

目 录

1 协议报文限速.....	1-1
1.1 协议报文限速简介.....	1-1
1.2 协议报文限速配置限制和指导.....	1-1
1.3 配置协议报文限速.....	1-1
1.4 协议报文限速显示和维护.....	1-2
1.5 协议报文限速典型配置举例.....	1-2
1.5.1 基于协议的报文限速配置举例.....	1-2
1.5.2 基于流的协议报文限速配置举例.....	1-3

1 协议报文限速



说明

仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 协议报文限速简介

协议报文限速功能通过对上送 CPU 的报文基于协议进行分类并加以限速处理，避免指定协议报文占用过多的 CPU 资源，导致合法服务请求得不到及时处理。协议报文限速功能可以有效防范设备受到泛洪攻击和 DoS 攻击。

设备支持两种方式的协议报文限速：

- 基于协议的报文限速：限制指定协议报文的最大传输速率，超过该传输速率的流量会被丢弃。
- 基于流的协议报文限速：对同一个源 IP 或源 MAC 的指定协议报文进行限速。同时基于流的协议报文限速功能会记录用户的指定协议报文的流量统计情况，为网络管理者判断该用户是否存在流量异常行为提供依据。

1.2 协议报文限速配置限制和指导

针对同一协议类型的报文，可以同时配置两种方式的协议报文限速功能。同时配置的情况下，首先对报文按照流速率进行限制，然后再按照报文的最大传输速率进行限制。

1.3 配置协议报文限速

表1-1 配置协议报文限速

操作	命令	说明
进入系统视图	system-view	-
开启报文限速功能	anti-attack enable [slot slot-number]	缺省情况下，报文限速功能处于关闭状态
开启所有协议或指定协议的报文限速功能	anti-attack protocol { all protocol } enable [slot slot-number]	缺省情况下，所有协议的报文限速功能处于关闭状态
（可选）配置指定协议报文的最大传输速率	anti-attack protocol protocol threshold rate-limit [slot slot-number]	可以在未修改缺省限速速率的情况下，通过 display anti-attack protocol 命令查看缺省限速速率
（可选）配置协议报文处理优先级	anti-attack protocol protocol priority priority [slot slot-number]	可以在未修改协议报文处理优先级的情况下，通过 display anti-attack protocol 命令查看缺省优先级

操作	命令	说明
开启基于流的协议报文限速功能，并限制指定协议报文的流速率	anti-attack protocol protocol flow-threshold flow-rate-limit [slot slot-number]	缺省情况下，所有协议基于流的协议报文限速功能处于关闭状态 该步骤仅用于基于流的协议报文限速

1.4 协议报文限速显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示协议报文限速的相关情况，通过查看显示信息验证配置的效果。

表1-2 协议报文限速显示和维护

操作	命令
显示所有协议或指定协议的限速信息	display anti-attack protocol [protocol] [slot slot-number]

