Contents

Ping, tracert, and system debugging commands

debugging

Use **debugging** to enable debugging for a module.

Use **undo debugging** to disable debugging for a module or for all modules.

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

Default

Debugging is disabled for all modules.

Views

User view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name, such as **arp** or **device**. For a list of supported modules, use the **debugging ?** command.

option: Specifies the debugging option for a module. Available options vary by module. To display the debugging options supported by a module, use the **debugging** *module-name* **?** command.

all: Specifies all modules.

Usage guidelines

Output from debugging commands is memory intensive. To guarantee system performance, enable debugging only for modules that are in an exceptional condition.

In an IRF 3.1 system, PEXs do not send debugging information to the parent fabric. To debug a PEX, use the **switchto pex** command to log in to the PEX and then enable the debugging functions as needed. For more information about the **switchto pex** command, see IRF 3.1 commands in *Virtual Technologies Command Reference*.

The system sends generated debug messages to the device information center, which then sends the messages to appropriate destinations based on the log output configuration. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable debugging for the device management module.

```
<Sysname> debugging dev
```

Related commands

display debugging

display debugging

Use **display debugging** to display the enabled debugging features for a module or for all modules.

Syntax

display debugging [*module-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

module-name: Specifies a module by its name. For a list of supported modules, use the **display debugging ?** command. If you do not specify a module name, this command displays the enabled debugging features for all modules.

Examples

Display all enabled debugging features.

```
<Sysname> display debugging
DEV debugging switch is on
```

Related commands

debugging

ping

Use **ping** to test the reachability of the destination IP address and display ping statistics.

Syntax

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*

Views

Any view

Predefined user roles

network-admin

Parameters

ip: Distinguishes between a destination host name and the **ping** command keywords if the name of the destination host is **i**, **ip**, **ipv**, **ipv6**, **l**, **ls**, or **lsp**. For example, you must use the command in the form of **ping ip ip** instead of **ping ip** if the destination host name is **ip**.

-a *source-ip*: Specifies an IP address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IP address of ICMP echo requests is the primary IP address of the outbound interface.

-c *count*: Specifies the number of ICMP echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-f: Sets the "Don't Fragment" bit in the IP header.

-h *ttl*: Specifies the TTL value of ICMP echo requests. The value range is 1 to 255, and the default is 255.

-i *interface-type interface-number*: Specifies the source interface for ICMP echo requests. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMP echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send ICMP echo requests. The value range is 1 to 65535, and the default is 200.

-n: Disables domain name resolution for the *host* argument. If the *host* argument represents the host name of the destination, and if this keyword is not specified, the device translates *host* into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits. The *pad* argument is in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, such as 0x010203…feff01….

-q: Displays only the summary statistics. If this keyword is not specified, the system displays all the ping statistics.

-r: Records the addresses of the hops (up to 9) the ICMP echo requests passed. If this keyword is not specified, the addresses of the hops that the ICMP echo requests passed are not recorded.

-s *packet-size*: Specifies the length (in bytes) of ICMP echo requests (excluding the IP packet header and the ICMP packet header). The value range is 20 to 9600, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMP echo reply. The value range is 0 to 65535, and the default is 2000. If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out.

-tos *tos*: Specifies the ToS value of ICMP echo requests. The value range is 0 to 255, and the default is 0.

-v: Displays non-ICMP echo reply packets. If this keyword is not specified, the system does not display non-ICMP echo reply packets.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the ping operation fails.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Sysname> ping 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
```

```
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 in VPN instance **vpn1** is reachable.

```
<Sysname> ping -vpn-instance vpn1 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. Only results are displayed.

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

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. The IP addresses of the hops that the ICMP packets passed in the path are displayed.

