目 录

1 Packet Capture

1.1 Packet Capture配置命令

1.1.1 display packet-capture status

display packet-capture status 命令用来显示报文捕获状态信息。

【命令】

display packet-capture status

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

显示报文捕获状态信息。

```
<Sysname> display packet-capture status
Status     : Capturing
File Name  : flash:/a.pcap
User Name  : N/A
Password   : N/A
```

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

字段	描述
Status	显示捕获状态，目前只有Capturing一种状态
File name	存储捕获报文的文件名称
Username	登录远程FTP服务器时的用户名
Password	登录远程FTP服务器时的密码，配置明文和密文时，均显示为****** 若不涉及或未配置则显示为N/A

【相关命令】

- **packet-capture remote interface**
- **packet-capture local interface**

1.1.2 packet-capture

如需使用本命令，请用户安装 Packet Capture 特性软件包，有关安装步骤的详细介绍，请参见“基础配置指导”中的“软件升级”或“通过 install 命令升级”。

packet-capture 命令用来配置接口的入方向报文捕获。

【命令】

捕获并保存报文到文件：

packet-capture interface *interface-type interface-number* [**capture-filter** *capt-expression* | **limit-captured-frames** *limit* | **limit-frame-size** *bytes* | **autostop filesize** *kilobytes* | **autostop duration** *seconds* | **autostop files** *numbers* | **capture-ring-buffer filesize** *kilobytes* | **capture-ring-buffer duration** *seconds* | **capture-ring-buffer files** *numbers*] * **write** *filepath* [**raw** | { **brief** | **verbose** }] *

捕获并显示报文内容：

packet-capture interface *interface-type interface-number* [**capture-filter** *capt-expression* | **display-filter** *disp-expression* | **limit-captured-frames** *limit* | **limit-frame-size** *bytes* | **autostop duration** *seconds*] * [**raw** | { **brief** | **verbose** }] *

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：表示接口类型和接口编号，用来对指定的接口开启报文捕获的功能，只能指定为二层以太网接口/三层以太网接口。

capture-filter *capt-expression*：指定用来捕获报文的过滤规则，*capt-expression* 为捕获过滤表达式，为 1～256 个字符的字符串，区分大小写。设备根据此参数指定的过滤规则对报文进行过滤并捕获匹配过滤规则的报文。捕获过滤语法规则请参见“网络管理和监控配置指导”中的“Packet Capture”。如果不指定此参数，则捕获该接口的所有入方向的报文。

display-filter *disp-expression*：指定显示被捕获的报文的过滤规则。*disp-expression* 为显示过滤表达式，为 1～256 个字符的字符串，区分大小写。设备对已捕获的报文指定的显示过滤规则，并将匹配的报文内容进行显示。与捕获过滤不同的是，显示过滤支持报文内容过滤，捕获过滤语法规则请参见“网络管理和监控配置指导”中的“Packet Capture”。如果不指定此参数，则显示所有捕获到的报文。

limit-captured-frames *limit*：指定捕获报文的最大个数，*limit* 为报文的最大个数，取值范围为 0～2147483647，单位为个，缺省值为 10。当达到捕获报文的最大个数时，则停止捕获报文，若指定报文最大个数为 0，则表示没有限制。

limit-frame-size *bytes*：指定捕获报文的最大长度，*bytes* 为报文的最大长度，取值范围为 64～8000，单位为字节，缺省值为 8000。当捕获到的报文超过此长度，会对报文进行截断。

autostop filesize *kilobytes*：指定存储报文文件大小，*kilobytes* 为文件长度最大值，取值范围为 1～65536，单位为千字节。当报文文件大小达到最大值时，捕获报文自动停止。如果没有指定本参数，表示对报文文件大小没有限制。

autostop duration *seconds*：指定捕获报文时长，*seconds* 为时长最大值，取值范围为 1～2147483647，单位为秒。当捕获报文时长达到最大值时，捕获报文自动停止。如果没有指定本参数，表示不对捕获报文的时长进行限制。

autostop files *numbers*：指定切换存储报文文件次数，*numbers* 为文件切换次数最大值，取值范围为 2～64。当指定本参数时，报文将被保存到文件名为扩展文件名的文件中，扩展文件名由 **write** 参数指定的文件名称、文件生成序号和写入时间组成，当切换到新文件时，新生成的扩展报文文件序号按序递增，例如，指定的文件名称为 a.pcap，则扩展名称为 a_00001_20140211034151.pcap，当达到切换写文件条件时，则将报文信息写入新生成 a_00002_20140211034207.pcap 文件中，依次类推。当切换文件次数达到最大值时，捕获报文自动停止。如果没有指定本参数，表示不对报文文件切换的次数进行限制。

capture-ring-buffer filesize *kilobytes*：指定切换存储报文文件大小，*kilobytes* 为报文文件长度最大值，取值范围为 1～65536，单位为千字节。当报文文件大小达到最大值时，切换到下一个文件来存储捕获报文。如果没有指定本参数，表示不以文件大小为限制切换报文文件。

