

目 录

1 系统维护与调试命令	1-1
1.1 系统维护命令.....	1-1
1.1.1 ping.....	1-1
1.1.2 ping ipv6	1-5
1.1.3 tracet	1-7
1.1.4 tracet ipv6.....	1-8
1.2 系统调试命令.....	1-9
1.2.1 debugging.....	1-9
1.2.2 display debugging	1-10

1 系统维护与调试命令

1.1 系统维护命令

1.1.1 ping

【命令】

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v | -vpn-instance vpn-instance-name ] * host
```

【视图】

任意视图

【缺省级别】

0: 访问级

【参数】

ip: 支持 IPv4 协议。不指定该参数时，也表示支持 IPv4 协议。

-a source-ip: 指定 ICMP 回显请求（ECHO-REQUEST）报文的源 IP 地址。该地址必须是设备上已配置的 IP 地址。不指定该参数时，ICMP 回显请求报文的源 IP 地址是该报文出接口的主 IP 地址。

-c count: 指定 ICMP 回显请求报文的发送次数，取值范围为 1~4294967295，缺省值为 5。

-f: 将长度大于接口 MTU 的报文直接丢弃，即不允许对发送的 ICMP 回显请求报文进行分片。

-h ttl: 指定 ICMP 回显请求报文中的 TTL 值，取值范围为 1~255，缺省值为 255。

-i interface-type interface-number: 指定发送 ICMP 回显请求报文的接口的类型和编号。不指定该参数时，将根据目的 IP 查找路由表或者转发表来确定发送 ICMP 回显请求报文的接口。

-m interval: 指定发送 ICMP 回显请求报文的时间间隔，取值范围为 1~65535，单位为毫秒，缺省值为 200 毫秒。

- 如果在 *timeout* 时间内收到目的主机的响应报文，则下次 ICMP 回显请求报文的发送时间间隔为报文的实际响应时间与 *interval* 之和；
- 如果在 *timeout* 时间内没有收到目的主机的响应报文，则下次 ICMP 回显请求报文的发送时间间隔为 *timeout* 与 *interval* 之和。

-n: 对 *host* 参数不进行域名解析。不指定该参数时，如果 *host* 参数表示的是目的端的主机名，则设备会对 *host* 进行域名解析。

-p pad: 指定 ICMP 回显请求报文的“PAD”字段的填充值，为 1~8 位的 16 进制数，取值范围为 0~ffffff。如果指定的参数不够 8 位，则会在首部补 0，使填充值达到 8 位。比如将 *pad* 设置为 0x2f，则会重复使用 0x0000002f 去填充报文，以使发送报文的总长度达到设备要求值。缺省情况下，填充值从 0x01 开始，逐渐递增，直到 0xff，然后又从 0x01 开始循环，形如 0x010203……feff01……，直至发送报文的总长度达到设备要求值。

-q: 只显示统计信息。不指定该参数时，系统将显示包括统计信息在内的全部信息。

-r: 记录路由信息。不指定该参数时，系统不记录路由。

-s packet-size: 指定发送的 ICMP 回显请求报文的长度（不包括 IP 和 ICMP 报文头），取值范围为 20~8100，单位为字节，缺省值为 56 字节。

-t timeout: 指定 ICMP 回显应答(ECHO-REPLY)报文的超时时间，发送 ICMP 回显请求报文 *timeout* 后还没有收到 ICMP 回显应答报文，源端则认为 ICMP 回显应答报文超时。取值范围为 0~65535，单位为毫秒，缺省值为 2000 毫秒。

-tos tos: 指定 ICMP 回显请求报文中的 ToS (Type of Service, 服务类型) 域的值，取值范围为 0~255，缺省值为 0。

-v: 显示接收到的非回显应答的 ICMP 报文。不指定该参数时，系统不显示非回显应答的 ICMP 报文。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

host: 目的端的 IP 地址或主机名，主机名为 1~255 个字符的字符串。

【描述】

ping 命令用来检查指定目的端是否可达，并输出相应的统计信息。

执行 **ping** 命令后，源端给目的端发送 ICMP 回显请求报文，

- 如果该目的端的名称不可识别，则输出提示信息 “Error: Ping: Unknown host *host-name*”。
- 如果在超时时间内收到目的端的 ICMP 回显响应报文，则输出响应报文的相关信息。
- 如果在超时时间内没有收到目的端的 ICMP 回显响应报文，则输出 “Request time out” 提示用户。

需要注意的是：

- 如果要使用目的端的主机名执行 ping 操作，事先必须在设备上配置 DNS (Domain Name System, 域名系统) 功能，否则会 ping 失败，DNS 的相关介绍和配置请参见 “三层技术-IP 业务配置指导” 中的 “域名解析”。而且当目的端的名称是 ping 命令的关键字（如 ip）时，命令形式应该是 **ping ip ip**，而不能直接输入 **ping ip**。
- 在使用 **-i** 参数指定发送报文的接口时，只能 ping 直连网段地址。

在执行命令过程中，键入 <Ctrl+C> 可终止 ping 操作。

【举例】

检查 IP 地址为 10.1.1.5 的设备是否可达。

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time = 20 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time = 12 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time = 12 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time = 13 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time = 12 ms

--- 10.1.1.5 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 12/13/20 ms
```

