15 常见 ACL 操作

关于本章

介绍ACL的常见操作，如删除生效时间段、删除ACL和ACL6、配置基于时间的ACL规则等。

15.1 删除生效时间段

删除生效时间段前，需要先删除关联生效时间段的ACL规则或者整个ACL。

例如，在ACL 2001中配置了rule 5，该规则关联了时间段time1。

```
#
time-range time1 from 00:00 2014/1/1 to 23:59 2014/12/31
```

```
#
acl number 2001
 rule 5 permit time-range time1
#
```

如果需要删除时间段time1，则需先删除rule 5或者先删除ACL 2001：

- 先删除rule 5，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] undo rule 5
[HUAWEI-acl-basic-2001] quit
[HUAWEI] undo time-range time1
```

- 先删除ACL 2001，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] undo acl 2001
[HUAWEI] undo time-range time1
```

15.2 删除 ACL 和 ACL6

- 系统视图下执行命令**undo acl** { [**number**] *acl-number* | **all** }或**undo acl name** *acl-name*，可以直接删除ACL，不受引用ACL的业务模块影响，即无需先删除引用ACL的业务配置。
- 系统视图下执行命令**undo acl ipv6** { **all** | [**number**] *acl6-number* }或**undo acl ipv6 name** *acl6-name*，可以直接删除ACL6，不受引用ACL6的业务模块影响，即无需先删除引用ACL6的业务配置。

15.3 配置基于时间的 ACL 规则

创建时间段working-time（周一到周五每天8:00到18:00），并在名称为work-acl的ACL中配置规则，在working-time限定的时间范围内，拒绝源IP地址是192.168.1.0/24网段地址的报文通过。

```
<HUAWEI> system-view
[HUAWEI] time-range working-time 8:00 to 18:00 working-day
[HUAWEI] acl name work-acl basic
[HUAWEI-acl-basic-work-acl] rule deny source 192.168.1.0 0.0.0.255 time-range working-time
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.4 配置基于源 IP 地址（主机地址）过滤报文的规则

在ACL 2001中配置规则，允许源IP地址是192.168.1.3主机地址的报文通过。


```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.5 配置基于源 IP 地址（网段地址）过滤报文的规则

在ACL 2001中配置规则，仅允许源IP地址是192.168.1.3主机地址的报文通过，拒绝源IP地址是192.168.1.0/24网段其他地址的报文通过，并配置ACL描述信息为Permit only 192.168.1.3 through。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
[HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] description Permit only 192.168.1.3 through
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.6 配置基于 IP 分片信息、源 IP 地址（网段地址）过滤报文的规则

在ACL 2001中配置规则，拒绝源IP地址是192.168.1.0/24网段地址的非首片分片报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255 fragment
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.7 配置基于 ICMP 协议类型、源 IP 地址（主机地址）和目的 IP 地址（网段地址）过滤报文的规则

在ACL 3001中配置规则，允许源IP地址是192.168.1.3主机地址且目的IP地址是192.168.2.0/24网段地址的ICMP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit icmp source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.8 配置基于 TCP 协议类型、TCP 目的端口号、源 IP 地址（主机地址）和目的 IP 地址（网段地址）过滤报文的规则

- 在名称为deny-telnet的高级ACL中配置规则，拒绝IP地址是192.168.1.3的主机与192.168.2.0/24网段的主机建立Telnet连接。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name deny-telnet
  [HUAWEI-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet source 192.168.1.3 0
  destination 192.168.2.0 0.0.0.255
  ```

- 在名称为no-web的高级ACL中配置规则，禁止192.168.1.3和192.168.1.4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80），并配置ACL描述信息为Web access restrictions。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name no-web
  [HUAWEI-acl-adv-no-web] description Web access restrictions
  [HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.3 0
  [HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.4 0
  ```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）

- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.9 配置基于 TCP 协议类型、源 IP 地址（网段地址）和 TCP 标志信息过滤报文的规则

在ACL 3002中配置规则，拒绝192.168.2.0/24网段的主机主动发起的TCP握手报文通过，允许该网段主机被动响应TCP握手的报文通过，实现192.168.2.0/24网段地址的单向访问控制。同时，配置ACL规则描述信息分别为Allow the ACK TCP packets through、Allow the RST TCP packets through和Do not Allow the other TCP packet through。