capture-ring-buffer duration *seconds*：指定切换存储报文文件时长，*seconds* 为时长最大值，取值范围为 1～2147483647，单位为秒。当捕获报文时长达到最大值时，切换到下一个文件来存储捕获报文。如果没有本参数，表示不以时长为限制切换报文文件。

capture-ring-buffer files *numbers*：指定存储报文文件最大存在个数，*numbers* 为报文文件个数最大值，取值范围为 2～64；当指定本参数时，报文将被保存到文件名为扩展文件名的文件中，扩展文件名由 **write** 参数指定的文件名称、文件生成序号和写入时间组成，当切换到新文件时，新生成的扩展报文文件序号按序递增，例如，指定的文件名称为 a.pcap，则扩展名称为 a_00001_20140211034151.pcap，当达到切换写文件条件时，则将报文信息写入新生成 a_00002_20140211034207.pcap 文件中，依次类推。当文件个数达到最大个数时，删除捕获报文过程中生成的最老文件，将捕获的报文写入新生成的扩展文件中。如果没有指定本参数，表示报文文件的最大存在个数没有限制。

write *filepath*：指定保存捕获报文的文件完整路径，为 1～64 字符的字符串，后缀必须为 pcap 格式，区分大小写。文件名命名规则的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果没有指定此参数，将不会保存捕获的报文。

raw：将报文内容以十六进制格式显示。如果不指定此参数则不将报文文件内容用十六进制格式显示。

verbose：显示捕获报文的详细信息。

brief：显示捕获报文的简要信息。

【使用指导】

开启指定接口的报文捕获功能，设备会实时显示捕获报文的信息，如果用户希望停止捕获，直接输入 Ctrl+C 停止捕获报文。

当指定 **autostop files** 参数或者 **capture-ring-buffer files** 参数时，如果同时指定 **autostop filesize** 参数，则 **autostop filesize** 参数为切换条件属性参数。

当指定 **autostop files** 参数或者 **capture-ring-buffer files** 参数时，则需指定一个具有切换捕获报文文件条件属性的参数。

当同时指定 **autostop filesize** 和 **capture-ring-buffer filesize** 时，**autostop filesize** 停止条件参数属性失效，**capture-ring-buffer filesize** 的切换条件参数属性生效，且以后指定参数的 *kilobytes* 为切换条件。

由于文件系统对文件个数有限制，所以保存捕获报文文件的最大个数同样会有限制，具体数目与设备使用的文件系统有关。当达到文件系统的最大个数时，将退出捕获。

当不指定 **raw**、**brief** 和 **verbose** 中的任何一个参数时，指定 **write** 参数，显示捕获的报文个数；当不指定 **raw**、**brief**、**verbose** 和 **write** 中的任何一个参数时，显示报文的简要信息。

【举例】

配置接口 GigabitEthernet2/1/1 的入方向报文捕获。

```
<Sysname> packet-capture interface gigabitethernet 2/1/1
```

【相关命令】

- **packet-capture read**

1.1.3 packet-capture local interface

packet-capture local interface 命令用来配置接口的本地报文捕获并将捕获的报文保存到本地或 FTP 服务器。

【命令】

packet-capture local interface *interface-type interface-number* [**capture-filter** *capt-expression* | **limit-frame-size** *bytes* | **autostop filesize** *kilobytes* | **autostop duration** *seconds*] * **write** { *filepath* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：表示接口类型和接口编号，用来对指定的接口开启报文捕获功能。只能指定为二层以太网接口/三层以太网接口。

capture-filter *capt-expression*：指定用来捕获报文的过滤规则，*capt-expression* 表示捕获过滤表达式，为 1～256 个字符的字符串，区分大小写。设备根据此参数指定的过滤规则对报文进行过滤并捕获过滤后的报文。捕获过滤语法规则请参见“网络管理和监控配置指导”中的“Packet Capture”。如果不指定此参数，则捕获该接口的所有入方向的报文。

limit-frame-size *bytes*：指定捕获报文的最大长度，*bytes* 为报文的最大长度，取值范围为 64～8000，单位为字节，缺省值为 8000。当捕获到的报文超过此长度，会对报文进行截断。

autostop filesize *kilobytes*：指定存储报文的文件大小，*kilobytes* 为文件的最大长度，取值范围为 1～65536，单位为千字节。当报文文件达到最大值时，报文捕获自动停止。如果没有指定本参数，表示对报文文件大小没有限制。

autostop duration *seconds*：指定捕获报文时长，*seconds* 为最大时长，取值范围为 1～2147483647，单位为秒。当捕获报文时长达到最大值时，报文捕获自动停止。如果没有指定本参数，表示不对捕获报文的时长进行限制。

write：保存报文文件。

filepath：存储报文文件的本地路径，为 1～64 字符的字符串，区分大小写。文件名命名规则的详细介绍，请参见“基础配置指导”中的“文件系统管理”。后缀必须为 pcap。如果没有指定此参数，还可以保存在远程目标路径上。

url *url*：指定存储报文文件的路径，*url* 为 FTP 服务器上的路径，为 1～255 个字符的字符串，区分大小写，路径中不能包含“@”，不能包含用户名和密码，用户名和密码由 **username** 和 **password** 参数指定。

username *username*：指定登录远程 FTP 服务器时使用的用户名，为 1～32 个字符的字符串，区分大小写。

password：设置用户密码。

cipher：以密文方式设置密码。

simple：以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～32 个字符的字符串；密文密码为 1～73 个字符的字符串。