以上信息表明，目的端可达，源端发出的 ICMP 回显请求均能得到回应，报文往返的最短时间、平均时间和最长时间分别为 12ms、13ms 和 20ms。

检查私网 vpn1 中 IP 地址为 1.1.2.2 的设备是否可达。

```
<Sysname> ping -vpn-instance vpn1 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
  Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

--- 1.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/41/205 ms
```

以上信息表明，私网 vpn1 中目的端可达，源端发出的 ICMP 回显请求报文均能得到回应，报文往返的最短时间、平均时间和最长时间分别为 1ms、41ms 和 205ms。

检查 IP 地址为 1.1.2.2 的设备是否可达，只显示检查结果。

```
<Sysname> ping -q 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break

--- 1.1.2.2 ping statistics ---
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 1/12/29 ms
```

检查 IP 地址为 1.1.2.2 的设备是否可达，并显示路由信息。

```
<Sysname> ping -r 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=53 ms
    Record Route:
      1.1.2.1
      1.1.2.2
      1.1.1.2
      1.1.1.1
  Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Record Route:
      1.1.2.1
      1.1.2.2
      1.1.1.2
      1.1.1.1
  Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Record Route:
      1.1.2.1
```

```

1.1.2.2
1.1.1.2
1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
Record Route:
1.1.2.1
1.1.2.2
1.1.1.2
1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms
Record Route:
1.1.2.1
1.1.2.2
1.1.1.2
1.1.1.1

--- 1.1.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/11/53 ms

```

以上显示信息表明本设备与 1.1.2.2 之间路由可达，具体路由为 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2。

表1-1 ping 命令显示信息描述表

字段	描述
PING 10.1.1.5	检查IP地址为10.1.1.5的设备是否可达
56 data bytes	每个ICMP回显请求报文中的数据字节数
press CTRL_C to break	在执行命令过程中，按快捷键<Ctrl+C>可终止ping操作
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time= 20 ms	<p>收到IP地址为10.1.1.5的设备回复的ICMP响应报文，若超时仍没有收到ICMP响应报文，则直接输出“Request time out”</p> <ul style="list-style-type: none"> • bytes 表示 ICMP 响应报文中的数据字节数 • Sequence 表示报文序号，用来判断报文是否有分组丢失、失序或重复 • ttl 表示 ICMP 响应报文中的 TTL 值 • time 表示响应时间
Record Route	ICMP回显请求报文经过的路由器，采用倒序显示，距离目的端越近的路由器越先显示
--- 10.1.1.5 ping statistics ---	Ping操作中收发数据的统计结果
5 packet(s) transmitted	发送的ICMP回显请求报文数
5 packet(s) received	接收的ICMP响应报文数
0.00% packet loss	未响应请求报文占发送的总请求报文的百分比

字段	描述
round-trip min/avg/max = 12/13/20 ms	响应时间的最小值、平均值和最大值，单位为ms（对于IPv4网络ping失败的时候不会打印该信息；对于IPv6网络ping失败的时候会打印round-trip min/avg/max = 0/0/0 ms）

