。

```
<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
```

表1-4 display arp detection statistics 命令显示信息描述表

字段	描述
State	接口状态： • U：ARP 非信任接口 • T：ARP 信任接口
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

【相关命令】

- **reset arp detection statistics**

1.6.8 reset arp detection statistics

reset arp detection statistics 命令用来清除 ARP Detection 的报文丢弃统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：表示清除指定接口下的 ARP Detection 的报文丢弃统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则清除所有接口下的 ARP Detection 报文丢弃统计信息。

【举例】

清除所有的 ARP Detection 的报文丢弃统计信息。

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

【相关命令】

- **display arp detection statistics**

1.7 ARP自动扫描、固化配置命令

1.7.1 arp fixup

arp fixup 命令用来将设备上的动态 ARP 表项转化成静态 ARP 表项。

【命令】

arp fixup

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令将当前的动态 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。

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* 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】

将设备上的动态 ARP 表项转化成静态 ARP 表项。

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

1.7.2 arp scan

arp scan 命令用来开启 ARP 自动扫描功能。

【命令】

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

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【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。

【使用指导】

ARP 自动扫描功能可以对接口下指定地址范围内的邻居进行扫描，对于已存在 ARP 表项的 IP 地址不进行扫描。

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。

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 Vlan-interface2 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

对接口 Vlan-interface2 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```