目 录

1 报文捕获

1.1 报文捕获命令

1.1.1 display packet capture buffer

【命令】

display packet capture buffer [*start-index* [*end-index*]] [**length** *display-length*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

start-index：查看缓冲区内容的起始位置。如果不指定本参数，缺省起始位置是缓冲区中写入时间最早的报文记录。

end-index：查看缓冲区内容的结束位置。如果不指定本参数，缺省结束位置是缓冲区中写入时间最晚的报文记录。

length *display-length*：单个报文记录的报文数据显示长度，单位为字节。取值范围为 14～256，缺省值为 68。

【描述】

display packet capture buffer 命令用来查看当前报文捕获缓冲区中的内容。

不带参数时，可以查看缓冲区中的所有报文记录，也可通过指定参数查看特定部分的报文记录。

需要注意的是：

- 本命令限制了单个报文记录的报文数据显示长度，如果希望查看完整的报文记录内容，请使用 **packet capture buffer save** 命令，将缓冲区内容保存为*.pcap 文件，并使用对应的工具软件查看。
- 在报文捕获的过程中，不能使用本命令。

相关配置可参考命令 **packet capture start**、**packet capture buffer save**。

【举例】

#查看当前报文缓冲区的全部内容。

```
<Sysname> display packet capture buffer
2012-07-26 12:03:15:318  Index 1  GE4/0/2  64 (original 64) Bytes captured
  01 80 c2 00 00 03 1c bd b9 e3 b5 02 81 00 00 01
  88 8e 01 01 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2012-07-26 12:03:25:749  Index 2  GE4/0/2  68 (original 90) Bytes captured
  33 33 00 00 00 12 00 00 5E 00 02 50 86 DD 6E 00
```

```
00 00 00 20 70 FF FE 80 00 00 00 00 00 00 00 00
00 00 00 00 00 81 FF 02 00 00 00 00 00 00 00 00
00 00 00 00 00 12 31 50 64 01 02 58 6A AE FE 80
00 00 00 00
```

1.1.2 display packet capture status

【命令】

display packet capture status

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

无

【描述】

display packet capture status 用来查看当前报文捕获状态。

【举例】

查看当前报文捕获状态。

```
<Sysname> display packet capture status
  Current status :          In process
  Mode :                    Linear
  Buffer size :             2097152 (bytes)
  Buffer used :             0 (bytes)
  Max capture length :      68 (bytes)
  ACL information :         Ethernet frame header ACL 4200
  Schedule datetime:        Unspecified
  Upper limit of duration : Unspecified (seconds)
  Duration :                60 (seconds)
  Upper limit of packets :  Unspecified
  Packets count :           0
```

表1-1 display packet capture status 命令显示信息描述

字段	描述
Current status	报文捕获状态： • In process：报文捕获正在进行 • Scheduled：已配置报文捕获计划，尚未开始 • Paused：报文捕获已暂停，可通过命令行查看、保存、清空报文捕获缓存内容
Mode	报文捕获模式： • Linear：线性模式 • Circurlar：循环模式
Buffer size	报文缓冲区长度

字段	描述
Buffer used	已使用缓冲区长度 单个报文记录由报文记录头部（记录报文入接口、报文捕获时间、被捕获报文长度、实际报文长度等信息）和报文数据两部分组成，因此单个报文记录占用的缓冲区长度会大于Max capture length的值
Max capture length	报文数据最大捕获长度
ACL information	报文捕获使用的ACL类型和编号
Schedule datetime	报文捕获计划的启动时间
Upper limit of duration	报文捕获持续时间上限
Duration	报文捕获持续时间
Upper limit of packets	报文捕获数量上限
Packets count	报文捕获计数

1.1.3 packet capture

【命令】

packet capture { **acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } }*

undo packet capture [**acl** |**buffer-size** | **length** | **mode**]