1.1.2 ping ipv6

【命令】

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout | -vpn-instance vpn-instance-name ] * host [ -i interface-type interface-number ]
```

【视图】

任意视图

【缺省级别】

0: 访问级

【参数】

-a source-ipv6: 指定 ICMP 回显请求报文中的源 IPv6 地址。该地址必须是设备上已配置的合法 IPv6 地址。不指定该参数时，ICMP 回显请求报文的源 IPv6 地址是该报文出接口的主 IPv6 地址。

-c count: 指定发送的 ICMPv6 回显请求报文的数目，取值范围为 1~4294967295，缺省值为 5。

-m interval: 指定发送 ICMPv6 回显请求报文的时间间隔，取值范围为 1~65535，单位为毫秒，缺省值为 200 毫秒。

- 如果在 *timeout* 时间内收到目的主机的响应报文，则下次 ICMP 回显请求报文的发送时间间隔为报文的实际响应时间与 *interval* 之和；
- 如果在 *timeout* 时间内没有收到目的主机的响应报文，则下次 ICMP 回显请求报文的发送时间间隔为 *timeout* 与 *interval* 之和。

-s packet-size: 指定发送的 ICMPv6 回显请求报文的长度，取值范围为 20~8100，单位为字节，缺省值为 56 字节。

-t timeout: 指定 ICMPv6 回显应答报文的超时时间，取值范围为 0~65535，单位为毫秒，缺省值为 2000 毫秒。

host: 目的端的 IPv6 地址或主机名，为 1~46 个字符的字符串。

-i interface-type interface-number: 指定出接口的接口类型与接口编号。此参数只用于目的地址是链路本地地址的情况，而且指定的出接口必需具有链路本地地址（链路本地地址的介绍和配置请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”）。不指定该参数时，将根据目的 IP 查找路由表或者转发表来确定发送 ICMP 回显请求报文的接口。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

【描述】

ping ipv6 命令用来检查指定 IPv6 地址是否可达，并输出相应的统计信息。

需要注意的是：

如果要使用目的端的主机名执行 ping 操作，事先必须在设备上配置 DNS（Domain Name System，域名系统）功能，否则会 ping 失败，DNS 的相关介绍和配置请参见“三层技术-IP 业务配置指导”中的“IPv6 域名解析”。当目的端的名称是 **ipv6** 时，命令形式应该是 **ping ipv6 ipv6**，而不能直接输入 **ping ipv6**。

在执行命令过程中，键入<Ctrl+C>可终止 ping ipv6 操作。

【举例】

检查 IPv6 地址为 2001::2 的设备是否可达。

```
<Sysname> ping ipv6 2001::2
PING 2002::2 : 56 data bytes, press CTRL_C to break
  Reply from 2002::2
    bytes=56 Sequence=1 hop limit=64 time = 117 ms
  Reply from 2002::2
    bytes=56 Sequence=2 hop limit=64 time = 22 ms
  Reply from 2002::2
    bytes=56 Sequence=3 hop limit=64 time = 24 ms
  Reply from 2002::2
    bytes=56 Sequence=4 hop limit=64 time = 37 ms
  Reply from 2002::2
    bytes=56 Sequence=5 hop limit=64 time = 29 ms
--- 2002::2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 22/45/117 ms
```

检查 vpn1 中 IPv6 地址为 2001::1 的设备是否可达。

```
<Sysname> ping ipv6 -vpn-instance vpn1 2001::1
PING 2001::1 : 56 data bytes, press CTRL_C to break
  Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64 time = 62 ms
  Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64 time = 26 ms
  Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64 time = 20 ms
  Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64 time = 4 ms
  Reply from 2001::1
    bytes=56 Sequence=5 hop limit=64 time = 16 ms
--- 2001::2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/25/62 ms
```

该显示信息中的“hop limit”字段与IPv4 ping命令显示信息中的“ttl”字段含义相同，均表示ICMP回显请求报文中的TTL值。其它字段的信息请参见 [表 1-1](#)。

1.1.3 tracert

【命令】

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout ] * host
```

【视图】

任意视图

【缺省级别】

0: 访问级

【参数】

-a source-ip: 指定 tracert 报文的源 IP 地址。该地址必须是设备上已配置的合法 IP 地址。不指定该参数时，tracert 报文的源 IP 地址是该报文出接口的主 IP 地址。