【使用指导】

开启接口的报文捕获，Packet Capture 终端允许用户执行其它操作。如果用户希望停止捕获，请输入 **packet-capture stop** 命令。

具有停止报文捕获条件属性的参数有 **autostop filesize** 参数、**autostop duration** 参数。不同条件的停止捕获参数同时存在时，只要满足任意一个参数，则报文捕获退出。

仅支持使用 FTP 协议将捕获的报文上传到远程 FTP 服务器，*url* 采用“ftp://服务器地址[:端口号]/文件名”的形式，其中服务器地址支持 IP 地址和 DNS 域名方式，若服务器地址为 IPv6 地址时需使用方括号“[”和“]”引用，若服务器地址为 DNS 域名格式时请勿使用方括号引用。如有用户名和密码请分别使用参数 *username* 和参数 *password* 进行配置，用户名和密码必须和服务器上的配置一致，如果服务器只对用户名进行验证，则不用输入密码。

当用户将捕获的报文保存到 FTP 服务器时，若指定的 **autostop duration** 时间较短时，可能设备还未连接到 FTP 服务器，捕获服务已经退出，此时 FTP 服务器不会产生保存捕获报文的文件。

【举例】

将捕获的报文保存到 IP 地址为 10.1.1.1 的 FTP 服务器，FTP 服务器工作目录下，用户名为 1，密码为 1，文件名为 database.pcap。

```
<Sysname> packet-capture local interface gigabitethernet 2/1/1 write url
ftp://10.1.1.1/database.pcap username 1 password simple 1
```

【相关命令】

- **display packet-capture status**
- **packet-capture stop**

1.1.4 packet-capture read

说明

如需使用本命令，请用户安装 Packet Capture 特性软件包，有关安装步骤的详细介绍，请参见“基础配置指导”中的“软件升级”或“通过 install 命令升级”。

packet-capture read 命令用来解析并显示保存的报文文件。

【命令】

packet-capture read *filepath* [**display-filter** *disp-expression*] [**raw** | { **brief** | **verbose** }] *

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filepath：指定读取的文件的完整路径，为 1～64 个字符的字符串，区分大小写。文件名命名规则的详细介绍，请参见“基础配置指导”中的“文件系统管理”。读取指定路径上的 pcap 或 pcapng 格式文件。

display-filter *disp-expression*：指定用来显示报文的过滤规则。*disp-expression* 为显示报文的过滤规则，为 1～256 个字符的字符串。设备报文文件内容匹配参数指定的显示过滤规则，并将匹配的报文内容进行显示。显示过滤语法规则参见 Packet Capture 配置手册。如果不指定此参数，则显示报文文件中的所有报文信息。

raw：将报文文件内容用十六进制格式显示。如果不指定此参数，则不将报文文件内容用十六进制格式显示。

brief：显示报文文件的简要信息。

verbose：显示报文文件的详细信息。

【使用指导】

配置解析并显示报文文件内容后，Packet Capture 终端显示从指定文件中读取解析的报文信息，如果用户希望退出此过程，可以直接输入 Ctrl+C 退出解析过程。

Packet Capture 支持解析 pcap 和 pcapng 格式的报文文件。

未指定 **raw**、**brief**、**verbose** 参数时，则显示简要信息。

【举例】

解析 flash:/test 目录下的报文文件 **aaaa.pcap**。

```
<Sysname> packet-capture read flash:/test/aaaa.pcap
```

【相关命令】

- **packet-capture**

1.1.5 packet-capture remote interface

packet-capture remote interface 命令用来配置接口远程报文捕获。

【命令】

packet-capture remote interface *interface-type interface-number* [**port** *port*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：指定捕获报文的接口。

port *port*：指定 RPCAP 服务端口号，若不指定本参数，缺省值为 2002。

【使用指导】

配置指定接口的远程报文捕获，客户端连接到 AP，就可以获取指定的接口的报文。

可以通过执行 **packet-capture stop** 命令来停止捕获。

【举例】

在 GigabitEthernet2/1/1 上配置远程报文捕获，并且指定服务端口号为 2014。

```
<Sysname> packet-capture remote interface gigabitethernet 2/1/1 port 2014
```

【相关命令】

- **display packet-capture status**
- **packet-capture stop**

1.1.6 packet-capture stop

packet-capture stop 命令用来停止报文捕获。

【命令】

packet-capture stop

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

停止报文捕获。

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

【相关命令】

- **packet-capture local interface**
- **packet-capture remote interface**