```
<Sysname> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:      1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

The output shows the following information:

- The destination is reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 1 Command output

Field	Description
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	Test whether the device with IP address 1.1.2.2 is reachable. There are 56 bytes in each ICMP echo request. Press **Ctrl+C** to abort the ping operation.
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	Received ICMP echo replies from the device whose IP address is 1.1.2.2. If no echo reply is received within the timeout period, no information is displayed. • **bytes**—Number of bytes in the ICMP echo reply. • **icmp_seq**—Packet sequence, used to determine whether a segment is lost, disordered or repeated. • **ttl**—TTL value in the ICMP echo reply. • **time**—Response time.
RR:	Routers through which the ICMP echo request passed. They are displayed in inversed order, which means the router with a smaller distance to the destination is displayed first.
--- Ping statistics for 1.1.2.2 ---	Statistics on data received and sent in the ping operation.
--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---	Ping statistics for a device in a VPN instance.
5 packet(s) transmitted	Number of ICMP echo requests sent.
5 packet(s) received	Number of ICMP echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

ping ipv6

Use **ping ipv6** to test the reachability of the destination IPv6 address and display IPv6 ping statistics.

Syntax

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

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ipv6*: Specifies an IPv6 address of the device as the source IP address of ICMP echo requests. If this option is not specified, the source IPv6 address of ICMP echo requests is the IPv6 address of the outbound interface. See RFC 3484 for information about the address selection rule.

-c *count*: Specifies the number of ICMPv6 echo requests that are sent to the destination. The value range is 1 to 4294967295, and the default is 5.

-i *interface-type interface-number*: Specifies the source interface for ICMPv6 echo requests. This option must be specified when the destination address is a multicast address or a link

local address. If you do not specify this option, the system uses the primary IP address of the matching route's egress interface as the source interface for ICMPv6 echo requests.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply. The value range is 1 to 65535, and the default is 1000.

-q: Displays only the summary statistics. If you do not specify this keyword, the system displays all the ping statistics.

-s *packet-size*: Specifies the length (in bytes) of ICMPv6 echo requests (excluding the IPv6 packet header and the ICMPv6 packet header). The value range is 20 to 9600, and the default is 56.

-t *timeout*: Specifies the timeout time (in milliseconds) of an ICMPv6 echo reply. The value range is 0 to 65535, and the default is 2000.

-tc *traffic-class*: Specifies the traffic class value in an ICMPv6 packet. The value range is 0 to 255 and the default is 0.

-v: Displays detailed information (including the **dst** field and the **idx** field) about ICMPv6 echo replies. If this keyword is not specified, the system only displays brief information (not including the **dst** field and the **idx** field) about ICMPv6 echo replies.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

To ping a device identified by its host name, configure the DNS settings on the device first. If the DNS settings are not configured, the IPv6 ping operation fails.

To abort the IPv6 ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the IPv6 address (2001::2) is reachable.

```
<Sysname> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Only the statistics are displayed.