-f first-ttl: 指定一个初始 TTL，即第一个报文所允许的跳数。取值范围为 1~255，且小于最大 TTL，缺省值为 1。

-m max-ttl: 指定一个最大 TTL，即一个报文所允许的最大跳数。取值范围为 1~255，且大于初始 TTL，缺省值为 30。

-p port: 指定目的端的 UDP 端口号，取值范围为 1~65535，缺省值为 33434。用户一般不需要更改此选项。

-q packet-number: 指定每次发送的探测报文个数，取值范围为 1~65535，缺省值为 3。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

-w timeout: 指定探测报文的响应报文的超时时间，取值范围是 1~65535，单位为毫秒，缺省值为 5000 毫秒。

host: 目的端的 IP 地址或主机名，主机名为 1~255 个字符的字符串。

【描述】

tracert 命令用来查看 IPv4 报文从源端传到目的端所经过的路径。

当用户使用 **ping** 命令测试发现网络出现故障后，可以用 **tracert** 命令分析出现故障的网络节点。

tracert 命令的输出信息包括到达目的端所经过的所有三层设备的 IP 地址，如果某路由器超时，则输出“* * * *”。

在执行命令过程中，键入<Ctrl+C>可终止此次 **tracert** 操作。

【举例】

查看报文从源端到目的端（IP 地址为 1.1.2.2）所经过的路径。

```
<Sysname> tracert 1.1.2.2
  traceroute to 1.1.2.2(1.1.2.2) 30 hops max,40 bytes packet, press CTRL_C to break
  1  1.1.1.2 673 ms 425 ms 30 ms
  2  1.1.2.2 580 ms 470 ms 80 ms
```

查看报文从源端到目的端（IP 地址为 192.168.0.46）所经过的路径（路中途经 MPLS 网络）。

```
<Sysname> tracert 192.168.0.46
  traceroute to 192.168.0.46(192.168.0.46) 30 hops max,40 bytes packet, press CTRL_C to break
```



```

1 192.0.2.13 (192.0.2.13) 0.661 ms 0.618 ms 0.579 ms
2 192.0.2.9 (192.0.2.9) 0.861 ms 0.718 ms 0.679 ms
  MPLS Label=100048 Exp=0 TTL=1 S=1
3 192.0.2.5 (192.0.2.5) 0.822 ms 0.731 ms 0.708 ms
  MPLS Label=100016 Exp=0 TTL=1 S=1
4 192.0.2.1 (192.0.2.1) 0.961 ms 8.676 ms 0.875 ms

```

表1-2 **tracert** 命令显示信息描述表

字段	描述
tracert to 1.1.2.2(1.1.2.2)	查看IP报文从当前设备传到地址为1.1.2.2的设备所经过的路径
hops max	探测报文的最大跳数，可使用 -m 参数配置
bytes packet	探测报文字节数
press CTRL_C to break	在执行命令过程中，键入<Ctrl+C>可终止此次 tracert 操作
1 1.1.1.2 673 ms 425 ms 30 ms	TTL值为1的探测报文的探测结果，内容包括：第一跳的IP地址、三份探测报文的往返时间 每次发送探测报文的份数可以使用 -q 参数配置
MPLS Label=100048 Exp=0 TTL=1 S=1	当源端到目的端途经MPLS网络时，ICMP超时报文中会携带MPLS标签信息： <ul style="list-style-type: none"> • Label: 标签值，用来标识一个 FEC • Exp: 保留，协议中没有明确规定，通常用作服务等级 • TTL: TTL 值 • S: MPLS 支持多重标签，值为 1 时表示此标签为最底层标签，值为 0 时表示此标签为其它层标签

1.1.4 tracert ipv6

【命令】

```
tracert ipv6 [-f first-ttl] [-m max-ttl] [-p port] [-q packet-number] [-vpn-instance vpn-instance-name] [-w timeout] * host
```

【视图】

任意视图

【缺省级别】

0: 访问级

【参数】

-f first-ttl: 指定一个初始 TTL，即第一个报文所允许的跳数。取值范围为 1~255，且小于最大 TTL，缺省值为 1。

-m max-ttl: 指定一个最大 TTL，即一个报文所允许的最大跳数。取值范围为 1~255，且大于初始 TTL，缺省值为 30。

-p port: 指定目的端的 UDP 端口号，取值范围为 1~65535，缺省值为 33434。用户一般不需要更改此选项。

-q packet-number: 指定每次发送的探测报文个数，取值范围为 1~65535，缺省值为 3。

-w timeout: 指定探测报文的响应报文的超时时间，取值范围为 1~65535，单位为毫秒，缺省值为 5000 毫秒。

host: 目的端的 IPv6 地址或主机名，为 1~46 个字符的字符串。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