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

acl：仅捕获按指定 ACL 过滤后的报文。如果不指定 ACL，则捕获设备收到的所有报文。

acl-number：IPv4 ACL 的编号，取值范围及其代表的 ACL 类型如下。

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL。

acl6-number：IPv6 ACL 的编号，取值范围及其代表的 ACL 类型如下。

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

buffer-size *size*：指定的报文缓冲区长度，单位为千字节（KB）。取值范围为 32～65535，缺省值为 2048。

length *capture-length*：报文数据最大捕获长度，从报文首个字节开始计算，超过此长度的报文数据不会被记录到缓冲区中，单位为字节。取值范围为 16～4000，缺省值为 68。

circular：报文捕获模式为循环模式。报文缓冲区写满后，继续进行报文捕获，并覆盖写入时间最早的记录。

linear：报文捕获模式为线性模式。报文缓冲区写满后，暂停报文捕获。缺省情况下，报文捕获模式为线性模式。

【描述】

packet capture 命令用来设置报文捕获参数。**undo packet capture** 命令用来恢复报文捕获参数缺省值，以及停止报文捕获。

需要注意的是：

- 在报文捕获的过程中，不能改变报文捕获参数。
- **undo packet capture** 命令携带可选参数时，恢复该参数为缺省值；未携带可选参数时，恢复所有可选参数为缺省值，并停止报文捕获。
- 如果要捕获按指定 IPv6 ACL 规则过滤的 IPv6 转发的报文，需要先执行 **acl ipv6 enable** 命令。有关该命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“ACL”。

关于启动报文捕获功能，请参考命令 **packet capture start**。

【举例】

先设置报文缓冲区长度为 4096 KB、只捕获来自 192.168.1.0/24 网段的报文，再启动报文捕获。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] quit
<Sysname> packet capture buffer-size 4096
<Sysname> packet capture acl 2000
<Sysname> packet capture start
```

使报文捕获参数恢复到缺省值，并停止报文捕获。

```
<Sysname> undo packet capture
```

1.1.4 packet capture buffer save

【命令】

packet capture buffer save [*filename*]

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

filename：待保存的文件名，文件名不能包含字符\ / : * " < > |。不指定参数时，以缺省文件名 pcapbuffer.pcap 保存。

【描述】

packet capture buffer save 命令用来保存报文捕获缓冲区中的内容。

需要注意的是：

- 请将.pcap 作为保存的文件名后缀。
- 在报文捕获的过程中，不能使用本命令。

相关配置可参考命令 **packet capture**。

【举例】

#保存报文捕获缓冲区中的内容到 example.pcap。

```
<Sysname> packet capture buffer save example.pcap
```

1.1.5 packet capture schedule

【命令】

packet capture schedule datetime *time date*

undo packet capture schedule

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

time：设置的时间，格式为 HH:MM:SS（小时:分钟:秒），HH 取值范围为 0～23，MM 和 SS 取值范围为 0～59。

date：设置的日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日），MM 的取值范围为 1～12，DD 的取值范围与月份有关，YYYY 的取值范围为 2000～2035。

【描述】

packet capture schedule 命令用来配置报文捕获计划。**undo packet capture schedule** 命令用来取消已配置的报文捕获计划。

缺省情况下，报文捕获计划未设置。

需要注意的是：

- 使用本命令配置报文捕获计划，与使用 **packet capture start** 命令手动启动报文捕获效果相同。
- 报文捕获计划尚未开始时，可使用 **packet capture** 命令改变报文捕获参数；也可使用 **packet capture start** 命令立刻启动报文捕获，已配置的报文捕获计划将被取消。
- 执行 **undo packet capture start** 命令或未携带参数的 **undo packet capture** 命令时，将停止报文捕获，并取消已配置的报文捕获计划。

相关配置可参考命令 **packet capture**。

【举例】

配置报文捕获计划。