```
<Sysname> ping ipv6 –q 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Test whether the IPv6 address (2001::2) is reachable. Detailed ping information is displayed.

```
<Sysname> ping ipv6 –v 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 dst=2001::1 idx=3 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 dst=2001::1 idx=3 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 dst=2001::1 idx=3 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 dst=2001::1 idx=3 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

Table 2 Command output

Field	Description
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break	An ICMPv6 echo reply with a data length of 56 bytes is sent from 2001::1 to 2001::2. Press **Ctrl+C** to abort the IPv6 ping operation.
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	Received ICMPv6 echo replies from the device whose IPv6 address is 2001::2. • The number of data bytes is 56. • The packet sequence is 1. • The hop limit value is 64. • The destination address is 2001::1. Specify the **-v** keyword to display this field. • The index for the packet inbound interface is 3. Specify the **-v** keyword to display this field. • The response time is 62 milliseconds.
--- Ping6 statistics for 2001::2 ------	Statistics on data received and sent in an IPv6 ping operation.
5 packet(s) transmitted	Number of ICMPv6 echo requests sent.
5 packet(s) received	Number of ICMPv6 echo replies received.
0.0% packet loss	Percentage of unacknowledged packets to the total packets sent.
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	Minimum/average/maximum/standard deviation response time, in milliseconds.

tracert

Use **tracert** to trace the path that the packets traverse from source to destination.

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-vpn-instance** *vpn-instance-name* [**-resolve-as** { **global** | **none** | **vpn** }] | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-a *source-ip*: Specifies an IP address of the device as the source IP address of probe packets. If this option is not specified, the source IP address of probe packets is the primary IP address of the outbound interface.

-f *first-ttl*: Specifies the TTL of the first packet sent to the destination. The value range is 1 to 255, and the default is 1. It must be no greater than the value of the *max-ttl* argument.

-m *max-ttl*: Specifies the maximum number of hops allowed for a probe packet. The value range is 1 to 255, and the default is 30. It must be no smaller than the value of the *first-ttl* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets to send per hop. The value range is 1 to 65535, and the default is 3.

-t *tos*: Specifies the ToS value of probe packets. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-resolve-as: Specifies a routing table for autonomous system (AS) resolution. Tracert searches the specified routing table for the AS that each hop along the path belongs to. If you do not specify this keyword, the global routing table is used. If the AS information is found, this command displays the AS number next to the address of the hop in the probe result.

- **global**: Specifies the global routing table.
- **none**: Disables AS resolution.
- **vpn**: Specifies the VPN routing table.

-w *timeout*: Specifies the timeout time in milliseconds of the reply packet for a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IP address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping** command, use the **tracert** command to locate failed nodes.

If the destination address is on the public network, you do not need to specify the **-resolve-as** keyword to obtain the AS information. The device automatically uses the global routing table for AS resolution.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table or the VPN routing table. To learn the AS path that the packets traverse, execute the **tracert** command twice, once with the **-resolve-as global** keywords and again with the **-resolve-as vpn** keywords.

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting a tracert operation, you must enable sending of ICMP destination unreachable messages on the intermediate devices between the source and destination. The tracert operation stops if any one of the following ICMP destination unreachable messages is received:

- **!N**—Network unreachable.

- **!H**—Destination host unreachable.
- !**P**—Protocol unreachable. The protocol number is unknown.
- **!F**—Fragmentation needed. This message indicates that packet fragmentation is needed but the "Don’t Fragment" bit is set on an immediate device.
- **!W**—Destination host unknown.
- **!Q**—Network unreachable for ToS.
- **!T**—Host unreachable for ToS.
- **!X**—Communication administratively prohibited by filtering policies.
- **!V**—Host precedence violation.
- **!C**—Precedence cutoff in effect.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (1.1.2.2).

```
<Sysname> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

Display the path that the packets traverse from source to destination (1.1.3.2) in VPN instance vpn1, as well as the AS information of the hops along the path.

```
<Sysname> tracert –vpn-instance vpn1 –resolve-as vpn 1.1.3.2
traceroute to 1.1.3.2 (1.1.3.2), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms
 3  1.1.3.2 (1.1.3.2) [AS 65535] 530 ms 472 ms 380 ms
```

Trace the path to destination (192.168.0.46) over an MPLS network.

```
<Sysname> tracert 192.168.0.46
traceroute to 192.168.0.46(192.168.0.46), 30 hops at most, 40 bytes each 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
```

Table 3 Command output

Field	Description
traceroute to 1.1.2.2 (1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
bytes each packet	Number of bytes of a probe packet.
press CTRL_C to break	During the execution of the command, press **Ctrl+C** to abort the tracert operation.

Field	Description
2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	Probe result of the probe packets that contain a TTL value of 2, including the following information about the second hop: • Domain name of the hop. If no domain name is configured, the IP address is displayed as the domain name. • IP address of the hop. The IP address is displayed in parentheses. • Number of the AS that the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.
MPLS Label=100048 Exp=0 TTL=1 S=1	ICMP timeout packets on an MPLS network, carrying MPLS label information: • **Label**—Label value that is used to identify a forwarding equivalence class (FEC). • **Exp**—Reserved, usually used for class of service (CoS). • **TTL**—TTL value. • **S**—MPLS supports multiple levels of labels. Value 1 indicates that the label is at the bottom of the label stack, and value 0 indicates that the label is in another label stack.

tracert ipv6

Use **tracert ipv6** to display the path that the IPv6 packets traverse from source to destination.

Syntax

tracert ipv6 [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-t** *traffic-class* | **-vpn-instance** *vpn-instance-name* [**-resolve-as** { **global** | **none** | **vpn** }] | **-w** *timeout*] * *host*

Views

Any view

Predefined user roles

network-admin

Parameters

-f *first-hop*: Specifies the TTL value of the first packet. The value range is 1 to 255, and the default is 1. The value must be no greater than the value of the *max-hops* argument.