完成以上配置，必须先配置两条permit规则，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
[HUAWEI-acl-adv-3002] display this   //如果配置规则时未指定规则编号，则可以通过此步骤查看到系统为该规则分配的编号，然后根据该编号，为该规则配置描述信息。
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack           //系统分配的规则编号是5
#
return
[HUAWEI-acl-adv-3002] rule 5 description Allow the ACK TCP packets through
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst       //系统分配的规则编号是10
#
return
[HUAWEI-acl-adv-3002] rule 10 description Allow the RST TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
 rule 10 description Allow the RST TCP packets through
 rule 15 deny tcp source 192.168.2.0 0.0.0.255       //系统分配的规则编号是15
#
return
[HUAWEI-acl-adv-3002] rule 15 description Do not Allow the other TCP packet through
```

也可以通过配置established参数，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established
[HUAWEI-acl-adv-3002] rule 5 description Allow the Established TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] rule 10 description Do not Allow the other TCP packet through
```



```
[HUAWEI-acl-adv-3002] display this
#

acl number
3002

 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag
established
 rule 5 description Allow the Established TCP packets
through
 rule 10 deny tcp source 192.168.2.0
0.0.0.255
 rule 10 description Do not Allow the other TCP packet
through
#

return
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.10 配置基于源 MAC 地址（单个 MAC 地址）、目的 MAC 地址（单个 MAC 地址）和二层协议类型过滤报文的规则

- 在ACL 4001中配置规则，允许目的MAC地址是0000-0000-0001、源MAC地址是0000-0000-0002的ARP报文（二层协议类型值为0x0806）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-
  protocol 0x0806
  ```

- 在ACL 4001中配置规则，拒绝PPPoE报文（二层协议类型值为0x8863）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule deny l2-protocol 0x8863
  ```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL

15.11 配置基于源 MAC 地址（MAC 地址段）和内层 VLAN 过滤报文的规则

在名称为deny-vlan10-mac的二层ACL中配置规则，拒绝来自VLAN10且源MAC地址在00e0-fc01-0000～00e0-fc01-ffff范围内的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-vlan10-mac link
[HUAWEI-acl-L2-deny-vlan10-mac] rule deny vlan-id 10 source-mac 00e0-fc01-0000 ffff-ffff-0000
```