【描述】

tracert ipv6 命令用来查看 IPv6 报文从源端传到目的端所经过的路径。

当用户使用 **ping** 命令测试发现网络出现故障后，可以用 **tracert** 命令分析出现故障的网络节点。本命令的输出信息包括到达目的端所经过的所有三层设备的 IP 地址，如果某设备超时，则输出“* * *”。

在执行命令过程中，键入<Ctrl+C>可终止此次 **tracert** 操作。

【举例】

查看报文从源端到目的端（IPv6 地址为 2001::1）所经过的路径。

```
<Sysname> tracert ipv6 2001::1
  traceroute to 2001::1 30 hops max,60 bytes packet, press CTRL_C to break
  1 2001::1 3 ms <1 ms 19 ms
```

查看报文从源端到目的端（假设目的端处于 vpn1 中，IPv6 地址为 2001::1）所经过的路径。

```
<Sysname> tracert ipv6 -vpn-instance vpn1 2001::1
  traceroute to 2001::1 30 hops max,60 bytes packet, press CTRL_C to break
  1 2001::1 3 ms <1 ms 19 ms
```

上述显示信息中各字段的含义请参见 [表 1-2](#)。

1.2 系统调试命令

1.2.1 debugging

【命令】

```
debugging { all [ timeout time ] | module-name [ option ] }
undo debugging { all | module-name [ option ] }
```

【视图】

用户视图

【缺省级别】

1: 监控级

【参数】

all: 所有的调试开关。

timeout time: 指定 **debugging all** 命令的生效时间。当使用 **all** 参数开启了所有的调试开关，则经过 *time* 时间，系统会自动执行 **undo debugging all** 命令来关闭所有的调试开关。取值范围为 1~1440，单位为分钟。

module-name: 功能模块的名称，比如 arp、device 等。可以使用 **debugging ?** 命令匹配出设备当前支持的模块名。

option: 模块中的调试选项。对于不同的模块，调试选项的数量和内容都不相同。可以使用 **debugging module-name ?** 匹配出设备当前支持的指定模块的调试选项。

【描述】

debugging 命令用来打开设备支持的功能项的调试开关。**undo debugging** 命令用来关闭设备支持的功能项的调试开关。

缺省情况下，所有功能项的调试开关均处于关闭状态。

需要注意的是：

- 由于调试信息的输出会影响系统的运行效率，所以建议在需要进行网络故障诊断时根据需要打开相应功能模块调试开关，不要同时打开多个功能模块的调试开关。
- 【缺省级别】描述的是 **debugging all** 的缺省级别，不同功能项 **debugging** 命令的缺省级别可能不同。
- 只有同时配置了 **debugging**、**terminal debugging** 和 **terminal monitor** 命令，才能在终端显示调试信息的具体内容。**terminal debugging** 和 **terminal monitor** 命令的详细介绍请参见“网络管理和监控命令参考”中的“信息中心”。

相关配置可参考命令 **display debugging**。

【举例】

打开 IP 模块中 Packet 选项的调试开关。

```
<Sysname> debugging ip packet
```

1.2.2 display debugging

【命令】

```
display debugging [ interface interface-type interface-number ] [ module-name ] [ | { begin | exclude | include } regular-expression ]
```

【视图】

任意视图

【缺省级别】

1: 监控级

【参数】

interface interface-type interface-number: 显示指定接口调试开关的设置情况，*interface-type interface-number* 表示接口类型和接口编号。

module-name: 功能模块的名称。

|: 使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin: 从包含指定正则表达式的行开始显示。

exclude: 只显示不包含指定正则表达式的行。

include: 只显示包含指定正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【描述】

display debugging 命令用来显示系统中已经打开的调试开关。

相关配置可参考命令 **debugging**。

【举例】

显示所有打开的调试开关。

```
<Sysname> display debugging
```

```
IP packet debugging is on
```