1.5 协议报文限速典型配置举例

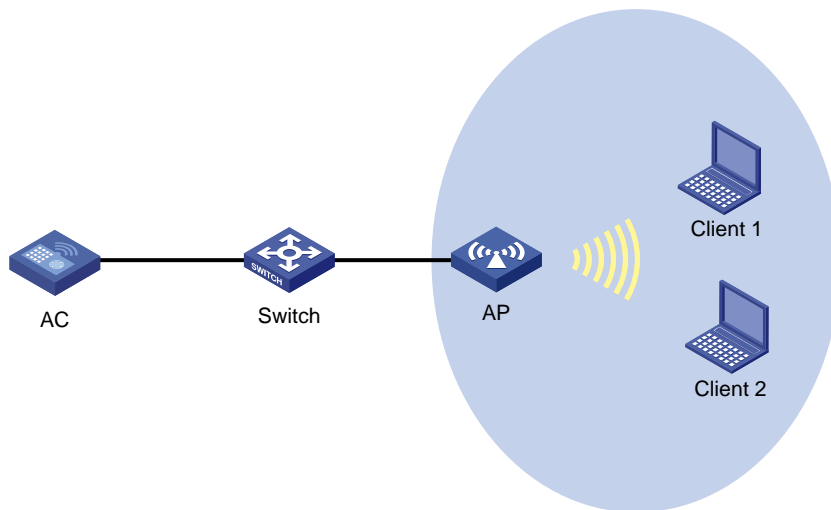
1.5.1 基于协议的报文限速配置举例

1. 组网需求

在 AC 上限制 ARP 协议报文的最大传输速率为 1000 包每秒。

2. 组网图

图1-1 基于协议的报文限速配置组网图



3. 配置步骤

开启报文限速功能。

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

```
[Sysname] anti-attack enable
# 开启 ARP 协议报文的限速功能。
[Sysname] anti-attack protocol arp enable
# 设置 ARP 协议报文的限速速率为 1000 包每秒 (pps)。
[Sysname] anti-attack protocol arp threshold 1000
```

4. 验证配置

当 Client 1 和 Client 2 用户接入后，可以通过 **display anti-attack protocol arp** 命令查看到 ARP 协议报文的限速信息。

```
<Sysname> display anti-attack protocol arp

Anti-attack statistics

Protocol      anti-attack Priority Limit(pps) Rate(pps) Passed   Dropped
arp           enable          1       1000      0        17907   0
```

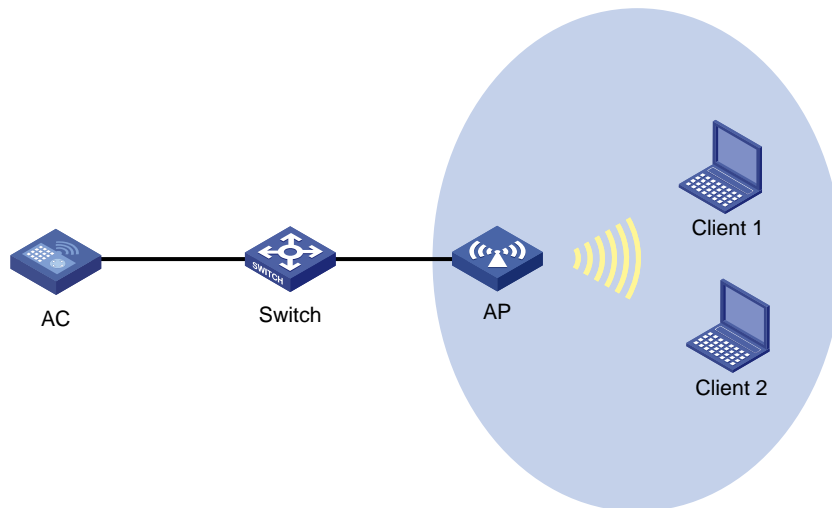
1.5.2 基于流的协议报文限速配置举例

1. 组网需求

在 AC 上限制 ARP 协议报文的流限速速率为 50 包每秒。

2. 组网图

图1-2 基于流的协议报文限速配置组网图



3. 配置步骤

```
# 开启报文限速功能。
<Sysname> system-view
[Sysname] anti-attack enable
# 开启 ARP 协议报文的限速功能。
[Sysname] anti-attack protocol arp enable
# 设置 ARP 协议报文的流限速速率为 50 包每秒 (pps)。
[Sysname] anti-attack protocol arp flow-threshold 50
```

4. 验证配置

当 Client 1 和 Client 2 用户接入后，可以通过 **display anti-attack protocol arp** 命令查看到 ARP 协议报文的限速信息。

```
<Sysname> display anti-attack protocol arp
```

```
Anti-attack statistics
Protocol      anti-attack Priority Limit(pps)  Rate(pps) Passed  Dropped
arp           enable       1          1024       0        17907   0
FlowSource           FlowLimit(pps)  FlowRate(pps)  Passed  Dropped
00e0-fc12-7723      50              0               2        0
0011-e212-8801     50              0              17905   0
```