相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

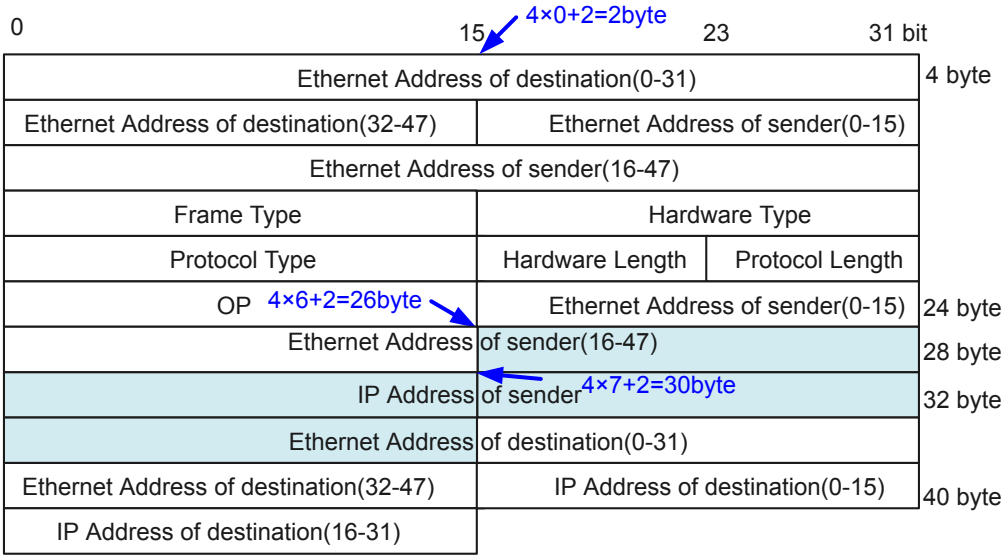
如何配置ACL

15.12 配置基于报文的二层头、偏移位置、字符串掩码和用户自定义字符串过滤报文的规则

- 在ACL 5001中配置规则，拒绝源IP地址为192.168.0.2的ARP报文通过。

  以下规则中的0x00000806是ARP帧类型，0x0000ffff是字符串掩码，10是设备内部处理不含VLAN信息的ARP报文中的协议类型字段的偏移量，c0a80002是192.168.0.2的十六进制形式，26和30分别是设备内部处理不含VLAN信息的ARP报文中源IP地址字段高两个字节和低两个字节的偏移量（ARP报文的源IP地址字段从二层头第28个字节开始占4个字节，受到用户自定义ACL规定二层头偏移位置只能是“4n+2”（n是整数）的限制，因此针对源IP地址，需要拆分成两段进行匹配，即偏移量为4×6+2=26的位置开始往后匹配4个字节的低两个字节以及偏移量为4×7+2=30的位置开始往后匹配4个字节的高两个字节）。如果要对携带VLAN信息的ARP报文进行过滤，则要将以下规则中的三个偏移量值再分别加上4。

图 15-1 ARP 报文源 IP 地址字段在二层头中的偏移量示意图




```
<HUAWEI> system-view
[HUAWEI] acl 5001
[HUAWEI-acl-user-5001] rule deny l2-head 0x00000806 0x0000ffff 10 0x0000c0a8 0x0000ffff 26
0x00020000 0xffff0000 30
```

说明

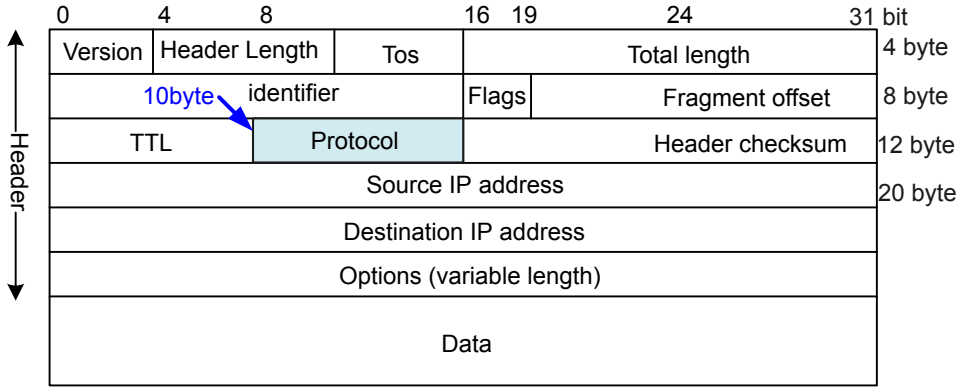
S1720GFR、S1720GW-E、S1720GWR-E、S1720X-E、S2720EI、S2750EI、S5700EI、S5700LI、S5700S-LI、S5700SI、S5710-C-LI、S5710-X-LI、S5720I-SI、S5720LI、S5720S-LI、S5720S-SI、S5720SI、S5730S-EI、S5730SI、S6720LI、S6720S-LI、S6720S-SI和S6720SI的用户自定义ACL不支持上述配置，仅支持指定一个匹配字符串。

- 在名称为deny-tcp的用户自定义ACL中配置规则，拒绝所有TCP报文通过。

  以下规则中的0x00060000是TCP协议号，8是设备内部处理IP报文中协议字段的偏移量（由于IP报文中的协议字段从IPv4头第10个字节开始占1个字节，并且受到用户自定义ACL规定IPv4头偏移位置只能是“4n”（n是整数）的限制，因此针对协议字段，需要从IPv4头偏移量为8的位置开始往后匹配4个字节的第二个高位字节）。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-tcp user
[HUAWEI-acl-user-deny-tcp] rule 5 deny ipv4-head 0x00060000 0x00ff0000 8
```

图 15-2 TCP 协议字段在 IPv4 头中的偏移量示意图



相关信息

技术论坛

- 细说ACL那些事儿（初步认识ACL）
- 细说ACL那些事儿（ACL匹配篇）
- 细说ACL那些事儿（ACL应用篇）

视频

如何配置ACL