```
<Sysname> packet capture schedule datetime 12:00:00 2012/12/25
```

1.1.6 packet capture start

【命令】

packet capture start [**acl** { *acl-number* | **ipv6** *acl6-number* } | **buffer-size** *size* | **length** *capture-length* | **mode** { **circular** | **linear** } | [**packets** *packet-number* | **seconds** *second-number*]]*

undo packet capture start

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

acl：仅捕获按指定 ACL 过滤后的报文。如果不指定 ACL，则捕获设备收到的所有报文。

acl-number：IPv4 ACL 的编号，取值范围及其代表的 ACL 类型如下。

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL。

acl6-number：IPv6 ACL 的编号，取值范围及其代表的 ACL 类型如下。

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

buffer-size *size*：指定的报文缓冲区长度，单位为千字节（KB）。取值范围为 32～65535，缺省值为 2048。

length *capture-length*：报文数据最大捕获长度，从报文首个字节开始计算，超过此长度的报文数据不会被记录到缓冲区中，单位为字节。取值范围为 16～4000，缺省值为 68。

circular：报文捕获模式为循环模式。报文缓冲区写满后，继续进行报文捕获，并覆盖写入时间最早的记录。

linear：报文捕获模式为线性模式。报文缓冲区写满后，暂停报文捕获。缺省情况下，报文捕获模式为线性模式。

packets *packet-number*：设置报文捕获数量上限，捕获报文数量超过此上限后自动暂停捕获。取值范围为 1～4294967295，缺省值为 4294967295。

seconds *second-number*：设置报文捕获持续时间，超过此时间则自动暂停捕获。取值范围为 1～4294967295，缺省值为 4294967295。

【描述】

packet capture start 命令用来启动报文捕获，并可以同时设置报文捕获参数。**undo packet capture start** 命令用来停止报文捕获。

缺省情况下，报文捕获功能处于停止状态。

需要注意的是：

- 在报文捕获的过程中，不能重复启动捕获或改变参数，也不能使用 **display packet capture buffer**、**reset packet capture buffer**、**packet capture buffer save** 命令；如有需要，请先使用 **packet capture stop** 命令暂停捕获。
- 已启动报文捕获且指定了 ACL 编号的情况下，如果不存在该编号对应的 ACL 规则，将无法捕获到任何报文；如果修改该 ACL 编号对应的 ACL 规则，不会影响本次报文捕获的结果，修改后的 ACL 规则将在下次执行 **packet capture start** 命令成功后生效。
- **undo packet capture start** 命令用来停止报文捕获，此后不能再查看或操作报文缓冲区中的内容，但之前配置的报文捕获参数仍然生效，再次执行 **packet capture start** 命令时无须重新配置。
- 如果要捕获按指定 ACL 规则过滤的 IPv6 转发的报文，需要先执行 **acl ipv6 enable** 命令。有关该命令的详细介绍，请参见“ACL 和 QoS 命令参考”中的“ACL”。

相关配置可参考命令 **packet capture stop**、**display packet capture status**、**display packet capture buffer**。

【举例】

设置报文数据最大捕获长度为 256 字节，并启动报文捕获。

```
<Sysname> packet capture length 256 start
```

1.1.7 packet capture stop

【命令】

packet capture stop

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

无

【描述】

packet capture stop 命令用来暂停报文捕获。

需要注意的是：

- 暂停报文捕获后，如果使用 **packet capture** 命令改变报文捕获参数，缓冲区中已捕获内容将被清空。
- 报文捕获未启动时，本命令不生效。
- 暂停报文捕获后，可使用 **display packet capture buffer**、**reset packet capture buffer**、**packet capture buffer save** 等命令查看或操作报文缓冲区中的内容，使用 **packet capture start** 命令再次启动捕获。

相关配置可参考命令 **packet capture**、**packet capture start**、**display packet capture buffer**、**reset packet capture buffer**、**packet capture buffer save**。

【举例】

暂停报文捕获。

```
<Sysname> packet capture stop
```

1.1.8 reset packet capture buffer

【命令】

reset packet capture buffer

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

无

【描述】

reset packet capture buffer 命令用来清除报文捕获缓冲区中的内容。

需要注意的是，在报文捕获的过程中，不能使用本命令。

相关配置可参考命令 **packet capture start**。

【举例】

#清除报文捕获缓冲区中的内容。

```
<Sysname> reset packet capture buffer
```