-m *max-hops*: Specifies the maximum number of hops allowed for a packet. The value range is 1 to 255, and the default is 30. The value must be no smaller than the value of the *first-hop* argument.

-p *port*: Specifies an invalid UDP port of the destination. The value range is 1 to 65535, and the default is 33434.

-q *packet-number*: Specifies the number of probe packets sent each time. The value range is 1 to 65535, and the default is 3.

-t *traffic-class*: Specifies the traffic class value in an IPv6 probe packet. The value range is 0 to 255, and the default is 0.

-vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance to which the destination belongs. The *vpn-instance-name* argument represents the VPN instance name, a

case-sensitive string of 1 to 31 characters. If the destination is on the public network, do not specify this option.

-resolve-as: Specifies a routing table for AS resolution. Tracert searches the specified routing table for the AS that each hop along the path belongs to. If you do not specify this keyword, the global routing table is used. If the AS information is found, this command displays the AS number next to the address of the hop in the probe result.

- **global**: Specifies the global routing table.
- **none**: Disables AS resolution.
- **vpn**: Specifies the VPN routing table.

-w *timeout*: Specifies the timeout time (in milliseconds) of the reply packet of a probe packet. The value range is 1 to 65535, and the default is 5000.

host: Specifies the IPv6 address or host name of the destination. The host name is a case-insensitive string of 1 to 253 characters. It can contain letters, digits, and special characters such as hyphen (-), underscore (_), and dot (.).

Usage guidelines

After identifying network failure with the **ping ipv6** command, you can use the **tracert ipv6** command to locate failed nodes.

If the destination address is on the public network, you do not need to specify the **-resolve-as** keyword to obtain the AS information. The device automatically uses the global routing table for AS resolution.

If the destination address is on a private network, address information of intermediate hops might be stored in either the global routing table or the VPN routing table. To learn the AS path that the packets traverse, execute the **tracert ipv6** command twice, once with the **-resolve-as global** keywords and again with the **-resolve-as vpn** keywords.

The output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message. The reason might be the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled.

Before starting an IPv6 tracert operation, you must enable sending of ICMPv6 destination unreachable messages on the intermediate devices between the source and destination. The IPv6 tracert operation stops if any one of the following ICMPv6 destination unreachable messages is received:

- **!N**—No route to destination.
- **!P**—Communication with destination administratively prohibited by filtering policies.
- **!A**—Address unreachable. The unreachable reason is unknown.
- **!S**—Beyond scope of source address. This message is displayed if the probe packet has a link-local source address and a non-link-local destination address. Such a packet cannot be delivered to the destination without leaving the scope of the source address.

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination (2001:3::2).

```
<Sysname> tracert ipv6 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets, press CTRL_C to break
 1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
 2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
 3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

Display the path that the packets traverse from source to destination (2001:3::2) in VPN instance vpn1, as well as the AS information of the hops along the path.

```
<Sysname> tracert ipv6 –vpn-instance vpn1 –resolve-as vpn 2001:3::2
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets , press CTRL_C to break
1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
2  2001:2::2  0.861 ms  0.718 ms  0.679 ms
3  2001:3::2 [AS 65535]  0.822 ms  0.731 ms  0.708 ms
```

Table 4 Command output

Field	Description
traceroute to 2001:3::2	Display the route that the IPv6 packets traverse from the current device to the device whose IP address is 2001:3:2.
hops at most	Maximum number of hops of the probe packets, which can be set by the **-m** keyword.
byte packets	Number of bytes of a probe packet.
2 2001:2::2 [AS 100] 0.861 ms 0.718 ms 0.679 ms	Probe result of the probe packets that contain a hoplimit value of 2, including the following information about the second hop: • IPv6 address of the hop. • Number of the AS the hop belongs to. The AS number appears only when it is found for the hop in the specified routing table. • The round-trip time of the probe packets. The number of packets that can be sent in each probe can be set by using the **-q** keyword.